HITACHI
Inspire the Next

News Release

2016 年 12 月 20 日
株式会社日立情報通信エンジニアリング
株式会社日立ソリューションズ

ネットワークセキュリティ対策自動化ソリューションを販売開始

セキュリティ脅威に対するネットワーク制御を自動化し、サイバー攻撃被害の拡大を最小限に

株式会社日立情報通信エンジニアリング(代表取締役社長:小菅 稔、本社:神奈川県横浜市／以下、日立情報通信エンジニアリング)と株式会社日立ソリューションズ(取締役社長:柴原 節男、本社:東京都品川区／以下、日立ソリューションズ)は、日立情報通信エンジニアリングのネットワークインテグレーション実績と、日立ソリューションズのセキュリティソリューション実績という両社の強みを生かし、セキュリティの脅威(インシデント)に対し、問題のある端末をネットワークから自動で切断または隔離するソリューションを 12 月 21 日から販売開始します。

本ソリューションを導入することで、企業や組織は、巧妙化するサイバー攻撃への対策を強靭化・迅速化・自動化して被害を最小限に抑え、対策の自動化により、運用管理コストを低減します。

本ソリューションは、マシンデータ利活用基盤「Splunk」(*1)のイベントログ収集・相関分析によって検知した脅威に対し、ネットワーク管理 SDN(*2)システム「Cisco Prime Infrastructure」(以下、Cisco PI)(*3)がネットワークを制御することで、セキュリティ対策初動の自動化を実現します。日立情報通信エンジニアリングは、セキュリティ脅威発生時に人手を介さずネットワークを自動制御する「Splunk」と「Cisco PI」の連携プログラム「インシデント レスポンス自動化 SDK(*4) for Prime Infrastructure」(以下、インシデント対応 SDK)(*5)を開発しました。

「インシデント対応 SDK」は、セキュリティ対策の初動に必要な切断や隔離などの機能を集約したライブラリであり、対象端末の IP アドレスを基に制御対象のネットワーク機器を自動的に認識して制御するなど、簡単なインタフェースでネットワーク制御を実現する連携プログラムです。「インシデント対応 SDK」が「Splunk」と「Cisco PI」を繋ぐことで、従来は人手を介して実施されていた初動対応を自動化することができ、サイバー攻撃被害の最小化と運用管理コストの低減を実現します。

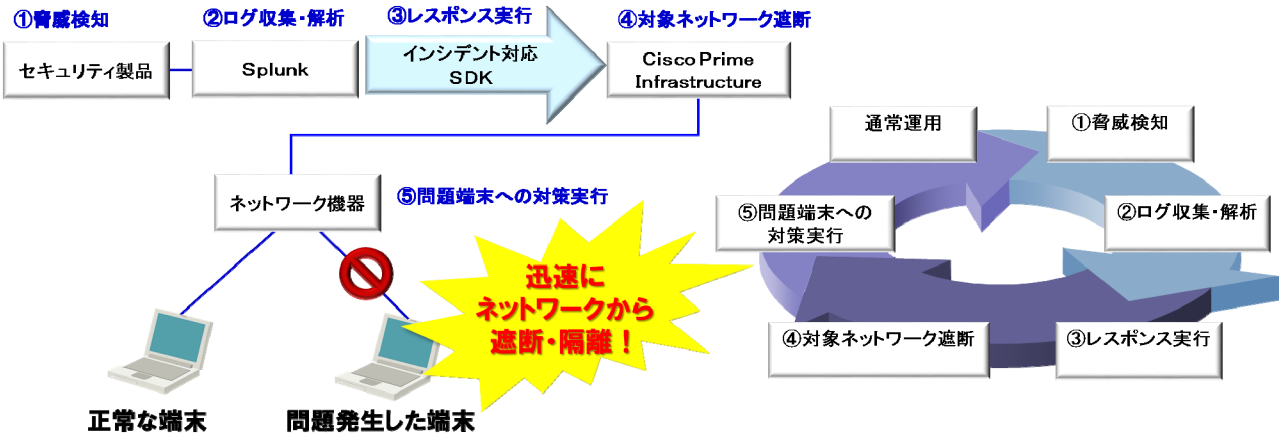
このプログラムは、業界トップシェア(*6)であるシスコ社のネットワーク製品を利用して数多くのネットワークシステムの設計・構築・運用業務に携わってきた日立情報通信エンジニアリングが、その経験を生かして、開発したものです。

今後も、日立情報通信エンジニアリングと日立ソリューションズは、両社のセキュリティ製品やプラットフォーム製品、関連サービスを組み合わせ、巧妙化する脅威にも迅速に対応できるソリューションを提供していきます。

*1 Splunk 社(Splunk Services Japan 合同会社)の製品で、日立ソリューションズが販売。
*2 Software Defined Networking の略。ネットワークを構成する通信機器を単一のソフトウェアによって集中的に制御し、ネットワークの構成、設定などを柔軟に、動的に変更することを可能とする技術。
*3 シスコ社(シスコシステムズ合同会社)の製品で、日立情報通信エンジニアリングが販売。
*4 Software Development Kit の略。あるシステムに対応したソフトウェアを開発するために必要なパッケージ化されたプログラム。

*5 日立情報通信エンジニアリングが開発したプログラム。
*6 平成 25 年度総務省通信白書より

■「ネットワークセキュリティ対策自動化ソリューション」の構成イメージ



■ソリューションの特長

1. セキュリティ対策自動化による運用管理コストの削減

サイバー攻撃が検知された場合、あらかじめ設定されたネットワーク制御ポリシーの下、自動でネットワークを制御します。夜間、休日など情報システム管理者が不在でも、人手を介さずセキュリティ対策の初動対応を完了することができ、運用管理コストを低減します。

2. 豊富な知見と導入実績に基づくノウハウを活用し、膨大なログをリアルタイムに解析

「Splunk」は、サーバーや PC、ネットワーク製品など多種多様な機器が出力する膨大なイベントログの中から不審な動きをリアルタイムに検出します。日立ソリューションズの豊富な導入実績とそれに基づく知見から、不正があると思われる機器やシステムのログを相関分析して、より高度なセキュリティ脅威の検知を行います。

3. 既存システムとの連携による投資コストの抑制

「インシデント対応 SDK」は、さまざまなセキュリティ製品との連携を柔軟にするユーザースクリプトを用意しており、セキュリティ製品ごとに簡単に作成することができます。これにより、さまざまなセキュリティ製品との連携が可能になり、すでに導入されているシステムを利用できるほか、より高度なマルウェア対策システムへのアップグレードにも対応することができます。

■価格

本ソリューションおよび「Splunk」、「Cisco PI」の価格は、個別見積となります。
「インシデント対応 SDK」の価格は、1,700,000 円（標準価格、税抜）です。

■Splunk Inc. Country Manager Japan 纐纈 昌嗣(こうけつ まさつぐ)氏のエンドースメント

このたびの日立ソリューションズ様と日立情報通信エンジニアリング様の発表を歓迎いたします。IoTの普及が加速する中、SDN においてもそのセキュリティを担保することは非常に重要です。多種多様なセキュリティインシデントに対応するため、マシンデータを迅速に収集し、リアルタイムな分析を可能とする「Splunk」のテクノロジーと、日立ソリューションズ様によるソューションのシナジーにより、新しい IoT 時代のセキュリティソリューションが実現されることを確信しております。

■シスコシステムズ合同会社 専務執行役員 パートナー事業統括 高橋 慎介(たかはし しんすけ)氏のエンドースメント

シスコは、日立情報通信エンジニアリング様の「インシデントレスポンス自動化 SDK for Prime Infrastructure」の販売開始を歓迎いたします。情報セキュリティに対する対策が企業活動で重要視されている今日、日立情報通信エンジニアリング様の開発されたソリューションと「Cisco Prime Infrastructure」をはじめとする弊社製品とともに導入いただくことで、お客様のセキュリティ対策が自動化され、運用の効率化による TCO 削減などの付加価値をもたらすと確信しております。

■関連リンク

- 日立ソリューションズ「Splunk」のホームページ
  http://www.hitachi-solutions.co.jp/splunk/
- シスコ社の Cisco Prime Infrastructure のホームページ
  http://www.cisco.com/web/JP/product/hs/netmgt/prime_infra/index.html

■商標について

■お客さまお問い合わせ先

・ 株式会社 日立情報通信エンジニアリング 営業戦略統括本部 ［担当：一ノ瀬］
〒220-6122 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 25 階
URL: http://www.hitachi-ite.co.jp/inquiry/form/sdx.html 電話：050-3163-1755(直通)

・ 株式会社 日立ソリューションズ
URL：https://www.hitachi-solutions.co.jp/inquiry/ 電話：0120-571-488

■報道機関お問い合わせ先

・ 株式会社 日立情報通信エンジニアリング 経営・事業企画本部 企画部 ［担当：中村］
〒220-6122 神奈川県横浜市西区みなとみらい 2 丁目 3 番 3 号 クイーンズタワーB 22 階
電話：050-3163-5726(直通)

・ 株式会社　日立ソリューションズ　経営企画本部　広報・宣伝部［担当：竹谷、安藤］
電話：03-5479-5013
E-Mail：koho@hitachi-solutions.com

以上
