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

申請受付日（受付番号）	**平成**17**年**9**月**30**日** (IT**認証**5068)
認証番号	C0102
認証申請者	**株式会社 日立製作所**
TOE**の名称**	SANRISE Universal Storage Platform **用** CHA/DKA **プログラム** (**日本国内**) TagmaStore Universal Storage Platform CHA/DKA Program (**海外**) SANRISE Network Storage Controller **用** CHA/DKA **プログラム** (**日本国内**) TagmaStore Network Storage Controller CHA/DKA Program (**海外**) SANRISE H12000 **用** CHA/DKA **プログラム** (**日本国内**) SANRISE H10000 **用** CHA/DKA **プログラム** (**日本国内**)
TOE**のバージョン**	50-04-34-00/00
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19年6月27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 2.1
② Common Methodology for Information Technology Security Evaluation Version 1.0
③ CCIMB Interpretations-0407

評価結果：合格

「SANRISE Universal Storage Platform 用 CHA/DKA プログラム (日本国内)、TagmaStore Universal Storage Platform CHA/DKA Program (海外)、SANRISE Network Storage Controller 用 CHA/DKA プログラム (日本国内)、TagmaStore Network Storage Controller CHA/DKA Program (海外)、SANRISE H12000 用 CHA/DKA プログラム (日本国内)、SANRISE H10000 用 CHA/DKA プログラム (日本国内) Version 50-04-34-00/00」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、「SANRISE Universal Storage Platform 用 CHA/DKA プログラム (日本国内)、TagmaStore Universal Storage Platform CHA/DKA Program (海外)、SANRISE Network Storage Controller 用 CHA/DKA プログラム (日本国内)、TagmaStore Network Storage Controller CHA/DKA Program (海外)、SANRISE H12000 用 CHA/DKA プログラム (日本国内)、SANRISE H10000 用 CHA/DKA プログラム (日本国内) Version 50-04-34-00/00」（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: SANRISE Universal Storage Platform 用 CHA/DKA プログラム (日本国内)
TagmaStore Universal Storage Platform CHA/DKA Program (海外)
SANRISE Network Storage Controller 用 CHA/DKA プログラム (日本国内)
TagmaStore Network Storage Controller CHA/DKA Program (海外)
SANRISE H12000 用 CHA/DKA プログラム (日本国内)
SANRISE H10000 用 CHA/DKA プログラム (日本国内)

バージョン: 50-04-34-00/00

開発者: 株式会社 日立製作所

1.2.2 製品概要

TOEはストレージ装置をコントロールするソフトウェアである。

TOEは、ストレージ装置内のユーザデータに対し、意図しないアクセス(すなわち変更されてはならないデータへの不正アクセスや誤操作による改変)が行われないようにアクセスの制御をするためのセキュリティ機能を持つ。

1.2.3 TOEの範囲と動作概要

TOEを含むストレージ装置は図1-1のような構成で使用される。

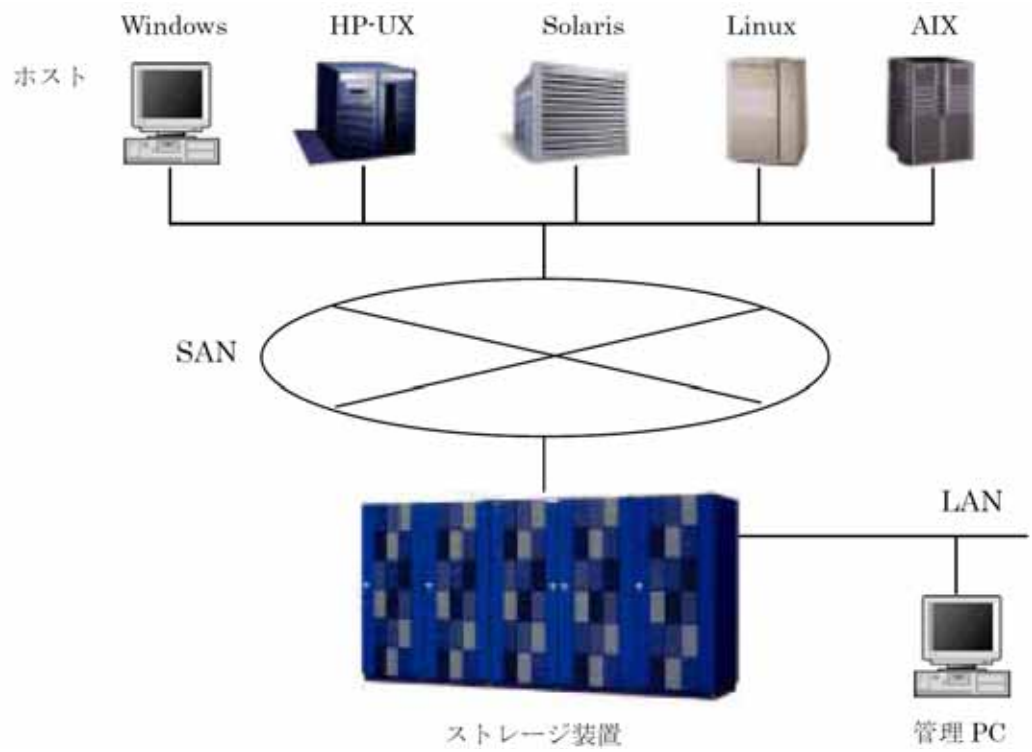

図1-1　ストレージ装置の構成

- ストレージ装置の設置場所

  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。

- SANとホスト

  Windows、HP-UX、Solaris 等の各種オープン系サーバ（本認証報告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、通常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。

- 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(Local Area Network)を介して接続される。

  LAN に接続された管理PC やその他のPC に関しては、組織により正規に接続されたものであり、OS の認証機能等により正当な人物しか操作できない環境を想定している。

ストレージ装置内は図1-2のような構成であり、その中で、TOEはストレージ装置内の「CHAプログラム」と「DKAプログラム」である。

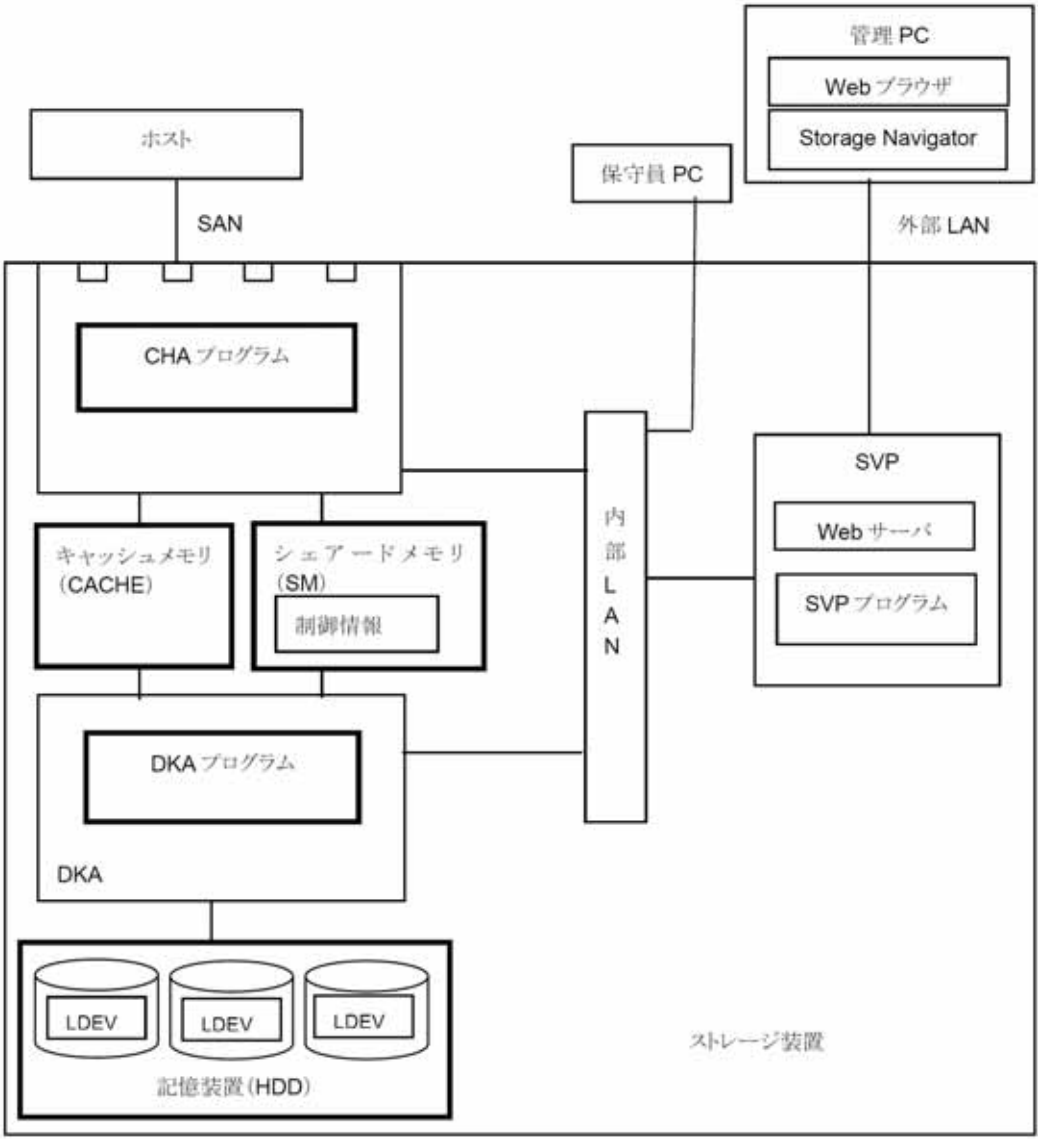

図1-2　ストレージ装置内の構成

- 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CHAプログラムが動作する。

- ディスクアダプタ（DKA）

  ディスクアダプタは､CACHEとHDD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DKAプログラムが動作する。CHAプログラムとDKA プログラムは連携して、「CHA/DKAプログラム」の機能を実現する。

- 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。

- シェアードメモリ（SM）

  シェアードメモリは、CHA プログラム、DKA 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の更新は、SVP、Storage Navigator からの指示により、TOE が行う。

- 記憶装置

  記憶装置（HDD）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。HDD 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 の単位で管理される。

- SVP

  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る。

- 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。

- Storage Navigator

  Storage Navigator は、顧客のストレージ管理者が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。

1.2.4 TOEの関係者

TOEでは、以下の役割の利用者を想定する。

- ストレージ管理者

  管理PC 上のStorage Navigatorを用いて、ストレージ装置の管理を行う。TOEの機能であるData Retention Utility機能の設定操作が可能である。

- 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人。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に伴う設定変更、異常時の復旧処理などを担当する。また、顧客からの要請により、ストレージ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。直接、ストレージ装置内の機器に触ったり、内部LANに接続した機器を操作したりできるのは、保守員だけである。

- ストレージ利用者

  ストレージ装置の利用者。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。

1.2.5 TOEの機能

TOEは以下の機能を持つ。

- LDEVへのアクセス仲介

  ホストからCHA上へのポートに対してアクセスの要求が来ると、TOEは、そのポートと関連付けられたLDEVの間のデータ転送の制御を行う。その結果、ホストから、CHA上のポートに関係付けられたLDEVにアクセスすることができる。

- ポートとLDEVの関連付け

  Storage Navigator/SVPからの要求に応じて、TOEはポートとLDEVの関連付けの設定を行う。

- LDEVの管理

  Storage Navigator/SVPからの要求に応じて、TOEは、LDEVの作成および更新操作（削除、フォーマット、シュレッディング）を行う。

- コピー機能

Storage Navigator/SVPからの要求に応じて、TOEは、LDEV間のコピーを行う。

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「SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 ユーザデータ保護機能 セキュリティターゲット」（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][14]のいずれか) 附属書C、CCパート2（[6][9][12][15]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][16]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、「SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000用 CHA/DKA プログラム Version 50-04-34-00/00 TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00 評価報告書」（以下「評価報告書」という。）[22]に示されている。なお、評価方法は、CEM（[14][15][16][17]のいずれか）に準拠する。また、CC及びCEMの各パートは補足（[20][21] のいずれか）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6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は、以下のとおりである。

- Data Retention Utility 機能

  Data Retention Utility 機能は、ストレージ装置内のLDEV に対して設定された「書き込み許可」または「書き込み拒否」のアクセス属性に基づいて、ホストからのLDEV へのアクセスとStorage Navigator/SVPから要求されるコピーを制御し、「書き込み拒否」属性が設定されたLDEV がストレージ利用者の誤操作や不正なアクセスによって変更されることを防止する機能である。

  Data Retention Utility 機能において、LDEV に「書き込み拒否」のアクセス属性を設定する場合、その属性の有効期限の設定を同時に行う。TOE は、有効期限が有効な間は、「書き込み拒否」から「書き込み許可」属性への変更を禁止しており、TOE 外からのいかなる要求であっても、「書き込み許可」に変更することはできない。有効期限が切れた場合は、「書き込み許可」への変更を許可する。また一度設定した有効期限を変更する場合、期限を延長することはできるが、短縮することはできない。この理由は、ストレージ装置で扱うユーザデータの重要性を考慮したためである。

アクセス属性および有効期限の設定は、Storage Navigator/SVP からのみ行うことができる。

1.5.5 脅威

本TOEが守るべき資産は、ストレージ装置に格納されているユーザデータの中で、ストレージ管理者（または保守員）により変更されてはならないと定義されたユーザデータである。このユーザデータに対して発生する脅威を以下に示す。なお、以下の記載の中で第三者とはストレージ管理者、ストレージ利用者、保守員のいずれにも該当しない人物であり、ストレージ装置の利用権限を持たないことを想定している。

また、攻撃者の攻撃能力は「低」であると想定している。

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. Delete/Change_User_Data	変更されてはならないユーザデータが格納されているLDEVに対して、ストレージ利用者または第三者がホストあるいはSAN に接続された機器から書き込み要求を行い、ユーザデータが変更や消去されてしまうかもしれない。

1.5.6 組織のセキュリティ方針

Data Retention Utility 機能に関して、組織のセキュリティ方針として以下の機能が求められている。下記要件は、Data Retention Utility 機能が実装すべき要件として求められているものであり、保護対象資産に対する攻撃に対応するものではない。

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.Protect_DRU	TOEは、変更されてはならないユーザデータが格納されているLDEVに設定されている有効期限の範囲内ならば、「書き込み拒否」から「書き込み許可」への属性の変更を禁止すること。
P.Retention_Period	TOEは、「書き込み拒否」のアクセス属性に設定されている有効期限の短縮を禁止すること。

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。

- SANRISE Universal Storage Platform (日本国内)
- TagmaStore Universal Storage Platform (海外)
- SANRISE Network Storage Controller (日本国内)
- TagmaStore Network Storage Controller (海外)
- SANRISE H12000 (日本国内)
- SANRISE H10000 (日本国内)

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.PhysicalProtection-Storage	ストレージ装置は、ストレージ管理者およ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。
A.Protection-Network	ストレージ装置を含む顧客のネットワーク環境（外部LAN）では、ストレージ管理者がストレージ装置の管理・運用を行う際に使用する管理PC 以外の機器からストレージ装置へ接続できないように管理されているものと想定する。
A.Protection-PC	管理PC は、ストレージ管理者のみが使用できるように管理されているものと想定する。
A.Responsibility-Admin	ストレージ管理者は、ストレージ装置の管理・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.Responsibility-Maintenance	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、不正行為をはたらかないことを信頼できるものと想定する。
A.Connect-Storage	ユーザデータのリモートコピーのために、TOEに対し他のストレージ装置を接続する場合、TOE内のLDEVのアクセス属性に基づいてコピー動作が実行されるストレージ装置が接続されるものと想定する。

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。

- SANRISE Universal Storage Platform / SANRISE Network Storage Controller /SANRISEH12000 / SANRISE H10000 ISO15408 認証取得機能取扱説明書

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17年10月に始まり、平成19年6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18年10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

開発者が実施したテストの構成を以下に示す。

- 評価用TOE
  - CHA/DKA プログラム Version 50-04-34-00/00

- ハードウェア
  - ストレージ装置
    装置：SANRISE Universal Storage Platform（H-65A3-5/A-65A3-5）
  - ホスト
    サーバ：HP-9000（PA-8000 875MHz）
    OS：HP-UX 11.23
  - 管理PC
    PC：NEC Mate MJ28V/L-H（Pentium4 2.4GHz）
    OS：Windows XP Professional SP2
  - ハブ：Accton ES3016A
- ソフトウェア
  - 管理PC
    Storage Navigator（SVP バージョン 50-04-34-00/00）

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

開発者が実施したテストの構成は上記のとおりである。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管理PC にインストールしたStorage Navigatorを用いて、評価用TOEに実行させる機能をメニュー画面から選択し、評価用TOEが設計通りにふるまうことを検証する。

②ホスト上のテストツールを用いて評価用TOE にデータのRead/Writeコマンドを送信し、Storage Navigatorから設定したセキュリティ属性に従って、TOEのセキュリティ機能が設計通りにふるまうことを検証する。

③ふるまいの検証は、管理PCもしくはホストに記録されるTOEへの入出力情報のログをファイルダンプし、期待されるテスト結果と実際のテスト結果を比較検証する。

c.実施テストの範囲

テストは開発者によって48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は、開発者テストと同様の構成である。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行われた。

c.実施テストの範囲

評価者が独自に考案したテストを4項目、開発者テストのサンプリングによるテストを12項目、計16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 機能仕様の記述から評価者が独立に導き出したテスト項目のうち、開発者テストを補強するのに効果的なテストを実施する。

② 開発者テストで実施されたテスト項目のパラメータの網羅度を高めるテストを実施する。

③ 複数のインタフェースを組み合わせて使用することで、開発者テストを補強するテストを実施する。

④ すべてのTSFIを必ず1回はテストするように開発者テストをサンプリングする。

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

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。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。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.1.3E	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。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_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。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_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。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.1.1E	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環境がないために非適用であること、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。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。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_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。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。
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がないために非適用であ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、STでSOF主張がなされているセキュリティメカニズムがないことが妥当である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。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。
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
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。
SAN	Storage Area Networkの略。ファイバチャネルによりストレージ装置とホストコンピュータを接続した、ストレージ専用のネットワークである。ファイバチャネルにより、高速・高信頼のデータ通信が可能。

6 参照

[1] SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 ユーザデータ保護機能 セキュリティターゲット, Version 3.7（2007年6月14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17年7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17年7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17年7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 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月

[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法

[20] CCIMB Interpretations-0407

[21] 補足-0210 第2版、補足-0407

[22] SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000用 CHA/DKA プログラム Version 50-04-34-00/00 TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00 評価報告書 第1.4版（2007年6月14日）株式会社電子商取引安全技術研究所 評価センター