Eメール脅威対策（ETP）クラウド

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プラットフォーム

データシート

ハイライト

- 高度なサイバー攻撃に対する包括的なEメール・セキュリティとアンチスパム/アンチウイルス
- ハードウェアやソフトウェアの追加導入が不要なクラウド型のソリューション
- 検証済みのアラートとともに、コンテキストに基づく具体的なインテリジェンスを提供
- 統合により、優れた運用効率を実現
- FireEyeネットワーク・セキュリティ（NX）プラットフォームとの統合により、複数の経路を使用するマルチベクタの攻撃を防御
- Eメールを解析し、ゼロデイ攻撃やアーカイブ・ファイル（ZIP/RAR/TNEF）に埋め込まれた脅威、不正なURLを使用した攻撃を検知
- EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4など、添付ファイルとして使用されるあらゆる種類のファイルを解析
- アクティブな防御モード（DNSのMXレコードを設定）、またはモニター・モード（BCCを使用）での運用に対応
- アクティブな防御モードでは、不正なEメールを隔離し、必要に応じてユーザーに通知
- セキュリティと機密性に関する「SOC 2 Type II」認定を取得

概要

スパムやウイルス、高度なマルウェアなど、Eメールを利用した脅威は増加の一途をたどっています。中でも、検知が困難なスピア・フィッシング攻撃は、APT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）を開始する主要な手段として攻撃者に使用され続けています。

FireEye®Eメール脅威対策（ETP）クラウドは、Eメールを利用した最新の高度なサイバー攻撃に対する防御機能と、アンチスパム/アンチウイルス機能の両方を提供するSaaSサービスです。クラウド型のEメール・サービスを保護する包括的なセキュリティを提供します。

Eメールを利用した攻撃は、組織宛てのEメールをETPクラウドに転送するだけで防御できます。ETPクラウドは、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FireEye Multi-Vector Virtual Execution™（MVX）エンジンを利用して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APT攻撃を防御します。

容易な導入と、FireEye環境全体との統合

導入する際に、新たなハードウェアやソフトウェアへの投資が一切不要なETPクラウドは、特に、ITインフラストラクチャのクラウドへの移行を進めている組織に最適です。ETPクラウドを使用すれば、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クラウドは、Advanced Threat Intelligence（ATI）経由でFireEye環境全体と連携し、脅威インテリジェンスをリアルタイムで共有します。コンテキストに基づく具体的なインテリジェンスの相関分析により、次に示す情報が取得できます。

- 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
- 攻撃グループの素性と目的（この情報に基づいて、ネットワークやシステム内での攻撃活動を追跡できます）
- 同種類のスピア・フィッシング・メール攻撃を受けたユーザー
- 標的となったユーザーのメール・ボックスに存在する不正なEメール
- 別の標的に転送されている不正なEメールの有無
- Eメールの配信後に不正な活動を開始したURL

優れた運用効率

高度な脅威対策と従来型のセキュリティを統合するETPクラウドは、投資の最適化、誤検知の削減、運用効率の向上を実現します。

Multi-Vector Virtual Executionエンジンをクラウドで実行

ETPクラウドは、クラウド上の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（各種Webブラウザ、Adobe Reader、Flashなどのプラグイン）で添付ファイルを実行します。オンプレミス版のFireEye Eメール・セキュリティ（EX

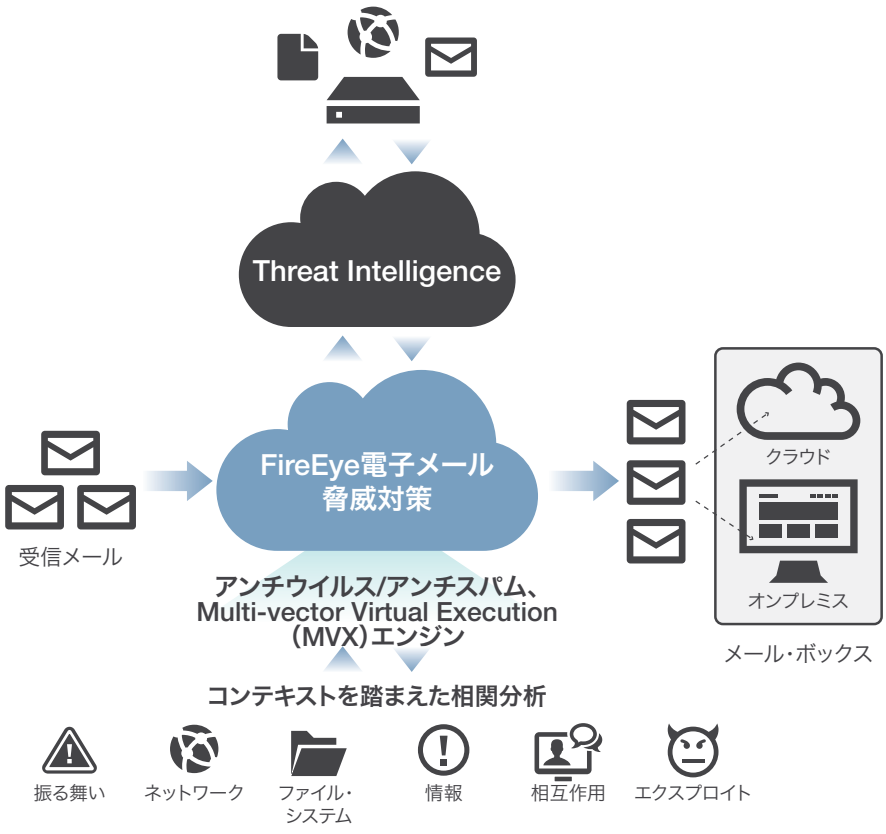
シリーズ）と同様、オペレーティング・システム、Webブラウザ、アプリケーションに存在する未知の脆弱性や、文書ファイルまたはマルチメディア・コンテンツに埋め込まれた不正なコードを利用する高度な攻撃をシグネチャなしで防御できます。

不正なEメールをリアルタイムで隔離
MVXエンジンを使用してすべての添付ファイルを解析するETPクラウドは、スピア・フィッシング・メールを正確に見つけ出し、最新の高度なサイバー攻撃を防御します。攻撃と判断されたEメールは自動的に隔離され、詳しい解析を行うか、あるいはそのまま削除するかを管理者が後から判断できます。

使い勝手に優れた管理ポータル
ETPクラウドのポータル上では、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。

EメールとWebを組み合わせた複合型の攻撃に対応
Eメールを利用した攻撃では、不正なコードを埋め込んだファイルを添付する以外にも、従来型のセキュリティ対策をすり抜けるためにEメールの本文に不正なリンクを記載してユーザーをWebサイトに誘導する、マルチベクタの攻撃手法が用いられる場合があります。ETPクラウドでは、オンプレミス版のFireEye NXプラットフォームとの連携により、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できます。

アクティブな防御モードとモニター・モードに対応
ETPクラウド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。



詳細

FireEyeは包括的なサービス・ポートフォリオを提供しています。詳細については、japan@FireEye.com 、または(03)4577-4401までお問い合わせください。

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 | TEL: 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