

# Symantec™ Mail Security for SMTP

アンチウイルス、アンチスパムなどSMTPゲートウェイにおける包括的なメールセキュリティを確保

ITリソースの無駄な消費、生産性の低下、システムダウン、悪質なフィッシング詐欺による被害の発生、内部情報の漏えいなど、電子メールの利用に伴うセキュリティリスクはさらに増大しています。進化するウイルス、ワーム、スパム、DHA攻撃などのメールを媒介にした攻撃からの防御、メールコンテンツに対するコンプライアンスチェックなど、メールのセキュリティを包括的に確保することの重要性はますます高くなっています。

## 製品の概要

Symantec Mail Security for SMTPは、信頼と実績のあるシマンテックのアンチウイルスと業界をリードするBrightmailのアンチスパムをはじめとしたセキュリティ機能を提供します。Symantec Mail Security for SMTPは、メールファイアウォール、アンチウイルス、アンチスパム、コンテンツコンプライアンスなどのセキュリティ機能を多層的に配置することが可能であり、メールを媒介としたさまざまな攻撃からネットワークを保護するとともに、重要な情報の漏えい防止、ネットワークインフラに対する負担の低減を実現します。

### 〈キーポイント〉

- ゲートウェイでSMTPのトラフィックを監視。メールセキュリティの課題に対し、優れた機能を提供
  - NEW** メールファイアウォール
  - アンチスパム
  - アンチウイルス
  - コンテンツコンプライアンス
- Webブラウザを使用して、ローカル/リモートを問わずに容易に管理メールサーバー上で動作させることが可能。既存のシステムに容易に導入することができます
- NEW** メールに添付されたスパイウェアおよびアドウェアの検出機能を強化
- 充実したレポート機能
- グローバル規模の情報収集にもとづく、信頼のコンテンツアップデート

## 製品の特長とベネフィット

### 複数のセキュリティ機能を提供

Symantec Mail Security for SMTPは、複数のセキュリティ機能を多層的に配置することにより、電子メールに対するさまざまな脅威や課題に対し、高度なセキュリティを確保することができます。

### メールファイアウォール (NEW)

SMTP接続の解析やリストをもとに、内蔵されたMTAと連携して通信を制御。メールを媒介とした攻撃をフィルタリングプロセスの前段階でブロックするとともに、真に必要なメールトラフィックのスルーレートを向上することができます。

[メールファイアウォール機能の例]

- インバウンドのSMTP接続を分析し、悪意があると識別されたメールホストとの接続レートを制御。また、スパムメールやウイルスによる攻撃の可能性を検知
- オープンプロキシを使用した送信者、スパムメールの送信元と疑わしき送信者、安全な送信者に関するリストをもとに、SMTP接続の可否を制御
- SPF (Sender Policy Framework) レコードを使用してメールを認証
- DHA (Directory Harvest Attack) 攻撃をブロックしてメールサーバーを保護

### アンチスパム

業界をリードするBrightmailテクノロジーによる技術を駆使し、マルチレイヤのフィルタリングによってスパムメールの評価と識別を高い精度で行います。グローバルに展開するオペレーションセンターが、300万以上のメールアドレスとドメインで構成されたハニーポットネットワークを使用してスパム情報を収集し、24時間体制で解析。それにもとづき、Symantec Mail Security for SMTPのスパムフィルタを更新します。管理者は、最新情報にもとづいたスパムフィルタリングを、高精度・低負荷で行うことができます。

[アンチスパム機能の例]

- レピュテーションサービスが提供するデータにもとづき、SMTP接続の可否を制御
- 各種のシグネチャを使用して効率良く、確実にスパムメールを検出
  - スパム送信者が誘導を意図するWebサイトのURL
  - ランダム化やHTMLの使用によりフィルタリングの回避を意図するスパムを検出
  - メール本文やメールヘッダのハッシュ値をベースにしたシグネチャ
  - 画像ファイルなどのMIME添付ファイルをベースとしたシグネチャ

- スпамメールのコンテンツやヘッダーに見られる傾向や共通性などの特徴にもとづき、ヒューリスティックに検出
- スпамメールの言語を識別。英語、日本語、イタリア語、オランダ語、韓国語、スペイン語、中国語、ドイツ語、フランス語、ポルトガル語、ロシア語といった各国の言語に対応

### アンチウイルス

グローバル規模で多数のユーザーに使用されている信頼と実績のあるシマンテックのアンチウイルスエンジンが、メール本文、添付ファイルをスキャン。メールに潜むウイルスやワームなどの悪意のあるコードを検出し、削除します。

- ウィルス定義ファイルとスキャンエンジンの更新を、システムの再起動やスキャンの中断を行うことなく自動的に実行 (NAVEX技術)
- ヒューリスティックなスキャンにより、新種/亜種などの未知のウイルスも検出。ヒューリスティックのレベルは調整可能
- メールを大量に送信するタイプのワームと、それにより生成されたメールも検出して削除

### コンテンツコンプライアンス

コンテンツフィルタを使用し、取り扱いに注意を要するコンテンツを含むメールの送受信をコントロール。情報漏えいの防止、メール利用上のポリシー遵守の徹底、法的なリスクの発生を抑止に役立てることができます。

[コンテンツフィルタリング機能の例]

- フィルタリングで利用可能な項目の例  
FROM/TO/CC/BCC、ヘッダー、件名、本文中の言葉/フレーズ、添付ファイル (ファイル名、拡張子、サイズ、MIMEタイプなど)、サイズ
- フィルタリングで使用する言葉を辞書に登録、または外部からインポート

### Symantec Security Responseによる信頼のバックアップ

Symantec Security Responseは、グローバル規模で、ウイルスやワームをはじめ、悪意のあるプログラム、不正侵入の手法、OSやアプリケーションの脆弱性とそれを利用した攻撃方法、スパムメールなどに関する情報収集と解析、また、それにもとづくシマンテック製品のバックアップを行っています。そして、インターネット上における脅威の動向を365日24時間体制で監視し、情報発信、ソリューションとサポートを世界中のユーザーに提供しています。

### システム要件

#### Symantec™ Mail Security 5.0 for SMTP

##### Windows

- Windows 2000 Server (SP4)
- Windows Server 2003 (SP1)
- 1 GB 以上のメモリー (2 GB 以上を推奨)
- 512 MB 以上のハードディスク空き容量 (2 GB 以上を推奨)

##### Solaris

- Solaris 9,10 (SPARCプラットフォーム)
- 1 GB 以上のメモリー (2 GB 以上を推奨)
- 512 MB 以上のハードディスク空き容量 (2 GB 以上を推奨)

##### Linux

- Red Hat Linux ES/AS 3.0 (Update 5)
- 1 GB 以上のメモリー (2 GB 以上を推奨)
- 512 MB 以上のハードディスク空き容量 (2 GB 以上を推奨)

##### 管理コンソール用ブラウザ

- Microsoft Internet Explorer 6.0
- Firefox 1.5以降

### 製品に関する最新の情報

シマンテックのWebサイトをご覧ください。

<http://www.symantec.com/region/jp/enterprise/index.html>