グレイメールの管理

この章は、次の項で構成されています。

グレイメールの概要

グレイメール メッセージとは、ニュースレター、メーリング リストのサブスクリプション、ソーシャル メディア通知など、スパムの定義に適合しないメッセージです。これらのメッセージは、ある時点では役に立ちますが、その後エンドユーザがもはや受信したくないところまで価値が減少します。

グレイメールとスパムの違いは、エンドユーザが購読していないメッセージであるスパムと異なり、いずれかの時点（エンド ユーザが e-コマース Web サイトでニュースレターを購読したり、会議中に組織に連絡先詳細を提供した場合など）でエンド ユーザが意図的に電子メール アドレスを提供した点です。

E メール セキュリティ アプライアンスでのグレイメール管理ソリューション

E メール セキュリティ アプライアンスのグレイメール管理ソリューションは、統合されたグレイメール スキャン エンジンとクラウド ベースの登録解除サービスの 2 つのコンポーネントで構成されます。

組織でグレイメール管理ソリューションを使用すると、以下が可能になります。

- 統合グレイメールエンジンを使用してグレイメールを識別し、適切なポリシー制御を適用します。

- 登録解除サービスを使用して、不要なメッセージを配信停止にする簡単なメカニズムをエンドユーザに提供します。

これらに加えて、グレイメール管理ソリューションでは、組織に以下を提供することもできます。

- **エンドユーザへの安全な配信停止オプション。**配信停止オプションを模倣することは、よくあるフィッシング技法です。そのため、一般にエンドユーザは、不明な購読解約リンクのクリックに慎重になります。このようなシナリオでは、クラウドベースの登録解除サービスが元の配信停止URIを抽出し、URIのレピュテーションをチェックして、エンドユーザに代わって配信停止プロセスを実行します。これにより、配信停止リンクを装った悪意のある脅威からエンドユーザを保護します。
- **エンドユーザを対象として統一されたサブスクリプション管理インターフェイス。**さまざまなグレイメール送信者が、ユーザに配信停止リンクを表示するためのさまざまなレイアウトを使用しています。ユーザは、メッセージ本文で配信停止リンクを探して、配信停止を行う必要があります。グレイメール送信者に関係なく、グレイメール管理ソリューションは、配信停止リンクを表示するための共通のレイアウトを提供します。
- **管理者にさまざまなグレイメールカテゴリに対するより良い可視性を提供。**グレイメールエンジンでは、各グレイメールを3つのカテゴリに分類し（グレイメールの分類（2ページ）を参照）、管理者はこれらのカテゴリに基づいてポリシー制御を設定できます。
- **スパムに対する有効性の改善**

グレイメールの分類

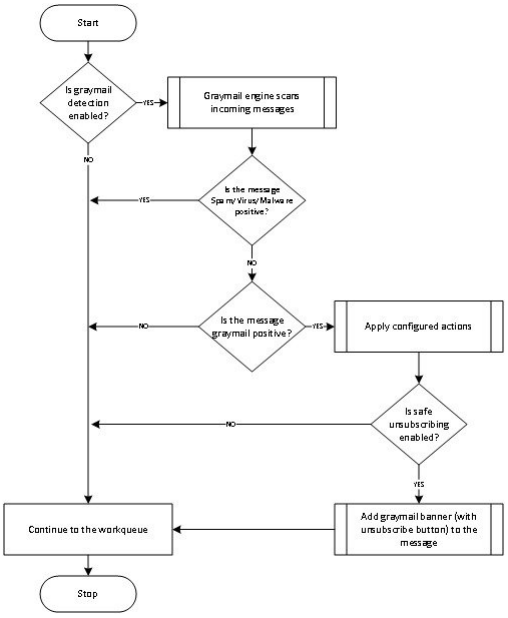
グレイメールエンジンでは、各グレイメールを次のいずれかのカテゴリに分類します。

- **マーケティングメール。**Amazon.comからの新たに販売される製品の詳細に関する記事など、プロフェッショナルマーケティンググループから送信された広告メッセージ。
- **ソーシャルネットワークメール。**ソーシャルネットワーク、出会い系/結婚Webサイト、フォーラムなどからの通知メッセージ。例として、以下からのアラートなどが挙げられます。
  - LinkedIn。関心があると思われるジョブについて
  - CNET Forum。ユーザが投稿に応答した場合。
- **バルクメール。**認識されないマーケティンググループから送信された広告メッセージ（テクノロジーメディア企業のTechTargetからのニュースレターなど）。

グレイメール管理ソリューションの仕組み

次の手順では、グレイメール管理ソリューションのワークフローを示します。

図 *1:* グレイメール管理ソリューションのワークフロー



ワークフロー（Workflow）

ステップ 1 E メール セキュリティ アプライアンスは、着信メッセージを受信します。

ステップ 2 E メール セキュリティ アプライアンスは、グレイメール検出がイネーブルかどうかを確認します。グレイメール検出が有効になっている場合は、ステップ 3 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 3 E メール セキュリティ アプライアンスは、メッセージがスパム、ウイルス、またはマルウェア陽性かどうかを確認します。陽性の場合は、ステップ 8 に進みます。それ以外の場合は、ステップ 4 に進みます。

ステップ 4 E メール セキュリティ アプライアンスは、メッセージがグレイメールかどうかを確認します。メッセージがグレイメールの場合は、ステップ 5 に進みます。それ以外の場合は、ステップ 8 に進みます。

ステップ 5 E メール セキュリティ アプライアンスは、削除、配信、バウンス、スパム隔離エリアへの隔離など、設定されたポリシー アクションを適用します。

ステップ 6 E メール セキュリティ アプライアンスは、安全な配信停止がイネーブルになっているかどうかを確認します。安全な配信停止が有効になっている場合は、ステップ 7 に進みます。それ以外の場合は、ステップ 8 に進みます。

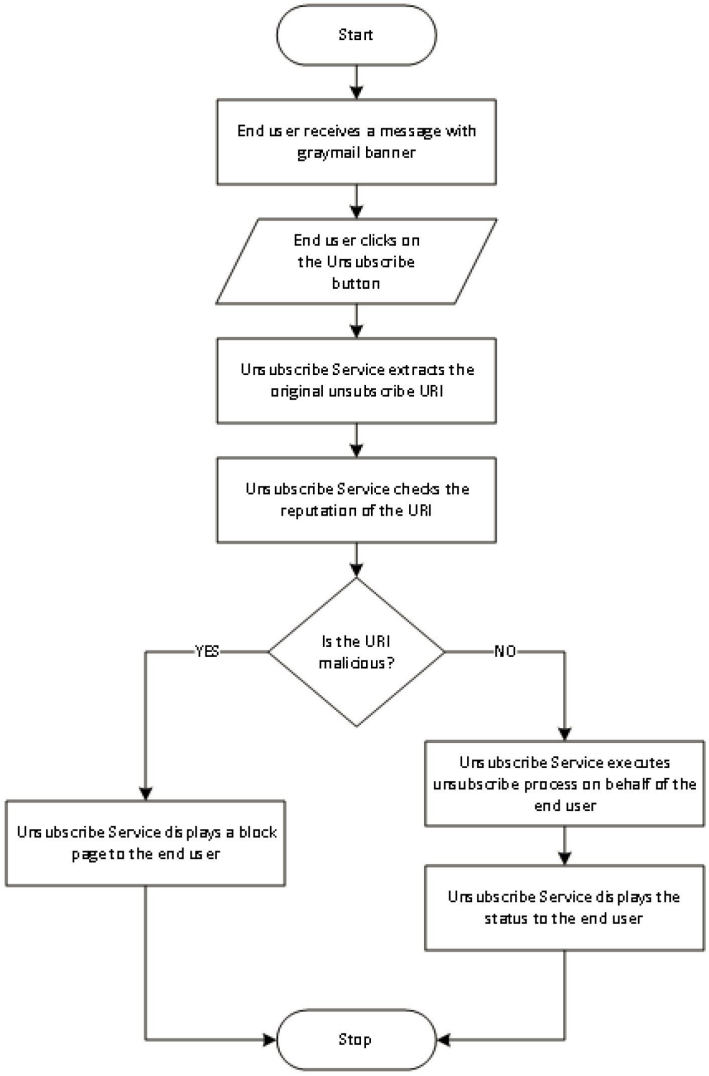
ステップ 7 E メール セキュリティ アプライアンスは、配信停止ボタン付きのバナーをメッセージに追加します。また、E メール セキュリティ アプライアンスは、メッセージ本文内の既存の配信停止リンクを書き換えます。

ステップ 8 E メール セキュリティ アプライアンスは、電子メールのワーク キューの次の段階でメッセージを処理します。

安全な登録解除の仕組み

次のフロー チャートで、安全な配信停止のしくみを示します。

図 *2:* 安全な配信停止のワークフロー



ワークフロー（Workflow）

ステップ 1 エンドユーザがグレイメール バナーを含むメッセージを受信します。

ステップ 2 エンドユーザが [購読解約（Unsubscribe）] リンクをクリックします。

ステップ 3 登録解除サービスは、元の配信停止 URI を抽出します。

ステップ 4 登録解除サービスは、URI のレピュテーションを確認します。

ステップ 5 URI のレピュテーションに応じて、登録解除サービスは次のいずれかのアクションを実行します。

- URI に悪意がある場合、登録解除サービスは配信停止プロセスを実行せず、エンド ユーザにブロック ページを表示します。
- URI に悪意がない場合、URI のタイプ（http または mailto）に応じて、登録解除サービスはグレイメール送信者に配信停止要求を送信します。
  - 要求が成功した場合、登録解除サービスはエンド ユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - 最初の配信停止要求が失敗した場合、登録解除サービスは[配信停止プロセスの進行中（Unsubscribe process in progress）] というステータスを表示し、配信停止のステータスを追跡できる URL を示します。

    エンドユーザはこのURLを使用して後でステータスを追跡することができます。最初の試行失敗後、登録解除サービスは 4 時間の間、定期的に配信停止要求を送信します。

    エンド ユーザが後から配信停止プロセスのステータスを確認した場合、次のようになります。

  - （最初の試行失敗から）4 時間以内にいずれかの要求が成功した場合、登録解除サービスはエンドユーザに [登録が解除されました（Successfully unsubscribed）] というステータスを表示します。
  - （最初の試行失敗から）4 時間以内にいずれの要求も成功しなかった場合、登録解除サービスはエンド ユーザに [登録できません（Unable to subscribe）] というステータスを表示し、グレイメールを手動で配信停止するための URL を示します。

グレイメールの検出および安全な配信停止の設定

グレイメールの検出と安全な配信停止の要件

- グレイメールを検出するには、アンチスパム スキャンをグローバルにイネーブルにする必要があります。これには IronPort Anti-Spam 機能またはインテリジェント マルチスキャン機能のいずれかを使用できます。参照先： スパム対策
- 安全な配信停止の場合、
  - 安全な配信停止機能キーを追加します。
  - エンドユーザのマシンは、インターネット経由で直接クラウドベースの登録解除サービスに接続できる必要があります。

クラスタ構成でのグレイメールの検出および安全な登録解除

グレイメールの検出および安全な配信停止は、マシン レベル、グループ レベルまたはクラスタ レベルでイネーブルにできます。

グレイメールの検出および安全な配信停止の有効化

はじめる前に

グレイメールの検出と安全な配信停止の要件 （5 ページ）を満たします。

ステップ 1 [セキュリティ サービス（Security Services）] > [検出と安全な配信停止（Detection and Safe Unsubscribe）] をクリックします。

ステップ 2 [グローバル設定を編集（Edit Global Settings）] をクリックします。

ステップ 3 [グレイメール検出を有効にする（Enable Graymail Detection）] をオンにします。

ステップ 4 （任意）グレイメール送信者から送信される大量のメッセージをスキャンできるようにしながら、アプライアンスのスループットを最適化するには、メッセージ スキャンのしきい値を構成します。

- アプライアンスでスキャンするメッセージの最大サイズ。
- メッセージのスキャン時に、タイムアウトになるまで待機する秒数。

ステップ 5 （任意）[自動アップデートを有効にする（Enable Automatic Updates）] をクリックして、エンジンの自動アップデートを有効にします。

アプライアンスは、アップデート サーバから特定のエンジンに必要なアップデートを取得します。

ステップ 6 [安全な配信停止を有効にする（Enable Safe Unsubscribe）] をオンにします。

ステップ 7 変更を送信し、保存します。

次のタスク

CLI でグレイメールの検出および安全な配信停止のグローバル設定を構成するには、graymailconfig を使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

グレイメールの検出と安全な配信停止の着信メール ポリシーの設定

はじめる前に

グレイメールの検出および安全な配信停止の有効化 （6 ページ）

ステップ 1 [メール ポリシー（Mail Policies）] > [受信メール ポリシー（Incoming Mail Policies）] をクリックします。

ステップ 2 変更するメール ポリシーの [グレイメール（Graymail）] 列のリンクをクリックします。

ステップ 3 要件に応じて、次のオプションを選択します。

- グレイメール検出の有効化
- 安全な配信停止の有効化
- 上記のアクションをすべてのメッセージまたは未署名のメッセージのいずれに適用するかを選択します。

（注） S/MIME を使用して暗号化されている場合または S/MIME 署名が含まれる場合、アプライアンスはメッセージを署名済みとみなします。

- さまざまなグレイメール カテゴリ（マーケティング メール、ソーシャル ネットワーク メール、およびバルク メール）に対して実行するアクション。
  - メッセージの削除、配信、バウンス、または（スパム隔離エリアへの）隔離

    （注） 安全な配信停止オプションを使用する場合、配信または隔離するアクションを設定する必要があります。

  - 代替ホストへのメッセージの送信
  - メッセージの件名の変更
  - カスタム ヘッダーの追加
  - 代替エンベロープ受信者へのメッセージの送信

    （注） グレイメール陽性メッセージを代替エンベロープ受信者に送信する場合、バナーは追加されません。

  - メッセージのアーカイブ

    （注） 検出されたグレイメールのみをモニタする場合、ポリシーごとにグレイメール検出を有効にできます。さまざまなグレイメール カテゴリに対するアクションを設定する必要はありません。このシナリオでは、E メール セキュリティ アプライアンスは、検出されたグレイメールに対して何もアクションを実行しません。

ステップ 4 変更を送信し、保存します。

次のタスク

（注） グレイメール検出の発信メール ポリシーを設定することもできます。このシナリオでは、安全な配信停止は設定できないことに注意してください。

CLI でグレイメールの検出および安全な配信停止用のポリシーを設定するには、**policyconfig** を使用します。詳細については、『*CLI Reference Guide for AsyncOS for Cisco Email Security Appliances*』を参照してください。

グレイメール スキャン中に追加された X-IronPort-PHdr ヘッダー

次の場合、グレイメール エンジンによって処理されるすべてのメッセージに、X IronPort PHdr ヘッダーが追加されます。

- アプライアンスでグレイメール エンジンがグローバルに有効である。
- グレイメール スキャンが特定のメール ポリシーに対して有効である。

（注） グレイメール スキャンが特定のメール ポリシーに対して有効になっていない場合、アプライアンスでグレイメールエンジンがブローバルに有効な場合は、すべてのメッセージにX-IronPort-PHdrヘッダーが追加されます。

X-IronPort-PHdrヘッダーには符号化された独自の情報が含まれており、顧客による復号はできません。このヘッダーは、グレイメールの設定に関する問題のデバッグに関する追加情報を提供します。

（注） スパム対策エンジンまたはアウトブレイク フィルタが特定のメール ポリシーに対して有効な場合、X-IronPort-PHdr ヘッダーは、特定のメール ポリシーを通過するすべてのメッセージに追加されます。

メッセージ フィルタを使用したグレイメール アクションのバイパス

特定のメッセージにグレイメール アクションを適用しない場合、次のメッセージ フィルタを使用してグレイメール アクションをバイパスできます。

メッセージ フィルタ アクション	説明
skip-marketingcheck	マーケティング メールに対するアクションのバイパス
skip-socialcheck	ソーシャル ネットワーク メールに対するアクションのバイパス
skip-bulkcheck	バルク メールに対するアクションのバイパス

次の例では、リスナー “private_listener” で受信したメッセージは、ソーシャル ネットワーク メールに対するグレイメール アクションをバイパスする必要があること指定しています。

```
internal_mail_is_safe:
if (recv-listener == 'private_listener')
{
skip-socialcheck
();
}
```

グレイメールのモニタリング

次のレポートを使用して、検出されたグレイメールに関するデータを表示できます。

レポート	含まれているグレイメールのデータ	詳細
[概要（Overview）] ページ > [受信メールサマリー（Incoming Mail Summary）]	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメールメッセージの数と、グレイメール メッセージの総数。	[概要（Overview）] ページ
[受信メール（Incoming Mail）] ページ > [グレイメールメッセージの送信者上位（Top Senders by Graymail Messages）]	グレイメールの上位送信者。	[受信メール（Incoming Mail）] ページ
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）]	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメール メッセージの数と、すべての IP アドレス、ドメイン名、またはネットワーク オーナーのグレイメール メッセージの総数。	
[受信メール（Incoming Mail）] ページ > [受信メールの詳細（Incoming Mail Details）] > [送信者プロファイル（Sender Profile）]（ドリル ダウン ビュー）	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメール メッセージの数と、指定された IP アドレス、ドメイン名、またはネットワーク オーナーのグレイメールメッセージの総数。	
[内部ユーザ（Internal Users）] ページ > [グレイメールの上位ユーザ（Top Users by Graymail）]	グレイメールを受信する上位エンドユーザ。	[内部ユーザ（Internal Users）] ページ
[内部ユーザ（Internal Users）] ページ > [ユーザメールフローの詳細（User Mail Flow Details）]	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの受信グレイメール メッセージの数と、すべてのユーザのグレイメールメッセージの総数。	
[内部ユーザ（Internal Users）] ページ > [ユーザメールフローの詳細（User Mail Flow Details）] > [内部ユーザ（Internal User）]（ドリル ダウン ビュー）	グレイメールカテゴリ（マーケティング、ソーシャル、およびバルク）ごとの着信グレイメール メッセージの数と、指定されたユーザのグレイメール メッセージの総数。	

AsyncOS 9.5 以降にアップグレード後、メール ポリシーのアンチスパム設定でマーケティングメールのスキャンをイネーブルにした場合は、次の点に注意してください。

- マーケティング メッセージの数は、アップグレードの前後に検出されたマーケティング メッセージの合計です。

- グレイメール メッセージの総数には、アップグレード前に検出されたマーケティング メッセージの数は含まれません。
- 試行されたメッセージの総数には、アップグレードの前に検出されたマーケティング メッセージの数も含まれます。

グレイメール ルールの更新

サービスのアップデートをイネーブルにした場合、シスコのアップデート サーバからグレイメール管理ソリューションのスキャン ルールを取得できます。しかし、一部のシナリオでは（たとえば、サービスの自動アップデートをディセーブルにした場合またはサービスの自動アップデートが機能していない場合）、グレイメール ルールを手動で更新できます。

グレイメール ルールを手動で更新するには、次のいずれかを実行します。

- Web インターフェイスで、[セキュリティ サービス（Security Services）] > [グレイメール検出と安全な配信停止（Graymail Detection and Safe Unsubscribing）] ページに移動して [今すぐ更新（Update Now）] をクリックします。
- CLI で graymailupdate コマンドを実行します。

既存のグレイメール ルールの詳細を把握するには、Web インターフェイスで [グレイメール検出と安全な配信停止（Graymail Detection and Safe Unsubscribing）] ページの [ルールの更新（Rule Updates）] を参照するか、CLI で graymailstatus コマンドを使用します。

エンドユーザに表示される [登録解除（Unsubscribe）] ページのカスタマイズ

エンドユーザが配信停止リンクをクリックすると、登録解除サービスにより、配信停止プロセスのステータスを示すシスコ ブランドの配信停止ページが表示されます（安全な登録解除の仕組み （4 ページ）を参照）。[セキュリティ サービス（Security Services）] > [ブロック ページ カスタマイズ（Block Page Customization）] を使用して、配信停止ページの外観および組織のブランディングの表示（企業ロゴ、連絡先情報など）をカスタマイズできます。この説明については、サイトに悪意がある場合にエンド ユーザに表示する通知のカスタマイズ を参照してください。

エンドユーザのセーフリスト

組織のエンド ユーザが自分の電子メール アカウントのセーフリストを設定している場合は、セーフリストの送信者からのグレイメール メッセージはグレイメール スキャン エンジンによってスキャンされません。セーフリストの詳細については、セーフリストおよびブロックリストを使用した送信者に基づく電子メール配信の制御を参照してください。

ログの表示

グレイメールの検出および安全な配信停止情報は、次のログに書き込まれます。

- **グレイメール エンジン ログ**グレイメール エンジン、ステータス、設定などの情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。
- **グレイメールアーカイブ**アーカイブされたメッセージ（スキャン済みの「アーカイブ メッセージ」アクションに関連付けられているメッセージ）が含まれます。この形式は、mbox 形式のログ ファイルです。
- **メール ログ**グレイメールの検出および安全な配信停止用のバナーの追加についての情報が含まれます。ほとんどの情報は [情報（Info）] または [デバッグ（Debug）] レベルです。

グレイメールの検出および安全な配信停止のトラブルシューティング

安全な配信停止を実行できない

問題

配信停止リンクをクリックした後、エンドユーザに「...を配信停止できません」というメッセージが表示されます。

ソリューション

この問題は、登録解除サービスがエンドユーザの代わりに安全な配信停止を実行できない場合に発生することがあります。次に、登録解除サービスが安全な配信停止を実行できない一般的なシナリオをいくつか示します。

- 配信停止 URI または mailto アドレスが間違っている。
- 配信停止にエンド ユーザのクレデンシャルを要求する Web サイト。
- エンド ユーザに自分の電子メール アカウントにログインし、配信停止要求を確認するように要求する Web サイト。
- Web サイトで captcha を解決するよう要求され、登録解除サービスで captcha を解決できない。
- インタラクティブな配信停止を必要とする Web サイト。

エンドユーザは [購読解約（Unsubscribe）] ページの下部に表示されている URL を使用して購読解約を手動で行えます。