情報処理学会論文誌　デジタルプラクティス　Vol.4　No.3　22–32 (July 2023)

クラウド環境を標的とするDDoS攻撃の対策訓練システム

眞鍋 督[1,a)]　谷口 義明[2,3,b)]　井口 信和[2,3,c)]

受付日 2022年11月22日, 採録日 2023年4月21日

概要：本研究では，クラウド環境を標的とするDDoS攻撃の対策演習を実施できる環境の提供を目的としてDDoS攻撃の対策訓練システムを開発した．本システムは，Infrastructure as a Serviceにおいて最も採用されているAmazon Web Serviceを用いた演習が可能である．また，高度化するDDoS攻撃にも対応できる力を身につけるために，対策手法に加えて攻撃手法に関する演習も実施できる．本システムによる演習を通して，クラウド環境を狙ったDDoS攻撃の対策手法に関する理解と知識の定着が期待できる．実験協力者20名を対象に実施した評価実験の結果，本システムを利用する学習が座学と比較して有効であることを確認した．

キーワード：DDoS攻撃，対策訓練，クラウド環境，セキュリティ，Amazon Web Service

Training System for Countermeasures Against DDoS Attacks Targeting Cloud Environments

Susumu Manabe[1,a)]　Yoshiaki Taniguchi[2,3,b)]　Nobukazu Iguchi[2,3,c)]

Received: November 22, 2022, Accepted: April 21, 2023

Abstract: In this paper, we developed a DDoS attack countermeasure training system to provide an environment where countermeasure exercises against DDoS attacks targeting cloud environments can be conducted from an attacker perspective. Our system enables countermeasure exercises using Amazon Web Service, which is the most widely used Infrastructure as a Service. In addition to countermeasures, our system can also provide exercises on attack methods so that learners can acquire the ability to respond to complex DDoS attacks. Through exercises using our system, learners can gain understanding and knowledge of countermeasures against DDoS attacks on cloud environments. Through evaluations with 20 experiment collaborators, the effectiveness of our system was confirmed compared with self-study with study materials.

Keywords: DDoS attacks, countermeasure training, cloud environment, security, Amazon Web Service

1. はじめに

企業等におけるクラウドサービスの利用率は年々上昇し，2021年には7割以上の企業が利用している[2]．クラウドサービスの利用形態の1つにInfrastructure as a Service（以下，IaaS）がある．IaaSはハードウェアリソースなどのデジタルインフラをインターネット経由で提供するサービスである．IaaSにおけるクラウドサービスの利用比率ではAmazon Web Service（以下，AWS）が最も高い[3]．

クラウドサービスの普及に伴い，企業が利用するクラウド環境を標的としたDDoS（Distributed Denial of Service）攻撃が増加している[4]．DDoS攻撃では，マルウェアに感染した機器で構成されるボットネットからサーバに大量のデータや制御パケット等を送信し，サービスを妨害する．一方，通信サービス事業に勤務する事業者を対象とした調査によると「DDoS攻撃を緩和するための適切な対策を講じている」と回答したのは29%であった[5]．この原因の1つとしてセキュリティ技術者の不足が挙げられ

1　近畿大学大学院総合理工学研究科
Graduate School of Science and Engineering Research, Kindai University, Higashiosaka, Osaka 577–8502, Japan
2　近畿大学情報学部
Faculty of Informatics, Kindai University, Higashiosaka, Osaka 577–8502, Japan
3　近畿大学情報学研究所
Cyber Informatics Research Institute, Kindai University, Higashiosaka, Osaka 577–8502, Japan
a)　manabe0123m@gmail.com
b)　y-tanigu@info.kindai.ac.jp
c)　iguchi@info.kindai.ac.jp

本稿は文献[1]を発展させ，まとめなおしたものである．

る [6]．この問題の解決のためには，クラウド環境を標的とする DDoS 攻撃の対策手法を取得したセキュリティ技術者を早期に養成しなければならない．

ここで，DDoS 攻撃を実施する代表的なマルウェアに Mirai がある．Mirai は Linux で動作する脆弱なパスワードの設定された IoT 機器に感染し，機器を遠隔操作可能なボットにする．また，多数のボットから構成されるボットネットを構築する．その後，攻撃者からの指令に応じて，ボットネット内の機器は指定されたターゲットに対して一斉に DDoS 攻撃を実行する．Mirai は 2016 年 9 月のセキュリティブログへの攻撃や，2016 年 10 月の DNS サーバープロバイダ Dyn 社への攻撃等に使われ，後者の攻撃では，当時史上最大規模である 1.2〜Tbps の DDoS 攻撃が観測された [7]．さらに，Mirai の作者がソースコードを公開したためこれを利用した亜種のマルウェアが出現している [8]．これらを背景に，ボットネットを踏み台とした DDoS 攻撃は種類が多様化し，年々複雑さを増している [4]．そのため，机上学習や対策視点のみの学習では，今後，高度化する DDoS 攻撃への対策が難しくなると予想される．

DDoS 攻撃に対応できる技術者養成のためには，ハンズオン形式の演習が可能な学習システムが有効であると考えられる．また，高度化する DDoS 攻撃に対応するためには，対策視点だけでなく攻撃視点で学ぶことが有効と考えられる．攻撃の実施を含めて DDoS 攻撃に関する演習を実施可能な学習システムはいくつか提案されている [9]–[12]．しかし，これらのシステムでは，近年普及の進むクラウド環境を標的としたサイバー攻撃に対する対策学習を想定していない．また，DDoS 攻撃の理解には攻撃の主要な要素であるボットネットや攻撃に使用されるサーバ群の理解も重要となるが，これら既存の検討ではボットネットやサーバ群の構築まで含めた攻撃手法の学習を想定していない．さらに，これら既存の検討では，実際に学習システムを使った場合の学習効果が十分に評価されていない．

本研究では，クラウド環境を標的とする DDoS 攻撃の対策演習を実施できる環境の提供を目的とし，攻撃視点を取り入れた DDoS 攻撃の対策訓練システム（以下，本システム）を開発した．本システムを利用する場合，学習者は 1 人で攻撃演習と対策演習に取り組むことができる．また，クラウド環境としては IaaS において最も採用されている AWS を対象としている．さらに，DDoS 攻撃の高度化が懸念される要因となった IoT マルウェア Mirai をモデルとし，ボットネットや攻撃サーバ群の構築から DDoS 攻撃まで一連の DDoS 攻撃演習を実施できる．本システムによる演習を通して，高度化する DDoS 攻撃に対応可能なセキュリティ技術者を養成できると考えられる．また，攻撃視点と対策視点からの学習により，DDoS 攻撃の対策手法に関する理解と知識の定着が期待できる．本研究では，座学の場合と本システムを用いて学習した場合の学習効果を比較することで，本システムの有効性を確認する．

以降の本稿の構成は以下のとおりである．2 章で関連研究について述べ，3 章で本研究で想定するシステムに求められる要件について述べる．4 章で開発したシステムの概要，5 章で本システムによる DDoS 攻撃演習，6 章で DDoS 対策演習について述べる．7 章で本システムの評価結果について述べ，8 章でまとめと今後の課題を述べる．

2. 関連研究

本章では，DDoS 攻撃の学習システムに関する研究と，AWS が提供するセキュリティ学習サービスを述べる．

2.1 DDoS 攻撃の学習システムに関する研究

サイバー攻撃に関する学習システムについては，ネットワークセキュリティに関する演習を行えるもの [14], [15]，Web セキュリティに関する演習を行えるもの [16], [17] など様々な検討がある．また，DoS 攻撃や DDoS 攻撃に関する演習を実施可能な学習システムに関してもいくつか検討がある [9]–[13]．

立岩らの研究 [13] では，セキュリティ技術者の養成を目的に，仮想化技術を用いたセキュリティ演習システムを開発している．遠隔演習環境とあらかじめ構築された仮想ネットワークへ自動攻撃する機能を用いることで，DoS 攻撃を含むサイバー攻撃の対策に関する学習が可能である．

千川らの研究 [9] では，安価なシングルボードコンピュータを利用し，IoT 機器の乗っ取りを題材にした DoS 攻撃の演習システムを開発している．学習者は，IoT 機器を踏み台にしてライブ動画配信サービスに対して DoS 攻撃の一種である HTTP flood 攻撃を実施できる．Fuertes らの研究 [10] では，ネットワークセキュリティの教育と学習プロセスを改善することを目的に，仮想ネットワークを使った DDoS 攻撃の対策訓練システムを開発している．このシステムでは，学習者はまず DDoS 攻撃の種類を選択し対象のサーバへ攻撃を実施する．その後，ファイアウォールを用いて選択した DDoS 攻撃に応じた対策を実施する．これらのシステムでは，攻撃を特定して対策するといった実践的なセキュリティ学習に取り組むことができない．

Kwon らの研究 [11] では，基本的なセキュリティに関する知識を学ぶことができる演習環境の提供を目的とし，実践型セキュリティ演習システムを開発している．このシステムは，あらかじめ準備している Web サーバに対して DDoS 攻撃である Slowloris と RUDY を実施する．学習者は，2 つの種類から実施される攻撃のうちどの攻撃を受けているか特定し，対策を施す演習に取り組むことが可能で

ある．このシステムではアプリケーション層で実施されるDDoS 攻撃の対策手法に関する学習のみ対応している．

八代らの研究 [12] では，IT ユーザ企業でのインシデントレスポンスにおける初期段階の学習機会の提供を目的とし，体験型サイバーセキュリティ学習システムを開発している．学習者は 2 人 1 組となり，システムから提供されるコンテンツを参照し演習に取り組む．クラウド上の接続用仮想 PC にアクセスし，あらかじめ準備されたシナリオに基づいて学習を進める．このシステムでは DDoS 攻撃の攻撃手法と分析手法に関する演習を実施できる．

DoS 攻撃や DDoS 攻撃に関するこれらの学習システムについて，学習対象となる攻撃，攻撃演習の実施方法，対策演習の実施方法，学習効果の評価方法をまとめたものを**表 1** に示す．これらの関連研究の共通の課題として，サイバー攻撃の対象はオンプレミス環境からクラウド環境に変化しているのに対して，これらの研究ではクラウド環境を標的とするサイバー攻撃の対策学習を想定していないことが挙げられる．また，実際の DDoS 攻撃の際に用いられるボットネットや攻撃サーバ群の構築を演習内容として想定していない，実際に学習システムを使った場合と他の手段を使った場合の学習効果が十分に評価されていない，といった課題もある．

2.2　AWS が提供するセキュリティ学習サービス

本研究の開発システムで対象としている AWS が提供するセキュリティ学習サービスもある [18], [19]．これらのサービスでは，AWS のクラウド環境を標的とするサイバー攻撃の対策手法を学ぶことができる．AWS Security Essentials [18] はクラウドセキュリティに関する知識を持たない初級レベルの学習者を対象としており，DDoS 攻撃の対策手法を学習できる．Security Engineering on AWS [19] はクラウドセキュリティに関する知識を持つ中級レベルの学習者を対象としており，DDoS 攻撃に対して脆弱な設定を特定する手法や，DDoS 攻撃の対策手法を学習できる．しかし，これらのサービスで準備されている DDoS 攻撃のコンテンツは，両コースとも座学を想定したものであり，ハンズオン形式による演習は実施できない．また，これらのサービスを受講するためには AWS が認定した講師が必要となる．

3.　システム要件

本システムの利用対象者（以降，学習者）は，サイバーセキュリティ分野を専攻する学生，DDoS 攻撃の対策手法またはクラウドセキュリティについて興味のある学生，中小企業社員などの中でクラウド環境を狙った DDoS 攻撃の対策に関する知識が不足している初級学習者を想定する．学習者は，基本情報技術者試験に合格相当の知識，Linux の基本的なコマンド操作技術を持つことを想定する．

2 章で述べた関連システムは，DDoS 攻撃に用いられる攻撃サーバ群やボットネット構築演習を実施できない，クラウド環境を標的とする DDoS 攻撃の対策学習を想定していない，学習システムを使った場合と他の手段を使った場合における学習効果が十分に評価されていない，といった課題がある．そのため，本システムおよびシステム評価の要件を以下のようにまとめた．

(1) ボットネットや攻撃サーバ群の構築から，DDoS 攻撃実施まで演習が可能であること
(2) クラウド環境を標的とする DDoS 攻撃の対策演習を実施できること
(3) 本システムを使った場合と座学の場合における学習効果を統計的検定により比較評価すること

本研究では，要件 1 を満たす攻撃演習ネットワークと，要件 2 を満たす対策演習ネットワークを開発し，要件 3 を満たすために評価実験を実施する．また，表 1 の最下部に，本システムの比較を載せる．

表 1　DoS/DDoS 攻撃に関する学習システムの比較
Table 1　Comparison of learning systems for DoS/DDoS attacks.

研究	学習対象	攻撃演習	対策演習	学習効果の評価
立岩ら [13]	DoS を含む種々の攻撃	–	オンプレミス環境での対策を実施	アンケートによる評価
干川ら [9]	DoS/DDoS	HTTP Get Flood スクリプトを記述，実行	–	システム利用の有無での試験結果を比較
Fuertes ら [10]	DDoS	あらかじめ準備されてるツールを実行	オンプレミス環境での対策を実施	アンケートによる評価
Kwon ら [11]	DDoS（脆弱性型）を含む種々の攻撃	あらかじめ準備されてるスクリプトを実行	オンプレミス環境での対策を実施	–
八代ら [12]	DDoS（脆弱性型）を含む種々の攻撃	あらかじめ準備されてるツールを実行	–	システム利用の前後の試験結果を比較
本システム	DDoS	攻撃サーバ，ボットネット構築を含めて実施	クラウド環境（AWS）での対策を実施	システム利用の有無，前後での試験結果を分散分析

4.　システム概要

本章では，本研究で開発したシステムの概要を述べる．本システムでは，多くの被害を発生させ，DDoS 攻撃の高度化の要因となっているマルウェア Mirai をモデルとした攻撃および対策演習を実施できる．

4.1　システム構成

本システムの構成を**図 1** に示す．本システムでは Amazon Virtual Private Cloud（以下，VPC）を用いて演習環境を構築している．本研究では，1 人の学習者が自身の PC から VPC に接続し，学習を進めることを想定している．

本システムの演習環境は Git リポジトリマネージャーである GitLab，DDoS 攻撃演習の環境を提供する攻撃演習ネットワーク，DDoS 対策演習の環境を提供する対策演習ネットワークから構成される．GitLab は演習で用いるファイルの管理，演習手順をまとめた学習用ページの提供に用いる．なお，学習用ページは演習概要ページ，DDoS 攻撃演習ページ，DDoS 対策演習ページから構成される．また，1 人の学習者が同じネットワークに対して攻撃と対策を同時に施すと，どのような攻撃が行われているか学習者が事前に知っている状態での演習となり現実的な演習でなくなるため，攻撃演習ネットワークと対策演習ネットワークは異なるネットワークとなるように構成している．なお，本システムで提供する攻撃演習ネットワークおよび本システムを使った攻撃演習の詳細については 5 章，対策演習ネットワークおよび対策演習の詳細については 6 章で述べる．

4.2　演習手順

学習者は，まず，自身の PC から VPC 上の GitLab にアクセスし，本演習における利用条件として下記の条件に対する同意を行う．

- 演習で取得した知識をサイバー犯罪に利用しない
- 攻撃手法を学ぶ目的を理解している
- 演習で得た知識を用いて他人に害を与えた場合，電子計算機損壊等業務妨害罪，不正アクセス行為の禁止等に関する法律などの違反の罪に問われることを理解している

すべての条件に同意した場合のみ，本システムは，攻撃演習ネットワークおよび対策演習ネットワークにアクセスできるユーザアカウントである AWS Identity and Access Management（以下，IAM）ユーザアカウントを学習者に提供する．これは，サイバー犯罪者を育成しないことを目的としている．

続いて，学習者は演習概要ページを使って学習を行う．演習概要ページの例を**図 2** に示す．演習概要ページでは，本システムの操作方法，DDoS 攻撃の概要，演習の流れについて学習できる．

演習概要ページによる学習が終わった後，学習者は，GitLab 上の DDoS 攻撃演習ページの手順を確認しながら，発行された IAM ユーザアカウントと攻撃演習ネットワークを使って DDoS 攻撃演習を実施する．その後，学習者は，GitLab 上の DDoS 対策演習ページの手順を確認しながら，対策演習ネットワークを使って DDoS 対策演習を実施する．次章以降でこれらの詳細について述べる．

5.　DDoS 攻撃演習

本章では，本システムの攻撃演習環境の構成と，本システムを使った DDoS 攻撃演習の手順を述べる．

5.1　攻撃演習環境

本システムで DDoS 攻撃演習を行うための攻撃演習ネットワークの構成を**図 3** に示す．本ネットワークの構成は Mirai で使われるネットワークと同等の構成である．Mirai で利用される攻撃サーバ群は複数存在する．攻撃演習ネットワークを構成する機器やサーバ群の役割，概要を**表 2** にまとめる．なお，仮想サーバ内の仮想プライベー

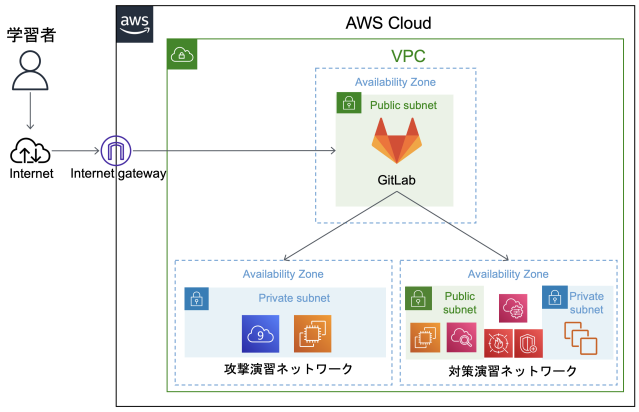

図 1　システム構成図
Fig. 1　Overview of our system.

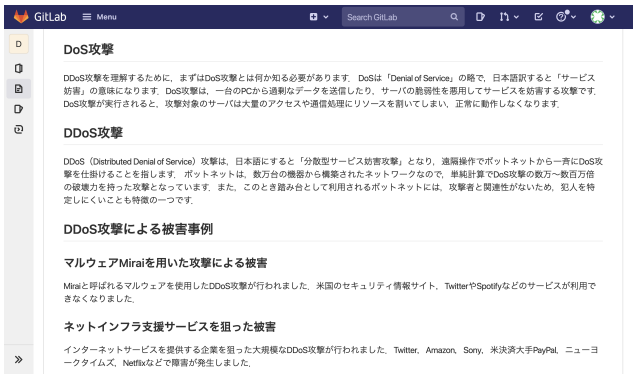

図 2　演習概要ページ（一部抜粋）
Fig. 2　An example of a learning web page.

トネットワーク上に攻撃演習ネットワーク環境を構築することにより，安全に演習を実施できるようにしている．

DDoS 攻撃演習環境の提供には AWS Cloud9 と EC2 を用いる．AWS Cloud9 は AWS で利用可能な統合開発環境であり，コードエディタ，デバッガー，ターミナル等が使用できる．EC2 は AWS に構築できる仮想サーバである．初期状態では，EC2 仮想サーバ内に Docker コンテナを使って Host と Target Server のみが起動している．Host はマルウェアに感染させる機器であり，脆弱なユーザ名とパスワードがあらかじめ設定されている．本システムの初期状態では 1 台の Host が起動しているが，複数台の Host を起動することも可能である．Target Server は，DDoS 攻撃の標的となる Web サーバである．なお，本ネットワークでは仮想サーバ，Host，Target Server の OS としていずれも Ubuntu 18.04.6 LTS を用いた．Mirai で利用される攻撃サーバ群である Command and Control Server（以　下，C2 Server），Download Server，Report Server，Loader および Bot（それぞれの役割は表 2 を参照）は学習者が構築する．具体的な演習手順を次節以降で説明する．

5.2　DDoS 攻撃演習手順

学習者は，自身の PC を使って AWS Cloud9 から EC2 仮想サーバにリモートアクセスし，演習に取り組む．AWS Cloud9 の操作画面の例を**図 4** に示す．画面左でファイル選択，画面右上でコーディング，画面右下でターミナル操作が可能である．学習者は GitLab 上の DDoS 攻撃演習ページの手順を確認しながら，攻撃に利用するマルウェアおよびサーバの構築，ボットネットの構築，Target Server を標的とする DDoS 攻撃の実行演習を実施することによって DDoS 攻撃の仕組みを学習する．以降，5.2.1 節，5.2.2 節，5.2.3 節でそれぞれの演習内容の詳細について説明する．

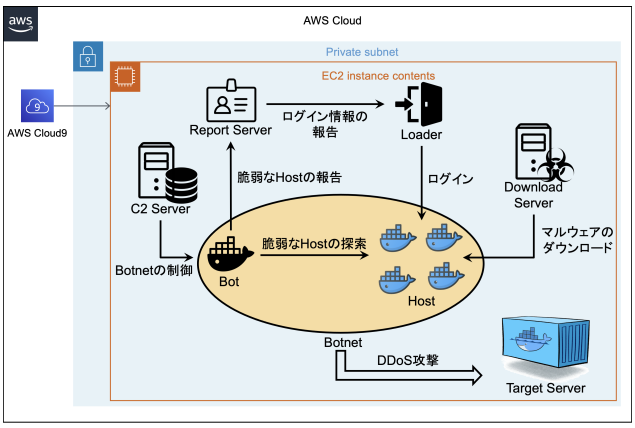

図 3　攻撃演習ネットワークの構成
Fig. 3　Network configuration for DDoS attack.

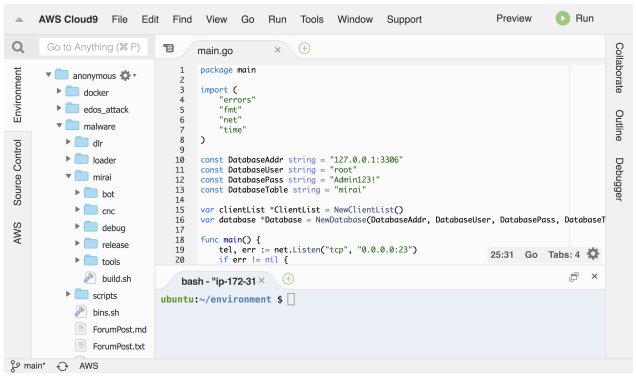

図 4　AWS Cloud9 の操作画面
Fig. 4　An operation screen of AWS Cloud9.

表 2　攻撃演習ネットワーク内の構成要素
Table 2　Modules of network for DDoS attack.

機器	役割	概要
Host	被害側	マルウェアに感染させる機器．本システムでは Docker コンテナで実現．
Target Server	被害側	DDoS 攻撃の標的となる Web サーバ．本システムでは Apache httpd で実現．
C2 Server	攻撃側	マルウェアに感染したボットから構成されるボットネットである Botnet の管理，遠隔操作を行うサーバ．　ボットをリストで管理し DDoS 攻撃の指示を伝達するボット管理機能，C2 Server に攻撃指示を出す DDoS 攻撃指示機能，C2 Server へログインするためのユーザ管理機能を持つ．ログインすると，ボットの台数，登録ユーザの確認，ボットへ攻撃指示を出すことが可能である．
Download Server	攻撃側	脆弱な機器に感染させるマルウェアを管理する Web サーバ．本システムでは Apache httpd で実現．
Report Server	攻撃側	Bot からスキャン機能により発見した脆弱な機器の情報（IP アドレス，ポート番号，ユーザ名，パスワード）を受け取るサーバ．受け取った情報を Loader へ送信する．
Loader	攻撃側	Report Server から受信した情報を元に機器へログインするサーバ．ログイン後に，Download Server で管理されているマルウェアを，機器にダウンロードさせる．マルウェアをダウンロードした機器はボット化する．
Bot	攻撃側	マルウェアに感染しボット化した機器．　感染直後にポートを塞いだりウォッチドッグを排除し他のマルウェアからの感染防御や Bot が活動する阻害要因を削減する防御機能，脆弱なユーザ名とパスワードが設定されている機器を探索するスキャン機能，C2 Server から送信された指示に従って DoS 攻撃を実施する DoS 攻撃機能等を持つ．本システムでは Docker コンテナで実現．

なお，攻撃環境の構築に必要な演習用のマルウェアやサーバプログラム，ファイルとして，公開されている Mirai のソースコードを演習用にカスタマイズしたものが本システムの GitLab に保存されており，演習ではそれを用いる．また，学習者は進捗に応じて，作業途中のプログラムを GitLab へ保存できる．そのため，学習者は演習を中断し，途中から取り組むことが可能である．また，演習の過程でエラーが発生して解決できない場合は，エラーが発生していない段階までプログラムを戻し，再度演習に取り組むことができる．

5.2.1　攻撃に利用するサーバの構築演習

はじめに学習者は C2 Server，Report Server，Loader，Download Server といった攻撃サーバ群を構築する．

まず，学習者は演習環境用に C2 Server プログラムを確認し，修正とコンパイルを行う．その後，C2 Server で利用する MySQL データベースの設定を行う．MySQL データベースはユーザリストや DDoS 攻撃履歴の記録に用いられる．学習者は MySQL データベースにユーザを追加し，さらに C2 Server を起動する．その後，学習者は，自身が追加したユーザを用いて C2 Server へログインできることを確認する．

続いて，学習者は Web サーバである Apache httpd を用いて Download Server を構築する．また，学習者は演習用マルウェア本体のソースコードを確認，修正を施した後コンパイルし，作成した演習用マルウェアを Download Server に格納する．さらに，学習者は Download Server に設置した演習用マルウェアを取得できるかを確認する．

最後に，学習者は Report Server プログラム，Loader プログラムそれぞれを確認，コンパイルし，起動する．

5.2.2　ボットネットの構築演習

続いて学習者は攻撃演習ネットワークにマルウェアに感染した機器である Bot を導入する．Bot は Host と同様の Docker コンテナで実現する．Bot 上で Download Server から演習用マルウェアをダウンロード，手動実行することにより，Bot を感染させる．その後，学習者は C2 Server のコンソール画面から，Bot が C2 Server に接続できているかを確認する．

演習用マルウェアに感染した Bot はスキャン機能により，脆弱なユーザ名とパスワードの設定された機器を探索し，機器へのアクセスを試みる．攻撃演習ネットワークの Host にはあらかじめ脆弱なユーザ名とパスワードが設定されており，本演習では Bot は Host にアクセス可能である．Host へのログインに成功した Bot は，Host のログイン情報を Report Server に送信する．さらに Report Server は Loader に情報を送信，Loader が Host にログインする．最終的に，Download Server から Host に演習用マルウェアがダウンロード，実行されることで，Host がボットとなる．学習者は C2 Server のコンソール画面から，Bot に加えて Host が C2 Server に接続できていることを確認する．また，一連のボットネット構築の流れの確認を行う．

5.2.3　DDoS 攻撃の実行演習

ボットネットの構築が完了すると，学習者はボットネットを使った DDoS 攻撃演習を実施する．攻撃の実施のために，学習者は C2 Server へログインする．C2 Server では 10 種類の DDoS 攻撃コマンドを実行可能である．攻撃コマンドに引数として Target Server の IP アドレス，攻撃の実行秒数を与えたものを C2 Server のコンソール画面に入力すると，C2 Server は設定した DDoS 攻撃をボットネットに指示する．攻撃指示を受け取ったボットネットは，設定された攻撃内容から，Target Server を狙った DDoS 攻撃を行う．学習者は，DDoS 攻撃中に Target Server がダウンし，アクセスできないことを確認する．

6.　DDoS 対策演習

本章では，本システムの対策演習環境の構成と，本システムを利用した DDoS 対策演習の手順を述べる．

6.1　対策演習環境

DDoS 対策演習を行うための対策演習ネットワークの構成を**図 5** に示す．対策演習ネットワークは攻撃演習ネットワークと異なるネットワークであり，DDoS 攻撃を受ける日本の東京リージョンにある機器と DDoS 攻撃を実施する米国バージニア北部リージョンにある機器から構成される．

東京リージョンは学習者が対策演習で操作する環境である．本リージョンには DDoS 攻撃の標的となる Web サーバである Target Server がある．Target Server は日本国内にサービスを展開する Web サーバを想定しており，EC2 仮想サーバを用いて実現している．なお，EC2 仮想サーバの OS は Amazon Linux 2 を使用した．本環境では Amazon CloudWatch，AWS WAF，AWS Shield が利用できる．Amazon CloudWatch は AWS のサービスにおけるトラフィック量や CPU 使用率などのリソースのモニタリン

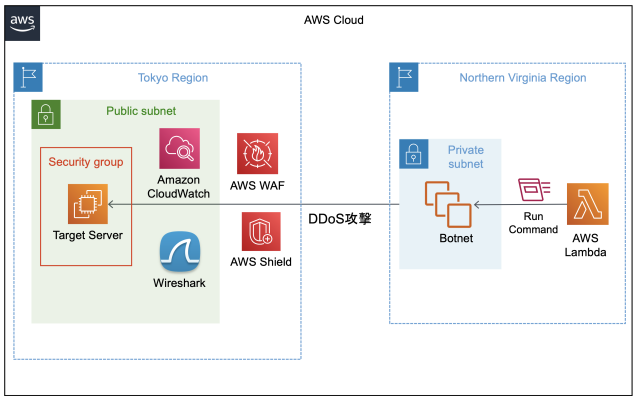

図 5　対策演習ネットワークの構成

Fig. 5　Network configuration for DDoS countermeasure.

グや管理が可能なサービスである．AWS WAF は AWS が提供するウェブアプリケーションファイアウォールであり，主にウェブの脆弱性を利用した攻撃からの保護が可能である．AWS Shield は AWS が提供する DDoS 攻撃対策の専用サービスであり，ネットワークレイヤー，トランスポートレイヤー，アプリケーションレイヤーを狙った DDoS 攻撃の検出と対策を実施できる．対策演習ではこれらのサービスを使って DDoS 対策を行う．

なお，対策演習においては，攻撃の分析のために Target Server に到着するパケットを解析する内容が含まれる．パケットのキャプチャ自体は，Target Server 上，あるいは，Target Server に流れてくるパケットを解析するために別途構築している EC2 仮想サーバ上で行う．一方，パケット解析は学習者の PC にインストールされた GUI プロトコルアナライザ Wireshark を用いて実施する．したがって，学習者は自身の PC に Wireshark をあらかじめインストールしておく必要がある．

バージニア北部リージョンは自動的に DDoS 攻撃を実施する環境である．なお，DDoS 攻撃を実施するボットネットは米国に最も多くあるため [20]，DDoS 実施環境として米国を選定した．本リージョンには Botnet と AWS Lambda がある．Botnet は DDoS 攻撃を実施するボットネットであり，EC2 仮想サーバを用いて実現している．なお，EC2 仮想サーバの OS は Ubuntu 20.04.3 LTS を使用した．AWS Lambda はサーバレスでプログラムを実行できる AWS のサービスである．AWS Lambda は対策演習開始時に SYN flood 攻撃，UDP flood 攻撃，ICMP flood 攻撃，HTTP flood 攻撃のうちいずれかの DDoS 攻撃をランダムに決定し，その攻撃コマンドを Botnet に送信する．なお，2020 年に検出された DDoS 攻撃の 99% がこの 4 種類の攻撃によるものである [21]．Botnet は受け取ったコマンドを元に東京リージョンに構築している Target Server を標的とする DDoS 攻撃を実施する．

6.2　DDoS 対策演習手順

学習者は，主に，自身の PC のブラウザを使って AWS マネジメントコンソールにアクセスし，DDoS 対策演習に取り組む．AWS マネジメントコンソールでは AWS に関するすべての操作が可能である．また，サービスごとに固有のダッシュボードが用意されており，様々な設定や管理を実施できる．

前述のように対策演習開始時点で，東京リージョンにある Target Server に対して，バージニア北部リージョンからランダムな種類の DDoS 攻撃が実施される．学習者は，GitLab 上の DDoS 対策演習ページの手順を確認しながら，AWS マネジメントコンソールを操作し，被害サーバである Target Server における異常の検出，通信内容の解析，攻撃に応じた対策演習を実施することによって DDoS 対策手法を学習する．以降，それぞれの演習内容の詳細について説明する．

6.2.1　DDoS 攻撃の検出演習

はじめに，学習者は，Target Server が提供する Web ページにアクセスを試みる．しかし，Web ページの応答時間が長い，またはアクセスできないことを確認する．その後，AWS マネジメントコンソールから Amazon CloudWatch を選択し，Target Server に送られてくるトラフィック量と Target Server の CPU 使用率を監視する．トラフィック量と CPU 使用率の急激な上昇を確認した場合，Target Server にアクセスが集中して，サーバダウンが発生していると判断する．

続いて，学習者は，DDoS 攻撃であるかどうかを判断するためパケットの解析を行う．学習者は，AWS マネジメントコンソール上で EC2 仮想サーバに SSH 接続する機能である EC2 Instance Connect を用いて，Target Server へリモートアクセスする．DDoS 攻撃の影響で Target Server へリモートアクセスできない場合は，Target Server に流れてくるパケットを解析するために別途構築している EC2 仮想サーバへアクセスする．リモートアクセス後にパケットキャプチャツール tcpdump を実行，通信内容をキャプチャし，結果をダンプファイルに出力する．出力したダンプファイルは GitLab 経由で学習者の PC 上に保存する．さらに，学習者の PC 上でプロトコルアナライザ Wireshark を起動しダンプファイルを読み込ませることでパケット解析を行う．これにより学習者は，GUI を使って，どのような IP アドレスからどのような種類のパケットが送信されているかを知ることができる．その後，学習者は，DDoS 攻撃を受けていると判断し，また，どのような DDoS 攻撃を受けているかを特定する．

6.2.2　DDoS 攻撃の対策演習

DDoS 攻撃の分析の完了後，学習者は，特定した DDoS 攻撃に有効な対策を施す．対策には EC2 仮想サーバのセキュリティグループ，AWS WAF，AWS Shield を用いる．ここで，大規模な DDoS 攻撃を受けた場合，通信事業者によるネットワークレベルでの対策が必要となる場合がある．しかし，本研究では，3 章で示しているようなクラウドサービスを利用する初級学習者を対象としているため，これら AWS が提供するサービスを用いた対策学習を演習内容として選定した．

学習者は AWS マネジメントコンソールから EC2 管理画面を選択し，Target Server のセキュリティグループの設定を確認する．初期状態のセキュリティグループ設定では，Target Server は，すべての送信元 IP アドレスからすべてのトラフィックを受け入れるインバウンドルール設定になっている．たとえば，HTTP flood 攻撃のように送信元 IP アドレスを偽装できない攻撃で，かつ，送信元 IP アドレスが特定少数の場合は，IP アドレスを制限するこ

とによる対策を実施できる．また，UDP flood 攻撃，ICMP flood 攻撃の場合はそれらのプロトコルを禁止する対策を実施できる．学習者はインバウンドルールの修正を行い，特定の IP アドレス，プロトコルからのトラフィックを制限することで DDoS 攻撃の対策を行う．

また，学習者は AWS マネジメントコンソールから AWS WAF を選択し，設定を確認する．AWS WAF は送信元 IP アドレスを偽装できない HTTP flood 攻撃に有効な対策である．本システムの対策演習ネットワークの Target Server は日本国内向けに展開している Web サーバを想定しており，Botnet は米国から攻撃を実施する．そのため，AWS WAF の Web ACLs の設定を確認し，通信を日本国内に限定する設定にすることで，DDoS 攻撃の対策ができる．

上記で対策できない DDoS 攻撃に対して，学習者は，AWS の DDoS 攻撃対策の専用サービスである AWS Shield を利用する．AWS Shield は本システムで実施する SYN flood 攻撃，UDP flood 攻撃，ICMP flood 攻撃，HTTP flood 攻撃のすべてに有効な対策である．学習者は AWS マネジメントコンソールから AWS Shield を選択，東京リージョンの環境に AWS Shield を導入し，Target Server を保護する設定を施す．

以上の対策の結果，Target Server が提供する Web ページの応答時間が短く，正常にアクセスできた場合，対策演習は終了する．学習者が他の種類の DDoS 攻撃に対する対策演習を実施したい場合は，再び，対策演習をはじめから実施する．

7. 評価

実験協力者に本システムを利用してもらい評価を行った．本章では，実験の詳細，結果，考察について述べる．

7.1 学習効果の検証

本システムを利用してクラウド環境を標的とする DDoS 攻撃の対策訓練を実施した場合の学習効果を検証するために，情報工学を専攻する学生 20 名を実験協力者として実験を行った．いずれの実験協力者も，3 章で述べた本システムが想定する対象者に該当する学生である．

実験手順としては，まず，すべての実験協力者に DDoS 攻撃に関する事前テストを受けてもらった．その後，実験協力者を DDoS 攻撃について本システムで学ぶグループ 10 名と座学で学ぶグループ 10 名に分割し，対策学習に取り組んでもらった．座学で学ぶグループのために，本システムで実施した演習内容と同様の学習内容となるよう座学資料を作成した．具体的には，情報処理推進機構の研究報告書 [22] と長柄らの研究報告 [23] をもとに DDoS 攻撃やマルウェア Mirai を学習する資料を作成し，AWS ホワイトペーパー [24] をもとに AWS を用いた DDoS 攻撃の対策手法を学ぶ資料を作成した．両グループともに 1 時間を目安に学習をしてもらった．なお，1 時間より早く学習が終了した場合はその時点で学習を終了してもらった．また，1 時間を超過した場合でも，終了するまで学習に取り組んでもらった．最後に，すべての実験協力者に DDoS 攻撃に関する事後テストを受けてもらった．

事前テストの例を**図 6** に，事後テストの例を**図 7** に示す．事前テスト，事後テストは，AWS ホワイトペーパー [24]，AWS 認定資格試験の模擬試験 [25]，情報処理安全確保支援士試験の過去問 [26] を元に作成した．事前テスト，事後テストともに同レベルの別の問題を用意した．問題数はそれぞれ 10 問であり，1 問 1 点の計 10 点満点で採点した．なお，事前テストの解答を実験協力者に公開しない状態で事後テストを実施した．

実験結果のうち，まず，実験協力者が学習に要した時間について述べる．本システムで学習したグループの平均学習時間は 59.5 分，標準偏差は 11.9 分であった．また，座学で学習したグループの平均学習時間は 50.1 分，標準偏差は 9.7 分であった．いずれのグループも 1 名が目安となる 1 時間の学習時間を超過した．座学と比較して，本システムで学習する場合はハンズオン形式の演習があるため，学習時間に違いが現れたものと考えられる．

第1問　IoT マルウェア Mirai について，もっとも適切なものを 1 つ選べ

(ア)Windows で動作している IoT 機器をボット化させて，遠隔操作するマルウェアである
(イ)ユーザ名とパスワードを初期値のまま利用している機器を対象に感染を広げる
(ウ)主なターゲットは，ネットワークカメラや家庭用ルータといった家庭内のオンライン機器ではない
(エ)脆弱な SSH 接続を利用して機器に感染するマルウェアである

第2問　AWS WAF が有効な攻撃を全て選べ

(ア)HTTP flood 攻撃
(イ)SYN flood 攻撃
(ウ)UDP flood 攻撃
(エ)Slowloris 攻撃

図 6　事前テスト例（一部抜粋）
Fig. 6　An example of pre-test.

第1問　IoT マルウェア Mirai の C2 サーバについて，もっとも適切なものを 1 つ選べ

(ア)C2 サーバの 101 番ポートに SSH 接続してコマンド発行することで，DDoS 攻撃に利用するボットの所在地を確認できる
(イ)DDoS 攻撃に必要なサーバの管理と脆弱な機器がないか探索を行う
(ウ)ボットの台数，登録されているユーザの確認，DDoS 攻撃指示を出すことが可能である
(エ)Bot が 48101 番ポートに Telnet 接続し，発見した脆弱な IoT 機器のログイン情報を受け取ることができる

第2問　AWS Shield Standard が有効な攻撃を全て選べ

(ア)HTTP flood 攻撃
(イ)SYN flood 攻撃
(ウ)UDP flood 攻撃
(エ)ICMP flood 攻撃

図 7　事後テスト例（一部抜粋）
Fig. 7　An example of post-test.

表 3　事前テスト，事後テストの結果
Table 3　Evaluation results.

	事前テスト		事後テスト	
	平均点	標準偏差	平均点	標準偏差
本システム	2.90	1.10	7.00	1.89
座学	3.20	1.03	5.00	1.05

続いて，事前テスト，事後テストの結果を**表 3** に示す．本システムで学習したグループは平均点が 4.1 点上昇し，座学で学習したグループの平均上昇点 1.8 点と比較して高い結果となった．座学のグループでは教材を熟読する学習だけに取り組んでもらったのに対して，本システムのグループでは，事前学習ページを読んだ後に実際に手を動かす演習に取り組んでもらった．このようなハンズオン形式で学習することで，知識の定着度に差が生じ，結果として平均点の上昇率に現れたものと考えられる．

加えて，統計学的な有意性を確認するために，実験協力者のテスト結果に関する 2 要因混合計画の分散分析（参加者間要因：学習者［本システム，座学］×参加者内要因：テスト［事前テスト，事後テスト］）を実施した．ここで，分散分析では検定統計量として F 値が用いられる．以降の結果の記述では，分散分析で用いられる表記にならって，分散分析により得られた F 値およびそのときの p 値の範囲を表記する．また，自由度をカッコ内に表記する．なお，有意でない場合を ns（nonsignificant）と表記する．

分散分析の結果，相互作用は有意（$F(1, 18)=8.43$, $p<0.01$）であった．相互作用が有意であったため，各要因における単純主効果を検証したところ，本システムで学習した参加者内要因の単純主効果（$F(1, 9)=37.0$, $p<0.001$），座学で学習した参加者内要因の単純主効果（$F(1, 9)=18.7$, $p<0.005$）のいずれもが認められた．したがって，本システムと座学のいずれも学習に有効であるといえる．また，事前テストにおける参加者間要因の単純主効果（$F(1, 18)=0.395$, ns）は認められなかったが，事後テストにおける参加者間要因の単純主効果（$F(1, 18)=8.57$, $p<0.01$）が認められた．このことから，座学より本システムを利用した参加者の方が有意に事後テストの点数が高いことが分かる．これらの結果から，本システムを用いた学習が座学と比較してクラウド環境を標的とする DDoS 攻撃の対策学習に有効であることを確認できた．

7.2　利用評価アンケート

本システムの有用性の確認を目的に，前節の実験で本システムを利用した学生 10 名を対象として，利用評価アンケートに回答してもらった．アンケートは，1 が最も悪く，5 が最も良いとした 5 段階評価とした．また，自由記述欄を設けており，任意でコメントを記入してもらった．

評価項目と，各項目に対する平均評点，標準偏差を**表 4** に示す．すべての項目で良好な結果を得ることができた．また，標準偏差から，各項目の評点のばらつきは小さく，安定して高い評価だったことが分かる．

表 4　利用評価アンケートの結果
Table 4　Questionnaire results.

評価項目	平均	標準偏差
AWS の説明は理解できたか	4.4	0.49
演習の流れは理解できたか	4.9	0.30
演習の流れは適切だったか	4.4	0.66
演習の難易度は適切だったか	4.4	0.66
システムの操作方法は理解できたか	4.5	0.67
DDoS 攻撃の検出手法は理解できたか	4.4	0.66
DDoS 攻撃の対策手法は理解できたか	4.5	0.50
DDoS 攻撃の原理は理解できたか	4.7	0.46
セキュリティへの関心は高まったか	4.3	0.78
演習を通して，DDoS 攻撃の対策には攻撃視点も必要だと感じたか	4.2	0.87

自由記述欄では，「初めてでもつまずくことなく取り組むことができた」とコメントをもらった．また，表 4 に示すように，演習の難易度や手法の理解に関連した評価項目はいずれも高い評価であった．今回の実験で本システムを利用したすべての学習者は，行き詰まることなくスムーズに演習を実施できた．特に，6.2.1 節で示した DDoS 攻撃の検出演習において攻撃の種類を当てなければ適切な対策を施せないが，いずれの学習者も一度の解析で攻撃の種類を正しく特定し，適切な対策を施すことができた．そのため，3 章で提示した本研究で想定している学習者のレベルに合わせた演習コンテンツを用意できたと考えられる．

その他の自由記述欄のコメントとして，「本システムを用いた演習が楽しかった」，「攻撃方法について，何となくでしか理解できていなかったが，実際に手を動かすことで理解できた」，「DDoS 対策演習の最後で，Target Server の Web ページへアクセスできるようになり，適切に対策できたことが分かりやすかった」，「パケットキャプチャし，そのキャプチャファイルを解析して攻撃を特定する部分が面白かった」，「サイバーセキュリティの研究に興味を持った」，「Wireshark をほどんど使ったことがなかったので，Wireshark 自体の見方等を載せてくれるとより分かりやすかった」などの意見が得られた．また，「攻撃視点もあわせて学習することで，対策視点を学習する際に，理解が深まりやすかった」とコメントをもらった．さらに，アンケートの評価項目「演習を通して，DDoS 攻撃の対策には攻撃視点も必要だと感じたか」において，平均評点が 4.2 点であった．そのため，攻撃視点を取り入れた学習は，複雑な攻撃に対応できるようになるだけでなく，対策演習の理解促進にもつながると考えられる．これらの結果から，本システムの有用性を確認できた．

8. おわりに

本研究では，クラウド環境を標的とするDDoS攻撃の対策演習を実施できる環境の提供を目的として，攻撃視点を取り入れたDDoS攻撃の対策訓練システムを開発した．開発システムは，IaaSで最も採用されているAWSを用いたDDoS攻撃の対策訓練が可能である．さらに，座学で学ぶ学習者と本システムを使って学ぶ学習者に対して事前テスト，事後テストを実施し，システムの有効性を検証した．分散分析の結果，本システムを利用した学習者のほうが，座学で学ぶ学習者と比較して有意に事後テストの点数が高いことを確認した．本システムによる演習を通して，攻撃視点と対策視点から，DDoS攻撃の対策手法に関する理解と知識の定着が期待できる．

一方，本研究における評価は学生を対象とした分析にとどまっており，企業における初級学習者など，本システムで想定している他の利用対象者に対する評価も必要である．また，サービス妨害攻撃には，本研究で対象としたボットネットを利用したDDoS攻撃の他にも，EDoS（Economic Denial of Service）攻撃やDRDoS（Distributed Reflection Denial of Service）攻撃などの攻撃があり，今後，これらの攻撃の学習への対応を検討している．さらに，IaaSとして採用されているメガクラウドのうちAWSは全体の6割を占めているが，残りのメガクラウドであるAzureとGoogle Cloud Platformを用いた演習システムの追加実装を検討している．

謝辞　本研究はJSPS科研費21K12185の助成を受けたものである．

参考文献

[1] 眞鍋　督，井口信和：クラウド環境を標的とするDDoS攻撃の対策演習システムの開発と評価，情報処理学会インターネットと運用技術シンポジウム2022論文集（2022）．

[2] 総務省：令和3年通信利用動向調査の結果（2022）．〈https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf〉（参照2022-11-15）．

[3] 株式会社MM総研：国内クラウドサービス需要動向調査（2021年度版）（2021）．〈https://www.m2ri.jp/release/detail.html?id=500〉（参照2022-11-15）．

[4] NETSCOUT: 14th Annual Worldwide Infrastructure Security Report.〈https://www.netscout.com/report/〉（参照2022-11-15）．

[5] Ponemon Institute: The State of DDoS Attacks against Communication Service Providers (2019).〈https://www.a10networks.com/wp-content/ uploads/A10-EB-14117-EN.pdf〉（参照2022-11-15）．

[6] 総務省：我が国のサイバーセキュリティ人材の現状について（2018）．〈https://www.soumu.go.jp/main_content/000591470.pdf〉（参照2022-11-15）．

[7] 齋藤　衛：IIJ Technical WEEK 2016セキュリティ動向2016〜ランサムウェアとMirai botについて〜（2016）．〈https://www.iij.ad.jp/dev/tech/techweek/pdf/161111_01.pdf〉（参照2022-11-15）．

[8] Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K. and Zhou, Y.: Understanding the Mirai Botnet, *Proceedings of USENIX Security 2017*, pp.1093–1110 (2017).

[9] 千川尚人，小林康浩，石原　学，白木厚司，下馬場朋禄，伊藤智義：サービス拒否攻撃演習システムの実装とそのアクティブラーニングシナリオによるセキュリティ技術教育，電子情報通信学会論文誌，Vol.J103-B, No.4, pp.180–183（2020）．

[10] Fuertes, W., Tunala, A., Moncayo, R., Meneses, F. and Toulkeridis, T.: Software-Based Platform for Education and Training of DDoS Attacks Using Virtual Networks, *Proceedings of ICSSA 2017*, pp.94–99 (2017).

[11] Kwon, M. J., Kwak, G., Jun, S., Kim, H.-J. and Lee, H. Y.: Enriching Security Education Hands-on Labs with Practical Exercises, *Proceedings of ICSSA 2017*, pp.100–103 (2017).

[12] 八代　哲，田邊一寿，齋藤祐太，齋藤孝道：体験型サイバーセキュリティ学習システムの提案と再評価，情報処理学会マルチメディア分散協調とモバイルシンポジウム2018論文集，pp.1809–1816（2018）．

[13] 立岩祐一郎，岩崎智弘，安田考美：仮想マシンネットワークによる継続的なクラッキング防衛演習システム，電子情報通信学会論文誌，Vol.J96-D, No.7, pp.1585–1594（2013）．

[14] 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，Vol.J103-D, No.8, pp.591–602（2020）．

[15] Hu, J., Meinel, C. and Schmitt, M.: Tele-lab IT security: an architecture for interactive lessons for security education, *Proceedings of ACM SIGCSE 2004*, pp.412–416 (2004).

[16] 竹下数明，小林偉昭，佐々木良一：脆弱性対策教育のためのeラーニングシステムの開発と評価，コンピュータセキュリティシンポジウム2009論文集，pp.1–6（2009）．

[17] 岸本和理，谷口義明，井口信和：攻撃者視点を取り入れたクロスサイトスクリプティング対策の実践的演習システムの開発と評価，情報処理学会論文誌：教育とコンピュータ，Vol.8, No.2, pp.76–81（2022）．

[18] AWS: AWS Security Essentials.〈https://aws.amazon.com/jp/training/classroom/aws-security-essentials/〉（参照2022-11-15）．

[19] AWS: Security Engineering on AWS.〈https://aws.amazon.com/jp/training/classroom/security-engineering-on-aws/〉（参照2022-11-15）．

[20] Cloudflare：2022年第2四半期におけるDDoS攻撃の傾向（2022）．〈https://blog.cloudflare.com/ja-jp/ddos-attack-trends-for-2022-q2-ja-jp/〉（参照2022-11-15）．

[21] Kaspersky: DDoS attacks in Q2 2020 (2020).〈https://securelist.com/ddos-attacks-in-q2-2020/〉（参照2022-11-15）．

[22] 独立行政法人情報処理推進機構セキュリティセンター：サービス妨害攻撃の対策等調査–報告書–.〈https://www.ipa.go.jp/files/000024437.pdf〉（参照2022-11-15）．

[23] 長柄啓悟，松原　豊，青木克憲，高田広章：組込みシステム向けマルウェアMiraiの攻撃性能評価，情報処理学会研究報告，Vol.2017-ARC-225, No.41, pp.1–6（2017）．

[24] Amazon Web Service: AWSホワイトペーパーとガイド. https://aws.amazon.com/jp/whitepapers/（参照2022-11-15）．

[25] Amazon Web Service: AWS Skill Builder.〈https://explore.skillbuilder.aws/learn〉（参照2022-11-15）．

[26]　独立行政法人情報処理推進機構：過去問題（問題冊子・配点割合・解答例・採点講評）.〈https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_mondai.html〉（参　照 2022-11-15）.

眞鍋 督（学生会員）

2021 年近畿大学理工学部卒業．同年同大学大学院総合理工学研究科博士前期課程入学，現在に至る．サイバーセキュリティの教育に関する研究に従事．

谷口 義明（正会員）

2008 年大阪大学大学院情報科学研究科博士後期課程修了，博士（情報科学）．大阪大学サイバーメディアセンター，近畿大学理工学部を経て，2022 年より同大学情報学部准教授．情報ネットワーク，サイバーセキュリティ分野の研究に従事．IEEE，情報処理学会，電子情報通信学会，電気学会各会員．

井口 信和（正会員）

1988 年三重大学大学院修士課程修了．同年（株）豊田自動織機製作所入社．1992 年和歌山県工業技術センター研究員．2001 年大阪大学大学院基礎工学研究科博士後期課程修了，博士（工学）．2002 年近畿大学理工学部助教授．2008 年同大学教授．2015 年近畿大学総合情報基盤センター長を兼務．2020 年近畿大学情報学研究所長代理を兼務．2022 年より同大学情報学部教授．ネットワーク運用管理支援，情報ネットワーク応用，教育システム開発に関する研究に従事．情報処理学会，電子情報通信学会，IEEE，教育システム情報学会，農業情報学会各会員．