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 （1 ページ）
- 中央集中型メッセージ トラッキングの設定 （2 ページ）
- メッセージ トラッキング データの有効性の検査 （5 ページ）
- 電子メール メッセージの検索 （5 ページ）
- トラッキング クエリ結果について （12 ページ）
- メッセージ トラッキングのトラブルシューティング （17 ページ）

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、E 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E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、Eメール セキュリティ アプライアンスによって処理されるメッセージの状態を簡単に把握できるようになります。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 クエリには次の項目を含めることができます。

- **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。
- **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**：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。
- **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。

  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

- **ファイル SHA256**：メッセージ ファイルの SHA-256 値を持つメッセージを検索します。
- **Cisco ホスト**：検索条件を特定の E メール セキュリティ アプライアンスに絞り込むか、管理されているすべてのアプライアンスを検索対象とします。
- **メッセージ ID ヘッダーおよび Cisco MID**：SMTP「Message-ID:」ヘッダー、または Cisco メッセージ ID（MID）を識別してメッセージを検索します。
- **送信者 IP アドレス/ドメイン/ネットワーク所有者**：特定の IP アドレス、ドメイン名、またはネットワーク所有者からのメッセージを検索します。
- **メッセージ 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。
- **拒否された接続**：拒否された接続の特定の IP アドレス、ドメイン名またはネットワーク所有者からのメッセージを検索結果で検索します。

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（3 ページ）

• E 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 （3 ページ）
• 管理対象の各 E 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 （4 ページ）

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

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [Management Appliance] > [Centralized Services] > [Email] > [Centralized Message Tracking] を選択します。

ステップ 3 [メッセージトラッキングサービス（Message Tracking Service）] セクションで [有効化（Enable）] をクリックします。

ステップ 4 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 5 変更を**送信**し、保存します。

E 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

ステップ 1 E 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 [設定の編集（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 フィルタまたはその他の本文スキャン機能が E メール セキュリティ アプライアンスで設定され、有効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 E 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 E メール セキュリティ アプライアンスに同様の手順を繰り返します。

管理対象の各 E 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 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [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 3 このページのリストに、すでに E 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) E 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 4 E メール セキュリティ アプライアンスをまだ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、E 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）] 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、IP アドレスに変換されます。

c) [集約メッセージトラッキング（Centralized Message Tracking）] サービスが事前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フレーズを入力し、[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 Security Management Appliance に保存されません。

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) [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 5 [送信（Submit）] をクリックします。

ステップ 6 中央集中型メッセージ トラッキングを有効にする各 E 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 7 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 トラッキングでの機密情報へのアクセスの制御を参照してください。

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。

ステップ 1 （新しい Web インターフェイスのみ）セキュリティ管理アプライアンスで ⚙ をクリックして、レガシー Web インターフェイスをロードします。

ステップ 2 [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

- 新しい Web インターフェイスでの電子メール メッセージの検索 （5 ページ）
- レガシー Web インターフェイスでの電子メール メッセージの検索 （8 ページ）

新しい Web インターフェイスでの電子メール メッセージの検索

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。

ステップ 1 セキュリティ管理アプライアンスで、[トラッキング（Tracking）] > [検索（Search）] を選択します。

ステップ 2 [メッセージ（Messages）] タブまたは [拒否された接続（Connections Rejected）] タブを選択し、検索結果を絞り込みます。

（注） 送信者 IP アドレス、ドメイン、またはネットワーク所有者に基づいて拒否された接続を検索することができます。

ステップ 3 （任意）[詳細検索（Advanced Search）] 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 4 次の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。

- （メッセージと拒否された接続の場合）[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。

  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。

- [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。
  - E メール ドメインの場合：*example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]*
  - 完全 E メール アドレスの場合：*user@example.com, user@[203.0.113.15] or user@[ipv6:2001:db8:80:1::5]*。
  - 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）]、[次を含む（Contains）]、または [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。

- [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。

  E 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。入力した内容は実行されません。

- [添付ファイル名（Attachment Name）]：[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。
- Reply-To：[次で始まる（Begins With）]、[次に合致する（Is）]、または [含む（Contains）] を選択して、メッセージの「`Reply-To`」ヘッダーに基づいてメッセージを検索する文字列を入力します。
- [ファイルSHA256（File SHA256）]：メッセージのファイルの SHA-256 値を入力します。

  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。
- [シスコのホスト（Cisco Host）]：[すべてのホスト（All Host）] を選択してすべての E メールセキュリティ アプライアンス間で検索するか、ドロップダウン メニューから必要な E メールセキュリティ アプライアンスを選択します。
- [メッセージIDヘッダーおよびCisco MID（Message ID Header and Cisco 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。
- （メッセージと拒否された接続の場合）[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）]：送信元 IP アドレス、ドメインまたはネットワーク所有者の詳細を入力します。
  - 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 箇所で、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、[ウイルス検出（Virus Positive）]、[明確なスパム（Spam Positive）]、[サスペクト スパム（Suspect Spam）]、[含まれている悪意のある URL（contained malicious URLs）]、[指定されたカテゴリに含まれている URL（contained URL in specified category）]、[DLP 違反（DLP Violations）]（DLP ポリシーの名前を入力して、違反の重大度または実行アクションを選択できます）、[DMARC 違反（DMARC violations）]、[送信完了（Delivered）]、[高度なマルウェア保護ポジティブ（Advanced Malware Protection Positive）]（添付ファイルで検出されるマルウェア用）、[ハードバウンス（Hard Bounced）]、[ソフト バウンス（Soft Bounced）]、[現在、ポリシー隔離に隔離（currently in policy quarantine）]、[現在、ウイルス隔離に隔離（currently in virus quarantine）]、[現在、アウトブレイク隔離に隔離（currently in outbreak quarantine）]、[メッセージ フィルタで検出（caught by message filters）]、[コンテンツ フィルタで検出（caught by content filters）]、[スパムとして隔離（Quarantined as Spam）] です。トラッキング クエリ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。

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、クエリは「AND」検索になります。このクエリは、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 5 [検索（Search）] をクリックします。

各行が 1 つの電子メール メッセージに対応します。ビューでメッセージをさらにロードするにはスクロールダウンします。

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、クエリを再実行します。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。

次のタスク

- 結果セットの絞り込み （11 ページ）
- メッセージ トラッキングおよび高度なマルウェア防御機能について （12 ページ）
- トラッキング クエリ結果について （12 ページ）

レガシー Web インターフェイスでの電子メール 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。

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 （任意）[詳細設定（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。

- E メール ドメインの場合：example.com, [203.0.113.15], [ipv6:2001:db8:80:1::5]
- 完全 E 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。入力した内容は実行されません。

- [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。

E 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）]、[次を含む（Contains）]、または [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。

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。

- [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 箇所で、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、[ウイルス検出（Virus Positive）]、[明確なスパム（Spam Positive）]、[サスペクト スパム（Suspect Spam）]、[含まれている悪意のある URL（contained malicious URLs）]、[指定されたカテゴリに含まれている URL（contained URL in specified category）]、[DLP 違反（DLP Violations）]（DLP ポリシーの名前を入力して、違反の重大度または実行アクションを選択できます）、[DMARC 違反（DMARC violations）]、[送信完了（Delivered）]、[高度なマルウェア防御ポジティブ（Advanced Malware Protection Positive）]（添

付ファイルで検出されるマルウェア用）、[ハードバウンス（Hard Bounced）]、[ソフトバウンス（Soft Bounced）]、[現在、ポリシー隔離に隔離（currently in policy quarantine）]、[現在、ウイルス隔離に隔離（currently in virus quarantine）]、[現在、アウトブレイク隔離に隔離（currently in outbreak quarantine）]、[メッセージ フィルタで検出（caught by message filters）]、[コンテンツ フィルタで検出（caught by content filters）]、[検出されたマクロ ファイル タイプ（Macro File Types Detected）]、[地理位置情報（Geolocation）]、[低リスク（Low Risk）]、[スパムとして隔離（Quarantined as Spam）] です。トラッキング クエリ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の実行時間を選択します。オプションは、[1分（1 minutes）]、[2分（2 minutes）]、[5分（5 minutes）]、[10分（10 minutes）]、および [時間制限なし（No time limit）] です。また、クエリが返す結果の最大数を選択します（最大 1000）。
- [添付ファイル名（Attachment name）]：[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。

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、クエリは「AND」検索になります。このクエリは、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。

各行で検索条件が強調表示されます。

返された行数が [ページ当たりの項目数（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、新しい検索基準を入力することにより検索を精密化し、クエリを再実行します。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。

次のタスク

- 結果セットの絞り込み （11 ページ）
- メッセージ トラッキングおよび高度なマルウェア防御機能について （12 ページ）
- トラッキング クエリ結果について （12 ページ）

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。

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
- メッセージ ID（MID）
- ホスト（E メール セキュリティ アプライアンス）
- 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 （新しい Web インターフェイスのみ）メッセージ トラッキング検索条件で [変更（Modify）] をクリックします。

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
- メッセージ ID（MID）
- Cisco ホスト（E メール セキュリティ アプライアンス）
- Sender
- 受信者（Recipient）
- メッセージの件名行、または件名の先頭語
- メッセージ イベント（Message Event）
- その他の詳細（メッセージの最後の状態、SBRS、送信者 IP、およびグループ）

ステップ 3 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 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 4 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） クエリ条件を削除するには、[クリア（Clear）] をクリックし、新しいトラッキング クエリを実行します。

メッセージ トラッキングおよび高度なマルウェア防御機能について

メッセージ トラッキングのファイル脅威情報を検索する際は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪質なファイルを検索するには、メッセージ トラッキングの [詳細設定（Advanced）] セクションで、[メッセージイベント（Message Event）] オプションの [高度なマルウェア保護ポジティブ（Advanced Malware Protection Positive）] を選択します。
- メッセージトラッキングにはファイル レピュテーション処理についての情報と、メッセージが処理されたときに返された元のファイル レピュテーションの判定のみが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

  メッセージ トラッキングの詳細の [処理詳細（Action Details）] セクションには、以下の情報が表示されます。

  - メッセージの各添付ファイルの SHA-256
  - メッセージ全体に対する高度なマルウェア防御の最終判定
  - マルウェアが検出された添付ファイル

    クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。

- 判定のアップデートは [AMP判定のアップデート（AMP Verdict Updates）] レポートでのみ使用できます。メッセージ トラッキングの元のメッセージの詳細は、判定が変更されても更新されません。特定の添付ファイルを含むメッセージを表示するには、判定アップデート レポートで SHA-256 をクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析（File Analysis）] レポートにのみ表示されます。

  分析済みファイルのその他の情報は、クラウドから入手できます。ファイルの使用可能なファイル分析情報を表示するには、[モニタ（Monitor）]>[ファイル分析（File Analysis）] を選択して、ファイルを検索する SHA-256 を入力します。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

  分析用に送信されたファイルの後続インスタンスをアプライアンスが処理すると、そのインスタンスはメッセージ トラッキングの検索結果に表示されるようになります。

トラッキング クエリ結果について

結果が予期したものでない場合は、メッセージ トラッキングのトラブルシューティング （17 ページ）を参照してください。

トラッキング クエリ結果には、トラッキング クエリ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、そのメッセージの新しい Web インターフェイスで [詳細の表示（More Details）] または、レガシー Web インターフェイスで [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 （13 ページ）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。
- （新しい Web インターフェイスのみ）クエリを指定する場合は、検索結果を表示するために下方向にスクロールすることができます。下方向へスクロールすると、より多くの結果がビューに表示されます。
- 検索結果セクションの上部にある [エクスポート（Export）] リンクを使用すると、検索結果を .csv ファイルにエクスポートできます。

  クエリを指定するとき、最大 1000 件の検索結果を表示することを選択できます。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ティングとトラッキングを両方同時におよび継続して有効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、レポーティング データおよびトラッキング データのエクスポートを参照してください。

関連項目

メッセージの詳細 （13 ページ）

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（More Details）] リンクをクリックします。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。

- 判定チャートと最後の状態の判定 （14 ページ）

- エンベロープとヘッダーのサマリー （15 ページ）
- ホスト サマリーの送信 （16 ページ）
- 処理詳細 （16 ページ）

判定チャートと最後の状態の判定

判定チャートには、E メール セキュリティ アプライアンス内の各エンジンによってトリガーされる可能性のあるさまざまな判定の情報が表示されます。

（注） 12.0 よりも前の AsyncOS では判定チャートが表示されず、最後の状態の判定は [最後の状態が使用不可（Last State Not Available）] として表示されます。

次の表に、各エンジンのさまざまな判定を示します。

表 *1*: 判定チャート

接続動作	メッセージ フィルタ	スパム対策	ウイルス対策	AMP	グレイメール	コンテンツ フィルタ	アウトブレイク フィルタ	DLP
N/A 承認（Accepted） リレー済み（Relayed）	未評価（Not Evaluated） 一致（Match） 不一致（No Match）	未評価（Not Evaluated） 負値 疑わしい（Suspect） バルク メール ソーシャル メール マーケティング メール 正値	未評価（Not Evaluated） 負値 修復されている（Repaired） 暗号化（Encryption） スキャン不可（Unscanable） 正値	未評価（Not Evaluated） クリーン（Clean） 保留中の FA 不明（Unknown） 省略（Skipped） 悪意のある（Malicious） スキャン不可（Unscanable） 低リスク（Low Risk）	未評価（Not Evaluated） 負値 正値	未評価（Not Evaluated） 一致（Match） 不一致（No Match）	未評価（Not Evaluated） 一致（Match） 不一致（No Match）	未評価（Not Evaluated） トリガーなし（No Trigger） 違反（Violation） 違反なし（No Violation）

メッセージの最後の状態に関する判定によって、アプライアンス内の各エンジンのすべての可能な判定の後にトリガーされる最終判定が決まります。

次に、いくつかの最後の状態の判定を示します。

- 配信済み（Delivered）：メッセージが配信された場合。
- ドロップ済み（Dropped）：メッセージがドロップされた場合。
- 中止（Aborted）：メッセージが中止された場合。（例：メール ポリシー制限により）
- バウンス済み（Bounced）：メッセージがバウンスされた場合。
- 分裂済み（Splintered）：メッセージの MID が複数の最終状態を持つ複数の MID に分割された場合。
- 隔離済み（Quarantined）：メッセージがエンジンによって隔離された場合。
- キュー登録済み（Queued）：メッセージが、エンド受信者、オフボックス スパム隔離や一元化されたポリシー、ウイルスやアウトブレイクの隔離への配信のキューに登録された場合。
- 処理中（Processing）：メッセージがすべてのエンジンによって完全に処理されていない場合。または、メッセージがキュー内で特定のエンジンを待機中の場合。
- 最後の状態が使用不可（Last State Not Available）：メッセージの最後の状態を取得できない場合。（例：メッセージがエンジンによって処理されている場合、まだ最終状態に到達していない場合。）

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）]：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。

[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E 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。

[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 ホスト（Cisco Host）]：メッセージを処理した E メール セキュリティ アプライアンス

[SMTP 認証ユーザ 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「なし（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。

[送信者グループ（Sender Group）]：メッセージを受信した送信者グループ

[メッセージ サイズ（Message Size）]：メッセージのサイズ

[ポリシー一致（受信または送信）（Policy Match (Incoming or Outgoing)）]：メッセージを受信したポリシー

（注） エンジンが詳細を取得できない場合は、値が「N/A」として表示されます。

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「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。

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。

[サマリー（Summary）] タブ

このタブには、メッセージ処理中のすべてのイベントのサマリー ログが表示されます。

[DLPに一致した内容（DLP Matched Content）] タブ

このタブには、データ損失の防止（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無効

化する必要が生じることがあります。「メッセージ トラッキングでの機密情報へのアクセスの制御」を参照してください。

[URL 詳細（URL Details）] タブ

このタブは、URL レピュテーションおよびURL カテゴリ コンテンツ フィルタ、（メッセージ フィルタではなく）アウトブレイク フィルタで検索されたメッセージのみに表示されます。

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

E メール セキュリティ アプライアンスが上記の情報を表示するように設定した場合のみ、このタブを表示できます。『*User Guide for AsyncOS for Cisco Email Security Appliances*』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

[SMTPログ（SMTP Log）] タブ

このセクションでは、電子メールの送信者がSMTP認証に失敗した場合のメッセージのログを表示します。

[AMPログ（AMP Log）] タブ

このセクションには、高度なマルウェア防御ファイル レピュテーションおよびファイル分析サービスで検出されたメッセージのログが表示されます

メッセージ トラッキングのトラブルシューティング

- 予想されるメッセージが検索結果に表示されない （17 ページ）
- 添付ファイルが検索結果に表示されない （18 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

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

- 多くの検索（特にメッセージイベント検索）は、アプライアンスの設定によって結果が異なります。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。

- メッセージ トラッキング データの有効性の検査 （5 ページ）を参照してください。

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

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 ESA で設定され、有効になっています。設定要件（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 （3 ページ））および添付ファイル名検索の制約事項（トラッキング サービスの概要 （1 ページ））を参照してください。