メッセージ

[メッセージ(Messages)] ページにはメッセージと検索結果が表示され、侵害の可能性を調べることができます。1 ページあたり最大 100 件のメッセージを表示できます。

[メッセージ(Messages)] ページのアイコン

次の表に、[メッセージ(Messages)] ページで使用されるアイコンとその意味を示します。

表 1　[メッセージ(Messages)] ページのアイコン

アイコン	名前	説明
	リンク	メッセージにリンクが含まれています。
	添付ファイル	メッセージに添付ファイルが含まれています
	手動で修正または手動で再分類	メッセージが手動で修正または再分類されました。メッセージが修正された場合は [アクション(Action)] の横に、メッセージが再分類された場合は [判定(Verdict)] の横にアイコンが表示されます。
	レトロスペクティブな判定	レトロスペクティブな判定が適用されました。レトロスペクティブな判定は、メッセージが Secure Email Threat Defense によって最初にスキャンされた後に適用されたものです。
	許可	メッセージが、指定された項目(許可リスト、MS 許可リスト、または安全な送信者)に基づいて許可されました。
	判定のオーバーライド	判定が、判定のオーバーライド メッセージ ルールに基づいてオーバーライドされました。
	バイパス分析	バイパス分析メッセージルールにより、メッセージが分析されませんでした。ルールのタイプ(安全な送信者またはフィッシングテスト)が指定されています。
	BEC	メッセージが手動で、または自動修復によってビジネスメール詐欺(BEC)としてマークされました。
	詐欺	メッセージが手動で、または自動修復によって詐欺としてマークされました。

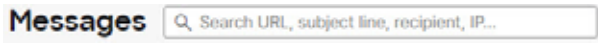
表 1　[メッセージ(Messages)] ページのアイコン(続き)

アイコン	名前	説明
	フィッシング	メッセージは、手動または自動修復によってフィッシングとしてマークされています。
	悪意あり	メッセージは、手動または自動修復によって悪意のあるものとしてマークされています。
	スパム	メッセージが手動または自動修復によってスパムとしてマークされました。
	グレイメール	メッセージがグレイメールとしてマークされています。グレイメールは、マーケティング、ソーシャル、またはジャンクと判断されたメールです。
	ニュートラル	メッセージがニュートラルとしてマークされています。
	着信	O365 テナント外から受信したメール。
	内部	O365 テナント内で送信されたメール。
	発信	O365 テナント外の受信者に送信されたメール。

検索およびフィルタ

カレンダーコントロールを使用して、定義された期間(直近の日、週、または月)のデータや、過去 90 日以内のカスタムタイムフレームのデータを表示します。

検索フィールドを使用して、文字列を検索したり、ハッシュや URL などの注目する指標を検索します。

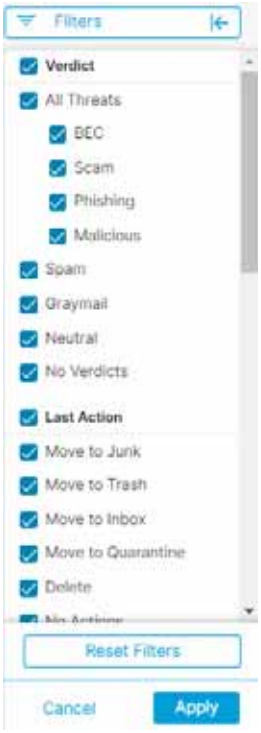


[フィルタ(Filter)] パネル

フィルタパネルを使用して検索を絞り込みます。たとえば、特定の送信者から送信されたすべてのメール、特定の判定のメール、添付ファイルやリンクがあるメール、再分類されたメール、[迷惑メール(Junk)] に移動されたメールなどを表示できます。

1. 矢印をクリックして、フィルタパネルを展開します。

2. 選択を行い、[適用(Apply)] をクリックします。[判定(Verdict)] の少なくとも 1 つの項目を選択する必要があることに注意してください。



フィルタをデフォルトにリセットには、[フィルタのリセット(Reset Filters)] ボタンを使用します。

メッセージグラフとクイックフィルタ

[メッセージ(Messages)] ページの上部にあるメッセージグラフとクイックフィルタは、メッセージトラフィックのグラフィカルビューを提供します。このグラフを使用して、メッセージをすばやくフィルタ処理します。グラフには、次のものが含まれています。

- 脅威とカテゴリのブレークアウトにより、合計を表示し、脅威を簡単にフィルタ処理します。
- 隔離された項目をフィルタ処理するために使用できる [隔離(Quarantine)] の合計
- 方向ですばやくフィルタ処理するために使用できる [メッセージの方向(Message Direction)] の合計

判定

Cisco Secure Email Threat Defense は、次の脅威判定をメッセージに適用します。

- [BEC]: ビジネスメール詐欺(BEC)は、ソーシャルエンジニアリングと侵入技術を使用して組織に経済的損害を与える高度な詐欺です。
- [詐欺(Scam)]: 詐欺は、宝くじ詐欺や強要詐欺などの手法を使用して、個人に経済的損害を与えることに焦点を当てています。

- [フィッシング(Fishing)]:これらのメッセージは、ユーザー名、パスワード、クレジットカード番号などの機密情報を取得しようとして、正規のサービスを不正にコピーまたは模倣したとして有罪判決を受けています。
- [悪意のある(Malicious)]:これらのメッセージは、悪意のあるソフトウェアの配信または拡散を含む、提供する、または支援するとして有罪判決を受けています。

レトロスペクティブな判定

レトロスペクティブな判定は、メッセージが Secure Email Threat Defense によって最初にスキャンされた後のある時点でメッセージに適用されたものです。

Secure Email Threat Defense のレトロスペクティブな判定は、他のシスコのセキュリティ製品とは若干異なります。Secure Email Threat Defense はインラインメールプロセッサではありませんが、メッセージの初期分析を完了するための固定の時間範囲があります。Talos のディープ URL 分析など、分析時間が長い新しいコンテンツエンジンは、レトロスペクティブな判定として扱われます。判定が遅れると、修復も遅れます。したがって、Secure Email Threat Defense はこれらの判定を明確にタグ付けします。

レトロスペクティブな判定は、[メッセージ(Messages)] ページの [判定(Verdict)] の隣に青いアイコンで示されます。アイコンにカーソルを合わせると、レトロスペクティブな判定が適用された時刻と、メッセージを受信した時刻と判定が適用された時刻の差異が表示されます。

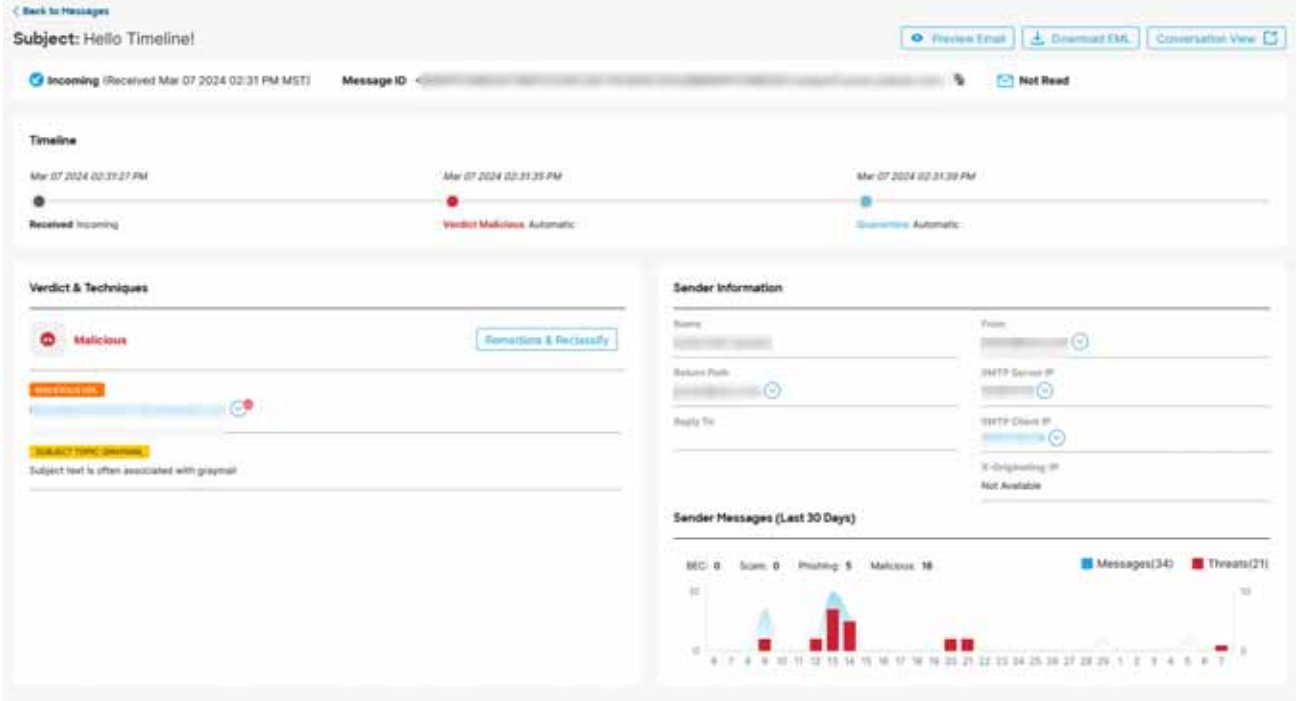
メッセージレポート

メッセージレポートを使用すると、メッセージに関する詳細を調査できます。**>** アイコンを選択するか、メッセージ行の任意の場所をクリックして、そのメッセージのレポートにアクセスします。

メッセージレポートには、次のようなメッセージに関する詳細が表示されます。

- メッセージの方向、Microsoft Message ID、および修復時にメッセージが開封されたかどうか
- タイムライン
- 判定と手法
- 送信者情報
- 送信者メッセージ
- 受信者、エンベロープ受信者、メールボックスなどの受信者情報
- リンク
- 添付ファイル
- 電子メールのプレビュー

メッセージレポートでは、カンバセーションビューや EML ダウンロードにもアクセスできます。



タイムライン

メッセージのタイムラインは、メッセージレポートに表示されます。

タイムラインには次の情報が表示されます。

- [受信(Received)]:メッセージを受信した時刻、およびメッセージの方向に関する詳細
- [ルール(Rule)]:適用されたメッセージルールに関する情報
- [判定(Verdict)]:示されたまたは適用された判定に関する情報と、アクションの実行者
- [アクション(Action)]:メッセージに対して実行されたアクションに関する情報と、アクションの実行者次の機能が含まれています。
  - メッセージの移動場所と移動方法
  - メッセージの修復エラーに関する情報と、エラーが発生したメールボックス

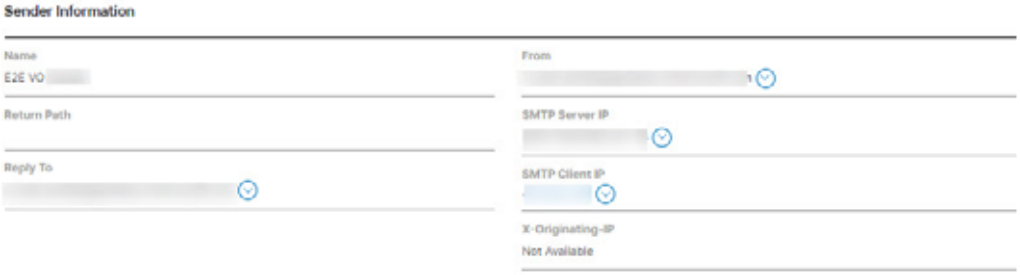
判定と手法

[判定と手法(Verdict and Techniques)] パネルには、メッセージに適用された判定と、検出された手法で判定に寄与した可能性があるものが視覚的に表示されます。手法は、その重大度を示すために色分けされています。悪意のあるファイルの名前/SHA256 および URL は、動的に表示されます(動的な表示が可能な場合)。動的テキストが使用できない場合は、静的な説明が表示されます。

このパネルから直接メッセージを修復または再分類できます。[修復と再分類(Remediate and Reclassify)] ボタンをクリックし、メッセージの移動と再分類(29 ページ)に記載されている手順に従います。

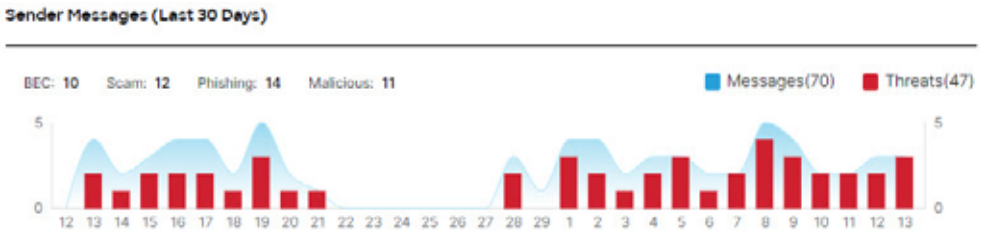
送信者情報

[送信者情報(Sender Information)] パネルには、名前、電子メールアドレス、リターンパス、返信先、SMTP サーバーとクライアントの IP、X-Originating IP など、メッセージの送信者に関する既知の情報が表示されます。



送信者メッセージ

[送信者メッセージ(Sender Messages)] グラフには、過去 30 日間にメッセージの送信者が送信したメッセージの合計数と脅威メッセージの合計数が表示されます。これにより、ユーザーからの脅威メッセージのパターンがあるかどうかをすばやく確認できます。

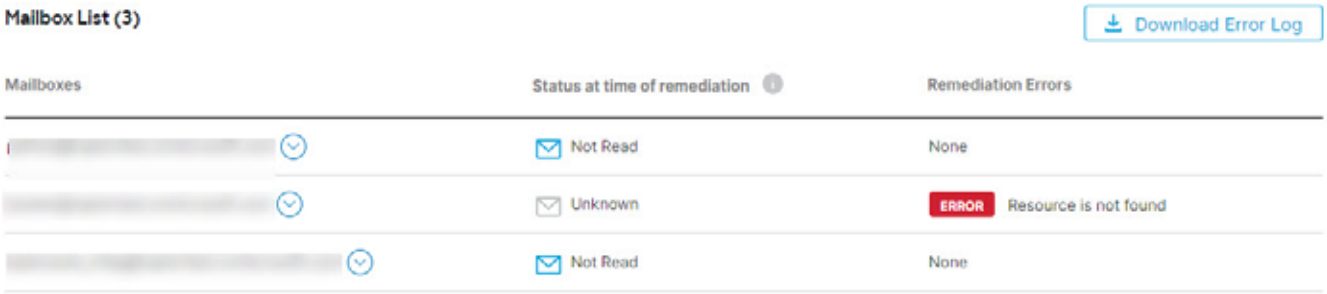


受信者情報

[受信者(Recipients)] パネルと [エンベロープ受信者(Envelope Recipients)] パネルには、メッセージの送信先に関する情報が表示されます。

メールボックスリスト

メールボックスリストには、着信メッセージと内部メッセージを受信したエンドユーザーのメールボックスのリストが表示されます。このリストには、メッセージが最後の修復アクションの前に開封されたかどうかと、メッセージの修復エラーも表示されます。修復エラーは、システムが修復を試みる前にユーザーがメッセージを削除または移動した場合に発生する可能性があります。

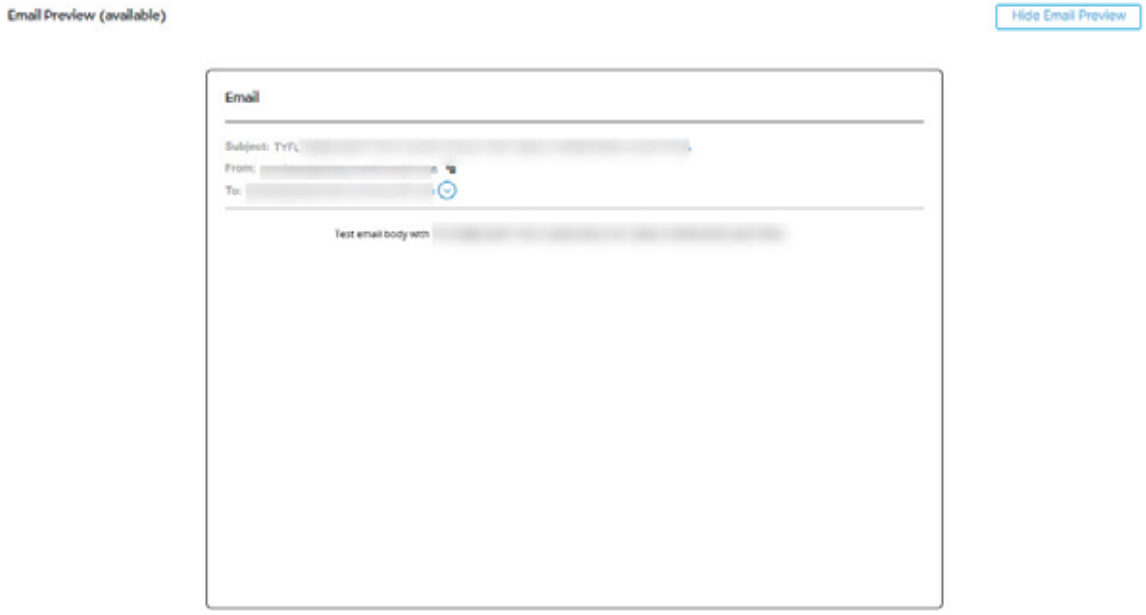


リンクと添付ファイル

[リンクと添付ファイル(Links and Attachment)] パネルには、メッセージ内で見つかったリンクと添付ファイルに関する情報が表示されます。

電子メールのプレビュー

電子メールプレビューを使用すると、ネットワーク管理者および管理者ユーザーは、EML ファイルをダウンロードすることなく、エンドユーザーに表示されるメッセージを要求して表示できます。メッセージはイメージとして表示されます。[電子メールプレビューを開く(Open Email Preview)] ボタンをクリックして、プレビューを表示します。



ユーザーがメッセージをプレビューすると、監査ログレコードが作成されます。監査ログは、[管理(Administration)] > [ビジネス (Business)] > [初期設定(Preferences)] からダウンロードできます。

カンバセーションビュー

カンバセーションビューでは、カンバセーションの全体ビューが表示されます。カンバセーションビューを使用して、カンバセーション内のメッセージを追跡し、メールフローを完全に把握します。これは、脅威の発生源と組織内で拡散する方法を判断するのに役立ちます。

メッセージレポートで、ページの右上にある [カンバセーションビュー(Conversation View)] ボタンをクリックして、特定の電子メールに関連するメッセージを表示します。

[+] アイコンをクリックしてカンバセーションのノードを展開すると、カンバセーションの前後のメッセージを確認できます。展開されたノードは、ノードの下に表示されるメッセージグリッドに追加されます。ノードとメッセージは、方向(着信、発信、または内部)を示すために色分けされています。

ノード円内の数字は、メッセージの送信先アドレス数を示します。ノード内のアイコンは、脅威が検出されたかどうか、または判定が適用されたかどうかを示します。ノードを選択すると、対応するメッセージがグリッド内で強調表示されます。

XDR ピボットメニュー

Cisco Secure Email Threat Defense ビジネスが Cisco XDR と統合されている場合、メッセージレポート内から XDR ピボットメニューにアクセスできます。XDR との統合の詳細については、XDR（55 ページ）を参照してください。

メッセージの移動と再分類

誤って分類されたと思われるメッセージを移動または再分類するには、[メッセージ（Messages）] ページを使用します。1 ページに表示されるメッセージ数を変更することで、一度に最大 100 件のメッセージを移動または再分類できます。[メッセージレポート（Message Report）] ページの [判定と手法（Verdict and Techniques）] パネルから直接メッセージを移動および再分類することもできます。

修復と再分類 API を使用して、メッセージを移動および再分類することもできます。詳細については、API ガイド（https://developer.cisco.com/docs/message-search-api/）を参照してください。

注: 再分類は、選択したメッセージの判定にのみ影響します。これは、選択した送信者からの今後のメッセージに対する、またはメッセージの内容に基づくアクションの変更を示すものではありません。メッセージは、Cisco Talos による確認のためにキューに入れられます。Talos は、今後の分類に影響を与えるためにこのフィードバックを使用する場合があります。誤検出メッセージについては、判定のオーバーライドルール（52 ページ）の追加を検討してください。

ハイブリッド Exchange アカウントについて

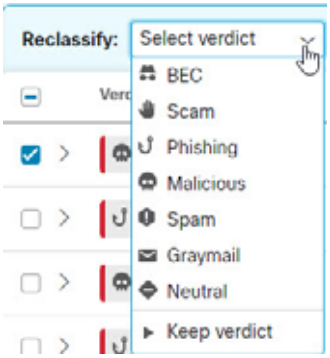
Secure Email Threat Defense は、Exchange Online（O365）に存在するメールボックス上でのみ動作します。メールボックスをオンプレミスの Exchange から Exchange Online（O365）に移行中の場合、修復（移動または削除）は、Exchange Online（O365）にあるメールボックスに対してのみ機能します。オンプレミスの Exchange メールボックスの修復が失敗したことは通知されません。

読み取り修復モード

読み取りモードでは、メッセージの再分類（異なる判定の適用）が可能です。

1. 再分類するメッセージを選択します。

2. ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



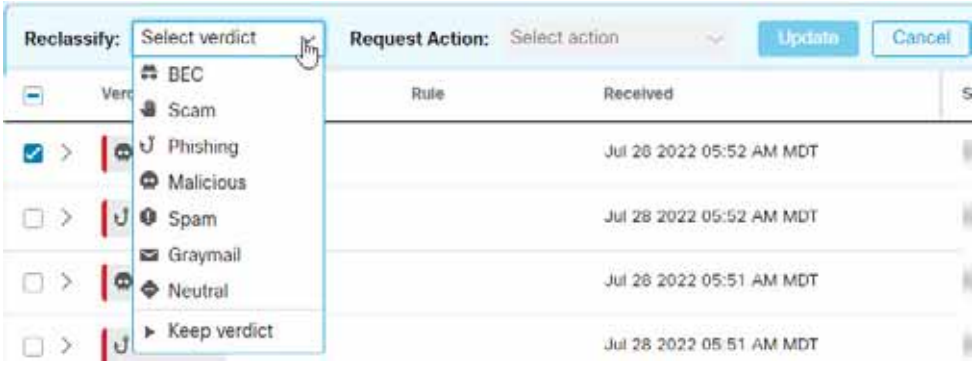
3. 新しい分類を適用するには、[更新(Update)] をクリックします。

読み取り/書き込み修復モード

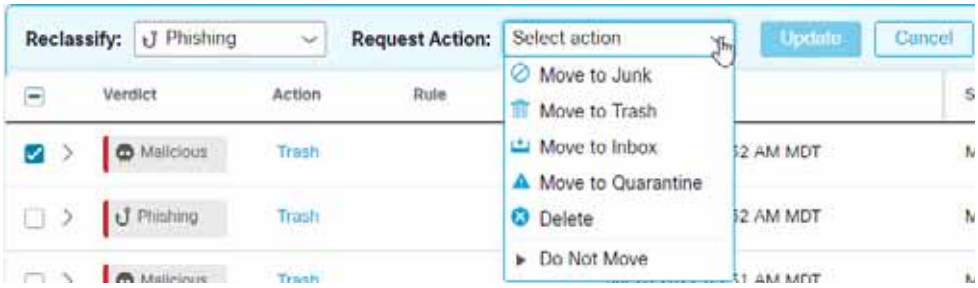
読み取り/書き込み修復モードでは、疑わしいメッセージをユーザーの受信トレイから迷惑メールまたはゴミ箱に移動するか、ユーザーがアクセスできない検疫フォルダに移動できます。同様に、迷惑メール、ゴミ箱、または検疫に移動されたメッセージが疑わしくないと判断した場合は、そのメッセージをユーザーの受信トレイに戻すことができます。メッセージを完全に削除することもできます。このプロセスでは、メッセージを再分類(異なる判定を適用)することもできます。

1. 移動または再分類するメッセージを選択します。

2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューからアクションを選択します。[迷惑メールに移動(Move to Junk)]、[ゴミ箱に移動(Move to Trash)]、[受信トレイに移動(Move to Inbox)]、[隔離に移動(Move to Quarantine)]、[削除(Delete)]、または [移動しない(Do Not Move)] を選択できます。



4. [更新(Refresh)] をクリックして新しい分類を適用し、メッセージに対してアクションを実行します。

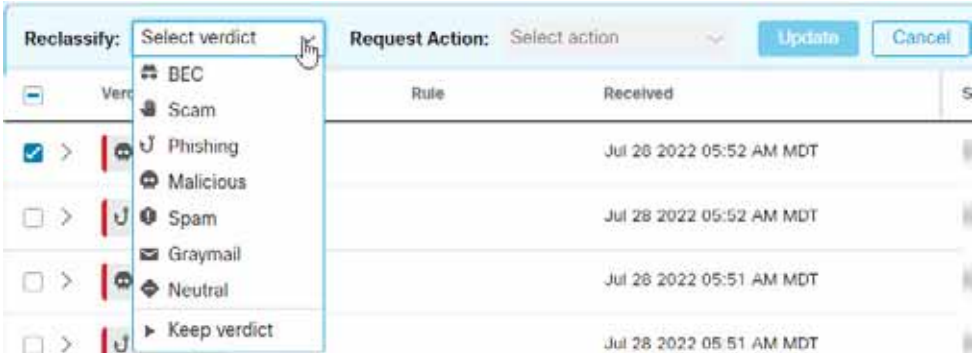
メッセージが移動された場合は、[最後のアクション(Last Action)] 列に示されます。

注: 発信メッセージと内部メッセージの場合、[受信トレイに移動(Move to Inbox)] アクションは、メッセージを受信トレイではなく、メッセージの最初の送信者の [送信済み(Sent)] フォルダに移動します。

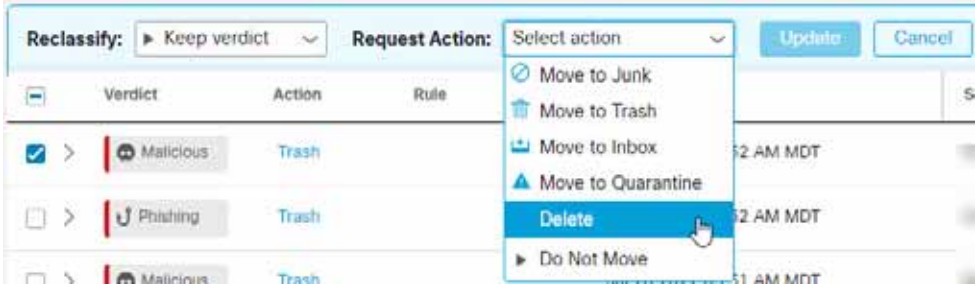
メッセージを削除する

スーパー管理者および管理ユーザーは、再分類/修正ワークフローの削除アクションを使用して、メールボックスからメッセージを完全に削除できます。削除されたメッセージは、**recoverableitemspurges** フォルダに移動されます。ユーザーはこのフォルダにアクセスできず、Secure Email Threat Defense では削除されたメッセージを受信トレイに復元できません。

1. 削除するメッセージを選択します。
2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] を選択できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [削除(Delete)] を選択します。



4. [更新(Update)] をクリックしてメッセージを削除します。
5. [削除の確認(Confirm Deletion)] ダイアログに、メッセージは復元できないことが表示され、続行するかどうか確認されます。続行するには、[削除(Delete)] をクリックします。

[最後のアクション(Last Action)] 列に削除が表示されます。

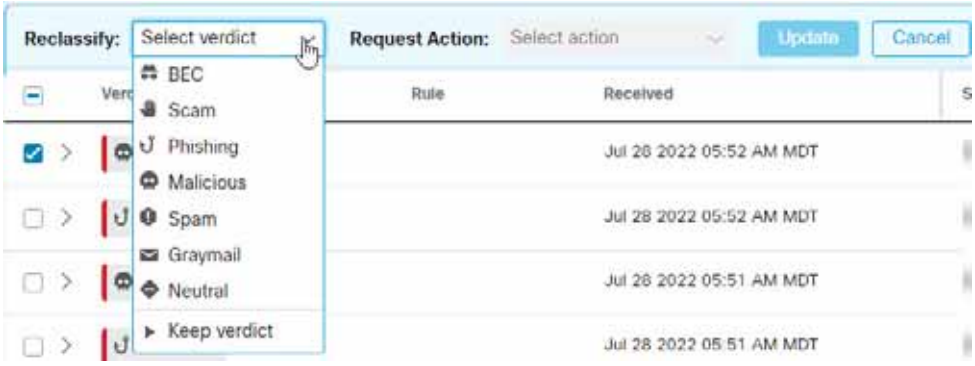
メッセージの隔離

検疫フォルダはメールボックスごとに自動的に作成され、Outlook ユーザーには表示されません。シークレットフォルダ名は、[管理(Administration)] > [ビジネス(Business)] ページで、ネットワーク管理者および管理者ユーザーに表示されます。Outlook では、検疫フォルダ内のメッセージは、削除済み項目の消去設定に従って自動的に消去されます。Secure Email Threat Defense では、検疫フォルダから消去されたメッセージをユーザーの受信トレイに復元することはできません。

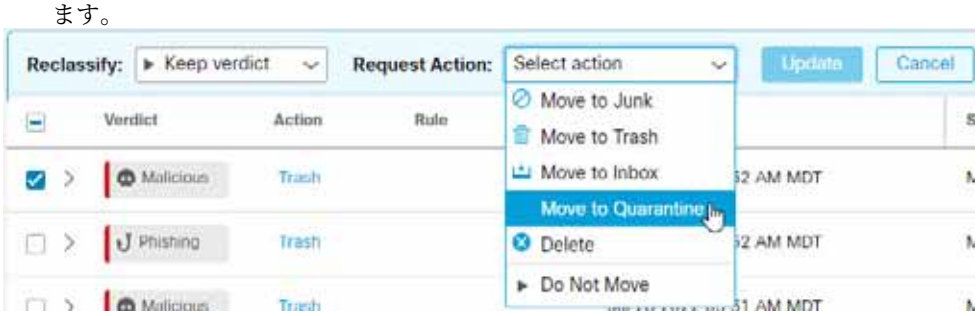
メッセージを手動で隔離に移動するには、次の手順を実行します。

1. 隔離に移動するメッセージを選択します。

2. [再分類(Reclassify)] ドロップダウンメニューから判定を選択します。メッセージは、[BEC]、[詐欺(Scam)]、[フィッシング(Phishing)]、[悪意のある(Malicious)]、[スパム(Spam)]、[グレイメール(Graymail)]、[ニュートラル(Neutral)] に再分類するか、または [判定を保持(Keep verdict)] できます。



3. [リクエストアクション(Request Action)] ドロップダウンメニューから [隔離に移動(Move to Quarantine)] を選択します。



4. [更新(Update)] をクリックして、メッセージを隔離します。

[隔離に移動(Move to Quarantine)] は、[最後のアクション(Last Action)] 列に表示されます。

検索結果のダウンロード

検索結果のメッセージに関するデータの CSV ファイルをダウンロードできます。ダウンロードは 10,000 メッセージに制限されています。データをダウンロードするには、次の手順を実行します。

1. [ダウンロード(Download)] ボタンをクリックし、[ダウンロードの作成(.csv)(Create Download (.csv))] を選択します。

2. 要求が進行中であることを示すバナーが表示されます。テキストをクリックして、[ダウンロード:メッセージ(Downloads: Messages)] ページに移動します。

3. ダウンロードの準備ができたら、[アクション(Actions)] 列の [ダウンロード(Download)] アイコンをクリックしてファイルをダウンロードします。

ダウンロード履歴

ダウンロード履歴は 90 日間保持されます。[ダウンロード(Download)] ボタンをクリックし、[ダウンロード履歴の表示(View Download History)] を選択して [ダウンロード:メッセージ(Download: Messages)] ページに移動します。

このページには、日付範囲、ダウンロードを要求したユーザー、ダウンロードが開始された日付、およびステータスが表示されます。[アクション(Actions)] 列の [ダウンロード(Download)] アイコンを選択して、ファイルをダウンロードします。

検索結果のダウンロード

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。