2014 年 5 月 29 日
NRI セキュアテクノロジーズ株式会社

# セキュリティ運用監視サービスに<br>標的型攻撃の対策メニューを追加

## ～24 時間 365 日体制で未知のサイバー攻撃から企業・組織を防御～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：増谷 洋、以下「NRI セキュア」）は、セキュリティ運用監視サービスを行う「FNC サービス[*1]」のメニューに、米国 FireEye 社[*2]のセキュリティ製品群[*3]を採用し、標的型攻撃[*4]から企業・組織を防御する「FireEye 管理サービス（以下「本サービス」）」を追加しました。

NRI セキュアは、本サービスの提供にあたって、FireEye 社とマネージド・セキュリティ・サービス・プロバイダー契約を日本で初めて締結し、同社製品に関する技術的サポートを直接受けられる体制を整備しました。

本サービスの特長は下記の 3 点です。

### ■ 仮想実行エンジンによる、未知のサイバー攻撃の検知

近年、標的型攻撃ではゼロデイ攻撃[*5]や未知のマルウェア[*6]を用いるサイバー攻撃手法が激増しており、既知の攻撃をデータベース化して検知する従来型のセキュリティ製品では、その検出は非常に困難になっています。

本サービスで使用する FireEye 社のセキュリティ製品群は、電子メールに添付されたファイルや、閲覧したウェブサイトのコンテンツを、同製品に備わった「仮想実行エンジン[*7]」上で実行し、疑わしい動作を行うか否かを分析します。これにより、既知・未知に関わらず、脆弱性を突く攻撃や高度なマルウェアを検知します。

検知されたマルウェアに対しては、後述の「24 時間 365 日体制サポート」にあるように、NRI セキュアのセキュリティアナリストが適切な対応を行います。

### ■ 設計から構築、運用監視、インシデント対応までの、オールインワン・サービス

NRI セキュアの「FNC サービス」は、顧客ごとに最適なセキュリティ環境の設計・構築から、導入後の運用監視、インシデント対応に至るまでのすべてをワンストップで提供するマネージドサービスです。「FNC サービス」に追加された「FireEye 管理サービス」を活用することにより、企業・組織は FireEye 社製品の導入に要する初期投資を抑え、短期間で利用開始できます。また、利用開始後においても、運用の手間やコストを大幅に削減しながら、同製品に精通した NRI セキュアのセキュリティアナリストによる運用監視やインシデント発生時の対応により、高度なセキュリティ対策を実現できます。

■ **24 時間 365 日体制サポート**

本サービスに加入された企業のシステムに対しては、高度なセキュリティ資格を保有するアナリストで構成する NCSIRT[*8] が、24 時間 365 日体制でサイバー攻撃を監視、分析し、FireEye 社製品により検知されたセキュリティインシデントに対して適切な対応を行います。また、本サービスでは、同製品の技術サポートを、NRI セキュアが FireEye 社から直接受けることができるため、迅速なサポート体制の提供が可能です。

本サービスの詳細については、以下の URL をご参照ください。

http://www.nri-secure.co.jp/service/mss/fireeye.html

NRI セキュアは、今後も企業・組織の情報システムや情報資産を守る情報セキュリティ対策をワンストップで提供し、安全な情報システムを安心して利用できる環境づくりに貢献していきます。

***1 FNC（Firewall Network Center）サービス：**

NRI セキュアが提供するマネージド・セキュリティ・サービスです。

詳細は、以下の URL を参照ください。

http://www.nri-secure.co.jp/service/mss/index.html

***2 FireEye 社（ファイア・アイ社）：**

本社を米国カリフォルニア州ミルピタスに置くセキュリティ企業です。同社は、業界をリードする技術で、さまざまなサイバー攻撃から、ネットワークを防御するソリューションを提供しています。

***3 FireEye 社のセキュリティ製品群：**

今回採用した製品は以下の通りです。

・NX Series/WebMPS　http 通信に対するマルウェア解析を行うアプライアンス

・EX Series/EmailMPS　メールに対するマルウェア解析を行うアプライアンス

・CM Series/CMS　NX Series と EX Series 間のマルウェア情報共有を行う管理用アプライアンス

***4 標的型攻撃：**

特定の企業・組織・人に対して、機密情報の詐取やシステムの破壊を目的に行われるサイバー攻撃を指します。

***5 ゼロデイ（0-day）攻撃：**

ソフトウエアにセキュリティ上の脆弱性が発見された際、問題の存在が広く公表される前にその脆弱性を悪用して行われるサイバー攻撃を指します。

***6 マルウェア：**

コンピュータウイルスやワーム等、悪意のある不正なソフトウエアの総称です。

***7 仮想実行エンジン：**

ファイルの実行や URL へのアクセスを、仮想化環境上で実行する機能です。

***8 NCSIRT（エヌシーサート）**：

NRI SecureTechnologies Computer Security Incident Response Team の略語で、24 時間体制でセキュリティモニタリングやインシデントハンドリングおよびセキュリティ情報の収集・発信を行っている、NRI セキュアのセキュリティアナリストチームの名称です。

**【ニュースリリースに関するお問い合わせ】**
株式会社野村総合研究所　コーポレートコミュニケーション部　十河、川越
TEL：03-6270-8100　E-mail：kouhou@nri.co.jp
**【サービスに関するお問い合わせ】**
NRI セキュアテクノロジーズ株式会社　MSS 事業推進部　京山、広報　若尾
TEL：03-6706-0622　E-mail：　info@nri-secure.co.jp