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19年4月18日** (IT**認証**7147)
認証番号	C0117
認証申請者	**ヤマハ株式会社**
TOE**の名称**	**ヤマハポリシーフィルタリングモジュール**
TOE**のバージョン**	1.02(2)
PP**適合**	**なし**
適合する保証パッケージ	EAL1
開発者	**ヤマハ株式会社**
評価機関の名称	**社団法人　電子情報技術産業協会　ITセキュリティセンター**

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9月27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

「ヤマハポリシーフィルタリングモジュール」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、「ヤマハポリシーフィルタリングモジュール」（以下「本TOE」という。）について社団法人　電子情報技術産業協会　ITセキュリティセンター（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ヤマハ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：　ヤマハポリシーフィルタリングモジュール
バージョン：　1.02(2)
開発者：　ヤマハ株式会社

1.2.2 製品概要

本製品は、ステートフルインスペクション方式で通信パケットをフィルタリングする機能（以下ポリシーフィルターという）を持つファイアウォール製品である。ヤマハのルーターに搭載されるファームウェアの一部として提供される。機能を実現するルーターには、少なくとも二つの（通信パケットを入出力することができる）LANポートと、一つの制御用のCONSOLEポートを備えている必要がある。このTOEはSRT100に搭載される。

1.2.3 TOEの範囲と動作概要

図1-1にTOEの論理的な範囲を示す。図中の実線はデータの流れを、破線は設定の適用の流れを表している。

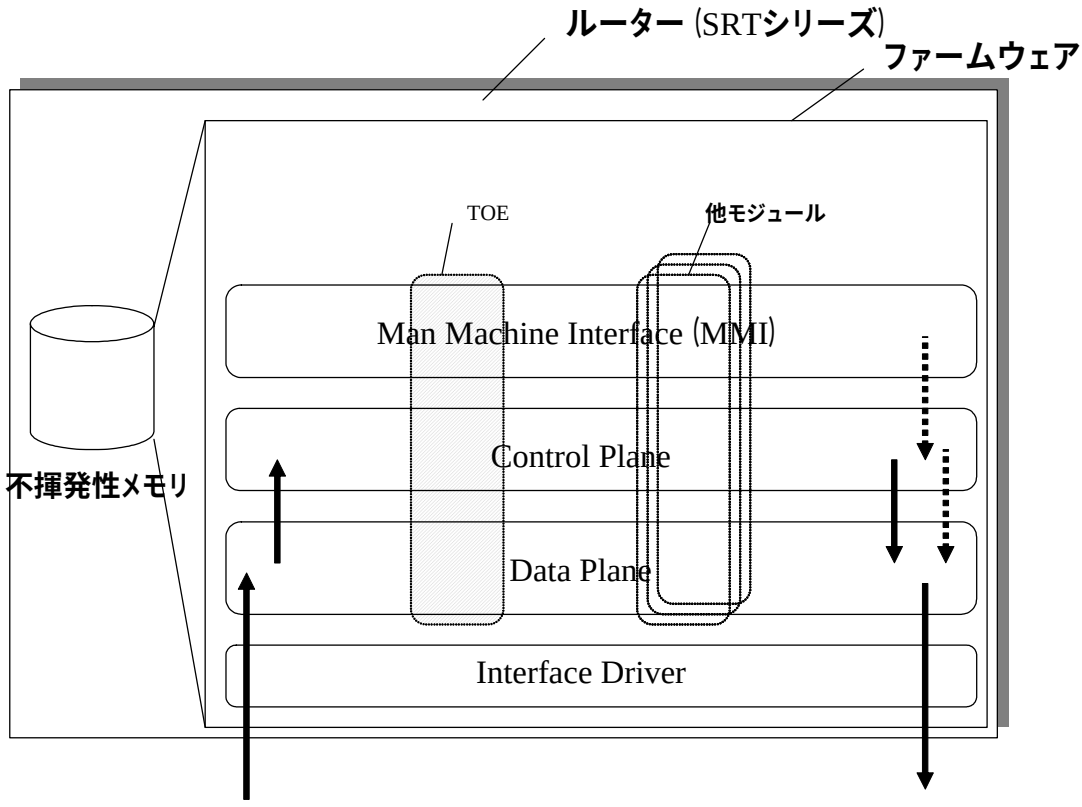


図 1-1 TOEの論理的な範囲

TOEの実装された機器は、内部に書き換え可能な記憶領域（不揮発性メモリ）を装備している。ファームウェアはこの不揮発性メモリに保存される。

ファームウェアは、（MMI、Control Plane、Data Plane、Interface Driver）4つの部分から構成されており、それぞれに役割がある。

Interface Driverは、LAN1ポートやLAN2ポート（通常は外部ネットワーク側のポートとなる）から入力された通信パケットを TOEや他のモジュールが解釈できるフォーマットに変換する役割である。また、TOEや他のモジュールによって処理された後はLAN1ポートやLAN2ポートへ出力される。

Data Planeは、Interface Driverから引き渡されたパケットの中身をチェックし、個々のパケットのフィルタリングやルーティングを行う役割である。この役割はTOEの実装された機器の中核の機能であり、高速に処理を行う必要がある。そのた

め、処理により時間を要する上位層の機能についてはここでは処理しない。例えば、TOEではステートフルインスペクション方式でフィルタリングの処理のみを行う（設定やステートフルインスペクションの状態保持はData Planeでは行わず、Control Planeにて行う）。

Control Planeは、Data Planeで処理する機能以外の動的経路制御プロトコルやVPN、バックアップ管理、その他の上位層の機能を持つ役割である。例えば、TOEはControl Planeでは、ステートフルインスペクションのコネクション状態を保持しており、通信パケットの状態との突合せを行う。ここではData Planeから引き渡されたデータに対してそれぞれの上位層の機能が処理を行う。

MMIは、TOEの実装された機器の設定を行う役割である。MMIで行われた設定は、Control PlaneとData Planeの設定にそれぞれ反映される。例えば、TOEでは、ポリシーフィルターの設定を行ったり、TOE管理のための識別・認証を行ったりする。

ファームウェア内の各モジュールは、（MMI、Control Plane、Data Plane）の3つの部分に縦断的に配置される。

での網掛けの部分が、TOE（ヤマハポリシーフィルタリングモジュール）である。

1.2.4 TOEの機能

TOEが持つ機能を以下に示す。

（1） 識別・認証機能

識別・認証機能は、TOEの実装された機器の設定や設定の参照を行うために必ず実施される識別・認証機能である。識別・認証機能により認証されたユーザーは、ユーザーの属性値（administrator）によって、管理ユーザーへ昇格ができる。また、無操作状態で放置した場合、ユーザーの属性値（login-timer）の設定によって、自動的にTOEからログアウトされる。識別・認証されるユーザーは、「識別・認証管理機能」によりユーザーの追加、削除、属性値の変更がされる。

（2） ポリシーフィルター

ポリシーフィルターは、通信パケットに付属するセキュリティ属性の値を判断に利用し、ステートフルインスペクション方式で通信パケットのフィルタリングを実現する機能である。

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「ヤマハポリシーフィルタリングモジュール 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、「ヤマハポリシーフィルタリングモジュール1.02(2)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、EAL1適合である。

1.5.3 セキュリティ機能強度

本TOEの保証レベルは、EAL1であるため、AVA_SOF.1は含まれない。そのため、SOFを宣言する必要は無い。

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) 識別・認証機能（SF.I&A）

「識別・認証機能」は、TOEの実装された機器の設定や設定の参照を行うために必ず通過しなければならない識別・認証機能である。識別・認証機能により認証されたユーザーは、ユーザーの属性値（administrator）によって、管理ユーザーへ昇格ができる。また、無操作状態で放置した場合、ユーザーの属性値（login-timer）の設定によって、自動的にTOEからログアウトされる。識別・認証されるユーザーは、「識別・認証管理機能」によりユーザーの追加、削除、属性値の変更がされる。

TOEへのログイン手段は、SSH又はCONSOLEポートを利用した場合のみであり、TELNET及びHTTPなど、セキュアな通信が行えないログイン手段は、前提条件から利用しないようにしている。

管理ユーザーがパスワードを忘れてTOEにアクセスできなくなった際に、非常用パスワードを利用してTOEにログインすることができる。CONSOLEポートを経由したターミナルソフトウェアによるアクセスでのみ、非常用パスワードでのログインが可能である。非常用パスワード機能は管理ユーザーによって有効/無効が設定できる。デフォルト設定では、有効（利用できる）に設定されている。

(2) ポリシーフィルター（SF.POLICYFILTER）

本セキュリティ機能は、ポリシーフィルターに関するセキュリティ機能である。ポリシーフィルターに関する機能は、(1)ポリシーフィルターを設定する機能、(2)フィルタリングを実施する機能、(3)ポリシーフィルターに関するログを取得する機能、に分類できる。

① ポリシーフィルターを設定する機能

TOEのユーザーを管理する役割として、管理ユーザーと一般ユーザーが存在する。管理ユーザーは、フィルター条件（ポリシー及びポ

リシーセット）を参照・変更を行うことができ、一般ユーザーは、フィルター条件を参照のみ行うことができる。

ポリシーは、通信パケットの以下のセキュリティ属性値の条件を設定し、その条件にマッチした通信パケットの振る舞い（通過又は遮断）を設定する。

- source_interface
- dest_interface
- source_address
- dest_address
- service

IPアドレスにはIPv4とIPv6アドレスを指定できる。それぞれのセキュリティ属性は、それらの管理を容易にするためにグループ化して名前を付与することができる。

ポリシーを複数組み合わせてフィルタリングのルールとして作成する。ルールは階層構造をとることができ、最大4階層までの設定ができる。ポリシーを複数組み合わせたものは、ポリシーセットと呼ばれる。

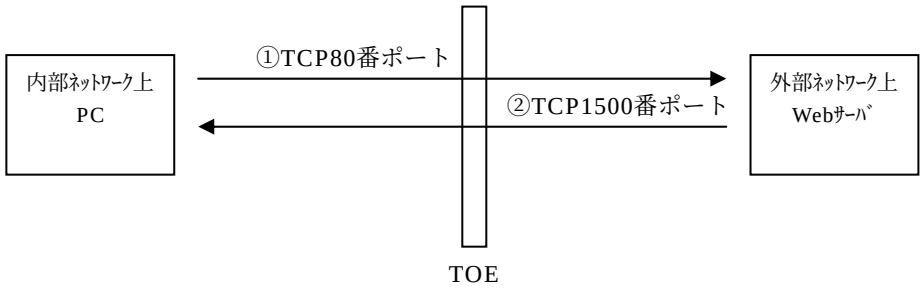
通信パケットがポリシーとマッチした際のTOEの動作として、表1-1の4通りが設定できる。

表 1-1　通信パケットがポリシーとマッチした際のTOEの動作

項番	動作	説明
1.	pass	通信パケットを通過させる。TCPとUDPとpingについては、 ステートフルインスペクション方式で通過させ、それ以外の通信パケットについては、そのまま通過させる
2.	static-pass	ステートフルインスペクション方式を使わずに通信パケットを通過させる
3.	reject	通信パケットを遮断する
4.	restrict	通信パケットを送信しようとするインタフェースがupしており、通信パケットを送信できる状態になっているならば通過させ、 そうでなければ通信パケットを遮断する。通信パケットを通過させる時には、TCPとUDPとpingについては、 ステートフルインスペクション方式で通過させ、それ以外の通信パケットについては、そのまま通過させる

② フィルタリングを実施する機能

TOEは、TOEに入力された全ての通信パケットのセキュリティ属性を確認し、ポリシーとのマッチングを行うことでステートフルインスペクション方式にてフィルタリングを行う（図 1-2参照）。また、ステートフルインスペクション方式での通過が許可される条件は表 1-2のとおりである。



ポリシーフィルター設定を以下のように設定したと仮定する。
- 内部ネットワークから外部ネットワークへは全端末から HTTP（TCP80 番ポート）のみステートフルインスペクション方式で通過を許可する。
- 外部ネットワークから内部ネットワークへは全ての通信を遮断する。

内部ネットワーク上PCから外部ネットワーク上Webサーバへアクセスした際のフローは以下のようになる。
① 内部ネットワーク上 PC から外部ネットワーク上 Web サーバへ TCP80 番ポートでリクエストを送信する。
② TOE は、ステートフルインスペクション方式にて、①の応答であることを確認し、通過を許可する。
③ ・・・

つまり、通常は遮断されるはずである外部ネットワークからの通信が、内部ネットワークからのリクエストに対する適切な応答であった場合のみ通過が許可されるように、必要に応じて動的にポートが開閉する方式がステートフルインスペクション方式である。

図 1-2　ステートフルインスペクション方式の通信イメージ

表 1-2　ステートフルインスペクション方式で通過が許可される条件

項番	TCP*1 又は UDP*2	アプリケーション*3	アプリケーション固有の許可条件*4（ポートを開く条件、ポートを閉じる条件）
1.	TCP	FTP（制御用のコネクション）	（ポートを開く条件）21番ポート宛てのTCPコネクションが発生し、それに対する応答パケットを検知した場合
			（ポートを閉じる条件）そのコネクションに属するパケットが一定時間*5発生しないか、RST/FINを受信して一定時間*5経った場合
2.	TCP	FTP（データ転送用のコネクション）	（ポートを開く条件）あらかじめ制御用のコネクションにおけるPORT/PASV/EPRT/EPSVコマンドでポート番号の交渉ができている場合
			（ポートを閉じる条件）制御用のコネクションと同様
3.	UDP	TFTP	（ポートを開く条件）TFTPコマンドの最初のパケットに対する応答ACKパケットが来た場合
			（ポートを閉じる条件）データ部が短い(512バイト未満)DATAパケットに対するACKパケットを受信した場合（一定時間*5を短縮させそのタイムアウトによって閉じる）
4.	UDP	DNS	（ポートを開く条件）問い合わせパケットに対する応答パケットが来た場合
			（ポートを閉じる条件）応答パケットが通過するかあるいは一定時間*5経過した場合
5.		PING	（ポートを開く条件）要求パケットに対して応答パケットが来た場合

項番	TCP*1 又は UDP*2	アプリケーション*3	アプリケーション固有の許可条件*4 （ポートを開く条件、ポートを閉じる条件）
			（ポートを閉じる条件）要求パケットが発生してから応答パケットが一定時間*5全くないか、あるいは応答パケットが一つでも通過してから一定時間経過した場合

*1 TCPでは、内部ネットワークから最初のパケットが発生して確立されたTCPコネクションのパケットについて、一定時間*5内に通信がある限り外部ネットワークから来たものの通過を許可（ポートを開く）する。またそのTCPコネクションでFINやRSTパケットが観測されると一定時間*5を短縮し、そのタイムアウトによってポートを閉じる。

*2 UDPでは、内部ネットワークから外部ネットワークへ通信が発生した場合に、外部ネットワークから内部ネットワークへの応答パケットの通過を許可（ポートを開く）する。該当ポートでパケットのやりとりが一定時間*5なければタイムアウトし、ポートを閉じる。

*3 ここで挙げた以外のアプリケーションは、そのアプリケーション固有の許可条件はなく、利用するTCP及びUDPの処理のみ適用される。

*4 TCP、UDPとは別にアプリケーション固有の通過が許可される条件が適用される。

*5 一定時間は、ip policy filter timerコマンドでそれぞれ以下のように変更することができる。

オプション名	意味
tcp-syn-timeout	SYNを受けてから設定された時間内にデータが流れなければセッションを切断する
tcp-fin-timeout	FINを受けてから設定された時間が経てばセッションを強制的に解放する
tcp-idle-time	設定された時間内にTCPセッションのデータが流れなければセッションを切断する
udp-idle-time	設定された時間内にUDPセッションのデータが流れなければセッションを切断する
dns-timeout	DNSのqueryを受けてから設定された時間内にデータが流れなければセッションを切断する
icmp-timeout	設定された時間内にICMPセッションのデータが流れなければセッションを切断する (pingに適用される)

(3)　ポリシーフィルターに関するログを取得する機能

ポリシーフィルターは、ログ管理機能に対して以下の条件にて監査情報（ログ）を出力する。

- ポリシーに合致するコネクションやパケットの発生の際に監査する
（追加の監査情報）ポリシー番号、プロトコル、パケットの情報
- ポリシーフィルター変更の際に監査する
（追加の監査情報）なし
- ポリシーフィルター設定情報の参照の際に監査する
（追加の監査情報）なし

取得されるログの監査情報は、「事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)、上記の追加の監査情報」である。日付・時刻は、ログ管理機能によりログ出力時に付与されるため、TOEは付与しない。

設定変更、参照他コマンド実行のログ出力はsyslog execute commandで設定できる。またnoticeレベルのログは主にフィルタリングで処理されるパケットに関わる情報のログである。この出力を行うか否かをsyslog noticeコマンドで設定できる。

なお、識別・認証機能とポリシーフィルターのログ出力の起動と終了（監査の起動と終了）は、それぞれが独立して起動あるいは終了できるものではなく、同一の操作により行われる。監査の起動と終了は、管理ユーザーのみ切り替えることができ、そのログは、関連するコマンド実行の組み合わせのログを確認することにより判断することができる。

ログの出力のON（監査の起動）：

- syslog execute command onかつ
- syslog info onかつ
- syslog notice on

ログ出力例：

2007/05/30 17:32:13: [MMI] Executed by Serial(user): syslog execute command on

2007/05/30 17:32:16: [MMI] Executed by Serial(user): syslog info on

2007/05/30 17:32:20: [MMI] Executed by Serial(user): syslog notice on

ログの出力のOFF（監査の終了）：

- syslog execute command offあるいは
- syslog info offあるいは
- syslog notice off

ログ出力例：

2007/05/30 17:32:46: [MMI] Executed by Serial(user): syslog notice off

2007/05/30 17:32:50: [MMI] Executed by Serial(user): syslog execute command off

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.NET_FLOW	悪意ある者は、外部ネットワークからアクセスが許可されていない内部ネットワークリソースに対して不正にアクセスするかもしれない。
T.NOAUTH	悪意ある者は、TOEの設定を不正に変更し、内部ネットワークリソースへの不正アクセスを試みるかもしれない。

1.5.6 組織のセキュリティ方針

本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ヤマハ株式会社製のSRT100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。

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1-４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1-4　TOE使用の前提条件

識別子	前提条件
A.ENVIRONMENT	システム管理者は、システム管理者以外触れられない場所にTOE及び、TOEにCONSOLEポートで接続するPCを設置する。
A.ADMIN_USER	システム管理者は、信頼でき、悪意を持った行動はしないものとする。
A.MANAGE	管理ユーザーは、以下の運用を行う。 ・ 必要最低限のユーザーを作成すること ・ 一般ユーザー及び管理ユーザーのパスワードは 15 文字以上で設定すること
A.CONFIG	管理ユーザーは、以下の設定を行う。 ・ ポリシーを最低 1 つ以上設定すること ・ TOE を管理する際の一般ユーザー及び管理ユーザーの TOE への通信手段として、CONSOLE ポート又は SSH のみ利用できるように設定する（他の通信手段を利用できないようにする）こと ・ TOE が動作する上で必要なポート（LAN ポート、CONSOLE ポート）以外は利用できないようにすること
A.BOUNDARY	システム管理者は、内部ネットワークと外部ネットワークを接続する口は1つとし、その境界にTOEを設置する。

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。

・コマンド設定運用説明書（0707　第1版）
・コマンドリファレンス(0707　第11版)
・お知らせ（0707　第1版）

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4月に始まり、平成19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19年7月に開発者サイトで開発者のテスト環境を使用し、評価者テストを実施、その後評価者サイトにて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

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 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2-1～図2--3に示す。

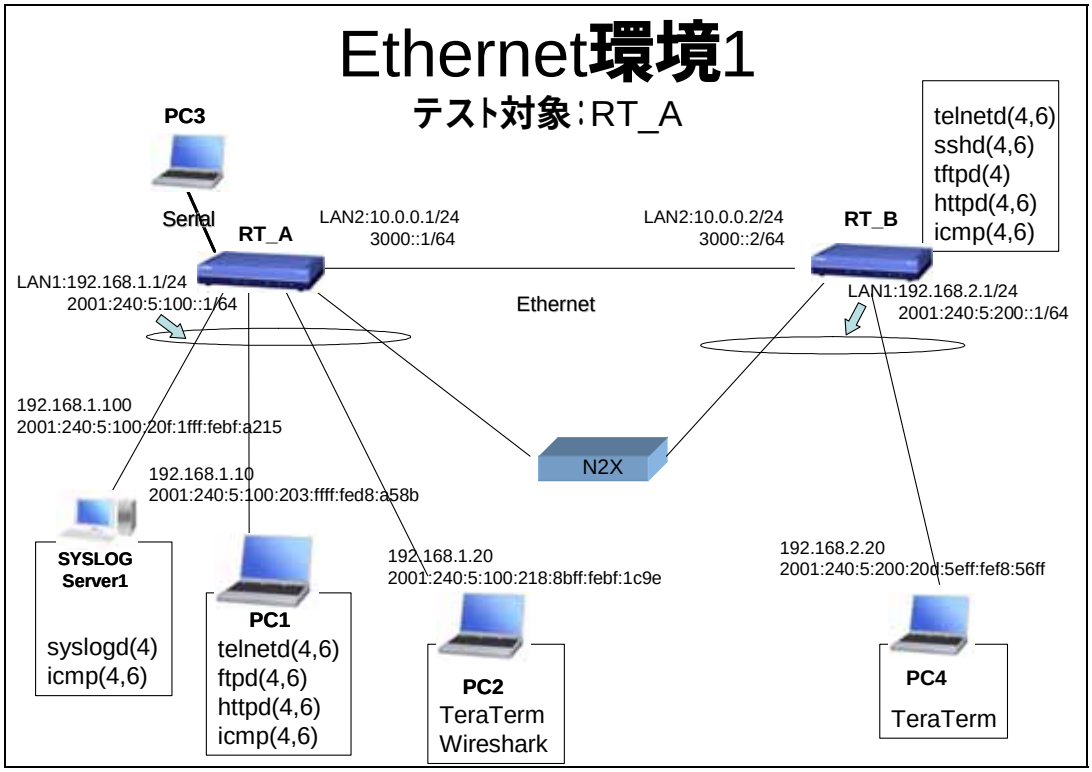


図2-1　評価環境(1)

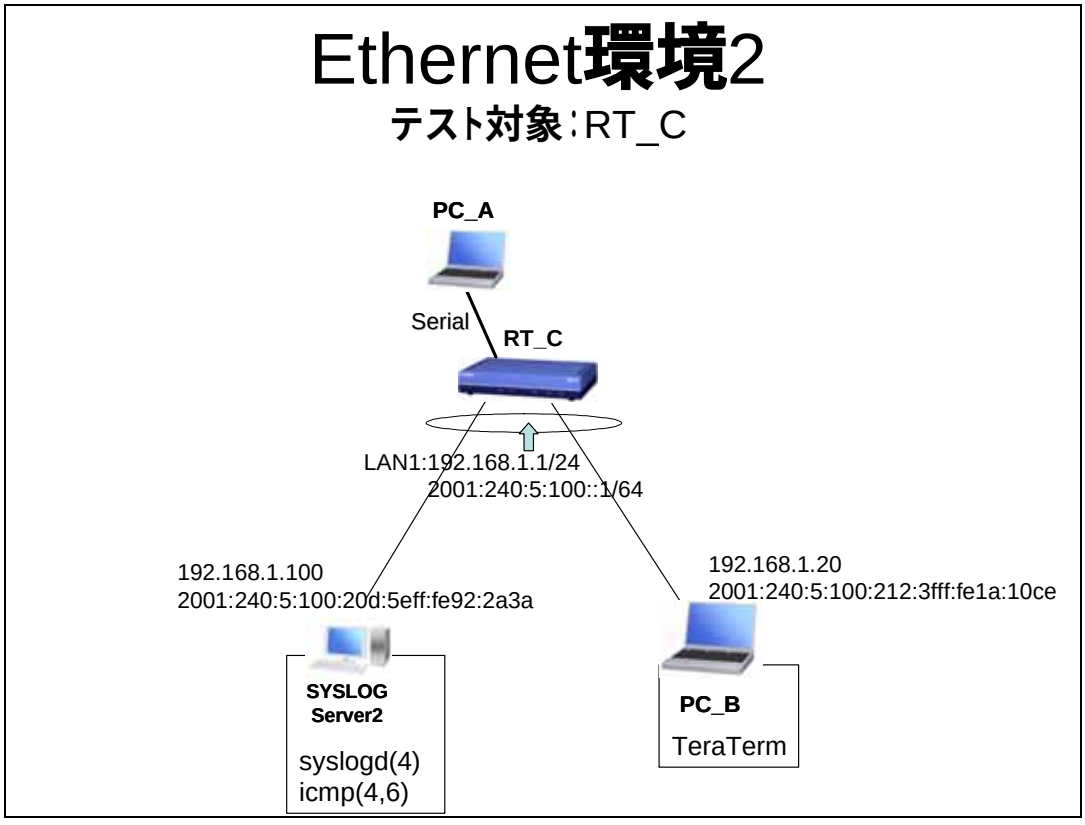


図2-2　評価環境(2)

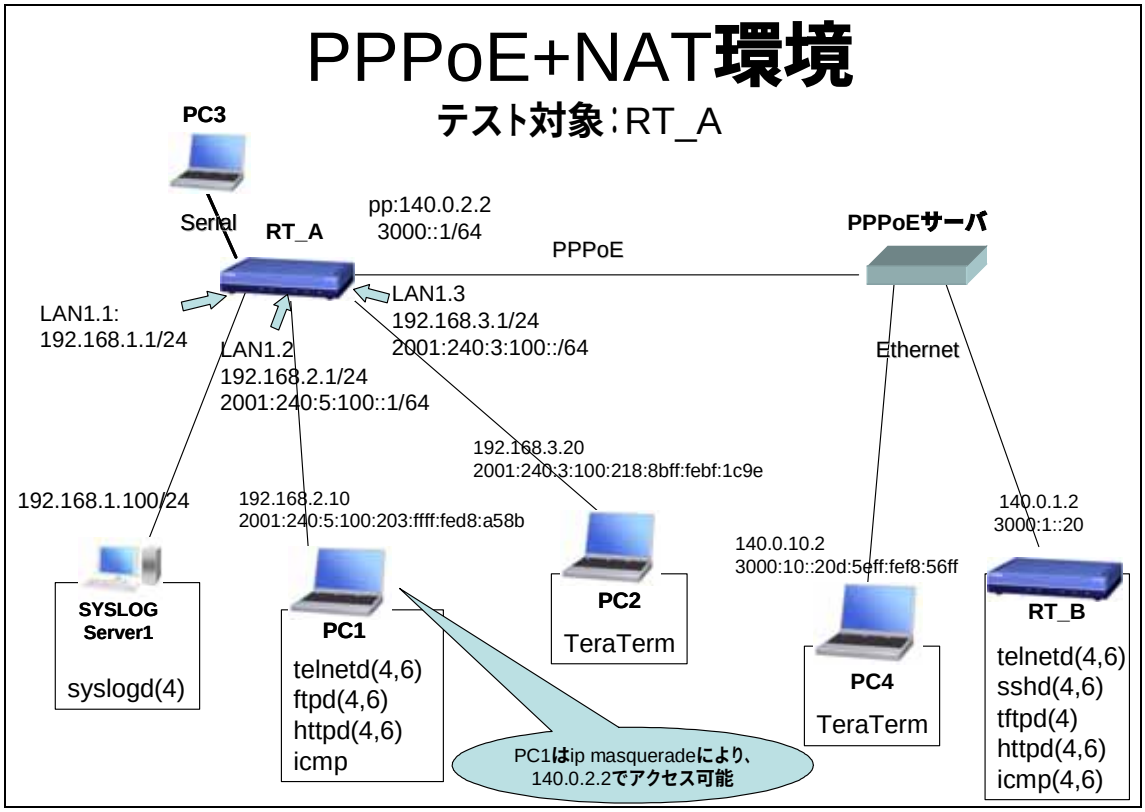


図2-3 評価環境(3)

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2-1～図2-3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の種別に一般的に関係する、知られている公知の弱点の評価
デフォルトパスワードの無効化の確認

② 各セキュリティ機能のTSFIによる動作確認
IPv6、IPv4を交えたフィルタリング機能の確認

③ 管理機能をコンソールポート、LANインタフェース両面からの動作確認

c.実施テストの範囲

評価者が独自に考案したテストを215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 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EAL1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、CCを参照せずに明示された要件は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、CCを参照せずに明示された要件は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_CAP.1.1E	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。
配付と運用	**適切な評価が実施された**
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.1.1E	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.1.2E	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_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ることを、それらの対応分析により確認している。
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。
テスト	**適切な評価が実施された**
ATE_IND.1.1E	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が正しく設定されていることを確認している。
ATE_IND.1.2E	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。

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。

ルーター	ネットワーク上に流れるデータを他のネットワークにルーティング（経路選択）する機器、及びそのようなソフトウェアのことである。OSI参照モデルでいうところの第3層（ネットワーク層）と第4層（トランスポート層）のプロトコルを解析し、転送処理を行う。ルーターが処理できないパケットや、管理ユーザーが遮断するよう設定したパケットがルーターに到着した場合、そのパケットを廃棄するなど、フィルタリング機能を持つものがほとんどである。
フィルタリング	ルーターを通過するパケットやコネクションを解析し、IPアドレス、プロトコルやポート番号などの情報から、通過を許可したり、拒否したりするためのふるいにかける機能のことである。どのパケットを許可・拒否するかは、管理ユーザーが事前に設定をする。
ファームウェア	ルーターのハードウェアに組み込まれたソフトウェアのことである。書き換え可能な不揮発性メモリにインストールされており、アップデートにより継続して機能拡張やバグフィックスの修正を行うことができる。本TOEはルーターのファームウェア内の1機能として提供される。
モジュール	１つの機能を実現するためのソフトウェアの集合のことである。

ターミナルソフトウェア	端末として動作するアプリケーションのことであり、遠隔地に設置されたサーバやネットワーク機器を操作するために利用するものである。ターミナルソフトウェアは、端末エミュレータとも呼ばれ、Windowsではハイパーターミナル、Unix系ではGNOME端末、ktermなどがある。
ステートフルインスペクション	TCPやUDPでの通信のやり取り（状態）を保持しておき、正常なやり取りではない場合などに通信を遮断する機能のことである。パケットのヘッダを解析してフィルタリングするダイナミックパケットフィルタリングに対して、パケットの情報の内容まで解析し、フィルタリングを行う。セキュリティ的にはパケットの偽装対策に効果がある。
ポリシー	通信パケットの状態によって、通過・遮断を定義したもののことである。「LAN2からLAN1へ抜けるTELNETを破棄する 」、「LAN1からLAN2へ抜けるpingを許可する 」などのように、フィルター条件と動作を組み合わせて定義する。
ポリシーセット	ポリシーフィルターでの、ポリシーを適用される順に並べたもののことである。ポリシーは適用される順番に評価されていき、一致するポリシーの動作内容によって通過・遮断がされる。また、順番に評価され一つも一致するポリシーが無かった場合、その通信パケットは遮断される。ただし、フィルター条件が一つも設定されていない場合は、通信パケットは全て通過する。
内部ネットワークと外部ネットワーク	ルーターを境界に、情報資産が存在する側を内部ネットワーク、そうではない側を外部ネットワークと呼ぶ。
非常用パスワード	管理ユーザーがパスワードを忘れてTOEにアクセスできなくなった際に、非常用パスワードを利用してTOEにログインすることができる。CONSOLEポートを経由したターミナルソフトウェアによるアクセスでのみ、非常用パスワードでのログインが可能である。非常用パスワード機能は管理ユーザーによって有効/無効が設定できる。デフォルト設定では、有効（利用できる）に設定されている。

6 参照

[1] ヤマハポリシーフィルタリングモジュール　セキュリティターゲット バージョン1.14（2007年9月14日）ヤマハ株式会社

[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] ヤマハポリシーフィルタリングモジュール1.02(2) 評価報告書 第1.2版 2007年9月14日
社団法人電子情報技術産業協会IT セキュリティセンター