introフェーズ

本日のやること

・プロトコルについて

・パケット解析（Wireshark）

先にWiresharkのインストール

インストール先

- https://www.wireshark.org/download.html

参考

- https://beginners-network.com/wireshark.html

プロトコル

プロトコルとは、

”””通信におけるプロトコルとは、複数の主体が滞りなく信号やデータ、

情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。”””

引用：IT用語辞書 e-Words

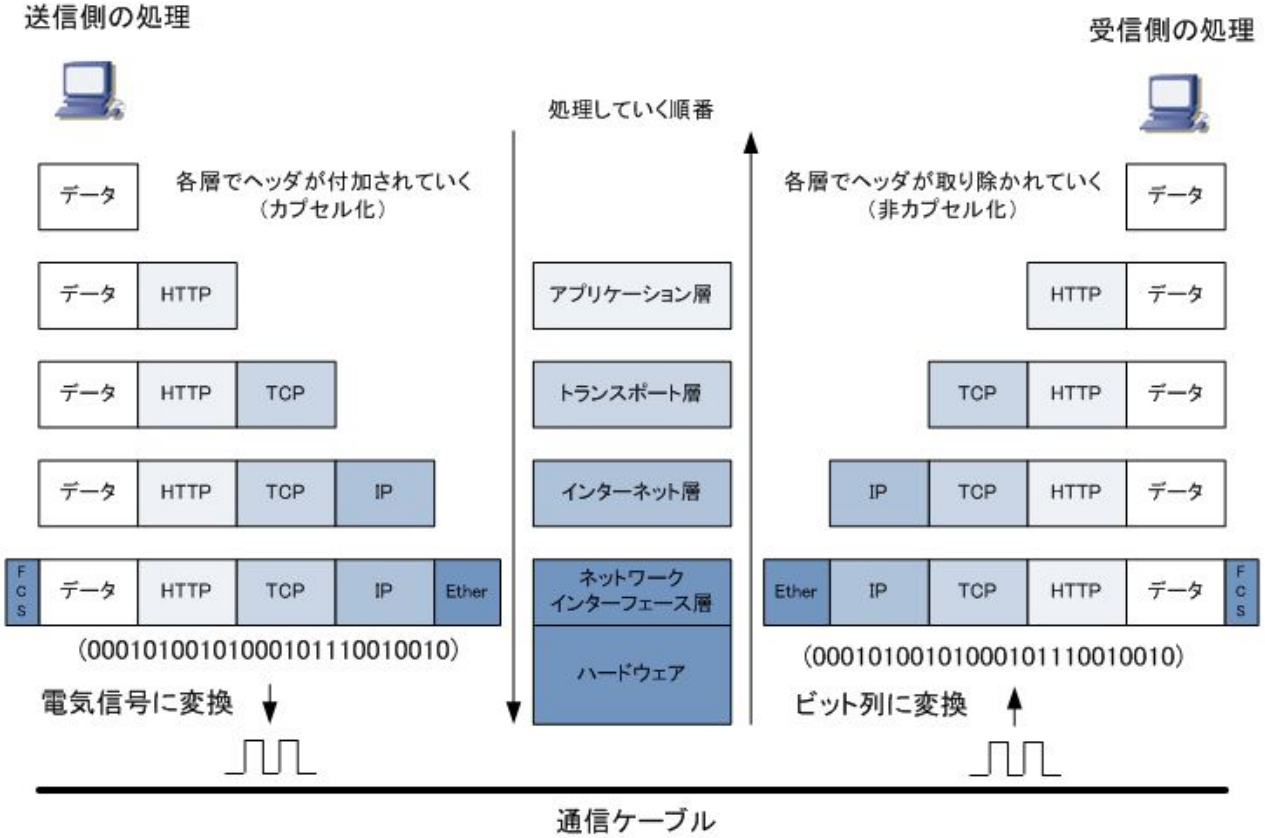
階層ごとのプロトコル

<table>
<tr><th>OSI参照モデル</th><th>TCP/IPの階層モデル</th><th>TCP/IPプロトコル</th><th>コンピュータ上の処理</th></tr>
<tr><td>アプリケーション層</td><td rowspan="3">アプリケーション層</td><td rowspan="3">HTTP, SMTP, POP3
FTP, SSH, RIP, SNMP...</td><td rowspan="3">通信アプリケーション
プログラム</td></tr>
<tr><td>プレゼンテーション層</td></tr>
<tr><td>セッション層</td></tr>
<tr><td>トランスポート層</td><td>トランスポート層</td><td>TCP, UDP</td><td rowspan="2">OS</td></tr>
<tr><td>ネットワーク層</td><td>インターネット層</td><td>IP, ARP, ICMP, OSPF...</td></tr>
<tr><td>データリンク層</td><td rowspan="2">ネットワーク
インターフェース層</td><td rowspan="2">Ethernet, PPP...</td><td rowspan="2">デバイスドライバ
NIC</td></tr>
<tr><td>物理層</td></tr>
</table>

出典：https://www.infraexpert.com/study/tcpip.html

今回見てみるプロトコル

- HTTP
- TCP・UDP
- IP
- (Ethernet)



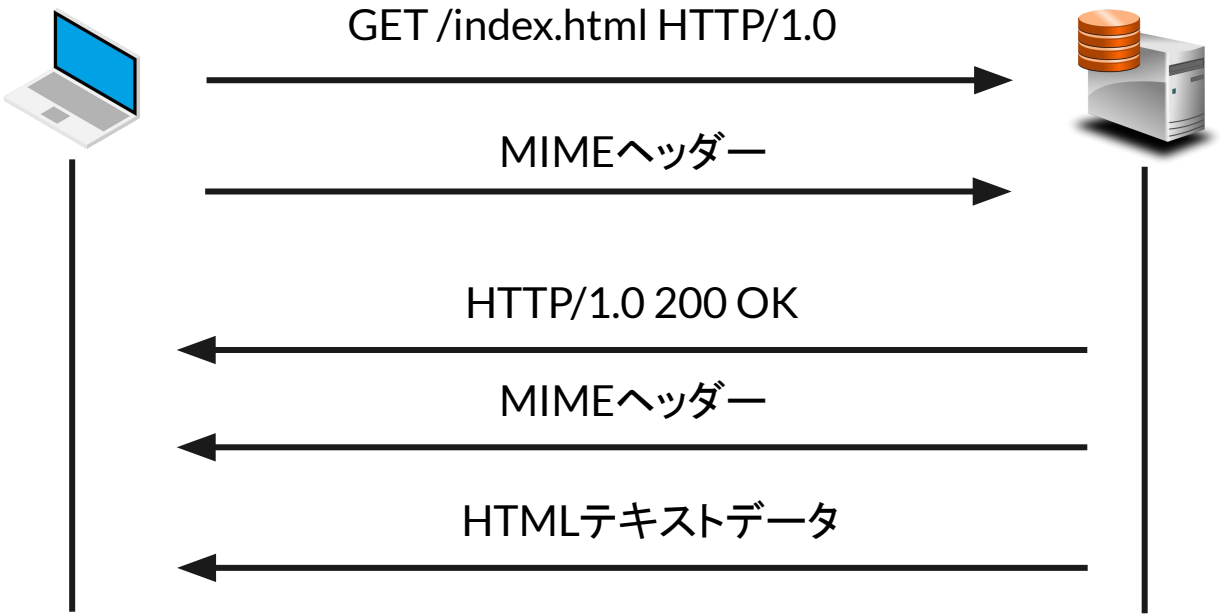
出典：https://www.infraexpert.com/study/tcpip.html

HTTP

“”ブラウザとサーバー間の通信に使われるプロトコル””

- **文書・画像・音声・動画**を送受信する際に利用する
- 送信に主に使われるフォーマットが**HTML**

HTTP


GET /index.html HTTP/1.0
MIMEヘッダー
HTTP/1.0 200 OK
MIMEヘッダー
HTMLテキストデータ

TCP・UDP

TCP

コネクション型のプロトコル.

UDP

コネクションレス型のプロトコル

TCP

出典：https://www.infraexpert.com/study/tcpip8.html

UDP

出典：https://www.infraexpert.com/study/tcpip12.html

IP

IPとは、

””IPとは、複数の通信ネットワークを相互に接続し、データを中継・伝送して一つの大きなネットワークにすることができる通信規約（プロトコル）の一つ。””

引用：「IT用語辞書 e-Worlds」https://e-words.jp/w/IP.html

IP

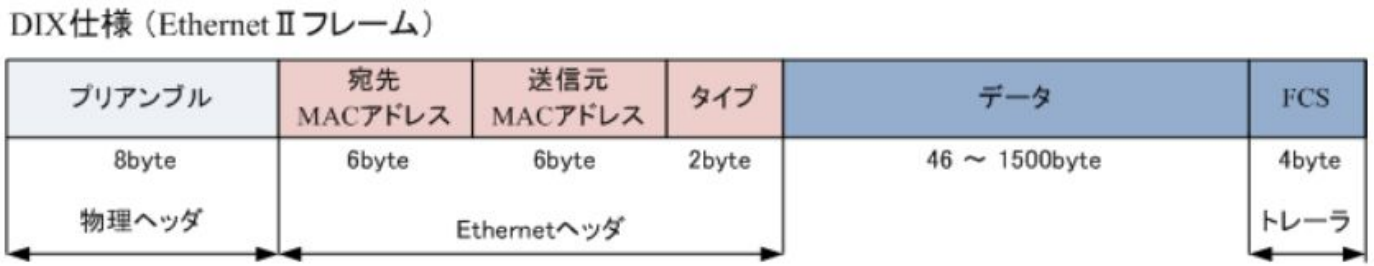
役割

- IPアドレスに基づいて宛先まで届ける
- パケットの分割と再構築

IP

出典：https://www.infraexpert.com/study/tcpip1.html

ちなみにEthernet

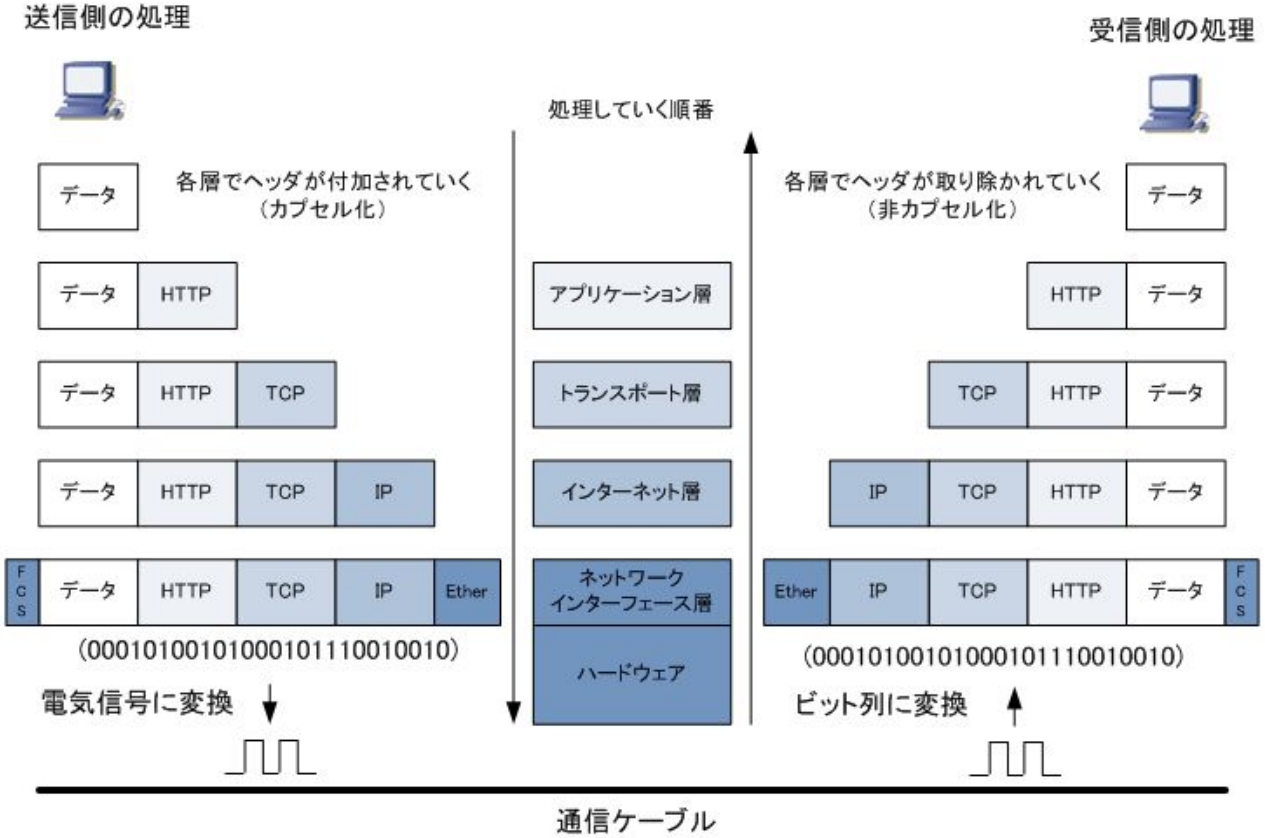


出典：https://www.infraexpert.com/study/ethernet4.html

階層ごとのプロトコル

<table>
<tr><th>OSI参照モデル</th><th>TCP/IPの階層モデル</th><th>TCP/IPプロトコル</th><th>コンピュータ上の処理</th></tr>
<tr><td>アプリケーション層</td><td rowspan="3">アプリケーション層</td><td rowspan="3">HTTP, SMTP, POP3
FTP, SSH, RIP, SNMP...</td><td rowspan="3">通信アプリケーション
プログラム</td></tr>
<tr><td>プレゼンテーション層</td></tr>
<tr><td>セッション層</td></tr>
<tr><td>トランスポート層</td><td>トランスポート層</td><td>TCP, UDP</td><td rowspan="2">OS</td></tr>
<tr><td>ネットワーク層</td><td>インターネット層</td><td>IP, ARP, ICMP, OSPF...</td></tr>
<tr><td>データリンク層</td><td rowspan="2">ネットワーク
インターフェース層</td><td rowspan="2">Ethernet, PPP...</td><td rowspan="2">デバイスドライバ
NIC</td></tr>
<tr><td>物理層</td></tr>
</table>

出典：https://www.infraexpert.com/study/tcpip.html



出典：https://www.infraexpert.com/study/tcpip.html

パケット解析

CTFのネットワーク問題を解いてもらいます.

pcapファイル

- https://onedrive.live.com/redir?resid=5EC2715BAF0C5F2B!10056&authkey=!ANE0wqC_trouhy0&ithint=folder%2czip

参考サイト

- https://www.slideshare.net/ctf4b/ctf-for-60147258

Wiresharkの機能

・検索機能

・追跡機能（TCPストリーム、HTTPストリーム）

HTTPリクエストには，**GET**、**POST**がある．

POSTには，機密性のある文章を送るときに使う．（パスワードとか…）

キーワード：http，tcp，udp，arp，icmp，ftp，ftp-data，

flag，C: DATA, hint, png

decode(←これが出たら周りに聞いて)

参考サイト

階層の話

・https://www.infraexpert.com/study/tcpip.html

TCP・UDPのお話

・https://www.infraexpert.com/study/tcpip8.html

・https://www.infraexpert.com/study/tcpip12.html

IPのお話

・https://www.infraexpert.com/study/tcpip1.html

VALN

参考サイト

・https://www.infraexpert.com/study/vlanz1.html

・https://www.infraexpert.com/study/vlanz2.html