Cloud Mailbox Defense ユーザガイド

初版:2020 年 9 月 2 日

最終更新日:2021 年 5 月 21 日

Cloud Mailbox Defense

Cloud Mailbox Defense（CMD）は、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、CMD 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

Cloud Mailbox Defense（CMD）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。

- CMD 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 アカウントを所有している。
- 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。CMD の分析対象とするアドレスを使用しないでください。

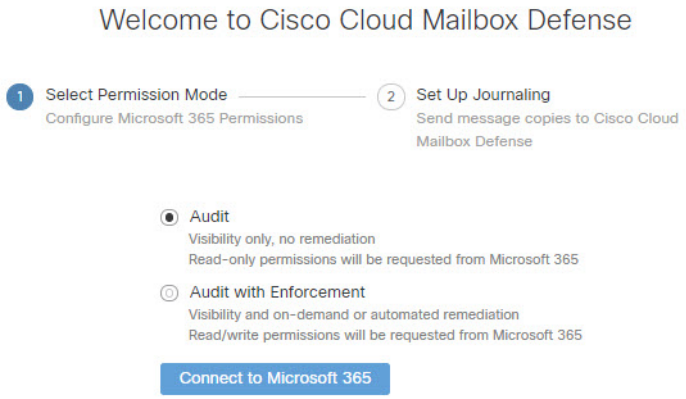
ビジネスの設定

CMD 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（1 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。

   CMD は、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。Cisco Threat Response、Threat Grid、または AMP の既存のお客様の場合は、必ず既存のログイン情報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（4 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 CMD 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、Cloud Mailbox Defense の FAQ「CMD 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 CMD?）」を参照してください。

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

4. Microsoft 365 でジャーナリングを設定します。

   CMD 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 CMD 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 CMD 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 Threat Grid アカウントが作成され、Threat Grid から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 Threat Grid アカウントにリンクされていません。CMD を設定するために Threat Grid アカウントで必要なアクションはありません。

   a. CMD 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。CMD 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. CMD 設定ページからコピーしたジャーナルアドレスを [Send journal reports to] フィールドに貼り付けます。

g. [Name] フィールドに **CiscoCMD** 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。

- CMD のお客様の場合は、[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。

5. CMD の設定ページに戻ります。[enable policy enforcement] をクリックします。

6. ジャーナルが CMD に直接かつ確実に送信されるようにするには、設置する外部の電子メール ゲートウェイ アプライアンスをバイパスすることを推奨します。アプライアンスによっては、CMD ジャーナルアドレスを含む許可ルールを追加する必要が生じる場合があります。

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（4 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、ここで [自動修復（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 domain not in domain list] トグルを [On] に設定します。

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。

1. [Settings]（歯車アイコン）> [Policy] に移動します。

2. [Import Domains] ボタンをクリックして、ドメインを CMD にインポートします。

3. 各ドメインの横にあるトグルを使用して、そのドメインの自動修復設定を調整します。

ポリシー設定

[Settings]（歯車アイコン）> [Policy] ページの設定によって、Cloud Mailbox Defense（CMD）によるメールの処理方法が決まります。ビジネスの設定（1 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、変更後に [保存して適用（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：[Audit with Enforcement] モードを選択した場合は、[Automated Remediation] の設定もオンにする必要があります。
[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**
[Attachment Analysis]	Cisco Threat Grid によって分析されるメール添付ファイルの方向。	■ **着信** ■ **発信** ■ **内部**	**着信**
[Remediation Actions]	**悪意あり**、**スパム**、**グレイメール**、または**フィッシング**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。	■ **[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。	■ [Malicious] - [Move to Trash] ■ [Phishing] - [Move to Trash] ■ [Spam] - [Move to Junk] ■ [Graymail] - [No Action]

表 1　ポリシー設定（続き）

設定	説明	オプション	デフォルト
[Automated Remediation]			
[Apply auto-remediation to domains not in the domain list]	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、CMD にインポートされていない場合などです。	[On] または [Off]	[Off]。[Audit with Enforcement] モードをオンにする場合は、このトグルを [On] に設定して、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。
[Apply auto-remediation to all domains in the domain list]	リスト内のすべてのドメインに同じ自動修復設定を適用します。	[On] または [Off]	[Off]。[Audit with Enforcement] モードをオンにする場合は、このトグルを [On] に設定して、リストに含まれているすべてのドメインに自動修復が適用されるようにします。
[Domain-specific auto-remediation]	特定のドメインに自動修復を適用します。	[On] または [Off]	[Off]。[Audit with Enforcement] モードをオンにする場合は、このトグルを [On] に設定して、特定のドメイン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
[Message Analysis]	[Outgoing] と [Internal]
[Attachment Analysis]	なし
[Remediation Actions]	■ [Malicious] - [Move to Trash] ■ [Phishing] - [Move to Trash] ■ [Spam] - [Move to Junk]

また、ジャーナルが CMD 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。アプライアンスによっては、CMD ジャーナルアドレスを含む許可ルールを追加する必要が生じる場合があります。

CES IMD のお客様向けのポリシー設定

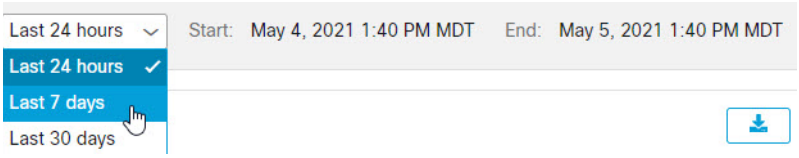
CES Internal Mailbox Defense（IMD）のお客様の場合、ポリシー設定は標準の CMD を使用している場合とは若干異なります。

- [Message Analysis] は [Internal] に設定され、[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。

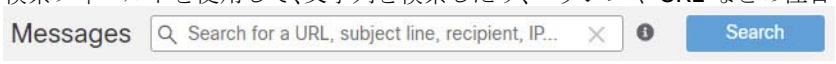
メッセージ

[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。



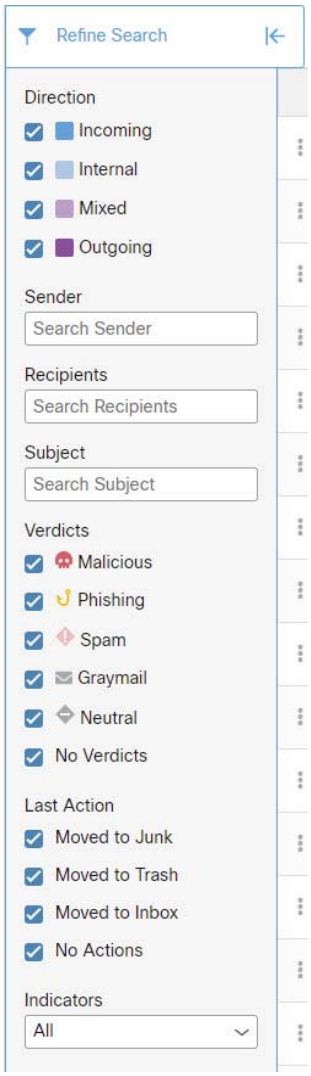
検索フィールドを使用して、文字列を検索したり、ハッシュや URL などの注目する指標を検索します。



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、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戻すには、[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 3　[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 CMD によって自動修復されました。

表 3　[Messages] ページのアイコン

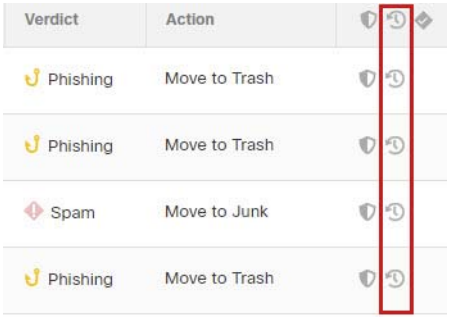
アイコン	名前	説明
	レトロスペクティブな判定	レトロスペクティブな判定が適用されました。レトロスペクティブな判定は、メッセージが CMD によって最初にスキャンされた後に適用されたものです。
	MS 許可リスト	CMD は Microsoft 365 スパムフィルタの許可リストを優先しました。
	ニュートラル	メッセージがニュートラルとしてマークされています。
	スパム	メッセージが手動または自動修復によってスパムとしてマークされました。
	フィッシング	メッセージは、手動または自動修復によってフィッシングとしてマークされています。
	悪意あり	メッセージは、手動または自動修復によって悪意のあるものとしてマークされています。
	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。

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 CMD 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。

CMD 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。CMD 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、CMD 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、[Messages] ページの右側の列に示されます。



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

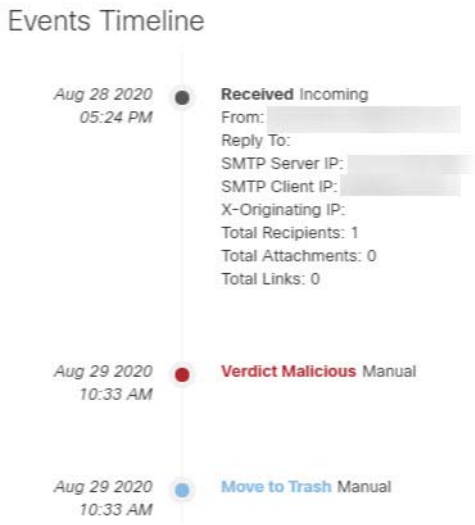
[Messages] ページの検索結果内のメッセージを調査するには、[>] アイコンを選択してメッセージを展開し、送信者 IP、Microsoft メッセージ ID、添付ファイル、リンクなどの詳細を確認します。

[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
- [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



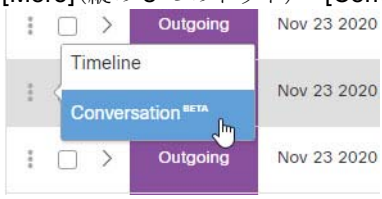
[Conversation]（ベータ）

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。

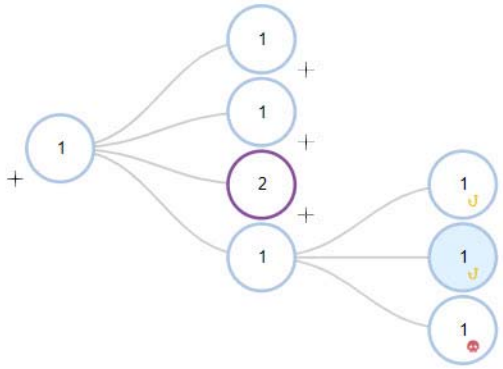
カンバセーションビューでは、カンバセーションの全体ビューが表示されます。カンバセーションビューを使用して、カンバセーション内のメッセージを追跡し、メールフローを完全に把握します。これは、脅威の発生源と組織内で拡散する方法を判断するのに役立ちます。

[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。



強調表示されたノード（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、下の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。



	Direction	Received	Sender	Recipients	Subject
>	Internal	Nov 20 2020 01:55 PM			Unix system invoice
>	Internal	Nov 20 2020 01:55 PM			FW: Unix system invoice
>	Internal	Nov 20 2020 01:55 PM			Re: Unix system invoice
>	Outgoing	Nov 20 2020 01:55 PM		+1 more	FW: Unix system invoice
>	Internal	Nov 20 2020 01:55 PM			FW: Unix system invoice

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。

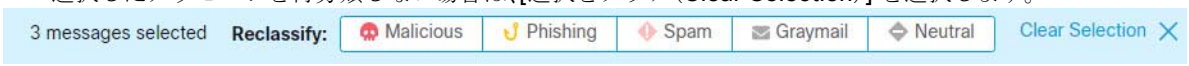
注: 再分類は、選択したメッセージの判定にのみ影響します。選択した送信者からの今後のメッセージ、またはメッセージの内容に基づいた今後のメッセージへの変更は示すものではありません。メッセージは、Cisco Talos による確認のためにキューに入れられます。Talos は、今後の分類に影響を与えるためにこのフィードバックを使用する場合があります。

[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. 表示されるオプションのいずれかを選択します。電子メールを、[Malicious]、[Phishing]、[Spam]、[Graymail]、または [Neutral] に再分類できます。

   選択したメッセージを再分類しない場合は、[選択をクリア（Clear Selection）] を選択します。

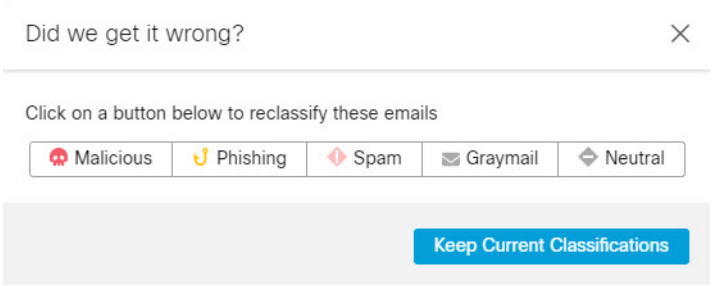


[Audit with Enforcement] モード

[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。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、必要に応じて [迷惑メールに移動（Move to Junk）]、[ごみ箱に移動（Move to Trash）]、[受信箱に移動（Move to Inbox）]、または [移動しない（Do Not Move）] をクリックします。

2. 表示されるダイアログでいずれかのオプションを選択します。電子メールを [Malicious]、[Phishing]、[Spam]、[Graymail] または [Neutral] に再分類できます。または、**現在の分類を維持**できます。



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。

検索結果のダウンロード

[Messages] ページのダウンロード  ボタンをクリックして、検索結果をダウンロードできます。結果は CSV ファイルとしてエクスポートされます。

インサイト

[Insights] 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、インサイト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、[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。

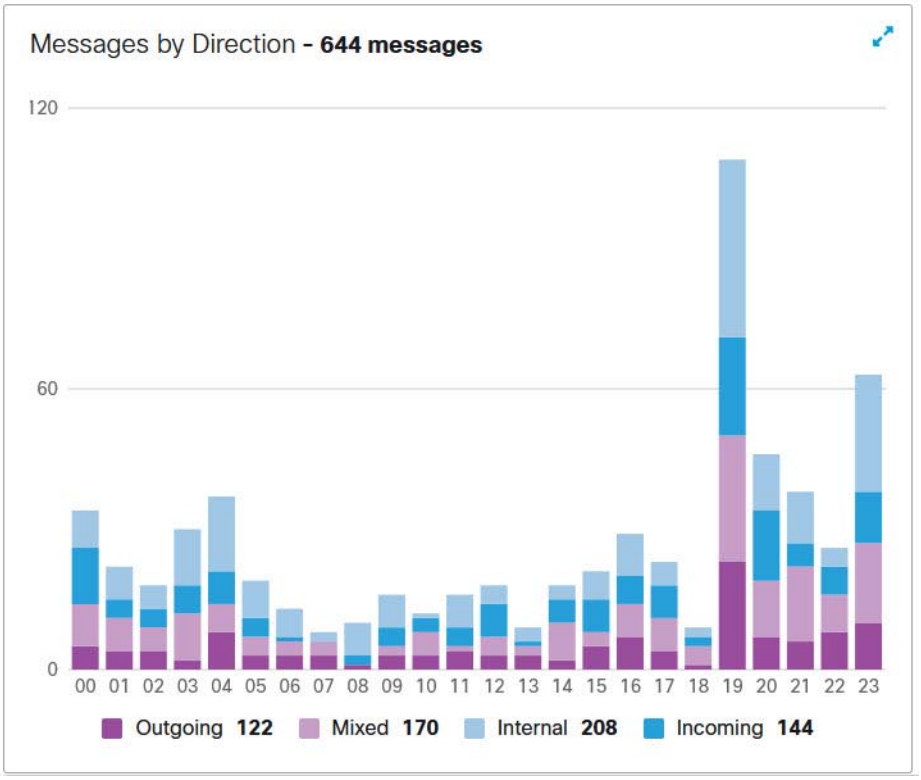
[Messages by Direction]

[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

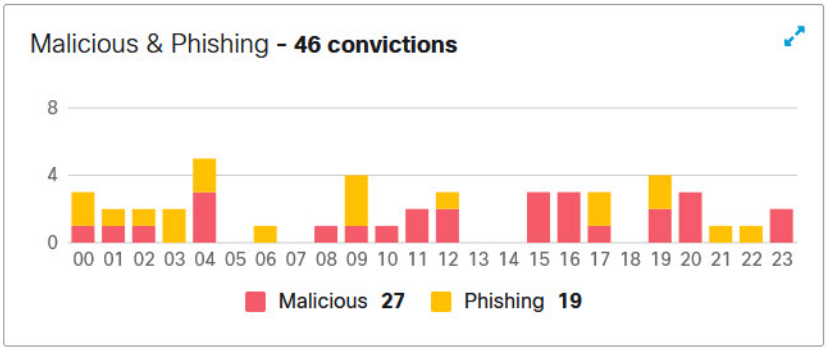
- [Internal]：社内に送信されたメール
- [Incoming]：社外から受信したメール

凡例には、各カテゴリのメッセージ数が表示されます。



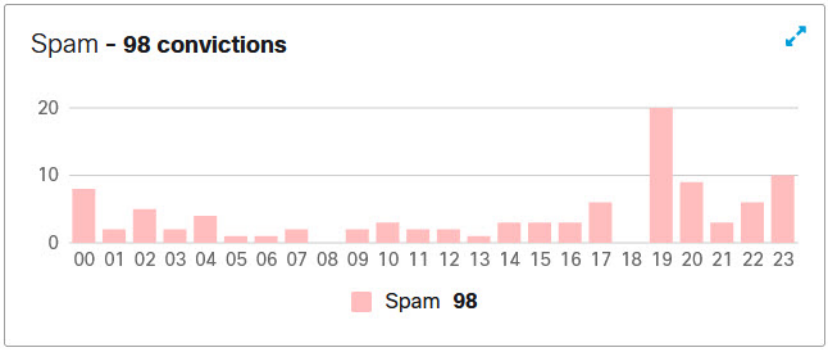
[Malicious & Phishing]

[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。



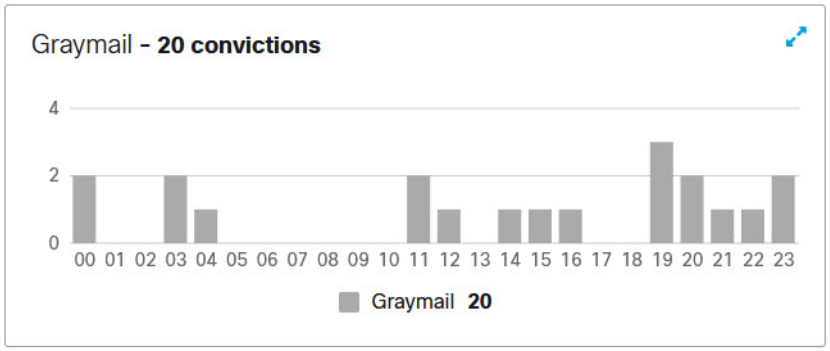
[Spam]

[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。



ユーザの管理

[Administration] ページからユーザアカウントを管理します。

CMD は、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 Cisco Threat Response、Threat Grid、または AMP のお客様は、既存のログイン情報を使用してサインインする必要があります。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。次の表に示すロールに属する CMD ユーザを作成できます。

表 4　ユーザ ロール

ロール	説明
super-admin	このユーザは、CMD 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。
read-only	これらのユーザは、CMD の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、アカウント設定やポリシーの変更、新規ユーザの作成はできません。

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 CiscoCloud Mailbox Defense**」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。

ユーザの編集

ユーザが名前を変更した場合は、[Administration] ページでインラインで編集できます。ユーザの電子メールアドレスまたはロールは編集できません。

ユーザの情報を編集するには、次の手順を実行します。

1. [Settings](歯車アイコン) > [Administration] > [Users] の順に選択します。
2. 変更する名前にカーソルを合わせ、鉛筆アイコンをクリックして名前を編集します。
3. 更新したテキストを入力し、チェックマークをクリックして変更を保存します。

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 CMD 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設定には、[Settings]（歯車アイコン）> [Administration] > [Business] からアクセスできます。

ビジネス情報

[ビジネス情報（Business Information）] 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
- サブスクリプション ID のサポート

ライセンス情報

[License Information] テーブルには、ライセンスのタイプ、シート数、契約 ID、およびライセンスの開始日と終了日が表示されます。

通知電子メールアドレス

通知電子メールアドレスは、シスコが CMD 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。このアドレスは、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、[Download] をクリックします。

Google アナリティクス

Google アナリティクスは、CMD 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 CMD 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。

CMD の非アクティブ化

CMD 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 CMD ジャーナルエントリを削除する
- Microsoft Azure テナントから CMD アプリケーションを削除する

CMD 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. CMD ジャーナルルールを選択して、[削除] 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 CMD 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. **CMD** または **CMD (Read Only)** 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。

よく寄せられる質問(FAQ)

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

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。