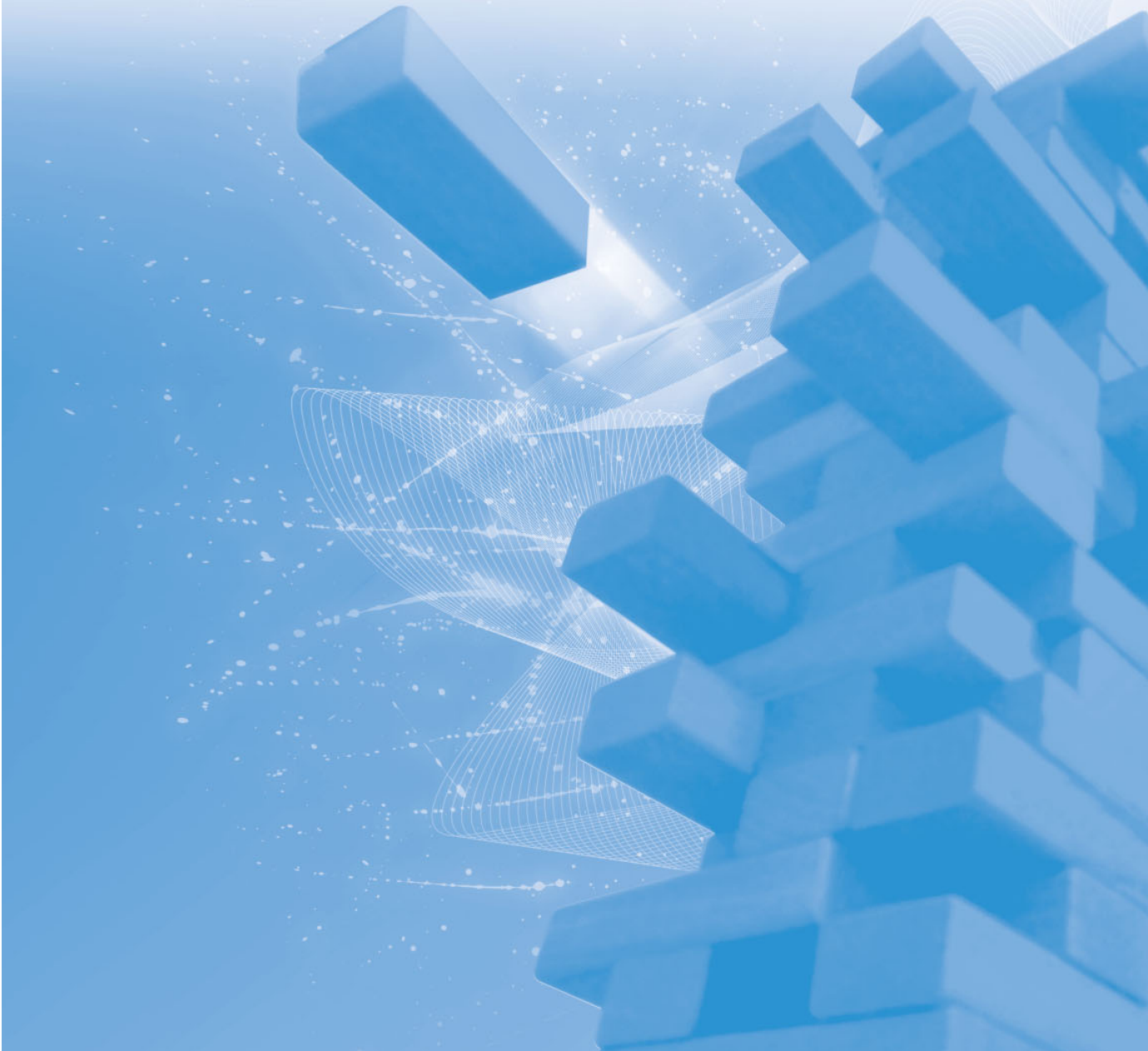
A.T.WORKS
The Next Quality

Sentinel Beagle Model 200

操作マニュアル



Sentinel 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。

目 次

目次

第1章 Sentinel Beagleとは

1. はじめに

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

Sentinel Beagleは、オープンソースソフトウェアを弊社が独自にカスタマイズした迷惑メールフィルタ機能を搭載する、アプライアンスサーバです。

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。

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．Sentinel 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

■導入が容易
・既存のメールサーバの設定を変更することなく導入することが可能

■迷惑メールフィルタリング
・迷惑メールフィルタリングエンジンとしてtarpitting + S25R + greylistingを採用

■迷惑メールスコアリング
・迷惑メールスコアリングエンジンとしてSpamAssassinを採用
・スコアリング自動学習機能によりメンテナンスフリー

■ウイルスチェック
・ウイルスチェックエンジンとしてClamAV + AMaViSを採用
・ウイルス定義ファイルは自動更新されるためメンテナンスフリー

■ホワイト／ブラックリスト機能
・ホワイト／ブラックリストに登録することで確実に通過／破棄
差出元アドレス、宛先アドレス、送信元IPアドレス単位で設定可能

■運用管理
・Webブラウザから操作できる専用管理インタフェイスを搭載
・メールの処理状況をグラフ表示
・本製品の各種状態（CPU使用率、メモリ使用量、ネットワークトラフィック、ディスク使用量）をグラフ表示

■保守性
・設定情報・学習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

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

本製品のハードウェアの取り扱いについて説明いたします。

■フロントパネルの説明

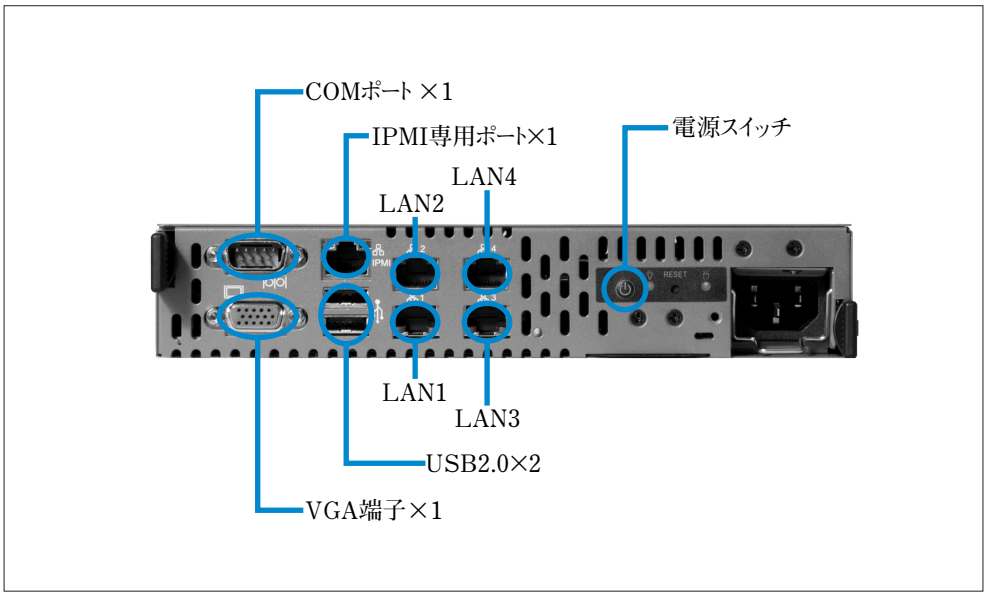


図1-1　フロントパネル

電源スイッチ	押下すると電源が投入されます。
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コネクター	LAN1を使用します。

LAN2、LAN3、LAN4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、変なにおいや音がしたら、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
- 振動が発生する場所
- 平坦でない場所
- 強い磁界が発生する場所
- 直射日光が当たる場所
- 火気の近く、または高温になる場所
- 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）
- 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 迷惑メール対策の仕組み

1．迷惑メール対策フロー

Sentinel Beagleではインターネットより配送されてきたメールを下記のフローで段階的に判定し迷惑メールかどうかを判定しています。

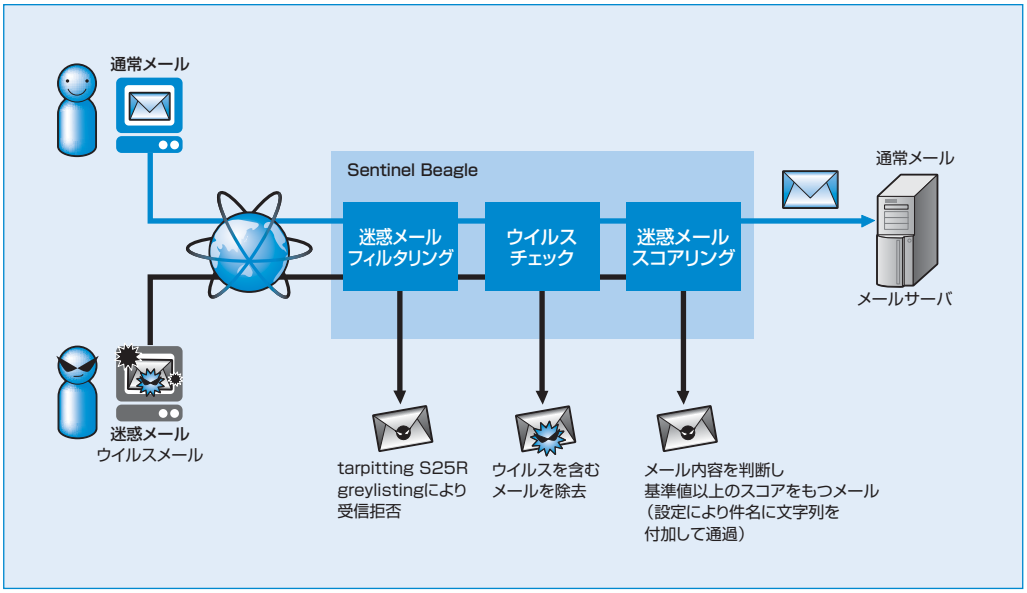


図2-1

2. 迷惑メールフィルタリング

Sentinel Beagleはインターネットより配送されてきたメールに対して最初に迷惑メールフィルタリング処理を実施します。
具体的にはS25Rに該当する接続元からのメールに対しtarpittingによる応答遅延、またはgreylistingによる一時配送拒否を行います。
このフィルタ処理により、大半の迷惑メールの配送を拒否します。

S25R、tarpitting、greylistingについてはP12～14の迷惑メールフィルタリング技術を参照してください。

3. ウイルスチェック

ウイルスを含んだメールかどうかを判定します。ウイルスを含んだメールはメールサーバに配送せずに、差出元に返送するか破棄します。
Sentinel Beagleではウイルスデータベースは定期的に自動更新しますので管理者のメンテナンスを必要としません。常に最新のデータベースを用いてウイルスチェックを行います。

4. 迷惑メールスコアリング

メールの本文とヘッダを解析し、迷惑メールによく見られる特徴がどの程度含まれているかのスコアリングを行います。このスコアが基準値以上であれば迷惑メールとみなされます。
迷惑メールと判定された場合、メールの件名に迷惑メールと判定したタグ（識別文字列）を付加し、さらに迷惑メールであることを示す識別文字列（X-Spam-Flag: YES）をメールヘッダに付加してメールサーバに配送します。
また、迷惑メールのスコアリング結果を学習していくため、運用を続けることでより精度の高いスコアリング判定を行うようになります。

迷惑メールフィルタリング技術

S25R (Selective SMTP Rejection)

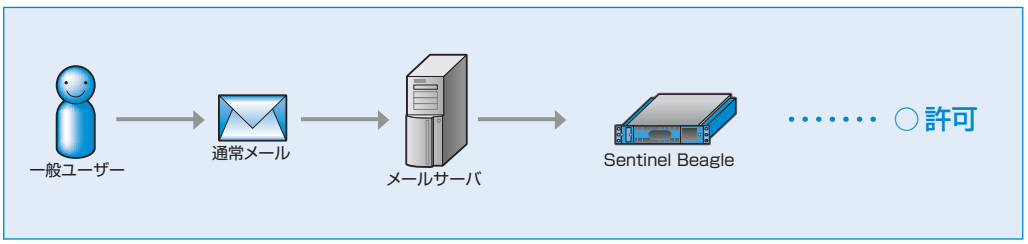
S25Rは浅見秀雄氏が考案した、メールを配送しようとする接続元のIPアドレスを逆引きして得られるドメイン名の特徴から、接続元がメールサーバか一般ユーザのコンピュータかを判別し、メールサーバからのメールのみを受け入れる方式です。

通常メールはメールサーバ経由でメール配送が行われることに対し、迷惑メールの配信者はメールの大量配信ソフトウェアを利用してメールサーバを経由せずにメールの配送を試みることが多いという特徴を利用しています。

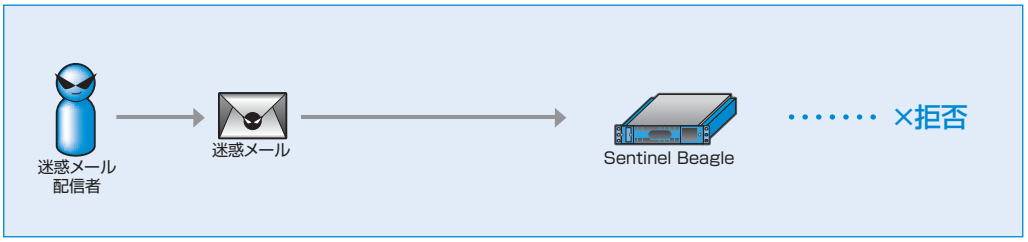
なお、メールサーバのホスト名の特徴によっては一般ユーザのホスト名と誤認されてしまう可能性があります。

http://www.gabacho-net.jp/anti-spam/

■通常メール



■迷惑メール



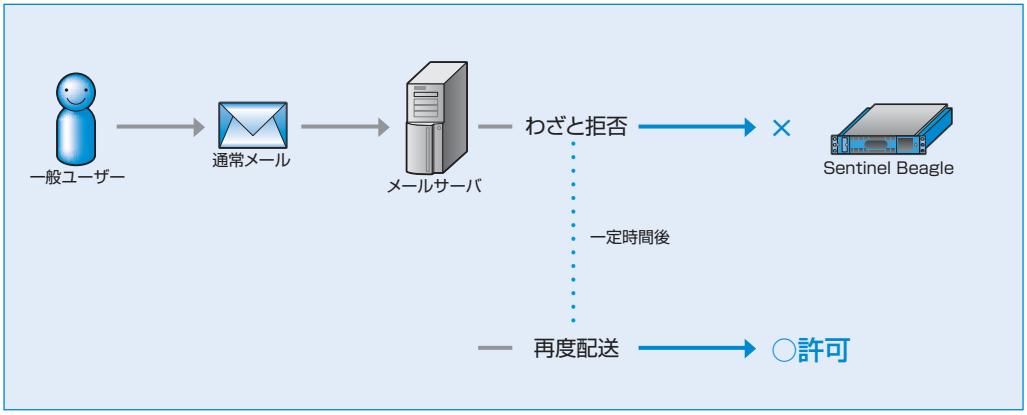
greylisting

greylistingはメールの配送を一度わざと拒否し、再度配送されてきた際に受け入れる方式です。

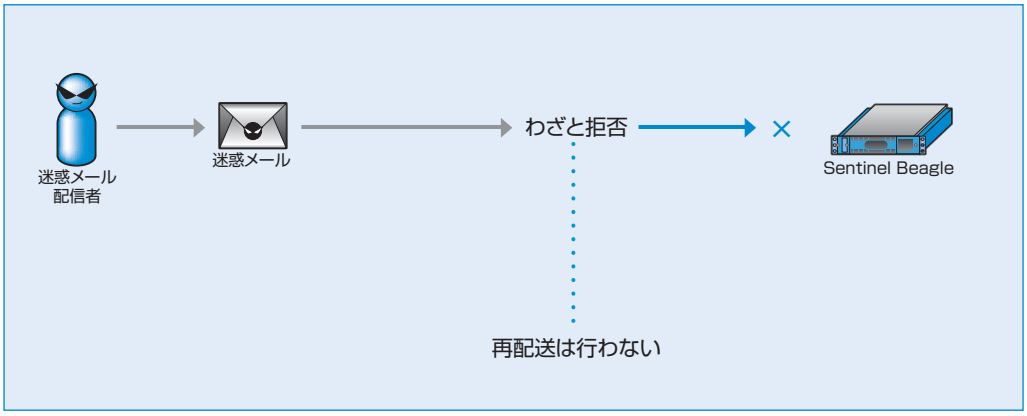
通常メールを配送するメールサーバは拒否された場合は一定時間後に再配送を試みることに対し、迷惑メール配送ソフトウェアは拒否された場合に再配送を行うように作られていないことが多いという特徴を利用しています。

なお、メールサーバによっては配送を一度でも拒否されたらそれで諦めて再送を行わないものがあります。

■通常メール



■迷惑メール



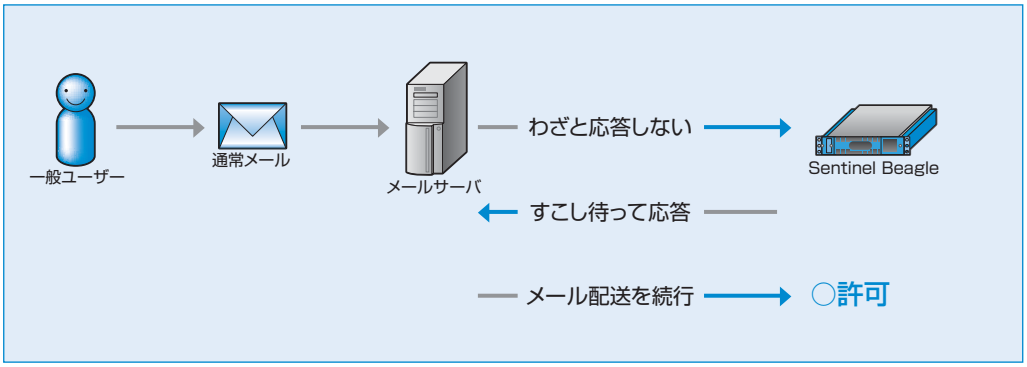
tarpitting

tarpittingはメールの配送しようとする接続元に対し、わざと応答を遅らせる方式です。

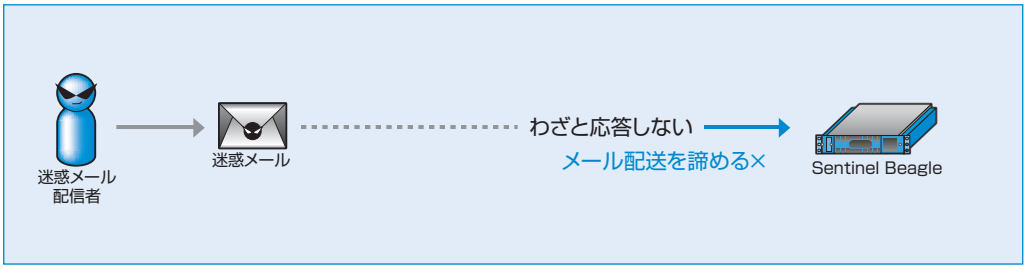
通常メールを配送するメールサーバは接続先の応答がすぐにない場合でも一定時間待つことに対し、迷惑メール配送ソフトウェアは短時間に大量の迷惑メールを配送するために接続先のメールサーバの応答がすぐにない場合にあまり待たずに配送を諦めるという特徴を利用しています。

なお、メールサーバによっては待ち時間が短いものがあります。

■通常メール



■迷惑メール



taRgrey

S25R、greylisting、tarpittingを組み合わせることで、各方式の弱点を補った方式が佐藤潔氏が開発したtaRgreyという方式です。

S25Rにより接続元を一般ユーザのコンピュータであると判断した場合、接続を切断するのではなくtarpittingによる応答遅延を行います。
接続元が tarpittingの応答を待たずに切断し、再接続してきた場合、greylistingにより受け入れます。

この組み合わせにより、各方式の迷惑メール拒否方法を最大限活用しつつ、通常メールを迷惑メールと誤判定する可能性を極力少なくしています。

http://k2net.hakuba.jp/targrey/

第3章 セットアップ

1. 設置計画

Sentinel Beagleは既存のネットワーク構成を変更することなく設置が可能です。

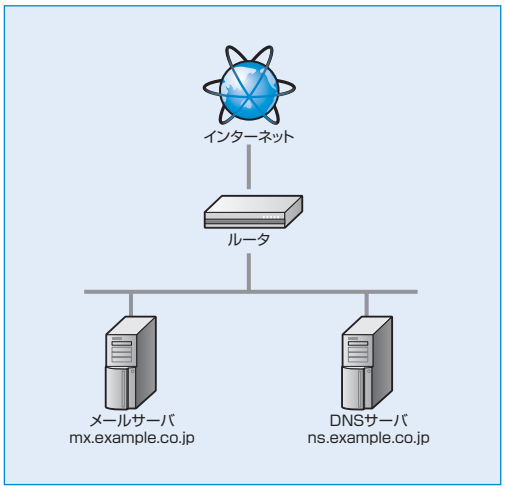


図3-1　既存のネットワーク構成例

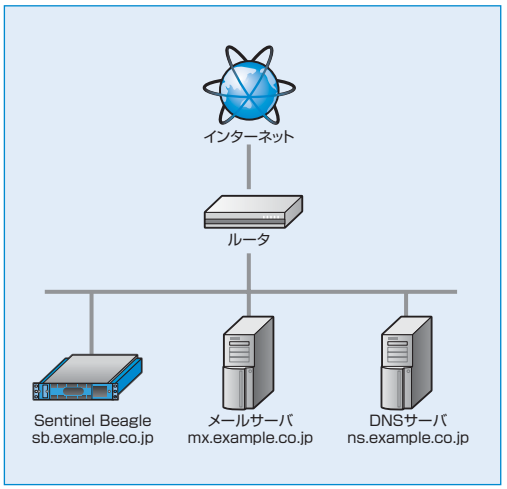


図3-2　Sentinel Beagleを追加

2. 初期設定

Sentinel 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	192.168.1.2
ネットマスク	255.255.255.0
ゲートウェイ	192.168.1.1

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。

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 ハブとストレートケーブル

1 Sentinel Beagleとメンテナンスの接続

Sentinel 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3-3のような状態となります。
ハブとストレートケーブルを使用してSentinel Beagleとメンテナンスそれぞれを接続する方法でもかまいません。この場合、ハブにSentinel 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。

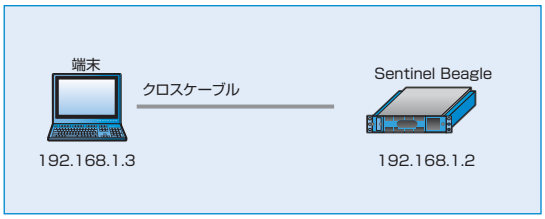


図3-3　メンテナンス端末との接続

2 メンテナンスPCのネットワーク設定

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	192.168.1.3
ネットマスク	255.255.255.0
ゲートウェイ	192.168.1.1（任意）

3 Sentinel Beagleの電源投入

Sentinel 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://192.168.1.2:18180/

図 3-4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3-4　ログイン画面

図3-4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。
- Sentinel Beagleが電源投入されているか（電源ランプの確認）
- Sentinel Beagleとメンテナンス PC、ハブ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

Sentinel Beagleのネットワーク設定が変更されている場合、このURLでは接続ができません。
Sentinel 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環境にあわせてネットワーク設定を行ってください。
【基本設定】→【ネットワーク】にてネットワーク設定を行います。

ネットワーク設定についてはP52を参照してください。

プライマリDNSサーバは必ず設定してください。
DNSサーバが設定されていない場合、受信メールを適切に処理することができません。

ネットワーク設定は即座に反映されます。

ネットワーク設定後はメンテナンスPCからの操作が行えなくなります。
メンテナンスPCのネットワーク設定を変更し、再度管理画面にログインしてください。

https://【Sentinel Beagleに設定したIPアドレス】:18180/

6 管理者パスワードの変更

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】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P55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Sentinel 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P56を参照してください。

8 Sentinel Beagleの停止と設置

Sentinel Beagleのシャットダウンを実行します。

Sentinel Beagleのシャットダウンについては P78を参照してください。

Sentinel 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 Sentinel Beagleに設定したIPアドレスを指定して管理画面が開けることを確認してください。

https://【Sentinel Beagleに設定したIPアドレス】:18180/

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、LAN1インタフェイスのIPアドレス、ネットマスク、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（DVI端子）
キーボード（PS/2端子）

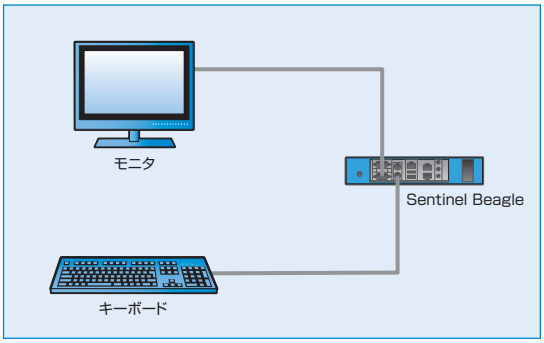


図3-5　コンソール使用方法

1 Sentinel Beagleと機器の接続

Sentinel BeagleのDVI端子にモニタを接続します。
Sentinel Beagleのキーボード端子にPS/2キーボードを接続します。

2 Sentinel Beagleの電源投入

Sentinel 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Sentinel 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、LAN1ネットワークの次の項目に限定されます。

- IPアドレス
- ネットマスク
- ゲートウェイ

☞ コンソール管理から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 Sentinel Beagleの停止と設置

Sentinel Beagleのシャットダウン処理を実行します。

☞ コンソール管理からシャットダウンする方法はP83を参照してください。

Sentinel 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://【Sentinel Beagleに設定したIPアドレス】:18180/

! 本手順では、ホスト名、ドメイン、プライマリDNSサーバ、セカンダリDNSサーバの設定、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。
Sentinel 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。

☞ ネットワーク設定についてはP52を参照してください。
☞ 管理者パスワードの変更方法についてはP55を参照してください。
☞ 接続許可IPアドレスの制限についてはP56を参照してください。

3. 初期設置例

既存のネットワーク構成に設置する例です。

ネットワーク構成例のネットワークに便宜上10.0.0.0/24のネットワークを使用しております。

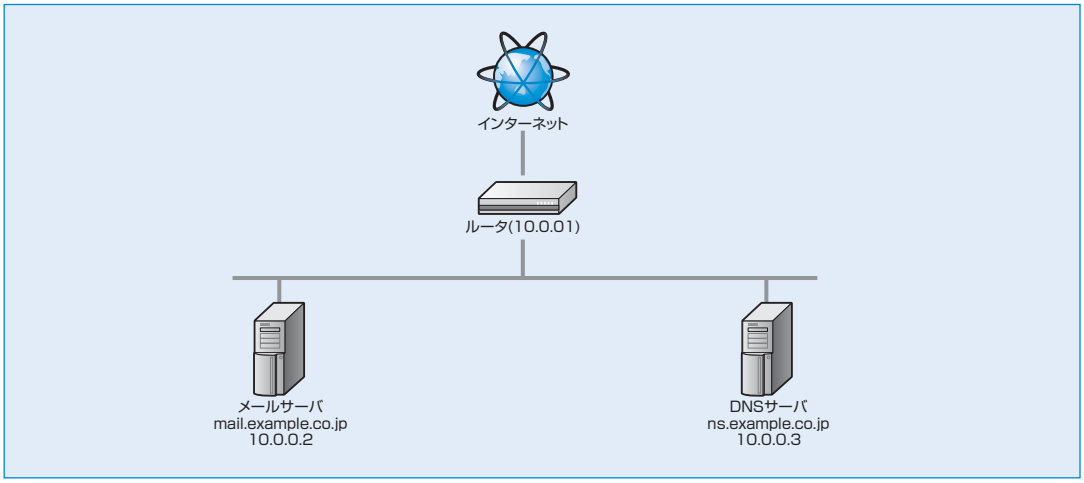


図3-6　既存のネットワーク構成例

1 Sentinel Beagleの初期設定

3-2 初期設定の手順に従って下記のようにネットワーク設定を行います。

IPアドレス	10.0.0.10
ネットマスク	255.255.255.0
ゲートウェイ	10.0.0.1
プライマリDNSサーバ	10.0.0.3
セカンダリDNSサーバ	0.0.0.0
ホスト名	sb
ドメイン名	example.co.jp

2 Sentinel Beagleの設置

下記のようにSentinel Beagleをネットワークに設置します。

メールサーバと通信できれば同一ネットワークでなくても構いません。

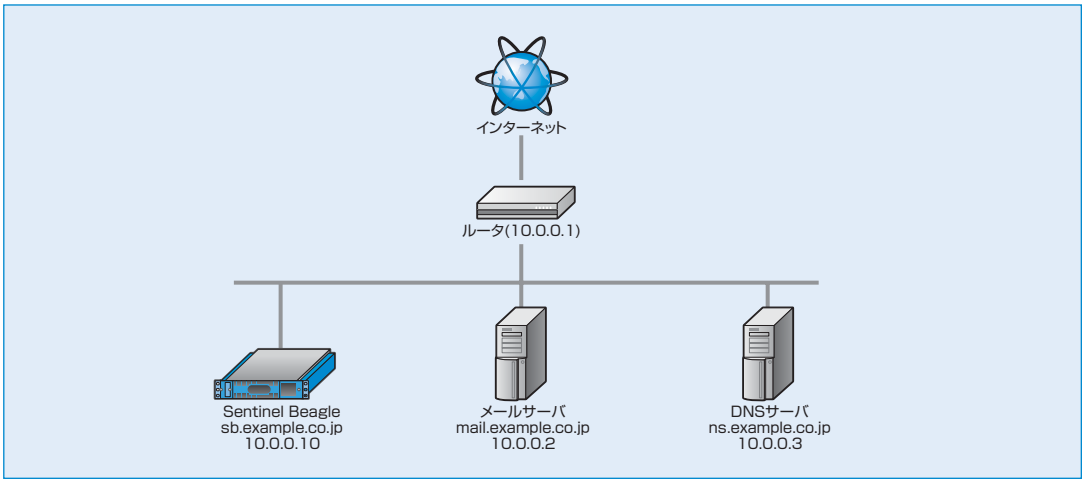


図3-7

3 メールドメインの登録

Sentinel Beagleにて迷惑メールフィルタを行う対象ドメインとメールサーバのアドレスを登録します。

❶ Sentinel Beagleの管理画面にログインします。

❷ 【設定】→【メールドメイン】を選択します。

❸ **「ドメイン追加」**にてドメインとメールサーバを登録します。
今回の設定例では

ドメイン	example.co.jp
メールサーバ	10.0.0.2

となります。

メールドメインの登録方法についてはP54を参照してください。

4. DNSサーバの修正

手順3で登録したドメインを管理するDNSサーバの修正を行います。
MXレコードをmx.example.co.jpからsb.example.co.jp に変更します。

DNSサーバの設定を行う前に、必ず Sentinel Beagleのメールドメインの設定を行ってください。
Sentinel Beagleはメールドメインに設定されていない宛先のメールはすべて拒否します。

■example.co.jp.zone　修正前

```
$TTL 86400
@       IN    SOA    sv.example.co.jp. postmaster.example.co.jp. (
                     2009010101; Serial
                     3H        ; Refresh3 hours
                     15M       ; Retry1 hour
                     1W        ; Expire1000 hours
                     1D )      ; Minimum 24 hours
        IN    MX     10 mail.example.co.jp.
        IN    NS     ns.example.co.jp.
mail    IN    A      10.0.0.2
ns      IN    A      10.0.0.3
```

■example.co.jp.zone　修正後

```
$TTL 86400
@       IN    SOA    sv.example.co.jp. postmaster.example.co.jp. (
                     2009010102;Serial
                     3H        ;Refresh3 hours
                     15M       ;Retry1 hour
                     1W        ;Expire1000 hours
                     1D )      ;Minimum 24 hours
        IN    MX     10 sb.example.co.jp.
        IN    NS     ns.example.co.jp.
mail    IN    A      10.0.0.2
ns      IN    A      10.0.0.3
sb      IN    A      10.0.0.10
```

MXレコードの設定変更が伝搬することで、Sentinel Beagleにメールが配送されます。

第4章 迷惑メール対策設定

1．迷惑メールフィルタリング

迷惑メールフィルタリングについての設定を変更することができます。
基本的にはデフォルト設定で問題ありません。

❶【アンチスパム】→【迷惑メールフィルタリング】を選択します。

❷ 各種設定を変更したい場合は「**編集**」をクリックします。

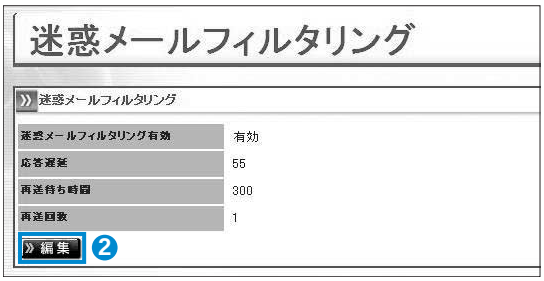


図4-1　迷惑メールフィルタリング

迷惑メールフィルタリング設定　デフォルト:有効
迷惑メールフィルタリング機能の有効／無効を設定します。

応答遅延　デフォルト:55秒
メールの配送要求に対して応答を遅延する時間を設定します。

再送待ち時間　デフォルト:300秒
メールの配送要求に対して再送要求を行った場合、メールの再送を受け入れない時間を設定します。

再送回数　デフォルト:1回
メールの配送要求に対して再送要求を行う回数を設定します。

❸ 設定変更が完了したら「**適用**」をクリックします。

! 設定は即座に反映されます。

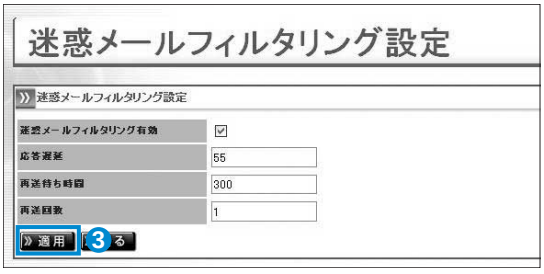


図4-2　迷惑メールフィルタリング設定

2. 迷惑メールスコアリング

迷惑メールスコアリングについての設定を変更することができます。

❶【アンチスパム】→【迷惑メールスコアリング】を選択します。

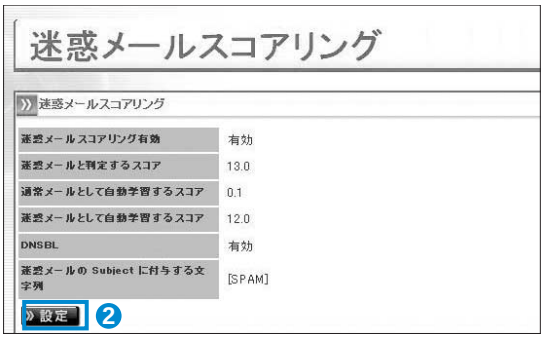


図4-3　迷惑メールスコアリング

❷ 各種設定を変更したい場合は「**編集**」をクリックします。

迷惑メールスコアリング有効　デフォルト:有効
迷惑メールフィルタリング機能の有効／無効を設定します。

迷惑メールと判定するスコア　デフォルト:13.0
対象メールのスコアがこの値以上であれば、迷惑メールと判定します。

通常メールとして自動学習するスコア　デフォルト:0.1
対象メールのスコアがこの値未満であれば、通常メールとして学習します。

迷惑メールとして自動学習するスコア　デフォルト:12.0
対象メールのスコアがこの値以上であれば、迷惑メールとして学習します。

DNSBL　デフォルト:有効
DNSBLとは迷惑メールを送信した送信元メールアドレスのリストです。
対象メールの差出元がこのリストに含まれていれば、対象メールのスコアを加算します。

迷惑メールの Subject に付与する文字列　デフォルト:[SPAM]
迷惑メールと判定した場合にメールのSubject に付与する文字列です。

! 迷惑メールのSubjectに付与する文字列には半角英数字を使用してください。

❸ 設定変更が完了したら「**適用**」をクリックします。

! 設定は即座に反映されます。

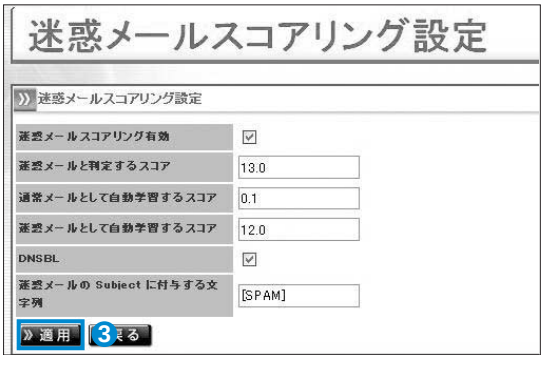


図4-4　迷惑メールスコアリング設定

3. ウイルスチェック

ウイルスチェックについての設定を変更することができます。

❶【アンチスパム】→【ウイルスチェック】を選択します。

❷ 各種設定を変更したい場合は「**編集**」をクリックします。

図4-5　ウイルスチェック

ウイルスチェックを有効　デフォルト:有効
ウイルスチェック機能の有効／無効を設定します。

ウイルス検出時の動作　デフォルト:拒否
ウイルスを検出した場合の対象メールの扱いを設定します。
拒否の場合、対象メールを差出元に返送します。
破棄の場合、対象メールを破棄します。
どちらの場合も本来の宛先であるメールサーバへ配送は行いません。
許可の場合、対象メールをメールサーバに転送します。

ウイルス検出通知有効　デフォルト:無効
ウイルスを検出した場合、その旨を指定したメールアドレスに通知する機能の有効／無効を設定します。

ウイルス検出通知差出元メールアドレス
ウイルス検出通知が有効の場合、ウイルス検出通知メールの差出元メールアドレスを設定します。

ウイルス検出通知宛先メールアドレス
ウイルス検出通知が有効の場合、ウイルス検出通知メールの宛先メールアドレスを設定します。

❸ 設定変更が完了したら「**適用**」をクリックします。

! 設定は即座に反映されます。

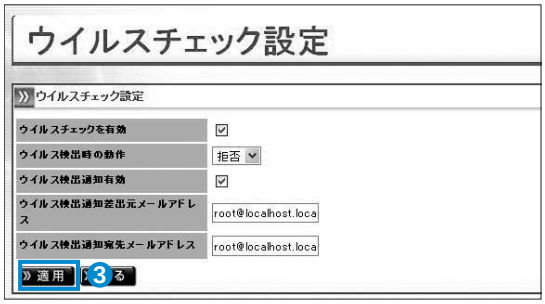


図4-6　ウイルスチェック設定

4. ブラック／ホワイトリスト

ブラック／ホワイトリストは、特定の条件にあったメールに対して、指定した方法でメールを処理する機能です。

特定の条件とは以下の3種類から設定可能です。

差出元メールアドレス
差出元IPアドレス
宛先メールアドレス

特定の条件とは以下の3種類から設定可能です。

許可
タグ
拒否

となります。
「許可」を指定すると通常メールと判定されます。
「タグ」を指定すると迷惑メールと判定されます。
「拒否」を指定すると対象メールを受け付けません。

差出元メールアドレスにてブラック／ホワイトリストを利用する場合

❶【ブラック／ホワイトリスト】→【差出元メールアドレス】を選択します。

図4-7　差出元メールアドレス ブラック／ホワイトリスト

❷差出元メールアドレス追加にて対象の差出元メールアドレスと動作を選択し、**「適用」**をクリックします。

❸リストに追加されたことを確認します。

設定は即座に反映されます。

差出元IPアドレスにてブラック／ホワイトリストを利用する場合

❶【ブラック／ホワイトリスト】→【IPアドレス】を選択します。

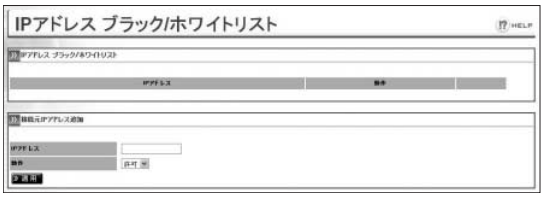


図4-8　IPアドレス　ブラック／ホワイトリスト

❷IPアドレス追加にて対象のIPアドレスと動作を選択し、**「適用」**をクリックします。

❸リストに追加されたことを確認します。

! 設定は即座に反映されます。

宛先メールアドレスにてブラック／ホワイトリストを利用する場合

❶【ブラック／ホワイトリスト】→【宛先メールアドレス】を選択します。

図4-9　宛先メールアドレス　ブラック／ホワイトリスト

❷宛先メールアドレス追加にて対象の宛先メールアドレスと動作を選択し、**「適用」**をクリックします。

❸リストに追加されたことを確認します。

! 設定は即座に反映されます。

第5章 状況

1．システム状況

Sentinel Beagleのシステム状況（CPU使用率、メモリ使用量、トラフィック、Disk使用量）とメールグラフ（メール送受信数、メール処理結果）を確認することができます。
システム状況およびメールグラフは過去1日、過去一週間、過去1ヶ月、過去1年分のグラフを表示可能です。

【状況】→【システム状況】を選択します。

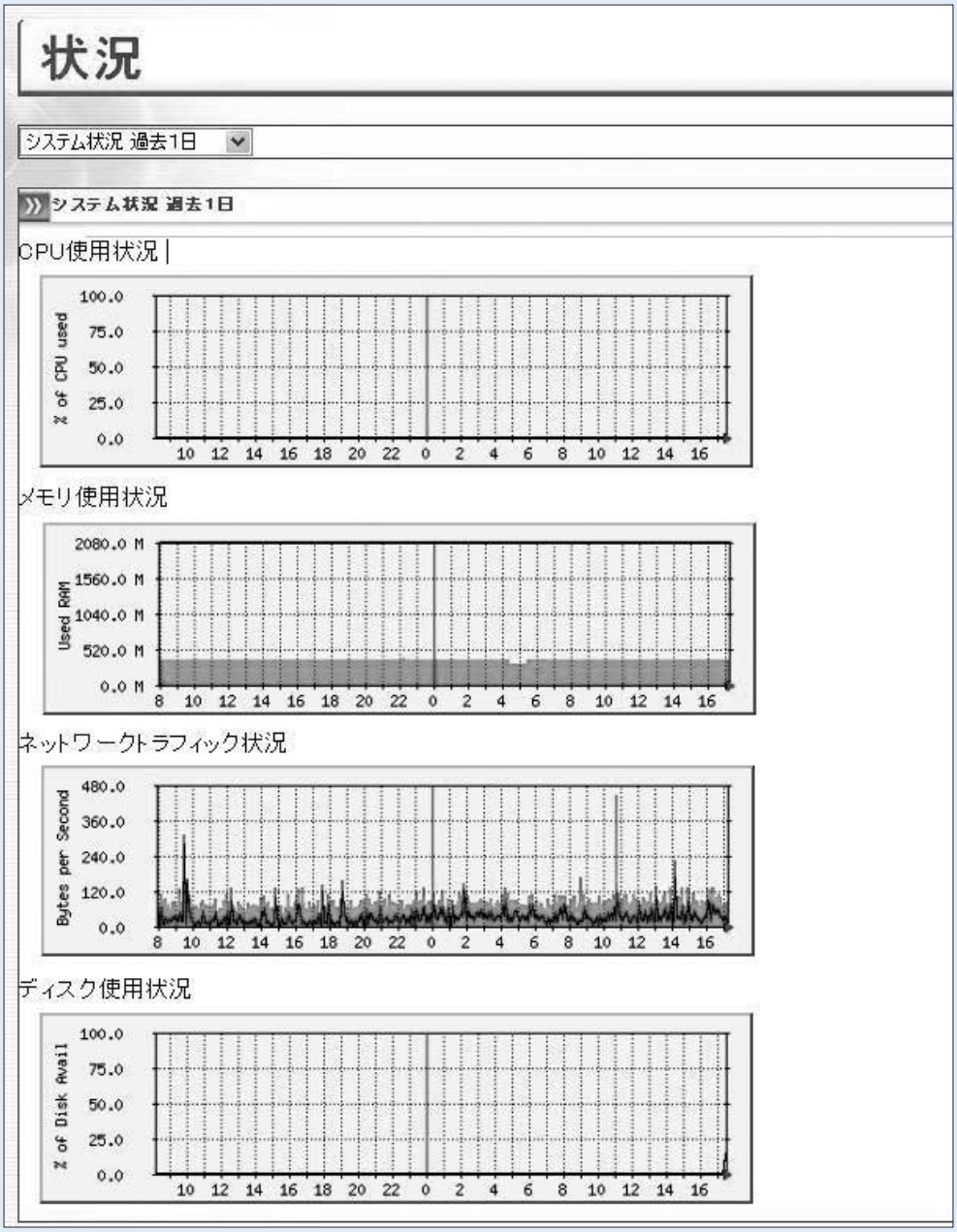


図5-1　システム状況

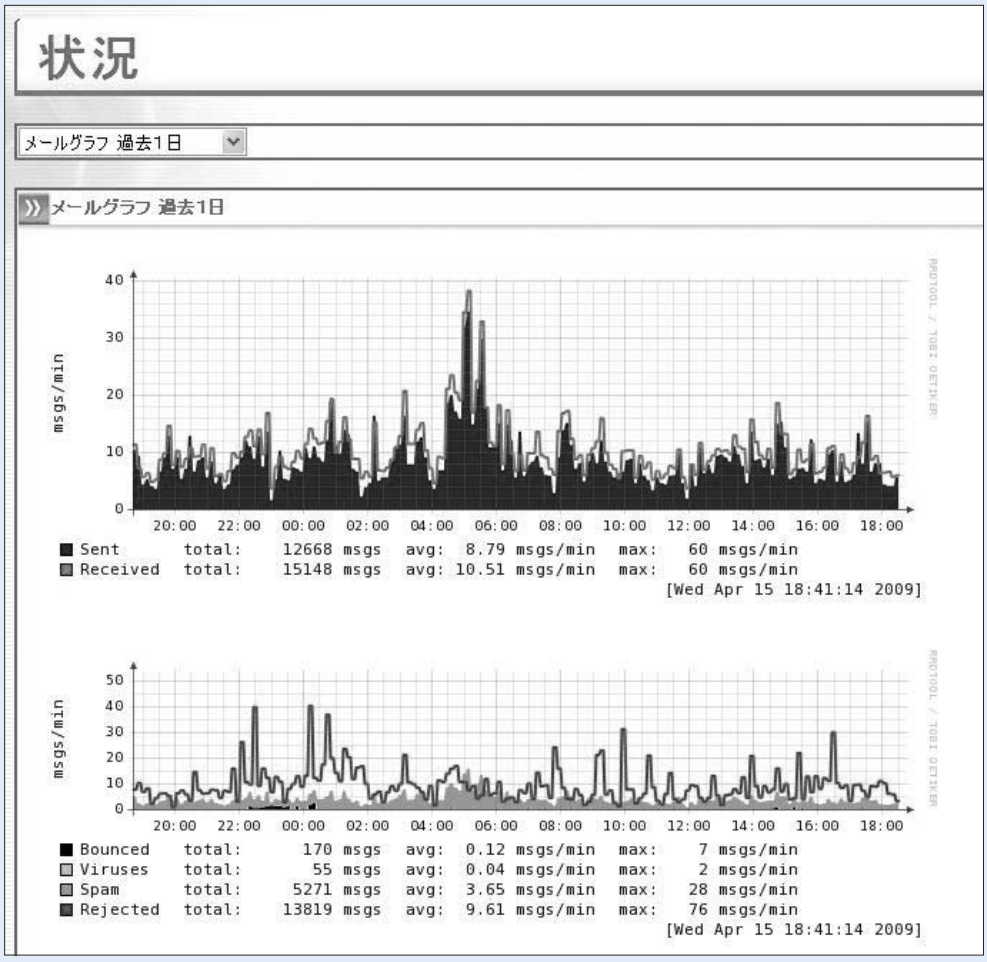

状況
メールグラフ 過去1日
メールグラフ 過去1日
msgs/min
40
30
20
10
0
20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00
Sent total: 12668 msgs avg: 8.79 msgs/min max: 60 msgs/min
Received total: 15148 msgs avg: 10.51 msgs/min max: 60 msgs/min
[Wed Apr 15 18:41:14 2009]
msgs/min
50
40
30
20
10
0
20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00 16:00 18:00
Bounced total: 170 msgs avg: 0.12 msgs/min max: 7 msgs/min
Viruses total: 55 msgs avg: 0.04 msgs/min max: 2 msgs/min
Spam total: 5271 msgs avg: 3.65 msgs/min max: 28 msgs/min
Rejected total: 13819 msgs avg: 9.61 msgs/min max: 76 msgs/min
[Wed Apr 15 18:41:14 2009]

図5-2　メールグラフ

2. メールログ

Sentinel Beagleではメール処理結果をロギングしており各種検索条件にて受信メールの処理結果を確認することができます。

【状況】→【メールログ】を選択します。

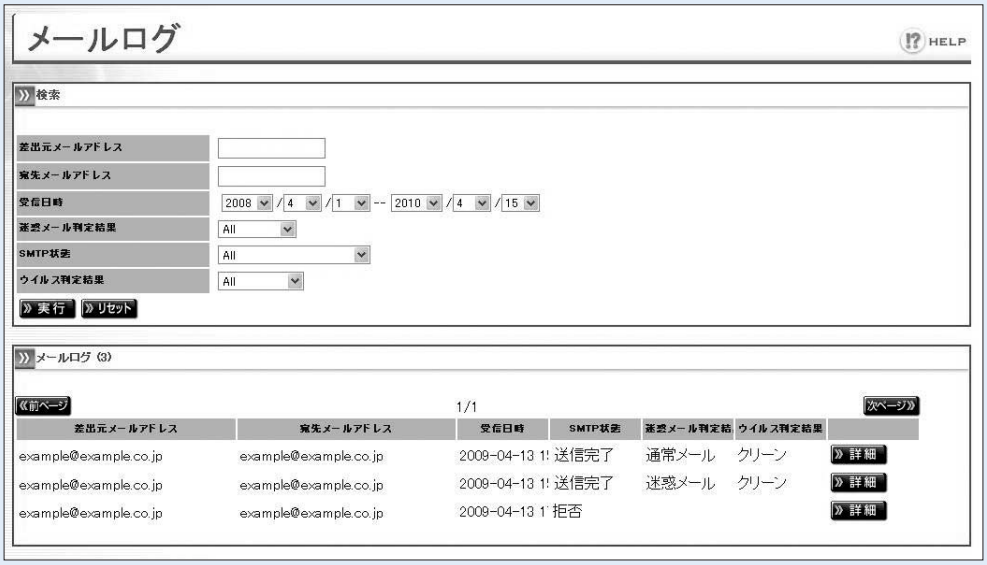


図5-3

検索条件

差出元メールアドレス

差出元メールアドレスにより抽出することができます。
メールアドレスの一部（ユーザー名、ドメイン名）だけを入力した場合でも条件にマッチしたログが抽出されます。

宛先メールアドレス

宛先メールアドレスにより抽出することができます。
メールアドレスの一部（ユーザー名、ドメイン名）だけを入力した場合でも条件にマッチしたログが抽出されます。

受信日時

受信メールの期間によりログを抽出することができます。

迷惑メール判定結果

迷惑メールの判定結果によりログを抽出することができます。

SMTP状態

SMTP状態によりログを抽出することができます。

ウイルス判定結果

ウイルス判定結果によりログを抽出することができます。

抽出ログの「詳細」をクリックすると対象メールの処理内容を細かく確認することができます。

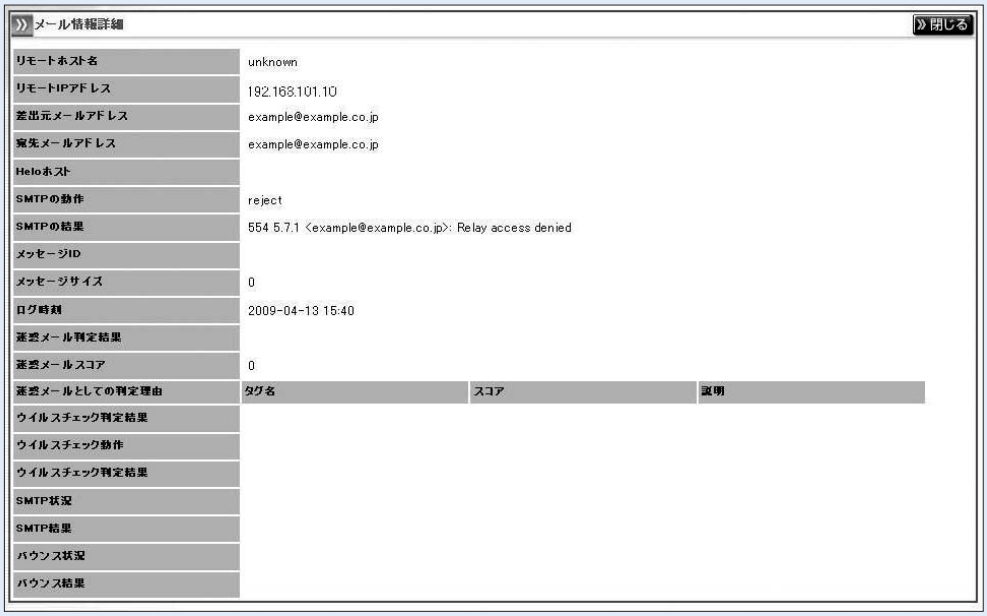


図5-4

3. 迷惑メールフィルタリング学習

Sentinel Beagleで行っているメールフィルタリングの学習状況を確認することができます。

グレイリスティング状況

グレイリスティング状況は、再送要求が正常に行われ、再送を待っているメールのリストです。
本リストに登録されているものと同じ差出元IPアドレス、差出元メールアドレス、宛先メールアドレスを持つメールに対しては再送要求は行われません。

図5-5

接続元ホワイトリスト状況

接続元ホワイトリスト状況は、グレイリスティング処理による再送要求に正常に応じたIPアドレスのリストです。
本リストに登録されているものと同じ差出元IPアドレスに対しては再送要求は行われません。

図5-6

応答遅延状況

応答遅延状況は、tarpittingによる応答遅延を待たなかったIPアドレスのリストです。

図5-7

グレイリスティング状況、接続元ホワイトリスト状況、応答遅延状況の学習状況はバックアップ、リストア、初期化することができます。

学習状況のバックアップ、リストアについてはP42を参照してください。
学習状況の初期化についてはP45を参照してください。

4. 迷惑メールスコアリング学習

Sentinel Beagleで行っているメールスコアリングの学習状況を確認することができます。

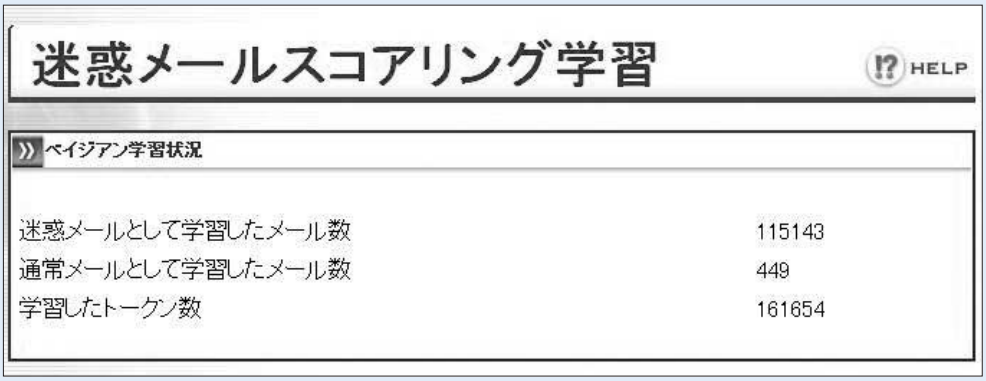


図5-8

運用を続けていき、より多くの迷惑メール、通常メールを学習することで迷惑メールスコアリング処理の精度が高まります。

迷惑メールスコアリング学習状況はバックアップ、リストア、初期化することができます。

学習状況のバックアップ、リストアについてはP42を参照してください。
学習状況の初期化についてはP45を参照してください。

第6章 運用管理

1．プロセス

Sentinel Beagleで動作する各プロセスの稼動状態を表示します。

各プロセスは操作欄の【停止】【起動】【再起動】にて停止、起動、再起動の操作を行うことができます。

図6-1

2. バックアップ／リストア

システム設定、迷惑メールフィルタリング学習状況、迷惑メールスコアリング学習状況をバックアップできます。
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または学習状態に戻すことができます。

システム設定のバックアップ手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「システム設定のバックアップ」の**「実行」**をクリックすると、システム設定ファイルがダウンロードされます。

図6-2

ファイルの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。

ダウンロードしたファイルを編集すると、正常にリストアできなくなります。
ダウンロードしたファイルは編集を行わずそのまま保管してください。

システム設定のリストア手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「システム設定のリストア」のファイル入力欄にバックアップ手順にて取得した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。

❸**「実行」**をクリックすると設定情報のリストアが開始されます。

図6-3

リストア完了後は即座にシステムが再起動されます。

リストアに失敗した場合、以下の項目をご確認ください。
・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。

迷惑メールフィルタリング学習状況のバックアップ手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「迷惑メールフィルタリング」の**「実行」**をクリックすると、システム設定ファイルがダウンロードされます。

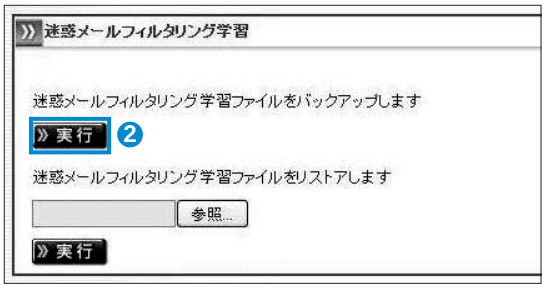


図6-4

ファイルの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。

ダウンロードしたファイルを編集すると、正常にリストアできなくなります。
ダウンロードしたファイルは編集を行わずそのまま保管してください。

迷惑メールフィルタリング学習状況のリストア手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「迷惑メールフィルタリング学習」のファイル入力欄にバックアップ手順にて取得した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。

❸**「実行」**をクリックすると迷惑メールフィルタリング学習状況のリストアが開始されます。

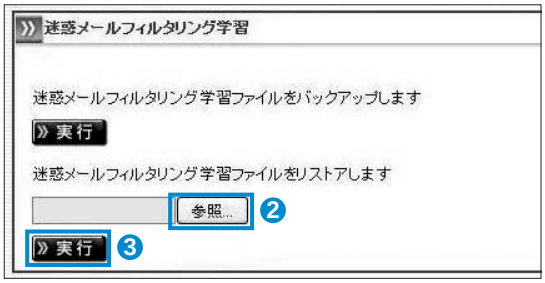


図6-5

リストア完了後は即座に迷惑メールフィルタリング学習状況が反映されます。

迷惑メールフィルタリング学習状況の確認はP70を参照してください。

リストアに失敗した場合、以下の項目をご確認ください。
・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。

迷惑メールフィルタスコアリング学習状況のバックアップ手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「迷惑メールスコアリング」の**「実行」**をクリックすると、システム設定ファイルがダウンロードされます。

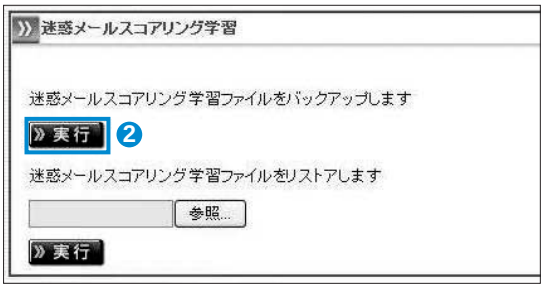


図6-6

> ファイルの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。

> ダウンロードしたファイルを編集すると、正常にリストアできなくなります。
> ダウンロードしたファイルは編集を行わずそのまま保管してください。

迷惑メールスコアリング学習状況のリストア手順

❶【運用管理】→【バックアップ／リストア】を選択します。

❷「迷惑メールスコアリング学習」のファイル入力欄にバックアップ手順にて取得した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。

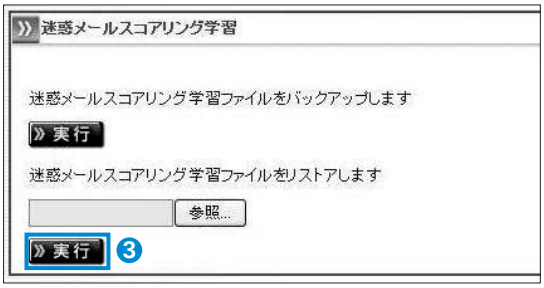


図6-7

❸**「実行」**をクリックすると迷惑メールスコアリング学習状況のリストアが開始されます。

> リストア完了後は即座に迷惑メールスコアリング学習状況が反映されます。

迷惑メールスコアリング学習状況の確認はP73を参照してください。

> リストアに失敗した場合、以下の項目をご確認ください。
> ・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。

3. ファームウェア

Sentinel 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/product/index.html

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、P75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Sentinel 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

Sentinel Beagleのファームウェアのバージョンは
下記手順で確認することができます。

❶【運用管理】→【ファームウェア】を選択します。

❷バージョン欄にファームウェアバージョンおよび
ウイルスチェックデータベースバージョンが表示されます。

図6-8

ファームウェアのアップデート手順

本手順はSentinel Beagleの再起動が発生します。

❶最新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/product/index.html

❷【運用管理】→【ファームウェア】を選択します。

❸ファームウェアアップグレード欄のアップロードURL、ユーザー名、パスワードを入力し、**「実行」**をクリックしてください。ファームウェアがダウンロードされます。

ファームウェアが正常にダウンロードできない場合は、アップロードURL、ユーザー名、パスワードを再度確認してください。

❹ファームウェアのダウンロードが完了後、アップデートの実施のため**「実行」**をクリックしてください。
アップデートが始まります。

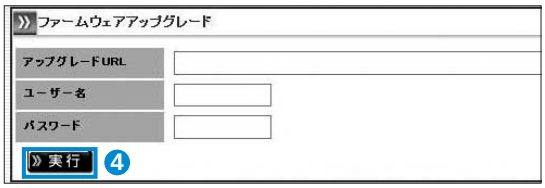


図6-9

❺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。再起動後は「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。

4. 初期化

システム設定初期化

システム設定を工場出荷時に初期化します。

システム設定初期化後は再起動が実行されます。

❶【運用管理】→【初期化】を選択します。

❷「実行」をクリックします。

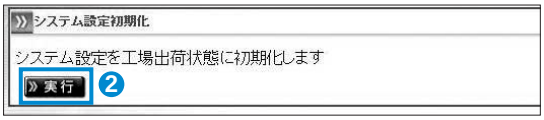


図6-10

迷惑メールフィルタリング学習状況初期化

迷惑メールフィルタリング学習状況を初期化します。

❶【運用管理】→【初期化】を選択します。

❷「実行」をクリックします。

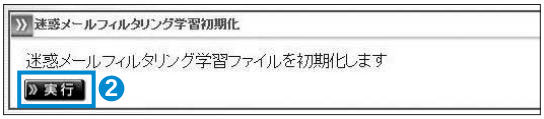


図6-11

迷惑メールスコアリング学習状況初期化

迷惑メールスコアリング学習状況を初期化します。

❶【運用管理】→【初期化】を選択します。

❷「実行」をクリックします。

図6-12

メールログ初期化

メールログを初期化します。

❶【運用管理】→【初期化】を選択します。

❷「実行」をクリックします。

図6-13

5. サポート情報取得機能

Sentinel Beagleの動作について弊社で調査を行う場合に、取得してご提供いただく場合に使用します。

サポート情報取得手順

❶【運用管理】→【サポート情報取得】を選択します。

❷「**実行**」をクリックするとサポート情報のダウンロードが開始されます。

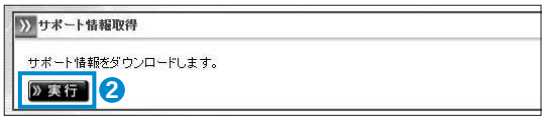


図6-14

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。

第7章

管理画面の機能説明

1．ログイン画面

1 Sentinel Beagleのログイン画面を表示します。

ブラウザにて以下のURLを入力します。

https://【Sentinel BeagleのIPアドレス】:18180/

図7-1

2 Sentinel 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。

ログインに成功すると、管理画面が表示されます。

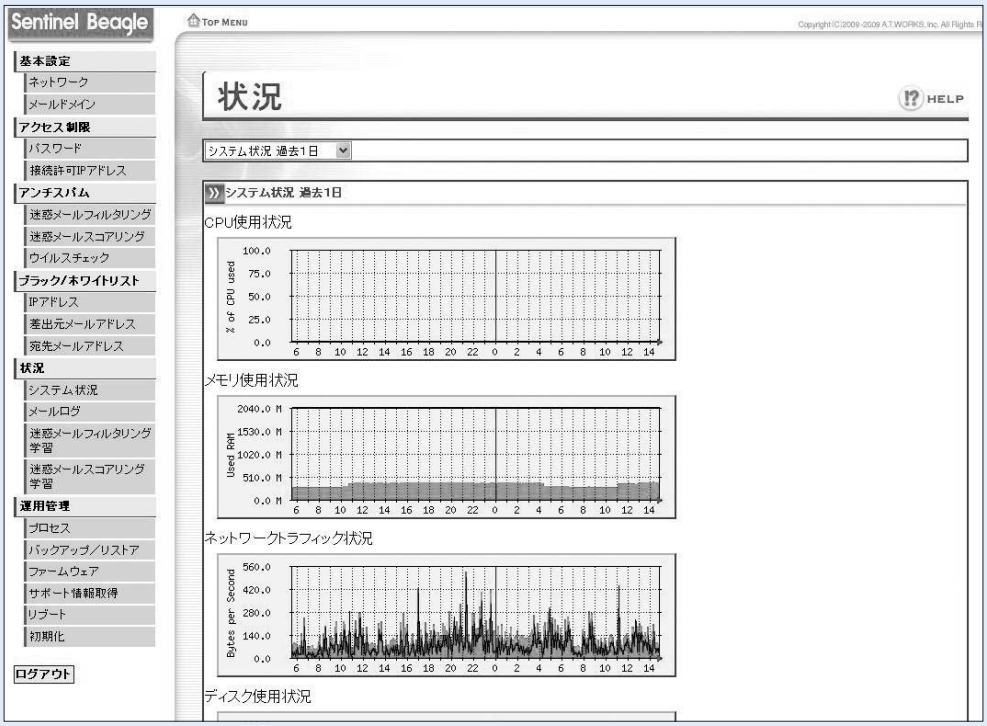


図7-2

■設定

❶ネットワーク

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

P52

❷メールドメイン

Sentinel Beagleにて迷惑メール対策を行うメールドメインとメールサーバを設定します。

P54

図7-3

■アクセス制限

❸パスワード

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。

P55

❹接続許可IPアドレス

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。

P56

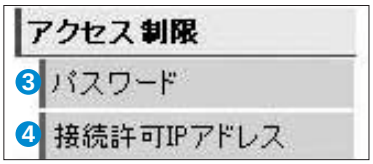


図7-4

■アンチスパム

❺迷惑メールフィルタリング

迷惑メールフィルタリング設定を表示･設定する場合に使用します。

P57

❻迷惑メールスコアリング

迷惑メールスコアリング設定を表示･設定する場合に使用します。

P59

❼ウイルスチェック

ウイルスチェック設定を表示･設定する場合に使用します。

P61

図7-5

■ブラック／ホワイトリスト

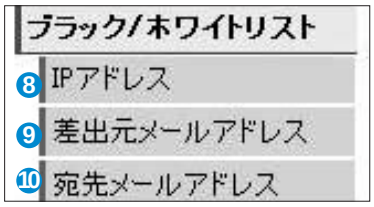


図7-6

⑧ IPアドレス

送信元IPアドレスのブラック／ホワイトリストを表示・設定する場合に使用します。

P63

⑨ 差出元メールアドレス

差出元メールアドレスのブラック／ホワイトリストを表示・設定する場合に使用します。

P64

⑩ 宛先メールアドレス

宛先メールアドレスのブラック／ホワイトリストを表示・設定する場合に使用します。

P65

■状況

図7-7

⑪ システム状況

システムの各種リソースの状況およびメール処理状況を表示する場合に使用します。

P66

⑫ メールログ

Sentinel Beagleが処理したメールログを表示・検索する場合に表示する場合に使用します。

P68

⑬ 迷惑メールフィルタリング学習

迷惑メールフィルタリング学習状況を表示する場合に使用します。

P70

⑭ 迷惑メールスコアリング学習

迷惑メールスコアリング学習状況を表示する場合に使用します。

P73

■運用管理

⑮プロセス

各種プロセスの稼働状況を表示、またプロセスの起動・停止を行う場合に使用します。

P74

⑯バックアップ／リストア

Sentinel Beagleの設定情報、迷惑メールフィルタリング学習状況、迷惑メールスコアリング学習状況のバックアップ／リストアを行う場合に使用します。

P75

⑰ファームウェア

ファームウェア情報の表示、及びファームウェアのアップデートを行う場合に使用します。

P76

⑱サポート情報取得

サポート情報を取得する場合に使用します。

P77

⑲リブート

Sentinel Beagleの再起動を行う場合に使用します。

P78

⑳初期化

Sentinel Beagleの設定情報、迷惑メールフィルタリング学習状況、迷惑メールスコアリング学習状況の初期化を行う場合に使用します。

P78

㉑ログアウト

Sentinel Beagleの管理画面からログアウトします。

図7-8

図7-9

2. 基本設定

ネットワーク

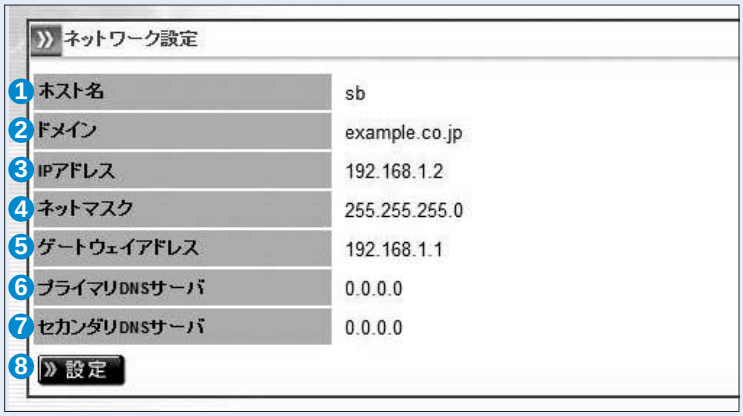


図7-10

❶ホスト名
Sentinel Beagleのホスト名を設定します。

❷ドメイン
Sentinel Beagleのドメイン名を設定します。

❸IPアドレス
Sentinel BeagleのIPアドレスを設定します。

❹ネットマスク
Sentinel Beagleのネットマスクを表示します。

❺ゲートウェイアドレス
Sentinel Beagleのゲートウェイを表示します。

❻プライマリDNSサーバ
Sentinel Beagleの参照する主系統のDNSサーバを表示します。

❼セカンダリDNSサーバ
Sentinel Beagleの参照する副系統のDNSサーバを表示します。

❽【設定】
Sentinel Beagleのネットワーク設定の変更画面に移ります。

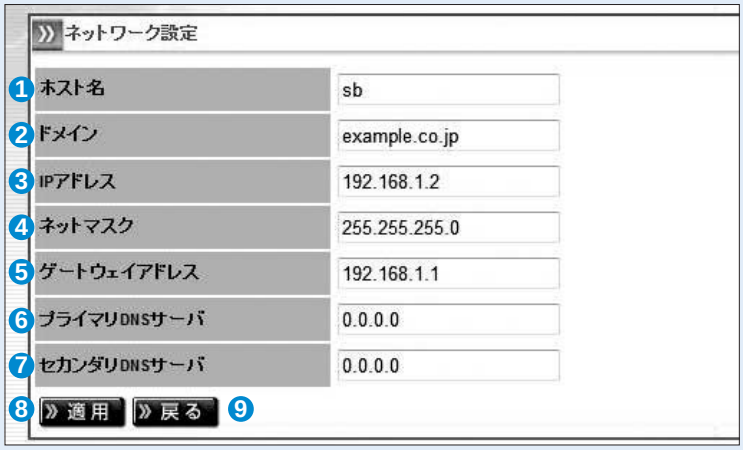


図7-11

❶ホスト名

Sentinel Beagleのホスト名を設定します。

❷ドメイン

Sentinel Beagleのドメイン名を設定します。

❸IPアドレス

Sentinel BeagleのIPアドレスを設定します。

❹ネットマスク

Sentinel Beagleのネットマスクを設定します。

❺ゲートウェイアドレス

Sentinel Beagleのゲートウェイを設定します。

❻プライマリDNSサーバ

Sentinel Beagleの参照する主系統のDNSサーバを設定します。

❼セカンダリDNSサーバ

Sentinel Beagleの参照する副系統のDNSサーバを設定します。

❽【適用】

Sentinel Beagleに設定を適用します。

❾【戻る】

Sentinel Beagleのネットワーク設定の表示画面に移ります。

メールドメイン

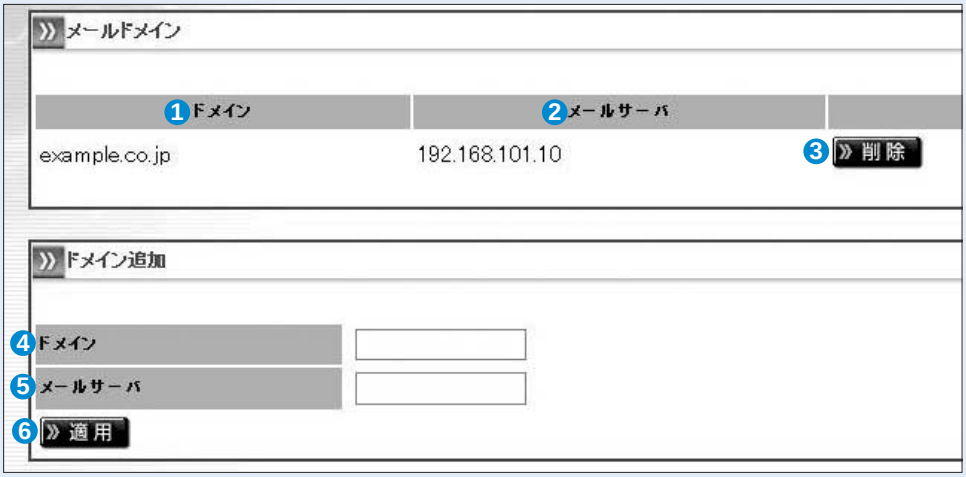


図7-12

❶ドメイン

Sentinel Beagleがメールを受け付けるドメインを表示します。

❷メールサーバ

Sentinel Beagleが受け付けたメールを転送するメールサーバを表示します。

❸【削除】

受け付けるドメインと転送先メールサーバを削除します。

Sentinel Beagleはメールドメインに登録されていないドメイン宛のメールは全て拒否します。

❹ドメイン

追加するドメインを指定します。

❺メールサーバ

追加するメールサーバを指定します。

❻【適用】

Sentinel Beagleに設定を適用します。

3．アクセス制限

パスワード

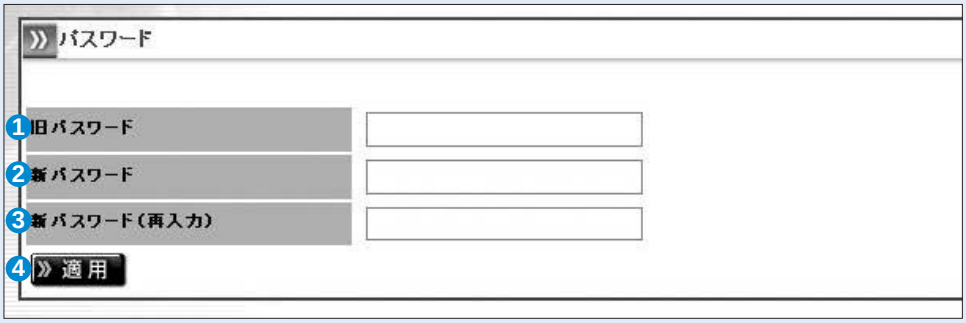


図7-13

❶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。

❷新パスワード

新しいパスワードを入力します。英数字だけが使用可能です。

❸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。

❹【適用】

Sentinel 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

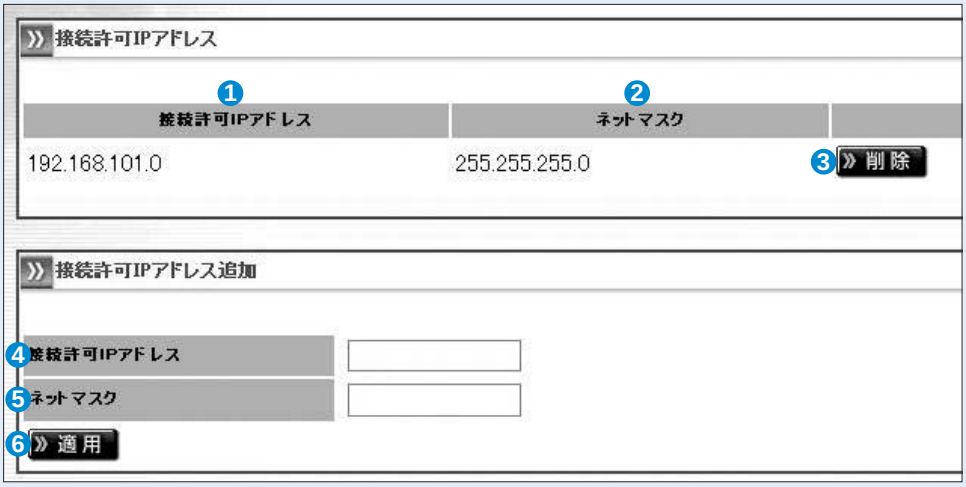


図7-14

❶接続許可IPアドレス

Sentinel Beagleの管理画面に接続を許可するIPアドレスまたはネットワークアドレスを表示します。

❷ネットマスク

Sentinel Beagleの管理画面に接続を許可するネットワークのネットマスクを表示します。

❸【削除】

Sentinel Beagleの管理画面に接続を許可するIPアドレスまたはネットワークアドレスを削除します。

❹接続許可IPアドレス

追加するIPアドレスまたはネットワークアドレスを指定します。

❺ネットマスク

追加するネットマスクを指定します。

❻【適用】

Sentinel Beagleの管理画面に接続を許可するIPアドレスまたはネットワークアドレスを追加します。

設定はただちに反映されます。

4. アンチスパム

迷惑メールフィルタリング

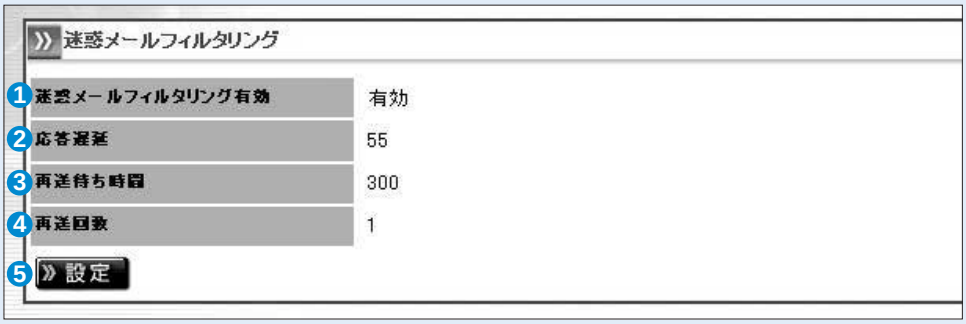


図7-15

❶迷惑メールフィルタリング有効

迷惑メールフィルタリング機能の有効／無効を表示します。

❷応答遅延

メールの配送要求に対して応答を遅延する時間を表示します。

❸再送待ち時間

メールの配送要求に対して再送要求を行った場合、メールの再送を受け入れない時間を表示します。

❹再送回数

メールの配送要求に対して再送要求を行う回数を表示します。

❺【設定】

迷惑メールフィルタリングの設定画面に移ります。

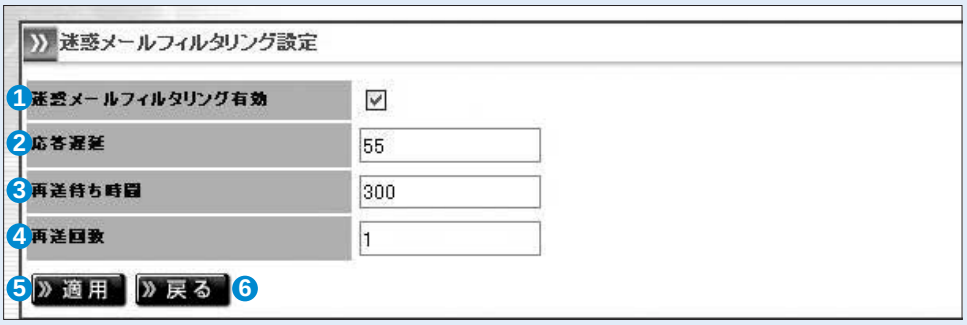


図7-16

❶ 迷惑メールフィルタリング有効

迷惑メールフィルタリング機能を有効にするには、このチェックボックスにチェックを入れます。

❷ 応答遅延

メールの配送要求に対して応答を遅延する時間を設定します。

❸ 再送待ち時間

メールの配送要求に対して再送要求を行った場合、メールの再送を受け入れない時間を設定します。

❹ 再送回数

メールの配送要求に対して再送要求を行う回数を設定します。

❺【適用】

Sentinel Beagleに設定を適用します。

❻【戻る】

迷惑メールフィルタリングの表示画面に移ります。

迷惑メールスコアリング

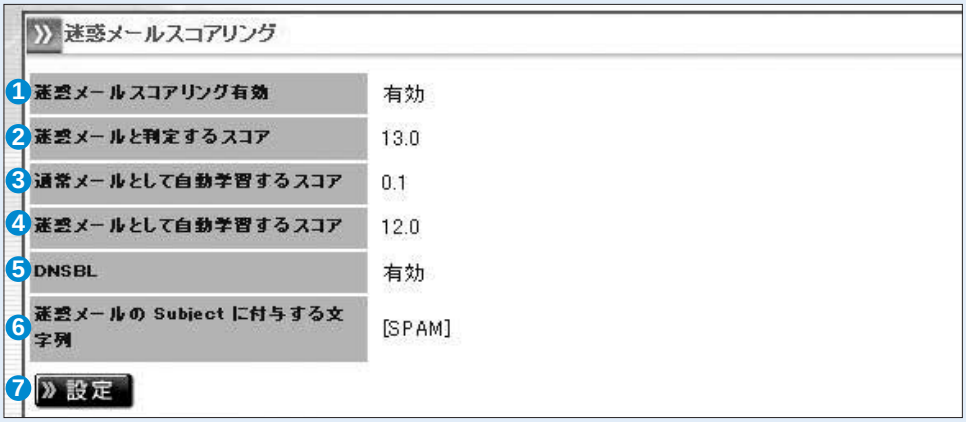


図7-17

❶迷惑メールスコアリング有効

迷惑メールフィルタリング機能の有効／無効を表示します。

❷迷惑メールと判定するスコア

迷惑メールと判定する下限のスコアを表示します。

❸通常メールとして自動学習するスコア

通常メールとして学習する上限のスコアを表示します。

❹迷惑メールとして自動学習するスコア

迷惑メールとして学習する下限のスコアを表示します。

❺DNSBL

DNSBLの有効／無効を表示します。

❻迷惑メールのSubjectに付与する文字列

迷惑メールと判定した場合にメールのSubjectに付与する文字列を表示します。

❼【設定】

迷惑メールスコアリングの設定画面に移ります。

図7-18

❶迷惑メールスコアリング有効

迷惑メールフィルタリング機能を有効にするには、このチェックボックスにチェックを入れます。

❷迷惑メールと判定するスコア

迷惑メールと判定するスコアを指定します。
対象メールのスコアがこの値以上であれば、迷惑メールと判定します。

❸通常メールとして自動学習するスコア

通常メールとして自動学習するスコアを指定します。
対象メールのスコアがこの値未満であれば、通常メールとして学習します。

❹迷惑メールとして自動学習するスコア

迷惑メールとして自動学習するスコアを指定します。
対象メールのスコアがこの値以上であれば、迷惑メールとして学習します。

❺DNSBL

DNSBL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。

DNSBLとは迷惑メールを送信した差出元IPアドレスのリストです。
対象メールの差出元がこのリストに含まれていれば、対象メールのスコアを加算します。

❻迷惑メールのSubjectに付与する文字列

迷惑メールと判定した場合にメールのSubjectに付与する文字列を指定します。

❼【適用】

Sentinel Beagleに設定を適用します。

❽【戻る】

迷惑メールスコアリングの表示画面に移ります。

ウイルスチェック

図7-19

❶ウイルスチェックを有効

ウイルスチェック機能の有効／無効を表示します。

❷ウイルス検出時の動作

ウイルスを検出した場合の対象メールの扱いを表示します。

❸ウイルス検出通知有効

ウイルスを検出した場合、メール通知する機能の有効／無効を表示します。

❹ウイルス検出通知差出元メールアドレス

ウイルス検出通知メールの差出元メールアドレスを表示します。

❺ウイルス検出通知宛先メールアドレス

ウイルス検出通知メールの宛先メールアドレスを表示します。

❻【設定】

ウイルスチェックの設定画面に移ります。

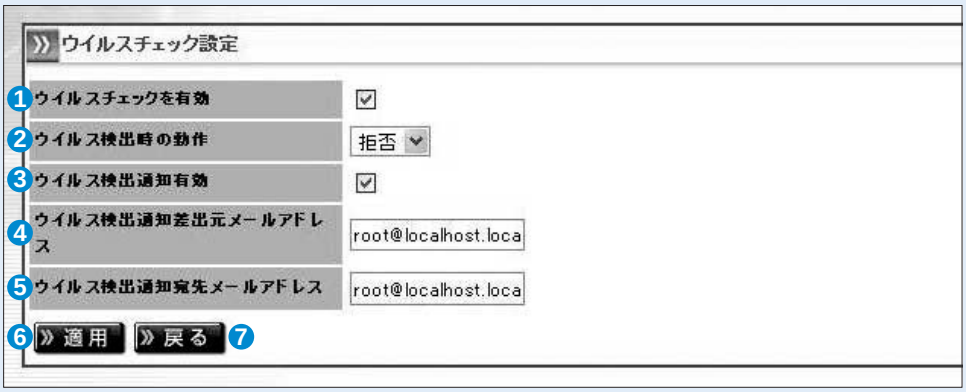


図7-20

❶ウイルスチェックを有効

ウイルスチェック機能を有効にするには、このチェックボックスにチェックを入れます。

❷ウイルス検出時の動作

ウイルスを検出した場合の対象メールの扱いを設定します。

許可	対象メールをメールサーバに転送します。
拒否	対象メールを差出元に返送します。
破棄	対象メールを破棄します。

❸ウイルス検出通知有効

ウイルスを検出した場合、メール通知する機能を有効にするには、このチェックボックスにチェックを入れます。

❹ウイルス検出通知差出元メールアドレス

ウイルス検出通知メールの差出元メールアドレスを設定します。

❺ウイルス検出通知宛先メールアドレス

ウイルス検出通知メールの宛先メールアドレスを設定します。

❻【適用】

Sentinel Beagleに設定を適用します。

❼【戻る】

ウイルスチェックの表示画面に移ります。

5. ブラック／ホワイトリスト

IPアドレスブラック/ホワイトリスト

図7-21

❶IPアドレス

ブラック/ホワイトリストの対象となるIPアドレスを表示します。

❷動作

ブラック/ホワイトリストの対象であるIPアドレスからメールの配送要求があった場合の動作を表示します。

❸【削除】

ブラック/ホワイトリストからIPアドレスを削除します。

❹IPアドレス

ブラック/ホワイトリストの対象として追加するIPアドレスを指定します。

❺動作

ブラック/ホワイトリストの対象であるIPアドレスからメールの配送要求があった場合の動作を指定します。

許可	配送要求を受け入れ、迷惑メールフィルタリング、迷惑メールスコアリングの両者で通常メールと判定します。
タグ	配送要求を受け入れますが、メールのSubjectに迷惑メールと判定したタグ（識別文字列）を付与し、さらに迷惑メールであることを示す識別文字列（X-Spam-Flag: YES）をメールヘッダに追加します。
拒否	配送要求を受け入れず、メールを拒否します。

IPアドレス ブラック/ホワイトリストで対象となったメールは、差出元メールアドレス、宛先メールアドレスブラック/ホワイトリストでの判定が行われません。

❻【適用】

Sentinel Beagleに設定を適用します。

差出元メールアドレス ブラック/ホワイトリスト

図7-22

❶差出元メールアドレス

ブラック/ホワイトリストの対象となる差出元メールアドレスを表示します。

❷動作

ブラック/ホワイトリストの対象である差出元メールアドレスからメールの配送要求があった場合の動作を表示します。

❸【削除】

ブラック/ホワイトリストから差出元メールアドレスを削除します。

❹差出元メールアドレス

ブラック/ホワイトリストの対象として追加する差出元メールアドレスを指定します。

❺動作

ブラック/ホワイトリストの対象である差出元メールアドレスからメールの配送要求があった場合の動作を指定します。

許可	配送要求を受け入れ、迷惑メールフィルタリング、迷惑メールスコアリングの両者で通常メールと判定します。
タグ	配送要求を受け入れますが、メールのSubjectに迷惑メールと判定したタグ(識別文字列)を付与し、さらに迷惑メールであることを示す識別文字列(X-Spam-Flag: YES)をメールヘッダに追加します。
拒否	配送要求を受け入れず、メールを拒否します。

先に IPアドレス ブラック/ホワイトリストで対象となったメールは差出元メールアドレス ブラック/ホワイトリストでの判定が行われません。

差出元メールアドレス ブラック/ホワイトリストで対象となったメールは宛先メールアドレス ブラック/ホワイトリストでの判定が行われません。

❻【適用】

Sentinel Beagleに設定を適用します。

宛先メールアドレス ブラック/ホワイトリスト

図7-22

❶宛先メールアドレス

ブラック/ホワイトリストの対象となる宛先メールアドレスを表示します。

❷動作

ブラック/ホワイトリストの対象である宛先メールアドレスからメールの配送要求があった場合の動作を表示します。

❸【削除】

ブラック/ホワイトリストから宛先メールアドレスを削除します。

❹宛先メールアドレス

ブラック/ホワイトリストの対象として追加する宛先メールアドレスを指定します。

❺動作

ブラック/ホワイトリストの対象である宛先メールアドレスへのメールの配送要求があった場合の動作を指定します。

許可	配送要求を受け入れ、迷惑メールフィルタリング、迷惑メールスコアリングの両者で通常メールと判定します。
タグ	配送要求を受け入れますが、メールのSubjectに迷惑メールと判定したタグ(識別文字列)を付与し、さらに迷惑メールであることを示す識別文字列(X-Spam-Flag: YES)をメールヘッダに追加します。
拒否	配送要求を受け入れず、メールを拒否します。

先に IPアドレス、差出元メールアドレス ブラック/ホワイトリストで対象となったメールは宛先メールアドレス ブラック/ホワイトリストでの判定が行われません。

❻【適用】

Sentinel Beagleに設定を適用します。

6. 状況

システム状況

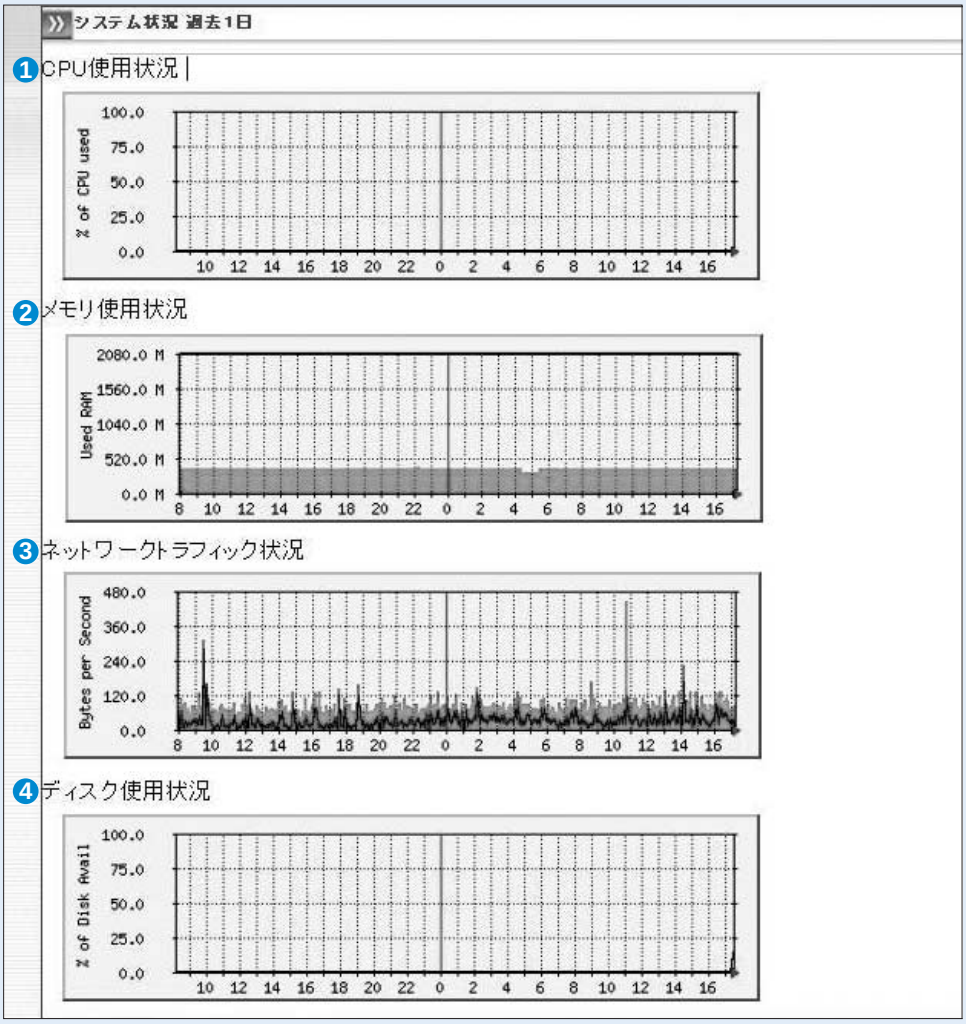


図7-23

Sentinel Beagleの過去1日、1週間、一ヶ月、一年のシステム状況を表示します。

1 CPU使用状況

Sentinel BeagleのCPU使用状況を表示します。

2 メモリ使用状況

Sentinel Beagleのメモリ使用状況を表示します。

3 ネットワークトラフィック状況

Sentinel Beagleのネットワークトラフィック状況状況を表示します。

緑線は受信トラフィック、青線は送信トラフィックを表示します。

4 ディスク使用状況

Sentinel Beagleのディスク使用状況を表示します。

■メールグラフ

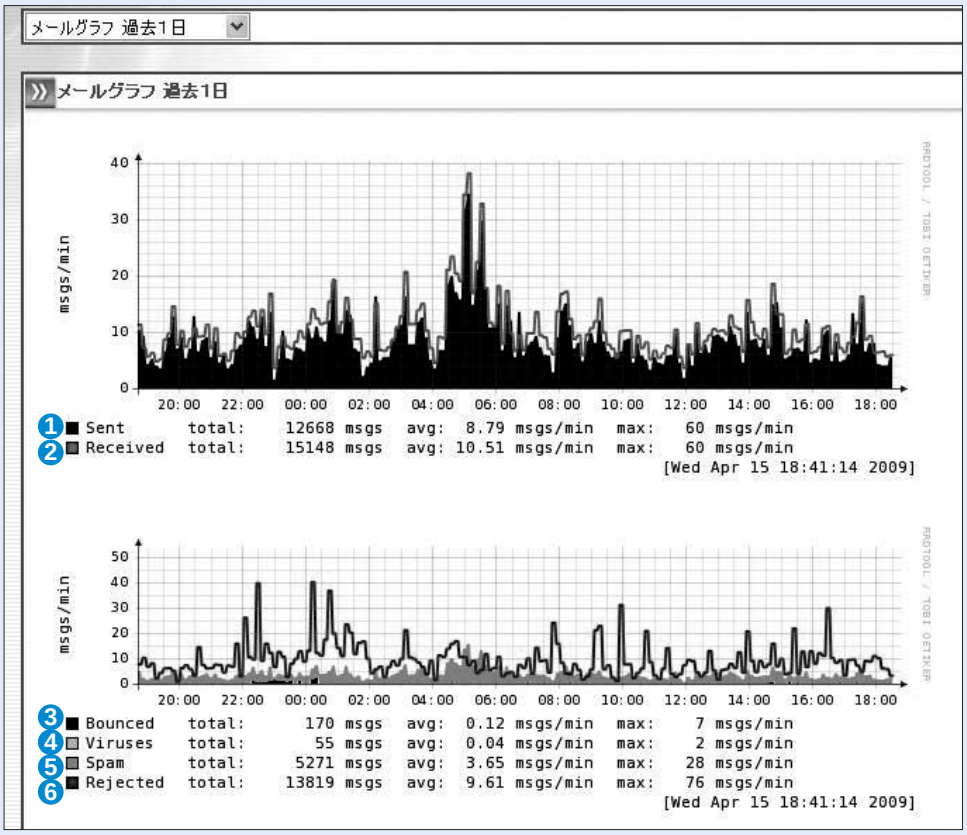


図7-24

Sentinel Beagleの過去1日、1週間、一ヶ月、一年のメール処理状況を表示します。

❶Sent
Sentinel Beagleから送信したメール数を表示します。

❷Received
Sentinel Beagleが受信したメール数を表示します。

❸Bounced
メール処理の結果、差出元に返送したメール数を表示します。

❹Viruses
メール処理の結果、ウイルスを含んでいるメール数を表示します。

❺Spam
メール処理の結果、迷惑メールと判定したメール数を表示します。

❻Rejected
メール処理の結果、拒否したメール数を表示します。

メールログ

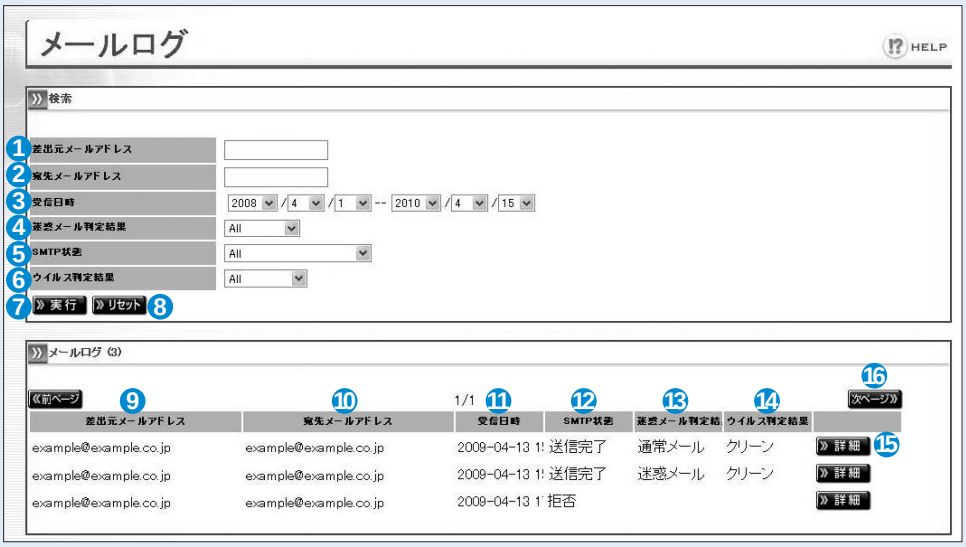


図7-25

❶差出元メールアドレス
検索対象の差出元メールアドレスを指定します。

❷宛先メールアドレス
検索対象の宛先メールアドレスを指定します。

❸受信日時
検索する期間を指定します。

❹迷惑メール判定結果
検索対象のメール判定結果を指定します。

❺SMTP状態
検索対象のSMTP状態を指定します。

❻ウイルス判定結果
検索対象のウイルス判定結果を指定します。

❼【実行】
指定の条件でメールログを検索します。

❽【リセット】
検索条件をリセットします。

❾差出元メールアドレス
差出元メールアドレスを表示します。

❿宛先メールアドレス
宛先メールアドレスを表示します。

⓫受信日時
メールを受信した日時を表示します。

⓬SMTP状態
SMTP状態を表示します。

⓭迷惑メール判定結果
迷惑メール判定結果を表示します。

⓮ウイルス判定結果
ウイルス判定結果を表示します。

⓯【詳細】
詳細な判定結果の表示画面に移ります。

⓰【前ページ】【次ページ】
検索結果が多数の場合に改ページを行います。

■メール情報詳細

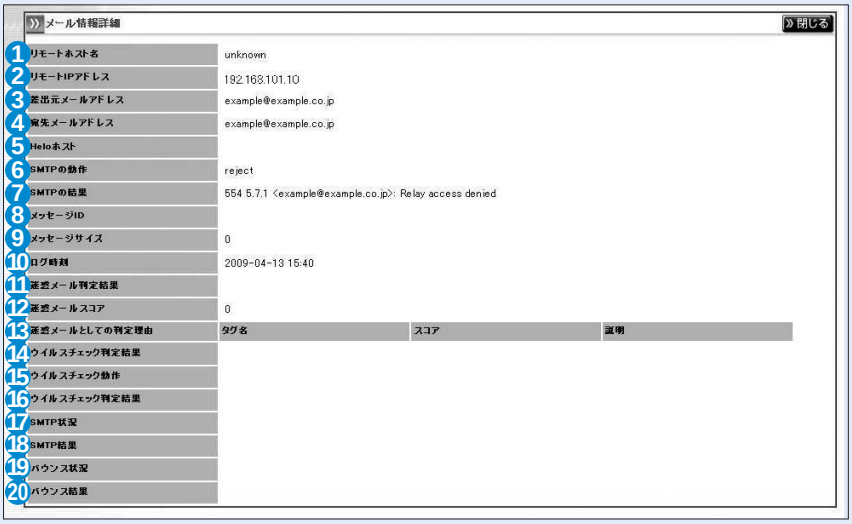


図7-26

❶リモートホスト名
リモートホスト名を表示します。

❷リモートIPアドレス
リモートIPアドレスを表示します。

❸差出元メールアドレス
差出元メールアドレスを表示します。

❹宛先メールアドレス
宛先メールアドレスを表示します。

❺Heloホスト
Heloホストを表示します。

❻SMTPの動作
SMTPの動作を表示します。

❼SMTPの結果
SMTPの結果を表示します。

❽メッセージID
メッセージIDを表示します。

❾メッセージサイズ
メッセージサイズを表示します。

❿ログ時刻
ログ時刻を表示します。

⓫迷惑メール判定結果
迷惑メール判定結果を表示します。

⓬迷惑メールスコア
迷惑メールスコアを表示します。

⓭迷惑メールとしての判定理由
迷惑メールとしての判定理由を表示します。

⓮ウイルスチェック判定結果
ウイルスチェック判定結果を表示します。

⓯ウイルスチェック動作
ウイルスチェック動作を表示します。

⓰ウイルスチェック判定結果
ウイルスチェック判定結果を表示します。

⓱SMTP状況
SMTP状況を表示します。

⓲SMTP結果
SMTP結果を表示します。

⓳バウンス状況
バウンス状況を表示します。

⓴バウンス結果
バウンス結果を表示します。

迷惑フィルタリング学習

■グレイリスティング状況

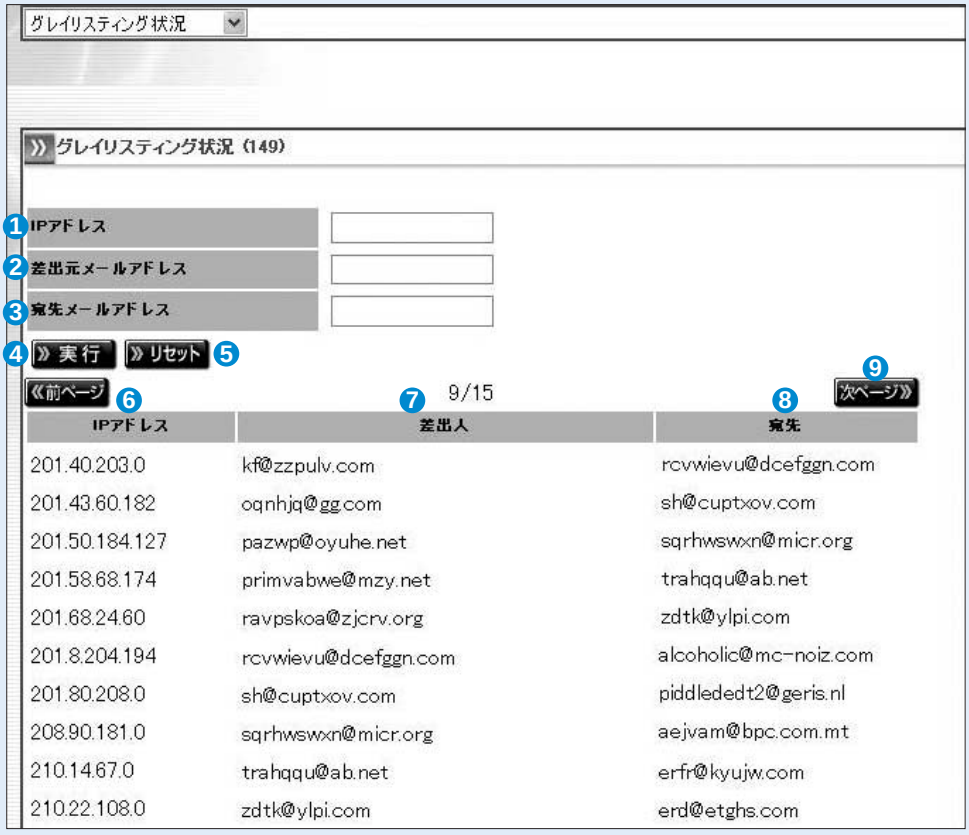


図7-27

❶ IPアドレス
検索対象の差出元IPアドレスを指定します。

❷ 差出元メールアドレス
検索対象の差出元メールアドレスを指定します。

❸ 宛先メールアドレス
検索対象の宛先メールアドレスを指定します。

❹【実行】
指定の条件でグレイリスティング状況を検索します。

❺【リセット】
検索条件をリセットします。

❻ IPアドレス
差出元IPアドレスを表示します。

❼ 差出元メールアドレス
差出元メールアドレスを表示します。

❽ 宛先メールアドレス
宛先メールアドレスを表示します。

❾【前ページ】【次ページ】
検索結果が多数の場合に改ページを行います。

■応答遅延状況

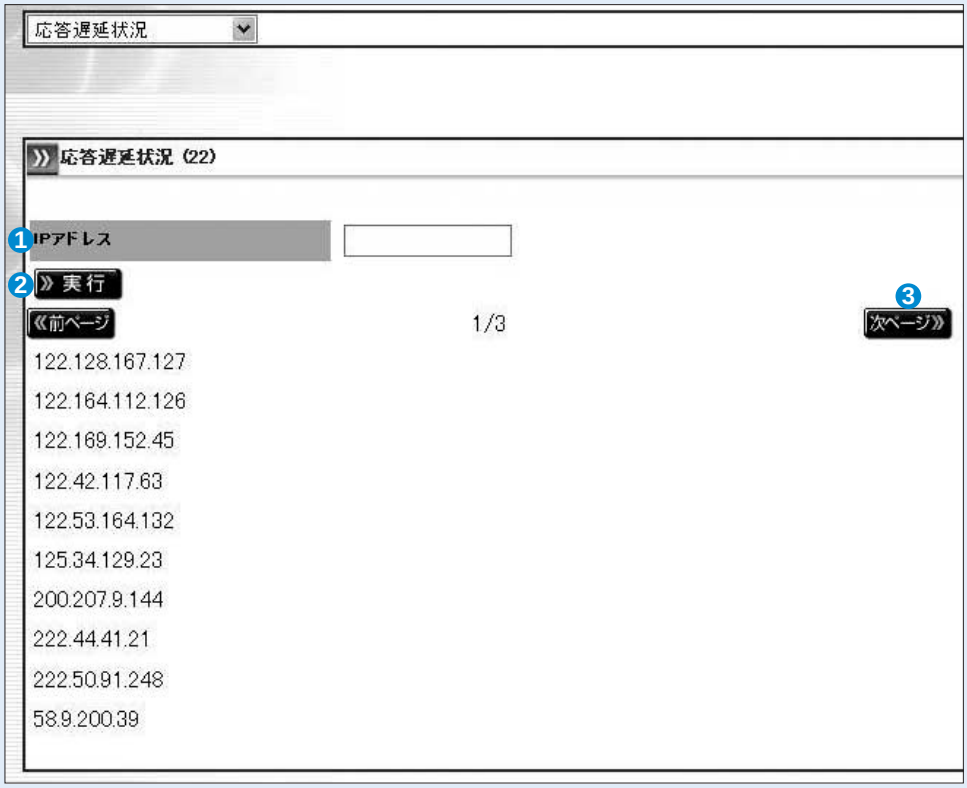


図7-28

❶IPアドレス

検索対象の差出元IPアドレスを指定します。

❷【実行】

指定の条件で接続元ホワイトリスト状況を検索します。

❸【前ページ】【次ページ】

検索結果が多数の場合に改ページを行います。

■接続元ホワイトリスト状況

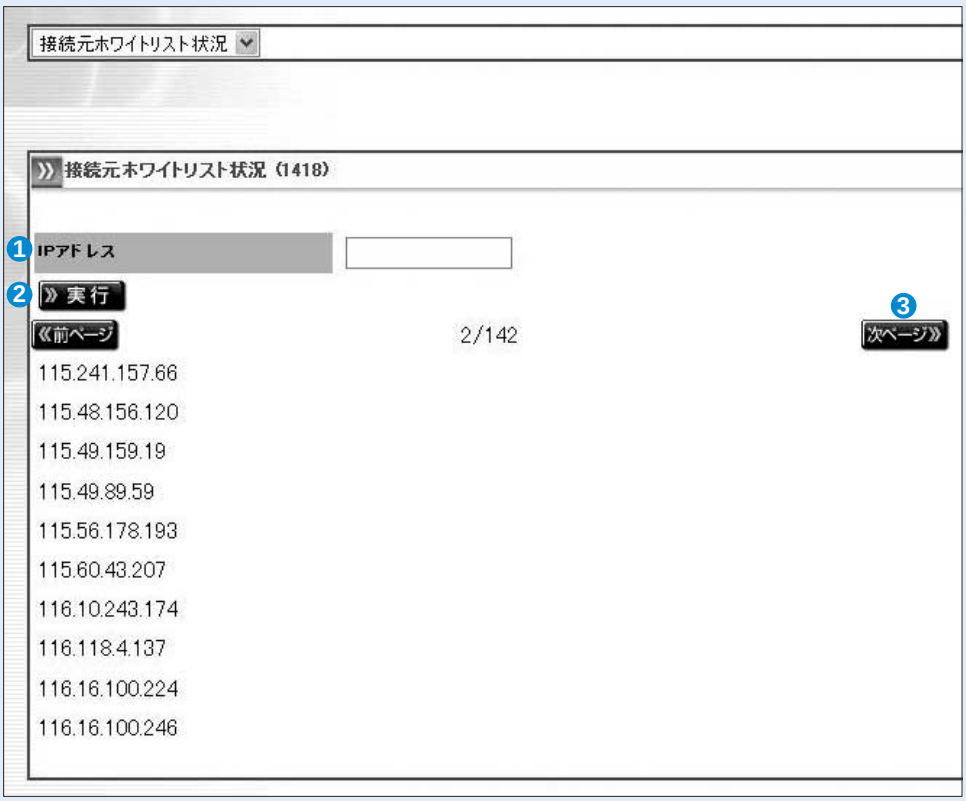


図7-29

❶IPアドレス

検索対象の差出元IPアドレスを指定します。

❷【実行】

指定の条件で接続元ホワイトリスト状況を検索します。

❸【前ページ】【次ページ】

検索結果が多数の場合に改ページを行います。

迷惑メールスコアリング学習

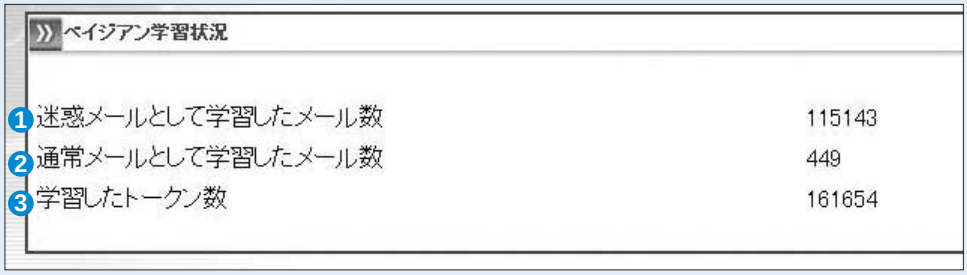


図7-30

❶迷惑メールとして学習したメール数
迷惑メールとして学習したメール件数です。

❷通常メールとして学習したメール数
通常メールとして学習したメール件数です。

❸学習したトークン数
迷惑メールによくみられる単語の学習数です。

7. 運用管理

プロセス

図7-31

❶ postfix
postfixの稼動状況を表示します。

❷ postgrey（taRgrey）
postgrey（taRgrey）の稼動状況を表示します。

❸ spamd（SpamAssassin）
spamd（SpamAssassin）の稼動状況を表示します。

❹ clamd（ClamAV）
clamd（ClamAV）の稼動状況を表示します。

❺ amavisd
amavisdの稼動状況を表示します。

❻【停止】
起動しているプロセスを停止します。

❼【起動】
停止しているプロセスを起動します。

❽【再起動】
プロセスを再起動します。

バックアップ／リストア

図7-32

❶【実行】
システム設定をバックアップします。

❷【参照】
システム設定のバックアップファイルを指定します。

❸【実行】
システム設定をリストアします。

❹【実行】
迷惑メールフィルタリング学習をバックアップします。

❺【参照】
迷惑メールフィルタリング学習のバックアップファイルを指定します。

❻【実行】
迷惑メールフィルタリング学習をリストアします。

❼【実行】
迷惑メールスコアリング学習をバックアップします。

❽【参照】
迷惑メールスコアリング学習のバックアップファイルを指定します。

❾【実行】
迷惑メールスコアリング学習をリストアします。

ファームウェア

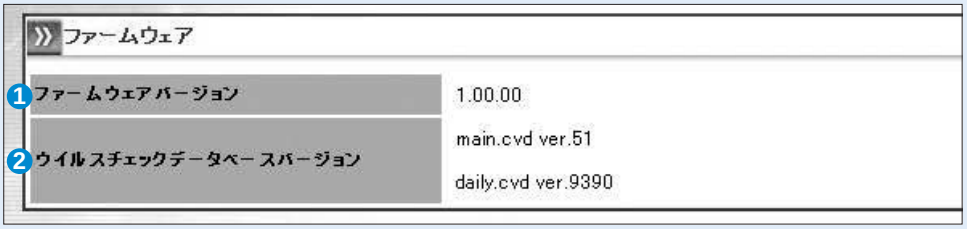


図7-33

1 ファームウェアバージョン

Sentinel Beagleのファームウェアバージョンを表示します。

2 ウイルスチェックデータベースバージョン

ウイルスチェック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グレード

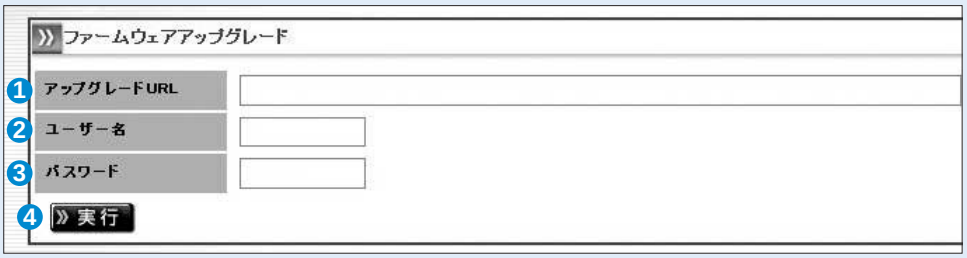


図7-34

1 アップグレードURL

Sentinel Beagleのファームウェアが格納されているURLを指定します。

2 ユーザー名

アップグレードURLに基本認証が施されている場合、ユーザー名を指定します。

3 パスワード

アップグレードURLに基本認証が施されている場合、パスワードを指定します。

4 【実行】

ファームウェアアップグレードを行います。

サポート情報取得

図7-35

❶【実行】
サポート情報をダウンロードします。

リブート

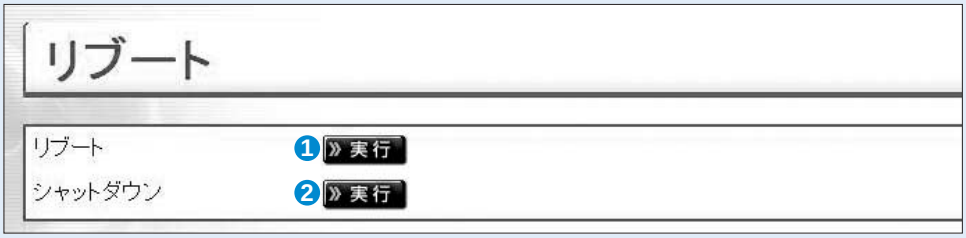


図7-36

❶【実行】
Sentinel Beagleを再起動します。

❷【実行】
Sentinel Beagleをシャットダウンします。

初期化

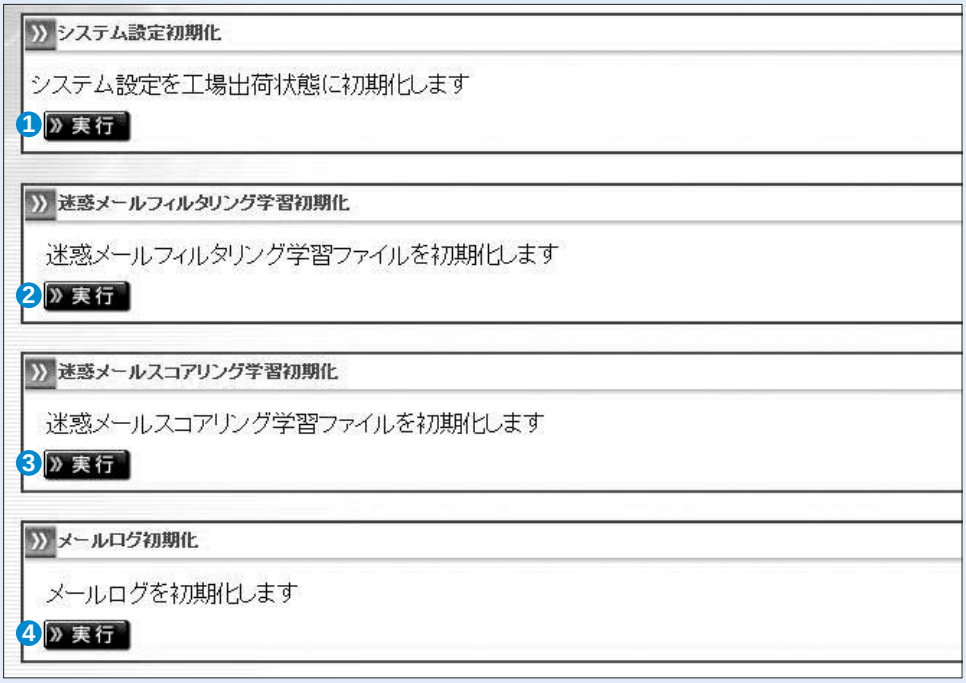


図7-37

❶【実行】
システム設定を工場出荷状態に初期化します。

❷【実行】
迷惑メールフィルタリング学習内容を初期化します。

❸【実行】
迷惑メールスコアリング学習内容を初期化します。

❹【実行】
メールログを初期化します。

第8章
コンソール管理

1. コンソール管理

Sentinel 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。

Sentinel Beagleにモニタ、キーボードを接続してください。

Sentinel Beagleのフロントパネルは P6を参照してください。

Sentinel 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。

ログインID	admin
パスワード	*******

```
login: admin
Password:
```

図8-1　ログイン画面

このログインIDとパスワードはSentinel 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。

```
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 -- Exit
Please input [1-8]:
```

図8-2　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

Sentinel 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。

```
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 -- Shutdown
9 -- Exit
Please input [1-9]: 1

Do you want to initialize the configuration?[y/n]:y
```

図8-3　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。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 2

Input new password: newpassword
```

図8-4　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

Sentinel 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。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 3

Input new IP address: 192.168.1.2

Input new Netmask: 255.255.255.0

Input new Gateway: 192.168.1.1
```

図8-5　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

Sentinel BeagleのWebインタ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インタフェイスにて再度アクセス制限を行ってください。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 4

Do you want to clear allowed IP?[y/n]: y

Allowed IP cleared.
```

図8-6　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

ネットワーク設定を確認したい場合、管理メニューにて 5 を入力します。
現在のネットワーク設定が表示されます。

```
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 -- Shutdown
9 -- Exit
Please input [1-9]: 5

Current Setting:
IP Address:          192.168.0.10
Net Mask:            255.255.255.0
Default Gateway:     192.168.0.1
```

図8-7　ネットワーク設定確認

ネットワークの疎通を確認したい場合

Sentinel Beagleのネットワークの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。
対象のIPアドレスとの疎通結果が表示されます。
もし疎通結果が失敗していた場合（図6-9）、Sentinel Beagleのネットワーク設定やネットワークの配線をみなおしてください。

```
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 -- Shutdown
9 -- Exit
Please input [1-9]: 6

Input destination IP address: 192.168.0.1
PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=128 time=1.5 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=128 time=1.5 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=128 time=1.1 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=128 time=1.6 ms

-- 192.168.24.1 ping statistics --
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.4/1.6 ms
```

図8-8　ネットワーク疎通確認（疎通成功）

```
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 -- Shutdown
9 -- Exit
Please input [1-9]: 6

Input destination IP address: 192.168.0.100
PING 192.168.0.100 (192.168.0.100): 56 data bytes

-- 192.168.0.100 ping statistics --
4 packets transmitted, 0 packets received, 100% packet loss
```

図8-9　ネットワーク疎通確認（疎通失敗）

Sentinel Beagleを再起動したい場合

Sentinel Beagleを再起動する場合、管理メニューにて 7 を入力します。
再起動してよい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。
Sentinel Beagleは再起動されます。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 7

Do you want to reboot the system?[y/n]:y

Please wait for system rebooting...
```

図8-10　Sentinel Beagleの再起動

Sentinel Beagleをシャットダウンしたい場合

Sentinel Beagleをシャットダウンする場合、管理メニューにて 8 を入力します。
シャットダウンしてよい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。
Sentinel Beagleはシャットダウンされます。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 8

Do you want to shutdown the system?[y/n]: y

Please wait for system shuting down...
```

図8-11　Sentinel Beagleをシャットダウン

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。

```
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 – Shutdown
9 – Exit
Please input [1-9]: 9

Login:
```

図8-12　コンソール管理メニューの終了

付録A. 仕様

Sentinel Beagle

ネットワークインターフェース	1000BASE-T（4ポート）※1	
機能	迷惑メールフィルタリング	
	ウイルスチェック	
	迷惑メールスコアリング	
メールドメイン最大登録数	50	
同時メール処理数	100	
使用電力	AC100V（50／60Hz）	
平均電力消費量	30W	
寸法	単体 42.4（H）×217（W）×365（D）mm	※2
	冗長構成時 44.45（H）×441（W）×365（D）mm（ラックマウントキットを含む）	
質量	単体 3kg	
	冗長構成時 9.8kg（ラックマウントキットを含む）	
付属品	電源ケーブル、Sentinel Beagle専用ラックマウントキット	
	Sentinel Beagle操作マニュアル	

（※1）ポートは1つのみ使用します。
（※2）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。

メモ

メモ

Sentinel Beagle Model 200 操作マニュアル

2012年6月1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
http://online.atworks.co.jp（オンラインショップページ）
http://www.at-link.ad.jp（at+link 専用サーバサービス）

株式会社 エーティーワークス