

Symantec AntiVirus for Microsoft ISA Server 実装ガイド



このマニュアルで説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

著作権

Copyright (C) 2000–2003 Symantec Corporation.

All Rights Reserved.

このマニュアルの一部または全部を許可なく複写することはできません。

商標

Symantec、Symantec ロゴ、LiveUpdate は Symantec Corporation の米国における登録商標です。Bloodhound、Symantec AntiVirus、Symantec Security Response は Symantec Corporation の商標です。Microsoft、Windows、Windows NT、ActiveX は Microsoft Corporation の登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

第 1 章	Symantec AntiVirus for ISA Server の紹介	
	Symantec AntiVirus for ISA Server について	1-2
	ソフトウェアコンポーネント	1-2
	Symantec AntiVirus for ISA Server コネクタ	1-3
	Symantec AntiVirus Scan Engine について	1-3
	スキャンと修復の概要	1-4
	ファイルのスキャン時の処理	1-4
	ISA 管理コンソールを通したウイルス対策の設定	1-5
	配置オプション	1-6
	オフボックスとオンボックスの設定	1-6
	大規模なトラフィック量の扱い	1-7
	マニュアルの読み方	1-7
	さらに詳しく知るには	1-8
	ヘルプの表示	1-8
	シマンテック社の Web サイト	1-9
第 2 章	Symantec AntiVirus for ISA Server のインストール	
	ソフトウェアのインストールについて	2-2
	インストールの準備	2-2
	Microsoft 社の Active Directory を正しく設定する	2-2
	ホストコンピュータをウイルス感染から保護する	2-3
	Symantec AntiVirus Scan Engine のインストール	2-3
	Symantec AntiVirus for ISA Server コネクタのインストール	2-5
	リモート管理コンポーネントのインストール	2-11
	ソフトウェアのアンインストール	2-12
	Symantec AntiVirus Scan Engine のアンインストール	2-12
	Symantec AntiVirus for ISA Server コネクタの アンインストール	2-12
第 3 章	Symantec AntiVirus for ISA Server のフィルタの設定	
	Symantec AntiVirus のフィルタについて	3-2
	SMTP フィルタについて	3-2
	Web フィルタについて	3-3
	SMTP フィルタのプロパティの設定	3-4
	Symantec AntiVirus for ISA Server SMTP Filter の設定	3-5

SMTP フィルタに使うスキャンエンジンの指定	3-6
SMTP フィルタ用のスキャンエンジンの接続をテスト	3-9
スキャンエンジンが利用不能な場合の SMTP トラフィック の遮断	3-9
形式不良な MIME メッセージの遮断	3-10
SMTP スキャンポリシーの設定	3-11
SMTP フィルタの場合にスキャンするファイルの指定	3-12
Symantec AntiVirus for ISA Server SMTP Filter の有効化	3-14
Web フィルタのプロパティの設定	3-15
Symantec AntiVirus for ISA Server Web Filter の設定	3-16
Web フィルタの使うスキャンエンジンの指定	3-17
Web フィルタ用のスキャンエンジンの接続のテスト	3-20
スキャンエンジンが利用不能な場合の Web トラフィック の遮断	3-21
ブラウザの快適化	3-21
Web スキャンポリシーの設定	3-22
Web フィルタの場合にスキャンするファイルの指定	3-23
ある種の MIME をスキャンから除外する	3-25
Symantec AntiVirus for ISA Server Web Filter の有効化	3-26
HTTP リダイレクタフィルタの設定	3-26

第 4 章

Symantec AntiVirus for ISA Server の警告とログ記録

Symantec AntiVirus for ISA Server のログ記録と警告について	4-2
警告について	4-2
ログ記録について	4-6

第 5 章

LiveUpdate の使い方

LiveUpdate について	5-2
ウイルス定義ファイルについて	5-2
Symantec AntiVirus Scan Engine 用のウイルス定義の更新	5-3
LiveUpdate 経由の製品更新版の入手	5-3

索引

Symantec AntiVirus for ISA Server の紹介

この章には次の大見出しがあります。

- [Symantec AntiVirus for ISA Server について](#)
- [ソフトウェアコンポーネント](#)
- [スキャンと修復の概要](#)
- [配置オプション](#)
- [マニュアルの読み方](#)
- [さらに詳しく知るには](#)

Symantec AntiVirus for ISA Server について

ウイルスによる攻撃の可能性はインターネットの否定的な側面です。インターネット環境においてウイルスは伝染しやすく、重要な取り引き活動や財務投資に重大な脅威を投げかけます。ゲートウェイにウイルス対策保護を実装することは、ネットワークをウイルスやその他の関連する脅威から保護する上で重要な手順です。Symantec AntiVirus for ISA Server は Microsoft ISA (Internet Security and Acceleration) Server に対するウイルススキャンと修復のサービスを電子メールと Web の両方のトラフィックについて提供します。Microsoft ISA Server に対するウイルススキャンは Microsoft ISA Server と一体化して統合されるので、個々のプロキシによってウイルススキャンを制御でき、ほとんどのオプションは ISA 管理コンソールを通して直接設定できます。

Symantec AntiVirus for ISA Server のウイルススキャンは SMTP と Web のトラフィックに個別のフィルタを使うことによって実装されます。ISA 管理コンソールを通してフィルタのプロパティを設定すれば、ウイルススキャンの対象にしたいファイルのみが個別にインストールした Symantec AntiVirus Scan Engine に渡ります。選択する設定オプションに応じて、スキャンの完了時に修復不能な感染ファイルは遮断され、未感染のファイルや修復できる感染ファイルは許可されてユーザーに渡ります。

Symantec AntiVirus for ISA Server は数々の賞に輝きシマンテック社をウイルス対策ソフトウェア業界の第一人者にした Symantec AntiVirus 技術の主なすべてを備えた Symantec AntiVirus Scan Engine を搭載しています。Symantec AntiVirus は悪質なウイルスの攻撃を検出や防止する上で最も効果的な最速のウイルスソリューションの 1 つです。

ソフトウェアコンポーネント

Symantec AntiVirus 4.3 for ISA Server は個別にインストールされる 2 つのコンポーネントで構成されます。Symantec AntiVirus Scan Engine はウイルススキャンと修復のサービスを提供し、Symantec AntiVirus for ISA Server コネクタはスキャンのダイアログボックスようになるファイルを渡せるように Symantec AntiVirus Scan Engine との通信を提供します。

p.1-3 の「[Symantec AntiVirus for ISA Server コネクタ](#)」を参照してください。

p.1-3 の「[Symantec AntiVirus Scan Engine について](#)」を参照してください。

Symantec AntiVirus for ISA Server コネクタ

Symantec AntiVirus for ISA Server コネクタは Microsoft ISA Server を実行するサーバーと同じコンピュータにインストールする必要があります。Microsoft ISA Server のアレイを設定した場合、アレイに属するサーバーごとにコネクタをインストールする必要があります。コネクタを使うとそれぞれの Microsoft ISA Server が Symantec AntiVirus Scan Engine と通信してスキャンの対象になるファイルを提出できるようになります。

コネクタには Symantec AntiVirus の SMTP と Web のフィルタが入っています。それぞれのフィルタは ISA 管理コンソールを通して個別に設定できます。管理コンソールを通して、Symantec AntiVirus Scan Engine に対する接続を確立するために必要な情報を入力したり、スキャンの対象として送信するファイルの種類を（拡張子や MIME の種類によって）指定したり、感染ファイルの扱い方を指定したり、製品を更新するために LiveUpdate を起動したり、ヘルプを表示したりできます。

「[第 3 章 Symantec AntiVirus for ISA Server のフィルタの設定](#)」を参照してください。

Symantec AntiVirus Scan Engine について

Symantec AntiVirus Scan Engine は Symantec AntiVirus for ISA Server にウイルススキャンと修復のサービスを提供するスキャンエンジンです。Symantec AntiVirus Scan Engine は Microsoft ISA Server やコネクタと同じコンピュータ上またはネットワーク上の異なるコンピュータ上にインストールできます。スキャンエンジンはそれ自体の Web ベースの管理インターフェースを通してコネクタとは別に設定できます。

確立したスキャンの基準に合うファイルはスキャンの対象として Microsoft ISA Server から Symantec AntiVirus Scan Engine に渡ります。スキャンが完了すると、スキャンエンジンはファイルが未感染か感染状態かについての情報を返します。感染ファイルが修復可能でスキャンエンジンが修復を試みる設定になっている場合、スキャンエンジンはクリーニングしたファイルを返します。

Symantec AntiVirus Scan Engine はキャリアクラスで利用可能な最速で最も効果的なスキャンエンジンの 1 つです。Symantec AntiVirus 技術を使って、スキャンエンジンは主なすべてのファイルの種類におけるウイルス、トロイの木馬、インターネットワームからの総合的な保護を提供します。Symantec AntiVirus Scan Engine は圧縮形式のファイルや入れ子になったファイルを扱う分解プログラムも備えています。

Symantec AntiVirus Scan Engine は Java、ActiveX、スタンドアロンスクリプトベースの脅威などのモバイルコードも検出します。Symantec AntiVirus Scan Engine はシマンテック社の主なウイルス対策エンジン技術を使います。具体的には、新種つまり未知のウイルスをヒューリスティックに検出する Bloodhound、LiveUpdate 経由で新種のウイルスから自動的に保護する NAVEX などが使われます。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

スキャンと修復の概要

Microsoft ISA Server は拡張性の高い企業向けファイアウォールと Web キャッシュのサーバーであり、ポリシーベースのセキュリティ、加速性、ネットワークやインターネットの管理を提供します。Symantec AntiVirus for ISA Server を使うと ISA Server のセキュリティオプションを拡張して総合的なウイルス対策を備えることができます。

Microsoft ISA Server をファイアウォール、キャッシュ、統合のいずれのモードで実行するかに応じて、Symantec AntiVirus for ISA Server を使えばフィルタを個別に設定して次のことができます。

- HTTPやブラウザベースのFTPを含めてすべてのWebトラフィックをウイルススキャンします（HTTPはHypertext Transfer Protocol、FTPはFile Transfer Protocolの略です）。
- 着信と発信のSMTPトラフィックをウイルススキャンします（SMTPはSimple Mail Transfer Protocolの略です）。

ファイルのスキャン時の処理

いったん Symantec AntiVirus for ISA Server コネクタと Symantec AntiVirus Scan Engine をインストールして正しく設定すれば、スキャンしたいファイルが分析の対象としてスキャンエンジンに渡ります。ウイルスが検出されると、選択した設定オプションに応じて Symantec AntiVirus Scan Engine は次の 1 つ以上のことをします。

- 感染が見つかったというログエントリを記録する：Symantec AntiVirus Scan Engine で追加のログ記録と警告のオプションをアクティブにすれば Microsoft ISA Server とアプリケーションイベントログを通した Symantec AntiVirus for ISA Server のログ記録と警告を補足できます。
- 感染ファイルの修復を試みる：ファイルを修復できる場合、スキャンエンジンは修復つまりクリーニングしたファイルを Microsoft ISA Server に返します。

- 修復不能なファイルを削除する：ファイルを修復できない場合、Symantec AntiVirus Scan Engine でファイルを削除するように設定できます。

SMTPトラフィックの場合にスキャンエンジンで修復不能なファイルを削除するオプションを設定すると、感染添付ファイルを電子メールメッセージから削除できます。Webトラフィックの場合、ファイルに対するアクセスは拒否されます。SMTPとWebの両方のトラフィックの場合、コンテナまたはアーカイブファイルに修復不能な埋め込みファイルが入っていると、修復不能なファイルはコンテナまたはアーカイブファイルから削除され、残りの未感染の内容は本来の送信先に転送されます。

Symantec AntiVirus Scan Engine でウイルスが見つからない場合、スキャンエンジンはファイルが未感染なので適切に処理できることを示します。

ISA 管理コンソールを通したウイルス対策の設定

ウイルス対策保護を設定するためのほとんどのオプションは ISA 管理コンソールを通して Web フィルタと SMTP フィルタに対して個々に設定できます。

「[第3章 Symantec AntiVirus for ISA Server のフィルタの設定](#)」を参照してください。

ウイルス対策保護を設定するときには次のことをする必要があります。

- 感染ファイルの処理のしかたを決める：Symantec AntiVirus Scan Engine はファイルをスキャンして未感染か感染状態をログに記録のみするか、感染ファイルの修復を試みるか、すべての感染ファイルを削除するかのいずれかに設定できます。

スキャンしたファイルの処置のしかたについては Symantec AntiVirus Scan Engine の設定よりも SMTP フィルタスキャンポリシーの設定が優先されます。スキャンポリシー情報は ICAP ヘッダー経由で SMTP フィルタから Symantec AntiVirus Scan Engine に直接提供されます。スキャンエンジンは ICAP ヘッダーにある情報を使ってスキャンしたファイルの処置を決定します。

- スキャンするファイルまたは添付ファイルの種類を選択する：ウイルスがいる可能性があるのは特定の種類のファイルのみです。ウイルススキャンの対象になるファイルの種類を制御することによって帯域幅を節約できて処理速度が向上します。拡張子や MIME の種類によってスキャンを限定するか、またはセキュリティを最大限に強化したければすべての種類のファイルをスキャンするように設定できます。

スキャンしたファイルの処置とスキャンするファイルの種類については Symantec AntiVirus Scan Engine の設定よりも SMTP フィルタと

Web のフィルタの設定が優先されます。スキャンするファイルの種類についての情報は ICAP ヘッダー経由で SMTP フィルタまたは Web フィルタから Symantec AntiVirus Scan Engine に直接提供されます。メッセージは MIME エンコードなので、フィルタはファイルの種類 of 初期判断を試みません。フィルタは単純にすべてのトラフィックを Symantec AntiVirus Scan Engine に渡します。スキャンエンジンは添付ファイルやアーカイブファイルに入っている個々のファイルを含めたメッセージの各部の処置とスキャンをするときに ICAP ヘッダーにある情報を使ってスキャンするファイルを決定します。

- 修復できない感染ファイルに対するアクセスを遮断する。
- ウイルスが見つかったことをユーザー（たとえば、感染メールメッセージの送信者と受信者）に警告する：Symantec AntiVirus Scan Engine にはメッセージの受信者に感染について警告するために感染電子メールメッセージの本文にテキストを追加するオプションがあります。
- イベントをログに記録する：選択したイベントは Symantec AntiVirus for ISA Server によって Microsoft ISA Server が動作するコンピュータ上のアプリケーションイベントログに自動的に記録されます。Symantec AntiVirus Scan Engine を通して追加のログ記録オプションも利用可能です。イベントのログ記録に関してサイトのニュースを検討し、それに応じてスキャンエンジンを設定してください。

「[第 4 章 Symantec AntiVirus for ISA Server の警告とログ記録](#)」を参照してください。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

配置オプション

Symantec AntiVirus for ISA Server を配置する上でいくつかのオプションが利用可能です。Symantec AntiVirus Scan Engine は Microsoft ISA Server と同じコンピュータまたはネットワーク上の異なるコンピュータにインストールできます。Microsoft ISA Server を実行するコンピュータごとに Symantec AntiVirus for ISA Server コネクタをインストールする必要があります。

オフボックスとオンボックスの設定

Symantec AntiVirus Scan Engine と Microsoft ISA Server をネットワーク上の異なるコンピュータ上にインストール（オフボックス設定）すると、ファイルはネットワーク上のソケット経由で Symantec AntiVirus Scan Engine に

渡ります。コネクタがスキャンエンジンに交信できるようにスキャンエンジンに適切な IP アドレスとポート番号を割り当てる必要があります。

Symantec AntiVirus Scan Engine は Microsoft ISA Server と同じコンピュータ上にインストール（オンボックス設定）もできます。ほとんどの場合、オフボックス設定よりもオンボックス設定の方が高い処理効率を提供します。

大規模なトラフィック量の扱い

単純な Symantec AntiVirus for ISA Server の設定においては単一の Symantec AntiVirus Scan Engine が単一の Microsoft ISA Server に対してスキャンと修復のサービスのサービスを扱います。ただし、通常は大規模なトラフィックボリュームには Microsoft ISA Servers のアレイが必要です。ウイルススキャンの負荷分散も複数の Symantec AntiVirus Scan Engine に渡ってできます。

Symantec AntiVirus Scan Engine の処理速度はスキャンボリューム、Symantec AntiVirus Scan Engine に要求を作成するクライアント ISA サーバーの台数、メモリ容量とディスク容量の必要条件に依存します。大規模なトラフィックボリュームを処理しようとする場合またはスキャン要求を作成する複数の ISA サーバーがある場合は、複数の Symantec AntiVirus Scan Engine を設定してウイルススキャンの負荷を扱うことができます。

Symantec AntiVirus for ISA Server には SMTP と Web のフィルタを個別に設定するオプションがあり、具体的な必要条件に合わせてスキャンエンジンのリソースを割り当てるのが可能です。Web または SMTP のトラフィックにサービスを提供するために個別のスキャンエンジンを指定することも複数のスキャンエンジンを使って両方のフィルタにスキャンを提供することもできます。複数の Symantec AntiVirus Scan Engine を登録すると、登録済みのすべてのスキャンエンジンに渡って負荷分散が自動的に扱われます。

マニュアルの読み方

『Symantec AntiVirus for Microsoft ISA Server 実装ガイド』は Symantec AntiVirus for ISA Server のインストールと設定を説明します。対象は Microsoft ISA Server と Symantec AntiVirus for ISA Server の管理者です。

このソフトウェアとは別にインストールするコンポーネントである Symantec AntiVirus Scan Engine のインストールと設定について詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

ソフトウェアを確実に効果的に活用するには次の手順に従います。

- Symantec AntiVirus for ISA Server の設計と機能を理解します。
「[第 1 章 Symantec AntiVirus for ISA Server の紹介](#)」を参照してください。
- ネットワーク上に個別にインストールする Symantec AntiVirus Scan Engine を具体的な必要条件に合わせてどう配置するかを決めます。
『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
- Symantec AntiVirus Scan Engine をインストールします。
『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
- Symantec AntiVirus for ISA Server コネクタを正しくインストールして設定します。
「[第 2 章 Symantec AntiVirus for ISA Server のインストール](#)」と「[第 3 章 Symantec AntiVirus for ISA Server のフィルタの設定](#)」を参照してください。
- Symantec AntiVirus for ISA Server のイベントについて理解するためにログ記録と警告の使い方についての説明を読みます。
「[第 4 章 Symantec AntiVirus for ISA Server の警告とログ記録](#)」を参照してください。
- Symantec AntiVirus Scan Engine が新種のウイルスを検出や除去するために必要な情報を常に入手できるように LiveUpdate を設定します。
「[第 5 章 LiveUpdate の使い方](#)」を参照してください。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

さらに詳しく知るには

この製品には実装ガイドとヘルプシステムが付属しています。さらに別にインストールする Symantec AntiVirus Scan Engine に別のマニュアルが付属しています。

ヘルプの表示

マニュアルのほかに Symantec AntiVirus for ISA Server にはヘルプシステムがあります。ISA の管理コンソールで直接表示できます。

ヘルプを表示するには

- ◆ 次のいずれかの操作をします。
 - [Symantec SMTP AV Filter のプロパティ] ダイアログボックスで F1 キーを押します。
 - [Symantec Web AV Filter のプロパティ] ダイアログボックスで F1 キーを押します。

シマンテック社の Web サイト

製品に関する追加情報や FAQ に対する回答についてはシマンテック社の Web サイトを参照してください。

www.symantec.co.jp

Symantec AntiVirus for ISA Server のインストール

この章には次の大見出しがあります。

- ソフトウェアのインストールについて
- インストールの準備
- Symantec AntiVirus Scan Engine のインストール
- Symantec AntiVirus for ISA Server コネクタのインストール
- リモート管理コンポーネントのインストール
- ソフトウェアのアンインストール

ソフトウェアのインストールについて

Symantec AntiVirus for ISA Server のソフトウェアは個別にインストールされる 2 つのコンポーネントで構成されます。

- Symantec AntiVirus Scan Engine バージョン 4.0: Symantec AntiVirus Scan Engine はウイルススキャンと修復のサービスを提供し、Microsoft ISA Server と同じコンピュータまたはネットワーク上の異なるコンピュータにインストールできます。
- Symantec AntiVirus for ISA Server コネクタ: コネクタは Microsoft ISA Server を実行するコンピュータごとにインストールする必要があります。

ISA 管理を使って ISA サーバーをリモートで管理しようとする場合には、ISA Server をリモートで管理するためのコンピュータごとに Symantec AntiVirus for ISA Server のリモート管理コンポーネントもインストールする必要があります。Symantec AntiVirus for ISA Server リモート管理スナップインコンポーネントを使うと SMTP や Web のフィルタをリモートで管理できます。

p.2-11 の「[リモート管理コンポーネントのインストール](#)」を参照してください。

インストールの準備

Symantec AntiVirus Scan Engine をインストールする前に次のことを考慮してください。

- アレイ設定を使おうとする場合、Microsoft 社の Active Directory をネットワークに合わせて正しく設定してあることを確認します。
- Symantec AntiVirus Corporate Edition などのウイルス対策製品を使って Symantec AntiVirus Scan Engine や Microsoft ISA Server を実行するコンピュータを確実に保護します。

Microsoft 社の Active Directory を正しく設定する

Microsoft ISA Server のアレイ設定を使おうとする場合には、Microsoft 社の Active Directory ドメインコントローラをネットワークに合わせて正しく設定してあることを確認します。Active Directory は Windows アーキテクチャに不可欠のコンポーネントです。該当するマイクロソフト製品のマニュアルに従って設定してください。

ホストコンピュータをウイルス感染から保護する

設計上、Symantec AntiVirus Scan Engine はスキャンエンジンにファイルを渡すように設計してあるクライアントアプリケーションから届くファイルのみをスキャンします。Symantec AntiVirus Scan Engine はそれが動作中のコンピュータや Microsoft ISA Server が動作中のホストコンピュータは保護しません。これらのサーバーは両方とも潜在的に感染ファイルを扱うので、オペレーティングシステムのウイルスに対するリアルタイム保護がなければ脆弱です。

Symantec AntiVirus Scan Engine による総合的な保護を実行するには、ホストコンピュータをウイルスの攻撃から保護することも重要です。ホストコンピュータを保護するには、Symantec AntiVirus Scan Engine や Microsoft ISA Server を実行しているサーバー上で Symantec AntiVirus Corporate Edition を実行します。

警告 Symantec AntiVirus Scan Engine とホストコンピュータ上で動作しているウイルス対策製品の競合を防ぐために、ホストコンピュータ上のウイルス対策製品のオプションで Symantec AntiVirus Scan Engine がスキャンに使う一時ディレクトリをスキャンしないように設定する必要があります。

Symantec AntiVirus Scan Engine のインストール

Symantec AntiVirus for ISA Server は Symantec AntiVirus Scan Engine のバージョン 4.3 と連携して働きます。Symantec AntiVirus Scan Engine は Microsoft ISA Server と同じコンピュータか、またはネットワーク上の異なるコンピュータにインストールできます。ネットワーク上の異なるコンピュータにスキャンエンジンをインストールしようとする場合にはスキャンエンジンがサポートする任意のオペレーティングシステムにインストールできます。サポートするオペレーティングシステムは Sun Solaris、Red Hat Linux、Microsoft Windows 2000 Server/Server 2003 です。Symantec AntiVirus Scan Engine のインストール先になる予定のサーバーが『Symantec AntiVirus Scan Engine 実装ガイド』に載っているシステムの必要条件に合うことを確認してください。

コネクタのインストール時に Symantec AntiVirus Scan Engine に対する接続を確認できるように Symantec AntiVirus for ISA Server コネクタの前に Symantec AntiVirus Scan Engine をインストールする必要があります。

スキャンエンジンのインストールと設定について詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

Symantec AntiVirus Scan Engineを正しくインストールして設定するには次の指針に従ってください。

- 通信プロトコルとして ICAP を選択します。

インストール時の選択に応じて、ICAP が事前選択されてこのオプションが利用不能になることがあります。たとえば、コネクタとスキャンエンジンの両方を同時にインストールするオプションを選択した場合などです。
- Symantec AntiVirus Scan Engine の ICAP バインドアドレスを調べて内部アクセスのみが許可されることを確認します。

デフォルトではスキャンエンジンはすべてのインターフェースにバインドするので、内部アクセスのみを許可するにはこの設定を変更する必要があります。Symantec AntiVirus Scan Engine を ISA Server と同じコンピュータ上で実行しようとする場合にはループバックインターフェースを使ってスキャンを限定することを検討します。
- SMTPトラフィックに対するウイルススキャンを提供しようとする場合にはSymantec AntiVirus Scan Engine でメールメッセージの本文を更新する機能をアクティブにします。

この機能を使うと添付ファイルが感染していたメッセージの受信者に警告するためにMIMEエンコードメッセージの本文にテキストを追加できます。メッセージの（編集できる）デフォルトテキストは添付ファイルにウイルスが入っていて修復したか修復できなかったために削除したことを示します。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
- Symantec AntiVirus Scan Engine のログ記録の機能を Microsoft ISA Server のログ記録とレポートのシステムを通して直接利用可能なウイルス検出に関するログ記録と警告と考え合わせ、それに従って必要なSymantec AntiVirus Scan Engineのログ記録の機能をアクティブにします。

選択肢はコネクタとSymantec AntiVirus Scan Engineを同じコンピュータまたは異なるコンピュータのいずれかで実行するかに応じて変わる可能性があります。

「[第4章 Symantec AntiVirus for ISA Server の警告とログ記録](#)」を参照してください。
- ウイルススキャンに加えて電子メールトラフィックに対するメールポリシーを確立する計画がある場合には、Symantec AntiVirus Scan Engine と Microsoft ISA Server で類似のメールポリシーオプションが

利用可能であることに注目してください。たとえば、件名またはメッセージの送信元によってメッセージを遮断するなどです。

ポリシーオプションを設定するときには、重複するポリシーや競合するポリシーを作成していないことを確認してください。競合を防ぐにはスキャンエンジンまたはISA Serverのいずれかのポリシーオプションを使い、両方を使うのは避けます。これはSymantec AntiVirus Scan EngineがISA Serverに加えてネットワーク上の他のクライアントアプリケーションにスキャンサービスを提供する場合に重要になる可能性があります。

メモ Symantec AntiVirus Scan Engineでメールポリシーオプションを使ってMIMEエンコードメッセージでウイルスが見つかった場合に感染メッセージの受信者に警告するためにスキャンエンジンでメールメッセージの本文を更新する機能をアクティブにすると、メールポリシーに違反するメッセージも受信者に違反を知らせるように更新されます。スキャンエンジンのメールメッセージの本文を更新する機能はMicrosoft ISA Serverで確立したメールポリシーの結果であるメールポリシー違反を報告しません。

- ブラウザの快適化を（異常に大きいファイルや複雑なファイルのスキャン時にブラウザが時間切れになるのを防ぐために）使う計画がある場合、Microsoft for ISA ServerのWebフィルタを通して利用可能なブラウザの快適化機能を使ってください。冗長になるのを防ぐにはSymantec AntiVirus Scan Engineのデータ細流化機能を有効にしないでください。

Symantec AntiVirus for ISA Server コネクタのインストール

コネクタはMicrosoft ISA Serverと同じコンピュータ上にインストールする必要があります。Microsoft ISA Serverとコネクタのインストール先になるコンピュータはMicrosoft ISA Serverのマニュアルに載っているシステムの必要条件に合い、さらに次の必要条件に合わなければなりません。

- Microsoft Windows 2000 Server Service Pack 3/Advanced Server をインストールしてあること

メモ Symantec AntiVirus for ISA ServerはMicrosoft Windows 2000 Data Center Server Service Pack 2をインストールしてあるコンピュータ上でも機能します。

- Microsoft Internet Security and Acceleration Server 2000 Service Pack 1 をインストールしてあること

コネクタをインストールする前に Microsoft ISA Server をインストールして正しく働くようにしておく必要があります。Microsoft ISA Server のインストールと設定について詳しくはマイクロソフト製品のマニュアルを参照してください。

Symantec AntiVirus for ISA Server コネクタのインストール

インストール時に両方 SMTP フィルタと Web フィルタの両方をインストールするか 1 つのフィルタのみをインストールすることによってインストールをカスタマイズするかをオプションで選択できます。

SMTP フィルタと Web フィルタの両方をインストールするには

- 1 Microsoft ISA Server をインストールしてあるコンピュータに管理者としてか管理者権利付きでログオンします。
- 2 Symantec AntiVirus for ISA Server の配布 CD を CD-ROM ドライブに挿入します。
- 3 インストールする製品のリストで次のいずれかを選択します。
 - [Symantec AntiVirus for Microsoft ISA Server のインストール (I)] : Symantec AntiVirus Scan Engine を異なるコンピュータ上にインストールしようとする場合にコネクタのみを選択します。コネクタは Microsoft ISA Server が動作するコンピュータ上にインストールする必要があります。Symantec AntiVirus Scan Engine はシステムの必要条件に合う別のコンピュータ上にインストールできます。
 - [両製品のインストール (B)]: Microsoft ISA Server を実行するコンピュータ上にコネクタと Symantec AntiVirus Scan Engine をインストールしようとする場合に両方の製品を選択します。Symantec AntiVirus Scan Engine が最初にインストールされます。コネクタのインストールはスキャンエンジンのインストールが終了すると自動的に開始されます。
詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
- 4 使用許諾契約の条項に同意することを示してから [次へ (N)] をクリックします。
同意しないとインストールを続行できません。
- 5 [セットアップタイプ] グループで [完全] を選択してから [次へ (N)] をクリックします。

- 6 [インストール先の場所を選択してください] の下でフィルタのインストール先になるフォルダを選択してから [次へ (N)] をクリックします。

デフォルトの場所は <ドライブ>:\Program Files\Symantec\Symantec AntiVirus for ISA Server (<ドライブ> は Microsoft ISA Server をインストールしてあるドライブ) です。複数の ISA Server のアレイを使う場合、アレイに属するすべてのコンピュータ上の ISA Server に対して同じ相対パスを維持する必要があります。このオプションはアレイに属する 1 台目のコンピュータに Symantec AntiVirus for ISA Server をインストールした直後には利用不能な場合があります。

- 7 [Symantec AntiVirus Scan Engine の設定] グループで [スキャンエンジンアドレスの設定] を選択してから次のすべての操作をします。

- [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで [追加 (A)] をクリックします。

- [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスで [Symantec AntiVirus Scan Engine の IP] フィールドにスキャンエンジンの IP アドレスを入力します。

スキャンエンジンが動作するコンピュータに複数の IP アドレスがある場合には Symantec AntiVirus Scan Engine が応答準備するアドレスを指定します。Symantec AntiVirus Scan Engine が Microsoft ISA Server と同じコンピュータ上で動作する場合には 127.0.0.1 (ループバックインターフェース) を使います。

- [Symantec AntiVirus Scan Engine のポート] フィールドにスキャンエンジンが応答準備するポートの番号を入力します。

ここで入力するポート番号は Symantec AntiVirus Scan Engine のインストール中に指定するポート番号と一致する必要があります。通信プロトコルとして ICAP を使うときの Symantec AntiVirus Scan Engine のデフォルトポート番号は 1344 です。

- スキャンエンジンに対する接続が確立されたことを確認するために [設定のテスト (T)] をクリックします。

インストール中に接続をテストするには Symantec AntiVirus Scan Engine をすでにインストールしてなければなりません。

p.3-9 の「SMTP フィルタ用のスキャンエンジンの接続をテスト」を参照してください。

p.3-20 の「Web フィルタ用のスキャンエンジンの接続のテスト」を参照してください。

- [追加 (A)] をクリックします。

- すべての Symantec AntiVirus Scan Engines を追加し終わるまでステップ 7 のすべてを繰り返します。

- スキャンエンジンを追加し終わったら [OK] をクリックします。
- 8 インストールに続いて自動的にファイアウォールや Web プロキシのサービスを再開するには [サービスを再開します] にチェックマークを付けます。

このオプションにチェックマークを付けない場合、SMTP や Web のフィルタを使う前にファイアウォールや Web プロキシのサービスを再開する必要があります。
 - 9 ISA のログ記録と警告のサブシステムで選択した Symantec AntiVirus for ISA Server イベントに対してデフォルト警告とログエントリを設定するには [デフォルト警告を設定します] にチェックマークを付けます。

インストール時にデフォルト警告を設定するオプションを選択しない場合、標準 ISA 管理ツールを使って記録したい警告を手動で設定する必要があります。インストール時にデフォルト警告を設定しない場合、手動で設定しないかぎり Symantec AntiVirus for ISA Server のイベントはアプリケーションイベントログに記録されません。

「[第 4 章 Symantec AntiVirus for ISA Server の警告とログ記録](#)」を参照してください。
 - 10 [次へ(N)] をクリックします。

インストーラはこの時点からインストールを続行します。インストール中に特に指定しないかぎり、インストールの完了時にフィルタが正しく機能するようにファイアウォールと Web プロキシのサービスが再開されます。デフォルト警告を設定しない場合を除いて、重要なインストール活動はアプリケーションイベントログに記録されます。

Web フィルタまたは SMTP フィルタのいずれかをインストールするには

- 1 Microsoft ISA Server をインストールしてあるコンピュータに管理者としてか管理者権利付きでログオンします。
- 2 Symantec AntiVirus for ISA Server 配布 CD を CD-ROM ドライブに挿入します。
- 3 インストールする製品のリストで次のいずれかを選択します。
 - [Symantec AntiVirus for Microsoft ISA Server のインストール (I)] : Symantec AntiVirus Scan Engine を異なるコンピュータ上にインストールしようとする場合にコネクタのみを選択します。コネクタは Microsoft ISA Server が動作するコンピュータ上にインストールする必要があります。Symantec AntiVirus Scan Engine はシステムの必要条件に合う別のコンピュータ上にインストールできます。

- [両製品のインストール (B)]: Microsoft ISA Server を実行するコンピュータ上にコネクタと Symantec AntiVirus Scan Engine をインストールしようとする場合に両方の製品を選択します。Symantec AntiVirus Scan Engine が最初にインストールされます。コネクタのインストールはスキャンエンジンのインストールが終了すると自動的に開始されます。
詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
- 4 使用許諾契約の条項に同意することを示してから [次へ (N)] をクリックします。
同意しないとインストールを続行できません。
 - 5 [セットアップタイプ] グループで [カスタム] を選択してから [次へ (N)] をクリックします。
 - 6 [機能の選択] グループで次のいずれかの操作をします。
 - SMTP フィルタをインストールするには [Symantec AntiVirus for ISA Server SMTP filter] にチェックマークを付けます。
 - Web フィルタをインストールするには [Symantec AntiVirus for ISA Server Web filter] にチェックマークを付けます。
 - 7 フィルタのインストール先になるフォルダを選択してから [次へ (N)] をクリックします。
デフォルトの場所は <ドライブ >:\Program Files\Symantec\Symantec AntiVirus for ISA Server (<ドライブ > は Microsoft ISA Server をインストールしてあるドライブ) です。複数の ISA Server のアレイを使う場合、アレイに属するすべてのコンピュータ上の ISA Server に対して同じ相対パスを維持する必要があります。このオプションはアレイに属する 1 台目のコンピュータに Symantec AntiVirus for ISA Server をインストールした直後には利用不能な場合があります。
 - 8 [Symantec AntiVirus Scan Engine の設定] グループで [スキャンエンジンアドレスの設定] を選択してから次のすべての操作をします。
 - [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで [追加 (A)] をクリックします。
 - [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスで in Symantec AntiVirus Scan Engine IP] フィールドにスキャンエンジンの IP アドレスを入力します。
スキャンエンジンが動作するコンピュータに複数の IP アドレスがある場合には Symantec AntiVirus Scan Engine が応答準備するアドレスを指定します。Symantec AntiVirus Scan Engine が Microsoft

ISA Server と同じコンピュータ上で動作する場合には 127.0.0.1 (ループバックインターフェース) を使います。

- [Symantec AntiVirus Scan Engine のポート] フィールドにスキャンエンジンが応答準備するポートの番号を入力します。
ここで入力するポート番号は Symantec AntiVirus Scan Engine のインストール中に指定するポート番号と一致する必要があります。通信プロトコルとして ICAP を使うときの Symantec AntiVirus Scan Engine のデフォルトポート番号は 1344 です。
 - スキャンエンジンに対する接続が確立されたことを確認するために [設定のテスト (T)] をクリックします。
インストール中に接続をテストするには Symantec AntiVirus Scan Engine をすでにインストールしてなければなりません。
p.3-9 の「SMTP フィルタ用のスキャンエンジンの接続をテスト」を参照してください。
p.3-20 の「Web フィルタ用のスキャンエンジンの接続のテスト」を参照してください。
 - [追加 (A)] をクリックします。
 - すべての Symantec AntiVirus Scan Engines を追加し終わるまでステップ 8 のすべてを繰り返します。
 - スキャンエンジンを追加し終わったら [OK] をクリックします。
- 9 インストールに続いて自動的にファイアウォールや Web プロキシのサービスを再開するには [サービスを再開します] にチェックマークを付けます。
このオプションにチェックマークを付けない場合、SMTP や Web のフィルタを使う前にファイアウォールや Web プロキシのサービスを再開する必要があります。
- 10 ISA のログ記録と警告のサブシステムで選択した Symantec AntiVirus for ISA Server イベントに対してデフォルト警告とログエントリを設定するには [デフォルト警告を設定します] にチェックマークを付けます。
インストール時にデフォルト警告を設定するオプションを選択しない場合、標準 ISA 管理ツールを使って記録したい警告を手動で設定する必要があります。インストール時にデフォルト警告を設定しない場合、手動で設定しないかぎり Symantec AntiVirus for ISA Server のイベントはアプリケーションイベントログに記録されません。
「第 4 章 Symantec AntiVirus for ISA Server の警告とログ記録」を参照してください。
- 11 [次へ (N)] をクリックします。

インストーラはこの時点からインストールを続行します。インストール中に特に指定しないかぎり、インストールの完了時にフィルタが正しく機能するようにファイアウォールと Web プロキシのサービスが再開されます。デフォルト警告を設定しない場合を除いて、重要なインストール活動はアプリケーションイベントログに記録されます。

リモート管理コンポーネントのインストール

ISA 管理を使って ISA サーバーをリモートで管理しようとする場合には、ISA Server をリモートで管理するためのコンピュータごとに Symantec AntiVirus for ISA Server のリモート管理コンポーネントもインストールする必要があります。Symantec AntiVirus for ISA Server リモート管理スナップインコンポーネントを使うと SMTP や Web のフィルタをリモートで管理できます。

リモート管理コンポーネントをインストールするには

- 1 Microsoft ISA Server をリモートで管理するためのコンピュータに管理者としてか管理者権利付きでログオンします。
- 2 Symantec AntiVirus for ISA Server の配布 CD を CD-ROM ドライブに挿入します。
- 3 インストールする製品のリストで [Symantec AntiVirus for Microsoft ISA Server のインストール] を選択します。
- 4 使用許諾契約の条項に同意することを示してから [次へ (N)] をクリックします。
同意しないとインストールを続行できません。
- 5 [セットアップタイプ] グループで [リモート管理] を選択してから [次へ (N)] をクリックします。
- 6 次のいずれかの操作をします。
 - SMTP フィルタをリモートで管理するには [Symantec AntiVirus for ISA Server SMTP 管理スナップイン] にチェックマークを付けます。
 - Web フィルタをリモートで管理するには [Symantec AntiVirus for ISA Server HTTP 管理スナップイン] にチェックマークを付けます。
- 7 リモート管理スナップインコンポーネントのインストール先になるフォルダを選択してから [次へ (N)] をクリックします。

デフォルトの場所は C:\Program Files\Symantec\Symantec AntiVirus for ISA Server です。

インストーラはこの時点からインストールを続行します。重要なインストール活動はアプリケーションイベントログに記録されます。

ソフトウェアのアンインストール

Symantec AntiVirus Scan Engine と Symantec AntiVirus for ISA Server コネクタは別々にアンインストールする必要があります。

Symantec AntiVirus Scan Engine のアンインストール

Symantec AntiVirus Scan Engine のマニュアルに従って Symantec AntiVirus Scan Engine をアンインストールします。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

Symantec AntiVirus for ISA Server コネクタのアンインストール

複数の Microsoft ISA サーバーのアレイを使っている場合、アレイにあるコンピュータごとから Symantec AntiVirus for ISA Server コネクタをアンインストールする必要があります。

Symantec AntiVirus for ISA Server コネクタをアンインストールするには

- 1 コントロールパネルで [アプリケーションの追加と削除] を開き、リストで [Symantec AntiVirus for ISA Server] を選択します。
- 2 [変更と削除 (C)] をクリックします。
- 3 画面の指示に従って操作しながらアンインストールを完了します。

Symantec AntiVirus for ISA Server のフィルタの設定

この章には次の大見出しがあります。

- [Symantec AntiVirus のフィルタについて](#)
- [SMTP フィルタのプロパティの設定](#)
- [Symantec AntiVirus for ISA Server SMTP Filter の有効化](#)
- [Web フィルタのプロパティの設定](#)
- [Symantec AntiVirus for ISA Server Web Filter の有効化](#)
- [HTTP リダイレクタフィルタの設定](#)

Symantec AntiVirus のフィルタについて

Symantec AntiVirus for ISA Server は独立したフィールドの使用を通して SMTP と Web のトラフィック用にウイルススキャンを提供します。いずれのフィルタもウイルススキャンと修復のサービスの対象になるファイルを本来の送信先に転送する前に Symantec AntiVirus Scan Engine を通してリダイレクトします。

Symantec AntiVirus for ISA Server SMTP Filter は電子メールトラフィック用のスキャンを提供します。

p.3-2 の「[SMTP フィルタについて](#)」を参照してください。

Symantec AntiVirus for ISA Server Web Filter は Web トラフィック用のスキャンを提供します。

メモ ブラウザベースの FTP 交換は Symantec AntiVirus for ISA Server Web Filter によるウイルススキャンを受けません。ウイルススキャンは非ブラウザ FTP クライアント（コマンドラインまたは GUI のユーティリティ）には利用不能です。このようなクライアントは FTP ホストと直接 FTP セッションを確立するので、FTP トラフィックはスキャン用にリダイレクトされません。保護を最大限に強化するには、この種類のトラフィックをファイアウォールで遮断すれば非ブラウザ FTP 交換を通したウイルス感染を防止できます。

p.3-3 の「[Web フィルタについて](#)」を参照してください。

SMTP フィルタについて

Symantec AntiVirus の SMTP フィルタは ISA Server のアプリケーションフィルタ拡張として書かれています。Symantec AntiVirus の SMTP フィルタは Microsoft ISA Server をファイアウォールモードまたは統合モードで実行するときに使われ、SMTP トラフィックに対するウイルススキャンを提供します。発着信する SMTP トラフィックはその送信先に転送される前に透過的なプロキシによって Symantec AntiVirus の SMTP フィルタでウイルススキャンできるようにリダイレクトされます。

SMTP が SMTP メッセージを受信すると、メッセージ全体がスキャンの対象として ICAP 経由で Symantec AntiVirus Scan Engine に転送されます。スキャンが完了すると、スキャンエンジンはファイルが未感染か感染していたかと修復したかどうかについての情報が入った ICAP ヘッダーを返します。感染ファイルを修復した場合には修復したファイルも返ります。

ICAP の限度

メッセージで複数の感染が見つかった場合、スキャンエンジンから SMTP フィルタに返る ICAP ヘッダーには 1 つ目の感染に関する情報のみが入ります。ヘッダーで返るデータの量は ICAP の限度です。ヘッダーはファイルの最終的な扱い方（たとえば、すべての感染が見つかったかどうか）を正確に示しますが、Microsoft ISA サーバー上のログ記録やレポートの目的で複数の感染が個々に列挙されることはありません。

この限度は Symantec AntiVirus Scan Engine のレポートやログ記録には影響しません。Symantec AntiVirus Scan Engine には見つかったすべての情報をログに記録するオプションがあり、メッセージの受信者に感染が見つかったことを通知するために感染電子メールメッセージの本文にテキストを追加するオプションを選択できます。Symantec AntiVirus Scan Engine のログエントリやレポートには（スキャンエンジンでウイルスの活動をログに記録するように設定していれば）たとえ単一メッセージに複数の感染があった場合にも見つかったすべてのウイルスについての正確な情報が入ります。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

Web フィルタについて

Symantec AntiVirus の Web フィルタは ISAPI (Internet Server Application Programming Interface) を使って書かれた Web フィルタのプラグインです。Web フィルタは Microsoft ISA Server がキャッシュモード、統合モード、ファイアウォールモードのいずれかで動作しているときに使われます。

ユーザーが HTTP 要求を作成すると、要求は Symantec AntiVirus の Web フィルタにリダイレクトされます。Symantec AntiVirus の Web フィルタはスキャンが必要かどうかを判断するために HTTP ヘッダーを解析します。スキャンが必要である場合（スキャンするファイルの種類はオプションで設定でき）、コンテンツは ICAP 経由で Symantec AntiVirus Scan Engine に送信されます。スキャンが完了すると、Symantec AntiVirus Scan Engine は（ICAP ヘッダーに入った）スキャン結果と潜在的に修正済みの要求を Symantec AntiVirus の Web フィルタに返します。コンテンツが未感染ならば、要求は要求側のユーザーに転送されます。コンテンツが感染していて修復した場合、修正済みの要求が要求側のユーザーに転送されます。修復不能な感染が見つかった場合（またはスキャンポリシーを [スキャンと削除] に設定した場合）、感染コンテンツに対するアクセスは拒否されます。この場合、フィルタは修復不能な感染が見つかったためにファイルに対するアクセスが拒否されることを示すためにユーザーに表示するメッセージを提供します。

Microsoft ISA Server はキャッシュデータが以前に Symantec AntiVirus Scan Engine によってスキャン済みかどうかについての情報を保守しません。キャッシュからのコンテンツは要求のたびに再スキャンされます。

SMTP フィルタのプロパティの設定

SMTP フィルタのプロパティを使うと SMTP フィルタ用のウイルススキャンの実装のしかたを指定できます。SMTP フィルタのプロパティを変更するには、Symantec AntiVirus for ISA Server SMTP Filter の設定オプションを表示する必要があります。

p.3-5 の「[Symantec AntiVirus for ISA Server SMTP Filter の設定](#)」を参照してください。

SMTP フィルタを設定すると次のことができます。

- SMTP フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine ごとの IP アドレスとポート番号を指定します。
p.3-6 の「[SMTP フィルタに使うスキャンエンジンの指定](#)」を参照してください。
- SMTP フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine に対する接続をテストします。
p.3-9 の「[SMTP フィルタ用のスキャンエンジンの接続をテスト](#)」を参照してください。
- スキャンエンジンが利用不能な場合に SMTP トラフィックを遮断します。
p.3-9 の「[スキャンエンジンが利用不能な場合の SMTP トラフィックの遮断](#)」を参照してください。
- 形式不良な MIME メッセージを遮断します。
p.3-10 の「[形式不良な MIME メッセージの遮断](#)」を参照してください。
- SMTP フィルタスキャンポリシーを設定します。
p.3-11 の「[SMTP スキャンポリシーの設定](#)」を参照してください。
- スキャンするファイルの種類を指定します。
p.3-12 の「[SMTP フィルタの場合にスキャンするファイルの指定](#)」を参照してください。

ウイルススキャンが起きるためには SMTP フィルタを有効にする必要があります。

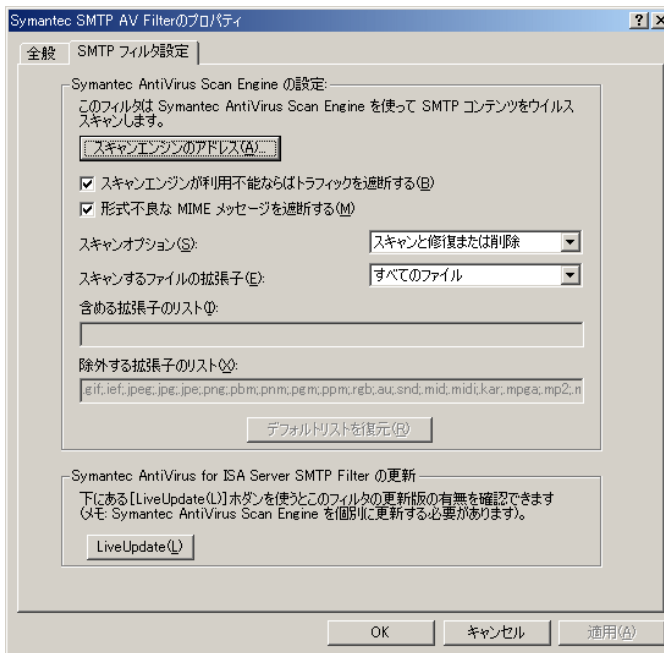
p.3-14 の「Symantec AntiVirus for ISA Server SMTP Filter の有効化」を参照してください。

Symantec AntiVirus for ISA Server SMTP Filter の設定

SMTP フィルタのプロパティを変更するには、Symantec AntiVirus for ISA Server SMTP Filter の設定オプションを表示する必要があります。

Symantec AntiVirus for ISA Server SMTP Filter を設定するには

- 1 ISA 管理コンソールの左ペインで適切な ISA サーバーまたは配列を選択して [拡張] を展開します。
- 2 [アプリケーションフィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server SMTP Filter] を右クリックしてから [プロパティ] を選択します。
- 4 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスで [SMTP フィルタ設定] ページを表示します。



SMTP フィルタに使うスキャンエンジンの指定

ウイルススキャンの対象になるファイルが SMTP フィルタからスキャンエンジンに渡るように、それぞれの Symantec AntiVirus Scan Engine が応答準備する IP アドレスとポート番号を表 3-1 次の表で示すとおり指定する必要があります。

表 3-1 SMTP フィルタ用のスキャンエンジンのアドレス情報

オプション	説明
IP アドレス	SMTP フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine ごとの IP アドレスを指定します。Symantec AntiVirus Scan Engine は Microsoft ISA サーバーと同じコンピュータまたはネットワーク上の異なるコンピュータにインストールできます。 詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。
ポート番号	ウイルススキャンの対象になるファイルを Symantec AntiVirus Scan Engine に渡す TCP/IP ポートの番号を指定する必要があります。ポート番号は Symantec AntiVirus Scan Engine の排他的な番号でなければなりません。Symantec AntiVirus Scan Engine のインストール中に指定したポート番号を使ってください。

Symantec AntiVirus Scan Engines をリストに追加またはリストから削除することはいつでもできます。SMTP フィルタ設定用に登録した Symantec AntiVirus Scan Engines は SMTP フィルタのみに対するスキャンサービスを提供します。Web トラフィックもスキャンしようとする場合には Web フィルタ設定用にもスキャンエンジンを登録する必要があります。これで Web と SMTP のトラフィックに基いてスキャンエンジンリソースを割り当てできます。

Symantec AntiVirus Scan Engine の IP アドレスとポート番号を入力した後で、正しく入力したことを確認するために接続をテストできます。

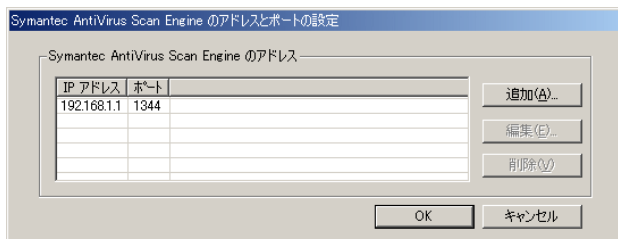
p.3-9 の「[SMTP フィルタ用のスキャンエンジンの接続をテスト](#)」を参照してください。

SMTP フィルタに使うスキャンエンジンの指定

スキャンエンジンをリストに追加したり、リストから削除したり、エントリを編集したりできます。

スキャンエンジンをリストに追加するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。



- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで [追加 (A)] をクリックします。
- 3 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスの [Symantec AntiVirus Scan Engine の IP] フィールドにスキャンエンジンの IP アドレスを入力します。

スキャンエンジンが動作するコンピュータに複数の IP アドレスがある場合には Symantec AntiVirus Scan Engine が応答準備するアドレスを指定します。Symantec AntiVirus Scan Engine が Microsoft ISA Server と同じコンピュータ上で動作する場合には 127.0.0.1 (ループバックインターフェース) を使います。

- 4 [Symantec AntiVirus Scan Engine のポート] フィールドにスキャンエンジンが応答準備するポートの番号を入力します。

ここで入力するポート番号は Symantec AntiVirus Scan Engine のインストール中に指定するポート番号と一致する必要があります。通信プロトコルとして ICAP を使うときの Symantec AntiVirus Scan Engine のデフォルトポートは 1344 番です。

- 5 [追加 (A)] をクリックします。
- 6 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。
- 7 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

スキャンエンジンをリストから削除するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。
- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで削除したいスキャンエンジンを選択します。
- 3 [削除 (V)] をクリックします。
- 4 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。
- 5 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

スキャンエンジンエントリを編集するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。
- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで編集したいスキャンエンジンを選択します。
- 3 [編集 (E)] をクリックします。
- 4 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスエントリに必要なだけ変更を加えます。
- 5 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。
- 6 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

SMTP フィルタ用のスキャンエンジンの接続をテスト

フィルタ用に登録したそれぞれの Symantec AntiVirus Scan Engine に対する接続をテキストできます SMTP filter. スキャンエンジンに対する接続をテストすると表 3-2 次の表で示す値のいずれかが返ります。

表 3-2 SMTP フィルタ用のスキャンエンジンのテスト値

戻り値	説明
正常に完了	スキャンエンジンに対する接続が正常に完了しました。
失敗	スキャンエンジンに対する接続が失敗しました。
有効なライセンスなし	スキャンエンジンに対する接続は正常に完了しましたがスキャンエンジンに有効なライセンスがありません。

SMTP フィルタ用のスキャンエンジンの接続をテストするには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。
- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで接続をテストしたいスキャンエンジンを選択します。
- 3 [編集 (E)] をクリックします。
- 4 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスで [設定のテスト (T)] をクリックします。
テストの結果が返って [テスト状態] ボタンの右に表示されます。
- 5 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで [OK] をクリックします。
- 6 [OK] をクリックします。

スキャンエンジンが利用不能な場合の SMTP トラフィックの遮断

Symantec AntiVirus Scan Engine によるスキャンが利用不能なときには SMTP トラフィックを遮断できます。SMTP トラフィックを遮断するオプションを選択した場合、フィルタがスキャンエンジンに交信できないとメッセージは拒否されます。メッセージは本来の送信先に転送されることなく、ウイルス対策スキャンエンジンが利用可能ではないことを示すメッセージが返ります。

スキャンエンジンが利用不能な場合に SMTP トラフィックを遮断するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [スキャンエンジンが利用不能ならばトラフィックを遮断する (B)] にチェックマークを付けます。
この機能はデフォルトで有効です。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

形式不良な MIME メッセージの遮断

コンピュータウイルスや悪質なプログラム（たとえば、自己メール送信するウイルス）は形式不良な電子メールメッセージを作成できます。歪んだ MIME メッセージは Symantec AntiVirus Scan Engine によって認識され、潜在的な感染ファイルを拒否するための基準として使われます。形式不良な MIME メッセージを遮断するオプションを設定すると、メッセージは本来の送信先に転送されることなくメッセージが拒否されたことを示すエラーメッセージが返ります。

形式不良な MIME メッセージを遮断するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページで [形式不良な MIME メッセージを遮断する (M)] にチェックマークを付けます。
この機能はデフォルトで有効です。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

SMTP スキャンポリシーの設定

感染ファイルが見つかったときに Symantec AntiVirus for ISA Server でできる処理は次のいずれかです。

- スキャンとログ記録: 感染ファイルに対するアクセスを許可して感染を記録するログエントリを生成します (が感染ファイルに対しては何もしません)。
- スキャンと削除: 修復を試みることなくすべての感染ファイルを削除してログエントリを生成します。
- スキャンと修復または削除: 感染ファイルの削除を試みます。修復不能な感染ファイルの最上位レベルに対するアクセスを拒否し、アーカイブファイルから修復不能なファイルを削除します。

メモ MIME エンコードメッセージに入っている感染添付ファイル (スキャンポリシーを [スキャンと削除] に設定しているか [スキャンと修復または削除] に設定していてファイルが修復不能であるために) 削除しなければならない場合には、削除したファイルは受信者にウイルスが入っていたファイルを削除したことを知らせるテキストファイル (deleted.txt) に置き換わります。

SMTP スキャンポリシーを設定するには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページにある [スキャンオプション (S)] リストで Symantec AntiVirus for ISA Server による感染ファイルの扱い方を選択します。

デフォルト設定は [スキャンと修復または削除] です。

- 2 変更を加え終わったら [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

メモ スキャンしたファイルの処置のしかたについては Symantec AntiVirus Scan Engine の設定よりも SMTP フィルタスキャンポリシーの設定が優先されます。スキャンポリシー情報は ICAP ヘッダー経由で SMTP フィルタから Symantec AntiVirus Scan Engine に直接提供されます。スキャンエンジンは ICAP ヘッダーにある情報を使ってスキャンしたファイルの処置を決定します。

SMTP フィルタの場合にスキャンするファイルの指定

スキャンしたいファイルの拡張子を含めるリストを使って) 指定またはスキャンしたくないファイルの拡張子(除外リストを使って) 指定することによってスキャンするファイルの種類を制御するか、または拡張子にかかわらずすべての種類のファイルのスキャンできます。Symantec AntiVirus for ISA Server SMTP Filter はデフォルトでは拡張子にかかわらずすべてのファイルのスキャンする設定になっています。

SMTP フィルタで除外リストにある拡張子が付くファイルを除くすべてのファイルのスキャンする設定にしたい場合、Symantec AntiVirus for ISA Server に付属のデフォルトの除外リストを利用できます。デフォルトの除外リストにはウイルスがいそうな種類のファイルの拡張子のみが入っていますが、このリストは編集できます。

定義による含めるリストや除外リストに入っていない種類のファイルもあるので新種のウイルスが常に検出されるとはかぎりません。拡張子にかかわらずすべてのファイルのスキャンするのが最も安全な設定ですが、そうするとリソース要求が増えます。たとえ通常は含めるリストまたは除外でファイルの種類を制御するとしてもウイルスアウトブレイク中にはすべてのファイルのスキャンするのが安全です。

警告 含めるリストを使ってスキャンするファイルの種類を制御するのは最も安全性の低い設定です。含めるリストで具体的に指定するファイルしかスキャンされないからです。つまり、含めるリストを使うとスキャンしないファイルの拡張子はほとんど無数に近くなります。このような理由により含めるリストは事前設定がありませんが、スキャンするファイルの種類を限定したい場合には含めるリストを編集できます。

スキャンするファイルの種類についてはSymantec AntiVirus Scan Engineの設定よりも SMTP フィルタ設定の設定が優先されます。スキャンするファイルの種類についての情報は ICAP ヘッダー経由で SMTP フィルタから Symantec AntiVirus Scan Engine に直接提供されます。

SMTP メッセージは MIME エンコードなのでフィルタはファイルの種類を判断を開始しようとはしません。フィルタは単純に Symantec AntiVirus Scan Engine に対するすべての SMTP トラフィックを解析しします。スキャンエンジンはアーカイブファイルを分解してメッセージの部分を(添付ファイルやアーカイブファイルに入っている個々のファイルを含めて)スキャンするときに ICAP ヘッダーに入っている情報を使ってどのフィルタをスキャンするかを判断します。

SMTP フィルタの場合にスキャンするファイルの指定

拡張子にかかわらずすべてのファイルのスキャンするか、またはスキャンしたい（またはしたくない）ファイルの拡張子を指定することによってどの種類のファイルのスキャンするかを制御できます。

拡張子にかかわらずすべてのファイルのスキャンするには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [すべてのファイル] を選択します。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

除外リストにある拡張子が付くファイルを除くすべてのファイルのスキャンするには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [除外リストにある項目を除くすべて] を選択します。
- 2 [除外する拡張子のリスト(X)] を編集してスキャンしたくないファイルを追加またはスキャンしたいファイルを削除します。
リストでは拡張子ごとにピリオド (.) を付けます。拡張子ごとをセミコロンで区切って（たとえば、.com;.doc;.bat というように）列記します。拡張子がないファイルを除くには 2 つのセミコロンを続けて（たとえば、.com;.exe;; というように）使います。
- 3 デフォルトリストを復元するには [デフォルトリストを復元 (R)] をクリックします。
- 4 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

含めるリストにある拡張子が付くファイルのみをスキャンするには

- 1 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [SMTP フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [含めるリストにある項目のみ] を選択します。
- 2 [含める拡張子のリスト (I)] を編集してスキャンしたいファイルを追加またはスキャンしたくないファイルを削除します。
含めるリストはデフォルトでは空白です。リストでは拡張子ごとにピリオド (.) を付けます。拡張子ごとをセミコロンで区切って (たとえば、.com;.doc;.bat というように) 列記します。拡張子がないファイルをスキャンするには 2 つのセミコロンを続けて (たとえば、.com;.exe;; というように) 使います。
- 3 デフォルトリストを復元するには [デフォルトリストを復元 (R)] をクリックします。
- 4 変更を加え終わったら [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

Symantec AntiVirus for ISA Server SMTP Filter の有効化

Microsoft ISA サーバーを使うと必要に応じて Symantec AntiVirus for ISA Server SMTP Filter の有効と無効を切り替えできます。フィルタはデフォルトで有効になります。フィルタが無効な場合、ウイルススキャンは起きません。

Symantec AntiVirus for ISA Server SMTP Filter を有効にするには

- 1 ISA 管理コンソールの左ペインで適切な ISA サーバーまたは配列を選択して [拡張] を展開します。
- 2 [アプリケーションフィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server SMTP Filter] を右クリックしてから [プロパティ] を選択します。
- 4 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスの [全般] ページで [このフィルタを有効にする] にチェックマークを付けます。
- 5 [OK] をクリックします。

Web フィルタのプロパティの設定

Web フィルタのプロパティを使うと Web フィルタ用のウイルススキャンの実装のしかたを指定できます。Web フィルタのプロパティを変更するには、Symantec AntiVirus for ISA Server Web Filter の設定オプションを表示する必要があります。

p.3-16 の「[Symantec AntiVirus for ISA Server Web Filter の設定](#)」を参照してください。

Web フィルタを設定すると次のことができます。

- Web フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine ごとの IP アドレスとポート番号を指定します。
p.3-17 の「[Web フィルタの使うスキャンエンジンの指定](#)」を参照してください。
- Web フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine に対する接続をテストします。
p.3-20 の「[Web フィルタ用のスキャンエンジンの接続のテスト](#)」を参照してください。
- スキャンエンジンが利用不能な場合に Web トラフィックを遮断します。
p.3-21 の「[スキャンエンジンが利用不能な場合の Web トラフィックの遮断](#)」を参照してください。
- ブラウザの最適化を有効にします。
p.3-21 の「[ブラウザコンフォーティング](#)」を参照してください。
- Web フィルタスキャンポリシーを設定します。
p.3-22 の「[Web スキャンポリシーの設定](#)」を参照してください。
- スキャンするファイルの種類を指定します。
p.3-23 の「[Web フィルタの場合にスキャンするファイルの指定](#)」を参照してください。
- ある種の MIME をスキャンするのを防止します。
p.3-25 の「[ある種の MIME をスキャンから除外する](#)」を参照してください。

ウイルススキャンが起きるためには Symantec AntiVirus for ISA Server Web Filter が有効になっていて HTTP リダイレクトフィルタを適切に設定しておく必要があります。

p.3-26 の「[Symantec AntiVirus for ISA Server Web Filter の有効化](#)」を参照してください。

p.3-26 の「[HTTP リダイレクタフィルタの設定](#)」を参照してください。

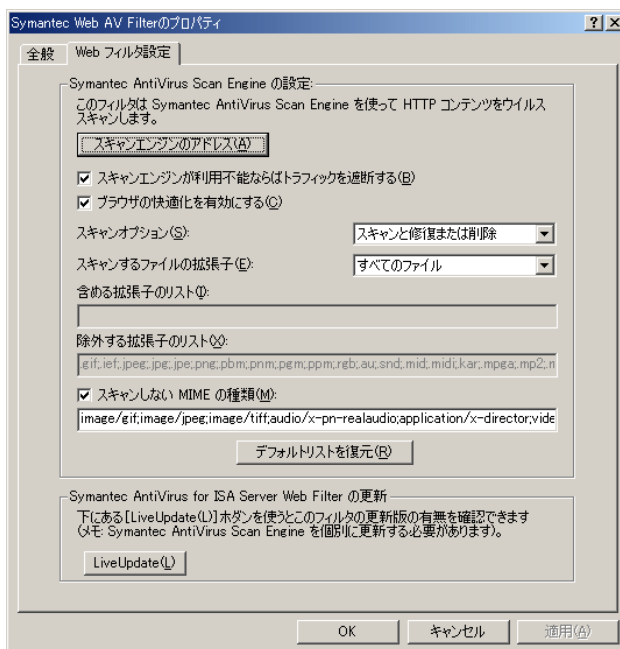
Symantec AntiVirus for ISA Server Web Filter の設定

Web フィルタのプロパティを変更するには、Symantec AntiVirus for ISA Server Web Filter の設定オプションを表示する必要があります。

Symantec AntiVirus for ISA Server Web Filter を設定するには

- 1 ISA 管理コンソールの左ペインで適切な ISA サーバーまたは配列を選択して [拡張] を展開します。
- 2 [Web フィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server Web Filter] を右クリックしてから [プロパティ] を選択します。

- 4 [Symantec Web AV Filter のプロパティ] ダイアログボックスで [Web フィルタ設定] ページを表示します。



Web フィルタの使うスキャンエンジンの指定

ウイルススキャンの対象になるファイルが Web フィルタからスキャンエンジンに渡るように、それぞれの Symantec AntiVirus Scan Engine が応答準備する IP アドレスとポート番号を表 3-3 次の表に示すとおり指定する必要があります。

表 3-3 Web フィルタ用のスキャンエンジンのアドレス情報

オプション	説明
IP アドレス	Web フィルタ用のスキャンサービスを提供する Symantec AntiVirus Scan Engine ごとの IP アドレスを指定します。Symantec AntiVirus Scan Engine は Microsoft ISA サーバーと同じコンピュータまたはネットワーク上の異なるコンピュータにインストールできます。 詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

表 3-3 Web フィルタ用のスキャンエンジンのアドレス情報

オプション	説明
ポート 番号	ウイルススキャンの対象になるファイルを Symantec AntiVirus Scan Engine に渡す TCP/IP ポートの番号を指定する必要があります。ポート 番号は Symantec AntiVirus Scan Engine の排他的な番号でなければなりません。Symantec AntiVirus Scan Engine のインストール中に指定したポート 番号を使ってください。

Symantec AntiVirus Scan Engines をリストに追加またはリストから削除することはいつでもできます。Web フィルタ設定用に登録した Symantec AntiVirus Scan Engines は Web フィルタのみに対するスキャンサービスを提供します。SMTP トラフィックもスキャンしようとする場合には SMTP フィルタ設定用にもスキャンエンジンを登録する必要があります。これで Web と SMTP のトラフィックに基いてスキャンエンジンリソースを割り当てできます。

Symantec AntiVirus Scan Engine の IP アドレスとポート番号を入力した後で、正しく入力したことを確認するために接続をテストできます。

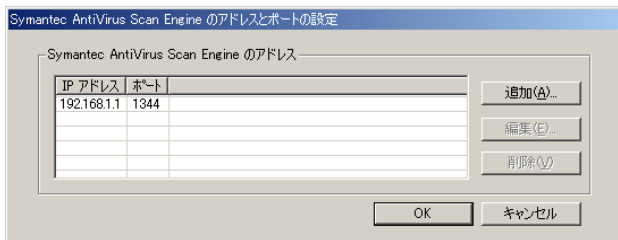
p.3-20 の「[Web フィルタ用のスキャンエンジンの接続のテスト](#)」を参照してください。

Web フィルタに使うスキャンエンジンの指定

スキャンエンジンをリストに追加したり、リストから削除したり、エントリを編集したりできます。

スキャンエンジンをリストに追加するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。



- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで [追加 (A)] をクリックします。

- 3 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスの [Symantec AntiVirus Scan Engine の IP] フィールドにスキャンエンジンの IP アドレスを入力します。

スキャンエンジンが動作するコンピュータに複数の IP アドレスがある場合には Symantec AntiVirus Scan Engine が応答準備するアドレスを指定します。Symantec AntiVirus Scan Engine が Microsoft ISA Server と同じコンピュータ上で動作する場合には 127.0.0.1 (ループバックインターフェース) を使います。

- 4 [Symantec AntiVirus Scan Engine のポート] フィールドにスキャンエンジンが応答準備するポートの番号を入力します。

ここで入力するポート番号は Symantec AntiVirus Scan Engine のインストール中に指定するポート番号と一致する必要があります。通信プロトコルとして ICAP を使うときの Symantec AntiVirus Scan Engine のデフォルトポートは 1344 番です。

- 5 [追加 (A)] をクリックします。

- 6 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。

- 7 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

スキャンエンジンをリストから削除するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。

- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで削除したいスキャンエンジンを選択します。

- 3 [削除 (V)] をクリックします。

- 4 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。

- 5 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

スキャンエンジンエントリを編集するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。
- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで編集したいスキャンエンジンを選択します。
- 3 [編集 (E)] をクリックします。
- 4 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスエントリに必要なだけ変更を加えます。
- 5 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスで変更を加え終わったら [OK] をクリックします。
- 6 [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

Web フィルタ用のスキャンエンジンの接続のテスト

Web フィルタ用に登録したそれぞれの Symantec AntiVirus Scan Engine に対する接続をテストできます。スキャンエンジンに対する接続をテストすると表 3-4 次の表に示す値のいずれかが返ります。

表 3-4 Web フィルタ用のスキャンエンジンのテスト値

戻り値	説明
正常に完了	スキャンエンジンに対する接続が正常に完了しました。
失敗	スキャンエンジンに対する接続が失敗しました。
有効なライセンスなし	スキャンエンジンに対する接続は正常に完了しましたがスキャンエンジンに有効なライセンスがありません。

Web フィルタ用のスキャンエンジンの接続をテストするには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンエンジンのアドレス (A)] をクリックします。

- 2 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスの [Symantec AntiVirus Scan Engine のアドレス] リストで接続をテストしたいスキャンエンジンを選択します。
- 3 [編集 (E)] をクリックします。
- 4 [Symantec AntiVirus Scan Engine の IP とポート] ダイアログボックスで [設定のテスト (T)] をクリックします。
テストの結果が返って [テスト状態] ボタンの右に表示されます。
- 5 [Symantec AntiVirus Scan Engine のアドレスとポートの設定] ダイアログボックスでコネクタをテストし終わったら [OK] をクリックします。
- 6 [OK] をクリックします。

スキャンエンジンが利用不能な場合の Web トラフィックの遮断

Symantec AntiVirus Scan Engine によるスキャンが利用不能なときには Web トラフィックを遮断できます。Web トラフィックを遮断するオプションを選択した場合、フィルタがスキャンエンジンに交信できないとファイルに対するは拒否されます。要求側のユーザーにはウイルス対策スキャンエンジンが利用可能ではないことを示すメッセージが表示されます。

Web が利用不能な場合の Web トラフィックを遮断するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンエンジンが利用不能ならばトラフィックを遮断する (B)] にチェックマークを付けます。
この機能はデフォルトで有効です。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

ブラウザの快適化

ファイルをスキャンできるようにするにはファイル全体をダウンロードする必要があります。大きいファイルを Web からダウンロードしてウイルススキャンするときには、スキャンが完了する前にブラウザが時間切れになることがあります。ブラウザの快適化が有効なときには、この期間中にブラウザが時間切れにならないように少量のデータがブラウザに渡ります。ブラウザの快適化はデフォルトでは無効です。

ブラウザの快適化を有効にするには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [ブラウザの快適化を有効にする (C)] にチェックマークを付けます。
この機能はデフォルトでは無効です。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

Web スキャンポリシーの設定

感染ファイルが見つかったときに Symantec AntiVirus for ISA Server でできる処理は次のいずれかです。

- スキャンとログ記録: 感染ファイルに対するアクセスを許可して感染を記録するログエントリを生成しますが感染ファイルに対しては何もしません。
- スキャンと削除: 感染ファイルの最上位レベルに対するアクセスを (修復を試みることなく) 拒否します。アーカイブファイルから感染ファイルを削除します。
- スキャンと修復または削除: 感染ファイルの削除を試みます。修復不能な感染ファイルの最上位レベルに対するアクセスを拒否し、アーカイブファイルから修復不能なファイルを削除します。

Web スキャンポリシーを設定するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページにある [スキャンオプション (S)] リストで Symantec AntiVirus for ISA Server による感染ファイルの扱い方を選択します。
デフォルト設定は [スキャンと修復または削除] です。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

Web フィルタの場合にスキャンするファイルの指定

スキャンしたいファイルの拡張子を（含めるリストを使って）指定またはスキャンしたくないファイルの拡張子を（除外リストを使って）指定することによってスキャンするファイルの種類を制御するか、または拡張子にかかわらずすべての種類のファイルをスキャンできます。Symantec AntiVirus for ISA Server Web Filter はデフォルトでは拡張子にかかわらずすべてのファイルをスキャンする設定になっています。

Web フィルタで除外リストにある拡張子が付くファイルを除くすべてのファイルをスキャンする設定にしたい場合、Symantec AntiVirus for ISA Server に付属のデフォルトの除外リストを利用できます。デフォルトの除外リストにはウイルスが似そうな種類のファイルの拡張子のみが入っていますが、このリストは編集できます。

定義による含めるリストや除外リストに入っていない種類のファイルもあるので新種のウイルスが常に検出されるとはかぎりません。拡張子にかかわらずすべてのファイルをスキャンするのが最も安全な設定ですが、そうするとリソース要求が増えます。たとえ通常は含めるリストまたは除外でファイルの種類を制御するとしてもウイルスアウトブレイク中にはすべてのファイルをスキャンするのが安全です。

警告 含めるリストを使ってスキャンするファイルの種類を制御するのは最も安全性の低い設定です。含めるリストで具体的に指定するファイルしかスキャンされないからです。つまり、含めるリストを使うとスキャンしないファイルの拡張子はほとんど無数に近くなります。このような理由により含めるリストは事前設定がありませんが、スキャンするファイルの種類を限定したい場合には含めるリストを編集できます。

Web フィルタ設定のスキャンするファイルの種類についての設定は Symantec AntiVirus Scan Engine の設定よりも優先されます。Symantec AntiVirus の Web フィルタが HTTP 要求を受信すると、スキャンが必要かどうかを判断するためにスキャンするファイルの種類についての情報が最上位ファイルの種類に基づいて使われます。スキャンが必要な場合、コンテンツはスキャンの対象として ICAP 経由で Symantec AntiVirus Scan Engine に渡ります。スキャンするファイルの種類についての情報は ICAP ヘッダー経由で Symantec AntiVirus Scan Engine にも提供されます。スキャンエンジンはアーカイブファイルを分解して個々のファイルをスキャンするときにこの情報を使ってどのフィルタをスキャンするかを判断します。

Web フィルタの場合にスキャンするファイルの指定

拡張子にかかわらずすべてのファイルをスキャンするか、またはスキャンしたい（またはしたくない）ファイルの拡張子を指定することによってどの種類のファイルをスキャンするかを制御できます。

拡張子にかかわらずすべてのファイルをスキャンするには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [すべてのファイル] を選択します。
- 2 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

除外リストにある拡張子が付くファイルを除くすべてのファイルをスキャンするには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [除外リストにある項目を除くすべて] を選択します。
- 2 [除外する拡張子のリスト(X)] を編集してスキャンしたくないファイルを追加またはスキャンしたいファイルを削除します。
リストでは拡張子ごとにピリオド (.) を付けます。拡張子ごとをセミコロンで区切って（たとえば、.com;.doc;.bat というように）列記します。拡張子がないファイルを除外するには 2 つのセミコロンを続けて（たとえば、.com;.exe;; というように）使います。
- 3 デフォルトリストを復元するには [デフォルトリストを復元 (R)] をクリックします。
- 4 変更を加え終わったら [OK] をクリックします。
フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

含めるリストにある拡張子が付くファイルのみをスキャンするには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページにある [スキャンするファイルの拡張子] リストで [含めるリストにある項目のみ] を選択します。
- 2 [含める拡張子のリスト (I)] を編集してスキャンしたいファイルを追加またはスキャンしたくないファイルを削除します。

含めるリストはデフォルトでは空白です。リストでは拡張子ごとにピリオド (.) を付けます。拡張子ごとをセミコロンで区切って (たとえば、.com;.doc;.bat というように) 列記します。拡張子がないファイルをスキャンするには 2 つのセミコロンを続けて (たとえば、.com;.exe;; というように) 使います。

- 3 デフォルトリストを復元するには [デフォルトリストを復元 (R)] をクリックします。
- 4 変更を加え終わったら [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

ある種の MIME をスキャンから除外する

ウイルススキャンが起きるためにはファイル全体をダウンロードする必要があります。定義上、ある種の MIME (たとえば、ストリーム媒体) には始まりや終わりの定義がなくスキャンできません。このようにスキャンから除外したい MIME の種類を指定できます。スキャンから除外する MIME の種類のデフォルトリストには適切な MIME の種類が入っていますが、必要に応じてリストを編集できます。

ある種の MIME をスキャンから除外するには

- 1 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [Web フィルタ設定] ページで [スキャンしない MIME の種類 (M)] にチェックマークを付けます。
- 2 [スキャンしない MIME の種類 (M)] のリストを編集してスキャンしたくない MIME の種類を追加またはスキャンしたい MIME の種類を削除します。

MIME の種類ごとをセミコロン (;) で区切ります。

- 3 デフォルトリストを復元するには [デフォルトリストを復元 (R)] をクリックします。
- 4 変更を加え終わったら [OK] をクリックします。

フィルタ設定に加えた変更を Microsoft ISA サーバーが登録するには約 1 分ほどかかります。通知処理が終わるまで待ちたくない場合には Microsoft ISA のサービスを停止して再開してください。

Symantec AntiVirus for ISA Server Web Filterの有効化

Microsoft ISA Server を使うと Symantec AntiVirus for ISA Server Web Filter 必要に応じての有効と無効を切り替えられます。フィルタはデフォルトで有効になります。フィルタが無効な場合、ウイルススキャンは起きません。

Symantec AntiVirus for ISA Server Web Filter を有効にするには

- 1 ISA 管理コンソールの左ペインで適切な ISA サーバーまたは配列を選択して [拡張] を展開します。
- 2 [Web フィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server Web Filter] を右クリックしてから [プロパティ] を選択します。
- 4 [Symantec Web AV Filter のプロパティ] ダイアログボックスの [全般] ページで [このフィルタを有効にする] にチェックマークを付けます。
- 5 [OK] をクリックします。

HTTP リダイレクタフィルタの設定

Symantec AntiVirus for ISA Server Web Filter を使おうとする場合、Symantec AntiVirus の Web フィルタでフィルタ処理するための HTTP 要求がローカル Web プロキシを通してリダイレクトされるように ISA 管理コンソールを通して HTTP リダイレクタフィルタを設定する必要があります。

HTTP リダイレクタフィルタを設定するには

- 1 ISA 管理コンソールの左ペインで [拡張] を展開します。
- 2 [アプリケーションフィルタ] を選択します。
- 3 右ペインで [HTTP redirector filter] を右クリックしてから [プロパティ] を選択します。

[Symantec Web AV Filter のプロパティ] ダイアログボックスの [全般] ページで [このフィルタを有効にする] にチェックマークを付けます。

[OK] をクリックします。

- 4 [オプション] ページで [ローカル Web Proxy サービスにリダイレクトする] を選択します。
- 5 [OK] をクリックします。

Symantec AntiVirus for ISA Server の警告とログ記録

この章には次の大見出しがあります。

- [Symantec AntiVirus for ISA Server のログ記録と警告について](#)
- [警告について](#)
- [ログ記録について](#)

Symantec AntiVirus for ISA Server のログ記録と警告について

Symantec AntiVirus for ISA Server コネクタと Symantec AntiVirus Scan Engine は個別のコンポーネントであり潜在的に異なるコンピュータにインストールできるので、2つのコンポーネントで個別のログ記録と警告の機能が利用可能です。

Symantec AntiVirus for ISA Server コネクタに対する警告は ISA サーバーの警告サブシステムを通して扱われ、イベントはアプリケーションイベントログに記録されます。Symantec AntiVirus for ISA Server コネクタのインストール中にデフォルト警告を設定するオプションを選択すると、選択したイベントに対するログ記録と警告が自動的に設定されます。インストール時にデフォルト警告を設定しない場合、ISA の管理ツールを使って記録したい警告やログエントリを手動で設定する必要があります。

メモ Symantec AntiVirus for ISA Server のイベントは標準 ISA レポートには利用可能ではありません。

Symantec AntiVirus Scan Engine も総合的なログ記録オプションを備えています。Symantec AntiVirus Scan Engine でログ記録を設定するときには、特にスキャンエンジンを Microsoft ISA サーバーと同じコンピュータ上で実行するのであれば Symantec AntiVirus for ISA Server コネクタを通して直接利用可能なログ記録と警告の機能を考慮してください。

警告について

Symantec AntiVirus for ISA Server コネクタのインストール中には、デフォルト警告を設定するオプションを選択できます。デフォルト警告を設定あるオプションを選択すると、選択したイベントに対する警告が ISA サーバーの警告サブシステムで自動的に設定されます。インストール時にデフォルト警告を設定しない場合、標準 ISA 管理ツールを使って記録したい警告を設定する必要があります。

インストール時にデフォルト警告を設定するオプションを選択すると、Symantec AntiVirus for ISA Server は表 4-1 次の表に示すイベントに対する警告を設定します。(1 つしかフィルタをインストールしなかった場合にはそのフィルタに適用されるイベントのみが設定されます。)

表 4-1 Symantec AntiVirus for ISA Server の警告

警告	説明
SMTP AV フィルタ : すべてのエンジン接続失敗	Symantec AntiVirus for ISA Server SMTP Filter を使うためのすべての Symantec AntiVirus Scan Engine に対する接続が失敗しました。
SMTP AV フィルタ : 設定をロードできません	Symantec AntiVirus for ISA Server SMTP Filter の設定をロードできません。
SMTP AV フィルタ : 設定変更	Symantec AntiVirus for ISA Server SMTP Filter に設定変更が加われました。
SMTP AV フィルタ : エンジン接続失敗	Symantec AntiVirus for ISA Server SMTP Filter を使うための Symantec AntiVirus Scan Engine に対する接続が失敗しました。
SMTP AV フィルタ : エンジンからのエラー	Symantec AntiVirus for ISA Server SMTP Filter がスキャンエンジンからのエラーを受信しました。
SMTP AV フィルタ : フィルタ終了	Symantec AntiVirus for ISA Server SMTP Filter が終了しました。
SMTP AV フィルタ : フィルタ起動	Symantec AntiVirus for ISA Server SMTP Filter が起動しました。
SMTP AV フィルタ : フィルタを更新	Symantec AntiVirus for ISA Server SMTP Filter を更新しました。
SMTP AV フィルタ : 内部エラー	Symantec AntiVirus for ISA Server SMTP Filter の内部エラーが起きました。
SMTP AV フィルタ : 形式不良な MIME を検出	Symantec AntiVirus for ISA Server SMTP Filter が形式不良な MIME メッセージを検出しました。
SMTP AV フィルタ : 設定済みエンジンなし	Symantec AntiVirus for ISA Server SMTP Filter を使うために設定した Symantec AntiVirus Scan Engine がありません。

表 4-1 Symantec AntiVirus for ISA Server の警告

警告	説明
SMTP AV フィルタ : 違反を検出	<p>Symantec AntiVirus for ISA Server SMTP Filter が次のいずれかを検出しました。</p> <ul style="list-style-type: none"> ■ ウイルス ■ メールポリシー違反 (Symantec AntiVirus Scan Engine で選択する設定オプションに基づく) ■ コンテナ違反 (Symantec AntiVirus Scan Engine で選択する設定オプションに基づく) <p>メモ 警告テキストが示すのは違反を検出したことのみです。違反についてさらに詳しくは、アプリケーションイベントログのログエントリを参照してください。</p>
Web AV フィルタ : すべてのエンジン 接続失敗	Symantec AntiVirus for ISA Server Web Filter を使うためのすべての Symantec AntiVirus Scan Engine に対する接続が失敗しました。
Web AV フィルタ : 設定をロード できません	Symantec AntiVirus for ISA Server Web Filter の設定をロードできません。
Web AV フィルタ : 設定変更	Symantec AntiVirus for ISA Server Web Filter に設定変更が加われました。
Web AV フィルタ : エンジン 接続失敗	Symantec AntiVirus for ISA Server Web Filter を使うための Symantec AntiVirus Scan Engine に対する接続が失敗しました。
Web AV フィルタ : エンジンからのエラー	Symantec AntiVirus for ISA Server Web Filter がスキャンエンジンからのエラーを受信しました。
Web AV フィルタ : フィルタ 終了	Symantec AntiVirus for ISA Server Web Filter が終了しました。
Web AV フィルタ : フィルタ 起動	Symantec AntiVirus for ISA Server Web Filter が起動しました。
Web AV フィルタ : フィルタを 更新	Symantec AntiVirus for ISA Server Web Filter を更新しました。
Web AV フィルタ : 内部エラー	Symantec AntiVirus for ISA Server Web Filter の内部エラーが起きました。
Web AV フィルタ : 設定済みエンジンなし	Symantec AntiVirus for ISA Server Web Filter を使うために設定した Symantec AntiVirus Scan Engine がありません。

表 4-1 Symantec AntiVirus for ISA Server の警告

警告	説明
Web AV フィルタ : 違反を検出	Symantec AntiVirus for ISA Server Web Filter が次のいずれかを検出しました。 <ul style="list-style-type: none">■ ウイルス■ メールポリシー違反 (Symantec AntiVirus Scan Engine で選択する設定オプションに基づく)■ コンテナ違反 (Symantec AntiVirus Scan Engine で選択する設定オプションに基づく) <p>メモ 警告テキストが示すのは違反を検出したことのみです。違反についてさらに詳しくは、アプリケーションイベントログのログエントリを参照してください。</p>

メモ 場合によっては、警告テキストは起きた Symantec AntiVirus for ISA Server のイベントに関する具体的な情報のすべてを示しません。イベントについてのさらに詳しい情報はアプリケーションイベントログにある同じイベントのログエントリに見つかります。たとえば、違反の警告テキストは違反が検出されたことのみを示し、違反の種類は指定しません。さらに詳しい情報 (ウイルス、コンテナ違反、メールポリシー違反のいずれかなど) はアプリケーションイベントログにあるそのイベントのログエントリに見つかります。

ログ記録について

インストール時にデフォルト警告を設定するオプションを選択すると、Symantec AntiVirus for ISA Server のイベントのログ記録が自動的に設定されます。イベントは Microsoft ISA サーバーとして動作するコンピュータ上のアプリケーションイベントログに記録されます。イベントのデフォルトリストは表 4-1 にある [Symantec AntiVirus for ISA Server の警告](#) のデフォルトリストと同一です。

インストール時にデフォルト警告を設定しないと、Symantec AntiVirus for ISA Server のイベントは（手動で設定しないかぎり）アプリケーションイベントログに記録されません。

一般にイベントのログエントリには同じイベントに対する警告よりも詳しい情報が入ります。

場合によっては、警告テキストは起きた Symantec AntiVirus for ISA Server のイベントに関する具体的な情報のすべてを示しません。たとえば、違反の警告テキストは違反が検出されたことのみを示し、違反の種類は指定しません。さらに詳しい情報（ウイルス、コンテナ違反、メールポリシー違反のいずれかなど）を入手するにイベントのログエントリを使ってください。

メモ Symantec AntiVirus Scan Engine も総合的なログ記録オプションを備えています。Symantec AntiVirus Scan Engine でログ記録を設定するときには、Symantec AntiVirus for ISA Server コネクタを通して直接利用可能なログ記録と警告の機能を考慮してください。選択肢はスキャンエンジンを Microsoft ISA サーバーと同じコンピュータ上で実行するかどうか大きく依存する可能性があります。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

LiveUpdate の使い方

この章には次の大見出しがあります。

- [LiveUpdate について](#)
- [ウイルス定義ファイルについて](#)
- [Symantec AntiVirus Scan Engine 用のウイルス定義の更新](#)
- [LiveUpdate 経由の製品更新版の入手](#)

LiveUpdate について

シマンテック社の LiveUpdate 技術を使うと コンピュータ上にインストール済みのシマンテック製品のための利用可能な更新版や更新済みのウイルス定義を入手できます。LiveUpdate を実行すると LiveUpdate はインストールしてある製品の利用可能な更新版のリストを表示し、ユーザーはそのセッションで更新したい製品を選択できます。

Symantec AntiVirus for ISA Server の場合、LiveUpdate は 2 つの目的で使われます。

- ネットワークを新種のウイルスによる感染の危険から確実に守るために個別にインストールした Symantec AntiVirus Scan Engine 用の更新済みのウイルス定義を入手する
p.5-3 の「[Symantec AntiVirus Scan Engine 用のウイルス定義の更新](#)」を参照してください。
- Symantec AntiVirus for ISA Server の SMTP フィルタや Web フィルタの製品更新版を入手する
p.5-3 の「[LiveUpdate 経由の製品更新版の入手](#)」を参照してください。

ウイルス定義ファイルについて

シマンテック社の技術者は新種のウイルスを識別するとウイルスについての情報（ウイルスシグネチャ）をウイルス定義ファイルに格納します。ウイルス定義ファイルは Symantec AntiVirus 製品によって使われるウイルスを検出や除去するために必要な情報が入ったファイルです。ウイルス定義ファイルはシマンテック社によって少なくとも週に 1 回と新種のウイルスの脅威の発見時にいつでも提供され、自動 LiveUpdate 機能を通して更新されます。新しいウイルス定義ファイルが利用可能なときに LiveUpdate セッションを開始すると、LiveUpdate 技術は適切なファイルを自動的にダウンロードして適切な場所にインストールします。

p.5-3 の「[Symantec AntiVirus Scan Engine 用のウイルス定義の更新](#)」を参照してください。

Symantec AntiVirus Scan Engine 用のウイルス定義の更新

新種のウイルスに脅威に確実に対応するには Symantec AntiVirus for ISA Server に対してスキャンと修復のサービスを提供する Symantec AntiVirus Scan Engine を定期的に更新する必要があります。

Symantec AntiVirus Scan Engine は他の Symantec AntiVirus 製品のように LiveUpdate に登録されません。Symantec AntiVirus Scan Engine を Microsoft ISA Server や Symantec AntiVirus for ISA Server コネクタと同じコンピュータにインターフェースするときには、定期的なウイルス定義の更新版を入手するために Symantec AntiVirus Scan Engine の管理インターフェースを通して LiveUpdate を個別にスケジュール設定する必要があります。

警告 [Symantec SMTP AV Filter のプロパティ] または [Symantec Web AV Filter のプロパティ] のダイアログボックスで実行する LiveUpdate は Symantec AntiVirus Scan Engine のウイルス定義を更新しません。

Symantec AntiVirus Scan Engine をネットワーク上の異なるコンピュータで実行する場合、Symantec AntiVirus Scan Engine が動作するコンピュータ上で『Symantec AntiVirus Scan Engine 実装ガイド』に従って LiveUpdate をスケジュール設定する必要があります。複数のスキャンエンジンを実行しようとする場合、スキャンエンジンが動作するコンピュータごとに LiveUpdate をスケジュール設定する必要があります。

詳しくは『Symantec AntiVirus Scan Engine 実装ガイド』を参照してください。

LiveUpdate 経由の製品更新版の入手

Symantec AntiVirus for ISA Server コネクタの製品の更新版も LiveUpdate 経由で入手できます。LiveUpdate を実行すると LiveUpdate は Symantec AntiVirus for ISA Server (と同じコンピュータにインストールしてあって LiveUpdate に登録済みのその他のシマンテック製品) の更新版が利用可能かどうかを表示します。ユーザーはその LiveUpdate セッションでダウンロードしたい更新版を選択できます。

警告 [Symantec SMTP AV Filter のプロパティ] または [Symantec Web AV Filter のプロパティ] のダイアログボックスで実行する LiveUpdate は (たとえスキャンエンジンを Symantec AntiVirus for ISA Server コネクタと同じコンピュータにインストールしてあっても) Symantec AntiVirus Scan Engine のウイルス定義を更新しません。スキャンエンジンは他のシマンテック製品と同じようには LiveUpdate に登録されないので Symantec AntiVirus Scan Engine 用に個別に LiveUpdate をスケジュール設定する必要があります。

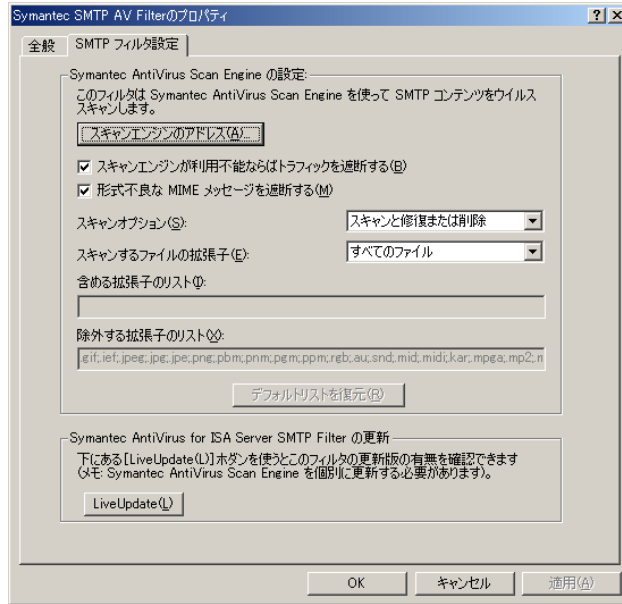
LiveUpdate 経由の製品更新版の入手

製品を更新するための LiveUpdate は [Symantec SMTP AV Filter のプロパティ] または [Symantec Web AV Filter のプロパティ] のいずれかのダイアログボックスで実行できます。

[Symantec SMTP AV Filter のプロパティ] ダイアログボックスで製品の更新版を入手するには

- 1 適切な ISA サーバーまたはアレイの ISA 管理コンソールの左ペインで [拡張] を展開します。
- 2 [アプリケーションフィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server SMTP Filter] を右クリックしてから [プロパティ] を選択します。

- 4 [Symantec SMTP AV Filter のプロパティ] ダイアログボックスで [SMTP フィルタ設定] ページを選択します。

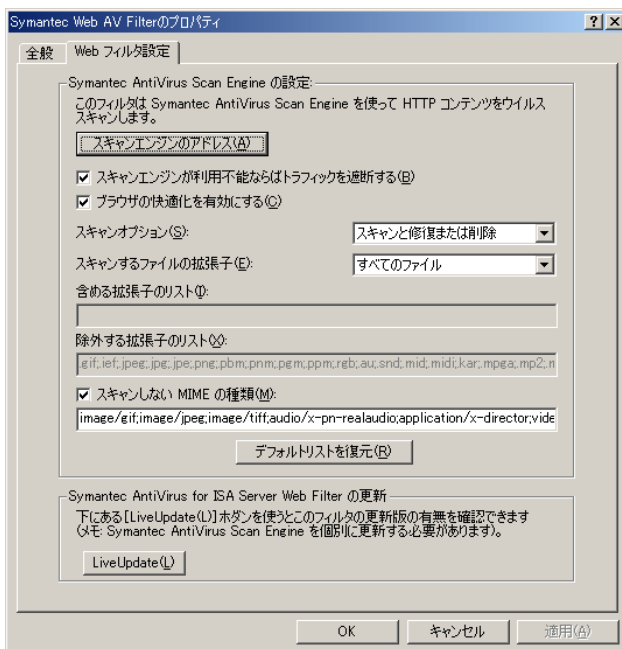


- 5 [Symantec AntiVirus for ISA Server SMTP Filter の更新] グループで [LiveUpdate(L)] をクリックします。
- 6 画面の指示に従って操作しながら LiveUpdate セッションを完了します。

[Symantec Web AV Filter のプロパティ] ダイアログボックスで製品の更新版を入手するには

- 1 適切な ISA サーバーまたはアレイの ISA 管理コンソールの左ペインで [拡張] を展開します。
- 2 [Web フィルタ] を選択します。
- 3 右ペインで [Symantec AntiVirus for Microsoft ISA Server Web Filter] を右クリックしてからドロップダウンリストで [プロパティ] を選択します。

- 4 [Symantec Web AV Filter のプロパティ] ダイアログボックスで [Web フィルタ設定] ページを表示します。



- 5 [Symantec AntiVirus for ISA Server Web Filter の更新] グループで [LiveUpdate(L)] をクリックします。
- 6 画面の指示に従って操作しながら LiveUpdate セッションを完了します。