CHAPTER 3

電子メール メッセージのトラッキング

この章は、次の内容で構成されています。

トラッキング サービスの概要

メッセージ トラッキング サービスにより、AsyncOS で処理されるメッセージのステータスを簡単に調べられるようになります。それにより、メッセージの正確な場所を確定して、ヘルプ デスク コールを迅速に解決できます。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ために、メッセージ トラッキングを使用できます。

メッセージ トラッキングは、ローカルの IronPort 電子メール セキュリティ アプライアンス上でイネーブルにできます。また、M-Series アプライアンス上で集中トラッキングをイネーブルにして、複数の電子メール セキュリティ アプライアンスに対してメッセージをトラッキングすることもできます。集中トラッキングをイネーブルにする手順については、『*Cisco IronPort AsyncOS for Security Management User Guide* 』を参照してください。ローカル トラッキングをイ

ネーブルにする手順については、「ローカル メッセージ トラッキングのイネーブル化とディセーブル化」（P.3-84）を参照してください。

「grep」などのツールを使用してログ ファイル全体を検索しなくても、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の場所を特定できます。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。

トラッキング クエリーには次の条件を含められます。

- **エンベロープ情報：**一致するテキスト 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受信者のメッセージを探します。
- **件名ヘッダー：**件名行のテキスト ストリングと一致します。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。
- **タイム フレーム：**指定された日時の間に送信されたメッセージを探します。
- **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。
- **イベント情報：**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 IronPort Message ID（MID; メッセージ ID）を識別してメッセージを探します。

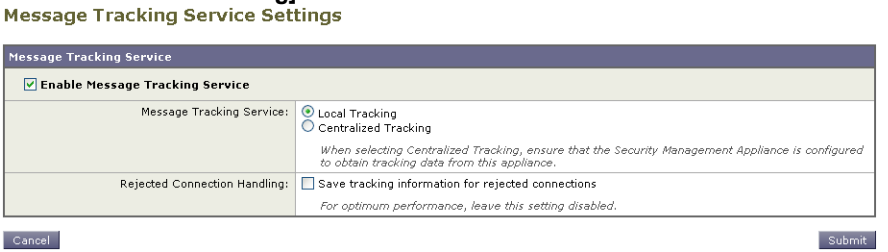
ローカル メッセージ トラッキングのイネーブル化とディセーブル化

ローカル メッセージ トラッキングをイネーブルにするには、次の手順を実行します。

ステップ 1　[Services] > [Message Tracking] をクリックします。

[Message Tracking] ページが表示されます。

図 3-1　ローカル メッセージ トラッキングをイネーブルにした [Message Tracking] ページ



ステップ 2　[Message Tracking] セクション内で、[Enable Message Tracking Service] をクリックします。

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、[Accept] をクリックします。

ステップ 3　必要に応じて、拒絶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。

ステップ 4　変更を送信し、保存します。

ローカル メッセージ トラッキングのディセーブル化

ローカル メッセージ トラッキング サービスをディセーブルにするには、次の手順を実行します。

ステップ 1　[Services] > [Message Tracking] で、[Edit Settings] ボタンをクリックします。

ステップ 2　[Enable Message Tracking Service] チェックボックスをオフにします。

ステップ 3　変更を送信し、保存します。

トラッキング クエリーのセットアップについて

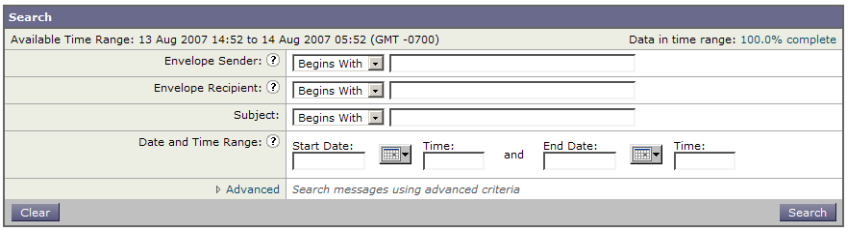
メッセージ トラッキング サービスにより、管理者は、メッセージ件名行、日時の範囲、エンベロープ送信者または受信者、処理イベント（たとえば、メッセージがウイルス陽性またはスパム陽性かどうか、ハード バウンスまたは配信されたかどうか等）などの指定した基準に一致する特定の電子メール メッセージまたはメッセージのグループを検索できるようになります。管理者は、メッセージ トラッキングを使用して、メッセージ フローを詳細に確認できます。また、処

理イベントや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。

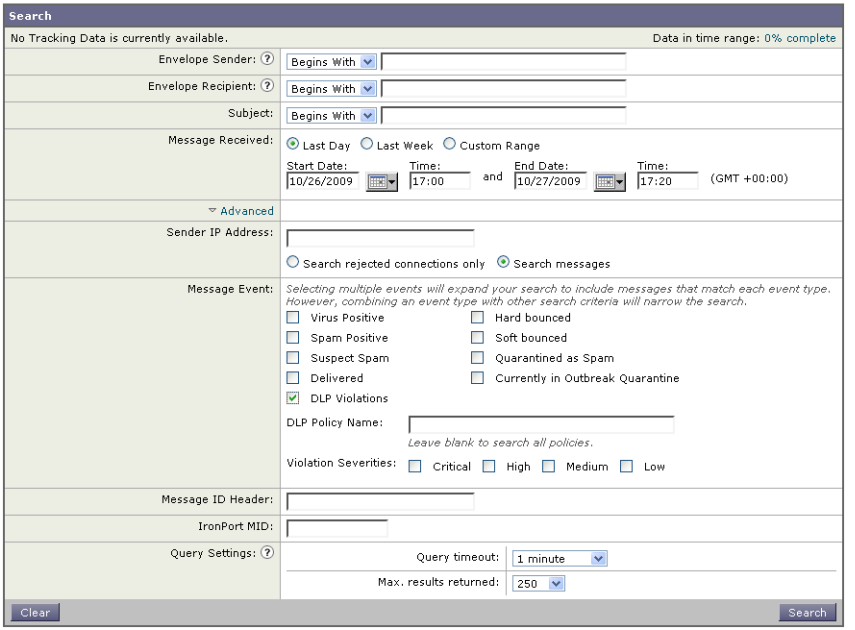
[Monitor] > [Message Tracking] ページを使用して、電子メール メッセージの場所を特定します。

図 3-2　[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 3-3　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。トラッキング検索では、大文字と小文字は区別されません。

メッセージ トラッキング クエリーを実行するとき、次の検索パラメータを使用できます。

- [Envelope Sender] : [Begins With]、[Is]、または [Contains] を選択し、エンベロープ送信者に対して検索するテキスト ストリングを入力します。有効なパラメータ値は、電子メール アドレス、ユーザ名、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に対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、およびドメインです。

  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、この検索では、元のエンベロープ アドレスではなく、拡張後の受信者アドレスが検索されます。それ以外の場合、メッセージ トラッキング クエリーでは、元のエンベロープ受信者アドレスが検索されます。

- [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 ストリングを入力します。

（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。

- **日付と時間：**クエリーの日付と時間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。

  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に変換されます。

  メッセージは、ロギング済みのものだけが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。詳細については、第 5 章「ロギング」を参照してください。

- [Message Event] : トラッキング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]、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、[DLP Violations]、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他の多くの条件とは異なり、イベントは「OR」演算子で追加されます。複数のイベントを選択すると、検索結果は拡大します。

  [DLP Violations] を選択すると、AsyncOS によって追加の DLP 関連オプションが表示されます。オプションには、メッセージが違反した DLP ポリシーとその違反の重大度（[Critical]、[High]、[Medium]、および [Low]）があります。

- [Message-ID Header] と MID :「Message-ID:」ヘッダーのテキスト ストリングと IronPort Message ID（MID; メッセージ ID）のいずれかまたは両方を入力します。

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。

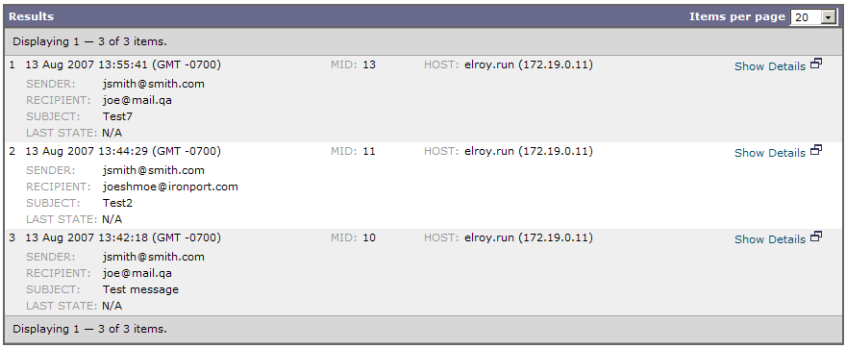
ステップ 1　[Monitor] > [Message Tracking] ページで、必要な検索フィールドを入力します。

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.3-85）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 2　[Search] をクリックして、クエリーを送信します。クエリーの結果がページの下部に表示されます。各行が 1 つの電子メール メッセージに対応します。

図 3-4　メッセージ トラッキング クエリーの結果



ステップ 3　返された行の数が [Items per page] フィールドに指定された値を上回ると、それらの結果は複数ページにわたって表示されます。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。

ステップ 4　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、クエリーを再実行します。あるいは、次の項の説明に従って、結果セットを絞り込むことにより検索を精密化することもできます。

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しなくても、行内の値をクリックして結果セットを絞り込めます。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できます。

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、検索を精密化できます。

- 日付と時間
- Message ID（MID; メッセージ ID）
- 送信者のユーザ名
- 送信者のドメイン
- 受信者のユーザ名
- 受信者のドメイン
- メッセージの件名行

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、元のクエリー パラメータと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] ボタンをクリックし、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 クエリーに指定された基準に一致するすべてのメッセージが一覧されます。[Message Event] オプションを除き、各クエリー条件は「AND」演算子で追加されます。結果セット内のメッセージは、これらの「AND」条件をすべて満たす必要があります。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。

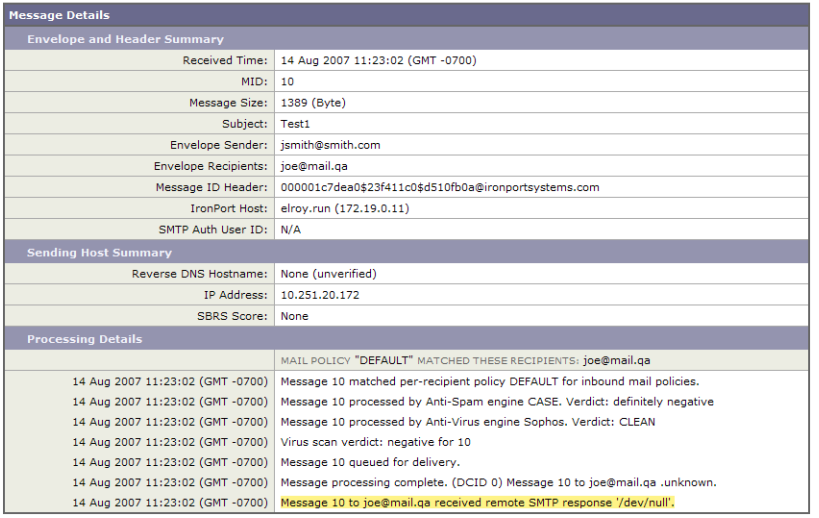
メッセージごとに、日付/時間、送信者、受信者、件名、最終状態、および IronPort Message ID（MID; メッセージ ID）が表示されます。メッセージの詳細情報を表示するには、各メッセージの [Show Details] リンクをクリックします。詳細については、「メッセージの詳細」（P.3-91）を参照してください。

（注）　セキュリティ管理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。それ以降のレコードにアクセスするには、クエリーを調整して、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、[Show Details] リンクをクリックします。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。

図 3-5　メッセージの詳細



メッセージの詳細には、[Envelope and Header Summary]、[Sending Host Summary] および [Processing Details] のセクションが含まれます。

[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]：電子メール 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。

[MID]：IronPort 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 IronPort 電子メール セキュリティ 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。

件名ヘッダーをロギングするように電子メール セキュリティ アプライアンスを設定する方法の詳細については、第 5 章「ロギング」を参照してください。

[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るときに挿入されます。「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。

[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、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 [N/A] になります。

[Sending Host Summary]

[Reverse DNS Hostname]：送信元ホストのホスト名。リバース DNS（PTR）ルックアップで検証されます。

[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ギングされたさまざまなステータス 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、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。