2016 年 5 月 11 日
株式会社日立ハイテクソリューションズ
日本通信株式会社

マルウェアに感染したモバイル端末からの情報漏洩防止を目的とした モバイル向け標的型サイバー攻撃対策ソリューションを販売開始

日立・米国ファイア・アイの「NX NetMonitor＋FireEye NX 連携ソリューション」と 日本通信の「モバイル専用線」を連携

株式会社日立ハイテクノロジーズ(執行役社長:宮﨑 正啓)の 100%子会社である株式会社日立ハイテクソリューションズ(取締役社長:飯泉 孝／以下、日立ハイテクソリューションズ)と、日本通信株式会社(代表取締役社長:福田 尚久／以下、日本通信)は、株式会社日立製作所(執行役社長 兼 CEO:東原 敏昭／以下、日立)が提供する「NX NetMonitor＋FireEye NX 連携ソリューション」(以下、連携ソリューション)と、日本通信が提供する無線の専用線サービス「モバイル専用線」を連携させた、モバイル向け標的型サイバー攻撃対策ソリューション(以下、本ソリューション)の提供を開始します。

日立ハイテクソリューションズは、日立の「NX NetMonitor」[*1] と、ファイア・アイ株式会社(所在地:東京都千代田区、代表:茂木正之、本社所在地:米国カリフォルニア州ミルピタス／以下、ファイア・アイ)の「FireEye NX」[*2] を連携させた標的型サイバー攻撃対策ソリューションの販売協力を行っています。本ソリューションは、連携ソリューションに、日本通信の「モバイル専用線」を組み合わせた、モバイル向け標的型サイバー攻撃対策ソリューションです。

近年、特定の企業や団体を狙う標的型サイバー攻撃の巧妙化に備え、各組織による組織内ネットワークの保護対策が進む一方、モバイル端末への対策は遅れています。従来、モバイル端末は空港や駅、ホテルなどで提供されているホットスポットなどからインターネットへ直接アクセスしていたため、接続標的型サイバー攻撃[*3] による情報漏えいが危惧されていました。そのため、現在モバイル端末へ侵入したマルウェア[*4] の C&C サーバ[*5] への通信を検出・ブロックし、情報漏えいを防止する必要性が高まっています。

日立が提供する連携ソリューションは、マルウェア感染端末の早期検出から強制排除までを自動的に行うことで感染拡大防止を図ることが可能なソリューションです。一方、日本通信が提供する「モバイル専用線」は、固定の専用線と同様に、インターネットを介さずダイレクトに、お客様のセンター拠点に携帯網を使って接続する特許技術を用いた専用線サービスです。
このたび販売を開始する本ソリューションでは、日本通信の「モバイル専用線」を用いることで、従来のホットスポットを経由したインターネット接続から、連携ソリューションにより監視・保護されているセンター拠点を経由したインターネット接続へ変更し、モバイル端末利用時においても高いセキュリティ環境を実現しています。また、感染したモバイル端末が持ち出された場合でも、センター拠点上の通信を監視している「FireEye NX」がマルウェアを検知し、C&C サーバとの通信を遮断し、情報漏えいを防止することが可能です。さらに、連携ソリューションを既に導入いただいているお客様であれば、新たに専用ソフトをインストールする必要がないため、導入・運用が容易です。

本ソリューションは、日立ハイテクソリューションズが官公庁施設や製造業や流通業の企業など幅広い業界に向けて販売を行い、日本通信はセキュアな無線「モバイル専用線」[*6] の提供を行います。また、ファイア・アイの日本における一次代理店であるソフトバンク・テクノロジー株式会社(代表取締役社長 CEO:阿多親市)が、技術的な支援を行います。

日立ハイテクソリューションズと日本通信は、本ソリューションの提供により、社外の業務端末のセキュリティ強化を図り、安全なモバイルワークの実現に貢献します。

*1 NX NetMonitor ： 各端末に専用ソフトをインストールせずに、ネットワークに専用監視装置を設置するのみで、不正 PC・スマートデバイスを検知した場合に、自動的に強制排除やアクセス制御を行えるシステム

*2 FireEye NX ： 独自に収集した脅威情報を、専用クラウドを介して世界規模で共有・配信し、標的型サイバー攻撃などの重大なサイバー攻撃を検知し、外部の悪意のあるサイトとの通信を遮断し、組織内ネットワークからの情報漏えいを防ぐシステム

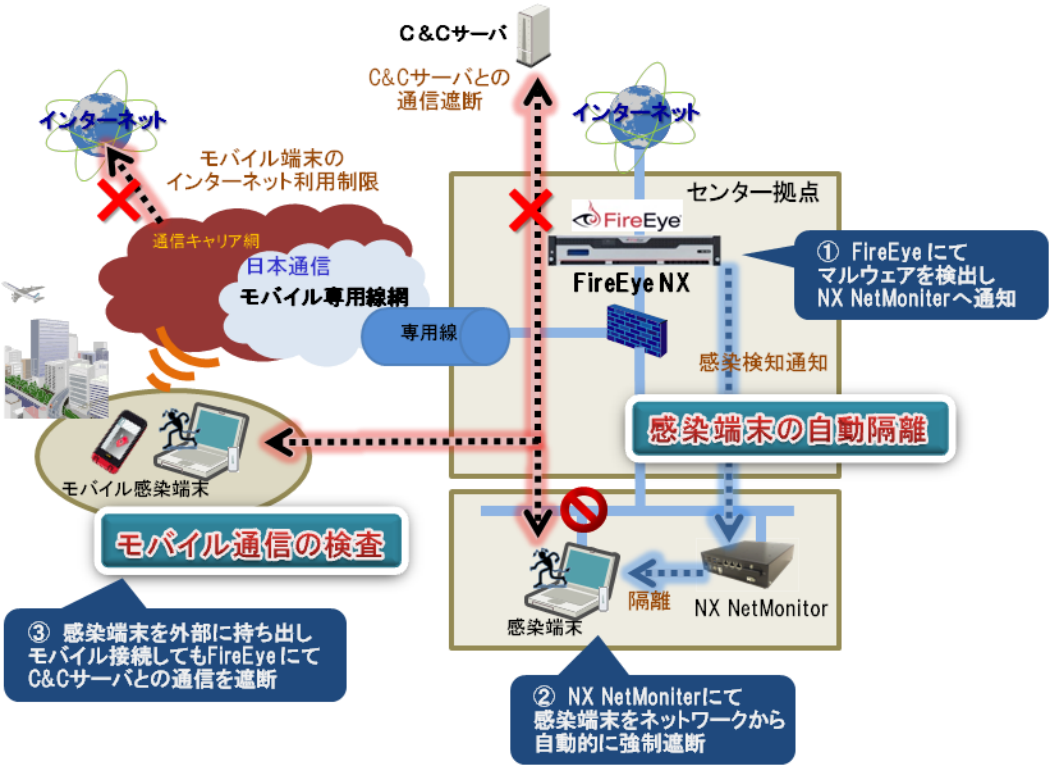
*3 標的型サイバー攻撃 ： 特定の組織内の重要な情報を不正に入手することを目的に行われる一連のサイバー攻撃

*4 マルウェア ： 悪意をもったソフトウェアの総称

*5 C&C サーバ ： Command & Control サーバ。インターネットから PC のマルウェアに不正な命令や制御を与えるために、攻撃者が用いるサーバの総称。標的型サイバー攻撃において、外部から高度な攻撃を行うために用いられる

*6 モバイル専用線 ： 日本通信の特許技術を活用したモバイル網による無線の専用線。PCI DSS の認定を取得し、金融系や制御系分野、企業活動等の分野において、高度なセキュリティを確保するために用いられる

【本ソリューションの全体イメージ】



■本ソリューションの特徴

・モバイル端末を使用の場合も、組織内ネットワークのセンター拠点にダイレクトに接続し、セキュアな環境で情報資産にアクセスすることが可能

・モバイル端末を使用の場合も、センター拠点を経由してインターネットへアクセスするため、「FireEye NX」により悪意のあるサイトへの接続を切断する出口対策が可能

・「FireEye NX」がマルウェア感染端末からの組織内ネットワーク接続を検知・通知し、「NX NetMonitor」により感染端末を組織内ネットワークから自動的に切り離して隔離することが可能

■提供開始時期
2016 年 5 月 11 日

■提供価格
個別見積

■キャンペーン情報
発売を記念した販売キャンペーンを実施します。キャンペーンでは、10 社限定で、本ソリューションの無償お試しや特別価格での提供を実施します。

キャンペーン受付期間：2016 年 5 月 11 日～2016 年 6 月 30 日
キャンペーン連絡先：
株式会社日立ハイテクソリューションズ ソリューション事業統括本部 ソリューション営業部
[担当：小澤、稲田]
Tel：050-3154-7235 E-MAIL：systemsales.dg@hitachi-hightech.com

※お申し込みが多数の場合は、お待ちいただく、もしくはお断りする場合がございますが、ご了承ください。

■製品 WEB サイト
・日立ハイテクソリューションズ「モバイル向け標的型サイバー攻撃対策ソリューション」
http://www.hitachi-hightech.com/hsl/product_detail/?pn=mobile_cyber_attack

・日本通信「モバイル専用線」
http://www.j-com.co.jp/biz/solution/layout_free.html

■関連情報
・日立製作所「NX NetMonitor」＋ファイア・アイ「FireEye NX」連携ソリューション
https://www.softbanktech.jp/service/list/fireeye/netmonitor/(ソフトバンク・テクノロジー)
http://www.hitachi-hightech.com/hsl/products/ict/cloud/netmonitor_fireeye.html（日立ハイテクソリューションズ）

・日立製作所「NX NetMonitor」
http://www.hitachi.co.jp/nxnm/

■お問い合わせ先
株式会社日立ハイテクソリューションズ
ソリューション事業統括本部 ソリューション営業部
担当：小澤、稲田 TEL：050-3154-7235

日本通信株式会社
ビジネスデベロップメント
担当：原田、赤西 TEL：03-5776-1700

■報道機関お問い合わせ先
株式会社日立ハイテクノロジーズ
CSR 本部
CSR・コーポレートコミュニケーション部
担当：佐野、松本 TEL: 03-3504-3933

日本通信株式会社
コーポレートコミュニケーションズ
担当：田尻、堀江 TEL： 03-5776-1774