

2015年9月14日
株式会社日立ソリューションズ

情報漏洩防止ソリューション「秘文」とマルウェア対策製品「FireEye」を連携 マルウェア感染端末への警告から遮断までを自動実行し、感染拡大を防止

株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:佐久間 嘉一郎/以下、日立ソリューションズ)は、標的型攻撃対策として、ネットワーク接続やファイルの持ち出しを制御する「秘文 Device Control」と、高度なサイバー攻撃の対策製品・サービスを提供するファイア・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)のマルウェア対策製品「FireEye NX」を連携し、マルウェア感染端末の自動隔離による感染拡大の防止ソリューションを9月15日から提供開始します。

昨今、特定の団体や企業を狙う標的型攻撃は巧妙化しており、未然に攻撃を防ぐだけでなく、マルウェアに感染した場合に、いかに早期に発見し、被害の拡大防止につなげるかが重要です。

このような背景の下、日立ソリューションズは、「秘文 Device Control」と「FireEye NX」の連携ソリューションを提供します。

具体的には、「FireEye NX」によって検知された通知内容(インシデント)の重要度に応じて、「秘文 Device Control」がマルウェア感染端末への警告や、ネットワークから自動遮断などの対応を行います。自動遮断することで感染端末を媒介とした内部ネットワークにおける感染拡大を防ぐとともに、感染端末から行われる情報収集などを妨害し、情報漏洩のリスクを低減します。さらに、感染端末に警告画面を表示することで、利用者は自動遮断された理由を把握し、迅速な対応を行うことができます。これにより、システム管理者が行う感染端末の物理的な場所の特定や、手動による隔離処理が不要となります。

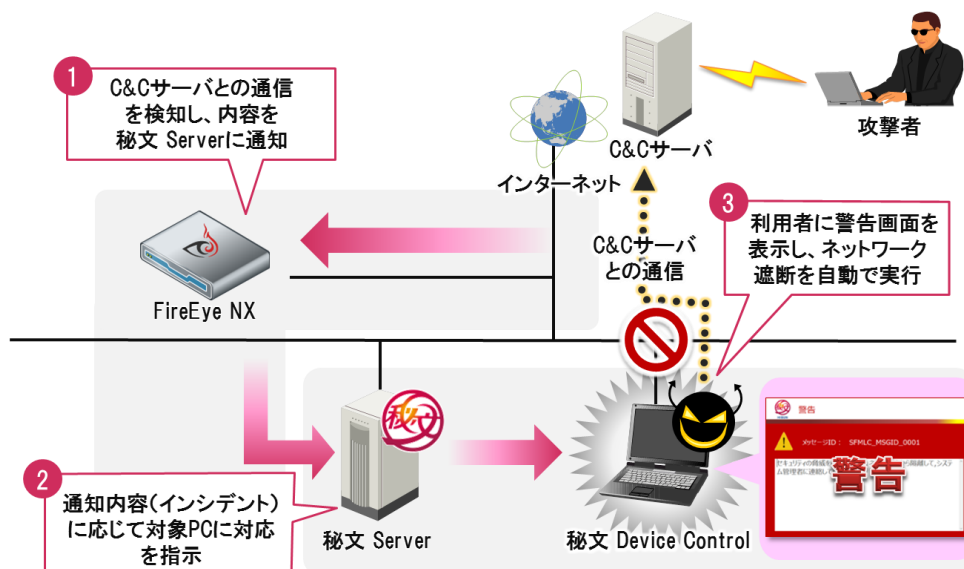


図:「FireEye NX」で重要度「高」が検知された場合の「秘文」の動作

本ソリューションでは、「FireEye NX」が検知したインシデントと重要度に応じて、マルウェア感染の可能性と影響度を判断し、「秘文」でそれぞれ下表のように対応できます。

「FireEye」のインシデント	重要度		「秘文」の対応例
C&Cサーバ*1との通信を検知	高	マルウェアに感染している可能性が極めて高い	利用者への 警告 ネットワークの 自動遮断
サンドボックスでマルウェアらしき振る舞いを検知	中	マルウェアが侵入した可能性がある	利用者への 警告
既知のマルウェアの検知	低	他のセキュリティ製品(アンチウイルスソフトやFW/GW)で対応が可能	特になし

*1:コマンド&コントロール サーバ。サイバー攻撃などで、ウイルスに感染したコンピュータを制御したり命令を出したりする役割を担う。

また、「秘文 Device Control」のファイルアクセスログやネットワーク通信ログと、「FireEye NX」のアラートログを分析し、マルウェアがどのようなローカル/ネットワークファイルにアクセスしたかを確認できるログ分析サーバを導入することで、インシデント発生時に漏洩した可能性のあるファイルの迅速な特定をサポートします。

ログ分析サーバで利用する製品・サービスとしては、ビッグデータ利活用基盤ソリューション「Splunk」や、ソフトバンク・テクノロジー株式会社が提供するログの管理・分析クラウドサービス「4DP LogSearch」など、お客様の環境や要望に合った適切な手法を提案します。

なお、今回の発表に際し、ファイア・アイ株式会社と両製品の連携の技術検証を支援したソフトバンク・テクノロジー株式会社よりエンドースメントをいただいています。

■ ファイア・アイ株式会社のエンドースメント

「ファイア・アイ株式会社は、弊社『FireEye NX』との連携ソリューション発表を心より歓迎いたします。『FireEye NX』がマルウェアを検知、『秘文 Device Control』に通知、ブロックすることにより、マルウェアに対する防衛力を飛躍的に高めることが可能です。さまざまな業種で実績を有する両社の協力により、被害が拡大している企業の情報漏洩対策に大きく貢献できると確信しております。マイナンバー対応をはじめ、セキュリティの重要性は一層高まることが予想されますので、連携してより良い製品・サービスを提供してまいります。」

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

■ ソフトバンク・テクノロジー株式会社のエンドースメント

「ソフトバンク・テクノロジー株式会社は、『秘文 Device Control』と『FireEye NX』の連携ソリューションの発表を心より歓迎いたします。株式会社日立ソリューションズの情報漏洩防止ソリューションと、ファイア・アイ株式会社のマルウェア対策製品との連携は、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。弊社はサイバーセキュリティ分野において、機能実装やログ分析における協業体制をより一層強化し、企業の情報漏洩対策に貢献してまいります。」

ソフトバンク・テクノロジー株式会社

執行役員 技術統括 セキュリティソリューション本部長 鈴木 重雄

■ 構成する製品・サービス: 秘文 Server、秘文 Device Control、FireEye NX、ログ分析サーバ(オプション)

■ 製品紹介URL: <http://www.hitachi-solutions.co.jp/hibun/sp/>

■ 提供価格: 個別見積

■ 提供開始時期: 2015年9月15日

■ セミナー情報

10月15日(木)、ソフトバンク・テクノロジー(本社)において、ファイア・アイとソフトバンク・テクノロジー、日立ソリューションズの3社による共同セミナーを開催し、今回発表したソリューションを紹介します。

詳細はこちら: <http://www.hitachi-solutions.co.jp/events/2015/cyber1015/>

<商品・サービスに関するお問い合わせ先>

ホームページ: <https://www.hitachi-solutions.co.jp/inquiry/> Tel:0120-571-488

<報道機関からのお問い合わせ先>

担当部署: 経営企画本部 広報・宣伝部

担当者: 安藤、竹谷


Tel:03-5479-5013 Fax:03-5780-6455 E-mail:koho@hitachi-solutions.com

日立ソリューションズグループは、お客様の業務ライフサイクルにわたり、豊富なソリューションを全体最適の視点で組み合わせ、ワンストップで提供する「ハイブリッドインテグレーション」を実現します。

※ FireEye は、FireEye, Inc. の登録商標です。

※ 秘文、ハイブリッドインテグレーションは、株式会社日立ソリューションズの登録商標です。

※ その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

 株式会社 日立ソリューションズ

本社 〒140-0002 東京都品川区東品川四丁目12番7号
Tel:03-5780-2111 ホームページ:<http://www.hitachi-solutions.co.jp/>

日立ソリューションズ

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。

