5ZC-03

# DDoS 攻撃対策演習を可能とするネットワークセキュリティ学習支援システム

眞鍋督[†]　岸本和理[‡]　柏崎礼生[§]　井口信和[†||]

近畿大学理工学部情報学科[†]　近畿大学大学院総合理工学研究科[‡]

国立情報学研究所[§]　近畿大学情報学研究所[||]

## 1. 序 論

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，85%が「今後も DDoS 攻撃はさらに増加する」，または「今後も DDoS 攻撃は高いレベルを維持する」と予想している．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」と答えた事業者は，わずか 29%であった．原因として対策予算およびセキュリティ技術者の不足が挙げられる [2]．後者のセキュリティ技術者の不足を改善するためには，各組織が DDoS 攻撃対策のネットワークセキュリティ教育を実施するだけでなく，個人が DDoS 攻撃対策の学習可能な環境を用意し，セキュリティエンジニアを早期に養成することが挙げられる．

世界のセキュリティ事情を調査・分析したレポート [3]によると SaaS やデータセンターサービス，クラウドサービスへの DDoS 攻撃を経験した企業は 2018 年の 1 年間で 3 倍に増加している．さらに DDoS 攻撃は年々複雑さを増している．2020 年には DDoS 攻撃件数が 3 ヶ月で 2 倍以上に急増し，より深刻になっている [4]．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び，対策に活かすことが有効であると考えられる [5]．

攻撃視点と対策視点からセキュリティを学べる演習として，Capture The Flag（以下，CTF）がある．CTF の演習では，安全上の理由から実環境を模倣した演習用のネットワークを実機で用意する必要がある．しかし，演習用に実機を用意する場合，機器の設定やネットワークの配線などの設置コストが発生してしまう．一方，仮想のネットワーク環境上で演習を実施できるサイバーレンジがある．これにより，実環境や実機に影響を与えることなく演習ができる．しかし，導入にあたって予算，時間，人員といったコストが発生するため，学習者が手軽に演習に取り組む用途には向かない．

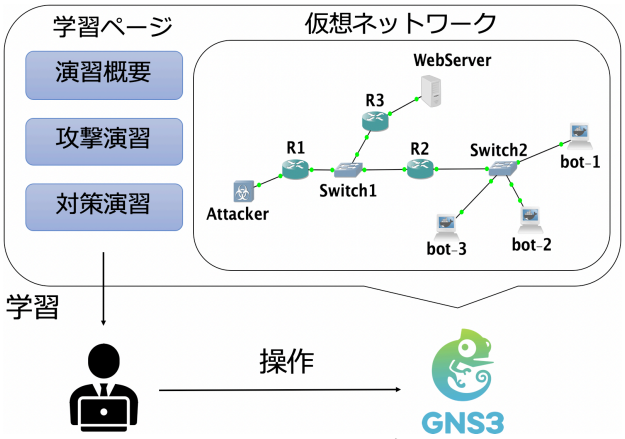


図 1 システム構成図

そこで本稿では，攻撃視点を取り入れた DDoS 攻撃の対策演習を安全かつ手軽に実施できる環境の提供を目的として，DDoS 攻撃対策演習を可能とするネットワークセキュリティ学習支援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，仮想マシンを用いることで，実機を用意する必要がなく，低コストで実施することができる．本システムを用いて攻撃視点と対策視点から演習することで，DDoS 攻撃の対策に関する理解と知識の定着が期待できる．

## 2. 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，Graphical Network Simulator-3（以下，GNS3）を用いて仮想的なネットワーク機器を動作させる．GNS3 上で動作させたネットワーク機器を相互接続することで，1 台の PC 上で実機を用いた場合と同様のネットワークを構築することができる．

演習を実施するための教材として，GNS3 上に学習ページを設けている．学習ページは，演習概要，DDoS 攻撃演習，DDoS 対策演習から構成される．学習者は，学習ページを参考に GNS3 を操作することで，DDoS 攻撃演習と DDoS 対策演習を実施する．

## 3. 演習内容

本システムでは DDoS 攻撃の中でも主流な SYN Flood 攻撃を扱う．演習は GNS3 上にあらかじめ準備した仮想ネットワークで実施する．仮想ネットワークは Web サーバ，ホスト，攻撃ホスト，被害ホスト，ルータ，スイッチから構成される．

演習で必要な知識を学習するために，演習概要ペ

---

Network Security Learning Support of DDoS Attack Detection Exercise System

†Susumu MANABE, Nobukazu IGUCHI, Department of Informatics, Faculty of Science and Engineering, Kindai University

‡Kazuri KISHIMOTO, Graduate School of Science and Engineering Research, Kindai University

§Hiroki KASHIWAZAKI, National Institute of Informatics

||Nobukazu IGUCHI, Cyber Informatics Research Institute, Kindai University

ージを準備している．演習概要ページでは，DDoS 攻撃の説明や攻撃演習と対策演習の流れ，構築されたネットワークについて学習できる．演習概要ページによる学習後に，学習者は演習を開始する．

### 3.1 DDoS 攻撃演習

DDoS 攻撃演習では，ペネトレーションテストツールである Metasploit Framework（以下，Metasploit）と hping3 を用いる.まず，ホストから Web サーバに正常にアクセスできることを確認する．次に攻撃ホストから Metasploit を用いて，被害ホストにリモートでコマンドを実行可能とするバックドアを設置する．攻撃ホストは設置したバックドアを利用し，被害ホストに不正侵入する．不正侵入後に，攻撃ホストが被害ホストを踏み台として，標的となる Web サーバへ攻撃する．攻撃には，hping3 を用いて，被害ホストの送信元 IP アドレスを詐称し，SYN Flood 攻撃を実施する．攻撃後，ホストから再度 Web サーバへアクセスを試みる．攻撃が成功し，アクセスができないことを確認した場合，攻撃演習は終了する．これらの演習を通じて，DDoS 攻撃の原理を学習することが可能となる．

### 3.2 DDoS 対策演習

DDoS 対策演習では，ネットワークアナライザである Wireshark を用いて，仮想ネットワーク内の監視を実施し，SYN Flood 攻撃を検出する．検出した攻撃を分析し，SYN Flood 攻撃の仕組みについて理解する．次に DDoS 攻撃の加担者にならないための対策を被害ホストに施す．さらに，SYN cookies の有効化などの設定を Web サーバ上で実施し，SYN Flood 攻撃の対策を施す．再度 DDoS 攻撃を実施することで，対策できているかの確認する．適切に対処できていた場合，対策演習は終了する．これらの演習を通じて，DDoS 攻撃の検出方法や対策方法について学習することが可能となる．

## 4. 実験・考察

本システムの有用性を確認することを目的に，情報系を専攻する大学生９名を対象として利用評価実験を実施した．実験で再現したネットワークは Web サーバ１台，ホスト１台，攻撃ホスト１台，被害ホスト１台，ルータ３台，スイッチ２台である．準備した仮想ネットワーク上で本システムの演習に取り組んでもらった．

攻撃演習と対策演習終了後，本システムに関するアンケートを回答してもらった．アンケートは，1 が最も悪く，5 が最も良いとした 5 段階評価となっている．また，アンケートには自由記述欄を設けており，コメントを記入してもらう．評価項目と各項目に対する評点結果を表 1 に示す．全ての項目で良好な結果が得られた．自由記述欄では「攻撃視点から学ぶことで DDoS 攻撃の仕組みを理解する事ができた」，「1 人で簡単に攻撃視点と対策視点まで学習できたのはよかった」，「DDoS 攻撃対策の興味や関心が芽生えた」などの意見が得られた．これにより，本システムによって DDoS 攻撃対策学習の支援ができていることを確認した．

表 1 評価項目と評点（単位：点）

| 評価項目 | 平均 | 標準偏差 |
|---|---|---|
| 検出手法について理解できたか | 4.3 | 0.94 |
| 対策手法について理解できたか | 4.2 | 1.03 |
| 攻撃演習による DDoS 攻撃の理解度は向上したか | 4.7 | 0.47 |
| 対策学習に役立つと思うか | 4.3 | 0.82 |

しかし，「DDoS 攻撃の対策に関する知識や理解ができたか客観的に確認できなかった」という指摘を受けた．本システムでは，学習ページを参考に GNS3 を操作することで演習を実施する．そのため，学習者が客観的に対策の知識や理解度を確認することができない．そこで，本システムにテスト形式で DDoS 攻撃と対策を仮想ネットワーク上で実施する機能を追加する必要がある．実践形式のテストを設けることで，DDoS 攻撃の対策に関する知識や理解の定着度を客観的に評価することが可能となる．

## 5. 結 論

本稿では，DDoS 攻撃対策演習を可能とするネットワークセキュリティ学習支援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，仮想マシンを用いることで，実機を用意する必要がなく，低コストで実施することができる．これにより，本システムを用いて攻撃視点と対策視点から演習することで，DDoS 攻撃の対策に関する理解と知識の定着が期待できる．

今後の課題として，仮想ネットワーク上で実施する DDoS 攻撃対策演習テスト機能の追加を検討している．また，演習で扱う DDoS 攻撃の種類を多様化させ，様々なネットワークで演習が可能な環境の開発を予定している．さらに，複数人での攻防戦型演習を可能とするために，複数の学習者が同時に演習を実施できる環境を構築する予定である．

## 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 2020-01-04）
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 2020-01-04）
3) NETSCOUT: Worldwide Infrastructure Security Report(2019) 入手先＜https://www.netscout.com/report/＞（参照 2020-01-04）
4) Kaspersky: DDoS attacks in Q1 2020 入手先＜https://securelist.com/ddos-attacks-in-q1-2020/96837/＞（参照 2020-01-04）
5) Uma, M. and Padmavathi, G.: A Survey on Various Cyber Attacks and Their Classification, IJNS, Vol. 15, No.5, pp.390-396(2013).