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

部分観測マルコフ決定過程によるニューラルエージェント強化学習を使用した自律型 SQL インジェクション攻撃手法

The autonomous SQL injection exploitation using neural agent reinforcement learning by partial observation Markov decision process

佐竹 達也 *　　大塚 玲 *
Tatsuya Satake　　Akira Otsuka

キーワード 深層強化学習, 部分観測マルコフ決定過程, ニューラルエージェント, SQL インジェクション

あらまし

本研究では, 部分観測マルコフ決定過程に基づく強化学習モデルについて, GRU による状態推定と Attention を使用したニューラルエージェントにより, 状態空間と行動空間を分散表現で近似して最適な方策を学習する強化学習モデルを構築した. このモデルを実践的な CTF の SQL インジェクション問題に適用した結果を報告する.

これまでの研究で, すでに, 自然言語文字列からなる観測情報をニューラル自然言語処理により分散表現に変換し, その系列をリカレントネットワークの一種である GRU で認識して推定状態する. さらに, 環境から与えられる行動集合も分散表現の系列として表現し, 推定状態と組み合わせて Attention で最適な行動を選択する強化学習モデル (Le Deep Chef[1]) が提案されている. 本研究では,Le Deep Chef をセキュリティの分野におけるサイバー推論システムへの適用可能性を探る.

既に,SQL インジェクションを題材として一般的な CTF 問題を解く深層強化学習モデルとしては,Erdodi ら [2] において,DQN を適用して有効性が確認されている. しかし,Erdodi らの研究は,1) 完全観測マルコフ決定過程に基づいていること, 並びに 2) 固定された 51 個の行動空間から環境から与えられた状態に応じて最適な行動を選択するという単純なモデルに基づいている. このため, 自由度が極めて低く実用にはほど遠いと考えられる. 我々は, 様々な実践的な Web アプリ環境を用意しニューラルエージェントの学習汎用性を高めた.

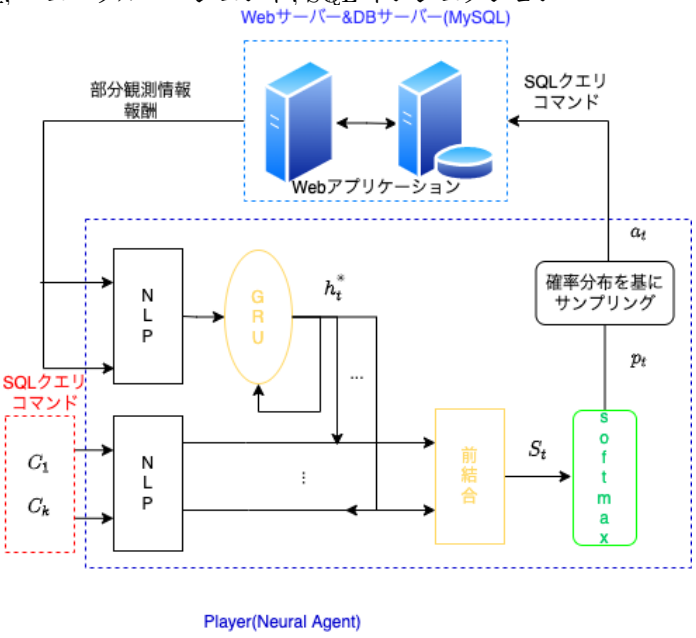

図 1: 提案手法

参考文献

[1] Adolphs, Leonard and Thomas Hofmann (Apr. 2020). “LeDeepChef Deep Reinforcement Learning Agent for Families of Text-Based Games”. In: Proceedings of the AAAI Conference on Artificial Intelligence 34.5.

[2] Erdodi, Laszlo, Avald Aslaugson Sommervoll, and Fabio Massimo Zennaro (May 22, 2021). “Simulating SQL Injection Vulnerability Exploitation Using Q-Learning Reinforcement Learning Agents”.

* 情報セキュリティ大学院大学, 〒 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1, Institute of Information Security, 2-14-1, Tsuruya-cho, Yokohama City, Kanagawa Pref., 221-0835, Japan.