

インターネットの中の中の中を見る -インターネットを分解してみよう-

インターネット



インターネットの分解って何かな、パソコンやルーターを分解するのかな

でも、中の中の中ってなんだろう。

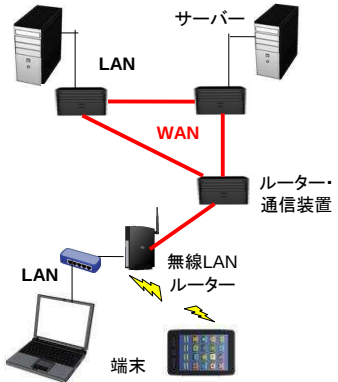
普段インターネットを使っている時はその中の仕組みを意識する必要はありません。ただし、トラブルが発生した時や機器の設定、セキュリティの設定などでは、仕組みを理解していた方がいいでしょう。




画像引用: <http://blogs.yahoo.co.jp/pory61dw8000/23284822.html>

© Go Ota, 2015/02/12 1

インターネットの見える部分



インターネットの目に見える部分としては、次のようなハードウェアがあります。

- ・サーバー: インターネット上でサービスを提供する。
- ・通信回線: データを電氣的に通信する。
- ・ルーター: データの通信を制御する。
- ・端末: PC、タブレット、携帯などでインターネットを使用する

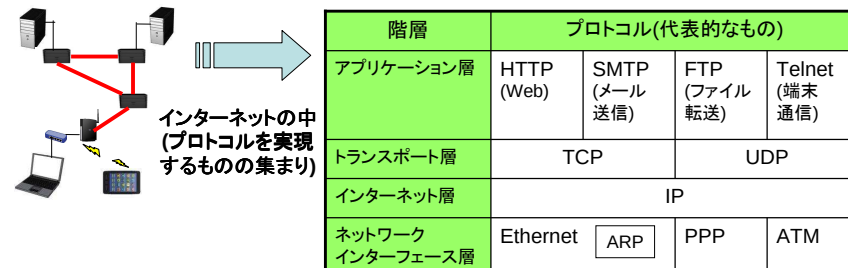
目に見える部分としてルーターや通信装置はいろいろな形態があります。例えばWANの通信回線だけでも有線(光ファイバー、メタル)と無線(衛星通信を含む)などあり、皆さんが聞いたこともあるイーサネット以外にATMやFDDIなどの通信機器が使われています。



2

インターネットの中を見る: インターネット・プロトコル・スイート

インターネット・プロトコル・スイート



インターネットの中ってなんでしょう？ インターネット自体、いろいろなハードやソフトから作られていますが、何を中身と呼んだらいいのでしょうか？

一つの見方としてインターネット・プロトコル・スイートというものがあります。これはインターネットとして通信など動作するため、またウェブのようなサービスを提供するための約束や手順に従って作られたもの(ハード・ソフト)の集まりを示します。

例えばHTTPのプロトコルに従ってWebを実現するものにはサーバーとブラウザもあるし、またブラウザにもいろいろな種類があります。これらをすべて合わせて、プロトコル・スイートと呼んでいます。

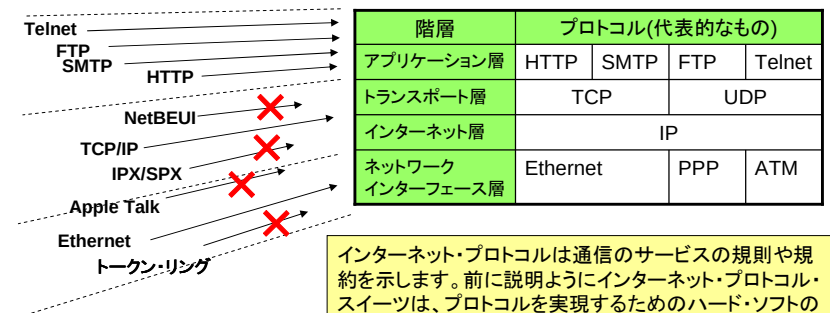
プロトコルはもう少し後で説明します



3

インターネット・プロトコルは一日にしてならず

ネットワーク・LANの歴史 (1970年～)



インターネット・プロトコルは通信のサービスの規則や規約を示します。前に説明ようにインターネット・プロトコル・スイートは、プロトコルを実現するためのハード・ソフトの集まりを示します。

インターネット・プロトコル・スイートは今の形が急に割れではありません。1970年代から多くの製品や規格(プロトコル)が集まった物です。

下位の層ではいろいろな物がありましたが、TCP/IPがベースになり、Ethernetが主流です。アプリケーションではインターネット以前のものも残り、現在でも多くのものが開発され続けています。

4

いろいろな意味を持つTCP/IP

TCP/IP(プロトコル):
インターネット・プロトコルと同等の
意味

TCP/IP:
UDPを含めたトランスポート層とIP
のインターネット層を合わせた物

TCP:
パケットでデータを確実に転送する
通信方法のプロトコル

階層	プロトコル(代表的なもの)			
アプリケーション層	HTTP	SMTP	FTP	Telnet
トランスポート層	TCP		UDP	
インターネット層	IP			
ネットワーク インターフェース層	Ethernet		PPP	ATM

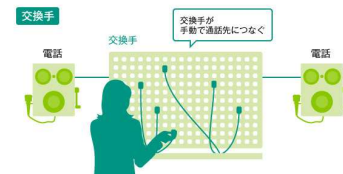


TCP/IPが設計・開発された時に、すでに、これまで示した階層構造や基本的に仕組みがすでにできあがっていました。別の見方をするとTCP/IPをもとにして作られた世界的なネットワークがインターネットであるとも考えることもできます。

インターネット(Internet)はInter=間、相互とNetwork=通信網を合わせたものと理解されますが、TCP/IPが生まれた米国国防高等研究計画局では、TCP/IPが動き始めた時あたりから、これを使ったネットワークをインターネットと呼んでいたという話もあるようです。あと、初めはTCPという規格の中にTCPとIPの機能がありましたが、後にTCP/IPという規格の名前に変更されました。

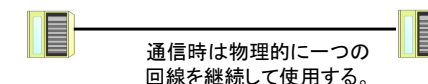
どうしてTCP/IPは生まれたか (TCP トランスポート層)

昔の電話の交換手による接続

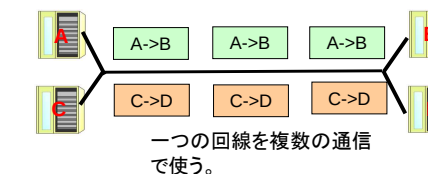


昔の電話は交換手が一本一本線を繋いで通話していました。コンピュータも以前は、一本の線をつなぐことによって通信していました。電話と違ってコンピュータは常に通信しているわけではなく、回線を効率的につかう方法が必要になりました。そこで通信の内容のデータを細かく分けて荷物のようなパケットにして、同じ回線を複数のコンピュータで利用できるようになりました。このパケット交換の方法としてTCPが生まれました。

回線交換によるコンピュータのデータ通信



パケット交換によるコンピュータのデータ通信



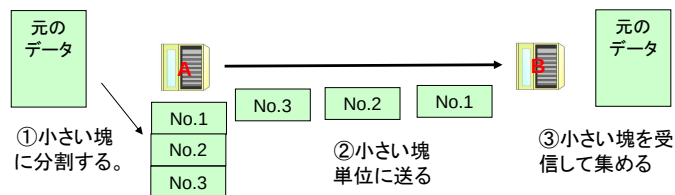
画像引用:NTT東日本 http://www.ntt-east.co.jp/business/magazine/nw_system/01/



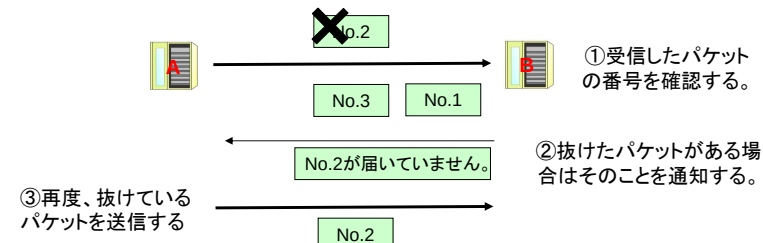
6

TCP/IPの具体的な通信方法 (TCP トランスポート層)

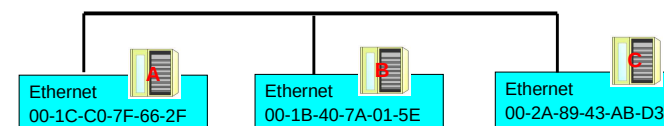
パケットに分割した通信



パケット通信で途中でパケットが無くなった場合



IPはどうして生まれたか? その前に根本の通信方法



AからCへ送る場合の一つのパケット内容

	送信先	送信元
パケットとして分割されたデータ	00-2A-89-43-AB-D3	00-1C-C0-7F-66-2F

ネットワークで通信を行う装置としてEthernetにはMACアドレス(マック・アドレス、Media Access Control address)と呼ばれる物理アドレスが番号がつけられています。原則として個々の製品が作られた時に、アドレスが与えられ世界中にあるMACアドレスは重複がありません。

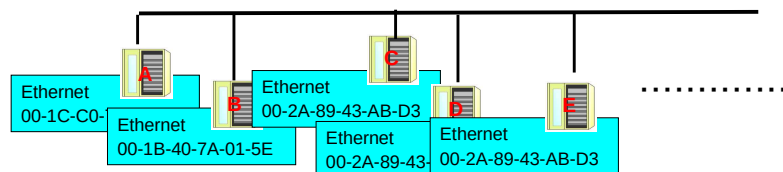
コンピュータ同士の通信は、最終的には物理アドレスをもとに行われます。Ethernetの場合は、個々のパケットには送信先と送り先のMACアドレスとデータが入ります。受信するコンピュータは、送信先に自分のMACアドレスが入っているパケットだけを取り出して処理します。



8

7

IPはどうして生まれたか？ 世界中で物理アドレスだけで通信すると



例えばアメリカのパソコンから日本のパソコンにパケットを使ってデータを送る場合

問題点1
おくる場合に相手のパソコンのMACアドレスを知らないと送れない。MACアドレスはパソコンを変えたと変わってしまう。

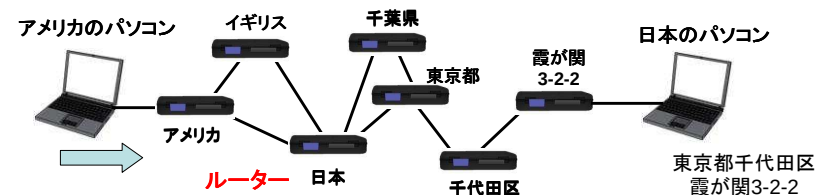
問題点2
少なくともアメリカと日本のパソコンが全部一つの線につながっていると、そこに流れるパケットは非常に多く、自分宛てのパケットを探すのが非常に難しくなる。

実際に1本の通信回線が使用出来たり、家庭や1フロアなどでは、物理アドレスだけのデータ通信が可能です。但し、不特定多数のパソコン同士で通信する場合は限界があります。



9

IPはどうして必要か？ IPアドレスとルーター



物理アドレスだけで通信する問題点を解決する方法がIP層で、ここではIPアドレスとルーターという2つが働きます。IPアドレスは物理アドレスにつけられた住所みたいなものです。また、ルーター自体はこのIPアドレスをもとに、どのような経路でデータを送ればいいのか知っている機械で、また、その経路にあるルーターが丁度伝言ゲームのように、パケットを送っていきます。例えば、上図でアメリカから日本の比喻で「東京都千代田区霞が関3-2-2」のパソコンにデータを送る場合は、まず「アメリカ」ルーターから「日本」ルーターへ送信します。次々「日本」->「東京」->「千代田区」->「千代田区」->「霞が関3-2-2」のルーターへパッケージが伝言されます。ルーティングには最適なルートを見つける機能もあり、例えば「アメリカ」->「日本」の回線が使えない場合、イギリス経由で送ることもあります。

東京都千代田区
霞が関3-2-2
IPアドレス
=202.232.190.211

注意:
この説明で使用している住所はあくまで比喻で、実際のインターネットは、このように明確に地域や地区で分けられているものではありません。

10

インターネットの中の中を見る: プロトコルって何

階層	プロトコル(代表的なもの)			
アプリケーション層	HTTP	SMTP	FTP	Telnet
トランスポート層	TCP		UDP	
インターネット層	IP			
ネットワーク インターフェース層	Ethernet		PPP	ATM

ファーストフードのプロトコル



「いらっしゃいませ、こんにちは」
「店内でお召し上がりでしょうか？」→
←「はい」
「かしこまりました」
「何ご注文しますか」→ 「ハンバーガー」
←「セットを」
「セットのお飲み物をお選びください」→
←「コーラください」
「かしこまりました」
「ほかにもご注文はございますか？」→
←「いや、いいです」

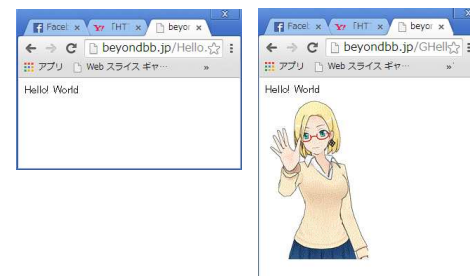
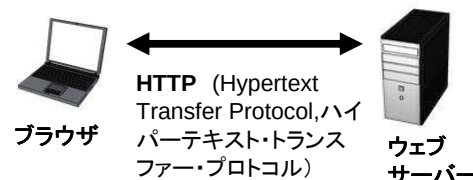


プロトコルは通信規約又は通信手順という意味です。通信の場合は2個の機械でデータのやりとりをするため、その手順や約束を決めていないと、うまく会話することができません。人間の世界でもプロトコルがあります。明確なものではありませんが、ファーストフードで注文するときも暗黙のプロトコルが存在するかと思います。



11

インターネットの中の中を見る: ウェブのプロトコルを見る



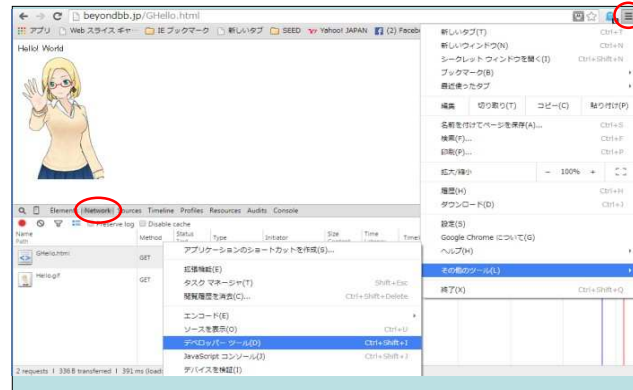
ホームページを見る場合は、ブラウザからウェブサーバーに見たいページを送るように要求します。このときのやりとりはHTTPというプロトコルに従って行われます。ここでは、単純なページを表示するときに、どのような通信が行われているか見ていきましょう。

ネットワーク上ではいろいろなサービスがありますが、サービスを要求する方をクライアント、サービスを提供する方をサーバーと呼びます。



12

ブラウザの機能を使ってウェブのプロトコルの概要を見る - Chrome編-

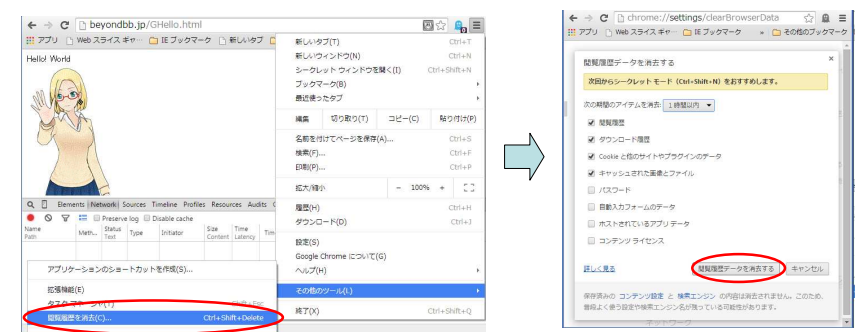


Chromeの「その他のツール」の「デベロッパーツール」の中の「Network」を見てみましょう。Chromeのネットワークのやりとりを表示することができます。



上図のように「Network」のウィンドウが開いたら
<http://beyondbb.jp/Hello.html>
<http://beyondbb.jp/GHello.html>
<http://beyondbb.jp/no.html>
 をアクセスしましょう。どんなふうに動作しているか判りますか？

ブラウザの機能を使ってウェブのプロトコルの概要を見る その2 - Chrome編-

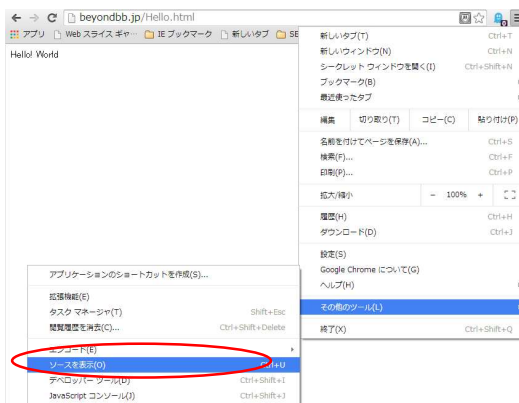


履歴データを消してからアクセスすると、結果がどうなるか確認しましょう。一回ごとに履歴を消して確認してください。



14

送られてきたHTMLファイルを見る - Chrome編-

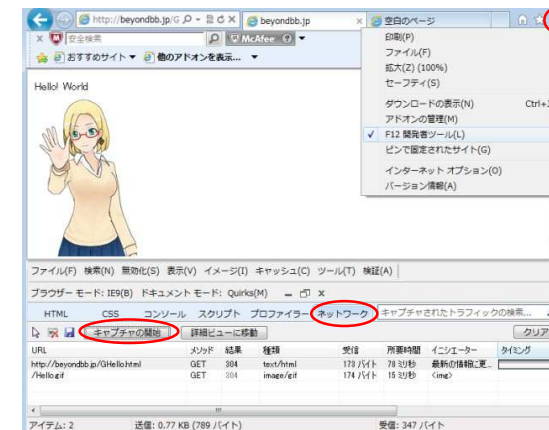


HTMLファイル

現在表示されているブラウザ画面のもとになっているHTMLファイルの内容を表示することができます。ブラウザはこのHTMLをもとに、画面を表示しています。

15

ブラウザの機能を使ってウェブのプロトコルの概要を見る - IE編-

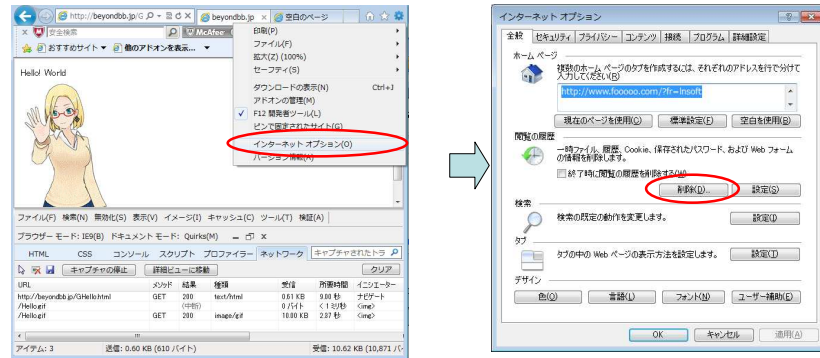


IEの「開発者ツール」の「ネットワーク」を見てみましょう。ブラウザのネットワークのやりとりを表示することができます。



上図のように「キャプチャー開始」を指定した後
<http://beyondbb.jp/Hello.html>
<http://beyondbb.jp/GHello.html>
<http://beyondbb.jp/no.html>
 をアクセスしましょう。どんなふうに動作しているか判りますか？

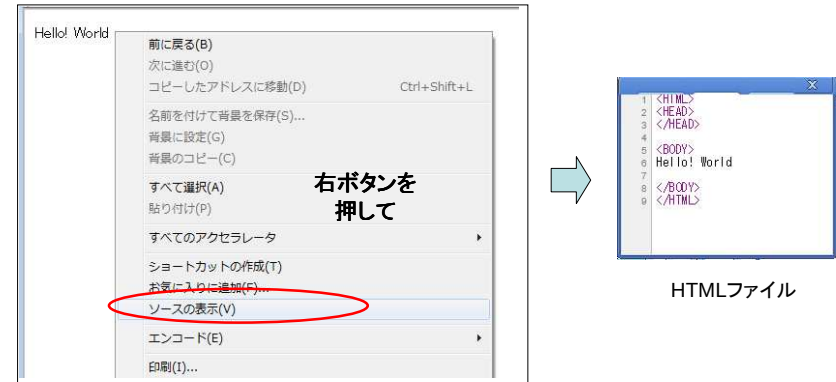
ブラウザの機能を使ってウェブのプロトコルの概要を見る その2 -I.E編-



履歴データを消してからアクセスすると、結果がどうなるか確認しましょう。一回ごとに履歴を消して確認してください。

17

送られてきたHTMLファイルを見る -I.E編-

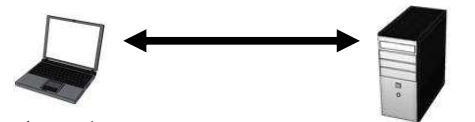


HTMLファイル

現在表示されているブラウザ画面のもとになっているHTMLファイルの内容を表示することができます。ブラウザはこのHTMLをもとに、画面を表示しています。

18

HTTPのウェブのプロトコルの流れの概要



正しいファイルを指定した場合(A)

GET http://beyondbb.jp/Hello.html

← ステータス 200 "OK"
Hello.htmlファイルの内容

正しいファイルを指定した場合(B)

GET http://beyondbb.jp/Hello.html

← ステータス 304 "Not Modified"

存在しないファイルを指定した場合

GET http://beyondbb.jp/Hello2.html

← ステータス 404 "Not Found"

ウェブサーバーとパソコンの間のHTTPのプロトコルは非常にシンプルです。GETで表示するファイル名を要求すると、サーバーがそのファイルの内容を返します。もしファイルが無い場合は、見つからないことを示す、404というステータスを返します。

"Not Modified"が帰ってきた場合は、普通はキャッシュで持っている情報が最新なので、それを表示します。

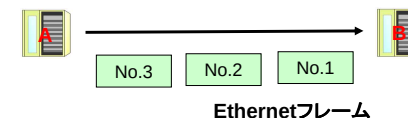


19

インターネットの中の中の中を見る



コンピュータの中の情報は電氣的なオン・オフで表されています。通信を行う場合でも基本は同じです。ではインターネットの中(プロトコル)の中(プロトコルの流れ)の中(1/0で表せる通信の内容)を見ていきましょう



パケット交換の場合、送りたい情報は小さいパケットに分けられて送ると説明しました。ここでは、このパケットを見ていきましょう。また、現在はEthernetが主流ですので、このEthernetのパケットであるEthernetフレームを見ることになります。



20

Ethernet フレームの構成

階層	プロトコル(代表的なもの)			
アプリケーション層	HTTP	SMTP	FTP	Telnet
トランスポート層	TCP		UDP	
インターネット層	IP			
ネットワーク インターフェース層	Ethernet			

1つにEthernetフレームはインターネットプロトコルの構成に対応しています。各階層の情報が順番に積み重なって、一つのフレームができあがります。

アプリケーションの情報

分割1	分割2		分割n		分割last
-----	-----	------	-----	------	--------

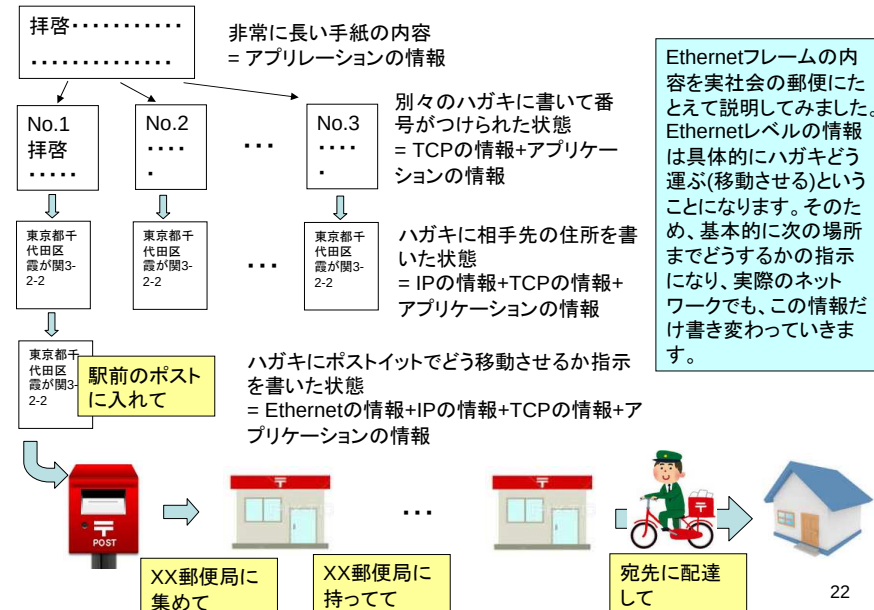
アプリケーションの情報(分割)			
アプリケーションの情報(分割)	TCPの情報		
アプリケーションの情報(分割)	TCPの情報	IPの情報	
アプリケーションの情報(分割)	TCPの情報	IPの情報	Ethernetの情報

1つのEthernetフレーム



21

Ethernet フレームをもとにした通信と実社会の郵便の配達の対比



22

インターネットの中の中の中を見るための基本情報の収集(1) パソコンの情報



インターネット層	IPアドレス
ネットワーク インターフェース層	Ethernet: MAC/物理アドレス

コマンドで
ipconfig /all
で使っているパソコンのMAC/物理アドレスとIPアドレスを調べることができます。

```

C:\>ipconfig /all

Windows IP 構成

Wireless LAN adapter ワイヤレス ネットワーク接続:

   接続固有の DNS サフィックス . . . . . : 
   説明 . . . . . : Atheros AR9285 Wireless Network Adapter
   物理アドレス . . . . . : 78-00-08-04-22-08
   DHCP 有効 . . . . . : はい
   自動構成有効 . . . . . : はい
   IPv4 アドレス . . . . . : 192.168.11.7(優先)
   サブネット マスク . . . . . : 255.255.255.0
   リース取得 . . . . . : 2015年2月8日 5:47:11
   リースの有効期限 . . . . . : 2015年2月10日 12:56:00
   デフォルト ゲートウェイ . . . . . : 192.168.11.1
   DHCP サーバー . . . . . : 192.168.11.1
   DNS サーバー . . . . . : 192.168.11.1
   NetBIOS over TCP/IP . . . . . : 有効

   物理アドレス . . . . . : 00-00-00-00-00-00-E0
   DHCP 有効 . . . . . : いいえ
   自動構成有効 . . . . . : はい
  
```

これからフレームの中をみますが、そこに入っている通信に必要なアドレスを調べておきましょう。まずパソコンのアドレスです。



23

インターネットの中の中の中を見るための基本情報の収集(1) パソコンの情報



コマンドで
nslookupでサーバー名からIPアドレスを調べることができます。

```

C:\>nslookup

Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\F0wner>nslookup
既定のサーバー: Unknown
Address: 192.168.11.1

> beeyondbb.jp
サーバー: Unknown
Address: 192.168.11.1

制限のない回答:
名前: beeyondbb.jp
Address: 202.218.79.73
  
```

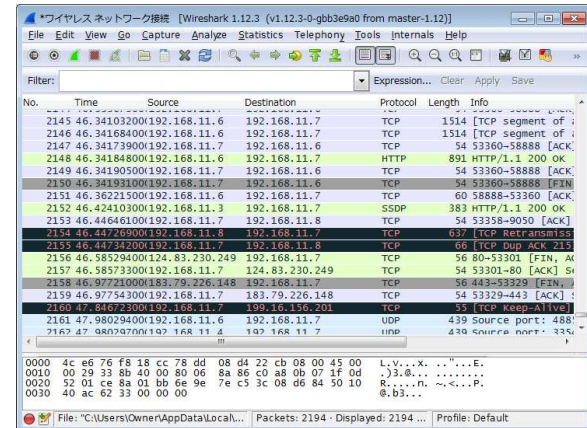
相手になるウェブサーバーのIPアドレスも調べましょう。



24

インターネットの中の中の中を見るツール

ネットワークアナライザネットワークプロトコルアナライザ

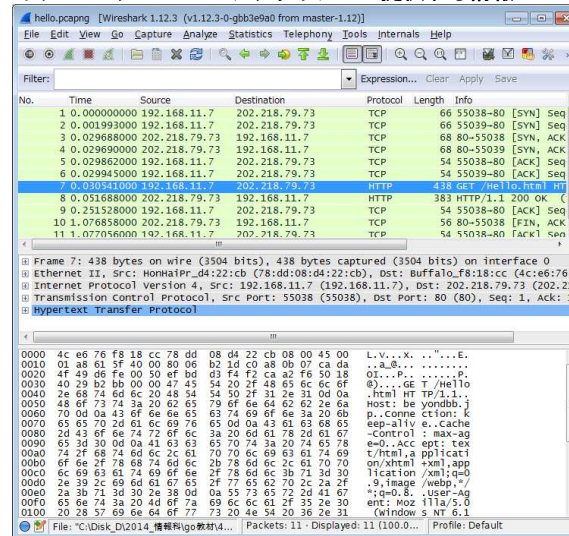


ネットワークアナライザを使うと、パソコンやLANの中の通信の内容を詳細まで見ることが出来ます。またプロトコルアナライザとして、どのようなプロトコルの流れで動作しているか表示・分析できます。



25

ネットワークプロトコルアナライザが提供する情報



多くのネットワークプロトコルアナライザは下記のような情報をキャプチャーし提供します。

フレームリスト

ネットワーク上を順番に流れたフレームのリストで発信元・送信先や使用しているプロトコルなどの概要の情報が個々のフレームごとに表示。

フレーム詳細

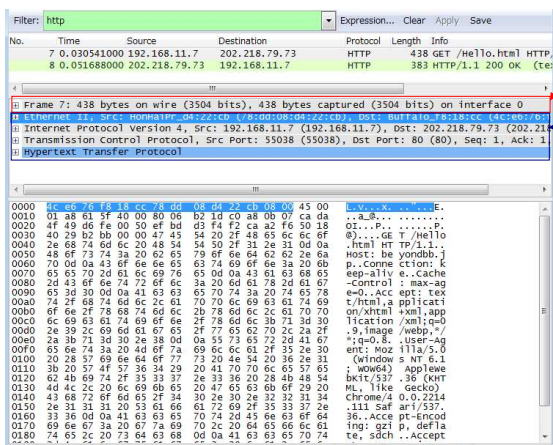
フレームリストで選択したフレームの内容の詳細を表示。

フレームの生データ

フレームの1/10データを16進数とテキストで表示。(フレームの詳細はこの1/10データの意味を表示したもの)

26

フレームの中の階層を見る



フレーム全体の情報

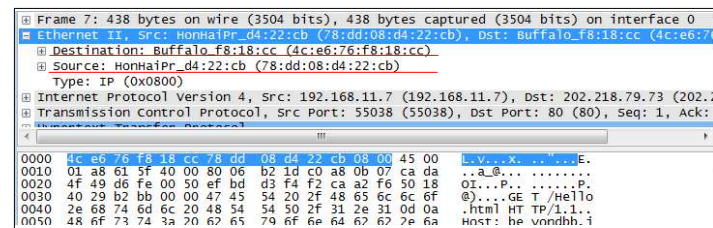
フレームが438バイトの大きさであることを示す。

フレームの中の階層に対応した分析結果

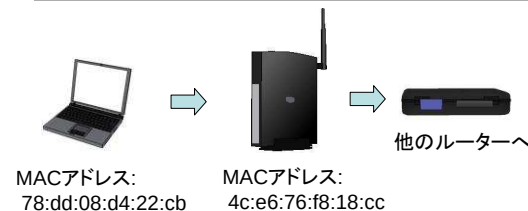
Ethernet, IP(Internet Protocol), TCP(Transmission control protocol), HTTP(Hypertext Transfer Protocol)の4階層情報がフレームに入っていることを示す。

上のウィンドウのフレーム詳細で指定したプロトコルがどの生データに対応するか色が変わる。(この図ではIPを指定した場合)

フレームの中の個々の階層を見る: Ethernet



この階層のプロトコルの内容を見ることが出来ます。



27

パソコンから出ているフレームはまず、最初にデフォルトゲートウェイとよばれるルーターに送信されるのが判ります。家庭などではインターネットに接続されている無線LANルーターなどにあたります。これは、前に説明したまづハガキを郵便ポストにいれるような作業に類似しています。

28

フレームの中の個々の階層を見る: HTTP

[illegible]

この例では、ウェブサーバーからの返信のフレームを見ています。ステータスが200 "OK"だということがわかります。またフレームの中には、要求したHTMLファイルの内容が入っています。

今度はアプリケーション層の
情報を見てみましょう。



参考: OSI参照モデルとTCP/IPプロトコル

OSI参照モデル

レイヤー	階層
7	アプリケーション層
6	プレゼンテーション層
5	セッション層
4	トランスポート層
3	ネットワーク層
2	データリンク層
1	物理層

OSI参照モデル (OSI reference model) は、国際標準化機構 (ISO) によって策定された、コンピュータの持つべき通信機能を階層構造に分割したモデルである。通信機能 (通信プロトコル) を7つの階層に分けて定義している。OSI自体は普及せず、OSI参照モデルがネットワークの基本モデル (概念) として広く参照されるようになった。

TCP/IP プロトコル

階層	プロトコル(代表的なもの)			
アプリケーション層	HTTP	SMTP	FTP	Telnet
トランスポート層	TCP		UDP	
インターネット層	IP			
ネットワーク インターフェース層	Ethernet		PPP	ATM

OSI参照モデルはあくまで現在では理論的なものと考えた方がいいと思います。またTCP/IPプロトコルはOSI参照モデルとは先に、別に開発された現在最も普及しているものです。よくTCP/IPの階層をOSI参照モデルで説明したものがありますが、あくまで、対応を考えた場合のもので、但し公式な試験などではISO参照モデルが出てくることもあります。

