1G-02

通信ネットワークにおける盗聴技術を題材としたアクティブラーニングシナリオ

干川　尚人†　　井手尾　光臣†　　石原　学†

国立高等専門学校機構　小山工業高等専門学校†

1. はじめに

現在の社会システム運用においてネットワークシステムが欠かせないが，これを支えるシステムエンジニアや情報セキュリティなどの ICT 人材の供給不足が進行しており，技術者教育の重要性が増している[1]．しかし，セキュリティスキルの醸成には，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不可欠であるため，机上の学習だけでは質の高い教育が困難である．また，その教材にも普及の容易なコスト性，教師の運用性も求められる．そこで本研究では通信盗聴の演習を題材にした安価で運用性の高い初学者向けのアクティブラーニングシナリオを提案する．本稿はこのシステム構成とシナリオを説明し，これを用いた授業実践結果を報告する．

2. 初学者向けネットワーク技術教育の課題

2.1. 学習対象者を取り巻く環境

近年の 10 代の学生は日常的にオンラインサービスを利用していることもあり，情報端末の利用スキルは高いが，それは必ずしもセキュリティリスクの理解度にはつながらない．これは目に見えるサービス利用の経験がシステムの仕組みを学ぶことにつながらないからだと考えられる．しかし，得意な端末操作によって身近なサービスなどの通信データの流れや潜むリスクを可視化できれば，実感の伴った効果的な教育成果を期待できる．

2.2. 実習型ネットワークシステムの演習

アクティブラーニングはグループワークや実践的実習による能動的な学びを誘発する手法である．その学習効果の高さが知られており，セキュリティスキルの習得にも有効だと考えられるが，一方でネットワークサービスを動かす演習システム教材を開発し，これを配備・維持することは容易ではない．そこで本研究グループの過去の取り組みでは，安価なシングルボードコンピュータ（以下 SBC）とスイッチングハブを用いた可搬性のある安価な演習教材を開発している[2]．この研究では普段身近な Web サイトサービスを攻撃する演習を通して学習者がサーバやネットワークの仕組みを学ぶ実践結果を評価しており，演習実施によって座学の学習者と比べて確認テストの成績がおよそ 15%向上する結果を示した．

しかし，この演習教材は複数の学習者が操作する端末群とサーバをつなぐネットワークシステムが必要で，その構築の要求スキルや準備時間の負担に加え，参加者全体で攻撃演習を行うシナリオ設計上，授業が学生の進行状況に影響されやすい点が問題であった．これは限られた教育リソースで短期間に効果的な指導実施する際の障害になるため，改善する教材とシナリオの考案が課題であった．

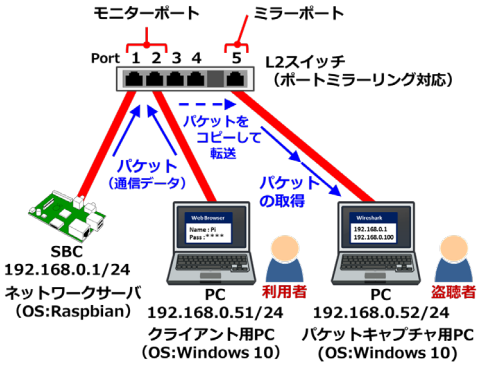

図 1 演習システムの概要

3. 通信盗聴を題材とした演習シナリオ

前述の課題解決のために，我々は通信盗聴の演習を行う演習システム教材を提案する．通信盗聴は暗号化なしの通信の危険性をわかりやすく示し，日常の利用で経験するパスワードなどの個人情報漏洩リスクとつながるため，利用者観点でも興味を引きやすい題材である．

3.1. 演習教材のシステム構成

通信盗聴の演習教材は図 1 に示す SBC，L2 スイッチ，2 台のパーソナルコンピュータ(以下 PC)，および 3 本のネットワークケーブルで構成される．1 台の SBC はネットワークサーバとして Raspbian（Raspberry Pi OS）を搭載した Raspberry pi3 または 4 を使用し，Web，ファイル転送，リモート接続，ファイル共有サービスを提供する Apache HTTP (Hyper Transfer Protocol)サーバ，FTP (File Transfer Protocol)サーバ，Telnet および SSH (Secure Shell)サーバ，Samba サーバを動作させる．2 台の PC はどちらも Windows10 を搭載し，これを学習者の操作端末として利用する．1 台はクライア

A Proposal for an Active Learning Scenario on the Subject of Eavesdropping Technology in Communication Networks
†Naoto HOSHIKAWA, †Mitsuomi IDEO, †Manabu ISHIHAR
†National Institute of Technology, Oyama College

表 1　グループごとの試験結果（最大スコア 20 点）

		授業前	授業後	スコア伸び値
グループ A（座学のみ）	平均値	12.3	14.8	2.5
	中央値	12	15	3
グループ B（座学と演習）	平均値	13.4	16.7	3.3
	中央値	13	17	4

ント用 PC としてネットワークサーバの各種サービスを利用するための Web ブラウザ，FTP クライアント，telnet および SSH ターミナルクライアントを使用する．もう 1 台はパケットキャプチャ用 PC として，ネットワークパケットアナライザソフトの Wireshark をインストールする．L2 スイッチは NETGEAR 製 5 Port Gigabit Ethernet Smart Managed Plus Switch GS105E を使用する．これは指定したモニターポート上のパケットデータをミラーポートにコピーして転送するポートミラーリング機能に対応しているので，これをパケットキャプチャ用 PC につなぎ通信盗聴する．本教材では 1，2 番をモニターポート，5 番をミラーポートとして設定している．

3.2. 指導シナリオ

本演習講義は高専生や大学生のネットワーク技術の初学者を対象に以下に示す 160 分で実施する．

A) ネットワークシステムの基礎知識（座学 15 分）
B) 演習システムの解説（座学 10 分）
C) Ping コマンド実習（演習 30 分）
D) ネットワークスイッチ技術の解説（座学 15 分）
E) ネットワーク盗聴実習（演習 90 分）

実習 E では演習教材を用いて次の項目を実施する．

- ping 通信の盗聴
- Web サイトへのアクセスの盗聴
- BASIC 認証（平文データ）による Web サイトのログイン ID とパスワードの盗聴
- リモート接続（telnet）の盗聴
- ファイル転送（FTP）の盗聴
- ダイジェスト認証（ハッシュデータ）による Web サイトのログイン ID とパスワードの盗聴
- 暗号化ありのリモート接続（SSH）の盗聴
- 暗号化ありのファイル転送（FTPS）の盗聴

この演習では教材を二人一組のグループ単位で利用し，学習者の一人がクライアント用 PC でサービスを利用し，もう一人がパケットキャプチャ用 PC で通信を盗聴する役割分担で進める．パケットキャプチャ用 PC は Wireshark で各種情報を確認し，情報が容易に漏洩する状況を理解する．

4. 実践の評価と考察

本シナリオで演習授業を実践し，全 20 問の 2 択の確認テストをそれぞれ授業前後に 10 分間実施し，その結果を評価した．なお，演習の実施有無による定着度の差を確認するため，座学のみのグループ A と，全て実施したグループ B を比較する．グループ

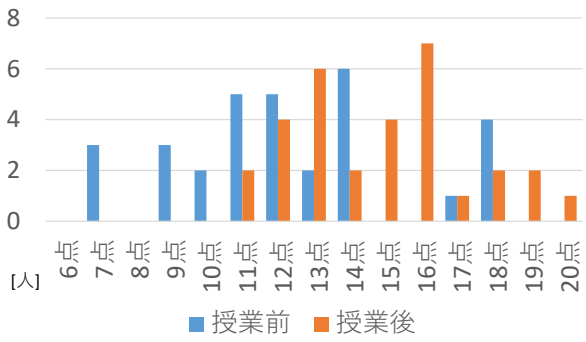

図 2 グループ A（座学のみ）

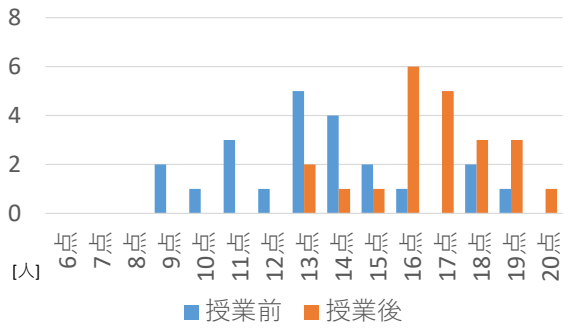

図 3 グループ B（座学と演習）

A は小山高専電気電子創造工学科の本科 5 年生計 31 名，グループ B は国立高等専門学校機構サイバーセキュリティ人材育成事業の特別授業参加者（本科 1 年生から 5 年生および専攻科 2 年生）計 22 名である．これらの確認テスト結果を表 1，またそれぞれのヒストグラム分析を図 2，図 3 に示す．グループ B は平均値，中央値ともにグループ A より授業後のスコアの伸び値が大きく，定着率の高さが示されており，ヒストグラム図からも高得点の割合が大きくなる傾向が確認できた．

5. おわりに

本報告では初学者向けのネットワークシステム教育教材とその実施シナリオについて示し，その実践学習の効果を明らかにした．今後は多くの教育現場で活用可能な教材を目指して改良を進めていく．

謝辞

本研究は電気通信普及財団電気通信普及財団(The Telecommunications Advancement Foundation)の支援を受けて進められている．

文　献

[1] 総務省，“データ主導経済と社会変革”，情報通信白書 ICT 白書，第 1 部， p.150, (2017).
[2] 干川 尚人，小林 康浩，石原 学，白木 厚司，下馬場 朋禄，伊藤 智義，“サービス拒否攻撃演習システムの実装とそのアクティブラーニングシナリオによるセキュリティ技術教育”，電子情報通信学会論文誌，Vol. J103-B, No.4, pp.180-183, (2019).