

Barracuda Spam Firewall User's Guide



著作権

Copyright 2004, Barracuda Networks
www.barracudanetworks.com

無断複写・転載を禁じます。本製品と本マニュアルを使用するには、ライセンスが必要です。本書に記載される情報は、予告なく変更されることがあります。

商標

バラクーダスパムファイアウォールはバラクーダネットワークスの商標です。本書に記載されるその他すべてのブランド名および製品名は、個々の所有者の登録商標または商標です。

安全にお使いいただくために

本製品を安全に正しくお使いいただき、お客様や他の人々への危害や財産への損害を未然に防ぐために、この説明書の記載内容を十分ご理解の上、必ずお守りください。



警告

この表示のある欄は「誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される」内容を示しています。



注意

この表示のある欄は「誤った取り扱いをすると、人が傷害を負ったり、物的損害が発生する可能性が想定される」内容を示しています。



この表示のある説明は、それが「禁止の行為」であることを告げるものです。



この表示のある説明は、それが「必要な行為」であることを告げるものです。

設置について

警告



本機にコップや花瓶など、水や液体が入った容器を置かないでください。

機器内に水や液体が入ると、故障や火災・感電の原因になります。水などをこぼした場合は使用を中止し、電源を切って、電源プラグを抜いてください。修理や技術的なご相談は、ネットワークサービスセンターへお問い合わせください。

注意



本機を湿気やほこりの多い場所、直射日光のあたる場所に置かないでください。

故障や火災・感電の原因になります。



本機を傾いた所など不安定な場所や振動の多い場所に置かないでください。

機器が落ちたり倒れたりして、ケガや故障の原因になります。水平な場所に設置してください。持ち運びは衝撃を与えないようご注意ください。



本機の上に重いものを載せたり、乗ったりしないでください。

故障や火災・感電の原因になります。

取扱について

警告



本機を絶対に分解・修理・改造などしないでください。

故障や火災・感電の原因になります。修理や技術的なご相談は、ネットワークサービスセンターへお問い合わせください。



異常（発熱・発煙・異臭など）が発生した場合は、すぐに電源スイッチを切り、電源プラグを抜いてください。

故障や火災・感電の原因になります。修理や技術的なご相談は、ネットワークサービスセンターへお問い合わせください。



異物（金属片・水・液体）が機器の内部に入った場合は、すぐに電源スイッチを切り、電源プラグを抜いてください。

故障や火災・感電の原因になります。修理や技術的なご相談は、ネットワークサービスセンターへお問い合わせください。

注意



本機を移動・接続するときは、電源スイッチを切ってください。

電源を入れたまま移動・接続すると、故障や感電の原因になります。



ベンジンやシンナーなど化学薬品を含んだ雑巾で手入れしないでください。

機器の塗装がはげたり、変質したりします。科学雑巾を使用するときは、その注意書きに従ってください。

電源について

警告



電源コードを強く引っ張ったり、重いものを載せたりしないでください。

傷ついた部分から漏電して、火災・感電の原因になります。



電源コードを傷つけたり、破損したり、束ねたり、加工したりしないでください。

傷ついた部分から漏電して、火災・感電の原因になります。



濡れた手で電源プラグを抜き差ししないでください。

感電によるケガや故障の原因になります。



電源プラグはコンセントの奥までしっかりと差し込んでください。

しっかり差し込まないと、感電や発熱による火災の原因になります。



タコ足配線を行ったり、100V以外の電源に接続したりしないでください。

故障や感電、発熱による火災の原因になります。



電源プラグのほこりを定期的に拭き取り、コンセント周辺のたまったほこりを取り除いてください。

ほこりがたまったままで使用していると、湿気などで絶縁不良となり、火災の原因になります。電源プラグやコンセント周辺のほこりは、乾いた布で拭き取ってください。

開梱時の注意

注意



本機を箱から取り出した際、機器本体に結露が発生した場合は、すぐに電源を入れしないでください。

機器を箱から取り出す際、冷えた機器本体が部屋の暖かい空気により結露が発生することがあります。結露があるまま電源を入れると、機器本体が破損したり、部品の寿命が短くなる場合があります。機器を取り出したら室温になじませてください。結露が発生した場合は、水滴が蒸発してから設置や接続の作業を行ってください。

目次

第1章 はじめに	5
概要	5
最小の管理労力で最大の保護力をもたらすエネルギー充填サービス	6
スパムスコアリングについて	7
バラクーダスパムファイアウォールのモデル	8
テクニカルサポート	8
保証方針	8
本書での情報の記載場所	9
第2章 バラクーダスパムファイアウォールの設定	11
バラクーダスパムファイアウォールの設置	11
システム IP アドレスの設定	12
バラクーダスパムファイアウォールの構成	12
ファイアウォールの設定とファームウェアの更新	14
MX レコードの変更による受信メールのルーティング	15
設置後の作業	15
設置例	16
バラクーダスパムファイアウォールをファイアウォールの内側に 配置する場合	16
バラクーダスパムファイアウォールをファイアウォールの前に 配置する場合	17
第3章 バラクーダスパムファイアウォールの管理	19
システムステータスと統計の表示	20
インジケータランプについて	20
システム統計の表示	21
受信メールのモニタリングと分類	22
管理者画面でのメールの分類	23
メールクライアントでのメールの分類	24
メッセージログについて	25
メールの詳細の表示	25
スパム設定の構成	26
グローバルスパムスコアリングの設定	26
件名テキストとタグ付きメールの優先度の指定	26
ウイルスチェックと通知の有効化 / 無効化	27
隔離の設定	28
隔離タイプの指定	28

グローバル隔離設定の指定	29
ユーザ単位隔離設定の指定	29
ユーザ単位隔離アカウント設定の変更	30
システム IP 情報の設定	31
管理者画面へのアクセス制御	32
管理者パスワードの変更	32
管理者画面へのアクセスの制限	32
ウェブインターフェースポートとセッション持続時間の変更	32
システムのシャットダウンとリセット	33
システムのシャットダウン	33
フロントパネルを使用して行うシステムのリセット	33
ページアンデータベースのリセット	33
システムレポート送付の自動化	34
ブラックリストサービスへの加入	34
ブラックリストサービスについて	35
拒否 / 許可フィルターの使用	36
IP アドレス / ネットワークによるフィルタリング	36
送信元ドメインによるフィルタリング	37
送信者メールアドレスによるフィルタリング	37
受信者メールアドレスによるフィルタリング	38
添付ファイルタイプによるフィルタリング	38
件名によるフィルタリング	39
本文の内容によるフィルタリング	40
ヘッダーの内容によるフィルタリング	40
システム設定のバックアップとリストア	41
システムデータのバックアップ	41
システムデータのリストア	42
エネルギー充填サービスを使用したスパムとウィルス定義の更新	43
管理者画面の外観のカスタマイズ	44
高度な設定の構成	45
フィンガープリンティングの動作の変更	45
メールプロトコル検査の設定	46
メッセージレートコントロールの設定	48
個別アカウントの有効化	48
システムファームウェアバージョンの更新	49
Syslog サーバを使用したシステムログの集中管理	49
クラスタ化環境の設定	50
シングルサインオンの導入	52
スパム設定のローカライズ	53
ドメインの管理と設定	53
新規ドメインの追加	53
ドメイン設定の編集	54
バラクーダ MS エクスチェンジアクセラレータを使用した辞書攻撃の阻止	55

ユーザアカウントの管理.....	56
ユーザアカウントの表示.....	56
ユーザアカウントへの機能の割り当て.....	58
新規ユーザアカウントの作成.....	59
ユーザ設定のバックアップとリストア.....	59
SSLの有効化.....	60
配送不能レポート（NDR）のカスタマイズ.....	61
トラブルシューティング.....	63
第4章 バラクーダスパムファイアウォールを使用した	
メールのフィルタリング.....	65
バラクーダスパムファイアウォールからのメールの受信.....	65
グリーティングメール.....	65
隔離サマリーレポート.....	65
隔離インターフェースの使用.....	66
隔離インターフェースへのログイン.....	66
隔離受信ボックスの管理.....	67
ユーザ設定の変更.....	68
アカウントパスワードの変更.....	68
隔離設定.....	68
メールのスパムスコアリングの有効化と無効化.....	69
ホワイトリストおよびブラックリストへのメールアドレスとドメインの追加.....	70
付録 A 正規表現について.....	71
正規表現での特殊文字の使用.....	72
例.....	72
索引.....	73

第 1 章 はじめに

この章ではバラクーダスパムファイアーウォールの概要を示します。この章は、以下のトピックで構成されます。

- 概要（本ページ）
- バラクーダスパムファイアーウォールのモデル（P.8）
- テクニカルサポート（P.8）
- 保証方針（P.8）
- 本書での情報の記載場所（P.9）

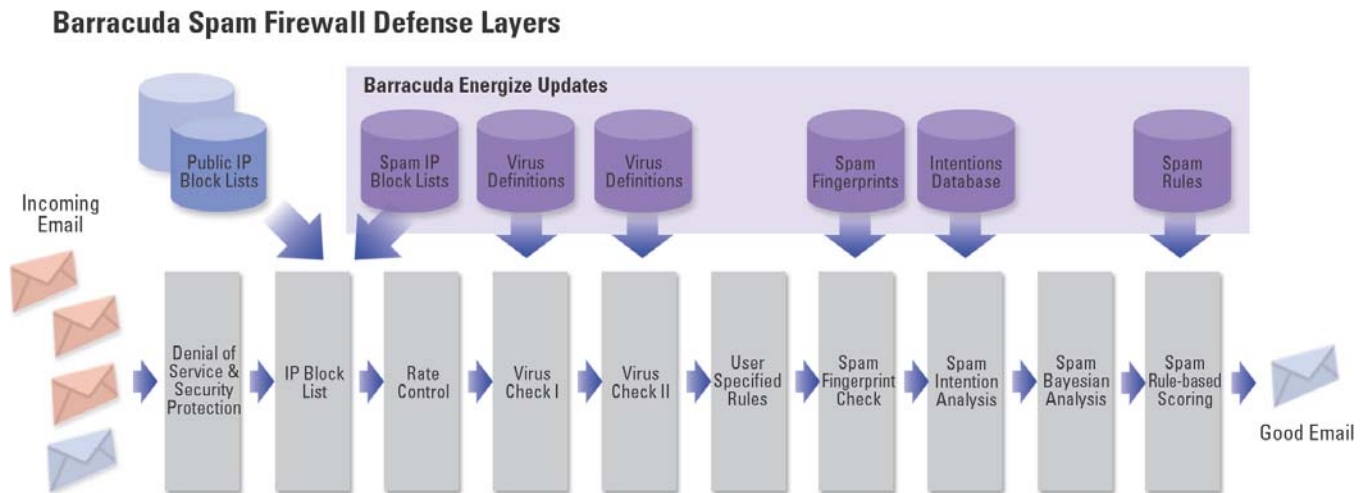
概要

バラクーダスパムファイアーウォールは、スパムとウィルスブロックするためのハードウェア/ソフトウェア統合ソリューションです。強力でスケーラブルなブロック機能を提供する本製品を導入すると、迷惑メールによるメールサーバの停止を防止することができます。このシステムではユーザごとのライセンス料は発生しませんので、一度お買い求めいただくだけで、数万人ものアクティブなメールユーザを同時にサポートすることができます。

ウェブベースの管理者画面を使用して、スパムやウィルスからユーザを保護するための防御層を最大 10 層まで構成できます。この 10 層の防御層には、以下のものが含まれます。

- サービス拒否攻撃（DoS）およびセキュリティ保護
- IP ブロックリスト
- レートコントロール
- アーカイブ解凍付きウィルスチェック
- バラクーダネットワークス独自のウィルスチェック
- ユーザ設定ルール
- スпамフィンガープリントチェック
- インテンション解析
- ベイジアン解析
- ルールベースのスパムスコアリング

下図は、各防御層の動作を示したものです。



最小の管理労力で最大の保護力をもたらすエネルギー充填サービス

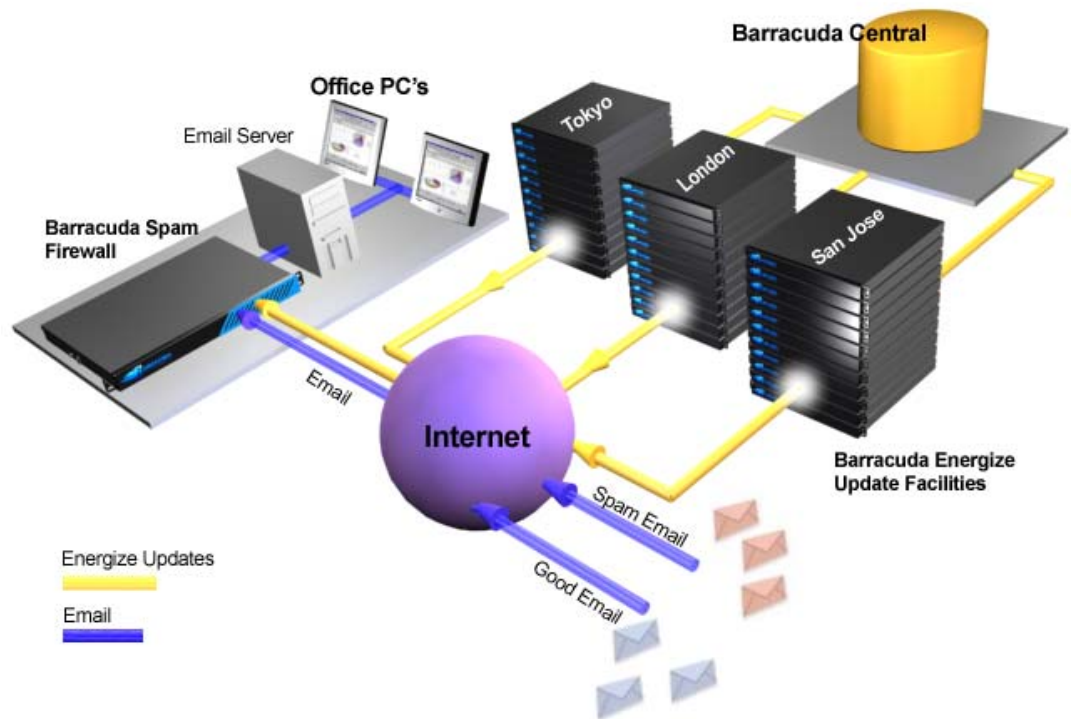
バラクーダネットワークスは、最新タイプのスパムとウィルスに対して最大の保護を提供するため、「バラクーダセントラル」と呼ばれる強力なオペレーションセンターを運営しています。このセンターでは、エンジニアがインターネットを常時監視してスパムやウィルスによる攻撃の最新動向を掴み、最新の定義をバラクーダセントラルに通知しています。更新データは、エネルギー充填サービスによって、組織内に導入されたバラクーダスパムファイアーウォールに自動的にダウンロードされます。

最新のスパム動向を早期に特定することにより、バラクーダセントラルでさらに改良されたブロック手法やウィルス定義をいち早く開発し、お手元のバラクーダスパムファイアーウォールに即座に提供することが可能になります。

エネルギー充填サービスは、お使いのバラクーダスパムファイアーウォールに以下の利点を提供します。

- 既知の攻撃元 IP アドレスへのアクセス
- 既知のスパムメッセージを即座にブロック
- 既知のスパムコンテンツをブロック
- ウィルス定義の常時更新

下図は、バラーダセントラルがバラーダエネルギー充填サービスを介して最新のスパム/ウイルス定義を提供する方法を示したものです。



スパムスコアリングについて

バラーダスパムファイアーウォールは、メッセージのすべての特性を詳細に検査し、複雑なスコアシステムを利用してそのメッセージがスパムかどうかを判定します。メールがスパムスコアリングフィルタに到達すると、メッセージのすべてのプロパティにスコアを割り当てます。

以下に、バラーダスパムファイアーウォールが行う検査の例を示します。

- メッセージのヘッダーと件名に、不愉快な文字や単語が含まれているかどうか
- メッセージに含まれる HTML の割合
- メッセージに「登録解除」リンクが含まれているかどうか

上記は、バラーダスパムファイアーウォールが検査するプロパティのほんの一部にすぎません。バラーダスパムファイアーウォールはこれらすべてのプロパティを検査して、メッセージのスパムスコアを決定します。スパムスコアは、管理者画面の [メッセージログ] ページに表示されます。

スパムルールとスコアは、バラーダエネルギー充填サービスによって最新の状態に維持されます。バラーダスパムファイアーウォールはこの情報をもとに、スパム送信者が使用する最新の攻撃テクニックに対抗します。

バラクーダスパムファイアーウォールのモデル

バラクーダスパムファイアーウォールは、4つのモデルで構成されます。各モデルの処理能力と機能については、下図を参照してください。

機能	モデル 200	モデル 300	モデル 400	モデル 600
アクティブメールユーザ数	1,000	2,000	10,000	25,000
ドメイン	50	250	500	5,000
全メールサーバとの互換性	✓	✓	✓	✓
強固なセキュア OS	✓	✓	✓	✓
スパムブロック	✓	✓	✓	✓
ウィルススキャン	✓	✓	✓	✓
ウェブベース管理者画面	✓	✓	✓	✓
ユーザごとの設定と隔離		✓	✓	✓
MS エクスチェンジ /LDAP アクセラレータ		✓	✓	✓
Syslog のサポート		✓	✓	✓
クラスタリング			✓	✓
RAID (Redundant Disk Array)			✓	✓
SNMP サポート			✓	✓
ユーザごとのスコア設定				✓
ブランドロゴのカスタマイズ				✓

テクニカルサポート

バラクーダ社製品に関するお問い合わせは：

- TEL : 045-476-2010/045-476-2163
- email : barracuda@cs.macnica.net

保証方針

バラクーダスパムファイアーウォールでは、製造上の瑕疵に対して 90 日間の保証が提供されます。

本書での情報の記載場所

管理者画面の各ページに関する情報の記載場所については、下表を参照してください。

管理者画面のページ	記載場所
【基本設定】 タブ	
ステータス	システムステータスと統計の表示 (P.20)
メッセージログ	受信メールのモニタリングと分類 (P.22)
スパムスコアリング	スパム設定の構成 (P.26)
ウィルスチェック	ウィルスチェックと通知の有効化 / 無効化 (P.27)
隔離	隔離の設定 (P.28)
IP 設定	システム IP 情報の設定 (P.31)
アドミニストレーション	管理者画面へのアクセス制御 (P.32) システムのシャットダウンとリセット (P.33) システムレポート送付の自動化 (P.34) メールの詳細の表示 (P.25)
ベジアン / フィンガープリンティング	フィンガープリンティングの動作の変更 (P.45) メールクライアントでのメールの分類 (P.24) (モデル 200 では利用できません) ベジアンデータベースのリセット (P.33)
【拒否 / 許可】 タブ	
外部ブラックリスト	ブラックリストサービスへの加入 (P.34)
IP アドレスでの拒否 / 許可	IP アドレス / ネットワークによるフィルタリング (P.36)
送信元ドメインによる拒否 / 許可	送信元ドメインによるフィルタリング (P.37)
送信者メールアドレスによる拒否 / 許可	送信者メールアドレスによるフィルタリング (P.37)
受信者メールアドレスによる拒否 / 許可	受信者メールアドレスによるフィルタリング (P.38)
添付ファイル拡張子フィルタリング	添付ファイルタイプによるフィルタリング (P.38)
件名によるフィルタリング	件名によるフィルタリング (P.39)
本文によるフィルタリング	本文の内容によるフィルタリング (P.40)
ヘッダーによるフィルタリング	ヘッダーの内容によるフィルタリング (P.40)
【ユーザ】 タブ	
アカウント一覧	ユーザアカウントの表示 (P.56)
ユーザ機能	ユーザアカウントへの機能の割り当て (P.58)
ユーザの追加 / 更新	新規ユーザアカウントの作成 (P.59)
設定のバックアップ / リストア	ユーザ設定のバックアップとリストア (P.59)

管理者画面のページ	記載場所
[ドメイン] タブ	
ドメイン管理	ドメインの管理と設定 (P.53) ドメイン設定の編集 (P.54) (モデル 200 と 300 では利用できません。) バラクーダ MS エクスチェンジアクセラレータを使用した辞書攻撃の阻止 (P.55) (モデル 200 では利用できません。)
[高度な設定] タブ	
メールプロトコル	メールプロトコル検査の設定 (P.46)
レートコントロール	メッセージレートコントロールの設定 (P.48)
明示的ユーザ	個別アカウントの有効化 (P.48)
設定のバックアップ / リストア	システム設定のバックアップとリストア (P.41)
エネルギー充填サービス	エネルギー充填サービスを使用したスパムとウィルス定義の更新 (P.43)
ファームウェア更新	システムファームウェアバージョンの更新 (P.49)
外観	管理者画面の外観のカスタマイズ (P.44)
Syslog	Syslog サーバを使用したシステムログの集中管理 (P.49)
クラスタ化	クラスタ化環境の設定 (P.50) (モデル 200 と 300 では利用できません。)
シングルサインオン	シングルサインオンの導入 (P.52) (モデル 200 と 300 では利用できません。)
SSL	SSL の有効化 (P.60)
スパムルール管理	スパム設定のローカライズ (P.53)
バウンス /NDR メッセージ	配送不能レポート (NDR) のカスタマイズ (P.61)
トラブルシューティング	トラブルシューティング (P.63)

第 2 章 バラクーダスパムファイアーウォールの設定

バラクーダスパムファイアーウォールを設定するには、以下の手順を実行します。

1. バラクーダスパムファイアーウォールを設置します (本ページ)。
2. システム IP アドレスを設定します (P.12)。
3. バラクーダスパムファイアーウォールを構成します (P.12)。
4. ファイアーウォールの構成とファームウェアの更新を行います (P.14)。
5. MX レコードを修正することにより、受信メールの経路を変更します (P.15)。
6. 設置後の手順 (P.15)。

この章の最後には、バラクーダスパムファイアーウォールをネットワーク環境に統合する際のリファレンスとして役立つ設置シナリオも示しています。

バラクーダスパムファイアーウォールの設置

バラクーダスパムファイアーウォールを設置するには、以下の手順を実行します。

1. 19 インチの標準ラックかその他の安定した場所に、バラクーダスパムファイアーウォールを設置します。

警告：ユニットの前後にある冷却孔をふさがないでください。

2. CAT5 イーサネット・ケーブルをバラクーダスパムファイアーウォールの背面に接続します。

バラクーダスパムファイアーウォールは 10BaseT および 100BaseT イーサネットをサポートしています。最良のパフォーマンスを得るため、100BaseT 接続をお勧めします。

注意：バラクーダスパムファイアーウォール 600 は、ギガビットイーサネットをサポートしています。使用可能な LAN ポートは 2 つあります。この 600 モデルでは、イーサネットケーブルは LAN 2 ポートに接続してください (LAN 1 ポートはプラグでふさがります)。

ユニットの他のコネクタに上記以外のケーブルを接続しないでください。これらのコネクタは診断用に使用します。

3. 電源コードをユニットに接続します。
4. ユニット前面にある **【電源】 ボタン**を押します。

システム前面の電源ランプが点灯します。各インジケータランプの説明については、「インジケータランプについて」(P.20)を参照してください。

システム IP アドレスの設定

バラクーダスパムファイアウォールのデフォルト IP アドレスは、192.168.200.200 です。このアドレスを変更するには、以下のいずれかを行います。

- キーボードとモニタをバラクーダスパムファイアウォールに直接接続してから、コンソールインターフェースで新しい IP アドレスを指定します。
- フロントパネル上の [リセット] ボタンを押し続けます。[リセット] ボタンを 8 秒間押し続けると、デフォルト IP アドレスが 192.168.1.200 に変更されます。12 秒間押し続けると、IP アドレスが 10.1.1.200 に変更されます。

バラクーダスパムファイアウォールに直接接続して新しい IP アドレスを設定するには、以下の手順を実行します。

1. 標準 VGA モニターと PS2 キーボードをバラクーダスパムファイアウォールのバックパネルに取り付けます。

[Barracuda login:] プロンプトがモニターに表示されます。

2. ログイン名として「**admin**」と入力し、パスワードにも「**admin**」と入力します。

[User Confirmation Requested] ウィンドウに、システムの現在の IP 設定が表示されません。

3. <Tab> キーを使用して **[Yes]** を選択し、IP 設定を変更します。
4. バラクーダスパムファイアウォールの新しい IP アドレス、ネットマスク、デフォルトゲートウェイを入力し、**[OK]** を選択します。
5. IP 設定を変更する場合は、表示されたプロンプトで **[No]** を選択します。

バラクーダスパムファイアウォールの構成

システム IP アドレスを指定したら、管理者画面を使用してバラクーダスパムファイアウォールを構成する必要があります。バラクーダスパムファイアウォールの構成を行っているコンピュータが同じネットワークに接続されていて、ウェブブラウザを介してバラクーダスパムファイアウォールの IP アドレスに接続できるようにルートされていることを確認してください。

バラクーダスパムファイアウォールを構成するには、以下の手順を実行します。

1. ウェブブラウザで、前項で指定したバラクーダスパムファイアウォールの IP アドレスを入力し、続いてポート番号の 8000 を入力します。

例 : `http://192.168.200.200:8000`

2. ログイン情報のプロンプトが表示された場合は、ログインとパスワードの両方に「**admin**」と入力します。

3. [基本設定] → [IP 設定] ページを表示し、必要な情報を入力します。

下表は、情報の入力が必要なフィールドについての説明をまとめたものです。

フィールド	説明
TCP/IP 設定	<p>バラクーダスパムファイアウォールの IP アドレス、サブネットマスク、デフォルトゲートウェイ</p> <p>TCP ポートは、バラクーダスパムファイアウォールが入ってくるメールを受信するポートです。通常はポート 25 が使用されます。</p>
送付先メールサーバの TCP/IP 設定	<p>送付先メールサーバのホスト名または IP アドレス (例: <i>mail.yourdomain.com</i>)。これはスパムやウィルススの検査が完了したメールを受信するメールサーバです。</p> <p>メールサーバの IP アドレスではなく、ホスト名を指定してください。これにより、送付先メールサーバの移動や DNS の更新を行った場合も、バラクーダスパムファイアウォールを変更する必要がなくなります。</p> <p>TCP ポートは、送付先メールサーバが入ってくるメールを受信するポートです。通常はポート 25 が使用されます。</p> <p>複数のドメインまたはメールサーバの設定が必要な場合は、「高度な設定の構成」(P.45) を参照してください。</p>
DNS 設定	<p>ネットワーク上で使用するプライマリおよびセカンダリ DNS サーバのリストです。</p> <p>プライマリ DNS サーバとセカンダリ DNS サーバを指定することが強く推奨されます。バラクーダスパムファイアウォールの一部の機能 (送信者ドメイン偽造の検出など) は、DNS が使用可能な場合にのみ実行できます。</p>
ドメイン設定	<p>デフォルトホスト名は、バラクーダスパムファイアウォールが送信するメールメッセージ (配送不能通知、ウィルス警告通知など) の返信用アドレスで使用されるホスト名です。ホスト名は、デフォルトドメインに付加されます。</p> <p>デフォルトドメイン名は、バラクーダスパムファイアウォールが送信するメールメッセージ (配送不能通知、ウィルス警告通知など) の返信用アドレスで使用されるドメイン名です。</p>
許可する受信ドメイン	<p>バラクーダスパムファイアウォールが管理するドメイン。このリストにすべてのドメインが含まれているか確認してください。バラクーダスパムファイアウォールは、リストにないメッセージを拒否します。</p> <p>メールサーバと一致するすべてのドメインのメッセージを許可するには、このフィールドにアスタリスク (*) を入力します。</p> <p>注意: 1 台のバラクーダスパムファイアウォールで複数のドメインとメールサーバをサポートできません。複数のメールサーバを使用している場合は、[ドメイン] タブを表示し、各ドメインに対応するメールサーバを入力してください。</p>

4. **[変更保存]** をクリックします。

IP アドレスを変更した場合は、バラクーダスパムファイアウォールへの接続を切断し、新しい IP アドレスを使用して再度ログインする必要があります。

5. [基本設定] → [アドミニストレーション] ページを表示し、以下を実行します。
 - a. バラクーダスパムファイアーウォールに新しい管理者パスワードを割り当てます（任意）。
 - b. ローカルタイムゾーンが正確に設定されているか確認します。

バラクーダスパムファイアーウォールの時間は、NTP（ネットワークタイムプロトコル）によって自動的に更新されます。したがって、お使いのファイアーウォールをインバウンドおよびアウトバウンド UDP トラフィックが通過できるように、ポート 123 を開放しておく必要があります（バラクーダスパムファイアーウォールがファイアーウォールの内側に配置される場合）。

この情報はメッセージの送信時間を特定するために使用され、メール読み取りプログラムに表示されることもあるので、タイムゾーンは必ず正確に設定してください。
 - c. **[変更保存]** をクリックします。

これでバラクーダスパムファイアーウォールの構成は完了です。バラクーダスパムファイアーウォールはすべての受信メールをフィルタリングし、スパムでないメールだけをメールサーバに配送します。

ファイアーウォールの設定とファームウェアの更新

バラクーダスパムファイアーウォールがファイアーウォールの内側に配置される場合には、特定のポートを開放して、システムとリモートサーバ間で適切に通信できるようにする必要があります。これが完了すると、（必要に応じて）バラクーダスパムファイアーウォールに最新バージョンのファームウェアをダウンロードすることができます。

ファイアーウォールを設定し、最新バージョンのファームウェアをダウンロードするには、以下の手順を実行します。

1. ファイアーウォールを設定します。どのポートを開放するかについては、下表を参照してください。

ポート	方向	プロトコル	用途
22	In	TCP	リモート診断
25	In/Out	TCP	電子メール送信、バウンスメール送信
53	Out	TCP/UDP	DNS
80	Out	TCP	ウィルス、ファームウェア、スパムルール更新
123	Out	TCP/UDP	NTP

2. 必要があれば、受信メールをバラクーダスパムファイアーウォールに向けるために、ファイアーウォールの NAT ルーティングを変更します。必要な変更については、ファイアーウォールのマニュアルか、ファイアーウォールの管理者に問い合わせてください。

3. バラクーダスパムファイアウォールのファームウェアを更新します。
 - a. [高度な設定] → [ファームウェア更新] ページを表示します。
 - b. 最新バージョンのファームウェアをダウンロードするには、**[今すぐダウンロード]** をクリックします。

 ファームウェアの更新には数分かかることがあります。更新中はユニットの電源を切らないでください。

 最新バージョンのファームウェアがすでにシステムにインストールされている場合には、**[今すぐダウンロード]** ボタンは無効になります。
4. 「システムデータのバックアップ」(P.41) の説明に従ってシステム設定のバックアップを作成します。

MX レコードの変更による受信メールのルーティング

バラクーダスパムファイアウォールが (ファイアウォールで保護されていない) DMZ にある場合は、[DNS MX レコード] を変更して、受信メールをバラクーダスパムファイアウォールに向けます。

警告: メールがバラクーダスパムファイアウォールを**通**って送信されるようにしないでください。このユニットは、**送信メール用のメールリレーとして機能しません**。送信メールについては、**既存のメールサーバを経由する**ようにする必要があります。バラクーダスパムファイアウォールから送信されるメールは、**バウンスまたは拒否メッセージ**だけです。

[DNS MX レコード] の変更は、通常、DNS サーバまたは DNS サービスで行います。[DNS MX レコード] を変更する場合は、バラクーダスパムファイアウォール用の DNS エントリを作成する必要があります。

以下の例は、「*barracuda*」という名前と IP アドレス *66.233.233.88* を持つバラクーダスパムファイアウォール用の DNS エントリです。

```
barracuda.yournetwork.com IN A 66.233.233.88
```

以下の例は、優先番号 10 を持つ関連の MX レコードです。

```
IN MX 10 barracuda.yournetwork.com
```

設置後の作業

バラクーダスパムファイアウォールの設置が完了したら、ユニットはデフォルトのシステム設定に基づいて受信メールのフィルタリングを行います。このフィルタリングでは、受信メールの自動ウイルスチェックや、バラクーダブラックリストを使用したスパムの分類などが行われます。

デフォルト設定でほとんどのスパムを排除できますが、一部の設定値については、ユーザ独自の環境に基づいてカスタマイズする必要があります。

下表は、システムの最初の設定時に必要となる最も一般的な作業をまとめたものです。設定作業の一覧については次章を参照してください。

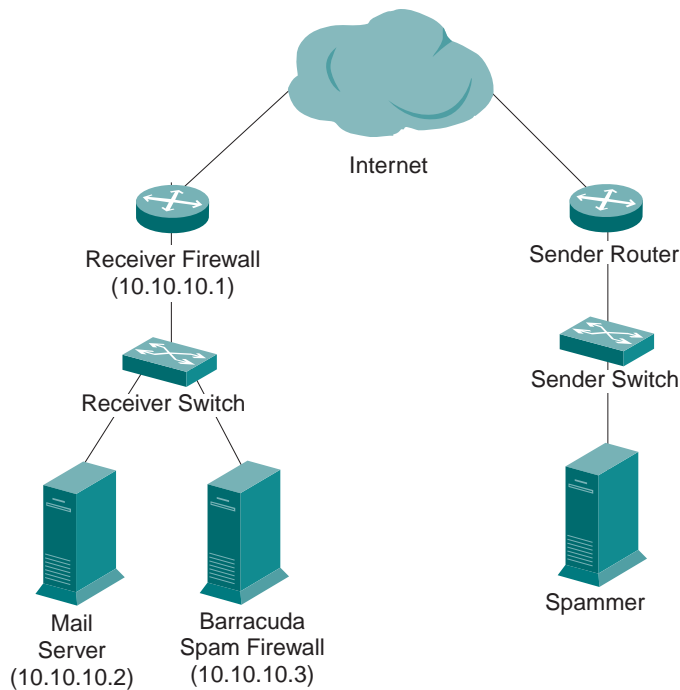
作業	記載場所
受信メールの監視と分類	「受信メールのモニタリングと分類」(P.22)
スパムスコアリングのデフォルト値の検証	「スパム設定の構成」(P.26)
隔離の設定 (任意)	「隔離の設定」(P.28)
特定の IP アドレス、ドメイン、またはメールアドレスからのメッセージの拒否	「拒否 / 許可フィルターの使用」(P.36)

設置例

この項では、2 タイプの設置例を紹介します。これを参考に、お使いのネットワーク環境にバラクーダスパムファイアウォールを統合するのに最も適した方法を決定してください。

バラクーダスパムファイアウォールをファイアウォールの内側に配置する場合

下図は、バラクーダスパムファイアウォールをファイアウォールの内側に設置する場合の設置例です。この例では、メールサーバの IP アドレスは 10.10.10.2、バラクーダスパムファイアウォールの IP アドレスは 10.10.10.3 です。



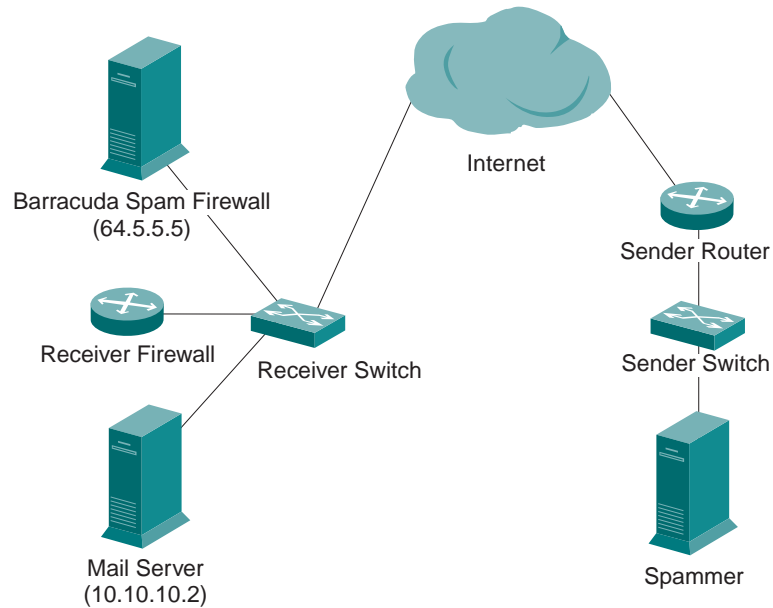
このタイプの設定では、以下の作業を行う必要があります。

- ポート 25 の受信 SMTP トラフィックをバラクーダスパムファイアウォール (10.10.10.3) に転送 (ポートリダイレクション) します。
- バラクーダスパムファイアウォールを、フィルタリング済みトラフィックが送信先メールサーバ (10.10.10.2) に転送されるように設定します。

このタイプの設定では、MX レコードを変更する必要はありません。

バラクーダスパムファイアウォールをファイアウォールの前に配置する場合

下図は、バラクーダスパムファイアウォールをファイアウォールの前に配置する場合の設置例です。この例では、メールサーバの IP アドレスは 10.10.10.2、バラクーダスパムファイアウォールのパブリック IP アドレスは 64.5.5.5 です。



このタイプの設定では、以下の作業を行う必要があります。

- 利用可能な外部 IP アドレスをバラクーダスパムファイアウォールに割り当てます。
- DNS (ドメインネームサーバ) 上の MX (メールエクスチェンジ) レコードを、トラフィックがバラクーダスパムファイアウォールに流れるように変更します。バラクーダ用の DNS に A レコードと MX レコードを作成します。

以下の例は、「*barracuda*」という名前と IP アドレス *64.5.5.5* を持つバラクーダスパムファイアウォール用の DNS エントリです。

```
barracuda.yourdomain.com IN A 64.5.5.5
```

以下の例は、優先番号 10 を持つ関連の MX レコードです。

```
IN MX 10 barracuda.yournetwork.com
```


第 3 章 バラクーダスパムファイアーウォールの管理

この章では、バラクーダスパムファイアーウォールの管理と設定について説明します。この章で説明する作業は以下のとおりです。

作業	記載場所
システムステータスと統計の表示	P.20
受信メールのモニタリングと分類	P.22
スパム設定の構成	P.26
ウィルスチェックと通知の有効化 / 無効化	P.27
隔離の設定	P.28
システム IP 情報の設定	P.31
管理者画面へのアクセス制御	P.32
システムのシャットダウンとリセット	P.33
システムレポート送付の自動化	P.34
ブラックリストサービスへの加入	P.34
拒否 / 許可フィルターの使用	P.36
システム設定のバックアップとリストア	P.41
エネルギー充填サービスを使用したスパムとウィルス定義の更新	P.43
管理者画面の外観のカスタマイズ	P.44
高度な設定の構成	P.45
ドメインの管理と設定	P.53
バラクーダ MS エクスチェンジアクセラレータを使用した辞書攻撃の阻止	P.55
ユーザアカウントの管理	P.56
SSL の有効化	P.60
配送不能レポート (NDR) のカスタマイズ	P.61
トラブルシューティング	P.63

システムステータスと統計の表示

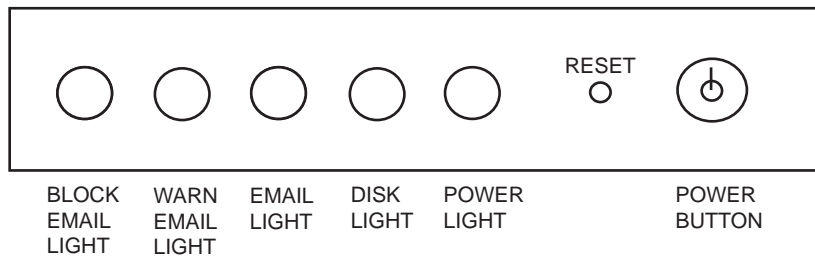
この項では、以下のトピックについて説明します。

- インジケータランプについて (本ページ)
- 「システム統計の表示」(P.21)

インジケータランプについて

バラクーダスパムファイアウォールには、フロントパネルに5個のインジケータランプがあります。これらのランプは、システムがメールを処理するときに点滅します。

下図に、各ランプの位置を示します。



下図に、各ランプの位置を示します。

ランプ	色	説明
メール拒否	赤	スパムまたはウィルスの検出によってメールが拒否された場合に点滅します。
警告メール	黄	スパムとしてタグ付けまたは隔離されたメールが発生した場合に点滅します。
メール	緑	ユニットがメールを受信すると点滅します。
ディスク	緑	ディスクの稼動中に点滅します。
電源	緑	システムの電源がオンのときに緑のランプが常時点灯します。

システム統計の表示

[基本設定] → [ステータス] ページには、メール統計、システム環境の状態、1 時間毎および日次のメール統計が示されています。

メール統計

下表は、[基本設定] → [ステータス] ページに示されるメール統計についての説明をまとめたものです。

統計	説明
拒否	システムが拒否したウィルスとスパムメールの数。
拒否: ウィルス	システムが拒否したウィルスメールの数。
隔離	システムが隔離したメールの数。この数字は、グローバル隔離アドレスに送られたメールと、ユーザが隔離したメールの合計です。デフォルトでは、システムはメールを隔離しません。隔離機能を有効にする方法については、「隔離の設定」(P.28) を参照してください。
許可: タグ付	システムがタグ付けしたメールの数。タグ付けされたメールは、件名が [スパムスコアリング] ページ (P.26 で説明) の設定に基づいて修正されます。
許可	拒否または修正されずに受信者に送付されたメールの数。
合計	インストール後または最後のリセット実行後のシステムの統計。
今日	現在の暦日 (午前 00 時から翌日の午前 00 時まで) の統計。
この 1 時間	現在の 1 時間の開始時から始まる統計。例えば、現在 10 時 45 分の場合、午前 10 時から午前 10 時 45 分までの統計が示されます。

パフォーマンス統計

[基本設定] → [ステータス] ページには、以下のようなシステム環境条件が表示されます。

- 受信メールと送信メールのキューサイズ

メールのキューサイズは、「10/5」のような割合として示されます。最初の数字はキューに含まれる受信メール数、2 番目の数字はキューに含まれる送信メール数です。

- システムのファン、プロセッサ、RAID ディスク (該当する場合) の現在の状態
- システムが受信メールのフィルタリングに要した時間の平均
- 最後のメール配送からの経過時間

値が正常域値 (しきい値) を超えると、赤字の警告が表示されます。

注意: RAID ディスクが付属するのは、バラクーダスパムファイアウォール 400 および 600 だけです。そのため、モデル 200 および 300 の場合は、RAID ディスクの統計は表示はされません。

ファームウェアとメール / ログストレージは、各パーティションの使用領域のパーセンテージを表示します。バラクーダスパムファイアウォールは、いずれかのパーティションの利用率が 90% に近づくとシステム警告のメールを送ります。

1 時間毎および日次のメール統計

過去 25 日間および過去 24 時間の拒否、隔離、許可されたメールの数を示します。

受信メールのモニタリングと分類

[基本設定] → [メッセージログ] ページで受信メールを定期的にモニターしてできるだけ多くのメールをスパムまたは非スパムとして分類するとともに、メールをホワイトリストに追加してください。

メールを分類すると、ベイジアンデータベースに、バラクーダスパムファイアウォールが今後類似したメールをどのように処理すべきかを決定するルールが作成されます。

注意：メッセージログの表示方法を変更するには、[参照] ボタンをクリックします。このボタンでは、カラムの表示/非表示、カラムの順序、カラムの幅を変更できます。

受信メールをスパム / 非スパムとして分類、またはホワイトリストに追加します。

<input type="checkbox"/>	Spam Classification	White Listed	Date	From	To	Subject
<input checked="" type="checkbox"/>	N/A	N/A	03/21 13:51			
<input type="checkbox"/>	UNKNOWN	No	03/21 13:51	tspada@valley...	dave@envirote...	Sunol Golf
<input type="checkbox"/>	UNKNOWN	No	03/21 13:51	charles_bentl...	edwardr@gourm...	More effici
<input type="checkbox"/>	N/A	N/A	03/21 13:51			
<input type="checkbox"/>	N/A	N/A	03/21 13:50			
<input type="checkbox"/>	N/A	N/A	03/21 13:50			
<input type="checkbox"/>	N/A	N/A	03/21 13:50			

メッセージエントリをクリックすると、そのメールの詳細が表示されます。

管理者画面でのメールの分類

メールの分類によって、バラクーダスパムファイアウォールによる受信メールの処理方法のルールを作成することができます。これは、最も簡単なルール作成方法の1つです。下表は、[基本設定] → [メッセージログ] ページでメールの分類に使用するボタンについての説明をまとめたものです。

ボタン	説明
スパム	<p>ベイジアンデータベースでメールをスパムとして分類します。</p> <p>ベイジアンデータベースは、200 通のスパムメールと 200 通の非スパムメールが分類されるとアクティブになります。バラクーダスパムファイアウォールはこの時点でメールのスキャンを開始し、ルールと一致するメールが検出されるとメールのスコアリングを変更します。</p> <p>ユーザ単位隔離が有効な場合は、個々のユーザが実行したメール分類もベイジアンデータベースに適用されます。</p> <p>現在スパムとして分類されているメール数を表示するには、[基本設定] → [ベイジアン/フィンガープリンティング] ページを選択します。</p> <p><i>注意</i> [基本設定] → [ベイジアン/フィンガープリンティング] ページ (P.45) の [バラクーダネットワークスにメールを送る] フィールドが [いいえ] に設定されていない場合には、スパムとして分類されたメッセージは解析のためにバラクーダネットワークスに送信されます。</p>
非スパム	<p>ベイジアンデータベースでメールを非スパムとして分類します。</p> <p>ベイジアンデータベースは、200 通のスパムメールと 200 通の非スパムメールが分類されるとアクティブになります。バラクーダスパムファイアウォールはこの時点でメールのスキャンを開始し、ルールと一致するメールが検出されるとメールのスコアリングを変更します。</p> <p>ユーザ単位隔離が有効な場合は、個々のユーザが実行したメール分類もベイジアンデータベースに適用されます。</p> <p>現在非スパムとして分類されているメール数を表示するには、[基本設定] → [ベイジアン/フィンガープリンティング] ページを選択します。</p>
ホワイトリスト	<p>メールの送信者を [ホワイトリスト] に追加します。ホワイトリスト化した送信者のメールには、スパムスコアが付きません。</p> <p>ただし、ホワイトリスト化した送信者のメールであっても、以下の機能は実行されます。</p> <ul style="list-style-type: none"> ・ウィルスチェック ・添付ファイルタイプのフィルタリング (P.38 参照) ・ヘッダー、本文、件名による拒否フィルター (P.39 参照)
ホワイトリストから外す	[ホワイトリスト] からメールの送信者を除去します。
メッセージログのクリア	現在表示されているすべてのログをクリアします。受信メールを対象に設定したルールを格納するベイジアンデータベースはクリアされません。

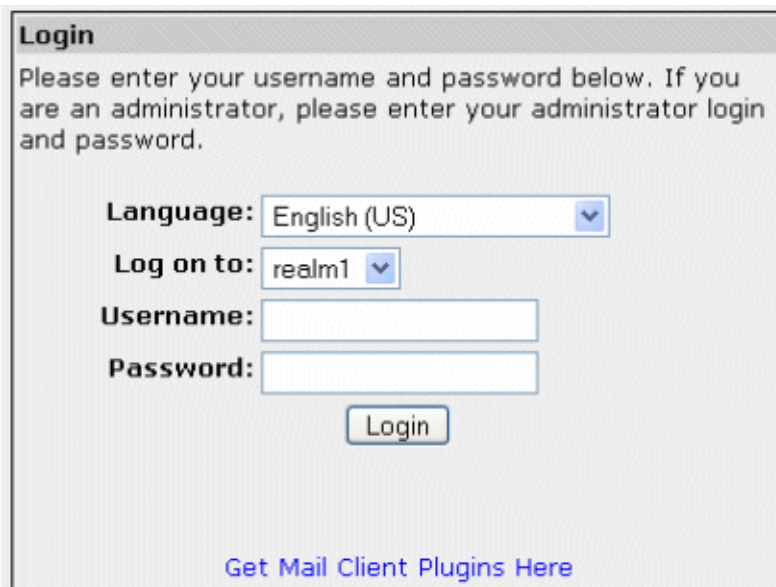
メールクライアントでのメールの分類



クライアントプラグインを使うと、エンドユーザが Microsoft Outlook から直接、自分宛のメールをスパムまたは非スパムとして分類することができます。この機能は、バラクーダスパムファイアーウォール 300、400、600 でのみ利用できます。

ユーザに Outlook クライアントプラグインを提供するには、以下の手順を実行します。

1. [基本設定] → [ベイジアン / フィンガープリンティング] ページの [ユーザにプラグインのダウンロードを許可します] フィールドを [はい] に設定します。
2. [変更保存] をクリックします。

管理者画面ログインページの最下部にメールプラグインへのリンクが表示されます (下図参照)。



プラグインのダウンロードとインストールが完了すると、メールクライアントからこれらのボタンを使ってメールを分類できます。   最初のボタン (赤色) を押すとメールはスパムとして分類され、2 番目のボタン (緑色) を押すとメールは非スパムとして分類されます。

注意：プラグインをインストールした後は、スパムまたは非スパムとして分類されたメールに対して実行される様々なオプションをユーザ自身が設定できるようになります。これらのオプションは、Microsoft Outlook の [ツール] → [オプション] で設定できます。

メッセージログについて

下表は、メッセージログテーブルの各カラムについての説明をまとめたものです。

カラム	説明
スパム分類	メールがスパムまたは非スパムとして分類されたことを示します。[メッセージログ] の最上部のボタンを使ってメールをスパムまたは非スパムとしてマークすると、その分類がこのカラムに表示されます。
ホワイトリスト化	送信者がホワイトリストに含まれていることを示します。メールにウイルスが検出されたか、許可されない添付ファイルが添付されている場合を除き、ホワイトリストの送信者からのメールはすべて許可されます。
日付	バラクーダスパムファイアウォールがメールを受信した日付。
From / To	送信者と受信者のメールアドレス。
件名	メールの件名の内容。
アクション	メールに対して実行されたアクション（許可、タグ付け、拒否、隔離）。
理由	アクションの理由。送信者がブラックリストに載っている、メールがスパムとして分類された、など。 場合によっては、このカラムに、メールが許可される理由として [メールサイズ] が表示されることがあります。この理由が表示された場合は、メールのサイズが 65k を超えていたために、メールのスパムスキャンが実行されなかったことを意味します。65k を超えるメールのスキャンが行われなないのは、スパムメールがこのサイズ制限を超えることはきわめて稀であり、スパムの可能性の低い大きなメールをスキャンすることはシステム資源の利用効率を低下させる原因となるためです。 メールのサイズが 65k を超える場合、スパムスキャンは実行されませんが、ウイルススキャンは実行されます。
スコア	メールのスパムスコア。このスコアの範囲は、0（確実に非スパム）～10 以上（確実にスパム）です。
ソース IP	送信者の IP アドレスまたはホスト名。

メールの詳細の表示

[基本設定] → [メッセージログ] ページでメールの詳細情報を表示するには、メールをクリックし、詳細ウインドウを表示します。

詳細ウインドウで、以下をクリックします。

- [メッセージビュー] タブをクリックすると、メッセージの内容が表示されます。
- [ソースビュー] タブをクリックすると、ヘッダーを含むメールの内容が表示されます。
- [配送] リンクをクリックすると、メールが受信者に送信されます。

メールの本文を読むと、本文のフィルタリングに組み込むべき単語や文字を容易に判別できます。例えば、多数のメールの本文に「as seen on TV」という広告文が含まれることに気付いた場合は、キーワードとして「as seen on」を追加すると、これらの単語が含まれるメッセージが拒否、隔離、またはタグ付けされます。本文のフィルタリングの詳細については、「本文の内容によるフィルタリング」(P.40) を参照してください。

プライバシー保護の理由でメール本文の表示を望まない場合は、[基本設定] → [アドミニストレーション] ページの [メッセージログのプライバシー] でメール本文を非表示に設定できます。

スパム設定の構成

[基本設定] → [スパムスコアリング] ページでは、グローバルスコアリング値をの修正や、スパムメールに付ける件名タグを指定することができます。

このページを変更した後、**【変更保存】** をクリックしてください。

グローバルスパムスコアリングの設定

拒否 / 許可フィルターを通過したメールには、スパムの可能性を示すスコアが付けられます。このスコアの範囲は、0（確実に非スパム）～10以上（確実にスパム）です。

バラクーダスパムファイアーウォールは、このスコアに基づいて、タグ付け、隔離、拒否、許可のいずれかを行います。

下表は、スパムスコアリングに関連する設定についての説明をまとめたものです。設定を10にすると、そのオプションは無効になります。

注意：バラクーダスパムファイアーウォール 400 および 600 では、[ドメイン] タブでドメイン毎のスパムスコアリング境界を設定できます。詳細については、「ドメインの管理と設定」(P.53) を参照してください。

設定	説明
タグ付けスコア	スコアがこの値を上回り、かつ隔離スコアを下回るメールは、件名に「[BULK]」という単語が追加されて送信者に送付されます。 「スパムタグ設定」セクションで新しいテキストを入力することによって、件名に追加されるデフォルトのテキストを変更できます（このページの最後を参照）。 スコアがタグ付けスコアを下回るメールはすべて、自動的に許可されます。デフォルト値は4です。
隔離スコア	スコアがこの値を上回り、かつ拒否スコアを下回るメールは、指定した隔離メールボックスに転送されます。隔離メールボックスの指定に関する詳細については、「グローバル隔離設定の指定」(P.29) を参照してください。 デフォルトでは、システムはメールを隔離しません。 隔離機能を有効にするには、この設定で拒否スコアよりも低い値を指定します。
拒否スコア	スコアがこの値を上回るメールは受信者に配送されず、送信者に配送不能通知 (NDR/ バウンスメール) が送付されます。 デフォルト値は9です。

件名テキストとタグ付きメールの優先度の指定

[基本設定] → [スパムスコアリング] ページでは、タグ付きメールの件名の先頭に表示されるテキストを入力することができます。デフォルトのテキストは、「[BULK]」です。

システムは、以下の場合にメールにタグ付けします。

- メールがスパムスコアがタグ付けスコアを上回る（かつ隔離スコアを下回る）場合
- 拒否 / 許可フィルターが、タグ付けを要するメールとして分類した場合。拒否 / 許可フィルターによるメールのタグ付けを設定する方法については、「拒否 / 許可フィルターの使用」(P.36) を参照してください。

[低優先度に設定] を [はい] に設定すると、タグ付けされたメールはすべて低優先度としてマークされます。

デフォルトでは、メールにスパムのタグが付けられたために受信者に配送されない場合には、送信者に通知が送付されます。自動通知機能をオフにするには、[バウンス送信] を [いいえ] に設定します。

注意：多数のメールクライアントでは、ルールを作成して、タグ付きメールを別のメールフォルダに入れることができます。例えば、「[BULK]」という件名タグの付いたスパムメールを受信すると、「Possible Spam」という名前のフォルダに自動的に配送するようにメールクライアントを設定できます。

ウイルスチェックと通知の有効化 / 無効化

バラクーダスパムファイアーウォールでは、ウイルススキャンが自動的に有効化され、定期的（デフォルトでは1時間毎）に定義更新の有無がチェックされます。

[基本設定] → [ウイルスチェック] ページを使用して、下表で説明するウイルスチェック設定と通知設定を行います。このページの変更が完了したら **【変更保存】** をクリックします。

設定	説明
ウイルススキャンを有効化	<p>ウイルススキャンが有効な場合は、すべてのメールに対して自動的にウイルススキャンが実行されます。ウイルスを含むメールは常に拒否されます。これらのメールは隔離されず、送信者がホワइटリスト化されている場合でも受信者に送付されません。ウイルススキャンは常に有効にしておくことをお勧めします。</p> <p><i>注意：バラクーダスパムファイアーウォール 400 および 600 では、[ドメイン] タブでドメイン毎にウイルスチェックを有効化または無効化することができます。詳細については、「ドメインの管理と設定」(P.53) を参照してください。</i></p>
受信者にウイルス検出を通知	<p>ウイルスが検出されたためにメールが拒否された場合に、受信者に通知するかどうかを指定します。</p>
送信者にウイルス検出を通知	<p>ウイルスが検出されたためにメールが拒否された場合に、送信者に通知するかどうかを指定します。</p> <p>このオプションは [いいえ] に設定しておいてください。これにより、ウイルスが広範囲で発生した場合に、バラクーダスパムファイアーウォールがメール通知の送信トラフィックを大量に発生させる恐れがなくなります。</p>

隔離の設定

デフォルトでは、バラクーダスパムファイアウォールはメールを隔離しないように設定されています。

システムの隔離機能を設定するには、以下の手順を実行します。

1. スパムスコアリングのしきい値を使用して、隔離機能を有効にします。詳細については、「グローバルスパムスコアリングの設定」(P.26)を参照してください。
2. [基本設定] → [隔離] ページを表示します。
3. [隔離タイプ] (P.28 参照) を選択します。
4. 以下のいずれかを実行します。
 - ・ グローバル隔離タイプの場合は、グローバル隔離メール通知アドレス (P.29 参照) を入力します。
 - ・ ユーザ単位隔離タイプの場合は、ユーザ単位隔離設定 (P.29 参照) を構成します。
5. **【変更保存】** をクリックします。

隔離タイプの指定

[隔離タイプ] は、隔離されたメールを、[グローバル隔離メール通知アドレス] とユーザ毎の隔離ボックスのどちらに送付するかを決定します。

注意：バラクーダスパムファイアウォール 400 および 600 では、[高度な設定] → [高度なドメイン設定] ページで、ドメイン毎に隔離タイプを指定できます。

下表は、2つの隔離タイプについての説明をまとめたものです。

隔離タイプ	説明
ユーザ単位	<p>各ユーザのメールアカウントに、個別に作成された隔離サマリーレポートを送付します。このレポートは、毎日午後 3 時 30 分に送信されます。ユーザは、このレポートに含まれるリンクからログインして、以下の作業を実行できます。</p> <ul style="list-style-type: none"> ・ 件名に「隔離通知件名テキスト」が挿入された隔離メールを受信する、または、バラクーダスパムファイアウォールに隔離メールを保存する (デフォルト)、のいずれかを指定する。 ・ メールボックスのスパムスキャンをすべて停止する。 ・ 個別のホワイトリストとブラックリストを設定する。 <p>ユーザ単位の隔離タイプは、バラクーダスパムファイアウォール 200 では使用できません。</p>
グローバル	<p>すべての隔離メールを指定されたグローバルアドレスに送付します。</p>

グローバル隔離設定の指定

下表は、グローバル隔離設定フィールドについての説明をまとめたものです。

フィールド	説明
隔離メール通知アドレス	<p>すべての隔離メールの送付先とするメールボックスを指定します。指定できるメールボックスは、バラクーダスパムファイアウォールによって保護されているメールサーバ (yourname@yourdomain.com)、またはリモートメールサーバのいずれかです。</p> <p><i>注意：バラクーダスパムファイアウォール 400 および 600 では、[高度な設定] → [高度なドメイン設定] ページで、ドメイン毎に隔離メール通知アドレスを指定できます。</i></p>
隔離通知件名テキスト	<p>隔離メールの件名の先頭に挿入するテキストを入力します。デフォルトのテキストは「[SPAM]」です。</p> <p>これにより、通常メールも受信するメールボックスに隔離メールが送付された場合に、隔離メールを見分けることが可能になります。</p>

ユーザ単位隔離設定の指定

下表は、ユーザ単位の隔離設定についての説明をまとめたものです。このセクションは、バラクーダスパムファイアウォール 200 では表示されません。

設定	説明
隔離通知に付加される Reply-To アドレス	<p>ユーザ隔離領域について、ユーザに送信されるすべての通信で使用される送信元アドレス。</p> <p>ユーザが返信した場合はすべてこのアドレスに送られます。</p>
隔離ホスト	<p>ユーザに送付されるすべての隔離通知メールに含まれる、ログイン用の IP アドレスまたはホスト名。</p> <p>バラクーダスパムファイアウォールとユーザネットワークの間にアドレス変換装置などがあり、ユーザがバラクーダスパムファイアウォールの IP アドレスに直接アクセスできない場合、アドレス変換装置で公開しているバラクーダスパムファイアウォールの外部 IP アドレスを指定します。</p> <p>ユーザが直接バラクーダスパムファイアウォールの IP アドレスにアクセスできる場合は、このフィールドは空白にしておいてください。</p>
隔離デフォルト	<p>作成される隔離アカウントのデフォルトの状態。</p> <p>【有効化】 に設定すると、作成されるすべての新規アカウントでユーザ単位隔離機能を使用できます。</p> <p>【無効化】 に設定すると、ユーザの隔離受信ボックスにはメールが送付されません。メールは件名に隔離通知件名テキストがタグ付けされ、ユーザの受信ボックスに送付されます。</p> <p>ユーザ単位隔離機能を一部のユーザに対してのみ有効にするには（他のユーザに対しては無効）、このフィールドを 【無効化】 に設定し、「ユーザ単位隔離アカウント設定の変更」(P.30) の指示に従ってください。</p>

設定	説明
リンクドメイン	<p>異なるドメインが同じユーザ単位設定とユーザ単位隔離受信ボックスを共有するかどうかを決定します。</p> <p>【有効化】 に設定した場合は、ドメインが異なる同じ名前のメールアドレスに対して、同じユーザ単位の設定と隔離領域が使用されます。例えば、ドメインリンクが有効であれば、<i>someuser@yourdomain.com</i> と <i>someuser@yourdomain.net</i>、<i>someuser@corp.yourdomain.com</i> が同じ設定と隔離領域を共有します。</p> <p>この機能を使用する場合は、以下のことに注意してください。</p> <ul style="list-style-type: none"> ・ [リンクドメイン] はグローバル設定です。特定のドメインやユーザのみを対象に、ドメインリンクを有効にすることはできません。 ・ この機能は、ドメインが同じで名前が異なるメールアドレスには機能しません。例えば、<i>someuser@yourdomain.com</i> は <i>s.user@yourdomain.com</i> にリンクできません。
通知間隔	ユーザに隔離領域内のメールを送信する間隔。

ユーザ単位隔離アカウント設定の変更

[基本設定] → [隔離] ページの [ユーザ単位の隔離アカウント設定変更] セクションでは、デフォルトの隔離設定をユーザ単位に変更できます。

例えば、デフォルトの隔離設定を無効に設定している場合は、このフィールドにメールアドレスを入力することによって、特定ユーザのユーザ単位隔離機能を有効にすることができます。

この機能は、バラクーダスパムファイアウォール 200 では使用できません。

デフォルトの隔離設定を変更するには、以下の手順を実行します。

1. [ユーザアカウント] ボックスで、隔離設定を変更するユーザのメールアドレスを入力します。
2. [ユーザ隔離を有効] オプションについては、以下のいずれかを選択します。
 - ・ 指定したユーザアカウントの隔離を有効にする場合は、**【はい】**
 - ・ 指定したユーザアカウントの隔離を無効にする場合は、**【いいえ】**
3. [変更保存] をクリックします。

システム IP 情報の設定

[基本設定] → [IP 設定] ページには、バラクーダスパムファイアーウォールのネットワークとメールサーバの設定が含まれています。

下表は、このページの各セクションの説明をまとめたものです。

セクション	説明
TCP/IP 設定	<p>バラクーダスパムファイアーウォールの IP アドレス、サブネットマスク、およびデフォルトゲートウェイ。</p> <p>TCP ポートは、バラクーダスパムファイアーウォールがメールを受信するポートです。通常はポート 25 が使用されます。</p>
送付先メールサーバの TCP/IP 設定	<p>[サーバ名 /IP:] 送付先メールサーバのホスト名または IP アドレス (例: <i>mail.yourdomain.com</i>)。これはスパムやウィルスの検査が完了したメールを受信するメールサーバです。</p> <p>メールサーバの IP アドレスではなく、ホスト名を指定してください。これにより、送付先メールサーバの移動や DNS の更新を行った場合も、バラクーダスパムファイアーウォールを変更する必要がなくなります。</p> <p>TCP ポートは、送付先メールサーバがメールを受信するポートです。通常はポート 25 が使用されます。</p> <p>[有効なテストメールアドレス:] メール送信のテストを行う場合は、このフィールドにアドレスを入力して [SMTP 接続テスト] をクリックします。指定したアドレスにメールが送信されます。このメールの送信元アドレスは「<i>smtptest@barracudanetworks.com</i>」です。</p>
DNS 設定	<p>ネットワーク上で使用するプライマリおよびセカンダリ DNS サーバのリストです。</p> <p>プライマリ DNS サーバとセカンダリ DNS サーバを指定してください。バラクーダスパムファイアーウォールの一部の機能（「送信者ドメイン詐称」の検出など）は、DNS が使用可能な場合にのみ実行できます。</p>
ドメイン設定	<p>デフォルトホスト名は、バラクーダスパムファイアーウォールが送信するメールメッセージ（配送不能通知、ウィルス警告通知など）の返信用アドレスで 사용되는ホスト名です。ホスト名は、デフォルトドメインに付加されます。</p> <p>デフォルトドメイン名は、バラクーダスパムファイアーウォールが送信するメールメッセージ（配送不能通知、ウィルス警告通知など）の返信用アドレスで 사용되는ドメイン名です。</p>
許可メール受信者ドメイン	<p>バラクーダスパムファイアーウォールが管理するドメインがリストされます。このリストにすべてのドメインが含まれているか確認してください。バラクーダスパムファイアーウォールは、このリストにないメッセージを拒否します。</p> <p>メールサーバと一致するすべてのドメインのメッセージを許可するには、このフィールドにアスタリスク (*) を入力します。</p> <p>注意: 1 台のバラクーダスパムファイアーウォールで複数のドメインとメールサーバをサポートできます。複数のメールサーバを使用している場合は、[高度な設定] → [高度なドメイン設定] ページを表示し、各ドメインに対応するメールサーバを入力してください。</p>

管理者画面へのアクセス制御

この項では、以下のトピックについて説明します。

- 「管理者パスワードの変更」 (本ページ)
- 「管理者画面へのアクセスの制限」 (本ページ)
- 「ウェブインターフェースポートとセッション持続時間の変更」 (P.32)

管理者パスワードの変更

管理者画面にアクセスするためのパスワードを変更するには、[基本設定] → [アドミニストレーション] ページで、要求される情報を入力して [パスワード保存] をクリックします。

管理者画面へのアクセスの制限

[基本設定] → [アドミニストレーション] ページの [管理者 IP/ 範囲] セクションでは、管理者画面へのアクセスを許可する IP アドレスの範囲を指定できます。許可されない IP アドレスから管理者画面にログインしようとする、ログインが無効であるという意味のエラーメッセージが表示されます。

注意： (ネットワーク全体ではなく) 個別の IP アドレスを追加するには、ネットマスクとして 255.255.255.255 を指定します。

IP アドレスまたはネットワークのいずれも指定しない場合は、パスワードが正しい限り、すべてのシステムからアクセスが可能になります。

ウェブインターフェースポートとセッション持続時間の変更

[基本設定] → [アドミニストレーション] ページの [ウェブインターフェース HTTP ポート] セクションで、下表のように設定します。

フィールド	説明
ウェブインターフェース HTTP	ウェブブラウザから管理者画面にアクセスするときに使用するポート (デフォルトは HTTP ポート 80)。この値を変更するには、以下の手順を行います。 <ol style="list-style-type: none">1. このフィールドに新しいポート番号を入力します。2. [ウェブインターフェース再起動] をクリックします。 管理者画面から自動的にログアウトします。3. ウェブブラウザで、管理者画面へのアクセスに使用するポートを変更します。
セッション終了期限	ユーザが管理者画面にログインしてから自動的にログオフされるまでの時間 (デフォルトは 60 分間)。この値を変更するには、以下の手順を実行します。 <ol style="list-style-type: none">1. セッションの持続時間を分単位で入力します。2. [変更保存] をクリックします。

システムのシャットダウンとリセット

この項では、以下のトピックについて説明します。

- 「システムのシャットダウン」(本ページ)
- 「フロントパネルを使用して行うシステムのリセット」(本ページ)
- 「ベイジアンデータベースのリセット」(P.33)

システムのシャットダウン

[基本設定] → [アドミニストレーション] ページの [リセット/シャットダウン] セクションでは、バラクーダスパムファイアウォールのシャットダウン、リセット、リロードを行うことができます。

警告: システムのシャットダウン、リセット、またはリロードを行うと、メールの配送が中断されることがあります。

下表は、上記のオプションについての説明をまとめたものです。

ボタン	説明
シャットダウン	システムをシャットダウンし、電源を切ります。
リセット	システムをリセットします。
リロード	最新の変更が有効にならない場合に、システム設定を再度適用します。

フロントパネルを使用して行うシステムのリセット

リセットボタンによるシステムのリセットは Firm3.3 から可能となる予定です。Firm3.1 及びそれより古い Firm ではリセットボタンを使用しないでください。

ベイジアンデータベースのリセット

[基本設定] → [ベイジアン/フィンガープリンティング] ページでは、ベイジアンデータベースをリセットできます。このデータベースには、スパムまたは非スパムとして分類したメッセージなど、[メッセージログ] ページで設定したすべてのルールが格納されています。ベイジアンデータベースを使用すると、スパム認識率が大幅に向上します。

ベイジアンデータベースをリセットして設定したルールを消去するには、**[リセット]** をクリックします。

システムレポート送付の自動化

[基本設定] → [アドミニストレーション] ページでは、指定したメールアドレスにメールの日次のシステムステータスレポートとシステム警告が自動的に送付されるように設定できます。

該当するフィールドにメールアドレス（カンマで区切る）を入力し、**【変更保存】** をクリックします。日次のシステムステータスレポートは毎日夜間に送信され、システムアラートは必要になる都度送信されます。

日次のシステムステータスレポートには、その日の 1 時間毎の拒否、隔離、タグ付け、および許可されたメッセージの数が示されます。

ブラックリストサービスへの加入

[拒否 / 許可] → [外部ブラックリスト] ページでは、各種ブラックリストサービスを設定できます。外部ブラックリストは、スパム送信者の可能性のあるインターネットアドレスのリストのことで、DNSBL または RBL とも呼ばれます。バラクーダスパムファイアウォールは、これらのリストを使用して受信メールの信憑性を検証します。システムがブラックリストにある送信者からメールを受信すると、ブラックリストの設定に基づいて、ブロック、隔離、タグ付けのいずれかをメールに対して行います。

デフォルトでは、バラクーダブラックリストサービスと spamhaus.org 外部ブラックリストサービスが使用されます。

ブラックリストにより、誤検知メール（スパムとして拒否される非スパムメール）が発生する可能性があります。バラクーダスパムファイアウォールは、正常メールをスパムメールと誤検知した場合でも、それを送信者に通知することが可能です。そのため、メールを誤検知した場合も、合法的な送信者はそれに気付いて再送することができます。

ブラックリストの設定	説明
バラクーダブラックリストサービス	バラクーダネットワークスが保持するブラックリストを有効化または無効化します。このリストには、大量なスパムの送信元として手動で確認されたサーバが含まれます。
一般的なブラックリスト	バラクーダスパムファイアウォールに組み込まれたブラックリストサービスを有効化または無効化します。指定したブラックリストに対して選択されているアクションを変更し、 【変更保存】 ボタンをクリックしてください。
カスタム外部ブラックリスト	使用を希望する上記以外のブラックリストを入力し、実行するアクションを指定します。入力したら 【追加】 をクリックし、続いて 【変更保存】 をクリックしてください。
ブラックリストに対するフルヘッダースキャン	[はい] に設定すると、ブラックリスト化された IP アドレスの有無を調べるためにメールのヘッダーがスキャンされます。 ヘッダーをスキャンするように設定すると、各ヘッダーについて DNS ルックアップが実行されるため、システムのパフォーマンスに影響が出る可能性があります。そのため、この機能は、インターネットからのメールがバラクーダスパムファイアウォールに直接配送されない場合にのみ有効にしてください。

ブラックリストサービスについて

下表は、利用可能なブラックリストサービスについての説明をまとめたものです。

ブラックリストサービス	説明
sbl.spamhaus.org	Spamhaus はインターネットのスパム送信者、スパム集団、スパム業者を追跡して、インターネット・ネットワークに信頼性の高いリアルタイム・アンチスパム・プロテクションを提供しています。また、警察当局との協力により、世界中のスパム送信者の特定・追跡を行っています。
xbl.spamhaus.org	Spamhaus は、違法な手口を使ったスパムの増加を阻止するために、Exploits Block List (XBL) を公表しました。このリストは、サードパーティの違法な手口に使われる IP アドレスのリアルタイム DNS ベースデータベースです。このデータベースには、オープンプロキシ、スパムエンジンに組み込まれたワーム / ウィルスなど、スパム送信者が使用する様々なタイプのトロイの木馬が含まれます。
relays.ordb.org	ORDB.org は、オープンリレーデータベースです。ORDB.org は、検証済みオープン SMTP リレーの IP アドレスを蓄積する非営利団体です。これらのリレーは、無断で送信されるバルクメールの経路として使用されます。システム管理者は、このリストを使い、これらのアドレスでのサーバとのメール交換を許可するか、あるいは拒否するかを選択できます。
bl.spamcop.net	SpamCop は最もアグレッシブなスパムサービスで、非スパムをスパムと誤認するエラーが頻繁に発生します。多数のメールサーバではブラックリストを「タグ付けのみ」モードで利用できますので、SpamCop を使用する場合はこのモードにすることをお勧めします。

拒否 / 許可フィルターの使用

[拒否 / 許可] タブには、バラクーダスパムファイアウォールのスパム / ウィルス検出用のデフォルト機能を強化するための様々なフィルターが用意されています。

バラクーダスパムファイアウォールでは、拒否 / 許可フィルターで正規表現を使用できません。正規表現の詳細については、付録 A を参照してください。

下表は、これらの拒否 / 許可フィルターについての説明の記載場所をまとめたものです。

拒否 / 許可フィルター	記載場所
送信者 IP アドレス	P.36
送信先ドメイン	P.37
送信者メールアドレス	P.37
受信者メールアドレス	P.38
添付ファイルのタイプ	P.38
件名の内容	P.39
本文の内容	P.40
ヘッダーの内容	P.40

IP アドレス / ネットワークによるフィルタリング

[拒否 / 許可] → [IP アドレスでの拒否 / 許可] ページでは、送信者 IP ネットワークによるメールのフィルタリングを設定できます。

下表は、このページのフィールドについての説明をまとめたものです。

フィルター	説明
許可する IP 範囲	<p>ホワイトリストに任意の IP アドレスまたはネットワークを登録します。IP アドレスを個別に登録するには、ネットマスク 255.255.255.255 を使用します。</p> <p>ホワイトリスト化された IP アドレスは、スパムスコアリングと、添付ファイルフィルター、本文フィルター、件名フィルターを除くすべてのブラックリストを参照しません。</p> <p>許可する IP アドレスにノートを追加する場合は、コメントフィールドを使用します。</p> <p>1 つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックしてください。</p>
拒否する IP 範囲	<p>ブラックリストに任意の IP アドレスまたはネットワークを登録します。IP アドレスを個別に登録するには、ネットマスク 255.255.255.255 を使用します。</p> <p>ブラックリスト化された IP アドレス / ネットワークは、IP アドレス / ネットワークに基づくホワイトリスト以外のすべてのホワイトリストを参照しません。特定の IP / 範囲に対して、拒否、隔離、またはタグ付けのアクションを指定することができます。</p> <p>コメントフィールドを使用して、拒否する IP アドレスにノートを付記することができます。</p> <p>1 つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックしてください。</p>

送信元ドメインによるフィルタリング

[拒否 / 許可] → [送信元ドメインによる拒否 / 許可] ページでは、送信元ドメインによるメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。

フィルター	説明
許可する送信者ドメイン / サブドメイン	<p>ホワइटリストに含めるドメインまたはサブドメインを登録します。ドメインをホワइटリスト化すると、サブドメインもすべて自動的にホワइटリスト化されます。例えば、<i>customer.com</i>を追加すると、<i>joe@office1.customer.com</i> や <i>joe@customer.com</i> からのメールも許可されます。</p> <p>ホワइटリスト化されたドメイン / サブドメインは、スパムスコアリングと、IP 拒否 / 許可フィルターおよび本文 / 件名フィルターを除くすべてのブラックリストを参照しません。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>
拒否する送信者ドメイン / サブドメイン	<p>拒否するドメインまたはサブドメインを登録します。ドメインを拒否すると、すべてのサブドメインも自動的に拒否されます。例えば、<i>spammer.com</i>を追加すると、<i>joe@server1.spammer.com</i> や <i>joe@spammer.com</i> からのメールも拒否されます。</p> <p>ブラックリスト化されたドメイン / サブドメインは、IP アドレス / ネットワークとドメイン / サブドメインに基づくホワइटリストを除くすべてのホワइटリストを参照しません。特定のIP / 範囲に対して、拒否、隔離、またはタグ付けのアクションを指定することができます。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>

送信者メールアドレスによるフィルタリング

[拒否 / 許可] → [送信者メールアドレスによる拒否 / 許可] ページでは、送信者のメールアドレスに基づくメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。

フィルター	説明
許可するメールアドレス	<p>ホワइटリストに含める送信者メールアドレスを登録します。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>
拒否するメールアドレス	<p>ブラックリストに含める送信者メールアドレスを登録し、拒否、隔離、またはタグ付けのアクションを指定します。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>

受信者メールアドレスによるフィルタリング

[拒否 / 許可] → [受信者メールアドレス拒否 / 許可] ページでは、受信者メールアドレスによるメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。

フィルタ	説明
許可するメールアドレスまたはドメイン	<p>ホワइटリストに含める受信者メールアドレスを登録します。</p> <p>このリストに登録された受信者のメールに対しては、スパムスコアリングは行われません。ホワइटリスト化された受信者は、IP 拒否 / 許可フィルターおよび本文 / 件名フィルターを除くすべてのブラックリストを参照しません。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>
拒否するメールアドレスまたはドメイン	<p>ブラックリストに含める受信者のメールアドレスを登録し、拒否、隔離、またはタグ付けのアクションを指定します。</p> <p>受信者のメールアドレスを拒否する最も一般的な理由の1つとしては、ユーザが会社を辞めた後も、メールアカウントをメールサーバに残しておきたい場合が挙げられます。</p> <p>このリストに登録された受信者は、送信者の IP アドレス、ドメイン、メールアドレス、または本文 / 件名 / ヘッダーに対して許可フィルターが設定されない限り、メールを受信することはできません。</p> <p>1つのエントリを登録したら 【追加】 をクリックし、次に 【変更保存】 をクリックします。</p>

添付ファイルタイプによるフィルタリング

[拒否 / 許可] → [添付ファイル拡張子フィルタリング] ページでは、特定のファイル拡張子を持つファイルが添付されたメールの拒否または隔離を設定できます。

下表は、このページのパラメータについての説明をまとめたものです。これらの値を変更した後、**【変更保存】** をクリックしてください。1つのフィルターに複数行を入力できます。1行に1つのファイル拡張子タイプを入力してください。

フィルタ	説明
添付ファイル拒否	
拒否する添付ファイル拡張子	拒否する添付ファイルの拡張子を登録します（拡張子の前にドット「.」は付けません）。拒否する拡張子を含むファイルがメールに添付されている場合、バラクーダスパムファイアーウォールはメール全体を拒否します。
圧縮された添付ファイルの拡張子による拒否	拒否する拡張子の有無を調べるために圧縮された添付ファイル（zip ファイルなど）をスキャンさせる場合は、 【はい】 を選択します。拒否する拡張子を含む圧縮ファイルがメールに添付されている場合、バラクーダスパムファイアーウォールはメール全体を拒否します。
パスワード保護付きで圧縮された添付ファイルの拡張子による拒否	<p>パスワード保護付きで圧縮された添付ファイル（zip ファイルなど）を含むメールをシステムに拒否させる場合は、【はい】 を選択します。</p> <p>パスワード保護付きの圧縮ファイルの場合は、ファイルの拡張子をスキャンすることはできません。そのため、これらのタイプのアーカイブは拒否するのが一般的です。</p>

フィルタ	説明
拒否の通知	
対象の受信者に禁止されている添付ファイルによる遮断を通知	禁止されたファイル拡張子が検出されたために受信メールが拒否されたときに受信者に通知する場合は、[はい] を選択します。
禁止されている添付ファイルによる遮断を送信者に通知	禁止されたファイル拡張子が検出されたためにメールが拒否されたときに送信者に通知する場合は、[はい] を選択します。
添付ファイルによる隔離	
隔離する添付ファイル拡張子	隔離する添付ファイルの拡張子を登録します（「.」は付けません）。添付ファイルを含むメール全体が隔離アカウントに送られます。
アーカイブ内の添付ファイル拡張子による隔離	隔離する拡張子の有無を調べるために圧縮された添付ファイル（zip ファイルなど）をシステムにスキャンさせる場合は、 【はい】 を選択します。隔離する拡張子を含む圧縮ファイルがメールに添付されている場合、バラクーダスパムファイアーウォールはメール全体を隔離します。
パスワード保護付きのアーカイブ添付による隔離	パスワード保護付きの圧縮ファイル（zip ファイルなど）を含むメールをシステムに隔離させる場合は、 【はい】 を選択します。 パスワード保護付きの圧縮ファイルの場合は、ファイルの拡張子をスキャンすることはできません。そのため、これらのタイプのアーカイブは拒否するのが一般的です。

注意：添付ファイルフィルタリングは、ホワイトリスト化された送信者からのメールを含む、すべてのメールに対して実行されます。そのため、ホワイトリスト化された送信者が許可されないタイプの添付ファイルを含むメールを送信してきた場合には、そのメッセージは（受信者の設定に応じて）拒否または隔離されます。

件名によるフィルタリング

[拒否 / 許可] → [件名によるフィルタリング] ページでは、件名によるメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。変更後、**【変更を保存】** をクリックしてください。

フィルタ	説明
件名による拒否	件名に含まれる場合にメールを拒否（廃棄）する単語、正規表現、または文字を入力します。
件名による隔離	件名に含まれる場合にメールを隔離する単語、正規表現、または文字を入力します。
件名によるタグ付け	件名に含まれる場合にメールにタグ付けする単語、正規表現、または文字を入力します。
件名ホワイトリスト化	件名に含まれる場合にメールをホワイトリスト化する単語、正規表現、または文字を入力します。

内容によるフィルタリングを使用する場合は、以下のことに注意してください。

- 1つのフィルターに複数行を入力できますが、各行に入力できる正規表現または単語は1つだけです。各行は個別に適用されます。

- HTMLソース内の文字の間に埋め込まれているHTMLの注釈やタグは取り除かれるため、内容によるフィルタリングはウェブブラウザ上に実際に表示される単語に対して適用されます。

本文の内容によるフィルタリング

[拒否 / 許可] → [本文によるフィルタリング] ページでは、メッセージ本文によるメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。このページを変更した後、**【変更保存】** をクリックしてください。

フィルタ	説明
メッセージ本文による拒否	メッセージ本文に含まれる場合にメールを拒否する単語、正規表現、または文字を入力します。
メッセージ本文による隔離	メッセージ本文に含まれる場合にメールを隔離する単語、正規表現、または文字を入力します。
メール本文によるタグ付け	メッセージ本文に含まれる場合にメールにタグ付けする単語、正規表現、または文字を入力します。
メッセージ本文のホワイトリスト化	メッセージ本文に含まれる場合にメールをホワイトリスト化する単語、正規表現、または文字を入力します。

内容によるフィルタリングを使用する場合は、以下のことに注意してください。

- 1つのフィルターに複数行を入力できますが、各行に入力できる正規表現または単語は1つだけです。各行は個別に適用されます。
- HTMLソース内の文字の間に埋め込まれているHTMLの注釈やタグは取り除かれるため、内容によるフィルタリングはウェブブラウザ上に実際に表示される単語に対して適用されます。

ヘッダーの内容によるフィルタリング

[拒否 / 許可] → [ヘッダによるフィルタリング] ページでは、ヘッダーによるメールのフィルタリングを設定できます。

下表は、このページのパラメータについての説明をまとめたものです。これらの値を変更した場合は、**【変更を保存】** をクリックしてください。

フィルター	説明
ヘッダーによる拒否	ヘッダーに含まれる場合にメールを拒否する単語、正規表現、または文字を入力します。
ヘッダーによる隔離	ヘッダーに含まれる場合にメールを隔離する単語、正規表現、または文字を入力します。
ヘッダーによるタグ付け	ヘッダーに含まれる場合にメールにタグ付けする単語、正規表現、または文字を入力します。
ヘッダーのホワイトリスト化	ヘッダーに含まれる場合にメールをホワイトリスト化する単語、正規表現、または文字を入力します。

内容によるフィルタリングを使用する場合は、以下のことに注意してください。

- 1つのフィルターに複数行を入力できますが、各行に入力できる正規表現または単語は1つだけです。各行は個別に適用されます。
- HTMLソース内の文字の間に埋め込まれているHTMLの注釈やタグは取り除かれるため、内容によるフィルタリングはウェブブラウザ上に実際に表示される単語に対して適用されます。

システム設定のバックアップとリストア

バラクーダ管理者画面では、以下の情報のバックアップとリストアを行うことができます。

- バラクーダスパムファイアウォールのシステム設定。これには、管理者画面の各ページで設定されたすべての設定値が含まれます。
- ユーザ単位の設定。これには、各ユーザが作成した許可するメールのリストや拒否（廃棄）するメールのリスト、ユーザの隔離通知間隔、ユーザが設定したパスワードが含まれます。
- ベイジアンデータベースに格納される情報。これには、スパムまたは非スパムに設定されたすべてのメールが含まれます。

システムデータのバックアップ

システムのバックアップを作成するには、以下の手順を実行します。

1. 以下の手順で、システム設定のバックアップを作成します。
 - a. [高度な設定] → [設定のバックアップ/リストア] ページで、**[バックアップ]** をクリックします。
 - b. システム設定のバックアップファイル (`barracuda.conf`) をローカルシステムに保存します。
2. 以下の手順で、ユーザ設定のバックアップを作成します。
 - a. [ユーザ] → [ユーザバックアップ/リストア] ページで、**次のどちらか**をクリックします。
 - 最新のバックアップファイルを指定した場所に保存する場合は、[バックアップファイルダウンロード]
 - (すでに存在するバックアップファイルを保存するのではなく) バックアップファイルを新規作成する場合は、[バックアップファイルをすぐに作成]
 - b. ユーザ設定のバックアップファイル (`pu_config.tgz`) をローカルシステムに保存します。
3. 以下の手順で、ベイジアンデータベースのバックアップを作成します
 - a. [基本設定] → [ベイジアン/フィンガープリンティング] ページで、**[バックアップ]** をクリックします。
 - b. ベイジアンのバックアップファイル (`bayes.tgz`) をローカルシステムに保存します。

注意：バックアップファイルを編集しないでください。設定の変更は、必ず管理者画面で行う必要があります。設定バックアップファイル (*barracuda.conf*) にはチェックサムが含まれているため、このファイルを変更するとシステムにアップロードできなくなります。

システムデータのリストア

バックアップファイルからシステム設定をリストアするには、以下の手順を実行します。

注意：システムのリストアは、メールトラフィックの少ない営業時間外の時間帯に行うようにしてください。リストアには数分しかかかりませんが、スパムファイアーウォールはこの間サービスを停止します。

1. 以下の手順で、システム設定のリストアを行います。
 - a. [高度な設定] → [設定バックアップ/リストア] ページで、**【参照】** をクリックします。
 - b. 設定バックアップファイル (*barracuda.conf*) を選択し、**【今すぐアップロード】** をクリックします。
2. 別のバラクーダスパムファイアーウォール上に設定をリストアする場合は、以下も更新します。
 - ・ ウィルスとスパムの定義 ([高度な設定] → [エネルギー充填サービス] ページで更新)
 - ・ ファームウェア ([高度な設定] → [ファームウェア更新] ページで更新)
3. 以下の手順で、ユーザ設定をリストアします。
 - a. [ユーザ] → [ユーザバックアップ/リストア] ページで、**【参照】** をクリックします。
 - b. ユーザ設定バックアップファイル (*pu_config.tgz*) を選択し、**【今すぐアップロード】** をクリックします。
4. 以下の手順で、ベイジアンデータベースをリストアします。
 - a. [基本設定] → [ベイジアン/フィンガープリンティング] ページで、**【参照】** をクリックします。
 - b. ベイジアンバックアップファイル (*bayes.tgz*) を選択し、**【今すぐアップロード】** をクリックします。

エネルギー充填サービスを使用したスパムとウィルス定義の更新

[高度な設定] → [エネルギー充填サービス] ページでは、スパムとウィルスの現在の定義を手動で更新できるほか、バラクーダスパムファイアウォールが更新の有無を確認する間隔を変更できます。

エネルギー充填サービスは、バラクーダスパムファイアウォールにスパムとウィルスの最新の定義を提供します。

下表は、このページに用意されている [スパム定義更新] フィールドについての説明をまとめたものです。このページを更新した場合は、**【変更を保存】** をクリックしてください。

フィールド	説明
現在のスパム定義バージョン	バラクーダスパムファイアウォール上で現在稼働しているバージョンを表示します。
利用可能な最新バージョン	利用可能な最新バージョンを表示します。バラクーダスパムファイアウォール上で現在稼働しているバージョンが最新でない場合は、 【更新】 をクリックして最新バージョンをダウンロードしてください。すでに最新のバージョンが稼働している場合は、[更新] ボタンは無効になります。
前バージョン	システム上で稼働していた前バージョンを表示します。このバージョンのスパム定義に戻す場合は、[戻す] をクリックします。
スパム定義自動更新	新バージョンが利用可能になったときに、定義を自動的に更新するかどうかを指定します。 【はい】 に設定することをお勧めします。
スパム定義更新頻度	スパムファイアウォールが、更新の有無を確認する頻度を指定します。 【1 時間毎】 に設定することをお勧めします。 1 時間毎の更新は毎時 00 分に行われます。日次更新は、12:20a.m. (午前 0 時 20 分) に行われます。

下表は、このページの [ウィルス定義更新] フィールドについての説明をまとめたものです。このページを更新した場合は、**【変更を保存】** をクリックしてください。

フィールド	説明
現在のウィルス定義バージョン	バラクーダスパムファイアウォール上で現在稼働しているバージョンを表示します。表示されるバージョン情報の量を増やす場合は、 【リリースノートを表示】 をクリックしてください。
利用可能な最新バージョン	利用可能な最新バージョンを表示します。バラクーダスパムファイアウォール上で現在稼働しているバージョンが最新でない場合は、 【更新】 をクリックして最新バージョンをダウンロードしてください。すでに最新のバージョンが稼働している場合は、[更新] ボタンは無効になります。
前バージョン	システム上で稼働していた前バージョンを表示します。このバージョンのウィルス定義に戻す場合は、[戻す] をクリックします。
ウィルス定義自動更新	新バージョンが利用可能になったときに、定義を自動的に更新するかどうかを指定します。 【はい】 に設定することをお勧めします。
ウィルス定義更新頻度	スパムファイアウォールが、更新の有無を確認する頻度を指定します。 【1 時間毎】 に設定することをお勧めします。 1 時間毎の更新は毎時 00 分に行われます。日次更新は 12:40a.m. (午前 0 時 40 分) に行われます。

管理者画面の外観のカスタマイズ

[高度な設定] → [外観] ページでは、管理者画面とユーザに送られるメール隔離通信文で使用されるデフォルトイメージをカスタマイズできます。このタブはスパムファイアウォール 600 のみ表示されます。

下表は、このページのフィールドについての説明をまとめたものです。このページを更新した場合は、**[変更を保存]** をクリックしてください。

フィールド	説明
全般	
スパムファイアウォール名	ログイン画面上に表示するシステム名を指定します（ユーザ名フィールドとパスワードフィールドの上）。デフォルト名は「Barracuda Spam Firewall」です。
ウェブインターフェース	
イメージプレビュー	管理者画面で使用されている現在のイメージを表示します。このプレビューは新しいイメージをシステムにアップロードすると更新されます。
新イメージのアップロード	管理者画面でカスタムイメージを使用するには、 [参照] をクリックし、使用するイメージを指定してから、 [今すぐアップロード] をクリックします。 アップロードされたイメージは、管理者画面の左上隅に表示されます。推奨されるイメージサイズは 159 × 64 ピクセルです。形式は jpg、gif、または png、大きさは 50k 未満としてください。
イメージ URL	カスタムイメージをクリックすると表示される URL。
リセット	システムを出荷時のデフォルトイメージと URL に戻します。デフォルトイメージはバラクーダネットワークスのロゴです。
隔離メール	
イメージプレビュー	ユーザに送られる隔離メールで使用される現在のイメージを表示します。このプレビューは、新しい隔離通知メールイメージをシステムにアップロードすると更新されます。
新イメージのアップロード	隔離メールでカスタムイメージを使用するには、 [参照] をクリックし、使用するイメージを指定してから、 [今すぐアップロード] をクリックします。 アップロードされたイメージが、隔離メールの左上隅に表示されます。推奨されるイメージサイズは 159 × 64 ピクセルです。形式は jpg、gif、または png、大きさは 100k 未満としてください。
ヘッダー背景色	隔離メールで使用されるテーブルヘッダーの背景色を指定します。この値には標準 HTML16 進コードを使用してください。
ヘッダーフォント色	隔離メールで使用されるテーブルヘッダーのフォント色を指定します。この値には標準 HTML16 進コードを使用してください。
リセット	隔離メールのカスタム設定をクリアして、デフォルトのイメージと色に戻すことができます。

高度な設定の構成

この項では、[高度な設定] タブで利用できるいくつかの高度な設定について説明します。ほとんどの場合、この項で説明するデフォルト設定を変更する必要はありません。この項で説明する作業を行う場合は、事前にテクニカルサポートにご相談になることをお勧めします。

この項では以下のトピックについて説明します。

- 「フィンガープリンティングの動作の変更」 (P.45)
- 「メールプロトコル検査の設定」 (P.46)
- 「メッセージレートコントロールの設定」 (P.48)
- 「個別アカウントの有効化」 (P.48)
- 「システムファームウェアバージョンの更新」 (P.49)
- 「Syslog サーバを使用したシステムログの集中管理」 (P.49)
- 「クラスタ化環境の設定」 (P.50)
- 「シングルサインオンの導入」 (P.52)

フィンガープリンティングの動作の変更

デフォルトでは、メールフィンガープリンティングはバラクーダスパムファイアウォール上で有効化されています。この設定は変更しないことをお勧めします。

フィンガープリンティングは、すでにスパムとして確認されているメールの特徴を調べ、この情報を使用して、スパムファイアウォールを通過する同一または類似のメールを分類する機能です。

スパムとして特定されたメールは、デフォルトではバラクーダセントラルに送られ「フィンガープリント (指紋)」が採取されます。このフィンガープリンティング処理により、システムが他の類似したメールをスパムとして分類することが可能になります。

フィンガープリンティング機能では専門的な URL 分析も行われます。この分析では、疑わしいメールメッセージに含まれる URL が詳細に検査され、バラクーダデータベースに保持される既知のスパム発信者 URL と比較されます。これにより、偽造 URL をユーザに届く前に削除することが可能になります。

システム上のフィンガープリンティングの動作を変更するには、以下の手順を実行します。

1. [基本設定] → [ベイジアン / フィンガープリンティング] ページを表示します。
2. このページの [バラクーダメールフィンガープリンティング] セクションの設定を更新します。

このセクションの各フィールドの説明については、下表を参照してください。

3. **【変更保存】** をクリックします。

フィールド	説明
メールフィンガープリントを検査	メールに対してフィンガープリント検査を実行するかどうかを選択します。 [はい] を選択すると、受信メールが、スパムメッセージのフィンガープリントを蓄積したデータベースと照合されます。
インテンション解析	メールに対してインテンション解析を実行するかどうかを選択します。 [はい] を選択すると、バラクーダスパムファイアウォールはメールに含まれる URL からメールの意図を推定します。
インテンション解析によるタグ付け	インテンション解析によってスパムと判定されたメールを（拒否する代わりに）タグ付けするかどうかを選択します。 推奨される設定値は、[いいえ] です。
バラクーダネットワークスにメールを送る	スパムに分類されたメールのコピーをさらに詳しく解析するためにバラクーダネットワークスに転送するかどうかを選択します。 [はい] に設定すると、ユーザがメッセージログでスパムと分類したすべてのメールが転送されます。これによりバラクーダネットワークスがメールを解析することが可能になり、当社が保持するスパム定義とインテンション解析の精度が向上します。

メールプロトコル検査の設定

[高度な設定] → [メールプロトコル] ページでは、SMTP 検査のデフォルト設定を変更できます。下表は、このページの各設定についての説明をまとめたものです。変更後には、**【変更保存】** をクリックしてください。

設定	説明
メールプロトコル (SMTP) 検査	
SMTP HELO を要求	バラクーダスパムファイアウォールに接続するメールクライアントが、SMTP HELO コマンドを使って自身を紹介するかどうかを指定します。 このオプションで 【はい】 を選択すると、スパム送信者が使用する自動スパム送信プログラムを拒否できることがあります。 デフォルト設定は、 【いいえ】 です。
RFC 821 コンプライアンスを強制	SMTP の MAIL FROM および RCPT TO コマンドが「<」と「>」で囲まれたアドレスを含むことを必須とするかどうかを指定します。必須とする場合は、SMTP の MAIL FROM および RCPT TO コマンドが RFC 822 形式のフレーズまたはコメントを含まないことも必須となります。 このオプションを 【はい】 に設定すると、スパム送信者からのメッセージだけでなく、RFC 821 標準に適合しないいくつかの Windows メールプログラム (MS-Outlook など) も拒否されます。そのため、デフォルト設定は 【いいえ】 になっています。
完全修飾ドメイン名を要求	完全修飾ドメイン名を必須とするかどうかを指定します。
偽造 From ドメイン名を拒否	DNS エントリを持たないドメインから送信されたメールを拒否するかどうかを指定します。

設定	説明
送信者スプーフィング プロテクション	<p>部外者がこのドメインを送信元アドレスとしてメールを送信する「送信者なりすまし」を防止するかどうかを選択します。このオプションを [はい] に設定すると、バラクーダスパムファイアウォールがメール受信を行うドメインを送信元とするすべてのメールが拒否されます。</p> <p>このオプションは、ユーザのドメインから送信されるすべてのメールが、バラクーダスパムファイアウォールを介さず直接メールサーバに配送される場合にのみ有効にしてください。</p>
SPF/Caller ID の設定	
送信者ポリシーフレームワーク (SPF) / マイクロソフト Caller ID	<p>SPF (Sender Policy Framework) と Microsoft Caller ID の検査は、スパムと正当なメールの判別に役立ちます。</p> <p>SPF の仕組み - ドメイン所有者が、DNS に含まれる送信メールサーバのアドレスを指定します。SMTP 受信機 (バラクーダスパムファイアウォールなど) は、メールが届くと、それに含まれる送信メールサーバをドメイン所有者の DNS レコードと照合します。この検査で送信メールサーバのレコードが検出されない場合、そのメールはスパムと判定されます。</p> <p>この機能を有効にすると、ドメインの SPF または Caller ID レコード (存在する場合) を検索するために複数の DNS クエリーが実行されるため、バラクーダスパムファイアウォールのパフォーマンスに影響が出ます。このオプションをオンにした場合は、この検査に合格しないメールは拒否されます。デフォルト設定は、[いいえ] です。</p>
信頼できる送信者 IP アドレス	<p>外部ソースからのメールをバラクーダスパムファイアウォールに転送するように設定したマシンの IP アドレスをまとめたリストです。</p> <p>SPF/Caller ID 検査の実行中には、このリストに含まれる IP アドレスは無視され、Received ヘッダーリストの次の IP アドレスがチェックされません。</p>
Incoming SMTP タイムアウト	
Incoming SMTP タイムアウト	<p>1 回の Incoming SMTP トランザクションに費やす時間に制限を設けます。デフォルト設定は 30 秒間です。</p> <p>SMTP トランザクションに時間制限を設定すると、スパム送信者がバラクーダスパムファイアウォールへの接続を長時間維持することが不可能になり、システムリソースへの影響を防止することができます。SMTP トランザクションでこの制限時間を超えたメールは、[メッセージログ] ページに、[タイムアウト] を理由として [拒否] されたメールとして表示されます。</p>
SMTP セッション毎のメール数	
SMTP セッション毎のメール数	<p>1 回の SMTP セッションで扱うことのできるメール数の上限を設定します。1 回のセッションでメール数がこのしきい値を超えると、それ以降のメールは拒否されます。これらのメールは、メッセージログに、「拒否」メールとして「コネクション毎の最大メール数」という理由とともに記載されます。</p>
SMTP ウェルカムバナー	
SMTP ウェルカムバナー	<p>バラクーダスパムファイアウォールに接続する SMTP クライアントに表示されるウェルカムバナーを指定します。</p> <p>この値は、お使いのネットワーク内で一意でなければなりません。この値が一意でない場合は、ウェルカムバナーが重複するサーバを宛先とするメールは配送されません。この値を空白にして、バラクーダスパムファイアウォールによる自動設定を選択することもできます。</p>

設定	説明
バラクーダヘッダーを削除	
バラクーダヘッダーを削除	メールがシステムから送信される前に付加されるバラクーダのカスタム X ヘッダーを削除します。 バラクーダのヘッダーには、メッセージがタグ付け、隔離、または拒否された理由が含まれるので、削除しないことをお勧めします。この情報は、メール処理で問題が発生したときの原因究明と解決に役立ちます。

メッセージレートコントロールの設定

[高度な設定] → [レートコントロール] ページでは、30 分間に同一の IP アドレスからの接続を許可する回数を設定できます。レートコントロールにより、短時間に大量のメールをサーバに送信してくるスパム送信者やスパムプログラムからユーザを保護することができます。

下表は、このページの各設定についての説明をまとめたものです。変更後には、**[変更保存]** をクリックしてください。

設定	説明
メッセージレートコントロール	30 分間に同一の IP アドレスからの接続を許可する最大数を指定します。接続回数がこのしきい値を超えると、バラクーダスパムファイアウォールは以降の接続 / メールを拒否します。 送信元が合法的なメールサーバであれば、通知のメールに反応し、送信者または送信元メールサーバに再試行を要求するでしょう。一方、送信元がスパム送信者の場合は、通知メールに反応せず、送信に失敗した時点でメール送信を停止すると予想されます。
レートコントロール除外 IP アドレス / IP アドレス範囲	レートコントロールから除外する IP アドレスの範囲を入力します。(範囲ではなく) 単一の IP アドレスを入力する場合は、ネットマスクとして 255.255.255.255 を入力します。

個別アカウントの有効化

バラクーダスパムファイアウォールの導入直後には、管理者がシステムに慣れるために数個のアカウントだけを有効にすることをお勧めします。この間に数人のユーザに操作方法を習得してもらい、その上で組織全体に新機能を導入すると、作業をスムーズに進めることができます。

個別アカウントを有効にするには、以下の手順を実行します。

1. [高度な設定] → [明示的ユーザ] ページを表示します。
2. [メールアドレス] フィールドに、有効にするアカウントのメールアドレスを入力します。
3. [追加] をクリックします。

注意：スパム / ウィルス保護は、*Email Address* リストに登録されたアカウントだけに適用されます。RBL、レートコントロール、受信者検証は、このリストには関係なく、すべての受信メールに適用されます。

システムファームウェアバージョンの更新

[高度な設定] → [ファームウェア更新] ページでは、手動操作により、システムのファームウェアバージョンを更新するか、以前のバージョンに戻すことができます。

以前のファームウェアバージョンに戻す必要があるのは、ダウンロードした新バージョンに予期しない問題が発生した場合だけです。この場合は、前バージョンのファームウェアに戻す前に、テクニカルサポートにご連絡ください。

最新バージョンのファームウェアを手動でロードするには、以下の手順を実行します。

注意：新しいファームウェアバージョンを適用すると、一時的にサービスが停止します。そのため、新しいファームウェアバージョンの適用は問題のない時間に行うようにしてください。

1. 最新のファームウェアバージョンのリリースノートを読んで、新機能の情報を確認します。

2. **[今すぐダウンロード]** をクリックします。

すでに最新のファームウェアバージョンがある場合には、このボタンは無効化されています。

3. ファームウェアバージョンのダウンロード終了後、以下の手順で起動します。

- a. 管理者画面からログアウトします。
- b. 管理者画面に再度ログインし、[高度な設定] → [ファームウェア更新] ページを表示します。
- c. **[適用]** をクリックします。

ダウンロードしたファームウェアを起動すると、バラクーダスパムファイアウォールはリセットされます。リセット後、メールのフィルタリングは自動的に継続されます。

Syslog サーバを使用したシステムログの集中管理

[高度な設定] → [Syslog] ページでは、バラクーダスパムファイアウォールが syslog データを送信するサーバーを指定できます。下表は、syslog サーバに送信できる 2 種類のデータについての説明をまとめたものです。

Syslog フィールド	説明
Mail Syslog 設定	<p>メールフローに関連するデータを受信する syslog サーバの IP アドレスを入力します。このデータは、メッセージログの作成に使用されるデータと同じ内容です。</p> <p>このデータには、接続中の IP、送信元アドレス、送信先アドレス、メールのスパムスコアなどの情報がすべて含まれます。この syslog データは、指定された syslog サーバに搭載されている mail ファシリティのデバッグ最優先レベルで表示されます。</p>
ウェブ GUI Syslog 設定	<p>ウェブインターフェースに関連するデータを受信する syslog サーバの IP アドレスを入力します。このデータには、ユーザのログイン時刻と、バラクーダスパムファイアウォールに行った設定変更の情報が含まれます。</p> <p>この syslog データは、local1 ファシリティに、ログイン情報の場合は情報最優先レベルで、設定変更の場合はデバッグ最優先レベルでそれぞれ表示されます。</p>

Syslog はリモートにシステムログを送信するための標準 UNIX/Linux ツールで、すべての UNIX/Linux システムで利用できます。Syslog サーバは、無償・有償の多数のベンダから Windows プラットフォーム用も提供されています。

Syslog のサポートは、バラクーダスパムファイアウォール 200 には含まれていません。

クラスタ化環境の設定

[高度な設定] → [クラスタリング] ページでは、複数のバラクーダスパムファイアウォールシステムをリンクして環境設定を同期化できるほか、アクティブなシステムが停止した場合に使用するスタンバイシステムを指定することもできます。

クラスタ化の機能は、バラクーダスパムファイアウォール 400 および 600 でのみ利用できます。

クラスタ化により、複数のバラクーダスパムファイアウォールシステムの管理が容易になるだけでなく、伝播されたデータを 100% カバーする冗長性も得られます。

下表は、他のクラスタ化システムに伝播される情報と伝播されない情報をまとめたものです。

伝播されるデータ	伝播されないデータ
管理者画面で設定されたシステム設定 (グローバル、ドメイン)	システム IP 設定 (P.31) を参照。
ユーザの隔離インターフェースで指定されたユーザ毎隔離設定	SSL 設定 (P.60) を参照。
メッセージログ	
ベイジアンデータベース	
隔離受信ボックス	

各ユーザアカウントは、クラスタ内に 1 台のプライマリサーバと 1 台のセカンダリサーバを持ちます。プライマリサーバは最初にクラスタに加わり、セカンダリサーバはその次にクラスタに加わります。各アカウントに対し、常に、同じ情報 (設定と隔離メッセージ) を保持する 2 台のサーバが存在します。

下表は、[高度な設定] → [クラスタリング] ページ上の設定についての説明をまとめたものです。

フィールド	説明
クラスタ設定	
クラスタ共有鍵	<p>クラスタ内のすべてのバラクーダスパムファイアウォールによって共有されるパスコード。クラスタ内のすべてのバラクーダスパムファイアウォールは同じ共有パスコードを保持しなければなりません。</p> <p>システムをクラスタに追加する前に、既存のシステムに設定されているパスコードを確認してください。</p>

フィールド	説明
クラスタホスト名	<p>システムのホスト名。クラスタ内の他のシステムは、このホスト名を使ってシステムと通信します。このフィールドが空白の場合は、自動的にシステムの IP アドレスが使用されます。</p> <p>このホスト名が DNS で解決不能な場合は、このシステムをクラスタに加える前に、クラスタ内の各バラクーダスパムファイアーウォールについて、このページの最下部にある [ローカルホストマップ] にエントリを作成してください。</p>
クラスタシステム	
クラスタフィールド	<p>システムを加えるクラスタ内のいずれかのバラクーダスパムファイアーウォールシステムの IP アドレスまたはホスト名を入力し、[クラスタシステム追加] をクリックします。</p> <p>このシステムがクラスタに加わると、そのクラスタから環境設定が引き出され、このシステムの設定に変更されます。ユーザリストはクラスタとこのシステムの間で同期されるため、このシステム上のユーザは失われず、クラスタに統合されます。</p> <p>システムがクラスタに正常に追加されると、クラスタ内の各システムの IP アドレスが、アクティブな状態（ステータスランプが緑色）で表示されます。</p>
クラスタシステムリスト	<p>[クラスタシステム] には、このクラスタ内の他のシステムが表示されます。</p> <p>[モード] は、そのシステムが「スタンバイ」、「アクティブ」のどちらかを示します。いずれかのシステムが停止したときに切り替える予備システムが必要な場合は、1 台のサーバを「スタンバイ」として指定します。「アクティブ」として指定されたサーバだけが受信メールをフィルタリングします。</p> <p>スタンバイサーバ上でメールのフィルタリングを開始する場合は、スタンバイサーバを手動で「アクティブ」に切り替える必要があります。この切り替えは、アクティブなサーバが停止すると自動的に行われるわけではありません。</p> <p>[ステータス] は、そのシステムが稼働中かどうかを緑色のドットによって示します。</p>
ローカルホストマップ	
ホスト名 /IP アドレス	<p>ローカルホスト名を、クラスタ内のシステムの IP アドレスにマップします。このマッピングにより、DNS ホスト名から IP アドレスへのルックアップがローカルで変更されます。新しいエントリを指定したら、その都度 [追加] をクリックします。このマッピングは、クラスタ内の他のシステムと同期されません。</p> <p>ローカルホストマップ機能は、次のような状況で使用してください。</p> <ul style="list-style-type: none"> 複数のプライベートネットワーク上でバラクーダスパムファイアーウォールがクラスタ化されていて、同じプライベートネットワーク上のシステムは他のシステムのプライベート IP アドレスを使って通信し、別のネットワーク上のシステムは他のシステムのパブリック IP アドレスを使って通信する場合。 バラクーダスパムファイアーウォールの複数のクラスタが、それぞれ異なる宛先メールサーバにメールを転送する場合。例えば、[ドメイン] 設定ページの [送付先メールサーバ] フィールドが「localmail」で、クラスタ内の各バラクーダスパムファイアーウォールには、[ローカルホストマップ] フィールド内の「localmail」に異なる IP アドレスが割り当てられている場合がこれに相当します。

シングルサインオンの導入

[高度な設定] → [シングルサインオン] ページでは、バラクーダスパムファイアウォールが LDAP または Active Directory サーバを使ってユーザアカウントを許可するように設定できます。この機能は、バラクーダスパムファイアウォール 400 および 600 でのみ利用できます。

シングルサインオン機能を導入すると、ユーザは、バラクーダスパムファイアウォールで別々に管理されるパスワードではなく、自分のドメインパスワードを使って隔離インターフェースや管理者画面に自動的にログインできるようになります。

下表は、[高度な設定] → [シングルサインオン] ページ上のフィールドについての説明をまとめたものです。

フィールド	説明
ログインレルムセレクト	このオプションを有効にすると、ログイン画面に領域選択用のドロップダウンメニューが表示されます。ユーザはこのメニューで領域を選択し、ユーザ名だけでログインすることができます。シングルサインオンは、このメニューでサポートされます。
ローカルレルム名	ローカル認証用に表示される領域名（パスワードが生成され、バラクーダスパムファイアウォール上に格納されている場合）。
高度なシングルサインオンの設定	
レルム名	[ログインレルムセレクト] でユーザに対して表示される領域名。このフィールドは、管理者用の [ドメイン設定] にも表示されます。このフィールドへの入力必須です。
認証方法	作成する領域のタイプを制御します。以下のオプションが用意されています。 <ul style="list-style-type: none"> ・ LOCAL（バラクーダスパムファイアウォールがパスワードを管理する場合） ・ LDAP（パスワードが外部の LDAP データベースに保持される場合） ・ RADIUS（パスワードが RADIUS データベースに保持される場合）
認証ホスト	バラクーダスパムファイアウォールが認証のために接続する LDAP サーバまたは RADIUS サーバの名前。LOCAL 認証の場合は無視されません。
認証ポート	バラクーダスパムファイアウォールが認証のために LDAP サーバまたは RADIUS サーバに接続するときに使用するポート。LOCAL 認証の場合は無視されます。
ユーザ名テンプレート	LOCAL 認証を使用する場合、このフィールドは無視されます。 LDAP 認証を使用する場合、このフィールドには、バラクーダスパムファイアウォールがバインドするユーザ名（例： cn=__USERNAME__,dc=mydomain,dc=com）のテンプレートが保持されます。__USERNAME__ は、完全なメールアドレス、ユーザ名部分の両方と置換されます。 RADIUS 認証を使用する場合は、このフィールドには RADIUS で共有される秘密情報が保持されている必要があります。
デフォルトの認証	ユーザが領域を選択しないか、ユーザが選択した領域へのログインに失敗した場合には、ここで指定した領域がデフォルトとして使用されます。

スパム設定のローカライズ

[高度な設定] → [地域設定] ページでは、バラクーダスパムファイアウォールの中国語と日本語のメールを対象とするスパム検出能力を高めることができます。下表は、このページのオプションについての説明をまとめたものです。

オプション	説明
中国政府基準準拠	バラクーダスパムファイアウォールを中華人民共和国 (PRC) に設置する場合には、このオプションを有効にすると効果が高まる可能性があります。 バラクーダスパムファイアウォールを PRC 以外に設置する場合には、このオプションを [いいえ] に設定してください。
中国語スパムルール	会社に中国語のメールが大量に届く場合には、このオプションを有効にします。そうでない場合は、このオプションは無効にしてください。
日本語スパムルール	会社に日本語のメールが大量に届く場合には、このオプションを有効にします。そうでない場合は、このオプションは無効にしてください。

ドメインの管理と設定

[ドメイン] → [ドメイン管理者] ページでは、新規ドメインの追加と、ドメイン毎の変更を行うことができます。

新規ドメインの追加

お使いのバラクーダスパムファイアウォールで複数のメールサーバとドメインのフィルタリングを行う場合は、[ドメイン] → [ドメイン管理者] ページで各サーバに対応するドメインを入力する必要があります。

バラクーダスパムファイアウォール 400 または 600 をお使いの場合は、ドメイン毎のスパムスコアリング、隔離タイプ、スパム / ウイルス検査の設定も行うことができます。

ドメインを追加および設定するには、以下の手順を実行します。

1. [ドメイン] → [ドメイン管理者] ページを表示します。
2. [高度なドメイン設定] セクションで、関連するドメインを入力し、[ドメイン追加] をクリックします。

テーブルに追加したドメインが表示されます。

3. 追加したドメインの隣にある [ドメイン編集] をクリックします。

[ドメイン編集] ページが開きます。

4. 「ドメイン設定の編集」(P.54) の説明に従って、ドメインの設定を行います。

ドメイン設定の編集

特定のドメインの設定を編集するには、以下の手順を実行します。

1. [ドメイン] → [ドメイン管理者] ページで、編集するドメインの隣にある [ドメイン編集] をクリックします。

[ドメイン編集] ページが開きます。

2. 下表の説明を参考にして、ドメイン毎の設定を指定します。これらの設定は、バラクーダスパムファイアーウォール 400 および 600 でのみ利用できます。

注意：ドメイン毎の設定は、管理者画面の他の場所で設定した値よりも優先されます。

設定	説明
配送先サーバおよびポート MX レコードを使用する	選択したドメインに関連するメールサーバのホスト名と宛先ポート。 指定した宛先サーバ上で MX ルックアップを実行するかどうかを指定します。
正しいテストメールアドレス	選択したドメインのメールが正常にフィルタリングされるかどうかをテストする正しいメールアドレスを入力し、[SMTP 接続テスト] をクリックします。 続いて、[メッセージログ] をチェックし、ログに表示されるテストメッセージを読んで、メッセージがテストメールアドレスに送信されたことを確認します。テストメールの送信元アドレスは「 <code>smtptest@barracudanetworks.com</code> 」です。
レルム名	[ログインレルムセレクト] でユーザに対して表示される領域名。このフィールドは、管理者用の [ドメイン設定] にも表示されます。 領域とは、有効なユーザを識別するユーザ名とパスワード、および各ユーザに関連するロールのリストを保持するデータベースです。
タグ付けスコア、隔離スコア、拒否スコア	スパムスコアリングの詳細については、「グローバルスパムスコアリングの設定」(P.26) を参照してください。
ユーザ単位隔離	ドメインの隔離タイプを指定します。 [はい] を選択すると、隔離タイプは「ユーザ単位」に設定されます。 [いいえ] を選択すると、隔離タイプは「グローバル」に設定されます。隔離タイプの詳細については、「隔離タイプの指定」(P.28) を参照してください。
グローバル隔離メールアドレス	ドメインのグローバル隔離メールアドレスとして使用するアドレスを指定します。詳細については、「グローバル隔離設定の指定」(P.29) を参照してください。
スパムスキャン有効、ウイルススキャン有効	ドメインのスパム検査とウイルス検査を有効化または無効化できます。
スプーフィングプロテクション	部外者がユーザのドメインを送信元アドレスとしてメールを送信する「送信者なりすまし」を防止するかどうかを選択します。このオプションを [はい] に設定すると、バラクーダスパムファイアーウォールがメール受信を行うドメインを送信元とするすべてのメールが拒否されます。 このオプションは、ユーザのドメインから送信されるすべてのメールが、バラクーダスパムファイアーウォールを介さず直接メールサーバに配送される場合にのみ有効にしてください。

3. **[変更保存]** をクリックします。

バラクーダ MS エクスチェンジアクセラレータを使用した辞書攻撃の阻止

「辞書」すなわち NDR (Non-Delivery Report : 配送不能レポート) 攻撃とは、スパム送信者がメールサーバ上の受信者名に対してメッセージの連続配送を試みることです。

マイクロソフトエクスチェンジは「辞書」攻撃に対して、不正な宛先を拒否せずにすべてのメールを受け入れることによって、スパム送信者にアカウントが有効であることを知らせてしまうことがないようにしています。しかしながらこの処理によって、有効でない受信者に配送不能通知を送信することを試みるために、しばしばエクスチェンジサーバに非常に高い CPU 負荷をかける場合があります。

バラクーダ MS エクスチェンジアクセラレータは、MS エクスチェンジサーバにメールを配送し貴重なリソースを浪費する前に、エクスチェンジに組みこまれている LDAP サービスを使用し宛先を検証します。受信者を検証できない場合、バラクーダスパムファイアウォールはメールを配送しません。このプレミアムサービスはすべての MS エクスチェンジ構成にお勧めいたします。

注意：バラクーダ MS エクスチェンジアクセラレータを使用するには、エクスチェンジサーバ上で LDAP プロトコルが利用可能に設定されていなければなりません。LDAP は大半の MS エクスチェンジのインストールにおいてデフォルトで利用可能になっています。

バラクーダ MS エクスチェンジアクセラレータサービスを設定するには、以下の手順を実行します。

1. [ドメイン] → [ドメイン管理者] ページを表示します。
2. [アクション] カラムの [LDAP 編集] をクリックします。
3. リストに記載された各ドメインについて、必要な情報を入力します。

下表は、このページの各フィールドについての説明をまとめたものです。

フィールド	説明
LDAP サーバ	MS エクスチェンジサーバ用の LDAP サーバの名前。
エクスチェンジアクセラレータ有効	エクスチェンジアクセラレータ機能が指定されたドメインで有効化されているかどうか。
メールエイリアス統合	単一のユーザのメールエイリアスを統合するかどうかを指定します。[はい] を選択すると、ユーザのエイリアスを宛先とするすべてのメールに同じユーザ設定が適用され、同じ隔離受信ボックスに配送されます。 メールエイリアス統合機能を使用するには、このページで LDAP サーバを指定する必要があります。 この機能は、バラクーダスパムファイアウォール 200 では使用できません。 エイリアス統合機能は複数のエイリアスを互いにリンクさせます。例えば、あるアカウントに sanderson@acme.com、sandy_anderson@acme.com、sanderson@acme.com という 3 つのエイリアスが設定されているとすると、このすべてのエイリアスがプライマリサーバにリンクされます。
LDAP ポート	エクスチェンジサーバとの通信に使用される LDAP ポート。デフォルトでは、このポートは 389 です。

フィールド	説明
LDAP/ エクスチェンジユーザ名	LDAP/ エクスチェンジサーバ用のユーザ名。 完全修飾ユーザ名を確認するには、[Active Directory] を開いて [Active Directory Users and Computers] に進み、該当するユーザアカウントをダブルクリックします。[アカウント] タブでは、LDAP ユーザ名として @xxx.xxx を末尾に付加したユーザログイン名を使用します。
LDAP/ エクスチェンジパスワード	LDAP/ エクスチェンジサーバ用のパスワード。
LDAP フィルタ	ドメインに適用するカスタム LDAP フィルター（任意）。
LDAP 検索ベース	LDAP ツリー内の検索開始点を制御する値を入力します。デフォルト値では、「defaultNamingContext」の最上層の属性が検索され、それが検索ベースとして使用されます。
正しいメールアドレス（テスト用）	LDAP ルックアップが正確に作動していることを検証するために使用される正しいメールアドレスを入力します。このアドレスを入力した後、[LDAP をテスト] をクリックします。

4. **[変更保存]** をクリックします。

ユーザアカウントの管理

[ユーザ] タブ（このタブは、バラクーダスパムファイアウォール 300、400、および 600 モデルにあります）では、以下を実行することができます。

- ユーザアカウントの表示
- ユーザアカウントへの機能の割り当て
- ユーザアカウントの追加と削除
- ユーザ設定のバックアップとリストア

ユーザアカウントの表示

[ユーザ] → [アカウント一覧] ページでは、各ユーザのアカウント設定を表示し、隔離インターフェースにログインしてユーザ個人の設定を変更することができます。また、システム上の任意のユーザ単位隔離アカウントを削除することも可能です。

下表は、このページの各カラムについての説明をまとめたものです。

カラム	説明
アカウントアドレス	アカウントのメールアドレス。
通知間隔	システムがユーザに隔離サマリーメッセージを送信する間隔。
隔離使用？	ユーザが有効になっている隔離アカウントを持っているかどうか。 【いいえ】 に設定されている場合、すべての隔離メッセージは（隔離領域に置かれるのではなく）件名を変更してユーザに配送されます。
スパムスキャン？	ユーザのスパムスコアリングが有効になっているかどうか。 【いいえ】 に設定されている場合、このユーザのメールに対してはスパムスキャンが実行されません。

カラム	説明
管理者アクション	問題のトラブルシューティングやユーザ設定の変更を行うためにユーザの隔離アカウントを表示するには、[アカウント編集] をクリックします。 システムからすべてのユーザ設定と隔離されたメールを含む隔離アカウントを削除するには、[削除] リンクをクリックします。
無効なアカウントを全て削除	受信者検証機能で各ユーザアカウントを検査し、現在無効となっているアカウントを削除するには、このボタンをクリックします。

このページに表示されるアカウントを限定するには、下表に示すフィルターを必要に応じて使用してください。

フィルタ	説明
なし	システム上のすべてのアカウントを、最新のものから順に表示します。
"アカウント" (メールアドレス)	[パターン] テキストボックスに入力されたメールアドレスのアカウントのみを表示します。
"アカウント" (パターン*)	[パターン] テキストボックスに入力された完全または部分的なユーザ名と一致するアカウントのみを表示します。この照合は、バラクーダスパムファイアーウォール上のすべてのドメインを対象に実行されます。 <i>注意：ワイルドカードはパターンの右側になります。そのため、「bob」で検索すると、bob@domain.com や bobby@domain.com は一致しますが、billybob@domain.com は一致しません。</i>
"アカウント" (*パターン)	[パターン] テキストボックスに入力された完全または部分的なユーザ名と一致するアカウントのみを表示します。この照合は、バラクーダスパムファイアーウォール上のすべてのドメインを対象に実行されます。 <i>注意：ワイルドカードはパターンの左側になります。そのため、「domain.com」で検索すると、user@domain.com や user@corp.domain.com は一致しますが、user@domain1.com は一致しません。</i>
"隔離有効"	隔離が有効化されているすべてのアカウントを表示します。
"隔離無効"	隔離が無効化されているすべてのアカウントを表示します。
"スパムスキャン有効"	スパムスキャンが有効化されているすべてのアカウントを表示します。
"スパムスキャン無効"	スパムスキャンが無効なすべてのアカウントを表示します。

ユーザアカウントへの機能の割り当て

[ユーザ] → [ユーザ機能] ページでは、ユーザが隔離インターフェースから管理できる機能を指定できます。

下表は、このページ上の設定についての説明をまとめたものです。

ユーザ機能	説明
隔離の有効 / 無効設定機能	<p>ユーザが隔離受信ボックスの有効 / 無効を設定できるかどうかを指定します。この値を 【いいえ】 に設定した場合は、すべてのメッセージが以下のいずれかに基づいて隔離されます。</p> <ul style="list-style-type: none"> ・ [基本設定] → [隔離] ページ上で設定された隔離タイプ ・ [高度な設定] → [高度なドメイン設定] ページで設定されたドメイン毎隔離タイプ。詳細については、「ドメインの管理と設定」(P.53) を参照してください。 <p><i>注意: この値を 【いいえ】 に設定した場合、ユーザが行った隔離設定は反映されません。</i></p>
スパムスキャンの有効 / 無効設定機能	<p>ユーザが受信メールのスパムスキャンを有効 / 無効に設定できるかどうかを指定します。この値を 【いいえ】 に設定した場合、すべてのユーザのメールは以下のいずれかに基づいてスキャンされます。</p> <ul style="list-style-type: none"> ・ [基本設定] → [スパムスコアリング] ページで行われた設定 ・ [高度な設定] → [高度なドメイン設定] ページで行われたドメイン毎設定。詳細については、「ドメインの管理と設定」(P.53) を参照してください。 <p><i>注意: この値を 【はい】 に設定した場合、ユーザがスパムスキャンを無効にしても、[スパムスキャンの有効 / 無効設定機能] を 【いいえ】 に変更するとユーザのスパムスキャンが再び有効になります。</i></p>
通知変更機能	<p>ユーザが隔離サマリー通知を受け取る頻度をユーザ自身が変更できるかどうかを指定します。この値を 【いいえ】 に設定した場合、すべてのユーザは [基本設定] → [隔離] ページの [隔離通知] 設定で指定された頻度に基づいて通知を受け取ります。</p> <p><i>注意: この値を 【はい】 に設定していて、ユーザが通知の間隔を変更した場合は、[通知変更機能] を 【いいえ】 に変更したときにユーザの変更が保存されます。</i></p>
ホワイトリスト / ブラックリスト機能	<p>ユーザ個人のホワイトリストとブラックリストにメールアドレスやドメインをユーザが追加できるかどうかを指定します。</p> <p><i>注意: この値が 【はい】 に設定していて、ユーザがホワイトリストとブラックリストにエントリを追加した場合は、[ホワイトリスト / ブラックリスト機能] を 【いいえ】 に変更したときにユーザの追加は無視されません。</i></p>

ユーザ機能	説明
スコアリング変更機能	<p>メールにタグ付け、隔離、または拒否するレベルをユーザが変更できるかどうかを指定します。この値を [いいえ] に設定した場合、すべてのメッセージは以下のいずれかに基づいてスコアされます。</p> <ul style="list-style-type: none"> ・ [基本設定] → [スパムスコアリング] ページで行われた設定 ・ [高度な設定] → [高度なドメイン設定] ページで行われたドメイン毎の設定。詳細については、「ドメインの管理と設定」(P.53) を参照してください。 <p><i>注意: この値を [はい] に設定していて、ユーザがスパムスコアリングを変更した場合は、[スコアリング変更機能] を [いいえ] に変更したときにユーザの変更は保存されません。</i></p>
ユーザ機能を無効にする	<p>このセクションでは、特定のユーザアカウントに [デフォルトユーザ機能] セクションで指定されていない機能を割り当てることができます。</p> <p>[ユーザアカウント] ボックスに設定変更するアカウントのメールアドレスを入力してから、これらのアカウントに割り当てる機能を指定します。[変更保存] をクリックします。</p>

新規ユーザアカウントの作成

[ユーザ] → [ユーザ追加 / 更新] ページでは、設定を個別に指定して新規ユーザアカウントを作成できます。新規ユーザアカウントをシステムに追加するには、以下の手順を実行します。

1. [ユーザアカウント] ボックスで、新規ユーザアカウントのメールアドレス（1行に1つずつ）を入力します。
2. 新規ユーザアカウントにユーザ隔離機能を付加するかどうかを指定します。

ユーザ隔離機能の詳細については、「隔離タイプの指定」(P.28) を参照してください。

注意: ユーザ隔離機能を有効にした場合は、エイリアスとパブリックフォルダを無効にして、これらのアイテムに対してユーザ毎アカウントが作成されないようにしてください。

3. 新規ユーザにログイン情報をメールで通知するオプションを選択します。ログイン情報を記載したグリーティングメールの例を表示する方法については、「グリーティングメール」(P.65) を参照してください。
4. [変更保存] をクリックします。

ユーザアカウントにその他の機能を割り当てる方法については、P.58 を参照してください。

ユーザ設定のバックアップとリストア

[ユーザ] → [バックアップ / リストア] ページでは、ユーザ設定をテキストファイルに保存しておき、必要に応じてそれをリストアすることができます。ユーザ設定には、各ユーザが作成した許可および拒否メールのリスト、ユーザの隔離通知間隔、ユーザが設定したパスワードなどの設定が含まれます。

ユーザ設定のバックアップとリストアの詳細については、「システム設定のバックアップとリストア」(P.41) を参照してください。

SSLの有効化

[高度な設定] → [SSL] ページでは、バラクーダスパムファイアウォール上の SSL を有効にすることができます。このページの変更が完了したら [変更保存] をクリックしてください。

SSL を有効にする最も一般的な理由としては、ユーザパスワードの保護が挙げられます。シングルサインオン機能 (P.52) を使用する場合は、パスワードを暗号化されていない元の形でバラクーダスパムファイアウォールに渡すことが要求される可能性があるため、SSL も有効にしてください。シングルサインオンを使用しない場合は、SSL でパスワードを保護する必要はありません。

SSL では、パスワードだけでなく、管理者画面との間で送受信されるデータの残りの部分も暗号化されます。

下表は、[高度な設定] → [SSL] ページの各フィールドについての説明をまとめたものです。

フィールド	説明
ウェブインターフェース HTTPS/SSL 設定	
HTTPS/SSL アクセスだけに限定する	SSL を有効にして、SSL を経由した管理者画面へのアクセスだけを許可する場合は、[はい] を選択します。標準 HTTP をアクセスする場合は、[いいえ] を選択します。
電子メールに HTTPS リンクを使用する	システムメールに含まれるリンクで (http:// ではなく) https:// を使用するかどうかを指定します。これは、システムが送信する日次システムレポート、隔離メール、システムアラートに適用されます。この設定は、ユーザが送信するメールには適用されません。 この設定は、HTTPS/SSL アクセスを有効にすると自動的に [はい] に設定されます。
ウェブインターフェース HTTPS/SSL ポート	バラクーダスパムファイアウォールが使用する SSL ポート。デフォルトの SSL ポートは、443 です。
SSL 証明書設定	
証明書タイプ	SSL 用証明書として以下のいずれかを選択してください。 <ul style="list-style-type: none"> デフォルト (バラクーダネットワークス)。ブラウザのアラートを生成する SSL 接続で使用します。デフォルト証明書は、バラクーダネットワークスが署名し、デフォルトタイプの証明書として無償で提供されます。 プライベート (自己署名) 証明書。トラステッド証明局 (CA) から有料の証明書を購入しなくても、強力な暗号を実現できます。ただし、ウェブブラウザは証明書の信憑性を検証できないため、管理者画面にアクセスするたびに警告が表示されます。この警告が表示されないようにする場合は、プライベートルート証明書をダウンロードして、ブラウザにインポートしてください。 信頼できる証明書。これは、ウェブブラウザが通常認識するトラステッド認証局 (CA) によって発行される証明書なので、特別な設定は必要ありません。

フィールド	説明
証明書生成	
組織情報	証明書と証明書署名要求に含まれる情報。以下の情報を入力してください。 コモンネーム—管理者画面にアクセスするときに使用する公式フルドメイン名。例：barracudayourdomain.com 国—組織が所在する2文字の国コード。 都道府県—組織が所在する州または省の完全な名前。 市区町村—組織が所在する都市。 組織名—会社または組織の正式名称。 部署名—組織内の部署を指定するための任意指定のフィールド。
証明書署名要求（CSR）のダウンロード	トラステッド認証局から署名入り証明書を購入するために必要な証明書署名要求を入手する場合は、[ダウンロード] をクリックします。証明書は1024ビットのキー長で生成されます。
秘密鍵のダウンロード	CSR で使用する秘密鍵のコピーを入手する場合は、[ダウンロード] をクリックします。証明書を購入した認証局から、この鍵を要求されることがあります。この鍵は、CSR をダウンロードした後でなければ入手できません。
プライベートルート証明書のダウンロード	プライベートルート証明書を入手して、ウェブブラウザにインポートする場合は、[ダウンロード] をクリックします。 証明書をインポートすると、ウェブブラウザから、バラクーダシステムのSSL 証明書の信憑性を検証できるので、管理者画面にアクセスしても警告は表示されなくなります。
信頼できる証明書	
署名付き証明書のアップロード	CSR を使用して証明書を購入した後に、証明書のある場所に移動し、[アップロード] をクリックします。証明書をアップロードすると、バラクーダスパムファイアーウォールは自動的にそれを使用します。 署名入り証明書をアップロードした後に、証明書タイプとして [信頼できる証明書] が選択されていることを確認してください（上記参照）。
秘密鍵のアップロード	CSR を使用して秘密鍵を購入した後に、鍵のある場所に移動し、[アップロード] をクリックします。

配送不能レポート（NDR）のカスタマイズ

[高度な設定] → [NDRのカスタマイズ] ページでは、NDR の情報を変更できるほか、メールで使用するデフォルト言語を選択することもできます。

バラクーダスパムファイアーウォールでは、メールが拒否されると、NDR がメールの受信者と送信者に送付されます。NDR には、メールが拒否された理由が記述されたテキストが含まれます。ユーザが拒否されたメールについて問い合わせることができるように、NDR にバラクーダシステム管理者のコンタクト情報を含めることがお勧めします。

注意：[基本設定] → [スパムスコアリング] ページと [基本設定] → [ウイルスチェック] ページが有効でない場合には、配送不能レポートは送付されません。

下表は、[高度な設定] → [NDR のカスタマイズ] ページ上の設定についての説明をまとめたものです。

フィールド	説明
NDR の言語を選択	
デフォルト言語	<p>配送不能レポートで使用する言語を選択します。デフォルト NDR メッセージは、自動的に指定した言語に翻訳されます。</p> <p>NDR に含まれる情報をカスタマイズする場合は、[カスタム] を選択し、[カスタマイズされた NDR] セクションにテキストを入力します。</p> <p><i>注意：NDR をカスタマイズした後、事前に定義された言語に切り替えると、カスタマイズした内容はすべて失われ、指定した言語のデフォルトメッセージに戻ります。</i></p>
カスタマイズされた NDR	
禁止添付ファイル (受信者)	禁止されたファイルタイプが添付されたメールがユーザに送信された場合、受信メールは拒否され、この通知がメールの受信者に送付されます。
禁止添付ファイル (送信者)	禁止されたファイルタイプが添付されたメールが送信された場合、送信メールは拒否され、この通知がメールの送信者に送付されます。
スパム (送信者)	スパムと判定されたためにメールが拒否された場合は、この通知が送信者に送付されます。
ウイルス (受信者)	メールにウイルスが含まれていると判定された場合は、この通知が拒否されたメールの受信者に送付されます。
ウイルス (送信者)	メールにウイルスが含まれていると判定された場合は、この通知がメールの送信者に送付されます。

下表は、NDR で使用できるマクロについての説明をまとめたものです。

マクロ	説明
%f	バラクーダスパムファイアウォール管理者のメールアドレス (通常は、NDR の「送信元:」ヘッダーで使用されます)。
%C	NDR の「コピー先 (Cc:)」ヘッダーで使用する受信者のリスト。
%d	RFC 2822 形式の日付と時刻 (現在時刻)。
%m	「メール ID」ヘッダーフィールドの本文。
%j	「件名」ヘッダーフィールドの本文。
%s	元のエンベロープ送信者。rfc2821 形式の角括弧で囲まれます。
%S	送信者通知の送付先となるアドレス。これは通常、送信者アドレス (%s) だけを含む 1 エントリのリストですが、ウイルスによって偽造されたアドレスを元に戻すために組み替え / 再構成することも可能です。
%v	(最後の) ウィルス検査プログラムの出力。
%F	禁止ファイル名のリスト。

トラブルシューティング

[高度な設定] → [トラブルシューティング] ページでは、バラクーダスパムファイアウォールのパフォーマンスに影響するネットワーク接続の問題のトラブルシューティングに役立つ様々なツールが用意されています。

下表は、[高度な設定] → [トラブルシューティング] ページの各フィールドについての説明をまとめたものです。

トラブルシューティングツール	説明
診断のサポート	
バラクーダセントラルへの接続の確立	問題のトラブルシューティングと診断で助けが必要になったら、このボタンをクリックしてバラクーダセントラルへの接続を確立し、バラクーダネットワークスのサポートエンジニアに表示されたシリアル番号を提示してください。この作業の完了後は、[停止] ボタンをクリックして、バラクーダシステムへのすべての接続を停止します。
ネットワーク接続性	
Ping 対象デバイス	バラクーダスパムファイアウォールから指定したシステムに ping 要求を送信します。ping を実行するシステムの IP アドレスまたはホスト名（および、使用する ping オプション）を入力し、[Ping 開始] をクリックしてテストを開始してください。
Telnet 対象デバイス	バラクーダスパムファイアウォールから指定したシステムへの telnet セッションの確立を試みます。このセッションは非対話型です。 このテストを使って、接続性と、リモートサーバからの初期応答を確認することができます。telnet セッションを実行する IP アドレスまたはホスト名（および、使用するオプション）を入力し、[Telnet 開始] をクリックしてテストを開始してください。
Dig/NS-lookup 対象デバイス	バラクーダスパムファイアウォールで「dig」コマンドを実行します。「dig」は nslookup コマンドを高度化したもので、任意のタイプの DNS レコードのルックアップを実行できます。 dig を実行する IP アドレスまたはホスト名（および、使用するオプション）を入力し、[Dig 開始] をクリックしてテストを開始します。例えば、mx レコードをルックアップする場合は、「mx mydomain.com」を入力します。
TCP Dump	ネットワークのトラフィックをモニターするために、バラクーダスパムファイアウォールで tcpdump を実行します。 接続のモニターで使用する情報（および、tcpdump 出力を調整するためのオプション、例: -x -X port 53）を入力し、[TCP Dump の開始] をクリックしてテストを開始してください。
Traceroute 対象デバイス	接続経路を特定するために、バラクーダスパムファイアウォールから指定したシステムへのトレースルートを実行します。宛先サーバの IP アドレスまたはホスト名を入力し、[Traceroute の開始] をクリックしてテストを開始してください。

第 4 章 バラクーダスパムファイアウォールを使用したメールのフィルタリング

この章では、エンドユーザがバラクーダスパムファイアウォールで行う、隔離メールの確認、メールのスパム / 非スパム分類、ユーザ設定の変更の方法について説明します。この章では、以下のトピックについて説明しています。

- バラクーダスパムファイアウォールからのメールの受信（次節）
- 「隔離インターフェースの使用」(P.66)
- 「ユーザ設定の変更」(P.68)

バラクーダスパムファイアウォールからのメールの受信

バラクーダスパムファイアウォールは、エンドユーザに次の 2 種類のメールを送信します。

- グリーティングメール
- SPAM 隔離サマリーレポート

グリーティングメール

バラクーダスパムファイアウォールがユーザ宛のメールを初めて隔離すると、システムから「ユーザ隔離アカウント情報」という件名のグリーティングメールが送られてきます。グリーティングメールには以下の情報が記載されています。

Welcome to the Barracuda Spam Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences.

Your account has been set to the following username and password:

Username: <user's email address>

Password: <user's default password>

Access your Spam Quarantine directly using the following link:

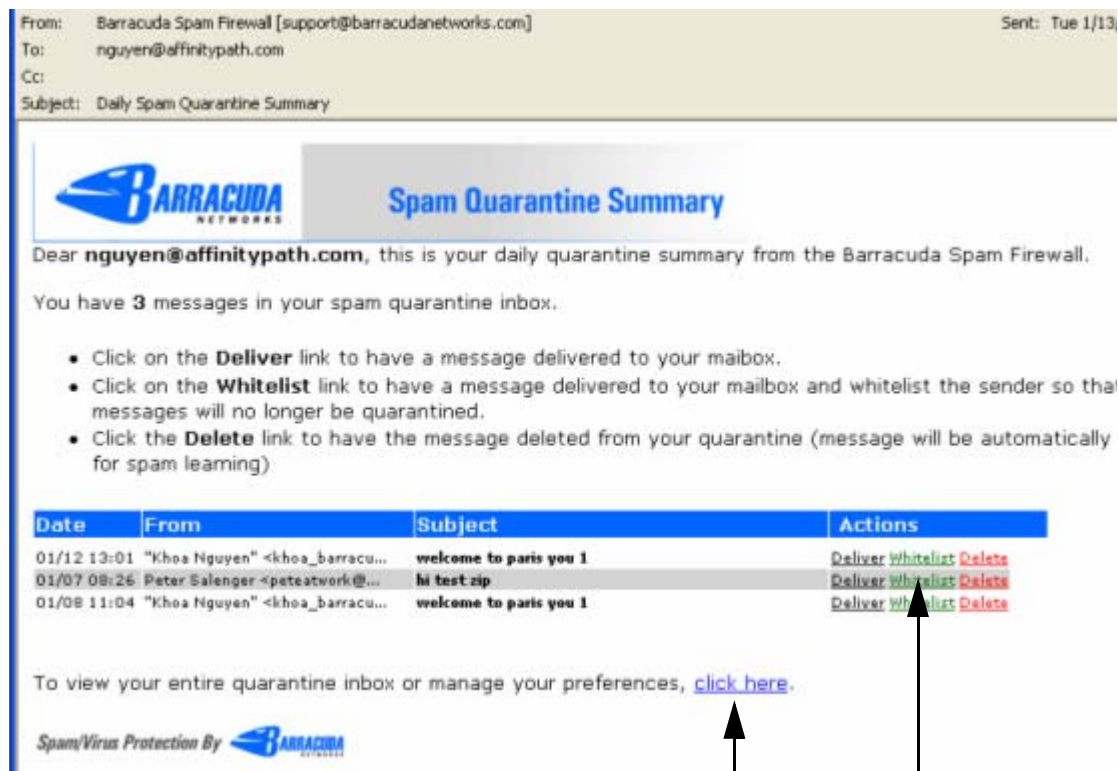
<http://<barracuda system address or name>:80>

隔離インターフェースにアクセスするためのログイン情報（ユーザ名とパスワード）およびリンクは、バラクーダスパムファイアウォールから自動的に提供されます。今後システムから送られてくるメールにログイン情報は記載されないため、このメールは保存しておいてください。

隔離サマリーレポート

受信しなかった隔離メールは、バラクーダスパムファイアウォールからユーザに毎日送られてくる日次隔離サマリーレポートで閲覧することができます。この隔離サマリーレポートでは、ホワイトリストへのメールの追加、メールの削除、メールの受信ボックスへの配送の指定を行うこともできます。

下図は隔離サマリーレポートの例です。



隔離インターフェースにアクセスして、ユーザ設定の指定とメールの分類を行う場合は、ここをクリックします。

隔離メールの配送、ホワイトリスト化、削除を行う場合は、ここを選択します。

隔離インターフェースの使用

隔離サマリーレポートの最後に、隔離インターフェースへのリンクが用意されています。このインターフェースでは、追加のユーザ設定を指定し、メールをスパムまたは非スパムとして分類することができます。

隔離インターフェースへのログイン

隔離インターフェースにログインするには、以下の手順を実行します。

1. 隔離サマリーレポートの最下部にあるリンクをクリックします（上図参照）。

ログインページが表示されます。

2. ユーザ名とパスワードを入力し、[ログイン] をクリックします。

ログイン情報は、バラクーダスパムファイアウォールから送られてきたグリーティングメールに記載されています。

隔離受信ボックスの管理

隔離インターフェースにログインした後、[隔離受信ボックス] タブを選択して、隔離メールのリストを表示します。隔離インターフェースを使用し始めてからしばらくは、このリストを毎日表示して、できるだけ多くのメールを分類してください。

バラーダスパムファイアーウォールには学習エンジンが備えられています。この学習エンジンは、ユーザが行ったスパム / 非スパムの分類に基づいて、今後のメールの処理方法を学習します。学習エンジンは、分類方法を教示したメールの数と、ホワイトリストとブラックリストに基づいて設定したルールが増えるほど効果が高まります。

メールをクリックすると、生テキスト形式でメッセージの内容が表示されます。この形式では、画像を含むメールを認識できない可能性があります。メールクライアントにメール画像を含むメールを正常に表示する場合は、メールの配送を選択してください。

下表は、このページで実行できるアクションの説明をまとめたものです。

アクション	説明
配送	<p>選択したメールを標準のメール受信ボックスに配送します。</p> <p><i>注意：メールの分類またはホワイトリストへの追加を行う前に、必ずメールを受信ボックスに配送してください。バラーダスパムファイアーウォールが配送したメールは、隔離リストから削除されます。</i></p>
ホワイトリスト	<p>選択したメールをホワイトリストに追加します。今後この送信者から受信するメールはすべて、ウィルスまたは禁止ファイルタイプが含まれない限り隔離されません。</p> <p>送信元メールアドレスは、メールに表示されたとおりの形でホワイトリストに追加されます。</p> <p>広告メールは類似した複数のサーバから送られてくることがあることに注意してください。例えば、最初に「mail3.abcbank.com」から届くと、その後は「mail2.abcbank.com」から届く可能性があります。ホワイトリストの指定を詳細にして効果を高める方法については、ホワイトリストとブラックリストの管理に関する項に記載されるヒントを参照してください。</p>
削除	<p>選択したメールを隔離リストから削除します。メールを削除することによって、確認済みの隔離メールが追跡しやすくなります。</p> <p>削除したメールを元に戻すことはできません。</p>
非スパムと類別	<p>選択したメールを非スパムとして分類します。</p> <p><i>注意：大量に一括送信される広告メールが有益か迷惑かは、ユーザによって異なります。これらのメールを分類すると、ユーザの間に分類の対立が発生する可能性があるため、効果はあまり期待できません。一括送信された広告メールを分類する代わりに、ホワイトリスト（受信したいメールの場合）またはブラックリスト（受信したくないメールの場合）に追加する方が効果的です。</i></p>
スパムと類別	<p>選択したメールをスパムとして分類します。</p>

ユーザ設定の変更

隔離インターフェースにログインした後、[参照] タブを選択すると、アカウントパスワードの変更、隔離設定とスパム設定の変更、ホワイトリストとブラックリストの管理を行うことができます。

アカウントパスワードの変更

アカウントパスワードを変更するには、以下の手順を実行します。

- 隔離インターフェースのログインページで、[新パスワード生成] をクリックします。
- 隔離インターフェースにログインした後、[参照] → [パスワード] を選択します。

表示されるフィールドに、現在のパスワードを入力し、続いて新しいパスワードを2回入力します。[変更保存] をクリックします。

注意：パスワードを変更すると、受信済みの隔離サマリーレポートとのリンクが切れますので、これらのレポートからメールの削除、配送、ホワイトリスト化を行うことはできません。新しい隔離サマリーレポートには更新されたリンクが含まれますので、パスワードを変更する前と同じように利用できます。

隔離設定

下表は、[参照] → [隔離設定] ページから変更できる隔離設定についての説明をまとめたものです。

隔離設定	説明
隔離有効	<p>メールを隔離するかどうかを指定します。</p> <p>[はい] を選択すると、隔離メールは通常のメール受信ボックスに配送されません。これらのメールは、隔離インターフェースまたは隔離サマリーレポートから閲覧することができます。</p> <p>[いいえ] を選択すると、隔離の対象となるメールの件名行に「[SPAM]」が付加され、通常のメール受信ボックスに配送されます。</p>
通知間隔	<p>ユーザに隔離サマリーレポートを送信する間隔。デフォルトは、1日1回です。</p> <p>[通知しない] を選択した場合、隔離インターフェースから隔離メールを閲覧することはできますが、隔離サマリーレポートは送信されません。</p>
通知アドレス	<p>隔離サマリーレポートの送信に利用されるメールアドレス。ユーザアカウントに関連するメールアドレスを利用する場合は、このフィールドを空白のままにしてください。</p>

メールのスパムスコアリングの有効化と無効化

スパムの内容のスキャンをしらない場合は、[参照] → [スパム設定] ページを無効に設定します。このページでは、メールのタグ付け、隔離、拒否を行う際の基準となるデフォルトスパムスコアリングを変更することもできます。

バラクーダスパムファイアウォールは、ユーザ宛のメールを受信すると、それがスパムである確率をスコアリングします。このスコアの範囲は、0（確実に非スパム）～10以上（確実にスパム）です。バラクーダスパムファイアウォールは、このスコアに基づいて、タグ付け、隔離、拒否、許可のいずれかを行います。

設定を10にすると、そのオプションは無効になります。

設定	説明
スパムスキャンの有効化 / 無効化	
スパムフィルタリング有効	メールをスキャンしてスパムかどうかを判定する場合は、[はい] を選択します。メールをスキャンしてスパムかどうかを判定しない場合は、[いいえ] を選択します。
スパムスコアリング	
システムデフォルトを使用する	デフォルトのスコアリングレベルを使用する場合は、[はい] を選択します。自分でスコアリングレベルを設定する場合は、[いいえ] を選択し、次の [スパムスコアリングレベル] のセクションで必要な変更を行ってください。
スパムスコアリングレベル	
タグ付けスコア	スコアがこのしきい値を上回り、かつ隔離しきい値を下回るメールは、件名に「[BULK]」という単語が追加されてユーザに配送されます。 スコアがこの設定値を下回るメールはすべて、自動的に許可されます。デフォルト値は3.5です。
隔離スコア	スコアがこのしきい値を上回り、かつ拒否しきい値を下回るメールは、ユーザの隔離メールボックスに転送されます。 デフォルト設定値は10です（隔離機能は無効）。 隔離機能を有効にするには、この設定で拒否しきい値よりも低い値を指定します。
拒否スコア	スコアがこのしきい値を上回るメールは、ユーザの受信ボックスに配送されません。システムの設定によっては、ユーザと送信者に「拒否されたメールは配送されない」という意味の通知が送付されることがあります。 デフォルト値は7です。

ホワイトリストおよびブラックリストへのメールアドレスとドメインの追加

[参照] → [ホワイトリスト / ブラックリスト] ページでは、メールを受信または拒否するメールアドレスとドメインを指定することができます。

リストタイプ	説明
ホワイトリスト	このリストに含まれるメールアドレスまたはドメインからのメールは、常に受信されます。ホワイトリストにある送信者からのメールは、ウィルスまたは禁止された添付ファイル拡張子が含まれる場合にのみフィルタリングされます。
ブラックリスト	このリストに含まれる送信者からのメールは、常に拒否され、直ちに破棄されます。これらのメールはタグ付けまたは隔離の対象とはならず、復元することはできません。メールが破棄されたことは、送信者にも受信者にも通知されません。

送信者をホワイトリスト化またはブラックリスト化するには、以下の手順を実行します。

1. [参照] → [ホワイトリスト / ブラックリスト] ページを表示します。

このページには、現在ホワイトリスト化またはブラックリスト化されているアドレスが表示されています。

2. ホワイトリストまたはブラックリストのエントリを削除する場合は、アドレスの隣にあるゴミ箱のアイコンをクリックします。
3. ホワイトリストまたはブラックリストにエントリを追加する場合は、該当するフィールドにメールアドレスを入力し、それに対応する [追加] ボタンをクリックします。

アドレス指定のヒント

ホワイトリストまたはブラックリストにアドレスを追加する際には、以下のヒントを参考にしてください。

- *johndoe@yahoo.com* のような完全なメールアドレスを入力した場合は、そのユーザだけが指定されます。*yahoo.com* のようにドメインのみを入力した場合は、そのドメインのすべてのユーザが指定されます。
- *nasa.gov* のようなドメインを入力した場合は、*hq.nasa.gov* や *ksc.nasa.gov* などのサブドメインも含まれます。
- 大量に送信されるメールは、企業のウェブサイト名とは名前が類似しないドメインから送信されることは少なくありません。例えば、*historybookclub.com* からメールが届いたとしても、実際に送信したドメインは *hbcbfyi.com* かもしれません。入力する前に、ホワイトリスト化またはブラックリスト化しようとしている実際のメールの送信元アドレスを確認してください。

付録 A 正規表現について

バラクーダスパムファイアウォールの多数の機能では、正規表現を使用することができません。正規表現を使うとテキストを柔軟に記述できるため、考えられる様々な表現についてマッチングを試みることができます。

正規表現を使用する際には、以下のことに注意してください。

- テキスト内で特殊文字（例：|, *, '!）を使用する場合は、特別な注意が必要です。詳細については、「正規表現での特殊文字の使用」（P.72）を参照してください。
- マッチングでは、大文字と小文字が区別されます。

下表は、バラクーダスパムファイアウォールでサポートされる最も一般的な正規表現についての説明をまとめたものです。

正規表現	マッチする文字列
演算子	
*	直前の文字の 0 回以上の出現
+	直前の文字の 1 回以上の出現
?	直前の文字の 0 または 1 回の出現
	「 」の両側にある文字のうちいずれか
()	「()」で括られた文字列
文字クラス	
.	改行文字以外の文字列
[ac]	文字「a」または「c」
[^ac]	「a」および「c」以外の文字
[a-z]	「a」～「z」の文字
[a-zA-Z]	「a」～「z」および「A」～「Z」の文字、およびドット
[a-zA-Z]	「a」～「z」の文字、およびダッシュ
\d	数字、[0-9] のショートカット
\D	非数字文字、[^0-9] のショートカット
\a	数字、[0-9] のショートカット
\w	単語の一部:[A-Za-z0-9_] のショートカット
\W	非単語文字:[^\w] のショートカット
\s	スペース文字:[\n\r\t] のショートカット
\S	非スペース文字:[^\s] のショートカット
その他	
^	行頭
\$	行末
\b	単語の境界
\t	タブ文字

正規表現での特殊文字の使用

正規表現では以下の文字は特殊な意味で使われるため、文字通り解釈させたい場合はバックスラッシュ (\) を前に付加してください。

. \$
[(
])
\ |
* ^
? @

例

下表は、正規表現の使用方法の理解に役立つ例をまとめたものです。

例	マッチする文字列
viagra	viagra、VIAGRA、vIaGRa
d+	1 つ以上の数字: 0、42、007
(bad good)	「bad」または「good」
^free	行頭の「free」
v[i]agra	viagra、vIaagra
v(ia l)a)gra	viagra、vIaagra
v\ agra	v agra
v(i l \)?agra	vagra、viagra、vIaagra、v agra
FREE	*FREE*
FREE V.*GRA	*FREE* VIAGRA、*FREE* VEHICLEGRA など

索引

数字

1 時間毎のメール統計 21

B

barracuda.conf ファイル 41

bayes.tgz ファイル 41

C

Caller ID 47

D

Dig/NS-lookup ツール 63

DNS MX レコード 15

DNSBL 34

DNS サーバの指定 31

H

HTTPS アクセス 60

I

Incoming SMTP タイムアウト設定 47

[IP アドレスでの拒否 / 許可] ページ 36

IP アドレスの設定 12

[IP 設定] ページ 31

L

LDAP 55

LED (フロントパネル) 20

M

MX レコード 54

N

NDR 61

NDR 攻撃の阻止 55

NDR のカスタマイズ 61

NTP 14

O

ORDB ブラックリスト 35

Outlook クライアントプラグイン 24

P

Ping ツール 63

pu_config.tgz ファイル 41

R

RAID 8

RBL 34

RFC 821 コンプライアンス 46

S

Send Bounce field 27

Sender Policy Framework (SPF) 47

SMTP HELO 46

SMTP ウェルカムバナー設定 47

Spam Bounce (NDR) Configuration 27

Spam Cop ブラックリスト 35

Spamhaus ブラックリスト 35

SPF 47

SSL の有効化 60

[Syslog] ページ 49

T

TCP Dump ツール 63

TCP/IP 設定 31

TCP ポート 14

Telnet ツール 63

Traceroute ツール 63

U

UDP ポート 14

あ

[アカウント一覧] ページ 56

アカウントの作成 59

アカウントの有効化 48

アカウントパスワードの変更 68

い

インジケータランプ 20

インテンション解析 46

う

ウイルスチェック

無効化 27

有効化 27

ウイルス通知

無効化 27

有効化 27

ウイルス定義の更新 43

ウェブインターフェースポートの設定 32

え		
エイリアスの統合	55	
エネルギー充填サービス	6, 43	
か		
[外観] ページ	44	
隔離		
サマリーレポート	28	
タイプ	28	
通知間隔	30	
メール設定	26	
隔離インターフェースへのログイン	66	
隔離機能		
設定	28	
メール設定	69	
隔離サマリーレポート	65	
隔離受信ボックスの管理	67	
隔離スコア	26	
カスタマイズ		
管理者画面	44	
配送不能レポート (NDR)	61	
管理		
隔離受信ボックス	67	
バラクーダスパムファイアウォール	19	
[管理者 IP/ 範囲] の設定	32	
管理者画面	32	
ログイン	12	
管理者画面のカスタマイズ	44	
き		
許可メール受信者ドメイン	31	
[拒否 / 許可] タブ	34	
拒否スコア	26	
拒否メールの設定	69	
く		
クライアントプラグイン	24	
クラスタ化	50	
グリーティングメール	65	
グローバル隔離		
設定	29	
タイプ	28	
け		
件名		
隔離	39	
拒否	39	
タグ付け	39	
ホワイトリスト化	39	
[件名によるフィルタリング] ページ	39	
こ		
更新		
ファームウェア	49	
構成		
バラクーダスパムファイアウォール	12	
個別アカウントの有効化	48	
さ		
削除		
バラクーダヘッダー	48	
し		
システム環境条件	21	
システム警告の送付	34	
システム設定		
バックアップ	41	
リストア	42	
システム統計	21	
システムのシャットダウン	33	
システムのリセット	33	
[受信者メールアドレス拒否 / 許可] ページ	38	
証明書生成	61	
新規ユーザアカウントの作成	59	
シングルサインオンの設定	52	
す		
[ステータス] ページ	21	
ステータスレポートの送付	34	
スパム		
スコアリング	7, 26	
分類	25	
メッセージを分類	23	
スパムスコアリング		
有効化と無効化	69	
スパム設定のローカライズ	53	
スパム定義の更新	43	
スパムメールの件名行	26	
せ		
設置後の作業	15	
設定		
ドメイン	53	
そ		
[送信者メールアドレスによる拒否 / 許可] ページ	37	
[送信元ドメインによる拒否 / 許可] ページ	37	
送付先メールサーバの設定	31	
た		
タグ付きメールの設定	26, 69	

タグ付けスコア 26

ち

中国語スパムルール 53

て

テクニカルサポート 8

添付ファイル

 隔離 39

 ブロック 38

[添付ファイル拡張子フィルタリング] ページ .. 38

と

ドメイン設定 31

ドメイン設定の編集 54

トラブルシューティング 63

な

なりすまし保護 47

に

日次メール統計 21

日本語スパムルール 53

ね

ネットワークタイムプロトコル 14

は

配送不能レポート 61

パスワードの変更 32, 68

バックアップ

 システム設定 41

 ベジアンデータベース 41

 ユーザ単位の設定 41

パフォーマンス統計 21

バラクーダスパムファイアウォール

 概要 5

 管理 19

 機能 8

 構成 12

 設置 11

 設置後の作業 15

 保証方針 8

 モデルの比較 8

バラクーダヘッダーを削除 48

ひ

非スパム

 メッセージを分類 23

ふ

[ファームウェア更新] ページ 49

ファイアウォールの設定 14

ファイル拡張子 38

 隔離 39

フィンガープリンティング

 動作の変更 45

ブラックリストサービス 35

へ

ベジアンデータベース

 バックアップ 41

 リストア 42

ベジアンデータベースのリセット 33

[ベジアン/フィンガープリンティング] ページ

..... 45

ヘッダー

 隔離 40

 拒否 40

 タグ付け 40

 ホワイトリスト化 40

ヘッダー (バラクーダ)

 削除 48

[ヘッダーによるフィルタリング] ページ 40

変更

 ユーザ設定 68

編集

 ドメイン 54

ほ

防御層 5

保証方針 8

ホワイトリスト

 メッセージを追加 23

ホワイトリストから外す 23

[本文によるフィルタリング] ページ 40

本文の内容

 隔離 40

 拒否 40

 タグ付け 40

 ホワイトリスト化 40

む

無効化

 スパムスコアリング 69

 フィンガープリンティング 45

め

メール

 統計 21

メールエイリアスの統合 55

メールサーバ 53

メール詳細情報の表示	25
メール統計	21
メールのキューサイズ	21
メールの詳細	25
[メールプロトコル] ページ	46
メッセージログのクリア	23
メッセージログのプライバシー	25
[メッセージログ] ページ	22

ゆ

有効化

SSL	60
スパムスコアリング	69
フィンガープリンティング	45
[ユーザ機能] ページ	58

ユーザ毎の隔離

設定	29
タイプ	28

ユーザ設定

リストア	42
ユーザ設定の変更	68
[ユーザ] タブ	56

ユーザ単位隔離

アカウント設定の変更	30
ユーザ単位隔離アカウントの削除	56

ユーザ単位の設定

バックアップ	41
--------------	----

ら

ライト (フロントパネル)	20
---------------------	----

り

リストア

システム設定	42
ペイジアンデータベース	42
ユーザ設定	42

リセット

システム	33
ペイジアンデータベース	33

リンクドメイン	30
---------------	----

れ

[レートコントロール] ページ	48
-----------------------	----

ろ

ログイン

隔離インターフェース	66
------------------	----