News Release

2015 年 3 月 12 日

米大手サイバーセキュリティ企業 FireEye と協業し、
エンドポイントにおけるリアルタイムマルウェア検知を実現

～未知のマルウェアの検知から、感染端末の特定、隔離までのトータルマネジメント～

NTT コミュニケーションズ株式会社（略称：NTT Com）は、米大手サイバーセキュリティ企業 FireEye, Inc. [*1]（略称：FireEye）と協業し、未知のマルウェア（ウイルス）を検出する「WideAngle マネージドセキュリティサービス リアルタイムマルウェア検知（RTMD）」の対応範囲をエンドポイント(ネットワークに接続された PC やサーバーなど)にまで拡大し、2015 年度第 1 四半期より提供開始します。

今回の戦略的パートナーシップにより、お客さまは自社の ICT 環境においてこれまで検知が難しかった、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や長期間潜伏して情報収集活動を行うマルウェア、USB メモリなどを経由して端末に感染するマルウェアなどを捕捉できるようになり、さらに感染機器の迅速な切り離しが可能となるため、情報漏洩などのセキュリティ脅威リスクを大幅に低減できます。

１．背景

新種のマルウェアが次々と発生・蔓延し、巧妙な手口による不正アクセスなどのセキュリティリスクが増加するなか、企業が機密情報や顧客情報を守るためには、未知のサイバー攻撃を受けたとしても、それらを迅速に検知し、情報漏洩を防ぐことができる対策が必要不可欠です。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サイバー攻撃が急増する傾向があり、2020 年に向けて行政機関や電力・ガス・通信などの重要社会基盤事業者へのサイバー攻撃が更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 の「WideAngle マネージドセキュリティサービス」では、ICT 環境へのマルウェア侵入を検知するため、従来のマルウェア対策や侵入検知・防御対策に加えて、それらのパターンファイルやシグネチャベースでは検知できない未知のマルウェアをサンドボックス（Sandbox）と呼ばれる仮想実行環境で検出する「リアルタイムマルウェア検知（RTMD）」機能および感染に伴う外部向け通信を遮断する防御機能を提供中です。これら機能は中央省庁や大企業を中心とした多くのお客さまに導入が進む中、ネットワークにおける検知・遮断に加えて、PC やサーバーなどエンドポイントも含めた網羅的なマルウェア感染状況の把握と迅速な復旧対応が、被害・リスクを最小化するうえで必要な手段となってきました。

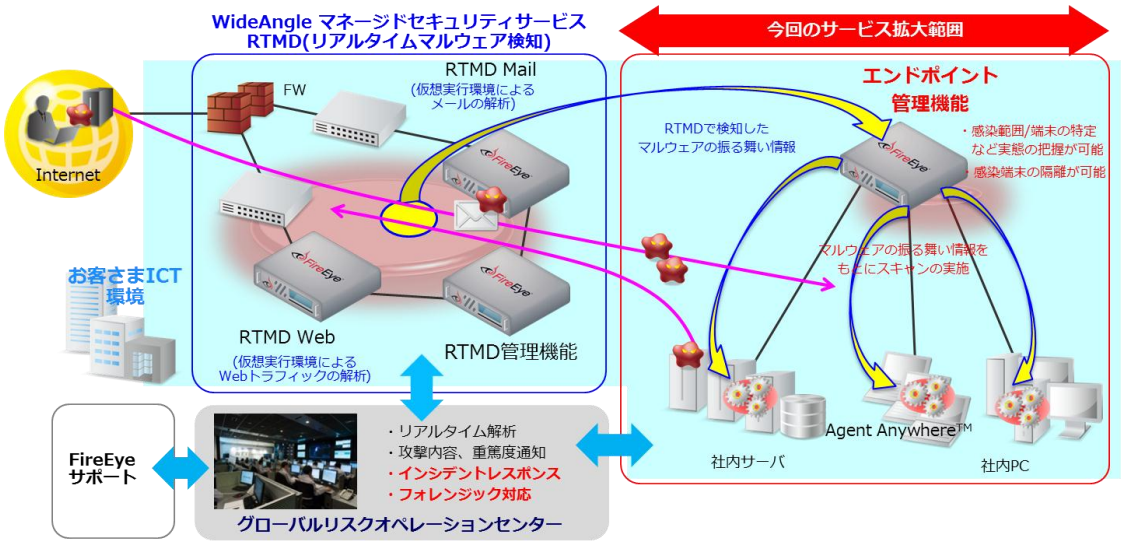
NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

2. 概要

NTT Com は、独自の仮想実行環境（MVX エンジン[*2]）を搭載しネットワークからエンドポイントまで複数経路から侵入したマルウェアの感染を検知および分析できる米大手サイバーセキュリティ企業 FireEye との戦略的パートナーシップにより、「WideAngle マネージドセキュリティサービス」の RTMD 機能を強化し、エンドポイントも含めた、お客さま ICT 環境における未知の脅威並びにマルウェア対策のトータルマネジメントを実現します。

これにより、感染端末や範囲の特定、情報漏洩の有無など、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。

【サービス提供イメージ】



■インシデントレスポンス：
・送受信ファイルの感染有無確認（RTMDサービスによる振る舞いでの未知のマルウェア検知）情報を活用し、LAN内の全PC/サーバーに対する総スキャンを行い、感染範囲を確認。
・エンドポイント管理機能を活用し、感染端末をLAN内からリモート操作で迅速に隔離。以降のマルウェア拡散を防止。

■フォレンジック機能：
・サーバー/PCの感染範囲証跡を記録し、情報漏洩など攻撃の活動範囲や内容を確認。

3. 提供価格

個別にお問い合わせください。

4. 提供範囲および提供開始日

日本に本拠地のあるお客さまへ、2015 年度第 1 四半期より提供開始です。

海外のお客さまへは、順次提供を開始していく予定です。

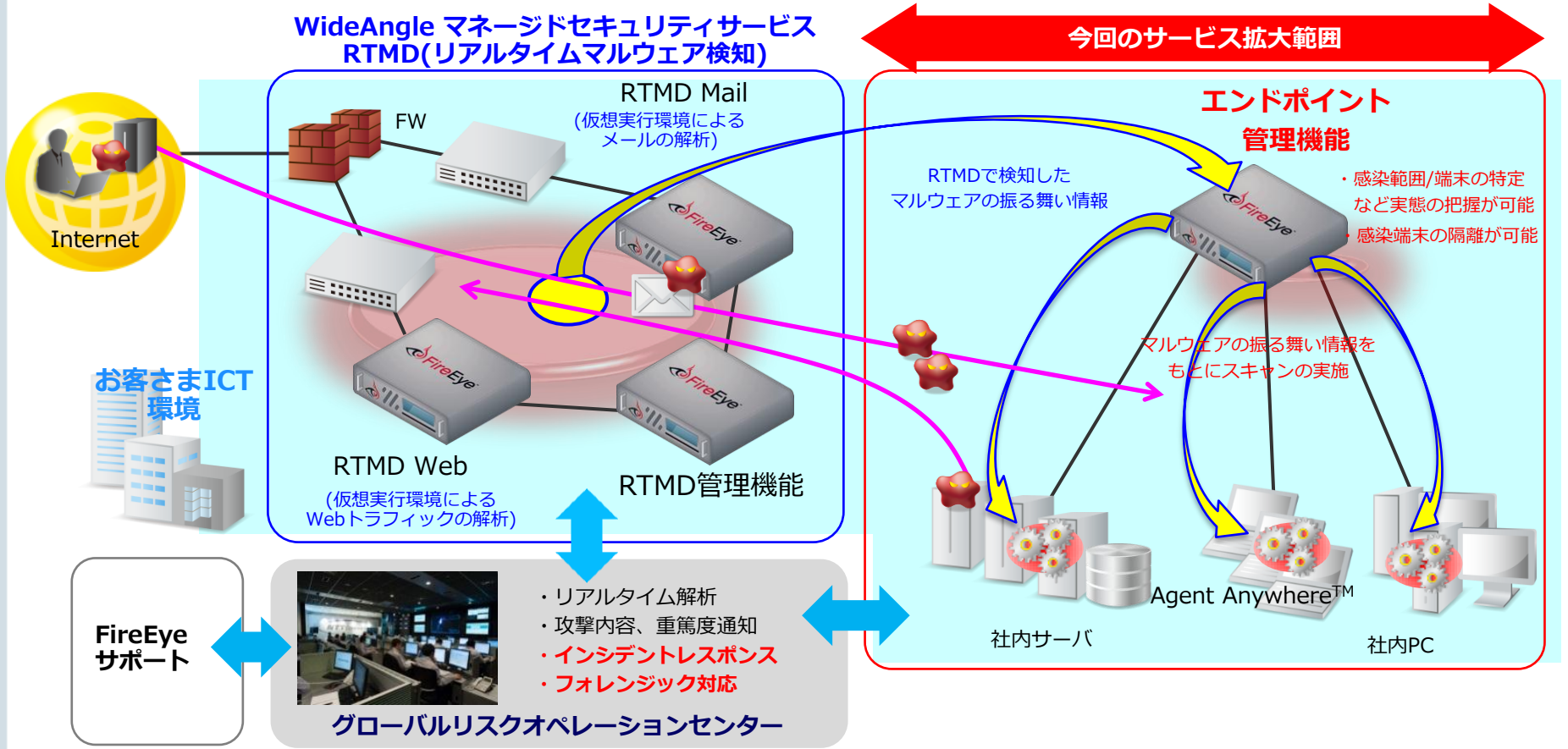
*1 FireEye のソリューションは、世界 67 カ国以上の 2,700 を超える組織にて導入されており、Fortune 500 企業の 157 社以上で利用されています。

*2 Multi-Vector Virtual Execution（MVX）エンジンは高度なマルウェアをリアルタイムで動的に解析する FireEye プラットフォームの核となる特許技術です。

*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。

【サービス提供イメージ】



■インシデントレスポンス：

・送受信ファイルの感染有無確認（RTMDサービスによる振る舞いでの未知のマルウェア検知）情報を活用し、LAN内の全PC/サーバーに対する総スキャンを行い、感染範囲を確認。

・エンドポイント管理機能を活用し、感染端末をLAN内からリモート操作で迅速に隔離。以降のマルウェア拡散を防止。

■フォレンジック機能：

・サーバー/PCの感染範囲証跡を記録し、情報漏洩など攻撃の活動範囲や内容を確認。

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.