

# 教授者の負担軽減に向けたセキュリティ演習環境の 自動構築システムの開発

石塚 美伶<sup>1,†1</sup> 竹原 一駿<sup>1</sup> 喜田 弘司<sup>1</sup> 最所 圭三<sup>1</sup>

**概要：**近年、サイバー攻撃の原因となるサーバやネットワーク機器の特定や、設定変更などの適切なセキュリティ対策が実施できる人材が求められている。そこで、このような実践的な技術を体験し、身につけることができるセキュリティ演習が注目されている。この演習を行う環境では、複数台のサーバマシンやネットワーク機器を用いたり、演習内容毎にこれらを設定したりする必要がある。しかし、中小企業や地方の教育機関においては、専門にこれらを設定する人員は無く、セキュリティ演習を実施することが困難である。本研究では、セキュリティ演習における教授者が行う、環境構築の負担を軽減する演習環境の自動構築システムを開発する。評価実験では、演習環境として仮想マシンを構築する際の起動時間を計測し、台数に対し線形に増加することを確認した。

**キーワード：**サイバーセキュリティ、セキュリティ演習、仮想化技術、環境構築、自動化

## Development of an Automatic Construction System for Security Training Environments to Reduce Instructor Burden

MIREI ISHIZUKA<sup>1,†1</sup> ICHITOSHI TAKEHARA<sup>1</sup> KOJI KIDA<sup>1</sup> KEIZO SAISHO<sup>1</sup>

**Abstract:** In recent years, there has been a demand for personnel who can identify servers and network devices that are the source of cyber-attacks and implement appropriate security measures, such as changing their settings. As a way to develop such personnel, security exercises, which allow participants to experience and acquire such practical skills, have become popular. The environment in which these exercises are conducted requires the use of multiple server machines and network devices, and these must be set up for each exercise. However, small and medium enterprises and regional educational institutions have no dedicated personnel to set up these environments, making it difficult to conduct security exercises. In this research, we develop an automatic exercise environment construction system that reduces the burden of environment construction for instructors of security exercises. In the evaluation, we measured the startup processing time when building virtual machines as a training environment. As a result, we confirmed that it increased linearly with the number of machines.

**Keywords:** Cyber Security, Security Exercises, Virtualization Technology, Environment Construction, Automation

### 1. はじめに

近年、サイバー攻撃の件数や手口が増加・巧妙化しており [1], [2], 脆弱性を持つソフトウェアへの対策や不審な活動を行っていないか監視するなどの継続的な活動が必要で

ある [3]. 一方で、セキュリティ人材は不足の一途を辿っており [1], [4], 特に「セキュリティインシデント発生時の緊急対応」や「サイバー攻撃の高度化への対応」ができる人材が求められている [5]. これらを受けて大学などの教育機関においては、攻撃者からのサイバー攻撃に備えた防御ができ、攻撃を発見した際にいち早い察知と、的確な対処ができるセキュリティ技術者の育成が求められている。

<sup>1</sup> 香川大学 Kagawa University

<sup>†1</sup> 現在, 既卒  
Presently with Graduate

セキュリティ技術者の育成には攻撃に気づくことや攻撃を受けたときの対策方法を実践できるセキュリティ演習が有効であり、有名なものではハードニング演習（サーバ防御演習）がある。これは、実際のサービスの運営を模した演習システムで、セキュリティ対応チームの一員に切り切って攻撃からサービスを守る演習である [6]。防御するには、ログファイルを閲覧することでサーバ内の状況を把握したり、不正なアクセスを遮断するための Firewall の操作などを行う。日本では“Microhardening”や“Mini Hardening”が、ヨーロッパでは ENISA (European Union Agency for Cybersecurity) による“Cyber Europe”が有名である [7], [8], [9]。

ハードニング演習は、サイバー攻撃や防御の影響を防ぐため、組織内のネットワークから隔離された環境で実施することが求められる。香川大学でもハードニング演習を実施しているが大学単体での演習の実施は難しく、企業との協力により構築された環境を用いている [10], [11]。将来、中小企業や地方の教育機関においてもセキュリティ演習を実施するためには、自身の組織で環境構築ができる必要がある。

本研究では、演習環境を構築する上で必要となる教授者に対する手間と計算機資源について着目した、自動構築システムを開発する [12]。このシステムは、演習内容に応じた仮想環境を容易に構築するために GUI を導入し、さらに Firecracker を用いることで短い起動時間で仮想環境を構築する。本論では、開発した自動構築システムの概要と、起動時間における評価を示す。

## 2. 課題

香川大学で実施しているハードニング演習から、課題を導出する。著者らは、演習の授業補助を行った経験があり、演習方法について理解している。本演習は図 1 に示す環境が必要である。演習システムは、演習監視用サーバ、EC サイトを構成するサーバ群、エージェント群にて構成される。EC サイトを構成するサーバ群は下記で構成される。

- EC サイトを運営するための Web サーバ
  - 必要となるデータを管理するデータベースサーバ (DB)
  - サービスと利用者のやり取りを実現するメールサーバ
- また、エージェント群は下記で構成される。
- Web サーバを構成する攻撃者エージェント
  - EC サイトを利用する利用者エージェント

演習が始まると、利用者エージェントは商品の購入を行うために、EC サイトにアクセスする。また、攻撃者エージェントは Web サーバに対して、SSH のパスワードクラックにおける侵入や Web ページの改竄や設定変更などのサイバー攻撃を行う。学習者は 8~10 人が 1 チームとなり、セキュリティ対応チームの一員としてサーバに RDP や SSH などと接続し、サービス (Apache などのデーモン) の起動

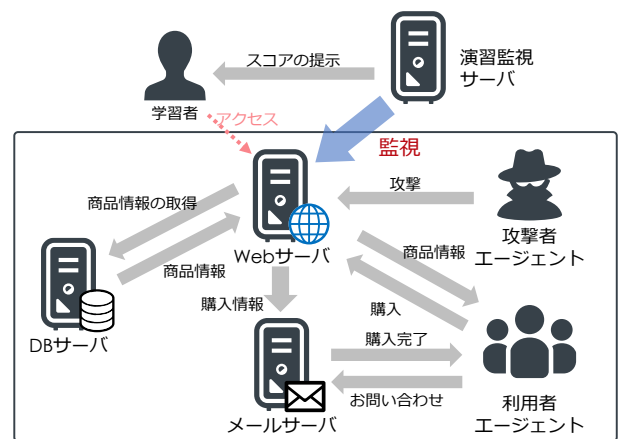


図 1 香川大学における演習環境

Fig. 1 Exercises Environment at Kagawa University.

や停止、ログの確認、サーバ毎に Firewall の設定を変更などを行う。演習監視用サーバでは、利用者エージェントの動作を監視し購入に成功した数や、演習のシナリオに応じて攻撃者エージェントに攻撃を行うタイミングを指示する。

このような演習では、演習中の攻撃内容や防御内容が学内や他チームに影響しないように、ネットワークを分離する必要がある。また、EC サイトなどの演習内容に応じた複数のサーバをチーム数分構築する必要がある。例えば、香川大学の演習では 5 チームで実施しているが、上述の構成では 15 台のサーバが必要である。

著者らは、環境構築の負担を体験するために、上述した構成と同様の演習環境を構築した。サーバ群は KVM による仮想マシンを用いて構築し、さらに、接続する機器ごとに異なるネットワークセグメントを与えることで分離した。その結果、構築と動作確認を終えるまでに約 50 時間を要した。その原因は、想定していない事象が発生した際に、原因の究明や解決方法の調査に多くの時間を要したためである。

このように、演習環境の構築に多くの時間と知識を要するため、専門的な知識が必要となり、演習を担当する教授者の負担が大きい。さらに、演習内容に応じてサーバの構成を変更する必要がある。演習環境の構築は、必ずしも教授者が実施するとは限らず、教育機関や企業におけるシステム管理者や TA が担当することもある。これらのことからセキュリティ演習環境の構築において、専門的な知識や詳細な設定作業を必要とせず、短時間かつ容易に構築作業を行えるシステムが求められる。

## 3. 提案システム

### 3.1 利用イメージ

本システムの利用イメージを説明する。教授者は、提案システムが提供する Web インタフェースにアクセスする。Web インタフェースでは、図 2 に示すホーム画面と、図 3 に示す編集画面を提供する。ホーム画面では、登録されて

Home

Login

Create New

Home

新規作成

id	name	details	status	create_at	
1	keishiro	Demo	stop 起動 停止	2022-02-17 06:02:03	edit
2	MotobuNet	Demo	stop 起動 停止	2022-02-17 06:37:13	edit
3	SekitoNet	Demo	stop 起動 停止	2022-02-17 06:45:46	edit
4	TatsuhiroNet	Demo	stop 起動 停止	2022-02-17 07:25:26	edit
5	UedaNet	Demo	stop 起動 停止	2022-02-17 08:06:53	edit
6	pochi	Demo	stop 起動 停止	2022-02-22 05:38:11	edit
7	test	Demo	stop 起動 停止	2023-01-17 08:40:02	edit
8	test	Demo	stop 起動 停止	2023-01-17 08:43:33	edit
10	seminar	for seminar	stop 起動 停止	2023-10-16 05:45:44	edit

起動停止

edit

図 2 ホーム画面

Fig. 2 Home Screen.

Home
Login
Create New

Edit

環境ID: / new 保存 追加

ネットワークマップ

図 3 編集画面

Fig. 3 Edit Screen.

seminar 保存
追加

ID: 11
Name: seminar-vnet
Gateway: 10.0.10.1
Netmask: 255.255.255.0
IP: 10.0.10.10
10.0.10.254
ok

図 4 仮想ネットワークの詳細設定

Fig. 4 Virtual Network Detail Settings

いる演習環境の一覧を表示する。教授者は、「Create New」を押下することで、編集画面に遷移する。

編集画面では、演習環境を構築できる。「+追加」ボタンにて仮想マシンのイメージの一覧と選択肢が提示されるので、教授者が演習に即したものを選択する。選択したイメージは、仮想マシンとして図 3 のネットワークマップに配置される。また、「+追加」からは仮想ネットワークの追加画面に遷移でき、図 4 に示すように仮想ネットワークの詳細設定が行える。仮想マシンを選択すると図 5 に示すように、仮想マシンの詳細設定が可能であり仮想ネットワークを指定できる。「保存」を押下することで、演習環境の設定がデータベースに保存される。保存後、ホーム画面に戻ると、編集した演習環境が一覧に表示される。

演習開始時は、教授者がホーム画面の「起動」を押下することで、演習環境の仮想マシンの展開と起動と IP アド

seminar 保存
追加

ID: 88
Name: nginx
Purpose: web
Image: 2 / /home/misizuka/go\_doc
Networks:
seminar-vnet x
ok

図 5 仮想マシンの詳細設定

Fig. 5 Virtual Machine Detail Settings

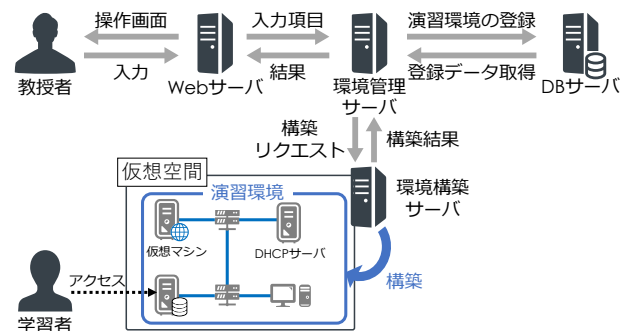


図 6 提案システムの構成

Fig. 6 System Configuration of Proposed System.

レスの割り当てが行われる。仮想マシンに割り当てられた IP アドレスは環境構築サーバ内のローカルな IP アドレスであるため、学習者は環境構築サーバを踏み台とすることで仮想マシンにアクセスできる。

「停止」からは仮想マシンの停止が行われる。

### 3.2 構成

図 6 に提案システムの構成を示す。本システムは演習環境の設定情報を格納するデータベースサーバ (DB サーバ)、仮想マシンや仮想ネットワークを構築し、演習環境を構築するための土台となる環境構築サーバ、教授者の操作内容を受け取り、データの操作や設定ファイルの生成、演習構築用サーバへの構築リクエストを送信する環境管理サーバ、教授者の GUI 操作を実現する Web サーバで構成する。

本稿では、Web サーバでは React を用いて GUI を実装し、環境管理サーバと環境構築サーバでは Go 言語による echo フレームワークを用いて実装し、API の提供とデータベースへのアクセスや演習環境の構築を行う。データベースサーバには MySQL を用いた。

演習環境内で構築する仮想マシンについては、ホストマシンで多くの仮想マシンを起動できることと、それらの起動時間の短縮を狙い、Firecracker[13] を用いて構築した。Firecracker とは、仮想マシンに対し不必要なデバイス割り当てやゲスト機能を削減することで高速な起動を実現し、かつ簡易な構築を可能とする VMM(仮想マシンモニタ)で

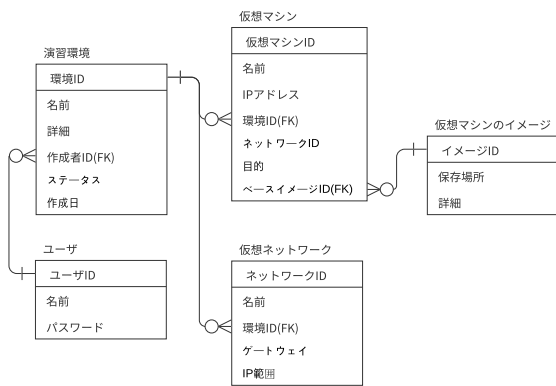


図 7 提案システムの ER 図  
Fig. 7 Entity-Relationship Diagram.

ある。Firecracker による仮想マシンの起動には、OS の中核となるカーネルと仮想マシンのルートファイルシステム (/) となる “rootfs” が必要であり、仮想マシンに関する設定を記入した “config” ファイルを Firecracker 実行時に読み込むことで、必要な機能を持つ仮想マシンを作成することができる。

### 3.3 データベース設計

図 7 に提案システムの ER 図を示す。各テーブルは下記の役割を持つ。

**ユーザ** 本システムを利用する教授者の情報を格納する。

**演習環境** 演習環境の状態を格納する。

**仮想マシン** 演習環境内の仮想マシンの情報を格納する。

また、ネットワーク ID の要素には、接続するネットワークの ID を複数個格納する。

**仮想マシンのイメージ** 仮想マシンの “rootfs” イメージのパスと用途を格納する。

**仮想ネットワーク** 演習環境内の仮想ネットワークの情報を格納する。ゲートウェイはホストマシンが持つ IP アドレスを格納する。IP アドレスの範囲は仮想マシンに DHCP で割り当てる IP アドレスの範囲である。

### 3.4 演習環境の起動と停止

演習環境は、3.1 節に述べたとおり、教授者が Web サーバの GUI で入力することで、データベースに登録される。起動時には、データベースの内容を元に、仮想マシンと仮想ネットワークを作成する。まず、データベースを元に、演習環境用の “config” ファイルを生成する。仮想マシンについては、仮想マシン毎に指定の “rootfs” イメージをコピーし、“config” ファイルに指定する。仮想ネットワークについては、データベースを元に仮想ネットワークに関する XML ファイルを作成し、“virsh” コマンドを用いて仮想 DHCP サーバを構築する。なお、このとき仮想 DHCP サーバで管理する tap デバイスを仮想マシンの台数分作成

表 1 スペック

Table 1 Machine Specifications.

項目	ホストマシン	仮想マシン
CPU	Core i9-9900KS (12 コア)	2 コア
メモリ	32GB	1024 MB
OS	Devuan GNU/Linux 5	Ubuntu 20.04 LTS

※ ホストマシンは、Proxmox VE 8.4.0 にて構築した仮想マシン

```

1 Last login: Mon Jul 28 06:35:16 UTC
  2025 on ttyS0
2 root@ubuntu-focal:~ #
    
```

図 8 コマンド入力を受け付けるプロンプト

Fig. 8 Prompt for Command Input.

する。tap デバイスは、“config” ファイルにて、仮想マシン 1 台に 1 つを設定する。

“config” ファイルを “firecracker” コマンドに指定することで、設定した仮想マシンを起動できる。起動後は仮想 DHCP サーバより、ローカルの IP アドレスが割り当てられる。仮想マシンを起動した後は、そのプロセス ID を環境管理サーバにて管理し、データベースの演習環境の状態を起動中に更新する。

演習環境を停止する場合は、仮想マシンのプロセス ID を “kill” し、仮想ネットワークを削除したのちに、データベースの演習環境の状態を停止に更新する。

## 4. 評価

### 4.1 目的と手法

本システムにおける演習環境の実現可能性と拡張性を評価するため、指定した個数の仮想マシンを同時に起動したときの処理時間を計測する。

本評価を行うホストマシンと仮想マシンのスペックを表 1 に示す。仮想マシンは、Apache や MySQL などを用いて Web サービスを提供できる性能を有しており、セキュリティ演習を行えるスペックである。なお、ディスクは SSD を使用している。本稿で評価する仮想マシンの台数は、ホストマシンのメモリサイズを超えない範囲である、1~25 台を評価する。

起動処理は、“firecracker” コマンドを実行してから、仮想マシンの OS の起動処理が始まりユーザからのコマンド入力を待ち受けるプロンプト (図 8) が表示されるまでである。

### 4.2 結果と考察

仮想マシン台数ごとの起動に掛かった処理時間を図 9 に示す。実験では、No.1~No.5 に示すように 5 回の計測を行った。25 台の時でも約 50 秒で起動できており、十分短時間で起動処理を行えた。

各回の計測とも概ね同じ傾向を示しており、仮想マシン

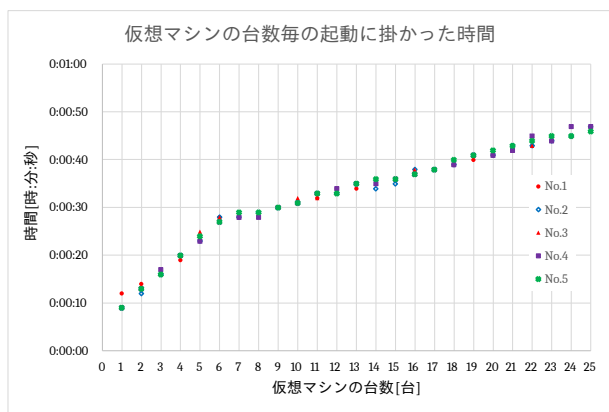


図 9 仮想マシンの起動時間

Fig. 9 Boot Processing Time of Virtual Machines.

の台数が増えると傾きが緩やかになるが、全体的に仮想マシンの台数に対する比例関係が見られる。これにより、演習シナリオに応じて、必要な仮想マシンの台数を増減しても、起動時間が予測できることがわかる。

1 章でも述べた中小企業や地方の教育機関では、複数のホストマシンを用意できず 1 台のホストマシンにて、複数の演習シナリオやセキュリティ演習以外のプログラミングやソフトウェアの動作確認などを実施することが考えられる。そのような状況において起動時間が短く、かつ予測できるということは、ホストマシンを効率的に使用することができる。例えば、今回の仮想マシンのスペックは表 1 に示すように初学者向けの C 言語の演習程度には十分なスペックである。ある授業コマでは学習者数分の C 言語の演習を実施し、休憩時間 (10 分) 中にセキュリティ演習の環境 (2 章では 15 台) を起動するなどのような運用が可能である。企業においては、業務のシステム開発に、提案システムで構築した仮想マシンを用いることができる。セキュリティ演習を実施する際には、一部のシステム開発に使用しているマシンを停止し、演習環境を起動できる。このとき、起動時間が予測できるため時間管理が行いやすく、業務に影響を与えることなく演習を行うことができる。

またホストマシンのメモリを増やすことで、さらに多くの仮想マシンを起動できる。その場合も実験結果から、線形に起動時間が増加すると言えるため、例えば学習者数が倍増した場合では、100 分程度で起動できると予測できる。

## 5. 関連研究

### 5.1 セキュリティ演習が行える仮想空間の構築

Cuong らは、セキュリティ演習のための仮想空間を構築するためのシステム “CyRis” を開発している [14]。このシステムは、教授者の用意する演習環境の定義に応じてサイバーレンジを自動的に構築するが、定義の記述に YAML を用いるため、Syntax エラーなど演習環境の構築の本質とは異なる箇所に時間が割かれる。

湯川らは、2 人 1 組で攻防戦型ネットワークセキュリティ演習を行う演習システムを開発している [15]。このシステムでは、軽量ではあるが低機能な仮想化ソフトウェアである User Mode Linux (UML) を用いているため、集中管理が難しく、演習の内容に応じて仮想マシンを操作することが難しい。これに対して、提案システムで用いている Firecracker は API により仮想マシンの制御を行うことができるため、2 章で述べたようなエージェントを伴う演習シナリオにも対応することができる。

### 5.2 コンテナを用いた演習環境の構築

コンテナの利点は、仮想マシンと比べてシステム運用にかかるリソースが少ないことである。Nakata らは、ランダムな演習シナリオを生成し、Docker コンテナを用いて演習環境を作成でき、仮想マシンよりも CPU 負荷やストレージの使用量が少ない演習システムを開発した [16]。岸本らは、Docker コンテナを用いることで実運用から隔離した演習環境を構築できるとし、HTTP リクエストの改ざんなどの体験や Web アプリケーションの修正を行える演習システムを開発した [17]。

しかし、コンテナはホスト OS とカーネルを共有するため、コンテナ内で再現した脆弱な状態がホスト OS に影響を及ぼす可能性がある [18]。ホスト OS に影響が無い演習シナリオを選択する必要がある、システムによって演習できる内容が制限される。以上よりコンテナを用いて演習を行う場合は、物理マシン全体のネットワークからの隔離が必要となるため、運用の負担が大きい。

### 5.3 シミュレータによる演習環境の構築

一方で、セキュリティ演習環境において、学習者の入力に対し機器の挙動を模倣するシミュレータに関する研究もある。宮城らは、ネットワーク構築演習において Slack を通じてネットワークシミュレータ (GNS3 [19]) の操作を可能とした [20]。IPA は、脆弱性を体験できる Web アプリケーションのコンテンツと Apache [21] を合わせて 1 つのツールとして提供している [22]。

これらは、開発者が想定している範囲でしか演習ができず、演習シナリオの内容が制限される。例えば、学習者による SSH の総当たりなどの演習を行う場合、学習者が入力した設定内容に応じた Syntax エラーやアクセス (挙動) を再現する必要がある。また、学習者にとっては自身の入力に対するシミュレータの結果が想定と異なったとき、それが適切であるか、シミュレータのバグや機能不足であるかの判断が難しい。

## 6. おわりに

セキュリティ技術者の育成が重要である一方で、セキュリティ演習環境の構築には専門的な知識と多くの時間を要

する。本研究では、セキュリティ演習環境の自動構築システムを開発している。このシステムは、演習内容に応じた仮想環境を容易に構築するために GUI を導入し、さらに Firecracker を用いることで、短い起動時間で仮想環境を構築する。実験により、1~25 台の仮想マシンの起動時間を評価し、仮想マシンの台数に対して線形に起動時間が増加することを確認した。5 回の計測を行ったが、ほぼ一致したことから、台数を増加させても起動時間が予測でき、本システムを効率的に運用できる。

最近では、文献 [23] や [24] に示すように、自組織において受けたサイバー攻撃の詳細や利用された脆弱性を公開することが増えている。一方で、テキスト生成 AI の進化がめざましく、これを用いてマルウェアを生成した事例もある [25]。また、テキスト生成 AI の技術の 1 つであり、外部資料を用いたテキスト生成を可能とする RAG (Retrieval Augmented Generation) [26] も有名である。これらにより、サイバー攻撃の報告資料を用いた脆弱性を持つ環境と、報告資料に従った攻撃を行うスクリプトを自動生成することが可能であり、演習シナリオ自体の自動生成が行えるようになると考えている。

**謝辞** 本研究は JSPS 科研費 JP25K17074 の助成を受けたものです。

## 参考文献

- [1] ISC2: How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, [https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity\\_Workforce\\_Study\\_2023.pdf](https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity_Workforce_Study_2023.pdf). (2025.08.17).
- [2] 総務省: 関係情報: 情報通信関連: 情報通信白書令和 6 年版, <https://www.soumu.go.jp/johotsusintokei/whitepaper/r06.html>. (参考 2024-09-26).
- [3] サイバーセキュリティ戦略本部: サイバーセキュリティ 2024 (2023 年度年次報告・2024 年度年次計画), <https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>. (参考 2024-09-26).
- [4] IPA 独立行政法人情報処理推進機構: 情報セキュリティ白書 2024 変革の波にひそむ脅威: リスクを見直し対策を, [https://www.ipa.go.jp/publish/wp-security/eid2eo0000007gv4-att/2024\\_ALL.pdf](https://www.ipa.go.jp/publish/wp-security/eid2eo0000007gv4-att/2024_ALL.pdf). (参考 2024-10-22).
- [5] NRI セキュアテクノロジー株式会社: NRI Secure Insight 2023: 企業における情報セキュリティ実態調査, <https://www.nri-secure.co.jp/download/insight2023-report>. (参考 2024-10-27).
- [6] Seker, Ensar and Ozbenli, Hasan Huseyin: The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation (2018).
- [7] 株式会社川口設計: MicroHardening, <https://www.sec-k.co.jp/mh>. 2021-05-09.
- [8] Hardening, M.: MINI Hardening Project - connpass, <https://minihardening.connpass.com/> (2022).
- [9] the European Union Agency for Cybersecurity: Cyber Europe — ENISA, <https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/>
- [10] 喜田弘司: 情報セキュリティが得意な情報システムの専門家を育てる演習授業 | 授業紹介 | 国立大学 55 工学系学部 HP, <https://www.mirai-kougaku.jp/lesson/pages/97.php>. (参考 2024-05-16).
- [11] 香川大学: 香川大学教務システム Campus-Xs, [https://kyoumusyst.kagawa-u.ac.jp/campusweb/slbbssbdr.do?value\(risyunen\)=2023&value\(semekikn\)=1&value\(kougicd\)=E5005150-1&value\(crc1umcd\)=9999](https://kyoumusyst.kagawa-u.ac.jp/campusweb/slbbssbdr.do?value(risyunen)=2023&value(semekikn)=1&value(kougicd)=E5005150-1&value(crc1umcd)=9999). (参考 2024-12-16).
- [12] 石塚美伶, 竹原一駿, 亀井仁志, 喜田弘司, 最所圭三: セキュリティ演習環境の自動構築システムの提案, 令和 4 年度電気・電子・情報関係学会四国支部連合大会講演論文集, Vol. 16-2, p. 159 (2022).
- [13] Amazon Web Services, I.: Firecracker, <https://firecracker-microvm.github.io/>. (参考 2024-11-26).
- [14] Pham, C., Tang, D., Chinen, K.-i. and Beuran, R.: CyRIS: A Cyber Range Instantiation System for Facilitating Security Training, *Proceedings of the 7th Symposium on Information and Communication Technology*, pp. 251–258 (2016).
- [15] 湯川誠人, 谷口義明, 井口信和: 攻防戦型ネットワークセキュリティ学習支援システム, 電子情報通信学会論文誌 D, Vol. 103, No. 8, pp. 591–602 (2020).
- [16] Nakata, R. and Otsuka, A.: CyExec\*: Automatic Generation of Randomized Cyber Range Scenarios, *International Conference on Information Systems Security and Privacy* (2021).
- [17] 岸本和理, 谷口義明, 井口信和: 攻撃者視点を取り入れた Web アプリケーションセキュリティに関するセキュアプログラミングの実践的演習システム, 第 84 回全国大会講演論文集, Vol. 2022, No. 1, pp. 657–658 (2022).
- [18] Souppaya, M., Morello, J. and Scarfone, K.: Application Container Security Guide. (IPA 情報処理推進機構訳) (参考) 2017-09-25.
- [19] : GNS3 — The software that empowers network professionals, <https://www.gns3.com/>. (参考 2024-11-05).
- [20] 宮城勝, 吉原和明, 越智洋司, 井口信和: Slack を用いたネットワーク構築演習における学習状況可視化機能の実装, 情報処理学会論文誌, Vol. 65, No. 1, pp. 255–260 (2024).
- [21] Foundation., T. A. S.: Welcome! - The Apache HTTP Server Project, <https://httpd.apache.org/> (2024). (参考 2024-10-25).
- [22] IPA 独立行政法人情報処理推進機構: 脆弱性体験学習ツール AppGoat — 情報セキュリティ — IPA 独立行政法人情報処理推進機構, <https://www.ipa.go.jp/security/vuln/appgoat/index.html>. (参考 2024-11-05).
- [23] お茶大 CSIRT: お茶の水女子大学研究室サーバへの不正アクセスについて — お茶の水女子大学, <https://www.ocha.ac.jp/news/d014455.html>. (参考 2024-12-05).
- [24] ぴあ株式会社: 【4337 ぴあ】不正アクセスによる、個人情報流出に関するお詫びとご報告 20170425, [https://corporate.pia.jp/news/files/security\\_incident20170425.pdf](https://corporate.pia.jp/news/files/security_incident20170425.pdf). (参考 2024-12-05).
- [25] Incorporated., T. M.: 生成 AI でランサムウェアを作成した容疑者の摘発事例を考察 — トレンドマイクロ (JP), [https://www.trendmicro.com/ja\\_jp/jp-security/24/e/breaking-securitynews-20240529-02.html](https://www.trendmicro.com/ja_jp/jp-security/24/e/breaking-securitynews-20240529-02.html). (参考 2024-12-05).
- [26] 野村総合研究所: RAG — 用語解説 — 野村総合研究所 (NRI), <https://www.nri.com/jp/knowledge/glossary/lst/alphabet/rag>. (参考 2024-12-05).