Kaspersky Security Linux Mail Server

マルウェアの脅威からメールシステムを守る次世代の保護機能

メールは、企業の IT セキュリティを脅かすマルウェアの攻撃手段として最も多く使用されています。[1]
Kaspersky Security for Linux Mail Server は、高度なヒューリスティック分析、サンドボックス、レピュテーションなど、機械学習を利用した次世代の保護機能を提供します。この保護機能により、ランサムウェア、悪意のあるメール添付ファイル、スパムメール、フィッシングメールおよび未知の脅威からメールシステムを保護し、さらに誤検知率も低減させることができます。

利点

高度なスパム検知技術で業務の生産性を向上

Kaspersky Security for Linux Mail Server には、高度なスパム検知技術が実装されており、メールシステムを介してスパムメールの侵入を阻止し、ユーザーの業務遂行に悪影響が及ばないようにします。また、誤検知率は極めて低いため、通常のメールが誤ってスパムと判断されて隔離されることがなく、業務に支障をきたさないようにします。

マルウェアや脆弱性を悪用する攻撃からの高度な保護

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は、マルウェアの高い検知率と高速なスキャンによって、メッセージの本文とソフトウェアの脆弱性を利用するように作られた悪意のある添付ファイルを迅速かつ正確に検知します。この技術によって脆弱性を利用する攻撃からメールシステムをより強固に保護します。

効率的なシステム運用

高機能なメールトラフィックルールを備え、OpenLDAP と Microsoft Active Directory に対応しているため、企業のセキュリティ要件に沿ったポリシーを容易に設定できます。また、ユーザーが個人用のブラックリストとホワイトリストを設定し、隔離されている項目をユーザー自身で管理できるため、ヘルプデスクへの問い合わせ件数を削減することができます。これにより、管理者の作業負担が軽減でき、より多くの時間を他の管理業務に割り当てることが可能になります。

高いスループットとパフォーマンス

Kaspersky Security for Linux Mail Server は、システムに多大な影響を与えることなく高いスループットを実現できるように設計されており、ビジネスの生産性が飛躍的に向上します。

特長

- 高度なアンチマルウェアエンジンでリアルタイムに保護
- Kaspersky Security Network を活用したクラウド型脅威インテリジェンスで最新の脅威に対応
- 送信ドメイン認証技術で、なりすましメールやビジネスメール詐欺（BEC）の防止対策を強化
- ゼロアワー脅威からの保護
- Kaspersky Anti Targeted Attack Platform（KATA）と連携し、標的型攻撃の侵入を阻止
- メールおよび添付ファイルのフィルタリングと隔離管理
- MS Officeファイルに埋め込まれた悪意のあるマクロを利用した攻撃を防御
- メールによって配信されるランサムウェアの侵入を阻止
- OpenLDAP と Microsoft Active Directory のサポート
- IPv6 のサポート
- SIEM 製品との連携

1 出典「Verizon Data Breach Investigations Reports（2017年）」

機能

多層防御型のマルウェア対策 HuMachine™

カスペルスキーのマルウェア対策では、機械学習および脅威インテリジェンスなどを含む高度な多層防御技術が利用されており、受信したメールに悪意のある添付ファイル、既知および未知のマルウェアをフィルタリングしてメッセージから除外します。

- **グローバルな脅威インテリジェンス：**
  カスペルスキーのクラウド内に収集されたリアルタイムの脅威情報を利用することで、最新のマルウェアや脅威への迅速な対応が可能になります。
- **機械学習：**
  グローバルから収集された脅威に関するビッグデータは、機械学習のアルゴリズム、エキスパートの専門知識との組み合わせによって詳細に分析され、誤検知を最小限に抑えながら高い検知レベルを実現します。
- **エミュレート可能なサンドボックス：**
  最も高度で、非常に難解なマルウェアから保護するために、メールの添付ファイルは、サンドボックス内でファイルをエミュレートして新しい脅威を検知することができ、危険なマルウェアの侵入からメールシステムを保護します。

機械学習を取り入れたアンチスパムシステム（コンテンツレピュテーション含む）

カスペルスキーのアンチスパムシステムは、機械学習をもとにした検知モデルを実装しています。Kaspersky Labのエキスパートは、自動的に分析されたスパムメールの脅威情報を監修します。機械学習を取り入れた高度な分析手法とエキスパートによる分析を組み合わせることで精度が向上し、誤検知の可能性を最小限に抑え、脅威に対して迅速に対処することができます。

高度なアンチフィッシング

カスペルスキーの高度なアンチフィッシングシステムの検知モデルは、機械学習のひとつであるニューラルネットワークモデルを採用しています。カスペルスキーのアンチフィッシングモジュールは、1000件を超える画像、言語、特定のスクリプトを含む条件が組み込まれたクラウド型のKaspersky Security Network からリアルタイムで最新の脅威情報を受け取ります。これにより、フィッシングサイトへのリンクが含まれるメールを効率よく検知することができ、既知と未知またはゼロアワーのフィッシングメールの攻撃からメールシステムを保護します。

なりすましメール防止対策

SPF、DKIM、DMARC などの信頼性の高い送信ドメイン認証技術を利用して、メール送信者の認証確認を行うことができます。これは、最近被害報告が多くなってきているビジネスメール詐欺（BEC）対策の強化に有効な手段です。

添付ファイル対策

攻撃者は、マルウェアを組み込んだファイルをメールに添付して送信する手段を用いるため、添付ファイル付きのメールを受信することは、企業にとって感染のリスクが増大します。カスペルスキーが提供する添付ファイルのフィルタリング機能では、添付ファイルの検知ルールを柔軟に設定することができます。攻撃者によってよく利用されるファイルの種別を検知することで、感染によって情報が不正に盗み取られるリスクを低減することができます。

メッセージのバックアップ

ウイルスの駆除やメッセージの削除などによって重要な情報が消失しないように、元のメッセージをバックアップストレージに保存できます。
また、管理者は必要に応じて元のメール形式でユーザーに再配信することができます。バックアップの条件は、検知ルールごとに設定することができます。

標的型攻撃対策

Kaspersky Anti Targeted Attack Platform（KATA）[2]との統合により、標的型攻撃など高度なサイバー脅威の兆候が含まれるメールを検知します。KATA の分析結果にもとづいて危険なコンテンツを含むメッセージをブロックでき、より強固なメールシステムを運用することができます。

2 Kaspersky Anti Targeted Attack Platformは、別途ご購入いただく必要があります。

詳細レポートと通知機能

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な情報が記録されるため、管理者は運用状況を把握し、障害発生時に適切な対策を講じることができます。また、通知システムより、管理者やユーザーはイベント通知をメール形式で受け取ることができ、容易に状況を確認することができます。

Kaspersky HuMachine™ のアプローチ
ビッグデータを解析した脅威インテリジェンス、機械学習、エキスパートの専門知識を組み合わせることで、より強固な多層防御を実現しています。それらを緊密に連携させることで各要素の強みが最大化され、より高い保護が可能になります。

購入方法
Kaspersky Security for Linux Mail Serverは、以下の製品に含まれています。
- Kaspersky Security for Linux Mail Server

株式会社カスペルスキー
製品情報：http://www.kaspersky.co.jp/business-security/mail-server
ご購入相談窓口：jp-sales@kaspersky.com

www.kaspersky.co.jp
#truecybersecurity

PMM-1023-201711