「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」
平成 29 年度採択研究代表者

H29 年度
実績報告書

関谷 勇司

東京大学情報基盤センター
准教授

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

§1. 研究実施体制

(1)東大グループ
① 研究代表者:関谷 勇司(東京大学情報基盤センター 准教授)
② 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格納
・サイバー攻撃の予測

(2)IIJ グループ
① 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 主幹研究員)
② 研究項目
・サイバー脅威データのサーベイ

(3)東工大グループ
① 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)
② 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

(4)奈良先グループ
① 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)
② 研究項目

・単一のデータセットによる異常検知

§2. 研究実施の概要

本研究のゴールは、人工知能技術を用いることで、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行うことである。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す。

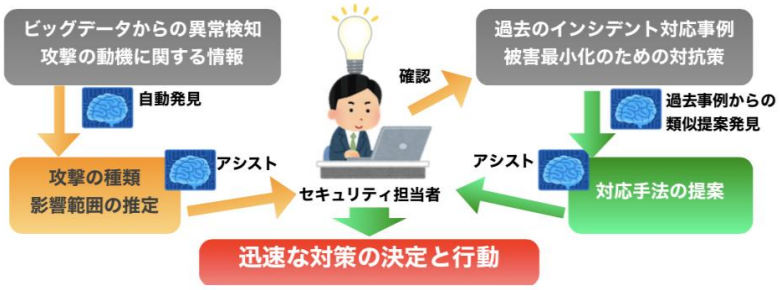

図 1 ： サイバーセキュリティ対策における人工知能によるアシスト

このアシストを実現するために、本年度は主に、(1) リアルタイムデータ蓄積・解析基盤の設計と実装、(2)機械学習技術を利用した攻撃者の挙動解析、(3) サイバー脅威解析に利用できるデータセットの分類とインシデントレスポンスのフロー分類、の 3 点を重点とした研究を行った。どれも人工知能技術を用いたセキュリティ対策をアシストするための要素技術であり、本研究の基礎となる部分である。

(1)の成果としては、多種多量のデータをリアルタイムに蓄積し、解析するためのシステムを設計ならびに構築した。10 台のサーバを用いた環境において、毎秒 5 万メッセージを記録しつつ、蓄積された 140 億メッセージの情報からキーワードの全文検索を 5 秒で行う性能を達成した。この成果の詳細に関しては、論文[1]にて公開した。

(2)に関しては、組織外からの攻撃を検知するための技術と、組織内からの危険なサイトへのアクセス検知に取り組んだ。これらの検知は、従来の手法では「シグネチャ」と呼ばれる、過去に発生した攻撃パターンを蓄積することで実現されていた。しかし本研究では、機械学習を利用して攻撃を判定することで、過去の攻撃パターンを蓄積する必要もなく、かつ亜種の攻撃も検知できる可能性がある技術を確立した。また、ネットワークから得られるデータセットを機械学習に適用するにあたっても、パケットのベクトル化や URL のベクトル化(図 2)など、既存研究とは異なる新しいアプローチを実現した。この成果は、論文[2]にて公開した。

(3)に関しては、サイバーセキュリティ事故対策をワークフローとして定義し、機械学習のデータセットとして利用するための定義と分類を行った。この成果に関しては、論文[3]にて発表した。以上の通り、今年度は本研究の基礎技術となる要素の研究に取り組み、それぞれ成果を達成した。

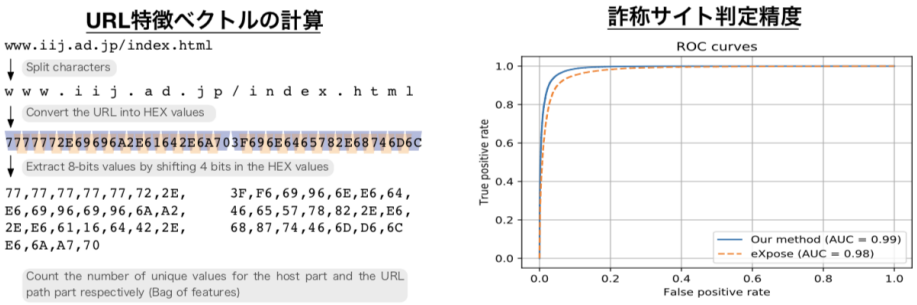

図 2 ： URL のベクトル化による詐称サイトの判定

[1] 阿部博，篠田陽一，敷田幹文，″イベントネットワークにおける syslog を用いた異常検知手法の提案と実データを用いた評価″， 情報処理学会論文誌, 59 巻 3 号, pp. 1006−1015

[2] Keiichi Shima, Daisuke Miyamoto, Hiroshi Abe, Tomohiro Ishihara, Kazuya Okada, Yuji Sekiya, Hirochika Asai and Yusuke Doi, "Classification of URL bitstreams using Bag of Bytes", in Proceedings of the 1st workshop on Network Intelligence (NI2018), Feb 2018

[3] Y. Jin, M. Tomoishi, S. Matsuura and Y. Kitaguchi: “A Secure Container-based Backup Mechanism to Survive Destructive Ransomware Attacks", Proceedings of IEEE International Conference on Computing, Networking and Communications (ICNC2018), Maui, Hawaii, USA, March 5-8, 2018