情報工学実験 III　実験⑤ ネットワークプロトコル

第 2 回 Linux プラットフォーム上での実験 【Rel. 20190426A】

目的

TCP/IP プロトコルと、関連する各種上位プロトコルの基礎を学ぶ。具体的には、各プロトコルを実装したコマンド（アプリケーション プログラム）を実行し、各プロトコルの機能等を確認する。また、同じプロトコルを実装したコンピュータ間では、OS プラットフォームに関係なく通信が行えることを確認する。

0. 実験環境の準備
- OS の起動とシャットダウン -

本実験では、Linux プラットフォームとして ubuntu を使用する。ubuntu は、Debian GNU/Linux をベースとし、Canonical 社の支援の元でコミュニティにより開発されているフリーの Linux ディストリビューションである。また、Windows や macOS の代替たり得るデスクトップ OS として、Linux 系 OS の中では近年最も利用されているディストリビューションの一つである。

【OS 起動手順】

1. PC の電源オン後、しばらくすると、『GNU GRUB』というブートマネージャが数秒表示される。
2. デフォルトで選択されている（反転している）最上段の項目『*Windows Boot Manager (on /dev/sda2)』から、『↓』矢印キーを使用して、項目『Ubuntu』を選択する（図 1 参照）。
3. 『Enter』キーを押下する。
4. 残念ながら、間に合わずに Windows が起動してしまった場合、指示を待つ（特別な手続きが必要）。
5. ログインする。

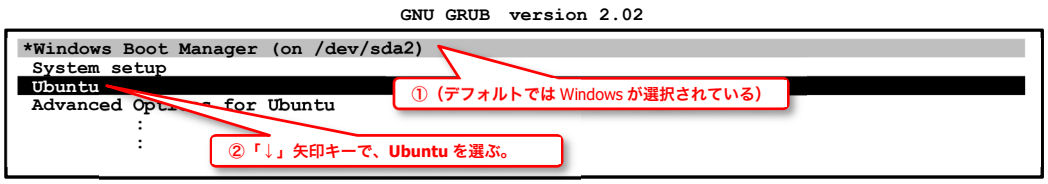

図 1　起動 OS 選択画面(GNU GRUB ブートマネージャ)

【OS シャットダウン手順】

1. デスクトップ画面上部（パネル）右端『  』をクリックし、表示されたダイアログの中から Power ボタン『  』→『電源オフ』と選ぶ。

1. コンピュータのネットワークインタフェース情報を調査する
- ifconfig コマンド -

Linux/UNIX プラットフォーム上でネットワークインタフェース情報を得るには、**ifconfig** コマンドを用いる。このコマンドで自コンピュータ（自ホスト）の IP アドレス等、多くの情報を得ることができる。

◆実験　自席パソコンのネットワークインタフェース情報を調べる。

【手順 1】端末アプリケーション（コマンド操作アプリケーション）を起動する。（画面左端のランチャー下部の『  （アプリケーションを表示する）』をクリックする。現れた検索ボックスに、英語名で『terminal』と入力すると『端末』(和名)アイコンが下部に表示されるので、クリックして起動する。）

図 2　端末アプリケーション起動の例

【手順 2】端末プログラム画面に 『ifconfig』と入力する。（※コマンド名の 2 文字目は「エフ」）
『enp3s0』と『lo』との 2 段落に分けて情報が表示されるが、『enp3s0』のほうの『inet アドレス: 』に続くアドレスが、自ホストの IP アドレスである。

▼ 出力された内容を全て記録する。また、次の用語『MAC アドレス』・『ループバックインタフェース』・『ブロードキャスト』の意味を別途調べ、説明せよ。
これらを【レポート 1】とする。

```
jikkenuser@XXXXXXX:~$ ifconfig
enp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 150.43.61.122  netmask 255.255.255.192  broadcast 150.43.61.127
        inet6 fe80::1fef:35a3:420a:6d45  prefixlen 64  scopeid 0x20<link>
        ether 08:62:66:4c:e4:8b  txqueuelen 1000  (イーサネット)
        RX packets 11549  bytes 2543418 (2.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 838  bytes 105675 (105.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
       inet 127.0.0.1  netmask 255.0.0.0
       inet6 ::1  prefixlen 128  scopeid 0x10<host>
       loop  txqueuelen 1000  (ローカルループバック)
       RX packets 395  bytes 35117 (35.1 KB)
       RX errors 0  dropped 0  overruns 0  frame 0
       TX packets 395  bytes 35117 (35.1 KB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

jikkenuser@XXXXXXX:~$
```

【自ホストの IP アドレス】

図 3　ifconfig コマンド実行画面の例

2. ホスト名と IP アドレスを調査する
- DNS: Domain Name System -

通常、私たちが Web ブラウザ上から各種サイトを指定する際には、www.fit.ac.jp 等の英数字からなるホスト名を使用するが、実際に自コンピュータが、あるサイトのコンピュータ（サーバ）と通信するには、IP アドレスを知る必要がある。ここで、ホスト名と IP アドレスとの変換を行う仕組みが DNS(Domain Name System)である。私たちが、ホスト名を用いて相手コンピュータを指定した場合でも、多くの場合はプログラム内部で自動的に、DNS による変換が行われ、実際には IP アドレスを使用した通信が行われる。ここでは、nslookup コマンドを使用し、DNS サーバへの問い合わせを手動で行う。

```
jikkenuser@XXXXXXX:~$ nslookup www.fit.ac.jp
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
www.fit.ac.jp   canonical name = fitweb.ipc.fit.ac.jp.
Name:   fitweb.ipc.fit.ac.jp
Address: 150.43.1.10

jikkenuser@XXXXXXX:~$
```

問い合わせに利用した DNS サーバに関する情報 (本 ubuntu 環境では dnsmasq というソフトを使用しているため、特殊なアドレスを使用している) ※今回は不要(参考)

…【ホスト名(本名)】
…【IP アドレス】

問い合わせに対する回答
（www.fit.ac.jp の本名は、fitweb.ipc.fit.ac.jp であることと、その fitweb.ipc.fit.ac.jp の IP アドレスは 150.43.1.10 であることをを表している）

図 4　ホスト名『www.fit.ac.jp』を DNS サーバに問い合わせた場合の例

◆実験　表 1 のコンピュータのホスト名・IP アドレスを調査し、表を完成させる。

表 1　ホスト名と IP アドレスの対応

コンピュータの種類	ホスト名	IP アドレス
情報基盤センターサーバ 1	cen.ipc.fit.ac.jp	
情報基盤センターサーバ 2	nas01service.bene.fit.ac.jp	
情報基盤センターサーバ 3	nas02service.bene.fit.ac.jp	
情報基盤センターサーバ 4	jyo.cs.fit.ac.jp	
日本経済新聞	www.nikkei.co.jp	
読売新聞	www.yomiuri.co.jp	
Microsoft	www.microsoft.co.jp	
(任意のサイト 1)		
(任意のサイト 2)		
(任意のサイト 3)		

【手順】　端末画面に『nslookup **www.abc.jp**』や『nslookup **123.45.67.89**』の形式で入力し、対応する IP アドレスやホスト名を調べる。

▼ 結果を記録し、完成した表の全体を【レポート 2】とする。

※注 1　DNS サーバへ問い合わせた結果、複数のホスト名／IP アドレスが返却されることがある。このような場合、表には最初に現れたホスト名／IP アドレスを記入する（すべて記入しても良い）。

※注 2　DNS サーバへ問い合わせた結果、（入力したアドレスが間違っていないにもかかわらず）「＊＊＊ server can't find yyy : zzz... 」等と返却されることがある。これは、DNS（データベース）上にホスト名が正しく登録されていない等の理由による。このような場合、表には「<不明>」と記入すること。

3. 通信相手からの応答があるかどうかを調査する
- ICMP: Internet Control Message Protocol -

IP プロトコルのレベルで、通信できるかどうかを確認するために、ping コマンドがよく使用される。ping コマンドは、通信相手にパケットを送信し、相手からの応答を要求する。ネットワークアプリケーションで通信が正常に行えない場合、まず、ping コマンドで通信相手からの応答があるかどうかを調べることにより、問題を初期段階で切り分けることができる。なお、ping コマンドは、ICMP プロトコル(Internet Control Message Protocol)を利用している。図 5 に、ping コマンドの実行例を示す。

```
jikkenuser@XXXXXXX:~$ ping xxx.ac.jp
PING xxx.ac.jp (n.n.n.n) from m.m.m.m : 56(84) bytes of data.
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=1 ttl=251 time=3.93ms
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=2 ttl=251 time=3.93ms
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=3 ttl=251 time=3.93ms
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=4 ttl=251 time=3.93ms        :
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=5 ttl=251 time=3.93ms
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=6 ttl=251 time=3.93ms
64 bytes from from xxx.ac.jp (n.n.n.n): icmp_seq=7 ttl=251 time=3.93ms
        : 【無限に続く】
```

★デフォルトでは、パケットを送り続けるので、適宜 Ctrl+C で終了させる
★相手ホストからの応答がない場合は、何も出力されない（Ctrl+C で終了）

図 5　ホスト名『xxx.ac.jp』に対して ping コマンドを実行した場合の例

◆実験　表 2 のコンピュータに対し、ping コマンドを実行し、完成させる。

【手順】　端末画面に 『ping **www.abc.jp**』や『ping **123.45.67.89**』の形式で入力し、応答の有無を調べる。

▼ 結果を記録し、完成した表の全体を【レポート 3】とする。

【注】前回使用した Windows 版の ping コマンドは、4 回の試行を行った後自動的に終了する様な仕様となっているが、今回使用する Linux/UNIX 版 ping では、Ctrl+C を入力するまで終了せず、ずっと ICMP パケットを送信し続ける仕様になっている。もし、相手からの応答がない場合、一見コマンドが固まったように見えるが、実は裏ではパケットを送信し続けており、相手からの応答がないため、画面上に何も表示されず、固まったように見える。この場合も、Ctrl+C の入力で終了し、コマンド入力を続けることができる。

表 2　ping コマンドを使用した応答あり/なしの調査

コンピュータの種類	ホスト名または IP アドレス	応答あり/なし
実験室パソコン（教員席）	150.43.61.□ ←当日発表	
福工大タイムサーバ	fitntp.fit.ac.jp	
情報基盤センターサーバ 1	bene.fit.ac.jp	
情報基盤センターサーバ 2	jyo.cs.fit.ac.jp	
相良研サーバ 1	maltese.cs.fit.ac.jp	
相良研サーバ 2	tamanegi.cs.fit.ac.jp	
不明なアドレス	150.43.248.42	
(任意のサイト)		

ping コマンドで使用される ICMP プロトコル（ICMP echo パケット）は、ファイアウォール・ルータ類によって遮断する設定にされることが多くなってきている。したがって、ping コマンドの応答がない場合、本当に相手ホストが応答していない場合だけでなく、経路上で遮断されている可能性も考慮しなければならない。

4. タイムサーバと時刻を同期する
- NTP: Network Time Protocol -

NTP(Network Time Protocol)は、ネットワーク上のコンピュータどうしで内蔵時計の時刻（日時）を同期するプロトコルである。UDP の上位層プロトコルとして動作する。ネットワーク上で、パケットをやりとりする際の遅延についてある程度考慮されており、正確な時刻合わせができる。Linux/UNIX プラットフォーム上で、NTP サーバ（タイムサーバ）との時刻同期を行うには ntpdate コマンドを用いる。本実験では、福工大 NTP サーバ(fitntp.fit.ac.jp)との時刻同期を行う。

この実験では管理者権限が必要なので、su コマンドを使用し管理者権限を得る。

◆実験　ntpdate コマンドを使用して、内蔵時計の時刻を NTP サーバの時刻と同期させる。

【手順 1】sudo コマンドにより root ユーザとなり管理者権限でコマンドを実行する（パソコンの内蔵時計を変更するには管理者権限が必要なので）。
端末画面に『sudo△-s』と入力（△はスペース）する。その後、パスワードの入力を求められたら、ログイン時と同じパスワードを入力する。
【注】ここでパスワード入力時にタイプする文字は、セキュリティ上、一切画面上に表示されないので慎重にタイプする（●や＊等の伏せ字も表示されず、何文字タイプしたかすら分からない。一見フリーズしたようにも見えるが、実はキー入力を受け付けている）。
▼ プロンプトが『jikkenuser@XXXXXXX:~$』から、『**root**@XXXXXXX:~**#**』へ変わることを確認する。

【手順 2】ntpdate コマンドを使用し、内蔵時計を福工大 NTP サーバに同期させる。

端末画面に『ntpdate　fitntp.fit.ac.jp』と入力し、しばらく待つ。

▼ 端末画面に出力された内容（ntpdate コマンドの出力）を記録し、これを【レポート 4】とする。

【参考】ntpdate コマンドの出力中、『offset』以降が調整した秒数を示す。

→ 直後に再度、『ntpdate　fitntp.fit.ac.jp』コマンドを繰返すと、通常は調整した秒数が前回より減少していることが確認できる。

5. 自ホストに届くパケットを調査する
- Wireshark ネットワークプロトコルアナライザ アプリケーション -

ここでは、前回の実験（第 1 回）で使用した、Wireshark の Linux 版を使用して、自ホストに届くパケットについて調査する。前回実験の「6. 不正アプリケーション（もどき）の調査（オプション）」では、不正なアプリケーションが自ホストから送信するパケットを調査対象とした。今回、本実験では外部から攻撃や侵入を試みるパケットを調査する方法を学ぶ。具体的には、自ホスト宛に届く（受信する）パケットについて調査を行う（不正侵入を試みる様な本当に危険なパケットを実験室内パソコン宛てに送信するのは問題があるため、実際には自ホスト宛に届く一般のパケットについて調査することになる）。

◆Wireshark プログラムの起動

画面左端のランチャー上の『  Wireshark (GTK+) アイコン』をクリックする。

または、図 2 で端末アプリケーションを terminal と入力して起動したのと同様に、検索ボックスに『wireshark』と入力し、現れた『  Wireshark (GTK+) アイコン』をクリックして起動する。

Wireshark では、プログラム内にパケットを取り込むことを『キャプチャ』と呼ぶ。キャプチャを開始してから、停止ボタンを押すまでの間は、パソコンの NIC（ネットワークインタフェースカード）上を通過するパケットをキャプチャし続ける。

◆実験　Wireshark でキャプチャ中に、自ホストあてに届いたパケットを調査し、**10 種類以上**抽出した結果を表 3 の様にまとめる。

【注】　調査をはじめる前に、以降の【手順 1～5】に続く「注意点・ヒントなど」を良く読んで、どのようなパケットを抽出すれば良いかを理解しておくこと。

表 3　自ホスト宛に届くパケット

	時刻 Time	プロトコル Protocol	発信元 IP アドレス Source	発信元のホスト名 【自分で調査する】
【例】	14:01:00.542257	HTTP	150.43.1.10	fitweb.ipc.fit.ac.jp

【手順 1】キャプチャ対象インターフェイスを指定し、キャプチャを開始する。
Wireshark ツールバー左端の『(List the available capture interfaces...)』ボタンを押し、出現した『Wireshark: Capture Interfaces』ダイアログで、Device『enp3s0』をチェックし、『Start』ボタンを押す（図 6 参照）。

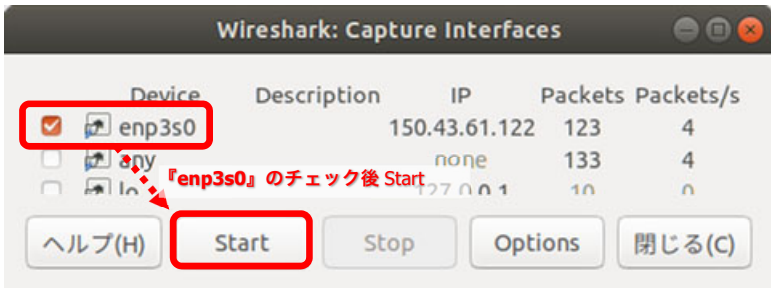

図 6　Wireshark: Capture Interfaces ダイアログ

▼ 同ダイアログが消え、現在送受信中のパケットのキャプチャが開始されたことを確認する（Wireshark のメイン画面上に、キャプチャしたパケットが 1 行ずつリアルタイムに表示される）。

【手順 2】しばらくの間キャプチャを続ける。その間、Web サイトを閲覧する・各種コマンドを実行するなど、ネットワーク上でのパケットのやりとりが生じそうな操作を**いろいろ**と行ってみる（この**いろいろ**がポイント。通常、相手ホストに対し何らかのリクエストのパケットを送信すればその返事のパケットが自ホスト宛に送られてくるはずである）。

【手順 3】キャプチャを停止する。
Wireshark ツールバーの左側から 4 番目にある『■(赤い四角形 : Stop the running live capture)』ボタンを押す。

【手順 4】『Time』フィールドの表示形式を日付＋時刻形式に変更する。
日付時刻が、すでに、[20yy-mm-dd hh:mm:ss.nnnnnn]形式で表示されていれば不要。この形式になっていない場合は、メニュー上の『View』-『Time Display Format』-『・Date and Time of Day:』と選ぶ。（または、ショートカットキー『Ctrl+Alt+1』を使用する。）

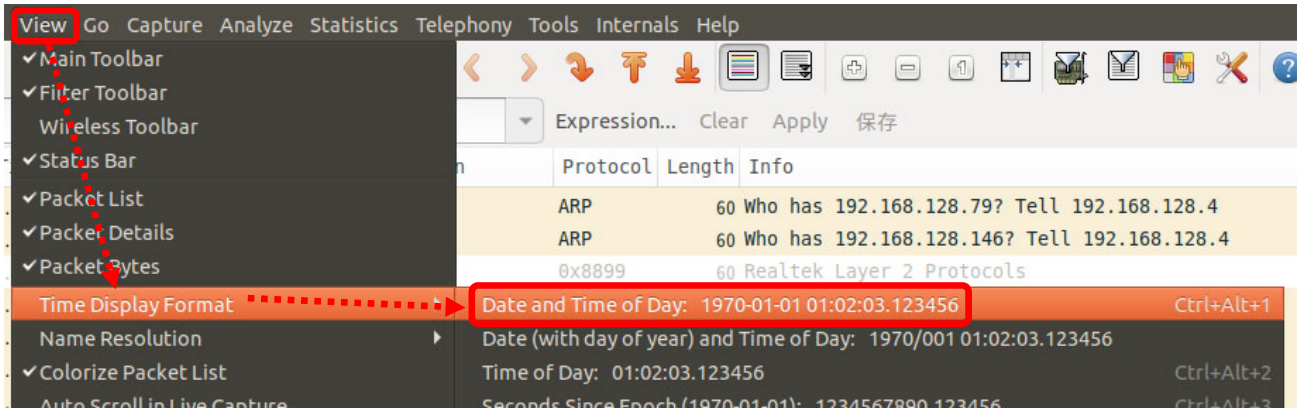

図 7　Time フィールドの表示形式を日付+時刻形式に変更する方法

【手順 5】自ホストあてに届いたパケットから 10 種類を抽出し、表 3 を完成させる。完成した表の全体を【レポート 5】とする。（抽出する 10 種類をカウントするには条件がある。詳しくは「注意点・ヒントなど」参照）

注意点・ヒントなど

- 自ホストあてに届いた、異なる種類のパケットを 10 種類以上抽出する。
- Wireshark でキャプチャしたパケットには、自ホスト宛に届いたパケットと、自ホストから送り出したパケットの 2 種類がある。そのうち、自ホスト宛に届いたパケットとは、宛先『Destination』フィールドが自ホストの IP アドレス※1と等しくなっているものである※2。
- プロトコル『Protocol』と発信元『Source』アドレスが異なる組み合わせのパケットは、異なる種類のパケットとしてカウントする。（逆に、プロトコルと発信元が同じ組み合わせのパケットは、いくつ受信しても、1 種類と見なす）
- DNS/ICMP/NTP/HTTP の各プロトコルのパケットを最低 1 つは含むこと。
- パケットの『発信元のホスト名』は、通常は Wireshark の画面上には現れない。ただし、前出の nslookup コマンドで別途調査することができる。

※1　自ホストの IP アドレスは、（DHCP の仕組み上）実験当初のアドレスから変わる場合があるので、自ホストの IP アドレスが見当たらない場合は、前出の ifconfig コマンドを用いて、再度自ホストの IP アドレスを調べる。
※2　実際はブロードキャストアドレスあてのパケットも自ホストに届くが、本実験では、ブロードキャストアドレスあてのパケットは対象外とする。

本実験で使用した Wireshark は、非常に多機能で強力なツールです。このようなツールは、便利な半面、使い方によっては不正な行為ができてしまいます。ネットワークの学習やトラブル解析などの正しい目的でのみ利用するようにしてください。

6. traceroute コマンドを用いたネットワーク構成の調査（オプション）

インターネットは、複数の LAN をルータで接続することで成り立っている。例えば図 8 に示すネットワークの例では、4 つの LAN(LAN a～d)を 3 つのルータ（ルータ ab,bc,bd）で接続した構成となっている。ホスト a1 からホスト c1 へのアクセスは、ルータ ab およびルータ bc を経由して行われる。同一 LAN 内のアクセス（ホスト a1←→ホスト a2）はルータを経由する必要はなく、直接アクセスする。

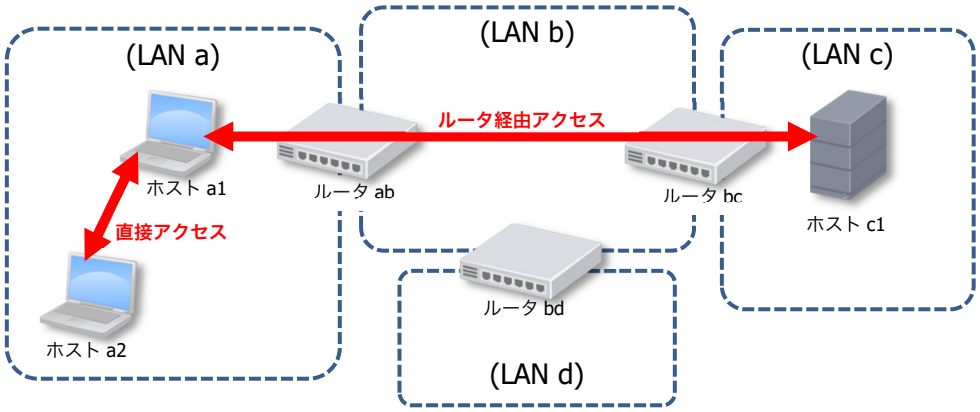

図 8　ネットワークの例（ルータ経由アクセスと直接アクセス）

通常、自ホストから相手ホストまでに経由するルータについて、意識することはないが、traceroute コマンドを用いることで、経由するルータの IP アドレスを調査することができる。例えば、ネットが突然つながらなくなった場合、相手ホストまでの経路のうち、どのルータまでつながっているのかを調査するような場合に便利である。

ここでは、traceroute コマンドを用いて、本学内のネットワーク構成を調査する。図 9 に、実際に traceroute コマンドを用いて、自ホストから 4 種類の目的ホストまでの経由ルータを調査した結果の例を示す。『traceroute （目的ホスト）』と実行すると、経由ルータおよび目的ホストのホスト名＋IP アドレス（ルータの多くは DNS サーバにホスト名を登録していないため、IP アドレスのみ）および、そのルータ・ホストからの応答に要した時間を 3 回の試行分表示する。

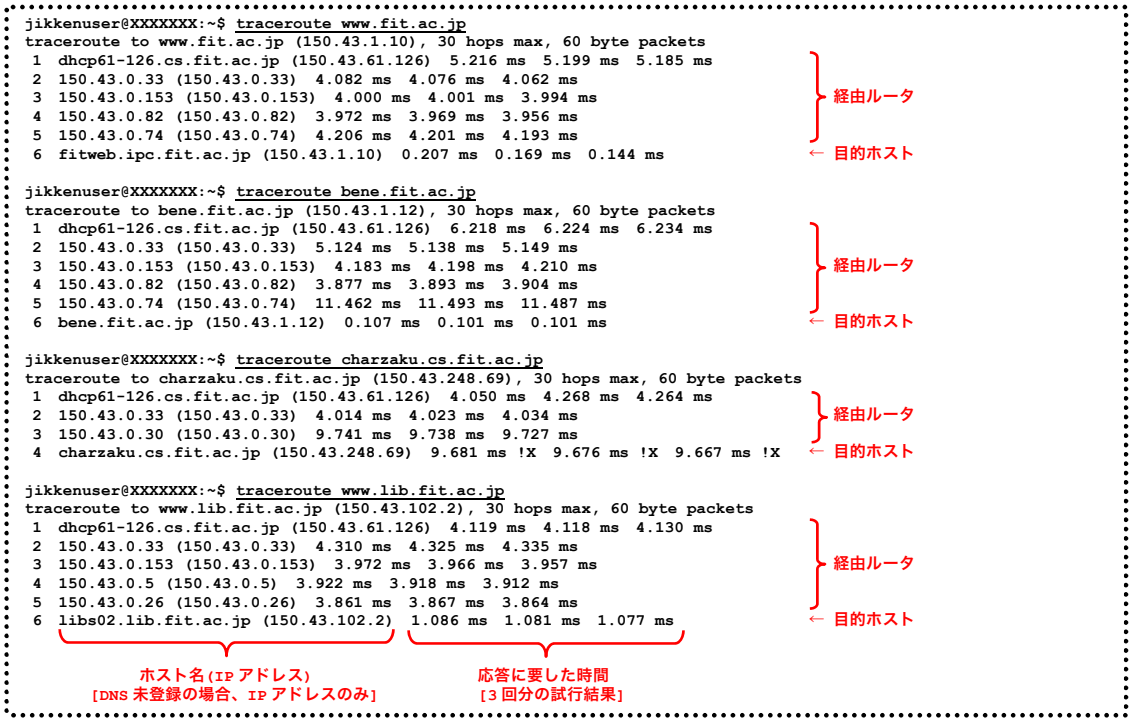

図 9　traceroute コマンドによる、目的ホストまでの経由ルータ調査例

これらの調査結果をもとに、簡単なネットワーク構成図として表したものが、次の図 10 である。

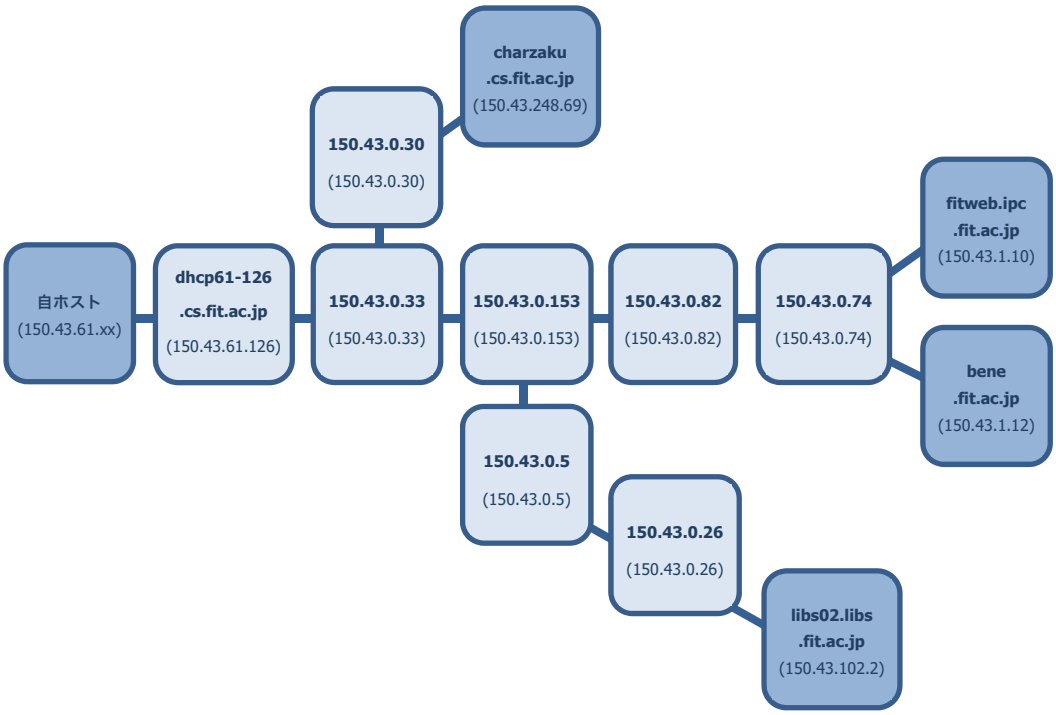

図 10　図 9 の調査結果をもとにしたネットワーク構成図の例

◆実験　表 4 に示す目的ホストについて、自ホストからの経由ルータを調査し、簡単なネットワーク構成図を作成する。

表 4　調査対象の目的ホスト

maltese.cs.fit.ac.jp	my.fit.ac.jp	www.ipc.fit.ac.jp
tamanegi.cs.fit.ac.jp	charzaku.cs.fit.ac.jp	jyo.cs.fit.ac.jp

【手順 1】図 9 同様に、『traceroute』コマンドを用いて自ホストから目的ホストまでの経由ルータを調査する。

【手順 2】手順 1 の結果をもとに、簡単なネットワーク構成図を作成する（形式は図 10 を参考にして良いが、同じ形式にこだわる必要はない）。完成した図を【レポート 6】とする。

7. レポート

レポートは、A4 用紙を用い、次の指示にしたがって作成・提出する。

◆レポート形式

下図を参考にする。複数のメンバで実験を行った場合は、レポート作成例の点線内のように、表紙に共同実験者を記入する（実験時、特に色々教えてもらったり助けてもらったりしたときは、その人を実験協力者として記入する）。共同実験者および実験協力者がいない場合は、点線内を記述する必要はない。また、PC 番号には、自分が実験時に着席した席の座席番号を記入する（掲示している座席レイアウト図を参照する）。

レポートの本文は、本テキスト中【レポート n】と記載されている箇所の指示にしたがって作成する。

レポートは左上をステープラ（ホッチキス）等で綴じる。（両面印刷可／手書き可）

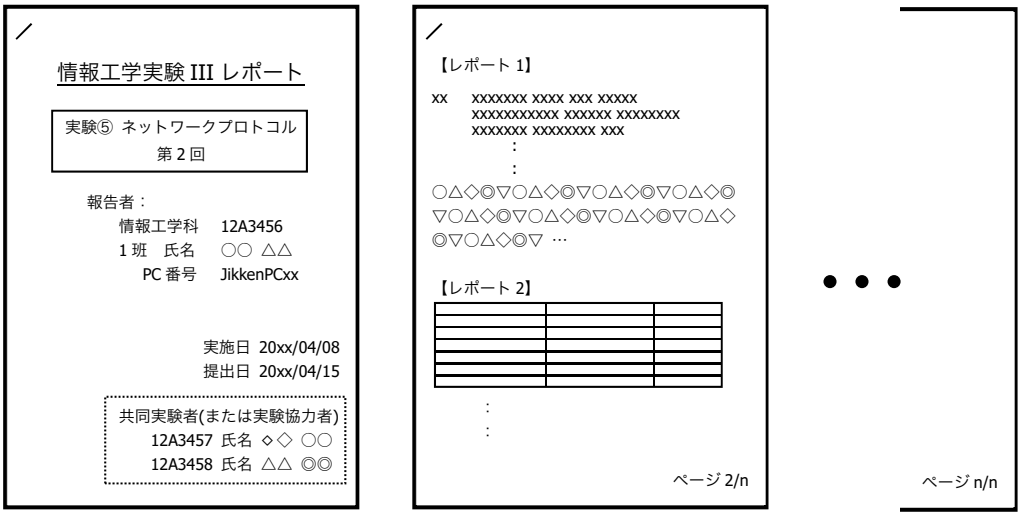

図 11　レポート作成例

◆提出締め切り・方法

次回の『情報工学実験 III』の実験日を提出締め切り日とする。次週の実験（次の実験テーマ）開始前に、実験室 **4**（今回の実験を行った実験室）内の『レポート提出 BOX』へ提出する（実験室 4 施錠時には、C 棟 8F 相良研究室ドアポストへ）。