アクティブラーニングによるセキュリティ技術教育シナリオの開発と効果測定

代表研究者	干川　尚人	独立行政法人　国立高等専門学校機構 小山工業高等専門学校　電気電子創造工学科　准教授
共同研究者	石原　学	独立行政法人　国立高等専門学校機構 小山工業高等専門学校　電気電子創造工学科　教授
共同研究者	井手尾　光臣	独立行政法人　国立高等専門学校機構 小山工業高等専門学校　教育研究技術支援部 技術室　技術専門員

1 研究背景

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 Information and Communication Technology（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]．昨今は産業界の ICT 関連投資が増加するとともに，社会においてもデジタルトランスフォーメーション（DX）推進に伴い情報システムの需要は増加する一方である．それに対して供給の面では労働人口，特に若年層の減少が著しく，教育機関においては量をカバー可能な質の高い人材育成が求められている．

その中でも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．アクティブラーニング（能動的学習）は学習者が主体的に多くの操作を行い，多くの情報を獲得して統合的な知識や経験を得ることができるため，セキュリティスキルの学習に特に有望である．しかし，実践的なサーバコンピュータや多数の情報端末を配備した演習ネットワークシステムは高コストであり，またその構築・運用・保守も容易ではないことが課題である．幅広い対象へアクティブラーニングを可能にするためには，その教材は普及が容易なコスト性を持ち，更に教師が扱いやすい運用性も求められる．

2 研究報告

本研究は 10 代後半から 20 代前半の情報系の学問を学ぶ初学者に対して，そのセキュリティスキルの醸成に必要なネットワーク，コンピュータの総合的な技術習得を促進するため，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．本報告では考案したセキュリティ教材システムの構成とシナリオを説明し，これを用いた授業実践結果を説明する．

2-1 初学者向けネットワーク技術教育の課題

セキュリティ性とは情報システムごとにそれぞれ求められる性質であるため，情報システムそのものが理解できなければその十分な品質は得られない．しかし，情報システムを総合的に理解することは容易ではない．情報系人材を採用する通信インフラ事業者など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，いわゆる On the Job Training（OJT）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．

ネットワークセキュリティ分野の教育では，遊びの要素を活用することによって初学者の学習を促進させる取り組みがある[2]．しかし，これは大学などの専門教育を学ぶ前の学習の導入においては有効であるものの，実践的な知識習得にはギャップが大きい．一方で，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（CTF）の取り組みもある[3][4]．この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．しかし，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．そこで，初学者でも導入が容易な攻防演習型のセキュリティ教育教材も提案されている[5]．これは一般的なネットワークサービスの利用で身近な「サービス拒否攻撃」を題材にしたグループワーク形式の演習教材で，演習ネットワーク上のサービスサイトを協力して攻撃してサービス不能状態を作ることを目指しつつ，ネットワークサービス技術を学んでいくアクティブラーニングシナリオである．しかし，同教材システムは参加者が共通して利用するある種の演習ネットワークシステムを導入する必要があり，その環境構築，運用，トラブル時の切り分けなど実施者の負担が非常に大きい点が課題になる．これは，演習授業の進捗管理を著しく困難にさせ，また攻撃端末のノード数の設定も難しいことから，参加する学習者の人数も調整しづらい．そのため，教育指導の実施者観点の運用性を考慮したシナリオが求められる．

2-1-1 学習対象者を取り巻く環境

本取り組みの学習対象者は情報系の教育工程を学ぶ高校生から大学生の低学年（高専 1～5 年）を念頭に，将来情報システムの開発や運用，保守に携わる学生を想定している．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ばかりか，リスクの高い行動を取る可能性も高まる（図 1）．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．

図 1 近年の 10 代の学生の情報端末利用スキルの傾向

2-1-2 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[5]．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．

2-2 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．

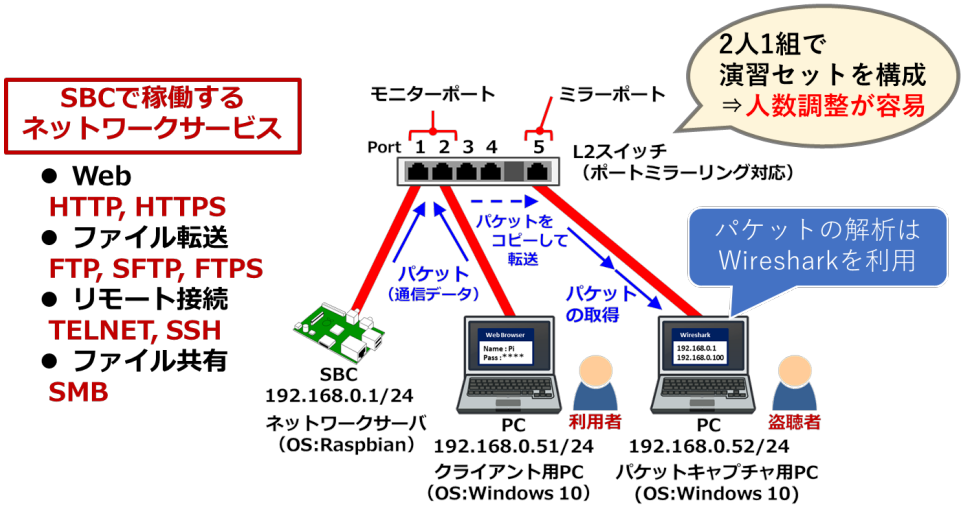


図 2 演習システムの構成および稼働するサービス

2-2-1 演習教材システムの構成

通信盗聴の演習教材は図 2 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．

2-2-2 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．

〈1〉　ping 通信の盗聴
〈2〉　Web サイトへのアクセスの盗聴
〈3〉　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
〈4〉　リモート接続（telnet）の盗聴
〈5〉　ファイル転送（FTP）の盗聴
〈6〉　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
〈7〉　暗号化ありのリモート接続（SSH）の盗聴
〈8〉　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．

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

2-3 実践の評価と考察

2-3-1 シナリオ実践による評価

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[付録 A]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 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 3，図 4 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．

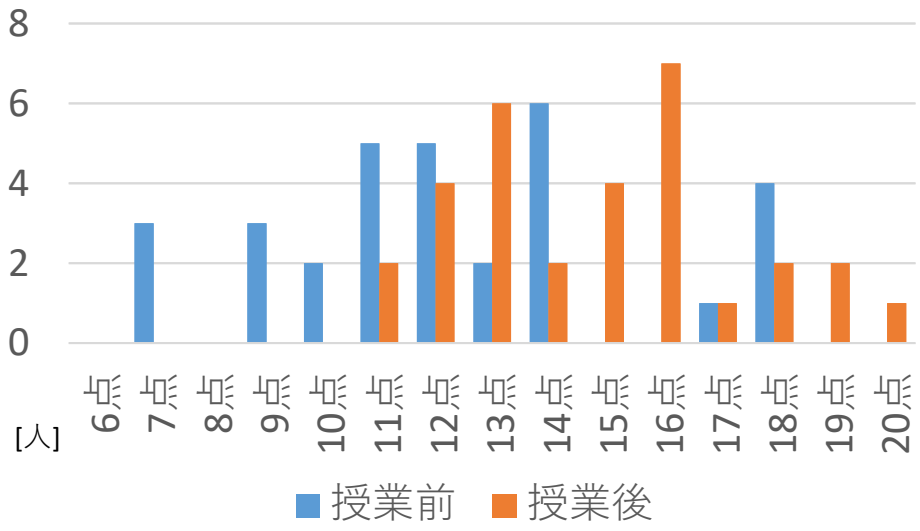


図 3 グループ A（座学のみ）

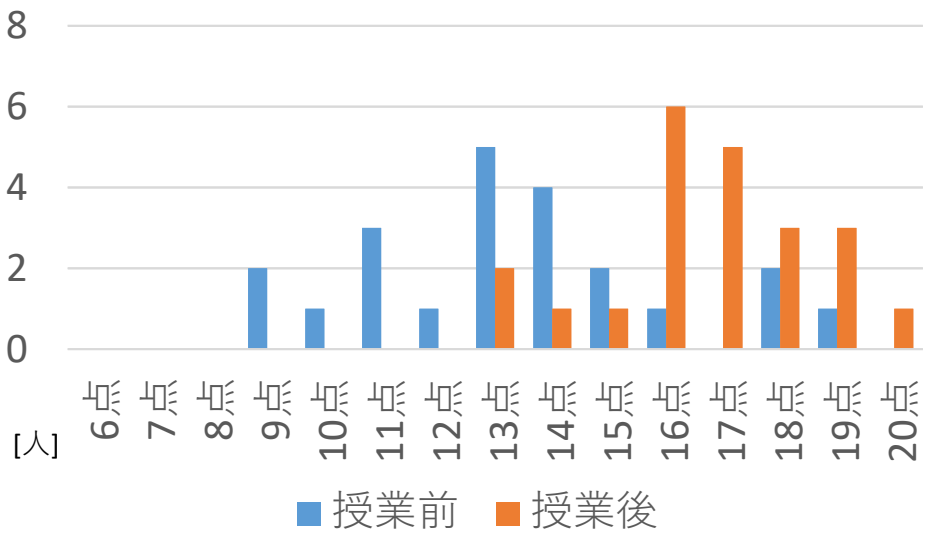


図 4 グループ B（座学と演習）

2-3-2 教材システムの運用性

本教材は 1 つのセットに対して 2 名グループで演習を行うため，学習者の参加人数は 2 の倍数で設定できる．また，それぞれのセットはサーバとネットワーク機器，端末が接続された独立したネットワークシステムとして運用できるため，グループ数は演習ネットワークシステムの構築に影響しない．これは従来のシステム[5]と比べたとき，教育指導者のシステム運用を簡便にする効果をもたらすと共に，学習者ごとのシナリオ実施の遅延の影響も抑制可能である（ある程度分離できる）．また故障などのトラブル発生時も教材セットを交換することで対応できる．そのため，本提案はネットワークシステムの総合的な動作を学ぶことができる教材ながら，優れた運用性を保つことができると言える．

2-3-3 実装システムの導入性

本教材のセットは 2-2-2 節で示した通り，SBC と L2 スイッチをそれぞれ 1 台で構成される．本取り組みでは試作の段階では SBC として Raspberry pi3B+を採用し，システムイメージを開発したが，後に機器の入手性を考慮して Raspberry pi4 にも対応できるイメージも作成した．演習のネットワークは独立しているため，ネットワーク設定やアプリケーションのインストールを済ませた SBC のイメージは一度作成すれば後は microSD カードへイメージデータを展開するだけで，容易にそのレプリカを作成できる．これらの SBC は 1 台 10,000 円前後で入手可能であり，供給量も十分なので調達性にも優れている．

L2 スイッチとして採用した NETGEAR 製 5 Port Gigabit Ethernet Smart Managed Plus Switch GS105E は 5,000 円程度で入手可能なネットワーク管理性能に優れたネットワーク機器である．通信の優先制御（QoS）機能や IEEE802.1Q 規格に準拠したタグ VLAN 機能に加え，通信パケットを複製するポートミラーリング機能を設定できる．このような機能は通信インフラ事業などで使われるエンタープライズ向けネットワークアプライアンス機器では一般的だが，安価な民生用機器では珍しい．本教育シナリオにおける通信盗聴はこのポートミラーリング機能が不可欠であるが，この設定もブラウザ画面ベースの管理画面で容易に設定が可能である．

これらの教材セットを構成する機器群は，導入するイニシャルコストが優れていることに加え，構築の容易性を有しており，高い導入性がある．学習対象者の規模に合わせて機器の数も調整できるため，初学者向けのセキュリティ教育を行おうとしている教育機関にとって最適である．

2-4 結論と今後の展望

2-4-1 本取り組みの成果

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．併せて，教材セットの構成方法を示すことで，提案コンセプトに基づくアクティブラーニング教育実施に必要なノウハウを展開できた．

2-4-2 今後の展望

本教育研究の取り組みにおいて，将来多くの教育現場で活用可能な教材を目指すためにその完成度を高め，より実用性を上げるために，次に着手すべき 2 つの項目を説明する．

1 つは本教材を用いた授業実施数を増やすことである．2020 年はコロナ感染症の影響があり，特に機器を直接操作するグループ演習スタイルの授業実施が非常に困難だったため，十分な対策を採りつつ行えた試行は 1 回に限られている．今後，コロナ感染症の影響が収まり次第，本校の情報系学科の授業科目や，全国高専生向けの特別授業を開講するなど，実施数を増やしていくことで，改良を進めていく．

また，効果測定についての改良も必要である．今回は座学講義内容の情報も抽出して[付録 A]に示すような選択式問題を作成し，これを評価に使用した．評価指標としての妥当性をより高めるためには，より客観的なスキルを把握できるような問題に改善する余地があると考える．一方で，授業ごとに実施する効果測定試験は授業時間を減らす問題があり，なるべく簡便な実施スタイルが実現することが望ましい．今後は授業前の実施やオンライン形式の出題など，試験実施方法についても改善を検討していく．

【参考文献】

[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] Mark Gondree, Zachary N.J. Peterson, and Tamara Denning，“Security through play,”IEEE Security & Privacy, Vol.11, No.3, pp.64-67，2013.

[3] 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.

[4] 湯川誠人，井口信和，“仮想マシンを用いた攻防戦型ネットワークセキュリティ学習支援システムにおけるネットワーク型 IDS を用いた不正侵入シナリオの実装,”情報処理学会 インターネットと運用技術シンポジウム 2018，pp.92-99，Dec, 2018.

[5] 千川 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.

〈発 表 資 料〉

題　　名	掲載誌・学会名等	発表年月
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	情報処理学会 第83回全国大会, 1G-02, pp.4-367-368	2021 年 3 月 18 日

-Appendix-

[付録 A] 評価で用いた問題

■問 1　通信端末から ID とパスワードを用いて Web アプリケーションサービスへログインする際，ID，パスワードの漏洩を防ぐために必要な措置を**全て**答えよ

1. 端末はパーソナルファイアウォールで保護し，内部から外部への ID，パスワードの漏洩を防ぐ

2. Web サービスとは HTTPS 通信で接続する

3. SSL/TLS 通信で用いるサーバ証明書がクライアント側でエラーが無いことを確認する

4. 発行済みセッション ID を HTTP レスポンスボディ中のリンク先の URI のクエリ文字列に設定する

■問 2　IP 通信サービスについて正しいものを**全て**答えよ.

1. サービスを提供するコンピュータまたはソフトウェアをサーバ，利用者が使うコンピュータまたはソフトウェアをクライアントと呼ぶ.

2. HTTP（Hypertext Transfer Protocol）はテキスト形式のプロトコルで，Web ブラウザが Web サーバの 80 番ポートに接続して要求し，これに対して Web サーバが該当するコンテンツを応答として返す処理で成り立つ

3. HTML（HyperText Markup Language）は欧州電子計算機工業会(ECMA: European Computer Manufacturers Association)が標準化を進めている Web ページ上でプログラム処理を行うためのプログラミング言語である

4. IP アドレスは通信サービスを識別するために使う番号で，SSH は 22，DNS は 53，HTTP は 80，POP は 110 のように代表的なサービスごとに予約された well-known 番号と独自に利用可能な番号に分かれている

■問 3　ping コマンドについて正しい文章を**全て**答えよ.

1. ネットワーク疎通を確認したいホストに対して IP パケットを発行し，そのパケットが正しく届いて返答が行われるか確認するためのコマンドである

2. 通信プロトコルとして TCP/IP を利用し，相手ホストとのコネクションを確立して通信先ホストが確実に存在するかどうかを確認できる

3. ping コマンドの宛先ホストから応答がない場合，通信相手がダウンしていることがわかる

4. Windows，macOS，Linux など，さまざまなコンピュータの OS プラットフォームだけでなく，スイッチングハブやルータなどのネットワーク機器でもその機能を備えていることが多い

■問 4　Web アプリケーションサービスにおける暗号化について，正しいものを**全て**答えよ

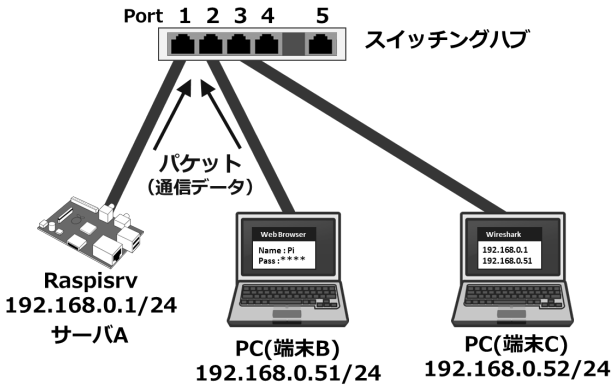
1. HTTP 通信では ID およびパスワードを平文で送信すると盗聴される可能性があるため，文字列を BASE64 で符号化する BASIC 認証を用いることで安全を担保できる

2. HTTP 通信において暗号化によるデータ保護性で BASIC 認証はダイジェスト認証より優れているが，対応していないブラウザがある点が問題である

3. SSL/TLS による HTTPS 通信では通信データを暗号化されるので，通信データに含まれている ID およびパスワードも同様に暗号化されている

4. SSL/TLS による HTTPS 通信ではクライアント側で検証できない証明書（オレオレ証明書）が使われている場合であっても，その通信データは暗号化されている

■問 5　図に示す通り，スイッチングハブの物理ポート 1 にサーバ A，物理ポート 2 に端末 B，物理ポート 3 に端末 C が接続されている．次の文章のうち，正しい選択肢を**全て**答えよ



1. 端末 B とサーバ A で送受する通信パケットは端末 C も常に受信できる

2. 端末 B とサーバ A で送受されている通信パケットは暗号化されている

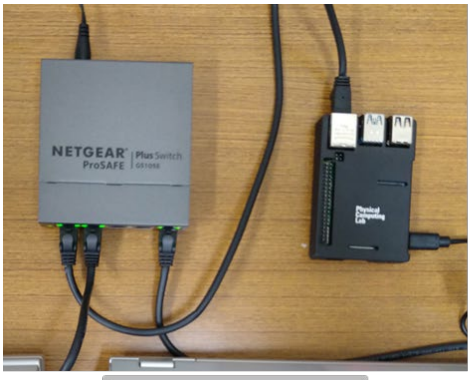
3. 物理ポート 1～2 と物理ポート 3 のネットワークは仮想的に分かれている

4. スイッチイングハブが物理ポートの接続先機器 MAC アドレスを学習した後は，該当しない送信先の物理ポートへはパケットを流さない

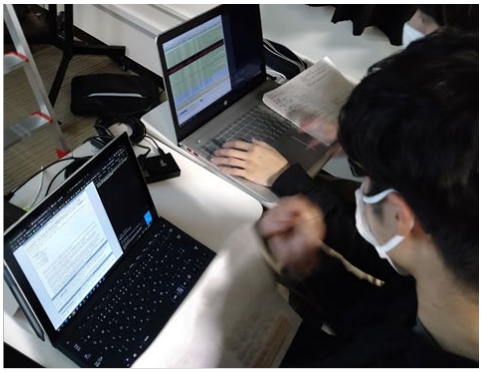
【解答】
問 1. 1×, 2○, 3○, 4×
問 2. 1○, 2○, 3×, 4×
問 3. 1○, 2×, 3×, 4○
問 4. 1×, 2×, 3○, 4○
問 5. 1×, 2×, 3×, 4○
○×の正答数をスコア 20 点と換算する

[付録 B] 教材セットの構成で用いた機器類

物品のカテゴリ	詳細
ポートミラーリング機能付き L2 スイッチングハブ	NETGEAR GS105E-200JPS
マイクロ SD カード	microSDHC 16GB Class10
シングルボードコンピュータ	Raspberry Pi4 4GB, Raspberry Pi3 1GB
情報端末	Windows PC（サービス利用者，盗聴者それぞれ 2 台）
ネットワークケーブル	イーサネットケーブル Cat5e，Cat6



演習教材セット



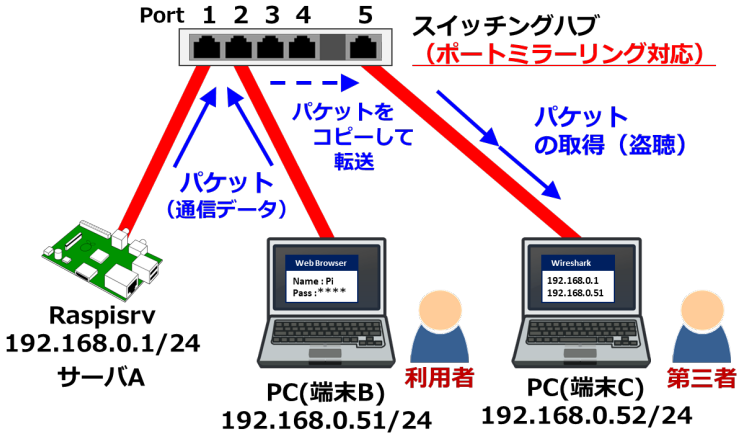
演習の風景

教材の実機写真および実施風景

[付録 C] 盗聴演習のシナリオ

ポートミラーリングで通信盗聴

スイッチングハブのポート 5 番はポートミラーリング設定されています. これを用いて, 端末 C でサーバ A と端末 B の通信データを盗聴しましょう.



サーバ A, 端末 B 間で行われる通信を端末 C でネットワークアナライザを用いてパケットキャプチャして, 内容を分析しよう

演習 1:ping の盗聴

【端末 B】

・コマンドライン（cmd）から, 192.168.0.1 へ ping を打つ

【端末 C】

・Wireshark を起動し, ip.addr == 192.168.0.51 でフィルタする

演習 2:Web アクセスの盗聴

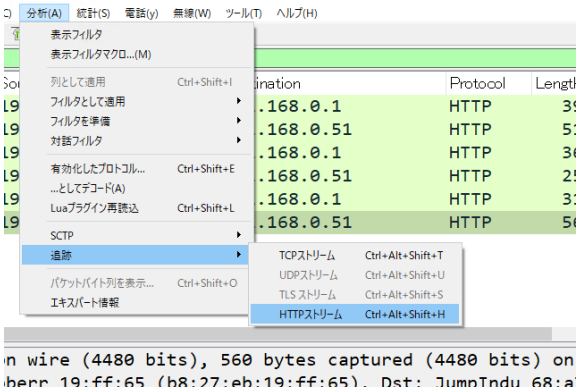
【端末 B】

・Web ブラウザを開き, 192.168.0.1/index.html へアクセスする

【端末 C】

・Wireshark を起動し, ip.addr == 192.168.0.51 and http でフィルタする

・分析→追跡→HTTP ストリームを選択,
save as...を選択し,
index.html と名前を
付けて保存.
これを開いてみる.



Wireshark の画面表示例

演習 3：Web の ID，パスワードの盗聴
【端末 B】
・Web ブラウザを開き，192.168.0.1/basic/へアクセスする
・ユーザ名：○○，パスワード：××を入力する
【端末 C】
・Wireshark を起動し，ip.addr == 192.168.0.51 and http でフィルタする
・BASIC 認証通信をしているパケットを探し，通信で入力された文字列を探し，復号化する

演習 4：telnet の盗聴
【端末 B】
・rlogin を開き，telnet でサーバへログインする
  ホスト設定：192.168.0.1
  ユーザ名：○○
  パスワード：××
・適当に操作する（ls，pwd などの Linux コマンドを使うなど）
【端末 C】
・Wireshark を起動し，ip.addr == 192.168.0.51 でフィルタする
・分析→追跡→TCP ストリームを選択する．通信内容を確認し，ユーザ名，パスワードほか，端末 B が行った操作を解析する．

演習 5：FTP の盗聴
【端末 B】
・FFFTP を開き，下記の設定でサーバへログインする
  ホスト設定：192.168.0.1
  ユーザ名：○○
  パスワード：××
・画像フォルダから一つのファイルをダウンロードする
・ダウンロードしたファイルを開き，中身を確認する
【端末 C】
・Wireshark を起動し，ip.addr == 192.168.0.51 and ftp-data でフィルタする
・Info を参考に，画像ファイルのダウンロードをしている行を選択．右クリックして，分析→追跡→TCP ストリームを選択する．「データを表示して保存する」の形式を「Raw（無加工）形式」に変更し，Save as...を押してファイル名を指定（test.png または test.jpg）して保存する．
・保存ファイルを開き，端末 B と同じ画像か確認する．

応用演習（※演習時間が余ったグループへの課題）
暗号化した場合，どんなデータが盗聴できるか，実際に試してみよう
その①：telnet を SSH に変えるとどうなるか？
その②：Web アクセスの BASIC 認証をダイジェスト認証に変えるとどうなるか？
その③：FTP を「暗号化あり（FTPS）」にするとどうなるか？