SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

疑似攻撃ログによるAIを用いた攻撃検知技術の強化
Enhancement of Attack Detection Technology using AI with Synthetic-Log Generation

山本 匠 †
Takumi Yamamoto

中井 綱人 †
Tsunato Nakai

大塚 瑠莉 †
Ruri Otsuka

Ye Wang ‡

Kyeong Jin Kim ‡

Toshiaki Koike-Akino ‡

Iván Sanz Gorrachategui *

Aolin Ding **

阿部衛 ***
Mamoru Abe

吉村 礼子 †
Ayako Yoshimura

河内 清人 †
Kiyoto Kawauchi

キーワード 機械学習，オートエンコーダ，検知回避，敵対的サンプル，疑似ログ，サイバー攻撃

あらまし

近年，特定の企業や組織を狙った標的型攻撃が増加している．一方，セキュリティ監視の現場においては，専門的な知識を必要とするスタッフ不足が問題となっている．そのため，少ないスタッフでもサイバー攻撃を高精度かつ効率よく検知することができる技術が必要である．

サイバー攻撃を監視する技術としては，既知の不正なパターンを検出する方法や，攻撃手口や攻撃者のふるまいを検知する方法など，ルールベースの攻撃検知技術がよく知られている．本技術では，あらかじめ監視対象の情報ごと適切な検知ルールを定義する必要があり専門的な能力が求められる．昨今のセキュリティ人材不足や攻撃増加の背景から，ルールベースの検知技術の限界が近づいていると言える．

そのため，あらかじめルールを定義する必要のない，もしくは，正常と異常とを識別する境界が自動的に決められる高度な検知技術が望まれる．また昨今，ルールベース検知では見つからないよう巧妙に作りこまれた高度な攻撃も増えてきており，ルールベースでは対応できないような巧妙な攻撃も検知可能な検知技術が望まれる．

これを実現する技術として機械学習などの Artificial Intelligence（以降 AI と略す）が注目されている．AI はあらかじめ用意された複数のクラスのデータを学習し，クラス間を切り分ける境界を自動的に見つけ出す．クラスごとのデータを大量に用意することができれば，AI は適切に境界を見つけることができる．AI をサイバー攻撃の監視に応用することができれば，これまで専門的な知識やスキルを持つスタッフが行ってきたルールの定義や更新を AI が代替してくれると期待される．

しかし，ネットワークセキュリティにおいては，AI を学習する上で重要となるクラスごとのデータを大量に用意することが困難であるという課題がある．特に攻撃に関してはその発生が稀であり，攻撃データを学習用に大量に用意することは非常に難しい．そのため，攻撃データが少ない環境においても，効果的に攻撃を異常として検知することができる AI 技術が必要である．

そこで本研究では，正常なデータは大量に手に入るが，大量の攻撃データを入手することは困難な環境を想定し，攻撃データの近傍にあるデータを疑似的に生成し学習データに含めることで，教師有学習による攻撃検知システムの強化を図る．攻撃データの近傍にある正常データの特徴の傾向を使い，敵対的サンプル生成の要領で，疑似攻撃ログを効率よく生成する．

また本研究では，公開されている攻撃データセットを利用し，教師有学習による攻撃検知精度において，疑似攻撃ログの有無に関して比較検証を行い，提案方式の優位性を示した．さらに，疑似攻撃ログの生成効率に関して，攻撃データの近傍にある正常データの傾向を利用した敵対的サンプル生成アプローチ，単純な敵対的サンプル生成アプローチ，ランダムに特徴を変更するアプローチの 3 つを比較し，提案方式の優位性を示した．

† 三菱電機株式会社 情報技術総合研究所, 〒247-8501 神奈川県鎌倉市大船 5-1-1
‡ Mitsubishi Electric Research Laboratories, 201 Broadway, 8th Floor Cambridge, MA 02139-1955
* University of Zaragoza, c/ Pedro Cerbuna, 12 50009 Zaragoza
** Rutgers University, Rutgers, The State University of New Jersey 57 US Highway 1 New Brunswick, NJ 08901-8554
*** 東邦大学 〒274-8510 千葉県船橋市三山 2-2-1