2016 年 1 月 21 日
株式会社日立製作所

日立の「NX NetMonitor」と米国ファイア・アイの「FireEye NX」を連携させた標的型サイバー攻撃対策ソリューションを提供開始

マルウェア感染端末を自動的に早期検出・強制排除し、感染拡大を防止

株式会社日立製作所(執行役社長兼 COO:東原 敏昭/以下、日立)は、標的型サイバー攻撃対策として、日立の不正 PC 監視・強制排除ソフトウェア「NX NetMonitor」および統合システム運用管理ソフトウェア「JP1」と、サイバー攻撃検知やインシデント対策サービスを提供するファイア・アイ株式会社(取締役会長兼 CEO:デビッド・デウォルト/以下、ファイア・アイ)のサイバー攻撃検知製品「FireEye NX」を連携させ、マルウェア*1 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ソリューションを 2 月 1 日から提供を開始します。また、「FireEye」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)、および株式会社日立ハイテクノロジーズ(執行役社長:宮﨑 正啓)の子会社で「FireEye」と日立グループ製品との連携ソリューションの推進を担当する株式会社日立ハイテクソリューションズ(取締役社長:水谷 隆一)は、本ソリューションの販売協力を行います。

本ソリューションは、標的型サイバー攻撃を自動的に検知し、感染した端末を強制排除することで、マルウェアによるシステム障害や情報漏えいを防止します。また専用ソフトのインストールが困難な機器(IoT デバイス*2 や専用 OS 搭載機、持ち込み PC など)や既設の機器に対して、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。今後、本ソリューションを、データセンターや官公庁施設、社会インフラ施設、工場・プラント、商業施設など幅広い業界に向けて拡販していきます。

近年、特定の企業や団体を狙う標的型サイバー攻撃が巧妙化しており、情報漏えいや業務停止などの被害が増加しています。最近の攻撃には、未知のマルウェアが用いられており、一般型のセキュリティ対策であるファイアウォールやアンチウイルスソフトウェアでは、マルウェアの侵入や感染、情報漏えいを検出できず、被害が拡大する傾向があります。そのため、侵入したマルウェアを早期に検出し、無効化することで、被害を最小化することが必要です。また、常に攻撃の脅威にさらされているネットワークに対して、24 時間人手で検出・無効化することは運用上困難であるため、対策の自動化が求められています。

日立の「NX NetMonitor」は、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、検知した不正 PC・スマートデバイスを、自動的に強制排除やアクセス制御するシステムで、情報システムだけでなく、制御システムにも豊富な納入実績があります。一方、ファイア・アイの「FireEye NX」は、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する製品で、世界的に広く普及しています。そこで日立は、情報システムから制御システムの幅広い分野にわたる実績・ノウハウを持つ日立の「NX NetMonitor」と、グローバルで実績のある高度なマルウェア検知能力を持つファイア・アイの「FireEye NX」を組み合わせることで、高いセキュリティ環境を実現する標的型サイバー攻撃対策ソリューションを開発・提供することにしました。

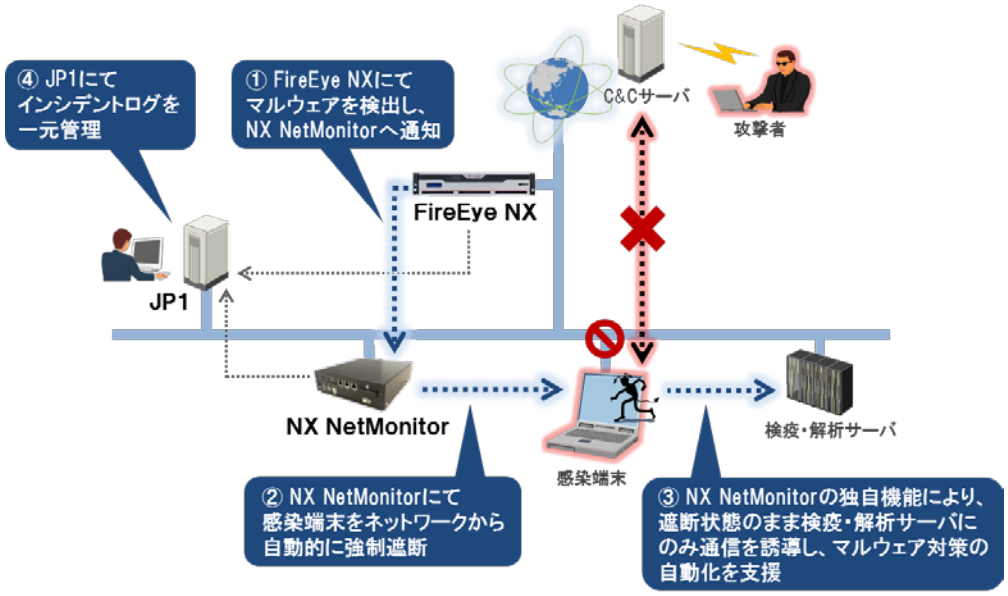
具体的には、ネットワーク上の通信を監視している「FireEye NX」がマルウェアを検出すると、「NX NetMonitor」がその情報をもとにマルウェア感染した端末をネットワークから自動的に強制排除し、感染拡大による 2 次的被害や情報漏えいを防止することができます。

また、「NX NetMonitor」の独自機能により感染端末を隔離しつつ、検疫サーバ*3 や解析サーバ*4 にのみ通信を誘導し、自動的に感染端末の検疫や解析をすることで、セキュリティ対策の運用性を向上することができます。

なお、「JP1」の統合管理製品「JP1/Integrated Management」は「NX NetMonitor」および「FireEye NX」と連携し、両製品からのインシデントログを一元的に監視できます。また、「FireEye NX」は日立が「JP1」と連携できる製品を認定する「JP1 Certified」制度で連携製品として登録されています。

日立では、新たな潮流であるIoTに対応するサイバー、フィジカル両面のセキュリティソリューションを提供しており、システムとしての強じん性に、適応性、即応性、協調性を加えたセキュリティコンセプト「H-ARC*5」を提唱しています。今回、「NX NetMonitor」と「FireEye NX」の連携ソリューションの提供により、サイバーセキュリティソリューションのラインアップ強化を図り、より安全・確実なセキュリティ対策の実現に貢献します。

■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長

・マルウェアに感染した端末を自動的に検知・隔離し、他の端末やサーバへの感染拡散や C&C サーバ*6 による遠隔攻撃を防止、機密情報を保有するサーバへのアクセスを禁止（接続遮断）することで、乗っ取りによるシステム障害や情報漏えいの防止が図れます。

・従来はマルウェアに感染した端末をネットワークから切り離して、解析担当部門に移送し検体を取り出す必要があったマルウェアの解析や対策を、「NX NetMonitor」の独自機能により、感染端末を隔離しつつ検疫サーバや解析サーバにのみ通信を制限することで自動化することが可能であり、セキュリティ対策の運用性が向上します。

・「NX NetMonitor」と「FireEye NX」は共にエンドポイント型セキュリティ対策*7 製品のように端末ごとに新たな専用ソフトをインストールする必要がないため、既存ネットワークへの導入が容易です。
・「JP1」でインシデントログの一元管理を行うことで、ネットワーク管理者が容易に状況を把握でき、早期対応につなげることができます。

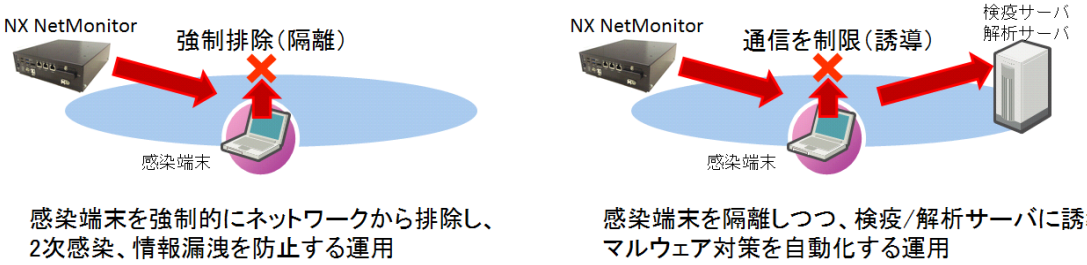


図 1：「NX NetMonitor」による強制排除と通信誘導の仕組み

*1 マルウェア：悪意をもったソフトウェア
*2 IoT デバイス：IoT（Internet of Things）により通信機能を持ち、ネットワークに接続が可能なデバイス
*3 検疫サーバ：端末のマルウェア感染を確認するためのサーバ
*4 解析サーバ：感染端末のマルウェアを解析するためのサーバ
*5 H-ARC：Hitachi-Adaptivity(適応性)、Responsivity(即応性)、Cooperativity(協調性)
*6 C&C サーバ： Command & Control サーバ。マルウェアに命令や制御を与えるために、攻撃者が用いるサーバ。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。
*7 エンドポイント型セキュリティ対策：ネットワークに接続された各端末側で実施するセキュリティ対策。専用ソフトウェアのインストールなどが必要になる。

■本ソリューションで連携している各社のコメント

ファイア・アイ株式会社
プレジデント 執行役社長 茂木 正之 氏のコメント

ファイア・アイ株式会社は、弊社NXシリーズと連携するソリューションを日立製作所様が販売開始されることを心から歓迎いたします。弊社のNXシリーズは標的型攻撃への防御を支援する製品として、業界を問わず多数のお客様にご利用されています。標的型攻撃による被害が増大する中、日立製作所様の「NX NetMonitor」ならびに「JP1」との連携により新たなお客様が本ソリューションをご利用され、標的型攻撃の早期検知ならびに最小化に役立てていただくことを期待いたします。

ソフトバンク・テクノロジー株式会社
執行役員 セキュリティソリューション本部長 鈴木 重雄 氏のコメント

ソフトバンク・テクノロジーは、標的型サイバー攻撃の被害拡大防止を図るソリューションの提供開始を歓迎いたします。ソフトバンク・テクノロジーはこれまで「FireEye」の導入や運用支援サービスを提供して参りました。本連携は、標的型攻撃による情報漏洩リスクを抱える企業にとって、セキュリティ強度を格段に向上させる防衛策であることを確信しております。ソフトバンク・テクノロジーが培ってまいりました技術力をもとに日立製作所様の本連携ソリューションを御支援し、本ソリューションの販売も行うことで連携体制を構築し、共同でお客様により良いセキュリティソリューションを提供して参ります。

■関連情報
「NX NetMonitor」および本ソリューションに関する日立の Web サイト
http://www.hitachi.co.jp/nxnm/
「NX NetMonitor」と「FireEye NX」の連携に関するソフトバンク・テクノロジーの Web サイト
https://www.softbanktech.jp/service/list/fireeye/netmonitor/
「JP1」に関する日立の Web サイト
http://www.hitachi.co.jp/jp1/

■提供開始時期
2016 年 2 月 1 日

■提供価格
個別見積

■キャンペーン情報
今回の連携を記念し、日立製作所、日立ハイテクソリューションズ、ソフトバンク・テクノロジーの 3 社合同で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、連携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 2 月 1 日～2016 年 3 月 31 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]
電話: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、ご了承下さい。

■照会先
株式会社日立製作所 インフラシステム社 大みか事業所 制御プラットフォーム開発本部
制御プラットフォーム設計部 製品問合せ窓口 [担当:中三川(なかみかわ)]
〒319-1293 茨城県日立市大みか町五丁目 2 番 1 号
電話:0294-52-7086 (直通)

以 上