認 証 報 告 書

独立行政法人情報処理推進機構
理事長　富田　達夫

原紙押印済

評価対象

申請受付日（受付番号）	平成26年4月8日 (IT認証4503)
認証番号	C0513
認証申請者	株式会社 日立製作所
TOEの名称	Hitachi Unified Storage VM用制御プログラム
TOEのバージョン	73-03-09-00/00(H7-03-10_Z)
PP適合	なし
適合する保証パッケージ	EAL2 及び追加の保証コンポーネントALC_FLR.1
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28年6月1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4
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4

評価結果：合格

「Hitachi Unified Storage VM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 VM 用制御プログラム バージョン 73-03-09-00/00(H7-03-10_Z)」(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 28 年 4 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、本 TOE を購入する調達者、一般消費者、及び Hitachi Data Systems Corporation 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 及び追加の保証コンポーネント ALC_FLR.1 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、Hitachi Unified Storage VM ディスクストレージ装置(以下「ストレージ装置」という。)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。)からストレージ装置の記憶装置へのアクセス要求を受け、ホストと記憶装置の間のデータのやりとりを制御する。ホストからはそのホストに対して定められた記憶領域のみにアクセスできるように、本 TOE は、ホストの識別、アクセス制御の機能を提供する。

本 TOE は、記憶装置からのデータの漏えいの防止のため、記憶装置へのダミーデータの上書きによる消去の機能と、記憶装置へ書き込まれるデータの暗号化を支援する機能を提供する(暗号化機能はストレージ装置のハードウェアが提供する)。

本 TOE は、調達者の要求に応じるため、ファイバチャネルスイッチを識別・認証する機能を提供する。

これらの機能を有効に動作させるため、本 TOE は、これらの機能に関連する設定等の管理を特定の役割の者に制限する機能を提供する。

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、ホストに割り当てられたストレージ装置の記憶領域が別のホストから閲覧されたり改ざんされたりすることを防ぐために、ホストの識別とアクセス制御を実施する。そうすることで、記憶領域を割り当てられたホストのみ、その記憶領域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､ストレージリソース管理者、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 TLS 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とホストは、ファイバチャネルスイッチを介して接続すること。
- 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)､SAN 環境を構成する機器(ファイバチャネルスイッチ､ケーブル)、他のストレージ装置（ストレージ装置同士を接続する場合)、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。また、セキュリティ管理者は、SAN 環境の接続状態やホストの識別に関する設定が維持されるように、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環境に設置すること。
- 本 TOE と外部認証サーバの間は、LDAPS、LDAP+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。
- 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

- 特定の運用環境以外の TOE の動作は、本評価では保証されない。運用環境についての詳細は「4.2 運用環境と構成」参照。以下の場合、TOE の動作が本評価の保証対象外となることを特記事項として示す。
  - SAN 環境にファイバチャネルスイッチが複数存在する
  - SAN 環境にホストが複数存在する
  - ストレージ装置のポートに他のディスクストレージ装置を接続する
- 本 TOE と外部認証サーバの間のプロトコルとして Kerberos(v5)の利用も可能であるが、その場合の認証の安全性は保証の対象外である。
- ストレージ装置にはユーザデータを暗号化して記憶装置へ保存する機能があるが、その暗号化の機能は本評価では保証されない。暗号化はストレージ装置に搭載される LSI により実施され、その LSI は TOE の範囲外である。
- 海外への配付の場合、本評価で TOE の配付の安全性が保証されるのは、海外への本 TOE を販売する会社である Hitachi Data Systems Corporation への受け渡しまでである。

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 28 年 4 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 Unified Storage VM用制御プログラム
バージョン： 73-03-09-00/00(H7-03-10_Z)
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、利用者は以下の方法によって確認することができる。

- 国内への配付の場合

  製品が格納されている 4 枚の CD-R のラベルに、それぞれの識別情報が記載されている。エンドユーザ（実際に TOE を使用する調達者、一般消費者）は、ガイダンスの記載に従いそれぞれの識別情報を確認することにより、製品が評価を受けた本 TOE であることを確認できる。

- 海外への配付の場合

  Hitachi Data Systems Corporation は、開発者からのメールに記載された情報（ファイル名称やハッシュ値）に基づき、別途取得したファイル群が本 TOE であることを確認できる。

  評価を受けた本 TOE であることをエンドユーザ（実際に TOE を使用する調達者、一般消費者）に伝えるのは Hitachi Data Systems Corporation の責任となる。

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と目的は以下のとおりである。

- ホストの識別とアクセス制御により、ホスト経由のユーザデータの改ざんや漏えいを防止する。
- 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り、取り出した記憶装置上からの漏えいを防止する。
- ファイバチャネルスイッチを識別・認証することにより、調達者から求められる要求を満足する
- 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。
- 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 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　想定する脅威

識別子	脅威
T.TSF_COMP	第三者が、外部LANから不正にストレージ管理者のIDとパスワードなどを含む通信データを取得することにより、ストレージ管理者になりすましてディスクストレージ装置の設定を変更し、ユーザデータが格納されているLDEV（論理ボリューム）にアクセスできてしまうかもしれない。
T.LP_LEAK	複数のホストが同一ポートに接続するSAN環境で、第三者が、他のホストから特定ホストのLDEV（論理ボリューム）にアクセスすることにより、ユーザデータの漏洩、改ざん、削除が行えるかもしれない。 本評価で想定する動作環境においては、ホストを異なるWWNを持つホストに繋ぎ変えた場合、またはホストのWWNを変更した場合、他のホストが接続されたことになる。
T.CHG_CONFIG	第三者が、ディスクストレージ装置のLDEV（論理ボリューム）へのアクセス設定を不正に変更することにより、ユーザデータの漏洩、改ざん、削除が行えるかもしれない。
T.HDD_THEFT	予防保守や故障のため、ディスクドライブをベンダに返却する際、そのディスクドライブの搬送中に盗難され、ユーザデータが漏えいするかもしれない。
T.HDD_REUSE	ディスクストレージ装置の再使用または、ディスクドライブの再使用により、ディスクドライブ内に残っているユーザデータが第三者に漏洩するかもしれない。

3.1.1.2　脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 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。

(1) 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 間の通信路及び 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 とパスワード及びグループ情報は、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。

⑵ 脅威「T.LP_LEAK」への対抗

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。

⑶ 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 利用者及び保守員を識別・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。

⑷ 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記憶装置から、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記憶装置へ保存したり、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｡記憶装置上のユーザデータは常に暗号化されており、その記憶装置が取り出されても、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。

(5) 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記憶装置を再使用した場合、記憶装置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記憶装置上の記憶領域の使用を停止する時やストレージ装置の記憶装置を交換する時に、該当する記憶領域のユーザデータを上書き消去し、取り出した記憶装置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 3-2 に示す。

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.MASQ	顧客要求によってホストが接続されるファイバチャネルスイッチの認証が求められる場合は、ホストが接続されるファイバチャネルスイッチの識別・認証が行われる。

この方針は、ストレージ装置に接続するファイバチャネルスイッチの制限を、ストレージ装置を運用する調達者が要求する場合があるという想定から導かれる。

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 3-2 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、ファイバチャネルスイッチの認証を行う。ファイバチャネルスイッチの認証が求められる場合は、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。

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.NOEVIL	ストレージ管理者のうち、セキュリティ管理者、監査ログ管理者は、ディスク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、不正行為を働かないことを信頼できるものと想定する。 ストレージリソース管理者は、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、不正行為を働かないことを信頼できるものと想定する。
A.PHYSICAL_SEC	セキュリティ管理者は、ディスクストレージ装置、ホスト(ファイバチャネル接続アダプタを含む)、SAN環境を構成する機器(ファイバチャネルスイッチ、ケーブル)、他のディスクストレージ装置、外部認証サーバを入退室が管理されたセキュアなエリアに設置し、各機器に設定されている設定値（WWNなど）や接続状態（SANへの接続状態）が維持されるよう適切に運用管理が行われるものと想定する。
A.MANAGE_SECRET	ホストが接続されるファイバチャネルスイッチに設定されているファイバチャネルスイッチ認証用のシークレットは、セキュリティ管理者の責任において、許可されていない人物に利用されないように管理されているものと想定する。
A.MANAGEMENT_PC	ストレージ管理者は、管理PCの不正な利用が行われないように適切に設置及び管理を行うものと想定する。

識別子	前提条件
A.MAINTENANCE_PC	組織の責任者が、保守契約を結んだ場合は、保守員と保守員PCの受入れを許可し、セキュアなエリアで保守員に入室させ、保守員に保守員PCの設置を許可する。また保守員以外の人間が保守員PCに不正に利用しないと想定する。
A.CONNECT_STORAGE	TOEに接続する他のディスクストレージ装置はTOEの搭載されているディスクストレージ装置に限定される運用を想定する。
A.EXTERNAL_SERVER	外部認証サーバは、TOEがサポートするSVP PC（管理保守IF PC）との通信を保護することができる認証プロトコル(LDAPS、LDAP+starttls、及びRADIUS（認証プロトコルはCHAP）)が利用可能であり、ユーザ識別情報及びユーザグループ情報をTOEと整合の取れた状態で適切に登録及び管理できるものと想定する。

4.2 運用環境と構成

本 TOE が搭載されたストレージ装置(内部 LAN と保守員 PC を含む)、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、不正な利用が行われないように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 の保証の対象となる運用環境を図 4-1 に示す。運用環境の詳細は表 4-2 に示す。

以下に運用環境についての注意点を示す。

- ファイバチャネルスイッチとホストは各 1 台である。
- ストレージ装置とホストは、ファイバチャネルスイッチを介して接続する。
- ストレージ装置のポートに「他のディスクストレージ装置」を接続してストレージ装置間でデータのコピー等をする機能については、「他のディスクストレージ装置」は使用せず、同じストレージ装置の異なるポートを接続する。

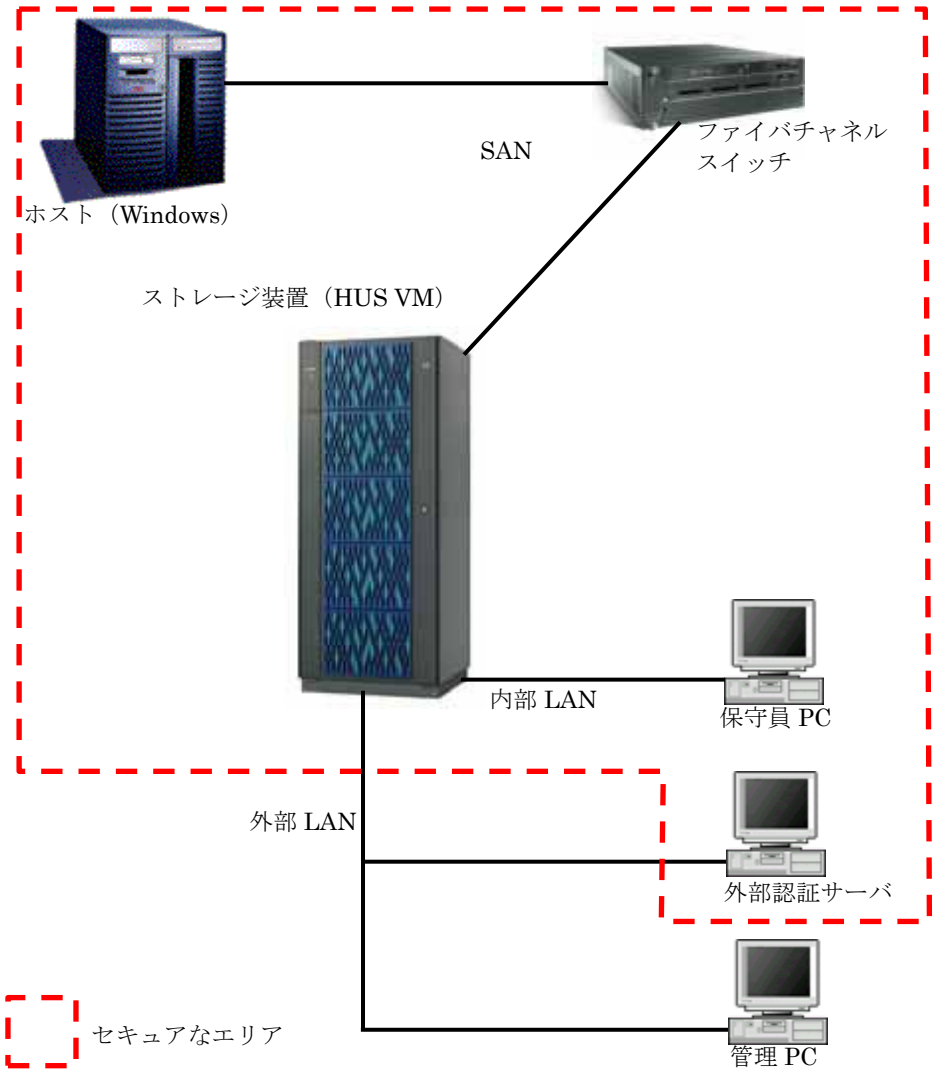


図4-1 保証の対象となるTOEの運用環境

表4-2　保証の対象となるTOEの運用環境詳細

端末・機器名	製品
ストレージ装置	Hitachi Unified Storage VM のハードウェア(詳細は以下の構成) ・ MP ブレード 2 台 ・ CHB 4 台 ・ DKB 2 台 ・ Cache 4G×16 枚 ・ 2.5 インチディスクドライブ 12 台を、RAID1(2D+2D)のパリティグループ 3 個の構成 Windows Vista Business US 版(64bit 版) SP2 (SVP PC 部分の OS)

端末・機器名	製品
ホスト	以下のソフトウェアとハードウェアを搭載したサーバ機 ・ Windows Server 2008 ・ 以下のいずれかの組み合わせ - ファイバチャネル接続アダプタ Qlogic Fibre Channel Adapter 型名 QLE2564-CK (対応するドライバ Fibre Channel Adapter STOR miniport driver 3.14.0.0) - ファイバチャネル接続アダプタ Brocade 16G FC HBA 型名 BR-1860-2P00 (対応するドライバ bfa 3.2.1.0)
ファイバチャネルスイッチ	以下のいずれか ・ Brocade300 型名 BR-360-0008 (ファームウェア Fabric OS v6.4.1b) ・ Brocade6505 型名 ER-7000-0340 (ファームウェア Fabric OS v7.2.0c)
管理 PC	以下のソフトウェアを搭載した PC ・ Windows7 SP1 ・ Internet Explorer 8 ・ Flash Player 10.1 または Flash Player 16.0 ・ JRE 1.6.0_20
保守員 PC	以下のソフトウェアを搭載した PC ・ Windows7 SP1 ・ Internet Explorer 8 ・ Flash Player 10.1 ・ JRE 1.6.0_20
外部認証サーバ	以下のソフトウェアを搭載したサーバ機 ・ Windows Server 2008

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。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。

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。

4.3 運用環境におけるTOE範囲

本 TOE の以下の機能は、保証の対象外である。

- Kerberos(v5)の方式により外部認証をする機能。

5 アーキテクチャに関する情報

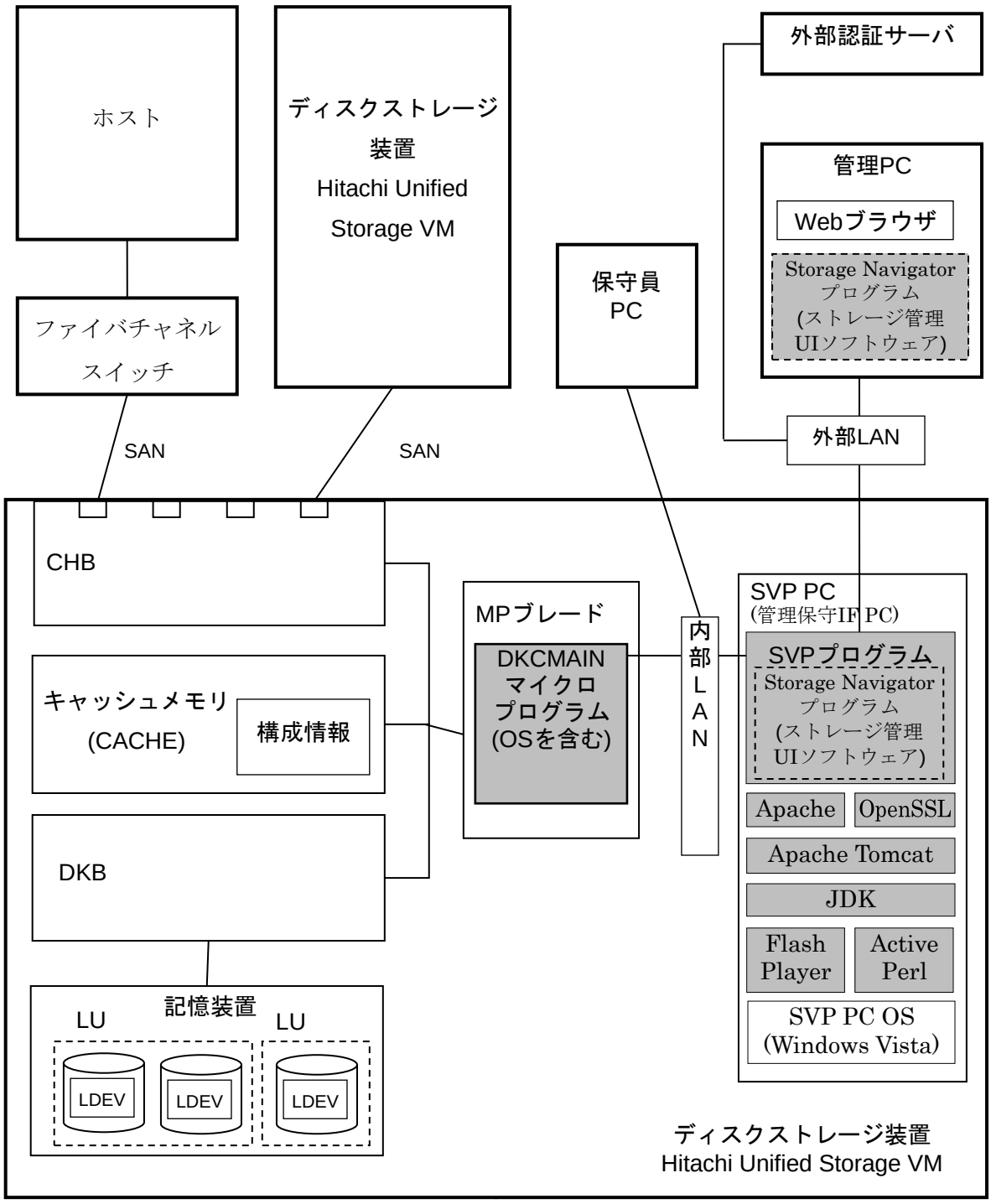
本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

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、以下のプログラムに大きく分かれる。

- MP ブレードで動作する DKCMAIN マイクロプログラム(OS を含む)
- SVP PC で動作する SVP プログラムと、SVP プログラムの動作に必要な機能を提供するプログラム群(JDK、Apache, Apache Tomcat, OpenSSL, Flash player, ActivePerl)
- 管理 PC で動作する Storage Navigator プログラム(SVP プログラムにデータとして含まれ、管理 PC に転送されて動作する)

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。



Storage Navigatorプログラム（ストレージ管理UIソフトウェア） は、Flexアプリケーションとjavaアプレットで構成され、SVP及び管理PCで動作する。

LU : 論理ユニット。ホストから使用するアクセス単位で1個または複数のLDEV(論理ボリューム)から構成される。

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 ブレード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-CHAP 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（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、及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 US 版（64bit 版) SP2) 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 TLS 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
  - 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、TLS 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、認証及び暗号化した通信を使用する。

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 及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 TLS 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、CHB、CACHE、DKB、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 6-3　ディスクサブシステムの保守マニュアル(日本語版)**」と「表 6-4 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6-1　ユーザーズガイド(日本語版)

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 Unified Storage VM ISO15408 認証取得機能 取扱説明書	2.9
2	Hitachi Unified Storage VM Storage Navigator ユーザガイド	第 8 版
3	Hitachi Unified Storage VM Storage Navigator メッセージ	第 8 版
4	Hitachi Unified Storage VM システム構築ガイド	第 10 版
5	Hitachi Unified Storage VM Encryption License Key ユーザガイド	第 2 版
6	Hitachi Unified Storage VM Volume Shredder ユーザガイド	第 4 版
7	Hitachi Unified Storage VM 監査ログ リファレンスガイド	第 6 版
8	Hitachi Unified Storage VM スプレッドシート運用ガイド	第 3 版
9	Hitachi Unified Storage VM 利用者ガイダンス	1.8

表6-2　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 Unified Storage VM Manual for Obtaining ISO15408 Certification	1.9
2	Hitachi Unified Storage VM Block Module Hitachi Storage Navigator User Guide	MK-92HM 7016-06
3	Hitachi Unified Storage VM Block Module Hitachi Storage Navigator Messages	MK-92HM 7017-03f
4	Hitachi Unified Storage VM Block Module Provisioning Guide	MK-92HM 7012-07
5	Hitachi Unified Storage VM Block Module Hitachi Encryption License Key User Guide	MK-92HM 7051-00
6	Hitachi Unified Storage VM Block Module Hitachi Volume Shredder User Guide	MK-92HM 7021-03
7	Hitachi Unified Storage VM Block Module Hitachi Audit Log User Guide	MK-92HM 7009-03d
8	Hitachi Unified Storage VM Hitachi System Operations Using Spreadsheets	MK-92HM 7015-01
9	Hitachi Unified Storage VM User's Guidance	1.5

表6-3　ディスクサブシステムの保守マニュアル(日本語版)

No	製品添付ドキュメント名（保守マニュアル）	バージョン
1	Hitachi Unified Storage VM ISO15408 認証取得機能 メンテナンスマニュアル	2.3
2	HT-40SA メンテナンスマニュアル	REV.4.5

表6-4　ディスクサブシステムの保守マニュアル(英語版)

No	製品添付ドキュメント名（保守マニュアル）	バージョン
1	Hitachi Unified Storage VM Obtaining ISO15408 Certification Maintenance Manual	1.6
2	DW700 Maintenance Manual	REV.4.5

- 「HT-40SA」「DW700」は、「Hitachi Unified Storage VM」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。「DW700 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、本 TOE に添付されず、保守員向けの文書として存在する。

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施したみずほ情報総研株式会社 情報セキュリティ評価室は、IT セキュリティ評価及び認証制度により承認されるとともに、ILAC（国際試験所認定協力機構）と相互承認している認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 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。

7.3 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 26 年 4 月に始まり、平成 28 年 4 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 26 年 8 月及び 12 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 26 年 7 月、平成 27 年 2 月、9 月、平成 28 年 2 月、及び 4 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。

7.4 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。

7.4.1 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は、以下を除き「4.2 運用環境と構成」と同じである。「4.2 運用環境と構成」の構成は、ST において保証の対象とされている構成である。

- 「4.2 運用環境と構成」において OS に選択の余地があり、開発者のテストの構成においては具体的に選択されている。(例えば、管理 PC の OS は Windows7 Professional SP1 が選択されている。) これらの選択はテストに影響しないことが評価者により判断されている。

開発者テストが対象とした TOE は「Hitachi Unified Storage VM 用制御プログラム バージョン 73-03-09-00/00(H7-03-10_Z)」である。これは、ST に記載されている TOE の識別と一致する。

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 構成と同一とみなせる 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。

本 TOE の応答を観察する手法として、以下の手法も使用した。

- ネットワークプロトコルアナライザを用いて通信パケットをキャプチャして観察した。
- ホストから記憶装置の内容をセクタ単位で観察した。

本 TOE の応答を観察することでは確認が困難なふるまいに関しては、以下の手法が用いられた。

- TOE のソースコードレビューを実施した。

＜開発者テストツール＞

開発者テストにおいて利用したツールを以下に示す。

- Wireshark 1.10.3 (利用目的はネットワークプロトコルアナライザ)

＜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、以下の確認を実施した。

- 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。
- ホストから記憶装置の内容をセクタ単位で観察し、シュレッディング機能が動作していることを確認した。

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。ファイバチャネルスイッチ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(1)の TLS 通信及び下記(4)の認証について、Wireshark を使用して通信の内容を観察し、使用されている TLS 及び認証のプロトコルが正しく実装されていることを確認した。

(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

記憶装置へ保存するデータの暗号化のための暗号鍵が正しい方法で生成されることは、上記の(1)～(4)のインタフェースを使用しての確認が難しいため、ソースコードレビューにより確認した。

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125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セキュリティ機能と外部インタフェースに対するテストのカバレージが確認された。一部の外部インタフェースに対してはカバレージが不十分と判断され、評価者独立テストで補足された。

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。

7.4.2 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

独立テストの構成は、開発者テストの構成とほぼ同じであり、一部の OS の選択が異なる。OS の選択の相違はテストに影響しないことが評価者により判断されている。独立テスト環境の構成品やテストツールは、開発者が用意したものを利用しており、それらの妥当性確認及び動作試験は、評価者によって実施されている。

評価の対象とした TOE は「Hitachi Unified Storage VM 用制御プログラム バージョン 73-03-09-00/00(H7-03-10_Z)」である。これは、ST に記載されている TOE の識別と一致する。

独立テストは、本 ST において識別されている TOE の構成と同一とみなせる環境で実施された。

(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。

開発者テストのサンプリングに関しては､すべてのインタフェースの種別やテストの手法が対象となることを考慮し、十分な量のテストを選択した。
開発者テスト及び提供された評価証拠資料から､以下の観点に基づいてテストを考案した。

① 開発者テストにより動作が確認されていないと判断したTOEのふるまいに対し、テストを補足する。
② 開発者テストに対し､テスト手順や観察を追加してTOEのふるまいの確認をより厳密にする。
③ 開発者テストで確認されているTOEのふるまいに対し､異なるパラメタやインタフェースの組み合わせでテストすることにより厳密さを補足する。
④ 開発者テストで確認されているTOEのふるまいに対し､他のふるまいと競合する状況をテストすることにより厳密さを補足する。

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、上記の観点で68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、上記の観点で11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＞

開発者テストと同じ手法を用いた。

＜独立テストの実施内容＞

独立テストは、評価者によって 11 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 7-1 に示す。

表7-1 実施した独立テスト

No	テスト概要
1	①の観点より。 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。
2	①の観点より。 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、URL を指定してアクセスを試みても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。

No	テスト概要
3	②の観点より。 TOE が保持しているファイバチャネルスイッチのシークレットの設定を様々に変更してふるまいを確認する開発者テストの後、この設定を正しい内容にし、ファイバチャネルスイッチが認証されることを確認する。
4	②の観点より。 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）を削除する開発者テストの後、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。
5	①の観点より。 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。
6	③の観点より。 保守員の連続認証失敗でロックアウトされる機能に関して、リモートデスクトップのインタフェースと外部認証を使用する場合を確認する。
7	②③の観点より。 保守員のパスワード変更の際の強度確認機能を確認する開発者テストにおいて、実際に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。同じテストにおいて、パスワードの文字数や文字種について開発者テストと異なるパターンのテストを実施する。
8	③の観点より。 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。
9	①の観点より。 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。
10	④の観点より。 以下のふるまいを、ホストからストレージ装置へアクセスしている途中で確認する。 TOE に登録された WWN を変更した場合、変更前の WWN を持つ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。
11	①の観点より。 LDEV の削除後に、ホストからその LDEV にアクセスできなくなることを確認する。

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。

7.4.3 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 想定外の入力や操作に対する挙動

想定外の入力や操作に対し、予期しない動作の懸念がある。

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対し、通信の改変や URL の直接指定といった方法で回避して TOE の機能を利用できる懸念がある。

③ オープンポートに関係する公知の脆弱性

公知の脆弱性情報であるネットワークサービスの不正利用、Web の各種脆弱性について、外部 LAN から SVP PC へのアクセスで悪用できる懸念がある。

④ 通信における暗号アルゴリズム

SVP PC と管理 PC 間の暗号化通信において、弱い暗号方式が使われる懸念がある。

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排他制御、競合する操作、予期しない停止に関する脆弱性。

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 7-1 に示す。本環境は、「4.2 運用環境と構成」へ検査 PC と検査ツールを追加している。

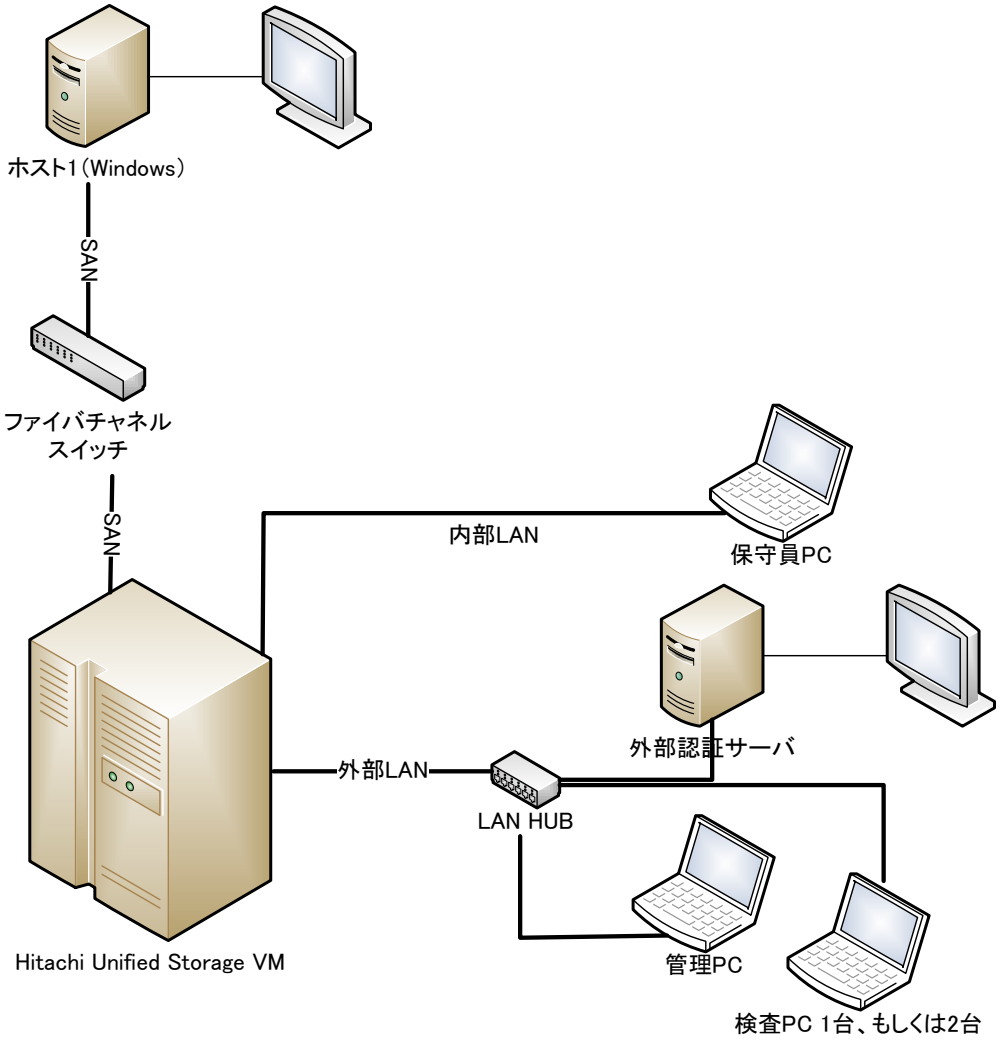


図7-1　侵入テスト環境

侵入テストの環境の構成要素、及び侵入テストで使用したツールの詳細を表 7-2 に示す。

表7-2　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 6.47	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 向けにオープンされたポートを調査する。
Nessus Ver 6.5.4	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、2016 年 2 月 10 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 2.1.5	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、2016 年 2 月 10 日のデータを使用。TOE の Web サーバを調査する。
Fiddler Ver.4.4.9.0 または Ver.4.4.9.6	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。

ツール名称	概要・利用目的
Wireshark Ver. 1.10.8 または Ver. 1.12.6	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。
OWASP ZAP Ver. 2.3.3	Web アプリケーションの脆弱性を検査する統合ペネトレーションテストツール。
openssl Ver. 1.0.2f	SSL/TLS のクライアント機能、ハッシュ関数や暗号化・復号の機能を持つツール。

＜侵入テスト手法＞

Storage Navigator プログラムと保守員 PC から TOE に対する操作を行い、TOE の画面遷移や表示されたメッセージ、ログを確認する。

表 7-2 に示したツールの使用については、表 7-3 のテスト概要に個別に記載する。

＜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 に示す。

表7-3　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
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
2	ファイバチャネルスイッチポート・ケーブル差し替え	ホストからストレージ装置へのアクセスが行われているときに、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
3	ポートスキャン(SVP PC)	Nmap を用いて、SVP PC に不要なポートが開いていないかどうかを確認する。	③
4	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
5	Web 系脆弱性スキャン (SVP PC)	Web サーバの脆弱性診断ツール Nikto, OWASP ZAP を用いて、SVP PC の Web サーバ系の脆弱性を確認する。 Web サーバのディレクトリを表す URL を Web ブラウザから指定して、ディレクトリの情報を不正に参照できないかどうかの確認も別途行う。	③
6	セッション管理	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。 Web ブラウザから URL を指定してセッション管理を回避できないかどうかを確認する。	②
7	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
8	不正な構成情報ファイル	構成情報ファイルの読み込み機能に対して、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

No	テスト名	テスト概要	懸念される脆弱性
9	競合する操作	ストレージ管理者が LDEV の編集をする直前に、競合の可能性のある設定(ストレージ管理者の権限、保守員による LDEV の設定)の変更をした場合の挙動を確認する。	⑤
10	弱い暗号方式	openssl を用いて TOE に対して弱い暗号方式による接続を試み、Wireshark で通信内容を観察することで弱い暗号方式が受け入れられないことを確認する。	④
11	プロセス停止	SVP PC の OS から操作を行い、TOE のプロセスが停止した場合の挙動を確認する。	⑤

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。

7.5 評価構成について

本評価では、「4.2 運用環境と構成」に示す動作環境を想定して評価を行った。

この構成は ST において保証の対象としている動作環境と同じである。ただし、調達者が想定する運用環境とは異なる可能性があるため、注意が必要である。(「8.2 注意事項」参照)

7.6 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
- 追加の保証コンポーネント ALC_FLR.1

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。

7.7 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 及び保証コンポーネント ALC_FLR.1 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

- 調達者の環境に本 TOE が受け入れられるかどうかは、評価ではどのような動作環境や設定において TOE の動作が保証されたかに基づき調達者が判断する。この判断の際、以下の点に注意する必要がある。
  - TOE の動作が保証された動作環境が特に限定されている。限定された動作環境については「4.2 運用環境と構成」参照。
  - TOE と外部認証サーバの間のプロトコルとして Kerberos(v5)を使用する場合の安全性は保証されない。
- 海外において本 TOE の導入を検討する調達者は、本 TOE の保証が十分かどうかの判断において、以下に注意する必要がある。
  海外への配付の場合、Hitachi Data Systems Corporation に TOE が受け渡された後の安全性は、ガイダンスに従い Hitachi Data Systems Corporation 及び以降の TOE の利用者がそれぞれの責任で維持することになる。
  例えば、Hitachi Data Systems Corporation が実際に TOE の安全性を維持しているかどうかは保証されない。

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 VM セキュリティターゲット バージョン 4.8
2016 年 4 月 18 日　株式会社 日立製作所

このセキュリティターゲットの名称はストレージ装置のセキュリティターゲットであるような名称となっているが、TOE はストレージ装置ではなくストレージ装置の制御ソフトウェアである。

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。

CHB	Channel Blade
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKB	Disk Blade
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel Security 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
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 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
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 及び管理 PC で動作する。Storage Navigator 利用者及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、及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。
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)	サーバなどと記憶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 Unified Storage VM 等を指す
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記憶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
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。

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27年6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27年10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 Part 1: Introduction and general model, Version 3.1 Revision 4, September 2012, CCMB-2012-09-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012, CCMB-2012-09-003

[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4版, 2012年9月, CCMB-2012-09-001, (平成24年11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4版, 2012年9月, CCMB-2012-09-002, (平成24年11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4版, 2012年9月, CCMB-2012-09-003, (平成24年11月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 4, September 2012, CCMB-2012-09-004

[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4版, 2012年9月, CCMB-2012-09-004, (平成24年11月, 翻訳第1.0版)

[12] Hitachi Unified Storage VM セキュリティターゲット バージョン 4.8 2016年4月18日 株式会社 日立製作所

[13] Hitachi Unified Storage VM 用制御プログラム 評価報告書 第6版 (125869-01-R003-06) 2016年4月26日 みずほ情報総研株式会社 情報セキュリティ評価室