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. 6.14

株式会社 日立製作所

他社商標

Microsoft、Windows は、米国およびその他の国における米国 Microsoft Corp.の商標または登録商標です。

Solaris は、米国およびその他の国における Sun Microsystems, Inc.の商標または登録商標です。

HP-UX は、米国 Hewlett-Packard Company の登録商標です。

RedHat は、米国およびその他の国で RedHat, Inc.の商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標または登録商標です。

AIX は、IBM Corporation の商標または登録商標です。

その他記載されている会社名、製品名は各社の商標または登録商標です。

―目次―

1. ST 概説

本章では、ST や TOE の識別情報、ST の概要、および CC への適合性や使用する用語の説明を記述する。

1.1. ST 識別

以下に、ST および ST が対象とする TOE の識別情報を示す。

ST: 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. 6. 14, 株式会社 日立製作所

TOE: ・SANRISE Universal Storage Platform 用　CHA/DKA プログラム

Version 50-04-34-00/00 （日本国内）

・TagmaStore Universal Storage Platform CHA/DKA Program

Version 50-04-34-00/00 （海外）

・SANRISE Network Storage Controller 用　CHA/DKA プログラム

Version 50-04-34-00/00 （日本国内）

・TagmaStore Network Storage Controller CHA/DKA Program

Version 50-04-34-00/00 （海外）

・SANRISE H12000 用　CHA/DKA プログラム　Version 50-04-34-00/00 （日本国内）

・SANRISE H10000 用　CHA/DKA プログラム　Version 50-04-34-00/00 （日本国内）

本 ST の開発では次の基準を使用した。

- Common Criteria for Information Technology Security Evaluation Version 2.1（参考文献[1][2][3]）
- 情報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 2.1 平成 13 年 1 月翻訳第 1.2 版（参考文献[4][5][6]）
- CCIMB Interpretations-0407（参考文献[7]）
- 補足-0210 第 2 版（参考文献[8]）
- 補足-0407（参考文献[9]）

1.2. ST 概要

株式会社日立製作所製ストレージ装置「SANRISE Universal Storage Platform」(*1)および「SANRISE H12000」は、大容量、高速処理、高信頼性を実現したエンタープライズ向けストレージ装置である。また「SANRISE Network Storage Controller」(*1)および「SANRISE H10000」は、SANRISE Universal Storage Platform の大容量、高速処理、高信頼性を受け継いだミッドレンジクラス向けのストレージ装置である（以降、これらを“ストレージ装置”と記す）。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。そのため、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必要がある。

本 ST は、SANRISE Universal Storage Platform、SANRISE H12000、SANRISE Network Storage Controller および SANRISE H10000 におけるユーザデータの完全性を保護するためのセキュリティ機能について記述したものである。

(*1) 海外名は、「TagmaStore Universal Storage Platform」、「TagmaStore Network Storage Controller」である。

1.3. CC 適合

本 ST の CC 適合性は以下のとおりである。

- CC パート 2 適合
- CC パート 3 EAL 2 適合
- 適合する PP はない

1.4. 用語集

・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。

・RAID（Redundant Arrays of Inexpensive Disks）

ハードディスクなどの記憶装置を複数台用いてアクセスを分散させることにより、高速、大容量で信頼性の高いディスク装置を実現するための技術。RAID はその機能によって、RAID0 から RAID6 まで定義されている。

・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。

・アクセス属性

LDEV が読み書き可能になっているか読み取り専用になっているかを示す属性である。アクセス属性には「書き込み許可」と「書き込み拒否」が存在する。アクセス属性を変更するには、Data Retention Utility を使用する。

・副 VOL

ストレージ装置のコピー機能で使用される、コピー先のボリュームを指す。

・リモートコピー

ユーザデータのバックアップや災害リカバリの目的で、ストレージ装置間でユーザデータのコピーを行う機能のこと。ストレージ装置間はファイバチャネルインタフェースで接続される。

本 ST では、他のストレージ装置より TOE へユーザデータをコピーする場合に使用する。

2. TOE 記述

本章では、TOE の種別と範囲・境界を定義し、TOE についての全般的な情報を提供する。

2.1. TOE の種別

TOE である「SANRISE Universal Storage Platform 用 CHA/DKA プログラム Version 50-04-34-00/00」、「SANRISE Network Storage Controller 用 CHA/DKA プログラム Version 50-04-34-00/00」、「TagmaStore Universal Storage Platform CHA/DKA Program Version 50-04-34-00/00」、「TagmaStore Network Storage Controller CHA/DKA Program Version 50-04-34-00/00」、「SANRISE H12000 用 CHA/DKA プログラム Version 50-04-34-00/00」および「SANRISE H10000 用 CHA/DKA プログラム Version 50-04-34-00/00」（以降、“CHA/DKA プログラム”と記す）は、株式会社日立製作所製ストレージ装置「SANRISE Universal Storage Platform」、「SANRISE Network Storage Controller」「TagmaStore Universal Storage Platform」、「TagmaStore Network Storage Controller」、「SANRISE H12000」、「SANRISE H10000」上で動作するプログラム（ソフトウェア）である。上記ストレージ装置は、ハードウェアとしての装置の規模は異なるが、ともに“CHA/DKA プログラム”で制御される。これらのストレージ装置で使用される“CHA/DKA プログラム”は完全に同一のものである。TOE は、ストレージ装置内の複数の基板上に搭載され、ストレージ装置に接続されたホストとストレージ装置との間のデータ転送を制御する役割を持つ。

本 TOE は、変更されてはならないユーザデータとして定義されたデータを、操作ミスや故意の不正アクセスによる変更から保護する機能を提供するものである。

2.2. ストレージ装置を含むシステムの一般的な構成

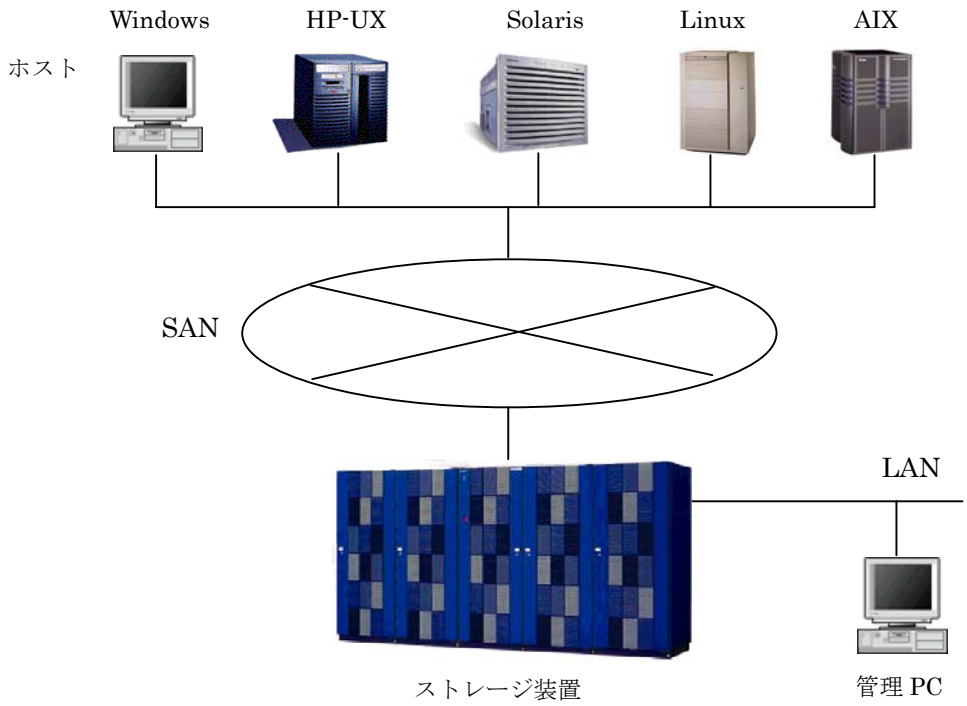

図 2.1 ストレージ装置を含むシステムの一般的な構成

図 2.1 に、ストレージ装置を含むシステムの一般的な構成を示す。図 2.1 に関する説明を以下に示す。

（1） 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。

（2）SAN とホスト

Windows、HP-UX、Solaris 等の各種オープン系サーバ（本 ST 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。

（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(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。

（4）TOE を含むストレージ装置

TOE を含むストレージ装置は、リモートコピー用のストレージ装置とファイバチャネルインタフェースで接続される。リモートコピー用のストレージ装置には、ガイダンスで接続が許可されているストレージ装置が接続された環境を想定している。

2.3. TOE とストレージ装置

図 2.2 に、ストレージ装置の一般的な構成を示す。

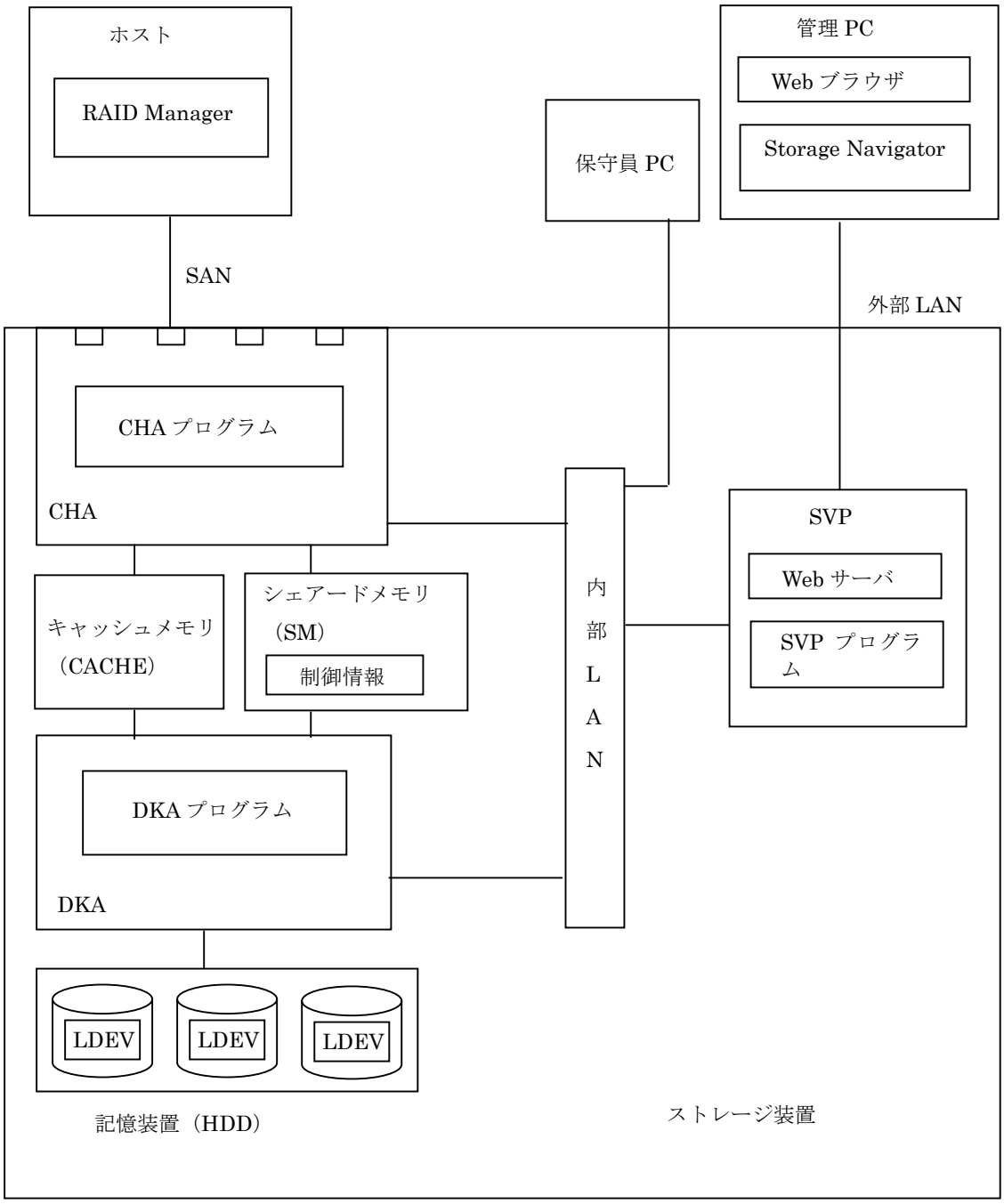

図 2.2　ストレージ装置の構成

ストレージ装置は、チャネルアダプタ（CHA）、シェアードメモリ（SM）、キャッシュメモリ（CACHE）、ディスクアダプタ（DKA）、記憶装置（HDD）が含まれる制御系と、SVP（Service Processor）が含まれる管理系に分けられる。制御系は、ディスクへのデータ入出力の制御を行い、管理系はストレージ装置の保守や管理を行う。これらの構成要素の説明を以下に示す。

2.3.1. 制御系

（1）チャネルアダプタ

チャネルアダプタ（CHA）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。

（2）ディスクアダプタ

ディスクアダプタ（DKA）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。

（3）キャッシュメモリ

キャッシュメモリ（CACHE）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

シェアードメモリ（SM）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（2.3.2 参照） からの指示により、TOE が行う。

（5）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。HDD は RAID 構成により、信頼性を向上させている。

CHA、SM、CACHE、DKA は高速クロスバ・スイッチで接続されている。

2.3.2. 管理系

（1）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。SVP 上で動作する SVP プログラムは、ストレージ装置の保守機能（各種構成部品の増設・減設・交換やプログラムのアップデート等）およ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、また Storage Navigator から受け取った装置制御情報の設定指示を TOE 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（Data Retention Utility 機能を指す。詳細は 2.6.2 節を参照。）の動作に関わる設定機能を有する。SVP プログラムは TOE には含まれない。

（2）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。

（3）Storage Navigator

Storage Navigator は、顧客のストレージ管理者（2.4 節参照）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。Storage Navigator は Applet プログラムであり、SVP から顧客の PC（管理 PC）にダウンロードされて使用される。悪意を持った第三者（3.2 節参照）による Storage Navigator の不正使用を抑止するため、Storage Navigator は利用者の識別認証機能を有する。

Storage Navigator は、ストレージ装置におけるセキュリティ機能（Data Retention Utility 機能を指す。詳細は 2.6.2 節を参照。）の動作に関わる設定機能を有する。Storage Navigator から TOE である CHA/DKA プログラムへの設定指示は、SVP を介して行なわれる。管理 PC と SVP は外部 LAN で接続される。

Storage Navigator は TOE には含まれない。

（4）RAID Manager

RAID Manager 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。顧客のストレージ管理者（2.4 節参照）が、顧客のホスト上で RAID Manager を動作させる。RAID Manager は TOE には含まれない。なお、本 ST では RAID Manager を使用していない装置構成を対象とする。（RAID Manager を使用するには、Storage Navigator からコマンドデバイス（RAID Manager のコマンド受信用 LDEV）を作成する必要が有るが、本 ST ではコマンドデバイスが作成されていない環境を想定している。）

制御系ネットワーク（CHA、SM、CACHE、DKA の高速クロスバ・スイッチ接続）と管理系ネットワーク（内部 LAN、外部 LAN）は完全に独立したものである。この構造により、内部 LAN や外部 LAN に接続されている SVP、Storage Navigator、保守員 PC から直接、SM、CACHE、HDD にアクセスすることはできない。そのため、管理系ネットワークからのユーザデータへの攻撃は完全に防御されている。

なお、ストレージ装置に内蔵される機器は出荷時に組み込まれており、利用者側で準備したり、変更したりすることはない。

2.3.3. TOE の範囲

図 2.3 に TOE の範囲を示す。

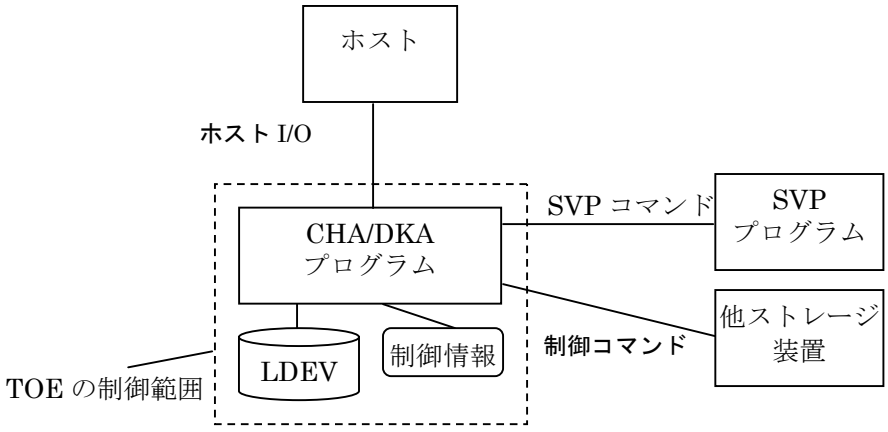

図 2.3　TOE の制御範囲

図 2.3 中の CHA/DKA プログラムが TOE であり、点線で囲った範囲が TOE の制御下にある。TOE は、シェアードメモリ内に格納される制御情報に基づき、記憶装置（HDD）内に作成された LDEV へのアクセスを制御する。

2.4. ストレージ装置の利用者

ストレージ装置に関係する者として、本 ST では以下のような利用者を想定している。

・ 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（詳細は 2.6.2 節を参照の事。）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。

2.5. 保護対象資産

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り、その完全性の維持が必要である。本 ST では、ストレージ管理者（または保守員）の指示により変更を禁止されたユーザデータを保護対象資産とする。TOE は、変更されてはならないユーザデータが格納された LDEV に対してアクセス制御を行い、ストレージ利用者の操作ミスや不正アクセスによる変更からユーザデータの完全性を確実に保護する、というセキュリティ機能を提供する。なお、アクセスが許可されている LDEV を不正にアクセス拒否に変更するような可用性の問題に関しては、本 ST では主張しない。

2.6. TOE の機能

TOE が提供する一般的 IT 機能、およびストレージ装置のデータセキュリティ機能の概要を以下に示す。

2.6.1 TOE が提供する一般的な IT 機能

TOE である CHA/DKA プログラムは、ストレージ装置の動作を制御するソフトウェアである。CHA プログラムは、ホストとストレージ装置間のデータ転送を制御するためのプログラムであり、DKA プログラムは、キャッシュ・ディスクドライブ間のデータ転送を制御するためのプログラムである。

ホストが 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 の関連付けを行う必要がある。この関連付けの設定は Storage Navigator/SVP にて行う。具体的には、ホストグループ（プラットフォームが等しい 1 つまたは複数個のホストをグループ化したもの）を作成して、ホストグループとアクセスを許可する LDEV との間に 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グループに属しているホストからのみ可能となり、LU パス設定が行なわれていないホストグループに属しているホストからのデータの読み書きは許可されない。

なお、CHA/DKA プログラムには、2.6.2 節に示すセキュリティ機能が含まれている。

2.6.2 TOE が提供するセキュリティ機能

（1）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 から行うことができる。ストレージ管理者の識別認証および設定操作機能は TOE の範囲外であるが、Storage Navigator/SVP から受け取った設定情報をストレージ装置の制御情報に反映させる処理は TOE で行われる。

ストレージ装置は、ユーザデータのバックアップ等の目的でユーザデータのコピー機能を持っている。コピー機能において、アクセス属性が「書き込み拒否」の LDEV に対するコピー動作は抑止される。（Storage Navigator/SVP からのコピー機能の運用に関しては、アクセス属性が「書き込み許可」に設定された LDEV に対するコピー操作は、ストレージ管理運用の中で計画的に行われる。）

また、リモートコピー機能において、TOE 内の副 VOL に対する他ストレージ装置からの書き込み指示に関しては、TOE としてはアクセス属性によらず書き込みを実施する。ただし、TOE 内の副 VOL に対する書き込み指示を TOE に送信するか否かの判断を他ストレージ装置にて行っており、ストレージシステム全体としては「書き込み拒否」の副 VOL に対する書き込みは抑止されている。

また、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）に関しては、TOE としては指示されたこれらの操作をアクセス属性によらず実施する。ただし、更新操作の実施可否の判断を Storage Navigator/SVP で行っており、ストレージ装置全体としては「書き込み拒否」の LDEV への更新操作は抑止されている。なお、LDEV の更新操作についてはユーザデータに直接関わる極めて重要な操作であり、ストレージ管理運用の中で計画的に行われる。このため、Storage Navigator/SVP から「書き込み拒否」属性が設定されている LDEV に対する更新操作が運用の中で行われることはない。

また、ストレージ利用者が LDEV に対してデータの書き込みまたは読み込み操作を行っている最中に、ストレージ管理者により LDEV のアクセス属性および有効期限の設定変更が行われることは運用上ない。この設定変更抑止に関しては、設定変更指示を TOE へ送信するか否かの判断を Storage Navigator/SVP で行っている。

TOE の一般機能であるホストグループと LDEV との関連付けの設定が誤って設定されてしまった場合や、ホストと CHA 上のポートとの接続が誤って行われた場合に対しても、LDEV に「書き込み拒否」属性が設定されていれば、LDEV 内のユーザデータは保護される。

本機能が必要となる背景を以下に示す。

ホスト OS の機能により LDEV に対するアクセスを Read Only に制限しようとする場合、LDEV を Read Only マウントすることが考えられる。しかし、ホストによっては OS に Read Only マウントの機能が無く、これが不可能なケースがある。このようなケースでは、ストレー

ジ側でその LDEV のアクセス属性を「書き込み拒否」属性に設定することが必要となる。また、ホスト側で Read Only マウントが可能なケースであっても、その LDEV にアクセスするホストが複数存在するようなケースでは、誤操作を防ぐため、ストレージ側でその LDEV を「書き込み拒否」属性に設定する必要がある。

また、ホストにマウントせずに、ホストのアプリケーションからブロック単位でアクセスするようなケース（データベース等）では、OS のファイルシステムによるアクセス制御がかけられないため、ストレージ側で「書き込み拒否」属性の設定が必要である。

3. TOE セキュリティ環境

本章では、ST が意図している TOE の使用環境や使用方法、保護すべき資産とそれらに対する脅威、および TOE が従うべき組織のセキュリティ方針を定義する。

3.1. 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。

3.2. 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。

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。

3.3. 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。

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。

4. セキュリティ対策方針

本章では、TOE およびその環境に対するセキュリティ対策方針を定義する。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に示す。

O.Protect_LDEV

TOE は、LDEV に設定されているアクセス属性に基づき、ホストから LDEV への書き込み可否を制御できなければならない。

具体的には、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」の属性に基づいて、書き込み可否の制御を行わなければならない。

O.Protect_DRU

TOE は、アクセス属性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」への属性の変更を抑止しなければならない。

O.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抑止しなければならない。

4.2. 環境のセキュリティ対策方針

環境のセキュリティ対策方針を以下に示す。

OE.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保護されていなければならない。

OE.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なければならない。

OE.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なければならない。

OE.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人物が割り当てられなければならない。

OE.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、不正行為を働かないことを信頼できる人物が割り当てられなければならない。

OE.Connect-Storage

TOE に接続されるストレージ装置は、日立製作所製のエンタープライズ向けストレージ装置でなければならない。なお、接続可能な機種はガイダンスに記載される。

5. IT セキュリティ要件

本章では､TOE またはその環境が満たしていなければならない IT セキュリティ要件を定義する。

なお、セキュリティ要件に対して割付、選択、および詳細化を実施した箇所は、『［　］』で示す。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

以下のコンポーネントは全て CC パート２に含まれるものである。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1　TSF は、[割付:

- サブジェクト；ホスト要求を代行するプロセス、SVP 要求を代行するプロセス、および他ストレージ装置要求を代行するプロセス
- オブジェクト；LDEV

操作；ホスト要求を代行するプロセス、SVP 要求を代行するプロセス、および他ストレージ装置要求を代行するプロセスから LDEV への書き込み操作]に対して[割付：DRU アクセス制御 SFP]を実施しなければならない。

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1　TSF は、以下の[割付:

- サブジェクト；ホスト要求を代行するプロセス、SVP 要求を代行するプロセス、および他ストレージ装置要求を代行するプロセス
- オブジェクト；LDEV
- セキュリティ属性；アクセス属性

]に基づいて、オブジェクトに対して、[割付：DRU アクセス制御 SFP]

を実施しなければならない。

FDP_ACF.1.2　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない: [割付:

SM 上の制御情報に定義されているアクセス属性に基づき、ホスト要求を代行するプロセス、SVP を代行するプロセス、および他ストレージ装置要求を代行するプロセスからの LDEV へのアクセスが制御される。具体的には以下の規則となる。

ホスト要求を代行するプロセス：

アクセス属性	オブジェクトに対する操作の規則
書き込み許可	ホストからの I/O による書き込みを許可する。
書き込み拒否	ホストからの I/O による書き込みを拒否する。

SVP 要求を代行するプロセス：

SVP からの LDEV の作成および更新操作に関しては、アクセス属性によらず下記の操作を可能とする。

・LDEV の作成（オブジェクト自体の作成処理。）

・LDEV の削除（オブジェクト自体の削除処理。）

・LDEV のフォーマット（LDEV へフォーマットデータを書き込む処理。オブジェクト自体は削除しない。）

・LDEV のシュレッディング（LDEV へダミーデータの書き込みを複数回行い、データを完全に消去する処理。オブジェクト自体は削除しない。）

また、SVP からのコピー機能実行指示に対して、LDEV のアクセス属性により、下記の規則を実行する。

アクセス属性	オブジェクトに対する操作の規則
書き込み拒否	コピー動作による書き込みを拒否する。

他ストレージ装置要求を代行するプロセス：

LDEV のアクセス属性によらず、他ストレージ装置からの LDEV への書き込みを実行する。

]。

FDP_ACF.1.3　TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: なし]。

FDP_ACF.1.4　TSF は、[割付: なし]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FMT_MSA.3 TSF 静的属性初期化

下位階層: なし

FMT_MSA.3.1　TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択：許可的]デフォルト値を与える[割付：DRU アクセス制御 SFP]を実施しなければならない。

FMT_MSA.3.2　TSF は、オブジェクトや情報が生成されるとき、[割付：なし]が、デフォルト値を上書きする代替の初期値を指定することを許可しなければならない。

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_SMR.1 セキュリティ役割

下位階層: なし

FMT_SMR.1.1　TSF は、役割[割付：ホスト、Storage Navigator/SVP、他ストレージ装置]を維持しなければならない。

FMT_SMR.1.2　TSF は、利用者を役割に関連付づけなければならない。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1　TSF は、セキュリティ属性[割付：アクセス属性]に対し[選択：改変]をする能力を[割付：Storage Navigator/SVP]に制限するために[割付：DRU アクセス制御 SFP]を実施しなければならない。

依存性: [FDP_ACC.1 サブセットアクセス制御　または

FDP_IFC.1　サブセット情報フロー制御]

FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティの役割

FMT_MSA.2　セキュアなセキュリティ属性

下位階層: なし

FMT_MSA.2.1　TSF は、セキュアな値[詳細化：

・「書き込み拒否」アクセス属性の「書き込み許可」への変更はアクセス属性の有効期限の範囲外である場合のみ受け入れる。

・「書き込み許可」アクセス属性の「書き込み拒否」への変更はアクセス属性の有効期限に関係なく受け入れる。

・アクセス属性に対する有効期限を変更する際には、既に設定されている有効期限以上の期間のみを受け入れる。

上記規則を満足する値]だけがセキュリティ属性として受け入れられることを保証しなければならない。

依存性:　ADV_SPM.1 非形式的TOEセキュリティ方針モデル

[FDP_ACC.1 サブセットアクセス制御または

FDP_IFC.1 サブセット情報フロー制御]

FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティ役割」

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1　TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1　TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：アクセス属性管理機能、有効期限管理機能]。

依存性: なし

FPT_STM.1 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1　TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

FMT_SAE.1 時限付き許可

下位階層: なし

FMT_SAE.1.1　TSF は、[割付：アクセス属性]に対する有効期限の時間を特定する能力を、[割付：Storage Navigator/SVP]に制限しなければならない。

FMT_SAE.1.2　これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、[割付：アクセス属性の「書き込み拒否」から「書き込み許可」への変更が可能な状態への変更]を行えなければならない。

依存性: FMT_SMR.1 セキュリティ役割

FPT_STM.1 高信頼タイムスタンプ

FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1　TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2　TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性: なし

5.1.2. 最小機能強度レベル

この TOE の最小機能強度レベルは、SOF-基本である。ただし、本 TOE には確率的または順列的メカニズムを利用する機能要件はない。

5.1.3. TOE セキュリティ保証要件

TOE セキュリティ保証要件は、EAL2 に含まれる以下のものである。

表 5.1 TOE セキュリティ保証要件

セキュリティ保証要件	
ACM_CAP.2	構成要素
ADO_DEL.1	配付手続き
ADO_IGS.1	設置、生成、及び立上げ手順
ADV_FSP.1	非形式的機能仕様
ADV_HLD.1	記述的上位レベル設計
ADV_RCR.1	非形式的対応の実証
AGD_ADM.1	管理者ガイダンス
AGD_USR.1	利用者ガイダンス
ATE_COV.1	カバレージの証拠
ATE_FUN.1	機能テスト
ATE_IND.2	独立試験 – サンプル
AVA_SOF.1	TOE セキュリティ機能強度評価
AVA_VLA.1	開発者脆弱性分析

5.2. IT 環境に対するセキュリティ要件

TOE が IT 環境に依存するセキュリティ要件はない。

6. TOE 要約仕様

本章では、TOE セキュリティ要件を満たす TOE のセキュリティ機能および保証手段を記述する。

6.1. TOE セキュリティ機能

6.1.1 SF.DRU

【満たしている要件】FDP_ACC.1、FDP_ACF.1、FMT_MSA.3 、FMT_SMR.1 、FIA_UID.2 、FMT_MSA.1 、 FMT_MSA.2 、 FPT_RVM.1 、 FMT_SMF.1 、 FPT_STM.1 、 FMT_SAE.1 、 FPT_SEP.1

TOE は、LDEV のアクセス属性に基づき、ホスト要求を代行するプロセス、SVP 要求を代行するプロセス、および他ストレージ装置要求を代行するプロセスからの LDEV へのアクセスに対して、「DRU アクセス制御 SFP」を実施する。

「書き込み拒否」のアクセス属性には有効期限が設定される。アクセス属性および有効期限は、SM 上の制御情報として管理・格納される。

「DRU アクセス制御 SFP」は、以下の規則からなる。

- ホストから LDEV へのアクセスが行われる際、TOE は LDEV のアクセス属性をチェックし、許可されたアクセス（書き込み許可、書き込み拒否）が行われるようにアクセス制御を行う。
- SVP からのコピー機能実行指示に対して、副 VOL のアクセス属性が「書き込み拒否」の場合、コピー先 LDEV への書き込みは拒否される。
- 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）は、LDEV のアクセス属性によらず可能とする。（ただし TOE 外である Storage Navigator/SVP の機能により、アクセス属性が書き込み拒否の場合、これらの更新処理は行われない。）
- コピー機能実行に伴う他ストレージ装置からの LDEV に対する書き込みは、副 VOL のアクセス属性によらず可能とする。（ただし TOE 外である他ストレージ装置の機能により、副 VOL のアクセス属性が書き込み拒否の場合、この書き込み処理は行われない。）
- 「DRU アクセス制御 SFP」は、LDEV が生成された場合、アクセス属性として許可的デフォルト値を与える。これは、LDEV が作成された際のアクセス属性のデフォルト値として、「書き込み許可」属性が与えられているため、ホストから LDEV へのアクセスを制限しな

いことを意味する。なお、このデフォルト値の代替となる初期値を変更できる役割は存在しない。

- 「書き込み拒否」属性に設定されている有効期限の範囲内ならば、これらの属性から「書き込み許可」への変更は抑止される。
- アクセス属性の更新は、Storage Navigator/SVP のみから可能とする。

アクセス属性の変更可否を以下に示す。

表 6.1　アクセス属性の変更可否

変更後 / 変更前	有効期限の範囲内		有効期限の範囲外	
	書き込み許可	書き込み拒否	書き込み許可	書き込み拒否
書き込み許可	－(*1)	－(*1)	－	○
書き込み拒否	×	－	○	－

(*1) 「書き込み許可」属性には有効期限の設定無し　　×：変更不可、　○：変更可

TOE は、ホスト、Storage Navigator/SVP、他ストレージ装置の役割を維持し、これらの識別を他のセキュリティ機能の動作前に実施する。

TOEは、TOEの機能が実行される際に、かならず「DRUアクセス制御SFP」が適用されることを保証する。
また、SF.DRUに関するTSFは自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらない事を保証する。

さらに、TOE は、有効期限に関して下記の機能を有する。

- 有効期限経過後は、「書き込み拒否」属性から「書き込み許可」属性への変更が可能な状態となる。なお、有効期限経過後もアクセス属性は自動的に変更されることはない。「書き込み許可」属性への変更を行う場合は、ストレージ管理者（または保守員）操作により行う。
- 一度設定した「書き込み拒否」属性の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。

なお、SM 上の制御情報内に管理・格納されている有効期限に関しては、CHA/DKA 上のハードウェアが管理しているカウンタ値を元にして、TOE が経過時間を算出し、有効期限の情報を更新する。

6.2. セキュリティ機能強度

本 TOE には、順列的または確率的メカニズムによって実現される IT セキュリティ機能は存在しないため、セキュリティ機能強度レベルを主張しない。

6.3. 保証手段

以下に、セキュリティ保証要件を満たす文書の参照を示すことによって保証手段を定義する。

表 6.2 セキュリティ保証と保証手段

セキュリティ保証要件		保証手段
ACM_CAP.2	構成要素	・SANRISE USP マイクロプログラム構成管理リスト ・DKCMAIN/SVP バージョンの付与方法
ADO_DEL.1	配付手続き	・SANRISE USP 配付手順説明書
ADO_IGS.1	設置、生成、及び 立上げ手順	[SANRISE Universal Storage Platform / SANRISE H12000] ・A/H-65A3, A/H-65A7, A-65B3, A-65B7, HT-40B3, HT-40B7 ディスクサブシステム　メンテナンスマニュアル [SANRISE Network Storage Controller / SANRISE H10000] ・A/H-65A4, A-65B4, HT-40B4 ディスクサブシステム　メンテナンスマニュアル [TagmaStore Universal Storage Platform] ・DKC510I, DKU505I　Maintenance Manual [TagmaStore Network Storage Controller] ・DKC515I　Maintenance Manual
ADV_FSP.1	非形式的機能仕様	・SANRISE USP Data Retention Utility 機能仕様
ADV_HLD.1	記述的上位レベル設計	・SANRISE USP Data Retention Utility 機能仕様

セキュリティ保証要件	保証手段
ADV_RCR.1 非形式的対応の実証	・SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 ユーザデータ保護機能 表現対応分析書
AGD_ADM.1 管理者ガイダンス	・SANRISE Universal Storage Platform / SANRISE Network Storage Controller / SANRISE H12000 / SANRISE H10000 ISO15408 認証取得機能　取扱説明書 ・TagmaStore Universal Storage Platform / TagmaStore Network Storage Controller ISO15408 Certification Instructions Manual
AGD_USR.1 利用者ガイダンス	なし
ATE_COV.1 カバレージの証拠	・SANRISE USP テスト分析書
ATE_FUN.1 機能テスト	・SANRISE USP テスト仕様書
ATE_IND.2 独立試験 – サンプル	・SANRISE USP テスト仕様書 ・TOE
AVA_SOF.1 TOE セキュリティ機能強度評価	・SANRISE USP 機能強度分析書
AVA_VLA.1 開発者脆弱性分析	・SANRISE USP 脆弱性分析書

7. PP 主張

本 ST は、いかなる PP への適合も主張しない。

8. 根拠

本章は、主に ST を評価する際に用いられる証拠を提示する。

8.1. セキュリティ対策方針根拠

本章では、セキュリティ対策方針が TOE セキュリティ環境において識別されたすべての側面をカバーするのに適していることを説明する。

表 8.1 は、本 ST に記述されたセキュリティ対策方針が、前提条件、脅威、あるいは組織のセキュリティ方針にまでたどれることを示している。

表 8.1 TOE セキュリティ環境とセキュリティ対策方針との対応

		セキュリティ対策方針								
		O.Protect_LDEV	O.Protect_DRU	O.Retention_Period	OE.PhysicalProtection-Storage	OE.Protection-Network	OE.Protection-PC	OE.Responsibility-Admin	OE.Responsibility-Maintenance	OE.Connect-Storage
TOE セキュリティ環境	A.PhysicalProtection-Storage				X					
	A.Protection-Network					X				
	A.Protection-PC						X			
	A.Responsibility-Admin							X		
	A.Responsibility-Maintenance								X	
	A.Connect-Storage									X
	T.Delete/Change_User_Data	X								
	P.Protect_DRU		X							
	P.Retention_Period			X						

表 8.2 は、セキュリティ対策方針によって、脅威が対抗されていることを示している。

表 8.2　脅威に対するセキュリティ対策方針の正当性

脅威	脅威が対抗されていることの根拠
T.Delete/Change_User_Data	T.Delete/Change_User_Data は、下記に示す通り、 O.Protect_LDEV によって除去される。 ・ LDEV に対して、「書き込み許可」または「書き込み拒否」の各属性をストレージ管理者（または保守員）が設定し、その設定に基づいて TOE がアクセスを制御することにより、LDEV 内のデータに対する不適切な書き込みを抑止することができるからである。例えば、変更されては困るユーザデータに対しては、そのユーザデータが存在する LDEV に対して「書き込み拒否」の設定を行うことで、LDEV への書き込みが禁止され、ユーザデータを保護することができる。

表 8.3 は、セキュリティ対策方針によって前提条件がカバーされていることを示している。

表 8.3 前提条件に対するセキュリティ対策方針の正当性

前提条件	前提条件がカバーされていることの根拠
A.PhysicalProtection-Storage	A.PhysicalProtection-Storage は、 OE.PhysicalProtection-Storage にあるように、ストレージ装置を物理的に保護することによって実現される。
A.Protection-Network	A.Protection-Network は、 OE.Protection-Network にあるように、ストレージ装置を含むネットワークに不正な PC やホスト等の機器を接続させないことよって実現される。
A.Protection-PC	A.Protection-PC は、 OE.Protection-PC にあるように、管理 PC をストレージ管理者以外の人物が操作できないことによって実現される。
A.Responsibility-Admin	A.Responsibility-Admin は、 OE.Responsibility-Admin にあるように、ストレージ管理者に信頼できる人物を割り当てることによって実現される。
A.Responsibility-Maintenance	A.Responsibility- Maintenance は、 OE.Responsibility- Maintenance にあるように、保守員に信頼できる人物を割り当てることによって実現される。
A.Connect-Storage	A.Connect-Storage は、 OE.Connect-Storage にあるように、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、日立製作所製のストレージ装置が接続されることによって実現される。

表 8.4 は、セキュリティ対策方針によって組織のセキュリティ方針がカバーされていることを示している。

表 8.4 組織のセキュリティ方針に対するセキュリティ対策方針の正当性

組織のセキュリティ方針	組織のセキュリティ方針がカバーされていることの根拠
P.Protect_DRU	P.Protect_DRU は、O.Protect_DRU にあるように、TOE がアクセス属性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」への属性の変更を抑止する機能を提供することにより実現される。
P.Retention_Period	P.Retention_Period は、O.Retention_Period にあるように、TOE が「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抑止する機能を提供することにより実現される。

8.2. セキュリティ要件根拠

本章では、セキュリティ要件のセットがセキュリティ対策方針を満たすのに適していることを説明する。

8.2.1. セキュリティ機能要件根拠

表 8.5 は、本 ST に記述されたセキュリティ機能要件が対策方針にまでたどれることを示している。

表 8.5　セキュリティ対策方針とセキュリティ機能要件との対応

		TOE セキュリティ機能要件											
		FDP_ACC.1	FDP_ACF.1	FMT_MSA.3	FMT_SMR.1	FIA_UID.2	FMT_MSA.1	FMT_MSA.2	FPT_RVM.1	FMT_SMF.1	FPT_STM.1	FMT_SAE.1	FPT_SEP.1
セキュリティ対策方針	O.Protect_LDEV	X	X	X		X			X				X
	O.Protect_DRU				X	X	X	X		X	X	X	
	O.Retention_Period				X	X		X		X	X	X	

表 8.6 は、TOE のセキュリティ機能要件によって、TOE のセキュリティ対策方針が実現されていることを示している。

表 8.6　TOE のセキュリティ対策方針に対するセキュリティ機能要件の正当性

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
O.Protect_LDEV	O.Protect_LDEV では、本 TOE が保護対象資産である LDEV を守るために、TOE が LDEV に設定されているアクセス属性に基づいて、LDEV に対する書き込み可否の制御を行うことを要求している。 この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。 a.TOE 利用前に利用者を識別する。 TOE が利用される前に、ホストからの要求か、SVP からの要求か、他ストレージ装置からの要求かのいずれであるかを TOE が識別しなければならない。よって、他のセキュリティ機能の動作前に利用者の識別を実施する必要があり、この要件に該当するセキュリティ機能要件は FIA_UID.2 である。 b.アクセス制御を規定し、実施する。 TOE は各利用者に対して LDEV のアクセス属性に基づいて、「DRU アクセス制御 SFP」として定義された規則に従って LDEV への書き込みの可否を決定し、その通りにアクセス制御を行う必要がある。これによりホストまたは他ストレージ装置から LDEV への書き込み可否を制御できる。この要件に該当するセキュリティ機能要件は FDP_ACC.1 および FDP_ACF.1 である。 c.意図したアクセス制御が行われるために、アクセス属性の初期値を規定する。 アクセス制御で用いられるセキュリティ属性であるアクセス属性として、デフォルトではホストまたは他ストレージ装置からの LDEV に対する書き込み許可が設定されている。このデフォルト値の代替となる初期値を変更する役割は存在しないことが「DRU アクセス制御 SFP」に規定されており、これを実現する必要がある。この要件に該当するセキュリティ機能要件は FMT_MSA.3 である。

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	d.アクセス制御を確実に実施する。 アクセス制御が確実に行われるためには、アクセス制御に関する TSF はサブジェクトがオブジェクトを操作する前には必ず呼び出されなければならない。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b、c、d すべての対策を満たすことにより、O.Protect_LDEV を満足できる。よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_UID.2、FDP_ACC.1、FDP_ACF.1、FMT_MSA.3、FPT_RVM.1、FPT_SEP.1 の達成により、O.Protect_LDEV を実現できる。
O.Protect_DRU	O.Protect_DRU では、不当にアクセス属性が変更され、ユーザデータに対する改変がなされることを防ぐために、TOE が「書き込み拒否」のアクセス属性に対して有効期限を設定することと、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」への属性の変更を抑止することを要求している。この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。 a.TOE 利用前に利用者を識別する。 TOE が利用される前に、ホストからの要求か、SVP からの要求か、他ストレージ装置からの要求かのいずれであるかを TOE が識別しなければならない。よって、他のセキュリティ機能の動作前に利用者の識別を実施する必要があり、この要件に該当するセキュリティ機能要件は FIA_UID.2 である。 b.有効期限の範囲内では「書き込み拒否」属性から「書き込み許可」属性への変更を抑止する。 TOE は各利用者に対して、「書き込み拒否」属性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」への変更を抑止しなければならない。よって、TOE は、「DRU アクセス制御 SFP」として定義された規則に従ってアクセス属性に対する変更を制御する必要がある。この要件に該当するセキュリティ機能要件は、FMT_SMF.1、FMT_MSA.1 および FMT_MSA.2 である。 また、TOE は有効期限が経過した場合、「書き込み拒否」から「書き込み許可」へのアクセス属性の変更を可能としなければならない。この要件に該当するセキュリ

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	ティ機能要件は、FMT_SAE.1 である。 また、アクセス属性の管理ができる役割を特定するために、ホスト、Storage Navigator/SVP、他ストレージ装置という役割を維持し、利用者と関連付ける必要があり、この要件に該当するセキュリティ機能要件は FMT_SMR.1 である。 更に、TOE が有効期限の管理を実施するためにタイムスタンプが提供される必要がある。この要件に該当するセキュリティ機能要件は FPT_STM.1 である。 以上 a、b すべての対策を満たすことにより、O.Protect_DRU を満足できる。 よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_UID.2 、FMT_SMF.1、FMT_MSA.1、FMT_MSA.2、FMT_SAE.1、FMT_SMR.1 、FPT_STM.1 の達成により、O.Protect_DRU を実現できる。
O.Retention_Period	O.Retention_Period では、有効期限内のアクセス属性が不当に変更されることを防ぐために、TOE が「書き込み拒否」のアクセス属性に対して設定されている有効期限の短縮を抑止することを要求している。この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。 a.TOE 利用前に利用者を識別する。 TOE が利用される前に、ホストからの要求か、SVP からの要求か、他ストレージ装置からの要求かのいずれであるかを TOE が識別しなければならない。よって、他のセキュリティ機能の動作前に利用者の識別を実施する必要があり、この要件に該当するセキュリティ機能要件は FIA_UID.2 である。 b.有効期限の管理を行う。 TOE は、有効期限管理機能（Storage Navigator/SVP から設定されたアクセス属性の有効期限を SM 上の制御情報に反映する機能）を持つ必要がある。この要件に該当するセキュリティ機能要件は FMT_SMF.1 である。 また、有効期限の管理ができる役割を特定するために、ホスト、Storage Navigator /SVP、他ストレージ装置という役割を維持し、利用者と関連付ける必要があり、この要件に該当するセキュリティ機能要件は FMT_SMR.1 である。

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	c.有効期限の管理に当たり、有効期限の短縮を抑止する。 TOE は有効期限を管理するに当たり、「書き込み拒否」属性に対して設定された有効期限の短縮を抑止し、期限の延長のみを許可しなければならない。この要件に該当するセキュリティ機能要件は FMT_SAE.1 および FMT_MSA.2 である。 また、TOE が有効期限の管理を実施するためにタイムスタンプが提供される必要がある。この要件に該当するセキュリティ機能要件は FPT_STM.1 である。 以上 a、b、c すべての対策を満たすことにより、O.Retention_Period を満足できる。よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_UID.2 、FMT_SMF.1、FMT_SMR.1、FMT_SAE.1、FMT_MSA.2、FPT_STM.1 の達成により、O.Retention_Period を実現できる。

8.2.2. セキュリティ要件内部一貫性根拠

下表に、セキュリティ機能要件の依存性について示す。

表 8.7 セキュリティ機能要件の依存性

項番	TOE/IT 環境	セキュリティ機能要件	CC part2 に定義されている依存性	本 ST で対応する機能要件の項番
1	TOE	FDP_ACC.1	FDP_ACF.1	2
2	TOE	FDP_ACF.1	FDP_ACC.1	1
			FMT_MSA.3	3
3	TOE	FMT_MSA.3	FMT_MSA.1	6
			FMT_SMR.1	4
4	TOE	FMT_SMR.1	FIA_UID.1	5 *1
5	TOE	FIA_UID.2	なし	－
6	TOE	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	1
			FMT_SMF.1	9
			FMT_SMR.1	4
7	TOE	FMT_MSA.2	ADV_SPM.1	依存性を充足せず
			FDP_ACC.1 or FDP_IFC.1	1
			FMT_MSA.1	6
			FMT_SMR.1	4
8	TOE	FPT_RVM.1	なし	－
9	TOE	FMT_SMF.1	なし	－
10	TOE	FPT_STM.1	なし	－
11	TOE	FMT_SAE.1	FMT_SMR.1	4
			FPT_STM.1	10
12	TOE	FPT_SEP.1	なし	－

*1:FIA_UID.1 の上位階層コンポーネントである FIA_UID.2 により依存関係を充足している。

本STにおいて、ITセキュリティ機能要件および保証要件間の依存性はFMT_MSA.2が依存するADV_SPM.1を除いて満たされている。ただし、FMT_MSA.2に対して詳細化を行なっており、その従うべき規則は明示されているのでADV_SPM.1に対する依存性は除去できる。
また、ITセキュリティ要件同士の競合も存在しない。各TOEセキュリティ機能要件について、同カテゴリの機能要件についてその定義が一貫性を持つことの根拠を表8.8に示す。

表 8.8 セキュリティ機能要件間の一貫性

項番	カテゴリ	セキュリティ機能要件	一貫性の根拠
1	アクセス制御	FDP_ACC.1 FDP_ACF.1	これらの機能要件によりアクセス制御について定義しているが、同一のサブジェクト、オブジェクトに対して同一の SFP の適用を要求しており競合や矛盾は存在せず、その内容は一貫している。
2	管理	FMT_MSA.1 FMT_MSA.2 FMT_MSA.3 FMT_SAE.1 FMT_SMF.1 FMT_SMR.1	これらの機能要件によりセキュリティ管理について定義しているが、対象とするセキュリティ属性やアクションにおいて競合や矛盾は存在せず、その内容は一貫している。
3	識別と認証	FIA_UID.2	この機能要件により識別を実現しているが、このカテゴリ内では 1 つの機能要件しか無いので内容が一貫しているのは自明である。
4	補完	FPT_RVM.1 FPT_SEP.1 FPT_STM.1	これらの機能要件は他の機能要件を補完するものである。FPT_RVM.1 はバイパス防止、FPT_SEP.1 はセキュリティドメイン分離の要件であることから他の要件と競合や矛盾が無いのは自明である。このカテゴリの機能要件間では競合や矛盾は存在せず、その内容は一貫している。
5	カテゴリ間	＃1－＃2	アクセス制御の要件は保護対象資産である LDEV に対する制御を定義しており、管理の要件は TSF データの管理を定義するものであることから両者に競合や矛盾は存在しない。
		＃1－＃3 ＃2－＃3	識別の要件とアクセス制御もしくは管理の要件との間では競合や矛盾は存在しない。
		＃1－＃4 ＃2－＃4 ＃3－＃4	前述の通り FPT_RVM.1 および FPT_SEP.1 が他の要件との間で競合や矛盾が生じないのは自明である。 また、FPT_STM.1 は SMT_SAE.1 に対して時間情報を提供するものであり、その他の要件との間で競合や矛盾は存在しない。

さらに、以下に述べるように依存関係のないセキュリティ機能要件によっても相互支援がなされている。

- FPT_RVM.1 は、他のセキュリティ機能要件が呼び出され成功することを保証し、バイパスを防ぐ。
- 本 TOE では、セキュリティ機能は常時起動しており、セキュリティ機能のみを停止して TOE を動作させることは出来ない。よって、非活性化防止については考慮する必要がない。
- FPT_SEP.1 は、セキュリティドメインへの干渉および改ざんを防ぐ。

- 本 TOE では、確率的・順列的メカニズムによって実現されるセキュリティ機能が存在せず、無効化攻撃については考慮する必要がないため、FAU クラスの機能要件は必要としない。

上述のとおり、ST に記述された IT セキュリティ要件は一体となって相互にサポートし、内部的に一貫性がある全体を形成している。

8.2.3. 最小機能強度レベル根拠

3.2 章において、脅威エージェントのもつ攻撃能力は「低」と想定している。

したがって、TOEは低レベルの脅威エージェントに対抗できる必要があり、最小機能強度レベルはSOF-基本が妥当である。また、5.1.2.節においてTOEに対し最小機能強度レベルとしてSOF-基本を求めており、攻撃能力と最小機能強度レベルは一貫している。

8.2.4. 評価保証レベル根拠

本TOEを含むストレージ装置は、入退室が管理されているセキュアなエリアに設置されており、TOEへの攻撃経路としてはホスト経由に限定される。このため、明白な脆弱性に対する評価を実施すれば十分である。

また、TOEはソフトウェアであり、かつ暗号鍵などの秘匿すべき情報を含まないので、開発セキュリティでの保護は不要である。

したがって、評価保証レベルとしてEAL2が妥当である。

8.3. TOE 要約仕様根拠

本章では、TOE のセキュリティ機能および保証手段が TOE セキュリティ要件を満たすのに適していることを説明する。

8.3.1. TOE セキュリティ機能根拠

表 8.9 は、本 ST に記述された IT セキュリティ機能が、TOE セキュリティ機能要件にまでたどれることを示している。

表 8.9 TOE セキュリティ機能要件と TOE の IT セキュリティ機能との対応

		TOE の IT セキュリティ機能
		SF.DRU
TOE セキュリティ機能要件	FDP_ACC.1	X
	FDP_ACF.1	X
	FMT_MSA.3	X
	FMT_SMR.1	X
	FIA_UID.2	X
	FMT_MSA.1	X
	FMT_MSA.2	X
	FPT_RVM.1	X
	FMT_SMF.1	X
	FPT_STM.1	X
	FMT_SAE.1	X
	FPT_SEP.1	X

表 8.10 は、IT セキュリティ機能が TOE セキュリティ機能要件を満たし、相互に補完し一体となって機能していることを示している。

表 8.10　TOE セキュリティ機能要件に対する IT セキュリティ機能の正当性

TOE セキュリティ機能要件	IT セキュリティ機能
FDP_ACC.1	FDP_ACC.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『TOE は、LDEV のアクセス属性に基づき、ホスト要求を代行するプロセス、SVP 要求を代行するプロセス、および他ストレージ装置要求を代行するプロセスからの LDEV へのアクセスに対して、「DRU アクセス制御 SFP」を実施する。』
FDP_ACF.1	FDP_ACF.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『・ホストから LDEV へのアクセスが行われる際、TOE は LDEV のアクセス属性をチェックし、許可されたアクセス（書き込み許可、書き込み拒否）が行われるようにアクセス制御を行う。 ・SVP からのコピー機能実行指示に対して、副 VOL のアクセス属性が「書き込み拒否」の場合、コピー先 LDEV への書き込みは拒否される。 ・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）は、LDEV のアクセス属性によらず可能とする。（ただし TOE 外である Storage Navigator/SVP の機能により、アクセス属性が書き込み拒否の場合、これらの更新処理は行われない。） ・コピー機能実行に伴う他ストレージ装置からの LDEV に対する書き込みは、副 VOL のアクセス属性によらず可能とする。（ただし TOE 外である他ストレージ装置の機能により、副 VOL のアクセス属性が書き込み拒否の場合、この書き込み処理は行われない。） 』
FMT_MSA.3	FMT_MSA.3 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『「DRU アクセス制御 SFP は」は、LDEV が生成された場合、アクセス属性として許可的デフォルト値を与える。…. なお、このデフォルト値の代替となる初期値を変更できる役割は存在しない。』

TOE セキュリティ機能要件	IT セキュリティ機能
FMT_SMR.1	FMT_SMR.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『TOE は、ホスト、Storage Navigator/SVP、他ストレージ装置の役割を維持し、…』
FIA_UID.2	FIA_UID.2 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『TOE は、ホスト、Storage Navigator/SVP、他ストレージ装置の役割を維持し、これらの識別を他のセキュリティ機能の動作前に実施する。』
FMT_MSA.1	FMT_MSA.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『「DRU アクセス制御 SFP」は、以下の規則からなる。 ・アクセス属性の更新は、Storage Navigator/SVP のみから可能とする。』
FMT_MSA.2	FMT_MSA.2 は、SF.DRU に関して以下のように記述されており、これらの内容によって実現されている。 『「DRU アクセス制御 SFP」は、以下の規則からなる。 ・「書き込み拒否」属性に設定されている有効期限の範囲内ならば、これらの属性から「書き込み許可」への変更は抑止される。』 『また TOE は、有効期限に関して下記の機能を有する。 ・有効期限経過後は、「書き込み拒否」属性から「書き込み許可」属性への変更が可能な状態となる。なお、有効期限経過後もアクセス属性は自動的に変更されることはない。 ・一度設定した「書き込み拒否」属性の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。』

TOE セキュリティ機能要件	IT セキュリティ機能
FPT_RVM.1	FPT_RVM.1 は、SF.DRU に関して以下のように記述されている。 『TOE は、ホスト、Storage Navigator/SVP、他ストレージ装置の役割を維持し、これらの識別を他のセキュリティ機能の動作前に実施する。』とあり、各機能の動作が許可される前に識別機能が呼び出され、成功することを保証する。また、 『TOE は、TOE の機能が実行される際に、かならず「DRU アクセス制御 SFP」が適用されることを保証する。』とあり、TSP 実施機能が呼び出され成功することを保証する。これらの内容により FPT_RVM.1 は実現されている。
FMT_SMF.1	FMT_SMF.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『 「書き込み拒否」のアクセス属性には有効期限が設定される。アクセス属性および有効期限は、SM 上の制御情報として管理・格納される。』
FPT_STM.1	FPT_STM.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『なお、SM 上の制御情報内に管理・格納されている有効期限に関しては、CHA/DKA 上のハードウェアが管理しているカウンタ値を元にして、TOE が経過時間を算出し、有効期限の情報を更新する。』
FMT_SAE.1	FMT_SAE.1 は、SF.DRU に関して以下のように記述されており、この内容によって実現されている。 『また TOE は、有効期限に関して下記の機能を有する。 ・有効期限経過後は、「書き込み拒否」属性から「書き込み許可」属性への変更が可能な状態となる。なお、有効期限経過後もアクセス属性は自動的に変更されることはない。 ・ 一度設定した「書き込み拒否」属性の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。』

TOE セキュリティ機能要件	IT セキュリティ機能
FPT_SEP.1	FPT_SEP.1 は、SF.DRU に関して以下のように記述されている。 『また、SF.DRU に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらない事を保証する。』 この内容により、SF.DRUにおいて、その機能に用いられるTSFと情報が干渉・改ざんから保護されており、これらを維持することでその他のサブジェクトからの干渉・改ざんから保護する。 また、SF.DRUは自身の必要なサブジェクトをセキュリティドメインに格納し、それ以外のサブジェクトとは分離する。 したがって、SF.DRU の実装により FPT_SEP.1 は実現されている。

8.3.2. TOE 機能強度根拠

本 ST では、確率的または順列的メカニズムに基づく IT セキュリティ機能は含まれていないため、本根拠に関しては対象外である。

8.3.3. 保証手段根拠

表 6.2 に示した保証手段は、対応したセキュリティ保証要件を満たしていることが読み取れる名称の文書名となっており、セキュリティ保証要件と保証手段の対応が取れている。なお、保証手段に関する特記事項を以下に示す。

- ADO_IGS.1 に関しては、４種類のマニュアルを記載しているが、これはそれぞれの装置の種類に対応したマニュアルである。
- ADV_HLD.1 に関しては、「SANRISE USP Data Retention Utility 機能仕様」に上位レベル設計の内容を記載している。
- AGD_ADM.1 に関しては、２種類のマニュアルを記載しているが、これらは日本語版と英語版の違いだけであり、内容については同一である。
- AGD_USR.1 に関しては、対応する保証手段が存在しない。これは、ストレージ装置の利用者は、ストレージ装置の管理者が構築した環境に基づいて、ホストからストレージ装置内のユーザボリュームを使用するため、ホストに関する一般的な知識があればユーザボリュームを利用でき、ストレージ装置に関する特別な知識は必要無いためである。

上記の通り、本 ST に記述された各保証手段が、TOE セキュリティ保証要件にまでたどれることを示し、また記述されたすべての保証手段が実装されることによってすべての TOE セキュリティ保証要件が満たされることも示している。

8.4. PP 主張根拠

本 ST は、いかなる PP への適合も主張しない。

9. 参考文献

[1] Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model
Version 2.1, August 1999, CCIMB-99-031

[2] Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements
Version 2.1, August 1999, CCIMB-99-032

[3] Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements
Version 2.1, August 1999, CCIMB-99-033

[4] 情報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
平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会セキュリティセンター

[5] 情報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
平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会セキュリティセンター

[6] 情報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
平成 13 年 1 月翻訳第 1.2 版, 情報処理振興事業協会セキュリティセンター

[7] CCIMB Interpretations-0407 (as of 01 December 2003)

[8] 補足-0210 第 2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

[9] 補足-0407
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室