Cisco Advanced Phishing Protection ユーザーガイド

初版：2022 年 12 月 19 日

シスコシステムズ合同会社

www.cisco.com/jp

シスコは、世界各国に 200 を超えるオフィスを開設しています。

各オフィスの住所、電話番号、FAX 番号は当社の Web サイト

（www.cisco.com/jp/go/offices）をご覧ください。

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1

ミッドタウン・タワー

www.cisco.com/jp

更新日：2022 年 12 月 16 日（金曜日）

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報と推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。ソフトウェアライセンスまたは限定保証書が見つからない場合は、CISCO 代理店に連絡してコピーを入手してください。

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルとソフトウェアは、障害も含めて「現状のまま」として提供されます。CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

データはすべて「現状のまま」提供され、CISCO, INC は、明示、黙示、法定を問わず一切の保証を行いません。これらの保証には、正確性、商品適格性、特定目的への適合性、非侵害性の黙示的保証、または履行の過程、取引の過程、使用もしくは取引から生じるあらゆる保証が含まれますが、これらに限定されません。また、CISCO, INC は、代替の物品の調達費用、または利益、データ、もしくはビジネスの損失、または特殊な損害、または間接的、付随的、懲罰的、もしくは結果的に生じる損害について一切の責任を負いません。

いかなる場合においても、CISCO およびその供給者は、このマニュアルの使用または使用不可によって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性が CISCO またはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスと電話番号は、実際のアドレスと電話番号を示すものではありません。マニュアル内の例、コマンド表示出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

目次

第 1 章

高度なフィッシング防御について

Cisco Advanced Phishing Protection では、外部から組織に届く電子メール、組織から外部に送信される電子メール、および組織内でやり取りされる電子メールに関して、これまでにないインサイトを得ることができます。組織への電子メールトラフィックの履歴に基づくCisco 独自の機械学習技術である Cisco アイデンティティ インテリジェンスにより有効になった、高度なフィッシング防御は、すべての正当な電子メール送信者の固有な動作をモデル化するため、正常なメッセージと不正の可能性があるメッセージをすばやく区別できます。アイデンティティ インテリジェンスと、世界中の数十億の電子メールメッセージの分析に基づいて構築された Cisco のデータプラットフォームを組み合わせることで、組織内のすべてのメッセージと、組織に電子メールを送信する送信者のリスクの概要を把握できます。

フィッシング試行、または悪意のあるペイロードや不審なリンクを含まないことがある「ビジネスメール詐欺（BEC）」メッセージなどの危険なメッセージは、既知の正常なメッセージから区別されます。

高度なフィッシング防御 は、従来の対処型のセキュア電子メールゲートウェイ（SEG）セキュリティ「層」において典型的な弱点であったスピアフィッシング、標的型、低ボリューム、およびゼロデイ攻撃を捕捉することで、SEG ソリューションを補完します。

高度なフィッシング防御内のポリシーエンジンを使用して、ほぼリアルタイムで、不正なメッセージに関してエンドユーザーに送信するアラートを設定できるとともに、潜在的に危険なメッセージをエンドユーザーの受信トレイから除外することもできます。

サービス規約

組織内のユーザーが高度なフィッシング防御を使用する場合は、事前に必ずCisco サービス規約（TOS）を確認して同意する必要があります。TOS は、次の 2 つの方法のいずれかで提示されます。

- ほとんどの組織の場合、高度なフィッシング防御に最初にログインするユーザーが初めてログインすると、TOS が表示されます。初めてログインしたときに TOS に同意する必要があります。
- マスター販売契約を結んでいる組織の場合、TOS の管理と同意は 高度なフィッシング防御アプリケーションの外部で Cisco 販売チームによって行われます。

はじめる前に

組織に高度なフィッシング防御を導入する準備ができたら、導入がスムーズに進むように、事前にいくつかのステップを実行する必要があります。このセクションでは、事前準備としてやっておくべきことを詳しく説明します。内容は次のとおりです。

- 重要なプロジェクトチームのメンバーの確認
- 重要な資料のレビュー
- 初期データの収集

重要なプロジェクトチームのメンバーの確認

高度なフィッシング防御の導入にあたっては、適切な人材が適切なロールを担っていることが重要です。

複数のロールを担う人もいれば、複数の人によって担われるロールもあります。

組織内で担うべきロールは次のとおりです。

- **エグゼクティブスポンサー**：重要な問題とプロジェクト障害のエスカレーション先として機能します。
- **プロジェクトオーナー**：このプロジェクトの全体的な成功に責任を持ちます。
- **プロジェクトマネージャ**：主要な連絡先であり、組織へのインターフェイスとなって、次の業務の責任を持ちます。
    - 合意したスケジュールに従ってプロジェクトが進行するようにする
    - 内部の他のグループや部門と連携する
- **導入エンジニア**：導入のエキスパートであり、プロジェクトの主要な技術連絡先です。
- **対象分野のエキスパート**：設計と統合へのインプットを提供する技術リーダーです。決定が組織のビジネス上の戦略に即していることを確認します。
- **メッセージングアーキテクト**
- **セキュリティアーキテクト**

重要な資料のレビュー

高度なフィッシング防御の根底にある概念と、高度なフィッシング防御が電子メールインフラストラクチャとどのように連携してやり取りするかを理解すると、高度なフィッシング防御の導入時に適切な決定を下せるようになります。事前に次の情報を確認してください。

- Cisco Advanced Phishing Protection ユーザーガイド

初期データの収集

電子メールインフラストラクチャに関する重要な詳細を 1 か所ですばやく参照できるようにすることをお勧めします。

- お使いの電子メールアーキテクチャはどのようになっていますか。環境に最適なセンサー配置を決定するためにエンドツーエンドのメールフローを示す図を作成してください。センサーは、基本的に SMTP の「メッセージシンク」として機能し、電子メールメッセージのコピーを SMTP で受信して、ストリーミング方式でメタデータを抽出します。メッセージ本文と添付ファイルは廃棄されます。SMTP メッセージはセンサーに残りません。
- センサーが組織によってホステッド型（優先）として配置されるかオンプレミス型として配置されるかを決定します。

- DKIM および SPF チェックを現在実行中ですか。実行していない場合、DKIM と SPF を有効にすることをお勧めします（これには、Cisco Domain Protection が便利です）。

これらの認証結果がないとデータ モデリングは調整に時間がかかり、より不完全になることに注意してください。

- センサーのインストール要件を確認します。
- 保護する重要なユーザーまたは重要なグループをキャプチャします。
- この準備作業ガイドを完了するときに、質問のメモを取り、サポートとの連絡をスケジュールするのに最適な時間を提供します。

第 2 章

高度なフィッシング防御の新機能

Cisco は、問題の修正から既存の機能の改善、新しい機能の追加まで、常に高度なフィッシング防御製品の改善に取り組んでいます。このセクションでは、高度なフィッシング防御の機能の変更について説明します。また、製品の機能に必ずしも関連しているわけではありませんが、ドキュメントの更新についても説明します。

リリース	日付	更新の詳細
2022.12	2022 年 12 月	• センサーの導入についてのハードウェアとソフトウェアの要件を更新しました。「「センサーの前提条件」 ページ 24」を参照してください。
2022.10	2022 年 10 月	• Graph API では、CDR の適用の制限は 10,000 です。同じことを示すために、「ドメイン固有の言語リファレンス」と「オンデマンドポリシーを作成する」を更新しました。「「ドメイン固有の言語リファレンス」 ページ 142」、「「オンデマンドポリシーを作成する」 ページ 165」を参照してください。 • Graph 適用が有効になっている場合、「センサー」ページの適用ステータスは使用できません。同じことを示すように「センサー」ページを更新しました。「「適用センサーステータス」 ページ 102」、「「センサーのステータスを表示する」 ページ 44」を参照してください。 • Rapid DMARC ポリシーの信頼スコアが 0 ～ 10 の範囲になり、Rapid DMARC ポリシーが新しい画像と詳細で更新されました。「「Rapid DMARC を使用した送信者管理」 ページ 187」を参照してください。
2022.08	2022 年 8 月	• 「組織設定」の更新、[Microsoft API権限（Microsoft API Permissions）] タブのドキュメント化、取り込みや適用を無効化する新しい機能。「「組織設定」 ページ 197」を参照してください。 • 「適用の設定：Office 365」を更新しました。Office 365 は、適用に MS Graph API のみを使用します。「「適用の設定：MS Graph API を使用した Office 365」 ページ 89」を参照してください。
2022.07	2022 年 7 月	• 「ドメインタグ」を更新して、新しいドメインタグ機能（トラフィックを含むドメインとタグのあるすべてのドメイン）を反映させました。「「ドメインタグ」 ページ 133」を参照してください。
2022.06	2022 年 6 月	• 「「継続的な検出および応答」 ページ 136」の画像を更新しました。
2022.04	2022 年 4 月	• マイナーな編集と修正。
2022.02	2022 年 2 月	• 現在のアプリケーション UI に一致するようにすべての画像を更新しました。
2022.01	2022 年 1 月	• Cisco CES/ESA BCC 設定を更新して、古い「Tomki」スクリーンショットを削除しました。「「デュアル配信の設定：Cisco ESA」 ページ 67」を参照してください。 • 検索、リアルタイムポリシー、および CDR での部分一致やワイルドカード照合を説明する注記を追加しました。「「添付ファイルと URI の分析」 ページ 180」を参照してください。

リリース	日付	更新の詳細
		• アラートサーバーをホワイトリストに登録する手順を更新しました。「「デュアル配信の設定：Office 365」 ページ 54」を参照してください。
2021.10	2021 年 10 月	• URL のブロックに関する更新を行い、新しい URL の調整機能を反映しました。「「スコアリング調整」 ページ 118」を参照してください。
2021.03	2021 年 3 月	• 新しい CDR イベントの保留状態を追加しました。「「継続的な検出および応答イベントの状態を変更する」 ページ 140」を参照してください。 • MS Graph API のサポートと機能を追加しました。「「適用の設定：MS Graph API を使用した Office 365」 ページ 89」を参照してください。
2020.12	2020 年 12 月	• 適用ボタンの動作を更新しました。「「ポリシーを作成する」 ページ 156」を参照してください。
2020.10	2020 年 10 月	• マイナーアップデートとバグの修正
2020.09	2020 年 9 月	• 信頼スコアの調整機能のフェーズ 1 が追加され、ドキュメント化されました。「「スコアリング調整」 ページ 118」を参照してください。 • Microsoft Exchange でのアップグレード後にセンサーを再起動する手順を追加しました。「「適用の設定：Microsoft Exchange」 ページ 99」を参照してください。
2020.08	2020 年 8 月	• CDR ルール DSL 構文の説明を更新し、同じフィールド演算子の組み合わせの複数の使用が AND で結合された場合にエラーを返す新しい制限を反映させました。「「ドメイン固有の言語リファレンス」 ページ 142」を参照してください。 • センサーのインストールスクリプトに必要な URL のリストを更新しました。「「センサーの前提条件」 ページ 24」を参照してください。
2020.07	2020 年 7 月	• センサー診断ファイルのダウンロードは、オンプレミスセンサーでのみ使用でき、ホステッド型センサーでは使用できません。「「センサー診断情報をダウンロードする」 ページ 45」の注記を参照してください。 • 「「継続的な検出および応答ルール」 ページ 141」の可能性のあるメッセージの SPF 結果のリストに [永続的なエラー（Permanent Error）] を追加しました。 • Agari の送信コネクタの Microsoft Exchange の最大メッセージサイズを 100MB に増やすことを推奨する注記を追加しました。「「デュアル配信の設定：Microsoft Exchange」 ページ 59」を参照してください。
2020.06	2020 年 6 月	• 継続的な検出および応答（CDR）ルールを作成するために使用できる検索言語に大幅な変更が加えられました。詳細については、「「ドメイン固有の言語リファレンス」 ページ 142」を参照してください。 • 継続的な検出および応答（CDR）についてのカスタムローカルルールの作成機能が追加されました。「「継続的な検出および応答ルール」 ページ 141」を参照してください。
2020.04	2020 年 4 月	• （CDR）ルールが追加されました。「「継続的な検出および応答ルール」 ページ 141」を参照してください。
2020.03	2020 年 3 月	• メッセージの詳細では、メッセージのスコアと攻撃の分類がどのように決定されたかについて分析情報を確認できるようになりました。「「攻撃の分類」 ページ 109」には、さまざまな攻撃タイプの詳細が示されています。
2020.02	2020 年 2 月	• ジャーナリングトピックの電子メールアドレスに、高度なフィッシング防御に関連する不正なドメインが含まれていました。この問題は修正されました。 • メッセージが評価されないように例外の処理を定義できるようになりました。詳細については、「「組織設定」 ページ 197」を参照してください。

リリース	日付	更新の詳細
2020.01	2020 年 1 月	• 検索結果から作成されたオンデマンドポリシーは、受信メッセージにのみ適用できることを明確にしました。これは、内部関係者偽装が有効になっていて、受信、送信、および内部メッセージがセンサーによって取り込まれている場合に関連するものです。詳細については、「「オンデマンドポリシーを作成する」 ページ 165」を参照してください。
2019.12	2019 年 12 月	• G Suite のメールルーティング設定を明確にしました。「「デュアル配信の設定：G Suite」 ページ 48」を参照してください。 • Azuru Active Directory アドレスグループの同期でスキップされるアドレスに関する項を追加しました。「「Azure Active Directory のアドレスグループとの同期」 ページ 194」を参照してください。 • 組織の設定にある［センサー設定（Sensor Settings）］セクションの［許可された転送 IP（Allowed Forwarding IPs）］の設定に関する情報を追加しました。「「組織設定」 ページ 197」を参照してください。
2019.11	2019 年 11 月	• センサーの要件を更新しました。オンプレミスセンサーでは Python 2.7 以降が必要になりました。 • センサー設定の名称を修正しました。
2019.10	2019 年 10 月	• このガイドでは、いくつかの箇所で「グローバル管理者」を使用していましたが、これは高度なフィッシング防御がシステムにアクセスするためにロールが必要であるという誤解をユーザーに与えるものでした。実際には、特定のアクセス権限が必要になるのは、それらのシステムが高度なフィッシング防御によるアクセスを許可するように設定するためだけです。これをより正確に表すために、それらの箇所の内容が変更されました。 • Google は用語を変更し、「Google Developers Console」と表記しなくなりました。G Suite での適用を設定するためのトピックを、Google の新しい名称を反映するように更新しました。 • Cisco の従業員が高度なフィッシング防御ユーザーアカウントに変更を加えることができないことを明確にしました。「「ユーザーアカウント」 ページ 206」を参照してください。 • 高度なフィッシング防御のプレーンテキスト検索フィールドは 100 文字に制限されるようになりました。
2019.09	2019 年 9 月	高度なフィッシング防御は内部関係者偽装防止（IIP）を追加し、受信メッセージ、送信メッセージ、および内部メッセージの全方向でのメールストリームの監視を提供するようになりました。 IIP では Microsoft 365 または Exchange を電子メールプロバイダーとして使用する必要があり、また、次を行う必要があります。 • 組織の設定でこの機能を明示的に有効にします。詳細については、「「メッセージ設定」 ページ 198」を参照してください。 • すべてのメッセージに適切な方向性のヘッダーが追加されていることを確認します。詳細については「「デュアル配信の設定：Office 365」 ページ 54」と「「デュアル配信の設定：Microsoft Exchange」 ページ 59」を参照してください。 メッセージの方向性も検索およびポリシーの条件に使用できます。詳細については、「「メッセージ検索」 ページ 127」と「「ポリシー設定」 ページ 157」を参照してください。

リリース	日付	更新の詳細
2019.08	2019 年 8 月	• メッセージ検索とポリシー設定では、上限と下限を設定する数値のパラメータの場合、その上限値と下限値が含まれるようになりました。
2019.07	2019 年 7 月	• 値を明確にするように攻撃対ピア適用グラフを拡張しました。「「ピアと比較した場合の攻撃/保護の程度レポート」 ページ 177」参照してください。 • 高度なフィッシング防御を使用するための準備(「「はじめる前に」 ページ 11」を参照してください)と高度なフィッシング防御APIドキュメントへのアクセス方法(「「アプリケーション プログラミング インターフェイス」 ページ 214」を参照してください)に関する情報をこのガイドに追加しました。 • デフォルトポリシーに関する詳細をこのガイドに追加しました。「「デフォルトポリシー」 ページ 154」を参照してください。
2019.06	2019 年 6 月	• 高度なフィッシング防御によるインラインアーキテクチャでのセンサーの正式なサポートは終了したため、このガイドから情報を削除しました。 • メッセージ検索の参照コンテンツを追加しました。詳細については、「「メッセージ検索」 ページ 127」を参照してください。 • メッセージの検索結果をダウンロードできるようになりました。詳細については、「「メッセージの検索結果をダウンロードする」 ページ 130」を参照してください。
2019.05	2019 年 5 月	ガイドのこのバージョンでの変更は、修正、明確化、他のシステムが変更されたことによる更新、およびバグ修正がほとんどです。
2019.04	2019 年 4 月	• このガイドでは、レポートの値を変更できるユーザーを明確にしています。詳細については、「「高度なフィッシング防御の導入による節約量のレポートを設定する」 ページ 175」を参照してください。 • 内部タグおよびパートナータグの使用方法と、それらをドメインに適用するためのベストプラクティスに関する追加情報を「ドメインタグ」のトピックに追加しました。詳細については、「「ドメインタグ」 ページ 133」を参照してください。
2019.03	2019 年 3 月	• 脅威トレンドとエグゼクティブ サマリー レポートのカスタムの日付範囲を設定できるようになりました。 • センサーポートの要件およびサポートされているセンサーアーキテクチャについての説明を追加しました • 追加の組織設定は、組織の分類方法で使用できます。これらの地域、業種、組織の規模などの分類は、エグゼクティブ サマリー レポートの 1 つに使用されます。「「高度なフィッシング防御 の導入による節約量のレポート」 ページ 174」を参照してください。

リリース	日付	更新の詳細
2019.01	2019 年冬	• レポートの改善 新しい一連のレポートは、ホームページの [脅威トレンド（Threat Trends）] タブと [エグゼクティブサマリー（Executive Summary）] タブで利用できます。これらのレポートは高度なフィッシング防御を使用することの利点がひと目でわかるように表示されます。これらのレポートには、高度なフィッシング防御が提供する値が毎日更新されて表示されます。また、いずれのページのスナップショットも Adobe Acrobat（PDF）ファイルとしてダウンロードできます。組織の追加設定によって、レポート内のメッセージデータをカスタマイズできます。詳細については、「「脅威トレンドレポート」 ページ 170」と「「エグゼクティブ サマリー レポート」 ページ 172」をご覧ください。 • メッセージのフィードバックの改善 高度なフィッシング防御によって、個別のメッセージに関するフィードバックを送信するときに、詳細情報を提供できるようになりました。詳細については、「「メッセージのフィードバックを送信する」 ページ 126」を参照してください。

第 3 章

センサー

Cisco 高度なフィッシング防御 は、組織にインバウンドで送信されたすべてのメッセージのコピーを受信するためにセンサーを使用しています。センサーの設置は、高度なフィッシング防御の価値を実現するための最初の重要なステップです。

センサーの目的は、組織の受信電子メールストリームからメッセージごとの情報を収集し、その情報を分析のために高度なフィッシング防御クラウドにリレーすることです。この情報に以下が含まれています。

- メッセージのメタデータ
- 添付ファイル（有効な場合）
- URL（有効な場合）

センサーは安全で軽量（必要なリソースは最小限）で、最適化され、高い性能を実現しています。これは、悪意のあるメッセージを適用する上で重要な役割を果たします。

センサーは、最大 100 MB のサイズのメッセージを受け入れることができます。添付ファイルのスキャンを有効にしている場合（「「添付ファイルと URI の分析」 ページ 180」を参照してください）、メッセージと添付ファイルの合計サイズは、センサーがメッセージを受け入れるために、エンコードに必要なオーバーヘッドを含めて 100 MB を超えてはなりません。

インフラストラクチャへのセンサーの配置

センサーを配置する場所については、2 つの基本的な選択肢があります。

- センサーを実行する独自の環境にホストシステムをプロビジョニングできます。通常、効率を高めるためにセンサーをメールストアの近くに配置する必要があるため、この設定は独自の Exchange サーバーも実行している場合にのみ推奨されます。ただし、更新が利用可能な場合はセンサーのインスタンスを明示的に更新し、メールの負荷が増加した場合は手動でセンサーを追加する必要もあります。
- 管理上独立した、安全なクラウドで Cisco に自身のセンサーをホストさせることもできます。これは、Office 365 や G Suite などのクラウドサービスを使用している場合に推奨される設定です。ホステッド型センサーは Cisco によって必要に応じて更新されるだけでなく、ホステッド型センサーの容量も必要に応じて Cisco によって拡張されます（Cisco ホステッド型センサーの詳細については、Cisco のセールスエンジニアにお問い合わせください）。

独自のセンサーをプロビジョニングする場合、メッセージに対して他のスキャン（スパム対策、ウイルス対策、マルウェア対策）が行われた後に、内部的に配信されたメッセージのコピーを受信できるインフラストラクチャ内に接続して統合する必要があります。高度なフィッシング防御のセンサーは、これらのフィルタを通過し、配信する価値があると見なされるメッセージを「確認」するだけです。

ホストされた電子メールインフラストラクチャ（Google Apps や Microsoft Office 365 など）がある場合は、同じ理論が適用されます。つまり、電子メールストリームのコピーは、他のすべてのフィルタリングおよびスキャンが行われた後に、高度なフィッシング防御センサーに送信されます。

Cisco は以下の、デュアル配信として設定され、Cisco ホステッド型またはオンプレミスとして導入されたセンサーをサポートしています。

デュアル配信センサー	
Cisco ホステッド型（推奨）	Cisco によって管理されたセンサーの拡張と更新における堅牢性を備えた、最高のパフォーマンスのデュアル配信オプションを提供します。この組み合わせが推奨されるオプションです。
オンプレミス	最高のパフォーマンスのデュアル配信オプションを提供しますが、センサーとセンサーのホストの更新はお客様が実行します。通常、セキュリティルールにより、電子メールトラフィックが電子メールインフラストラクチャの外部に送信されないようにする場合に使用されます。

オンプレミスのセンサーでは、ベアメタルマシンを設定して使用するか、仮想マシンでセンサーソフトウェアを実行できます。後者の場合、仮想マシンを手動で設定するか、事前設定済みの仮想マシンパッケージをダウンロードできます。

オンプレミスのセンサーをベアメタルまたは独自の仮想マシンで実行する場合、すべてのセンサーの操作はコマンドラインを介して実行されるため、セキュアシェル（SSH）からマシンにアクセスする必要があります。事前設定済みの仮想マシンパッケージを使用すると、文字ベースのフロントエンドでセンサー情報とその制御コマンドに簡単にアクセスできます。

IP アドレス、NTP、DNS、およびパスワードを含むセンサーの初期設定は、ssh 経由でセンサーにアクセスする前に、VMWare コンソール経由で VMWare 管理者によって実行されます。

センサーの計画

センサーのインストール方法と設定方法は、次のような多くの考慮事項によって決まります。

- メールインフラストラクチャ
- ホステッド環境
- 配置

メールインフラストラクチャ

メールインフラストラクチャは、センサーのインストールタイプを決定するのに役立ちます。いくつかの基本的な質問が、インストールの種類を決定するために役立つことがあります。

MX 配信の場所

組織の MX レコードは、組織のドメインに関する一般公開された MX レコードです。MX レコードは、次を示している場合があります。

- SEG：Cisco ESA などのセキュアな電子メールゲートウェイ
- Office 365：Microsoft のホステッド ソリューション

- Google：Google のホステッド ソリューション

最初の受信電子メールのプラットフォームホップとは

一部の顧客は、「階層型」環境を保持しています。その場合、内部「ホップ」が MX レコード環境のアドレスから 2 番目のゲートウェイに電子メールをルーティングします。たとえば、この「ネクスト ホップ」は次である場合があります。

- Google（G Suite）
- Office 365（O365）
- Exchange オンプレミス（on-prem）
- 複数のサイトのいずれかで条件付きで、それぞれが Exchange on-prem を備える

すべてのユーザーメールボックスのメールボックス配信の場所

メールボックス配信（エンドユーザーのメールボックスが保存されている場所）が、別の「ホップ」を必要とすることがあるかどうか。たとえば、この質問への回答として次が考えられます。

- 最初の電子メール プラットフォーム ホップと同じ環境（上記の質問 2）
- ハイブリッド環境全体にわたる（Office 365 または Exchange on-prem のいずれか）
- どのメールボックスに依存しているか（部分的なメールボックス移行を伴うハイブリッド）

一部の顧客は、ハイブリッド環境を保持しています。その場合、一部のメールボックスがオンプレミス環境からホステッド環境に移行されつつあります。

ホステッド環境

さらに、環境が G Suite または Office 365 でホストされている場合は、次の質問が、センサーのインストール戦略を決定するために役立ちます。

Office 365 と Exchange オンプレミスの両方を備えたハイブリッド環境であるか

ハイブリッド環境では、ユーザーメールボックスを Exchange オンプレミスから Office 365 に移行できます。

ハイブリッド環境である場合、Office 365 へのユーザーメールボックスの移行は現在どのような状態であるか

メールボックスの移行には、3 つのフェーズと関連付けられたタイムラインがあります。

- 移行前：すべてのメールボックスが引き続き Exchange on-prem 上にあります
- 部分的な移行：一部のメールボックスが O365 に移動され、その他は引き続き Exchange on-prem 上にあります
- 移行後：すべてのメールボックスが O365 上にあります

次を実現するために、クライアントがどのタイミングで、すべてのユーザーメールボックスを Office 365 上で保持するかを把握することが重要です。

- できる限り早くすべての高度なフィッシング防御機能を使用する能力を最大化する。
- インストールの移行に伴う変更要求と関連するリスクを最小化する。

センサーの導入

センサーの導入は、オンデマンド適用（Office 365 および G Suite 顧客の場合）が可能で、クライアントの変更管理に起因するリスクが軽減されることからデュアル配信になっています。

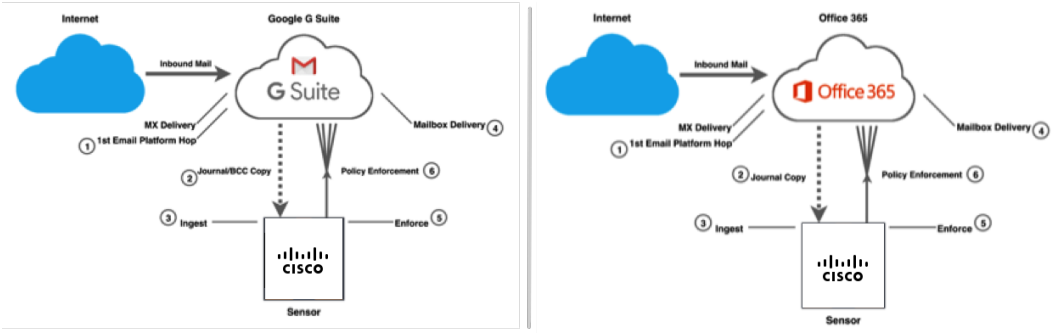
デュアル配信

センサーは、基本的に SMTP の「メッセージシンク」として機能します。SMTP 経由で電子メールメッセージのコピーを受け入れ、以下の攻撃分析に必要なメッセージの一部をストリーミング形式で抽出します。

- メッセージのメタデータ
- 添付ファイル（有効な場合）
- URL（有効な場合）

メッセージ本文は廃棄されます。SMTP メッセージはセンサーに残りません。

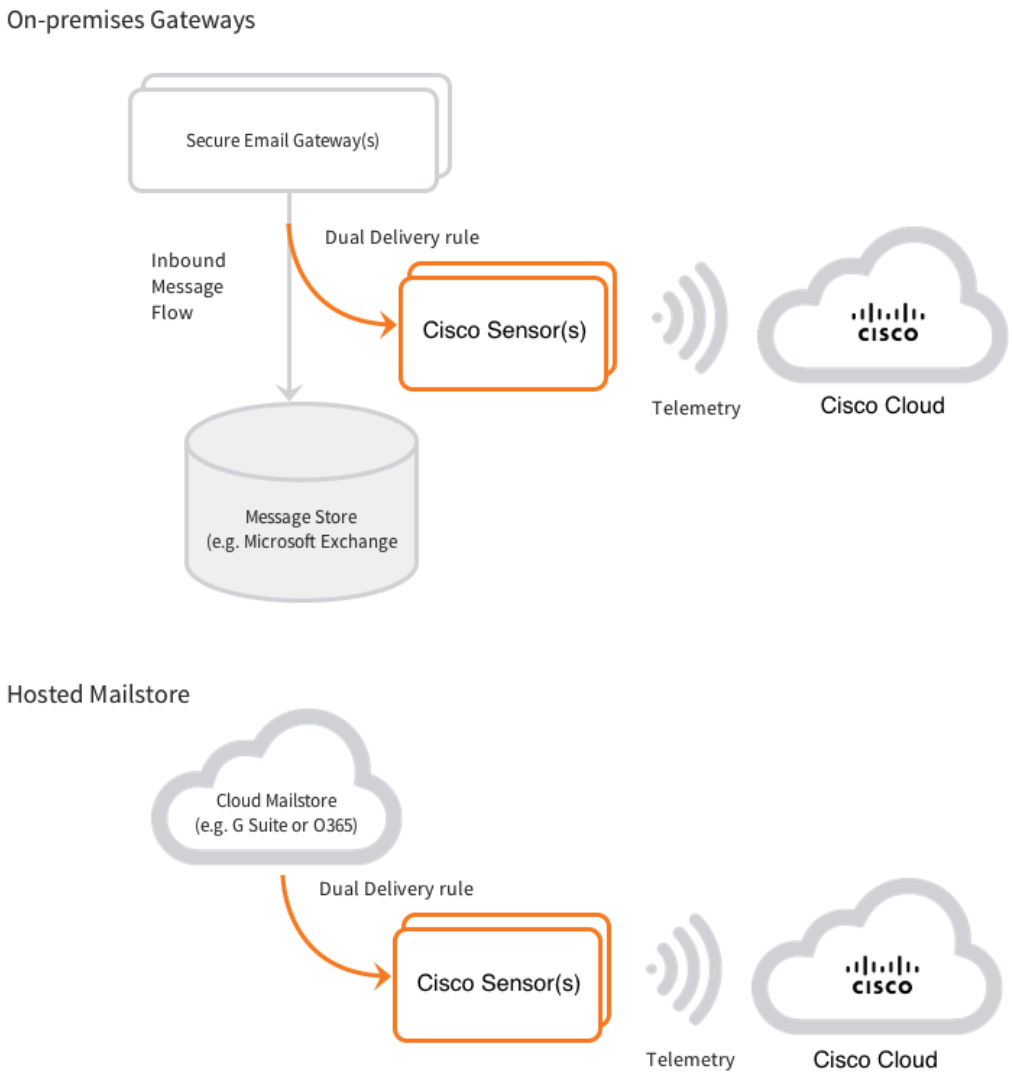
デュアル配信は通常、Office365 や G Suite などのホステッド電子メールアーキテクチャで使用されます。



ジャーナリング/API メールフローを使用したデュアル配信インストール

1. 最初の電子メールのプラットフォームホップに送信される受信メールです（SEG が前面にある場合とそうでない場合があります）。これにより、スパム、ウイルス、およびその他の不要なメッセージが除外されます。
2. Office 365 または G Suite は、ジャーナルされたコピーまたは bcc: コピーをセンサーに送信し、元の配信を続行します。
3. センサーは、ジャーナルコピーを取り込み、得点を付け、ポリシーを評価します。
4. Office 365 または G Suite は、元のメッセージをメールボックスへ配信します。
5. センサーは個々のメールボックスにアクセスするために、API を使用してポリシーを適用します。
6. ポリシーの適用アクションは、ポリシーの結果に基づいてメールボックスで発生します。

デュアル配信センサーのアーキテクチャとデータフロー



デュアル配信センサーのアーキテクチャ

ステップ 1

メッセージは、顧客のセキュアな電子メールゲートウェイ（SEG）またはホストされているメールストアに到着し、スパムおよびウイルスのフィルタリング用に受け入れられます。

ステップ 2

最初のレベルのスパムおよびウイルスのフィルタリングの後、顧客の SEG は、通常はポート 25（Cisco センサーがインストールされている場合、異なるポートに設定されていることがあります）で SMTP 接続を経由して、メッセージのコピー（デュアル配信ルールまたはジャーナリング機能を介して）を Cisco センサーへ配信します。Cisco milter プロセスが、得点付けとポリシー評価のために Cisco パイプラインへ送信されるメッセージデータを解析している間、受信メッセージはキューに入れられます。

解析された電子メールメッセージのデータは、ポート 443 を使用して HTTPS 接続経由で Cisco パイプラインへ送信されます。

センサーの前提条件

オンプレミス導入では、ベアメタルインストールまたはホステッド仮想マシン（VM）でセンサーをインストールできます。仮想マシンを使用する場合は、このガイドの指示に従って自身で設定するか、事前にパッケージ化され、事前設定済みの仮想マシンのディスクイメージをダウンロードできます。

ベアメタルインストールまたは独自の仮想マシンの場合、高度なフィッシング防御センサーは、組織に固有のキーを持つインストールスクリプトを介して Cisco によって配布されます。インストールスクリプトが、Docker コンテナを介して配布されたセンサーアプリケーションをインストールします。このコンテナは、アプリケーションを実行するために必要なすべてのもの（コード、ランタイム、システムツール、およびシステムライブラリ）を含んでいる完全なファイルシステムで、センサーアプリケーションをラップします。

事前にパッケージ化され、事前設定済みの仮想マシンのディスクイメージの場合は、OVA ファイルを高度なフィッシング防御内からダウンロードし、サポートされている仮想化ソフトウェアにインポートできます。

最初のセンサーをインストールするためのスクリプトは、Cisco のセールス担当者から取得する必要があります。Web アプリケーションへのアクセスを取得後、[管理（Manage）] > [センサー（Sensors）] ページから追加のセンサーをインストールするためのスクリプトを取得できます。このスクリプトには、組織に固有のキーが設定されています。

ハードウェアおよびソフトウェアの要件

ベアメタルや独自の仮想マシンでインストールする場合は、マシンまたはマシンインスタンスは次の最小要件を満たしている必要があります。仮想マシンのディスクイメージを使用している場合は、これらの要件に合わせて事前設定済みです。そして、これらの要件を満たすハードウェアで仮想化ソフトウェアを実行する必要があります。

システム	要件
CPU	Intel または AMD x 86_64、8 コア
メモリ	32GB
ディスク	最小割り当ては次のとおりです。 • /var/opt/agari/：100GB • /opt/agari/：20GB • /var/lib/docker：20GB
オペレーティング システム	最新の 64 ビット Linux： • Red Hat Enterprise Linux 7.x • CentOS 7.x • Ubuntu 16 から 20
Docker	17.06 以降
パッケージ	Python 2.7、および $PATH 環境変数に追加 Ubuntu 20：python-is-python2
ネットワーク	1 Gbit/秒を推奨
ハイパーバイザ	VMWare ESXi

ファイアウォールの要件

センサーをインフラストラクチャにインストールする場合は、Cisco Cloud と通信できなければなりません。センサーに対するファイアウォールの要件の一覧を次に示します。

ポート要件	定義
インバウンド：25（SMTP）	ゲートウェイから受信した重複メッセージのストリームを受信する場合。 このポートは、ファイアウォールで分離された Exchange サーバーとは別のネットワークにセンサーが存在する設定で開く必要があります。
アウトバウンド：443（HTTP/S）	Cisco Cloud およびその他のクラウドサービスへの HTTP/S リクエスト（詳細は下記を参照してください）。 センサーは、送信 HTTP/S 接続にプロキシを使用するように設定されていることがあります。
送信：53（DNS）	ホスト名/IP アドレス解決のための DNS。 ホストシステムが DNS 解決に 127.0.* または localhost を使用している場合、Docker はそれをコンテナの /etc/resolv.conf ファイルに複製しません。代わりに、DNS を 8.8.8.8 および 8.8.4.4 に設定します。ファイアウォールを介してこれらのアドレスを使用できない場合、DNS に問題が生じます。 ホストの DNS サーバーを企業内で使用されている内部 DNS サーバーの実際のアドレスに設定する必要が生じることがあります。
送信：123（NTP）	時間同期サービス用の NTP。注：RedHat システムでは、次のコマンドを実行することで、NTP が正しく動作していることを確認できます。 ntpstat echo $? NTP サーバーにアクセスしている場合、最後のコマンドの出力を 0 にする必要があります。NTP のステータスの確認の詳細については、RedHat に関するドキュメントを参照してください。 https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/s1-Checking_the_Status_of_NTP.html

ファイアウォールルール：必要な HTTPS アクセス

インストールスクリプトを実行するシステムは、次のエンドポイントにアクセスできる必要があります。

https://sensor-provisioner.ep.prod.agari.com

https://agari-ep-collector-config-prod.s3.amazonaws.com

https://agari-ep-collector-config-prod.s3.us-west-2.amazonaws.com

https://agari-ep-collector-ingest-avro.s3.amazonaws.com

https://agari-ep-collector-ingest-avro.s3.us-west-2.amazonaws.com

https://agari-ep-collector-milter.s3.amazonaws.com

https://agari-ep-collector-milter.s3.us-west-2.amazonaws.com

https://kinesis.us-west-2.amazonaws.com

https://publicsuffix.org

https://registry-cdn.ep.agari.com

https://registry.ep.agari.com

https://s3-r-w.us-west-2.amazonaws.com

https://sns.us-west-2.amazonaws.com

https://us-west-2.queue.amazonaws.com

https://sqs.us-west-2.amazonaws.com/

Docker のインストール

以下の Docker に関するドキュメントには、Cisco がセンサーの実行をサポートしている Linux バージョンで Docker をインストールする手順が記載されています。

- Red Hat：https://docs.docker.com/install/linux/docker-ee/rhel/ [英語]（Docker EE）
- CentOS：https://docs.docker.com/install/linux/docker-ee/centos/ [英語]（Docker EE）または https://docs.docker.com/install/linux/docker-ce/centos/[英語]（Docker CE）
- Ubuntu：https://docs.docker.com/install/linux/docker-ee/ubuntu/ [英語]（Docker EE）または https://docs.docker.com/install/linux/docker-ce/ubuntu/ [英語]（Docker CE）

パッケージ

Linux ディストリビューションを変更する場合は、インストール スクリプトとセンサーに必要なパッケージ、またはこれらと互換性がないパッケージを認識している必要があります。

Postfix

一部の Linux ディストリビューションでは、Postfix サーバーがデフォルトで有効になっています。デフォルトの Postfix サーバーが稼働している場合、センサーのインストール スクリプトを実行する前に、それを無効にする必要があります（センサーはメッセージを受信するために、独自のカスタマイズされたバージョンの Postfix サーバーをインストールします）。

次のコマンドを実行して、Postfix サーバーを無効にして削除します。

```
# sudo yum remove postfix
```

センサーのインストール

センサーをインストールする方法は以下の中から選ぶことができます。

- Cisco から取得したスクリプトを使用して、ベアメタルまたは独自の仮想マシンにセンサーをインストールします。「「スクリプトでセンサーをインストールする」 次のページ）」を参照してください。
- ダウンロード可能な、事前にパッケージ化されて事前設定済みの仮想マシンのディスクイメージ（OVA）でセンサーをインストールします。「「OVA でセンサーをインストールする」 ページ 33」を参照してください。

追加のセンサーのインストール

個々のメッセージのメタデータに加えて、有効になっている場合は抽出された添付ファイルと URL のみを評価し、メッセージ本文は破棄するため、Cisco のセンサーは非常に効率的です。メールストアや電子メールゲートウェイから複製させる予定の受信メッセージ数に基づいて、冗長性またはスループットの向上のいずれかを目的に追加のセンサーを設定できます。

必要なセンサー数

単一のセンサーは、添付ファイルと URL の分析が有効な場合は約 1.6MB/秒（メガバイト/秒）、添付ファイルと URL の分析が無効な場合は約 20MB/秒のスループットを維持できます。少なくとも非ホスト型センサーの場合は実稼動環境で冗長性を確保するために、負荷分散されたデュアルセンサー設定を強く推奨します。

自身で管理している場合に必要なセンサー数を決定するには、処理するメッセージの数とそれらのメッセージの平均サイズに関するデータを収集する必要があります。脅威トレンドレポート（「「脅威トレンドレポート」 ページ 170」を参照してください）には、1 日あたりに処理されたメッセージの数が表示されます。

あとは計算するだけです。（計算を簡単にするために）1 日あたり 864,000 件のメッセージを処理するとします。平均すると、1 秒あたり 10 件です。そして、メッセージの平均サイズが 100KB だとすると、1MB/秒で処理することになります。添付ファイルと URL の分析を有効にしている場合、センサーは約 1.6MB/秒、つまり 1 秒あたり約 16 件のメッセージを処理できます。

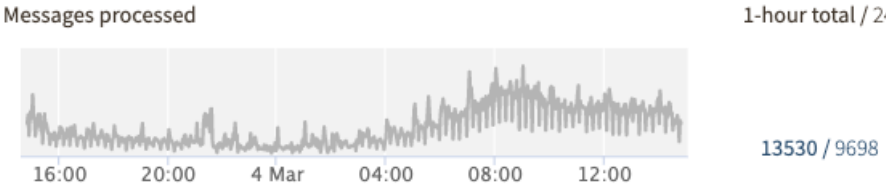
いくつかの例を紹介します。

センサーごとのおおよそのメッセージ処理率。

平均メッセージサイズ、センサーごとのメッセージ処理率、添付ファイルと URL の分析		
	有効	無効
100KB	16 件のメッセージ/秒	200 件のメッセージ/秒
150KB	11 件のメッセージ/秒	133.3 件のメッセージ/秒
250KB	6 件のメッセージ/秒	80 件のメッセージ/秒
1MB	1.6 件のメッセージ/秒	20 件のメッセージ/秒

これはセンサーごとの最大持続容量であることに注意してください。メッセージの急増と冗長性の両方に十分に対応できるように、センサーをプロビジョニングする必要があります。これらの制限は電子メールトラフィックの短時間の急増に対応できますが、これらの制限を超える持続的なピークには対応できません。

もちろん、メッセージは一日中同じ速度で処理されるわけではありません。多くの組織では、夜明け前よりも日中に受信するメッセージの方が多くなっています。24 時間の間にセンサーが受信したメッセージの例を次に示します。



24 時間の間に 1 つのセンサーによって処理されたメッセージの例。

この例からわかるように、短時間のトラフィックの急増は 1 日中ランダムな時間に発生しますが、持続的なピークは午前の中頃に発生します。したがって、必要なセンサー数、またはセンサーをいつ追加するかを検討する際には、次の点にも留意してください。

- ピーク時に受信したメッセージの数。
- 一時的な急増時に受信する可能性のあるメッセージの数。
- 提供するヘッドルームまたはバッファの量。

たとえば、平均メッセージサイズに基づいて考えると、センサーは 1 日を通して 1 時間あたり 10,000 件のメッセージを処理すると予想できます。ですが、正午から午後 3 時までは 1 時間あたり 25,000 件、午前 0 時から午前 3 時までは 1 時間あたり 1,500 件のメッセージを処理すると予想されます。この場合、午後のピーク時における、1 時間あたり 25,000 件のメッセージを処理するのに十分なセンサーが必要です。

もちろん、これらの数値は非常に大まかな見積もりです。センサーを監視して、センサーがどれだけ容量に近づいているかを確認する必要があります。

センサーが容量に達すると、メッセージをバッファし、そのバッファ内のメッセージを最大限のスループットで処理します。メッセージは破棄されませんが、脅威検出と適用が若干遅れる可能性があります。

スクリプトでセンサーをインストールする

最初のセンサーのインストールスクリプトは、Cisco のセールスエンジニアリング担当者から取得します。スクリプトには、次のような名前が付いています。

sensor-install-<orgname>-<date>.sh

スクリプトを受け取ったらすぐに実行する必要があります。時間が経ってからインストールを試みると、古いバージョンのセンサー インストール スクリプトのためにエラーが発生することがあります。疑わしい場合は、受け取ったセンサーのインストールスクリプトが最新バージョンであるかを確認します。

ファイルの名前は変更できます。

ホスト システムへファイルを移動します（たとえば、SCP 経由）。場合によっては、ファイルを移動した後に、スクリプトを実行できるように権限を設定する必要が生じることがあります。次に例を示します。

```
# chmod +x sensor-install-examplecom-2018-02-01.sh
```

「「センサーの前提条件」ページ 24」で説明されている前提条件に加えて、センサーのインストールスクリプトを実行する前に、次の項目を順番に確認してください。

プロビジョニング済みの Linux マシンでルートへアクセスできますか。

ファイアウォールは、Cisco Cloud およびインストールリポジトリへの DNS、NTP、SMTP（インバウンド）、HTTP/S アクセスを許可するように設定されていますか。

プロキシ：HTTP トラフィックのプロキシを使用している場合、プロキシの種類（HTTP または NTLMO）、ホスト名、ポート、ユーザー名、およびパスワードは利用可能ですか。

TLS トラフィック：インストール時に、センサーへのインバウンド トラフィックを、TLS 経由で配信するように設定できます。センサーへの TLS 経由の SMTP 配信を使用予定の場合、秘密キー（.key ファイル）、署名付き TLS 証明書（.pem ファイル）、および証明書チェーン（.pem ファイル）を持っていますか。

スクリプトの実行

前提条件と依存関係をすべて考慮したら、インストール スクリプトを実行できます。

スクリプトは次の段階で構成されています。

1. スクリプトのバージョンを印刷する
2. /opt/agari および /var/opt/agari/etc ディレクトリを作成する
3. 既存の Cisco センサーサービスを停止する（必要な場合）
4. インストールファイルを一時ディレクトリに解凍する
5. Docker をインストールする
6. PyYAML をインストールする（必要な場合）
7. AWS ツール（AWS、AWS SSL）をインストールする
8. ログとコンフィギュレーション ファイル（オプション。デフォルトではルートグループが使用される）に対する追加の UNIX グループ権限を要求する
9. HTTPS プロキシ設定を要求する（オプション）
10. データをアップロードするための正しい S3 バケットへのアクセスをテストする
11. センサーへの接続（デフォルトでは OFF – TLS 接続が必須）用の TLS 証明書と TLS 設定を要求する
12. デバッグレベルのログ出力（デフォルトではオフ）を要求する
13. ファイルを適切なディレクトリに移動し、一時ファイルを削除する
14. センサーのバージョンをアップグレードする（必要な場合）

Linux Ubuntu イメージで実行されているスクリプトの例を以下に示します。次の例では、以下の点に注意してください。

- インストール スクリプトの出力は同一ではありません。以下のテキストは、例として提供されています。
- 組織 ID は一意です。
- アクセス キー ID は AWS へのアクセス用です。
- Docker と AWS ツールがホスト システム上に存在しない場合は、それらがインストールされます。
- ログと設定データへアクセスするための、UNIX グループ権限を指定できます。
- HTTPS プロキシを指定するオプションがあります。
- センサーへの SMTP 接続に使用する TLS 証明書を指定できます。
- デバッグ レベルのロギングを指定できます。

実行中のセンサースクリプトの例:

スクリプトのバージョン番号 Cisco ディレクトリを作成する	$ sudo ./sensor-install-examplecom-2017-09-27.sh Cisco 高度なフィッシング防御 Sensor Installation ... Wed Sep 27 21:49:03 UTC 2017 VERSION: 17.09.27035106 + mkdir -p /opt/agari /var/opt/agari/etc Extracting install files into /var/opt/agari/tmp/agari.df8jXF Running extracted install Running Install/Upgrade steps... · agari-collector.service - LSB: start and stop agari-collector-milter Loaded: loaded (/etc/init.d/agari-collector; bad; vendor preset: enabled) Active: inactive (dead) since Wed 2017-09-27 14:46:21 PDT; 2min 42s ago Docs: man:systemd-sysv-generator(8) Process: 4664 ExecStop=/etc/init.d/agari-collector stop (code=exited, status=0/SUCCESS) Process: 4284 ExecStart=/etc/init.d/agari-collector start (code=exited, status=0/SUCCESS) Sep 27 13:38:33 ubuntu systemd[1]: Starting LSB: start and stop

	agari-collector-milter... Sep 27 13:38:33 ubuntu agari-collector[4284]: net.ipv4.ip_forward = 1 Sep 27 13:38:33 ubuntu agari-collector[4284]: Waiting for agari-collectord to start... Sep 27 13:38:34 ubuntu agari-collector[4284]: Started agari-collectord: PID 4299. Sep 27 13:38:34 ubuntu systemd[1]: Started LSB: start and stop agari-collector-milter. Sep 27 14:46:21 ubuntu systemd[1]: Stopping LSB: start and stop agari-collector-milter... Sep 27 14:46:21 ubuntu agari-collector[4664]: agari-collectord is not running. Sep 27 14:46:21 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-milter. Sep 27 14:48:36 ubuntu systemd[1]: Stopped LSB: start and stop agari-collector-milter. Warning: agari-collector.service changed on disk. Run 'systemctl daemon-reload' to reload units. Writing sensor configuration to file: /var/opt/agari/tmp/agari.df8jXF/etc/collector.yml
ログと設定データへアクセスするための UNIX グループ権限を指定できる HTTPS プロキシを指定できる	Do you want to verify the AWS SSL server certificates used for communications from this sensor to AWS? [y/N](no)>no You may optionally specify a Unix group that will be given read access to logs as well as write access to the collector's configuration and data. Group name (root): Will this sensor use an HTTPS proxy to send data to the cloud? [y/N](no)> Testing access to download S3 bucket... OK.

センサーへの SMTP 接続に使用する TLS 証明書を指定できる デバッグ レベルのロギングを指定できる	Testing access to configuration S3 bucket... OK. Testing access to data ingest S3 bucket... OK. Testing access to statistical ping SNS topic... OK. Testing access to data ingest Kinesis stream... OK. Do you want to configure TLS Certificates for incoming SMTP traffic to this sensor? [y/N](no)> n Require that all SMTP sessions use TLS? [y/N](no)?> n Which port should this sensor listen on for incoming SMTP connections? [25]> Enable DEBUG-level logging? [y/N](no)> n + : Creating directories ... + mkdir -p /var/opt/agari/etc /var/opt/agari/run /var/opt/agari/spool /var/opt/agari/shared /var/opt/agari/log + mkdir -p /opt/agari/bin /opt/agari/lib + ln -Tsf /var/opt/agari/etc/ /opt/agari/etc + ln -Tsf /var/opt/agari/etc/ /etc/agari + ln -Tsf /var/opt/agari/log/ /var/log/agari
	Running Install/Upgrade steps...

	Moving new files to /opt/agari Downloading docker image from S3... Deleting old docker containers... Deleting old docker images... Loading new docker image... Updated version to 17.09.27035106 Running post-installation Running post-installation Running post-install steps... Removing temporary install files in /var/opt/agari/tmp/agari.df8jXF Installation Complete

この時点で、センサーは正常にインストールされています。

高度なフィッシング防御にアクセスできる場合は、[管理(Manage)] > [センサー(Sensors)] ページに移動して、センサーが接続されていることを確認できます。

センサーのステータス

センサーは約 2 分後にホームを呼び出します。

OVA でセンサーをインストールする

組織が独自のハードウェアでセンサーをホストしている場合、その組織用に設定されたセンサーを含む仮想マシンパッケージ(OVA ファイル)を、手動のコマンドラインインストールおよび設定の合理化された代替手段として使用できます。次の内容を取り上げます。

- その組織からの仮想マシンパッケージのダウンロード
- 仮想マシンのパスワードの変更
- センサーの初期化
- センサーの設定

センサーは、事前設定済みのオペレーティングシステムとソフトウェアを含む仮想マシンで実行されます。仮想マシン自体は、「「センサーの前提条件」 ページ 24」で説明されている要件を満たすように設定されています。

OVA ファイルについて

OVA ファイルは、OVF パッケージを含む tar アーカイブファイルです。OVF はオープン仮想化フォーマット（open virtualization format）の略で、仮想マシンで実行するソフトウェアをパッケージ化および配布するためのオープンスタンダードです。OVF パッケージには、パッケージ内のすべてのファイルの説明、仮想マシンの 1 つ以上のディスクイメージ、場合によっては証明書やその他のサポートファイルが含まれています。OVF は、VirtualBox、Red Hat Enterprise Virtualization、VMware など、12 を超える仮想化プロバイダーによってサポートされています。

ダウンロードできる OVA ファイルは、センサーをインストール、実行、および管理するように設定された仮想マシンディスクイメージを含むパッケージです。

組織の仮想マシンパッケージ（OVA ファイル）をダウンロードする

前提条件

この手順で生成され、後で必要になる情報を貼り付けるための空のテキストファイルが必要になります。この情報には次のものが含まれます。

- 組織に固有の URL。
- インストール後にセンサーを初期化するために使用する 6 文字のランダムシーケンスであるプロビジョニングキー（これはライセンスファイルではありません。センサーと高度なフィッシング防御の組織間のリンクを検証します）。

1. [管理（Manage）] > [センサー（Sensors）] に移動します。
2. [インストール（Installation）] タブをクリックします。
3. [センサーインストーラのダウンロード（Download Sensor Installer）] > [OVAイメージ（OVA Image）] をクリックします。
4. ダウンロードする URL とプロビジョニングキーの両方をコピーして、**テキストファイルに保存します**。

   URL は OVA ファイルをダウンロードする場所です。プロビジョニングキーは、後でセンサーのインストールを完了するために必要になる 6 文字のランダムシーケンスです。ダウンロードリンクは、ダウンロードのダイアログボックスに示された日時に期限切れになります。プロビジョニングキーは、生成されてから 7 日後に期限切れになります。

5. ブラウザによってファイル拡張子が .ovf に変更された場合は、ファイル拡張子を .ova に変更します（ファイル拡張子を表示するようにオペレーティングシステムを設定する必要があります）。
6. [OK] をクリックします。
7. 新しいブラウザのウィンドウまたはタブで、アドレスバーに URL を貼り付けて、そのアドレスに移動します。OVA ファイルがコンピュータに自動的にダウンロードされます。

約 1.2GB の OVA ファイルには、すべてのセンサーソフトウェアの最新バージョンが含まれています。

OVA ファイルを再度ダウンロードすると、新しいプロビジョニングキーが生成され、以前のキーは無効になります。これによって現在プロビジョニングされているセンサーは無効化されないことに注意してください。

始める前の注意事項

センサーにスタンドアロンボックスを使用している場合は、センサーを実行するコンピュータに仮想化ソフトウェア（VirtualBox、VMware など）をインストールし、ダウンロードした OVA ファイルをそのマシンにコピーする必要があります。ハイパーバイザを使用している場合（VMWare ESXi のみがサポートされます）、ダウンロードした OVA ファイルは、ハイパーバイザ上の新しい仮想マシンインスタンスにアップロードされます。

OVA の最初の起動（次のタスクの最初のステップ）は、センサーアプリケーションのソフトウェアプリロードを完了している間は低速です。アプリケーションバンドルの読み込みで起動がハングしたように見える場合は、完了するまで少なくとも 3 分待ってください。

管理パスワードを変更する

1. 仮想マシンを起動し、OVA ファイルをインポートします。これにより、仮想化ソフトウェアに仮想マシンインスタンスが作成されます。
2. センサーの管理メニューから、4（パスワードの変更）を入力します。
3. パスワードを変更するかどうかを尋ねられたら、y を入力します。
4. 新しいパスワードを入力し、Enter を押します。パスワードは次の要件を満たす必要があります。
    - 最小文字数：6 文字
    - ユーザー名に類似していないこと
    - ホスト名に類似していないこと
    - 古いパスワードと類似していないこと
    - 少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字を含むこと
5. もう一度パスワードを入力し、Enter キーを押します。

仮想マシンを設定する

1. 仮想マシン設定の [ネットワーク（ネットワーキング）（network(ing)）] セクションで、目的の DNS および NTP サーバーに接続できること、および AWS への HTTP/HTTPS アクセスが必要であることを確認します（一部の仮想化ソフトウェアでは、これらの接続を許可するファイアウォールルールがすでに有効になっています）。
2. ポート 22 を開きます。センサーはポート 22 で使用できます（一部の仮想化ソフトウェアでは、ポート 22 がデフォルトで開いています）。
3. 残りの仮想マシンの設定が、「「センサーの前提条件」 ページ 24」で説明されている最小要件を満たしていることを確認します（仮想マシンはこれらの要件を満たすように事前に設定されているはずです。これは単なる検証手順です）。
4. 仮想マシンの設定を保存します。

センサーを初期化する

センサーの初期化には、仮想マシンのセンサーの管理メニューではなく、リモートのコマンドラインログインによって行う初回のセンサーのセットアップの実行が含まれます。

前提条件

- OVA ファイルをダウンロードしたときに生成して保存した 6 文字のプロビジョニングキー
- HTTP トラフィックにプロキシを使用している場合：プロキシのホスト名、ポート、ユーザー名、およびパスワード
- センサーへの TLS 経由の SMTP 配信を使用予定の場合：秘密キー（.key ファイル）、署名付き TLS 証明書（.pem ファイル）、および証明書チェーン（.pem ファイル）

1. コマンド プロンプトを開きます。
2. TLS 経由の SMTP を使用する場合は、scp を使用して秘密キーと証明書ファイルを /data/tls-certs/ にアップロードします。
   たとえば、次のコマンドを入力します。
   scp private_key.pem admin@sensor:/data/tls-certs/
3. 管理者として仮想マシンに SSH で接続し、管理者パスワードを入力します。
4. コマンド first-time-setup を入力し、Enter キーを押します。
5. プロンプトに 6 文字のプロビジョニングキーを貼り付け、Enter キーを押します。

センサーの初期化では、組織に合わせて正しく設定するために、いくつかの質問が行われます。

質問	オプション
このセンサーから AWS への通信に使用される AWS SSL サーバー証明書を確認しますか。	Amazon Web Services（AWS）が高度なフィッシング防御アプリケーションをホストし、SSL サーバー証明書がセンサーから高度なフィッシング防御への接続を認証します。 • [はい（yes）]（デフォルト） • [いいえ（no）]
オプションで、ログへの読み取りアクセスと、センサーの設定とデータへの書き込みアクセスを許可する Unix グループを指定できます。	root はデフォルトのグループであり、ほとんどのインスタンスで問題ありません。
このセンサーは、HTTPS プロキシを使用してデータをクラウドに送信しますか。	[はい（yes）] を選択した場合は、ホスト名、ポート、ユーザー名、パスワードの入力が求められます。 • [はい（yes）] • [いいえ（no）]（デフォルト）
このセンサーへの着信 SMTP トラフィック用に TLS 証明書を設定しますか。	これは、メールサーバーからセンサーへのトラフィックを暗号化する必要がある場合に必要です。 • [はい（yes）] • [いいえ（no）]（デフォルト）
すべての SMTP セッションで TLS を使用する必要がありますか。	• [はい（yes）] • [いいえ（no）]（デフォルト）
このセンサーは、着信 SMTP 接続をどのポートでリッスンする必要がありますか。	25 がデフォルトで、従来から SMTP によく使用されているポートです。インフラストラクチャによっては、これを変更する必要がある場合があります。587 は 25 の代わりに使用されることが多く、暗号化されていない接続または TLS 接続に役立ち、SSL 接続では多くの場合 465 が使用されます。

質問	オプション
デバッグレベルのロギングを有効にしますか。	デバッグレベルのロギングはより多くのデータを送信します。センサーに問題がある場合に使用できます。追加のデータによってデータ処理が遅くなる可能性があるため、センサーに既知の問題がない限り、この設定はデフォルト値の [いいえ(no)] のままにしてください。 • [はい(yes)]:各メッセージの処理に関する追加データを生成して送信します。 • [いいえ(no)](デフォルト):センサーデータのみを生成して送信します。

初期化が完了すると、センサーが自動的に起動します。少し待ってから、組織の [センサー(Sensors)] ページを更新すると、新しいセンサーが表示されます。

デフォルトのセンサー設定

センサーが初期化されると、デフォルトで以下のように設定されます。

設定	値
ステータス(Status)	Started
自動起動(AutoStart)	Enabled
DHCPまたは静的IPアドレス(DHCP/Static IP address)	DHCP センサーは DHCP を使用するように設定できますが、静的 IP アドレスが必要です。この IP アドレスは、センサーと通信する電子メールインフラストラクチャの他の部分を設定するときに使用されるためです。センサーに静的 IP アドレスを設定しない場合(「「静的 IP アドレスを設定する」 ページ 40」を参照)、DHCP サーバーでセンサーの IP アドレスのリースを予約する必要があります。
IPアドレス(IP address)	使用されている仮想マシンソフトウェアによって異なります。ほとんどの場合、デフォルト値または値の範囲が設定されています。
ホスト名(Hostname)	sensor
NTP サーバー(NTP Server)	us.pool.ntp.org

センサーの設定および操作

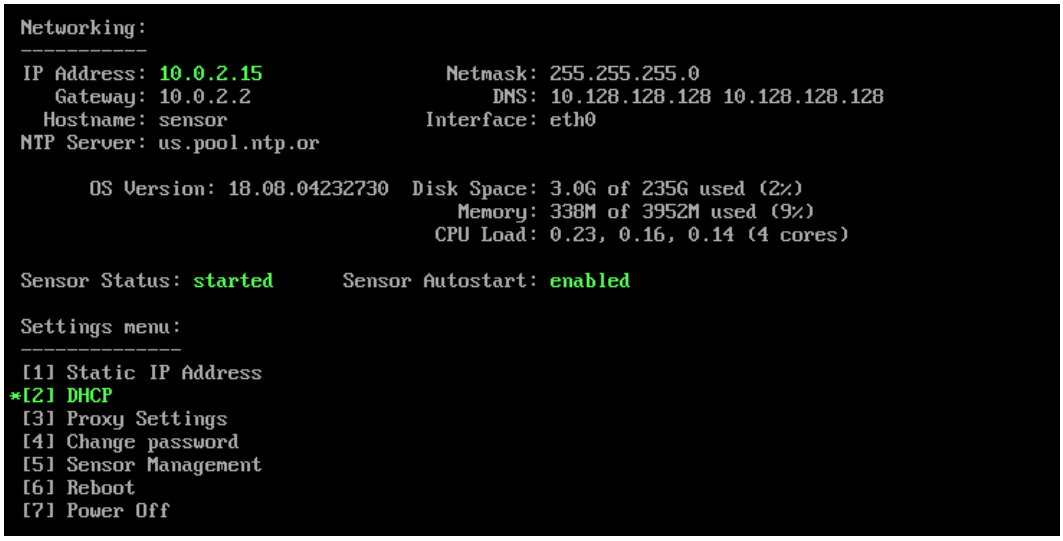
このセクションでは、OVA でインストールされたセンサーについてのみ説明します。

OVA のセンサーでは基本設定が事前に設定されています。追加の設定なしで起動してネットワーク上で使用できるようになっています。起動時に DHCP 経由で IP アドレスが割り当てられるようにもなっています。センサーの設定は、文字ベースのメニューで行います。次の操作を実行できます。

- センサーの起動、自動起動、再起動、および停止
- 静的 IP アドレスの設定または DHCP の有効化

- プロキシの設定

センサーの設定は、仮想マシンのセンサー管理メニューから実行します。



すべてのセンサー管理は、ここから始めることを前提としています。

センサーを起動する

センサーは、停止している場合にのみ起動できます。

1. 5(センサー管理)を押します。
2. 1(センサーの起動)を押します。
3. y を押します。
4. 3(メインメニュー)を押します(何もしなければ、センサー管理アプリは数秒後に自動的にメインメニューに戻り、アクションを保存しません)。

仮想マシンへの SSH 接続時には、コマンドラインからセンサーを起動することもできます。詳細については、「管理者アカウントコマンド」セクションを参照してください。

センサーを停止する

センサーは実行中のみ停止できます。

1. 5(センサー管理)を押します。
2. 1(センサーの停止)を押します。
3. y を押します。
4. 3(メインメニュー)を押します(何もしなければ、センサー管理アプリは数秒後に自動的にメインメニューに戻り、アクションを保存しません)。

仮想マシンへの SSH 接続時には、コマンドラインからセンサーを停止することもできます。詳細については、「管理者アカウントコマンド」セクションを参照してください。

仮想マシンを再起動する

1. 6(再起動)を押します。
2. y を押します。

セーフモードで起動する

仮想マシンの起動時に、トラブルシューティングを目的としてセーフモードで直接起動するか、通常モードまたはセーフモードを選択できる起動メニューを表示させることができます。

1. 起動時、起動画面が表示される前に以下の操作を行います。
    - S キーを押したままにして、セーフモードで起動します（セーフモードでは、起動時にカスタム設定は復元されません）。
    - D または S 以外のキーを押し続けると、起動メニューが表示されます。

仮想マシンの電源を切る

1. 7（電源オフ）を押します。
2. y を押します。

センサーが停止し、仮想マシンが終了します。

センサーの自動起動を有効にする

センサーの自動起動を有効にすると、仮想マシンを立ち上げた際にセンサーが自動的に起動します。初期化時にはデフォルトで有効になっています。センサーの自動起動は、無効になっている場合にのみ有効にできます。

1. 5（センサー管理）を押します。
2. 2（再起動時に自動起動を有効にする）を押します。
3. y を押します。
4. 3（メインメニュー）を押します（何もしなければ、センサー管理アプリは数秒後に自動的にメインメニューに戻り、アクションを保存しません）。

仮想マシンへの SSH 接続時には、コマンドラインからセンサーの自動起動を有効にすることもできます。詳細については、「管理者アカウントコマンド」セクションを参照してください。

センサーの自動起動を無効にする

センサーの自動起動を無効にすると、仮想マシンを立ち上げた際にセンサーは自動的に起動しません。センサーの自動起動は、有効になっている場合にのみ無効にできます。

1. 5（センサー管理）を押します。
2. 2（再起動時に自動起動を無効にする）を押します。
3. y を押します。
4. 3（メインメニュー）を押します（何もしなければ、センサー管理アプリは数秒後に自動的にメインメニューに戻り、アクションを保存しません）。

仮想マシンへの SSH 接続時には、コマンドラインからセンサーの自動起動を無効にすることもできます。詳細については、「管理者アカウントコマンド」セクションを参照してください。

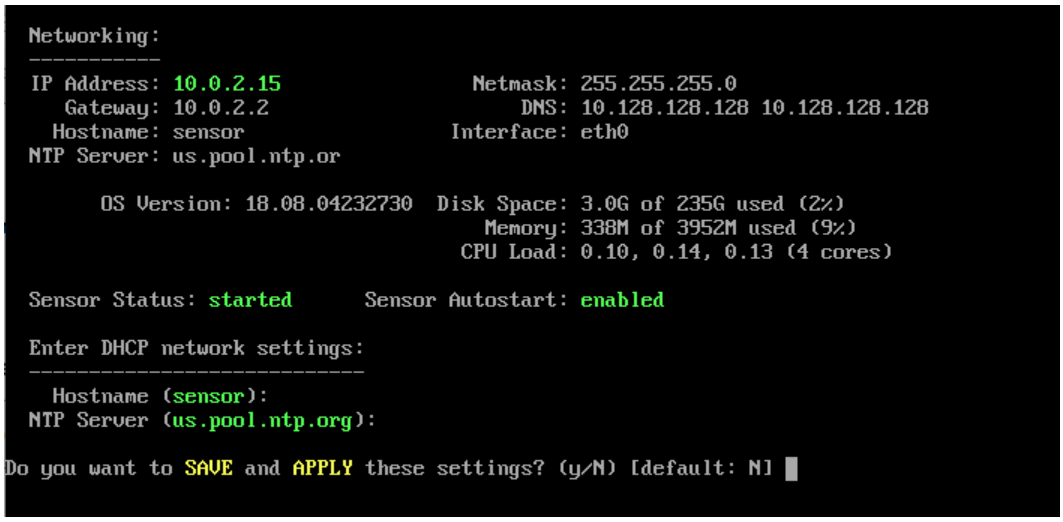
DHCP を有効にする

DHCP を有効にする必要があるのは、DHCP 予約を設定して、DHCP サーバーでセンサーの静的 IP アドレスを永続的にリースする場合だけです。

DHCP を有効にすることで、IP アドレスとその他のネットワーク設定パラメータが動的に設定されます。DHCP を有効にする場合は、ホスト名と NTP サーバーを設定します。

1. 2（DHCP）を押します。
2. ホスト名の値を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
3. NTP サーバーの値を入力して Enter を押します（現在の値を維持するには、Enter を押すだけです）。

   画面は次のようになります。



4. y を押します。

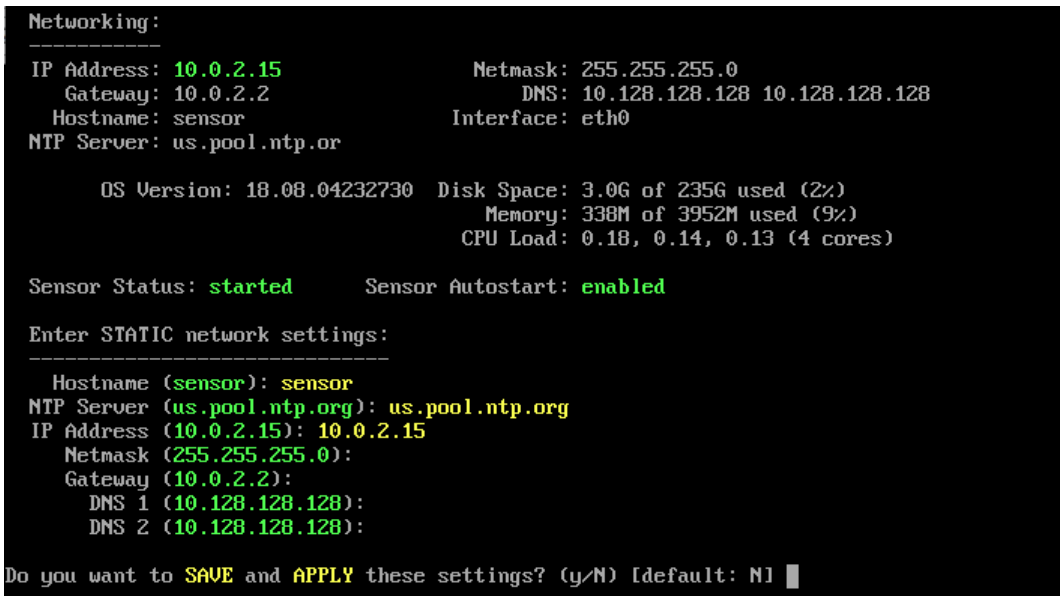
静的 IP アドレスを設定する

静的 IP アドレスを設定することで、センサーが接続するために必要な他のネットワークパラメータも定義されます。通常、静的 IP アドレスを設定し、独自のネットワーク インフラストラクチャ内で機能するようにネットワークパラメータを定義することをお勧めします。

DHCP のない環境にセンサーをインストールした場合、デフォルト値は割り当てられません。その場合、「現在の値」はなく、各パラメータに特定の有効な値を入力する必要があります。

1. 1（静的 IP アドレス）を押します。
2. ホスト名の値を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
3. NTP サーバーの値を入力して Enter を押します（現在の値を維持するには、Enter を押すだけです）。
4. 有効な IP アドレスを入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
5. 有効なネットマスク値を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
6. 有効なゲートウェイ値を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
7. 有効な DNS 値（DNS 1 は通常、内部 DNS サーバーになります（ある場合））を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。
8. 2 番目の有効な DNS 値（DNS 2 は、DNS 1 が使用できない場合に使用される外部のフォールバック DNS サーバーであることがよくあります）を入力して Enter を押します（現在の値を保持するには、Enter を押すだけです）。

   画面は次のようになります。



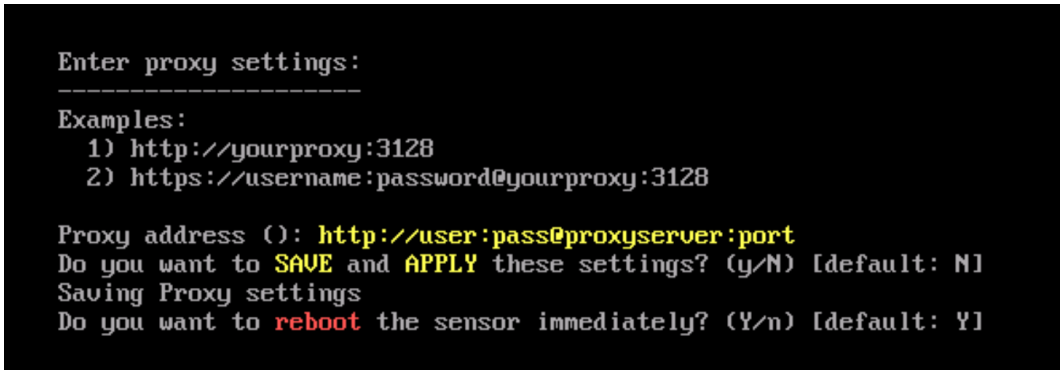
9. y を押します。

プロキシを設定する

組織がプロキシサーバーを使用してインターネットに接続している場合、そのプロキシを使用するようにセンサーを設定できます。

1. 3(プロキシの設定)を押します。
2. プロキシサーバーが NTLM 認証を使用する場合は y を、使用しない場合は n(デフォルト)を押します。
3. プロキシサーバーの接続文字列を入力し、Enter を押します。接続文字列には、プロトコル、サーバー、ポート、およびオプション(サーバーが認証を必要としない場合)のユーザー名とパスワードが含まれます。プロトコルは http または https(推奨)のいずれかです。次に例を示します。
   - https://username:password@server:port
   - http://server:port

   画面は次のようになります。



4. y を押して設定を保存します。
5. y を押して仮想マシンを再起動します。

プロキシを無効にする

このオプションは、プロキシが設定されている場合にのみ使用できます。

1. 3(プロキシの設定)を押します。
2. プロキシを無効にするかどうかを尋ねられたら、y を押します。

管理者アカウントコマンド

センサーの管理メニューを使用する代わりに、仮想マシンに ssh で接続すると、センサーの管理に次のコマンドを使用できます。

- first-time-setup:センサーの設定を実行します
- sensor-start:設定後にセンサーを起動します
- sensor-stop:設定して起動したらセンサーを停止します
- sensor-service-enable:起動時のセンサーの自動起動を有効にします
- sensor-service-disable:起動時のセンサーの自動起動を無効にします

2 番目のネットワーク インターフェイスを有効にする

1. 管理者として仮想マシンに接続します。
2. ホームディレクトリで、eth1.conf ファイルを次のように編集します。
    - DHCP:必要に応じて、ipv4 または ipv6 の interface のコメントを外します
    - 静的 IP:必要に応じて、interface、ip、および subnet のコメントを外します
3. 仮想マシンを再起動します。

センサーをテストする

最初のセンサーがインストールされ、Cisco に接続できるようになったら、テスト電子メールをセンサーに直接送信できます。

センサーはインストールスクリプトで指定したポートで SMTP カンバセーションをリッスンしているため、直接センサーにテストメッセージを挿入することができます。インストール スクリプトで設定した SMTP ポートに telnet で接続でき、SMTP コマンドを直接実行する方がやりやすい場合は、テストメッセージを作成できます。

$ telnetsensor_name:sensor_port

Trying IP_address...

Connected to sensor_name

Escape character is '^]'.

220 collector-milter ESMTP Postfix

HELO example.com

250 collector-milter

MAIL FROM: <test@example.com>

250 2.1.0 Ok

RCPT TO: user@yourcompany.com

DATA

354 End data with <CR><LF>.<CR><LF>

Received: from 1.2.3.4 by test.example.com

Received: from 192.168.3.3. by internal

From: "John Smith" <jsmith@example.com>

To: "Jane Doe" <jdoe@example.net>

Subject: test message sent from manual telnet session

Date: Wed, 11 May 2011 16:19:57 -0400

Message-Id: <testing-testing>

Hello World,

This is a test message sent from a manual telnet session.

Yours truly,

SMTP administrator

。

250 2.0.0 Ok: queued as message_ID

quit

メッセージの DATA に Received: ヘッダーが含まれていることを確認します。それ自体の行に「.」文字を入力すると、データコマンドは終了します。「250 2.0.0. Ok: queued as…」コマンドは、テストメッセージが正常に受信され、センサーがいつでも、デュアル配信構成からルーティングされたメッセージを受信できることを意味しています。

テスト電子メールのトラブルシューティング

MAIL FROM: 行を入力した後に、次のようなエラーメッセージが表示された場合：

>451 4.7.1 Service unavailable - try again later

…it is likely the Sensor is not up and running yet. 以下を試してください。

- ホストの /var/log/agari/container.log を調べて、次のような行があるかどうかを確認します。

  Feb 01 2017 05:07:59 INFO collector-milter is ready.

  ない場合は、まだ milter プロセスが起動していません。数分間待ってから、もう一度試してください。
- センサーを起動してから 5 分以上経過していますか。

経過していない場合は、完全に 5 分経過するまで待ち、それでもまだ milter が起動していない場合は、コンテナを再起動します。

$ /opt/agari/bin/agari-ep restart

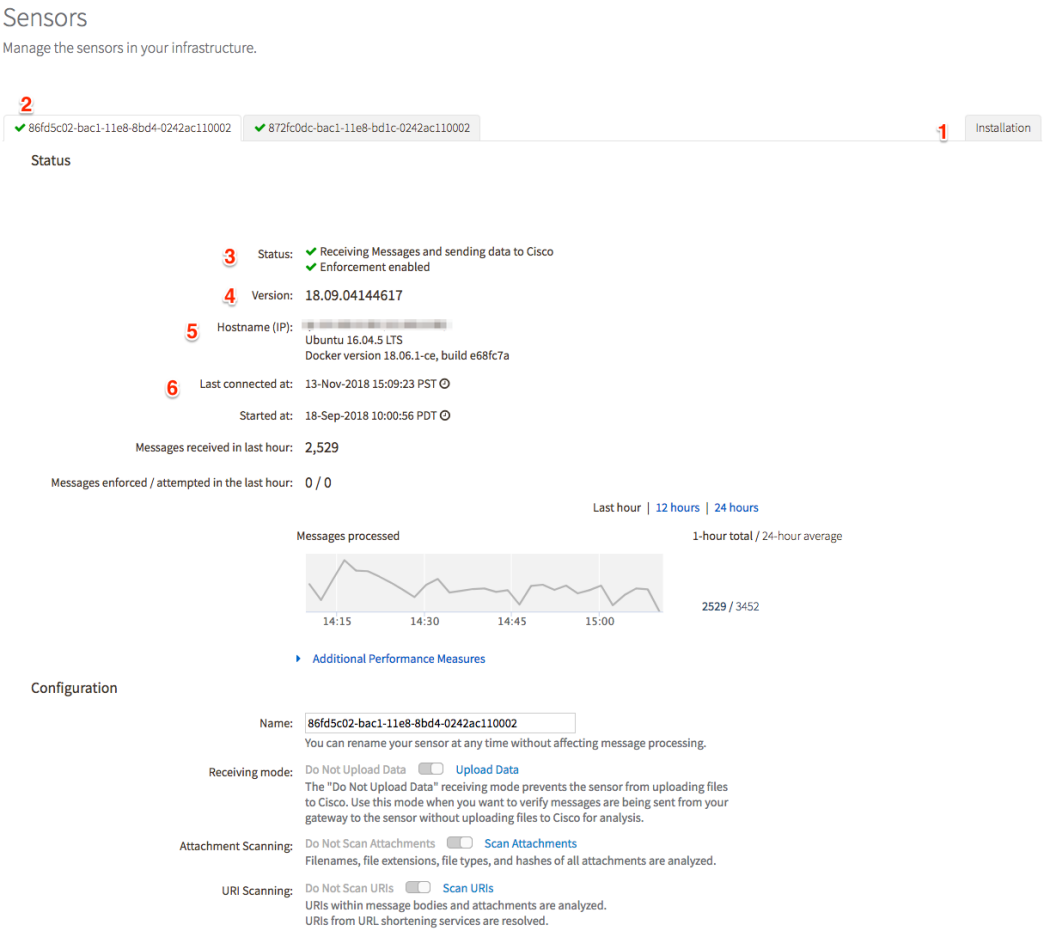
- コンテナの再起動後も問題が解決されない場合は、センサー全体の再起動を検討します。

  $ sudo service agari-collector restart

センサーのステータスを表示する

[管理(Manage)] > [センサー(Sensors)] ページでセンサーのステータスを表示し、管理します。

組織で Graph API 適用が有効になっている場合、適用センサーのステータスは冗長であり、[センサー(Sensor)] ページに表示されません。



[センサー(Sensor)] ページ

1	[センサー(Sensor)] ページから、組織固有のキーが付加されたセンサーのインストールスクリプトまたは仮想マシンパッケージをダウンロードできます。これを使用して、追加のセンサーをインストールし、増加したトラフィックを処理できます。詳細については、「「スクリプトでセンサーをインストールする」 ページ 28」および「「OVA でセンサーをインストールする」 ページ 33」を参照してください。
2	複数のセンサーがある場合は、タブの一覧からセンサーを選択します。このページでセンサーの現在のステータスを表示し、設定を変更できます。センサーの全体的なステータスは、タブ上のアイコン(緑/黄/赤)によって示されます。
3	適用が有効になっている場合は、タブ内で送信および受信と適用に対応した個別のステータスアイコンを確認できます。適用対象のメッセージの 80 % 超に適用されている場合、[適用(Enforcement)] アイコンは緑色です。そのしきい値を下回る場合は、黄色です。適用アクションが指定された任意のポリシーの [ポリシーレポート(Policy Report)] ページ([管理(Manage)] > [レポート(Reports)] ページでポリシー名の右側にある [一致するメッセージ数(Number of Matching Messages)] バーをクリック)で、[一部のメッセージが移動されない理由(Why are some messages not moved?)] リンクを参照してください。
4	センサーを更新します。使用可能なバージョンの一覧から選択し、[更新(Update)] をクリックします。
5	センサーが導入されている仮想マシンのホスト名および IP アドレスです。
6	最終接続時間は Cisco によって、センサーが最後にチェックされた時間です。これは、直近 2 分間以内になるはずです(センサーがアクティブな場合)。

Office 365 顧客の場合のみ、センサーが適用アクティビティを実行するために使用するクレデンシャル用の [クレデンシャルファイルのダウンロード(Download Credentials File)] ボタンがあります。

センサーに加えた変更を保存するには、[設定の保存(Save Configuration)] をクリックします。変更はセンサーに伝搬され、5 分以内に有効になります。

センサー診断情報をダウンロードする

この機能を使用するには、ユーザーアカウントに組織の管理者ロールが必要です。ユーザーロールの詳細については、「「ユーザーロール」 ページ 209」を参照してください。

センサーとそのパフォーマンスは常にモニタリングされます。各センサーとそのパフォーマンスに関する情報は一連の診断ファイルにコンパイルされ、Cisco の安全なサーバーで 24 時間ごとに更新および保存されます。Cisco のテクニカルサポートから、オンデマンドの一連のファイルをリクエストできます。

ダウンロードが利用できるのはオンプレミスセンサーのみです。ホステッド型センサーには適用されません。

オンデマンドの一連の診断ファイルは、高度なフィッシング防御の [センサー(Sensors)] ページから直接ダウンロードすることもできます。

オンデマンドの一連のセンサー診断ファイルをリクエストまたはダウンロードすると、Cisco の安全なサーバーで次の一連の診断ファイルを更新および保存するまでの 24 時間の時計がリセットされます。

1. [管理(Manage)] > [センサー(Sensors)] に移動します。
2. 一連の診断ファイルをダウンロードするセンサーのタブをクリックします。
3. [診断情報のダウンロードリンクの取得(Get link to download diagnostic information)] をクリックします。

4. リンクをコピーしてブラウザのアドレスバーに貼り付け、そのアドレスに移動します（ アイコンをクリックすると、URL をクリップボードにコピーできます）。

ファイルは、ブラウザのダウンロード用のデフォルトの場所に自動的にダウンロードされます。ファイルの名前は、Diagnostics-YYYYMMDD-HHMMSS.tar.gz です。このファイルタイプは、一般に tarball として知られる二重圧縮ファイルです。解凍すると、通常、/shared、/container、/host、および /log を含む一連のフォルダが得られます（生成および保存される診断情報の量は時間の経過とともに変化する可能性があるため、ファイルセットの実際の内容は時間の経過とともに変化する可能性があります）。診断を実行している場合は、センサーアクションの記録を含むいくつかのログファイルが含まれている /log フォルダ内のファイルを確認することをお勧めします。

第 4 章

センサーへの配信の設定

センサーをインストールしたら、メッセージのストリームをセンサーに送信するように電子メールゲートウェイを設定します。

配信を設定する手順は、電子メールゲートウェイの種類によって異なります。電子メールゲートウェイの配信設定に関するガイドを参照してください。

配信は、初期のスパム対策、ウイルス対策、マルウェア対策、またはその他のフィルタリングやサンドボックス分析が実行された後に行われるように設定する必要があります。高度なフィッシング防御は防御の最前線に立つものではなく、スパム対策やマルウェア対策の代わりになるものではありません。このフィルタリングをクリアした本物でないメッセージを検出することを目的としています。

デュアル配信の設定

センサーをインストールしたら、メッセージのストリームをセンサーに送信（デュアル配信）するように電子メールゲートウェイを設定する必要があります。

デュアル配信を設定する手順は、電子メールゲートウェイの種類によって異なります。電子メールゲートウェイのデュアル配信設定に関するガイドを参照してください。

ゲートウェイの種類にかかわらず、次を実行します。

- デュアル配信は、企業への「ラストホップ」からのものにするように設定する必要があります。企業によっては、複数のゲートウェイ「階層」や、複数の MTA（メール転送エージェント）または SEG（セキュアな電子メールゲートウェイ）の層が存在することがあります。デュアル配信は必ず最後のルーティングポイントとなるように設定します。通常、そのポイントから内部メッセージストア（Microsoft Exchange など）にメッセージが送信されます。
- デュアル配信は、すべてのスパム対策、ウイルス対策、マルウェア対策、またはその他のフィルタリングやサンドボックス分析が実行された後に行われるように設定する必要があります。Cisco 高度なフィッシング防御 は防御の最前線に立つものではなく、スパム対策やマルウェア対策の代わりになるものではありません。このフィルタリングをクリアした本物でないメッセージを検出することを目的としています。

デュアル配信の割り込み

センサーから Cisco へのメッセージに割り込めるポイントが 2 か所あります。

- センサー自体に［受信モード（Receiving Mode）］設定が含まれ、デフォルトでは［データのアップロード（Upload Data）］に設定されています。

処理のために Cisco へデータをアップロードせずに、センサーへの配信をテストする必要がある場合は、[受信モード(Receiving Mode)]を[データをアップロードしない(Do Not Upload Data)]に設定できます。

- 組織には、[取り込みモード(Ingest Mode)]トグルがあります。これは、高度なフィッシング防御でメッセージが表示される前に Cisco セールスエンジニアが設定する必要があります。

  [取り込みモード(Ingest Mode)]トグルは、システムへデータを送信する新しい組織による、トラフィックの急増から保護するために、Cisco が使用する安全対策です。

特定のデュアル配信の手順

このガイドには、以下の環境でデュアル配信を設定する方法に関する情報が含まれています。

- 「デュアル配信の設定:Cisco ESA」 ページ 67

デュアル配信の設定:G Suite

このセクションでは、Google Apps Gmail 管理ユーザーインターフェイス内から直接デュアル配信を設定する方法について説明します。この管理インターフェイスにアクセスするには、Google Apps 管理コントロールパネル(https://admin.google.com/AdminHome)に適切な管理者ログイン情報でログインします。

Google Chrome ブラウザを使用して、Google Apps を設定することをお勧めします。Cisco の UI にはバグがあり、他のブラウザ(特に Safari)ではデュアル配信設定を完了できません。

全般的な手順は次のとおりです。

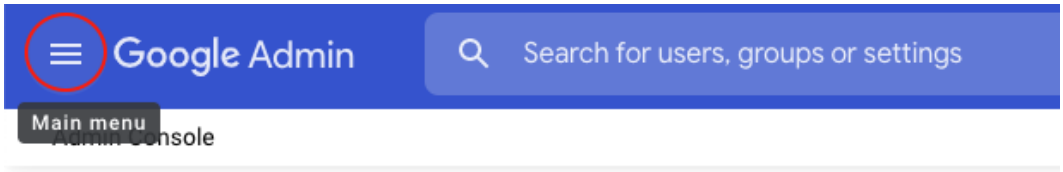
ステップ 1:新しいルートを作成します。1 つのホストまたは複数のホストを組み合わせて、それを電子メールのコピーの送信先となる Cisco センサーへのもう 1 つの「ルート」とします。

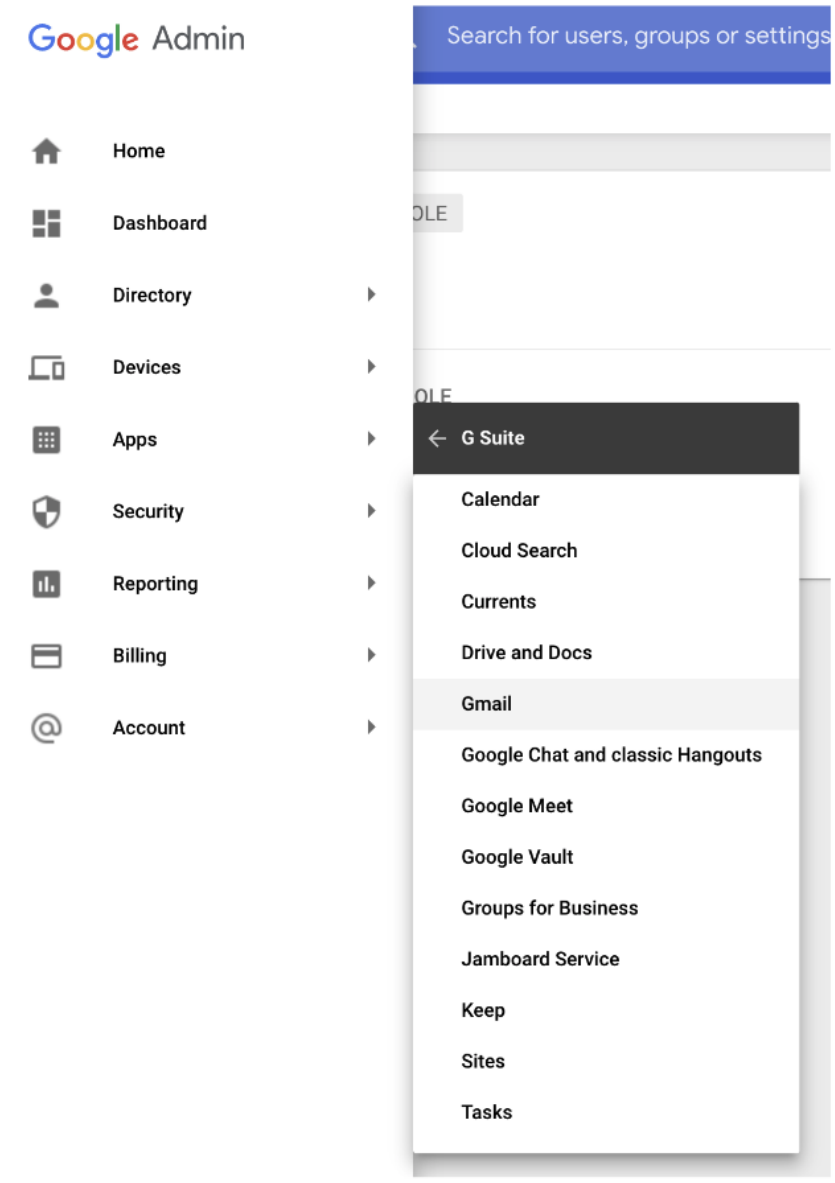
ステップ 2:その新しいルート経由でセンサーにメッセージをコピーする「デフォルトルーティング」ルールを追加します。

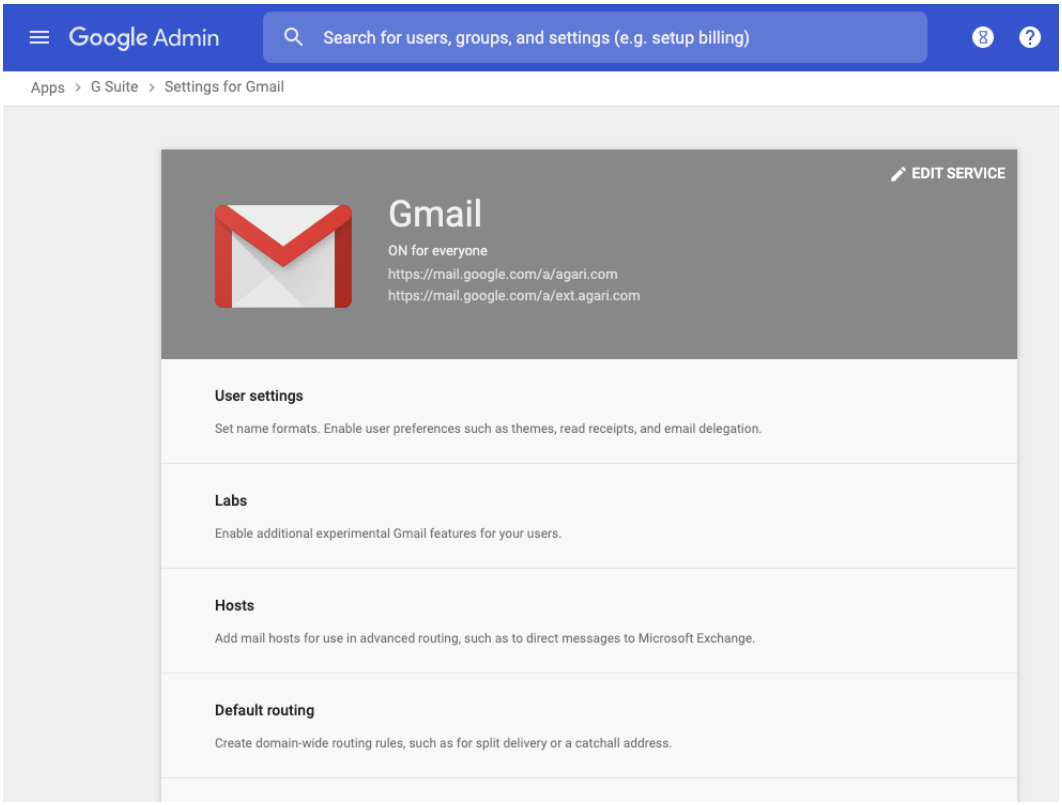
ステップ 3:自身と自身のユーザーが確実にアラートを受信するように、Cisco のアラートサーバーをホワイトリストに登録します。

ステップ 1:新しいルートを作成する

1. Google Apps 管理コントロールパネルで、[Google Admin] の横にあるメニューアイコンをクリックして、ドロップダウンメニューにアクセスし、[Apps] > [G Suite] を選択して、メニューの [Hosts] をクリックします。




Google Admin
Search for users, groups or settings
Home
Dashboard
Directory
Devices
Apps
Security
Reporting
Billing
Account
G Suite
Calendar
Cloud Search
Currents
Drive and Docs
Gmail
Google Chat and classic Hangouts
Google Meet
Google Vault
Groups for Business
Jamboard Service
Keep
Sites
Tasks



2. [Hosts] 画面で、[ADD ROUTE] をクリックします。
3. メールルートの詳細を入力します。
    - わかりやすい名前を入力します。たとえば、「Cisco センサー」とします。
    - 電子メールサーバーの値を 1 つ以上入力します。これは、ホスト名（推奨）か、センサーのネットワークの場所に対応する IP アドレスとポート番号です。
        - Cisco がセンサーをホストしている場合は、[Single host] を選択し、ホスト名を入力します（ここに入力する情報は、営業担当者またはサポート担当者から「*symbolicname*.hosted.appc.cisco.com」という形式で提供されます。*symbolicname* は、組織で使用されるシンボル名です）。また、センサーのポート番号（25）も入力します（厳密には、ホスト名は使用するすべてのセンサーの「前」にあるロードバランスの名前です）。
        - センサーをホストしている場合、1 つのセンサーを使用しているのであれば [Single host] を選択し、複数のセンサーを使用しているのであれば [Multiple hosts] を選択します。後者の場合は、[Add] をクリックし、使用するセンサーごとに IP アドレス、ポート番号、および負荷率を入力します。ホストは、プライマリとしてもセカンダリとしても定義できます（後者はフォールバック用）。ただし、カテゴリごとに負荷率の合計が 100% になる必要があります。たとえば、3 個のセンサーをプライマリホストとして定義してそれぞれの負荷率を 34、33、33 にしたり、2 個のセンサーをセカンダリホストとして定義してそれぞれの負荷率を 50 ずつにしたりできます。
    - TLS 証明書がセンサーにすでに設定されているため、[Require secure transport (TLS)] を有効にできます。また必要に応じて、[Require CA signed certificate] も有効にできます（適宜、営業担当者またはサポート担当者と協力して、適切な設定を決定します）。
4. [SAVE] をクリックします。

ステップ 2：センサーにメッセージをコピーする「デフォルトルーティング」ルールを追加する

センサーにメッセージのコピーを転送するには、デフォルトルーティングの下にルーティングルールを作成します。この新しいルーティングルール設定では、上記のセクションで作成したルートを参照します。

1. Google Apps 管理コントロールパネルで、[Apps] > [G Suite] > [Gmail] > [Advanced settings] に移動します。
2. [Default routing] タブをクリックします。
3. [ADD SETTING] をクリックします。
4. ルート設定の詳細を入力します。
    1. [Specify envelope recipients to match] で、[All recipients] を選択します。
    2. [Add more recipients] チェックボックスをオンにします。
    3. [ADD] をクリックします。
    4. [Basic] ビューから [Advanced] ビューに切り替えます。
    5. [Change route] チェックボックスをオンにし、「「ステップ 1：新しいルートを作成する」 ページ 48」で作成したセンサーメールルートを選択します。
    6. [Spam and delivery options] セクションで、[Do not deliver spam to this recipient] チェックボックスと [Suppress bounces from this recipient] チェックボックスをオンにします。
    7. [Headers] セクションで、[Add X-Gm-Original-To header] チェックボックスと [Add X-Gm-Spam and X-Gm-Phishy headers] チェックボックスをオンにします。
    8. [SAVE] をクリックします。
    9. [Options] セクションで、[Perform this action on non-recognized and recognized addresses] を選択します。
5. [SAVE] をクリックします。

センサーへのメールの配信が始まります。

「デフォルトルーティング」の他のオプションを設定することもできます。その場合、この新しい設定を設定可能な他のルートのどこに配置するかを慎重に検討する必要があります。Cisco は、このルートを最初の設定（Order = "1"）として追加して、配信可能なすべてのメールもセンサーに配信されるようにすることを推奨しています。ただし、場合によっては、組織と組織のポリシーに固有のルーティングポリシーを検討する必要があります。

ステップ 3：Cisco の通知サーバーをホワイトリストに登録する

Cisco が電子メールを疑わしいと見なした場合、高度なフィッシング防御では必要に応じて管理者と疑わしいメッセージの元の受信者、またはどちらか一方に電子メールアラートを送信できます。

脅威となっているメッセージを特定する以外にも、アラート電子メールには、脅威の種類やシビラティ（重大度）に関する追加の情報を含めることができます。運用上の問題が発生した場合、Cisco 通知サーバーはセンサーおよび高度なフィッシング防御サービスの全体的な健全性に関するアラートを送信することもできます。こうしたアラートの重要性と有用性を考慮して、Cisco ではシステムがこれらのメッセージをブロックまたは隔離しないようにするため、Cisco 通知サーバーをホワイトリストに登録することを推奨しています。

たとえば、Cisco 通知サーバーが送信したメッセージに、元のメッセージのコンテンツの一部が含まれることがあります。元のメッセージにスパムが含まれていたり、電子メールのフィルタリングソフトウェアによって疑わしいと見なされたりする場合があるため、Cisco がアラート自体を偶発的に脅威と見なす可能性があります。

そのため、フィルタリングソフトウェアの誤検出がトリガーされないようにするには、Cisco 通知サーバーをホワイトリストに登録することが非常に重要です。中間フィルタリング手順がある場合（たとえば、他の中間 MTA、または電子メールをフィルタ処理する他のフィッシング対策ソリューション）、それらも Cisco 通知サーバーをホワイトリストに登録するように設定する必要があります。Cisco のセールスエンジニアチームとカスタマーサクセスチームが必要に応じてホワイトリストの設定を支援できます。

Gmail には、アップストリーム MTA をホワイトリストに登録する基本的な方法が 2 つ用意されています。

- 電子メールホワイトリスト（推奨）
- 着信ゲートウェイ

電子メールホワイトリストを介してアップストリーム MTA をホワイトリストに登録する

「電子メールホワイトリスト」という方法には、小さなリスクがあります。Gmail が使用するスパムとレピュテーションのスキャンに基づいて、指定した IP アドレスが依然としてブロックされたり、遅延したりするというリスクです。Cisco のアラートサーバーはレピュテーションに優れ、メールの送信量が比較的少ないため、アラートがブロックされたり抑制されたりするリスクは非常に低くなっています。Cisco アラートがブロックされたり抑制されたりする懸念がある場合は、次に示す「着信ゲートウェイ」を使用して、Cisco アラートサーバーをホワイトリストに登録できます。

1. Google Apps 管理コントロールパネルで、[Apps] > [G Suite] > [Gmail] > [Advanced settings] に移動します。
2. [General Settings] タブをクリックします。オプションリストを [Spam, phishing, and malware] セクションまでスクロールダウンします。
3. [Email whitelist] 設定で、[Enter the IP addresses for your email whitelist] フィールドに 198.2.132.180 と入力します。
4. [SAVE] をクリックします。

Cisco アラートサーバーの IP アドレスは 198.2.132.180 です。また、Cisco はドメイン「outbound.cisco.com」でこのアドレスの DNS エントリを維持します。一般に、このホワイトリストルールには明示的な IP アドレスを使用することをお勧めします。

着信ゲートウェイを介してアップストリーム MTA をホワイトリストに登録する

次に示すステップは、前述の方法で Cisco アラートサーバーをホワイトリストに登録できない場合にのみ実行してください。

Cisco アラートサーバーをホワイトリストに登録する場合は上記のセクションで説明している「電子メールホワイトリスト」の方法をお勧めしますが、この方法が現実的でない場合は「着信ゲートウェイ」の方法を使用できます。この方法では、Cisco アラートサーバーから送信されたメッセージが確実に配信されるようになります。ただし、ステップが少し複雑です。

着信ゲートウェイがまだ設定されていない場合でも、この方法を使用できます。少なくとも 1 つの着信ゲートウェイがすでに設定されている場合に、この方法を使用すると、他のすべての着信ゲートウェイに対するスパムチェックが無効になるという点に留意してください。そうしたゲートウェイがそれぞれスパムチェックを行っている場合、チェックの無効を容認することもできますが、容認できない場合は「電子メールホワイトリスト」の方法を検討してください。

1. Google Apps 管理コントロールパネルで、[Apps] > [G Suite] > [Gmail] > [Advanced settings] に移動します。
2. [Spam, phishing, and malware] セクションの [Inbound gateway] 設定で、[Configure]（着信ゲートウェイをまだ設定していない場合）または [Edit]（着信ゲートウェイをすでに設定している場合）をクリックします。
3. ゲートウェイ設定の説明を入力します。たとえば、「Cisco アラートサーバーをホワイトリストに登録する」とします。
4. IP アドレス/範囲ボックスの [ADD] をクリックします。

5. IP アドレス 198.2.132.180 を入力します。
6. [SAVE] をクリックします。

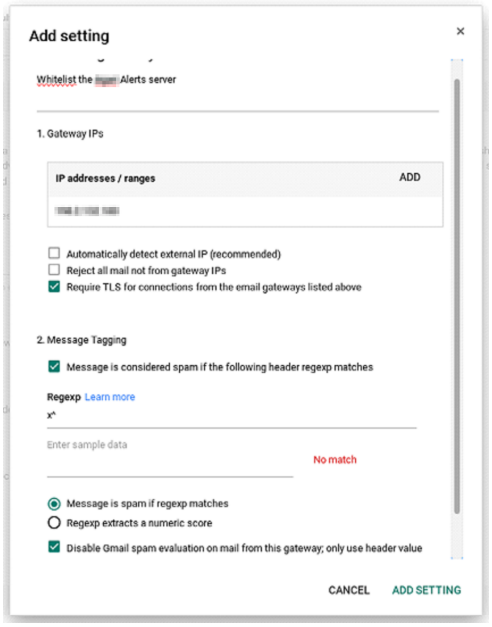
   [Automatically detect external IP (recommended)] オプションを選択しないでください。これは、メッセージの IP アドレスの「最後のホップ」に関するものです。Cisco 通知サーバーが外部メッセージをリレーすることはないため、このオプションは必要ありません。設定に間違いはないという確信がない場合は、[Reject all mail not from gateway IPs] オプションを選択しないでください。選択した場合、メールサービスが中断する可能性があります。
7. [Require TLS for connections from the email gateways listed above] チェックボックスをオンにします。ただし、このオプションをオフにする必要があるゲートウェイが他にある場合を除きます。
8. [Message is considered spam if the following header regexp matches] チェックボックスをオンにします。

   このセクションでは、どのメッセージにも一致しない正規表現(「regexp」)を作成します。これは直感に反して、Gmail が IP アドレス 198.2.132.180 から受信したメッセージをブロックしなくなります(代わりに「電子メールホワイトリスト」の方法を使用した場合、IP アドレスが本当にホワイトリストに登録されるのかは保証されません。その IP を介して渡されたメッセージはスパムと判別されないというだけです)。
9. [Regexp] フィールドに、x^ をこのとおりに(つまり、小文字の x とキャレット記号)入力します。

   これは、どのメッセージにも一致しないことを目的とした表現です(つまり、「文字 x が文字列の先頭の前にある場合に一致する」ということであり、不可能です)。
10. [Message is spam if regexp matches] チェックボックスをオンのままにします。
11. [Disable Gmail spam evaluation on mail from this gateway; only use header value] チェックボックスをオンにします。

    繰り返しになりますが、以上のオプションは設定済みのすべての着信ゲートウェイ IP に適用されるため、組織に適していることもあれば適していないこともあります。使用する場合は、事前にその影響を検討してください。

    設定が完了すると、ウィンドウは次のようになります。



12. [ADD SETTING] をクリックします。

次のように、着信ゲートウェイが全体的な設定にリストされます。

着信ゲートウェイを使用した方法の設定のまとめ

ラップアップ

上記の手順を完了すると、Cisco センサーは組織に送信された電子メールメッセージのコピーを受信し始めます。Google のシステムが変更をコミットして変更が完全に有効になるまでに、数分間のわずかな遅延が生じることがあります。https://appc.cisco.com で高度なフィッシング防御にログインし、[管理(Manage)] > [センサー(Sensors)] に移動してインストールしたセンサーのステータスを表示してトラフィックフローを確認できます。

デュアル配信の設定:Office 365

このセクションでは、ジャーナリングルールを使用して、Microsoft Office 365 環境のデュアル配信を設定する方法について説明します。

全般的な手順は次のとおりです。

ステップ 1:ジャーナリングされたメッセージをセンサーにルーティングするコネクタを作成する。

ステップ 2:センサーにメッセージをコピーするジャーナルルールを Office 365 に作成する。

ステップ 3:自身と自身のユーザーが確実にアラートを受信するように、アラートサーバーの IP アドレスをホワイトリストに登録する。

高度なフィッシング防御では、メッセージ方向性に適切な値を設定した X-MS-Exchange-Organization-AuthAs: ヘッダーをすべてのメッセージに追加する必要があります。これを設定する方法については、Microsoft Exchange のドキュメントを参照してください。高度なフィッシング防御が正しく機能するには、次のヘッダーと値が必要です。

- 内部メッセージ:X-MS-Exchange-Organization-AuthAs: Internal
- 着信/発信メッセージ:X-MS-Exchange-Organization-AuthAs: Anonymous

着信/発信メッセージでこのヘッダーに Internal 値が追加されると、高度なフィッシング防御によってそのメッセージは内部メッセージとして扱われ、異なるスコアが付けられるため、高度なフィッシング防御の外部攻撃に対する効果が低下する可能性があります。詳細については、https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/allow-anonymous-relay?view=exchserver-2019 [英語] および https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-inboundconnector?view=exchange-ps [英語] を参照してください。

ステップ 1:ジャーナリングされたメッセージをセンサーにルーティングするコネクタを作成する

ジャーナリングされたメッセージをセンサーにルーティングするには、メッセージのルーティング先となるプレースホルダドメインを作成します。

より複雑な設定がされている場合があります。目標は、ジャーナリング機能からのメッセージが特別なルーティングを受信するように、このコネクタを設定することです。

1. 必要なルールを作成するための適切な管理者権限を持つアカウントを使用して、https://portal.office.com で Office 365 ダッシュボードにログインします。
2. [管理センター(Admin Centers)] > [Exchange] に移動します。
3. [メールフロー(mail flow)] をクリックします。
4. [コネクタ(Connectors)] タブをクリックします。
5. [+] をクリックして新しいコネクタを作成します。
6. [メールフローシナリオの選択(Select your mail flow scenario)] ページで、次の手順を実行します。
   - [差出人(From)] ドロップダウンリストで、[Office 365] を選択します。
   - [宛先(To)] ドロップダウンリストで、[パートナー組織(Partner organization)] を選択します。
7. [次へ(Next)] をクリックします。
8. [新しいコネクタ(New connector)] ページで、次の手順を実行します。
   - コネクタ名とオプションの説明を入力します。「Cisco センサー」など、わかりやすい名前にします。
   - [オンにする(Turn it on)] チェックボックスはオンのままにします。このチェックボックスがオンになっていない場合、コネクタの検証プロセス(このウィザードの後半でアクセス)が失敗するという Microsoft の既知のバグがあります。参照:https://support.microsoft.com/en-us/help/3179588/the-domain-of-the-recipient-is-not-configured-as-part-of-connector-err [英語]
9. [次へ(Next)] をクリックします。
10. [これらのドメインに電子メールメッセージが送信される場合のみ(Only when email messages are sent to these domains)] オプションボタンを選択します。
11. [+] をクリックして新しいドメインを追加します。
12. このコネクタを使用するためにメッセージをリダイレクトするドメインを入力します。営業担当者またはサポート担当者から、ここで入力する情報が提供されます。この情報は、「symbolicname.hosted.appc.cisco.com」の形式で提供されます。symbolicname は、組織で使用されるシンボル名です。
13. [次へ(Next)] をクリックします。
14. [これらのスマートホストを使ってメールをルーティングする(Route email through these smart hosts)] オプションボタンを選択します。
15. [+] をクリックしてスマートホストを追加します。
16. センサーの完全修飾ドメイン名を入力します。
    - cisco.com ホステッド型センサーの場合、これはステップ 12 のアドレスになります。
    - ホストするセンサーの場合、センサーの仮想マシンインターフェイスからセンサーのドメイン名を取得します。
17. [次へ(Next)] をクリックします。

18. センサーへの接続の TLS 設定を行います。次のことをお勧めします。
    - [常にTLSを使用(Always use Transport Layer Security)] チェックボックスをオンにします。
    - [任意のデジタル証明書。自己署名証明書も含まれます(Any digital certificate, including self-signed certificates)] オプションボタンを選択します。(センサーに検証済みの TLS 証明書をインストールしている場合は、[信頼できる認証局(CA)によって発行済み(Issued by a trusted certificate authority (CA))] オプションボタンを選択することができます)
19. [次へ(Next)] をクリックし、確認画面で、もう一度 [次へ(Next)] をクリックします。
20. センサーが到達可能であることを確認します。
21. [+] をクリックします。
22. 前に指定したのと同じプレースホルダドメインを使用する電子メールアドレスを入力します(上の例では、「symbolicname.hosted.appc.cisco.com」)。「@」記号の左側のアドレスのローカル部分は無関係です。任意のアドレスを使用できます。
23. [検証(Validate)] をクリックします。
24. しばらくすると、確認ウィンドウが表示されます。

    検証に失敗した場合は、営業担当者またはサポート担当者に連絡してトラブルシューティングを依頼してください。別のトランスポートルールが優先されたり、検証メッセージを受信した場合、検証が失敗する可能性があります。Microsoft 管理ポータルに遅延がある場合も、検証が失敗することがあります(このような場合は、しばらく待ってから再度検証を試みてください)。
25. [閉じる(Close)] をクリックします。

    失敗した結果の鉛筆アイコンをクリックして、そのテストのログを表示し、設定の問題に対処できます。
26. 両方のタスクに「成功(Succeeded)」と表示されている場合は、[保存(Save)] をクリックします。

コネクタのリストに、新しく作成されたコネクタが表示されます。

ステップ 2:メッセージをセンサーにコピーするジャーナルルールを作成する

最初のジャーナルルールを作成する前に、配信不能レポート(「NDR」または「バウンス」メッセージと呼ばれることもあります)の受信に使用する既存の電子メールアカウントを指定するか、新しい電子メールアカウントを作成する必要があります。このアドレスに送信されるメッセージを定期的に監視して、Office 365 とセンサーをホストしているマシンとの間に接続の問題がないことを確認する必要があります。

ジャーナリング用の新しいアカウントを作成する

1. [アドレスの選択(Select Address)] をクリックします。
2. [受信者(recipients)] をクリックします。
3. [共有(shared)] タブをクリックします。
4. [+] をクリックして、新しい共有メールボックスを作成します。
5. メールボックス情報を入力します。わかりやすい表示名と電子メールアドレスを入力します。たとえば、表示名に「JournalReportNDR」、電子メールアドレスに「journal@yourdomain.onmicrosoft.com」を指定します。必要に応じて、特定のユーザーにアクセスを許可して、この共有メールボックスを監視することができます。必要に応じて、[その他のオプション...(More options...)] を選択して、この共有メールボックスのエイリアスを定義することもできます。
6. [保存(Save)]をクリックします。

ジャーナリングルールを作成する

1. 必要なルールを作成するための適切な管理者権限を持つアカウントを使用して、https://portal.office.com で Office 365 ダッシュボードにログインします。
2. [管理センター(Admin Centers)] > [Exchange] に移動します。
3. [コンプライアンス管理(compliance management)] をクリックします。
4. [ジャーナルルール(journal rules)] タブをクリックします。
5. 配信不能ジャーナルレポートの送信先の値として電子メールアドレスがある場合は、次の手順に進みます。値が、アドレスの選択(Select Address)の場合は、「「ジャーナリング用の新しいアカウントを作成する」(前のページ)」の説明に従って、[アドレスの選択(Select Address)] をクリックして新しいアドレスとして追加し、続行します。
6. [+] をクリックします。
7. ジャーナリングルールの詳細を入力します。
   - [ジャーナルレポートの送信先(Send journal reports to)] フィールドに、「「ステップ 1:ジャーナリングされたメッセージをセンサーにルーティングするコネクタを作成する」 ページ 54」で指定したドメインを使用するアドレスを入力します。たとえば、次のように入力します。「journal@symbolicname.hosted.appccisco.com.」
   - [名前(Name)] フィールドに、「Cisco Sensor」と入力します。
   - [メッセージの送信先または受信元が次の場合(If the message is sent to or received from)] ドロップダウンリストで、次のように選択します。
     - すべてのメッセージを分析のために送信する場合は、[すべてのメッセージに適用(Apply to all messages)] を選択します。

       [外部メッセージ(External Messages)] を選択すると、Office 365 のジャーナリング機能で、内部ドメインからのスプーフィングされた外部メッセージが失われる可能性があります。
     - テスト目的などで、ユーザーベースのサブセットへのメッセージのみを評価する場合は、[特定のユーザーまたはグループ(specific user or group)] でグループを選択します。ここで選択するグループは、Exchange 管理センターの [受信者(recipients)] > [グループ(groups)] セクションで作成する必要があります。配布グループ、セキュリティグループを指定できます。または、新しいメンバーが組織に参加したときや組織を離れたときにグループを変更したくない場合は、動的配布グループを使用できます。
8. [以下のメッセージをジャーナリングします(Journal the following messages)] ドロップダウンリストで、[すべてのメッセージ(All messages)] を選択します。
9. [保存(Save)]をクリックします。
10. 確認メッセージで、[はい(Yes)] をクリックします。

センサーへメッセージフローがすぐに開始されます。

ステップ 3:アラートサーバーをホワイトリストに含める

電子メールが疑わしいと思われる場合、高度なフィッシング防御はオプションで、管理者および疑わしいメッセージの元の受信者、またはどちらか一方に電子メールアラートを送信できます。

脅威となっているメッセージを特定する以外にも、アラート電子メールには、脅威の種類やシビラティ(重大度)に関する追加の情報を含めることができます。運用上の問題が発生した場合、通知サーバーは、センサーおよび高度なフィッシング防御サービスの全体的な健全性に関するアラートを送信することもできます。これらのアラートの重要性と有用性を考慮して、システムがこれらのメッセージをブロックまたは検疫しないようにするため、通知サーバーをホワイトリストに含めることをお勧めします。

たとえば、通知サーバが送信したメッセージに、元のメッセージのコンテンツの一部が含まれることがあります。元のメッセージがスパムを含んでいたり、それ以外でも、電子メールのフィルタリングソフトウェアによって疑わしいと見なされたりする場合があるため、アラート自体が、偶発的に脅威として見なされる可能性があります。

そのため、フィルタリング ソフトウェアの誤検出のトリガーを防ぐために、通知サーバをホワイトリストに含めることが非常に重要です。中間フィルタリング手順がある場合（たとえば、他の中間 MTA、または電子メールをフィルタ処理する他のフィッシング対策ソリューション）、それらも通知サーバをホワイトリストに含めるように設定する必要があります。セールス エンジニア チームと顧客の成功チームが、必要に応じて、ホワイトリストの設定を支援できます。

Office 365 のみを使用している場合は、サーバーをホワイトリストに追加します。Exchange Online Protection も使用している場合は、メールフロールールも追加して、アラートのスパムフィルタリングを防止します。

これらの手順は次のことを対象としています。

（O365 のみ）サーバーを [接続フィルタ（connection filter）] ホワイトリストに追加、および

（O365 および EOP）アラートのスパムフィルタリングを防ぐために「メールフロールール」を追加

アラートサーバーをホワイトリストへ追加

このタスクの目的は、該当する接続フィルタの「IP 許可リスト」を設定することです。通常、これは「デフォルト」接続フィルタです。

1. 必要なルールを作成するための適切な管理者権限を持つアカウントを使用して、https://portal.office.com で Office 365 ダッシュボードにログインします。
2. [管理センター（Admin centers）] > [セキュリティ（Security）] に移動します。
3. [脅威管理（Threat Management）] をクリックします。
4. [ポリシー（Policy）] をクリックします。
5. [スパム対策（Anti-spam）] をクリックします。
6. デフォルトの接続フィルタを選択します。
7. [接続フィルタポリシー（デフォルト）（Connection filter policy (Default)）] をクリックします。
8. [接続フィルタポリシーの編集（Edit connection filter policy）] をクリックします。
9. アラートサーバーの IP アドレス：198.2.132.180 を [次のIPアドレスまたはアドレス範囲からのメッセージを常に許可（Always allow messages from the following IP addresses or address range:）] に入力し、ブロックされた IP アドレスでないことを確認します。
10. IP に関連付けられたポップアップボックスをクリックします。
11. [セーフリストを有効にする（Turn on safe list）] を選択します。
12. [保存（Save）]をクリックします。

デフォルトの接続フィルタの画面右側に [IP許可リスト：設定済み（IP Allow list: Configured）] と表示されていることを確認します

（Cisco のアラートサーバーの IP アドレスは 198.2.132.180 です。Cisco はドメイン「outbound.cisco.com」でこのアドレスの DNS エントリも維持します。一般に、このホワイトリストルールには明示的な IP アドレスを使用することをお勧めします）。

アラートのスパムフィルタリングを防ぐためのメールフロールールを追加する

Office 365 で Exchange Online Protection を使用している場合は、これを行う必要があります。

それぞれのセンサーでこの手順を繰り返します。

1. 必要なルールを作成するための適切な管理者権限を持つアカウントを使用して、https://portal.office.com で Office 365 ダッシュボードにログインします。
2. [管理センター(Admin Centers)] > [Exchange] に移動します。
3. [メールフロー(mail flow)] をクリックします。
4. [ルール(Rules)] タブをクリックします。
5. [+] をクリックし、[スパムフィルタをバイパスする(Bypass spam filtering)] を選択します。
6. フィルタリングルールの詳細を入力します。
    - 「ホワイトリストのアラートサーバー」や「ホワイトリストのセンサー」など、わかりやすい名前を入力します。
    - [このルールを適用する条件(Apply this rule if)] ドロップダウンリストで、[IPアドレスがこれらの範囲内にあるか、または完全に一致(IP address is in any of these ranges or exactly matches)] を選択します。
        1. アラートサーバーの IP アドレスを入力します(この例では 198.2.132.180)。
        2. [+] をクリックして、IP アドレスを追加します。
        3. [OK] をクリックします。
    - [その他のルールの処理を停止する(Stop processing more rules)] チェックボックスがオフになっていることを確認します。メールを正しく処理するには、後続のルールを処理する必要があります。
7. [保存(Save)]をクリックします。

リストにある他のルールの順序を考慮してください。他のルールが配信を妨げないように、ホワイトリストルールをリストの最初に配置するのが理想です。アラートサーバーのホワイトリストルールは、組織へのアラートの配信に影響を与える可能性のある他のルーティングルールよりも前に配置する必要があります。

上図のとおり、アラート サーバの IP アドレスは 198.2.132.180 です。アラートサーバードメインでのアドレスの DNS エントリも維持されますが、一般に、このホワイトリストルールには明示的な IP アドレスを使用することをお勧めします。

デュアル配信の設定:Microsoft Exchange

このセクションでは、ジャーナリングルールを使用して、Microsoft Exchange 環境のデュアル配信を設定する方法について説明します。

Exchange のデュアル配信を設定するステップは、Exchange のすべてのバージョン(2010、2013、2016)で同様ですが、Exchange 管理ユーザーインターフェイスが 2010 バージョンから 2016 バージョンに変更されています。

ジャーナリングに使用する送信コネクタを設定します。Microsoft Exchange では、ジャーナル受信者はメールボックスまたは連絡先にすることができます。連絡先を使用する場合は、プレースホルダドメインを使用して連絡先を定義できます。そうすると、その連絡先を送信コネクタの宛先として使用できます。これにより、何らかの理由でセンサーに到達できない場合、転送キューをバックアップする代わりに、メッセージを dev/null に送信できます。

ほとんどの環境で、プレミアムジャーナリングが必要になります。これには、Microsoft が提供する Exchange Enterprise ライセンスが必要であり、場合によってはサーバーライセンスやクライアント アクセス ライセンス（CAL）が含まれることもあります。プレミアムジャーナリングのライセンスがあると、ジャーナルルールを使用して、受信者とスコープの両方を定義できます。Microsoft は、標準ジャーナリングも提供しています。これは、すべての Exchange サーバー上にあるメールボックスデータベースを対象とした全部かゼロかのジャーナリングです。標準ジャーナリングライセンスのみを保有し、ジャーナリングをすでに別の目的で使用している場合は、Cisco センサーに別のジャーナリングを設定できることがあります。

「デュアル配信の設定：Exchange 2010」下

「デュアル配信の設定：Exchange 2013/2016」ページ 64

「Exchange デュアル配信のテスト」ページ 67

各設定は、次の 3 つの部分からなります。

- プレースホルダドメインを作成する
- そのプレースホルダドメインを使用して連絡先を作成する
- 送信コネクタを作成する

高度なフィッシング防御では、メッセージ方向性に適切な値を設定した X-MS-Exchange-Organization-AuthAs: ヘッダーをすべてのメッセージに追加する必要があります。これを設定する方法については、Microsoft Exchange のドキュメントを参照してください。高度なフィッシング防御が正しく機能するには、次のヘッダーと値が必要です。

- 内部メッセージ：X-MS-Exchange-Organization-AuthAs: Internal
- 着信/発信メッセージ：X-MS-Exchange-Organization-AuthAs: Anonymous

着信/発信メッセージでこのヘッダーに Internal 値が追加されると、高度なフィッシング防御によってそのメッセージは内部メッセージとして扱われ、異なるスコアが付けられるため、高度なフィッシング防御の外部攻撃に対する効果が低下する可能性があります。詳細については、https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/allow-anonymous-relay?view=exchserver-2019 [英語] および https://docs.microsoft.com/en-us/powershell/module/exchange/mail-flow/set-inboundconnector?view=exchange-ps [英語] を参照してください。

デュアル配信の設定：Exchange 2010

プレースホルダドメインの作成：Exchange 2010

1. Exchange 管理コンソールで、[組織の設定] > [ハブトランスポート] に移動します。
2. [リモートドメイン] タブをクリックします。
3. [リモートドメインの新規作成] をクリックします。
4. cisco.sensor と入力します。
5. [次へ] をクリックします。
6. [終了] をクリックします。
7. [適用] をクリックします。
8. [OK] をクリックします。

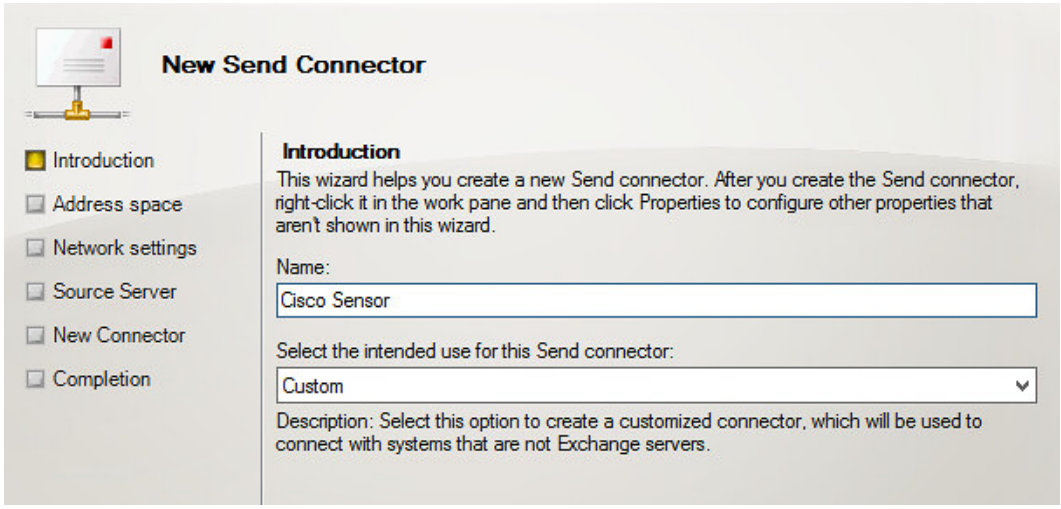
プレースホルダドメインを使用した連絡先の作成：Exchange 2010

1. [連絡先の作成] に移動します。
2. 次の値を入力します。
    - [FirstName]：Cisco
    - [LastName]：Sensor
    - [エイリアス]：Cisco Sensor
    - [外部電子メールアドレス]：journal@cisco.sensor
3. 連絡先を保存します。

送信コネクタの作成：Exchange 2010

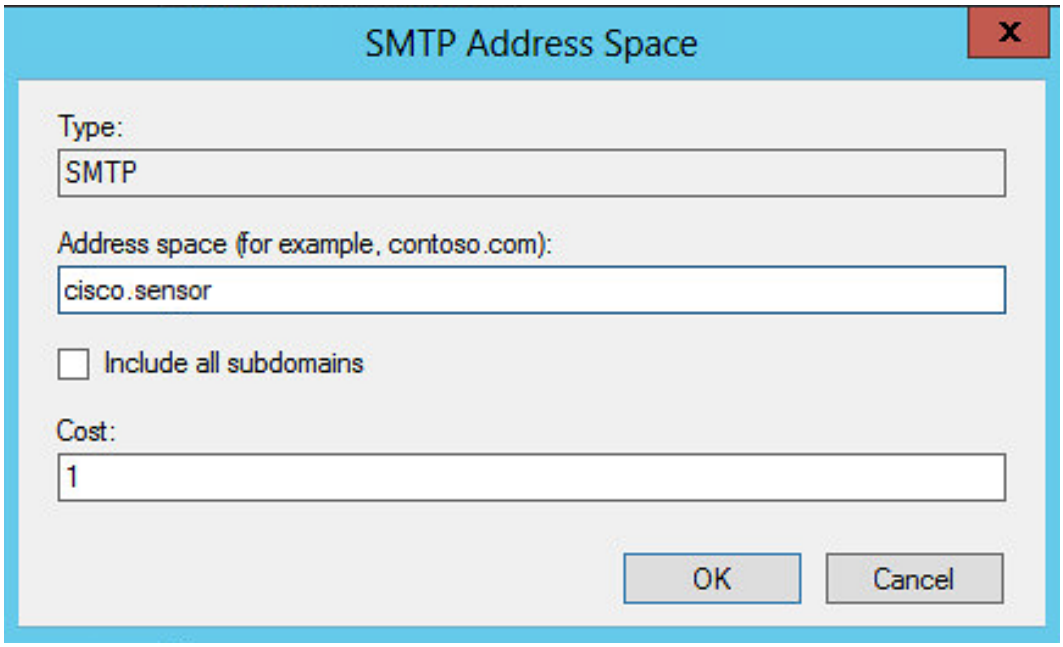
Exchange で送信コネクタのデフォルトを上書きして、最大メッセージサイズを増やす場合は、Agari センサーの最大メッセージサイズもデフォルトの 35MB から最大 100MB（許容される最大量）まで増やしてください。

1. Exchange 管理コンソール（2010）にサインインします。
2. 新しい送信コネクタを作成します。
3. 送信コネクタの詳細を入力/選択します。
    - [名前]：Cisco Sensor
    - [この送信コネクタの使用目的を選択してください]：Custom



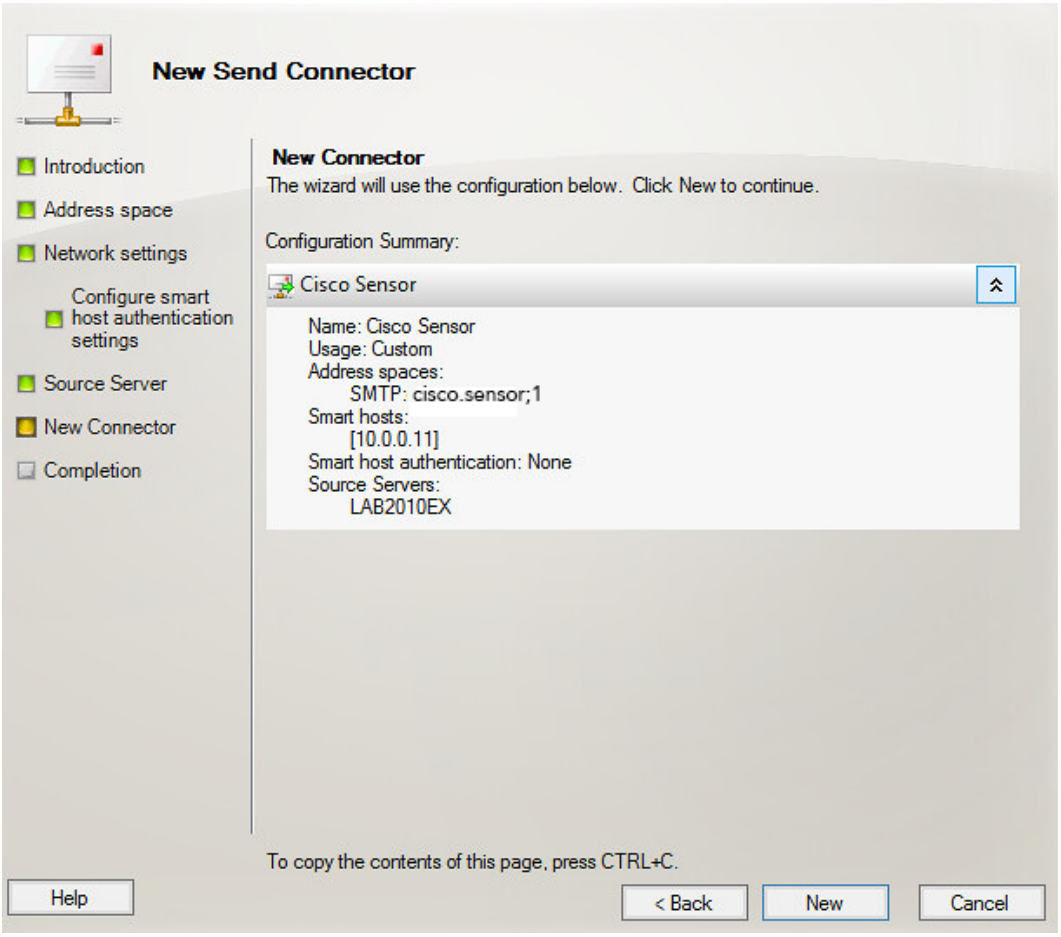
4. [追加] をクリックします。
5. SMTP アドレススペースに関する情報を入力します。
    - [種類]：SMTP（これはデフォルトであり、ここで変更することはできません）
    - [アドレススペース]：cisco.sensor

- [コスト]：1



6. [OK] をクリックします。
7. [次へ] をクリックします。
8. [ネットワーク設定] で、[メールを次のスマートホストを経由してルーティングする] を選択します。
9. [追加] をクリックします。
10. センサーの [IP アドレス] を入力します。
11. [OK] をクリックします。
12. [スマートホスト認証設定の構成] で、[なし] を選択します。
13. [次へ] をクリックします。
14. [送信元サーバー] で、適切な電子メールゲートウェイサーバーが選択されていることを確認してください。
15. [次へ] をクリックします。

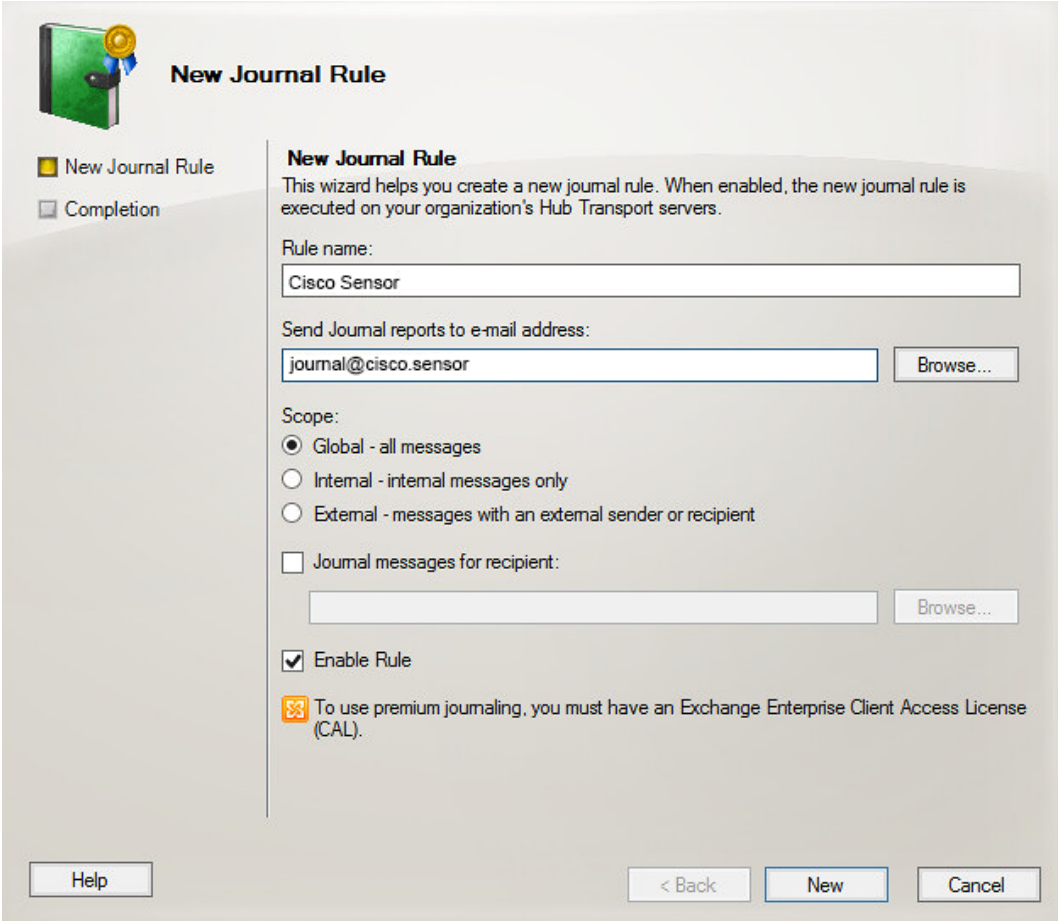
16. 設定を調べて正しいことを確認します。



17. [新規] をクリックします。
18. 新しいジャーナルルールを作成します。
19. ジャーナルルール設定を入力します。
    - ドメインが前のステップに示した送信コネクタと一致していることを確認します。
    - [ルール名]：Cisco Sensor
    - [Send Journal reports to email address]：journal@cisco.sensor
    - [スコープ]：[グローバル - すべてのメッセージ]

      [外部 – 外部の送信者または受信者を持つメッセージ] を選択すると、Exchange ジャーナリング機能が内部ドメインからのメッセージになりすました外部メッセージを見逃す可能性があります。

- [ルールを有効にする] チェックボックスをオンにします。



20. [新規] をクリックします。
21. 設定を調べて正しいことを確認します。
22. [終了] をクリックします。

デュアル配信の設定：Exchange 2013/2016

プレースホルダドメインの作成：Exchange 2013/2016

プレースホルダドメインを作成する機能が 2013/2016 バージョンで Exchange 管理コンソールから削除されたため、これはコマンドラインから行う必要があります。

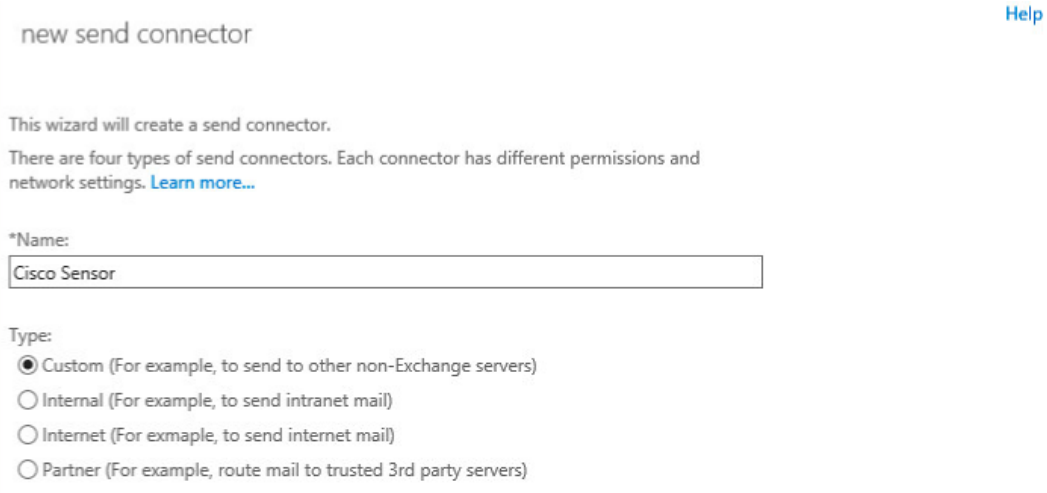
1. Exchange Management PowerShell を開きます。
2. 以下のコマンドを入力します。
    a. プレースホルダドメインを作成します。
    New-RemoteDomain -DomainName cisco.sensor -Name " Cisco APP"
    b. 自動転送を設定します。
    Get-RemoteDomain | Where {$_.DomainName -eq "cisco.sensor"}
    | Set-RemoteDomain -TNEFEnabled $false -AutoForwardEnabled $true
    c. 検証します。
    Get-RemoteDomain | Where {$_.DomainName -eq "cisco.sensor"}
    |Format-table Name, DomainName, TNEFEnabled, AutoForwardEnabled

プレースホルダドメインを使用した連絡先の作成：Exchange 2013/2016

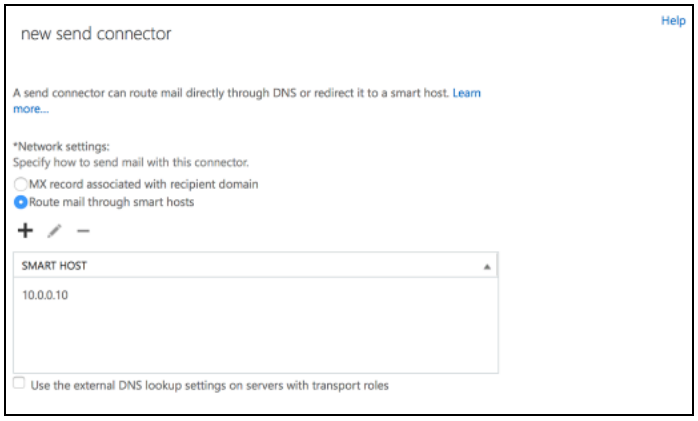
1. [連絡先の作成] に移動します。
2. 次の値を入力します。
    - [FirstName]：Cisco
    - [LastName]：Sensor
    - [エイリアス]：Cisco Sensor
    - [外部電子メールアドレス]：journal@cisco.sensor
3. 連絡先を保存します。

送信コネクタの作成：Exchange 2013/2016

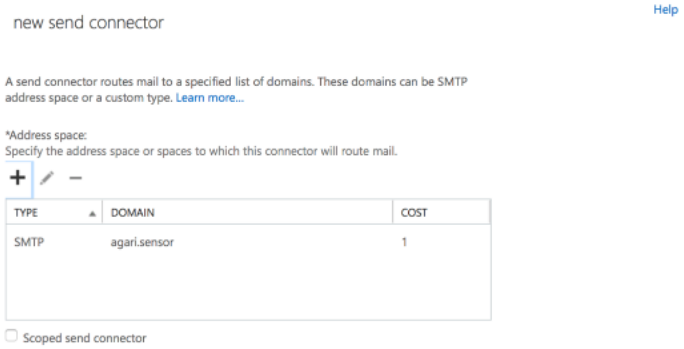
1. Exchange 管理センター（2013/2016）にサインインします。
2. 新しい送信コネクタを作成します。
3. 送信コネクタの詳細を入力/選択します。
    - [名前]：Cisco Sensor
    - [種類]：[カスタム]



4. [次へ] をクリックします。
5. [ネットワーク設定] で、[メールを次のスマートホストを経由してルーティングする] を選択し、センサーの IP アドレスを追加します。

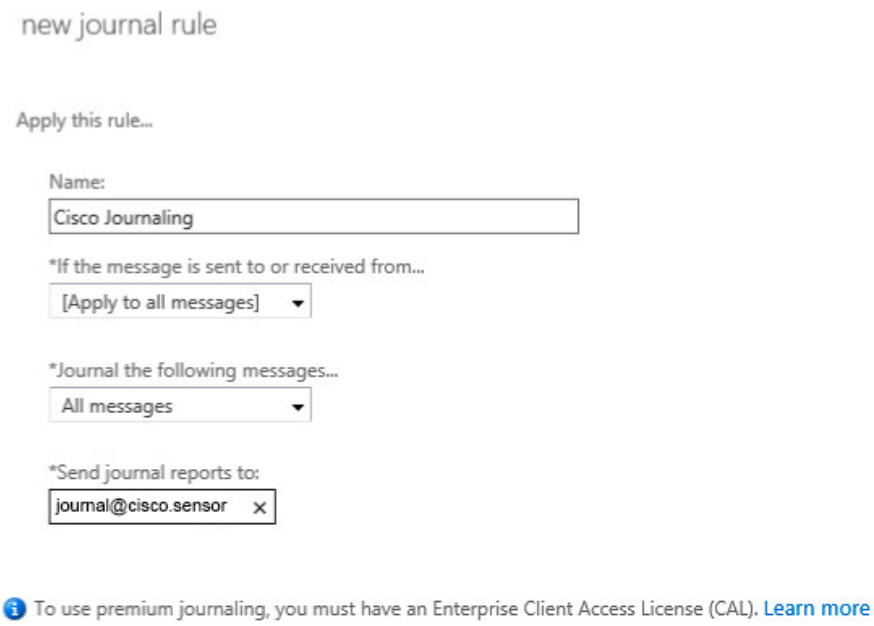


6. [次へ] をクリックします。
7. [スマートホスト認証設定の構成] で、[なし] を選択します。
8. [次へ] をクリックします。
9. [アドレススペース] に、cisco.sensor と SMTP を入力します。



10. [次へ] をクリックします。
11. [送信元サーバー] で、適切な電子メールゲートウェイサーバーが選択されていることを確認してください。
12. [OK] をクリックします。
13. 新しいジャーナルルールを作成します。
14. ジャーナルルール設定を入力します。
    - [ジャーナルレポートの送信先]：journal@cisco.sensor
    - [名前]：Cisco Journaling
    - [メッセージの送信先または受信元が次の場合]：[すべてのメッセージに適用]
    - [Journal the following]：[すべてのメッセージ]

      [External Messages] を選択すると、Exchange ジャーナリング機能が内部ドメインからのメッセージになりすました外部メッセージを見逃す可能性があります。



15. [保存] をクリックします。

Exchange デュアル配信のテスト

1. 組織/ネットワークの外部からいずれかのユーザーにテストメッセージを送信します。
2. 高度なフィッシング防御でメッセージが取り込まれたことを確認します。

デュアル配信の設定：Cisco ESA

このセクションでは、Cisco E メール セキュリティ アプライアンス（旧 IronPort）環境から Cisco 高度なフィッシング防御 センサーへのデュアル配信を設定する方法について説明します。

全般的な手順は次のとおりです。

ステップ 1：Cisco ESA で SPF/DKIM/DMARC チェックを有効にする。

ステップ 2：Bcc: アクションを使用してメッセージをセンサーにコピーするコンテンツフィルタを作成する。

ステップ 3：配信済みのメールのみ（スパムや PVO（ポリシー、ウイルス、アウトブレイク）で隔離されたメールは対象外）がセンサーにコピーされるように、そのフィルタを参照する適切なメールポリシーを設定する。

ステップ 4：予期しない配信の失敗を適切に管理するためのバウンス処理を設定する。

ステップ 5：任意の目的のシステムアラートが問題を管理者に通知するように設定されていることを確認する。

ステップ 6：その他のホワイトリストに含める電子メールストリームを検討する。

ステップ 7：自身と自身のユーザーが確実にアラートを受信するように、アラートサーバーをホワイトリストに登録する。

「Authentication-Results」ヘッダーに関する重要な考慮事項

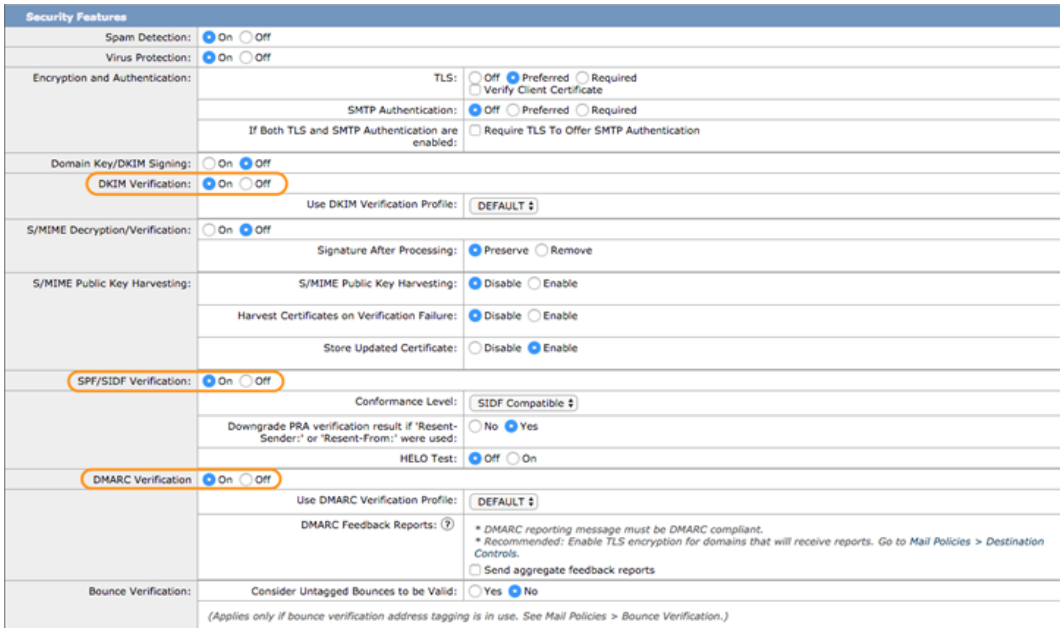
センサーは、送信側のアイデンティティの評価に役立つ、正確で破損していない Authentication-Results ヘッダーに依存しています。通常、企業の「境界」MTA（つまり、インターネット上の送信側 MTA から企業への最初の侵入ポイント）が、受信メッセージを評価し、Authentication-Results ヘッダーを追加します。このヘッダーの整合性を保持するように施設内のダウンストリーム MTA を慎重に設定します（つまり、正確な情報で上書きできない限り、ヘッダーを自身のヘッダーで上書きすることはできず、メッセージからヘッダーを取り除くこともできません）。

ただし、メール ルーティング環境が複雑になる場合があり、各ダウンストリーム MTA のヘッダーの整合性を確保することが、常に実用的であるとは限りません。この状況を簡素化するため、センサーは、X-Agari-Authentication-Results と呼ばれるヘッダーの重複を最初に検出します。何も見つからない場合は、Authentication-Results ヘッダーにフォールバックします。

これによって、代替名で Authentication-Results ヘッダーを作成（複製）するように境界 MTA を設定できます。そのため、破損せずに、さまざまなダウンストリーム MTS を経由させることができる可能性が高くなります。このガイドでは、さまざまな MTA 製品に対して、これを実行する方法について説明しています。

ステップ 1：Cisco ESA で SPF/DKIM/DMARC チェックを有効にする

1. [メールポリシー（Mail Policies）] > [メールフローポリシー（Mail Flow Policies）] に移動します。
2. [デフォルト ポリシー パラメータ（Default Policy Parameters）] をクリックします。
3. [DKIM検証（DKIM Verification）]、[SPF/SIDF検証（SPF/SIDF Verification）]、[DMARC検証（DMARC Verification）] のいずれも、[オン（On）] に設定されていることを確認します。関連する設定を次に示したとおりにします。



[DKIM検証（DKIM Verification）]、[SPF/SIDF検証（SPF/SIDF Verification）]、[DMARC検証（DMARC Verification）] のいずれの設定も、Cisco ESA に正しく設定されています。

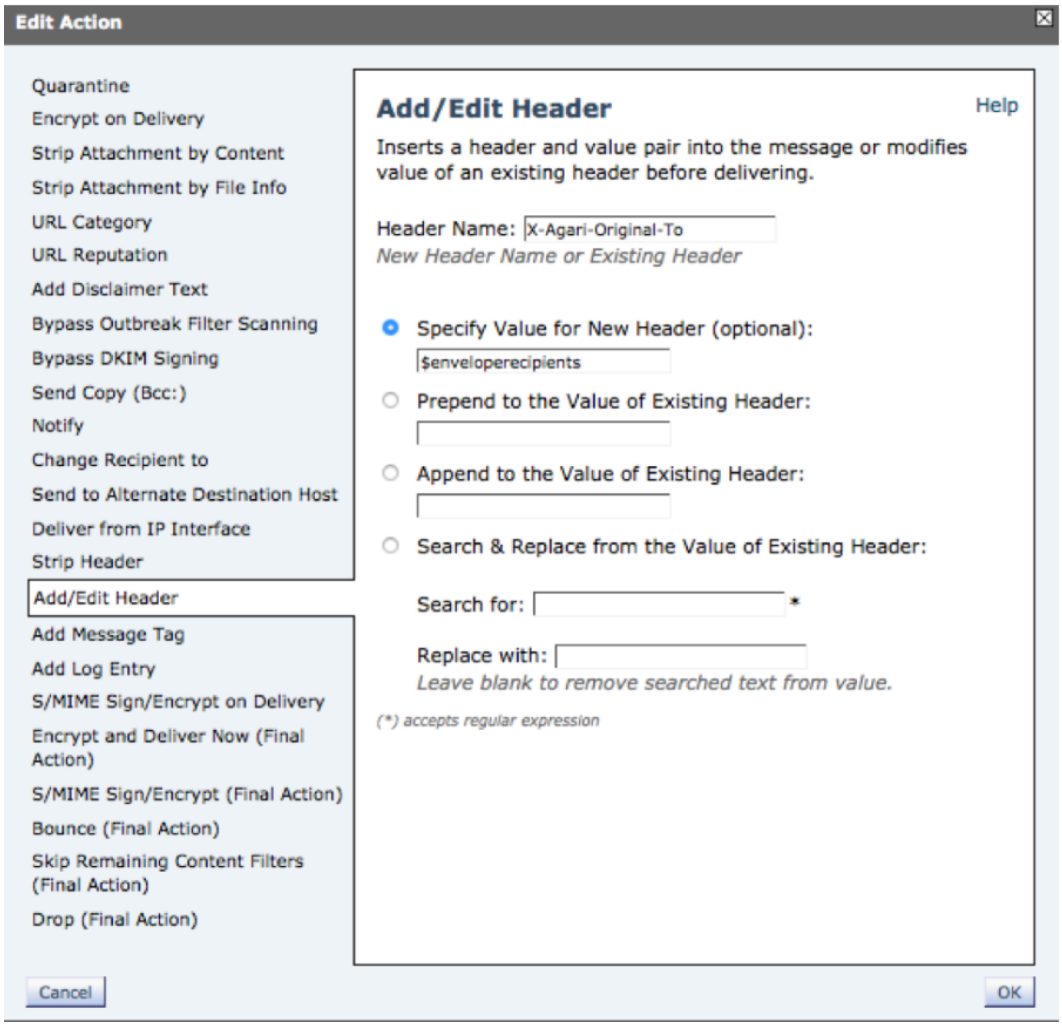
ステップ 2：Bcc: フィルタを作成してメッセージを転送する

1. Cisco ESA（E メール セキュリティ アプライアンス）に管理者ユーザーとしてログインします。
2. [メールポリシー（Mail Policies）] > [受信コンテンツフィルタ（Incoming Content Filters）] に移動します。

クラスタ管理用に Cisco ESA 環境が設定されている場合：アクションの目的が、E メール セキュリティ アプライアンス（ESA）インスタンスの特定のセットにのみ影響を及ぼすことである場合は、トップクラスタレベルまたはサブグループレベルのいずれかで次の手順を完了する必要があります。

3. [フィルタを追加（Add Filter）] をクリックし、フィルタに「Cisco_sensor」などのわかりやすい名前を付けます。
4. [説明（Description）] フィールドに、将来の管理者がフィルタ処理の対象と連絡先を把握できるように説明を入力します。例：「これは、メッセージの BCC ストリームをセンサーに送信するためのフィルタで、メッセージヘッダーと認証データの特定の側面を保存して通信します。ご質問がある場合は、joeadmin@example.com で Joe 管理者に問い合わせてください」
5. センサーがエンドユーザーに配信される予定のすべてのメッセージを受信できるように、すべてのスパムおよびウイルスのスキャンが実行された後と、メッセージを廃棄するその他のメッセージ フィルタリング ポリシーの後で、フィルタを順序付けします。コンテンツフィルタの「マスターリスト」でフィルタがすぐに配信をトリガーしたり、後続のフィルタを回避したりするその他の高度なフィルタリングを使用している場合は、ユーザーに配信されるすべてのメッセージのコレクションという目的の結果が得られるように、これらのフィルタリングを考慮して、センサーフィルタを適切に配置する必要があります。
6. 必要に応じて、コンテンツフィルタに条件を追加します。環境によっては、フィルタを、特定の受信者またはドメインの特定の着信メール ポリシー（これらの手順で後述）に関連付けることができます。スパム対策やウイルス対策で陽性となったメッセージが廃棄される（およびユーザーに配信されない）フィルタリングロジックがある場合は、センサーフィルタが合致しないように、フィルタに条件を含める必要があります。それ以外の場合は、コンテンツフィルタへの条件の追加をスキップできます。そうすると、どのメッセージに対しても「True」と評価されます。ここでも、コンテンツフィルタの目的は、エンドユーザーに直接配信される予定のメッセージに対してのみ動作することです。
7. メッセージにヘッダーを追加するアクションを追加します。X-Agari-Original-From と X-Agari-Original-To をメッセージに追加します。Cisco ESA が境界ゲートウェイの場合は、X-Agari-Authentication-Results ヘッダーも追加します。アクションごとに 1 つのヘッダーを追加するため、アクションごとに次のサブステップを繰り返します。
    a. [アクションを追加（Add Action）] をクリックします。
    b. [アクションの追加（Add Action）] ダイアログボックスで、[ヘッダーの追加/編集（Add/Edit Header）] を選択します。
    c. 次の表に従って、[ヘッダー名（Header Name）] 値を入力します。
    d. [新しいヘッダーの値を指定（Specify Value for New Header）] を選択し、次の表に従って値を入力します。
    e. 入力ミスがないか、名前を二重にチェックします。
    f. [OK] をクリックします。

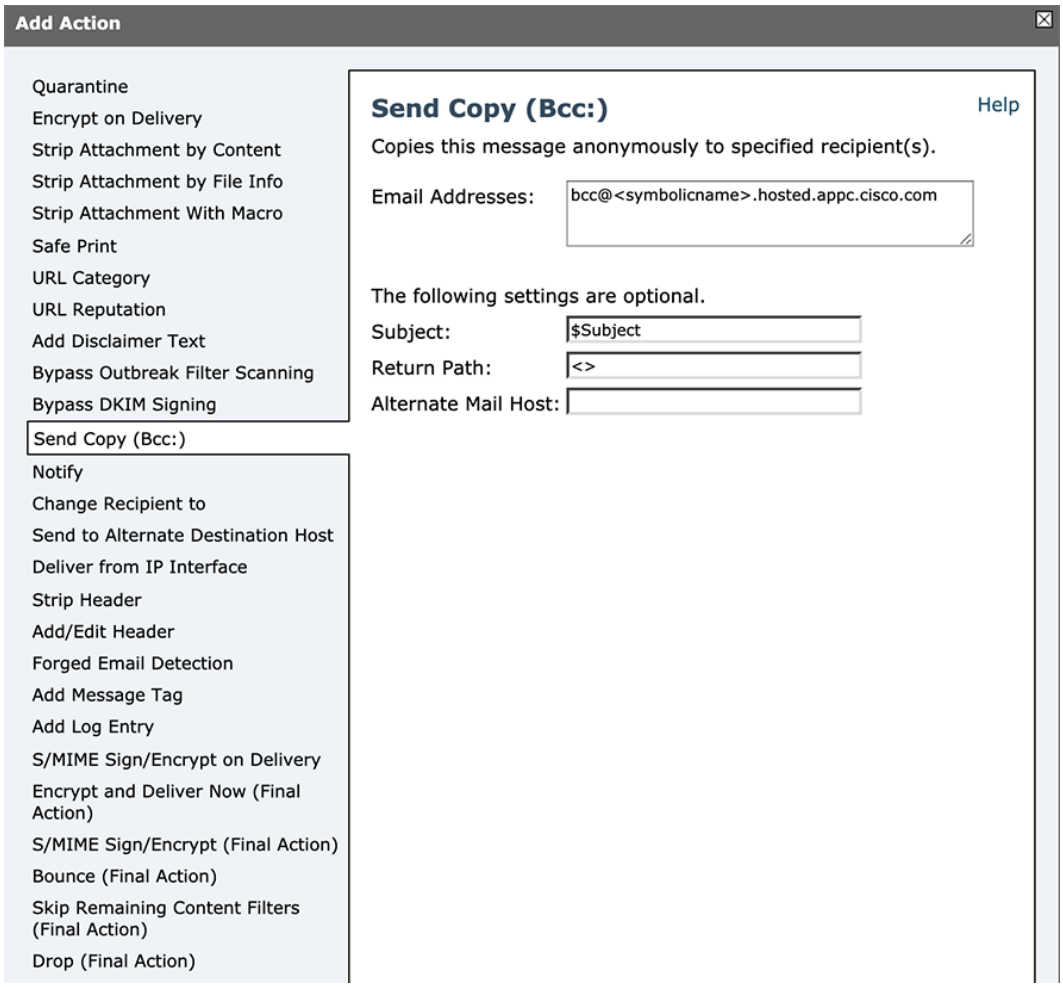
[ヘッダー名（Header Name）] 値	[新しいヘッダーの値を指定（Specify Value for New Header）] 値
X-Agari-Original-From	$EnvelopeFrom
X-Agari-Original-To	$enveloperecipients
X-Agari-Authentication-Results	$Header['Authentication-Results'] Cisco ESA が境界ゲートウェイ MTA である場合にのみ、このヘッダーを追加します。



X-Agari-Original-To ヘッダーのコンテンツ フィルタ アクションの例。

8. このフィルタのプライマリアクションを作成します。つまり、センサーへのメッセージ全体を BCC します。
    - BCC アクションの電子メールアドレスは次のようにする必要があります。
        - [username]@[symbolic_name].hosted. Cisco .com（Cisco がホストするセンサーの場合）
        - [username]@[sensor_IP_address]（センサーが独自のインフラストラクチャにある場合）
    - Bcc: メッセージの件名は元のものと同じにする必要があります。そのため、[件名（Subject）] フィールドは「$Subject」のままにします。
    - [リターンパス（Return Path）] エントリは、最初に適切なアドレスに設定する必要があります。そのアドレスで、バウンスが全体的に無視されるか、センサーへの配信の失敗が監視されるかのいずれかになります。[リターンパス（Return Path）] フィールドは空白のままにしないでください。空白のままにすると、センサーへの配信で問題が生じた場合に、元のメッセージ送信者にメッセージが戻される場合があります。設定した配信が正しく動作していることを確認したら、後から、[リターンパス（Return Path）] エントリを「<>」に変更できます。これにより、明らかな配信の失敗はすぐに配信キューから削除されます。
    - Bcc 電子メールアドレスに指定したドメインでは、メッセージが適切な目的の宛先に配信されない場合、[代替メールホスト（Alternate Mail Host）] エントリを使用できます。この設定の結果、電子メール

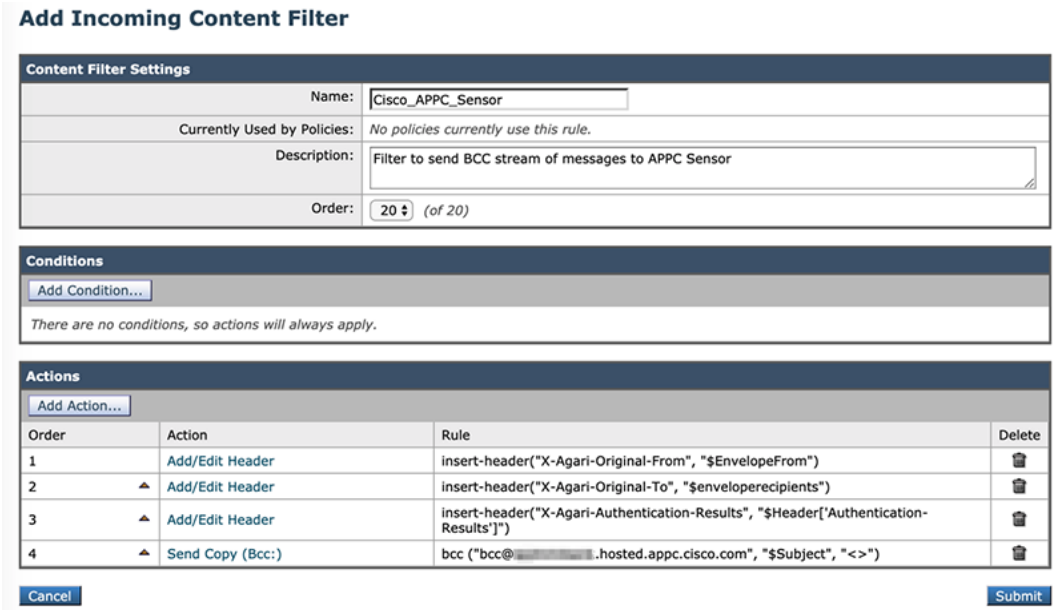
アドレスまたは Cisco ESA の「SMTP ルート」機能の MX レコードで指定されたものに対してではなく、指定したホストに対して直接配信が試行されます。つまり、このフィールドを使用して、センサーのホストまたは IP アドレスを直接指定できます（IP アドレスは角括弧で囲む必要があります。例：[123.123.45.67]）。上記で指定した電子メールアドレスで使用されるドメインは、以下で説明するとおり、引き続きバウンス処理に関連する点に注意してください。



Bcc: アクション

9. [OK] をクリックします。

   次の例は、上記のコンテンツ フィルタの定義（[送信（Submit）] のクリック前）を示しています。

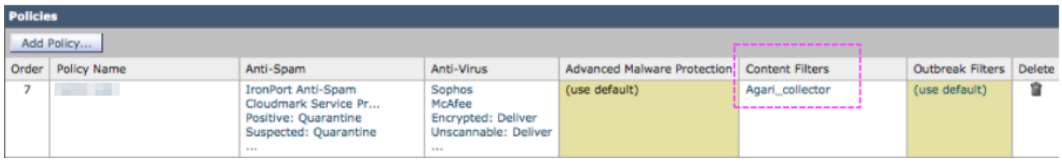


コンテンツフィルタの概要

上図は、追加された X-Agari-Authentication-Results ヘッダーを示しています。このヘッダーは、Cisco ESA MTA が境界ゲートウェイ MTA の場合にのみ、追加する必要があります。Cisco ESA MTA が境界ゲートウェイのダウンストリームの場合は、このヘッダーを追加しないでください。

10. [送信(Submit)]をクリックして新しいフィルタを保存します。
11. フィルタを適切なすべての着信メールポリシーに関連付けます。
    a. [メールポリシー(Mail Policies)]>[受信メールポリシー(Incoming Mail Policies)]に移動します。
    b. 適切な行の[コンテンツフィルタ(Content Filters)]列で、新たに作成されたフィルタを参照する(有効にする)ように、割り当てられたコンテンツフィルタを編集します。場合によっては、プロセス内でそのポリシーのコンテンツフィルタを完全に有効にする必要があります。

変更された[ポリシー(Policy)]行は、次のようになります。



コンテンツフィルタが含まれているポリシー行

ポリシーに従ってエンドユーザーに電子メールを配信する場合(およびメッセージを隔離フォルダに配置したり、メッセージを削除したりしない場合)、そのポリシーではセンサーにメッセージを BCC するためのコンテンツフィルタを参照する必要があります。センサーは、配信したすべてのメッセージの BCC コピーを取得する必要があります。一方、ドロップまたは隔離されたスパムメールやウイルスメールを取得する必要はありません。

12. [変更を確定(Commit Changes)]をクリックします。

変更を確定後に、メールがセンサーにルーティングし始める点に注意してください。メッセージのバウンスで問題がある場合は、システムに負荷がかかることがあります。代わりに、次のセクションのバウンス処理手順を完了するまで、変更の確定を待機することができます。

ステップ 3:隔離されたメッセージがセンサーにコピーされないようにする

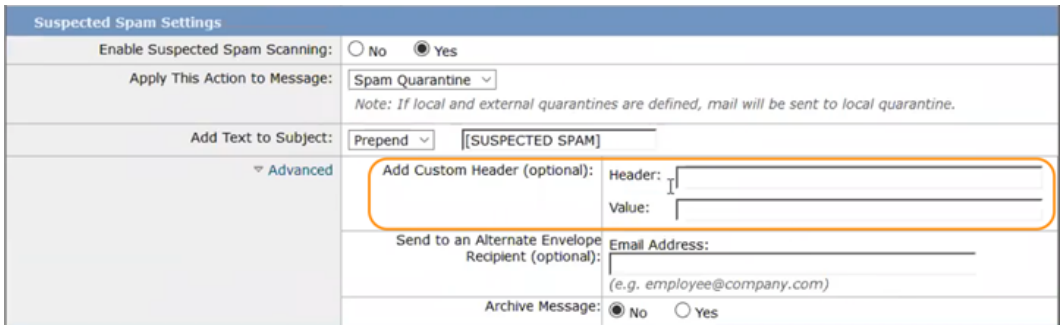
スパム、ウイルス、グレイメールのほか、ポリシーで隔離した同様のメッセージは、Cisco センサーに送信しないでください。こうして隔離されたメッセージが上記の手順で作成した BCC コンテンツフィルタの影響を受けないようにするには、隔離されたさまざまなタイプのメッセージに固有のヘッダーを挿入するアクションを受信メールポリシーに追加します。そうしたヘッダーのいずれかが存在すれば、メッセージをコンテンツフィルタでトリガーせず、センサーにコピーしないようにするための条件として使用されます。

メッセージをスパムとして識別するためのカスタムヘッダーをメッセージに追加しないようにポリシーを設定している場合は、除外するメッセージをフィルタ条件で適切に識別できるように、このフィルタがアタッチされるポリシーを変更することもできます。

このフィルタを使用するポリシーの変更

ポリシーに 1 つ以上のカスタムヘッダーが追加されます。ここでの目的は、スパムと隔離メッセージを識別するために使用すると定義したポリシーに対してこのアクションを実行することです。

1. [メールポリシー(Mail Policies)] > [受信メールポリシー(Incoming Mail Policies)] に移動します。
2. 編集するポリシーの行で、スパム対策(スパムの場合)、ウイルス対策、高度なマルウェア防御、グレイメール(隔離されたメッセージの場合)のいずれかの設定をクリックします。
3. [詳細設定(Advanced)] をクリックします。(変更する設定によっては、対象の設定が [サスペクトスパムの設定(Suspected Spam Settings)]、[ウイルス感染したメッセージ(Virus Infected Messages)]、[バルクメールに対するアクション(Action on Bulk Email)] のいずれかのセクションに存在する可能性があります)



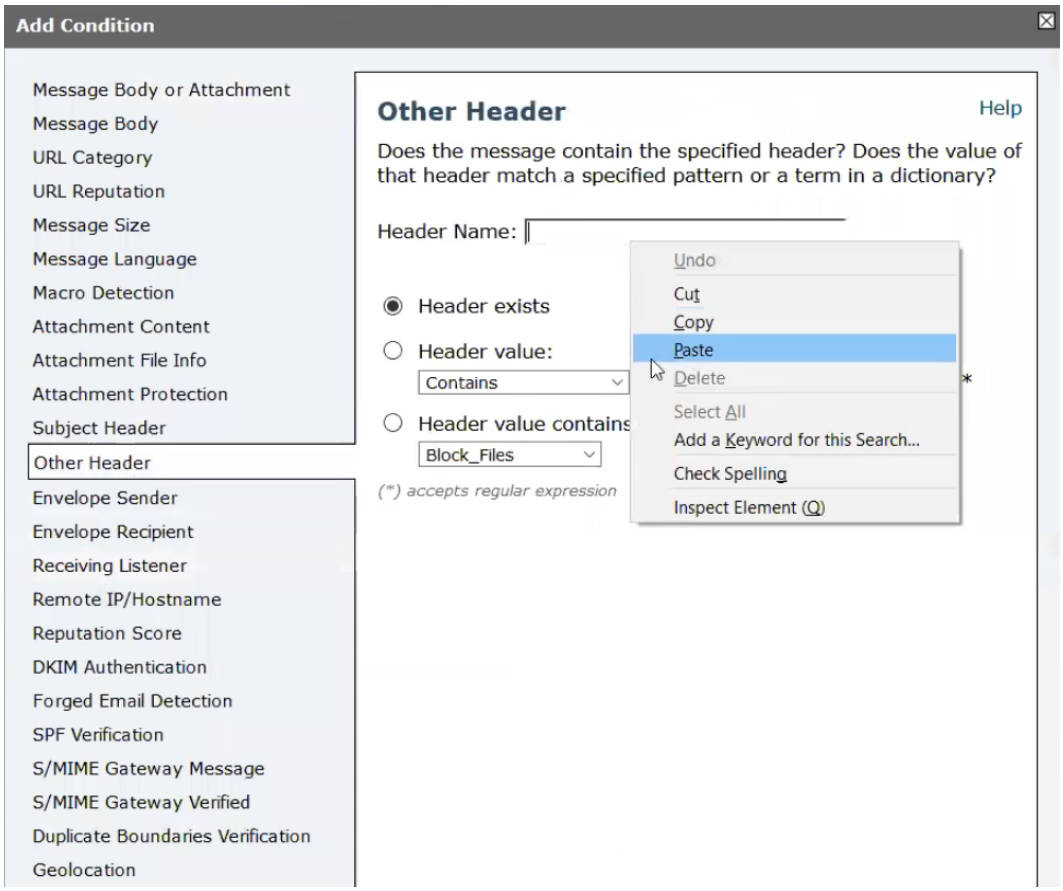
4. [カスタムヘッダーの追加(Add Custom Header)] セクションで、[ヘッダー(Header)] と [値(Value)] の値を入力します。ヘッダーは、一意かつ自明である必要があります。たとえば、スパムであれば、*MyCompany_suspected_spam* というようにします。値は、使用する語彙にとって意味のあるもの(*positive* や *true* など)にします。
5. [ヘッダー(Header)] の値は、次のセクション「「フィルタへの条件の追加」 下」で使用できるように書き留めておきます。
6. [送信(Submit)] をクリックします。

メッセージを隔離するすべてのスパムポリシー、ウイルス対策ポリシー、グレイメールポリシーに対して繰り返します。

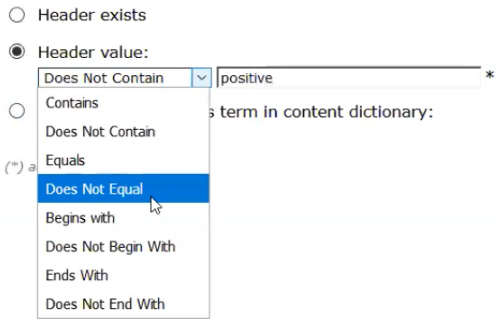
スパムを識別するときにメッセージ件名を変更するようにポリシーを設定することもできます。たとえば、企業によっては、識別したスパムメッセージの先頭に [SUSPECTED SPAM] を付加するようにスパムルールを設定する場合もあります。メッセージ件名の変更に一致するようにポリシー条件を設定できますが、これは複雑な作業であり、長い時間がかかることがあります。ヘッダー値の方が迅速で信頼性が高くなります。

フィルタへの条件の追加

1. [メールポリシー(Mail Policies)] > [受信メールフィルタ(Incoming Mail Filters)] に移動します。
2. ステップ 1 で作成したフィルタの名前をクリックします。
3. [条件を追加(Add Condition)] をクリックします。
4. [その他のヘッダー(Other Header)] をクリックします。
5. [ヘッダー名(Header Name)] フィールドに、「「このフィルタを使用するポリシーの変更」(前のページ)」で作成したカスタムヘッダーの名前を入力します。

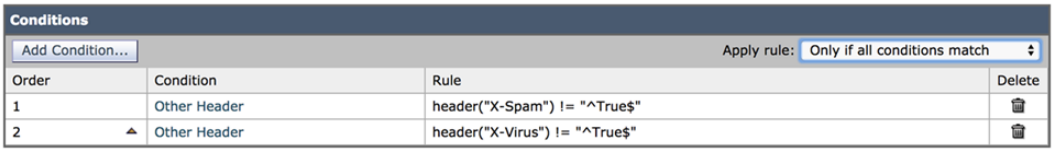


6. [ヘッダー値(Header Value)] ドロップダウンリストで、[等しくない(Does Not Equal)] を選択し、先ほど作成したカスタムヘッダーの値を入力します。



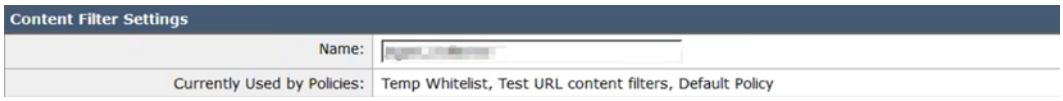
7. [OK] をクリックします。

8. 「「このフィルタを使用するポリシーの変更」 ページ 73」で追加したすべてのヘッダーに対してステップ 3 ～ 7 を繰り返します。
9. [ルールの適用(Apply Rule)]ドロップダウンリストで、[すべての条件が一致した場合のみ(Only if all conditions match)]を選択します。



10. [送信(Submit)]をクリックします。

ステップ 1 で、bcc: を介して Cisco センサーにコピーを送信するようにこのコンテンツフィルタを設定したことを思い出してください。この条件により、bcc: を介して Cisco センサーにコピーを送信するようにこのディレクティブが変更されます。ただし、スパムとして識別されたために存在するメッセージにカスタムヘッダーがある場合を除きます。



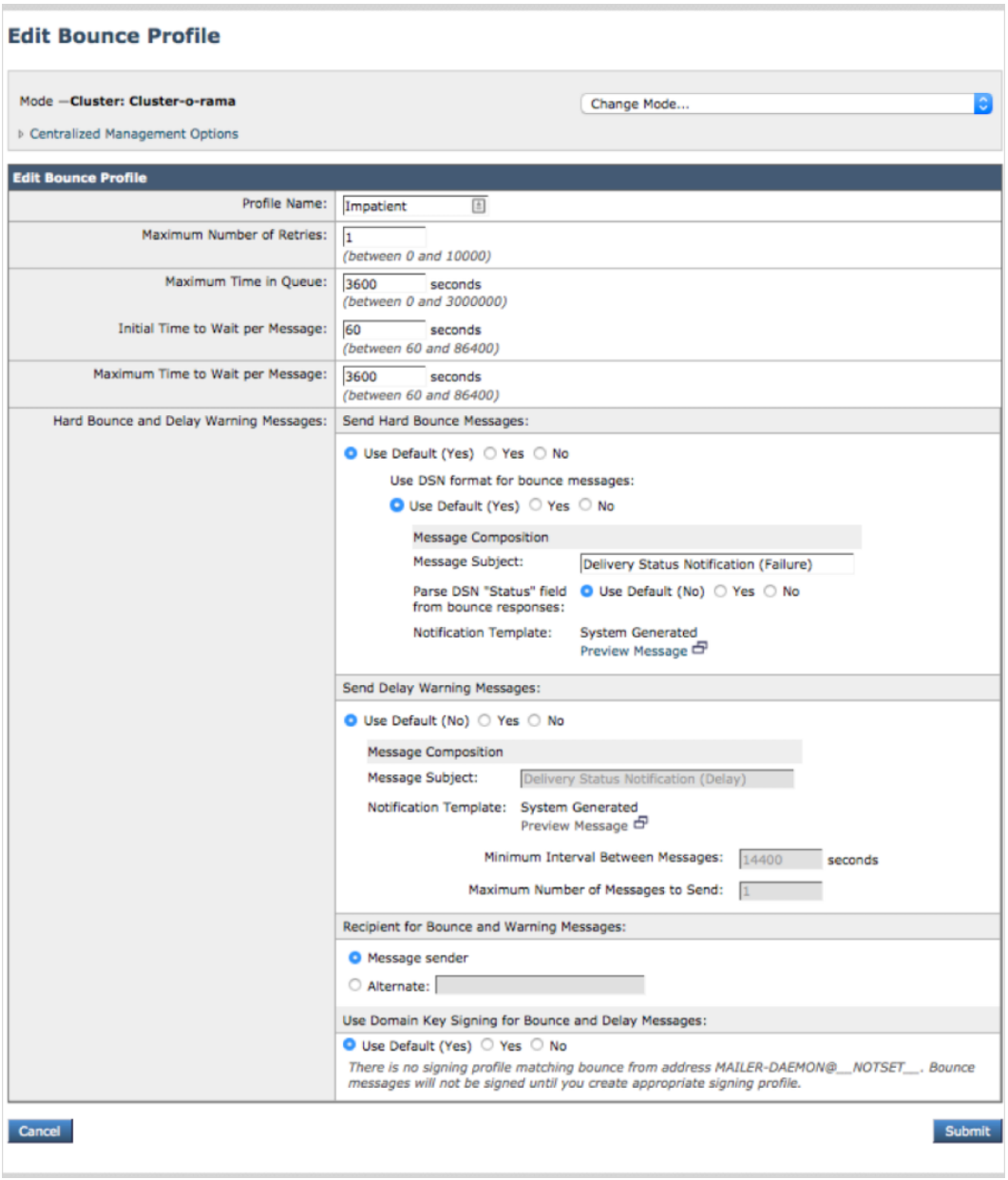
このコンテンツフィルタを使用するポリシー。

このコンテンツフィルタをポリシーで使用する場合は、そのポリシーでこのフィルタが参照され、有効になっている必要があることに注意してください。コンテンツフィルタで使用されるカスタムヘッダーを追加したポリシーに、そのコンテンツフィルタが含まれ、アクティブになっていることを確認します。

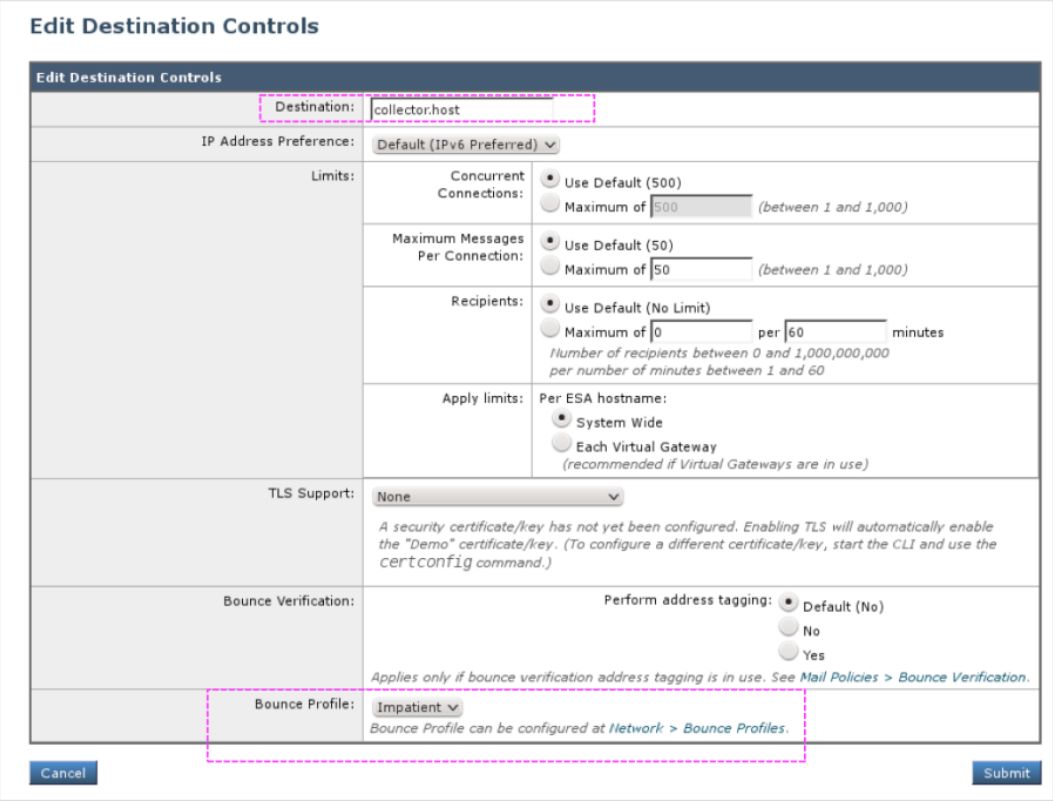
ステップ 4:センサーに対するバウンス処理を設定する

使用する EAS システムリソースを最小限に抑えるには、センサーへの配信が失敗したらすぐにバウンスメッセージが失敗するようにシステムを設定する必要があります。

1. 宛先ホストが受け入れる一意のドメインまたはサブドメイン内の Bcc: 配信先電子メールアドレスを入力します。[代替メールホスト(Alternate Mail Host)]配信アクションは、そのサーバー宛てのメッセージを処理します。そのため、電子メールアドレスのドメインに固有の DNS エントリを作成する必要はありません。この例では、ドメインに「symbolic_name.hosted.appc.cisco.com」を使用します。
2. バウンス メッセージを迅速に失敗させるためのバウンス プロファイルを作成します。
    1. [ネットワーク(Network)]>[バウンスプロファイル(Bounce Profiles)]に移動します。
    2. [バウンスプロファイルを追加(Add Bounce Profile)]をクリックして、新しいエントリを作成します。
    3. 次の図に示すように値を入力します。



3. 前述した一意のセンサードメインに固有の送信先コントロールを作成します（この例では、「symbolic_name.hosted.appc.cisco.com」）。この送信先コントロールは、前のステップで作成したアグレッシブ バウンス プロファイル（この例では、「Impatient」という名前）を参照します。
    1. [メールポリシー（Mail Policies）] > [送信先コントロール（Destination Controls）] に移動します。
    2. 次の図に示すように値を入力します。



4. 保護されたネットワーク内にセンサーが存在せず、センサー宛てのメールストリームを暗号化する場合は、[TLSサポート(TLS Support)]オプションを[必須(Required)]に変更できます。これで、Cisco ESAはリモートセンサーに(「STARTTLS」を介してポート 25 で)安全に接続されます。
5. [変更を確定(Commit Changes)]をクリックします。

ステップ 5:システムアラートを確認する

[システム管理(System Administration)]>[アラート(Alerts)]に移動し、デュアル配信のセットアップと構成に問題がある場合に、システムアラートとハードウェアアラートがモニタリング対象のアドレスに送信されることを確認します。

ステップ 6:他にホワイトリストに登録する電子メールストリームがないか検討する

Cisco ESA にメールを送信しているアップストリーム MTA をホワイトリストに登録するファイアウォールルールを設定できます。これは通常、メッセージを配信し、後続のコンテンツフィルタをスキップするホストアクセステーブル(HAT)によって実現されます。このドキュメントで説明しているようにデュアル配信が設定されていると仮定すると、このようなメッセージはセンサーへのコピーが失敗します。デュアル配信メカニズムがコンテンツフィルタの一部であり、電子メールパイプラインで後から評価されるためです。

この問題の対処方法は着信電子メールフローの仕様によって異なりますが、その 1 つに、ホストアクセステーブルではなくコンテンツフィルタを使用して、着信トラフィックをホワイトリストに登録する方法があります。また、次のようなコンテンツフィルタルールを作成することもできます。送信者の IP アドレスで照合し、センサーにコピーを送信して(このドキュメントで説明しているものと同じ設定を使用します)、これ以上フィルタは使用せずに([残りのコンテンツフィルタをスキップ(Skip Remaining Content Filters)]アクションを使用)メッセージの配信をトリガーするというルールです。その後、送信側 IP に該当する HAT エントリを非アクティブ化することができます。

ステップ 7:アラートサーバーをホワイトリストに含める

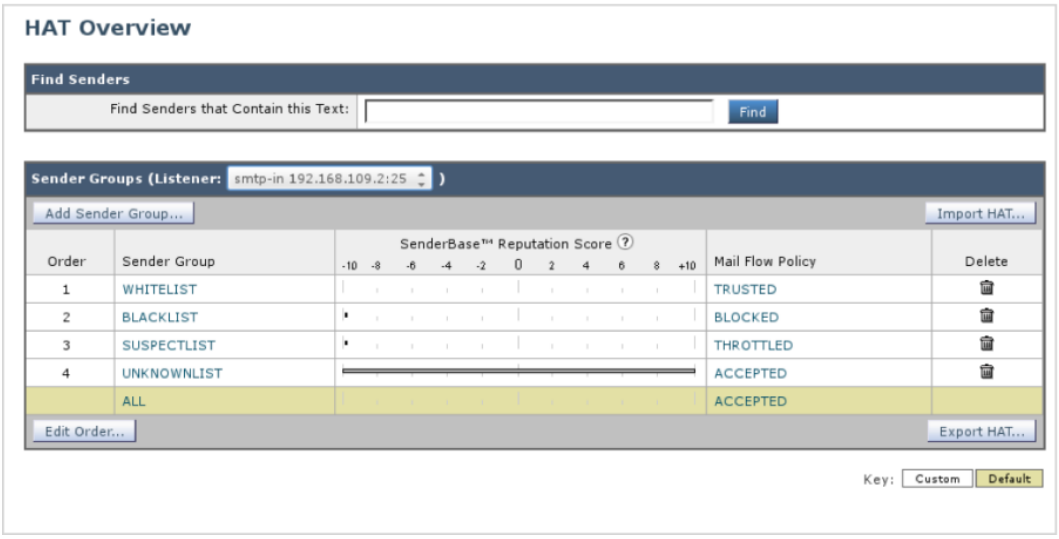
電子メールが疑わしいと思われる場合、高度なフィッシング防御はオプションで、管理者および疑わしいメッセージの元の受信者、またはどちらか一方に電子メールアラートを送信できます。

脅威となっているメッセージを特定する以外にも、アラート電子メールには、脅威の種類やシビラティ（重大度）に関する追加の情報を含めることができます。運用上の問題が発生した場合、通知サーバーは、センサーおよび高度なフィッシング防御サービスの全体的な健全性に関するアラートを送信することもできます。これらのアラートの重要性と有用性を考慮して、システムがこれらのメッセージをブロックまたは検疫しないように確保するため、通知サーバをホワイトリストに含めることをお勧めします。

たとえば、通知サーバが送信したメッセージに、元のメッセージのコンテンツの一部が含まれることがあります。元のメッセージがスパムを含んでいたり、それ以外でも、電子メール フィルタリング ソフトウェアによって疑わしいと見なされたりする場合があるため、アラート自体が、偶発的に脅威として見なされる可能性があります。

そのため、フィルタリング ソフトウェアの誤検出のトリガーを防ぐために、通知サーバをホワイトリストに含めることが非常に重要です。中間フィルタリング手順がある場合（たとえば、他の中間 MTA、または電子メールをフィルタ処理する他のフィッシング対策ソリューション）、それらも通知サーバをホワイトリストに含めるように設定する必要があります。セールス エンジニア チームと顧客の成功チームが、必要に応じて、ホワイトリストの設定を支援できます。

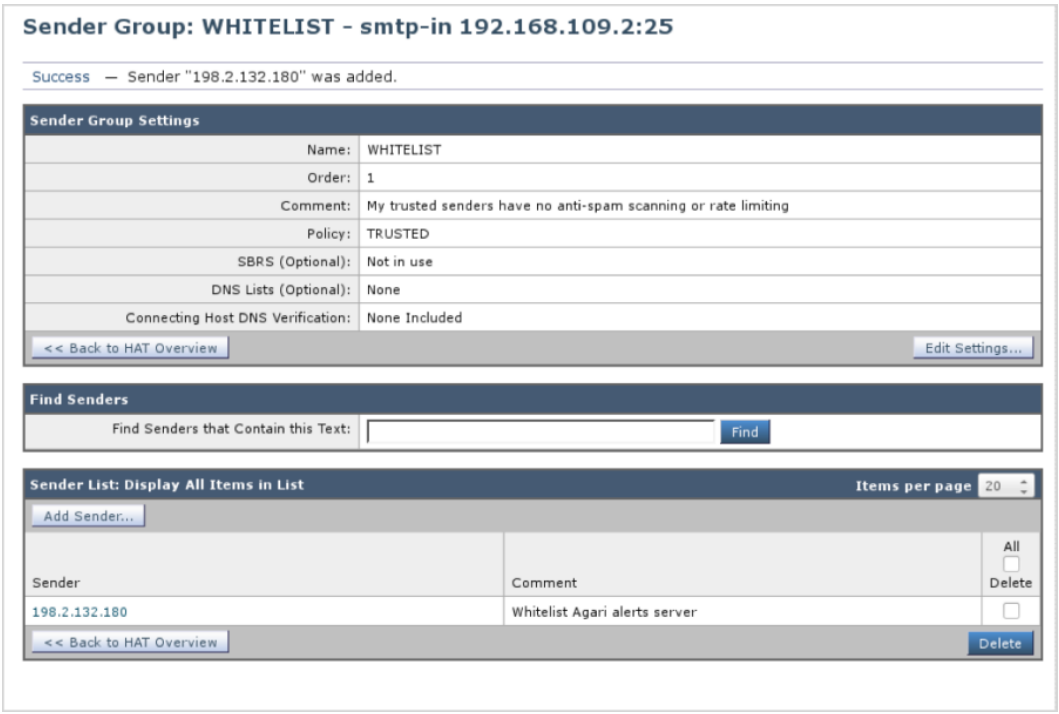
1. [メールポリシー（Mail Policies）] > [HAT概要（HAT Overview）] に移動します。「ホストアクセステーブル」の設定が表示されるので、信頼済み送信者の一覧にアラートサーバーを追加できます。構成ペインは次のように表示されます。



構成はさまざまな面で異なる場合があり、特定の環境に合わせて以下の手順を調整する必要が生じることがあります。たとえば、すべての設定済みのインバウンド リスナーに関してアラート サーバがホワイトリストに含まれるように、インバウンド リスナーごとにこの構成を繰り返す必要があります。

2. デフォルトの送信者グループが設定されていることを前提に、[ホワイトリスト（WHITELIST）] リンクをクリックします。代替の送信者グループがある場合は、[信頼済み（TRUSTED）] メールフローポリシーまたはそれと同等のものにマッピングされているグループを使用します。
3. [送信者一覧：一覧内のすべての項目を表示（Sender List: Display All Items in List）] セクションで、[送信者の追加（Add Sender）] をクリックします。
4. [送信者（Sender）] フィールドに、アラートサーバーの IP アドレス「198.2.132.180」を入力します。
5. [コメント（Comment）] フィールドに、「アラートサーバーをホワイトリストに登録する（Whitelist alerts server）」などのコメントを追加します。

6. [送信(Submit)]をクリックします。
7. [送信者グループ(Sender Group)]ペインで、IP アドレスが[送信者一覧(Sender List)]セクションに存在することを確認します。



8. [変更を確定(Commit Changes)]をクリックします。

上の図に示すように、アラートサーバーの IP アドレスは 198.2.132.180 です。このアドレスの DNS エントリも維持されますが、一般に、このホワイトリストルールには明示的な IP アドレスを使用することをお勧めします。

X-Agari-Authentication-Results ヘッダーを追加するように Cisco ESA を設定する

このセクションは、設定している Cisco ESA システムが境界ゲートウェイであり、デュアル配信には使用されていない場合のみを想定しています。Cisco ESA システムを使用してデュアル配信ストリームを生成している場合は、このセクションを使用しないでください。代わりに、X-Agari-Authentication-Results ヘッダーを追加する適切な方法など、前述の手順に従ってください。

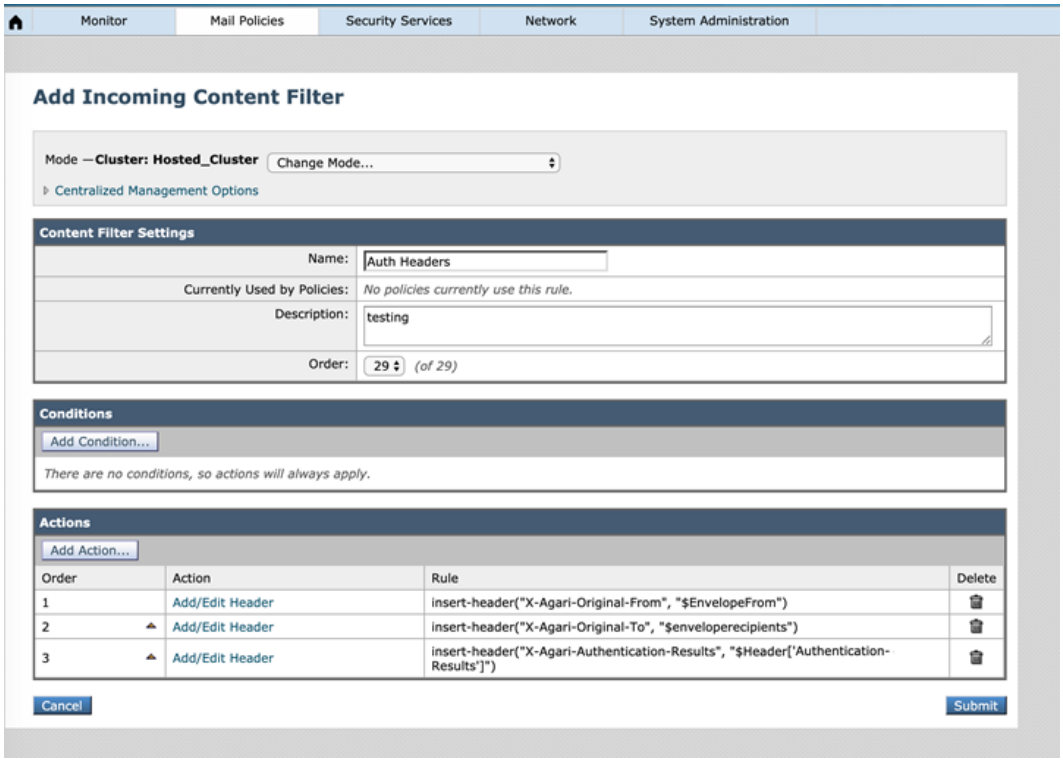
1. 管理者として Cisco ESA にログインします。
2. [メールポリシー(Mail Policies)]>[受信コンテンツフィルタ(Incoming Content Filters)]に移動します。

   環境がクラスタ化されている場合は、残りの手順をトップレベルまたはグループレベルのいずれかで実行します(Cisco ESA インスタンスの特定のセットにのみ影響を及ぼすことがアクションの目的である場合)。マシン レベルではこれらの次の手順を実行しないでください。
3. [フィルタの追加(Add Filter)]をクリックします。
4. フィルタに「Agari_auth_header」という名前を付けます。
5. フィルタの内容がわかるように説明を追加します。たとえば、「X-Agari-Authentication-Results ヘッダーをすべての着信電子メールに追加する」とします。

6. ヘッダーがすべての着信電子メールに追加されるように、フィルタの順序を調整します。その後、フィルタを一覧の上位近くに配置する必要があります。既存のフィルタと相対的に、このフィルタの配置を検討します。
7. フィルタに条件は必要ありません。条件なしのフィルタは、デフォルトですべてのメッセージに一致します。環境によっては、特定の受信者またはドメインに固有の着信メール ポリシー（後述）にフィルタを関連付けることができます。
8. メッセージにヘッダーを追加するアクションを 3 つ追加します。「「「Authentication-Results」ヘッダーに関する重要な考慮事項」 ページ 68」を参照してください。以上のステップを繰り返します。ステップごとに次の表の値を使用してください。
    1. [アクションを追加（Add Action）] をクリックします。
    2. [アクションの追加（Add Action）] ダイアログボックスで、[ヘッダーの追加/編集（Add/Edit Header）] タブをクリックします。
    3. [新しいヘッダーの値を指定（オプション）（Specify Value for New Header (optional)）] オプションをクリックします。
    4. そのフィールドに次の表の値を入力します。
    5. [OK] をクリックします。

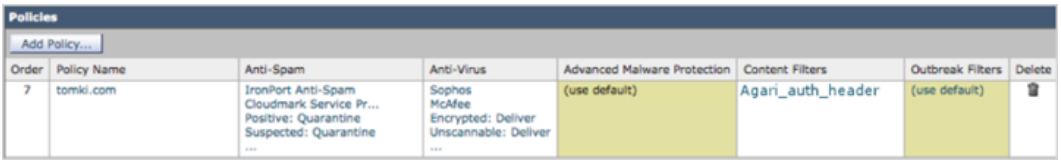
入力する値	目的
X-Agari-Original-From Header data: $EnvelopeFrom	元の送信者。
X-Agari-Original-To Header data: $enveloperecipients	元の受信者。
Header Name: X-Agari-Authentication-Results "Specify Value for New Header": $Header['Authentication-Results']	Authentication-Results ヘッダーの複製。

9. 完成した着信コンテンツ フィルタは、次のように表示されます。



10. [送信（Submit）] をクリックします。

11. フィルタを適切な着信メールポリシーに関連付けます。
    1. [メールポリシー(Mail Policies)] > [受信メールポリシー(Incoming Mail Policies)] に移動します。
    2. 適切な行の [コンテンツフィルタ(Content Filters)] 列で、新たに作成したフィルタを参照するように、割り当てられたコンテンツフィルタを編集します。プロセス内で、そのポリシーのコンテンツフィルタを有効化する必要が生じることがあります。変更されたポリシー行は、次のように表示されます。



12. [変更を確定(Commit Changes)] をクリックします。

「X-Agari-Authentication-Results」ヘッダーが正しいデータと一緒に入力されるように、SPF、DKIM、およびその他の認証メカニズム(送信者 ID、DMARC など)が Cisco ESA 上で有効であることも確認する必要があります。

ラップアップ

上記の手順を完了すると、センサーは、組織に送信された電子メールメッセージのコピーを受信し始めます。変更が完全に有効になるまでに、数分間のわずかな遅延が生じることがあります。https://appc.cisco.com で高度なフィッシング防御にログインし、[管理(Manage)] > [センサー(Sensors)] に移動してインストールしたセンサーのステータスを表示してトラフィックフローを確認できます。

第 5 章

適用

適用は、識別したメッセージをユーザーの受信トレイから特別なフォルダに移動するように Cisco 高度なフィッシング防御 を設定する場合に使用される用語です。高度なフィッシング防御とユーザーのメールボックスとの間でメッセージを移動する場合に API(アプリケーション プログラミング インターフェイス)を使用してプログラムでやり取りするため、API 適用とも呼ばれます。

適用アクションは、ポリシーを強化したものです。ロギングと警告の他に、一致したメッセージを指定のフォルダに移動するようにシステムを設定できます。

API 適用は、Office 365、Exchange(2010、2013、2016)、および G Suite 環境でのみ使用できます。

適用の設定:G Suite

G Suite ユーザーの適用は、センサーをホストしている組織でのみ利用できます。詳細については、「「センサー」ページ 19」を参照してください。

このトピックでは、Google G Suite の適用を設定する方法について説明します。

全般的な手順は次のとおりです。

ステップ 1:G Suite のサービスアカウントを設定する。

ステップ 2:センサーで適用を有効にする。

ステップ 3:Web アプリケーションで適用を有効にする。

ステップ 4:適用の問題に関するシステム通知を有効にする。

ステップ 5:適用ポリシーアクションをテストする。

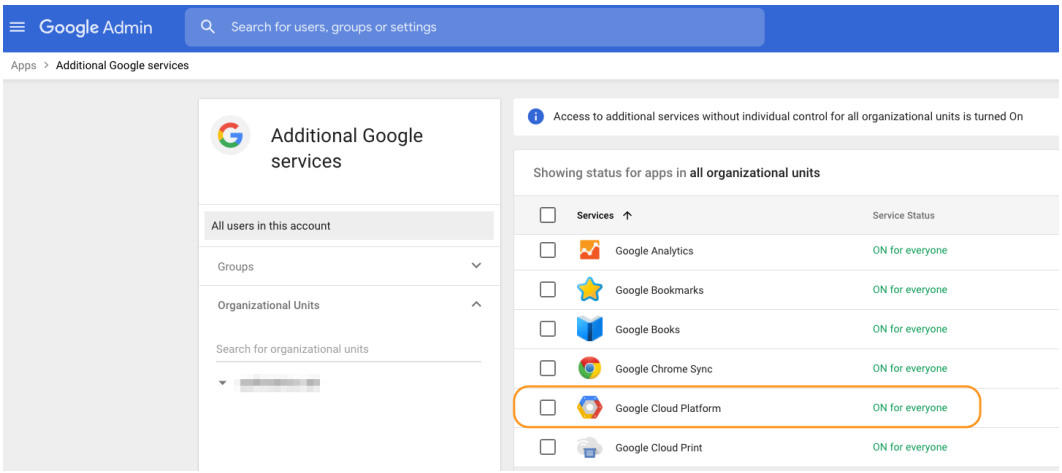
ステップ 1:サービスアカウントを設定する

このセクションでは、G Suite のサービスアカウントを設定する方法について説明します。具体的には、サービスアカウントを作成し、サービスアカウントにスコープを付与します。

サービスアカウントの作成

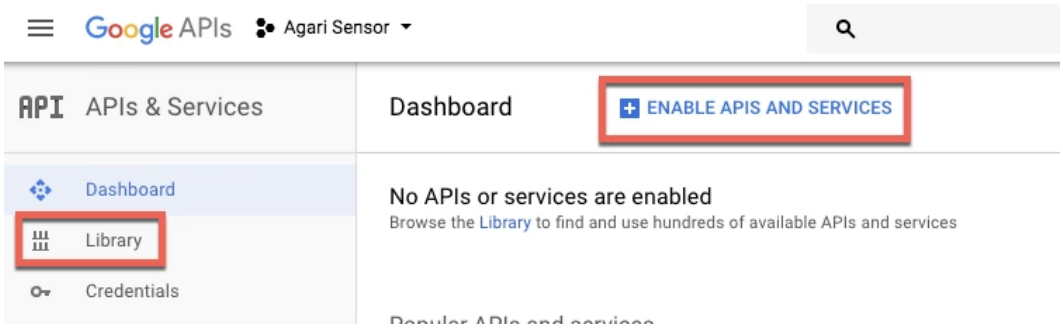
1. G Suite アカウントが Google Cloud Platform で有効になっていることを確認します。
    1. http://admin.google.com に移動し、管理者権限を持つユーザーとしてログインします。
    2. [Apps: Manage apps and their settings] をクリックします。
    3. [Additional Google Services] をクリックします。

4. 追加のサービスのリストから、スクロールして Google Cloud Platform を見つけます（ページが複数あるため、検索バーに *cloud platform* と入力する方が簡単な場合があります）。

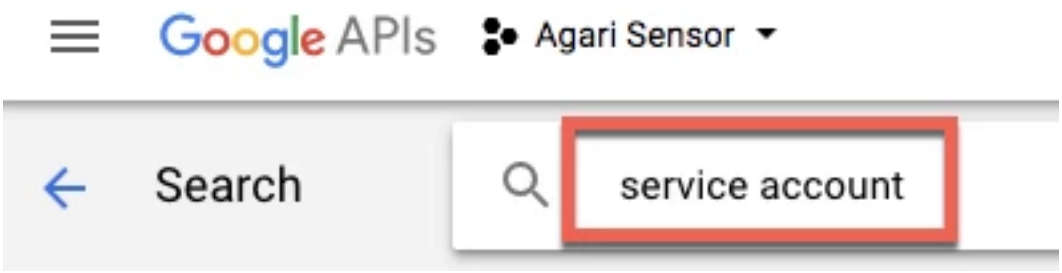


5. [Google Cloud Platform] チェックボックスを選択して、[On for everyone] になるようにします。

2. https://console.developers.google.com/ で開発者コンソールに移動します。プロジェクトを作成し、高度なフィッシング防御が Gmail アプリケーションにアクセスするための認証情報ファイルを生成します。
3. API 認証情報は「プロジェクト」に関連付けられています。新しいプロジェクトを作成するには、[Select a project] ドロップダウンリストをクリックし、新しいウィンドウで [New Project] をクリックします。
4. プロジェクト名に Cisco Sensor と入力します。
5. [Create] をクリックします。詳細オプションを設定する必要はありません。プロジェクトが完全に作成されるまで、最大 2 分かかる場合があります。
6. プロジェクトが作成されたら、リストから選択します（自動的に開かない場合）。
7. API を有効にします。API ライブラリが自動的に開かない場合は、[ENABLE APIS AND SERVICES] または [Library] をクリックするとアクセスできます。これで、使用可能な API のリストが表示されます。



8. Service Account を検索します。



9. [Identity and Access Management (IAM) API] をクリックします。
10. [Enable] をクリックします。
11. [Credentials] をクリックします。
12. [Create credentials] > [Service account key] をクリックします。
13. [Service account] ドロップダウンリストで、[New service account] を選択します。
14. 次の設定を入力または選択します。
    - [Service Account Name]: [Cisco Sensor]
    - [Select a Role]: [Service Accounts] > [Service Account Token Creator] と [Service Account User]
    - [Service Account ID]: 自動的に入力されます。
    - [Key Type]: [JSON]
15. [Create] をクリックします。
16. .json ファイルを保存します。

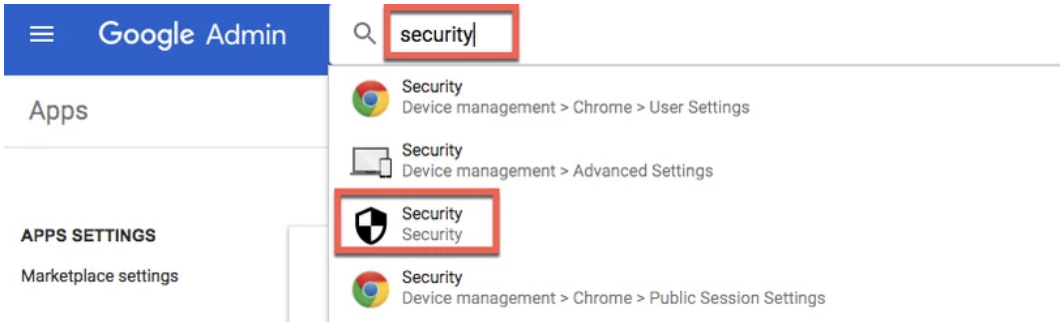
    このファイルを安全な場所に保存して、失わないようにしてください。このファイルに含まれている認証情報は、組織内のすべての受信トレイへのアクセスを制限付きで許可します。次のセクションではこうした認証情報を使用して、センサーへのアクセスを許可します。
17. [Close] をクリックします。
18. [Manage service accounts] をクリックします。
19. [Edit] をクリックします。
20. [Enable G Suite Domain-wide Delegation] チェックボックスをオンにします。
21. [Product name for consent screen] フィールドに、Cisco Sensor と入力します。
22. [Save] をクリックします。
23. Gmail API を使用する場合は、認証情報に関連付けられているプロジェクトをアクティブ化する必要があります。トップメニューにある [Google API] リンクをクリックします。
24. [Library] をクリックします。
25. Gmail を検索し、[Google API] を選択します。
26. [Enable] をクリックします。
27. [Library] をクリックします。
28. Admin SDK を検索し、[Admin SDK] を選択します。
29. [Enable] をクリックします。

サービスアカウントが、Gmail API および Admin SDK API で使用できるように設定されました。

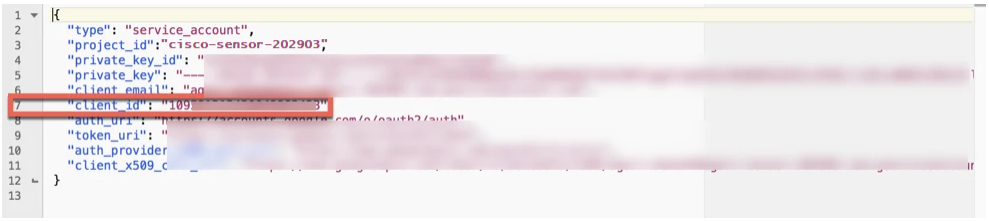
サービスアカウントへのスコープの付与

続いて、「「サービスアカウントの作成」 ページ 82」で作成したサービスアカウントにアクセススコープ（Gmail に固有）を付与する必要があります。

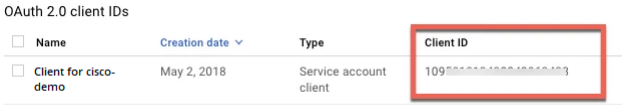
1. 管理者コンソール（http://admin.google.com）に移動し、必要に応じて、管理者権限を持つユーザーとしてログインします。
2. [Apps] に移動します。
3. security を検索し、表示された次の Security アプリを選択します。



4. [API reference] をクリックします。
5. [Enable API Access] チェックボックスをオンにします。
6. [Advanced settings] をクリックします。
7. [Manage API client access] をクリックします。
8. [Client Name] フィールドに、「「サービスアカウントの作成」 ページ 82」で作成したサービスアカウントのクライアント ID を入力します。この ID は次の 2 つの場所にあります。
   - ダウンロードした .json ファイルでは、単独で 1 行に表示されます。この例では、client_id は 7 行目にあります。



   - 開発者コンソール（https://console.developers.google.com/）で、[Credentials] をクリックします。クライアント ID が表示されます。



   クライアント ID（引用符を除く）をコピーして、[Client Name] フィールドに貼り付けます。
9. [One or More API Scopes] フィールドに、次の文字列を以下のとおり正確に入力します。変更を加えず、余分な情報を追加しないでください。文字列全体をフィールドにコピーして貼り付けるだけです。このドキュメントでは複数行にわたって折り返されていますが、1 行として貼り付けられます。

https://mail.google.com/, https://www.googleapis.com/auth/gmail.labels, https://www.googleapis.com/auth/gmail.modify, https://www.googleapis.com/auth/gmail.readonly, https://www.googleapis.com/auth/admin.directory.user.readonly

URL の文字列全体をコピーしてフィールドに貼り付けた場合は、URL 自体にスペースが追加されていないことを確認します。

10. [Authorize] をクリックします。

指定したクライアント ID に権限が付与されたことを示す行が表示されます。

ステップ 2：センサーで適用を有効にする

「「サービスアカウントの作成」 ページ 82」でダウンロードした JSON 認証情報を使用して、各センサーで適用を有効にできるようになりました。これは、高度なフィッシング防御内で行うことも、センサーごとにコマンドライン インターフェイスを使用して行うこともできます。

高度なフィッシング防御でのセンサーの適用の有効化

前提条件：「「サービスアカウントの作成」 ページ 82」でダウンロードした JSON ファイル。

1. [管理（Manage）] > [センサー（Sensors）] に移動します。
2. 複数のセンサーがある場合は、センサーに適したタブを選択します。
3. [API適用の有効化（Enable API Enforcement）] をクリックします。
4. JSON サービス認証情報ファイルの内容全体をコピーして、[サービスアカウント認証情報（Service account credentials）] フィールドに貼り付けます。
5. テスト管理者のメールアドレスを入力します。指定するテスト電子メールアドレスは、G Suite 環境で実際に使用している正常な受信トレイである必要があります。このテストアドレスは、高度なフィッシング防御が API を正常に認証し、その API を使用して環境内のメールボックスを表示およびアクセスできることをテストするために使用します。
6. [API適用のテストおよび有効化（Test and Enable API Enforcement）] をクリックします。

この有効化ステップでは、テストメールは送信されません。

G Suite サービスアカウントから権限が正常に付与されたことを通知する成功メッセージが表示されます。

このプロセスでは、高度なフィッシング防御が API を介してメッセージを適用できるようにするだけです。適用はまだ有効になりません。続いて、メッセージをユーザーの受信トレイから移動する前に、高度なフィッシング防御内で適用を組織レベルで有効にし、適用アクションを使用するようにポリシーを設定する必要があります。

ステップ 3：組織の適用を有効にする

少なくとも 1 つのセンサーで適用を有効にしたら、Web アプリケーションで組織の適用を設定できるようになります。

1. [管理（Manage）] > [組織（Organizations）] に移動します。
2. 組織の名前をクリックします。
3. [適用の設定（Enforcement Settings）] セクションで、[適用（Enforcement）] スイッチを [有効（Enable）] に設定します。
4. 適用ラベルを入力します。適用ラベルは、適用対象のメッセージに追加される「タグ」または「フォルダ名」です。事実上、メッセージはこのフォルダ名に移行され、電子メールクライアントでユーザーに表示されるフォルダの名前になります。
5. [保存（Save）]をクリックします。

ステップ 4：適用関連のシステム通知を有効にする

組織で適用を有効にした場合は、センサーが適用に使用している認証情報が破損したときに警告するシステム通知を追加で設定できます。

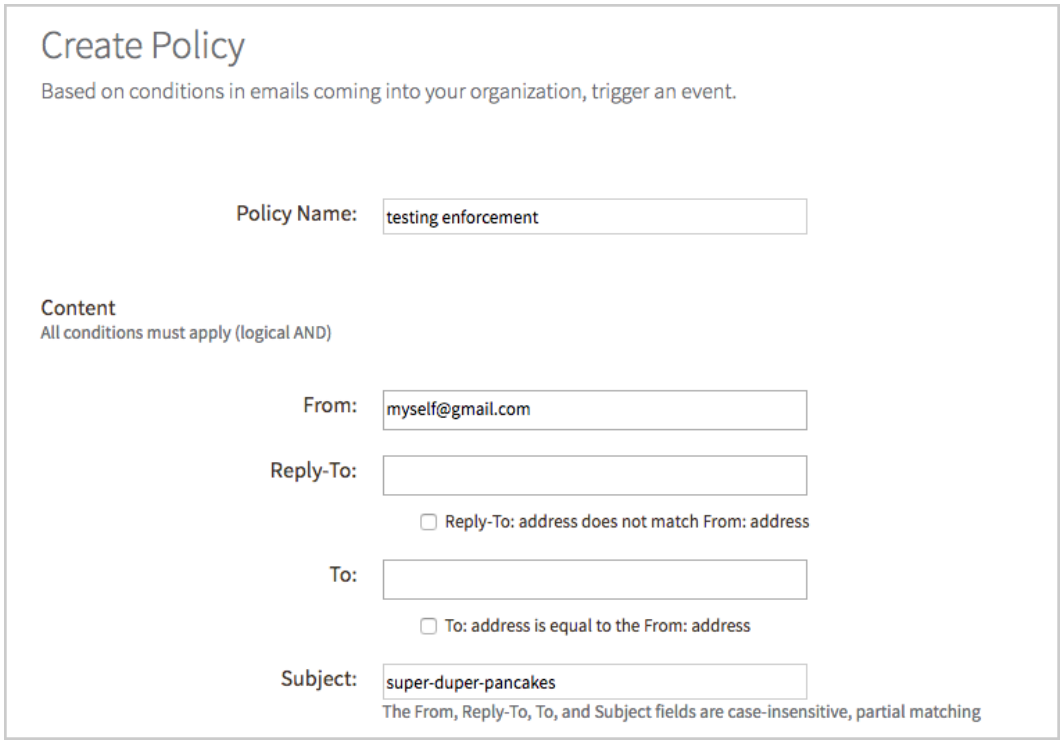
1. [管理（Manage）] > [ポリシー（Policies）] に移動します。
2. [システム通知（System Notifications）] タブをクリックします。
3. [認証情報を指定する（The credentials supplied for...）] チェックボックスをオンにします。
4. [保存（Save）]をクリックします。

ステップ 5：ポリシーによる適用アクションをテストする

組織の適用がすでに各センサーでグローバルに有効になっている場合は、適用アクションを使用したポリシーの作成を開始できます。

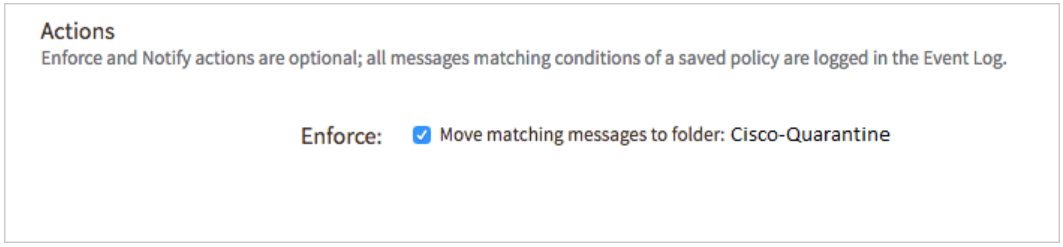
適用アクションをテストするには、まず、条件セットを大幅に絞り込み、確実に一致する条件だけを指定したポリシーを作成します。

たとえば、From: アドレスに自分の正しい個人的な（公開）メールアドレスを指定し、非常に具体的な件名を付けたポリシーを作成します。



ポリシーの作成：条件

ポリシー作成ページの [アクション（Actions）] セクションで、適用アクションを指定します。

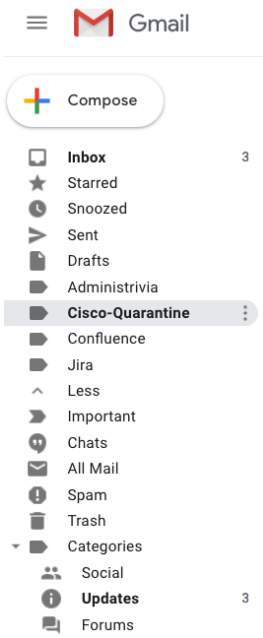


ポリシーでの適用アクションの定義

ポリシーを保存し、ポリシーの条件に一致するテストメッセージを送信します。

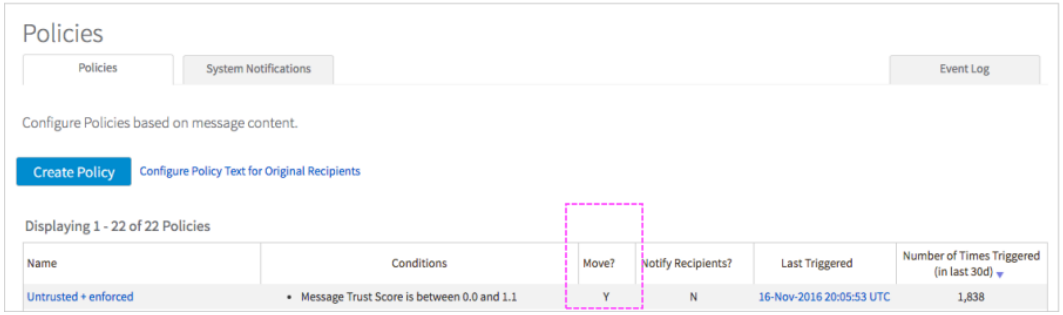
メッセージが（電子メールストリーム内の他のアップストリームプロセスでフィルタ処理されていない場合）、適用アクションに指定されているフォルダに移動します。

たとえば、Gmail クライアントにはフォルダが次のように表示されます。



Gmail の [Cisco – Quarantine] フォルダ

また、[ポリシー（Policies）] ページには、どのポリシーに適用アクションがあるかを示す列が含まれていることに注意してください。



[ポリシー（Policies）] ページの [移動（Move）] 列

ラップアップ

この時点で実行できるアクションには、適用に関するレポートを表示すること(「「API 適用に関するレポート」 ページ 102」を参照)と、適用がセンサーで機能していることを確認すること(「「適用センサーステータス」 ページ 102」を参照)があります。

適用アクションを使用したポリシーを作成するときに、広範囲に電子メールが一致するように条件を拡大できます。

また、通知先を増やすこともできます(追加の受信者と元の受信者)。

適用の設定:MS Graph API を使用した Office 365

Microsoft Graph API は、Cisco 高度なフィッシング防御 が組織に届いたすべてのメッセージのコピーを受信し、従業員のメールボックス内のメッセージを移動および削除する場合に使用します。

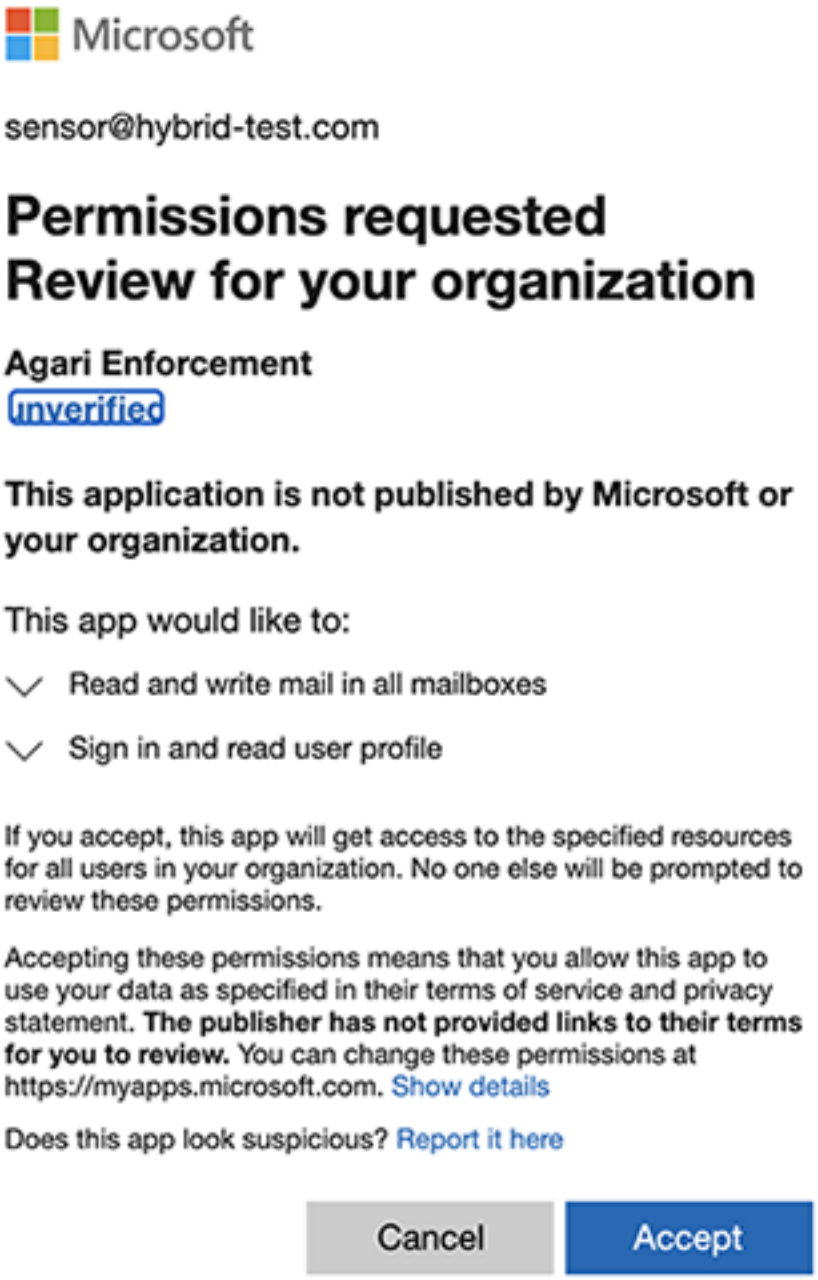
始める前に、Microsoft グローバル管理者が Cisco 高度なフィッシング防御 の承認を 1 回にかぎり実行できるようにしておきます。

- 適用の対象となるメッセージの宛先としてデフォルトの迷惑フォルダを使用します。
- 最大 10,000 個の項目をまとめて適用します。

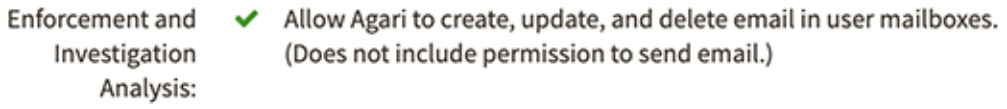
次の手順に従って、MS Graph API を使用した適用を行います。

1. [管理(Manage)] > [組織(Organizations)] に移動します。
2. 組織を選択し、[Microsoft API権限(Microsoft API Permissions)] タブを選択します。
3. [適用および調査分析(Enforcement and Investigation Analysis)] というラベルの横にある [有効(Enable)] ボタンをクリックします。
4. ポップアップに示された必要な権限を確認します。承認するには、もう一度 [有効(Enable)] をクリックします。Office 365 ログイン画面が開きます。
5. グローバル管理者のログイン情報でログインします。

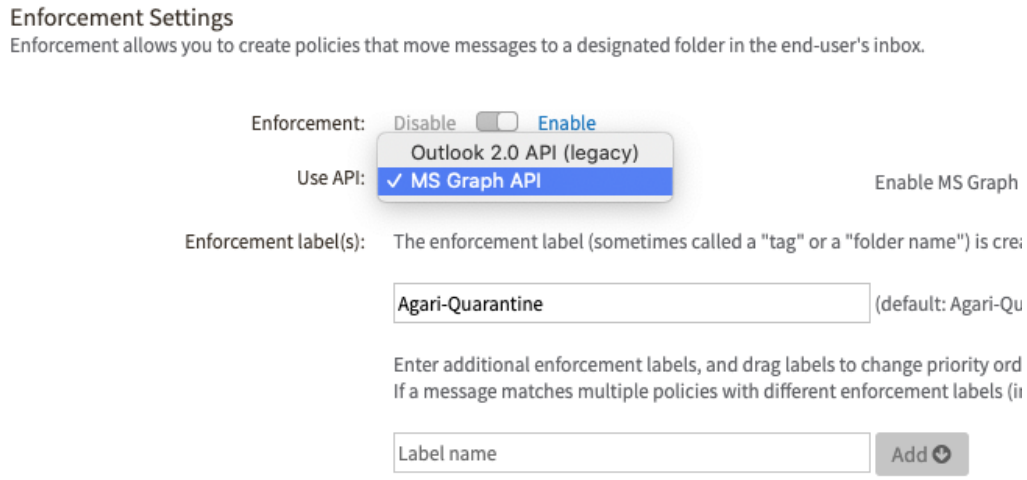
6. Microsoft 権限リストを確認して承認します。



7. 必要な権限がない場合は、エラーメッセージが表示され、管理者にアプリの権限を付与してもらうように指示されます。承認すると、前のページに戻り、緑色のチェックマークが付いた確認メッセージが表示されます。

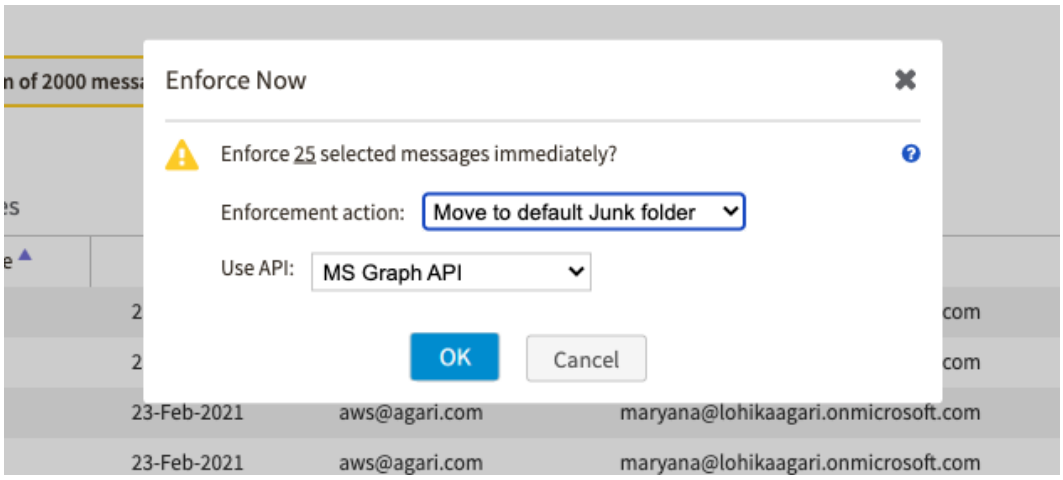


8. [組織設定(Organization Settings)] ページで、[APIの使用(Use API)] の横にあるドロップダウンメニューを見つけます。この設定は、デフォルトで [MS Graph] に設定されます。新しい顧客として設定している場合、従来の Outlook 2.0 オプションは有効になっていないため選択できません。以前に有効にしている場合は、ドロップダウンメニューに選択肢として表示されます。[MS Graph] を選択したままにします。



9. [保存(Save)]をクリックします。

[MS Graph API] が有効になったため、迷惑メールフォルダの言語やスペル(Junk Mail、Junk E-Mail、Courrier indésirable)に関係なく、このフォルダを適用の宛先として使用できます。[デフォルトの迷惑フォルダに移動(Move to default Junk folder)] がメニューの選択肢として表示されます。



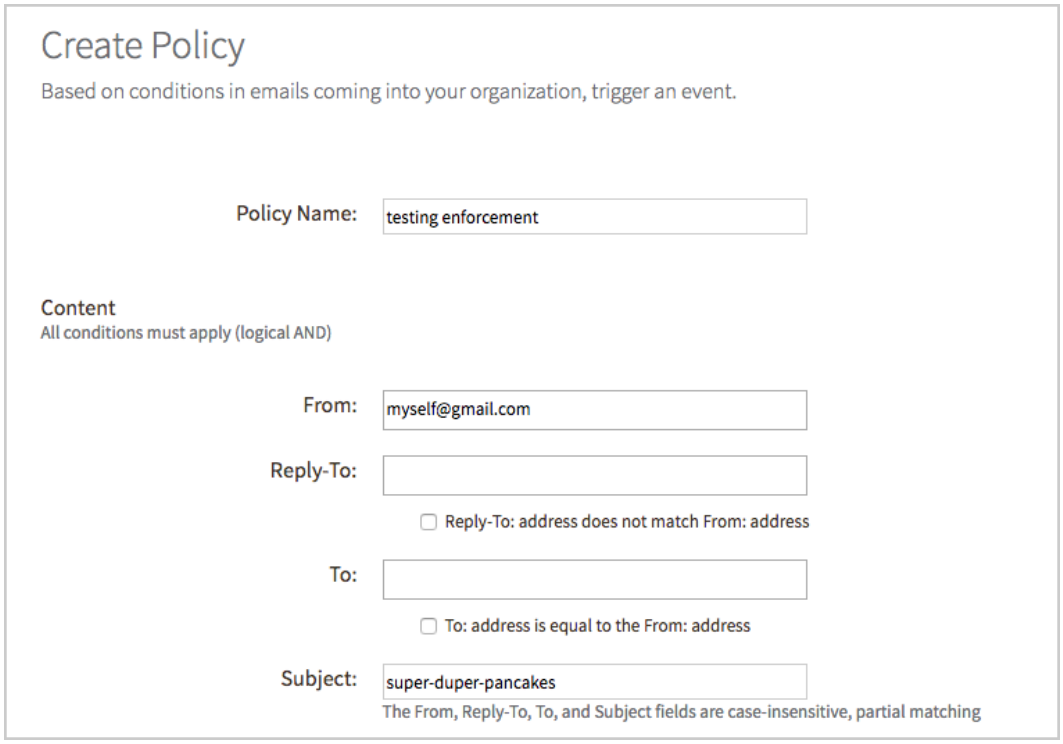
MS Graph API を使用すると、1 回の適用アクションで 10,000 件のメッセージを適用することもできます。

ポリシーによる API 適用アクションのテスト

適用がすでに有効になっている場合は、適用アクションを使用したポリシーの作成を開始できます。このセクションで説明しているように、明示的に定義したポリシーを作成することも、オンデマンドでポリシーを作成することもできます。後者の方法については、「「オンデマンドポリシー」 ページ 164」を参照してください。

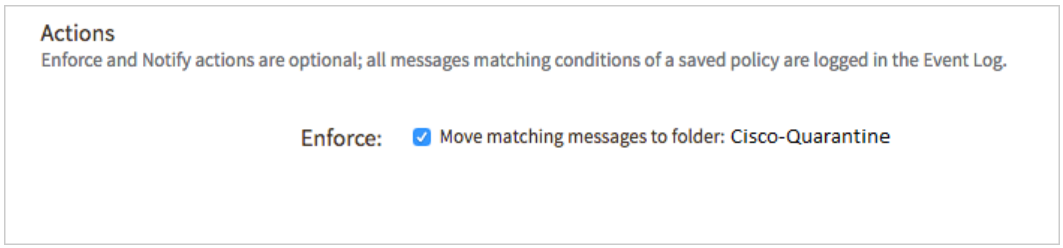
適用アクションをテストするには、まず、条件セットを大幅に絞り込み、確実に一致する条件だけを指定したポリシーを作成します。

たとえば、From: アドレスに自分の正しい個人的な（公開）メールアドレスを指定し、非常に具体的な件名を付けたポリシーを作成します。



ポリシーの作成：条件

ポリシー作成ページの [アクション（Actions）] セクションで、適用アクションを指定します。

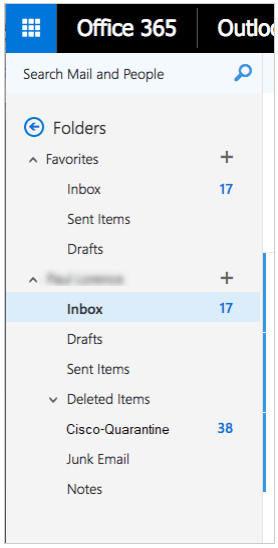


ポリシーでの適用アクションの定義

ポリシーを保存し、ポリシーの条件に一致するテストメッセージを送信します。

メッセージが（電子メールストリーム内の他のアップストリームプロセスでフィルタ処理されていない場合）、適用アクションに指定されているフォルダに移動します。

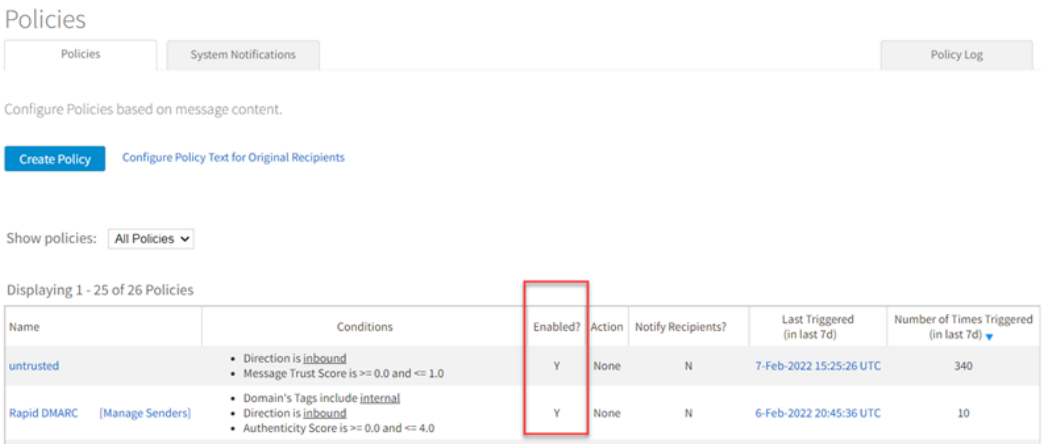
たとえば、O365 クライアントにはフォルダが次のように表示されます。



Office 365 クライアントの隔離フォルダ

ユーザーによっては、フォルダの作成後すぐに「Cisco -Quarantine」フォルダを表示する場合に、ブラウザをリフレッシュする必要があります。

また、[ポリシー(Policies)] ページには、どのポリシーに適用アクションがあるかを示す列が含まれていることに注意してください。



[移動アクション(Move action)] 列

Microsoft Office 365 監査ツールを使用した適用の管理

監査の有効化

Office 365 では、メールボックス、ユーザーのアクション、および管理者のアクションを広範に監査できます。ただし、デフォルトでは有効になっていません。

監査を有効にするには、https://technet.microsoft.com/en-us/library/jj150552(v=exchg.150).aspx の記事に示された手順に従ってください。

監査を有効にする重要な PowerShell コマンドは次のとおりです。

Set-Mailbox <Identity> -AuditEnabled $true

適用アクションは、「所有者」ログオンタイプとしてログに記録されます。特定のイベントの監査を有効にする PowerShell コマンドは、次のようになります。

Set-Mailbox <Identity> -AuditOwner MailboxLogin,HardDelete,SoftDelete,Move,MovetoDeletedItems $true

PowerShell を介して O365 にアクセスできる場合は、次のコマンドを発行して、特定のメールボックスの監査アクションをチェックできます。

Get-mailbox "mailbox_name" | Select-Object -ExpandProperty AuditAdmin

Get-mailbox "mailbox_name" | Select-Object -ExpandProperty AuditDelegate

Get-mailbox "mailbox_name" | Select-Object -ExpandProperty AuditOwner

次に例を示します。

PS C:¥Windows¥system32> Get-mailbox plorence | Select-Object -ExpandProperty AuditOwner

Creating a new session for implicit remoting of "Get-Mailbox" command...

WARNING: Commands available in the newly opened remote session are different than when the im

created. Consider recreating the module using Export-PSSession cmdlet.

Update

Move (<--)

MoveToDeletedItems

SoftDelete

HardDelete

MailboxLogin

監査の実行

個々のメールボックスの監査がすでに有効になっている場合は、Microsoft の PowerShell コマンドを使用して、ユーザーの受信トレイを監査し、高度なフィッシング防御がメッセージを適用したかどうかを確認できます。

たとえば、Get-MessageTrace コマンドは、一意の MessageTraceID を明確にリクエストできます。

PS C:¥Windows¥system32> Get-MessageTrace -SenderAddress "plorence@gmail.com" -StartDate 06/04/2017 -EndDate 06/06/2017 |

Select-Object Received, SenderAddress, RecipientAddress, Subject, Status, ToIP, FromIP, Size, MessageID, MessageTraceID

Received : 6/5/2017 5:16:09 PM

SenderAddress : plorence@gmail.com

RecipientAddress : plorence@saintmetrics.com

Subject : move this message automatically enforce me

Status : Delivered

ToIP :

FromIP : 209.85.161.180

Size : 11049

MessageId : <CAEKxqn+Qabt8aHg=Pp=pPW2tYyHuO9TO8dJgs09=bp4uv-ndnw@mail.gmail.com>

MessageTraceId : 8d02ca26-1f78-4185-aa07-08d4ac368ef1

MessageTraceID を使用すると、トレース詳細のリクエストを発行できます。

PS C:¥Windows¥system32> Get-MessageTraceDetail -MessageTraceId 8d02ca26-1f78-4185-aa07-08d4ac368ef1 -RecipientAddress "p

lorence@saintmetrics.com" -StartDate 06/04/2017 -EndDate 06/06/2017

Date Event Detail

---- ----- ------

6/5/2017 5:16:10 PM Receive Message received by: MWHPR16MB1375

6/5/2017 5:16:12 PM Journal Message was journaled. Journal report was sent to test_stage@stage.enfor...

6/5/2017 5:16:12 PM Journal Message was journaled. Journal report was sent to test_stage@stage.enfor...

6/5/2017 5:16:12 PM Deliver The message was successfully delivered.

6/5/2017 5:16:12 PM Spam Diagnostics

トレースを見ると、メッセージは配信されたものの、高度なフィッシング防御API によって移動されていないことに注意してください。

ただし、このコマンドを実行すると、指定したユーザーに検索結果を XML 添付ファイルとして電子メールで送信するジョブが設定されます。

New-MailboxAuditLogSearch – https://technet.microsoft.com/en-us/library/ff522362(v=exchg.160).aspx

適用アクションのログの例：PowerShell

監査ログを検索して、高度なフィッシング防御が API で実行した移動（適用）アクションを表示できます。

PS C:¥Windows¥system32> Search-MailboxAuditLog -Identity "plorence" -LogonTypes Owner -ShowDetails |select Operation,Fol

derPathName,DestFolderPathName,LogonType,ClientInfoString,LogonUserDisplayName,SourceItemSubjectsList,L-astAccessed

Operation : Move

FolderPathName : ¥Inbox

DestFolderPathName : ¥Agari-Quarantine

LogonType : Owner

ClientInfoString : Client=REST;Client=RESTSystem;;

LogonUserDisplayName : Paul Lorence

SourceItemSubjectsList : Thursday enforce me

LastAccessed : 6/8/2017 9:11:10 AM

「移動」操作がどのようにリクエストされたかに注意してください。DestinationFolderPathname が「Agari-Quarantine」（デフォルト）で、LogonType 監査アクションが「Owner」になっています（API によって移動されるメッセージは、「委任」所有者ログオンアクションとも「外部アクセス」監査アクションとも見なされません）。

適用アクションのログの例：WebUI

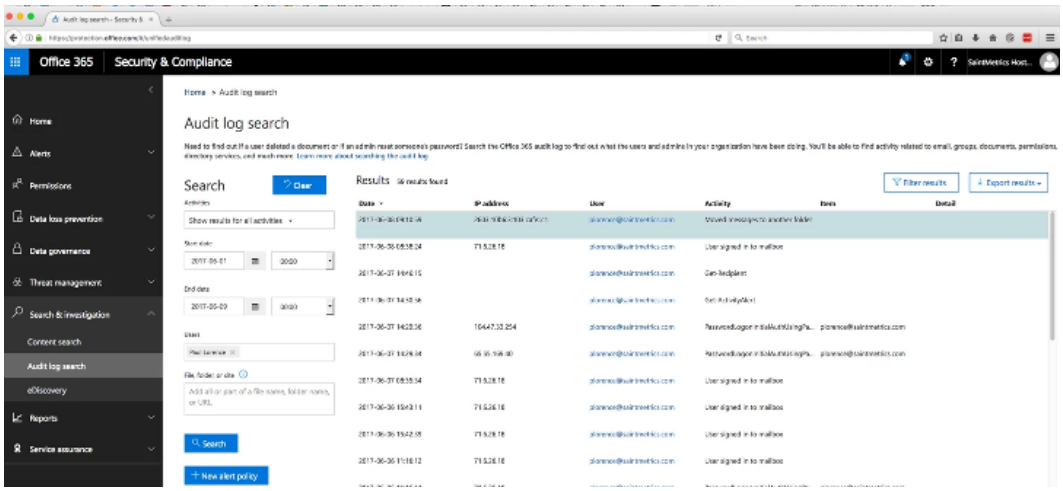
これと同じ監査情報が、Exchange Online Protection（EOP）のお客様向けの「セキュリティとコンプライアンス」WebUI に表示されます。

Office 365 組織で監査が有効になっている場合：

1. https://protection.office.com に移動し、Office 365 管理者として認証を行います。
2. [セキュリティ/コンプライアンス] 管理センターを選択します。
3. [検索と調査] > [監査ログの検索] を選択します。
4. 検索パラメータを入力します。
5. 詳細を表示します。

たとえば、次のようなメッセージが検索結果に表示されます。

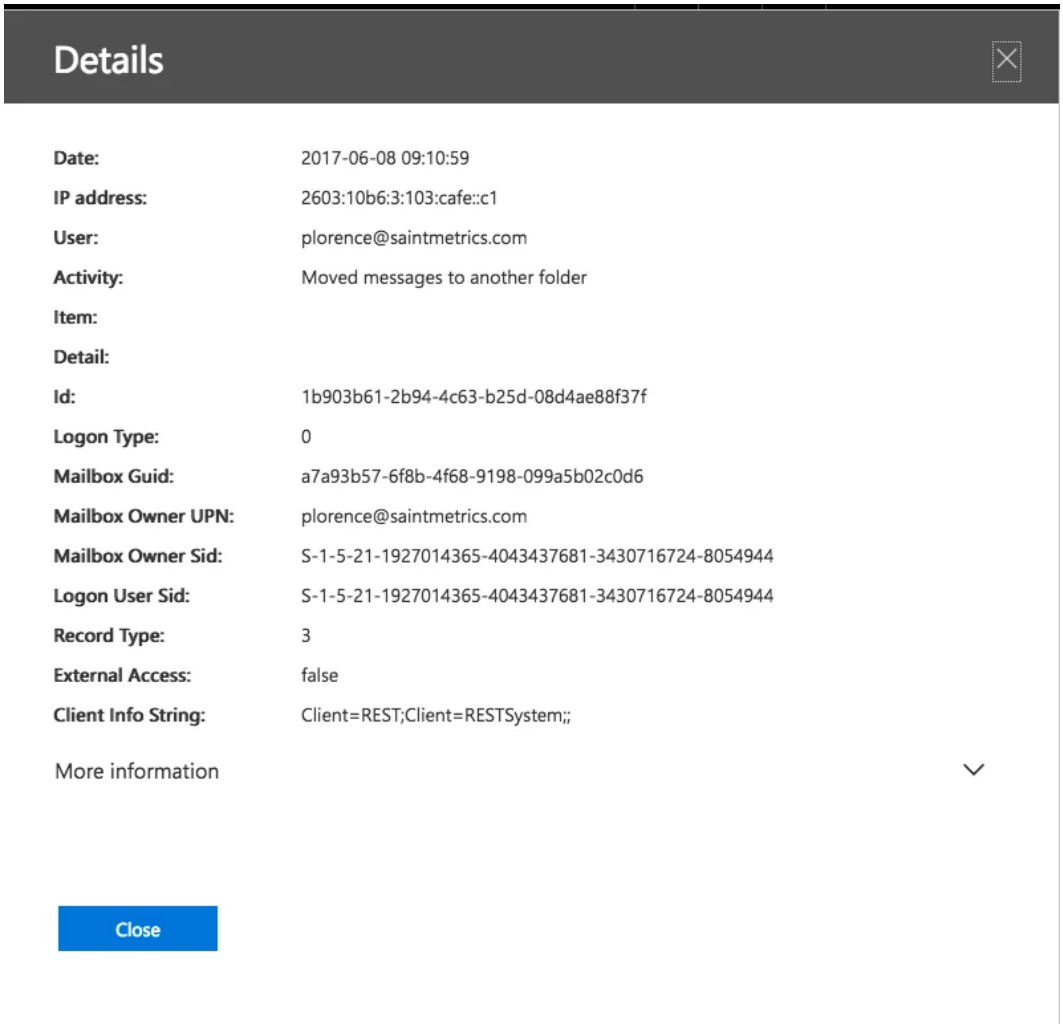
アクティビティは「別のフォルダにメッセージを移動」であることに注意してください。



[監査ログの検索] メッセージの結果

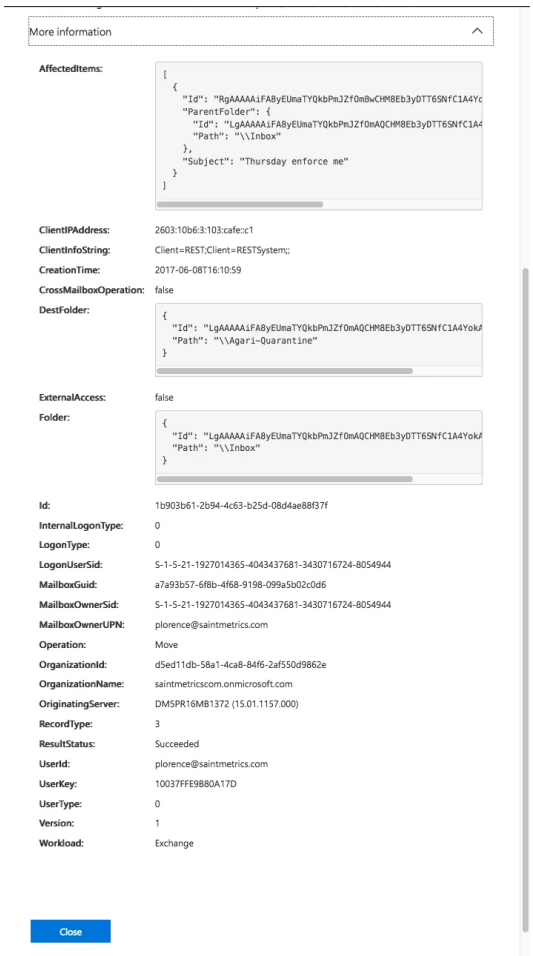
詳細を掘り下げます。

「メールボックスの所有者」の [Logon Type] 値が「0」であることに注意してください。



監査ログの詳細

詳細については、[詳細情報] をクリックしてください。ClientInfoString と DestFolder の値に注意してください。



監査ログの詳細：詳細

次に、PowerShell コマンドを使用して Office 365 受信トレイを監査する場合に参考になるリファレンスを示します。

http://techgenix.com/using-powershell-simplify-mailbox-auditing-part1/

http://techgenix.com/using-powershell-simplify-mailbox-auditing-part2/

http://techgenix.com/using-powershell-simplify-mailbox-auditing-part3/

ラップアップ

この時点で実行できるアクションには、適用に関するレポートを表示すること（「「API 適用に関するレポート」ページ 102」を参照）と、適用が機能していることを確認することがあります。

適用アクションを使用したポリシーを作成するときに、広範囲に電子メールが一致するように条件を拡大できます。

また、通知先を増やすこともできます（追加の受信者や元の受信者）。

適用の設定：Microsoft Exchange

このトピックでは、Microsoft Exchange バージョン 2010、2013、2016 の適用を設定する方法について説明します。

全般的な手順は次のとおりです。

ステップ 1：センサーを最新バージョンにアップグレードする。

ステップ 2：センサーをリブートする。

ステップ 3：Exchange 適用を設定する。

ステップ 4：高度なフィッシング防御で適用を有効にする。

ステップ 1：センサーをアップグレードする

適用を行うには、センサーを最新バージョンにアップグレードする必要があります。

センサーは、高度なフィッシング防御またはコマンドラインでアップグレードできます。

アップグレードしたら、センサーをリブートして有効にする必要があります。

高度なフィッシング防御でのセンサーのアップグレード

1. [管理（Manage）] > [センサー（Sensors）] に移動します。

   最新バージョンを実行していないアクティブなセンサーには、アップグレードリンクが表示されます。
2. [アップグレードを開始（Upgrade Now）] をクリックします。
3. 日付が最新のバージョンを選択します。バージョンは、YYYY.MM.DDHHMMSS 形式で設定されています。YYYY はリリースされたバージョンの年、MM は月、DD は日、HHMMSSS は時刻です。

コマンドラインからのセンサーのアップグレード

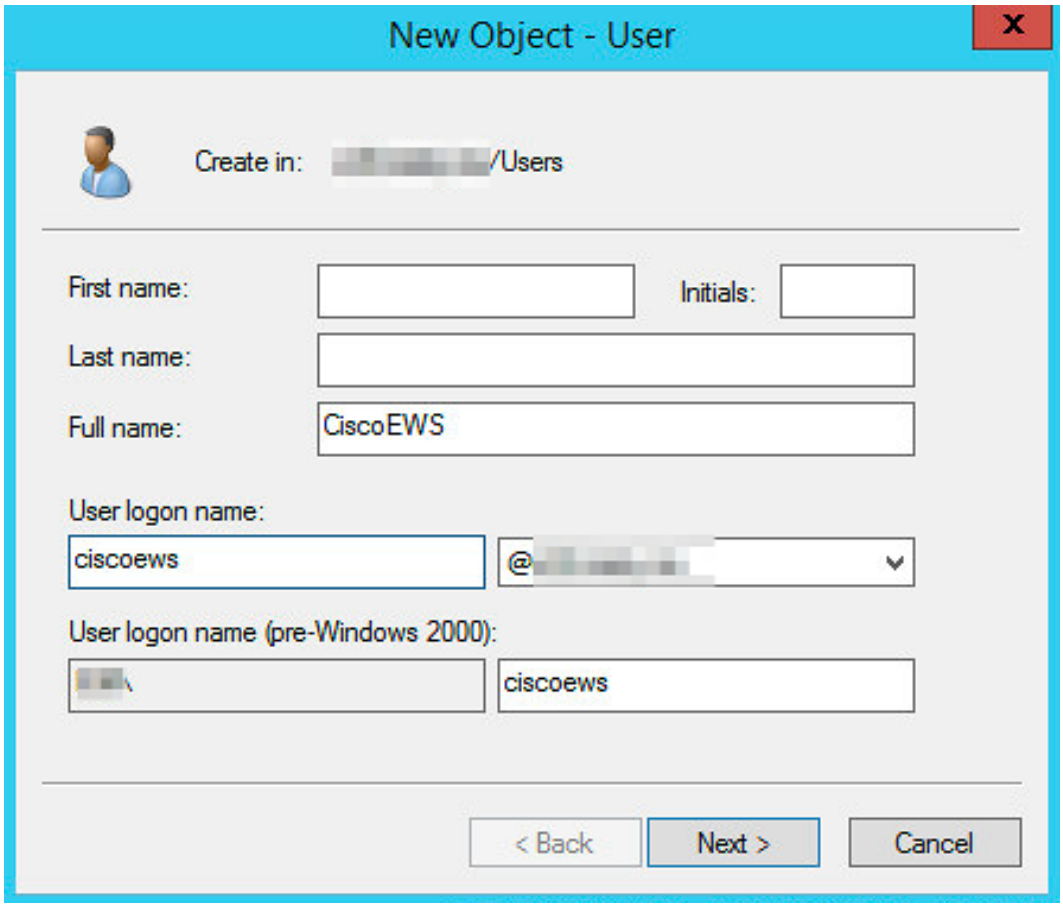
1. センサーマシンに ssh で接続します。
2. 次のコマンドを入力します。

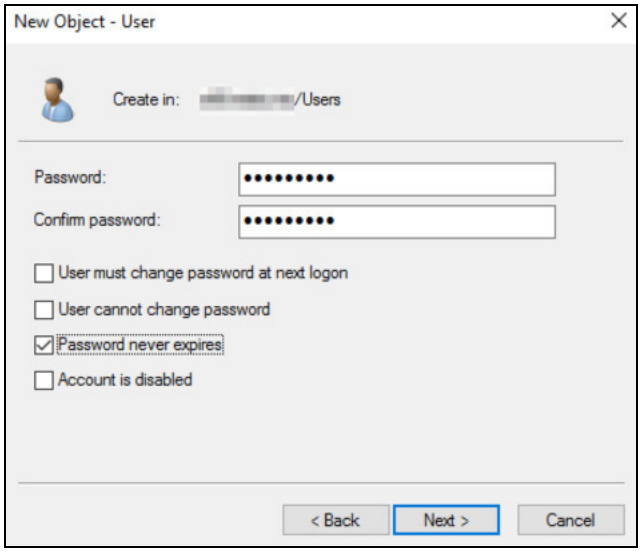
   ```
   sudo /opt/agari/bin/agari-ep update
   ```

ステップ 2：Exchange 適用を設定する

1. Active Directory にサインインします。
2. 新規ユーザーを作成します。
3. ユーザーの詳細を入力または選択します。
   - [フルネーム]：ciscoEWS
   - [ユーザーログオン名]：ciscoews

- [パスワードを無期限にする] チェックボックスをオンにし、入力したパスワードをメモします。





4. Exchange になりすまし権限を付与します。
5. Exchange 管理シェル（Powershell）で、次のコマンドを実行します。

   New-ManagementRoleAssignment -Name " Cisco Sensor EWS" -Role "ApplicationImpersonation" -User "ciscoews"

（このコマンド全体で 1 行です。コピーして貼り付ける場合は、余分な文字が誤って追加されないようにしてください）

6. Exchange Web Services 仮想ディレクトリの基本認証を設定します。
    - Exchange 2010
        1. IIS 7 を開きます。
        2. [サイト] > [既定のWebサイト] を展開します。
        3. [Exchange Web Services] を選択します。
        4. [認証] をクリックします。
        5. [基本認証] が [有効] になっていることを確認します。
    - Exchange 2013/2016
        1. [サーバー] > [仮想ディレクトリ] に移動します。
        2. [Exchange Web Services]（[既定のWebサイト]）を編集します。
        3. [認証] タブをクリックします。
        4. [基本認証] が [有効] になっていることを確認します。
7. 自動検出の DNS 値が正しいことを確認します。Autodiscover.domain.tld のようになっている必要があります。
8. SSH でセンサーに接続します。
9. コマンドを実行します。

    sudo /opt/agari/bin/configure-ews-enforcement

10. センサーを最初にインストールして起動したときに設定したパスワードを入力します。
11. 手順の最初に作成したサービスアカウントを使用します。ユーザー名は、domain¥user（netbios¥serviceAccount）の形式にする必要があります。
12. 適用をテストします。
    - コマンドを実行します。

    sudo /opt/agari/bin/agari-ep test-api-creds user@email.address

    - user@email.address は、上記のサービスアカウントではなく、有効なユーザーである必要があります。
    - このテストが正常に完了するまでに最大 10 分かかる場合があります。

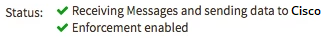
ステップ 3：高度なフィッシング防御で適用を有効にする

1. 高度なフィッシング防御で、[管理（Manage）] > [組織（Organization）] に移動します。
2. 組織名をクリックします。
3. [適用の設定（Enforcement Settings）] セクションで、[適用（Enforcement）] スイッチを [有効（Enable）] に移動します。
4. [保存（Save）]をクリックします。

適用センサーステータス

組織で Graph API 適用が有効になっている場合、適用センサーのステータスは冗長であり、[センサー（Sensor）] ページに表示されません。

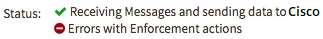
センサーの適用がすでに有効になっている場合、適用ステータスはそのセンサーの [管理（Manage）] > [センサー（Sensors）] ページにリストされます。



センサーが機能している場合の適用ステータス

この 2 つの状態の組み合わせは、センサーのタブに反映されます。

高度なフィッシング防御 から [適用アクションにエラーあり（Errors with enforcement actions）] というステータスが報告されることがあります。



適用ステータスのエラー

[適用アクションにエラーあり（Errors with enforcement actions）] ステータスは次のように定義されています。

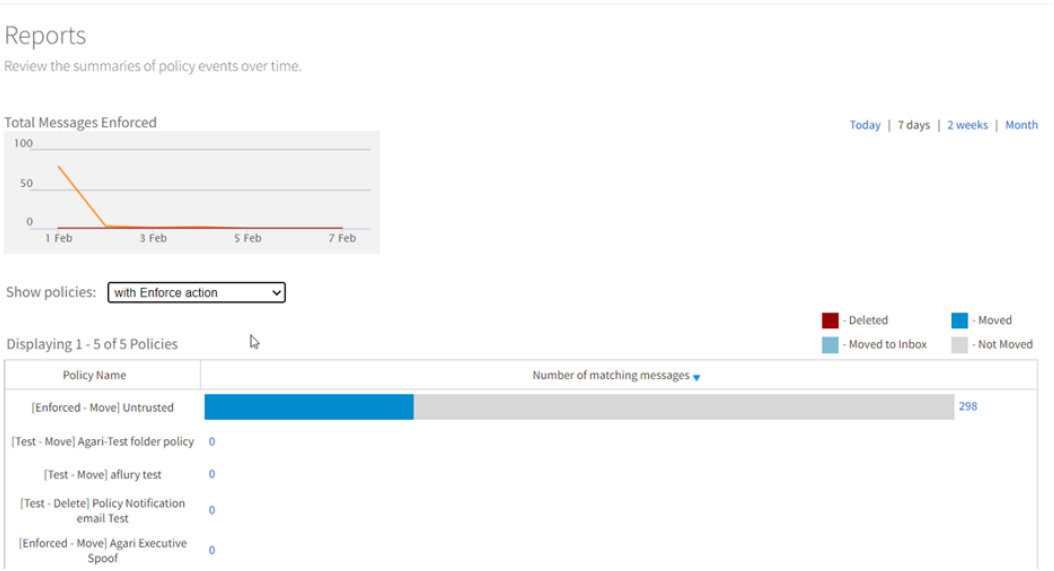
適用できたメッセージが過去 100 件のうち 80 件未満

このステータスは、適用をテストする際の最初の段階で表示されることがあります。

API 適用に関するレポート

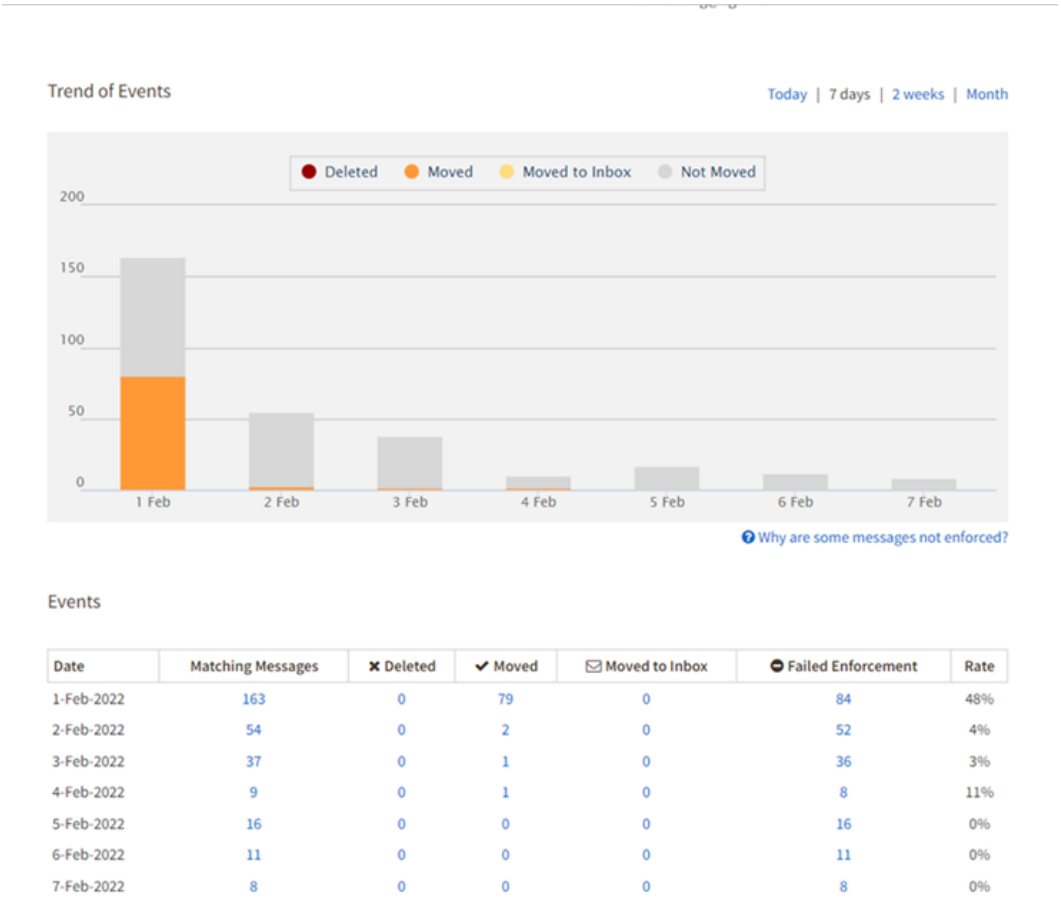
[レポート（Reports）] ページに移動（[管理（Manage）] > [レポート（Reports）]）し、[ポリシーの表示（Show policies）] リストから [適用アクションを使用（with Enforce action）] を選択すると、適用アクションを指定したすべてのポリシーに関して、移動済みメッセージと未移動のメッセージの概要を表示できます。

API 適用のために移動されたメッセージについては、水平棒グラフがオレンジ色で表示されることに注意してください。



レポートのインデックスページ

水平棒グラフをクリックすると、そのポリシー（適用アクションあり）の経時的な傾向が表示されます。

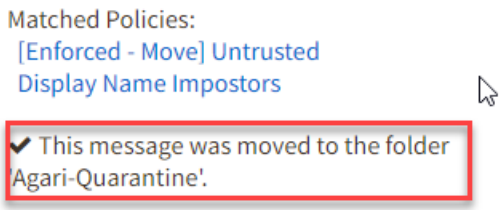


Date	Matching Messages	✖ Deleted	✔ Moved	Moved to Inbox	Failed Enforcement	Rate
1-Feb-2022	163	0	79	0	84	48%
2-Feb-2022	54	0	2	0	52	4%
3-Feb-2022	37	0	1	0	36	3%
4-Feb-2022	9	0	1	0	8	11%
5-Feb-2022	16	0	0	0	16	0%
6-Feb-2022	11	0	0	0	11	0%
7-Feb-2022	8	0	0	0	8	0%

レポートの詳細ページ

[一致するメッセージ（matching messages）] 列のリンクをクリックして、ポリシーに一致し、正常に移動されたメッセージの検索結果を表示できます。

移動済みのメッセージのステータスは、メッセージの詳細ビューにも表示されます。



メッセージの詳細での移動済みメッセージのステータス

一部のメッセージが移動されない理由

メッセージは、次の 2 つの理由で「移動されていません」と表示される場合があります。

- ポリシーに適用アクションが定義されていない。

- API でメッセージを移動できなかった。これは、API コールが行われる前にユーザーが受信トレイからメッセージを削除した場合、またはユーザーアカウントが削除またはロックされた場合に発生する可能性があります。

センサーごとに、適用アクションが /var/log/agari/enforcer.log* ファイルに記録されます。

第 6 章

高度なフィッシング防御の使用

高度なフィッシング防御を完全に設定したら、それを使用して電子メールトラフィックを監視し、そのトラフィックの問題を特定します。

ワークフロー

概要ページを使用して、問題となる送信者およびメッセージを検索できます。左側にあるさまざまな攻撃の分類をクリックすると、調査に役立ちます。

[IP アドレス(IP Addresses)] ページと [ドメイン(Domains)] ページを介して送信者を調査し、ページを切り替えながら、疑わしい送信者と彼らが送信したメッセージを特定できます。必要に応じて、一部の社内およびパートナーのドメインにタグを適用する場合があります(下記の「ドメインのタギング」を参照)。すべての [分析(Analyze)] ページが最終的に [メッセージの検索(Search Message)] 結果につながりますが、そこに至るまでの複数のパスがあります。

疑わしいメッセージの検索や表示を行い、以下を実行します。

- スコアリングを確認する。
- [メッセージの詳細(Message Details)] ページのリンクを使用して、ポリシーを作成する。
- 特定のメッセージのフィードバックを送信する。
- メイン ウィンドウでメッセージを表示し、それに直接リンクする。

疑わしいメッセージを管理する

一部の疑わしい送信者とメッセージを特定したら、実際にメッセージに対して機能するポリシーを作成できます([管理(Manage)] > [ポリシー(Policies)])。

ヒント:[メッセージの詳細(Message Details)] ページでメッセージを表示している場合は、ベルアイコンを使用してポリシーを作成できます。メッセージの検索結果を表示している場合は、[ポリシーの作成(Create a Policy)] リンクをクリックして同じことを実行できます。

ポリシーを使用して、疑わしいメッセージが到着したときに通知を送信したり、メッセージを異なるメールボックスやフォルダに移動したり(適用が有効な場合)できます。

ポリシーの作成方法の詳細については、「「ポリシー」 ページ 153」を参照してください。

受信電子メールトラフィックを分析する

Cisco 高度なフィッシング防御 は、電子メールメッセージの送信元（IP、ドメイン）、それらのメッセージと送信者に関連付けられたリスクなどの洞察を組織の受信電子メールトラフィックに提供します。

概要ページは、組織のインバウンド電子メール トラフィックのリスクの概要を独自に可視化したものです。高度なフィッシング防御センサーによって受信されるメッセージはすべて、信頼スコアが付けられ、次の観点からプロットされます。

- **メッセージの真正性**：送信元を偽って送信されたメッセージではないか
- **ドメインレピュテーション**：信頼できるドメインであるか、つまり、信頼できるビジネス関係にある相手であるか
- **送信者の正当性**：SENDERBASE レピュテーションスコア（SBRS）によって評価された送信者の IP アドレスが本物であるか

信頼スコア

信頼スコアは、組織のユーザーに配信されたすべての受信メッセージに関して計算されます。「このメッセージをどのぐらい信頼すべきか?」という基本的な質問に回答します。信頼得点は、電子メールを「非信頼」、「疑わしい」、「信頼済み」の 3 つのグループに分けるために使用されます。メッセージは、0 ～ 10 のスケールで得点が付けられ、0 は信頼性が最も低く、10 が最高となります。

信頼スコアでは、ドメインレピュテーションのスコア、メッセージの真正性のスコア、メッセージごとの機能、そして実行したスコアリング調整が考慮されます。

メッセージの本文は、信頼スコアの要素ではありません。これに対する例外は、URI 分析を有効にしている場合です（「「添付ファイルと URI の分析を有効にする」 ページ 183」を参照してください）。この場合、メッセージ本文から抽出された URI は、悪意あるものである可能性についてスコア付けされます。

- 真正性のスコアが高い送信者からで、ドメインレピュテーションのスコアが低い = 疑わしい。
- 真正性のスコアが高い送信者からで、ドメインレピュテーションのスコアが高い = 信頼できる。
- 真正性のスコアが低い送信者からで、ドメインレピュテーションのスコアが高い = 疑わしい（特に、ドメインが適切かつ頻繁に認証している場合）。
- 真正性のスコアが低い送信者からで、ドメインレピュテーションのスコアが低い = 通常はバルク電子メール、またはゼロデイのドメイン。

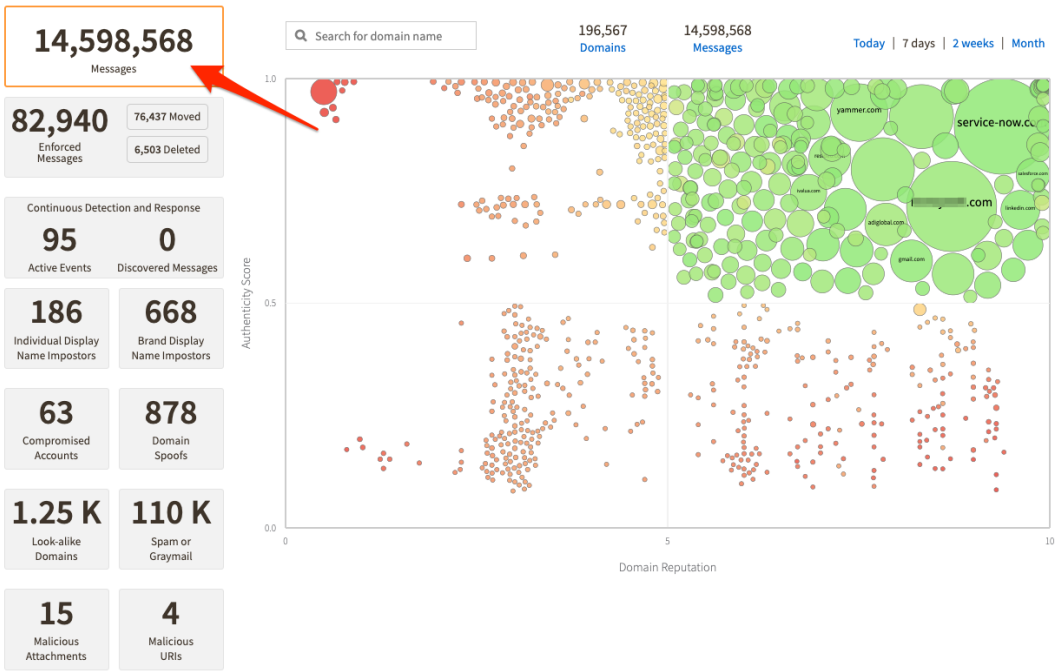
[概要（Overview）] ページの円はそれぞれ送信側ドメインを表し、選択した期間内にそれらが送信したトラフィックの相対量に基づいて円のサイズが示されています。信頼済みのボリュームの大きい正常なメッセージは、右上に緑色の丸で表されます。このクワドラントには、よく知っている送信者の名前が表示されます。上位 200 ドメインが、各クワドラントに表示されます。円をマウスオーバーすると、送信側ドメインからのメッセージ数を確認できます。

信頼性の低い送信者ほど、左下に位置します。

[概要（overview）] ページのクアドラント

結果をフィルタリングして、基本的な攻撃タイプの 1 つのみに限定するには、クアドラント表示の左側にある小さなボックスのいずれかをクリックします。この機能を使用して、潜在的に問題となるメッセージと送信者をすばやく特定できます。

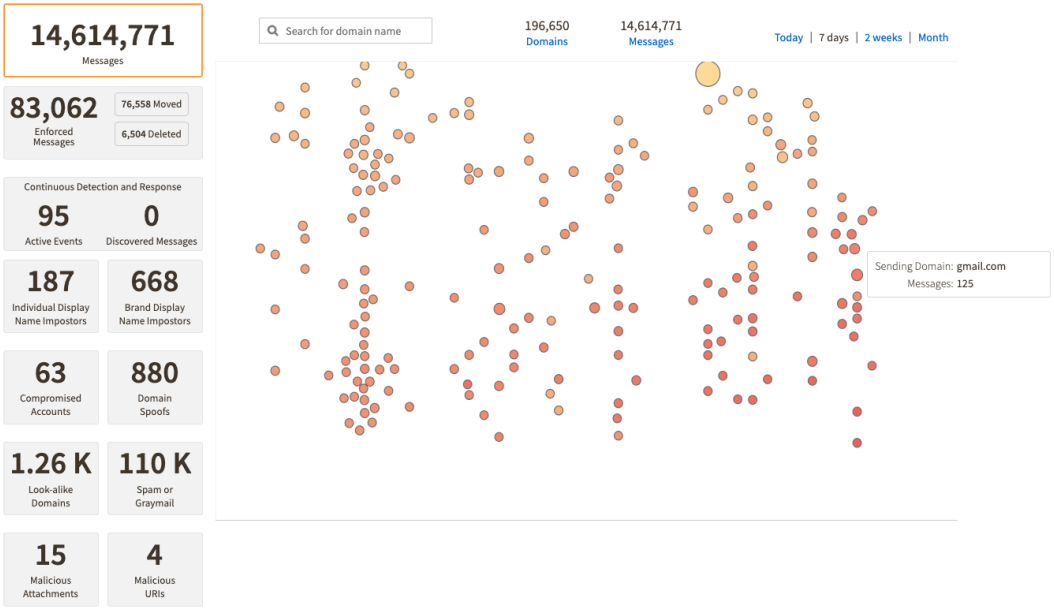
元のトラフィックビューに戻るには、[メッセージ（Messages）] フィルタをクリックします。



[メッセージ（Messages）] フィルタ

ズームイン

いずれかのクワドラント内の空きスペースをクリックすると、そのクアドラントをズームインすることができます。不良な送信者がより簡単に見つかります。円をマウスオーバーすると、送信側ドメインを確認できます。次に例を示します。



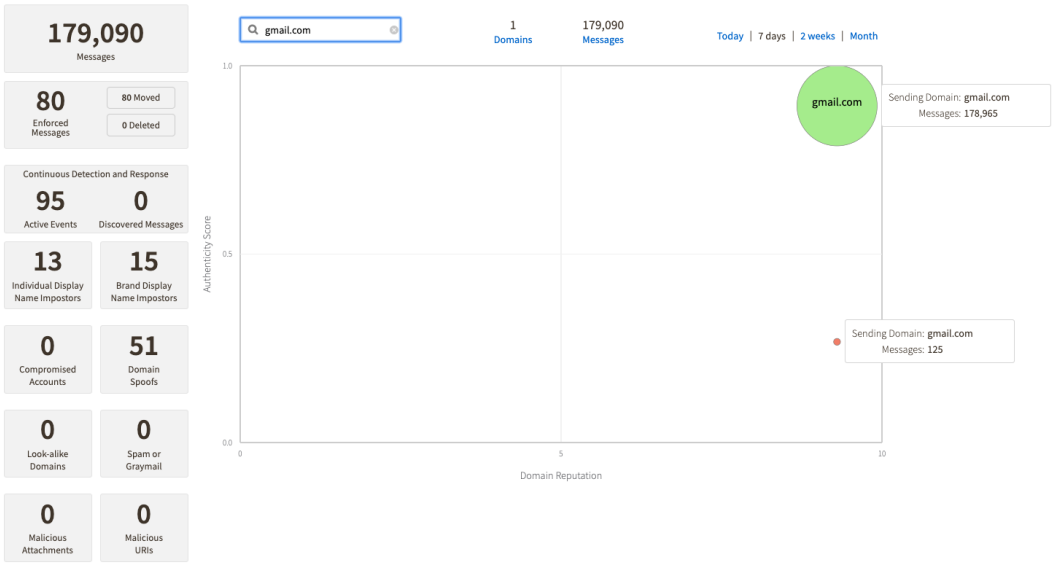
ズームインされたクアドラント

空きスペースを再度クリックすると、ズームアウトして元に戻ります。

クイックドメイン検索

メインの可視化ページで検索ボックスを使用して、特定のドメインから受信したメールの信頼性をすばやく分類することもできます。

たとえば、検索ボックスに「gmail.com」と入力します。次のようなパターンが表示されます。



ドメイン Gmail.com からのメールの検索

これは、高度なフィッシング防御が過去 7 日間に gmail.com ドメインからの 161,016 件の正当なメッセージを分析したことを示しています。より小さい円をマウスオーバーすると、818 件のメッセージは真正性のスコアが低いため、さらに調査が必要な可能性があることが表示されます。

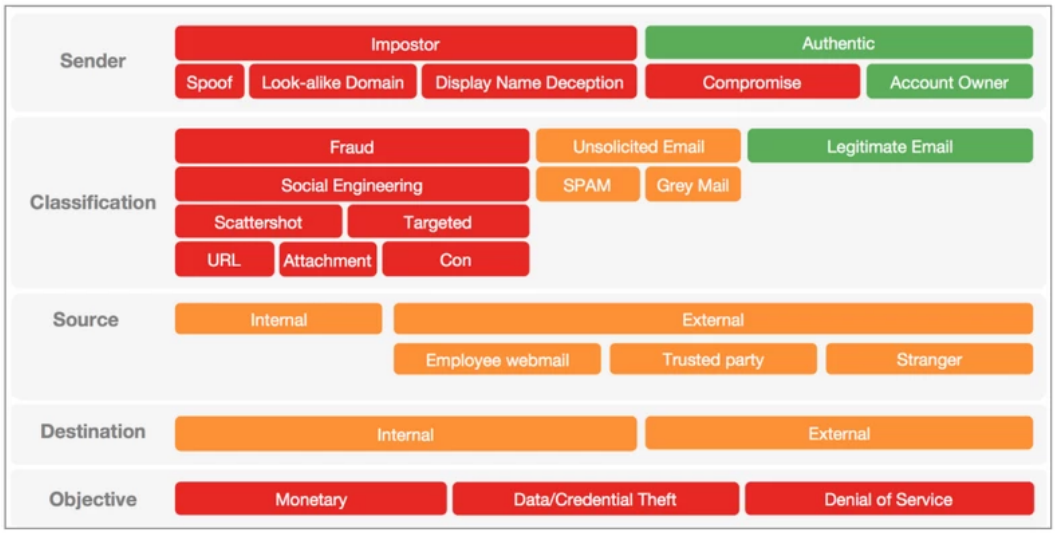
検索ボックスをクリアすると、元の表示に戻ります。

攻撃の分類

このトピックでは、さまざまなタイプの電子メール攻撃について説明します。

攻撃の分類学

信頼できないメッセージ（メッセージの信頼スコアに基づく）は、高度なフィッシング防御によって下図に示される攻撃分類学クラスの 1 つまたは複数に分類されます。



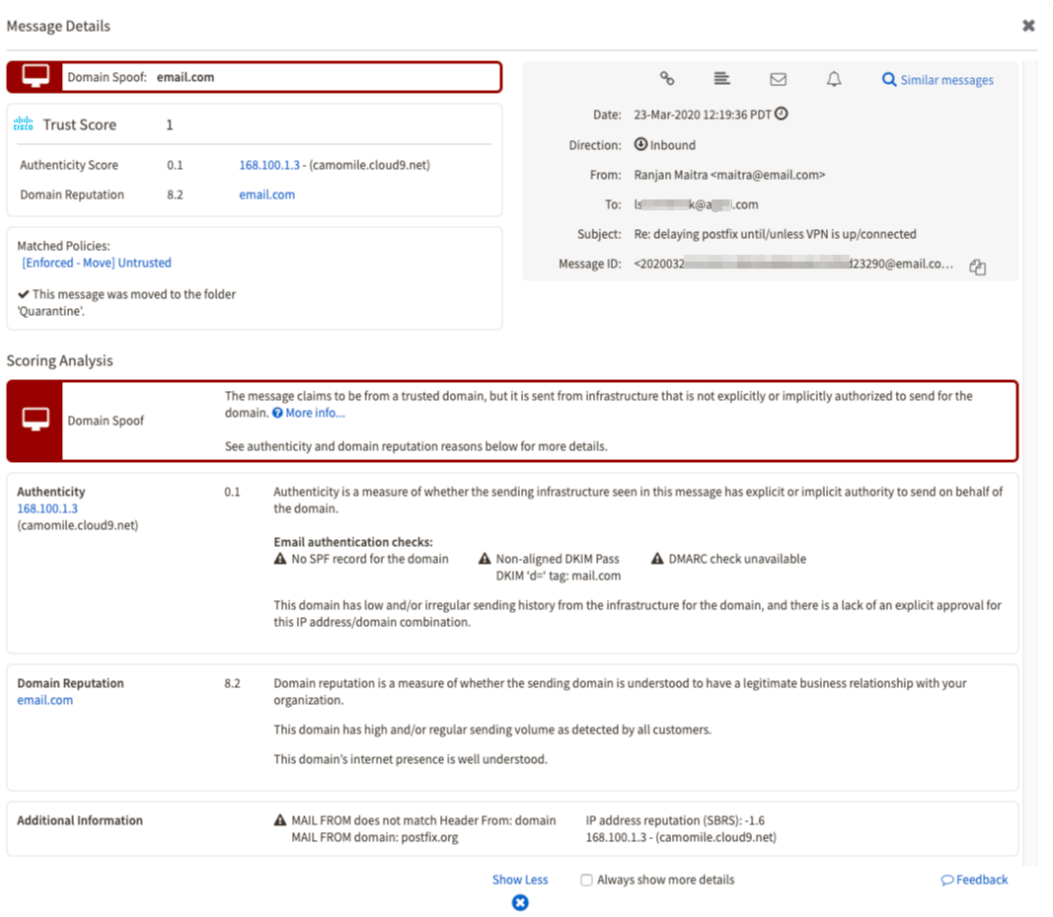
攻撃の分類の分類学

攻撃の分類は、[メッセージの詳細(Message Details)]ビューに表示され、検索やポリシーで使用できます。

分類学の攻撃の分類については、以下で詳しく説明します。

ドメインスプーフィング

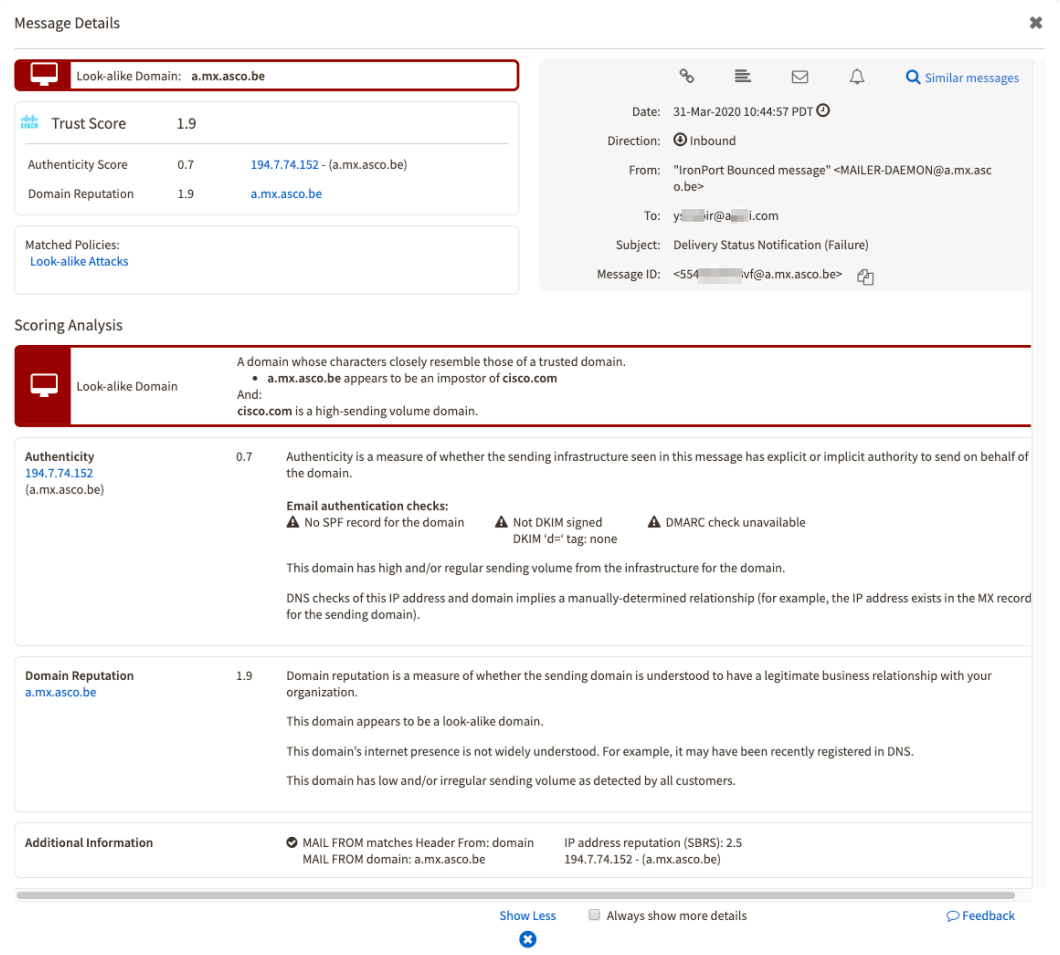
ドメインスプーフィングは、レピュテーションの高いドメインによって送信されたが、高度なフィッシング防御によって、それがそのドメインの本物の送信元から送信されたものでないことが検出されたメッセージです。



ドメインスプーフィングの例

類似ドメイン

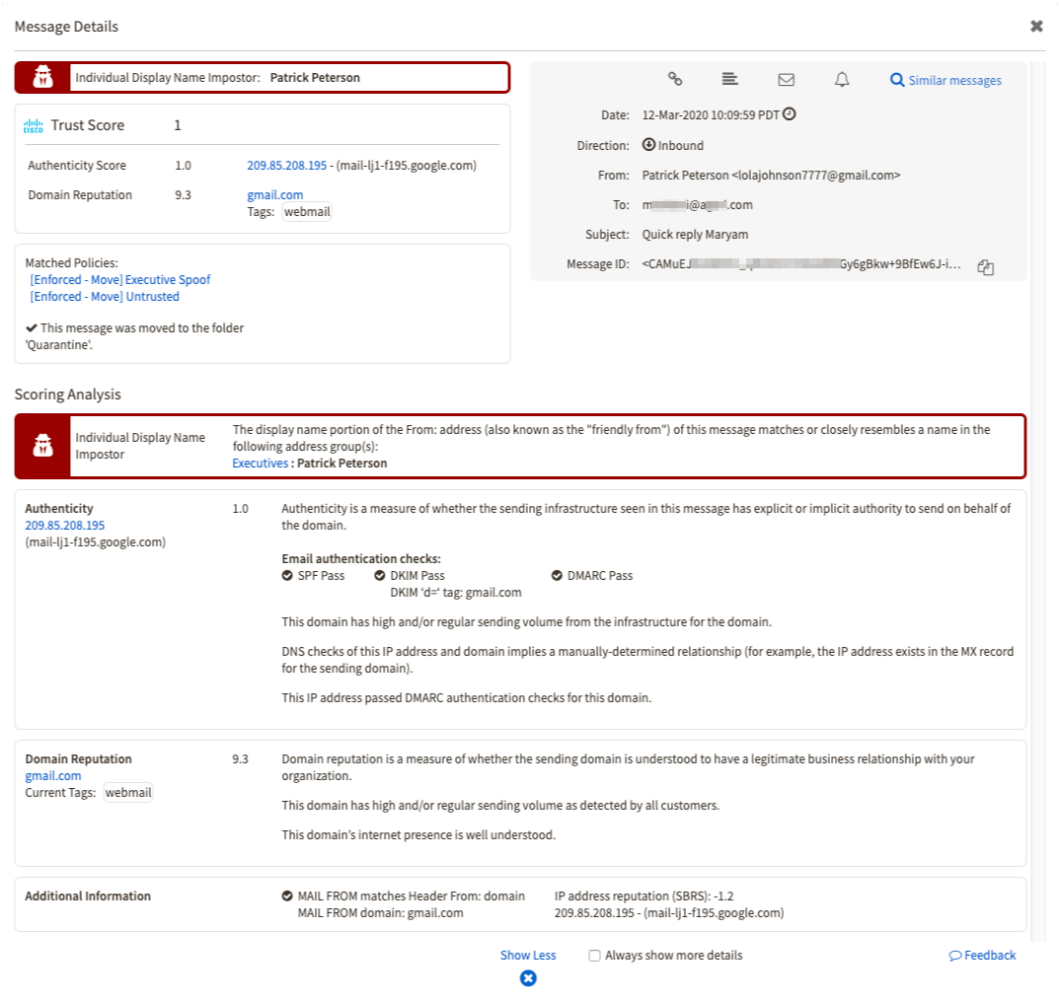
類似ドメイン攻撃とは、ドメインが、社内またはパートナードメインのいずれかのように、非常に信頼できるよく知られたドメインに見せかけようとする場合です。



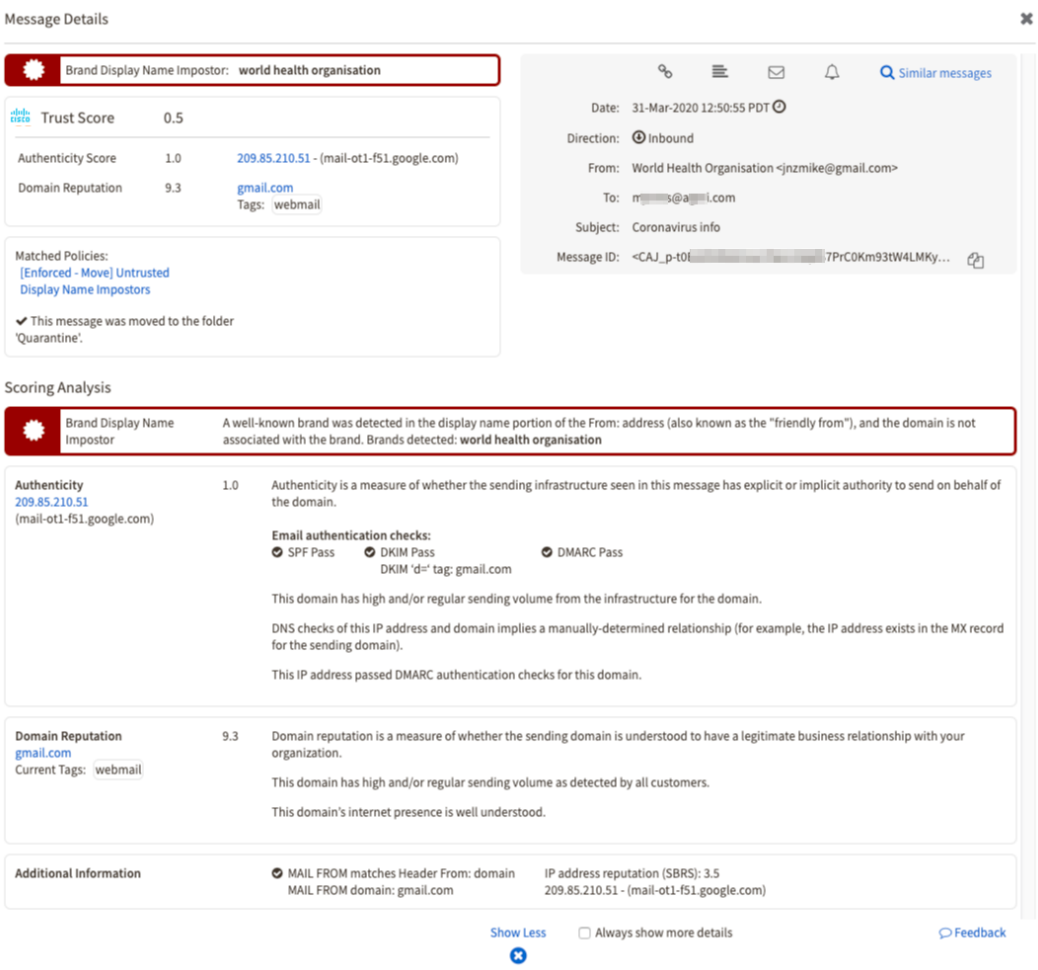
類似ドメインの例

表示名偽装

表示名の偽装は、[差出人(From)]フィールドの表示名部分が、よく知られているブランドや別の個人にみせかけて変更されている場合です。表示名の偽装は、類似ドメインや感染したアカウントなどのその他の攻撃タイプと一緒に頻繁に使用されます。高度なフィッシング防御では、表示名偽装は、個別の表示名偽装とブランドの表示名偽装の 2 つのクラスに分けられます。


Message Details
Individual Display Name Impostor: Patrick Peterson
Trust Score 1
Authenticity Score 1.0 209.85.208.195 - (mail-lj1-f195.google.com)
Domain Reputation 9.3 gmail.com
Tags: webmail
Matched Policies:
[Enforced - Move] Executive Spoof
[Enforced - Move] Untrusted
This message was moved to the folder 'Quarantine'.
Similar messages
Date: 12-Mar-2020 10:09:59 PDT
Direction: Inbound
From: Patrick Peterson <lolajohnson7777@gmail.com>
To:
Subject: Quick reply Maryam
Message ID:
Scoring Analysis
Individual Display Name Impostor
The display name portion of the From: address (also known as the "friendly from") of this message matches or closely resembles a name in the following address group(s):
Executives : Patrick Peterson
Authenticity
209.85.208.195
(mail-lj1-f195.google.com)
1.0
Authenticity is a measure of whether the sending infrastructure seen in this message has explicit or implicit authority to send on behalf of the domain.
Email authentication checks:
SPF Pass
DKIM Pass
DKIM 'd=' tag: gmail.com
DMARC Pass
This domain has high and/or regular sending volume from the infrastructure for the domain.
DNS checks of this IP address and domain implies a manually-determined relationship (for example, the IP address exists in the MX record for the sending domain).
This IP address passed DMARC authentication checks for this domain.
Domain Reputation
gmail.com
Current Tags: webmail
9.3
Domain reputation is a measure of whether the sending domain is understood to have a legitimate business relationship with your organization.
This domain has high and/or regular sending volume as detected by all customers.
This domain's internet presence is well understood.
Additional Information
MAIL FROM matches Header From: domain
MAIL FROM domain: gmail.com
IP address reputation (SBRS): -1.2
209.85.208.195 - (mail-lj1-f195.google.com)
Show Less
Always show more details
Feedback

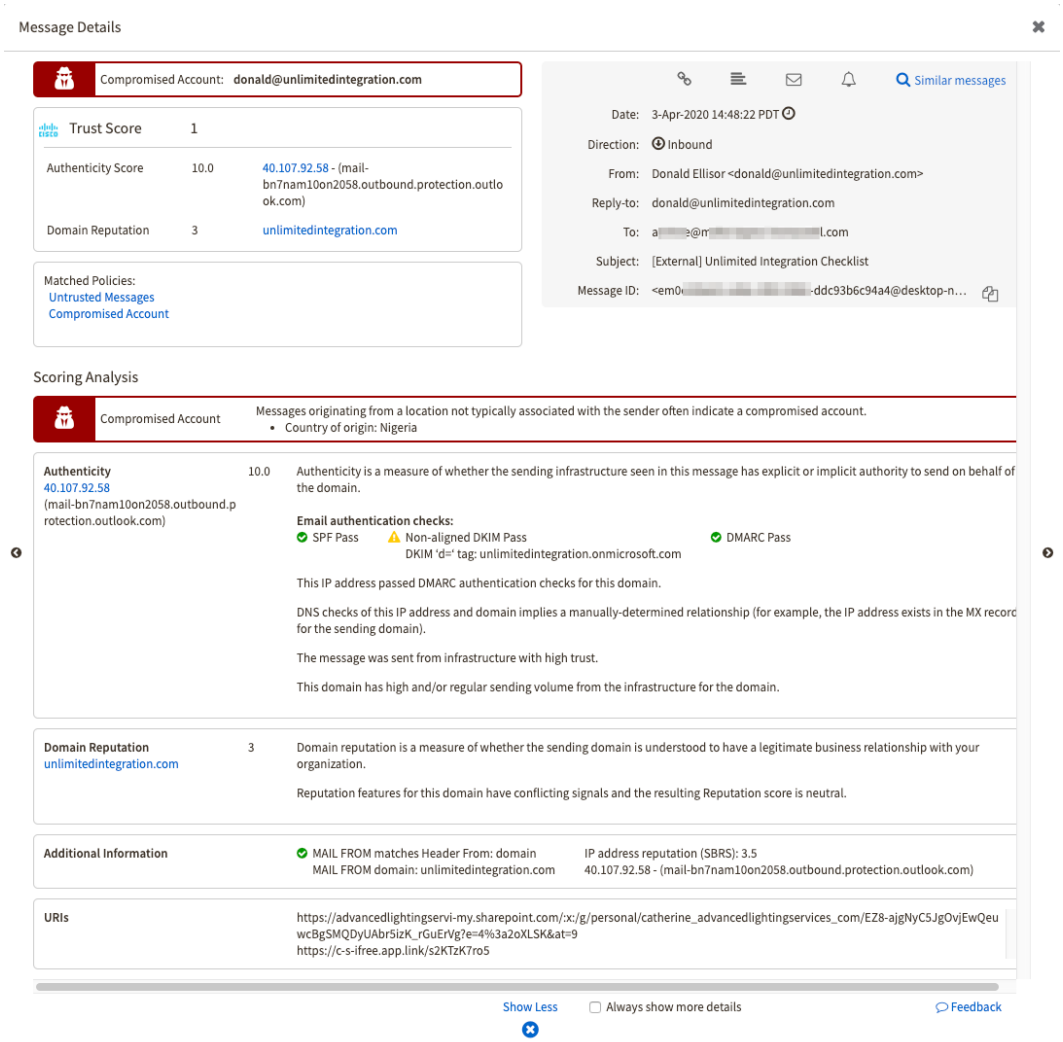
個別の表示名偽装の例



ブランドの表示名偽装の例

感染したアカウント(アカウントテイクオーバー)

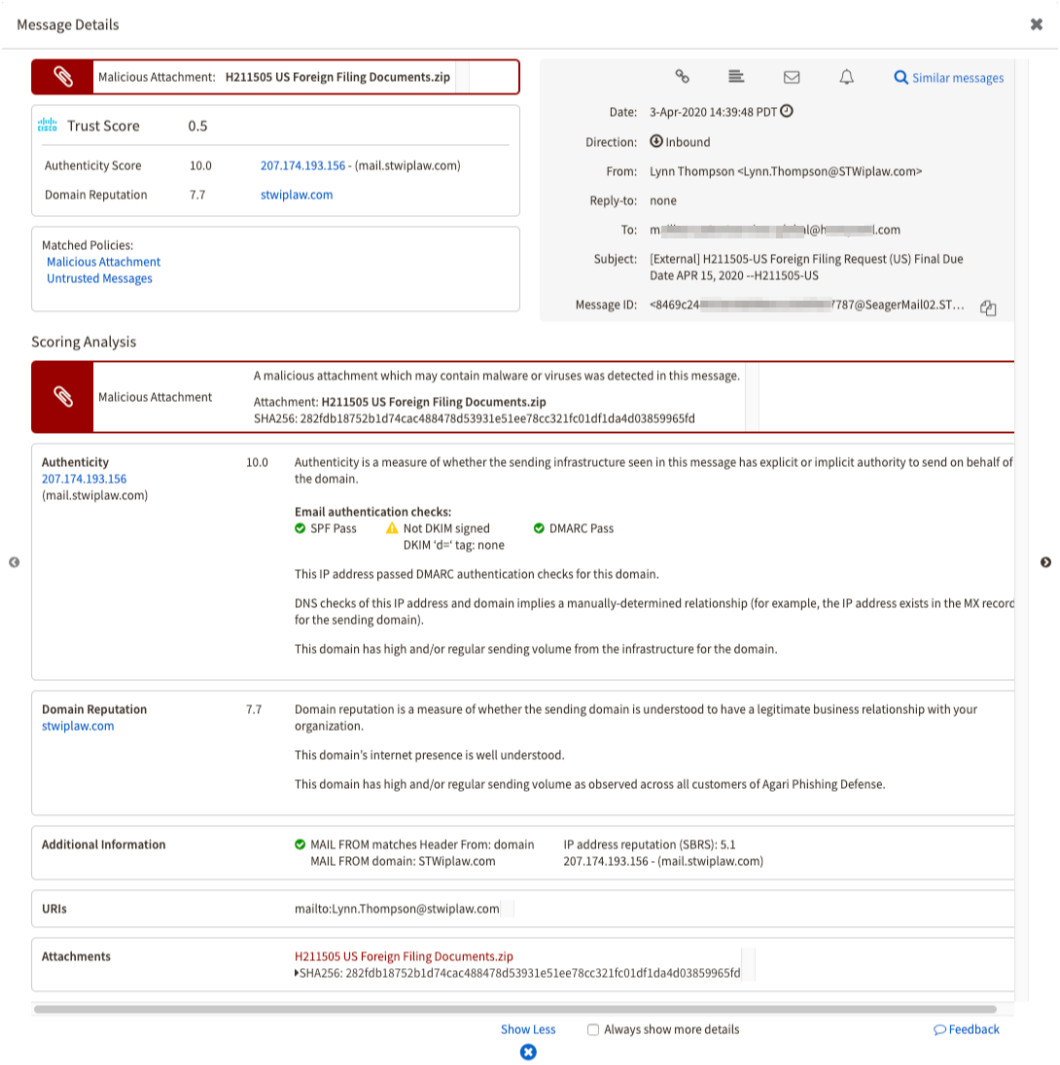
感染したアカウントは、実際の人物/ユーザーに属しているが、不良な攻撃者によって奪取され、悪意のある目的で使用されているアカウントです。高度なフィッシング防御がアカウント テイクオーバーの兆候を見つけた場合、それは感染したアカウントからのメッセージとして分類されます。



感染したアカウントの例

悪意のある添付ファイル

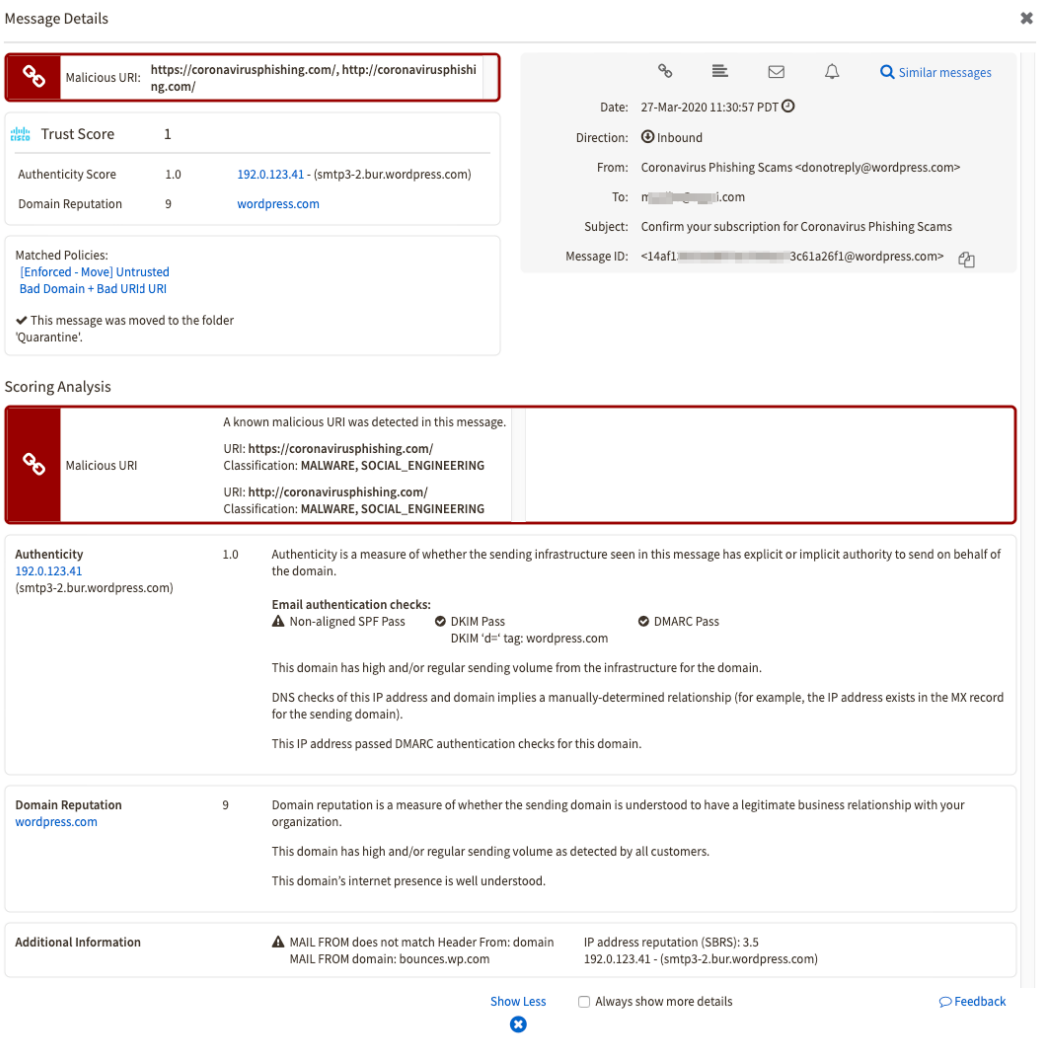
添付ファイルのスキャンが有効な場合、高度なフィッシング防御は、添付ファイルが悪意のあるものである可能性が高い場合に通知します。



悪意のある添付ファイルの例

悪意のある可能性のある URI

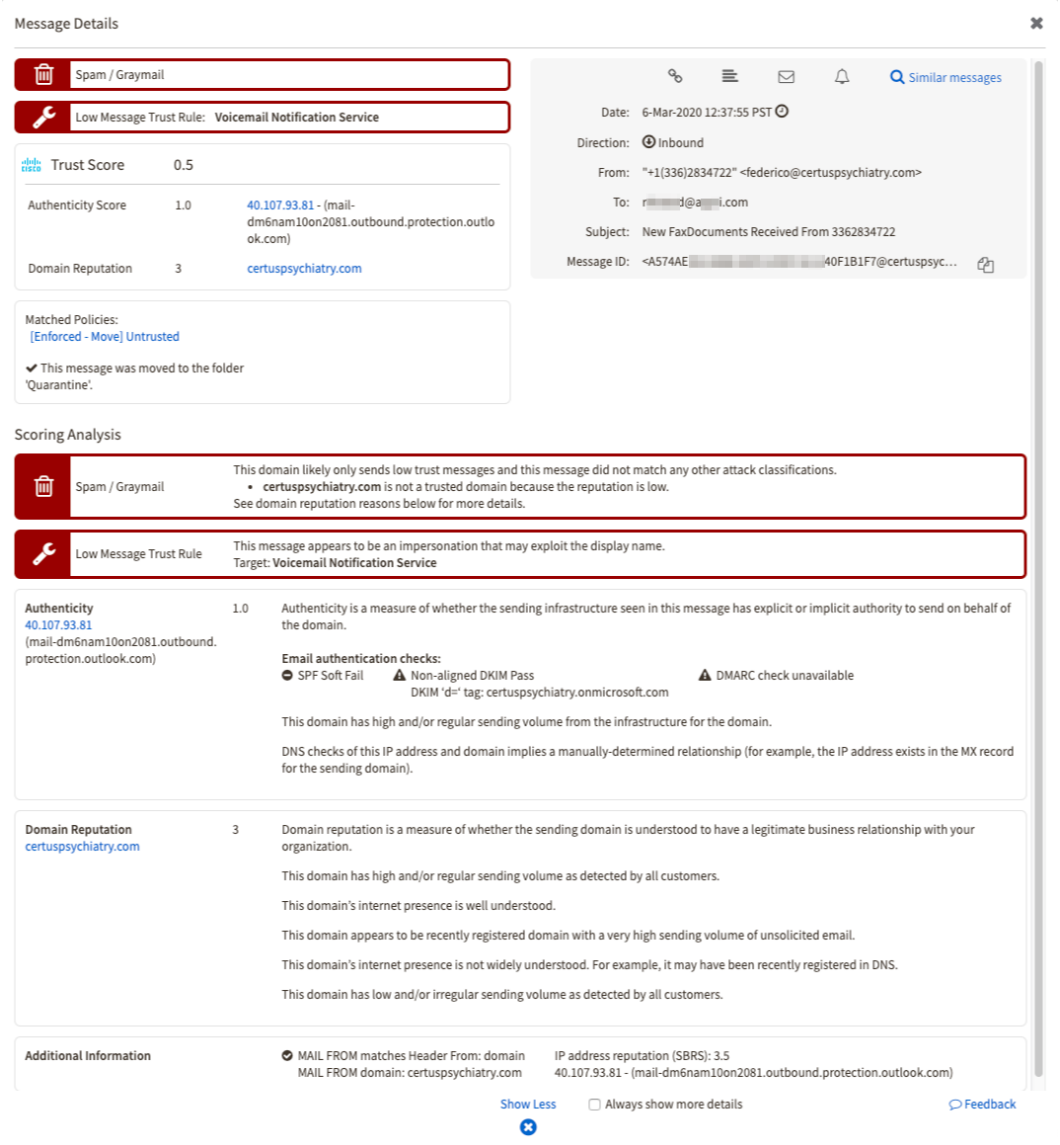
URI スキャンが有効になっている場合、高度なフィッシング防御は、メッセージの本文に悪意のある可能性のある URI が見つかったときに通知します。



悪意のある URI の例

スパムまたはグレイメール

悪意あるメッセージを識別する送信者の分類に加えて、高度なフィッシング防御は、悪意があるとは限らないが、望ましくない電子メールまたは迷惑メールを表すメッセージも分類します。スパムまたはグレイメールの分類に該当するメッセージは、他の送信者の分類に関係なく、信頼するべきではありません。



スパムまたはグレイメールの例

高度なフィッシング防御は、攻撃の分類に加えて、単に信頼性の低いメッセージのルールで送信されたメッセージも分類します。詐欺および未承諾電子メール（スパムおよびグレーメール）の分類学の分類に適合する多くのメッセージは、送信者の分類に関係なく、信頼するべきでないドメインから送信されています。この例では、スパムやグレイメールの攻撃分類のメッセージだけでなく、メッセージの信頼性が低いと識別されたメッセージも示しています。

スコアリング調整

Cisco 高度なフィッシング防御 がメッセージやメッセージに関連付けられた URL に割り当てた信頼スコアを調整する必要がある場合があります。

たとえば、ブランド表示名偽装（BDNI）攻撃と評価されているが、実際には悪意がないことがわかっているメッセージが検出される場合があります。その場合、手動で信頼スコアのスコアリング調整を行うと、すぐに反映され、同様のメッセージがすべて組織に確実に届くようになります。

また、悪意のある BDNI 攻撃として評価されない可能性があるメッセージが、実際には悪意のあるものであることがわかっている場合があります。その場合、BDNI 攻撃と評価するように調整できます。

同様に、悪意のある個別の表示名偽装（IDNI）攻撃として評価されない可能性があるメッセージが、実際には悪意のあるものであることがわかっている場合があります。その場合、IDNI 攻撃として評価するように調整できます。

URL

別の機能では、電子メールに埋め込まれた特定の URL を許可またはブロックできます。URL 全体、ドメイン、またはサブドメインに基づいて URL を許可またはブロックできます。

このガイドでは、悪意があると識別されたことを意味する場合に［陽性（positive）］を使用し、悪意がないと識別されたことを意味する場合に［陰性（negative）］を使用します。

スコアリング調整に関係するメッセージのタイプは次のとおりです。

［BDNI偽陽性（BDNI False Positive）］：悪意ある BDNI 攻撃として評価された悪意のないメッセージ。

［BDNI偽陰性（BDNI False Negative）］：悪意ある BDNI 攻撃であるが、悪意がないと評価されたメッセージ。

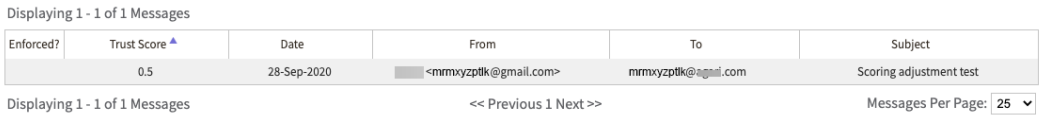
［IDNI偽陰性（IDNI False Negative）］：悪意ある IDNI 攻撃であるが、悪意がないと評価されたメッセージ。

次のチュートリアルでは、これらすべてのシナリオについて説明します。

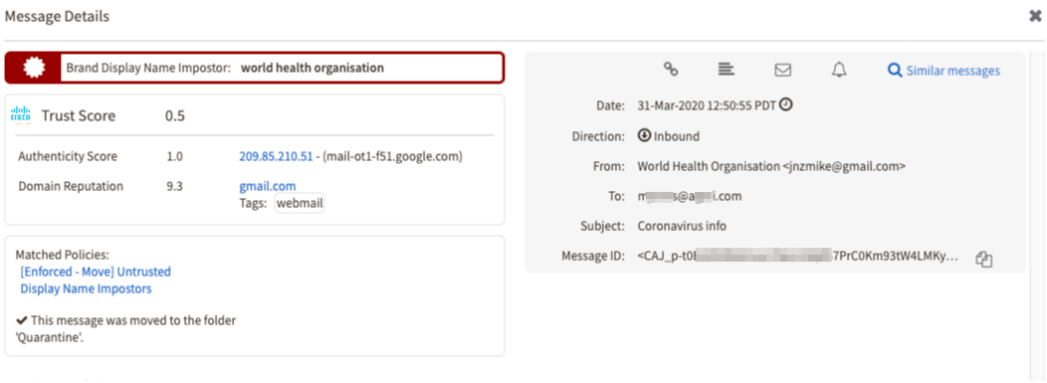
スコアリング調整：BDNI 偽陽性

このウォークスルーでは、脅威として評価されたメッセージを識別し、脅威ではないと評価するように調整を行います。

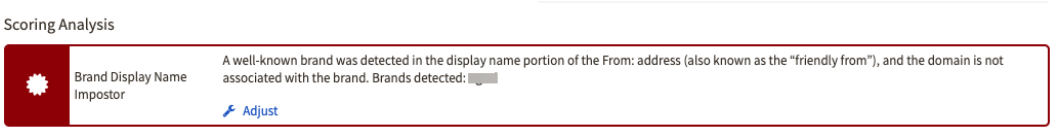
1. ブランド表示名偽装（BDNI）として識別されたメッセージを見つけます。



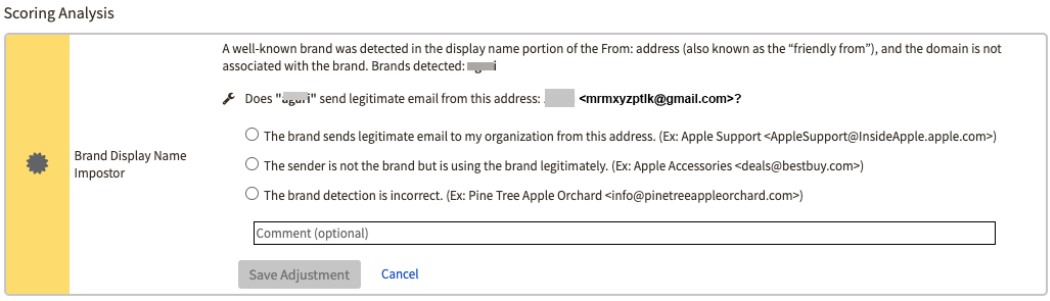
2. メッセージをクリックすると、メッセージの詳細ウィンドウが開きます。この例では、このメッセージは BDNI 攻撃として評価されていますが、実際にはあなたが自分に送信した無害なメッセージであることがわかります。



3. [詳細を表示（Show More）] の下のプラス記号をクリックして画面を展開し、[スコアリング分析（Scoring Analysis）] を表示します。



4. [調整（Adjust）] リンクをクリックします。ウィンドウが開き、スコアリングオプションが表示されます。

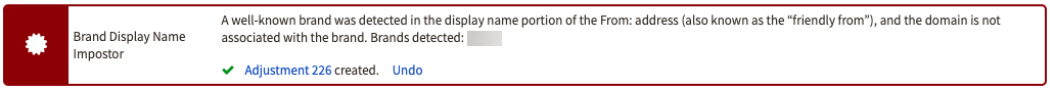


5. [送信者はブランドではありませんが、ブランドを正当に使用しています（The sender is not the brand but is using the brand legitimately）] の横にあるボタンを選択します。下のフィールドにコメントを入力できます（例：「*自分の Gmail アカウントからのメッセージ*」）。完了したら、[調整の保存（Save Adjustment）] をクリックします。

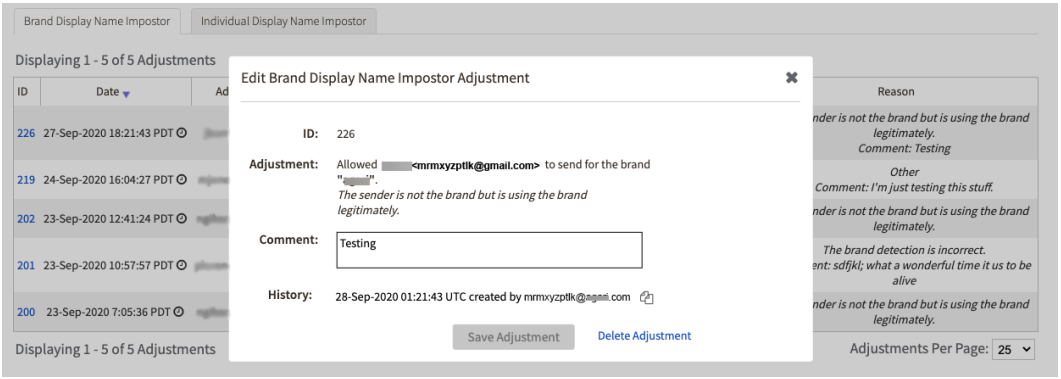
   調整を作成したので、送信者と表示名の組み合わせからメッセージは引き続き他のすべてのリスク要因に基づいてスコアリングされますが、BDNI 攻撃としてスコアリングされることはありません。

   スコアリング調整が反映されるまでには、約 5 分かかります。

6. すべてのスコアリング調整を表示するには、[<adjustment number>の調整（Adjustment <adjustment number>）] をクリックします。たとえば、ここでは [226の調整（Adjustment 226）] として示されています。



7. 調整のリストから任意の調整を選択します。コメントを変更して調整を再保存するか、調整を削除できる新しいウィンドウが表示されます。



   調整を削除すると、その送信者と表示名の組み合わせからメッセージが再び評価され、BDNI 攻撃として分類されます。

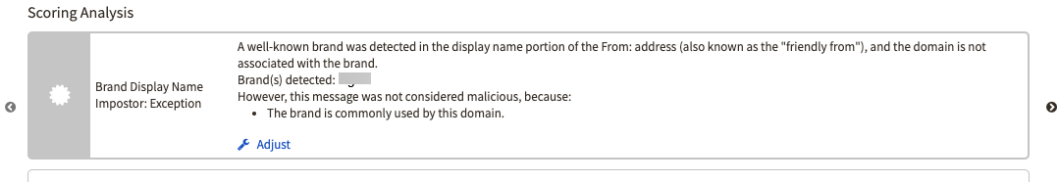
削除された調整は、調整のインデックスには表示されません。監査ログには、調整の削除の記録が含まれています。

スコアリング調整：BDNI 偽陰性

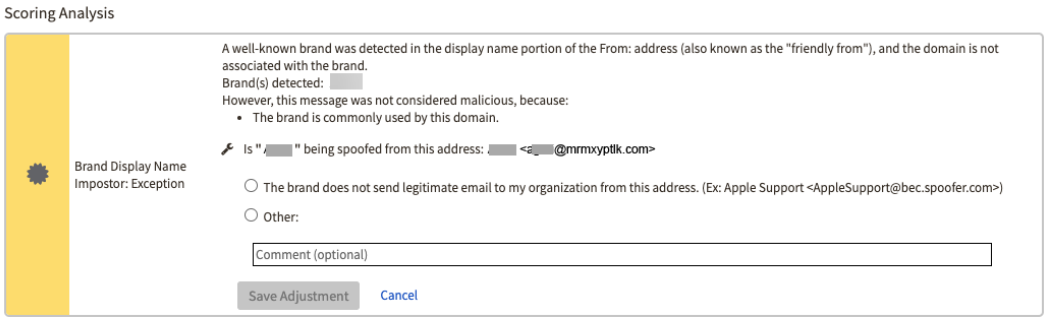
このウォークスルーでは、信頼できると評価されたメッセージを識別し、脅威であると評価するように調整を行います。

1. ブランド表示名偽装（BDNI）の可能性があるとして識別されたが、悪意がないと判断され、高いスコアが与えられたメッセージを見つけます。

2. メッセージをクリックしてメッセージの詳細を表示し、[スコアリング分析（Scoring Analysis）] を見つけて、メッセージが BDNI 攻撃としてスコアリングされなかった理由を確認します。



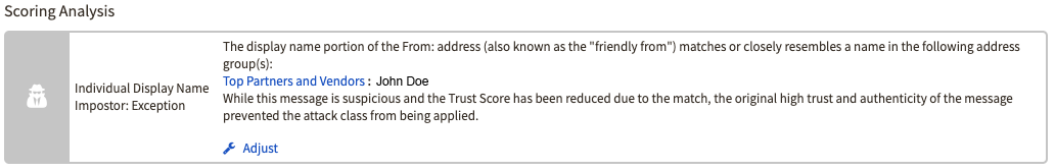
3. [調整（Adjust）] リンクをクリックして、調整の詳細を開きます。このメッセージが実際に悪意があると思われる場合は、含まれている理由の 1 つを選択するか、[その他（Other）] を選択してコメントを入力して理由を含めることができます。



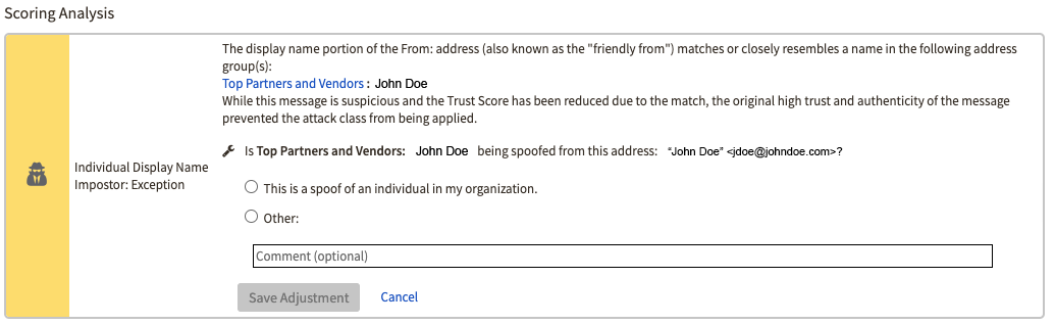
完了したら、[調整の保存（Save Adjustment）] をクリックします。

スコアリング調整：IDNI 偽陰性

IDNI 偽陰性のスコアリング調整を行う手順は、BDNI スコアリング調整を行う手順と同じです。このような場合は、悪意がないと評価されたメッセージを識別し、上記の手順を使用して、必要に応じてスコアリング調整を行います。



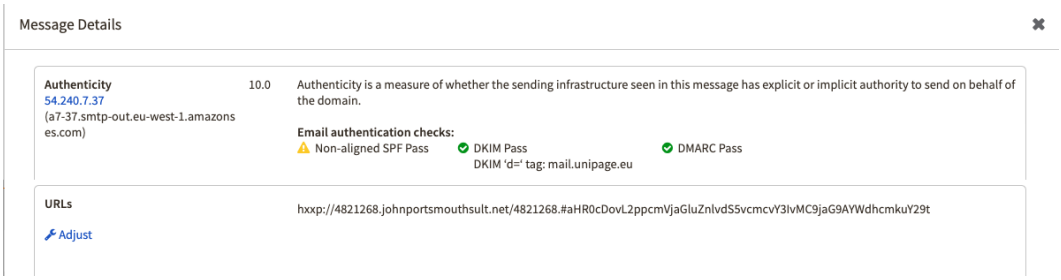
上記のメッセージは疑わしいものとして識別されましたが、本物であると評価されました。以下に示すように、[調整（Adjust）] をクリックしてこのスコアリングを変更できます。詳細については、上記の BDNI スコアリングの手順に従ってください。



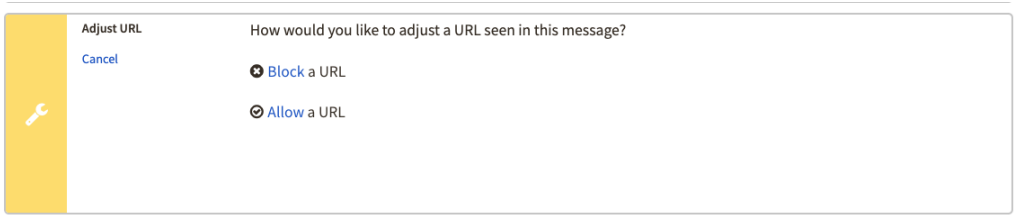
URL をブロックまたは許可する

URL 全体、ドメイン、またはサブドメインに基づいて、メッセージに埋め込まれた URL をブロックまたは許可できます。これを行うには、まず、URL が埋め込まれたメッセージの [メッセージの詳細（Message Details）] ページを見つけます。（メッセージに URL が埋め込まれていない場合、この機能はメッセージの詳細に表示されません）

1. [メッセージの詳細（Message Details）] ページを開き、[URL] のラベルまで下にスクロールします。

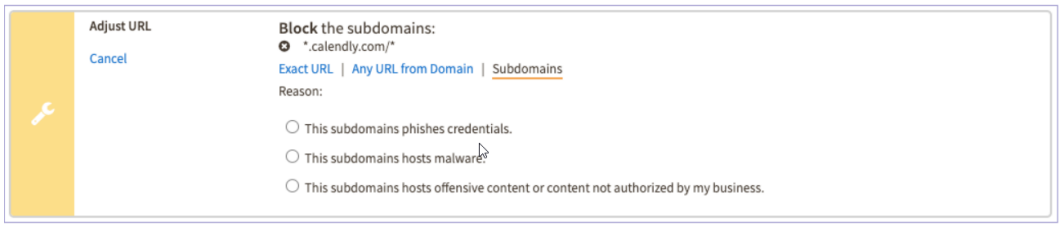


URL をブロックするか許可するかを調整するには、[調整（Adjust）] をクリックします。開いた画面で、URL をブロックするか許可するかを選択できます。[ブロック（Block）] を選択しましょう。



2. ブロックする URL をクリックします。選択できる URL のリストがある場合がありますが、この場合は 1 つだけです。

3. 3 つのブロックのオプションからいずれかを選択します。
    - 正確な URL をブロックする
    - ドメインからのすべての URL をブロックする
    - サブドメインからのすべての URL をブロックする
4. 例として、[すべてのサブドメインをブロック(Block any Subdomains)] を選択してみましょう。



5. [URLの調整(Adjust URL)] パネルを下にスクロールして追加のオプションを表示し、必要なものを選択したら、[サブドメインのブロック(Block Subdomains)] ボタンをクリックします。

メッセージ

Cisco 高度なフィッシング防御 によって分析されたメッセージ、およびそれらのメッセージに関するデータと攻撃分析は、いくつかの方法で表示できます。リアルタイムのダッシュボードビュー([分析(Analyze)] > [ダッシュボード(Dashboard)]、[リアルタイム(Real time)] タブ)に加えて、メッセージリスト([分析(Analyze)] > [メッセージ(Messages)])とメッセージの検索([分析(Analyze)] > [メッセージの検索(Search Messages)])の 2 つの便利なビューがあります。

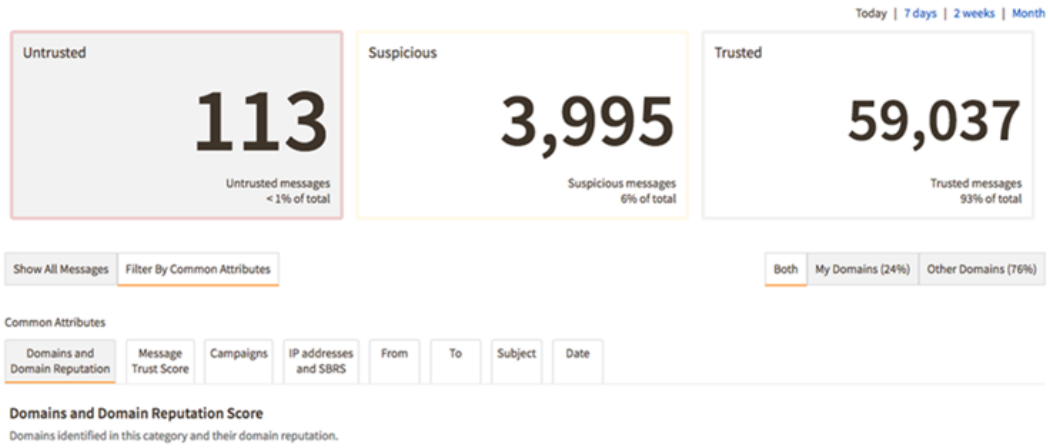
メッセージを表示する

概要ページでは、スプーフィング、名前の偽装、類似ドメイン、および正常なメッセージのインタラクティブな可視化が提供されますが、[分析(Analyze)] > [メッセージ(Message)] ページでは [運用(Operational)] 表示より多くのことが提供され、データを調査するために役立ちます。

[メッセージ(Messages)] ページの集計カウント

メッセージは、[非信頼(Untrusted)]、[疑わしい(Suspicious)]、[信頼済み(Trusted)] の 3 つのカテゴリに分けられます。ボックスをクリックすると、そのカテゴリを選択できます。

さらにドリルダウンするには、[共通の属性によるフィルタ処理(Filter by Common Attributes)] をクリックします。



共通の属性によるフィルタリング

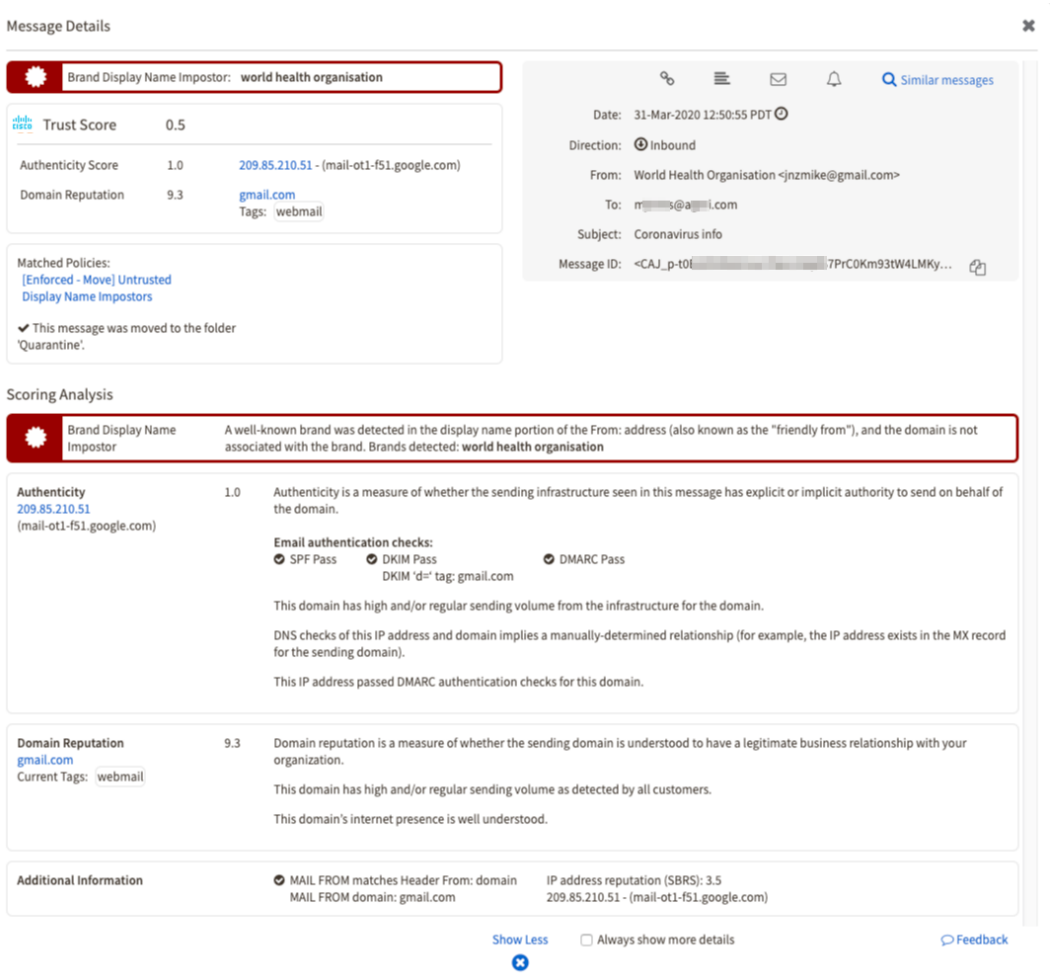
デフォルト表示では、非信頼メッセージがドメイン別にソートされます。ソートする他のタブをクリックして、視覚化することもできます。

- [メッセージの信頼スコア(Message Trust Score)]:信頼スコアによるこれらの信頼できないメッセージの分布はどうなっているか確認できます。
- [キャンペーン(Campaigns)]:これらの信頼できないメッセージのうち、同じ件名の送信者からのメッセージの数を確認できます。
- [IPアドレス/SBRS(IP Address/SBRS)]:信頼できないとスコアリングされたすべてのメッセージのうち、どれがそれらのメッセージの上位送信側 IP アドレスであり、それらの IP のレピュテーションスコアがいくつであるかを確認できます。
- [差出人/宛先/件名/日付(From / To / Subject / Date)]:最もリスクの高い送信者は誰かを確認できます。最もリスクの高い受信者は誰か? 特定の日に攻撃されたか?

メッセージの詳細を表示する

信頼できない送信者から送信されたメッセージの詳細を表示したいというケースは多くあります。特定の攻撃タイプによって送信されたメッセージは左側のタイルで表示され、特定の送信者によって送信されたメッセージは赤い丸で表示されます。

1. 攻撃タイプのタイルの 1 つをクリックし、[メッセージの表示(View messages)] をクリックしてその攻撃タイプのメッセージのリストを表示するか、赤い丸のいずれかをクリックして、その送信者によって送信されたメッセージのリストを表示します。このメッセージは、メッセージの検索結果に表示されます。一覧をさらに限定するためにフィルタ処理することができます。
2. メッセージをクリックすると、[メッセージの詳細(Message Details)] が表示されます。



[メッセージの詳細(Message Details)] ペイン

[メッセージの詳細(Message Details)] ページには、次のようなメッセージに関する情報が表示されます。

- ヘッダーとスコアリング(および付けられたスコアの理由)
- 組織の [メッセージの評価(Evaluate Messages)] 設定(「「[メッセージの評価(Evaluate Messages)]」ページ 199」を参照してください)で [すべてのメッセージ(All messages)] が選択されている場合のメッセージの方向性(受信、送信、または内部)
- メッセージが一致した場合、どのポリシーが一致したか(各ポリシーは特定のポリシーイベントへのリンクです)
- メッセージが適用されたかどうか(適用が有効になっている場合)

内部メッセージと送信メッセージには、[メッセージの信頼スコアの理由(Message Trust Score Reasons)] セクションが表示されません。

高度なフィッシング防御はメッセージの本文を追跡しないことに留意してください。

ただし、多くの場合は、[送信側ドメイン(Sending Domain)] と [送信側IPアドレス(Sending IP Address)] のクロスリンクに従った方がより役立ちます。

- [送信側ドメイン(Sending Domain)] リンクは、次の質問に答えます。このドメインが組織に電子メールを送信している頻度はどのぐらいか、また、どのぐらい多くの IP アドレスから送信されているのか? メッセージの大半は正当なものなのか?

- [送信側IPアドレス(Sending IP Address)]リンクは、次の質問に答えます。この IP アドレスは、他のどのドメインのために、組織へ電子メールを送信しているのか? その IP は、信頼できるのか? それは少数のドメイン、または多数のドメイン宛てに送信しているのか?

[メッセージの詳細(Message Details)] ページの右上では以下のアイコンがクリックできます。

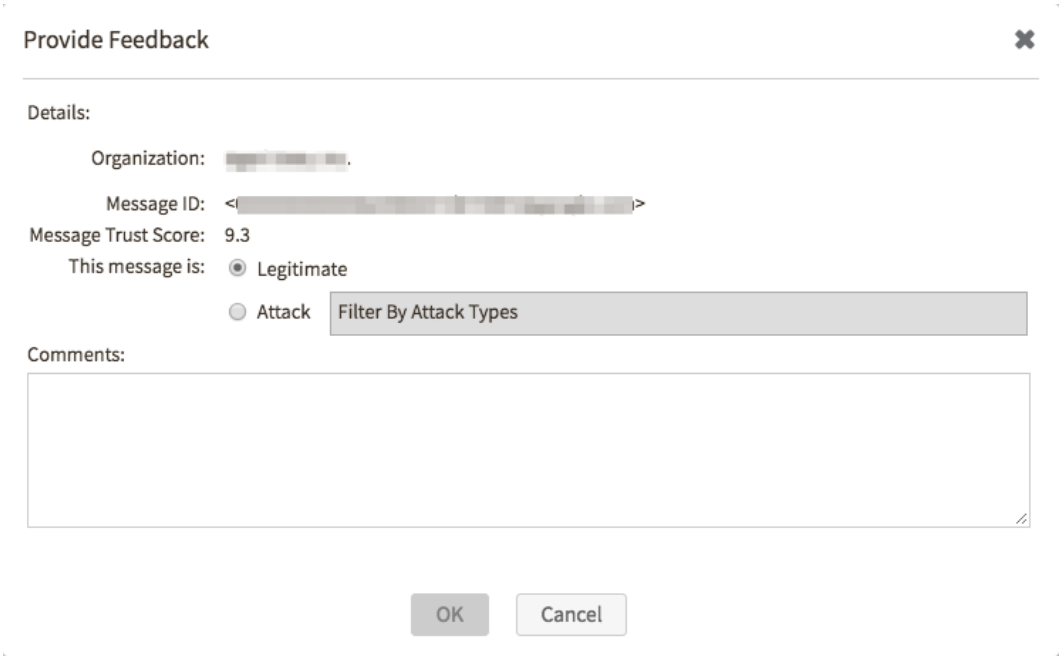
- [メッセージの詳細リンク(Message Details link)]アイコン( ) : メインウィンドウ(この表示に直接リンクする URL を持つ)内でメッセージの詳細を表示できます。
- [ヘッダー(Headers)]アイコン( ) : メッセージ内のすべてのヘッダーを表示できます。
- [メール(Mail)]アイコン( ) : メッセージの詳細の表示を同僚に送信できます。
- [ベル(Bell)]アイコン( ) : このメッセージに一致する条件を持つポリシーを作成できます。ポリシーの作成の詳細については、「「ポリシーを作成する」 ページ 156」を参照してください。
- [メッセージのフィードバック(Message Feedback)]アイコン( ) : メッセージのスコアリングに関するフィードバックを提供できます。詳細については、「「メッセージのフィードバックを送信する」 下」を参照してください。

メッセージのフィードバックを送信する

高度なフィッシング防御が電子メールを正しく識別する方法を改善する優れた方法は、個別のメッセージについてフィードバックを提供することです。これは、電子メールプロバイダーやクライアントソフトウェアに、受信トレイのメッセージについて「これはスパムです」と伝えるのとまったく同じですが、高度なフィッシング防御では、メッセージの脅威に関するより具体的な詳細を提供できます。

1. [メッセージの分析(analyze messages)] ページ([すべてのメッセージの表示(Show All Messages)] タブの[分析(Analyze)] > [メッセージ(Messages)])または [メッセージの検索(Search Messages)] ページ([分析(Analyze)] > [メッセージの検索(Search Messages)])など、メッセージのリストが表示されているビューでメッセージをクリックして、メッセージの詳細を表示します。
2. [メッセージの詳細(Message Details)] ダイアログボックスの右上隅にある [メッセージのフィードバック(Message Feedback)] アイコン( )をクリックします。

   [フィードバックの提供(Provide Feedback)] ダイアログボックスでは、メッセージの信頼スコアに基づいて、メッセージはすでに正規または攻撃として分類されています。



3. 次の操作を実行できます。
    - オプションボタンをクリックして、メッセージを正規から攻撃に、またはその逆に切り替えます。
    - [攻撃(Attack)] フィールドをクリックし、追加の攻撃タイプを選択するか、すでにフィールドにある攻撃タイプの [X] をクリックして、攻撃タイプを追加または削除します([攻撃(Attack)] が選択されている場合)。
4. [OK] をクリックします。([OK] ボタンは、変更を加えた場合にのみ有効になります)

メッセージに関して提供した情報は Cisco に返送され、データモデルに組み込まれて将来のメッセージ分類の改善につながることがあります。

メッセージ検索

高度なフィッシング防御には、非常に強力で詳細なメッセージ検索機能が含まれています。特定のメッセージデータを検索できるだけでなく、高度なフィッシング防御によって識別されるメッセージの特性を検索することもできます。

メッセージ検索が単なる空白の状態ではなく、それぞれの、そしてすべての検索条件を定義するための単なる出発点でもないというのが高度なフィッシング防御の強みの 1 つです。多くの場所で、1 つ以上の検索条件が事前に定義されたメッセージの検索結果ページにジャンプできます。たとえば、ダッシュボードで [ドメインスプーフィング(Domain Spoofs)] をクリックし、[メッセージの表示(Show Messages)] をクリックすると、次の条件が事前に定義されたメッセージの検索結果ページが表示されます。

- 日付の範囲:ダッシュボードページで設定した範囲
- 攻撃タイプ:ドメインスプーフィング
- 信頼スコアの範囲:0.0 ～ 5.1

同様に、[分析(Analyze)] > [メッセージ(Messages)] ページに移動し、[疑わしいメッセージ(Suspicious messages)] をクリックし、[差出人(From)] などの一般的な属性をクリックしてからリスト内の番号をクリックすると、メッセージの検索結果ページに移動します。このページでは、そのアドレスからのメッセージのうち、指定された期間内の、疑わしいメッセージについての信頼スコアの範囲内にあるものすべてが表示されます。

これらのショートカットは非常に便利ですが、ゼロから開始するか多くのショートカットのいずれかから開始するかにかかわらず、検索結果を微調整する機能も便利です。

検索が実行されると、検索に使用されたフィールドがオレンジ色で囲まれます。

このトピックでは、[メッセージの検索(Search Messages)] ページのすべてのフィールドについて説明します。

検索フィールド	説明
差出人(From)、宛先(To)、返信先(Reply-To)、件名(Subject)	これらはすべて、高度なフィッシング防御によってメッセージが取り込まれたときにメッセージヘッダーのそれぞれのフィールドから収集されます。電子メールアドレスまたは件名の全部または一部を入力します。これらのフィールドの検索は、大文字と小文字を区別しない部分一致です。たとえば、[件名(Subject)] フィールドに「pens」と入力すると、「Shop My Etsy Pens Store」、「That's too expensive for me」、「Please buy some pens from Amazon」などの件名のメッセージがすべて検索されます。 ⚠ 100 文字に制限されています。
添付ファイル(Attachment)	このフィールドは、組織の設定(「「組織設定」 ページ 197」を参照してください)で添付ファイルのスキャンが有効になっている場合にのみ使用でき、次の 5 つのオプションがあります。 • [添付ファイルあり(has any attachment)]: 添付ファイルのあるメッセージを検索します。 • [悪意のある可能性のある添付ファイルあり(has a likely malicious attachment)]: 高度なフィッシング防御によって悪意のある可能性があると判断された添付ファイルが 1 つ以上あるメッセージを検索します。 • [添付ファイル名あり(has attachment name)]: このフィールドに入力された内容のすべてまたは一部を含む添付ファイル名を持つメッセージを検索します。他のテキスト検索フィールドと同様に、これは部分一致であり、大文字と小文字は区別されません。 • [添付ファイル名拡張子あり(has attachment filename extension)]: 入力した拡張子のいずれかが含まれている添付ファイル名を持つメッセージを検索します。ファイル名拡張子は、ファイル名の右端のピリオドに続く部分です。1 つまたは複数の拡張子をカンマで区切って入力します。他のテキスト検索フィールドと同様に、これは部分一致であり、大文字と小文字は区別されません。たとえば、PROP と入力すると、system.properties という名前のファイルが検索されます。 • [添付ファイルハッシュあり(has an attachment hash of)]: 入力されたハッシュに一致するメッセージを検索します。ハッシュは、暗号化アルゴリズムによって生成され、ファイルの内容を一意に識別します。ファイルに変更が加えられた場合、そのファイルに対して生成されたハッシュは通常大幅に変更されるため、元のハッシュと現在のハッシュを比較すると、ファイルが変更されたかどうかを簡単に判断できます。これは、大文字と小文字を区別する完全一致です。 ⚠ 100 文字に制限されています。
受信した期間(Received between)	これは、検索の開始日と終了日(その日を含む)を定義します。 • 開始日は、現在の日付から 60 日前までにする必要があります。(高度なフィッシング防御は 60 日より前のメッセージデータを消去します)

検索フィールド	説明
	• 終了日は、現在の日付より後にすることはできません。
信頼スコアの範囲（Trust Score Range）	これは、検索で見つかるメッセージの信頼スコアの上限と下限（選択した値を含む）を定義します。範囲を変更するには、下限と上限のスライダをドラッグします。
真正性スコアの範囲（Authenticity Score Range）	これは、検索で見つかるメッセージの真正性スコアの上限と下限（選択した値を含む）を定義します。範囲を変更するには、下限と上限のスライダをドラッグします。
一致したポリシー（Matched policy）	これは、検索で見つかるようメッセージが適用される必要がある単一のポリシーを定義します。選択できるポリシーのリストには、有効（およびアクティブ）、無効、およびオンデマンドポリシー（「「オンデマンドポリシー」 ページ 164」を参照してください）といった高度なフィッシング防御のすべてのポリシーが含まれます。

適用（Enforcement）	これは、メッセージがポリシーによって適用されているかどうか、および適用の方法を定義します。次から 1 つのオプションを選択します。
	• [すべてのメッセージ（All Messages）]（デフォルト）：何らかの方法で適用されたメッセージ。
	• [保留中（Pending）]：適用が定義されているが、まだ実施されていないポリシーに一致するメッセージ。
	• [適用済み（Enforced）]：ポリシーによって適用されたメッセージ。以下の適用のサブカテゴリも選択できます。
	  • 任意のフォルダに移動済み（Moved（to any folder））
	  • 受信トレイに移動済み（Move to Inbox）
	  • 削除（Deleted）
	• [適用失敗（Enforcement failed）]：適用アクションのあるポリシーに一致したが、ポリシーによって適用されなかったメッセージ。これは通常、MS enforcement API がエラーを返したことによるものです。
	• [適用不試行（Enforcement not attempted）]：適用が試みられなかったメッセージ。これは、メッセージがポリシーに一致しなかったか、適用アクションがないポリシーに一致したことが原因である可能性があります。この検索パラメータは、オンデマンドポリシーで適用するメッセージを見つけるのに役立ちます。

メッセージID（Message ID）	メッセージ ID に一致する高度なフィッシング防御の特定のメッセージを検索するには、このフィールドに単一のメッセージ ID を入力します。 ⚠ 100 文字に制限されています。
方向（Direction）	これは、メッセージの方向性を定義します。フィールドをクリックして、次から 1 つ以上の方向を選択します。 • [受信（Inbound）]：組織外のどこかから組織に送信されたメッセージ。[方向（Direction）] 列では、受信メッセージが ⓘ アイコンで示されます。 • [送信（Outbound）]：組織内から組織外のどこかに送信されたメッセージ。[方向（Direction）] 列では、受信メッセージが ⓘ アイコンで示されます。 • [内部（Internal）]：組織内で開始および終了したメッセージ。[方向（Direction）] 列では、

検索フィールド	説明
	アイコンで示されます。
攻撃タイプ（Attack Type）	フィールドをクリックして、1 つ以上の攻撃タイプを選択します。選択した攻撃タイプのいずれかに一致するメッセージが検索で見つかります。
ドメインのレピュテーションの範囲（Domain Reputation Range）	これは、検索で見つかるメッセージのドメインレピュテーションの上限と下限（選択した値を含む）を定義します。範囲を変更するには、下限と上限のスライダをドラッグします。
送信ドメイン（Sending Domain）	1 つまたは複数の送信ドメインをカンマで区切って入力します。そのドメインのいずれかに一致するメッセージが検索で見つかります。 ⚠ 100 文字に制限されています。
ドメインタグ（Domain Tags）	フィールドをクリックして、1 つ以上のドメインタグを選択します。選択したドメインタグのいずれかに一致するメッセージが検索で見つかります。
ホスト名（Hostname）	単一の PTR ホスト名を IP アドレスに入力します。そのホスト名を含むメッセージが検索で見つかります。 ⚠ 100 文字に制限されています。
SBRS範囲（SBRS Range）	これは、検索で見つかるメッセージの SENDERBASE レピュテーションスコア（SBRS）の上限と下限（選択した値を含む）を定義します。範囲を変更するには、下限と上限のスライダをドラッグします。
IP アドレス（IP Address）	単一の IP アドレスまたは CDR を入力します。その IP アドレスを含むメッセージが検索で見つかります。 ⚠ 100 文字に制限されています。

メッセージを検索する

[メッセージの検索（Search Messages）] ページを使用して、着信メールを検索およびフィルタ処理することができます。メニューを介して、または [ドメインの詳細（Domains Detail）] ページか [IP アドレスの詳細（IP Address Details）] ページでメッセージの番号をクリックすることで、[分析（Analyze）] > [メッセージの検索（Search Messages）] ページに直接移動できます。

1. [分析（Analyze）] > [メッセージの検索（Search Messages）] に移動します。
2. 検索条件を入力します。それぞれの検索フィールドの詳細については、「「メッセージ検索」 ページ 127」を参照してください。
3. [検索（Search）] をクリックします。

メッセージの検索結果をダウンロードする

[検索結果（Search Results）] ページにいるときはいつでも、現在の検索フィルタに一致するメッセージのリストに関する情報をダウンロードできます。

ダウンロードしたファイルには、最大 10,000 件のメッセージに関する情報が含まれます。検索結果に 10,000 件を超えるメッセージが含まれている場合、ダウンロードされたファイルには、表示順序に従って最初の 10,000 件が含まれます。表示順序は検索結果テーブルの任意の列の上部をクリックして変更できます。

1. [分析(Analyze)] > [メッセージの検索(Search Messages)] に移動します。(メッセージの [検索結果(Search Results)] ページにアクセスする方法は他にも多くあります。たとえば、ダッシュボードで脅威の種類をクリックし、[メッセージの表示(Show messages)] をクリックすると、フィルタとして定義済みの脅威の種類が表示された [メッセージの検索(Search Message)] ページに移動します)
2. リストに表示するメッセージのフィルタを定義します。
3. [検索(Search)] をクリックします。
4. [結果のダウンロード(Download Results)] をクリックします。
5. [CSVのダウンロード(Download CSV)] をクリックします。

message export.csv という名前のファイルが、ブラウザで設定したダウンロードファイル用のデフォルトの場所に自動的にダウンロードされます。このファイルには、次のような各メッセージからの情報や各メッセージに関する情報が含まれます(利用可能な場合)。

- 日付
- 差出人
- 返信先、転送元
- 宛先
- 件名
- Message-ID
- メッセージの信頼スコア *
- 送信ドメイン
- ドメインのレピュテーション *
- 送信側の IP アドレス
- PTR 名
- SBRS(SENDERBASE レピュテーションスコア)

*高度なフィッシング防御による算出。

ドメインと IP アドレス

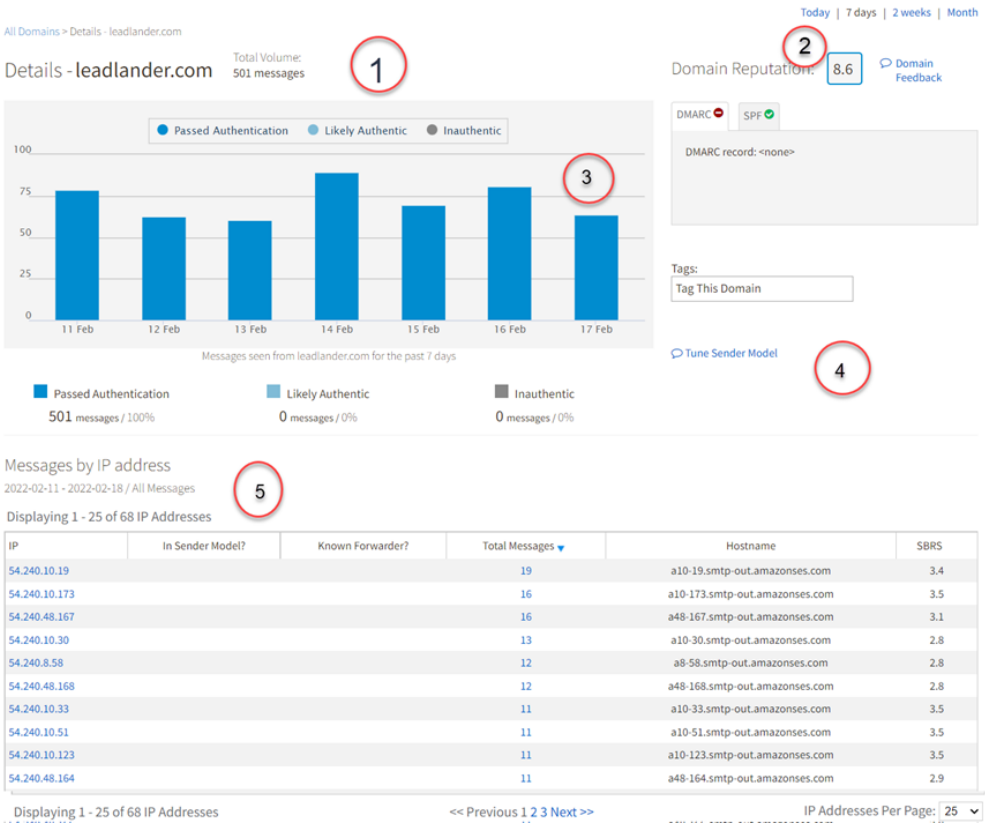
[分析(Analyze)] メニューから送信側のドメインと IP アドレスの一覧を表示できます([分析(Analyze)] > [ドメイン(Domains)]、[分析(Analyze)] > [IPアドレス(IP Addresses)])。これらのページは同じように機能し、着信トラフィックを調査する際に切り替えることができます。一覧内の IP アドレスまたはドメインをクリックすると、その項目の [詳細(Details)] ページを表示できます。IP アドレスの場合、[詳細(Details)] ページには、その IP アドレスから組織へ送信しているドメインのリスト、それぞれのドメインによって送信されたメッセージへのリンクなど、その IP に関する情報が表示されます。ドメインの場合、[詳細(Details)] ページには、そのドメインから組織へ送信している IP アドレスのリストと送信されたメッセージなど、そのドメインに関する情報が表示されます。

IP アドレスとドメイン、およびそれぞれからの関連付けられたメッセージの表示を切り替えて調べるやり方が、詳細にドリル ダウンし、着信トラフィックを分析するための強力な方法となります。

ドメインの詳細を表示する

ドメインと IP アドレスの関係は、高度なフィッシング防御の送信者モデリング機能のキーコンポーネントであり、[ドメインの詳細(Domain Details)] ページには送信者モデルに関する多くの情報が表示されています。

1. [分析(Analyze)] > [ドメイン(Domains)] に移動します。
2. ドメイン名をクリックします。



[ドメインの詳細(Domain Details)] ページ

[ドメインの詳細(Domain Details)] ページには次の情報が表示されます。

1	ドメイン名、ドメインのボリューム、およびそのドメインからインバウンド電子メール ストリームがボリューム全体に占めるパーセンテージが、ページの上部にリストされます。
2	ドメイン レピュテーション(高度なフィッシング防御による得点付け)が右上にリストされます。[ドメインフィードバック(Domain Feedback)] リンクを使用すると、ドメインのスコアが間違っていると感じた場合に、フィードバックを送信できます。ドメイン レピュテーションは、0.0 ～ 10.0 の範囲で得点付けされ、0.0 が最低のレピュテーションを表し、10.0 が最も信頼できることを表しています。

3	送信側ドメインから到達したメッセージのボリュームのグラフが、ページ中央にあります。メッセージは、[認証に合格済み（Passed Authentication）]、[本物でない（Inauthentic）]、または [高い確率で本物（Likely Authentic）] として分類されます。 • 本物のメッセージとは、そのドメイン自身によって公開されているとおり、認証標準（SPF、DMARC、または DKIM）に準拠しているメッセージです。 • 本物でないメッセージとは、認証に失敗し、そのドメインの送信者モデルに含まれないと見なされたメッセージです。 • 高い確率で本物のメッセージとは、認証に合格していないが、送信側ドメインから「高い確率で本物」であると見なされたメッセージです。 チャートの上部にあるキーをクリックして、[認証に合格済み（Passed Authentication）]、[本物でない（Inauthentic）]、および [高い確率で本物（Likely Authentic）] の棒グラフの表示を切り替えることができます。同様に、チャートの時間範囲は、ページの右上にある時間範囲セレクタによって制御されます（7 日間/2 週間/30 日間）。 棒グラフでいずれかの棒をクリックすると、特定の日を選択できます。選択をクリアするには、[IPアドレス別メッセージ（Messages by IP address）] テーブルのヘッダーで [クリア（Clear）] を選択します。
4	該当する場合、ドメインの DMARC レコードと SPF レコードがここに提示されます。そのエリアの下には、ドメイン レピュテーションに影響するプラスの要因とマイナスの要因が表示されます。たとえば、この画面は、ドメインに「一貫した送信履歴」があることを示しています。
5	[IPアドレス別メッセージ（Messages by IP Address）] は、一定期間にそのドメインに送信した各 IP アドレスを分類しています。 • IP アドレスをクリックすると、効果的に表示が回転します。該当するドメインのすべての IP アドレスを表示するではなく、単一の IP がメッセージを送信したすべてのドメインを表示できます。 • [詳細（Detail）] ページの [メッセージの合計（Total Messages）] で数字をクリックすると、[メッセージの検索（Search Messages）] ページに送信者（IP またはドメイン）のメッセージの一覧が表示されます。

ドメインタグ

ドメインにはタグを割り当てることができます。タグは、スコアリングに影響を与え、ドメインの使用を分析し、ポリシーを作成するために使用されます。高度なフィッシング防御で組織によって追跡されている任意のドメインに、定義済みのタグのリストから 1 つ以上のタグを割り当てることができます。

[内部（internal）] および [パートナー（partner）] の 2 つのタグは、メッセージスコアリングのプロセスで使用されます。一般的には以下のように割り当てます。

- [内部（internal）] タグ：所有し、制御でき、ドメインレピュテーションを本質的に信頼できるドメインへ割り当てます。
- [パートナー（partner）] タグ：電子メールを交換し、信頼関係を確立し、ドメインレピュテーションを信頼できる外部組織のドメインへ割り当てます。

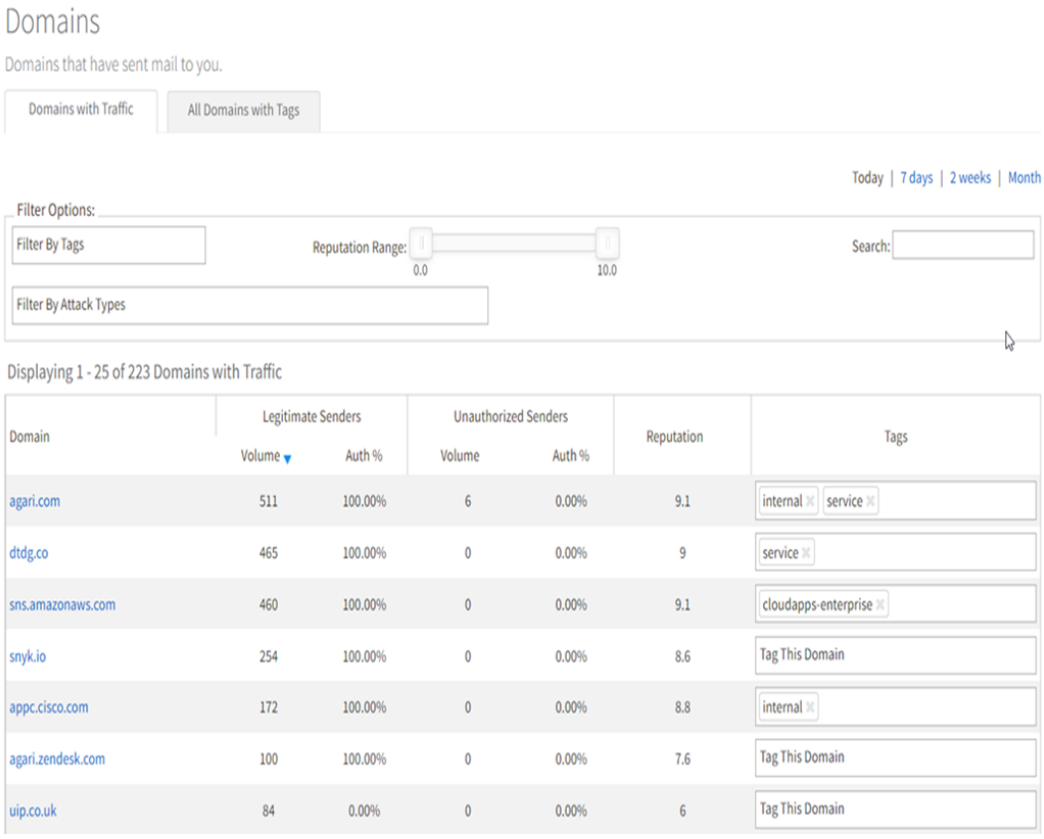
ドメインに [内部（internal）] タグまたは [パートナー（partner）] タグを追加すると、適切に認証されたメッセージに対するそのドメインのレピュテーションが向上します。

[内部（internal）] タグと [パートナー（partner）] タグの両方を同じドメインに追加しないでください。

ドメインに追加できるその他のタグは、[分析（Analyze）] > [概要（Overview）] ページでの視覚化、検索結果、およびポリシーの作成に役立ちます。

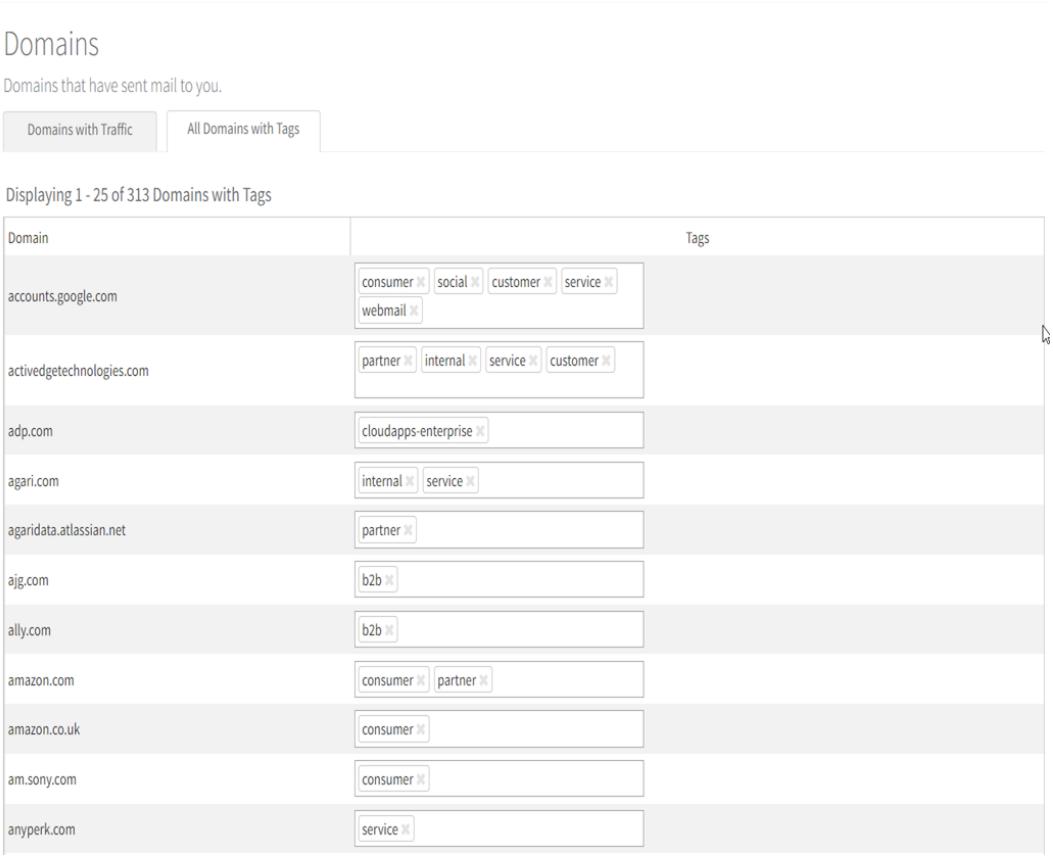
タグ付きドメインを表示する

1. [分析（Analyze）] > [ドメイン（Domains）] に移動します。
2. [トラフィックを含むドメイン（Domains with Traffic）] をクリックして、過去 60 日間の電子メールメッセージを含む、組織におけるすべてのタグ付きドメインのリストを表示します。



過去 60 日間の電子メールメッセージを含むタグ付きドメイン。

3. [すべてのタグ付きドメイン（All Domains with Tags）] をクリックして、組織内のすべてのタグ付きドメインのリストを表示します。



組織で使用可能なすべてのタグ付きドメイン。

ドメインにタグを追加する

1. [分析(Analyze)] > [ドメイン(Domains)] に移動します。
2. 任意のドメインの [タグ(Tags)] フィールドをクリックします。
3. 未使用のタグを選択します。

タグは自動的に追加されます。

[ドメインの詳細(Domain Details)] ページ([分析(Analyze)] > [ドメイン(Domains)] を選択し、ドメイン名をクリック)でドメインにタグを追加することもできます。[タグ(Tags)] フィールドは右側にあります。

ドメインからタグを削除する

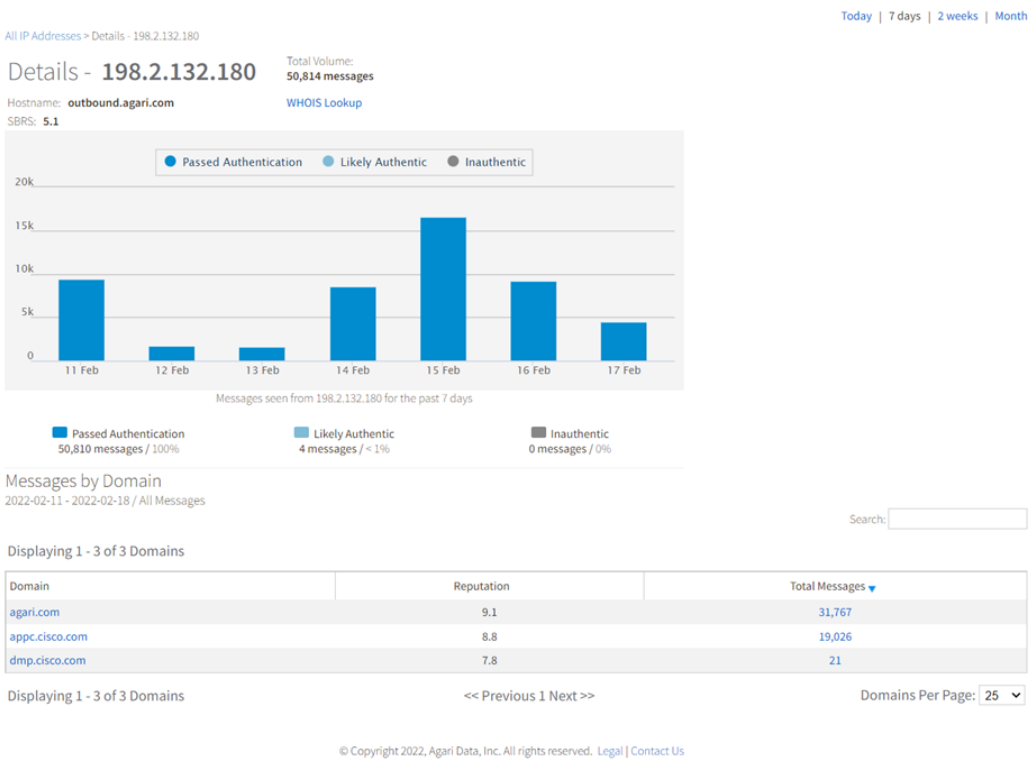
1. [分析(Analyze)] > [ドメイン(Domains)] に移動します。
2. ドメインの [タグ(Tags)] フィールドで、ドメインから削除するタグの [x] をクリックします。

タグはすぐに削除されます。

IP アドレスの詳細を表示する

特定の IP アドレスの詳細を表示すると、IP アドレスが次に当てはまるかどうか確認するために役立ちます。

- 送信側ドメインによって完全に所有されている（ごくわずかなドメインにのみ送信）
- 共有 IP アドレス（多数のドメインに送信）
- メール フォワーダ（かなり多数のドメインに送信）



[IPの詳細（IP Details）] ページ

[ドメインの詳細（Domain Details）] ページでは、IP のホスト名、特定の期間に組織が確認したその IP からのメッセージの総ボリューム、および高度なフィッシング防御からの SBRS（SENDERBASE レピュテーションスコア）を表示できます。

また、ページには、特定の IP アドレスの WHOIS 情報へのリンクも含まれています。

[ドメインの詳細（Domain Details）] ページの時系列チャートと同様に、時間範囲を変更し、本物、本物でない、高い確率で本物のメッセージ数の表示を切り替えることができます。

この例では、「smtp106.biz.mail.ne1.yahoo.com」というホスト名を持つ送信側の IP アドレス 98.138.207.13 が、42 件のメッセージを組織に送信しました。ドメイン「dataservicesww.com」のメッセージが 42 件で、「echelonconsulting.net」のメッセージが 1 件です。

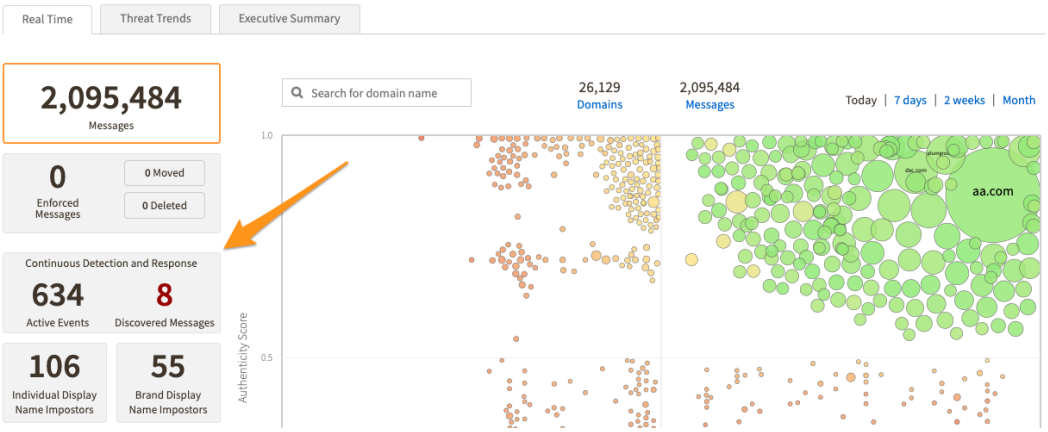
[詳細（Detail）] ページの [メッセージの合計（Total Messages）] で数字をクリックすると、[メッセージの検索（Search Messages）] ページに送信者（IP またはドメイン）のメッセージの一覧が表示されます。

継続的な検出および応答

高度なフィッシング防御 の継続的な検出および応答（CDR）機能により、組織は、隠れた悪意のあるメッセージから保護し、新しい脅威インテリジェンスが発見されたときにデータ侵害を防止または軽減できます。

CDR は、組織全体の受信トレイに潜む悪意のある電子メールメッセージを検出し、悪意のあるメッセージを削除または隔離して自動的に削除し、悪意のあるメッセージのインシデントが組織内でどの程度広がっているかを判断します。

高度なフィッシング防御 のダッシュボードの左側にある CDR インジケータは、CDR が検出した脅威の数を示します。

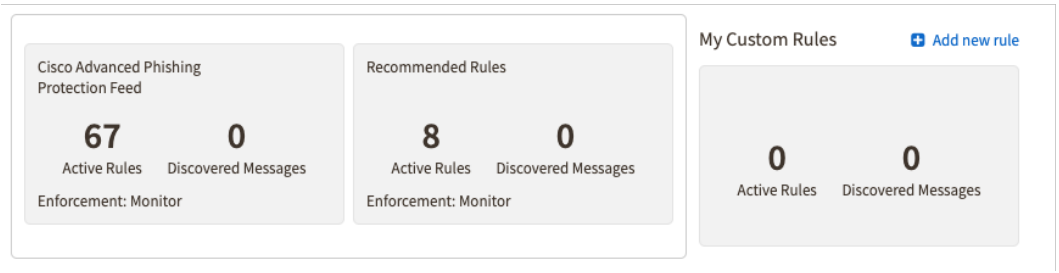


高度なフィッシング防御 のダッシュボードおよびレポートページの CDR インジケータ。

[アクティブイベント(Active Events)] の数字は、CDR ネットワークを介して現在認識されている CDR イベントの数です。[検出されたメッセージ(Discovered Messages)] の数字は、CDR を介して検出された組織内のメッセージを表します。

継続的な検出および応答の詳細

脅威インテリジェンスは、複数のフィードから CDR に入ります。



CDR は、高度なフィッシング防御 および Phishing Response のエコシステム内で機能し、他の組織によって識別されたフィッシングキャンペーンを識別して削除します。これは以下によって実行されます。

- IOC を検索条件として使用して、組織内の類似メッセージを検索する
- それらのメッセージに対して自動的にアクションを実行する

脅威が検出されると、明示的に作成されたポリシーがこれらのアクションを実行する方法と同様に、CDR はそれらの脅威を含むメッセージを組織全体の受信トレイから隔離または削除できます。

メッセージが異なる適用アクションを持つ複数のポリシーに一致する場合、[受信トレイに移動(Move to Inbox)] アクションが最も優先され、次に [削除(Delete)] アクションが続き、続いて [適用の設定(Enforcement Settings)] で最も高い位置にあるラベルが続きます。詳細については、「「ポリシー」 ページ 153」を参照してください。

継続的な検出および応答の要件

継続的な検出および応答には、次のものが必要です。メッセージをジャーナルするように設定された高度なフィッシング防御センサー（デュアル配信とも呼ばれます。詳細については、「「センサーの導入」 ページ 22」を参照してください）。

継続的な検出および応答イベント

継続的な検出および応答（CDR）イベントは、CDR エコシステム内の脅威の検出のことです。脅威の特定は、次のような多くのベクトルに起因する可能性があります。

- Cisco Identity Graph（CDR を強化するデータサイエンス）
- 高度なフィッシング防御 自体が特定した脅威

CDR イベントは、お使いの環境にすでに存在するメッセージと新しい受信メッセージを調べるために使用される一連の条件です。

メッセージ数がゼロの CDR イベントが表示されることがあります。これは、メッセージ数が、CDR イベントに一致する組織内で見つかったメッセージの数を表すためです。既知の脅威によって組織が攻撃されないのが良いのはもちろんですが、CDR が提供する既知の脅威に関する情報は次のことに役立ちます。

- 現在の脅威の状況に注意する
- セキュリティのインフラストラクチャを最新の状態に保ち、現在および将来の脅威に備えるのに役立つ情報を提供する

CDR イベントは継続的にチェックされ、すべての新しい受信メッセージは、期限切れになっていない既存の CDR イベントに対してチェックされます。CDR イベントは、Cisco に保護された組織で一致した最後のメッセージから 60 日後に自動的に期限切れになります。期限切れの CDR イベントは、高度なフィッシング防御 から削除され、[継続的な検出および応答（Continuous Detection and Response）] ページ（[管理（Manage）] > [継続的な検出（Continuous Detection）]）に表示されなくなります。

継続的な検出および応答イベントを表示する

高度なフィッシング防御のホーム画面には、期限が切れていないすべての CDR イベントが、最新のアクティビティがあるものを先頭にしてリストされます。

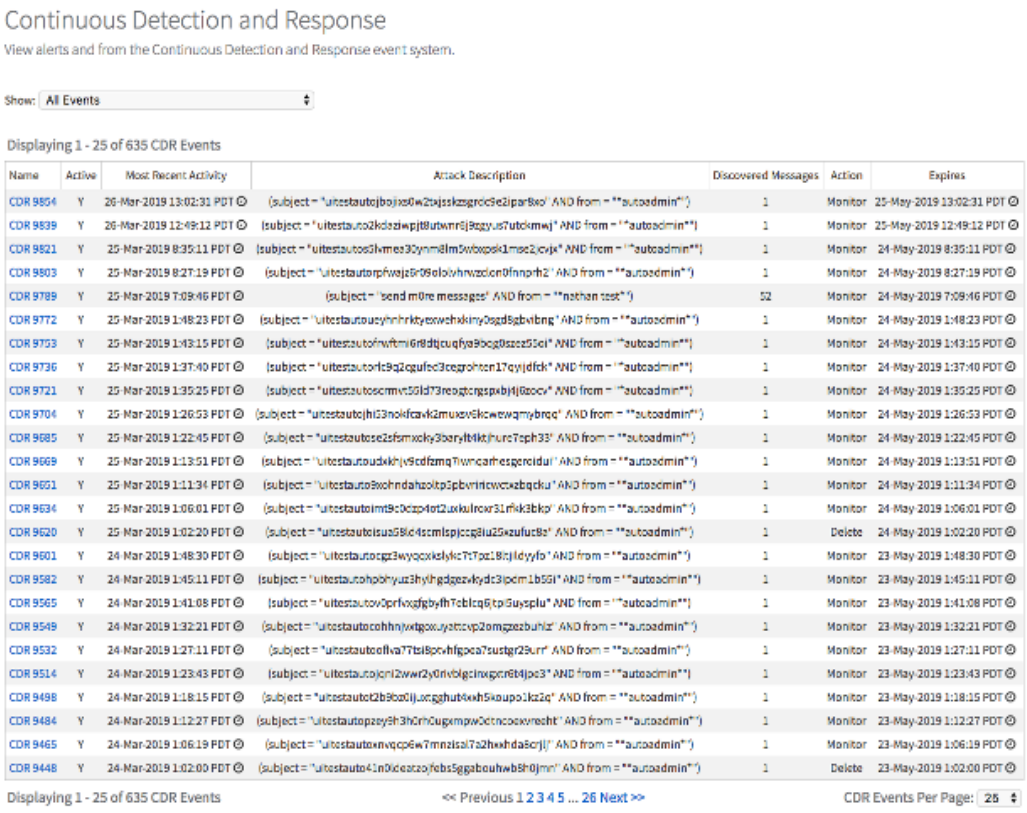
で継続的な検出および応答イベントを表示するには以下の手順を行います。高度なフィッシング防御

- [管理（Manage）] > [継続的な検出（Continuous Detection）] に移動します。

高度なフィッシング防御 のダッシュボードで、[継続的な検出および応答（Continuous Detection and Response）] タイルをクリックすることもできます。

ページの上部にある [表示（Show）] ドロップダウンリストを使用して、以下を表示できます。

- すべてのイベント（デフォルト表示）
- すべてのアクティブイベント
- メッセージが検出されたすべてのアクティブイベント（[検出されたメッセージ（Discovered Messages）] 列にゼロ以外の数が表示されているイベント）
- すべての非アクティブイベント



継続的な検出および応答イベントのリストの例。

リスト内のイベントに対して、[最新のアクティビティ(Most Recent Activity)] または [有効期限(Expires)] 列の時刻をクリックして、現地時間と UTC を切り替えます。

継続的な検出および応答イベントの詳細を表示する

高度なフィッシング防御 と Cisco アプリの両方で、継続的な検出および応答イベントの詳細を表示できます。Cisco アプリのイベントの詳細には、基本的なイベントの詳細と静的メッセージの詳細が表示されます。

1. [管理(Manage)] > [継続的な検出(Continuous Detection)] に移動します。
2. イベントの [名前(Name)] をクリックします。

CDR イベントの [詳細(Details)] ページには、次の情報が含まれています。

- イベントが現在アクティブか非アクティブか。ここでこの状態を切り替えることができます。
- イベントの説明(高度なフィッシング防御 でのみ)。
- イベントで組織内のメッセージを検索するために使用される特定の検索条件。

  他の CDR 組織での悪意のある調査が終了したときに、CDR イベントが組織に表示されます。組織内に CDR イベントの一部として識別されたメッセージがある場合とない場合がありますが、組織内でメッセージが見つかった場合はこのリンクが CDR イベントに表示されます。詳細については、「「継続的な検出および応答イベント」(前のページ)」を参照してください。

- **メッセージステータス**バーとして表示される、イベントでのメッセージの適用のステータス。

  メッセージステータスバーは、選択した CDR に適用アクションが適用されている場合にのみ表示されます。

- イベント内のメッセージのリスト。一致するメッセージとも呼ばれます。このリストには、各メッセージの適用の有無、送信者、宛先、件名、そして 高度なフィッシング防御 においてメッセージが読まれたかどうかとその信頼スコアが含まれます。高度なフィッシング防御 のこのリストでは、次のことを実行できます。
    - [表示(Show)]ドロップダウンリストから [すべてのメッセージ(All Messages)]、[適用済み(Enforced)]、または [失敗した適用(Failed Enforcement)] を選択して、メッセージリストをフィルタリングします。
    - 列ヘッダーをクリックして、任意の列のデータで並べ替えます(デフォルトは [信頼スコア(Trust Score)] の降順です)。
    - メッセージ行の任意の場所をクリックして、メッセージの詳細を表示します。[メッセージの詳細(Message Details)] ダイアログボックスの詳細については、「「メッセージの詳細を表示する」 ページ 124」を参照してください。

まとめると、条件とアクションはポリシーで定義するのと似たもので、同じ結果になります。

継続的な検出および応答イベントの状態を変更する

継続的な検出および応答(CDR)イベントは、次のいずれかの状態になります。

- [アクティブ(Active)]:これは、すべての新しい受信メッセージがこの CDR イベントの条件と比較され、一致するすべてのメッセージに CDR イベントアクションが適用されることを意味します(定義されたアクションを変更するには、「「継続的な検出および応答イベントアクションを変更する」 下」を参照してください)。これは、新しいイベントが作成されたときのデフォルトです。
- [非アクティブ(Inactive)]:これは、CDR がこのイベントに一致する可能性のあるメッセージをチェックしないことを意味します。CDR イベントは、脅威ではないと判断されたときに手動で非アクティブに設定できます。
- [保留中(Pending)]:これは、イベントは作成されましたが、公開されていないことを意味します。イベントが 4 時間以上保留中の状態のままである場合、イベントは失敗した可能性があり、アクティブになりません。最善の方法は、ルールを書き直し、複雑さを軽減することです。たとえば、ルールをいくつかのより単純なルールに分割します。保留中のルールは失敗として表示されませんが、削除されるまで保留中としてラベルが付けられたままになります。

CDR イベントの詳細ページで状態を変更します。

高度なフィッシング防御で継続的な検出および応答イベントの状態を変更します。

1. [管理(Manage)] > [継続的な検出(Continuous Detection)] に移動します。
2. イベントの [名前(Name)] をクリックします。
3. [CDRの詳細(CDR Details)] ページの上部で、[非アクティブ/アクティブ(Inactive/Active)] トグルをクリックします。

継続的な検出および応答イベントアクションを変更する

継続的な検出および応答(CDR)イベントは、現在のメッセージと将来のメッセージの両方を含む、イベントに一致するすべてのメッセージに適用される適用アクションを定義できます。内部的には、イベントアクションは CDR ポリシーの自動作成によって処理され、将来のメッセージは、CDR イベントに対する新しい受信メッセージの継続的なチェックによって処理されます。

新しく作成された CDR イベントのデフォルトアクションは、組織の設定によって決まります。詳細については、「「組織設定」 ページ 197」を参照してください。

CDR イベントのアクションは次のとおりです。

- [削除(Delete)]:メッセージを完全に削除します(Microsoft Office 365 を使用している組織の場合、削除済みアイテムの回復機能を使用してメッセージを回復できます。その他の組織では削除の回復はできません)。
- [隔離(Quarantine)]:電子メールクライアントの隔離フォルダにメッセージを移動します。
- [監視(Monitor)]:メッセージに対して明示的なアクションを実行せず、CDR イベントに一致するメッセージの通知を引き続き受信します。

高度なフィッシング防御で継続的な検出および応答イベントアクションを変更するには以下の手順を行います。

1. [管理(Manage)]>[継続的な検出(Continuous Detection)]に移動します。
2. イベントの[名前(Name)]をクリックします。
3. [進行中のアクション(Ongoing Action)]セクションで、[アクションの変更(Modify Action)]をクリックします。
4. 処理を選択します。
5. 選択したアクションを、すでに検出されたメッセージに適用するかを決定します。適用しない場合、アクションは将来の一致するメッセージにのみ適用されます。
6. [保存(Save)]をクリックします。

継続的な検出および応答ルール

継続的な検出および応答(CDR)ルール(カスタムルールとも呼ばれます)を使用すると、脅威を捕捉してアクションを実行するために、組織に送られてくるメッセージに関する独自のインテリジェンスと独自の知識を適用できます。CDR ルールは、ポリシー(「「ポリシー」 ページ 153」を参照)よりも詳細できめ細かい検索メカニズムと、特定のメッセージ基準を定義するために使用するドメイン固有の言語を使用します。

CDR ルールは、検索結果を使用してポリシーを作成できる高度なフィッシング防御の検索ページ(「「メッセージ検索」 ページ 127」を参照)で使用できるよりも多くの基準に基づいてメッセージを検索できます。使用できるメッセージ基準は、「「ドメイン固有の言語リファレンス」 次のページ)」のフィールドリストのすべての項目です。

CDR ルールは組織に対してローカルです。CDR ルールを作成すると、そのルールに基づく CDR イベントが自動的に作成され、ソースとしてカスタムルールが表示されます。CDR イベントは、高度なフィッシング防御によって保存された 60 日間のメッセージデータのセット全体に適用されます。

ポリシーと同様に、1 つのメッセージが複数の CDR ルールに一致する場合があり、メッセージに対する CDR ルールの適用アクションは、定義された優先順位に従って発生します。詳細については、「「ポリシー」 ページ 153」を参照してください。

ドメイン固有言語(DSL)を使用してカスタム検索クエリを作成することにより、独自のきめ細やかなローカルルールを作成できます。これらの検索クエリは、DSL で定義した特性を持つメッセージを見つけて一致させます。Cisco 高度なフィッシング防御 で利用可能な DSL の詳細と、DSL を使用したクエリの例については、「「ドメイン固有の言語リファレンス」 次のページ)」を参照してください。

Cisco 高度なフィッシング防御 の[ローカルCDRルール(Local CDR Rule)]ページの[ルールの説明(Rule Description)]フィールドに検索クエリを入力します。

継続的な検出および応答ルールを作成する

CDR ルールを作成するには、組織の管理者ロールが必要です。

1. [管理(Manage)] > [継続的な検出(Continuous Detection)] に移動します。
2. [新しいルールの追加(Add new rule)] をクリックします。
3. [カスタムルール名(Custom Rule Name)] とオプションの [説明(Description)] を入力します。
4. CDR ルールが期限切れになるまでの期間を決定します。
    - [非アクティブの日数(days of inactivity)] の数を入力します。入力した日数内にルールに一致するメッセージがない場合、ルールはここに入力した日数の終了時に期限切れになります。
    - ルールを永続的にするには、[無期限(Never expire)] を選択します。
5. 組織で内部関係者偽装を有効にしている場合(詳細については、「「メッセージ設定」 ページ 198」を参照してください)、ルールを適用するメッセージの方向性を選択します。
6. ルールに一致するメッセージに適用するアクションを選択します。
7. ドメイン固有言語(DSL)を使用した検索式であるルールの説明を入力します。詳細については、「「ドメイン固有の言語リファレンス」 下」を参照してください。
8. [メッセージのプレビュー(Preview Messages)] をクリックします。
9. この時点で、高度なフィッシング防御は、CDR ルールに一致する現在データストアにある過去 60 日間のすべてのメッセージのリストをコンパイルするため、結果を確認して、設計したルールが意図に一致するかどうかを確認できます。
10. [カスタムルールの追加(Add Custom Rule)] をクリックします。

数分後、[継続的な検出および応答(Continuous Detection and Response)] ページで新しく作成されたイベントが表示されます([マイカスタムルール(My Custom Rules)] タイルをクリックすると、カスタムルールから作成された CDR イベントだけでリストをフィルタリングできます)。CDR イベントのソースは [カスタムルール(Custom Rules)] になり、条件は CDR ルールに入力した検索式になります。

ドメイン固有の言語リファレンス

継続的な検出および応答(CDR)では、利用可能な Cisco のドメイン固有言語(DSL)を使用して検索クエリを作成することにより、独自のきめ細やかなカスタムルールを作成できます。これらの検索クエリは、DSL で定義した特性を持つメッセージを見つけて一致させるためのものです。この セクション では、Cisco 高度なフィッシング防御 で利用可能な DSL のコンポーネントを定義し、DSL を使用したクエリの例をいくつか提供します。

高度なフィッシング防御の [ローカルCDRルール(Local CDR Rule)] ページにある [ルールの説明(Rule Description)] フィールドに検索クエリを入力します。詳細については、「「継続的な検出および応答ルールを作成する」 (前のページ)」を参照してください。

構文

検索クエリには、*field operator operand* の 1 つ以上の検索式を含めることができ、追加の検索式はそれぞれ AND/OR 結合で区切られます。

AND で結合されている場合、CDR は式内での同じフィールドと演算子の組み合わせの複数の使用をサポートせず、OR で結合されている場合にのみサポートします。

たとえば、次の search_dsl は無効です。

from != "foo" and from != "bar"

この search_dsl を使用して CDR ルールをプレビューしようとすると、次のエラーメッセージが生成されます。

フィールド「from」は、同じステートメント内で複数回使用することはできません。

これは、フィールドと演算子のすべての組み合わせに当てはまります。演算子 = と EQ は、!= と NOT EQ と同様に、同じであると見なされます。

リスト演算子をサポートするフィールドの場合、式内で AND を使用すると、別のエラーメッセージが生成されます。たとえば、次の search_dsl 式を見てください。

domain_tags != 'internal' および domain_tags != 'marketing'

これにより、次のエラーメッセージが表示されます。

フィールド「domain_tags」は、リスト演算子をサポートしています。複数の値を指定する場合は、IN または NOT IN を使用します。

この search_dsl を有効にするには、次のように書き換えます。

domain_tags NOT IN ['internal', 'marketing']

前述のように、フィールドと演算子の組み合わせを複数回使用することは、それぞれの使用が OR で区切られている場合に有効です。たとえば、これらは有効です。

domain_tags = 'internal' OR domain_tags = 'marketing'

(subject = "foobar" AND domain_tags != 'internal') OR (subject = "barbaz" AND domain_tags != 'marketing')

クエリ内の複数の検索式を評価する場合、デフォルトの優先順位は左から右です。検索式を括弧でグループ化して、評価の優先順位を制御できます。ワイルドカードは使用できません。

明確さと一貫性を保つために、すべての文字列のオペランドを二重引用符で囲む必要があります。技術的には、演算子文字 = や > など、スペースや予約済み文字を含まないオペランドには引用符は必要ありませんが、エラーの可能性をなくすために、常に引用符を使用して文字列のオペランドを囲んでください。数値または日付のオペランドを引用符で囲まないでください。一重引用符ではなく、二重引用符のみを使用できます。

フィールド

フィールドは、検索できるメッセージの特性のことです。次のフィールドを検索式の *field* コンポーネントとして使用できます。タイプは、どのオペランドが使用できるかを示します。たとえば、タイプが float のフィールドは、数値を評価できる任意のオペランドで使用できます。

以下で [完全一致のみ(Exact matches only)] として説明されているフィールドは、[any] 演算子をサポートしていませんが、[=] 演算子はサポートしています。

以下で [完全一致のみ(Exact matches only)] として説明されているフィールドは、[any] 演算子をサポートしていませんが、[=] 演算子はサポートしています。

フィールド	タイプ	説明
attachment_extension	string	文字列としての添付ファイル拡張子の完全一致。たとえば、doc は docx と一致しません。完全一致のみ。 「.」は含めないでください。「.」(ピリオドまたはドット)は通常、ファイル名の拡張子の前に付けられます。

<table>
<tr><th>フィールド</th><th>タイプ</th><th>説明</th></tr>
<tr><td>attachment_filename</td><td>string</td><td>添付ファイル名の完全一致。完全一致のみ。</td></tr>
<tr><td>attachment_sha256</td><td>string</td><td>添付ファイルの SHA256 ハッシュの完全一致。完全一致のみ。</td></tr>
<tr><td>attack_types</td><td>string</td><td>文字列またはリストとしての攻撃タイプの分類。次の表は、attack_types フィールドと関連する攻撃タイプを使用して検索式で使うことのできる値を示しています。

<table><tr><th>検索式フィールド</th><th>攻撃タイプ</th></tr><tr><td>low_trust</td><td>スパムまたはグレイメール</td></tr><tr><td>spoof</td><td>ドメインスプーフィング</td></tr><tr><td>dni</td><td>ブランド表示名偽装</td></tr><tr><td>address_group</td><td>個別の表示名偽装</td></tr><tr><td>compromised_webmail</td><td>感染したアカウント</td></tr><tr><td>likely_malicious_uri</td><td>悪意のある可能性のある URI</td></tr><tr><td>malicious_attachments</td><td>悪意のある可能性のある添付ファイル</td></tr><tr><td>covid_19</td><td>COVID-19</td></tr></table></td></tr>
<tr><td>authenticity</td><td>float</td><td>浮動小数点値として表される真正性スコア（0.0 ～ 10.0）。</td></tr>
<tr><td>dkim_result</td><td>string</td><td>可能性のあるメッセージの DKIM 結果のリスト。次の表は、dkim_result フィールドを使用して検索式で使うことのできる値と、それぞれに関連する意味を示しています（値はすべて単一の文字であることに注意してください）。

<table><tr><th>検索式の値</th><th>DKIM 結果</th></tr><tr><td>+</td><td>DKIM 合格</td></tr><tr><td>n</td><td>未署名</td></tr></table></td></tr>
<tr><td>dmarc_result</td><td>string</td><td>可能性のあるメッセージの DMARC 結果のリスト。次の表は、dmarc_result フィールドを使用して検索式で使うことのできる値と、それぞれに関連する</td></tr>
</table>

<table>
<tr><th>フィールド</th><th>タイプ</th><th>説明</th></tr>
<tr><td></td><td></td><td>意味を示しています（値はすべて単一の文字であることに注意してください）。

<table><tr><th>検索式の値</th><th>DMARC 結果</th></tr><tr><td>+</td><td>DMARC 合格</td></tr><tr><td>–</td><td>DMARC 失敗</td></tr><tr><td>n</td><td>使用不可</td></tr></table></td></tr>
<tr><td>domain_reputation</td><td>float</td><td>浮動小数点値として表される送信者ドメインのレピュテーション（0.0 ～ 10.0）。</td></tr>
<tr><td>domain_tags</td><td>string</td><td>文字列またはリストとしてのドメインタグの完全一致。</td></tr>
<tr><td>from</td><td>string</td><td>メッセージヘッダー内の完全な差出人。</td></tr>
<tr><td>from_domain</td><td>string</td><td>完全な差出人のメッセージヘッダー内のドメイン部分のみ。</td></tr>
<tr><td>from_to_match</td><td>boolean</td><td>完全なヘッダーの送信元の電子メールアドレス部分が宛先の電子メールアドレスと一致するかどうか。</td></tr>
<tr><td>has_attachment</td><td>boolean</td><td>メッセージに添付ファイルがあるかどうか。</td></tr>
<tr><td>has_malicious_attachment</td><td>boolean</td><td>メッセージに悪意があると判断された添付ファイルがあるかどうか。</td></tr>
<tr><td>ip</td><td>string</td><td>IP アドレスまたは CIDR（CIDR の詳細については、https://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing を参照してください）。</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th>フィールド</th><th>タイプ</th><th>説明</th></tr>
<tr><td>mail_from_domain</td><td>string</td><td>ドメインからのメール。エンベロープ送信者のドメイン。ドメインからのメール全体にのみ一致します（部分一致はありません）。</td></tr>
<tr><td>message_id</td><td>string</td><td>一意のメッセージ識別子。メッセージ識別子全体にのみ一致します（部分一致はありません）。</td></tr>
<tr><td>message_trust_score</td><td>float</td><td>浮動小数点値として表されるメッセージの信頼スコア（0.0 ～ 10.0）。</td></tr>
<tr><td>reply_to</td><td>string</td><td>メッセージヘッダー内の完全な返信先。</td></tr>
<tr><td>reply_to_no_match</td><td>boolean</td><td>返信先アドレスが送信元アドレスと一致しないかどうか（一致しない場合はオペランドで true を使用して検出し、一致する場合はオペランドで false を使用して検出します）。完全一致のみ。</td></tr>
<tr><td>sbrs</td><td>float</td><td>浮動小数点値として表される SENDERBASE レピュテーションスコア（-10.0 ～ 10.0）。</td></tr>
<tr><td>spf_result</td><td>string</td><td>可能性のあるメッセージの SPF 結果のリスト。次の表は、spf_result フィールドを使用して検索式で使うことのできる値と、それぞれに関連する意味を示しています（値はすべて単一の文字であることに注意してください）。

<table><tr><th>検索式の値</th><th>SPF 結果</th></tr><tr><td>+</td><td>SPF 合格</td></tr><tr><td>–</td><td>SPF 失敗</td></tr><tr><td>~</td><td>SPF ソフト障害</td></tr><tr><td>n</td><td>SPF レコードなし</td></tr><tr><td>p</td><td>永続的なエラー</td></tr></table></td></tr>
<tr><td>start_date</td><td>date</td><td>一致する最も早いメッセージの日時を定義する ISO 8601 形式の日付（一致する受信メッセージには適用されません）。</td></tr>
</table>

フィールド	タイプ	説明
		これは、ルール内の唯一の式にすることはできません。また、次の演算子のみを含めることができます。 = > >= 例: 次の条件を追加して、検索を 2020 年 7 月 14 日 14 時 44 分 25 秒（UTC）以降のメッセージに限定します。 start_date > 2020-07-14T14:44:25Z
subject	string	メッセージの件名。たとえば、subject ANY "login" の検索式を入力すると、件名「Change your login password」と一致します。subject eq "login" の検索式を入力すると、件名「login」に完全に一致します。
to	string	メッセージヘッダー内の完全な宛先。
uri	string	メッセージ内の任意の場所の URL。完全一致のみ。

演算子およびオペランド

演算子は、検索式で検索できるものと、検索方法を定義します。検索式の各演算子には、特定の有効なオペランドタイプがあります。演算子は、次の 2 つのタイプに分けられます。

- 数値：数値比較用。
- String テキストの検索と照合用。

次の表に、検索式で使用できる演算子を示します。

数値演算子

演算子	説明
=	フィールドがオペランド値の全部または一部に等しい
!=	フィールドがオペランド値の全部または一部と等しくない
>=	フィールドがオペランド値以上
>	フィールドがオペランド値より大きい
<	フィールドがオペランド値より小さい
<=	フィールドがオペランド値以下

文字列演算子

演算子	説明
in	フィールドはオペランドリスト内にあり、オペランドリストは 1 つ以上のカンマで区切られた値であり、角括弧で囲まれています。
not in	フィールドはオペランドリスト内になく、オペランドリストは 1 つ以上のカンマで区切られた値であり、角括弧で囲まれています。
any	フィールドの一部がオペランド全体に一致します。
not any	フィールドのどの部分もオペランド全体と一致しません。

オペランドは、フィールドで探している値を定義します。

タイプ

タイプとは、検索式のオペランドで使用できる値のデータタイプを指します。

タイプ	説明
string	1 つ以上の文字。検索式では、文字列を引用符で囲む必要があります。 数字を含む文字列は、数値と同じではありません。
float	小数点を含む数値。
integer	小数点を含まない数値。
date	ISO 8601 日付形式の数値。この形式には、ハイフンなどの非数値文字が含まれていますが、それでも数値タイプとして解釈されることに注意してください。注：日付を引用符で囲まないでください。
boolean	true または false で表されるバイナリ値。これらは文字列とは見なされず、引用符で囲まれないことに注意してください。
list	検索式のオペランドで複数の文字列を組み合わせられる複合タイプ。["item 1", "item 2"] の形式を使用します。

結合子

結合子は、単純な検索式を接続して複雑な検索式を作成します。

論理積	説明
AND、&	どちらも true である必要がある
OR、|	どちらかが true であればよい

エラー

高度なフィッシング防御検索式を処理する前に、検索式の構文エラーをチェックします。他のエラーが発生する可能性もあります。このセクションでは、考えられるエラーをリストし、エラーを解決するために検索式で何を見るべきかについて説明します。

「DSL構文にエラーがありました（There was an error in your DSL syntax.）」「[snippet]付近の入力が途中で終了しました（Premature end of input near [snippet].）」

これは、括弧や引用符などの何かが閉じられていないことを意味します。すべてのグループ化記号はペアで使用する必要があり、このエラーは、グループ化記号のペアの 2 番目のインスタンスが見つからなかったことを示します。[snippet] は、エラーにできるだけ近い検索式のセクションです。

「DSL構文にエラーがありました（There was an error in your DSL syntax.）」「[snippet]付近に予期しない入力があります（Unexpected input near [snippet].）」

これは、不当なオペランド、一致しないオペランド、または余分な閉じ括弧があることを意味します。「不当な」とは、オペランドのタイプミスを意味する可能性があるため、このトピックの情報を使用して、スペルミスがないか慎重に確認してください。[snippet] は、エラーにできるだけ近い検索式のセクションです。一致しないオペランドとは、to >= username@gmail.com のようなものです。これは、to フィールドが文字列値を取り、以上として評価できないためです。

「DSL構文にエラーがありました（There was an error in your DSL syntax.）」「[snippet]で何をするのか不明です（Don't know what to do with [snippet].）」

これは、エラーが検出され、上記のエラーのいずれかであると明確に判断できない場合の一般的なエラーメッセージです。これが発生する理由の 1 つは、検索式で field operator operand のパターンを使用していない場合です。これは、フィールドまたは演算子を誤って入力した場合も発生する可能性があります。

「使用できないワイルドカードがあります（Wildcards not allowed）」

これは、オペランドにワイルドカード文字が見つかったことを意味します。文字列リテラルとして * や ? の文字を検索式に含める場合は、^* や ^? のように、^ でエスケープする必要があります。

「括弧内で使用できないORステートメントがあります（OR statements not allowed in parentheses.）」「クエリを書き直してください（Please rewrite your query.）」

OR 結合を含む複数用語の検索式を括弧で囲むことはできません。

誤り：

from_domain = foo.com and (subject = "x" OR subject = "y")

正しい:

(from_domain = foo.com and subject= "x") OR (from_domain = foo.com and subject = "y")

MS Graph API を適用している組織は、10,000 件の既存メッセージを超えることのできないカスタム CDR ルールを作成できるようになりました。また、センサーが適用されている組織は、2,000 件の既存メッセージを超えるカスタム CDR ルールを作成できません。より少ないメッセージセットを返すように検索条件を絞り込んでください。

検索式は、MS Graph API では 10,000 件を超える結果、またはセンサーの適用では 2,000 件を超える結果を返しました。検索結果の合計数を制限するには、field operator operand 構造を追加します。以下に例を示します。

検索式がゼロの結果を返した場合でも、エラーであるとは限りません。これらのエラーは構文エラーとシステム制限をキャッチしますが、検索式の他のエラーである可能性も十分にあります。たとえば、to または from フィールドを使用しているときにオペランドに電子メールアドレスを誤って入力した場合、または現在データストアに一致するものがない場合などです。結果が表示されるはずなのに表示されない場合は、スペル、日付形式、その他の可能性(オペランドの類似文字など)を再確認してください。たとえば、I(大文字の i)と l(小文字の L)、または O(大文字の o)と 0(ゼロ)などです。

また、存在することがわかっているがまだ組織に侵入していないメッセージの脅威をキャッチするためのローカルルールを作成する際に、まず検索式を設計した場合は結果がゼロになると予想される場合があります。

「[field name]はサポートされているフィールドではありません([field name] is not a supported field.)」

これは、CDR ルールでサポートされていない検索式の一部としてフィールドが入力されたことを意味します。CDR の検索式で使用できるのは上記のフィールドのみです。

「リストは[field name]のフィールドでサポートされている値ではありません(Lists are not a supported value for field: [field name].)」

フィールドを使用する検索式では、値のリストをオペランドとして使用できません。検索式に指定できる値は 1 つだけです。

別の方法として、OR 結合で結合された複数の検索式を使用できます。ですので、以下のようにはできません。

field = ["value1", "value2", "value3"]

上記は次のように書き換えることができます。

field = "value1" OR field = "value2" OR field = "value3"

「[field name]の値は数値である必要があります(The value of [field name] must be numeric.)」

このフィールドを使用した検索式では、オペランドとして有効なのは数値のみです。オペランドが数字で、引用符で囲まれていないことを確認してください。引用符で囲まれた値は文字列と見なされます。

「[field name]の値は文字列または有効なリストである必要があります（The value of [field name] must be a string or valid list.）」

このフィールドを使用した検索式では、オペランドとして有効なのは文字列または文字列のリストのみです。このフィールドを使用した検索式に数値またはブール値が含まれていないこと、およびオペランドが引用符で囲まれていることを確認してください。

「[field name]の値はtrueまたはfalseである必要があります（The value of [field name] must be true or false.）」

このフィールドを使用した検索式では、オペランドとして有効なのはブール値のみです。このフィールドを使用した検索式には true または false のいずれかのオペランド値のみが含まれていること、および値が引用符で囲まれていないことを確認してください。

「[field name]の値を空の文字列にすることはできません（The value of [field name] cannot be an empty string.）」

CDR ルールの検索式では、空の文字列（""）は使用できません。

「search_dslには継続的な監視のために少なくとも1つの有効なフィールドが含まれている必要があります（search_dsl must contain at least one valid field for ongoing monitoring.）」

これは、CDR ルールを最初に検証して保存した後に予期しないことが発生したというエラーです。詳細については、Cisco サポートにお問い合わせください。

例

このセクションでは、検索式の例を示します。

内部ドメイン

内部のドメイン、つまり所有し、制御し、信頼しているドメインを識別する必要があります。これらは、内部タグを指定したドメインです（これはメッセージ検索でも実行できる検索式であることに注意してください。メッセージ検索で実行できることはすべて DSL 検索式でも実行できますが、後者ではさらに多くのことを実行できます。この例は、非常に単純な検索式を示しています）。

domain_tags = "internal"

この検索式は、内部タグが付けられたドメインを含むすべてのメッセージに一致します。

IP アドレスと評価結果

特定の IP アドレスを含むメッセージを識別したい場合は以下の検索式を使用します。

(ip = "1.2.3.4") OR (ip = "2.3.4.5")

この検索式は、IP アドレス 1.2.3.4 または IP アドレス 2.3.4.5 のいずれかを含み、SBRS 値も含むすべてのメッセージに一致します。

添付ファイルを受信するユーザー

特定のユーザーに送信されたメッセージの添付ファイルについて懸念がある場合は以下の検索式を使用します。

to = "jsmith@mycompany.com" AND has_attachment = "true"

この検索式は、jsmith@mycompany.com に送信された、あらゆる種類の添付ファイルを持つすべてのメッセージに一致します。

特定の種類の添付ファイルのみを検索することもできます。

(to="jsmith@mycompany.com" & has_attachment="true"& attachment_extensions="doc") OR

(to="jsmith@mycompany.com" & has_attachment="true"& attachment_extensions="docx") OR

(to="jsmith@mycompany.com" & has_attachment="true" & attachment_extensions="rtf")

この検索式は、jsmith@mycompany.com に送信され、添付ファイルがあり、その添付ファイルの拡張子が doc、docx、または rtf であるすべてのメッセージに一致します。これらの拡張子は、Microsoft Word ドキュメントの一般的な拡張子です。

レピュテーションの低い特定の用語

特にブロックしたいと考えている特定のキャンペーンの一部であると思われるメッセージについて懸念がある場合は以下の検索式を使用します。

(subject="important" AND domain_reputation <= 2 AND domain_tags NOT IN ["service", "customer"]) OR

(subject="urgent" AND domain_reputation <= 2 AND domain_tags NOT IN ["service", "customer"])

この検索式は、件名に「urgent」または「important」が含まれるメッセージ(大文字と小文字は区別されないことに注意してください)で、ドメインのレピュテーションが低く、信頼できるタイプの 1 つとしてタグ付けしたドメインからのものではないすべてのメッセージに一致します。

通知

高度なフィッシング防御Advanced Phishing Protection は、システムイベントの発生を知らせる通知システムを提供します。これらの通知は次のカテゴリに分類されます。

- センサー
- ホストシステム
- ポリシー

有効にできる通知は、システムの設定によって異なります。たとえば、Google G Suite を使用している場合、有効にできる通知の 1 つは、[G Suiteに提供された資格情報が適切に認証されていません(The credentials supplied for G Suite stop authenticating correctly)] です。

送信する通知のチェックボックスをオンにします。送信しない通知のチェックボックスをオフにします。終わったら [保存(Save)] をクリックします。

選択した通知は、[通知(Notification)] セクションの [電子メールアドレス(Email Address)] リストにあるすべての電子メールアドレスに送信されます。

通知受信者を追加する

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [システム通知(System Notifications)] タブをクリックします。
3. [通知(Notification)] セクションで、[追加受信者(Additional Recipients)] フィールドに電子メールアドレスを入力します。
4. [追加(Add)] をクリックします。
5. [保存(Save)]をクリックします。

通知受信者を削除する

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [システム通知(System Notifications)] タブをクリックします。
3. [通知(Notification)] セクションで、[電子メールアドレス(Email Address)] リストの名前の横にある [x] をクリックします。
4. [保存(Save)]をクリックします。

ポリシー

ポリシーを使用して、組織が特定の条件を満たすメッセージを受信したときに、どうなるかを指定できます。たとえば、特定の送信側ドメインからのすべてのメッセージを検索し、受信者と管理者に通知するポリシーを記述することができます。または、疑わしいメッセージを隔離フォルダに移動するポリシーを作成することもできます(Enforcement の顧客のみ)。基本的な考え方は、受信メールトラフィックの特定の条件(指定した条件)に反応することです。

考えられるアクションとしては、Web UI で検索およびレポートするための受信メッセージのロギング(デフォルトのアクション)、(元の受信者や指定された管理ユーザーへの)通知の送信、特定のメールフォルダへのメッセージの移動(適用の設定のみ)、またはメッセージ全体の削除(適用の設定のみ)などがあります。

いくつかのポリシーを作成または編集する前に知っておくべき重要な点がいくつかあります。

- 各メッセージに対してすべてのポリシーが評価され、単一のメッセージが複数のポリシーと一致することがあります。

- 複数の適用ポリシーと一致するメッセージへの適用アクションは、次の優先順位で実行されます。
    a. 受信トレイ
    b. 削除
    c. デフォルト フォルダの移動
    d. 組織の適用設定(「「組織設定」 ページ 197」を参照してください)で設定した順序での追加フォルダの移動。
- 通知アクションまたは適用アクションなしのポリシーを作成できます。ポリシーと一致するすべてのメッセージが、イベントログとレポートに記録されます。

[ポリシー(Policies)] ページには、既存のポリシーがリストされます。このページから、ポリシーの作成、システム通知への登録、ポリシーに関するイベントログエントリの表示を実行できます。ポリシーの詳細については、「「ポリシーの結果を表示する」 ページ 162」を参照してください。事前に定義されているポリシーについては、「「デフォルトポリシー」 下」を参照してください。自分でポリシーを試すには、「「テストポリシーを作成する」 ページ 161」を参照してください。

デフォルトポリシー

高度なフィッシング防御で最初に組織が作成される際に、一連のデフォルトの事前設定済みのポリシーが自動的に作成されます。これらのポリシーは、Cisco 顧客が高度なフィッシング防御を使ってキャッチする最も一般的な条件と一致します。メッセージの照合を開始し、通知や適用アクションをポリシーに定義するには、ポリシーを有効にする必要があります。最初にアクションのないポリシーを有効にすることをお勧めします。ポリシーの一致をログに記録し、結果を監視することから始めて、それから通知や適用アクションを選択します。

この セクション では、デフォルトポリシーのすぐに使用できる設定について説明します。

この情報は、これらのポリシーのいずれかの設定を変更し、それらをデフォルトの状態に戻す必要がある場合に役立ちます。

以下の表で特に定義されていない設定には、次の値があります。

- 方向:受信
- テキストフィールド:空白
- チェックボックス:オフ
- ドロップダウンリスト:値が選択されていません
- 2 つのハンドルを持つスライダ:左端に左ハンドル、右端に右ハンドル([メッセージ数が超える場合(When message count exceeds)] 制御ではハンドルは 1 つのみで、デフォルトは 10)

ポリシー名	設定	値	説明
ブランド表示名偽装	攻撃タイプ	ブランド表示名偽装	攻撃タイプには、ブランド表示名偽装が含まれます。表示名で共通のブランドがスプーフィングされているブランドの偽装をキャッチします。
C レベル偽装	差出人	C レベルエグゼクティブ(アドレスグループ)	アドレスグループの C レベルエグゼクティブの表示名を照合します。BEC 攻撃、および CEO、CFO、その他のトップエグゼクティブの偽装をキャッチします。このポリシーでは、「最高責任者エグゼクティブ」アドレス グループを入力する必要がある点に注意してください。このグループは、デフォルト アドレス グループとしても作成されます。

ポリシー名	設定	値	説明
エグゼクティブ偽装	差出人	エグゼクティブ（アドレスグループ）	アドレスグループのエグゼクティブの表示名を照合します。BEC 攻撃、および組織におけるその他のエグゼクティブの偽装をキャッチします。このポリシーでは、「エグゼクティブ」アドレス グループを入力する必要がある点に注意してください。このグループは、デフォルト アドレス グループとしても作成されます。
類似ドメイン	攻撃タイプ	類似ドメイン	攻撃タイプには、類似ドメインが含まれます。ciisco.com や paypa1.com. のような、意図的に類似した名前を使用して偽装したドメインをキャッチします。
信頼性の低いメッセージとレピュテーションの低いサーバー	信頼スコアの範囲	0.0 ～ 2.5	メッセージの信頼スコアは <= 2.5 で、SBRS スコアは <= −2.0 です。SEG をすり抜ける一般的なスパムやグレイメールをキャッチします。
	SBRS 範囲	−10.0 ～ −2.0	
Rapid DMARC	ドメインのタグ	内線	ドメインタグは「内部」であり、攻撃タイプにはドメインスプーフィングが含まれます。従業員に送信される自身のドメインのスプーフィングをキャッチします。このポリシーは、すべての送信元を認証する長いプロセスを経由する必要のない DMARC 拒否ポリシーを模倣しています。Cisco 高度なフィッシング防御の信頼モデルは、インバウンド送信元の信頼性を学習します。
	攻撃タイプ	ドメインスプーフィング	
パートナードメインのスプーフィング	ドメインのタグ	パートナー	ドメインタグは「パートナー」であり、攻撃タイプにはドメインスプーフィングが含まれます。パートナーのドメインのスプーフィングをキャッチします。
	攻撃タイプ	ドメインスプーフィング	
C レベルへの疑わしいメッセージ	目的	C レベルエグゼクティブ（アドレスグループ）	メッセージの信頼スコアが 0 以上、3.0 以下である C レベルエグゼクティブの電子メールアドレスを照合します。C レベルエグゼクティブの 1 人に送信された、信頼できない、または非常に疑わしいメッセージをキャッチします。
	信頼スコアの範囲	0.0 ～ 3.0	
信頼できないメッセージ	信頼スコアの範囲	0.0 ～ 1.1	メッセージ信頼スコアは 0 以上 1.0 以下です。

これらのデフォルト ポリシーの条件は、組織のメール フローの経験および特性に基づいて編集できます。初期状態の条件は、Cisco カスタマーベース全体にわたり何が有効であるかに基づいています。

ポリシーを作成する

ポリシーの作成は簡単です。特定の種類のメッセージを照合する条件を指定し、それらの条件に一致するメッセージに対して実行するアクションを設定します。

1. [管理(Manage)]>[ポリシー(Policies)]に移動します。
2. [ポリシーの作成(Create Policy)]をクリックします。
3. ポリシー設定を定義します。詳細については、「「ポリシー設定」見開きページ」を参照してください。
4. [作成(Create)]をクリックします。

ポリシーを編集する

1. [管理(Manage)]>[ポリシー(Policies)]に移動します。
2. ポリシー名をクリックします。
3. ポリシー設定に必要な変更を加えます。詳細については、「「ポリシー設定」見開きページ」を参照してください。
4. [保存(Save)]をクリックします。

ポリシーを有効または無効にする

1. [管理(Manage)]>[ポリシー(Policies)]に移動します。
2. ポリシー名をクリックします。
3. ポリシー名の下のスライダをクリックして、ポリシーを有効または無効にします。

4. [保存(Save)]をクリックします。

ポリシーを削除する

1. [管理(Manage)]>[ポリシー(Policies)]に移動します。
2. ポリシーの名前をクリックします。
3. ページの下部で[[policy name]の削除(Delete [policy name])]をクリックします。
4. [OK]をクリックします。

ポリシー通知をカスタマイズする

ポリシー通知には、定義済みのメッセージコンテンツを含む変数プレースホルダの使用など、カスタマイズ可能なテキストが含まれています。

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [元の受信者のポリシーテキストを設定(Configure Policy Text for Original Recipients)] リンクをクリックします。
3. ポリシー通知に必要なコンテンツを入力します。ここで定義されたコンテンツは、すべてのポリシー通知に使用されます。詳細については、以下の「ポリシー通知のコンテンツ設定」および「ポリシー通知のコンテンツ変数」セクションを参照してください。
4. [OK] をクリックします。

ポリシー通知のコンテンツ設定

ポリシー通知には、次のセクションが含まれています。

セクション	説明	デフォルトのコンテンツ
件名	これが通知の件名になります。	[信頼できないメッセージ] $subject
メッセージを開く	これは、通知メッセージの先頭に使用できるオプションのテキストです。	警告: システムが信頼できないメッセージを検出しました。
メッセージ本文	これにより、通知をトリガーしたメッセージの差出人と件名が表示されます。これは変更できません。	差出人:「$from」 件名:「$subject」
メッセージを閉じる	これは、通知メッセージの最後に使用できるオプションのテキストです。	注意して続行してください。

ポリシー通知のコンテンツ変数

これらは、ポリシー通知の [件名(Subject)]、[メッセージを開く(Message Open)]、[メッセージを閉じる(Message Close)] セクションで使用できる変数です。[件名(Subject)] セクションでは、大量のコンテンツを表す変数を使用しないでください。

変数	定義
$from	通知をトリガーしたメッセージの [差出人(From)] フィールドのコンテンツを表します。
$subject	通知をトリガーしたメッセージの件名を表します。

ポリシー設定

このトピックでは、ポリシー設定について説明します。メッセージにポリシーを適用するには、メッセージがポリシーのすべての設定と一致する必要があります。

ポリシーが有効なポリシーであるために、必要なのは 1 つの条件のみであり、アクションは必要ありません。(アクションが定義されていないポリシーは、「監視」ポリシーと呼ばれることもあります)ポリシーを作成するためのインターフェイスを使用して、かなり具体的なメッセージセットを照合する非常に限られた条件を作成できます(たとえば、「ユーザー A からユーザー B 宛てで、送信側 IP レピュテーションが -6.7 以上 -6.6 以下」など)。また、インターフェイスを使用して、かなり多数の(ほぼすべてに近い)受信メッセージに一致する可能性がある非常に幅広い条件を設定することもできます(たとえば、「信頼スコアが 2.2 以上 10.0 以下の任意のメッセージ」)。ポリシーの設定時には、過度に幅広いポリシーを作成しないように注意してください。

範囲、つまり上限値と下限値を設定するポリシー設定では、常に包含範囲となります。つまり、範囲には上限と下限が含まれるということです。技術用語では、これは「以上」および「以下」の境界を定義することを意味し、厳密には境界値は含まない「超過」および「未満」ではありません。

<table>
<tr><th>設定</th><th>説明</th></tr>
<tr><td>ポリシー名</td><td>名前は、ポリシーが何をするように設計されているかを適切に説明するものでなければなりません。</td></tr>
<tr><td>有効化/無効化</td><td>ポリシーが電子メールストリームに適用されるかどうかを決定します。</td></tr>
<tr><td>メッセージの方向</td><td>照合するメッセージの方向を次の中から選択します。
[受信(inbound)]:組織外から組織に送信されたメッセージ
[送信(outbound)]:組織内から組織外に送信されたメッセージ
[内部(internal)]:組織内で開始および終了したメッセージ
次の表に示すように、一部のポリシー設定は、一部のメッセージの方向でのみ使用できます。
<table>
<tr><th>ポリシー設定</th><th>着信</th><th>発信</th><th>内線</th></tr>
<tr><td>差出人/返信先/宛先</td><td>✔</td><td>✔</td><td>✔</td></tr>
<tr><td>件名</td><td>✔</td><td>✔</td><td>✔</td></tr>
<tr><td>送信ドメイン</td><td>✔</td><td></td><td></td></tr>
<tr><td>ドメインのタグ</td><td>✔</td><td></td><td></td></tr>
<tr><td>添付ファイル</td><td>✔</td><td>✔</td><td>✔</td></tr>
<tr><td>信頼スコアの範囲</td><td>✔</td><td></td><td></td></tr>
<tr><td>攻撃タイプ</td><td>✔</td><td>✔</td><td>✔</td></tr>
<tr><td>詳細(真正性スコアの範囲、ドメインレピュテーションの範囲、SBRS 範囲、IP アドレス)</td><td>✔</td><td></td><td></td></tr>
<tr><td>適用</td><td>✔</td><td></td><td>✔</td></tr>
<tr><td>通知</td><td>✔</td><td>✔</td><td>✔</td></tr>
</table></td></tr>
<tr><th colspan="2">コンテンツ</th></tr>
<tr><td colspan="2">[差出人(From)]、[返信先(Reply-To)]、および [宛先(To)] フィールドでは、次のいずれかを実行できます。
個別の電子メールアドレスを入力する
フィールドをクリックしアドレスグループを選択する</td></tr>
</table>

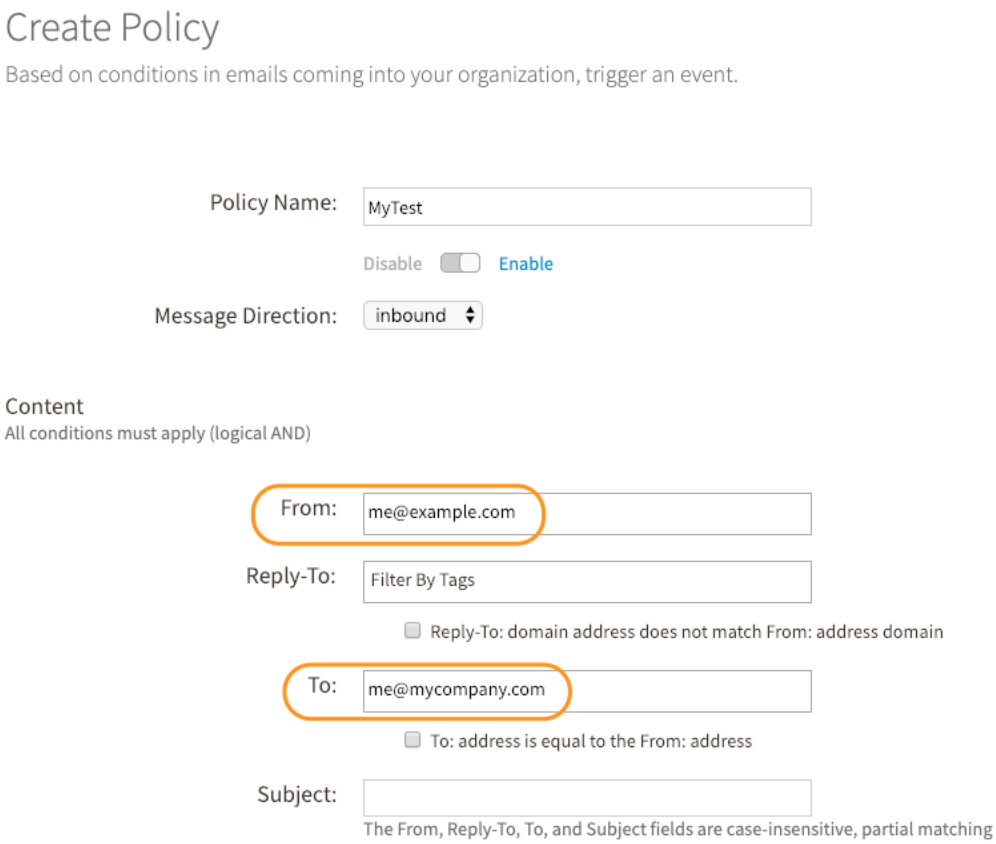
設定	説明
（一般的には、アドレスグループを使用することでポリシーの管理が容易になります）[差出人（From）]、[返信先（Reply-To）]、[宛先（To）]、および [件名（Subject）] フィールドは、大文字と小文字を区別せず、部分一致です。	
差出人	アドレスグループ内のユーザーの偽装を検出する場合は、ポリシー条件の [差出人（From）] フィールドでアドレスグループを使用します。条件は、[差出人（From）] ヘッダーの表示名（つまり、フレンドリ形式）でアドレス グループ メンバーの名前を検索します。特定の [差出人（From）] ヘッダーが表示名を使用していない場合、条件は、アドレスグループ内の電子メールアドレスのローカル部分を評価し、それが [差出人（From）] ヘッダーの電子メールアドレスと一致するかどうかを確認します。 差出人のアドレスが入力したアドレスと一致する場合、条件は、メッセージの真正性も考慮します。 たとえば、次のアドレスを含むアドレスグループを考えます。 「John Doe」<jdoe@example.com> • 「John Doe」<jdoe@not-example.com> という差出人からメッセージを受信した場合、危険性のない送信元の John Doe の偽装として条件が一致すると、ポリシーに定義されたアクション（アラート、適用など）が実行されます。 • 本物でないメッセージを「John Doe」<jdoe@example.com> という差出人から受信した場合、実際の電子メールアドレスが使用されていたとしても本物ではないため John Doe の偽装として条件が一致します。アクションが実行されます。 • フレンドリ形式の部分が存在しない場合は、アドレスのローカル部分が評価され、[差出人（From）] ヘッダーの電子メールアドレスのローカル部分に基づいて、アドレス <jdoe@example3.com> が一致します。
返信先	アドレスグループは単に、[返信先（Reply-To）] や [宛先（To）] フィールドがアドレスグループ内のエントリと完全一致するメッセージを検索し、表示部分は無視します。[返信先（Reply-To）] や [宛先（To）] フィールドでアドレスグループに一致するポリシーは、一般に、件名の文字列の一致や、メッセージの信頼スコアなどの他の条件と一緒に使用されます。たとえば、ポリシーの条件を次のように指定できます。財務アドレスグループのメンバー宛てで、件名に「請求書（Invoice）」が含まれており、メッセージ信頼得点が 0 ～ 4.9。
宛先	
件名	メッセージの件名に一致させるものを入力します。ポリシーは、件名のあらゆる場所で値全体を検索します。たとえば、「goo」と入力すると、ポリシーは、「Google Password Confirmation」、「Goo-Goo Dolls tickets」、「Check out this gooey brownie recipe」を含む件名に一致します。または、「red fish blue fish」と入力すると、ポリシーは「one fish two fish red fish blue fish」を含む件名には一致しますが、「there were fish in the blue sea」を含む件名には一致しません。
送信ドメイン	単一のドメイン名を入力します。この設定は、メッセージヘッダー内の DKIM レコードの送信ドメイン値の一致を探します。
ドメインのタグ	フィールドをクリックして、1 つ以上のドメインタグを選択します。条件は、ドメインに選択したタグのいずれかが含まれているかどうかを評価します。
得点付け	
信頼スコアの範囲	スライダを使用して、ポリシーが考慮されるためにメッセージに必要な信頼スコアの範囲を定義します。選択した値は範囲に含まれます。つまり、範囲は包括的です。たとえば、信頼スコア範囲の境界を下限が 1.0、上限が 2.0 になるように選択した場合、ポリシーは、信頼スコアがぴったり 1.0 または 2.0 のメッセージと一致します。
攻撃タイプ	フィールドをクリックして、ポリシーが考慮されるためにメッセージに必要な 1 つ以上の攻

設定	説明
	撃タイプを選択します。いずれかの攻撃タイプがメッセージに適用される場合、ポリシーは考慮されます。
詳細設定	
真正性スコアの範囲 ドメインのレピュテーションの範囲 SBRS 範囲	ポリシーをデフォルト以外の範囲（範囲内のすべて）に一致させる場合は、スライダを調整します。選択した値は範囲に含まれます。つまり、範囲は包括的です。たとえば、ドメインレピュテーションの範囲の境界を下限が 1.0、上限が 2.0 になるように選択した場合、ポリシーは、ドメインレピュテーションがぴったり 1.0 または 2.0 のメッセージと一致します。
IP アドレス	1 つ以上の IP アドレスをカンマで区切って入力します。IP アドレス範囲を入力することもできます。条件は、ヘッダー内の IP アドレスが一致するかどうかを評価します。
アクション	
ここで定義する設定により、メッセージがポリシーに一致したときに実行される追加のアクションが決まります。デフォルトのアクションでは、ポリシーに一致するメッセージはポリシーログに記録されますが、メッセージ自体とその目的のルートは変更されません。	
適用	Office 365 または G Suite をメールストアとして使用し、適用を有効にしている場合（「「適用の設定：MS Graph API を使用した Office 365」 ページ 89」または「「適用の設定：G Suite」 ページ 82」を参照してください）は、一致するメッセージを削除するか、または受信トレイから指定したフォルダに移動するように選択できます。ポリシー条件のセットに一致するときに、メッセージを受信トレイに移動するように選択することで、「ホワイトリスト」ポリシーを作成することもできます。 適用アクションは、元の受信者への通知と組み合わせて使用できます。それによって、エンドユーザーは、高度なフィッシング防御がポリシー条件の一致に基づいてメッセージを移動するたびに、通知を受信できます。 複数の適用ポリシーと一致するメッセージへの適用アクションは、次の優先順位で実行されます。 • 受信トレイ • 削除 • デフォルト フォルダの移動 • 組織の適用設定（「「組織設定」 ページ 197」 を参照してください）で設定した順序での追加フォルダの移動。
通知	通知先と通知方法を指定できます。 通知の元の受信者は、ポリシーがトリガーされた際にメッセージのすべての受信者へ個々に通知を送信します。（これによりバウンスメッセージが発生する可能性があることに注意してください。たとえば、センサーがメッセージを解析し、存在しないメールボックスに通知を送信しようとした場合に発生する可能性があります） 通知管理者は、すべての一致するメッセージに関して単一の通知メッセージを送信するか、または特定のポリシーに一致するメッセージの数が定義したしきい値を超えたときに単一のダイジェスト通知を送信します。 ユーザーが受け取る通知の内容をカスタマイズできます。詳細については、「「ポリシー通知をカスタマイズする」 ページ 157」を参照してください。

テストポリシーを作成する

基本ポリシーの作成は簡単です。入力する必要があるのは 3 種類の情報だけです。

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [ポリシーの作成(Create Policy)] をクリックします。
3. 次の情報を入力します。
    - [ポリシー名 : (Policy Name:)] : MyTest
    - [差出人 : (From:)] : 個人用電子メールアドレス
    - [宛先 : (To:)] : 会社の電子メールアドレス



この時点で、ポリシーは完了です。アクションを指定しなかったことに注意してください。すべての一致したポリシーのデフォルト アクションは、メッセージをポリシー ログに記録することです。

4. [作成(Create)] をクリックします。
5. 個人アカウントから会社のアドレスにメッセージを送信します。
6. [管理(Manage)] > [ポリシー(Policies)] ページで、[ポリシーログ(Policy Log)] タブをクリックします。ログ内に、ポリシーと送信したメッセージのエントリが表示されています。

ポリシーイベントのポリシーイベントログ

以上です。受信メールを照合するためのポリシーが正常に作成されました。

条件に基づく受信メッセージの照合は、ポリシーを作成するための基本的な構成要素です。ここから、詳細と複雑さ、照合する情報カテゴリ、特定のドメイン、または IP アドレスを追加できます。送信者または受信者のグループを照合するためのアドレスグループを作成できます。（詳細については、「「アドレスグループ」 ページ 188」を参照してください）得点オプションの範囲を指定できます。

次に、一致したメッセージに対して実行するアクションを指定します。

アクションの指定

これで、メッセージを照合するためのポリシーの作成については十分に理解しました。次に、それらの照合が行われたときに何が起きるかを指定します。デフォルトのロギングに加え、通知と適用（enforcement 顧客のみ）の 2 つのその他のアクションを指定できます。アクションは連続体の一部と考えます。つまり、ロギングが最も影響の少ないアクションで、続いて、通知アクション、さらに、適用が最大の影響を及ぼします。ポリシーについて慣れるまでの間は、最初にロギングのみを試し、その後、管理者への通知、次にメッセージ受信者への通知、その後、適用を検討します。

適用顧客：広範になり過ぎないようにするため（あまりに広範なポリシーは誤検出につながることがあります）、適用を有効にする前にポリシーをテストします。

ポリシーの結果を表示する

いくつかのポリシーを作成し、有効にした後は、その結果についての考察や以下の質問に対する回答を行うことをお勧めします。

- ポリシーが期待どおりに機能しているか
- 何件のメッセージが一致しているか
- 一致数が増加傾向にあるか

この種の情報を確認するには、次の 3 つの方法があります。

- ポリシーログは、ポリシー一致の実行ログです。
- [管理（Manage）] > [レポート（Reports）] ページには、時間の経過に伴うポリシー一致の集計が表示されます。
- [メッセージの検索（Search Messages）] ページで、一致したポリシーを検索できます。

ポリシーログ

[管理（Manage）] > [ポリシー（Policies）] ページで、[ポリシーログ（Policy Log）] タブをクリックします。これは、すべてのポリシー一致とシステム通知イベントのログです。

ポリシーログでは、各ポリシーの一致が発生すると、それが表示されます。これは、メッセージ別のポリシー一致のリストです（一致ごとに 1 メッセージ）。

ポリシーの名前をクリックして、一致したポリシーを表示します。[イベント（Event）] 列の行をクリックして、ポリシーに一致するメッセージの詳細を表示します。

ポリシーログをフィルタリングして、特定のポリシーに一致するメッセージを表示し、このビューにシステム通知を表示するかどうかを選択できます。

ポリシーレポート

[管理(Manage)] > [レポート(Reports)] ページでは、時間の経過に伴うポリシーイベントのサマリー、つまり、ポリシーごとの一致数が示されます。

ポリシーエディタ内でポリシー名をクリックすると、ポリシーの条件とアクションを確認できます。

メッセージ数(または、水平バー)をクリックすると、そのポリシーの詳細なポリシーレポートを表示できます。

ポリシー レポートには、現在の日付の一致数が表示されます。右側でより長い期間を選択すると、タイムラインを展開できます。この表示で、そのポリシーの一致における傾向を確認できます。現在、そのポリシーに一致するメッセージは増加しているか。減少しているか。ポリシーレポートでメッセージ数をクリックすると、[メッセージの検索(Search Message)] 結果にメッセージが表示されます。

適用に関するレポート

[ポリシーの表示(Show policies)] ドロップダウンリストで [適用アクションを使用(with Enforce action)] を選択すると、適用アクションを指定したすべてのポリシーに関して、移動済みメッセージと未移動のメッセージのサマリーを表示できます。

適用アクションによるポリシーレポートのフィルタ処理

メッセージを検索する

[分析(Analyze)] > [メッセージの検索(Search Messages)] ページで、[一致したポリシー(Matched Policy)] フィールドでポリシーを選択して、選択したポリシーをトリガーしたメッセージを検索できます。

オンデマンドポリシー

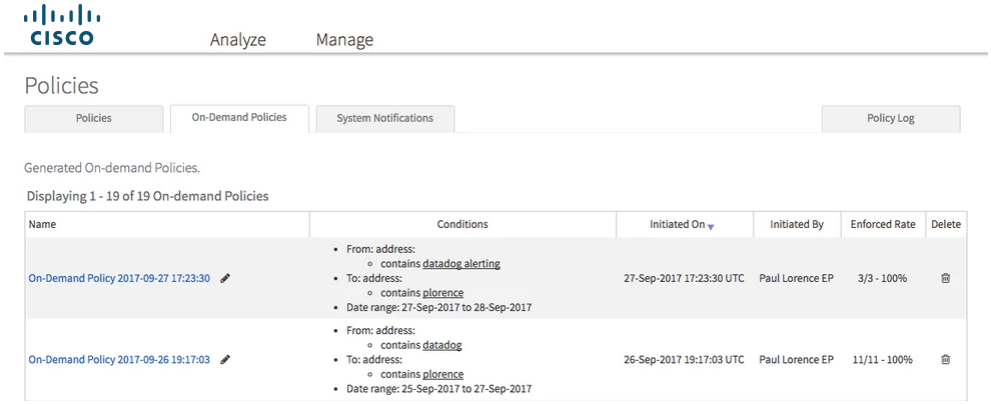
オンデマンドポリシーは、メッセージ検索に使用される条件に基づいてすばやく簡単に作成できるポリシーです。G Suite または Office365 環境で適用を有効にしている Cisco 高度なフィッシング防御 の顧客が使用できます。

オンデマンドポリシーを使用して、メッセージ セットにポリシー アクションを選択的に適用できます。これには、ユーザーの受信ボックスから特定のフォルダへのメッセージの移動（メッセージの移動先として複数のフォルダを使用可能にすることができる）、メッセージの削除、メッセージのユーザーの受信トレイへの再移動が含まれます。ユーザーの受信トレイに配信された後に、メッセージに適用することで、高度なフィッシング防御は、脅威を軽減する別のツールを提供します。たとえば、特定の電子メールメッセージが既存の防御ライン（スパムやウイルスフィルタリングなど）をくぐり抜けた場合、高度なフィッシング防御のオンデマンドポリシーを使用して、それらのメッセージをユーザーの受信トレイから移動することができます。

オンデマンドポリシーは、組織で適用が有効になっている場合にのみ使用できます。

オンデマンドポリシーのインデックスページ

オンデマンドポリシーはすべて、オンデマンドポリシーのインデックスページに時系列でリストされます。[管理（Manage）] > [ポリシー（Policies）] ページで、[オンデマンドポリシー（On-Demand Policies）] タブをクリックすると、オンデマンドポリシーが表示されます。



オンデマンドポリシーのインデックスページ

この表示から、オンデマンドポリシーの名前を変更したり、条件、誰がいつポリシーを開始したか、およびポリシーの適用レートを表示したりすることができます。

[削除（Delete）] アイコンをクリックすると、一覧からオンデマンドポリシーを削除できます。[削除（Delete）] アイコンをクリックすると、一覧からオンデマンドポリシーが削除されますが、メッセージの判定結果には影響しない点に注意してください。

最後の注意事項

オンデマンドポリシーは、検索ページから検索できます。

オンデマンドポリシーは、組織の監査ログで追跡されます。監査ログを表示するには、[管理（Manage）] > [組織（Organizations）] に移動し、組織名の下にある [監査（Audit）] リンクをクリックします。

パフォーマンスに関する注意事項

メッセージの移動レートは、メールボックス プロバイダー（G Suite または Office365）への API コールの速度と遅延によって異なります。

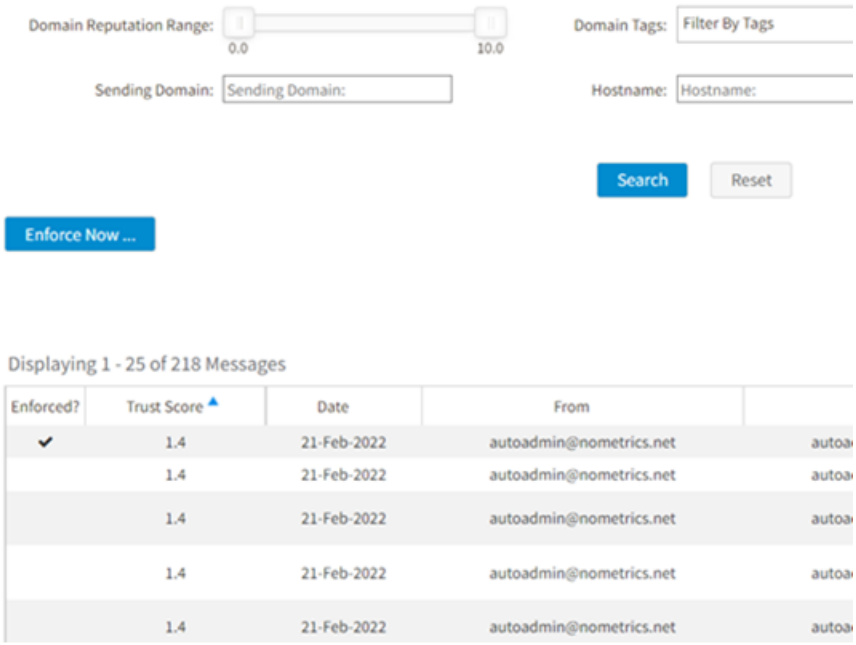
オンデマンドポリシーと「通常」（進行中）のメッセージポリシーの両方で、適用アクションには同じキューイング システムが使用されます。日常的に、メッセージポリシーからかなり多数のメッセージに対して適用を行っている場合は、オンデマンドポリシーからキューに適用アクションを追加すると、高度なフィッシング防御におけるメッセージへの適用のパフォーマンス全体に影響します。キューイング システムは、すべてのセンサーからの適用アクションを同時に受け入れます。/var/log/cisco/enforcer.log で、任意のセンサーの適用アクションのログを表示できます。

オンデマンドポリシーを作成する

オンデマンドポリシーは、検索結果ページから作成します。詳細については、「「メッセージ検索」 ページ 127」を参照してください。

オンデマンドポリシーの作成は、メッセージの検索結果ページの [今すぐ適用（Enforce Now）] ボタンを使用して行います。[今すぐ適用（Enforce Now）] ボタンは、組織で適用が有効になっている場合にのみ表示されます。メッセージの検索結果を表示しているときに、[今すぐ適用（Enforce Now）] ボタンをクリックします。

MS Graph API 適用を使用している組織では、オンデマンドポリシーを使って一度に適用できるのは 10,000 件以下のメッセージのみです。検索結果が 10,000 件を超える場合は、結果から最大 10,000 件のメッセージを選択して適用できます。センサーの適用を使用している組織では、オンデマンドポリシーを使用して一度に適用できるのは 2,000 件以下のメッセージのみです。検索結果が 2,000 件を超える場合は、結果から最大 2,000 件のメッセージを選択して適用できます。



[今すぐ適用（Enforce Now）] ボタン

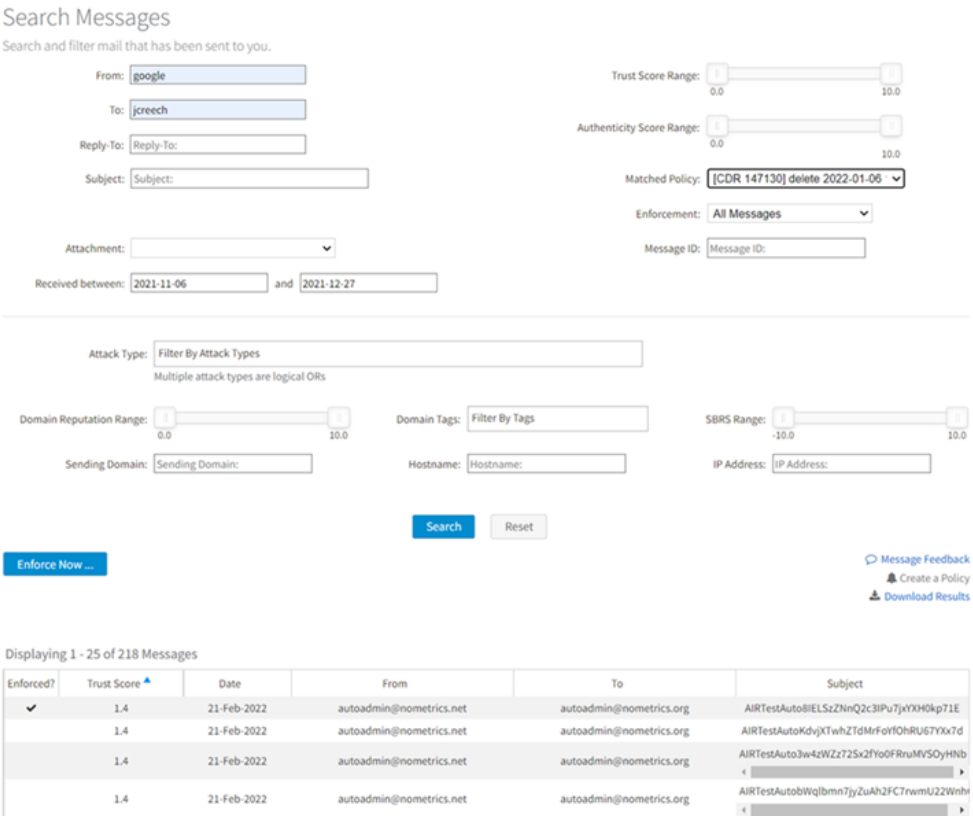
1. [分析（Analyze）] > [メッセージ検索（Search Messages）] に移動するか、ダッシュボード（[分析（Analyze）] > [ダッシュボード（Dashboard）]）の [メッセージ（Message）] リンクをクリックして、メッセージ

のリストを表示します。

2. 必要に応じて、表示される結果が、Graph API が適用されている組織では 10,000 件未満、センサーの適用を使用している組織では 2,000 件未満になるように検索条件を絞り込みます。

   検索条件にさらに条件を追加することで、結果を絞り込むことができます。たとえば、[宛先：(To:)]、[差出人：(From:)]、[件名(Subject)] などの検索条件に特定の Message-ID を追加できます。

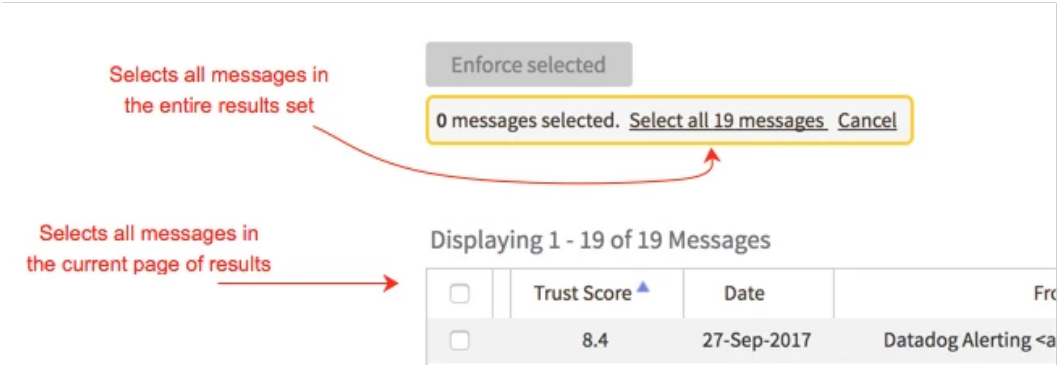
   この例では、検索条件は、特定のドメインから単一のユーザーへのメッセージ セットに絞り込まれています。



検索結果の絞り込み

3. [今すぐ適用(Enforce Now)] をクリックします。ボタンが [Enforce Selected(適用を選択済み)] に変わり、適用するメッセージを選択するまで非アクティブです。

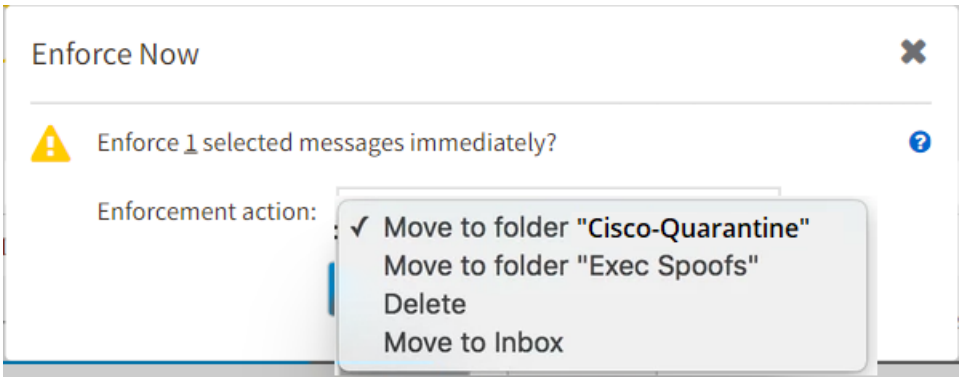
4. リンクをクリックして検索結果のすべてのメッセージを選択するか、検索結果の左側の列にあるボックスをクリックして検索結果の個別のメッセージやページを選択します。セット全体内のすべてのメッセージを選択することと、現在の結果ページに表示されているすべてのメッセージを選択することの相違点に注意してください。



個別のメッセージの選択とすべてのメッセージの選択の違い。

組織で**内部関係者偽装防止**が有効になっていて、すべてのメッセージを評価している場合(「組織設定」の「[メッセージの評価(Evaluate Messages)]」 ページ 199」の設定を参照してください)、オンデマンドポリシーは受信メッセージと内部メッセージにのみ適用されます。オンデマンドポリシーの作成時に選択した送信メッセージはすべて除外され、ポリシーの基礎として使用されません。

5. 少なくとも 1 件のメッセージを選択した後、[適用を選択済み(Enforce selected)] をクリックします。
6. [今すぐ適用(Enforce Now)] ダイアログボックスで、適用対象のメッセージ数を確認し、実行する適用アクションを選択します。(疑問符アイコンは、一部のメッセージを移動できない理由に関する追加情報を提供します)。

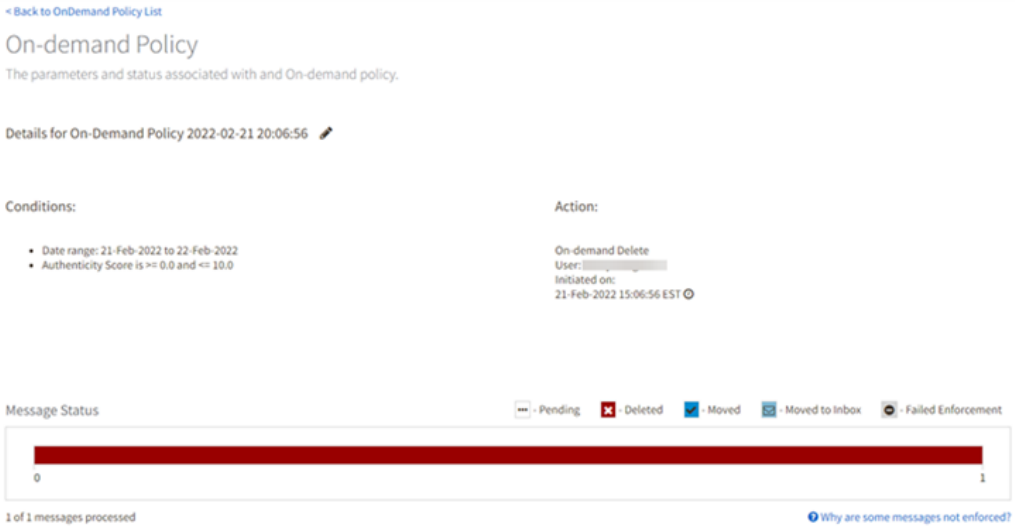


適用アクションの選択

7. [OK] をクリックして、メッセージをすぐに適用します。

[OK] をクリックすると、高度なフィッシング防御がセンサーに接続する間、オンデマンドポリシーの詳細ページが表示されます。センサーが接続されると、[メッセージステータス(Message status)] エリアに、適用対象のメッセージのリストが表示されます。

最初はメッセージセット全体のステータスが [保留中(pending)] としてリストされます。



オンデマンドポリシーの進行中のステータス。

システムがメッセージセットの処理を続行する間、メッセージの判定結果（[削除済み（Deleted）]、[移動済み（Moved）]、[受信トレイに移動済み（Moved to Inbox）]、[未適用（Not Enforced）] のいずれか）に関する新たな情報が受信されると、ページが更新されます。

すべてのメッセージが処理された後、ページには、オンデマンド ポリシーの最終結果が表示されます。

必要に応じて、鉛筆アイコンをクリックして、オンデマンド ポリシーの名前を変更します（例：「Deleted Spam messages」）

適用アクションのステータスに加え、適用が行われた時点で、メッセージの受信者がメッセージを既読であったかどうかを確認することもできます。[既読？（Read?）] 列に開封された封筒がある場合は、受信者によってそのメッセージが読まれたことを意味しています。

レポート

Cisco 高度なフィッシング防御 では次の 2 種類のレポートが用意されています。

- 高度なフィッシング防御で定義された、適用アクションありまたはなしのポリシーに関する情報（[管理（Manage）] > [レポート（Reports）] ページで利用可能）。
- グラフィック形式で表示される主要な脅威メトリックに関する情報（高度なフィッシング防御のダッシュボード（[分析（Analyze）] > [ダッシュボード（Dashboard）]、または製品ロゴをクリック）の [エグゼクティブサマリー（Dashboard）] タブと [脅威トレンド（Threat Trends）] タブで利用可能）。

レポートページ

レポートページでは時間の経過に伴うポリシーイベントのサマリーが表示されます。具体的には、選択した期間中における各ポリシーに一致したメッセージの数です。ポリシー名をクリックすると、ポリシーエディタでポリシーの設定を表示できます。メッセージ数（または、水平バー）をクリックすると、そのポリシーのポリシーレポートを表示できます。

デフォルトでは、ポリシーレポートには、現在の日付の一致数が表示されます。右側でより長い期間を選択すると、タイムラインを展開できます。このビューでは、そのポリシーに一致するメッセージの経時的な傾向を表示できます。現在、そのポリシーに一致するメッセージは増加しているか。減少しているか。ポリシーレポートでメッセージ数をクリックすると、[メッセージの検索(Search Message)] 結果にメッセージのリストが表示されます。

脅威トレンドレポートとエグゼクティブ サマリー レポート

ホームページ([分析(Analyze)] > [ダッシュボード(Dashboard)])の [脅威トレンド(Threat Trends)] タブと [エグゼクティブサマリー(Executive Summary)] タブの両方に、高度なフィッシング防御によって蓄積された最近のデータがまとめられています。

折れ線および棒グラフのレポート表示では、任意の日付の表示にカーソルを合わせると、その日付の詳細データを含むポップアップを表示できます。

このページでは、すべてのレポートの期間を選択できます。次から選択します。

- 7 日間
- 2 週間
- 1 ヵ月
- カスタム(開始日と終了日を選択します)

レポートの集約データには、現在の日付のデータや、組織からデータを蓄積し始めた日付よりも前のデータは含まれません。データは次のようにチャートに表示されます。

- 期間が 7 日間と 2 週間の場合、各データポイントが 1 日分のデータになります。たとえば、7 日間を選択すると、過去 7 日分のデータが表示されますが、今日のデータは表示されません。
- 期間が 1 ヵ月の場合、各データポイントは月曜から日曜までの 1 週間分のデータになり、月曜日で始まる週がその月の最初の週になります。つまり、曜日と当月の日数によっては、最初の週または最後の週が 7 日未満のデータになる可能性があります。
- カスタムの場合、1 日から 2 週間までの期間を選択すると、各データポイントは 1 日分のデータ。2 週間を超える期間を選択すると、各データポイントは月曜から日曜までの 1 週間分のデータになります。開始日を組織でレポートデータの蓄積が始まった日付よりも前の日付に設定すると、各チャートの最上部に「…以降(Since…)」と表示され、チャートのデータの最も早い日付が示されます。タブやページから離れてもリセットされず、ログアウトしたときにのみリセットされるという点では、カスタム日付範囲も「固定」です。

現在のページを Adobe Acrobat(PDF)形式でダウンロードできます。詳細については、「「脅威トレンドまたはエグゼクティブ サマリー レポートをダウンロードする」 ページ 180」を参照してください。

詳細については、「「脅威トレンドレポート」 次のページ)」と「「エグゼクティブ サマリー レポート」 ページ 172」、および各レポートの個別の説明 セクション を参照してください。これらのレポートのグローバル設定を変更するには、「「組織設定」 ページ 197 セクション」の「「レポートの設定」 ページ 199」を参照してください。

脅威トレンドタブ

[脅威トレンド(Threat Trends)] タブには、時間の経過に伴う攻撃の主要な傾向を詳細に示すデータビューが含まれています。次の項目が表示されます。

- メッセージ

  このグラフには、1 日あたりの合計メッセージ数、スパムやグレイメール、攻撃、ポリシーに一致したメッセージなど、さまざまな重要な数値が時系列で表示されます。

- 攻撃

  このグラフは、高度なフィッシング防御が検出した攻撃数を示しています。

- 上位のポリシー

  このグラフは、トリガーされた上位 5 つのポリシーを示しています。

「「脅威トレンドレポート」 下」を参照してください。

エグゼクティブサマリータブ

[エグゼクティブサマリー(Executive Summary)] タブには、高度なフィッシング防御を使用して従業員を保護することの累積的な影響と価値を詳述するデータビューが含まれています。これは次の質問に答えます。

- 検出された攻撃数

  このグラフは、高度なフィッシング防御が検出した攻撃数を示しています。(1 つのメッセージに複数の攻撃ベクトルが含まれている可能性があることに注意してください)

- Cisco 高度なフィッシング防御 の導入による節約量

  このグラフは、フィッシングやその他の悪意のある攻撃に対する高度なフィッシング防御の保護によって組織が節約した金額を算出します。

- ピアと比較した場合の攻撃および保護の程度

  この 2 つのグラフパネルは、攻撃数と高度なフィッシング防御による保護の程度をピア組織と比較して示しています。

「「エグゼクティブ サマリー レポート」 ページ 172」を参照してください。

[脅威トレンド(Threat Trends)] タブと [エグゼクティブサマリー(Executive Summary)] タブのレポートには、集約データが表示されます。集約データは、1 日に 1 回、UTC の午前 0 時に更新されます。

脅威トレンドレポート

脅威トレンドレポートは、Cisco 高度なフィッシング防御 のホームページ([分析(Analyze)] > [ダッシュボード(Dashboard)]) の [脅威トレンド(Threat Trends)] タブにダッシュボード形式で表示される一連のレポートです。このレポートは、高度なフィッシング防御によって生成された主要なデータを要約し、確認しやすいチャートでそのデータを示します。

脅威トレンドに関するレポートには次のものがあります。

- [メッセージ(Messages)]:組織が直面した脅威と攻撃を示します。(「「メッセージレポート」 見開きページ」を参照してください)
- [攻撃(Attacks)]:組織が直面している攻撃のタイプを示します。(このグラフのデータは、グラフの上部に攻撃の総数がないことを除けば、[エグゼクティブサマリー(Executive Summary)] タブの [検出された攻撃数(How many attacks were found?)] のレポートのデータと同じです。「「検出された攻撃数のレポート」 ページ 173」を参照してください)

- [上位5つのポリシー(Top 5 Policies)]:どのポリシーが最もトリガーされたかを示します。(「「上位ポリシーレポート」 次のページ)」を参照してください)

このページのレポートビューは、単なる累積数ではなく、時間の経過に伴う主要な傾向を確認できるように設計されています。

一部のレポートでは、データセットをカスタマイズできます。レポートで使用されるデータの詳細とレポートの設定方法については、各レポートの セクション を参照してください。

メッセージレポート

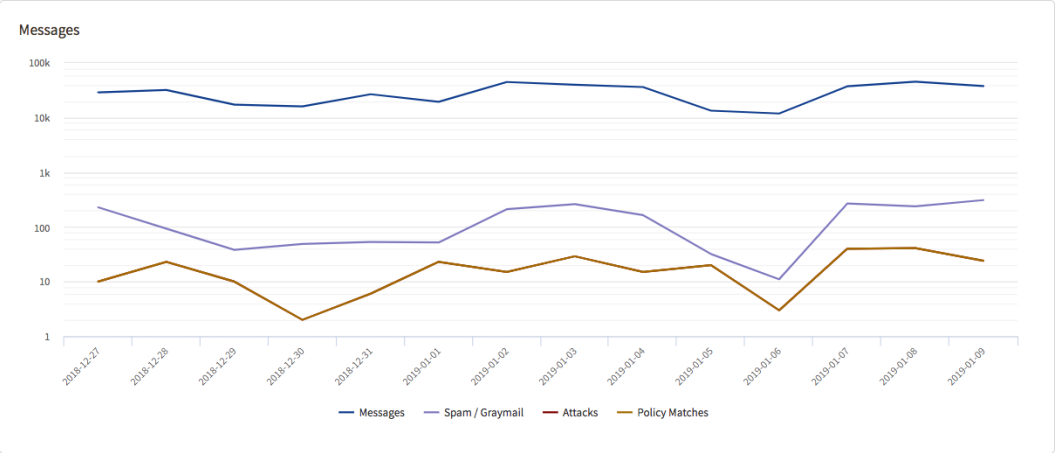
メッセージレポートには次の情報が表示されます。

- 高度なフィッシング防御が受信したメッセージの数
- 以下のメッセージの数
    - スパムまたはグレイメール
    - あらゆるタイプの攻撃として識別されたもの
    - 任意のポリシーに一致する攻撃

グラフは折れ線グラフ形式です。単一の期間(日または週)を表す線上の任意のポイントにカーソルを合わせると、その期間のデータが表示されます。

7 日または 2 週間のデータを表示すると、各ポイントは 1 日のデータを表します。1 ヵ月のデータを確認する場合は、各ポイントは 1 週間のデータを表します。

凡例の項目もトグルになっています。凡例の項目をクリックして、レポートに含めたり、レポートから除外したりできます。



2 週間のメッセージを示すレポートのサンプル。

他のレポートとは異なり、このグラフの Y 軸は対数になっています。

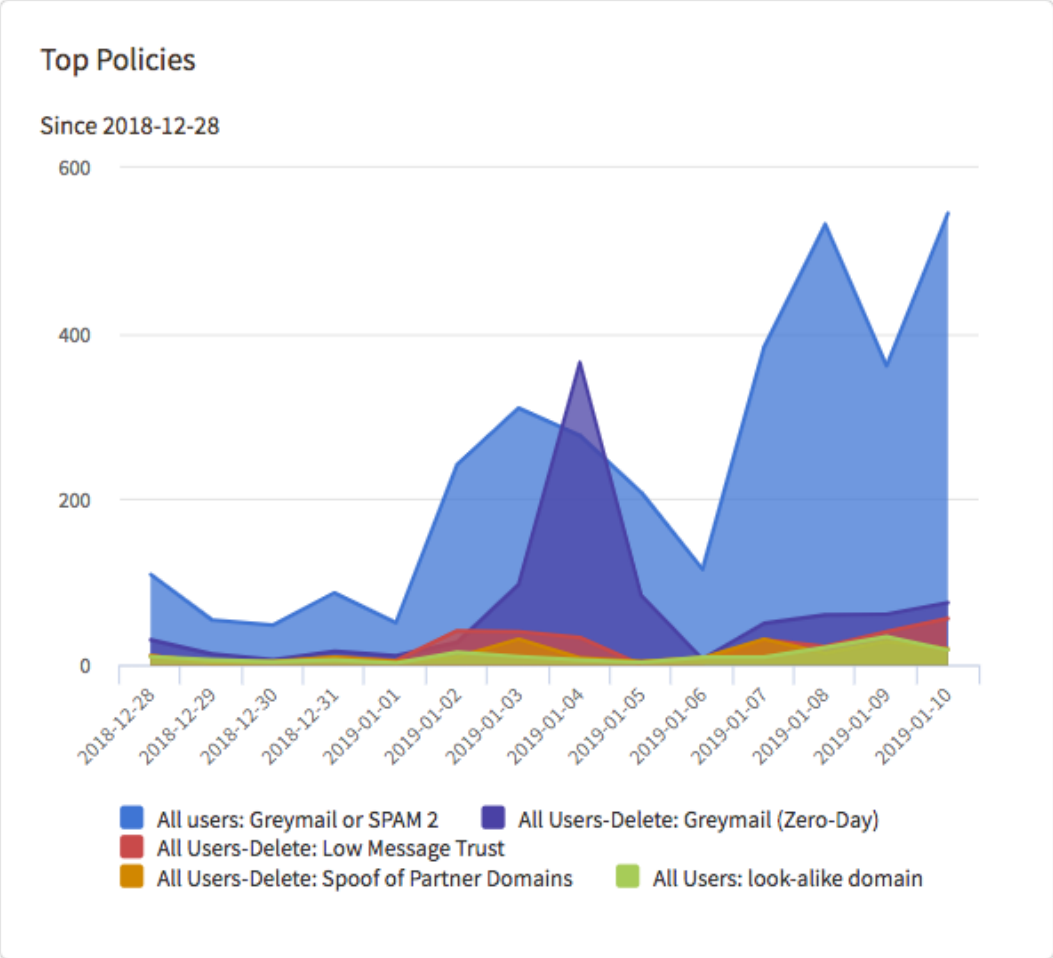
受信する攻撃に一致するようにポリシーが適切に調整されている場合(「「ポリシー」 ページ 153 」を参照してください)、[攻撃(Attacks)] と [ポリシー一致(Policy Matches)] の行は非常に近いか、重複している必要があります。(この例では重複しています。つまり、少なくとも 1 つのポリシーが受信したすべての攻撃に一致しています。このため、3 本の線しか表示されません)

攻撃レポート

攻撃タイプのレポートには、グラフの上部に合計数がないことを除けば [エグゼクティブサマリー(Executive Summary)] タブの [検出された攻撃数(How many attacks were found?)] のレポートと同じデータと双方向性が含まれています。このレポートに含まれるデータの詳細と、レポートに表示する内容をカスタマイズする方法については、「「検出された攻撃数のレポート」見開きページ」を参照してください。

上位ポリシーレポート

このレポートには、期間中に最も多くのメッセージに一致した 5 つのポリシーが表示されます。具体的には、期間(7 日、2 週間、または 1 ヵ月)を選択すると、高度なフィッシング防御はその期間中により多くのメッセージに一致した 5 つのポリシーを調べ、各ポリシーの増分のプロットを作成します(7 日間および 2 週間ビューの場合は 1 日の増分、1 ヵ月ビューの場合は 1 週間の増分)。



2 週間のポリシー一致を示すレポートのサンプル。

エグゼクティブ サマリー レポート

エグゼクティブ サマリー レポートは、Cisco 高度なフィッシング防御 のホームページ([分析(Analyze)] > [ダッシュボード(Dashboard)])の [エグゼクティブサマリー(Executive Summary)] タブにダッシュボード形式で表示される一連のレポートです。このレポートは、高度なフィッシング防御によって生成された主要なデータを要約し、確認しやすいチャートでそのデータを示します。

エグゼクティブ サマリー ページのレポートは、以下について答えてくれます。

- 検出された攻撃数（「「検出された攻撃数のレポート」 下」を参照してください）
- Cisco 高度なフィッシング防御 の導入による節約量（「「高度なフィッシング防御 の導入による節約量のレポート」 次のページ）」を参照してください）
- ピアと比較した場合の攻撃および保護の程度（「「ピアと比較した場合の攻撃/保護の程度レポート」 ページ 177」を参照してください）

一部のレポートでは、データセットをカスタマイズできます。レポートで使用されるデータの詳細とレポートの設定方法については、各レポートの セクション を参照してください。

検出された攻撃数のレポート

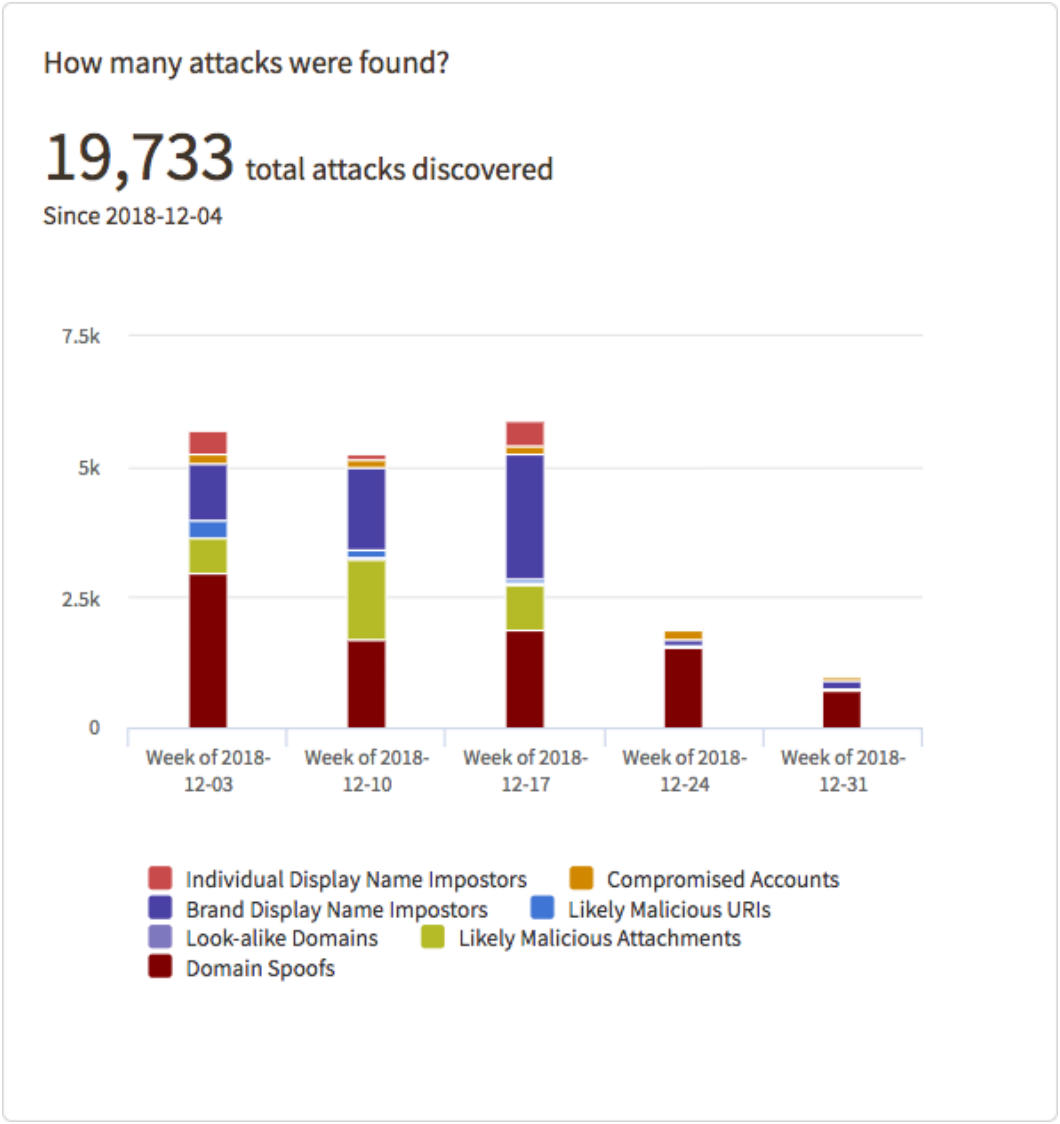
このレポートには、高度なフィッシング防御が検出した攻撃数、攻撃の合計数と攻撃タイプ別の攻撃数の両方が棒グラフ形式で表示されます。バー内の特定の攻撃タイプを表すセグメントにカーソルを合わせると、そのタイプの攻撃数が表示されます。

上部の数字は、タイトルの質問に対する回答になっていて、表示されている期間に検出された攻撃の総数を示しています。これは常に、すべての攻撃タイプの累積数です。

7 日または 2 週間のデータを表示すると、各バーは 1 日のデータを表します。1 ヵ月のデータを確認する場合は、各バーは 1 週間のデータを表します。

攻撃タイプの凡例もトグルになっています。攻撃タイプをクリックして、棒グラフに含めたり除外したりできます。

棒グラフに表示される攻撃の種類を変更しても、上部に表示される攻撃の総数は変わりません。



1ヵ月の攻撃を示すレポートのサンプル。

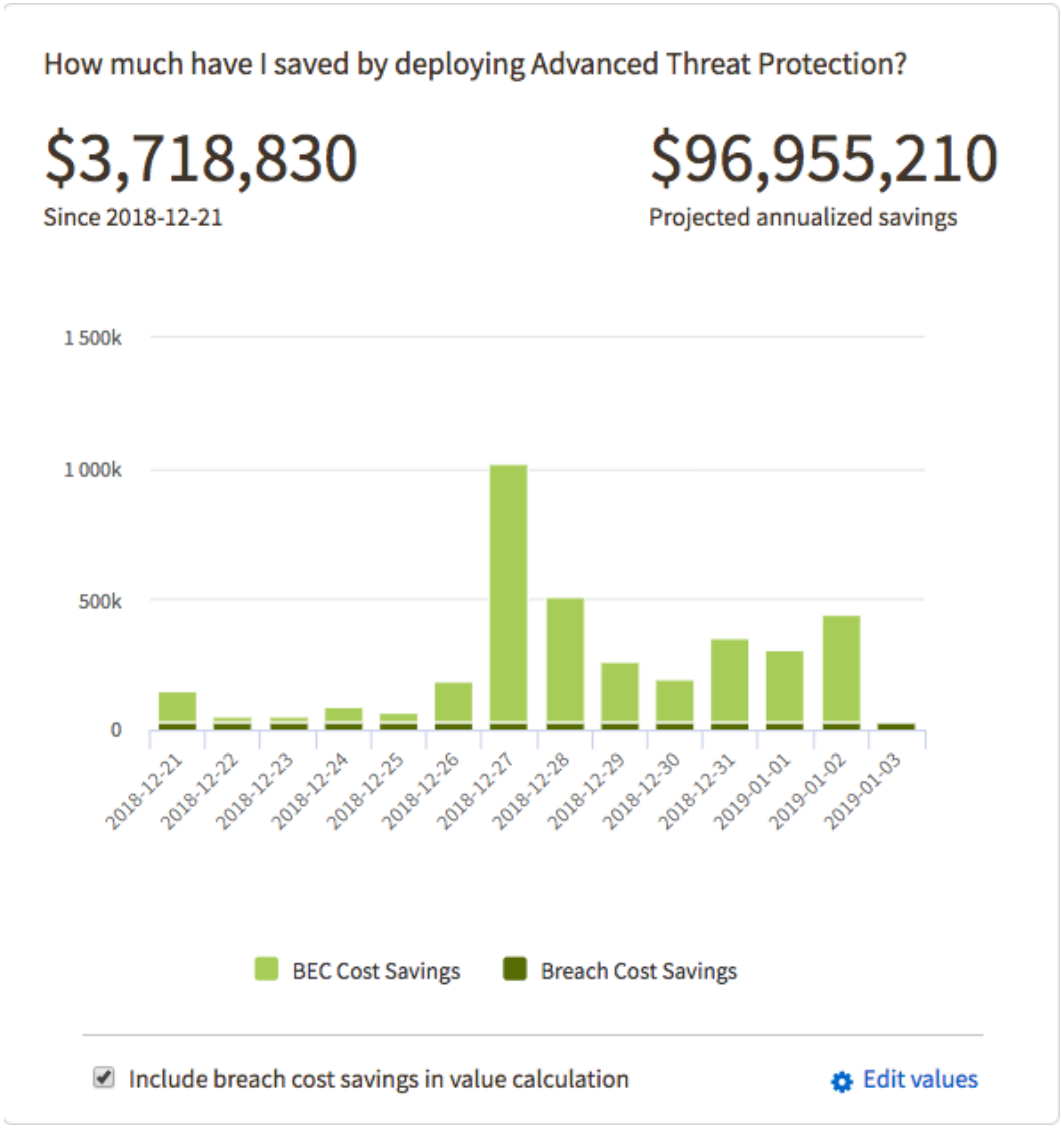
各バーは、期間ごとの攻撃の合計数を示します（7 日および 2 週間のビューでは 1 日あたり、1ヵ月のビューでは 1 日あたりの平均）。グラフのセグメントは、攻撃タイプごとの攻撃数に対応しています。セグメントにカーソルを合わせると、セグメントによって表されるタイプの攻撃数が表示されます。

高度なフィッシング防御 の導入による節約量のレポート

このレポートは、高度なフィッシング防御によってどれだけの金額が節約できたかを示します。リアルタイムポリシーとオンデマンドポリシーの両方によって削除または移動されたビジネス用の電子メール侵害の脅威メッセージ数を追跡し、それらのメッセージが組織の受信トレイに入ることを許可された場合や受信トレイに保持された場合に組織にかかるコストをグラフ化します。

必要に応じて、電子メール侵害を阻止したことで節約された金額を含めることもできます。

このレポートで使用される値を設定する方法の詳細については、「「高度なフィッシング防御の導入による節約量のレポートを設定する」見開きページ」を参照してください。



2 週間の節約量を示すレポートのサンプル。

上部の数字は、タイトルの質問への答えになっています。最初の数字は、表示されている期間中の入力した値に基づく節約量です。2 番目の数値は、最初の数値から推定された年換算の数値です。

高度なフィッシング防御の導入による節約量のレポートを設定する

高度なフィッシング防御の導入による節約量のレポートは、2 つの方法で設定できます。次の操作が可能です。

- レポートの計算に侵害によるコストを含める
- 脅威によるコストを調整する

このレポートを設定できるのは、組織管理者ロールを持つユーザーのみです。詳細については、「「ユーザーロール」 ページ 209」を参照してください。

比較に使用する値を変更する

レポートで使用されているデフォルト値は、Cisco の広範な脅威調査のデータセットに基づいています。Cisco のデータセットと異なるデータがある場合は、別の値を入力して、より具体的で組織に関連する計算を作成できます。

1. [分析(Analyze)] > [ダッシュボード(Dashboard)] に移動します。
2. [エグゼクティブサマリー(Executive Summary)] タブをクリックします。
3. [高度なフィッシング防御の導入による節約量(How much have I saved by deploying Advanced Phishing Protection?)] のレポートの下部で、[値の編集(Edit values)] をクリックします。
4. 必要な値を入力します。各レポートの値の詳細については、以下の説明を参照してください。
5. [値の保存(Save Values)] をクリックします。

入力した値でレポートが更新されます。

ダイアログボックスの下部にある [すべてを既定値にリセット(Reset all to default values)] をクリックして、行った変更を元に戻し、Cisco のデフォルトに置き換えます。

変更はユーザーごとではなく、これらのレポートを表示する組織内のすべてのユーザーに適用されます。

高度なフィッシング防御の導入による節約量のレポートの値

デフォルトより低い値を入力すると、警告インジケータが表示されます。一般に、デフォルト値を下回る値、つまり広範囲にわたる世界規模の調査に基づいた値は、実際のデータを反映していない結果をもたらす可能性があります。

通貨

[ドル(Dollar)] または [ユーロ(Euro)] を選択できます。

侵害のコストの削減

1 つの侵害によって組織にもたらされるコストの値を具体的に定義できます。

デフォルト値は、自身の地域と業界に基づいた平均値であり、広範な調査に基づいた値です。

- [侵害が成功した場合の平均コスト(Average cost of a successful breach)]: 多くの人は、電子メール侵害の総コストを認識していません。デフォルト値は高く見えるかもしれませんが、実際のデータに基づいたものです。
- [電子メールを介して開始されたデータ侵害の割合(Percentage of data breaches initiated through email)]: データ侵害で圧倒的に多いのは、何らかの電子メール攻撃によるものです。
- [毎年の新しい電子メール侵害の確率(Probability of a new email breach annually)]: このデフォルトは、実際の電子メールベースのデータ侵害の何年にもわたるデータ分析の累積結果を反映したものです。

BEC のコストの削減

ここに示されている攻撃の種類は、Cisco 高度なフィッシング防御 が識別しているものです。組織内の各攻撃タイプの実際の平均値がわかっている場合、各攻撃タイプに値を入力することでこのレポートの精度が大幅に向上します。通常、攻撃が成功した場合の平均コストは、推定されるよりも高くなります。これは攻撃によって直接的なコストと付随するコストの両方が発生するからです。

たとえば、電子メールシステムが、いかなる種類の添付ファイルも許可しないように設定されている場合があります。システムでは発生しないと確信できるため、しきい値を 0 に設定できます。

成功確率は、高度なフィッシング防御なしでの確率であることに注意してください。

[高度な電子メールの脅威におけるBEC攻撃の割合（What percentage of Advanced Email Threats are BEC attacks）] 設定に、電子メール攻撃の合計における BEC 攻撃の割合を入力します。この計算に使用される合計にスパムまたはグレイメールを含めないでください。

ピアと比較した場合の攻撃/保護の程度レポート

このレポートは、どの程度攻撃されているか、Cisco 高度なフィッシング防御 によって組織がどの程度保護されているかの両方をピア組織と比較して示しています。十分なピア組織がない場合、レポートはより広いデータセットにフォールバックします。「ピア」階層は次のとおりです。

- 地域、業界、および組織内のメールボックス
- 業界と組織内のメールボックス
- 組織内のメールボックス
- Cisco データセット全体におけるすべての組織の平均

「地域」は、北米または EMEA（ヨーロッパ、中東、アフリカ）などの定義された地理的エリアです。

「産業」は製造業や金融などのカテゴリです。

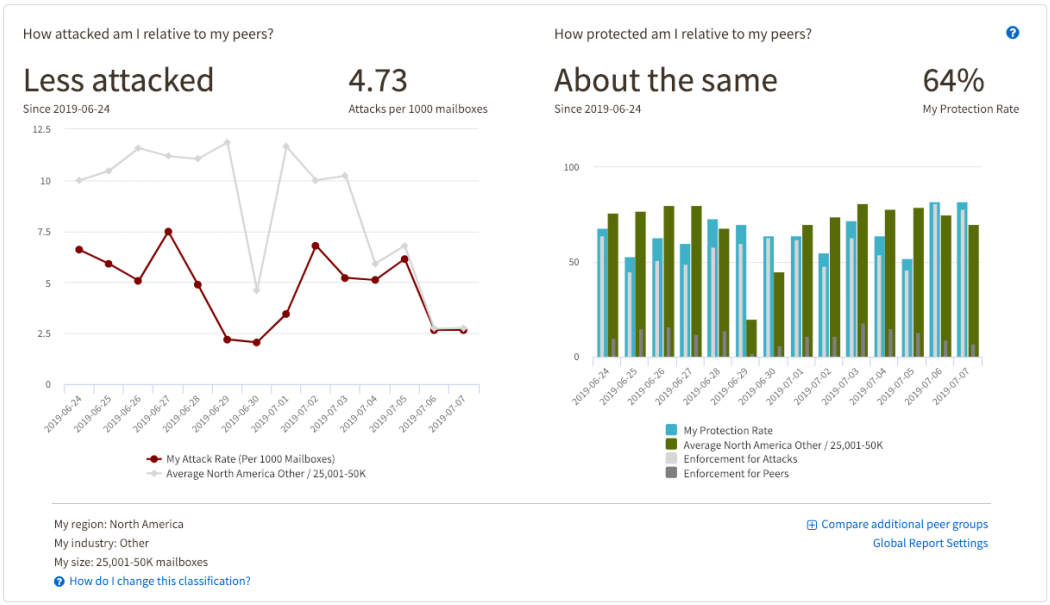
「メールボックス」は、一連の階層によって定義されます。たとえば、組織に 10,000 個のメールボックスがある場合、比較するのは 10,000 個のメールボックスを含む階層内の他の組織に限定されます。

階層の各レベルについて、そのレベルに比較に使用できる組織が 5 つ以上存在しない場合、次のレベルが使用されます。たとえば、ある南米の航空機部品メーカーがあったとして、同じ業界の組織は南米に 2 社しかないとします。この場合、最初のレベルは使用されません。しかし、同じ業界の組織が世界中に 5 つ以上あり、ほぼ同じサイズのものが十分にある場合（「サイズ」は同じ量のメールボックスとして定義されます）、このレポートには 2 番目のレベルが使用されます。

レポートの下部に、組織に定義され、現在のレポートに使用されている地域、業界、およびメールボックスのサイズが表示されます。[追加比較（Compare additional）] をクリックして、組織と比較するファセットを変更します。詳細については、「「追加のピアグループと比較する」 ページ 179」を参照してください。

レポート自体は、高度なフィッシング防御を使用した場合と高度なフィッシング防御を使用していない場合の日々の値をグラフ化します。エグゼクティブ ダッシュボードのすべてのレポートと同様に、過去 7 日間（デフォルト）、過去 2 週間、または過去 1 ヵ月の期間を選択できます。

このレポートの設定方法の詳細については、「「追加のピアグループと比較する」 ページ 179」を参照してください。



2 週間の比較データを示すレポートのサンプル。

[ピアと比較した場合の攻撃の程度(How attacked am I relative to my peers)] の折れ線グラフでは、1 本の線は、期間におけるメールボックス 1,000 個あたりの攻撃レートを表しています(7 日および 2 週間のビューでは 1 日あたり、1 ヵ月のビューでは 1 日あたりの平均)。もう 1 つの行は、ピア(地域、業界、メールボックスの数)の平均攻撃レートです。比較のためにピアグループを追加した場合、3 行目にそのグループの攻撃レートが表示されます。

上部のサマリーは、グラフのタイトルの質問に回答し、表示されている期間の 1 日あたりの平均攻撃レート(メールボックス 1,000 個あたり)を数値化します。答えは次のいずれかになります。

- [多く攻撃されている(More attacked)]:表示されている期間のピアの平均レートよりも 10% を超えて高い
- [やや多く攻撃されている(Slightly more attacked)]:表示されている期間のピアの平均レートよりも 2% から 10% 高い
- [ほぼ同じ(About the same)]:表示されている期間のピアの平均レートとの差が 2% 以内
- [やや攻撃されていない(Slightly less attacked)]:表示されている期間のピアの平均レートよりも 10% から 2% 低い
- [あまり攻撃されていない(Much less attacked)]:表示されている期間のピアの平均レートの 10% 未満

[ピアと比較した場合の保護の程度(How protected am I relative to my peers)] の棒グラフでは、1 本の棒が期間における保護レートを示しています(7 日および 2 週間のビューでは 1 日あたり、1 ヵ月のビューでは 1 日あたりの平均)。もう 1 つのバーは、ピアの平均保護レート(地域、業界、メールボックスの数)を示しています。比較のためにピアグループを追加した場合、3 番目のバーにそのグループの攻撃レートが表示されます。ポリシーの適用を有効にしている場合、内部のバーに適用と保護のレートが表示されます。

算出方法は以下のとおりです。

- 保護レートについては、いずれかのポリシーに一致する攻撃メッセージの数を、攻撃メッセージの総数を 100 で割った値で割ったものです。
- 適用レートについては、既存のポリシーによって適用された攻撃メッセージの数を、攻撃メッセージの総数を 100 で割った値で割ったものです。

これらは異なる場合があります。高度なフィッシング防御で設定したポリシーには、メッセージが一致してもメッセージを適用しない、つまり、メッセージを受信トレイから移動または削除しないものがあるためです。

上部のサマリーは、グラフのタイトルの質問に回答し、表示されている期間の 1 日あたりの平均保護レート（メールボックス 1,000 個あたり）を数値化します。答えは次のいずれかになります。

- [多く保護されている（More protected）]：表示されている期間のピアの平均レートよりも 10% を超えて高い
- [やや多く保護されている（Slightly more protected）]：表示されている期間のピアの平均レートよりも 2% から 10% 高い
- [ほぼ同じ（About the same）]：表示されている期間のピアの平均レートとの差が 2% 以内
- [やや保護されていない（Slightly less protected）]：表示されている期間のピアの平均レートよりも 10% から 2% 低い
- [あまり保護されていない（Much less protected）]：表示されている期間のピアの平均レートの 10% 未満

数値が高いほど、直面する攻撃から保護するように設定されたポリシーがあることを意味します。

追加のピアグループと比較する

[ピアと比較した場合の攻撃/保護の程度（How attacked/protected am I relative to my peers）] のレポートで比較に使用する企業は、あなたの地域、あなたの業界の企業であり、メールボックスのサイズが類似した企業です。地域、業界、またはメールボックスのサイズを追加して比較することもできます。

1. [分析（Analyze）] > [ダッシュボード（Dashboard）] に移動します。
2. [エグゼクティブサマリー（Executive Summary）] タブをクリックします。
3. [ピアと比較した場合の攻撃/保護の程度（How attacked/protected am I relative to my peers）] レポートの下部で、[追加のピアグループの比較（Compare additional peer groups）] をクリックします。
4. 以下を選択します。
    - [地域（Region）] は、次の中から選択できます。
        - すべての Cisco 顧客
        - 北米
        - EMEA（ヨーロッパ、中東、アフリカ）
        - APAC（アジア太平洋）
    - [業種（Industry）] は、次の中から選択できます。
        - すべての Cisco 顧客
        - 金融
        - 政府/自治体
        - 医療
        - その他
        - 小売
        - テクノロジー
    - [メールボックスサイズ（(Mailbox) Size）] は、次の中から選択できます。
        - すべての Cisco 顧客
        - 0 ～ 250

- 250 ～ 1,000
- 1,001～ 3,000
- 3,001 ～ 5,000
- 5,001 ～ 10,000
- 10,001 ～ 25,000
- 25,001 ～ 50,000
- 50,001 ～ 100,000
- 100,001 以上

5. [更新（Update）] をクリックします。

レポートは、新しい比較のファセットを使用して更新されます。選択するのに十分なデータソースがなく、レポートが次の階層に拡張された場合（詳細については、「「ピアと比較した場合の攻撃/保護の程度レポート」 ページ 177」を参照してください）、レポートは変更されない可能性があることに注意してください。凡例には選択が反映されますが、レポートでは、有用な比較を行うのに十分なデータを含む最初の階層が使用されます。

このレポートに使用されるピアのセットを追加すると、変更は「固定」されます。つまり、ページから離れて戻ってきても、データには追加のピアのセットが引き続き表示されます。

脅威トレンドまたはエグゼクティブ サマリー レポートをダウンロードする

脅威トレンドやエグゼクティブサマリーの現在のビューをダウンロードできます。これにはすべてのグラフが Adobe Acrobat（PDF）ファイルとして含まれています。

1. [分析（Analyze）] > [ダッシュボード（Dashboard）] に移動します。
2. [脅威トレンド（Threat Trends）] または [エグゼクティブサマリー（Executive Summary）] タブをクリックします。
3. レポートの期間を設定します。エグゼクティブサマリーのレポートを表示している場合は、[高度なフィッシング防御の導入による節約量（How much have I saved by deploying Advanced Phishing Protection?）] および [ピアと比較した場合の攻撃/保護の程度（How attacked/protected am I relative to my peers）] のグラフでデータを設定することもできます。詳細については、「「高度なフィッシング防御の導入による節約量のレポートを設定する」 ページ 175」および「「追加のピアグループと比較する」（前のページ）」を参照してください。
4. [PDFのダウンロード（Download PDF）] をクリックします。

現在のビューの PDF が作成され、ブラウザのデフォルトのダウンロード場所に自動的にダウンロードされます。

添付ファイルと URI の分析

Cisco 高度なフィッシング防御 では、アイデンティティ インテリジェンスに加え、メッセージの添付ファイルとメッセージ本文の URI を分析し、その分析の結果を使用して、メッセージ全体の信頼性を判別することができます。

高度なフィッシング防御で可能な、悪意のあるコンテンツの分析には 2 つのレベルがあります。

- 検索とポリシーで使用できる名前やファイル拡張子などの添付ファイル情報の基本的なコレクション。
- 得点付けとメッセージの分類を強化するための、悪意のある目的の兆候を調べる添付ファイルのスキャン。

URI 分析では次のことを行います。

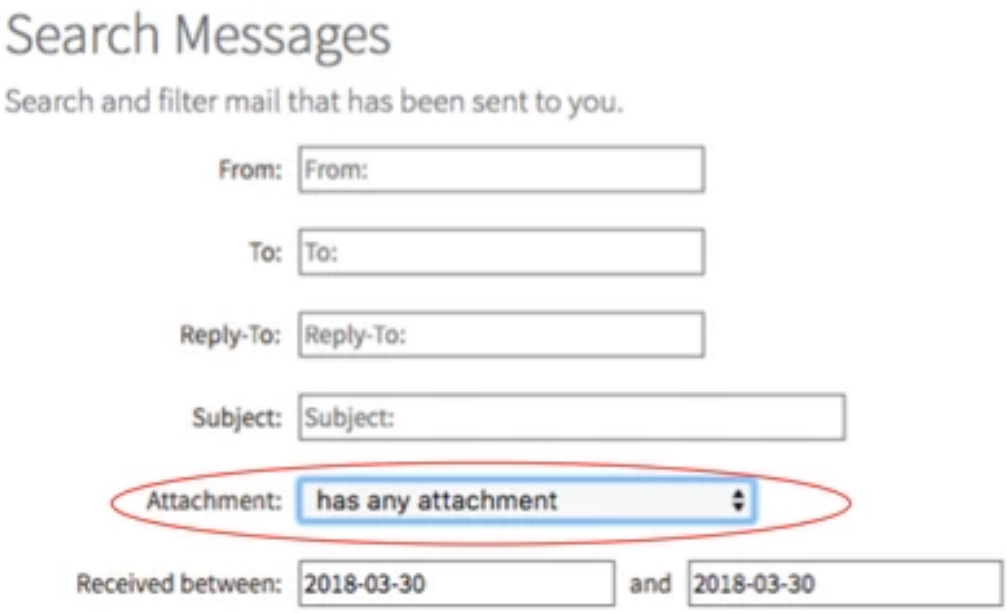
- 以下から URI を抽出します。
  - ヘッドセクションからのベース URI を含む、メッセージの text/HTML MIME 部分。
  - メッセージに添付された Microsoft Office および Adobe Acrobat ドキュメント。
- http スキームと https スキームの両方を解析します。
- メッセージの詳細ビューに URI が表示されますが、それらの URI はクリックできません。
- 一般的な URI 短縮サービスを使用する URI を識別し、それらの URI 短縮サービスの背後にある Web サイトを特定します。

添付ファイルの分析の使用

添付ファイルの分析を有効にすると、添付ファイルの分析の結果をさまざまな方法で使用できます。

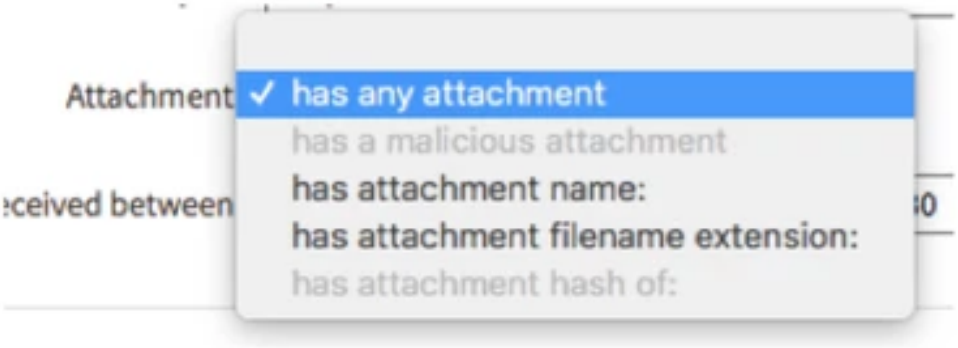
検索およびポリシーでの添付ファイル分析結果の使用

[分析（Analyze）] > [メッセージの検索（Search Messages）] ページに新しいオプションが表示されます。ポリシーを作成または編集する場合の [管理（Manage）] > [ポリシー（Policies）] でも同じフィールドが表示されます。



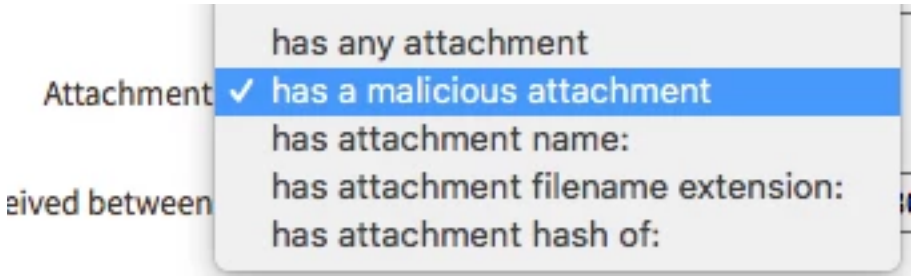
添付ファイル付きメッセージの検索

添付ファイルの名前の情報のみ収集する場合は、それを検索してポリシーを設定するために、次のオプションを利用できます。



添付ファイルの検索：限定された選択肢

添付ファイルのスキャンを有効にした後、検索とポリシーのすべてのオプションが利用可能になります。

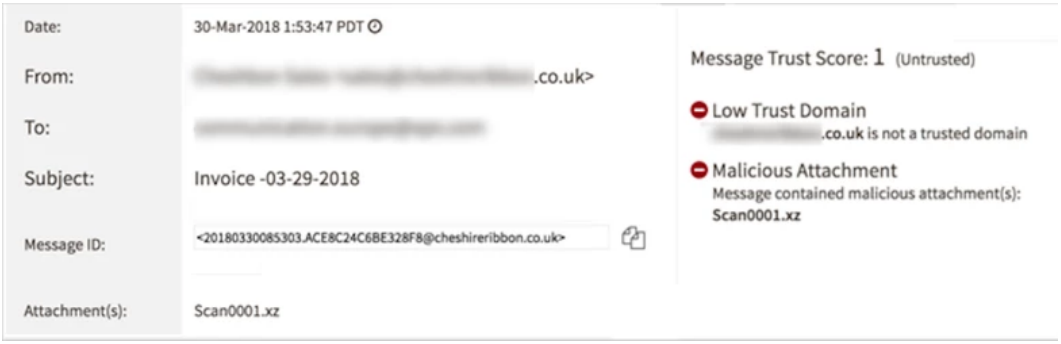


添付ファイルの検索：添付ファイルのスキャンが有効

添付ファイル名の検索でのワイルドカード照合または部分的なエントリはサポートされていません。たとえば、「attachment name is 'foo.*.bar」は「foo.banana.bar」と一致しません。

添付ファイルのスキャン結果

添付ファイルのスキャンが有効な場合、高度なフィッシング防御はスコアリングモデルとメッセージの分類モデルでスキャン結果を使用します。たとえば、[メッセージの詳細（Message Details）] に以下のような [悪意のある添付ファイル（Malicious Attachment）] などのメッセージ分類が表示されます（注：まもなく、検出された悪意のあるコンポーネントの詳細を表示するように、悪意のある添付ファイルの分類を拡張できるようにもする予定です）。



[メッセージの詳細（message details）] ペインでの添付ファイルのスキャン結果

添付ファイルのスキャンの詳細

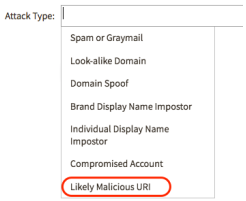
高度なフィッシング防御の添付ファイルのスキャンでは、ドキュメントベースの添付ファイルに潜在する悪意のある動作を識別することに重点が置かれています。それは、サンド ボックスではなく、悪意のあるコードを強制的に実行させようとはしません。

高度なフィッシング防御は、次の種類のファイルの解凍、難読化解除、および静的分析を実行します。

- アーカイブ ファイル形式（zip/rar/tar/{gz/gzip/tgz}/{bz2/bzip2/tbz2/tbz}/cab）
- Office ファイル、PDF、MHTML、電子メール ファイル、画像ファイル、フラット データ ファイル、RTF
- フラッシュ、ビデオ形式、Javascript、VBA

URI 分析の使用

URI 分析は、メッセージ検索とポリシー作成の両方で使用できます。どちらの場合も、[攻撃タイプ（Attack Type）]ドロップダウンリストから [悪意のある可能性のあるURI（Likely Malicious URI）] を選択して、検索またはポリシーフィルタに含めることができます。



これを選択すると、悪意のある可能性のある URI を含むメッセージが検索またはポリシーに含まれます。

添付ファイルと URI の分析を有効にする

高度なフィッシング防御の添付ファイルと URI の分析は、実行する分析のレベルに応じた複数のステップから成るプロセスです。

ここで説明する添付ファイルと URI の分析を有効にするプロセスは、Cisco ホステッド型センサーを使用するすべての顧客、および 18.05.21222056 リリース（2018 年 5 月）以降がインストールされたオンプレミスセンサーを使用し、そのリリースのホストシステムの仕様を満たす顧客に適用されます。

18.05.21222056 リリースより前の独自のオンプレミスセンサーをホストしている顧客は、ホストのアップグレードが必要になる可能性があり、添付ファイルのスキャンと URI のスキャンのスイッチを有効にするよう Cisco サポートにリクエストする必要があります。これが完了したら、以下のプロセスを続行して、添付ファイルと URI の分析を有効にすることができます。

基本的な添付ファイル情報の収集

添付ファイルと URI のスキャンを許可するには、組織レベルの設定を有効にして、高度なフィッシング防御がこの情報を収集できるようにする必要があります。この設定はデフォルトで有効になっています。無効になっている場合、有効にするには次の手順を実行します。

1. [管理（Manage）] > [組織（Organization）] に移動します。
2. [メッセージコンポーネント（Message Components）] タブを選択します。
3. 組織で有効にするには、[メッセージコンポーネントを処理する（Process message contents）] チェックボックスをオンにします。
4. [保存（Save）]をクリックします。

組織が添付ファイルとURIのスキャンを許可すると、この機能がセンサーレベルで、そしてセンサー単位で有効になります。

この設定を有効にしたが、センサーの添付ファイルのスキャンは有効にしていない場合、高度なフィッシング防御は検索とポリシーで使用できる、名前やファイル拡張子などの添付ファイルの情報について基本的な収集を実行します。

添付ファイルのスキャン

悪意のある目的に関する添付ファイルのコンテンツのスキャンは、センサー単位で有効にする必要があります。自身のセンサー環境を管理している場合は、センサーのサブセットでのみ添付ファイルをスキャンし、添付ファイル付きの電子メールをそれらの特定のセンサーにルーティングするように選択できます。センサーがCiscoによってホストされている場合（推奨設定）は、すべてのセンサーでスキャンを有効にする必要があります。

添付ファイルをスキャンするには、センサー ホスト システム VM またはマシンにアップグレードする必要があります。センサーホストシステムの仕様については、「「センサーの前提条件」 ページ 24」を参照してください。

最初に上記の手順を実行して、添付ファイル名コレクションの組織レベル ポリシーを設定する必要があります。

1. [管理（Manage）] > [センサー（Sensors）] に移動します。
2. [設定（Configuration）] セクションまで下方向にスクロールします。
3. [添付ファイルのスキャン（Attachment Scanning）] スライダを [添付ファイルをスキャンする（Scan Attachments）] に移動します。
4. [設定の保存（Save Configuration）] をクリックします。

自身の環境（Ciscoにホストされていない）で管理しているセンサーで添付ファイルのスキャンを初めて有効にすると、バックグラウンドでスキャンエンジンのコンテナがダウンロードされ、その後、センサーが再起動します。このプロセスには30分以上かかることがあります。一度に1つのセンサーでこのアクションを実行することをお勧めします。

複数のセンサーがある場合は、添付ファイルのスキャンを実行するセンサーの各タブでこれらの手順を繰り返します。

URIのスキャン

悪意のある目的に関するURIのスキャンは、センサー単位で有効にする必要があります。自身のセンサー環境を管理している場合は、センサーアプライアンスのサブセットでのみURIをスキャンし、添付ファイル付きの電子メールをそれらの特定のセンサーにルーティングするように選択できます。センサーがCiscoによってホストされている場合（推奨設定）は、すべてのセンサーでスキャンを有効にする必要があります。

高度なフィッシング防御は、メッセージに添付されたMicrosoft OfficeおよびAdobe Acrobatドキュメントの URIもスキャンできますが、これを行うには添付ファイルのスキャンも有効にする必要があります。

URIをスキャンするには、センサーホストシステムの VM またはマシンにアップグレードする必要があります。センサーホストシステムの仕様については、「「センサーの前提条件」 ページ 24」を参照してください。

最初に上記の手順を実行して、URIの収集に関する組織レベルのポリシーを設定する必要があります。

1. [管理（Manage）] > [センサー（Sensors）] に移動します。
2. [設定（Configuration）] セクションまで下方向にスクロールします。
3. [URIのスキャン（URI Scanning）] スライダを [URIをスキャンする（Scan URIs）] に移動します。
4. [設定の保存（Save Configuration）] をクリックします。

複数のセンサーがある場合は、URI のスキャンを実行するセンサーの各タブでこれらの手順を繰り返します。

送信者管理および Rapid DMARC

Cisco 高度なフィッシング防御 の [送信者（Senders）] ページでは、内部ドメインを使用して、組織にメッセージを送信していることがわかっている既知の送信者が表示されます。高度なフィッシング防御が内部ドメインの送信者からのトラフィックをどのようにモデル化しているかをすばやく把握でき、特定の送信者をワンクリックで明示的に承認または拒否することもできます。この送信者モデルの理解と、手動の調整機能によって、高度なフィッシング防御に Rapid DMARC ポリシーを安全に実装し、自身のドメインからの本物でないメッセージを拒否できます。

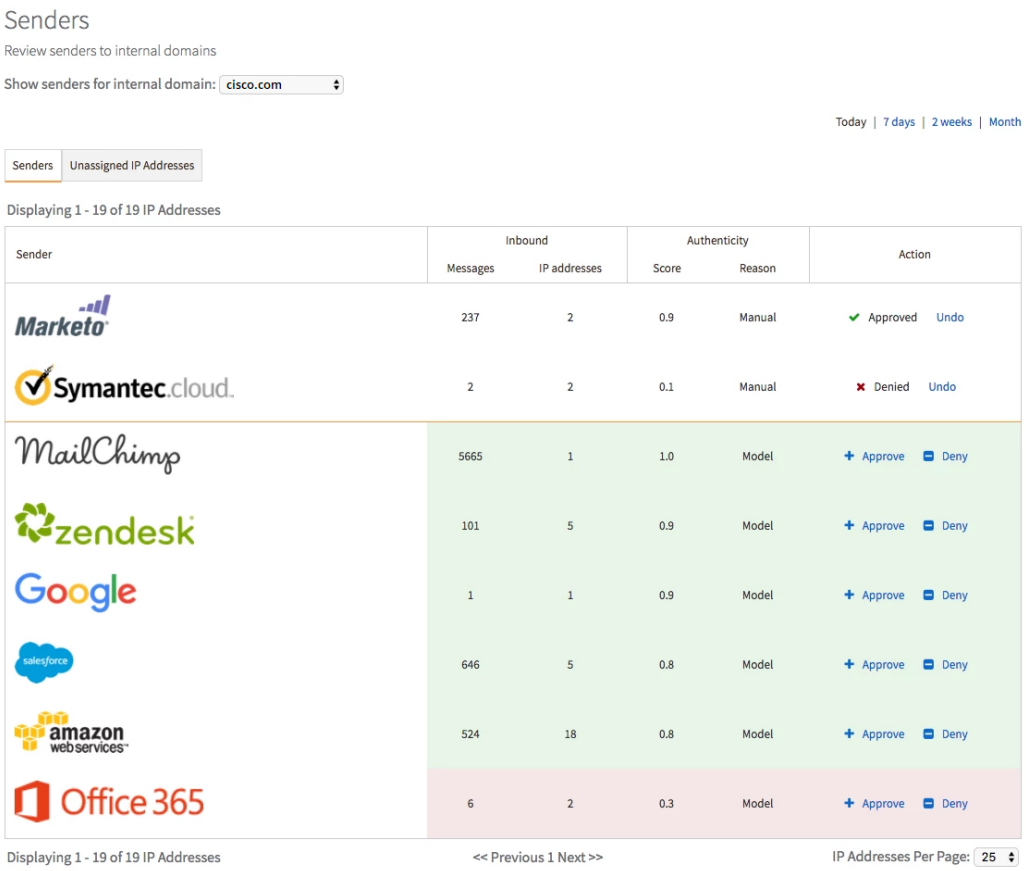
送信者を管理する

[管理（Manage）] > [送信者（Senders）] に移動すると、ドメインの [既知の送信者（Well Known Senders）] の表示を取得できます。ページは、最大ボリュームの内部ドメインにフィルタ処理され、デフォルトで今日のデータが表示されます。

表示するドメインを変更するには、ドメイン名の横にある上/下矢印をクリックします。

[分析（Analyze）] > [ドメイン（Domains）] ページで [内部（internal）] としてタグ付けしたドメインは、ここにあるドメインのリストに表示されます。

また、ページは、次の図のように、デフォルトで [送信者（Senders ）] を表示するように設定されています。既知の送信者に割り当てられていない IP アドレスを表示するのには、[未割り当てのIPアドレス（Unassigned IP Addresses）] タブをクリックします。



[送信者（Senders）] ページ

列の意味と使用方法

[送信者（Sender）]：既知の送信者の名前やロゴ。送信者をクリックすると、1 レベル ドリル ダウンし、個々 の IP のメッセージ数が表示されます。

[受信（Inbound）] の [メッセージ（Messages）]：指定された期間中に、このドメインと送信者の組み合わせから検出されたメッセージ数。

[受信（Inbound）] の [IPアドレス（IP addresses）]：指定された期間中に、このドメインと送信者の組み合わせからそれらのメッセージを送信したことが検出された IP アドレス数。

[真正性（Authenticity）] の [スコア（Score）]：この送信者とドメインの組み合わせの送信者モデリングからのグローバルな信頼性スコアの平均です。

ここに表示される真正性スコアは、全期間にわたってシステムで検出された、この送信者とドメインの組み合わせに関連付けられたすべての IP からのすべてのメッセージの平均です。そのため、特定のメッセージへドリル ダウンすると、通常、単一のメッセージの信頼性得点にばらつきがあることが予測されます。

[真正性（Authenticity）] の [理由（Reason）]：信頼性スコアを決定する方法。

[手動（Manual）] は、送信者が手動で承認または拒否されたことを意味します。平均信頼性は、送信者または IP アドレスの承認または拒否時に即座には変更されませんが、変更から数分以内に、送信者/ドメインまたは IP/ドメインの組み合わせからの新しいメッセージは、承認された場合は 1.0 の信頼性得点、拒否された場合は 0 の信頼性得点を受信し始めます。

[モデル(Model)] は、高度なフィッシング防御の送信者モデリングに基づいて、スコアが計算されたことを意味します。

[認証済み(Authenticated)] は、その送信者とドメインの組み合わせから検出されたメッセージの大半が、完全な DMARC アライメントで認証標準を満たしていることを意味します。

[アクション(Action)]:これらは送信者を承認または拒否したり、以前の承認や拒否を元に戻すために実行するアクションです。

[元に戻す(Undo)] は、高度なフィッシング防御の送信者モデリングによってモデル化された状態に送信者を戻します。いつでも、承認または拒否を元に戻すことができます。

[承認(Approve)] は、そのドメインの送信者を明示的に承認します。それ以降のその送信者からのメッセージは、高度なフィッシング防御によって確実に本物と見なされます。

[拒否(Deny)] は、そのドメインの送信者を明示的に拒否します。それ以降のその送信者からのメッセージは、高度なフィッシング防御によって確実に本物ではないと見なされます。

Rapid DMARC を使用した送信者管理

公開 DMARC ポリシーと同様に、Rapid DMARC では、ドメインからの本物でないメッセージを削除または検疫するために安全にポリシーを適用できるように、送信者を適切に認証する必要があります。

違いは、Rapid DMARC 送信者管理が高速で容易な点です。内部ドメインの送信者と IP を確認し、さらに、高度なフィッシング防御がそれらをモデル化した方法を確認するだけです。モデルに合致する場合は、多数の送信者を明示的に承認することを選択した場合でも、それ以上のアクションは必要ありません。公開 DMARC での配置アイデンティティと異なる送信者がいる場合は、Rapid DMARC についてそれを心配する必要はありません。送信者に連絡して、DNS の変更を実装する必要はありません。[送信者(Senders)] ページで [承認(Approve)] をクリックするだけで、完了します。

高度なフィッシング防御内の送信者が安全であることを確認したら、[管理(Manage)] > [ポリシー(Policies)] ページに移動して、適用する Rapid DMARC ポリシーをセットアップします。

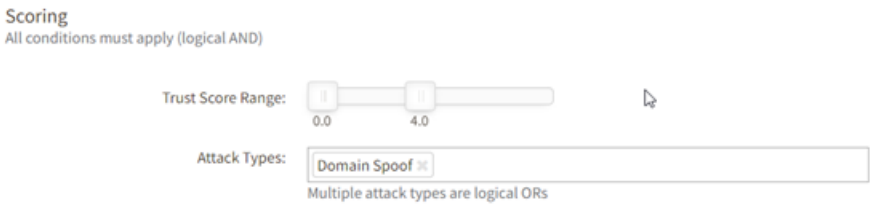
2018 年 1 月以降にオンボードされた顧客は、デフォルト Rapid DMARC ポリシーがすでに作成されています。

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. Rapid DMARC のポリシー名をクリックします。
3. ポリシー名の下で、スライダを [有効(Enable)] まで移動します。
4. [アクション(Actions)] セクションまで下にスクロールして、このポリシーの適用アクションをセットアップし、ポリシーに一致したときのアラートを有効にします。
5. [保存(Save)]をクリックします。

2018 年 1 月より前に高度なフィッシング防御でセットアップされた顧客は、Rapid DMARC ポリシーを受け取っていません。次の手順で、Rapid DMARC ポリシーを作成できます。

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [ポリシーの作成(Create Policy)] をクリックします。
3. [ポリシー名(Policy Name)] に「Rapid DMARC」と入力します。
4. [ドメインタグ(Domain Tags)] まで下にスクロールして、空のボックスをクリックします。使用可能なドメインタグのリストから [内部(internal)] を選択します。

5. [スコアリング(Scoring)]まで下にスクロールします。
6. [信頼性スコアの範囲(Trust Score Range)]の上限を 4 に移動します。次のようになります。



7. [攻撃タイプ(Attack Type)]で、空のボックスをクリックし、利用可能な攻撃タイプのリストから[ドメインスプーフィング(Domain Spoof)]を選択します。
8. [保存(Save)]をクリックします。

アドレスグループ

アドレスグループは、単に 1 つ以上(最大 1,000)の電子メールアドレスの名前付きグループのことです。アドレスグループはポリシーでよく使用され、次の理由で使用されることがあります。

- 一連のユーザーのスプーフィングを特定するため。ポリシーの[差出人(From)]フィールドでアドレスグループを指定すると、そのグループにおけるメンバーの表示名のスプーフィングについてポリシーのマッチングが行われます。デフォルトでは、表示名のスプーフィングとして特定されたメッセージの信頼スコアは低くなります。アドレスグループでポリシーマッチングを実行する場合でも信頼スコアに影響を与えないようにするには、[このグループを使用してメッセージスコアリングに影響を与える(Use this group to affect message scoring)]ポリシー設定をオフにします。[差出人(From)]フィールドでのアドレスグループのマッチングの具体例を以下に示します。
- メッセージ受信者のグループに基づいてポリシーをフィルタリングするため。ポリシーの[宛先(To)]フィールドでアドレスグループを指定すると、メッセージの受信者がそのアドレスグループに属している場合にのみポリシーのマッチングが行われます。[宛先(To)]フィールドでアドレスグループを使用しても、メッセージスコアリングには影響しません。
- [返信先(Reply-To)]アドレスのグループに基づいてポリシーをフィルタリングするため。ポリシーの[返信先(Reply-To)]フィールドでアドレスグループを指定すると、[返信先(Reply-To)]アドレスがそのアドレスグループにある場合にのみポリシーのマッチングが行われます。[返信先(Reply-To)]フィールドでアドレスグループを使用しても、メッセージスコアリングには影響しません。

新しい組織を作成すると、次の 3 つのアドレスグループが事前に作成されます。

- エグゼクティブ(エグゼクティブの偽装のポリシーに自動的に関連付けられます。詳細については、「「デフォルトポリシー」 ページ 154」を参照してください)
- C レベルエグゼクティブ(C レベルの偽装および C レベルへの疑わしいメッセージのポリシーに自動的に関連付けられます。詳細については、「「デフォルトポリシー」 ページ 154」を参照してください)
- トップパートナーおよびベンダー(パートナーまたはベンダーのタグが付けられたドメインから最大 1000 個の電子メールアドレスが自動的に入力されます。詳細については、「「ドメインタグ」 ページ 133」を参照してください)

新しい組織を設定するときに最初に行う必要があるタスクの 1 つは、これらのアドレスグループにエグゼクティブおよび C レベルエグゼクティブの電子メールアドレスを入力し、関連するポリシーを設定することです。

トップパートナーおよびベンダーのアドレスグループは、毎週自動的に更新されます。高度なフィッシング防御は、組織の従業員と定期的に通信するパートナーおよびベンダー（パートナーとしてタグ付けされたドメインのパートナーおよびベンダー。詳細については、「「ドメインタグ」 ページ 133」を参照してください）の個人を検出し、これらの個人をトップパートナーおよびベンダーのアドレスグループに入力します（最大 1,000 件）。

他のアドレスグループについては、独自の個別の電子メールアドレスを使用してそれらを作成できます。その場合は、アドレスグループの変更を手動で行うか、Azure AD グループを同期して作成することができます。この場合、Azure AD グループが変更されるとアドレスグループが更新されます。詳細については、「「アドレスグループを作成する」 次のページ）」および「「Azure Active Directory のアドレスグループとの同期」 ページ 194」を参照してください。

大規模なアドレスグループを作成する必要があり、Azure AD を利用できない場合は、Cisco ではカンマ区切り値（CSV）レコードのリストをアップロードしてアドレスグループを作成することもできます。詳細については、サポート担当者にお問い合わせください。

アドレスグループの例外

例外リスト内のアドレスは、誤検出を回避するために、アドレスグループ内のユーザーの「既知の適正な」電子メールアドレス、または個人用電子メールアドレスなどを指定するためのものです。

たとえば、会社のエグゼクティブの名前を使用した正当なメッセージが、アドレス <yourco_announce@example.com> から送信されたものとします。エグゼクティブ アドレス グループの例外リストにその電子メールアドレスを追加できます。こうすることで、<yourco_announce@example.com> からの本物のメッセージが検出されたときには、このアドレスグループに基づいてアラートは発行されません。

例外リストのアドレスは、メッセージ自体が本物でない場合を除き偽装としてタグ付けされることはなく、アドレスグループがポリシー内の [差出人（From）] および [返信先（Reply-To）] 条件によって参照された場合のみ、考慮されます。

アドレスグループ内のユーザーが「John Doe <messenger@webex.com>」または「John Doe <reply@chatter.salesforce.com>」のように正当な目的でスプーフィングした際に、条件が一致しないように、messenger@webex.com または reply@chatter.salesforce.com などのアドレスを追加できます。

上記アドレスの [危険性のない送信元（Friendly From）] を共有することのある「johndoe@gmail.com」などの個人アドレスを追加することもできます。

一部の電子メールサービスは、Sieve フィルタリングの標準に従って、「+」アドレッシングを使用します。このような場合、電子メールアドレスのローカル部分は、アドレスの「+」の後にランダムなテキスト文字列が続くため、アドレスグループに例外を設定する際に問題が発生する可能性があります。「John Doe <notifications+2hef98h2uibf8h@yammer.com>」を例に見てみます。このような場合、アドレスグループのマッチングでは「+」および「+」と「@」の間のすべての文字が自動的に無視されます。したがって、「notifications@yammer.com」だけを例外リストに追加してこれを無視し、John Doe の表示名と一致しないようにすることができます。

一部のメッセージは、Cisco によって一致するアドレスグループの表示名から自動的に除外されます。たとえば、認証に成功し、「内部」、「パートナー」、または「サービス」としてタグ付けされたドメインから送信されたメッセージは、アドレスグループの一致とは見なされません。

アドレスグループの例

このセクションでは、アドレスグループとポリシーがどのように連携するかについて説明します。

ポリシーの [差出人(From)] フィールドのアドレスグループ

ポリシーの [差出人(From)] フィールドでアドレスグループが参照されている場合、グループ内のユーザーの名と姓は、受信メールでグループメンバーの偽装を識別するために使用されます。

たとえば、Genius アドレスグループに Albert Einstein <aeinstein@genius.com> が含まれているとします。このグループは、Genius Spoofs というタイトルのポリシーで使用されています。aeinstein@genius.com は彼の本物のビジネスアドレスであるため、「Albert Einstein <aeinstein@genius.com>」からの本物の電子メールは受信メール内に表示され、高度なフィッシング防御はポリシーをトリガーしません。これは、Albert Einstein の既知の適正な電子メールの送信元であるためです。

しかし、Albert Einstein <genius_spoofer@not-a-genius.com> からの電子メールが組織に送信されたのを確認すると、高度なフィッシング防御は Genius Spoofs ポリシーのマッチングをトリガーします。

では、Einstein 氏が個人の AOL アドレス(<IQ160@aol.com>)を使用して組織に電子メールを送信することもある場合は、どうすればよいでしょうか。それが例外リストの目的です。IQ160@aol.com を例外リストに追加すると、「Albert Einstein <IQ160@aol.com>」からの本物の電子メールも Genius Spoofs ポリシーのマッチングをトリガーしません。

ポリシーの [宛先(To)] フィールドのアドレスグループ

ポリシーの [宛先(To)] フィールドでアドレスグループが参照されている場合、それは単にポリシーの受信者フィルタです。ポリシーは、受信者のアドレスがアドレスグループにある場合にのみ適用されます。

たとえば、Genius アドレスグループには現在、Albert Einstein <aeinstein@genius.com> と Stephen Hawking <shawking@genius.com> が含まれているとします。ここで、Untrusted messages sent to geniuses というポリシーを作成し、Genius アドレスグループをポリシーの [宛先(To)] フィールドに配置すると、そのポリシーは、信頼できる基準を満たし、aeinstein@genius.com または shawking@genius.com を受信者として含むメッセージのみをマッチングします。[宛先(To)] フィールドでのアドレスグループの使用には、例外は適用されません。

アドレスグループを作成する

アドレスグループは、一度に 1 つずつ追加する個別の電子メールアドレスで構成できます。または、Azure Active Directory に接続している場合は、アドレスグループを既存の Active Directory グループで構成できます。

個別の電子メールアドレスからアドレスグループを作成する

1. [管理(Manage)] > [アドレスグループ(Address Groups)] に移動します。
2. [アドレスグループの作成(Create Address Group)] をクリックします。
3. 名前を入力します。名前は、グループに入れる予定の電子メールアドレスを反映したものにする必要があります。
4. 1 つ以上のアドレスを追加します。
    1. [個別(Individual)] タブが選択されていることを確認してください。
    2. [姓(First Name)]、[名(Last Name)]、および有効な [電子メールアドレス(Email Address)] を入力します。
    3. [追加(Add)] をクリックします。
5. 例外の電子メールアドレスを追加する場合は、有効な電子メールアドレスを一度に 1 つずつ入力し、それぞれを入力した後に [追加(Add)] をクリックします。
6. [作成(Create)] をクリックします。

この方法で作成されたアドレスグループは、手動で更新する必要があります。詳細については、「「アドレスグループを編集する」次のページ)」を参照してください。

Azure Active Directory グループからアドレスグループを作成する

1. [管理(Manage)]>[アドレスグループ(Address Groups)]に移動します。
2. [アドレスグループの作成(Create Address Group)]をクリックします。
3. 名前を入力します。名前は、グループに入れる予定の電子メールアドレスを反映したものにする必要があります。
4. [Azure AD経由(via Azure AD)]タブをクリックします。
5. [Azure ADグループ(Azure AD group)]フィールドをクリックします。
6. [Active Directoryグループ(Active Directory group)]を選択します。姓名の両方を含む Active Directory グループの名前と電子メールアドレスがアドレスグループリストに追加されます。
7. 例外の電子メールアドレスを追加する場合は、有効な電子メールアドレスを一度に 1 つずつ入力し、それぞれを入力した後に[追加(Add)]をクリックします。
8. [作成(Create)]をクリックします。

この方法で作成されたアドレスグループは、リンクされている Azure AD グループが変更されると自動的に更新されます。アドレスグループ名の変更やアドレスグループのリンク解除など、実行できるその他の変更については、「「アドレスグループを編集する」次のページ)」を参照してください。

電子メールアドレスをアドレスグループに追加する

1. [管理(Manage)]>[アドレスグループ(Address Groups)]に移動します。
2. アドレスグループの名前をクリックします。
3. [アドレスの追加(Add Addresses)]セクションで、[名(First name)]、[姓(Last name)]、および[電子メールアドレス(Email address)]を入力します。
4. [追加(Add)]をクリックします。
5. [保存(Save)]をクリックします。

アドレスグループから電子メールアドレスを削除する

1. [管理(Manage)]>[アドレスグループ(Address Groups)]に移動します。
2. アドレスグループの名前をクリックします。
3. [アドレスの追加(Add Addresses)]リストで、電子メールアドレスの横にある をクリックします。
4. [保存(Save)]をクリックします。

アドレスグループを編集する

アドレスグループが個別のアドレスで構成されている場合、アドレスグループエントリのいずれかを追加、編集、または削除できます。アドレスグループが Azure Active Directory にリンクされている場合、アドレスグループで使用される Active Directory グループのみを切り替えることができます。

個別の電子メールアドレスで構成されているアドレスグループを編集する

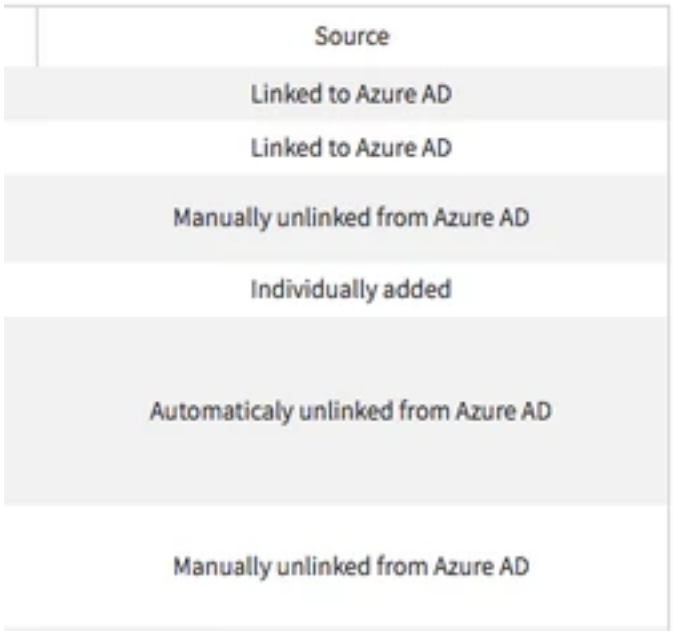
1. [管理(Manage)] > [アドレスグループ(Address Groups)] に移動します。
2. 追加された個別の送信元を持つアドレスグループの名前をクリックします。
3. 必要な変更を加えます。次の操作を実行できます。
    - アドレスグループ名を変更します。
    - [姓(First Name)]、[名(Last Name)]、および有効な[電子メールアドレス(Email Address)]を入力し、[追加(Add)]をクリックしてアドレスグループにメンバーを追加します。
    - アドレスリストの名前の横にある をクリックして、アドレスグループからメンバーを削除します。
    - 有効な電子メールアドレスを入力し、[追加(Add)]をクリックして例外を追加します。
    - 例外リストの名前の横にある をクリックして例外を削除します。
4. [保存(Save)]をクリックします。

Azure Active Directory にリンクされたアドレスグループを編集する

1. [管理(Manage)] > [アドレスグループ(Address Groups)] に移動します。
2. Azure AD にリンクされた送信元を持つアドレスグループの名前をクリックします。
3. 必要な変更を加えます。次の操作を実行できます。
    - アドレスグループ名を変更します。
    - [Azure ADグループ(Azure AD group)]フィールドをクリックし、Active Directory グループを選択します。
    - 同期されたアドレスグループのリンクを解除します。
    - 有効な電子メールアドレスを入力し、[追加(Add)]をクリックして例外を追加します。
    - 例外リストの名前の横にある をクリックして例外を削除します。
4. [保存(Save)]をクリックします。

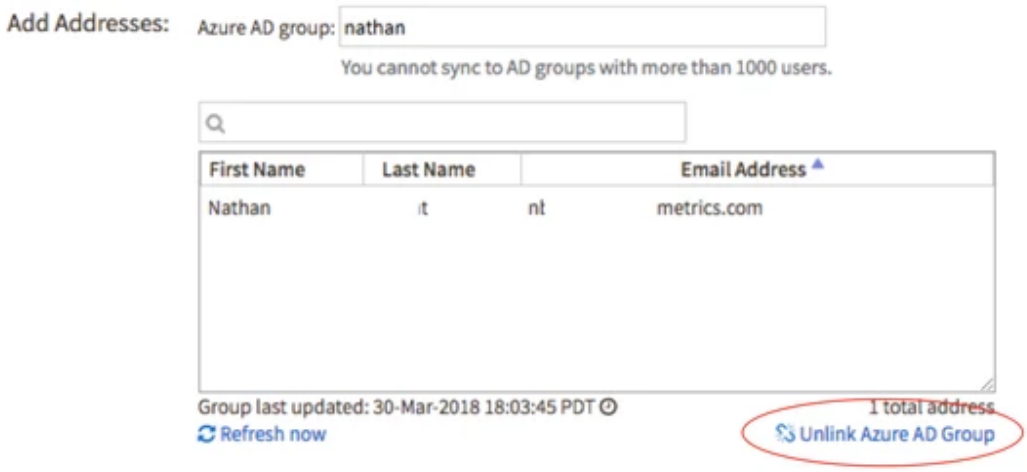
Azure Active Directory にリンクされたアドレスグループのリンクを解除する

[管理(Manage)] > [アドレスグループ(Address Groups)] ページの [送信元(Source)] 列で、アドレスグループが Azure Active Directory と同期されていることを確認できます。[Azure ADにリンク済み(Linked to Azure AD)]と表示されます。その他のステータスには、[個別に追加済み(Individually Added)]、[手動でAzure ADからのリンクを解除済み(Manually Unlinked from Azure AD)]、[自動でAzure ADからのリンクを解除済み(Automatically unlinked from Azure AD)]などがあります。



アドレスグループのインデックスページの[送信元(Source)]列

1. [アドレスグループの編集(Edit Address Group)]ページに移動するには、リンク済みのグループの名前をクリックします。右側にある名前のボックスの下に[Azure ADグループのリンクを解除(Unlink Azure AD Group)]へのリンクが表示されます。



2. [Azure ADグループのリンクを解除(Unlink Azure AD Group)]リンクをクリックします。これによりそのグループの Azure Active Directory との同期は停止されますが、現在のグループメンバーシップは維持されます。この時点で、手動でグループを変更できますが、変更内容は次回の同期まで上書きされません。
3. [保存(Save)]をクリックします。

アドレスグループを削除する

ポリシーで使用されているアドレスグループは削除できません。

1. [管理(Manage)] > [アドレスグループ(Address Groups)] に移動します。
2. アドレスグループの名前をクリックします。
3. ページの下部で [[address group name]の削除(Delete [address group name])] リンクをクリックします。
4. [OK] をクリックします。

Azure Active Directory のアドレスグループとの同期

Office 365 を使用している場合、高度なフィッシング防御のアドレスグループを Azure Active Directory グループと同期することにより、アドレスグループベースのポリシーをより効率的に管理できます。高度なフィッシング防御は、Azure AD グループのメンバーを同期された高度なフィッシング防御のアドレスグループに自動的にプルするため、手動で更新する必要はありません。

作成できる Azure AD グループにはいくつかの種類があります。

- Office 365
- 同報リスト
- メール対応のセキュリティ
- セキュリティ

Cisco 高度なフィッシング防御は、これらすべての種類の Azure AD グループを同期できます。ただし、ネストされた Azure AD グループとの同期は現在サポートされていません。

ポリシーでアドレスグループを使用する方法については、「「ポリシー」 ページ 153」を参照してください。

Azure AD グループの同期エラーの通知

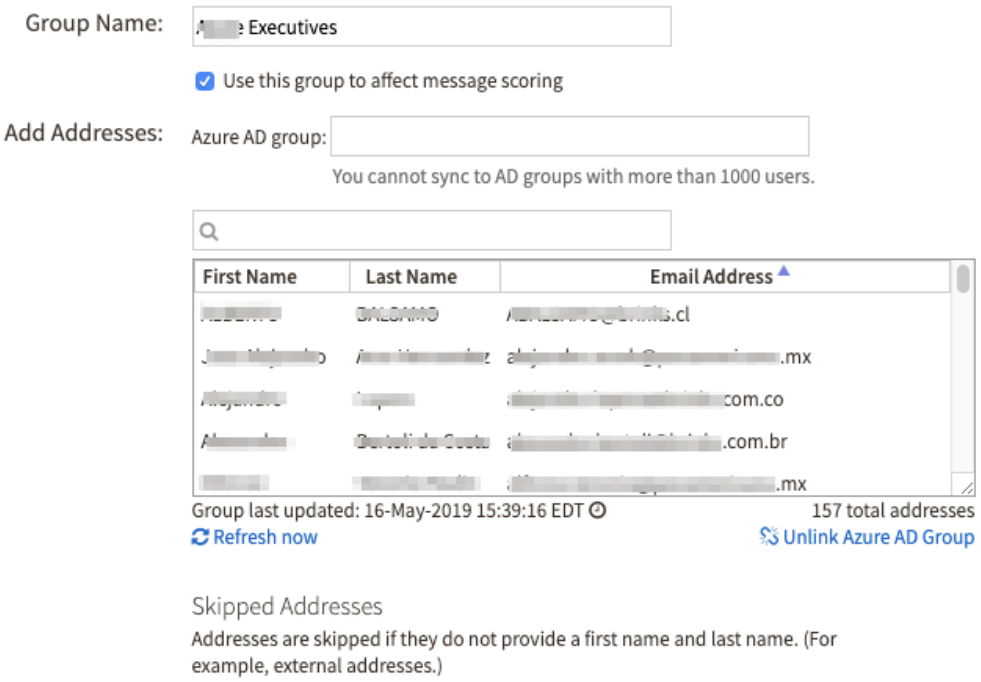
同期したアドレスグループを設定した後、定期的な同期ジョブのエラーについてのシステム通知にサインアップすることをお勧めします。

1. [管理(Manage)] > [ポリシー(Policies)] に移動します。
2. [システム通知(System Notifications)] タブをクリックします。
3. [ポリシー(Policies)] セクションまで下にスクロールし、[1日以内のアドレスグループとの同期に対するAzure AD同期エラー(Azure AD sync fails to sync an Address Group)] チェックボックスをオンにします。
4. [保存(Save)]をクリックします。

詳細については、「「通知」 ページ 152」を参照してください。

スキップされたアドレス

高度なフィッシング防御が、名、姓、または電子メールアドレスが欠落しているエントリを含む Azure Active Directory アドレスグループと同期すると、それらのエントリはアドレスグループに含まれません。代わりに、高度なフィッシング防御は [スキップされたアドレス(Skipped Addresses)] セクションをアドレスグループに追加し、それらのエントリをそのセクションにリストします。

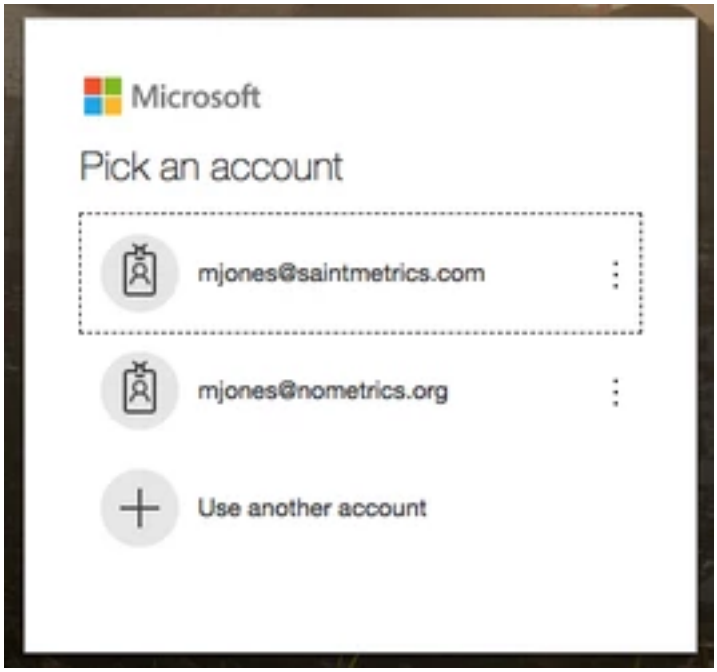


アドレスグループ内の [スキップされたアドレス（Skipped Addresses）] セクション。

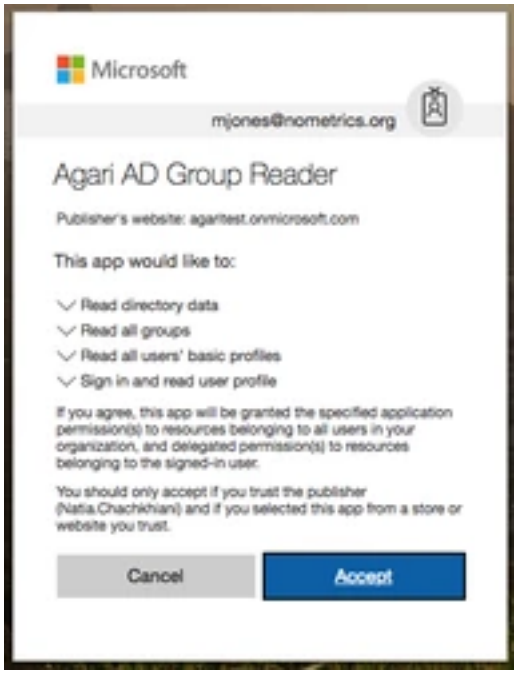
アドレスグループの同期を承認する

アドレスグループの同期を設定するには、最初に、Azure Active Directory と同期するように Cisco を承認する必要があります。

1. [管理（Manage）] > [組織（Organizations）] に移動します。
2. 組織名をクリックします。
3. [Microsoft API権限（Microsoft API Permissions）] タブを選択します。
4. [アドレスグループ（Address Groups）] の横にある [有効（Enable）] ボタンをクリックします。
5. Azure AD に接続し、権限を付与するためのダイアログが表示されます。適切な管理権限を持つアカウントとしてログインします。
6. Microsoft のページが表示されます。同意を付与するために使用するアカウントを選択すると、そのアカウントにログインするように求められます。



7. ログインすると、Agari AD Group Reader アプリケーションを承認するオプションが表示されます。[承認（Accept）] をクリックします。



承認後に、高度なフィッシング防御アプリケーションに戻され、グループと Azure Active Directory との同期が承認されます。

第 7 章

管理

高度なフィッシング防御の管理には、組織設定の定義、組織内のアクティビティの確認、組織内の高度なフィッシング防御ユーザーの管理などがあります。

組織管理者ロールを持っている場合にのみ、組織設定の変更、監査証跡の表示、およびユーザーの管理を行うことができます。

組織設定

組織設定によって、組織内での高度なフィッシング防御の 動作が決まります。[組織の編集(Edit Organization)]ページで組織を管理します。[組織の編集(Edit Organization)]ページには設定が収集されたタブが含まれ、各タブには関連する設定のセクションが含まれています。ここでは、次のカテゴリの設定を構成します。

- [管理(Administrative)]タブ
    - 管理
    - 組織
    - レポート
    - センサー
    - 適用
    - ユーザー アカウント
    - 関係会社管理
- [Microsoft API権限(Microsoft API Permissions)]タブ
- [メッセージコンポーネント(Message Components)]タブ
- [例外処理(Processing Exceptions)]タブ
- [監査(Audit)]タブ

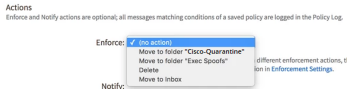
組織設定を表示または編集するには、[管理(Manage)]>[組織(Organizations)]に移動し、組織名をクリックします。

組織管理者ロールを持っている場合にのみ、組織設定を変更できます(設定によっては、Cisco 管理者のみが使用できる高いレベルのロールが必要です。ビューに設定が表示されない場合や、設定を変更できない場合は、これが原因である可能性があります)。

[管理(Administrative)]タブ

設定	説明
管理	
[組織名(Organization Name)]	組織の名前。これは、監査証跡など組織に関して表示する情報がある場所に表示されます。組織名を変更できます。
[シンボリック名(Symbolic Name)]	組織を一意に定義するために、当初設定された組織名から作成される一意の文字列です。この識別子は、システムによって使用され、ここにのみ表示されます。これは変更できません。
[サブドメイン(Subdomain)]	組織に固有のアプリケーション URL の一部。appc.cisco.com のサブドメインです。
[作成日(Creation Date)]	組織が作成された日付と時刻が表示されます。 をクリックすると、現地時間と UTC(協定世界時)が切り替わります。
組織設定	
[主要な管理担当者(Primary Administrative Contact)]	ここで組織内のユーザーを選択すると、管理作業に関する問い合わせはすべてそのユーザーが Cisco から受信することになります。
[親組織(Parent Organization)]	選択した子組織を管理するパートナー組織。
[組織のタイプ(Organization Type)]	組織が次のいずれであるかを定義します。 • [評価(Eval)]:高度なフィッシング防御の確認中です。 • [サブスクライバ(Subscriber)]:高度なフィッシング防御の料金を支払い済みです。
[有効期限(Expiration)]	いつ組織のサブスクリプションが期限切れになって更新が必要になるかを定義します。
分類設定	
組織の分類設定はレポートで使用され、特に 組織の集約データと同業他社の集約データを比較する場合に使用されます。 詳細については、「「レポート」 ページ 168」を参照してください。	
[地域(Region)]	これは、地域の同業他社を特定するために使用します。
[業種(Industry)]	これは、同業他社を特定するために使用します。組織が定義済みの選択肢のいずれにも分類されない場合は、[その他(Other)]を選択します。
[メールボックス(Mailboxes)]	これは、組織規模のプロキシとして、メールボックスサイズの範囲に基づいて同業他社を特定するために使用します。
[正確なメールボックス数(Exact mailbox count)]	組織内の実際のメールボックス数を入力します。これは、先ほど選択した範囲内の数値である必要があります。
メッセージ設定	
組織のメッセージ設定によって、高度なフィッシング防御が取り込むメッセージが決まります。 これらの設定は、[センサー設定(Sensor Settings)]セクションの [メッセージングプラットフォーム(Messaging Platform)] 設定が [Microsoft Office 365またはExchange Online(ジャーナリング)(Microsoft Office 365 or Exchange Online (journaled))] または [Microsoft Exchange Server(ジャーナリング)(Microsoft Exchange Server (journaled))] である場合にのみ使用できます。 また、ジャーナリングを正しく設定する必要があります。	

設定	説明
「「デュアル配信の設定：Office 365」 ページ 54」と「「デュアル配信の設定：Microsoft Exchange」 ページ 59」を参照してください。	
[メッセージの評価（Evaluate Messages）]	取り込むメッセージを定義します。次から選択してください。 • [着信メッセージ（Inbound messages）]：組織に送信されたメッセージのみがセンサーに取り込まれて評価されます。 • [すべてのメッセージ（着信、内部、発信）（All messages (Inbound. Internal, Outbound)）]：組織に送信されたメッセージ、組織から送信されたメッセージ、組織内で送信されたメッセージのすべてがセンサーに取り込まれて評価されます。これを選択するには、メッセージをジャーナリングし、電子メールを受け入れるドメインを特定する必要があります。
[受け入れ済みドメイン（Accepted Domains）]	メッセージを受け入れるドメインを定義します。[メッセージの評価（Evaluate Messages）] で [すべてのメッセージ（All messages）] を選択した場合には必須です。 これは、電子メールメッセージを受信するドメイン（サブドメインを含む）のリストにする必要があります。たとえば、mycompany.com はドメインですが、電子メールサーバーとして mail.mycompany.com を保持しています。これら（および場合によっては他のドメイン）をこのリストに含める必要があります。高度なフィッシング防御は、このリストを使用して、メッセージの方向性を判断します。 このリストに追加したドメインには、自動的に内部というタグが付けられます（まだタグがない場合）。IIP を有効にする前に内部というタグが付けられたドメインも、このリストに自動的に追加されます。IIP を有効にした後で内部というタグが付けられたドメインは、[受け入れ済みドメイン（Accepted Domains）] リストに自動的には追加されません。詳細については、「「ドメインタグ」 ページ 133」を参照してください。
レポートの設定	
攻撃タイプごとに、以下を選択できます。 • [信頼できない（Untrusted）]：メッセージトラストスコアは 0.0 ～ 1.0 • [信頼できず疑わしい（Untrusted and Suspicious）]：メッセージトラストスコアは 0.0 ～ 5.0 トラストスコアが 0.0 ～ 1.0（スケールは 0.0 ～ 10.0）のメッセージは信頼できないと見なされます。 トラストスコアが 1.0 より大きく 5.0 までのメッセージは疑わしいと見なされます。 この設定にすると、レポートに信頼できないメッセージのみを含めるか、 信頼できないメッセージと疑わしいメッセージの両方を含めるかを攻撃タイプごとに定義できます。 ドメインスプーフィングを除くすべての攻撃タイプのデフォルトは [信頼できず疑わしい（Untrusted and Suspicious）] です。	
センサーの設定	
[センサー設定（Sensor Settings）] セクションは、組織のグローバルなセンサー設定を参照しています。	
[動作モード（Operational Mode）]	電子メールインフラストラクチャにセンサーを配置する方法を定義します。詳細については、「「センサーへの配信の設定」 ページ 47」を参照してください。
[メッセージングプラットフォーム（Messaging Platform）]	メッセージング プラットフォームを定義します。次を選択します。

設定	説明
	• G Suite（旧 Google Apps for Work） • Microsoft Office 365 または Exchange Online（ジャーナリング） • Microsoft Exchange Server（ジャーナリング） • その他
[元の宛先ヘッダー名（Original-To Header Name）]	センサー処理の上書きにのみ使用します。Cisco から特に指示がない限り、そのままにしておきます。 このフィールドに値を入力すると、メッセージがセンサーで処理される際に、[元の宛先ヘッダー（Original-To Header）] がその値に置き換わります。そのため、ポリシーを作成する場合に、センサーで処理されたメッセージを容易に識別できます。
[元のmail-fromヘッダー名（Original-Mail-from Header Name）]	センサー処理の上書きにのみ使用します。Cisco から特に指示がない限り、そのままにしておきます。
[内部MTA IP（Internal MTA IPs）]	キャプチャするトラフィックを送信しているアップストリーム MTA の IP アドレスを一覧します。形式は、IP アドレスの範囲を指定するための CIDR 表記を受け入れます。 これは、アップストリーム MTA の場合にのみ使用します。
[許可された転送IP（Allowed Forwarding IPs）]	センサーが転送メッセージを受け入れる IP アドレスを指定します。このフィールドに 1 つ以上の IP アドレスを入力すると、リストにない IP アドレスからメールが転送されなくなります。 これは一般にセキュリティ対策を強化する場合に使用し、通常は空白のままにします。 また、SMTP 接続のテストにも影響します。 リストに IP アドレスを追加するには、[IPアドレス（IP Address）] フィールドに IP アドレスを入力し、[追加（Add）] をクリックします。このリストの IP アドレスは、センサーにメッセージを転送する電子メールインフラストラクチャ内のサーバーの IP アドレスのみにしてください。
適用の設定	
[適用（Enforcement）] を使用すると、エンドユーザーの受信トレイ内の指定のフォルダにメッセージを移動するポリシーを作成できます。[適用（Enforcement）] は、Gmail、Office 365、および Exchange Web Services（EWS）の環境でのみ使用できます。	
[適用（Enforcement）]	[有効（Enable）] に設定すると、ポリシー設定に基づいてメッセージにルールを適用できます。
[適用ラベル（Enforcement Label(s)）]	[適用の設定（Enforcement Settings）] で、デフォルトの適用フォルダを変更したり、追加フォルダを設定したりすることができます。これらのフォルダは、ポリシーの作成/編集内のすべてのポリシーの適用アクションに表示され、電子メールクライアントでエンドユーザーに対して表示されるフォルダまたはラベルの名前となります。  ポリシー内の適用アクション

設定	説明
ユーザーアカウント設定	
[シングルサインオン（Single Sign-on）]	ユーザーが高度なフィッシング防御にアクセスする場合にユーザー名だけでなくパスワードも入力する必要があるかどうかや、ユーザーが既存の認証を使用できるかどうかを決定します。詳細については、「「シングルサインオン（SSO）」 ページ 211」および「「組織のシングルサインオンの有効化」 ページ 212」を参照してください。
[セッションが非アクティブならログオフ（Session Inactivity Logoff）]	ユーザーが高度なフィッシング防御にサインインしたままにできる時間を決定します。これを過ぎると、自動的にサインアウトします。デフォルトは 4 時間です。
[セッションの絶対ログオフ（Session Absolute Logoff）]	自動ログオフの方法を指定します。次から選択してください。 • [相対（Relative）]（デフォルト）：[セッションが非アクティブならログオフ（Session Inactivity Logoff）] に設定された期間内に高度なフィッシング防御でアクションが行われないと自動的にログオフします。 • [絶対（Absolute）]：ログイン後に [セッションが非アクティブならログオフ（Session Inactivity Logoff）] に設定された期間が経過すると、自動的にログオフします。つまり、[セッションが非アクティブならログオフ（Session Inactivity Logoff）] のクロックは、ログイン時に開始され、ユーザーがアクションを行ってもリセットされません。この設定にすると、ユーザーがアクションを行っている最中にログオフする可能性があります。
[パスワードの有効期限（Password expiration）]	ユーザーが次に新しいパスワードを選択するまでの期間を決定します。デフォルトは [なし（Never）] です。
[ログイン試行失敗の最大回数（Maximum failed login attempts）]	ユーザーがログインに失敗できる回数を決定します。この回数を超えると、ロックアウトされ、新しいアクティベーションリンクを送信する必要があります。ログインの試行を制限しない場合は、[無効（Disabled）] を選択します。
[パスワードポリシー（Password Policy）]	ログイン時にパスワードの入力を必須にした場合（非 SSO）、パスワードの複雑さの最小要件を決定します。デフォルトは次のとおりです。 • 最小文字数：10 文字 • 大文字の最小数：1 • 小文字の最小数：1 • 記号（英数字以外）の最小数：1 • 数字の最小数：1 • 過去 N 個のパスワードの再利用を防止する：0 ユーザーに対するこうしたパスワード特性のいずれかを変更するには、[カスタム（Custom）] を選択します。
関係会社管理者設定	
[取り込み（Ingest）]	APD データパイプラインで組織のメッセージデータを取り込むための機能を有効にします。 これは、設定したグラフ取り込みまたはジャーナリングによって異なります。
[解析中（Parsing）]	初期設定後に有効に設定してください。[解析中（Parsing）] を有効なステータスに設定する前に、APD Web アプリケーションで、適切にフォーマットされたメッセージデータが取り込まれていることを確認します。これにより、有効な

設定	説明
	データのみがスコアリングモデルに入力されるようになります。

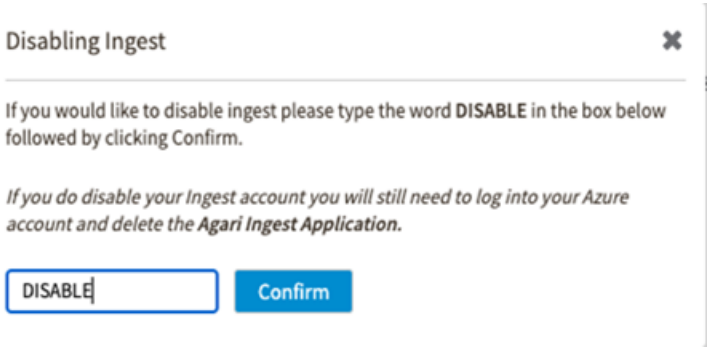
[Microsoft API権限（Microsoft API Permission）] タブ

設定	説明
	[Microsoft API権限（Microsoft API Permission）]
Cisco 高度なフィッシング防御 から Microsoft API のデータにアクセスして、取り込み、適用、アドレスグループ、調査分析といった特定の機能を利用するには、そのための許可が必要です。	
[取り込み（Ingest）] ユーザーのメールボックスにある電子メールを読み、すべてのサービス使用状況レポートを読み込む	こうした権限を有効にすると、Cisco 高度なフィッシング防御 はスコアを付ける目的でユーザーの電子メールボックスから電子メールを取得し、電子メールをスキャンして、ビジネス電子メールの侵害を特定できます。[取り込み（Ingest）] を有効にすると、高度なフィッシング防御を許可するための Microsoft ページに移動します。 これらの権限を有効にするには、次のメール権限が必要です。 • Mail.Read • Reports.Read.All • User.Read.All
[適用（Enforcement）] ユーザーのメールボックスで電子メールを作成、更新、および削除する	これらの権限を有効にすると、ユーザーの電子メールの調査分析とメッセージの適用を行うことができます。 これらの権限を有効にするには、次のメール権限が必要です。 • Mail.ReadWrite • User.Read.All
[アドレスグループ同期（Address Group Sync）] Azure Active Directory に接続して同期する	これらの権限を有効にすると、ポリシーで使用するアドレスグループをすばやく作成できます。また、適用の対象となるユーザーのメールボックスの場所（オンプレミスまたはクラウド）を指定できます。 この権限を有効にするには、次の電子メール権限が必要です。 • Directory.ReadAll

取り込み/適用を無効にするステップ

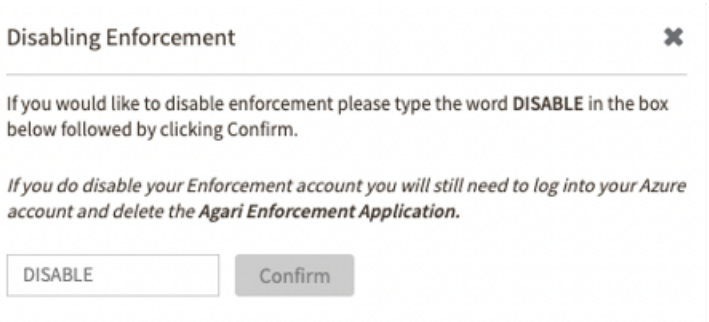
取り込みと適用の権限を無効にするには、Cisco 高度なフィッシング防御 に**マスター管理者**としてログインする必要があります。

1. [管理（Manage）] > [組織（Organizations）] に移動し、組織名をクリックします。
2. [Microsoft API権限（Microsoft API Permission）] タブを選択します。
3. [取り込み（Ingest）] オプションで、[無効（Disable）] をクリックします。[取り込みの無効化（Disabling Ingest）] ポップアップで、**DISABLE** と入力し、[確認（Confirm）] をクリックします。[取り込み（Ingest）] アカウントが組織で永久に無効になります。



組織での取り込みの無効化

4. [適用(Enforcement)]オプションで、[無効(Disable)]をクリックします。[適用の無効化(Disabling Enforcement)]ポップアップで、**DISABLE** と入力し、[確認(Confirm)]をクリックします。[適用(Enforcement)]アカウントが組織で永久に無効になります。



組織での適用の無効化

Agari Ingest / Enforcement Application を APP から使用不可にした後で削除するには、Microsoft Azure にグローバル管理者としてログインする必要があります。

組織で再度取り込みまたは適用を有効にするには、新しい取り込み/適用アカウントを作成する必要があります。

[メッセージコンポーネント(Message Components)]タブ

設定	説明
	[メッセージコンポーネント(Message Components)]
Cisco が分析のために、メッセージのどのコンポーネントをアップロードするかを選択します。 Cisco すべてのメッセージコンポーネントを有効にすることをお勧めします。	
[メッセージコンポーネント(Message Components)]	メッセージのどのコンポーネントをセンサーにアップロードして分析するかを指定します。Cisco では、利用可能なすべてのメッセージコンポーネントを分析することを推奨しています。デフォルトでは、すべてのコンポーネントが選択されます。 [含める(Include)]オプション(件名ヘッダー、完全な差出人、返信先、および受信者)を使用すると、センサーはメッセージのメタデータをさらに的確に分析できるようになり、その結果、スコアリングの精度が向上します。 [メッセージコンテンツの処理(Process message content)]オプションを使用すると、センサーはメッセージの本文から添付ファイルと URI のみを抽出し、そのコンポーネントのみを分析して悪意の有無を確認できます。添付ファイルでも URL でもないコンテンツは分析されず、添

設定	説明
	付ファイルと URL が抽出されるとすぐに破棄されます。また、メッセージの詳細を表示するときに、すべての URI を表示することも（デフォルト）、悪意のある URI のみを表示することもできます。

[例外処理（Processing Exceptions）] タブ

設定	説明
	[例外処理（Processing Exceptions）]
例外処理の設定は、どのメッセージの処理を評価しないかを高度なフィッシング防御に指示するルールです。 こうしたルールのいずれかを満たすメッセージは、センサーによる評価、脅威のスコア付け、ポリシーによる管理が行われません。 高度なフィッシング防御によって処理されないメッセージは、レポートや検索に個別にも累積としても表示されません。	
[Office 365スパム処理（Office 365 Spam Processing）]	Office 365 を導入している組織のみ。 Office 365 スパムフィルタリングを介して送信されたメッセージには、スパムスコアが割り当てられてます。スパムスコアは、スパム信頼度レベル（SCL）評価にマップされています。スパムスコアが 5 以上であると、Office 365 ではスパムと見なされ、デフォルトではユーザーの迷惑メールフォルダに移動されます。（出典：スパム信頼度レベル） 組織によっては、Office 365 に別のスパムスコアを設定して、メッセージをユーザーの迷惑フォルダに送信するようにしている場合もあります。Office 365 がすでにスパムと判断したメッセージを高度なフィッシング防御で処理するのは通常推奨されないため、この設定は組織の Office 365 と同じ値にするのが最適です。
[メッセージスコアリング例外ルール（Message Scoring Exception Rules）]	メッセージルールを定義します。処理をスキップするメッセージを高度なフィッシング防御に指示するルールです。こうしたルールは、電子メールクライアントのメッセージ処理ルールと同じように機能します。ルールタイプを選択し、そのタイプの値を入力します。 メッセージにあるヘッダー、つまり次のようなヘッダーに対してルールを使用できます。 • IP アドレスまたは CDR • MAIL FROM ドメイン • 送信者：（From:） • 宛先：（To:） • 件名：（Subject:） • X-Header 例外ルールを追加するには、ルールタイプを選択し、単一の値を入力して、[例外を追加（Add Exception）] をクリックし、[保存（Save）] をクリックします。 値フィールドには、1 つの値のみ（X-Header の場合は、X-Header 自体とオプションで X-Header 値）を入力できます。ワイルドカードや正規表現はサポートされていません。厳格な完全テキスト一致のみです（ただし、[件名（Subject）] は例外で、入力した値がメッセージ件名の

設定	説明
	どこかに含まれていれば一致します）。値が適切かどうか検証されてから、例外ルールを追加できます。 例外ルールを削除するには、ルールの横にある をクリックし、[保存（Save）] をクリックします。

[監査（Audit）] タブ

組織のすべてのユーザーについて、過去のセッションアクティビティとデータ変更がすべて表示されます。各アイコンの説明については、「監査証跡」を参照してください。

監査証跡

高度なフィッシング防御 は、組織内のすべてのアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。組織（「「組織アクティビティの表示」次のページ）」を参照）と組織内の各ユーザー（「「ユーザーアクティビティの表示」ページ 208」を参照）の両方のアクティビティがすべて、新しい順に [アクティビティログの監査（Audit the activity log）] ページにリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。

ログの検索および使用方法の詳細については、[監査ログ（Audit log）] ページの上部にある [ヘルプ（Help）] アイコン（疑問符）をクリックしてください。

アイコン	アクティビティのカテゴリ
	ユーザーが高度なフィッシング防御自体または高度なフィッシング防御内の組織にサインインしたことを示します。
	ユーザーが高度なフィッシング防御自体または高度なフィッシング防御内の組織からサインアウトしたことを示します。
	ユーザーがユーザーアカウント、ポリシー、またはアドレスグループを作成、編集、または削除したことを示します。
	ユーザーがドメインに対して作成、編集、削除、またはその他のアクションを実行したことを示します。
	ユーザーが送信者に対して作成、編集、削除、またはその他のアクションを実行したことを示します。
	ユーザーがレポートリクエストを作成したことを示します。
	ユーザーがドメイングループに対して作成、編集、削除、またはその他のアクションを実行したことを示します。
	ユーザーが、Cisco サービス規約（TOS）に同意する、組織設定を変更するなど、組織レベルのアクティビティを実行したことを示します。

組織アクティビティの表示

高度なフィッシング防御 は、組織内のすべてのアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。

組織のアクティビティを表示するには、組織管理者ロールが必要です。

1. [管理(Manage)] > [組織(Organizations)] に移動します。
2. 組織名の下にある [監査(Audit)] リンクをクリックします。

高度なフィッシング防御組織内のすべてのアクティビティが、新しい順にリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。各アイコンの説明については、「「監査証跡」(前のページ)」を参照してください。

ユーザーアカウント

ユーザーアカウントでは、高度なフィッシング防御ユーザーのログイン情報とアクセス機能を定義します。高度なフィッシング防御は、ロールベース アクセス コントロール(RBAC)を使用していて、高度なフィッシング防御機能にアクセスするためのロールを各ユーザーに 1 つ以上割り当てることができます。

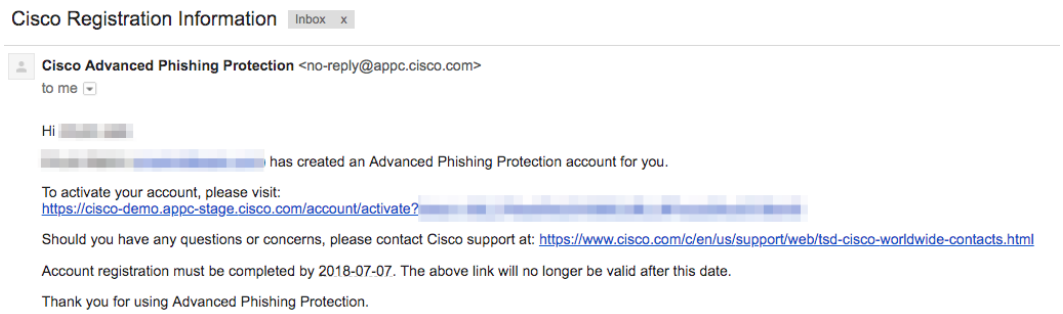
Cisco のサポート担当者には、高度なフィッシング防御 組織でユーザーアカウントを作成、有効化、編集、または削除するためのアクセス権がありません。

ユーザーアカウントの作成

ユーザーアカウントを作成できるのは、組織管理者ロールを持つユーザーのみです。

1. [管理(Manage)] > [ユーザー(Users)] に移動します。
2. [ユーザーの作成(Create User)] をクリックします。
3. [氏名(Full Name)] と [電子メール(Email)] にそれぞれ氏名とアドレスを入力します。

   有効なメールアドレスを入力する必要があります。このメールアドレスが招待メールメッセージの送信先になります。招待メールメッセージには作成した新規ユーザーに固有のリンクが含まれ、ユーザーはそのリンクをクリックして自身の新規アカウントを検証する必要があります。



   招待電子メールメッセージのサンプル。

4. シングルサインオンに加えて、またはシングルサインオンの代わりに、このユーザーアカウントでセカンダリ認証(パスワード形式のローカル認証)を使用できるようにする場合に選択します(詳細については、「「シン

グルサインオン（SSO）」 ページ 211」を参照してください）。このオプションを選択した場合は、次も選択します。

- [シングルサインオンが失敗したときのみ（Only when Single Sign-On Fails）]：シングルサインオンが機能しないときは、このユーザーアカウントがパスワードを入力できるようにします。
- [排他的（シングルサインオンで認証しない）（Exclusively（Do Not Authenticate via Single Sign-On））]：このユーザーアカウントをローカル認証にのみ制限します。つまり、ユーザーは常にユーザー名とパスワードの両方を入力する必要があり、SSO を使用できません。

5. ユーザーアカウントに付与するロールを選択します。詳細については、「「ユーザーロール」 ページ 209」を参照してください。
6. [新規ユーザーを招待（Invite New User）] をクリックします。

入力したメールアドレスに電子メールが送信されます。メールにはユーザーを検証するためのリンクが含まれ、検証されたユーザーはアカウントのパスワードを設定できます。

販売担当者は、高度なフィッシング防御にアクセスするための最初の管理者アカウントを有効にする必要があります。通常、最初のアカウントには、組織のユーザーアカウントを追加で作成できるように、組織管理者ロールを含めた複数の管理者ロールが割り当てられます。

ユーザーアカウントの編集

1. [管理者（Admin）] > [ユーザー（Users）] に移動します。
2. ユーザーの名前をクリックします。
3. ユーザー情報と設定に必要な変更を加えます。詳細については、「「ユーザーアカウント設定」 次のページ）」を参照してください。
4. [更新（Update）] をクリックします。

ユーザーアカウントの削除

1. [管理者（Admin）] > [ユーザー（Users）] に移動します。
2. ユーザーの名前をクリックします。
3. 右下の [[ユーザー名]を完全に削除...（Delete [username] entirely from...）] リンクをクリックします。
4. [OK] をクリックします。

高度なフィッシング防御へのサインイン

高度なフィッシング防御にサインインする前に、自身のアカウントを作成しておく必要があります（「「ユーザーアカウントの作成」（前のページ）」を参照してください）。また、ウェルカム電子メールのリンクをクリックして、電子メールアドレスを確認しておく必要があります。

1. サポートされているブラウザで、URL https://appc.cisco.com から高度なフィッシング防御にアクセスします。
2. 自分の電子メールアドレスを入力します。

3. オプションとして、組織がシングルサインオン（SSO）を有効にしていない場合は、パスワードを入力します。
4. [次へ（Next）]をクリックします。

ユーザーアクティビティの表示

高度なフィッシング防御 は、すべてのユーザーアクティビティを文書化して認証するために綿密で詳細な監査証跡を作成します。ユーザーアクティビティを表示するには、監査ユーザーロールが必要です。

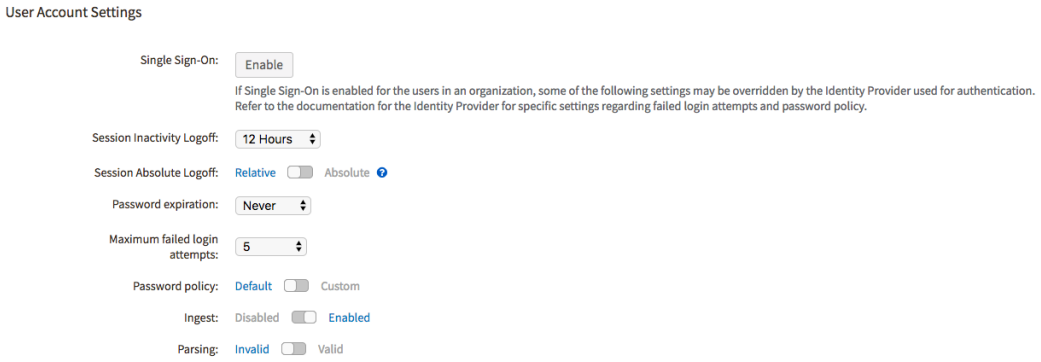
1. [管理者（Admin）]>[ユーザー（Users）]に移動します。
2. ユーザー名の下にある[監査（Audit）]リンクをクリックします。

高度なフィッシング防御組織内のすべてのユーザーアクティビティが、新しい順にリストされます。リストでは、アイコンを使用してアクティビティのタイプを分類しています。各アイコンの説明については、「「監査証跡」 ページ 205」を参照してください。

また、[CSVをダウンロード（Download CSV）]をクリックして、ユーザーのアクティビティがすべて記録されたカンマ区切り値のテキストファイルをダウンロードすることもできます。

グローバルなユーザーアカウント設定の構成

グローバルなユーザーアカウント設定には、ユーザーのログオン方法、ログオフするタイミング、パスワードポリシーなどがあります。



[ユーザーアカウント設定（User Account Settings）]セクション

1. [管理（Manage）]>[組織（Organizations）]に移動します。
2. 組織名をクリックします。
3. ユーザーアカウント設定に必要な変更を加えます。詳細については、「「組織設定」 ページ 197」の「ユーザーアカウント設定」セクションを参照してください。
4. [保存（Save）]をクリックします。

ユーザーアカウント設定

このトピックでは、高度なフィッシング防御ユーザーアカウントの設定について説明します。

ユーザー情報

設定	説明
正式名称	ユーザーがログインしているときに各ページの上部に表示されるユーザーのフルネーム（ユーザーのリストに表示されるものと同じ）。アクティビティの監査ログにも表示されます。
E メール	ユーザーの電子メール アドレス。ユーザーのログイン クレデンシャルと、レポートおよびアラートの宛先アドレスに使用されます。この電子メール アドレスは、初期アクティベーション トークンが添付された招待電子メールに使用されることに注意してください。
セカンダリ認証	組織がシングルサインオン（SSO）を使用している場合、このオプションによって、セカンダリ認証（ユーザー名とパスワード）をオプションにするか必須にするかが決まります。このオプションを選択しないと、常に SSO が使用されます。そのため、サインイン時に SSO プロバイダーが利用できない場合は、アプリケーションにアクセスできません。このオプションを選択すると、さらに次の 2 つのオプションが表示されます。 • [SSOが失敗したときのみ（Only when SSO fails）]：SSO プロバイダーが利用できない場合、ユーザーはパスワードフィールドに入力するように求められます。 • [排他的（SSOで認証しない）（Exclusively（do not authenticate with SSO））]：ユーザーは、常にパスワードの入力を求められます（SSO は使用されません）。

また、ユーザーには 1 つ以上のロールが割り当てられます。高度なフィッシング防御ユーザーロールの詳細については、「「ユーザーロール」 下」を参照してください。

ユーザーロール

このトピックでは、高度なフィッシング防御でユーザーアカウントを割り当てることができるユーザーロールについて説明します。高度なフィッシング防御のロールは、次の 2 つのカテゴリに分類されます。

- ユーザーロール。読み取り専用のロールで、ユーザーは高度なフィッシング防御の特定の領域のみを表示できます。よく使用される「CRUD」（作成、読み取り、更新、削除）パラダイムの「R」の部分です。
- 管理者ロール。ユーザーは、高度なフィッシング防御のさまざまな領域に変更を加えることができます。「CRUD」の「C」、「U」、「D」の部分です。

ロールは、デフォルトでは階層形式になっています。つまり、ユーザーアカウントにロールを割り当てると、選択したロールの「下」にあるすべてのロールも自動的に割り当てられます。選択したロールの下にあるロールは、手動で割り当てを解除できます。

次の表に、使用可能なロールを階層順に示します。

ロール	説明
	管理者のロール
組織の管理者	組織管理者は、デフォルトでは、該当する権限が特にオフになっていない限り、読み取り専用ユーザー、監査ユーザー、およびユーザー管理者のすべての権限を保持しています。さらに、組織管理者は組織の設定、ポリシー、およびアドレスグループに変更を加えることができます。 • [管理（Manage）] > [組織（Organization）] で組織の設定を表示および編集する。 • [管理（Manage）] > [ポリシー（Policies）] でポリシー設定を表示、作成、および編集する。 • [メッセージの検索（Search Messages）] でオンデマンドポリシーを作成する（顧客の設定に適用可能な場合）。

ロール	説明
	• [管理(Manage)] > [送信者(Senders)] で送信者とIP の表示、承認、拒否、または元に戻す機能を実行する。 • [管理(Manage)] > [センサー(Sensors)] でメトリックを表示し、設定を更新する。 • [管理(Manage)] > [アドレス グループ(Address Groups)] でアドレス グループを表示、作成、および編集する。
ユーザー管理者	ユーザー管理者は、デフォルトでは、該当する権限が特にオフになっていない限り、読み取り専用ユーザーと監査ユーザーのすべての権限を保持しています。さらに、監査ユーザーは次のことができます。 • [管理(Manage)] > [ユーザー(Users)] でユーザーを作成および編集する。
ユーザーの役割	
監査ユーザー	監査ユーザーは、デフォルトでは、読み取り専用権限が特にオフになっていない限り、読み取り専用ユーザーのすべての権限を保持しています。さらに、監査ユーザーは次のことができます。 • [管理(Manage)] > [ユーザー(Users)] でユーザーの監査ログを表示および検索する。
読み取り専用ユーザー	読み取り専用ユーザーは、高度なフィッシング防御内でデータを検索および表示することはできますが、いずれの場所でも変更または編集することはできません。 • すべてのページにおいて、[分析(Analyze)] メニューの下でデータを表示および検索する([概要(Overview)]、[メッセージ(Messages)]、[ドメイン(Domains)]、[IP アドレス(IP Addresses)]、および [メッセージの検索(Search Messages)])。 • [管理(Manage)] > [ポリシー(Policies)] ページでポリシー設定を表示する。新しいポリシーの作成、オンデマンド ポリシーの作成、またはポリシーの変更は実行できません。 • [管理(Manage)] > [レポート(Reports)] でレポートを表示する。 • [管理(Manage)] > [送信者(Senders)] で送信者を表示する。送信者または IP の [承認(Approve)]、[拒否(Deny)]、または [元に戻す(Undo)] は実行できません。 • [管理(Manage)] > [センサー(Sensors)] でメトリックと設定を表示する。センサーの設定を変更することはできません。 • [管理(Manage)] > [ユーザー(Users)] で自身のユーザー設定を表示し、API クレデンシャルを有効化する。自身のユーザーロールを変更することはできません。 • [管理(Manage)] > [アドレス グループ(Address Groups)] でアドレス グループ設定を表示する。アドレス グループを作成または編集することはできません。

ロールの例

ユースケースによっては、ロールを設定することになります。このトピックでは、その設定方法の例を示します。

電子メールによるレポートとアラートを受け取ることができる読み取り専用ユーザーを作成します。

ユーザーの読み取り専用ロールをオンにすると、レポート受信者ロールもデフォルトでオンになります。電子メールによるレポートとアラートを受け取ることもできる読み取り専用ユーザーを作成するには、単にこれらのデフォルトを受け入れます。レポート受信者ロールをオフにすると、読み込み専用ユーザーは、レポートを送信するために使用可能なユーザーのリストに表示されず、アラートに登録できるユーザーのリストにも表示されません。

読み取り専用アクセス権を持ち、他の読み取り専用ユーザーを作成できるユーザー管理者を作成します。

ユーザー管理者を、そのユーザーの最上位アクセス ロールとしてオンにします。このユーザー管理者は、読み取り専用アクセス以下のアクセス権を持つユーザーのみを作成して管理できるようにするため、ユーザー管理者ロールの真下にある [ユーザーの管理（Manage Users）] チェックボックスで [すべての権限（All privileges）] オプションをオフにします。その後に、[読み取り専用（Read Only）] オプションと [レポート受信者（Report Recipient）] オプションをオンにします。このユーザーは、読み取り専用以下の権限を持つユーザーを作成して管理することができます。

他のユーザーを作成することだけができるユーザー管理者を作成します。

他のユーザーを作成または編集することだけを目的とするユーザー管理者を作成します。このロールは、製品を使用してデータを表示したり、レポートやアラートを受け取ったりすることはできません。

新しいユーザーを作成した後に、作成したユーザーに対してユーザー管理者ロールをオンにして、ユーザー管理者の下で自動的にオンになっているすべてのロールをオフにします。ユーザー管理者ロールの下にある [ユーザーの管理（Manage Users）] ボックスで設定を変更しない限り、作成したユーザー管理者は、「すべての権限」を持つ他のユーザーを作成できます。

この新しいユーザー管理者が組織管理者とユーザー管理者を除くすべてのロールを作成できるようにするには、[x] を選択して [すべての権限（All Privileges）] を削除します。その後に、[ロールタイプの選択（Select Role Types）] 入力を使用して、組織管理者とユーザー管理者を除く各ロールをオンにします。

シングルサインオン（SSO）

高度なフィッシング防御 は現在、SAML 2.0 プロトコルを介して、組織内のユーザーを認証するためのシングルサインオン（「SSO」）メカニズムを有効化する機能が組み込まれています。

シングルサインオンを使用して、次のことを実行できます。

- 「ワンクリック」ログインの体験を作成する。既存の企業ログインアイデンティティ（アカウント）を高度なフィッシング防御のユーザー名にバインドできます。それによって、個別の高度なフィッシング防御のパスワードは必要なくなります。
- ユーザーアクセスを一元的に取り消す。従業員が退職した場合は、高度なフィッシング防御へのアクセスを高度なフィッシング防御内で個別にではなく SSO プロバイダー内で削除できます。
- オプションのセカンダリ認証を提供する。特定のユーザー（たとえば、請負業者は ID プロバイダーシステムでは利用不可）を、高度なフィッシング防御に保存されているログイン情報を使用して、排他的に認証できます（効果的にシングルサインオン メカニズムをバイパス）。また、SSO アイデンティティ サービスが失敗した場合でも、高度なフィッシング防御のみに保存されているクレデンシャルを使用して、特定のユーザーを認証することができます。

SSO でのログイン

SSO が有効なユーザーのログイン プロセスは、SSO の実装方法によって異なります。

- ID プロバイダーが開始した SSO の場合、ユーザーはクレデンシャルを入力したり、ログイン ページに移動したりする必要はありません。ID プロバイダーは、組織のアイデンティティ サービス プロバイダーを通じて接続を開始し、ログインします。
- サービスプロバイダーが開始した SSO の場合、ユーザーは https://appc.cisco.com で高度なフィッシング防御ログインページに移動し、電子メールアドレスを入力します。セカンダリ認証を有効にしない限り、高度なフィッシング防御ログインページに [パスワード（Password）] フィールドは表示されません（必要な場合、セカンダリ認証によって、ユーザーはパスワードを介してログインできます）。代わりに、ID プロバイダーのページが表示されます。ユーザーがまだ ID プロバイダーに認証されていない場合、認証

を得ることを求められます（ID プロバイダーは、複数の画面で認証を提示することがあります）。ユーザーが ID プロバイダーに認証されると、再度、高度なフィッシング防御の概要ページにリダイレクトされます。

組織のシングルサインオンの有効化

開始する前に、シングルサインオン プロバイダーから次の 2 つの情報を入手する必要があります。

- SAML 2.0 エンドポイント（HTTP）URL（ID プロバイダーシステムでは、「宛先」や「SAML 受信者」とも呼ばれます）
- パブリック証明書（X.509）

このタスクを実行するには、組織管理者ロールが必要です。

1. [管理者（Admin）] > [組織（Organization）] に移動します。
2. [組織の詳細を編集（Edit Organization Details）] をクリックします。
3. [ユーザーアカウント設定（User Account Settings）] セクションで、[シングルサインオンを有効にする（Enable Single Sign-On）] を選択します。
4. 確認メッセージで、[OK] をクリックします。
5. SSO パラメータを入力します。

シングルサインオン パラメータ	説明
[識別子フォーマット名を指定（Name Identifier Format）]	次から選択してください。 • urn:oasis:names:tc:SAML:1.1nameid-format:unspecified • urn:oasis:names:tc:SAML:1.1nameid-format:emailAddress • urn:oasis:names:tc:SAML:2.0nameid-format:persistent（デフォルト）
[SAML 2.0エンドポイント（HTTPリダイレクト）（SAML 2.0 Endpoint（HTTP Redirect））]	シングルサインオン プロバイダーから入手した SAML 2.0 エンドポイント URL を入力します。
[公開証明書（Public Certificate）]	シングルサインオン プロバイダーから受け取った証明書のテキスト全体を入力します。（コピーして貼り付けるのが最も簡単です）

6. [設定をテスト（Test Settings）] をクリックして、ID プロバイダーから提供されたエンドポイント URL と証明書の値を検証します。高度なフィッシング防御は、指定の場所にある公開証明書認証情報で ID プロバイダーを呼び出します。

   まだログインしていない場合は、ID プロバイダーによる認証が必要です。
7. [設定の保存（Save Settings）] をクリックします。
8. 確認メッセージで、[OK] をクリックします。
9. [情報を更新（Update Information）] をクリックします。

この時点で、シングルサインオンは有効になり、次のことが行われます。

- 既存のすべてのユーザーに電子メールが届き、高度なフィッシング防御にアクセスする際にはシングルサインオン ID プロバイダーのログイン情報を使用するように指示されます。

- 高度なフィッシング防御に現在ログインしているユーザーは、中断することなくセッションが継続されますが、今後ログインしようとするとIDプロバイダーのページが表示されます。

第 8 章

アプリケーション プログラミング インターフェイス

高度なフィッシング防御 にはアプリケーション プログラミング インターフェイス（API）が組み込まれているため、組織内の開発者は 高度なフィッシング防御 内のデータにプログラムでアクセスできます。

高度なフィッシング防御 API のエンドポイントでは、クエリ単位で結果の量が制限されています。この制限は、API ドキュメントにエンドポイントごとに記載されています。

- 高度なフィッシング防御 API は、RESTful の原則に基づいて JSON データ表現で構築されています。
- クライアントは、OAuth 2.0 プロトコルを使用して、API リクエストを認証します。

ユーザーアカウントに、API クライアント ID とクライアントシークレットで構成される 1 つの API 認証情報を割り当てることができます。こうした認証情報で利用できるリソースとデータは、アカウント管理者が 高度なフィッシング防御 ユーザーインターフェイスを使用してそのユーザーに割り当てた権限に直接結び付けられます。

Agari 開発者向けドキュメント（https://developers.agari.com/agari-platform）には、広範な情報が含まれています。ステップバイステップガイドとチュートリアルの両方があり、Agari API を対話形式で説明する完全なリファレンスとなっています。

API シークレットの生成

ユーザーが Cisco Domain Protection API を使用できるようにするには、事前にそのユーザーの API（アプリケーション プログラミング インターフェイス）認証情報（API シークレットとも呼ばれます）を生成する必要があります。

ユーザー管理者ロールを持つユーザーのみが、API 認証情報を生成できます。

1. [管理（Manage）] > [ユーザー（Users）] に移動します。
2. ユーザー名をクリックします。
3. [APIアクセスUID（API Access UID）] セクションで、[APIシークレットの生成（Generate API Secret）] をクリックします。
4. API シークレットを安全な場所にコピーして保存します。API をテストするときや、API 経由で Cisco 統合を使用しているときに、API ドキュメントページに入力する必要があります。

API ドキュメントの表示

高度なフィッシング防御 API（アプリケーション プログラミング インターフェイス）ドキュメントを表示する場合は、事前にユーザーアカウントの API 認証情報を生成する必要があります。詳細については、「「API シークレットの生成」上」を参照してください。

1. 高度なフィッシング防御 ページの右上で、自分の名前をクリックし、をクリックします。
2. 高度なフィッシング防御 をクリックします。