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

Attack graphを用いたサイバーレンジシナリオの自動生成
Automatic generating of cyber range scenarios using attack graph

中田　亮太郎 *　　大塚　玲 †
Ryotaro Nakata　　Akira Otsuka

キーワード サイバーレンジ，Attack graph，DAG，Docker，コンテナ，サイバー推論システム

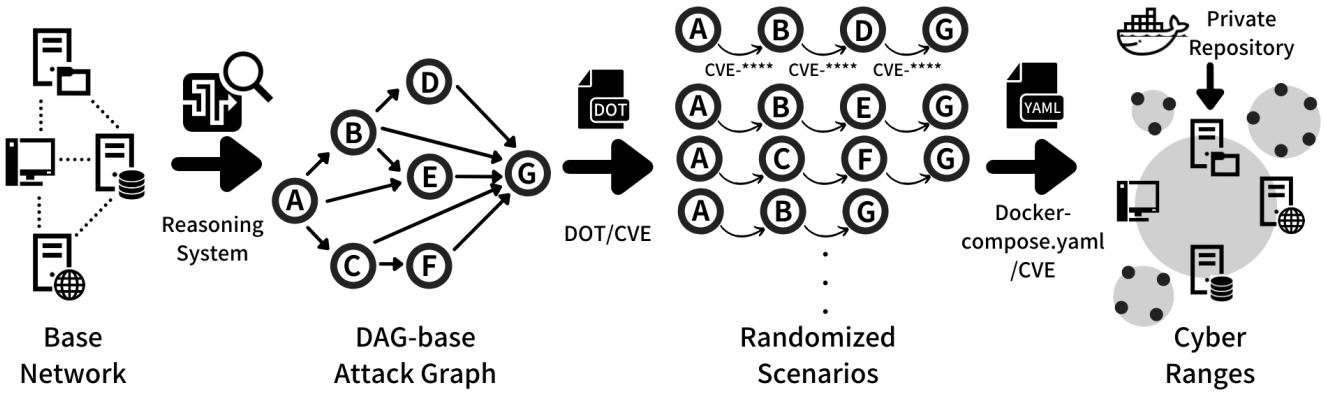
あらまし

情報セキュリティ人材育成に使われる演習システムであるサイバーレンジは，リアリティの高い演習による高い教育効果が期待できるが，コスト面やシナリオ生成，運用面などで課題があり，普及が進んでいない．商用のサイバーレンジは多くの企業で開発されているが，高度な専門家の育成やセキュリティを専業とする企業による専門教育での利用が中心である．

不足するセキュリティ人材の育成には，高等教育機関でも広く普及が可能なサイバーレンジを実現させる必要があるが，シナリオの開発や環境の構築，演習の実施・管理や学習・成績管理など，多くの面で教員の負担が大きく，企業や専門組織などの協力が得られる場合を除き，導入が困難である．

我々はこれまでの研究で，Docker によるコンテナを用いることで，少ないリソースで高性能なサイバーレンジ環境を構築する手法の有効性を確認し，多くのシナリオを円滑に実行できる新たなサイバーレンジプラットフォームとして提案した [1]．しかし，演習シナリオの開発は手動で行われており，演習効果を高めるために必要な多くのシナリオを準備するには膨大な作業を伴う．

そこで本稿では，システムの脆弱性やネットワーク上の到達性を分析して可視化する Attack Graph の技術を用いてサイバーレンジシナリオを生成し，そのシナリオを用いて演習を実行できる環境の構築までを自動化する手法を提案する．コンテナを用いたサイバーレンジプラットフォーム CyExec 上に実装することで．多くの脆弱性をランダムに選択したシナリオが実行できる環境が実現でき，高等教育機関でも普及が可能な現実的な演習プラットフォームとして利用できる．



参考文献

[1] Ryotaro Nakata and Akira Otsuka,“CyExec*: A High-Performance Container-Based Cyber Range With Scenario Randomization,” IEEE Access 2021 Vol.9 pp.109095-109114

* 一橋大学, 東京都国立市中 2-1, Hitotsubashi University, 2-1 Naka, Kunitachi, Tokyo, Japan, nakata.ryotaro@r.hit-u.ac.jp
† 情報セキュリティ大学院大学, 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, Kanagawa-ku, Yokohama, Kanagawa, Japan, otsuka@iisec.ac.jp