認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成20年1月4日** (IT**認証**8190)
認証番号	C0185
認証申請者	**富士通株式会社**
TOE**の名称**	Si-R Security Software
TOE**のバージョン**	V02.02
PP**適合**	**なし**
適合する保証パッケージ	EAL4**及び追加の保証コンポーネント**ALC_FLR.1
開発者	**富士通株式会社**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成20年9月24日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「Si-R Security Software　V02.02」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

1.1 はじめに

この認証報告書は、「Si-R Security Software V02.02」（以下「本TOE」という。）についてみずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である富士通株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　Si-R Security Software
バージョン：　V02.02
開発者：　富士通株式会社

1.2.2 製品概要

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、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。

1.2.3 TOEの範囲と動作概要

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

メイン又は別セグメントのルータ機器）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。

トンネルを開設するIPsecのモードには、「事前共有秘密鍵認証方式」と「RSAデジタル署名認証方式」の２方式が存在する。事前共有秘密鍵認証方式及びRSAデジタル署名認証方式で動作する場合の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、事前共有秘密鍵認証方式及びRSAデジタル署名認証方式で動作する場合の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。TOEは「演算チップ」が、円滑に動作するよう制御を行う。

上記のことから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。

1.2.4 TOEの機能

TOEが持つ機能を以下に示す。

- 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

設することにより、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」における通信相手の機器認証として、「事前共有秘密鍵認証方式」または「RSAデジタル署名認証方式」の何れかを選択し、利用することができる。

「事前共有秘密鍵認証方式」では、「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。

一方、「RSAデジタル署名認証方式」では、通信相手のパケット内の署名を、IT環境である演算チップを利用し検証することで認証するため、通信相手のデジタル証明書を登録する必要がある。登録方法は以下の2通り（両方選択はできず、以下の何れかから選択する）

1. 通信相手にデジタル証明書の要求を行い入手することで登録する。但し、通信相手のデジタル証明書の真正性を認証局のデジタル証明書にて確認するため、予め認証局のデジタル証明書をTOEに登録しておく必要がある。
2. TOEに、コマンドを使用して通信相手のデジタル証明書を手入力により登録する。

上記、1.における「認証局のデジタル証明書」、及び2.における「通信相手のデジタル証明書」は管理者が信頼できると判断したものを使用する運用を行わなければならない。

- 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。

IPsec暗号制御機能の動作概要を図1-1及び表1-1に示す。

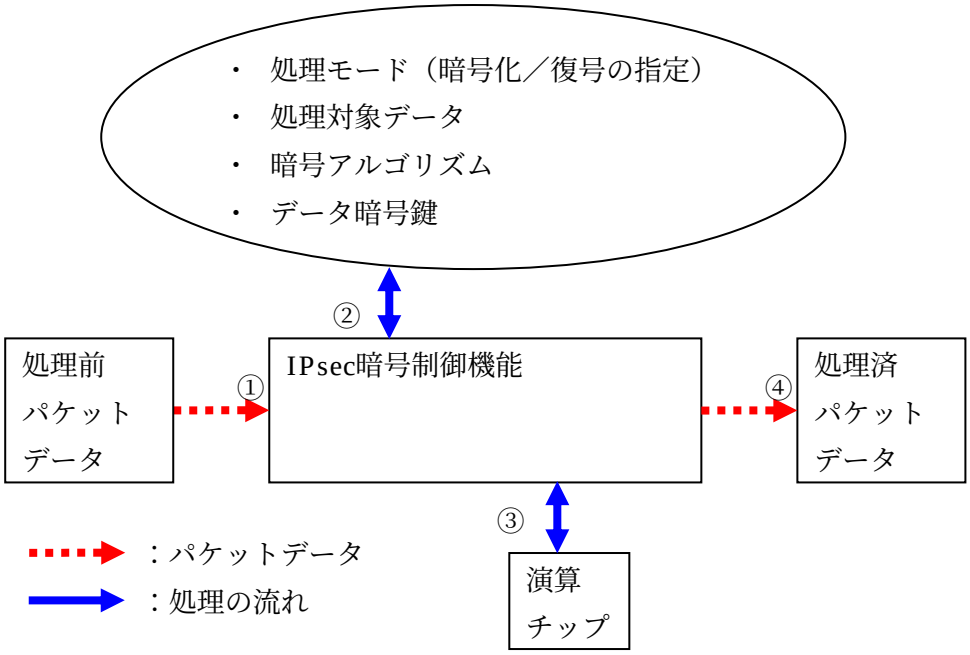

図1-1 IPsec暗号制御機能の動作概要

表1-1 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。

No.	動作
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。

- 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ことが確認された場合、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、ログアウトを行い運用支援機能の使用を終了する。

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「Si-R Security Software　V02.02 セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]

のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「Si-R Security Software　V02.02 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成20年9月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL4追加である。
追加の保証コンポーネントは、ALC_FLR.1である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

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SOF-基本で十分である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

（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、以下の利用環境を設定する。

・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
・RSAデジタル署名認証方式かつ、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

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。）

暗号鍵交換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1-2に示す。

表1-2 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、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。

（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。

（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改変及び問い合わせ
・高信頼チャネルの諸条件の登録・改変
（IPsec通信を行うための、高信頼チャネルの更新条件（「鍵の有効期間」及び「転送パケット量の閾値」）、動作対象範囲（ネットワークアドレスのレンジ）の管理を行っている。）
・高信頼チャネルの動作タイプの改変
（「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」、「通信相手の認証方式」の管理を行っている。）
・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
・AAAの機能による管理者と一般ユーザのログインの可否の設定
・IKEセッション用証明書要求の送信機能の設定
・テンプレート情報を使用するIPsec/IKE機能の設定

【構成定義情報の内、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
・事前共有秘密鍵の設定
・デジタル証明書の設定

[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）

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。

1.5.5 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅 威
T.PACKET_TAP	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	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	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。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-4に示す。

表1-4 組織のセキュリティ方針

識別子	組織のセキュリティ方針
OSP.TOE_MNG	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。

1.5.7 構成条件

本TOEは富士通株式会社製の以下の製品の基本ソフトウェアV34.01の上で動作するファームウェアとして標準実装され、提供される。

- Si-R570、Si-R370、Si-R260B、Si-R240B、Si-R220C、Si-R180B

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-5に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-5　TOE使用の前提条件

識別子	前提条件
A.TRUST	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	本装置は、信頼さ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	事前共有秘密鍵認証方式を選択する場合、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.CERT_REGIST	RSAデジタル署名認証方式を選択、かつ、通信機器のデジタル証明書を手入力により直接登録する運用の場合、管理者は、暗号鍵交換機能が使用する通信相手ルータのデジタル証明書として信頼できるもののみを登録する運用を行う。また、この通信相手に、同様の環境設定の運用を求める。
A.TRUST_CA	RSAデジタル署名認証方式を選択、かつ、通信機器のデジタル証明書を通信開始時に自動的に通信相手から入手する場合、管理者はそのデジタル証明書を検証することが可能な認証局のルート証明書を入手し、本装置に登録する運用を行う。本装置のデジタル証明書と同じルート証明書により検証に成功したデジタル証明書を持つ相手装置を信用する運用を行う。RSAデジタル署名認証方式において認証局の証明書を使用する場合は、IKEセッション用証明書要求の送信の指定で、証明書要求を送信する設定とし、送信する認証局の識別番号を必ず指定する設定にする。この通信相手にも同様の

	環境設定の運用を求める。また、認証局は信頼できる装置のみにデジタル証明書を発行する運用とする。
A.SERVICE	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	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。
A.DATA_KEY	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	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。また、AAAの機能による管理者と一般ユーザ用の利用者IDの使用はしない。
A.IPSEC&IKE_SETUP	管理者は、TOEの暗号通信のモードとして、以下の利用環境を設定する。 －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 －RSAデジタル署名認証方式、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 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。 テンプレート情報を使用するIPsec/IKE機能を使用しない設定にする。
A.PACKET	本装置のWAN側には、ファイアウォールを設置する。ファイアウォールには、宛先が本装置のWAN側インタフェースであるパケットのみを、本装置に転送する設定を行う。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

ドキュメント名	バージョン
IP アクセスルータ Si-R シリーズ　機能説明書 V34	2008 年 3 月 管理番号： P3NK-3072-01Z0
IP アクセスルータ Si-R シリーズ　コマンド設定事例集 V34	2008 年 3 月 管理番号： P3NK-3122-01Z0
IP アクセスルータ Si-R シリーズ　コマンドリファレンス-構成定義編- V34	2008 年 9 月 管理番号： P3NK-3132-01Z0
IP アクセスルータ Si-R シリーズ　コマンドリファレンス-運用管理編- V34	2008 年 3 月 管理番号： P3NK-3142-01Z0
IP アクセスルータ Si-R シリーズ　コマンドユーザーズガイド V34	2008 年 3 月 管理番号： P3NK-3112-01Z0
IP アクセスルータ Si-R シリーズ Si-R570　ご利用にあたって	2008 年 9 月 管理番号： P3NK-3062-01Z0
IP アクセスルータ Si-R シリーズ Si-R370　ご利用にあたって	2008 年 9 月 管理番号： P3NK-3052-01Z0
IP アクセスルータ Si-R シリーズ Si-R260B ご利用にあたって	2008 年 9 月 管理番号： P3NK-3042-01Z0
IP アクセスルータ Si-R シリーズ Si-R240B ご利用にあたって	2008 年 9 月 管理番号： P3NK-3032-01Z0
IP アクセスルータ Si-R シリーズ Si-R220C ご利用にあたって	2008 年 9 月 管理番号： P3NK-3022-01Z0
IP アクセスルータ Si-R シリーズ Si-R180B ご利用にあたって	2008 年 9 月 管理番号： P3NK-3012-01Z0

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年1月に始まり、平成20年9月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年4月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理と運用・ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。なお、配付に関するサイト訪問は、前回の認証TOE（認証番号：C0111）で評価済みの手続きが適用されることを開発者に確認済みであることを理由として、評価者が不要と判断し、実施されていない。また、平成20年5月から７月にかけて開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1から図2-3に示す。

開発者テストは以下の3つの環境を使って実施された。本TOEには、3つのセキュ

リティ機能がある。そのうちの1つである運用支援機能は、図2-1を使ってテストが実施された。それ以外の暗号鍵交換機能及びIPsec暗号制御機能は、図2-2及び図2-3を使用してテストが実施された。

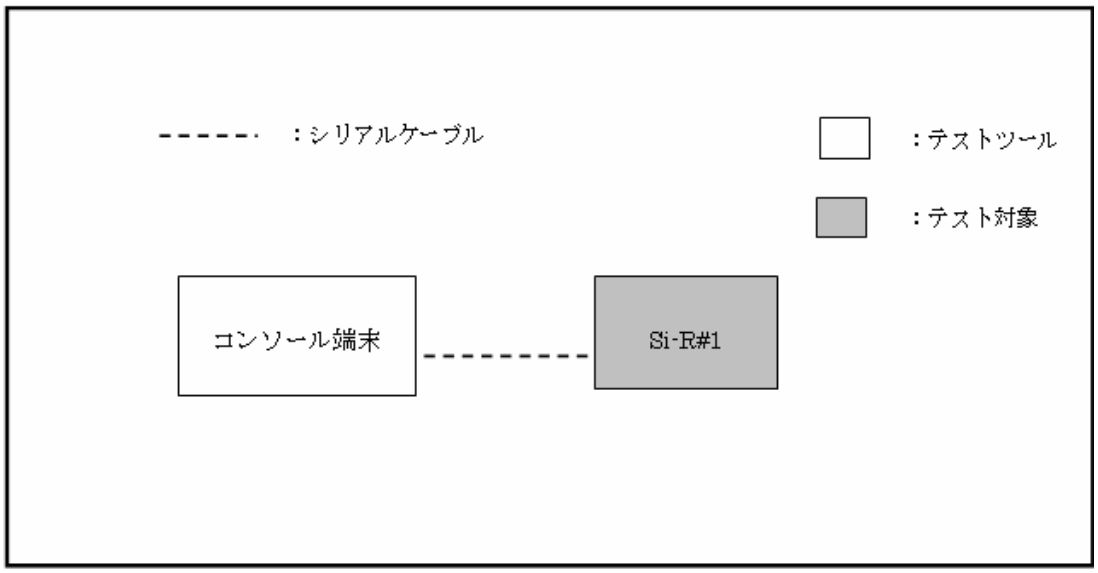

図2-1　運用支援機能の開発者テスト環境

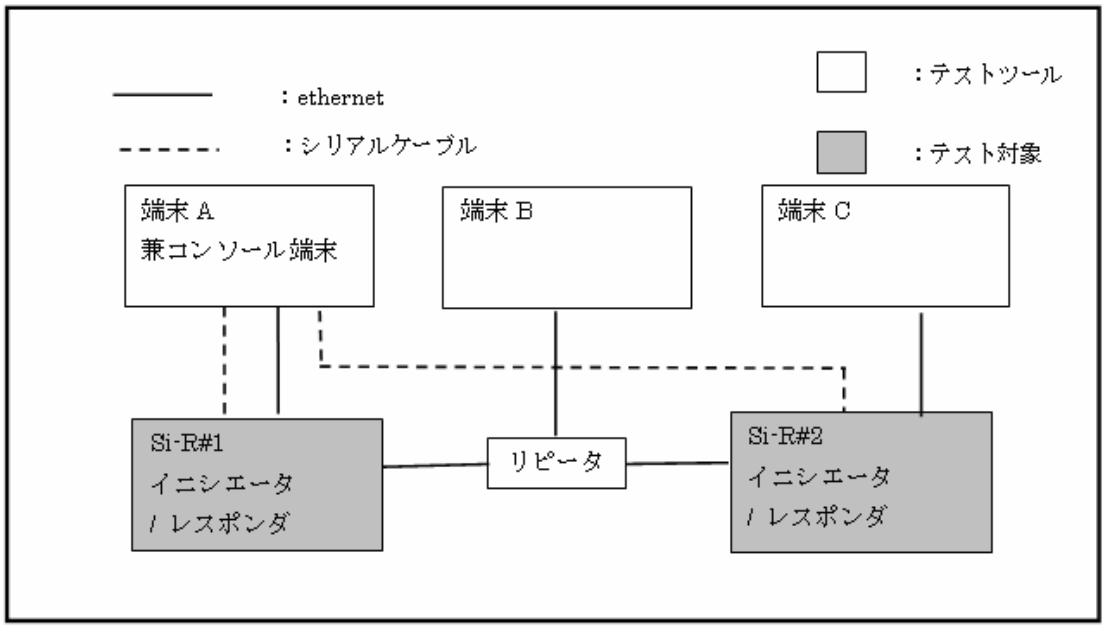

図2-2　IPsecの開発者テスト環境（A）

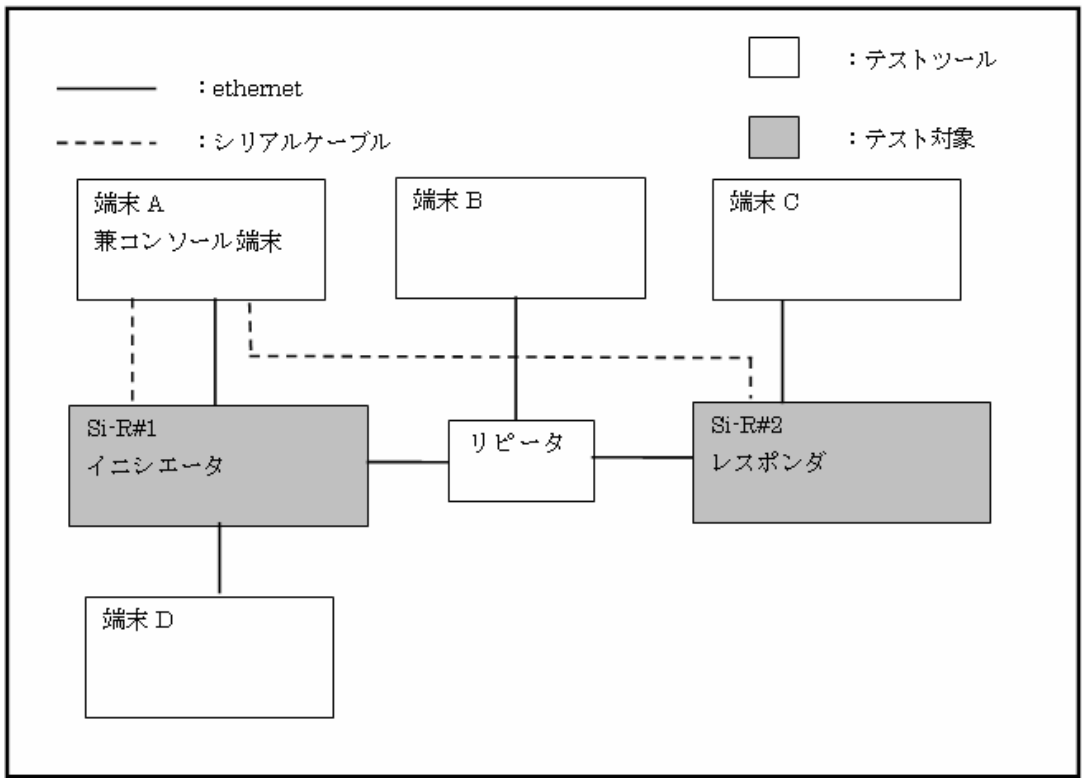

図2-3　IPsecの開発者テスト環境（B）

図2-1に示されているテスト環境では、Si-R#1として以下のものがテスト対象となっている。

・Si-R570、Si-R370、Si-R260B、Si-R240B、Si-R220C、Si-R180B

図2-2及び図2-3に示されているテスト環境では、Si-R#1とSi-R#2の組み合わせとして以下のものがテスト対象となっている。

・Si-R#1：Si-R570　←→　Si-R#2：Si-R570
・Si-R#1：Si-R370　←→　Si-R#2：Si-R370
・Si-R#1：Si-R260B　←→　Si-R#2：Si-R240B
・Si-R#1：Si-R240B　←→　Si-R#2：Si-R260B
・Si-R#1：Si-R220C　←→　Si-R#2：Si-R180B
・Si-R#1：Si-R180B　←→　Si-R#2：Si-R220C

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a. テスト構成

開発者が実施したテストの構成を図2-1から図2-3に示す。開発者テストは

STにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b. テスト手法

テストには、以下の手法が使用された。

①利用者が操作可能な外部インタフェースを持つ機能については手動操作により、機能を実行し、動作を観察する
②利用者が操作可能な外部インタフェースを持たない通信機能等については、ネットワーク上のパケットデータをキャプチャーし、解析する

c. 実施テストの範囲

テストは開発者によって51項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。また、本評価中に発生したTOEの改修においては、改修の影響範囲について実装表現等を用いて分析し、開発者テストの要否を判断した上で、テストが必要であると判断したものについて開発者テストの追加・再実施を行っている。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成を図2-4から図2-11に示す。

評価者テストは以下の8つの環境を使って実施された。評価者が独自に考案したテスト及び開発者テストのサンプリングテストは、図2-4から図2-8を使って実施された。開発者による脆弱性分析に基づく侵入テストは、図2-9及び図2-10を使って、評価者による脆弱性分析に基づく侵入テストは、図2-11を使って実施された。

評価者によるテスト環境の選定にあたっては、TOEが動作する環境に依存しないことについて実装表現等の確認を行い、その結果に基づいてテストの実施が必要であるものを判断している。

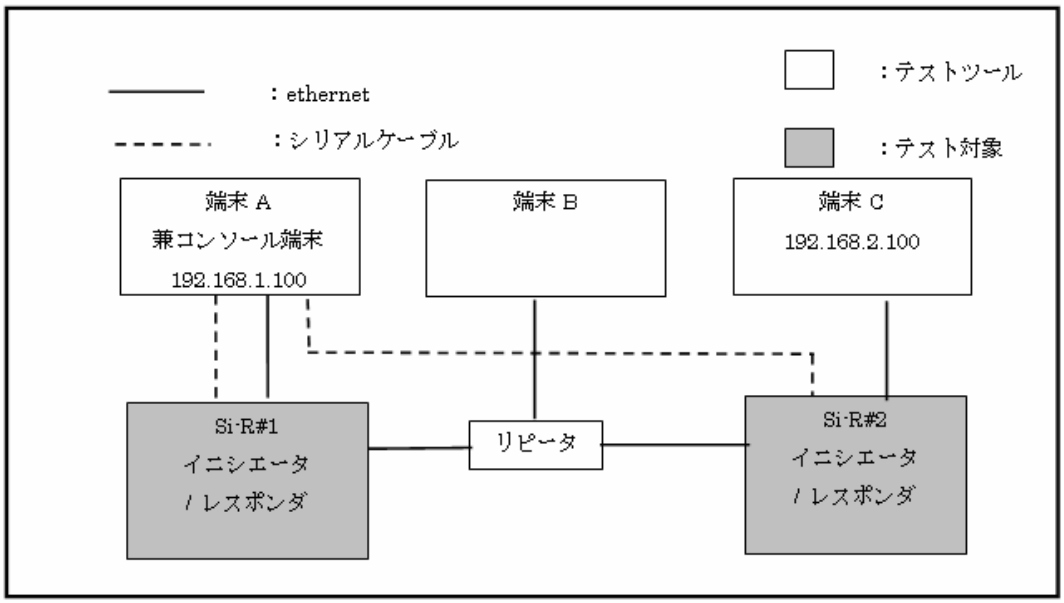

図2-4　IPsec**の評価者テスト環境（**A**）**

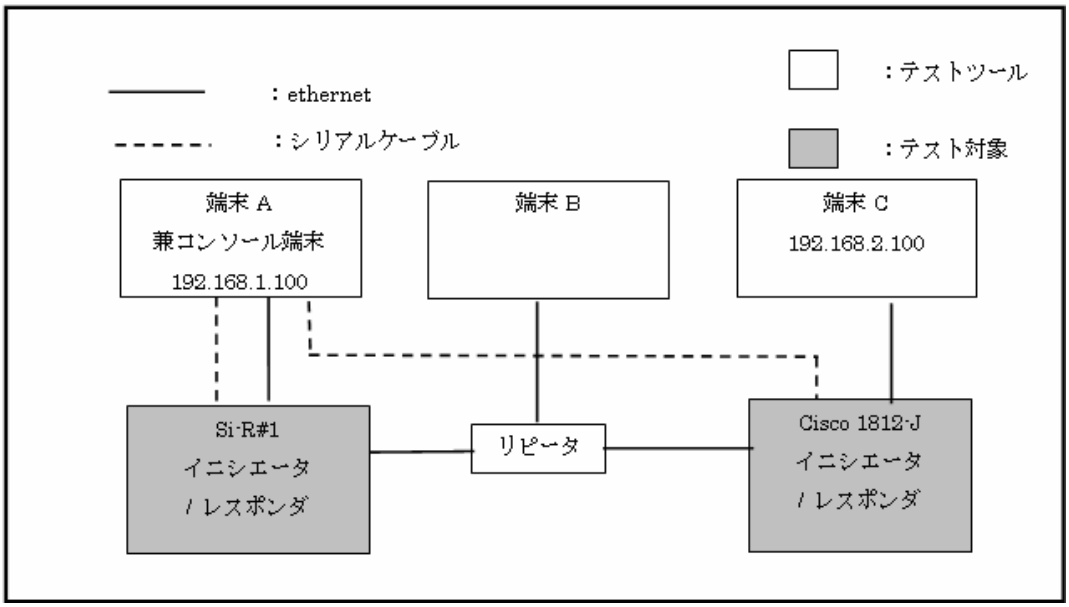

図2-5　IPsec**の評価者テスト環境（**B**）**

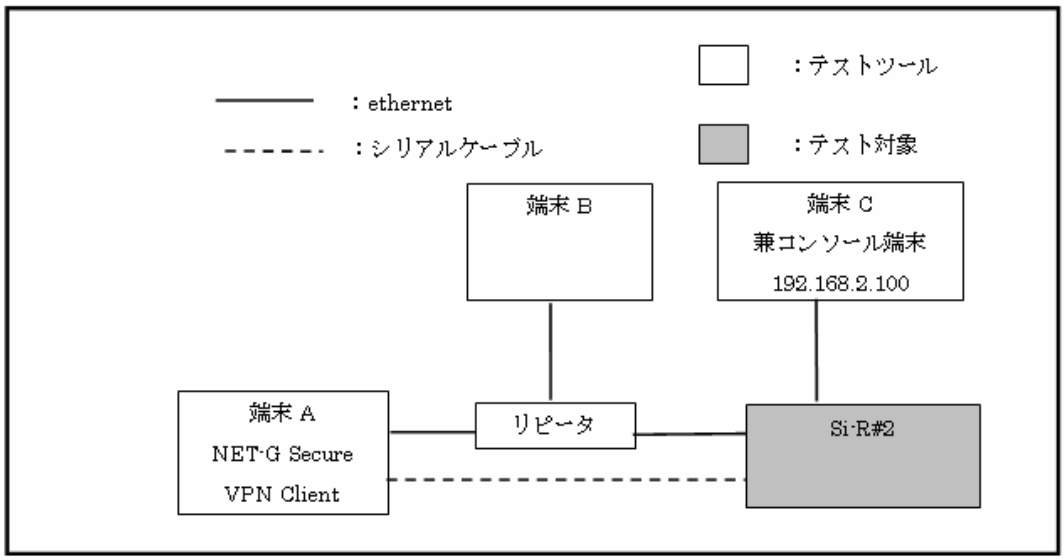

図2-6　IPsecの評価者テスト環境（C）

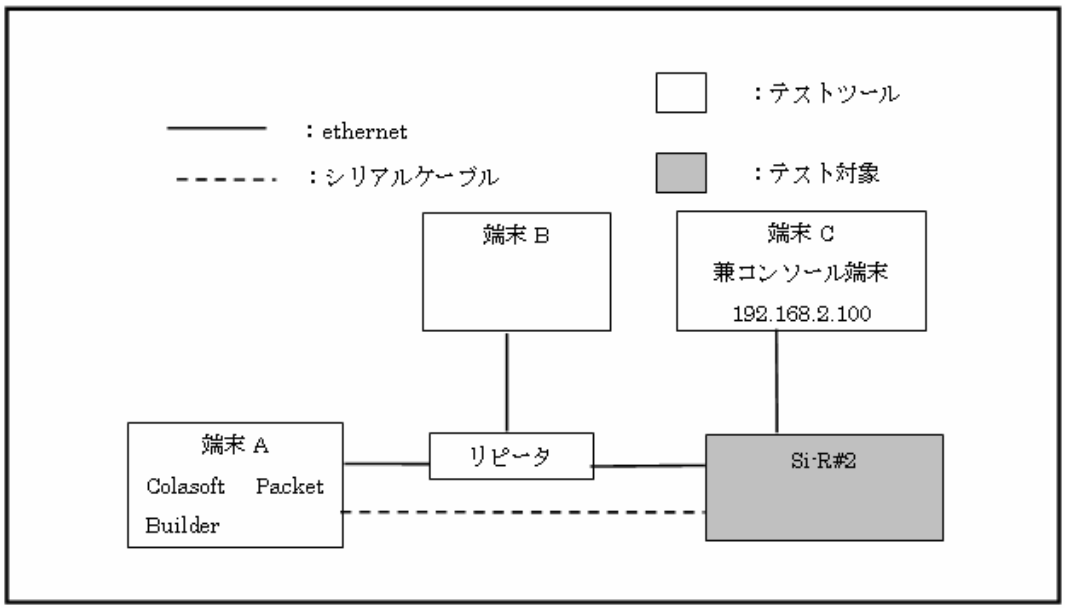

図2-7　IPsecの評価者テスト環境（D）

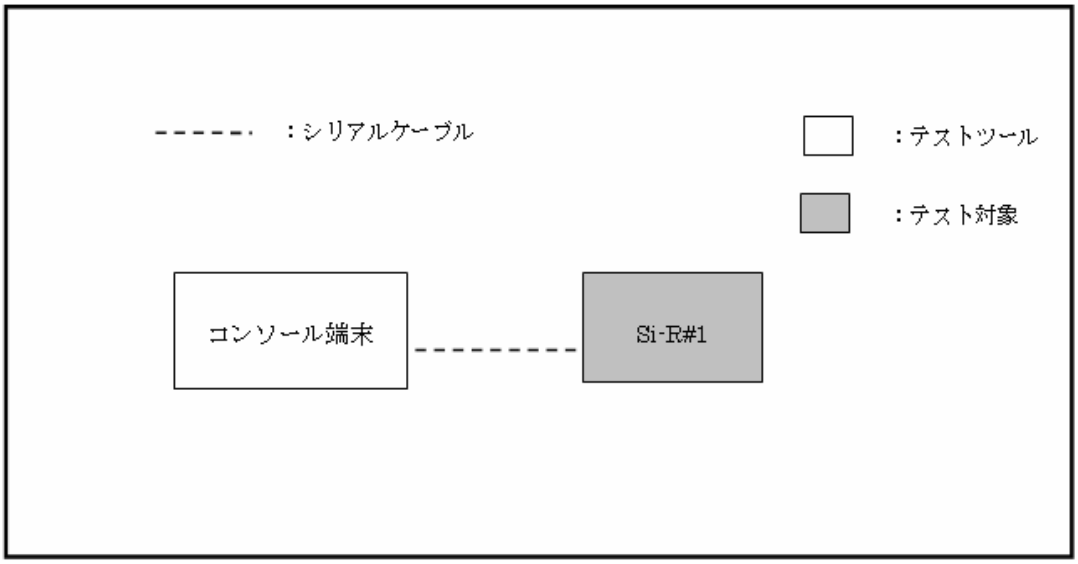

図2-8　IPsec**の評価者テスト環境（**E**）**

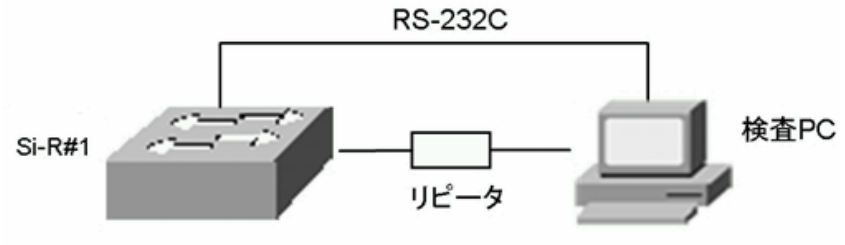

図2-9　**侵入テスト環境（その**1**）**

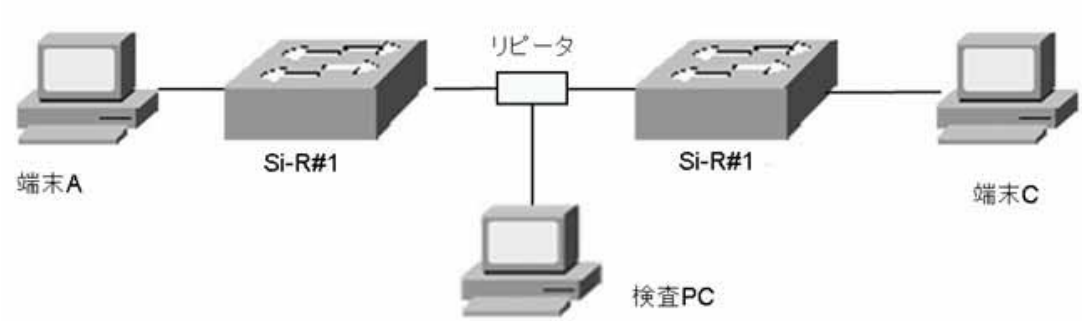

図2-10　**侵入テスト環境（その**2**）**

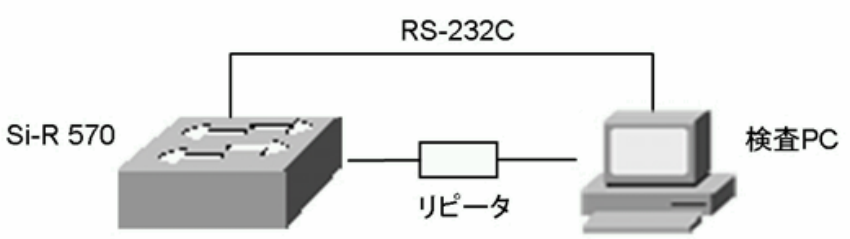

図2-11　侵入テスト環境（その3）

図2-4に示されているテスト環境では、Si-R#1とSi-R#2の組み合わせてとして以下のものがテスト対象となっている。

・Si-R#1：Si-R570　←→　Si-R#2：Si-R570
・Si-R#1：Si-R220C　←→　Si-R#2：Si-R220C
・Si-R#1：Si-R180B　←→　Si-R#2：Si-R240B
・Si-R#1：Si-R260B　←→　Si-R#2：Si-R370

図2-5から図2-8に示されているテスト環境では、Si-R#1、Si-R#2として以下のものがテスト対象となっている。

・Si-R570、Si-R370、Si-R260B、Si-R240B、Si-R220C、Si-R180B

図2-9及び図2-10に示されているテスト環境では、Si-R#1として以下のものがテスト対象となっている。

・Si-R570、Si-R220C（動作するCPUの差異（コンパイラが異なる）を考慮するため）

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a. テスト構成

評価者が実施したテストの構成を図2-4から図2-11に示す。評価者テストはSTにおいて識別されているTOE構成を満たすTOEテスト環境で実施されている。

b. テスト手法

テストには、以下の手法が使用された。

①利用可能な外部インタフェースを持つ機能についてはその外部インタフェースを使用してセキュリティ機能を実行する
②利用可能な外部インタフェースを持たない機能については、セキュリティ機能の実行結果を取得し、ツールを使って解析する

c. 実施テストの範囲

評価者が独自に考案したテストを25項目、開発者テストのサンプリングによるテストを39項目、侵入テストを9項目、計73項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

[評価者が独自に考案したテストの選択基準]
① 使用頻度が高いセキュリティ機能であるIPsecのシーケンス及びパラメータのバリエーションに着目する
② 機能の使用時の環境が安全であり、使用頻度が低い運用支援機能は対象外とする

[開発者テストのサンプリングによるテストの選択基準]
① すべてのセキュリティ機能を網羅する
② すべてのTSFIを網羅する
③ 運用支援機能はすべての機能をテストする
④ IPsecに関する機能（暗号鍵交換機能及びIPsec暗号制御機能）はサンプリングによりテストする

[侵入テストの選択基準]
① IPsecの一部を構成するISAKMPの公知の脆弱性の確認を行う自動テストツール（PROTOS）の実行及び自動テスト後の動作確認をする
② 未確認のサービスの起動確認をする
③ 開発者テストで想定外のISAKMPのパラメータのバリエーション確認をする
④ IPsecのイニシエータとしての不正パケット受信時の動作確認をする

d. 結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。本評価中に発生したTOEの改修においては、改修の影響範囲について実装表現等を用いて分析し、開発者テストの要否を判断した上で、テストが必要であると判断したものについて開発者テストの追加・再実施が行われている。その内容を踏まえて、評価者は、評価者テストの要否を判断した上で、テストが必要であると判断したものについて評価者テストの追

加・再実施を行っている。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL4及び保証コンポーネントALC_FLR.1に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件へ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、機能拡張要件が適切に定義されていることを確認している。保証要件はCCの範囲内であるため、対象外である。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、機能拡張要件の依存性がすべて識別されていることを確認している。保証要件はCCの範囲内であるため、対象外である。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.2.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**

ADV_FSP.2.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.2.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェア、ファームウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_IMP.1.1E	評価はワークユニットに沿って行われ、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが内部的に一貫していることを確認している。
ADV_IMP.1.2E	評価はワークユニットに沿って行われ、実装表現のサブセットがその関連するTOEセキュリティ機能要件を正しく具体化したものであることを確認している。

ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。
ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計の正しく完全な表現であることを、それらの対応分析により確認している。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。

AGD_USR.1.1E	ガイダンスはすべてTOE管理者向けのものであり、利用者が留意するような点は存在しない。よってワークユニットは適応されず満足していることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、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の意図を明確に定義していることを確認している。
ALC_FLR.1E	評価はワークユニットに沿って行われ、TOEの欠陥修正手続きについてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。

ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.2.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、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確認している。

AVA_MSU.2.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.2.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。
AVA_MSU.2.4E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEのすべての操作モードにおいてのセキュアな操作を提供していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.2.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.2.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテストの概要について報告がなされている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用されたTOE特有の略語を以下に示す。

AAA	Authentication, Authorization, Accounting
IKE	Internet Key Exchange
SPD	Security Policy Database

本報告書で使用された用語を以下に示す。

AAA	Authentication, Authorization, Accounting の略語。 認証（Authentication）、承認（Authorization）、アカウンティング（Accounting）のサービスの総称。
IKE	Internet Key Exchange の略語。 IPsec で利用されている暗号鍵交換プロトコル。
IPsec	暗号技術を用いて、パケットデータ単位でデータの改ざん防止や盗聴防止機能を提供するプロトコル。
RSA デジタル署名認証方式	TOE が、通信相手との間で仮想的な通信路を開設する際に行う通信相手を認証する方式の一つであり、通信相手のデジタル証明書又は通信相手のデジタル証明書を発行した認証局のデジタル証明書を事前に Si-R へ登録する方式を示す。
SPD	Security Policy Database の略語。 IPsec で使用する Security Policy を管理するデータベースのこと。
演算チップ	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。
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。

	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。
クイックモード	IPsec の暗号通信で使用するデータ暗号鍵を作成するためのパラメータを折衝する際に利用されるモード。
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。
事前共有秘密鍵	暗号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。
事前共有秘密鍵認証方式	TOE が、通信相手との間で仮想的な通信路を開設する際に行う通信相手を認証する方式の一つであり、通信相手との間で共通の秘密鍵を事前に共有する方式を示す。
デジタル証明書	暗号鍵交換機能で使用する証明書であり、パケットデータ内のデジタル署名を検証するために使用する。
トンネルモード	パケットデータの IP のヘッダを含めた IP パケットデータ全体を暗号化して送信データとした上で、新たに IP ヘッダをつけて送信するモードである。IP のヘッダを含めた暗号化を行うため、IP ヘッダに含まれる最終あて先の IP アドレスも隠蔽できる。
認証局	本人と公開鍵を関連付けるデジタル証明書を発行する第三者機関。
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。
メインモード	通信相手を識別する情報として IP アドレスを使用するモード。これに対し、IP アドレス以外の情報(ID 情報)を使用して通信相手を識別する方法として、アグレッシブモードがある。

6 参照

[1] Si-R Security Software V02.02 セキュリティターゲット 第1.10版（2008年7月7日）富士通株式会社

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 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 バージョン2.3 2005年8月 CCMB-2005-08-001　(平成17年12月翻訳第1.0版)

[9] 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 バージョン2.3 2005年8月 CCMB-2005-08-002　(平成17年12月翻訳第1.0版)

[10] 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 バージョン2.3 2005年8月 CCMB-2005-08-003　(平成17年12月翻訳第1.0版)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] Si-R Security Software V02.02 評価報告書 評価報告書 第3版 2008年9月4日 みずほ情報総研株式会社　情報セキュリティ評価室