McAfee Email Protection

メールボックスを常時保護する高度なセキュリティ対策

高度な電子メール保護を必要としている企業が増えています。SANS Instituteの調査によると、ネットワーク攻撃の95%はスピア フィッシングが原因で発生しています[1]。いまだに多くのユーザーがソーシャル エンジニアリングで騙されています。サイバー犯罪者の手口はさらに巧妙化し、セキュリティ意識の高い攻撃でも被害が発生しています。知的財産を狙う高度なマルウェアは大きな問題となっています。攻撃が発生すれば、組織にとって致命的な打撃となりかねません。また、多くの企業がメールボックスをホスティング環境に移行し始めていますが、この流れがリスクを増大させています。従来の電子メール保護では柔軟な対応ができないため、新たなソリューションが求められています。この問題を解決するのがMcAfee® Email Protectionです。この強力なソリューションはデータ損失防止（DLP）技術と電子メールの継続性を統合したエンタープライズ クラスの保護機能を提供し、標的型のフィッシング攻撃を阻止します。柔軟な配備オプションが用意されているので、必要に応じてクラウド、オンプレミスまたはハイブリッドで実装できます。

主な特長

標的型フィッシング詐欺の阻止

- ClickProtectで不正なURLをリアルタイムで阻止します。
- McAfee Advanced Threat Defenseと連携し、ステルス型マルウェアを阻止します。
- データ損失防止技術を搭載しています。

ホスティングされたメールボックスの保護

- 電子メールの配信先に関係なく、標的型攻撃をブロックします。
- エンドユーザーがグレーメールを制御できます。
- 電子メールの接続性を維持できます。
- 高度なデータ損失防止と暗号化機能を提供します。

柔軟な配備オプション

- 必要なときに必要なモードで配備できます。
- ハイブリッド配備オプションでは、1つのコンソールで管理とレポーティングを実行できます。

ソーシャル エンジニアリングを超える新しいスピア フィッシング

フィッシング詐欺に対する防御で最も弱い部分がユーザーです。『The Verizon Data Breach Investigation Report, 2014』（2014年データ侵害調査報告書）[2]によると、5人に1人がフィッシング詐欺メールのリンクをクリックしています。サイバー犯罪者はソーシャル エンジニアリングでユーザーの弱点につけ込むだけでなく、脅威メールの追跡を回避するため、より高度な戦術を駆使しています。一例を挙げましょう。

- **ワンタイムURL:** ユーザーがフィッシング詐欺に騙され、感染に成功すると、サイバー犯罪者は不正なURLを閉鎖します。これにより、検出とフォレンジックの回避しようとします。
- **時間差での感染:** 攻撃をすぐに実行せず、電子メールがスキャンされ、会社の受信ボックスに配信された後で攻撃を開始し、その後に標的のサイトにペイロードをドロップする場合があります。従業員は職場で受信したメールを信用する傾向があるため、最終的に不正なリンクをクリックしてしまいます。
- **サンドボックスを回避するマルウェア:** このタイプの不正コードは、しばらく潜伏してから攻撃を開始し、検出を回避しようとします。

高度な多層型防御

クリック時の保護

McAfee Email Protectionは、巧妙なスピア フィッシング詐欺とそれに伴うステルス型マルウェアを多層型防御で阻止します。McAfee Email Protectionは、McAfee Web GatewayのMcAfee Gateway Anti-Malware Engine[3]と連動し、URL

のクリック時にもスキャンを実行します。この ClickProtect機能により、デバイスがどこにあってもスピア フィッシング詐欺から保護できます。ClickProtectは、電子メールに埋め込まれたURLの脅威を検出し、排除します。メッセージがスキャンされてからユーザーがリンクするまでにURLが変更されていないかどうか確認します。この処理はURLの危険性に関係なく実行されます。

たとえば、無害に見えるURLを含む電子メールが会社の財務責任者に送信されたとします。電子メール セキュリティ ソリューションがこの電子メールを受信し、安全性を確認して対象の受信ボックスに配信します。電子メールが届いた後に、攻撃者がリンク先にマルウェアをドロップし、ユーザーがこのリンクをクリックしてしまうと、ネットワークは感染してしまいます。

ClickProtectを使用すると、電子メールのURLをクリックしたときにURLの安全性が確認されます。URLの変更が確認されると、McAfee Gateway Anti-Malware Engineが挙動をエミュレーションし、不正なWebコンテンツを検出します。この処理でシグネチャは使用されません。

不正なサイトも安全にプレビューできるので、ベストプラクティスを確認したり、セキュリティを強化して全体的なリスクを減らすことができます。ClickProtectを使用しなくてもメッセージは受信者に安全に転送されます。電子メールは常に保護されます。

ステルス型マルウェアの検出とブロック
McAfee Advanced Threat Defenseとの統合により、McAfee Email Protectionは不審な添付ファイルに潜むステルス型のゼロディ マルウェアを検出し、受信ボックスに届く前にブロックします。この革新的な多層型アプローチでは、詳細な静的コード分析（リバース エンジニアリング）と動的なマルウェア分析（サンドボックス）を組み合わせ、マルウェアの実際の挙動を分析します。詳細な静的コード分析を行うことで、マルウェアの詳しい分類情報を取得できるので、回避技術を駆使し、巧妙に偽装された脅威も検出できます。また、同じコードを再利用したマルウェアも検出できます。コードを解凍して詳細な静的コード分析を行うので、サンドボックスでの実行を回避するコードも検出できます。

データ損失防止の搭載
標的型のスピア フィッシング攻撃の目的は、価値のある機密データを盗み出すことです。McAfee Email Protectionには、業界最高のDLP技術が搭載されています。PCI DSS、医療、金融データ、プライバシー保護法などのコンテンツ ルールが組み込まれているので、機密データの識別、保管、転送に関するコンプライアンス ポリシーを簡単に作成できます。

McAfee Email Protectionは、文書のデジタル フィンガープリントを保存することで、ポリシーによる制御が必要なコンテンツの種類を識別します。正規表現ツール、カスタマイズ可能なディクショナリ、しきい値カウンター、300以上の文書タイプに対する詳細なコンテンツ スキャン、ホワイトリストにより、組織内のユーザー グループごとに添付ファイル ポリシーとコンテンツ ポリシーを作成し、施行することができます。

McAfee Email Protectionは、オンボックスのプッシュ/プル機能とTLS、S/MIME、PGP暗号化機能を搭載しています。また、追加費用なしで仮想アプライアンス、ハードウェア アプライアンス、ブレードサーバーとして配備できます。

ビジネスの継続性維持に必要な電子メールの保護
電子メール ネットワークの停止で業務を止めることはできません。McAfee Email Protectionを利用すれば、自然災害や停電、あるいは定期保守でネットワークにアクセスできない場合でも、従業員、顧客、パートナー、サプライヤーの接続を維持できます。メール サーバーの停止中に送受信されたメールはすべて保管され、サーバー復旧後に自動的に同期されます。

脅威情報とレピュテーション
McAfee Email Protectionは、業界で最も広範囲な脅威情報サービスであるMcAfee Global Threat Intelligence (McAfee GTI)とも統合されています。これにより、世界各地にある1億台以上のセンサーから情報を収集し、ファイル、Web、メール、ネットワーク デバイスに対する脅威を阻止します。McAfee GTIのレピュテーション分析は不審な送信元から届いた電子メール、不審なサイトへの誘導リンクを含む電子メール、不正なファイルが添付されている電子メールをブロックし、リスクを最小限に抑えます。

McAfee Email Gateway

仮想アプライアンス環境とシステム要件

- VMware vSphere 4.x以降
- VMware vSphere Hypervisor（ESXi）4.x以降
- プロセッサー: 2つの仮想プロセッサー
- 使用可能な仮想メモリー: 2 GB
- ハードディスクの空き容量: 80 GB

ハードウェア アプライアンス

- 別売りで2つのモデルを用意
- ブレード サーバーのフォーム ファクターでも使用可能

McAfee Email Protectionは3年連続で**SC Magazineから5つ星の評価**を得ています。

マルウェアによるフィッシング詐欺、ネットワークへの侵入を試みる高度な持続型攻撃の可能性を劇的に減らすことで、組織の保護レベルを強化できます。また、コストのかかる修復作業の費用を抑えることができます。

ホスティングされたメールの問題

Microsoft Office 365、Google Apps for Workなどのホスティング メール サービスを利用する企業が増えています。ホスティング メール ソリューションの多くは、サービスの一部としてセキュリティを提供していますが、これで十分でしょうか。フィッシング詐欺、スパム、グレーメールは増加を続けていますが、データの漏えいを防ぐセキュリティ機能が組み込まれていません。また、Office 365で電子メールの送受信が停止してしまうと、業務に支障をきたします。McAfee Email Protectionはテスト環境、移行中、移行後にエンタープライズ クラスのセキュリティ対策で標的型フィッシング詐欺と高度なマルウェアを阻止します。McAfee Email Protectionは、メールボックスの配備先やタイミングに関係なく、完全なコンプライアンス対応と電子メールの接続を維持します。

将来の変更にも対応可能な柔軟配備オプション

McAfee Email Protectionは柔軟に配備できる電子メール セキュリティです。クラウド ベースのSaaS（Software-as-a-Service）、オンプレミス ソリューション（仮想アプライアンス、ハードウェア アプライアンス、ブレード サーバー）、あるいはこの2つを合わせたハイブリッド モードで配備できます。現在の要件に最適な方法でMcAfee Email Protectionを配備し、後で拡張したり、配備方法を変更することができます。

選択した配備方法に関わらず、McAfee Email Protectionの集中管理コンソールで統合レポートを作成し、電子メール セキュリティ プログラムの効果を簡単に測定できます。ポリシーは、このソリューションのクラウド ベース コンポーネントとオンプレミス コンポーネントの両方に適用されます。

McAfee Email Protectionの評価をご希望の方は、弊社の営業担当までご連絡いただくか、**www.mcafee.com/jp/products/email-and-web-security/email-security.aspx** をご覧ください。

1. http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox
2. https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf
3. AV-TEST: McAfee Web Gateway Securityアプライアンスのテスト

McAfee. Part of Intel Security.
東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 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
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 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