



The Next Quality

ファイアウォール

Secure Beagle

Model 10/30/200 共通

操作マニュアル



Secure Beagle操作マニュアル

株式会社エーティーワークスは本マニュアルの記述のいかなる誤りに対しても責任を負うものではありません。

また、株式会社エーティーワークスは本マニュアルの記述の使用によるいかなる結果に対しても責任を負うものではありません。本マニュアルはお客様の責任で使用してください。

本マニュアルの内容は情報提供のみを目的としており、予告なしに変更される場合があります。

事前に株式会社エーティーワークスによる許可がない限り、本マニュアルのいかなる部分も複製することはできません。

また、株式会社エーティーワークスによる許可がない限り、本マニュアルを配布することはできません。

目次

P.03 第1章 Secure Beagleとは

- 04 1. はじめに
- 04 2. 商標について
- 05 3. Secure Beagleの特徴
- 05 4. 本文中に使用される記号について
- 06 5. ハードウェアの取り扱いについて
- 09 6. ハードウェアを取り扱う上での注意事項

P.11 第2章 セットアップ

- 12 1. 設置計画
- 16 2. 初期設定
- 20 3. Secure Beagle導入例

P.25 第3章 ファイアウォール

- 26 1. ポリシーリスト
- 27 2. ポリシー追加
- 31 3. ポリシーの編集
- 32 4. ポリシーの削除
- 32 5. インポート
- 33 6. エクスポート
- 34 7. ポリシーの優先度の変更

P.35 第4章 冗長化構成

- 36 1. 冗長化構成のメリット
- 37 2. 冗長化構成例
- 40 3. 冗長化構成時の動作について

P.45 第5章 運用管理

- 46 1. バックアップ・リストア手順
- 47 2. ファームウェアアップデート
- 48 3. GeolPデータベースアップデート
- 49 4. 通知設定

P.53 第6章 管理画面の機能説明

54	1. ログイン画面
57	2. 基本設定
57	ネットワーク
59	ルーティング
60	冗長化設定
63	3. アクセス制限
63	パスワード変更
64	接続許可IPアドレス
65	4. ファイアウォール
65	ポリシー
70	5. 通知設定
70	Syslog
71	メール通知設定
71	SNMP
73	6. 運用管理
73	バックアップ/リストア
74	状態
76	ファームウェア
77	サポート情報取得
77	再起動
78	設定初期化

P.79 第7章 コンソール管理

80	1. コンソール管理
----	------------

P.85 付録

86	付録A. 仕様
87	付録B. 通知メールの内容
88	付録C. パケットログ形式

第1章

Secure Beagleとは

1. はじめに	4
2. 商標について	4
3. Secure Beagleの特徴	5
4. 本文中に使用される記号について	5
5. ハードウェアの取り扱いについて	6
6. ハードウェアを取り扱う上での注意事項	9

1. はじめに

このたびは株式会社エーティーワークスのSecure Beagleをお買い上げいただき、誠にありがとうございます。

Secure Beagleは、弊社独自開発による透過型ファイアウォールを搭載する、アプリケーションサーバです。

筐体は弊社オリジナルの1/4Uシャーシを採用しており、ラックを非常に効率よく使用することができます。

専用の管理インターフェイスを搭載していますので、セットアップや運用管理を全てWebブラウザから行うことができます。

本書をよくお読みいただき、本製品の機能や使用方法を十分理解したうえで、本製品をご使用になってください。

2. 商標について

Linuxは、Linus Torvaldsの米国およびその他の国における登録商標あるいは商標です。

Microsoft、Windowsは、米国Microsoft Corporationの米国およびその他の国における登録商標です。

MaxMindおよびGeoIPは、米国MaxMind社の商標です。

その他、記載されている会社名、製品名は、各社の登録商標または商標です。なお、本文中では、®、TMマークは明記しておりません。

3. Secure Beagleの特徴

■省スペース

- ・ラックを非常に有効に利用できる弊社オリジナルの1/4Uシャーシを採用。

■ファイアウォール機能

- ・弊社独自開発のファイアウォールエンジンを搭載
- ・IPアドレスを直接指定してのフィルタリングに加え、GeoIPデータベースを利用してIPアドレスの割り当て国によるフィルタリングに対応
- ・透過型ファイアウォールであるため、既存のネットワーク機器を変更することなく導入可能
- ・複数のネットワーク構成に対応（Inside—Outside構成、Inside—Outside—DMZ構成）
- ・ステートフルインスペクション機能を搭載

■運用管理

- ・Webブラウザから操作できる専用管理インターフェイスを搭載
- ・冗長化構成時には、マスター—スタンバイの切り替え時にメール通知
- ・SNMPエージェントとしてSNMPマネージャから管理可能

■保守性

- ・設定情報のバックアップリストア機能
- ・ファームウェアアップデート機能

■信頼性

- ・記憶装置にFlashメモリを採用。駆動部品を最小限にすることにより高稼働率を実現
- ・本製品2台にて冗長化構成に対応（マスター—スタンバイ構成）

4. 本文中に使用される記号について

本書では、本文中に以下の記号を使用しております。



注意

装置の取り扱いや設定手順において守らなければならない事項や注意が必要な事項を記述しています。



ポイント

装置の取り扱いや設定手順において知っておくと便利な点を記述しています。



参照

関連する項目やページを記述しています。

5. ハードウェアの取り扱いについて

Model 10

■フロントパネルの説明

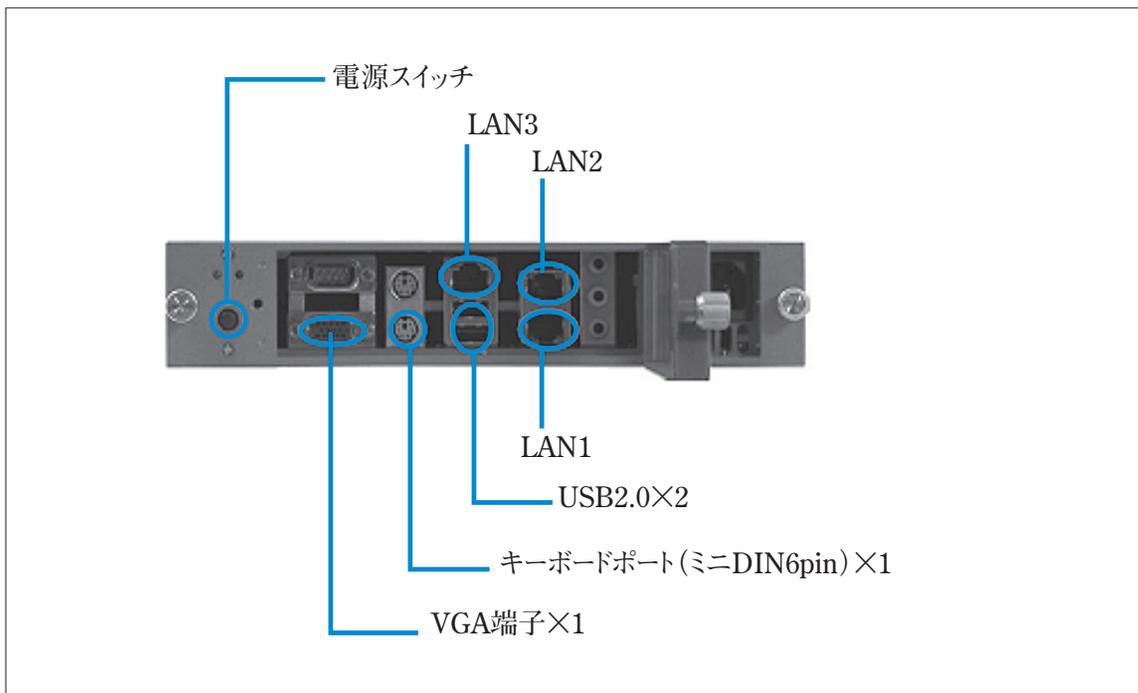


図1-1 フロントパネル

電源スイッチ	押下すると電源が投入されます。
VGA端子	コンソール接続する場合、モニタを接続します。
キーボードミニポート	コンソール接続する場合、キーボードを接続します。
USB2.0	USB2.0ポートです。
LANコネクタ	InsideゾーンのネットワークにLAN1を接続します。
	OutsideゾーンのネットワークにLAN2を接続します。
	DMZゾーンのネットワークにLAN3を接続します。



DMZのネットワークを使用しない場合はLAN3は使用しません。

■フロントパネルの説明

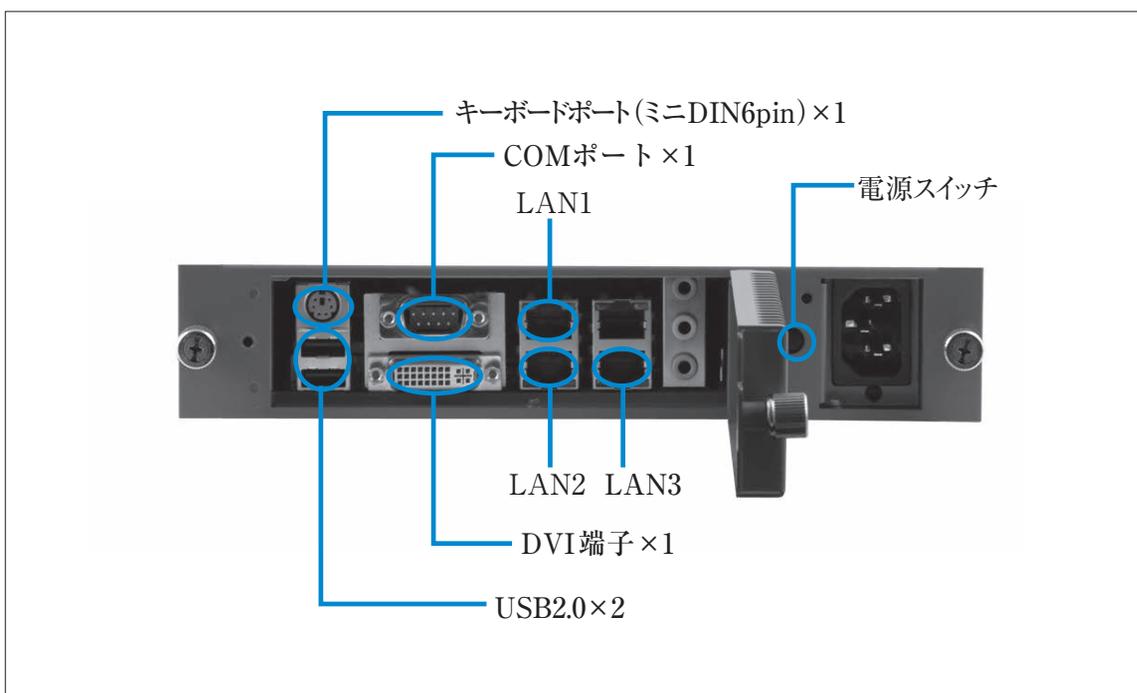


図 1-2 フロントパネル

電源スイッチ	押下すると電源が投入されます。
DVI端子	コンソール接続する場合、モニタを接続します。
キーボードミニポート	コンソール接続する場合、キーボードを接続します。
USB2.0	USB2.0ポートです。
LANコネクタ	InsideゾーンのネットワークにLAN1を接続します。
	OutsideゾーンのネットワークにLAN2を接続します。
	DMZゾーンのネットワークにLAN3を接続します。

! DMZのネットワークを使用しない場合はLAN3は使用しません。

■フロントパネルの説明

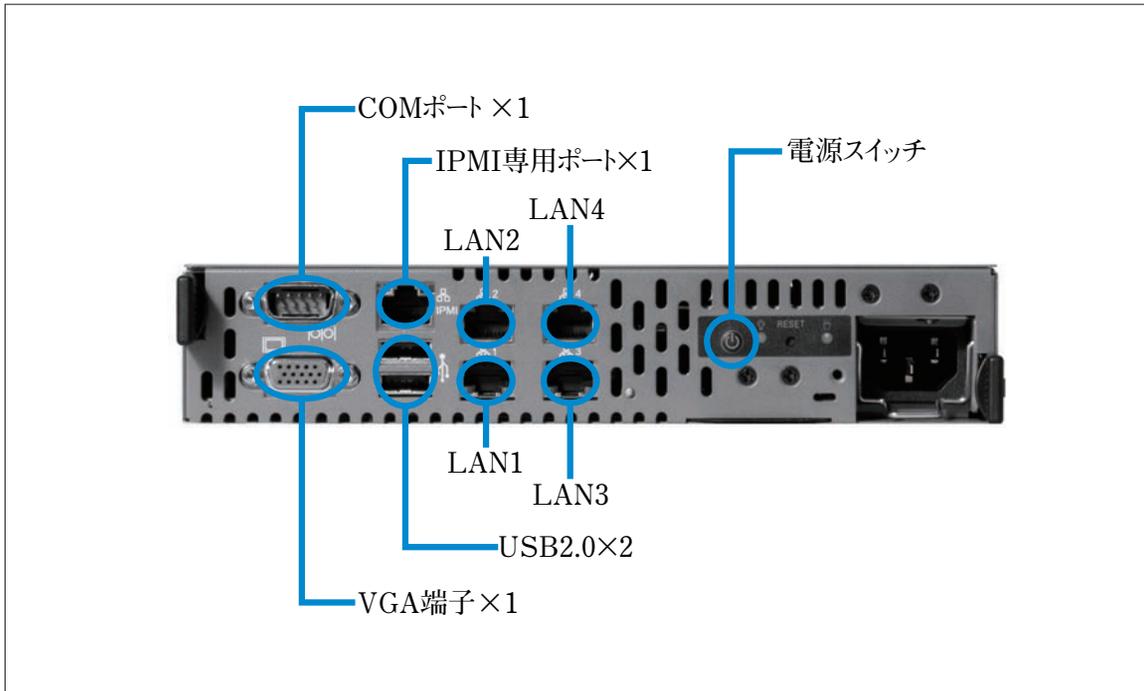


図 1-3 フロントパネル

電源スイッチ	押下すると電源が投入されます。
COMポート	シリアルポートです。
VGA端子	コンソールを接続する場合、モニタを接続します。
USB2.0	USB2.0ポートです。
LANコネクタ	InsideゾーンのネットワークにLAN1を接続します。
	OutosideゾーンのネットワークにLAN2を接続します。
	DMZゾーンのネットワークにLAN3を接続します。

! DMZのネットワークを使用しない場合はLAN3は使用しません。

6. ハードウェアを取り扱う上での注意事項

! 安全にお使いいただくために必ずお守りください。

お客様や他の方への危害や損害を未然に防ぎ、本製品を安全にご使用いただくために必ずお守りいただきたい事項を記載しました。安全にご使用いただくために必ずお読みになり、内容をよく理解された上でご使用ください。

警告及び注意

■表示された電源電圧で使用する

表示された電源電圧以外では使用しないでください。火災や感電の原因になります。

■もし異常が起こったら

本機から煙が出たり、変なおいや音がしたら、直ちに安全にスイッチを切りコンセントからプラグを抜いてください。そのまま使用すると、火災や感電の原因となります。

(修理につきましては弊社にお問い合わせください)

■濡れた手で本製品を触らないでください。また、濡れた手で電源プラグの抜き差しはしないでください

本体及び周辺機器の電源プラグが入っているときに濡れた手で触れると、感電や故障の原因となります。また、電源プラグが接続されていなくても故障の原因となります。

濡れた手で電源プラグの抜き差しをすると、感電をする恐れがありますので、必ず乾いた手で抜き差ししてください。

■電源コードやプラグを破損させないでください

無理に曲げて設置したりすると、電源コードやプラグが破損し、火災や感電につながります。

■電源プラグは確実に差し込んでください

電源プラグを確実に差し込まないと、接触不良により火災や感電につながりますので、必ず根元まで確実に差し込んでください。また、定期的にプラグの状態を確認してください。

■電源コードのアース線は確実に配線してください

■雷が鳴っている時は、電源プラグに触れないでください

落雷時に感電する恐れがあります。

■電源プラグは定期的に埃などを取り除いてください

電源プラグに埃がついたまま使用しますと、ショートや絶縁不良となり、火災や感電の原因となります。埃を取り除く際は、プラグを抜き、乾いた布で拭き取ってください。

■本体内部に、液体や異物を入れないでください

本体内に液体や異物が入った状態で使用すると、火災や感電、故障につながる恐れがあります。液体や異物が内部に入った場合は、直ちに安全にスイッチを切り、コンセントからプラグを抜いてください。(修理につきましては弊社にお問い合わせください)

■高電圧機器の周辺で作業する場合、または高電圧機器を取り扱う場合は必ず2人以上で作業してください
高電圧機器の周辺で作業する場合や、高電圧機器を取り扱う場合は、万一の場合にそなえ、必ず作業
者以外に主電源を切断することができるように人員を配置してください。また、予めブレーカーなどの主電
源スイッチの場所を確認してください。

■水分や湿気の多い場所でのご使用はお避けください

火災や感電、故障の原因となります。

■本体通気孔をふさがないでください

本体通気孔をふさいだ状態で使用すると、本体内部の温度が上がり、故障ややけどの原因となります。

■動作中のファンには指や異物を入れないでください

けがや故障の原因になります。

■本機の上に物をのせないでください。また、本機の上に乗らないでください

落下して怪我をしたり、本機が破損する恐れがあります。本機の上に重量物を置くと、ケースが変形し、
内部の機器が破損し、火災や感電の原因となる恐れがあります。

■本製品を次のような場所に設置しないでください

- ・ 許容動作環境以外の場所
- ・ 直射日光が当たる場所
- ・ 振動が発生する場所
- ・ 火気の近く、または高温になる場所
- ・ 平坦でない場所
- ・ 漏電や漏水の恐れのある場所（故障や感電の恐れがあります）
- ・ 強い磁界が発生する場所
- ・ 不安定な場所

■本製品を落としたり、強い衝撃を与えないでください

本製品は精密機械ですので、衝撃を与えないように慎重に取り扱ってください。強い衝撃を与えると
故障の原因となります。

■本機を移動する際はコード類を取り外してください

コードが破損し、火災や感電につながる恐れがありますので、必ずすべての接続をはずしてから
移動してください。

■静電気による破損を防ぐ為、以下のことをお守りください

静電気によって、本製品が破損したり、データの損失、破損を引き起こす恐れがあります。

- ・ 本製品に触れる前に、必ず身近な金属に触れ、身体の静電気を取り除いてください。
- ・ メモリやその他部品の端子部分に手を触れないでください。

■本製品を分解、修理、改造しないでください

火災・感電・故障のおそれがあります(保証の対象外となります)

第2章

セットアップ

1. 設置計画	12
2. 初期設定	16
3. Secure Beagle導入例	20

1. 設置計画

2

セットアップ

ゾーンについて

Secure Beagleは3つのEthernetポートがあり、それぞれが、Insideゾーン、Outsideゾーン、DMZゾーンに対応しています。そのため、ゾーン間の通信を制御することができます。

同じゾーン内の通信はSecure Beagleを通過しないため制御することはできません。制御したい通信がSecure Beagleを通過するように機器を分類し、どの機器をどのゾーンに配置するか検討します(図2-1)。

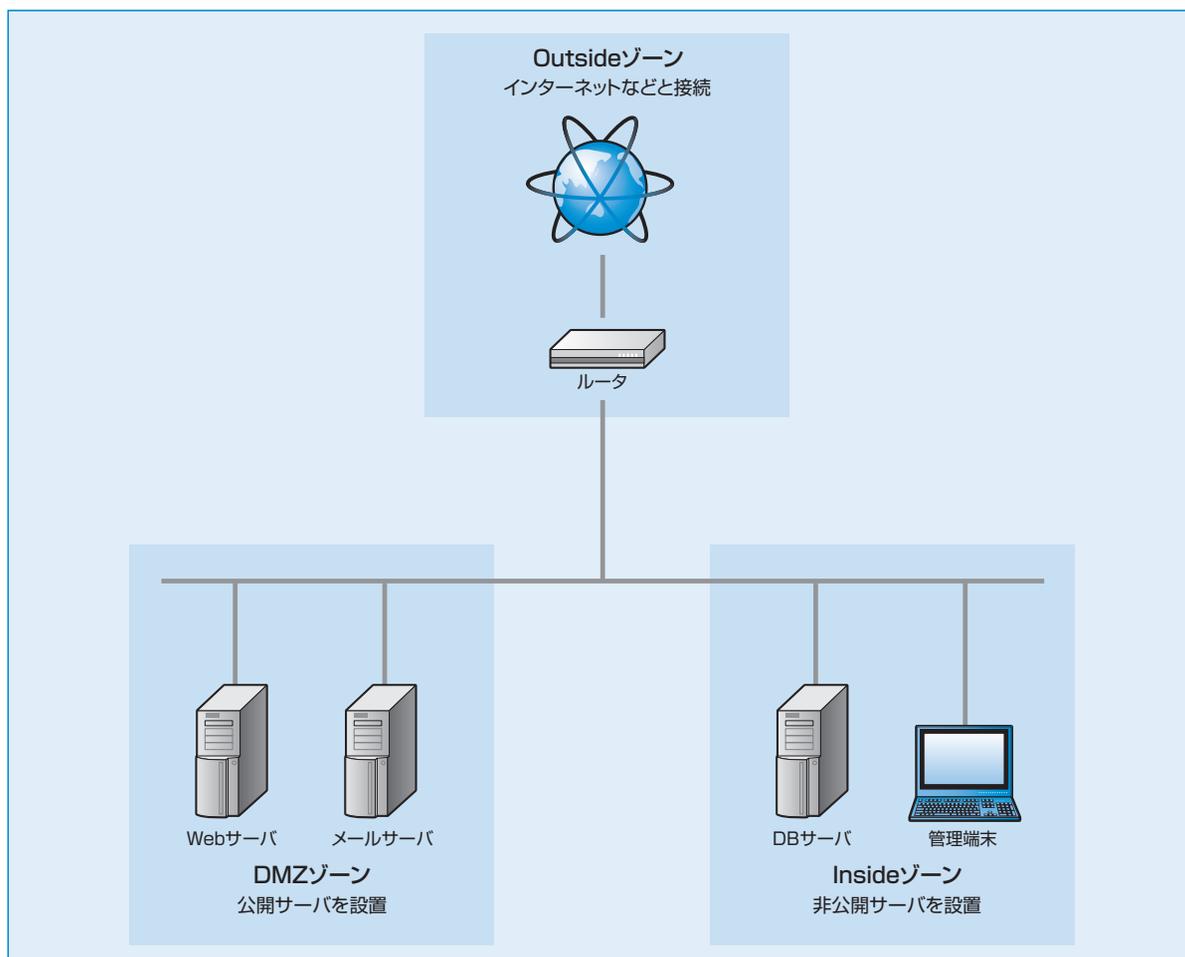


図2-1 Inside-Outside-DMZに適したネットワーク構成例

各ゾーンのネットワークアドレスについて

Secure Beagleの各ゾーン用のEthernetポートはL2レベルで接続されています。ポリシー設定で通過することが許可されているパケットは、Secure BeagleがL2スイッチの様に働き、転送されます。

このため各ポートに接続する機器は、同一のネットワークアドレスに設定してある必要があります。

各ゾーンのアドレスを異なるものにする必要がないため、既存のネットワークにIPアドレスの変更などを伴わず導入することができます。

Secure BeagleにL3ルータの機能を持たせることはできません。

Inside-Outside-DMZゾーンのポリシーの検討

Secure Beagleによって管理するゾーンが3つの場合、InsideゾーンとOutsideゾーン、DMZゾーンを使用します。例えば、Internet回線、Internetにサービスを公開するサーバ、外部に直接サービスを公開しないサーバがあり、3つのゾーンに分ける場合などで、このゾーン構成を使用します(図2-2)。

InsideゾーンにはOutsideゾーンからの直接の接続を防ぐDBサーバなどを設置し、DMZゾーンにはWebサーバなど外部からの接続を許可するサーバを設置する構成が考えられます。

3つのゾーンを構成する場合、次の図2-2の①～⑥についてポリシーを検討し設定します。

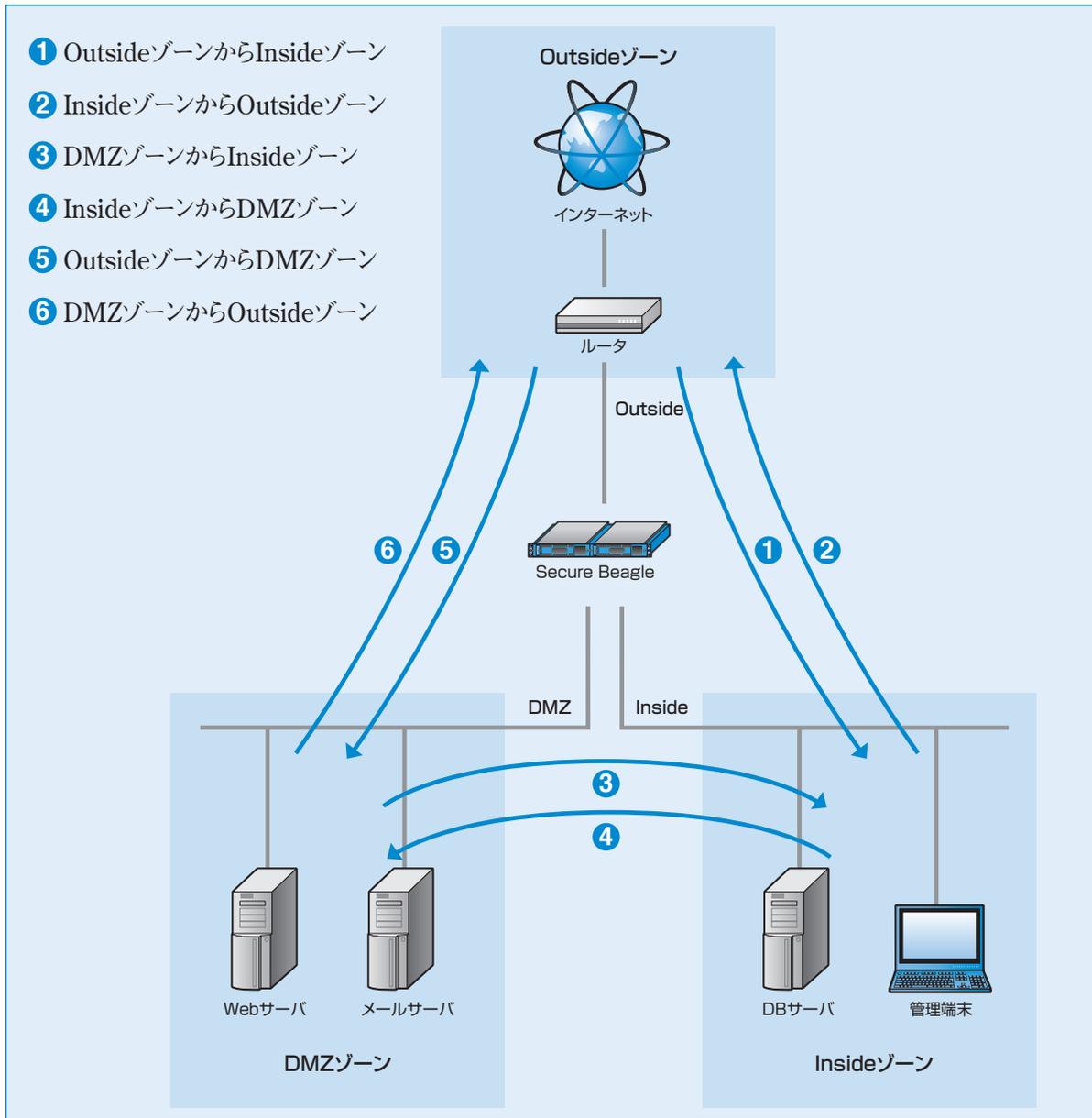


図2-2 Inside-Outside-DMZ型ネットワークへのSecure Beagle導入例

Inside-Outsideゾーン構成の場合

Secure Beagleは最大3つのゾーンを管理できますが、管理するゾーンが2つの場合、InsideゾーンとOutsideゾーンを使用します(図2-3)。

Insideゾーンには、Webサーバやメールサーバなど外部から接続を受けるサーバを設置し、Outsideゾーンにはルータなど外部と通信する機器を設置します。

外部からの接続をWebサーバやメールサーバのサービスで使用するポートに制限することができます。

2つのゾーンを構成する場合、図2-4の①、②のポリシー(通信を許可、禁止する条件)を検討し設定します。

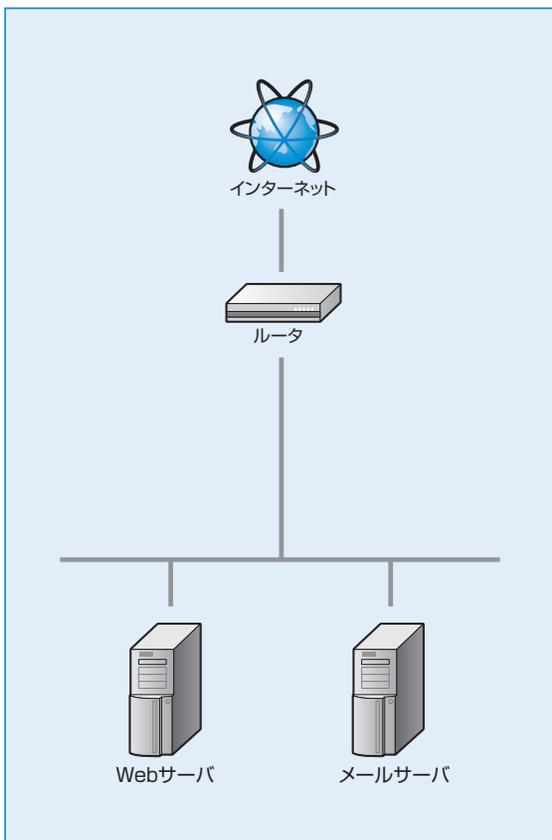


図2-3 Inside-Outside型に適したネットワーク構成

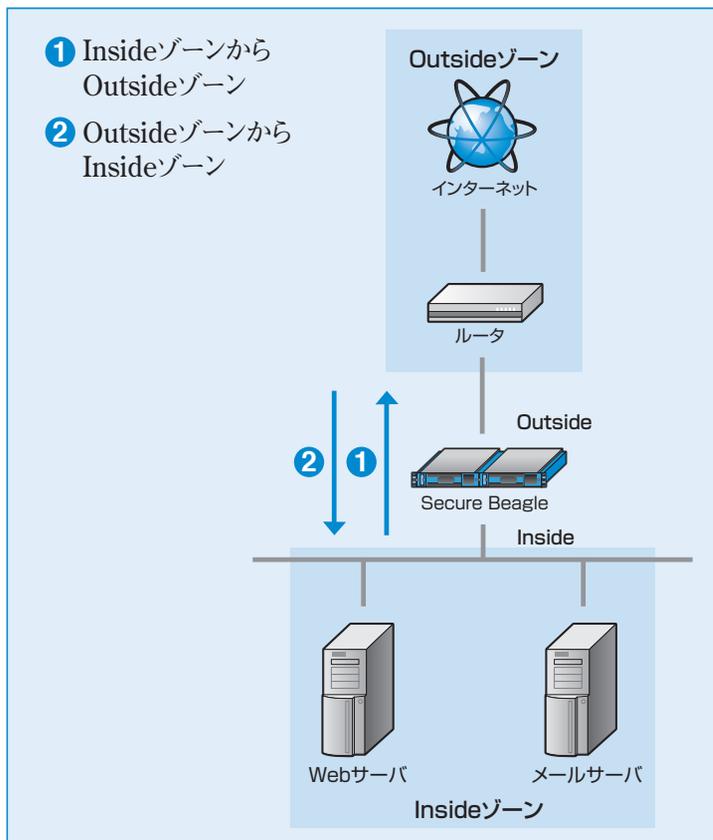


図2-4 Inside-Outside型ネットワークへのSecure Beagle導入例

2. 初期設定

Secure Beagleの工場出荷時は、次のようにネットワークが設定されています。

IPアドレス	192.168.1.1
プレフィックス	24
ゲートウェイ	192.168.1.254

次のいずれかの方法でネットワークの設定を行ってください。メンテナンスPCを利用した方法では、ネットワーク以外の項目についても設定可能ですので、こちらの方法を推奨します。

1. メンテナンスPCを利用して設定する (推奨)

■必要機器

- ・ Webブラウザ (Internet ExplorerまたはFirefox) が使用できるメンテナンスPC (WindowsノートPC など)
- ・ クロスケーブル、またはHUBとストレートケーブル

1 Secure BeagleとメンテナンスPCの接続

Secure BeagleのLAN1とメンテナンスPCを、クロスケーブルを使用して接続します。図2-5のような状態となります。

HUBとストレートケーブルを使用してSecure BeagleとメンテナンスPCそれぞれを接続する方法でもかまいません (図2-6)。この場合、HUBにSecure Beagle、メンテナンスPC以外を接続しないようにご注意ください。



図2-5 メンテナンス端末との接続

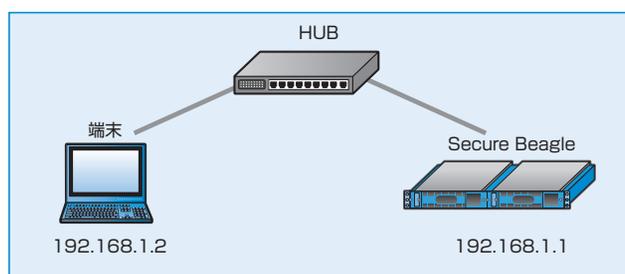


図2-6 ストレートケーブル使用時

2 メンテナンスPCのネットワーク設定

Secure Beagleの工場出荷時のネットワーク設定は192.168.1.1/24となっています。メンテナンスPCのネットワークを次のように設定します。

IPアドレス	192.168.1.2
プレフィックス	24
ゲートウェイ	192.168.1.254 (任意)

3 Secure Beagleの電源投入

Secure Beagleのコンセントを電源に接続し、電源スイッチを押下します。

4 メンテナンスPCからWebブラウザによる接続

メンテナンスPC上のWebブラウザにて次のURLを開きます。

<https://192.168.1.1:18180>

図2-7のログイン画面が表示されます。

電源投入後、システムが起動するまで約1分程度の時間をおいてから、Webブラウザによる接続を行ってください。

工場出荷時のログインIDおよび初期パスワードは、装置に添付されているシートのWeb管理画面のログインID、パスワードを入力してください。



図2-7 ログイン画面



図2-7のログイン画面が表示されない場合は、次の確認を行ってください。

- ・ Secure Beagleが電源投入されているか(電源ランプの確認)
- ・ Secure BeagleとメンテナンスPC、HUBがケーブルでしっかり結線されているか
- ・ メンテナンスPCのネットワーク設定が正しいか
- ・ 入力したURLが正しいか

Secure Beagleのネットワーク設定が変更されている場合、このURLでは接続できません。
Secure Beagleのネットワーク設定が不明な場合は、コンソール接続を利用してネットワークの再設定を行ってください。

5 ネットワーク設定

設置するネットワーク構成にあわせてネットワーク設定を行います。

【基本設定】→【ネットワーク】を選択します。

- ・ ネットワーク(IPアドレス、プレフィックス、ゲートウェイ)を設定します。



ネットワークの編集については P58 を参照してください。

6 パスワード変更

工場出荷時は初期パスワードのため、必ずパスワード変更を行ってください。

【アクセス制限】→【パスワード変更】にてパスワード変更を行います。



管理者パスワードの変更については P63 を参照してください。

7 接続許可IPアドレスの制限

工場出荷時はどのIPアドレスからも管理画面への接続を許可する状態のため、接続を許可するIPアドレスを設定して制限を行ってください。

【アクセス制限】→【接続許可IPアドレス】にてSecure Beagleの管理画面への接続を許可するIPアドレスの制限を行います。接続許可IPアドレスの登録が無い場合は、IPアドレスによる制限は働きませんが、1件以上登録されているときには、登録IPアドレス以外からの接続はできなくなります。



接続許可IPアドレスの制限についてはp.86を参照してください。

8 Secure Beagleの停止と設置

Secure Beagleの電源ボタンを長押し(4秒程度)、電源を切ります。

Secure Beagleを使用するネットワークに設置し電源を入れると、設定したIPアドレスで起動します。WebブラウザでSecure Beagleに設定したIPアドレスを指定して管理画面を開き、設定を継続します。

[https://\[Secure Beagleに設定したIPアドレス\]:18180](https://[Secure Beagleに設定したIPアドレス]:18180)

2.コンソール接続を利用して設定する

コンソール接続の場合、設定できるのは、IPアドレス、プレフィックス、デフォルトゲートウェイのみになります。コンソール接続による設定を行った後、メンテナンスPCを使用してWebブラウザからその他の項目の設定を行う必要があります。

■必要機器

モニタ (Model 10 の場合 : D-sub 15ピン VGA 端子
Model 30、Model 200 の場合 : DVI 端子)
キーボード (PS/2 端子)

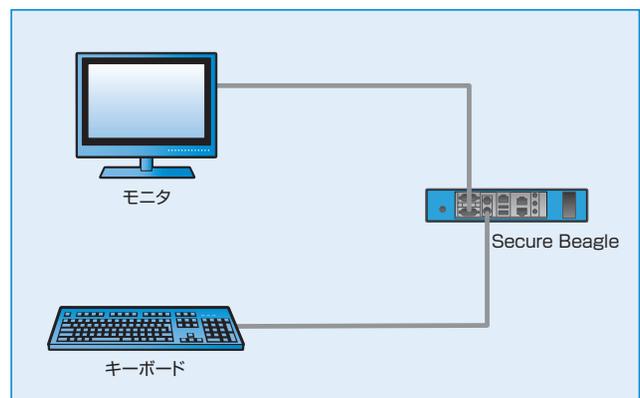


図2-8 コンソール使用方法

1 Secure Beagleと機器の接続

Secure Beagle とモニタを接続します。

Secure Beagleのキーボード端子にPS/2キーボードを接続します。

2 Secure Beagleの電源投入

Secure Beagleのコンセントを電源に接続し、電源スイッチを押下します。

モニタにログインプロンプトが表示されますのでログインIDとパスワードを入力します。

このログインIDおよびパスワードは、装置に添付されているシートのコンソールログインID、パスワードを入力してください。



このログインIDとパスワードはSecure Beagleの管理画面へのログインID、パスワードとは異なります。変更することはできません。

3 ネットワーク設定

ログインに成功するとメニューが表示されますので、ネットワーク設定を選択します。
本設定で設定可能な項目は、次の項目に限定されます。

- IPアドレス
- プレフィックス
- ゲートウェイ

上記以外の設定項目はネットワーク設定後、メンテナンスPCを使用してWebブラウザから設定してください。



コンソール管理からのネットワーク設定を変更する方法は P81 を参照してください。

4 Secure Beagleの停止と設置

Secure Beagleの電源ボタンを長押しすることで、電源を切ることができます。

Secure Beagleを使用するネットワークに設置し、電源を入れると設定したIPアドレスで起動します。Webブラウザで次のURLを開き、設定を継続します。

[https://\[Secure Beagleに設定したIPアドレス\]:18180](https://[Secure Beagleに設定したIPアドレス]:18180)



本手順では、管理者パスワードの変更、接続元IPアドレスの制限は行われておりません。
Secure Beagleを使用するネットワークに設置後、Webブラウザより管理画面にログインし、
管理者パスワードの変更、接続元IPアドレスの制限を実施してください。



管理者パスワードの変更方法については P63 を参照してください。



接続元 IP アドレスの制限については P64 を参照してください。

3. Secure Beagle導入例

ここでは一般的な図2-9のネットワーク構成にSecure Beagleを導入する手順を紹介します。

! ネットワーク構成例のIPアドレスに便宜上、10.1.1.0のIPアドレスを使用しております。

1 Secure Beagleの初期設定

Secure Beagle初期設定手順に従って
Secure Beagleのネットワーク設定を変更してください。

👉 Secure Beagle の初期設定手順については
P16 を参照してください。

本構成例では、Secure Beagleのネットワークを次の
ように設定します。

IPアドレス	10.1.1.2
プレフィックス	24

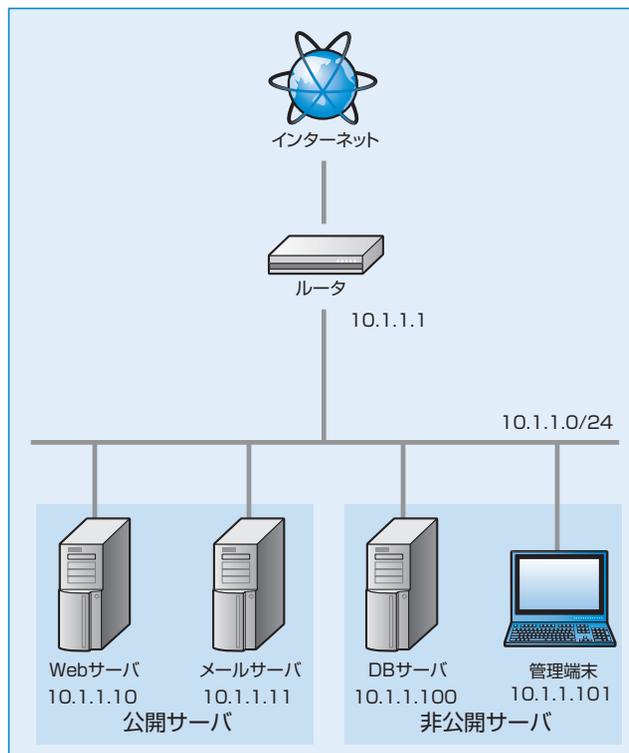


図2-9 Secure Beagle導入前のネットワーク構成

2 Secure Beagleの設置

図2-10のネットワークにSecure Beagleを設置します。

Secure Beagleの各LANを以下のように接続します。

Inside (LAN1) には非公開サーバ (DBサーバ、
管理端末) を接続します。

Outside (LAN2) にはインターネットに接続している
ルータ (10.1.1.1) を接続します。

DMZ (LAN3) には公開サーバ (Webサーバ、メール
サーバ) を接続します。

全て接続すると図2-10のようなネットワーク構成図
になります。

💡 各サーバおよびクライアントのIPアドレス
などネットワーク設定を変更する必要はあり
ません。

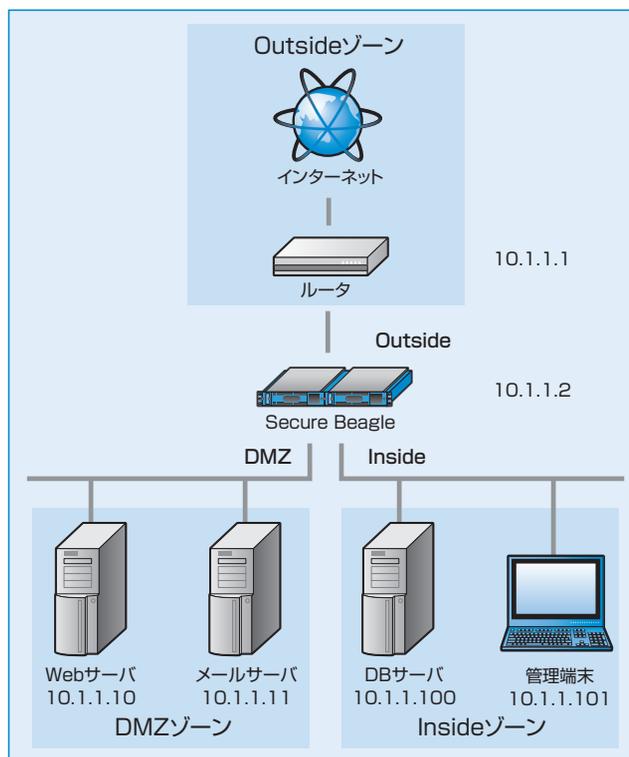


図2-10 Secure Beagle導入後のネットワーク構成

3 ポリシー設定例

図2-10のシステムの各ゾーン(Inside、Outside、DMZ)間のアクセス制御を行うポリシー設定を行います。

例として各ゾーンは次のような役割とします。

Outsideゾーン	インターネットとの接続をする。
DMZゾーン	外部にサービスを公開するサーバを設置する。 Outsideゾーンからの接続はサービスに使用する通信のみに限定する。
Insideゾーン	インターネットからの直接の接続を許可しないサーバを設置する。Outsideゾーンからの接続は許可せず、DMZからについてはサービスに必要なものだけに限定する。

役割条件をもとに、各ゾーン間のアクセスポリシーを具体的に定めます。

例として次のように定めます。

- OutsideゾーンからInsideゾーンへのアクセスは拒否とする。
- OutsideゾーンからDMZゾーンへのアクセスは下記の条件のみ許可する。

Webサーバへはhttp(80番ポート)、https(443番ポート)へのtcpのみ許可
メールサーバへはsmtp(25番ポート)、pop3(110番ポート)へのtcpのみ許可

- DMZゾーンからOutsideゾーンへのアクセスは全て拒否する。



Outsideゾーンから公開サーバへのアクセスの応答はステートフルインスペクション機能により自動的に通信が許可されます。

- DMZゾーンからInsideゾーンへのアクセスは下記の条件のみ許可する。

WebサーバからDBサーバへの3306番ポート(DBサービスのポート番号)へのtcpのみ許可

- InsideゾーンからOutsideゾーンへのアクセスは全て許可する。
- InsideゾーンからDMZゾーンへのアクセスは全て許可する。

上記ポリシー情報をSecure Beagleに設定します。



ポリシー設定条件のいずれにも一致しない通信はSecure Beagleを通過しません。許可する条件を実際には設定します。拒否する条件を記述しその後に無制限に許可する設定を記述すれば、拒否の条件以外は許可するような設定も可能です。

1. Inside→Outsideゾーンのポリシー設定

- 1 【ファイアウォール】→【ポリシー】を選択し、各ゾーン間のポリシーリストを表示します(図2-11)。

 ゾーン指定をAny以外に指定することで指定のゾーンだけを表示することができます。

- 2 ポリシー設定画面にてInside→Outsideゾーンの右側にある「追加」ボタンをクリックすると対象ゾーンのポリシー追加画面が表示します(図2-12)。

- 3 本構成例では、Inside→Outsideゾーンのポリシーは「Inside→Outsideゾーンへのアクセスは全て許可する。」であるため、全てのパケットを許可するポリシーを設定します。

送信元	IPアドレス指定 0.0.0.0/32
送信先	IPアドレス指定 0.0.0.0/32
プロトコル	全てのプロトコル
動作	許可



図 2-11 各ゾーンのポリシーリスト

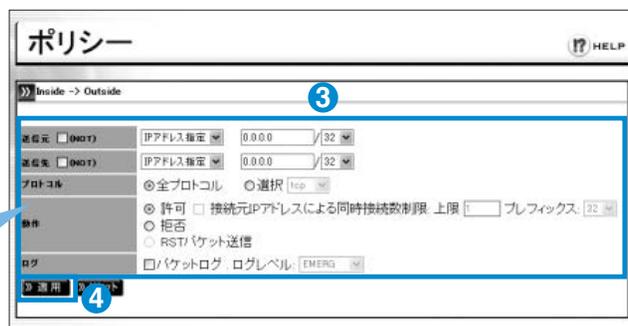


図2-12 ポリシー追加画面

- 4 「適用」ボタンをクリックすると設定が反映されます。適用後は再びポリシーリスト画面に切り替わりますので、設定したポリシーを確認してください(図2-13)。



図 2-13 ポリシーリスト (ポリシー追加後)

Inside→DMZゾーンへのポリシー定義も同様に設定します。

2. Outside→DMZゾーンのポリシー設定

- 1 ポリシーリストから、Outside→DMZゾーンの右側にある「追加」ボタンをクリックし、Outside→DMZゾーンのポリシー追加画面を表示させます。



図 2-14 各ゾーンのポリシーリスト

- 2 Outside→DMZゾーンのポリシー設定のうち「Webサーバ(10.1.1.10)へは、http(80番ポート)、https(443番ポート)へのtcpのみ許可」のポリシーを設定します(図2-15)。

送信元	IPアドレス指定 0.0.0.0/32
送信先	IPアドレス指定 10.1.1.10/32
プロトコル	選択「tcp」
送信元ポート	0
送信先ポート	80,443
動作	許可

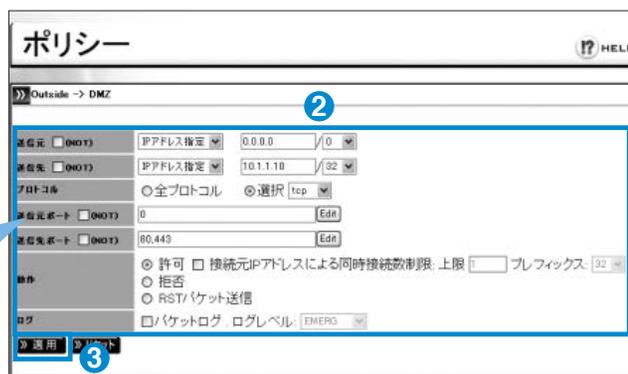


図2-15 Webサーバへのポリシー追加

- 3 「適用」ボタンをクリックすると設定が反映されます。
メールサーバ(10.1.1.11)についても同様の手順でポリシー設定を行います(図2-16)。



図 2-16 Outside → DMZ ゾーンのポリシーリスト

3. DMZ → Inside ゾーンのパリシー設定

- 1 ポリシーリストから、DMZ → Inside ゾーン
の右側にある「追加」ボタンをクリックし、
Outside → DMZ ゾーンのパリシー追加画面
を表示させます。

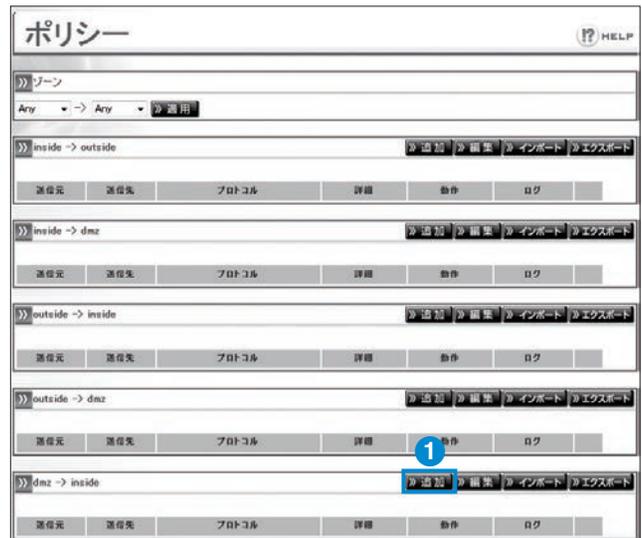


図 2-17 各ゾーンのパリシーリスト

- 2 DMZ → Inside ゾーンのパリシーである「Web
サーバ(10.1.1.10) から DB サーバ(10.1.1.100)
への 3306 番ポート(DB サービスのポート番号)
への tcp のみ許可」を設定します (図 2-18)

送信元	IP アドレス指定 10.1.1.10/32
送信先	IP アドレス指定 10.1.1.100/32
プロトコル	選択「tcp」
送信元ポート	0
送信先ポート	3306
動作	許可

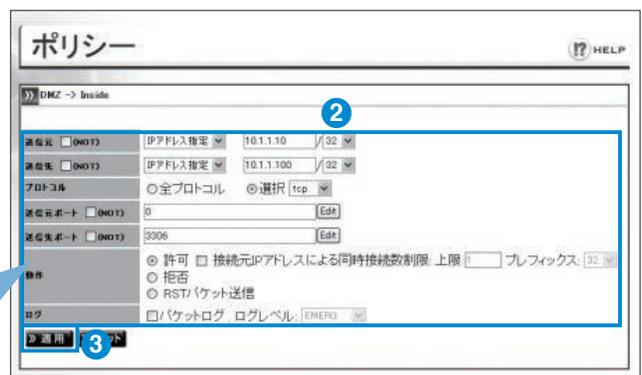


図 2-18 ポリシーリスト (ポリシー追加後)

- 3 ポリシーリストは図 2-19 のようになります。



図 2-19 ポリシーリスト (ポリシー追加後)

4. Outside → Inside ゾーンのパリシー設定

本構成例では、Outside → Inside ゾーンのパリシーは「Outside ゾーンから Inside ゾーンへのアクセスは拒否とする」です。Secure Beagle ではポリシーが未設定の場合、対象ゾーンの packets を全て拒否しますので、ポリシーを設定しなくても問題ありません。なお、ポリシーを明記する目的で全て拒否するポリシーを設定しても動作に影響はありません。

以上で全てのゾーン間のポリシー設定が完了しました。
各ゾーンの機器から対象ゾーンへアクセスを行い、ポリシーどおりか確認してください。

第3章

3

ファイアウォール

1. ポリシーリスト	26
2. ポリシー追加	27
3. ポリシーの編集	31
4. ポリシーの削除	32
5. インポート	32
6. エクスポート	33
7. ポリシー優先度の変更	34

1. ポリシーリスト

- 1 【ファイアウォール】→【ポリシー】を選択することによりSecure Beagleに設定されているポリシー設定内容を表示することができます。



図 3-1 ポリシーリスト

- 2 ゾーン指定することで指定したゾーン間のポリシー設定だけが表示されます。
図3-2は、OutsideからInsideへのポリシー設定を表示した例です。Anyを指定した場合、Outside、Inside、DMZのすべてを指定したことになります。

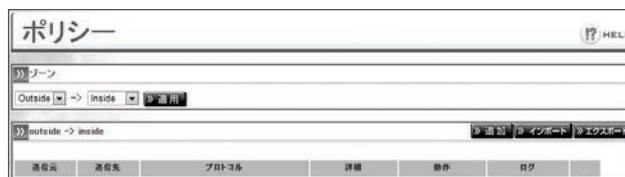


図 3-2 ポリシーリスト (Outside → Inside)

! 初期状態ではポリシーが何も設定されていません。この為、ポリシーの一覧表示でも図3-2のように設定ポリシーは表示されません。この場合は、このポリシーのゾーン間の通信は全て拒否されます。

2. ポリシー追加

① ポリシーリストの対象ゾーンの右上の「追加」ボタンをクリックすることで対象ゾーン間のポリシーの追加画面が表示されます(図3-3)。

② ポリシー追加画面では、以下の項目を入力し、ポリシーを決定します。

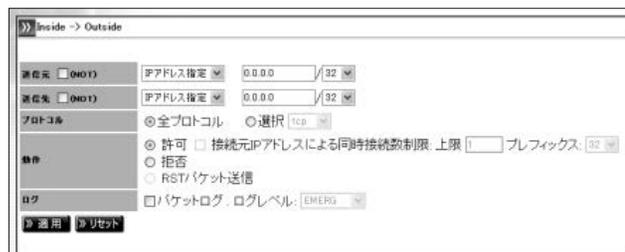


図3-3 ポリシー追加

送信元

設定方法は P28 を参照してください。

送信先

設定方法は P28 を参照してください。

プロトコル

設定方法は P29 を参照してください。

動作

設定方法は P30 を参照してください。

ログ

設定方法は P31 を参照してください。

③ ポリシー決定後、「適用」をクリックすることでポリシーが作成されます。

④ 再びポリシーリスト画面に戻ります。

⑤ 設定した通りの内容になっているか確認してください。

「適用」ボタンをクリックしてポリシーを登録すると、直ちに動作に反映されます。



図3-4 ポリシーリスト

送信元・送信先

送信元…送信先アドレスです。IPアドレス、ネットワークアドレス、国単位で指定することができます。
送信先…送信先アドレスです。IPアドレス、ネットワークアドレス、国単位で指定することができます。



送信元、送信先にany (0.0.0.0/32)を指定した場合、全てのIPアドレスが対象となります。
ポリシー追加画面の初期状態ではanyが指定されています。

3

ファイアウォール

指定したIPアドレス以外を条件にする場合

指定したIPアドレス以外の場合についての条件を記述する場合には、 (NOT) のチェックボックスにチェックを入れます。

例) 10.1.2.0/24のネットワーク以外を対象にする場合

送信元 (NOT) IPアドレス指定 10.1.2.0/24

と、指定します。

この場合、ポリシーリストではIPアドレスの前に ~ が付加され、

~10.1.2.0/24

のように表示されます。

特定の国からのアクセスを制限する

国指定でアクセスを制御する場合は、送信元もしくは送信先にて国指定を指定します。

例) 送信元を日本とする場合

送信元 国指定 JP

と、国名を表すアルファベット二文字のコードで指定します。

「編集」ボタンをクリックすると国選択画面が表示されます。この画面では国名が一覧表示されますので、一覧から選択して指定することができます(図3-5)。



各国のIPアドレス情報はGeoIPデータベースによって管理されています。
IPアドレス情報を最新に保つにはGeoIPデータベースを定期的に更新する必要があります。



GeoIP データベースのアップデートは P48 を参照してください。

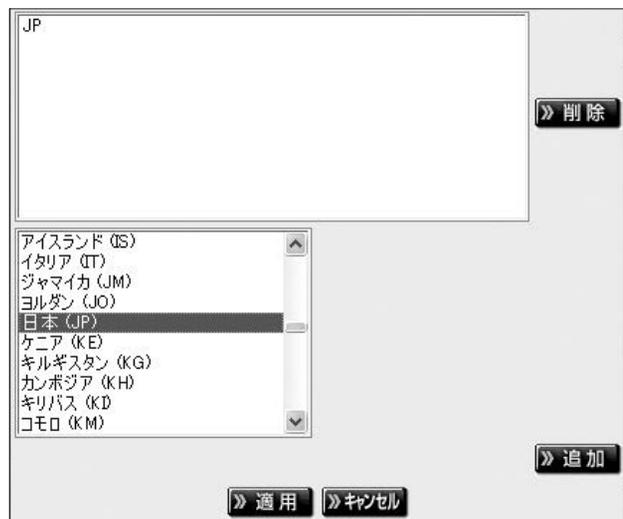


図3-5 国編集画面

特定の国以外のアクセスを制限する

国指定で指定した国以外のアクセスを制御する場合は、 (NOT) のチェックボックスにチェックを入れます。国指定方法は「特定の国からのアクセスを制限する」と同様の手順で指定します。

例) 送信元を日本以外とする場合

送信元 (NOT) 国指定 JP

と、指定します。

! GeoIPデータベースはIPアドレスを割り当てた国の情報を元に行っているため実際に利用者のいる場所と一致しない場合があります。例えば、日本国内のプロバイダでも日本以外に割り当てられたIPアドレスを使用している場合があります。また新規に割り当てられGeoIPデータベースに反映されていないIPアドレスの場合も正しく判断がされません。

プロトコル

パケットのプロトコルを指定することができます。

特定のプロトコルに対してポリシー設定を行いたい場合、プロトコル指定で「選択」を選び、プロトコルを指定します。

Secure Beagleでは以下のプロトコルに対して制御を行うことができます。

tcp	udp	l2tp
icmp	igmp	
ipip	gre	



「全プロトコル」を選択した場合は全てのプロトコルが対象になります。

tcpもしくはudpを選択した場合

ポート番号を番号で指定します。

「編集」ボタンをクリックすることによりポート番号選択画面が表示されます。この画面ではポートを使用するサービス名での指定やポート番号の範囲での指定が可能です(図3-6)。

図3-6 ポート編集画面

icmpを選択した場合

ICMP typeを指定することができます。

動作

送信元、送信先、プロトコルで指定したパケットに対しての動作を記述します。
対象パケットの通過を許可する場合は、「許可」、通過させない場合は「拒否」を選択します。また、プロトコル指定で「tcp」を指定している場合、「RSTパケット返信」することもできます。

送信元IPアドレスによる同時接続数制限 (tcpの場合)

プロトコルでtcpを指定している場合、特定のIPアドレスからの同時接続数の上限値を設定しこれをこえる場合に接続を制限することができます。接続元IPアドレスによる同時接続数制限のチェックボックスをチェックし、制限数を入力します。ネットマスク欄は、接続元のIPアドレス毎に制限する場合は32を選択します。ネットワークアドレス単位に制限する場合は、ネットワークアドレスのビット数を設定します。

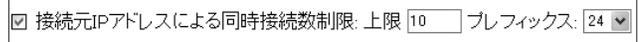


図3-7 接続制限

例) 各IPアドレスからの接続を1ずつにしたい場合

接続元IPアドレスによる同時接続数制限	<input checked="" type="checkbox"/>
上限	1
プレフィックス	32

と指定します。

例) クラスCネットワーク単位での同時接続を合わせて10にしたい場合

接続元IPアドレスによる同時接続数制限	<input checked="" type="checkbox"/>
上限	10
プレフィックス	24

と指定します。

ログ取得

各ポリシーに該当するアクセスログをSyslog出力することができます。
また、ログレベル欄の設定によってSyslogのpriorityの値を変更することができ、ポリシーの重要度に応じてpriorityの値を変えることができます。

例) 対象ポリシーのログをALERTレベルで採取する

パケットログ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> パケットログ、ログレベル: ALERT
ログレベル	ALERT	

図3-8 ログ編集画面

と指定します。



ログを採取するにはSyslog設定を行う必要があります。



Syslog 設定は P51 を参照してください。

3. ポリシーの編集

ポリシーの内容を編集したい場合

- 1 ポリシーリスト上で対象ポリシーの「**編集**」をクリックします。
- 2 編集画面が表示されますので変更したい項目を編集します。
- 3 「**適用**」をクリックすると変更が完了します。

4. ポリシーの削除

ポリシーを削除したい場合

- 1 ポリシーリスト上で対象ポリシーの「削除」をクリックします。
- 2 確認ダイアログが表示されますので「OK」を選択します。

5. インポート

ポリシーをインポートしたい場合

- 1 ポリシーリストの対象ゾーンの右上の「インポート」をクリックすることで対象ゾーン間のポリシーのインポート画面が表示されます(図 3-9)

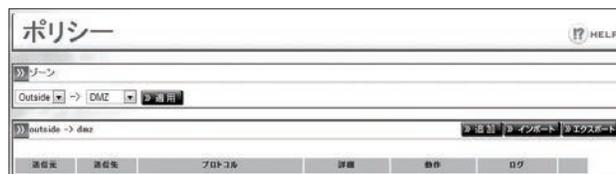


図 3-9 ポリシー一覧画面

- 2 ポリシーインポート画面で、インポートするファイルを選択し「実行」をクリックします。(図 3-10)



図 3-10 インポート画面

-  インポート項目については、33 ページを参照してください。

- 3 ファイルの内容が画面に表示されます(図 3-11) そのままインポートする場合は「実行」、キャンセルする場合は「キャンセル」をクリックします。

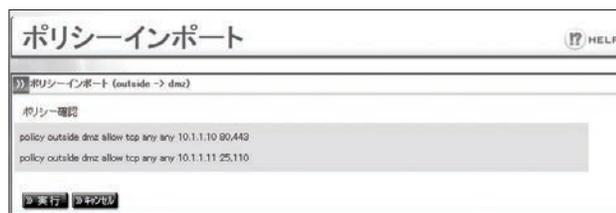


図 3-11 インポート内容確認

6. エクスポート

ポリシーをエクスポートしたい場合

- 1 ポリシーリストの対象ゾーンの右上の「エクスポート」をクリックすると、ポリシーファイルのダウンロードが開始されます。
- 2 エクスポートファイルの各項目は以下の通りです。辻辻達辻達達
例) 指定したポートのみを許可しログレベル「6:INFO」でログ出力する場合

policy outside inside allow tcp any any any 80,443 log 6
 a b c d e h i j k l m

	項目名	入力条件	説明
a	ポリシー	必須	「policy」固定
b	送信元ゾーン	必須	「inside」「outside」「dmz」
c	送信先ゾーン	必須	「inside」「outside」「dmz」
d	動作	必須	「allow : 許可」 「deny : 拒否」 「connlimit [接続元 IP アドレスによる同時接続数上限数] [プレフィックス] : 送信元接続制限」 「reject : RST パケット送信」 ※プロトコルで「tcp」選択時のみ「connlimit」「reject」を指定可能
e	プロトコル	必須	「ip (全プロトコル)」「tcp」「udp」「icmp」「igmp」「igip」「gre」「l2tp」
f	ICMP	任意	プロトコルで「icmp」を選択した場合「type」固定 ※プロトコルで「icmp」を選択した場合必須
g	ICMP タイプ	任意	「any」「ping」「pong」「source-quench」「destination-unreach」「redirect」 「router-advertisement」「router-solicitation」「ttl-exceeded」「parameter-problem」 「timestamp-request」「timestamp-reply」「address-mask-request」「address-mask-reply」 ※プロトコルで「icmp」を選択した場合必須
h	送信元制限	必須	国指定の場合「c: [国コード, 国コード, ...]」 IP 指定の場合「[IP アドレス] / [プレフィックス]」 ※制限しない場合「any」 ※指定した送信元以外を制限する場合頭に「~」をつける
i	送信元ポート	任意	[ポート, ポート, ...] ※指定したポート以外を制限する場合頭に「~」をつける ※プロトコルに「tcp」「udp」を指定した場合必須
j	送信先制限	必須	国指定の場合「c: [国コード, 国コード, ...]」 IP 指定の場合「[IP アドレス] / [プレフィックス]」 ※制限しない場合「any」 ※指定した送信先以外を制限する場合頭に「~」をつける
k	送信先ポート	任意	[ポート, ポート, ...] ※指定したポート以外を制限する場合頭に「~」をつける ※プロトコルに「tcp」「udp」を指定した場合必須
l	ログ	任意	ログ出力する場合「log」固定
m	ログレベル	任意	「0 : EMERG」「1 : ALERT」「2 : CRIT」「3 : ERR」「4 : WARNING」 「5 : NOTICE」「6 : INFO」「7 : DEBUG」 ※ログ出力する場合のみ設定



以下インポートファイルの作成に参考にしてください。

例 1. 特定のネットワーク (192.168.1.0/24) からの接続を許可する場合

```
policy inside outside allow ip 192.168.1.0/24 any
```

例 2. 特定のポート (http,https) のみを許可する場合

```
policy outside inside allow tcp any any any 80,443
```

例 3. 特定の国 (日本、アメリカ、フランス) のアクセスを許可する場合

```
policy outside inside allow ip c:JP,US,FR any
```

例 4. 指定した ICMP タイプのみを許可する場合

```
policy outside inside allow icmp type ping any any
```

例 5. 同時接続に上限を設ける場合

```
policy outside inside connlimit 30 32 tcp ~c:JP,AF,AG any any any
```

7. ポリシーの優先度の変更

複数のポリシーを設定した場合、ポリシーはリスト表示で上に表示されているものから順に評価されます。動作がすべてallowまたはdenyの場合、ポリシー評価順序は動作に影響をあたえませんが、allowの条件とdenyの条件が混在している場合は評価順序が動作に影響します。例えば、allowの条件があってもそれよりも上の行に同じ条件で動作がdenyの条件があった場合はdenyが優先されます。評価順序は次の方法で変更することができます(図3-9)。



図 3-12 ポリシー優先度

優先度変更手順

- ① ポリシー 一覧画面より、対象ゾーンの「編集」ボタンをクリックする。
- ② ポリシーの優先度を上げたい場合対象ポリシーの「↑」ボタンをクリックします。
- ③ ポリシーの優先度を下げたい場合対象ポリシーの「↓」ボタンをクリックします。



ポリシーの評価順序の変更を行うと、直ちに動作に反映されます。

第4章

冗長化構成

4

1. 冗長化構成のメリット	36
2. 冗長化構成例	37
3. 冗長化構成時の動作について	40

1. 冗長化構成のメリット

図4-1はSecure Beagleを導入した一般的な構成ですが、この構成の場合、Secure Beagle部分が冗長化構成になっておらず、この部分に障害が発生した場合、サービスが停止してしまいます。

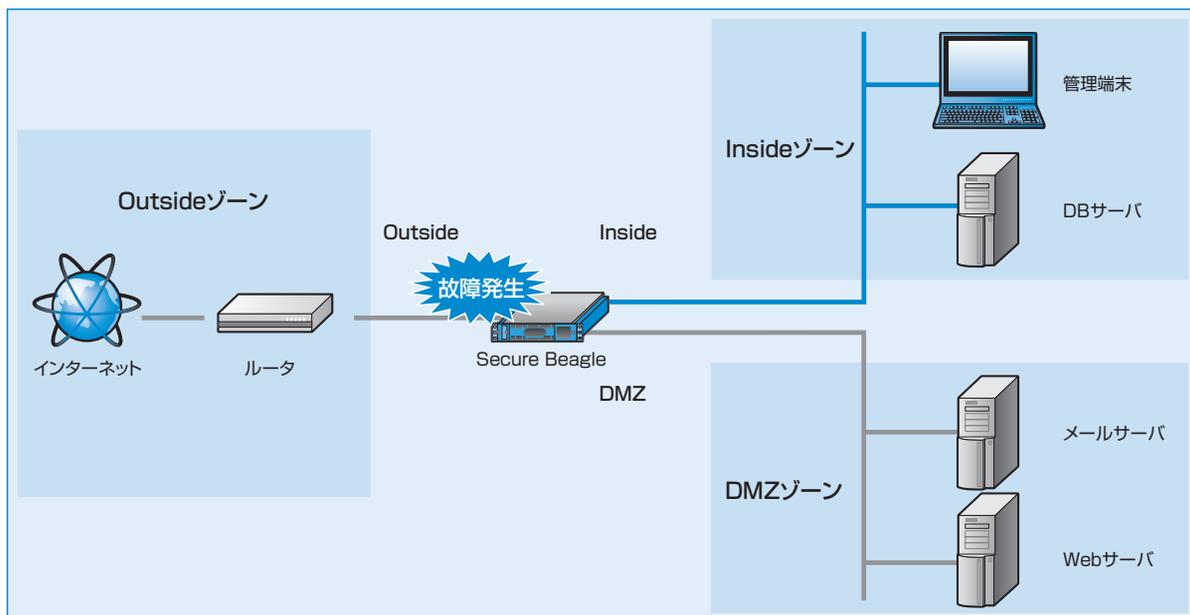


図4-1 単体構成のSecure Beagle構成

Secure Beagleは冗長化構成に対応していますので、同一の機種を2台使用して冗長化構成を構築することができます。スタンバイ機はマスター機に障害が発生したことを検知すると、フェイルオーバーを行い、動作を継続します(図4-2)。

また、Secure Beagleのメンテナンスなどを行う場合でも、動作の停止を最小限にとどめることができます。

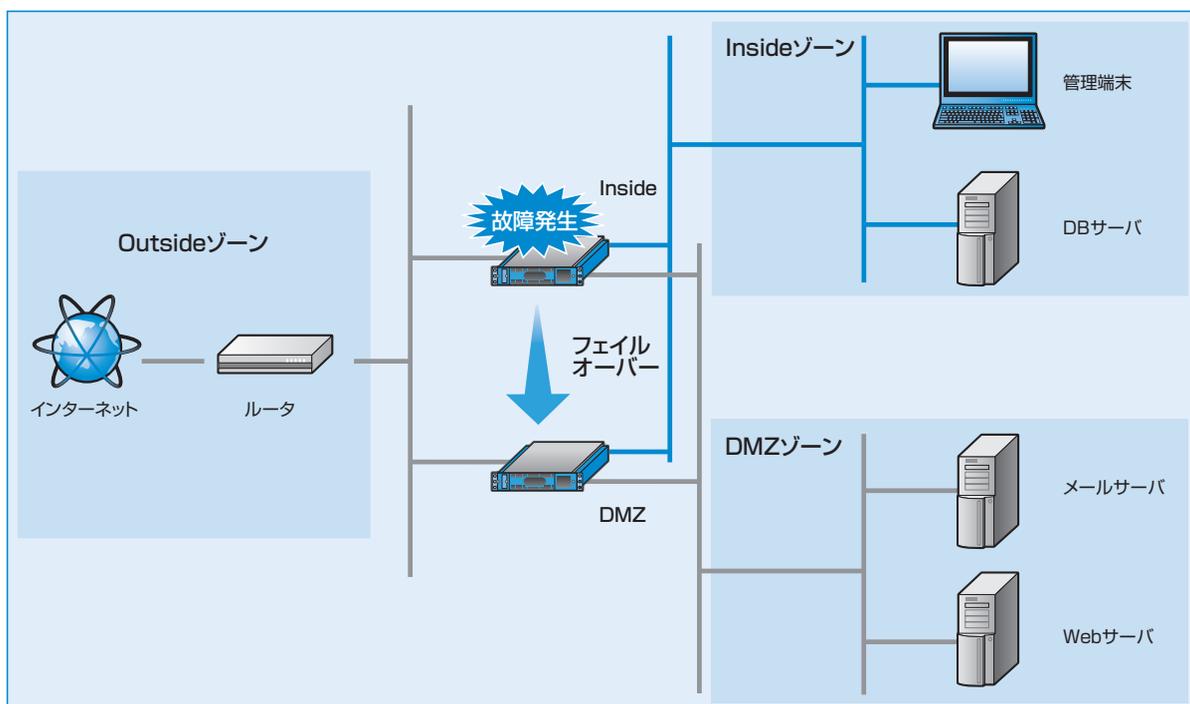


図4-2 冗長化構成のSecure Beagle構成

2. 冗長化構成例

単体構成から冗長化構成への変更はSecure Beagleを2台用意することでいつでも可能です。

ここでは2.3章で導入したInside-Outside-DMZゾーン構成のネットワーク構成に冗長化構成でSecure Beagleを導入する場合を例に説明します。Inside-Outsideゾーン構成のネットワーク構成でも、冗長化構成を構築する手順は同一です。

1 Inside-Outside-DMZゾーンのセットアップ

「2章-3 Secure Beagle導入例」(P20)に従い、まず図4-3のようなInside-Outside-DMZゾーンの構成を構築します。

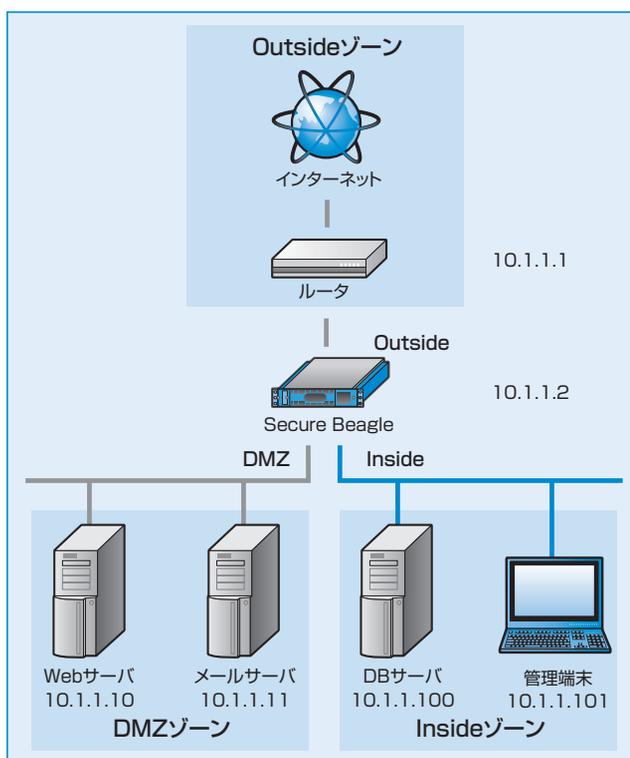


図4-3 Inside-Outside-DMZゾーンの単体構成

2 マスター機の冗長化設定

現在、稼働しているSecure Beagle (10.1.1.2)をマスター機として動作するよう、冗長化構成の変更を行います(図4-4)。

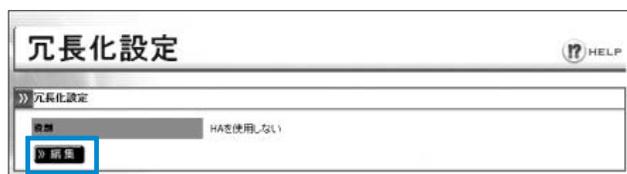


図4-4 冗長化設定画面

Secure Beagle (10.1.1.2)の管理画面にログインします(図4-5)。

【基本設定】→【冗長化設定】を選択し、冗長化設定の「編集」を行います。

役割を「マスター」に変更すると、さらに設定項目が表示されます(図4-5)。

導入例では、以下のように設定します。

役割	マスター
パートナーIPアドレス	10.1.1.3
同期パスワード	securebeaglesync
VRID	111

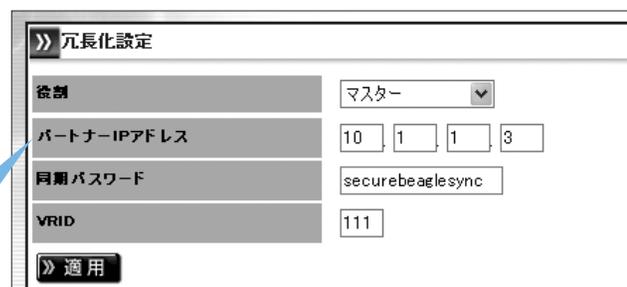


図4-5 冗長化設定編集画面(マスター)

 冗長化設定については P60 を参照してください。

 同期パスワードは、第三者に推測されにくい、独自の文字列を設定してください。同期パスワードには、半角英数字のみ使用可能です。

 VRIDは1から255までの整数を設定することができます。冗長化構成を行う機器同士には同じ値を設定します。同一ネットワーク内の機器にVRRPを使用する機器がある場合には、設定されているVRIDを調査の上、重複しないように設定してください。同一ネットワーク内に、冗長化構成の別のSecure Beagleを設置する場合にもVRIDが重複しないように設定してください。

 同一ネットワーク内の機器で重複したVRIDを設定すると、通信異常などの不具合が発生することがあります。

「適用」をクリックすると設定が反映されます。

再起動後、【冗長化設定】を選択して冗長化設定が変更されていることを確認してください(図4-6)。

役割	マスター
現在の動作状態	稼働中



冗長化設定	
役割	マスター
パートナーIPアドレス	10.1.1.3
同期パスワード	securebeaglesync
VRID	111
現在の動作状態	稼働中
HA同期状態	未同期

図4-6 装置の状態表示画面

3 スタンバイ機の初期設定

「2章-2 初期設定」(P16)に従い、スタンバイ機のSecure Beagleの初期設定を行います。本構成例では、スタンバイ機のIPアドレスは以下のように設定します。

IPアドレス	10.1.1.3
プレフィックス	24
ゲートウェイ	10.1.1.1

4 スタンバイ機の冗長化設定

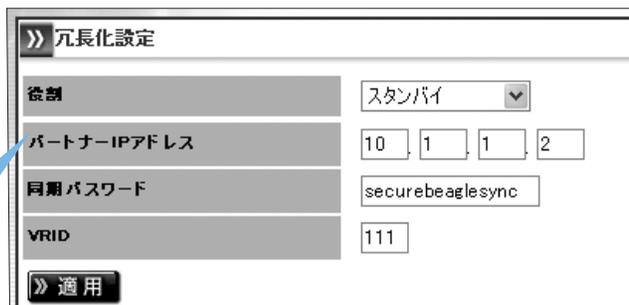
スタンバイ機として動作するよう、冗長化設定の変更を行います。

【基本設定】→【冗長化設定】を選択し、冗長化設定の編集を行います。

役割を「スタンバイ」に変更すると、さらに設定項目が表示されます(図4-7)。

導入例では、以下のように設定します。

役割	スタンバイ
パートナーIPアドレス	10.1.1.2
同期パスワード	securebeaglesync
VRID	111



冗長化設定	
役割	スタンバイ
パートナーIPアドレス	10 . 1 . 1 . 2
同期パスワード	securebeaglesync
VRID	111
適用	

図4-7 冗長化設定編集画面(スタンバイ)

 冗長化設定については P60 を参照してください。

 同期パスワードおよびVRIDはマスター機で設定したものと同じ値を設定してください。

「適用」をクリックすると設定が反映されます。

 スタンバイ機の冗長化設定が完了するまでは、スタンバイ機を運用中のネットワークには設置しないでください。

5 スタンバイ機の設置

図4-8のスタンバイ機の位置に設置してください。

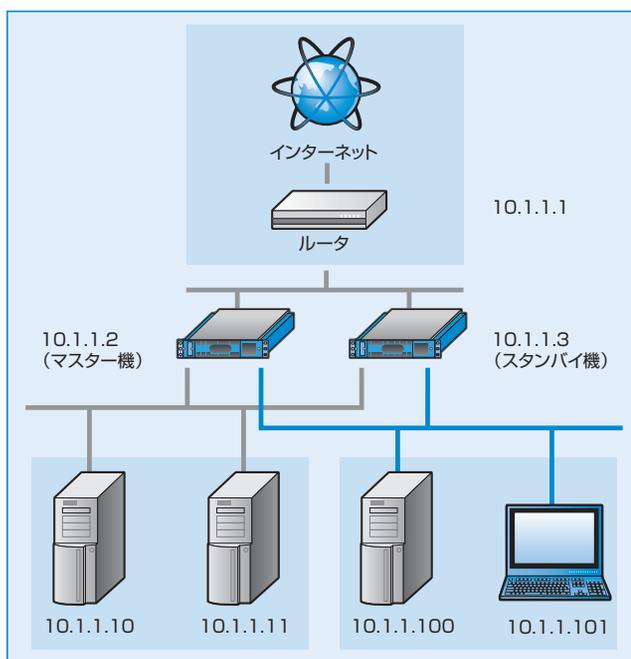


図4-8 Inside-Outside-DMZゾーンの冗長化構成

6 冗長化状態(同期)の確認

スタンバイ機を起動後、【冗長化設定】を確認し正常に冗長化されていることを確認してください。

役割	スタンバイ
現在の動作状態	待機中
設定情報同期状態	同期中

このように表示されていれば、冗長化構成の構築が完了となります。



図4-9 装置の状態表示画面

! 同期が完了しなかった場合

再起動後の状態が図4-10の状態の場合

役割	スタンバイ
現在の動作状態	待機中
設定情報同期状態	未同期



図4-10 装置の状態表示画面(未同期)

マスター機から情報の同期中という状態を表します。通常であれば、数分で同期処理が完了し、現在の動作状態は待機中に遷移します。しかし、しばらく待っても現在の動作状態が変更されない場合、以下の原因によって同期処理が正常に行われていないことが考えられます。

- マスター機およびスタンバイ機の冗長化設定が正しくない。
- パートナーIPアドレスにお互いのIPアドレスを設定していない。
- 同期パスワードが一致していない。
- VRIDが一致していない。
- ネットワーク内に重複したVRIDを設定している機器が存在する。

上記の点に注意して、再度両機の冗長化設定を確認してください。

3. 冗長化構成時の動作について

冗長化構成時のマスター機およびスタンバイ機がダウンした場合のフェイルオーバーの動作について説明します。図は、Inside-Outsideゾーンの場合ですが、DMZゾーンを使用した場合でも、同様に動作します。

■基本構成

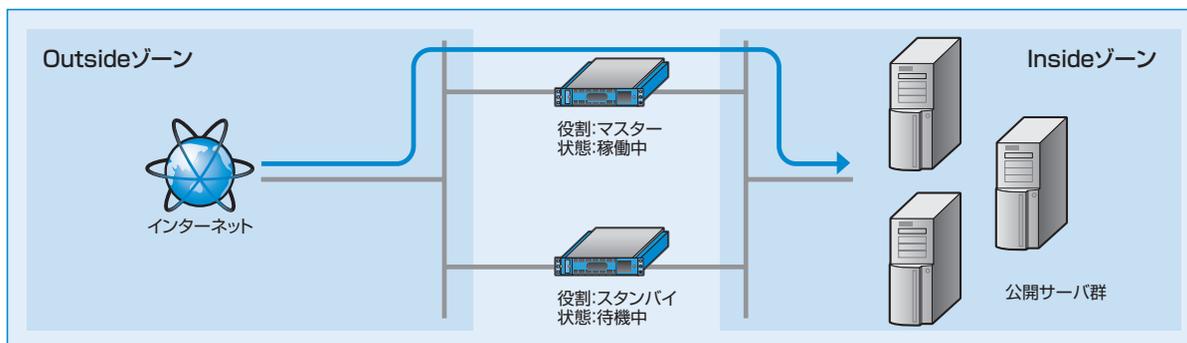


図4-11 基本構成

マスター機がダウンしたときの動作

マスター機がダウンした場合、ダウンしたことをスタンバイ機が自動的に検知し、スタンバイ機の動作状態が自動的に「稼働中」となり、動作を継続します。この動作を「フェイルオーバー」と呼びます（図4-12、図4-13）。

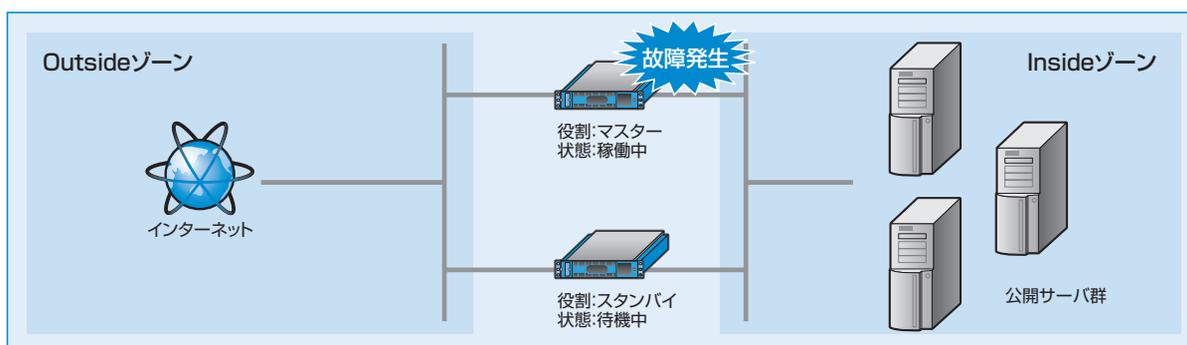


図4-12 マスター機で障害発生

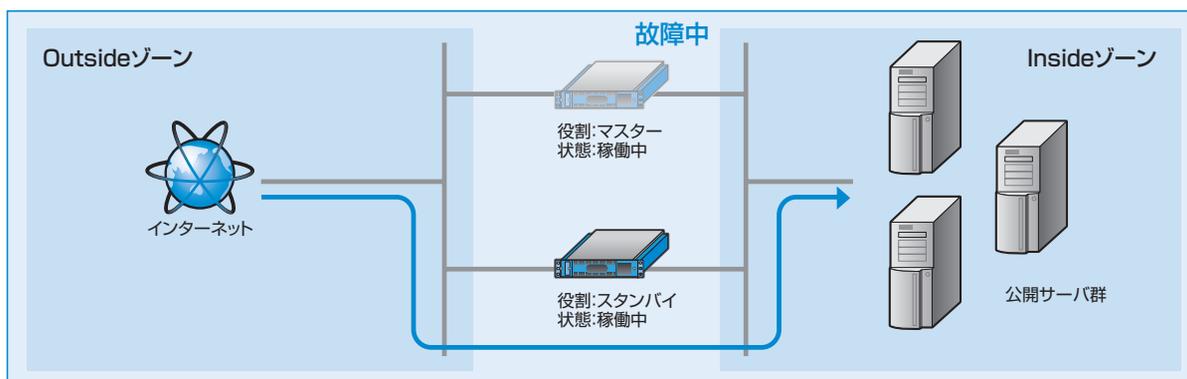


図4-13 フェイルオーバーが発生し、スタンバイ機で動作継続

マスター機が障害から復帰すると、再びスタンバイ機は「待機中」に遷移し、動作はマスター機で行われるようになります(図4-14、図4-15)。

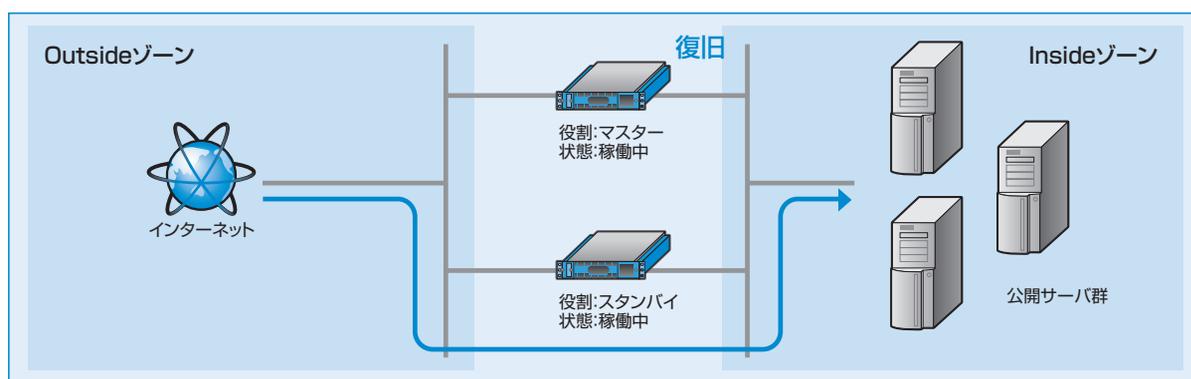


図4-14 マスター機が復帰

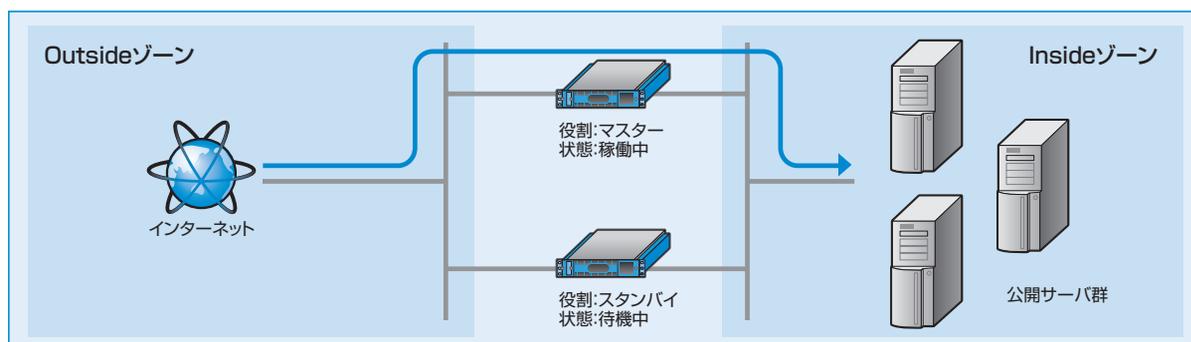


図4-15 再び通常構成で動作継続

スタンバイ機がダウンしたときの動作

スタンバイ機がダウンした場合、マスター機への影響はなく、引き続きマスター機で動作を継続します。スタンバイ機が復帰すると、自動的に基本構成にもどります(図4-16、図4-17)。

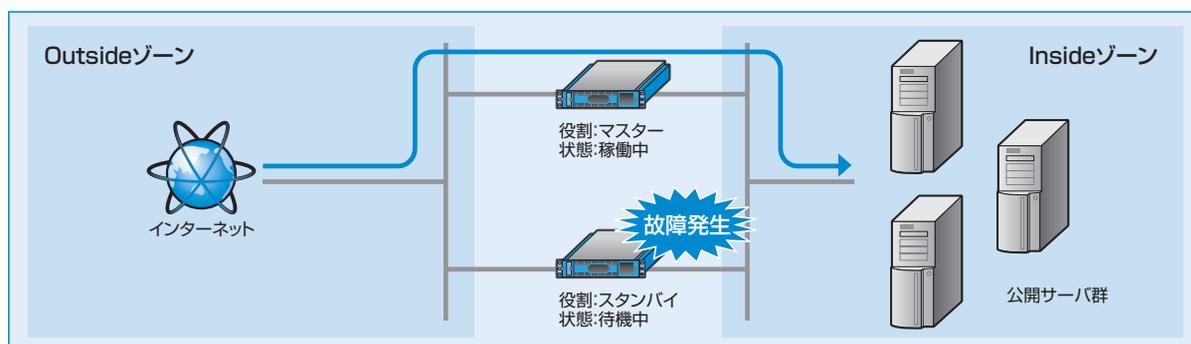


図4-16 スタンバイ機で障害が発生

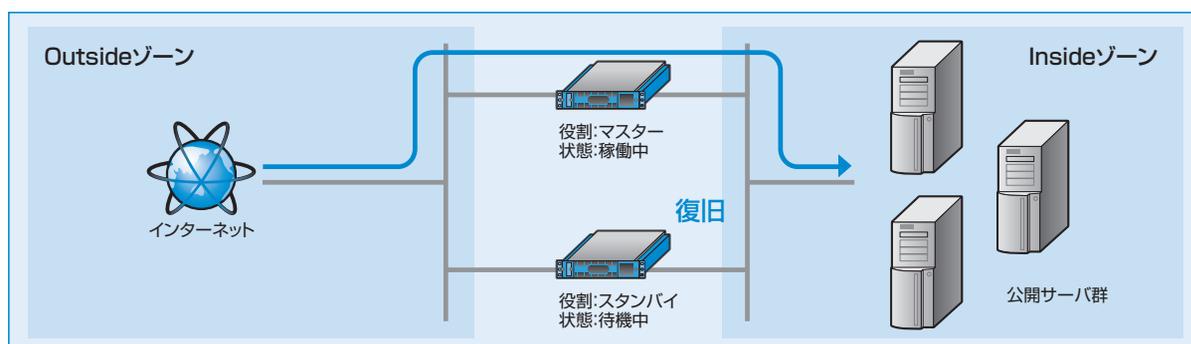


図4-17 スタンバイ機が復帰

プロモートについて

障害によりダウンしたマスター機がメンテナンスや部品交換などでただちに復旧できない場合、スタンバイ機で運用を継続する必要があります。

しかし、ポリシー変更はマスター機の管理インターフェイスからしか操作できないため、スタンバイ機のみではポリシー設定の変更はできません(図4-18)。ポリシー設定の変更を行う場合は、役割をスタンバイからマスターに昇格させる必要があります。この処理をプロモートと呼びます。

プロモートによってスタンバイ機の役割をマスターに昇格させることで、マスター機として運用管理を続行することができます(図4-19)。

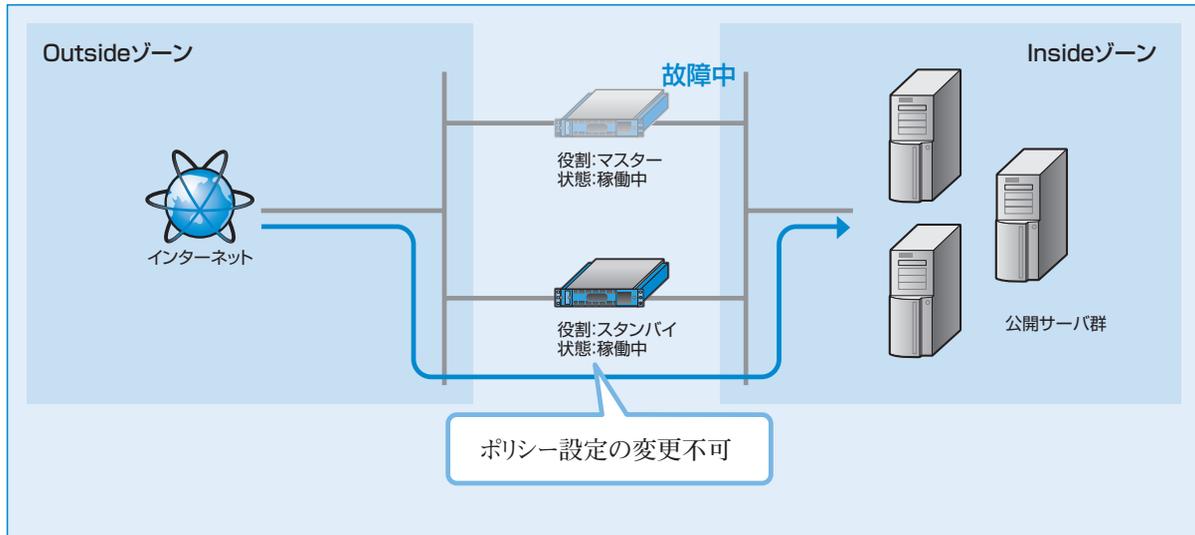


図4-18 スタンバイ機にフェイルオーバーした状況

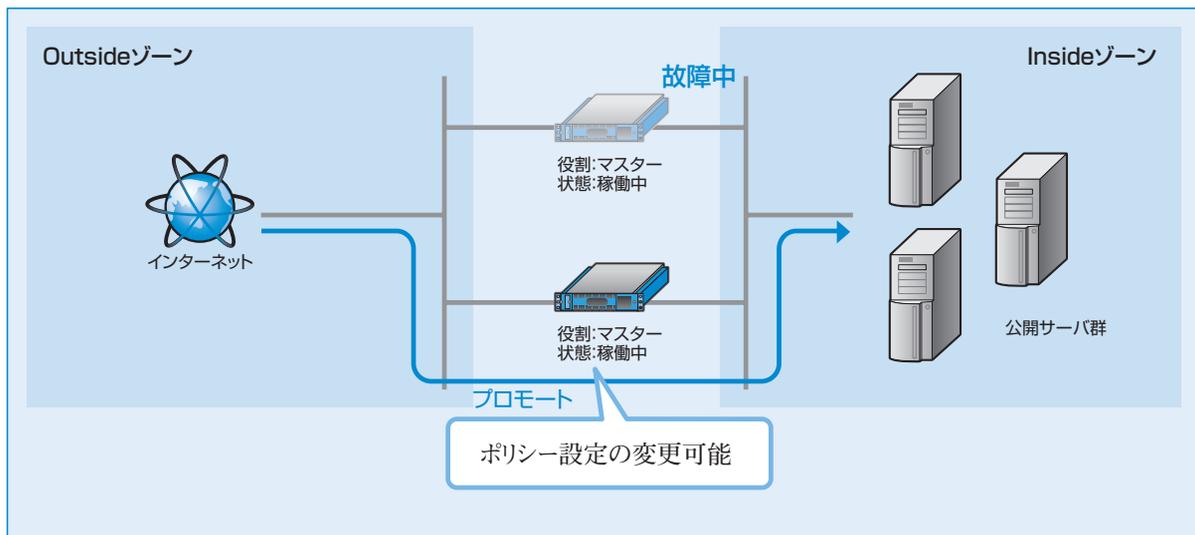


図4-19 プロモートにより、マスターに昇格

なお、プロモート操作を行うとスタンバイ機はマスター機に変更されます。故障していたマスター機をマスター機の設定のまま接続すると、マスター機が2台存在する状態となり冗長化構成が正常に動作しません(図4-20)。

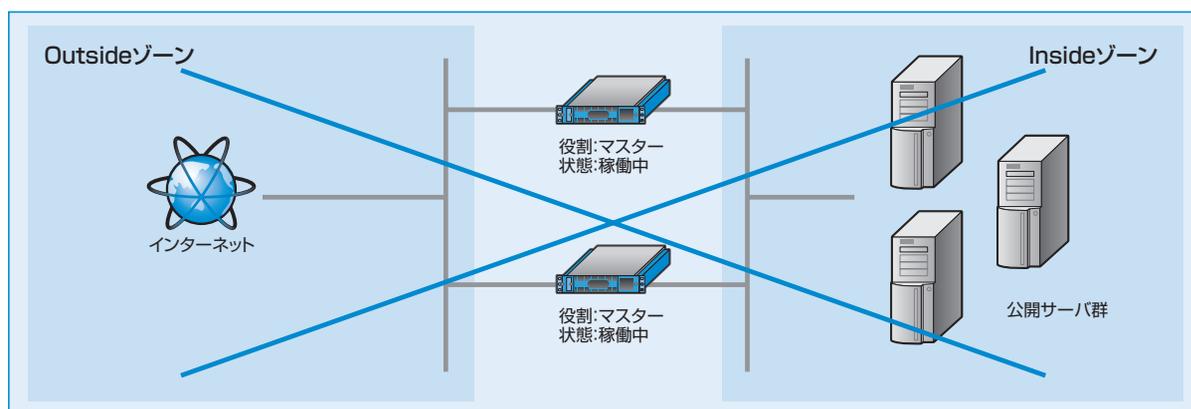


図4-20 誤った設置状態



プロモートを行いバックアップ機をマスター機に変更した場合は、役割を「スタンバイ」に設定した Secure Beagleを接続して冗長化構成を構築してください(図4-21)。自動的にマスター機の情報に同期し、それ以降、スタンバイ機として振舞います。

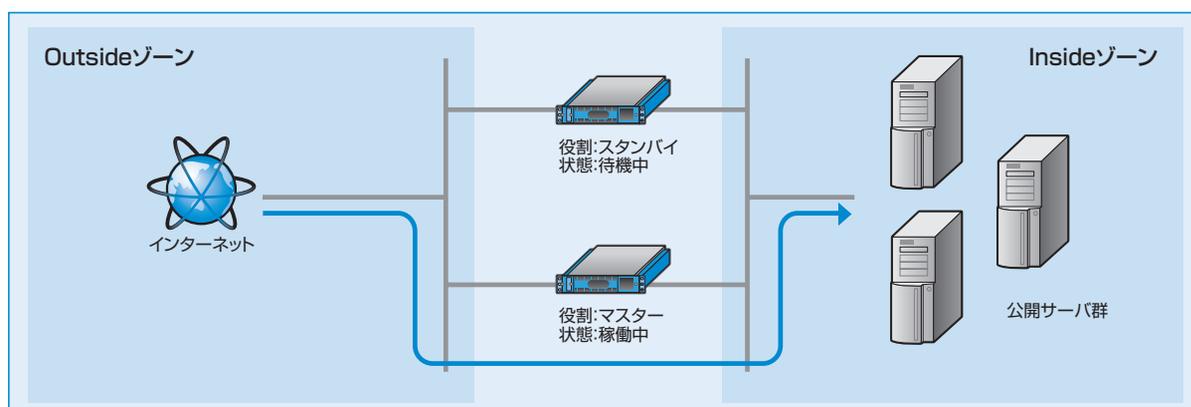


図4-21 スタンバイ機の設置

 Secure Beagleが自動的にスタンバイに降格することはありません。

 冗長化設定方法については P60 を参照してください。

プロモート実行手順

【基本設定】→【冗長化設定】にて冗長化設定画面を表示します(図4-22)。

役割がスタンバイ、現在の動作状態が稼働中のときのみ、プロモート実行ボタンが表示されます。

プロモート「実行」ボタンをクリックすると、即座に役割が【スタンバイ】→【マスター】に変更します(図4-23)。



プロモート操作ではSecure Beagleの再起動は必要ありません。また、サービスの停止も起こりません。

冗長化設定	
役割	スタンバイ
パートナーIPアドレス	10.1.1.2
同期パスワード	securebeaglesync
VRID	111
現在の動作状態	稼働中
設定情報同期状態	同期中 同期情報をクリアします
HA同期状態	未同期
編集	マスターに昇格します
実行	

図4-22 冗長化設定画面

冗長化設定	
役割	マスター
パートナーIPアドレス	10.1.1.2
同期パスワード	securebeaglesync
VRID	111
現在の動作状態	稼働中
HA同期状態	未同期
編集	

図4-23 プロモートによりマスターに昇格

第5章

運用管理

5

1. バックアップ・リストア手順	46
2. ファームウェアアップデート	47
3. GeolPデータベースアップデート	48
4. 通知設定	49

1. バックアップ・リストア手順

Secure Beagleで設定した設定情報をバックアップすることができます。また、バックアップファイルをリストアすることで以前の設定状態に戻すことができます。

バックアップ手順

- 1 【運用管理】→【バックアップ／リストア】を選択します(図5-1)。
- 2 「設定情報のバックアップ」の「実行」をクリックします。設定ファイルのダウンロードが開始されます(図5-1)。

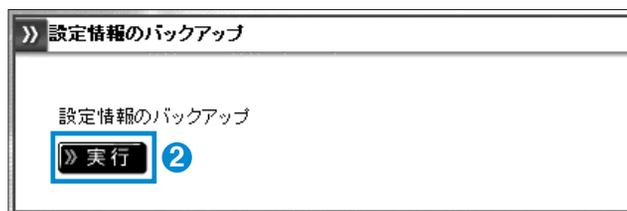


図5-1 設定情報のバックアップ

- ! ダウンロード手順はご使用のブラウザによって異なります。
- ! ダウンロードした設定ファイルをエディタなどで編集すると、正常にリストアできなくなります。そのため、設定ファイルの編集は行わないでください。

リストア手順

- 1 【運用管理】→【バックアップ／リストア】を選択します(図5-2)。
- 2 バックアップ手順にて取得した設定ファイル名を入力します。
または、「参照」をクリックすると、ディレクトリ一覧が表示されます。ここからバックアップファイルを選択します。



図5-2 設定情報のリストア

- 3 「実行」をクリックすると、設定情報のリストアが開始します。リストアに成功すると、リストアの成功および装置の再起動を促すメッセージが表示されます。
- 💡 リストアされた設定情報は再起動後に有効になります。
 - ! リストアに失敗した場合、以下の項目を確認してください。
 - 指定したファイルがバックアップ手順で取得したファイルかどうか。
 - 取得したファイルを編集していないか。

2. ファームウェアアップデート

Secure Beagleでは、機能追加や不具合対応によりファームウェアの提供を行うことがあります。最新のファームウェアは弊社ウェブページをご確認の上、入手してください。

<http://www.atworks.co.jp/store/>

! ファームウェアのアップデートを行う前に「設定情報のバックアップ」を実施し、設定情報を控えておいてください。

📖 「設定情報のバックアップ」については P46 を参照してください。

! ファームウェアのアップデート中は、管理画面の操作、ブラウザの操作を行わないでください。ファームウェアのアップデート失敗やSecure Beagle本製品の故障の原因となる場合があります。

ファームウェアバージョンの確認

Secure Beagleのファームウェアのバージョンは下記の手順で確認することができます(図5-3)。

【運用管理】→【ファームウェア】を選択してください。

ファームウェア	
モデル名	Secure Beagle Model 200
ファームウェアバージョン	1.08.00
GeolPバージョン	201306

図 5-3 バージョン表示画面

ファームウェアのアップデート手順

! 本手順はSecure Beagleの再起動が発生します。

① 弊社ウェブページより、更新するファームウェアをダウンロードしてください。

<http://online.atworks.co.jp>

② 【運用管理】→【ファームウェア】を選択してください。

③ 取得したファームウェアを入力してください。

または、「参照」をクリックすると、ディレクトリ一覧が表示されます。

ここからファームウェアを選択します。

④ ファームウェアを選択後、「実行」をクリックするとファームウェアのアップデートが開始されます(図5-4)。ファームウェアのアップデートに成功すると、自動的に再起動が実施されます。再起動後に再度「ファームウェアバージョンの確認」手順にてアップデートされたことを確認してください。

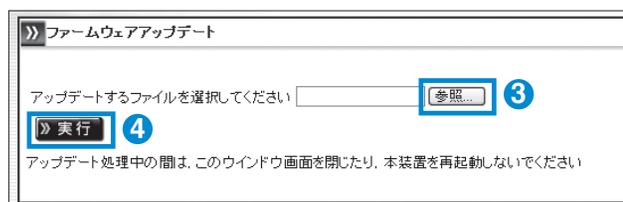


図 5-4 ファームウェアアップデート画面

3. GeoIPデータベースアップデート

GeoIPデータベースとは、各国への割り当てているIPアドレスの状況を管理しているデータベースです。Secure Beagleでは、このデータベースを基に国別のアクセス制御を行っています。IPアドレスは現在でも新規に割り当てられたり、割り当て先の国が変更になる場合もあります。このため正確な判定を行うためには、定期的にGeoIPデータベースを更新する必要があります。

Secure Beagle用GeoIPデータベースは弊社ウェブページより入手してください。

<http://www.atworks.co.jp/store/>



国別アクセスポリシーを行っていない場合は、GeoIPデータベースを更新する必要はありません。

GeoIPデータベースバージョンの確認

Secure BeagleのGeoIPデータベースのバージョンは【運用管理】→【ファームウェア】で確認することができます(図5-5)。

ファームウェア	
モデル名	Secure Beagle Model 200
ファームウェアバージョン	1.08.00
GeoIPバージョン	201306

図 5-5 バージョン表示画面

GeoIPデータベースバージョンのアップデートの手順

- 1 弊社ウェブページより、更新するファームウェアをダウンロードしてください。
- 2 【運用管理】→【ファームウェア】を選択してください。

- 3 手順①にて取得したデータベースファイルを入力してください。または、「参照」をクリックすると、ディレクトリ一覧が表示されます。ここからデータベースを選択します(図5-6)。

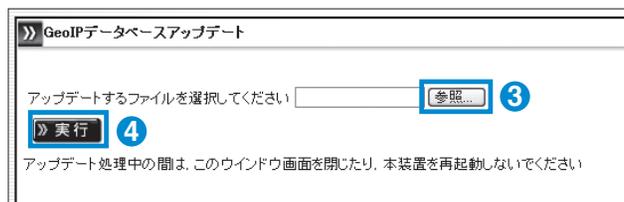


図 5-6 ファームウェアアップグレード画面

- 4 ファームウェアを選択後、「実行」をクリックするとデータベースのアップデートが開始されます。データベースのアップデート後に「GeoIPデータベースバージョンの確認」手順にてアップデートされたことを確認してください。



GeoIPデータベースアップデートではSecure Beagleの再起動は発生しません。

4. 通知設定

Secure Beagleでは、機器の状態や仮想サービスの状態を通知する手段として、以下の通知設定をサポートしています。

- メール通知
- SNMP
- Syslog

メール通知

Secure Beagleで検出したメッセージを管理者へメールで通知する機能です。

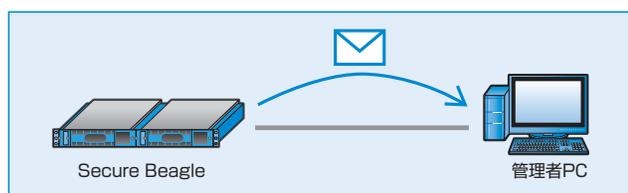


図5-7 メール通知

送信するメッセージは以下の内容です。

- Secure Beagle自身がマスター／スタンバイ状態で稼働開始したことの通知

メール通知設定手順

- ① 【通知設定】→【メール通知設定】を選択してください(図5-8)。

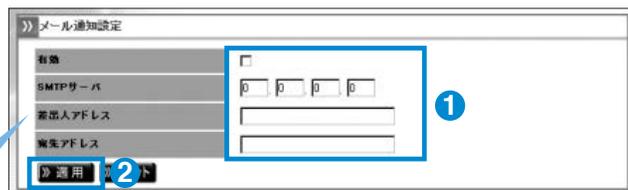


図5-8 メール通知設定

有効	チェックボックスにチェックをいれます。
SMTPサーバ	メールの送信に用いる SMTP サーバの IP アドレスを設定します。
差出人アドレス	通知メールの差出人メールアドレスを設定します。
宛先アドレス	通知メールの宛先メールアドレスを設定します。

- ② 上記の設定を行い、「適用」をクリックしてください。

設定した宛先アドレスにメールが通知されることを確認してください。

! SMTPサーバに指定するメールサーバでは、宛先アドレスに指定したメールを受信または中継する設定になっている必要があります。

📖 通知メールの内容については P87 の付録 B を参照してください。

SNMP

Secure BeagleをSNMPエージェントとして、MIB情報を通知する機能です。

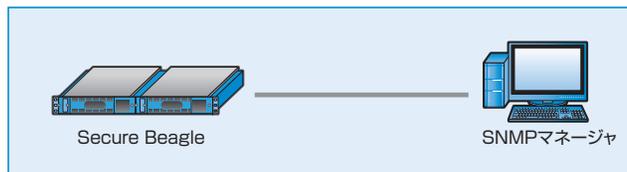


図5-9 SNMPマネージャとの通信

SNMP設定手順

Secure Beagleの設定

- 1 【通知設定】→【SNMP】を選択してください。

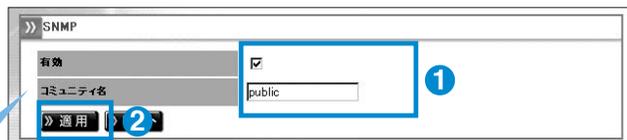


図5-10 SNMP設定画面

有効	チェックボックスにチェックをいれます。
コミュニティ名	コミュニティ名を設定します。

- 2 上記の設定を行い、「適用」をクリックしてください(図5-10)。

SNMP接続許可IPアドレスの設定

MIB情報の取得を許可するSNMPマネージャのIPアドレスを設定してください(図5-11)。

- ! 初期状態では、接続許可IPアドレスを追加しないと接続することはできません。

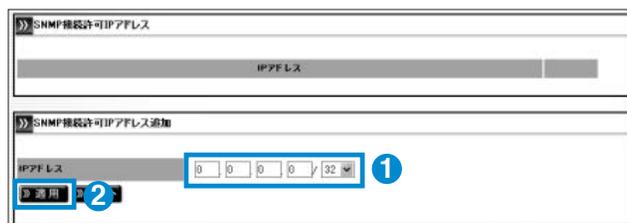


図5-11 SNMP接続許可IPアドレスの登録

SNMPマネージャの設定

SNMPマネージャソフトウェアにSecure Beagleに設定したコミュニティ名をSNMPマネージャソフトウェアに設定します。

Secure BeagleへのMIB取得を行い、MIB情報が取得できることを確認します。

- ! SNMPマネージャソフトウェアの使用方法については、各ソフトウェアのマニュアルを参照してください。

Syslog

Secure Beagleが出力するSyslogをSyslogサーバに転送する機能です。



パケットログの出力内容については P88 の付録 C を参照してください。

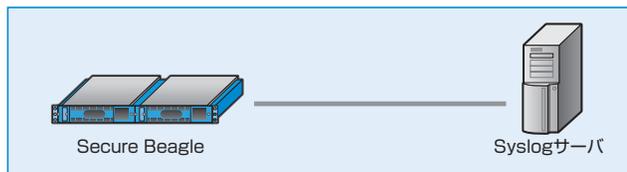


図5-12 Syslogサーバとの通信

Secure Beagleの設定

① 【通知設定】→【Syslog】を選択してください。

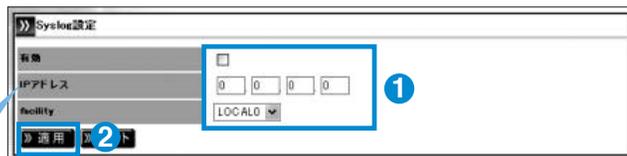


図5-13 Syslog設定画面

Syslogを有効にする場合

有効	チェックボックスにチェックをいれます。
IPアドレス	Syslogの転送先サーバを設定します。
facility	Syslogのfacilityを設定します。

② 上記の設定を行い、「適用」をクリックしてください(図5-13)。

Syslogサーバの設定

Syslogサーバにて、Secure BeagleのSyslogを受信できるよう設定してください。設定後、Secure BeagleからのSyslogが受信されていることを確認してください。



SyslogサーバにおけるSyslog設定については、SyslogサーバのOSもしくはソフトウェアのマニュアルを参照してください。

Syslog サービスの再起動

「実行」をクリックすると、Secure Beagle の Syslog サービスを再起動します(図 5-14)。



図 5-14 Syslog 再起動

5

運用管理

第6章

管理画面の機能説明

6

1. ログイン画面	54
2. 基本設定	57
3. アクセス制限	63
4. ファイアウォール	65
5. 通知設定	70
6. 運用管理	73

1. ログイン画面

1 Secure Beagleのログイン画面を表示します。

ブラウザにて以下の URI を入力します。

[https:// \[Secure BeagleのIPアドレス\]:18180](https://[Secure BeagleのIPアドレス]:18180)

2 Secure Beagleにログインします。

ログイン名・ログインパスワードを、入力してログインします。



パスワードを忘れた場合は、P81 を参照してください。

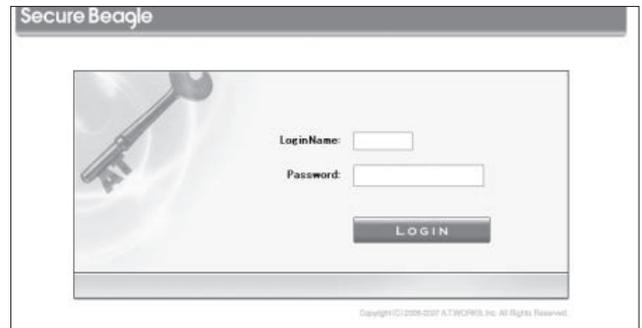


図6-1

ログインに成功すると、管理画面が表示されます。

装置状態

装置状態

GPU使用率	0%
MEM使用率	6%
総コネクション数	24
検知	HAを使用しない
現在の動作状態	-

Inside トラフィック

受信パケット数	送信パケット数	受信バイト数	送信バイト数
9921	3235	1553085	282979
受信パケット数/s	送信パケット数/s	受信バイト数/s	送信バイト数/s
4	1	452	115

Outside トラフィック

受信パケット数	送信パケット数	受信バイト数	送信バイト数
0	4746	0	320820
受信パケット数/s	送信パケット数/s	受信バイト数/s	送信バイト数/s
0	3	0	211

DMZ トラフィック

受信パケット数	送信パケット数	受信バイト数	送信バイト数
0	4684	0	318537
受信パケット数/s	送信パケット数/s	受信バイト数/s	送信バイト数/s
0	3	0	204

図6-2

■基本設定

① ネットワーク

Secure Beagleのネットワーク設定を表示・編集する場合に使用します。



② ルーティング設定

Secure Beagleのルーティング設定を表示・編集する場合に使用します。



③ 冗長化設定

Secure Beagleの冗長化設定を表示・編集する場合に使用します。



図6-3

■アクセス制限

④ パスワード変更

Secure Beagleの管理画面にログインするためのパスワードを変更する場合に使用します。



⑤ 接続許可IPアドレス

Secure Beagleの管理画面に接続を許可するIPアドレスの表示・変更する場合に使用します。

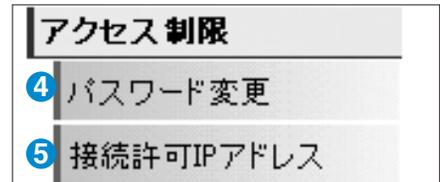


図6-4

■ファイアウォール

⑥ ポリシー

Secure Beagleのポリシーを表示・変更する場合に使用します。



図6-5

通知設定

7 Syslog

Secure BeagleのログをSyslogに転送する設定を表示・変更する場合に使用します。



P70

8 メール通知設定

Secure Beagleの状態をメールで通知する設定を表示・変更する場合に使用します。



P71

9 SNMP

Secure BeagleのSNMP設定を表示・変更する場合に使用します。



P71

運用管理

10 バックアップ／リストア

Secure Beagle の設定のバックアップとリストアを行う場合に使用します。



P73

11 状態

Secure Beagle の状態を表示します。



P74

12 ファームウェア

Secure Beagle のファームウェア情報の表示・アップデートを行う場合に使用します。



P76

13 サポート情報取得

サポート情報をダウンロードします。



P77

14 再起動

Secure Beagle の再起動を行う場合に使用します。



P77

15 設定初期化

Secure Beagle の設定を工場出荷時に初期化する場合に使用します。



P78

ログアウト

16 サポート情報追加

サポート情報を取得します。



図6-6



図 6-7



図6-8

2. 基本設定

ネットワーク

Secure Beagleのネットワーク設定を表示・編集する場合に使用します。

■ ネットワーク設定表示

ネットワーク設定表示	
ホスト名	securebeagle
IPアドレス	10.1.1.8/24
DNSサーバ	10.1.1.1
NTPサーバ	ntp.nict.jp
管理画面接続ポート	18180
レイヤ2プロトコルパススルー	許可
» 編集	

図6-9

- 1** ホスト名
Secure Beagleのホスト名を表示します。
- 2** IPアドレス
Secure BeagleのIPアドレスとプレフィックスを表示します。
- 3** DNSサーバ
Secure Beagleの参照するDNSサーバを表示します。
- 4** NTPサーバ
Secure Beagleの参照するNTPサーバを表示します。
- 5** 管理画面接続ポート
Secure Beagleの管理画面に接続するためのSSLポートを表示します。
- 6** レイヤ2プロトコルパススルー
レイヤ2プロトコルの通過設定を表示します。
- 7** 【編集】
Secure Beagleのネットワーク設定編集画面に移ります。



③、④の項目は、メール通知を使用する場合に必要となります。

■ネットワーク設定編集

ネットワーク設定編集

1 ホスト名 securebeagle

2 IPアドレス 10 1 1 8 / 24

3 DNSサーバ 10 1 1 1

4 NTPサーバ ntp.nict.jp

5 管理画面接続ポート 18180

6 レイヤ2プロトコルパススルー 許可

7 適用 8 リセット

図6-10

1 ホスト名

Secure Beagleのホスト名を設定します。

2 IPアドレス

Secure BeagleのIPアドレスとプレフィックスを設定します。

3 DNSサーバ

Secure Beagleの参照するDNSサーバを設定します。

4 NTPサーバ

Secure Beagleの参照するNTPサーバを設定します。

5 管理画面接続ポート

Secure Beagleの管理画面に接続するためのSSLポートを表示します。

6 レイヤ2プロトコルパススルー

レイヤ2プロトコルを設定します。

許可した場合	全てのレイヤ2プロトコルの通過を許可します。
許可しない場合	ipv4以外のレイヤ2プロトコルの通過を拒否します。

7 【適用】

Secure Beagleに設定を適用します。

8 【リセット】

変更内容を破棄します。

ルーティング

Secure Beagleのルーティング設定の表示・変更する場合に使用します。

■ルーティング

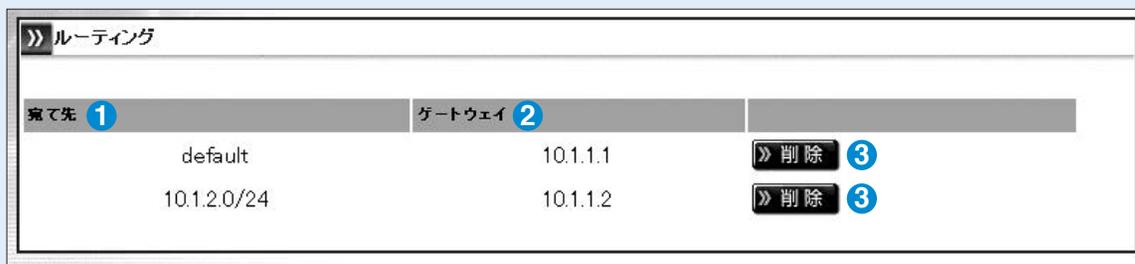


図6-11

① 宛て先

パケットの宛て先のネットワークを表示します。

② ゲートウェイ

パケットを「宛て先」のネットワークへ配送する際の中継機器のIPアドレスを表示します。
デフォルトゲートウェイの場合、宛て先は「default」と表示されます。

③ 【削除】

対象のルーティング設定を削除します。

■ルート追加

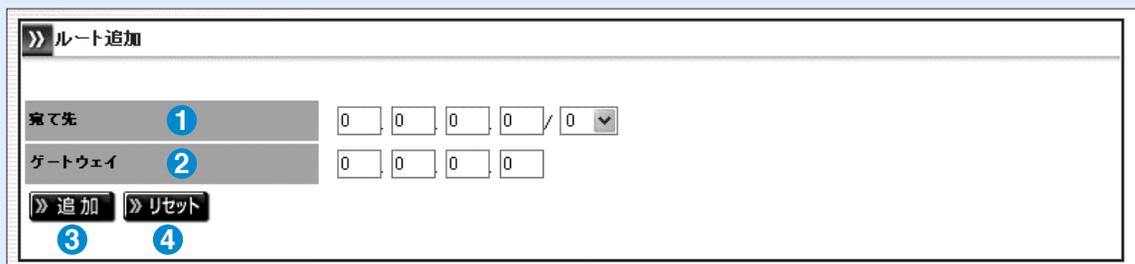


図6-12

① 宛て先

パケット宛て先ネットワークアドレスを入力します。
デフォルトゲートウェイの場合は、「0.0.0.0/0」を入力します。

② ゲートウェイ

「宛て先」に入力したパケットを転送するIPアドレスを入力します。
Secure Beagleに設定しているIPアドレスと同一のネットワークアドレスを指定する必要があります。

③ 【追加】

入力した内容ルーティングテーブルに追加します。

④ 【リセット】

入力内容を破棄します。

冗長化設定

Secure Beagleの冗長化設定を表示・編集する場合に使用します。

冗長化設定の表示



図6-13

1 役割

Secure Beagleの現在の役割を表示します。HAを使用しない、マスター、スタンバイのいずれかとなります。

2 パートナーIPアドレス

パートナー機のIPアドレスを表示します。

3 同期パスワード

パートナー機と情報を同期するためのパスワードを表示します。

4 VRID

VRRPで使用するVRIDを表示します。

5 現在の動作状態

Secure Beagleの現在の動作状態を表示します。稼働中、待機中のいずれかとなります。

6 HA同期状態

パートナー機との同期状態を表示します。同期中、未同期のいずれかとなります。

7 【編集】

Secure Beagleの役割の変更画面に移ります。

■現在の動作状態が待機中の場合



図6-14

8 同期情報をクリアします【実行】

マスターとの同期情報をクリアします。クリアを行うとマスター機から同期情報が再送されます。マスター機が変更になった場合など、強制的にスタンバイ機の同期情報を更新する場合に使用します。

■役割がスタンバイの場合



図6-15

9 マスターに昇格します【実行】

Secure Beagleの役割をバックアップからマスターに変更します。元のマスターであったパートナー機については、手動で役割をスタンバイに変更してください。

冗長化設定の編集

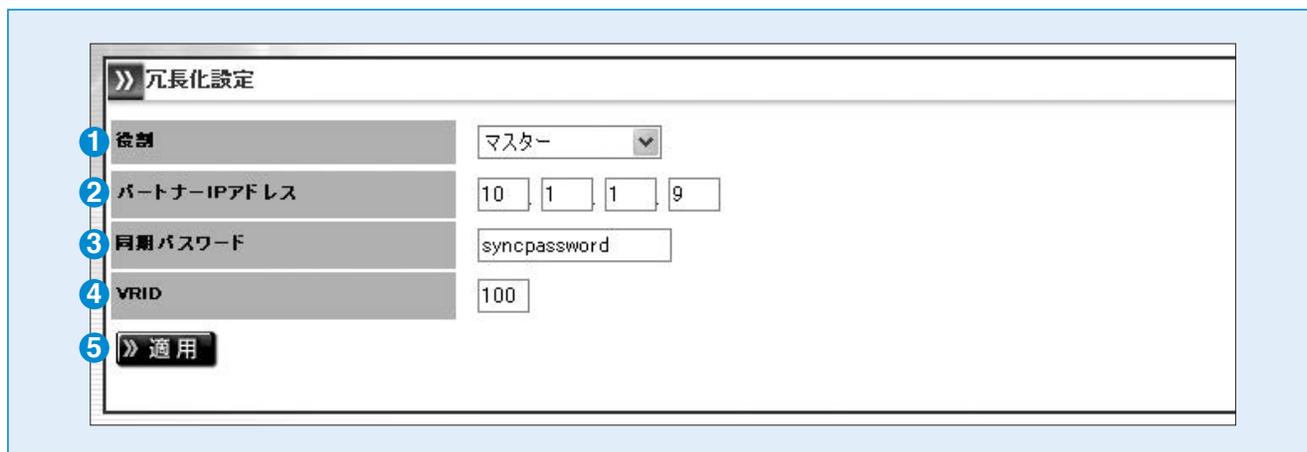


図6-16

1 役割

Secure Beagleの現在の役割を変更します。HAを使用しない、マスター、スタンバイのいずれかとなります。

マスターおよびスタンバイの場合はさらにパートナーIPアドレス、同期パスワード、VRIDを設定します。

2 パートナーIPアドレス

パートナー機のIPアドレスを変更します。

Secure Beagleがマスター機の場合は同期対象のスタンバイ機のIPアドレスを、Secure Beagleがスタンバイ機の場合は同期対象のマスター機のIPアドレスを入力してください。

3 同期パスワード

パートナー機と情報を同期するためのパスワードを変更します。

マスター機とスタンバイ機で同じパスワードを入力してください。



同期パスワードは、第三者に推測されにくい、独自の文字列を設定してください。
同期パスワードには、半角英数字のみ使用可能です。

4 VRID

VRRPで使用するVRIDを変更します。

マスター機とスタンバイ機で同じVRIDを入力してください。



VRIDは1から255までの整数を設定することができます。冗長化構成を行う機器同士には同じ値を設定します。同一ネットワーク内の機器にVRRPを使用する機器がある場合には、設定されているVRIDを調査の上、重複しないように設定してください。同一ネットワーク内に、冗長化構成の別のSecure Beagleを設置する場合にもVRIDが重複しないように設定してください。

5 【適用】

Secure Beagleに設定を適用します。設定を有効にするには再起動を行う必要があります。

3. アクセス制限

パスワード変更

Secure Beagleの管理画面にログインするためのパスワードを変更する場合に使用します。

Figure 6-17 shows a web form for changing a password. The form is titled 'パスワード変更' (Change Password). It contains four numbered steps: 1. '旧パスワード' (Old Password) with an input field; 2. '新パスワード' (New Password) with an input field; 3. '新パスワード(再入力)' (New Password (Re-entry)) with an input field; and 4. '適用' (Apply) button.

図6-17

- 1 旧パスワード**
現在のパスワードを入力します。パスワードが一致しなければ変更できません。
- 2 新パスワード**
新しいパスワードを入力します。
- 3 新パスワード(再入力)**
新しいパスワードを再入力します。
新パスワードと再入力したパスワードが一致しなければ変更できません。
- 4 【適用】**
Secure Beagleにパスワードの変更を適用します。

接続許可IPアドレス

Secure Beagleの管理画面に接続を許可するIPアドレスの表示・変更する場合に使用します。



工場出荷時はどのIPアドレスからも管理画面へ接続を許可する状態です。

■接続許可IPアドレス

Secure Beagleの管理画面に接続を許可するIPアドレスを表示します。

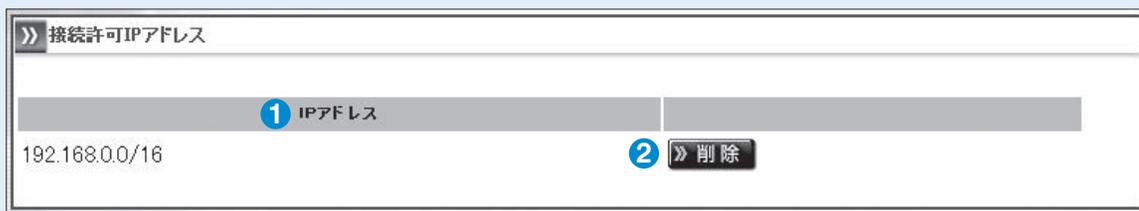


図6-18

① IPアドレス

管理画面に接続を許可するIPアドレスとプレフィックスを表示します。

② 【削除】

管理画面に接続を許可するIPアドレスを削除します。

■接続許可IPアドレス追加

Secure Beagleの管理画面に接続を許可するIPアドレスを追加します。



図6-19

① IPアドレス

追加するIPアドレスとプレフィックスを指定します。

② 【追加】

Secure Beagleの管理画面に接続を許可するIPアドレスを追加します。



設定はただちに反映されます。

③ 【リセット】

変更内容を破棄します。

4. ファイアウォール

ポリシー

Secure Beagleのポリシーの編集およびポリシーリストを表示する場合に使用します。

ゾーン

各ゾーン間のポリシーを抽出することができます。

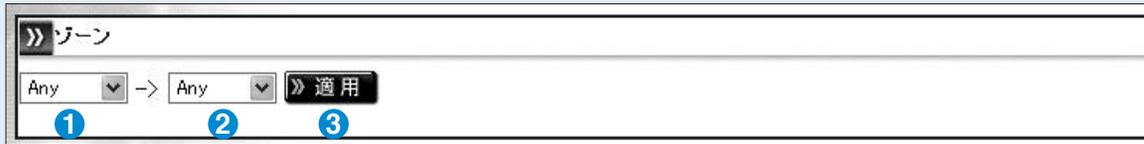


図6-20

- ① パケットの転送元ゾーンを「Any」、「Inside」、「Outside」、「DMZ」から選択します。
- ② パケットの転送先ゾーンを「Any」、「Inside」、「Outside」、「DMZ」から選択します。
- 💡 「Any」を選択した場合は、全てのゾーンを選択したこととなります。
「Any」→「Any」を選択した場合は全てのゾーン間のポリシーが表示されます。
- ③ 【適用】
指定したゾーン間のポリシーリストを抽出して一覧を表示します。

■ポリシーリスト



図6-21

1 送信元

対象ポリシーの送信元を表示します。

2 送信先

対象ポリシーの送信先を表示します。



国指定した場合は先頭にc:という記号が付加されます。

NOT指定した場合は先頭に~記号が付加されます。

対象が制限されていない場合、「any」と表示されます。

3 プロトコル

対象ポリシーのプロトコルを表示します。

ip, tcp, udp, icmp, igmp, ipip, gre, l2tpのいずれかとなります。



プロトコル指定されていない場合、「ip」と表示されます。

4 詳細

プロトコルの詳細な情報が表示されます。

sport:	プロトコルで「tcp」を選択した場合の送信元ポート番号です。
dport:	プロトコルで「tcp」を選択した場合の送信先ポート番号です。
type:	プロトコルで「icmp」を選択した場合のICMPタイプです。

5 動作

対象ポリシーの動作を表示します。

許可、拒否、RSTパケット送信、送信元接続制限のいずれかとなります。



送信元接続制限は、接続元IPアドレスによる同時接続数制限をしていることを表します。

6 ログ

対象ポリシーのログ設定を表示します。

ログ設定を行っている場合、DEBUG、INFO、NOTICE、WARNING、ERR、CRIT、ALERT、EMERG、のいずれかが表示されます。

7 【追加】

対象ゾーンに新規ポリシーを追加します。

8 【インポート】

対象ゾーンにポリシーをインポートします。

9 【エクスポート】

対象ゾーンのポリシーをエクスポートします。

10 【削除】

対象ポリシーを削除します。

11 【編集】

対象ポリシーを修正します。

12 【^】

対象ポリシーの優先度を上げます。

13 【v】

対象ポリシーの優先度を下げます。



ポリシー優先度の変更を行うと直ちに有効になります。

ポリシー追加

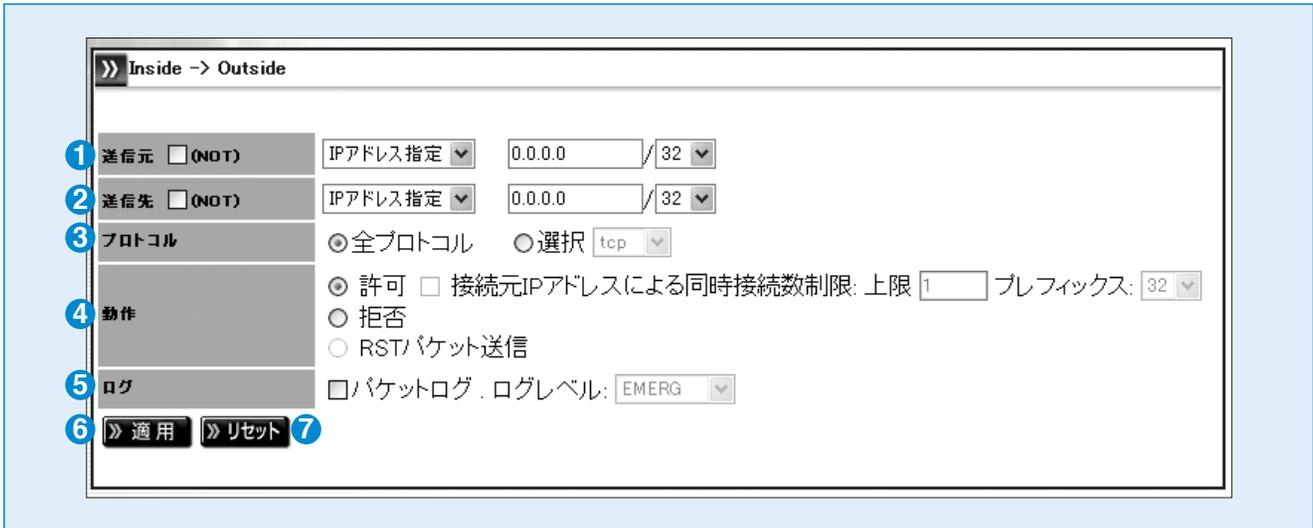


図6-22

1 送信元

パケットの送信元を指定します。

2 送信先

パケットの送信先を指定します。



送信元および送信先は「IPアドレス指定」と「国指定」から指定可能です。

○IPアドレス指定:チェックボックスを「IPアドレス指定」としIPアドレスまたはネットワークアドレスを入力します(図6-23)。指定したIPアドレス以外を対象とする場合は、NOTチェックボックスをチェックします。

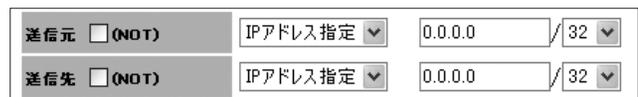


図6-23

○国指定:チェックボックスを「国指定」とし国名を入力します(図6-24)。指定した国以外を対象とする場合は、NOTチェックボックスをチェックします。



図6-24



「国指定」とした場合、Editボタンをクリックすることで、国指定補助画面が表示されます。この画面を利用することで簡単に対象の国を選択することができます(図6-25)。

1 【削除】

対象の国を削除します。

3 【適用】

設定した内容を適用します。

2 【追加】

指定した国を追加します。

4 【キャンセル】

設定内容を破棄し、ポリシー追加画面に戻ります。



「国指定」では、本体に登録されている、GeoIPデータベースによって国名とIPアドレスの対応を管理しています。IPアドレスの各国への割り当ては更新されるのでGeoIPデータベースのアップデートを定期的実施してください。



図6-25



GeoIP データベースのアップデートは P48 を参照してください。

③ プロトコル

対象のプロトコルを指定します。

プロトコルはtcp、udp、icmp、igmp、ipip、gre、l2tpから選択可能です。

全プロトコルを指定した場合は、プロトコル指定を行いません。

○tcp、udpを選択した場合、ポート番号を指定する必要があります(図6-27)。

指定したポート番号以外を対象とする場合は、NOTチェックボックスをチェックします。

① 送信元ポート

送信元のポート番号を指定します

② 送信先ポート

送信先のポート番号を指定します。

③ [Edit]

ポート指定補助画面を表示します。



Editボタンをクリックすることで、ポート番号指定補助画面が表示されます。

この画面を利用することで簡単にポート番号を選択することができます(図6-27)。

① 【削除】

追加したポート番号を削除します。

② 【追加】

サービス名からポート番号を追加します。

③ 【追加】

範囲指定でポート番号を追加します。

④ 【適用】

設定した内容を適用します。

⑤ 【キャンセル】

設定内容を破棄し、ポリシー追加画面に戻ります。

プロトコル	<input type="radio"/> 全プロトコル	<input checked="" type="radio"/> 選択	tcp
① 送信元ポート	<input type="checkbox"/> (NOT)	0	Edit
② 送信先ポート	<input type="checkbox"/> (NOT)	0	Edit

図6-26

① >> 削除

サービス名による指定

② >> 追加

or

番号による指定

~

③ >> 追加

④ >> 適用

⑤ >> キャンセル

図6-27

○icmpを選択した場合、ICMPタイプを指定する必要があります(図6-28)。

ICMPタイプを指定する必要がない場合、「any」を選択します。

プロトコル	<input type="radio"/> 全プロトコル	<input checked="" type="radio"/> 選択	icmp
icmpタイプ	any		

図6-28

ICMPタイプ	ICMPタイプを指定します。
---------	----------------

4 動作

「送信元」「送信先」「プロトコル」で指定したパケットに対する動作を設定します。

パケットの通過を許可する場合は「許可」を選択します。

パケットの通過を拒否する場合は「拒否」を選択します。



プロトコルにてtcp指定を行った場合、RSTパケット送信を選択することができます。

この場合パケットは通過せず、接続元にRSTパケットを送信します。



プロトコルにてtcp指定を行い、動作を許可した場合、接続制限をすることができます(図6-29)。

図6-29

① 接続元IPアドレスによる同時接続制限

同時接続制限を行う場合は、このチェックボックスにチェックをいれます。

② 上限

同時接続数の上限を指定します。

③ ネットマスク

同時接続のネットワーク単位を指定します。

5 ログ

対象ポリシーに該当するパケットログを取得することができます。

パケットログ	取得する場合、チェックボックスにチェックをいれます。
ログレベル	ログのpriorityを指定します。



ログを取得するにはSyslog設定を有効にする必要があります。



Syslog 設定については P51 を参照してください。

6 【適用】

変更内容を適用します。

7 【リセット】

変更内容を破棄します。

5. 通知設定

Syslog

Secure BeagleのログをSyslogに転送する設定を表示・変更する場合に使用します。

Syslog設定

The screenshot shows a web-based configuration page for Syslog. The title is 'Syslog設定'. There are five numbered callouts: 1 points to the '有効' checkbox, 2 points to the 'IPアドレス' field (which contains four '0' characters), 3 points to the 'facility' dropdown menu (set to 'LOCAL0'), 4 points to the '適用' button, and 5 points to the 'リセット' button.

図6-30

- 1 有効**
Secure BeagleのログをSyslogサーバに転送するには、このチェックボックスにチェックを入れます。
- 2 IPアドレス**
Secure Beagleのログの転送先SyslogサーバのIPアドレスを設定します。
- 3 facility**
Secure Beagleのログのfacilityを設定します。
- 4 【適用】**
Secure Beagleに設定を適用します。
- 5 【リセット】**
変更内容を破棄します。

Syslog再起動

The screenshot shows a web-based configuration page for restarting Syslog. The title is 'Syslog再起動'. There is one numbered callout: 1 points to the '実行' button.

図 6-31

- 1 【実行】**
Secure Beagle の Syslog サービスを再起動します。

メール通知設定

Secure Beagleの状態をメールで通知する設定を表示・変更する場合に使用します。

■メール通知設定

1 有効

2 SMTPサーバ 10 1 1 1

3 差出人アドレス securebeagle@example.co.jp

4 宛先アドレス admin@example.co.jp

5 適用 リセット 6

図 6-32

1 有効

メールによる状態の通知を行うには、このチェックボックスにチェックを入れます。

2 SMTPサーバ

メールの送信に用いるSMTPサーバのIPアドレスを設定します。

3 差出人アドレス

通知メールの差出人メールアドレスを設定します。

4 宛先アドレス

通知メールの宛先メールアドレスを設定します。

5 【適用】

Secure Beagleに設定を適用します。

6 【リセット】

変更内容を破棄します。

SNMP

Secure BeagleのSNMP設定を表示・変更する場合に使用します。

■SNMP

1 有効

2 コミュニティ名 public

3 適用 リセット 4

図 6-33

1 有効

Secure BeagleのSNMPを有効にするには、このチェックボックスにチェックを入れます。

2 コミュニティ名

SNMPのコミュニティ名を設定します。

3 【適用】

Secure Beagleに設定を適用します。

4 【リセット】

変更内容を破棄します。

■SNMP接続許可IPアドレス

SNMPに接続を許可するIPアドレスを表示します。



図 6-34

① IPアドレス

SNMPに接続を許可するIPアドレスとプレフィックスを表示します。

② 【削除】

SNMPに接続を許可するIPアドレスを削除します。

■SNMP接続許可IPアドレス追加

SNMP に接続を許可するIPアドレスを追加します。

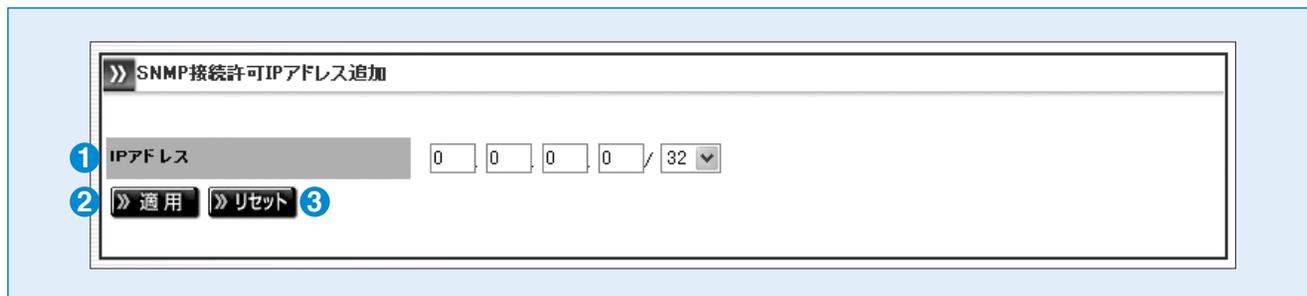


図 6-35

① IPアドレス

追加するIPアドレスとプレフィックスを指定します。

② 【適用】

SNMPに接続を許可するIPアドレスを追加します。



設定はただちに反映されます。

③ 【リセット】

変更内容を破棄します。

6. 運用管理

バックアップ／リストア

Secure Beagleの設定のバックアップとリストアを行う場合に使用します。

■設定情報のバックアップ

Secure Beagleの設定情報をバックアップします。

「実行」ボタンをクリックすると、Secure Beagleの設定情報がダウンロードできます。



図 6-36

①【実行】

Secure Beagleの設定情報をバックアップします。

■設定情報のリストア

バックアップしたSecure Beagleの設定情報をリストアします。

「参照」ボタンをクリックし、Secure Beagleの設定情報のバックアップファイルを指定します。

「実行」ボタンをクリックすると、指定したバックアップファイルを用いて、Secure Beagleの設定情報がリストアできます。

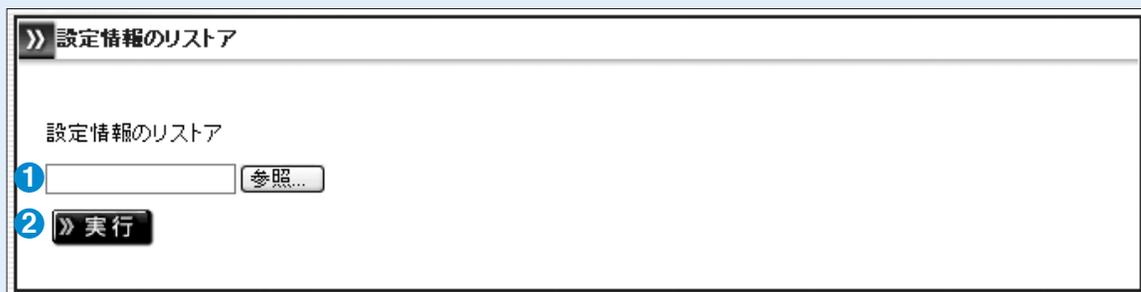


図 6-37

①【参照】

Secure Beagleの設定情報のバックアップファイルを指定します。

②【実行】

Secure Beagleの設定情報をリストアします。

状態

Secure Beagleの状態を表示します。

装置の状態

Secure Beagleのシステム情報を表示します。

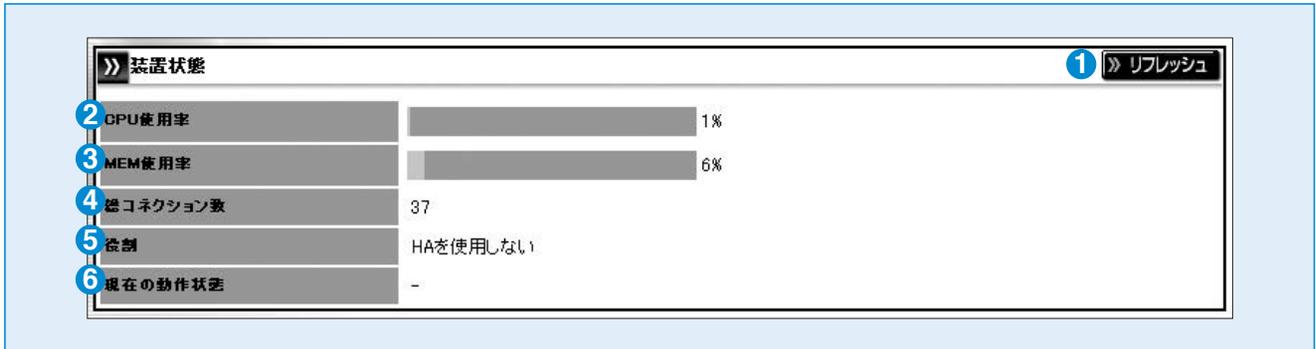


図 6-38

トラフィック (Insideゾーン)

Insideゾーンのネットワークトラフィック情報を表示します。



図 6-39

トラフィック (Outsideゾーン)

Outsideゾーンのネットワークトラフィック情報を表示します。



図 6-40

トラフィック (DMZゾーン)

DMZゾーンのネットワークトラフィック情報を表示します。



図 6-41

1 【リフレッシュ】

本画面の表示を更新します。

2 CPU使用率

Secure BeagleのCPU使用率を表示します。単位は%です。

3 MEM使用率

Secure Beagleのメモリ使用率を表示します。単位は%です。

4 総コネクション数

Secure Beagleが通信中のコネクション数を表示します。

5 役割

Secure Beagleの現在の役割を表示します。

HAを使用しない、マスター、スタンバイのいずれかとなります。

6 現在の動作状態

Web Beagleの現在の動作状態を表示します。

稼働中、待機中のいずれかとなります。HAを使用しない場合は「-」が表示されます。

7 【リフレッシュ】

本画面の表示を更新します。

8 各ゾーンの通信状態

各ゾーン(Inside、Outside、DMZ)のネットワークの状態を表示します。

UPの場合、対象ゾーンのネットワークが有効であり、DOWNの場合、無効であることを表します。

9 受信パケット数

受信したパケット数の合計を表示します。

10 送信パケット数

送信したパケット数の合計を表示します。

11 受信バイト数

受信したバイト数の合計を表示します。

12 送信バイト数

送信したバイト数の合計を表示します。

13 受信パケット数/s

受信したパケット数の1秒あたりの平均値を表示します。

14 送信パケット数/s

送信したパケット数の1秒あたりの平均値を表示します。

15 受信バイト数/s

受信したバイト数の1秒あたりの平均値を表示します。

16 送信バイト数/s

送信したバイト数の1秒あたりの平均値を表示します。

ファームウェア

Secure Beagleのファームウェア情報の表示・アップデートを行う場合に使用します。

■バージョン情報



ファームウェア	
モデル名	Secure Beagle Model 200
ファームウェアバージョン	1.08.00
GeolPバージョン	201306

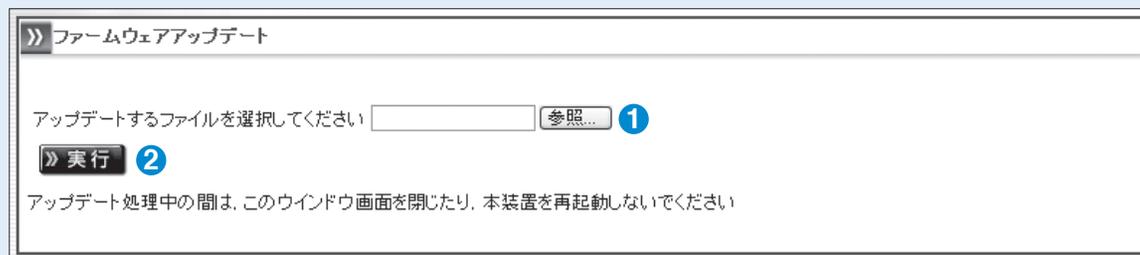
図 6-42

- 1 モデル名
Secure Beagle のモデル名を表示します。
- 2 ファームウェアバージョン
Secure Beagle のファームウェアのバージョンを表示します。
- 3 GeolP データベース
GeolP データベースのバージョンを表示します。

■ファームウェアアップデート

Secure Beagleのファームウェアをアップデートします。

! アップデート処理中は、ブラウザを閉じたり、Secure Beagleを再起動しないでください。



ファームウェアアップデート

アップデートするファイルを選択してください 参照... 1

実行 2

アップデート処理中の間は、このウィンドウ画面を閉じたり、本装置を再起動しないでください

図 6-43

- 1 【参照】
Secure Beagleのファームウェアファイルを指定します。
- 2 【実行】
Secure Beagleのファームウェアの更新を行います。

■GeoIPデータベースのアップデート

GeoIPデータベースをアップデートします。

アップデート処理中は、ブラウザを閉じたり、本機を再起動しないでください。

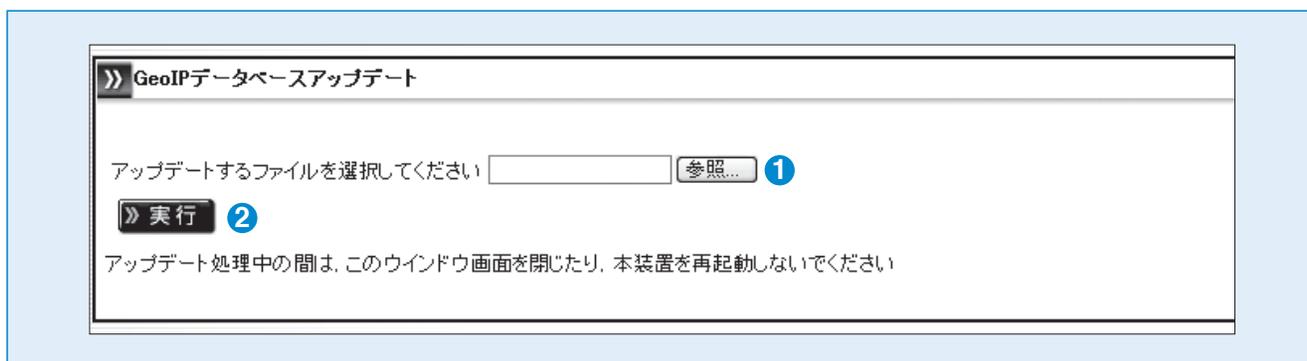


図 6-44

①【参照】

GeoIPデータベースファイルを指定します。

②【実行】

GeoIPデータベースの更新を行います。

サポート情報取得

サポート情報をダウンロードする場合に使用します。

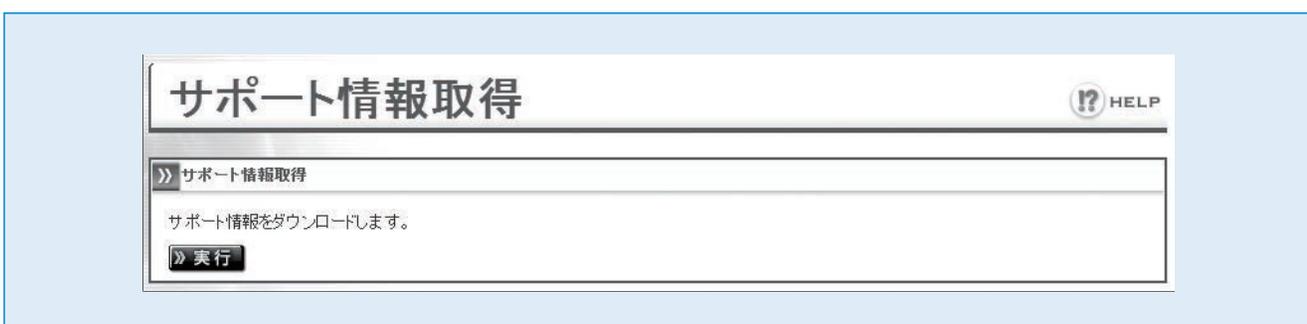


図 6-45

①【実行】

サポート情報のダウンロードを行います。

再起動

Secure Beagleの再起動を行う場合に使用します。

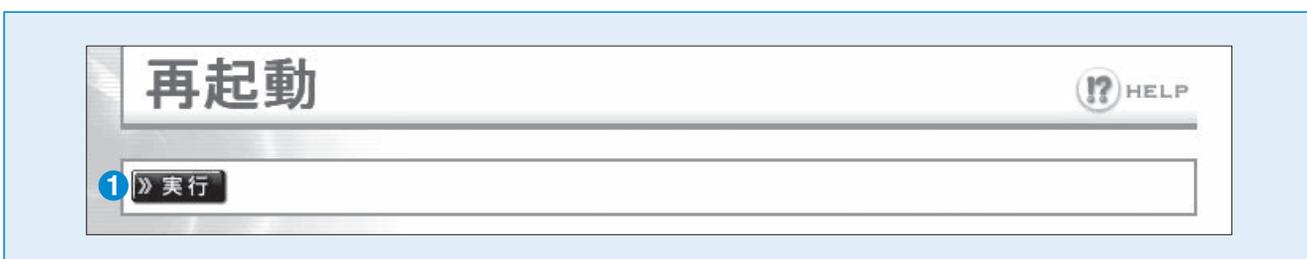


図 6-46

①【実行】

Secure Beagleの再起動を行います。

設定初期化

Secure Beagleの設定を工場出荷設定に初期化する場合に使用します。

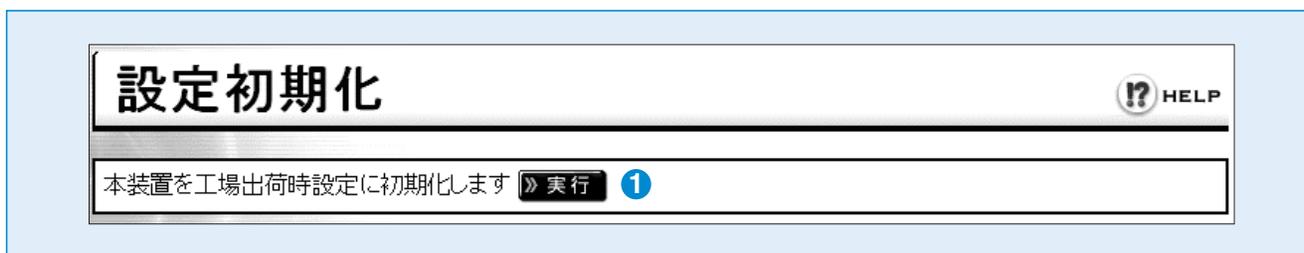


図 6-47

①【実行】

Secure Beagleを工場出荷時設定に初期化します。

第7章

コンソール管理

1. コンソール管理

80

7

1. コンソール管理

Secure Beagleのコンソール管理画面をお使いいただくための手順を説明します。

Secure Beagleにモニタ、キーボードを接続してください。



Secure Beagle のフロントパネルについては P6、P7、P8 を参照してください。

Secure Beagleのコンセントを電源に接続し、電源スイッチを押下します。

モニタにログインプロンプトが表示されますのでログインIDとパスワードを入力します。このログインIDおよびパスワードは、装置に添付されているシートのコンソールログインID、パスワードを入力してください。

```
atsb login: admin
password:
```

図 7-1 ログイン画面



このログインIDとパスワードはSecure Beagleの管理画面へのログインID、パスワードとは異なります。変更することはできません。

ログインすると、コンソール管理メニューが表示されます。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]:
```

図 7-2 コンソール管理メニュー

工場出荷時設定に戻したい場合

Secure Beagleの設定を工場出荷時に戻す場合、管理メニューにて 1 を入力します。設定を初期化するか確認を求められますので、よろしければ y を入力してください。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 1
Do you want to initialize the configuration?[y/n]: y
Configuration initialized
```

図 7-3 設定の初期化

管理者パスワードを忘れた場合

Web インターフェイスの管理者パスワードを忘れた場合、管理メニューにて 2 を入力します。新しいパスワードの入力を求められますので、パスワードの再設定を行います。

```
atsb login: admin
password:
1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 2
Input new password: newpasswd
```

図 7-4 パスワードの再設定

ネットワーク設定を変更したい場合

Secure Beagle のネットワーク設定を変更する場合、管理メニューにて 3 を入力します。新しい IP アドレス、ネットマスク、ゲートウェイを入力し、再設定を行ってください。

```
atsb login: admin
password:
1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 4
Allow IP address list cleared!
```

図 7-5 ネットワーク設定の変更

管理画面へのアクセス制限をクリアしたい場合

Secure Beagle の Web インターフェイスへのアクセス制限をクリアする場合、管理メニューにて 4 を入力します。ただちにアクセス制限は解除されますので、Web インターフェイスにて再度アクセス制限を行ってください。

```
atsb login: admin
password:
1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 5
Current Setting:
IP Address:      10.1.1.2/24
Default GW:     10.1.1.1
Current System Network Status:
IP Address:     10.1.1.2
Network mask:  255.255.255.0
Default GW:    10.1.1.1
```

図 7-6 アクセス制限のクリア

ネットワーク設定を確認したい場合

Secure Beagle のネットワーク設定を確認する場合、管理メニューにて5を入力すると、ネットワーク設定が表示されます。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting settings
9 ... Exit
Please input [1-9]: 5
Current Setting:
IP Address:      10.1.1.2/24
Default GW:     10.1.1.1
Current System Network Status:
IP Address:     10.1.1.2
Network mask:  255.255.255.0
Default GW:    10.1.1.1
```

図 7-7 ネットワーク設定確認

ネットワーク疎通を確認したい場合

ネットワーク疎通を確認したい場合、管理メニューにて6を入力します。疎通を確認したいIPアドレスを入力すると、ping コマンドで疎通を確認します。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 6
Input Destination IP Address: 10.1.1.3
PING 10.1.1.3 (10.1.1.3) 56 data bytes
64 bytes from 10.1.1.3: icmp_seq=0 ttl=64 time=2.2 ms
64 bytes from 10.1.1.3: icmp_seq=1 ttl=64 time=2.1 ms
64 bytes from 10.1.1.3: icmp_seq=2 ttl=64 time=1.8 ms
64 bytes from 10.1.1.3: icmp_seq=3 ttl=64 time=1.9 ms

--- 10.1.1.3 ping statistics ---
8 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.8/2.0/2.2 ms
```

図 7-8 ネットワーク疎通確認

Secure Beagle を再起動したい場合

Secure Beagle を再起動する場合、管理メニューにて7を入力します。ただちに Secure Beagle は再起動されます。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 5
Current Setting:
IP Address:      10.1.1.2/24
Default GW:     10.1.1.1
Current System Network Status:
IP Address:     10.1.1.2
Network mask:  255.255.255.0
Default GW:    10.1.1.1
```

図 7-9 アクセス制限のクリア

接続設定を変更したい場合

Secure Beagle の接続設定を変更したい場合、管理メニューにて 8 を入力します。現在の設定が表示され、変更したい設定を入力を求められます。TSO 設定を変更する場合は 1 を、NIC 設定を変更する場合は 2 を、管理メニューに戻る場合は 3 を入力します。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 8
TSO setting: off
eth0: auto
eth1: auto
eth2: auto

1 --- Change TSO setting
2 --- Change NIC setting
3 --- Exit
Please input [1-3]:
```

図 7-10 接続設定変更

1 TSO 設定

TSO の「on」「off」を入力することができます。

```
1 --- Change TSO setting
2 --- Change NIC setting
3 --- Exit
Please input [1-3]: 1

Change TSO setting
1 --- on
2 --- off[default]
Please input [1-2]:
```

図 7-11 TSO 設定

2 NIC 設定

変更したい NIC に該当する数字を入力します。画面に表示されている設定の数字を入力して、設定を変更します。

```
1 --- Change TSO setting
2 --- Change NIC setting
3 --- Exit
Please input [1-3]: 2

Select NIC
1 --- eth0
2 --- eth1
3 --- eth2
Please input [1-3]: 1

Select Connection setting
1 --- auto[default]
2 --- 1000M full
3 --- 100M full
4 --- 10M full
5 --- 100M half
6 --- 10M half
Please input [1-6]:
```

図 7-12 NIC 設定

コンソール管理メニューを終了したい場合

コンソール管理メニューを終了する場合、管理メニューにて 9 を入力します。ただちにコンソール管理メニューは終了し、ログインプロンプトが表示されます。

```
atsb login: admin
password:

1 ... Initialize configuration
2 ... Change WEB UI password
3 ... Change network setting
4 ... Clear allow IP address list
5 ... Show network setting
6 ... Execute ping
7 ... Reboot
8 ... Connecting setting
9 ... Exit
Please input [1-9]: 9

atsb login:
```

図 7-13 コンソール管理メニューの終了

7

コンソール管理

付録

1. 付録 A	86
2. 付録 B	87
3. 付録 C	88

付録A. 仕様

モデル名		Model 10	Model 30	Model 200
ネットワークインターフェース		1000/100/10 BASE-T (3ポート)		1000 BASE-T (4ポート)
ファイアーウォール機能		ステートフルインスペクション、パケットフィルタリング		
対応ネットワーク構成		透過型		
冗長化構成		アクティブ/スタンバイの冗長化構成が可能 (同一機種を2台用意)		
最大ポリシー数		1000		
使用電力		AC 100V ± 10V (50 / 60Hz)		
平均電力消費量	単体	50W		30W
	冗長化構成時 (2台の合計電力消費)	100W		60W
寸法	単体	45 (H) × 200 (W) × 350 (D) mm		42.4 (H) × 217 (W) × 365 (D) mm
	冗長化構成時 (ラックマウントキットを含む)	45 (H) × 450 (W) × 350 (D) mm ^{※1}		44.45 (H) × 441 (W) × 365 (D) mm ^{※1}
質量	単体	3kg / シャーシ 2kg		3kg
	冗長化構成時 (ラックマウントキットを含む)	8kg		9.8kg
付属品		電源ケーブル、Secure Beagle 専用ラックマウントキット、Secure Beagle 操作マニュアル		

(※1) 1/4U サーバーをラッキングする際は、付属のラックマウントキットが必要です。

付録B. 通知メールの内容

件名	[ホスト名] - Entering MASTER state
本文	=> Message Code 001: Device is turning to Active mode <=
内容説明	Secure Beagle (ホスト名)の動作状態が〔稼働中〕で稼働していることを表します。 または、対象のSecure Beagleに、フェイルオーバーが発生して動作状態が〔待機中〕から〔稼働中〕に遷移したことを表します。

件名	[ホスト名] - Entering BACKUP state
本文	=> Message Code 002: Device is turning to Wait mode <=
内容説明	Secure Beagle (ホスト名)の動作状態が〔待機中〕で稼働していることを表します。

付録C. パケットログ形式

ポリシー設定にてパケットログを取得する設定を行った場合、ポリシーに該当するパケットを受信したときにパケットログを出力します。

パケットログは以下のログ形式で出力されます。

Jun	7	16:49:36	10.1.1.2	kernel: allow	IN=br0	OUT=br0	PHYSIN=eth1	PHYSOUT=eth2	SRC=10.0.0.100	DST=10.1.1.10		
①	②	③	④	⑤	⑥	⑦						
LEN=48	TOS=0x00	PREC=0x00	TTL=128	ID=55834	DF	PROTO=TCP	SPT=3029	DPT=21	WINDOW=65535	RES=0x00	SYN	URGP=0
⑧		⑨		⑩						⑪		

① ログ出力日時

ログが出力された日時です。

② ホスト名もしくはIPアドレス

ログを出力したSecure Beagleのホスト名もしくはIPアドレスです。

③ 通過判定結果

対象パケットに対するSecure Beagleの通過判定結果です。以下のいずれかとなります。

allow	許可
deny	拒否
reject	RSTパケットを返信 (TCPプロトコルの場合のみ)

④ 転送元ゾーン

パケットを受信したゾーンです。

⑤ 転送先ゾーン

受信したパケットの転送先のゾーンです。

④⑤は以下のいずれかとなります。

eth0	Insideゾーン
eth1	Outsideゾーン
eth2	DMZゾーン

⑥ 送信元IPアドレス

対象パケットの送信元のIPアドレスです。

⑦ 送信先IPアドレス

対象パケットの送信先のIPアドレスです。

⑧ パケット長

対象パケットのパケット長です。

⑨ 詳細情報

対象パケットの詳細情報です。

⑩ プロトコル

対象パケットのプロトコルです。以下のいずれかとなります。

TCP	TCP
UDP	UDP
ICMP	ICMP
2	IGMP
94	IPIP
47	GRE
115	L2TP

⑪ プロトコルの詳細情報

プロトコルの詳細情報です。この内容は⑩がTCP、UDP、ICMPの場合のみ出力されます。プロトコル毎に出力内容が異なります。

TCPの場合の出力例

```
PROTO=TCP SPT=3029 DPT=21 SEQ=0 ACK=0 WINDOW=65535 RES=0x00 SYN URG=0
```

- ① 送信元ポート番号**
対象パケットの送信元ポート番号です。
- ② 送信先ポート番号**
対象パケットの送信先ポート番号です。
- ③ シーケンス番号**
データの順序を示す番号です。データ送信が複数パケットとなる場合に設定されます。
- ④ 応答確認番号**
データを受信したことを示す番号です。データ送信が複数パケットとなる場合に設定されます。
- ⑤ ウィンドウ**
受信バッファサイズです。
- ⑥ リザーブ**
TCPヘッダのリザーブ領域の値です。
- ⑦ TCPフラグ**
TCP制御用フラグです。

UDPの場合の出力例

```
PROTO=UDP SPT=137 DPT=137 LEN=58
```

- ① 送信元ポート番号**
対象パケットの送信元ポート番号です。
- ② 送信先ポート番号**
対象パケットの宛先ポート番号です。
- ③ データサイズ**
対象パケットのデータ部分のサイズです。

ICMPの場合の出力例

```
PROTO=ICMP TYPE=8 CODE=0 ID=50951 SEQ=17
```

- ① リクエストタイプ**
ICMPリクエストの内容です。
- ② 応答コード**
①のリクエストに対する結果です。
- ③ 詳細情報**
詳細情報です。
ICMPリクエスト毎に出力内容が異なります。

Secure Beagle Model 10/30/200 共通 操作マニュアル

2013年7月17日(第1版)

株式会社 エーティーワークス

東京本社：〒106-6137

東京都港区六本木6丁目10番1号 六本木ヒルズ森タワー37階

富山本社：〒930-0856

富山県富山市牛島新町4号5番 エーティーワークス本社ビル

TEL：0120-0-41414

E-Mail：query@atworks.co.jp

<http://www.atworks.co.jp>

<https://www.atworks.co.jp/store/>

<http://www.at-link.ad.jp> (at+link 専用サーバサービス)



The Next Quality

Copyright © A.T.WORKS, Inc. All rights reserved.