認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	平成19年8月27日 (IT認証7165)
認証番号	C0200
認証申請者	株式会社 日立製作所
TOEの名称	Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000用 制御プログラム
TOEのバージョン	60-02-32-00/00(R6-02A-14)
PP適合	なし
適合する保証パッケージ	EAL2
開発者	株式会社 日立製作所
評価機関の名称	株式会社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20年12月24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　鈴木　秀二

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

「Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000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

1.1 はじめに

この認証報告書は、「Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000用 制御プログラム」(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: Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000用 制御プログラム
バージョン: 60-02-32-00/00(R6-02A-14)
開発者: 株式会社 日立製作所

1.2.2 製品概要

TOEは、株式会社 日立製作所製ストレージ装置「Hitachi Universal Storage Platform V」、「Hitachi Universal Storage Platform H24000」、「Hitachi Universal Storage Platform VM」「Hitachi Universal Storage Platform H20000」上で動作するソフトウェアである。ストレージ装置にはSAN環境やIPネットワーク環境を介

して、様々なプラットフォームの多数のホストが接続される。

TOEは、特定のストレージ利用者に割り当てられたストレージ装置に対する他のストレージ利用者からの不正アクセスを防止する機能を提供するものである。

1.2.3 TOEの範囲と動作概要

TOEを含むストレージ装置は一般的に図1-1の構成で使用される。

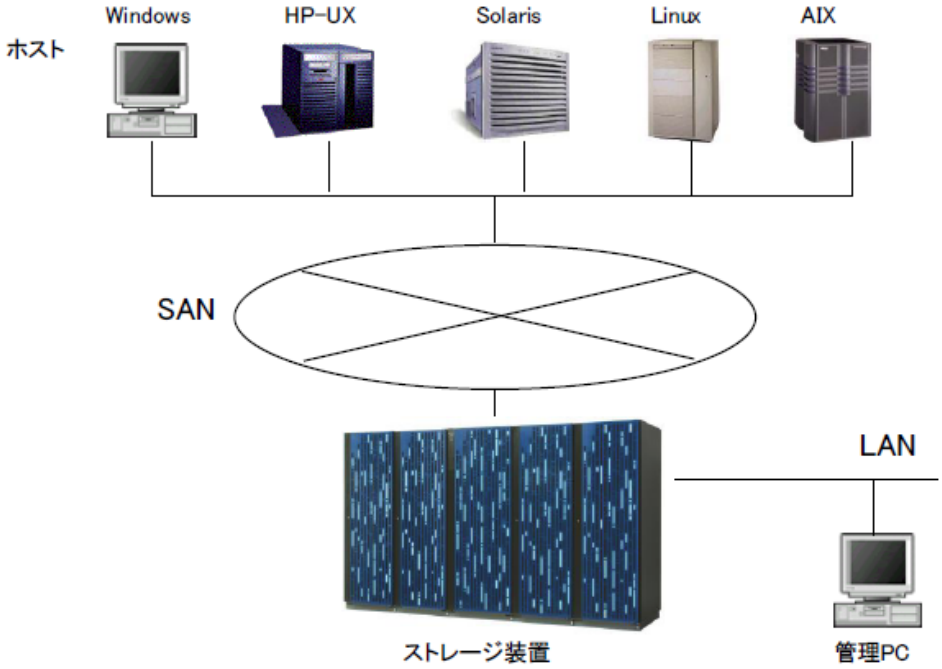

図1-1　ストレージ装置を含むシステム構成

以下にシステム構成を説明する。

(1)　ストレージ装置

通常、ストレージ装置は、入退室が管理されているセキュアなエリアに設置される。

(2)　SANとホスト

Windows、HP-UX、Solaris等の各種オープン系サーバ（本書ではこれらの機器を“ホスト”と総称する。）とストレージ装置との接続は、SAN(Storage Area Network)を介して行われる。SANは、ホストとストレージ装置をファイバチャネルによって接続するストレージシステム専用ネットワークである。

(3)　管理PC

管理PCは、ストレージ装置の装置制御情報の設定をリモートから行うためのPCである。管理PC上で、ストレージ装置の管理者が装置制御情報の設定を行うためのプログラムを動作させる。管理PCとストレージ装置はLANを介して接続される。

ストレージ装置の構成とTOEの関係は図1-2であり、TOEは、「DKCMAINマイクロプログラム」、「SVPプログラム」、「Storage Navigatorプログラム」である。

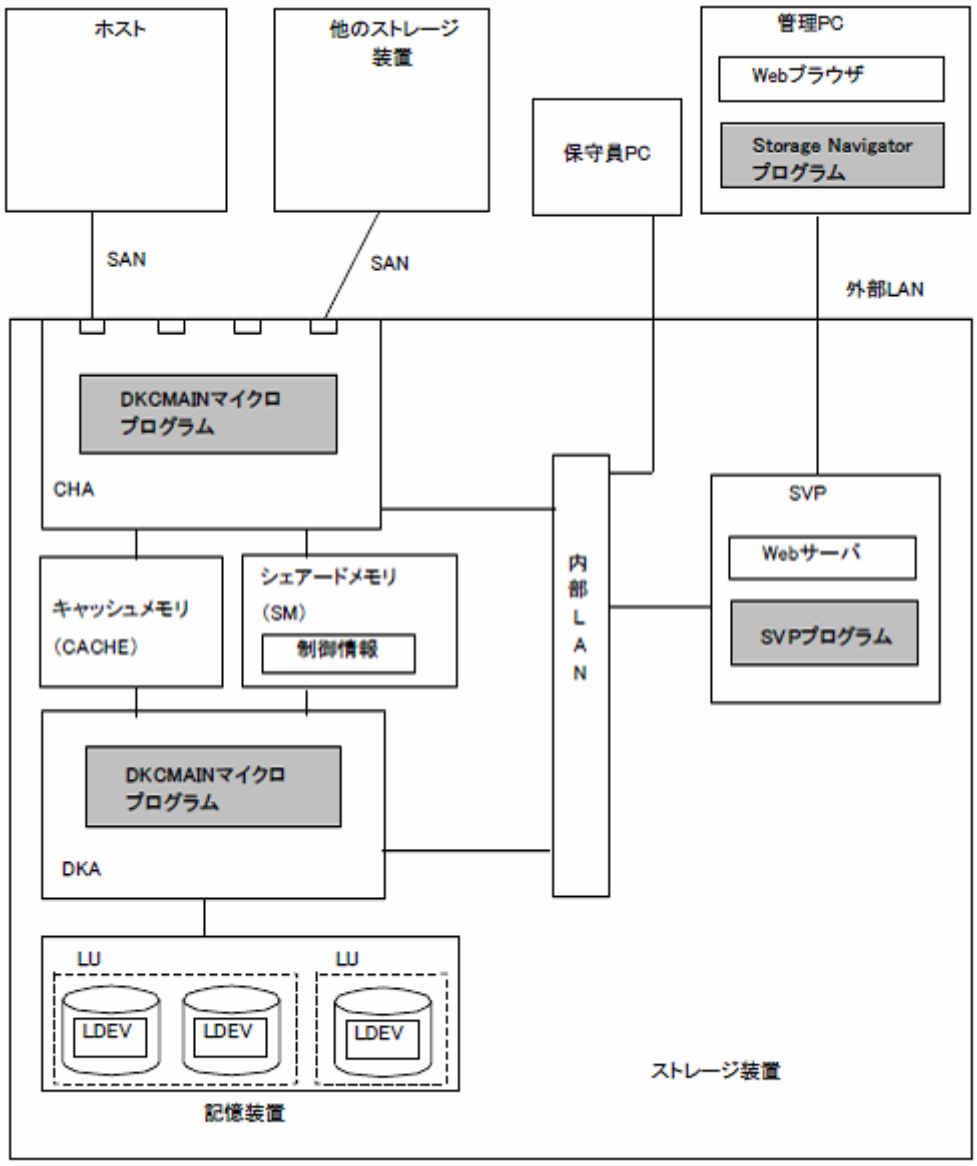

図1-2　ストレージ装置の構成とTOE

以下にストレージ装置の構成を説明する。

（1）　チャネルアダプタ（CHA）

チャネルアダプタは、ホストからストレージ装置に対する命令を処理して、データ転送を制御するアダプタである。ホストはファイバチャネルを介して、CHA上のファイバポートに接続される。CHAでは、TOEの一部であるDKCMAINマイクロプログラムが動作する。

（2）　ディスクアダプタ（DKA）

ディスクアダプタは、キャッシュメモリ（CACHE）と記憶装置間のデータ

転送を制御するアダプタである。DKAでは、TOEの一部であるDKCMAINマイクロプログラムが動作する。

(3) キャッシュメモリ（CACHE）

キャッシュメモリは、CHAとDKAとの間にあるメモリであり、データのRead/Writeを行うために使用する。

(4) シェアードメモリ（SM）

シェアードメモリは、CHA上のDKCMAINマイクロプログラム、DKA上のDKCMAINマイクロプログラムから共通にアクセス可能なメモリである。CHA、DKAからデータにアクセスするための制御情報が格納される。この制御情報には、セキュリティ機能の動作に必要な設定情報も含まれる。シェアードメモリ上の制御情報はDKCMAINマイクロプログラムを経由しないとアクセスできない。また、制御情報の更新は、SVP、Storage Navigatorからの指示により、TOEが行う。

(5) 記憶装置

記憶装置は複数のハードディスクで構成されており、ユーザデータが記憶される。 記憶装置内には、ユーザデータを格納するボリュームであるLDEV（論理デバイス）が作成される。ユーザデータへのアクセスは、LDEVの単位で管理され、DKCMAINマイクロプログラムを経由して行われる。LU(論理ユニット)はホストからのアクセス単位であり、1個または複数のLDEVにマッピングされる。

(6) SVP（サービスプロセッサ）

SVPは、ストレージ装置全体の管理を行うためにストレージ装置に内蔵されているサービスプロセッサであり、TOEの一部であるSVPプログラムが動作する。SVPプログラムは、ストレージ装置の保守機能及び装置制御情報の管理を行うためのソフトウェアであり、管理PC上で動作するStorage Navigatorプログラムから受け取った装置制御情報の設定指示をDKCMAINマイクロプログラムに対して送信する機能を有する。SVPプログラムは、ストレージ装置におけるセキュリティ機能の動作に関わる設定機能を有する。

(7) 保守員PC

保守員PCは、保守員が保守作業を行う際に使用するPCである。ストレージ装置内ネットワークである内部LAN経由で、リモートデスクトップ機能によりSVPに接続して使用する。

(8) 管理PC

管理PCは、Storage Navigator利用者がストレージ装置の運用と保守作業を行うために使用する顧客のPCであり、TOEの一部であるStorage Navigatorプログラムが動作する。管理PCとSVPは外部LANで接続される。

(9) Storage Navigatorプログラム

Storage Navigatorプログラム（以下、Storage Navigatorという。）は、ストレージ装置の装置制御情報の管理を行うために使用するソフトウェアである。

Storage NavigatorはJava applet programであり、SVPから管理PCにダウンロードされてWebブラウザ上で動作する。

(10) 他のストレージ装置

ストレージ装置のポートには、ホスト以外に、他のストレージ装置を接続することができる。他のストレージ装置を接続することにより、ストレージ装置間のデータコピー、バックアップ等が可能になる。他のストレージ装置から実施されるコピー操作は、信頼できるストレージ管理者が実施するものである。従って、ストレージ装置と接続する他のストレージ装置は、TOEを搭載するストレージ装置に限定される。

1.2.4 TOEの関係者

TOEでは以下のような利用者を想定している。

- 全体アカウント管理者

  管理者（全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者）のStorage Navigatorの操作に関するアカウントの登録、変更、削除ができる。

  システム構築時、初期アカウントとしてビルドインされている。

- 全体ストレージ管理者

  ストレージ装置全体の管理権限を持ち、TOEの機能であるVirtual Partition Manager機能により、ストレージ装置のリソース（ポート、キャッシュメモリ、LDEV）を論理パーティションに分割することができる。

- 分割ストレージ管理者

  全体ストレージ管理者から割り当てられた論理パーティション内のリソース(ポート、キャッシュメモリ、LDEV)を管理でき、ホストの識別情報であるWWNと、アクセスを許可するLDEV番号の関係付けを行う。

- 分割アカウント管理者

  分割した論理パーティションのアカウントを管理でき、分割ストレージ管理者用アカウント及び分割アカウント管理者用アカウントの作成、変更、削除を行うことが可能である。

- 監査ログ管理者

  ストレージ装置で取得している監査ログを管理でき、監査ログの参照やダウンロード、及びsyslogに関する設定が可能である。

- 保守員

  保守員は、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し、ストレージ装置を設置する際の初期立上げ処理、部品の交換や追加等の保守作業に伴う設定変更、異常時の復旧処理等を担当する。また、顧客からの要請により、全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者が行う設定作業を代行

する場合もある。保守員は、保守員用PCからSVPへアクセスし、保守作業を実施する。

・ ストレージ利用者

ストレージ装置の利用者でホストを表す。ストレージ装置と接続されたホストから、ストレージ装置内に保存されたデータを使用する。

全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者をまとめて、Storage Navigator利用者と呼ぶ。

1.2.5 保護資産

ストレージ装置にとって最も重要な資産は、ディスクドライブ内に格納されているストレージ利用者のユーザデータである。ユーザデータの完全性及び機密性を維持するため、Storage Navigator利用者による権限外の設定変更、またはストレージ利用者による権限外のアクセスからの保護が必要である。

複数に分割された論理パーティションが存在する環境において、パーティション内のLDEVに存在するストレージ利用者のユーザデータが保護対象資産であり、許可されていないストレージ利用者のアクセスから保護対象資産を保護する。さらに、論理パーティションで識別された範囲への操作権限を持たない分割ストレージ管理者による保護対象資産の削除を防止する。

1.2.6 TOEの機能

TOEはストレージ装置に接続される様々なホストからストレージ装置内に存在するユーザデータへの意図しないアクセスを行うことができないようにアクセス制御を実現するために、以下の機能を提供する。

・ Storage Navigator機能（セキュリティ機能）

セキュリティ機能の設定を含むディスクサブシステムの管理のためのVirtual Partition Manager機能、LUN Manager機能、監査機能の各設定（作成、変更、削除）はStorage Navigator機能による識別認証を介して初めて利用可能となる。またStorage Navigator利用者アカウントの設定（作成、変更、削除）はこのStorage Navigator機能を用いて行う。

ストレージ装置と管理PC間の通信データの漏洩、改ざんを防ぐため、Storage NavigatorとSVP間の通信はSSLにより暗号化する。

・ Virtual Partition Manager 機能（セキュリティ機能）

ディスクサブシステム全体のリソース（ポート、キャッシュメモリ、LDEV）を複数の仮想ディスクサブシステムに分割し、それぞれの仮想ディスクサブシステムの分割ストレージ管理者が、それぞれの仮想ディスクサブシステムだけにアクセスできる。これにより、他の組織のボリュームを壊したり、特定の組

織のデータが漏洩したりすることを防ぐことができる。図1-3に仮想ディスクサブシステムの概要を示す。

CLPR：キャッシュ論理パーティション
キャッシュメモリを論理的に分割することによって作成されるパーティション。

SLPR：ストレージ論理パーティション
ストレージ装置内のキャッシュとハードディスクドライブを論理的に分割することによって作成されるパーティション。

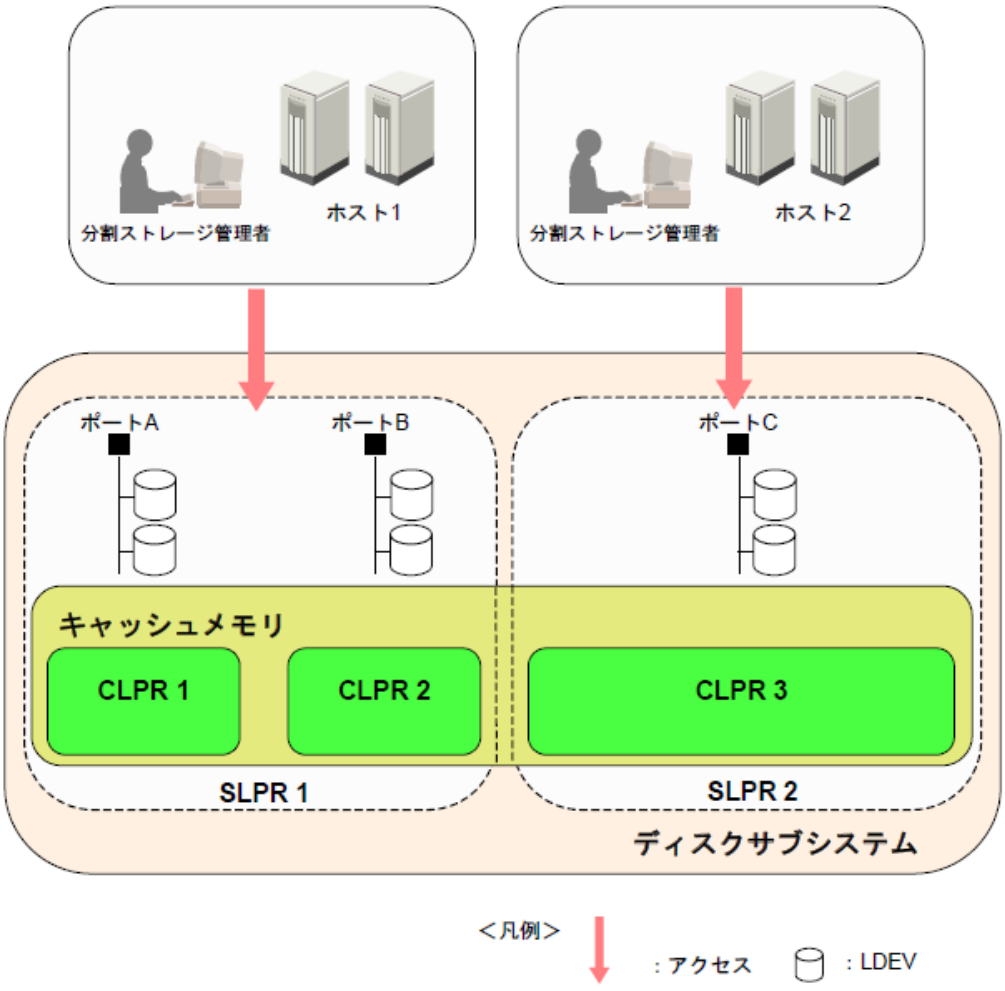

図1-3　仮想ディスクサブシステム

・ LUN Manager機能（セキュリティ機能）

ユーザデータを格納するLDEVはStorage Navigatorを利用して生成され、生成時にSLPRとの関連付けが行われる。ホストからLDEVへアクセスを行うためには、ホストを接続したCHA上のポートとLDEVの関連付けを行う。具体的には、ホストとアクセスを許可するLDEV とを関係付けるLU 番号を付与して

LU パスを設定する。当該LDEV に対するデータの読み書きは、LU パス設定が行なわれたホストからのみ可能となり、LU パス設定が行われていないホストからのデータの読み書きは許可されないように、LDEVへのアクセス制御を行う。

・ ホストの識別・認証機能（セキュリティ機能）

ホストをＳＡＮに接続する場合、不正なホストが接続されないように、FC-SP機能による認証を行う。ホスト認証の設定は、全体ストレージ管理者または分割ストレージ管理者がLUN Managerを使用して、ホストの認証を行うかどうかを各ホストに設定する。認証を行うホストはユーザ情報(WWN、シークレット（パスワード）)を登録する。

・ 監査ログ機能（セキュリティ機能）

Storage Navigator及びDKCMAINマイクロプログラムによって提供される。Storage Navigatorは、ログインの成功・失敗、構成や設定の変更等のセキュリティに関連するイベントを記録している。DKCMAINマイクロプログラムは、LUパス情報の作成、削除、変更等のセキュリティに関連するイベントを記録している。

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セキュリティ認証申請手続等に関する規程」[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」[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「Hitachi Universal Storage Platform V セキュリティターゲット」（以下「ST」という。）[1] 、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B、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、「評価報告書(URE-ETR-0001-02)」（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20年12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適合である。

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は、脅威エージェントのもつ攻撃能力は「低」であることを想定しているため、SOF-基本で十分である。

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、「1.2.6 TOEの機能」を参照。

1.5.5 脅威

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_XCNTL	Storage Navigator利用者のうち、分割ストレージ管理者、分割アカウント管理者が、自身の権限を越えた範囲のストレージ装置の設定変更を行うことにより、ホストがアクセ

	スを許可されていないLDEVにアクセスできてしまうかもしれない。
T.TSF_COMP	第三者が、Storage Navigator－SVP間の通信路に不正に機器を接続し、データの盗聴、または改ざんを行うかもしれない。
T.LP_LEAK	ホスト機器管理者等の第三者が、接続を許可されていないホストをSANに接続してLDEVにアクセスにすることにより、データの漏えい、改ざんが行われるかもしれない。
T.CHG_CONFIG	第三者が、Storage Navigatorを使用してストレージ装置の設定を変更してしまうかもしれない。

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.MASQ	顧客要求によってホストの識別認証が求められる場合、FC-SPの識別認証が終了するまでは、当該ポートのアクセスは禁止されなければならない。

1.5.7 構成条件

TOEは、以下のストレージ製品のいずれかに含まれる。

- Hitachi Universal Storage Platform V
- Hitachi Universal Storage Platform H24000
- Hitachi Universal Storage Platform VM
- Hitachi Universal Storage Platform H20000

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.NOEVIL	Storage Navigator利用者のうち、全体ストレージ管理者、全体アカウント管理者、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、不正行為を働かず信頼できるものと想定する。 分割ストレージ管理者、分割アカウント管理者は、権限を持つ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、不正行為を働かず信頼できるものと想定する。
A.NOEVIL_MNT	保守員は、ホストとCHA上のポートと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、不正行為を働かず信頼できるものと想定する。
A.PHYSICAL_SEC	ストレージ装置は、全体ストレージ管理者、全体アカウント管理者、監査ログ管理者及び保守員のみ入退出が許可されているセキュアなエリアに設置され、許可されない物理的アクセスから完全に保護されているものと想定する。 注）内部LANに関する保護も含んでいる。
A.ILLEGAL_SOFT	管理PCには不正なソフトウェアがインストールされないものと想定する。
A.CONNECT_STORAGE	TOEは、他のストレージ装置を接続してストレージ装置間のデータコピー、またはデータのバックアップを取得する機能を持っている。この機能を使用すれば、他のストレージ装置から、TOEの保護対象資産であるユーザデータの変更及び閲覧が可能である。これらの機能の操作は、信頼できるストレージ管理者しか操作できない運用を想定する

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。

【日本語】

- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000　ISO15408認証取得機能 取扱説明書
- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000 利用者ガイダンス

【英語】

- Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM ISO15408 Certification Instructions Manual
- Hitachi Universal Storage Platform V / Hitachi Universal Storage

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19年8月に始まり、平成20年12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20年8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20年8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

開発者が実施したテストの構成を図2-1、表2-1に示す。

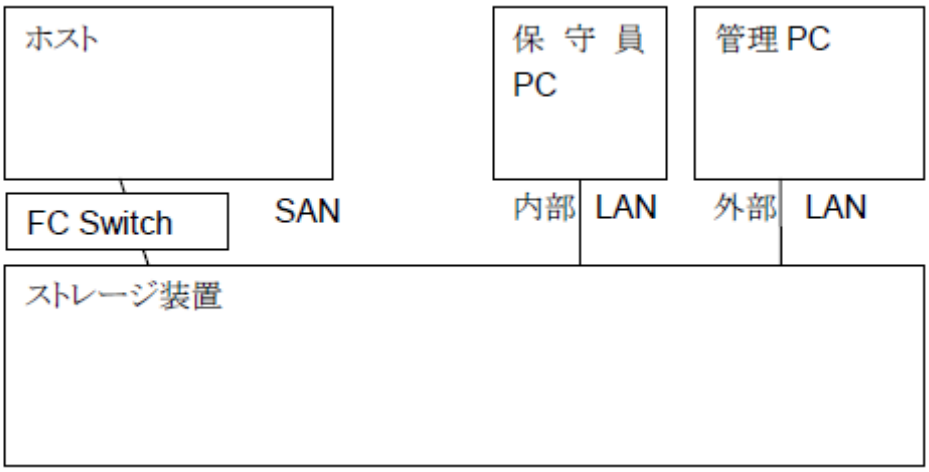

図2-1　開発者テストの構成図

表2-1　テスト構成要素

構成要素	使用機器/ソフトウェア
ストレージ装置 （TOE、保守員PC含む）	Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000 【TOE】 ・ DKCMAIN マイクロプログラム バージョン60-02-32-00/00 ・ SVPプログラム バージョン60-02-26/00 （管理PCのStorage Navigatorを含む）
ホスト	Windows 2000 SP3 CPU：Intel Xeon 2.0 GHz
管理PC	Windows XP Professional (SP2) ・ CPU： Pentium 4 2.4GHz 推奨：Pentium 4 3GHz 以上 ・ RAM： 1GB; 推奨： 1 GB ・ 有効なHDD 空き領域： 150 MB 以上 ・ モニター： High-Color 16-bit; 解像度 1024x768 ・ LAN カード： 100Base-T
FCストレージネットワーク	Cisco 型名：MDS 9216i 2Gbps 14 ポート
Webサーバ	Apache バージョン2.2.4

Webブラウザ	Internet Explorer 6.0 SP2
Javaランタイム環境	JRE 1.5.0_06

1) 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

開発者が実施したテストの構成を図2-1に示す。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。

なお、Hitachi Universal Storage Platform VM、Hitachi Universal Storage Platform H20000は、同一のTOEが搭載される。各々の機器の違いは、搭載できるディスク容量、ファイバチャネルポート数の違い及び販売時のブランド名が違うだけである。TOE に関係するハードウェアおよびソフトウェアが同一であるため、1 種類のストレージ装置でのテストを実施した。

b. テスト手法

テストには、以下の手法が使用された。

①Storage Navigator の操作検証についてはStorage Navigator に入力したパラメタが操作結果画面に表示されていることを検証する。

②監査ログファイルの検証についてはStorage Navigator からの各操作において、監査ログが取得されていること、監査ログの内容が監査ログリファレンスガイドの内容と一致していることを検証する。

③ホストのアクセス結果の検証についてはテストツールを使用してホストからTOE にアクセスした時の画面をキャプチャし、結果を検証する。

c. 実施テストの範囲

テストは開発者によって134項目実施されている。

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

評価者が実施したテストの構成は、開発者テストと同様の構成である。

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

評価者が実施したテストの構成を図2-1に示す。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

テストは、開発者テストと同じ手法で実施された。

c. 実施テストの範囲

評価者が独自に考案した独立テストを13項目、侵入テストを11項目、開発者テストのサンプリングによるテストを41項目、計65項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストとは異なるパラメタの追加のテスト、SOF主張の観点でのテストを実施する。(独立テスト)

② 開発者テストの結果が正当であることを確認するために、開発者が設定したテストのサブセット内から1つは実施する。(サンプリングテスト)

③ 脆弱性が悪用されることがないという開発者の根拠に論理的な問題はないが、別の手法、条件を用いた場合に、この脆弱性が問題とならないかを確認するため(反証)にテストを実施する。(侵入テスト)

④TOE が意図する環境で、開発者が考慮していない動作環境要素(JRE:Javaランタイム環境)で明白な脆弱性を持つかどうかを調べるためにテストを実施する。(侵入テスト)

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

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 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に対する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種別、境界の記述が明瞭であることを確認している。
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。
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概説が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、前提条件のいずれかへ遡れ、

	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。
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適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。
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環境がないため非適応であること、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。

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。
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

- TOEが搭載されるストレージ装置は、日本国外でも販売されるが、本評価の対象は、株式会社 日立製作所 RAIDシステム事業部が製造し、出荷したものである。
- ホストの管理（SAN情報の改ざん防止等）はTOEの関心事項ではない。

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

本報告書で使用されたTOE特有の略語を以下に示す。

CHA	Channel Adapter
DKA	Disk Adapter
DKC	Disk Controller
LAN	Local Area Network
SAN	Storage Area Network
SVP	Service Processor
WWN	World Wide Name

本報告書で使用された用語を以下に示す。

キャッシュメモリ	最近または頻繁にアクセスされたデータの一時的な高速ストレージ領域。
ディスクサブシステム	ストレージ装置のことで、Hitachi Universal Storage Platform V、Hitachi Universal Storage Platform VM等を指す。
ファイバチャネル	Storage Area Network（SAN）を構築するための高速ネットワークテクノロジー。
ポート	ファイバチャネルの終端。各ポートはポート番号により識別される。
CLPR（Cache Logical Partition）	キャッシュ論理パーティション。 キャッシュメモリを論理的に分割することによって作成されるパーティション。CLPR内に1つ以上のパリティグループを割り当てる。
FC-SP	Fibre Channel Security Protocol

	ホストまたはファイバチャネルスイッチとストレージ装置との通信を行う際、お互いの機器認証を行うためのプロトコル。
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ボリュームの単位。論理ボリュームとも呼ばれる。
LU（論理ユニット）	ホストから使用するLDEVをLUと呼ぶ。ファイバチャネルインタフェースでは1個または、複数のLDEVにマッピングされたLUにアクセスできる。
LU パス	オープンシステム用ホストとLU 間を結ぶデータ入出力経路。
LUN （Logical Unit Number）	論理ユニット番号。 ファイバチャネルポートに関係付けられて、ホストからアクセス可能であるLDEV。または、オープンシステム用のボリュームに割り当てられたアドレス。
SLPR （ Storage Logical Partition）	ストレージ論理パーティション。 ストレージ装置内のキャッシュとハードディスクドライブを論理的に分割することによって作成されるパーティション。１つ以上のCLPRと１つ以上の対象ポートを割り当てる。
WWN （World Wide Name）	ファイバチャネルなどのハード固有の64bitのアドレス

6 参照

[1] Hitachi Universal Storage Platform V セキュリティターゲット バージョン 1.13（2008年10月8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19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] 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

[4] 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

[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] 評価報告書(URE-ETR-0001-02) 第1.2版 2008年12月8日
株式会社電子商取引安全技術研究所 評価センター