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

鈴木大助[†1]

概要：本研究の目的は，通信の仕組みを理解するためのパケットキャプチャ演習を考案し，実際の授業に適用し，その演習が受講生の理解に及ぼす効果を明らかにすることである．演習では，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，演習室内 PC 同士での ping および演習室外サーバへの ping において送受信されるパケットをキャプチャし，そのデータに基づいてワークシートを用いたグループワークを行う．演習後の達成度自己評価からは，どの到達目標に関しても 6 割以上の受講生が「十分達成できた」「達成できた」と評していることがわかる．しかし，説明問題における受講生の解答および事前事後テスト結果からは，本演習は現状のままでは受講生が通信の仕組みを理解する助けとなるとは言えない．今回の実践から明らかになった課題をふまえた上で，改良した演習を実施し，その効果を測定する必要がある．

キーワード：情報通信ネットワーク，プロトコル，能動的学習，パケットキャプチャ，Wireshark，可視化

Effect of a Packet Capture Exercise on Students' Understanding of TCP/IP network

DAISUKE SUZUKI[†1]

Abstract: The aim of this study is to invent a packet capture exercise, to put it into practice, and to clarify its effect on students' understanding of TCP/IP network. In the exercise, students capture packets sent and received when they ping a PC in the laboratory and ping a server outside the laboratory using packet capture software installed on their PC. Subsequently, based on captured data, students perform group work using worksheets. The self-assessment on achievement after the exercise shows that, with respect to every specific behavioral objective, more than 60% of the students assess themselves as "achieved enough" or "achieved". However, from students' answers in description questions and analysis of pre and post results, it became clear that the exercise as is cannot be said to help students understand TCP/IP network. Based on problems clarified from this practice, it is necessary to carry out improved exercises and measure their effects.

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

1. はじめに

インターネットは現代社会における必須のインフラである．人々は，家庭や学校，職場においてインターネットに接続されたスマートフォンや PC を利用して，日々の生活を送り，業務を行っている．しかし，ネットワークにつながらない，通信速度が遅いなど，ネットワークに関する日常的な問題は多い．そのため，情報技術を専門とする者はもちろんのこと，単なる一利用者であっても，ネットワークの仕組みについて相応の知識・理解が求められる．各教育機関の情報系科目における学習を通じて，すべての人がネットワークに関する基本的な知識・素養を身につけることが望ましい．

しかし，ネットワークの学習は初学者にとっては簡単ではない．データの流れが目に見えるものではないため，学習していても実感が伴わず，曖昧な理解に留まる恐れがある．逆に言えば，データの流れを可視化することで，確かな理解が促進されると期待される．

筆者は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[1], [2]．演習では，パケットやフレームといったデータを象徴する入れ子構造になった具体物の「箱」を，PC 役，スイッチ役，ルータ役を演じる各受講生の間で，通信プロトコルに従って受け渡すことでネットワーク通信を再現する．これは特にデータリンク層およびネットワーク層に関するネットワーク階層構造や通信プロトコルの理解，ルータやスイッチ，PC 等各種ネットワーク機器の役割の理解を促進する顕著な効果が見られた．

本研究ではネットワークを学習する別の学習手法としてパケットキャプチャを取り入れた演習を考案・実践し，その効果を測定する．パケットキャプチャはネットワーク構築運用の現場でトラブルシューティングのために頻繁に行われる行為であり，そのためのソフトとして Wireshark[3] や tcpdump[4] などがよく知られている．これらを用いると，実際にネットワーク上を流れているデータを取り込み，可視化し，解析することができる．パケットキャプチャソフトを高校や大学のネットワークの授業で利用すること自体は珍しいことではないが，その利用が受講生の理解にもたらす効果の測定は十分になされているとは言えない．ネットワーク学習におけるパケットキャプチャの効果的な活用のためには，効果測定が必須である．

†1 北陸大学
Hokuriku University

本研究では,特にデータリンク層およびネットワーク層のデータ構造とプロトコルを理解するためのパケットキャプチャを取り入れた演習を考案し，実験授業を通じてその演習が受講生の理解におよぼす効果を測定することを目的とする.

2. 関連研究

Goldstein et al. (2005) はネットワークシミュレータやパケットキャプチャソフトがネットワーク教育において利用されるものの，効果測定がなされないまま利用されることが多い点を指摘している．その上で，大学 2 年生のネットワークの授業において，ネットワークシミュレータの 1 つである Cisco Packet Tracer をアクティブラーニングのために利用し，その効果を測定したところ，受講生のネットワークの概念理解が深まったことを明らかにしている [5].

Makasiranondh et al. (2010) は，ネットワーク教育において利用するネットワークシミュレータとして，Cisco Packet Tracer と GNS3 の二つを比較検討している [6].

Ghazali et al. (2011) はネットワーク学習におけるアクティブラーニングの観点から Cisco Packet Tracer および GNS3 をはじめ，各種ネットワークシミュレータを比較検討している [7].

一方パケットキャプチャソフトについてであるが，Wu (2011) は，TCP 3 ウェイハンドシェイクに注目し，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 を利用する教案が提案されているが，その効果については明確に示されていない [8].

Desai et al. (2017) はネットワーク研究に対する興味関心を促進するために授業で Wireshark を利用しその効果を測定しているが，紹介事例が主にトランスポート層に関する演習であり，その他の層に関する演習の詳細は不明である [9].

本研究はネットワーク教育において，特に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 を利用した演習を考案し，その演習が受講生の理解にもたらす効果を測定することを目的としている.

3. 演習環境

本パケットキャプチャ演習を行う演習室内外のネットワーク概略図を図 1 に示す．この演習室は，筆者が所属する北陸大学に所在しており,日ごろから IT 系の様々な授業が実施されている．左半分の枠で囲まれた範囲が演習室を表す．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[10]を用いている.

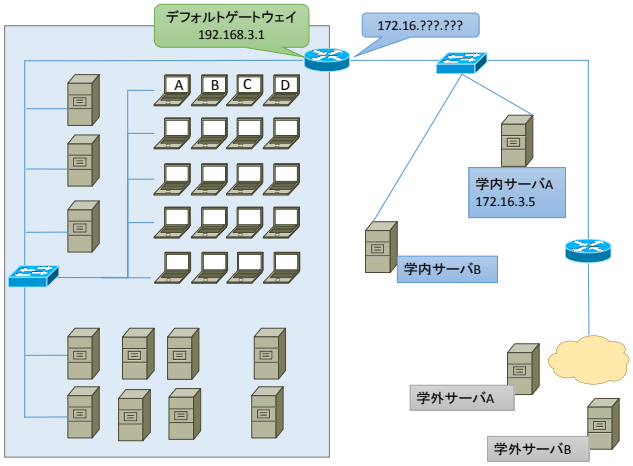

図 1　演習室内外のネットワーク概略図

Fig. 1　Schematic diagram of the network inside and outside the laboratory.

演習室内には学生用ノート PC と練習用サーバ機が各 20 台，教師用ノート PC とサーバ機が各 1 台，有線 LAN に接続され, 192.168.3.0/24 のプライベート IP アドレスを DHCP によって割り振られている．なお，図 1 は概略図のため，PC やスイッチは一部のみを描いているが, 実際には演習室内では複数のスイッチがカスケード接続されている. また，無線 LAN アクセスポイントを一基設置しており，WPA2-PSK にて接続できるようにしている.

演習室にはルータが 1 台設置されている．ルータの演習室内側インターフェイスは演習室内 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．このルータは演習室内 PC に対する DHCP サーバとして機能するほか，NAT 機能を提供している．演習室内 PC はこのルータを経由して，上流である 172.16.0.0/12 の学内 LAN へ接続可能である．また，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.

受講生は一人一台ノート PC を貸与されており，その管理者権限を保有している．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のみをキャプチャする．実際のネットワーク環境の構築運用現場ではトラブルシューティングのために，自分の PC 以外が送受信するパケットでもキャプチャできるプロミスキャスモードにし，スイッチのミラーポートを利用してキャプチャを行うが，本演習ではこれを行わない．ネットワークに関する机上の学習を終えた受講生が，自分の管理下にある PC を利用して実施できる演習とするためである. なお, ノート PC は DELL VOSTRO 15 シリーズであり，その OS については Windows 8.1 と Windows 10 が混在している.

4. パケットキャプチャ演習

4.1 本演習授業の目的と到達目標

本演習授業の目的は「ARP や ICMP，デフォルトゲートウェイのような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 ICMP パケットを抽出できる
3. キャプチャしたパケットおよびプロトコルの理解に基づいて，同一ネットワーク内での通信の過程を説明できる
4. キャプチャしたパケットおよびプロトコルの理解に基づいて，異なるネットワーク間の通信の過程を説明できる

演習は，上記授業の目的と到達目標の説明 5 分，演習準備 10 分，Wireshark の使用法 10 分，演習 1（同じネットワークのホストに対する ICMP エコー要求実験）25 分，演習 2（異なるネットワークのホストに対する ICMP エコー要求実験）25 分，ワークシートの記入・提出 15 分で全 90 分からなる．以降の節で順に説明する．

4.2 演習準備

演習開始前に以下の準備を行う．

1. 実験に使用しない PC をシャットダウンする
2. 実験に使用する PC のネットワークアダプタのうち，実験に使用しないアダプタをすべて無効にする
3. WEB ブラウザ等，すべてのアプリケーションを終了する

これは，注目すべき通信以外の通信の発生を抑えるためである．次に，管理者権限でコマンドプロンプトを起動し，「ipconfig /all」を実行し，NIC 設定情報を図 2 に示すワークシートに記入する．

・管理者権限でコマンドプロンプトを起動し、「ipconfig /all」を実行せよ。
その実行結果から必要な情報を読み取り、以下の表を完成させよ。

イーサネットアダプター	
物理アドレス	
IPv4 アドレス	
サブネットマスク	
デフォルト ゲートウェイ	

図 2 NIC 設定情報の確認ワークシート

Fig. 2 Worksheet for checking the NIC configuration.

4.3 Wireshark の使用法

Wireshark の使用法を簡単に確認する．Wireshark のキャプチャ画面構成を図 3 に示す．この図は，受講生への説明の便宜のために，Wireshark User's Guide[11]の図に日本語の吹き出しを付加したものである．

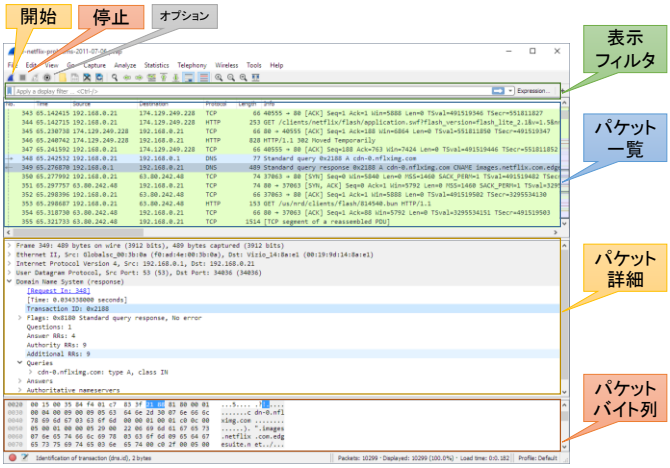

図 3 Wireshark キャプチャ画面構成

Fig. 3 Wireshark's main window.

オプションからプロミスキャスモードの解除を行う．これは自分に関係のあるパケットのみをキャプチャ対象とするためである．また，表示メニューから，名前解決を行わない設定にする．MAC アドレスの OUI の名前解決を行わせないためである．続いて，実際にキャプチャ開始・停止の操作を行い，次々にパケットがキャプチャされること，パケット一覧で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パケット詳細，パケットバイト列が表示されることを確認する．さらに，表示フィルタにおいて「arp」や「icmp」など，プロトコル名を入力して簡単に表示フィルタリングができることを確認する．

4.4 演習 1 同じネットワーク内での通信

演習 1 では同じネットワーク内での通信において，必要な宛先 MAC アドレスの取得のために ARP が働いていることを理解することを目的の一つとする．演習 1 の実験概略図を図 4 に，実験手順を図 5 に示す．

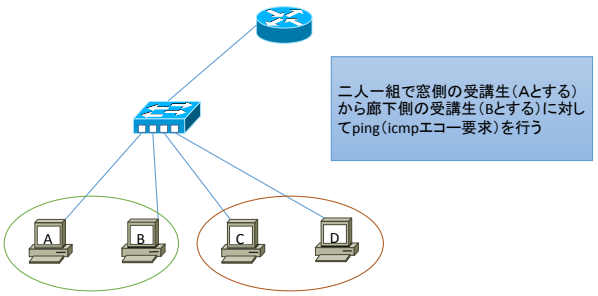

図 4 実験概略図（演習 1）

Fig. 4 Schematic diagram of the experimental setup (ex.1).

1. Wireshark起動、キャプチャ開始
2. 管理者権限でコマンドプロンプトを起動し、「arp -d *」実行してarpテーブルを消去
3. 「arp -a」を実行し、全てのエントリが削除されたことを確認する
4. Aはコマンドプロンプトで「ping 192.168.3.*」を打つ。ここで「192.168.3.*」はBのIPアドレスとする
5. 4回応答があり、pingが終了したことを確認する
6. A、Bの双方とも、Wiresharkのキャプチャを停止し、「ファイル」⇒「…として保存」⇒「演習１」として保存する
7. ワークシート１～３に取り組む

図 5　実験手順（演習 1）

Fig. 5　Experimental procedure (ex.1).

演習 1 では，図 4 に示す通り二人一組となり，一方から他方に ping（ICMP エコー要求）を行う．各自 Wireshark を起動，キャプチャ開始したあと，管理者権限でコマンドプロンプトを起動し，「arp -d *」を実行することで，PC が保持している ARP テーブルを消去する．「arp -a」により ARP テーブルのすべてのエントリが削除されていることを確認後，一方から他方へ ping（ICMP エコー要求）を実行する．ping による疎通確認が完了した後，キャプチャ停止・保存を行う．受講生は取得したキャプチャデータに関して，図 6，図 7，図 8 に示すワークシートを用いて作業を行う．

・管理者権限でコマンドプロンプトを起動し、「arp -a」を実行せよ。その実行結果から動的エントリを読み取り、以下の表を完成させよ。

インターネットアドレス	物理アドレス	種類
		動的
		動的
		動的
		動的
		動的

図 6　ARP テーブルの確認（演習 1 ワークシート 1）

Fig. 6　Checking the ARP table (ex.1, wksht.1).

・Wiresharkでキャプチャしたデータ「演習1.pcapng」からARPリクエストもしくはARPリプライを一つ取り上げ、以下の表を完成させよ。
  ・表示フィルタで「arp」とすると、ARPパケットを表示する
  ・「arp and eth.addr == *自分のMACアドレス*」とすると、フレームの宛先もしくは送信元が自分自身のARPパケットだけを表示する

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）か応答（2）か	
		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 7　ARP パケットの確認（演習 1 ワークシート 2）

Fig. 7　Checking an ARP packet (ex.1, wksht.2).

・Wiresharkでキャプチャしたデータ「演習1.pcapng」からICMPエコー要求もしくはICMPエコー応答を一つ取り上げ、以下の表を完成させよ。
  ・表示フィルタで「icmp」とすると、icmpパケットだけを表示できる
  ・「icmp and ip.addr == *自分のIPアドレス*」とすると、パケットの宛先もしくは送信元が自分自身であるicmpパケットだけを表示できる

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	IPv4 (0x0800)
	パケット	Protocol:	ICMP（1）かTCP（6）かUDP（17）か	ICMP (1)
		Source:	パケットの送信元IPアドレス	
		Destination:	パケットの宛先IPアドレス	
	ICMPメッセージ	Type:	エコー要求（8）かエコー応答（0）か	
		Data (32 bytes):	データ	

図 8　ICMP パケットの確認（演習 1 ワークシート 3）

Fig. 8　Checking an ICMP packet (ex.1, wksht.3).

ワークシート 1（図 6）では，コマンドプロンプトにて「arp -a」を実行し，ARP テーブルが更新されていることを確認する．ワークシート 2（図 7）では，ARP パケットの構造とその内容を理解する．ワークシート 3（図 8）では ICMP パケットの構造とその内容を理解する．なお，図 7，図 8 中の項目名は Wireshark のパケット詳細ウィンドウの項目名に対応しており，作業を通じてパケットの構造を理解できるようになることを企図している．

演習 1 の作業は以上であるが，Wireshark のパケット一覧を観察することで，ICMP エコー要求・応答に先立って ARP 要求・応答がなされることが確認できる．また，PC の ARP テーブルの変化を観察することで，ARP 要求・応答の結果として，ARP テーブルが更新され，互いの MAC アドレスを学習していることが確認できる．

4.5　演習 2　異なるネットワーク間の通信

演習 2 では，異なるネットワークに所属するホストへの通信において，パケットは宛先ホスト宛てであるがフレームがデフォルトゲートウェイ宛てになること，ルータがフレームの送信元と宛先を書き換えて転送することを理解することを目的とする．演習 2 の実験概略図を図 9 に，演習 2 の実験手順を図 10 に示す．

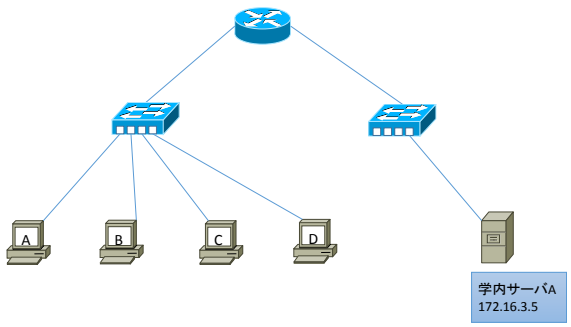

図 9　実験概略図（演習 2）

Fig. 9　Schematic diagram of the experimental setup (ex.2).

1. Wireshark起動、キャプチャ開始
2. 管理者権限でコマンドプロンプトを起動し、「arp -d *」実行してarpテーブルを消去
3. 「arp -a」を実行し、全てのエントリが削除されたことを確認する
4. コマンドプロンプトで「ping 172.16.3.5」を打つ。なお、「172.16.3.5」は学内サーバであり、演習室ネットワークの外にある
5. 4回応答があり、pingが終了したことを確認する
6. Wiresharkのキャプチャを停止し、「ファイル」⇒「…として保存」⇒「演習2」として保存する
7. ワークシート4～6に取り組む

図 10　演習 2 実験手順

Fig. 10　Experimental procedure (ex.2).

演習 2 では，演習室外サーバに対して各自が ping（ICMP エコー要求）を行う．Wireshark を起動，キャプチャ開始したあと，管理者権限でコマンドプロンプトを起動し，「arp -d *」を実行することで，PC が保持している ARP テーブルを消去する．「arp -a」により ARP テーブルのすべてのエントリが削除されていることを確認後，演習室外サーバへ ping（ICMP エコー要求）を実行する．ping による疎通確認が完了した後，キャプチャ停止・保存を行う．受講生は取得したキャプチャデータに関して，図 11，図 12，図 13 に示すワークシートを用いて作業を行う．

・管理者権限でコマンドプロンプトを起動し、「arp -a」を実行せよ。その実行結果から動的エントリを読み取り、以下の表を完成させよ。

インターネットアドレス	物理アドレス	種類
		動的
		動的
		動的
		動的
		動的

図 11　ARP テーブルの確認（演習 2 ワークシート 4）

Fig. 11　Checking the ARP table (ex.2, wksht.4).

・Wiresharkでキャプチャしたデータ「演習2.pcapng」からICMPエコー要求を一つ取り上げ、以下の表を完成させよ。
  ・表示フィルタで「icmp」とすると、icmpパケットだけを表示できる
  ・「icmp and ip.addr == *自分のIPアドレス*」とすると、パケットの宛先もしくは送信元が自分自身であるicmpパケットだけを表示できる

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	IPv4 (0x0800)
	パケット		Protocol:	ICMP（1）かTCP（6）かUDP（17）か	ICMP (1)
			Source:	パケットの送信元IPアドレス	
			Destination:	パケットの宛先IPアドレス	
		ICMPメッセージ	Type:	エコー要求（8）かエコー応答（0）か	8 (Echo (ping) request)
			Data (32 bytes):	データ	

図 12　ICMP エコー要求の確認（演習 2 ワークシート 5）

Fig. 12　Checking an ICMP echo request (ex.2, wksht.5).

・Wiresharkでキャプチャしたデータ「演習2.pcapng」からICMPエコー応答を一つ取り上げ、以下の表を完成させよ。
  ・表示フィルタで「icmp」とすると、icmpパケットだけを表示できる
  ・「icmp and ip.addr == *自分のIPアドレス*」とすると、パケットの宛先もしくは送信元が自分自身であるicmpパケットだけを表示できる

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	IPv4 (0x0800)
	パケット		Protocol:	ICMP（1）かTCP（6）かUDP（17）か	ICMP (1)
			Source:	パケットの送信元IPアドレス	
			Destination:	パケットの宛先IPアドレス	
		ICMPメッセージ	Type:	エコー要求（8）かエコー応答（0）か	0 (Echo (ping) reply)
			Data (32 bytes):	データ	

図 13　ICMP エコー応答の確認（演習 2 ワークシート 6）

Fig. 13　Checking an ICMP echo response (ex.2, wksht.6).

ワークシート 4（図 11）では，コマンドプロンプトにて「arp -a」を実行し，ARP テーブルが更新されていることを確認する．ワークシート 5（図 12）では ICMP エコー要求において，宛先 IP アドレスは演習室外サーバであるが，宛先 MAC アドレスがデフォルトゲートウェイを指していることを理解する．ワークシート 6（図 13）では，ICMP エコー応答において，送信元 IP アドレスは演習室外サーバであるが，送信元 MAC アドレスがデフォルトゲートウェイを指していることを理解する．

演習 2 の作業は以上であるが，ワークシート 5 とワークシート 6 の結果から，異なるネットワーク間での通信においてはルータがフレームの送信元と宛先を書き換えて転送していることを理解する．

4.6　ワークシートの提出

受講生は最後に，ワークシートの問題に取り組み，達成度自己評価のための振り返りアンケートに回答して提出する．演習 1 の問題は以下の 3 問である．

1. PC-A から PC-B に ping を打ち応答が返るまでに，ARP や ICMP に従ってどのような処理がなされているか，キャプチャしたパケットデータを用いて説明せよ
2. ある PC が，ターゲット IP アドレスが自分自身ではない ARP 要求を受け取ったとき，その PC はどのような処理を行うか答えよ
3. フレームの宛先がブロードキャストである ARP 要求がスイッチに着信したとき，スイッチはどのような処理を行うか答えよ

演習 2 の問題は以下の 1 問である．

1. PC-A から異なるネットワークのサーバ（学内サーバ A）に ping を打ち応答が返るとき，ルータがどのような処理を行っているか，キャプチャしたパケットデータを用いて説明せよ

最後に授業冒頭で掲げた四つの到達目標のそれぞれについて，「4.十分達成できた，3.達成できた，2.あまり達成できなかった，1.全く達成できなかった」で回答を求めた．

5. 授業実践と評価の枠組み

5.1 授業スケジュール

2018 年度北陸大学未来創造学部 3 年前期科目「ネットワーク論Ⅰ」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
Table 1 Syllabus for Computer Networks I.

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	IPv4アドレスとサブネット
6	事前テスト・ケーブル作成の説明
7	パケットキャプチャ演習（実験群）／ケーブル作成（統制群）
8	事後テスト
9	第7回の入れ替え（ケーブル作成／パケットキャプチャ演習）
10	確認テスト・実機操作の説明
11〜15	実機演習
16	期末試験

全 16 回のうち第 7 回に実験群に対してパケットキャプチャ演習を実施し，統制群に対してはケーブル作成演習を実施した．ケーブル作成演習では，第 11 回以降の実機演習で用いるためのクロスケーブルとストレートケーブルの作成を行っている．2018 年度第 7 回授業は 2018 年 5 月 28 日（月）11:00-12:30 の授業時間枠に実施した．なお，本科目は後期科目「ネットワーク論Ⅱ」とあわせて，CCENT (Cisco Certified Entry Networking Technician)レベルに到達することを一つの目標としている．

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 20 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，本パケットキャプチャ演習までに 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前提である．

5.2 事前・事後テスト

ネットワークに関する事前・事後テストを実施した．実施日時は,事前テストは 2018 年 5 月 21 日(月)11:00-11:40, 事後テストは 2018 年 6 月 4 日（月）11:00-11:40 である．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 [12] 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」から抜粋して出題した．20 問の分野別問題数内訳を表 2 に示す.

表 2 分野別問題数 [2]
Table 2 Number of questions by category [2]

分野	事前	事後
ネットワーク基礎	7	7
OSI参照モデル	5	5
TCP/IP	2	2
スイッチング	4	4
ルーティング	2	2

なお，この問題はロールプレイ演習[2]の効果測定で用いたものと同一である．よって，分野別問題数内訳の説明は文献[2]と同一となるが，本稿で内容を完結するために，再度同一の説明を記載する．「ネットワーク基礎」は，基数変換やブロードキャストドメインの理解の他に，IP アドレス，MAC アドレス，ARP の理解やデフォルトゲートウェイの設定，ルータやスイッチの挙動を問う問題が含まれる．「OSI 参照モデル」にはセグメント，パケット，フレームの関係やカプセル化について問う問題が含まれる．「TCP/IP」は ARP やデフォルトゲートウェイの設定について,「スイッチング」はスイッチの挙動やフラッディングについて,「ルーティング」はルータの挙動やルーティングにおける MAC アドレスの書換えについて，それぞれ問う問題からなる. CCENT の本来の問題では「スイッチング」「ルーティング」ではスイッチやルータの実際のコマンドやさらに詳細な設定を問う問題が多く出題されるが，今回は対象外としている．

6. 結果と考察

6.1 演習の取組みの様子

演習は 90 分で終了する予定であったが，いくつかのトラブルに見舞われ，延長を余儀なくされた．トラブルの事例としては，たとえば，Windows アップデートが突然始まり，演習を開始できない学生がいた．PC 管理は受講生各自に任せているが，Windows アップデートの自動更新を停止するなどの処置をあらかじめ指導しておくべきであった．

また,いくつかの PC に対してコマンドプロンプトで ping を実行しても「要求がタイムアウトしました」と表示されるため，通信できないと誤認する例が見られた．リクエストタイムアウトの原因は，当該 PC の Windows ファイアウォールにおいて ICMP エコー要求に対する応答を許可していないためである．演習開始前にあらかじめ ICMP エコー要求に応答する設定に変更する指導が必要であった．

ワークシートを用いた課題の取組み状況はおおむね良好であった．NIC 設定情報の確認，ARP テーブルの削除・確認，パケットキャプチャの実施および関連する作業は基本的にすべての受講生が実行できていた．取得した ARP パケットや ICMP パケットを表示フィルタリングし，必要な項目を読み取って記録できていた．

しかし，通信の過程を説明する問題については，すべて

の受講生が取り組んでいるものの，問題の意味がわからない，日本語が難しい，という意見が見られた．実際，演習 1 問 1「PC-A から PC-B に ping を打ち応答が返るまでに，ARP や ICMP に従ってどのような処理がなされているか，キャプチャしたパケットデータを用いて説明せよ」において誤解が見られた．

演習 1 問 1 は，PC の ARP テーブルに通信相手の MAC アドレスが記憶されていない状態で ping を実行した場合，宛先 MAC アドレスが不明のためまず ARP 要求を行い，ARP 応答によって宛先の MAC アドレスを取得した後，ICMP エコー要求・応答がなされる旨についてキャプチャデータのワークシートに基づいて説明してもらう意図であった．しかし，解答の中には，受講生自身が操作した手順や入力したコマンド履歴を解答する例が見られた．改善案としては，たとえば，演習 1 問 1「なぜ ICMP の前に ARP が生じているのか答えよ」演習 2 問 1「なぜ異なるネットワーク通信では宛先 MAC と宛先 IP が異なるホストを指すのか答えよ」といった，より簡潔な問題文に変更することが考えられる．

6.2 受講生自身による達成度評価

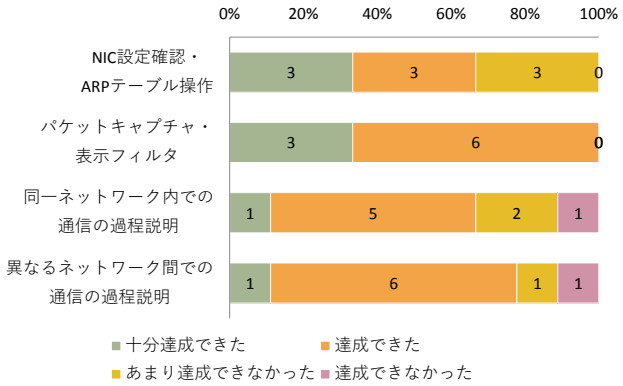

図 14　受講生自身による達成度評価

Fig. 14　Self-assessment on achievement.

演習の最後に受講生は振り返りアンケートとして，四つの授業到達目標のそれぞれについて，達成できたかどうかを回答して提出した．この受講生自身による達成度自己評価の結果を構成比グラフとして図 14 に示す．グラフ上の数値はそれぞれの実解答人数である．1 番目の項目，NIC の設定情報の確認や，ARP テーブルの削除や確認は，単なる操作であり，特段難しいことではない．それでも，3 人は「あまり達成できなかった」と評している．これは，コマンドプロンプトを管理者権限で実行する際に手間取ったためと見られる．2 番目の項目，パケットキャプチャ・表示フィルタリングは受講生全員が「十分達成できた」「達成できた」と評している．3 番目，4 番目の項目は通信の過程を理解し自らの言葉で説明できたかを問うている．「十分達成できた」，「達成できた」とする割合が高いが，「達成できなかった」と回答する者が 1 名見られる．全体的な自己評価は低くは無いものの，前節でも述べたとおり，通信の過程を説明する問題については改訂が必要であると考えられる．

6.3 事前・事後テスト結果

事前テスト・事後テストの両方を受験した学生 16 名を分析の対象とする．統制群は 8 名，実験群は 8 名である．統制群・実験群の事前・事後テストの結果を表 3 に，各群における事前・事後テストの平均点の推移を図 15 に示す．なお，エラーバーは標準誤差である．

表 3　事前・事後テスト結果

Table 3　Summary of pre-test and post-test results

グループ	人数	テスト	平均	標準偏差
実験群	8	事前	30.0	15.6
		事後	32.5	9.6
統制群	8	事前	29.4	11.2
		事後	33.8	7.4

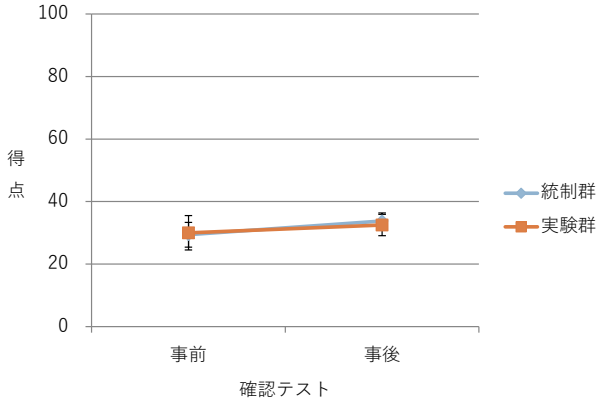

図 15　平均点推移の群間比較

Fig. 15　Difference in mean score improvement between two groups

統制群の平均点の上昇 4.4 点に対し，実験群の平均点の上昇は 2.5 点にとどまった．事後得点から事前得点を引いた差得点について群間で Welch の t 検定 を行ったところ，t 値 ＝-0.41, p 値 ＝.69 より，有意差は認められなかった．本パケットキャプチャ演習がネットワークに関する理解を促進する効果があったとは言えないことがわかる

6.4 本パケットキャプチャ演習の効果に関する考察

本研究はパケットキャプチャ演習を考案し，実際の授業に適用し，その効果を測定することを目的としている．本研究で考案したパケットキャプチャ演習は，受講生自身の PC が送受信するパケットをキャプチャし，そのキャプチャデータの観察を通じて通信プロトコルを理解することを目指している．達成度自己評価によると，どの到達目標に関しても 6 割以上の受講生が「十分達成できた」「達成できた」

と評しているものの，通信の過程を説明する問題については，「達成できなかった」と評する受講生がいた．また，事前事後テスト結果から，ネットワークに関する理解を促進する効果があったとは言えないことがわかる．

効果が得られなかった要因は三つ考えられる．第 1 に，ルータやスイッチの挙動を直接観察していない点である．本演習は，特別な実験環境を必要とせず，受講生が管理者権限を有する PC が LAN につながってさえいれば実践可能な演習とした．演習における観察対象は受講生自身の PC が送受信するパケットだけに限られている．そのため，ルータやスイッチの挙動については，取得したパケットデータに基づいて想像するしかない．ネットワーク通信の可視化という観点からはこの点が本演習の弱点であり，結果的にプロトコルの理解の促進やネットワーク機器の挙動の理解に結びつかなかった一つの要因と考えられる．

第 2 に，ワークシートの設問が適切ではなかった可能性がある．パケットの送受信において，ICMP や ARP がどのように働いているか解答することを意図した設問において，受講生自身が操作した手順や入力したコマンド履歴を解答するなどの齟齬がみられた. 操作の結果得られた ARP パケットや ICMP パケット，ARP テーブルからその背後にあるプロトコルの働きを想像するのはただでさえ簡単ではない．ましてや，留学生にとって，簡潔ではない日本語の質問文が理解の妨げになった可能性は否定できない．

第 3 に，実質的な演習時間の不足がある．設計段階では 90 分ちょうどの演習となるよう設計したつもりであったが，実施段階でさまざまなトラブルに見舞われ，演習時間を延長してもなお，実質的な演習時間が不足していた可能性がある．また，そもそもワークシートの設問解答のための所要時間の見積もりが甘かったと考えられる．設問に解答する過程において，キャプチャしたデータを材料にしながら，それまでの配布プリントや教科書を見直したり，インターネットで調べたりすることで，理解が確かなものになると期待されるが，そのためには相応の時間を設ける必要がある．

以上，想定される三つの要因を挙げた．第 1 の要因はルータやスイッチを直接扱わないとする制約条件ととらえることもできるが，第 2，第 3 の要因については，修正対応すべき点である．次回実施時には，ワークシートの設問を簡潔にすること，トラブル防止のための事前準備を十分に行うこと，ワークシートの設問に取り組む時間を十分に確保する必要がある．

7. おわりに

本研究では，情報通信ネットワークの仕組みを理解するためのパケットキャプチャ演習を考案・実践し，その効果を検証した．パケットキャプチャにより実際に送受信されるデータを可視化し，キャプチャデータの理解を促すワークシートを設計することで，ネットワークの理解を容易にすることを目指した．

演習後の達成度自己評価では，どの到達目標に関しても 6 割以上の受講生が「十分達成できた」「達成できた」と評しているものの，用意した設問に対する受講生の解答からは，通信の仕組みを説明することができるとは言えない結果となった．また事前事後テストからも現状では本演習の効果は見られないことがわかった．

演習実施にあたって解決すべき課題は今回の実践から明らかになっており，ワークシートの設問を簡潔にすること，トラブル防止のための事前準備を十分に行うこと，ワークシートの設問に取り組む時間を十分に確保することが必要である．本稿で明らかとなった課題をふまえて実施するパケットキャプチャ演習の効果については稿を改めて論じる予定である．

参考文献

[1] 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).

[2] 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).

[3] Wireshark, available from <https://www.wireshark.org/> (accessed 2018-06-01).

[4] Tcpdump, available from <https://www.tcpdump.org/> (accessed 2018-06-01).

[5] Goldstein, C., Leisten, S., Stark, K. and Tickle, A.: Using a network simulation tool to engage students in active learning enhances their understanding of complex data communications concepts, Proceedings of the 7th Australasian conference on Computing education, Vol.42 pp. 223-228 (2005).

[6] Makasiranondh, W., Maj, S. P. and Veal, D.: Pedagogical evaluation of simulation tools usage in Network Technology Education, World transactions on engineering and technology education, Vol.8, No.3, pp.321-326 (2010).

[7] Ghazali, K. W. M., Hassan, R. and Ali, Z. M.: Simulation tool for active learning of introductory computer network subjects, 1st National Conference on Active Learning, pp. 119-122 (2011).

[8] 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).

[9] 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).

[10] Network Topology Icons, available from <https://www.cisco.com/c/en/us/about/brand-center.html> (accessed 2018-06-01).

[11] Wireshark User's Guide, available from <https://www.wireshark.org/docs/wsug_html_chunked/> (accessed 2018-06-01).

[12] ping-t, 入手先 <https://ping-t.com/> (参照 2018-06-01).

