

# R6. 07. 17

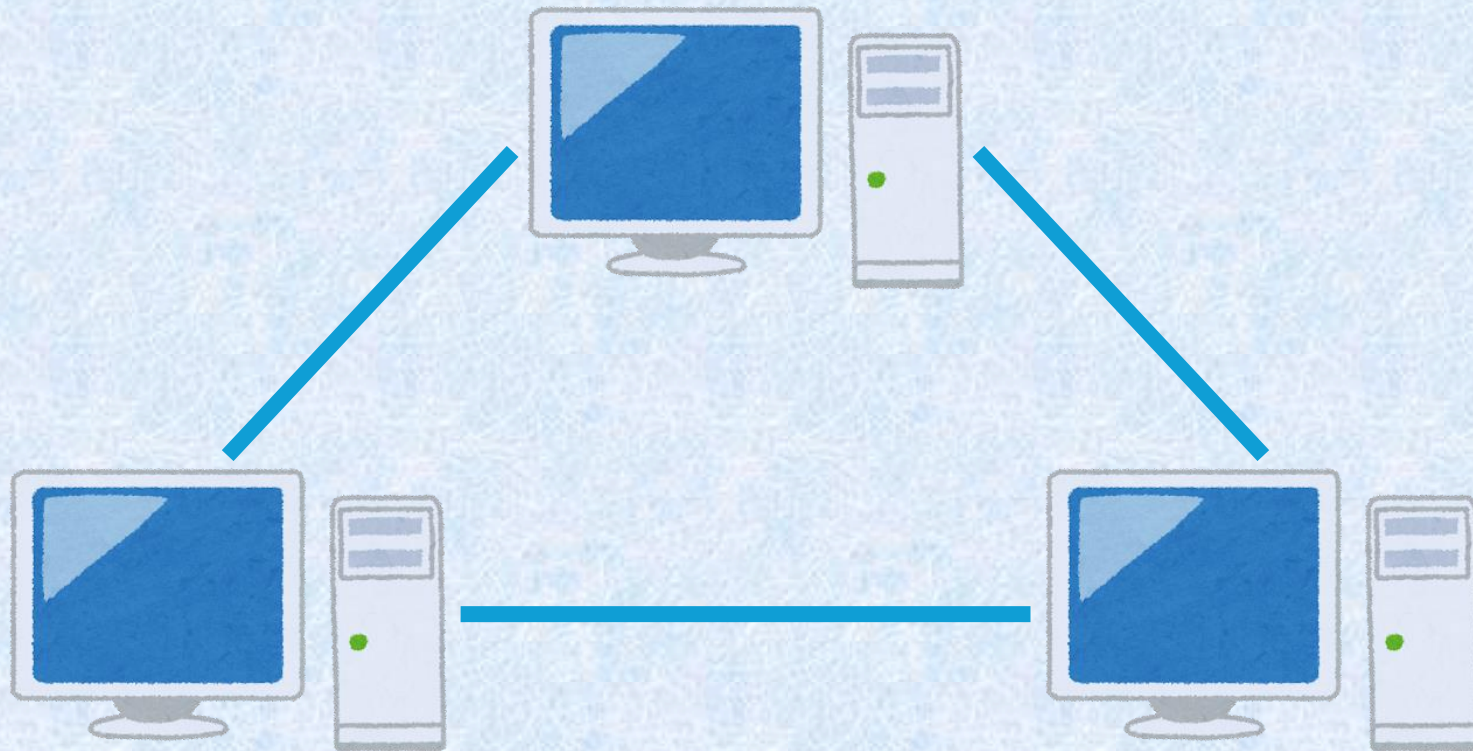
## Network ②

大城 優賀

先週の復習

# ネットワークとは

複数のコンピュータを互いに接続して使うこと

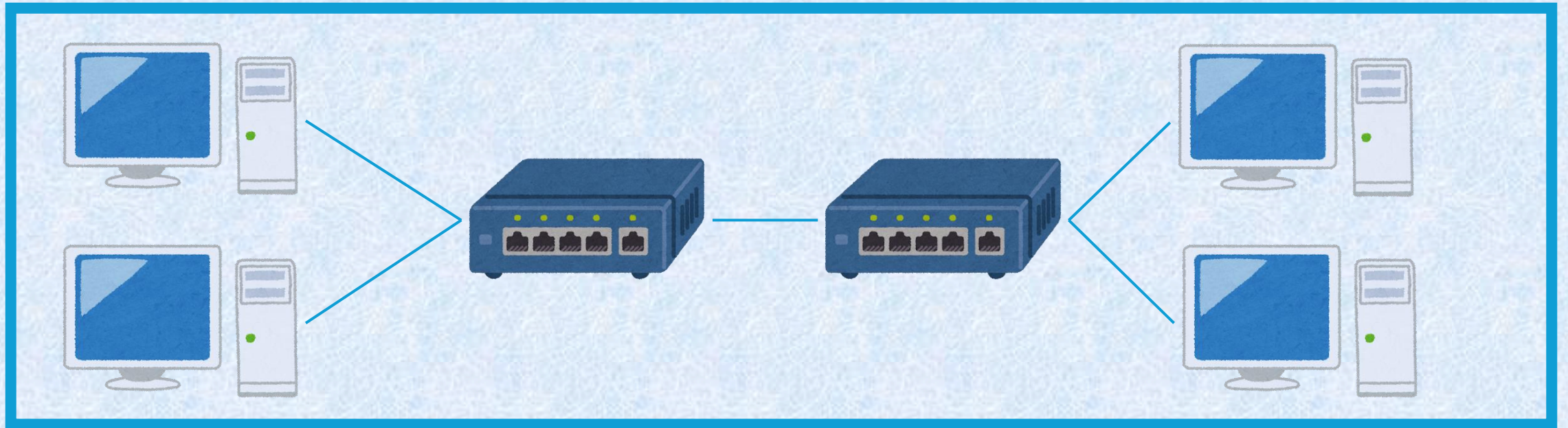


# ネットワークの分類

LAN(ラン) と WAN(ワン)

# ネットワークの分類

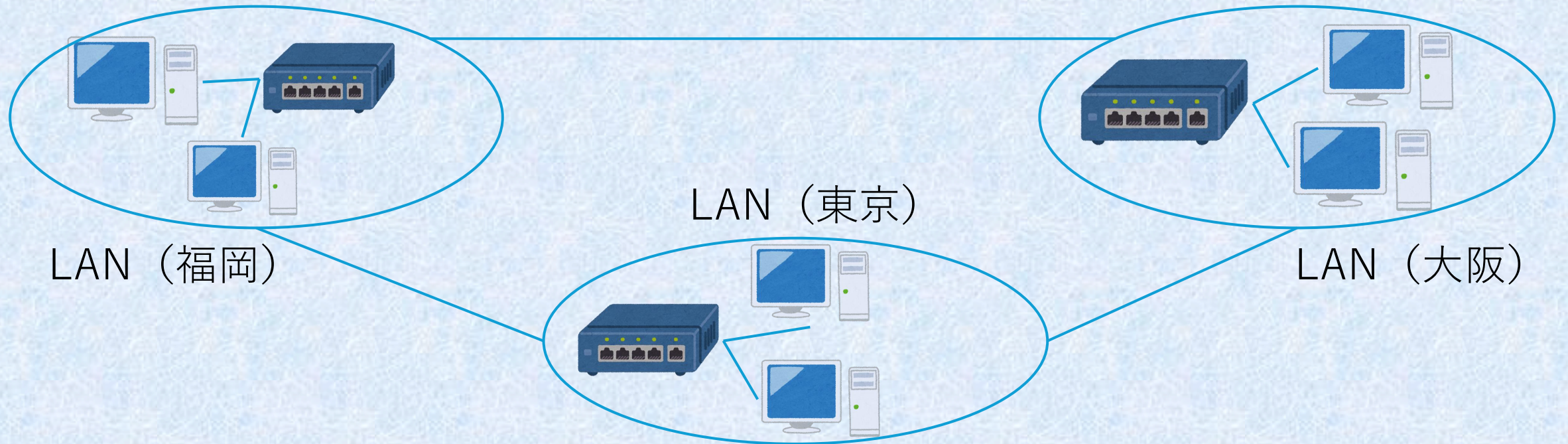
LAN：1つの建物内や学内等の限られた狭い地域のネットワークのこと





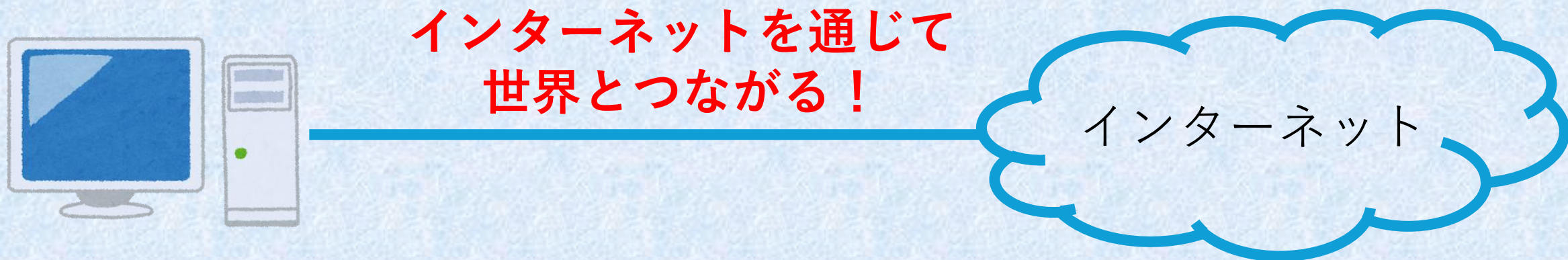
# ネットワークの分類

WAN：離れた地域のコンピュータやLAN同士を接続したネットワークのこと



# インターネットとは

WANを世界規模で実現しているのが、インターネットである（世界規模のネットワーク）



# 通信の仕組み

コンピュータ同士が通信できているわけには

「**プロトコル**」と呼ばれる「約束事」を決めているからである



# 通信の仕組み

同じ「**プロトコル**」を用いることで、メーカーやOSが異なるコンピュータ同士でも通信ができる！

コンピュータ同士の通信は  
複数のプロトコルを  
用いて通信をしている

# OSI参照モデルとは

国際標準化機構（ISO）によって、策定された  
コンピュータネットワークに求められる通信機能  
を7階層に分割、定義したものである

# OSI参照モデル

層	名称	主な役割
第7層	アプリケーション層	アプリケーションごとの規定
第6層	プレゼンテーション層	データフォーマットの交換
第5層	セッション層	通信の管理
第4層	トランスポート層	データ転送の管理
第3層	ネットワーク層	アドレスの管理と経路選択
第2層	データリンク層	データフレームの識別と転送
第1層	物理層	物理的な接続の規定



※これは「モデル」であり、プロトコルの設計や勉強する時のガイドラインである

現在、使われているプロトコル  
はTCP/IPである

# TCP/IPとは

現在のインターネット通信等で最も利用されているプロトコルである。プロトコル群の総称である中心的な役割を果たすのがTCPとIPの2つのプロトコルであるため、この名称である。

# TCP/IPとOSI参照モデルの対応付け

層	OSI参照モデル名称	TCP/IP	プロトコル
第7層	アプリケーション層	アプリケーション層	HTTP, POP SMTP TELNET, IMAP
第6層	プレゼンテーション層		
第5層	セッション層		
第4層	トランスポート層	トランスポート層	UDP, TCP
第3層	ネットワーク層	インターネット層	IP, ICMP
第2層	データリンク層	ネットワークインターフェース層	Ethernet, PPP
第1層	物理層		



# 「IP」とは

OSI参照モデルの第3層ネットワーク層の「IP」は  
パケットを送り届けるためのプロトコルである。  
パケットを目的のコンピュータまで届ける役割が  
ある

# IPアドレスとは

ネットワークに接続するコンピュータにはIPアドレスという識別子が割り当てられている。

例. 204.56.3.1

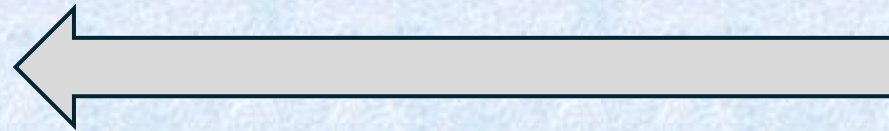
郵便物を送るとき住所のようなもの

# IPアドレスとは

IPアドレス  
「204. 56. 3. 1」



IPアドレスが  
「204. 56. 3. 1」に  
データを届けよう



# IPアドレスとは

現在多く使われているのがIPv4である

「11001011000000000111000100000000」

このような2進数32桁の数字の列



人間にとってわかりずらい  
普段使っている10進数のほうが  
分かりやすい

# IPアドレスとは

なので、IPアドレスを記述するときは

8桁ずつ4つに分け、2進数から10進数に変換

**11001011|00000000|01110001|00000000**

「203.0.113.0」のようにピリオドで区切る

IPv4アドレスが割り当てられる数  
は $2^{32}$ 、約43億である

インターネットが発達したこと  
により、IPアドレスが  
不足し始めた。



# 対策として

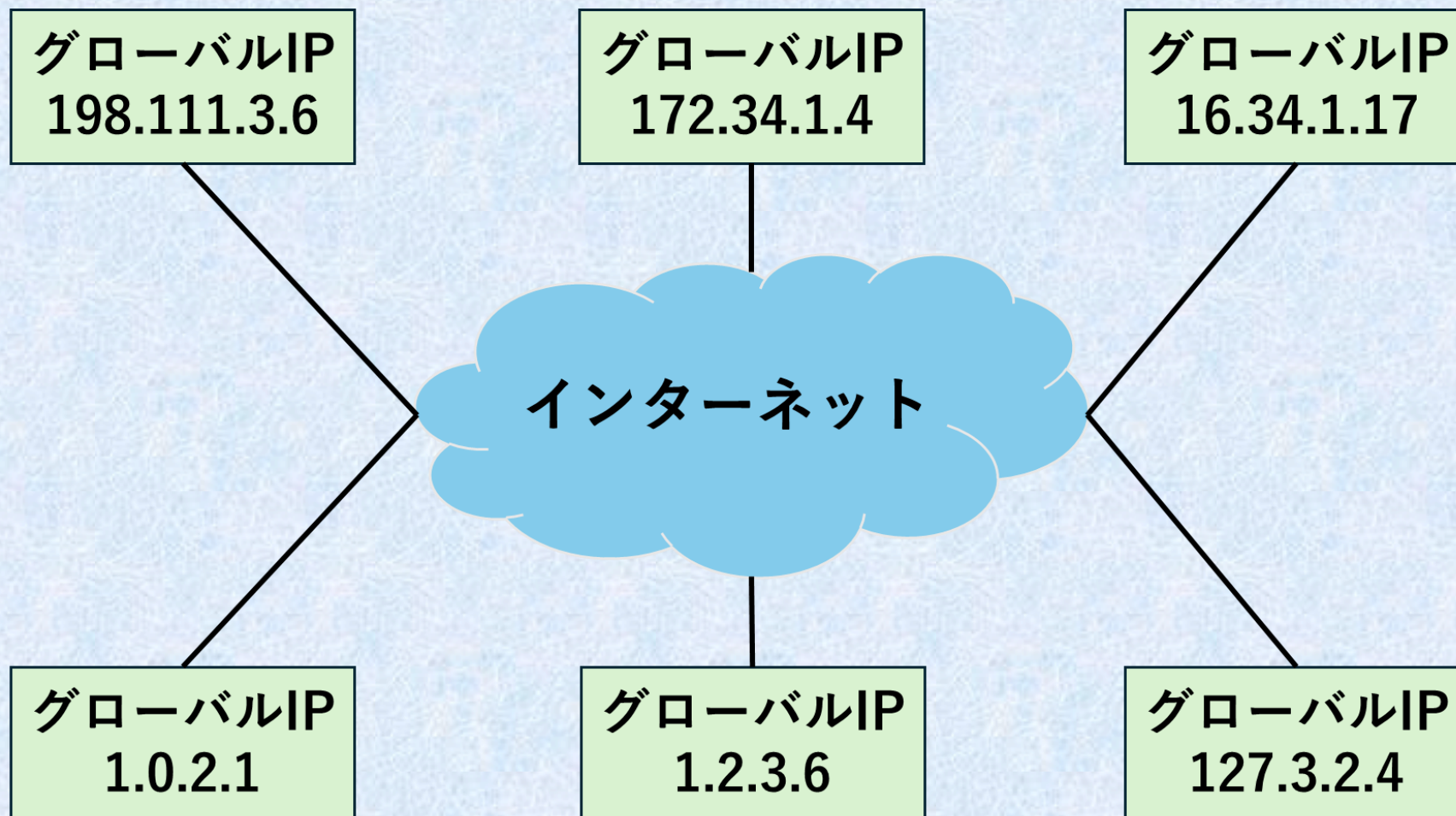
自宅や社内などの限定されたネットワーク内ではプライベートIPアドレスが各デバイスに割り振ることにした

グローバルIPアドレスと  
プライベートIPアドレス  
とは？

# IPアドレスの種類

グローバルIPアドレス：インターネットに接続するとき際に割り当てられるIPアドレス  
世界でユニーク（唯一）である

# グローバルIPアドレス



IPアドレスの  
重複がない！

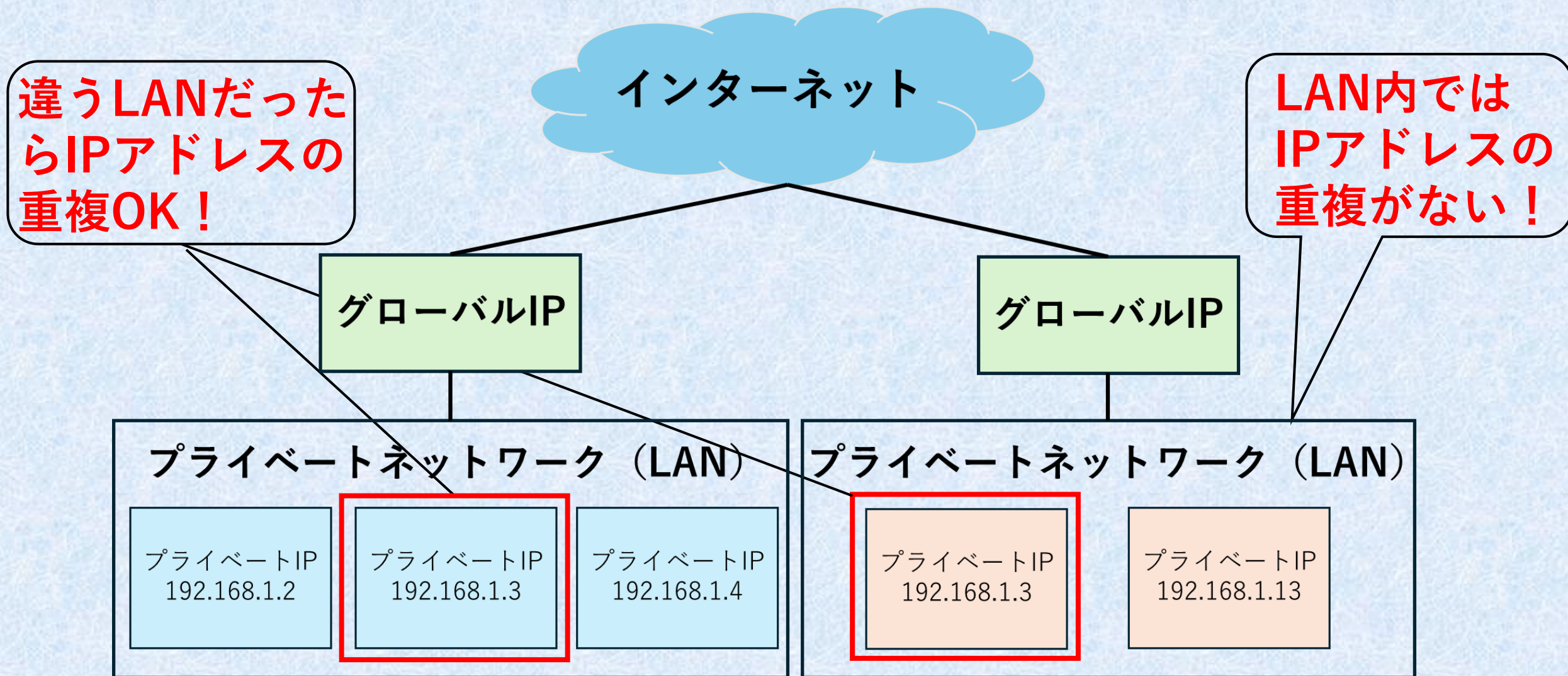
# IPアドレスの種類

プライベートIPアドレス：特定のネットワーク内で割り当てられるIPアドレスのこと。

そのネットワーク内でユニーク（唯一）である



# プライベートIPアドレス



サブネットマスクとは？

# サブネットマスクとは？

ネットワークの範囲を定義するためのもの  
1つの大きなネットワークを小さなネットワーク  
に分割する

# サブネットマスクとは？

IPアドレスはネットワーク部とホスト部に分けることができる

サブネットマスクとはネットワーク部とホスト部を示している

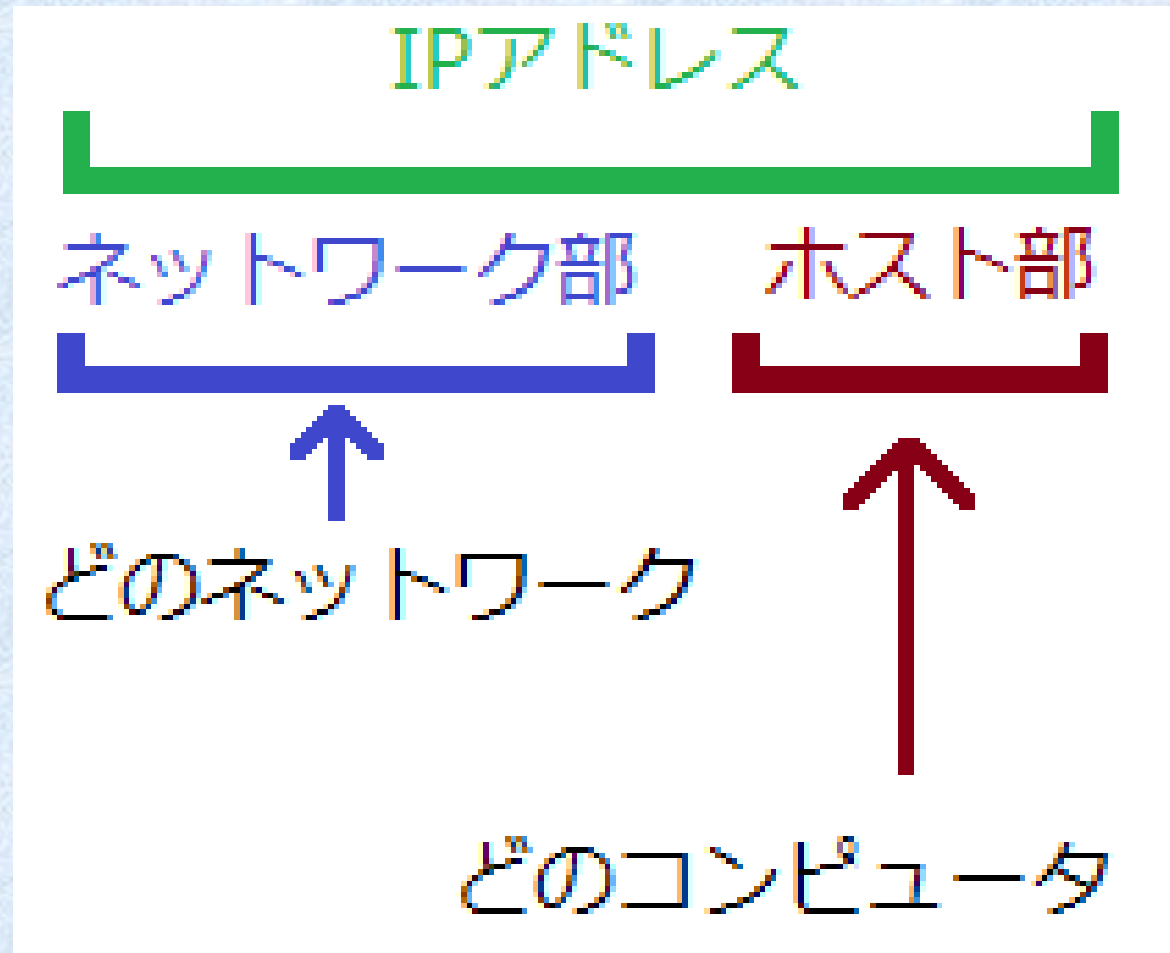
# サブネットマスクとは？

ネットワーク部：「どのネットワークですよ」  
という情報を示している

ホスト部：「どのコンピュータですよ」という  
情報を示している



# サブネットマスクとは？



先週の復習はここまで

今日やること  
wiresharkを使って  
通信を可視化してみよう

Wiresharkとは

# Wiresharkとは

ネットワークを流れるデータをキャプチャしたり  
それを解析したりできるツール

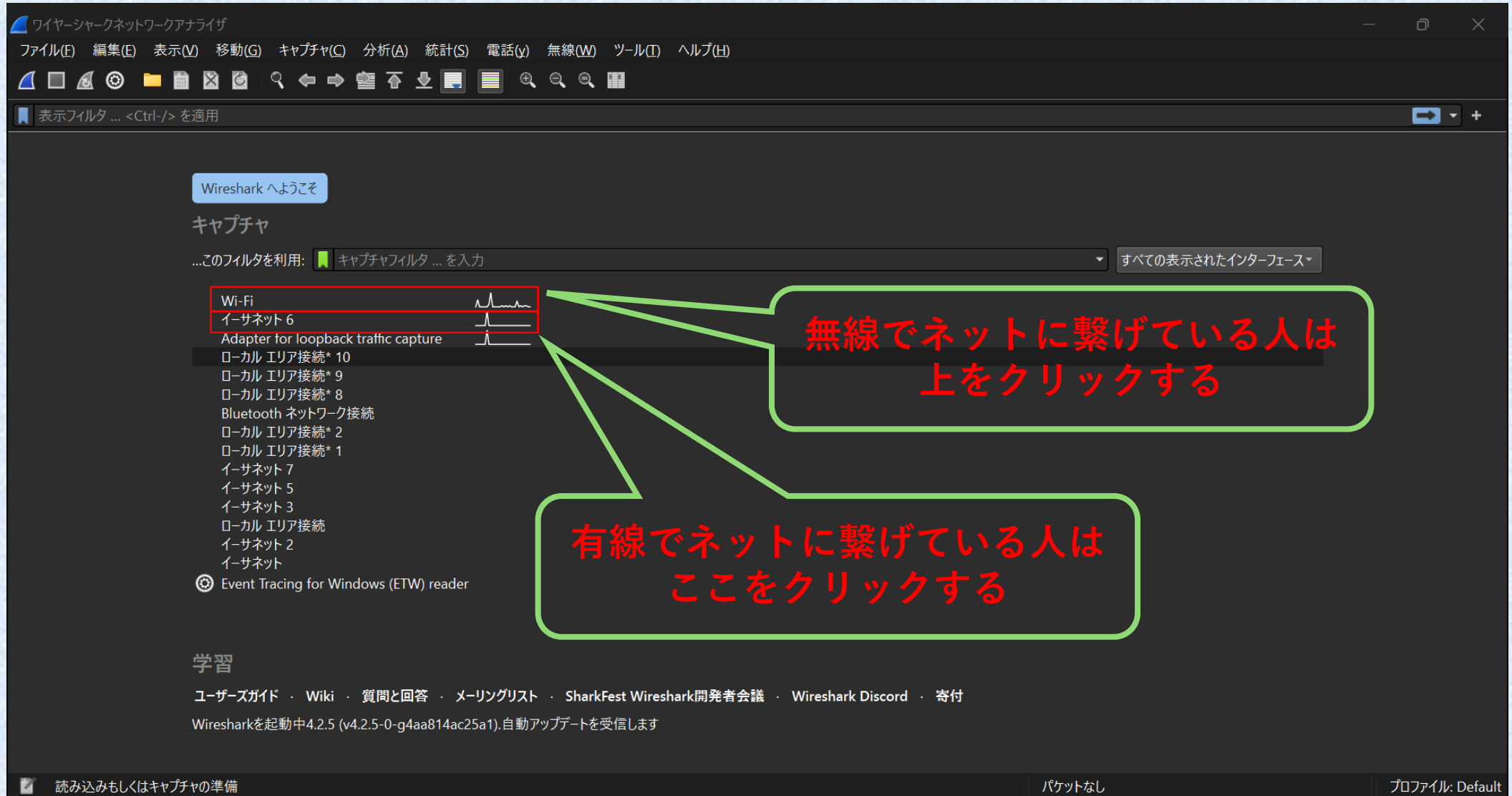


通信は目に見えない

Wiresharkを使用することで  
通信状況を可視化する  
ことができる

使ってみよう！

# Wireshark起動画面



# Wireshark動作確認

The image shows the Wireshark network traffic capture interface. The main pane displays a list of captured packets. Packet 7 is highlighted in red, indicating a Reset (RST) packet. The packet details pane shows the structure of the captured frame, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.30.117	20.194.180.207	TCP	55	57748 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassemb
2	0.022112	20.194.180.207	172.16.30.117	TCP	66	443 → 57748 [ACK] Seq=1 Ack=2 Win=251 Len=0 SLE=1 SRE=2
3	0.031210	172.16.30.117	142.251.8.188	TCP	55	58458 → 5228 [ACK] Seq=1 Ack=1 Win=256 Len=1
4	0.076426	142.251.8.188	172.16.30.117	TCP	66	5228 → 58458 [ACK] Seq=1 Ack=2 Win=290 Len=0 SLE=1 SRE=2
5	0.158539	Century_94:f6:fc	Broadcast	ARP	60	Who has 172.16.30.143? Tell 172.16.0.1
6	0.195365	172.16.30.117	172.16.0.1	TCP	66	60344 → 8013 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7	0.198330	172.16.0.1	172.16.30.117	TCP	60	8013 → 60344 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
8	0.357528	172.16.30.117	54.150.70.46	TLSv1.2	110	Application Data
9	0.358824	172.16.30.117	54.150.70.46	TLSv1.2	110	Application Data
10	0.360621	172.16.30.117	54.150.70.46	TLSv1.2	110	Application Data
11	0.362631	172.16.30.117	54.150.70.46	TLSv1.2	110	Application Data
12	0.364081	172.16.30.117	54.150.70.46	TLSv1.2	110	Application Data
13	0.421941	54.150.70.46	172.16.30.117	TCP	60	443 → 57604 [ACK] Seq=1 Ack=57 Win=8 Len=0
14	0.427174	54.150.70.46	172.16.30.117	TCP	60	443 → 57598 [ACK] Seq=1 Ack=57 Win=8 Len=0
15	0.427266	54.150.70.46	172.16.30.117	TCP	60	443 → 57603 [ACK] Seq=1 Ack=57 Win=8 Len=0

Frame 15: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF...  
Ethernet II, Src: Century\_94:f6:fc (00:80:6d:94:f6:fc), Dst: Intel\_19:0b:36 (d4:54:8b:19:0b:36)  
Internet Protocol Version 4, Src: 54.150.70.46, Dst: 172.16.30.117  
Transmission Control Protocol, Src Port: 443, Dst Port: 57603, Seq: 1, Ack: 57, Len: 0

0000 d4 54 8b 19 0b 36 00 80 6d 94 f6 fc 08 00 45 00  
0010 00 28 1a dd 40 00 38 06 e0 a9 36 96 46 2e ac 10  
0020 1e 75 01 bb e1 03 bd de 8e 84 5a b7 c9 4d 50 10  
0030 00 08 15 5c 00 00 00 00 00 00 00 00 00 00 00

wireshark\_Wi-Fi2MANP2.pcapng      パケット数: 548 · 表示: 548 (100.0%) · 欠落: 0 (0.0%)      プロファイル: Default



スライド通りの画面が  
表示されるはず

1つ1つ流れているのが  
パケット

# パケットとは

インターネットなどTCP/IPネットワークで通信を行う際、データはIPによって分割される  
この分割されたデータのことをパケットと呼ぶ

172.16.30.117	52.111.232.50	TLSv1.2	82 Application Data
34.230.174.202	172.16.30.117	TCP	66 443 → 65524 [ACK] Seq=1 Ack=2 Win=324 Len=0
52.111.232.50	172.16.30.117	TCP	60 443 → 49943 [ACK] Seq=1 Ack=29 Win=16380 Len=0
Century_94:f6:fc	Broadcast	ARP	60 Who has 172.16.30.142? Tell 172.16.0.1
172.16.30.114	224.0.0.251	MDNS	139 Standard query 0x0000 PTR _companion-link._tcp
fe80::1001:ea5c:3cf::	ff02::fb	MDNS	159 Standard query 0x0000 PTR _companion-link._tcp
Century_94:f6:fc	Broadcast	ARP	60 Who has 172.16.30.142? Tell 172.16.0.1
172.16.30.117	142.250.199.106	TCP	55 50293 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1
142.250.199.106	172.16.30.117	TCP	66 443 → 50293 [ACK] Seq=1 Ack=2 Win=272 Len=0
172.16.30.117	172.217.175.67	TCP	55 50307 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1
Century_94:f6:fc	Broadcast	ARP	60 Who has 172.16.30.142? Tell 172.16.0.1
172.217.175.67	172.16.30.117	TCP	66 443 → 50307 [ACK] Seq=1 Ack=2 Win=290 Len=0
Century_94:f6:fc	Broadcast	ARP	60 Who has 172.16.30.142? Tell 172.16.0.1
Century_94:f6:fc	Broadcast	ARP	60 Who has 172.16.30.142? Tell 172.16.0.1
172.16.30.117	54.95.144.31	TLSv1.2	110 Application Data

1つ1つがパケット！



Destination	Protocol	Length	Info
54.95.144.31	TCP	54	63369 → 443 [ACK] Seq=1 Ack=1 Win=258 Len=0
54.95.144.31	TCP	54	63349 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=0
142.251.170.188	TCP	55	63320 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [T
172.16.30.117	TCP	66	443 → 63320 [ACK] Seq=1 Ack=2 Win=265 Len=0 SL
34.230.174.202	TCP	55	65524 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [T
ff02::16	ICMPv6	90	Multicast Listener Report Message v2
224.0.0.2	IGMPv2	46	Leave Group 224.0.0.251
224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
224.0.0.251	MDNS	139	Standard query 0x0000 PTR _companion-link._tcp
ff02::fb	MDNS	159	Standard query 0x0000 PTR _companion-link._tcp
52.111.232.50	TLSv1.2	82	Application Data
Broadcast	ARP	60	Who has 172.16.31.50? Tell 172.16.0.1
Broadcast	ARP	60	Who has 172.16.30.142? Tell 172.16.0.1
172.16.30.117	TCP	60	443 → 49936 [ACK] Seq=1 Ack=29 Win=16385 Len=0
52.111.232.50	TLSv1.2	82	Application Data
172.16.30.117	TCP	66	443 → 65524 [ACK] Seq=1 Ack=2 Win=324 Len=0 SL
172.16.30.117	TCP	60	443 → 49943 [ACK] Seq=1 Ack=29 Win=16380 Len=0
Broadcast	ARP	60	Who has 172.16.30.142? Tell 172.16.0.1
224.0.0.251	MDNS	139	Standard query 0x0000 PTR _companion-link._tcp
ff02::fb	MDNS	159	Standard query 0x0000 PTR _companion-link._tcp
Broadcast	ARP	60	Who has 172.16.30.142? Tell 172.16.0.1
142.250.199.106	TCP	55	50292 → 443 [ACK] Seq=1 Ack=1 Win=259 Len=1 [T

Length がパケットサイズ



パケットには最大サイズがあり  
一般的には1500bytesと  
なっている

現在、使われているプロトコルは  
TCP/IPである

# TCP/IPとは

現在のインターネット通信等で最も利用されているプロトコルである。プロトコル群の総称である

※プロトコルは「決まり事、約束事」のこと

# 通信の仕組み

同じ「**プロトコル**」を用いることで、メーカーやOSが異なるコンピュータ同士でも通信ができる！

コンピュータ同士の通信は  
複数のプロトコルを  
用いて通信をしている



# TCP/IPの構造

アプリケーション層

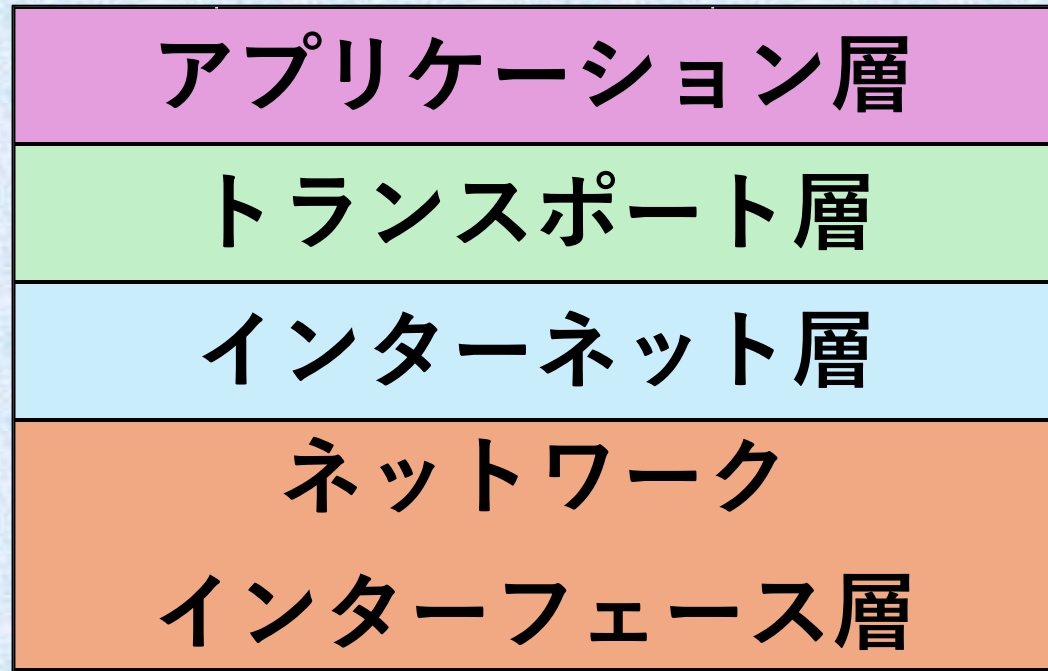
トランスポート層

インターネット層

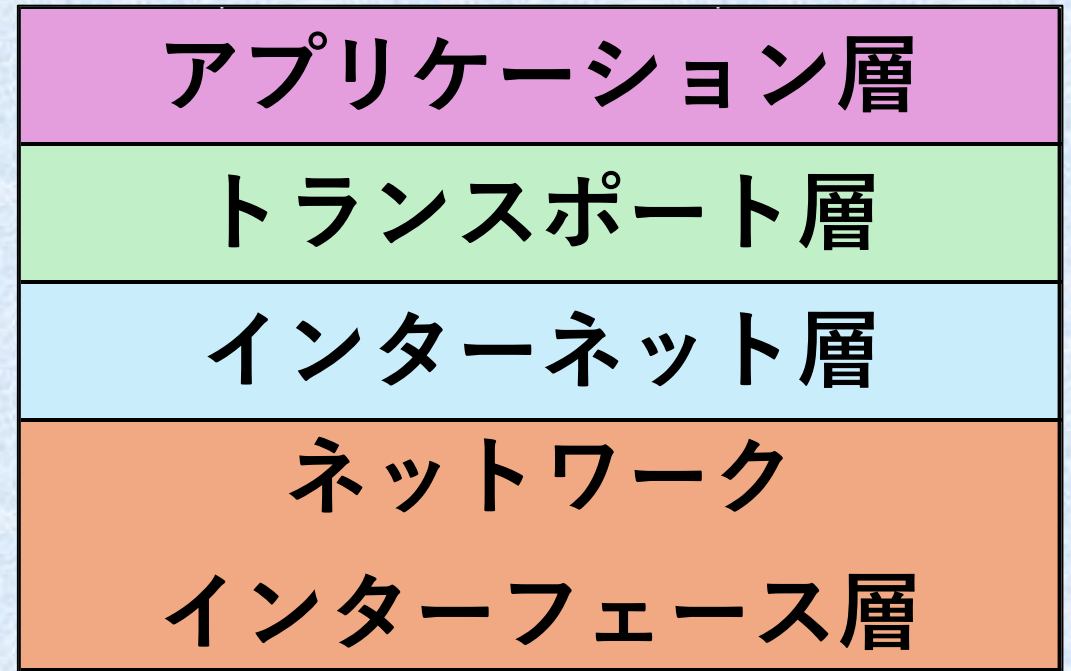
ネットワークインターフェース層

# データ送受信の流れ

送信側



受信側



httpパケットの層を  
見てみよう

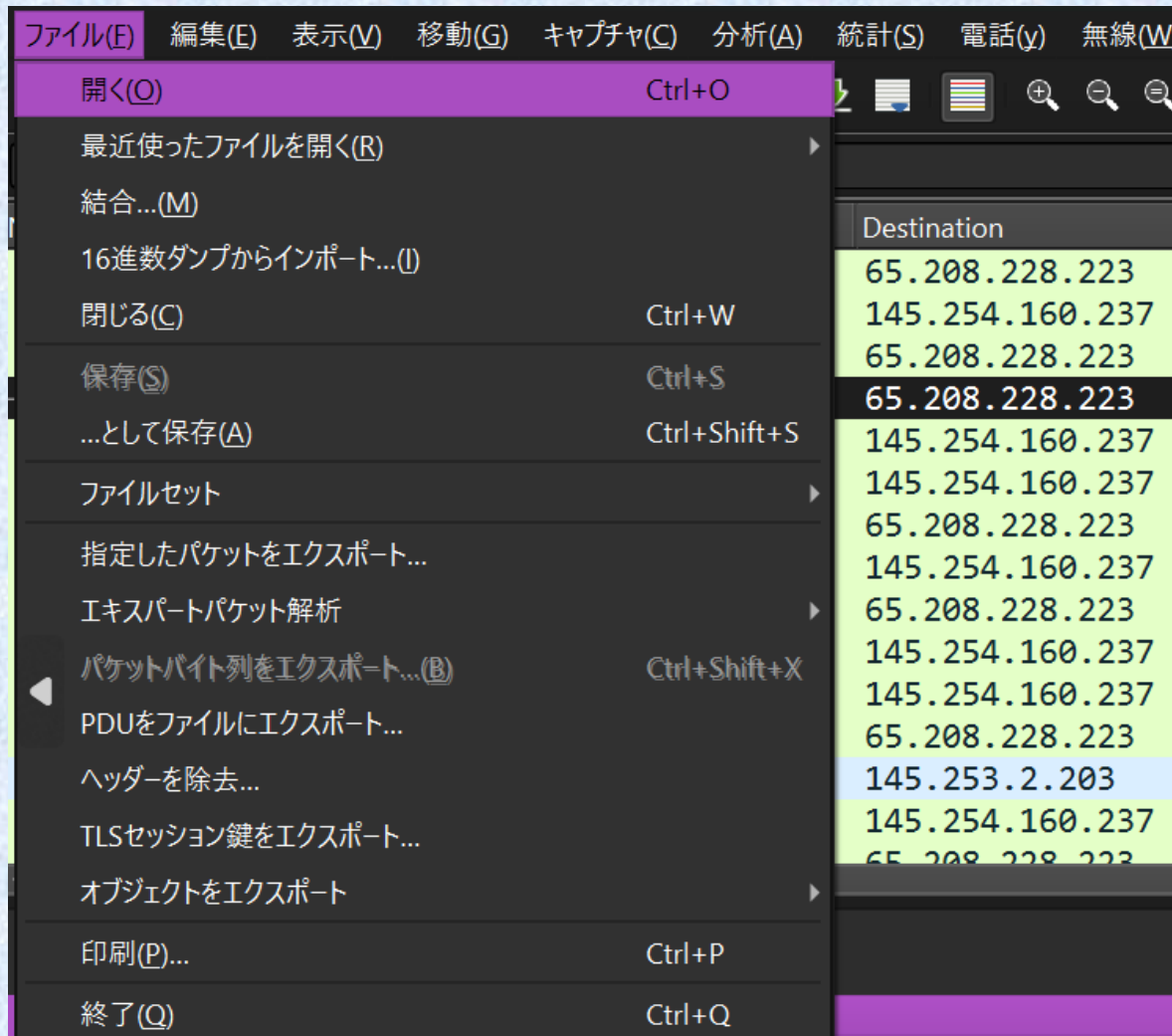
# httpパケットの層を確認する

以下のurlをクリック、ダウンロードする

<https://wiki.wireshark.org/uploads/27707187aeb30df68e70c8fb9d614981/http.cap>

http.cap をダウンロード

# httpパケットの層を確認する



右上の「ファイル」  
から「開く」をクリック  
ダウンロードした  
http.capを選択する



# httpパケットの層を確認する

The image shows a Wireshark packet capture of an HTTP transaction. The packet list pane at the top shows several packets. Packet 4, at time 0.911310, is an HTTP GET request from 145.254.160.237 to 65.208.228.223. This packet is highlighted with a red box. The packet details pane below shows the structure of the selected packet, including the TCP segment and the HTTP GET request. The packet bytes pane on the right shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	145.254.160.237	65.208.228.223	TCP	62	3372 → 80 [SYN] Seq=0 Win=8760 Len=0 MSS=1460 SACK_PERM
2	0.911310	65.208.228.223	145.254.160.237	TCP	62	80 → 3372 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380 SACK_PERM
3	0.911310	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=1 Ack=1 Win=5840 Len=0
4	0.911310	145.254.160.237	65.208.228.223	HTTP	533	GET /download.html HTTP/1.1
5	1.472110	65.208.228.223	145.254.160.237	TCP	54	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=0
6	1.682419	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1 Ack=480 Win=6432 Len=1380 [TCP segment of a reas
7	1.812606	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=1381 Win=9660 Len=0
8	1.812606	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=1381 Ack=480 Win=6432 Len=1380 [TCP segment of a r
9	2.012894	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=2761 Win=9660 Len=0
10	2.443513	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=2761 Ack=480 Win=6432 Len=1380 [TCP segment of a r
11	2.553672	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [PSH, ACK] Seq=4141 Ack=480 Win=6432 Len=1380 [TCP segment o
12	2.553672	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=5521 Win=9660 Len=0
13	2.553672	145.254.160.237	145.253.2.203	DNS	89	Standard query 0x0023 A pagead2.google syndication.com
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK] Seq=5521 Ack=480 Win=6432 Len=1380 [TCP segment of a r
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK] Seq=480 Ack=6901 Win=9660 Len=0

Flags: 0x018 (PSH, ACK)  
Window: 9660  
[Calculated window size: 9660]  
[Window size scaling factor: -2 (no window scaling used)]  
Checksum: 0xa958 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
TCP payload (479 bytes)  
Hypertext Transfer Protocol  
GET /download.html HTTP/1.1\r\n  
Host: www.ethereal.com\r\n

0020 e4 df 0d 2c 00 50 38 af fe 14 11 4c 61 8c 50 18  
0030 25 bc a9 58 00 00 47 45 54 20 2f 64 6f 77 6e 6c  
0040 6f 61 64 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e  
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 74 68  
0060 65 72 65 61 6c 2e 63 6f 6d 0d 0a 55 73 65 72 2d  
0070 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35  
0080 2e 30 20 28 57 69 6e 64 6f 77 73 3b 20 55 3b 20  
0090 57 69 6e 64 6f 77 73 20 4e 54 20 35 2e 31 3b 20  
00a0 65 6e 2d 55 53 3b 20 72 76 3a 31 2e 36 29 20 47  
00b0 65 63 6b 6f 2f 32 30 30 34 30 31 31 33 0d 0a 41  
00c0 63 63 65 70 74 3a 20 74 65 78 74 2f 78 6d 6c 2c  
00d0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 2c  
00e0 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78 68 74 6d

Text item (text)      パケット数: 43 · 表示: 43 (100.0%)      プロファイル: Default

# httpパケットの層を確認する

12	2.553672	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK]
13	2.553672	145.254.160.237	145.253.2.203	DNS	89	Standard query
14	2.633787	65.208.228.223	145.254.160.237	TCP	1434	80 → 3372 [ACK]
15	2.814046	145.254.160.237	65.208.228.223	TCP	54	3372 → 80 [ACK]

▶	Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
▶	Ethernet II, Src: Xerox_00:00:00 (00:00:01:00:00:00), Dst: fe:ff:20:00:01:00 (fe:ff:20:00:01:00)
▶	Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
▶	Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
▶	Hypertext Transfer Protocol

# 各層の役割

```
▶ Frame 4: 533 bytes on wire (4264 bits), 9216 capture length (7374 bytes captured on interface 0)
▶ Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00), Dst: Intel_00:00:00:00:00:00
▶ Internet Protocol Version 4, Src: 145.254.254.254, Dst: 145.254.254.254
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 80
▶ Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

# アプリケーション層

役割：アプリケーションごとの固有の規定

## 主なプロトコル

HTTP・・・HTML文章や画像、音声、動画などの送受信に用いられる

HTTPS・・・TLS/SSLを使ってHTTPの通信を暗号化したもの

FTP・・・異なるコンピュータ間でファイルを転送する時に用いられる

SSH・・・暗号化された遠隔ログインシステム



# 各層の役割

```
▶ Frame 4: 533 bytes on wire (4264 bits), 9  
▶ Ethernet II, Src: Xerox_00:00:00 (00:00:00:00:00:00)  
▶ Internet Protocol Version 4, Src: 145.254.254.254  
▶ Transmission Control Protocol, Src Port: 80  
▶ Hypertext Transfer Protocol
```

ネットワークインターフェース層  
インターネット層

トランスポート層

アプリケーション層



# トランスポート層

役割：ノード間のデータ転送の信頼性を確保

## 主なプロトコル

TCP・・・コネクション型で、信頼性のあるプロトコル

スピード遅い

UDP・・・コネクションレス型で、信頼性のないプロトコル

スピード速い

# 各層の役割

```
▶ Frame 4: 533 bytes on wire (4264 bits), 9216 captured (21.7% capture rate)
▶ Ethernet II, Src: Xerox 00:00:00 (00:00:00:00:00:00), Dst: Intel 00:00:00:00:00:00
▶ Internet Protocol Version 4, Src: 145.254.254.254, Dst: 145.254.254.254
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 80
▶ Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

# インターネット層

役割：ネットワーク間のエンドツーエンドの通信

## 主なプロトコル

IPv4・・・ネットワークデバイスを識別するためのプロトコル

32ビットのアドレス空間をもつ

IPv6・・・ネットワークデバイスを識別するためのプロトコル

128ビットのアドレス空間をもつ

ARP・・・IPアドレスからMACアドレスを調べる

# 各層の役割

```
▶ Frame 4: 533 bytes on wire (4264 bits), 9  
▶ Ethernet II, Src: Xerox 00:00:00 (00:00:00:00:00:00)  
▶ Internet Protocol Version 4, Src: 145.254.254.254  
▶ Transmission Control Protocol, Src Port: 80  
▶ Hypertext Transfer Protocol
```

ネットワークインターフェース層

インターネット層

トランスポート層

アプリケーション層

# ネットワークインターフェース層

役割：物理的に接続されたノード間の通信

## 主なプロトコル

Ethernet(有線LAN)

IEEE802.11(無線LAN)

PPP・・・コンピュータ同士の1対1の通信を行うプロトコル



http パケット層の確認が  
できた

ちょっとした

セキュリティについて触れる

※ここからやることは絶対に  
公衆回線で使用しないこと

公衆回線で使用了た場合  
法律に触れることになる

Wiresharkはネットワークに  
流れるデータをキャプチャ  
解析できるツール



つまり、同じネットワークを利用する他人のデータを  
みることができる

それを踏まえて絶対に公衆回線で  
使用しないようにして  
下さい

实践！

Wiresharkを使って自分が見ている  
ウェブページを確認しよう

# ウェブページ確認

以下のurl をクリックする

<http://www.chiseki.go.jp/>



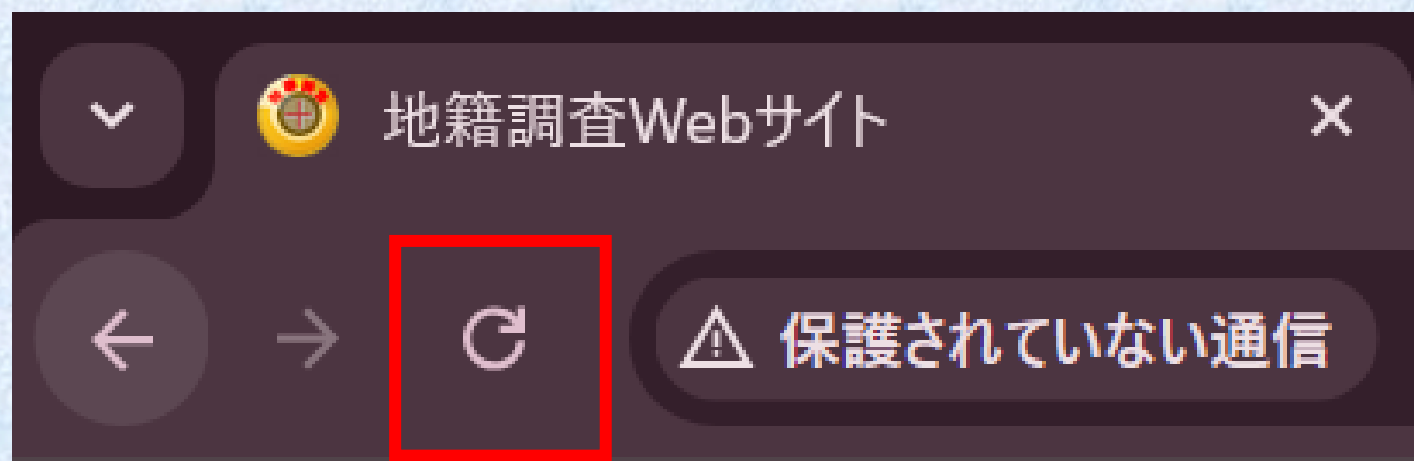
# ウェブページ確認



# ウェブページ確認

Wireshark を閉じてもう一度  
パケットが確認できる状態にする  
すぐにウェブページに戻る

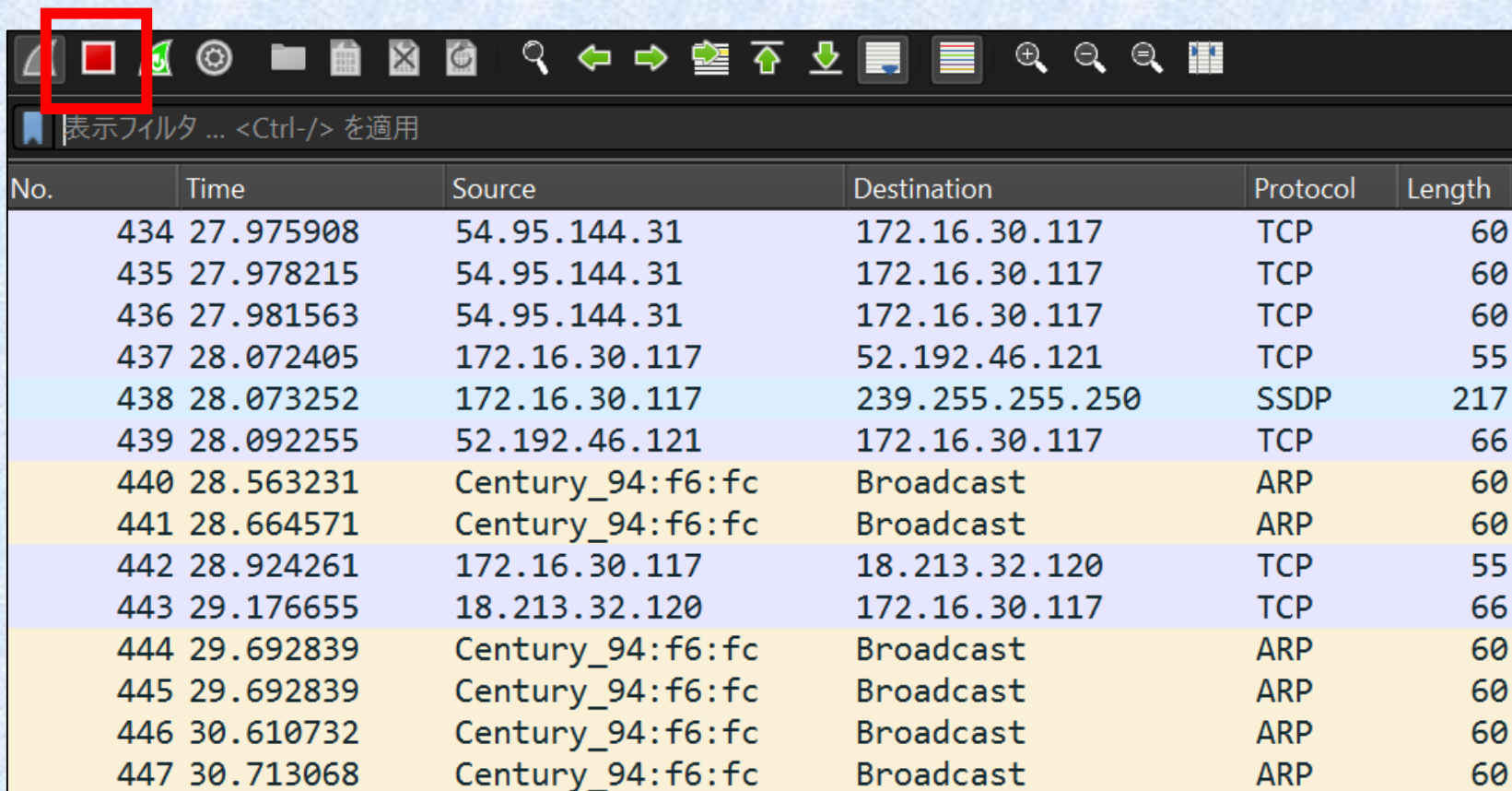
# ウェブページ確認



先ほどウェブページの左上を  
1クリックする（再読み込み）



# ウェブページ確認




No.	Time	Source	Destination	Protocol	Length
434	27.975908	54.95.144.31	172.16.30.117	TCP	60
435	27.978215	54.95.144.31	172.16.30.117	TCP	60
436	27.981563	54.95.144.31	172.16.30.117	TCP	60
437	28.072405	172.16.30.117	52.192.46.121	TCP	55
438	28.073252	172.16.30.117	239.255.255.250	SSDP	217
439	28.092255	52.192.46.121	172.16.30.117	TCP	66
440	28.563231	Century_94:f6:fc	Broadcast	ARP	60
441	28.664571	Century_94:f6:fc	Broadcast	ARP	60
442	28.924261	172.16.30.117	18.213.32.120	TCP	55
443	29.176655	18.213.32.120	172.16.30.117	TCP	66
444	29.692839	Century_94:f6:fc	Broadcast	ARP	60
445	29.692839	Century_94:f6:fc	Broadcast	ARP	60
446	30.610732	Century_94:f6:fc	Broadcast	ARP	60
447	30.713068	Century_94:f6:fc	Broadcast	ARP	60

Wireshark の画面に戻る  
そして、左上の停止ボ  
タンをクリック

ここまでやってみよう



# ウェブページ確認

					
No.	Time	Source	Destination	Protocol	Len
622	42.931555	52.111.232.55	172.16.30.117	TCP	
623	42.933156	52.111.232.55	172.16.30.117	TCP	
624	42.951196	52.111.232.55	172.16.30.117	TCP	
625	43.207524	Century_94:f6:fc	Broadcast	ARP	
626	43.211525	52.111.232.55	172.16.30.117	TLSv1.2	1
627	43.256014	172.16.30.117	52.111.232.55	TCP	
628	43.263473	172.16.30.117	52.111.232.55	TLSv1.2	1
629	43.288568	52.111.232.55	172.16.30.117	TLSv1.2	
630	43.334725	172.16.30.117	52.111.232.55	TCP	
631	43.431188	172.16.30.117	52.111.232.50	TLSv1.2	
632	43.453714	52.111.232.50	172.16.30.117	TLSv1.2	

フィルタのところに「http」を入力、Enterキーを押す

# ウェブページ確認

\*Wi-Fi

ファイル(F) 編集(E) 表示(V) 移動(G) キャプチャ(C) 分析(A) 統計(S) 電話(y) 無線(W) ツール(T) ヘルプ(H)

http

No.	Time	Source	Destination	Protocol	Length	Info
43	3.228227	172.16.30.117	203.180.136.104	HTTP	647	GET / HTTP/1.1
51	3.255200	203.180.136.104	172.16.30.117	HTTP	757	HTTP/1.1 200 OK (text/html)
53	3.364086	172.16.30.117	142.250.196.142	HTTP	409	GET /cse.js?cx=001531663788242660047:vg1csqr_tno HTTP/1.1
57	3.447595	142.250.196.142	172.16.30.117	HTTP	1224	HTTP/1.1 200 OK (text/javascript)

Frame 43: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Device\NPF{...} Ethernet II, Src: Intel\_19:0b:36 (d4:54:8b:19:0b:36), Dst: Century\_94:f6:fc (00:80:6d:94:f6:fc) Internet Protocol Version 4, Src: 172.16.30.117, Dst: 203.180.136.104 Transmission Control Protocol, Src Port: 51862, Dst Port: 80, Seq: 1, Ack: 1, Len: 593 Hypertext Transfer Protocol

0000 00 80 6d 94 f6 fc d4 54 8b 19 0b 36 08 00 45 00 ..  
0010 02 79 e1 f0 40 00 80 06 f7 eb ac 10 1e 75 cb b4 .y  
0020 88 68 ca 96 00 50 0c 96 93 69 c4 e3 ff 77 50 18 .h  
0030 fa f0 9f 8c 00 00 47 45 54 20 2f 20 48 54 54 50 ..  
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /1  
0050 63 68 69 73 65 6b 69 2e 67 6f 2e 6a 70 0d 0a 43 ch  
0060 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d on  
0070 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 6f 6e al  
0080 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d 30 0d tr  
0090 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 .U  
00a0 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 e-  
00b0 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c se  
00c0 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la  
00d0 4e 54 20 31 30 2e 30 3h 20 57 69 6e 36 34 3h 20 NT

Hypertext Transfer Protocol: Protocol

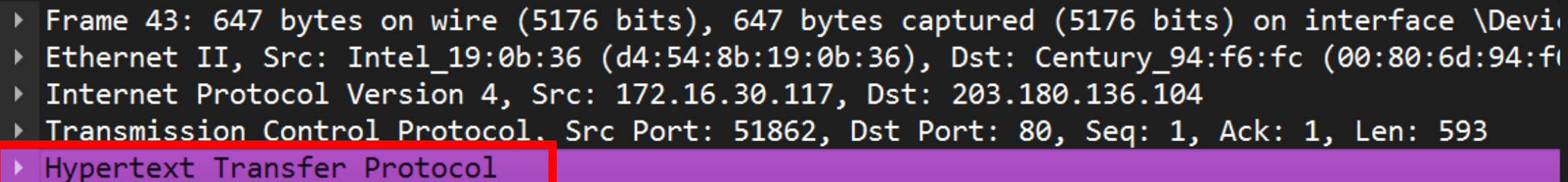
パケット数: 70 · 表示: 4 (5.7%) · 欠落: 0 (0.0%) プロファイル: Default

# ウェブページ確認

http						
	Time	Source	Destination	Protocol	Length	Info
43	3.228227	172.16.30.117	203.180.136.104	HTTP	647	GET / HTTP/1.1
51	3.255200	203.180.136.104	172.16.30.117	HTTP	757	HTTP/1.1 200 OK
53	3.364086	172.16.30.117	142.250.196.142	HTTP	409	GET /cse.js?cx=
57	3.447595	142.250.196.142	172.16.30.117	HTTP	1224	HTTP/1.1 200 OK

「Info」の欄に「GET/HTTP」と  
書かれているパッケージをクリック

# ウェブページ確認



A screenshot of the Wireshark network protocol analyzer interface. The 'Packet Details' pane on the left shows a list of protocols for Frame 43. The protocols listed are Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The 'Hypertext Transfer Protocol' entry is highlighted with a red rectangular box. The main pane on the right shows the details of the selected protocol, which is currently empty.

- ▶ Frame 43: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Device\NPF{...}
- ▶ Ethernet II, Src: Intel\_19:0b:36 (d4:54:8b:19:0b:36), Dst: Century\_94:f6:fc (00:80:6d:94:fc)
- ▶ Internet Protocol Version 4, Src: 172.16.30.117, Dst: 203.180.136.104
- ▶ Transmission Control Protocol, Src Port: 51862, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
- ▶ Hypertext Transfer Protocol

アプリケーション層の横の「▶」をクリック



# ウェブページ確認

```
▶ Frame 43: 647 bytes on wire (5176 bits), 647 bytes captured (5176 bits) on interface \Dev
▶ Ethernet II, Src: Intel_19:0b:36 (d4:54:8b:19:0b:36), Dst: Century_94:f6:fc (00:80:6d:94:
▶ Internet Protocol Version 4, Src: 172.16.30.117, Dst: 203.180.136.104
▶ Transmission Control Protocol, Src Port: 51862, Dst Port: 80, Seq: 1, Ack: 1, Len: 593
▼ Hypertext Transfer Protocol
  ▶ GET / HTTP/1.1\r\n
    Host: www.chiseki.go.jp\r\n
    Connection: keep-alive\r\n
    Cache-Control: max-age=0\r\n
    Upgrade-Insecure-Requests: 1\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
    Referer: https://www.google.com/\r\n
    Accept-Encoding: gzip, deflate\r\n
```

「Host」 が [www.chiseki.go.jp](http://www.chiseki.go.jp) だと分かる



# ウェブページ確認

```
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) App
Accept: text/html,application/xhtml+xml,application/xml;q=
Referer: https://www.google.com/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: ja,en-US;q=0.9,en;q=0.8\r\n
If-None-Match: "4cc4-61d55a5398451-gzip"\r\n
If-Modified-Since: Tue, 16 Jul 2024 04:19:01 GMT\r\n
\r\n
[Full request URI: http://www.chiseki.go.jp/]
[HTTP request 1/1]
[Response in frame: 51]
```

下にスクロールすると、URLが  
「[http://www.chiseki.go.jp](http://www.chiseki.go.jp/)」だと分かる

# ウェブページ確認



<http://www.chiseki.go.jp/>

webページとwiresharkで取得したパケット  
情報と一致している！

なぜwiresharkで  
確認できたのか？

# 確認できた理由

「地籍調査Webサイト」を見ていること  
ができた理由は「http」を  
使っているため。

ほとんどのウェブページは  
暗号化されている



ウェブページのurlを見ると、

「https」が付いている

これはSSL/TLSを用いて暗号化し

ているためである

なので、機密情報を扱う際は  
httpsが付いているサイトを使用  
しよう！

※今日やったことは絶対に  
公衆回線で使用しないこと

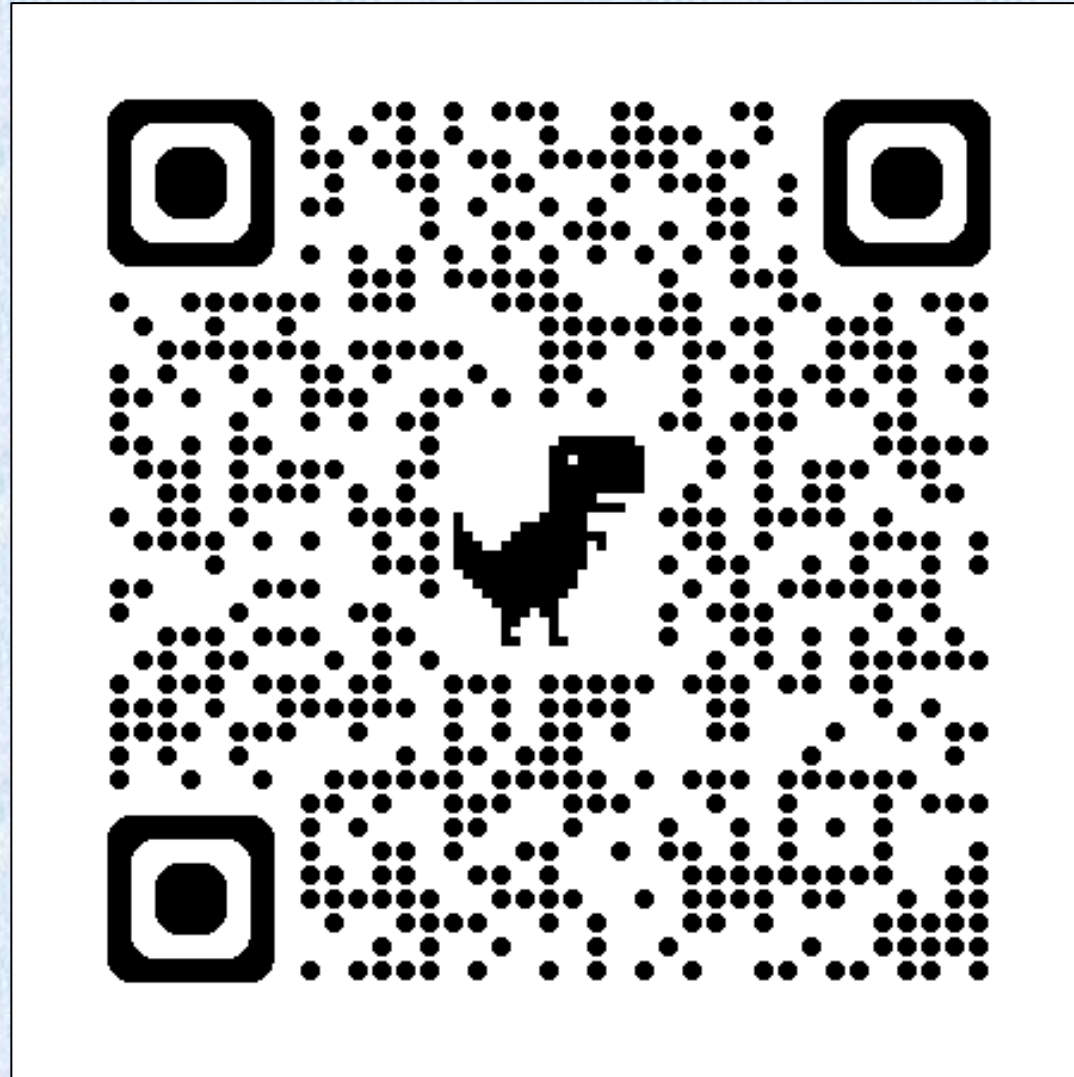
おしまい

ありがとうございました



**アンケートの回答を  
お願いします。**





<https://forms.gle/XKgZ6qdXG4nRJXoS6>