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 E メール セキュリティ アプライアンス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、セキュリティ管理アプライアンスを設定します。『Cisco Content Security Management Appliance User Guide』を参照してください。

手順

ステップ 1 [サービス（Services）] > [集中管理サービス（Centralized 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）	このアプライアンスでメッセージ 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 E メール セキュリティ アプライアンスのメッセージをトレースするためにセキュリティ管理アプライアンスを使用します。

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。

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。

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	[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。
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。

オプション	説明
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 E メール セキュリティ アプライアンス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。
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。

オプション	説明
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、E メール セキュリティ アプライアンス上の各電子メール メッセージを一意に識別します。
Cisco IronPortホスト（Cisco IronPort Host）	特定の E メール セキュリティ アプライアンスを選択してそのアプライアンスで処理されたメッセージだけに検索対象を限定するか、またはすべてのアプライアンスを選択します。

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 （5 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。

- E メール セキュリティ アプライアンスのログに記録され、セキュリティ管理アプライアンス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。

- 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。

（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 （6 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	

項目	説明
受信時間（Received Time）	E メール セキュリティ アプライアンスがメッセージを受信した時間。 日時は、E メール セキュリティ アプライアンス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。
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。

項目	説明
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。
[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。
SBRS スコア（SBRS Score）	SenderBase 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。 SBRS の詳細については、送信者レピュテーション フィルタリングを参照してください。
[処理詳細（Processing Details）] セクション	

項目	説明
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アプライアンス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アプライアンス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

- 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 [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 2 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 3 [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　（11 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 （11 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 （11 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 （6 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

- さまざまな検索の結果、特にメッセージ イベントに関連する検索の結果は、アプリケーション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 E メール セキュリティ アプライアンス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。

予想されるメッセージが検索結果に表示されない