Cisco Secure Email Cloud Mailbox
ユーザー ガイド

Contents

はじめに

Cisco Secure Email Cloud Mailbox（旧 Cloud Mailbox Defense（クラウド メールボックス））Microsoft 365 向けの統合型クラウドネイティブ セキュリティ ソリューションで、シンプルな導入、簡単な攻撃修復、優れた可視性に重点を置いています。

Cisco CES のお客様は、クラウド メールボックス のサブセットを内部メールボックス防御（IMD）として使用できます。IMD を使用すると、CES のお客様は内部メールをスキャンして修復できます。

要件

Cisco Secure Email Cloud Mailbox を正常に設定して使用するための要件は次のとおりです。

- クラウド メールボックス を購入し、ウェルカムメールを受信している。
- 次のいずれかのブラウザの最新バージョンを使用している。
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- グローバル管理者権限を持つ Microsoft 365 アカウント（設定用）。
- 配信不能なジャーナルレポートを受信できる Microsoft 365 環境の電子メールアドレスを所有している。使用される電子メールアドレスはジャーナリングされません。クラウド メールボックス の分析対象とするアドレスを使用しないでください。

ビジネスの設定

クラウド メールボックス ビジネスを設定するには、次の手順を実行します。次の手順は、**要件（9 ページ）**を満たしていることを前提としています。

1. シスコからのウェルカム メールの指示に従って、アカウントを設定します。

   クラウド メールボックス Cisco SecureX サインオンを使用してユーザ認証を管理します。SecureX サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。既存の SecureX Threat Response、Cisco Secure Malware Analytics（旧 Threat Grid）、または Cisco Secure Endpoint（旧 AMP）のお客様は、必ず既存のクレデンシャルでサインインしてください。既存のユーザでない場合は、新しい SecureX サインオンアカウントを作成するように求められます。

   これで、[Welcome to Cisco Cloud Mailbox Defense] ページにアクセスできます。

2. [Permission Mode] を選択します。

   [Permission Mode] は、適用できる修復ポリシーのタイプを定義します。[Permission Mode] には次の 2 つのオプションがあります。

   - [Audit]：可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。
   - [Audit with Enforcement]：可視性、およびオンデマンドまたは自動の修復（疑わしいメッセージの移動または削除）が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。

     注：[Audit with Enforcement] を選択した場合は、**ポリシー設定（15 ページ）**で [Automated Remediation] をオンにする必要があります。すべての内部電子メールに自動修復を適用するには、[Apply auto-remediation to domains not in the domain list] トグルを [On] に設定します。

3. Microsoft 365 に接続します。

   a. [Connect to Microsoft 365] をクリックします。

   b. 指示に従って、Microsoft 365 アカウントにログインします。Microsoft 365 でジャーナリングを設定するには、このアカウントにグローバル管理者権限が必要です。このアカウントは クラウド メールボックス で保存または使用されません。これらの権限が必要な理由については、Cisco Secure Email Cloud Mailbox の FAQ「Cloud Mailbox を設定するために Microsoft 365 グローバル管理者権限が必要なのはなぜですか。(Why are Microsoft 365 Global Admin rights required to set up Cloud Mailbox?)」を参照してください。

   c. [承認(Accept)] をクリックして、Cloud Mailbox アプリケーションの権限を承認します。クラウド メールボックス の設定ページにリダイレクトされます。

4. **Cisco Secure Email Gateway(SEG)を使用しているユーザーの場合**:Microsoft 365 にコネクタを追加します。

   ジャーナルが Cisco Secure Email Gateway を経由することなく、Microsoft 365 から Cloud Mailbox に直接送信されるようにするには、Microsoft 365 に送信コネクタを追加することをお勧めします。コネクタはジャーナルを設定する前に追加する必要があります。

   Microsoft 365 Exchange 管理センターから、[コネクタの追加(Add a connctor)] ウィザードの次の設定を使用して新しいコネクタを作成します。

   - [接続元(Connection from)]:Office 365
   - [接続先(Connection to)]:パートナー組織
   - [コネクタ名(Connector name)]:Cisco Secure Email Cloud Mailbox へのアウトバウンド([オンにする(Turn it on)] チェックボックスを選択)
   - [コネクタの使用(Use of connector)]:電子メールメッセージがこれらのドメインに送信される場合のみ(mail.cmd.cisco.com を追加)
   - [ルーティング(Routing)]:パートナーのドメインに関連付けられた MX レコードを使用
   - [セキュリティの制限(Security restrictions)]:接続を保護するために、常に信頼できる認証局(CA)によって発行されたトランスポート層セキュリティ(TLS)を使用します(推奨)。
   - [検証用の電子メール(Validation email)]:クラウド メールボックス の設定ページのジャーナルアドレス。

   注:設定が完了したら、[Cloud Mailbox ポリシー(Cloud Mailbox Policy)] ページで Cisco Secure Email Gateway(SEG)の存在を示す必要があります。詳細については、ゲートウェイを使用している場合のポリシー設定(17 ページ)を参照してください。

5. Microsoft 365 でジャーナリングを設定します。

   クラウド メールボックス にジャーナルを送信するように Microsoft 365 を設定する必要があります。これを行うには、ジャーナルルールを追加します。

   注:ジャーナルルールを設定すると、すぐにクラウド メールボックス バックエンドへのデータフローが始まります。デフォルトの クラウド メールボックス ポリシー設定が適用されます。ジャーナルルールを有効にしてから 10 ~ 60 分以内に、コンソールにデータが表示されます。

   注:最小限の Cisco Secure Malware Analytics(旧 Threat Grid)アカウントが作成され、ウェルカムメールが届きます。新しいアカウントは、既存のマルウェア分析/Threat Grid アカウントにリンクされていません。クラウド メールボックス を設定するためにマルウェア分析/Threat Grid アカウントで必要なアクションはありません。

   a. クラウド メールボックス の設定ページから、ジャーナルアドレスをコピーします。後でこのプロセスを繰り返す必要がある場合は、[管理(Administration)] ページでジャーナルアドレスを確認することもできます。

   b. Microsoft 365 管理センター(https://admin.microsoft.com/AdminPortal/Home#/homepage)に移動します。

      注:これらの手順は、従来の Exchange 管理センターを使用していることを前提としています。

c. [管理センター] > [Exchange] > [コンプライアンス管理] > [ジャーナルルール] の順に移動します。

d. [Send undeliverable journal reports to] フィールドに Exchange の受信者を追加します。使用される電子メールアドレスはジャーナリングされません。クラウド メールボックス の分析対象とするアドレスを使用しないでください。この目的で使用する受信者がいない場合は、受信者を作成する必要があります。

e. [+] ボタンをクリックして、新しいジャーナルルールを作成します。

f. クラウド メールボックス 設定ページからコピーしたジャーナルアドレスを [ジャーナルレポートの送信先(Send journal reports to)] フィールドに貼り付けます。

g. [Name] フィールドに **Cisco クラウド メールボックス** と入力します。

h. [If the message is sent to or received from] ドロップダウンから [Apply to All Messages] を選択します。

i. [Journal the following messages] ドロップダウンから適切なオプションを選択します。

– クラウド メールボックス のお客様の場合は、[すべてのメッセージ(All messages)] を選択してください。

– CES Internal Mailbox Defense(IMD)のお客様の場合は、[Internal messages only] を選択してください。

j. [保存(Save)] をクリックします。

6. クラウド メールボックス の設定ページに戻ります。[enable policy enforcement] をクリックします。

注:ジャーナルルールを有効にしてから 10 ~ 60 分以内にコンソールにデータが表示されます。テナント統合時からジャーナリングが完全に有効になるまでのこのキャッシングの遅延中に、Microsoft 365 から配信不能メッセージレポートを受信する場合があります。これらのメッセージは、システム統合が完了すると停止します。

ポリシー設定の確認または変更については、**ポリシー設定(15 ページ)**を参照してください。[監査と施行(Audit with Enforcement)] モードを選択した場合は、[自動修復(Automated Remediation)] 設定を確認する必要があります。すべての内部電子メールに自動修復を適用するには、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domain not in domain list)] がオンに設定されていることを確認します。

ドメインのインポート

ドメインをインポートして、特定のドメインに自動修復を適用できるようにします。Cloud Mailbox は、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] ボックスがオンかオフかによって、新しくインポートされたドメインを異なる方法で処理します。

- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオンになっている場合、インポートされるすべての新しいドメインに自動修復が適用されます。
- [ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] がオフになっている場合、インポートされる新しいドメインに自動修復は適用されません。

デフォルトでは、[ドメインリストにないドメインに自動修復を適用する(Apply auto-remediation to domains not in the domain list)] はオフになっています。

手動インポート

ドメインを手動でインポートするには、次の手順を実行します(ビジネスをセットアップするときに推奨):

1. [Settings](歯車アイコン)> [Policy] に移動します。
2. [インンポートされたドメインの更新(Update Imported Domains)] ボタンをクリックし、ドメインを クラウド メールボックス にインポートします。
3. 各ドメインの横にあるチェックボックスを使用して、そのドメインの自動修復設定を調整します。

4. また、[ドメインリストにないドメインに自動修復を適用する（Apply auto-remediation to domains not in the domain list）] をオンにして、自動修復がすべての内部メールと後で自動的にインポートされるドメインに適用されるようにすることもお勧めします。
5. [Save and Apply] をクリックします。

自動インポート

リストを最新にするために、ドメインは 24 時間ごとに自動的にインポートされます。

ポリシー設定

[設定(Settings)](歯車アイコン)> [ポリシー(Policy)] ページの設定によって、Cisco Secure Email Cloud Mailbox によるメールの処理方法が決まります。**ビジネスの設定(11 ページ)**の手順では、デフォルト設定が適用されます。設定を変更するには、変更を行い、[Save and Apply] ボタンをクリックします。

表 1　ポリシー設定

設定	説明	オプション	デフォルト
Permission Mode	適用できる修復ポリシーのタイプを定義します。	■ [Audit]:可視性のみを許可し、修復は許可しません。読み取り専用権限が Microsoft 365 から要求されます。 [Audit] を選択した場合は、[Attachment Analysis] および [Message Analysis] の方向をのみを設定する必要があります。その他のポリシー設定は適用されません。 ■ [Audit with Enforcement]:可視性、およびオンデマンドまたは自動の修復(疑わしいメッセージの移動または削除)が可能です。読み取り/書き込み権限が Microsoft 365 から要求されます。	ビジネスの設定時に選択します。 [Permission Mode] を変更すると、Microsoft 365 権限を再設定するようにリダイレクトされます。 ジャーナリングを設定するように指示される場合もあります。すでにジャーナリングを設定している場合は、この手順を省略できます。 **注**:[監査と施行(Audit with Enforcement)] モードを選択した場合は、[自動修復(Automated Remediation)] の設定も確認する必要があります。
Cisco Secure Email Gateway(SEG)	Cisco Secure Email Gateway(SEG)の有無は、Cloud Mailbox が送信者 IP を識別する方法に影響します。	■ [何も選択されていません(SEG はありません)(Nothing selected (No SEG))] ■ [SEG があります(SEG is present)] – [Cisco SEG のデフォルトヘッダーを使用する(Use Cisco SEG default header)] (X-IronPort-RemoteIP)。 – [SEG のカスタムヘッダーを使用する(Use Custom SEG header)]。使用するヘッダーを追加する必要があります。	[何も選択されていません(SEG はありません)(Nothing selected (No SEG))]。 この設定が有効になるまでに最大で 5 分かかることがあります。 詳細については、ゲートウェイを使用している場合のポリシー設定(17 ページ)を参照してください。
Message Analysis	動的に分析されるメッセージの方向。	■ **着信** ■ **発信** ■ **内部**	**すべて**

表 1　ポリシー設定（続き）

設定	説明	オプション	デフォルト
Attachment Analysis	Cisco Secure Malware Analytics（以前の Cisco Threat Grid）によって分析されるメールの添付ファイルの方向。	■ **着信** ■ **発信** ■ **内部**	**着信**
Remediation Actions	**悪意のある**、**フィッシング**、**スパム**、または**グレイメール**のコンテンツを含むことが判明したメッセージの修復アクション。	■ [隔離に移動（Move to Quarantine）] ■ [Move to Trash] ■ [Move to Junk] ■ [No Action] **注**：送信者アドレスが Exchange の送信者許可リストに属している場合、またはメッセージが Microsoft 365 によってすでに修復されている場合、修復アクションは適用されません。	■ 悪意がある：[隔離に移動（Move to Quarantine）] ■ フィッシング：[隔離に移動（Move to Quarantine）] ■ [Spam] - [Move to Junk] ■ [Graymail] - [No Action]
[安全な送信者（Safe Sender）]	このボックスがオンになっている場合、スパムまたはグレイメールと判定された安全な送信者メッセージ（Microsoft のジャーナルヘッダーにタグ付け）は修復されません。	**選択**または**選択解除**	**オフ**
Automated Remediation			
Domain-specific auto-remediation	特定のドメインに自動修復を適用します。	**選択**または**選択解除**	**選択解除**。[監査と施行（Audit with Enforcement）] モードをオンにする場合は、チェックボックスをオンに設定し、特定のドメインに自動修復が適用されるようにします。
Apply auto-remediation to domains not in the domain list above	ドメインが明示的にリストに含まれていない場合に適用されます。たとえば、新しいドメインが Microsoft 365 アカウントに追加されているが、クラウドメールボックス にインポートされていない場合などです。	**選択**または**選択解除**	**選択解除**。[監査と施行（Audit with Enforcement）] モードをオンにする場合は、このチェックボックスをオンに設定し、すべての内部電子メールに自動修復が適用されるようにします。

ゲートウェイを使用している場合のポリシー設定

Cisco E メール セキュリティ アプライアンスまたは同様のゲートウェイを配置している場合は、次のポリシー設定の使用を検討してください。

表 2　ゲートウェイで推奨されるポリシー設定

設定名	推奨される選択
Cisco Secure Email Gateway（SEG）	[SEG があります（SEG is present）]。ヘッダーを表示します
Message Analysis	[Outgoing] と [Internal]
Attachment Analysis	**なし**
Remediation Actions	■ 悪意がある：[隔離に移動（Move to Quarantine）] ■ フィッシング：[隔離に移動（Move to Quarantine）] ■ [Spam] - [Move to Junk]

Cisco Secure Email Gateway（SEG）があり、受信ジャーナルで SEG の識別に使用できるヘッダーを示すことで、Cloud Mailbox でメッセージの真の発信者を特定できるようにすることが重要です。この設定を行わないと、SEG から送信されたすべてのメッセージが表示され、誤検出が発生する可能性があります。

Cisco Secure Email Cloud Gateway（旧 CES）または Cisco Secure Email Gateway（旧 ESA）のヘッダーの確認または設定については、
https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox
を参照してください。

また、ジャーナルが Microsoft 365 から クラウド メールボックス に直接送信されるように、アプライアンスをバイパスすることを推奨します。バイパスするには、ビジネスの設定（11 ページ）で説明されているように、Microsoft 365 にコネクタを追加します。

CES IMD のお客様向けのポリシー設定

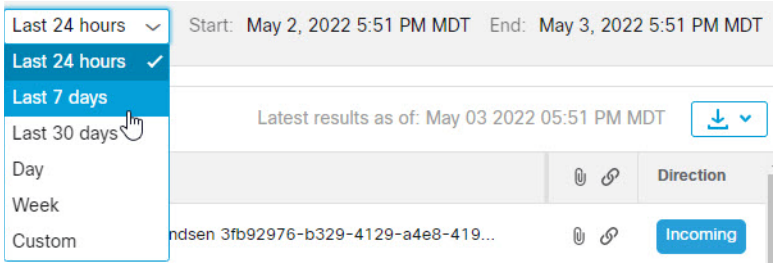
CES Internal Mailbox Defense（IMD）のお客様の場合、ポリシー設定は標準の クラウド メールボックス を使用している場合とは若干異なります。

- [メッセージ分析（Message Analysis）] は [内部（Internal）] に設定され、[ポリシー（Policy）] ページには表示されません。
- [Attachment Analysis] は、[Enabled] または [Disabled] に設定できます。これを [Enabled] に設定すると、内部添付ファイルがスキャンされます。
- 他のすべてのポリシー設定は、前のセクションで説明したとおりです。

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。

ドロップダウンメニューを使用して、既定の期間(過去 24 時間、過去 7 日間、過去 30 日間)のデータを表示するか、過去 90 日間の特定の日、週、またはカスタム時間枠を設定します。

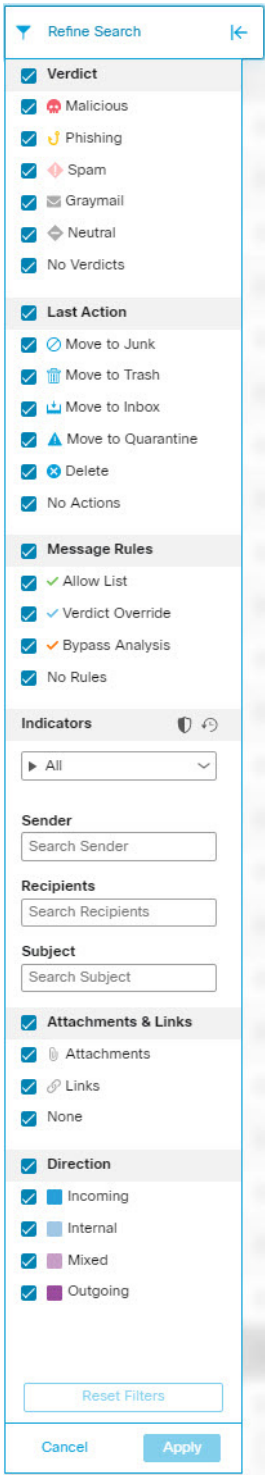


検索フィールドを使用して、文字列を検索したり、ハッシュや URL などの注目する指標を検索します。

[検索の絞り込み(Refine Search)] 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、または迷惑メール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。少なくとも 1 つの判定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。

Messages ページのアイコン

次の表に、[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　Messages ページのアイコン

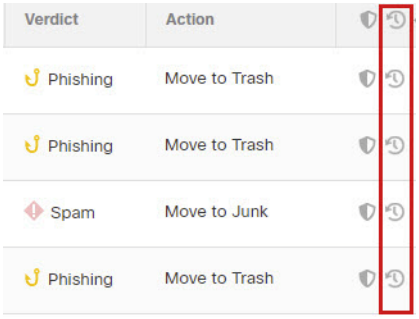
アイコン	名前	説明
	リンク	メッセージにリンクが含まれています。
	添付ファイル	メッセージに添付ファイルが含まれています
	自動修復	メッセージは クラウド メールボックス によって自動修復されました。
	レトロスペクティブな判定	レトロスペクティブな判定が適用されました。レトロスペクティブな判定は、メッセージが クラウド メールボックス によって最初にスキャンされた後に適用されたものです。
	許可	メッセージが、指定された項目（許可リスト、MS 許可リスト、または安全な送信者）に基づいて許可されました。
	判定のオーバーライド	判定が、判定のオーバーライド メッセージ ルールに基づいてオーバーライド 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。
	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。
	Spam	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。
	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。
	Graymail	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。

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 クラウド メールボックス 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。

クラウド メールボックス 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。クラウド メールボックス 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、クラウド メールボックス 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、次のように [メール(Messages)] ページに示されます。



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. [Settings](歯車アイコン)> [Administration] > [Business] を選択します。
2. [Notification Email Address] で、[Send Notifications for Retrospect Verdicts] を選択または選択解除します。

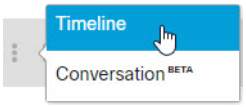
このチェックボックスがオンの場合、レトロスペクティブンな判定の電子メール通知が通知用に指定された電子メールアドレスに送信されます。これらの通知はデフォルトでオンになっています。

メッセージの調査

[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、送信者 IP、Microsoft メッセージ ID、添付ファイル、リンクなどの詳細を確認します。

Timeline

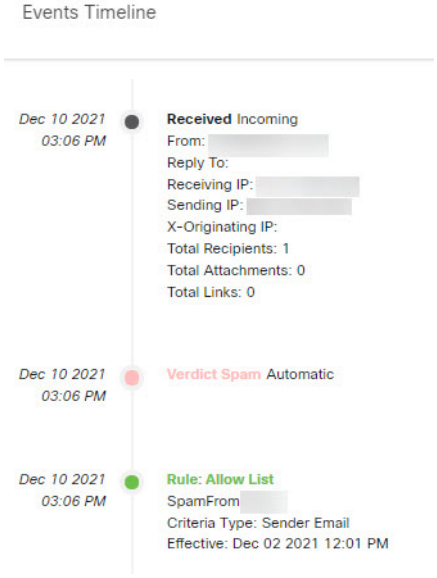
特定のメッセージのイベント タイムラインを表示するには、[More](縦の 3 つのドット)> [Timeline] を選択します。



イベント タイムラインには次の情報が表示されます。

- [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
- [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
- [メッセージルール(Message Rule)]: 適用されたルールに関する情報

- [ルール(Rule)]:適用されたメッセージルールに関する情報



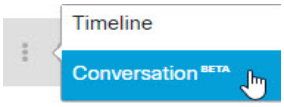
Conversation(ベータ)

注: この機能は現在ベータ版です。改善への取り組み中であるため、いくつか問題が発生する可能性があります。既知の問題は次のとおりです。

- 追加のメッセージがない場合でも、[+] 記号はクリックするまで表示されたままです。
- 水平ノードは 9 個に制限されています。

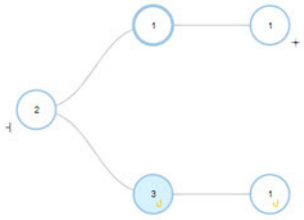
カンバセーションビューでは、カンバセーションの全体ビューが表示されます。カンバセーションビューを使用して、カンバセーション内のメッセージを追跡し、メールフローを完全に把握します。これは、脅威の発生源と組織内で拡散する方法を判断するのに役立ちます。

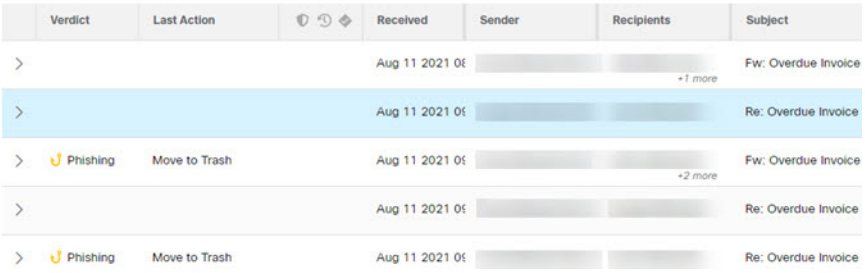
[More](縦の 3 つのドット) > [Conversation] を選択すると、特定の電子メールと繋がりがあるメッセージが表示されます。



ノード(青色で塗りつぶし)は、開始したメッセージを表します。[+] 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。





メッセージの移動と再分類

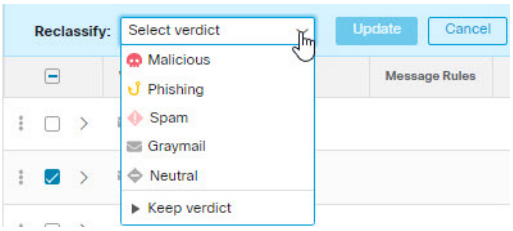
誤って分類されたと思われるメッセージを移動または再分類するには、[Messages] ページを使用します。1 ページに表示されるメッセージ数を変更することで、一度に最大 100 件のメッセージを移動または再分類できます。

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（44 ページ）をビジネスに追加することを検討してください。

Audit モード

[Audit] 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、[悪意のある（Malicious）]、[フィッシング（Phishing）]、[スパム（Spam）]、[グレイメール（Graymail）]、または [ニュートラル（Neutral）] に再分類できます。

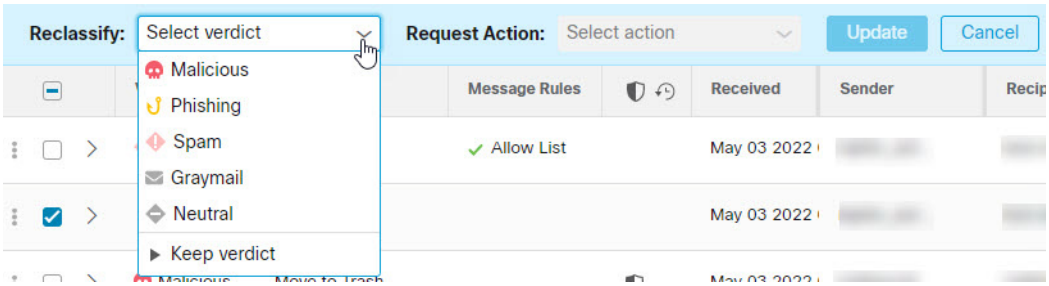


3. 新しい分類を適用するには、[更新（Update）] をクリックします。

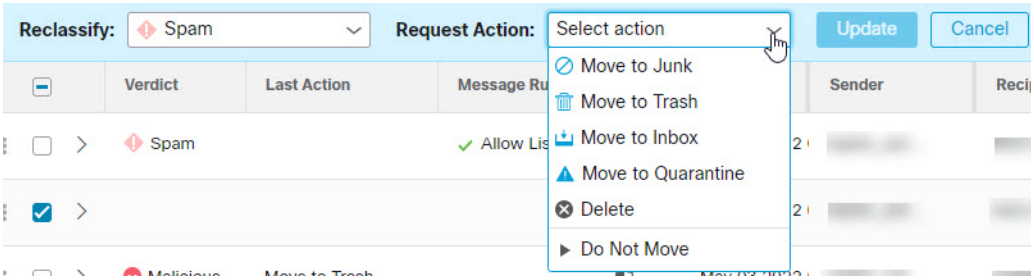
Audit with Enforcement モード

[Audit with Enforcement] モードでは、疑わしいメッセージをユーザの受信トレイから迷惑メール（Junk）またはゴミ箱（Trash）に移動できます。同様に、迷惑メールまたはごみ箱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、[悪意のある（Malicious）]、[フィッシング（Phishing）]、[スパム（Spam）]、[グレイメール（Graymail）]、または [ニュートラル（Neutral）] に再分類するか、または判定を保持することができます。



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。



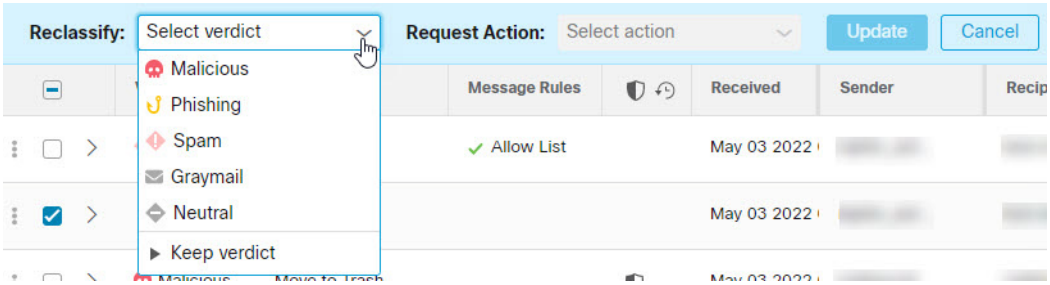
4. [更新（Refresh）] をクリックして新しい分類を適用し、メッセージに対してアクションを実行します。

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。

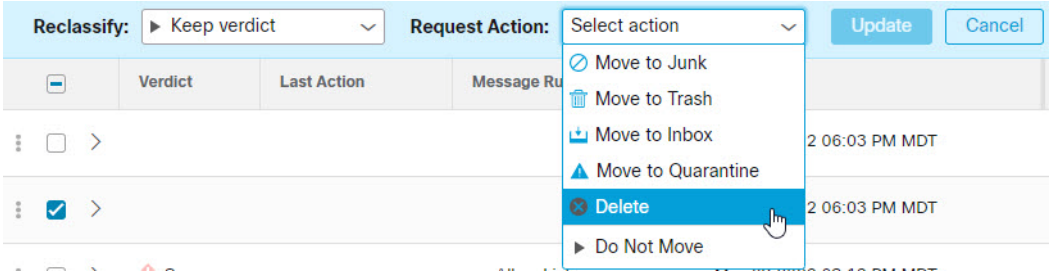
メッセージを削除する

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、Cloud Mailbox 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、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類するか、または判定を保持することができます。



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。

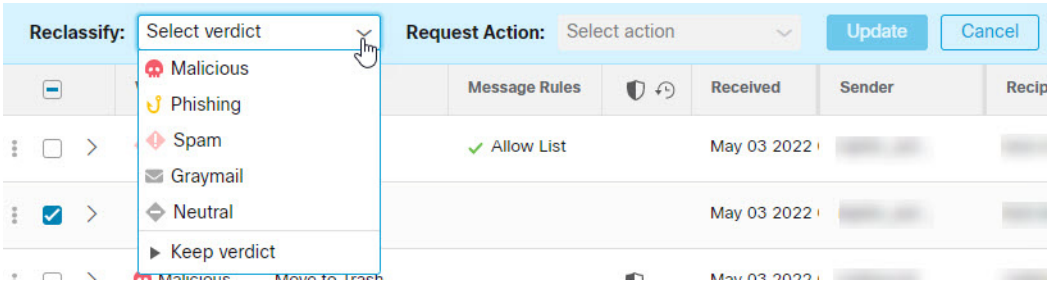
[最後のアクション(Last Action)] 列に削除が表示されます。この項目を選択または操作することはできません。

メッセージの隔離

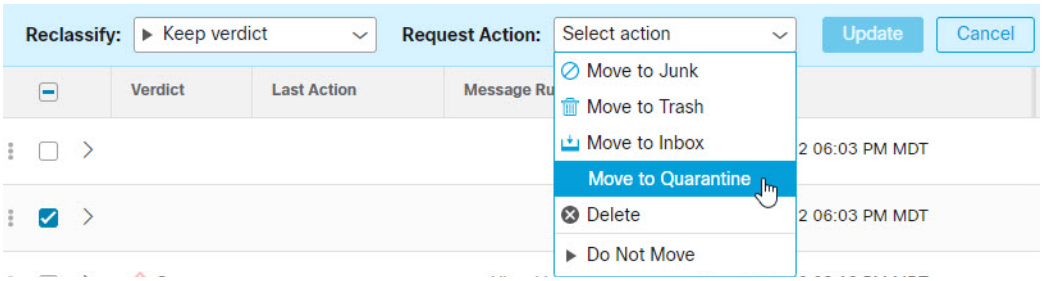
検疫フォルダはメールボックスごとに自動的に作成され、Outlook ユーザーには表示されません。シークレットフォルダ名は、[管理(Administration)] > [ビジネス(Administration)] ページで、スーパー管理者および管理者ユーザーに表示されます。Outlook では、検疫フォルダ内のメッセージは、削除済み項目の消去設定に従って自動的に消去されます。Cloud Mailbox では、検疫フォルダから消去されたメッセージをユーザーの受信トレイに復元することはできません。

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、[悪意のある(Malicious)]、[フィッシング(Phishing)]、[スパム(Spam)]、[グレイメール(Graymail)]、または [ニュートラル(Neutral)] に再分類するか、または**判定を保持**することができます。



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。

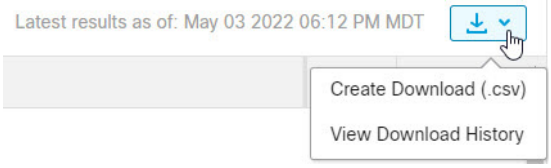
ハイブリッドアカウントについて

Cloud Mailbox 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。

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。

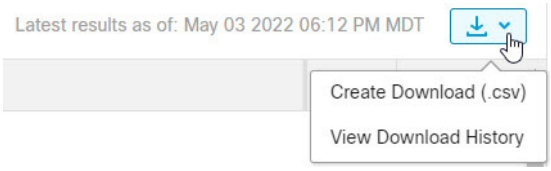


2. 要求が進行中であることを示すバナーが表示されます。テキストをクリックして、[ダウンロード履歴：メッセージ（Download History: Messages）] ページに移動します。

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、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。

ダウンロード

[設定(Settings)](歯車アイコン)> [ダウンロード(Downloads)] のページでは、検索結果の CSV と修復エラーログの CSV を作成および管理できます。

メッセージ

メッセージデータは次の 2 つの方法でダウンロードできます。

- 検索結果のダウンロード(28 ページ)で説明されているように、[メッセージ(Messages)] ページから。特定のフィルタリングされたデータまたは長期間のデータをダウンロードする場合は、このオプションを使用します。現在の検索結果とフィルタ結果にあるメッセージのデータの CSV ファイルを作成します。
- 以下で説明するように、[設定(Settings)](歯車アイコン)> [ダウンロード(Downloads)] > [メッセージ(Messages)] タブから。これは、過去 24 時間、過去 7 日間、特定の日や週など、特定の期間のすべてのメッセージデータをダウンロードする場合に便利です。

[ダウンロード(Downloads)] ページからメッセージデータの CSV を作成してダウンロードするには、次の手順を実行します。

1. [設定(Settings)](歯車アイコン)> [ダウンロード(Downloads)] を選択します。
2. [メッセージ(Messages)] を選択します。
3. [CSV を作成(Create CSV)] をクリックします。
4. 表示されるダイアログで、ダウンロードを作成する日付範囲を選択し、[CSV を作成(Create CSV)] をクリックします。
5. 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。

修復エラーログ

修復エラーログを使用すると、個々のメールボックスの修復失敗を調査できます。たとえば、メールボックスの所有者によってメッセージがすでに削除されている場合、Move to Trash リクエストは失敗する可能性があります。修復エラーログには、リソースが見つからないことが示されます。

修復エラーログを作成してダウンロードするには、次の手順を実行します。

1. [設定(Settings)](歯車アイコン)> [ダウンロード(Downloads)] を選択します。
2. [修復エラーログ(Remediation Error Log)] を選択します。
3. [CSV を作成(Create CSV)] をクリックします。
4. 表示されるダイアログで、ダウンロードを作成する日付範囲を選択し、[CSV を作成(Create CSV)] をクリックします。
5. 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。

修復エラーログ

インサイト

トレンド

[トレンド(Trends)] ページには、電子メールデータに関するグラフィカル情報が表示されます。

- ドロップダウンメニューを使用して、過去 24 時間、過去 30 日、または過去 90 日間の特定の日のデータを表示します。
- グラフ内の注目するデータをクリックすると、[Messages] ページのデータの詳細に移動します。
- 凡例項目をクリックして、[メッセージ(Messages)] ページの関連データに移動します。たとえば、[着信(Incoming)] をクリックすると、チャートに現在表示されているすべての着信メッセージが表示されます。
- ダウンロード ボタンをクリックして、トレンドデータをダウンロードします。結果は、次を含む CSV ファイルとしてエクスポートされます。
  - 過去 24 時間または特定の日を表示している場合、過去 90 日間のデータの 1 時間ごとのロールアップ
  - 過去 30 日間のデータを表示している場合、過去 90 日間のデータの 24 時間のロールアップ
- 印刷 ボタンをクリックして、[インサイト(Insights)] のチャートを印刷するか PDF として保存します。

タイムゾーンについて

[過去 24 時間(Last 24 Hours)] または 特定の [日(Day)] チャートの各棒は、1 時間分のデータを示します。これらのチャートは、ブラウザのローカルタイムゾーンに基づいています。

[過去 30 日間(Last 30 Days)] チャートの各棒は、1 日分(24 時間)のデータを示します。日は UTC 00:00 ~ 午後 11:59 を基準とし、ブラウザのローカル時間に変換されます。

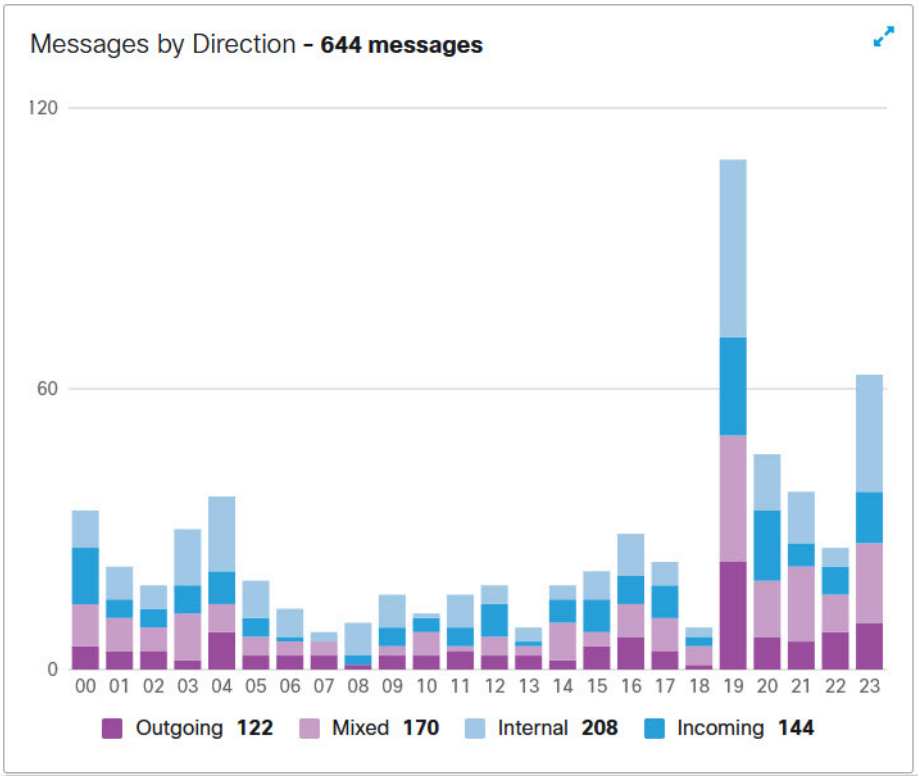
たとえば、太平洋夏時間（PDT）で UTC 07:00 の場合、[過去 30 日間（Last 30 Days）] チャートの棒は、3 月 24 日の午後 5 時から 3 月 25 日の午後 4 時 59 分までのデータを表示します。

Messages by Direction

[宛先別メッセージ（Messages by Direction）] グラフには、電子メールトラフィックの合計が表示されます。メールは、次のカテゴリに分かれています。

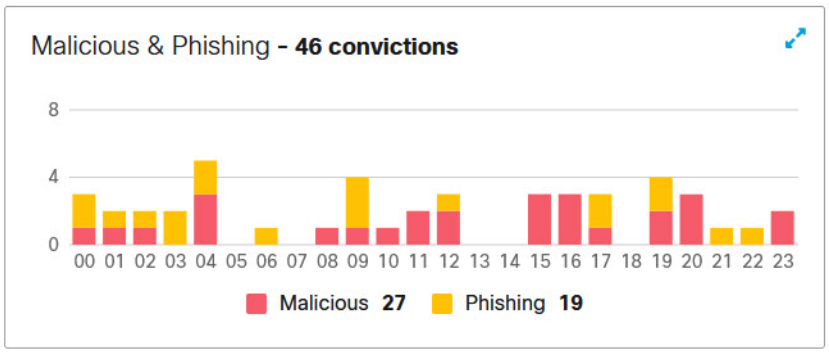
- [Outgoing]：社外の受信者に送信されたメール
- [Mixed]：社内および社外の受信者を含むメール
- [Internal]：社内に送信されたメール
- [Incoming]：社外から受信したメール

凡例には、各カテゴリのメッセージ数が表示されます。



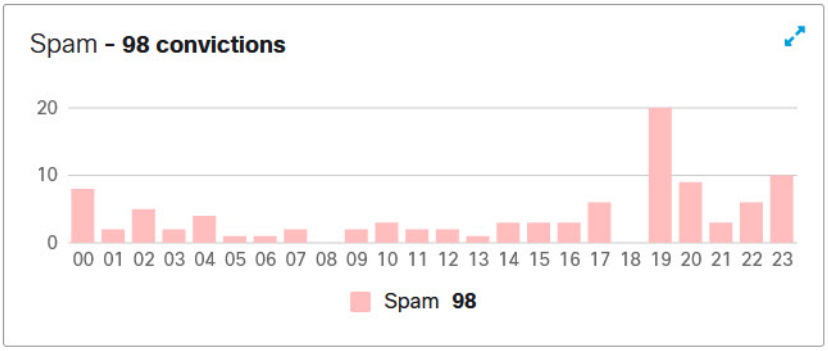
Malicious & Phishing

[悪意あり＆フィッシング（Malicious & Phishing）] グラフには、悪意のある、またはフィッシングであると判定されたメッセージのスナップショットが表示されます。凡例には、各カテゴリのメッセージ数が表示されます。データをクリックすると [Messages] ページに移動し、グラフ上のポインタの位置に応じて、悪意のあるメッセージまたはフィッシングメッセージが表示されます。



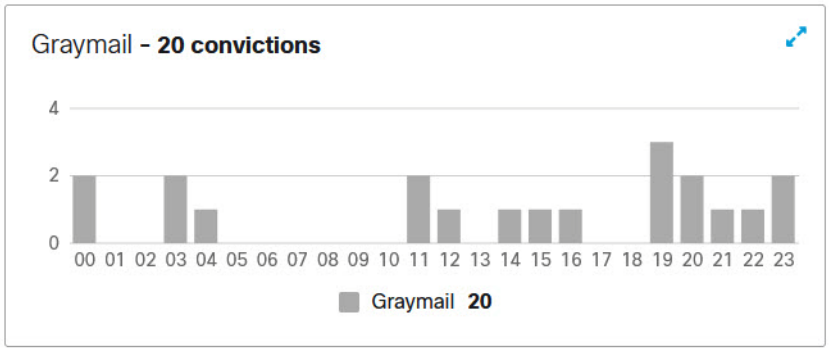
Spam

[スパム（Spam）] グラフには、スパムと判定されたメッセージのスナップショットが表示されます。凡例には、スパムと判定されたメッセージの総数が表示されます。



Graymail

[グレイメール（Graymail）] グラフには、グレイメールと判定されたメッセージのスナップショットが表示されます。凡例には、グレイメールと判定されたメッセージの合計数が表示されます。

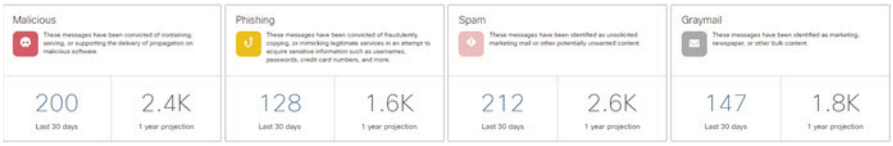


影響レポート

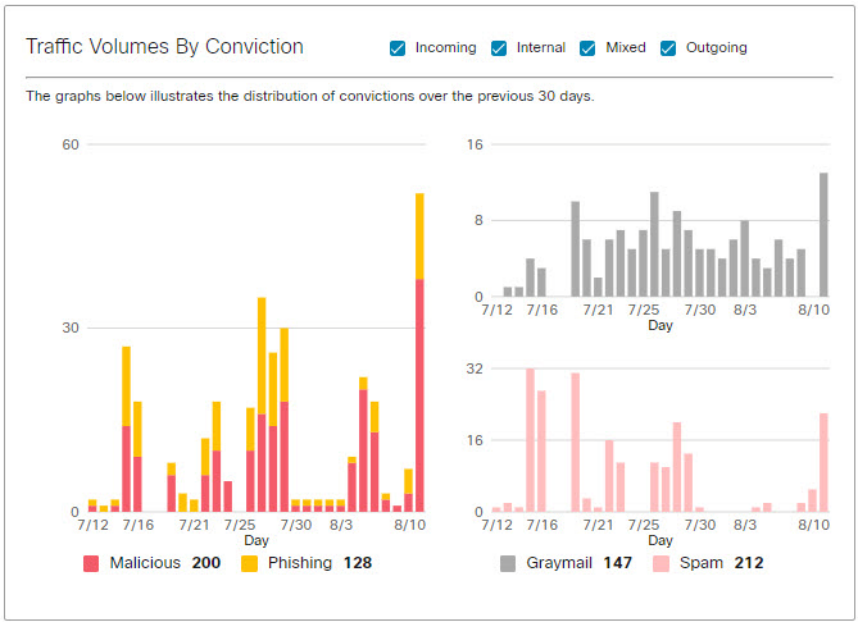
影響レポートには、過去 30 日間に クラウド メールボックス がビジネスにもたらしたメリットが表示されます。レポート内の注目するデータをクリックすると、[メッセージ（Messages）] ページのデータの詳細に移動します。

表示されるデータは次のとおりです。

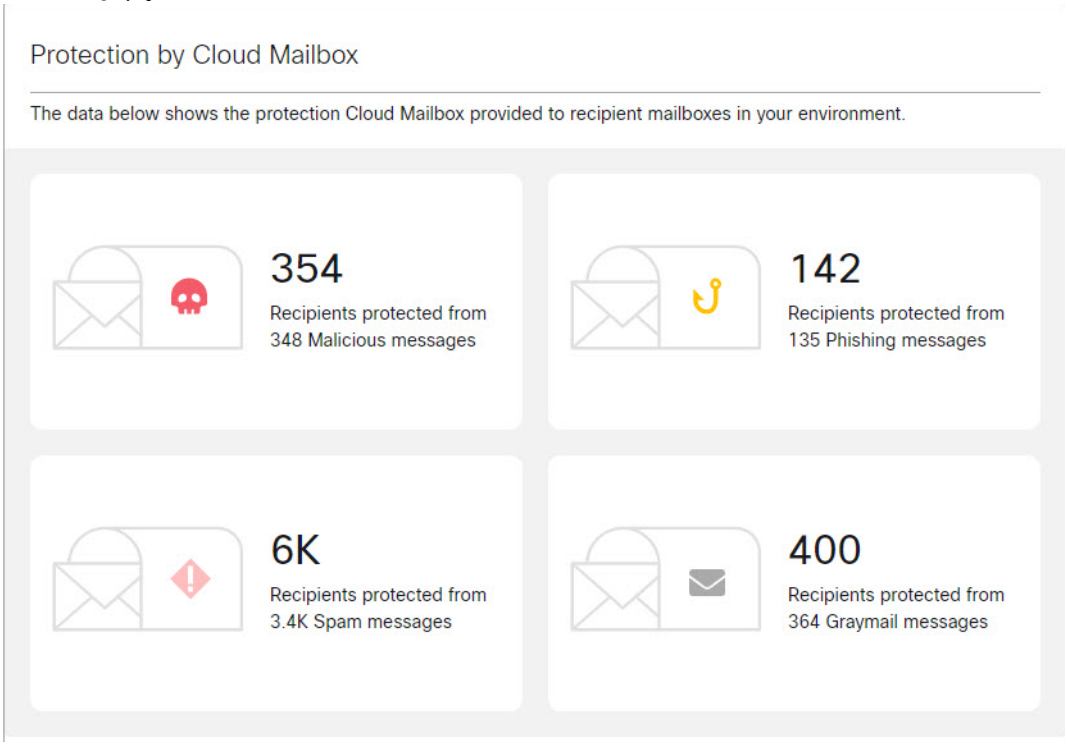
- 過去 30 日間に クラウド メールボックス で検出された悪意のある、フィッシング、スパム、およびグレイメールメッセージ、およびこのデータの 1 年間の予測。1 年間の予測は、1 日の平均に 365 を掛けて計算されます。



- [判定別トラフィック量（Traffic Volumes by Conviction）]。このチャートには、過去 30 日間の判定の分布が表示されます。このチャートは宛先別にフィルタ処理できます。

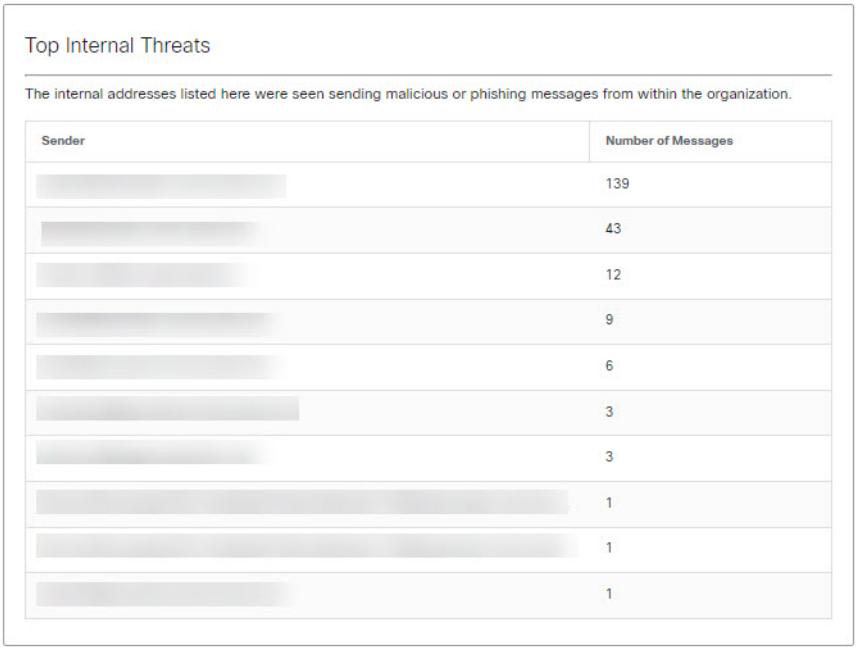


- Cloud Mailbox による保護。このチャートは、環境内の受信者のメールボックスに提供される保護 Cloud Mailbox を示しています。



- [悪意のあるメッセージとフィッシングメッセージのターゲット上位 10 件（Top Ten Targets of Malicious and Phishing Messages）]。このチャートには、悪意のあるメッセージとフィッシングメッセージの内部ターゲット上位 10 件が表示されます。

- [上位の内部の脅威（Top Internal Threats）]。このチャートには、悪意のあるメッセージまたはフィッシングメッセージの内部送信者上位 10 件が表示されます。


Top Internal Threats

The internal addresses listed here were seen sending malicious or phishing messages from within the organization.

Sender	Number of Messages
[redacted]	139
[redacted]	43
[redacted]	12
[redacted]	9
[redacted]	6
[redacted]	3
[redacted]	3
[redacted]	1
[redacted]	1
[redacted]	1

ユーザの管理

[設定(Settings)](歯車アイコン)> [管理(Administration)] ページからユーザーアカウントを管理します。

クラウド メールボックス ユーザ認証管理にシスコの SecureX サインオン SSO ソリューションを使用します。SecureX サインオンの詳細については、https://cisco.com/go/securesignon を参照してください。

注:既存の SecureX Threat Response、Cisco Secure Malware Analytics(旧 Threat Grid)、または Cisco Secure Endpoint(旧 AMP)のお客様は、必ず既存のクレデンシャルでサインインしてください。既存のユーザでない場合は、SecureX サインオン アカウントを新規に作成する必要があります。

SecureX サインオンを使用すると、他のタイプのアカウントでサインオンできますが、シスコのセキュリティ製品アカウントの接続状態を維持するために、SecureX サインオンアカウントを使用することをお勧めします。

ユーザ ロール

ロールベース アクセス コントロール(RBAC)により、アプリケーション内で異なるレベルの制御権またはアクセス権を持つユーザを設定できます。クラウド メールボックス 次の表に示すロールに属するユーザを作成できます。

表 1　　ユーザ ロール

ロール	説明
super-admin	これらのユーザは、クラウド メールボックス のすべての機能にアクセスできます。設定やポリシーの変更、メッセージの再分類や修復が可能です。
admin	これらのユーザーは、スーパー管理者または管理者ユーザーを作成、編集、または削除できないことを除いて、スーパー管理者のすべての機能を備えています。
アナリスト	これらのユーザーは、検索およびインサイト機能を使用できます。メッセージの再分類と修復はできますが、ユーザーのメールボックスからメッセージを削除することはできません。ビジネス設定やポリシーを変更したり、新しいユーザーを作成したりすることはできません。
read-only	これらのユーザーは、検索およびインサイト機能を使用できます。メッセージの再分類や修復、ビジネス設定やポリシーの変更、新規ユーザーの作成はできません。

注:既存のユーザーのロールは編集できません。ユーザーのロールを変更する場合は、既存のユーザーを削除してから、同じ電子メールアドレスと目的のロールを持つ新しいユーザーを作成します。

新規ユーザの作成

次の手順を実行して、新規ユーザを作成します。

1. [Settings](歯車アイコン) > [Administration] > [Users] の順に選択します。
2. [新規ユーザを追加(Add New User)] をクリックします。
3. ユーザのログイン情報を入力し、ロールを選択して、[Create] をクリックします。

   注:ユーザの電子メールアドレスは、そのユーザの SecureX サインオンアカウントの電子メールアドレスと *一致する必要があります*。

ユーザに「**Welcome to CiscoCisco Secure Email Cloud Mailbox**」という件名の電子メールが配信されます。ユーザは電子メールの指示に従って SecureX サインオンアカウントをセットアップし（まだアカウントを持っていない場合）、ログインする必要があります。

ユーザの削除

ユーザを削除するには、次の手順を完了します。

1. [Settings]（歯車アイコン）> [Administration] > [Users] の順に選択します。
2. ユーザ名の横にあるごみ箱アイコンをクリックします。
3. [Confirm Deletion] ダイアログで [Delete] をクリックし、アクションを完了します。

削除が完了したことを示すステータスメッセージが表示されます。これにより、ユーザのアカウントが クラウド メールボックス から削除されますが、ユーザの SecureX サインオンアカウントは削除されません。

管理設定

このセクションで説明する管理設定には、[設定（Settings）]（歯車アイコン） > [管理（Administration）] > [ビジネス（Business）] からアクセスできます。

アカウントの詳細情報

アカウントの詳細セクションには、ビジネスの次の識別子が表示されます。

- Microsoft 365 のテナント ID
- ジャーナルアドレス
- 会社 ID
- 検疫フォルダ ID
- サブスクリプション ID のサポート

また、ライセンスタイプ、サブスクリプション ID、シート数、およびライセンスの開始日と終了日を示すライセンス情報テーブルも含まれています。

初期設定

[設定（Preferences）] セクションには、通知電子メールアドレス、監査ログへのアクセス、および Google Analytics の設定が含まれます。

通知メール

通知電子メールアドレスは、シスコが クラウド メールボックス に関する電子メールを送信するアドレスです。たとえば、システムの更新、新機能、定期メンテナンスなどに関する通知を送信する場合があります。最初にビジネスの初期ユーザの電子メールに設定されます。

レトロスペクティブな判定の通知を通知電子メールアドレスに送信するかどうかを選択できます。レトロスペクティブな判定がメッセージに適用されると、電子メールが送信されます。

監査ログ

過去 3 ヵ月の監査ログを CSV ファイルとしてダウンロードできます。ドロップダウンから日付範囲を選択し、[CSV のダウンロード（Download CSV）] をクリックします。

Google Analytics

Google アナリティクスは、クラウド メールボックス を設定して利用規約に同意すると、最初に有効または無効になります。有効にすると、シスコは個人を特定できない使用状況データ（送信者、受信者、件名、URL など）が収集して、そのデータを Google アナリティクスと共有する場合があります。このデータにより、シスコは クラウド メールボックス がユーザのニーズにどのように対応しているかをよりよく理解できるようになります。

SecureX

Cloud Mailbox は SecureX と統合されています。SecureX を使用すると、他のシスコセキュリティ製品からのデータと一緒に Cloud Mailbox の情報を確認することができます。この設定の詳細については、**SecureX との統合（47 ページ）**を参照してください。

ユーザー設定

個々のユーザープロファイルの設定には、[ユーザー（User）]（プロフィールアイコン）> [ユーザー設定（User Settings）] からアクセスできます。

詳細

詳細セクションには、ユーザー名、役割、および組織が含まれています。

初期設定

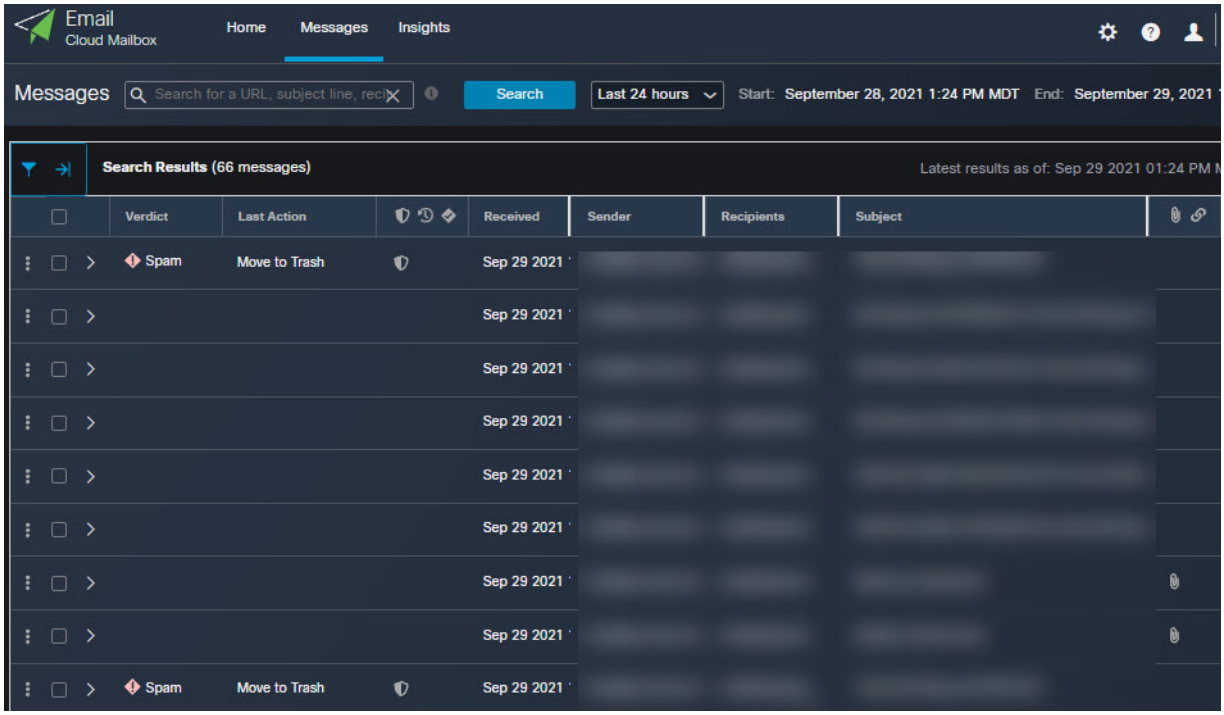
[初期設定（Preferences）] セクションには、SecureX リボンの承認とテーマの外観設定が含まれます。

SecureX のリボン

Cloud Mailbox は SecureX リボンと統合されています。リボンを使用すると、シスコのセキュリティ製品間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりできます。SecureX リボンはユーザーごとに承認されます。詳細については、SecureX との統合（47 ページ）を参照してください。

テーマ

Cloud Mailbox の表示を明るい背景または暗い背景とするように選択できます。モードを切り替えるには、[ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] > [初期設定(Preferences)] > [テーマ(Theme)] に移動します。このガイドの画像は、通常、ライトテーマで表示されます。暗い背景(Dusk)を下に示します。

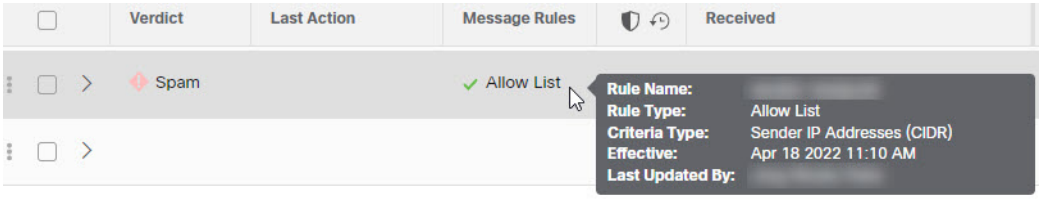


メッセージ ルール

メッセージルールを使用すると、一部のタイプのメッセージを修復またはスキャンしないように指定できます。許可リストルール、判定のオーバーライドルール、およびバイパス分析ルールを作成できます。バイパス分析ルールは、フィッシングテストまたはセキュリティメールボックス用に作成できます。

[設定(Settings)] > [メッセージルール(Message Rules)] ページから、メッセージルールを作成および管理します。

バイパス分析ルールは、許可リストルールと判定のオーバーライドルールよりも優先されます。メッセージがルールの影響を受ける場合は、[メッセージ(Messages)] ページの [メッセージルール(Message Rules)] 列に表示されます。[メッセージルール(Message Rules)] 列の項目にカーソルを合わせると、適用されたルールが表示されます。



許可リストルール

許可リストルールを使用すると、特定の送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレスからのスパムおよびグレイメールメッセージの修復を防ぐことができます。メッセージは引き続き分析されますが、自動修復は適用されません。たとえば、Cloud Mailbox で特定の送信者からの項目がスパムであると判断されたが、その項目をユーザーの受信トレイに残しておきたい場合は、許可リストルールを作成して該当するメッセージを修正するポリシーをオーバーライドできます。許可リストルールは、ポリシーの例外として機能します。許可リストルールに一致するメッセージは、引き続き影響レポートに表示されます。

許可リストルール:

- グレイメールおよび/またはスパムに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス(IPv4 または CIDR ブロック)を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、またはアドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

判定のオーバーライドルール

判定のオーバーライドルールを使用すると、ルールで指定された基準に一致するスパムおよびグレイメールの判定をオーバーライドできます。メッセージは「ニュートラル（Neutral）」判定とマークされ、修正されません。判定がオーバーライドされたメッセージは、影響レポートに表示されません。

判定のオーバーライドルール：

- グレイメールおよび/またはスパムに適用します。
- 許可された送信者の電子メールアドレス、送信者のドメイン、または送信者の IP アドレス（IPv4 または CIDR ブロック）を指定します。
- ルールごとに最大 50 の基準を設定できます。つまり、50 個の電子メールアドレス、ドメイン、または IP アドレスを設定できます。

アクティブなルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

バイパス分析ルール

バイパス分析ルールを使用すると、フィッシングテストまたはセキュリティ メールボックス メッセージの分析をバイパスできます。ルール基準を満たすメッセージによってすべてのエンジン分析がバイパスされるため、エンジンに干渉することなくセキュリティテストを処理できます。添付ファイルとリンクは、Cloud Mailbox によって開いたりスキャンされたりしません。

フィッシングテストルール：

- 指定した送信者の電子メールアドレス、送信者のドメイン、または IP アドレス（IPv4 または CIDR ブロック）から送信されたすべての受信メッセージに適用します。メッセージは分析されません。
- ルールごとに最大 50 の基準を設定できます。

セキュリティ メールボックス ルール：

- 指定した受信者の電子メールアドレスの受信メッセージに適用します。メッセージは分析されません。

  注：指定した受信者がメッセージの唯一の受信者である場合、セキュリティ メールボックス ルールが適用されます。他の受信者がコピーされているか、BCC（ブラインドカーボンコピー）として含まれている場合、メッセージは分析エンジンをバイパスしません。
- ルールごとに最大 50 の基準を設定できます。

アクティブなバイパス分析ルールは 20 に制限されています。ルールは非アクティブ化できますが、削除することはできません。

メッセージルールの追加

メッセージルールを追加する手順は、ルールのカテゴリによって若干異なります。

新しい許可リストまたは判定のオーバーライドルールの追加

新しいルールを作成するには、次の手順を実行します。

1. [設定（Settings）]（歯車アイコン）> [メッセージルール（Message Rules）] を選択します。
2. 作成するルールのカテゴリを、[許可リスト（Allow List）] または [判定オーバーライド（Verdict Override）] のいずれかから選択します。

3. [新規ルールの追加(Add New Rule)] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 基準のタイプを選択します。[送信者の電子メール(Sender Email)]、[送信者のドメイン(Sender Domain)]、[送信者の IP アドレス(IPv4)(Sender IP Addresses (IPv4))]、または [送信者の IP アドレス(CIDR)(Sender IP Addresses (CIDR))] を選択できます。
6. 許可された項目をコンマで区切って入力します。
7. 許可する判定に応じて、[スパム(Spam)] および/または [グレイメール(Graymail)] を選択します。
8. [送信(Submit)] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

新しいバイパス分析ルールの追加

新しいルールを作成するには、次の手順を実行します。

1. [設定(Settings)](歯車アイコン)> [メッセージルール(Message Rules)] を選択します。
2. [バイパス分析(Bypass Analysis)] を選択します。
3. [新規ルールの追加(Add New Rule)] ボタンをクリックします。
4. ルール名を作成します。各ルールには固有の名前が必要です。
5. 作成するルールタイプを、[フィッシングテスト(Phish Test)] または [セキュリティメールボックス(Security Mailbox)] のいずれかから選択します。
6. [フィッシングテスト(Phish Test)] ルールの場合は、基準タイプを [送信者の電子メールアドレス(Sender Email Addresses)] または [送信者のドメイン(Sender Domains)]、[送信者の IP アドレス(IPv4)(Sender IP Addresses (IPv4))]、[送信者の IP アドレス(CIDR)(Sender IP Addresses (CIDR))] のいずれかから選択します。次に、コンマで区切って項目を入力します。

   [セキュリティメールボックス(Security Mailbox)] ルールの場合は、受信者の電子メールアドレスをコンマで区切って入力します。
7. [送信(Submit)] をクリックして、ルールの作成を終了します。

ルールがリストに追加されます。変更が適用されるまでに最大で 20 分かかる場合があります。

ルールの編集

編集できるのは有効なルールのみです。規則を編集するには、次の手順を実行します。

1. [設定(Settings)](歯車アイコン)> [メッセージルール(Message Rules)] を選択します。
2. 編集するルールのタイプを選択します。
3. [アクション(Action)] 列で、編集するルールの横にある鉛筆アイコンをクリックします。
4. 必要な変更を行ったら、[変更の保存(Save Changes)] をクリックします。

ルールが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

ルールの有効化または無効化

既存のルールを有効または無効にするには、次の手順を実行します。

1. [設定(Settings)](歯車アイコン)> [メッセージルール(Message Rules)] を選択します。
2. 有効または無効にするルールのタイプを選択します。
3. [アクション(Action)] 列で、ステータスを変更するルールの横にある有効または無効アイコンをクリックします。

ルールのステータスが更新されます。変更が適用されるまでに最大で 20 分かかる場合があります。

Microsoft 許可リストと安全な送信者

クラウド メールボックス は、スパムおよびグレイメールメッセージに関して、Microsoft 365 のスパムフィルタ許可リストに追加された送信者とドメインを受け入れます。MS 許可リストは、悪意の判定やフィッシング判定では適用されません。詳細については、「Cisco Secure Email Cloud Mailbox FAQ: Cloud Mailbox and Microsoft 365」を参照してください。

個々のユーザーがメールボックス内の許可リストを設定することを組織が許可し、メッセージがユーザーの許可リストに含まれる場合、Microsoft 許可リストが Cloud Mailbox で常に適用されることはありません。Cloud Mailbox でこれらの設定を適用する場合は、[ポリシー(Policy)] ページの [スパムまたはグレイメールと判定された Microsoft Safe Sender メッセージを修復しない(Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts)] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、悪意とフィッシングの判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

SecureX との統合

Cisco SecureX は、シスコのセキュリティ製品を統合プラットフォームに接続します。Cloud Mailbox は、SecureX および SecureX リボンと統合されています。

- SecureX を使用すると、他のシスコセキュリティ製品からのデータと一緒に Cloud Mailbox の情報を確認することができます。
- SecureX リボンを使用すると、シスコのセキュリティ製品間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりできます。

本書に記載されていない SecureX の詳細については、SecureX のドキュメントを参照してください：
https://securex.us.security.cisco.com/help/securex/topic/introduction

SecureX

Cloud Mailbox には、SecureX ダッシュボードで表示できる次のタイルがあります。

- [宛先別メッセージ（Messages by direction）]：電子メールトラフィックの合計が宛先別に表示されます。電子メールは、[送信（Outgoing）]、[混合（Mixed）]、[内部（Internal）]、および [受信（Incoming）] に分けられます。
- [悪意ありおよびフィッシング（Malicious & Phishing）]：悪意のある、またはフィッシングであると判定されたメッセージのスナップショットが表示されます。
- [スパム（Spam）]：スパムと判定されたメッセージのスナップショットが表示されます。
- [グレイメール（Graymail）]：グレイメールと判定されたメッセージのスナップショットが表示されます。

SecureX ダッシュボードの詳細については、SecureX のドキュメントを参照してください：
https://securex.us.security.cisco.com/help/securex/topic/dashboard

Cloud Mailbox Business 向けに SecureX を承認する

SecureX for Cloud Mailbox を承認する前に、SecureX アカウントを持ち、SecureX 組織の一員である必要があります。詳細については、SecureX のドキュメントを参照してください：
https://securex.us.security.cisco.com/help/securex/topic/introduction

注：Cloud Mailbox アカウントは、一度に 1 つの SecureX 組織とのみ統合できます。

Cloud Mailbox のスーパー管理者および管理者ユーザーは、Cloud Mailbox Business 向けに SecureX モジュールを承認できます。

1. [設定（Settings）]（歯車アイコン）> [管理（Administration）] > [Business] を選択します。
2. [初期設定（Preferences）] > [SecureX] で、[SecureX 統合の承認（Authorize SecureX Integration）] をクリックします。
3. 承認フローを完了します。

SecureX 設定が成功したことを示すバナーが表示されます。

SecureX ダッシュボードに Cloud Mailbox のタイルを追加できるようになりました。その手順については、SecureX のドキュメントを参照してください：https://securex.us.security.cisco.com/help/securex/topic/configure-tiles

Cloud Mailbox Business 向けの SecureX 認証を取り消す

注:スーパー管理者または管理者ユーザーがこのタスクを実行できます。Business 向けに SecureX を承認したユーザーでなくてもこのタスクを実行できます。

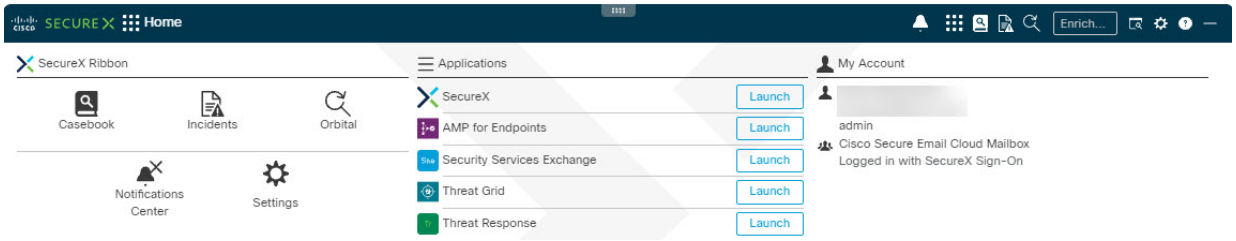
Cloud Mailbox Business 向けの SecureX 認証を取り消すには、次の手順を実行します。

1. [Settings](歯車アイコン)> [Administration] > [Business] を選択します。
2. [初期設定(Preferences)] > [SecureX] で、[承認を取り消す(Revoke Authorization)] をクリックします。

SecureX 設定が正常に更新されたことを示すバナーが表示されます。

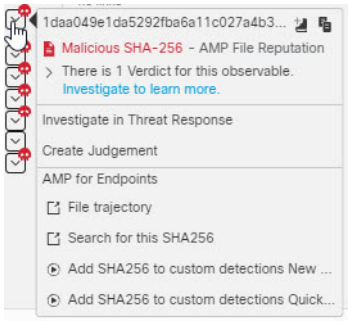
SecureX のリボン

SecureX リボンはページの下部に配置されており、ご使用環境内で Cloud Mailbox と他のシスコセキュリティ製品間を移動しても保持されます。すべての Cloud Mailbox ユーザーは、SecureX リボンの使用を承認できます。リボンを使用して、シスコのセキュリティ アプリケーション間を移動したり、ケースブックにアクセスしたり、オブザーバブルを検索したり、インシデントを表示したりします。



SecureX リボンの詳細については、SecureX のドキュメントを参照してください:
https://securex.us.security.cisco.com/help/securex/topic/ribbon

リボンを承認すると、Cloud Mailbox の展開メッセージ ビュー内に SecureX ピボット メニューが追加されます。これらのメニューは、購入したシスコのセキュリティ製品に応じて、各オブザーバブルに関する追加情報にアクセスするための中心地点となります。



SecureX ピボット メニューの詳細については、SecureX のドキュメントを参照してください:
https://securex.us.security.cisco.com/help/securex/topic/pivot-menu

SecureX リボンの承認

SecureX リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューからリボンを承認できます。

注:リボンを承認する前に、SecureX アカウントをアクティブ化する必要があります。これを行うには、Cloud Mailbox Business 向けに SecureX を承認する(47 ページ)の指示に従うか、他のモジュールを SecureX に統合します。

SecureX リボン内からの承認

リボン内から SecureX リボンを承認するには、次の手順を実行します。

1. SecureX リボンで [SecureX を取得(Get SecureX)] をクリックします。
2. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Cisco Secure Email Cloud Mailbox リボンを承認(Authorize Cisco Secure Email Cloud Mailbox Ribbon)] をクリックします。

SecureX リボンが認証されました。SecureX 設定が正常に更新されたことを示すバナーが表示されます。

Cloud Mailbox のユーザー設定からの承認

[ユーザー設定(User Settings)] メニューから SecureX リボンを承認するには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. [初期設定(Preferences)] > [SecureX リボン(SecureX Ribbon)] で、[SecureX リボンの承認(Authorize SecureX Ribbon)] をクリックします。
3. [アプリケーションアクセスの許可(Grant Application Access)] ダイアログで、[Cisco Secure Email Cloud Mailbox リボンを承認(Authorize Cisco Secure Email Cloud Mailbox Ribbon)] をクリックします。

SecureX リボンが認証されました。SecureX 設定が正常に更新されたことを示すバナーが表示されます。

SecureX リボンの承認を取り消す

SecureX リボンはユーザーレベルで承認されます。リボン内または [ユーザー設定(User Preferences)] メニューから承認を取り消すことができます。

Secure X リボン内から承認を取り消す

リボン内から SecureX リボンの承認を取り消すには、次の手順を実行します。

1. SecureX リボンで [設定(Settings)] > [承認(Authorization)] > [取り消し(Revoke)] を選択します。
2. [取り消し(Revoke)] ダイアログで、[確認(Confirm)] をクリックします。

SecureX リボンが Cloud Mailbox アカウントに対して承認されなくなりました。

Cloud Mailbox のユーザー設定からの承認の取り消し

[ユーザー設定(User Settings)] メニューから SecureX リボンの承認を取り消すには、次の手順を実行します。

1. [ユーザー(User)](プロフィールアイコン)> [ユーザー設定(User Settings)] を選択します。
2. [初期設定(Preferences)] > [SecureX リボン(SecureX Ribbon)] で、[承認を取り消す(Revoke Authorization)] をクリックします。

SecureX リボンが Cloud Mailbox アカウントに対して承認されなくなりました。SecureX 設定が正常に更新されたことを示すバナーが表示されます。

SecureX のリボン

クラウド メールボックスの非アクティブ化

クラウド メールボックス を非アクティブ化するには、主に次の 2 つのタスクを使用します。

- Microsoft Exchange 管理センターから クラウド メールボックス ジャーナルエントリを削除する
- Microsoft Azure テナントから クラウド メールボックス アプリケーションを削除する

クラウド メールボックス ジャーナルエントリの削除

1. Microsoft 365 管理センター（https://admin.microsoft.com/AdminPortal/Home#/homepage）に移動します。
2. [管理センター] > [Exchange] > [コンプライアンス管理] > [ジャーナルルール] の順に移動します。
3. クラウド メールボックス ジャーナルルールを選択して、[削除（Delete）] をクリックします。[はい] を選択して、ジャーナルルールを削除することを確認します。

Azure からの クラウド メールボックス アプリケーションの削除

1. portal.azure.com に移動します。
2. [エンタープライズアプリケーション] を見つけて選択します。

   注：Azure で古いビューを使用している場合、これは**アプリの登録**と呼ばれることがあります。
3. **Cisco Secure Email Cloud Mailbox** および/または **Cisco Secure Email Cloud Mailbox（読み取り専用）**アプリケーションを見つけて選択します。
4. 左側のペインで、[プロパティ]を選択します。
5. [削除] ボタンをクリックして [はい] を選択し、CMD アプリを削除することを確認します。

Azure からの クラウドメールボックス アプリケーションの削除

よく寄せられる質問(FAQ)

よく寄せられる質問については、Cisco Secure Email Cloud Mailbox の FAQ を参照してください。

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。

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。