Kaspersky Security for Linux Mail Server

- **業界で最高クラスのスパム検知率**
- **マルウェアやぜい弱性からの高度な保護**
- **容易な統合、監視、管理**

メールは組織内の重要なコミュニケーションツールですが、一方で以下のようなさまざまな課題があります。

- 増え続けるメールトラフィック
- 深刻化するセキュリティのリスク
- 管理コストの増大

メールのトラフィックが増大している一番の理由は、メールの約65%*[1]を占めるスパムメールです。また、最近ではフィッシングメールや標的型攻撃のようなメールを媒介にした脅威が増加しています。これらの脅威に対応するためシステム管理者は複雑なシステムの管理を求められています。

Kaspersky Security for Linux Mail Serverは、オンプレミスソリューションのプライバシー保護とコントロールを利用して、スパム、標的型攻撃、および最新のマルウェアから内部ユーザーとモバイルユーザー（ノートPC、タブレット、スマートフォン）の両方を保護します。

スパム対策

Kaspersky Security for Linux Mail Serverでは、自社開発によるカスペルスキーのアンチスパムエンジンを、クラウド対応のテクノロジーと組み合わせて利用しています。

- **アンチスパムのプッシュ型アップデート** - プッシュテクノロジーを利用することで、クラウドからリアルタイムに直接アップデートを適用
- **レピュテーションフィルタリング** – 疑わしいメールを隔離してアップデート後の情報と照らし合わせて再分析することで、未知のスパムに対抗

これらのテクノロジーを組み合わせることで、Kaspersky Security for Linux Mail Serverでは誤検知率を最小に抑えながら、最大99.93%*[2]のスパムをブロックできます。

セキュリティ対策

Kaspersky Security for Linux Mail Serverでは、受賞歴のある**カスペルスキーのアンチマルウェアエンジン**と、新しい**ZETA**（Zero-day Exploits and Targeted Attacks、ゼロデイエクスプロイトおよび標的型攻撃）**Shield**の2つのテクノロジーを組み合わせて利用しています。ZETA Shieldは、マルウェアのシグネチャが判明しないうちにゼロアワーのぜい弱性を利用するAdvanced Persistent Threat（APT）から防護するためのカスペルスキーのテクノロジーです。

添付ファイル対策

Kaspersky Security for Linux Mail Serverは、不適切なメールの添付ファイルの監視、フィルタリング、ブロックを実行します。ファイル形式の認識機能により、ファイルの内容からファイル形式を分析し、宣言されたファイル拡張子にかかわらず、迷惑メールをブロックします。

使いやすい管理インターフェイス

Web経由のコンソール

メールセキュリティのあらゆる面に関する管理、監視が非常に容易になります。新しいダッシュボードでは製品の状態や、時間別、日別、月別のメールトラフィックの配信状況、製品のさまざまな機能を示すリンクなどを一目で確認できます。

定義済みのカスタムホワイトリスト/ブラックリストの作成

送信者のホワイトリスト/ブラックリストに基づいた、カスタマイズされたメールフィルタリングルールを使用して、グローバルレベルでも個人レベル（スパムに限る）でもメールトラフィックを管理できます。

IPv6対応の柔軟性の高いメールトラフィック管理ルール

送信者および受信者のグループに関する定義済みのルールに従ってメールを処理できます（IPv4およびIPv6、ワイルドカード、正規表現を使用）。

グローバル/個人用隔離フォルダー

システム管理者はスパム、マルウェアを含む疑わしいメールや、コンテンツフィルタリングルールによってブロックされたメールをグローバル隔離フォルダーに保存するためのポリシーを定義し、隔離後に処理（判断）を行うことができます。また、各ユーザーが個人用隔離フォルダーにアクセスして、メッセージの検索や選択したメッセージの転送を自分で行うことができるため、ヘルプデスクの負荷が減少します。

詳細レポート/通知機能

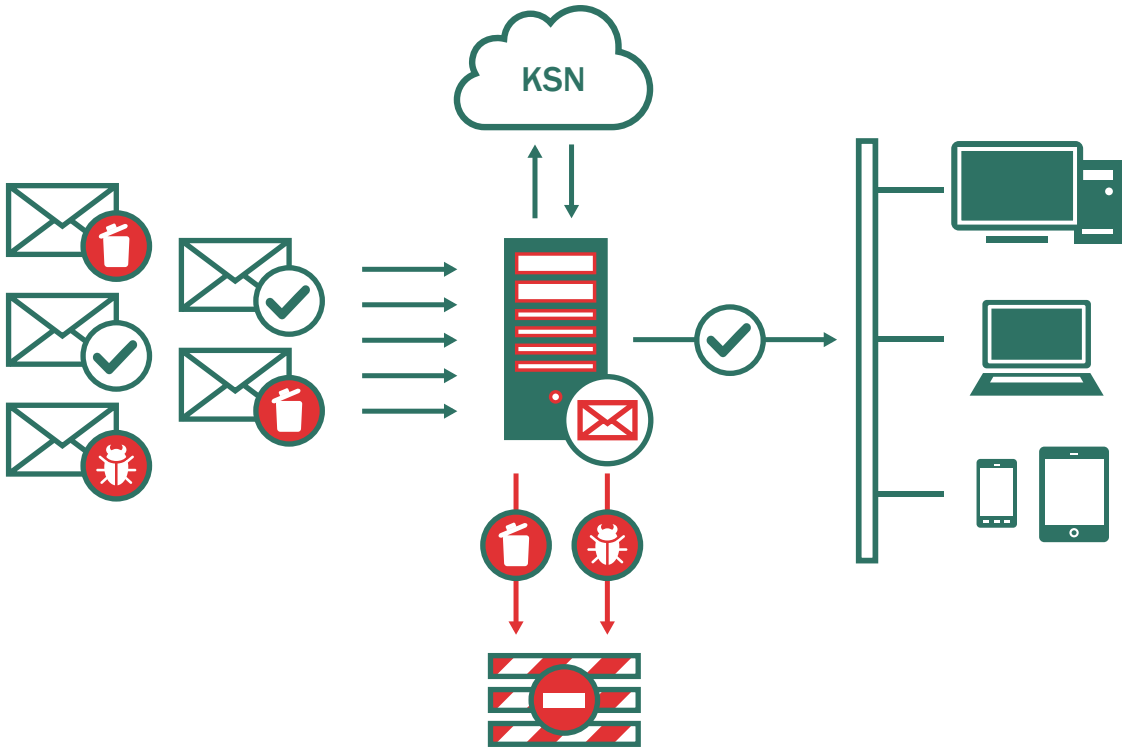
カスタマイズ可能なレポートには、セキュリティイベントの監視や分析に必要となる詳細情報が記載されます。また、通知システムより、管理者やドキュメント所有者はポリシー違反に関するアラートを受け取ることができます。

*1 出典：総務省 電気通信事業者13社の全受信メール数と迷惑メール数の割合（2012年5月時点）
*2 出典：Virus Bulletin Anti-Spam Comparative Review（2012年9月）

システムの概要

企業のメールインフラストラクチャへの統合。
Kaspersky Security for Linux Mail Server は、一般的に普及している Linux ベースのメールサーバーとの統合をサポートしています。また、AMaViS インターフェイスやオンデマンドのファイルスキャナーもサポートしています。

LDAP サービスとの統合。
管理者はLDAP サーバーのユーザーアカウントとグループ（OpenLDAP またはMicrosoft Active Directory）を使用して、企業のメール管理のための特別な処理ルールを作成できます。



KSN : Kaspersky Security Network

オペレーティングシステム（x86/x64）：

- Red Hat Enterprise Linux 6.6 Server(32/64ビット)
- Red Hat Enterprise Linux 7（64ビット）
- SUSE Linux Enterprise Server 11 SP3（32/64ビット)
- SUSE Linux Enterprise Server 12（64ビット）
- CentOS-6.6（32/64ビット）
- CentOS-7（64ビット）
- Ubuntu Server 12.04.4 LTS（32/64ビット）
- Ubuntu Server 14.04 LTS（32/64ビット）
- Debian GNU / Linux 6.0.10（32/64ビット）
- Debian GNU / Linux 7.7（32/64ビット）
- FreeBSD 8.3（32/64ビット）
- FreeBSD 9.3（32/64ビット）
- FreeBSD 10.1（32/64ビット）

最小ハードウェア要件:

- CPU:Intel® Xeon 3040 or Core 2 Duo 1.86 GHz以上
- メモリ：2GB 以上
- スワップ領域:4 GB
- ハードディスク：4GB 以上の空き容量

メールサーバー：

- exim-4.71 以降
- postfix-2.5 以降
- sendmail-8.14 以降

Kaspersky Security for Linux Mail Serverの詳細については、
www.kaspersky.co.jpをご覧ください。

※Kaspersky Security for Linux Mail serverはKaspersky Lab ZAOの登録商標です。
※その他記載された会社名または製品名などは、各社の登録商標または商標です。本文中では、TM、®マークは明記していません。
※記載された内容は、改良のために予告なく変更されることがあります。
©2015 Kaspersky Labs Japan