

## GSXから新サービス「FireEye 製品アラート解析サービス」正式リリース

---

グローバルセキュリティエキスパート株式会社（本社：東京都港区西新橋1-2-9、代表取締役社長：松本 松仁、<http://www.gsx.co.jp>）は、同社アドバンスドテクノロジーサービス（ATS事業部）の新ラインナップとして、2013年12月25日に「FireEye製品アラート解析サービス」をサービスリリースしました。

FireEye製品アラート解析サービスは、FireEye製品専用のインシデント運用支援サービスです。お客様に代わって、GSXの専門コンサルタントが発生したアラートの内容を解析・評価し、迅速且つ最適なインシデント対応をサポート致します。

近年、標的型攻撃をはじめとするサイバー攻撃は依然として沈静化することなく、被害が増大し続けています。トレンドでは、標的型攻撃の見えない化が深刻化しており、標的型メールを介してマルウェアを仕込ませたり、ドライブバイダウンロード手法を用いてWeb改ざんを行う高度な脅威に晒されています。このような背景の中、標的型攻撃などを阻止する防御対策を行い、ソリューションを用いて身構える必要があります。

### ◆標的型攻撃対策ソリューションFireEyeとは

FireEyeはゼロデイ攻撃や標的型攻撃からシステムを保護する、次世代の脅威対策ソリューションです。ファイアウォールやIPS、アンチウイルスなどのシグネチャーベースの従来型セキュリティでは防げない最新の攻撃手法にも対応し、情報資産を守るアプライアンス型ソリューションです。

- 従来型セキュリティ製品では防げない、未知の脅威を利用した標的型攻撃を検知・ブロック  
標的型攻撃は、シグネチャをはじめとした静的解析のセキュリティ製品をすり抜けて、企業に侵入します。FireEyeは未知の攻撃や高度な標的型メール攻撃をシグネチャに依存することなく発見できるソリューションです。
- FireEye独自仮想実行エンジン  
FireEyeは実際に流れる通信をキャプチャし、MVXと呼ばれる仮想実行エンジン内で実際に実行することで、攻撃の有無を検知する動的解析のアーキテクチャを搭載しています。MVXには仮想マシンだけでなく、仮想Webサーバ、仮想DNSサーバなどにより、外部通信の再現も可能ですので、マルウェア感染後に接続するC&Cサーバ情報の取得を行うことも可能です。
- 世界中でリアルタイムの情報共有  
世界中に導入されているFireEyeのMVXで検出した脅威情報やC&Cサーバの情報をDTI-Cloudで収集し、最新の脅威情報を自社アプライアンスに配信する仕組みを保有しています。

◆解析サービスが必要な背景

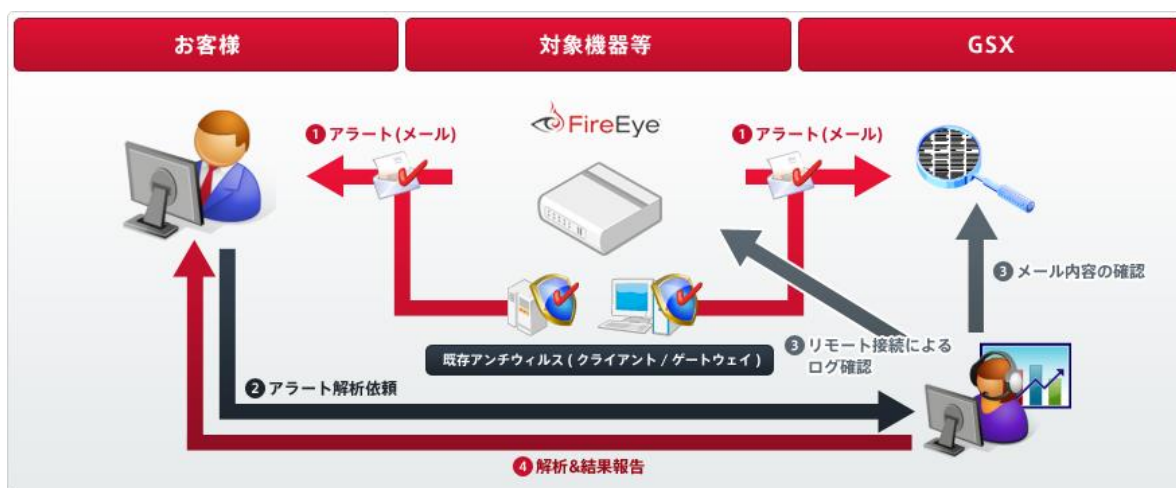
FireEye製品が自動作成する脅威のレポート（アラート）は、英語であることはもちろん、脅威やマルウェアに関係する専門用語が羅列されている、あるいはマルウェアが検出されるまでの過程を余すことなく記載している為に、有用ではあるものの、専門的な知見を有していない限り、事象を正確かつ精緻に理解するのが難しいという一面があります。

一方で、FireEye製品からアラートが発せられるということは、既存のセキュリティ対策をすり抜けた脅威が組織内に侵入しようとしている事を示すもので、組織としてはその脅威の判定や対処の検討を早急に進めなければいけません。

GSXの専門コンサルタントがお客様や運用事業者様に代わってFireEye製品アラートを解析し、脅威の内容や対策をご報告します。お客様はGSXのレポートを参考に脅威判定、事後対策に早急に着手することができます。

◆サービスの流れ

アラート解析サービスでは、通常運用時からGSXにアラートをメールにて共有、またFireEye製品に接続できる環境を設定頂きます。お客様が解析が必要と判断されるアラートについて、ご依頼を頂く都度、適宜その解析し結果をご報告させていただきます。



◆ご提供価格

項目	価格（税抜き）	内容
初期費用	¥200,000	運用開始に必要な設定、疎通確認等
月額費用	¥300,000	月/15件までのアラート解析
追加費用	¥20,000	追加のアラート解析 1件につき

◆その他サービスに関する情報

本サービスの実施内容、結果報告書サンプル、実施条件（対象機器・必要な環境・サービスレベル等）などは以下、FireEye製品アラート解析サービス紹介ページよりご覧ください。

FireEye製品アラート解析サービス：<http://www.gsx.co.jp/service/fireeye.html>

◆本リリースに関するファイア・アイ株式会社からのエンドースメント

ファイア・アイ株式会社  
カントリーマネージャー  
茂木 正之

従来型のセキュリティ製品では対応が出来なかった未知のマルウェア、標的型攻撃などを素早く正確に検知し、お客様の企業財産、信用を守るファイア・アイの製品はここ数年、急速に多くのお客様に採用されてまいりました。

また一方では、標的型対策システム導入後の効果的な運用や施策のための人的リソース不足により、システム導入に踏み出せないお客様もいらっしゃいます。

GSX様が培ってきた豊富なセキュリティコンサルティング実績に裏付けされた「FireEye製品アラート解析サービス」はこのようなお客様のニーズにマッチしたものであり、弊社アプライアンスとの連携によりお客様に対して最適なセキュリティソリューションが提供されるものと確信いたします。

◆グローバルセキュリティエキスパート株式会社について

社名：グローバルセキュリティエキスパート株式会社  
本社：〒105-0003 東京都港区西新橋 1-2-9 日比谷セントラルビル 21F  
代表者：代表取締役社長 松本 松仁  
資本金：2億7,000 万円  
コーポレートサイト：<http://www.gsx.co.jp/>

事業内容：

国内初の情報セキュリティ専門コンサルティング会社として2000年に設立され、セキュリティ診断、セキュリティポリシーの導入、リスクマネジメント、システム実装、監視サービスにいたる広範な情報セキュリティサービスを提供しています。

情報セキュリティポリシーの国際標準基準となった英国規格協会(BSI)のBS7799(現ISO27000)を日本に初めて紹介し、高品質な情報セキュリティコンサルテーションを行っています。

さらに、高い技術を有し、システムの脆弱性の発見のために侵入検査などさまざまな診断を行う「タイガーチームサービス(Tiger Team Service)」や標的型メール訓練サービスを始めとする新しい脅威に対抗するソリューションをご提案する「アドバンスドテクノロジーサービス」を組織しております。

**【本件に関するお問い合わせ先】**

グローバルセキュリティエキスパート株式会社 事業開発部 マーケティング担当  
TEL : 03-3507-1360 (代) E-mail : [mktg@gsx.co.jp](mailto:mktg@gsx.co.jp)