Si-R Security Software V01.00
セキュリティターゲット

２００７年７月１２日

富士通株式会社

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FUJITSU

—— 目 次 ——

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FUJITSU

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FUJITSU

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

＜表目次＞

＜図目次＞

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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　　：Si-R Security Software V01.00 セキュリティターゲット
バージョン：第 1.29 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　　：Si-R Security Software
バージョン：V01.00
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/IEC15408:2005
補足-0512 適用

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

1.2. ST 概要

本 ST は、富士通株式会社が提供する IP アクセスルータ GeoStream Si-R シリーズ（以下、Si-R と記載）に搭載されているソフトウェアのセキュリティ機能について記述している。

「Si-R Security Software V01.00」として実装するセキュリティ機能は、以下の通りである。

- 暗号化した利用者パケットデータの送受信を行う仮想的な通信路を開設する「暗号鍵交換機能」
- 暗号通信を行う通信相手との間で送受信されるパケットデータの暗号化／復号を行う「IPsec 暗号制御機能」
- 正当な人物のみに、Si-R の環境設定を行えるようにする「運用支援機能」

Si-R 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。Si-R 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 拡張

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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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
- ISO/IEC 15408:2005 Information Technology -Security techniques-Evaluation criteria for IT Security -Part1
- ISO/IEC 15408:2005 Information Technology -Security techniques-Evaluation criteria for IT Security -Part2
- ISO/IEC 15408:2005 Information Technology -Security techniques-Evaluation criteria for IT Security -Part3

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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。コンポーネントと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。

■ Si-R

富士通製 IP アクセスルータ GeoStream Si-R シリーズ。

Si-R は、処理性能やネットワークポート数の違いにより複数のモデルが提供されている。

本 ST では、GeoStream Si-R シリーズを示す名称として、「Si-R」を使用する。

■ ネットワーク機器

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

PC、プリンタ、複合機、ネットワークデータストレージに搭載されている。

■ 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。

本 ST では、製品のコンソールポートと専用ケーブルで接続された PC を示す。

管理者は、管理コンソール上のターミナルソフトでコマンドを入力し、TOE の操作を行う。

■ コンソールポート

RS-232C の物理インタフェースを示す。

Si-R 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

■ ネットワークポート

IEEE802.3 の物理インタフェースを示す。

Si-R では、内部ネットワーク及び外部ネットワーク用のネットワークポートを搭載している。

■ ネットワークセグメント

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。

■ ハードウェア制御プログラム（ドライバ）

基本ソフトウェアにより管理され、Si-R 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及び暗号処理専用チップ）の制御を行うプログラム。

■ 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。

■ 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。

■ I/F（インタフェース）

Si-R が提供する物理的、論理的な接続箇所を示す。

物理的なインタフェースとしては、シリアル、ＬＡＮインタフェースが該当する。

論理的なインタフェースとしては、ソフトウェア製品のモジュールを構成するサブシステム間のインタフェースが該当する。

■ 事前共有秘密鍵

鍵交換機能で使用する暗号鍵であり、通信相手との間で事前に共有する秘密鍵を示す。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

■ 演算チップ

本 TOE と同じ筐体に実装された計算処理に特化したハードウェアであり、TOE がデータ暗号鍵の生成、利用者パケットデータの暗号化／復号及びハッシュ値生成の際に行う大量の計算を補助している。

■ DH グループ

暗号鍵を生成する際に使用するパラメータが取り得る値の範囲を示す。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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
- IPv6 : Internet Protocol Version 6
- IKE : Internet Key Exchange
- IPsec : IP Security Protocol
- AH : Authentication Header
- ESP : Encapsulating Security Payload
- SA : Security Association
- RIP : Routing Information Protocol
- BGP4 : Border Gateway Protocol version 4
- OSPF : Open Shortest Path First
- ECMP : Equal Cost Multi Path
- VoIP : Voice over Internet Protocol
- VLAN : Virtual LAN
- MPLS : Multi Protocol Label Switching
- WFQ : Weighted Fair Queueing
- SNMP : Simple Network Management Protocol
- VRRP : Virtual Router Redundancy Protocol
- SSH : Secure Shell または Secure Socket Shell
- RADIUS : Remote Authentication Dial In User Service

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

Si-R は、異なるネットワークセグメント間の接続を行うルータ機器である。

TOE は、鍵交換機能と連携する IPsec 暗号制御機能により、高度なセキュリティを実現するルータ機器の機能である。TOE の種別は、ネットワーク環境において異なるネットワークセグメント間を流れる利用者のパケットデータを保護する機能と、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

本 TOE は、異なるネットワーク間の接続を行う Si-R に搭載され、通信相手（別ドメインのルータ機器）との間で送受信される利用者のパケットデータを保護するために利用される。

本 TOE では、通信相手との間に利用者パケットデータの送受信を行なう仮想的な通信路（以降、トンネルと表記）を開設し、そのトンネルの中を通過するパケットデータの暗号化／復号を行う。

なおトンネルは、複数のプロトコルで構成された IPsec で開設される。

トンネルの開設及び利用者パケットデータの暗号化／復号の際には、本 TOE と同じ筐体に搭載された「演算チップ」（IT 環境として動作、後述）を使用している。

「演算チップ」は、トンネルの開設及び利用者パケットデータの暗号化／復号の際に必要となる各種の計算を補助するために採用されている。

なお TOE は「演算チップ」が、トンネルの開設及び利用者パケットデータの暗号化／復号を円滑に行うように制御を行う。

上記の事から TOE の利用者は、信頼できるプロトコルにより、定められた通信相手と保護されたパケットデータで通信を行うことができる。

また本 TOE は、正当な人物にのみ Si-R の設定を行うことを可能とする機能を提供するため、TOE の利用者は、セキュアに Si-R の運用を行うことができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.2.2. TOE の利用環境

TOE を搭載する Si-R は、図 2.1 のように異なるネットワークセグメントの境界に設置されるルータ機器であり、ルータ間でパケットデータの通信を行う。

ルータで接続された外側のネットワーク（例えばインターネットの場合）は、多数のサーバを経由して通信が行われており、パケット目的地までの経路は、パケットデータに対する機密性、完全性が保証されないネットワークとなっている。

本 TOE は、Si-R と Si-R の通信相手が管理するネットワーク間を流れる利用者のパケットデータを保護するため、暗号化通信のプロトコルとして IPsec を実装している。

IPsec は、複数プロトコルの集合を示す名称であり、通信相手との間に利用者パケットデータの送受信を行なうトンネルを開設する暗号鍵交換、そのトンネルの中を通過するパケットデータの暗号化／復号を行う機能に大別される。

各機能は複数の動作モードを提供しているが、本 ST では、事前共有秘密鍵認証方式かつ、メインモードを使用した鍵交換を行いかつ、トンネルモードによる認証付き暗号化通信を利用環境として想定している。

Si-R の通信相手は、あらかじめ定義された通信相手に限定しない。Si-R と未定義の通信相手が管理するネットワークの間を流れる利用者のパケットデータは、保護されない。

また Si-R の通信相手は、Si-R に限定しない。同等の暗号化通信プロトコルを持つルータ機器であれば、本 TOE が提供する外部ネットワークにおける脅威への対抗機能を利用する事ができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

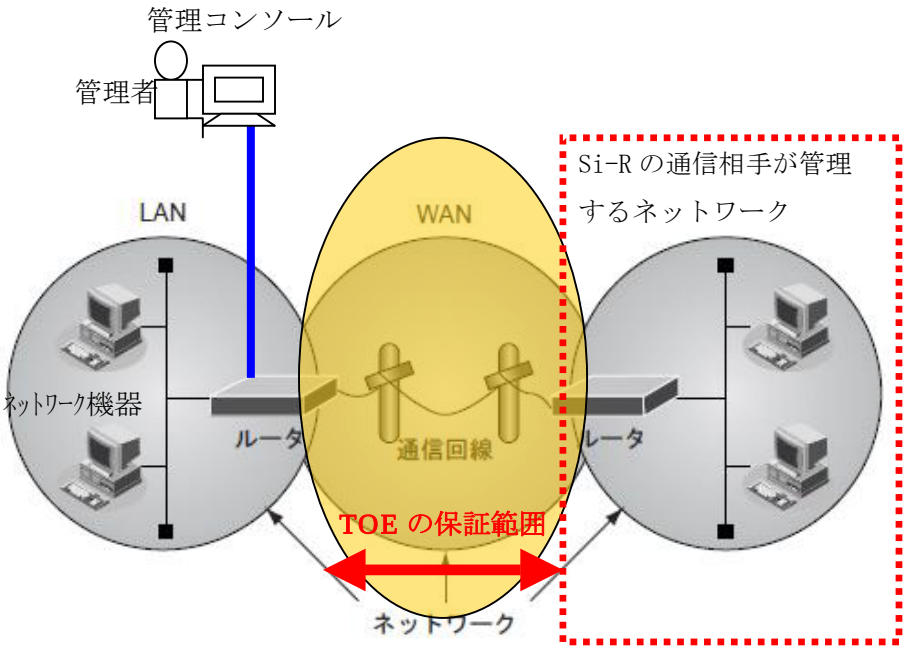

図 2.1 利用環境（概念）

【項目説明】

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ネットワーク機器であり、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、他ネットワークセグメントとの接続に使用される外部ネットワークインタフェースを持っている。

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。

ネットワーク機器

Si-R に接続可能な機器の総称であり、PC、プリンタ、複合機、ネットワークデータストレージなどを示す。

Si-R に接続されるネットワーク機器は、同じネットワークに接続されたネットワーク機器間及び外部ネットワークとの通信のみ行う。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.2.3. TOE の関連者

本 TOE の関連者としては、以下を想定している。

関連者	役割に許可された操作内容
組織の責任者	Si-R を運用する組織の責任者である。 組織の責任者は、Si-R 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。
管理者	管理者権限を有し、Si-R の構成変更／運用操作のすべての運用操作が可能である。 Si-R に対するすべての操作権限を持つ人物であるため、信頼できる人物であることが求められる。
利用者	内部ネットワークセグメントにネットワーク機器を接続して、同一のネットワークセグメント間及び「信頼できないネットワーク」を介して、異なるネットワークセグメント間との通信を行なう者である。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.2.4. TOE の利用方法

TOE の関連者毎の利用方法を以下に示す。

関連者	利用方法
管理者	【運用支援機能の操作】 管理コンソール上でターミナルソフトを起動し、TOE の運用支援機能にアクセスする。 運用支援機能が提供する識別認証の機能により正当な管理者である事が確認された後、TOE を利用する事ができる。
利用者	【運用支援機能の操作】 利用者に対し、運用支援機能は提供されない。 【通信の利用】 内部ネットワークセグメントに接続されたネットワーク機器から、Si-R 経由で外部ネットワークセグメントとの通信を行う。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.3. TOE 構成

2.3.1. TOE の物理的構成

TOE は、図 2.2 の破線に囲まれた装置（Si-R）に搭載されているソフトウェアである。

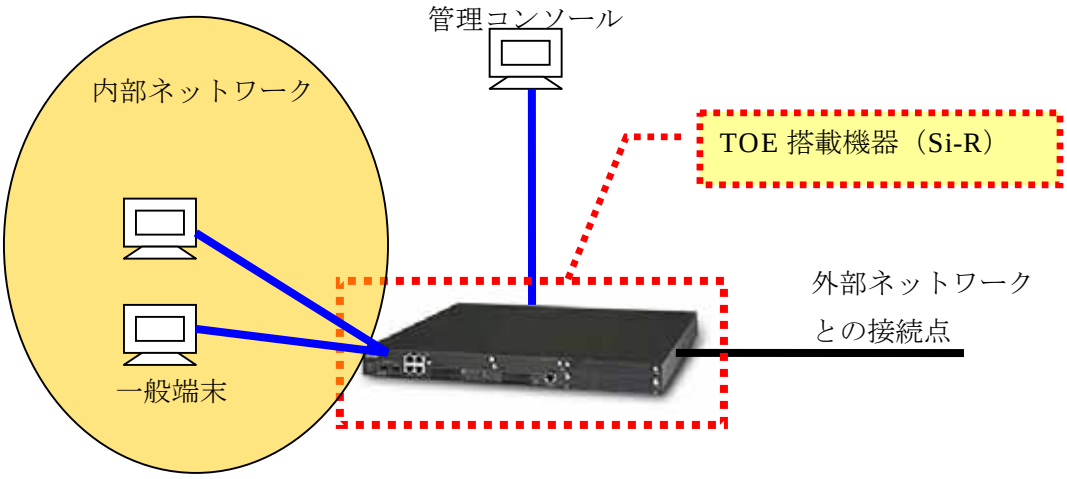

図 2.2 TOE の物理構成（装置外観）

【TOE 範囲について】

Si-R は、異なるネットワークセグメント間を接続するルータ機器であり、単純なパケットルーティングから、IPsec プロトコルに基づく暗号通信までネットワーク接続に関する多くの機能を実装している。

Si-R に関係する資産の内、特に重要な資産は Si-R に接続されたネットワーク機器と外部ネットワーク間で送受信されている「パケットデータ」である。従って本 TOE では、このパケットデータを保護対象資産とする。

従って本 ST では、Si-R が提供する機能の中で、上記パケットデータの保護と関係する部分（トンネルの開設処理部、パケットデータの暗号化／復号部及び環境設定部）を TOE の範囲としている。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

TOE 本体の物理的構成を図 2.3 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。

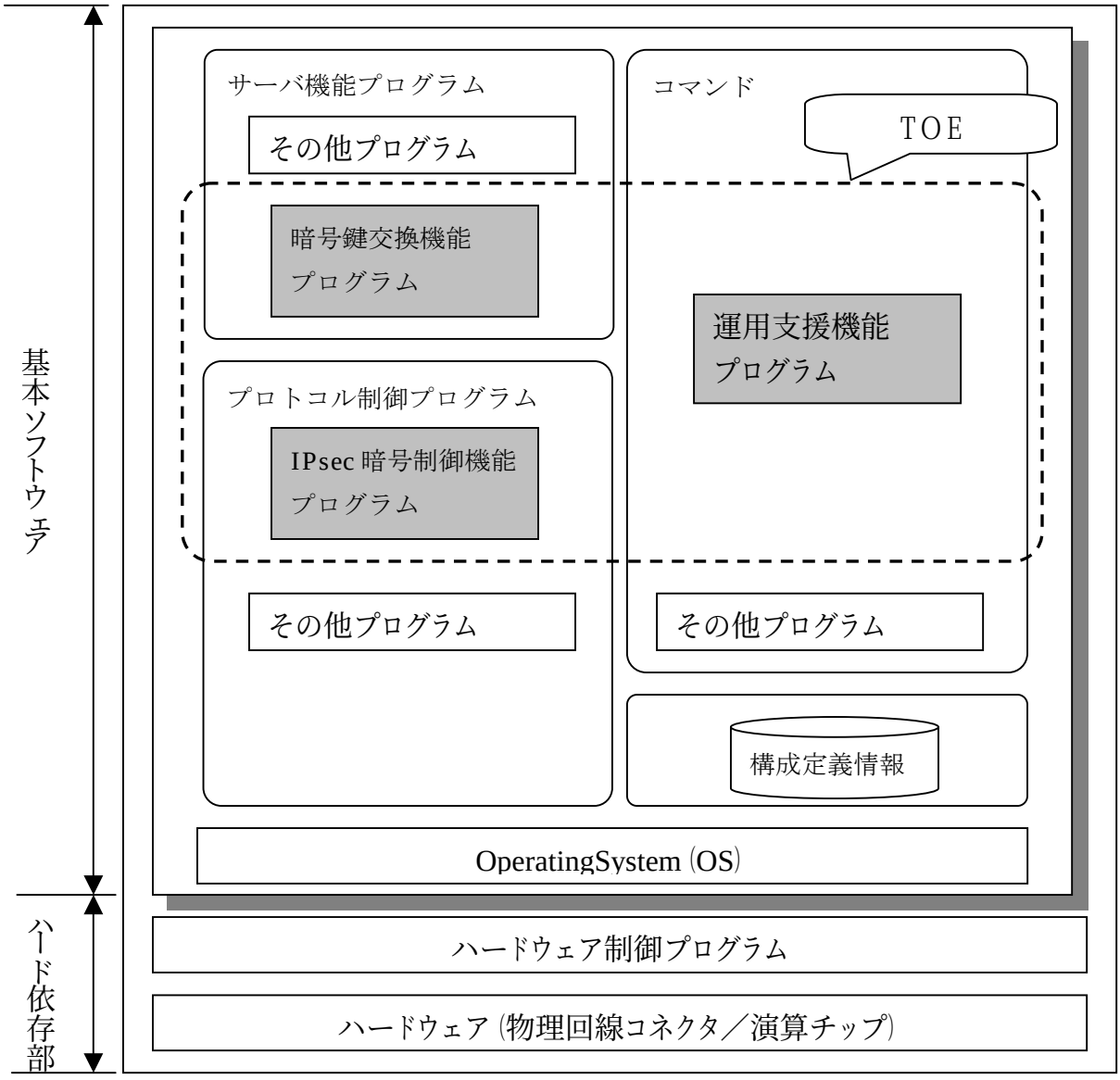

図 2.3 TOE の物理構成（装置内部）

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

【図 2.3 の説明】

TOE を搭載する Si-R は、処理性能やネットワークポート数の違いにより複数のモデルが提供されており、内部には各種プログラムが動作している。

Si-R の搭載ソフトウェアは、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、モデル間に存在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、本 ST で記述するセキュリティ機能は、「基本ソフトウェア」のソフトウェアとして、実装されている。

図 2.3 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。

【基本ソフトウェア】

■ サーバ機能プログラムの暗号鍵交換機能プログラム

サーバ機能プログラムは Si-R 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、暗号鍵交換機能を制御するプログラムである。

このプログラムは、通信相手との間に利用者パケットデータの送受信を行なうトンネルを開設する制御を行う。

なお暗号鍵交換プログラムは、利用者のパケットデータを暗号化／復号する際に使用するデータ暗号鍵の生成パラメータを鍵交換プロトコル（IKE：RFC2409）に基づいて通信相手と共有し、IT 環境である演算チップを使用して、データ暗号鍵の生成、ハッシュ値の生成を制御する。

なお、暗号鍵交換機能では、事前共有秘密鍵認証方式を使用して、データ暗号鍵を生成するパラメータを通信相手と共有する。

■ プロトコル制御プログラムの IPsec 暗号制御機能プログラム

プロトコル制御プログラムは Si-R が提供するプロトコル制御機能のプログラム群である。プログラム群の中で TOE は、IPsec 暗号制御機能を制御するプログラムである。

このプログラムは、利用者のパケットデータを送信する際に、処理対象のパケットデータが、暗号化の対象であるかを各種の条件から判断し、処理対象であった場合は、IT 環境である演算チップに暗号化を行わせるためのパラメータ設定を制御する。

また利用者のパケットデータを受信する際に、処理対象のパケットデータが、復号の対象であるかを各種の条件から判断し、処理対象であった場合は、IT 環境である演算チップに復号を行わせるためのパラメータ設定を制御する。

なお受信したパケットデータの復号時には、パケットデータの改ざん検知を行っている。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

■ コマンドの運用支援機能プログラム

コマンドは Si-R 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、暗号鍵交換機能プログラム及び IPsec 暗号制御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 Si-R のコンソールポートに接続して利用するか、Si-R の TELNET サーバ機能及び 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。

■ 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 の暗号鍵交換機能プログラム以外のプログラムも含まれる。暗号鍵交換機能プログラム以外のプログラムの一覧を表 2-1 に示す。

■ プロトコル制御プログラムのその他プログラム

プロトコル制御機能プログラムには、TOE の IPsec 暗号制御機能プログラム以外のプログラムも含まれる。IPsec 暗号制御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。

■ 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

【ハード依存部】

■ ハードウェア制御プログラム

基本ソフトウェアから制御され、ハードウェアの制御を行うプログラムである。

Si-R 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。

■ ハードウェア(物理回線コネクタ／演算チップ)

本 TOE が動作するハードウェア装置である。

通信相手とのトンネル開設の際に必要となる演算、利用者パケットの暗号化／復号処理及びハッシュ値生成を行う演算チップもハードウェアに含まれる。

表 2-1 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	SSH サーバ機能プログラム
4	SFTP サーバ機能プログラム
5	ProxyDNS プログラム
6	DHCP プログラム
7	syslog プログラム
8	マルチキャストプログラム
9	TIME/SNTP プログラム
10	SNMP プログラム
11	動的定義反映プログラム
12	スケジュール制御プログラム
13	セッション監視プログラム
14	MAC アドレス認証プログラム
15	AAA 制御プログラム
16	RADIUS サーバ制御プログラム
17	ルーティング制御プログラム(RIPv1, RIPv2, BGP4, OSPFv2, OSPFv3, RIPng)
18	STP 制御プログラム
20	HTTP サーバ機能プログラム
21	DVPN サーバ機能プログラム

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

表 2-2 プロトコル制御機能のプログラム一覧

	名称
1	TCP 制御
2	UDP 制御
3	IPv4/IPv6 制御
4	ブリッジ
5	VLAN
6	MPLS
7	フィルタ
8	NAT
9	QoS 制御

TOE である「Si-R Security Software V01.00」は、Si-R570 に基本ソフトウェア V33 を搭載した環境で検証を行った。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.3.2. TOE の論理的構成

表 2-3 に利用者パケットデータの暗号化／復号を提供する機能の構成要素一覧を示す。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”を示す。

表 2-3 セキュリティ機能の構成一覧と TOE 対象

No.	名称	TOE
1	運用支援（IPsec 環境設定コマンド）機能	○
2	暗号鍵交換機能	○
3	IPsec 暗号制御機能	○
4	ハードウェア演算機能	“IT 環境”

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.4. TOE のセキュリティ機能

本節では、「2.3.2 TOE の論理的構成」に示した、TOE の機能について詳細を説明する。

2.4.1. **暗号鍵交換機能**

「暗号鍵交換機能」は、鍵交換プロトコル（IKE：RFC2409）に準拠した実装を行っており、通信相手とのトンネル開設の際に必要となる「データ暗号鍵」の生成に必要となるパラメータを通信相手と安全に共有する機能を提供している。

鍵交換プロトコル（IKE：RFC2409）には、複数のモードが規定されているが、本機能ではメインモードとクイックモードの組み合わせによる動作を行う。

共有されたパラメータは、「暗号鍵交換機能」が制御する演算チップに受け渡され、「データ暗号鍵」を生成する。

「データ暗号鍵」は、「運用支援機能（IPsec 通信環境設定）」で設定された条件に従って定期的に更新する。本機能では、トンネルが生成されてからの経過時間及びトンネルを利用したパケットデータの総和が設定された条件を満たした場合に、鍵の更新処理が動作する。

なお通信相手との暗号通信は、利用者のパケットデータに対して「データ暗号鍵」を使用した暗号化／復号操作を行うトンネル（仮想的な通信路）を開設する事により、実現している。トンネルは、「運用支援機能（IPsec 通信環境設定）」で設定された条件に従って開設される。本機能では、通信対象機器の IP アドレス、暗号化されたパケットデータのフォーマット、使用する暗号アルゴリズム及び認証アルゴリズムを条件として設定する。

「暗号鍵交換機能」は、「事前共有秘密鍵認証方式」を使用して、「データ暗号鍵」を生成するパラメータを通信相手と共有するため、通信相手との間で同じ事前共有秘密鍵を共有し、ルータ機器に設定する必要がある。

この事前共有秘密鍵は、第三者に漏洩しない手順で共有する運用を行いかつ、本装置の管理者及び通信相手は共有後も漏洩しない運用を行わなければならない。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.4.2. IPsec 暗号制御機能

IPsec 暗号制御機能は、Si-R 部ネットワークインタフェースと暗号鍵交換機能により開設されたトンネルを介して、通信相手との間で送受信される利用者パケットデータの暗号化／復号／改ざん検知／認証（以後、暗号操作と記載）の実施に必要なパラメータ制御と IT 環境である演算チップへのパラメータを設定する機能である。

本機能は、パケットデータの IP アドレス及びトンネルの開設状態をもとにパケットデータが暗号操作の対象であるか判断を行う。

暗号操作に使用するパラメータは、開設されたトンネル毎に異なるため、暗号操作の対象であった場合は、使用するトンネルに応じたパラメータに従った暗号化／復号／ハッシュ値生成の各演算処理を、演算チップに要求する。

[暗号化／復号演算をソフトウェアで行わない理由]

パケットデータに対する暗号操作は、複雑かつ大量の演算処理が必要となるため、すべての演算をソフトウェアで実施した場合、著しい性能劣化が発生する事が予想される。

Si-R では、この問題に対処するため、演算処理が必要となる部分を IT 環境である演算チップで高速に処理を行ない、性能劣化を抑止している。

IPsec 暗号制御機能の動作概要を図 2.4 及び表 2-4 に示す。

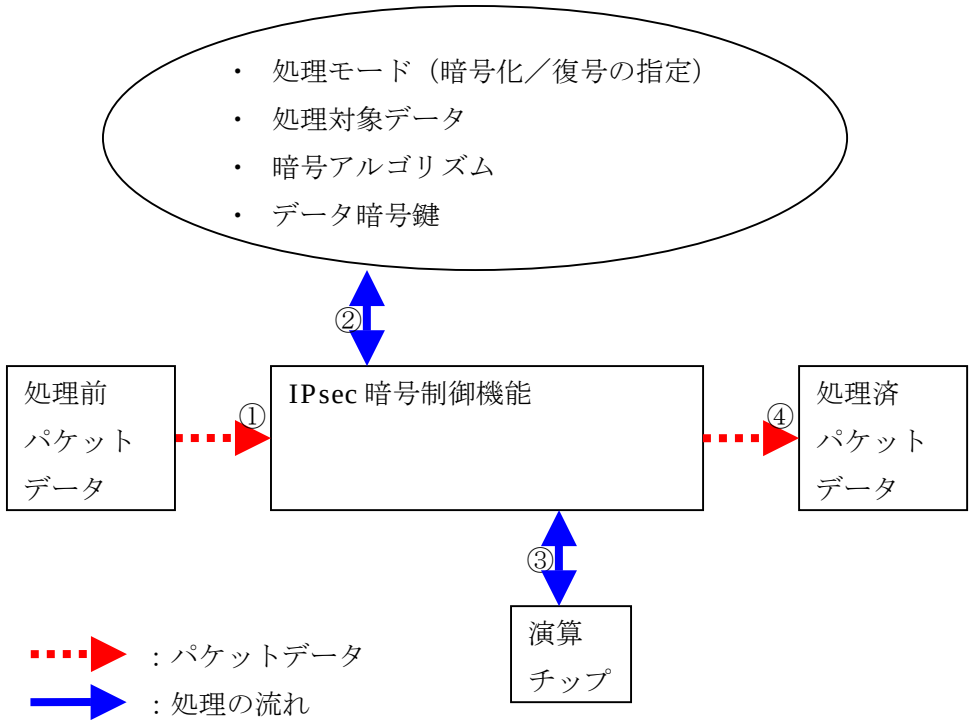

図 2.4 IPsec 暗号制御機能の動作概要

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

表 2-4 IPsec 暗号制御機能の動作概要

No.	動作
①	Si-R の内部または外部ネットワークセグメントから、利用者のパケットデータ（以降、処理前パケットデータ）が到着する。
②	WAN 側から届いた処理前パケットデータが暗号操作の対象であった場合、パケットの処理に必要となる情報を準備する。 【送信時】 暗号化／認証情報の付加に必要な制御情報を「運用中構成定義」及び Si-R の実メモリ上の暗号鍵格納領域から取り出す。 【受信時】 復号／改ざん検知／認証に必要な制御情報を「運用中構成定義」及び Si-R の実メモリ上の暗号鍵格納領域及び処理前パケットデータから、取り出す。
③	暗号操作で行う大量の計算を高速に処理するため、Si-R に搭載されている「演算チップ」に、②により準備した情報を設定する。
④	IPsec 暗号制御機能で処理された処理済パケットデータを、Si-R の外部または内部のネットワークセグメントに転送する。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.4.3. 運用支援機能

運用支援機能は、Si-R の環境設定情報が保存されている「構成定義情報」を設定、更新、参照する機能である。

アクセス対象資源である「構成定義情報」は、Si-R の動作に関わる各種設定情報（利用者のパスワード、ネットワーク定義、IPsec 通信を行うための設定情報）が記録された定義情報であり、シリアルインタフェースで接続された管理コンソールから、コマンドを使用して操作を行う。

管理者は、管理コンソール接続時に表示されるログインプロンプトで識別認証を行い、正当な管理者である事が確認された場合、運用支援機能が提供するコマンドの操作が許可されるため、管理者は本装置に対する環境設定を行う。

環境設定後は、ログアウトを行ない運用支援機能の使用を終了する。

【コマンドによる運用手順】

コマンドによる運用手順を以下に示す。

1）本装置にログインする

2）運用支援機能が提供するコマンドを実行して運用管理を行う

3）ログアウトする

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

2.5 IT 環境のセキュリティ機能

本 TOE が依存する、IT 環境の機能は以下の通りである。

2.5.1 ハードウェア演算機能

本機能は、TOE からの要求により、暗号鍵交換機能が制御を行う通信相手とのトンネル開設で必要となる一部の演算及び IPsec 暗号制御機能からの要求により、パケットデータの暗号化／復号及びハッシュの演算を行なう機能である。

2.6 保護対象となる資産

保護対象資産	説明
IPsec通信を行う通信相手との間で暗号化された状態で送受信される利用者のパケット	本装置の内部ネットワークセグメントの利用者及び通信相手の内部ネットワークセグメントの利用者が送信するパケットデータに対し、「改ざん」、「漏洩」への保護が必要となる。

上記の保護対象資産を保護する上で、TOE セキュリティ機能に関連する情報を以下に示す。

- 管理コンソールにおける認証情報(パスワード)
- 鍵交換機能の動作に必要な環境設定情報
- IPsec 暗号制御機能の動作に必要な環境設定情報

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

TOE には、意図する使用方法及び使用環境に関して、以下の前提条件が存在する。

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.PLACE（設置場所）

本装置は、限られた人物のみが入室できる区画（データセンタ、サーバルームなど）に設置される。

A.KEY_SHARE（事前共有秘密鍵）

管理者は、暗号鍵交換機能が使用する事前共有秘密鍵を通信相手と共有する運用を行う。事前共有秘密鍵は推測されにくい十分な強度を持つ値を使用し、またこの通信相手に、事前共有秘密鍵を第三者に漏洩しない運用を求める。

A.SERVICE（提供するサービスの前提）

TOE が動作する Si-R 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。

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

A.PASSWORD（識別認証のパスワード）

管理者は、TOE が動作する Si-R の管理コンソールの識別認証に使用するパスワードに、8 文字以上のパスワードを使用する。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

A.DATA_KEY（データ暗号鍵）

TOE は、利用者データの暗号化／復号に使用するデータ暗号鍵に、128 ビット以上の鍵長を持つ暗号アルゴリズムを指定する。

また使用する暗号アルゴリズム種別には、電子政府推奨暗号のアルゴリズムである 3DES または AES を指定する。

A.CONSOLE（管理コンソール）

TOE が動作する Si-R 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。

A.IPSEC&IKE_SETUP（暗号通信モード）

管理者は、TOE の暗号通信のモードとして、事前共有秘密鍵認証方式かつ、メインモードを使用した鍵交換を行いかつ、トンネルモードによる認証付き暗号化通信の環境を設定する。

また鍵交換クイックモードの認証アルゴリズムには、HMAC-MD5 または HMAC-SHA1 を使用する環境を設定する。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

3.2. 脅威

TOE には、意図する使用方法及び使用環境に関して、以下の脅威が存在する。

本 TOE では、低レベルの攻撃者を想定する。

T.PACKET_TAP（パケットの盗聴）

外部ネットワークインタフェースを介して送受信されるパケットデータは、攻撃者により盗聴され、その通信内容が漏洩する可能性がある。

T.PACKET_MODIFY（パケットの改ざん）

外部ネットワークインタフェースを介して送受信されるパケットデータは、攻撃者により改ざんされ、その通信内容が改変される可能性がある。

T.MECHA_AUTH（通信機器のなりすまし）

攻撃者が所有するルータ機器からの IPsec による通信接続要求を受け入れ、TOE 利用者のパケットデータの内容が漏洩する。

または攻撃者の所有するルータ機器に対し、IPsec による通信接続要求を行い、TOE 利用者のパケットデータの内容が漏洩する可能性がある。

3.3. 組織のセキュリティ方針

TOE には、意図する使用方法及び使用環境に関して、以下に示す組織のセキュリティ方針が存在する。

OSP.TOE_MNG（管理機能の制限）

TOE の運用環境に関わらず、本装置に対する管理行為は、管理者のみに制限しなければならない。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

本節は、脅威に対抗し、組織のセキュリティ方針を実現するための TOE のセキュリティ対策方針を示す。

O.IPSEC_CHANNEL（IPsec 通信チャネルの制御）

TOE は、外部ネットワークインタフェースを介して送受信されるパケットデータのため、IPsec 通信を行う通信チャネルを提供する。

O.TSFD_MNG（運用支援機能）

TOE は、TSF の動作に係わるデータに対する操作、及び TSF の動作に係わる IT 環境の機能のデータに対する操作を管理者のみに可能とする。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

4.2. 環境のセキュリティ対策方針

本節は、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。

脅威に対抗するための技術的な環境のセキュリティ対策方針を以下に示す。

OE.CRYPTO（データの暗号化）

IT 環境は、外部ネットワークインタフェースを介して送信するパケットデータの漏洩を防止するために、パケットデータの暗号化で必要となる演算（「データ暗号鍵」の生成、パケット暗号化時の計算）を行なう。

なおパケットデータの暗号化に使用する「データ暗号鍵」は、通信相手と改ざんや盗聴の無い、安全な方法で共有する仕組みで共有する。

OE.DETECT_MODIFY(パケットデータの改ざん検知)

IT 環境は、外部ネットワークインタフェースを介して受信されるパケットデータの改ざんを検知するため、照合に用いるハッシュ値の生成と受信パケットデータに付加されているハッシュ値との照合を行う。

OE.PRE_SHARE_KEY（事前認証秘密鍵の共有）

IT 環境は、通信相手が環境設定で定義された通信相手であることを確認するため、識別と認証を行う。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

前提条件を実現するための非技術的な環境のセキュリティ対策方針を以下に示す。

OE.TRUST（管理者及び利用者への教育）

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.SERVICE（サービスの停止）

管理者は、以下に示すリモートからの運用支援機能のサービスや、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.PASSWORD（パスワード長）

管理者は、TOE が動作する Si-R の管理コンソールの識別認証に使用するパスワードに、8 文字以上のパスワードを設定する。

OE.DATA_KEY（データ鍵）

管理者は、IPsec 通信で使用する暗号鍵の条件に、鍵長が 128 ビット以上の暗号鍵を生成する暗号アルゴリズムを指定する。また使用する暗号アルゴリズム種別には、電子政府推奨暗号のアルゴリズムである 3DES または AES を指定する。

OE.KEY_SHARE（事前共有秘密鍵の共有）

管理者は、暗号鍵交換機能が、事前共有秘密鍵認証方式を使用するよう環境設定を行い、事前共有秘密鍵を推測されにくい十分な強度を持つ値を使用しかつ、第三者に漏洩させない運用を行った上で、通信相手と共有する。

本装置の管理者及び通信相手は、事前共有秘密鍵の共有後も第三者に漏洩させない運用を行う。

OE.CONSOLE（利用者の制限）

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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

OE.PLACE（設置場所）

管理者は、本装置を限られた人物のみが入室できる区画（データセンタ、サーバルームなど）に設置しなければならない。

OE.IPSEC&IKE_SETUP（暗号通信モード）

管理者は、TOE の暗号通信のモードとして、事前共有秘密鍵認証方式かつ、メインモードを使用した鍵交換を行いかつ、トンネルモードによる認証付き暗号化通信の環境を設定しなければならない。

また鍵交換クイックモードの認証アルゴリズムには、HMAC-MD5 または HMAC-SHA1 を使用する環境を設定しなければならない。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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示す。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

本 ST では、「TSF 間高信頼チャネルの操作」と「TSF 間高信頼チャネルの実装」に関する機能要件コンポーネントとして CC パート 2 で規定されている FTP_ITC.1 を拡張し FTP_ITX.1 及び FTP_ITZ.1 を設けている。これ以外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直接使用している。

TSF 間高信頼チャネルの操作とは、高信頼チャネルの操作（通信相手機器の識別、チャネルの開設と維持）に関わる一連の処理を制御することである。

FTP_ITX.1 TSF 間高信頼チャネルの操作

FTP_ITX.1　TSF間高信頼チャネルの操作は、高信頼チャネルの操作に関わる一連の処理を制御する。

管理：FTP_ITX.1

以下のアクションは FMT における管理機能と考えられる:

a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定。

監査：FTP_ITX.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 高信頼チャネル機能の失敗。

b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。

c) 基本: 高信頼チャネル機能のすべての使用の試み。

d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

下位階層: なし

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FTP_ITX.1.1

TSF は、[選択: TSF、リモート高信頼 IT 製品]が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

[選択: *TSF*、*リモート高信頼 IT 製品*]

- TSF

FTP_ITX.1.2

TSF は、[割付: 高信頼チャネルが要求される機能のリスト]のために、高信頼チャネルを介して通信を開始しなければならない。

[割付: *高信頼チャネルが要求される機能のリスト*]

- 暗号鍵交換ネゴシエーションパケットの送受信
- 利用者パケットの送受信

依存性: FTP_ITZ.1 TSF間高信頼チャネルの実装

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

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＞
管理者を代行するTOEのスレッド

＜オブジェクト＞
構成定義情報。但し、構成定義情報内のTSFに関係しない以下の情報部のみ対象とする。

- データ暗号鍵の鍵長
- 暗号アルゴリズム
- 認証アルゴリズム
- DHグループ
- TELNET サーバ機能の設定情報
- SSH ログインサーバ機能の設定情報
- HTTP サーバ機能の設定情報
- FTP サーバ機能の設定情報
- SSH FTP サーバ機能の設定情報
- 通信対象機器の識別認証情報（IP アドレス、事前共有秘密鍵）

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

＜SFPで扱われるサブジェクトとオブジェクト間の操作＞
設定と変更

［割付：アクセス制御SFP］
運用条件操作制御設定 SFP

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層：なし

FDP_ACF.1.1

TSFは、以下の[割付：*示されたSFP下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP関連セキュリティ属性、またはSFP関連セキュリティ属性の名前付けされたグループ*]に基づいて、オブジェクトに対して、[割付：*アクセス制御SFP*]を実施しなければならない。

[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
構成定義情報	無し	無し

[割付：アクセス制御SFP]
運用条件操作制御設定 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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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]

サブジェクトである管理者権限を有するTOEのスレッドに、オブジェクトである構成定義情報の設定と変更を許可する。

FDP_ACF.1.3

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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FIA_UAU.2 アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1

運用支援機能は、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、各利用者に認証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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FIA_UID.2 アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1

運用支援機能は、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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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*]

- 高信頼チャネル通信機能
- 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
高信頼チャネル通信機能	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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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*]

- 管理者のログインパスワード
- 高信頼チャネルの更新条件（鍵の有効期間、転送パケット量の閾値）
- 高信頼チャネルの動作タイプ（自動鍵交換方式、メインモード、認証付き暗号化方式、トンネリング）
- 高信頼チャネルの対象範囲（ネットワークアドレスのレンジ）

[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
管理者のログインパスワード	・改変 ・問い合わせ
高信頼チャネル通信機能の更新条件	・改変 ・[割付: その他の操作]　設定
高信頼チャネル通信機能の動作タイプ （自動鍵交換方式、メインモード、 認証付き暗号化方式、トンネリング）	・改変
高信頼チャネルの対象範囲 （ネットワークアドレスのレンジ）	・[割付: *その他の操作*]　登録 ・改変

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

[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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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*]

- 運用支援機能における管理者のログインパスワードの設定、改変、及び問い合わせ機能
- 事前共有秘密鍵の設定及び改変機能

依存性： なし

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FPT_SEP.1　　TSF ドメイン分離

下位階層：なし

FPT_SEP.1.1

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

FPT_SEP.1.2

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

依存性：なし

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

5.1.2. TOE セキュリティ保証要件

本 ST で主張する評価保証レベルは、EAL4 に ALC_FLR.1 を追加である。

EAL4 に ALC_FLR.1 を追加に対応する TOE セキュリティ保証要件を『表 5-1 TOE セキュリティ保証要件一覧』に示す。

表 5-1 TOE セキュリティ保証要件一覧

保証クラス	保証要件	
構成管理	ACM_AUT.1	部分的な CM 自動化
	ACM_CAP.4	生成の支援と受入手続き
	ACM_SCP.2	問題追跡の CM 範囲
配付と運用	ADO_DEL.2	改変の検出
	ADO_IGS.1	設置、生成、及び立上げ手順
開発	ADV_FSP.2	完全に定義された外部インタフェース
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_IMP.1	TSF の実装のサブセット
	AVD_LLD.1	記述的下位レベル設計
	ADV_RCR.1	非形式的対応の実証
	ADV_SPM.1	非形式的な TOE セキュリティ方針モデル
ガイダンス文書	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート	ALC_DVS.1	セキュリティ手段の識別
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
	ALC_TAT.1	明確に定義された開発ツール
	ALC_FLR.1	欠陥の修正
テスト	ATE_COV.2	カバレージの分析
	ATE_DPT.1	テスト：上位レベル設計
	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_MSU.2	誤使用
	AVA_SOF.1	TOE セキュリティ機能強度
	AVA_VLA.2	脆弱性分析

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

5.1.3. 最小機能強度主張

TOE セキュリティ機能要件に対する最小機能強度は、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_UAU.2、FIA_SOS.1 であり、機能強度は SOF-基本である。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FTP_ITZ.1 TSF 間高信頼チャネルの実装

FTP_ITZ.1 TSF間高信頼チャネルの実装は、高信頼チャネルの実装に関わる一連の処理を制御する。

管理：FPT_ITZ.1

以下のアクションは FMT における管理機能と考えられる:

a) もしサポートされていれば、高信頼チャネルを要求するアクションの設定。

監査：FTP_ITZ.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである:

a) 最小: 高信頼チャネル機能の失敗。

b) 最小: 失敗した高信頼チャネル機能の開始者とターゲットの識別。

c) 基本: 高信頼チャネル機能のすべての使用の試み。

d) 基本: すべての高信頼チャネル機能の開始者とターゲットの識別。

下位階層: なし

FTP_ITZ.1.1

TSF は、それ自身とリモート高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

依存性: FTP_ITX.1 TSF間高信頼チャネルの操作

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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 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	暗号鍵交換機能	FTP_ITX.1
2	IPsec 暗号制御機能	FTP_ITX.1
3	運用支援機能	FDP_ACC.1 FDP_ACF.1 FIA_SOS.1 FIA_UAU.2 FIA_UAU.7 FIA_UID.2 FMT_MOF.1 FMT_MTD.1 FMT_SMF.1 FMT_SMR.1 FPT_RVM.1 FPT_SEP.1

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

6.1.1. 暗号鍵交換機能

暗号鍵交換機能は、通信相手との間に利用者パケットデータの送受信を行なう仮想的なトンネルを開設する一連の処理を実現した機能である。その際、利用者パケットデータの暗号化／復号を行なうための「データ暗号鍵」が通信相手との間で共有される。

「データ暗号鍵」は、暗号鍵交換機能が実装する「暗号鍵交換プロトコル（IKE：RFC2409)」により、通信相手と共有した鍵生成パラメータから、「Diffie-Hellman 鍵共有法（RFC2631 / ANSI X9.42)」に基づく演算処理を行い生成する。

「暗号鍵交換プロトコル」は、複数のモードが規定されているが、本 TOE の暗号鍵交換機能は、事前共有秘密鍵認証方式かつ、メインモードを使用した鍵交換を行いかつ、トンネルモードによる認証付き暗号化通信の環境を設定する。また鍵交換クイックモードの認証アルゴリズムには、HMAC-MD5 または HMAC-SHA1 を使用する環境を設定する。

本 TOE の暗号鍵交換機能では、トンネルを開設（「データ暗号鍵」の生成）する際に必要となる演算処理を、IT 環境のハードウェア（演算チップ）に依頼しているが、演算チップを動作させるための条件設定、鍵生成パラメータの受け渡し、演算結果の受け取りは、暗号鍵交換機能で制御を行っている。

なおデータ暗号鍵の鍵長は、「128 ビット」、「168 ビット」、「192 ビット」または「256 ビット」から選択される。（運用支援機能にて指定された暗号鍵長に従う。）

暗号鍵生成機能が提供する鍵交換の動作概要及び機能の実装箇所を表 6-2 に示す。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

表 6-2 鍵交換機能の動作概要

No	実装機能	動作
1	トンネルの開設	【トンネル開設条件の折衝】 TOE は通信相手との間で開設する仮想的なトンネルを、暗号鍵交換のメインモード及びクイックモードを使用して、開設する。 暗号鍵交換は、トンネル開設の諸条件（暗号アルゴリズム、ハッシュアルゴリズム、相手認証方式、セキュリティプロトコル、アルゴリズム、データ暗号鍵の有効期間、カプセル化モードなどのパラメータ）を通信相手と折衝し、合意する。 ※ トンネルの開設により、利用者パケットデータの暗号化／復号に使用する「データ暗号鍵」が生成される。
		【鍵生成】 （演算アシスト） TOE は運用によって、合意されたトンネル開設のパラメータ値を使用して、「データ暗号鍵」の素材を生成する。 ※ 「データ暗号鍵」素材の生成処理では、IT 環境である演算チップのサポートを受けている。
		【鍵生成】 （鍵加工） TOE は「鍵生成（演算アシスト）」が生成した鍵素材を加工して、「データ暗号鍵」を生成する。
2	監視	運用支援機能により、条件が設定されている「データ暗号鍵」の更新条件の監視を行う。 更新条件を満たした場合は、トンネルの開設処理を行う。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

6.1.2. IPsec 暗号制御機能

IPsec 暗号制御機能は、暗号鍵交換機能が開設したトンネルの中を流れる利用者パケットデータの暗号化／復号操作を IT 環境である演算チップを使用して行う機能である。

その際、演算チップにパケットデータの暗号化／復号に必要となる制御情報を設定する。

制御情報の設定は、暗号操作対象であるパケットデータの通信先から暗号／復号対象かを判断する段階と、制御情報及び演算対象のデータを演算チップに設定する段階に分けられる。以下に実現している機能を段階毎に分けて記載する。

［暗号／復号対象の判断］

暗号制御プログラムが制御しているパケットデータの IP アドレスが、SPD に登録されている場合、「SPD」「構成定義情報」「処理前パケットデータ」から「動作モード」「データ暗号鍵及び暗号鍵長」「鍵暗号鍵及び暗号鍵長」「使用する暗号アルゴリズムの種別」「使用する認証アルゴリズムの種別」の取り出し操作が許可される。

なお、「使用する暗号アルゴリズムの種別」に関しては、データ送信時、受信時により取り出し場所が異なる。以下に、それぞれの場合について示す。

(送信時)

暗号化の対象であった場合は、構成定義情報から「使用する暗号アルゴリズムの種別」の取り出しを行う。

(受信時)

復号の対象であった場合は、処理前パケットデータから「使用する暗号アルゴリズムの種別」の取り出しを行う。

「使用する暗号アルゴリズムの種別」以外の情報に関しては、パケットの送信／受信時に関わらず SPD から取り出しされる。

［制御情報の設定］

演算チップに対し、データ暗号鍵、使用する暗号アルゴリズムの種別、認証鍵、使用する認証アルゴリズムの種別、動作モード及び演算対象のデータを設定する。

設定に従い、演算チップは、パケットデータに対する演算処理（暗号化／復号／改ざん検知）を行う。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

6.1.3. 運用支援機能

運用支援機能は、Si-R の動作に関わる各種環境の設定を行う機能であり、管理者のみにコマンドによる以下の管理行為を提供する。

設定された情報は、Si-R に搭載された不揮発性メモリに存在する「構成定義情報」に格納される。

［運用支援機能の操作］

管理者が運用支援機能を使用して行うセキュリティ機能の環境設定を以下に示す。

(構成定義情報の内、TOE のセキュリティ機能に関わる情報の操作)

- ログインパスワードの設定、変更及び問い合わせ
  (管理者はパスワードとして、８文字以上の文字列を設定し、運用支援機能における識別認証機能を使用する。)
- 高信頼チャネルの諸条件の設定・改変
  (IPsec 通信を行うための「プロトコル、暗号アルゴリズム、認証アルゴリズム、チャネル有効期間、鍵交換の動作モード、暗号化方式」の管理を行っている。)
- 高信頼チャネルを利用する高信頼 IT 機器情報の登録・改変
  (IPsec 通信を行うための「通信相手機器の情報」の管理を行っている。)

(構成定義情報の内、TOE 以外の Si-R の設定に関わる情報の操作)

- TELNET サーバ機能の設定
- SSH ログインサーバ機能の設定
- HTTP サーバ機能の設定
- FTP サーバ機能の設定
- SSH FTP サーバ機能の設定
- CE 保守ログインの可否の設定
- 一般ユーザログインの可否の設定

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

[運用支援機能における識別認証機能]

本機能が提供する運用支援機能の操作を行う前に、管理者の識別認証を実施する。

識別認証は、ユーザ名とパスワードにより実施する。パスワードの情報（規則）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

なお運用支援機能が提供する環境設定を行うコマンドでは、コマンドのパラメータとして指定されるセキュリティプロトコルの種別、暗号アルゴリズムの種別、暗号鍵の有効時間、更新までのパケット量の閾値が、定められた範囲内であることをチェックしている。

値が定められた範囲内であった場合のみ、「構成定義情報」に格納される。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

6.2 セキュリティメカニズム

本 TOE が採用するセキュリティメカニズムは、運用支援機能における識別認証機能に適用されるパスワードメカニズムである。

6.3 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暗号鍵生成機能、運用支援機能における識別認証機能であり、機能強度は SOF-基本である。

6.4 保証手段

本節では、TOE の保証手段を説明する。表 6-3 に示すように、以下のセキュリティ保証手段は、表 5-1 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

表 6-3 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	ACM_AUT.1	－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
	CM 能力	ACM_CAP.4	
	CM 範囲	ACM_SCP.2	
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	－GeoStream Si-R シリーズ Si-R570 ご利用にあたって
開発	機能仕様	ADV_FSP.2	－Si-R シリーズ IPsec／IKE 機能仕様書 －Si-R/SR-S コマンド運用支援機能仕様書
	上位レベル設計	ADV_HLD.2	－Si-R シリーズ IPsec/IKE 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 －Si-R シリーズ IPsec/IKE 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 －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
	実装表現	ADV_IMP.1	
	下位レベル設計	ADV_LLD.1	
	表現対応	ADV_RCR.1	－Si-R 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	－Si-R Security Software V01.00 セキュリティポリシーモデル

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

TOE セキュリティ保証要件		コンポーネント	保証手段
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	－Geostream Si-R シリーズ Si-R570 ご利用にあたって －GeoStream Si-R シリーズ 機能説明書　V33 －GeoStream Si-R シリーズ コマンド設定事例集　V33 －GeoStream Si-R シリーズ コマンドリファレンス　V33 －GeoStream Si-R シリーズ コマンドユーザーズガイド　V33
	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 －FJ-WAN 利用基準
	ライフサイクル定義	ALC_LCD.1	
	ツールと技法	ALC_TAT.1	

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

TOE セキュリティ保証要件		コンポーネント	保証手段
	欠陥の修正	ALC_FLR.1	－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 －バックアップ管理規定 －ログインアカウント管理規定 －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 －エンタープライズ部門 設計変更処理規定 －欠陥修正対応規定 －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	ATE_COV.2	－Si-R シリーズ IS015408 カバレージ分析書 －Si-R シリーズ IS015408 深さ分析書 －IPsec／IKE 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
	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	－Si-R Security Software V01.00 脆弱性分析書
	TOE セキュリティ機能強度	AVA_SOF.1	
	脆弱性分析	AVA_VLA.2	

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

7. PP 主張

本 ST が適合する PP は存在しない。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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（脅威と対策方針)』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（脅威と対策方針）

―	脅威			組織のセキュリティ方針
TOE セキュリティ環境 / セキュリティ対策方針	T.PACKET_TAP	T.PACKET_MODIFY	T.MECHA_AUTH	OSP.TOE_MNG
O.IPSEC_CHANNEL	✔	✔		
O.TSFD_MNG				✔
OE.CRYPTO	✔			
OE.DETECT_MODIFY		✔		
OE.PRE_SHARE_KEY			✔	
OE.TRUST	これらセキュリティ対策方針は、前提条件に対応する。			
OE.PLACE				
OE.KEY_SHARE				
OE.SERVICE				
OE.PASSWORD				
OE.DATA_KEY				
OE.CONSOLE				
OE.IPSEC&IKE_SETUP				

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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（脅威と対策方針）』の根拠を示す。

T.PACKET_TAP

「T.PACKET_TAP」は、外部ネットワークインタフェースを介して送受信されるパケットデータが攻撃者により盗聴され、その通信内容が漏洩するという脅威である。

この脅威に対抗するためには、攻撃者が外部ネットワークインタフェースを介して送受信されるパケットデータの盗聴を試みても、パケットデータの内容を解析できないようにすることが必要である。

O.IPSEC_CHANNEL により、TOE は外部ネットワークインタフェースを介して送受信されるパケットデータのために、IPsec による暗号化通信を行う通信チャネルを提供する。

その際、OE.CRYPTO により、パケットデータの暗号化における演算を行う。

従って、O.IPSEC_CHANNEL、OE.CRYPTO 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。

T.PACKET_MODIFY

「T.PACKET_MODIFY」は、外部ネットワークインタフェースを介して送受信されるパケットデータが攻撃者により改ざんされる脅威である。

この脅威に対抗するためには、パケットデータに対する改ざんが行なわれた場合、その事象を検出可能とすることが必要である。

O.IPSEC_CHANNEL により、TOE は外部ネットワークインタフェースを介して送受信されるパケットデータのために、IPsec による暗号化通信を行う通信チャネルを提供する。

通信チャネルを通過するパケットには、パケットデータの改ざん検知を行う認証データが付加されている。

OE.DETECT_MODIFY は、パケットデータの改ざん検知を行う認証データを生成し、この認証データとの照合を行うことで、外部ネットワークインタフェースを介して送受信されるパケットデータが改ざんされたことを検出することができる。

従って、O.DETECT_MODIFY、OE.DETECT_MODIFY 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

T.MECHA_AUTH

T.MECHA_AUTH は、攻撃者の所有する機器が通信相手になりすまし、通信折衝が成立することで、結果的に送受信されるパケットデータの通信内容が漏洩するという脅威である。

この脅威に対抗するためには、通信相手となるルータ機器が、希望する機器であることの識別認証を行うことが必要である。

OE.PRE_SHARE_KEY により、TOE は通信相手との通信前に、識別認証によって通信相手となるルータ機器が希望する機器であることを確認するため、ルータ機器のなりすましに対抗することができる。

従って、OE.PRE_SHARE_KEY 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。

OSP.TOE_MNGR

「OSP.TOE_MNG」は、本装置の運用環境に関わらず、本装置の管理行為を行う人物を管理者のみに制限する事を規定した組織のセキュリティ方針である。

この組織のセキュリティ方針を実現するには、本装置の運用環境に関わらず、本装置の管理行為を行う人物を管理者のみに制限することが必要である。

O.TSFD_MNG により、運用環境に関わらず、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ため、本装置の管理行為を行なう人物を管理者に制限することができる。

従って、O.TSFD_MNG が満たされることにより、本組織のセキュリティ方針を実現することができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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 8.2 TOE セキュリティ環境とセキュリティ対策方針の対応（前提条件と対策方針)』に示す。

表 8-2 TOE セキュリティ環境とセキュリティ対策方針の対応（前提条件と対策方針）

―	前提条件							
TOE セキュリティ環境 / セキュリティ対策方針	A.TRUST	A.PLACE	A.KEY_SHARE	A.SERVICE	A.PASSWORD	A.DATA_KEY	A.CONSOLE	A.IPSEC&IKE_SETUP
O.IPSEC_CHANNEL	これらセキュリティ対策方針は、脅威及び組織のセキュリティ方針に対応する。							
O.TSFD_MNG								
OE.CRYPTO								
OE.DETECT_MODIFY								
OE.PRE_SHARE_KEY								
OE.TRUST	✔							
OE.PLACE		✔						
OE.KEY_SHARE			✔					
OE.SERVICE				✔				
OE.PASSWORD					--			
OE.DATA_KEY						--		
OE.CONSOLE							--	
OE.IPSEC&IKE_SETUP								✔

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

A.TRUST

「A.TRUST」は、本装置の運用支援機能を使用する管理者が、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.PLACE

「A.PLACE」は、本装置が限られた人物のみが入室できる区画（データセンタ、サーバルームなど）に設置されることを規定した前提条件である。

この前提条件を実現させるためには、本装置を入室できる人物が制限された区画（データセンタ、サーバルームなど）に設置することが必要である。

OE.PLACE により、本装置を限られた人物のみが入室できる区画（データセンタ、サーバルームなど）に設置することが要求されているため、本装置を限られた人物のみが入室できる区画（データセンタ、サーバルームなど）に設置することができる。

従って、セキュリティ対策方針 OE.PLACE が満たされることにより、本前提条件を実現することができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

A.KEY_SHARE

「A.KEY_SHARE」は、暗号鍵交換機能で使用する事前共有秘密鍵を、第三者に漏洩させない運用で通信相手と共有を行い、事前共有秘密鍵の共有後も第三者に漏洩させない運用を行うことを規定した前提条件である。

この前提条件を実現するためには、「鍵交換制御」機能の環境設定として、「事前共有秘密鍵認証方式」のメインモードを使用する設定及び事前共有秘密鍵をあらかじめ通信相手と共有する環境設定を行なう必要がある。また、事前共有秘密鍵を本装置と通信相手の双方で漏洩させないように運用管理する事が必要である。

OE.KEY_SHARE により、管理者は、暗号鍵交換機能が使用する事前共有秘密鍵を通信相手と共有する運用を行う。事前共有秘密鍵には、推測されにくい十分な強度を持つ値を使用する。

また、本装置及び通信相手の管理者は、事前共有秘密鍵を第三者に漏洩させない運用を行う。

従って、セキュリティ対策方針 OE.KEY_SHARE が満たされることにより、本前提条件を実現することができる。

A.SERVICE

「A.SERVICE」は、TOE が動作する Si-R では、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、及び SSH FTP サーバ機能によるリモートログインサービス及びファイル転送サービスを提供し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、TOE が動作する Si-R において、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、及び SSH FTP サーバ機能を動作させない設定にすることが必要である。

OE.SERVICE では、TOE が動作する Si-R において、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、及び SSH FTP サーバ機能を使用させない設定とすることを管理者に要求している。

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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

A.PASSWORD

「A.PASSWORD」は、TOE が動作する Si-R 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として、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、8 文字以上のパスワードを設定することを管理者に要求している。そのため管理コンソールの識別認証のパスワードを 8 文字以上のパスワードにすることができる。

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.DATA_KEY

「A.DATA_KEY」は、TOE が動作する Si-R では、利用者データの暗号化／復号に使用するデータ暗号鍵には、電子政府推奨暗号のアルゴリズムである 3DES または AES を用いて作成した 128 ビット以上の鍵長を持つデータ暗号鍵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、運用支援機能における暗号アルゴリズムの指定に電子政府推奨暗号アルゴリズムを設定しかつ、データ暗号鍵の鍵長を 128 ビット以上に設定し、使用する必要がある。

OE.DATA_KEY では、データ暗号鍵に、電子政府推奨暗号のアルゴリズムである 3DES または AES を用いて作成した 128 ビット以上の鍵長を持つデータ暗号鍵を使用することを管理者に要求している。そのためデータ暗号鍵に、電子政府推奨暗号のアルゴリズムである 3DES または AES を用いて作成した 128 ビット以上の鍵長を持つデータ暗号鍵を使用することができる。

従って、OE.DATA_KEY 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

A.CONSOLE

「A.CONSOLE」は、TOE が動作する Si-R 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、保守用及び一般ユーザの利用者 ID による使用は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、保守用及び一般ユーザの利用者 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。

A.IPSEC&IKE_SETUP

「A.IPSEC&IKE_SETUP」は、TOE の暗号通信のモードとして、事前共有秘密鍵認証方式かつ、メインモードを使用した鍵交換を行いかつ、トンネルモードによる認証付き暗号化通信の環境を設定し、鍵交換クイックモードの認証アルゴリズムには、HMAC-MD5 または HMAC-SHA1 を使用する環境を設定する前提条件である。

この前提条件を満足するためには、鍵交換機能及び IPsec の環境を条件通りに設定する必要がある。

OE.IPSEC&IKE_SETUP では、鍵交換機能及び IPsec の環境を条件通りに設定することを管理者に要求しているため、条件に合致した環境を設定することができる。

従って、OE.IPSEC&IKE_SETUP 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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 FTP_ITX.1 及び FTP_ITZ.1 の導入理由

本 ST では、CC パート 2 を参照せず新規に TOE セキュリティ機能要件「FTP_ITX.1 TSF 高信頼チャネルの操作」及び「FTP_ITZ.1　TSF 高信頼チャネルの実装」を作成し、使用している。

これら TOE のセキュリティ機能要件と IT 環境のセキュリティ機能要件が協調して動作することにより、CC パート２で規定されている FTP_ITC.1 と同等のセキュリティ機能要件を実現している。

本 ST における TSF 高信頼チャネルとは、TOE が IT 環境と協調して動作する事により、生成される IPsec 通信を行うための通信路であり、暗号鍵を共有するために生成するトンネル及び利用者のパケットデータを盗聴、改ざんから保護するために生成するトンネルが該当する。

このトンネル内で送信されるパケットデータには、送信者（送信機器）を示すハッシュが付加されており、パケットデータの受信側で通信相手が正しい事を確認する。

従って、セキュリティ機能要件「FTP_ITX.1」及び「FTP_ITZ.1」は、TOE が搭載される装置に実装された高信頼 IT 装置を使用して、高信頼チャネルを生成する一連の制御を行う。

なお、管理項目として、FTP_ITX.1、FTP_ITZ.1 ともに、CC パート２で規定されている FTP_ITC.1 と同等の管理項目を規定している。

また、監査項目として、FTP_ITX.1、FTP_ITZ.1 ともに、CC パート２で規定されている FTP_ITC.1 と同等の項目を規定している。

依存性については、FTP_ITX.1 及び FTP_ITZ.1 は、CC パート２で規定されている FTP_ITC.1 のエレメントを分割したセキュリティ機能要件であるため、この２つのセキュリティ機能要件が、相互に依存する関係を規定している。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

8.2.2. 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 8-3 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	セキュリティ対策方針 / セキュリティ機能要件	O.IPSEC_CHANNEL	O.TSFD_MNG	OE.CRYPTO	OE.DETECT_MODIFY	OE.PRE_SHARE_KEY
TOE セキュリティ機能要件	FTP_ITX.1	✔				
	FDP_ACC.1		✔			
	FDP_ACF.1		✔			
	FIA_SOS.1		✔			
	FIA_UAU.2		✔			
	FIA_UAU.7		✔			
	FIA_UID.2		✔			
	FMT_MOF.1		✔			
	FMT_MTD.1		✔			
	FMT_SMF.1		✔			
	FMT_SMR.1		✔			
	FPT_RVM.1		✔			
	FPT_SEP.1		✔			
IT 環境のセキュリティ機能要件	FTP_ITZ.1			✔	✔	✔

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

以下に、『表 8.3 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.IPSEC_CHANNEL について

「O.IPSEC_CHANNEL」は、TOE は、外部ネットワークインタフェースを介して送受信されるパケットデータのため、IPsec 通信を行う通信チャネルを生成する対策方針である。

このセキュリティ対策方針を実現するためには、高信頼チャネルを生成する機能要件があり、既存の機能要件「FPT_ITC.1」で表現する事が可能であるが、本 TOE では、高信頼チャネルの生成に関わる一部の操作(演算)を行なうことができないため、IT 環境に一部の操作(演算)を依頼して、高信頼チャネルの開設に関わる操作を行なわせる機能要件を導出する。

FTP_ITX.1 によって、通信相手と利用者のパケットデータの送受信を行うための高信頼性チャネルの開設操作が行われる。この高信頼チャネルの開設は、通信相手と暗号鍵を共有する操作が行われた上で高信頼チャネルの生成操作が行われる。

従って、FTP_ITX.1 が満たされることにより、本セキュリティ対策方針を実現することができる。

・ O.TSFD_MNG について

「O.TSFD_MNG」は、TSF の動作に係わるデータに対する操作、及び TOE の動作に係わる IT 環境の機能のデータに対する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。

このセキュリティ対策方針を実現するためには、操作者が管理者であることを確認しかつ、TSF の動作に係わるデータに対する操作、及び TOE の動作に係わる IT 環境の機能のデータに対する操作を管理者のみ行えるよう制限することが必要となる。

FIA_UAU.2 及び FIA_UID.2 によって、TSF の動作に係わるデータに対する操作、及び TOE の動作に係わる IT 環境の機能のデータに対する操作を行なう前に、操作者の識別と認証が行なわれる。識別又は認証が成功した場合、FDP_ACC.1 及び FDP_ACF.1 によって、IPsec 通信に関係する諸データの設定を許可し、不成功の場合は該当する設定を拒否する。

FIA_UAU.7 によって、操作者から入力されたパスワードのフィードバックを非表示にすることで入力画面上からのフィードバックの漏洩を防ぐことができる。

FIA_SOS.1 によって、パスワードに対する品質尺度を設定し、品質尺度に合致しないパスワードの利用を禁止することができる。

FMT_MOF.1 及び FMT_MTD.1 により、セキュリティ機能のふるまい(高信頼チャネル通信機能の停止の設定、CE 保守及び一般ユーザのログイン可否の設定)及び

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

TSF データの設定を管理者に制限することができ、FMT_SMF.1 により実体となる管理機能を提供する。

FMT_SMR.1 により、管理者の役割が維持される。

FPT_RVM.1 によって、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。

従って、FDP_ACC.1、FDP_ACF.1、FIA_UAU.2、FIA_UID.2、FIA_UAU.7、FIA_SOS.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 が満たされることにより、本セキュリティ対策方針を実現することができる。

・ OE.CRYPTO について

「OE.CRYPTO」は、IT 環境が外部ネットワークインタフェースを介して送信するパケットデータの漏洩を防止するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、パケットデータの暗号化を行う機能要件を導出する必要があるが、IT 環境としては、暗号化における演算部分のみを行なう。（O.IPSEC_CHANNEL と一緒に動作することで、暗号化を行う）

FTP_ITZ.1 により、通信相手と利用者パケットデータの送受信を行うための高信頼チャネルの開設に必要となる一部の操作（演算）を行う。

この高信頼チャネルの開設は、通信相手と暗号鍵を共有する一部の操作（演算）が行われた上で高信頼チャネルの生成操作が行われる。

従って、FTP_ITZ.1 が満たされることにより、本セキュリティ対策方針を実現することができる。

・ OE.DETECT_MODIFY について

「OE.DETECT_MODIFY」は、IT 環境が外部ネットワークインタフェースを介して送受信されるパケットデータの改ざんを検知するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、目的に従いパケットデータのハッシュ値演算を行うことが必要である。（O.DETECT_MODIFY と一緒に動作することで、ハッシュ値演算を行う）

FTP_ITZ.1 により、高信頼チャネルを介して受信した暗号鍵を生成する素材及び利用者パケットデータの改変を検知するため、ハッシュ値演算と照合が行われる。

従って、FTP_ITZ.1 が満たされることにより、本セキュリティ対策方針を実現することができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

・ OE.PRE_SHARE_KEY について

「OE.PRE_SHARE_KEY」は、IT 環境が受信したパケットデータに付加された識別情報から、通信相手が環境設定で定義された通信相手であることを確認するセキュリティ対策方針である。

このセキュリティ対策方針を実現するためには、高信頼チャネルによる通信相手の識別を行うことが必要である。既存の機能要件では、「FPT_ITC.1」で表現する事が可能であるが、TOE の機能要件である「FTP_ITX.1」の制御下で高信頼チャネルによる通信機器の識別時に必要となる演算を、IT 環境の演算チップで行っているので、IT 環境が演算を実施して、高信頼チャネルが提供する通信機器の識別を行なわせる機能要件を導出する。

FTP_ITZ.1 によって、高信頼チャネルが受信したパケットデータの送信者（機器）の識別と認証操作を行う。識別及び認証が成功し、相手が TOE の意図する通信相手であることが確認できた場合は、受信パケットデータの通信を許可し、識別又は認証が不成功の場合は、受信パケットデータの通信を一切拒否する。

従って、FTP_ITZ.1 が満たされることにより、本セキュリティ対策方針を実現することができる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

8.2.3. セキュリティ機能要件間の依存関係

セキュリティ機能要件の依存関係を『表 8.3 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	FTP_ITX.1	なし	FPT_ITZ.1	14	
2	FDP_ACC.1	なし	FDP_ACF.1	3	
3	FDP_ACF.1	なし	FDP_ACC.1	2	
			FMT_MSA.3		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
4	FIA_SOS.1	なし	なし		
5	FIA_UAU.2	FIA_UID.1	FIA_UID.2	7	本来の依存関係は FIA_UID.1 であるが、FIA_UID.2 はその上位コンポーネントである。
6	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2	5	本来の依存関係は FIA_UAU.1 であるが、FIA_UAU.2 はその上位コンポーネントである。
7	FIA_UID.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
8	FMT_MOF.1	なし	FMT_SMF.1	10	
			FMT_SMR.1	11	
9	FMT_MTD.1	なし	FMT_SMF.1	10	
			FMT_SMR.1	11	
10	FMT_SMF.1	なし	なし		

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

NO	セキュリティ機能要件	下位階層	依存関係	参照NO	備考
11	FMT_SMR.1	なし	FIA_UID.2	7	FIA_UID.2 は FIA_UID.1 の上位階層コンポーネントである
12	FPT_RVM.1	なし	なし		
13	FPT_SEP.1	なし	なし		
14	FPT_ITZ.1	なし	FTP_ITX.1	1	

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

8.2.4. 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 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 セキュリティ機能要件の相互作用について

相互支援 / 機能要件	迂回防止	干渉防止	非活性化防止
FTP_ITX.1	N/A	FMT_MTD.1	FMT_MOF.1
FDP_ACC.1	FIA_UAU.2	FPT_SEP.1	N/A
FDP_ACF.1	FIA_UAU.2	FPT_SEP.1	N/A
FIA_SOS.1	N/A	N/A	N/A
FIA_UAU.2	FPT_RVM.1	FMT_MTD.1	N/A
FIA_UAU.7	N/A	N/A	N/A
FIA_UID.2	N/A	N/A	N/A
FMT_MOF.1	N/A	N/A	N/A
FMT_MTD.1	N/A	N/A	N/A
FMT_SMF.1	N/A	N/A	N/A
FMT_SMR.1	N/A	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A
FPT_SEP.1	N/A	N/A	N/A
FTP_ITZ.1	N/A	N/A	N/A

N/A ： 適用しない。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FPT_RVM.1<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、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、運用支援機能を使用する人物の認証を行う FIA_UAU.2 である。

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

FIA_UAU.2<迂回防止>

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。

FMT_MTD.1<干渉防止>

FMT_MTD.1 により、IPsec 通信に関係する諸データ（高信頼チャネルの更新条件、動作タイプ及び高信頼チャネルの対象範囲）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。

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

従って、FMT_MTD.1 によって FIA_UAU.2、FTP_ITX.1 が干渉防止のサポートを受けている。

FPT_SEP.1<干渉防止>

FPT_SEP.1 により、アクセス制御機能に関するセキュリティ機能要件は、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、FPT_SEP.1 によって FDP_ACC.1、FDP_ACF.1 が干渉防止のサポートを受けている。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

FMT_MOF.1<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。

・FTP_ITX.1

8.2.5. 最小機能強度根拠

本 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 Si-R 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、ルータ機器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 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_UAU.2、FIA_SOS.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。

8.2.6. 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ち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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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	暗号鍵交換機能	IPsec 暗号制御機能	運用支援機能
FTP_ITX.1	✔	✔	
FDP_ACC.1			✔
FDP_ACF.1			✔
FIA_SOS.1			✔
FIA_UAU.2			✔
FIA_UAU.7			✔
FIA_UID.2			✔
FMT_MOF.1			✔
FMT_MTD.1			✔
FMT_SMF.1			✔
FMT_SMR.1			✔
FPT_RVM.1			✔
FPT_SEP.1			✔

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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。

・ FTP_ITX.1 について

FTP_ITX.1 は、TSF 高信頼チャネルの操作を行うことを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FTP_ITX.1 で通信相手との間で暗号鍵を共有し、共有した暗号鍵で TSF 高信頼チャネルの開設操作を行う機能の実装が必要である。

また高信頼チャネルの開設後は、IT 環境を制御して、高信頼チャネルを通過する利用者パケットデータの暗号化／復号操作を行う機能の実装が必要である。

高信頼性チャネルの開設操作及びパケットデータの復号操作時に、受信されたパケットデータの送信者（通信要求者）に対する認証前のあらゆる機能の利用を禁止する機能の実装が必要である。

暗号鍵交換機能によって、利用者パケットデータの暗号化に必要な TSF 高信頼チャネルの開設操作を行う事ができる。

IPsec 暗号制御機能によって、利用者パケットデータの暗号化／復号操作を行う事ができる。

従って、暗号鍵交換機能及び IPsec 暗号制御機能の実装により、FTP_ITX.1 を実現できる。

・ FDP_ACC.1 について

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。

このセキュリティ機能要件を実現するためには、FDP_ACC.1 で規定した、管理者が、TOE 以外の Si-R の設定に関する情報(パケットデータの暗号化／復号処理に必要となる暗号条件（パラメータ）、通信相手装置との間で設定される事前共有秘密鍵、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の設定情報)を、構成定義情報に設定する機能の実装が必要である。

運用支援機能によって、管理者は、TOE 以外の Si-R の設定に関わる情報を構成定義情報に設定する事ができる。

従って、運用支援機能の実装により、FDP_ACC.1 を実現できる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

・ FDP_ACF.1 について

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 のスレッドに構成定義情報（TOE 以外の Si-R の設定に関する情報部）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。

なお構成定義情報には、パケットデータの暗号化／復号処理（IPsec 通信）を動作させる諸条件、通信相手装置との間で設定される事前共有秘密鍵を設定する。

運用支援機能によって、管理者のみが、構成定義情報（TOE 以外の Si-R の設定に関する情報部）に、パケットデータの暗号化／復号処理（IPsec 通信）を動作させる諸条件、通信相手との間で設定される事前共有秘密鍵を設定する事ができる。

従って、運用支援機能の実装により、FDP_ACF.1 を実現できる。

・ FIA_SOS.1 について

FIA_SOS.1 は、定められた品質尺度に従って秘密が定義されていることを検証することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、FIA_SOS.1 で規定した品質尺度に従って管理者のパスワードをチェックする機能の実装が必要である。

運用支援機能によって、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ことができる。

従って、運用支援機能の実装により、FIA_SOS.1 を実現できる。

・ FIA_UAU.2 について

FIA_UAU.2 は、利用者の認証前に利用者に対する TSF 調停アクションを許可しないことを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理者に対する認証前のあらゆる機能の利用を禁止する機能の実装が必要である。

運用支援機能によって、管理者に対する未認証時のあらゆる TOE 機能の利用を禁止することができる。

従って、運用支援機能の実装により、FIA_UAU.2 を実現できる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

・ FIA_UAU.7 について

FIA_UAU.7 は、認証時に認証情報を保護することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理者のパスワードのフィードバックを保護する機能の実現が必要である。

運用支援機能によって、管理者のパスワードを入力する際のフィードバックを非表示にし、フィードバックを保護することができる。

従って、運用支援機能の実装により、FIA_UAU.7 を実現できる。

・ FIA_UID.2 について

FIA_UID.2 は、利用者の識別前に利用者に対する TSF 調停アクションを許可しないことを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理者に対する識別前のあらゆる機能の利用を禁止する機能の実装が必要である。

運用支援機能によって、管理者に対する識別前のあらゆる TOE 機能の利用を禁止することができる。

従って、運用支援機能の実装により、FIA_UID.2 を実現できる。

・ FMT_MOF.1 について

FMT_MOF.1 は、セキュリティ機能のふるまいを許可された管理者のみに制限することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、セキュリティ機能のふるまい（高信頼通信チャネルの停止、CE 保守及び一般ユーザによるログイン可否の設定）を管理者のみに制限する機能の実装が必要である。

運用支援機能によって、セキュリティ機能のふるまいを管理者のみに制限することができる。

従って、運用支援機能の実装により、FMT_MOF.1 を実現できる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

・ FMT_MTD.1 について

FMT_MTD.1 は、TSF データを管理する能力を特定の役割のみに制限することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、ログインパスワードに対する改変・問い合わせの操作、高信頼チャネル通信機能の更新条件の改変・設定、高信頼チャネル通信機能の動作タイプの改変及び高信頼チャネル通信機能の動作対象範囲の登録の操作、を管理者のみに提供する機能の実装が必要である。

運用支援機能によって、ログインパスワードに対する改変、問い合わせの操作、高信頼チャネル通信機能の更新条件の改変・設定、高信頼チャネル通信機能の動作タイプの改変及び高信頼チャネル通信機能の動作対象範囲の登録操作を行なう能力を、管理者のみに制限することができる。

従って、運用支援機能の実装により、FMT_MTD.1 を実現できる。

・ FMT_SMF.1 について

FMT_SMF.1 は、セキュリティ管理機能を行う能力を提供することを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、「運用支援機能における管理者のログインパスワードの設定、改変及び問い合わせ機能」、「高信頼チャネル通信機能の更新条件の改変・設定機能」、「高信頼チャネルの動作タイプの改変機能」、「高信頼チャネル通信機能の動作対象範囲の登録・改変機能」及び「CE 保守及び一般ユーザによるログイン可否の設定機能」を実装する必要がある。

運用支援機能によって、「運用支援機能における管理者のログインパスワードの設定、改変、及び問い合わせ機能」、「高信頼チャネル通信機能の更新条件の改変・設定機能」、「高信頼チャネル通信機能の動作タイプの改変機能」、「高信頼チャネル通信機能の動作対象範囲の登録・改変機能」及び「CE 保守及び一般ユーザによるログイン可否の設定機能」を提供することができる。

従って、運用支援機能の実装により、FMT_SMF.1 を実現できる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

・ FMT_SMR.1 について

FMT_SMR.1 は、セキュリティ役割を維持し、利用者に役割を関連付けることを要求するセキュリティ機能要件である。

このセキュリティ機能要件を実現するためには、管理者という役割を維持し、利用者に関連付ける機能を実装する必要がある。

運用支援機能によって、管理者という役割を維持し、管理者の識別認証成功後に、管理者を代行するプロセスに役割を関連付けることができる。

従って、運用支援機能の実装により、FMT_SMR.1 を実現できる。

・ FPT_RVM.1 について

FPT_RVM.1 は、セキュリティ機能が迂回されないで必ず動作する事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、TOE の環境設定を行う運用支援機能は、管理者のみに環境を設定する操作を許可する必要がある。

運用支援機能は自身が持つ利用者の識別認証機能により、利用者が管理者である事を識別、認証された後に動作するため、運用支援機能の実装により、FPT_RVM.1 を実現できる。

・ FPT_SEP.1 について

FPT_SEP.1 は、信頼されないサブジェクトによる干渉や改ざんから保護するセキュリティドメインの維持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、使用する環境設定のパラメータが改ざんされないようにする必要がある。

運用支援機能は、環境設定を行う人物を識別認証し、管理者であった場合は、TOE 自身が管理する主記憶及び不揮発性メモリにパラメータ値の設定を許可しているため、運用支援機能の実装により、FPT_SEP.1 を実現できる。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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_UAU.2、FIA_SOS.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、運用支援機能が持つ識別認証機能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 に ALC_FLR.1 追加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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」

【保証要件根拠】

保証手段である「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」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】

「Si-R シリーズ IPsec／IKE 機能仕様書」

「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「Si-R シリーズ IPsec／IKE 機能仕様書」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】

「Si-R シリーズ IPsec/IKE 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「Si-R シリーズ IPsec/IKE 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

ADV_IMP.1

【保証手段】

「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「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】

「Si-R シリーズ IPsec/IKE 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「Si-R シリーズ IPsec/IKE 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】

「Si-R シリーズ　ISO15408 表現対応表」

【保証要件根拠】

保証手段である「Si-R 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

ADV_SPM.1

【保証手段】

「Si-R Security Software V01.00 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「Si-R Security Software V01.00 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】

「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」

「GeoStream Si-R シリーズ　機能説明書　V33」

「GeoStream Si-R シリーズ　コマンド設定事例集　V33」

「GeoStream Si-R シリーズ　コマンドリファレンス　V33」

「GeoStream Si-R シリーズ　コマンドユーザーズガイド　V33」

【保証要件根拠】

保証手段である「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」、「GeoStream Si-R シリーズ　機能説明書　V33」、「GeoStream Si-R シリーズ　コマンド設定事例集 V33」、「GeoStream Si-R シリーズ　コマンドリファレンス　V33」、「GeoStream Si-R シリーズ　コマンドユーザーズガイド　V33」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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

AGD_USR.1　　利用者ガイダンス

【保証手段】

「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」

「GeoStream Si-R シリーズ　機能説明書　V33」

【保証要件根拠】

保証手段である「Geostream Si-R シリーズ　Si-R570 ご利用にあたって」、「GeoStream Si-R シリーズ　機能説明書　V33」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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

ALC_FLR.1

【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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

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】

「Si-R 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「Si-R 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】

「Si-R シリーズ　ISO15408 深さ分析書」

【保証要件根拠】

保証手段である「Si-R 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

ATE_FUN.1　　機能テスト

【保証手段】

「IPsec／IKE 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「IPsec／IKE 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」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】

IP アクセスルータ GeoStream Si-R シリーズ Si-R Security Software

【保証要件根拠】

保証手段である「IP アクセスルータ GeoStream Si-R シリーズ Si-R Security Software」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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

AVA_MSU.2　　ガイダンスの検査

【保証手段】

「Si-R Security Software V01.00 脆弱性分析書」

【保証要件根拠】

保証手段である「Si-R Security Software V01.00 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「Si-R Security Software V01.00 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】

「Si-R Security Software V01.00 脆弱性分析書」

【保証要件根拠】

保証手段である「Si-R Security Software V01.00 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】

「Si-R Security Software V01.00 脆弱性分析書」

【保証要件根拠】

保証手段である「Si-R Security Software V01.00 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。

All Rights Reserved, Copyright©富士通株式会社, 2006-2007

（　最終ページ　）

All Rights Reserved, Copyright©富士通株式会社, 2006-2007