FireEye Eメール・セキュリティ（EXシリーズ）

柔軟性と拡張性に優れたインテリジェントな
Eメール脅威対策

EX 5400およびEX 8420（このほかにEX 3400とEX 8400をラインナップ）

概要

FireEye Eメール・セキュリティ（EXシリーズ）は、Eメールによる高度な攻撃を防御するソリューションです。FireEyeのグローバル脅威管理プラットフォームの主要コンポーネントであり、シグネチャ・マッチングに依存しない技術ですべての添付ファイルを解析し、高度な標的型攻撃で使用されるスピア・フィッシング・メールを隔離します。

今日のインターネットでは、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だまし、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。FireEye　Eメール・セキュリティは、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、認証情報を狙うフィッシング攻撃をリアルタイムで防御します。またFireEye　Network　Security（NXシリーズ）との統合により、複合型の攻撃に対する高度な脅威対策が実現し、不正なURLが記載されたEメールの隔離や、Webベースの攻撃とその元になったスピア・フィッシング・メールの関連付けをすることができます。

ハイライト

- Eメールに対するスピア・フィッシング攻撃を防御
- 認証情報を狙うフィッシング攻撃を自動的に検知、防御
- 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
- FireEye Network Securityとの統合により、複数の経路を使用するマルチベクター攻撃を防御
- 段階的に実行され、検知が困難なマルウェア・キャンペーンを検知、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
- パスワード保護やサンドボックス回避などの手法を備えた攻撃から保護
- アクティブな防御モード（MTAとして導入）とモニター・モード（スパン/BCCの宛先として導入）に対応
- 不正なEメールを隔離してユーザーに通知（通知はオプション）
- 脅威をリアルタイムおよび遡及的に検知
- 発生したアラートを具体的な
- 脅威インテリジェンスと関連付け
- メッセージの可視化、追跡、管理機能を提供

FireEye
SECURITY REIMAGINED

不正なEメールをリアルタイムで隔離

FireEye Eメール・セキュリティは、最新の高度なサイバー攻撃の正確な検知を目的とする専用技術FireEye Multi-Vector Virtual Execution (MVX) エンジンを使用してすべての添付ファイルとURLを解析し、スピア・フィッシング・メールを見つけ出します。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。

WebとEメールを組み合わせた複合型の攻撃に対応

高度なサイバー攻撃の多くは複数の経路を使用しますが、攻撃の第1段階として、スピア・フィッシング・メールが使われます。FireEye Eメール・セキュリティをFireEye Network Securityおよび集中管理システム・シリーズ (CMシリーズ) と組み合わせて使用すると、不正なURLを最初に使用されたEメールや標的のユーザーと関連付け、攻撃のライフサイクル全体を明らかにできます。FireEye集中管理システムはこの結果に基づき、新しいマルウェアに関するインテリジェンスをローカルのFireEye環境全体にリアルタイムで配信します。

Eメールを悪用したゼロデイ攻撃をリアルタイムで解析

FireEye Eメール・セキュリティは、シグネチャ・マッチングに依存しないMVXエンジンを使用して、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脆弱性や、一般的な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ブロックします。MVXエンジンはその後、バッファ・オーバーフロー攻撃などで悪用されている脆弱性や、外部へのデータ送信に使用されるコールバック先などの情報をレポートします。

ネットワーク全体で脅威インテリジェンスを共有

FireEye集中管理システム・プラットフォームを導入している場合、ダイナミックに生成されたリアルタイムの脅威インテリジェンスをすべてのFireEye製品で共有し、ローカル・ネットワークの保護に利用できます。

またこのインテリジェンスは、FireEye Dynamic Threat Intelligence™ (DTI) クラウドを介して世界規模で共有され、同クラウドに参加するすべてのFireEyeプラットフォームに新しい脅威の情報が行き渡ります。

YARAベースのルールでカスタマイズに対応

カスタムYARAルールをサポートしているFireEye Eメール・セキュリティは、独自のテスト済みルールでEメールの添付ファイルを解析し、特定の組織を狙った脅威を見つけ出すことができます。

技術仕様

	EX 3400	EX 5400	EX 8400	EX 8420
パフォーマンス*	最大15万通/日	最大30万通/日	最大60万通/日	最大60万通/日
ネットワーク・インタフェース・ポート	10/100/1000BASE-Tポート x 2	10/100/1000BASE-Tポート x 2	10/100/1000BASE-Tポート x 2	1000BASE-SX光ファイバ 2ポート (LCマルチモード)
管理ポート	10/100/1000BASE-Tポート x 1	10/100/1000BASE-Tポート x 1	10/100/1000BASE-Tポート x 1	10/100/1000BASE-Tポート x 1
IPMIポート (背面パネル)	搭載	搭載	搭載	搭載
前面パネルLCDおよびキーパッド	搭載	搭載	搭載	搭載
PS/2キーボードおよびマウス用ポート、DB15 VGAポート (背面)	搭載	搭載	搭載	搭載
USBポート (背面パネル)	Type A USB 2ポート	Type A USB 2ポート	Type A USB 2ポート	Type A USB 2ポート
シリアル・ポート (背面パネル)	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット	115,200 bps、パリティなし、8ビット、1ストップ・ビット
ストレージ容量	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応	600 GB HDD 2台、RAID 1、2.5インチ、フィールド交換対応
エンクロージャ	1RU、19インチ・ラックに適合	1RU、19インチ・ラックに適合	1RU、19インチ・ラックに適合	1RU、19インチ・ラックに適合
シャーシの寸法 (幅×奥行×高さ)	437×706×43.2 mm	437×706×43.2 mm	437×711×86.6 mm	437×711×86.6 mm
AC電源	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60Hz、IEC60320-C14インレット、フィールド交換対応	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60Hz、IEC60320-C14インレット、フィールド交換対応	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60Hz、IEC60320-C14インレット、フィールド交換対応	冗長 (1+1) 750ワット、100～240 VAC、9-4.5 A、50-60 Hz、IEC60320-C14インレット、フィールド交換対応
DC電源	非搭載	非搭載	非搭載	非搭載
消費電力 (最大) (ワット)	296W	468W	509W	509W
熱放散 (最大) (BTU/時)	1,010 BTU/時	1,597 BTU/時	1,737 BTU/時	1,737 BTU/時
平均故障間隔 (時)	35,400時間	34,600時間	59,800時間	59,800時間
重量 (アプライアンスのみ/梱包時)	14 kg / 21 kg	15 kg / 21 kg	19 kg / 26 kg	19 kg / 26 kg
セキュリティ認定	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1
温度 (動作時)	10°C～35°C	10°C～35°C	10°C～35°C	10°C～35°C
相対湿度 (動作時)	10%～85% (結露なきこと)	10%～85% (結露なきこと)	10%～85% (結露なきこと)	10%～85% (結露なきこと)
動作高度	1,500 m	1,500 m	1,500 m	1,500 m

注：パフォーマンス値は、システム構成や処理するトラフィックの特性によって異なります。

具体的な脅威インテリジェンス

FireEye Eメール・セキュリティのアラートをオプション・サービスのFireEye Advanced Threat Intelligence (ATI) ポータルで解析すると、Eメールの送信元や深刻度、リスクの程度、対応策など、そのEメール攻撃のコンテキスト情報を入手できます。このポータルには統計情報が視覚的にわかりやすく表示されるため、セキュリティ担当者は重要なコンテキストやトレンドを素早く確認できます。

FireEyeからのさらなる詳細情報を希望される場合は、ATI+をご利用いただけます。ATI+をご利用のお客様はFireEye Intelligence Center (FIC) にアクセスし、継続的な監視を実現できます。

FICでは、高度なサイバー攻撃の実行者に関する一連の調査情報、トレンド、ニュース、解析情報に加え、標的とされている業種のプロファイル情報が提供されます。継続的な監視を追加すると、FireEyeのアナリストが24時間体制で重要なアラートおよび検知性能を監視します。

メッセージ・キューの管理

FireEye Eメール・セキュリティでは、検査対象のEメール・メッセージをきめ細かく制御できます。アクティブな防御モードで運用している場合は、MTAキューを移動するメッセージの追跡と管理、Eメール属性によるメッセージの検索と検証 (メッセージの受信、解析、次のホップへの転送が完了しているかどうかなど) 、使いやすいダッシュボードを利用したトレンド追跡を行えます。また、明示的な許可リスト、ブロック・リストを設定すると、Eメールの処理方法をカスタマイズできます。

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825社を含む、世界67か国以上の5,300を超える組織で利用されています。

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

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

FireEye