6J-02

シングルボードコンピュータを用いたサービス拒否攻撃演習システムの提案

干川 尚人† 小林 康浩† 石原 学† 白木 厚司‡ 下馬場 朋禄‡ 伊藤 智義‡

国立高等専門学校機構 小山高専† 千葉大学‡

1. はじめに

今日ではネットワークシステムを利用した社会システムの運用が不可欠になっており，社会から対応するセキュリティ人材が強く求められている．しかし，これを支える ICT 人材の供給不足が深刻化しており，特に 2020 年以降は情報セキュリティに関わる人材はおよそ 15%が「質・量ともに不足する」とも指摘されている[1]．教育機関は社会から効率的な人材の育成が求められているが，情報システムのセキュリティ運用には，ネットワーク，コンピュータなどの多方面にわたる技術分野の統合的な理解が必要で，その習熟に費やす長い教育時間が課題になる．そこで，本研究グループでは攻防戦型演習の手法を取り入れた効率的なネットワークセキュリティ教育手法を提案する．本稿では提案手法による実装システムとシナリオを示し，併せて本手法による講義事例について紹介する．

2. 従来のネットワーク技術者教育

情報系の専門教育を行う職業専門学校や高専・大学などの高等教育機関では，コンピュータ，ネットワーク，セキュリティといったシステム構築・運用に必要な幅広い基礎知識を履修させている．しかし，既卒者でも総合的な仕組みを理解できる人材は限られているため，ネットワークシステムを統合的に理解できる質の高い人材を教育工程において育成できれば人材不足の課題解決に寄与できる．これらの人材を採用する企業においては現場教育や運用系の検証システムを通した実践的な学習によって，運用の効率的な習熟を行っている．しかし，実務で取り扱う高価なサーバやネットワーク機器を配備した演習システムを教育のために維持管理していくことは容易ではなく，また実システムを用いた現場教育も実務部署の業務負担を大きくする問題がある．よって，現場や検証システムのような本物の環境に依らず，教育工程において実践的技術習得のギャップを埋めることができれば，効率的な教育効果を期待できる．

ネットワークセキュリティ分野では，参加者が攻撃，防御の立場になり攻防を行う実践的な攻防戦型の演習 Capture The Flag(以下 CTF)が行われている[2]．演習遂行にはシステム構築・運用の理解が不可欠であるため，このような能動的な演習型教育は統合的な技術習熟効果を期待できる．一方で，一般的な CTF 演習参加者は一定水準以上の技術を習得済みなので，この競技型の演習手法をそのまま教育に適用することは困難である．

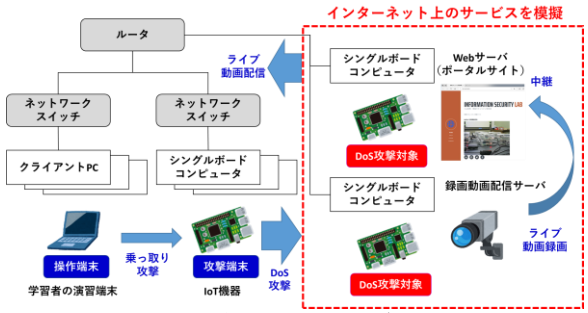

図 1 実装システムの概要

3. 攻撃演習を通した教育システム

システム構築や運用などの経験がない机上学習者に対して実践型教育を行うために，我々は CTF 演習のような攻防型演習の特徴を利用したネットワークセキュリティ教育システムを提案する．

3.1. サービス拒否攻撃演習

CTF 演習は有スキル者による競技が主目的であり，その幅広いテーマは机上学習者のレベルに適さない．そこで我々は演習の題材として「インターネットサービスのセキュリティ」を設定し，アプリケーションサーバに対するサービス拒否（Denial of Service ：以下 DoS）攻撃を行う演習型シナリオを提案する．この DoS 攻撃演習はネットワークシステム技術者に対する教育題材として下記に述べる効果を期待できる．

- システム構成や運用などの専門的な技術内容と現実のサービスとの対応を実感しやすい
- システム開発に不可欠な負荷試験に対する実践スキルを学べる
- セキュリティ分野において課題となっている DoS 攻撃について仕組みを学べる

Proposal of Denial of Service Attack Exercise System Using Single Board Computer

†Naoto HOSHIKAWA, †Yasuhiro KOBAYASHI, †Manabu ISHIHARA, ‡Atsushi SHIRAKI, ‡Tomoyoshi SHIMOBABA and ‡Tomoyoshi ITO

†National Institute of Technology, Oyama College and ‡Chiba University

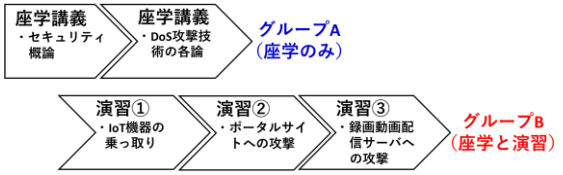

図 2 学習シナリオのフロー

3.2. 演習システム

本演習システムは孤立したネットワーク上で構築し，録画したストリーム動画の配信サーバとこれを仲介するポータルサイト，そして学習者の操作端末と攻撃端末から成る．実装システムの概要を図 1 に示す．まず，論理ノードとして，ライブ動画配信を中継するポータルサイトの Web サーバ，ライブ動画を録画する録画動画配信サーバ，攻撃端末である複数の IoT 機器，そして攻撃を指示する操作端末のクライアント PC を配置する．このとき，ポータルサイトおよび録画動画配信サーバはインターネット上のサービス，攻撃端末および操作端末はインターネットに接続された一般機器を模している．この環境で学習者は操作端末によって攻撃端末である IoT 機器を踏み台にしてライブ動画配信サービスに対して DoS 攻撃を行う．操作端末は一般的な Windows PC を用い，それ以外の動画配信サーバ，ポータルサイト，攻撃端末は安価なシングルボードコンピュータを用いる．ネットワーク機器も市販の民生用ルータ，スイッチが利用可能なので，実運用型の教育システムと比べて安価かつ柔軟に構築・運用が可能である．

3.3. 学習シナリオ

学習シナリオのフローを図 2 に示す．最初に座学講義として概論を述べ，その後に DoS 攻撃に関わる各論を講義する．次に DoS 攻撃演習を実施する．演習は Web サイトのデータ取得リクエストを繰り返す HTTP GET Flood 攻撃を用いて「ポータルサイトを閲覧するユーザに対して映像を閲覧できない（サービス拒否）状態を作ること」を課題設定する．学習者は①IoT 機器の乗っ取り，②ポータルサイトへの攻撃，③録画動画配信サーバへの攻撃の 3 つを行う．まず，学習者は演習①，②によってこれを試みるが，実装システムでは予めこの攻撃でポータルサイトのサービス拒否状態は実現できない設定にしてあるため，達成はできない．そこで，演習③によってネットワークで連携している録画動画配信サーバの脆弱性に気付かせて，改めてこちらへ直接攻撃することで目的達成，というシナリオを経て演習を完了する．なお，サービス拒否状態の実現は録画動画配信サーバの上限セッション数で調整し，演習で使う HTTP GET Flood 攻撃も繰り返し動画ストリームの接続要求を行うだけの単純なスクリプトである．そのため，学習者が習得する知識は「攻撃」を実現する技術ではなく，システムの開発や負荷試験などで必要な「ネットワークの基本的な技術知識」に留まる．

表 1 グループごとの試験結果（正答率）

設問	グループ A	グループ B	問題出典
DNS 水責め攻撃(ランダムサブドメイン攻撃)の方法はどれか。	57.1%	72.7%	H30 春期 データベーススペシャリスト 午前Ⅱ 問 20
DoS 攻撃の一つである Smurf 攻撃の特徴はどれか。	28.6%	31.8%	H28 春期 情報セキュリティスペシャリスト 午前Ⅱ 問 7
ICMP Flood 攻撃に該当するものはどれか。	61.9%	59.1%	H29 春期 情報処理安全確保支援士 午前Ⅱ 問 18
DNS の再帰的な問合せを使ったサービス不能攻撃(DNS amp)の踏み台にされることを防止する対策はどれか。	38.1%	68.2%	H29 秋期 ネットワークスペシャリスト 午前Ⅱ 問 21
次の攻撃において、攻撃者がサービス不能にしようとしている標的はどれか。	38.1%	63.6%	H28 春期 情報セキュリティスペシャリスト 午前Ⅱ 問 2
平均正答率	44.8%	59.1%	

4. 方式の評価と考察

本方式の評価を行うため，座学のみ実施したグループ A および座学と演習を実施したグループ B の 2 つの母集団に対して講義を行った．両者は国立高専機構情報セキュリティ人材育成事業（K-SEC）で開講した特別講義の参加者で，全国の高等専門学校の本科生 1〜5 年および専攻科生が対象である．それぞれの参加人数はグループ A で 21 名，グループ B で 22 名であり，全員情報工学または電気電子工学の教育課程に属している．学習効果の比較のために両グループに対して講義後に試験を行った．ここでは，恣意的な問題設定を避けるために情報処理技術者試験，情報処理安全確保支援士試験の過去問題から，攻撃技術に関連する選択問題を 15 題抽出している．このうち DoS 攻撃手法に関連する問題についてグループごとの正答率を表 1 に示す．平均正答率はおよそ 15%程度グループ B が高く，グループ A の正答率が上回る設問 C においてもその差は小さく，全般的にグループ B が優れていることがわかる．グループ B は座学講義に加えて 90 分の演習講義を行っているので，純粋な学習時間は同一ではないが，試験問題をターゲットにした対策講義でなくとも正答率が上がるという実験結果を示しており，これらは実システムを用いた演習の効用を証明している．

5. おわりに

本報告では考案したネットワークセキュリティ教育方式の実装システムについて示し，実施した講義結果の評価を示した．今後は演習シナリオの改良と実施前後の効果測定指標を改善し，より効果的な教育システムの考案と厳格な定量評価を図る．

文　献

[1] 商務情報政策局 情報処理振興課 “IT 人材の最新動向と将来推計に関する調査結果〜報告書概要版〜”, 経済産業省, p9, June, 2016, Available: http://www.meti.go.jp/policy/it_policy/jinzai/27FY/ITjinzai_report_summary.pdf, Dec, 2018.

[2] 西村拓海, 中矢誠, 富永浩之 “情報セキュリティの導入教育を目的とした出題型ハッキング競技 CTF の環境構築と運用実践-高校生への試行実践の分析と問題編成の支援機能-”, 情報処理学会研究報告, Vol. 2018-CE-147, No.6, Dec, 2018.