

tcp wrapper

2002年9月24日

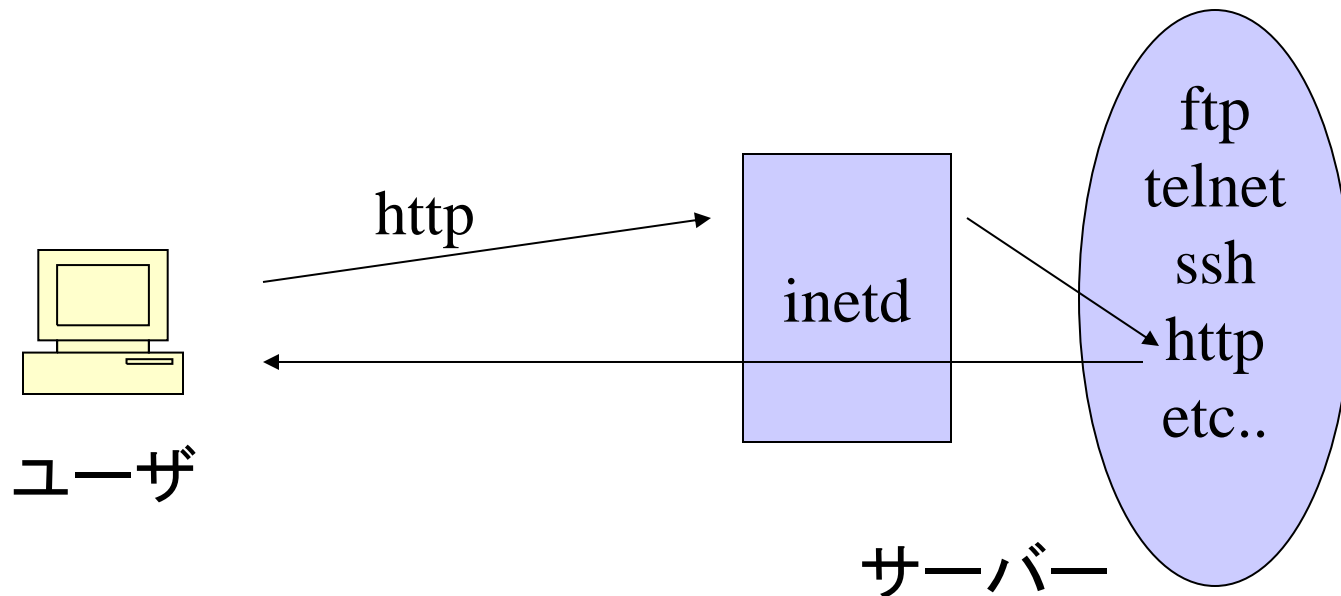
大橋 巧

牧之内研究室「インターネット実習」Webページ

<http://www.db.is.kyushu-u.ac.jp/rinkou/internet/>

▪ inetd

- ユーザーからサービスへの接続要求があったとき必要なサービスを起動
- /etc/inetd.confに記述



▪ inetd.conf

• 要求に応じて起動するサービスを記述

▪ 例

```
ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l
```

▪ サービス名

▪ ソケットの種類 TCPならstream、UDPならdgram

▪ プロトコル TCP or UDP

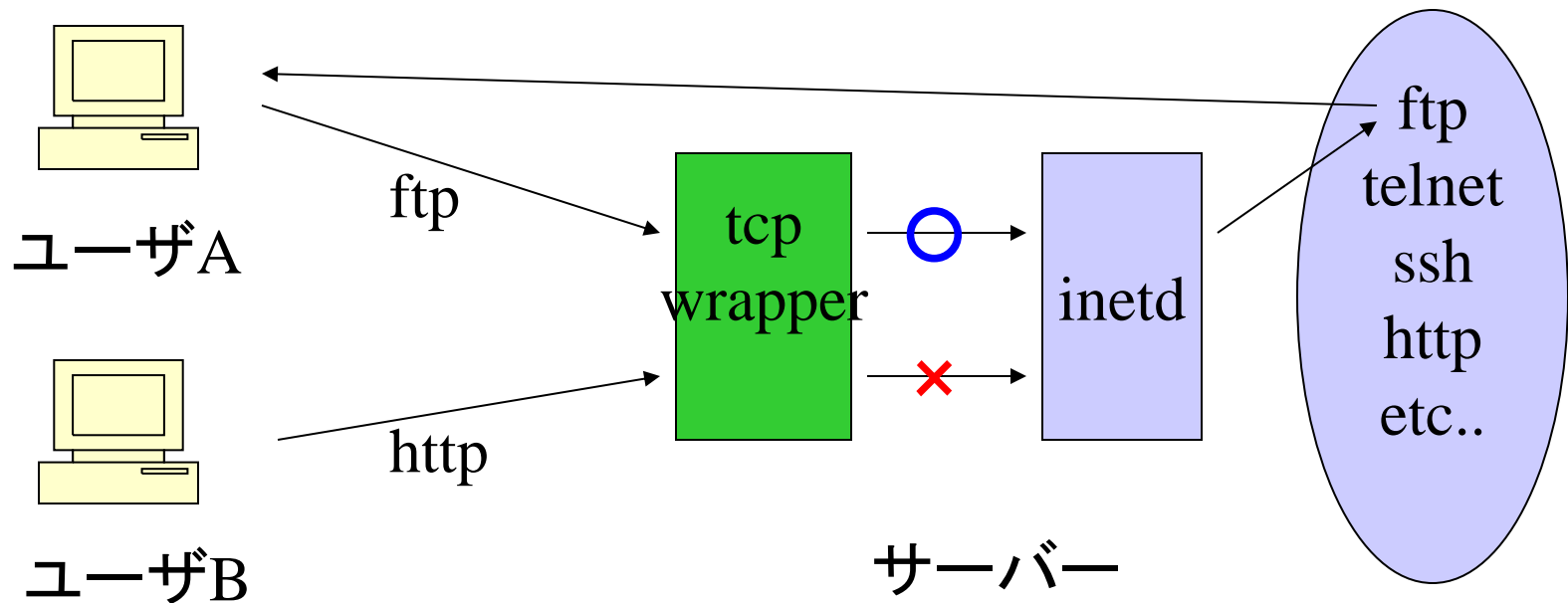
▪ フラグ wait or nowait

▪ 実行ユーザ root, nobody など

▪ 実行するプログラム

▪ tcp wrapperとは？

- inetdを使ってネットワークサービスを動かす場合、そのアクセスを制限



▪ tcp wrapperによる制限

▪ inetd.conf

```
ftp stream tcp nowait root /usr/libexec/ftpd ftpd -l
```



Tcp wrapperで制限



```
ftp stream tcp nowait root /usr/sbin/tcpd ftpd -l
```

- 現在はinetdにtcp wrapperの機能が組み込まれているのでtcpdを介さずともよい。

▪ hosts.allow , hosts.deny

- 接続を許可、拒否するホストを記述
- /etc/hosts.allow, /etc/hosts.deny
- 現在、hosts.allowのみに記述
- デーモン名 : ホスト : allow or deny

▪ 例

telnetd : .db.is.kyushu-u.ac.jp : allow

ftpd : 192.168.33. : allow

ALL : 133.5.18.0/255.255.255.0 : allow

ALL : ALL : deny

・アクセス制御の確認

- `tcpdchk -av`・・・`hosts.allow`の書式のチェック
- `tcpdmatch`

`tcpdmatch` デーモン名 アクセス元

```
% tcpdmatch ftpd 192.168.33.47
client: address 192.168.33.47
server: process ftpd
matched: /etc/hosts.allow line 2
option: allow
access: granted
```

```
% tcpdmatch ftpd ホスト名
client: address ホスト名
server: process ftpd
matched: /etc/hosts.allow line 4
option: deny
access: denied
```

▪ 実験

- inetd.confの書換え
 - kill -HUP inetdのプロセスID
- hosts.allowの書換え
- tcpdchk,tcpdmatchで、アクセス制御が行われていることを確認
- ポートスキャンを行い、アクセス制御が行われていることを確認(open or filterd)