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27年12月4日 (IT認証5576)
認証番号	C0536
認証申請者	株式会社日立製作所
TOEの名称	Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software
TOEのバージョン	8.0.1-02
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29年2月13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 Device Manager Software, Hitachi Tiered Storage Manager Software」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 Device Manager Software, Hitachi Tiered Storage Manager Software バージョン 8.0.1-02」(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 29 年 1 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、本書とともに提供され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、TOE 利用者（ストレージ管理者、アカウント管理者、システム構築者）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 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 Device Manager Software と Hitachi Tiered Storage Manager Software を合わせたものである。

本 TOE は、ストレージシステムの構成を表す情報(以降、ストレージリソース情報と記載)の入力や変更等の管理をする機能を持つ。

本 TOE は、不正な使用に対する警告バナーの表示、利用者の識別・認証、ストレージリソース情報や警告バナーの文面情報(以降、バナー情報と記載)へのアクセス制御をセキュリティ機能として提供する。

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。

保護資産であるストレージリソース情報が、不正な利用者により、あるいは、認証されたストレージ管理者またはアカウント管理者が、ストレージ管理クライアントから本来は許可されていない操作を実行することにより、削除、改ざん、暴露されること及び警告バナー機能で使用する文面情報が削除、改ざんされることを脅威と想定する。

TOE は、その脅威に対抗するため、利用者がストレージ管理クライアントからTOE にアクセスする際、利用者の識別・認証を行う。また、各利用者がストレージリソース情報やバナー情報に対して許可された操作のみを実行できるようにするためのアクセス制御を行う。

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 は管理サーバに導入され、周辺機器等とともに業務サーバエリアに設置される。業務サーバエリアに入室を許可されるのは、悪意を持たない、信頼できるハードウェア・ソフトウェアの管理者のみである。

TOE は業務サーバエリア外のストレージ管理クライアントから利用される。TOE が接続される業務サーバエリアのネットワークの外部から内部への通信は､ストレージ管理クライアントから TOE の通信に限定されるように管理されたネットワーク環境を想定している。

TOE の識別・認証機能を外部認証サーバ・認可サーバに代行させる場合、それらはストレージ管理ソフトウェアのサーバと同一の業務サーバエリアに設置する。両サーバを異なるサーバエリアに設置する場合は、両サーバ間の通信路は秘匿性と完全性が確保されているものとする。

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。
- 開発者から一般に公表される情報では、本 TOE は現実のストレージシステムの資源管理を行うための製品とされているが、現実のストレージシステムの資源管理を行う構成は本評価では保証されない。
  本評価では、現実のストレージシステムではなく、管理サーバ内のデータである「ストレージリソース情報」を TOE により管理する構成が保証された。
- 本 TOE は、ストレージ管理クライアントから TOE への攻撃のみに対抗することを想定する。それ以外の攻撃手段に関しては、TOE が対抗することは本評価では保証されず、運用環境により防止されていることを前提とする。
- 外部認証機能、外部認証グループ連携機能を利用する場合の、外部認証サーバ・外部認可サーバが持つ識別・認証機能は本評価の対象外である。また、外部認証サーバ・認可サーバのなりすましは運用環境で防止されていることを前提とする。

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 29 年 1 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 Device Manager Software, Hitachi Tiered Storage Manager Software
バージョン：	8.0.1-02
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。

ガイダンスに記述されたバージョン確認手順に従い操作することで、Hitachi Device Manager Software と Hitachi Tiered Storage Manager Software のそれぞれが正しいバージョン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。

本TOEの利用目的は、ストレージリソース情報の入力や変更等の管理である。

TOEは、市場の要請に対応するため、不正な使用に対する警告バナーを表示する機能を持つ。

TOEは、ストレージリソース情報及びバナー情報に対し許可されない操作が行われることを防止するため、識別・認証とアクセス制御の機能を持つ。

ストレージリソース情報に対するアクセス制御においては、各利用者に対し、ストレージリソース情報のどの範囲(ホストグループ、論理的なストレージなどのストレージリソース情報の要素)の、どのような操作(参照、変更、作成など)が許可されるかを制御できる。

なお、TOEは、使用に関して以下の役割を想定している。

・システム構築者

TOEを動作させるシステムの構築、システム運用に必要なセキュリティパラメタの決定・設定を行う。ストレージ管理クライアントからの操作だけでなく、業務サーバエリアでの作業も想定する。

・アカウント管理者

アカウント管理(アカウントの登録、削除、権限の設定)を行う。ストレージ管理クライアントからの操作を想定する。

・ストレージ管理者

ストレージリソース情報の入力や変更等の操作を行う。ストレージ管理クライアントからの操作を想定する。

以下の役割は、TOEを使用することは想定されないが、運用環境に関連する役割として想定される。

・外部認証サーバ管理者

外部認証サーバ・認可サーバの運用管理、認証または認可情報の設定を行う。業務サーバエリアでの作業を想定する。

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、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.ILLEGAL_ACCESS（不正な接続）	TOEのアカウントを持たない不正な利用者が、ストレージ管理クライアントから、TOEで管理するストレージリソース情報を削除、改ざん、暴露し、バナー情報を削除、改ざんするかもしれない。 また、TOEのアカウントを持つ不正な利用者が、本来は許可されていない利用者として認識され、ストレージ管理クライアントから、TOEで管理するストレージリソース情報、バナー情報を削除、改ざんするかもしれない。 （補足）この脅威は、なりすましにより許可されない操作が行われることを表している。
T.UNAUTHORISED_ACCESS（権限外のアクセス）	認証されたストレージ管理者またはアカウント管理者が、ストレージ管理クライアントから、本来は許可されていない操作を実行することによって、TOEで管理するストレージリソース情報、バナー情報を削除、改ざんするかもしれない。

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.ILLEGAL_ACCESS」への対抗

ストレージ管理クライアント端末の利用者が TOE およびストレージ管理ソフトウェアにアクセスする際に、内部認証を指定された利用者の場合は TOE で、外部認証を指定された利用者の場合は外部認証サーバが、その利用者の識別・認証を行い、許可された利用者であるかどうかの確認を行う。

TOE および外部認証サーバは、推測されにくいパスワードが設定されるようパスワードの登録パターンを制限するとともに、利用者自身も、パスワードの長さ、パスワードに利用する文字種の組み合わせから、推測困難なパスワードを設定し、適切な頻度で変更する上、パスワードを漏えいさせないことで、安全なパスワード管理を実現する。さらに、TOE が所定の回数以上連続して認証に失敗した場合、利用者のアカウントを自動的にロックすることで、総当りによるパスワード攻撃にも対抗する。

⑵ 脅威「T.UNAUTHORISED_ACCESS」への対抗

TOE は、TOE の各利用者に与えられた権限に従って、ストレージリソース情報、バナー情報へのアクセスを制御する。

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.BANNER（警告バナー)	TOEは、不正な使用に関する勧告的な警告メッセージを表示する機能を持たなければならない。

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 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。

⑴ 組織のセキュリティ方針「P.BANNER」への対応

TOE は、不正な使用に関する勧告的なメッセージを表示する機能をもつ。

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.PHYSICAL（ハードウェア等の管理)	TOEが動作する管理サーバと周辺機器、TOEが利用する外部認証サーバ・外部認可サーバ、内部ネットワーク、および内部ネットワークの境界に位置するファイアウォールは、物理的に隔離された業務サーバエリアに設置されるものとする。 そのエリアに入室を許可される人物はそのエリアに設置されたハードウェア・ソフトウェアの管理者のみであり、その管理者はエリア内に対し悪意を働かない信頼できる人物であるものとする。
A.NETWORKS (ネットワーク)	管理サーバが接続される管理ネットワークを含めた業務サーバエリアに設置される内部ネットワークは、ファイアウォールなどにより、ストレージ管理クライアント端末からの通信に制限する。 （補足）この前提条件の実現のためには、ストレージ管理クライアント端末への偽装も防がれる必要がある。

識別子	前提条件
A.ADMINISTRATORS（管理者）	システム構築者は信頼できる。アカウント管理者、ストレージ管理者、外部認証サーバ管理者は、それぞれに正式に与えられた権限内の操作において、TOEの利用者のアカウントおよび権限情報の管理業務、ストレージ管理業務に関して、悪意のある操作を行わない。 他サーバの管理者は、それぞれに正式に与えられた権限内の操作において、他サーバの管理業務に関して、悪意のある操作を行わない。 （補足）上記の「ストレージ管理業務」は管理サーバ内のストレージリソース情報の操作であり、現実のストレージシステムの管理ではない。
A.SECURE_CHANNEL（通信の秘匿性）	TOEが動作する管理サーバとストレージ管理クライアントとの間のネットワークは、通信の秘匿性と完全性が確保されているものとする。 TOEが利用する外部認証サーバ・外部認可サーバとTOEが異なる業務サーバエリアにある場合、その間のネットワークは、通信の秘匿性と完全性が確保されているものとする。
A.PASSWORD（複雑なパスワード）	アカウント管理者、システム構築者、外部認証サーバ管理者は適切なパスワード複雑性/アカウントロック回数を把握し、適切に設定するものとする。 各ストレージ管理者、アカウント管理者、システム構築者、外部認証サーバ管理者は、適切なタイミングでパスワード更新をし、そのパスワードは物理的漏えい(PC横付箋紙、ショルダーハッキング)、人為的漏えい(更新の怠慢、更新時に同じパスワードにする、個人情報に基づくパスワードや他アプリケーションとのパスワードの使い回し、キャッシュ情報等)により盗まれないようにする。
A.CLIENTS（ストレージ管理クライアント端末の管理）	ストレージ管理クライアント端末には、悪意のあるソフトウェアは存在しない。

識別子	前提条件
A.SRV_MGMT (サーバの管理)	管理サーバは、ストレージ管理クライアントから内部ネットワークに対してTOEを介さずに直接アクセスされることがないように、サーバで実行するサービスやサーバの設定、サーバに登録するアカウントを管理されているものとする。 （補足）SSHやtelnetによるリモートアクセスは、内部ネットワークへのアクセスとみなされるために禁止されていることを前提とする。

4.2 運用環境と構成

前提条件 A.PHYSICAL に従い、本 TOE が動作する管理サーバと周辺機器、TOE が利用する外部認証サーバ・外部認可サーバ、内部ネットワーク、および内部ネットワークの境界に位置するファイアウォールはセキュアなエリア(業務サーバエリア)に設置される。本 TOE の保証の対象となる運用環境を図 4-1 に示す。

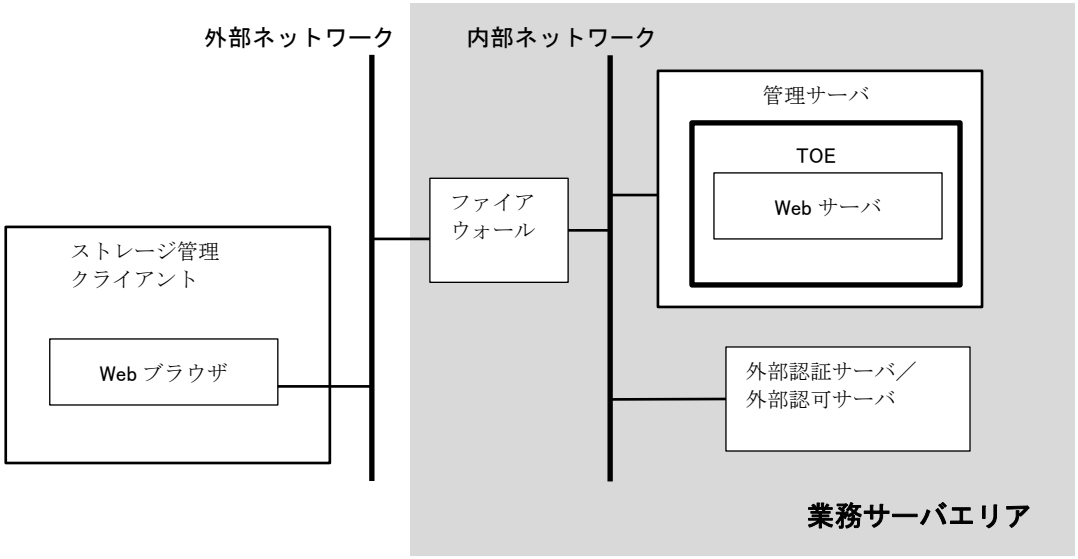

図4-1 保証の対象となるTOEの運用環境

保証の対象となる運用環境の詳細は以下の通りである。

・管理サーバ
以下のソフトウェアを搭載したサーバ機。
- Windows Server 2012 R2 (64bit)
- Java™ SE Development Kit 8, Update 92

・ストレージ管理クライアント端末
以下のソフトウェアを搭載した PC。

- Windows 7 SP1
- Internet Explorer 9 (32bit)
- Flash Player 14.0

・外部認証サーバ／外部認可サーバ
以下のソフトウェアを搭載したサーバ機であり、TOE の識別・認証機能を外部認証サーバ・認可サーバに代行させる場合に必要である。
- Windows Server 2012 R2 (64bit)

・ファイアウォール
外部ネットワークから内部ネットワークへの通信を、ストレージ管理クライアント端末からの通信に制限する目的のために設置する。
この目的が達成されれば異なる手段(例えば、ストレージ管理クライアント端末も内部ネットワークに接続する)でもよい。

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

業務サーバエリア内に、外部認証サーバ・外部認可サーバを設置し、TOE の識別・認証機能を代行させる「外部認証機能」、「外部認証グループ連携機能」も使用することが可能であるが、外部認証サーバ・外部認可サーバの持つ識別・認証機能自体は TOE の範囲ではなく、セキュリティ対策方針に則りセキュアに運用されることは、運用者の責任となる。

TOE は汎用の OS 上で稼動（OS の機能に（プロセス管理/プロセス分離等）に依存）するサーバプログラムであるが、前提条件から TOE へのアクセスはストレージ管理クライアントからのアクセスに限定されており、さらにストレージ管理クライアントに悪意のあるソフトウェアは存在せず、OS のコマンド等が悪用されることもない。

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 は管理サーバで動作するソフトウェアであり、OS を含まない。

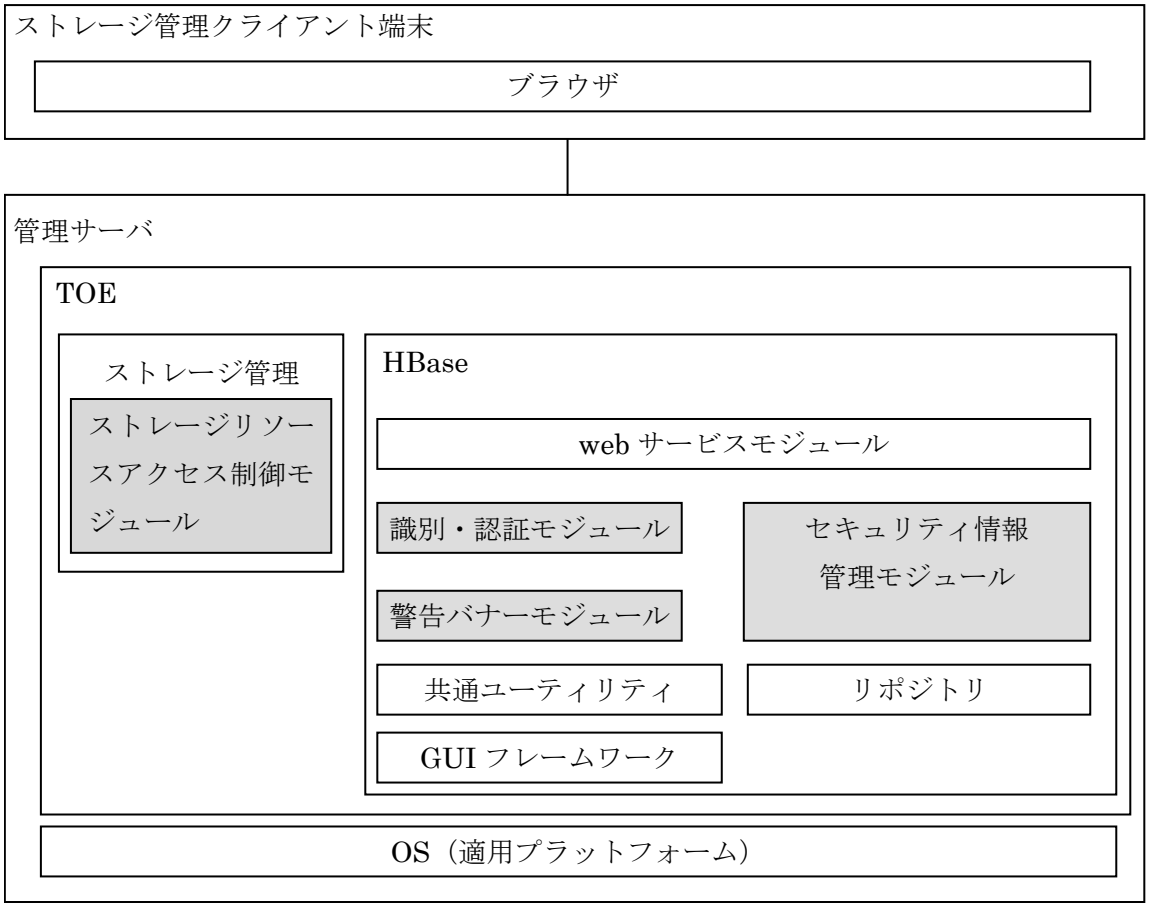

図5-1　TOE境界

- 識別・認証モジュールは、TOEの識別・認証機能を実現しているモジュールである。
- セキュリティ情報管理モジュールは、TOEのセキュリティ情報管理機能を実現しているモジュールである。
- 警告バナーモジュールは、TOEの警告バナー機能を実現しているモジュールである。
- 共通ユーティリティは、TOEの共通ユーティリティを実現しているモジュールである。
- webサービスモジュールは、TOEのwebサービスを実現しているモジュールである。

・ GUIフレームワークは、TOEのGUIフレームワークを実現しているモジュールである。
・ リポジトリは、TOEが有するデータを保持しているDBである。
・ ストレージリソースアクセス制御モジュールは、TOEが有するストレージリソース情報をセキュリティ情報管理モジュールと関連づけ、そのリソースへのアクセスを制御するモジュールである。

5.2 IT環境

本 TOE は、動作プラットフォームとして、Windows Server 2012 R2 (64bit)（Java™ SE Development Kit 8, Update 92 が動作する）を OS とする管理サーバ上にインストールされる。

TOE 利用者は、ストレージ管理クライアント端末から、ブラウザとして Internet Explorer 9 (32bit) を介して操作を行う。

認証サーバでは、Microsoft Active Directory（Windows Server 2012 R2 (64bit) 付属のもの）を利用する。

外部認証では、LDAP ディレクトリサーバ、RADIUS サーバ、Kerberos サーバの認証機能を利用する。

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。

- Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software セキュリティガイド P-2Z13-3084
- Hitachi Command Suite インストールガイド 3021-9-006-10
- Hitachi Command Suite ユーザーズガイド 3021-9-003-10
- Hitachi Command Suite システム構成ガイド 3021-9-008-10
- Hitachi Command Suite メッセージ 3021-9-011-10

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）の相互承認に加盟している認定機関（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 27 年 12 月に始まり、平成 29 年 1 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 28 年 7 月に TOE と同じ配付方法で実際に配付された製品の観察により、配付の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 28 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。

7.4 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を図 7-1 に示す。

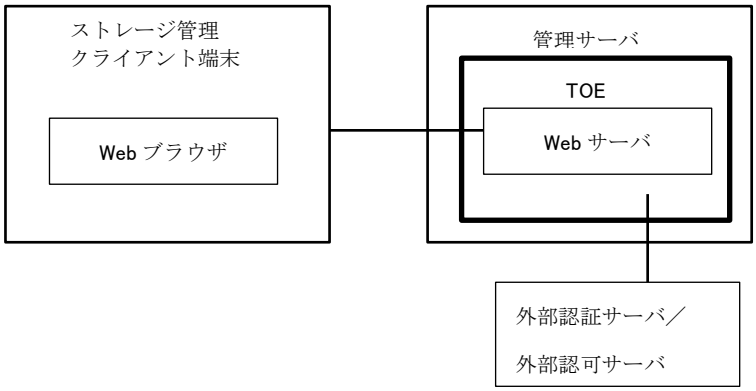

図7-1　開発者テストの構成図

開発者がテスト対象とした TOE は以下の通りであり、ST と一致する。

・Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software バージョン 8.0.1-02

開発者が実施したテストの環境における構成要素は以下の通りである。この構成は ST において識別されている構成と同等であり、本 TOE の機能の確認には問題ないことが評価者により評価されている。

・管理サーバ
以下のソフトウェアを搭載したサーバ機
- Windows Server 2012 R2 Datacenter x64 (64bit)
- Java™ SE Development Kit 8, Update 92

・外部認証サーバ／外部認可サーバ
以下のソフトウェアを搭載したサーバ機
- Windows Server 2012 R2 Datacenter x64 (64bit)

・ストレージ管理クライアント端末
以下のソフトウェアを搭載した PC
- Windows 7 Professional SP1 (64bit)
- Internet Explorer 9 (32bit)
- Flash Player 14.0

(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＞

本 TOE の外部インタフェースを TOE の通常の利用方法(ストレージ管理クライアント端末の Web ブラウザからの操作、管理サーバのコンソールからの操作、管理サーバ内の TOE の設定ファイルの変更)で刺激し、TOE の応答の確認を行った。ストレージリソース情報の入力の効率化のため、一部のテストではストレージのシミュレータを使用した。

TOE の通常の利用方法での確認が難しい TOE のふるまいに対し、fiddler を使用して Web サーバへの入力を変更した場合の TOE の応答の確認を行った。

本 TOE の応答は、ストレージ管理クライアント端末の Web ブラウザ及び管理サーバのコンソールから観察した。

＜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表 7-1 に示す。

表7-1　開発テストツール

ツール名称	概要・利用目的
Fiddler	Fiddler バージョン2.4.2.6 WebブラウザとWebサーバの間の通信を仲介し、その間の通信データの参照と変更を行う。
ストレージのシミュレータ	ストレージリソース情報を提供する。

＜開発者テストの実施内容＞

TOE の通常の利用方法により、セキュリティ機能要件に対する許可されるケースと拒否されるケース、不適切な入力を与えるケース、同じデータに対する複数の操作により不整合が起き得る懸念のあるケースのテストを実施した。

fiddler を使用して、Web ブラウザの通常の使用では入力できないパラメタの値を入力するテストを実施した。

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65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

評価者が実施した独立テストの環境は、開発者テストと同じ環境である。

テスト環境の要素やテスト用プログラムは、開発者テストに用いられたものを利用しているが、これら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。

以下の観点により、開発者のテスト仕様書からテスト項目を抽出した。

①セキュリティ機能の観点

セキュリティ機能に偏りなくテストを行うために、セキュリティ機能（識別・認証、アクセス制御、警告バナー機能）それぞれからサンプリングする。

②インタフェースの観点

Webブラウザからの操作、管理サーバのコンソールからの操作、管理サーバ内のTOEの設定ファイルの変更によるふるまいを確認するために､それぞれのインタフェースタイプからサンプリングすると共に､全てのSFRを網羅するようサンプリングする。

③その他のテストの特徴の観点

同じデータに対する複数の操作のあるテスト､fiddlerを使用してWebサーバへの入力を変更するテストのような､テストのシナリオや方法に特徴のあるテストをサンプリングする。

以下の観点により、追加のテストを考案した。

ⅰ）開発者テストのバリエーション(役割)

複数の役割が操作可能な機能に対し､開発者テストとは異なる役割(システム構築者、アカウント、管理者ストレージ管理者)のテストを補足する。

ⅱ）開発者テストのバリエーション(入力パラメタ)

パラメタの入力を受ける機能に対し、開発者テストとは異なるパラメタの値のテストを補足する。

ⅲ）開発者テストのカバレージ補足

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。

各インタフェースタイプ(Webブラウザからの操作、管理サーバのコンソールからの操作、管理サーバ内のTOEの設定ファイルの変更)が追加のテストを検討する対象となるよう考慮した。

b) **独立テスト概要**

開発者テストのサンプリングテストとして58件のテストを実施した。サンプルの選択にあたっては、上記の「a) 独立テストの観点」①, ②, ③で示したような観点を考慮した。

評価者テストとして、11件のテストを実施した。テストの考案に当たっては、上記の「a) 独立テストの観点」ⅰ), ⅱ), ⅲ)で示したように開発者テストを補足した。

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。

＜独立テストの実施内容＞

独立テストの観点とそれに対応したテスト内容を表 7-2 に示す。

表7-2 実施した独立テスト

独立テストの観点	テスト概要
① 利用者追加機能テスト 考案の観点 ⅰ), ⅲ)	アカウント管理者による利用者登録のふるまいを確認する。 開発者はシステム構築者による利用者登録をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
② パスワード変更機能テスト 考案の観点 ⅰ), ⅲ)	アカウント管理者による自分のパスワード変更のふるまいを確認する。 開発者はシステム構築者による自身のパスワード変更をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
③ パスワード複雑性設定の変更機能テスト 考案の観点 ⅱ)	パスワード複雑性設定のふるまいを確認する。 開発者はパスワード複雑性設定として「0」や負の数を含む場合を確認していない。「0」や負の数を含む規則に関するふるまいを確認する。
④ Webインタフェースにおける警告バナーの変更機能テスト 考案の観点 ⅱ)	警告バナーの設定時のふるまいを確認する。 開発者は単独のHTMLタグについてテストしているが、タグを構成する文字や属性を含む場合を確認していない。タグを構成する文字や属性を含む文字列を設定する場合のふるまいを確認する。

独立テストの観点	テスト概要
⑤ コマンドインタフェースにおける警告バナーの変更機能テスト 考案の観点 iii)	コマンドインタフェースでの警告バナー設定のふるまいを確認する。 開発者は新規にバナーを設定する場合についてテストしているが、Webインタフェースでの設定後について確認していない。Webインタフェースでの設定後にコマンドを実行した場合のふるまいを確認する。
⑥ アカウントのロック解除機能テスト 考案の観点 ii)	アカウントのロック解除のふるまいを確認する。 開発者は所定のパスワード長以上のパスワードを入力した場合について確認していない。設定されている以上のパスワード長を入力した場合のふるまいを確認する。
⑦ 外部認証の認証機能テスト(LDAP) 考案の観点 i), iii)	外部認証としてLDAPを指定している場合の外部認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
⑧ 外部認証の認証機能テスト (RADIUS) 考案の観点 i), iii)	外部認証としてRADIUSを指定している場合の外部認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
⑨ 外部認証の認証機能テスト(Kerberos) 考案の観点 i), iii)	外部認証としてKerberosを指定している場合の外部認証機能のふるまいを確認する。 開発者はストレージ管理者による外部認証機能をテストしているが、その他の管理者の場合を確認していない。異なる役割の管理者によるふるまいを確認する。
⑩ 設定ファイル内の不正な値のテスト 考案の観点 ii)	管理サーバ内のTOEの設定ファイルにおいて不正な値を設定した場合のふるまいを確認する。 開発者はTOEの設定ファイルに想定される値が設定される場合に対してテストしているが、値が空欄(未指定)や想定外の値の場合について確認していない。それらの値を指定した場合のふるまいを確認する。

独立テストの観点	テスト概要
⑪ 利用者ID、パスワードのテスト 考案の観点 ii)	利用者ID、パスワードとして上限の長さの文字列、許可されない文字を含む文字列を設定した場合の、利用者追加、ログインのふるまいを確認する。 開発者は利用者IDとパスワードに上限の長さの文字列を設定した場合を確認していないため、その場合のふるまいを確認する。また、許可されていない文字に関しては開発者テストとは値を変えてふるまいを確認する。

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、提供された証拠資料（セキュリティアーキテクチャ仕様書、構造設計書、機能仕様書）や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 直接攻撃の観点から、トークンのランダム性が不十分である可能性および不正なトークンにより攻撃される可能性が考えられる。
② 監視の観点から、TOE は、ストレージ管理クライアントから入力されたパスワードを受け取り、TOE 自身はログイン画面を提供していないため認証フィードバックの SFR が選択されていないが、ログイン時のパスワード入力時に、画面にパスワードが表示されるなどして、盗み見られる危険が考えられる。
③ ウェブアプリケーション、データベース、OS に関係する脆弱性を含む、その他の公知の脆弱性

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＞

侵入テストは独立テストを実施した環境に検査 PC を追加した環境で実施した。

検査 PC で使用したソフトウェアの詳細を表 7-3 に示す。これらのソフトウェア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。検査 PC 以外の部分については独立テストを実施した環境と同一である。

表7-3　侵入テストで使用したソフトウェア

ソフトウェア名称	概　要
OS	Windows 7 SP1
Webブラウザ	Internet Explorer 9 (32bit) on　Windows 7 SP1 with Flash Player 14.0
Nessus	Nessus 6.7.0 ・セキュリティスキャナ ・脆弱性データベースは2016年7月7日現在最新のものを使用
Nikto	Nikto 2.1.5 ・Webサーバを対象とするセキュリティスキャナ ・脆弱性データベースは2016年7月7日現在最新のものを使用
OWASP ZAP	ZAP 2.5.0 ・Webアプリケーションの脆弱性検査ツール
Tamper IE	TamperIE 1.0.1.13 ・Internet Explorerからの送信データをキャプチャし、任意のデータに改ざんすることができる。

＜侵入テスト手法＞

独立テストを実施した環境に設置されている管理サーバを対象に、ストレージ管理クライアント及び検査PCからTOEのインタフェースを刺激した。

・TSFI から刺激をあたえて振る舞いを確認する

・ストレージ管理クライアントから TOE に対して送信されるパケットをツールを使ってキャプチャし内容を確認する

・脆弱性検査ツールによるスキャンを実施する

バイナリ検査においては、「バイナリファイル中に秘密のパラメタが抽出可能な形で存在していないか」という観点で、評価機関により作成したバイナリ解析ツールを使用して、文字列として認識できる部分を確認した。

＜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 7-4 に示す。

表7-4　侵入テスト概要

脆弱性	テスト概要
①トークンのランダム性の確認と不正なトークンによる実行性の確認	トークンを取得し規則性がないことを確認する。パラメタに不正なトークンを入力して、TOE の動作を確認する。 トークンの取得や不正なトークンの入力には Tamper IE を使用する。
② パスワード入力時の入力値保護のテスト	パスワード入力時に、画面にパスワードが表示されるなどして、盗み見られる危険が無いかどうかを確認する。
③ ツールによる検査	ウェブアプリケーション、データベース、OS に関係する脆弱性を含むその他の公知の脆弱性を検査するためツール(Nessus、Nikto、OWASP ZAP)による検査を行う。

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、ST において想定の運用環境が単一に特定されており、ST で特定された運用環境と同等の環境で評価を行った。

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。

  - 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。
  - 本TOEの機能により現実のストレージシステムの資源管理を行う構成は本評価の保証の対象ではない。
    本評価では、現実のストレージシステムではなく、管理サーバ内のデータである「ストレージリソース情報」をTOEにより管理する構成が保証された。
  - ストレージ管理クライアント以外からTOEへの攻撃は､TOEが対抗することは本評価では保証されず、運用環境により防止されている必要がある。

・ 製品のオンラインヘルプは、保証対象ガイダンスには含まれない。保証対象ガイダンスについては、「6. 製品添付ドキュメント」を参照のこと。

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 Device Manager Software, Hitachi Tiered Storage Manager Software
セキュリティターゲット バージョン 1.0.28　2017 年 01 月 10 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用語の定義を以下に示す。

外部認証	TOE内部から、TOE外部の外部認証サーバ（LDAPディレクトリサーバ、RADIUSサーバ、Kerberosサーバ）の認証機能を利用する認証方式。
外部認証グループ連携	外部認可サーバに登録された、グループとそのグループに属するアカウントの情報をTOEが取得し、TOE内部で権限情報を付与する機能。TOE外部の認証機能を前提とし、アカウントはグループに属していることから、「外部認証グループ連携」と呼ぶ。
警告バナー	TOEの利用者に対する、利用前の警告文面表示。主に不正利用に対する注意喚起に用いられる。
ストレージリソース情報	ストレージシステムの構成を表す以下のような情報であり、管理サーバ内に保存される。 どのホストのグループがどの論理的なストレージを利用できるか、それぞれの論理的なストレージにどの物理的ディスクグループからどれだけの容量を確保できるか、それぞれの物理的ディスクグループはどの物理的ディスクにより構成されるか。
セキュリティパラメタ	TOEのセキュリティ機能に関連するパラメタ情報。パスワードの文字数やパスワードに使用する文字種別、ログインの連続失敗回数とその閾値、閾値を超えた（アカウントがロックされたか）などの情報。
内部認証	TOEの内部認証機能のみを利用する認証。
バナー情報	警告バナーとして表示する文面情報。

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27年10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 Device Manager Software, Hitachi Tiered Storage Manager Softwareセキュリティターゲット バージョン1.0.28　2017年01月10日
株式会社日立製作所

[13] Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software 評価報告書 第3版(143599-01-R003-03)　2017年1月16日
みずほ情報総研株式会社 情報セキュリティ評価室