Hitachi Device Manager Software,
Hitachi Tiered Storage Manager Software

セキュリティターゲット

2017/01/10

Version 1.0.28

株式会社 日立製作所

「Hitachi Device Manager Software,Hitachi Tiered Storage Manager Software セキュリティターゲット」

■ 商標類

- Active Directory は，米国Microsoft Corporation の，米国およびその他の国における登録商標または商標です。
- Microsoft は，米国Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Windows は，米国Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Windows Server は，米国およびその他の国における米国 Microsoft Corp.の商標です。
- Internet Explorer は，米国Microsoft Corporation の米国及びその他の国における登録商標または商標です。
- Java 及びJDK は，Oracle Corporation 及びその子会社，関連会社の米国 及びその他の国における登録商標または商標です。
- Kerberos は，マサチューセッツ工科大学（MIT：Massachusetts Institute of Technology）で開発されたネットワーク認証のプロトコルの名称です。

■ 著作権

「Hitachi Device Manager Software,Hitachi Tiered Storage Manager Software セキュリティターゲット」

－ 目次 －

1. ST 概説

本章では, ST 参照, TOE 参照, TOE 概要, TOE 記述について記述する。

1.1. ST 参照

ST 名称: Hitachi Device Manager Software,Hitachi Tiered Storage Manager Software セキュリティターゲット

バージョン: 1.0.28

識別名: HDvM_HTSM-ST

作成日: 2017 年 01 月 10 日

作成者: 株式会社日立製作所

1.2. TOE 参照

名称: Hitachi Device Manager Software,Hitachi Tiered Storage Manager Software

TOE のバージョン: 8.0.1-02

キーワード: Access Control Device and Systems

開発者: 株式会社日立製作所

1.3. TOE 概要

1.3.1. TOE の種別およびセキュリティ機能

(1) TOE 種別

TOE 種別は Access Control Device and Systems である。

TOE は Hitachi Command Suite シリーズのストレージ管理ソフトウェア Hitachi Device Manager Software(以降, HDvM と略記)と Hitachi Tiered Storage Manager Software(以降, HTSM と略記)である。

Hitachi Command Suite シリーズのストレージ管理ソフトウェアには, HDvM, HTSM, Hitachi Replication Manager Software(以降, HRpM と略記), Hitachi Tuning Manager Software(以降, HTnM と略記), Hitachi Compute Systems Manager(以降, HCSM と略記)等があり, Hitachi Command Suite シリーズは1つの媒体に組み込まれて提供され, その中から必要なソフトウェアを選択してインストールする。

なお, TOE である HDvM と HTSM はセキュリティ機能を共通管理しており, この共通のセキュリティ機能を共通コンポーネント(以降, HBase)と呼ぶ。

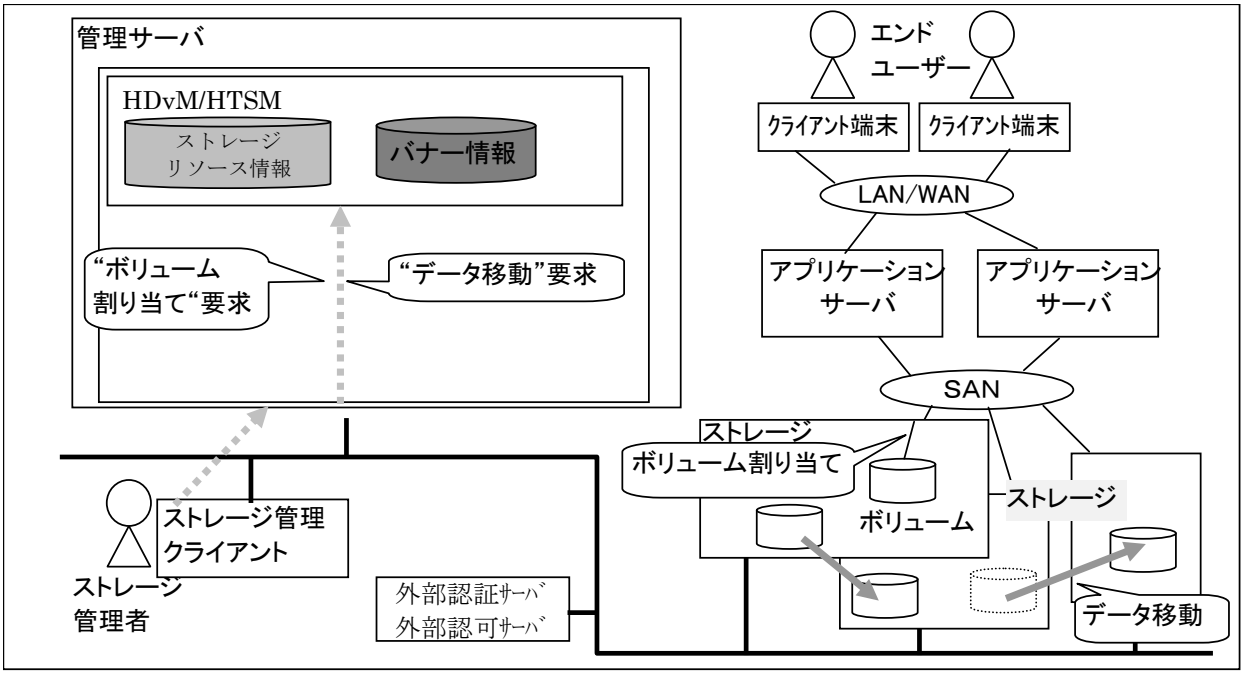


図 1-1 概要図

ストレージシステム(以降, ストレージと略記)は, ストレージの筐体の中に複数のボリュームを有している。さらに, ストレージは, 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, ボリュームの中に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。TOE(HDvM/HTSM)は, ストレージを管理するにあたり, ボリューム割り当て(アプリケーションサーバからストレージのボリュームへアクセスを可能に設定する)等の役割を担っている。

多数のボリュームやストレージを上記のように操作するために, ストレージ管理者は操作対象となる多数のストレージと接続した管理用の機器から, TOE を実行してストレージの一元的な管理を実施する。

図 1-1 においてストレージ管理者は, ストレージ管理クライアントから, 必要なストレージ管理ソフトウェアにアクセスし, ボリューム割り当て等, 必要な操作を要求する。

TOE は, HBase を共通で用いて登録されたリソース情報へのアクセスを制御する機能を提供する。

(2) セキュリティ機能

TOE が提供するセキュリティ機能は以下の通り。

- 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て識別・認証し, その結果に基づきセッションを生成・維持する機能。
- セキュリティ情報管理基盤機能
  アカウント情報の削除, 権限情報の改変・削除, バナー情報の作成・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。
- ストレージリソースアクセス制御機能
  ストレージリソース情報をリソースグループに割り当て, セキュリティ情報管理基盤機能と連携して, ストレー

ジリソース情報への改変を管理する機能。

・ 警告バナー機能
TOE を操作する人物に対する，警告用のメッセージデータを入力・表示する機能。

1.3.2. TOE の構成

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範囲である。TOE を含めたソフトウェア構成図を**図 1-2** に示す。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。

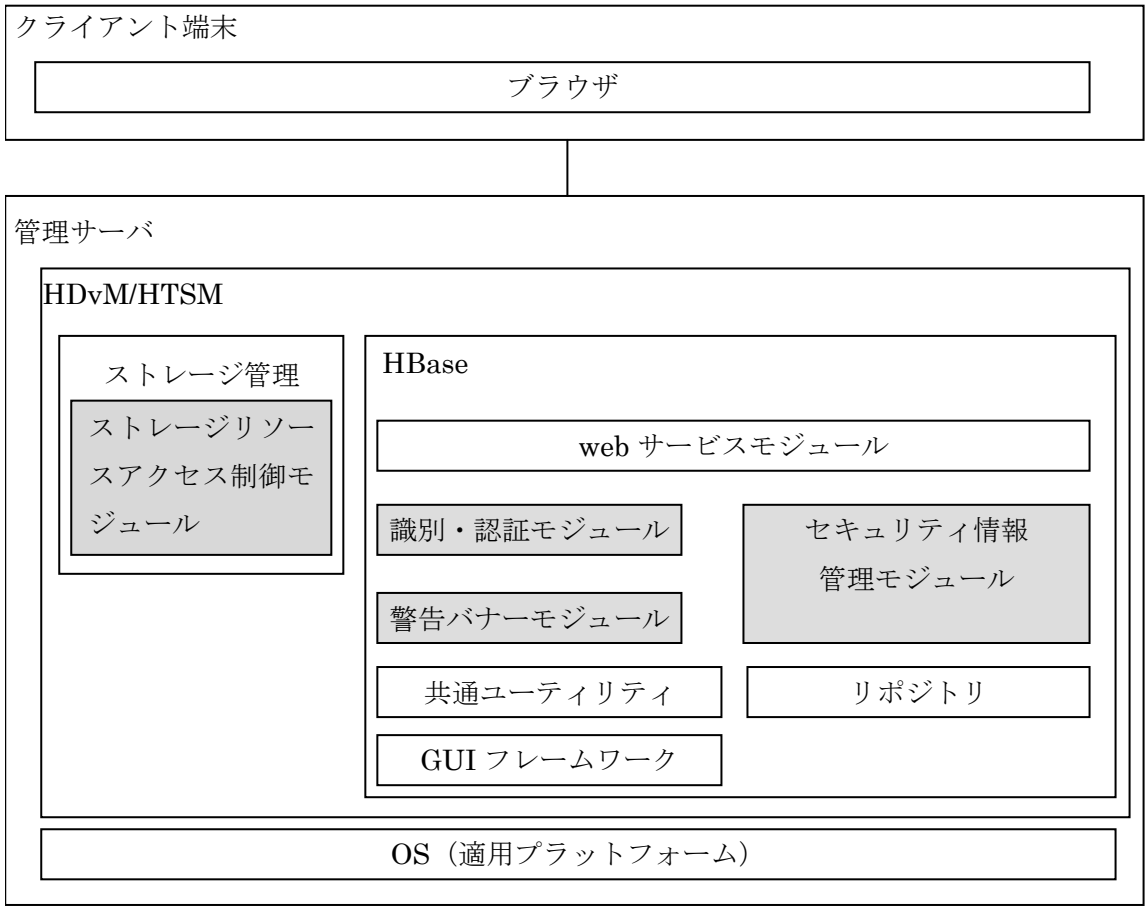


図 1-2 TOE を含めたソフトウェア構成図

- 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基盤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。
- ストレージ管理は，TOE が扱うストレージを管理する機能で，ストレージシステムの環境設定やボリュームの作成等ストレージに関する管理を可能にする。

ストレージリソースアクセス制御モジュールは， TOE が有するストレージリソース情報を HBase のセキュリティ機能(セキュリティ情報管理モジュール)と関連づけ，そのリソースへのアクセスを制御するモジュールである。

1.3.3. TOE の動作環境

1.3.3.1. TOE 運用環境

TOE を利用したシステム構成の一例を**図 1-3** に示す。

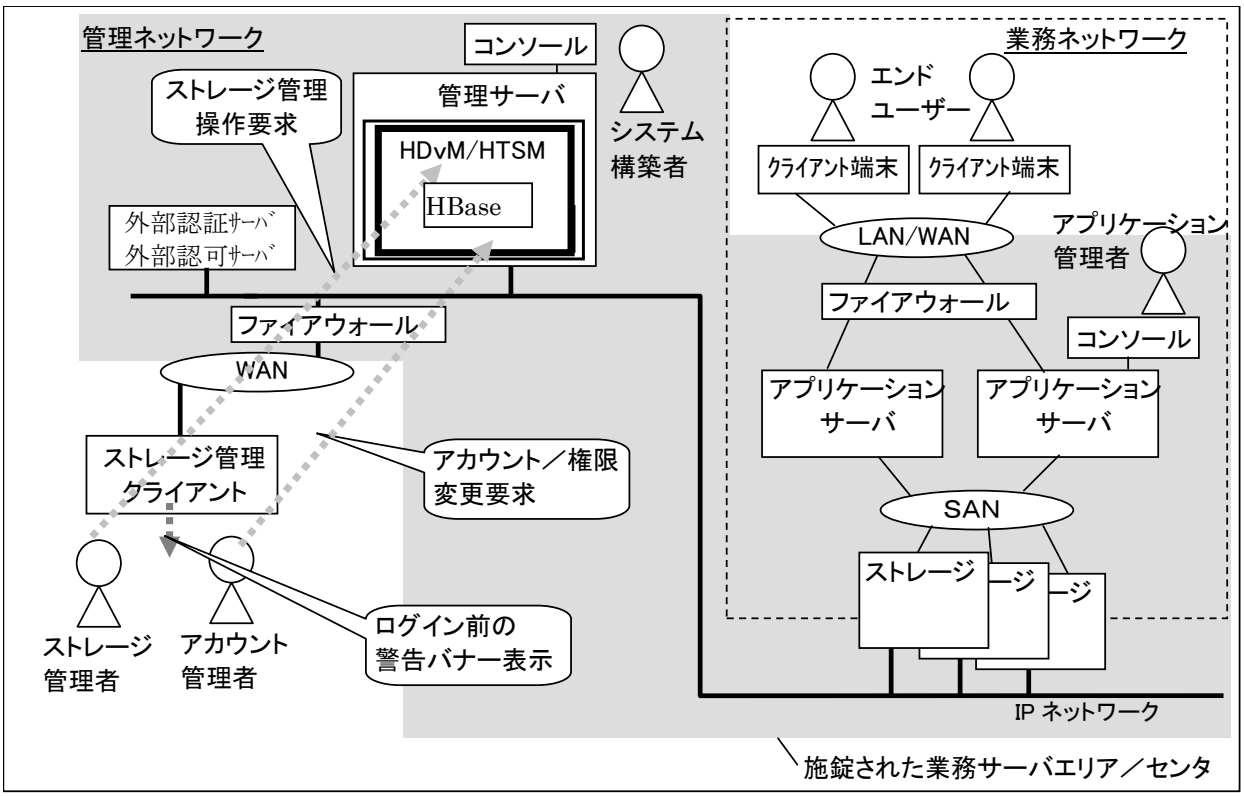


図 1-3 モデル図

図 1-3 では，物理的な配線や装置等は実線で，動作や範囲は点線で示している。また，センタなどの施錠された業務サーバエリアは網かけで示している。

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，業務サーバエリアは，施錠等により入退場が制限されている。

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は，両者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は外部ネットワークと呼ぶ。

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る。また，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る。内部ネットワークは，いずれもファイアウォールによって，外部のネットワークから保護されている。

また，管理ネットワークと業務ネットワークの両方のネットワークに属するストレージは，二つの独立したネットワークカードを搭載しており，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している。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。

ストレージ管理者及びアカウント管理者は，ストレージ管理クライアントを用いて外部ネットワーク経由で TOE にアクセスする。このとき，TOE はログイン画面に警告バナーを常時表示しておくことで，ユーザーを含めた TOE を操作する者に，不正利用に対する警告を喚起する。また，ストレージ管理者及びアカウント管理者は，類推しにくいパスワードを使用して TOE にアクセスする。

図 1-3 では，外部認証サーバ・外部認可サーバを設置している。外部認証サーバは，TOE の識別・認証機能を代行させる場合に利用できる。また，TOE は，外部認可サーバに登録済みのグループ(但し，グループ名は TOE に事前登録しておく)に役割を付与することが出来る。そのグループに属するユーザーは，外部認証サーバで識別・認証に成功することにより，TOE が付与した役割で TOE を使用することが出来る。

外部認証サーバ・外部認可サーバは TOE のサーバと同一の業務サーバエリアに設置されている。但し，両サーバは，異なる業務サーバエリアに設置してもよい。この場合，サーバの間の通信路は秘匿性と完全性が確保されているものとする。逆に，サーバの間の通信路で秘匿性と完全性が確保できない場合，サーバは施錠された同一の業務サーバエリアに設置するものとする。

1.3.4. TOE の評価構成

TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェアは以下のとおりである。

1.3.4.1. ハードウェア条件(TOE をインストールする管理サーバのハードウェア条件)

モデル名:HP Compaq dc7900SF/CT
CPU:Intel Core2 Quad
メモリ:8GB
仮想メモリ:11701MB
HDD:1000GB

1.3.4.2. ソフトウェア条件

(1) ストレージ管理クライアント

Internet Explorer 9 (32bit) on Windows 7 SP1 with Flash Player 14.0

(2) 外部認証サーバ／外部認可サーバ

Microsoft Active Directory(Windows Server 2012 R2 (x64))

(3) 管理サーバ

Windows Server 2012 R2 (x64)

(4) 管理サーバ前提ソフトウェア

Java™ SE Development Kit 8, Update 92

1.4. TOE 記述

1.4.1. TOE の論理的範囲

TOE の機能を**表 1-1** 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 1-1 TOE 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て識別・認証し，その結果に基づきセッションを生成・維持する機能。
セキュリティ情報管理機能	セキュリティ情報管理基盤機能	アカウント情報の削除，権限情報の改変・削除，バナー情報の作成・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。
	ストレージリソースアクセス制御機能	ストレージリソース情報をセキュリティ情報管理基盤機能とくくりつけ，アクセスを制御する機能。
警告バナー機能		TOE を操作する人物に対する，警告用のメッセージデータを入力・表示する機能。
ストレージ管理機能		ストレージシステムの環境設定やボリュームの作成等ストレージに関する管理を可能にする。

(1) 識別・認証機能

ログインする際，識別・認証を行い，ACL テーブルにより導出されたセキュリティ役割が決まる。セキュリティ役割の定義は 1.4.4 を参照のこと。

なお，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 は TOE の利用者のアカウントを自動的にロックする。このとき，識別機能は，TOE 内部の識別機能を利用する。

TOE は，TOE が持つ内部認証機能と， TOE 外にある外部認証サーバが提供する外部認証機能のいずれかを利用できる。アカウント管理者は，アカウント管理者が TOE 内部にアカウントを登録する際，内部認証機能または外部認証機能のどちらを利用するかをアカウント別に設定する。これは，内部認証機能と外部認証機能は独立した機能であり，各アカウントは内部認証機能または外部認証機能のいずれか一方でのみ認証されるためである。なお，この設定は，運用開始後もアカウント管理者によってアカウント別に変更可能である。

外部認証機能を使用する場合，外部認証サーバに登録されているユーザ ID は，TOE 内部にも登録する必要がある。外部認証サーバにのみアカウントを登録しても，そのアカウントは TOE での識別で失敗となる。各アカウントは，アカウント管理者が指定した内部認証機能または外部認証機能のいずれか一方によって認証され，セキュリティ役割を得る。

外部認証グループ連携機能は，TOE 内部で管理している権限情報を，外部認可サーバ上で管理するグループとそのグループに属するアカウントに与える機能である。権限は，TOE が外部認可サーバからグループと

そのグループに属するアカウントの情報を取得した後，TOE 内部で与えられる。なお，外部認証グループ連携機能を使う場合，外部認証機能で識別・認証することが前提となる。

外部認証グループ連携機能では，外部認証サーバに登録されているアカウントは，TOE 内部に登録する必要はない。TOE 内部にユーザ ID とパスワードの登録が無い場合，TOE は外部認証サーバで識別・認証する。そして，外部認証サーバは，外部認証サーバに登録されているユーザ ID とパスワードで識別・認証し，その結果を TOE に返す。TOE は，識別・認証に成功した場合，その結果を元に，外部認可サーバに登録されたグループとそのグループに属するアカウントの情報を問い合わせする。

この外部認証グループ連携機能において，TOE 内部に外部認証サーバと同じユーザ ID が登録されていた場合，TOE 内部のアカウント情報を利用して識別・認証する。（よって，システム構築者のアカウント（system）が外部認証サーバに存在しても，system アカウントは TOE 内部のアカウントが使用される。このため，外部認証サーバに system アカウントを作成しても，システム構築者の権限を得ることはできない）。

外部認証機能または外部認証グループ連携機能を用いた場合，TOE は，TOE に登録されているアカウントまたは外部認証サーバのアカウントを自動的にロックしない。外部認証サーバを使う場合，TOE のアカウント自動ロックと同等の機能を持つ外部認証サーバを利用し，外部認証サーバが不正な連続認証試行によるログインなどの脅威に対抗する。

(2)-1 セキュリティ情報管理基盤機能

TOE は，TOE 内部に登録されたユーザに対し，TOE 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。また，各利用者の「セキュリティ役割」に関連する権限情報も管理する。
TOE は，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している。そして，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。外部認証機能，外部認証グループ連携機能を利用する場合，TOE の上記機能は利用できない。この場合，TOE の持つ上記機能を備えた外部認証サーバを用いることで，不正な連続試行によるログインなどの脅威に対抗する。

TOE は，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。

(2)-2 ストレージリソースアクセス制御機能

ストレージリソース情報をセキュリティ情報管理基盤機能のアカウント情報とくくりつけ，ACL テーブルを作成し，ACL テーブルから導出される TOE 利用者のセキュリティ役割毎にストレージリソース情報へのアクセスを制御する。

(3)警告バナー機能

バナー情報は，システム構築者またはアカウント管理者が，TOE の警告バナーメッセージ編集画面から入力する。また，システム構築者は，TOE のインストールされたマシンにログインし，警告バナー編集コマンドを用いてバナー情報を設定してもよい。バナー情報は，TOE の運用開始前に設定する。

いずれかの方法でバナー情報を設定することによって，設定したバナー情報をログイン画面内に表示する。

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セキュリティ役割を取得する。

●TOE の認証後，取得したセキュリティ役割に合った業務を行う。

1.4.2. TOE の物理的範囲

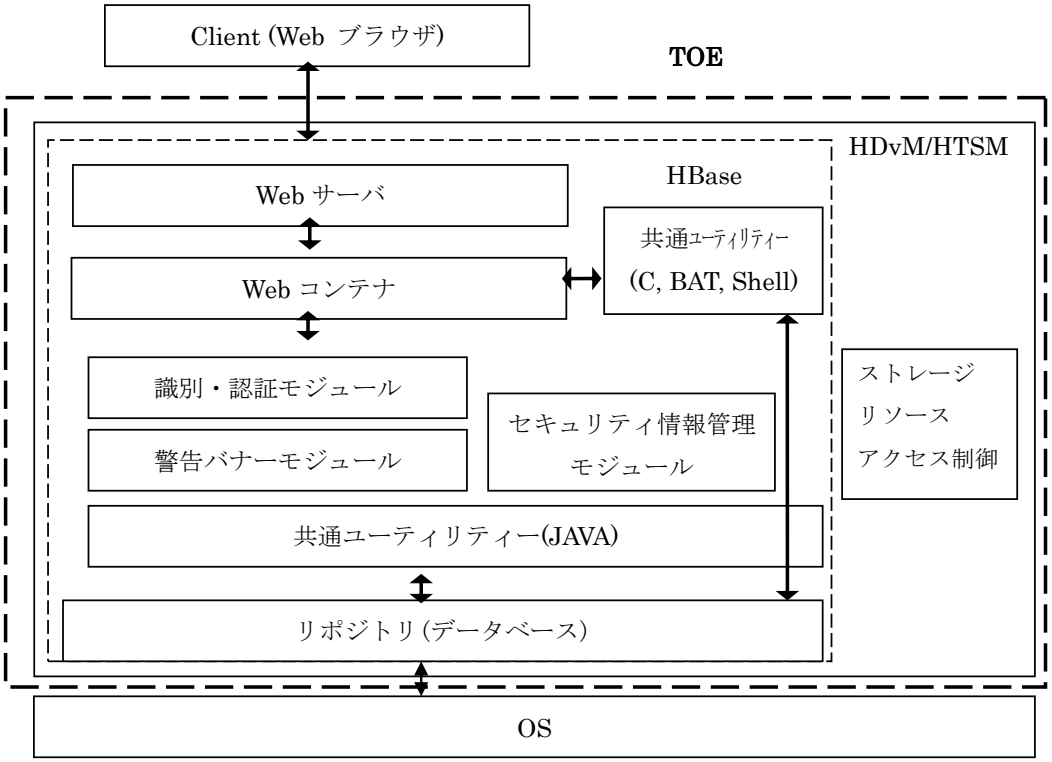


図 1-4 TOE の物理的範囲(外側破線内)

図 1-4 で示した破線のうち, 外側の太い破線で示す範囲が TOE の物理的範囲である。TOE は, 図中に記載する各機能を共通で利用している。

1.4.3. ガイダンス文書

TOE に付属のガイダンス文書は以下の通りである。

- Hitachi Device Manager Software, Hitachi Tiered Storage Manager Software セキュリティガイド
- Hitachi Command Suite インストールガイド（3021-9-006-10）
- Hitachi Command Suite ユーザーズガイド（3021-9-003-10）
- Hitachi Command Suite システム構成ガイド（3021-9-008-10）
- Hitachi Command Suite メッセージ（3021-9-011-10）

1.4.4. TOE の関係利用者役割

本STでは，以下の(1)-(4)の利用者を想定する。利用者は各々の役割を持ち，その役割に従って業務を行う。TOE に認証認可されたプロセスには利用者の役割に相当するセキュリティ役割が割り当てられ，その役割の範囲で操作が可能となる。セキュリティ役割は，システム構築者，アカウント管理者，ストレージ管理者（上位のストレージ管理者を含む）に分類される。セキュリティ役割は，ユーザーID と各操作対象に対する操作権限の組み合わせが定義される ACL テーブルから導出される。

システム構築者は，TOE 上，system アカウントとして認証認可され，TOE の全ての権限を持ち，アカウント管理者やストレージ管理者のセキュリティ役割を導出する ACL テーブルの更新（変更，削除等）ができる。

アカウント管理者は，TOE において，User Management 権限を持ち，アカウント管理者やストレージ管理者のセキュリティ役割を導出する ACL テーブルの更新（変更，削除等）ができる。

ストレージ管理者は，システム構築者，アカウント管理者により設定された各操作対象に対する操作権限の組み合わせの権限を持ち，設定された権限に合わせて業務を遂行できる。ストレージ管理者のアクセス権限管理モデル，およびストレージ管理者のセキュリティ役割は，1.4.4.1，1.4.4.2 にて，説明する。

上位のストレージ管理者は，ストレージシステムの登録や削除，更新や編集等，リソースグループの削除から，ストレージリソース情報への割り当て，割り当て解除権限を合わせて所持する。

また，外部認証サーバ管理者は，TOE が外部認証サーバ・外部認可サーバと連携する際に，TOE 外の外部認証サーバ・外部認可サーバを管理する業務を行う。

(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，アカウント管理者やストレージ管理者のセキュリティ役割の更新（変更，削除等）ができる。
- システム構築者のセキュリティ役割は，システム構築者から他のセキュリティ役割変更されない。
- システム構築者のセキュリティ役割に，他の TOE のセキュリティ役割が追加されることも無い。
- システム構築者は，TOE にて system アカウントとして登録済みであり，TOE の全ての権限を持つ。

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どの権限がそのアカウントに許されるべきかといったアカウントの元となる情報は，職制などの組織情報を元に決定される。アカウント管理者はこの情報を元に権限を付与され，運用業務を行う。
- このため，アカウント管理者やストレージ管理者のセキュリティ役割の更新（変更，削除等）ができる。

- アカウント管理者は上位のストレージ管理者の役割を自分に割り当てることで，上位のストレージ管理者の権限を得ることが可能であり，ユーザーグループへのリソースグループおよびロールの割り当て，ストレージシステムの登録，削除，更新や編集，リソースグループの削除から，ストレージリソース情報への割り当て，割り当て解除まで，ACL テーブルの管理に対する全権を所持することができる。
- アカウント管理者は，TOE において，User Management 権限を持つ。

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：

- 上位のストレージ管理者は，ストレージシステムの登録，削除，更新や編集，リソースグループの削除ができ，ストレージリソース情報への割り当て，割り当て解除を制御できる。
- 通常のストレージ管理者は，システム構築者，上位のストレージ管理者によって設置されたストレージ内のリソースに関し，ボリューム割り当てなどを設定をする。この際，自身に与えられたセキュリティ役割を問い合わせるために権限情報の参照ができる。
- ストレージ管理者は，TOE 上，システム構築者，アカウント管理者の設定する ACL テーブルから導出された操作対象への操作権限の組み合わせを有す。
- ストレージ管理者のセキュリティ役割を導出する ACL テーブルは，ユーザーをグルーピングしたユーザーグループとストレージリソース情報をグルーピングしたリソースグループにロールの関係が定義され，操作対象への操作権限が詳細に設定されている。
- 少なくても，1つのリソースグループに対して Admin，Modify，View，CUSTOM などのストレージの操作に関するロールを持つ。

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。

(4)外部認証サーバ管理者

役割:外部認証サーバ・外部認可サーバに関する管理業務を行う。

権限：

- 業務サーバエリアで外部認証・認可サーバに関する設定をする。
- TOE が外部認証サーバ・外部認可サーバを使用する場合，TOE 内の認証または認可情報を外部認証サーバ・外部認可サーバに設定することができる。

信頼度：自己の業務に対して責任を持っており，自己の業務範囲内で信頼できる。

1.4.4.1. ストレージ管理者のアクセス権限管理モデル

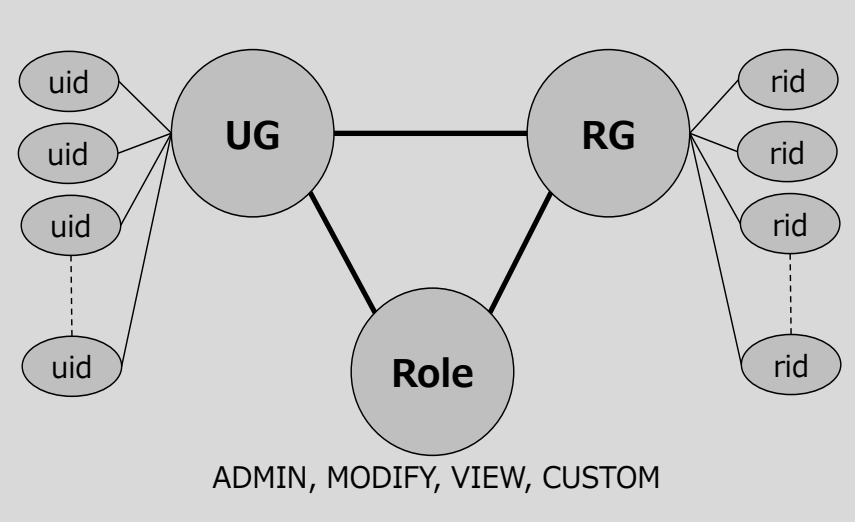


図 1-5 ストレージ管理者のアクセス権限管理モデル

uid: 各ストレージ管理者に割り当てられる識別子。

rid: 各ストレージリソース情報に割り当てられる識別子。

Role:操作権限の組み合わせ

Admin(Role):Admin権限&Modify権限＆View権限の組み合わせ。

Modify(Role): Modify権限＆View権限の組み合わせ。

View(Role): View権限

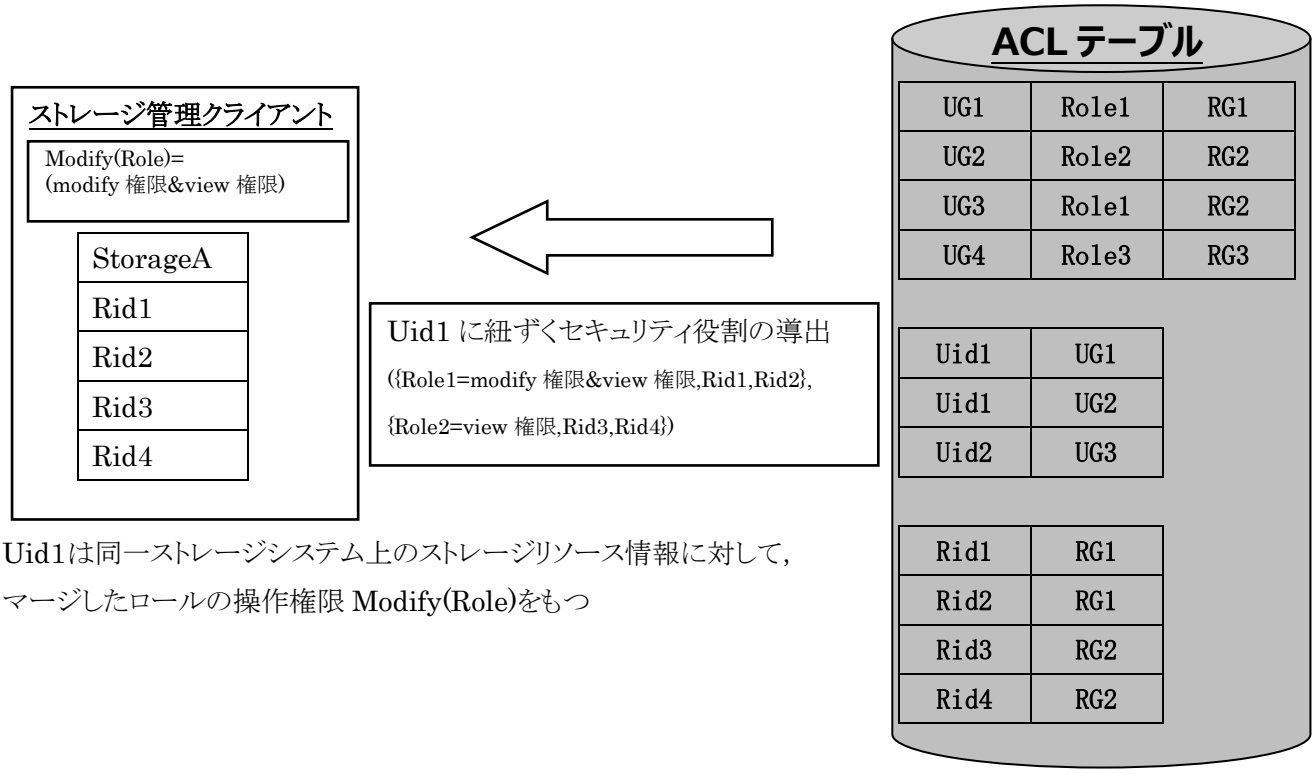
Custom(Role): Admin権限, Modify権限, View 権限よりも細かい操作権限の組み合わせを表現できる。

UG:ユーザーグループ。uid と関連をもつ。また, Role,RG の組み合わせと関連をもつ。

RG:リソースグループ。ストレージリソース情報と関連を持つ。また, Role,UG の組み合わせと関連をもつ。

1.4.4.2. ストレージ管理者のセキュリティ役割説明

ストレージ管理者のアクセス権限管理モデルで構成された ACL テーブルから導出される。TOE ではストレージリソース情報はストレージシステム単位に情報が操作され，ストレージシステム上のリソースに対して，マージされたロールとなる。以下は， UG1，UG2(ユーザーグループ)に属している Uid1(ストレージ管理者に割り当てられる識別子)が，StorageA(ストレージシステム)に関する画面を開いたとき，操作対象の rid1,rid2,rid3,rid4(ストレージリソース情報)に対し，マージしたロールの操作権限 Modify(Role)で操作可能となることを示す。



Uid1は同一ストレージシステム上のストレージリソース情報に対して，
マージしたロールの操作権限 Modify(Role)をもつ

2. 適合主張

2.1. CC 適合主張

本 ST は以下の CC に適合している。

2.1.1. ST が適合主張する CC のバージョン

- パート 1:概説と一般モデル バージョン 3.1 改訂第4版［翻訳第 1.0 版］
- パート 2:セキュリティ機能コンポーネント バージョン 3.1 改訂第4版［翻訳第 1.0 版］
- パート 3:セキュリティ保証コンポーネント バージョン 3.1 改訂第4版［翻訳第 1.0 版］

2.1.2. CC パート2に対する適合

CC パート2適合

2.1.3. CC パート3に対する適合

CC パート3適合

2.2. PP 主張, パッケージ主張

2.2.1. PP 主張

本 ST は PP(プロテクションプロファイル)を適用しない。

2.2.2. パッケージ主張

本 ST の評価保証レベルは EAL2 適合, ALC_FLR.1 を追加する。

3. セキュリティ課題定義

本章では，脅威，前提条件，組織のセキュリティ方針について記述する。

3.1. 脅威

3.1.1. 保護対象資産

TOE は，セキュリティ役割に基づき，ストレージリソース情報，バナー情報へのアクセスを管理する。以下が TOE の保護対象資産である。

●バナー情報

●ストレージリソース情報

3.1.2. 脅威

T.ILLEGAL_ACCESS（不正な接続）

TOE のアカウントを持たない不正な利用者が，ストレージ管理クライアントから，TOE で管理するストレージリソース情報を削除，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。また，TOE のアカウントを持つ不正な利用者が，本来は許可されていない利用者として認識され，ストレージ管理クライアントから，TOE で管理するストレージリソース情報，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，ストレージ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 で管理するストレージリソース情報，バナー情報を削除，改ざんするかもしれない。

3.2. 前提条件

A.PHYSICAL（ハードウェア等の管理）

TOE が動作する管理サーバと周辺機器，TOE が利用する外部認証サーバ・外部認可サーバ，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ものとする。そのエリアに入室を許可される人物はそのエリアに設置されたハードウェア・ソフトウェアの管理者のみであり，その管理者はエリア内に対し悪意を働かない信頼できる人物であるものとする。

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，ファイアウォールなどにより，ストレージ管理クライアントからの通信に制限する。

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，外部認証サーバ管理者は，それぞれに正式に与えられた権限内の操作において，TOE 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に関して，悪意のある操作を行わない。他サーバの管理者は，それぞれに正式に与えられた権限内の操作において，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 が動作する管理サーバとストレージ管理クライアントとの間のネットワーク，TOE が利用する外部認証サーバ・外部認可サーバが異なる業務サーバエリアにある場合，外部認証サーバ・外部認可サーバとTOE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.PASSWORD （パスワードの設定・更新）

アカウント管理者，システム構築者，外部認証サーバ管理者は適切なパスワード複雑性/アカウントロック回数を把握し，適切に設定するものとする。各ストレージ管理者，アカウント管理者，システム構築者，外部認証サーバ管理者は，適切なタイミングでパスワード更新をし，そのパスワードは物理的漏えい(PC 横付箋紙，ショルダーハッキング)，人為的漏えい(更新の怠慢，更新時に同じパスワードにする，個人情報に基づくパスワードや他アプリケーションとのパスワードの使い回し，キャッシュ情報等)により盗まれないようにする。

A.CLIENTS （ストレージ管理クライアント端末の管理）

ストレージ管理クライアント端末には，悪意のあるソフトウェアは存在しない。

A.SRV_MGMT(サーバの管理)

管理サーバは，ストレージ管理クライアントから内部ネットワークに対してTOEを介さずに直接アクセスされることがないように，サーバで実行するサービスやサーバの設定，サーバに登録するアカウントを管理されているものとする。

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，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 のセキュリティ対策方針，運用環境のセキュリティ対策方針，およびセキュリティ対策方針の根拠について記述する。

4.1. TOE の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， TOE で管理する権限情報・ストレージリソース情報にアクセスできるよう，内部認証を使用するように指定されたストレージ管理クライアントの利用者を識別・認証しなければならない。TOE は，内部認証を指定された利用者がアカウント管理者の定めた回数以上連続で認証に失敗した場合，そのアカウントを自動的にロックしなければならない。

O.MGMT

TOE は，各利用者の認証方式，権限情報・ストレージリソース情報，およびバナー情報を設定する手段を提供し，所定のセキュリティ役割を持つストレージ管理クライアントの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しなければならない。

O.BANNER

TOE は，識別認証前に，不正な使用に関する勧告的な警告メッセージを表示しなければならない。

O.PASSWORD

TOE は，内部認証を使用するように指定された利用者に対し，設定されたセキュリティパラメータの値に従って，その利用者のパスワードの登録パターンを制限しなければならない。

4.2. 運用環境のセキュリティ対策方針

4.2.1. 運用により実現するセキュリティ対策方針

OM.SECURE_CHANNEL

TOE が動作する管理サーバとストレージ管理クライアントとの間のネットワーク，TOE が利用する外部認証サーバ・外部認可サーバが異なる業務サーバエリアにある場合，外部認証サーバ・外部認可サーバとTOE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を用い，通信の秘匿性と完全性を確保するネットワークを構築しなければならない。

OM.I&A

外部認証サーバ管理者は，外部認証を使用するように指定された利用者を識別・認証する機能、アカウントロック回数を制限する機能を有する外部認証サーバを用意しなければならない。

OM.PASSWORD_EX

外部認証サーバ管理者は，外部認証を使用するように指定された利用者に対し，適切なパスワード複雑性を制限する機能を有する外部認証サーバを用意しなければならない。

OM.PASSWORD

アカウント管理者，システム構築者，外部認証サーバ管理者は適切なパスワード複雑性/アカウントロック回数を把握し，適切に設定しなければならない。各ストレージ管理者，アカウント管理者，システム構築者，外部認証サーバ管理者は，適切なタイミングでパスワード更新をし，そのパスワードは物理的漏えい(PC 横付箋紙，ショルダーハッキング)，人為的漏えい(更新の怠慢，更新時に同じパスワードにする，個人情報に基づくパスワードや他アプリケーションとのパスワードの使い回し，キャッシュ情報等)により盗まれないようにしなければならない。

OM.PHYSICAL

TOE が動作する管理サーバと周辺機器，TOE が利用する外部認証サーバ・外部認可サーバ，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しなければならない。また，業務サーバエリアに入室を許可される人物は，そのエリアに設置されたハードウェア・ソフトウェアの管理者のみとするよう入退室管理するとともに，エリア内に設置されたハードウェア・ソフトウェアに対し悪意のある行為をしない，信頼できる人物を管理者にするよう人員管理しなければならない。

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，ストレージ管理クライアントからの通信に制限するようファイアウォールを設定し

なければならない。

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，外部認証サーバ管理者，および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しなければならない。

OM.TOE_ACCOUNT

システム構築者，アカウント管理者，外部認証サーバ管理者自身が作成した利用者のパスワードを他人に漏らしてはならない。また，システム構築者，アカウント管理者，外部認証サーバ管理者およびストレージ管理者はパスワードの長さ，またはパスワードに利用する文字種の組み合わせから，推測困難なパスワードを設定しなければならない。

OM.CLIENTS

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 TOE にアクセスするために利用するクライアント端末に悪意のあるソフトウェアがインストールされないよう監視しなければならない。

OM.SRV_MGMT

システム構築者は，ストレージ管理クライアントから内部ネットワークに対して TOE を介さずに直接アクセスされることがないように，管理サーバで実行するサービスや設定，登録するアカウントを管理しなければならない。

4.3. セキュリティ対策方針根拠

セキュリティ対策方針は，セキュリティ課題定義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 4-1** に示す。

表 4-1 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

セキュリティ課題定義 ＼ セキュリティ対策方針	A.PHYSICAL	A.NETWORKS	A.ADMINISTRATORS	A.SECURE_CHANNEL	A.PASSWORD	A.CLIENTS	A.SRV_MGMT	T.ILLEGAL_ACCESS	T.UNAUTHORISED_ACCESS	P.BANNER
O.I&A								○		
O.MGMT								○	○	
O.BANNER										○
O.PASSWORD								○		
OM.I&A								○		
OM.PASSWORD_EX								○		
OM.PHYSICAL	○									
OM.FIREWALL		○								
OM.ADMINISTRATORS			○							
OM.SECURE_CHANNEL				○						
OM.PASSWORD					○					
OM.CLIENTS						○				
OM.SRV_MGMT							○			
OM.TOE_ACCOUNT								○		

表 4-1 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脅威

T.ILLEGAL_ACCESS（不正な接続）

O.I&A，**O.MGMT** および **OM.I&A** により，ストレージ管理クライアントの利用者が TOE にアクセスする際に，所定の権限を持つ利用者によって内部認証を指定された利用者の場合は TOE が単独で，外部認証を指定された利用者の場合は外部認証サーバが，その利用者の識別・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。このとき，**O.PASSWORD** および **OM.PASSWORD_EX** により，TOE および外部認証サーバは，推測されにくいパスワードが設定されるようパスワードの複雑性設定をするとともに，**OM.TOE_ACCOUNT** により，利用者自身も，パスワードの長さ，またはパスワードに利用する文字種の組み合わせから，推測困難なパスワードを設定する。これにより，安全なパスワード管理を実現する。さらに，**O.I&A** ，**OM.I&A** により，TOE が所定の回数以上連続して認証に失敗した利用者のアカウントを自動的にロックすることで，総当りによるパスワード攻撃にも対抗する。

以上により，**T.ILLEGAL_ACCESS** は，**O.I&A** ，**O.MGMT** ，**O.PASSWORD** ，**OM.I&A** ，**OM.PASSWORD_EX**，**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， TOE の利用者に与えられたセキュリティ役割に従って，ストレージ管理クライアントの利用者による権限，ストレージリソース情報，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 が動作する管理サーバと周辺機器，外部認証サーバ・外部認可サーバ，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，そのエリアに入室を許可される人物は，そのエリアに設置されたサーバの管理者のみでありその管理者は，エリア内に設置されたサーバに対し悪意のある行為をしない，信頼できる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，各ネットワークは論理的に分離される。その結果，ストレージ管理クライアントからの通信以外は内部ネットワークに流入しなくなる。

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，外部認証サーバ管理者および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，外部認証サーバ管理者および他サーバの管理者は，それぞれに課せられた TOE 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）

OM.SECURE_CHANNEL により，管理サーバとストレージ管理クライアントとの間，TOE が利用する外部認証サーバ・外部認可サーバが異なる業務サーバエリアにある場合，外部認証サーバ・外部認可サーバと TOE 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，**OM.SECURE_CHANNEL** によって実現できる。

A.PASSWORD （複雑なパスワード）

OM.PASSWORD により，アカウント管理者，システム構築者，外部認証サーバ管理者は，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，適切なパスワード複雑性/アカウントロック回数を把握し，推測困難なパスワードを設定し，認証の繰り返し試行を制限するような設定を行う。ストレージ管理者，アカウント管理者，システム構築者，外部認証サーバ管理者は，適切なタイミングでパスワード更新をし，そのパスワードは物理的漏えい(PC 横付箋紙，ショルダーハッキング)，人為的漏えい(更新の怠慢，更新時に同じパスワードにする，個人情報に基づくパスワードや他アプリケーションとのパスワードの使い回し，キャッシュ情報等)により盗まれないようにする。

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

A.CLIENTS (ストレージクライアントの管理)

OM.CLIENTS により，システム構築者，アカウント管理者は，自身がストレージ管理ソフトウェアにアクセスするために利用するクライアント端末に悪意のあるソフトウェアがインストールされないよう監視する。

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

A.SRV_MGMT(サーバに登録するアカウントの管理)

OM. SRV_MGMTにより，管理サーバで実行するサービス，サーバ設定，サーバに登録するアカウントは管理されており，ストレージ管理クライアントから内部ネットワークに対してTOEを介さない直接アクセスは行われない。

以上により，**A.SRV_MGMT** は，**OM. SRV_MGMT** 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，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もつ。

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

5. 拡張コンポーネント定義

本 ST では，拡張コンポーネントを定義しない。

6. セキュリティ要件

6.1. セキュリティ機能要件

本章では，TOE セキュリティ機能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。

FDP_ACC.1 サブセットアクセス制御

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

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。

[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:ストレージ管理クライアントの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
操作:参照，改変，生成，削除

サブジェクト:ストレージ管理クライアントの利用者を代行するプロセス
オブジェクト:ストレージリソース情報
操作:改変

[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

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

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を決定するために，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，次の追加規則，[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許可する規則*]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許可しなければならない:。

FDP_ACF.1.4 TSF は，次の追加規則，[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。

[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:ストレージ管理クライアントの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セキュリティ役割 オブジェクト属性:なし	ACLアクセス制御SFP
サブジェクト:ストレージ管理クライアントの利用者を代行するプロセス オブジェクト:ストレージリソース情報 サブジェクト属性:サブジェクトに関連付けられたセキュリティ役割 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
ストレージ管理クライアントの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セキュリティ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。
ストレージ管理クライアントの利用者を代行するプロセス	ストレージリソース情報	サブジェクトに関連付けられたセキュリティ役割がストレージリソース情報の改変権限を持つ場合，そのストレージリソース情報に対して改変できる。

[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許可する規則]

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許可する規則
ストレージ管理クライアントの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]
なし

FMT_MSA.1 セキュリティ属性の管理

下位階層: なし

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

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 [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。

上述の割付及び選択を下表に示す。

セキュリティ属性のリスト	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
アカウント管理者のセキュリティ役割(サブジェクトのユーザーID と同一のアカウント管理者を除く)	割付:割り当て, 割り当て解除	アカウント管理者, システム構築者	ACLアクセス制御SFP
ストレージ管理者(上位のストレージ管理者)のセキュリティ役割に関連するユーザーグループ	選択:削除 割付:ユーザーID の割り当て, 割り当て解除	アカウント管理者, システム構築者	ACLアクセス制御SFP

ストレージ管理者のセキュリティ役割に関連するユーザーグループ, ロール, リソースグループの関連	割付:ユーザーグループへのリソースグループの割り当て, 割り当て解除, ロール編集	システム構築者, 自身に上位のストレージ管理者の権限を付与したアカウント管理者	ACLアクセス制御SFP
ストレージ管理者のセキュリティ役割に関連するリソースグループ	選択:削除 割付:ストレージリソース情報の割り当て, 割り当て解除	システム構築者, 上位のストレージ管理者	ACLアクセス制御SFP

FMT_MSA.3 静的属性初期化

下位階層: なし

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_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に対して, [選択: *制限的, 許可的 , [割付 : その他の特性]*:から1つのみ選択]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特定することを許可しなければならない。

[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

[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

依存性: FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

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。

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
ユーザーID(システム構築者を除く)に関連付けられたパスワード	選択:改変 割付:登録	システム構築者, アカウント管理者
	選択:改変	改変対象のユーザーIDであるストレージ管理者
システム構築者に関連付けられたパスワード	選択:改変	システム構築者, アカウント管理者
ストレージ管理者のロックステータス	選択:問い合わせ, 改変	システム構築者, アカウント管理者
システム構築者のロックステータス	選択:問い合わせ, 改変	アカウント管理者
アカウント管理者のロックステータス	選択:問い合わせ, 改変	システム構築者, アカウント管理者 (アカウント管理者自身のロックステータスの改変は除く)
セキュリティパラメータ	選択:問い合わせ, 改変, 消去	システム構築者, アカウント管理者
外部認証・内部認証の選択値	選択:デフォルト値変更, 問い合わせ, 改変	システム構築者, アカウント管理者
ユーザーID(但し, システム構築者のユーザーIDおよびサブジェクトのユーザーID と同一のユーザIDを除く)。	選択:削除	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

依存性: なし

FMT_SMF.1.1 TSF は, 以下の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*]。

[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]

セキュリティ管理機能
システム構築者以外のユーザーID削除機能
ユーザーID(システム構築者を除く)に関連付けられたパスワード登録機能
ユーザーID(システム構築者を除く)に関連付けられたパスワード改変機能
システム構築者に関連付けられたパスワード改変機能
ストレージ管理者のロックステータス問い合わせ機能
ストレージ管理者のロックステータス改変機能
システム構築者のロックステータス問い合わせ機能
システム構築者のロックステータス改変機能
アカウント管理者のロックステータス問い合わせ機能
アカウント管理者のロックステータス改変機能
セキュリティパラメータ問い合わせ機能
セキュリティパラメータ改変機能
セキュリティパラメータ消去機能
外部認証・内部認証の選択値デフォルト値変更機能
外部認証・内部認証の選択値問い合わせ機能
外部認証・内部認証の選択値改変機能
アカウント管理者のセキュリティ役割の割り当て機能
アカウント管理者のセキュリティ役割の割り当て解除機能
ストレージ管理者のセキュリティ役割に関連するユーザーグループ削除機能
ストレージ管理者のセキュリティ役割に関連するユーザーグループへの ユーザーID の割り当て機能
ストレージ管理者のセキュリティ役割に関連するユーザーグループからの ユーザーID の割り当て解除機能
ストレージ管理者のセキュリティ役割に関連するユーザーグループへの リソースグループの割り当て機能
ストレージ管理者のセキュリティ役割に関連するユーザーグループへの リソースグループ関連ロール編集機能

ストレージ管理者のセキュリティ役割に関連するユーザーグループからの リソースグループの割り当て解除機能
ストレージ管理者のセキュリティ役割に関連するリソースグループ削除機能
ストレージ管理者のセキュリティ役割に関連するリソースグループへの ストレージリソース情報の割り当て機能
ストレージ管理者のセキュリティ役割に関連するリソースグループからの ストレージリソース情報の割り当て解除機能

FMT_SMR.1 セキュリティ役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

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。

[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

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSF は, [*詳細化: 利用者*]が認証される前に[*詳細化: 利用者*]を代行して行われる[*割付: TSF 仲介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[*詳細化: 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, [*詳細化: 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。

[割付: TSF 仲介アクションのリスト]

警告バナー機能, ライセンス管理機能(製品バージョン表示機能)

[詳細化: 利用者]

内部認証を使用することを指定されたストレージ管理クライアントの利用者

[詳細化: 各利用者]

内部認証を使用することを指定されたストレージ管理クライアントの各利用者

FIA_UID.1 識別のタイミング

下位階層: なし

依存性: なし

FIA_UID.1.1 TSF は, [*詳細化: 利用者*]が識別される前に[*詳細化: 利用者*]を代行して実行される[*割付: TSF 仲介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[*詳細化: 利用者*]を代行する他の TSF 仲介アクションを許可する前に, [*詳細化: 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。

[割付: TSF *仲介*アクションのリスト]

警告バナー機能, ライセンス管理機能(製品バージョン表示機能)

[詳細化: 利用者]

ストレージ管理クライアントの利用者

[詳細化: 各利用者]

ストレージ管理クライアントの各利用者

FIA_SOS.1 秘密の検証

下位階層: なし

依存性: 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。

[割付: 定義された品質尺度]

最小文字数:セキュリティパラメータで設定された文字数

複雑さ:セキュリティパラメータで設定された複雑さ(英数字、記号の組み合わせ)

FIA_ATD.1 利用者属性定義

下位階層: なし

依存性: 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を維持しなければならない。: [*割付: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]

ユーザーID, セキュリティ役割

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1 TSF は, 以下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, 以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [*割付: 属性の最初の関連付けの規則*]

FIA_USB.1.3 TSFは, 以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない: [*割付: 属性の変更の規則*]

[割付: 利用者セキュリティ属性のリスト]

ユーザ ID, セキュリティ役割

[割付: 属性の最初の関連付けの規則]

利用者	利用者を代行して動作するサブジェクト	利用者セキュリティ属性とその値（属性:値）
システム構築者	システム構築者を代行するプロセス	ユーザ ID:System セキュリティ役割:システム構築者
アカウント管理者	アカウント管理者を代行するプロセス	ユーザ ID:認証されたユーザ ID セキュリティ役割:ユーザ ID に関連付けて登録されているセキュリティ役割
ストレージ管理者	ストレージ管理者を代行するプロセス	ユーザ ID:認証されたユーザ ID セキュリティ役割:ユーザ ID に関連付けて登録されているセキュリティ役割

[割付: 属性の変更の規則]

なし

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

依存性: FIA_UAU.1 認証のタイミング

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[選択:に達する, を上回った]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。

[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 TOE 外部の認証機能を用いた場合は除く)

[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

[選択:に達する, を上回った]
選択:に達する

[割付: アクションのリスト]
アカウントをロックする(但し TOE 外部の認証機能を用いた場合は除く)。

FTA_TAB.1 デフォルト TOE アクセスバナー

下位階層: なし

依存性: 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。

6.2. 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 6-1** に示す。

表 6-1 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	
開発（ADV クラス）	**ADV_FSP.2**	セキュリティ実施機能仕様
	ADV_TDS.1	基本設計
	ADV_ARC.1	セキュリティアーキテクチャ記述
ガイダンス文書（AGD クラス）	**AGD_OPE.1**	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート（ALC クラス）	**ALC_CMC.2**	CM システムの使用
	ALC_CMS.2	TOE の一部の CM 範囲
	ALC_DEL.1	配付手続き
	ALC_FLR.1	基本的な欠陥修正
セキュリティターゲット評価（ASE クラス）	**ASE_CCL.1**	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.2	セキュリティ対策方針
	ASE_REQ.2	派生したセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
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_VAN.2**	脆弱性分析

6.3. セキュリティ要件根拠

TOE が提供するセキュリティ機能要件の根拠を記述する。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。

6.3.1. セキュリティ機能要件根拠

本 ST で選択した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 6-2** に示す。

表 6-2 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
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	○			
FTA_TAB.1			○	

表 6-2 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。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，FIA_UAU.1，FIA_UID.1 により，ストレージ管理クライアントの利用者を識別し，内部認証を使用することを指定されたストレージ管理クライアントの利用者を認証している。このとき TOE は，内部認証を指定された利用者に対しては，**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，利用者のユーザーID とセキュリティ役割を維持しており，**FIA_USB.1** により，識別・認証に成功した利用者を代行するプロセスに対して，そのユーザーID とセキュリティ役割を関連付け

る。

また TOE は，**FMT_MTD.1** により，利用者ごとに登録されているユーザー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。

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

O.MGMT

TOE は，**FDP_ACC.1 FDP_ACF.1 により,** バナー情報ファイル，ストレージリソース情報に対するアクセス制御を実施し，サブジェクトに関連付けられたセキュリティ役割がストレージリソース情報の改変権限を持つ場合，そのストレージリソース情報に対して改変できるように制限している。また，セキュリティ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。**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セキュリティ役割を維持し，**FMT_MSA.1** により，セキュリティ属性であるユーザーID，セキュリティ役割を通常のストレージ管理者が管理できないように制限する。また TOE は，**FMT_MSA.3** により，セキュリティ役割生成時に指定したユーザーID を制限的初期値として与える。

また TOE は，**FMT_MTD.1** により，ユーザーID の削除，利用者の他者パスワード，認証方式（内部認証/外部認証の選択），セキュリティパラメータ，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 **FMT_SMF.1** により，管理項目に示した管理機能を行う能力を持つ。

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** によって実現できる。

O.BANNER

FTA_TAB.1 により，TOE の不正な使用に関する勧告的な警告メッセージを利用者セション確立前(ログイン画面)に表示する。**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。

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

O.PASSWORD

TOE は，**FIA_SOS.1** により，内部認証を利用している利用者の秘密（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。

6.3.2. 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 6-3** に示す。

表 6-3 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 または FDP_IFC.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	○
FTA_TAB.1	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。

6.3.3. 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。

7. TOE 要約仕様

本章では，TOE セキュリティ機能について記述する。

7.1. 識別・認証機能（SF.I&A）

SF.I&Aは，ストレージ管理クライアントの利用者がTOEを利用する際に利用者の識別・認証を行い，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，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，内部認証を指定されたストレージ管理クライアントの利用者の識別・認証を行う。一方で，外部認証を指定されたストレージ管理クライアントの利用者については，TOE外の外部認証サーバを利用して識別・認証を行い，TOE はその結果を外部認証サーバから受け取る。

ストレージ管理クライアントの利用者が，TOE の内部認証機能での識別・認証に成功した場合，または，外部認証サーバでの識別・認証に成功した場合，**SF.I&A** は，利用者を代行するプロセス（サブジェクト）に利用者から入力されたユーザ ID を関連付ける。そして，ACL テーブルへのアクセスを行い，その利用者の役割を取得する。

そして，取得した役割に TOE を利用するためのセキュリティ役割が含まれている場合，以下(3)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，その利用者のアカウントがロック中である場合，または取得した役割に TOE を利用するためのセキュリティ役割が含まれていない場合，**SF.I&A** は GUI を介して，エラーを表示する。

TOE は，**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**）機能やライセンス管理機能(製品バージョン表示機能)を除いて，いかなる動作も実行しない。TOE は，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。

(2)アカウント自動ロック

SF.I&A は，TOE の内部認証機能を利用して，ログインする利用者の識別・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のアカウントを自動的にロックする。アカウントがロックされる期間は無期限である。**SF.MGMT** は，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を設定する。**SF.I&A** は，TOE の内部認証機能を利用する各利用者ごとの認証連続失敗回数を管理しており，TOE の内部認証機能を利用して認証に成功した場合，および TOE の内部認証機能を利用して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。

(3)セッション管理

SF.I&A は，上記の利用者の識別・認証，および必要なセキュリティ役割の取得に成功した場合，その利用者のユーザーID，セキュリティ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 とセキュリティ役割を関連付ける。

GUI 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。

新たな利用者のログイン認証を要求されると，**SF.I&A** は新たにログインする利用者のセッションを生成し識別する。既にログインしている利用者のログイン認証を要求している場合，**SF.I&A** はその利用者に新たなセッションを生成し識別する。すなわち，**SF.I&A** は利用者のログインごとに異なるセッションを生成し利用者を識別するため，同じユーザーが複数回ログインした場合は，そのユーザにログインと同じ回数のセッションを生成し識別する。

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，GUI より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を確認する。

利用者のセッションが有効な場合，**SF.I&A** は GUI に対し，当該利用者に対応付けられたユーザーID，セキュリティ役割を GUI に返信する。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** はエラーを返信する。

SF.MGMT によって利用者のアカウントが削除またはアカウントロックされた場合は，既にログイン済みのアカウントのセッションを無効にし，新たなセッション作成を抑止する。

7.2. セキュリティ情報管理機能(SF.MGMT)

SF.MGMT は, 各利用者の認証方式, アカウント情報, ACL テーブルと, 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, その利用者のセキュリティ役割が付与され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), 認証方式(外部認証/内部認証のいずれか)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, ロックステータスの問い合わせ, 改変, 外部認証・内部認証の選択値のデフォルト値変更, 問い合わせ, 改変の操作を行う手段を提供する。

SF.MGMT は, 削除・登録対象のユーザ ID ではないアカウント管理者およびシステム構築者に対して, 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, ロックステータスの問い合わせ, 改変, 外部認証・内部認証の選択値のデフォルト値変更, 問い合わせ, 改変の操作を許可し, 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, 複数の記号を扱うことが可能であり, 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, 利用者ごとのユーザーID, ACL テーブルを管理する。**SF.MGMT** は, 利用者からの要求に応じてACLテーブルから導出されたセキュリティ役割へのアクセスを行い, 許可された役割に従い, ACLテーブルの登録, 改変, 削除の操作を行う手段を提供する。

SF.MGMT は, ストレージ管理クライアントの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 およびセキュリティ役割に基づいて, 以下のルールに従いACL テーブルに対するアクセスを制御する。

- **SF.MGMT** は, サブジェクトに関連付けられたセキュリティ役割がアカウント管理者, システム構築者の場合, 利用者(ユーザーID)に対するセキュリティ役割を生成, 削除, 改変できる。
  なお, セキュリティ役割の生成はユーザーID を指定して行い, セキュリティ役割生成直後からこの対応関係を維持する。
  また, アカウント管理者およびシステム構築者は, ユーザーIDを指定して対応するセキュリティ役割を削除

するほかに，ユーザーID（アカウント）を削除することにより，対応するセキュリティ役割も削除することができる。

- **SF.MGMT** は，サブジェクトに関連付けられたセキュリティ役割がシステム構築者，アカウント管理者であるプロセスだけがアカウント管理者のセキュリティ役割の割り当て，割り当て解除，または，ストレージ管理者のセキュリティ役割に関連するユーザーグループを削除，ユーザーID の割り当て，割り当て解除できる。
- **SF.MGMT** は，サブジェクトに関連付けられたセキュリティ役割がシステム構築者，アカウント管理者自身に上位のストレージ管理者の権限を付与したプロセスだけが，ストレージ管理者のセキュリティ役割に関連するユーザーグループへのリソースグループの割り当て，割り当て解除，ロール編集ができる。また，システム構築者，上位のストレージ管理者の権限を付与したプロセスだけが，ストレージ管理者のセキュリティ役割に関連するリソースグループの削除，ストレージリソース情報の割り当て，割り当て解除できる。

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。

ACL テーブルの情報は，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 テーブルの情報が，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」の各セキュリティ機能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 7-1** 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 7-1 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きい値	アカウント自動ロック機能において，アカウントを自動的にロック状態にするための認証の連続失敗回数のしきい値。
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，TOE 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，ストレージ管理クライアントの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）に関連付けられたセキュリティ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。

(6)ストレージリソース情報管理

SF.MGMT は，ストレージ管理クライアントの利用者を代行するプロセスがストレージリソース情報の改変を行う際，そのプロセス（サブジェクト）に関連付けられたセキュリティ役割がストレージリソース情報の改変権限を持つの場合，ストレージリソース情報の改変ができる。

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。

7.3. 警告バナー機能（SF.BANNER）

SF.BANNER は，**SF.MGMT** において設定されたバナー情報をストレージ管理クライアントの利用者の識別・認証を行うためのログイン画面に表示する。

7.4. TOE セキュリティ機能要件と TOE セキュリティ機能の対応関係

本節では，TOE セキュリティ機能について記述する。**表 7-2** に示すように，本節で説明するセキュリティ機能は，6.1 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 7-2 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	FTA_TAB.1
SF.I&A								○	○		○	○	○	
SF.MGMT	○	○	○	○	○	○	○			○				
SF.BANNER	○	○												○

FDP_ACC.1：

FDP_ACF.1：

SF.MGMT により，TOE は，ストレージ管理クライアントの利用者を代行して動作するプロセス（サブジェクト）がストレージリソース情報の改変およびバナー情報ファイル（オブジェクト）の改変，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セキュリティ役割でアクセス制御を行う。

SF.BANNER により，TOE は，ストレージ管理クライアントの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，そのバナー情報の参照を許可している。

以上により，**FDP_ACC.1**，**FDP_ACF.1** は， **SF.MGMT**，**SF.BANNER** により実現できる。

FMT_MSA.1：

SF.MGMT により，サブジェクトに関連付けられたセキュリティ役割がシステム構築者，アカウント管理者であるプロセスだけがアカウント管理者のセキュリティ役割の割り当て，割り当て解除，または，ストレージ管理者のセキュリティ役割に関連するユーザーグループを削除，ユーザーID の割り当て，割り当て解除できる。

SF.MGMT により，サブジェクトに関連付けられたセキュリティ役割がシステム構築者，アカウント管理者自身に上位のストレージ管理者の権限を付与したプロセスだけが，ストレージ管理者のセキュリティ役割に関連するユーザーグループへのリソースグループの割り当て，割り当て解除，ロール編集ができる。また，システム構築者，上位のストレージ管理者の権限を付与したプロセスだけが，ストレージ管理者のセキュリティ役割に関連するリソースグループの削除，ストレージリソース情報の割り当て，割り当て解除できる。

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，セキュリティ属性を生成する際に，そのセキュリティ属性を付与する利用者のユーザーID を ACL テーブルのセキュリティ属性であるユーザーID の制限的初期値として与える。

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，内部認証・外部認証の選択，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。TOE は，セキュリティ役割に関連付けられたユーザーID の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，自分自身のユーザーID とシステム構築者のユーザーID の削除は除く。）

また，パスワードの登録，改変，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，内部認証・外部認証の選択値のデフォルト値変更，問い合わせ，改変を，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，自分自身のユーザーID とシステム構築者のロックステータスの改変は除く。）

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：

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（TSF によって提供されるセキュリティ管理機能のリスト）はすべて，7.2 節に示したとおり **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, ACLテーブルで管理することで, ストレージ管理者, アカウント管理者, およびシステム構築者の各役割を維持する。

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 により, 内部認証を指定したストレージ管理クライアントの利用者の識別・認証するTOEは, 識別・認証の前に, 警告バナー機能(**SF.BANNER**)およびライセンス管理機能(製品バージョン表示機能)の参照を許可している。

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, TOE内部におけるアカウント新規作成時のパスワード登録, またはパスワードの改変時に, 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。
- セキュリティパラメータで決定されるパスワードの複雑さ(英数字、記号の組み合わせ)に関する条件を満たす。

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, 各利用者のユーザーID, セキュリティ役割を維持・管理し, 識別・認証に成功したストレージ管理クライアントの利用者を代行するプロセスに対して, そのユーザーIDとセキュリティ役割を関連付ける。

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, 内部認証を指定された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利用者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。

FTA_TAB.1:

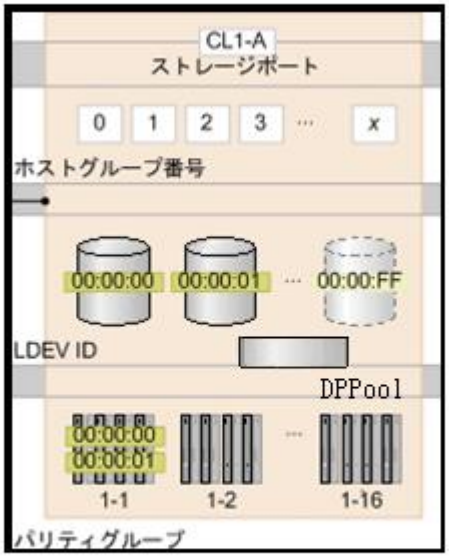
SF.BANNER により, TOEは, TOEの不正な使用に関する勧告的警告メッセージをログイン画面に表示する。

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

8. 用語

本 ST で用いる用語・略語の意味(要約)を**表 8-1** に示す。

表 8-1 用語・略語の意味

用語	意味
SAN	Storage Area Network の略。
バナー情報	警告バナー機能で使用する文面情報である。
ストレージリソース情報	TOE の管理するストレージシステムのリソース情報(ストレージポート, ホストグループ番号, LDEV ID, DP プール, パリティグループ)。以下にて, ストレージシステム上のストレージリソースの概念図を示す。パリティグループは物理的ディスクの配列であり. DP プールやボリュームはパリティグループを論理的なアクセス単位に分割したものである。その際, LDEV ID は, 論理的に分割された識別子として用いられる。また, 物理的なストレージポートに対して, ホストグループ番号は, ボリュームへの I/O を許可されたグループ識別子として用いられる。  ストレージシステム
権限	TOEが許可する操作対象に対する操作の種類を表す。ユーザ情報を管理するUser Management権限, ストレージ情報の参照, 改変, タスクを実行するための Admin,Modify View,CUSTOM(プロビジョニング,,,)権限などがある。

ロール	TOEの権限の組み合わせ。マニュアル上でのストレージ管理者のロールは，Admin=Admin&Modify&Viewの権限の組み合わせのこと。ストレージ管理者のアクセス制御テーブル作成時，ユーザーグループにリソースグループを割り当てる際，ロールを選択して割り当てる。Admin権限は管理権限，Modify権限は編集権限，View権限は参照権限である。特に，すべての操作対象に対してAdmin権限を与えることで，リソースグループやストレージシステムを管理することができる。
ACL テーブル	TOE の ACL を定義するテーブルのこと。 ユーザーID がもつ各操作対象への操作権限を定めるテーブル。
セキュリティ役割	TOE の利用者を代行するプロセスがもつセキュリティ観点で分類した役割。TOE 上のセキュリティ役割には，システム構築者，アカウント管理者，ストレージ管理者の3つの役割があり，TOE 上では役割ごとに可能な操作が制限される。
ユーザーグループ	ユーザーグループは，操作権限が同じストレージ管理者をグルーピングしアカウント管理しやすくしたもの。
リソースグループ	リソースグループは，リソースへのアクセス制御を実施するためにストレージシステム，パリティグループ，LDEV ID，ストレージポートなどの単位で，ストレージリソース情報をグルーピングし，アクセス制御管理をしやすくしたもの。
HBase	Hitachi Command Suite に属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。
HDvM	Hitachi Device Manager Software。 Hitachi Command 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	Hitachi Replication Manager Software。 Hitachi Command 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管理機能を提供する。
HTSM	Hitachi Tiered Storage Manager Software。 Hitachi Command 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。
HTnM	Hitachi Tuning Manager Software。 Hitachi Command Suite の1つであるストレージ管理ソフトウェア。ストレージのリソース利用効率の管理機能を提供する。
HGLM	Hitachi Global Link Manager Hitachi Command Suite の1つであるストレージ管理ソフトウェア。グローバル入出力パス稼働管理機能を提供する。

HCSM	Hitachi Compute Systems Manager Hitachi Command Suite の1つであるストレージ管理ソフトウェア。サーバ管理の効率化とサーバの可用性の向上を支援する。
セキュリティパラメータ	TOE のセキュリティ機能に関連するパラメタ情報。パスワードの文字数やパスワードに使用する文字種別，ログインの連続失敗回数とその閾値，閾値を超えた(アカウントがロックされたか)などの情報。
警告バナー	TOE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。
内部認証	TOE の内部認証機能のみを利用する認証。
外部認証	TOE 内部から，TOE 外部の外部認証サーバ（LDAP ディレクトリサーバ，RADIUS サーバ，Kerberos サーバ）の認証機能を利用する認証方式。
外部認証グループ連携	外部認可サーバに登録された，グループとそのグループに属するアカウントの情報を TOE が取得し，TOE 内部で権限情報を付与する機能。TOE 外部の認証機能を前提とし，アカウントはグループに属していることから，「外部認証グループ連携」と呼ぶ。
ストレージ管理クライアント	ストレージ管理ソフトウェアに通信し，ストレージ管理者等の代行を行うブラウザ等のクライアントプロセス
ストレージ管理クライアント端末	ストレージ管理クライアントのプロセスを実行するマシン