TCP/IP ネットワークの理解を促進する 無線パケットキャプチャ演習の開発と実践

鈴木大助[†1]

概要：本研究の目的は，TCP/IP ネットワークの理解を促進するための無線パケットキャプチャ演習を開発・実践し，その効果を明らかにすることである．本演習において受講生は，自分の PC にインストールしたパケットキャプチャソフトを使って，外部 WEB サーバとの HTTP 通信において送受信される無線パケットをキャプチャする．ワークシートに基づいて各種アドレスを記録するワークを行い，また，コマンドプロンプト上で各種コマンドを実行しネットワーク経路図を完成させる．確認テストを演習の事前事後に行ったところ，有意ではないもののある程度平均点の向上が見られた．また，受講生自身による事後自己評価では，「ある程度できる」「できる」と評価する受講生は半数程度にとどまったが，当該受講生の自由記述からは演習を通じて理解が進んだ様子がうかがえた．本演習は TCP/IP ネットワークの理解を促進しうると考えられる．

キーワード：TCP/IP ネットワーク，プロトコル，能動的学習，パケットキャプチャ，Wireshark

Development and Practice of a Wireless Packet Capture Exercise to Facilitate Students' Understanding of TCP/IP Network

DAISUKE SUZUKI[†1]

Abstract: This study aims to develop a wireless packet capture exercise and to clarify the effect of the exercise to facilitate students' understanding of TCP/IP network. In this exercise, students use a packet capture software installed on their own PC to capture wireless packets sent and received in HTTP communication with an external web server. Students record various addresses on the worksheet, and execute various commands on the command prompt to complete the network route map. Results of the confirmation tests conducted before and after the exercise showed that, although it was not significant, the average score was improved to some extent. Students' post self-assessment showed that, with respect to every specific behavioral objective, only about half of the students assess themselves good or excellent. Their free descriptions, however, indicated that their understanding of TCP/IP network had progressed. It indicates that the exercise has the potential to facilitate students' understanding of TCP/IP network.

Keywords: TCP/IP network, protocols, active-learning, packet capture, Wireshark

1. はじめに

現代のビジネスや日常生活は情報ネットワーク，特に TCP/IP ネットワークに支えられており，現代の社会人は基本的な素養として TCP/IP に関する知識をある程度身につけていることが望ましい．TCP/IP ネットワークをはじめとする情報ネットワークは，一般情報教育の知識体系（GEBOK2017.1）の知識エリアのひとつに位置づけられており，大学の一般情報教育において学習することが期待される分野である[1].

しかし，講義や問題演習のみで TCP/IP ネットワークを理解することは，特に初学者にとっては簡単ではない．その目で自分が実際に見たこともないパケットやフレームの存在を認知し，それらが従うプロトコルを机上の学習のみで理解しようとしても理解が曖昧になりやすい．確かな理解のためには実験・実習を取り入れることが望まれる．

実験・実習についてはいくつかの方法が考えられる．ルータやスイッチ等の機器を用いたネットワーク構築演習はネットワークの理解に有効である．しかし，機器の準備や設定に費用や手間がかかるため，授業のクラスサイズや予算によってはいつでも最善の方法というわけではない．

Cisco Packet Tracer 等のシミュレータを用いる演習は，自由に使用できる PC さえあれば実施可能であり，学習効果も見込める[2]．しかし，あくまでシミュレーションであって実際の通信を扱う体験とは異なる．特に初学者であれば，一度は本当の通信におけるパケットをその目で見て学ぶ経験をすることが望ましい．

アンプラグドな学習活動も初学者には有効である．筆者は TCP/IP ネットワークを学習する一つの学習手法としてロールプレイ演習を考案した[3][4]．演習において，受講生はルータやスイッチ等のネットワーク機器や PC の役割を演じ，パケットやフレームを象徴する入れ子構造の箱を通信プロトコルにしたがって受け渡すことでネットワーク通信を再現する．これはデータリンク層およびネットワーク層に関するプロトコルやネットワーク階層構造の理解，ネットワーク機器の役割理解を促進する顕著な効果が見られ

†1 北陸大学
Hokuriku University

た．しかし，この学習法も通信を模擬して理解する方法である．この方法とは別に，実際の通信を見て学ぶ経験をすることが期待される．

Wireshark 等のパケットキャプチャソフトを用いた演習は，自由に使用できる PC と通信環境さえあれば実施可能であり，実際にネットワーク上を流れているパケットを取り込んで，その目で見て学ぶことが可能である．パケットキャプチャソフトの利用がパケットやフレームの存在の認知および通信プロトコルの学習の助けになると期待される．

筆者は，学生の TCP/IP ネットワークに対する理解を促進するため，Wireshark を利用して無線パケットをキャプチャ・分析する演習を考案・実践した．本研究は考案した演習の効果を，受講生自身による自己評価アンケートおよび客観テストを通じて明らかにすることを目的とする．

2. 演習環境

無線パケットキャプチャ演習で想定するネットワーク概略図を図 1 に示す．左の枠で囲まれた範囲が本演習を実施する教室のネットワークを表す．なお，本稿図中でネットワーク機器を表すアイコンは Cisco のネットワークトポロジーアイコン[5]を用いている．

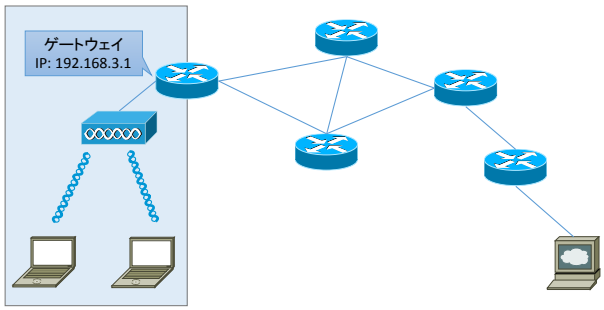

図 1　ネットワーク概略図

受講生はひとり 1 台 Windows ノート PC を専有している．受講生はパケットキャプチャソフト Wireshark を各自の PC にインストールし，自分の PC が送受信するパケットをキャプチャする．ノート PC は演習室内に設置された無線 LAN アクセスポイントに WPA2-PSK にて接続している．演習室に設置されたルータが DHCP サーバとして機能しており，各ノート PC は DHCP クライアントとして 192.168.3.0/24 の範囲の IP アドレスを与えられる．

ルータの演習室内側インターフェイスは各ノート PC から見たデフォルトゲートウェイであり，IP は 192.168.3.1 である．ルータは，NAT 機能を提供しており，演習室内 PC はこのルータを経由して，上流である学内 LAN へ接続可能であり，学内 LAN を経由してさらにインターネットへ接続することも可能である．

3. 無線パケットキャプチャ演習

3.1 本演習授業の目的と到達目標

本演習授業の目的は「ARP やデフォルトゲートウェイといった仕組みがどのように IP 通信を支えているかパケットキャプチャに基づいて理解する」ことであり，具体的な到達目標として以下の四つを挙げている．

1. 管理者権限でコマンドプロンプトを使用し，MAC アドレスや IP アドレスの確認および ARP テーブルの削除や確認ができる
2. Wireshark を用いてパケットをキャプチャし，適切なフィルタを施し，ARP パケットや HTTP パケットを抽出できる
3. 同じネットワーク内での通信における ARP の意義を説明できる
4. 異なるネットワーク間の通信におけるルータの役割を説明できる

なお，MAC アドレスや IP アドレスの確認，ARP テーブルの確認については管理者権限不要であるが，演習作業中に ARP テーブルの削除等で管理者権限が必要になる場面があるため，管理者権限でのコマンドプロンプト使用ができるようになることを求めている．

演習は 90 分一コマで実施することを前提としており，各種 IP アドレス等調査，HTTP 通信のパケットキャプチャ，キャプチャデータ分析，ネットワーク経路調査，ARP リクエストパケット分析，ワークシートの記入・提出からなる．なお，時間中に終わらない作業については宿題とする運用とした．また，Wireshark のダウンロード・インストールと基本的な使用法の確認については別の回にあらかじめ実施する．演習の内容について以降の節で順に説明する．

3.2 Wireshark の使用法

本報告の便宜のため，Wireshark の使用法について説明する．図 2 は，受講生への説明のために，Wireshark User's Guide[6]の図に日本語の吹き出しを付加したものである[7]．

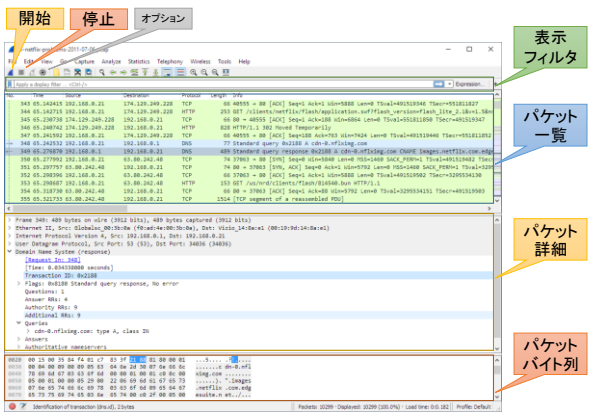

図 2　Wireshark キャプチャ画面構成 [7]

開始ボタンを押すと，キャプチャされたパケットがパケット一覧に次々に表示される．パケット一覧において任意のパケットを選択すると，下のペインに選択したパケットの詳細やバイト列が表示される．表示フィルタにおいて「arp」や「http」など，プロトコル名を入力すると該当するパケットだけがパケット一覧に表示される．

3.3 WEB サーバ，ゲートウェイ，クライアントの IP アドレス等調査

本演習は，各自の PC とインターネット上の WEB サーバとの間の HTTP 通信パケットをキャプチャし，そのデータの分析を通じて TCP/IP ネットワークを理解するという演習である．

まず，各自の PC において，コマンドプロンプトを起動し，「nslookup」を用いて通信先 WEB サーバのドメイン名に対応する IP アドレスを調査する．続いて，「ipconfig /all」を実行し，クライアントである自分自身の PC の NIC 設定情報を図 3 に示すワークシートに記入する．さらに「arp -a」を実行し，デフォルトゲートウェイの MAC アドレスを調査・記録する．

Wireless LAN adapter ワイヤレス ネットワーク接続	
物理アドレス（MACアドレス）	
IPv4 アドレス	
サブネットマスク	
デフォルト ゲートウェイ	
DNSサーバー	

図 3　NIC 設定情報の確認ワークシート

3.4 HTTP 通信のパケットキャプチャ

Wireshark を起動し，無線 LAN アダプタを選択してキャプチャを開始する．次に，Chrome 等 WEB ブラウザにおいて URL を直接入力し，指定したインターネット上の WEB サーバと HTTP 通信を行う．適当に閲覧したりリンクをクリックしたりなどブラウジングしたのち，キャプチャを終了しデータを保存する．

3.5 キャプチャデータ分析

3.4 でキャプチャしたデータに対して「http」で表示フィルタリングを行い，HTTP リクエストパケット「GET / HTTP/1.1」について MAC アドレス，IP アドレス，TCP ポート番号等を図 4 に記録する．この際，それぞれの値が何を指しているか，3.3 で実施した記録と照合したり，自分で調査したりして解答する．HTTP レスポンスパケット「HTTP/1.1 200 OK」についても同様のワークを行う．なお，標準的な Windows PC において Wireshark で無線 LAN パケットをキャプチャした場合，Ethernet II の仮想ヘッダが表示される[8]ため，それを記録する運用としている．

項目名	アドレス／値	どこのアドレスか／なんの値か pp.18-20と照合の上解答せよ
Ethernet II, Src:		
Ethernet II, Dst:		
IPv4, Src:		
IPv4, Dst:		
TCP, Src Port:		
TCP, Dst Port:		
HTTP		

図 4　HTTP パケットの確認ワークシート

3.6 ネットワーク経路調査

コマンドプロンプトで「tracert」を実行し，目的 WEB サーバまでのルートを調査する．また，tracert で判明したルータのうち最も目的サーバに近いルータの IP について，APNIC Whois で所有者／所在地を調査し，既に調査した情報と合わせて図 5 ネットワーク経路図の空欄を埋める．

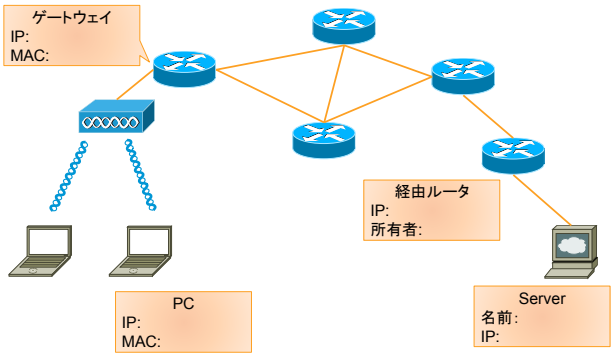

図 5　ネットワーク経路図

3.7 ARP リクエストパケット分析

3.4 でキャプチャしたデータに対し，「arp」や「arp.opcode == 1」などで表示フィルタリングを行い，図 6 に各種アドレスを記録する．

PDU		項目名	説明	値
フレーム		Destination:	フレームの宛先MACアドレス	
		Source:	フレームの送信元MACアドレス	
		Type:	パケットのデータタイプ	ARP (0x0806)
	ARPパケット	Opcode:	要求（1）	
		Sender MAC address:	送信元MACアドレス	
		Sender IP address:	送信元IPアドレス	
		Target MAC address:	ターゲットのMACアドレス	
		Target IP address:	ターゲットのIPアドレス	

図 6　ARP リクエストパケットの分析

3.8 ワークシートの記入・提出

受講生は最後に，ワークシートの問題に取り組んで提出する．問題は以下の 9 問である．

1. ドメイン名から IP アドレスを知るためのプロトコルをなんというか
2. クライアント PC がデフォルトゲートウェイの IP アドレスや DNS サーバの IP アドレス，自分の IP アドレスを自動で取得するためのプロトコルをなんというか
3. IP アドレスから MAC アドレスを知るためのプロトコルをなんというか
4. 自組織外の WEB ページ閲覧に伴う HTTP リクエストにおいて, 宛先 IP アドレスは当該 WEB サーバであるが，宛先 MAC アドレスはどこのアドレスか
5. 自組織外の WEB ページ閲覧に伴う HTTP レスポンスにおいて, 送信元 IP アドレスは当該 WEB サーバであるが，送信元 MAC アドレスはどこのアドレスか
6. 無線 LAN 通信においてあなたの PC 宛てのデータは電波に乗って教室中の PC に届くが，あなたの PC だけが受信するのはどのような仕組みによるか
7. 有線 LAN 通信の場合，あなたの PC 宛てのデータに対してスイッチはどのように働くか
8. 記録した ARP リクエストは「どこから」「どこに」「なんのために」送信されたものか
9. ARP リクエストは外部ネットワークに対して可能か

これらの問題はワークシートのワークの内容と対応しており，ワークを単純作業として終わらせず，学生各自がワークの意味を考えなおしたり，これまでに学習した内容を改めて調べなおしたりするきっかけとする狙いがある．

4. 実践方法

本演習の実践は，2019 年度北陸大学経済経営学部 3 年前期科目「ネットワーク論 I」において行った．本科目の授業スケジュールを表 1 に示す．

表 1 「ネットワーク論 I」授業スケジュール

授業回	授業内容
1	イントロダクション
2	イーサネット（データリンク層以下）
3	TCP/IP（ネットワーク層）
4	TCP/IP（トランスポート層以上）
5	事前テスト／Wireshark準備
6	無線パケットキャプチャ演習
7	事後テスト／ケーブル作成説明
8	ケーブル作成
9	実機操作の説明
10～15	実機演習
16	期末試験

全 16 回のうち第 5 回に事前準備と事前テスト，第 6 回に無線パケットキャプチャ演習，第 7 回に事後テストを実施する．

受講生は日本語と IT 専門学習のために中国から来た編入留学生 3 年生 8 人で，受講段階では，日本語能力は日本語能力試験 2 級レベルである．ネットワークについては，第 2 回でデータリンク層以下，第 3 回でネットワーク層について講義を受けており，本演習までに MAC アドレスや IP アドレス，ARP，デフォルトゲートウェイについて一通り学んでいる．

5. 評価方法

ネットワークに関するテストを演習の事前と事後で行い，その変化によって演習の効果を測定した．なお，事前・事後テストはロールプレイ演習[3][4]および有線パケットキャプチャ演習[7]と同一の問題を用いている．問題の詳細な説明は文献[3][4][7]に譲るが，報告の便宜のため重複を厭わず，その概要について以下記載する．

事前テスト･事後テストともに選択問題 20 問からなり，1 問 5 点の 100 点満点とする．問題は ping-t [9] 最強 WEB 問題集 CCNA Routing and Switching (v3.0) の中から CCENT 範囲のうち「ネットワーク基礎」「OSI 参照モデル」「TCP/IP」「スイッチング」「ルーティング」から抜粋して出題する．さらなる詳細については文献[3][4][7]を参照されたい．

また，本演習終了後に自己評価アンケートを実施した．3.1 節で提示した 4 つの授業到達目標のそれぞれについて「1. できない，2. あまりできない，3. ある程度できる，4. できる」で回答を求めたほか，重要だと思った点，疑問に思った点，感想等を自由記述で求めた．

6. 結果と考察

6.1 受講生のワーク取り組み状況

元々は，最初に演習の流れを説明した後は，配布したワークシートの指示を読みながら各自のペースでワークに取り組んでもらい，授業担当教員である筆者は机間巡視・質問対応を行う予定であった．

しかし，実際に演習を開始してみると，自分で指示を読み解きながらワークを進めることができる受講生がいる一方で，ワークシートの指示が読めない受講生や，何をすればよいかわからず戸惑う受講生も少なからずおり，ある程度ペースをそろえて演習を進めざるを得なかった．筆者がコマンドプロンプトを開いて見せたり，必要なコマンドを打って見せたりすることで，見様見真似でなんとか取り組むという形で演習を進めざるを得ない受講生もいた．

最終的には，すべての受講生が，各種アドレス調査やパケットキャプチャとその分析, ネットワーク経路調査, ARP

リクエストパケット内のアドレス記録等の作業を終えることができた．

ワークシートの確認問題については，配布資料を見ればわかるよう説明を記載しており，計画当初は受講生各自で宿題として取り組む予定であった．しかし，自分では資料を読み解けない受講生もおり，自学自習ではなく後日に一斉授業のような形で対応せざるを得ない場面が生じた．

意図した運用ではなかったものの，結果的にすべての受講生がワークシートの作業を完了するに至った．

6.2 事前・事後テスト結果

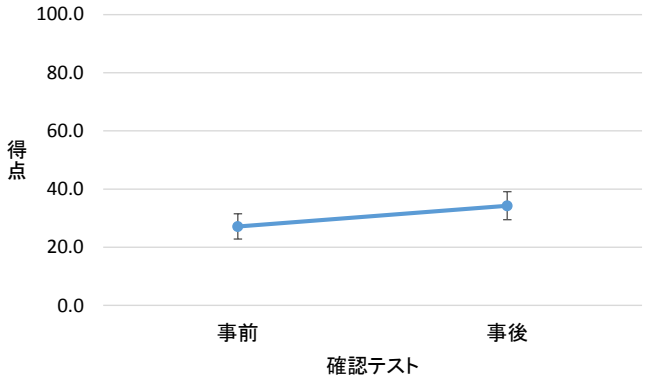

図 7 平均点の推移

事前テスト・事後テストの両方を受験した学生 7 人に関して，平均点の推移を図 7 に示す．なお，エラーバーは標準誤差である．

平均点は 27.1 点から 34.3 点へと 7.2 点向上している．しかし，事前と事後で対応のある t 検定を行ったところ，t 値 =-1.26 であった．有意水準を 5%（両側検定）とすると，P 値 = .25 となり，棄却されない．結局，事前から事後にかけて平均点がある程度向上したものの，統計的には有意ではないという結果となった．

6.3 受講生自身による事後自己評価

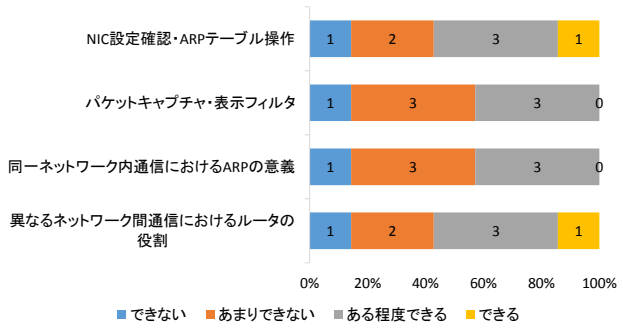

図 8 受講生自身による事後自己評価

演習終了後の受講生自身による達成目標別の自己評価結果を構成比グラフの形で図 8 に示す．グラフ上の数値はそれぞれの実解答人数である．どの達成目標においても，「ある程度できる」「できる」と自己評価する学生の割合は半数程度にとどまっている．評価が低い理由を明らかにすべく，自由記述回答の内容を精査する．

すべての項目について「できない」と回答した受講生は，「重要だと思った点」「疑問に思った点」において，難しくて理解できない，この科目は得意ではない旨回答しており，「自由感想」では，個人的な理由により勉強に集中できない旨を述べていた．すべての項目について「あまりできない」と回答した受講生は，日本語が得意ではないので理解できない，難しい，と訴えていた．

一方で，ほぼすべての項目で「ある程度できる」と回答している受講生は，「自由感想」において「LAN の利用がもっとよく理解できました」「データ転送プロセスで必要なデータとアドレスをさまざまな方法で見つけることは非常に興味深いです」と述べており，演習を通じた学習の効果が窺える．疑問点として，「ARP の役割」「たくさんの専門名称があります．例えば，ハブとスイッチの区別は難しいと思っています」が挙げられていた．

「できない」「あまりできない」と回答する受講生は，日本語で提示される専門用語の理解に困難を示していること，「ある程度できる」と回答する受講生は，日本語で示された専門用語を理解した上で，演習における操作と結果の意味を理解していると思われる．

6.4 本演習の効果と課題

ある受講生については，確認テストのスコアが 35 点から 60 点へと上昇していた．当該受講生は，ワークシートの作業にしっかり取組み，ワークシートの確認問題についてもほぼ的確に解答していた．演習を通じて成績が向上しており，この点からは本演習がネットワークの理解を促す効果がうかがえる．

一方で，ワークシートに自力で取り組むことができず，見様見真似で作業した受講生もおり，当該受講生の成績は伸びていない．言語の壁が大きいのはおそらく間違いなく，受講生の母国語に翻訳した資料を用意し，受講生の母国語で説明することで，理解が改善されるであろうことは想像される．しかし，この問題はネットワークの教育法とは別の次元の問題であるため，本稿ではこれ以上取り上げない．

ARP に関するワークの取り扱いについては検討が必要である．送信元ホストは，フレームの宛先 MAC アドレスがわからない場合に宛先 MAC アドレスをブロードキャストにして ARP リクエストを行う．本演習と確認問題はその事実について受講生が学習済みであることを前提としているが，本演習の結果からその事実を思い起こす過程について受講生は困難を感じるようである．また，ARP リクエストの宛先は本来的にはブロードキャストであるが，ARP テーブルエントリの保持のためにユニキャストでリクエスト

を行う場合がある. ユニキャストで送信される ARP リクエストについて説明する必要があり, 混乱を招く要因となる. 以上より，ARP に関するワークの取り扱いについてはさらなる検討が必要であると考える.

7. 先行研究と本研究の関係

パケットキャプチャソフトを利用した演習として，Wu (2011) は，セキュリティ教育の初級コースにおいて特にトランスポート層に関して Wireshark を利用する教案を提案しているが，その効果は明確に示されていない [10].

Desai ら(2017) は Wireshark を利用した授業を行い, その効果を測定しているが，トランスポート層に関する演習を主に紹介しており，その他の層に関する演習の詳細は不明である [11].

筆者 (2018) はデータリンク層およびネットワーク層の理解のために Wireshark を利用して有線 LAN のパケットをキャプチャして分析する演習の開発・実践を行ったが，ワークシートの設問が難解である，演習時間に比べて演習内容が多すぎる等の問題があり，期待した効果が得られていなかった[7].

今回新たに考案した無線パケットキャプチャ演習では，ワークシートの設問を容易にし，演習内容を比較的簡素化するとともに，無線 LAN 上で行う演習へと改訂を行っている．無線 LAN 上で行う演習とすることで，演習場所の制限を緩和し，演習が実施可能な場所が増えると期待される．また，本演習について今回は本学の情報専門コース 3 年留学生を対象に実践検証を行っているが，問題やワークの簡易化により，一般情報教育でも実施可能となることを意図している.

8. おわりに

本研究では，TCP/IP ネットワークの理解を促進するための無線パケットキャプチャ演習を開発・実践し，受講生自身による事後自己評価および事前と事後に実施する客観テストを通じて演習の教育効果を検討した.

演習の事前事後に実施した確認テストの結果は，有意ではないもののある程度の平均点の向上を示した．また，受講生自身による事後自己評価では，「ある程度できる」「できる」と評価する受講生は半数程度にとどまったが，当該受講生の自由記述回答からは演習を通じて TCP/IP ネットワークに対する理解が進んだ様子がうかがえた．本演習は TCP/IP ネットワークの理解を促進しうると考えられる.

今後は，一般情報教育における実践を予定している．本演習をアクティブラーニングのひとつの形態として効果的に運用するため，演習の前提となる知識をどのように伝えるか，ワークシートや補足説明資料の専門用語をわかりやすい形でどのように提示するか等が今後の検討課題である.

謝辞

本研究の一部は JSPS 科研費 19K03015 の助成を受けたものである.

参考文献

[1] カリキュラム標準一般情報処理教育（GE），入手先 https://www.ipsj.or.jp/annai/committee/education/j07/ed_j17-GE.html (参照 2019-05-19).
[2] 鈴木 大助: コンピュータネットワーク構築の学習における学習者から見た実機演習とシミュレータ演習の比較, 情報処理学会 研究報告, Vol.2019-CE-149, No.11, pp.1-5 (2019).
[3] 鈴木 大助: 通信の仕組みを理解するためのロールプレイ演習の開発と実践, 情報処理学会研究報告, Vol.2017-CE-140, No.10, pp.1-7 (2017).
[4] 鈴木 大助: 通信の仕組みを理解するためのロールプレイ演習の実践と評価, 情報処理学会論文誌 教育とコンピュータ, Vol.4, No.2, pp.37-46 (2018).
[5] Network Topology Icons, available from <https://www.cisco.com/c/en/us/about/brand-center.html> (accessed 2018-06-01).
[6] Wireshark User's Guide, available from <https://www.wireshark.org/docs/wsug_html_chunked/> (accessed 2018-06-01).
[7] 鈴木 大助: パケットキャプチャ演習が通信の仕組みの理解にもたらす効果, 情報教育シンポジウム論文集, Vol. 2018, No.11, pp.76-83 (2018).
[8] CaptureSetup/WLAN - The Wireshark Wiki, available from <https://wiki.wireshark.org/CaptureSetup/WLAN> (accessed 2019-05-31).
[9] ping-t, 入手先 <https://ping-t.com/> (参照 2018-06-01).
[10] Wu, Y. A.: TCP Three-way Handshake as a Pedagogical Tool, Proceedings of the 14th Colloquium for Information Systems Security Education, pp.49-56 (2010).
[11] Desai, P., Vijayalakshmi, M. and Raikar, M. M.: Encourage research thinking in network domain using traffic analysis tool, Journal of Engineering Education Transformations, Vol.30, No.3, pp.123-129 (2017).