CL-004

自律サイバー推論システムを利用したサイバーレンジシナリオの生成手法の検討
Generating cyber range scenarios using an autonomous cyber reasoning system.

中田　亮太郎†‡　　米田 智紀‡　　大塚 玲‡
Ryotaro Nakata　　Tomonori Yoneda　　Akira Otsuka

1. はじめに

サイバー攻撃の高度化・巧妙化に伴い，セキュリティ人材の不足が顕在化し，セキュリティ教育の重要度が増している．専門業者による高度な人材育成や高等教育機関の教育では，サイバーレンジを用いた演習によるセキュリティ教育が注目されている．サイバーレンジは，実際のセキュリティインシデントを仮想環境上で再現する演習システムとして利用され，実践的で教育効果の高い演習が実施できるが，人的・経済的コストの高さなどの課題があり，普及は限定的である [1].

サイバーレンジによる演習を実施するには，高度な知識や技術を持つ専門家がシナリオの開発や環境構築を行う必要がある．より効果的な演習を行うには，増え続ける脆弱性や進化し続ける攻撃手法に対応した多くのシナリオが必要になるが，開発にかかる負担が大きく，シナリオの使い回し等による教育効果の低下を招いている [2].

シナリオの不足を補うため，演習プラットフォームを公開・共有する取り組みや，シナリオ開発・環境構築の自動化に関する研究が行われている．しかし，既存の研究は既知のいくつかの脆弱性や攻撃手法を扱うための限定的な環境であり，常に最新のインシデントに対応したより多くの実践的シナリオの開発が必要とされている[3].

そこで本稿では，機械学習等のAI技術によりサイバー攻撃の検知や対処を自動化することを目標とした「自律サイバー推論システム」の研究を，サイバーレンジのシナリオ開発に利用することを検討する．既知の攻撃手法や脆弱性に対応した多くのシナリオ開発の自動化や，最新のインシデントへのいち早い対応により，サイバーレンジ最大の懸念であるシナリオの不足を解消し，教育効果を維持向上してセキュリティ人材の不足への対応や技術レベル向上が期待できる．

2. サイバーレンジ

2.1 環境構築と仮想化

サイバーレンジの運用には，演習で扱う攻撃や防御の流れを表すシナリオと，それらを再現するための環境構築が必要である．環境構築はサーバやネットワーク機器，利用者端末およびセキュリティ機器など，通常の情報システム・ネットワーク環境の構築と同等の状況を再現するだけでなく，演習目的となる攻撃や脆弱性を再現するために，特定の設定やソフトウェアバージョンの変更など，組織や企業の一般的なシステム・ネットワーク環境の構築とは異なる知識や技術が求められる．

また、演習の実施に際しては，多くの受講者用の環境準備や迅速な入れ替えなどが必要であるため，実機を用いた演習は現実的ではなく，仮想化技術により演習環境が構築される．商用のサイバーレンジでは，管理機能や対応 OS の多さなどから，VMWare などハイパーバイザ型の仮想化製品を利用したサイバーレンジ製品が普及しているが，導入や維持管理に数億円規模の経済的負担が必要となるため，VirtualBox や Docker など安価で容易に利用できるホスト型およびコンテナ型の仮想化を利用したサイバーレンジの研究や，それらを用いた演習環境の公開が行われている[3].

我々はこれまでの研究で，各仮想化方式の違いによる脆弱性の再現性能の違いはなく，同等の脆弱性の再現性能を有することを確認した．また，その中でもコンテナ型仮想化は，消費リソースを大幅に抑制しつつ高速で軽量な演習環境が実行でき，近年の docker の普及と利便性の向上も伴って，コンテナ型仮想化を用いたサイバーレンジの研究が増加している．

2.2 シナリオ

サイバーレンジのシナリオは，特定の攻撃手法や脆弱性を体験することで理解するものや，インシデント全体での攻撃や対処法の流れを体験しながら総合的に知識や技術学ぶものなど，様々な目的やレベルのシナリオが存在する．ただし，開発には情報セキュリティ全般の知識や技術が必要である他，最新の攻撃手法や脆弱性への対応の困難さなどの課題があり，シナリオの不足や漏洩による教育効果の低下を招いている[2].

我々はこれまでの研究で，シナリオのランダム化や Attack Graph を用いたシナリオ生成手法などの提案を行ってきた[1,4].

図 1 に，サイバーレンジのシナリオ自動生成の流れを示す.

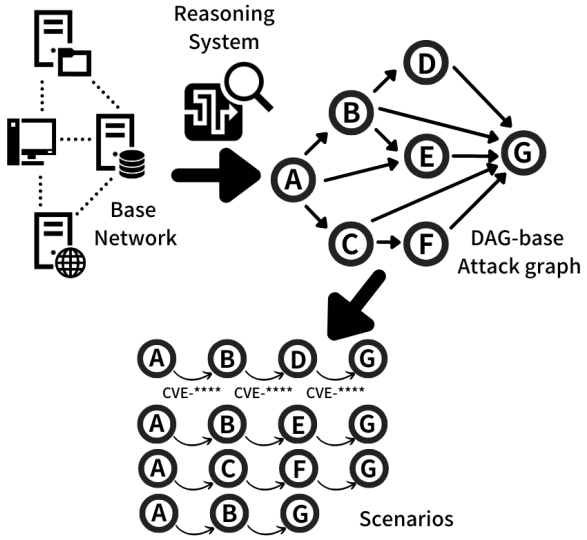

図 1　サイバーレンジシナリオ自動生成の流れ

†一橋大学　Hitotsubashi University
‡情報セキュリティ大学院大学　Institute of Information Security

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

シナリオの元となるネットワーク環境に対して，推論システムによって存在する脆弱性を洗い出し，それらに有効な攻撃手法やネットワークの到達性などを考慮することで DAG（有向非循環グラフ）形式の Attack Graph を生成し，その経路を辿る形でシナリオ化する．

ただしこの手法は特定のネットワーク環境をターゲットとした限定的な手法であり，新たな攻撃手法や脆弱性への対応の他，既知の攻撃手法や脆弱性への対応をさまざまな環境を想定して汎用的に行うには十分ではない．また，推論システムには Nmap や OpenVAS など，一般的にも使われるツールが用いられるが，対応する攻撃手法の抽出や検討はツール単体では困難で，それぞれの脆弱性に対して Metasploit の Exploit モジュールや，公開されている攻撃用コード等を組み合わせて確認するなど一部で手動での対応を要したり，新たな脆弱性へツール側が対応するのを待つ必要があるなど，汎用化するには課題がある．

したがって，シナリオ生成を効率よく様々なシステム・ネットワーク環境を対象として行うには，脆弱性やそれに対応する攻撃手法を効率よく推論できる高度なサイバー推論システムが求められる．

3. 自律サイバー推論システムの利用

3.1 サイバー推論と人工知能技術

サイバー推論をはじめ，様々なセキュリティ技術によって高度化・巧妙化するサイバー攻撃への対応が検討されているが，従来の手法では対応しきれないサイバー攻撃が増加している．そこで近年注目されているのが人工知能（AI）技術を用いたセキュリティである．

AI を用いたセキュリティ技術の概要について図 2 に示す．

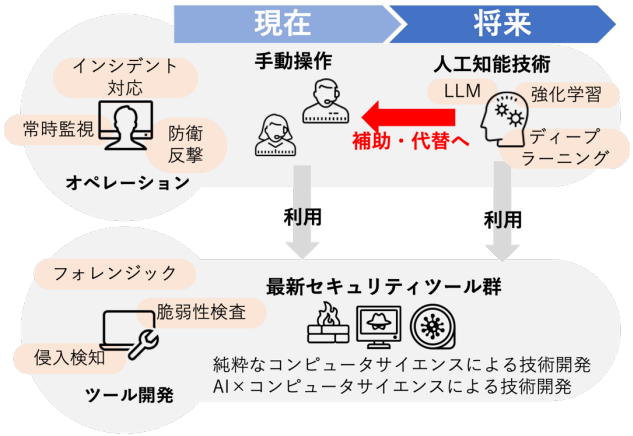

図 2　AI を用いたセキュリティ技術の概要

現在のセキュリティに関するオペレーションは，さまざまな情報を元に有効な対応策を検討し，手動による操作によって実施される．各種ツールによる操作の自動化や監視作業の簡素化は既に行われているが，インシデント発生の際の対応策の検討や攻撃手法の分析のほか，未知の攻撃手法への対応など定型的ではない対応が求められ，それらの負担を補助・代替できるような AI 技術の研究が進んでおり，自律サイバー推論システムの研究ではこれまで人間が手動で行なっていた検知や各種対応などのオペレーションを全自動で実施できることを目標としている．

なお，これまでの AI 技術を用いたセキュリティ対応手法は，過去に発生した正当な通信又は悪意のある通信を学習させ，実際の通信と比較し分類を行うものが主流であった．

しかし，過去の通信から学習させた場合，珍しい正当な通信を悪意のある通信と誤分類したり，未知の攻撃に対応できないといった問題が発生し得る．また，画像分類の分野で特に研究が盛んな，AI を騙すような敵対的攻撃をサイバー空間に適用する研究も行われるなど，過去の通信からの学習のみでは対応できない攻撃が懸念される．

そこで，従来の機械学習と異なり，訓練データを与えずとも与えられた環境で試行錯誤を行い，報酬を最大化することで最適な行動を導き出す強化学習と呼ばれる手法による自律サイバー推論システムの研究が行われている[5]．

強化学習の概要を図 3 に示す．

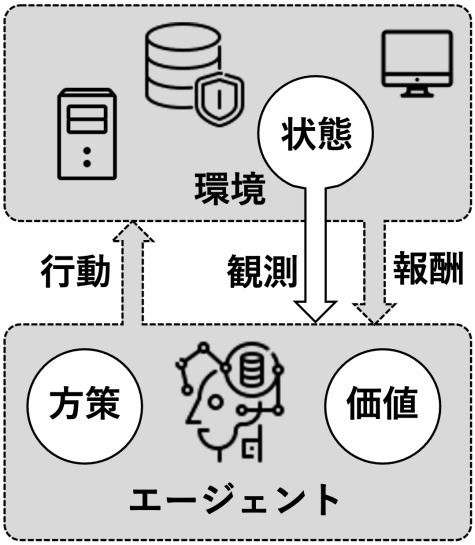

図 3　強化学習の概要

強化学習は，エージェント (行動主体) がある環境の状態に応じて，どのように行動すれば報酬が多くもらえるかを求める手法である．教師なし学習や教師あり学習とは違い，学習データなしに自身の試行錯誤のみで学習するのが特徴である．強化学習の学習サイクルは下記の通りである．

1. エージェントは最初に何を判断すべきか分からないので，初期値としてランダムな方策をもとに行動を選択する．
2. 行動に伴う報酬に応じて，エージェントが行動を決定する方策を求める
3. ランダムな動きは残しつつ，方策を手掛かりに価値の高い行動を決定する．
4. 2-3 を繰り返し，将来的に多くの報酬を得られる最適な方策を求める．

自律サイバー推論システムは，セキュリティインシデントにおける行動の決定に強化学習を用いたもので，既存の攻撃行動や脆弱性に対する対応だけでなく，未知の攻撃に対しても迅速かつ的確に対応することを目標に研究されたシステムである．ソフトウェアの脆弱性検知，エクスプロイト作成，パッチ作成等の各種行動を自動的に行うもので，

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

コンピュータ同士が全自動で戦うハッキングコンテストである「サイバーグランドチャレンジ」で用いられるなどして脚光を浴びた．サイバー推論システムに関連する研究は，ファジング，シンボリック実行，異常検知，バイナリパッチ，行動戦略等多岐にわたり，コンテストでも用いられたように完全に自律したサイバー推論システムによって，サイバーインシデントに関する行動を自動化することを目標とした研究が行われている[5,6].

3.2 強化学習によるペネトレーションテスト手法

自律サイバー推論システムの研究の一つに，強化学習を用いたペネトレーションテスト手法がある[7].

ペネトレーションテストはサイバー攻撃に対抗する手法の 1 つであり，実際に対象環境に対して侵入テストを行うことによりセキュリティリスクを顕在化させ，インシデントに備える手法である．従来のペネトレーションテストは，脆弱性検査ツール等のサイバー推論システムを手動で利用した結果から攻撃方法を検討するなど多くの手間や時間がかけられてきたが，自律サイバー推論システム化の研究が進んでおり，Autopentest-DRL や DeepExploit などの手法が提案されている[8,9].

DeepExploit では，攻撃に使われるコードに対し，本来手動でのチューニング作業が必要な OS 情報や CMS，利用フレームワークなどの様々な環境情報を強化学習により学習させることで，自動的に有効な攻撃コードを実行する推論システムとして利用できる．実際のペネトレーションテストで使われるツールである Metasploit や Nmap などを用いて得られる情報を基に攻撃手法を学習していくが，学習段階においては一部しか最適化されておらず，テスト段階ではポートスキャンから獲得されたポートに総当たりで攻撃していくという手法をとっているため，多くのターゲットに対して推論を行うには非効率であるほか，使われているツールのバージョンが古く，最新の環境や脆弱性・攻撃手法への対応が困難であるなどの課題がある．

そこで我々の研究では，各種ツールによって攻撃を細分化した DeepExploit の手法と，部分観測マルコフ決定過程（POMDP）ベースの深層強化学習手法であるニューラルエージェントを組み合わせた手法により，攻撃手法の推論に対する最適化が可能な RedChef を開発した[7].

図 4 に RedChef の概要を示す.

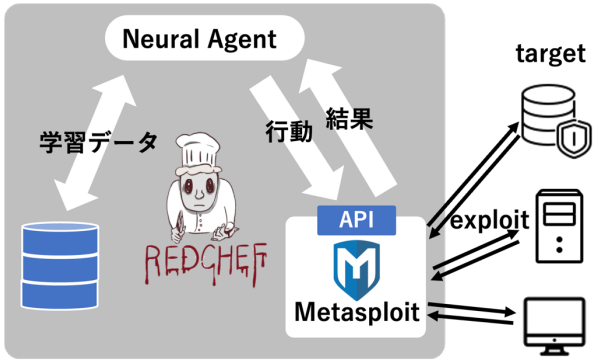

図 4　RedChef の概要

RedChef は DeepExploit の手法を参考に，metasploit の RPC API を通じてターゲットへ試行する状態推定や行動選択の精度向上を目指したものである．環境に Metasploit の実システムを用い，実行コマンドに Metasploit で使用するコマンドを用いる．DeepExploit の場合，Metasploit の payload の選択のみを行なっているが，RedChef では RPORT/exploit module/exploit target/payload の 4 種類の行動を最適化する．

図 5 に DeepExploit との比較実験の結果を示す.

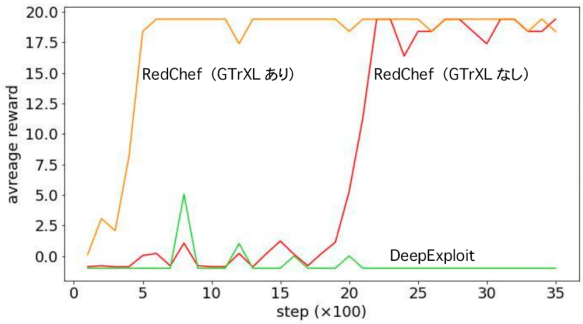

図 5　Redchef と DeepExploit の比較実験結果

RedChef は，ニューラルエージェントの状態推定の精度向上のため，GTrXL(Gated Transformer-XL)と呼ばれる手法を取り入れており，学習段階における実験では約 500 ステップ目で最適な平均報酬となるなど高い精度の学習が可能であることを示した．Redchef は効率的にターゲットの状態を推定し，攻撃可能な Metasploit の exploit モジュールを推定することが可能であり，サイバーレンジシナリオの生成においても有効なサイバー推論システムとしての利用が期待できる.

3.3 サイバーレンジシナリオ生成への利用

従来のサイバーレンジシナリオの開発では，特定の攻撃手法や脆弱性を学習目的とし，それらを再現できる環境の構築や有効な攻撃コードの検討など，実際のインシデントを想定した開発が行われてきた．ペネトレーションテストにおいても，実際の環境に対して攻撃可能性を検討し，様々な攻撃シナリオを検討してテストが実施されるため，サイバーレンジのシナリオ開発と同等の内容が検討されていると言える.

したがって，図 1 に示したサイバーレンジシナリオ生成の流れにおける推論システムにおいて，強化学習によるペネトレーションテスト手法を利用することで，自動的かつ効率的にシナリオ開発を行うことが期待できる．ただし，そのためには学習や推論のベースとなる多くのターゲットを用意しなければならない.

そこで，Docker のコンテナイメージをインターネット常に公開しているリポジトリである Docker HUB に注目した．Docker HUB は，公式の OS イメージだけでなく，独自に作られた Web サーバ，DB サーバなどあらゆるコンテナイメージが公開されており，利用者はイメージをダウンロードしてコンテナとして起動し，即座に様々なシステム環境を再現して利用が可能である．tag と呼ばれるバージョン管理機能もあり，古いバージョンの OS や各種ソフトウェアを用いたイメージも公開されていることが多く，脆弱性が存在するバージョンや設定の不備が含まれたコンテナイメージも多く存在する.

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

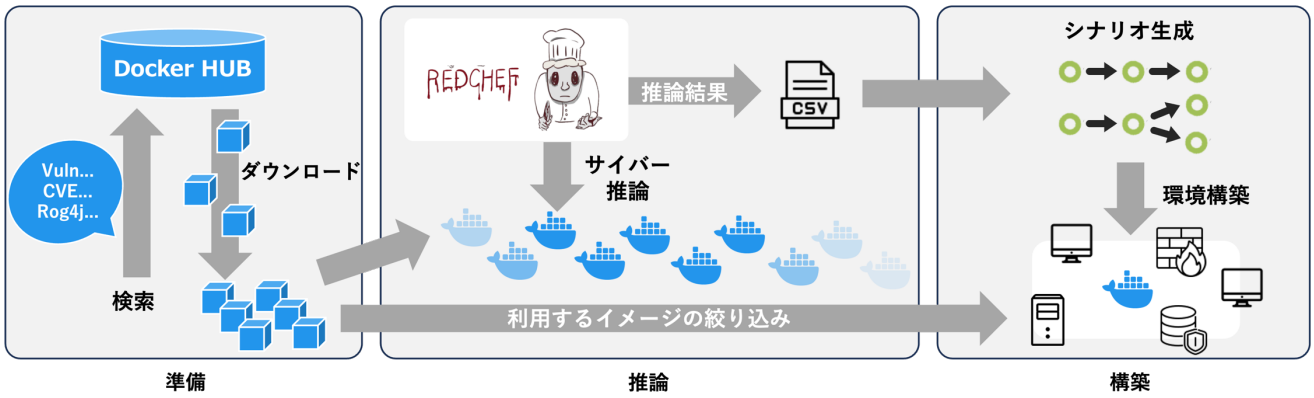

図 6　自律サイバー推論システムと Docker HUB によるシナリオ生成システムの概要

RedChef を用いたサイバー推論により，Docker HUB に公開されているコンテナイメージから攻撃可能な脆弱性を持つターゲットやそれに対応する攻撃手法が取得できれば，効率的なサイバーレンジのシナリオ生成に利用できるだけでなく，環境構築にも同じコンテナイメージをそのまま利用できる．また，Docker HUB には最新の脆弱性の検証用環境（PoC）として再現されたイメージが提供されていることもあり，これらのイメージに対して自律サイバー推論システムが機能すれば，最新の脆弱性にいち早く対応したシナリオの生成も期待できる．

4. 実装

図 6 に，redchef を自律サイバー推論システムとしてシナリオ生成に利用し，Docker HUB のコンテナイメージをターゲットとしたシナリオ生成システムの概要を示す．

Docker HUB の膨大なコンテナイメージをターゲットとしてサイバー推論を行い，各イメージに存在する脆弱性および対応する攻撃行動からシナリオを生成 し，対象となるコンテナを環境構築にもそのまま使用することで，シナリオ生成から環境構築までを自動化するシステムである．

このシステムは準備・推論・構築の 3 つのフェーズに分かれており，準備フェーズでは Docker HUB 上のコンテナイメージをダウンロードするための検索ワードとダウンロードするイメージ数を指定する．たとえば具体的な CVE 番号や，"wordpress"など特定のアプリケーション環境などを指定することで，関連するイメージや PoC（検証環境）として作られたイメージのほか，特定のアプリ環境が構築されたものなどがさまざまなイメージが検索されダウンロードすることができるほか，tag により管理されたバージョン違いのイメージも利用できる．

推論フェーズでは，ダウンロードしたコンテナを順次起動させて RedChef によるサイバー推論を実施する．学習はその回数や何番目のコンテナまでを対象とするか，過去の学習データを利用するかなどを設定して変更し，さまざまな推論パターンを取ることができる．

尚，Doker HUB のイメージは Docker run コマンドでコンテナとして起動しているが，その際に存在するサービスを起動するスクリプトを実行し，実機や仮想マシンでの起動と可能な限り同等の状態で起動するようにした．これは，docker コンテナの場合は通常の OS 起動プロセスを経ずに動作するため，Web サーバや DB が存在してもサービスの起動は別途指示が必要な場合もあるためで，検索されたイメージがその目的通りに正しく動作するために必要である．

最後に構築フェーズでは，推論によって得られた結果から DAG 形式の Attack Graph を生成する．推論から得られる内容は，主にどのイメージに対してどの攻撃手法（Metasploit の exploit モジュール）が有効かという内容であり，攻撃の流れを表すシナリオとしてそのまま利用することが可能である．グラフの経路が演習用のシナリオとして使用され，演習環境の構築についても推論の対象となったコンテナそのまま利用することで，自律サイバー推論システムを利用したシナリオ生成から環境構築までを自動化する．

5. 検証

実装したシステムの動作を検証するため，いくつかの検索ワードを用いた動作実験を行った．

実験の結果を表 1 に示す．

表 1　検索ワード毎の推論結果とシナリオ生成への利用

	検索イメージ数			シナリオ
検索ワード	10	20	30	生成
ubuntu(official)	-	-	-	×
wordpress(official)	1	2	2	×
mysql(official)	-	1	1	×
metasploitable2	5	12	19	◎
metasploitable3	2	4	7	○
cve-2016	3	4	4	○
cve-2023	1	1	1	△

それぞれの検察ワードに対して 10,20,30 の 3 つのパターンでコンテナイメージの検索数を設定し，tag が存在するものは検索して出た順に利用した．各コンテナに対して学習を行った後に有効な攻撃行動をテストするようにした結果，確認できた脆弱性と攻撃モジュールの組み合わせの数を示している．また，それらの結果を用いてシナリオ生成行い，実際に演習として利用できる内容となったかを確認した．

最も効率的に推論が成功したのは，脆弱なサーバとして検証や演習でもよく使われる"metasploitable2"を検索ワードとした場合で，Docker HUB に存在するイメージの数も一定数あるだけでなく，一つのイメージに存在する脆弱性の

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

数が非常に多く，効果的に学習および推論を進めることができ，多くの攻撃パターンを確認することできた．さらにこの結果を用いてシナリオ生成から環境構築までを実行し，さまざまな攻撃や脆弱性を再現した演習環境として利用できることが確認できた．

同じく脆弱なサーバとして知られる"metasploitable3"を検索ワードとした場合は，Docker HUB に存在するイメージ数が 4 つと少なく，学習できるデータや推論できる脆弱性が少なかったためかあまり多くの結果は得られなかったものの，シナリオとしての利用は可能であった．

また，"ubnutu"を検索した場合，多くの tag が存在するため検索対象となるイメージは非常に多いが，最新のイメージやそれに近いものからは脆弱性がほぼ発見できず，学習もうまくいかなかった．同じく公式イメージとして公開されている wordpress や mysql なども、検索対象となる tag が非常に多く存在するが，最新のイメージでは脆弱性対策が十分にされている場合もあり，あまり効率的な推定ができなかったため，これらの公式イメージを検索する場合は古い tag 情報から遡って利用するなどの工夫が必要である．

PoC 環境などをターゲットとするために cve 番号を年まで指定した場合，2023 で検索したイメージは現状では数が少なく対象となった脆弱性も少なかったため，推論できた数が少なくなってしまったが，2016 の場合は一定数のイメージが存在し，シナリオとして利用可能な結果を得ることができた．

6. 考察

強化学習によるペネトレーションテスト手法をサイバーレンジのシナリオ生成における推論システムとして利用し，シナリオ生成の実験を行った結果，学習および推論のターゲットとするコンテナイメージの数やそこに存在する脆弱性の数によって大きく結果が異なったが，Docker HUB に存在するイメージが多く，かつそれぞれのイメージに多くの脆弱性が存在する場合は推論が効率的に機能し，多くのシナリオを生成することができた．

一方で，検索対象となるイメージが少なかったり，公式イメージのように多くの tag が存在した場合でも，脆弱性が存在しなかったり少ない場合には学習や推論がうまく機能せず，いくつかのシナリオを生成することはできても，非効率で実用性の乏しい結果となる．

これらの結果は，各イメージで学習を行う回数の設定やさらに多くの検索対象数をターゲットとした場合など，さらに効率的に推論を実施できるような調整の検討・検証の余地はあるが，自律サイバー推論システムを用いることで，手動でのシナリオ開発と比較して効率的なシナリオ開発ができる可能性を示している．

今回の実験で確認したシステムを利用したシナリオ開発を，手動による一般的なシナリオ開発の状況と比較したものを表 2 に示す．

一般的なシナリオ開発の場合，演習の学習目的や内容を知識や技術を持つものが既知の攻撃手法や脆弱性の情報を元に検討したり，インシデントを再現した環境の構築や検証作業などを手動で実施する必要があるが，自律サイバー推論システムを利用した今回のシステムは，開発の環境として GPU 等を用いた機械学習に適した計算機環境を利用する必要があるが，これまで教員や専門の技術者が手動で行っていた作業を自動化し，かつこれまでに無かったほど多くのパターンのシナリオを生成できる新たなシナリオ開発手法として利用することができる．

表 2 システム利用時と手動開発の比較

	システム利用	手動開発
学習目的や内容の検討	脆弱性情報や対象とする環境から検索ワードを検討	既存のシナリオからの選択や脆弱性情報などから再現可能性を考慮して検討
シナリオの開発	推論結果を利用した自動生成	攻撃や防御の流れを都度検討して開発
開発環境	効率的な開発に機械学習用のハードウェアが必要	仮想マシンやコンテナが動作する一般的な環境
環境構築	コンテナによる自動構築	攻撃手法の確認や脆弱性再現を含めた構築や検証

7. 課題と今後の展望

今回の実験ではシナリオの生成手法として一定の成果を得たが，対応すべき課題も明らかとなった．今後検討すべきと考えられる内容を以下に示す．

- Docker HUB 上で検索されるイメージ数が一定数以上の検索ワードを対象とする：metasploitable3 や cve-2023 など，検索結果として取得できるイメージ数が極端に少ない場合は効果的な学習が行えない可能性が高い．一定数以上の検索結果が得られる場合のみを対象としたり，複合的に検索できるようにするなどして，十分な学習データを得て推論が実行できるようにする必要がある．
- 対象のイメージは一定以上の脆弱性が存在するものとする：脆弱性がそもそも存在しないイメージや，ごく僅かしか存在しない場合なども効果的な学習が行えないため，事前に一定数以上の脆弱性の有無を判断するなどしてターゲットを限定する必要がある．
- 公式イメージを検索対象としない，もしくはバージョンの古い tag から対象とする：ubuntu や wordpress，mysql などの検索では docker の公式イメージとして公開されており，新しいバージョンのイメージは，バージョンが最新になるほど脆弱性の数も極端に少なくなる．古いバージョンのイメージから対象とすることで多くの脆弱性を持つターゲットが利用できる．
- Post-Exploitation を含めた推論の実行：現在の推論はエージェントからターゲットに対して 1 対 1 で行われており，例えば 2 つ以上のターゲットを移動するような攻撃のシナリオ生成はサイバー推論部とは別のグラフ生成時に実施している．複数のターゲットを対象に Post-Exploitation の推論が行えるようにすることで，より高度で複雑なシナリオの効率的な生成が可能となる．

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

これらの課題への対応を行っていくことで，さらに効率的かつ実用性の高いシナリオ生成の可能性が考えられる．

なお，推論のターゲットとなるコンテナイメージに存在する脆弱性の数については，これまで OpenVAS 等の脆弱性検査ツールを使う方法を検討してきたが，一つのイメージに対する検査時間が非常に長くなってしまうため，現実的ではなかった．

そこで，最近 docker に実装された機能である docker scout にも注目している．docker scout は，イメージに存在する脆弱性を docker の独自エンジンで迅速に確認することができるため，例えば学習のターゲットとするイメージを docer scout で事前に絞り込むことで学習の妨げとなるようなイメージを迅速に排除することができる．

また，Post-Exploitation についても，脆弱性検査やペネトレーションテスト等を拡張するものとしてさまざまな研究が行われている[10]．RedChef に Post-Exploitation の機能を実装し，複数のステップを持つシナリオの推論を実行できるよう検討し，より高度で効果的なシナリオの開発を実現させる．

8. あとがき

サイバー攻撃の高度化・巧妙化に伴い，セキュリティ人材の数や技術レベルの不足が懸念される中，サイバーレンジによる効率的で効果の高いセキュリティ教育が注目されている．しかし，シナリオ開発の困難さなどの課題から，普及は限定的で十分な活用がされていないなどの課題があった．

サイバーレンジによる効果的なセキュリティ教育を充実させるため，シナリオ開発の困難さやシナリオ不足に対応する研究が行われているが，これまでのシナリオ生成手法の研究では，特定の脆弱性や攻撃手法を扱うための限定的な自動化にとどまるなど課題があり，より汎用性の高い手法が検討されていた．

そこで，人工知能技術を使ってサイバーインシデントに関連する様々な行動を推論する自律サイバー推論システムの研究を利用することを検討し，既存の機械学習によるペネトレーションテストの手法を改良して開発した Redchef を使ったサイバー推論によるシナリオ生成システムを実装して実験を行った．

ターゲットとして docker HUB に公開されたコンテナイメージを使った実験結果から，複数のシナリオを効率的に生成できることを確認し，サイバーレンジのシナリオ開発に利用できることが確認できた．

ターゲットとなるコンテナイメージの決定方法や脆弱性の有無などの確認方法などの他，複数台のネットワークに対するシナリオを想定した Post-Exploitation への対応などの課題はあるが，今後の研究により対応を行なっていく．

また，自律サイバー推論システムの精度向上も今後の重要な課題である．AI による情報セキュリティ技術は急速に発展を遂げており，特に最近では大規模言語モデル（LLM）を用いた情報セキュリティ技術にも注目が集まっている．

これらの技術を有効的に活用していくことで研究を継続し，自律サイバー推論システムの精度の向上と活用の可能性を広げていく．

謝辞

本研究は、電気通信普及財団の 2022 年度研究調査助成を受けたものです．

参考文献

[1] 中田 亮太郎， 大塚 玲, “Attack Graph を用いたサイバー レンジシナリオの自動生成” , 2022 年暗号と情報セキュリ ティシンポジウム(2022).

[2] 中田 亮太郎， 慎 祥揆, 笠井 洋輔, 豊田 真一, 瀬戸 洋一, “エ コシステムを実現するサイバーセキュリティ演習システ ム cyexec の開発” , 情報処理学会デジタルプラクティス，Vol.11, No.2, pp.414–433(2020).

[3] Muhammad Mudassar Yamin, Basel Katt, Vasileios Gkioulos, ”Cyber ranges and security testbeds:Scenarios, functions, tools and architecture”, Computers Security, Volume 88(2020).

[4] Ryotaro Nakata，Akira Otsuka，”Cyexec*:A highperformance container-based cyber range with scenario randomization”，IEEE Access, Vol.9(2021).

[5] 藤本 大輔，大塚 玲, “深層強化学習を用いた自律サイバー 推論システムの研究” , 2021 年暗号と情報セキュリティシ ンポジウム(2021).

[6] 佐竹 達也，大塚 玲, “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” , 2022 年暗号と情報セキュリ ティシンポジウム(2022).

[7] 米田 智則，大塚 玲, “深層強化学習に基づくペネトレーションテスト手法の提案” , 第 37 回人工知能学会全国大会(2023).

[8] Z. Hu, R. Beuran， Y. Tan, ”Automated Penetration Testing Using Deep Reinforcement Learning”， 2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)(2020).

[9] DeepExploit，”Metasploit Meets Machine Learning”, https://www.mbsd.jp/research/20180228/metasploit-machine-learning/，2023 年 6 月 11 日確認.

[10] Ryan Benito，Alan Shaffer，Gurminder Singh，”An Automated Post-Exploitation Model for Cyber Red Teaming”, Proceedings of the 18th International Conference on Cyber Warfare and Security，Vol.18，No.1(2023).

Copyright © 2023 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.