



CHAPTER 6

電子メール メッセージのトラッキング

- 「トラッキング サービスの概要」 (P.6-1)
- 「中央集中型メッセージトラッキングの設定」 (P.6-2)
- 「メッセージトラッキングデータアベイラビリティの確認」 (P.6-4)
- 「電子メールメッセージの検索」 (P.6-5)
- 「トラッキングクエリー結果について」 (P.6-8)

トラッキング サービスの概要

シスコのコンテンツ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を補完します。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

手順

-
- | | |
|---------------|--|
| ステップ 1 | セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [集約管理 サービス (Centralized Services)] > [メール (Email)] > [集約メッセージ トラッキング (Centralized Message Tracking)] を選択します。 |
| ステップ 2 | [メッセージ トラッキング サービス (Message Tracking Service)] セクションで [有効 (Enable)] をクリックします。 |
| ステップ 3 | 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、[承認 (Accept)] をクリックします。 |
| ステップ 4 | 変更を送信し、保存します。 |
-

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

手順

-
- 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** [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)] に移動します。
- ステップ 3** [設定を編集 (Edit Settings)] をクリックします。
- ステップ 4** [集約管理トラッキング (Centralized Tracking)] を選択します。
- ステップ 5** [送信 (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、ご使用の電子メール セキュリティ アプライアンスのマニュアルまたはオンライン ヘルプ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

ここで実行する手順は、他の中央集中型管理機能の設定時に、すでにこのアプライアンスを追加したかどうかによって異なります。

手順

-
- ステップ 1** セキュリティ管理アプライアンスで、[管理アプライアンス (Management Appliance)] > [集約管理サービス (Centralized Services)] > [セキュリティ アプライアンス (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. [集約メッセージ トラッキング (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. [メール アプライアンスの追加 (Add Email Appliance)] をクリックします。
 - b. [アプライアンス名 (Appliance Name)] および [IP アドレス (IP Address)] テキスト フィールドに、電子メール セキュリティ 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 アドレス (IP Address)] テキスト フィールドに DNS 名を入力した場合でも、[送信 (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. [集約メッセージ トラッキング (Centralized Message Tracking)] サービスがすでに選択されています。
- d. [接続の確立 (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、[接続の確立 (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. [成功 (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. [テスト接続 (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 [送信 (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、データ漏洩防止 (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.13-24) を参照してください。

メッセージ トラッキング データ アベイラビリティの確認

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。

ステップ 1 [メール (Email)] > [メッセージ トラッキング (Message Tracking)] > [有効なメッセージ トラッキング データ (Message Tracking Data Availability)] を選択します。

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。

手順

- ステップ 1** セキュリティ管理アプライアンスで、[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** (任意) [拡張 (Advanced)] リンクをクリックし、その他の検索オプションを表示します。
- ステップ 3** 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。

- [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。
 - 電子メールドメインの場合
example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]
 - 完全な電子メールアドレスの場合
user@example.com, user@[203.0.113.15] または *user@[ipv6:2001:db8:80:1::5]*
 - 文字を入力できます。入力の検証は実行されません。
- [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、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。

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。入力の検証は実行されません。

- [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 [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。

- [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 [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ト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。
- [送信者 IP アドレス (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。
 - 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、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。オプションは、コンテンツ フィルタによって検出され、ポリシー、ウイルス、またはアウトブレイク隔離に現在ある [ウイルス検出 (Virus Positive)]、[明確なスパム (Spam Positive)]、[サスペクト スпам (Suspect Spam)]、[送信完了 (Delivered)]、[DLP 違反 (DLP Violations)] (DLP ポリシー名を入力し違反の重大度または対処を選択可能)、[ハード バウンス (Hard Bounced)]、[ソフト バウンス (Soft Bounced)]、および [スпамとして隔離 (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。
- [メッセージ ID ヘッダーと Cisco IronPort MID (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。
- [クエリ設定 (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 分 (1 minute)]、[2 分 (2 minutes)]、[5 分 (5 minutes)]、[10 分 (10 minutes)]、[時間制限なし (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。
- [添付ファイル名 (Attachment name)]: [次に始まる (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。

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 4 [検索 (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 6-1 メッセージトラッキングクエリーの結果

Results			Items per page 20
Displaying 1 – 20 of 197 items.			Page 1 of 10 < Previous 1 2 3 4 5 Next >
1	26 Apr 2011 10:02:21 (GMT -07:00)	MID: 114390707	HOST: Security1 (192.0.2.255) Show Details
SENDER: joeshmoe@test.com			
RECIPIENT: test1@ironport.com			
SUBJECT: Successfull Order 984890			
LAST STATE: Message 114390709 to test1@ironport.com received remote SMTP response 'sent'.			
Order details.zip			
2	26 Apr 2011 10:01:10 (GMT -07:00)	MID: 114390700	HOST: Security1 (192.0.2.255) Show Details
SENDER: user1@test.com			
RECIPIENT: test2@ironport.com			
SUBJECT: Successfull Order 807915			
LAST STATE: Message 114390702 to test2@ironport.com received remote SMTP response 'sent'.			
Order details.zip			
3	26 Apr 2011 09:56:02 (GMT -07:00)	MID: 114390628	HOST: Security1 (192.0.2.255) Show Details
SENDER: jsmith@smith.com			
RECIPIENT: joeshmoe@ironport.com			
SUBJECT: Successfull Order 872528			
LAST STATE: Message 114390629 quarantined to Virus. Anti-Virus verdict VIRAL.			
Order details.zip			
4	26 Apr 2011 09:55:15 (GMT -07:00)	MID: 114390621	HOST: Security1 (192.0.2.255) Show Details

各行で検索条件が強調表示されます。

返された行数が [ページ当たりのアイテム数 (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

クエリを実行すると、結果セットに必要な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。

手順

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。

- 日時 (Date and time)
- メッセージ ID (Message ID) (MID)
- ホスト (Host) (電子メールセキュリティ アプライアンス)
- 送信者 (Sender)
- 受信者 (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。

[結果 (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、[消去 (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。[メッセージ イベント (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。

メッセージの詳細情報を表示するには、各メッセージの [詳細の表示 (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)**
- 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、今後のリリースで解決される予定です。
 - クエリーを指定するとき、最大 1000 件の検索結果を表示するを選択できます。条件に一致したメッセージを最大 50,000 件表示するには、検索結果セクションの上の [すべてをエクスポート (Export All)] リンクをクリックし、別のアプリケーションで結果の .csv ファイルを開きます。
 - 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、その結果が予期しないものであった場合、これは、確認期間中にレポートとトラッキングを同時におよび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。
 - メッセージ トラッキングの検索結果の印刷およびエクスポートについて詳しくは、「[レポート データおよびトラッキング データの印刷およびエクスポート](#)」(P.3-10) を参照してください。

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 [詳細の表示 (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。

- 「[エンベロープとヘッダーのサマリー](#)」(P.6-9)
- 「[ホスト サマリイの送信](#)」(P.6-9)
- 「[処理詳細](#)」(P.6-9)

エンベロープとヘッダーのサマリー

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。

[受信時間 (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。

[件名 (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「(件名なし (No Subject))」という値になることがあります。

[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)] : SMTP エンベロープ内の受信者のアドレス。

[メッセージ ID ヘッダー (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 ホスト (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 ユーザ ID (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。

[添付ファイル (Attachments)] : メッセージに添付されたファイルの名前。

ホスト サマリーの送信

[逆引き DNS ホスト名 (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 アドレス (IP Address)] : 送信側ホストの 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「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。

処理詳細

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。たとえば、メッセージが配信され、コピーが隔離に保存されている場合があります。

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

このセクションには、データ漏洩防止 (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.13-24) を参照してください。