目次

[概要](#)
[何 Cisco 電子メール送信およびトラッキングの使用は門脈ですか。](#)
[だれが Cisco 電子メール送信をトラッキング ポータル使用し、か。](#)
[管理者はどのようにポータルと開始できますか。](#)
[管理者は何をポータルですることができますか。](#)
[ビューアはどのようにポータルと開始できるか。](#)
[ビューアはどのように管理者に似合うまたは逆にことができるか。](#)
[ポータルで見られる異なるステータスとは何、ものが意味しますか。](#)

概要

この資料は Cisco 電子メール送信を記述したもので、ポータルを、ポータルの使用方法トラッキングして、および一般のハウツーはポータルの使用の手順を開始します。

何 Cisco 電子メール送信およびトラッキングの使用は門脈ですか。

Cisco 電子メール ゲートウェイは > 99%捕獲物比率および 0.001% false positive が付いている伝染性スパム、ハム、マーケティングおよび graymail メッセージに推奨に残りました。 （傑作 1 レポートを詳細については参照して下さい）。 ただし、バーを高いままにし、全面的な効力を改善するために、Cisco は顧客に不正確に時々分類されるメッセージを入れるように勧めます。 詳細な使用説明書に関しては、Cisco に電子メール メッセージを出す方法を参照して下さい

各顧客送信は Cisco の重要なピースを形成しますか。s 脅威 知性 システム。 それ故に完全情報を用いるおよび右の形式（RFC 822）の服従を持っていることは重要です。 場合によっては、送信は入っただれもその情報を知らないことを得ます方法が理由で重要な情報を失い。

Cisco 電子メール送信およびトラッキング ポータルは組織からのすべての送信をトラッキングし、同時に各送信のステータスを知る顧客向けの方法です。 ポータルはまた抜けていたスパムを入れる方法です。

そこの情報は Cisco とそれ以上の相互対話に使用することができます

だれが Cisco 電子メール送信をトラッキング ポータル使用し、か。

Cisco CCO ユーザー ID およびパスワードをもらうどのユーザでもポータルにアクセスできます。

ただし、ポータルは 2 種類のユーザに役立ちます:

1. **組織の管理者:** すべての送信のステータスを知るために興味を起こさせられる電子メール ゲートウェイ 管理者は組織/ドメインのユーザによって作りました。 あらゆる組織のための複

数の管理者および管理者が組織内のマルチプルドメインを管理する可能性があるそこにある可能性があります。
2. **送信のビューア:** 組織の送信を表示するために管理者によって承認されるユーザー（たとえば、Cisco TAC か顧客 の 代表）。 ビューアは複数の組織からの送信を表示できます。 ビューアは更に調査するのに一般的にポータルの情報を使用します。 たとえば、顧客が Cisco に優先順位の送信をチェックしてほしければそれらは Cisco に同じメッセージを再度出す必要がありません。 その代り、それらは Cisco TAC と送信 ID を共有、Cisco TAC は更に詳しい情報についてはポータル調べることができます。

管理者はどのようにポータルと開始できますか。

ドメインのグループを管理している電子メール管理者はポータルとこれらの手順に従うことによって開始できます:

1. Ciscoセキュリティ ハブに行き、電子メール送信および門脈リンクをトラッキングすることをクリックして下さい。 このステップは Cisco アカウントがあるように要求します。 Cisco アカウントがない場合、登録し、次に開始して下さい。
2. としてレジスタか。管理者か。 そして有効な 16 文字 登録 ID を入力して下さい。

   注AsyncOS 10.0 またはそれ以降を使用している場合、同じユニークな登録 ID がすべてのアプライアンスで最初に入るようにして下さい。 GUI から、**システム 管理 > スパム送信トラッキング門脈登録**。 それから同じ登録 ID はポータルで入ります。

   AsyncOS 10.0 以前のリリースを使用している場合、ポータルのランダム 登録 ID を入力し、続けて下さい。 AsyncOS 10.0 にまたはそれ以上に移行するとき、ESA から完了した場合同じ登録 ID がすべてのアプライアンスでそれから使用されることを確かめて下さい。

1. ポータルに管理されたドメインすべてを追加して下さい。 **新しいドメインは設定 > ドメイン** > Add に行きます。 ドメインが追加されればそれがそのドメインから送信にアクセスしている確実な人であることを確認するために、電子メールは *postmaster@your_domain.com* に送信 されます。

   注このステップはドメインが RFC 5321 不平であり、信頼された人々だけ postmaster@domain メールボックスにアクセスできると仮定します。

   postmaster@your_domain.com がどういうわけかない、それをされます使用できるように確認すれば場合ドメインを追加して下さい、さもないと ESA を設定して下さいか。有効なeメールアドレスに *postmaster@your_domain.com* に電子メールをルーティングする **aliasconfig** CLI コマンドを使用する s。

1. 最終的には、*postmaster@your_domain.com* メールボックスに行き、電子メールで受け入れられる確認リンクをクリックして下さい。

すべての上記のステップが実行されれば、どの送信でも（組織からのあらゆるユーザによって）管理者によって表示することができるポストを作りました。

管理者は何をポータルですることができますか。

管理者はできます:

- すべての送信のダッシュボードを表示し、単一 ペインのステータスをトラッキングして下さい
- 各送信をリストする表をステータス表示し、それらを基づいていましたタイムスタンプ、送信 ID、提出者および他のパラメータにフィルタリングして下さい。
- レポートをダウンロードして下さい
- 送信が管理されなければならないドメインを追加するか、または取除いて下さい
- すべてのビューアおよび権限を管理して下さい
- 門脈によって抜けていたスパムを入れて下さい（EML 形式だけ現在サポートされます。）

ビューアはどのようにポータルと開始できるか。

ビューアはこれらの手順に従うことによって彼ら自身を登録できます:

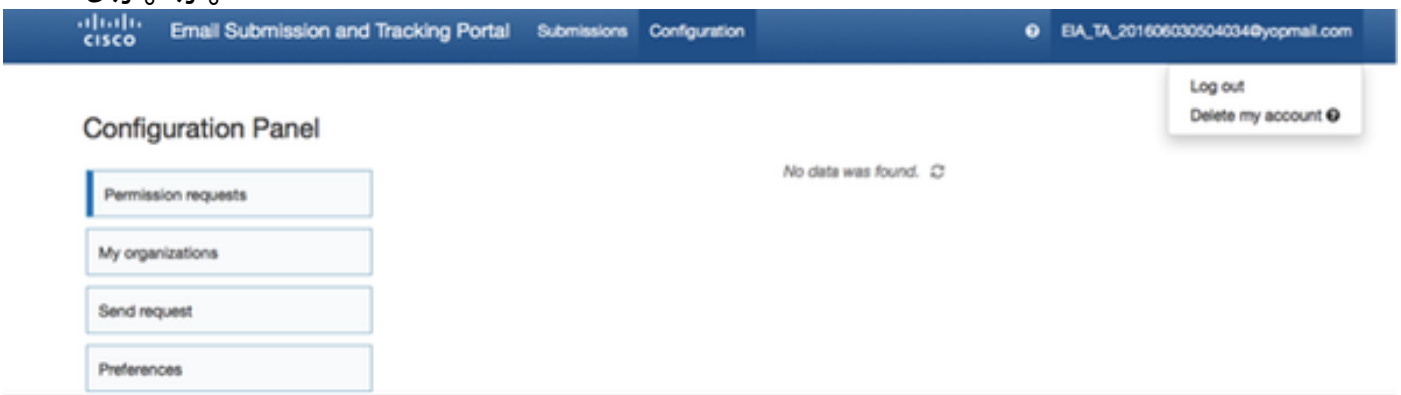
1. Ciscoセキュリティ ハブに行き、電子メール送信および門脈リンクをトラッキングすることをクリックして下さい。 このステップは Cisco アカウントがあるように要求します。 Cisco アカウントがない場合、登録し、次に開始して下さい。
2. レジスタようにか。ビューアか。
3. 組織からのスパム送信を表示するために、その組織の管理者に要求を送信 して下さい。 **設定 > 送信要求**に行って下さい。
4. 次のいずれかを入力して下さい: ポータルで入力される組織の管理者の Eメールアドレス。ビューアが追加詳細を探すことを試みていること送信 ID（少なくとも 1 送信 ID）

入力されて、認証要求は対応した 管理者に送信 されます。 管理者は資格情報を使用してポータルになりますログイン **設定 > アクセス許可要求**への行き、**割り当てを**クリックして承認するか、または**否定するために**。 要求が許可されるか、または否定されれば、ビューアは電子メール確認を受け取ります。

ビューアはどのように管理者に似合うまたは逆にことができるか。

ビューアとして登録し、（または逆に）管理者になりたいと思ったら、次の作業が必要です:

1. 右上隅から、***ユーザ名* > Delete をアカウント** クリックして下さい。
2. 要件によっては、述べられる次のいずれかのトピックでステップを実行して下さい: ?管理者はどのようにポータルと開始できますか。か。 ビューアはどのようにポータルと開始できるか。か。



?

ポータルで見られる異なるステータスとは何、ものが意味しますか。

各送信は Cisco 知性 システムを入力した上で自動的に処理され、評価されます。 分析に基づい

て、システムは送信のための次のいずれかのステータスを設定 します:

ステータス	定義
名誉棄損となる	右の形式で行われるすべてのオリジナル インターネット ヘッダが、電子メ ボディ名誉棄損となる考慮されます。 名誉棄損となるために判別される送信サンプルは他の顧客からの名誉棄損 イス テレメトリーおよび外部/パートナー データ フィードとともに結合さ このすべて重くすること自動化され、E メール セキュリティ デバイスによ
名誉棄損となるしかし不完全	子メール機能へ 10 のためにマシン 学習 システム、テクノロジー、新しい 完全なメッセージ ボディ、等診断 X ヘッダのような行方不明の重要なヘッ 追加しました。 これは使用されたクライアント（例えば展望）が理由で送 注： Outlook 別のバージョンはヘッダを時々削除するために確認しました
非名誉棄損となる	抜けた重要なヘッダは分析を妨げ、送信の影響を制限するかもしれません 理されますか。」可能な限り次数に名誉棄損となる。 （リストされているが、に制限されない）1つ以上の基準が「非名誉棄損と 送信はマークされた非名誉棄損となります。 電子メール メッセージを Cisco に出し再度入る方法の推奨事項に従って下 この状態の送信はこれからの プロセスのために奪取 されません。

注送信サンプルはこれからの プロセスや人間確認が発生すると同時に名誉棄損となるから の非名誉棄損となるへのより遅い変更、または逆にかもしれないです。

非名誉棄損となるステータスのためのメッセージ属性および原因:

メッセージ アトリビュート	非名誉棄損となる
メッセージフォーマット	メッセージは RFC-822 MIME によって符号化される接続機構として入りません 例： メッセージ送信はインライン転送されます
メッセージヘッダー	1つ以上のオリジナル インターネット ヘッダは抜けているまたは不正です。
経過時間/新鮮さ	メッセージのオリジナル アプライアンス スキャン日付は IPAS トレーニングで されるには余りにも古い/旧式です。
本文コンテンツ	• バウンス通知、自動応答またはユーザ確認のための質問への応答はありま メッセージは不正 なまたは NULL 本文コンテンツが含まれています。 • 内部 会社 phishing トレーニング演習。 • スパム コンテンツを論議する正当 な メッセージ。 例： セキュリティ情報および通知。