実験② ネットワークプロトコル　第 2 回

Rel. 20080425A

情報工学実験 III@実験室 4

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。

第 2 回　Linux プラットフォーム上での実験

0. OS の起動とシャットダウン - 1CD Linux ディストリビューション KNOPPIX -

本実験では、Linux プラットフォームとして KNOPPIX を使用する。KNOPPIX とは、CD でブート可能な Linux ディストリビューションで、ドイツの Knopper 氏が Debian パッケージを元に開発し、産業技術総合研究所により日本語対応版に改良されている。

【OS 起動手順】

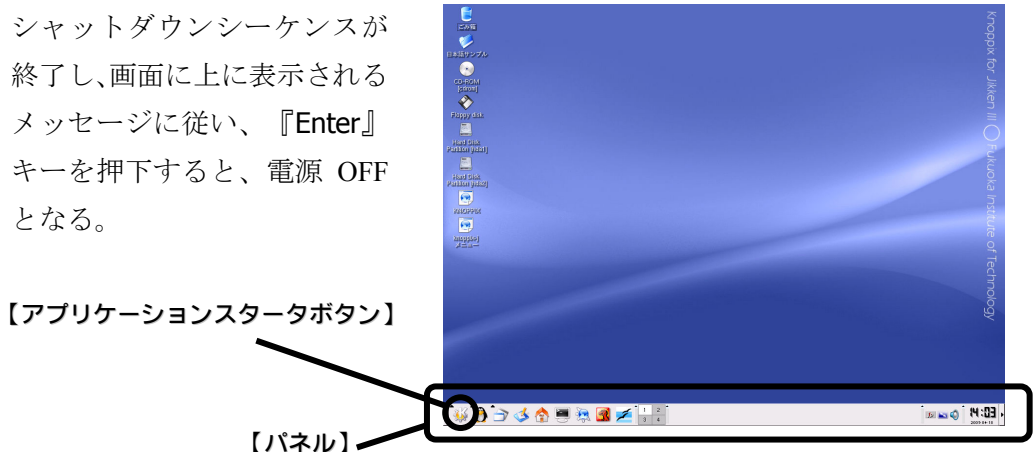
1. PC の電源 ON 後、速やかに CD トレイへ KNOPPIX の CD(CD-R)をセットする。
   ―――――― Windows が起動してしまった場合、再起動する。
2. CD によるブートが開始される。
3. ブート直後、画面下部に『boot:』と表示されたところで、
   a) 『jikken3(Enter)』と入力すると、HDD 内に予め格納された CD イメージ（iso イメージファイル）からの起動に移り、通常より高速に起動する。
   b) そのまま『Enter』キーを押下すると、通常の CD ブートが継続される(遅い)。
4. しばらくたつと、デスクトップ※が現れる。

※ KNOPPIX のデスクトップ環境には、多くの Linux ディストリビューションで採用されている KDE(K desktop environment)が採用されている。

【シャットダウン手順】

1. デスクトップ画面下部（パネル）、左端の『  ボタン（アプリケーションスタータボタン）』-『ログアウト...』と選び、『"knoppix"のセッションの終了』ダイアログに対し、『コンピュータを停止(T)』を選ぶ。
2. シャットダウンが開始される。

3. シャットダウンシーケンスが終了し､画面に上に表示されるメッセージに従い、『Enter』キーを押下すると、電源 OFF となる。



実験 III 用 KNOPPIX(Ver3.7)デスクトップ画面例

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】ターミナルプログラム（シェル- Konsole）を起動する。（パネル上の『  』）

【手順 2】ターミナルプログラム（シェル- Konsole）画面に 『ifconfig』と入力
『eth0』と『lo』との 2 段落に分けて情報が表示されるが、『eth0』の方の『inet addr: 』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『イーサネットアドレス（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。

```
knoppix@ttyp0[knoppix]$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:01:80:xx:xx:xx
          inet addr:150.43.61.xx  Bcast:150.43.61.127 Mask:255.255.255.192
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1868 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1353 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1936659 (1.8 MiB)  TX bytes:201007 (196.2 KiB)
          Interrupt:17 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:474 errors:0 dropped:0 overruns:0 frame:0
          TX packets:474 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:40977 (40.0 KiB)  TX bytes:40977 (40.0 KiB)

knoppix@ttyp0[knoppix]$
```

【自ホストの IP アドレス】

ifconfig コマンド実行画面

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。

```
knoppix@ttyp0[knoppix]$ nslookup www.fit.ac.jp
Note:  nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead.  Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
Server:  cen.ipc.fit.ac.jp              【DNS サーバのホスト名】
Address:  150.43.110.1                  【DNS サーバの IP アドレス】
                                        } DNS サーバに関する情報【参考】

Non-authoritative answer:               →【canonical≒正式な】
www.fit.ac.jp   canonical name = fitweb.ipc.fit.ac.jp.
Name:   fitweb.ipc.fit.ac.jp            【ホスト名(本名)】
Address: 150.43.1.10                    【IP アドレス】
                                        } 問い合わせに対する回答情報
```

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　次表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。

コンピュータの種類	ホスト名	IP アドレス
情報処理センターサーバ 1	pca1io01.bene.fit.ac.jp	
情報処理センターサーバ 2	pca2io01.bene.fit.ac.jp	
情報処理センターサーバ 3	pcbio01.bene.fit.ac.jp	
情報処理センターサーバ 4	pccio01.bene.fit.ac.jp	
毎日新聞	www.mainichi.co.jp	
読売新聞	www.yomiuri.co.jp	
Microsoft	www.microsoft.com	
(任意のサイト 1)		
(任意のサイト 2)		
(任意のサイト 3)		

【手順】　シェル画面に『nslookup（調べたいホスト名 or IP アドレス）』と入力
▼ 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こと。

※注 2　DNS サーバへ問い合わせた結果、「＊＊＊ xxx can't find yyy：zzz... 」と返却されることがある。これは、DNS データベース上に問い合わせに対する回答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プログラムである。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、問題の早期段階での切り分けを行うことができる。ping コマンドは、ICMP プロトコル(Internet Control Message Protocol)を利用している。下図に、ping コマンドの実行例を示す。

```
knoppix@ttyp0[knoppix]$ 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
        :                                                    【応答がある場合】
        :
```

★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）

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　次表のコンピュータに対し、ping コマンドを実行し、表を完成させる。

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.□	
福工大タイムサーバ	fitntp.fit.ac.jp	
情報処理センターサーバ 1	pca1io01.bene.fit.ac.jp	
情報処理センターサーバ 2	pca2io01.bene.fit.ac.jp	
情報処理センターサーバ 3	pcbio01.bene.fit.ac.jp	
情報処理センターサーバ 4	pccio01.bene.fit.ac.jp	
不明なマシン	150.43.248.40	
九州大学	www.kyushu-u.ac.jp	
福岡大学	www.fukuoka-u.ac.jp	
(任意のサイト)		

【手順】 シェル画面に 『ping（ホスト名 or IP アドレス）』と入力
▼ 結果を記録し、完成した表の全体を【レポート 3】とする。

近年のウィルス・ワーム等の流行により、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・ルータ類によって通さない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、経路上でブロック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同士で内蔵時計の時刻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(なお、Windows 上のフリーな NTP クライアントソフトの代表としては『桜時計』等が挙げられる)。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。

以降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。（実験室のパソコンは、ある程度正確な時刻となっており、NTP による時刻合わせの結果が確認しづらい。そこで、内蔵時計の時刻を一度狂わせた上で、NTP による時刻同期を試みる）。

【手順 1】su コマンドにより root ユーザとなり、管理者権限を得る（パソコンの内蔵時計を変更するには管理者権限が必要）。
シェル画面に『su』と入力
▼ プロンプトが『knoppix@ttyp0 [knoppix]』から、『**root**@ttyp0 [knoppix]』へ変わることを確認する。

【手順 2】date コマンドを使用し、内蔵時計を不正な時刻（4 月 1 日 13 時）に設定する。
シェル画面から『date 04011300』と入力
▼ 次の 2 点を確認する。

1. シェル画面に『20xx 年 4 月 1 日 ○曜日 13:00:00 JST』と表示される。
2. デスクトップ画面右下、パネル上の時計が上記日付時刻となる。

【手順 3】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。

シェル画面に『ntpdate　fitntp.fit.ac.jp』と入力

▼ デスクトップ画面右下、パネル上の時計が、正確な(と思われる)日付時刻に変わることを確認する。シェル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。

※注　ntpdate コマンド実行後、ディスプレイ画面がブラックアウトする（真っ黒になる）ことがある。これは、時刻が大きく進んでしまったことにより、スクリーンセーバが誤動作してしまうことによる。Shift キー等の、適当なキーを押下すれば、画面は復帰するのであわてないように。

5. 自ホストに届くパケットを調査する - Ethereal ネットワークアナライザ プログラム -

ここでは、前回の実験（第 1 回）で使用した、Ethereal 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。

◆Ethereal プログラムの起動

（前実験で、su コマンドにより管理者権限を取得した状態の）シェル画面から、『ethereal &』と入力する。

▼ Ethereal が起動することを確認する。

Ethereal 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　Ethereal 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、抽出した結果を次表にまとめる。

※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。

	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】キャプチャを開始する。

Ethereal ツールバー左端の『  』ボタンを押し、出現した『Ethereal: Capture Options』ダイアログで『OK(O)』ボタンを押す。

▼ 『Ethereal: Capture』ダイアログ（下部に『停止(S)』ボタンがある）が出現し、キャプチャが開始されたことを確認する。

【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色々と行ってみる（この色々がポイント）。

【手順 3】キャプチャを終了し、パケットの調査を行う。

『Ethereal: Capture』ダイアログの『停止(S)』ボタンを押す。

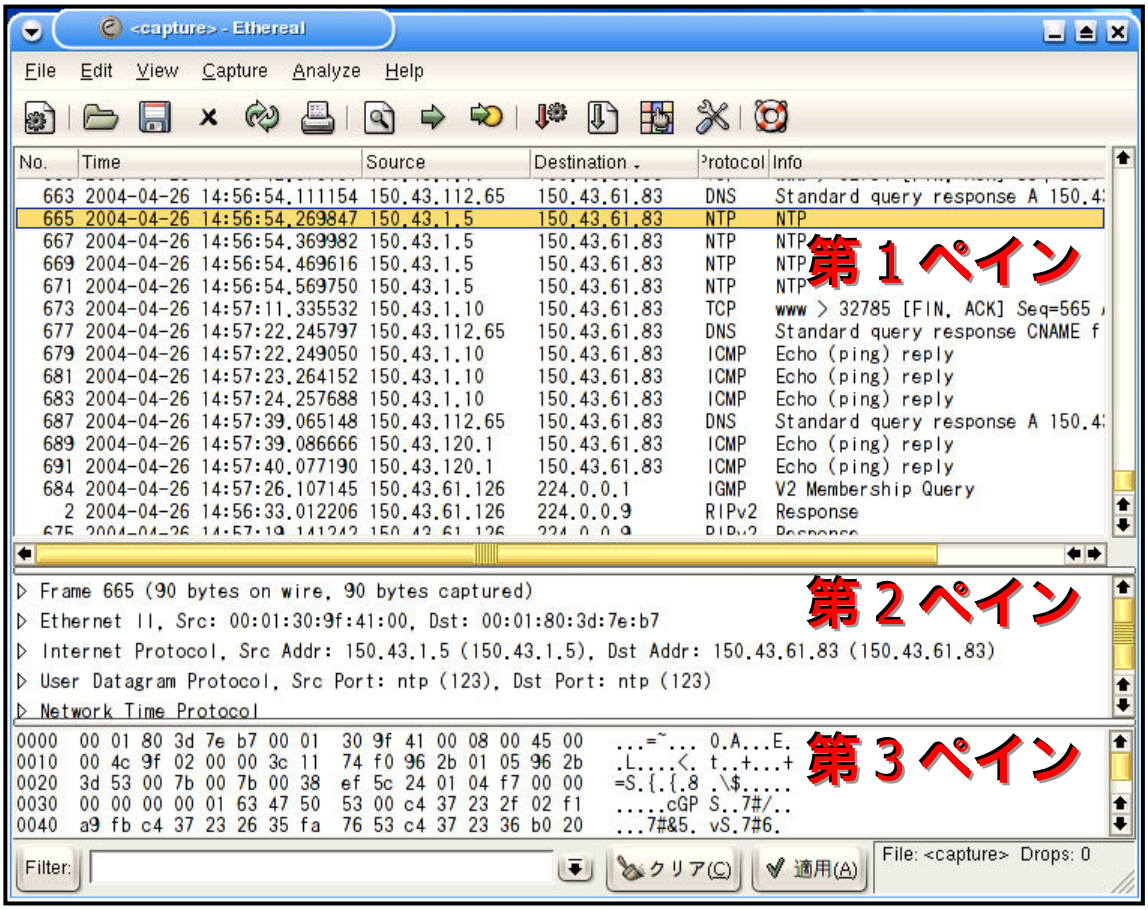
▼ Ethereal のメイン画面が表示されることを確認する。

【手順 4】『Time』フィールドの表示形式を変更する。

『View』-『Time Display Format』-『◎ Date and time of day』をチェックする。（日付時刻の表示形式が、次ページ図のように、[20yy-mm-dd hh:mm:ss.nnnnnn] に変わることを確認する。）

【手順 5】 自ホストあてに届いたパケットから 10 種類抽出し、表を完成させる。完成した表の全体を【レポート 5】とする。

（抽出する 10 種類は、次ページの「注意点・ヒントなど」参照）



Ethereal メイン画面(Time フィールドの表示形式変更後)

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。
- Ethereal でキャプチャしたパケットには、自ホストあて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、自ホストあて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 アドレスとなっているものである。
- 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、1 種類とカウントする。
  （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 Ethereal の画面上には現れない。ただし、前出の nslookup コマンドや、Ethereal の表示オプションの設定等により調査することができる。

★★★　Ethereal 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。

　なお、現在フリーソフトとしての Ethereal の開発は終了しており、その実質的な後継ソフトは、**WireShark** という名称になっています(商標登録の関係上、Ethereal という名称をフリー版が継続使用するのが難しくなったため)。

6. 考察：Konqueror（オプション）

ここでは、多機能な Web ブラウザ／ファイルマネージャである Konqueror を使用したネットワーク越しのファイルアクセスに関して考察する。

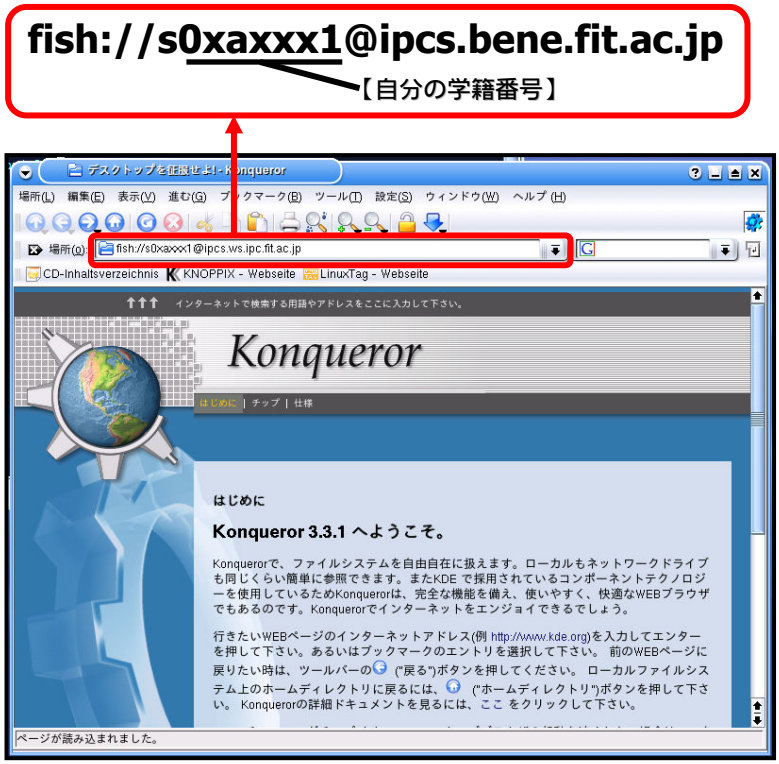
◆Konqueror プログラムの起動

シェル画面から、『Konqueror &』と入力するか、パネル上の『  』を選ぶ。

▼ Konqueror が起動することを確認する。

◆Konqueror によるネットワーク越しのファイルアクセス

【手順 1】　Konqueror の『場所(O)』欄に次の URL を入力する。



【手順 2】　『The authenticity of host ..』との問い合わせダイアログに『はい(Y)』と答え、その後パスワードをきかれるので入力する。

【手順 3】　Konqueror ウィンドウ上に、接続相手のファイル一覧が表示されることを確認する。

◆考察　前述の手順 1～3 によるアクセスについて、次の a) b)を調査し、可能な限りの情報を入手する。

a) 接続相手のサーバについて

b) 接続の際に使用したプロトコルについて

また、これらに

c) 上記 a), b)を調査するにあたってどのような手法を用いたか

を加えた、

a)～c) の内容を【レポート 6 （オプション）】としてまとめる。

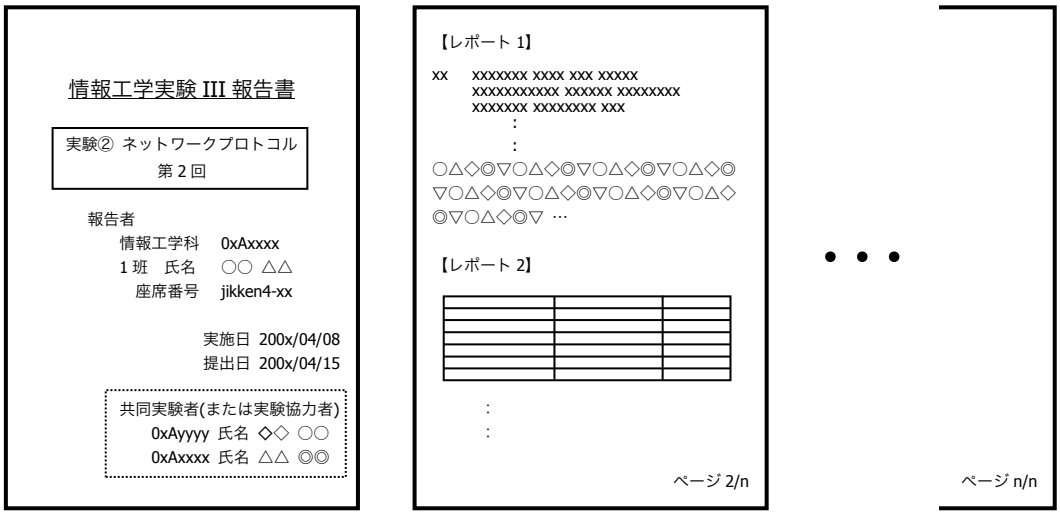
7. レポート

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）。また、座席番号には、自分が実験時に着席した席の座席番号を記入する（黒板の座席レイアウト図か、Windows 起動中であれば『コントロールパネル』-『システム』-『コンピュータ名』を参照する）。

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



レポート作成例

◆提出締め切り・方法

次週の『情報工学実験 III』の実験（次の実験テーマ）開始前に、実験室 **4**(今回の実験テーマ)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）。