G-59

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検討

A Study of Practice Support System Against DDoS Attack Targeting Cloud Computing

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年々上昇しており，それに伴い企業が利用するクラウド環境を狙った DDoS 攻撃も増加している．しかし，2019 年に通信サービス事業に勤務する 325 人に対して実施した調査[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」と答えた事業者は，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 攻撃対策方法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 攻撃の種類は多様化しており，様々な攻撃手法を組み合わせたマルチベクトル型など，DDoS 攻撃は年々複雑さを増している[3]．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は難しくなっている．この現状の解決には，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び，対策に活かすことが有効と考えられる[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）を検討する．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，クラウド環境を対象とした DDoS 攻撃の対策演習を実施できる．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的に攻撃する機能を用いることで，対策手法を演習できる環境を実現している．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演習も実施する．

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

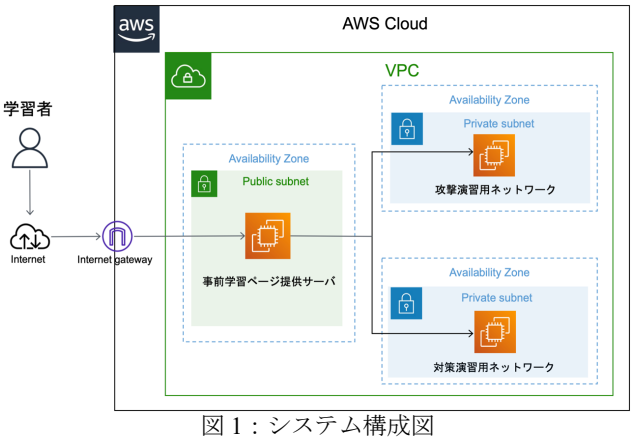

図 1：システム構成図

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．

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，AWS を用いて，仮想マシンを動作させる．動作させた仮想マシンを相互接続することで，実機を用いた場合と同様の仮想ネットワークをクラウド上に構築している．仮想ネットワークには，事前学習ページ提供サーバと攻撃演習用ネットワーク，対策演習用ネットワークがある．

事前学習ページ提供サーバには，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，DDoS 攻撃演習ページ，DDoS 対策演習ページから構成される．学習者は，それぞれの学習ページを閲覧後，攻撃演習用ネットワークまたは，対策演習用ネットワークにアクセスして演習に取り組む．

4. 演習内容

本システムで扱う DDoS 攻撃の種類は，SYN Flood 攻撃，ICMP Flood 攻撃，UDP Flood 攻撃，HTTP Flood 攻撃である．演習は AWS 上にあらかじめ構築された仮想ネットワークで実施する．

4.1. DDoS 攻撃演習

DDoS 攻撃演習の流れを図 2 に示す．DDoS 攻撃演習は，攻撃演習用ネットワークで実施する．攻撃演習用ネットワークは，Web サーバ，攻撃ホスト，踏み台ホストから構成される．

はじめに，学習者は踏み台ホストへ不正侵入するためのマルウェアを作成する．作成したマルウェアを，攻撃ホストから複数台の踏み台ホストに送信して感染させることで，DDoS 攻撃の踏み台に利用するボットを構築する．

次に，複数台のボットを一括で制御する Command and Control サーバ（以下，C2 サーバ）を作成する．複数台のボットと C2 サーバをそれぞれ接続させることで，ボットネットを構築する．

ボットネットの構築後，学習者は DDoS 攻撃のスクリプトを作成する．作成したスクリプトは，C2 サーバを経由して，攻撃ホストからボットネットに送信する．学習者は，攻撃ホストから C2 サーバを用いて，ボットネットに Web サーバを狙った攻撃スクリプトを実行させる．

攻撃の実施後，攻撃ホストから Web サーバへアクセスを試みる．攻撃が成功して，アクセスできないことを確認した場合，DDoS 攻撃演習は終了する．これらの演習を通じて，DDoS 攻撃の原理を学習することが可能となる．

4.2. DDoS 対策演習

DDoS 対策演習の流れを図 3 に示す．DDoS 対策演習は，対策演習用ネットワークで実施される．対策演習用ネットワークは，Web サーバ，自動攻撃ホスト，ボットネット，C2 サーバから構成される．

演習が開始されると，自動攻撃ホストが C2 サーバへアクセスして，ボットネットを遠隔操作することで，Web サーバへ自動で攻撃を仕掛ける．攻撃の種類はランダムに選択される．

学習者は AWS 上に構築された仮想ネットワーク内を監視して，Web サーバへの攻撃を検出する．検出した攻撃を分析し，攻撃の種類を特定する．正しく特定できた場合，自動攻撃ホストの攻撃が一時中止される．

その後，Web サーバに対して特定した攻撃の対策を施す．さらに，踏み台ホストに感染しているマルウェアを検出して，DDoS 攻撃に加担することを防ぐボット対策を施す．

自動攻撃ホストが攻撃を再度行うことで，対策できているかを確認する．適切に対策できていた場合，対策演習は終了する．これらの演習を通じて，DDoS 攻撃の検出手法や対策手法について学習が可能となる．

5. 実験

本システムの有用性を確認することを目的に，情報系大学生と大学院生を対象に実験する予定である．はじめに 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けて，それぞれ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．加えて，本システムで学習したグループは，利用評価アンケートに回答してもらう．2 つのグループにおける事前テスト・事後テストの点数差と，利用評価アンケートから，本システムがクラウド環境に対する 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．

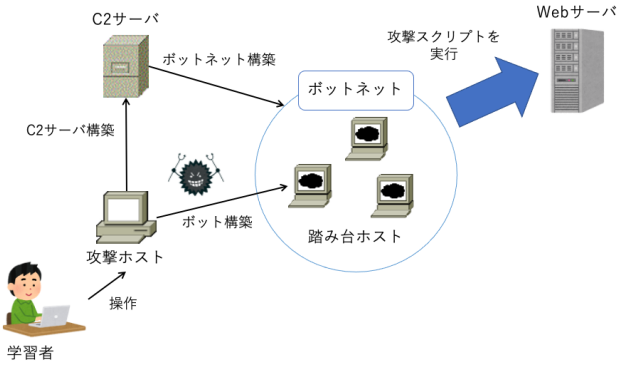

図 2：DDoS 攻撃演習の流れ

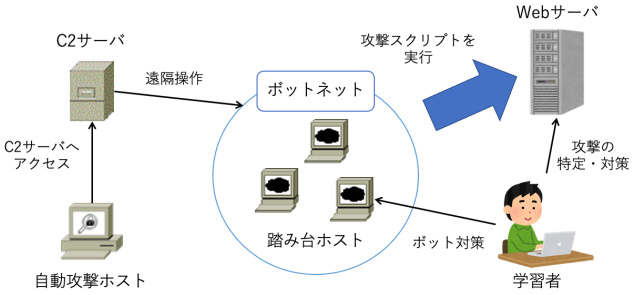

図 3：DDoS 対策演習の流れ

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検討した．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 2021-07-05）

[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 2021-07-05）

[3] NETSCOUT: Worldwide Infrastructure Security Report (2019)，入手先<https://www.netscout.com/report/>(参照 2020-07-05)

[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，電子情報論文誌,，Vol.96，No.7，pp.1585-1594 (2013).

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