FireEye

巧妙化する メール攻撃に備えよ

概要

メールは、本文やヘッダに細工をすることで簡単に受信者を騙し、標的型やランサムウェアなどの攻撃のきっかけとすることができるため、今でも攻撃者の間では人気の手段です。従来型のスパム対策やアンチウイルス・ソフトウェアは、古くからある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・セキュリティは、無差別送付型スパム対策やアンチウイルス・ソフトウェアを利用しているため、旧来型のスパムやウイルスはブロックできますが、未知の攻撃を検知するための自動分析機能がありません。通常の場合でさえ対応に数分かかるのに、暗号化などで検知回避をするウイルスの場合は、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。

昨今のスパムやランサムウェア、スピア・フィッシング、なりすまし攻撃などから身を守るために、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、未知脅威も検知できる
- 少ない誤検知で、最大の検知を行う
- 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を活用する

なぜ、今の対策では不十分なのか

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。企業のビジネスは妨害され、評判は落ち、お客様からの信頼も失いかねません。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、そのきっかけはフィッシング・メールであることが少なくありません。過去窃取されたEメールの総量が、他のすべての流出経路によるデータ窃取を合わせたよりも大き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今の攻撃に対して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. 未知脅威、不正なドキュメントやURLが添付されたメール、認証情報を窃取する目的のフィッシングやなりすましメール攻撃を検知できるかどうか
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、それに対する対策をクラウドで行う企業が増えています。**
企業は、情報、運用、資産などのクラウド移行を始めています。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・セキュリティ Cloudエディションは、高度に進化したメール攻撃から組織を守る、クラウドベースのソリューションです。本ソリューションは、クラウド時代に求められる包括的なEメール・セキュリティ対策を提供し、アンチウイルス、アンチスパム機能によりスパム攻撃やなりすまし攻撃を検知するほか、スパム・キャンペーンや標的型メールなどからも、企業、組織を守ります。

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しない

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、有害な添付ファイルやURLを持つ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・セキュリティ対策が見逃してしまうようなスパムや標的型攻撃を正確に検知し、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、あるお客様は、以前他の有名なゲートウェイ型メール・セキュリティを導入していましたが、1日に185,000件以上の不正なファイルが添付されたメールの検知漏れが発生していました。

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、新たな攻撃が発生しても迅速かつ効果的にスパムを検知し、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、直接調査した結果得られた情報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より、高度な脅威が封じ込める速さを加速します。

グローバルに共有されている本当の証拠により、これまで知られていなかった攻撃を直ちにブロックし、脅威への対応を加速します。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ができます。これにより、セキュリティ・チームのリソースを実際の攻撃に集中でき、運用コストを削減し、組織のリスクを最小限に抑えることができます。

4 **多くの攻撃は、ネットワーク（Web）とEメールを狙った戦術を複数の段階で組み合わせることで、高度な攻撃の1つの段階にのみ照準を絞ったWeb専用およびEメール専用の防御をすり抜けます。**1つのサイバー攻撃が、ゼロデイ脆弱性を悪用する洗練されたマルウェア、スピア・フィッシング・メール、悪意のあるURL、侵害されたデバイスを制御し、標的とした資産を窃取するためのコマンド・サーバーの複雑なネットワークで構成されている場合があります。

ランサムウェア攻撃はEメールから始まりますが、データを暗号化するために指令（C&C）サーバーとの通信が必要となります。Eメールから始まり段階的に実行されるこれらの攻撃は、ファイルを単体で解析するサンドボックス技術を簡単にすり抜けます。ほとんどのセキュリティ製品が問題を発見するまでに、被害者のデータはすでに暗号化されてしまっています。FireEye　Eメール・セキュリティとネットワーク・セキュリティは、シームレスに統合され、複合型の攻撃を検知して阻止します。これらが連動して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。

4　FireEyeブログ（2016年7月20日）。「Gaps In Email Threat Detection Open The Door to Cybercrime.（Eメール脅威の検知のギャップがサイバー犯罪の扉を開く）」

FireEye Eメール・セキュリティとMulti-Vector Virtual Execution テクノロジー

FireEye Eメール・セキュリティの中核となる技術は、Multi-Vector Virtual Execution™ (MVX) テクノロジーです。MVXは、疑わしいオブジェクトの添付ファイルやURLに検知しにくい攻撃が隠されていないか検査することを目的として設計された動的解析エンジンです。不正なEメールはリアルタイムで隔離され、さらに詳しい解析を実施する、またはそのまま削除することが可能です。直接調査で得られた攻撃と攻撃者の情報を使用することで、ノイズと誤検知はほぼゼロで脅威を特定することができます。これにより、セキュリティ・チームは、希少なリソースを効率的に使用して実際の攻撃の調査と対応に集中できます。

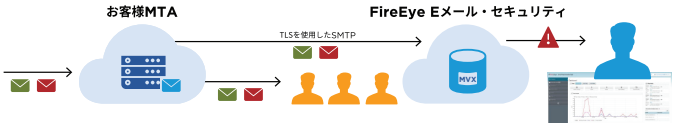
柔軟に選択できる導入形態

FireEye Eメール・セキュリティをインラインで導入することで、ソリューションをきめ細かく制御し、攻撃の発生にリアルタイムで対応することができます。特に予防が唯一の効果的な防御であるランサムウェアなどの攻撃では、インライン・モードは不正なマルウェアレス・コンテンツがエンドユーザーに配信されることを防止できます。

FireEye EメールセキュリティのCloudエディションはハードウェアやソフトウェアの導入が不要なので、Eメール・システムのクラウド移行を検討しているお客様に最適なソリューションです。Microsoft Office 365のようなクラウドベースのEメール・システムとシームレスに統合できます。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、新しいスパム攻撃やなりすまし攻撃を最初から防止することができます (図2) 。

より慎重なアプローチで運用を開始する場合は、図3のように、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。この構成では、すべてのトラフィックで不正な活動が監視され、レポートが生成されますが、自動防御は実施されません。

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

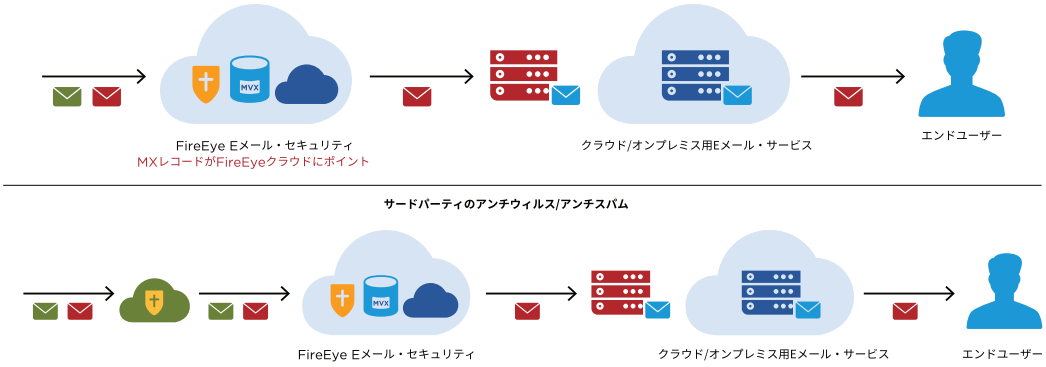


FireEye EメールセキュリティのServerエディションは、オンプレミス用アプライアンスのファミリーです。FireEyeまたはその認定パートナーは、お客様の環境に最適な導入方法を判断し、導入作業を支援するサービスを提供しています。

次のステップ

現在の洗練されたサイバー攻撃者や動的な脅威環境では、組織は脅威プロファイルを理解する必要があります。これには、どの資産が危険にさらされているかを知り、脅威の迅速な検知と対応に集中し、インシデントを迅速に解決することが含まれます。組織の使命に集中し、リスクを最小限に抑えるために、組織はEメールによる脅威を最初に出会ったときに検知してブロックすることに重点を置いたEメール・セキュリティを必要としています。これには、重要なサイバー攻撃の直接調査から得られたセキュリティ・テクノロジとサイバー脅威情報が含まれます。

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



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

FireEyeについて

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。FireEyeは「Forbes Global 2000」企業の45%以上を含む、世界67か国以上の6,600を超える組織で利用されています。

FireEye