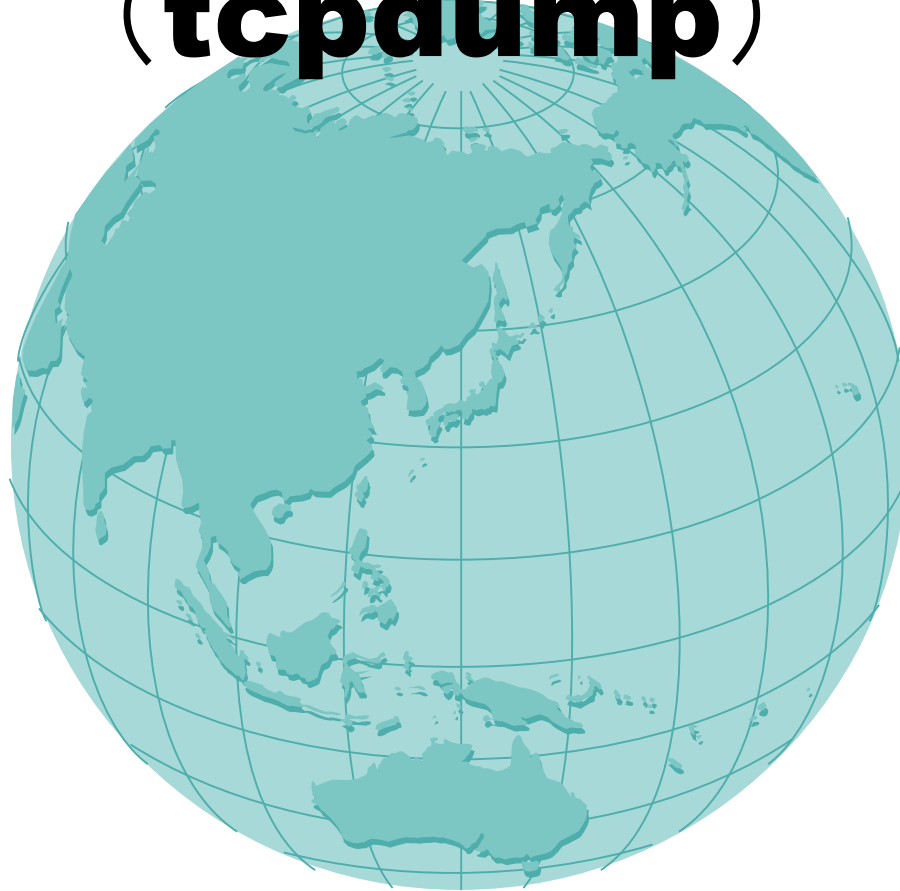


TCP/IPの通信手順 (`tcpdump`)



7月19日 森田 互昭

内容



- **TCPでの通信手順**

**tcpdumpを用いて、
実際のtcpパケットの内容を出力し、説明**

tcpdump

- ネットワーク上のパケットを
モニタリングするコマンド。

```
# tcpdump host tsuji and port 80
```

```
11:26:59.113561 tsuji.4376 >www.google.com.http: S
```

```
3898758850:3898758850(0) win 16384 <mss 1460> (DF)
```

tcpdumpの出力例

```
# tcpdump host tsuji and port 80
```

```
11:26:59.113561 tsuji.4376 >www.google.com.http: S
```

```
3898758850:3898758850(0) win 16384 <mss 1460> (DF)
```

時刻	HH:MM:SS.マイクロ秒
送信元アドレス	ホスト名(またはIPアドレス). ポート番号
宛先アドレス	ホスト名(またはIPアドレス). ポート番号:
フラグ	S: SYN(コネクション確立要求) P: PUSH(即時にデータを送るよう要求) F: FIN(コネクション開放要求) R: RST(コネクション強制切断要求)
シーケンス番号	・新しいデータの最初のバイトのシーケンス番号 ・今までに送ったデータの最後のバイトのシーケンス番号+1 ・バイト数

tcpdumpの出力例

```
# tcpdump host tsuji and port 80
```

```
11:26:59.113561 tsuji.4376 >www.google.com.http: S
```

```
3898758850:3898758850(0) win 16384 <mss 1460> (DF)
```

ACK番号	ACK:ACK(確認応答)番号
ウィンドウサイズ	受信可能なデータ長
フラグメント禁止	(DF):フラグメント(パケット分割)禁止ビットON
mss	最大パケット長を指定したバイト数に制限

tcpdumpによる **TCP**動作観察

```
#tcpdump host tsuji and port 80
```

・・・ポート番号80

host tsujiでのTCPパケットを取得

```
%netscape
```

tsujiでnetscapeを起動し、

その時のパケットの内容を観察

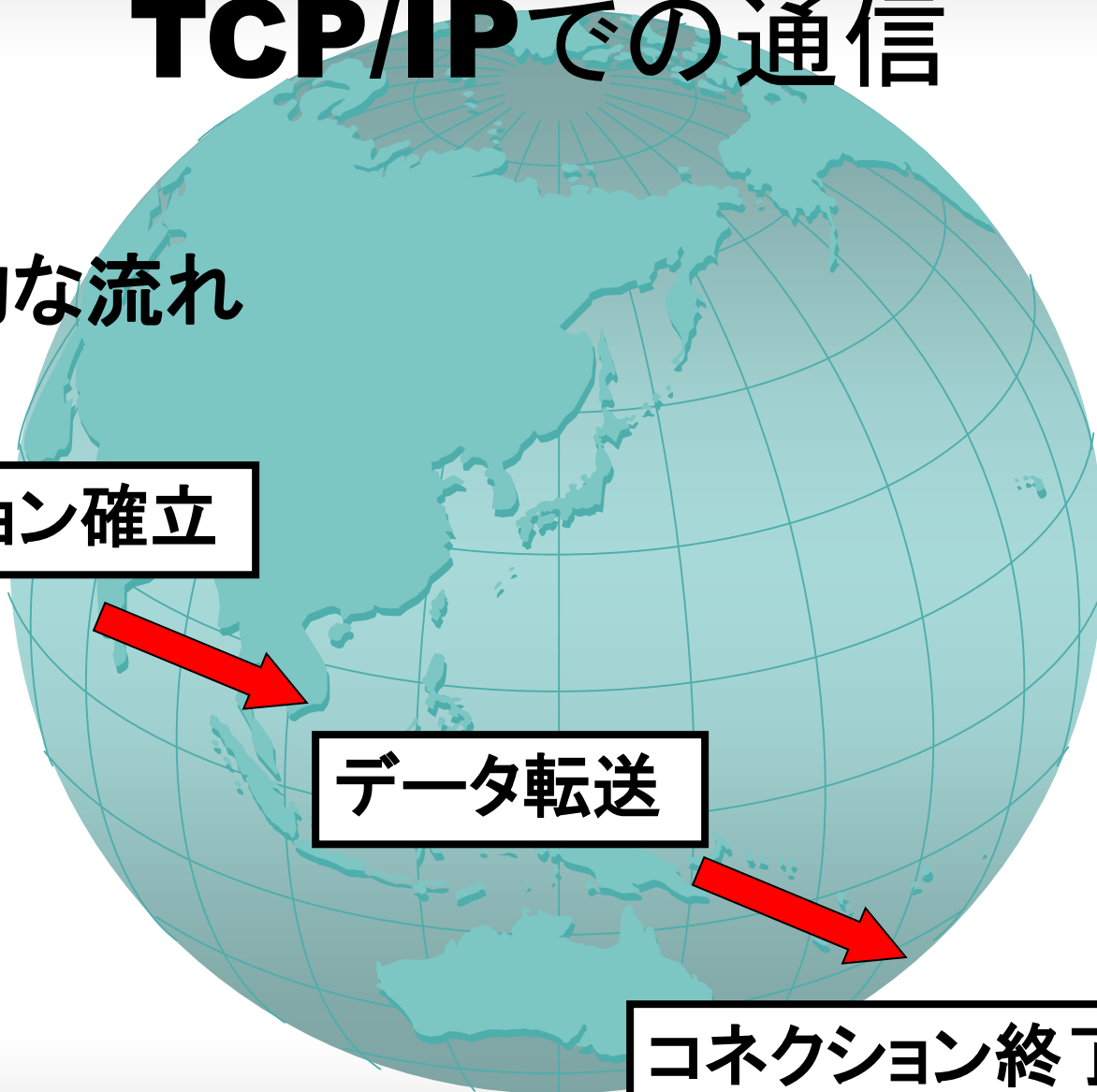
TCP/IPでの通信

- 基本的な流れ

コネクション確立

データ転送

コネクション終了処理



コネクション確立

21:19:27.445117 tsuji.4376 > www.google.com.http: **S**
3898758850:3898758850(**0**) win 16384 <mss 1460> (DF)



サーバ側に**S(SYN)**を送信、コネクション確立を要求
送信バイト0、受信可能データ長16KB、最大パケット長1460B

21:19:27.706707 www.google.com.http > tsuji.4376: **S**
3317888770:3317888770(0) **ack 3898758851 win 32120**
<mss 1460> (DF)



ACK(シーケンス番号+1)を送信
クライアント側に下りのコネクション確立を要求

21:19:27.706813 tsuji.4376 > www.google.com.http: .
ack 1 win 17520 (DF)

下りのコネクション確立を通知

データ転送

21:19:27.723972 tsuji.4376 > www.google.com.http: **P**
1:346(**345**) ack 1 win 17520 (DF)

345 バイトのシーケンスを発生

P(PUSH)フラグ: 速やかに受信データをアプリケーションに渡すよう指定

21:19:27.977446 www.google.com.http > tsuji.4376: **P**
1:184(**183**) ack **346** win 32120 (DF)

ACK番号により、サーバはクライアントから送信された **346** までのデータ(つまり全部)を受信できたことを示す

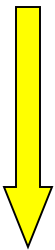
⋮

コネクション終了処理



21:19:37.982740 www.google.com.http > tsuji.4376: **F**
1690:1690(**0**) ack 346 win 32120 (DF)

F(FIN) ビットを立てクライアント側に下りコネクションの開放要求



21:19:37.982849 tsuji.4376 > www.google.com.http: . ack
1691 win 17520 (DF)

FIN に対する **ACK** を返す

クライアント→サーバに同様の処理を行い、コネクション終了

実習



- 自分のマシンで

```
#tcpdump host hostname and port 80
```

別のターミナルから

```
%netscape
```

パケットの内容を調べ、TCPの動作を確認。