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

図1：EX 3500、EX 5500、EX 8500

概要

日々膨大な数がネットワークを出入りするEメールは、攻撃者にとって最も利用しやすい攻撃手段となっています。スパム・メールやウイルス、高度な脅威、標的型攻撃など、組織が直面するセキュリティ上の課題は増加する一方ですが、攻撃の多くは、不正な添付ファイルまたはリンクを含むEメールや、認証情報の窃取を目的とするフィッシング・メールを送りつけるところから始まります。スパム・フィルターやアンチウイルス・ソフトウェアは、既知の不正な添付ファイルやリンク、コンテンツを含む、大量送信型のフィッシング・メールには一定の効果を発揮します。しかし、従来型のソリューションをすり抜けるように作られた高度な攻撃や標的型のスピア・フィッシング攻撃は検知できません。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。オンプレミス向けアプライアンスのEXシリーズは、スピア・フィッシングやランサムウェアなどの高度な攻撃や標的型攻撃を正確に検知し、ネットワークの手前で即座にブロックします。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。高い精度で脅威を検知し、誤検知は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・セキュリティおよびエンドポイント・セキュリティと組み合わせて使用すると、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。

ハイライト

- スピア・フィッシングなど、段階的に実行される高度な攻撃やゼロデイ攻撃に対する包括的なEメール・セキュリティ機能を提供
- Eメール・スループットのピーク期間中は、クラウド・バースト機能で検知および解析のリソースを追加
- Microsoft WindowsおよびApple Mac OS Xオペレーティング・システム・イメージでの解析をサポート
- Eメールを解析し、ファイルに潜む脅威を検知。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や不正なURLに対応
- 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情報に基づいて脅威の優先度を判断、封じ込め
- FireEyeの各種テクノロジーと統合
- アクティブな防御モードまたはモニター・モードでオンプレミスに導入
- メッセージとアラートの可視化、追跡、管理機能を提供

セキュリティ脅威を正確に検知

FireEye 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となる技術は、Multi-Vector Virtual Execution™ (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を行う手法で、ゼロデイ攻撃や複数のフローにわたる攻撃など、発見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・スループットのピーク期間中は、FireEye MVX Smart Gridへのクラウド・バーストにより、Eメール経由の脅威を検知、解析するためのリソースを追加できます。

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。

- 添付ファイル (対応するファイル形式の一例：EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4、ZIP/RAR/TNEFアーカイブ)
- 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メールに含まれるURL、Microsoft Office文書、PDFおよびアーカイブ・ファイル (ZIP、ALZip、JAR) 、その他のファイル形式 (UUエンコード、HTML)
- URL経由でダウンロードされたファイル
- 難読化されたURL、偽装されたURL、短縮URL、リダイレクト先URL
- 認証情報を狙うフィッシング、著名サイトに似せたURL
- Microsoft WindowsおよびApple Mac OS Xオペレーティング・システム・イメージ、Webブラウザ、アプリケーションの未知の脆弱性
- 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

ランサムウェア攻撃はEメールから始まりますが、多くの場合、データを暗号化するためにC&Cサーバーとの通信が必要となります。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。また、リスクウェアの個別検知により、本物のセキュリティ侵害の試みと、悪質性は低いものの好ましくない活動 (アドウェアやスパイウェアなど) を区別して、アラート対応の優先度を判断できます。

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

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。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エンジンを利用してすべての添付ファイルと本文中のURLを解析し、高度な攻撃をリアルタイムで防御します。

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Eメール・セキュリティに転送し、MVXエンジンで解析します。

一段上のレベルのセキュリティ・オペレーションを実現

Eメール・セキュリティは、FireEye Helixを構成するコンポーネントの1つであり、FireEye集中管理システムと連携します。

- FireEye Helixの一部として、脅威の検知から撃退までを迅速かつ低コストで実施できるよう組織を支援します。
- FireEye集中管理システムは、Eメール・セキュリティとFireEye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。

YARAベースのルールでカスタマイズに対応
Eメール・セキュリティは、カスタムYARAルールをサポートしています。このため、独自のルールでEメールの添付ファイルを解析し、特定の組織を狙った標的型の脅威を見つけ出すことができます。

メッセージ・キューとアラートおよび隔離メッセージの管理
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とブロック・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。一般的なアラート属性の検索と選択、アラートおよび隔離したメッセージに対する一括処理を行うことも可能です。

表1：技術仕様

	EX 3500	EX 5500	EX 8500
パフォーマンス*	処理可能な添付ファイル（ユニーク・ファイル）数：最大700個/時	処理可能な添付ファイル（ユニーク・ファイル）数：最大1,800個/時	処理可能な添付ファイル（ユニーク・ファイル）数：最大2,650個/時
ネットワーク・インタフェース・ポート	1GigE BaseT 2ポート	1GigE BaseT 2ポート	SFP+ 4ポート、1GigE BaseT 2ポート
管理ポート	LSI9341-4i、1GigE BaseT 2ポート	LSI9341-4i、1GigE BaseT 2ポート	LSI9341-4i、1GigE BaseT 2ポート
IPMIによるモニタリング	サポート	サポート	サポート
PS/2キーボードおよびマウス、DB15 VGAポート（背面パネル）	搭載	搭載	搭載
USBポート（背面パネル）	USB2 2ポート、USB3 2ポート	USB2 2ポート、USB3 2ポート	USB2 2ポート、USB3 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
ストレージ容量	2TB 4台、RAID 10、3.5インチHDD、フィールド交換対応	2TB 4台、RAID 10、3.5インチHDD、フィールド交換対応	2TB 4台、RAID 10、3.5インチHDD、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	2RU、19インチ・ラックに適合	2RU、19インチ・ラックに適合
シャーシの寸法（幅×奥行×高さ）	437×650×43.2 mm	438×620×88.4 mm	438×620×88.4 mm
AC電源	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	冗長（1+1）800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	冗長（1+1）800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
熱出力（最大）（BTU/時）	245ワット（836 BTU/時）	456ワット（1,556 BTU/時）	530ワット（1,808 BTU/時）
平均故障間隔（時）	54,200	19,970	11,880
重量（アプライアンスのみ/梱包時）	13.6 kg/18.6 kg	20.0 kg/29.6 kg	20.2 kg/29.8 kg
安全性に関する適合規格	UL 60950-1-2014; CAN/CSA C22.2 No. 60950-1-07、Am.1:2011+Am.2:2014; AS/NSZ 60950.1- 2011	EN 60950-1、1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013	EN 60950-1、1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013

表1：技術仕様

	EX 3500	EX 5500	EX 8500
EMCの適合規格	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN55022 Class A; VCCI V-3 Class A; EN 55024; EN 61000-3-2 Class A; EN 61000-3-3; CNS 13438 (2006) Class A; CISPR22 Class A; AS/NZS CISPR 22 Class A; KN 32; KN 35	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;
セキュリティ認定**	FIPS 140-2、CC NDPP v1.1	FIPS 140-2、CC NDPP v1.1	FIPS 140-2、CC NDPP v1.1
環境規制への対応	RoHS、REACH、WEEE	RoHS、REACH、WEEE	RoHS、REACH、WEEE
温度（動作時）	0～35° C（32～95° F）	0～35° C（32～95° F）	0～35° C（32～95° F）
相対湿度（動作時）	10～95% @ 40° C（結露なきこと）	10～95% @ 40° C（結露なきこと）	10～95% @ 40° C（結露なきこと）
動作高度	1,500 m	1,500 m	1,500 m

* パフォーマンス値は、システム構成や処理する E メール・トラフィックの特性によって異なります。1 時間あたりに受信する実際の添付ファイル（ユニーク・ファイル）数に基づいてアプライアンスを選択してください。
** 検証中

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®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。