未来を拓くチカラと技術。

NTT AT

News Release

2017年6月15日
NTTアドバンステクノロジ株式会社

標的型攻撃やランサムウェア対策のシステム運用を代行
～「マネージド標的型攻撃対策サービス」を提供～

NTTアドバンステクノロジ株式会社（以下：NTT-AT、本社：神奈川県川崎市、代表取締役社長：木村丈治）は、企業や組織における標的型攻撃対策やランサムウェア対策の一環として、6月15日（木）より月額利用型サービス「マネージド標的型攻撃対策サービス」の提供を開始します。

各企業などにおいては、急増する標的型攻撃やランサムウェアによる被害に対し、サイバーセキュリティ対策の重要性や必要性は感じているものの、導入時の対応や導入後のシステム運用などの負荷が導入障壁の一つとなっており、導入に踏み込めない実態があります。

NTT-ATは、4年にわたり株式会社FFRI（本社：東京都渋谷区、代表取締役社長：鵜飼裕司）の一次販売店として標的型攻撃対策ソフトウェア FFRI yarai を販売しており、製品および標的型攻撃やランサムウェア対策の豊富なノウハウを保有しています。こうした実績を踏まえ、各企業が抱える課題に対応するため、安価なコストで運用代行までを行う「マネージド標的型攻撃対策サービス」を提供することといたしました。

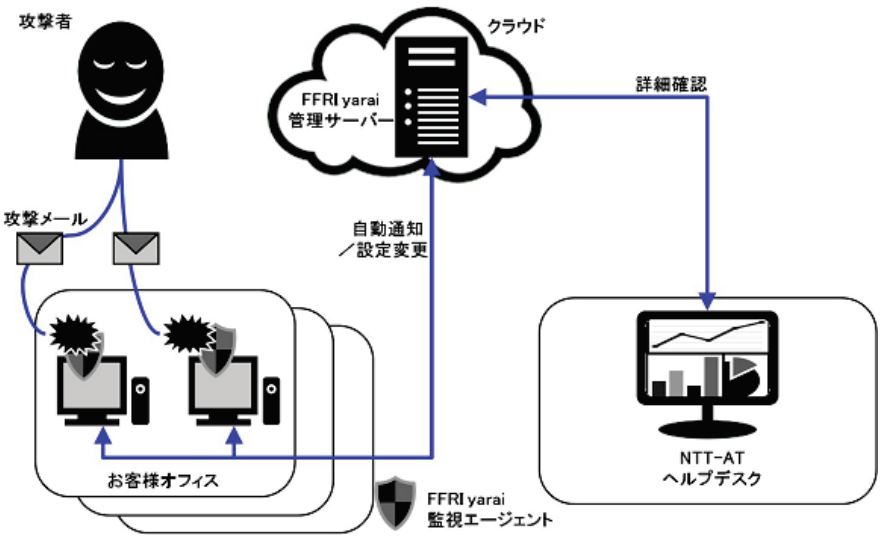
■背景およびサービス提供に至った経緯

近年、企業や政府機関を狙ったサイバー攻撃による被害が深刻化しています。なかでも本年5月、世界規模で発生し、多くの企業や公共機関に被害をもたらしたランサムウェア「WannaCry」は、世界中を震撼させました。急速に増え続けるこうしたマルウェアによる攻撃は、従来のウイルス対策ソフトでの検知や防御が難しく、重大な脅威になっています。

しかしながら、多くの企業、特に中堅・中小企業においては、サイバーセキュリティ対策の重要性や必要性は感じているものの、専門の組織や人材を抱える状況になく、導入時のライセンス管理などの対応や導入後のシステム運用の負荷が導入障壁の一つとなっており、導入が進まない要因となっています。

このような状況の中、NTT-ATが提供中の標的型攻撃対策ソフトウェア FFRI yarai は、この攻撃に利用されるマルウェア特有の“振る舞い”をリアルタイムに検知・防御し、機密情報の流出やパソコンやサーバーへの遠隔攻撃などを未然に防止することで、情報資産のみならず信頼を守ります。

今回NTT-ATが提供を開始する「マネージド標的型攻撃対策サービス」は、システム運用を代行することで、標的型攻撃対策やランサムウェア対策を早期にかつ安価で継続的に利用することが可能です。



【NTT-AT が提供するマネージドサービス】

■サービスの概要

- 標的型攻撃やランサムウェアは、メールまたは Web 経由で侵入してきます。
- お客様がパソコン上で攻撃ファイルを開くと、FFRI yarai がリアルタイムに攻撃を検知・防御します。
- それと同時に、クラウド上に設置されている FFRI yarai の管理サーバーへ自動的に通知されるとともに、NTT-AT ヘルプデスクへも第一報が届きます。
- NTT-ATの技術者が検知内容を調査し、監視条件のチューニングを実施します。また、お客様管理者へ検知内容を通知し、お客様社内で実施される侵入経路の調査などに活用いただきます。

■サービスの特長

「マネージド標的型攻撃対策サービス」の主な特長は以下のとおりです。

・安価な利用料
　標的型攻撃やランサムウェアの防御実績豊富な FFRI yarai を月額払いで利用可能。端末当たりのライセンス利用料は 500 円

・お客様専用ポータルサイト(予定)
　ライセンス追加・削減申請や、組織内における監視結果の一覧表示を希望されるお客様専用ポータルサイトなど、NTT-AT独自機能の提供

・付加サービス(予定)
　万が一の被害発生時の調査・復旧費用を支援する保険サービスも付加

■利用料金

区　分	価　格	内　容	備　考
初期登録料	120,000 円	初期登録作業費	初年度のみ
FFRI yarai 利用料	500 円／月	・FFRI yarai ライセンス利用権 ・FFRI yarai 運用代行費	・端末当たり ・インシデント保険付き （検知できなかったランサムウェア等に対する復旧支援費）

注 1:価格は税抜き　　注 2:最低利用数 100 端末、最低利用期間 1 年

【費用算出例(100 端末)】

①初期登録料　　1 登録×120,000 円　　＝　120,000 円

②FFRI yarai 利用料　　100 端末×500 円×12 ヶ月　＝　600,000 円　　合計　720,000 円

■今後の展開

標的型攻撃やランサムウェアへの対策には FFRI yarai が有効ですが、万全な不正アクセスへの備えとしてはネットワーク対策も重要です。特に、UTM※1／Firewall の機能を最大限に引き出すには、アウトソースによる効果的な運用が必要不可欠です。NTT-AT では、これらに対応するため多層防御ソリューションを用意しており、今後さらに強化していく考えです。

■標的型攻撃対策ソフトウェア「FFRI yarai」について

FFRI yarai シリーズは、従来のセキュリティ対策で用いられているパターンファイルなどに依存せず、標的型攻撃で利用される攻撃の特徴を 5 つのヒューリスティックエンジン※2 により、さまざまな角度から分析し、既知・未知の脅威に対し高い精度で攻撃を検知・防御します。官公庁を始め重要インフラ提供企業、金融機関で多数導入されています。

※1:UTM(統合脅威管理)とは、企業などで、コンピューターウイルスや不正アクセスなどネットワークセキュリティに関わる対策を統合的に管理する手法のこと。

※2:ヒューリスティックエンジンとは、パターン・マッチング方式ではなく、類推してウイルスかどうかを判定するエンジンのこと。

本件に関するお問い合わせ先

ＮＴＴアドバンステクノロジ株式会社
セキュリティ事業本部
ソリューション開発ビジネスユニット
yarai（ヤライ）担当
ＴＥＬ：044-589-6508
E-mail：ta-support.nan@ml.ntt-at.co.jp