News Release

2015 年 10 月 7 日

「WideAngle」のマネージドセキュリティサービス運用基盤に 人工知能を搭載し、サイバー攻撃への分析力を大幅強化

NTT コミュニケーションズ株式会社（略称：NTT Com）は、2015 年 10 月より、総合リスクマネジメントサービス「WideAngle」のマネージドセキュリティサービスの運用基盤（SIEM）において、人工知能の要素技術の 1 つとされる機械学習機能[*1] などを用いて、攻撃者との通信を検知する機能を独自開発し、企業 ICT 環境へのサイバー攻撃に対する検知・分析力を大幅に強化します。

1．背景

企業の機密情報などを詐取する標的型攻撃や Web サイトへの DDoS 攻撃は、新種のマルウェアや新しい攻撃手法などにより、日々、高度化しています。そうした未知のセキュリティ脅威を防御するには、過去の攻撃手法を基にしたパターンマッチングやブラックリスト方式による検知・遮断などの従来対策では不十分な状況です。また、昨今のサイバー攻撃の多くは、専門スキルを有した犯罪者集団により、膨大なコンピュータで構成される攻撃用ネットワーク（ボットネット）や外部から遠隔操作可能なコンピュータ（コマンド・アンド・コントロールサーバー）などが巧妙に組み合わされ、実行されています。

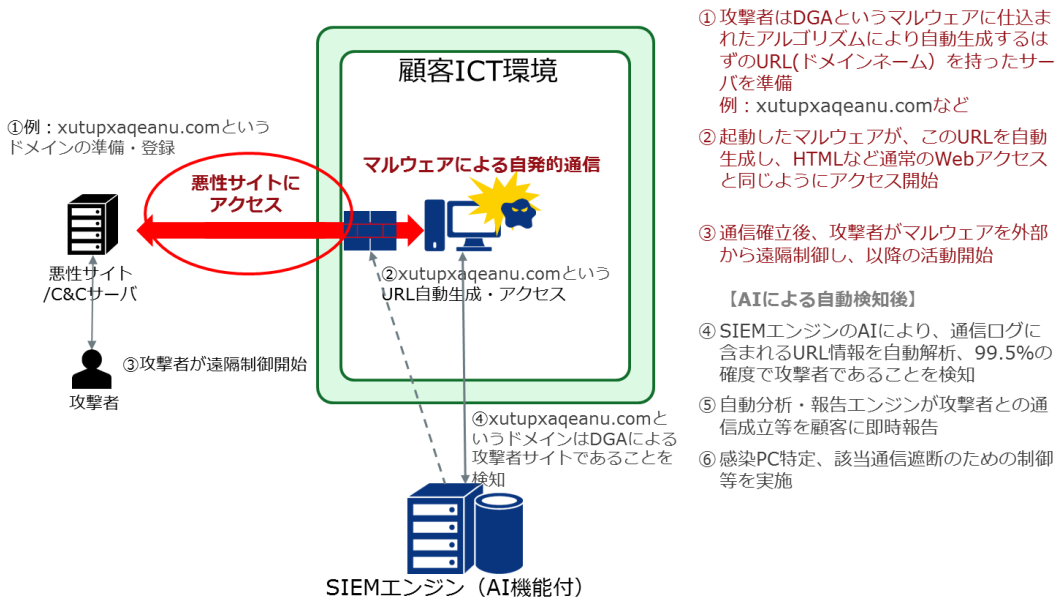
こうした中、企業の情報資産を守るためには、未知のセキュリティ脅威を用いるサイバー攻撃を、リアルタイムに検知・判別し、迅速に遮断する仕組みが重要となってきました。

2．概要

NTT Com は、数多の未知のセキュリティ脅威を、リアルタイムに検知・判別する仕組みとして「人工知能」を独自に開発し、「WideAngle」のマネージドセキュリティサービスの運用基盤（SIEM）に組み込みました。独自開発した人工知能では、DGA[*2] という計算手法や、自動生成していく悪性サイトの URL 生成特性を自律的かつリアルタイムに機械学習し、攻撃者との不正な通信のみを検知する検出ロジック[*3] などを活用し、過去のブラックリストに無い悪性サイトへの通信検知を実現します。このような悪性サイトとの不正通信を、人工知能を活用してリアルタイムに検知できるサービスは世界初であり、誤検知率も 0.5%と高精度の検知が可能です。

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

【人工知能（AI）による攻撃者との通信検知イメージ】



迅速な攻撃サイトとの通信検知を実現することにより、WideAngle MSS では精度の高い顧客への迅速な報告、感染エンドポイントの隔離・遮断や IPS[*4] や URL フィルタ[*5] などを用いた即時での悪性通信遮断へのアクションと結びつけていくことが可能となります。NTT Com では、これら人工知能活用による高度な攻撃検知に加えて、エンドポイントセキュリティ対策として攻撃の証跡データを活用した全ての感染エンドポイントの確定とネットワークからの遠隔での切り離し、IPS/URL フィルタ等を活用した即時遮断の実施などの総合的なサービスを提供しています。

3. 今後の予定

NTT Com は、企業の ICT 環境をサイバー攻撃から守る手段として、人工知能に関わる研究・開発活動を継続しており、顧客毎にカスタマイズされた巧妙な攻撃に対して、不審な通信・振る舞いを検知する機械学習機能[*6] についても開発着手しています。

また、通信情報を基に、ボットネットや APT 攻撃[*7] 特有の振る舞いを観察する機能や、情報詐取方法の特長を学習し、検知する機能の開発に着手しており、本機能は 2016 年春を目処にマネージドセキュリティサービスの自動分析基盤に組み込む予定です。今後も、NTT Com は、人工知能を活用したサイバー攻撃の検知機能の向上に継続して取り組む予定です。

*1: マネージドセキュリティサービスにおいて、継続的なエキスパートシステムとして、事例ベース推論を骨子とする AI 機能を盛り込んだ追加開発を経て、未知の脅威検知や検知精度の向上を実現します。

*2: Domain Generating Algorithm の略で、URL アドレスであるドメインネームを自動で生成するための計算手法であり、生成手法をカスタマイズ可能で、多くのマルウェアで活用されている。

*3: Random Forest、あるいは Gradient Boosting と呼ばれる回帰分析、クラスタリングによる集団学習アルゴリズムを採用し、悪性サイトへの通信要求時点で、その URL が正規で正当なものか攻撃者の用いるサイトの URL の特徴を有しているかを判定。

*4: Intrusion Protection System の略で、外からの既知の攻撃パターンに対する防御、マルウェアの削除などを実行するセキュリティアプライアンス製品。

*5: 企業内網の PC 等のエンドポイントから外部の Web サイトへの通信時に、代理人として通信を仲介する機能が主たる目的であるが、特定の Web サイトへの通信を遮断することが可能。

*6: Time Isolated Behavior Structures と呼ばれる、一見散発的に発生する通信パターンや、ボットネットのように複数の同期した通信パターンを検知し、マルウェアへの感染や、攻撃者からの遠隔制御時に見られる行動パターンを検知するもの。

*7: Advanced Persistent Threat の略で、特定のターゲットに狙いを定め、そのターゲットに適合した方法や手段を適宜用いて、システムへ侵入・潜伏し、数カ月から数年に渡って、継続的に行うサイバー攻撃。