公益財団法人トランスコスモス財団

学術・科学技術等の分野への助成事業 成果報告書

調査研究テーマ：マシンラーニング技術を用いたサイバー攻撃探索モデルの提案
研究期間：2020 年 4 月 ～ 2021 年 3 月
研究者氏名：慎　祥揆
研究者所属：東海大学情報理工学部コンピュータ応用工学科
助成金額：1000 千円

１．背景と目的

人工知能分野が人々の注目を集め始めてから，情報セキュリティ技術でも人工知能を応用する研究が行ったが，最近まであまり注目されなかった．その理由として大きく 2 つ挙げられる．

まず，敢えて人工知能が必要ではなかった．過去のプログラムは今まで通り複雑ではなく，攻撃技法もまたそれほど精を出さなかった．ファイアウォール，IDS，アンチウイルスといった防御システムさえうまく構成すれば，十分セキュリティ脅威に対応できた．

他に，不確実性を背景とする人工知能技術と確実性を求める情報セキュリティ分野の間には大きな壁が存在した．一度の誤った意思決定は，一歩間違えるだけで大きなセキュリティ事故につながりかねない．データと統計を基盤に最適な年を探していく人工知能技術に組職の重要な意思決定を任せるには大きな危険が伴う．

このような障害物と制約事項にも人工知能セキュリティが関心を受けるのは，従来使われた伝統的な手段で，これ以上の対応が難しいほど攻撃技法が進化し精巧になったことが最大の理由ではないかと思う．

本研究では，既知の攻撃パターンをベースに脅威に対応する伝統的な技術とは異なり，人工知能のマシンラーニング技術を用いた，データに隠された意味解析に焦点を当てたデータ中心手法をコア技術として使用，一度も見たことのないネットワーク上の攻撃も知能的に探知できる情報セキュリティシステムモデルの構築とこれを用いたセキュリティからディープラーニングを学べる e-Learning システム提供を目指す．

２．調査研究方法と内容

人工知能は，大きく２つの方式で最適の行動を決定する．

・データ中心(Data-driven)：観察と仮定に基づいた経験から判断
・アルゴリズム中心(Algorithm-driven)：数学と工学的な方式で判断

本研究では“データ中心”アプローチをベースとし，学習者にディープラーニングの基礎を学びながら情報セキュリティの知識を当時に取得できる学習環境の提供を目指す． 特に，学習データとそのデータから類推された結果を使った教師あり学習と，データから抽出された結果なしで，学習データだけで結果を類推する教師なし学習基盤のマシンラーニング／ディープラーニングを用いた情報セキュリティ技術モデルの両方を学べる環境開発を目指す．特に以下の２つのアプローチを対象にする．

１．教師あり学習(Supervised Learning)アプローチ

従来の攻撃と防御手法を基に，既存に知る法則と，これまでに確保したデータから探し出した共通の特性を抽出，類似しているものと異なるものを効率的に探し出すためのモデル構築を行うため，可能な限り多くの攻撃パターンを収集／分析し，独自の関数を提案，検知確率を上げられる新たなアルゴリズムについて検討する．

２．教師なし学習（Unsupervised Learning)アプローチ

攻撃プログラムの主用部分を探索，追跡，検証する一連のフレームワークの構築方法を検討する．このような方法を用いることで，適用範囲と考慮すべき部分は多くなるが，全体的なプロレムワークをシステムに委任するシステムが構築できるため，未発見の脆弱点と新たな攻撃パターンが探知可能になると期待できる．

３．研究概要と成果

本研究では、ネットワーク攻撃モデルを構築し，学習者がネットワーク上で行われる攻撃パケットを探知し，教師なし学習アプローチ基盤で，ネットワーク異常徴候探知モデルを構築できる学習モデルを構築した．

ネットワーク侵入検知モデル構築において最も重要な部分はデータ収集である．本研究は仮想環境上で行われるため，仮想環境上のネットワーク上のトラフィック（ログ）を収集し手がかりを見つけるようにした．この学習を実行することにより，学習者はセキュリティログの特性を理解し，非知道基盤の異常探知手法を実際の探知システムに適用する方法を

理解するようにした.

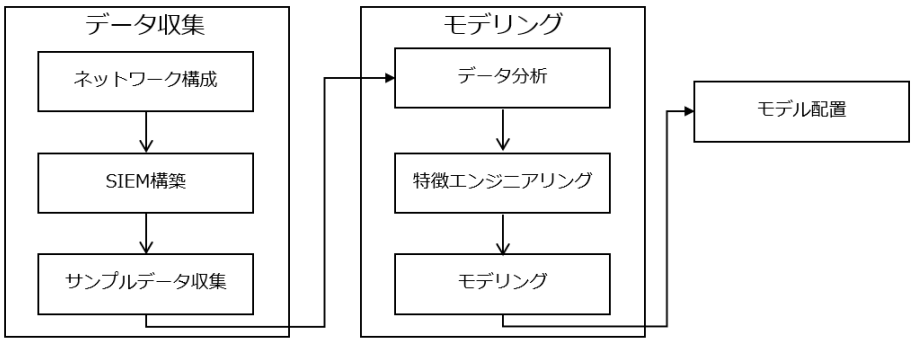

図１．学習の流れ

ネットワーク構成：データ収集や探知モデル配置のためのネットワーク構成は，Ubuntu を設置してゲートウェイと外部に Web サービスを適用するウェブサーバの役割を果たすように構成した．ウィンドウ側の仮想マシンが攻撃を受ける役割の組織内の内部ネットワークの役割を果たす.

SIEM 構築：外部インターネットと内部網を連結する関門の役割をする Ubuntu 仮想マシンに SIEM を構築することになる.

サンプルデータ：学習は，同題の仮想環境内でネットワークトラフィックを発生させ，このデータを収集するようにした.

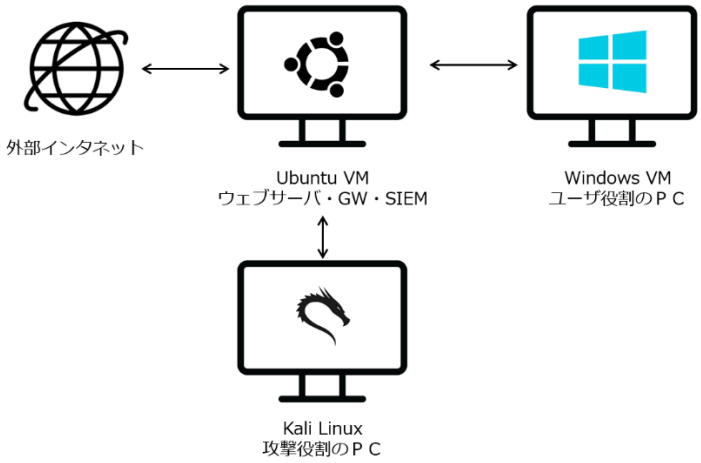

図２．仮想マシンを用いた学習環境構築

ネットワーク基盤の異常徴候探知モデルを構成するためには，悪性コード探知モデルに比べて構成しなければならない要素が多い．まだ初期構成であるため，学習に必要なデー

タ分析方法や特徴共有，学習者が理解しやすいモデリング方法についてのカリキュラム構成が必要な段階である．今後，体系的なデータ収集方法，学習シナリオによるカリキュラム，データマイニング基盤の特徴エンジニアリングを理解とそれによるデータ抽出方法，抽出したデータの視覚化に対する学習環境とのカリキュラム提供を目指し研究を進める計画である．

また，これらの成果については１ 件の発表済および 国際会議に 2 件の発表予定である．論文にはトランスコスモス財団からの助成金を受け入れて行った研究であることを明記している．

４．謝辞

本研究を実施するために，助成金を用いて購入した様々な機材は研究の環境構築には不可欠であった．本研究を支援して頂いた公益財団法人トランスコスモス財団に謝意を表する．