

# 最

近いろいろな局面において Intelligence (インテリジェンス) という言葉が注目を浴びており、異なった意味で使われている。サイバーセキュリティの観点から、この言葉がどのように使われどのように関連するか整理してみたい。

国家間の情報収集のためのインテリジェンスは、「政策決定者が、国家の安全保障に関する政策決定をするために提供される情報収集・分析活動」<sup>1)</sup>をいう。ここには、スパイ活動による情報入手を行うヒューマンインテリジェンス (Human Intelligence) や、通信などの傍受に基づく諜報活動であるシグイント (SIGINT, 英語: Signals Intelligence) がある。

通信の手段が発達してきて、インターネット等のサイバー空間のシステムを利用して情報を得ようというのが、シグイントの発展形であるサイバーインテリジェンスであり、本稿で対象とする1つ目のインテリジェンスである。警察庁によれば、サイバーインテリジェンスとは「情報通信技術を用いた諜報活動であり、機密情報が窃取されれば、我が国の治安、外交、安全保障、社会経済活動等に重大な影響が生じるおそれがある」としている<sup>2)</sup>。インターネットを流れる情報やサーバの中身を監視したり、標的型攻撃のようにインターネットを構成するサーバやPCに侵入して情報を取り出すということも行われている。

サイバーインテリジェンス等の目的のためのサイバー攻撃から自国の安全を確保するためには、適切なセキュリティ対策を行うことが大切になる。このためには攻撃側の出方を適切に把握するための手段が必要になる。これがセキュリティインテリジェンスであり、本稿で扱う2つ目のインテリジェンスである。セキュリティインテリジェンスは、「セキュリティ対策に必要な高度な情報やそれを得るための行動」と考えておくとよいだろう。情報のもととなるデータとしては、通信やシステムの大量のログが主対

象となる場合が多い。今後は、国際政治や社会状況もデータとして組み込みつつ、セキュリティインテリジェンスを行うことが必要になっていくだろう。

このセキュリティインテリジェンスを行うために、機械学習やデータマイニングなどの技術が使われ始めている。これがもう1つのインテリジェンス、アーティフィシャルインテリジェンス (AI: Artificial Intelligence) である。私は、セキュリティ対策におけるAIの応用分野はもっと広いだろうと考えている。標的型攻撃等の高度な攻撃に対処できるセキュリティ人材は非常に限られている。そこで、私たちは自動的な応急対応を可能とするとともに、運用者



[シニアコラム]

## IT好き放題



[No.63]

### サイバーセキュリティにおける3つのインテリジェンス

が適切な対策をとれるようにするため、ルールベースのAIを用いたLIFT (Live and Intelligent Network Forensic Technologies: 以下LIFT) システムの開発を2013年から行ってきた<sup>3)</sup>。この結果、過去に起こった種々の攻撃には適切な対策がとれる見通しが得られた。しかし、新しい攻撃に対応するのは困難であるという問題が残っている。この問題を解決し、Beyond the Attackersの実現を可能にするためマルチエージェントなどのAI技術を用いるSuper-LIFTの研究・開発をスタートした<sup>3)</sup>。

今後AI機能を持つマルウェアは確実に現れるのである。攻撃側が賢くなる以上、防御側もAIを用いて賢くならざるを得ないと思う。さらに、セキュリティ技術者は長い間、新しい攻撃が出てきて初めて後追いで研究を行ってきた。これでよいはずはないのである。困難ではあるが高い研究目標を設定し、なんとか先回りして対策ができるようにしていきたいと考えている。

#### 参考文献

- 1) 伊東 寛: サイバー・インテリジェンス, 祥伝社新書(2015).
- 2) 警察庁: <https://www.npa.go.jp/keibi/biki3/230804shiryuu.pdf>
- 3) 佐々木良一, 八楨博史: 標的型攻撃に対する知的ネットワークフォレンジックシステムLIFTの開発(その3) - 今後の研究構想 -, 情報処理学会 DICOMO2015.

(2015年12月19日受付)

佐々木良一 Ryoichi SASAKI

東京電機大学

[正会員] sasaki@im.dendai.ac.jp

1971年東京大学卒業。日立製作所入社。システム開発研究所にてセキュリティ等の研究を実施。2001年より東京電機大学教授。日本セキュリティ・マネジメント学会会長、内閣官房サイバーセキュリティ補佐官。