6ZH-09

クラウド環境に対するDDoS攻撃の対策演習を可能とする学習支援システムの開発

眞鍋督[†]　井口信和[‡§]

近畿大学大学院総合理工学研究科[†]　近畿大学理工学部情報学科[‡]　近畿大学情報学研究所[§]

1. 序論

企業のクラウドサービス利用率は年々上昇し，それに伴い企業が利用するクラウド環境に対するDDoS攻撃も増加している．しかし，通信サービス事業に勤務する325人へ実施した調査[1]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，わずか29%であった．原因としてセキュリティ技術者の不足が挙げられる[2]．この原因の改善には，クラウド環境に対するDDoS攻撃の対策技術を取得したセキュリティエンジニア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ており，様々な攻撃手法を組み合わせたマルチベクトル型など，年々複雑さも増している．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困難になっている．この現状の改善には，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[4]．

そこで本研究では，攻撃視点を取り入れたクラウド環境に対するDDoS攻撃の対策演習が実施できる環境の提供を目的として，DDoS攻撃の対策演習を可能とする学習支援システム（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の実施が可能である．また，Amazon Web Service（以下，AWS）を用いることで，クラウド環境を狙ったDDoS攻撃の対策演習が可能である．本システムを用いた演習を通して，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[5]がある．この研究では，セキュリティ技術者の早期養成を目的として，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．しかし，このシステムは対策視点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，対策手法と攻撃手法を学習する．

Waldenらの研究[6]では，セキュリティの概念と技術を学習することを目的として，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，攻撃と対策の両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，学習者が安全性を判別した上で入手する必要がある．そのため，中級者以上の

Development of a Learning Support System for DDoS Attack Countermeasure Exercise in Cloud Computing
†Susumu Manabe, Graduate School of Science and Engineering Research, Kindai University
‡Nobukazu IGUCHI, Department of Informatics, Faculty of Science and Engineering, Kindai University
§Nobukazu IGUCHI, Cyber Informatics Research Institute, Kindai University

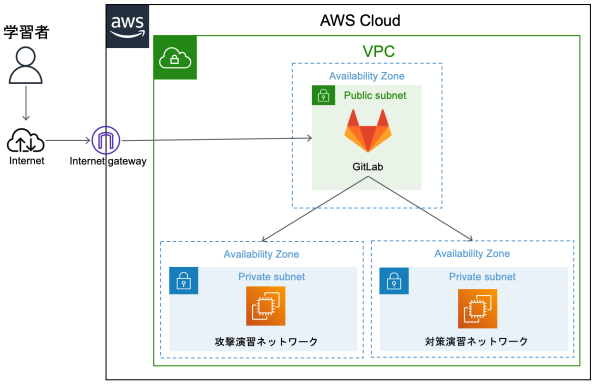

図1：システム構成図

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．

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．構築された仮想ネットワークにAmazon Elastic Compute Cloud（以下，EC2）インスタンスなどのAWSリソースを起動することで，演習環境を提供する．VPCには，GitLabサーバと攻撃演習ネットワーク及び対策演習ネットワークがある．

GitLabサーバには，攻撃演習で用いるソースコードを管理しており，演習開始時に自動でリポジトリをEC2インスタンスにクローンする．また，演習で必要な事前知識を学習する教材として学習ページを設けている．学習ページは，演習概要ページとDDoS攻撃演習ページ及び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

学習者は初めにGitLabサーバにアクセスして，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．それぞれの学習ページを閲覧後，AWS IAMユーザを取得する．取得したAWS 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．演習開始時に，EC2インスタンス内のDockerイメージをビルドして攻撃演習ネットワークを構築する．攻撃演習ネットワー

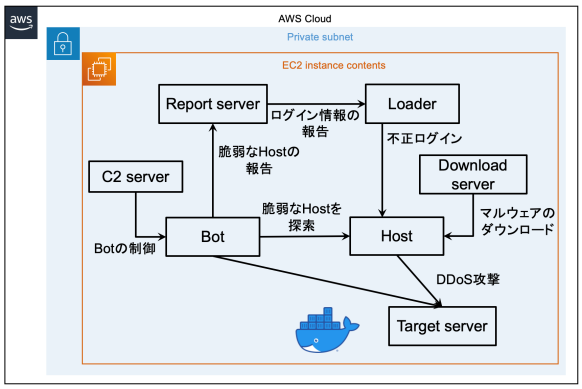

図 2：攻撃演習ネットワーク

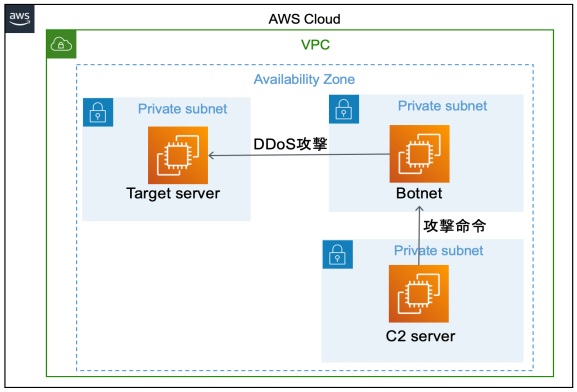

図 3：対策演習ネットワーク

クには，C2 server と Bot，Host，Report server，Loader，Download server，Target server がある．C2 server はマルウェアに感染した Bot の管理や制御する機能を持つ．Bot は脆弱な Host がないか探索する．脆弱な Host を発見した場合，Bot は結果を Report server へ報告する．Report server は Host のログイン情報を Loader へ送信する．Loader は Host へ不正ログインし，Download server にあるマルウェアを Host にダウンロードさせて，新たな Bot を構築する．構築された Bot は C2 server の指示で Target server へ DDoS 攻撃を行う．

4.1.2. 攻撃演習の流れ

学習者は C2 server と Report server，Loader，Download server を各コンテナに立ち上げて，Host をマルウェアに感染させることで Bot を構築する．次に，Bot を用いて Target server へ DDoS 攻撃を実施する．最後に，Target server へアクセスを試み，正常に動作していないことを確認した場合，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 Target server と DDoS 攻撃を実施する Botnet，攻撃指令を Botnet に送る C2 server から構成される．

4.2.2. 対策演習の流れ

対策演習を開始すると，C2 server が Botnet に Target server を狙った DDoS 攻撃を実行させる．学習者は Target server に送られてくるトラフィックを監視する．監視には AWS CloudWatch を用いる．トラフィックの異常を確認した場合，通信内容を tcpdump でキャプチャして Wireshark で解析することで，攻撃の種類を特定する．特定した攻撃の対策を Target server に施す．また，DDoS 攻撃に有効な AWS リソースを用いた対策も実施する．

本演習では，Target server への対策に加えて，Botnet に加担している機器への対策学習も行う．学習者は機器にログインして，脆弱な Telnet 設定になっていないか確認する．脆弱な Telnet 設定になっている機器には，安全性の高い ID とパスワードに変更して対策を施す．

再度 DDoS 攻撃を試みることで，適切に対処できているかを確認する．適切に対処できていた場合，対策演習は終了する．これらの演習を通して，DDoS 攻撃の分析手法や対策手法，DDoS 攻撃に加担しないための対策を学習することが可能である．

5. 実験

本システムの実装は完了したので，本システムの有用性の確認を目的に，情報工学を専攻する学生を対象として実験を行う予定である．初めに，DDoS 攻撃に関する事前テストを実施する．次に，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と書籍で学ぶグループに分割し，学習に取り組んでもらう．最後に，DDoS 攻撃に関する事後テストを実施する．2 グループにおける事前・事後テストの点数差から，本システムが DDoS 攻撃対策学習の支援ができていることを確認する予定である．

6. 結論

本研究では，攻撃視点を取り入れたクラウド環境に対する DDoS 攻撃の対策演習が実施できる環境の提供を目的として，DDoS 攻撃の対策演習を可能とする学習支援システムを開発した．本システムの活用により，学習者は 1 人で攻撃視点と対策視点から学習できる．さらに，AWS を用いることで，クラウド環境を対象とした DDoS 攻撃の対策演習が可能である．本システムを用いた演習を通して，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．

参考文献

[1] 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 2021-12-24）

[2] 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 2021-12-24）

[3] NETSCOUT: 14th Annual Worldwide Infrastructure Security Report, 入手先<https://www.netscout.com/report/>(参照 2021-12-24)

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

[5] 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).

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