

Symantec™ Mail Security for Microsoft® Exchange

Microsoft Exchangeによって実現されるメッセージングコラボレーション環境において、さまざまな脅威からメールを保護

製品の概要

ウイルス対策、スパムメール対策、コンテンツフィルタリングの機能を統合したSymantec Mail Security for Microsoft Exchangeは、メールのウイルス対策に加え、スパムメール対策、機密情報の漏えい防止、メール利用上の企業モラルの維持など、電子メールの利用全般に対するセキュリティの確保をMicrosoft Exchange環境において実現します。

＜キーポイント＞

- ウイルス/スパイウェア対策、スパムメール対策、コンテンツフィルタリングの機能を統合した、Microsoft Exchange環境のための包括的なメールセキュリティ
- 未知のウイルスにも対処可能な信頼性が高いウイルススキャン。さまざまなエンコード/圧縮形式のファイルに潜むウイルスを検出し、ファイルを修復（多重圧縮にも対応）
- より高い精度でスパムメールを検出でき、スパム対策をさらに省力化することができるSymantec Premium AntiSpamを利用可能（オプション）
- メール本文の内容をフィルタリングすることにより、不適切なコンテンツや情報漏えいを防止
- **NEW** 管理およびレポーティング機能の強化
- **NEW** Veritas ClusterエージェントおよびWindows Clusterサポートによる可用性の向上
- Symantec Enterprise Vaultとの連携により、メールの検索性、管理性を向上
- 世界をリードするインターネットセキュリティの専門機関、Symantec Security Responseによる信頼の支援体制

製品の特長

さまざまなウイルスの脅威からMicrosoft Exchangeのメッセージを保護

- 拡張性の高いNAVEX技術により、ウイルス定義ファイルと一括してスキャンエンジン自体も更新。LiveUpdate機能によりスケジュールに従って自動的に更新可能で、サービスの停止やシステムの再起動は必要ありません。ウイルス定義ファイルは差分だけをダウンロードできるため、更新に要するネットワークの負荷は最小限に抑えることができます。
- Bloodhound技術によるヒューリスティックなスキャンが、新種や亜種などの未知のウイルスも検出します。未知のウイルスに感染したファイルが検出された場合には、暗号化して隔離することにより2次感染を防ぎます（検疫機能）。
- 通常ウイルス定義ファイルの更新よりも短いサイクルで配信されるRapid Releaseに対応。より最新の脅威に対処することができます。
- メール大量送信型ワームによるメールを識別し、添付ファイルだけでなくメールそのものを自動的に削除可能。不要なトラフィックの増加、サーバー容量の無駄な消費、受信者の生産性の低下を防止することができます。
- インフォメーションストア内のメール本文と添付ファイルをスキャン。インフォメーションストアを経由せずに外部に直接送信されるSMTPメールのスキャンも可能です。

スパムメール対策とコンテンツフィルタリングの機能を統合し、包括的なメールセキュリティを実現

- **高精度、省メンテナンスのアンチスパムを利用可能**
世界中から収集したスパムメールをもとに多段構成の検出エンジンのチューニングを継続的に行っていくBrightmail AntiSpam技術をベースにしたSymantec Premium AntiSpamを、アドオンで利用することができます*。より高い精度でスパムメールを検出できるとともに、フレキシブルな管理と自動化されたスパムフィルタのアップデートにより、スパムメール対策をさらに省力化することができます。

*オプション機能となります。Symantec Premium AntiSpamは、Symantec Mail Security for Microsoft Exchangeに標準搭載されたアンチスパム機能と併用することはできません。

- **コンテンツフィルタリングにより、情報漏えいや不適切なメールの利用を防止**
メール本文のコンテンツをチェック可能。望ましくない内容をフィルタリングします。指定した言葉に対して重み付けが可能な辞書ベースのDynamic Document Review (DDR) 機能により、フィルタリングのための柔軟なルール設定を容易に行えます。

的確な対応とコスト削減を実現する管理機能

• ポリシーにもとづいた高度な管理

ウイルスや不適切な内容のメール、スパムメールなどに対し、ポリシーにもとづいた対応を行うためのさまざまな設定を、柔軟かつ容易に行えます。

• 複数のサーバーの管理

複数のサーバー上のSymantec Mail Security for Microsoft Exchangeを1つのコンソールから管理し、更新や設定変更を同時に行えます。

• ハートビート機能による稼動状態の監視

Symantec Mail Security for Microsoft Exchangeの稼動に関する検査を定期的に行うハートビート機能により、問題が発生していないかどうかの監視を容易に行えます。

• 処理状況を容易に把握

ログの記録、レポート、カスタマイズ可能な通知、統計情報の生成により、ウイルスインシデントに対する処理状況を容易に把握できます。また、複数のMicrosoft Exchange Server環境におけるアクティビティを単一のレポートにまとめることが可能です。

• Symantec Enterprise Vaultと連携

Symantec Enterprise Vaultをメールの転送先に設定することにより、柔軟かつ検索性に優れたメールの管理が可能です。

• 緊急事態の発生を監視

ウイルス感染の数、修復不能なファイル数などのウイルス関連インシデント、件名や添付ファイル名によるフィルタリング件数などが一定の時間内に設定量を超える場合には、自動的に通知。検出されたメールの件名や添付ファイル名を自動的にリストに登録し、以降のメールを自動的にブロックすることも可能です。

Symantec Security Responseによる信頼の支援体制

Symantec Security Responseは、グローバルに展開するインターネットセキュリティ全般に関するリサーチチームとテクニカルサポートチームで構成されています。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などに関する調査/研究、また、それに基づくシマンテック製品の支援を行っています。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 6.0 for Microsoft® Exchange

サーバーシステム

Exchange プラットフォームおよび対応OS

〈Microsoft Exchange 2000 / 2003 ベース〉

- Microsoft Exchange 2000 Server / Enterprise Server (SP3)
- Microsoft Exchange Server 2003 / Enterprise Server
- Windows 2000 Server / Advanced Server / Datacenter (SP4)
- Windows Server 2003 Standard / Enterprise / Datacenter (SP1)

〈Microsoft Exchange Server 2007 ベース〉

- Microsoft Exchange Server 2007
- Windows Server 2003 Standard x64 / Enterprise x64
- Windows Server 2003 R2 Standard x64 / Enterprise x64
- Windows Server 2008 Standard / Enterprise

その他の要件

- Microsoft .NET Framework 2.0
- Microsoft Data Access Components (MDAC) 2.8以降*
- Microsoft DirectX 9.0*

コンソールのみ

OS (32 bit)

- Windows 2000 Server (SP4)
- Windows Server 2003 (SP1)
- Windows XP (SP1)

その他の要件

- Microsoft .NET Framework 2.0
- Microsoft DirectX 9.0*

*検出されなかった場合は自動的にインストールされます。

※Windows環境での使用におけるメモリーとプロセッサの要件については、Microsoft社の推奨条件をご参照ください。

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/jp/business>