保証クラス	セキュリティターゲット（ASE クラス）
保証ファミリ	—
略名	ST
改定日	2007/07/09
総ページ数	47 ページ（表紙含む）

Firewall for beat-box

セキュリティターゲット（ASE クラス）

富士ゼロックス株式会社

オフィスサービス事業本部

ブロードバンド事業開発部

目次

1 ST 概説

本節では、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.　ST 識別

・ST 識別　　：Firewall for beat-box　セキュリティターゲット
・バージョン　：8
・作成者　　：富士ゼロックス株式会社　藤本 厚史
・作成日　　：2007 年 7 月 9 日
・CC 識別　　：CC v2.3
・PP 識別　　：なし
・キーワード　：ファイアウォール、完全遮蔽方式

2.　TOE 識別

・TOE 識別　　：Firewall for beat-box v1.0.0
・バージョン　：v 1.0.0
・TOE 種別　　：ソフトウェア
・製造者　　：富士ゼロックス株式会社

1．2　ST 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高機能アプライアンスサーバが「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。

本セキュリティターゲットは、「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る Firewall for beat-box を TOE とし、TOE が提供するファイアウォール機能のセキュリティ仕様について記述したものである。

具体的には、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。

1．3　保証評価レベル

TOE の評価保証レベルは EAL3+である。追加される保証要件は以下の通りである。

・ADV_LLD.1　：記述的下位レベル設計
・ADV_IMP.1　：TSF の実装のサブセット

・ALC_TAT.1　　：明確に定義された開発ツール
・AVA_VLA.2　　：独立脆弱性テスト

１．４　適合する PP

適合するプロテクションプロファイルはない。

１．５　関連する ST

関連するセキュリティターゲットはない。

１．６　CC 適合

本 TOE は、以下の情報セキュリティ評価基準に適合する。
・CC Version2.3 パート 2 適合
・CC Version2.3 パート 3 適合
なお以下の解釈を適用する。
・補足-0512 適用

１．７　略語

本 ST で使用する略語を以下に示す。

略語	定義	
CC	コモンクライテリア	(Common Criteria)
EAL	評価保証レベル	(Evaluation Assurance Level)
IT	情報技術	(Information Technology)
PP	プロテクションプロファイル	(Protection Profile)
SF	セキュリティ機能	(Security Function)
SFP	セキュリティ機能方針	(Security Function Policy)
ST	セキュリティターゲット	(Security Target)
TOE	評価対象	(Target of Evaluation)
TSC	TSF 制御範囲	(TSF Scope of Control)
TSF	TOE セキュリティ機能	(TOE Security Function)
TSFI	TSF インタフェース	(TSF Interface)
TSP	TOE セキュリティ方針	(TOE Security Policy)

１．８　用語

本 ST で使用する用語を以下に示す。

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。

beat-idc

beat-box を利用する組織のホームページ公開や利用者のメールサービスを送受信するためのインターネットデータセンター。

beat-box 責任者

利用者の組織の中で、beat-box を管理する者。

beat-noc オペレータ

beat-noc にて beat-box の遠隔管理を行う者。

利用者

beat-box によって分離されるネットワークのクライアント側のネットワークである内部ネットワークに接続して TOE を利用する者。

攻撃者

外部ネットワークから悪意を持って TOE を直接・間接的に利用する者。

内部ネットワーク

beat-box が管理するネットワークで、特定の企業等の中に敷かれ、企業の関係者のみがアクセス可能であるネットワークのこと。

外部ネットワーク

内部ネットワークではないネットワークで、インターネット及び、VPN 接続元など任意の者がアクセス可能であるネットワークのこと。

完全遮蔽方式

beat-box の外部ネットワーク側の全ポートをクローズし、原理的に外部からのアクセスを受け付けないようにする方式。

RAS 接続許可クライアント

外部ネットワークから内部ネットワークへアクセスが許可されたクライアント PC のこと。

VPN 接続許可拠点の beat-box

VPN 接続が許可された拠点において設置されている beat-box のことで、RAS 接続許可クライアントと同様に外部ネットワークから内部ネットワークへのアクセスが許可されるエンティティの１つになる。

１．９　参考資料

本 ST の参考資料を以下に示す。

[CC パート 1]：

Common Criteria for Information Technology Security Evaluation Part 1:Introduction and general model 2005 Version 2.3 CCMB-2005-08-001

[CC パート 2]：

Common Criteria for Information Technology Security Evaluation Part 2:Security functional requirements 2005 Version 2.3 CCMB-2005-08-002

[CC パート 3]：

Common Criteria for Information Technology Security Evaluation Part 3:Security assurance requirements　2005 Version 2.3 CCMB-2005-08-003

[CC パート 1　日本語翻訳]：

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-2005-001（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）

[CC パート 2　日本語翻訳]：

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-2005-001（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）

[CC パート 3　日本語翻訳]：

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-2005-001（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）

[補足-0512]：

補足-0512（平成 17 年 12 月　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）

2 TOE 記述

2．1　TOE 概説

TOE は、beat-box のファイアウォール機能を担うソフトウェアであり、外部ネットワーク、内部ネットワーク、及び beat-box 本体から発せられたトラフィックのフローの制御を行う。この機能により、外部ネットワークからの内部ネットワークへの不正アクセスから防御し、及び不正アクセスに伴う内部ネットワーク上の利用者クライアントのハードディスク内に蓄積された文書データなどの不正な暴露から保護する。

2．2　TOE の利用環境

TOE は内部ネットワークと外部ネットワークの境界に接続され利用される事を想定している。TOE の想定する利用環境を下図に示す。

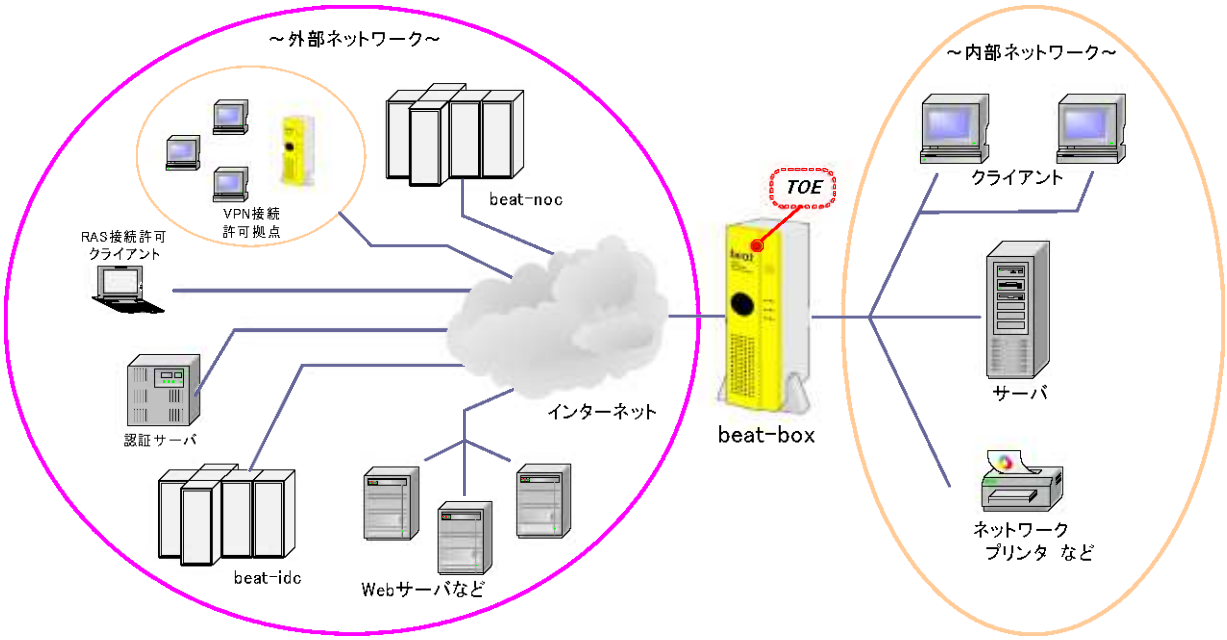

図 1　TOE の利用環境

上図に示される内部ネットワークには、以下のエンティティが接続されることを想定している。

○ クライアント：

・TOE を介して、WEB の閲覧、FTP でのファイル送受信などを行う利用者が扱う端末

・beat-box 責任者が WEB ブラウザを使って TOE の設定確認、変更操作を行うための端末

- サーバ：
  内部ネットワーク内で利用される各種サーバ
- ネットワークプリンタなどのネットワーク機器：
  内部ネットワーク内で利用されるプリンタなどのネットワーク機器

外部ネットワークには、以下のエンティティが接続されることを想定している。

- beat-noc：
  TOE を含む beat-box の動作状況の監視、管理を行う遠隔管理センター
- beat-idc：
  メールの送受信やホームページ公開を行うインターネットデータセンター
- WEB サーバなど：
  内部ネットワークからインターネットを介してアクセスされる WEB サーバなど
- RAS 接続許可クライアント
  外部ネットワークから内部ネットワークへアクセスが許可されたクライアント PC のこと。
- VPN 接続許可拠点
  beat-box が設置され VPN 接続が許可された拠点のこと。
- 認証サーバ
  RAS 接続許可クライアントが beat-box に接続する際に認証を受けるためのサーバ。

２．３　TOE の利用目的

TOE の利用目的は、内部ネットワークに接続しているクライアント、サーバに保存されているデータなどを、外部ネットワークからアクセスしてくる攻撃者から不正な暴露から保護することである。

２．４　TOE の構成

２．４．１　物理的構成

下図に beat-box 内のプログラムと、TOE の物理的範囲を示す。

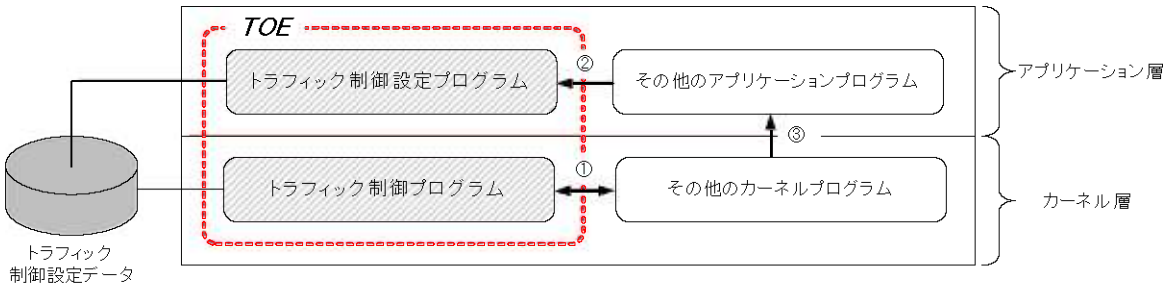

図 ２　TOE の物理的範囲

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。図中のその他のアプリケーションプログラム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。

２．５　TOE の関連者

TOE の利用目的は、内部ネットワークに接続している利用者クライアントに保存されているデータなどを、本 ST では、以下の関連者を想定する。

関連者	説明
組織の責任者	beat-box を利用、運用する組織の責任者
一般利用者	・内部ネットワークに接続している利用者 ・RAS 接続許可クライアントを利用する利用者
beat-box 責任者	・組織内で beat-box を管理する利用者
beat-noc オペレータ	beat-noc から beat-box をリモート管理する者

２．６　TOE が保護する資産

TOE は外部ネットワークからの不正行為に対して、内部ネットワークを保護することである。

２．７　beat-box の機能

TOE は、beat-box の一部のプログラムである。以下に、TOE の機能を含む beat-box の提供する機能を説明し、TOE の論理的範囲を明確にする。

２．７．１　TOE を含む beat-box の機能

beat-box は、高機能アプライアンスサーバとして複数のサービスを提供する。ここでは、beat-box の利用契約を結んだユーザに提供される基本的な機能について説明する。

○ **アンチウイルス機能**

メールの送受信、WEB アクセス時に紛れ込むウイルスを自動検出し、駆除を行う。

ウイルス定義ファイルは自動的に適用される。

○ **Windows 共有フォルダ機能**

Windows と互換のあるファイルシステムを提供する。ファイルサーバとして機能する。

○ **簡易グループウェア機能**

WEB ベースでスケジュール管理、掲示板、施設予約といったサービスを提供する。

○ **beat-noc 遠隔管理機能**

beat-noc にアクセスし、beat-box の稼働状況などを定期的に通知する。

TOE を含む beat-box の各ソフトウェアの更新が必要な場合は、beat-noc に準備されたソフトウェアを自動的にダウンロードし、更新する。

○ **アウトバウンドポートの閉口機能**

beat-box 責任者の操作より、アウトバンドのオープンポートを閉じさせる。

○ RAS 機能、VPN 機能

リモートアクセスサービス、VPN 拠点接続サービスを契約するユーザに対して、リモート接続、VPN 接続を行うための暗号機能等、一連の機能を提供している。

○ トラフィックフロー制御機能

TOE の機能。詳細は後述。

○ レポーティング機能

beat-box の状態についてレポートする機能。レポート内容の生成には、TOE の機能が一部関与している。（詳細は後述）具体的なレポート内容は以下の通り。

- 現在のインターネット接続
- 過去の不正アクセスの試み
- ファイルシステムの利用容量　など

２．７．２　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。

- 完全遮蔽方式情報フロー制御
  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。

本 ST では、トラフィックフロー制御機能を評価対象のセキュリティ機能として扱う。

２．８　TOE 評価検証環境

TOE は、beat-box の製造過程にてインストールされるソフトウェア（出荷ソフトウェア）に対して、シグネチャーと共に詳細が示される更新用 beat-box II 対応モジュールによって出荷ソフトウェアの一部が置き換えられる。以下は、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）

3 TOE セキュリティ環境

3．1　前提条件

本 TOE の動作/運用/利用に関わる前提条件を下表に示す。

前提条件	内容
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。

3．2　脅威

本 TOE に対するセキュリティ脅威および攻撃者を下表に示す。攻撃者は低レベルの攻撃力を持つものとする。

脅威	内容
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。

脅威	内容
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。

３．３　組織のセキュリティ対策方針

本 ST が想定する組織のセキュリティ方針はない。

4 セキュリティ対策方針

4．1　TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を下表に示す。

対策方針	説明
O.SHUTOUT	＜外部ネットワークからのアクセス遮断＞ TOE は、RAS、VPN、beat-noc からの接続が行なわれる以外の場合、外部ネットワークから到達可能なポートは Listen 状態を禁止とし、外部ネットワークからのアクセスを拒絶しなくてはならない。
O.NO-ICMP	＜存在応答の禁止＞ TOE は、外部ネットワークから発信される ICMP などの存在確認 IP パケットに対し、転送及び返信に伴って発信される IP パケットを禁止する。
O.NAPT	＜内部ネットワーク構成の隠蔽＞ TOE は、外部ネットワークに対して、内部ネットワーク構成情報を NAPT により隠蔽しなくてはならない。
O.STATE	＜通信状態の監視＞ TOE は、通信状態を記録し、記録に存在しない異常が認められるパケットを遮断しなければならない。

4．2　環境のセキュリティ対策方針

4．2．1　IT 環境のセキュリティ対策方針

IT 環境のセキュリティ対策方針を下表に示す。

対策方針	説明
OE.APP	＜認証サーバの正当性保証、beat-noc の正当性保証＞ ・beat-box アプリケーションは、beat-noc が正しい通信先であることを保証する。 ・beat-box アプリケーションは、認証サーバが正しい通信先であることを保証する。
OE.RAS	＜RAS 接続許可クライアントの正当性保証＞ 認証サーバは、RAS 接続許可クライアントが正しい通信先であることを保証する。
OE.VPN	＜VPN 接続許可拠点の beat-box の正当性保証＞ beat-noc は、VPN 接続許可拠点の beat-box が正しい通信先であることを保証する。
OE.SECURE-PORT	＜外部ネットワークエンティティの通信制御＞ beat-box アプリケーションは、beat-box と beat-noc 、RAS 接続許可クライアント、VPN 接続許可拠点の beat-box と通信する際に、各エンティティに利用が許可されるポートだけをオープンする。

対策方針	説明
OE.CHANNEL	＜セキュアな通信経路＞ ・beat-noc、RAS 接続許可クライアント、認証サーバ、VPN 接続許可拠点の beat-box と通信する際、beat-box アプリケーションは、外部ネットワークとの通信経路を、高信頼チャネルで接続しなければならない。 ・認証サーバは、RAS 接続許可クライアントと通信する際、通信経路を高信頼チャネルで接続しなければならない。 ・beat-noc は、VPN 接続許可拠点の beat-box と通信する際、通信経路を高信頼チャネルで接続しなければならない。
OE.BYPASS	＜TOE の完全動作＞ beat-box（TOE 以外の部分）は、TOE が提供するセキュリティ対策を beat-box を介するすべての通信に例外なく適用されなければならない。

４．２．２　非 IT 環境のセキュリティ対策方針

非 IT 環境のセキュリティ対策方針を下表に示す。

対策方針	説明
OEN.USER	＜信頼された管理者の選定、及び内部ユーザの利用条件＞ ・beat-box を利用する組織の責任者は、信頼出来る者を beat-box 責任者に指名しなければならない。 ・beat-box 責任者は、利用者に対し外部ネットワークへ情報を流出させるなどの行為を行なわないよう、注意喚起する。
OEN.NOC	＜信頼された beat-noc の維持＞ beat-noc を管理する責任者は、信頼出来る者を beat-noc オペレータに任命しなければならない。
OEN.PLACE	＜物理的に保護された beat-box＞ beat-box を管理する責任者は、攻撃者が物理的にアクセスすることができない保護された場所に beat-box を設置しなければならない。

5 IT セキュリティ要件

5．1　TOE セキュリティ要件

TOE が提供するセキュリティ要件を規定する。

5．1．1　TOE セキュリティ機能要件

FDP_IFC.1 (1)　サブセット情報フロー制御

下位階層：　なし

依存性　：　FDP_IFF.1（⇒FDP_IFF.1 (1)を適用）

FDP_IFC.1.1 (1)

TSF は、[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]に対して[割付: 情報フロー制御 SFP]を実施しなければならない。

[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]：

・**サブジェクト**　：　**トラフィック制御プログラム**

・**情報**　：　IP パケット

・**操作のリスト**　：　**TOE における情報の受信**

[割付: *情報フロー制御 SFP*]：

完全遮蔽方式情報フロー制御

FDP_IFC.1 (2)　サブセット情報フロー制御

下位階層：　なし

依存性　：　FDP_IFF.1（⇒FDP_IFF.1 (2)を適用）

FDP_IFC.1.1 (2)

TSF は、[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]に対して[割付: 情報フロー制御 SFP]を実施しなければならない。

[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]：

・**サブジェクト**　：　**トラフィック制御プログラム**

・**情報**　：　IP パケット

・**操作のリスト**　：　**TOE における情報の受信**

[割付: *情報フロー制御 SFP*]：

NAPT 情報フロー制御

FDP_IFC.1 (3)　サブセット情報フロー制御

下位階層：　なし

依存性　：　FDP_IFF.1（⇒FDP_IFF.1 (3)を適用）

FDP_IFC.1.1 (3)

TSF は、[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]に対して[割付: 情報フロー制御 SFP]を実施しなければならない。

[割付: *サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作のリスト*]：

・サブジェクト　：　トラフィック制御プログラム

・情報　　：　IP パケット

・操作のリスト　：　TOE における情報の受信

[割付: *情報フロー制御 SFP*]：

ステートフル情報フロー制御

FDP_IFF.1 (1)　単純セキュリティ属性

下位階層：　なし

依存性　：　FDP_IFC.1（⇒FDP_IFC.2(1)を適用）、FMT_MSA.3（⇒適用しない）

FDP_IFF.1.1 (1)

TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御 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情報のリスト、及び各々のセキュリティ属性*]。

[割付: *情報フロー制御 SFP*]：

完全遮蔽方式情報フロー制御

[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]：

表 1　完全遮蔽方式情報フロー制御に利用されるセキュリティ属性

N/A：Not Applicable

種別	対象	対象のセキュリティ属性
サブジェクト	・トラフィック制御プログラム	N/A
情報	・IP パケット	・NIC 識別子 ・送信元 IP アドレス ・プロトコルタイプ ・宛先 IP アドレス ・宛先ポート番号 ・セッションフラグ

FDP_IFF.1.2 (1)

TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]:

設定されたトラフィック制御設定データに基づき、以下の規則に従う。(外部からの IP パケットを遮断する。)

１．外部ネットワークからのアクセス遮断（TCP 以外）

＜情報のセキュリティ属性＞

・NIC 識別子：外部

・プロトコルタイプ：TCP 以外（ICMP など）

上記の IP パケットには何も処理を行わない。(レスポンスも返さない。)

２．外部ネットワークからのアクセス遮断（TCP）

＜情報のセキュリティ属性＞

・NIC 識別子：外部

・プロトコルタイプ：TCP

・セッションフラグ：SYN

上記の IP パケットには何も処理を行わない。(レスポンスも返さない。)

FDP_IFF.1.3 (1)

TSF は、[割付: *追加の情報フロー制御 SFP 規則*]を実施しなければならない。

[割付: *追加の情報フロー制御 SFP 規則*]:

beat-box アプリケーションが実行する完全遮蔽方式情報フロー制御機能のふるまい変更機能により変更されるトラフィック制御設定データに基づき、２の規則に置き換わって以下の規則が適用される。

３．RAS 接続、VPN 接続、beat-noc 接続時の情報フロー制御（遮断）

＜情報のセキュリティ属性＞

・NIC 識別子：外部

・宛先ポート番号：beat-box アプリケーションが一時的にオープンするポート番号以外

・プロトコルタイプ：TCP

・セッションフラグ：SYN

上記の IP パケットに対して、何も処理を行わない。

４．RAS 接続、VPN 接続、beat-noc 接続時の情報制御（通信許可）

以下の情報のセキュリティ属性の組み合わせに応じて情報フローを許可する。

表 2　完全遮蔽方式情報フロー制御にて許可されるトラフィック

情報のセキュリティ属性値

情報のセキュリティ属性値
・NIC 識別子：外部 ・送信元 IP アドレス　：beat-noc の IP アドレス ・宛先 IP アドレス　：beat-box の IP アドレス ・プロトコルタイプ　：TCP ・宛先ポート番号　：beat-noc 接続専用にオープンしたポート番号 ・セッションフラグ　：SYN
・NIC 識別子：外部 ・送信元 IP アドレス　：RAS 接続を許可されたクライアントの IP アドレス ・宛先 IP アドレス　：beat-box の IP アドレス ・プロトコルタイプ　：TCP ・宛先ポート番号　：RAS 接続専用にオープンしたポート番号 ・セッションフラグ　：SYN
・NIC 識別子：外部 ・送信元 IP アドレス　：VPN 接続を許可された拠点 beat-box の IP アドレス ・宛先 IP アドレス　：beat-box の IP アドレス ・プロトコルタイプ　：TCP ・宛先ポート番号　：VPN 接続専用にオープンしたポート番号 ・セッションフラグ　：SYN

FDP_IFF.1.4 (1)

TSF は、以下の[割付: *追加の SFP 能力のリスト*]を提供しなければならない。

[割付: *追加の SFP 能力のリスト*]:

追加の規則である FDP_IFF.1.3(1)の３及び４は、beat-box アプリケーションが実行する完全遮蔽方式情報フロー制御機能のふるまい変更機能により変更されるトラフィック制御設定データに基づき、FDP_IFF.1.2(1)に定義される１及び２の規則に戻る。（ふるまい変更によって閉じる。）

FDP_IFF.1.5 (1)

TSF は、以下の規則に基づいて、情報フロー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、明示的に情報フローを承認する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]:

なし

FDP_IFF.1.6 (1)

TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]:

なし

FDP_IFF.1 (2)　単純セキュリティ属性

下位階層：　なし

依存性　：　FDP_IFC.1（⇒FDP_IFC.2(2)を適用）、FMT_MSA.3（⇒適用しない）

FDP_IFF.1.1 (2)

TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御 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*

と情報のリスト、及び各々のセキュリティ属性]。

[割付: *情報フロー制御 SFP*]：

NAPT 情報フロー制御

[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]：

表 3　NAPT 情報フロー制御に利用されるセキュリティ属性

N/A：Not Applicable

種別	対象	対象のセキュリティ属性
サブジェクト	・トラフィック制御プログラム	N/A
情報	・IP パケット	・NIC 識別子 ・送信元 IP アドレス ・送信元ポート番号 ・宛先 IP アドレス ・宛先ポート番号

FDP_IFF.1.2 (2)

TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]：

設定されたトラフィック制御設定データに基づき、以下の規則に従う。

＜情報のセキュリティ属性＞

・NIC 識別子：内部

・送信元 IP アドレス　：　内部ネットワーク IP アドレス

・宛先 IP アドレス　：　外部ネットワーク IP アドレス

上記の IP パケットに対して、送信元である内部ネットワーク IT エンティティのセキュリティ属性を以下の通り変換し、通信を許可する。

＜書き換えられる情報のセキュリティ属性＞

・送信元 IP アドレス　⇒　beat-box の IP アドレス

・送信元ポート番号　⇒　beat-box にてその時点で利用されていない任意のポート番号

外部ネットワーク IT エンティティからのリターンで受け付ける IP パケット（NIC 識別子：外部）に対して、情報のセキュリティ属性を以下の通り変換し、通信を許可する。

＜書き換えられる情報のセキュリティ属性＞

・宛先 IP アドレス　⇒　元の内部ネットワーク IT エンティティの IP アドレス

・宛先ポート番号　⇒　元の内部ネットワーク IT エンティティのポート番号

FDP_IFF.1.3 (2)

TSF は、[割付: *追加の情報フロー制御 SFP 規則*]を実施しなければならない。

[割付: *追加の情報フロー制御 SFP 規則*]：

なし

FDP_IFF.1.4 (2)

TSF は、以下の[割付: *追加の SFP 能力のリスト*]を提供しなければならない。

[割付: *追加の SFP 能力のリスト*]:

なし

FDP_IFF.1.5 (2)

TSF は、以下の規則に基づいて、情報フロー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、明示的に情報フローを承認する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]:

なし

FDP_IFF.1.6 (2)

TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]:

なし

FDP_IFF.1 (3)　単純セキュリティ属性

下位階層：　なし

依存性　：　FDP_IFC.1（⇒FDP_IFC.2(3)を適用）、FMT_MSA.3（⇒適用しない）

FDP_IFF.1.1 (3)

TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付: *情報フロー制御 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情報のリスト、及び各々のセキュリティ属性*]。

[割付: *情報フロー制御 SFP*]:

ステートフル情報フロー制御

[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]:

表 4　ステートフル情報フロー制御に利用されるセキュリティ属性

N/A : Not Applicable

種別	対象	対象のセキュリティ属性
サブジェクト	・トラフィック制御プログラム	N/A
情報	・IP パケット	・送信元 IP アドレス ・宛先 IP アドレス ・セッションフラグ

FDP_IFF.1.2 (3)

TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

[割付: *各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]:

接続確立した情報は、情報、情報のセキュリティ属性とセットで記録される。（これを接続確立記録データとする。）

IP パケットがこの接続確立記録データより、現在情報フローが許可されている情報である場合（接続確立記録データと IP パケットの送信元 IP アドレスが一致する、または宛先 IP アドレスが一致する場合）のみ、当該 IP パケットの通信を許可する。（なお TOP の場合、セッションフラグ：SYN、または ACK の場合であることも検証する。）

FDP_IFF.1.3 (3)

TSF は、[割付: *追加の情報フロー制御 SFP 規則*]を実施しなければならない。

[割付: *追加の情報フロー制御 SFP 規則*]:

なし

FDP_IFF.1.4 (3)

TSF は、以下の[割付: *追加の SFP 能力のリスト*]を提供しなければならない。

[割付: *追加の SFP 能力のリスト*]:

なし

FDP_IFF.1.5 (3)

TSF は、以下の規則に基づいて、情報フロー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、明示的に情報フローを承認する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]:

なし

FDP_IFF.1.6 (3)

TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*]

[割付: *セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]:

なし

FMT_SMF.1(1)　管理機能の特定

下位階層：　なし

依存性　：　なし

FMT_SMF.1.1(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*]

完全遮蔽方式情報フロー制御機能のふるまい変更機能

５．１．２　TOE セキュリティ保証要件

TOE の評価保証レベルは、EAL3+である。[CC part3]に規定されている EAL3+保証パッケージのコンポーネントを以下に示す。(*印は EAL4、他は全て EAL3 である)

保証クラス	保証コンポーメント	保証コンポーネント
構成管理	ACM_CAP.3	許可の管理
	ACM_SCP.1	TOE の CM 範囲
配付と運用	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立ち上げ手順
開発	ADV_FSP.1	非形式的機能仕様
	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
	ADV_LLD.1　＊	記述的下位レベル設計
	ADV_RCR.1　＊	非形式的対応の実証
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	ALC_DVS.1	セキュリティ手段の識別
	ALC_TAT.1　＊	明確に定義された開発ツール
テスト	ATE_COV.2	カバレージ分析
	ATE_DPT.1	上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立試験・サンプル
脆弱性評定	AVA_MSU.1	ガイダンスの検査
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.2　＊	評価者脆弱性分析

５．１．３　TOE セキュリティ機能強度主張

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。

５．２　IT 環境セキュリティ要件

IT 環境が提供するセキュリティ要件を規定する。

５．２．１　IT 環境セキュリティ機能要件

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

依存性　：　FMT_SMF.1（⇒FMT_SMF.1(1)、FMT_SMF.(2)を適用）、
FMT_SMR.1（⇒FMT_SMR.1 を適用）

FMT_MOF.1.1

TSF（beat-box アプリケーション）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*]:

完全遮蔽方式情報フロー制御機能

[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*]

のふるまいを改変する

[割付: *許可された識別された役割*]

- beat-noc
- RAS 接続許可クライアント
- VPN 接続許可拠点の beat-box

FMT_SMF.1(2)　管理機能の特定

下位階層：　なし

依存性　：　なし

FMT_SMF.1.1(2)

TSF（beat-box アプリケーション）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*]

完全遮蔽方式情報フロー制御機能のふるまい変更機能

FMT_SMR.1　セキュリティ役割

下位階層：　なし

依存性　：　FIA_UID.1（⇒適用しない）

FMT_SMR.1.1

TSF（beat-box アプリケーション）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*]

・beat-noc

・RAS 接続許可クライアント

・VPN 接続許可拠点の beat-box

FMT_SMR.1.2

TSF（beat-box アプリケーション）は、利用者を役割に関連づけなければならない。

FTP_ITC.1(1)　TSF 間高信頼チャネル

下位階層：　なし

依存性　：　なし

FTP_ITC.1.1(1)

TSF（beat-box アプリケーション）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。

FTP_ITC.1.2(1)

TSF（beat-box アプリケーション）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*]：

リモート高信頼 IT 製品

FTP_ITC.1.3(1)

TSF（beat-box アプリケーション）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*]：

・beat-noc 遠隔管理機能

・RAS 接続機能

・VPN 接続機能

FTP_ITC.1(2)　TSF 間高信頼チャネル

下位階層：　なし

依存性　：　なし

FTP_ITC.1.1(2)

TSF（認証サーバ）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。

FTP_ITC.1.2(2)

TSF（認証サーバ）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*]：

リモート高信頼 IT 製品

FTP_ITC.1.3(2)

TSF（**認証サーバ**）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*]:

・RAS 接続機能

FTP_ITC.1(3)　TSF 間高信頼チャネル

下位階層：　なし

依存性　：　なし

FTP_ITC.1.1(3)

TSF（**beat-noc**）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。

FTP_ITC.1.2(3)

TSF（**beat-noc**）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*]:

リモート高信頼 IT 製品

FTP_ITC.1.3(3)

TSF（**beat-noc**）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*]:

・VPN 接続機能

FPT_RVM.1　　TSP の非バイパス性

下位階層：　なし

依存性　：　なし

FPT_RVM.1.1

TSF（**beat-box（TOE 以外の部分）**）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。

５．２．２　IT 環境に対するセキュリティ保証要件

TOE の IT 環境に対するセキュリティ保証要件はない。

6 TOE 要約仕様

6．1　TOE セキュリティ機能

本 TOE は､TOE セキュリティ機能要件を満足するために以下のセキュリティ機能を有する｡下表に、TOE セキュリティ機能と TOE セキュリティ機能要件の関係を示す。

IT セキュリティ機能 / TOE セキュリティ要件	SF.FILTER	SF.NAPT	SF.STATE
FDP_IFC.1(1)	●		
FDP_IFC.1(2)		●	
FDP_IFC.1(3)			●
FDP_IFF.1(1)	●		
FDP_IFF.1(2)		●	
FDP_IFF.1(3)			●
FMT_SMF.1(1)	●		

6．1．1　完全遮蔽方式情報フロー制御（SF.FILTER）

TOE は、トラフィック制御プログラムにより、外部ネットワークと beat-box 間の通信、beat-noc 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 パケットに対して完全遮蔽方式情報フロー制御を行う。具体的には以下の項目で示されるポリシーに従って制御される。

＜通常状態＞

NIC 識別子：外部でハンドリングされる IP パケットに対して、要求内容の如何を問わず、一切の処理を行わない。（レスポンスもしない。）

すなわち PING 等の ICMP による存在確認リクエストに対しても、一切レスポンスを行なわない。

RAS 接続等の必要が生じた場合、IT 環境である beat-box アプリケーションが動作（完全遮蔽方式情報フロー制御機能のふるまい変更機能が動作）して、＜通常状態＞のポリシーを緩和し､以下のポリシーが適用される。なお各場合において、許可されたポートへの接続が終了すると、当該ポートは閉口処理され、利用不可能になる。

＜beat-noc との接続状態＞

NIC 識別子：外部でハンドリングされる IP パケットに対して、送信元 IP アドレスが beat-noc の IP アドレス、宛先ポート番号が beat-box アプリケーションによって一時的にオープンされる beat-noc 接続専用のポート番号、プロトコルタイプが TCP、セッションフラグが SYN であるとき、通信を許可する。

ただし、beat-box アプリケーションによって、一時的にオープンするポート番号は、beat-box アプリケーションからの要求により閉じられ利用できなくなる。

＜RAS 接続を許可されたクライアントとの接続状態＞

NIC 識別子：外部でハンドリングされる IP パケットに対して、送信元 IP アドレス：RAS 接続が許可されたクライアントの IP アドレス、宛先ポート番号：beat-box アプリケーションによって一時的にオープンされる RAS 接続を許可されたクライアントが接続する専用のポート番号、プロトコルタイプ：TCP、セッションフラグ：SYN であるとき、通信を許可する。

ただし、beat-box アプリケーションによって、一時的にオープンするポート番号は、beat-box アプリケーションからの要求により閉じられ利用できなくなる。

＜VPN 接続を許可されたクライアントとの接続状態＞

NIC 識別子：外部でハンドリングされる IP パケットに対して、送信元 IP アドレス：VPN 接続が許可された拠点の beat-box の IP アドレス、宛先ポート番号：beat-box アプリケーションによって一時的にオープンされる VPN 接続が許可された拠点の beat-box が接続する専用のポート番号、プロトコルタイプ：TCP、セッションフラグ：SYN であるとき、通信を許可する。

ただし、beat-box アプリケーションによって、一時的にオープンするポート番号は、beat-box アプリケーションからの要求により閉じられ利用できなくなる。

上記のポリシーが適用された結果、許可された通信は、通信が完了するまで、許可されている通信として記録され、SF.STATE にて利用される。

６．１．２　NAPT 情報フロー制御（SF.NAPT）

TOE は、内部ネットワークから発信される外部ネットワーク IT エンティティと内部ネットワーク IT エンティティ間の通信において以下に示す処理（NAPT）を行う。

- ○ 内部ネットワークから開始される通信（NIC 識別子：内部）の IP パケットは、送信元の内部ネットワークの IP アドレス、ポート番号をそれぞれ beat-box IP アドレス、beat-box で利用されていないポート番号に変換し、通信を許可する。
- ○ 外部ネットワーク IT エンティティから返信される IP パケットに対して、宛先の IP アドレス、ポート番号を変換前の値に変換し、通信を許可する。

RAS 接続等の外部ネットワークから接続が開始するケースにおいても、その応答の IP パケットは、返信元の内部ネットワークの IP アドレス、ポート番号をそれぞれ beat-box IP アドレス、beat-box で利用されていないポート番号に変換し、通信を許可する。

６．１．３　ステートフル情報フロー制御（SF.STATE）

TOE は、外部ネットワークと beat-box 間の通信、beat-noc 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 パケットに対してステートフル情報フロー制御を行う。具体的には以下の項目で示されるポリシーに従う。

- 新たに受け付けた IP パケットのセキュリティ属性をチェックし、当該 IP パケットが既に確立している一連のデータストリームの一部であることが接続確立記録データより確認された場合、通信を許可する。
- 許可条件は以下の通り。
  - 送信元 IP アドレス、あるいは宛先 IP アドレスと接続確立記録データが一致していること。
    - IP パケットが TCP である場合は、セッションフラグ：SYN、あるいは ACK であること。

例えば通信記録にないのにもかかわらず、セッションフラグ：ACK で確立した通信になりすまして送信されてくるような不正な IP パケットを遮断することができる。

６．２　TOE セキュリティ機能強度

確率的・順列的メカニズムを有する TOE セキュリティ機能は、存在しない。

６．３　保証手段

表 5　TOE セキュリティ保証要件と保証手段の対応表

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 能力	ACM_CAP.3	・構成管理計画書 ・構成リスト ・CM 記録
	CM 範囲	ACM_SCP.1	
配付と運用	配付	ADO_DEL.1	配付説明書
	設置・生成・及び立上げ	ADO_IGS.1	設置ガイド
開発	機能仕様	ADV_FSP.1	セキュリティ機能仕様書
	上位レベル設計	ADV_HLD.2	・上位レベル設計 ・下位レベル設計
	実装表現	ADV_IMP.1	TOE ソースコード一式
	下位レベル設計	ADV_LLD.1	下位レベル設計
	表現対応	ADV_RCR.1	表現対応分析書
ガイダンス文書	管理者ガイダンス	AGD_ADM.1	・beat-box に搭載される管理用 Web ペー

TOE セキュリティ保証要件		コンポーネント	保証手段
	利用者ガイダンス	AGD_USR.1	ジ内の「ISO/IEC15408 認証の前提条件」の説明ページ ・セキュリティ機能仕様書・・・・(注)
ライフサイクルサポート	開発セキュリティ	ALC_DVS.1	開発セキュリティ説明書
	ツールと技法	ALC_TAT.1	ツールと技法説明書
テスト	カバレージ	ATE_COV.2	カバレージ分析書
	深さ	ATE_DPT.1	深さ分析書
	機能テスト	ATE_FUN.1	テスト仕様・結果報告書
	独立テスト	ATE_IND.2	TOE を含む beat-box の basic サービスにて提供される一連のソフトウェア
脆弱性評定	誤使用	AVA_MSU.1	AGD、AOD_IGS.1 における証拠等参照
	TOE セキュリティ機能強度	AVA_SOF.1	脆弱性分析書
	脆弱性分析	AVA_VLA.2	

※ 本 TOE は、利用者に対してセキュリティ機能の設定等を要求しない。TOE の操作等の記載は、beat サービスを提供する富士ゼロックス株式会社の開発スタッフが理解する必要があり、設計情報の一部としてセキュリティ機能仕様書にまとめられる。

7 PP 主張

本 ST は、PP 適合を主張しない。

8 根拠

8．1　セキュリティ対策方針根拠

本節では、脅威、組織のセキュリティ方針、及び前提条件に対するセキュリティ対策方針の必要性と十分性を示す。

8．1．1　セキュリティ対策方針の必要性

下表は、前提条件、脅威、組織のセキュリティ方針によって定義される TOE セキュリティ環境とセキュリティ対策方針が少なくとも、1 つの前提条件、脅威、組織のセキュリティ対策方針に対応していることを示している。

表 6　前提条件・脅威とセキュリティ対策方針の対応

前提・脅威 / セキュリティ対策方針	A.USER	A.NOC	A.PLACE	T.ACCESS	T.ATTACK	T.SPOOF	T.SNIFF
O.SHUTOUT				●			
O.NO-ICMP				●			
O.NAPT				●			
O.STATE					●		
OE.APP						●	
OE.RAS						●	
OE.VPN						●	
OE.SECURE-PORT						●	
OE.CHANNEL							●
OE.BYPASS				●	●		
OEN.USER	●						
OEN.NOC		●					
OEN.PLACE			●				

8．1．2　前提条件に対する十分性

A.USER：

OEN.USER によって beat-box 責任者が適切に選定され、利用者に対して情報流出行為を禁止する注意喚起が行なわれることから、内部ユーザの信頼性は実現される。

A.NOC：

OEN.NOC によって beat-noc オペレータは、信頼出来る者であるとすることにより beat-noc の信頼性は実現される。

A.PLACE：

OEN.PLACE によって物理的に保護されている場所に設置されるとする対策により、盗難、破壊、不正操作等の可能性が排除され、beat-box の設置条件は実現される。

８．１．３　脅威に対する十分性

T.ACCESS：

O.SHUTOUT により、外部ネットワークから到達可能なポートは基本的に Listen 状態を完全に禁止し、外部ネットワークからのアクセスは拒絶しており、beat-box への不正アクセスを防止している。
さらに O.NO-ICMP によって、外部ネットワークからの ICMP などの存在確認 IP パケットに対し、返信 IP パケットを送信せず、beat-box の存在自体を隠蔽し、脅威可能性を軽減している。
また O.NAPT により、NAPT 機能を利用して内部ネットワーク構成を隠蔽しており、外部ネットワークから直接内部ネットワークの IT エンティティに対する不正アクセスを防止している。
OE.BYPASS によってすべての通信に O.SHUTOUT、O.NO-ICMP、O.NAPT が適用され、より確実にセキュリティ対策が実施される。
したがって脅威は十分に対抗されている。

T.ATTACK：

O.STATE により、通信状態が記録されるため、不正に作り出された通常の通信では起こりえないパケットを遮断することにより、正常な通信をなりすましたセッションの不正利用攻撃に有効であり、不正アクセスの可能性を軽減している。
OE.BYPASS によってすべての通信に O.STATE が適用され、より確実にセキュリティ対策が実施される。
したがって脅威は十分に対抗されている。

T.SPOOF：

OE. RAS によって、認証サーバが RAS 接続許可クライアントの正当性を検証する。次に OE.APP によって beat-box アプリケーションが認証サーバの正当性を検証し、OE.SECURE-PORT により、beat-box アプリケーションが、RAS 接続許可クライアントが接続するためのポートをオープンすることによって、不正に各エンティティになりすましたアクセスを防止することができる。
OE.VPN によって、beat-noc が VPN 接続許可拠点の beat-box を認証する。次に OE.APP によって beat-box アプリケーションが beat-noc の正当性を検証し、OE.SECURE-PORT により、beat-box アプリケーションが、VPN 接続許可拠点の beat-box が接続するためのポートをオープンすることによって、不正に各エンティティになりすましたアクセスを防止することができる。

OE.APP によって、beat-box アプリケーションが beat-noc を認証する。次に OE.SECURE-PORT により、beat-box アプリケーションが、beat-noc が接続するためのポートをオープンすることによって、不正に各エンティティになりすましたアクセスを防止することができる。

T.SNIFF：

OE.CHANNEL により、beat-box アプリケーションの接続先となる beat-noc、RAS 接続許可クライアント、VPN 接続許可拠点の beat-box、認証サーバは、高信頼チャネルを介して通信する。認証サーバは、高信頼チャネルを介して RAS 接続許可クライアントと通信する。beat-noc は、高信頼チャネルを介して VPN 接続許可拠点の beat-box と通信する。

よって通信データを盗聴されるなどして、不正アクセスするための材料となる情報が漏洩する可能性を十分軽減している。

８．１．４　組織のセキュリティ対策方針に対する十分性

本 ST が想定する組織のセキュリティ方針はない。

８．２　セキュリティ要件根拠

本節では、セキュリティ対策方針に対するセキュリティ要件の必要性と十分性の根拠を示すとともに、各セキュリティ要件の依存性と相互補完性が満足されていることを示す。また、設定したセキュリティ保証要件が妥当である根拠を示す。さらに、設定した最小機能強度レベルが妥当であることを示す。

８．２．１　セキュリティ機能要件根拠

８．２．１．１ セキュリティ機能要件の必要性

下表は、セキュリティ対策方針とセキュリティ機能要件をマッピングしたものである。これにより、各セキュリティ機能要件が少なくても１つのセキュリティ対策方針をカバーしていることを示している。

表 7　セキュリティ対策方針とセキュリティ機能要件の対応

セキュリティ対策方針 / セキュリティ機能要件	O.SHUTOUT	O.NO-ICMP	O.NAPT	O.STATE	OE.APP	OE.RAS	OE.VPN	OE.SECURE-PORT	OE.CHANNEL	OE.BYPASS
FDP_IFC.1(1)	●	●								
FDP_IFC.1(2)			●							
FDP_IFC.1(3)				●						
FDP_IFF.1(1)	●	●								
FDP_IFF.1(2)			●							
FDP_IFF.1(3)				●						
FMT_SMF.1(1)	●									
FMT_MOF.1								●		
FMT_SMF.1(2)								●		
FMT_SMR.1								●		
FTP_ITC.1(1)					●				●	
FTP_ITC.1(2)						●			●	
FTP_ITC.1(3)							●		●	
FPT_RVM.1										●

８．２．１．２ セキュリティ機能要件の十分性

本節では、セキュリティ機能要件がセキュリティ対策方針を満たすのに十分である根拠を示す。

O.SHUTOUT：

FDP_IFC.1(1)、FDP_IFF.1(1)により、完全遮蔽情報フロー制御が実施されるため、外部からの接続行為は遮断され、また応答も返さない。RAS、VPN、beat-noc からの接続時には、FMT_SMF.1(1)により、情報フロー制御機能のふるまいが変更される。したがってセキュリティ対策方針は達成される。（※ FMT_SMF.1(1)の行為の妥当性は、OE.SECURE-PORT によって保証される。）

O.NO-ICMP：

FDP_IFC.1(1)、FDP_IFF.1(1)により、完全遮蔽情報フロー制御が実施されるため、ICMP による存在確認パケットも遮断され、応答も返さない。したがってセキュリティ対策方針は達成される。

O.NAPT：

FDP_IFC.1(2)、FDP_IFF.1(2)により、NAPT 情報フロー制御が実施されるため、外部ネットワーク、

内部ネットワークそれぞれのエンティティの IP アドレス、ポート番号は適切に変換される。したがってセキュリティ対策方針は達成される。

O.STATE：

FDP_IFC.1(3)、FDP_IFF.1(3)により、ステートフル情報フロー制御が実施されるため、通信確立したパケットのみの通信だけが許可され、他の不正なパケットは排除される。したがってセキュリティ対策方針は達成される。

OE.APP：

FTP_ITC.1(1)により、beat-box アプリケーションと beat-noc 間、beat-box アプリケーションと認証サーバに高信頼チャネルが生成される過程で、beat-box アプリケーションによる beat-noc の正当性が確認される（端点の保証された識別が実行される）。したがってセキュリティ対策方針は満たされる。

OE.RAS：

FTP_ITC.1(2)により、認証サーバと RAS 接続許可クライアント間に高信頼チャネルが生成される過程で認証サーバによる RAS 接続許可クライアントの正当性が確認される（端点の保証された識別が実行される）。したがってセキュリティ対策方針は満たされる。

OE.VPN：

FTP_ITC.1(3)により、beat-noc と VPN 接続許可拠点の beat-box 間に高信頼チャネルが生成される過程で、beat-noc による VPN 接続許可拠点の beat-box の正当性が確認される（端点の保証された識別が実行される）。したがってセキュリティ対策方針は満たされる。

OE.SECURE-PORT

FMT_MOF.1 により、beat-box アプリケーションは、完全遮蔽方式情報フロー制御機能のふるまいを改変することを、beat-noc、RAS 接続許可クライアント、VPN 接続許可拠点の beat-box に制限し、FMT_SMF.1(2)により当該機能が特定されている。また役割として、beat-noc、RAS 接続許可クライアント、VPN 接続許可拠点の beat-box を保持する。

ここで完全遮蔽方式情報フロー制御機能のふるまい変更機能とは、TOE のセキュリティ機能要件である FDP_IFF.1.3(1)にて、各エンティティが利用するための専用ポートを開放するための機能であることが示されており、当該セキュリティ対策方針は達成される。（※ FMT_SMF.1(2)の一部の機能は、FMT_SMF.1(1)が適用されている通り、TOE 処理でも実施される。O.SHUTOUT 参照）

OE.CHANNEL：

FTP_ITC.1(1)により、beat-box アプリケーションと beat-noc、RAS 接続許可クライアント、VPN 接続許可拠点の beat-box、認証サーバとの通信は、高信頼チャネルを介して行なわれる。FTP_ITC.1(2)によって認証サーバと RAS 接続許可クライアントとの通信は、高信頼チャネルが利用される。FTP_ITC.1(3)によって beat-noc と VPN 接続許可拠点の beat-box との通信は、高信頼チャネルが利用される。

したがってセキュリティ対策方針は達成される。

OE.BYPASS：

FPT_RVM.1 により、beat-box（TOE 以外の部分）によって TSP が必ず呼び出されて実施されることが保証されるため、当該セキュリティ対策方針は達成される。

８．２．２　セキュリティ機能要件の依存性根拠

本節では、セキュリティ機能要件全体が相互に補完し、内部的に一貫している根拠として、セキュリティ機能要件が依存性を満足していることを説明する。

セキュリティ機能要件には直接的及び間接的に依存するセキュリティ機能要件が存在することを踏まえ、これらの依存性のすべてが満たされていることと、満たされていない依存性についてはその正当性の根拠を示す。下表では、TOE セキュリティ機能要件が依存するセキュリティ要件とそれをカバーする TOE セキュリティ機能要件を示すことにより、TOE セキュリティ機能要件の依存性が満たされている範囲を明確にする。さらに、満たされていない依存性についてはそれが正当である根拠を別途示す。以上により、全体として依存性が満たされていることを示す。

表 8　IT セキュリティ機能要件コンポーネントの依存関係

N/A：Not Applicable

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1(1)
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1(2)
FDP_IFC.1(3)	FDP_IFF.1	FDP_IFF.1(3)
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1(1) ＜FMT_MSA.3 を適用しない理由＞ ・NIC 識別子以外の属性は、情報そのものの中に与えられている識別子であり、そのまま制御に利用する。従って値の初期化は不要であり、当該要件は適用されない。 ・NIC 識別子は、情報が beat-box に取り込まれる、または beat-box 内で生成された際に当該情報と関連付けらるものである。しかし情報の出所を判別するために付与される識別情報であり、許可的等の特性を有するものではなく、当該要件は適用されない。
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1(2) ＜FMT_MSA.3 を適用しない理由＞ ・NIC 識別子以外の属性は、情報そのものの中に与えられている識別子であり、そのまま制御に利用する。従って値の初期化は不要であり、当該要件は適用されない。

本 ST の機能要件コンポーネント	CC パート 2 の依存性	本 ST における依存関係
		・NIC 識別子は、情報が beat-box に取り込まれる、または beat-box 内で生成された際に当該情報と関連付けらるものである。しかし情報の出所を判別するために付与される識別情報の 1 つであり、許可的等の特性を有するものではなく、当該要件は適用されない。
FDP_IFF.1(3)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1(3) ＜FMT_MSA.3 を適用しない理由＞ ・NIC 識別子以外の属性は、情報そのものの中に与えられている識別子であり、そのまま制御に利用する。従って値の初期化は不要であり、当該要件は適用されない。 ・NIC 識別子は、情報が beat-box に取り込まれる、または beat-box 内で生成された際に当該情報と関連付けらるものである。しかし情報の出所を判別するために付与される識別情報の 1 つであり、許可的等の特性を有するものではなく、当該要件は適用されない。
FMT_SMF.1(1)	なし	N/A
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1(1)、FMT_SMF.1(2) FMT_SMR.1
FMT_SMF.1(2)	なし	N/A
FMT_SMR.1	FIA_UID.1	適用しない ＜FIA_UID.1 を適用しない理由＞ beat-box アプリケーションは、beat-box 内に存在するものである。不正なアプリケーションが外部ネットワークからの攻撃等で入り込む可能性はないことから、beat-box アプリケーションが許可された識別された役割であることを保証する処理は不要である。
FTP_ITC.1(1)	なし	N/A
FTP_ITC.1(2)	なし	N/A
FTP_ITC.1(3)	なし	N/A
FPT_RVM.1	なし	N/A

８．２．３　セキュリティ機能要件の相互サポート根拠

本節では、セキュリティ機能要件全体が相互に補完し、内部的に一貫している根拠として、セキュリティ機能要件が迂回、干渉・破壊、及び非活性化の各攻撃から保護されていること、無効化を検出できる事を説明する。

以下に機能要件の依存関係の分析には明示されない他のセキュリティ機能要件を有効に動作させるための IT セキュリティ機能要件を下表に示す。

表 9　IT セキュリティ機能要件の相互サポート関係

N/A : Not Applicable

IT セキュリティ機能要件	迂回防止	干渉/破壊防止	非活性化防止	無効化検出
FDP_IFC.1(1)	N/A	FMT_MOF.1	N/A	N/A
FDP_IFC.1(2)	N/A	N/A	N/A	N/A
FDP_IFC.1(3)	N/A	N/A	N/A	N/A
FDP_IFF.1(1)	FPT_RVM.1	N/A	N/A	N/A
FDP_IFF.1(2)	FPT_RVM.1	N/A	N/A	N/A
FDP_IFF.1(3)	FPT_RVM.1	N/A	N/A	N/A
FMT_SMF.1(1)	N/A	N/A	N/A	N/A
FMT_MOF.1	N/A	N/A	N/A	N/A
FMT_SMF.1(2)	N/A	N/A	N/A	N/A
FMT_SMR.1	N/A	N/A	N/A	N/A
FTP_ITC.1(1)	N/A	N/A	N/A	N/A
FTP_ITC.1(2)	N/A	N/A	N/A	N/A
FTP_ITC.1(3)	N/A	N/A	N/A	N/A
FPT_RVM.1	N/A	N/A	N/A	N/A

８．２．３．１　迂回防止の根拠

TOE の提供する情報フロー制御を規定する、FDP_IFF.1(1)、FDP_IFF.1(2)、FDP_IFF.1(3)は FPT_RVM.1 によって、必ず実施されることが保証されることによって、迂回可能性を防止している。

８．２．３．２　干渉・破壊防止の根拠

TOE の提供する情報フロー制御を規定する、FDP_IFF.1(1)は、FMT_MOF.1 によってふるまいを変更する操作が適切な役割に管理されており、干渉防止に貢献している。

８．２．３．３　非活性化防止の根拠

TOE のセキュリティ機能を非活性化防止するためのサポート構造はないが、非活性化に繋がるような仕様は存在しない。

８．２．３．４　無効化検出の根拠

TOE のセキュリティ機能の無効化を検出する仕組みは存在しない。

８．２．４　IT セキュリティ機能要件のセット一貫性根拠

本節では、競合可能性のある IT セキュリティ要件が存在しない論拠を示す。

- FDP_IFF.1 を繰り返して複数の情報フロー制御を規定している。ポリシー内容は、自由に割付可能であるため、要件同士が相反するポリシーが設定される可能性がある。
  完全遮蔽方式情報フロー制御、NAPT 情報フロー制御、ステートフル情報フロー制御は、それぞれフィルタリング、NAPT、許可パケットのステータス管理と異なる側面の制御ポリシーであることから、競合する可能性はない。
- FMT クラスなどの管理要件は、役割、操作の関係で齟齬を来たすケースが存在するが、本 ST では FMT_MOF.1 がただ１つだけ適用されているため、他の要件と干渉することはない。
- 完全遮蔽方式情報フロー制御によって一般的なアクセス要求の IP パケットはフィルタイリングされ、不正なパケットによるアクセス要求は、ステートフル情報フロー制御によって振り落とされる。したがって適用される情報フロー制御に関係する複数のセキュリティ要件によってファイアウォール機能として必要な処理を実現しているため、結果としてセキュリティ対策方針全体によって意図される内部ネットワークの保護は確かに達成されている。

上記以外に、競合可能性のある IT セキュリティ要件は存在せず、適用した IT セキュリティ要件は一貫している。

８．２．５　TOE 保証要件根拠

本 TOE は、インターネット等の外部ネットワークと、ユーザが扱う内部ネットワークを分離し、外部ネットワークからの攻撃から内部ネットワークを保護するという重要な役割を担うため、十分な実効性を保証する必要がある。

機能仕様、上位レベル設計書に基づくテスト、機能強度分析、脆弱性の探索が実施されている必要があり、また開発環境の制御、TOE の構成管理、セキュアな配付手続きが取られていることが望まれる。従って十分な保証レベルが提供される EAL3 以上が望まれるが、本 TOE は、EAL3 を選択の上で、これに追加する形で、開発設計の保証コンポーネントに ADV_LLD.1、ADV_IMP.1、ライフサイクルサポートにおいては ALC_TAT.1 を適用し、さらには脆弱性分析において AVA_VLA.2 を適用することによって保証のレベルを上げているため、本 ST の主張するセキュリティ機能を保証するにあたって、十分な保証コンポーネントが選択されているといえ、妥当である。

８．２．６　最小機能強度根拠

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、最小機能強度は定義されない。

８．３　TOE 要約仕様根拠

８．３．１　TOE セキュリティ機能根拠

本節では、セキュリティ機能全体が全てのセキュリティ機能要件を満足し、相互に補完し、一体となっていることを示す。

８．３．１．１ TOE セキュリティ機能の必要性

下表は、セキュリティ機能要件と TOE セキュリティ機能をマッピングしたものである。これにより、各セキュリティ機能要件が少なくても１つの TOE セキュリティ機能をカバーしていることを示している。

表 10　TOE セキュリティ機能要件に対する TOE セキュリティ機能の対応

	SF.FILTER	SF.NAPT	SF.STATE
FDP_IFC.1(1)	●		
FDP_IFC.1(2)		●	
FDP_IFC.1(3)			●
FDP_IFF.1(1)	●		
FDP_IFF.1(2)		●	
FDP_IFF.1(3)			●
FMT_SMF.1(1)	●		

８．３．１．２ TOE セキュリティ機能の十分性

本節では、TOE セキュリティ機能がセキュリティ機能要件を満たすのに十分である根拠を示す。

FDP_IFC.1(1)：

当該要件は、完全遮蔽方式情報フロー制御におけるサブジェクト、情報、情報の流れを引き起こすための操作について規定している。

SF.FILTER は、トラフィック制御プログラムが IP パケットを完全遮蔽方式と定められた規則に則りフィルタリング制御するとしており、満たされる。

FDP_IFC.1(2)：

当該要件は、NAPT 情報フロー制御におけるサブジェクト、情報、情報の流れを引き起こすための操作について規定している。

SF.NAPT は、トラフィック制御プログラムが IP パケットをアドレス、ポート変換する NAPT 情報

フロー制御をするとしており、満たされる。

FDP_IFC.1(3)：

当該要件は、ステートフル情報フロー制御におけるサブジェクト、情報、情報の流れを引き起こすための操作について規定している。

SF.STATE は、トラフィック制御プログラムが IP パケットの通信ステータスを記録し、これに基づいて、不正な IP パケットを制御するとしており、満たされる。

FDP_IFF.1(1)：

当該要件は、完全遮蔽方式情報フロー制御ポリシーの規則を定義している。

SF.FILTER は、外部ネットワークから受け付ける IP パケットをすべて遮断し、RAS 接続、VPN 接続、beat-noc 接続の際に、所定のポートをオープンにし、接続してくる対象のセキュリティ属性をチェックし、制御するとされおり、満たされる。

FDP_IFF.1(2)：

当該要件は、NAPT 情報フロー制御ポリシーの規則を定義している。

SF.NAPT は、内部ネットワークから開始され外部ネットワークへ発信される IP パケットを、送信元 IP アドレス、送信元ポート番号を変換する。そのリターンを受け付けた場合は、送信先 IP アドレス、ポート番号を元の内部ネットワークの IP アドレス、ポート番号に変換するとしており、満たされる。

FDP_IFF.1(3)：

当該要件は、ステートフル情報フロー制御ポリシーの規則を定義している。

SF.STATE は、受信する IP パケットを送信元 IP アドレス、宛先 IP アドレス、セションフラグをチェックして既に確立している通信の一部であることを確認した場合に、当該 IP パケットの通信を許可するとされており、満たされる。

FMT_SMF.1(1)：

当該要件は、完全遮蔽方式情報フロー制御機能のふるまい管理機能を定義している。

SF.FILTER は、外部ネットワークから受け付ける IP パケットをすべて遮断し、RAS 接続、VPN 接続、beat-noc 接続の際に、所定のポートをオープンにし、接続してくる対象のセキュリティ属性をチェックし、制御する。この際 beat-box アプリケーションをトリガーとして動作する所定のポートをオープンする機能が、完全遮蔽方式情報フロー制御機能に相当し、満たされる。

８．３．２　相互サポートする TOE セキュリティ機能

TOE 要約仕様で識別される IT セキュリティ機能が組み合わさることにより満たされる TOE セキュリティ機能要件は、前小項に記述される各根拠記述にて述べられる通りである。

８．３．３　機能強度の一貫性根拠

TOE セキュリティ機能の中で、確率的または順列的メカニズムによって実現されている機能は存在しないということで一貫している。

８．３．４　保証手段根拠

評価保証レベル EAL3＋において必要なドキュメントは 6.3 節において説明される保証手段に示されたドキュメント資料により網羅されている。これら保証手段として提示されているドキュメントに従った開発、テストの実施、脆弱性の分析、開発環境の管理、ツールの定義、構成管理、配付手続き等が実施されることにより、TOE セキュリティ保証要件が満たされる。

８．４　PP 主張根拠

本 ST が参照する PP はない。