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。

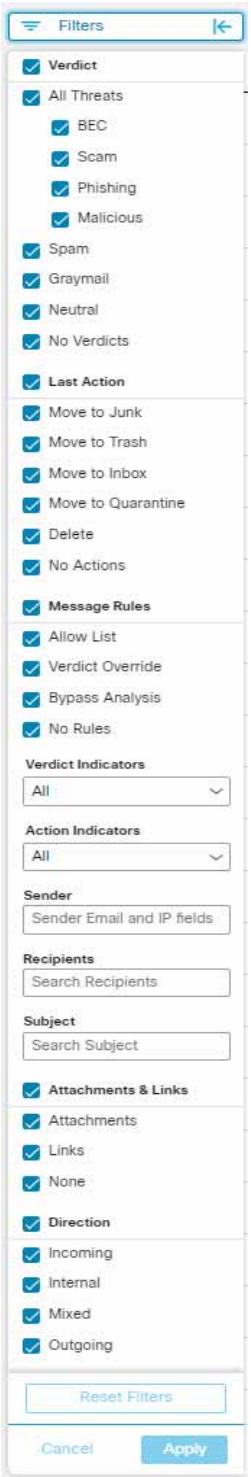
カレンダーコントロールを使用して、定義された期間(直近の日、週、または月)のデータや、過去 90 日以内のカスタムタイムフレームのデータを表示します。

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、または [迷惑メール(Junk)] に移動されたメールを表示できます。

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、[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(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。
	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。

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
	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。
	混合	内部および外部の受信者に受信されたメール。
	発信	O365 テナント外の受信者に送信されたメール。

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。

レトロスペクティブな判定の電子メール通知

レトロスペクティブな判定の電子メール通知をオンまたはオフにするには、次の手順を実行します。

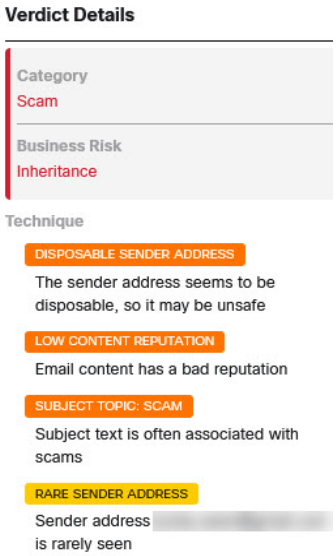
1. [設定(Settings)](歯車アイコン)> [管理(Administration)] > [ビジネス(Business)] を選択します。
2. [通知電子メールアドレス(Notification Email Address)] で、[レトロスペクティブな判定の通知を送信(Send Notifications for Retrospective Verdicts)] を選択または選択解除します。

このチェックボックスがオンの場合、レトロスペクティブな判定の電子メール通知が通知用に指定された電子メールアドレスに送信されます。これらの通知はデフォルトでオンになっています。

展開されたメッセージビュー

[メッセージ(Messages)] ページの検索結果内のメッセージを調査するには、[>] アイコンを選択してメッセージを展開し、判定の詳細、送信者 IP、Microsoft メッセージ ID、添付ファイル、リンクなどの詳細情報を確認します。このビューでは、タイムライン、カンバセーションビュー、EML ダウンロードにもアクセスできます。

[判定の詳細(Verdict Details)] 列には、判定、ビジネスリスク、使用された手法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。



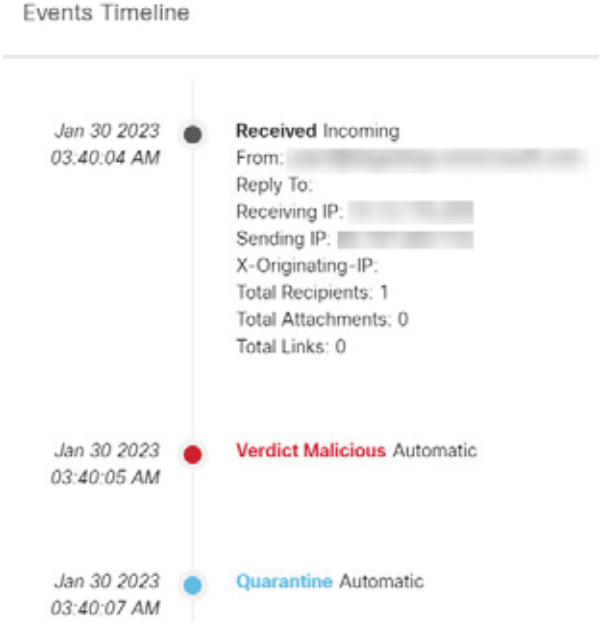
タイムライン

メッセージを展開したら、右隅にある [タイムライン(Timeline)] ボタンをクリックして、特定のメッセージのイベントタイムラインを表示します。

イベントタイムラインには次の情報が表示されます。

- [受信(Received)]:メッセージが受信された時刻、およびメッセージの詳細
- [判定(Verdict)]:示された判定に関する情報
- [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

- [ルール(Rule)]:適用されたメッセージルールに関する情報



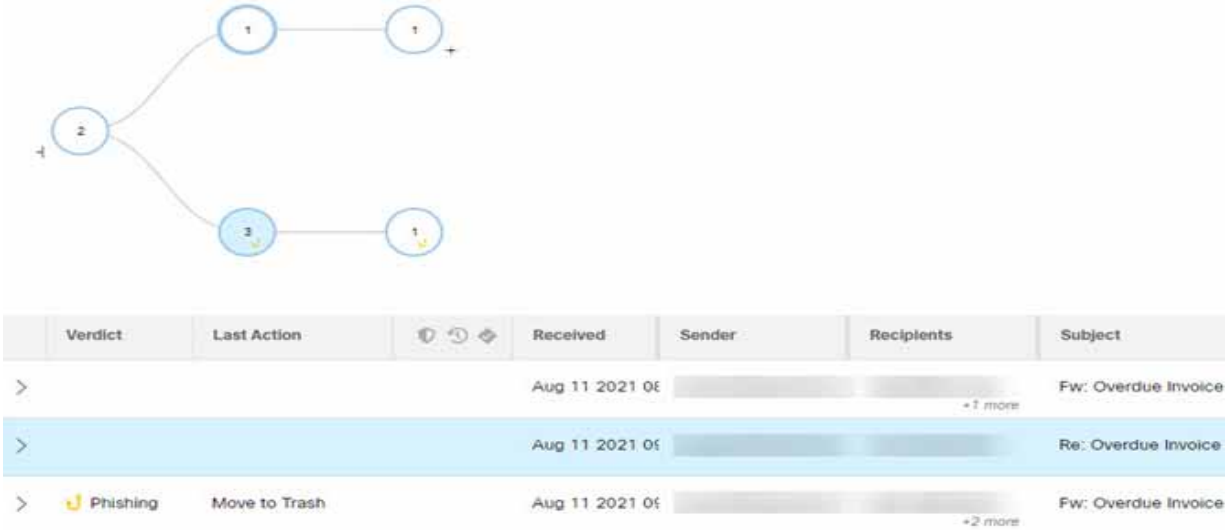
カンバセーションビュー

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。

メッセージを展開したら、[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、着信、発信、混合、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。



SecureX ピボットメニュー

Cisco Secure Email Threat Defense ビジネスが SecureX と統合されている場合、展開されたメッセージビュー内から SecureX ピボットメニューにアクセスできます。SecureX との統合については、SecureX（53 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。

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。選択した送信者からの今後のメッセージ、またはメッセージの内容に基づいた今後のメッセージへの変更は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。スパムまたはグレイメールメッセージの誤検出については、「判定のオーバーライドルール（50 ページ）」の追加を検討してください。

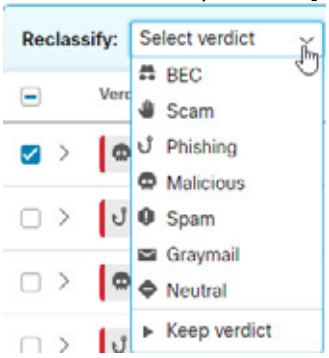
ハイブリッド Exchange アカウントについて

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。

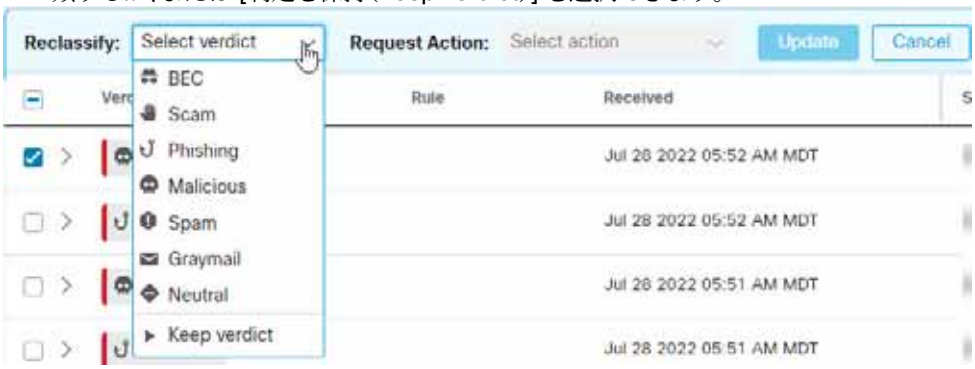


3. 新しい分類を適用するには、[更新（Update）] をクリックします。

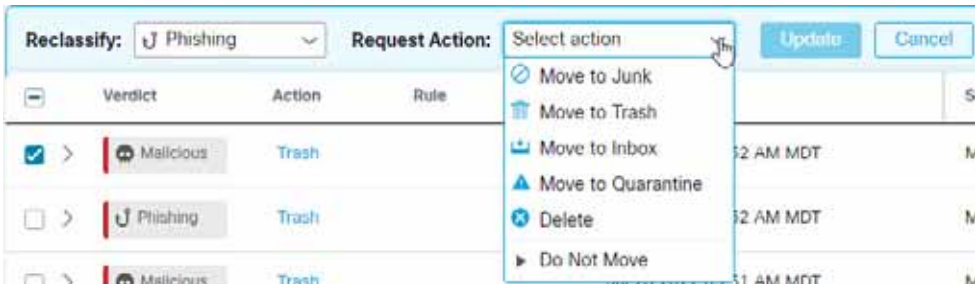
読み取り/書き込み修復モード

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。



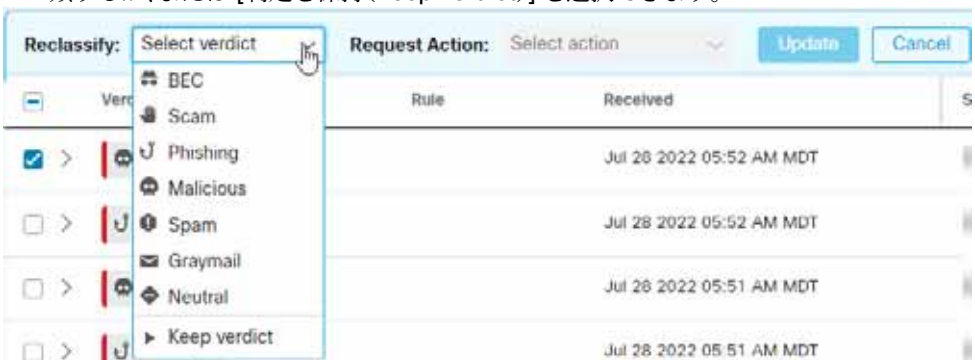
4. [更新(Refresh)] をクリックして新しい分類を適用し、メッセージに対してアクションを実行します。

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。

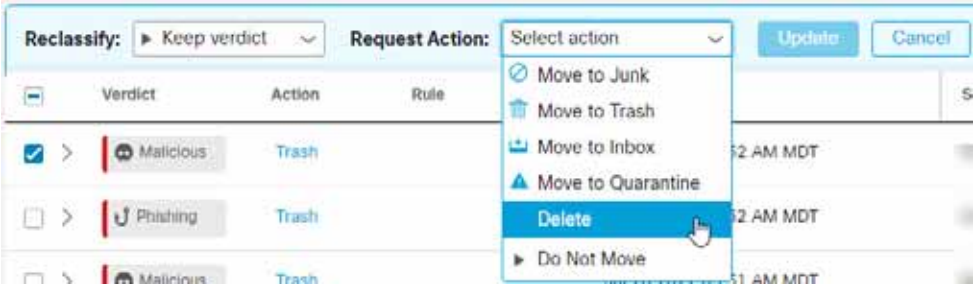
メッセージを削除する

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。

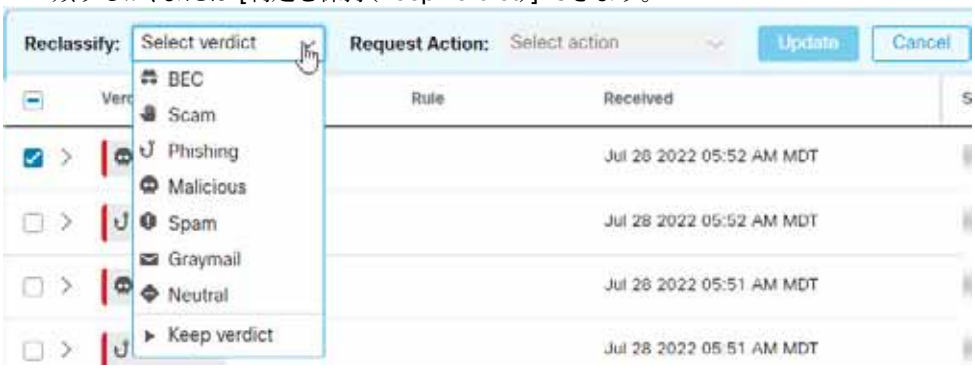
[最後のアクション(Last Action)] 列に削除が表示されます。

メッセージの隔離

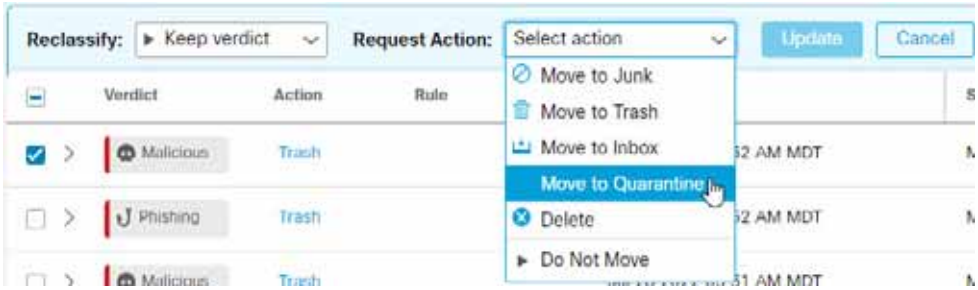
検疫フォルダはメールボックスごとに自動的に作成され、Outlook ユーザーには表示されません。シークレットフォルダ名は、[管理(Administration)] > [ビジネス(Business)] ページで、スーパー管理者および管理者ユーザーに表示されます。Outlook では、検疫フォルダ内のメッセージは、削除済み項目の消去設定に従って自動的に消去されます。Secure Email Threat Defense では、検疫フォルダから消去されたメッセージをユーザーの受信トレイに復元することはできません。

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。