HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target

April 8, 2011

Version 1.03

Hewlett-Packard Company

■ Trademark

- 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。
- Linux は, Linus Torvalds 氏の日本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。
- Red Hat は, 米国およびその他の国で Red Hat, Inc. の登録商標もしくは商標です。
- SUSE は日本における Novell, Inc.の商標です。
- 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。
- Firefox は Mozilla Foundation の登録商標です。

■ Copyright

Table of Contents

1. ST 概説 5
1.1. ST 参照 5
1.2. TOE 参照 5
1.3. TOE 概要 5
1.3.1. TOE の種別およびセキュリティ機能 5
1.3.2. TOE の構成 8
1.3.3. TOE の動作環境 9
1.3.4. TOE の評価構成 11
1.4. TOE 記述 13
1.4.1. TOE の論理的範囲 13
1.4.2. TOE の物理的範囲 16
1.4.3. ガイダンス文書 17
1.4.4. TOE の利用者役割 17
2. 適合主張 18
2.1. CC 適合主張 18
2.1.1. ST が適合主張する CC のバージョン 18
2.1.2. CC パート2に対する適合 18
2.1.3. CC パート3に対する適合 18
2.2. PP 主張, パッケージ主張 18
2.2.1. PP 主張 18
2.2.2. パッケージ主張 18
3. セキュリティ課題定義 18
3.1. 脅威 18
3.1.1. 保護対象資産 18
3.1.2. 脅威 19
3.2. 前提条件 19
3.3. 組織のセキュリティ方針 20
4. セキュリティ対策方針 21
4.1. TOE のセキュリティ対策方針 21
4.2. 運用環境のセキュリティ対策方針 21
4.2.1. IT 環境のセキュリティ対策方針 21
4.2.2. 運用により実現するセキュリティ対策方針 22
4.3. セキュリティ対策方針根拠 23
5. 拡張コンポーネント定義 27

6. セキュリティ要件 28
6.1. セキュリティ機能要件 28
6.2. セキュリティ保証要件 37
6.3. セキュリティ要件根拠 38
6.3.1. セキュリティ機能要件根拠 38
6.3.2. セキュリティ機能要件依存性 40
6.3.3. セキュリティ保証要件根拠 41
7. TOE 要約仕様 42
7.1. 識別・認証機能（**SF.I&A**） 42
7.2. セキュリティ情報管理機能（**SF.MGMT**） 44
7.3. 警告バナー機能（**SF.BANNER**） 46
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 46
8. 用語 50

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: HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Target

バージョン: 1.03

識別名: CVAE-ST-1.03

作成日: April 8, 2011

作成者: Hewlett-Packard Company

1.2. TOE 参照

名称: HP StorageWorks P9000 Command View Advanced Edition Software Common Component

TOE のバージョン: 7.0.1-00

キーワード: ストレージ管理ソフトウェア

開発者: Hewlett-Packard Company

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

本 TOE は, HP StorageWorks P9000 Command View Advanced Edition Software シリーズの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。

評価対象である HP StorageWorks P9000 Command View Advanced Edition Software Common Component(以降, CVAECC 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 HP StorageWorks P9000 Device Manager Software(以降, DevMgr と略記), HP StorageWorks P9000 Replication Manager Software(以降, RepMgr と略記), HP StorageWorks P9000 Tiered Storage Manager Software(以降, TSMgr と略記), HP StorageWorks P9000 Tuning Manager Software (以降, TunMgr と略記)等があり, これらの製品群と CVAECC を総称して HP StorageWorks P9000 Command View Advanced Edition Software と呼ぶ。

CVAECC は HP StorageWorks P9000 Command View Advanced Edition Software 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。

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。情報システムの規模に応じて，ストレージの規模は増加する傾向にある。情報システムを運用するために，ストレージ管理ソフトウェアは，大規模化し容量が増加し続けるストレージを管理する必要がある。すなわち，以下のような操作を適切に実施する必要がある。

- ボリューム割り当て（DevMgr が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可能に設定する等）
- コピー管理（RepMgr が業務データを格納したボリュームのコピーを管理する等）
- データ移動（TSMgr が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）
- 性能監視(TunMgr が SAN やボリュームの利用状況を監視し，効率的なシステム運用を実現する)

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，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ストレージの一元的な管理を実施する。HP StorageWorks P9000 Command View Advanced Edition Software は，上記のストレージを管理するソフトウェア群を提供する。HP StorageWorks P9000 Command View Advanced Edition Software を利用してストレージを管理するシステムの概要を**図 1** に示す。

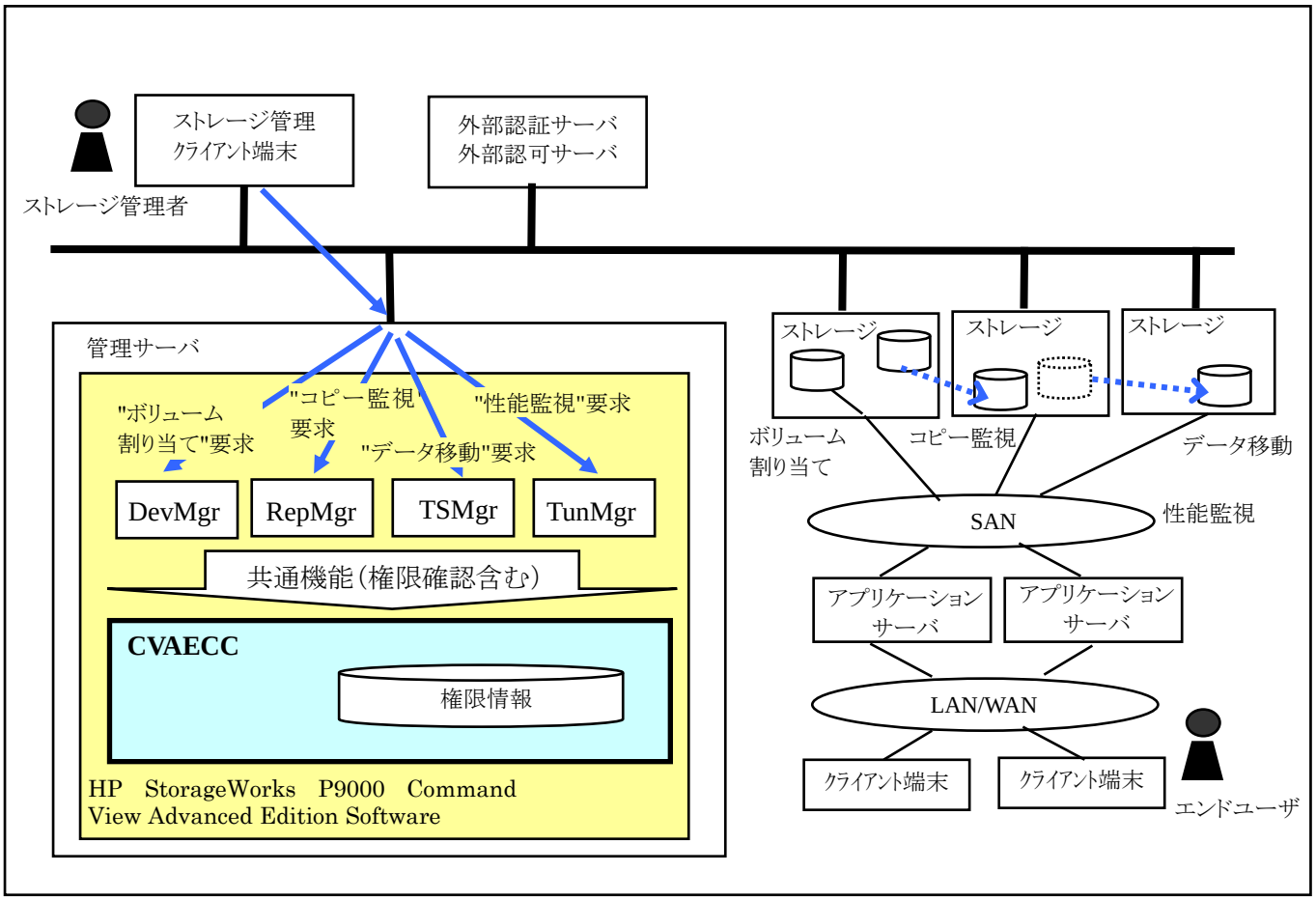

図 1　概要図

図 1においてストレージ管理者は，ストレージ管理クライアント端末から，必要なストレージ管理ソフトウェアにアクセスし，コピー等，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，権限情報の提示，そしてストレージ管理クライアント端末の GUI 表示をするなど，ストレージ管理ソフトウェア群に共通の機能を提供する。

TOE は，これらのストレージ管理要求に先立って識別・認証を行う。そして，TOE は，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のようなストレージ管理操作の要求が正しい権限の範囲で行われるようにするため，権限情報へのアクセスを制御する。

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) 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。また，認証結果に基づいて権限情報を要求元に渡す機能。
- セキュリティ管理機能
  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
  HP StorageWorks P9000 Command View Advanced Edition Software 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 2 に示す。TOE は CVAECC 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。

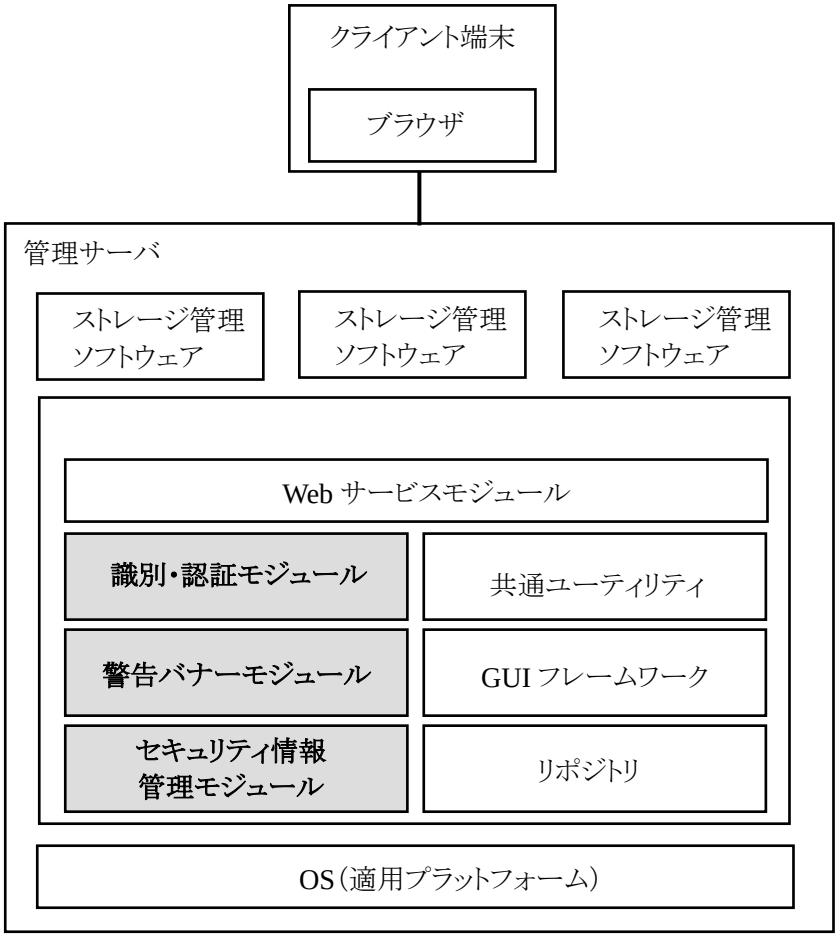

図 2 TOE を含めたソフトウェア構成図

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。

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 3** に示す。

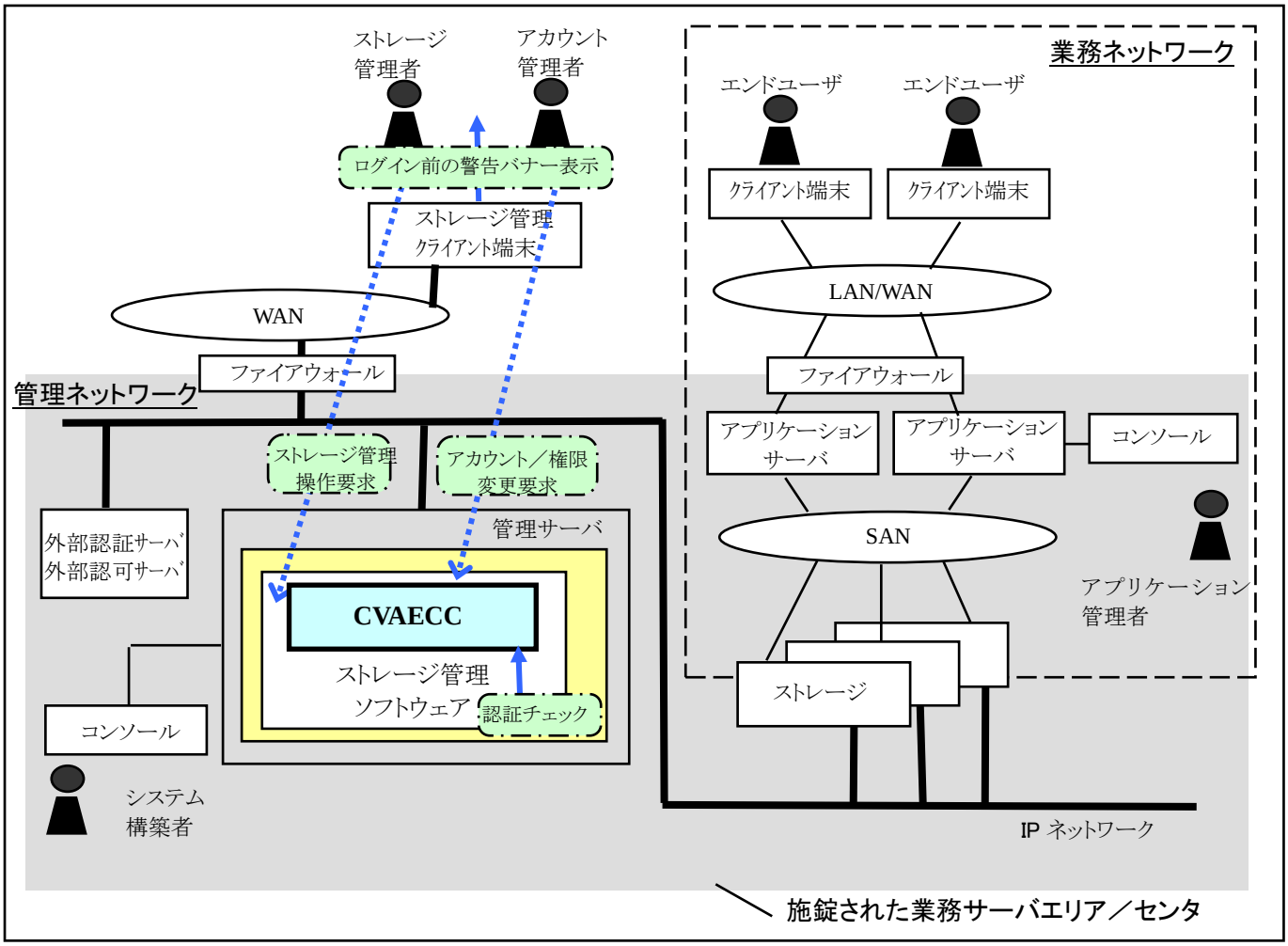

図 3 モデル図

図 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。

また外部と内部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を要求する。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 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)に権限を付与することが出来る。そのグループに属するユーザは，外部認証サーバで識別・認証に成功することにより，TOE が付与した権限でストレージ管理ソフトを使用することが出来る。

外部認証サーバ・外部認可サーバはストレージ管理ソフトウェア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，両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，両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，両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。なお，外部認証サーバと外部認可サーバの設置方法は問わない。具体的には，1. 外部認証サーバと外部認可サーバが物理的に異なる，2. 外部認証サーバと外部認可サーバは物理的に同じサーバで，外部認証サーバと外部認可サーバのソフトウェアが異なる，3. 外部認証サーバと外部認可サーバが物理的に同一のサーバであり，外部認証サーバと外部認可サーバが同一のソフトウェアで実現されているなどの場合がある。

1.3.3.2. ソフトウェア条件

以下に TOE のソフトウェア条件を示す。

(1) 管理サーバ

- Windows 版の HP StorageWorks P9000 Command View Advanced Edition Software Common Component がインストールする Java™VM（Version 1.5.0_11 **以降**）が動作するプラットフォーム。
- Linux 版の HP StorageWorks P9000 Command View Advanced Edition Software Common Component がインストールする Java™VM（Version 1.5.0_05 **以降**）が動作するプラットフォーム。

(2) ストレージ管理クライアント端末

[クライアントの OS が Windows の場合]

・Microsoft Internet Explorer 6.0, 7.0, 8.0

[クライアントの OS が Linux の場合]
・FireFox 3.6.0 以降

(3) 外部認証サーバ／外部認可サーバ
Microsoft Active Directory (Windows Server 2003 シリーズまたは Windows Server 2008 シリーズ付属のもの)

1.3.3.3. ハードウェア条件
以下に TOE のハードウェア条件を示す。
(1)Windows の場合
下記シリーズ中で 1.3.3.2 に示した適用プラットフォーム（Windows）が稼動する機種
HP BladeSystem series, HP ProLiant, Hewlett-Packard, または他社が販売する「PC/AT 互換機」

また, 以下を最小条件とする。
CPU クロック：2GHz
メモリ容量：2GB
ディスク容量：5GB

(2)Linux の場合
下記シリーズ中で 1.3.3.2 に示した適用プラットフォーム（Linux）が稼動する機種
HP BladeSystem series, HP ProLiant, Hewlett-Packard, または他社が販売する「PC/AT 互換機」

また, 以下を最小条件とする。
CPU クロック：2GHz
メモリ容量：2GB
ディスク容量：5GB

1.3.4. TOE の評価構成
1.3.4.1. ハードウェア条件
Windows/Linux 共通：
モデル名：HP Compaq dc7900SF/CT
CPU：Intel Core2 Quad
メモリ：4GB
HDD：1000GB

1.3.4.2. ソフトウェア条件

(1)TOE のバージョン

HP StorageWorks P9000 Command View Advanced Edition Software Common Component 7.0.1-00

(2)TOE を同梱する製品のバージョン

HP StorageWorks P9000 Device Manager Software 7.0.1-00

HP StorageWorks P9000 Replication Manager Software 7.0.1-00

HP StorageWorks P9000 Tiered Storage Manager Software 7.0.1-00

HP StorageWorks P9000 Tuning Manager Software 7.0.0-01

(3) 導入プログラム

- Windows の場合
  - Windows 2008 R2 Server Enterprise Edition
- Linux の場合
  - RedHatEnterpriseLinux Advanced Edition 5 update 4
  - SuSE Linux Enterprise Server 11
- 各 OS 共通で導入したソフトウェア
  - ActiveDirectory (Windows 2008 上のプログラム)
- ブラウザ
  - Windows の場合: Internet Explorer 7
  - Linux の場合:FireFox 3.6.9

1.4. TOE 記述

1.4.1. TOE の論理的範囲

TOE の機能を**表 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 TOE(CVAECC)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。また，認証結果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	HP StorageWorks P9000 Command View Advanced Edition Software 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
共通ユーティリティ	HP StorageWorks P9000 Command View Advanced Edition Software 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	HP StorageWorks P9000 Command View Advanced Edition Software 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	HP StorageWorks P9000 Command View Advanced Edition Software に提供するGUIフレームワーク。
リポジトリ	HP StorageWorks P9000 Command View Advanced Edition Software 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，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が持つ，操作権限の情報である。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の設定・変更する機能の実行を許可する「Modify」や，当該リソースに対して参照する機能の実行のみを許可する「View」などがある。

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，内部認証機能に代えて，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，TOE は，その結果を元に権限情報を応答する。

CVAECC7.0.1-00 では，新たに外部認証グループ連携機能をサポートする。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）セキュリティ情報管理機能

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。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。さらに，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。

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，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，バナー情報を設定し返信する。

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，ストレージ管理ソフト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，TOE は，TOE 利用者の権限・役割に関係なく，設定したバナー情報をストレージ管理ソフトウェアに返信する。そして，各ストレージ管理ソフトウェアは，ログイン画面内にバナー情報を表示する。

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つ。また，ACL は，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 ACL から読み出し，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(認証の機能は，TOE 内部または TOE 外部の機能)を介して TOE のセキュリティ情報管理機能にアクセスし，利用者のアカウント生成・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。しかし，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う。そして，利用者(ストレージ管理者など)が ACL 情報を元に役割に応じた参照，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。

1.4.2. TOE の物理的範囲

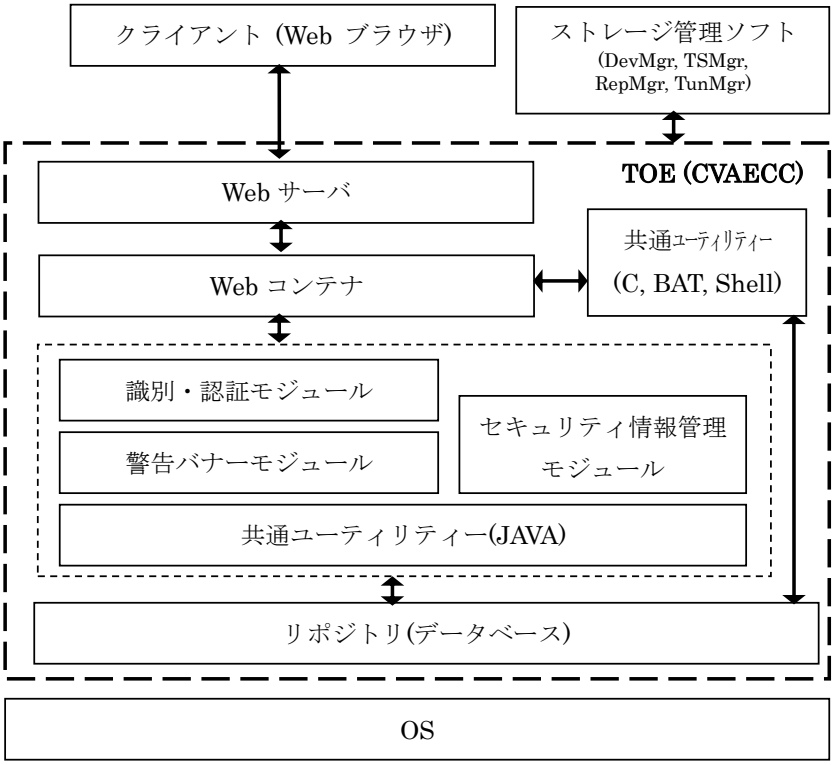

図 4 TOE の物理的範囲(外側破線内)

図 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。これは，TOE の論理的範囲と一致し，TOE は CVAECC そのものである。

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。

- HP StorageWorks P9000 Command View Advanced Edition Software Common Component Security Guide

1.4.4. TOE の利用者役割

本STでは，以下の利用者を想定する。利用者は各々の権限を持ち，そ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，システム構築者の権限は，システム構築者から他の権限に変更されない。また，システム構築者の権限に，他の権限が追加されることも無い。

システム構築者は，TOE において，system アカウントとして登録済みであり，ストレージ管理ソフト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，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。

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: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，ボリューム割り当てなどを設定をする。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。

ストレージ管理者は，TOE において， View，Modify，Execute などのストレージの操作に関する権限を持つ。

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。

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 3 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 3 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 3 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

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。

3.1.2. 脅威

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。

3.2. 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，TOE が利用する外部認証サーバ・外部認可サーバ，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端末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，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，TOE が利用する外部認証サーバ・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.VERSION （TOE と組み合わせて利用可能な製品バージョン）

TOE は，次の製品と組み合わせて利用されるものとする。

DevMgr v5.6.0 以降
TSMgr v5.5.0 以降
RepMgr v5.6.0 以降
TunMgr v7.0.0 以降

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，パスワードは，パスワードの長さ，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ものとする。さらに，認証の試行回数を制限する機能を利用し，無制限に認証が試行されることを防止するものとする。

A.CLIENTS （ストレージ管理クライアントの管理）
ストレージ管理クライアントには，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，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 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，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，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端末の利用者を識別・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 TOE 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，およびバナー情報を参照，設定する手段を提供し，所定の権限を持つストレージ管理クライアント端末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，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. IT 環境のセキュリティ対策方針

OE.SECURE_CHANNEL

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，TOE が利用する外部認証サーバ・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を確保しなければならない。

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たなければならない。

OE.I&A

外部認証サーバは，外部認証を使用するように指定された利用者を識別・認証しなければならない。

OE.PASSWORD

外部認証サーバは，外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長さ，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。

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，TOE が利用する外部認証サーバ・外部認可サーバ，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端末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，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，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のパスワードを他人に漏らしてはならない。また，パスワードの長さ，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，適切な頻度で変更しなければならない。

OM.VERSION

システム構築者は，TOE を次の製品と組み合わせて環境構築しなければならない。

DevMgr v5.6.0 以降
TSMgr v5.5.0 以降
RepMgr v5.6.0 以降
TunMgr v7.0.0 以降

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，パスワードの長さ，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，認証の繰り返し試行を制限するように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しなければならない。

OM.SRV_MGMT

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 2 に示す。

表 2　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.ADMINISTROTORS	A.SECURE_CHANNEL	A.VERSION	A.PASSWORD	A.CLIENTS	A.SRV_MGMT	T.ILLEGAL_ACCESS	T.UNAUTHORISED_ACCESS	P.BANNER
O.I&A									○		
O.MGMT									○	○	
O.BANNER											○
O.PASSWORD									○		
OE.SECURE_CHANNEL				○							
OE.BANNER											○
OE.I&A									○		
OE.PASSWORD									○		
OM.PHYSICAL	○										
OM.FIREWALL		○									
OM.ADMINISTROTORS			○								
OM.TOE_ACCOUNT									○		
OM.VERSION					○						
OM.PASSWORD						○					
OM.CLIENTS							○				
OM.SRV_MGMT								○			

表 2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 **OE.I&A** により，ストレージ管理クライアント端末の利用者が 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，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 **OE.PASSWORD** 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登録パターンを制限するとともに，**OM.TOE_ACCOUNT** により，利用者自身も，パスワードの長さ，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，適切な頻度で変更する上，パスワードを漏えいしない。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** 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**，**OE.I&A**，**OE.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，ストレージ管理クライアント端末の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，外部認証サーバ・外部認可サーバ，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，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端末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，

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，または TOE 外部の認証サーバ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.VERSION（TOE と組み合わせて利用可能な製品バージョン）

OM.VERSION により，システム構築者は，TOE と組み合わせて利用可能なバージョンの製品を用いて環境構築する。

以上により，**A.VERSION** は，**OM.VERSION** 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，パスワードの長さ，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，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。

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，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，管理クライアントから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，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。

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端末の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

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端末の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：ストレージ管理クライアント端末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
ストレージ管理クライアント端末からの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，当該利用者の権限情報を参照できる。
ストレージ管理クライアント端末の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，利用者の権限情報を生成，削除，改変できる。
ストレージ管理クライアント端末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端末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]

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
ストレージ管理クライアント端末の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役割がアカウント管理者の場合でも，当該利用者の権限情報を削除，改変できない。
ストレージ管理クライアント端末の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に対応する権限情報であった場合，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

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

オブジェクトに関連付けられたユーザー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 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

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
システム構築者以外のユーザーID	選択:削除 割付:登録	システム構築者, 削除・登録対象のユーザ ID ではないアカウント管理者
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, 問い合わせ・改変対象のユーザ ID ではないアカウント管理者
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

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]。

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。 b) セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	a) なし(相互に影響を及ぼし得る役割のグループはない。) b) なし(特定の値を引き継ぐための規則はない)
FMT_MSA.3	a) 初期値を特定し得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。 c)セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	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。) c) なし(特定の値を引き継ぐための規則はない)
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，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（セキュリティ属性を変更できない。）
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

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

[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端末の利用者

[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端末の各利用者

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

[詳細化: 利用者]
ストレージ管理クライアント端末の利用者

[詳細化: 各利用者]
ストレージ管理クライアント端末の各利用者

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]
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(但し, TOE 内部の認証機能を用いた場合)

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, 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, 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 役割:ストレージ管理者
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 役割:ユーザ ID に関連付けて登録されている役割
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 役割:ユーザ ID に関連付けて登録されている役割

[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 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	
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 5 に示す。

表 5　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 セキュリティ機能要件 ＼ TOE セキュリティ対策方針	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 5 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, ストレージ管理クライアント端末の利用者が 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, 内部認証を指定された利用者に対して, **FIA_UID.1** によりその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確認している。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_UAU.1**，**FIA_UID.1**，**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，**FMT_MSA.1** により，ACL テーブルのセキュリティ属性であるユーザーID 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_MSA.3** により，権限情報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，利用者の認証方式（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，認証に成功したストレージ管理クライアント端末の利用者の役割（権限情報）を ACL テーブルより取得する際，**FDP_ACC.1**，**FDP_ACF.1** により，その利用者のユーザーID に基づいて，ACL テーブルに対するアクセス制御を行う。さらに TOE は，その利用者が 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，**FDP_ACC.1**，**FDP_ACF.1** により，利用者のユーザーID と前述のアクセス制御を経て取得した役割（権限情報）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

TOE は，**FTA_TAB.1** 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。

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 に示す。

表 6　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端末の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，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端末の利用者の識別・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端末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端末の利用者が，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（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）に対するアクセスを制御する。

- 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 と一致した場合のみ，当該利用者の役割（権限情報）を取得できる。

そして，取得した役割（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（権限情報）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（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（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。

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**）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しない。

TOE は，ストレージ管理ソフトウェアから利用者の識別・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，TOEの内部認証機能を利用してストレージ管理ソフトウェアに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。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，その別セッションの操作へ影響を与えない。

(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（権限情報）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，TOEは**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，新たな利用者のログイン認証を要求している場合，**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。そして，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）等を返信する。

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TOE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 TOEの他のセキュリティ機能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テーブルの権限情報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権限情報を変更しない。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，ログイン時点での権限情報が適用され，ログアウトするまでその権限情報は有効である。

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（権限情報）の情報は，他のあらゆるプロセスからのアクセスによって変更されることはない。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。

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，その利用者の役割（権限情報）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，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，利用者ごとのユーザーID，権限情報との対応を，ACL テーブルとして管理する。**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，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，ストレージ管理クライアント端末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）に対するアクセスを制御する。

- **SF.MGMT** は，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，利用者

(ユーザーID)に対する権限情報を生成, 削除, 改変できる。
なお, 権限情報の生成はユーザーID を指定して行い, 権限情報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権限情報を削除するほかに, ユーザーID(アカウント)を削除することにより, 対応する権限情報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役割がアカウント管理者の場合でも, サブジェクトに関連付けられたユーザーID に対する権限情報を削除, 改変できない。
- **SF.MGMT** は, オブジェクトがシステム構築者(System)に対する権限情報であった場合, この権限情報はどの利用者にも削除, 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 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 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 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, 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, ストレージ管理クライアント端末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)に対するアクセスを制御する。

- 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・認証に成功したストレージ管理クライアント端末の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。

7.3. 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を制御する。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対する勧告的な警告メッセージの文面である。ストレージ管理ソフトウェアは，上記で返信された警告メッセージを，ストレージ管理クライアント端末の利用者の識別・認証を行うためのログイン画面に表示する。

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。

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 8 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 8 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.I&A により, TOE は, ストレージ管理クライアント端末の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を制御する。

SF.MGMTにより, TOEは, ストレージ管理クライアント端末の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(権限情報)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, ストレージ管理クライアント端末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 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。

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, 権限情報を生成する際に, その権限情報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。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, 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 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(**表 3**)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, 各役割を権限情報の形で利用者に関連付けて 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 による内部認証を指定したストレージ管理クライアント端末の利用者の識別・認証に成功する以前に, TOE は, 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することはない。

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, 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。
- 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, 各利用者のユーザーID, 役割(権限情報)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端末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(権限情報)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, 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は利用者の識別・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, **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 9** に示す。

表 9 用語・略語の意味

用語	意味
SAN	Storage Area Network の略。
権限 (権限情報)	TOE がストレージ管理ソフトに許可する操作の種類を表す。ユーザ情報を管理する User Management 権限, ストレージの参照, 改変, タスクを実行するための View, Modify, Execute,権限などがある。各利用者には, これらの各権限または各権限の組み合わせが権限情報として付与される。
ACLテーブル	アカウントとストレージ管理のための権限情報を管理するテーブル
CVAECC	HP StorageWorks P9000 Command View Advanced Edition Software Common Component。 HP StorageWorks P9000 Command View Advanced Edition Software の1つであり, HP StorageWorks P9000 Command View Advanced Edition Software 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。
DevMgr	HP StorageWorks P9000 Device Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Software 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。
RepMgr	HP StorageWorks P9000 Replication Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Software 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。
TSMgr	HP StorageWorks P9000 Tiered Storage Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Software 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。
TunMgr	HP StorageWorks P9000 Tuning Manager Software。 HP StorageWorks P9000 Command View Advanced Edition Software 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。
セキュリティパラメータ	CVAECC 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	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。

内部認証	TOE の内部認証機能のみを利用する認証。CVAECC 6.0.0-01 と同じ認証方式。
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。

Revision of History

No.	Date	Version	Revision
1	2010/12/15	1.00	Initial Version
2	2011/2/8	1.01	評価機関指摘事項の反映
3	2011/3/3	1.02	評価機関指摘事項の反映
4	2011/4/8	1.03	評価機関指摘事項の反映