認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太 原紙押印済

評価対象

申請受付日（受付番号）	**平成18年12月15日(IT認証6125)**
認証番号	C0112
認証申請者	**富士通株式会社**
TOEの名称	SR-S Security Software
TOEのバージョン	V01.01
PP適合	**なし**
適合する保証パッケージ	EAL4+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19年7月25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　田渕　治樹

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

「SR-S Security Software V01.01」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証手続規程に従い、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、「SR-S Security Software　V01.01」（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：　SR-S Security Software
バージョン：　V01.01
開発者：　富士通株式会社

1.2.2 製品概要

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。

1.2.3 TOEの範囲と動作概要

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。

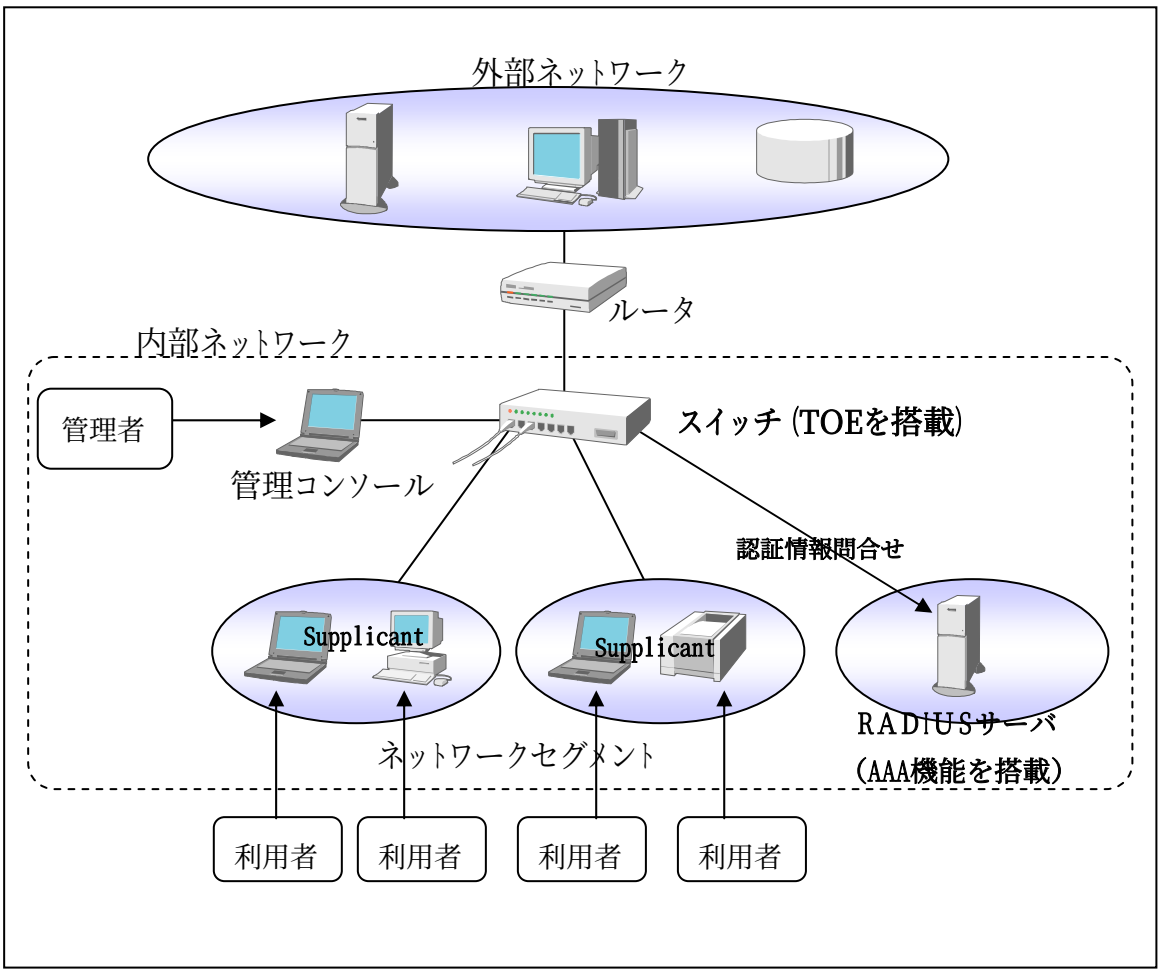

図 1.1 TOEの利用環境の概要

以下に、図1.1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。

1.2.4 TOEの機能

SR-Sでは、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。

SR-Sは以下の機能を持つ。

■ 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。

■ その他のサーバ機能プログラム

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1-１に示す。

	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

表1-1　サーバー機能一覧

■　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。

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セキュリティ認証手続規程」[3]、「評価機関承認手続規程」[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「SR-S Security Software V01.01 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、「SR-S Security Software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19年7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＋ALC_FLR.1適合である。

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への攻撃方法は、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、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。

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

1.5.5 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2　想定する脅威

識別子	脅　威
T.NET_CONNECT	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。

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は存在しない。

1.5.7　構成条件

本セキュリティターゲットは富士通株式会社製の以下の製品の基本ソフトウェアV10.01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。

- SR-S724TC1

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1-３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1-3　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.SUPPLICANT	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	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	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	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。 －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.NETWORK	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。 －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。
A.PASSWORD	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	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。

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
SR-S シリーズ セキュアスイッチ　機能説明書 V10	2007 年 3 月 管理番号： P3NK-2272-02Z0
SR-S シリーズ セキュアスイッチ　コマンド設定事例集 V10	2007 年 2 月 管理番号： P3NK-2322-02Z0
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	2007 年 3 月 管理番号： P3NK-2332-02Z0
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	2007 年 3 月 管理番号： P3NK-2312-02Z0
SR-S724TC1/324TC1 セキュアスイッチ ご利用にあたって V10	2007 年 7 月 管理番号： P3NK-2452-01Z0

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19年1月に始まり、平成19年7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19年2,3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・配付と運用・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。また、平成19年3,4月に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、図2-2に示す。

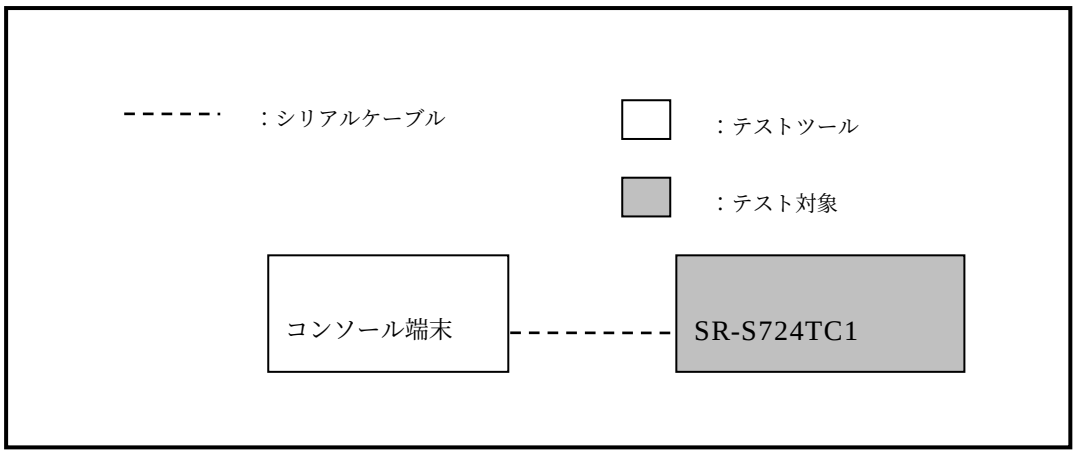

図 2-1 運用支援機能のテスト環境

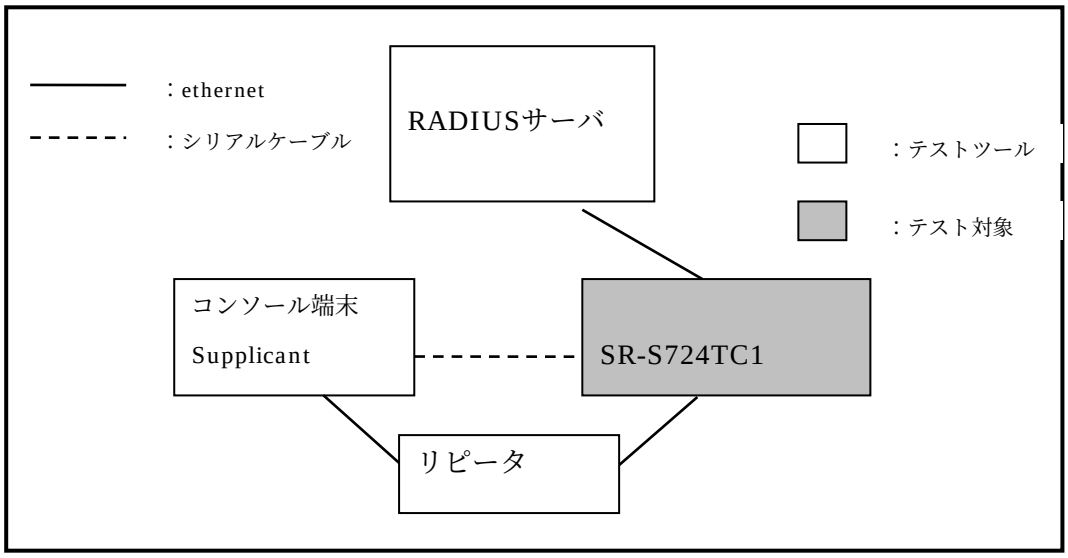

図 2-2 IEEE802.1X認証失敗時の抑止機能のテスト環境

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,図2-2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 TOEから送出されるデータ及びTOEに送られるデータをネットワーク上で取得するツールを使用し、それぞれの間でやり取りされるデータを取得し、解析する方法を採用

② 構成定義の反映インタフェース（IF-1）を使ったテスト（reset、commitコマンド実行）

③ 外部インタフェース（コンソール端末）を利用して、そのふるまいを確認

c.実施テストの範囲

テストは開発者によって41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。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は、開発者テストと同様の構成であり、図2-3の通りである。

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 2-3 に示す。

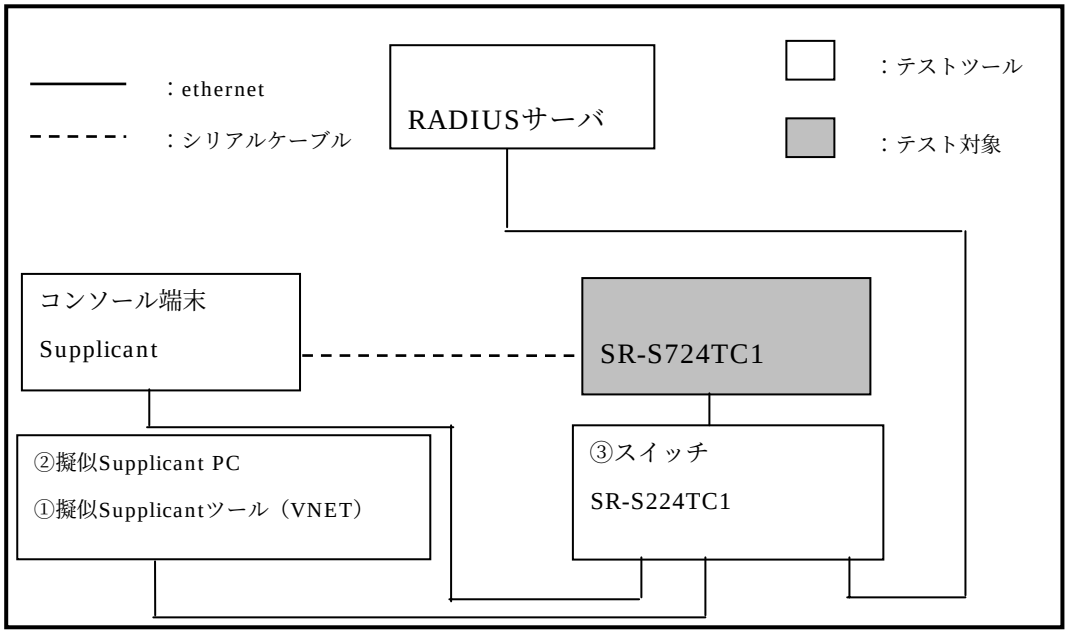

図2-3　評価者テスト環境

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開発者の手動操作により、機能を実行し、動作を観察することによって実施

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し、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3項目、開発者テストのサンプリングによるテストを41項目、計44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。

① 開発者テストからは仕様通りに動作することが疑われるセキュリティ機能

② 他のセキュリティ機能よりも重要なセキュリティ機能

③ 機能強度の対象となるセキュリティ機能

④ 異なるインタフェースから利用される機能

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。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+ALC_FLR.1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。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
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、拡張要件は使われていないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、拡張要件は使われていないため非適用であることを確認している。
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	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、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。
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、侵入テストは、テスト項目が考案されず、侵入テストは実施されないため非適用であることを確認している。
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。

AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

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用語を以下に示す。

利用者	TOE と対話する TOE 外部の任意のエンティティ（人間の利用者や外部 IT エンティティ）
識別情報	許可された利用者を一意に識別する表現（例えば、文字列）で、その利用者のフルネームまたは略称、または仮名。
認証情報	利用要求者の識別情報を検証する際に用いられる情報。
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に接続されたパソコンを示す。操作はコマンドで行う。
コンソールポート	RS-232C の物理インタフェースを示す。 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。
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。
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	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	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。

6 参照

[1] SR-S Security Software V01.01 セキュリティターゲット バージョン 1.20版（2007年7月12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18年9月　独立行政法人 情報処理推進機構　EC-01

[3] ITセキュリティ認証手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-03

[4] 評価機関承認手続規程　平成18年9月　独立行政法人 情報処理推進機構　EC-05

[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] SR-S Security Software V01.01 評価報告書　第2版　2007年7月12日　みずほ情報総研株式会社　情報セキュリティ評価室