

電子メールセキュリティサービス クイックリファレンスカード

基本的なセキュリティ設定

すべてのドメインの追加

電子メール保護サービスに、すべてのドメインとサブドメインを追加します。ユーザーリストを共有するドメインには、ドメインエイリアスを設定します。各ドメインとドメインエイリアスの MX レコードを更新してください。

SMTP (ポート 25)トラフィックの制限

すべてのドメインの追加後、ファイアウォールで SMTP (ポート 25)トラフィックを制限し、電子メールセキュリティサービスの IP アドレスからの接続のみを許可します。これにより、迷惑メール業者はサーバーに迷惑メールを直接送ることができなくなります。

<<Blatant Spam Blocking>>の有効化

<<Blatant Spam Blocking>>を使用すると、明白な迷惑メールをブロックして、ユーザー検疫が必要になるメールを最小限にします。

ユーザーとメーリングリストの追加

すべてのユーザーとそのエイリアス、およびメーリングリストを追加します。<<Directory Sync>>、<<SMTP Autorcreate >>、<<SmartCreate>>などの自動化メソッドを使用できます。すべてのユーザーの追加後、<<Non-Account Bouncing>>をオンして、無効なアドレスに送信されるメッセージをブロックする方法もあります。

ウイルスからの保護設定

ドメインに対して<<Non-Account Virus Blocking>>を有効にし、無登録ユーザーに送信される、ウイルスに感染したメッセージが自動的に削除されるようにします。ウイルスが隠れている可能性のある実行可能ファイルの添付されたメッセージを、ブロックまたは検疫するよう Attachment Manager も設定します。

<<Connection Manager>>によるブロックの有効化

<<Connection Manager>>で攻撃が検出されると、自動的にサーバーが保護されます。特定の IP 範囲をブロックしたり、信頼できるサーバーを指定してブロック対象から除外したりすることもできます。

アラートと通知の設定

重要なメールサーバーイベントを追跡するよう、<<Delivery Manager>>および<<Spooling Manager >>の管理者アラートを設定します。

障害復旧の設定

オプションの電子メールプール機能を使用できる場合は、障害復旧用に<<Spool Manager>>を設定します。

緊急時計画の作成

メール転送の問題に対して、緊急時計画を作成し、サポートオプションとトラブルシューティング手順をよく理解しておいてください。

電子メールセキュリティサービスの IP 範囲

| システム | IP 範囲 | CIDR 範囲 | IP/サブネットマスク |
|---------|------------------------------------|------------------|---------------------------------------|
| 5、6、7、8 | 64.18.0.0 – 64.18.15.255 | 64.18.0.0/20 | 64.18.0.0 マスク 255.255.240.0 |
| 200、201 | 207.126.144.0 – 207.126.159.255 | 207.126.144.0/20 | 207.126.144.0 マスク 255.255.240.0 |

技術サポートリソース

[パートナーのサポート情報とリソースをここに追加してください。]

迷惑メール発生時の対策

インターネットから大量の迷惑メールが発生することがあります。電子メールセキュリティサービスは、ほぼすべての迷惑メールをブロックします。ただし、新しい攻撃手段で大量のメールを送信してくる迷惑メール業者からの一部の迷惑メールが受信箱(Inbox)に届くことがあります。

必ず、電子メールセキュリティサービスがこの問題に対応できるようにし、攻撃から保護されるようフィルタを更新してください。迷惑メールの発生状況については、サポートサイトで確認してください。

ユーザーへの迷惑メールのトラブルシューティング

特定のユーザーに迷惑メールが配信されている場合は、次の手順でトラブルシューティングを行なってください。

そのユーザーのアドレスが電子メール保護サービスに追加されているか？

「Administration Console」でユーザーのアドレスを検索します。見つからない場合は、メールがフィルタなしで配信されています。そのユーザーのアドレスを追加し、次の点を確認してください。

- ◆ そのアドレスが登録済みユーザーのものである場合は、ユーザーエイリアスを追加します。
- ◆ サービスが、ドメインエイリアスでアドレスを認識できない場合は、そのユーザーのドメインのドメインエイリアスを作成します。
- ◆ アドレスが配布リストの可能性のある場合は、次に示す配布リストの対策を参照してください。

個別のユーザーではなく、メーリングリストまたは配布リスト宛に送信されたメールか？

メールのヘッダーの宛先(To)のアドレスを調べ、そのアドレスを「Administration Console」で検索します。アドレスがない場合は、メーリングリストを追加する必要があります。メーリングリストは組織外のアドレスを含んでいる可能性があるため、リストをユーザーとして追加しないでください。担当する所有者のエイリアスとして追加し、「Quarantine Summary」とパスワードメッセージがメーリングリスト全体ではなく、メーリングリスト所有者に送信されるようにします。

保護サービスをバイパスし、メールサーバーに直接送信されたメールか？

迷惑メール業者は、MXレコードを選択するときにDNS規格に従いません。電子メール保護サービスフィルタがバイパスされることを防止するには、保護サービスのIP範囲(裏面参照)からの電子メールのみを受け付けるよう、メールサーバーやファイアウォールを設定します。

送信者のアドレスは「Approved Senders」リストにあるか？

送信者または送信者のドメインが「Approved Senders」リスト(ユーザーの個人リストまたはユーザーの組織用に定義されたリスト)にある場合、迷惑メールのような内容であってもメールは配信されます。迷惑メール業者が、「Approved Sender」にある送信者アドレスになりすましている場合も同じです。

ユーザーレベルおよび組織レベルの「Senders Lists」を調べ、迷惑メール業者がなりすましに使用することの多い、大規模で広く知られているドメインを削除してください。

ユーザーは自分のアドレスまたはドメインを「Approved Mailing List」に追加しているか？

- ◆ 追加している場合は、迷惑メール設定に関係なく、そのユーザー宛のすべての迷惑メールがユーザーの受信箱(Inbox)に配信されます。
- ◆ 「Administration Console」で、ユーザーの「Approved Senders and Recipients」リストからそのユーザーのアドレスまたはドメインを削除してください。

メッセージを送信したのは組織内のユーザーか？

サーバーがドメイン内のフィルタリングを行うよう設定されている場合を除いて、同じサーバー上のユーザー同士で交換されるメッセージは、電子メール保護サービスで処理されません。メッセージヘッダーを調べて、電子メールが組織内から送信されたものでないか確認してください。

検疫所から配信されたメールか？

ユーザーまたは管理者が、検疫所からメッセージを送信している場合があります。