2014 年 12 月 18 日

(報道発表資料)

NTT コミュニケーションズ株式会社
日本マイクロソフト株式会社
株式会社 FFRI

日本独自のゼロデイ攻撃対策セキュリティサービス「Zero day Attack Protection」（仮称）を開発・提供

～NTT コミュニケーションズ、日本マイクロソフト、FFRI が サイバーセキュリティ基本法の成立を受け、セキュリティ対策サービスの開発・提供で協業～

NTT コミュニケーションズ株式会社（本社：東京都千代田区、略称：NTT Com）、日本マイクロソフト株式会社（本社：東京都港区、略称：日本マイクロソフト）および株式会社 FFRI（本社：東京都渋谷区、略称：FFRI）は、3 社協業により、標的型攻撃やゼロデイ攻撃などに対する日本独自のセキュリティ対策サービス「Zero day Attack Protection」（仮称）を開発・提供します。なお、本サービスの提供開始は 2015 年 4 月を予定しています。

1．背景

企業の機密情報や顧客情報を詐取する標的型攻撃が高度化するなか、未公開の脆弱性を狙ったゼロデイ攻撃など未知のセキュリティ脅威を検知・防御する対策が不可欠となっています。

日本でも 2014 年 11 月にサイバーセキュリティ基本法が成立し、同法におけるサイバーセキュリティの定義「情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること」の実現に向け、様々な施策が推進されています。

また、国際的なイベントが開催される度に開催国をターゲットにした攻撃が急増する傾向があり、2020 年に向けて行政機関および電力・ガス・通信などの重要社会基盤事業者への攻撃がさらに増えることが想定されるため、実効性のある対策が急務となっています。

こうした中、NTT Com、日本マイクロソフトおよび FFRI は、3 社で協業し、標的型攻撃やゼロデイ攻撃でターゲットとされるエンドポイント（ネットワークに接続された PC などの端末）への対策として、「Zero day Attack Protection」（仮称）を開発・提供することとしました。

2. セキュリティサービス「Zero day Attack Protection」（仮称）の概要

アンチウイルスのパターンファイルや侵入防御装置（IPS）のシグネチャなど、既存対策では防げない未知の脅威に対して、マイクロソフトが海外の政府機関などへの提供で培った脅威分析技術と FFRI のゼロデイ攻撃検出技術を、NTT Com のセキュリティサービス基盤へ統合・相互連携することにより、日本独自のセキュリティ対策サービスとして提供します。

本サービスでは、クライアント PC の OS 上だけでなく、カーネルモード[*1]への攻撃も検出されるため、APT 攻撃（Advanced Persistent Threat、ターゲットへの潜伏や攻撃を持続的に行い、様々な手法でスパイ行為・妨害行為を行うタイプの攻撃）など、非常に高度な攻撃にも対応可能です。検出した攻撃やプログラムの情報は、専門のセキュリティアナリストが分析し、セキュリティ脅威と判断された場合、攻撃情報をブラックリストとしてクライアント PC やセキュリティゲートウェイに配信し、以降の類似脅威をブロックします。

3. サービス提供開始日

2015 年 4 月提供開始予定

4. サービス提供における 3 社の役割

- NTT Com：
  - 総合リスクマネジメントサービス「WideAngle」のセキュリティ運用ノウハウを融合しつつ、「Zero day Attack Protection」（仮称）のサービス提供を通じて、顧客企業への総合的なセキュリティ対策の提示、他のセキュリティ対策への防御連動や脅威検知の高度化を実現します。

- 日本マイクロソフト：
  - カーネルモードまで含めた Windows 上の各種情報から攻撃を分析し、本サービスによるセキュリティ対策に反映します。

- FFRI：
  - 標的型攻撃対策ソフトウェア「FFR yarai」のヒューリスティック検知技術[*2]によるエンドポイント保護を担い、未知のマルウェアや脆弱性を悪用したゼロデイ攻撃から情報資産を守ります。

*1：Windows を実行しているコンピューターのプロセッサには、ユーザーモードとカーネルモードの 2 つの動作形態があり、ユーザーが利用するアプリケーションはユーザーモードで、OS の根幹部分（コア コンポーネント）はカーネルモードでそれぞれ実行されます。これまでの多くのセキュリティ対策サービスは、主にユーザーモードが対象であり、カーネルモードまで対象とするのは難しい状況にありました。

*2：マルウェアや攻撃コード等の不正プログラムを検知する際に、パターンファイルやシグネチャによるマッチングではなく、不正プログラムが持つ特徴的なプログラムの構造や振る舞いを検知する技術。