FIREEYE™

ソリューション概要

巧妙化するメール攻撃に備えよ

概要

標的を絞り込み、その標的に向けた作り込みが可能であり成功率が高いため、Eメールは、多くのサイバー攻撃者が使う手段であり続けています 従来型のスパム対策やアンチウイルス・ソフトウェアは無差別送付型フィッシングには対応できますが、高度な攻撃や標的型スピア・フィッシング、なりすまし攻撃などには対応できません。

多くのゲートウェイ型メール・セキュリティ（SEG）は、旧来型スパムや既知のマルウェアへの対応は可能ですが、未知の不正なEメール・キャンペーンや高度な脅威を検知するために、技術、インテリジェンス、専門知識を組み合わせることによって対応することができません。これらのソリューションは、大量ばらまき型への対応のために設計された、旧来型のスパムフィルタやアンチウイルスソフトを用いているからです。通常の場合でさえ対応に数分かかる上、手口が絶えず変化しているため、さらに検知に時間が必要になります。この時間差が、攻撃者を有利な立場に、被害者を不利な立場に追い込むのです。また、ランサムウェアやスピア・フィッシングを目的とするメールは、通常TLS（Transport Layer Security）経由で送られてくるため、ファイアウォールでは検知できません。

昨今のスパム・キャンペーンやランサムウェアの実行、なりすましによるスピア・フィッシング・メールから身を守るためには、対策側も攻撃に合わせて迅速に進化していく必要があります。そのポイントとして、以下の項目を挙げることができます。

- シグネチャに頼らず、未知の高度な脅威も検知する
- 最小の誤検知で、最大の検知を実現
- インライン構成で、ランサムウェアなどが環境に侵入する前にブロックする
- 脅威に対して迅速に対応し、自社を守るため、セキュリティの最前線から得られた脅威インテリジェンスと、攻撃者に関する予防的な知識を活用する

今の対策だけでは不十分な理由

データ侵害が発生すると、企業にとって重要な情報や人、業務などを危険にさらすことになります。ビジネスは妨害され、評判は落ち、お客様からの信頼も失う可能性があります。データ侵害によって発生する平均被害額は約4億円相当（362万ドル[2]）に上ると言われており、その多くはフィッシング・メールをきっかけとしています。過去窃取されたEメール情報の合計が、他のすべての流出経路によるデータ窃取量の合計よりも多い可能性すらあります。[3]

攻撃者にとってメールは非常に使い勝手の良い攻撃道具です。現在導入している対策が有効なものかどうかを、以下の点から見直してみてください。

1. アンチウイルス、アンチスパム、既知のマルウェア機能のほか、マルウェアが仕込まれた添付ファイルやURL、認証情報の窃取を目的とするフィッシング・サイト、なりすまし攻撃などの高度な脅威を検知してブロックできるか
2. 早急な対応が求められる攻撃を知らせ、どのような対応が必要なのかを、役立つ情報とともに教えてくれるかどうか
3. 攻撃に合わせて迅速に進化していくために必要な、最新かつ文脈に基づいた脅威インテリジェンスにアクセスすることができるかどうか
4. 利用中のEメール・セキュリティ・ソリューションは、他のセキュリティツールと連携し、さまざまな攻撃経路や、複数の手法をあわせた攻撃に対応できるかどうか
5. 事業の成長に合わせて柔軟に拡張が可能かどうか

サイバー攻撃の **91%** は、スピア・フィッシング・メールから始まる[1]

---

1 PhishMe (2016). “Enterprise Phishing Susceptibility and Resiliency Report.”
2 Ponemon Institute LLC (June 2017). “2017 Cost of Data Breach Study: Global Overview.”
3 Mandiant, A FireEye Company (2017). “M-Trends 2017 A View From The Front Lines.”

1 **メール攻撃が巧妙化するにつれ、対策をクラウドで行う企業が増えています。**
情報、運用、資産などのクラウド移行が進んでいます。パブリック・クラウドの成長とモバイル・デバイスなど、インターネットに接続する機器数の爆発的な増加を見る限り、攻撃者がクラウドを狙ってくるのは自然なことであり、それをクラウドで防ごうという動きもまた、当然、増加傾向にあります。

FireEye EメールのCloudエディションは、インバウンドとアウトバウンドのマルウェア、フィッシングURL、なりすまし攻撃、スパムをブロックする、セキュアEメール・ゲートウェイ（SEG）です。アンチウイルスおよびアンチスパム機能（AVAS）アドオンは、スパム・キャンペーンやなりすまし攻撃を防ぎ、スパム・キャンペーンや高度な標的型メールから組織を守る、シングル・ベンダーの包括的なEメール・セキュリティ対策です。このソリューションによって、他のEメール・セキュリティ対策を集約し、クラウドを最大限に活用することができます。

2 **旧式の対策を導入することで得られる安心感が、かえって危機を招くことがあります。**パターンファイルやレピュテーションなど、既知の脅威情報を第三者企業から購入して実装しているゲートウェイ型メール・セキュリティは、未知脅威を検知するようには作られていません。ファイアウォールもまた、ランサムウェアやスピア・フィッシングの対策にはなりえません。

図1：従来型のセキュリティ・ソリューションは、標的型サイバー攻撃を検知できない

ファイアウォールはアーキテクチャ的にメールを溜め込んで解析するということができないため、マルウェアが仕掛けられた添付ファイルやURLが含まれるメールやなりすましメールをユーザーに配信してしまうのです。

FireEye Eメール・セキュリティは、他のメール・セキュリティ対策では検出できない高度な標的型攻撃やEメール・トラフィックに紛れたスパムを正確に検知し、ブロックすることで、侵害によって発生するリスクを最小限に抑えます。実際に最近、消費財を扱うグローバル企業が価値検証（POV）を実施し、FireEyeが現行のゲートウェイでは阻止できなかった何千ものフィッシングやなりすまし攻撃を検知したことがわかっています。

3 **進化の速いメール攻撃に対し、旧来型のアプローチであるシグネチャは作成が追いつきません。**シグネチャやパターンファイルでは、来たるべき攻撃や求められる対策に関する情報提供はできません。実際、ポイント・ソリューションとしてさまざまなセキュリティ技術やソフトウェアを導入した結果、それぞれが連携せずにばらばらに動き、アラートの増加につながったという事実もあります。FireEye Eメール・セキュリティは、第三者の提供するシグネチャやレピュテーションに依存しない独自の検知技術を用いることにより、新たなスパム・キャンペーンが発生しても迅速かつ効果的に検知し、ブロックします。メールの送信者と送信ドメインを分析し、CEO詐欺などのなりすまし攻撃を検知します。これらのなりすまし攻撃は、マルウェアも不審なURLも用いないため、従来の対策での検知が困難なのです。

FireEye Eメール・セキュリティは、直接調査した結果や攻撃者の観察から得たインテリジェンスに基づいて、何をブロックするかを決めています。また、アラートの優先順位付けやコンテキスト情報にも役立っています。悪意のあるEメールは隔離され、コンテキストに基づくアクション可能なインテリジェンスと攻撃および攻撃者に関する詳細な情報に基づき、高度な脅威を迅速に封じ込めます。

グローバルに共有されている実際の証拠により、未知の攻撃を直ちにブロックし、迅速な対応を支援します。ノイズと誤検知を最小限に抑えながら脅威を見つけ出すことでセキュリティ・チームのリソースを本物の攻撃に集中させ、運用コストを削減し、組織のリスクを最小限に抑えられます。

4 **攻撃の多くは、ネットワーク（Web）とEメール組み合わせた攻撃を用いて、Web専用の対策や、Eメール専用の対策をすり抜けます。**たった1つのサイバー攻撃が成功することにより、ゼロデイ脆弱性を悪用するマルウェアや、スピア・フィッシング・メール、不正なURL、コマンドサーバー群の構築を許し、結果、侵害を受けたデバイスの制御や、目的とした資産の窃取などを引き起こします。

Eメールを起点とするランサムウェア攻撃は、データを暗号化する際にC&Cサーバーへのコールバック通信を発生させます。Eメールをきっかけとして段階的に実行されるこの攻撃は、ファイル単体を解析するサンドボックスのほとんどを簡単にすり抜けます。このため、問題が発覚する前に、被害者のデータはすでに暗号化されてしまうのです。FireEye Eメール・セキュリティとネットワーク・セキュリティを統合することで、複合型の攻撃を検知して阻止します。攻撃ライフサイクルの相関解析を行うことで、攻撃の発端であるスピア・フィッシング・メールと攻撃者を突き止めます。

優れた脅威検知

Eメール・セキュリティは、高度な標的型攻撃や、通常のトラフィックに偽装することで検知回避をする攻撃を特定して隔離することにより、甚大な被害をもたらすセキュリティ侵害の発生リスクを最小限に抑えます。攻撃を検知すると、直ちにブロックして解析し、今後の検出に利用するためのフィンガープリントを作成します。

Eメール・セキュリティの中核となるのは、Advanced URL DefenseとMVXエンジンです。最先端の機械学習と解析技術を用いて、シグネチャやポリシーに基づく従来型セキュリティ対策をすり抜けるサイバー攻撃を検知します。

Eメール・セキュリティ - Cloudエディションは、アンチウイルスとアンチスパム（AVAS）機能を提供しています。シグネチャ・マッチングで検知可能な攻撃や、従来型のなりすまし手法を使用する、知られた攻撃から保護します。

CEO詐欺（ビジネスメール詐欺とも呼ばれる）などのなりすまし攻撃は、企業に経済的な打撃を与えます。

この攻撃では、従来の攻撃に用いられていた不正な添付ファイルやリンクを使用せず、ソーシャル・エンジニアリングを使用していることが、被害増加の一つの要因となっています。これらの攻撃に対抗するため、FireEyeはなりすまし攻撃の検知と防御に特化した革新的なアルゴリズム、システム、ツールを開発しました。

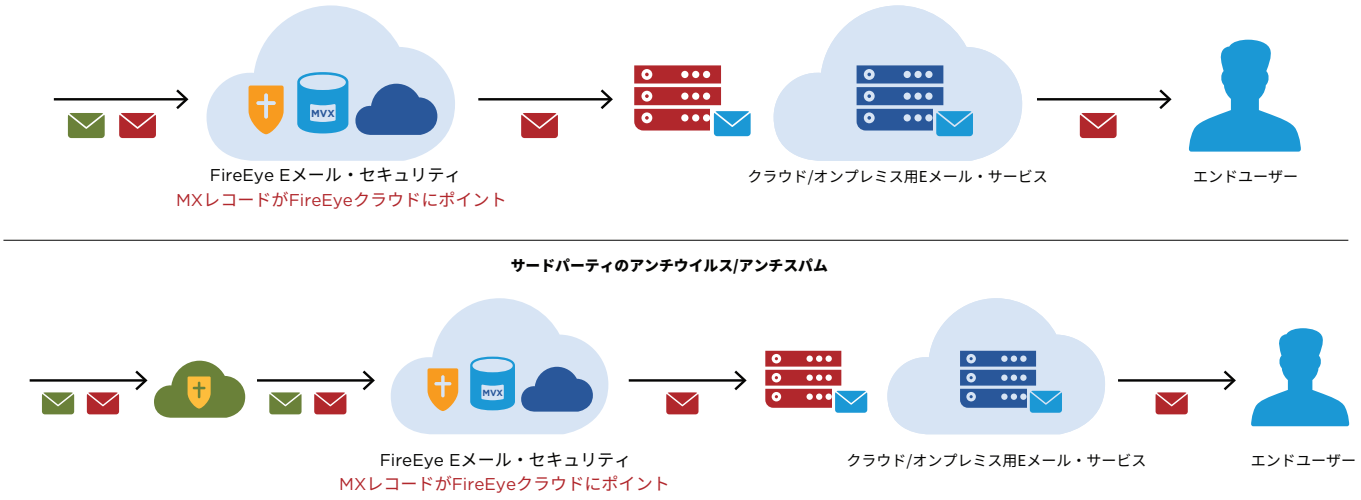
Eメール特有の脅威情報、直接の調査で得られた攻撃と攻撃者情報、攻撃者の特徴に関する情報を使用することで、脅威を特定しつつ、ノイズと誤検知を極限まで抑えることができます。その結果、セキュリティ担当は、希少なリソースを効率的に活用し、本物の攻撃の調査と対応に集中できます。

さまざまな導入形態

FireEye Eメール・セキュリティのインライン導入で、きめ細かな制御と、攻撃に対するリアルタイムな対応が可能になります。特にランサムウェアなどの、ブロックが唯一の効果的な対策となるような攻撃では、インライン・モードは不正なメールがエンドユーザーに届けられないようブロックできます。

ハードウェアやソフトウェアの導入が不要なFireEye Eメール・セキュリティCloudエディションは、Microsoft Office 365やG Suiteのようなクラウドベースのメール・システムへの移行を検討しているお客様にシームレスな統合を提供する、最適なソリューションです。AVASアドオンは、インラインのアンチスパムとアンチウイルス機能を利用して、新しいスパム・キャンペーンやなりすまし攻撃を防止することができます（図2）。

図2：FireEye Eメール・セキュリティ – Cloudエディション – インライン・モード



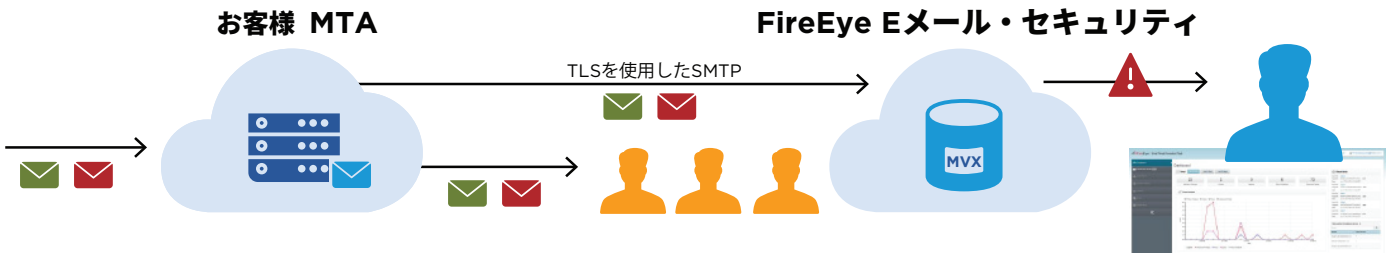
より慎重に運用を開始したい場合は、FireEye Eメール・セキュリティをスパン・タップ構成（モニター・モード）で導入することができます（図3）。この構成では、すべてのトラフィックに対してモニタリングが実施され、レポートも生成されますが、自動的なブロックは実行されません。

FireEye Eメール・セキュリティServerエディションは、オンプレミス用アプライアンスです。FireEyeまたはその認定パートナーは、お客様の環境に最適な導入方法を提案し、導入作業を支援するサービスを提供しています。

次のステップ

今日の高度なサイバー攻撃者や動的に変化する脅威環境を考慮すると、組織は脅威プロファイルを理解しておく必要があると言えます。どの資産が危険にさらされているかを把握し、脅威の素早い検知と対応に集中し、インシデントを迅速に解決するなども含まれます。組織が本来なすべきことに集中し、リスクを最小限に抑えるために、攻撃を初期段階で検知し、ブロックすることに重点を置いたEメール・セキュリティと、サイバー攻撃の直接調査から得られたセキュリティ・テクノロジと脅威インテリジェンスが求められています。

図3：FireEye Eメール・セキュリティ – Cloudエディション – BCCモード



FireEyeの詳細については、**www.FireEye.jp**をご覧ください。

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22
テラススクエア8階 | 03−4577−4401 |
Japan@fireeye.com

会社概要

FireEyeは、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデント対応といった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。