戦略的創造研究推進事業　CREST
研究領域「イノベーション創発に資する人工知能基盤技術の創出と統合化」
研究課題「サイバー脅威ビッグデータの解析によるリアルタイム攻撃検知と予測」

研究終了報告書

研究期間　2017年　10月～2020年　3月

研究代表者：関谷　勇司
（東京大学情報基盤センター、教授）

§1 研究実施の概要

(1)実施概要

本研究の目的は、人工知能技術を用いて個人の知識や経験に左右されないサイバーセキュリティ対策のアシストを実現することである。現在のセキュリティ対策は、セキュリティの専門家による知識と経験に依存している。すなわち、優れたセキュリティ専門家のいない組織はセキュリティ対策がおろそかになりがちであり、セキュリティ事故が発生した場合にも、対応が後手になり被害が拡大しがちである。そこで本研究では、図 1 に示すサイバーセキュリティ対策フローに人工知能技術を適用し、セキュリティ担当者のアシストを行う手法とシステムを確立することを目指した。

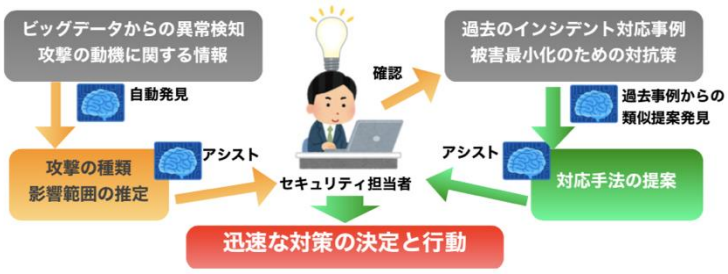

図 1： 人工知能を利用したサイバーセキュリティ対策のアシスト

スモールフェーズの主な成果として、(1) サイバーセキュリティ脅威の検知に関するデータセット前処理の手法と機械学習アルゴリズムへの適用手法の開発、(2) データセットの蓄積・解析基盤 Hayabusa の開発と実運用、(3) インシデント対応の自動アシストに向けたインシデントレスポンス情報の正規化と自然言語処理の適用、があげられる。これらの成果に関して、論文としての発表、オープンソースとしての公開、特許の出願を行った。それぞれの研究グループの主な成果を以下に述べる。

- 東大グループ

  サイバー脅威を検知するためのデータセットの収集、およびそのシステムの設計と開発を行った。また、収集したデータセットに機械学習を適用することで、複数種類の攻撃を検知するための手法を開発した。これにより、機械学習を用いたサイバー脅威の検知が可能であることを実証した。また、その手法に関する特許出願も行った。

  さらに、インシデントレスポンスの対策アシストに関して、自然言語処理を用いた類似事例の抽出に取り組んだ。これらの成果は、本研究成果の中核をなすものであり、最大の貢献を行った。

- 東工大グループ

  AI 技術を用いてインシデントレスポンスのアシストを行うにあたり必要となる、インシデントレスポンスデータセットの調査、及びデータフォーマットの正規化、また自然言語処理を利用した類似事例の抽出に関して取り組んだ。加速フェーズにつながる重要な研究課題に関する貢献を行った。

- IIJ グループ

  サイバー脅威検知に必要となるデータセットの調査と定義、およびそれらデータセットのリアルタイム収集と分析に必要となる解析基盤 Hayabusa の開発を行った。スモールフェーズでの中核となる要素技術の研究開発に取り組み、貢献した。

- 奈良先グループ

  単一データセット、および複数データセットを用いたサイバー脅威検知手法の開発に取り組んだ。特に、データセットの画像化に関する基本アイディアと、提案手法の評価に関して取り組み、チームに貢献した。

(2)顕著な成果

＜優れた基礎研究としての成果＞

1. サイバーセキュリティデータセットの AI 技術への適用手法

概要: まだデータセットの処理方法とアルゴリズムへの適用手法が確立していないサイバーセキュリティ脅威検知への AI 技術適用手法を提案した。データセットの前処理の手法や既存アルゴリズムへの適用手法を発案し、実データを用いた検証を行った結果を論文として公開し、手法を特許申請した。

2. インシデントレスポンスのデータセットおよびフローの正規化

概要: 今までは属人的な経験と知識に基づいて行われてきたインシデントレスポンスの処理フローを、AIによるアシストに適応すべくデータセットとフローの正規化を行った。また、正規化したデータセットを用いて自然言語処理を行うための基礎段階の手法を提案した。

＜科学技術イノベーションに大きく寄与する成果＞

1. インシデントレスポンスにおける「対策アシスト」を目指した手法

概要: サイバーセキュリティ脅威に対抗するにあたり、「対策のアシスト」を前提としたサポートシステムを構築した。これはサイバーセキュリティ分野において、個々の脅威の検知ではなく対応策のアシストを行うという意味において独自性のある研究であり、製品化の可能性を持つ研究である。

2. 実データを用いたサイバーセキュリティ脅威の検知

概要: 公開されているテストデータのみならず、大学の環境や Interop Tokyo 2018, 2019 における実ネットワークにおけるデータを用いて AI 技術を用いたリアルタイム検知の実証実験、及び評価を行っているため、実環境に適用しやすい技術開発となっている。

＜代表的な論文＞

1. Ryo Nakamura, Yuji Sekiya, Daisuke Miyamoto, Kazuya Okada and Tomohiro Ishihara, "Malicious Host Detection by Imaging SYN Packets and A Neural Network", IEEE International Symposium on Networks, Computers and Communications (IEEE ISNCC'18), Roma, Italy, June 2018
2. 阿部博, 島慶一, 宮本大輔, 関谷勇司, 石原知洋, 岡田和也, 中村遼, 松浦知史, 篠田陽一, "時間軸検索に最適化したスケールアウト可能な高速ログ検索エンジンの実現と評価", 情報処理学会論文誌, 60 巻 3 号, pp. 728-737, 2019 年 3 月
3. 石井将大, 森健人, 松浦知史, 金勇, 北口善明, 友石正彦 : "東工大 CERT におけるインシデント対応の分析とその自動化に関する考察", 研究報告インターネットと運用技術 (IOT), Vol. 2018-IOT-43, No. 2, pp. 1-8, 2018 年 9 月

§2 研究実施体制

(1)研究チームの体制について

① 東大グループ

研究代表者：関谷　勇司（東京大学情報基盤センター　教授）

研究項目

・ストリーミングデータ解析基盤の設計
・サイバー脅威データの収集及び蓄積
・データセットの定期的な見直し
・複数のデータセットを用いた異常検知
・サイバー攻撃の予測
・サイバー攻撃の影響範囲の予測

② IIJ グループ

主たる共同研究者：島　慶一（(株) IIJ イノベーションインスティテュート技術研究所　副所長）

研究項目

・サイバー脅威データのサーベイ
・ストリーミングデータ解析基盤の構築
・実験環境の要件定義
・テスト環境の設計

③ 東工大グループ

主たる共同研究者：松浦　知史（東京工業大学学術国際情報センター　准教授）

研究項目

・インシデントレスポンスの調査
・インシデントレスポンス自動化手法の開発
・インシデントレスポンス自動化基盤の設計・実装
・小規模環境での実験

④ 奈良先グループ

主たる共同研究者：門林　雄基（奈良先端科学技術大学院大学情報科学研究科　教授）

研究項目

・単一のデータセットによる異常検知

(2)国内外の研究者や産業界等との連携によるネットワーク形成の状況について

月に1回行っているグループ全体定期ミーティングに、株式会社 Preferred Networks の研究者に参加してもらい、機械学習アルゴリズムの適用や評価手法に関して助言をもらった。また、通信キャリアの実際のセキュリティ事情をふまえた研究課題の設定を行うために、通信事業者の研究者とも定期的に会合を行い、情報交換を行った。

海外との連携に関しては、ニュージーランドの Unitec 工科大学と交流を行い、東大グループに参加してもらうことで、データ収集と分析に関する助言を得た。また、

また、産業界との連携に関しては、Interop Tokyo 2018 という IT イベントに技術出展を行い、約14万人が来場する会場内のネットワークトラフィックを用いて、研究開発した攻撃検知手法のライブデモンストレーションを行った。その結果、いくつかの企業からコンタクトを頂き、手法の実用化に向けた検討を開始した。