Cisco コンテンツ（M シリーズ）セキュリティ管理アプライアンス の集中型サービス

この章は、次の項で構成されています。

- Cisco コンテンツ セキュリティ管理アプライアンス サービスの概要 （1 ページ）
- ネットワーク プランニング （2 ページ）
- 外部スパム隔離の操作 （2 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離について （6 ページ）
- 中央集中型レポーティングの設定 （12 ページ）
- 中央集中型メッセージ トラッキングの設定 （13 ページ）
- 中央集中型サービスの使用 （14 ページ）

Cisco コンテンツ セキュリティ管理アプライアンス 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（M-Series アプライアンス）は、複数の E メールセキュリティアプライアンス上の特定のサービスに対して一元化されたインターフェイスを提供する外部または「オフボックス」ロケーションです。

シスコのコンテンツセキュリティ管理アプライアンス には次の機能が含まれています。

- 外部スパム隔離。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離。アンチ ウイルス スキャン、アウトブレイク フィルタおよびポリシーにより隔離されたメッセージを保存し管理するために、ファイアウォールの内側の 1 つの場所を提供します。

- 中央集中型レポーティング。複数の E メール セキュリティ アプライアンスからの集計データに関するレポートを実行します。
- 中央集中型トラッキング。複数の E メール セキュリティ アプライアンスを通過する電子メールメッセージを追跡します。

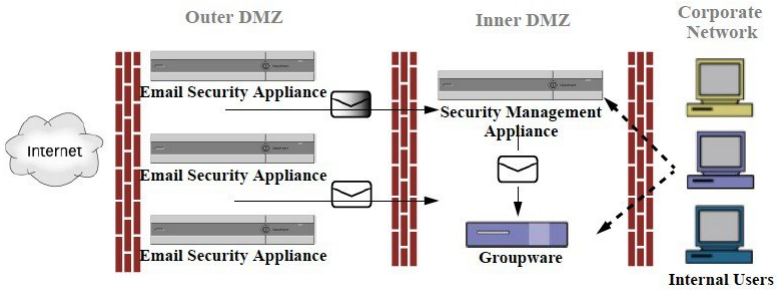
Cisco コンテンツ セキュリティ管理アプライアンスの設定および使用に関する詳細については、『 Cisco Content Security Management appliance User Guide』を参照してください。

ネットワーク プランニング

シスコのコンテンツセキュリティ管理アプライアンス を使用すると、エンドユーザ インターフェイス（メールアプリケーションなど）を、さまざまなDMZ内のよりセキュアなゲートウェイシステムから切り離すことができます。2 層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます。

次の図は、シスコのコンテンツセキュリティ管理アプライアンス と複数の DMZ を組み込んだ一般的なネットワーク設定を示しています。

図 *1:* シスコのコンテンツセキュリティ管理アプライアンス による一般的なネットワーク設定



大規模な企業データセンターは、1 つまたは複数の E メール セキュリティ アプライアンスの外部スパム隔離として機能する 1 つのシスコのコンテンツセキュリティ管理アプライアンスを共有できます。一方、リモートオフィスでは、E メール セキュリティ アプライアンス のローカル使用のためのローカルスパム隔離を維持できます。

外部スパム隔離の操作

- メールフローおよび外部スパム隔離 （3 ページ）
- ローカルのスパム隔離から外部の隔離への移行 （3 ページ）
- 外部スパム隔離と外部セーフリスト/ブロックリストの有効化 （4 ページ）
- ローカルのスパム隔離を無効化して外部隔離をアクティブ化する （5 ページ）
- 外部のスパム隔離のトラブルシューティング （6 ページ）

メールフローおよび外部スパム隔離

ネットワークがネットワーク プランニング （2 ページ） の説明に従って設定される場合、インターネットからの着信メールは外部 DMZ のアプライアンスによって受信されます。正規のメールは、内部 DMZ のメール転送エージェント（MTA）（グループウェア）に従って、最終的に企業ネットワーク内のエンドユーザまで送信されます。

スパムおよび陽性と疑わしいスパム（メールフローポリシー設定値に基づく）は、シスコのコンテンツセキュリティ管理アプライアンス のスパム隔離エリアに送信されます。次にエンドユーザが隔離エリアにアクセスして、スパムを削除し、自分宛に配信されるメッセージを解放することを選択できます。スパム隔離に残っているメッセージは、設定された期間後に自動的に削除されます。

シスコのコンテンツセキュリティ管理アプライアンス で外部隔離からリリースされているメッセージは、配信元の E メール セキュリティ アプライアンス に返されます。これらのメッセージは通常、配信前に、HAT およびその他のポリシーやスキャンの設定、RAT、ドメイン例外、エイリアシング、着信フィルタ、マスカレード、バウンス検証、およびワーク キューの各プロセスを通過しません。

シスコのコンテンツセキュリティ管理アプライアンス にメールを送信するように設定された E メール セキュリティ アプライアンス は、そのシスコのコンテンツセキュリティ管理アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。これを機能させるために、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 IP アドレスが変更されないようにしてください。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 IP アドレスが変わると、受信側の E メール セキュリティ アプライアンス は、メッセージを他の着信メッセージであるものとして処理します。シスコのコンテンツセキュリティ管理アプライアンス の受信と配信では、常に同じ IP アドレスを使用する必要があります。

シスコのコンテンツセキュリティ管理アプライアンス では、スパム隔離設定で指定されている IP アドレスから隔離対象のメールを受け入れます。セキュリティ管理アプライアンスでスパム隔離を設定するには、『Cisco Content Security Management Appliance User Guide』を参照してください。

シスコのコンテンツセキュリティ管理アプライアンスによってリリースされたメールは、スパム隔離設定で定義されたように、プライマリおよびセカンダリホストに配信されます（『Cisco Content Security Management Appliance User Guide』を参照）。したがって、シスコのコンテンツセキュリティ管理アプライアンス にメールを配信する E メール セキュリティ アプライアンス の数に関係なく、リリースされるすべてのメール、通知、およびアラートが単一のホスト（グループウェアまたはコンテンツ セキュリティ アプライアンス）に送信されます。シスコのコンテンツセキュリティ管理アプライアンスからの配信によって、プライマリホストが過負荷にならないように注意してください。

ローカルのスパム隔離から外部の隔離への移行

E メール セキュリティ アプライアンス 上で現在使用中のローカルのスパム隔離を、そのローカル隔離内のメッセージにアクセスできるようにしたまま、シスコのコンテンツセキュリティ

管理アプライアンス でホストされる外部スパム隔離に移行する場合は、移行中に新しいメッセージがローカル隔離に入らないようにする必要があります。

次の戦略の使用を検討します。

- スパム対策の設定：シスコのコンテンツセキュリティ管理アプライアンスを代替ホストとして指定して、メールポリシーにスパム対策を設定します。この処置により、ローカル隔離にアクセス可能なまま、新しいスパムは外部の隔離に送信されます。
- より短い有効期限の設定：ローカル隔離に対して [次の日数の経過後に削除（Schedule Delete After）] 設定をより短い期間に設定します。
- 残っているすべてのメッセージを削除：ローカル隔離内に残っているすべてのメッセージを削除するには、その隔離をディセーブルにし、ローカル隔離のページで [すべて削除（Delete All）] リンクをクリックします（スパム隔離からのメッセージの削除を参照）。このリンクは、まだメッセージが残っているローカルのスパム隔離がディセーブルになっているときにだけ使用可能になります。

これで外部隔離をイネーブルにし、ローカル隔離をディセーブルにする準備ができます。

（注） ローカル隔離と外部隔離の両方がイネーブルの場合、ローカル隔離が使用されます。

外部スパム隔離と外部セーフリスト/ブロックリストの有効化

E メール セキュリティ アプライアンス では、外部スパム隔離を 1 つだけイネーブルにすることができます。

はじめる前に

- メールフローおよび外部スパム隔離 （3 ページ）の情報を確認してください。
- ローカルのスパム隔離から外部の隔離への移行 （3 ページ）の情報を確認してから実行してください。
- 中央集中型スパム隔離およびセーフリスト/ブロックリスト機能をサポートするようにシスコのコンテンツセキュリティ管理アプライアンスを設定します。シスコのコンテンツセキュリティ管理アプライアンス のマニュアルを参照してください。
- これまで、E メール セキュリティ アプライアンスに別の外部スパム隔離を設定していた場合は、まず、その外部スパム隔離設定をディセーブルにする必要があります。

E メール セキュリティ アプライアンス ごとに次の手順を完了します。

手順

ステップ 1 [セキュリティサービス（Security Services）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2 [構成] をクリックします。

ステップ 3 [スパム外部隔離を有効にする（Enable External Spam Quarantine）] を選択します。

ステップ 4 [名前（Name）] フィールドに、シスコのコンテンツセキュリティ管理アプライアンス の名前を入力します。

この名前に意味はありません。参照目的でのみ使用されます。たとえば、シスコのコンテンツセキュリティ管理アプライアンス のホスト名を入力します。

ステップ 5 IP アドレスとポート番号を入力します。

これらは [スパム隔離設定（Spam Quarantines Settings）] ページ（[管理アプライアンス（Management Appliance）] > [集約管理サービス（Centralized Services）] > [スパム隔離（Spam Quarantine）]）でシスコのコンテンツセキュリティ管理アプライアンス に指定した IP アドレスとポート番号に一致する必要があります。

ステップ 6 （任意）**外部のセーフリスト/ブロック リスト**機能をイネーブルにするチェックボックスをオンにして、適切なブロック リスト アクションを指定します。

ステップ 7 変更を送信し、保存します。

ステップ 8 この手順を E メールセキュリティ アプライアンス ごとに繰り返します。

次のタスク

ローカル隔離を使用していた場合は、ローカルのスパム隔離を無効化して外部隔離をアクティブ化する （5 ページ）を参照してください。

関連項目

- ローカルのスパム隔離と外部のスパム隔離
- スパム隔離
- スパムおよびグレイメールの管理
- メッセージがスパムかどうかスキャンするためのアプライアンス の設定方法

ローカルのスパム隔離を無効化して外部隔離をアクティブ化する

外部スパム隔離をイネーブルにする前に、ローカルのスパム隔離を使用していた場合、外部検疫にメッセージを送信するためにはローカル隔離をディセーブルにする必要があります。

はじめる前に

外部スパム隔離と外部セーフリスト/ブロックリストの有効化 （4 ページ）の「はじめる前に」の項の情報を含む、すべての手順に従ってください。

手順

ステップ 1 [モニタ（Monitor）] > [スパム隔離（Spam Quarantine）] を選択します。

ステップ 2 [スパム検疫（Spam Quarantine）] セクションで、[スパム検疫（Spam Quarantine）] リンクをクリックします。

ステップ 3 [スパム隔離を有効にする（Enable Spam Quarantine）] をオフにします。

この変更によって生じたメール ポリシーを調整するための警告は無視します。外部隔離を設定していた場合、メール ポリシーは自動的に外部スパム隔離にメッセージを送信します。

ステップ 4 変更を送信し、保存します。

外部のスパム隔離のトラブルシューティング

電子メール セキュリティ アプライアンスが外部検疫からリリースされたメッセージを再処理する

問題：シスコのコンテンツセキュリティ管理アプライアンス からリリースされたメッセージが、E メール セキュリティ アプライアンス によって不必要に再処理されます。

解決策：これは、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 IP アドレスが変更された場合に発生することがあります。メールフローおよび外部スパム隔離 （3 ページ） を参照してください。

一元化されたポリシー、ウイルス、アウトブレイク隔離について

- 集約されたポリシー、ウイルス、およびアウトブレイク隔離 （6 ページ）
- ポリシー、ウイルス、アウトブレイク隔離の移行について （7 ページ）
- ポリシー、ウイルス、およびアウトブレイク隔離の集約 （8 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について （10 ページ）
- 一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング （11 ページ）

集約されたポリシー、ウイルス、およびアウトブレイク隔離

シスコのコンテンツセキュリティ管理アプライアンス 上でポリシー、ウイルス、およびアウトブレイク隔離を集約できます。メッセージは、E メール セキュリティ アプライアンス によって処理されますが、シスコのコンテンツセキュリティ管理アプライアンス 上の隔離に格納されます。

ポリシー、ウイルス、およびアウトブレイク隔離を一元化する利点としては、次のものがあります。

- 管理者は複数の E メール セキュリティ アプライアンス で隔離されたメッセージを 1 ヵ所で管理できます。
- セキュリティ リスクを減らすため、隔離されたメッセージは DMZ 内ではなくファイアウォールの内側に保管されます。

- 集約された隔離は、シスコのコンテンツセキュリティ管理アプライアンス の標準のバックアップ機能を使用してバックアップできます。

詳細については、お使いのシスコのコンテンツセキュリティ管理アプライアンス のユーザ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。

一元化されたポリシー、ウイルス、アウトブレイク隔離の制限事項

- 各 E メール セキュリティ アプライアンスでは、すべてのポリシー、ウイルス、アウトブレイク隔離を一元化するか、またはすべてローカルに保存する必要があります。
- スキャンエンジンが Cisco コンテンツ セキュリティ管理アプライアンスでは使用できないため、ウイルスについてのポリシー、ウイルス、またはアウトブレイク隔離のテストメッセージを手動でテストできません。

クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件

一元化されたポリシー、ウイルス、およびアウトブレイク隔離を、クラスタ化されたアプライアンスの任意のレベルでイネーブルにできます。

要件：

- E メール セキュリティ アプライアンスの特定のレベル（マシン、グループ、またはクラスタ）で一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにする前に、同じレベルに属するすべてのアプライアンスを最初に Cisco コンテンツ セキュリティ管理アプライアンスに追加する必要があります。
- コンテンツ、メッセージ フィルタおよび DLP メッセージ アクションは同じレベルで設定され、そのレベル以下のすべてのレベルで上書きされない必要があります。
- 一元化されたポリシー、ウイルス、アウトブレイク隔離は同じレベルで設定され、設定したレベル以下のすべてのレベルで上書きされない必要があります。
- Cisco コンテンツ セキュリティ管理アプライアンス との通信に使用するインターフェイスが、グループまたはクラスタ内のすべてのアプライアンスで同じ名前になっていることを確認します。

次に例を示します。

E メール セキュリティ アプライアンスで、クラスタまたはグループレベルで一元化されたポリシー、ウイルス、アウトブレイク隔離をイネーブルにしたい一方で、クラスタに接続されているが設定がマシンレベルで定義されている場合、クラスタまたはグループレベルでこの機能をイネーブルにする前に、マシンレベルでの集中型の隔離設定を削除する必要があります。

ポリシー、ウイルス、アウトブレイク隔離の移行について

ポリシー、ウイルス、アウトブレイク隔離を一元化すると、E メール セキュリティ アプライアンスの既存のポリシー、ウイルス、アウトブレイク隔離は Cisco コンテンツ セキュリティ管理アプライアンスに移行します。

Cisco コンテンツ セキュリティ管理アプライアンスで移行を設定しますが、E メール セキュリティ アプライアンスで一元化されたポリシー、ウイルス、およびアウトブレイク隔離のイネーブル化の変更を確定したときに移行が発生します。

この変更を確定すると、次が発生します。

- E メール セキュリティ アプライアンスのローカルポリシー、ウイルス、アウトブレイク隔離がディセーブルになります。これらの隔離に入る新しいメッセージはすべて、Cisco コンテンツ セキュリティ管理アプライアンスで隔離されます。
- Cisco コンテンツ セキュリティ管理アプライアンスへの既存の非スパム隔離の移行が開始されます。
- すべてのローカルポリシー、ウイルス、アウトブレイク隔離が削除されます。カスタム移行を設定した場合は、移行しないように選択したローカルポリシー隔離もすべて削除されます。ポリシー隔離の削除の影響については、ポリシー隔離の削除についてを参照してください。
- 移行前に複数の隔離に存在したメッセージは、移行後に該当の集中型隔離に存在します。
- 移行はバックグラウンドで実行されます。かかる時間は、隔離エリアのサイズとネットワークによって異なります。E メール セキュリティ アプライアンスで中央集中型の隔離をイネーブルにすると、移行が完了したときに通知を受け取るための 1 つまたは複数の電子メールアドレスを入力できます。
- 送信元ローカル隔離ではなく中央集中型の隔離の設定が、それらのメッセージに適用されます。ただし、元の有効期限は各メッセージに適用されたままです。

（注） 移行時に自動的に作成されるすべての中央集中型の隔離は、デフォルトの隔離設定になります。

ポリシー、ウイルス、およびアウトブレイク隔離の集約

始める前に

（注） メンテナンス ウィンドウからまたはピーク時間帯以外に、この手順を実行してください。

- 最初に Cisco コンテンツ セキュリティ管理アプライアンスに、一元化されたポリシー、ウイルス、アウトブレイク隔離の設定をします。オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の章の「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項にあるテーブル、または Cisco コンテンツ セキュリティ管理アプライアンスのユーザーガイドを参照してください。
- Cisco コンテンツ セキュリティ管理アプライアンスで中央集中型の隔離に割り当てられた容量が既存のローカル隔離が占める総容量よりも小さい場合、メッセージは Cisco コンテンツ セキュリティ管理アプライアンスの隔離の設定に基づいて早期に期限切れとなります。移行の前に、隔離エリアのサイズを減らす手動の操作を行うことを検討してくださ

い。早期の期限切れの詳細については、隔離メッセージに自動的に適用されるデフォルトアクションを参照してください。

- 自動的な移行を選択する場合、または移行中に中央集中型の隔離を作成するためのカスタム移行を設定する場合は、中央集中型の隔離を設定するためのガイドラインとして使用できるよう、現在の E メール セキュリティ アプライアンスの隔離設定を書き留めておくようにしてください。
- E メール セキュリティ アプライアンスをクラスタ コンフィギュレーションで展開している場合は、クラスタ構成の一元化されたポリシー、ウイルス、アウトブレイク隔離の要件（7 ページ）を参照してください。
- この手順で確定した変更は、すぐに発生することに注意してください。ポリシー、ウイルス、アウトブレイク隔離の移行について （7 ページ）を参照してください。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 [有効（Enable）] をクリックします。

ステップ 3 Cisco コンテンツセキュリティ管理アプライアンスとの通信に使用するインターフェイスおよびポートを入力します。

Cisco コンテンツセキュリティ管理アプライアンスからインターフェイスおよびポートに到達可能であることを確認します。

E メール セキュリティ アプライアンスがクラスタ化されている場合、選択したインターフェイスがクラスタ内のすべてのマシンで使用できる必要があります。

ステップ 4 移行が完了したときに通知を受け取るには、1 つまたは複数の電子メールアドレスを入力します。

ステップ 5 想定どおりであるか確認するために、移行された隔離に関する情報を確認します。

ステップ 6 カスタム移行を完了した場合は、この手順で変更を確定した際に削除される隔離に注意してください。

ステップ 7 コンテンツおよびメッセージ フィルタ、およびアップデートするための DLP メッセージ アクションに関する情報が、想定どおりであることを確認します。

（注） クラスタ設定では、フィルタおよびメッセージアクションが特定のレベルで定義され、そのレベル以下のすべてのレベルで上書きされていない場合に限り、メッセージ フィルタ アクションは特定のレベルで自動的にアップデートできます。移行後は、中央集中型の隔離名でフィルタおよびメッセージアクションを手動で再設定する必要があります。

ステップ 8 移行のマッピングを再設定する必要がある場合は、次を実行します。

a) Cisco コンテンツ セキュリティ管理アプライアンスに戻ります。
b) 移行のマッピングを再設定します。

Cisco コンテンツ セキュリティ管理アプライアンス で、再マッピングする隔離を選択し、**[集中型隔離から削除（Remove from Centralized Quarantine）]** をクリックします。その後、隔離を再マッピングできます。

c) Cisco コンテンツ セキュリティ管理アプライアンス で新たに移行の設定を確定します。

d) この手順を最初から繰り返します。

重要[セキュリティ サービス（Security Services）]>[集約管理サービス（Centralized Services）]>[ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] ページを必ずリロードしてください。

ステップ 9 [送信（Submit）] をクリックします。

ステップ 10 移行のマッピングを再設定する必要がある場合は、ステップ 8 の手順に従います。

ステップ 11 変更を保存します。

（注） 移行の進行中は、E メール セキュリティ アプライアンスまたは Cisco コンテンツ セキュリティ管理アプライアンスの構成を変更しないでください。

ステップ 12 ページの上部で移行ステータスを確認します。また、移行を設定するときに電子メールアドレスを入力した場合は、移行の完了を通知する電子メールを待ってください。

次のタスク

オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項目にある表、または Cisco コンテンツ セキュリティ管理アプライアンスのユーザーガイドに記載されているその他の作業を実行します。

関連項目

- ポリシー、ウイルス、およびアウトブレイク隔離にアクセスできるユーザ グループの指定

一元化されたポリシー、ウイルス、アウトブレイク隔離のディセーブル化について

アプライアンスで一元化されたポリシー、ウイルス、アウトブレイク隔離を無効にする場合、次が発生します。

- ローカル隔離は、アプライアンス上で自動的にイネーブルになります。
- システムに作成された隔離、およびメッセージフィルタ、コンテンツフィルタ、DLP メッセージアクションから参照される隔離は、自動的に E メール セキュリティ アプライアンスで作成されます。ウイルス、アウトブレイク、および未分類の隔離は、割り当て済みユーザルールを含め、隔離が一元化される前と同じ設定で作成されます。その他すべての隔離は、デフォルト設定で作成されます。
- 新しく隔離されたメッセージは、すぐにローカル隔離に入ります。
- 中央集中型の隔離エリア内のメッセージは、ディセーブルにされたとき、次のいずれかが発生するまでそのままです。

- 有効期限が切れたとき、メッセージは手動で削除するか自動的に削除されます。
- メッセージは次のいずれかに該当する場合、手動または自動的にリリースされます。

* Cisco コンテンツ セキュリティ管理アプライアンスで代替のリリースのアプライアンスが設定されている。Cisco コンテンツ セキュリティ管理アプライアンスのオンラインヘルプまたはマニュアルを参照してください。

* 中央集中型の隔離がEメール セキュリティ アプライアンス上で再度イネーブルになります。

中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化

始める前に

- 中央集中型のポリシー、ウイルス、アウトブレイク隔離のディセーブル化の影響を理解します。
- 次のいずれかを実行します。
  - 現在中央集中型のポリシー、およびウイルス アウトブレイク隔離内にあるすべてのメッセージを処理します。
  - ディセーブルにした後で、中央集中型の隔離エリアから解放されるメッセージを処理する代替のリリースのアプライアンスが指定されていることを確認します。詳細については、お使いの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オンラインヘルプまたはユーザーガイドを参照してください。

手順

ステップ 1 E メール セキュリティ アプライアンスで、[セキュリティサービス（Security Services）] > [集約管理サービス（Centralized Services）] > [ポリシー、ウイルスおよびアウトブレイク隔離（Policy, Virus, and Outbreak Quarantines）] を選択します。

ステップ 2 一元化されたスパム、ポリシー、ウイルス、およびアウトブレイク隔離をディセーブルにします。

ステップ 3 変更内容を送信し、確定します。

ステップ 4 新しく作成したローカル隔離の設定をカスタマイズします。

一元化されたポリシー、ウイルス、アウトブレイク隔離のトラブルシューティング

Cisco コンテンツ セキュリティ管理アプライアンスが使用できない場合

ポリシー、ウイルス、アウトブレイク隔離が使用できなくなった Cisco コンテンツ セキュリティ管理アプライアンスで一元化されている場合、E メール セキュリティ アプライアンスでこれらの中央集中型の隔離を無効にする必要があります。

交換用 Cisco コンテンツ セキュリティ管理アプライアンスを展開する場合は、Cisco コンテンツ セキュリティ管理アプライアンスと各 E メール セキュリティ アプライアンスで隔離の移行を再設定しなければなりません。オンラインヘルプの「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の章の「集約されたポリシー、ウイルス、およびアウトブレイク隔離」の項にあるテーブル、または Cisco コンテンツ セキュリティ管理アプライアンスのユーザーガイドを参照してください。

中央集中型レポーティングの設定

始める前に

- Cisco コンテンツ セキュリティ管理アプライアンスの中央集中型レポーティングを有効にし、設定します。前提条件と手順について、『Cisco Content Security Management Appliance User Guide』を参照してください。
- Cisco コンテンツ セキュリティ管理アプライアンスでレポーティングサービスに十分なディスク領域が割り当てられていることを確認します。

手順

ステップ 1 [セキュリティ サービス（Security Services）] > [レポート（Reporting）] をクリックします。

ステップ 2 [レポート サービス（Reporting Service）] セクションで [集約管理レポート（Centralized Reporting）] オプションを選択します。

ステップ 3 変更を送信し、保存します。

高度なマルウェア防御レポートの要件

Cisco コンテンツ セキュリティ管理アプライアンス での高度なマルウェア防御（ファイルレピュテーションとファイル分析）機能に関する完全なレポートに必要な設定については、オンラインヘルプの電子メールレポートの章の高度なマルウェア防御レポートについての情報、またはお使いのバージョンの Cisco コンテンツ セキュリティ管理アプライアンス ソフトウェアのユーザーガイドを参照してください。

中央集中型レポーティングに変更後のレポート情報の可用性

E メール セキュリティ アプライアンスで中央集中型レポーティングがイネーブルな場合

- 電子メール セキュリティ アプライアンスにある月次レポート用の既存データは、Cisco コンテンツ セキュリティ管理アプライアンスに転送されません。
- E メール セキュリティ アプライアンスにあるアーカイブレポートは、使用できなくなります。
- E メール セキュリティ アプライアンスは週次データのみ保存します。

- 月次レポートおよび年次レポート用の新規データは、Cisco コンテンツ セキュリティ管理アプライアンスに保存されます。
- E メール セキュリティ アプライアンスでスケジュール設定されたレポートは、停止されます。
- E メール セキュリティ アプライアンス上のスケジュール設定されたレポートの設定ページにはアクセスできなくなります。

中央集中型レポーティングのディセーブル化について

E メール セキュリティ アプライアンスで中央集中型レポーティングをディセーブルにした場合、E メール セキュリティ アプライアンスで新規月次レポートデータの保存が開始され、スケジュールされたレポートが再開し、アーカイブされたレポートにアクセスできます。中央集中型レポーティングをディセーブルにした場合に、E メール セキュリティ アプライアンスでは、過去の時間および日ごとのデータだけが表示され、過去の週ごとや月ごとのデータは表示されません。これは、一時的な変更です。十分なデータが蓄積されれば、過去の週および月のレポートが表示されます。E メール セキュリティ アプライアンスを中央集中型レポーティングモードに戻した場合、過去の週のデータはインタラクティブレポートに表示されます。

中央集中型メッセージ トラッキングの設定

始める前に

（注） E メール セキュリティ アプライアンスで中央集中型トラッキングおよびローカルトラッキングの両方をイネーブルにすることはできません。

手順

ステップ 1 [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）] をクリックします。

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 [設定を編集（Edit Settings）] をクリックします。

ステップ 3 [メッセージ トラッキング サービスを有効にする（Enable Message Tracking Service）] チェックボックスを選択します。

ステップ 4 [集約管理トラッキング（Centralized Tracking）] オプションを選択します。

ステップ 5 （任意）拒否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。

（注） 拒否された接続のトラッキング情報を保存すると、Cisco コンテンツ セキュリティ管理アプライアンスのパフォーマンスに悪影響を与えるおそれがあります。

ステップ 6 変更を送信し、保存します。

次の作業

中央集中型トラッキングを使用するには、E メール セキュリティ アプライアンスと Cisco コンテンツ セキュリティ管理アプライアンスの両方で監視機能をイネーブルにする必要があります。Cisco コンテンツ セキュリティ管理アプライアンスの集中型トラッキングを有効にするには、『 Cisco Content Security Management Appliance User Guide』を参照してください。

中央集中型サービスの使用

中央集中型サービスを使用する手順については、『Cisco Content Security Management Appliance User Guide』を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。