CHAPTER 6

電子メール メッセージのトラッキング

この章は、次の内容で構成されています。

トラッキング サービスの概要

セキュリティ管理アプライアンスのトラッキング サービスは、電子メール セキュリティ アプライアンスと補完関係にあります。セキュリティ管理アプライアンスによって、電子メール管理者はすべての電子メール セキュリティ 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 箇所から追跡できます。

セキュリティ管理アプライアンスを使用すると、電子メール セキュリティ アプライアンスで処理されるメッセージのステータスを容易に検出できます。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で、ヘルプ デスク コールを迅速に解決できます。管理者はセキュリティ管理アプライアンスを使用して、特定の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。

`grep` や同様のツールを使用してログ ファイルを検索する代わりに、セキュリティ管理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 クエリーには次の項目を含めることができます。

- **エンベロープ情報：**照合するテキスト文字列を入力し、特定のエンベロープ送信者または受信者から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。
- **タイム フレーム：**指定された日数と時間内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**：メッセージを添付ファイル名で検索できます。照会した名前の添付ファイルが少なくとも 1 つ含まれている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や .ZIP ファイルなどのアーカイブに含まれるファイル名は追跡されません。

添付ファイルの中には追跡されないものもあります。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、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でのみ使用できます。添付ファイル名が表示されない例を次に示します（ただしこれらに限られるわけではありません）。

  - システムがコンテンツ フィルタのみを使用しており、アンチスパム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か、その添付ファイルが除去された場合
  - 本文スキャンの実行前に、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や、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、またはウイルス アウトブレイク隔離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検索します。
- **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）を識別してメッセージを検索します。
- **電子メール セキュリティ アプライアンス（ホスト）：**検索条件を特定の電子メール セキュリティ アプライアンスに絞り込むか、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

中央集中型メッセージ トラッキングを設定するには、次の手順を順序どおりに実行します。

- 「セキュリティ管理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」（P.6-2）
- 「電子メール セキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定」（P.6-3）
- 「管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加」（P.6-3）

セキュリティ管理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

セキュリティ管理アプライアンスで中央集中型電子メール 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　セキュリティ管理アプライアンスの場合：

a. [Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。

b. [Message Tracking Service] セクションで [Enable] をクリックします。

c. システム セットアップ ウィザードを実行してから初めて中央集中型電子メッセージ 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。

[Centralized Message Tracking] ページが表示されます。中央集中型電子メール トラッキングをイネーブルにすると、[Message Tracking Service] ボックスの右側のカラムに [Enable] と表示されます。

d. セキュリティ管理アプライアンスでの変更を**送信**し、確定します。

電子メール セキュリティ アプライアンスでの中央集中型メッセージ トラッキングの設定

電子メール セキュリティ アプライアンス上で中央集中型メッセージ トラッキングを設定するには、次の手順を実行します。

ステップ 1　電子メール セキュリティ アプライアンスでメッセージ トラッキングが設定され、正常に動作していることを確認します。

ステップ 2　[Security Services] > [Message Tracking] に移動します。

ステップ 3　[Edit Settings] をクリックします。

ステップ 4　[Centralized Tracking] を選択します。

ステップ 5　[Submit] をクリックします。

ステップ 6　電子メールの添付ファイル名を検索および記録できるようにする場合は、次の点に注意してください。

少なくとも 1 つの受信コンテンツ フィルタまたは本文スキャン機能が 電子メール セキュリティ アプライアンスで設定され、イネーブルになっていることを確認します。コンテンツ フィルタおよび本文スキャンの詳細については、『*Cisco IronPort AsyncOS for Email Security Advanced Configuration Guide*』を参照してください。

ステップ 7　変更を保存します。

ステップ 8　管理対象の各電子メール セキュリティ アプライアンスに対してこの手順を繰り返します。

管理対象の各電子メール セキュリティ アプライアンスへの中央集中型メッセージ トラッキング サービスの追加

他の中央集中型管理機能を設定する際、すでにアプライアンスを追加したかどうかによって、ここでの手順は異なります。

ステップ 1　セキュリティ管理アプライアンスで、[Management Appliance] > [Centralized Services] > [Security Appliances] を選択します。

ステップ 2　このページのリストに、すでに電子メール セキュリティ アプライアンスを追加している場合は、次の手順を実行します。

a. 電子メール セキュリティ アプライアンスの名前をクリックします。

b. [Centralized Message Tracking] サービスを選択します。

ステップ 3　電子メール セキュリティ アプライアンスを追加していない場合は、次の手順を実行します。

a. [Add Email Appliance] をクリックします。

b. [Appliance Name and IP Address] テキスト フィールドに、Cisco IronPort アプライアンスの管理インターフェイスのアプライアンス名と IP アドレスを入力します。

（注）　[IP Address] テキスト フィールドに DNS 名を入力した場合でも、[Submit] をクリックすると、すぐに IP アドレスに解決されます。

c. [Centralized Message Tracking] サービスがすでに選択されています。

d. [Establish Connection] をクリックします。

e. 管理対象となるアプライアンスの管理者アカウントのユーザ名とパスワードを入力し、[Establish Connection] をクリックします。

（注）　ログイン資格情報を入力すると、セキュリティ管理アプライアンスからリモート アプライアンスへのファイル転送のための公開 SSH キーが渡されます。ログイン資格情報は、セキュリティ管理アプライアンスには保存されません。

f. [Success] メッセージがページのテーブルの上に表示されるまで待機します。

g. [Test Connection] をクリックします。

h. テーブルの上のテスト結果を確認します。

ステップ 4　[Submit] をクリックします。

ステップ 5　中央集中型メッセージ トラッキングをイネーブルにする各電子メール セキュリティ アプライアンスに対し、この手順を繰り返します。

ステップ 6　変更を保存します。

機密情報へのアクセスの管理

管理タスクを数人で分配する場合、データ消失防止（DLP）ポリシーに違反するメッセージに表示される機密情報へのアクセスを制限するには、「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.12-25）を参照してください。

電子メール メッセージの検索

セキュリティ管理アプライアンスのトラッキング 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。

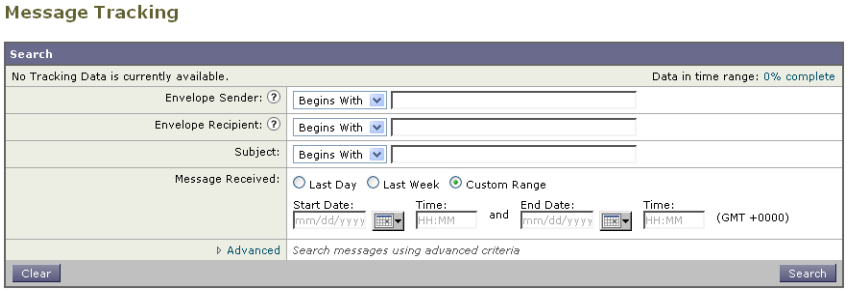
（注）　このトラッキング コンポーネントにより個々の電子メール メッセージの詳細な情報が提供されますが、このコンポーネントを使用してメッセージの内容を読むことはできません。

指定した条件に一致する個々の電子メール 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 appliance] ウィンドウで [Email] > [Message Tracking] > [Message Tracking] を選択します。

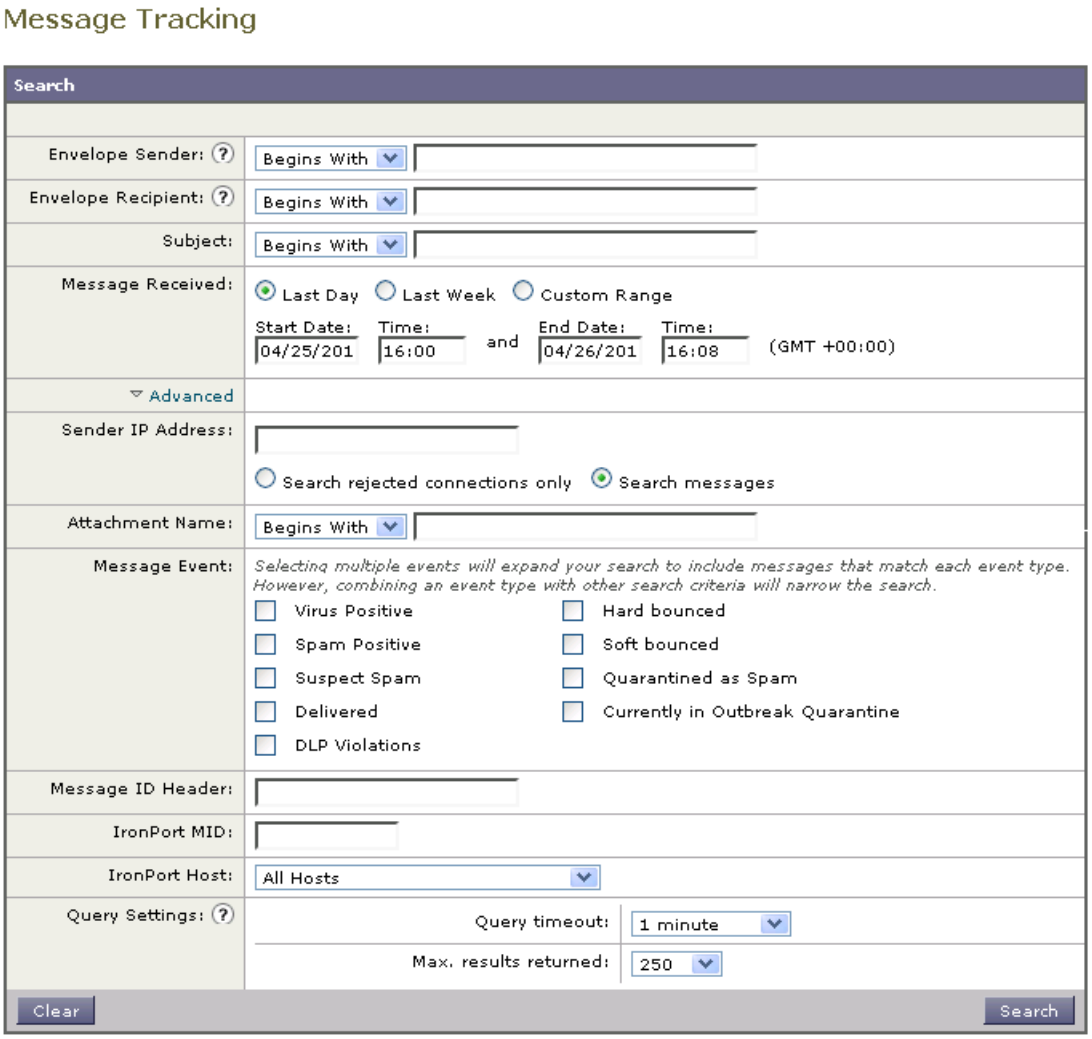
[Message Tracking] ページが表示されます。

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。トラッキング検索では大文字と小文字は区別されません。

ステップ 2　検索条件を入力します。

- [Envelope Sender] : [Begins With]、[Is]、または [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。
- [Envelope Recipient] : [Begins With]、[Is]、または [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 セキュリティ アプライアンス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。
- [Subject] : [Begins With]、[Is]、[Contains]、または [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。

（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 [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 [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、クエリー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。アプライアンス上で日付と時刻を表示する場合は、そのアプライアンスの現地時間で表示されます。

  メッセージの検索結果は、それらメッセージが電子メール 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した後でのみ表示されます。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] : 送信者の IP アドレスを入力し、メッセージを検索するか、あるいは拒否された接続だけを検索するかを選択します。
- [Message Event] : 追跡対象のイベントを選択します。オプションは、[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きます）、[Hard Bounced]、[Soft Bounced]、[Currently in Outbreak Quarantine]、[Quarantined as Spam] です。トラッキング クエリーに追加する多くの条件と違い、イベントは「OR」演算子を使用して追加します。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 and Cisco IronPort 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。
- [Query Settings] : ドロップダウン メニューから、タイムアウトまでのクエリーの実行時間を選択します。オプションは、[1 minute]、[2 minutes]、[5 minutes]、[10 minutes]、[No time limit] です。クエリーから返される結果の最大数（最大 1000）も選択します。

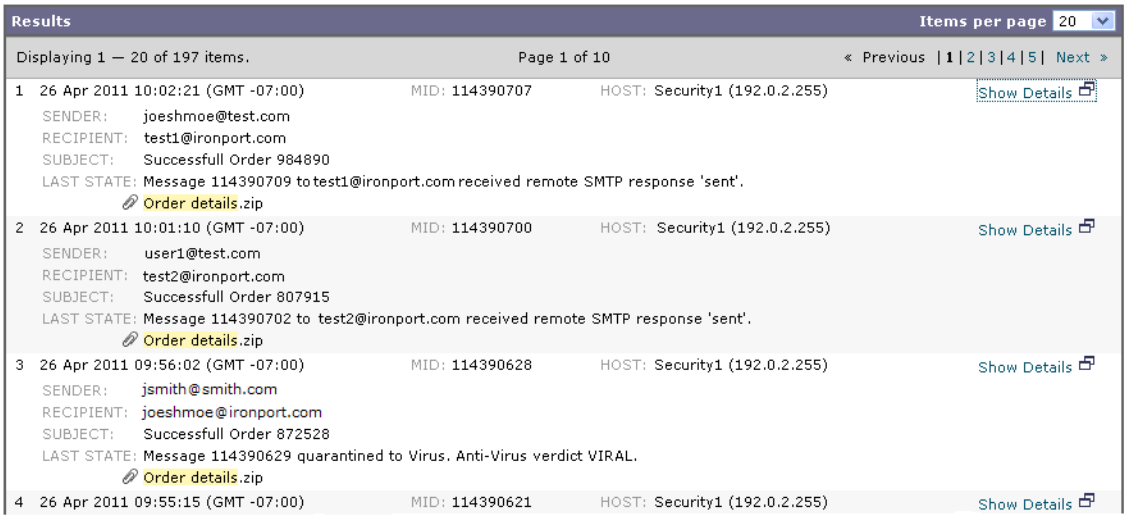
- [Attachment name] : [Begins With]、[Is]、または [Contains] を選択し、検索する添付ファイル名の ASCII または Unicode テキスト文字列を入力します。入力したテキストの先頭および末尾のスペースは除去されません。

すべてのフィールドに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。

返された行数が [Items per page] フィールドで指定した値よりも大きい場合、結果は複数のページに表示されます。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。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。

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のではなく、結果リストの行内の値をクリックし、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すると、その日付に受信されたメッセージだけが表示されます。

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、検索を精密化します。

- Date and time
- Message ID（MID）
- Host（電子メール セキュリティ アプライアンス）
- Sender
- Recipient
- メッセージの件名行、または件名の先頭語

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、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がリストされます。[Message Event] オプションを除き、クエリー条件は「AND」演算子を使用して追加します。結果セット内のメッセージは、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）　50 名以上の受信者がいるメッセージは、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、AsyncOS の今後のリリースで解決される予定です。

各メッセージについて、日付/時刻、送信者、受信者、件名、最終状態、メッセージに含まれていた添付ファイル、Cisco IronPort メッセージ ID（MID）、および Cisco IronPort ホスト（電子メール セキュリティ アプライアンス）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.6-8）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。その他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ます。

メッセージの詳細

メッセージ ヘッダー情報や処理の詳細など、特定の電子メール メッセージの詳細情報を表示するには、検索結果リストの任意のアイテムで [Show Details] をクリックします。メッセージの詳細が表示され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

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刻。

[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。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。「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]：メッセージを処理した電子メール セキュリティ 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。それ以外の場合、この値は「N/A」となります。

[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]：送信側ホストのホスト名。逆引き DNS（PTR）ルックアップで検証されます。

[IP Address]：送信側ホストの IP アドレス。

[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「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、アンチスパムおよびアンチウイルス スキャンなどの電子メール ポリシーの処理や、メッセージ分割などそ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ると、配信の詳細情報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。

通常、このコンテンツには機密情報、たとえば企業秘密や、クレジット カード番号、健康診断の結果などの個人情報が含まれるため、セキュリティ管理アプライアンスへのアクセス権はあるが管理者レベルの権限を所持していないユーザに対し、このコンテンツへのアクセスをディセーブルにする必要が生じることがあります。「メッセージ トラッキングでの DLP 機密情報へのアクセスの制御」（P.12-25）を参照してください。