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
2017 年度採択研究代表者

2018 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. 研究成果の概要

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す。

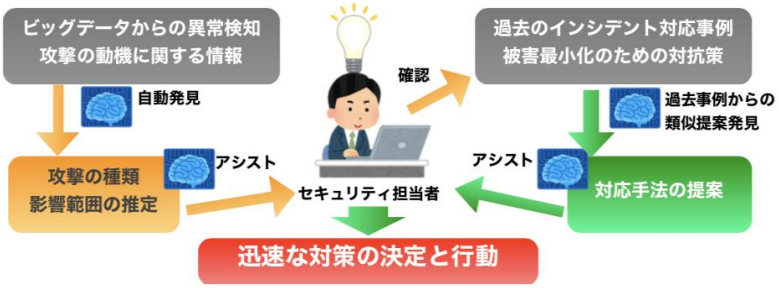

図 1： 人工知能を利用したサイバーセキュリティ対策のアシスト

本年度の主な成果として、(1) 通信データ等を画像化して深層学習を適用することで異常検知を行う「Picturization」手法の提案と実装、(2) データセットの蓄積・解析基盤 Hayabusa の分散アーキテクチャへの改良、(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。それぞれの成果は節末の論文番号に対応する。

(1)の研究成果では、通信データから攻撃の検知に適した特徴量を生成し、それを画像化することで深層学習の画像処理を適用する手法を提案し、実装した。既存研究の多くは、通信データの中にある通信元や通信先などの、人間が見て意味のある値を使って特徴量を生成していた。しかし本提案手法では、これらの値を単なる値として処理し、画像における色濃度や密度として表現することで通信挙動を画像として生成した。図 2 に、悪性ホストと良性ホストの通信挙動を画像化した例を示す。これにより、既に実用化されている深層学習を用いた画像判定の手法をサイバー脅威検知に適用することが可能となり、サイバー脅威検知のために新たな深層学習手法を開発せずとも、既に存在する多くの手法を利用することを可能とした。

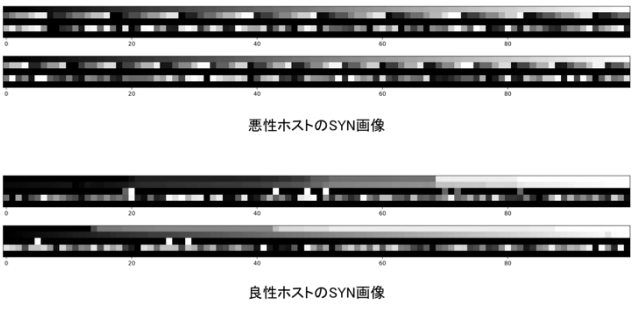

図 2： 画像化による悪性ホストと良性ホストの通信挙動

(2)の研究成果では、昨年度の研究成果である Hayabusa システムを拡張し、分散アーキテクチャを実現した。これにより、AWS に代表されるようなパブリッククラウド上へのサービス展開が可能となった。本研究成果の実用化に対する大きな進展である。

(3)の研究成果は、本研究課題の最終的な目標の一つである、インシデント対策のアシストを実現するための基礎的な成果である。様々なフォーマットによって報告されるインシデントや、既存のセキュリティ機器から送信されるアラート等を、フォーマットによりクラスタリングし、クラスタリング結果に応じてメッセージから特徴量を抽出した後に、自然言語処理にてインシデントの種別とその対応策を学習させた。

以上の通り、主に本年度は昨年度の研究成果を基としてアシストシステムを実現するための研究開発と、実サービスとして展開するためのシステム拡張に取り組んだ。これらをさらに加速させ、来年度は学内に対して試験的にサービスを実装し、実証実験を行うことを目指す。

【代表的な原著論文】

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)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

・サイバー脅威データの収集及び格納

・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

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

・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

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

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