スパム、誤分類、ウイルス性のEメールメッセージを報告する

内容

概要

このドキュメントでは、サポートまたは調査のために、スパム、誤分類、ウイルス、または追加の電子メールをシスコに報告する方法について説明します。

電子メールメッセージの送信タイプ

スパム、ハム、およびマーケティング電子メールメッセージは次のとおりです。

- スパム：受信者への不適切または不適切な電子メールメッセージ。
- ハム:スパムではない電子メールメッセージ。または、「非スパム」、「正常なメール」。
- *Marketing:*電子メールメッセージを直接販売する。

シスコは、誤って分類された電子メールの送信を受け付けます。

- false-negative（スパムの見逃し）
- 偽陽性（または「ハム」）
- 偽陰性のマーケティングメッセージ
- 誤検出のマーケティングメッセージ
- フィッシング疑いメッセージ、フィッシング陽性メッセージ
- ウイルスが疑われるウイルス陽性メッセージ

シスコに電子メールを報告する理由

欠落または誤ってマークされたEメールメッセージがシスコに報告され、内容の確認、全体的な有効性、関連するルールとスコアが記載されます。シスコにEメールを報告すると、Eメールステータスポータルを使用して追加のオブザーブと埋め込み添付ファイルを表示することもできます。

電子メールステータスポータル

有効なCCO IDを使用して、https://talosintelligence.com/tickets/email_submissionsにログインできます。Eメールステータスポータルは、シスコへのEメール送信のステータスを表示するツールです。シスコは、現在の検出内容をバイパスしたスパム/フィッシングと、誤ってフィルタリングされた望ましい電子メールであるハムの送信を推奨し、全体的な有効性を向上させます。Eメールステータスポータルでは、これらの提出物のステータスを追跡できます。送信を監視できます。ドメイン管理者またはドメインビューアーは、ドメインからのすべての送信を監視できます。

> **注**:2020年9月1日の時点で、従来のEメール送信および追跡ポータル(ESTP)は、Talosintelligence.comでホストされるEメールステータスポータルに置き換えられました。

シスコへの電子メールメッセージの報告方法

サポートされる方法は次のとおりです。

1. Cisco Secure Email Submissionアドイン
   Outlook(Windows、Mac、Web)をサポート
2. Cisco Eメールセキュリティプラグイン Outlookをサポート（Windowsのみ）
3. エンドユーザからのダイレクトメール送信

Cisco Secure Email Submissionアドイン

Cisco Secure Email Submissionアドインは、Microsoft Outlook for Windows、Mac、およびWebをサポートしています。お使いのOutlookのバージョンとの互換性を確認するには、『Cisco Secure Email Encryption Serviceの互換性マトリクス』の「Cisco Secure Email Encryption

Service Add-InおよびCisco Secure Email Submission Add-inのサポートされる構成」を参照してください。

ドキュメントのダウンロードとインストールについては、Cisco Secure Email Submission Add-inを参照してください。

Cisco Eメールセキュリティプラグイン

Cisco Eメールセキュリティプラグインは、Windows上のMicrosoft Outlookのみをサポートしています。ご使用のOutlookのバージョンとの互換性を確保するには、『Cisco Secure Email Encryption Serviceの互換性マトリクス』の「Cisco Email Reportingプラグインのサポートされる構成」を参照してください。

> **注**：古いバージョンのプラグインは、「IronPort Email Security Plug-in」または「Encryption Plug-in for Outlook」という名前です。 このバージョンのプラグインには、レポートと暗号化の両方が含まれています。2017年、シスコはサービスを分離し、プラグインの2つの新しいバージョン、「Email Reporting Plugin for Outlook」と「Email Encryption Plugin for Outlook」をリリースしました。 これらは1.0.0.xバージョンで使用できました。

ダイレクトメール送信

電子メールをRFC 822 Multipurpose Internet Mail Extension(MIME)でエンコードされた添付ファイルとして添付するには、指定された電子メールクライアントの手順に従ってください。使用しているEメールクライアントがサンプルに含まれていない場合は、Eメールクライアントのユーザガイドまたは製品サポートを直接参照して、Eメールクライアントが「添付ファイルとしての転送」をサポートしていることを確認してください。

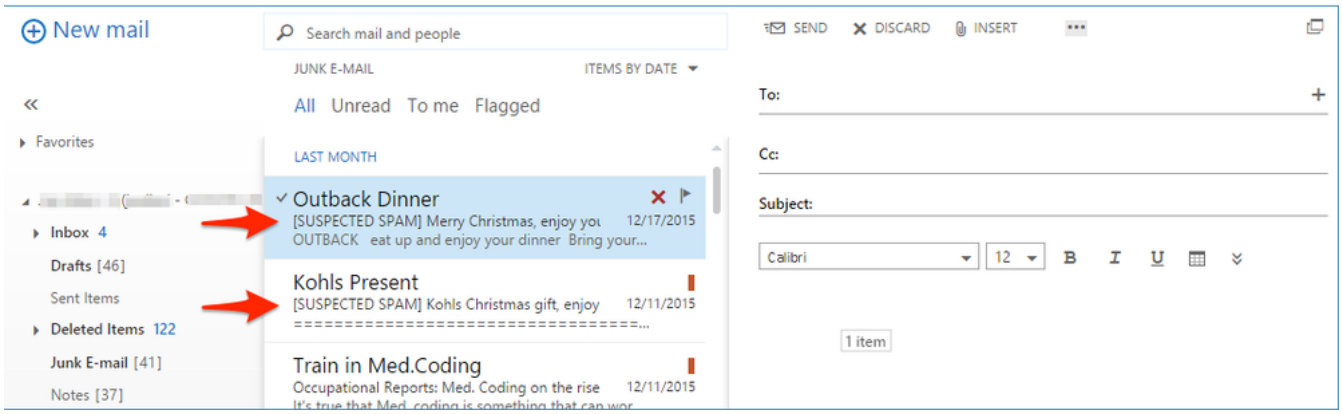
適切な電子メールアドレスに電子メールを送信してください。

spam@access.ironport.com	エンドユーザがEメールメッセージをスパムと見なすか、件名に[SUSPECTED SPA含まれています。
ham@access.ironport.com	エンドユーザは、Eメールメッセージをスパムとはみなしません。件名行に[SUSPESPAM]が含まれているか、件名行に追加タグが含まれています。
ads@access.ironport.com	エンドユーザは、電子メールメッセージがマーケティングコンテンツまたはグレイメであるか、含まれていると見なします。または、件名に[MARKETING]、[SOCIAL NETWORK]、または[BULK]が含まれています。
not_ads@access.ironport.com	エンドユーザは、電子メールメッセージをマーケティングまたはグレイメールと見なせん。または、件名に[MARKETING]、[SOCIAL NETWORK]、または[BULK]が含まいます。
phish@access.ironport.com	電子メールメッセージがフィッシング詐欺のように見える（ユーザー名、パスワードレジットカード情報、その他の個人情報を取得するように設計されている）、またはウェアの添付ファイルが含まれている（同様に、ユーザー名またはパスワードを取得ように設計されている）場合。 件名行の先頭には、[SUSPECTED SPAM]、[Possibl

	$threat_category Fraud]、または同様の文字列が付加されます。
virus@access.ironport.com	エンドユーザは、電子メールメッセージまたは添付ファイルをウイルス性と見なすか名に[WARNING:検出されたウイルス]。

すべての件名行に追加のテキストとタグが含まれているわけではありません。設定については、Cisco Secure Email GatewayまたはCloud Gatewayの設定で、スパム対策、ウイルス対策、グレイメール、アウトブレイクフィルタについて確認するか、電子メール管理者に連絡して問題がないか確認してください。

タグ付き件名行の例：



警告：Eメールメッセージを提出物として「転送」しないでください。このアクションでは、メールルーティングヘッダーの順序は保持されず、電子メールの発信元の属性を設定するために必要なメールルーティングヘッダーが削除されます。その代わり、必ず「添付ファイルとして転送」オプションを使用して問題の電子メールを送信してください。

電子メールは次のサイトから直接送信できます。

- Microsoft Outlook
- Microsoft Outlook Web App、Microsoft Office 365
- Microsoft Outlook 2011およびMicrosoft Outlook 2016 for Mac(OS X、macOS)
- メール(OS X、macOS)
- Mozilla Thunderbird
- モバイルプラットフォーム（iPhone、Android、その他）

Microsoft Outlook

- Microsoft Outlookからの推奨される送信方法は、Cisco Secure Email Submissionアドインを使用することです。

- スパム、ウイルス、フィッシングなど、迷惑メールや迷惑メールに関するメッセージをシスコに送信します。
- [Not Spam]ボタンを使用すると、スパムとしてマークされた正当な電子メールメッセージをすばやく再分類できます。

注：Cisco Eメールセキュリティプラグインをインストールできない、またはインストールしない場合は、次の手順に従ってください。

Microsoft Outlook Web App、Microsoft Office 365

1. Microsoft Outlook Web Appでメールボックスを開きます。
2. 送信するメッセージを選択します。
3. 左上の「New mail」をクリックします。
4. メッセージをドラッグし、添付ファイルとして新しいメッセージにドロップします。
5. このドキュメントに記載されているそれぞれのアドレスに電子メールメッセージを送信します。

Microsoft Outlook 2011およびMicrosoft Outlook 2016 for Mac(OS X、macOS)

1. メッセージペインでメッセージを選択します。
2. [Attachment]ボタンをクリックします。
3. このドキュメントに記載されているそれぞれのアドレスにメッセージを転送します。

メール(OS X、macOS)

1. 電子メールメッセージ自体を右クリックし、[Forward as Attachment] を選択します。
2. このドキュメントに記載されているそれぞれのアドレスに電子メールメッセージを転送します。

Mozilla Thunderbird

1. 電子メールメッセージ自体を右クリックし、[Forward As] > [Attachment] を選択します。
2. このドキュメントに記載されているそれぞれのアドレスに電子メールメッセージを転送します。

注：MailSentry IronPort Spam Reporterは、Mozilla Thunderbird用のサードパーティ製プラグインで、説明と同じアクションを実行しますが、[Spam/Ham]ボタンを提供します。**MailSentry IronPort Spam Reporterは、シスコがサポートするプラグインではありません。**

モバイルプラットフォーム（iPhone、Android、その他）

- お使いのモバイルプラットフォームに添付ファイルとして元の電子メールを転送する方法がない場合は、提供されている他の方法のいずれかへのアクセス権が得られてから送信してください。

シスコへの提出物の確認方法

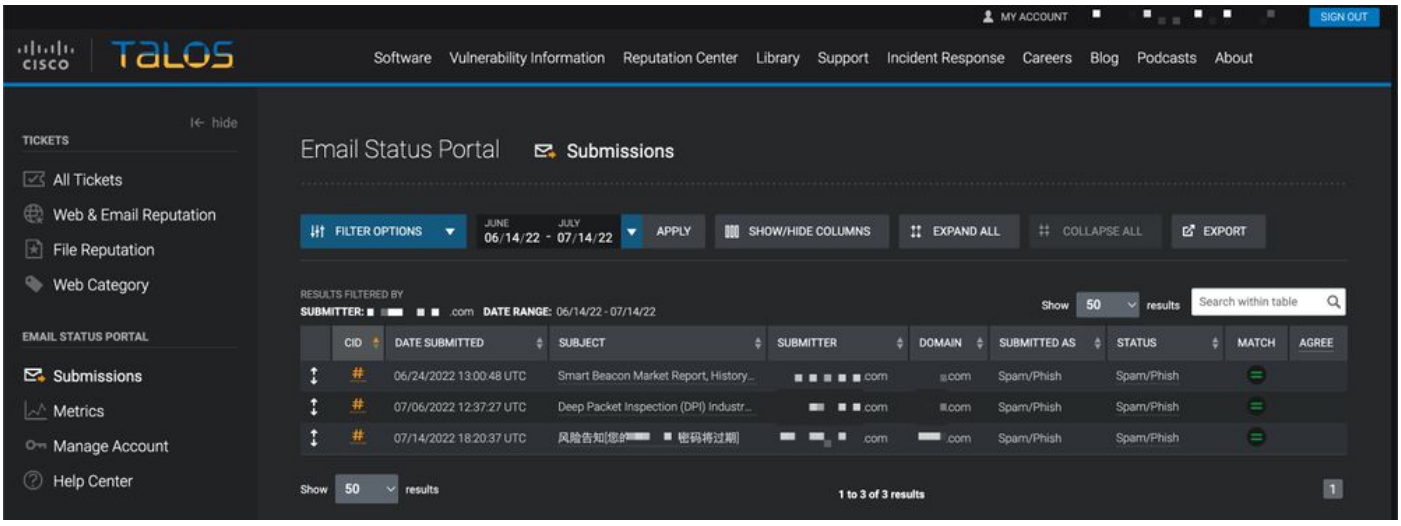
ダイレクトメール送信

シスコは、電子メールの送信に関して、確認の電子メールまたは受領通知を提供しません。代わりに、Talosintelligence.comでホストされているEmail Status Portalを使用して提出物を確認してください。

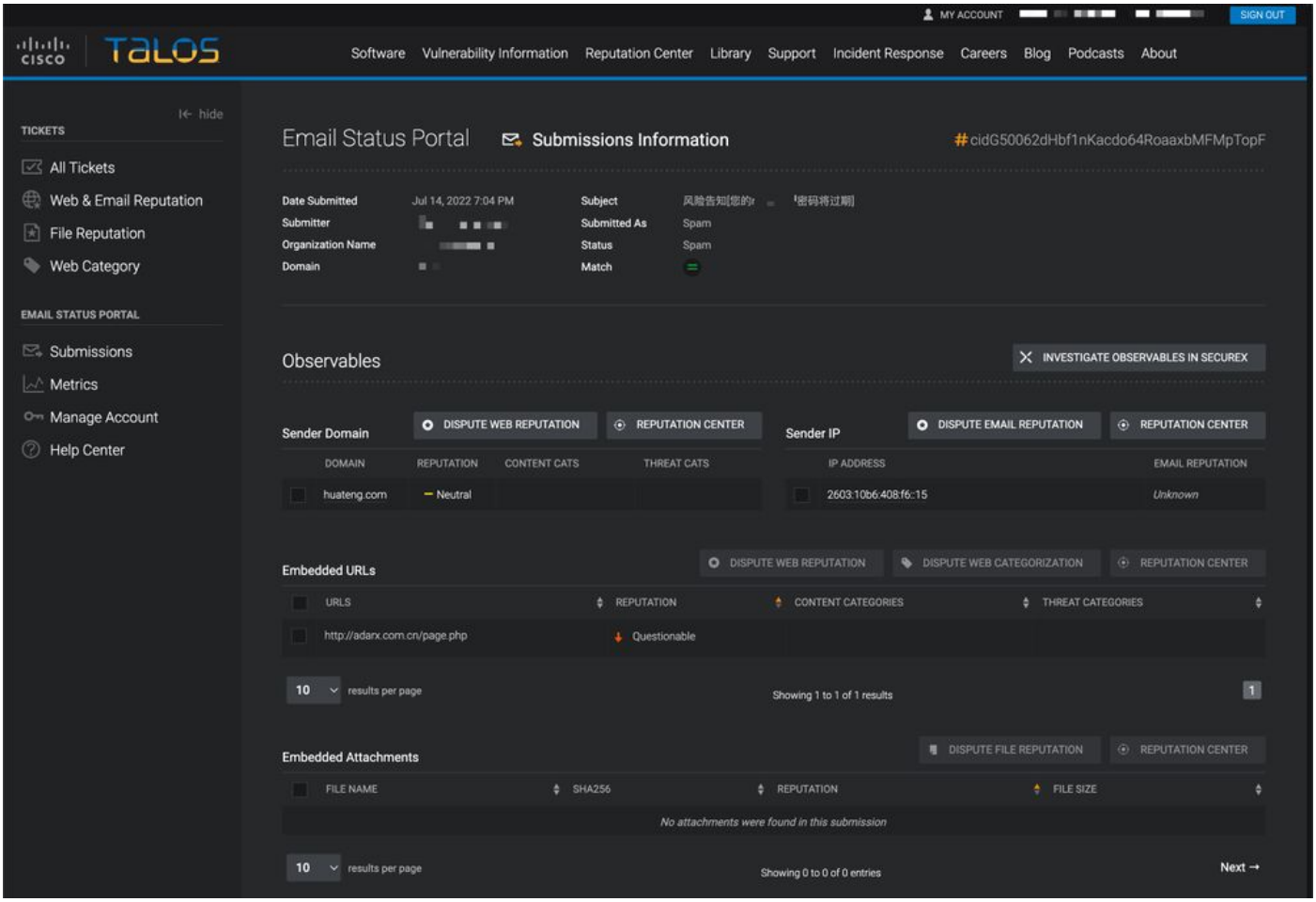
電子メールステータスポータル

Eメールステータスポータルから提出物を確認してください。ログインすると、指定した日時の範囲内のすべての提出物のリストが表示されます。

例：



一意のCID「#」をクリックすると、レポートされた電子メールに関連する詳細を確認できます。



報告された電子メールに関連付けられた送信者ドメイン、送信者IP、埋め込みURL、および埋め込み添付ファイルが表示されます。**Dispute Web Reputation**、**Dispute Email Reputation**、および**Dispute File Reputation**でさらにアクションを実行できます。

ネストされた各情報行には、埋め込みURLと埋め込み添付ファイルが最大5つ表示されます。電子メール送信のオブザーブが多い場合は、[Go to Email Submission Detail Page]をクリックすると、抽出されたオブザーブの完全なリストが表示されます。

目的の観察可能な単一の観察可能なレピュテーションの詳細を検索し、[Reputation Center]ボタンをクリックできます。

また、SecureXを使用して複数のオブザーブを調査することもできます。このダッシュボードは、お客様のシスコ製品ポートフォリオに基づいて、Cisco Secure製品のフルスイートからレピュテーションデータを結合します。[Investigate observables in SecureX]ボタンを使用すると、1回の送信から最大20個のオブザーブを選択して、SecureXで一度に調査できます。

ユーザは、レピュテーションに関するクレーム（Web、Eメール、またはファイル）を1つ提出す

るか、1件の提出物ごとに1つ以上のクレームを一括して適用することができます。URLとドメインに対してWeb分類のクレームを提出することもできます。

Eメールステータスポータルの詳細については、次のサイトを参照してください。
https://talosintelligence.com/tickets/email_submissions/help

追加情報

Cisco Secure Email Gatewayのドキュメント

- リリース ノート
- ユーザガイド
- CLIリファレンスガイド
- Cisco Secure Email GatewayのAPIプログラミングガイド
- Cisco Secure Email Gatewayで使用されるオープンソース
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（仮想クラウドゲートウェイを含む）

Secure Email Cloud Gatewayドキュメント

- リリース ノート
- ユーザガイド

Cisco Secure Email and Web Managerのドキュメント

- リリースノートと互換性マトリクス
- ユーザガイド
- Cisco Secure Email and Web ManagerのAPIプログラミングガイド
- Ciscoコンテンツセキュリティ仮想アプライアンスインストールガイド（仮想EメールとWeb Managerを含む）

Cisco Secure製品ドキュメント

- Cisco Secureポートフォリオの命名アーキテクチャ