Cisco Secure Email Reporting Plug-in の展開

この章は、次の項で構成されています。

Cisco Secure Email Reporting Plug-in

Cisco Secure Email Reporting Plug-in を使用すると、Outlook ユーザは、スパム、ウイルス、フィッシング、およびマーケティングメッセージなど、一方的に送りつけられる不要な電子メールメッセージについてシスコにフィードバックを送信できます。シスコでは、このフィードバックを活用してフィルタを更新し、不要なメッセージが受信トレイに配信されないようにします。

さらに、[Not Spam] ボタンを使用して、誤検出（誤って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）をシスコに報告することもできます。正当な電子メール メッセージは「ハム」とも呼ばれます。シスコでは、誤検出に関するレポートを活用してスパム フィルタを調整し、今後、正当な電子メールが誤分類されないようにします。あらゆる正当な電子メールを「**非スパム**」として報告できるので、フィルタの効率向上に役立ちます。

このプラグインは、ツールバー ボタンと右クリック コンテキスト メニューを使用してフィードバックを送信できる便利なインターフェイスです。メッセージを報告すると、メッセージが送信されたことを示すダイアログボックスが表示されます。送信したメッセージデータは、シスコ フィルタを改善するために自動システムによって使用されます。メッセージ データを提出することで、受信ボックスに一方的に送りつけられるメールの量を削減できます。

Cisco Secure Email Reporting Plug-in のインストール

ユーザ グループ向けに Cisco Secure Email Reporting Plug-in をインストールする場合、サイレントインストールを実行できます。サイレント インストールでは、エンド ユーザに入力を求め

ることなくインストールを実行できます。サイレントインストールの詳細については、一括インストールの実行を参照してください。

Cisco Secure Email Reporting Plug-in の設定

Cisco Secure Email Reporting Plug-in をインストールすると、Outlook の [Cisco Secure Email Reporting] タブから設定を変更できるようになります。

Outlook 2010/2013/2016 ではリボンの [プラグインオプション（Plug-in Options）] ボタンをクリックするか、[ファイル（File）] > [オプション（Options）] > [アドイン（Add-ins）] > [アドインオプション（Add-in Options）] > [Cisco Email Reporting] の順に選択します。

Reporting plug-in のインストールは変更が可能です。たとえば、Cisco Secure Email Reporting Plug-in のロギングを有効または無効にできます。

Outlook の設定を変更する場合は、Cisco Secure Email Reporting Plug-in for Outlook の設定と使用を参照してください。

Cisco Secure Email Reporting Plug-in に必要なシステムプロセス

Cisco Secure Email Reporting Plug-in で必要なものは、TCP/IP DNS や DHCP などの必須のシステム プロセスのみで、これらのものは無効にすることはできません。ただし、データベースマネージャ、HTTP サーバ、ハードウェア設定デーモンなどの必須ではないシステムプロセスは、Cisco Email Reporting Plug-in の機能に影響を与えずに無効にすることができます。

Cisco Secure Email Reporting Plug-in に必要な TCP サービス

Cisco Secure Email Reporting Plug-in では、次の TCP/IP サービスと関連ポートを使用する必要があります。これらのポートは、TCP/IP サービスで使用できる状態のままにしておく必要があります。

- DNS（ドメイン ネーム システム）

  DNS サービスは、インターネット ドメイン名とホスト名を IP アドレスに変換します。DNS は、Web ブラウザのアドレスバーに入力した名前を、それらのサイトをホストしている Web サーバの IP アドレスに自動的に変換します。

  ポート番号：53（TCP/UDP）

  詳細については、 http://en.wikipedia.org/wiki/Domain_Name_System を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- SMTP（Simple Mail Transfer Protocol）

  Simple Mail Transfer Protocol（SMTP）は、インターネット プロトコル（IP）ネットワークを介して電子メール（E メール）を伝送するためのインターネット標準です。

  ポート番号：25、587、465、475、2525（TCP）

  詳細については、http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- DHCP（ダイナミック ホスト コンフィギュレーション プロトコル）

  DHCP は、ネットワーク（ホスト）に接続するデバイスの設定に使用されるネットワーク プロトコルです。これによって、デバイスはインターネットプロトコル（IP）を使用してネットワーク上で通信できるようになります。

  ポート番号：67、68（TCP/UDP）

  詳細については、http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol を参照してください。

  影響：大

  処置：このサービスは、DHCP サーバから IP アドレスを自動取得するエンドユーザ全員に対してアクセス可能にする必要があります。

- Net BIOS over TCP/IP

  NetBIOS over TCP/IP（NBT または NetBT）は、NetBIOS API を利用しているレガシー コンピュータ アプリケーションで最新の TCP/IP ネットワークを使用できるようにするネットワーク プロトコルです。

  ポート番号：137（UDP）（ネームサービス）、138（UDP）（データグラムサービス）、139（TCP）（セッションサービス）

  詳細については、http://en.wikipedia.org/wiki/NetBIOS_over_TCP/IP を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- HTTP（Hypertext Transfer Protocol）

  Hypertext Transfer Protocol（HTTP）は、コラボレーション ハイパーメディア分散情報システム用のアプリケーション プロトコルです。

  ポート番号：80、8080（TCP）

  詳細については、http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol を参照してください。

影響：大

処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- HTTPS（Hypertext Transfer Protocol Secure）

  HTTPS は、コンピュータ ネットワーク上で安全に通信するための通信プロトコルであり、特にインターネット全体にわたって展開されています。

  ポート番号：443（TCP）

  詳細については、http://en.wikipedia.org/wiki/HTTP_Secure を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- Internet Message Access Protocol（IMAP）

  I nternet Message Access Protocol によって、電子メール クライアントはリモート メール サーバ上の電子メールにアクセスできます。

  ポート番号：143、993（TCP）

  詳細については、http://en.wikipedia.org/wiki/Internet_Message_Access_Protocol を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。

- POP3（Post Office Protocol）

  Post Office Protocol は、TCP/IP 接続を介してリモート サーバから電子メールを取得するために、電子メール クライアントによって使用されます。

  ポート番号：110、995（TCP）

  詳細については、http://en.wikipedia.org/wiki/Post_Office_Protocol を参照してください。

  影響：大

  処置：このサービスは、すべてのエンドユーザに対してアクセス可能にする必要があります。