FireEye Eメール・セキュリティ - Serverエディション

Eメールがきっかけとなる脅威に、今求められる対策

ハイライト

- 不正な添付ファイル、フィッシング・サイトのURL、なりすまし攻撃、ゼロデイ攻撃、段階的な攻撃等に対応した、統合Eメール・セキュリティ・アプライアンス
- Microsoft WindowsおよびApple macOS Xのオペレーティング・システム・イメージに対する解析をサポート
- パスワード保護や暗号化が施された添付ファイルや、本文および添付ファイル内のURLを解析
- FireEye DTIクラウドからリアルタイムの脅威情報を取得
- アラートにコンテキスト情報を付加することで攻撃の全容を把握しやすくし、対応の優先順位付けを可能に
- 統合型もしくは分散型のMVXを使用し、オンプレミスに導入

図1: 統合型Eメール・セキュリティ・アプライアンス(EX 3500、EX 5500、EX 8500)

概要

Eメールは、攻撃者にとっては格好の入り口です。なぜなら、今、多くの情報はメールを通じて入ってくるからです。スパムやウイルス、高度なマルウェアなど、Eメールを利用した攻撃は増加の一途をたどっています。高度なサイバー攻撃の大半は、認証情報を窃取するフィッシング・サイトへのURLが仕込まれたメールや、一見通常のファイルに見えるものの実際には不正なコードが仕込まれたファイルが添付されたメールなどをきっかけに発生しています。Eメールは、標的に向けた作り込みが容易で攻撃が成功しやすいため、攻撃者はEメールを攻撃手段としてよく利用する傾向があります。

FireEye Eメール・セキュリティは、高度なEメール攻撃による侵害の発生リスクを最小限に抑えます。FireEye Eメール・セキュリティServerエディションは、オンプレミス展開用のハードウェア・アプライアンスです。本製品は、URLや不正添付ファイルなどを用いたEメール攻撃から組織を守ります。脅威インテリジェンスに基づくコンテキストと検知プラグインの組み合わせにより、ビッグデータに基づく拡張性に富んだプラットフォーム上で、URLの有害/無害を判断します。シグネチャを用いないサンドボックス型検知エンジン、Multi-Vector Virtual Execution(MVX)エンジンは、さまざまなOS、アプリケーション、ブラウザを搭載した環境に対応しており、添付ファイルやURLを動的解析します。また、誤検知も最低限に抑えられます。

FireEyeは、請け負った数多くのセキュリティ侵害調査や、世界中で利用されている数百万台の製品をセンサーとして収集したデータに基づき、幅広い脅威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、リアルタイムで脅威をブロックしつつ、攻撃および攻撃者に関する具体的な証拠と、コンテキスト情報を含むインテリジェンスに基づいてアラートに優先度を設定します。

FireEyeのEメール・セキュリティ、ネットワーク・セキュリティおよびエンドポイント・セキュリティの3製品を併せて利用することで、複数の経路から実行されるマルチベクタ攻撃を視野に入れた、リアルタイムの対策が実施できるようになります。

Eメールに端を発する脅威への対策

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、認証情報を狙うフィッシング攻撃や送信者のなりすまし攻撃、スピア・フィッシング攻撃などを、リアルタイムで検知、防御します。もし攻撃が確認されれば、そのEメールを隔離します。

- 解析対象となる添付ファイル形式の例： EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4、ZIP/RAR/TNEFアーカイブ) など
- 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
- パスワードが設定された添付ファイルで、パスワードが画像化されて送付されるもの
- Eメールに埋め込まれたURL、Microsoft Officeドキュメント、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をクリックすることでダウンロードされるファイル (FTPにも対応)
- 検知回避策を施されたURL： 難読化URL、偽装URL、短縮URL、ダイナミックURLなど
- 認証情報を狙うフィッシング、著名サイトに似せたURL (タイポスクワッティング)
- 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C&Cサーバーへのコールバック通信を発生させます。Eメール・セキュリティは、このように複数段階に分けて展開される攻撃も検知、防御します。

優れた脅威検知

Eメール・セキュリティは、標的型攻撃や、正常な通信を装って検知回避しようとする攻撃を特定、隔離することで、甚大な被害をもたらしかねない攻撃から組織を守ります。攻撃は検知されると直ちにブロック、解析され、特徴 (フィンガープリント) を抽出して同様の攻撃を素早く検知するために利用します。

Eメール・セキュリティは、主にAdvanced URL Defense、MVXエンジン、MalwareGuardによって構成されます。機械学習および機械分析を活用するこれらの技術は、シグネチャやポリシーに基づく従来型対策を回避する攻撃の特定に役立ちます。

PhishVisionは、著名なサイトを装ったフィッシング・サイトへの誘導を行うURLの検知を行う機能です。狙われがちな数々の著名サイトのスクリーンショットを画像として取りまとめ、ディープラーニングをもとにEメールに記載されたURLが参照するWebページのイメージと比較し、正当なサイトへのリンクであるかを判断します。PhishVisionと共に動作するKrakenは、ドメインとページ・コンテンツを解析し、機械学習を強化します。Skyfeedも高度なURL検知技術の一つです。これは、専用に開発された自動マルウェア情報収集システムで、検知漏れをなくすために、ソーシャル・メディア・アカウント、ブログ、フォーラム、脅威フィードを収集します。Advanced URL Defenseは、Eメール・セキュリティによって保護された組織に、認証情報の収集とスピア・フィッシング攻撃に対して優れた防御を提供します。

MalwareGuardは、AIベースの未知脅威検知エンジンです。バイナリ・ファイルに対する疑わしさのレベルをスコア化します。通信上で見つかったすべてのPE (Portable Executable) ファイルは、MalwareGuardによって解析され、出力されたスコアに基づいて不正であるかが判断され、不正なものとして検知されたものには名前付けがなされます。

MVXエンジンは隔離された仮想環境で疑わしいコードを実行し、シグネチャを用いない動的解析を行います。ゼロデイ攻撃や段階的な攻撃などの発見が困難な攻撃や、未知のエクスプロイトや未知のマルウェアの検知を行います。

検知回避対策

Eメール・セキュリティは、管理された環境下でのライブ・モード機能により、リモート・オブジェクトに対する要求を回避する攻撃から防御します。MVXエンジンは、複数のダウンロードを要求するマルウェアを検知し、サンプル・バイナリによって要求されたリモート・オブジェクトを返します。管理された環境下でのライブ・モードは、段階的なダウンロード、高度なスピア・フィッシング攻撃、高度なランサムウェア侵入に対する検知漏れを減らします。

URL検知回避技術に対しては、進化を続けるAdvanced URL Defenseにより、検知回避対策を行っています。また、サンドボックスにGuest Imageを用意することで、不正なオブジェクトの回避策を回避することができます。Guest Imageとは、実際に存在するエンドポイントを模した環境であり、カスタマイズが可能です。Guest Imageには、エンドポイント・ドメイン、ドメイン・ユーザー、Outlookデータ、ブラウザ履歴などの要素が含まれます。

効率的なアラート・ハンドリング

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を解析します。世界中で利用されているFireEye製品が収集する脅威情報と、検知された攻撃のアラートの背景にいる攻撃グループを関連付けて考察することで、アラートの対応優先度を的確に判断し、効率的な対処が可能になります。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、リスクウェア検知は、本物のセキュリティ侵害と、アドウェアやスパイウェアなどを区別し、対応を優先すべきアラートを明確化します。

変化を続ける脅威トレンドに対する素早い適応

FireEye Eメール・セキュリティは、FireEye Dynamic Threat Intelligence（DTI）から収集されるリアルタイムの脅威インテリジェンスを通じて最適化し、お客様の環境を、メールをきっかけとした脅威からプロアクティブに保護します。脅威と攻撃者に関する詳細なインテリジェンスでは、攻撃者、感染マシン、被害者に関する情報を組み合わせて、以下を実現します。

- 脅威に対するタイムリーかつ広い視野
- 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特定
- 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
- Eメールに埋め込まれたすべてのURLを書き換え、悪意のあるリンクからユーザーを保護
- 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をハイライトすることでフィッシング・サイトへのアクセスを防止

対応ワークフローの統合

Eメール・セキュリティは、FireEye HelixおよびFireEye Central Managementとシームレスに連携します。

- セキュリティ・オペレーション・プラットフォームであるFireEye Helixは、インフラストラクチャ全体を可視化します。インテリジェンス、エンドポイントの相関分析、自動化、調査情報により、Eメールとサードパーティのアラートに情報を補完するFireEye Helixは、未知の脅威を可視化するとともに、セキュリティ担当者の意思決定を支援します。
- Central Managementは、Eメール・セキュリティとネットワーク・セキュリティ双方のアラートを相関分析して攻撃の全体像を解明し、被害の拡大防止のためのブロック・ルールを設定します。
- Central Managementは、標的を特定するためのロールベースのタグ機能を持っています。
- Central Managementは、役割別の基準に基づくアラートの対応と復旧をサポートしています。

さらなる機能

YARAルールのカスタマイズ

アナリストは、Eメール・セキュリティによってカスタム・ルールを設定およびテストすることで、自身の組織を標的とした添付ファイルの分析を行うことが可能になります。

経営幹部へのなりすまし対策

Eメール・セキュリティ Serverエディションのビジネスメール詐欺（BEC）対策機能により、従業員をなりすましメールから守ることができます。管理者はまず、ポリシーを作成します。次に、メールを受信した時にEメールの表示名やヘッダ情報がポリシーと比較され、なりすましメールかどうかの判断を行います。

メッセージ・キュー、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 Serverエディションでは、検査対象となる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では、MTAキューを移動するメッセージの追跡と管理を行います。Eメール属性は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）に使用され、ダッシュボードからモニタリングできます。また、許可リストとブロック・リストの設定により、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。

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。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、解析します。

柔軟な導入形態

Eメール・セキュリティServerエディションには、組織のニーズや予算に合わせたさまざまな導入方法があります。

- **統合型Eメール・セキュリティ：** MVXサービスと統合されたスタンドアロン型のオールインワン・ハードウェア・アプライアンスは、単一拠点のEメール対策に最適です。導入も管理も容易です。ルールやポリシーの設定、チューニングも必要ありません。
- **分散型Eメール・セキュリティ：** MVXサービスを複数のアプライアンスで共有する、拡張可能な展開方法で、複数拠点など、複数のEメール受信ポイントがある場合に適しています。
- **Email Smart Node：** Eメール・トラフィックを解析する仮想センサーです。不正なトラフィックを検知してブロックし、疑わしいトラフィックについては、詳細な解析のため、暗号化接続経由でMVXサービスに転送します。
- **MVX Smart Grid：** オンプレミスで集中管理する、柔軟性に優れたMVXサービスです。拡張性、耐障害性、自動ロード・バランシングの機能を備えています。

  Eメール・トラフィックが瞬間的に増加した場合には、アプライアンスからMVX Smart Gridへ解析をバーストすることにより、一時的に解析キャパシティを拡張できます。
- **FireEye Cloud MVX：** サブスクリプション形式のMVXサービスであるCloud MVXは、トラフィックの解析をEmail Smart Nodeで実施し、プライバシーを担保します。このうち、疑わしいオブジェクトのみが暗号化接続でMVXサービスに転送され、MVXサービスで無害と判定されたオブジェクトはその場で破棄されます。

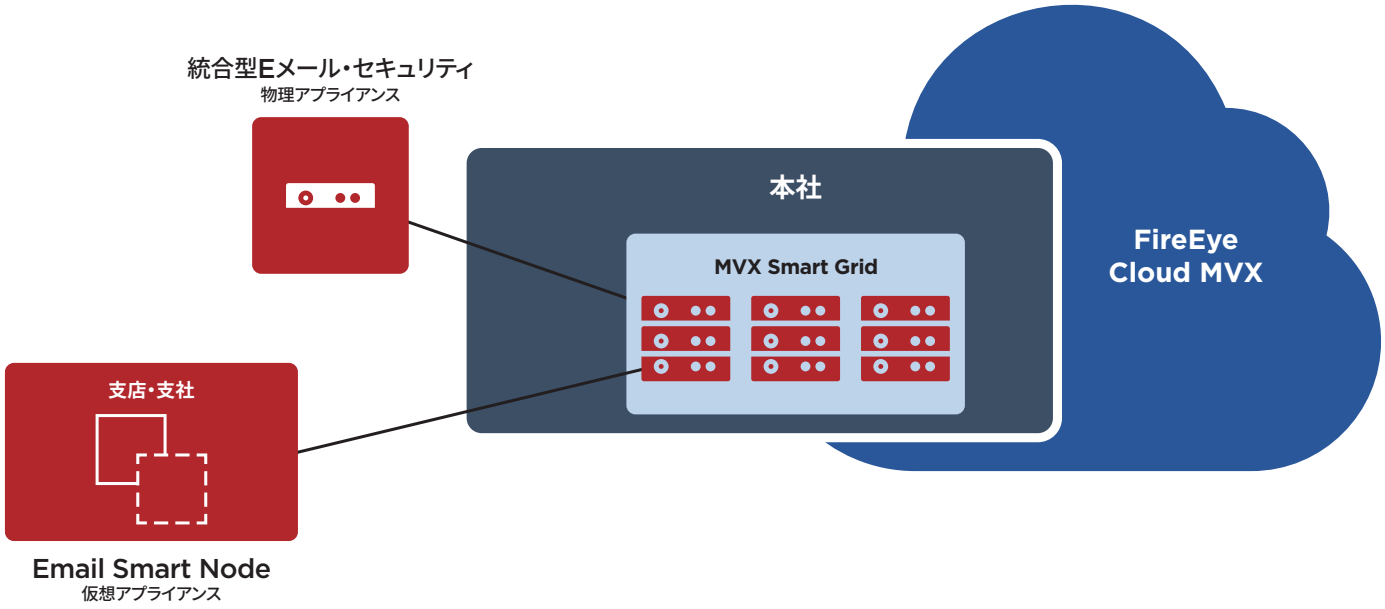

図2： Eメール・セキュリティの分散/バースト対応導入モデル

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+（10GigE光ファイバ、10GigEカッパー、1GigEカッパー）4ポート、1GigE BaseT 2ポート
管理ポート	1GigE BaseT 2ポート	1GigE BaseT 2ポート	1GigE BaseT 2ポート
IPMIによるモニタリング	搭載	搭載	搭載
VGAポート（背面パネル）	搭載	搭載	搭載
USBポート（背面パネル）	USB Type A 4ポート（背面）	USB Type A 2ポート（前面）、 USB Type A 2ポート（背面）	USB Type A 2ポート（前面）、 USB Type A 2ポート（背面）
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）750W、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）800W、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）800W、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）	245W（836 BTU/時）	456W（1,556 BTU/時）	530W（1,808 BTU/時）
平均故障間隔（時）	5万4,200時間	5万7,401時間	5万3,742時間
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	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
EMCの適合規格	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
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指令2011/65/EU、REACH、WEEE指令2012/19/EU	RoHS指令2011/65/EU、REACH、WEEE指令2012/19/EU	RoHS指令2011/65/EU、REACH、WEEE指令2012/19/EU
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	3,000 m / 9,842 ft	3,000 m / 9,842 ft	3,000 m / 9,842 ft

* 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。

表2： FireEye MVX Smart Gridの仕様

	VX 5500	VX 12550
サポートするOS	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
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480個/時	処理可能な添付ファイル（ユニーク・ファイル）数： 最大3,780個/時
高可用性**	N+1	N+1
管理ポート（背面パネル）	10/100/1000 Mbps BASE-T 1ポート	10/100/1000 Mbps BASE-T 1ポート
クラスタ・ポート（背面パネル）	10/100/1000 Mbps BASE-T 3ポート	10/100/1000 Mbps BASE-T 1ポート、 10 Gbps BASE-T 2ポート
IPMIポート（背面パネル）	搭載	搭載
前面LCD/キーパッド	非搭載	搭載
VGAポート	搭載	搭載
USBポート（背面パネル）	Type A USB 4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
ディスク容量	2 TB 3.5インチSAS HDD 2台、RAID 1、 ホットスワップ対応、フィールド交換対応	4 TB 3.5インチSAS-3 HDD 4台、RAID 1、 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
シャーシの寸法（幅×奥行×高さ）	437×650×43.2 mm	437×851×89 mm
DC電源	非搭載	非搭載
AC電源	冗長電源（1+1）750W、100～240 VAC、8-3.8 A、 50-60 Hz、IEC60320-C14、インレット、ホットスワップ 対応、フィールド交換対応	冗長電源（1+1）800W： 100-127V、9.8A-7A 1000W： 220-240V、7-5A、50-60 Hz、フィールド交換対応 IEC60320-C14インレット、フィールド交換対応
消費電力（最大）	285W	760W
熱放散（最大）	972 BTU/時	2,594 BTU/時
平均故障間隔（MTBF）	5万4,200時間	3万8,836時間
重量（アプライアンスのみ/梱包時）	15 kg/21.8 kg	21 kg/40.2 kg
セキュリティ認定	FIPS 140-2レベル1、CC NDPP v1.1	FIPS 140-2レベル1、CC NDPP v1.1
安全性に関する適合規格	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* 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。

** 適切な冗長ハードウェア構成を使用。

表3： Email Smart Node（仮想センサー）の仕様

	EX 5500V
サポートするOS	Microsoft Windows、Apple macOS X
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1,250個/時
ネットワーク・モニター・ポート	2ポート
ネットワーク管理ポート	2ポート
CPUのコア数	8
メモリ	16 GB
ディスク容量	384 GB
ネットワーク・アダプタ	VMXNet 3、vNIC
サポートするハイパーバイザ	VMware ESXi 6.0以降

* 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。

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
テラススクエア8階 | 03−4577−4401 |
Japan@fireeye.com

FES-EXT-DS-JA-JP-000044-02

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、インシデント対応といった、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