2016 年 12 月 13 日

各　位

株式会社　三井住友銀行
株式会社　日本総合研究所

AI を活用したサイバーセキュリティの強化について

株式会社三井住友銀行（頭取：國部　毅、以下「三井住友銀行」）、株式会社日本総合研究所（代表取締役社長：渕崎　正弘、以下「日本総研」）は、高度化するサイバー攻撃への対応力強化の為、AI を活用し、(1)サイバー攻撃に関する情報を自動分析、(2)セキュリティ監視での検知内容に関する情報を自動検索する取組みを開始いたしました。

(1) サイバー攻撃に関する情報を自動分析する取組みについて

FS-ISAC(*1)等の外部機関から共有された世界中のサイバー攻撃に関する手口や傾向等の膨大な脅威情報に対して、AI が自然言語処理技術を用いて自動的に分析し、セキュリティ対策に有用な情報を抽出することで、新たに確認されたサイバー攻撃に対する防御や検知を行います。

一般的には、こうした脅威情報に対して、セキュリティ技術者が１件１件内容を分析したうえで、監視システム等にサイバー攻撃を防ぐための設定を行いますが、AI の活用により、世界中の脅威情報を迅速かつ正確に監視システム等に反映することができ、日々高度化するサイバー攻撃に備えることが可能となります。

本件は、FS-ISAC に蓄積された 25 万件以上の脅威情報に対して自動で分析を行う本邦初の試みとなります。将来的には、本取組みで得られたノウハウを金融業界全体で活用することも検討しています。

(2)セキュリティ監視での検知内容に関する情報を自動検索する取組みについて

監視システムで検知した不審な通信・挙動について、AI が世界中の文献や専門家のブログ等の情報源から学習・蓄積したセキュリティ関連情報から、検知内容に対する攻撃手口や脅威度を検索することで、セキュリティ技術者が対処方法等を判断するための支援を行います。

一般的には、検知した不審な通信・挙動について、セキュリティ技術者が都度調査を行ったうえで対応を行いますが、AI の活用により、関連性が高い最新情報を的確に収集することができ、セキュリティ技術者はこれまで以上に迅速かつ正確に対応することが可能となります。

本件は、“IBM Watson for Cyber Security”(*2)を活用した、世界 8 大学、約 40 社が共同で取り組むトライアルプログラムに、三井住友銀行が本邦で唯一参加して行うものです。

三井住友銀行および日本総研では、これまでもサイバーリスクを経営上の重大なリスクのひとつと定義し、専任要員によるセキュリティ監視体制(*3)を構築し、サイバー攻撃の早期検知に取り組んでまいりましたが、本取組みを通じサイバー攻撃への対応力を更に高め、重要な社会インフラとして、お客さまの資産を安全に保護し、安心して金融サービスをご利用いただけるよう努めてまいります。

(*1)FS-ISAC
米国で業を行う金融機関を会員とするセキュリティ情報分析結果の共有を目的とする会員制組織。三井住友銀行も加盟。

(*2)IBM Watson for Cyber Security
膨大な自然言語を理解・学習し、より適切な意思決定を支援する IBM の Watson をサイバーセキュリティ対策に応用する取組み。なお、三井住友銀行ではこれまでに、コールセンター業務にて Watson を活用。

(*3)セキュリティ監視体制
Security Operation Center（SOC）と呼ばれ、専任要員がセキュリティ監視・分析とその対処を実施。

以　上