G-50

クラウド環境を標的とする DDoS 攻撃の対策訓練を可能とする演習システムの評価

Evaluation of an Exercise System That Enables Training in Countermeasures Against DDoS Attacks Targeting Cloud Environments

眞鍋 督†　　井口 信和‡§
Susumu Manabe　　Nobukazu Iguchi

1. 序論

企業のクラウドサービス利用率は上昇し[1]，それに伴いクラウド環境を標的とする DDoS 攻撃も増加している[2]．しかし，通信サービス事業に勤務する 325 人を対象とした調査[3]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」と回答した事業者は，29%であった．原因として，セキュリティ技術者の不足がある[4]．そのため，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[2]．このことから，従来のセキュリティ対策では，攻撃を防ぐことが難しくなっている．現状の改善には，対策を施す視点だけでなく，攻撃視点から攻撃の性質を学習し，対策に活かすことが有効である[5]．

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 攻撃の対策演習できる環境の提供を目的として，DDoS 攻撃の対策訓練を可能とする演習システム（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．また，IaaS で最も採用されている Amazon Web Service（以下，AWS）を用いた演習を実施する．これにより，クラウド環境を標的とする 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．

2. 関連研究

本システムの関連研究として，立岩らの研究[6]がある．この研究では，セキュリティ技術者の養成を目的に，仮想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．しかし，このシステムは，対策視点のみ演習可能である．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，攻撃手法の学習もできる．

Walden らの研究[7]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．

†近畿大学大学院総合理工学研究科，Graduate School of Science and Engineering Research, Kindai University
‡近畿大学情報学部，Faculty of Informatics, Kindai University
§近畿大学情報学研究所，Cyber Informatics Research Institute, Kindai University

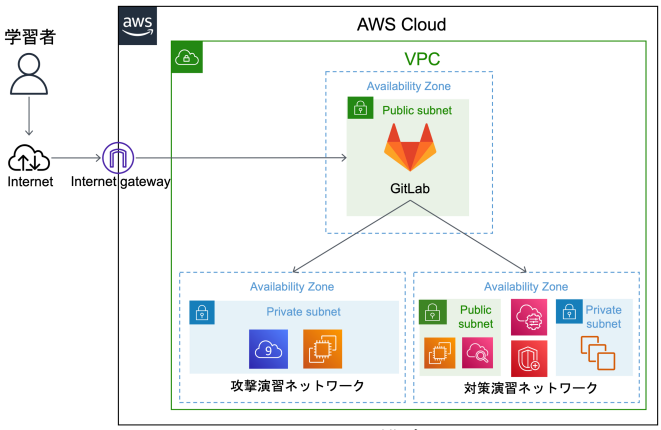

図 1：システム構成図

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，Amazon Virtual Private Cloud（以下，VPC）を用いて，AWS 上に仮想ネットワークを構築している．加えて，VPC に，Amazon Elastic Compute Cloud（以下，EC2）などの AWS リソースを起動することで，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，演習で用いるソースコードを管理する．また，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．さらに，攻撃演習ネットワークと対策演習ネットワークにアクセスするための AWS Identity and Access Management（以下，IAM）ユーザを学習者に提供する．

4. 演習内容

学習者は，GitLab にアクセスし，事前学習ページを閲覧することで，演習で必要な知識を学習する．事前知識の学習後，IAM ユーザを取得する．取得した IAM ユーザを用いて，攻撃演習ネットワークまたは対策演習ネットワークにアクセスし，演習に取り組む．

4.1 DDoS 攻撃演習

4.1.1 攻撃演習ネットワーク

攻撃演習ネットワークでは，DDoS 攻撃演習を実施する．

攻撃演習ネットワークの構成を図 2 に示す．AWS Cloud9 は，学習者が EC2 へアクセスする際に用いる．EC2 は，C2 Server，Bot，Report Server，Loader，Download Server を構築し，DDoS 攻撃が可能な演習環境を提供する．EC2 内で構築できる各サーバの詳細を以下に示す．

■ **C2 Server**

攻撃コマンドを発行し，Bot に DDoS 攻撃を実行させる．実行できる DDoS 攻撃の種類を表 1 に示す．

■ **Bot**

マルウェアに感染した仮想機器である．脆弱な Host がないか探索し， Report Server へ報告する．DDoS 攻撃の際，大量のパケットを Target Server へ送りつける．

■ **Report Server**

脆弱な Host のログイン情報を管理し，Loader へ送信する．

■ **Loader**

Host へ不正ログインし，Download Server にあるマルウェアをダウンロードさせて，新たに Bot を構築する．

■ **Download Server**

Host にダウンロードさせるマルウェアを管理する．

4.1.2 攻撃演習の流れ

学習者は，C2 Server，Report Server，Loader，Download Server を構築する．構築したサーバを用いて，Host にマルウェアをダウンロードすることで，Bot に感染させる．次に，C2 Server から Bot を遠隔操作して，Target Server へ DDoS 攻撃を実行させる．攻撃後に，Target Server へアクセスを試みて，サーバダウンを確認できた場合，攻撃演習は終了する．これらの演習を通して，DDoS 攻撃の仕組みを理解することが可能である．

4.2 DDoS 対策演習

4.2.1 対策演習ネットワーク

対策演習ネットワークでは，DDoS 対策演習を実施する．対策演習ネットワークの構成を図 3 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．

東京リージョンには，Target Server，Amazon CloudWatch，Wireshark，AWS Shield がある．Target Server は，EC2 を用いて構築している．Web サイトを提供し，DDoS 攻撃の対象となるサーバである．Amazon CloudWatch は，Target Server に送られてくるデータ量などを監視できるサービスである．AWS Shield は，AWS が提供する DDoS 攻撃対策の専用サービスであり，さまざまな攻撃に応じた対策を施すことが可能である．

バージニア北部リージョンには，AWS Lambda と Botnet がある． AWS Lambda は，SYN flood，UDP flood，ICMP flood，HTTP flood から DDoS 攻撃の種類をランダムに決定する．その後，Botnet へ決定した攻撃に対応するコマンドを発行する．Botnet は，EC2 を用いて構築しており，DDoS 攻撃を実施するボットネットを再現している． AWS Lambda から受け取ったコマンドをもとに，Botnet が東京リージョンの Target Server に向けて攻撃を実行する．

4.2.2 対策演習の流れ

演習を開始すると，AWS Lambda が Botnet に DDoS 攻撃を実行させる．このとき，攻撃の種類はランダムである．学習者は，Target Server が提供している Web サイトへアクセスできないことを確認する．次に，Amazon CloudWatch を用いて，Target Server に送られてくるデータ量を監視する．大量のデータが送られていたら，通信内容を Wireshark で解析し，DDoS 攻撃を受けているか判断する．また，送信されたパケットから，攻撃元や攻撃の種類を特定する．特定した攻撃に応じて，AWS Shield などを用いることで，対策を Target Server に施す．Botnet が再度 DDoS 攻撃を実

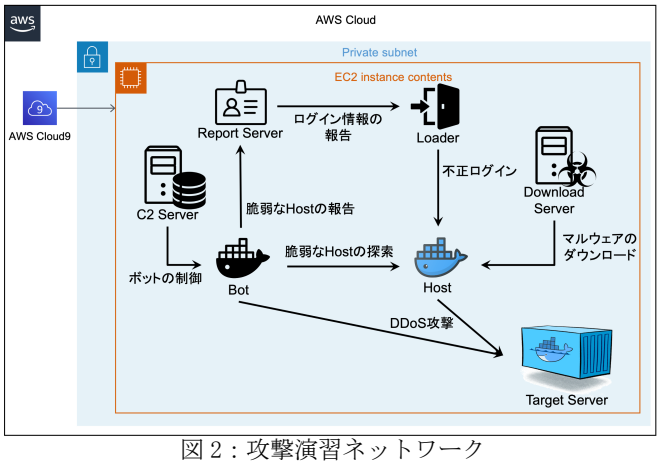

図 2：攻撃演習ネットワーク

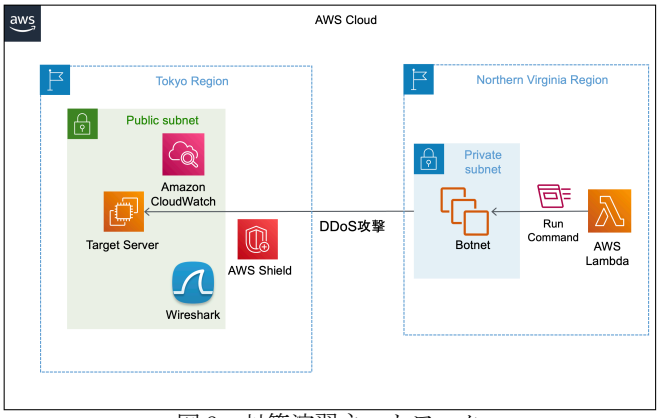

図 3：対策演習ネットワーク

表 1：実行できる攻撃の種類

種類	概要
HTTP flood	HTTP リクエストを大量に送信
UPD-PLAIN flood	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 パケットを大量に送信
ACK flood	ACK パケットを大量に送信
SYN flood	SYN パケットを大量に送信
GRE-IP flood	GRE プロトコルによるパケットを大量に送信
ACK-STOMP flood	TCP セッション確立後に ACK パケットを大量に送信
VSE flood	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 に存在しないドメイン名の名前解決を要求
GRE-ETH flood	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

行し，適切に対処できているか確認する．Target Server が提供している Web サイトにアクセスできた場合，対策演習は終了する．これらの演習を通して，クラウド環境を標的とする DDoS 攻撃の分析手法や対策手法を学習することが可能である．

5. 実験

5.1 事前・事後テスト

本システムが，クラウド環境を標的とする DDoS 攻撃の対策学習できることを確認するために，情報工学を専攻する学生 14 名を対象として実験した．実験対象者は，DDoS 攻撃について本システムで学ぶグループと，書籍で学ぶグループに分割し，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・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・事後テストは，AWS 認定資格試験と AWS ホワイトペーパーをもとに問題を作成した．事後テストは，事前テストと同レベルの別の問題を用いた．問題数はそれぞれ 10 問であり，1 問 1 点として点数をつけた．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 2 に示す．本システムを用いたグループは平均点が 5.14 点上昇し，書籍を用いたグループは平均点が 1.86 点上昇した．また，事後テストの標準偏差において，本システムは 1.92 点，書籍は 1.07 点であった．そのため，個人差はあるが，両グループで学習効果があったと考えられる．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 攻撃の対策学習できることを確認した．

5.2 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，実験で本システムを利用した学生 7 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 段階評価である．また，自由記述欄を設けており，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 3 に示す．全ての項目で良好な結果だった．また，標準偏差から，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．自由記述欄では，「全体を通して，説明・演習を繰り返した内容となっていたので，初めてでもつまずくことなく学習できた」，「実際に対策の効果をみられたことがよかった」などの回答を得られた．これらの結果から，本システムの有用性を確認した．

6. 結論

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 攻撃の対策演習できる環境の提供を目的として，DDoS 攻撃の対策訓練を可能とする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を実施できる．また，AWS を用いることで，クラウド環境を標的とする 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．

今後の予定として，クラウドサービスの普及以降，新たに登場した EDoS 攻撃の対策演習できるシステムの開発を検討している．

表 2：事前・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	2.29	0.88	7.43	1.92
書籍	3.14	0.99	5.00	1.07

表 3：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	4.6	0.49
演習の流れは理解できたか	4.8	0.35
演習の難易度は適切であったか	4.6	0.73
システムの操作方法は理解できたか	4.4	0.73
DDoS 攻撃の検出手法について理解できたか	4.6	0.73
DDoS 攻撃の対策手法について理解できたか	4.7	0.45
DDoS 攻撃の原理について理解できたか	4.9	0.35
セキュリティへの関心は高まったか	4.4	0.73
演習を通して，DDoS 攻撃の対策するには攻撃者視点も必要だと感じたか	4.3	0.88

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 2022-07-15).

[2] NETSCOUT: 14th Annual Worldwide Infrastructure Security Report, 入手先<https://www.netscout.com/report/> (参照 2022-07-15).

[3] 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 2022-07-15).

[4] 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 2022-07-15).

[5] Uma, M. and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification, IJNS, Vol. 15, No.5, pp.390-396(2013).

[6] 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).

[7] Walden, J.: A Real-time information Warfare Exercise on a Virtual Network, SIGCSE Bull, Vol. 37, No. 1, pp. 86–90 (2005).