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7月7日** (IT**認証**6088)
認証番号	C0110
認証申請者	**富士ゼロックス株式会社**
TOE**の名称**	Firewall for beat-box
TOE**のバージョン**	v1.0.0
PP**適合**	**なし**
適合する保証パッケージ	EAL3+ADV_LLD.1+ADV_IMP.1+ALC_TAT.1+AVA_VLA.2
開発者	**富士ゼロックス株式会社**
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

「Firewall for beat-box」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、「Firewall for beat-box」（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ゼロックス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：　Firewall for beat-box
バージョン：　1.0.0
開発者：　富士ゼロックス株式会社

1.2.2 製品概要

「beat」とは、富士ゼロックス株式会社が展開するオフィスネットワーク管理のアウトソーシングサービスである。このサービスの中で、ブロードバンド回線に接続するオフィスネットワーク内に設置されるサーバが「beat-box」である。この「beat-box」は、ファイアウォール機能以外にアンチウイルス機能、共有フォルダ機能、簡易グループウェア機能といった様々な機能を提供する。

本 TOE である「Firewall for beat-box」は、「beat-box」においてファイアウォール機能を実現するソフトウェアであり、ファイアウォール機能として外部からのアクセスを受け付けない「完全遮蔽方式」を実現するトラフィックフロー制御機能を TOE は提供する。

TOE は、beat-box 内部で動作する TOE 外のアプリケーションと協調して動作する仕組みにより、beat-noc や他の beat-box との VPN 接続、インターネットを経由したリモートアクセスなどの許可されたサービスを利用可能とするためのトラフィックフローの設定変更を受け付ける。

1.2.3 TOEの範囲と動作概要

beat-box内のプログラムと、TOEの物理的構成を図1-1に示す。

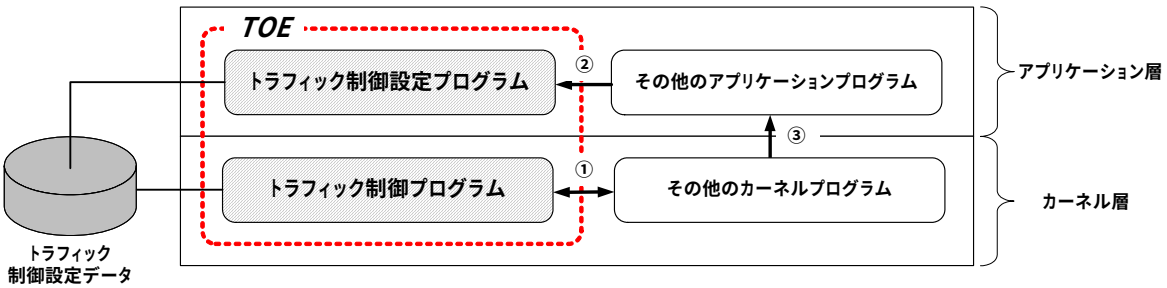

図1-1 TOEの物理的構成とプログラム構成

beat-box内には、メモリ管理、プロセス管理、パケット送受信処理といったカーネルプログラムや、トラフィック制御プログラムが処理するパケットに応じてトラフィック制御設定データを動的に変化させるためのアプリケーションを始めとして、Windows互換ファイルサーバを実現するプログラム、ウイルスチェックするプログラムなど各種アプリケーションプログラムなどが存在する。この中でファイアウォール機能を実現する2つの中核プログラムがTOEである。具体的にはアプリケーション層の「トラフィック制御設定プログラム」とカーネル層の「トラフィック制御プログラム」から構成される。

トラフィック制御プログラムは、その他のカーネルプログラムにあるパケット送受信プログラムにフックポイントを持つプログラムであり、チェックサム処理、ヘッダー解析処理などの処理の過程において、当該プログラムに処理が受け渡されてフィルタリング処理等を行った上で、その他のカーネルプログラムへ処理をリターンする。(図中：①)

トラフィック制御設定プログラムは、トラフィック制御プログラムの動作を決定するトラフィック制御設定データを編集するためのプログラムである。図中その他のアプリケーションで示されるプログラム群からの指示（図中：②）によって動作する。その他のアプリケーションプログラムは、その他のカーネルプログラム中のパケット送受信プログラムよりトラフィック制御設定データを変更する必要のあるパケットを捕捉（図中：③）した場合にトラフィック制御設定プログラムに対して変更する設定データ情報を通知する。

1.2.4 TOEの機能

TOEは以下の機能を提供する。

○トラフィックフロー制御機能

TOEは、外部ネットワークとbeat-box間の通信、内部ネットワークとbeat-box間の通信及び、外部ネットワークと内部ネットワーク間の通信に関わる全てのIPパケットに対して、トラフィックフローの制御を行う。

- 完全遮蔽方式フロー制御

  トラフィック制御の設定に基づき、通信データの送受信可否を行う。トラフィック制御の設定は、初期設定データが適用された後、トラフィックの制御が一旦開始されると、通信の状態に応じて適切に変更されてゆく。

- NAPT情報フロー制御

  Network Address Port Translation（NAPT）によって内部ネットワークに接続するエンティティが外部ネットワークにアクセスする際、内部ネットワークのプライベートアドレス、送信元ポート番号を変換して、内部ネットワークの情報を外部に送信せず、通信を確立する。

- ステートフル情報フロー制御

  確立された通信は、通信が終了するまで記録管理され、不正なパケットが紛れ込んだ場合でも記録管理される一連のデータストリームと認められない場合は、排除する仕組みを有する。

○レポーティング機能

IPパケットのトラフィックフロー制御機能の動作ログとして、特徴的なシグネチャのポートスキャン、連続したpingなどの回数をレポートに出力する。なお本機能はセキュリティ機能には該当しない。

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「Firewall for beat-box　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、「Firewall for beat-box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、EAL3追加である。

追加されるコンポーネントはADV_LLD.1、ADV_IMP.1、ALC_TAT.1及びAVA_VLA.2である。

1.5.3 セキュリティ機能強度

本TOEでは、確率的または順列的メカニズムを利用する機能は存在しないため、最小機能強度レベルの主張は行なわない。

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「1.2.4 TOEの機能」にも示されているト

ラフィック制御機能である。

○トラフィックフロー制御機能

TOEは、外部ネットワークとbeat-box間の通信、内部ネットワークとbeat-box間の通信及び、外部ネットワークと内部ネットワーク間の通信に関わる全てのIPパケットに対して、トラフィックフローの制御を行う。

- 完全遮蔽方式フロー制御

トラフィック制御の設定に基づき、通信データの送受信可否を行う。トラフィック制御の設定は、初期設定データが適用された後、トラフィックの制御が一旦開始されると、通信の状態に応じて適切に変更されてゆく。

- NAPT情報フロー制御

Network Address Port Translation（NAPT）によって内部ネットワークに接続するエンティティが外部ネットワークにアクセスする際、内部ネットワークのプライベートアドレス、送信元ポート番号を変換して、内部ネットワークの情報を外部に送信せず、通信を確立する。

- ステートフル情報フロー制御

確立された通信は、通信が終了するまで記録管理され、不正なパケットが紛れ込んだ場合でも記録管理される一連のデータストリームと認められない場合は、排除する仕組みを有する。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1　想定する脅威

識別子	脅　威
T.ACCESS	＜beat-box及び内部ネットワークへの不正アクセス＞ 攻撃者は、インターネットなどの外部ネットワークに接続し、beat-box及びbeat-boxが保護している内部ネットワークに対してアクセスする。 この攻撃は、beat-boxの存在を検知し、beat-boxにアクセスすることにより、beat-boxの権限を不正に取得し、beat-boxの設定の変更、不正利用、およびbeat-boxが保有しているデータの暴露、改竄または破壊を行うことを目的としている。またbeat-boxを介して内部ネットワークにアクセスすることにより、内部ネットワークに接続している機器の権限を不正に取得し、機器の設定の変更、不正利用、および機器が保有しているデータの暴露、改竄または破壊を行うことを目的としている。
T.ATTACK	＜不正パケットによる不正アクセス＞ 攻撃者は、インターネットなどの外部ネットワークに接続し、beat-boxが保護している内部ネットワークに対してアクセスする。 この攻撃は、内部ネットワークからの正常な通信に対する応答に見せかけるなどして、不正なパケットを通過させ、内部

	ネットワークに接続している機器の権限を不正に取得し、機器の設定の変更、不正利用、および機器が保有しているデータの暴露、改竄または破壊を行うことを目的としている。
T.SPOOF	＜beat-noc等への成りすまし＞ 攻撃者は、beat-noc、RAS接続許可クライアント、VPN接続許可拠点のbeat-boxを詐称し、正当な通信になりすましてアクセスする。 この攻撃は、内部ネットワークに対する不正アクセスなどの不正行為を目的としている。
T.SNIFF	＜beat-noc等の通信経路上の盗聴＞ 攻撃者は、beat-noc、RAS接続許可クライアント、VPN接続許可拠点のbeat-boxと外部ネットワークとの通信経路で盗聴を行う。 この攻撃は、盗聴によって知り得た通信内容を利用して、beat-boxや内部ネットワークに対する不正アクセスや情報の暴露などの不正行為を目的としている。

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ない。

1.5.7 構成条件

以下がTOEの評価において検証環境として利用したbeat-box 2の詳細情報である。

○TOEが搭載されるbeat-boxの出荷ソフトウェア　：V2.9.22

○更新用beat-box II対応モジュール　：Ver2.3.2

（シグネチャー発行日：2006/11/14）。

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1-2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1-2　TOE使用の前提条件

識別子	前提条件
A.USER	＜内部ユーザの信頼性＞ beat-boxが保護している内部ネットワーク上のユーザは、その所属する組織が責任を持って業務管理とスキル管理が行われる。また内部ユーザがbeat-boxや、外部ネットワークに対して保護を必要とする情報を流出させるなどの、セキュリティに

	関する不正行為は起こさないものとする。
A.NOC	＜beat-nocの信頼性＞ beat-boxを遠隔管理しているbeat-nocオペレータは、課せられた役割を遂行するために必要な知識を有し、beat-boxへの不正な行為は起こさないものとする。
A.PLACE	＜beat-boxの設置条件＞ beat-boxは、侵入者によるハードへの攻撃から回避されるべく適切な場所に設置される。したがって、beat-boxへの物理的な攻撃は行われないものとする。

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。

・beat-boxに搭載される管理用Webページ内の「ISO/IEC15408認証の前提条件」の説明ページ。

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18年8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18年11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18年12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、評価者テスト及び侵入テストを実施した。

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に示す。

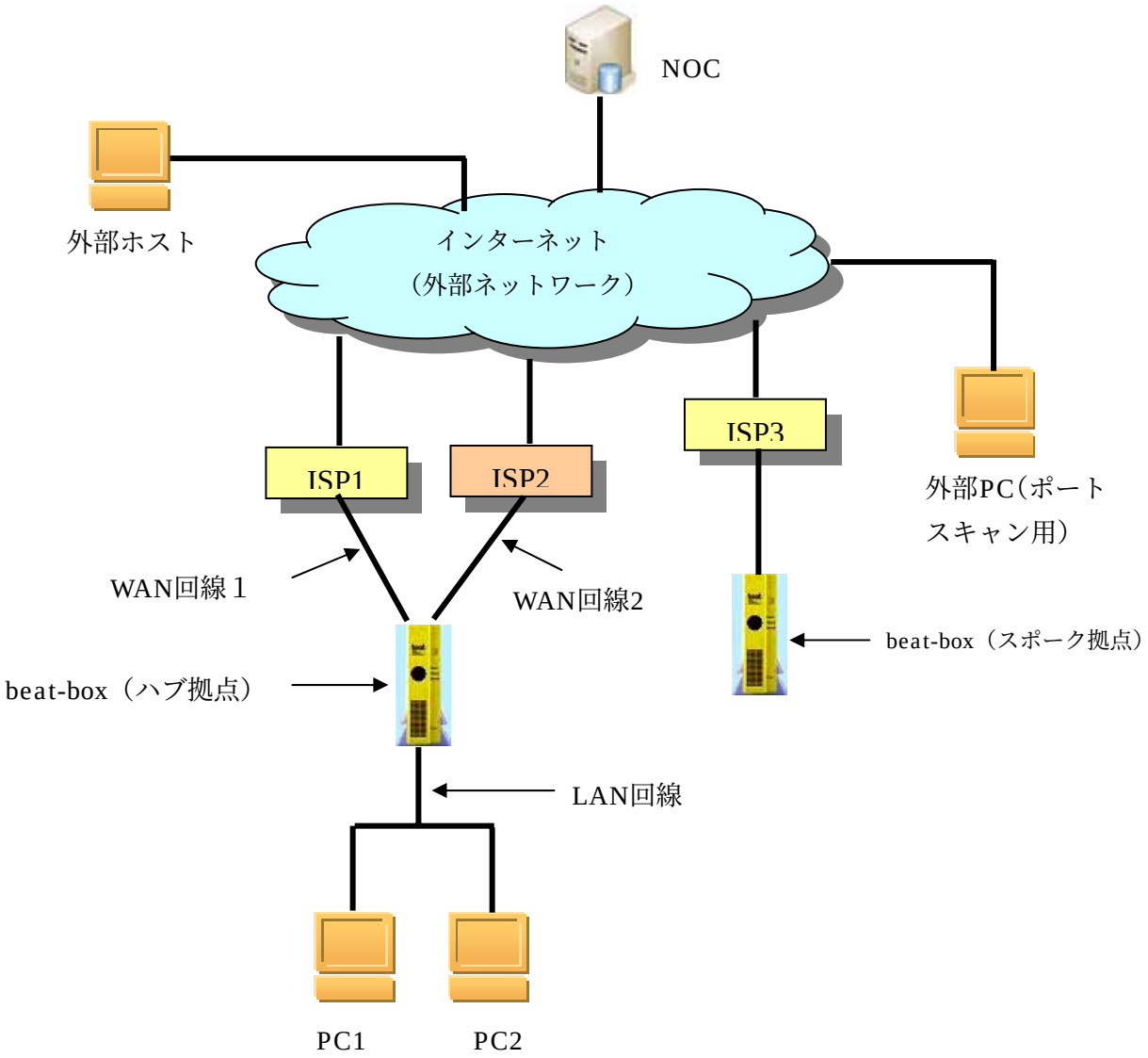

図2-1　開発者テストの構成図

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構成と同様の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、nmap（ポートスキャンツール）やhping（汎用IPパケット送信ツール）等を利用し、トラフィックフロー制御機能が正しく作動しているかの検査が実施されている。

c.実施テストの範囲

テストは開発者によって15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2-1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、pingコマンドやnetstatコマンド等を利用し、トラフィックフロー制御機能が正しく作動しているかの検査が実施されている。

c.実施テストの範囲

評価者が独自に考案したテストを10項目（評価者独立テスト6項目、侵入テスト4項目)、開発者テストのサンプリングによるテストを6項目、計16項目のテストを実施した。テスト項目の選択基準（①～②：評価者独立テスト、③～⑤：侵入テスト）として、下記を考慮している。

① 開発者テストにおけるテスト網羅度
② TOEの機能特性（完全遮蔽）を考慮してのフロー制御テスト
③ TOEの特性を考慮した脆弱性探索ツールの利用
④ ポートスキャンツール（Nmap）を利用したポートの開閉確認テスト
⑤ IPの偽装を考慮した接続テスト

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EAL3保証要件、ADV_LLD.1、ADV_IMP.1、ALC_TAT.1及びAVA_VLA.2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、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.3.1E	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.1.1E	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.1.1E	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.1.2D	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.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_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、実装表現が下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。

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_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。
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.1.1E	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.1.2E	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.1.3E	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_SOF.1.1E	評価はワークユニットに沿って行われ、TOEには確率的または順列的メカニズムが存在しないため、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、TOEには確率的または順列的メカニズムが存在しないため、SOF主張が満たされている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、開発者の脆弱性分析書を分析した結果、その脆弱性分析において疑わしい点、不足不備が見受けられないことが確認されたため、開発者の脆弱性分析に基づく侵入テストの実施は実施していない。
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。

beat-box	富士ゼロックス株式会社が開発した高機能アプライアンスサーバ
beat-noc	beat-boxのリモート管理を実施するインターネット上のネットワーク管理センター

6 参照

[1] Firewall for beat-box セキュリティターゲット バージョン 8（2007年7月9日）

[2] ITセキュリティ評価及び認証制度の基本規程　平成17年7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17年7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17年7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] Firewall for beat-box評価報告書 第2版 2007年7月9日