SR-S Security Software V01.01
セキュリティターゲット

２００７年７月１２日

富士通株式会社

FUJITSU

＜目次＞

FUJITSU

＜表目次＞

＜図目次＞

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語、略語について記述する。

1.1. ST 識別

1.1.1. ST の識別と管理

名称：SR-S Security Software V01.01 セキュリティターゲット

バージョン：第 1.20 版

作成日：2007 年 7 月 12 日

作成者：富士通株式会社

1.1.2. TOE の識別と管理

名称：SR-S Security Software V01.01

バージョン：V01.01

作成者：富士通株式会社

1.1.3. 適用する CC のバージョン

ISO/IEC 15408:2005

補足-0512 適用

1.2. ST 概要

本 ST は､富士通株式会社が提供するセキュリティ製品であるセキュアスイッチ SR-S シリーズ(以下、SR-S と略)のセキュリティ機能について記述している。

対象となる TOE のセキュリティ機能は、上記製品の IEEE802.1X 認証機能における認証失敗時の認証抑止機能とその運用支援機能である。

SR-S は、処理性能やネットワークポートの数の違いにより複数のモデルが提供されている。SR-S に搭載されているソフトウェアは、モデル間で共通のソフトウェアを使用する基本ソフトウェアと、各モデルに依存するハードウェア実装の差異を吸収するハードウェア依存部に大別される。

本 ST で記述する機能は、基本ソフトウェアの機能として実装されている。

1.3. CC 適合

本 ST は、以下を満たしている。

パート 2 適合

パート 3 適合

EAL 4 に ALC_FLR.1 を追加

適合する PP は存在しない

1.4. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 2005 Version 2.3 CCMB-2005-08-003
- Common Methodology for Information Technology Security Evaluation Evaluation Methodology August 2005 Version 2.3
- 情報技術セキュリティ評価のためのコモンクライテリア パート 1：
  概説と一般モデル 2005 年 8 月 バージョン 2.3 CCMB-2005-08-001
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2：
  セキュリティ機能要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-002
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 3：
  セキュリティ保証要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法
  評価方法 2005 年 8 月 バージョン 2.3 CCMB-2005-08-004
  平成 17 年 12 月翻訳第 1.0 版
  独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室
- 補足-0512

1.5. 表記規則、用語、略語

1.5.1. 表記規則

第 3 章の前提条件、脅威、組織のセキュリティ方針、及び、第 4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体**フォントで記述し、続けてその定義を通常フォントで記述する。

第 5 章のセキュリティ機能要件では、操作内容を*イタリック体*フォントで記述する。

同じ機能要件を繰り返す場合は、機能要件名に続けて追番を追記する。コンポーネントの繰り返し時は、「(n)」を、エレメントの繰り返し時は、「[n]」を用いる。

なお、 n には、任意の整数を記載する。

1.5.2. 用語

本 ST で使用する用語を定義する。

■ イーサネットフレーム

イーサネットおいて転送単位となるパケットを示す。

■ 運用管理コマンド

運用支援機能が提供するコマンドの種別を示す。

運用管理コマンドは、装置状態、動作状態、ネットワーク状態の表示／操作、蓄積情報表示／消去などの機能を提供する。

■ 管理コンソール

管理者が TOE の運用支援機能を利用する際に使う機器を示す。

本 ST では、製品のコンソールポートに接続されたパソコンを示す。操作はコマンドで行う。

■ 構成定義コマンド

運用支援機能が提供するコマンドの種別を示す。

構成定義コマンドは、動作情報設定、ネットワーク構成定義などの機能を提供する。

■ コンソールポート

RS-232C の物理インタフェースを示す。

SR-S では、管理コンソールの接続インタフェースとして搭載しており、製品添付の専用ケーブルを使用して接続を行う。

■ スレッド

SR-S の OS により提供されるプログラムが動作するための実行環境を示す。本 ST で記述する TOE はスレッドとして動作する。

■ ネットワーク機器

IEEE802.3 の物理インタフェースを持ち、SR-S に接続可能な機器の総称を示す。

■ ネットワークセグメント

VLAN において LAN 上の端末を仮想的にグループ化した集合体を示す。または、IP アドレスの付与体系が同じネットワークの集合体を示す。

■ ネットワークポート（ポート）

IEEE802.3 の物理インタフェースを示す。ネットワークポートは番号により識別可能である。本 ST では、ネットワークポートをポートと略して記す。

■ ハードウェア制御プログラム（ドライバ）

基本制御プログラムにより管理され、SR-S に実装されているハードウェア（シリアル、LAN の各物理インタフェース）の制御を行うプログラムを示す。

■ ポートアクセス制御

Supplicant が接続されたポートからのデータを特定のネットワークセグメント内のみに通過させる情報フロー制御機能を示す。

■ AAA 機能

AAA は、Authentication(認証)、Authorization(認可)、Accounting(課金)の略語である。それぞれ認証情報、認証した利用者に対するリソースへのアクセス権限、監査証跡や接続料金請求のために利用者が実行した事象や日時を記録することを意味する。AAA 機能は、認証・認可・課金の機能を持つことを示す。また AAA データは、認証・認可・課金に関するデータを示す。

■ EAP

Extensible Authentication Protocol の略語である。PPP を拡張して追加的なユーザー認証方法に対応するようにしたプロトコルを示す。リモートアクセスによるユーザー認証の際に用いられる。IEEE802.1X が採用し同規格にもとづいた認証プロトコルである。

■ IEEE802.1X

ネットワーク機器に接続する端末に対し認証を行い、アクセス制御を行う規格を示す。

■ RADIUS (Remote Authentication Dial In User Service)

ネットワーク利用者の認証と利用記録を一元的に行うためのプロトコルを示す。RADIUS サーバは、データベースに収容されたユーザー情報に基づいて接続の許可/不許可の認証を実施、接続の記録を取る AAA 機能を持つ。

■ Supplicant(サプリカント)

RADIUS により認証を実施する場合に、認証を依頼する利用者のサーバまたはクライアント等の端末を示す。

■ VLAN(Virtual LAN)

LAN において、LAN ケーブルやコンピュータなどの物理的な接続形態にかかわらず、LAN 上の端末を仮想的にグループ化する機能を示す。

■ VLAN-ID

VLAN において、グループを識別する番号を示す。

1.5.3. 略語

本 ST で使用する略語を定義する。

- CC ：Common Criteria
- EAL：Evaluation Assurance Level
- IT ：Information Technology
- PP ：Protection Profile
- SFP：Security Function Policy
- SOF：Strength Of Function
- ST ：Security Target
- TOE：Target Of Evaluation
- TSF：TOE Security Functions

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE 構成、TOE の機能、及び保護対象となる資産について記述する。

2.1. TOE 種別

TOE は、AAA 機能と連携する IEEE802.1X 認証機能により、高度なセキュリティを実現するセキュアスイッチの機能である。TOE の種別は、ネットワーク環境においてネットワークセグメントを保護する機能と、その運用支援機能を提供するソフトウェアである。

2.2. TOE 概要

2.2.1. TOE の利用目的

SR-S は、IEEE802.1X 認証機能により、攻撃者が不正に Supplicant をネットワークに接続し、ネットワーク上の利用者の資源への攻撃を防止する。IEEE802.1X 認証機能は、Supplicant との接続インタフェースを持つ SR-S と AAA 機能を持つ RADIUS サーバとの連携により行われる。

TOE は、SR-S における IEEE802.1X 認証機能の Supplicant 接続時の識別認証におけるブルートフォース攻撃や辞書攻撃を防止する機能とその運用支援機能を持つ。これらの機能によりセキュリティを確保したネットワークの運用と管理を行うことができる。

2.2.2. TOE の利用環境

TOE を搭載する SR-S は、ネットワークセグメントの境界に設置する、それぞれのネットワークセグメントを接続するスイッチである。管理者及び利用者が TOE を利用するためには、図 2.1 に示すネットワーク環境が必要となる。管理者は管理コンソールから利用する。利用者は Supplicant を SR-S のポートに接続して、ネットワークセグメントの資源を利用する。

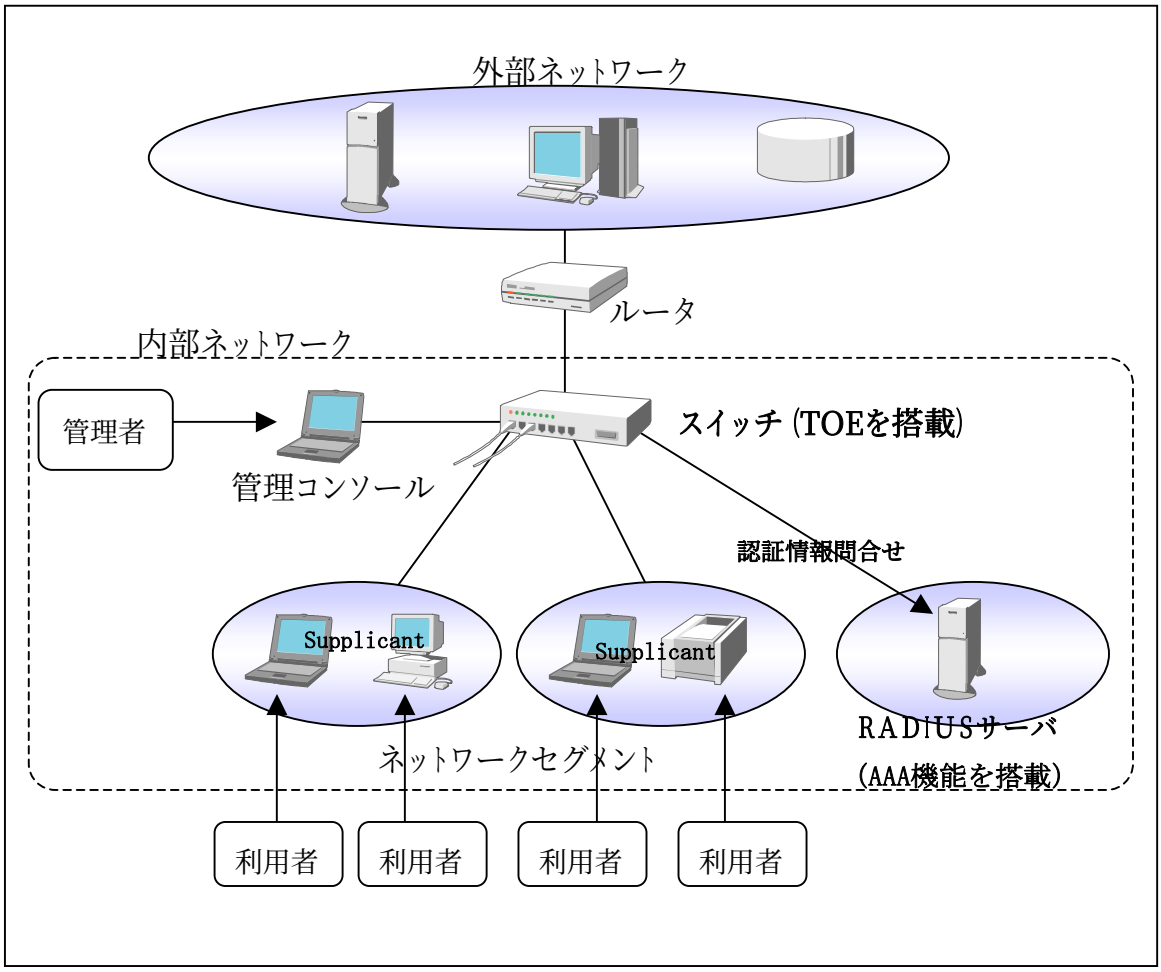

図 2.1 TOE の利用環境の概要

以下に、図 2.1 の項目の説明を以下に述べる。

■ ルータ

異なるネットワークセグメント間の境界に設置する機器であり、利用者が使用する機器を接続する内部ネットワークインタフェースと、他のネットワークセグメントに接続される外部ネットワークインタフェースを持っている。

■ スイッチ

異なるネットワークセグメント間の境界に位置する機器であり、利用者が使用する機器を接続する内部ネットワークを複数のネットワークセグメントに分割する機能を持つ。SR-S は本装置に該当する。TOE は SR-S に搭載され動作する。

■ 管理コンソール

管理者が、運用支援機能を使用する機器であり、TOE とはコンソールポートで接続されている。

■ RADIUS サーバ

IEEE802.1X 認証機能で使用する認証情報を格納する AAA 機能を持つサーバである。RADIUS サーバは、Supplicant からの認証情報の妥当性に関する問合せに応答する。認証が成功すると、RADIUS サーバは、SR-S に接続する Supplicant がアクセス可能なネットワークセグメントの VLAN-ID を本 TOE に通知する。

RADIUS サーバは、内部ネットワークに設置する必要がある。RADIUS サーバと SR-S は、共通の鍵である RADIUS シークレットをそれぞれ設定することにより、RADIUS サーバと SR-S の相互の認証及び通信データの完全性を保証することが可能である。

■ Supplicant

SR-S に接続する利用者のサーバまたはクライアント等の端末である。AAA 機能により Supplicant の識別認証が成功した場合、SR-S は Supplicant のポートアクセス制御を行う。ポートアクセス制御は、Supplicant が接続されたポートからのデータを特定のネットワークセグメント内のみに通過させる情報フロー制御機能である。この機能により、ネットワークを論理的に分離可能となる。

ここで、SR-S のポートにリピータを接続し、リピータに複数の Supplicant を接続するネットワーク構成では、認証された Supplicant の MAC アドレスを他の認証されていない Supplicant が成りすますことによりネットワークセグメントへのアクセスが可能となる。そのため、安全な運用を行うためには、１つのポートに複数の Supplicant を接続させないネットワーク構成で使用する必要がある。

2.2.3. TOE の関連者と利用方法

TOE の関連者と、その役割と許可された操作内容を以下に示す。

関連者	役割に許可された操作内容	利用方法
組織の責任者	SR-S を運用する組織の責任者である。組織の責任者は、SR-S に対する管理行為は行わず、信頼できる人物を管理者として、任命する。	ー
管理者	管理者権限を有し、スイッチの構成変更/運用操作のすべての運用操作が可能である。	管理者が TOE を利用するには、管理コンソールからログイン操作を行う必要がある。認証が成功すると、コマンド入力が可能となり運用支援機能の利用が可能となる。
利用者	SR-S に Supplicant を接続して、ネットワークを利用する者である。	利用者が TOE を利用するには、運用前に AAA 機能に識別認証情報と、接続する Supplicant がアクセスするネットワークセグメントの VLAN-ID を設定する必要がある。 ネットワークセグメントに Supplicant を接続する際に、TOE の認証機能によるアクセス許可後に運用前に指定したネットワークセグメントの利用が可能となる。

2.3. TOE 構成

2.3.1. TOE の物理的構成

SR-S の物理的構成を図 2.2 に示す。TOE の範囲と境界は図中の破線で囲まれた部分である。

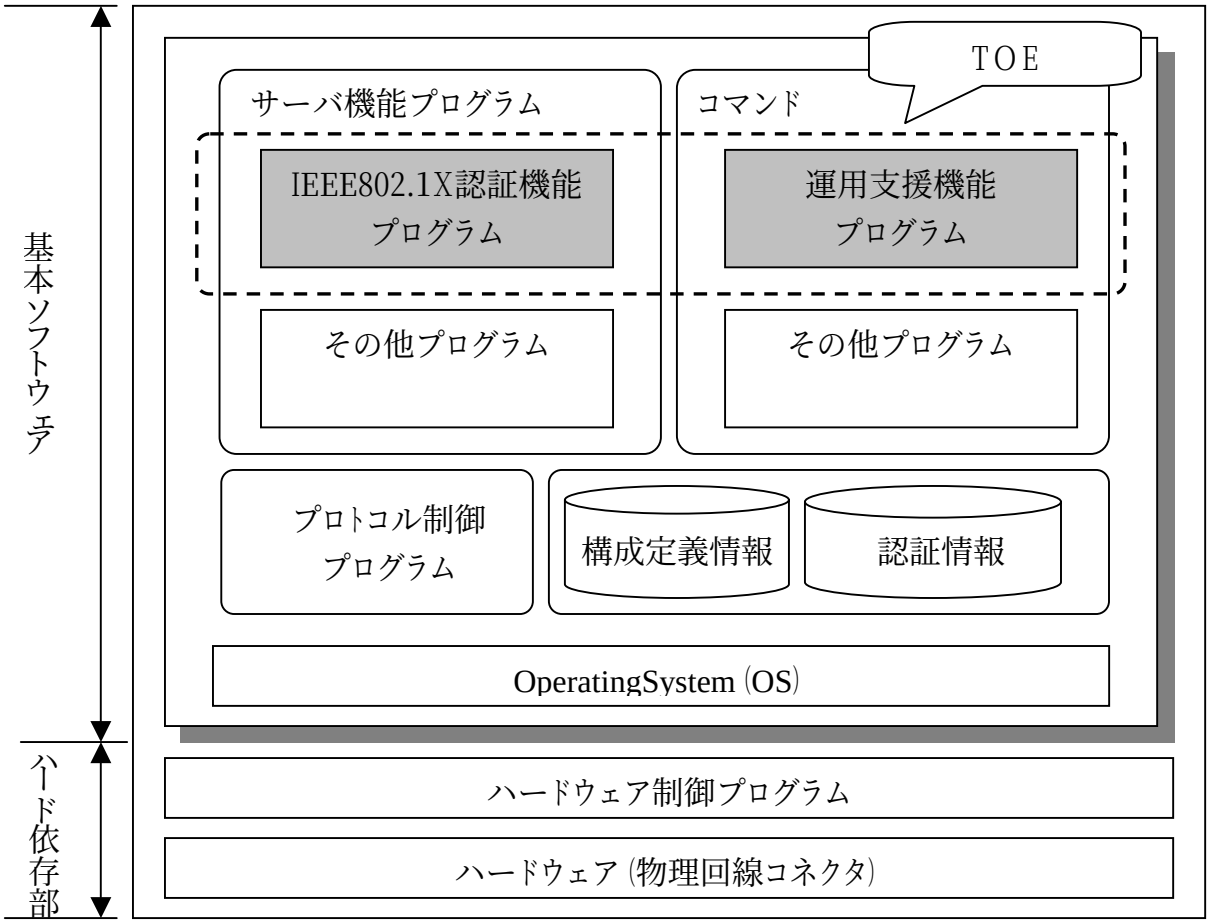

図 2.2 TOE の物理的構成

図 2.2 の TOE の物理的構成における構成要素の説明を以下に示す。

■ サーバ機能プログラムの IEEE802.1X 認証機能プログラム

サーバ機能プログラムは SR-S が提供するサーバ機能のプログラム群である。プログラム群の中で TOE は IEEE802.1X 認証機能を制御するプログラムである。このプログラムは、利用者の Supplicant 接続時の識別認証情報を受信し、AAA 機能に識別認証を依頼する。識別認証が成功した場合は、利用者が利用可能なネットワークセグメントの VLAN-ID をハードウェア制御プログラム(VLAN を制御するプログラム)に設定する。

TOE は、認証が成功した状態を以下の事象が発生するまで有効とする。

- Supplicant がポートから外されてリンクダウンを検出
- 利用者によるログオフ操作
- タイマーによる再認証間隔時間が経過

■ コマンドの運用支援機能プログラム

コマンドは SR-S が提供する機能の運用支援を実施するプログラム群である。プログラム群の中で TOE は IEEE802.1X 認証機能プログラムが動作するために必要な TSF データと、IT 環境のセキュリティ機能に関する制御データの管理を行うプログラムである。管理者は、管理コンソールを SR-S のコンソールポートに接続して利用するか、SR-S の TELNET サーバ機能または SSH ログインサーバ機能によりネットワークから利用する。

また、機能の運用支援を実施するプログラムには、コマンドの他にサーバ機能プログラムの HTTP サーバ機能プログラムによるネットワークから実施する方法もある。

IT 環境の物理的構成要素を以下に示す。また、表 2.1 に IT 環境として TOE が動作する際に必要なソフトウェアを示す。

■ サーバ機能プログラムのその他プログラム

サーバ機能プログラムには、TOE の IEEE802.1X 認証機能プログラム以外のプログラムも含まれる。IEEE802.1X 認証機能プログラム以外のプログラムの一覧を表 2.2 に示す。

■ コマンドのその他プログラム

コマンドには TOE 以外のサーバ機能プログラム、プロトコル制御プログラム及びハードウェア制御プログラムを運用支援するプログラムがある。

■ プロトコル制御プログラム

データリンク層、インターネット層のプロトコルを制御するプログラムである。ポートから一定回数のリンクダウンを検出すると、ポートを閉塞する機能を持つ。また、閉塞されたポートを開放する機能も持つ。

■ Operating System (OS)

本装置全体を制御するプログラムである。サーバ機能プログラム、プロトコル制御プログラム及びコマンドが正しく動作するよう制御を行う。

■ ハードウェア制御プログラム

OS から制御され、ハードウェアの制御を行うプログラムである。SR-S のモデル別で異なっているハードウェアの非互換部分を吸収している。VLAN 機能は、ハードウェア制御プログラムに含まれる。

■ ハードウェア(物理回線コネクタ)

本 TOE が動作するハードウェア装置である。

表 2.1 TOE の運用に必要なソフトウェア

名称	内容
Safeauthor	富士通製の AAA 機能を持つ RADIUS サーバである。 TOE は Safeauthor Version3.5 で動作保証されている。 利用者が IEEE802.1X 認証機能の利用の際に利用者の識別認証を行う。

表 2.2 サーバ機能のプログラム一覧

	名称
1	FTP プログラム
2	TELNET サーバ機能プログラム
3	ProxyDNS プログラム
4	DHCP プログラム
5	syslog プログラム
6	マルチキャストプログラム
7	TIME/SNTP プログラム
8	SNMP プログラム

9	動的定義反映プログラム
10	スケジュール制御プログラム
11	ループ検出プログラム
12	ダンプスイッチ制御プログラム
13	Web 認証プログラム
14	MAC アドレス認証プログラム
15	AAA 制御プログラム
16	ルーティング制御プログラム
17	IGMP スヌーププログラム
18	STP 制御プログラム
19	LACP 制御プログラム
20	HTTP サーバ機能プログラム

TOE である「SR-S Security Software V01.01」は、SR-S724TC1 に基本ソフトウェア V10.01 を搭載した環境で検証を行った。

2.3.2. TOE の論理的構成

表 2.3 に IEEE802.1X 認証機能の一覧を示す。TOE のセキュリティ機能には TOE 欄に”○“を示し、IT 環境で行う機能には“IT 環境”を示している。

表 2.3 IEEE802.1X 認証機能の構成一覧と TOE 対象

	名称	TOE
1	Supplicant の識別認証機能	IT 環境(AAA 機能)
2	IEEE802.1X 認証失敗時のアクセスの抑止機能	○
3	ポートアクセス制御機能	IT 環境(VLAN 機能)
4	運用支援機能	○

表 2.3 の IT 環境の説明を以下に説明する。

■ AAA 機能

AAA 機能は、IEEE802.1X 認証機能で使用する認証情報を格納し、本 TOE からの認証情報の妥当性の問合せに応答する機能である。 認証が成功すると、SR-S に接続する Supplicant がアクセス可能なネットワークセグメントの VLAN-ID を TOE に通知する機能を持つ。

■ VLAN 機能

VLAN 機能は、ハードウェア制御プログラムの一部であり、AAA 機能による認証が成功した場合に VLAN-ID により Supplicant がアクセス可能なネットワークセグメントを制限する機能を持つ。

2.4. TOE のセキュリティ機能

IEEE802.1X 認証機能は外部に接続した AAA 機能によって認証を行う機能である。SR-S では、IEEE802.1X の規格 に準拠した認証機能をサポートしている。IEEE802.1X 認証機能は、構成定義情報を参照して動作し、認証方式「EAP-MD5」、「EAP-TLS」、「EAP-TTLS」、「PEAP」に対応している。

本 TOE では、IEEE802.1X 認証機能における以下の機能を提供する。

(1) IEEE802.1X 認証失敗時のアクセスの抑止機能

Supplicant の AAA 機能による識別認証にて、パスワード、証明書の誤りを検出し、設定する抑止時間の間、Supplicant からのアクセスを抑止する機能である。TOE は、本機能により識別認証機能へのブルートフォース攻撃や辞書攻撃を防止する。

(2) 運用支援機能

運用支援機能は、管理者のみに以下の IEEE802.1X 認証機能の管理行為を行う能力を提供する。

- IEEE802.1X 認証機能の有効機能
- IEEE802.1X 認証機能の認証方式の設定機能
- IEEE802.1X 認証機能の認証失敗時におけるアクセス抑止中の状態の解除機能

運用支援機能は、管理者のみに TSF データの以下の管理行為を行う能力を提供する。

- 管理者のパスワード変更と退避

・ IEEE802.1X 認証機能の認証失敗時におけるアクセスの抑止時間の変更

管理コンソールから管理者が TSF データを操作する前に、運用支援機能は管理者の識別認証を実施する。識別認証はユーザー名とパスワードにより実施する。パスワードの情報を以下に示す。

・ パスワードのフィードバックは非表示
・ パスワードの構成文字種は ASCII 文字 (0x21,0x23～0x7e)
・ パスワードの文字列長は、1 文字以上、64 文字以下

利用者 ID には管理者以外に保守用と一般ユーザ用のものがある。保守用の利用者 ID のパスワードは固定値であるため、安全な運用を行うためには保守用の利用者 ID を無効化にする設定が必要である。また、一般ユーザ用のものも管理者への権限上昇が可能な機能を有するので、安全な運用を行うためには一般ユーザ用の利用者 ID を無効化する設定が必要である。

また、運用支援機能は、以下の機能のふるまいを管理者に制限する機能も提供する。

・ CE 保守ログインの可否
・ 一般ユーザログインの可否
・ TELNET サーバ機能
・ SSH ログインサーバ機能
・ HTTP サーバ機能
・ FTP サーバ機能
・ SSH FTP サーバ機能
・ RADIUS シークレット
・ リンクダウン検出時のポートの閉塞機能
・ 閉塞したポートの開放機能

2.5. 資産

TOE に関係する資産には、以下のものがある。

2.5.1. 内部ネットワーク資産

内部ネットワーク資産とは、Supplicant からアクセスされる可能性がある内部ネットワーク上の内部セキュリティポリシーによって特定される資産である。内部セキュリティポリシーは、内部ネットワークを統合的に管理するシステム運用管理部門によって定められ

る。

2.5.2. TOE 関連資産

TOE 関連資産には以下のものがある。

- 管理コンソールにおける認証情報(パスワード)
- IEEE802.1X 認証失敗時のアクセスの抑止機能に関する情報

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

本節では、TOE が動作する前提条件を示す。

■ A.TRUST(管理者の前提)

管理者は、役割に課せられた責務に責任を持ち、不正な行為を行わないものとする。

■ A.SUPPLICANT(Supplicant の認証情報の前提)

利用者は、Supplicant の認証情報には十分な強度を持つものを使用する。例えば、認証方式が EAP-MD5 の場合は、8 文字以上のパスワードを使用する。

■ A.PORT(IEEE802.1X 認証方式の前提)

TOE を搭載する SR-S では、IEEE802.1X 認証の機能を有効とし、IEEE802.1X 認証方式として物理ポート単位での認証 (ポートベース認証)を設定し、MAC アドレス単位での認証 (MAC ベース認証)は使用しない。

■ A.QUIETPERIOD(IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間の前提)

TOE を搭載する SR-S では、IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間には 60 秒以上の値を使用する。

■ A.SECRET(RADIUS シークレットの前提)

RADIUS サーバと TOE を搭載する SR-S に設定する RADIUS シークレットには十分な強度を持つものを使用する。例えば、8 文字以上の RADIUS シークレットを使用する。

■ A.SERVICE(提供するサービスの前提)

TOE が動作する SR-S は、以下に示すリモートからの運用支援機能のサービス及びファイル転送サービスを使用しない。

- TELNET サーバ機能
- SSH ログインサーバ機能
- HTTP サーバ機能
- FTP サーバ機能

- SSH FTP サーバ機能

■ A.NETWORK(ネットワーク構成の前提)

TOE が動作する SR-S は、認証済み Supplicant の成りすましや通信データの盗聴、及び管理者以外による電源断ができないネットワーク構成で運用する。例えば下記の対策を実施する。

- １つのポートには１つの Supplicant とするネットワーク構成とする。
- SR-S を管理者以外に電源断されないように物理的に保護する。

■ A.PASSWORD(管理コンソールの識別認証におけるパスワードの前提)

管理コンソールの識別認証に使用する管理者のパスワードには十分な強度を持つものを使用する。例えば、8 文字以上のパスワードを使用する。

■ A.CONSOLE(管理コンソール使用時の前提)

TOE が動作する SR-S は、管理コンソールの使用を管理者の利用者 ID のみ可能とし、保守用と一般ユーザ用の利用者 ID による使用はしない。

3.2. 脅威

本節では、TOE に対する脅威を示す。

■ T.NET_CONNECT (不正なネットワークセグメントへの接続)

管理者及び利用者以外の者が機器をネットワークに接続し、SR-S を経由してアクセスするネットワーク上のサーバ、クライアントの利用者の資産を攻撃する脅威である。

3.3. 組織のセキュリティ方針

TOE が従わなければならない組織のセキュリティ方針はない。

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、環境の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

本節では、脅威に対抗するための TOE のセキュリティ対策方針を示す。

- O.NET_AUT（IEEE802.1X 認証失敗時のアクセスの抑止機能）
  TOE は、AAA 機能の識別認証において、識別認証失敗時に Supplicant からのアクセスを一定間隔抑止する。

- O.TSF_MNG（運用支援機能）
  TOE は、TSF の動作に係わるデータと操作、及び TSF の動作に係わる IT 環境の機能のデータと操作を管理者のみに可能とする。

4.2. 環境のセキュリティ対策方針

本節では、前提条件を満足し、脅威及び組織のセキュリティ方針に対する TOE セキュリティ対策方針を支援するための環境のセキュリティ対策方針を示す。

- OE.NET_ID&AUT（機器のネットワーク接続時の識別認証）
  IT 環境である AAA 機能は、Supplicant がネットワークに接続する場合には識別と認証を実施し、接続を許可されていない者の接続要求を却下する。

- OE.LINKDOWN(リンクダウン検出時のポートの閉塞)
  IT 環境である SR-S のプロトコル制御プログラムは、リンクダウンを一定回数検出時にポートを閉塞する機能を持つ。ポートを閉塞する機能を有効とし、リンクダウンを一定回数検出した場合は、Supplicant のポートへの接続を却下する。

- OE.RADIUS(RADIUS サーバ接続時の識別認証)
  IT 環境である SR-S の AAA 制御プログラムは、RADIUS サーバが SR-S と接続する場合には識別と認証を実施し、接続が許可されていない RADIUS サーバの接続を却下する。

- OE.TRUST
  組織の責任者は、管理者のロールに課せられた責務に責任を持ち、不正な行為を行

わない者を管理者に任命する。

■ OE.SUPPLICANT

管理者は、利用者に Supplicant の認証情報には十分な強度を持つものを使用させる。例えば、認証方式が EAP-MD5 の場合は、8 文字以上のパスワードを使用させる。

■ OE.SECRET

管理者は、RADIUS サーバと TOE を搭載する SR-S に設定する RADIUS シークレットには十分な強度を持つものを使用する。例えば、8 文字以上の RADIUS シークレットを使用する。

■ OE.PORT

管理者は、TOE を搭載する SR-S では、IEEE802.1X 認証の機能を有効とし、IEEE802.1X 認証方式として物理ポート単位での認証（ポートベース認証）を使用させ、MAC アドレス単位での認証（MAC ベース認証）は使用させない設定にする。

■ OE.QUIETPERIOD

管理者は、TOE を搭載する SR-S に設定する IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間には 60 秒以上の値を使用する。

■ OE.SERVICE

管理者は、TOE が動作する SR-S の以下に示すリモートからの運用支援機能を提供するサービス及びファイル転送サービスを使用させない設定にする。

- TELNET サーバ機能
- SSH ログインサーバ機能
- HTTP サーバ機能
- FTP サーバ機能
- SSH FTP サーバ機能

■ OE.NETWORK

管理者は、TOE が動作する SR-S において、認証済み Supplicant の成りすましや通信データの盗聴、及び管理者以外による電源断ができないネットワーク構成で運用する。例えば下記の対策を実施する。

- １つのポートには１つの Supplicant とするネットワーク構成とする。
- 管理者以外に SR-S を電源断されないように SR-S を物理的に保護する。

■ OE.PASSWORD

管理者は、TOE が動作する SR-S の管理コンソールの識別認証に使用するパスワードには十分な強度を持つものを使用する。例えば、8 文字以上のパスワードを使用する。

■ OE.CONSOLE

管理者は、管理コンソールの使用を管理者の利用者 ID のみとし、保守用と一般ユーザ用の利用者 ID による使用を不可とする設定にする。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件、IT 環境に対するセキュリティ要件、セキュリティ機能強度を記述する。

5.1. TOE のセキュリティ要件

本節では、TOE が満たすべき IT セキュリティ要件の詳細について記述する。

5.1.1. TOE セキュリティ機能要件

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。

[割付: *認証事象のリスト*]
Supplicant の認証

［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」］]
[割付:*正の整数値*]
１回

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。

[割付: *アクションのリスト*]
Supplicantの次の認証を60～600秒の範囲で認証要求を抑止する。抑止が解除されるのは、下記の事象が発生した場合である。

- 指定された時間が経過した場合
- 管理者がポートまたは Supplicant の認証状態を初期状態に変更した場合

依存性: FIA_UAU.1 認証のタイミング

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。

[割付: *定義された品質尺度*]
運用支援機能を使用する管理者のパスワードに設定可能な文字は、以下の基準を満たす。

- パスワードの構成文字種は、ASCII 文字（0x21, 0x23～0x7e）

依存性: なし

FIA_UID.2(1) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1

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

依存性: なし

FIA_UAU.2(1) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1

TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に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

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

FIA_UAU.7.1

TSF は、認証を行っている間、[割付: *フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付: *フィードバックのリスト*]
・パスワードの表示は行わない。

依存性: FIA_UAU.1 認証のタイミング

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1

TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]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。

[割付: *機能のリスト*]

- IEEE802.1X 認証機能における認証失敗時のアクセスの抑止機能
- CE 保守ログインの可否の動作設定機能
- 一般ユーザログインの可否の動作設定機能

[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]

機能	操作
IEEE802.1X 認証機能における認証失敗時のアクセスの抑止機能	を停止する
CE 保守ログインの可否の動作設定機能 一般ユーザログインの可否の動作設定機能	のふるまいを決定する

[割付: *許可された識別された役割*]

・管理者

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 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。

[割付: *TSF データのリスト*]

- IEEE802.1X 認証機能における認証失敗時のアクセスの抑止時間
- 運用支援機能における管理者の認証情報

[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*]]

データ	操作
IEEE802.1X 認証機能における認証失敗時のアクセスの抑止時間	改変
運用支援機能における管理者の認証情報	改変、問い合わせ

[割付:*許可された識別された役割*]

・管理者

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_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*]。

[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*]

- IEEE802.1X 認証機能における認証失敗時のアクセスの抑止機能の動作設定機能
- IEEE802.1X 認証機能における認証失敗時のアクセス抑止時間の改変機能
- 運用支援機能における管理者の認証情報の改変機能
- 運用支援機能における管理者の認証情報の問い合わせ機能
- CE 保守ログインの可否の動作設定機能
- 一般ユーザログインの可否の動作設定機能

依存性： 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。

[割付: *許可された識別された役割*]

・管理者

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

FDP_ACC.1 サブセットアクセス制御方針

下位階層：なし

FDP_ACC.1.1

TOE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＞
管理者を代行するTOEのスレッド

＜オブジェクト＞
- TELNET サーバ機能プログラム
- SSH ログインサーバ機能プログラム
- HTTP サーバ機能プログラム
- FTP サーバ機能プログラム
- SSH FTP サーバ機能プログラム
- RADIUS シークレット機能プログラム
- リンクダウン検出時のポートの閉塞機能プログラム
- 閉塞したポートの開放機能プログラム

＜SFPで扱われるサブジェクトとオブジェクト間の操作＞
- TELNET サーバ機能プログラムの起動指示
- SSH ログインサーバ機能プログラムの起動指示
- HTTP サーバ機能プログラムの起動指示
- FTP サーバ機能プログラムの起動指示
- SSH FTP サーバ機能プログラムの起動指示
- RADIUS シークレット機能プログラムの起動指示
- リンクダウン検出時のポートの閉塞機能プログラムの起動指示
- 閉塞したポートの開放機能プログラムの起動指示

［割付：アクセス制御SFP］

IT 環境機能の制御ルール設定 SFP

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層：なし

FDP_ACF.1.1

TOE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。

[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*]

サブジェクト	SFP関連の属性	SFP関連セキュリティ属性の名前付けされたグループ
TOEのスレッド	管理者権限	無し

オブジェクト	SFP関連の属性	SFP関連セキュリティ属性の名前付けされたグループ
TELNET サーバ機能プログラム	無し	無し
SSH ログインサーバ機能プログラム		
HTTP サーバ機能プログラム		
FTP サーバ機能プログラム		
SSH FTP サーバ機能プログラム		
RADIUS シークレット機能プログラム		
リンクダウン検出時のポートの閉塞機能プログラム		
閉塞したポートの開放機能プログラム		

[割付：アクセス制御SFP]

IT環境機能の制御ルール設定SFP

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]。

[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	制御された操作
TOE のスレッド	TELNET サーバ機能プログラム	起動指示
	SSH ログインサーバ機能プログラム	
	HTTP サーバ機能プログラム	
	FTP サーバ機能プログラム	
	SSH FTP サーバ機能プログラム	
	RADIUS シークレット機能プログラム	
	リンクダウン検出時のポートの閉塞機能プログラム	
	閉塞したポートの開放機能プログラム	

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]。

[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]
なし。

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。

[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。

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

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と改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

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

依存性：なし

5.1.2. TOE のセキュリティ保証要件

TOE を搭載する SR-S は一般のコマーシャルシステムの中で利用される。このため、コマーシャルシステム用として、最高レベルである EAL 4 に ALC_FLR.1 を追加した評価保証レベルとする。表 5.1 に保証要件一覧を示す。

表 5.1 保証要件一覧

TOE セキュリティ保証要件		コンポーネント
構成管理	CM 自動化	ACM_AUT.1
	CM 能力	ACM_CAP.4
	CM 範囲	ACM_SCP.2
配付と運用	配付	ADO_DEL.2
	設置、生成、及び立上げ	ADO_IGS.1
開発	機能仕様	ADV_FSP.2
	上位レベル設計	ADV_HLD.2
	実装表現	ADV_IMP.1
	下位レベル設計	ADV_LLD.1
	表現対応	ADV_RCR.1
	セキュリティ方針モデル化	ADV_SPM.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1
	ライフサイクル定義	ALC_LCD.1
	欠陥修正	ALC_FLR.1
	ツールと技法	ALC_TAT.1
テスト	カバレージ	ATE_COV.2
	深さ	ATE_DPT.1
	機能テスト	ATE_FUN.1
	独立テスト	ATE_IND.2

脆弱性評定	誤使用	AVA_MSU.2
	TOEセキュリティ機能強度	AVA_SOF.1
	脆弱性分析	AVA_VLA.2

5.1.3. 機能強度

本 TOE における最小機能強度は、SOF-基本である

5.2. IT 環境に対するセキュリティ要件

本節では、TOE 環境が満たすべき IT セキュリティ要件の詳細について記述する。

FIA_UID.2(2) アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1

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

※ 下線部は詳細化操作を示す。

依存性: なし

FIA_UAU.2(2) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1

AAA機能は、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、各利用者に以下のいずれかの認証メカニズムが成功することを要求しなければならない。

- EAP-MD5
- EAP-TLS
- EAP-TTLS
- PEAP

※ 下線部は詳細化操作を示す。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2(3) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1

SR-SのAAA制御機能は、そのRADIUSサーバを代行する他のTSF調停アクションを許可する前に、RADIUSサーバに自分自身を識別することを要求しなければならない。

※ 下線部は詳細化操作を示す。

依存性: なし

FIA_UAU.2(3) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1

SR-SのAAA制御機能は、そのRADIUSサーバを代行する他のTSF調停アクションを許可する前に、RADIUSサーバにRADIUSシークレットによる認証メカニズムが成功することを要求しなければならない。

※ 下線部は詳細化操作を示す。

依存性: FIA_UID.1 識別のタイミング

FTA_TSE.1 TOE セション確立

下位階層: なし

FTA_TSE.1.1

SR-Sのプロトロコル制御プログラムは、[割付: 属性]に基づきSupplicantからのリンクの確立を拒否できなければならない。

[割付: 属性]
ether ポートのリンクダウン回数の上限値

※ 下線部は詳細化操作を示す。

依存性: なし

6. TOE 要約仕様

本章では、TOE セキュリティ機能を記述する。

6.1. TOE セキュリティ機能

本節では、TOE のセキュリティ機能を説明する。各機能に対応する TOE セキュリティ機能要件が示されているように、本節で説明するセキュリティ機能は、TOE セキュリティ機能要件で記述した TOE セキュリティ機能要件を満たす。表 6.1 に TOE 要約仕様の各機能と TOE セキュリティ機能要件の対応を示す。

表 6.1 TOE 要約仕様と TOE セキュリティ機能要件の対応

NO	TOE 要約仕様	TOE セキュリティ機能要件
1	IEEE802.1X 認証失敗時のアクセスの抑止機能	FIA_AFL.1 FPT_RVM.1
2	運用支援機能	FIA_AFL.1 FIA_SOS.1 FIA_UID.2(1) FIA_UAU.2(1) FIA_UAU.7 FPT_RVM.1 FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FDP_ACC.1 FDP_ACF.1 FPT_SEP.1 FPT_RVM.1

6.2. IEEE802.1X 認証機能

本節では、IEEE802.1X 認証機能の概要及び本 TOE の TSF について述べる。

IEEE802.1X 認証機能は、外部に接続した RADIUS サーバによって Supplicant の認証を行う機能である。SR-S では、IEEE802.1X の規格 に準拠した機能をサポートしている。TOE の IEEE802.1X 認証機能は、構成定義情報を参照して動作し、認証方式「EAP-MD5」、「EAP-TLS」、「EAP-TTLS」、「PEAP」に対応している。

本 TOE では、IEEE802.1X 認証機能における以下の TSF を提供する。

6.2.1. IEEE802.1X 認証失敗時のアクセスの抑止機能 (SF.AFL)

Supplicant の AAA 機能による識別認証にて、パスワード、証明書の誤りを検出し、設定する抑止時間の間、Supplicant からのアクセスを抑止する機能である。

TOE は、本機能により識別認証機能へのブルートフォース攻撃や辞書攻撃を防止する。

TOE は、Supplicant の識別認証に失敗すると、再度識別認証を許可するまでの時間を 60～600 秒の範囲で抑止する。

6.2.2. 運用支援機能 (SF.TSF_MNG)

運用支援機能は、管理者のみに以下の IEEE802.1X 認証機能の管理行為を行う能力を提供する。

- IEEE802.1X 認証機能の有効機能
- IEEE802.1X 認証機能の認証方式の設定機能(MAC ベース認証とポートベース認証)
- IEEE802.1X 認証機能の認証失敗時におけるアクセス抑止中の状態の解除機能

運用支援機能は、管理者のみに TSF データの以下の管理行為を行う能力を提供する。

- 管理者のパスワード変更と退避
- IEEE802.1X 認証機能の認証失敗時におけるアクセスの抑止時間の変更

運用支援機能は、管理者のみに IEEE802.1X 認証機能の認証失敗時におけるアクセス抑止中の状態を解除する機能を提供する。

管理コンソールから管理者が TSF データを操作する前に、管理者の識別認証を実施する。識別認証は、ユーザー名とパスワードにより実施する。パスワードの情報を以下に示す。

本機能にて使用するパスワードには以下の規則が存在する。

・ パスワードのフィードバックは非表示

・ パスワードの構成文字種は ASCII 文字 (0x21,0x23～0x7e)
・ パスワードの文字列長は、8 文字以上、64 文字以下

管理者が TOE を利用する前に、TOE に登録した管理者であることを識別、本人であることを認証する。識別と認証の前には、一切の機能を提供しない。また、パスワードの入力時、入力文字を非表示にすることにより、パスワードの漏洩を防ぐ。

また、運用支援機能は、以下の機能のふるまいを管理者に制限する機能も提供する。

- CE 保守ログインの可否
- 一般ユーザログインの可否
- TELNET サーバ機能
- SSH ログインサーバ機能
- HTTP サーバ機能
- FTP サーバ機能
- SSH FTP サーバ機能
- RADIUS シークレット機能
- リンクダウン検出時のポートの閉塞機能
- 閉塞したポートの開放機能

6.3. セキュリティメカニズム

本 TOE では、セキュリティメカニズムは管理コンソールの識別認証機能のパスワードのみが該当する。

6.4. セキュリティ機能強度

本 TOE において、機能強度の対象となる順列的・確率的メカニズムを有する IT セキュリティ機能は識別認証機能であり、機能強度は SOF-基本である。

また明示された機能強度が適用される TOE セキュリティ機能要件は、FIA_SOS.1、FIA_UAU.2(1)であり、機能強度は SOF-基本である。

TOE セキュリティ機能要件の FIA_AFL.1 も識別認証機能であるが、FIA_AFL.1 のみで TSF を構成しており、順列的・確率的メカニズムを持たないため機能強度の対象としていない。

6.5. 保証手段

本節では、TOE の保証手段を説明する。表 6.2 に示すように、以下のセキュリティ保証手段は、表で記述した TOE セキュリティ保証要件を満たすものである。なお、ASE クラスに対する保証手段は、本セキュリティターゲットである。

表 6.2 TOE の保証手段一覧

TOE セキュリティ保証要件		コンポーネント	保証手段
構成管理	CM 自動化 CM 能力 CM 範囲	ACM_AUT.1 ACM_CAP.4 ACM_SCP.2	- 構成管理規定 - ドキュメント管理ガイドライン - プログラムソースファイル管理ガイドライン - Si-R ソフトウェアバージョン管理規定 - 構成リスト
配付と運用	配付	ADO_DEL.2	- ソフトウェア原本登録規定 - ロードモジュール生成手順ガイドライン
	設置、生成、及び立上げ	ADO_IGS.1	- SR-S724TC1/324TC1 セキュアスイッチ ご利用にあたって V10
開発	機能仕様 上位レベル設計 実装表現 下位レベル設計	ADV_FSP.2 ADV_HLD.2 ADV_IMP.1 ADV_LLD.1	- SR-S IEEE802.1X 認証機能兼上位レベル仕様書 - SR-S IEEE802.1X 認証下位レベル仕様書 - SR-S IEEE802.1X ソースプログラム一式 - Si-R/SR-S コマンド運用支援機能仕様書 - Si-R/SR-S コマンド運用支援機能上位レベル設計書 - Si-R/SR-S コマンド実行機能下位レベル設計書 - Si-R/SR-S コマンド実行機能ソースプログラム一式
	表現対応	ADV_RCR.1	- SR-S シリーズ　ISO15408 表現対応表
	セキュリティ方針モデル化	ADV_SPM.1	- SR-S Security Softoware V01.01 セキュリティポリシーモデル
ガイダンス文書	管理者ガイダンス 利用者ガイダンス	AGD_ADM.1 AGD_USR.1	- SR-S724TC1/324TC1 セキュアスイッチ ご利用にあたって V10 - SR-S シリーズ セキュアスイッチ　機能説明書 V10 - SR-S シリーズ セキュアスイッチ　コマンド設定事例集 V10 - SR-S シリーズ セキュアスイッチ　コマンドリファレンス V10 - SR-S シリーズ セキュアスイッチ コマンドユーザーズガイド V10
ライフサイクルサポ	開発セキュリティ 欠陥修正	ALC_DVS.1 ALC_FLR.1	- ライフサイクル規定 - パソコン/ネットワーク利用規定 - 情報システムセキュリティ規定

TOE セキュリティ保証要件		コンポーネント	保証手段
ート	ライフサイクル定義 ツールと技法	ALC_LCD.1 ALC_TAT.1	- FJ-WAN 利用基準 - 情報管理ハンドブック - ウイルス対策実施基準 - ロードモジュール生成手順ガイドライン - ログインアカウント管理規定 - バックアップ管理規定 - 武蔵小杉タワープレイス入（退）室館管理規定 - エンタープライズ部門設計・開発プロセス管理規定 - エンタープライズ部門ソフトウェア設計開発規定 - エンタープライズ部門ソフトウェア工程移行規定 - エンタープライズ部門ソフトウェア構成管理規定 - エンタープライズ部門ソフトウェアレビュー実施規定 - コンパイル/リンクオプション体系 - 欠陥修正対応規定 - エンタープライズ部門 設計変更処理規定 - 公開ホームページ Download サイトコンテンツ公開手順書
テスト	カバレージ 深さ 機能テスト	ATE_COV.2 ATE_DPT.1 ATE_FUN.1	- SR-S シリーズ　ISO15408 カバレージ分析書 - SR-S シリーズ　ISO15408 深さ分析書 - Si-R/SR-S コマンド運用支援機能試験仕様書 - IEEE802.1X 試験仕様書(CT 工程) - IEEE802.1X 試験仕様書(IT 工程)
	独立テスト	ATE_IND.2	- セキュアスイッチ SR-S シリーズ SR-S Security Software
脆弱性評定	誤使用 TOE セキュリティ機能強度 脆弱性分析	AVA_MSU.2 AVA_SOF.1 AVA_VLA.2	- SR-S Security Software V01.01 脆弱性分析書

7. PP 主張

本 ST が適合する PP は存在しない。

8. 根拠

8.1. セキュリティ対策方針根拠

TOE セキュリティ環境に対応するセキュリティ対策方針の関係を『表 8.1 TOE セキュリティ環境とセキュリティ対策方針の対応』に示す。

表 8.1 TOE セキュリティ環境とセキュリティ対策方針の対応

TOE セキュリティ環境 / セキュリティ対策方針	T.NET_CONNECT	A.TRUST	A.SUPPLICANT	A.SECRET	A.QUIETPERIOD	A.PORT	A.SERVICE	A.NETWORK	A.PASSWORD	A.CONSOLE
O.NET_AUT	✔									
O.TSF_MNG	✔									
OE.NET_ID&AUT	✔									
OE.RADIUS	✔									
OE.LINKDOWN	✔									
OE.TRUST		✔								
OE.SUPPLICANT			✔							
OE.SECRET				✔						
OE.QUIETPERIOD					✔					
OE.PORT						✔				
OE.SERVICE							✔			
OE.NETWORK								✔		
OE.PASSWORD									✔	
OE.CONSOLE										✔

以下に、『表 8.1　TOE セキュリティ環境とセキュリティ対策方針の対応』の根拠を示す。

A.TRUST

A.TRUST は、管理者が権限に課せられた責務に責任を持ち、不正な行為を行わないことを

規定した前提条件である。

この前提条件を満足するためには、管理者が権限に課せられた責務に責任を持ち、不正な行為を行わないものであることを保証する必要がある。

OE.TRUST では、管理者に適した者を任命し、それぞれの権限に課せられた責務を理解させることを組織の責任者に要求しているため、管理者が権限に課せられた責務に責任を持ち、不正な行為を行わない者であることを保証できる。

従って、OE.TRUST が満たされることにより、本前提条件を満足することができる。

A.SUPPLICANT

A.SUPPLICANT は、利用者が Supplicant の認証情報には十分な強度を持つものを使用する前提条件である。例えば、認証方式が EAP-MD5 の場合は、8 文字以上のパスワードを使用する。

この前提条件を満足するためには、利用者に Supplicant の認証情報には十分な強度を持つものを使用させる必要がある。

OE.SUPPLICANT では、管理者が利用者に Supplicant の認証情報には十分な強度を持つものを使用させることを確認できる。

したがって、OE.SUPPLICANT が満たされることにより、本前提条件を満足することができる。

A.SECRET

A.SECRET は、RADIUS サーバと TOE を搭載する SR-S に設定する RADIUS シークレットには十分な強度を持つものを使用する前提条件である。例えば、8 文字以上の RADIUS シークレットを使用する。

この前提条件を満足するためには、RADIUS サーバと TOE を搭載する SR-S に設定する RADIUS シークレットには十分な強度を持つものを使用する必要がある。

OE.SECRET では、RADIUS サーバと TOE を搭載する SR-S に設定する RADIUS シークレットには十分な強度を持つものを使用して運用することが確認できる。

したがって、OE.SECRET が満たされることにより、本前提条件を満足することができる。

A.QUIETPERIOD

A.QUIETPERIOD は、TOE を搭載する SR-S に設定する IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間には 60 秒以上の値を使用する前提条件である。

この前提条件を満足するためには、TOE を搭載する SR-S に設定する IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間には 60 秒以上の値を使用する必要がある。

OE.QUIETPERIOD では、TOE を搭載する SR-S に設定する IEEE802.1X 認証失敗時のアクセスの抑止機能における抑止時間には 60 秒以上の値を使用して運用することが確認できる。

したがって、OE.QUIETPERIOD が満たされることにより、本前提条件を満足することができる。

A.PORT

A.PORT は、TOE を搭載する SR-S では、IEEE802.1X 認証の機能を有効とし、IEEE802.1X 認証方式として物理ポート単位での認証（ポートベース認証）を使用し、MAC アドレス単位での認証（MAC ベース認証）は使用しない前提条件である。

この前提条件を満足するためには、TOE を搭載する SR-S では、IEEE802.1X 認証の機能を有効とし、IEEE802.1X 認証方式として物理ポート単位での認証（ポートベース認証）を使用し、MAC アドレス単位での認証（MAC ベース認証）は使用させない設定にする必要がある。

OE.PORT では、TOE を搭載する SR-S では、IEEE802.1X 認証の機能を有効とし、IEEE802.1X 認証方式として物理ポート単位での認証（ポートベース認証）を使用させ、MAC アドレス単位での認証（MAC ベース認証）は使用させない設定で運用することを確認できる。

したがって、OE.PORT が満たされることにより、本前提条件を満足することができる。

A.SERVICE

A.SERVICE は、TOE が動作する SR-S では、リモートからの運用支援機能及びファイル転送サービスを使用しない前提条件である。

この前提条件を満足するためには、TOE が動作する SR-S において以下のリモートからの運用支援機能のサービス及びファイル転送サービスを使用させない設定にする必要がある。

- TELNET サーバ機能
- SSH ログインサーバ機能
- HTTP サーバ機能
- FTP サーバ機能
- SSH FTP サーバ機能

OE.SERVICE では、上記のリモートからの運用支援機能及びファイル転送サービスを使用させない設定にすることを管理者に要求しているため、上記のサービスが動作しないことを確認できる。

従って、OE.SERVICE が満たされることにより、本前提条件を満足することができる。

A.NETWORK

A.NETWORK は、TOE が動作する SR-S は、認証済み Supplicant の成りすましや通信データの盗聴、及び管理者以外による電源断ができないネットワーク構成で運用する前提条件である。

この前提条件を満足するためには、例として下記の対策を実施することが必要である。

- １つのポートには１つの Supplicant とするネットワーク構成とする。

- 管理者以外に SR-S を電源断されないように物理的に保護する。

OE.NETWORK では、TOE が動作する SR-S において、認証済み Supplicant の成りすましや通信データの盗聴、及び管理者以外に SR-S を電源断されないネットワーク構成で運用することを確認できる。

従って、OE.NETWORK が満たされることにより、本前提条件を満足することができる。

A.PASSWORD

A.PASSWORD は、TOE が動作する SR-S では、管理コンソールの識別認証機能で使用する管理者のパスワードには、十分な強度を持つものを使用する前提条件である。例えば、8 文字以上のパスワードを使用する前提条件である。

この前提条件を満足するためには、管理コンソールの識別認証機能における管理者のパスワードを 8 文字以上に設定し、使用する必要がある。

OE.PASSWORD では、管理コンソールの識別認証に使用するパスワードに十分な強度を持つものを使用して運用することが確認できる。

従って、OE.PASSWORD が満たされることにより、本前提条件を満足することができる。

A.CONSOLE

A.CONSOLE は、TOE が動作する SR-S では、管理コンソールの使用を管理者の利用者 ID のみ可能とし、通常の運用において保守用及び一般ユーザ用の利用者 ID は使用しない前提条件である。

この前提条件を満足するためには、管理者以外の保守用及び一般ユーザ用の利用者 ID による使用を不可にする設定にする必要がある。

OE.CONSOLE では、管理コンソールの使用を管理者の利用者 ID のみとし、保守用及び一般ユーザ用の利用者 ID による使用を不可とする設定を管理者に要求しているため、保守用及び一般ユーザ用の利用者 ID の使用を不可としていることを確認できる。

従って、OE.CONSOLE が満たされることにより、本前提条件を満足することができる。

T.NET_CONNECT

T.NET_CONNECT は、管理者及び利用者以外の者が機器をネットワークに接続し、SR-S を経由してアクセスするネットワーク上のサーバ、クライアントの利用者の資産に攻撃する脅威である。

この脅威に対抗するためには、Supplicant を SR-S に接続する際に識別認証を行い、その利用者の正当性を確認する必要がある。また、Supplicant からの短時間における連続した識別認証の試みを抑止することが必要である。

OE.RADIUS は、Supplicant の識別認証情報を持つ RADIUS サーバの安全性を確保するために、RADIUS サーバが SR-S と接続する場合には RADIUS サーバの識別認証を実施し、接続が

許可されていない RADIUS サーバの接続を却下する機能を提供する。

OE.NET_ID&AUT は、Supplicant が SR-S のポートへの接続時にアクセスした者が誰であるかを識別し、本人であることの認証を行っている。

O.NET_AUT は、Supplicant の認証失敗時に次の認証までの一定時間のアクセスを抑止するため、短時間における連続した識別認証の試みが不可能となり、認証情報へのブルートフォース攻撃や辞書攻撃を抑止できる。

ここで、O.NET_AUT による認証の一定時間のアクセス抑止中に Supplicant が接続されているポートからリンクダウンが検出されるとアクセス抑止が中断される。再度 Supplicant をポートに接続してリンクが確立すると、一定時間のアクセスが抑止されることなく識別認証の試みが可能となる。OE.LINKDOWN は、O.NET_AUT を迂回する行為にあたるリンクダウン検出時にはポートを閉塞する機能を提供しており、ポートを閉塞する機能を有効とし、一定回数リンクダウンを検出した場合は、ポートを閉塞して Supplicant の接続を却下する。

O.TSF_MNG は、TSF の動作に係わるデータと操作、及び TSF の動作に係わる IT 環境の機能のデータと操作を管理者のみに可能とする機能を提供する。

従って、OE.RADIUS、 OE.NET_ID&AUT 、O.NET_AUT、OE.LINKDOWN、O.TSF_MNG が満たされることにより、本脅威に対抗することができる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

セキュリティ対策方針に対するセキュリティ機能要件の対応を『表8.2 セキュリティ対策方針とセキュリティ機能要件の対応』に示す。

表 8.2 セキュリティ対策方針とセキュリティ機能要件の対応

種別	セキュリティ機能要件 ＼ セキュリティ対策方針	O.NET_AUT	O.TSF_MNG	OE.NET_ID&AUT	OE.RADIUS	OE.LINKDOWN
TOE セキュリティ機能要件	FIA_AFL.1	✔	✔			
	FIA_SOS.1		✔			
	FIA_UID.2(1)		✔			
	FIA_UAU.2(1)		✔			
	FIA_UAU.7		✔			
	FMT_MOF.1		✔			
	FMT_MTD.1		✔			
	FMT_SMF.1		✔			
	FMT_SMR.1		✔			
	FDP_ACC.1		✔			
	FDP_ACF.1		✔			
	FPT_RVM.1	✔	✔			
	FPT_SEP.1		✔			
IT 環境のセキュリティ機能要件	FIA_UID.2(2)			✔		
	FIA_UAU.2(2)			✔		
	FIA_UID.2(3)				✔	
	FIA_UAU.2(3)				✔	
	FTA_TSE.1					✔

表 8.2 より、各セキュリティ機能要件が１つ以上のセキュリティ対策方針に対応していることが分かる。

以下に、『表 8.2 セキュリティ対策方針とセキュリティ機能要件の対応』の根拠を示す。

O.NET_AUT

O.NET_AUT は、AAA 機能の識別認証において、認証失敗時に次の認証までの時間を一定間隔抑止し、認証情報の推測を困難にするセキュリティ対策方針である。

FIA_AFL.1 により、認証失敗時に次の認証までの時間を一定間隔抑止し、攻撃者による認証情報の推測を抑止する。

FPT_RVM.1 により、利用者の認証失敗時には、確実に次の認証までの時間を一定間隔抑止するセキュリティ機能が呼び出されることを保証する。

以上のセキュリティ機能要件によって、O.NET_AUT を満たす事ができる。

O.TSF_MNG

O.TSF_MNG は、TSF の動作に係わるデータと操作、及び TSF の動作に係わる IT 環境の機能のデータと操作を管理者のみに可能とするセキュリティ対策方針である。

FIA_AFL.1 により、管理者のみが IEEE802.1X 認証機能の認証失敗時におけるアクセス抑止中の状態を解除することができる。

FIA_UAU.2(1)及び FIA_UID.2(1)により、TOE の利用前に識別と認証を行うことができる。識別及び認証が成功した場合は、TOE の利用を許可し、識別又は認証が不成功の場合は、TOE の利用を一切拒否する。認証の実施の際には、FIA_UAU.7 により操作者によって入力されたパスワードを非表示にすることで画面上からの漏洩を防ぐことができる。認証に使用されるパスワードに対しては、FIA_SOS.1 により一定の強度を持つパスワードの品質を確保することができる。

FMT_MOF.1、FMT_MTD.1 及び FMT_SMR.1 により、SR-S の動作に関わる TSF データは、管理者だけが設定管理できるように制限することができ、FMT_SMF.1 により管理を行うことができる。

FDP_ACC.1 と FDP_ACF.1 により、リモートからの運用支援機能プログラム及びファイル転送サービス機能プログラム、、RADIUS シークレット機能プログラム、リンクダウンを一定回数検出した場合のポートの閉塞とその開放機能プログラムの起動指示を管理者のみに操作を許可する。

FPT_RVM.1 により、利用者が TOE 機能に関する情報にアクセスする場合には、確実に管理コンソールの識別認証機能が呼び出されることを保証する。

FPT_SEP.1 によって、環境設定に関わるセキュリティドメインが TSF の実行のために構築される。

以上のセキュリティ機能要件により、O.TSF_MNG を満たす事ができる。

OE.NET_ID&AUT

OE.NET_ID&AUT は、Supplicant がネットワークに接続する場合には識別と認証を実施し、接続を許可されていない者の接続要求を却下するセキュリティ対策方針である。

FIA_UAU.2(2)及び FIA_UID.2(2)により、TOE の利用前に Supplicant の識別と認証を行うことができる。識別及び認証が成功した場合は、ネットワークセグメントの利用を許可し、識別又は認証が不成功の場合は、TOE の利用を一切拒否する。

以上のセキュリティ機能要件により、OE.NET_ID&AUT を満たす事ができる。

OE.RADIUS

OE.RADIUS は、RADIUS サーバが SR-S と接続する場合には識別と認証を実施し、接続が許可されていない RADIUS サーバの接続を却下するセキュリティ対策方針である。

FIA_UAU.2(3)及び FIA_UID.2(3)により、RADIUS サーバが SR-S に接続する際に RADIUS サーバの識別と認証を行うことができる。識別及び認証が成功した場合は、SR-S による RADIUS サーバの利用が可能となり、識別または認証が不成功の場合は、RADIUS サーバの利用を一切拒否する。

以上のセキュリティ機能要件により、OE.RADIUS を満たす事ができる。

OE.LINKDOWN

OE.LINKDOWN は、リンクダウンを一定回数検出した場合、検出したポートを閉塞し、Supplicant の接続を却下するセキュリティ対策方針である。

FTA_TSE.1 により、Supplicant が接続しているポートのリンクダウンを一定回数検出した場合、検出したポートを閉塞し、Supplicant の接続を却下する

以上のセキュリティ機能要件により、OE.LINKDOWN を満たす事ができる。

8.2.2. セキュリティ機能要件間の依存関係

TOE 及び IT 環境のセキュリティ機能要件間の依存関係を『表 8.3　TOE セキュリティ機能要件間の依存関係』に示す。

表 8.3 セキュリティ機能要件間の依存関係

NO	セキュリティ機能要件	下位階層	依存関係	参照 NO	備考
1	FIA_AFL.1	なし	FIA_UAU.1	4	FIA_UAU.2 は FIA_UAU.1 の上位階層コンポーネントである
2	FIA_SOS.1	なし	なし		
3	FIA_UID.2(1)	FIA_UID.1	なし		FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
4	FIA_UAU.2(1)	FIA_UAU.1	FIA_UID.1	3	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
5	FIA_UAU.7	なし	FIA_UAU.1	4	FIA_UAU.2 は FIA_UAU.1 の上位階層コンポーネントである
6	FMT_MOF.1	なし	FMT_SMF.1	8	
			FMT_SMR.1	9	
7	FMT_MTD.1	なし	FMT_SMF.1	8	
			FMT_SMR.1	9	
8	FMT_SMF.1	なし	なし		
9	FMT_SMR.1	なし	FIA_UID.1	3	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
10	FDP_ACC.1	なし	FDP_ACF.1	11	
11	FDP_ACF.1	なし	FDP_ACC.1	10	FMT_MSA.3 は管理対象となるセキュリティ属性が無いため適用しない
			FMT_MSA.3		

12	FPT_RVM.1	なし	なし		
13	FPT_SEP.1	なし	なし		
14	FIA_UID.2(2)	FIA_UID.1	なし		FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
15	FIA_UAU.2(2)	FIA_UAU.1	FIA_UID.1	14	FIA_UAU.2 は FIA_UAU.1 の上位階層コンポーネントである
16	FIA_UID.2(3)	FIA_UID.1	なし		FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
17	FIA_UAU.2(3)	FIA_UAU.1	FIA_UID.1	16	FIA_UAU.2 は FIA_UAU.1 の上位階層コンポーネントである

8.2.3. TOE セキュリティ機能要件の相互作用

明示的な依存関係は要求されないが、相互支援を目的として選択されたセキュリティ機能要件を『表 8.4 TOE セキュリティ機能要件の相互作用について』に示す。

表 8.4 TOE セキュリティ機能要件の相互作用について

相互支援 / セキュリティ機能要件	迂回防止	干渉防止	非活性化防止
FIA_AFL.1	FPT_RVM.1	FMT_MTD.1	FMT_MOF.1
FIA_SOS.1	なし	なし	なし
FIA_UID.2(1)	FPT_RVM.1	なし	なし
FIA_UAU.2(1)	FPT_RVM.1	FMT_MTD.1	なし
FIA_UAU.7	なし	なし	なし
FMT_MOF.1	なし	なし	なし
FMT_MTD.1	なし	なし	なし
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	なし	なし	なし
FDP_ACC.1	FIA_UAU.2	FPT_SEP.1	なし
FDP_ACF.1	FIA_UAU.2	FPT_SEP.1	なし
FPT_RVM.1	なし	なし	なし
FPT_SEP.1	なし	なし	なし

〈迂回防止〉

FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、識別認証機能に関するセキュリティ機能要件が呼び出され成功することが保証される。

対象となるセキュリティ機能要件は、FIA_AFL.1、FIA_UID.2、FIA_UAU.2 である。

従って、FPT_RVM.1 によって FIA_AFL.1、FIA_UID.2、FIA_UAU.2 の迂回防止を支援しているため、セキュリティ対策方針 O.NET_AUT と O.TSF_MNG が達成される。

なお、本 TOE では識別認証機能が動作した後に運用支援機能が動作し、運用支援機能を使用して定義する環境設定に従って通信を行うため、これらのセキュリティ機能を構成するセキュリティ機能要件は、間接的に FPT_RVM.1 の相互サポートを受けている。

FIA_UAU.2 により、運用支援機能の環境設定が許可される前に、認証機能に関するセキュリティ機能要件が呼び出され成功することが保証される。

対象となるセキュリティ機能要件は、FDP_ACC.1、FDP_ACF.1 である。

従って、FIA_UAU.2 によって FDP_ACC.1、FDP_ACF.1 が迂回防止のサポートを受けている。

〈干渉防止〉

FMT_MTD.1 により、以下に示すに機能要件に関する TSF データの操作を、管理者だけに制限し、管理者以外の人物による干渉と改ざんの攻撃へ対抗している。

・FIA_AFL.1

・FIA_UAU.2(1)

従って、FMT_MTD.1 によって FIA_AFL.1、FIA_UAU.2 への干渉及び改ざん防止を支援しているため、セキュリティ対策方針 O.PAC_MNG が達成される。

FPT_SEP.1 により、以下に示すアクセス制御機能に関するセキュリティ機能要件において、信頼できないサブジェクトによる干渉と改ざんから保護するセキュリティドメインが構築されることを保証する。

・FDP_ACC.1

・FDP_ACF.1

従って、FPT_SEP.1 によって FDP_ACC.1、FDP_ACF.1 への干渉及び改ざん防止を支援しているため、セキュリティ対策方針 O.PAC_MNG が達成される。

〈非活性化防止〉

FMT_MOF.1 により、以下に示す機能要件に関する TSF データへの操作を、管理者だけに制限しているため、TOE を非活性化させる攻撃へ対抗している。

・FIA_AFL.1

8.2.4. 最小機能強度根拠

攻撃方法は、公開インタフェース、公開情報を利用したものとなる。TOEが想定する脅威は不正なネットワークへの接続であり、TOEが動作するSR-Sの外部インタフェースを利用した不正アクセスである。攻撃には高度な知識や攻撃ツールは不要であり、通常のスイッチとして想定される利用において起こり得る脅威である。従って、TOEのセキュリティ対策方針では低レベルの攻撃に対する対抗性が要求されるため、最小機能強度レベルとしてSOF-基本が必要となる。また、本STではTOEセキュリティ機能要件に対する最小機能強度としてSOF-基本を主張しており、低レベルの攻撃に対抗するために策定されたTOEのセキュリティ対策方針と一貫している。

また、特定の機能要件(FIA_SOS.1、FIA_UAU.2(1))の機能強度は SOF-基本であり、最小機

能強度の SOF-基本と一貫している。

8.2.5. セキュリティ保証要件根拠

本 ST の TOE セキュリティ対策方針の顧客サイトにおける実効性を保証するには、外部仕様から実装表現までのソフトウェア品質、及び開発者サイトから顧客サイトに至るまでの改ざん、セキュリティ欠陥への対策が必要である。

そこで、品質管理の製品ライフサイクル評価、外部仕様設計からソースコードレベルの設計評価、開発者のみならず評価者による脆弱性分析、顧客のサイトに届き設置され立上がるまでの間に改ざんの防止、及びセキュリティ欠陥の修正に関する手順の評価をもって、顧客サイトにおける TOE セキュリティ対策方針の実効性の保証となす。

そのため、この保証に必要であり、かつ、この保証を満たす EAL4 に ALC_FLR.1 を追加した保証要件を本 ST は選択する。

8.3　TOE 要約仕様根拠

8.3.1. TOE 要約仕様に対するセキュリティ機能要件の適合性

TOE 要約仕様に適合するセキュリティ機能要件の関係を『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』に示す。

表 8.5 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / TOE セキュリティ機能要件	SF.AFL(IEEE802.1X 認証失敗時のアクセスの抑止機能)	SF.TSF_MNG(運用支援機能)
FIA_AFL.1	✔	✔
FIA_SOS.1		✔
FIA_UID.2(1)		✔
FIA_UAU.2(1)		✔
FIA_UAU.7		✔
FMT_MOF.1		✔
FMT_MTD.1		✔
FMT_SMF.1		✔
FMT_SMR.1		✔
FDP_ACC.1		✔
FDP_ACF.1		✔
FPT_RVM.1	✔	✔
FPT_SEP.1		✔

以下に、『表 8.5 TOE 要約仕様とセキュリティ機能要件の対応』の根拠を示す。

FIA_AFL.1

SF.AFL において、Supplicant が識別認証失敗した際に、次の認証までの時間を抑止する機能により、認証失敗時の取り扱いの要件を満足することができる。

SF.TSF_MNG において、管理者のみに IEEE802.1X 認証機能の認証失敗時におけるアクセス抑止中の状態を解除する機能を提供することにより認証失敗時の取り扱いの要件を満足することができる。

FIA_SOS.1

SF.TSF_MNG において、管理者のパスワードがパスワード規則を満たしているかをチェックする機能により、パスワードに対する秘密尺度の検証の要件を満足することができる。

FIA_UID.2(1)

SF.TSF_MNG において、管理者に対する未識別時のあらゆる TOE 機能の利用を禁止した識別機能により、識別実施前のすべての操作を禁止した要件を満足することができる。

FIA_UAU.2(1)

SF.TSF_MNG において、管理者に対する未認証時のあらゆる TOE 機能の利用を禁止した認証機能により、認証実施前のすべての操作を禁止した要件を満足することができる。

FIA_UAU.7

SF.TSF_MNG において、管理者のパスワード入力時にパスワードを表示しない機能により、入力時におけるパスワード情報の保護を規定した要件を満足することができる。

FMT_MOF.1

SF.TSF_MNG において、セキュリティ機能のふるまいを管理者のみに制限する機能により、管理者の構成定義情報に対する操作を規定した要件を満足することができる。

FMT_MTD.1

SF.TSF_MNG において、セキュリティ機能の動作に関連する情報を改変、問い合わせる能力を管理者のみに制限する機能により、管理者の構成定義情報に対する操作を規定した要件を満足することができる。

FMT_SMF.1

SF.TSF_MNG において、下記の項目を管理する機能により、管理機能の提供を規定した要件を満足することができる。

- IEEE802.1X 認証機能における認証失敗時のアクセスの抑止機能の動作設定機能
- IEEE802.1X 認証機能における認証失敗時のアクセス抑止時間の改変機能
- 運用支援機能における管理者の認証情報の改変機能
- 運用支援機能における管理者の認証情報の問い合わせ機能
- CE 保守ログインの可否の動作設定機能
- 一般ユーザログインの可否の動作設定機能

FDP_ACC.1

FDP_ACC.1 は、サブジェクト、オブジェクト及び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、アクセス制御 SFP を実施することを要求するセキュリティ機能要件である。

このセキュリティ要件では、サブジェクトに管理者を代行するスレッドを定義し、オブジェクトに下記の IT 環境機能の制御ルールの設定機能を定義している。これらの機能はコマンドのその他プログラムによって実装されている。

- TELNET サーバ機能プログラム
- SSH ログインサーバ機能プログラム
- HTTP サーバ機能プログラム
- FTP サーバ機能プログラム
- SSH FTP サーバ機能プログラム
- RADIUS シークレット機能プログラム
- リンクダウン検出時のポートの閉塞機能プログラム
- 閉塞したポートの開放機能プログラム

従って、SF.TSF_MNG において FDP_ACC.1 を実現できる。

FDP_ACF.1

FDP_ACF.1 は、セキュリティ属性によるアクセス制御の適用を要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理者権限で動作する TOE のスレッドに IT 環境機能の制御ルールの設定を許可するアクセス制御機能の実装が必要である。

運用支援機能によって、TOE のスレッドは、構成定義情報に IT 環境機能の制御ルールを設定する事ができる。

従って、SF.TSF_MNG において、FDP_ACF.1 を実現できる。

FMT_SMR.1

SF.TSF_MNG において、識別情報に関連付けられた管理者という役割を維持し、管理者の識別認証成功後に、管理者を代行するスレッドに役割を関連付ける機能により、役割の維持を規定した要件を満足することができる。

FPT_RVM.1

SF.AFL は、Supplicant の識別認証失敗時にはアクセスの抑止機能を呼び出して、成功することを保証する。

SF.TSF_MNG は、管理者が TSF データの管理行為を行う場合には運用支援機能を呼び出して、成功することを保証する。

以上より、TSP のバイパス性の要件を満足することができる。

FPT_SEP.1

SF.TSF_MNG は、IT 環境機能の制御ルールを設定する際には、SR-S のすべてのスレッドにおいて独立したスレッド空間を作成することで、スレッド間の干渉発生を防止し、改ざん、漏洩、暴露が発生しないセキュリティドメインを構築する。

以上より、TSF のための区分されたドメインを提供し、かつ TSC 内のサブジェクト間の分離を提供する要件を満足することができる。

8.3.2. セキュリティ機能強度根拠

特定の TOE セキュリティ機能要件に対する機能強度は、FIA_SOS.1、FIA_UAU.2(1)、に対する機能強度である SOF-基本である。また、IT セキュリティ機能に対する機能強度は、運用支援機能（6 章の機能名）に対する機能強度である SOF-基本である。そのため、特定の TOE セキュリティ機能要件に対する機能強度と、IT セキュリティ機能に対する機能強度は一貫している。

8.3.3. 保証手段根拠

表 6.2 に示した通り、すべての TOE セキュリティ保証要件は保証手段により示されたドキュメントのセットによって対応付けられる。

以下に、EAL4 の保証要件セットが各保証手段により満たされる根拠を示す。

ACM_AUT.1

【保証手段】

「構成管理規定」

「ドキュメント管理ガイドライン」

「プログラムソースファイル管理ガイドライン」

【保証要件根拠】

保証手段である「構成管理規定」、「ドキュメント管理ガイドライン」、「プログラムソースファイル管理ガイドライン」、「構成リスト」には、TOE の実装表現に対する構成管理に使用している自動化ツール、及び当該自動化ツールの利用手順について規定する。そのため、保証要件、ACM_AUT.1 は満たされている。

ACM_CAP.4　　許可の管理

【保証手段】

「構成管理規定」

「ドキュメント管理ガイドライン」

「プログラムソースファイル管理ガイドライン」

「Si-R ソフトウェアバージョン管理規定」

【保証要件根拠】

保証手段である「構成管理規定」、「ドキュメント管理ガイドライン」、「プログラムソースファイル管理ガイドライン」、「Si-R ソフトウェアバージョン管理規定」には、TOE のバージョンを識別するための命名規則、構成要素の一覧表、構成要素の一意の識別方法、TOE を生成する手続き、及び外部から TOE の構成要素を受け入れる際の手続きを規定する。そのため、保証要件 ACM_CAP.4 は満たされる。

ACM_SCP.2　　TOE の CM 範囲

【保証手段】

「構成管理規定」

「構成リスト」

【保証要件根拠】

保証手段である「構成管理規定」、「構成リスト」には、TOE の構成要素の管理対象範囲を規定する。そのため、保証要件 ACM_SCP.2 は満たされる。

ADO_DEL.2　　配付手続き

【保証手段】

「ソフトウェア原本登録規定」

「ロードモジュール生成手順ガイドライン」

【保証要件根拠】

保証手段である「ソフトウェア原本登録規定」と「ロードモジュール生成手順ガイドライン」には、TOE をユーザサイトに配付する際に採用される、TOE の完全性、及び真正性を維持するための手続きを規定する。そのため、保証要件 ADO_DEL.2 は満たされる。

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって V10」

【保証要件根拠】

保証手段である「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって V10」には、TOE をセキュアな構成にするために採用される、設置手順及び起動の確認方法を規定する。そのため、保証要件 ADO_IGS.1 は満たされる。

ADV_FSP.2　　非形式的機能仕様

【保証手段】

「SR-S IEEE802.1X 認証機能兼上位レベル仕様書」

「Si-R/SR-S コマンド運用支援機能仕様書」

【保証要件根拠】

保証手段である「SR-S IEEE802.1X 認証機能兼上位レベル仕様書」と「Si-R/SR-S コマンド運用支援機能仕様書」には、TSF に対するすべての外部インタフェースの仕様を規定し、かつ、TSF を完全に表現している論拠を示す。そのため、保証要件 ADV_FSP.2 は満たされる。

ADV_HLD.2　　セキュリティ実施上位レベル設計

【保証手段】

「SR-S IEEE802.1X 認証機能兼上位レベル仕様書」

「Si-R/SR-S コマンド運用支援機能上位レベル設計書」

【保証要件根拠】

保証手段である「SR-S IEEE802.1X 認証機能兼上位レベル仕様書」と「Si-R/SR-S コマンド運用支援機能上位レベル設計書」には、TSF をサブシステム単位に分割し、各サブシステムの仕様及び、サブシステム間インタフェースの仕様を規定する。そのため、保証要件 ADV_HLD.2 は満たされる。

ADV_IMP.1

【保証手段】

「SR-S IEEE802.1X ソースプログラム一式」

「Si-R/SR-S コマンド実行機能ソースプログラム一式」

【保証要件根拠】

保証手段である「SR-S IEEE802.1X ソースプログラム一式」、「Si-R/SR-S コマンド実行機能ソースプログラム一式」には、実装表現のサブセットが、TOE セキュリティ機能

要件を正しく具体化していることを示す。そのため、保証要件 ADV_IMP.1 は満たされる。

ADV_LLD.1

【保証手段】

「SR-S IEEE802.1X 認証下位レベル仕様書」

「Si-R/SR-S コマンド実行機能下位レベル設計書」

【保証要件根拠】

保証手段である「SR-S IEEE802.1X 認証下位レベル仕様書」と「Si-R/SR-S コマンド実行機能下位レベル設計書」には、TSF をモジュール単位に分割し、各モジュールの仕様及び、モジュール間インタフェースの仕様を規定する。そのため、保証要件 ADV_LLD.1 は満たされる。

ADV_RCR.1　　非形式的対応の実証

【保証手段】

「SR-S シリーズ　ISO15408 表現対応表」

【保証要件根拠】

保証手段である「SR-S シリーズ　ISO15408 表現対応表」には、TOE のセキュリティ機能の各レベル（要約仕様－機能仕様－上位レベル設計－下位レベル設計）での完全な対応を記述する。そのため、保証要件 ADV_RCR.1 は満たされる。

ADV_SPM.1

【保証手段】

「SR-S Security Softoware V01.01 セキュリティポリシーモデル」

【保証要件根拠】

保証手段である「SR-S Security Softoware V01.01 セキュリティポリシーモデル」には、セキュリティ機能要件をセキュリティ方針モデルとして表現し、かつ、そのセキュリティ方針モデルが、機能仕様として正しく実現されていることを規定する。そのため、保証要件 ADV_SPM.1 は満たされる。

AGD_ADM.1　　管理者ガイダンス

【保証手段】

「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって　V10」

「SR-S シリーズ セキュアスイッチ　機能説明書　V10」

「SR-S シリーズ セキュアスイッチ　コマンド設定事例集　V10」

「SR-S シリーズ セキュアスイッチ　コマンドリファレンス　V10」

「SR-S シリーズ セキュアスイッチ　コマンドユーザーズガイド　V10」

【保証要件根拠】

保証手段である「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって　V10」、「SR-S シリーズ セキュアスイッチ　機能説明書　V10」、「SR-S シリーズ セキュアスイッチ　コマンド設定事例集　V10」、「SR-S シリーズ セキュアスイッチ　コマンドリファレンス　V10」、「SR-S シリーズ セキュアスイッチ　コマンドユーザーズガイド　V10」には、TOE の管理者が使用するインタフェース、TOE をセキュアに運用するための警告を含む使用方法、及び TOE の障害時に管理者が採るべきアクションについて規定する。そのため、保証要件 AGD_ADM.1 は満たされる。

AGD_USR.1　　利用者ガイダンス

【保証手段】

「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって　V10」

「SR-S シリーズ セキュアスイッチ　機能説明書　V10」

【保証要件根拠】

保証手段である「SR-S724TC1/324TC1 セキュアスイッチ　ご利用にあたって　V10」、「SR-S シリーズ セキュアスイッチ　機能説明書　V10」には、TOE の利用者が使用するインタフェース、及び TOE のセキュアな運用のための警告を含む使用方法を規定する。そのため、保証要件 AGD_USR.1 は満たされる。

ALC_DVS.1　　セキュリティ手段の識別

【保証手段】

「パソコン/ネットワーク利用規定」

「情報システムセキュリティ規定」

「FJ-WAN 利用基準」

「情報管理ハンドブック」

「ウイルス対策実施基準」

「バックアップ管理規定」

「武蔵小杉タワープレイス入（退）室館管理規定」

「ログインアカウント管理規定」

【保証要件根拠】

保証手段である「パソコン/ネットワーク利用規定」、「情報システムセキュリティ規定」、「FJ-WAN 利用基準」、「情報管理ハンドブック」、「ウイルス対策実施基準」、「バックアップ管理規定」、「武蔵小杉タワープレイス入（退）室館管理規定」、「ログインアカウント管理規定」には、TOE を保護するために開発環境で使用される、物理的、手続き的、人的、及びその他のセキュリティ手段を規定する。そのため、保証要件 ALC_DVS.1 は満たされる。

ALC_FLR.1　　欠陥修正

【保証手段】

「エンタープライズ部門 設計変更処理規定」

「公開ホームページ Download サイトコンテンツ公開手順書」

「欠陥修正対応規定」

【保証要件根拠】

保証手段である「エンタープライズ部門 設計変更処理規定」、「公開ホームページ Download サイトコンテンツ公開手順書」、「欠陥修正対応規定」には発見された TOE のセキュリティの欠陥が開発者により追跡、修正、欠陥の情報と修正を配付するための方針と手続きを規定する。そのため、保証要件 ALC_FLR.1 は満たされる。

ALC_LCD.1

【保証手段】

「ライフサイクル規定」

「エンタープライズ部門設計・開発プロセス管理規定」

「エンタープライズ部門ソフトウェア設計開発規定」

「エンタープライズ部門ソフトウェア工程移行規定」

「エンタープライズ部門ソフトウェア構成管理規定」

「エンタープライズ部門ソフトウェアレビュー実施規定」

「エンタープライズ部門 設計変更処理規定」

【保証要件根拠】

保証手段である「ライフサイクル規定」、「エンタープライズ部門設計・開発プロセス管理規定」、「エンタープライズ部門ソフトウェア設計開発規定」、「エンタープライズ部門ソフトウェア工程移行規定」、「エンタープライズ部門ソフトウェア構成管理規定」、「エンタープライズ部門ソフトウェアレビュー実施規定」、「エンタープライズ部門 設計変更処理規定」には、ライフサイクルモデルにより、開発と保守のプロセスをカバーすることを記述する。そのため、保証要件 ALC_LCD.1 は満たされる。

ALC_TAT.1

【保証手段】

「ライフサイクル規定」

「コンパイル/リンクオプション体系」

「ロードモジュール生成手順ガイドライン」

【保証要件根拠】

保証手段である「ライフサイクル規定」、「コンパイル/リンクオプション体系」、「ロ

ードモジュール生成手順ガイドライン」には、実装に用いられた開発ツールのステートメント、及び実装依存オプションを規定する。そのため、保証要件 ALC_TAT.1 は満たされる。

ATE_COV.2　　カバレージの分析

【保証手段】

「SR-S シリーズ　ISO15408 カバレージ分析書」

【保証要件根拠】

保証手段である「SR-S シリーズ　ISO15408 カバレージ分析書」には、TOE のセキュリティ機能及び外部インタフェースに対するテストの十分性及び完全性について記述する。そのため、保証要件 ATE_COV.2 は満たされる。

ATE_DPT.1　　テスト：上位レベル設計

【保証手段】

「SR-S シリーズ　ISO15408 深さ分析書」

【保証要件根拠】

保証手段である「SR-S シリーズ　ISO15408 深さ分析書」には、TOE のサブシステム及びサブシステム間インタフェースに対するテストの十分性及び完全性について記述する。そのため、保証要件 ATE_DPT.1 は満たされる。

ATE_FUN.1　　機能テスト

【保証手段】

「IEEE802.1X 試験仕様書(CT 工程)」

「IEEE802.1X 試験仕様書(IT 工程)」

「 Si-R/SR-S コマンド運用支援機能試験仕様書」

【保証要件根拠】

保証手段である「IEEE802.1X 試験仕様書(CT 工程)」と「IEEE802.1X 試験仕様書(IT 工程)」と「 Si-R/SR-S コマンド運用支援機能試験仕様書」には、TSF に対するテストの全体計画、テストを実施するための手順、及びテスト結果を記述する。そのため、保証要件 ATE_FUN.1 は満たされる。

ATE_IND.2　　独立テスト - サンプル

【保証手段】

SR-S Security Software V01.01

【保証要件根拠】

保証手段である「SR-S Security Software V01.01」は、TOE のセキュリティ機能のテスト環境再現及びテスト資材を提供する。そのため、保証要件 ATE_IND.2 は満たされる。

AVA_MSU.2　　ガイダンスの検査

【保証手段】

「SR-S Security Software V01.01 脆弱性分析書」

【保証要件根拠】

保証手段である「SR-S Security Software V01.01 脆弱性分析書」には、TOEの利用者が、誤使用によりTOEのセキュリティ機能を非セキュアな状態にしてしまう危険性の無いようにTOEの使用方法を記述する。また、「SR-S Security Software V01.01 脆弱性分析書」には、ガイダンスの完全性を保証する手段を開発者が講じていることを記述する。そのため、保証要件AVA_MSU.2は満たされる。

AVA_SOF.1　　TOE セキュリティ機能強度評価

【保証手段】

「SR-S Security Software V01.01 脆弱性分析書」

【保証要件根拠】

保証手段である「SR-S Security Software V01.01 脆弱性分析書」には、TOE のセキュリティ機能のセキュリティメカニズムに対しての TOE セキュリティ機能強度分析について記述する。そのため、保証要件 AVA_SOF.1 は満たされる。

AVA_VLA.2　　開発者脆弱性分析

【保証手段】

「SR-S Security Software V01.01 脆弱性分析書」

【保証要件根拠】

保証手段である「SR-S Security Software V01.01 脆弱性分析書」には、TOE の意図する環境において、セキュリティ機能の脆弱性が悪用され得ないことについて記述する。そのため、保証要件 AVA_VLA.2 は満たされる。

8.4.　PP 主張根拠

本 ST が参照する PP はない。

（　最終ページ　）