CHAPTER 9

アンチウイルス

IronPort アプライアンスには、Sophos, Plc 製および McAfee, Inc. 製のウイルス スキャン エンジンが統合されています。IronPort アプライアンスのライセンス キーを取得して、これらのウイルス スキャン エンジンのいずれかまたは両方を使用し、メッセージのウイルスをスキャンできます。

（一致する着信または発信メール ポリシーに基づいて）メッセージのウイルスをスキャンし、ウイルスが見つかった場合はメッセージに対してさまざまなアクション（たとえば、ウイルスの発見されたメッセージの「修復」、件名ヘッダーの変更、X-Header の追加、代替アドレスまたはメールホストへのメッセージの送信、メッセージのアーカイブ、またはメッセージの削除など）を実行するようにアプライアンスを設定できます。

ウイルス スキャンをイネーブルにした場合は、アンチスパム スキャンの直後に、アプライアンス上の「ワーク キュー」でウイルス スキャンが実行されます（「電子メール パイプラインの理解」（P.4-91）を参照）。

デフォルトでは、ウイルス スキャンはデフォルトの着信および発信メール ポリシーに対してイネーブルになります。

この章の内容は、次のとおりです。

アンチウイルス スキャン

IronPort アプライアンスは、McAfee または Sophos のアンチウイルス スキャン エンジンを使用してウイルスをスキャンするように設定できます。

McAfee および Sophos のエンジンには、特定のポイントでのファイルのスキャン、ファイルで発見されたデータとウイルス定義のパターン照合と処理、エミュレーション環境でのウイルス コードの復号化および実行、新しいウイルスを認識するための発見的手法の適用、および正規ファイルからの感染コードの削除に必要なプログラム ロジックが含まれています。

評価キー

IronPort アプライアンスには、使用可能な各アンチウイルス スキャン エンジンに対して 30 日間有効な評価キーが同梱されています。評価キーは、System Setup Wizard または [Security Services] > [Sophos] または [McAfee Anti-Virus] ページのライセンス契約書にアクセスするか（GUI）、または `antivirusconfig` または `systemsetup` コマンドを実行して（CLI）イネーブルにします。デフォルトでは、ライセンス契約書に同意すると、アンチウイルス スキャン エンジンはデフォルトの着信および発信メール ポリシーに対してただちにイネーブルになります。30 日間の評価期間後もこの機能をイネーブルにする場合の詳細については、IronPort の営業担当者にお問い合わせください。残りの評価期間は、[System Administration] > [Feature Keys] ページを表示するか、または `featurekey` コマンドを発行することによって確認できます（詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Common Administrative Tasks」にある、機能キーの操作に関する項を参照してください）。

マルチレイヤ アンチウイルス スキャン

AsyncOS は、複数のアンチウイルス スキャン エンジンによるメッセージのスキャン（マルチレイヤ アンチウイルス スキャン）をサポートしています。メール ポリシーごとに、ライセンスを受けたアンチウイルス スキャン エンジンのいずれかまたは両方を使用するように IronPort アプライアンスを設定できます。たとえば、経営幹部用のメール ポリシーを作成し、そのポリシーでは Sophos および McAfee の両方のエンジンを使用してメールをスキャンするように設定することもできます。

複数のスキャン エンジンでメッセージをスキャンすることにより、Sophos および McAfee のアンチウイルス スキャン エンジン双方の利点を組み合わせた「多重防衛」が実現します。各エンジンともに業界をリードするアンチウイルス捕捉率を誇りますが、各エンジンは別々のテクノロジー基盤（「McAfee Anti-Virus フィルタリング」（P.9-309）および「Sophos Anti-Virus フィルタリング」（P.9-305）を参照）に依存してウイルスを検出しているため、マルチスキャン方式を使用することで、より効果が高まります。複数のスキャン エンジンを使用することで、システム スループットが低下する場合があります。詳細は、IronPort のサポート担当者にお問い合わせください。

ウイルス スキャンの順序は設定できません。マルチレイヤ アンチウイルス スキャンをイネーブルにした場合、最初に McAfee エンジンによるウイルス スキャンが実行され、次に Sophos エンジンによるウイルス スキャンが実行されます。McAfee エンジンがメッセージはウイルスに感染していないと判断した場合は、Sophos エンジンはさらにメッセージをスキャンして、別の保護層を追加します。McAfee エンジンがメッセージはウイルスを含んでいると判断した場合は、IronPort アプライアンスは Sophos によるスキャンをスキップし、構成した設定に応じてウイルス メッセージに対してアクションを実行します。

Sophos Anti-Virus フィルタリング

IronPort アプライアンスには、Sophos の総合的なウイルス スキャン テクノロジーが含まれています。Sophos Anti-Virus は、プラットフォーム間のアンチウイルス保護、検出、および除去を提供します。

Sophos Anti-Virus は、ファイルをスキャンしてウイルス、トロイの木馬、およびワームを検出するウイルス検出エンジンを提供します。これらのプログラムは、「悪意のあるソフトウェア」を意味する *マルウェア*と総称されます。アンチウイルス スキャナは、すべてのタイプのマルウェアに共通する相似点を利用して、ウイルスだけでなく、すべてのタイプの悪意のあるソフトウェアを検出および削除します。

ウイルス検出エンジン

Sophos ウイルス検出エンジンは、Sophos Anti-Virus テクノロジーの中心的役割を担います。このエンジンは、Microsoft の Component Object Model（COM; コンポーネント オブジェクト モデル）と同様の、多くのオブジェクトと明確に定義されたインターフェイスで構成された独自のアーキテクチャを使用します。

エンジンで使用されるモジュラ ファイリング システムは、それぞれが異なる「ストレージ クラス」（たとえばファイル タイプなど）を処理する、個別の内蔵型動的ライブラリに基づいています。この方法では、タイプに関係なく汎用のデータ ソースにウイルス スキャン操作を適用できます。

エンジンは、データのロードおよび検索に特化したテクノロジーにより、非常に高速なスキャンを実現できます。次の機能が内蔵されています。

- ポリモーフィック型ウイルスを検出するためのフル コード エミュレータ。
- アーカイブ ファイル内をスキャンするためのオンライン解凍プログラム。
- マクロ ウイルスを検出および駆除するための OLE2 エンジン。

IronPort アプライアンスは、SAV インターフェイスを使用してウイルス エンジンを統合しています。

ウイルス スキャン

大まかにいうと、エンジンのスキャン機能は、検索する場所を特定する分類子と、検索する対象を特定するウイルス データベースという 2 つの重要なコンポーネントの高性能な組み合わせにより管理されています。エンジンは、識別子に依存せずに、タイプでファイルを分類します。

ウイルス エンジンは、システムが受信したメッセージの本文および添付ファイルでウイルスを検索しますが、スキャンの実行方法の決定には、添付ファイルのタイプが役立ちます。たとえば、メッセージの添付ファイルが実行ファイルであれば、エンジンは実行コードの開始場所が記述されているヘッダーを調べて、その場所を検索します。ファイルが Word ドキュメントであれば、エンジンはマクロ ストリームを調べます。MIME ファイル（メール メッセージに使用される形式）であれば、添付ファイルが保存されている場所を調べます。

検出方法

ウイルスの検出方法は、ウイルスのタイプに応じて異なります。スキャン処理中に、エンジンは各ファイルを分析してタイプを特定してから、該当する手法を適用します。すべての方法の根幹には、特定のタイプの命令または特定の命令の順序を検索するという基本概念があります。

パターン照合

パターン照合の手法では、エンジンは特定のコード シーケンスを知っており、そのコード シーケンスと完全一致するコードをウイルスとして特定します。たいていの場合、エンジンは既知のウイルス コードのシーケンスに類似した（必ずしも完全に同一である必要はありません）コードのシーケンスを検索します。スキャン実行中にファイルを比較する対象となる記述を作成する際、Sophos のウイルス研究者達は、エンジンが（次で説明する発見的手法を使用して）オリジナルのウイルスだけでなく、後の派生的なウイルスも発見できるように、識別コードを可能な限り一般的なものに維持することに努めています。

発見的手法

ウイルス エンジンは、基本的なパターン照合手法と発見的手法（特定のルールではなく一般的なルールを使用する手法）を組み合わせることで、Sophos の研究者があるファミリの 1 種類のウイルスしか分析していなかったとしても、そのファミリの複数のウイルスを検出できます。この手法では、記述を 1 つ作成すれば、ウイルスの複数の派生形を捕らえることができます。Sophos は、発見的手法にその他の手法を加味することで、false positive の発生を最低限に抑えています。

エミュレーション

エミュレーションは、ポリモーフィック型ウイルスに対して、ウイルス エンジンによって適用される手法です。ポリモーフィック型ウイルスは、ウイルスを隠す目的のために、ウイルス自体を別の形に変更する暗号化されたウイルスです。明らかな定型的ウイルス コードは存在せず、拡散するたびにウイルス自体が別の形に暗号化されます。このウイルスは、実行されたときに自己復号化します。ウイルス検出エンジンのエミュレータは、DOS または Windows 実行ファイルに使用されますが、ポリモーフィック型マクロは Sophos のウイルス記述言語で記述された検出コードによって発見されます。

この復号化の出力は実際のウイルス コードであり、エミュレータで実行された後に Sophos のウイルス検出エンジンによって検出されるのは、この出力です。

スキャン用にエンジンに送信された実行ファイルは、エミュレータ内で実行されます。エミュレータでは、ウイルス本文の復号化がメモリに書き込まれ、これに応じて復号化が追跡されます。通常、ウイルスの侵入ポイントはファイルのフロントエンドにあり、最初に実行される部分です。ほとんどの場合、ウイルスであ

ることを認識するためには、ウイルス本文のほんのわずかな部分を復号化するだけで十分です。クリーンな実行ファイルの多くは、数個の命令をエミュレートするだけでエミュレーションを停止して、負担を軽減します。

エミュレータは制限された領域で実行されるため、コードがウイルスであるとわかっても、アプライアンスに感染することはありません。

ウイルスの記述

Sophos は、他の信用されているアンチウイルス企業と毎月ウイルスを交換しています。さらに、顧客から毎月数千の疑わしいファイルが直接 Sophos に送られ、そのうち約 30 % はウイルスであると判明しています。各サンプルは、非常にセキュアなウイルス ラボで厳しく分析され、ウイルスかどうか判断されます。Sophos は、新しく発見された各ウイルスまたはウイルスのグループに対して、記述を作成します。

Sophos アラート

IronPort は、Sophos Anti-Virus スキャンをイネーブルにしているお客様に対して、Sophos のサイト（http://www.sophos.com/virusinfo/notifications/）から Sophos アラートを購読することを推奨しています。
購読して Sophos から直接アラートを受け取ることにより、最新のウイルスの発生および利用可能な解決方法が確実に通知されます。

ウイルスが発見された場合

ウイルスが検出されたら、Sophos Anti-Virus はファイルを修復（駆除）できます。通常、Sophos Anti-Virus は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、Email Security 機能（[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ（GUI）または `policyconfig -> antivirus` コマンド（CLI））を使用して受信者ごとに構成できます。これらの設定の構成に

関する詳細については、「ユーザのウイルス スキャン アクションの設定」（P.9-315）を参照してください。

McAfee Anti-Virus フィルタリング

McAfee® スキャン エンジンは、次の処理を行います。

- ファイルのデータとウイルス署名をパターン照合することにより、ファイルをスキャンします。
- エミュレーション環境でウイルス コードを復号化および実行します。
- 発見的手法を適用して新しいウイルスを認識します。
- ファイルから感染性のコードを削除します。

ウイルス署名とのパターン照合

McAfee は、アンチウイルス定義（DAT）ファイルをスキャン エンジンで使用して、特定のウイルス、ウイルスのタイプ、またはその他の潜在的に望ましくないソフトウェアを検出します。また、ファイル内の既知の場所を開始点としてウイルス固有の特徴を検索することにより、単純なウイルスを検出できます。多くの場合、ファイルのほんの一部を検索するだけで、ファイルがウイルスに感染していないと判断できます。

暗号化されたポリモーフィック型ウイルスの検出

複雑なウイルスは、次の 2 つの一般的な手法を使用して、署名スキャンによる検出を回避します。

- **暗号化**。ウイルス内部のデータは、アンチウイルス スキャナがメッセージまたはウイルスのコンピュータ コードを判読できないように、暗号化されます。ウイルスがアクティブになると、ウイルス自体が自発的に実行バージョンに変化し、自己実行します。
- **ポリモーフィック化**。この処理は暗号化に似ていますが、ウイルスが自己複製する際に、その形が変わる点で暗号化とは異なります。

このようなウイルスに対抗するために、エンジンはエミュレーションと呼ばれる手法を使用します。エンジンは、ファイルにこのようなウイルスが含まれていると疑った場合、ウイルスが他に害を及ぼすことなく自己実行して、本来の形が判読できる状態まで自分自身をデコードする人工的な環境を作成します。その後、エンジンは通常どおりウイルス署名をスキャンして、ウイルスを特定します。

発見的分析

新しいウイルスの署名は未知であるため、ウイルス署名を使用するだけでは、新しいウイルスは検出できません。そのため、エンジンは追加で発見的分析という手法を使用します。

ウイルスを運ぶプログラム、ドキュメント、または電子メール メッセージには、多くの場合、特異な特徴があります。これらは、自発的にファイルの変更を試行したり、メール クライアントを起動したり、またはその他の方法を使用して自己複製します。エンジンはプログラム コードを分析して、この種のコンピュータ命令を検出します。また、エンジンは、アクションを実行する前にユーザの入力を求めたりするようなウイルスらしくない正規の動作も検索して、誤ったアラームを発行しないようにしています。

このような手法を使用することで、エンジンは多くの新しいウイルスを検出できます。

ウイルスが発見された場合

ウイルスが検出されたら、McAfee はファイルを修復（駆除）できます。通常、McAfee は、ウイルスが発見されたファイルをすべて修復でき、修復後はそのファイルをリスクなく使用できます。的確なアクションは、ウイルスに応じて異なります。

ファイルの駆除の場合は、必ずしもファイルを元の状態に戻せるとは限らないため、時折、ある程度の制限が生じる場合があります。一部のウイルスは実行プログラムの一部を上書きしてしまうため、元に戻せません。この場合は、修復できない添付ファイルを含むメッセージをどのように処理するかを定義します。これらの設定は、Email Security 機能（[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ（GUI）または `policyconfig -> antivirus` コマンド（CLI））を使用して受信者ごとに構成できます。これらの設定の構成に関する詳細については、「ユーザのウイルス スキャン アクションの設定」（P.9-315）を参照してください。

ウイルス スキャンのイネーブル化およびグローバル設定の構成

ウイルス スキャンを実行するには、最初に IronPort アプライアンスでウイルス スキャンをイネーブルにする必要があります。ウイルス スキャン エンジン（1 つまたは複数）をイネーブルにした後に、ウイルス スキャン エンジンを着信または発信メール ポリシーに適用できます。

概要

ウイルス スキャン エンジンは、System Setup Wizard を実行したときにイネーブルにできます。または、[Security Services] > [Sophos] または [McAfee Anti-Virus] ページ（GUI）または `antivirusconfig` コマンド（CLI）を使用して、ウイルス スキャン エンジンのグローバル コンフィギュレーション設定をイネーブルにしたり、変更したりできます。次のグローバル設定を構成できます。

- システム全体に対してグローバルに McAfee または Sophos Anti-Virus スキャンをイネーブルにする。
- アンチウイルス スキャンのタイムアウト値を指定する。

グローバル設定ページの 2 つの値に加えて、[Service Updates] ページ（[Security Services] タブから使用できます）で、さらにアンチウイルス設定を構成できます。追加の設定には、次のようなものが含まれます。

- システムのアンチウイルス アップデートの取得方法（取得先 URL）。McAfee Anti-Virus エンジンを使用している場合は、ウイルス定義は動的 URL からアップデートされます。厳格なファイアウォール ポリシーを適用している場合は、静的 URL からアップデートを取得するように IronPort アプライアンスを設定する必要がある場合があります。
- システムが新しいウイルス定義をチェックする頻度（チェックの間隔を何分にするか定義します）。
- 任意で、アンチウイルス アップデートを取得するプロキシ サーバをイネーブルにできます。

追加設定の構成に関する詳細については、「システム時刻」（P.15-541）を参照してください。

ウイルス スキャンのイネーブル化およびグローバル設定の構成

アプライアンスでアンチウイルス スキャンをグローバルにイネーブルにするには、「[Edit Global Settings] をクリックします。」（P.9-312）を参照してください。

前もって System Setup Wizard でアンチウイルス エンジンをイネーブルにしていない場合（GUI については「手順 4：[Security]」（P.3-62）、CLI については「アンチウイルス スキャンのイネーブル化」（P.3-85）を参照してください）、アンチウイルス スキャンをイネーブルにするには、次の手順を実行してください。

ステップ 1　[Security Services] > [McAfee] を選択します。

または

[Security Services] > [Sophos] を選択します。

ステップ 2　[Enable] をクリックします。ライセンス契約書ページが表示されます。

（注）　[Enable] をクリックすると、アプライアンスで機能がグローバルにイネーブルになります。ただし、後で [Mail Policies] で受信者ごとの設定をイネーブルにする必要があります。

ステップ 3　ライセンス契約書を読み、ページの最後までスクロールしてから [Accept] をクリックして契約に同意します。図 9-1 とほぼ同じページが表示されます。

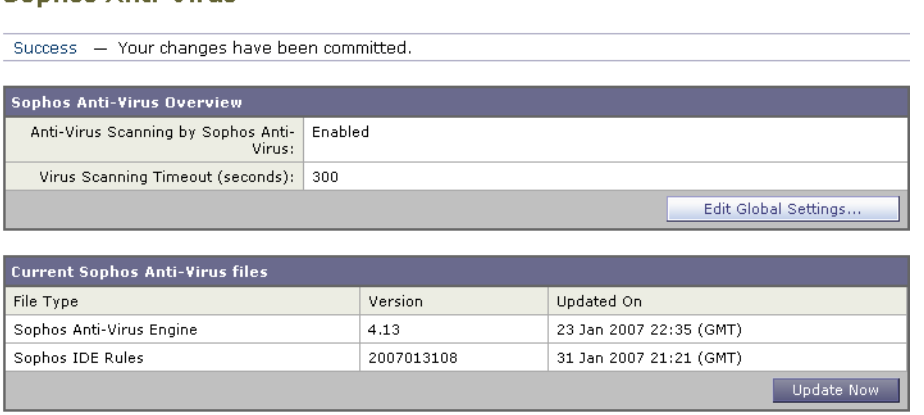
ステップ 4　[Edit Global Settings] をクリックします。

ステップ 5　ウイルス スキャンの最大タイムアウト値を選択します。

システムがメッセージに対するアンチウイルス スキャンの実行を停止する、タイムアウト値を設定します。デフォルト値は 60 秒です。

ステップ 6　[Submit] をクリックします。[Security Services] > [Sophos] または [McAfee Anti-Virus] ページがリフレッシュされて、これまでの手順で選択した値が表示されます。

図 9-1　アップデートされた Sophos Anti-Virus 設定



ステップ 7　[Commit Changes] ボタンをクリックします。

ステップ 8　これで、アンチウイルス設定を受信者ごとに構成できるようになりました。「ユーザのウイルス スキャン アクションの設定」（P.9-315）を参照してください。

（注）　アンチウイルス スキャンの適用方法および適用時期の詳細については、「電子メール パイプラインとセキュリティ サービス」（P.4-99）を参照してください。

HTTP を使用した Anti-Virus アップデートの取得

デフォルトでは、IronPort アプライアンスは、15 分ごとにアップデートをチェックするように設定されています。Sophos エンジンの場合は、サーバはアップデート サイト `http://downloads.ironport.com/av` からアップデートします。McAfee Anti-Virus エンジンの場合は、サーバは動的サイトからアップデートします。

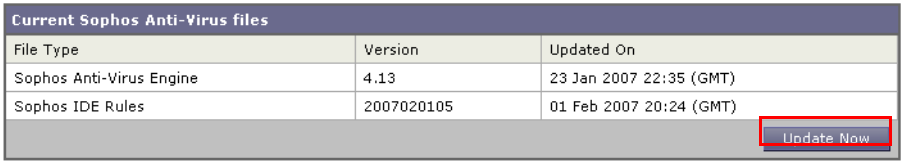
システムがタイムアウトせずに、アップデートが完了するまで待機する最大時間は、アンチウイルス アップデート間隔より 1 分短い値に定義された、動的な値です（[Security Services] > [Service Updates] で定義されています）。この設定値は、接続速度の遅いお客様が、アップデートの完了まで 10 分を超える大きいアップデートをダウンロードする場合に役立ちます。

モニタリングおよび手動でのアップデート チェック

ライセンス契約書に同意し、グローバル設定を構成したら、[Security Services] > [Sophos] または [McAfee Anti-Virus] ページ（GUI）または antivirusstatus コマンド（CLI）を使用して、最新のアンチウイルス エンジンおよび識別ファイルがインストールされていることを確認し、いつ最終のアップデートが実行されたか確認できます。

また、手動でアップデートを確認することもできます。[Security Services] > [Sophos] または [McAfee Anti-Virus] ページの [Current Anti-Virus Files] テーブルで、[Update Now] をクリックします。

図 9-2　Sophos アップデートの手動チェック



CLI では、antivirusstatus コマンドを使用してウイルス ファイルのステータスをチェックし、antivirusupdate コマンドを使用してアップデートを手動でチェックします。

表 9-1　Anti-Virus ステータスの表示

```
example.com> antivirusstatus
Choose the operation you want to perform:
- MCAFEE - Display McAfee Anti-Virus version information
- SOPHOS - Display Sophos Anti-Virus version information
> sophos
SAV Engine Version        4.13
    IDE Serial                2007020302
    Last Engine Update        Tue Jan 23 22:35:16 2007
    Last IDE Update           Sat Feb  3 14:13:49 2007
    Last Update Attempt       Sun Feb  4 00:33:43 2007
    Last Update Success Sat Feb  3 14:13:47 2007
```

表 9-2　新しい Anti-Virus アップデートのチェック

```
example.com> antivirusupdate
Choose the operation you want to perform:
- MCAFEE - Request updates for McAfee Anti-Virus
- SOPHOS - Request updates for Sophos Anti-Virus
>sophos
Requesting check for new Sophos Anti-Virus updates
```

表 9-2　新しい Anti-Virus アップデートのチェック

```
example.com>
```

antivirus ログを使用して、filename.ide に基づいた個別の識別ファイルが、すべて正常にダウンロード、抽出、またはアップデートされたことを確認できます。すべての「AntiVirus」ログ サブスクリプションの最終的なエントリを表示して、ウイルス アップデートが取得できていることを確認するには、tail コマンドを使用します。

ユーザのウイルス スキャン アクションの設定

IronPort アプライアンスに統合されているウイルス スキャン エンジンは、いったんグローバルにイネーブルにすると、[Email Security Manager] 機能を使用して設定したポリシー（設定オプション）に基づいて、着信および発信メール メッセージのウイルスを処理します。アンチウイルス アクションは、[Email Security Feature]（[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ（GUI）または policyconfig -> antivirus コマンド（CLI））を使用して受信者ごとにイネーブルにします。

メッセージ スキャン設定

- [Scan for Viruses Only] :

  システムにより処理されるメッセージには、ウイルス スキャンが実行されます。感染している添付ファイルがあっても、修復は試行*されません*。ウイルスが含まれるメッセージまたは修復できなかったメッセージについて、添付ファイルをドロップしてメールを配信するかどうかを選択できます。

- [Scan and Repair Viruses] :

  システムにより処理されるメッセージには、ウイルス スキャンが実行されます。添付ファイルにウイルスが発見された場合は、システムは添付ファイルの「修復」を試行します。

- [Dropping Attachments] :

  感染した添付ファイルをドロップするように選択できます。

アンチウイルス スキャン エンジンにより、メッセージの添付ファイルがスキャンされ感染したファイルが *ドロップ*されると、代わりに「Removed Attachment」という名前の新しいファイルが添付されます。この添付ファイルのタイプはテキストまたはプレーンで、次の内容が含まれています。

```
This attachment contained a virus and was stripped.

     Filename: filename

 Content-Type: application/filetype
```

悪質な添付ファイルによりメッセージが感染していたため、ユーザのメッセージに何らかの修正が加えられた場合は、必ずユーザに通知されます。二次的な通知アクションを設定することもできます（「通知の送信」（P.9-321）を参照）。感染した添付ファイルをドロップするように選択した場合は、通知アクションにより、ユーザにメッセージが修正されたことを通知する必要は*ありません*。

- [X-IronPort-AV Header]：

  アプライアンスのアンチウイルス スキャン エンジンにより処理されたすべてのメッセージには、`X-IronPort-AV:` というヘッダーが追加されます。このヘッダーは、特に「スキャンできない」と見なされたメッセージについて、アンチウイルス設定に関する問題をデバッグする際の追加情報となります。X-IronPort-AV ヘッダーをスキャンされたメッセージに含めるかどうかは、切り替えできます。このヘッダーを含めることを推奨します。

メッセージ処理設定

ウイルス スキャン エンジンは、リスナーにより受信される 4 つの独立したメッセージ クラスについて、それぞれ別々のアクションを実行して処理するように設定できます。図 9-3 に、ウイルス スキャン エンジンがイネーブルになっている場合にシステムが実行するアクションをまとめています。GUI 設定については、図 9-4 および図 9-5 を参照してください。

次の各メッセージ タイプについて、それぞれ実行するアクションを選択できます。アクションについては後述します（「メッセージ処理アクションの設定の構成」（P.9-318）を参照）。たとえば、ウイルスに感染したメッセージについて、

感染した添付ファイルがドロップされ、電子メールの件名が変更されて、カスタム アラートがメッセージの受信者に送信されるように、アンチウイルスを設定できます。

修復されたメッセージの処理

メッセージが完全にスキャンされ、すべてのウイルスが修復または削除された場合は、そのメッセージは*修復された*と見なされます。これらのメッセージはそのまま配信されます。

暗号化されたメッセージの処理

メッセージ内に暗号化または保護されたフィールドがあるために、エンジンがスキャンを完了できなかった場合は、そのメッセージは*暗号化されている*と見なされます。暗号化されているとマークされたメッセージも、修復可能です。

暗号化検出のメッセージ フィルタ ルール（『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「Encryption Detection Rule」を参照）と、「暗号化された」メッセージに対するウイルス スキャン アクションの違いに注意してください。暗号化メッセージ フィルタ ルールは、PGP または S/MIME で暗号化されたすべてのメッセージを「true」と評価します。暗号化ルールで検出できるのは、PGP および S/MIME で暗号化されたデータのみです。パスワードで保護された ZIP ファイル、もしくは暗号化されたコンテンツを含む Microsoft Word または Excel ドキュメントは検出できません。ウイルス スキャン エンジンは、パスワードで保護されたメッセージまたは添付ファイルはすべて「暗号化されている」と見なします。

（注） AsyncOS バージョン 3.8 以前からアップグレードして、Sophos Anti-Virus スキャンを設定する場合は、アップグレード後に [Encrypted Message Handling] の項を設定する必要があります。

スキャンできないメッセージの処理

スキャン タイムアウト値に到達した場合、または内部エラーによりエンジンが使用不可能になった場合は、メッセージは*スキャンできない*と見なされます。スキャンできないとマークされたメッセージも、修復可能です。

ウイルスに感染したメッセージの処理

システムが添付ファイルをドロップできない、またはメッセージを完全に修復できない場合があります。このような場合は、依然としてウイルスが含まれるメッセージのシステムでの処理方法を設定できます。

暗号化メッセージ、スキャンできないメッセージ、およびウイルス メッセージの設定オプションは、どれも同じです。

メッセージ処理アクションの設定の構成

適用するアクション

暗号化されたメッセージ、スキャンできないメッセージ、またはウイルス陽性のメッセージの各タイプについて、全般的にどのアクションを実行するか（メッセージをドロップする、新しいメッセージの添付ファイルとしてメッセージを配信する、メッセージをそのまま配信する、またはメッセージをアンチウイルス検疫エリアに送信する（「検疫およびアンチウイルス スキャン」（P.9-319）を参照））を選択します。検疫の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。

感染したメッセージを新しいメッセージの添付ファイルとして配信するようにアプライアンスを設定すると、受信者がオリジナルの感染した添付ファイルをどのように処理するか、選択できるようになります。

メッセージをそのまま配信するか、またはメッセージを新しいメッセージの添付ファイルとして配信することを選択した場合は、追加で次の処理を設定できます。

- メッセージの件名の変更
- オリジナルのメッセージのアーカイブ
- 一般的な通知の送信
  次のアクションは、GUI の [Advanced] セクションから実行できます。
- メッセージへのカスタム ヘッダーの追加
- メッセージ受信者の変更
- 代替宛先ホストへのメッセージの送信
- カスタムのアラート通知の送信（受信者宛てのみ）

（注） これらのアクションは、相互に排他的ではありません。ユーザのグループのさまざまな処理ニーズに合わせて、さまざまな着信または発信ポリシーで、これらのアクションを数個またはすべてを、さまざまに組み合わせることができます。これらのオプションを使用した、さまざまなスキャン ポリシーの定義に関する詳細については、後述のセクションおよび「アンチウイルス設定に関する注意事項」（P.9-328）を参照してください。

（注） 修復されたメッセージに対する拡張オプションは、[Add custom header] および [Send custom alert notification] の 2 つのみです。その他すべてのメッセージ タイプについては、すべての拡張オプションにアクセスできます。

検疫およびアンチウイルス スキャン

検疫フラグの付けられたメッセージは、電子メール パイプラインの残りの処理を継続します。メッセージがパイプラインの終点に到達したとき、メッセージに 1 つ以上の検疫フラグが付いていれば、そのメッセージはキューに入ります。メッセージがパイプラインの終点に到達しなかった場合は、そのメッセージは検疫されませんので注意してください。

たとえば、コンテンツ フィルタはメッセージをドロップまたは返送する場合がありますが、その場合、メッセージは検疫されません。

メッセージの件名ヘッダーの変更

特定のテキスト文字列を前後に追加することで、識別されたメッセージを変更すると、ユーザがより簡単に識別されたメッセージを判別したり、ソートしたりできるようになります。

（注） [Modify message subject] フィールドでは、空白は無視*されません*。このフィールドに入力したテキストの後ろまたは前にスペース追加することで、オリジナルのメッセージ件名と、追加テキストを分けることができます（追加テキストをオリジナルの件名の前に追加する場合は追加テキストの前、オリジナルの件名の後ろに追加する場合は追加テキストの後ろにスペースを追加します）。たとえば、`[WARNING: VIRUS REMOVED]` というテキストをオリジナルの件名の前に追加する場合は、この後ろに数個のスペースを追加します。

デフォルトのテキストは次のとおりです。

表 9-3　アンチウイルス件名行変更のデフォルト件名行テキスト

判断	件名に追加されるデフォルトのテキスト
暗号化されている	[WARNING: MESSAGE ENCRYPTED]
感染している	[WARNING: VIRUS DETECTED]
修復されている	[WARNING: VIRUS REMOVED]
スキャン不可	[WARNING: A/V UNSCANNABLE]

複数のステートが該当するメッセージについては、アプライアンスがメッセージに対して実行したアクションをユーザに知らせる、複数部分で構成された通知メッセージが作成されます（たとえば、ユーザに対してはメッセージがウイルスを修復されていると通知されていても、メッセージの他の部分は暗号化されている場合があります）。

オリジナル メッセージのアーカイブ

システムにより、ウイルスが含まれている（または含まれている可能性がある）と判断されたメッセージは、「avarchive」ディレクトリにアーカイブできます。この形式は、mbox 形式のログ ファイルです。「Anti-Virus Archive」ログ サブスクリプションを設定して、ウイルスが含まれているメッセージまたは完全にスキャンできなかったメッセージをアーカイブする*必要があります*。詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Logging」を参照してください。

（注） GUI では、場合により [Advanced] リンクをクリックして [Archive original message] を表示する必要があります。

通知の送信

システムにより、メッセージにウイルスが含まれていると識別されたときに、デフォルトの通知を送信者、受信者、およびその他のユーザまたはそのいずれかに送信できます。その他のユーザを通知対象に指定する場合は、複数のアドレスをコンマで区切ります（CLI および GUI の両方）。デフォルトの通知、メッセージは次のとおりです。

表 9-4　アンチウイルス通知のデフォルト通知

判断	通知
修復されている	The following virus(es) was detected in a mail message: <virus name(s)> Actions taken: Infected attachment dropped.（または Infected attachment repaired.）
暗号化されている	The following message could not be fully scanned by the anti-virus engine due to encryption.
スキャン不可	The following message could not be fully scanned by the anti-virus engine.
感染している	The following unrepairable virus(es) was detected in a mail message: <virus name(s)>.

メッセージへのカスタム ヘッダーの追加

アンチウイルス スキャン エンジンによってスキャンされたすべてのメッセージに追加する、追加のカスタム ヘッダーを定義できます。[Yes] をクリックし、ヘッダー名およびテキストを定義します。

また、`skip-viruscheck` アクションを使用するフィルタを作成して、特定のメッセージはウイルス スキャンを回避するようにもできます。詳細については、『*Cisco IronPort AsyncOS for Email Advanced Configuration Guide*』の「Using Message Filters to Enforce Email Policies」の章の「Bypass Anti-Virus System Action」を参照してください。

メッセージ受信者の変更

メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようにできます。[Yes] をクリックして、新しい受信者のアドレスを入力します。

代替宛先ホストへのメッセージの送信

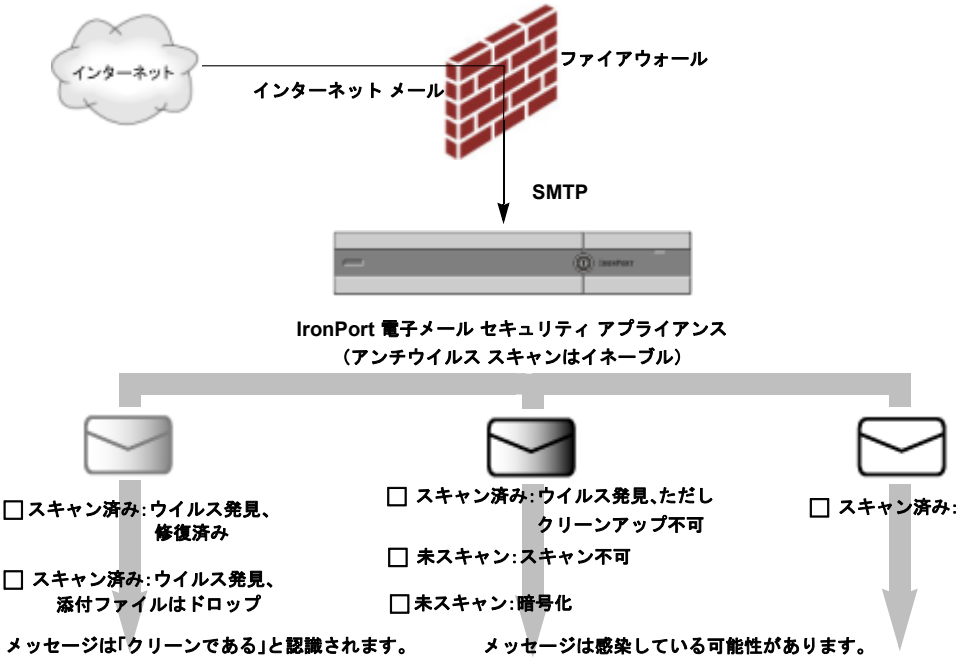
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[Yes] をクリックして代替アドレスまたはホストを入力します。

たとえば、疑わしいメッセージを管理者のメールボックスまたは専用のメールサーバに送信して、後で調査することができます。受信者が複数のメッセージの場合は、代替受信者に送信されるコピーは 1 つのみです。

カスタムのアラート通知の送信（受信者宛てのみ）

受信者にカスタム通知を送信できます。そのためには、この設定を構成する前に、まずカスタム通知を作成する必要があります。詳細については、「テキストリソース」（P.14-446）を参照してください。

図 9-3　ウイルス スキャンを実行したメッセージの処理に関するオプション



（注）　デフォルトでは、アンチウイルス スキャンは、WHITELIST 送信者グループが参照するパブリック リスナーの $TRUSTED メール フロー ポリシーでイネーブルになっています。「メール フロー ポリシー：アクセス ルールとパラメータ」（P.5-117）を参照してください。

メール ポリシーのアンチウイルス設定の編集

メール ポリシーのユーザごとのアンチウイルス設定を編集する処理は、着信メールと発信メールで基本的に同じです。

個々のポリシー（デフォルト以外）には、[Use Default] 設定値という追加のフィールドがあります。この設定は、デフォルトのメール ポリシー設定を継承するように選択します。

アンチウイルス アクションは、[Email Security Feature]（[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページ（GUI）または `policyconfig -> antivirus` コマンド（CLI））を使用して受信者ごとにイネーブルにします。アンチウイルス設定をグローバルにイネーブルにした後は、作成した各メール ポリシーに対して、これらのアクションを別々に設定します。さまざまなメール ポリシーに対して、異なるアクションを設定できます。

デフォルトのポリシーも含め、メール ポリシーのアンチウイルス設定を編集するには、次の操作を実行します。

ステップ 1　[Email Security Manager] の着信または発信メール ポリシー テーブルの任意の行で、アンチウイルス セキュリティ サービスへのリンクをクリックします。

図 9-4 および図 9-5 に示されている画面のような [Anti-Virus settings] ページが表示されます。

デフォルト ポリシーの設定を編集するには、デフォルト行のリンクをクリックします。図 9-4 および図 9-5 に、個別のポリシー（デフォルト以外）の設定を示します。

ステップ 2　[Yes] または [Use Default] をクリックして、そのポリシーのアンチウイルス スキャンをイネーブルにします。

このページの最初の設定値は、そのポリシーに対してサービスがイネーブルであるかどうかを定義します。[Disable] をクリックしてすべてのサービスをディセーブルにできます。

デフォルト以外のメール ポリシーでは、[Yes] を選択することで、[Repaired Messages]、[Encrypted Messages]、[Unscannable Messages]、および [Virus Infected Messages] 領域内の各フィールドがイネーブルになります。

ステップ 3　アンチウイルス スキャン エンジンを選択します。McAfee または Sophos のエンジンを選択できます。

ステップ 4　[Message Scanning] 設定を構成します。

詳細については、「メッセージ スキャン設定」（P.9-315）を参照してください。

ステップ 5　[Repaired Messages]、[Encrypted Messages]、[Unscannable Messages]、および [Virus Infected Messages] の設定を構成します。

図 9-4 および図 9-5 に、「Engineering」という名前のこれから編集するメール ポリシーのアンチウイルス設定を示します。「メッセージ処理設定」（P.9-316）および「メッセージ処理アクションの設定の構成」（P.9-318）を参照してください。

ステップ 6　[Submit] をクリックします。

[Mail Policies] > [Incoming Mail Policies] または [Outgoing Mail Policies] ページがリフレッシュされて、これまでの手順で選択した値が反映されます。

ステップ 7　変更を確定します。

図 9-4　メール ポリシーのアンチウイルス設定（デフォルト以外）：1/2

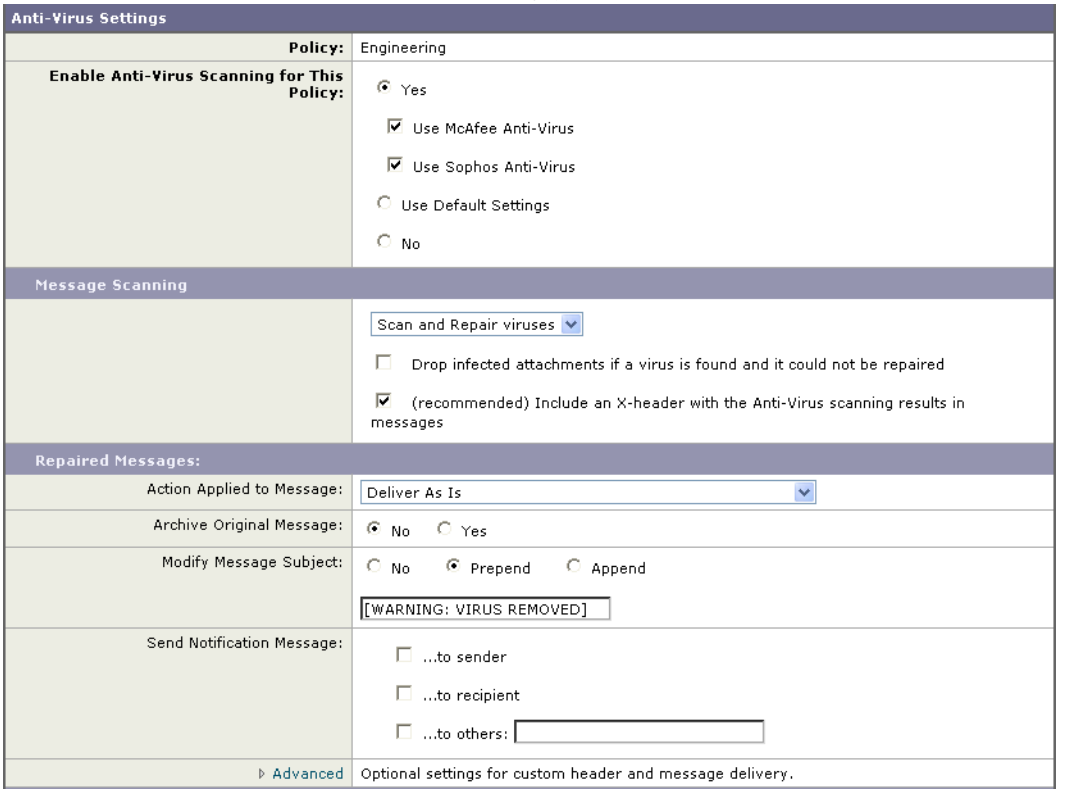
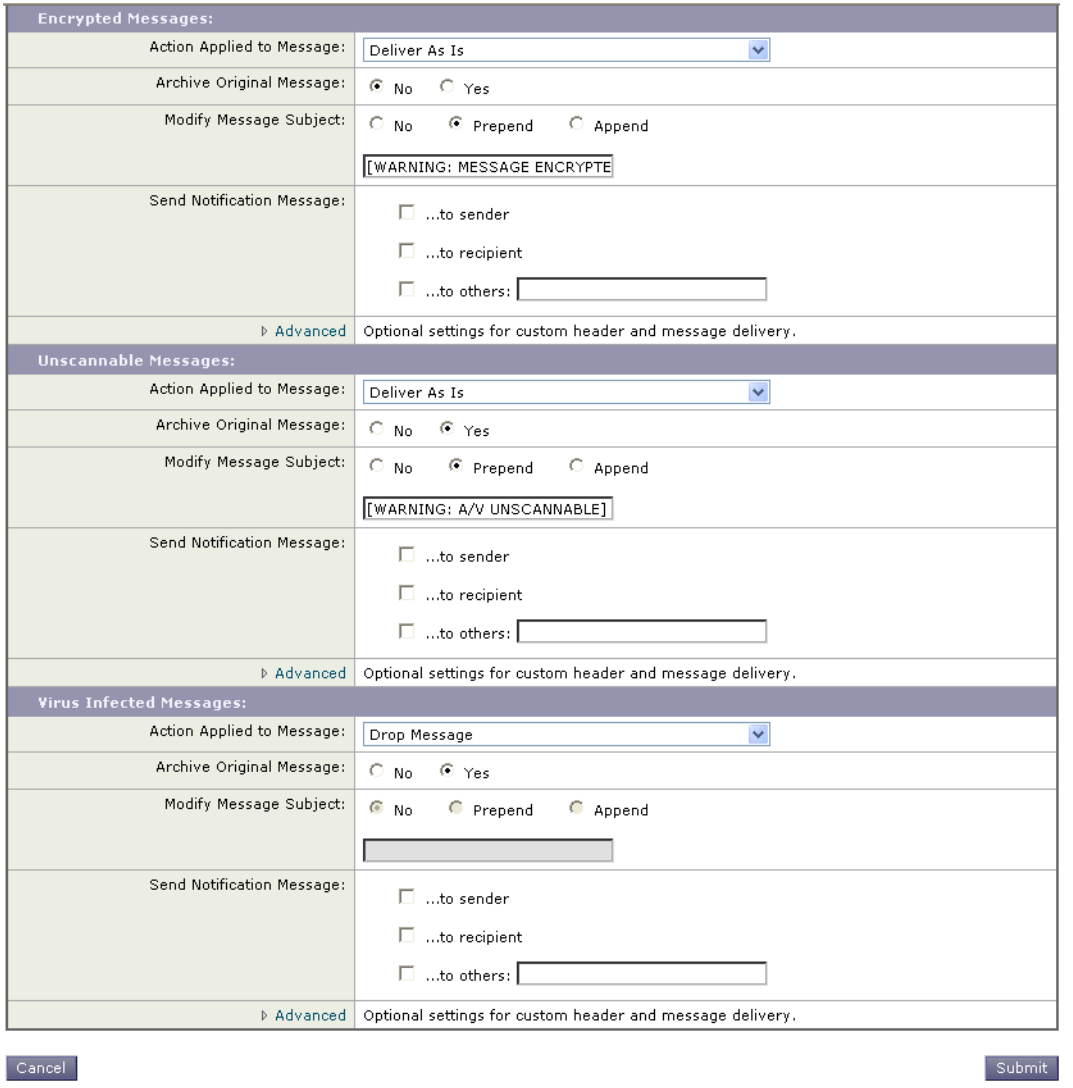


図 9-5　メール ポリシーのアンチウイルス設定（デフォルト以外）：2/2



アンチウイルス設定に関する注意事項

添付ファイルのドロップ フラグにより、アンチウイルス スキャンの動作は大きく異なります。システムが、[Drop infected attachments if a virus is found and it could not be repaired] ように設定されている場合は、ウイルス性またはスキャンできない MIME 部分はすべてメッセージから削除されます。そのため、アンチウイルス スキャンの出力は、ほとんど常に*クリーンな*メッセージになります。GUI ペインに表示された [Unscannable Messages] で定義されるアクションは、実行されることはほとんどありません。

[Scan for Viruses only] 環境では、これらのアクションは悪質なメッセージ部分をドロップすることで、メッセージを「クリーンに」します。RFC822 ヘッダーに限り、RFC822 ヘッダー自体が攻撃された、またはその他の問題に遭遇した場合は、スキャンできなかった場合のアクションが実行されます。ただし、アンチウイルス スキャンが [Scan for Viruses only] に設定されていながら、[Drop infected attachments if a virus is found and it could not be repaired] が選択されて*いない*場合は、スキャンできなかった場合のアクションが実行される可能性は非常に高くなります。

表 9-5 に、一般的なアンチウイルス設定オプションを示します。

表 9-5　一般的なアンチウイルス設定オプションの表示

状況	アンチウイルス設定
ウイルスが広範囲に発生 **ウイルス性のメッセージは単純にシステムからドロップされ、他の処理が実行されることはほとんどありません。**	**添付ファイルのドロップ**：しない。 **スキャン**：Scan-Only。 **クリーンアップされたメッセージ**：配信する。 **スキャンできないメッセージ**：メッセージをドロップする。 **暗号化されたメッセージ**：管理者に送るか検疫して、後で確認する。 **ウイルス性のメッセージ**：メッセージをドロップする。

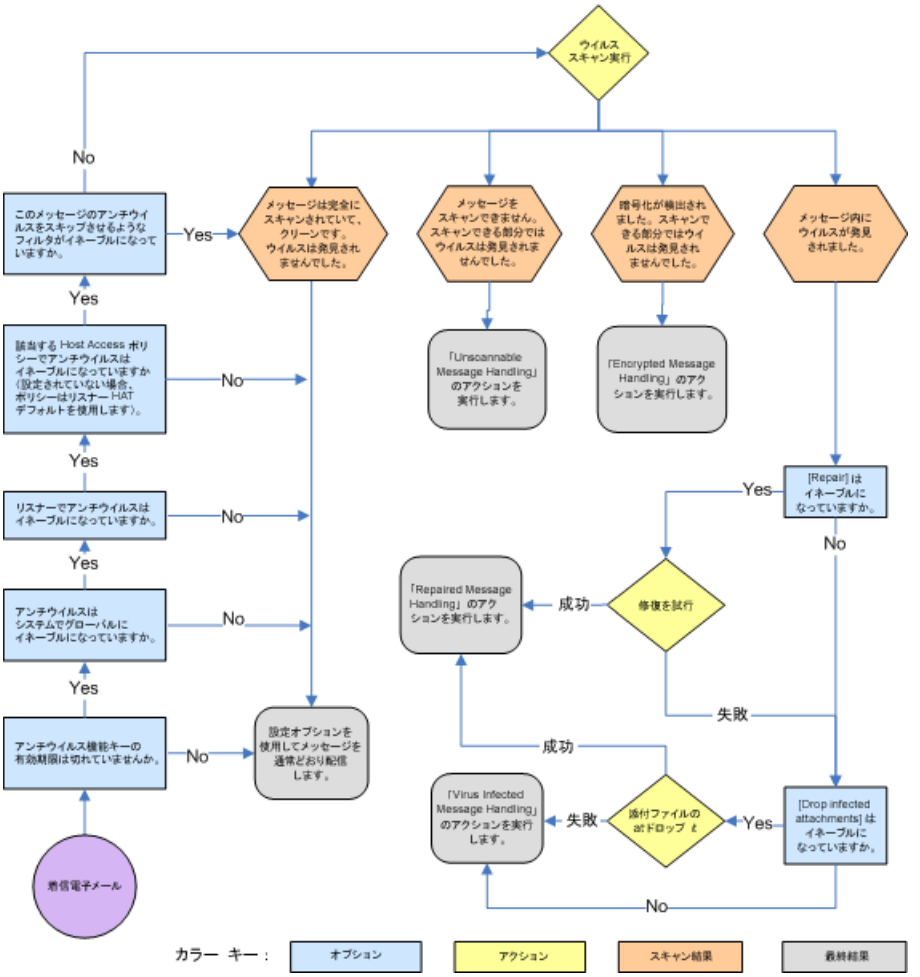
表 9-5　一般的なアンチウイルス設定オプションの表示（続き）

リベラルなポリシー **できる限り多くのドキュメントを送信します。**	**添付ファイルのドロップ**：する。 **スキャン**：Scan and Repair。 **クリーンアップされたメッセージ**: [VIRUS REMOVED] として配信する。 **スキャンできないメッセージ**：添付ファイルとして転送する。 **暗号化されたメッセージ**：マークして転送する。 **ウイルス性のメッセージ**：検疫するか、マークして転送する。
より保守的なポリシー	**添付ファイルのドロップ**：する。 **スキャン**：Scan and Repair。 **クリーンアップされたメッセージ**: [VIRUS REMOVED] として配信する (より慎重なポリシーでは、クリーンアップしたメッセージをアーカイブします)。 **スキャンできないメッセージ**：通知を送る、検疫する、またはドロップしてアーカイブする。 **暗号化されたメッセージ**：マークして転送する、またはスキャンできないメッセージとして処理する。 **ウイルス性のメッセージ**：アーカイブしてドロップする。
保守的なポリシーでレビューを実施する **ウイルス メッセージの可能性があるものは、後で管理者が内容を確認できるように、検疫メールボックスに送信されます。**	**添付ファイルのドロップ**：しない。 **スキャン**：Scan-Only。 **クリーンアップされたメッセージ**：配信する（通常、このアクションは実行されません)。 **スキャンできないメッセージ**：添付ファイル、`alt-src-host`、または `alt-rcpt-to` アクションとして転送する。 **暗号化されたメッセージ**：スキャンできないメッセージとして処理する。 **ウイルス性のメッセージ：**検疫するか管理者に転送する。

アンチウイルス アクションのフロー ダイアグラム

図 9-6（P.9-330）に、アンチウイルス アクションおよびオプションが、アプライアンスで処理されるメッセージにどのように影響を及ぼすかを示します。

図 9-6　アンチウイルス アクションのフロー ダイアグラム



（注） マルチレイヤ アンチウイルス スキャンを設定した場合は、IronPort アプライアンスは最初に McAfee エンジンでウイルス スキャンを実行し、次に Sophos エンジンでウイルス スキャンを実行します。アプライアンスは、McAfee エンジンがウイルスを検出しない限りは、両方のエンジンを使用してメッセージをスキャンします。McAfee エンジンがウイルスを検出した場合は、IronPort アプライアンスは、メール ポリシーで定義されたアンチウイルス アクション（修復、検疫など）を実行します。

ウイルス スキャンのテスト

アプライアンスのウイルス スキャン設定をテストするには、次の操作を実行します。

ステップ 1　メール ポリシーのウイルス スキャンをイネーブルにします。

[Security Services] > [Sophos] または [McAfee Anti-Virus] ページ、または `antivirusconfig` コマンドを使用してグローバル設定を行ってから、[Email Security Manager] ページ（GUI）または `policyconfig` の `antivirus` サブコマンドを使用して、特定のメール ポリシーの設定を構成します。

ステップ 2　標準のテキスト エディタを開き、次の文字列を *スペースまたは改行を使用せず、1 行で*入力します。

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

（注） 上記の行は、テキスト エディタ ウィンドウで 1 行で表示される必要があります。そのため、必ずテキスト エディタのウィンドウは最大にして、改行はすべて削除します。また、テスト メッセージ開始部の「X5O...」には、数字の「0」ではなく必ず文字の「O」を入力します。

このマニュアルをコンピュータでお読みの場合は、PDF ファイルまたは HTML ファイルから直接この行をコピーして、テキスト エディタに貼ることができます。この行をコピーする場合は、必ずすべての余分な復帰文字またはスペースを削除します。

ステップ 3　ファイルを **EICAR.COM** という名前で保存します。

ファイルのサイズは 68 ～ 70 バイトになります。

（注）　このファイルはウイルスでは*ありません*。拡散したり、他のファイルに感染したり、またはコンピュータに害を与えたりするものではありません。ただし、他のユーザにアラームを与えないために、テストを終了したらこのファイルは削除してください。

ステップ 4　ファイル EICAR.COM を電子メール メッセージに添付して、手順 1 で設定したメール ポリシーに一致するリスナーに送信します。

テスト メッセージで指定した受信者が、リスナーで許可されることを確認します（詳細は、「パブリック リスナー（RAT）上でのローカル ドメインまたは特定のユーザの電子メールの受け入れ」（P.5-177）を参照してください）。

IronPort 以外のゲートウェイ（たとえば Microsoft Exchange サーバ）で発信メールに対するウイルス スキャン ソフトウェアをインストールしている場合は、ファイルを電子メールで送信することが難しいことがあるため、注意してください。

（注）　テスト ファイルは、常に修復不可能としてスキャンされます。

ステップ 5　リスナー上のウイルス スキャンに設定したアクションを評価して、そのアクションがイネーブルであり、予想どおりに動作していることを確認します。

これは、次のいずれかのアクションを実行することで、最も簡単に達成できます。

- ウイルス スキャンを、[Scan and Repair] モードまたは [Scan Only] モードにして、添付ファイルをドロップしないように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[Virus Infected Messages] の処理で設定した内容（「ウイルスに感染したメッセージの処理」（P.9-318）の設定）と一致していることを確認します。

– ウイルス スキャンを、[Scan and Repair] モードまたは [Scan Only] モードにして、添付ファイルをドロップするように設定します。

EICAR テスト ファイルを添付ファイルとした電子メールを送信します。

実行されたアクションが、[Repaired Messages] の処理で設定した内容（「修復されたメッセージの処理」（P.9-317）の設定）と一致していることを確認します。

アンチウイルス スキャンのテスト用ウイルス ファイルの取得に関する詳細については、次の URL を参照してください。

`http://www.eicar.org/anti_virus_test_file.htm`

このページでは、ダウンロード可能な 4 つのファイルを提供しています。クライアント側にウイルス スキャン ソフトウェアをインストールしている場合は、これらのファイルをダウンロードして抽出するのは難しいため、注意してください。