メディア・情報教育プロジェクト

高等学校学習指導要領と情報通信ネットワークの理解

情報教育講座　　安本太一

Ⅰ　はじめに

平成 21 月 3 月 9 日に改訂された高等学校学習指導要領 [1]では，普通教科「情報」は，情報 A,情報 B,情報 C からの選択から，``社会と情報''，``情報の科学''からの選択へと再構成された．平成 25 年度の入学生から実施される．

新学習指導要領においては，``社会と情報''，``情報の科学''のどちらにおいても，**``情報通信ネットワークの仕組み''**という小項目がでてくるが，座学だけでは，パケット交換，プロトコル階層，情報セキュリティといったことの理解が困難であることが推測される．本稿では，情報通信ネットワークの仕組みの理解を容易にするための実験を，いくつか提案する．

Ⅱ　新学習指導要領における情報通信ネットワークの扱い

新学習指導要領では，情報通信ネットワークは次のように扱われている．

社会と情報

(1)情報の活用と表現
略

(2)情報通信ネットワークとコミュニケーション

ア コミュニケーション手段の発達
略

イ **情報通信ネットワークの仕組み**
情報通信ネットワークの仕組みと情報セキュリティを確保するための方法を理解させる．

ウ 情報通信ネットワークの活用とコミュニケーション
略

(3)情報社会の課題と情報モラル

ア 情報化が社会に及ぼす影響と課題
略

イ 情報セキュリティの確保
略

ウ 情報社会における法と個人の責任
略

(4)望ましい情報社会の構築
略

情報の科学

(1) コンピュータと情報通信ネットワーク

ア コンピュータと情報の処理
略

イ **情報通信ネットワークの仕組み**
情報通信ネットワークの構成要素，プロトコルの役割，情報通信の仕組み及び情報セキュリティを確保するための方法を理解させる．

ウ 情報システムの働きと提供するサービス
略

(2) 問題解決とコンピュータの活用
略

(3) 情報の管理と問題解決
略

(4) 情報技術の進展と情報モラル
略

プロトコルという用語まで言及があるように，情報の科学の方が，社会と情報より，掘り下げた内容を扱うことになっている．セキュリティについては，どちらにも含まれている．インターネットをはじめとする，情報通信ネットワークは，魔法の箱でなく，仕組みがあって動作している事を理解させたいのであろう．

社会と情報，情報の科学のどちらを学ぶにしても，``情報セキュリティを確保するための方

法”まで扱う事になっているので，詳細に立ち入らずとも，パケット交換，プロトコルの階層化，暗号化の必要性を直感的に理解できるようにすることは，授業で必要であろう．そのためには，通信の様子を目で見て理解できたり，内容が(普段生徒自身が使うあるいは将来使う可能性のある)身近な，実験が必要である．

Ⅲ　提案する実験

普段意識しない事に気がつくことから，情報通信ネットワークへの理解を深めることができる実験を提案する．この方針に基づき，パケットの観察，普段のネットワークアプリケーション利用から情報通信ネットワークの仕組みの推測及びこれらの組み合せから，ⅣからⅦに述べる 4 つの実験を提案する．

Ⅳ　パケット交換の様子を観察する実験

パケット交換方式や多重化についての理解を深めるために，パケット交換の様子を観察する実験を，最初に提案する．図 1 に示すように，ポートミラーリング機能を備えたスイッチングハブとネットワーク・アナライザ・ソフトウェアを使うと，LAN ケーブル上を流れているパケットの観察を容易に行う事ができる．

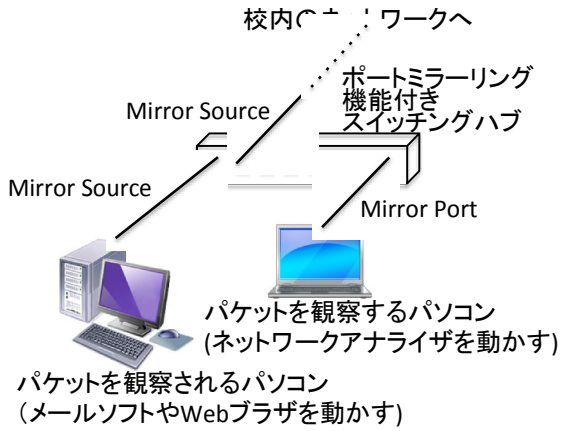

図 1：パケットの観察

ポートミラーリング機能とは，特定のポート(Mirror Source)で受信したパケットを，指定したミラーポート(Mirror Port)にコピーする機能である．アライドテレシス社から，この機能を備えた GS908S-TP という 8 ポートのギガビットイーサネットスイッチングハブが，税抜き価格¥24,800 で発売されている．安価ではないが，購入できないほど高価ではない．図 1 において Mirror Source が 2 ポート指定されているのは，GS908S-TP のポートミラーリング機能が，指定したポートが受信するパケットのみを，Mirror Port にコピーする仕様だからである(送信するパケットはコピーしない仕様である)．ネットワーク・アナライザについては，Wireshark というフリーソフトウェアを使う事ができるので，費用はかからない．

生徒に，本文が 3000 文字以上のメール送信のパケットを Wireshark を用いて見せ，一通のメールが複数のパケットに分割されていることを確認させる．一つのパケットには最大 1500 文字弱まで格納する事が可能であるので，例えば，メールの本文が 3000 文字ならば，3 つのパケットに分かれるはずである．

この様子を図 2 に示す．Wireshark では，メール送信時の本文は，プロトコル階層別表示の最下位の Simple Mail Transfer Protocol のさらに下に，Internet Message Format が出現 して，Line-based text data として表示されるので，本文に対応していないパケットとの区別が容易で，みつけやすい．

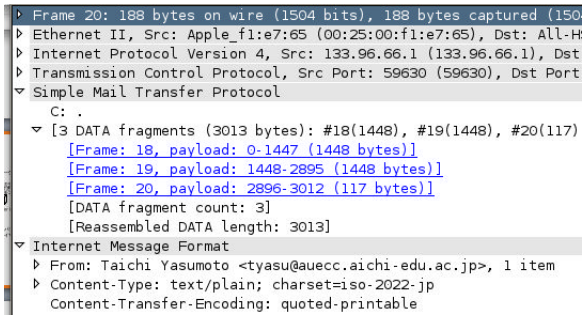

図 2：パケットに分割されたメールの表示

メール本文が分割されてできたパケットは，3 DATA fragments, Frame:18, Frame:19, Frame:20, Reassembled DATA length: 3013 というように表示される．Fame:番号のところをダブルクリックすれば，該当するパケットの表示が行われる．

同様に，ホームページ閲覧(WWW)においても，長い文章や写真を構成するデータが複数のパケットに分割されて，ユーザのコンピュータに送られてくることを生徒に示すと，パケット交換についての理解が深まる．

メールの本文が複数のパケットに分割され

ることを出発点にして，次に示すような，パケット交換方式の特徴を生徒に説明するのが適切である．

- 多重化
  一つの伝送媒体(例えば一本の LAN ケーブル)で，複数の通信が同時にできる．
- 公平性
  パケットの長さの上限が決まっているので，ある通信が，伝送媒体を長時間占有することなく，他の通信へ伝送媒体を明け渡すことが可能である．
- 効率の良いエラーリカバリ
  ビットの誤りや喪失といった，通信の事故が生じた場合は，全ての通信をやり直す必要はない．問題の生じたパケットだけを再送すれば良い．

多重化や公平性の実例は，メール送信のほか，他のネットワークアプリケーション(例えば WWW)や他のコンピュータ間のパケットを含むように Wireshark でパケットを採取して，生徒にみせればよいだろう．

V　パケットの中身の観察の実験

生徒にさらに気づかせる必要があるのは，メールの内容が，第三者にみられる可能性があることである．

図 3 に示すように，Wireshark の右下の方の表示において，通信の内容，すなわち，メールの本文が読み取れる様子を，生徒に見せる．

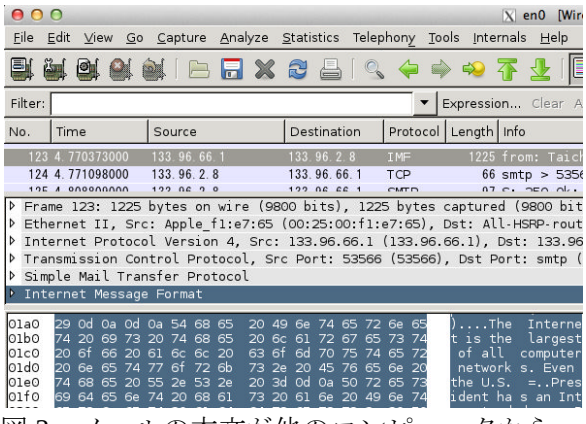

図 3：メールの本文が他のコンピュータからみえる様子

同様に，ホームページの閲覧やホームページの入力フォームへの入力の内容が，Wireshark で読み取れる様子を，生徒に見せる．

もし，学校において使用しているメールサーバが SSL による暗号化通信に対応しているならば，メールソフトウェアの送信メールサーバの設定において SSL を使用するように設定し，再度パケットを見せて，送信しているメールの本文を見ようとしても，意味不明な文字の羅列で暗号化されていることを，生徒に確認させることが望ましい．加えて，メールはバケツリレー方式で配送されるので，メール送信者のパソコンとメールサーバの間の通信が SSL で暗号化されていても，受信者のコンピュータに至るメールの配送経路に暗号化通信の保証がないこと，メール本文の暗号化を望むならば，S/MIME を使うといったメールソフトウェア間の暗号化でないと完全には暗号化できないことを生徒に説明する [2].

一方，ホームページの閲覧(WWW)は，ユーザのコンピュータとホームページのサーバコンピュータとの一対一通信であるから，SSL による暗号化通信(https から始まる URI による通信)は両端のコンピュータ間で有効であることを，暗号化され意味不明な文字の羅列になったパケットの中身を生徒に見せている時に，説明する．

VI　プロトコルの階層化の実験

プロトコルの階層化について理解を深めるため，様々な伝送媒体によるネットワークアプリケーションの利用と，ネットワークアプリケーションの同時利用の 2 つの小実験を行う．

1. 様々な伝送媒体の利用

ノートパソコンにおいて，有線 LAN，無線 LAN，Bluetooth PAN のいずれを使っても，同一のネットワークアプリケーション(例えば，Web ブラウザ Safari)を使用できること，すなわち，有線 LAN 用の Web ブラウザ，無線 LAN 用の Web ブラウザ，Bluetooth 用の Web ブラウザというように別々に使い分ける必要がないことを，生徒に見せるあるいは体験させて，確認させる．

さらに，スマートフォンである iPhone などのテザリング機能を使い，ノートパソコンのインターネット接続を実現する様子をみせる(あるいは体験させる)．無線 LAN, Bluetooth PAN, USB の 3 通りの方法を実践し，どの方法を使っても，同一のネットワークアプリケーション

(例えば，Web ブラザ Safari)を使用できる事を体験させる．

これらの体験から，ネットワークアプリケーションは，伝送媒体を直接利用していないこと，すなわち，伝送媒体から独立していることを，生徒に推測してもらう．

2. ネットワークアプリケーションの同時利用

ネットワークアプリケーションソフトの同時利用，例えば，メールの送受信(電子メールソフトの利用)とホームページの閲覧(Web ブラウザの利用)が同時にできることを，生徒の前で陽にやってみせる．

できることは当然のように思われるかもしれないが，そのためには，コンピュータに到着したパケットをアプリケーション(メールや Web ブラウザ)に振り分けたり，各アプリケーションから送信されたパケットをとりまとめて，コンピュータから送り出す何かが存在することを考えるように，生徒を誘導する．

3. プロトコル階層の推測

上記の 1.と 2.から，生徒に次の 2 点を意識させ，モデル図(プロトコル階層)を描かせる．

- 伝送媒体とネットワークアプリケーションの間に何かある．
- 伝送媒体の上から順に何かが積み重なっている．

最終的に，図 4 のような，おおざっぱなプロトコル階層に到達できるように生徒を誘導する．図 4 は，コンピュータネットワークの専門書にでてくる TCP/IP のプロトコル階層に近い．

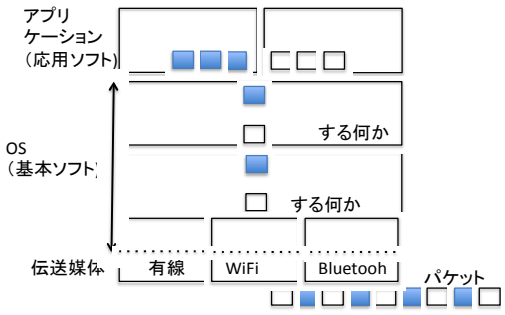

図 4: おおざっぱなプロトコル階層

ここまで到達できると，コンピュータ，スマートフォン，タブレット端末，ゲーム機において，ネットワークアプリケーションが利用できる仕組みを，理解できるのではないだろうか．最近のスマートフォンは，3G, LTE，無線 LAN, Bluetooth のいずれかを選択して，インターネットを利用できるが，それは，図 4 において伝送媒体を切り替えているといった具合である．

Ⅶ　無線 LAN の先のセキュリティの実験

無線 LAN 設定時の注意として，WPA といった暗号化についてよく語られるが，これは無線 LAN アクセスポイントと無線 LAN を使用するコンピュータなどの機器と間の通信のことである．無線 LAN アクセスポイントから先は，有線 LAN であり，無線 LAN の暗号化の機能は及ばず，その先の有線 LAN において，盗聴可能である事を，理解することが重要である．暗号化を徹底したい場合は，アプリケーションの通信の両端で，暗号化をする必要がある．

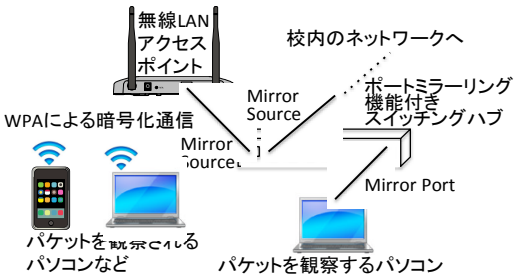

図 5：無線 LAN の先のパケットの観察

図 5 のような状況を用意して，ノートパソコン，タブレット端末，(無線 LAN 接続の)スマートフォンなどから，WPA などの暗号化通信有りで，メール送受信やホームページ閲覧を行う．そのパケットが別のノートパソコンからネットワーク・アナライザを用いて観察でき，パケットの中身まで見えてしまうことを，生徒に確認してもらう．特に，(無線 LAN 接続した)スマートフォンを行き来するパケットの中身が　見えてしまう(盗聴できてしまう)事実は，生徒に大きなインパクトを与える事が期待できる．

次に，同じく図 5 のような状況において，SSL 暗号化通信を伴うメールの送受信やホームページアクセス(https からはじまる URI へのアクセス)を試す．そして，別のパソコンからパケットを観察したとき，パケットが流れていることはわかるが，内容が暗号化されて判別できないことを生徒に確認してもらう．

これらの暗号化通信の設定は，OS のシステムのネットワークの設定(OS X ではシステム環境設定，Windows ではコントロールパネル)ではなく，アプリケーション毎に行われていることを，生徒に改めて認識させる．さらに説明を進めて，インターネットを構成しているネットワークは，メールやホームページのデータを送ることをするだけで，セキュリティについて，何も責任を負わないことを生徒に認識させる．

Ⅷ　実験を分かりやすくするための配慮

実験は，配慮によって，格段に解りやすくなる．ネットワーク・アナライザによるパケットの表示に加えて，スイッチングハブの Traffic ランプの点滅もきちんと生徒に説明し，パケットがハブを流れている様子を生徒に想像させる．適切に説明を続ければ，パケット交換方式おいては，一つの通信が，伝送媒体やハブのポートを占有せず，多重化の余地があることの理解に役立つ．

実験における，メールの本文やホームページの内容は，英文にすべきである．Wireshark を始めとするネットワーク・アナライザ・ソフトウェアは，一般に日本語文字データの復号化に対応していないからである．そのため，パケットの中身を観察するとき，英語文字データでなければ，(非暗号化通信の)パケットが盗聴可能である事が実感としてわからない．

Ⅸ　まとめ

情報通信ネットワークの仕組みのうち，現在のインターネット(や事業所や家庭の中のネットワーク)で使われている，パケット交換方式の理解に役立つような実験を提案した．パケットは目で直接見ることはできないことから，座学だけでは，パケット交換方式の実際を理解する事は難しい．

ポートミラーリング機能を有するスイッチングハブとネットワーク・アナライザ・ソフトウェアを用いると，パケットの可視化が可能となる．新たに購入すべき物は上記のハブと LAN ケーブル 1 本であり，費用と準備に多くを必要としない．

ネットワークアプリケーションの利用において普段何気なくできていることを，改めて関心をもって考えてみると，プロトコルの階層化の説明ができることを示した．

情報通信ネットワークの仕組みがわかることは，利便性の追求，セキュリティの確保，トラブル解消，新しい技術へ対応するためのセンスを涵養するために，必要である．

参考文献

[1]高等学校学習指導要領解説　情報編，文部科学省，2010 年 5 月．
[2]安本太一：高等学校学習指導要領改訂案と電子証明書について，愛知教育大学 大学・附属学校共同研究会報告書，pp. 141-145，2010 年 3 月．