# 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

眞鍋 督[1,a)]　井口 信和[2,3,b)]

**概要**：本研究では，クラウド環境を標的とする DDoS 攻撃の対策訓練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 攻撃の対策演習システムを開発した．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，Infrastructure as a Service で最も採用されている Amazon Web Service を用いた DDoS 攻撃の対策訓練が可能である．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．本稿では，本システムの開発と評価について述べる．

**キーワード**：クラウド環境，DDoS 攻撃，対策演習，セキュリティ

# Development and Evaluation of a Countermeasure Exercise System for DDoS Attacks Targeting Cloud Environments

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

***Abstract:*** In this study, we developed a DDoS attack countermeasure exercise system that incorporates an attack perspective in order to provide an environment in which countermeasure training for DDoS attacks targeting cloud environments can be conducted. Learners can engage in both attack and countermeasure exercises by themselves. The system also enables learners to practice countermeasures against DDoS attacks using Amazon Web Service, the most popular Infrastructure as a Service. Through the exercises using this system, users can expect to gain a better understanding and knowledge of DDoS attack countermeasures from both attack and countermeasure perspectives. This paper describes the development and evaluation of the system.

***Keywords:*** Cloud environment, DDoS attacks, Exercises for countermeasures, Security

## 1. はじめに

企業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 [1]．クラウドサービスにおける利用形態の一つに，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）が最も高いことが確認されている [2]．

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 攻撃が増加している．DDoS 攻撃は，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，サーバに大量のパケットを送信し，サービスを妨害する攻撃である．NETSCOUT が公表した世界のセキュリティレポート [3] によると，クラウド環境を標的と

[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
[2] 近畿大学情報学部
Faculty of Informatics, Kindai University
[3] 近畿大学情報学研究所
Cyber Informatics Research Institute, Kindai University
[a)] manabe0123m@gmail.com
[b)] iguchi@info.kindai.ac.jp

する DDoS 攻撃は，1 年間で 3 倍に増加している．しかし，「DDoS 攻撃を緩和するための適切な対策を講じている」と回答した事業者は，29%であった [4]．原因の一つに，セキュリティ技術者の不足が挙げられる [5]．この問題の解決には，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．

DDoS 攻撃は種類が多様化し，年々複雑さも増している [3]．また，IoT マルウェアである Mirai の登場により，DDoS 攻撃の規模も大きくなっている．Mirai は，Linux で動作する IoT 機器をボットに感染させて，DDoS 攻撃を実行させるマルウェアである．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確認され，DDoS 攻撃の高度化が懸念されている [6]．そのため，従来の対策視点のみの学習では，DDoS 攻撃の防御が難しくなっている．湯川らの研究 [7] では，改善策の一つに，従来の対策を施す視点だけでなく，攻撃視点から攻撃手法を学習し，対策に活かすことを提案している．また，実験結果から，この改善策の有効性が示されている．

そこで本研究では，攻撃視点を取り入れた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 攻撃の対策演習システム（以下，本システム）を開発した．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．本システムでは，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．また，亜種のマルウェアが多く出現している Mirai をモデルとした攻撃演習を実施する．これにより，従来のセキュリティ対策では防ぐことが難しい DDoS 攻撃にも対応可能なセキュリティ技術者の養成が可能である．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．

## 2. 関連研究

サイバー攻撃の学習システムに関する研究は，いくつか実施されている [8], [9], [10]．立岩らの研究 [8] 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，対策手法を学習できる環境を提供する．また，Hu らの研究 [9] では，ネットワークセキュリティツールの使用方法を学習できる演習環境 Telelab を提供している．このシステムを利用する際，学習者は遠隔地から VNC アプレットを用いて，演習環境にアクセスする．アクセスが完了したら，演習環境サーバ上で稼働している仮想マシン群を利用し，暗号化，認証，セキュリティスキャンなどの演習を実施する．しかし，これらのシステムでは，いずれも対策手法のみ学習可能である．これに対して，本システムでは，複雑な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，攻撃手法も学習できる．

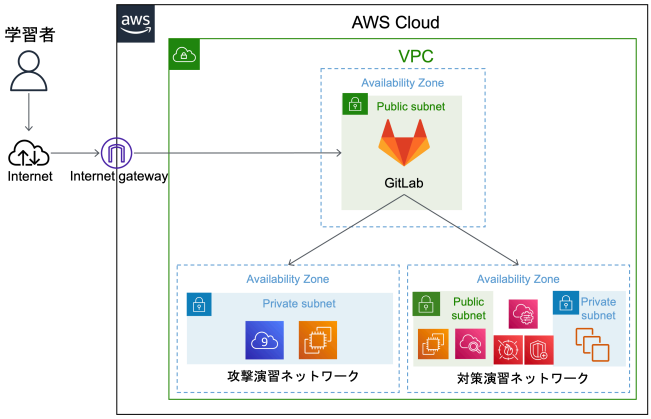


図 1　システム構成図

Walden の研究 [11] では，セキュリティの概念と技術を学習することを目的に，仮想化技術を用いたセキュリティ演習環境を開発している．このシステムでは，攻撃視点と対策視点から演習可能である．しかし，演習時に使用するセキュリティツールは，安全性を判別した上で，学習者が入手する必要がある．そのため，中級者以上のセキュリティに関する知識を有した学習者が対象である．これに対して，本システムでは，セキュリティに関する知識が不足している初学者を対象としている．

2 人 1 組で実施するセキュリティ演習システムは，いくつか提案されている [7], [12]．八代らの研究 [12] では，IT 企業及びユーザ企業でのインシデントレスポンスにおける学習機会の提供を目的に，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 組で，システムから提供されるコンテンツを参照しながら演習に取り組む．クラウド上の接続用仮想 PC に RDP 接続し，あらかじめ準備されたシナリオに基づいてセキュリティ学習を進める．このシステムでは，DDoS 攻撃の分析演習と攻撃演習が実施できる．一方，本システムでは，自動攻撃機能を有しているため，学習者は 1 人で演習に取り組むことが可能である．さらに，DDoS 攻撃の分析と攻撃に関する演習に加えて，検知と対策に関する演習も実施できる．

サイバー攻撃は，オンプレミス環境からクラウド環境に攻撃対象が変化している．しかし，これまで紹介した関連研究 [7], [8], [9], [10], [11], [12] 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は実施できない．さらに，DDoS 攻撃の攻撃演習と対策演習の両方が可能なシステムは開発していない．これに対して，本研究では，現状の問題を解決するために，攻撃視点を取り入れたクラウド環境を標的とする DDoS 攻撃の対策演習システムを開発した．

## 3. 開発内容

本システムの構成を図 **1** に示す．本システムでは，Ama-

zon Virtual Private Cloud（以下，VPC）を用いて，仮想ネットワークを構築している．さらに，Amazon Elastic Compute Cloud（以下，EC2），AWS Cloud9，Amazon CloudWacth，AWS WAF，AWS Shield などを利用し，VPC 上に演習環境を提供する．演習環境には，GitLab，攻撃演習ネットワーク，対策演習ネットワークがある．GitLab は，独自に構築できる Git リポジトリマネージャーである．攻撃演習ネットワークは，DDoS 攻撃演習の環境を提供し，対策演習ネットワークは，DDoS 対策演習の環境を提供する．3.1 節で GitLab の詳細，3.2 節で攻撃演習ネットワークの構成，3.3 節で対策演習ネットワークの構成について述べる．

### 3.1 GitLab

GitLab は，演習で用いるソースコードを管理する．ソースコード管理は，主に攻撃演習で実施する．攻撃演習では，学習者が攻撃ツールを開発し，DDoS 攻撃を実行する．その際に，開発のベースとなるソースコードを攻撃演習環境へクローンする．また，学習者それぞれの進捗に合わせて，開発途中のプログラムを GitLab に保存する．そのため，学習者は演習を中断でき，途中から取り組むことが可能である．開発の過程でエラーが発生した場合でも，エラーが発生していない段階までソースコードを瞬時に戻し，再度演習に取り組むことができる．

演習で分析するダンプファイルの管理も実施する．このファイル管理は対策演習で行う．対策演習では，攻撃の分析をするために，tcpdump を用いて通信内容をダンプファイルに出力する．出力したファイルは，Wireshark に読み込ませてパケットの中身を解析することで，どのような攻撃を受けているか分析する．その際に利用するダンプファイルを GitLab で管理している．

演習で必要な事前知識を学習する教材として，事前学習ページを提供する．事前学習ページの一部を図 **2** に示す．事前学習ページは，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．演習概要ページでは，本システムの操作方法，DDoS 攻撃の基礎知識，演習の流れについて学習できる．DDoS 攻撃演習ページでは，DDoS 攻撃演習で必要な知識を学ぶことが可能である．また，DDoS 対策演習ページでは，DDoS 対策演習で必要な知識を学ぶことができる．

AWS Identity and Access Management（以下，IAM）ユーザを学習者に提供する．IAM ユーザとは，AWS にアクセスするために用いられるユーザアカウントである．学習者は，この機能を利用することで，攻撃演習ネットワーク，対策演習ネットワークにアクセスする．

本演習における利用条件と，それに対して同意するか確認する機能を持つ．全条件の同意が確認できた場合のみ，本システムにアクセスできるユーザアカウントを学習者に

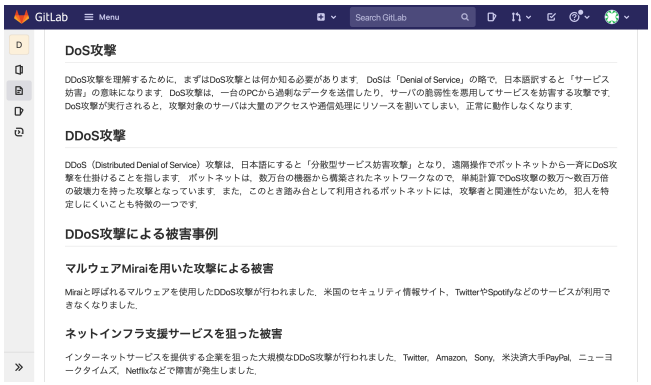


図 **2** 事前学習ページの一部

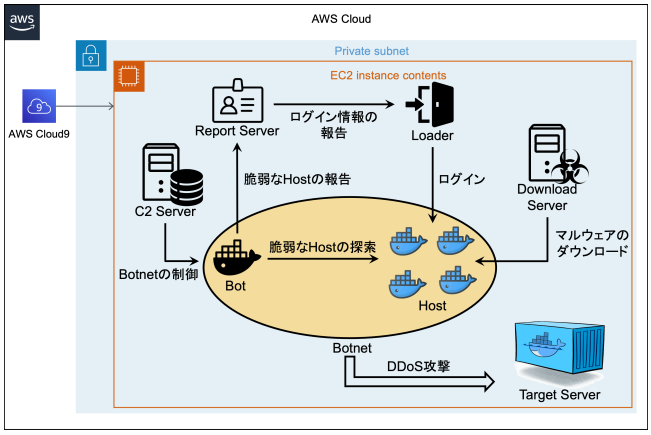


図 **3** 攻撃演習ネットワークの構成

提供する．これは，本システムにより，サイバー犯罪者を育成しないことを目的としている．提示する利用条件は，以下の通りである．

- 演習で得た知識をサイバー犯罪に扱わない
- 攻撃手法を学ぶ目的を理解している
- 攻撃演習で得た知識を用いて，他人に害を与えた場合，法律により罰せられることを理解している

### 3.2 攻撃演習ネットワーク

攻撃演習ネットワークの構成を図 **3** に示す．本ネットワークは，プライベートサブネット上に構築している．これにより，演習で用いるマルウェアが外部に流出する可能性を排除している．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る．コードエディタ，デバッガー，ターミナルが使用できる．EC2 には，Docker コンテナを用いて，Host と Target Server 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設定されている．Target Server は，DDoS 攻撃の対象となるサーバである．EC2 内では，DDoS 攻撃に用いるサーバと Botnet の構築，DDoS 攻撃の実行が可能である．構築できるサーバは，Command and Control Server（以下，C2 Server），Bot，Report Server，Loader，

Download Server である．各サーバにおける役割について，以下に示す．

C2 Server は，Botnet を管理・操作するサーバである．C2 Server には，ボット管理機能，DDoS 攻撃指示機能，ユーザ管理機能がある．ボット管理機能は，ボットをリストで管理し，DDoS 攻撃の指示をバッファーによって伝達する機能である．DDoS 攻撃指示機能は，C2 Server の 101 番ポートに Telnet 接続し，攻撃コマンドを入力して攻撃指示を出す機能である．ユーザ管理機能は，登録されたユーザが，23 番ポートに Telnet 接続し，ユーザ名とパスワードを入力することで，C2 Server へログインできる機能である．ログインが完了すると，コマンドを用いて，ボットの台数と登録されているユーザの確認，DDoS 攻撃指示機能と同様に攻撃の指示を出すことが可能である．

Bot は，マルウェアに感染し，ボット化した仮想機器である．この仮想機器は，Docker コンテナを用いて再現している．Bot には，防御機能，スキャン機能，DoS 攻撃機能がある．防御機能は，ボットに感染した直後にポートを塞いで，他のマルウェアからの感染を防ぐ．また，Linux のウォッチドッグを排除し，Bot が活動する阻害要因を削減する．スキャン機能は，脆弱なユーザ名とパスワードが設定されている Host を探索する．DoS 攻撃機能は，C2 Server から送信された指示に従って，DoS 攻撃を実施する機能である．

Report Server は，Bot から不正アクセスできる Host の情報を受け取る．Bot から報告される情報は，IP アドレス，ポート番号，ユーザ名，パスワードである．その後，Report Server が，受け取った情報を Loader へ送信する．

Loader は，Report Server から送信された情報を元に，Host へログインする．ログイン後には，Download Server からマルウェアをダウンロードさせる．マルウェアをダウンロードした Host は，ボットに感染し，あらかじめ構築している Bot と同様の機能を持つ．このようにマルウェアの感染を広げることで，ボットから構成されるネットワークである Botnet を構築する．

Download Server は，脆弱な Host に配布するマルウェアを管理する．Loader が脆弱な Host に侵入し，ダウンロードコマンドを発行することで，マルウェアの散布が可能である．

### 3.3 対策演習ネットワーク

対策演習ネットワークの構成を図 4 に示す．DDoS 攻撃を受ける日本の東京リージョンと，DDoS 攻撃を実施する米国のバージニア北部リージョンから構成される．それぞれのリージョンの説明について，以下に示す．

東京リージョンには，Target Server，Amazon CloudWatch，Wireshark，AWS WAF，AWS Shield がある．Target Server は，様々な脆弱性を含んでおり，DDoS 攻撃の対象となるサーバである．日本国内にサービスを展開する Web サーバを想定し，EC2 を用いて構築している．Amazon CloudWatch は，AWS のサービスに関するリソースのモニタリングや管理が可能である．この機能を用いて，送られてくるトラフィック量や Target Server の CPU 使用率を監視する．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る．様々なセキュリティルールを作成でき，ウェブの脆弱性を利用した DDoS 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る．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 攻撃の検出と緩和が可能である．

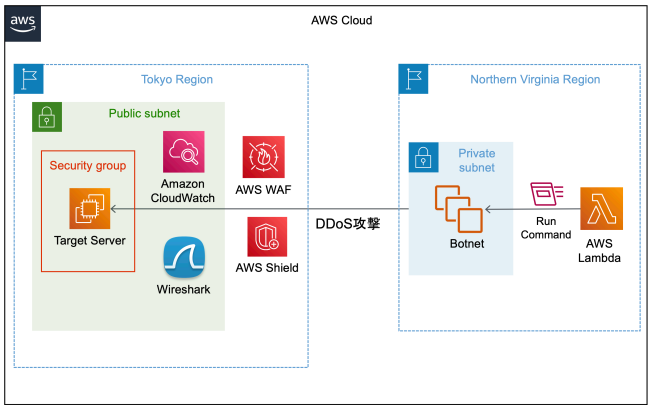


図 4　対策演習ネットワークの構成

バージニア北部リージョンには，AWS Lambda と Botnet がある．IP アドレスを偽装できない DDoS 攻撃の攻撃元は，米国が最も多いことが確認されている [13]．このことから，実際の DDoS 攻撃に近い現象を再現するために，攻撃環境は米国に構築している．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．この機能を用いて，DDoS 攻撃をランダムに決定し，攻撃コマンドを Botnet に発行する．Botnet は，DDoS 攻撃を実施するボットネットであり，EC2 を用いて再現している．AWS Lambda から発行されたコマンドを元に，Botnet が東京リージョンにある Target Server を標的とする DDoS 攻撃を実施する．

## 4. DDoS 攻撃演習

DDoS 攻撃演習は，攻撃演習ネットワークで実施する．多くの被害を発生させているマルウェア Mirai をモデルとした演習を行う．学習者は，AWS Cloud9 から EC2 にリモートアクセスして演習に取り組む．本演習では，主に AWS Cloud9 を扱うことで，攻撃手法を学習する．AWS Cloud9 の操作画面を図 5 に示す．画面左側でファイル選択，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．攻撃演習の流れとして，攻撃に利用するサーバと Botnet の構築後に，Target Server を標的とする

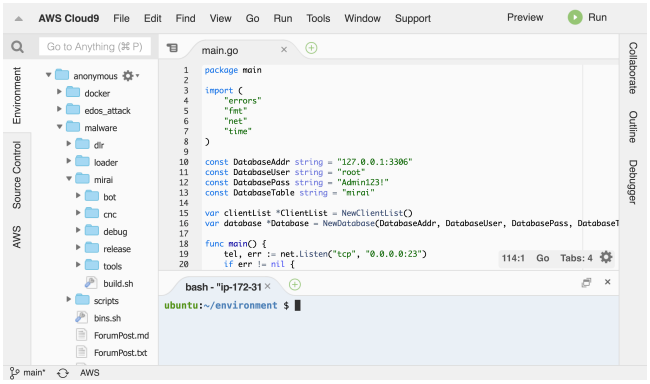


図 5　AWS Cloud9 の操作画面

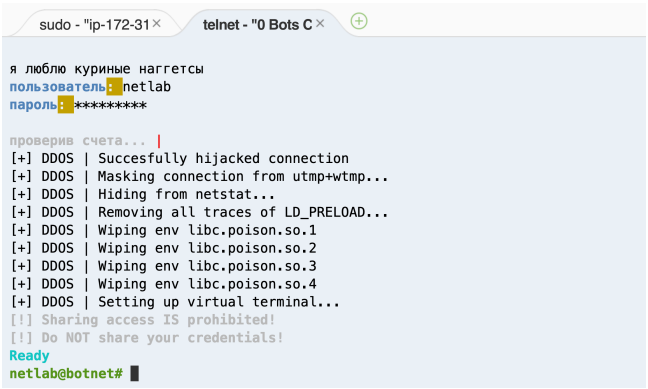


図 6　C2 Server のコンソール画面

DDoS 攻撃を実施する．これらの演習を通して，DDoS 攻撃の仕組みについて学習することが可能である．4.1 節で攻撃に利用するサーバの構築，4.2 節で Botnet の構築，4.3 節で DDoS 攻撃の実施について述べる．

### 4.1　攻撃に利用するサーバの構築

はじめに，学習者は，C2 Server，Bot，Report Server，Loader，Download Server を構築する．各サーバの具体的な構築演習の内容を以下に示す．

C2 Server は，Go 言語と MySQL を用いて構築する．Go 言語は，ユーザのログインやボットに接続するための Telnet サーバと API サーバを立てる際に利用する．MySQL は，ユーザリストや攻撃履歴の記録に用いる．ユーザリストには，C2 Server にアクセスするために必要な ID やパスワードが管理されている．攻撃履歴には，ユーザの ID，攻撃開始時間，攻撃の実行秒数，攻撃に使用したボットの数などが記録されている．構築が完了したら，学習者が作成した ID とパスワードを用いて，C2 Server へログインする．その後，ボット管理機能，DDoS 攻撃指示機能，ユーザ管理機能が正常に動作しているか確認する．

Bot は，まずはじめに，マルウェアを Docker コンテナに格納する．その後，格納したマルウェアを実行することで構築する．構築が完了したら，Bot が C2 Server に接続できているか確認する．また，防御機能，スキャン機能，DoS 攻撃機能が正常に動作しているか確認する．

Download Server は，まずはじめに，Apache を用いて Web サーバを立ち上げる．その後，マルウェアを Web サーバに格納することで構築する．構築が完了したら，ダウンロードコマンドを発行し，マルウェアを取得できるか動作確認する．

Report Server は Go 言語，Loader は C 言語を用いて構築する．構築が完了したら，Report Server が，Bot から脆弱な Host のログイン情報を受け取り，Loader に送信できているか確認する．また，Loader が，Report Server から送信されたログイン情報を元に，Host へ侵入できるか確認する．

### 4.2　Botnet の構築

攻撃に利用するサーバの構築が完了したら，Host をボットに感染させる．Host は，あらかじめユーザ名とパスワードが脆弱な設定になっている．そのため，Bot のスキャン機能を用いて，脆弱なユーザ名とパスワードの組み合わせを試し，不正アクセスできる Host を探索する．脆弱なユーザ名とパスワードは，「root と admin」，「root と 123456」，「root と（未設定のパスワード）」，「admin と password」など全 61 種類の組み合わせから，Bot がスキャンを行う．脆弱な Host を発見した場合，Bot は Host のログイン情報を Report Server に送信する．その後，Loader がログインし，Download Server から Host にマルウェアをダウンロードすることで，ボットに感染させる．以上の流れで，ボットの感染を広げて，Botnet を構築する．

### 4.3　DDoS 攻撃の実施

Botnet の構築が完了すると，学習者は C2 Server へログインする．C2 Server のコンソール画面を**図 6** に示す．ID とパスワードを入力し，ログインした直後の画面である．ログイン後に，C2 Server から Botnet を遠隔操作して，Target Server を標的とする DDoS 攻撃を実施する．実施できる DDoS 攻撃の種類を**表 1** に示す．本演習では，10 種類の DDoS 攻撃を実行可能である．「攻撃コマンド　Target Server の IP アドレス　攻撃の実行秒数」を C2 Server のコンソール画面に入力して，設定した攻撃内容を Botnet に送信する．Botnet が DDoS 攻撃を実施し，Target Server にサーバーダウン発生させて，アクセスできないことを確認した場合，攻撃演習は終了する．

## 5.　DDoS 対策演習

DDoS 対策演習は，対策演習ネットワークで実施する．はじめに，AWS Lambda が，DDoS 攻撃の種類をランダムに決定する．決定する攻撃の種類と概要を**表 2** に示す．2020 年に検出された DDoS 攻撃の種類 [14] の 99 %を，対策演習で学習できる．AWS Lambda は，確定した攻撃に対応するデータを Botnet へ送信する．送信されたデータ

表 1　実施できる攻撃の種類

| 種類 | 攻撃コマンド | 概要 |
|---|---|---|
| HTTP flood | http | HTTP リクエストを大量に送信 |
| UDP-PLAIN flood | udpplain | 高速化のために最適化した UDP パケットを大量に送信 |
| UDP flood | udp | UDP パケットを大量に送信 |
| ACK flood | ack | ACK パケットを大量に送信 |
| SYN flood | syn | SYN パケットを大量に送信 |
| GRE-IP flood | greip | GRE プロトコルによるパケットを大量に送信 |
| ACK-STOMP flood | stomp | TCP セッション確立後に ACK パケットを大量に送信 |
| VSE flood | vse | ゲームエンジンに対して UDP パケットを大量に送信 |
| DNS flood | dns | DNS に存在しないドメイン名の名前解決を要求 |
| GRE-ETH flood | greeth | イーサネットと GRE プロトコルによるパケットを大量に送信 |

表 2　AWS Lambda が決定する攻撃の種類

| 種類 | 概要 |
|---|---|
| SYN flood | SYN パケットを大量に送信 |
| UDP flood | UDP パケットを大量に送信 |
| ICMP flood | ICMP パケットを大量に送信 |
| HTTP flood | HTTP リクエストを大量に送信 |

を元に，Botnet が Target Server を標的とする DDoS 攻撃を行う．

学習者は，主に AWS マネジメントコンソールを用いて，対策演習に取り組む．AWS マネジメントコンソールのホーム画面を図 **7** に示す．Web ブラウザ上の GUI で AWS に関する全ての操作を可能とする機能である．サービスごとに固有のダッシュボードが用意され，様々な設定や管理を実施できる．

本演習では，Target Server に対する攻撃の検知，通信内容の解析，攻撃された種類に応じた対策を行う．これらの演習を通して，クラウド環境を標的とする DDoS 攻撃の対策手法を学習することが可能である．5.1 節で攻撃の検知，5.2 節で攻撃の分析，5.3 節で攻撃の対策について述べる．

### 5.1　攻撃の検知

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ず，何らかの問題が Target Server に


図 7　AWS マネジメントコンソールのホーム画面

起きていることを発見する．Amazon CloudWatch を用いて，Target Server に送られてくるトラフィック量，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，大量のデータを送信してサービスの提供を妨げる DDoS 攻撃を受けていると判断する．

### 5.2　攻撃の分析

DDoS 攻撃を受けていると判断できた場合，攻撃の分析を行う．学習者は，EC2 Instance Connect で Target Server にリモートアクセスする．EC2 Instance Connect は，AWS マネジメントコンソール上で，EC2 に SSH 接続する機能である．その後，tcpdump を用いて，通信内容をキャプキャし，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 にアップロードする．アップロードしたダンプファイルを，Wireshark に読み込ませることで，パケットを解析する．送信元 IP アドレスから，どの国または地域から攻撃されているか特定する．さらに，表 2 の種類の中から，どの攻撃を受けているか判断する．

### 5.3　攻撃の対策

特定した種類の攻撃に対応する対策を施す．EC2 のセキュリティグループの修正，AWS WAF，AWS Sheild による対策がある．対策が完了すると，適切に対処できているか確認する．それぞれの対策手法と確認方法について，以下に示す．

#### 5.3.1　EC2 のセキュリティグループの修正

Target Server には，全ての送信元 IP アドレスから，全てのトラフィックを受け入れるように設定されている．そのため，学習者は，特定した攻撃に応じて，受け入れるトラフィックを制限することで，Target Server にセキュアな設定を施す．これら設定には，EC2 のセキュリティグループにおけるインバウンドルールから修正を行う．

#### 5.3.2　AWS WAF

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．本システムで再現している Botnet は，

最も DDoS 攻撃を実施している米国 [13] から攻撃を行う．また，Target Server は，日本国内向けの Web サーバを想定しているため，通信を日本国内に限定することで，攻撃を遮断することができる．攻撃の遮断には，AWS WAF の Web ACLs から対策を施す．

#### 5.3.3 AWS Shield

SYN flood 攻撃，UDP flood 攻撃，ICMP flood 攻撃，HTTP flood 攻撃に有効な対策である．AWS Sheild を導入し，Target Server を保護する設定を施す．攻撃の対策は，AWS Shield の Protected resources から行う．

#### 5.3.4 対策できているかの確認

対策が完了した場合，対策する以前に行った種類と同様の DDoS 攻撃を，Botnet が Target Server へ再度実施する．これにより，適切に対処できているか確認する．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ら，対策演習は終了する．

## 6. 実験

事前テスト・事後テストと利用評価アンケートを行った．本章では，各実験の詳細，結果，考察について述べる．

### 6.1 事前テスト・事後テスト

本システムが，クラウド環境を標的とする DDoS 攻撃の対策訓練を実施できることを確認するために，情報工学を専攻する学生 20 名を対象として実験した．いずれの実験対象者も，DDoS 攻撃の対策に関する知識は取得していない学生である．実験対象者を，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．それぞれ学習の前後には，DDoS 攻撃に関する事前テストと事後テストを設けた．2 グループにおける事前テスト・事後テストの点数差から，クラウド環境を標的とする DDoS 攻撃の対策学習が可能であるか確認した．

事前テスト・事後テストは，情報処理安全確保支援士試験の過去問 [15]，AWS 認定資格の模擬試験 [16]，AWS ホワイトペーパー [17] を元に問題を作成した．事後テストは，事前テストと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．実験対象者に，事前テストの解答は公開せず，事後テストを実施した．

実験結果を**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 点上昇した．座学で学習したグループは，平均点が 1.8 点上昇した．本システムと座学における平均点の上昇率を比較すると，本システムが高い結果となった．この要因の一つに，本システムのハンズオン形式による学習が挙げられる．座学で学習したグループでは，教材を読むだけの学習に取り組んでもらった．これに対して，本システムで学習したグループでは，事前学習ページを読んだ後に，実際に手を動かして演習に取り組んでもらった．そのため，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．

**表 3** 事前テスト・事後テストの結果

| | 事前テスト | | 事後テスト | |
|---|---|---|---|---|
| | 平均 | 標準偏差 | 平均 | 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 |

学習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．分散分析の結果では，交互作用は有意 ($F(1,18) = 8.43,\ p < .01$) であった．さらに，交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．本システムで学習した参加者内要因の単純主効果 ($F(1,9) = 37.0,\ p < .001$) が認められ，座学で学習した参加者内要因の単純主効果 ($F(1,9) = 18.7,\ p < .005$) が認められた．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 ($F(1,18) = 8.57,\ p < .01$) が認められた．これにより，座学より本システムの方が，事後テストにおいて有意に高い結果となった．本システムの利用者が事後テストにおいて，より高い点数をとったことが示され，本システムが有効に機能したと考えられる．これらの結果から，本システムがクラウド環境を標的とする DDoS 攻撃の対策学習が可能であることを確認できた．

### 6.2 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，事前テスト・事後テストで本システムを利用した学生 10 名のグループを対象として，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と標準偏差を**表 4** に示す．全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わかる．

自由記述欄では，「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」，「初めてでもつまづくことなく取り組むことができた」，「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わかりやすかった」，「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の種類を特定する部分が面白かった」，「サイ

表 4　利用評価アンケートの結果

| 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 |

バーセキュリティの研究に興味を持った」，「Wireshark をほと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，「攻撃視点も合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，対策演習における理解促進にも繋がると考えられる．これらの結果から，本システムの有用性を確認できた．

## 7. おわりに

本研究では，クラウド環境を標的とする DDoS 攻撃の対策訓練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 攻撃の対策演習システムを開発した．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，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．加えて，本システムでは，多くの被害を発生させているマルウェア Mirai をモデルとした攻撃演習を実施する．これにより，従来のセキュリティ対策では防ぐことが難しい DDoS 攻撃にも対応できるセキュリティ技術者の養成が可能である．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．

サービス妨害攻撃には，DDoS 攻撃の他に，EDoS 攻撃や DRDoS 攻撃が存在する．そのため，今後の予定として，EDoS 攻撃と DRDoS 攻撃の対策演習システムの追加実装を検討している．また，対策訓練できるクラウド環境の拡張も検討している．IaaS で採用されているメガクラウドの内，本システムで用いた AWS は，6 割を占めている [2]．Azure と Google Cloud Platform を用いた演習を追加実装することで，残りのメガクラウドの対策訓練が可能となる．

**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] 総務省：令和 3 年通信利用動向調査の結果，入手先 ⟨https://www.soumu.go.jp/johotsusintokei/statistics/data/220527_1.pdf⟩(参照 2022-11-01).
[2] 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)，入手先 ⟨https://www.m2ri.jp/release/detail.html?id=500⟩(参照 2022-11-01).
[3] NETSCOUT: 14th Annual Worldwide Infrastructure Security Report, 入手先 ⟨https://www.netscout.com/report/⟩(参照 2022-11-01).
[4] Ponemon Institute: The State of DDoS Attacks against Communication Service Providers, 入手先 ⟨https://www.a10networks.com/wp-content/uploads/A10-EB-14117-EN.pdf⟩(参照 2022-11-01).
[5] 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，入手先 ⟨https://www.soumu.go.jp/main_content/000591470.pdf⟩ (参照 2022-11-01).
[6] 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, 26th USENIX Security Symposium, pp.1093-1110(2017).
[7] 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).
[8] 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.96, No.7, pp.1585-1594(2013).
[9] Hu, J., Meinel, C. and Schmitt, M.: Tele-lab IT security: an architecture for interactive lessons for security education, *ACM SIGCSE Bulletin*, Vol. 36, pp. 412-416(2004).
[10] 福山和生，谷口義明，井口信和：仮想マシンを活用したネットワークセキュリティ学習支援システムの実装と評価，情報処理学会論文誌，Vol.57，No.3，pp.931-935(2016).
[11] Walden, J.: A Real-time information Warfare Exercise on a Virtual Network, *SIGCSE Bull*, Vol. 37, No. 1, pp. 86–90(2005).
[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，マルチメディア分散協調とモバイル（DICOMO2018）シンポジウム，pp. 1809-1816(2018).
[13] Cloudflare: 2022 年第 2 四半期における DDoS 攻撃の傾向，入手先 ⟨https://blog.cloudflare.com/ja-jp/ddos-attack-trends-for-2022-q2-ja-jp/⟩ (参照 2022-11-01).
[14] Kaspersky: DDoS attacks in Q2 2020, 入手先 ⟨https://securelist.com/ddos-attacks-in-q2-2020/⟩ (参照 2022-11-01).
[15] 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），入手先 ⟨https://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_mondai.html⟩ (参照 2022-11-01).
[16] Amazon Web Service: AWS Skill Builder, 入手先 ⟨https://explore.skillbuilder.aws/learn⟩ (参照 2022-11-01).
[17] Amazon Web Service: AWS ホワイトペーパーとガイド，入手先 ⟨https://aws.amazon.com/jp/whitepapers/⟩ (参照 2022-11-01).