# 認　証　報　告　書

独立行政法人 情報処理推進機構
理事長　藤原　武平太　原紙押印済

評価対象

| | |
|---|---|
| **申請受付年月日(受付番号)** | **平成18年10月16日（IT認証6106）** |
| **認証番号** | C0096 |
| **認証申請者** | **株式会社 日立製作所** |
| **TOEの名称** | HiCommand Suite Common Component |
| **TOEのバージョン** | 05-51-01 |
| **PP適合** | **なし** |
| **適合する保証要件** | EAL2+ALC_FLR.1 |
| **TOE開発者** | **株式会社 日立製作所** |
| **評価機関の名称** | **株式会社電子商取引安全技術研究所 評価センター** |

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成19年5月30日

セキュリティセンター 情報セキュリティ認証室
技術管理者　田渕　治樹

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

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

**評価結果：合格**

「HiCommand Suite Common Component バージョン 05-51-01」は、独立行政法人 情報処理推進機構が定める ITセキュリティ認証手続規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

# 1 全体要約

## 1.1 はじめに

この認証報告書は、「HiCommand Suite Common Component バージョン 05-51-01」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社 日立製作所に報告するものである。

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

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

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

## 1.2 評価製品

### 1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称: HiCommand Suite Common Component

バージョン: 05-51-01

開発者: 株式会社 日立製作所

### 1.2.2 製品概要

評価対象であるHiCommand Suite Common Component（以降、HSCCと略記）は、ＳＡＮ環境に接続された複数のストレージデバイスを一元的に管理するストレージ管理ソフトウェアに対して、共通機能を提供する基盤モジュールとして動作する。

ストレージ管理ソフトウェアにはHiCommand Device Manager、HiCommand Replication Monitor、HiCommand Tiered Storage Manager等があり、これらの製品群とHSCCを総称してHiCommand Suiteと呼ぶ。

HSCCはHiCommand Suiteの基盤モジュール製品として、各製品パッケージに同梱されて提供される。

HSCCのセキュリティ機能は以下である。

- 識別・認証機能
- 権限情報(利用者ごとに存在し、ストレージ管理ソフトウェアがそのセキュリティ機能の動作を決めるための情報)管理機能
- 警告バナー機能

### 1.2.3 TOEの範囲と動作概要

#### 1.2.3.1 TOEの物理的範囲と構成

TOEはHiCommand Suite Common Component バージョン 05-51-01で識別されるソフトウェア全体である。

TOEは図1-1のような環境で使用される。

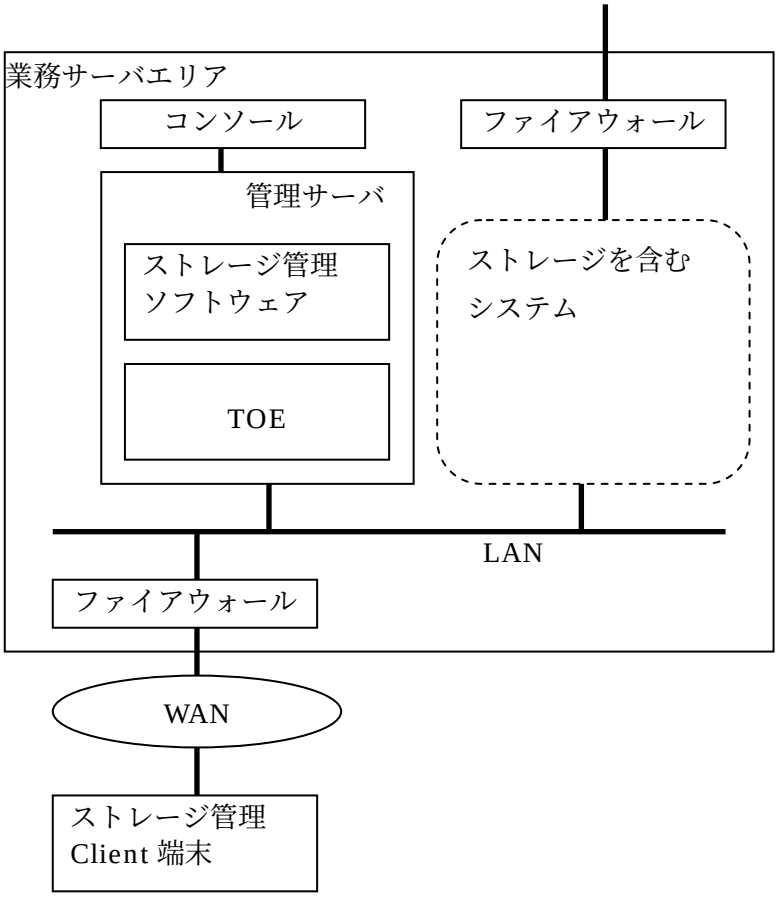


**図1-1 TOEの利用環境**

管理サーバは、以下のいずれかを満たすプラットフォームである。

- Windows版のHiCommand Suite Common Componentがインストールする Java™VM（Version 1.4.2_03）が動作するプラットフォーム。
- Solaris版のHiCommand Suite Common ComponentがインストールするJava™

VM（Version 1.4.2_03）が動作するプラットフォーム。

- Linux版のHiCommand Suite Common Componentがインストールする Java™ VM（Version 1.4.2_03）が動作するプラットフォーム。

業務サーバエリアは入退場が制限されていて、管理サーバやファイアウォールが設置される。業務サーバエリアには、それ以外にもストレージ管理ソフトウェアの管理の対象となるストレージを含むシステムが設置されることがある。

業務サーバエリア内のネットワークは、すべての業務サーバエリア外との接点において、ファイアウォールによって外部から保護されている。ファイアウォールの内側ネットワークを内部ネットワークと呼び、ファイアウォールの外側を外部ネットワークと呼ぶこととする。

ストレージ管理者及びアカウント管理者は、ストレージ管理Client端末を用いて外部ネットワーク経由でTOEにアクセスし、ストレージ管理ソフトウェアへの操作要求を行う。このとき、ログイン時には警告バナーを表示することで、不正利用への注意を喚起する。また、利用者は類推しにくいパスワードを利用する。

#### 1.2.3.2 TOEの動作概要

TOEは、以下のようにストレージ管理ソフトウェアから利用される。ストレージ管理ソフトウェアが以下のようにTOEを利用するつくりであれば、自らが識別・認証機能、権限情報管理機能、警告バナー機能を持たなくても、これらをTOEに代行させることができる。

- ストレージ管理ソフトウェアがTOEに警告バナー情報を要求すると、TOEから警告バナー情報が返答される。ストレージ管理ソフトウェアは、利用者に識別・認証情報を要求する際にその警告バナー情報を表示する。
- ストレージ管理ソフトウェアは、利用者の識別・認証情報を受け取ると、それをTOEに入力する。TOEはその識別・認証情報を検証し、正しければ利用者とTOEの間はセッションが確立した状態になる。セッションが確立すると、TOEはその利用者の権限情報を返答し、ストレージ管理ソフトウェアはその権限情報を受け取る。
- ストレージ管理ソフトウェアは、利用者がストレージに対して何かの操作を行おうとしたとき、現在でもその利用者とTOEのセッションが確立した状態であるかをTOEに問い合わせる。TOEから返答によりセッションが確立した状態であることがわかれば、ストレージ管理ソフトウェアは、その利用者の権限情報を使用してストレージへの操作の可否を判定する。

#### 1.2.3.2 TOEの関係者

TOEでは、以下の役割の利用者を想定する。利用者は各々の権限に従って業務を行う。

- システム構築者（サーバ・ネットワーク管理者）

  役割：サーバデータのバックアップなどを含むシステムの維持管理業務を行う。

  権限：システム構築、システム運用に必要な各種パラメタの決定・設定を行う。このため、利用者データである権限情報の更新（変更、削除等）ができる。また、システム構築者としての権限は変更されない。

  信頼度：システムに対して責任を持っており、信頼できる。

- アカウント管理者

  役割：システムにおける運用・設定を行う利用者のためのアカウント管理業務を行う。

  権限：アカウント作成の要否やそのアカウントに許されるべき権限といったアカウント元情報は、職制など組織情報を元に決定され、アカウント管理者はこの情報を元に運用業務を行う。このため、利用者データである権限情報の更新（変更、削除等）ができる。

  信頼度:自己の業務に対して責任を持っており、自己の業務範囲内で信頼できる。

- ストレージ管理者

  役割：ストレージのリソース管理など、ストレージ管理業務を行う。

  権限：システム構築者によって設置されたストレージ内のリソースに関し、割り当てなどの設定を行う。このため、自身に与えられた権限情報を問い合わせるために利用者データである権限情報の参照ができる。

  信頼度:自己の業務に対して責任を持っており、自己の業務範囲内で信頼できる。

### 1.2.4 TOEの機能

TOEは、ストレージ管理ソフトウェアに識別・認証機能、権限情報管理機能、警告バナー機能を提供するために以下のセキュリティ機能を持つ。

- 警告バナー機能

  TOEは、管理サーバで動作するストレージ管理ソフトウェアから警告バナー情報を要求されると、警告バナー情報を返答する。

- 識別・認証

  TOEは、管理サーバで動作するストレージ管理ソフトウェアから利用者の識別・認証情報を受け取ると、それを検証する。正しければ、要求(利用者のログインか、セキュリティ情報管理機能の実行か)に応じてセッション管理に移行する。

  TOEは、一定回数連続して認証に失敗したストレージ管理者またはアカウント管理者のアカウントを自動的にロックする。アカウントがロックされる期間は無期限である。

- セッション管理 (利用者のログインの場合)

  識別・認証が成功すると、TOEは、利用者とTOEの間のセッションが確立した状態を作り、そのセッション固有のトークンとその利用者の権限情報を返答する。

  TOEは、利用者からセッション切断の要求を受けるまでセッションが確立した状態を維持する。

  TOEは、管理サーバで動作するストレージ管理ソフトウェアから、トークンとともにそのトークンに関連するセッションが確立した状態であるか否かの問い合わせを受けると、現在セッションが確立した状態であるか否かを返答する。セッションが確立した状態であれば、ストレージ管理ソフトウェアからの要求に応じてそのセッションのストレージ管理者の識別と権限情報を返答することができる。

- セッション管理 (セキュリティ情報管理機能の実行の場合)

  識別・認証が成功すると、TOEは、利用者とTOEの間のセッションが確立した状態を作り、セキュリティ情報管理機能が実行される間はそのセッションが確立した状態を維持する。

- セキュリティ情報管理機能

  TOEは、セキュリティ情報管理機能として以下の機能を持つ。

  - アカウント管理

    TOEは、利用者からの要求に応じて、ユーザーID（アカウント）の登録、削除、パスワードの登録、改変、削除（アカウント全体として削除)、ロックステータスの問い合わせ、改変、の操作を行う手段を提供する。

    TOEは、アカウント管理者およびシステム構築者に対して、上記の全ての操作の実行を許可し、ストレージ管理者に対しては、自分自身のパスワードの改変の操作の実行のみ許可する。ただしシステム構築者の役割を持つアカウントの新規登録、削除の操作は、どの利用者に対しても許可しない。

    TOEは、以降に示されるセキュリティパラメータで決められる品質を満

たさないパスワードは受け付けない。

- 役割と権限情報の管理

  TOEは、ユーザーIDごとに役割と権限情報を維持する。ユーザーIDが作成されたときの役割と権限情報は未設定である。

  TOEは、アカウント管理者およびシステム構築者に限り、システム構築者以外の役割と権限情報を生成、削除、改変を許可する。ただし、TOEは、アカウント管理者が本人の役割と権限情報を削除､改変することは許可しない。

- 警告バナー情報管理

  TOEは、アカウント管理者またはシステム構築者に限り、警告バナー情報の生成・削除・改変を許可する。

- セキュリティパラメータ管理

  TOEは、以下のセキュリティパラメータを持ち、アカウント管理者またはシステム構築者に限り、これらの問い合わせ、改変、消去を許可する。

| パラメータ | 内容 |
|---|---|
| 認証の連続失敗回数のしきい値 | アカウント自動ロック機能において、アカウントを自動的にロック状態にするための認証の連続失敗回数のしきい値。 |
| パスワード最小文字数 | パスワードの最小文字数。 |
| パスワード複雑性条件 | パスワードが所定の文字種の文字を所定数以上含むことを規定した条件。 |

## 1.3 評価の実施

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

本評価の目的は、以下のとおりである。

(1) 本TOEのセキュリティ設計が適切であること。

(2) 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。

(3) 本TOEがセキュリティ設計に基づいて開発されていること。

(4) 上記(1)、(2)、(3)を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「HiCommand Suite Common Component セキュリティターゲット Version 1.08」

（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書C、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「HiCommand Suite Common Component バージョン 05-51-01 評価報告書」(以下「評価報告書」という。)[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

## 1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成19年5月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

## 1.5 報告概要

### 1.5.1 PP適合

適合するPPはない。

### 1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL2追加である。

追加されるコンポーネントはALC_FLR.1である。

### 1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOE が想定する攻撃者は、高度な専門知識を持たず管理者が操作できるクライアントからのインタフェースを利用する低レベルの脅威エージェントを想定している。このため、最小機能強度レベルは“ SOF-基本 ”が妥当であると言える。

### 1.5.4 セキュリティ機能

本TOEのセキュリティ機能については、「1.2.4TOEの機能」参照。

### 1.5.5 脅威

本TOEは、以下を脅威エージェントとして想定する。

- 不正な利用者（TOE および全てのストレージ管理ソフトウェアの使用を許可されていない者）
- ストレージ管理者（TOE およびいずれかのストレージ管理ソフトウェアの使用を許可されている者）

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

**表1-1　想定する脅威**

| 識別子 | 脅　威 |
|---|---|
| **T.ILLEGAL_ACCESS**<br>(不正な接続) | 不正な利用者が、管理クライアントから、TOEで管理する権限情報を削除、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。 |
| **T.UNAUTHORISED_ACCESS**<br>(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、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で管理する権限情報を削除、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。 |

### 1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

**表1-2　組織のセキュリティ方針**

| 識別子 | 組織のセキュリティ方針 |
|---|---|
| **P.BANNER**<br>(警告バナー) | ストレージ管理ソフトウェアは、ストレージ管理ソフトウェアの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。 |

### 1.5.7 構成条件

TOEは、以下のいずれかを満たすプラットフォームで動作する。

- Windows版のHiCommand Suite Common Componentがインストールする

Java™VM（Version 1.4.2_03）が動作するプラットフォーム。

- Solaris版のHiCommand Suite Common Componentがインストールする Java™VM（Version 1.4.2_03）が動作するプラットフォーム。
- Linux版のHiCommand Suite Common Componentがインストールする Java™VM（Version 1.4.2_03）が動作するプラットフォーム。

### 1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3に示す。

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

**表1-3 TOE使用の前提条件**

| 識別子 | 前提条件 |
|---|---|
| A.PHYSICAL<br>(ハードウェア等の管理) | TOE およびストレージ管理ソフトウェアが動作する管理サーバと周辺機器、ストレージ装置、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、許可された管理者のみが入室できるものとする。 |
| A.NETWORKS<br>(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、必要な通信に制限し、トラフィックを監視するファイアウォールにより、外部ネットワークと論理的に分離され、不正なトラフィックが監視されているものとする。 |
| A.ADMINISTRATORS<br>(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、およびアプリケーションサーバを含めた他サーバの管理者は、それぞれに課せられたストレージ管理ソフトウェア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、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。 |
| A.SECURE_CHANNEL<br>(通信の秘匿性) | TOE およびストレージ管理ソフトウェアが動作する管理サーバと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。 |
| A.TOKEN<br>(利用可能なトークン) | TOE は、TOE の外部で生成されたトークン、および十分な強度を持たないトークンを使用した製品と組み合わせた環境構築を行わないものとする。 |

| 識別子 | 前提条件 |
|---|---|
| **A.PASSWORD**<br>(複雑なパスワード) | 不正な利用者がパスワードを推測してログインしないように、十分な強度を持つ認証方式を使用するものとする。 |

### 1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- HiCommand Suite Common Component セキュリティガイド 解説・操作書 第1版
- JP1/HiCommand Device Manager Web Client ユーザーズガイド 解説・操作書 3020-3-J71-20 Version 3
- JP1/HiCommand Device Manager システム構成ガイド (サーバ編) 手引書 3020-3-J73-20 Version 3

# 2 評価機関による評価実施及び結果

## 2.1 評価方法

評価は、CCパート3の保証要件について、CEMパート2に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMパート2のワークユニットごとに評価した内容及び判断が記載されている。

## 2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成18年10月に始まり、平成19年5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19年2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、配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成19年3月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

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

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

## 2.3 製品テスト

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

### 2.3.1 開発者テスト

1) 開発者テスト環境

開発者テストは、表2-1に示す各OSの環境で実施された。

**表2-1 開発者テストの構成**

| TOE | バージョン等 |
|---|---|
| HiCommand Suite Common Component | 05-51-01 |
| HiCommand製品(ストレージ管理ソフトウェア製品) | バージョン等 |
| HiCommand Device Manger (Windows版) | 05-60-01 |
| HiCommand Global Link Availability Manager (Windows版) | 05-60-01 |
| HiCommand Device Manger (Linux版) | 05-60-01 |
| HiCommand Device Manger (Solaris版) | 05-60-01 |
| HiCommand製品と同時にインストールされるJava™VM | バージョン等 |
| (Windows版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03 |
| (Solaris版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03 |
| (Linux版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03 |
| OS | 備考 |
| Windows 2000 Professional SP4 | 管理サーバ<br>(CPU：Pentium4 1.5GHz) |
| Windows XP Professional SP2 | 管理サーバ<br>(CPU：Pentium4 2.4GHz) |
| Windows2003 Server Standard Edition | 管理サーバ<br>(CPU：Pentium4 2.4GHz) |
| Solaris 8 | 管理サーバ<br>(CPU：UltraSPARC-IIIi 1.28GHz) |

| | |
|---|---|
| Solaris 9 | 管理サーバ<br>(CPU：UltraSPARC-III 900MHz) |
| Solaris 10 | 管理サーバ<br>(CPU：UltraSPARC-IIIi 1.28GHz) |
| Red Hat Enterprise Linux AS 4 | 管理サーバ<br>(CPU：Pentium4 2.8GHz) |

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①ブラウザの操作画面からの操作及び画面表示の確認。

②コンソール画面からの操作及び画面表示の確認。

c.実施テストの範囲

テストは開発者によって、各OSの環境で155項目ずつ実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

d.結果

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

### 2.3.2 評価者テスト

1) 評価者テスト環境

評価者テストは、表2-2に示す各OSの環境で実施された。

**表2-2 評価者テストの構成**

| TOE | バージョン等 |
|---|---|
| HiCommand Suite Common Component | 05-51-01 |
| HiCommand製品(ストレージ管理ソフトウェア製品) | バージョン等 |
| HiCommand Device Manger (Windows版) | 05-60-01 |

| | |
|---|---|
| HiCommand Global Link Availability Manager (Windows版) | 05-60-01 |
| HiCommand Device Manger (Linux版) | 05-60-01 |
| HiCommand Device Manger (Solaris版) | 05-60-01 |
| HiCommand製品と同時にインストールされるJava™VM | バージョン等 |
| (Windows版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03-b02-CDK0205O |
| (Solaris版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03-b02-CDK0205F |
| (Linux版)<br>Java(TM) 2 Runtime Environment, Standard Edition<br>Java HotSpot(TM) Client VM | 1.4.2_03-b02-CDK0205I |
| OS | 備考 |
| Windows XP Professional SP2 | 管理サーバ<br>(CPU：Core2Duo 1.86GHz) |
| Solaris 8 | 管理サーバ<br>(CPU：UltraSPARCIIIi 1.2GHz) |
| Red Hat Enterprise Linux AS 4 | 管理サーバ<br>(CPU：Pentium4 2.8GHz) |
| Windows XP Professional SP2 | クライアント端末<br>(CPU：Pentium4 3.6GHz) |
| ブラウザ | 備考 |
| Microsoft Internet Explorer 6 SP2 | クライアント端末 |

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b.テスト手法

テストには、以下の手法が使用された。

①ブラウザの操作画面からの操作及び画面表示の確認。

②コンソール画面からの操作及び画面表示の確認。

c.実施テストの範囲

評価者が独自に考案したテストを12項目、開発者テストのサンプリングによる

テストを32項目、計44項目のテストを、各OSの環境で実施した。テスト項目の選択基準として、下記を考慮している。

① 全てのセキュリティ機能を含める。

② 各セキュリティ機能のインタフェースにおいて、テストされていないパラメタ範囲(限界値)はないか。

③ セキュリティ情報管理機能においてセキュリティパラメタの変更をした場合、即時に反映されるか。

d.結果

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

### 2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMパート2のワークユニットすべてを満たしていると判断した。

## 3 認証実施

評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。

② 当該所見報告書でなされた指摘内容が正しく反映されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

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

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

## 4 結論

### 4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、

認証機関は、本TOEがCCパート3のEAL2およびALC_FLR.1保証要件を満たしていることを確認した。

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

**表4-1　評価者アクションエレメント検証結果**

| 評価者アクションエレメント | 検証結果 |
|---|---|
| **セキュリティターゲット評価** | **適切な評価が実施された。** |
| ASE_DES.1.1E | 評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_DES.1.2E | 評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。 |
| ASE_DES.1.3E | 評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。 |
| ASE_ENV.1.1E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_ENV.1.2E | 評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.1E | 評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。 |
| ASE_INT.1.2E | 評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。 |
| ASE_INT.1.3E | 評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。 |
| ASE_OBJ.1.1E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。 |

| | |
|---|---|
| ASE_OBJ.1.2E | 評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_PPC.1.1E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_PPC.1.2E | 評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。 |
| ASE_REQ.1.1E | 評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| ASE_REQ.1.2E | 評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| ASE_SRE.1.1E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_SRE.1.2E | 評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。 |
| ASE_TSS.1.1E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。 |
| ASE_TSS.1.2E | 評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。 |
| **構成管理** | **適切な評価が実施された** |
| ACM_CAP.2.1E | 評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認してい |

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

| | |
|---|---|
| ADV_HLD.1.2E | 評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。 |
| ADV_RCR.1.1E | 評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。 |
| **ガイダンス文書** | **適切な評価が実施された** |
| AGD_ADM.1.1E | 評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| AGD_USR.1.1E | 評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。 |
| **ライフサイクルサポート** | **適切な評価が実施された** |
| ALC_FLR.1.1E | 評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供されることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。 |
| **テスト** | **適切な評価が実施された** |
| ATE_COV.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。 |

| | |
|---|---|
| ATE_FUN.1.1E | 評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。 |
| ATE_IND.2.1E | 評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。 |
| ATE_IND.2.2E | 評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。 |
| ATE_IND.2.3E | 評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。 |
| **脆弱性評定** | **適切な評価が実施された** |
| AVA_SOF.1.1E | 評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。 |
| AVA_SOF.1.2E | 評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。 |
| AVA_VLA.1.1E | 評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。 |

| | |
|---|---|
| AVA_VLA.1.2E | 評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。 |

## 4.2 注意事項

特になし。

# 5 用語

本報告書で使用された略語を以下に示す。

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

本報告書で使用された用語を以下に示す。

| | |
|---|---|
| トークン | TOEがセッション管理に用いる識別子。 |
| 警告バナー | ストレージ管理ソフトウェアの利用者に対する、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。 |

# 6 参照


[1] HiCommand Suite Common Component セキュリティターゲット Version 1.08 （2007年5月10日）株式会社 日立製作所

[2] ITセキュリティ評価及び認証制度の基本規程　平成18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

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

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

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

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

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

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

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

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

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

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

[17] 補足-0512　平成17年12月

[18] HiCommand Suite Common Component バージョン05-51-01 評価報告書 第3.0版 （2007年5月11日）株式会社電子商取引安全技術研究所 評価センター