HiCommand Suite Common Component

セキュリティターゲット

2007/5/10

Version 1.08

株式会社 日立製作所

「HiCommand Suite Common Component セキュリティターゲット」

－ 変更歴 －

項番	作成／変更年月日	ST バージョン	変更理由	作成	承認
1	2006/10/16	Ver 1.00	新規作成	藤井、平岩	伊藤
2	2006/12/15	Ver 1.01	EVE-EOR-0001-00，EVE-EOR-1101-00 の指摘事項反映	藤井	伊藤
3	2007/2/9	Ver 1.02	評価者の指摘事項反映	藤井、平岩	伊藤
4	2007/2/19	Ver 1.03	EVE-EOR-0002-00 ～ EVE-EOR-0007-00 の指摘事項反映	藤井	伊藤
5	2007/2/23	Ver 1.04	評価者の指摘事項反映	藤井	伊藤
6	2007/3/8	Ver 1.05	評価者の指摘事項反映	藤井	伊藤
7	2007/3/27	Ver 1.06	評価者の指摘事項反映	藤井	伊藤
8	2007/4/23	Ver 1.07	評価者の指摘事項反映	藤井	伊藤
9	2007/5/10	Ver 1.08	評価者の指摘事項反映	藤井	伊藤

■ 商標類

■ 著作権

「HiCommand Suite Common Component セキュリティターゲット」

－ 目次 －

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、用語の定義について記述する。

1.1. ST 識別

1.1.1. ST 識別情報

本 ST(セキュリティターゲット)の識別情報を以下に示す。

名称: HiCommand Suite Common Component セキュリティターゲット

バージョン: 1.08

識別名: HSCC-ST-1.08

作成日: 2007 年 5 月 10 日

作成者: 株式会社 日立製作所

1.1.2. TOE 識別情報

本 ST で評価する TOE(評価対象)を含む製品の名称を以下に示す。

名称: HiCommand Suite Common Component

TOE のバージョン: 05-51-01

作成者: 株式会社 日立製作所

適用プラットフォーム:

- 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。

キーワード: ストレージ管理ソフトウェア

1.1.3. 適用 CC

本 ST は以下の CC を適用する。

CC バージョン 2.3, 補足-0512

1.2. ST 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（以降、HDvM と略記）、HiCommand Replication Monitor（以降、HRpM と略記）、HiCommand Tiered Storage Manager（以降、HTSM と略記）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
- セキュリティ情報管理機能
- 警告バナー機能

1.3. CC 適合

本 ST は以下の通り CC 適合を主張する。

- CC バージョン 2.3 パート 2 適合
- CC バージョン 2.3 パート 3 適合

評価保証レベルは EAL2 適合、ALC_FLR.1 を追加する。

本 ST は PP（プロテクションプロファイル）を適用しない。

1.4. 用語の定義

本STで用いる用語・略語の意味(要約)を表 1に示す。

表 1 用語・略語の意味

用語	意味
ACL	Access Control List の略。
SAN	Storage Area Network の略。
トークン	HSCC がセッション管理に用いる識別子。
HSCC	HiCommand Suite Common Component。 HiCommand Suite の1つであり、HiCommand Suite に含まれ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。
HDvM	HiCommand Device Manager。 HiCommand Suite の1つであるストレージ管理ソフトウェア。ストレージのボリューム管理機能を提供する。
HRpM	HiCommand Replication Monitor。 HiCommand Suite の1つであるストレージ管理ソフトウェア。ストレージのボリューム間で行われるコピーの監視機能を提供する。
HTSM	HiCommand Tiered Storage Manager。 HiCommand Suite の1つであるストレージ管理ソフトウェア。ストレージのボリューム間でのデータ移動を制御する。
セキュリティパラメータ	HSCC のセキュリティ機能に関連するパラメタ情報。
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。

2. TOE 記述

2.1. TOE の種別

本 TOE は、HiCommand Suite に含まれるストレージ管理ソフトウェアに対し、共通機能を実現する基盤モジュールを提供するソフトウェア製品である。

2.2. TOE を利用したシステムと TOE の概要

2.2.1. TOE を利用したシステム概要

ストレージシステム(以降、ストレージと略記)は、筐体の中に複数のボリュームを有し、業務アプリケーションを実行するアプリケーションサーバに接続され、業務アプリケーション実行に必要な情報を保持している。情報システムの規模に応じて、ストレージの規模も増加する傾向にある。情報システムを運用するためには、ストレージを管理する必要がある。すなわち、以下のような作業を適切に実施する必要がある。

・ボリューム割り当て(HDvM を使用してアプリケーションサーバからアクセス可能にする設定を行う等)

・コピー監視(HRpM を使用して業務データを格納したボリュームのコピーを監視する等)

・データ移動(HTSM を使用して古くなったデータを別ストレージへ移動し、空きボリュームを確保する)

上記のような作業の操作を、多数のボリュームや多数のストレージに対して行うために、ストレージ管理者が、対象となる多数のストレージと接続した管理用の機器より、いずれかの機能を有するストレージ管理ソフトウェアを実行して一元的に実施する。HiCommand Suiteは、上述のストレージ管理を行うソフトウェア群を提供する。HiCommand Suiteを利用してストレージ管理を行っているシステムの概要を図 1に示す。

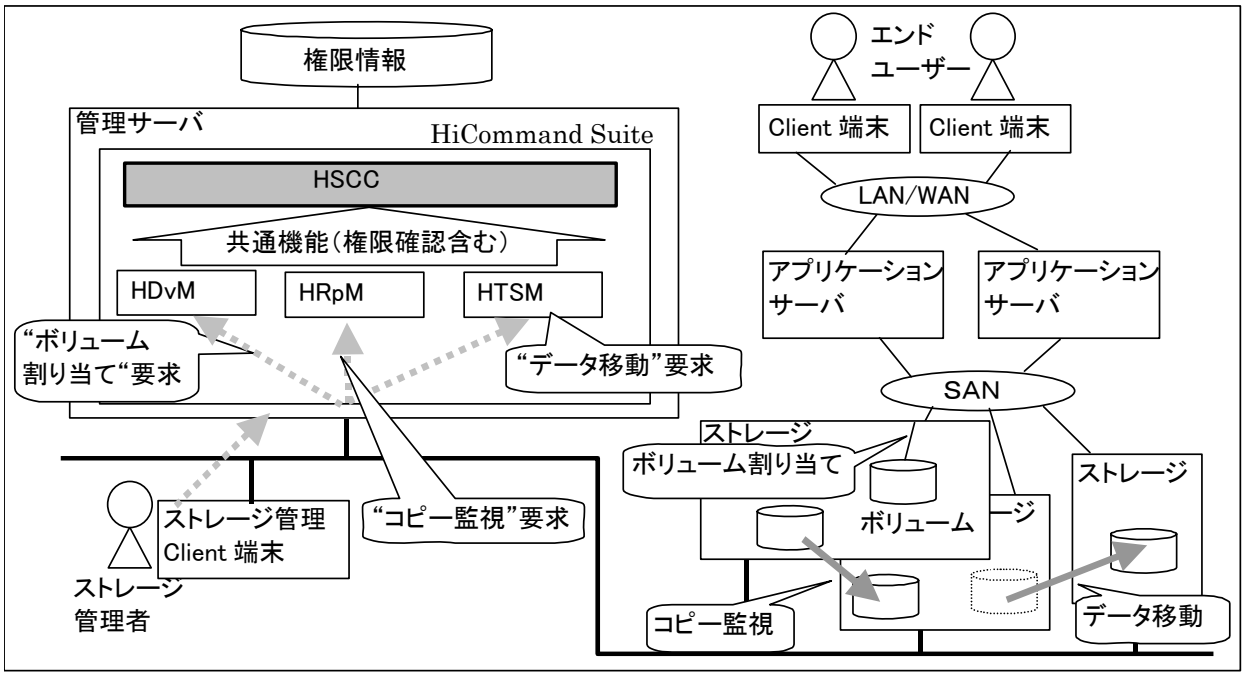

図 1 概要図

図 1においてストレージ管理者は、クライアント端末より、コピー等の必要な操作を行うためのストレージ管理ソフトウェアにアクセスし、必要な操作を要求する。TOEは、これらのストレージ管理ソフトウェア群に対する、認証や、権限情報の提示、ストレージ管理Client端末に表示を行うためのGUIといった共通の機能を提供する。

ストレージ管理者からのボリューム割り当てやコピー監視といったストレージ管理要求が正しい権限の範囲で行われるようにするため、TOE はこれらのストレージ管理要求に先立って認証を行い、権限情報へのアクセス制御を行う。

また、TOE は、認証のためのアカウント情報や、上記権限情報を設定するための、アカウント管理者用の機能を有する。

2.3. TOE の利用形態

2.3.1. モデル図

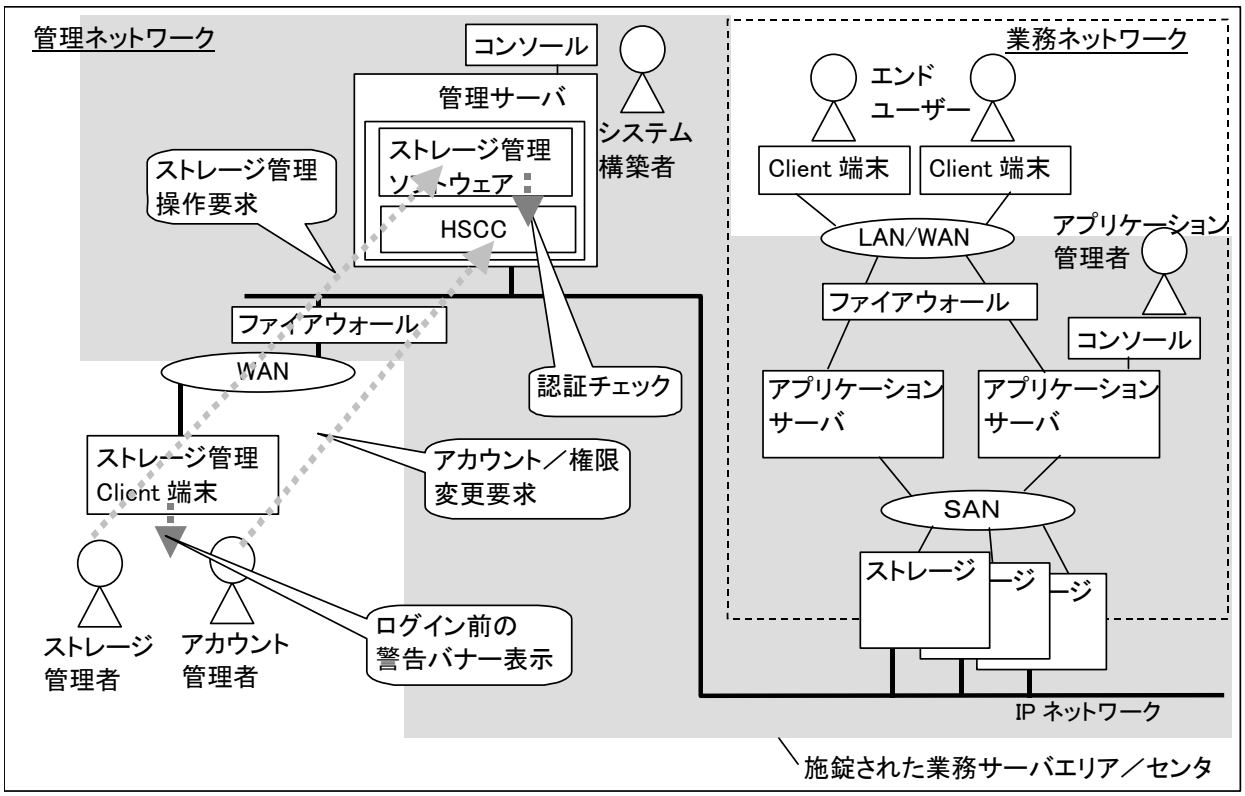

図 2 モデル図

図 2では、物理的な配線や装置等を実線で、動作や範囲を点線で示している。また、センタなどの施錠された業務サーバエリアを網かけにて示している。

業務サーバエリアには、管理サーバやアプリケーションサーバ、ストレージ、周辺機器等が設置され、入退場が制限されている。

管理ネットワークには管理サーバやストレージ、周辺機器等が接続され、業務ネットワークにはアプリケーションサーバやストレージ、周辺機器等が接続されている。各ネットワークは、いずれも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の管理ネットワークと業務ネットワークを合わせて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。

また両方のネットワークに属するストレージには、二つの独立した NIC が搭載されており、一方が管理ネットワーク、もう一方が業務ネットワークに接続されている。従って、管理ネットワークと業務ネットワークは分離され、相互に干渉しないものとする。

ストレージ管理者及びアカウント管理者、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。

2.3.2. TOE の利用者

本STでは、以下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。

(1)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。

(2)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。

(3)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。

2.3.3. ハードウェア構成

以下に TOE が稼動するためのハードウェア条件を示す。第 1.1 節に示した適用プラットフォームに対応して、以下では複数のハードウェア条件を示している。

(1) Windows の場合

下記シリーズ中で第 1.1 節に示した適用プラットフォーム(Windows)が稼動する機種

・日立 FLORA シリーズ

・日立 HA8000 シリーズ

・他社 PC/AT 互換機

・日立 BladeSymphony シリーズ

また、以下を最小条件とする。

CPU クロック:1GHz

メモリ容量:512MB
ディスク容量:4GB

(2) Linux の場合
下記シリーズ中で第 1.1 節に示した適用プラットフォーム(Linux)が稼動する機種
・日立 FLORA シリーズ
・日立 HA8000 シリーズ
・他社 PC/AT 互換機
・日立 BladeSymphony シリーズ

また、以下を最小条件とする。
CPU クロック:1GHz
メモリ容量:1GB
ディスク容量:4GB

(3) Solaris の場合
下記シリーズ中で第 1.1 節に示した適用プラットフォーム(Solaris)が稼動する機種
・Solaris SPARC

また、以下を最小条件とする。
CPU クロック:1GHz
メモリ容量:1GB
ディスク容量:4GB

2.3.4. ソフトウェア構成
以下に TOE が稼動するためのソフトウェア条件を示す。

(4) Windows の場合
・第 1.1 節に示した適用プラットフォーム
・Microsoft Internet Explorer ブラウザ

(5) Linux の場合
・第 1.1 節に示した適用プラットフォーム
・Mozilla ブラウザ

(6) Solaris の場合

・第 1.1 節に示した適用プラットフォーム
・Mozilla ブラウザ

2.4. TOE の範囲

2.4.1. TOE の物理的範囲

TOE の物理的範囲は、以下のライブラリ及びプログラムから構成される。

TOEを含めたソフトウェア構成図を図 3に示す。TOEはHSCCであり、TOEのセキュリティ機能を実現しているモジュールは、網かけにて示した部分である。

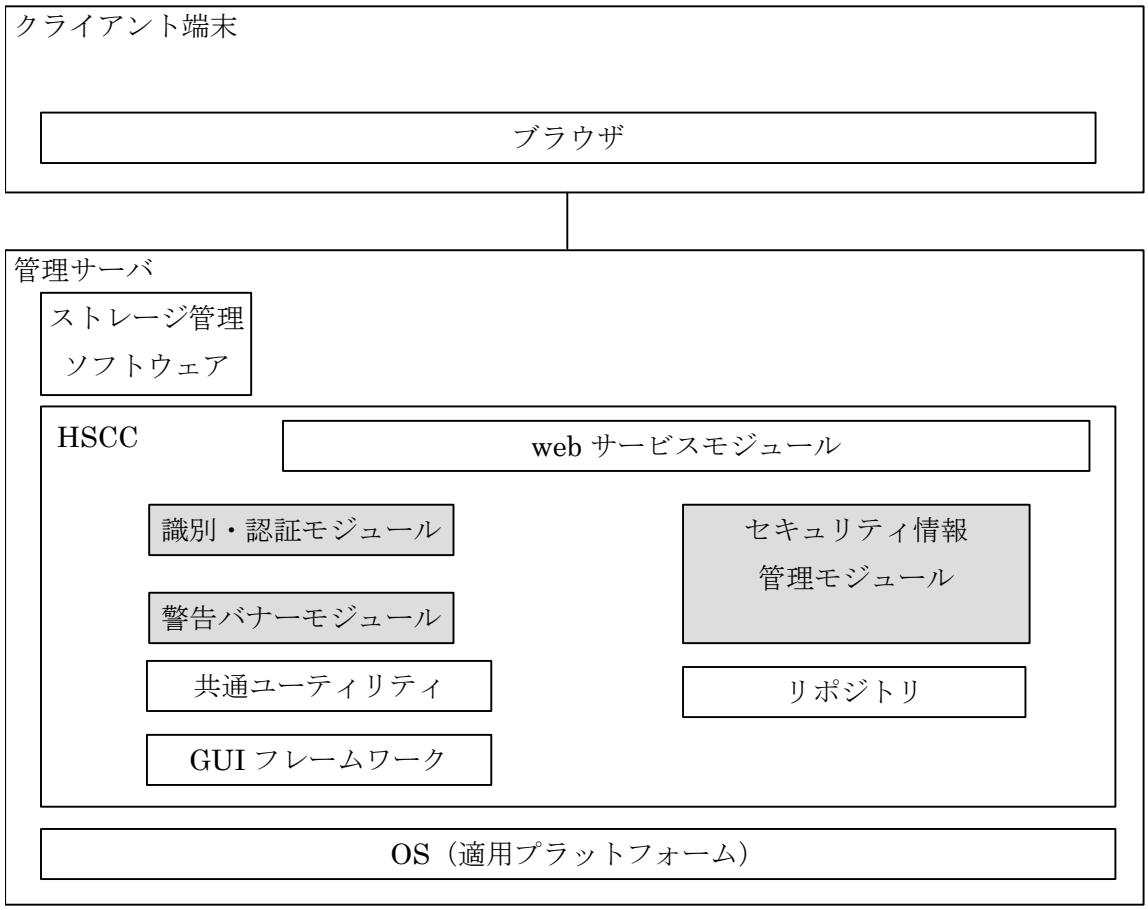

図 3 TOE を含めたソフトウェア構成図

識別・認証モジュールは、TOE の識別・認証機能を実現しているモジュールである。

セキュリティ情報管理モジュールは、TOE のセキュリティ情報管理機能を実現しているモジュールである。

警告バナーモジュールは、TOE の警告バナー機能を実現しているモジュールである。

共通ユーティリティは、TOE の共通ユーティリティを実現しているモジュールである。

web サービスモジュールは、TOE の web サービスを実現しているモジュールである。

GUI フレームワークは、TOE の GUI フレームワークを実現しているモジュールである。

リポジトリは、TOE が有するデータを保持している DB である。

2.4.2. TOE の論理的範囲

TOEの機能を表 2に示す。TOEのセキュリティ機能は、以下の機能のうち、網かけにて示した部分である。

表 2 TOE(HSCC)の機能一覧

機能	概要
識別・認証機能	ユーザーID及び対応するパスワードを用いた認証を行い、その結果に基づきセッションを維持する機能。また、認証に基づいて権限情報を要求元に渡す機能。
セキュリティ情報管理機能	アカウント情報・権限情報・バナー情報(作成・参照・改変・削除)を管理する。また、セキュリティパラメータを設定する機能。
警告バナー機能	HiCommand Suite に向けた警告用メッセージのデータを提供する機能。
共通ユーティリティ	HiCommand Suite のセットアップや運用のためのユーティリティ。
web サービス	HiCommand Suite がクライアント端末のブラウザとインタフェースを持つための web サービスを提供する機能。
GUIフレームワーク	HiCommand Suite に提供するGUIフレームワーク。
リポジトリ	HiCommand Suite の動作に利用するデータを格納する記憶領域。

(1)識別・認証機能

TOE の利用者がストレージ管理ソフトウェアにログインする際に識別・認証を行い、権限情報を応答する。権限情報とは、複数あるストレージ管理ソフトウェアに対し、いずれの権限を有するかを示す情報である。権限の例として、ストレージ管理ソフトウェアが管理するリソースに対する設定・変更を行う機能の実行を許可する「Modify」や、当該リソースに対して参照を行う機能のみの実行を許可する「View」などがある。

また、識別・認証において、一定回数連続して認証に失敗した場合、TOE の利用者のアカウントを自動的にロックする。

(2)セキュリティ情報管理機能

TOE の利用者のユーザーID、パスワード、ロックステータスをアカウント情報として管理する。パスワード設定時、セキュリティパラメータに設定されたパスワードの条件を満たしているかチェックする。また、ユーザーID に対応する権限情報が入力された場合、それを ACL 内に保持する。

アカウント自動ロックとパスワード複雑性チェックの可変パラメータをセキュリティパラメータとして保持する。

ストレージ管理ソフトウェアの不正な使用に関する警告メッセージをバナー情報として管理し、TOE の利用者からの要求に応じて生成、削除、改変を行う手段を提供する。

(3)警告バナー機能

ストレージ管理ソフトウェアからの要求に応じて、バナー情報を返信する。

TOE は、権限情報をストレージ管理ソフトウェアに応答するため、権限情報を格納したACLを権限外変更から保護する。ACLはユーザーIDに関係づけられ、TOE の利用者の役割(アカウント管理者等)のセキュリティ属性を持ち、ストレージ管理ソフトウェアにおける参照、変更処理の許可に関する権限情報からなる。TOEは、利用者を識別・認証する際に、必要に応じて当該ユーザーIDに対応するセキュリティ属性を読み出し、アクセス権限情報(セッションデータ)とする。

また、TOE は、認証のためのアカウント情報や、上記セキュリティ属性を設定するための、アカウント管理者用の機能を有する。アカウント管理者は、クライアント端末より、TOEの識別・認証を介してTOEのセキュリティ情報管理機能にアクセスし、利用者アカウントの生成・更新・削除・権限設定などのアカウント管理業務を行う。一般的にACLというとアクセス制御に使用されるTSFデータであり特定の管理者が管理するが、このTOEが主張するセキュリティ機能においては、ACLの権限情報を利用者データとして扱い、利用者(ストレージ管理者など)がACL情報に対し役割に応じた参照、更新などのアクセスを許可するものである。

また、TOEの利用方法を以下に示す。

(1)システム構築者による準備

●TOEを含む必要とされる情報システムリソースを購入する。

●TOE をインストールする機器の設置、接続、TOE の前提となる環境の構築、TOE のインストール、設定を行い、正しく動作することを確認する。

●デフォルトアカウント及びデフォルトパスワードを元に、アカウント管理権限を付与したアカウント管理者用のアカウントを作成し、アカウント管理者に通知する。

(2)アカウント管理者のアカウント管理業務

●アカウント管理者用のアカウント及びパスワードを取得する。

●アカウント管理者用のアカウント及びパスワードを用いてTOEにアクセスし、認証を受ける。

●設定すべきアカウント元情報をもとに、TOE に他のアカウント管理者及びストレージ管理者のアカウントを作成する。また、作成したアカウントに権限などの属性情報を設定する。

●他のアカウント管理者及びストレージ管理者に、作成したアカウント情報を通知する。

(3)ストレージ管理者のストレージ管理業務

●ストレージ管理者用のアカウント及びパスワードを取得する。

●ストレージ管理者用のアカウント及びパスワードを用いて TOE にアクセスし、認証を受ける。認証後、アカウントに対応した権限情報を取得する。

●TOEの認証後、取得した権限情報に合ったストレージ管理業務を行う。

2.5. 資産

ストレージ管理者が、認証に従った適切な権限情報を取得することで、ストレージ管理権限に基づく管理環境を得られるようにすることが TOE の主たる機能であることから、以下が TOE の保護対象資産である。

●権限情報

アカウントに対し許可されている権限情報であり、対応するユーザーID及びセキュリティ属性とともにACL内に保持される。

●バナー情報

警告バナー機能で使用する文面情報である。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 前提条件

A.PHYSICAL （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 （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 （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 （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 （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。

A.PASSWORD （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。

3.2. 脅威

3.2.1. 脅威エージェント

セキュリティ侵害を意図的、または偶然に試みる脅威エージェントを以下のように定義する。

- 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)

3.2.2. 脅威の識別

T.ILLEGAL_ACCESS (不正な接続)

不正な利用者が、管理クライアントから、ストレージ管理ソフトウェアの機能のために必要な、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 (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。

3.3. 組織のセキュリティ方針

P.BANNER (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。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境セキュリティ対策方針について記述する。

4.1. TOE セキュリティ対策方針

O.I&A

TOEは、許可された利用者のみが、ストレージ管理ソフトウェアの機能のために必要な、TOEで管理する権限情報にアクセスできるよう、利用者の識別・認証を行う。

O.MGMT

TOE は、権限情報、役割、およびバナー情報を参照、設定する手段を提供し、所定の権限を持つ利用者のみがその手段を使用できるようアクセス制御を実施する。

O.BANNER

TOE 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、ストレージ管理ソフトウェアに提供する。

O.PASSWORD

TOE は、設定されたセキュリティパラメータの値に従って、ストレージ管理ソフトウェアの利用者アカウントのパスワードの登録パターンを制限する。

4.2. 環境セキュリティ対策方針

4.2.1. IT 環境のセキュリティ対策方針

OE.SECURE_CHANNEL

管理サーバと管理クライアント間のネットワークは、暗号化などがなされた保護通信路を用い、暴露、改ざんから保護する。

OE.BANNER

ストレージ管理ソフトウェアは、TOE より提供された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メッセージを表示する機能を持つ。

4.2.2. 運用により実現するセキュリティ対策方針

OM.PHYSICAL

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、許可された管理者のみが入室できるよう入退出管理が行われた、物理的に隔離された業務サーバエリアに設置する。

OM.FIREWALL

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と、外部ネットワークとの間にはファイアウォールを設置し、外部ネットワークからの不要な通信が業務サーバエリア内のネットワークに流入しないように、ファイアウォールの設定および不正なトラフィックの監視を行う。

OM.ADMINISTRATORS

システム構築者が信頼できることを保証するために、そしてアカウント管理者、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が、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、悪意を持った行為を行わないことを保証するために、組織の責任者は適切な人選を行う。

OM.TOE_ACCOUNT

システム構築者、アカウント管理者、およびストレージ管理者は、自身が作成したストレージ管理ソフトウェアの利用者アカウントのパスワードを他人に漏らしてはならない。また推測されにくいパスワードを設定し、適切な頻度で変更する。

OM.TOKEN

システム構築者は、以下のトークンを使用した製品とTOEを組み合わせた環境構築を行わない。

- TOE以外によって生成されたトークン
- 利用者のユーザーID、パスワードが類推可能なトークン

OM.PASSWORD

システム構築者およびアカウント管理者は、不正な利用者によるパスワード推測によるログインを防ぐために、パスワードの複雑さを必要とし、認証の繰り返し試行を制限するような設定を行う。

5. IT セキュリティ要件

5.1. TOE セキュリティ要件

本章では、TOE セキュリティ要件について記述する。すべての機能要件コンポーネントは、CCパート2で規定されているものを使用する。

5.1.1. TOE セキュリティ機能要件

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、オブジェクト、及びSFPで扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: 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

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]

サブジェクト:利用者を代行するプロセス

オブジェクト:ACL テーブル、バナー情報ファイル

操作:参照、改変、生成、削除

[割付: アクセス制御 SFP]

ACLアクセス制御SFP

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: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: 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: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

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: セキュリティ属性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する規則]。

FDP_ACF.1.4 TSF は、[割付: セキュリティ属性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拒否する規則]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

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]および[割付: アクセス制御 SFP]

示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ	アクセス制御SFP
サブジェクト:利用者を代行するプロセス オブジェクト:ACL テーブル サブジェクト属性:サブジェクトに関連付けられたユーザーID、役割 オブジェクト属性:オブジェクトのユーザーID	ACLアクセス制御SFP
サブジェクト:利用者を代行するプロセス オブジェクト:バナー情報ファイル サブジェクト属性:サブジェクトに関連付けられたユーザーID、役割 オブジェクト属性:なし	ACLアクセス制御SFP

[割付: 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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

サブジェクト	オブジェクト	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、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則
利用者を代行するプロセス	ACL テーブル	サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致した場合のみ、当該利用者の役割と権限情報を参照できる。
利用者を代行するプロセス	ACL テーブル	サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致し、かつ、役割がアカウント管理者、システム構築者の場合、利用者の役割と権限情報を生成、削除、改変できる。
利用者を代行するプロセス	バナー情報ファイル	サブジェクトに関連付けられた役割がアカウント管理者、システム構築者の場合、バナー情報を生成、削除、改変できる。

[割付: セキュリティ属性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する規則]

サブジェクト	オブジェクト	セキュリティ属性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する規則
利用者を代行するプロセス	バナー情報ファイル	バナー情報の参照は常に許可される。

[割付: セキュリティ属性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拒否する規則]

サブジェクト	オブジェクト	セキュリティ属性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拒否する規則
利用者を代行するプロセス	ACL テーブル	サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致し、かつ、役割がアカウント管理者の場合でも、当該利用者の役割と権限情報を削除、改変できない。
利用者を代行するプロセス	ACL テーブル	オブジェクトがシステム構築者である役割とそれに対応する権限情報であった場合、当該役割と当該権限情報を削除、改変できない。

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: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限するために[割付: アクセス制御 SFP、情報フロー制御 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 セキュリティ役割

上述の割付及び選択を下表に示す。

セキュリティ属性	選択: デフォルト値変更、問い合わせ、改変、削除 割付: その他の操作	許可された識別された役割	アクセス制御 SFP、情報フロー制御 SFP

オブジェクトに関連付けられた、システム構築者およびサブジェクトのユーザーID 以外のユーザーID、役割	選択:改変、削除 割付:なし	アカウント管理者、システム構築者	ACLアクセス制御SFP
オブジェクトに関連付けられた、システム構築者またはサブジェクトのユーザーID と同一のユーザーID、役割	選択:なし 割付:なし	ー	ACLアクセス制御SFP

FMT_MSA.3 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: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]デフォルト値を与える[割付: アクセス制御 SFP、情報フロー制御 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: 許可された識別された役割]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

[選択: 制限的、許可的 : から一つのみ選択、[割付 : その他の特性]]

制限的、を選択

[割付 : その他の特性]

なし

[割付: アクセス制御 SFP、情報フロー制御 SFP]

ACLアクセス制御SFP

[割付: 許可された識別された役割]

なし

FMT_MTD.1 TSF データの管理

下位階層: なし

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付:許可された識別された役割]に制限しなければならない。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

上述の割付及び選択を下表に示す。

TSF データ	選択: デフォルト値変更、問い合わせ、改変、削除、消去 割付: その他の操作	許可された識別された役割
システム構築者以外のユーザーID	選択:削除 割付:登録	アカウント管理者、 システム構築者
システム構築者のユーザーID	選択:なし 割付:なし	ー
ユーザーIDに関連付けられたパスワード	選択:改変、削除 割付:登録	アカウント管理者、 システム構築者
	選択:改変	ユーザーIDに対応するストレージ管理者
ロックステータス	選択:問い合わせ、改変	アカウント管理者、 システム構築者
セキュリティパラメータ	選択:、問い合わせ、改変、消去 割付:なし	アカウント管理者、 システム構築者

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: TSF によって提供されるセキュリティ管理機能のリスト]。

依存性: なし

上述の割付を下表に示す。

表 3 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	管理要件	管理項目
FDP_ACC.1	なし	なし

FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	a) ユーザーIDとそれに関連付けられた権限情報の管理
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	a) なし(相互に影響を及ぼし得る役割のグループはない。)
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	a) なし(役割のグループはない。) b) なし(デフォルト値設定の管理はない。)
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) なし(相互に影響を及ぼし得る役割のグループはない。)
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	a) なし(役割の一部をなす利用者のグループはない。)
FIA_UAU.1	a) 管理者による認証データの管理; b) 関係する利用者による認証データの管理; c) 利用者が認証される前にとられるアクションのリストを管理すること。	a) パスワードの作成・改変 b) 利用者自身によるパスワード改変 c) なし(リストに変更はない。)
FIA_UID.1	a) 利用者識別情報の管理; b) 許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	a) アカウントのユーザーIDの作成・削除 b) なし(リストに変更はない。)
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	a) パスワード設定時に必要な文字数・構成文字種の指定
FIA_ATD.1	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	a) なし(セキュリティ属性の追加の定義はない。)

FIA_USB.1	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし(デフォルトではセキュリティ属性を付与しない。) b) なし(デフォルトではセキュリティ属性を付与しないため、ない。)
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) 管理者による閾値の設定・改変 b) なし(アカウントがロックされる以外のアクションはない。)
FTA_TAB.1	a) 許可管理者によるバナーの維持。	a) 管理者によるバナー内容の設定
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし

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: 許可された識別された役割]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づけなければならない。

依存性: FIA_UID.1 識別のタイミング

[割付: 許可された識別された役割]

ストレージ管理者、アカウント管理者、システム構築者

FIA_UAU.1 認証のタイミング

下位階層: なし

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: TSF 調停アクションのリスト]を許可しなければならない。

FIA_UAU.1.2 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、各利用者に認証が成功することを要求しなければならない。

依存性: FIA_UID.1 識別のタイミング

[割付: TSF 調停アクションのリスト]

警告バナー機能

FIA_UID.1 識別のタイミング

下位階層: なし

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付:TSF 調停アクションのリスト]を許可しなければならない。

FIA_UID.1.2 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、各利用者に識別が成功することを要求しなければならない。

依存性: なし

[割付: TSF 調停アクションのリスト]

警告バナー機能

FIA_SOS.1 秘密の検証

下位階層: なし

FIA_SOS.1.1 TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

依存性: なし

[割付: 定義された品質尺度]

セキュリティパラメータに記載されたパスワード生成条件

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリスト[割付:セキュリティ属性のリスト]を維持しなければならない。

依存性: なし

[割付:セキュリティ属性のリスト]

ユーザーID、役割

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1 TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない:[割付: 利用者セキュリティ属性のリスト]

FIA_USB.1.2 TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: 属性の最初の関連付けに関する規則]

FIA_USB.1.3 TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: 属性の変更に関する規則]

依存性: FIA_ATD.1 利用者属性定義

上述の割付及び選択を下表に示す。

利用者セキュリティ属性	属性の最初の関連付けに関する規則	属性の変更に関する規則
オブジェクトに関連付けられたユーザーID、役割	なし	なし

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

FIA_AFL.1.1 TSF は、[割付: 認証事象のリスト]に関して、[選択: [割付: 正の整数値],「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付: アクションのリスト]をしなければならない。

依存性: FIA_UAU.1 認証のタイミング

[割付: 認証事象のリスト]
最後に成功した認証以降の利用者の認証アカウント(但しシステム構築者は除く)

[選択: [割付: 正の整数値],「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」]
選択:「[割付: 許容可能な値の範囲] 内における管理者設定可能な正の整数値]」
許容可能な値の範囲:セキュリティパラメータ内で規定された数値の範囲

[割付: アクションのリスト]
アカウントをロックする(但しシステム構築者は除く)。

FTA_TAB.1 デフォルト TOE アクセスバナー

下位階層: なし

FTA_TAB.1.1 利用者セション確立前に、TSF は、TOE の不正な使用に関する勧告的警告メッセージを表示しなければならない。

依存性: なし

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

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や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

本 TOE の最小機能強度レベルは、SOF-基本である。確率的または順列的メカニズムに基づくセキュリティ機能要件は、FIA_UAU.1、FIA_SOS.1 である。

5.1.3. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 であり、追加する保証コンポーネントは ALC_FLR.1 である。

すべての保証要件コンポーネントは、CCパート 3 で規定されている保証コンポーネントを直接使用する。EAL2 追加(EAL2＋ALC_FLR.1)の保証コンポーネントを表 4に示す。

表 4 EAL2 追加(EAL2＋ALC_FLR.1)保証コンポーネント一覧

保証クラス	保証コンポーネント	
構成管理(ACM クラス)	**ACM_CAP.2**	構成要素
配付と運用(ADO クラス)	**ADO_DEL.1**	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
開発(ADV クラス)	**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
ガイダンス文書(AGD クラス)	**AGD_ADM.1**	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート (ALC クラス)	**ALC_FLR.1**	基本的な欠陥修正
テスト(ATE クラス)	**ATE_COV.1**	カバレージの証拠
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定(AVA クラス)	**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 環境のセキュリティ要件

IT 環境が提供するセキュリティ機能の機能要件を記述する。すべての機能要件コンポーネントは、CCパート2で規定されているものを使用する。

5.2.1. IT 環境のセキュリティ機能要件

FPT_ITC.1 送信中の TSF 間機密性

下位階層: なし

FPT_ITC.1.1 [詳細化:管理サーバと管理クライアント間のネットワーク]は、TSF からリモート高信頼 IT 製品に送信されるすべてのTSFデータを、送信中の不当な暴露から保護しなければならない。

依存性: なし

FTA_TAB.1E デフォルト TOE アクセスバナー

下位階層: なし

FTA_TAB.1.1 利用者セション確立前に、[詳細化:ストレージ管理ソフトウェア]は、TOE の不正な使用に関する勧告的警告メッセージを表示しなければならない。

依存性: なし

6. TOE 要約仕様

本章では、TOE セキュリティ機能、セキュリティ機能強度、セキュリティ保証手段について記述する。

6.1. TOE セキュリティ機能

本節では、TOE セキュリティ機能について記述する。表 5 に示すように、本節で説明するセキュリティ機能は、5.1.1 節で記述した TOE セキュリティ機能要件を満足している。

表 5 TOEセキュリティ機能とTOEセキュリティ機能要件の対応関係

TOE セキュリティ機能要件 / TOE セキュリティ機能	FDP_ACC.1	FDP_ACF.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FIA_UAU.1	FIA_UID.1	FIA_SOS.1	FIA_ATD.1	FIA_USB.1	FIA_AFL.1	FIA_TAB.1	FPT_RVM.1	FPT_SEP.1
SF.I&A	○	○						○	○		○	○	○		○	○
SF.MGMT	○	○	○	○	○	○	○			○					○	○
SF.BANNER	○	○												○	○	

6.1.1. 識別・認証機能(SF.I&A)

SF.I&A は、利用者がストレージ管理ソフトウェアおよび TOE を利用する際に利用者の識別・認証を行い、ストレージ管理ソフトウェアからの要求に応じて、ログイン中の利用者のセッションを管理して、ログインした利用者の識別・認証が維持されていることの確認を行う。

(1)識別・認証

SF.I&A は、利用者がストレージ管理ソフトウェアにログインする際、またはストレージ管理ソフトウェアが **SF.MGMT** の提供するセキュリティ情報管理機能を実行する際の、ストレージ管理ソフトウェアからの、ユーザーID、パスワードによる利用者アカウントの識別・認証要求を受け付けると、登録済みのアカウント情報(利用者のユーザーID、パスワード、ロックステータス(ロック中/ロック解除状態)の対応)と比較して、利用者アカウントの識別・認証を行う。

利用者アカウントの識別および認証に成功し、かつその利用者アカウントがロック解除状態である場合、**SF.I&A** は、 ACL テーブルへのアクセスを行い、その利用者の役割および権限情報を取得する。このとき **SF.I&A** は、利用者を代行するプロセス(サブジェクト)に関連付けられたユーザーID に基づいて、以下のルールに従い ACL テーブル(オブジェクト)に対するアクセス制御を行う。

・ サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致した場合のみ、当該利用者の権限情報を参照できる。

上記取得した役割および権限情報に当該ストレージ管理ソフトウェアを利用するための役割または権限情報が含まれている場合、以下のセッション管理の処理に移行する。

利用者の識別または認証に失敗した場合、またはその利用者アカウントがロック中である場合、または取得した役割および権限情報に当該ストレージ管理ソフトウェアを利用するための役割または権限情報が含まれていない場合、**SF.I&A** はストレージ管理ソフトウェアに対してエラーを返信する。

SF.I&A による利用者の識別・認証に成功する以前に、警告バナー機能(**SF.BANNER**)が提供する警告メッセージの通知を除いて、いかなる動作も実行されることはない。

SF.I&A は、ストレージ管理ソフトウェアからの利用者の識別・認証要求を受け付けたとき、**SF.I&A** が必ず実施されることを保証する。

SF.I&A は、上記の利用者を代行するプロセスが、ACL テーブルへのアクセスを行う際、上記のアクセス制御が必ず実施されることを保証する。

(2)アカウント自動ロック

SF.I&A は、ストレージ管理ソフトウェアにログインする際の利用者の識別・認証時において、一定回数連続して認証に失敗した利用者アカウントを自動的にロックする。ただし、システム構築者のアカウントのロックは行わない。アカウントがロックされる期間は無期限である。ロックの解除、および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の設定は、**SF.MGMT** によって実行される。**SF.I&A** は、各利用者アカウントごとの認証連続失敗回数を管理しており、認証に成功した場合、および認証連続失敗回数がしきい値に達しアカウントがロックされた場合のみ、そのアカウントの連続失敗回数をクリアする。アカウント自動ロックが行われた時点で既にストレージ管理ソフトウェアにログイン済みの同一アカウントの別セッションが存在する場合、アカウント自動ロックは、その既に認証に成功している同一アカウントの操作へは影響を与えない。

(3)セッション管理

SF.I&A は、上記の利用者アカウントの識別・認証、および必要な役割、権限情報の取得に成功した場合、その利用者のユーザーID、役割をセッションデータとして維持、管理し、利用者を代行するプロセスに対してそのユーザーIDと役割を関連付ける。

ストレージ管理ソフトウェアが、**SF.MGMT** の提供するセキュリティ情報管理機能の実行を要求している場合、**SF.MGMT** の処理に移行する。このとき **SF.I&A** は、上記セキュリティ情報管理機能が実行される間、上記セッションデータを維持、管理する。

ストレージ管理ソフトウェアが、利用者のログインの認証を要求している場合、**SF.I&A** はログインごとの利用者のセッションを識別するためのトークンを生成し、ストレージ管理ソフトウェアからの要求に応じて、ログインに成功した利用者に対応付けられたユーザーID、役割、権限情報、トークン等の返信を行う。

ストレージ管理ソフトウェアへのログインに成功した利用者のセッション確立後、**SF.I&A** は、ストレージ管理ソフトウェアまたは他の TSF より、トークンを用いた利用者のセッションの有効性確認要求を受け付けると、セッションデータを参照して、当該利用者のセッションの有効性確認を行う。

利用者のセッションの有効性を確認した場合、**SF.I&A** は、ストレージ管理ソフトウェアからの要求に応じて、当該利用者に対応付けられたユーザーID、役割、権限情報を返信する。

利用者のセッションの有効性を確認できなかった場合、**SF.I&A** はストレージ管理ソフトウェアまたは他の TSF に対してエラーを返信する。

SF.I&A は、**SF.MGMT** によって利用者のログイン中にその利用者に対応する ACL テーブルの役割が変更されたとしても、その利用者に対応するセッションデータ内の役割を変更しない。そのため利用者がストレージ管理ソフトウェアにログインしている間は、ログイン時点での役割が適用される。

SF.I&A は、利用者からログアウト要求を受け付けた場合、セッションデータから、その利用者のセッションに関する情報を削除し、そのセッションを終了する。

ログインに成功した利用者を代行するプロセスごとに関連付けられたユーザーID および役割の情報は、許可されたプロセスからのアクセスのみ許可される。従って **SF.I&A** は、上記ユーザーID および役割が、ログインに成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

6.1.2. セキュリティ情報管理機能(**SF.MGMT**)

SF.MGMT は、アカウント情報や ACL、バナー情報、セキュリティパラメータ等の管理を行う機能であり、**SF.MGMT** を利用するためには、**SF.I&A** によってその利用者アカウントの識別・認証に成功していることが前提となる。

(1)アカウント管理

SF.MGMT は、利用者アカウントごとのユーザーID、パスワード、ロックステータス(ロック中/ロック解除状態)の対応をアカウント情報として管理する。**SF.MGMT** 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。

SF.MGMT 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。

(2)パスワード複雑性チェック

SF.MGMT は、アカウントの新規作成およびパスワード登録、改変時に、パスワードが以下の品質尺度を満たしているかどうかの確認を行い、品質尺度を満たさないパスワードの設定を認めない。

- セキュリティパラメータで決定されるパスワード最小文字数の条件を満たす。

・ パスワードとして使用可能な文字種が英数字、記号であり、かつセキュリティパラメータで決定されるパスワード複雑性条件を満たす。

(3)ACL 管理

SF.MGMT は、利用者アカウントごとのユーザーID、役割、権限情報との対応を、ACL として管理する。**SF.MGMT** は、利用者からの要求に応じてACLテーブルへのアクセスを行い、役割および権限情報の登録、改変、削除、の操作を行う手段を提供する。

SF.MGMT は、ユーザーID に対する役割および権限情報に対して、役割未設定および権限未設定の初期値を与える。

SF.MGMT は、利用者を代行するプロセスが上記の操作を行う際、そのプロセス(サブジェクト)に関連付けられたユーザーID および役割に基づいて、以下のルールに従い ACL テーブル(オブジェクト)に対するアクセス制御を行う。

・ サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致し、かつ、役割がアカウント管理者、システム構築者の場合、利用者の役割と権限情報を生成、削除、改変できる。
・ サブジェクトに関連付けられたユーザーIDが、オブジェクトのユーザーIDと一致し、かつ、役割がアカウント管理者の場合でも、当該利用者の役割と権限情報を削除、改変できない。
・ オブジェクトがシステム構築者である役割とそれに対応する権限情報であった場合、当該役割と当該権限情報を削除、改変できない。

SF.MGMT は、上記のアクセス制御が必ず実施されることを保証する。

ACLの情報は、許可されたプロセスからのアクセスのみ許可される。従って **SF.MGMT** は、上記 ACLの情報が、識別・認証に成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

(4)セキュリティパラメータ管理

SF.MGMT は、「アカウント自動ロック」、「パスワード複雑性チェック」の TSF に関する可変パラメータをセキュリティパラメータとして管理する。セキュリティパラメータの一覧を表 6 に示す。**SF.MGMT** は、利用者からの要求に応じて、各パラメータの問い合わせ、改変、消去、の操作を行う手段を提供する。

SF.MGMT は、アカウント管理者およびシステム構築者に対してのみ、上記の全ての操作の実行を許可する。

表 6 セキュリティパラメータの一覧

#	パラメータ	内容
1	認証の連続失敗回数のし	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

	きい値	めの認証の連続失敗回数のしきい値。
2	パスワード最小文字数	パスワードの最小文字数。
3	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。

(5)バナー情報管理

SF.MGMT 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、バナー情報として管理する。**SF.MGMT** は、利用者からの要求に応じてバナー情報ファイルへのアクセスを行い、バナー情報の生成、削除、改変を行う手段を提供する。

SF.MGMT は、利用者を代行するプロセスが上記の操作を行う際、そのプロセス(サブジェクト)に関連付けられたユーザーID および役割に基づいて、以下のルールに従いバナー情報ファイル(オブジェクト)に対するアクセス制御を行う。

- サブジェクトに関連付けられた役割がアカウント管理者、システム構築者の場合、バナー情報を生成、削除、改変できる。

SF.MGMT は、上記のアクセス制御が必ず実施されることを保証する。

バナー情報は、バナー情報ファイル編集機能の使用を許可されたプロセス、および管理サーバへのログインに成功したシステム構築者からのアクセスのみ許可される。従って **SF.MGMT** は、上記バナー情報が、識別・認証に成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

6.1.3. 警告バナー機能(SF.BANNER)

SF.BANNER は、ストレージ管理ソフトウェアからの要求に応じて、**SF.MGMT** において設定されたバナー情報を返信する。このとき **SF.BANNER** は、バナー情報の参照が常に許可されるようアクセス制御を行う。バナー情報は、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の文面であり、ストレージ管理ソフトウェアでは、上記取得した警告メッセージを、利用者の識別・認証を行うためのログイン画面に表示する。

SF.BANNER は、上記のアクセス制御が必ず実施されることを保証する。

6.2. セキュリティ強度

確率的または順列的メカニズムに基づくセキュリティ機能は、識別・認証機能(**SF.I&A**)におけるセッション管理時のトークンの生成、パスワードの照合、およびセキュリティ設定機能(**SF.MGMT**)におけるパスワード複雑性チェックである。両者とも、そのセキュリティ強度は、SOF-基本である。

6.3. 保証手段

本 ST で適用するセキュリティ保証要件とセキュリティ保証手段の対応を表 7 に示す。本 ST で適用するセキュリティ保証手段として、以下に示すドキュメントおよび製品を提供する。

表 7　セキュリティ保証要件とセキュリティ保証手段の対応表

セキュリティ保証要件	セキュリティ保証手段
ACM_CAP.2　構成要素	HiCommand Suite Common Component 構成管理文書
ADO_DEL.1　配付手続き	HiCommand Suite Common Component 配付文書
ADO_IGS.1　設置、生成、および立ち上げ手順	HiCommand Suite Common Component セキュリティガイド
ADV_FSP.1　非形式的機能仕様	HiCommand Suite Common Component 機能仕様書
ADV_HLD.1　記述的上位レベル設計	HiCommand Suite Common Component 構造設計書
ADV_RCR.1　非形式的対応の実証	HiCommand Suite Common Component 対応分析書
AGD_ADM.1　管理者ガイダンス	HiCommand Suite Common Component セキュリティガイド
AGD_USR.1　利用者ガイダンス	HiCommand Suite Common Component セキュリティガイド
ALC_FLR.1　基本的な欠陥修正	HiCommand Suite Common Component セキュリティ欠陥修正規程書
ATE_COV.1　カバレージの証拠	HiCommand Suite Common Component テスト計画書
ATE_FUN.1　機能テスト	HiCommand Suite Common Component テスト報告書
ATE_IND.2　独立試験 – サンプル	HiCommand Suite Common Component 05-51
AVA_SOF.1　TOE セキュリティ機能強度評価	HiCommand Suite Common Component セキュリティ機能強度分析書
AVA_VLA.1　開発者脆弱性分析	HiCommand Suite Common Component 脆弱性分析書

7. PP 主張

本 ST では、主張すべき PP は存在しない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

セキュリティ対策方針は、TOE セキュリティ環境で規定した脅威に対抗するためのものであり、前提条件と組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対抗する脅威、実現する前提条件および組織のセキュリティ方針の対応関係を表 8 に示す。

表 8 セキュリティ対策方針と前提条件、脅威、組織のセキュリティ方針の対応表

TOE セキュリティ環境 / セキュリティ対策方針	A.PHYSICAL	A.NETWORKS	A.ADMINISTROTORS	A.SECURE_CHANNEL	A.TOKEN	A.PASSWORD	T.ILLEGAL_ACCESS	T.UNAUTHORISED_ACCESS	P.BANNER
O.I&A							○		
O.MGMT								○	
O.BANNER									○
O.PASSWORD							○		
OE.SECURE_CHANNEL				○					
OE.BANNER									○
OM.PHYSICAL	○								
OM.FIREWALL		○							
OM.ADMINISTROTORS			○						
OM.TOE_ACCOUNT							○		
OM.TOKEN					○				
OM.PASSWORD						○			

表 8 により、各セキュリティ対策方針は 1 つ以上の前提条件、脅威、または組織のセキュリティ方針に対応して

いる。

次に、各脅威、前提条件、組織のセキュリティ方針がセキュリティ対策方針で実現できることを説明する。

①セキュリティ脅威

T.ILLEGAL_ACCESS （不正な接続）

O.I&A により、TOE は、利用者が TOE およびストレージ管理ソフトウェアにアクセスする際に、その識別・認証を行い、許可された利用者であるかどうかの確認を行う。また **O.PASSWORD** により、TOE は、パスワードは推測されにくいものが設定されるようパスワードの登録パターンを制限する。また **OM.TOE_ACCOUNT** により、利用者は、自分自身が作成したパスワードを他人に漏らさない。パスワードは推測されにくいものが設定され、適切な頻度で変更されるため、不正な利用者が他人のパスワードを知ることは困難である。

以上により、**T.ILLEGAL_ACCESS** は、**O.I&A**、**O.PASSWORD**、**OM.TOE_ACCOUNT** によって対抗できる。

T.UNAUTHORISED_ACCESS （権限外の接続）

O.MGMT により、TOE は、ストレージ管理ソフトウェアおよび TOE の利用者に与えられた権限情報に従って、利用者による権限情報、バナー情報へのアクセスを制御する。

以上により、**T.UNAUTHORISED_ACCESS** は、**O.MGMT** によって対抗できる。

②前提条件

A.PHYSICAL （ハードウェア等の管理）

OM.PHYSICAL により、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る。また業務サーバエリアの入退出管理が行われ、許可された管理者のみが入室できる。

以上により、**A.PHYSICAL** は、**OM.PHYSICAL** によって実現できる。

A.NETWORKS （ネットワーク）

OM.FIREWALL により、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と、外部ネットワークとの間にはファイアウォールが設置され、外部ネットワークからの TOE に対する不要な通信やリモート操作が内部ネットワークに流入しなくなり、各ネットワークは論理的に分離され、不正なトラフィックが監視される。

以上により、**A.NETWORKS** は、**OM.FIREWALL** によって実現できる。

A.ADMINISTRATORS （管理者）

OM.ADMINISTRATORS により、組織の責任者は、システム構築者、アカウント管理者、ストレージ管理者、および業務サーバを含めた他サーバの管理者についての適切な人選を行う。従って、システム構築者は信頼

できる。またアカウント管理者、ストレージ管理者、および業務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、悪意を持った行為を行わない

以上により、**A.ADMINISTRATORS** は、**OM.ADMINISTRATORS** によって実現できる。

A.SECURE_CHANNEL（通信の秘匿性）

OE.SECURE_CHANNEL により、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、暗号化などがなされた保護通信路が用いられ、通信の秘匿性と完全性が確保される。

以上により、**A.SECURE_CHANNEL** は、**OE.SECURE_CHANNEL** によって実現できる。

A.TOKEN（利用可能なトークン）

OM.TOKEN により、システム構築者は、以下のトークンを使用した製品と TOE を組み合わせた環境構築を行わない。

- TOE 以外によって生成されたトークン
- 利用者のユーザーID、パスワードが類推可能なトークン

以上により、**A.TOKEN** は、**OM.TOKEN** によって実現できる。

A.PASSWORD（複雑なパスワード）

OM.PASSWORD により、管理者は、不正な利用者によるパスワード推測によるログインを防ぐために、パスワードの複雑さを必要とし、認証の繰り返し試行を制限するような設定を行う。

以上により、**A.PASSWORD** は、**OM.PASSWORD** によって実現できる。

③組織のセキュリティ方針

P.BANNER（警告バナー）

O.BANNER により、TOE 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、ストレージ管理ソフトウェアに提供する。**OE.BANNER** により、ストレージ管理ソフトウェアは、TOE より提供された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メッセージを表示する機能をもつ。

以上により、**P.BANNER** は、**O.BANNER**、**OE.BANNER** によって実現できる。

8.2. セキュリティ要件根拠

8.2.1. TOE セキュリティ機能要件根拠

本 ST で選択した TOE および IT 環境のセキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 9 に示す。

表 9　セキュリティ機能要件とTOEセキュリティ対策方針の対応関係

TOE セキュリティ対策方針 / TOE セキュリティ機能要件	O.I&A	O.MGMT	O.BANNER	O.PASSWORD	OE.SECURE_CHANNEL	OE.BANNER
FDP_ACC.1		○	○			
FDP_ACF.1		○	○			
FMT_MSA.1		○				
FMT_MSA.3		○				
FMT_MTD.1	○	○				
FMT_SMF.1		○				
FMT_SMR.1		○				
FIA_UAU.1	○					
FIA_UID.1	○					
FIA_SOS.1				○		
FIA_ATD.1	○					
FIA_USB.1	○					
FIA_AFL.1	○					
FIA_TAB.1			○			
FPT_RVM.1	○	○	○			
FPT_SEP.1	○	○				
FPT_ITC.1					○	
FIA_TAB.1E						○

表 9 より、TOE の各セキュリティ機能要件は、1 つ以上の TOE セキュリティ対策方針に対応している。また IT 環境の各セキュリティ機能要件は、1 つ以上の IT 環境のセキュリティ対策方針に対応している。

次に、TOE の各セキュリティ対策方針が、TOE のセキュリティ機能要件で実現できることを説明する。

O.I&A

TOE は、利用者が TOE およびストレージ管理ソフトウェアにアクセスする際に、**FIA_UID.1** により利用者が許可された利用者であることを識別し、**FIA_UAU.1** によりその利用者本人であることを認証している。このと

きTOEは、**FIA_AFL.1**により、一定回数連続して認証に失敗した利用者のアカウントをロックする。TOEは、**FIA_ATD.1**により、識別・認証に成功した利用者のユーザーID、役割をセッションデータとして維持・管理し、**FIA_USB.1**により、上記利用者を代行するプロセスに対して、そのユーザーIDと役割を関連付ける。

またTOEは、**FMT_MTD.1**により、利用者ごとのユーザーID、パスワード、ロックステータス、をアカウント管理者およびシステム構築者のみが管理できるように制限する。

またTOEは、**FPT_RVM.1**、**FPT_SEP.1**により、セキュリティ機能のバイパス、干渉・改ざんを防ぐ。

以上により、**O.I&A**は、**FIA_UAU.1**、**FIA_UID.1**、**FIA_ATD.1**、**FIA_AFL.1**、**FIA_USB.1**、**FMT_MTD.1**、**FPT_RVM.1**、**FPT_SEP.1**によって実現できる。

O.MGMT

TOEは、**FMT_MSA.1**により、利用者のセキュリティ属性であるユーザーID、役割をアカウント管理者およびシステム構築者のみが管理できるように制限し、**FMT_MSA.3**により、役割未設定の制限的初期値を与える。またTOEは、**FMT_MTD.1**により、セキュリティパラメータ、をアカウント管理者およびシステム構築者のみが管理できるように制限する。

TOEは、**FDP_ACC.1**、**FDP_ACF.1**により、認証に成功した利用者の役割および権限情報をACLテーブルより取得する際、利用者のユーザーIDに基づいて、ACLテーブルに対するアクセス制御を行い、利用者がACLテーブルおよびバナー情報ファイルへの操作を行う際、利用者のユーザーIDと役割に基づいて、ACLテーブルおよびバナー情報ファイルに対するアクセス制御を行う。

TOEは、**FMT_SMR.1**により、ストレージ管理者、アカウント管理者、システム構築者という役割を維持する。

TOEは**FMT_SMF.1**により、管理項目に示したセキュリティ管理機能を行う能力を持つ。

またTOEは、**FPT_RVM.1**、**FPT_SEP.1**により、セキュリティ機能のバイパス、干渉・改ざんを防ぐ。

以上により、**O.MGMT**は、**FDP_ACC.1**、**FDP_ACF.1**、**FMT_MSA.1**、**FMT_MSA.3**、**FMT_MTD.1**、**FMT_SMF.1**、**FMT_SMR.1**、**FPT_RVM.1**、**FPT_SEP.1**によって実現できる。

O.BANNER

FIA_TAB.1により、TOE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取得し、ストレージ管理ソフトウェアに提供する。その際、TOEは、**FDP_ACC.1**、**FDP_ACF.1**により、警告メッセージを含むバナー情報ファイルの参照が常に許可されるよう、バナー情報ファイルに対するアクセス制御を行う。

またTOEは、**FPT_RVM.1**により、上記アクセス制御のバイパスを防ぐ。

以上により、**O.BANNER**は、**FIA_TAB.1**、**FDP_ACC.1**、**FDP_ACF.1**、**FPT_RVM.1**によって実現できる。

O.PASSWORD

FIA_SOS.1により、TOEは、秘密(パスワード)の品質尺度を維持する。

以上により、**O.PASSWORD**は、**FIA_SOS.1**によって実現できる。

次に、IT 環境のセキュリティ対策方針が、IT 環境のセキュリティ機能要件で実現できることを説明する。

OE.SECURE_CHANNEL

FPT_ITC.1 により、TOE は、管理サーバと管理クライアントとの間のネットワークに対して、ユーザーID、パスワード、トークン等の通信データを改変や暴露から保護するための暗号化などがなされた保護通信路を提供することを要求する。

以上により、**OE.SECURE_CHANNEL** は、**FPT_ITC.1** によって実現できる。

OE.BANNER

FIA_TAB.1E により、TOE は、ストレージ管理ソフトウェアに対して、そ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ことを要求する。

以上により、**OE.BANNER** は、**FIA_TAB.1E** によって実現できる。

8.2.2. 最小機能強度レベル根拠

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。本 ST は、TOE に対して、最小機能強度レベルとして“SOF-基本”を求めており、一貫している。

8.2.3. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 10 に示す。

表 10 セキュリティ機能要件のコンポーネントの依存性

本 ST で選択した機能要件コンポーネント	CC パート 2 で規定されている依存コンポーネント	本 ST で選択した依存コンポーネント	充足性
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	○
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	○
	FMT_MSA.3	FMT_MSA.3	○
FMT_MSA.1	FDP_ACC.1	FDP_ACC.1	○
	FMT_SMF.1	FMT_SMF.1	○
	FMT_SMR.1	FMT_SMR.1	○
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	○
	FMT_SMR.1	FMT_SMR.1	○
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	○

	FMT_SMR.1	FMT_SMR.1	○
FMT_SMF.1	なし	―	―
FMT_SMR.1	FIA_UID.1	FIA_UID.1	○
FIA_UAU.1	FIA_UID.1	FIA_UID.1	○
FIA_UID.1	なし	―	―
FIA_SOS.1	なし	―	―
FIA_ATD.1	なし	―	―
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	○
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	○
FIA_TAB.1	なし	―	―
FPT_RVM.1	なし	―	―
FPT_SEP.1	なし	―	―
FPT_ITC.1	なし	―	なし
FIA_TAB.1E	なし	―	なし

以上により、各セキュリティ機能要件は、必要な依存関係をすべて満たしている。

8.2.4. セキュリティ保証要件依存性

ALC_FLR.1 から依存される保証コンポーネントはない。

8.2.5. セキュリティ機能要件相互補完性

依存関係を満たす全ての TOE セキュリティ機能要件が選択されており、機能要件の特性において不足することはない。

迂回防止

アクセス制御や識別・認証およびセキュリティ情報管理機能の要件について FPT_RVM.1 が選択され、バイパス防止が達成されている。また重複する機能要件は選択されていないため、矛盾や競合はおきない。

干渉防止

TSF および TSF データの保護の要件について FPT_SEP.1 が選択され、干渉から保護されている。

非活性化

本 TOE は、TOE がインストールされた時点からセキュリティ機能が活性化されており、TOE のビルトインアカウント(システム構築者のアカウント)は、活性化された状態のセキュリティ機能を使用することを前提としている。よって本 TOE は、セキュリティ機能を非活性化された状態で使用されることはなく、FMT_MOF.1 を選択する必要がない。

8.2.6. 監査対象事象根拠

本 TOE は、FIA_SOS.1 を機能要件として主張しており、TOE は、利用者の識別・認証のためのパスワードが、パスワード最小文字数、およびパスワード複雑性条件を満たすことを検証するメカニズムを提供し、OM.PASSWORD により、容易に類推できないパスワードしか使用できないようなセキュリティパラメータの設定が行われる。また TOE の使用環境として、信頼できる利用者が、容易に類推されないパスワードを TOE に設定することを前提としている。

また本 TOE は、FIA_AFL.1 を機能要件として主張しており、TOE は認証の連続失敗時にアカウントをロックする機能を提供し、OM.PASSWORD により、ログインの連続試行を制限するようなセキュリティパラメータの設定が行われる。

以上のことから、本 ST では、TOE に登録されていない利用者のログインの繰り返し試行などを監査手段によって検出することをセキュリティ対策方針としてあげていない。従って、セキュリティ機能要件 FAU_GEN.1 を選択していないため、監査対象事象の根拠は対象とはならない。

8.2.7. セキュリティ管理機能根拠

本 ST で選択した TOE セキュリティ機能要件について、CC パート 2 で規定された管理要件と TSF で管理する管理項目との対応を表 3 に示している。

表 11 に、表 3 で示した TSF の管理項目と第 6.1 節で述べた TOE セキュリティ機能との対応を示す。

表 11 TSFの管理項目とTOEセキュリティ機能との対応

機能要件	管理項目	TOE のセキュリティ機能
FDP_ACC.1	なし	－
FDP_ACF.1	a) ユーザーIDとそれに関連付けられた権限情報の管理	a) **SF.MGMT**
FMT_MSA.1	a) なし（相互に影響を及ぼし得る役割のグループはない。）	a) －
FMT_MSA.3	a) なし（役割のグループはない。） b) なし（デフォルト値設定の管理はない。）	a) － b) **SF.MGMT**
FMT_MTD.1	a) なし（相互に影響を及ぼし得る役割のグループはない。）	a) －
FMT_SMR.1	a) なし（役割の一部をなす利用者のグループはない。）	a) －

FIA_UAU.1	a) パスワードの作成・改変 b) 利用者自身によるパスワード改変 c) なし(リストに変更はない。)	a) **SF.MGMT** b) **SF.MGMT** c) －
FIA_UID.1	a) アカウントのユーザーIDの作成・削除 b) なし(リストに変更はない。)	a) **SF.MGMT** b) －
FIA_SOS.1	a) パスワード設定時に必要な文字数・構成文字種の指定	a) **SF.MGMT**
FIA_ATD.1	a) なし(セキュリティ属性の追加の定義はない。)	a) －
FIA_USB.1	a) なし(デフォルトではセキュリティ属性を付与しない。) b) なし(デフォルトではセキュリティ属性を付与しないため、ない。)	a) － b) －
FIA_AFL.1	a) 管理者による閾値の設定・改変 b) なし(アカウントがロックされる以外のアクションはない。)	a) **SF.MGMT** b) －
FTA_TAB.1	a) 管理者によるバナー内容の設定	a) **SF.MGMT**
FPT_RVM.1	なし	－
FPT_SEP.1	なし	－

8.2.8. セキュリティ保証要件根拠

本 TOE の評価保証レベルは、EAL2+ALC_FLR.1 である。

本TOEが想定する利用者は、ストレージの管理者で限定された者であり、登録された人が使うため、攻撃の意思は抑制される。EAL2 は、このような TOE の特性に対して、構造設計の観点での評価、セキュアな配付手続き、脆弱性評定を含むことから妥当な選択である。

また昨今、セキュリティ脆弱性問題への対応が重要となってきている。本製品はストレージの管理を行う重要な部分を受け持ち、セキュリティ欠陥を追跡し、脆弱性に対する迅速な対応が求められる。セキュリティ欠陥に対する保証は、利用者に対する安心を担保するうえで重要であり ALC_FLR.1 を選択する。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係を表 12 に示す。

表 12　TOEセキュリティ機能とTOEセキュリティ機能要件の対応関係

TOE セキュリティ機能要件 / TOE セキュリティ機能	FDP_ACC.1	FDP_ACF.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FIA_UAU.1	FIA_UID.1	FIA_SOS.1	FIA_ATD.1	FIA_USB.1	FIA_AFL.1	FIA_TAB.1	FPT_RVM.1	FPT_SEP.1
SF.I&A	○	○						○	○		○	○	○		○	○
SF.MGMT	○	○	○	○	○	○	○			○					○	○
SF.BANNER	○	○												○	○	

表 12 により、各 TOE セキュリティ機能が 1 つ以上の TOE セキュリティ機能要件に対応している。

次に、各 TOE セキュリティ機能要件が、TOE セキュリティ機能で実現できていることを説明する。

FDP_ACC.1:

FDP_ACF.1:

SF.I&A により、TOE は、利用者を代行してその識別・認証を行うプロセス(サブジェクト)が、ACL テーブル(オブジェクト)を参照して利用者に付与された役割および権限情報を取得する場合、そのサブジェクトに関連付けられたユーザーID とオブジェクトのユーザーID に基づいてオブジェクトに対するアクセス制御を行う。

SF.MGMT により、TOE は、利用者を代行して動作するプロセス(サブジェクト)が ACL テーブルおよびバナー情報ファイル(オブジェクト)の参照、改変、生成、削除の操作を行う場合、そのサブジェクトに関連付けられたユーザーID、役割とオブジェクトのユーザーID に基づいてオブジェクトに対するアクセス制御を行う。

SF.BANNER により、TOE は、利用者を代行するプロセス(サブジェクト)がバナー情報ファイル(オブジェクト)を参照して警告メッセージ等を取得する場合、その参照のみを許可するようアクセス制御を行う。

以上により、**FDP_ACC.1**、**FDP_ACF.1** は、**SF.I&A** 、**SF.MGMT**、**SF.BANNER** により実現できる。

FMT_MSA.1:

SF.MGMT により、TOE は、セキュリティ属性であるオブジェクト(ACL テーブル)に関連付けられたユーザーID、役割の改変、削除をアカウント管理者またはシステム構築者に制限する。ただし自分自身の役割とシステム構築者のアカウントの役割の改変は除く。

以上により、**FMT_MSA.1** は、**SF.MGMT** により実現できる。

FMT_MSA.3:

SF.MGMT により、TOE は、セキュリティ属性であるユーザーID に対する役割に対して、役割未設定の制限的初期値を与える。

以上により、**FMT_MSA.3** は、**SF.MGMT** により実現できる。

FMT_MTD.1:

SF.MGMT により、TOE は、利用者ごとのユーザーID(アカウント)、パスワード、ロックステータス、およびセキュリティパラメータを管理する機能を提供する。またユーザーID 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、セキュリティパラメータの問い合わせ、改変、消去を、アカウント管理者およびシステム構築者に制限する。

ただし TOE は、ストレージ管理者に対して、自分自身のパスワードの改変を許可する。

また TOE は、システム構築者のアカウントのユーザーID を登録、削除できない。

以上により、**FMT_MTD.1** は、**SF.MGMT** により実現できる。

FMT_SMF.1:

第 8.2.6 節に示したように、本 ST で選択した機能要件に対して CC パート 2 で規定された管理すべき要件のうち、TOE で管理すべき項目は、**SF.MGMT** で管理している。

以上により、**FMT_SMF.1** は、**SF.MGMT** により実現できる。

FMT_SMR.1:

SF.MGMT により、TOE は、ストレージ管理者、アカウント管理者、システム構築者、の各役割を維持し、各役割と利用者を関連付けて ACL テーブルで管理する。

以上により、**FMT_SMR.1** は、**SF.MGMT** により実現できる。

FIA_UAU.1、FIA_UID.1:

SF.I&A による利用者の識別・認証に成功する以前に、警告バナー機能(**SF.BANNER**)が提供する警告メッセージの通知を除いて、いかなる動作も実行されることはない。

以上により、**FIA_UAU.1**、**FIA_UID.1** は、**SF.I&A** により実現できる。

FIA_SOS.1:

SF.MGMT により、TOE は、アカウントの新規作成およびパスワード登録、改変時に、パスワードが以下の品質尺度を満たすことを検証するメカニズムを提供する。

- セキュリティパラメータで決定されるパスワード最小文字数の条件を満たす。
- パスワードとして使用可能な文字種が英数字、記号であり、かつセキュリティパラメータで決定されるパスワード複雑性条件を満たす。

以上により、**FIA_SOS.1** は、**SF.MGMT** により実現できる。

FIA_ATD.1、FIA_USB.1:

SF.I&A により、TOE は、は識別・認証に成功した利用者のユーザーID、役割を維持・管理し、その利用者を代行するプロセスに対して、そのユーザーID と役割を関連付ける。

以上により、**FIA_ATD.1** は、**SF.I&A** により実現できる。

FIA_AFL.1:

SF.I&A により、TOE は、ストレージ管理ソフトウェアにログインするための利用者の認証において、一定回数連続して認証に失敗したユーザのアカウントをロックする。

以上により **FIA_AFL.1** は、**SF.I&A** により実現できる。

FIA_TAB.1:

SF.BANNER により、TOE 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警告メッセージをストレージ管理ソフトウェアに通知し、ストレージ管理ソフトウェアではユーザの識別・認証を行うためのログイン画面にその警告メッセージを表示する。

以上により、**FIA_TAB.1** は、**SF.BANNER** により実現できる。

FPT_RVM.1:

SF.I&A は、ストレージ管理ソフトウェアからの利用者の識別・認証要求を受け付けたとき、**SF.I&A** が必ず実施されることを保証している。

SF.I&A は、上記の利用者を代行するプロセス(サブジェクト)が、ACL テーブル(オブジェクト)へのアクセスを行う際、アクセス制御が必ず実施されることを保証している。

SF.MGMT は、利用者を代行するプロセス(サブジェクト)が、ACL テーブル(オブジェクト)およびバナー情報ファイル(オブジェクト)へのアクセスを行う際、アクセス制御が必ず実施されることを保証している。

SF.BANNER は、利用者を代行するプロセス(サブジェクト)が、バナー情報ファイル(オブジェクト)へのアクセスを行う際、アクセス制御が必ず実施されることを保証している。

以上により、**FPT_RVM.1** は、**SF.I&A**、**SF.MGMT**、**SF.BANNER** において実現される。

FPT_SEP.1:

SF.I&A は、ログインに成功した利用者を代行するプロセスごとに関連付けられたユーザーID、役割が、許可されたプロセスからのアクセスに制限されるようなセキュリティドメインに分離しているため、ログインに成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

SF.MGMT は、ACL の情報が、許可されたプロセスからのアクセスに制限されるようなセキュリティドメインに分離しているため、識別・認証に成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

また **SF.MGMT** は、バナー情報が、バナー情報ファイル編集機能の使用を許可されたプロセス、および管

理サーバへのログインに成功したシステム構築者からのアクセスに制限されるようなセキュリティドメインに分離しているため、識別・認証に成功した利用者を代行するプロセス以外の信頼できないプロセスから変更されないことを保証する。

以上により、**FPT_SEP.1** は、**SF.I&A**、**SF.MGMT** において実現される。

8.3.2. セキュリティ機能強度根拠

本 TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、**SF.I&A** のトークン生成メカニズム、パスワード照合メカニズム、および **SF.MGMT** のパスワード複雑性チェックメカニズムである。これらのセキュリティ機能強度は、第 6.2 節において、SOF-基本を指定している。一方、この TOE の最小機能強度レベルは第 5.1.2 節において SOF-基本を指定している。従って両者は一貫している。

8.3.3. 保証手段根拠

本節では、セキュリティ保証手段がセキュリティ保証要件に対して必要かつ十分であることを記述する。セキュリティ保証要件とセキュリティ保証手段の対応関係を表 7 に示す。

表 7 より、すべてのセキュリティ保証手段が、何らかのセキュリティ保証要件のために必要であることが示される。また、保証手段(ドキュメント)に記述される内容は、本 ST が規定したセキュリティ保証要件が要求する証拠を網羅する。

従って、本 ST で適用するセキュリティ保証手段によって、セキュリティ保証要件を満たすことができる。

8.4. PP 主張根拠

参照した PP はない。