メッセージ トラッキング

この章は、次の項で構成されています。

メッセージ トラッキングの概要

メッセージ トラッキングにより、メッセージ フローの詳細なビューを表示することでヘルプデスク コールを解決に役立ちます。たとえば、メッセージが想定どおりに配信されない場合、ウイルス感染が検出されたか、スパム隔離に入れられたか、あるいはメール ストリーム以外の場所にあるのかを判断できます。

ユーザが指定した基準に一致する特定の電子メール メッセージまたはメッセージのグループを検索できます。

（注） メッセージの内容を読み取るためにメッセージ トラッキングは使用できません。

メッセージ トラッキングの有効化

（注） メッセージ トラッキングのデータは、この機能をイネーブルにした後で処理されたメッセージに対してのみ保持されます。

はじめる前に

- メッセージ トラッキングで添付ファイル名を検索して表示したり、ログ ファイル内の添付ファイル名を表示したりするには、メッセージ フィルタやコンテンツ フィルタなどの本文スキャン プロセスを少なくとも 1 つ設定してイネーブルにする必要があります。
- 件名での検索をサポートするには、ログファイルで件名ヘッダーを記録するように設定する必要があります。詳細については、ログを参照してください。
- 中央集中型トラッキングを設定する場合：該当する電子メールゲートウェイの中央集中型メッセージトラッキングをサポートするように、 Cisco Secure Manager Email and Web Gateway を設定します。『 Cisco Secure Manager Email and Web Gateway User Guide』を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）]>[メッセージ トラッキング（Message Tracking）] をクリックします。

このサービスを一元管理する予定ではない場合でも、このパスを使用します。

ステップ 2 [メッセージトラッキングサービスを有効にする（Enable Message Tracking Service）] を選択します。

ステップ 3 システム設定ウィザードを実行してから初めてメッセージトラッキングをイネーブルにする場合は、エンドユーザ ライセンス契約書を確認し、[承認（Accept）] をクリックします。

ステップ 4 メッセージ トラッキングサービスを選択します。

オプション	説明
ローカル トラッキング（Local Tracking）	この電子メールゲートウェイでメッセージトラッキングを使用します。
中央集中型トラッキング（Centralized Tracking）	これを含め複数の電子メールゲートウェイのメッセージをトレースするために Cisco Secure Manager Email and Web Gateway を使用します。

ステップ 5 （任意）拒否された接続に関する情報を保存するチェックボックスをオンにします。

最適なパフォーマンスを得るために、この設定を無効にしたままにします。

ステップ 6 変更を送信し、保存します。

次のタスク

ローカル トラッキングを選択した場合、次を実行します。

- 誰がDLP違反に関連したコンテンツにアクセスできるかを選択します。メッセージトラッキングでの機密情報へのアクセスの制御を参照してください。
- （任意）メッセージを保存するためのディスク領域の割り当てを調整します。ディスク領域の管理 を参照してください。

レガシー インターフェイスでのメッセージの検索

手順

ステップ 1 [メール（Email）] > [メッセージトラッキング（Message Tracking）] > [メッセージトラッキング（Message Tracking）]を選択します。**[モニタ（Monitor）] > [メッセージ トラッキング（Message Tracking）]**

ステップ 2 検索条件を入力します。

- すべてのオプションを表示するには、[詳細（Advanced）] リンクをクリックします。
- トラッキングでは、ワイルドカード文字や正規表現はサポートされません。
- トラッキング検索では大文字と小文字は区別されません。
- 特に指定のない限り、クエリーは「AND」検索です。クエリーは、検索フィールドに指定されたすべての条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行のパラメータにテキストストリングを指定すると、クエリーは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。
- 検索条件は、次のとおりです。

オプション	説明
エンベロープ送信者（Envelope Sender）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージ送信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。入力した内容は実行されません。
エンベロープ受信者（Envelope Recipient）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージ受信者を検索するための電子メールアドレス、ユーザ名、ドメインを入力します。 文字を入力できます。入力した内容は実行されません。

オプション	説明
件名（**Subject**）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、そしてメッセージの件名行で検索するテキスト文字列を入力します。 **警告**：規制によりそのようなトラッキングが禁止されている環境では、このタイプの検索を使用しないでください。
受信したメッセージ数（**Message Received**）	日時の範囲を指定します。 日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。 メッセージが電子メールゲートウェイによって受信された現地日時を使用します。
詳細オプション	
送信者IPアドレス/ドメイン/ネットワーク所有者（**Sender IP Address/ Domain / Network Owner**）	リモートホストのIPアドレス、ドメイン、またはネットワーク所有者を指定します。 拒否された接続のみまたはすべてのメッセージを検索の範囲で検索できます。

オプション	説明
添付ファイル（Attachment）	[次で始まる（Begins With）]、[次に合致する（Is）] または [次を含む（Contains）] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。 添付ファイル名でメッセージを検索できるのは、以下の操作を実行している場合だけです。 • メッセージ フィルタを使用した本文スキャン • コンテンツ フィルタを使用した本文スキャン • 高度なマルウェア防御（AMP）スキャン SHA-256 ハッシュに基づいたファイルの識別方法については、SHA-256 ハッシュによるファイルの識別を参照してください。 Advanced Malware Protection エンジンによって悪意があるとして検出されたメッセージを、脅威名で検索することができます。[カスタム検知（Custom Detection）] および [カスタムしきい値（Custom Threshold）] カテゴリに基づいて悪意があるとして検出されたメッセージを検索するには、[脅威名（Threat Name）] フィールドに *Simple_Custom_ Detection* または *Custom_Threshold* と入力します。また、特定のファイルが Advanced Malware Protection エンジンによってウイルス陽性として検出された場合は、メッセージをウイルス名で検索することもできます。
メッセージ イベント（Message Event）	1 つ以上のメッセージ処理イベントを選択します。たとえば、配信メッセージ、隔離メッセージ、ハードバウンス メッセージを検索できます。 メッセージ イベントは「OR」演算子を使用して追加されます。複数のイベントを選択して、指定した条件の任意のものと一致するメッセージを検索します。
メッセージ ID ヘッダー（Message ID Header）	SMTP メッセージ ID ヘッダーのテキスト文字列を入力します。 この RFC 822 メッセージヘッダーは、各電子メール メッセージを識別します。これは最初にメッセージが作成されるときに挿入されます。
Cisco IronPort MID	検索するメッセージ番号を入力します。IronPort MID は、 電子メールゲートウェイ上の各電子メールメッセージを一意に識別します。

オプション	説明
Cisco IronPortホスト（Cisco IronPort Host）	E メール セキュリティ アプライアンスを選択してその 電子メールゲートウェイで処理されたメッセージだけに検索対象を限定するか、またはすべての電子メールゲートウェイを選択します。

ステップ 3 [検索（Search）] をクリックして、クエリーを送信します。

クエリー結果がページの下部に表示されます。

次のタスク

関連項目

- メッセージ トラッキングの検索結果の使用　（9 ページ）

新しい Web インターフェイスでの電子メール メッセージの検索

電子メールゲートウェイのトラッキングサービスを使用して、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうかや、ハードバウンスまたは配信されたかどうか）など、指定した条件に一致する特定の電子メールメッセージまたはメッセージのグループを検索できます。メッセージ トラッキングでは、メッセージ フローの詳細なビューが表示されます。また、特定の電子メール メッセージをドリルダウンし、処理イベント、添付ファイル名、エンベロープおよびヘッダー情報など、メッセージの詳細情報を確認することもできます。

（注） このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

手順

ステップ 1 [トラッキング（Tracking）] タブをクリックします。

ステップ 2 [メッセージ（Messages）] タブまたは [拒否された接続（Connections Rejected）] タブを選択し、検索結果を絞り込みます。

（注） 送信者 IP アドレス、ドメイン、またはネットワーク所有者に基づいて拒否された接続を検索することができます。

ステップ 3 （任意）[詳細検索（Advanced Search）] をクリックし、その他の検索オプションを表示します。

ステップ 4 次の検索条件を入力します。

（注） トラッキング検索では、ワイルドカード文字や正規表現はサポートされません。トラッキング検索では大文字と小文字は区別されません。

- （メッセージと拒否された接続の場合）[受信したメッセージ数（Message Received）] : [前日（Last Day）]、[最近1週間（Last 7 Days）]、または [カスタム範囲（Custom Range）] を使用してクエリの日時の範囲を指定します。過去 24 時間以内のメッセージを検索するには [前日（Last Day）] オプションを使用し、過去 7 日間のメッセージを検索するには [最近1週間（Last 7 Days）] オプションと当日の経過時間を使用します。

  日付を指定しなければ、クエリーは、すべての日付に対するデータを返します。時間範囲だけを指定すると、クエリーは、すべての利用可能な日付にわたってその時間範囲内のデータを返します。終了日と終了時刻に現在の日付と 23:59 を指定すると、クエリは現在の日付に関するすべてのデータを返します。

  日付と時間は、データベースに保管される際に GMT 形式に変換されます。 電子メールゲートウェイ上で日付と時刻を表示する場合は、その電子メールゲートウェイの現地時間で表示されます。

  電子メールゲートウェイのログに記録され、 Cisco Secure Email and Web Gateway が取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。

- [エンベロープ送信者（Envelope Sender）] : [次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、テキスト文字列を入力してエンベロープ送信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。次の形式を使用します。
  - E メール ドメインの場合：*example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]*
  - 完全 E メール アドレスの場合：*user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5]*。
  - 文字を入力できます。入力した内容は実行されません。

- [件名（Subject）] : [次で始まる（Begins With）]、[次に合致する（IS）]、[次を含む（Contains）]、または [空である（Is Empty）] を選択し、テキスト文字列を入力してメッセージ件名行を検索します。

- [エンベロープ受信者（Envelope Recipient）] : [次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、テキストを入力してエンベロープ受信者を検索します。電子メール アドレス、ユーザ名、またはドメインを入力できます。

  電子メールゲートウェイでエイリアス拡張にエイリアステーブルを使用している場合は、本来のエンベロープアドレスではなく、拡張された受信者アドレスが検索されます。それ

以外のあらゆる場合においては、メッセージ トラッキング クエリによって本来のエンベロープ受信者アドレスが検索されます。

この点を除けば、エンベロープ受信者の有効な検索条件はエンベロープ送信者の場合と同じです。

文字を入力できます。入力した内容は実行されません。

- [添付ファイル名（Attachment Name）]：[次で始まる（Begins With）]、[次に合致する（IS）]、または [次を含む（Contains）] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。
- Reply-To：[次で始まる（Begins With）]、[次に合致する（Is）]、または [含む（Contains）] を選択して、メッセージの「`Reply-To`」ヘッダーに基づいてメッセージを検索する文字列を入力します。
- [ファイルSHA256（File SHA256）]：メッセージのファイルの SHA-256 値を入力します。

  SHA-256 ハッシュに基づいたファイルの識別方法については、SHA-256 ハッシュによるファイルの識別を参照してください。
- [シスコのホスト（Cisco Host）]：[すべてのホスト（All Host）] を選択してすべての 電子メールゲートウェイ間で検索するか、ドロップダウンメニューから必要な電子メールゲートウェイを選択します。
- [メッセージIDヘッダーおよびCisco MID（Message ID Header and Cisco MID）]：メッセージ ID ヘッダーのテキスト文字列、Cisco IronPort メッセージ ID（MID）、またはその両方を入力します。
- （メッセージと拒否された接続の場合）[送信者IPアドレス/ドメイン/ネットワーク所有者（Sender IP Address/ Domain / Network Owner）]：送信元 IP アドレス、ドメインまたはネットワーク所有者の詳細を入力します。
  - IPv4 アドレスは、ピリオドで区切られた 4 つの数値であり、それぞれの数値は 0 ～ 255 でなければなりません（例：203.0.113.15）。
  - IPv6 アドレスでは、8 つの 16 ビットの 16 進数値がコロンで区切られて構成されます。

    いずれか 1 箇所で、2001:db8:80:1::5 のようにゼロ圧縮を使用できます。
  - [メッセージイベント（Message Event）]：追跡対象のイベントを選択します。たとえば、配信メッセージ、隔離メッセージ、ハードバウンス メッセージを検索できます。メッセージ イベントは「OR」演算子を使用して追加されます。複数のイベントを選択して、指定した条件の任意のものと一致するメッセージを検索します。

すべてのフィールドに入力する必要はありません。[メッセージイベント（Message Event）] オプションを除き、クエリは「AND」検索になります。このクエリは、検索フィールドで指定された「AND」条件に一致するメッセージを返します。たとえば、エンベロープ受信者と件名行

のパラメータにテキスト ストリングを指定すると、クエリは、指定されたエンベロープ受信者と件名行の両方に一致するメッセージだけを返します。

ステップ 5 **[検索（Search）]** をクリックします。

各行が 1 つの電子メール メッセージに対応します。ビューでメッセージをさらにロードするにはスクロールダウンします。

必要に応じて、新しい検索基準を入力することにより検索を精密化し、クエリを再実行します。あるいは、次の項で説明するように、結果セットを絞り込んで検索精度を高めることもできます。

次のタスク

- メッセージ トラッキングの検索結果の使用 （9 ページ）

メッセージ トラッキングの検索結果の使用

次の点に留意してください。

- 電子メールゲートウェイのログに記録され、 Cisco Secure Manager Email and Web Gateway で取得済みのメッセージのみが検索結果に表示されます。ログのサイズとポーリングの頻度によっては、電子メール メッセージが送信された時間と、それがトラッキングとレポーティングの結果に実際に表示される時間との間にわずかな差が生じることがあります。
- 高度なマルウェア防御（ファイル レピュテーション スキャンおよびファイル分析）を使用する検索については、メッセージ トラッキング機能と高度なマルウェア防御機能についてを参照してください。

検索結果を使用する場合に実行できる操作：

- 検索条件に戻って、クエリー設定の[詳細（Advanced）]をクリックし、[クエリ設定（Query Settings）] までスクロールし、結果の最大数を 1000 に設定すると、250 件以上の検索結果を表示できます。
- 検索結果セクションの右上でオプションを選択すると、各ページに表示される結果を増やすことができます。
- 検索結果セクションの右上から、複数のページの検索結果内を移動できます。
- 条件として追加する検索結果の値の上でカーソルを移動すると、検索結果を限定できます。オレンジ色で強調表示されている場合は、その値をクリックすると、その条件で検索を絞り込むことができます。これで、検索条件が追加されます。たとえば、特定の受信者に送信されたメッセージを検索した場合は、検索結果で送信者の名前をクリックすると、最初に指定した時間範囲内の（および、その他の条件を満たす）、その送信者からその受信者へのすべてのメッセージを見つけることができます。
- 検索条件に 1000 件以上のメッセージが一致する場合、（検索結果セクションの右上にあるリンク）[すべてエクスポート（Export All）] をクリックし、最大 50,000 件の検索結果

をカンマ区切り形式ファイルとしてエクスポートし、他のアプリケーションでデータを使用できます。

- メッセージの行の [詳細の表示（Show Details）] をクリックすると、メッセージの詳細情報を表示できます。メッセージの詳細を表示した新しいブラウザ ウィンドウが開きます。
- 隔離されたメッセージの場合、メッセージが隔離された理由などの詳細情報を表示するにはメッセージ トラッキングの検索結果のリンクをクリックします。
- [メールボックスの検索と修復（Mailbox Search and Remediate）] アクションを使用して、ユーザメールボックスにある悪意のあるメッセージを修復します。詳細については、メールボックス内のメッセージの検索と修復を参照してください。

（注） レポート ページのリンクをクリックして、メッセージ トラッキングのメッセージ詳細を表示したが、その結果が予期したものでない場合があります。これは、確認している期間中に、レポーティングとトラッキングを同時に継続してイネーブルにしていない場合に発生する可能性があります。

関連項目

- メッセージ トラッキングの詳細 （10 ページ）

メッセージ トラッキングの詳細

項目	説明
[エンベロープとヘッダーのサマリー（Envelope and Header Summary）] セクション	
受信時間（Received Time）	電子メールゲートウェイがメッセージを受信した時間。 日時は、 電子メールゲートウェイで設定される現地時間を使用して表示されます。
MID	一義的な IronPort メッセージ ID。
メッセージ サイズ（Message Size）	メッセージ サイズ。
件名（Subject）	メッセージの件名リスト。 トラッキング結果の件名行は、メッセージの件名がないか、ログ ファイルで件名ヘッダーを記録するよう設定されていない場合、[（件名なし）（(No Subject)）] という値になる場合があります。詳細については、ログを参照してください。
エンベロープ送信者（Envelope Sender）	SMTP エンベロープ内の送信者のアドレス。

項目	説明
エンベロープ受信者（Envelope Recipients）	導入でエイリアス拡張のためのエイリアス テーブルを使用する場合、検索では元のエンベロープ アドレスではなく拡張された受信者アドレスを見つけます。エイリアステーブルの詳細については、「ルーティングおよび配信機能の設定」の章にある「エイリアステーブルの作成」を参照してください。 それ以外のあらゆる場合においては、メッセージ トラッキング クエリーによって本来のエンベロープ受信者アドレスが検索されます。
メッセージ ID ヘッダー（Message ID Header）	RFC 822 のメッセージ ヘッダー。
SMTP 認証ユーザ ID（SMTP Auth User ID）	送信者が SMTP 認証を使用してメッセージを送信した場合は、SMTP で認証された送信者のユーザ名。それ以外の場合、この値は「なし（N/A）」となります。
添付ファイル	メッセージに添付されたファイルの名前。 名前に対してクエリーが実行された少なくとも 1 つの添付ファイルを含むメッセージが検索結果に表示されます。 トラッキングできない添付ファイルもあります。パフォーマンス上の理由から、添付ファイル名のスキャンは他のスキャン動作の一環としてのみ実行されます。たとえば、メッセージまたはコンテンツ フィルタリング、DLP、免責事項スタンプなどです。添付ファイル名は、添付ファイルがまだ添付されている間に本文スキャンを通過するメッセージに対してのみ使用できます。添付ファイルの名前が検索結果に表示されない状況を含みます（ただし限定はされません）。 • システムがコンテンツフィルタのみを使用しているときに、メッセージがドロップされるか、またはその添付ファイルがアンチスパムまたはアンチウイルスフィルタによって削除された場合 • 本文スキャンが実行される前に、メッセージ分裂ポリシーによって一部のメッセージから添付ファイルが削除された場合 パフォーマンス上の理由から、添付ファイル内のファイルの名前（たとえば、OLE オブジェクトや、.ZIP ファイルなどのアーカイブ）は検索されません。
（新しいWebインターフェイスのみ）[メッセージイベント（Message Event）]	各イベント タイプに一致するメッセージが含まれている複数のイベントを選択します。

項目	説明
[ホスト サマリーの送信（Sending Host Summary）] セクション	
逆引き DNS ホスト名（Reverse DNS Hostname）	逆引き DNS（PTR）ルックアップによって検証される送信ホストの名前。
IP Address	送信元ホストの IP アドレス。
IP レピュテーション**スコア**	IP レピュテーションスコア。範囲は、10（最も信頼できる送信者）～-10（明らかなスパム送信者）です。スコアが「なし（None）」の場合、そのメッセージが処理された時点で、このホストに関する情報が存在しなかったことを意味します。 IP レピュテーションサービスの詳細については、IP レピュテーション フィルタリング
[処理詳細（Processing Details）] セクション	
要約情報 （以下のタブのいずれかが表示されている場合、この情報はタブに表示されます。常にサマリー情報を表示します）。	[サマリー（Summary）] タブでは、メッセージ処理中に記録されるステータス イベントを表示します。 エントリには、メールポリシーの処理（アンチスパム スキャンやアンチウイルス スキャンなど）とメッセージ分割などの他のイベントに関する情報、およびコンテンツまたはメッセージ フィルタによって追加されるカスタム ログ エントリが含まれます。 メッセージが配信された場合、配信の詳細がここに表示されます。 記録された最新のイベントは、処理の詳細内で強調表示されます。
DLP に一致した内容（DLP Matched Content） タブ	このタブは、DLP ポリシーによって検出されたメッセージに対してのみ表示されます。 このタブには、DLP ポリシーの一致をトリガーした機密のコンテンツに加え、一致に関する情報が含まれます。 この情報を表示するには 電子メールゲートウェイを設定する必要があります。「メッセージ トラッキングでの機密性の高い DLP データの表示」を参照してください。 このタブへのアクセスを制御するには、メッセージ トラッキングでの機密情報へのアクセスの制御を参照してください。

項目	説明
[URL の詳細（URL Details）] タブ	このタブは、URL レピュテーション コンテンツ フィルタと URL カテゴリ コンテンツ フィルタ、およびアウトブレイク フィルタによって捕捉されたメッセージに対してのみ表示されます。 このタブには、次の情報が表示されます。 • URL に関連付けられているレピュテーション スコアまたはカテゴリ • URL に対して実行されたアクション（書き換え、危険の除去、またはリダイレクト） • メッセージに複数の URL が含まれる場合、フィルタ アクションをトリガーした URL この情報を表示するには 電子メールゲートウェイを設定する必要があります。「メッセージ トラッキングの URL 詳細の表示」を参照してください。 このタブへのアクセスを制御するには、メッセージ トラッキングでの機密情報へのアクセスの制御を参照してください。

関連項目

- レガシー インターフェイスでのメッセージの検索 （3 ページ）

メッセージ トラッキング データの有効性の検査

メッセージ トラッキング データに含まれる日付範囲を確認すること、およびそのデータの欠落インターバルを識別することができます。

手順

ステップ 1 （新しい Web インターフェイスのみ）ページの右上隅にある歯車アイコンをクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [モニタ（Monitor）] > [メッセージトラッキング（Message Tracking）] を選択します。

ステップ 3 右上隅にある [検索（Search）] ボックスに表示される [時間範囲内のデータ:（Data in time range:）] を確認します。

ステップ 4 [時間範囲内のデータ:（Data in time range:）] で示される値をクリックします。

次のタスク

関連項目

- メッセージ トラッキングおよびアップグレードについて （14 ページ）

メッセージ トラッキングおよびアップグレードについて

新しいメッセージ トラッキング機能は、アップグレードの前に処理されたメッセージには適用できない場合があります。これは、これらのメッセージについては、必須データが保持されていない場合があるためです。メッセージ トラッキング データおよびアップグレードに関連する制限については、ご使用のリリースのリリース ノートを参照してください。

メッセージ トラッキングのトラブルシューティング

関連項目

- 添付ファイルが検索結果に表示されない （14 ページ）
- 予想されるメッセージが検索結果に表示されない （14 ページ）

添付ファイルが検索結果に表示されない

問題

添付ファイル名が検出されず、検索結果に表示されません。

解決方法

メッセージ トラッキングの有効化 （1 ページ）を参照してください。メッセージ トラッキングの詳細 （10 ページ）の添付ファイル名の検索の制約についても参照してください。

予想されるメッセージが検索結果に表示されない

問題

条件に一致するメッセージが検索結果に含まれていません。

解決方法

- さまざまな検索、特にメッセージイベントに関連する検索の結果は、電子メールゲートウェイの設定によって異なります。たとえばフィルタ処理していない URL カテゴリを検索すると、メッセージにそのカテゴリの URL が含まれていても、結果には表示されません。意図した動作を実現するように電子メールゲートウェイが正しく設定されていることを確認します。メール ポリシー、コンテンツ フィルタおよびメッセージ フィルタ、隔離の設定などを確認してください。
- レポートのリンクをクリックしても予想される情報が表示されない場合は、メール レポートのトラブルシューティングを参照してください。