データシート

FireEye Eメール・セキュリティCloud エディション

Eメールを使用した攻撃を検知、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

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、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・モードへの導入に対応
- FedRAMPのセキュリティ要件を満たし、「SOC 2 Type II」認定を取得

「FireEye Eメール・セキュリティには当社が求めている保護機能が備わっていると確信しているので、攻撃の可能性を見つけるのに時間をかけることはありません。」

ショーン・ガスリー（Shaun Guthrie）氏
情報テクノロジー部門部長
Go Auto

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。攻撃成功の確率を高めるために、さまざまな創意工夫や標的の絞り込みが可能なEメールは、依然として高度な攻撃やランサムウェア攻撃を開始するための主な手段であり続けています。

FireEye Eメール・セキュリティは、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。シグネチャ・マッチングに依存しない解析技術Multi-Vector Virtual Execution™（MVX）エンジンを搭載しており、多様なオペレーティング・システム、アプリケーション、Webブラウザの組み合わせに対して、Eメールに含まれる添付ファイルやURLがどのように動作するかを解析します。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は、自社で実施したセキュリティ侵害調査や数百万台のセンサーが記録したデータに基づく、攻撃者に関する広範なインテリジェンスを収集しています。Eメール・セキュリティは、攻撃および攻撃者に関する実際の証拠と、コンテキスト情報を含むインテリジェンスを根拠に、アラートに優先度を設定し、リアルタイムで脅威をブロックします。

Eメール・セキュリティをFireEyeネットワーク・セキュリティと統合すると、広範囲に及ぶ可視化を実現し、複数の経路から実行されるマルチベクタ攻撃をリアルタイムで連携して防御できます。

セキュリティ脅威を正確に検知

Eメール・セキュリティは、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かつ速やかに検知・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。

Eメール・セキュリティの中核をなす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知して、「キル・チェーン」と呼ばれる攻撃活動のステップのうち、感染および侵害の段階でサイバー攻撃を食い止めます。

Eメール・セキュリティ – Cloud エディションでは、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メール経由の脅威を防御

最近のインターネット環境からは、さまざまな個人情報が容易に手に入ります。この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欺き、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たりします。

Eメール・セキュリティでは、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。ドメインが著名サイトと酷似した不正サイト（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することもできます。

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。Eメール・セキュリティは、解析によってさまざまなファイルやURLなどに潜むマルウェアを見つけ出します。

- 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
- パスワードが設定された、または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、著名サイトに似せた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。Eメール・セキュリティでは、発見が難しい段階的なマルウェア攻撃も検知、防御できます。

発生したアラートに効率よく対応

Eメール・セキュリティは、Eメールに含まれるすべての添付ファイルとURLを解析して、最新の高度な攻撃を正確に検知します。FireEyeのセキュリティ・エコシステム全体からの情報に基づくリアルタイムのアップデート、および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ため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、および非マルウェアベースの脅威を検知できるため、本物の攻撃への対応に専念し、運用コストを削減できます。

変化を続ける脅威トレンドに素早く適応

Eメール・セキュリティでは、脅威および攻撃者に関する詳細なインテリジェンスを利用して、Eメール経由の脅威に対する予防的なセキュリティ対策を継続的に最適化できます。攻撃者および被害者に関するインテリジェンスと、マシンで収集されたインテリジェンスの組み合わせにより、さまざまな効果が実現します。

- 脅威に対するタイムリーかつ広範囲に及ぶ可視化
- 検知されたマルウェアや不正な添付ファイルの機能および特徴の把握
- 対応優先度の判断と作業の効率化を可能にするコンテキスト情報の提供
- 攻撃者の素性と目的の推定、組織内での攻撃活動の追跡
- 過去のスピア・フィッシング攻撃の遡及的な検知と、不正なURLの通知によるフィッシング・サイトへのアクセス防止

Eメール・セキュリティのポータル上では、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

Eメール・セキュリティ – Cloud エディションはクラウドベースであるため、ハードウェアもソフトウェアもインストール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。

Eメール・セキュリティ – Cloud エディションは、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できます。

Eメールを使用した攻撃は、組織宛てのEメールをEメール・セキュリティに転送するだけで防御できるようになります。Eメール・セキュリティは、まずEメールを解析し、スパムの可能性や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・モードに対応

Eメール・セキュリティ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。防御モードを使用する場合は、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

Eメール・セキュリティは、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集中管理システムは、Eメール・セキュリティとネットワーク・セキュリティ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、Eメール・セキュリティ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

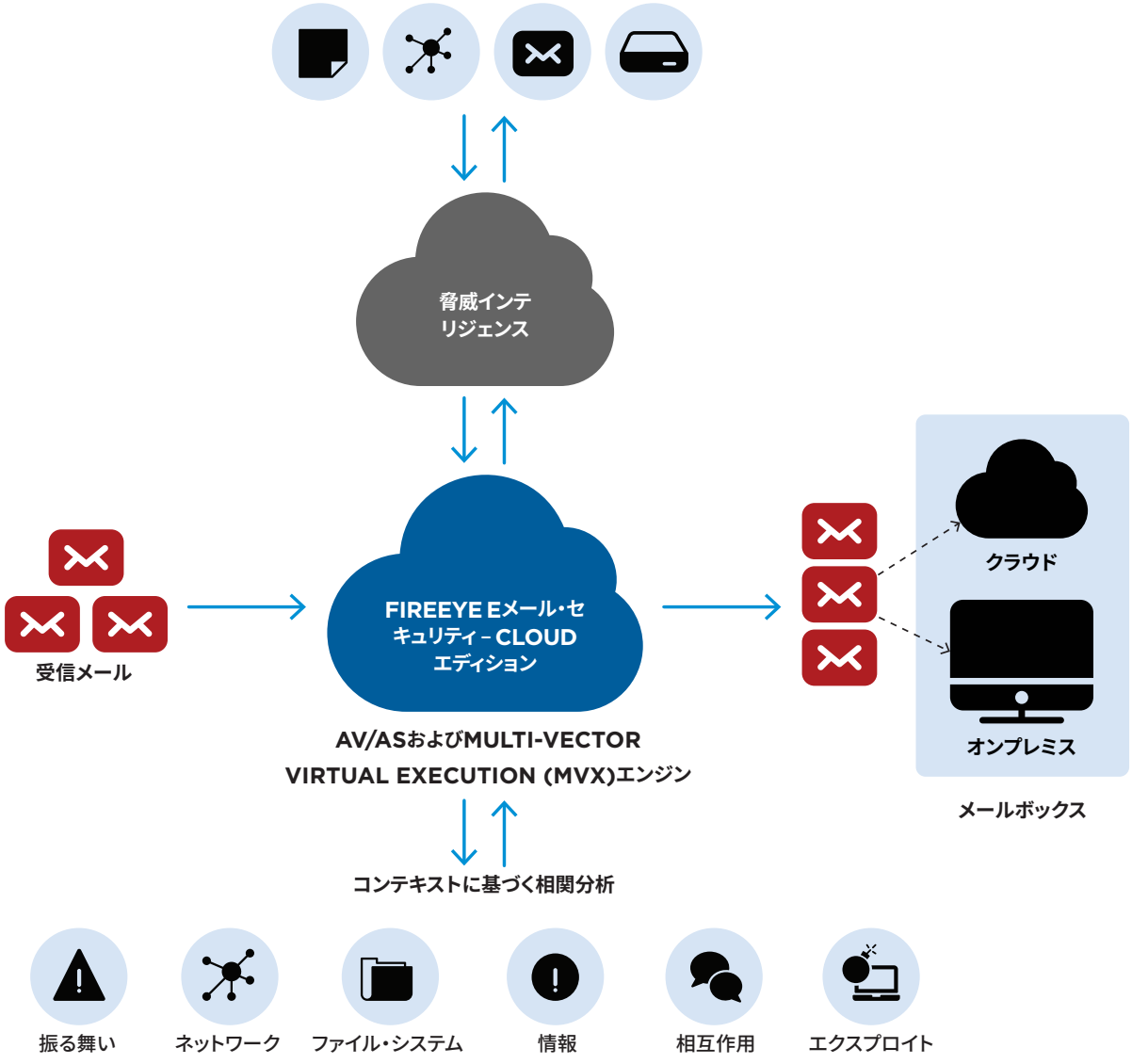
FedRAMP

Eメール・セキュリティ – Cloud エディションは、行政および公立教育機関が運営するクラウド・サービスを対象とするFedRAMPのセキュリティ要件を満たしています。

SOC 2 Type II

Eメール・セキュリティ – Cloud エディションは、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。

FireEye Eメール・セキュリティ – Cloud エディション



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。