アンチウイルス

この章は、次の項で構成されています。

- アンチウイルス スキャンの概要, on page 1
- Sophos アンチウイルス フィルタリング, on page 3
- McAfee アンチウイルス フィルタリング, on page 6
- 電子メールゲートウェイでのウイルスのスキャンの設定方法 , on page 7
- アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信 , on page 19
- ウイルス定義ファイルの更新, on page 21

アンチウイルス スキャンの概要

電子メールゲートウェイには、サードパーティの企業の Sophos および McAfee の統合されたウイルススキャンエンジンが含まれます。電子メールゲートウェイ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てメッセージのウイルスをスキャンし、どちらかのアンチウイルス 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電子メールゲートウェイを設定できます。

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。

（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）を実行するように電子メールゲートウェイを設定できます。

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、電子メールゲートウェイ上の「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 パイプラインとセキュリティ サービス 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。

関連項目

- 評価キー, on page 2
- 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, on page 2

評価キー

電子メールゲートウェイには、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、システム セットアップ ウィザードまたは [セキュリティサービス（Security Services）] > [Sophos] または [McAfee ウイルス対策（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）有効にします。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有効にする場合の詳細については、Cisco 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、[システム管理（System Administration）] > [ライセンスキー（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、ライセンス キーを参照してください。）

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

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電子メールゲートウェイを設定できます。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 アンチウイルス フィルタリング, on page 6およびSophos アンチウイルス フィルタリング, on page 3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、シスコ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、電子メールゲートウェイは 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 アンチウイルス フィルタリング

電子メールゲートウェイには、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。ウイルス対策スキャナは、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。

関連項目

- ウイルス検出エンジン, on page 3
- ウイルス スキャン, on page 4
- 検出方法, on page 4
- ウイルスの記述, on page 5
- Sophos アラート , on page 5
- ウイルスが発見された場合, on page 5

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。

電子メールゲートウェイは、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。

関連項目

- パターン照合, on page 4
- 発見的手法, on page 4
- エミュレーション, on page 5

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がメモリに書き込まれ、これに応じて復号が追跡されます。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、電子メールゲートウェイ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

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、E メール セキュリティ機能（[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（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, on page 9を参照してください。

McAfee アンチウイルス フィルタリング

McAfee®スキャン エンジン:

- ファイルのデータとウイルス シグニチャ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。

関連項目

- ウイルス シグニチャとのパターン照合, on page 6
- 暗号化されたポリモーフィック型ウイルスの検出, on page 6
- 発見的分析, on page 7
- ウイルスが発見された場合, on page 5

ウイルス シグニチャとのパターン照合

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、シグニチャ 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 シグニチャをスキャンして、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 シグニチャ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、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、E メール セキュリティ機能（[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（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, on page 9を参照してください。

電子メールゲートウェイでのウイルスのスキャンの設定方法

メッセージのウイルスのスキャン方法

	操作手順	詳細
ステップ 1	電子メールゲートウェイでアンチウイルススキャンをイネーブルにします。	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 , on page 8

	操作手順	詳細
ステップ 2	メッセージのウイルスをスキャンするユーザ グループを定義します。	送信者および受信者のグループのメール ポリシーの作成
ステップ 3	（オプション）ウイルス隔離でのメッセージの処理方法を設定します。	ポリシー、ウイルス、およびアウトブレイク隔離の設定
ステップ 4	電子メールゲートウェイでのウイルスに感染したメッセージの処理方法を決定します。	ユーザのウイルス スキャン アクションの設定, on page 9
ステップ 5	定義したユーザ グループに対するアンチウイルス スキャンのルールを設定します。	送信者および受信者のグループごとのアンチウイルス ポリシーの設定, on page 15
ステップ 6	（オプション）設定をテストするために電子メール メッセージを送信します。	アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信 , on page 19

関連項目

- 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 , on page 8
- ユーザのウイルス スキャン アクションの設定, on page 9
- 送信者および受信者のグループごとのアンチウイルス ポリシーの設定, on page 15
- ウイルス対策設定に関する注意事項, on page 17
- アンチウイルス アクションのフロー ダイアグラム, on page 18

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 エンジンは、システム セットアップ ウィザードを実行したときにイネーブルになった可能性があります。これにかかわらず、次の手順で設定をします。

Note ライセンス キーによって、Sophos、McAfee、またはその両方をイネーブルにできます。

Procedure

ステップ 1 [セキュリティサービス（Security Services）] > [McAfee] ページに移動します。

または

[セキュリティサービス（Security Services）] > [Sophos] ページに移動します。

ステップ 2 [有効（Enable）] をクリックします。

Note
[有効（Enable）] をクリックすると、電子メールゲートウェイ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 [メールポリシー（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 [承認（Accept）] をクリックして契約に同意します。

ステップ 4 [グローバル設定を編集（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 （オプション）[自動アップデートを有効にする（Enable Automatic Updates）] をクリックして、エンジンの自動アップデートを有効にします。

電子メールゲートウェイは、アップデートサーバから特定のエンジンに必要なアップデートを取得します。

ステップ 7 変更を送信し、保存します。

What to do next

アンチウイルス設定を受信者ごとに設定します。ユーザのウイルス スキャン アクションの設定, on page 9 を参照してください。

ユーザのウイルス スキャン アクションの設定

電子メールゲートウェイに統合されているウイルススキャンエンジンは、[電子メールセキュリティマネージャ（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、[メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（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。

関連項目

- メッセージ スキャン設定, on page 9
- メッセージ処理設定, on page 10
- メッセージ処理アクションの設定の構成, on page 11

メッセージ スキャン設定

- [ウイルス スキャンのみ（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。

- [ウイルスをスキャンして修復（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。

- [添付ファイルをドロップ（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, on page 14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ヘッダー（X-IronPort-AV Header）]：

  電子メールゲートウェイのアンチウイルス 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：ウイルスをスキャンするメッセージを処理するオプション」は、ウイルス スキャン エンジンが有効なときに、システムが実行するアクションの概要を示します。

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, on page 11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、ウイルス対策を設定できます。

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（暗号化検出ルールを参照）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。

Note 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「暗号化されたメッセージの処理」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, on page 12
- 隔離およびウイルス対策スキャン, on page 12
- メッセージの件名ヘッダーの変更, on page 13
- オリジナル メッセージのアーカイブ, on page 13
- 通知の送信, on page 14
- メッセージへのカスタム ヘッダーの追加, on page 14

- メッセージ受信者の変更, on page 14
- 代替送信ホストにメッセージを送る, on page 14
- カスタム アラート通知の送信, on page 15

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隔離エリアに送信する（隔離およびウイルス対策スキャン, on page 12を参照））を選択します。

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電子メールゲートウェイを設定すると、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 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 [詳細（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 アラート通知の送信

Note 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ウイルス対策設定に関する注意事項, on page 17を参照してください。

修復されたメッセージに対する拡張オプションは、[カスタムヘッダーを追加（Add custom header）] および [カスタムアラート通知を送信（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。

隔離およびウイルス対策スキャン

隔離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末尾に到達すると、メッセージに 1 つ以上の隔離に関するフラグが設定されていれば、該当するキューに入ります。メッセージがパイプラインの末尾に到達しなければ、隔離エリアには配置されません。

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、メッセージは隔離されません。

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、ログを参照してください。

Note GUI では、場合により [詳細（Advanced）] リンクをクリックして [オリジナルのメッセージをアーカイブ（Archive original message）] を表示する必要があります。

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。

Note [メッセージの件名を修正（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。

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

判定	件名に追加されるデフォルトのテキスト
暗号化	`[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（Unscannable）	`[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、電子メールゲートウェイ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）。

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。

アンチウイルス通知のデフォルト通知

判定	通知
修復されている	次のウイルスがメールメッセージで検出されました: <ウイルス名>（The following virus(es) was detected in a mail message: <virus name(s)>） 実行するアクション:感染している添付ファイルがドロップされました（または感染している添付ファイルが修復されました）。（Actions taken: Infected attachment dropped (or Infected attachment repaired).）
暗号化	暗号化されているため、次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine due to encryption.）
スキャン不可	次のメッセージをウイルス対策エンジンによって完全にスキャンできませんでした。（The following message could not be fully scanned by the anti-virus engine.）
感染している	次の修復不可能なウイルスがメールメッセージで検出されました:<ウイルス名>。（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。[はい（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。アンチウイルス システムのバイパス アクション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。[はい（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。

代替送信ホストにメッセージを送る

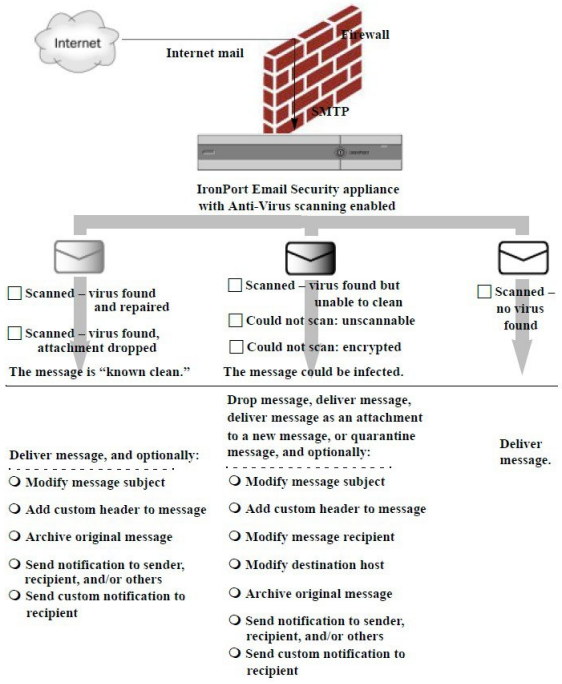
暗号化されたメッセージ、スキャンできないメッセージ、またはウイルスに感染したメッセージについて、異なる受信者または宛先ホストに通知を送信するように選択できます。[はい（Yes）] をクリックして代替アドレスまたはホストを入力します。

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 アラート通知の送信

送信者、受信者、およびその他のユーザ（メールアドレス）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 リソースについてを参照してください。

Figure 1: 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



Note デフォルトでは、アンチウイルススキャンは、ALLOWED_LIST 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有効になっています。メール フローポリシーを使用した電子メール送信者のアクセス ルールの定義 を参照してください。

送信者および受信者のグループごとのアンチウイルスポリシーの設定

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、[デフォルトを使用（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、[受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] を使用して受信者ごとにイネーブルにします。GUI または CLI の policyconfig > antivirus コマンドを使用してメール ポリシーを設定できます。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。

Procedure

ステップ 1 [メールポリシー（Mail Policies）] > [受信メールポリシー（Incoming Mail Policies）] または [送信メールポリシー（Outgoing Mail Policies）] ページに移動します。

ステップ 2 ポリシーを設定するアンチウイルス セキュリティ サービスのリンクをクリックします。

Note
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。

ステップ 3 [はい（Yes）] または [デフォルトを使用（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。[無効（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、[はい（Yes）] を選択することで、[修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（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 4 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 5 [メッセージのスキャン（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, on page 9を参照してください。

ステップ 6 [修復されたメッセージ（Repaired Messages）]、[暗号化されたメッセージ（Encrypted Messages）]、[スキャン不能なメッセージ（Unscannable Messages）]、および [ウイルス感染したメッセージ（Virus Infected Messages）] の設定を構成します。

メッセージ処理設定, on page 10およびメッセージ処理アクションの設定の構成, on page 11を参照してください。

ステップ 7 [送信（Submit）] をクリックします。

ステップ 8 変更を保存します。

ウイルス対策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、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする（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 [スキャン不能なメッセージ（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。

[ウイルスのみスキャン（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 [ウイルスのみスキャン（Scan for Viruses only）] に設定されていながら、[ウイルスが検出され修復できない場合、感染した添付ファイルをドロップする（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。

次の表に、一般的なアンチウイルス設定オプションを示します。

一般的なアンチウイルス設定オプション

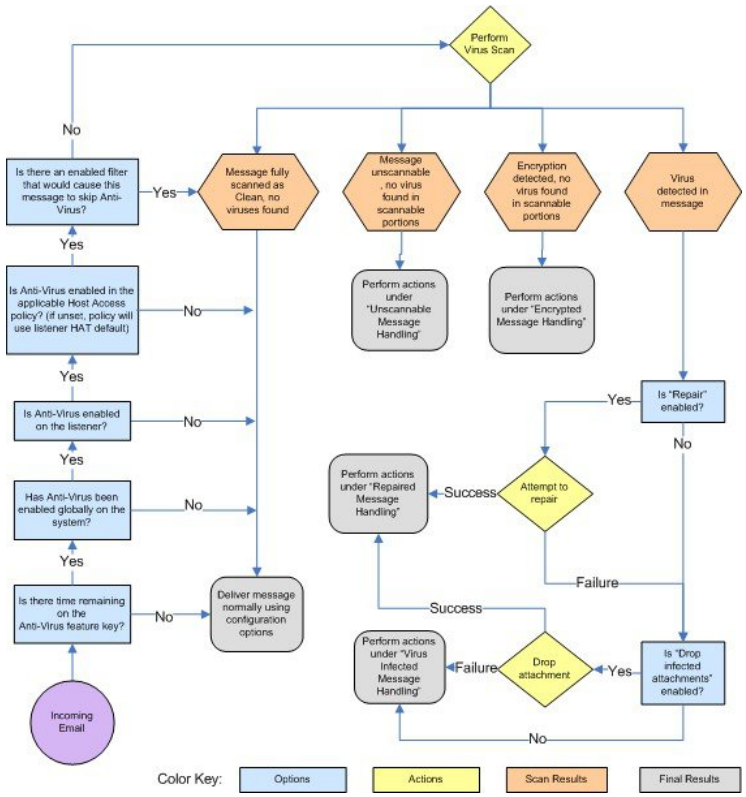
状況	アンチウイルス設定
ウイルスが広範囲に発生 ウイルス性のメッセージは単純にシステムからドロップされ、他の処理が実行されることはほとんどありません。	**添付ファイルのドロップ**：しない。 **スキャン**：スキャンのみ。 **クリーンアップされたメッセージ**：配信する。 **スキャンできないメッセージ**：メッセージをドロップする。 暗号化されたメッセージ：管理者に送るか隔離して、後で確認する。 ウイルス性のメッセージ：メッセージをドロップする。
リベラルなポリシー できる限り多くのドキュメントを送信します。	**添付ファイルのドロップ**：する。 **スキャン**：スキャンして修復。 **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：隔離するか、マークして転送する。

状況	アンチウイルス設定
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**：スキャンして修復。 **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、隔離する、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、隔離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**：スキャンのみ。 **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：隔離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

次の図に、アンチウイルスアクションおよびオプションが、電子メールゲートウェイ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。

Figure 2: アンチウイルス アクションのフロー ダイアグラム



Note 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、Cisco 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、電子メールゲートウェイは、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、隔離など）を実行します。

アンチウイルススキャンをテストするための電子メールゲートウェイへのメールの送信

Procedure

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。

[セキュリティサービス（Security Services）] > [Sophos] または [McAfeeウイルス対策（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、[電子メールセキュリティマネージャ（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*
```

Note
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。

Note
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、ステップ 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（詳細については、メッセージを受け入れるドメインおよびユーザの追加を参照してください。）

シスコ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。

Note
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。

a. ウイルス スキャンを、[スキャンして修復（Scan and Repair）] モードまたは [スキャンのみ（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、[ウイルス感染したメッセージ（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, on page 11の設定）と一致していることを確認します。

b. ウイルス スキャンを、[スキャンして修復（Scan and Repair）] モードまたは [スキャンのみ（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、[修復されたメッセージ（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, on page 11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。

ウイルス定義ファイルの更新

関連項目

- HTTP を使用したアンチウイルス アップデートの取得について , on page 21
- アップデート サーバ設定の構成 , on page 22
- モニタリングおよび手動での Anti-Virus アップデート チェック, on page 22
- 電子メールゲートウェイでのアンチウイルスファイルの更新の確認, on page 22

HTTP を使用したアンチウイルス アップデートの取得について

Sophos および McAfee は新たに識別されたウイルスのウイルス定義を頻繁にアップデートします。これらの更新は、電子メールゲートウェイに渡す必要があります。

デフォルトでは、電子メールゲートウェイは、5 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 および McAfee のアンチウイルス エンジンの場合は、サーバは動的 Web サイトからアップデートします。

アップデートを電子メールゲートウェイにダウンロードしている間は、アップデートのタイムアウトにはなりません。アップデートのダウンロードが長時間中断すると、ダウンロードがタイムアウトします。

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（[セキュリティ サービス（Security Services）]>[サービスのアップデート（Service Updates）] で定義されています）。

この設定値は、接続速度の遅いアプライアンスが、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。

アップデート サーバ設定の構成

[セキュリティサービス（Security Services）] > [サービスのアップデート（Service Updates）] ページでウイルス更新設定を設定できます。たとえば、システムがアンチウイルスの更新を受ける方法や更新を確認する頻度を設定できます。追加設定に関する詳細については、サービスアップデートを参照してください。

モニタリングおよび手動での Anti-Virus アップデート チェック

[セキュリティサービス（Security Services）] > [Sophos] または [McAfee] ページまたは CLI の `antivirusstatus` コマンドを使用して、電子メールゲートウェイに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実行することもできます。手動でのアンチウイルス エンジンの更新 , on page 22を参照してください

手動でのアンチウイルス エンジンの更新

Procedure

ステップ 1 [セキュリティサービス（Security Services）] > [Sophosウイルス対策（Sophos Anti-Virus）] または [McAfeeウイルス対策（McAfee Anti-Virus）] ページに移動します。

ステップ 2 [現在のMcAfee/Sophosウイルス対策ファイル（Current McAfee/Sophos Anti-Virus Files）] テーブルで、[今すぐ更新（Update Now）] をクリックします。

電子メールゲートウェイは最新のアップデートを確認してダウンロードします。

What to do next

これは、antivirusstatus および antivirusupdate コマンドを使用してコマンドライン インターフェイスでも構成できます。

電子メールゲートウェイでのアンチウイルスファイルの更新の確認

アップデータ ログを表示して、アンチウイルス 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。アップデータ 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。

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。