News Release

2015 年 10 月 2 日

総合リスクマネジメントサービス「WideAngle」において 未知のマルウェア（ウイルス）への対策を大幅に強化

NTT コミュニケーションズ株式会社（略称：NTT Com）は、2015 年 9 月 30 日より、総合リスクマネジメントサービス「WideAngle」において、プロフェッショナルサービス「コンサルティング」および「レスキューサービス」における未知のマルウェア（ウイルス）への対策を大幅に強化します。

従来、NTT Com は、お客さま企業のネットワーク環境にて、未知のマルウェアの侵入を検知し、当該検知と連動して外部向けの不正通信を迅速に遮断する「リアルタイムマルウェア検知（RTMD）」をサービス提供してきました。今回、本サービスの検知ノウハウなどを活用し、お客さま企業の PC やサーバーなど、エンドポイントまでを対象としたセキュリティ対策の立案・策定から、インシデント対応に至るまで、未知のマルウェアへの対策全般を強化し、標的型攻撃などによる、お客さまの情報詐取リスクを大幅に低減します。

1．背景

標的型攻撃などサイバー攻撃による企業や官公庁からの情報詐取には、アンチウイルスソフトなどの従来の対策では検知できない未知のマルウェアが関与しています。その対策として、ネットワーク環境での検知が有効ですが、多層防御を潜り抜けてエンドポイントに到達するマルウェア、長期間潜伏して情報収集活動を行うマルウェアや USB メモリなどネットワークを介さずに端末に感染するマルウェアなど、お客さま企業のエンドポイントにおける対策が重要な課題となっています。

こうした中、NTT Com は、PC やサーバーなどのエンドポイントも含め、網羅的にマルウェア感染状況の把握ができるマネージドセキュリティサービス「End Point Threat Protection Validation & Isolation（EPTP V&I）」を開発するなど、「WideAngle」全般において、エンドポイントへの未知のマルウェア対策強化に注力してきました。

2．概要

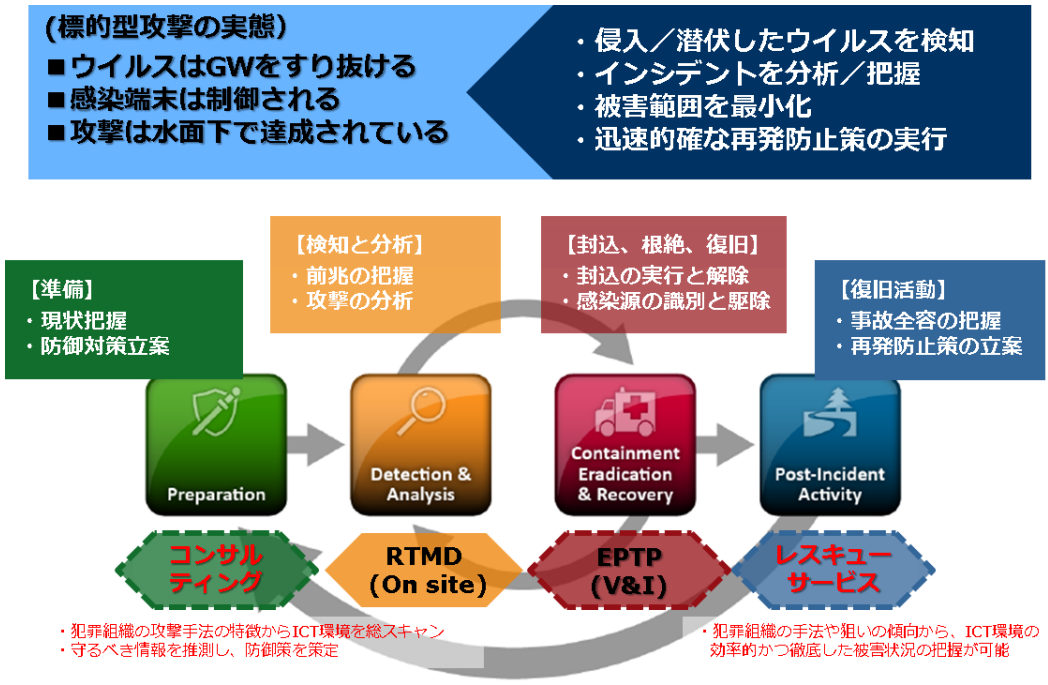
NTT Com は、「リアルタイムマルウェア検知（RTMD）」の提供を通じて蓄積した、未知のマルウェアに関する情報、それらを起因とした情報詐取活動の検知ロジックや分析ノウハウや、米大手サイバーセキュリティ企業 FireEye, Inc. [*1]（略称：FireEye）が保有する標的型攻撃を行う組織の侵入・攻撃手法などの知見を活用することにより、「WideAngle」において、

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

エンドポイントでの未知のマルウェア検知に加えて、潜伏・情報詐取を行うマルウェア有無の事前調査や感染後の事後調査・分析などを大幅に強化しました。

本強化により、従来提供していた、ICT 環境における不審なログの調査・分析に加えて、犯罪組織の攻撃手法や詐取対象とする情報種別などに関する傾向分析が可能となり、優先的に防御すべき情報を推測し、未知のマルウェアによる攻撃を受ける前に効果的な防御策を講ずることができます。

【サービス提供イメージ】*2



（1）コンサルティング（ICT 環境のリスクアセスメント）

一般的なセキュリティ対策とのギャップ分析によるリスク評価に加えて、自社の ICT 環境における感染状況を現状把握したいお客さま企業向けに、専用ソフトウェアなどを活用し、エンドポイントまでを対象として、マルウェアの潜伏状況や情報詐取の活動の有無を調査します。さらに、攻撃の痕跡から防御策を講ずることも可能となります。

（2）レスキューサービス（インシデント対応＆フォレンジック調査）

「リアルタイムマルウェア検知（RTMD）」で検出したお客さま固有のマルウェア情報などを活用することにより、セキュリティインシデント発生後の初動対応などに加えて、エンドポイントを含めたフォレンジック調査・分析や、犯罪組織の攻撃手法などの傾向分析を基にした迅速かつ効率的な被害状況の把握が可能です。

3．提供価格

（1）コンサルティング（ICT 環境のリスクアセスメント）：個別見積

提供価格例：初期費用 1,370 万円（税別）～

（前提条件）

・6 週間（実施～報告）

・調査対象端末（OS：Windows）4,000 台（ネットワーク経由で接続）

（2）レスキューサービス（インシデント対応＆フォレンジック調査）：個別見積

提供価格例：初期費用 4,125 万円（税別）～

（前提条件）

・3 カ月～4 カ月間（実施～報告）

・調査対象端末（OS：Windows）4,000 台（ネットワーク経由で接続）

4．提供範囲および提供開始日

日本：2015 年 9 月 30 日

海外：2016 年 3 月

（参考）End Point Threat Protection Validation & Isolation（EPTP V&I）

■サービスの特長

感染端末や範囲の特定など、マルウェアによる被害状況を把握できることに加えて、遠隔での感染端末の隔離も迅速かつ一元的に対応可能になります。また、NTT Com のセキュリティ運用ノウハウ*3 と FireEye の製品技術並びに専門的知識を組み合わせ、MSSP*4 モデルのサービスとしての提供により、お客さまは、従来、専門的なスキルが必要だったエンドポイントでのセキュリティ対策を、利用ユーザー数に応じた料金で導入することができます。

※詳細は 2015 年 3 月 12 日の報道発表を参照

■提供価格：個別見積

提供価格算定例（4,000-ID 利用時）：

初期工事費用 82 万円（税別）　　月額費用 194 万円（税別）

*1 FireEye のソリューションは、世界 67 カ国以上の 2,700 を超える組織にて導入されており、Fortune 500 企業の 157 社以上で利用されています。

*2 NIST (National Institute of Standards and Technology)発行「Guide to Malware Incident Prevention and Handling」（マルウェアによるインシデントの防止と対応のためのガイド）の「Figure 4-1. Incident Response Life Cycle」（インシデント対応のライフサイクル）を参考に作成

*3 NTT Com では、2012 年 7 月以降、約 20 社への導入・運用実績があります。また、NTT Com のグループ会社であり、WideAngle の提供事業者である NTT Com Security A.G では、多くの FireEye 技術者が在籍しており、同社では、FireEye の「トップ・パートナー・パフォーマンス」賞を APAC エリアとヨーロッパエリアの 2 つの地域で受賞しています。
FJSE（FireEye Certified Junior Systems Engineer） 20 名
FSE（FireEye Certified Systems Engineer） 8 名
FSP（FireEye Certified Support Professional） 32 名

*4 Managed Security Service Provider の略。ネットワークやシステムなどに関するセキュリティーサービスを提供する事業者。