FireEye Eメール脅威対策クラウド（ETP）

Eメールを利用した攻撃を検知、解析、
防御するクラウド型のセキュリティ・ソリューション

概要

大量のデータを送り込めるEメールは、サイバー攻撃の最も脆弱な経路になっています。Eメールを利用した脅威は、スパムやウイルス、高度なマルウェアなど増加の一途をたどっています。このような脅威の大半は、細工が施された添付ファイルや不正なリンク、電信送金を指示する詐欺メール、認証情報を狙うフィッシング攻撃という形で拡散します。アンチスパム/アンチウイルス・ソフトウェアは、既知の不正な添付ファイルやリンク、コンテンツを不特定多数に送りつける昔ながらのフィッシング攻撃の検知には対応できますが、このような従来型ソリューションの回避を可能とする高度で標的を絞ったスピア・フィッシング攻撃には無力です。特定の標的を狙うEメールは、内容を柔軟に変更して高い信ぴょう性を得られるため、高度な攻撃の窓口、またはランサムウェアを配布する主要な手段として攻撃者に利用され続けています。

FireEye Eメール脅威対策クラウド（ETP）は、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。クラウド上で展開されるETPは、スピア・フィッシングやランサムウェアなどの高度な標的型攻撃がネットワークに侵入する前に正確に検知して即座に防御できます。またシグネチャレスのMulti-Vector Virtual Execution™（MVX）エンジンを使用して、仮想環境の多様なオペレーティング・システムやアプリケーション、Webブラウザでメールの添付ファイルとURLを解析します。ノイズを最小限に抑えながら脅威を見つけ出すことが可能で、誤検知もほとんど発生しません。

FireEyeでは、攻撃者や独自に実施したセキュリティ侵害調査、および数百万台のセンサーを通じて、広範な脅威インテリジェンスを収集しています。ETPは、このような攻撃の証拠や攻撃者に関するコンテキスト情報に基づいて、アラートの優先度を判断し、脅威をリアルタイムでブロックします。

ETPは、FireEye Network Securityとの連携により可視性がさらに強化されており、複数の経路を使用するマルチベクタの攻撃をリアルタイムで防御します。

ハイライト

- スピア・フィッシングなどの高度な攻撃や段階的に実行される攻撃、ゼロデイ攻撃に対処する包括的なEメール・セキュリティとアンチスパム/アンチウイルス機能を提供
- Eメールを解析し、パスワードで保護/暗号化された添付ファイルに埋め込まれた脅威や、不正なURLを使用した攻撃を検知
- 認証情報を狙うフィッシング攻撃を自動的に検知して被害の拡大を阻止、または完全に防御
- アラートのコンテキストに基づく知見を活用して脅威の優先度を判断し、封じ込め
- Office 365やGoogle Mailのほか、FireEyeの各種テクノロジーと統合
- アクティブな防御モードとモニター・モードに対応
- FedRAMPのセキュリティ要件を満たし、「SOC 2 Type II」認定を取得

FireEye

脅威を効果的に検知

FireEye ETPは、強力なサイバー・セキュリティ・ソリューションです。高度な標的型攻撃など、Eメール・トラフィックに潜む発見困難なサイバー攻撃を正確に検知し、即座に防御して、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。

ETPの中核となる技術は、MVXエンジンです。シグネチャレスのダイナミックな解析エンジンであるMVXは、疑わしいEメール・トラフィックを検査して、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では対応できない巧妙なサイバー攻撃を検知します。安全性が確保された仮想環境で疑わしいコードを実行し、ダイナミックなシグネチャレスの解析により、ゼロデイ攻撃や複数のフローにわたる攻撃など、発見が困難な攻撃を検知します。未知のエクスプロイトやマルウェアをいち早く検出して、「キル・チェーン」と呼ばれる攻撃活動のステップに基づき、感染および侵害の段階でサイバー攻撃を食い止めます。

ETPでは、アンチスパム/アンチウイルス機能も利用できるため、一般的な攻撃にはシグネチャ・マッチング技術で対処します。

Eメールを利用する脅威を防御

インターネットからはさまざまな個人情報が容易に入手できるため、サイバー攻撃者は公開されている個人情報を利用したソーシャル・エンジニアリングによってユーザーを誘導し、フィッシング・メールに記載したURLをクリックさせたり、添付ファイルを実行させようと試みます。

ETPは、従来型のセキュリティ対策をすり抜けるスピア・フィッシング攻撃やランサムウェア、送信者のなりすまし、認証情報を狙うフィッシング攻撃をリアルタイムで検知、防御します。著名サイトと酷似したドメインの不正サイト（タイポスクワッティング）を検知して認証情報の窃取を阻止します。

攻撃が確認された場合はそのEメールを隔離します。隔離したEメールは、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。ETPは次に示すファイルやURLなどを解析し、マルウェアの有無を確認します。

- EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4、アーカイブ・ファイル（ZIP/RAR/TNEF）などあらゆる種類の添付ファイル
- パスワードで保護/暗号化された添付ファイル
- Eメールに埋め込まれたURL
- 認証情報を狙うフィッシング攻撃やタイポスクワッティングに使用されたURL
- オペレーティング・システムやWebブラウザ、アプリケーションに存在する未知の脆弱性
- スピア・フィッシング・メールに埋め込まれた不正なコード

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指令（C&C）サーバーへのコールバックが必要となります。ETPは、段階的に実行され検知が困難なマルウェア・キャンペーンも検知、防御します。

効率的なアラート対応

ETPは、すべての添付ファイルとURLを解析し、最新の高度なサイバー攻撃を正確に検知します。FireEyeのセキュリティ・エコシステムから得られる情報に基づくリアルタイムのアップデート、アラートと既知の攻撃グループの関連付け情報を利用すると、アラートの対応優先度を的確に判断し、スピア・フィッシング・メールをブロックするのに必要な対策を実施できます。ノイズや誤検知を最小限に抑えながら既知、未知、非マルウェアベースの脅威を検知するため、セキュリティ担当者は危険なサイバー攻撃への対応に専念できるようになり、運用コストが削減されます。

変化を続けるセキュリティ脅威トレンドに素早く適応

ETPでは、脅威や攻撃者に関する高度なインテリジェンスに基づいて、Eメールを利用する脅威に対するプロアクティブな防御機能を継続的に適応させることができます。攻撃者、デバイス、標的に関するインテリジェンスの組み合わせにより、次のようなメリットが実現します。

- 脅威を素早く広範囲に可視化
- 検知されたマルウェアや不正な添付ファイルの機能と特徴の特定
- コンテキストに基づく知見をもとに優先度を判断し、迅速に対応
- 攻撃者の可能性がある人物の身元と動機を特定し、侵入先のネットワーク内での活動を追跡
- スピア・フィッシング攻撃を遡及的に特定し、不正なURLを明らかにしてフィッシング・サイトへのアクセスをブロック

ETPのポータル上では、リアルタイムのアラートの確認やレポートの生成を容易に行えます。

容易な導入と、FireEye環境全体との統合

クラウド型のソリューションであるETPは、ハードウェアやソフトウェアを追加して導入する必要がありません。そのため、Eメール・インフラストラクチャをクラウドに移行している組織に最適です。ETPを使用すれば、Eメールに対するセキュリティのための物理的なインフラストラクチャの調達、導入、管理に伴う煩雑さから解放されます。

ETPは、Exchange Online Protectionを設定したMicrosoft Office 365やGoogle Mailなど、クラウド型のEメール・システムとシームレスに統合します。

Eメールを利用した攻撃は、組織宛てのEメールをETPに転送するだけで防御できるようになります。ETPは、まずEメールを解析し、スパムの可能性、さらに既知のウイルスが含まれていないかどうかを確認します。その後、シグネチャ・マッチング技術に依存しない実行環境であるMVXエンジンによりすべての添付ファイルと本文中のURLを解析し、脅威をリアルタイムで検知して高度な攻撃を防御します。

アクティブな防御モードとモニター・モード

ETPを防御モードで運用すると、Eメールの解析後に脅威が隔離されます。この場合は、EメールをFireEyeに転送するようDNSのMXレコードを設定します。モニター・モードで運用する場合は、透過的なBCCルールを設定してEメールのコピーをFireEyeに転送し、MVXエンジンで解析します。

対応ワークフローの統合

ETPは、アラート対応ワークフローを自動化する次のようなFireEyeのソリューションと連携します。

- FireEye CMシリーズ（集中管理システム）は、ETPとFireEye Network Securityからのアラートを相関分析して攻撃の全体像を明らかにし、被害の拡大を防ぐためのブロック・ルールを設定します。
- FireEye Helixプラットフォームは、ETPとスムーズに連携し、セキュリティ・オペレーションを簡素化、統合化、自動化します。

コンプライアンス認証

FedRAMP

FireEyeの政府機関向けETPサービスは、行政および公立教育機関が運用するクラウド・サービスを対象とする、FedRAMPのセキュリティ要件に適合します。

SOC 2 Type II

FireEye ETPを導入したクラウド環境は、セキュリティと機密性に関する、米国公認会計士協会（AICPA）の「Service Organization Controls（SOC 2）Type II」認定に対応しています。

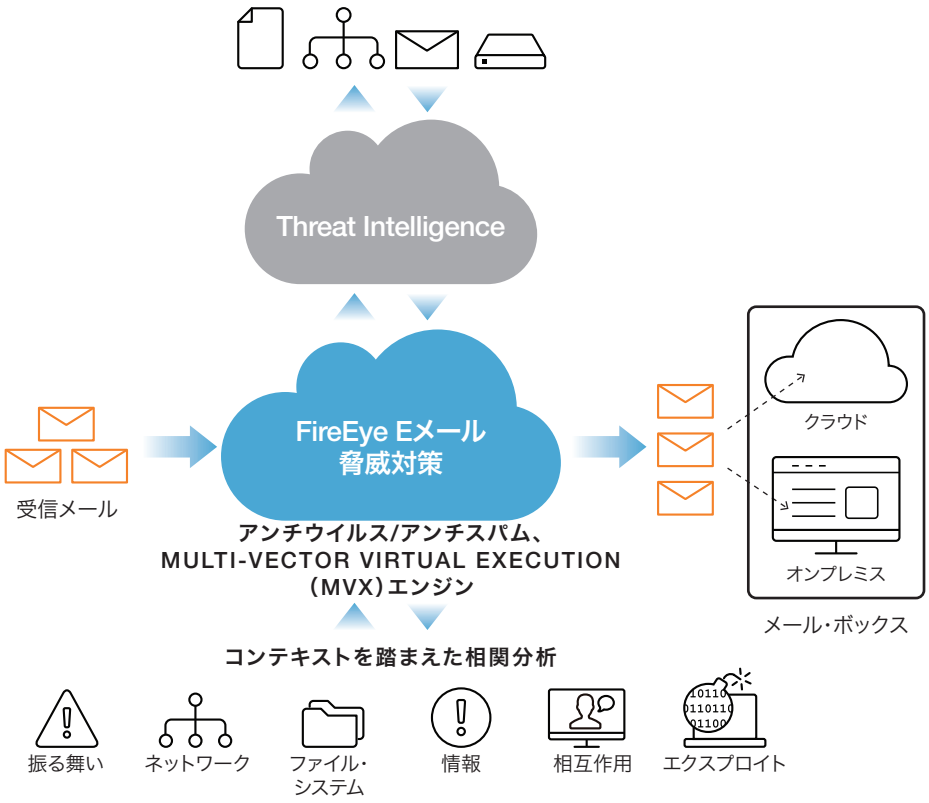

図1：FireEye Eメール脅威対策クラウド（ETP）

詳細については、FireEyeのWebサイトをご覧ください。
www.FireEye.jp

FireEyeについて

FireEye®は、インテリジェンス主導型のSecurity-as-a-Serviceのリーダー企業です。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MandiantR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、インシデントレスポンスといった、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4割以上を含む、世界67か国以上の6,000を超える組織で利用されています。

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 | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com

© 2017 FireEye, Inc. All rights reserved. FireEyeはFireEye, Inc.の商標です。
本資料のその他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。—DS.ETP.JA.052017

FireEye