



# McAfee Security for Email Servers

Microsoft Exchange ServerとLotus Domino Serverを保護する  
強固なコンテンツ セキュリティ

McAfeeでは、コンテンツ検査、レピュテーション分析、マルウェア対策を統合して電子メールを保護します。ネットワーク境界、ハブトランスポートサーバー、メールサーバーに多層型の防御を配置し、電子メールを保護します。

## 主な特長

システムを常時稼動 – 電子メールによるウイルスやワームの侵入を防ぎ、Microsoft ExchangeやLotus Domino内部での拡散を阻止します。

従業員の生産性を維持 – スパムやフィッシング詐欺攻撃を阻止します。

1つのコンソールで管理 – McAfee ePOの強力な一元管理コンソールで、セキュリティの制御、管理、レポートの作成を行います。

重要なデータを保護 – DLPとレピュテーション技術(IP、メッセージ、URL、ファイル)により、受信メールと送信メールをフィルタリングして情報の流出を防ぎ、法的責任を軽減します。

分かりやすいユーザーインターフェース – 使いやすいインターフェースで、レポートやグラフを作成し、メールトラフィックの統計をリアルタイムで確認できます。

McAfee® Security for Email Serversは、ウイルス、ワーム、トロイの木馬、不審なプログラムを検出し、フィルタリングします。Microsoft ExchangeとLotus Dominoサーバーに対応し、スパムのブロックやメッセージのフィルタリングを行います。不適切なコンテンツの侵入を阻止し、機密データの流出を防ぐので、ポリシーやコンプライアンス要件を満たすことができます。

Intel® Security製品の一部として、McAfee Security for Email Serversは送受信される電子メールを多層防御で保護します。マルウェアをオンデマンドでスキャンし、ポリシーによって重要なデータの流出や悪用を防ぎます。

業界最高の保護対策 – 業界最高のメモリー内スキャンとオンデマンドスキャンにより、受信メールと送信メールに潜むウイルス、ワーム、トロイの木馬などの脅威を阻止します。

強力な内部保護 – ネットワーク境界から入り込む脅威だけでなく、感染したラップトップや内部メールからネットワークに侵入する脅威を阻止します。スパム対策モジュールでスパムを阻止します。

強力なコンテンツフィルタリング – メールの使用に対して会社のポリシーを施行し、禁止されたファイルタイプや不適切なコンテンツをフィルタリングして機密データの流出を防ぎます。

単一コンソールでの管理 – McAfee ePolicy Orchestrator® (McAfee ePO™) プラットフォームで、グラフィカルなレポートを確認しながら、セキュリティの配備と管理を行うことができます。

## 多層型の電子メール保護

包括的なマルウェア対策

McAfee Security for Email Serversは、リアルタイムのファイルレピュテーションとマルウェア対策を使用して、新たに発生する脅威を未然に防ぎます。クラウドベースのGlobal Threat Intelligence (GTI)により、不審なファイルのフィンガープリントをMcAfee Labsに送信し、レピュテーションの分析を迅速に行います。フィンガープリントが既知のマルウェアとして識別されると、適切な応答を瞬時に戻し、ファイルをブロックまたは隔離します。McAfee GTIのメッセージレピュテーションは、メッセージと送信者のレピュテーションをリアルタイムで配信するクラウドベースの包括的なサービスです。弊社の製品はこのサービスを使用して、既知かどうかを問わず、スパムなどのメッセージの脅威から顧客を保護します。

## メッセージレピュテーション

メッセージレピュテーションは、スパム送信パターン、IPの挙動などの要素を考慮し、不正なメッセージである可能性を判定します。このスコアは、McAfeeクラウドに照会を行うセンサーからの情報、McAfee Labsの分析結果、Web、メール、ネットワークの脅威データを相関分析した結果から算出されます。

### 仕様

メールサーバーに格納される電子メールや共有データは急激に増加しています。McAfee Security for Email Serversは、Microsoft Exchange環境と Lotus Domino環境をサポートし、従業員と組織の生産性を低下させず、サーバーの稼働状況を維持します。

McAfee Security for Microsoft Exchangeの要件  
オペレーティングシステム  
Windows Server 2008  
Windows Server 2008 R2  
Windows Server 2012  
Windows Server 2012 R2

Microsoft Exchange Server  
Exchange Server 2007  
Exchange Server 2010  
Exchange Server 2013  
クラスター環境のExchange Serverにも対応

McAfee Security for Lotus Domino (Windows) の要件  
Microsoft Windows Server 2008, 2008 R2

Lotus Domino 8.5  
(32ビット/64ビット) に対応

### IPレピュテーション

送信サーバーのIPアドレスに基づいて、電子メールに潜む脅威を検出します。IPレピュテーションにより、ゲートウェイで電子メールがブロックされるので、攻撃や情報の流出を防ぐことができます。

### URLレピュテーション

電子メールに含まれるURLのレピュテーションに基づいて、Webの脅威を阻止します。既知の脅威だけでなく、新たに発生する脅威もブロックします。

### サーバーを常時保護

受信メールと送信メールをチェックし、ウイルス、ワーム、トロイの木馬などのマルウェアの存在を確認します。また、内部のメールをすべてスキャンし、組織内でのワームの拡散を阻止します。McAfee Security for Email Serversは最新のウイルス定義ファイル(.DAT)をHTTP、FTP、ネットワークファイル共有またはMcAfee ePO管理コンソールから自動的にダウンロードします。

### コンプライアンス対応

サイズ、メッセージや添付ファイルの内容に従ってメッセージをフィルタリングします。件名、本文または添付ファイルに禁止されたコンテンツを含むメッセージをブロックまたは隔離します。

### 少ない時間とリソースで管理可能

コンテンツフィルターが事前に定義されているので、ポリシーを簡単に作成し、施行できます。グローバルなルールを作成し、個人または部門の必要に応じて例外を設定します。管理作業は組み込みのHTMLインターフェースまたはMcAfee ePOで行います。

### コンテンツ フィルタリング

電子メールの件名や本文、添付ファイルに含まれるコンテンツとテキストをスキャンします。正規表現(Regex)を使用して、独自のコンテンツ フィルタリングルールを作成できます。

### データ損失防止とコンプライアンス

データ損失防止(DLP)により、送信中または保存中の電子メールを保護し、機密情報の漏えいを防ぎ、コンプライアンスを維持します。ディクショナリが事前に定義されているので、企業や国ごとに固有のコンプライアンスルールを簡単に作成できます。組み込みのワークフローにより、隔離されたメールが自動的に監査担当者に転送されます。

スパム フィルタリングで生産性が大幅に向上  
スパム対策モジュールでスパムとフィッシング詐欺メールを検出するので、従業員の生産性を低下させず、メールサーバーのストレージを節約できます。また、独自のホワイトリストとブラックリストを作成できます。弊社のゲートウェイメールソリューションでは同じ隔離ソリューションを利用しているので、隔離領域に簡単にアクセスできます。

### 製品の正常性を通知

McAfee Security for Email Serversは、指定された管理者に製品の状態を通知します。各ファイルのスキャンにかかる時間を監視し、問題がある場合には訂正処置を行い、Exchange Serverのパフォーマンス低下を防ぎます。

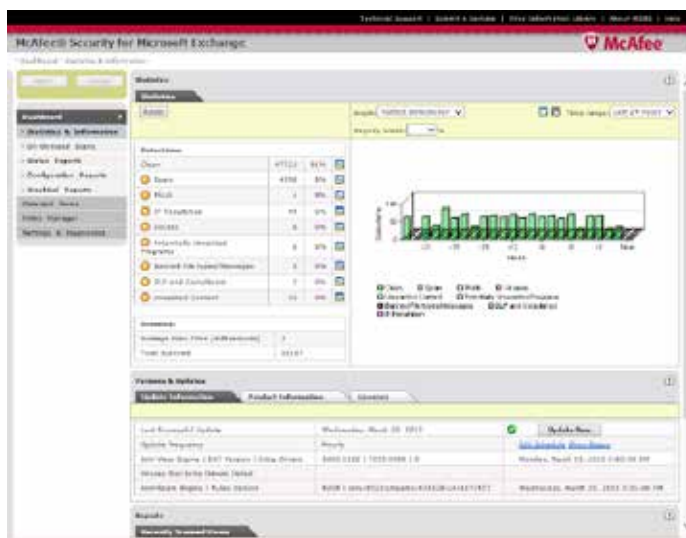


図 1. 使いやすいインターフェースで、レポートやグラフを作成し、メールトラフィックの統計をリアルタイムで確認できます。

## データシート

受信トレイをOffice365に移行しても心配いりません。  
[www.mcafee.com/o365](http://www.mcafee.com/o365)をご覧ください。

### 簡単な更新

自動更新により、世界最高の脅威研究機関であるMcAfee Labsから最新のセキュリティ情報を取得します。

### 隔離メールを一元管理

付属のMcAfee Quarantine Managerが隔離とスパム対策を行います。McAfee Quarantine Managerは管理しやすいソリューションです。McAfee Labsへのサンプル送信、きめ細かい制御、LDAPサーバーとユーザーの自動同期、グローバルなブラックリスト/ホワイトリスト、柔軟なレポート機能など、すべての作業をMcAfee ePOプラットフォームで実施できます。

### メールストアのスキャンと保護

McAfee Security for Email Serversでは、オンデマンドスキャンのスケジュールを柔軟に設定できます。従来のフルスキャンよりも迅速にスキャンを完了します。添付ファイル付きのメールや未読メールだけをスキャンしたり、件名、送信者、受信者、CC、メッセージIDだけをスキャンすることもできます。また、受信期間とサイズを指定してメールをスキャンできます。

詳細は、McAfee Security for Email Serversをご覧ください。



### McAfee. Part of Intel Security.

東京本社 〒150-0043 東京都渋谷区道玄坂 1-12-1  
渋谷マークシティ西棟 20F  
TEL 03-5428-1100 (代) FAX 03-5428-1480  
西日本支店 〒530-0003 大阪府大阪市北区堂島 2-2-2  
近鉄堂島ビル 18F  
TEL 06-6344-1511 (代) FAX 06-6344-1517  
〒450-0002 愛知県名古屋市中村区名駅 4-6-17  
名古屋営業所 名古屋ビルディング 13F  
TEL 052-551-6233 (代) FAX 052-551-6236  
福岡営業所 〒810-0801 福岡県福岡市博多区中洲 5-3-8  
アクア博多 5F  
TEL 092-287-9674 (代)  
[www.intelsecurity.com](http://www.intelsecurity.com)

IntelおよびIntelのロゴは、米国法人Intel Corporationまたは米国またはその他の国の関係会社における登録商標です。McAfee、McAfeeのロゴ、ePolicy Orchestrator、McAfee ePOは、米国法人McAfee, Inc.または米国またはその他の国の関係会社における登録商標または商標です。その他すべての登録商標および商標はそれぞれの所有者に帰属します。本資料は情報提供を目的としています。ここに記載されている製品計画、仕様、説明は予告なしに変更される場合があります。本資料の内容について弊社はいかなる保証も行いません。Copyright © 2014 McAfee, Inc. 61358ds\_security-email-servers\_1014