PRESS RELEASE

2017 年 10 月 30 日
株式会社インターネットイニシアティブ

IIJ、SDNで実現する次世代ネットワークセキュリティの実証実験を開始

-- 組織ネットワークのセキュリティ対応を、次世代のセキュリティアーキテクチャーで実現 --

株式会社インターネットイニシアティブ(IIJ、本社:東京都千代田区、代表取締役社長:勝 栄二郎、コード番号:3774 東証第一部)は、端末(デバイス)から社内 LAN、外部クラウドまで広範囲に拡がる企業ネットワークにおいて、SDN(※1)および NFV(※2)技術を活用し、セキュリティ脅威を早期に検知し動的に隔離することで、社内ネットワークへの拡散を防止する実証実験を行います。

IIJ では、SDN や NFV 技術をベースとした「フルレンジ・セキュリティ」の開発・検証を進めています。これは、ユーザやデバイス単位でセキュリティセグメントを論理的に設定する自社技術(Software-Defined Segmentation)を用い、各セグメントのセキュリティポリシーに合わせてネットワーク全体のセキュリティ監視・制御を動的に行うものです。開発・検証にあたっては、トレンドマイクロ株式会社(以下、トレンドマイクロ)の NFV 向けネットワークセキュリティ技術(Trend Micro Security VNF)(※3)を活用しており、昨年両社は、セキュリティの監視レベルをクラウド上で動的に変更し、不正通信を制御する技術検証を行いました(※4)。今回の実証実験では、検証範囲をオフィスネットワークやデバイスまで拡大し、動作連携を確認いたします。
今後 2018 年度下期を目途に、ネットワークサービスのソリューションとして、フルレンジ・セキュリティ機能を提供する予定です。

背景

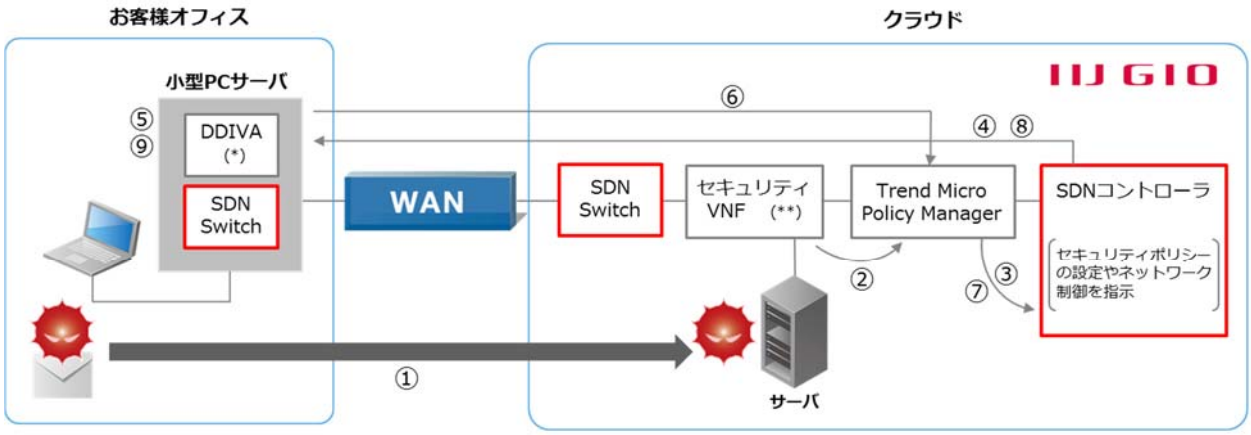
企業においてマルチクラウド利用が進み、ビジネスシーンにおけるスマートデバイスの利用が増える中で、企業ネットワークは多様化・複雑化しています。一方、ネットワーク内部を狙った標的型攻撃は巧妙化しており、従来のゲートウェイ型対策やデバイス側のウィルス対策だけでは十分なセキュリティを確保することが困難となっています。そのため、ネットワーク外部からの侵入防止に加え、ネットワーク内部におけるセキュリティ脅威の早期発見と拡散防止が不可欠となっています。IIJ では、ネットワークの運用効率化と被害の最小化を図りつつセキュリティレベルを維持するため、ユーザやデバイスを基点としたセキュリティセグメントを設け、個々のセグメントに設定した最適なセキュリティポリシーに基づき動的にネットワークを制御することで、新たなネットワークセキュリティを実現します。

概要

本実証実験では、セキュリティ機能をクラウドおよびオフィスネットワークに分散配置し、不正な通信を発見すると動的にネットワークが制御され、不正通信や不正ファイルをブロックします。不正アクセスの侵入検知システム等セキュリティ機能は、トレンドマイクロの Trend Micro Security VNF を使用いたします。

1) ユーザの PC や IoT デバイスなど IT 資産を経由してオフィスネットワーク内に未知のセキュリティ脅威が侵入すると、IIJ のクラウドサービス「IIJ GIO(ジオ)サービス」上にある侵入検知システムが不正な動きを発見
2) そのトラフィックの振る舞いを監視
3) 不正と判断した場合には、SDN の機能でトラフィックを遮断しセキュリティ脅威を隔離

■　概要図



(*) Deep Discovery Inspector Virtual Appliance
(**) Trend Micro Security VNF (vIPS)

①[攻撃]　クラウド上にあるサーバを攻撃
②[検知・通知]　攻撃を検知し通知
③[通知]　アクションすべき事象と通知
④[指示]　トラフィックのミラーリングおよびDDIで監視するよう指示
⑤[監視]　PCからのトラフィックを監視
⑥[検知・通知]　不正と判断し通知
⑦[通知]　アクションすべき事象と通知
⑧[指示]　PCをネットワークから隔離するよう指示
⑨[対処]　SDN SwitchがPCをネットワークから隔離

➢　本実証実験のデモを、IIJ 主催の技術セミナー「IIJ Technical WEEK 2017」（11 月 8 日）にて行います。IIJ Technical WEEK 2017 の詳細は、以下サイトをご覧ください。
https://www.iij.ad.jp/techweek2017/

IIJ では今後とも、SDN/NFV 技術を活用し、ネットワーク環境の安全を実現する技術開発に積極的に取り組んでまいります。

■　トレンドマイクロ株式会社様からのエンドースメント

トレンドマイクロは、株式会社インターネットイニシアティブ（IIJ）による、弊社の「NFV 向けネットワークセキュリティ技術（Trend Micro Security VNF）」を採用した次世代ネットワークセキュリティの実証実験開始を大変嬉しく思います。IIJ の新ネットワーク技術「Software-Defined Segmentation」とトレンドマイクロのセキュリティ技術の組み合わせは、企業ユーザ様のロケーションや環境に依存しない新しい企業向けネットワークセキュリティサービスを実現します。
トレンドマイクロは引き続き IIJ と協業を深め、お客様の IT インフラに最適なセキュリティソリューションを提供してまいります。

トレンドマイクロ株式会社
IoT 事業推進本部　ソリューション推進部　部長　津金　英行

※1　SDN（Software Defined Networking）：ネットワークをソフトウェアで定義し、動的な制御を可能にするという概念、およびそのアーキテクチャ。
※2　NFV（Network Function Virtualization）：ネットワークの各種機能を仮想化し、データセンターやネットワーク拠点に設置したサーバ等に機能集約して提供するネットワーク仮想化技術の総称。
※3　ネットワーク上の NFV 環境で動作するセキュリティ VNF（Virtual Network Function）
※4　2016 年 11 月 9 日付報道発表資料（「IIJ とトレンドマイクロ、NFV 向けのセキュリティで連携」：https://www.iij.ad.jp/news/pressrelease/2016/1109.html）をご参照ください。
＊　TRENDMICRO、Deep Discovery、Deep Discovery Inspector、および Trend Micro Policy Manager は、トレンドマイクロ株式会社の登録商標です。

報道関係お問い合わせ先
株式会社インターネットイニシアティブ　広報部　荒井、増田
TEL：03-5205-6310　FAX：03-5205-6377
E-mail：press@iij.ad.jp
www.iij.ad.jp