News Release

NTT Communications

2015 年 7 月 17 日

日米大手セキュリティ企業 3 社と連携し、
標的型攻撃に対する通信遮断機能を大幅強化

～未知のマルウェア検知から、外部へ情報漏洩する通信の遮断までを高速化～

NTT コミュニケーションズ株式会社（略称：NTT Com）は、日米大手セキュリティ企業であるパロアルトネットワークス社[*1]・ブルーコートシステムズ社[*2]・デジタルアーツ社[*3]のセキュリティ機器と連携することにより、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）」の通信遮断機能を大幅に強化し、2015 年 7 月 18 日より提供開始します。

今回の機能強化により、お客さまは、完全に防ぐことが困難であった標的型メールなどの攻撃に用いられる未知のマルウェアの侵入検知に加えて、マルウェア感染端末と外部攻撃者間の通信を迅速に遮断し、重要情報の漏洩リスクを大幅に低減できます。

１．背景

標的型攻撃などのサイバー攻撃において、攻撃者側は新種のマルウェアをターゲットとなる企業や組織に送り込み、PC 端末などのエンドポイント（ネットワークに接続された PC やサーバなど）へ感染させます。その後、マルウェア感染端末を遠隔操作し、重要情報を外部へ送信させて窃取します。これに対して、企業側も、機密情報や顧客情報を守るため、標的型メールへの対応訓練などにより、エンドポイントにおけるマルウェア感染防止対策を行うケースが増えていますが、依然として、完全な感染防止は困難な状況です。つまり、エンドポイントにおけるマルウェア感染を防ぐことは不可能という前提で、未知のマルウェアの侵入検知や情報流出経路となる外部との通信を迅速に遮断する対策が必要となってきています。

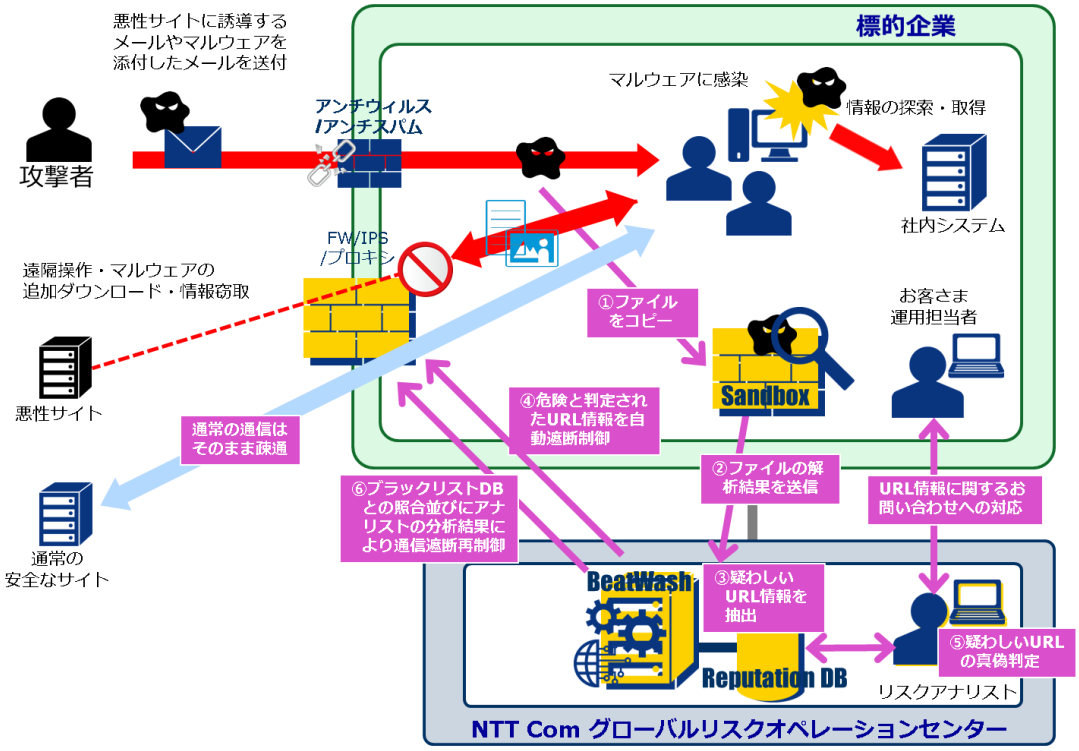
一方、NTT Com では、2012 年 7 月に未知のマルウェアの侵入を検知する「WideAngle マネージドセキュリティサービス リアルタイムマルウェア検知（RTMD）」を提供開始して以来、金融業界や中央省庁を中心に数十社で導入して頂き、さらに一部のお客さまには、通信遮断機能も先行導入して頂いておりました。また、2015 年 6 月から、NTT Com は、米大手サイバーセキュリティ企業 FireEye 社[*4]との戦略的パートナーシップにより、エンドポイントも含めた、お客さま ICT 環境における未知の脅威並びにマルウェア対策サービスの提供も開始しています。

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

今回、NTT Com は、「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）」において、エンドポイントでの防御対策に加えて、日米大手セキュリティ企業であるパロアルトネットワークス社・ブルーコートシステムズ社・デジタルアーツ社のセキュリティ機器などと連携し、情報漏洩を行う外部通信の迅速かつ高精度な遮断を実現します。これにより、情報漏洩リスクの低減や正常な通信の遮断による利便性低下の回避が実現可能です。

【サービス提供イメージ】



（1）迅速な通信遮断

パロアルトネットワークス社エンタープライズセキュリティプラットフォームの次世代ファイアウォールと連携し、マルウェアの疑いのあるプログラムの外部向け通信を平均 8 分（最大 15 分以内）で自動遮断します。また、多くの企業で採用されているブルーコートシステムズ社製のプロキシサーバ、並びにオープンソースであり同じく多用されている Squid によるプロキシサーバとも連携し、自動遮断します（平均 10 分、最大 20 分）。さらに、日本のお客さまに多く採用されているデジタルアーツ社製 Web フィルタリング製品（i-FILTER）への対応も可能となり、より多くの顧客の ICT 環境において防御機能を実現します。

（2）高精度な通信遮断

自動遮断開始と並行して、2 時間以内に、外部の通信先が真の攻撃者か否かの真偽判定・分析をセキュリティアナリストが行い、真の攻撃者であるという結果が出た場合、完全遮断へ移行、問題がなければ遮断解除を行います。

3．提供価格

「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）」の個別オプションとして提供します。価格は個別見積もりとさせて頂きます。

なお、2015 年 9 月に、標準オプションとして提供予定です。

4．提供範囲および提供開始日

日本および海外にて、2015 年 7 月 18 日より提供開始予定

5．今後の予定

NTT Com グループの保有するハニーポットや、国内外数百社以上のお客さま企業に対する「WideAngle マネージドセキュリティサービス」などの提供実績を通じて収集・蓄積された攻撃者情報を活用し、検知・防御能力の継続的な向上に努めます。

*1 パロアルトネットワークス社は、米国に本社を持ち、サイバー攻撃から数多くの企業、行政機関、プロバイダのネットワークを守るサイバーセキュリティのリーディングカンパニーです。同社の提供するセキュリティ・プラットフォームは、変化の激しい今日の IT 業界で重要となるアプリケーションやユーザー、コンテンツを基にセキュリティの保護を行い、お客さまのビジネス展開をサポートします。

*2 ブルーコート社は Web セキュリティ、高度な脅威防御、暗号化トラフィック管理、インシデント対応、フォレンジックまでを幅広く網羅し、最新の高度な脅威に対応する包括的なセキュリティソリューションを提供しています。ブルーコート全製品と連携する世界最大級の強固なクラウド型セキュリティインテリジェンスを特長とし、オンプレミスおよびクラウド型ソリューションを自由に組み合わせられるハイブリッド型の防御基盤を提供しています。Fortune Global 500 掲載企業の 86%（うち日本国内企業は 96%）を含む、世界中の 15,000 ものお客さまから、日本をはじめ世界中の大手企業の多くに採用され、世界的リーダーとして高い支持を得ています。

*3 デジタルアーツ社は、フィルタリング技術を核に、製品の企画・開発・販売・サポートまでを一貫して行う情報セキュリティ企業です。「i-FILTER」は国産初の Web フィルタリングソフトとして業界最

大級のデータベースと、世界 27 の国と地域で特許を取得したフィルタリングテクノロジー「ZBRAIN」により、業務中の閲覧が不適切な Web サイトを高い精度で遮断するほか、Web メールの利用や掲示板の書き込みなどといった、Web 経由の情報漏洩を防ぐとともに、その内容を記録・確認・保存することが可能なソリューションです。

*4 FireEye 社は、独自の仮想実行環境（MVX エンジン）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です。MVX エンジン（Multi-Vector Virtual Execution）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。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 Global 500 企業の 157 社以上で利用されています。

＊記載されている会社名および商品名は、各社の登録商標または商標です。