CHAPTER 6

電子メール メッセージのトラッキング

この章は、次の項で構成されています。

トラッキング サービスの概要

Security Management アプライアンスのトラッキング サービスは、Email Security アプライアンスを補完します。Security Management アプライアンスでは、電子メール管理者は、そのすべての Email Security アプライアンスを通過するメッセージのステータスを、1 つの場所で追跡します。

Security Management アプライアンスにより、Email Security アプライアンスが処理するメッセージのステータスを容易に検索できます。電子メール管理者は、メッセージの正確な場所を判断することにより、ヘルプ デスク コールを迅速に解決できます。管理者は、Security Management アプライアンスにより、あるメッセージについて、配信されたか、ウイルス感染が検出されたか、スパム検疫に入れられたか、それともメール ストリームの他の場所にあるのかを判断することができます。

grep や同様のツールを使用してログ ファイル全体を検索する代わりに、Security Management アプライアンスの柔軟なトラッキング インターフェイスを使用してメッセージを特定できます。さまざまな検索パラメータを組み合わせて使用できます。

次のトラッキング クエリーがあります。

- **エンベロープ情報：**照合するテキスト ストリングを入力することにより、特定のエンベロープ送信者またはエンベロープ受信者のメッセージを検索します。
- **件名ヘッダー：**件名行のテキスト文字列を照合します。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。
- **時間枠：**指定した日付と時刻の間に送信されたメッセージを検索します。
- **送信元 IP アドレスまたは拒否された接続：**特定の IP アドレスからのメッセージを検索します。または、検索結果内の拒否された接続を表示します。
- **添付ファイル名：**添付ファイル名に基づいてメッセージを検索できます。クエリーした名前の添付ファイルを少なくとも 1 つ含むメッセージが、検索結果に表示されます。

  パフォーマンス上の理由から、OLE オブジェクトなどの添付ファイル内にあるファイル名や、.ZIP ファイルなどのアーカイブ内にあるファイル名はトラッキングされません。

  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、たとえばメッセージやコンテンツのフィルタリング、DLP、または免責事項スタンプなど、その他のスキャン動作の一部としてのみ実行されます。添付ファイル名を使用できるのは、添付ファイルが添付された状態で行われる本文スキャンを通過したメッセージだけです。次に、添付ファイル名が表示されない場合のいくつかの例を示します（ただし、この場合に限定されません）。

  - システムがコンテンツ フィルタのみを使用し、アンチスパム フィルタまたはアンチウイルス フィルタによってメッセージがドロップされた場合や、メッセージの添付ファイルが除去された場合
  - 本文スキャンが行われる前に、メッセージ分裂ポリシーによっていくつかのメッセージから添付ファイルが除去された場合。
- **イベント：**ウイルス陽性、スパム陽性、またはスパムの疑いのフラグが設定されたメッセージ、配信された、ハード バウンスされた、ソフト バウンスされた、または Virus Outbreak 検疫に送信されたメッセージなど、指定されたイベントに一致するメッセージを探します。

- **メッセージ ID**：SMTP「Message-ID:」ヘッダーまたは Cisco IronPort メッセージ ID（MID）を識別することによってメッセージを検索します。
- **Email Security アプライアンス（ホスト）**：検索条件を特定の Email Security アプライアンスに絞り込みます。または、すべての管理対象アプライアンスを検索します。

中央集中型メッセージ トラッキングの設定について

中央集中型メッセージ トラッキングを設定するには、次の項を参照してください。

- 「Security Management アプライアンスでの中央集中型電子メール トラッキングのイネーブル化とディセーブル化」（P.3-6）。
- 「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）

トラッキング クエリーのセットアップについて

Security Management アプライアンスのトラッキング サービスにより、管理者は、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、ハード バウンスまたは配信されたかどうか等）などの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るようになります。管理者はメッセージ トラッキングにより、メッセージ フローを詳しく表示できます。また、処理イベント、添付ファイル名、またはエンベロープとヘッダーの情報など、メッセージの詳細情報を確認するために、特定の電子メール メッセージについて「掘り下げる」こともできます。

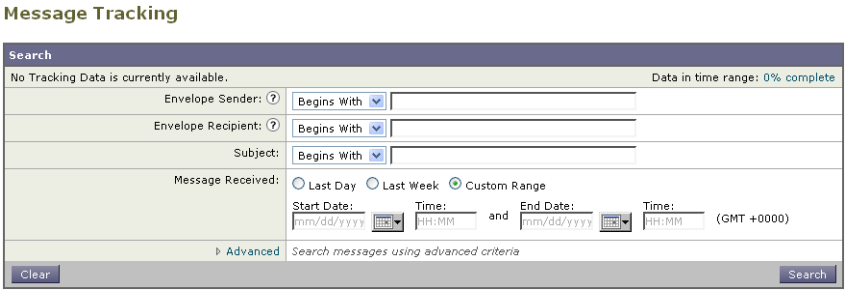
（注） このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

指定した基準と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するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Message Tracking] > [Message Tracking] を選択します。

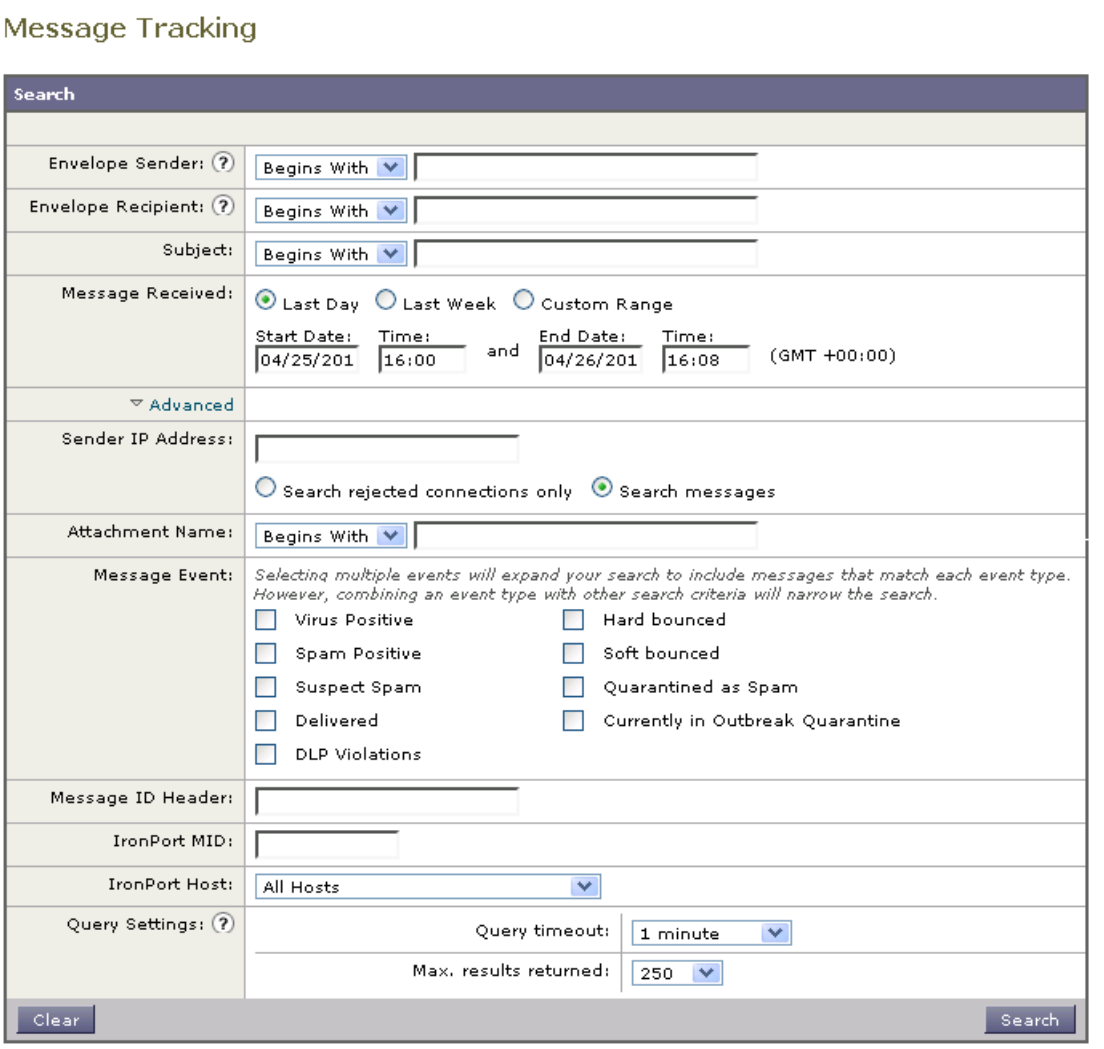
[Message Tracking] ページが表示されます。

図 6-1　[Message Tracking] ページ



必要に応じて、[Advanced] リンクをクリックして、トラッキング用の詳細オプションを表示します。

図 6-2　トラッキング用の詳細オプション



（注）　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。トラッキングの検索では、大文字と小文字が区別されません。

ステップ 2　追跡する電子メール メッセージを特定します。

メッセージ トラッキング クエリーを実行する場合は、次の検索パラメータを使用します。

- [Envelope Sender] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ送信者として検索するテキスト文字列を入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、添付ファイル名、およびドメインです。
- [Envelope Recipient] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ受信者として検索するテキストを入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、添付ファイル名、およびドメインです。

  Email Security アプライアンスでエイリアス拡張用のエイリアス テーブルを使用する場合、検索では、元のエンベロープ アドレスの代わりに、拡張された受信者アドレスが検出されます。それ以外の場合、メッセージ トラッキング クエリーは、元のエンベロープ受信者アドレスを検出します。
- [Subject] : [Begins With]、[Is]、[Contains]、または [Is Empty] を選択し、メッセージ件名行に対して検索するテキスト文字列を入力します。

（注） 国際文字セットは、件名ヘッダーでサポートされません。

- [Message Received] : [Last Day]、[Last 7 Days]、または [Custom Range] を使用して、クエリーの日付と時間範囲を指定します。過去 24 時間以内のメッセージを検索する場合は [Last Day] オプションを使用し、過去全 7 日間と検索当日の経過した時間までのメッセージを検索する場合は [Last 7 Days] オプションを使用します。

  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。終了日に現在の日付を指定し、終了時間を 23:59 に指定すると、クエリーは、現在の日付の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。アプライアンス上で日付と時間を表示するときは、そのアプライアンスの現地時間で表示されます。

メッセージは、Email Security アプライアンスでログに記録され、Security Management アプライアンスで取得されてから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。

- [Sender IP Address]：送信元 IP アドレスを入力し、メッセージを検索するか、または拒否された接続のみ検索するかを選択します。
- [Message Event]：追跡するイベントを選択します。オプションには、[Virus Positive]、[Spam Positive]、[Suspect Spam]、[Delivered]、[DLP Violations]（DLP ポリシーの名前を入力し、違反の重大度を選択でます）、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、および [Quarantined as Spam] があります。トラッキング クエリーに追加するほとんどの条件とは異なり、イベントは「OR」演算子で追加できます。複数のイベントを選択すると、検索結果は拡大します。
- [Message ID Header] と Cisco [IronPort MID]：メッセージ ID ヘッダーと Cisco IronPort メッセージ ID（MID）のいずれかまたは両方のテキスト文字列を入力します。
- [Query Settings]：ドロップダウン メニューで、クエリーがタイムアウトになるまで実行する期間を選択します。オプションには、[1 minute]、[2 minutes]、[5 minutes]、[10 minutes]、および [No time limit] があります。また、クエリーから返される、結果の最大数（最大 1000 個）も選択します。
- [Attachment Name]：[Begins With]、[Is]、または [Contains] を選択し、検索する 1 つの添付ファイル名を ASCII または Unicode のテキスト文字列で入力します。

ステップ 3　[Search] をクリックします。

検索クエリーの実行

クエリーを実行してメッセージを検索するには、次の手順を実行します。

ステップ 1　Security Management アプライアンスのウィンドウで、[Email] > [Message Tracking] > [Message Tracking] を選択します。

ステップ 2　必要な検索フィールドを入力します。

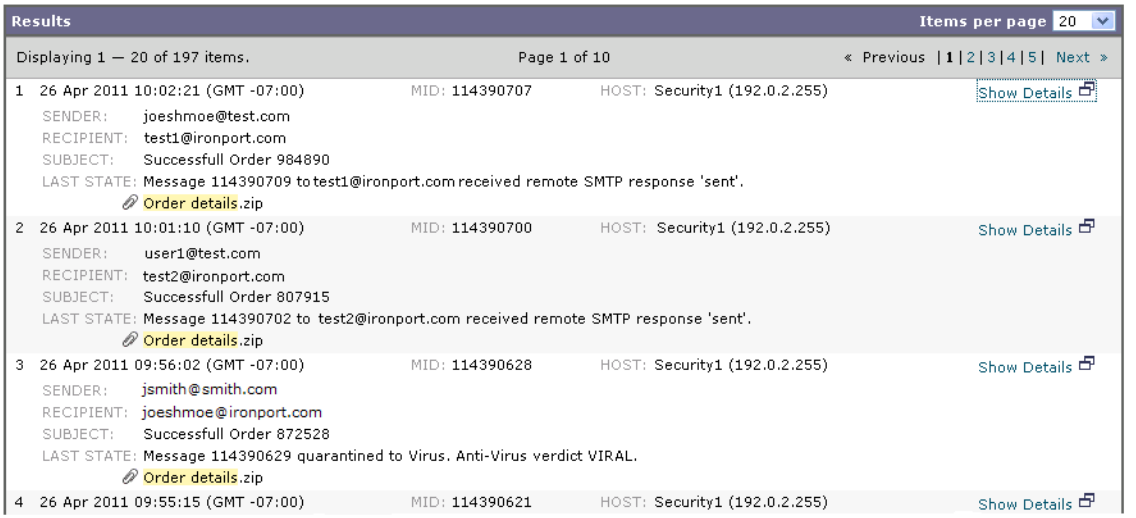
使用可能な検索フィールドの詳細については、「トラッキング クエリーのセットアップについて」（P.6-3）を参照してください。

すべてのフィールドを入力する必要はありません。[Message Event] オプションを除き、クエリーは「AND」検索になります。このクエリーは、検索フィールドに指定された「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。

ステップ 3　[Search] をクリックし、クエリーを送信します。

ページの下部にクエリー結果が表示されます。各行が 1 つの電子メール メッセージに対応します。

図 6-3　メッセージ トラッキング クエリーの結果



各行で検索条件が強調表示されます。

返される行数が [Items per page] フィールドで指定した値よりも大きい場合、結果は複数ページで表示されます。ページ間を移動するには、リストの上部または下部にあるページ番号をクリックします。

必要に応じて、新しい検索条件を入力して検索精度を高め、再びクエリーを実行します。または、次の項で説明するように、結果セットを絞り込むことによって検索精度を高めることができます。

結果セットの絞り込み

クエリーを実行すると、結果セットに必要以上の情報が含まれていることがあります。新しいクエリーを作成する代わりに、結果のリストにある行内の値をクリックすることによって結果セットを絞り込みます。値をクリックすると、そのパラメータ値が検索の条件として追加されます。たとえば、クエリー結果に複数の日付のメッセージが含まれている場合、行内の特定の日付をクリックして、その日付に受信されたメッセージだけを表示します。

結果セットを絞り込むには、次の手順を実行します。

ステップ 1　条件として追加する値の上にカーソルを移動します。値が黄色で強調表示されます。

次のパラメータ値を使用して、検索精度を高めます。

- Date and time
- Message ID（MID）
- Host（Email Security アプライアンス）
- Sender
- Recipient
- メッセージの件名行、または件名の最初の単語

ステップ 2　値をクリックして、検索を精密化します。

[Results] セクションには、元のクエリー パラメータ、*および*追加した新しい条件に一致するメッセージが表示されます。

ステップ 3　必要に応じて、結果内の他の値をクリックして、検索をさらに精密化します。

（注）　クエリー条件を削除するには、[Clear] をクリックし、新しいトラッキング クエリーを実行します。

トラッキング クエリー結果について

トラッキング クエリー結果には、トラッキング クエリーで指定した条件に一致するすべてのメッセージの一覧が表示されます。[Message Event] オプションを除き、クエリー条件は「AND」演算子で追加されます。結果セットのメッセージは、すべての「AND」条件を満たしている必要があります。たとえば、エンベロープ送信者は j で始まり、件名は t で始まることを指定すると、クエリーは、両方の条件を満たすメッセージだけを返します。

（注）　受信者が 50 以上のメッセージは、トラッキング クエリー結果に表示されません。この問題は、将来のリリースの AsyncOS で解決される予定です。

メッセージごとに、日付/時刻、送信者、受信者、件名、最後の状態、メッセージに含まれる添付ファイル、Cisco IronPort メッセージ ID（MID）、および Cisco IronPort ホスト（Email Security アプライアンス）の情報が表示されます。メッセージの詳細情報を表示するには、各メッセージの [Show Details] リンクをクリックします。詳細については、「メッセージの詳細」（P.6-10）を参照してください。

（注）　Security Management アプライアンスからは、最初の 10,000 行までのデータが返されます。さらに多くのレコードにアクセスするには、クエリー パラメータを調整し、新しいクエリーを実行してください。

メッセージの詳細

メッセージ ヘッダーや処理の詳細など、個々の電子メール メッセージに関する詳細情報を表示するには、検索結果リスト内の任意の項目に関して [Show Details] をクリックします。メッセージの詳細を表示した新しいウィンドウが開きます。

メッセージの詳細には、次のセクションが含まれます。

- 「Envelope and Header Summary」（P.6-11）
- 「Sending Host Summary」（P.6-11）
- 「Processing Details」（P.6-12）

Envelope and Header Summary

このセクションには、エンベロープ送信者や受信者など、メッセージのエンベロープとヘッダーの情報が表示されます。収集する情報は次のとおりです。

[Received Time] : Email Security アプライアンスがメッセージを受信した時間。

[MID] : メッセージ ID。

[Subject] : メッセージの件名行。

メッセージに件名がない場合、または Email Security アプライアンスがログファイルに件名行を記録するように設定されていない場合、トラッキング結果内の件名行は「(No Subject)」という値になることがあります。

[Envelope Sender] : SMTP エンベロープ内の送信者のアドレス。

[Envelope Recipients] : SMTP エンベロープ内の受信者のアドレス。

[Message ID Header] : 各電子メール メッセージを一意に識別する「Message-ID:」ヘッダー。メッセージが最初に作成されたときに、メッセージ内に挿入されます。「Message-ID:」ヘッダーは、特定のメッセージを検索する際に役立つ場合があります。

[Cisco IronPort Host] : メッセージを処理する Email Security アプライアンス。

[SMTP Auth User ID] : 送信者が SMTP 認証を使用して電子メールを送信した場合は、送信者の SMTP 認証ユーザ名。または、この値は「N/A」です。

[Attachments] : メッセージに添付されたファイルの名前。

Sending Host Summary

[Reverse DNS Hostname] : 逆引き DNS（PTR）ルックアップで確認された送信元ホストのホスト名。

[IP Address] : 送信元ホストの IP アドレス。

[SBRS Score]：SenderBase 評価スコア。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「None」の場合、そのメッセージが処理された時点において、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。

Processing Details

このセクションには、メッセージの処理中にログに記録されたステータス イベントが表示されます。

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 Matched Content

このセクションには、データ消失防止（DLP）ポリシーに違反するコンテンツが表示されます。

このコンテンツには、通常、企業の機密情報や、クレジット カード番号、健康診断結果などの個人情報が含まれるため、アプライアンスに対して管理者レベルのアクセス権を持たないユーザに対しては、このコンテンツへのアクセスをディセーブルにしたい場合があります。「メッセージ トラッキングでの機密情報へのアクセスのディセーブル化」（P.12-63）を参照してください。