ファイアウォール

ネットワークと情報セキュリティ2

菊池　浩明

講義内容

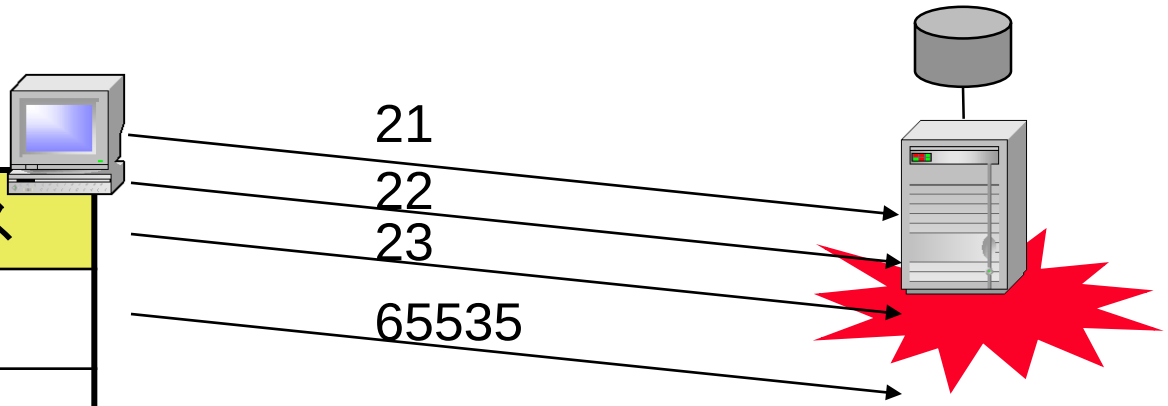
- 1. 不正アクセスの脅威
- 2. ファイアウォール
  - パケットフィルタリング，NAT, DMZ
- 3. アクセス制御
  - 経路制御表

1.不正アクセスの脅威

1. ポートスキャン

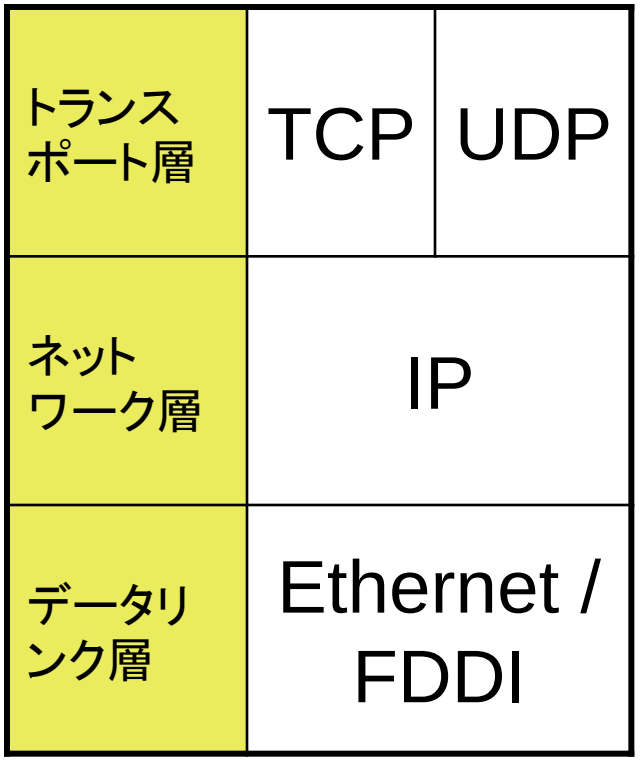
- 侵入可能なポートを自動検査
  - サーバのソフトウェアとバージョンを調査

ポート番号	サービス
21	ftp
23	telnet
25	smtp
80	http
110	pop3

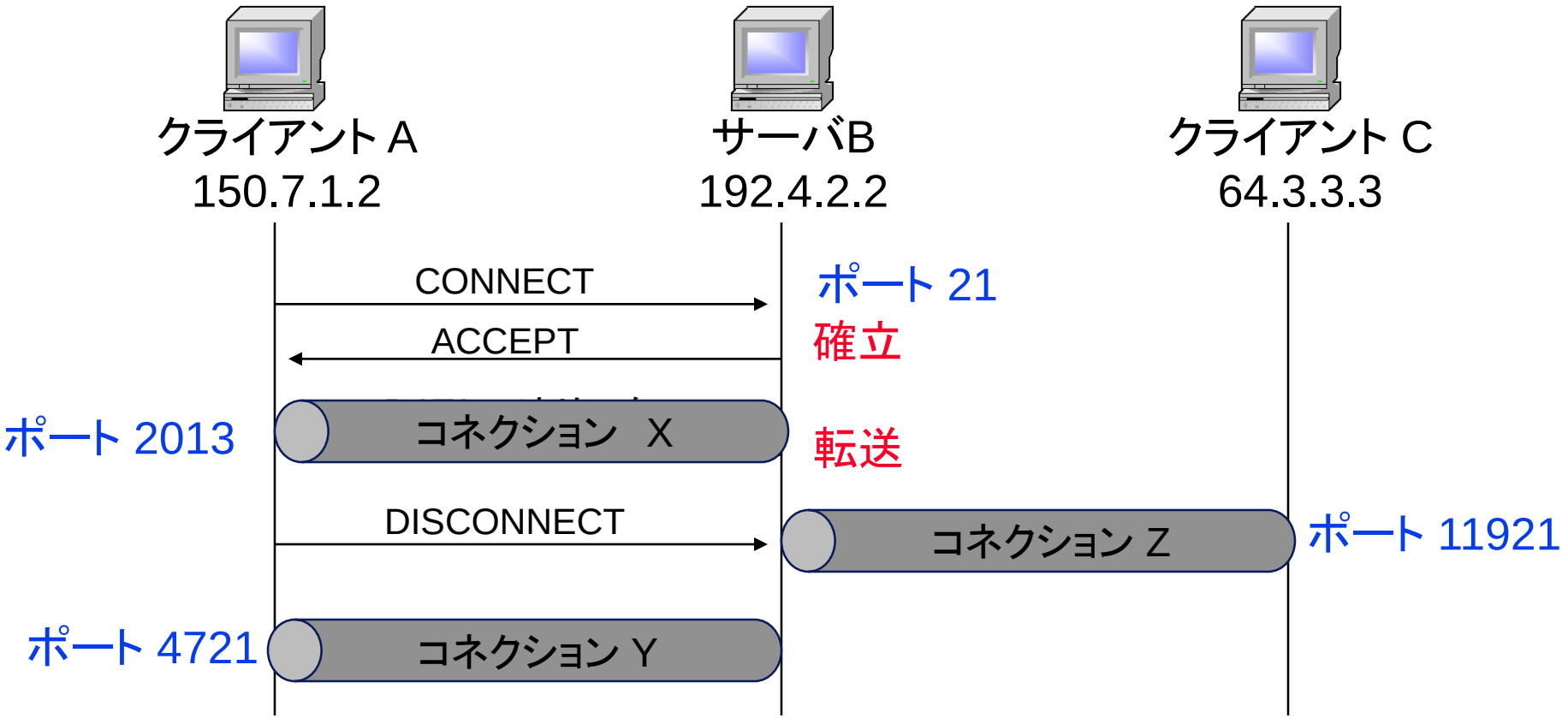


TCPとUDP

- TCP
  - Transmission Control Protocol
  - 信頼性のあるストリーム
    - » 再送と通信順序の保証
  - コネクション・バーチャルサーキット
- UDP
  - User Datagram Protocol
  - コネクションレス



コネクション



X の識別子: エンドポイント (150.7.1.2, **2013**) と (192.4.2.2,**21**)
Y の識別子: エンドポイント (150.7.1.2, **4721**) と (192.4.2.2,**21**)

Well-known port

- 1024までの共通ポート番号
  - サーバ側で利用
  - RFC 1700 Assigned Numbers

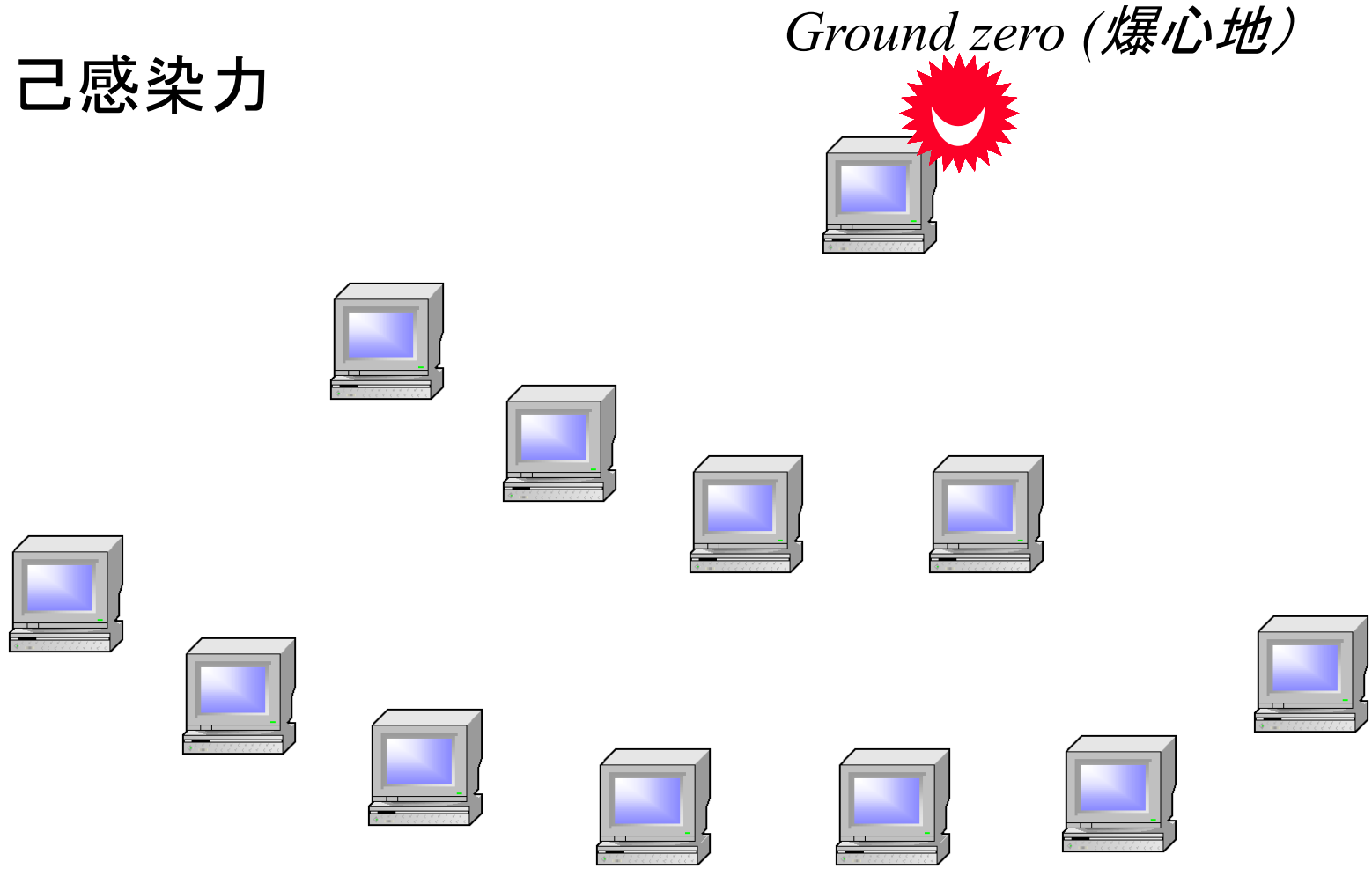
ポート番号	サービス
21	ftp
23	telnet
25	smtp
80	http
110	pop3

nmap 実行例

```
# nmap -sT -O target-host.u-tokai.ac.jp
    Starting nmap 3.48  at 2014-07-12 07:26 JST
    Interesting ports on XXX.u-tokai.ac.jp (150.7.XX.XX):
    PORT      STATE SERVICE
    21/tcp    open  ftp
    23/tcp    open  telnet
    25/tcp    open  smtp
    80/tcp    open  http
    110/tcp   open  pop-3
    111/tcp   open  rpcbind
    …
    515/tcp   open  printer
    Device type: general purpose
    Running: Linux 2.1.X|2.2.X
    OS details: Linux 2.1.19 - 2.2.25
    Uptime 72.815 days (since Fri Apr 30 11:53:05 2004)
    Nmap run completed -- 1 IP address (1 host up) scanned
      in 10.163 seconds
```

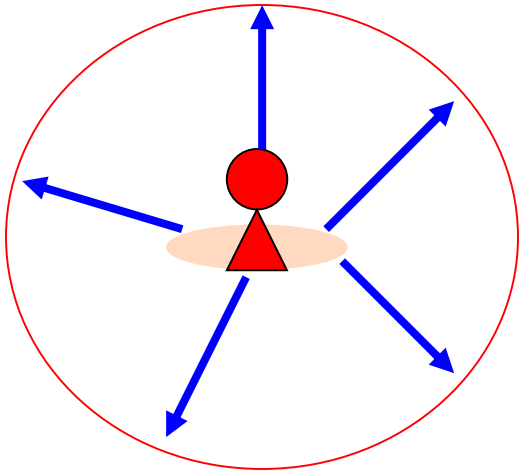
感染の早さ

- 自己感染力



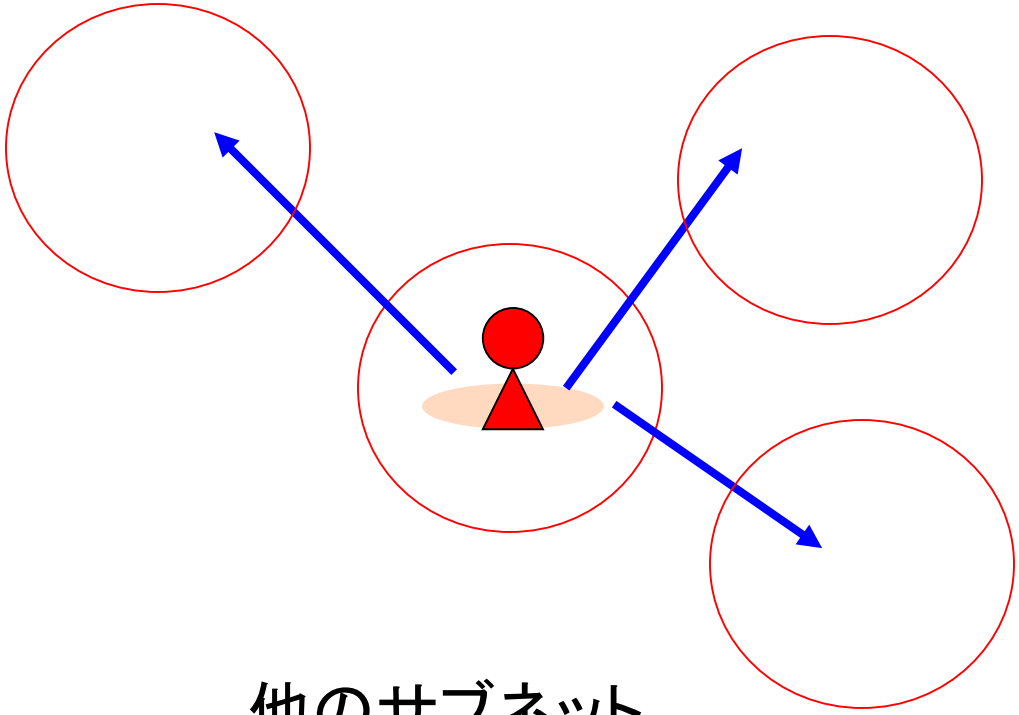
探索の戦略

近くを狙え　（ローカル）



同一サブネット
(sasser 23%)

遠くを狙え（グローバル）「渡り」



他のサブネット
(sasser 32%)

W32.CodeRed3.worm　ランダム型

- 2001/7/18
  - 最初の本格的ワーム
  - HTTPによる感染
  - TCP 135 によるネットワークからの侵入
  - ランダムなアドレスのPCを狙う（グローバル探索）

150. 7. 64. 23.

日立製作所 ワームノード探索活動の可視化ツール
http://www.hitachi.co.jp/hirt/publications/hirt-pub07004/07004-03.html

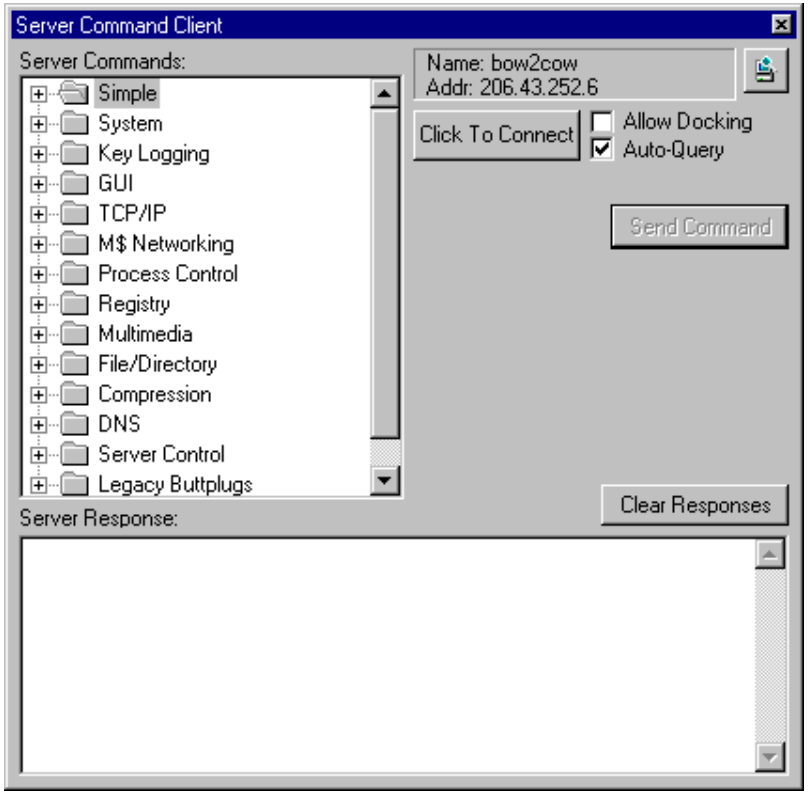
W32.Blaster.worm　ローカル型

- 2003/7/17
  - 世界19万台感染
  - TCP 135 によるネットワークからの侵入
  - 近くのPCを狙って感染（ローカルアドレス探索）

http://www.hitachi.co.jp/hirt/publications/hirt-pub07004/07004-03.html

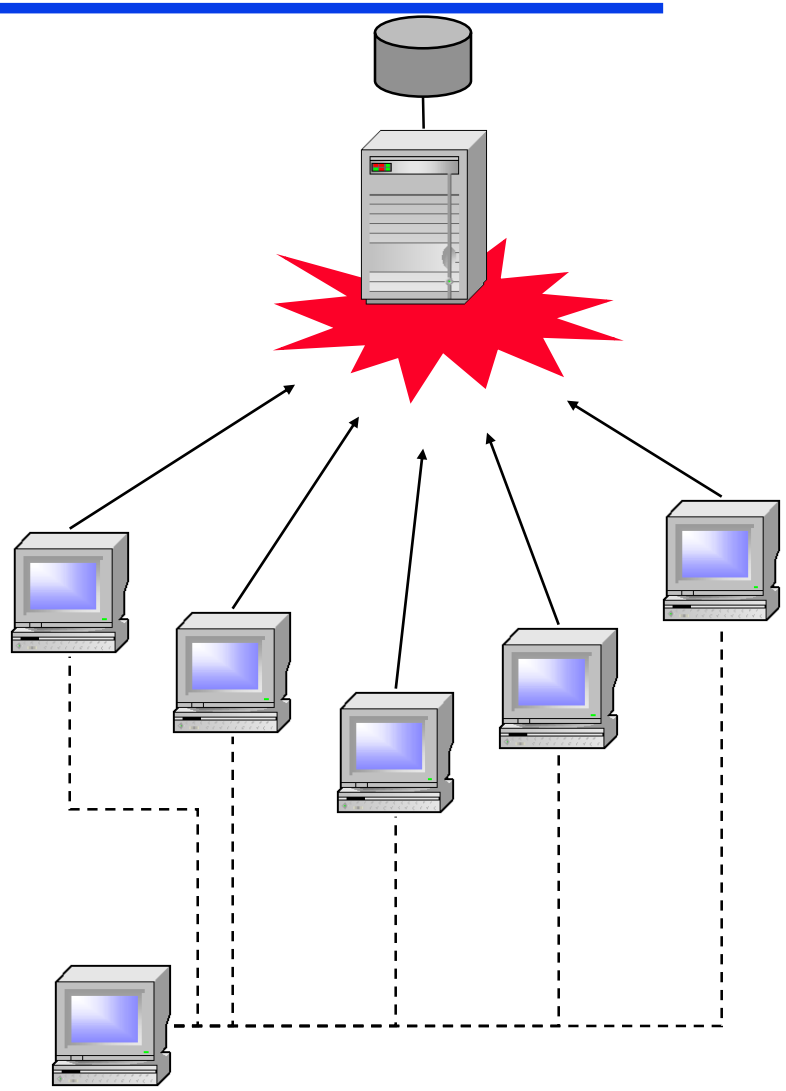
2. バックドア （裏口）

- Back Orifies (BO2k)
  - Win2000用遠隔操作
  - トロイの木馬
  - 攻撃先にインストール
  - 遠隔インストール，ネットワーク管理，
    リブート，DNS設定，プロセス制御，e.t.c.
  - 他のホストへの攻撃（踏み台）



3. ボットネット

- 新種ウィルス
  - IRC制御のトロイの木馬型
  - ロ「ボット」から
  - 命令されて攻撃やスキャンを実行
  - 例）PRIVMSG #plazm :.ddos.synflood 66.xxx.xxx.xxx 100 0 27015
  - 変種
    - » Gaobot, spybot, agobot, polybot



ボットの動作

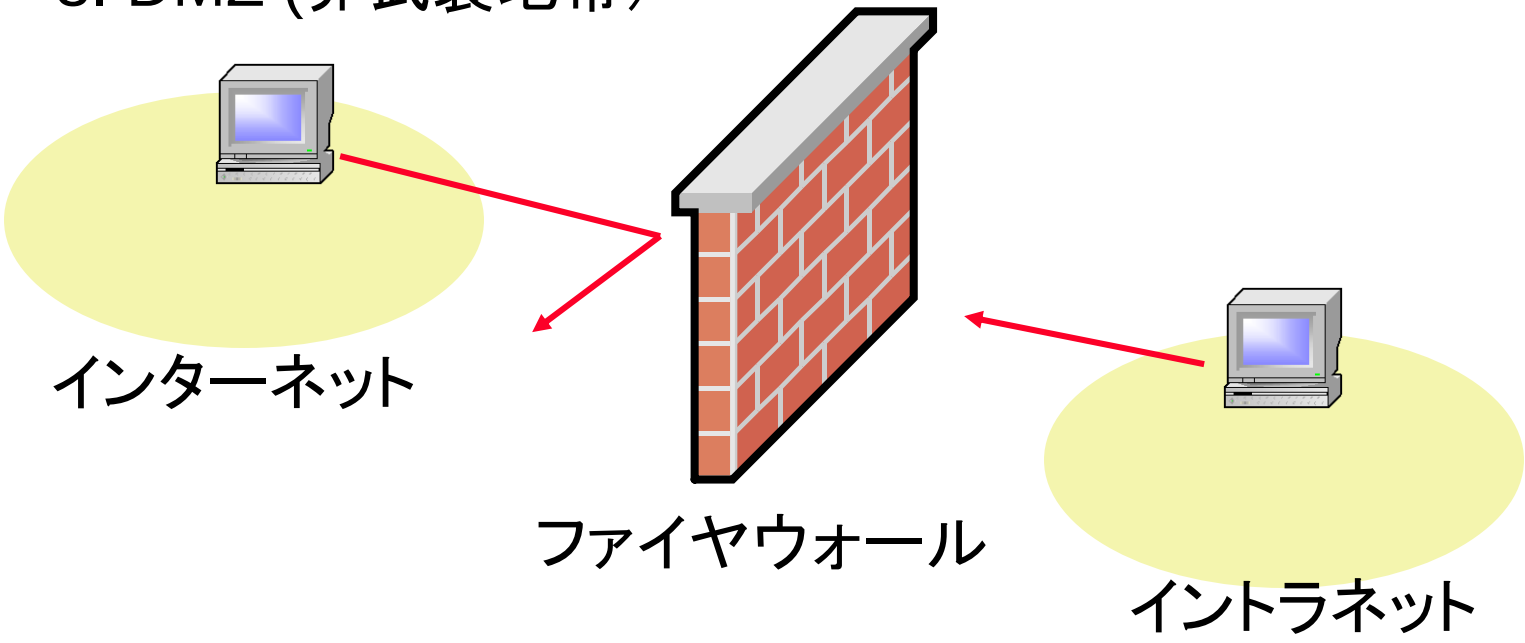
- ネットワークインシデント対策センター
  - 情報通信研究機構
  - 大規模不正行為（Bot)
  - サービス妨害攻撃 (DoS)

http://www.nict.go.jp/publication/NICT-News/0607/resarch/index.html

2. ファイアウォール

ファイアウォール （防火壁）

- 機能
  1. パケットフィルタリング
  2. NAT (アドレス変換）
  3. DMZ (非武装地帯）

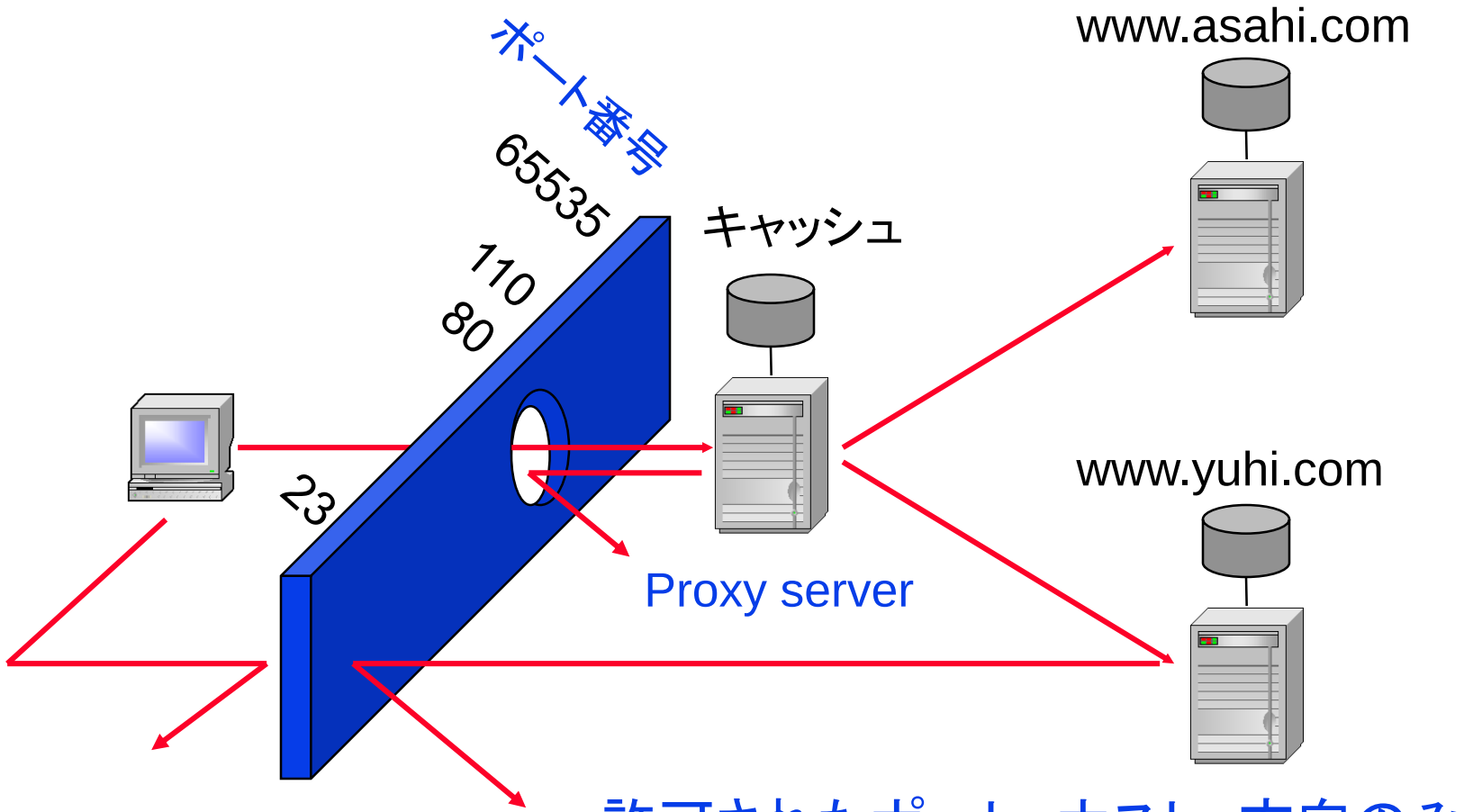


ファイヤウォール

- ファイアウォールの製品
- Check Point社
  - FireWall-1
  - IPSec, SSL VPN
  - ステートフル・インスペクション
  - リモートアクセス
- cf. パーソナルファイアウォール

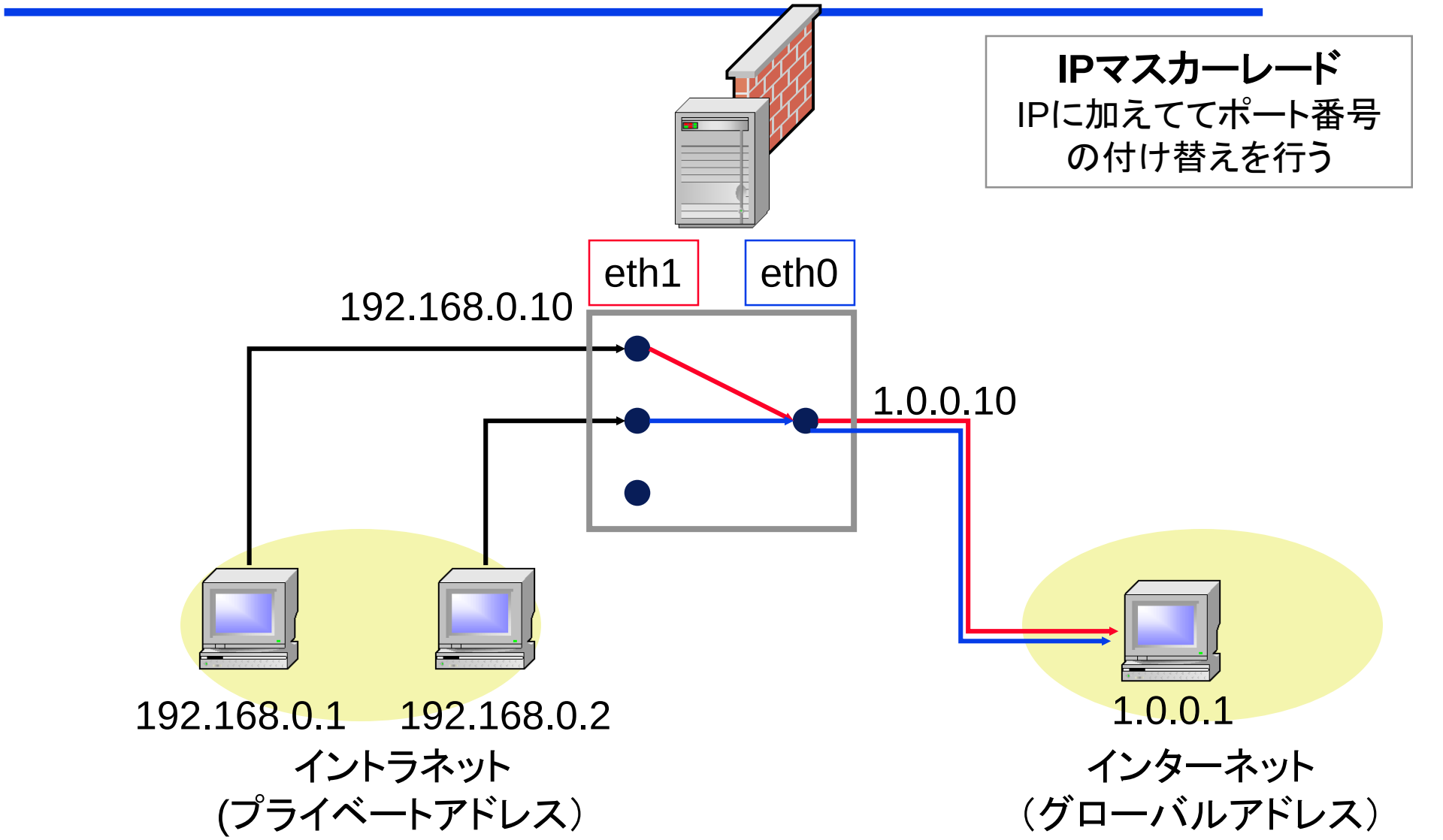
http://www.checkpoint.co.jp/products/firewall-1/

1. パケットフィルタリング

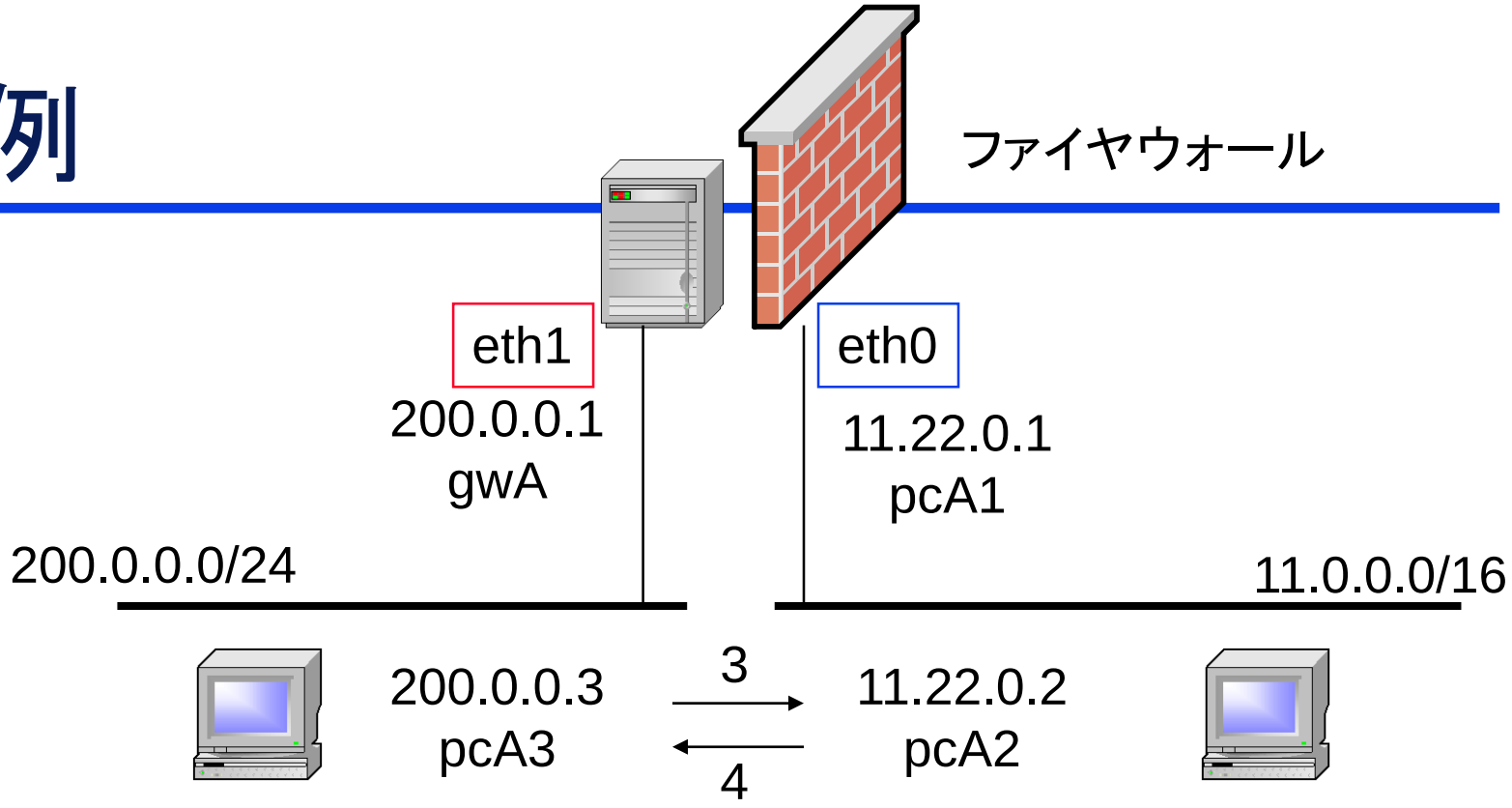


許可されたポート，ホスト，方向のみ
IPパケットを転送

2. NAT(Network Address Translation)

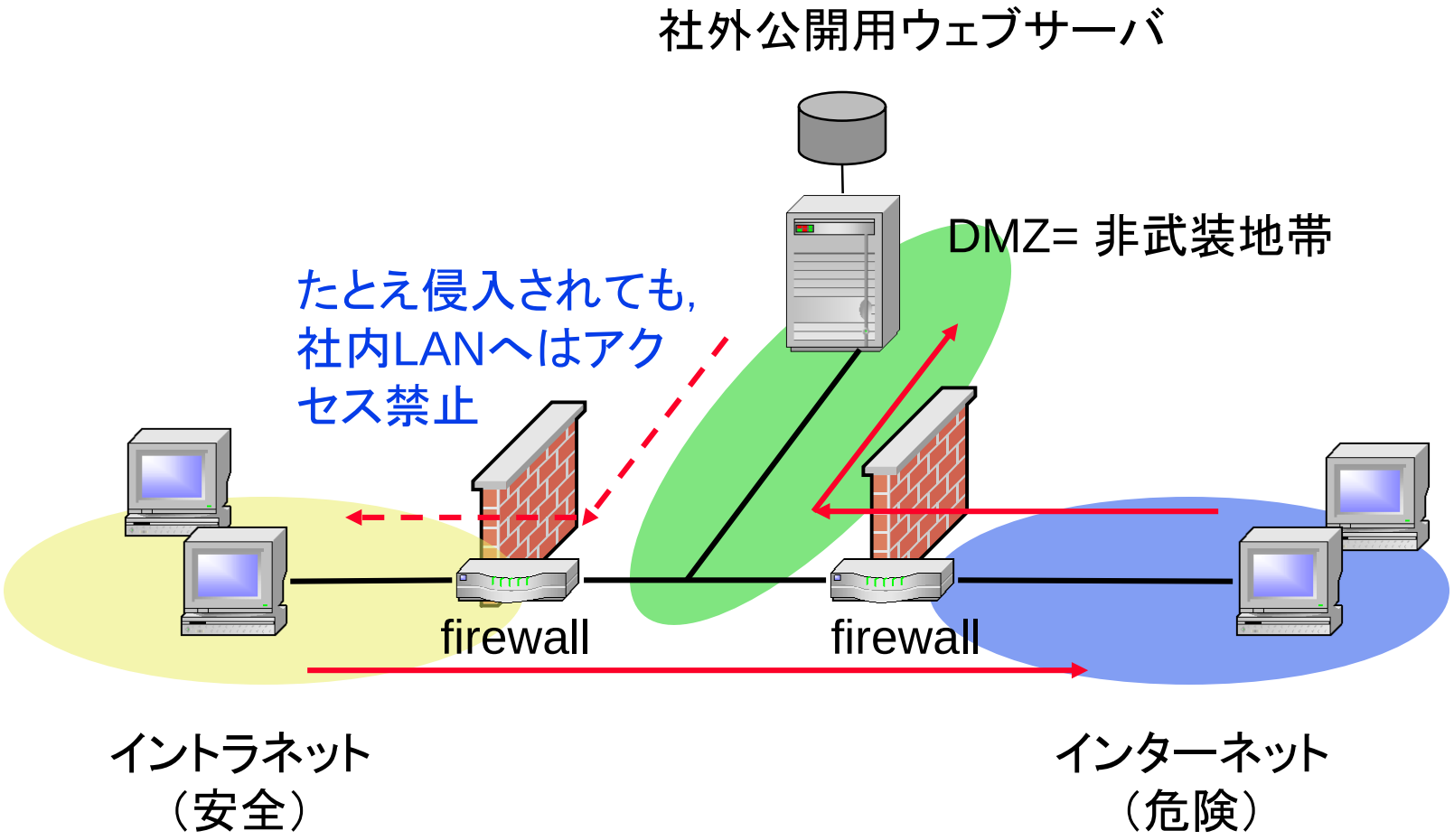


例

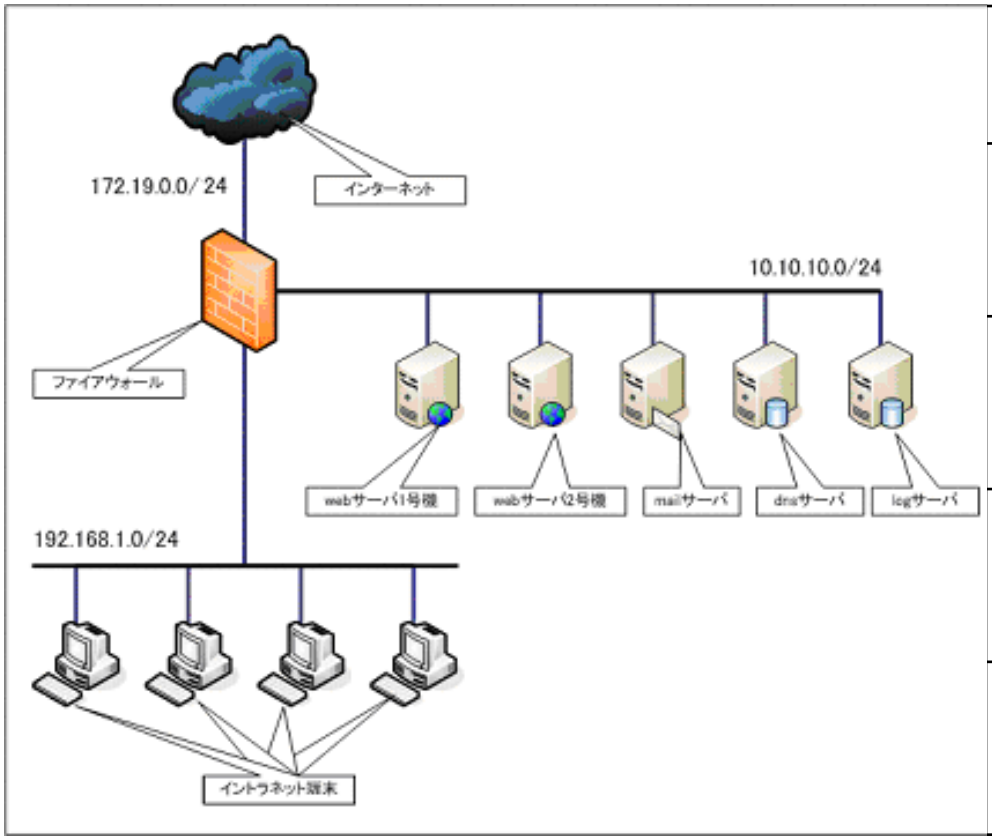


実行元	コマンド	pcA4 （内側）でのEthereal		pcA2 （外側）でのEthereal	
pcA3	ping pcA2	200.0.0.3	11.22.0.2	11.22.0.1	22.22.0.2

3. DMZ demilitarized zone



ポリシー設計の例 (Internet→DMZ)



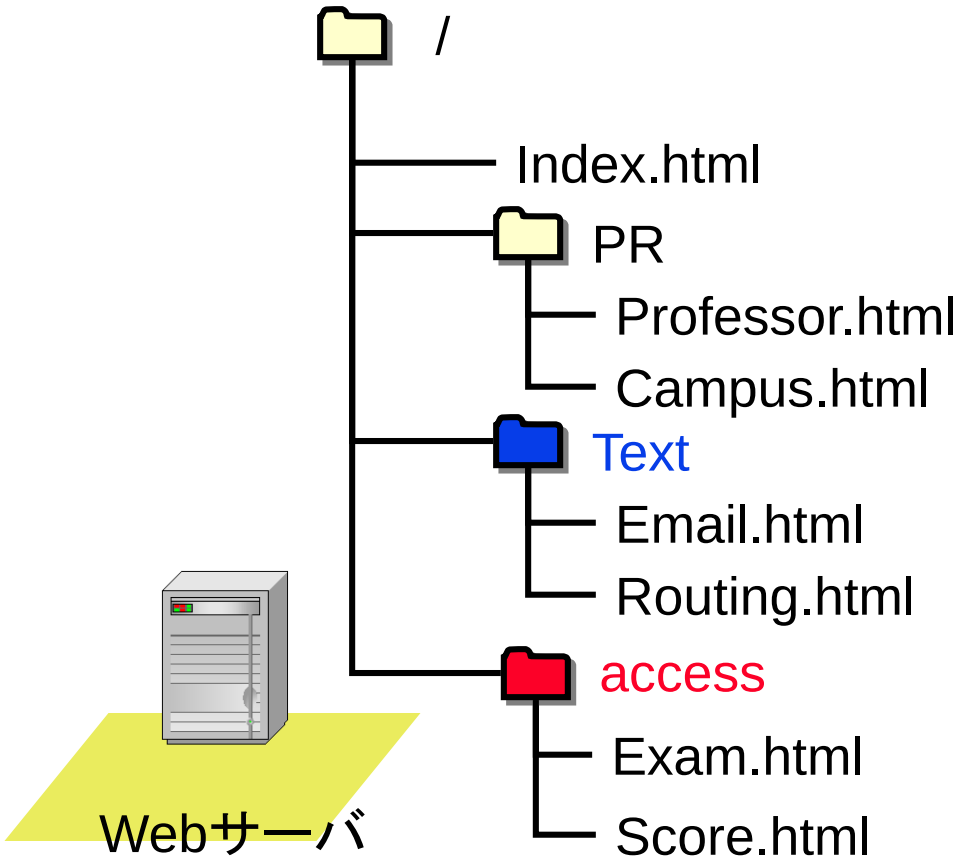
送信元アドレス	送信先アドレス(NATアドレス)	使用サービス	備考
Any	172.19.10.82 (10.10.10.80)	80/TCP 443/TCP	公開Webサーバ用
Any	172.19.10.83 (10.10.10.88)	80/TCP	公開Webサーバ用
Any	172.19.10.84 (10.10.10.110)	25/TCP	Mailサーバ用
Any	172.19.10.84 (10.10.10.53)	53/UDP	DNSサーバ用

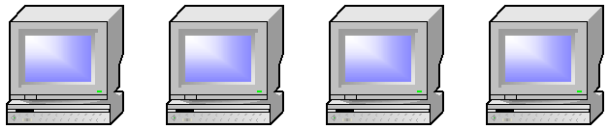
http://www.sec.ocn.ne.jp/information/column/co20060801_03.html

3. 経路制御とアクセス制御

アクセス制御の例

http://www.imedia.com



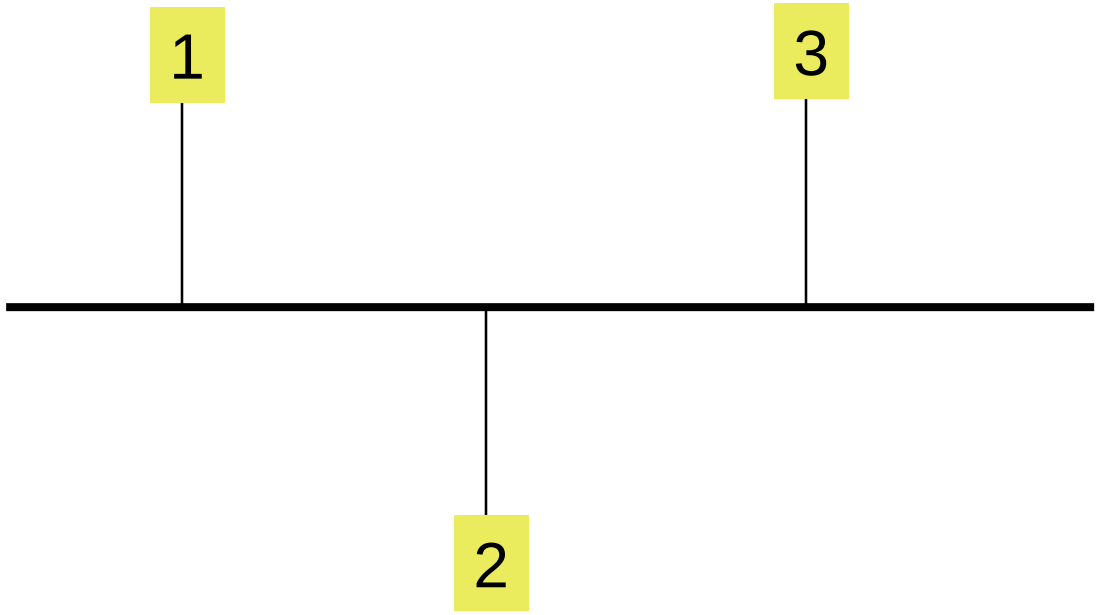


学外	学生	院生	教員
○	○	○	○
×	○	○	○
×	×	×	○

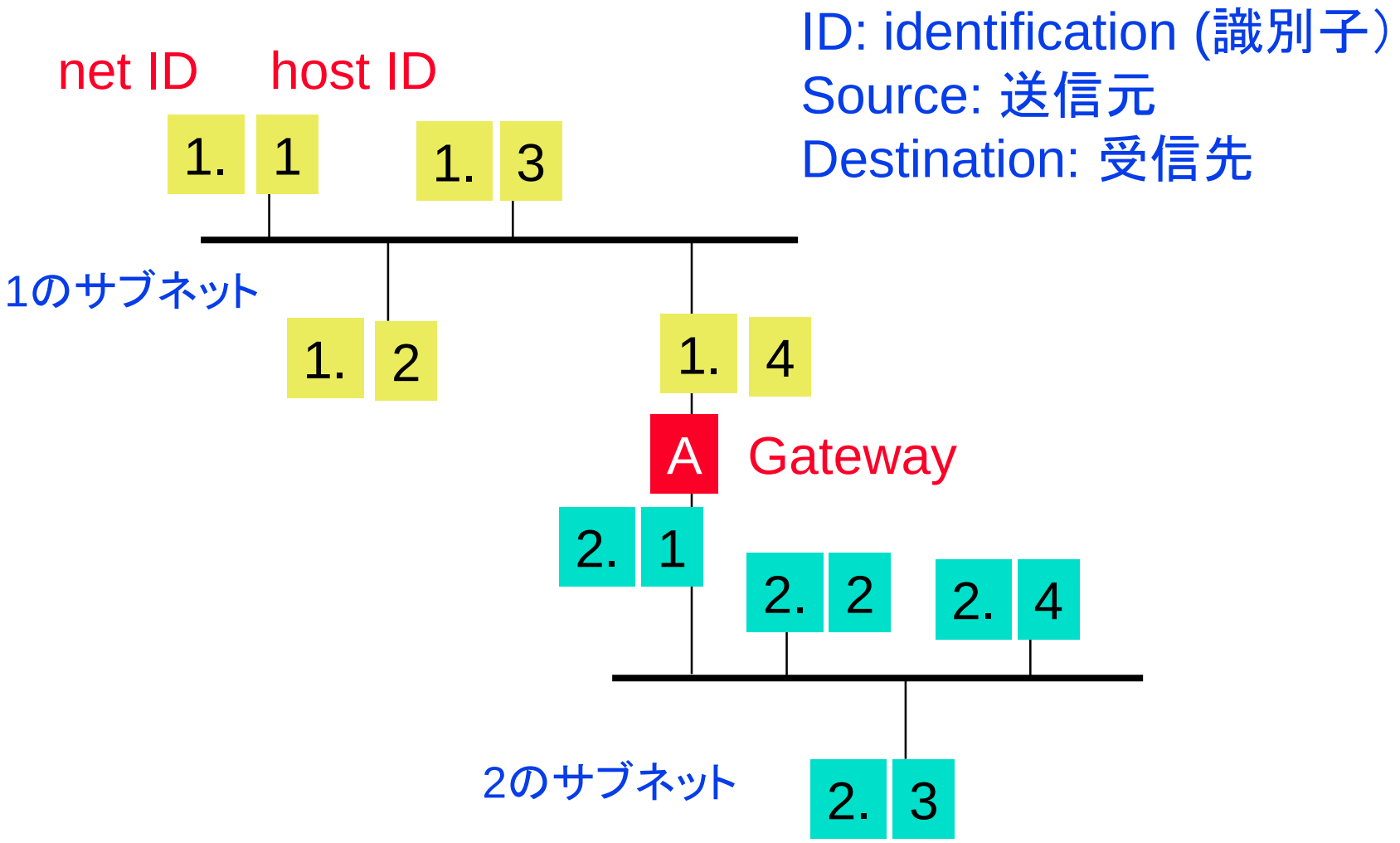
アクセス制御技術

- Capability
  - Subject が権限の証拠を持つ
- Access Control List (ACL)
  - Objectがアクセスできるsubjectを指定する.

LAN

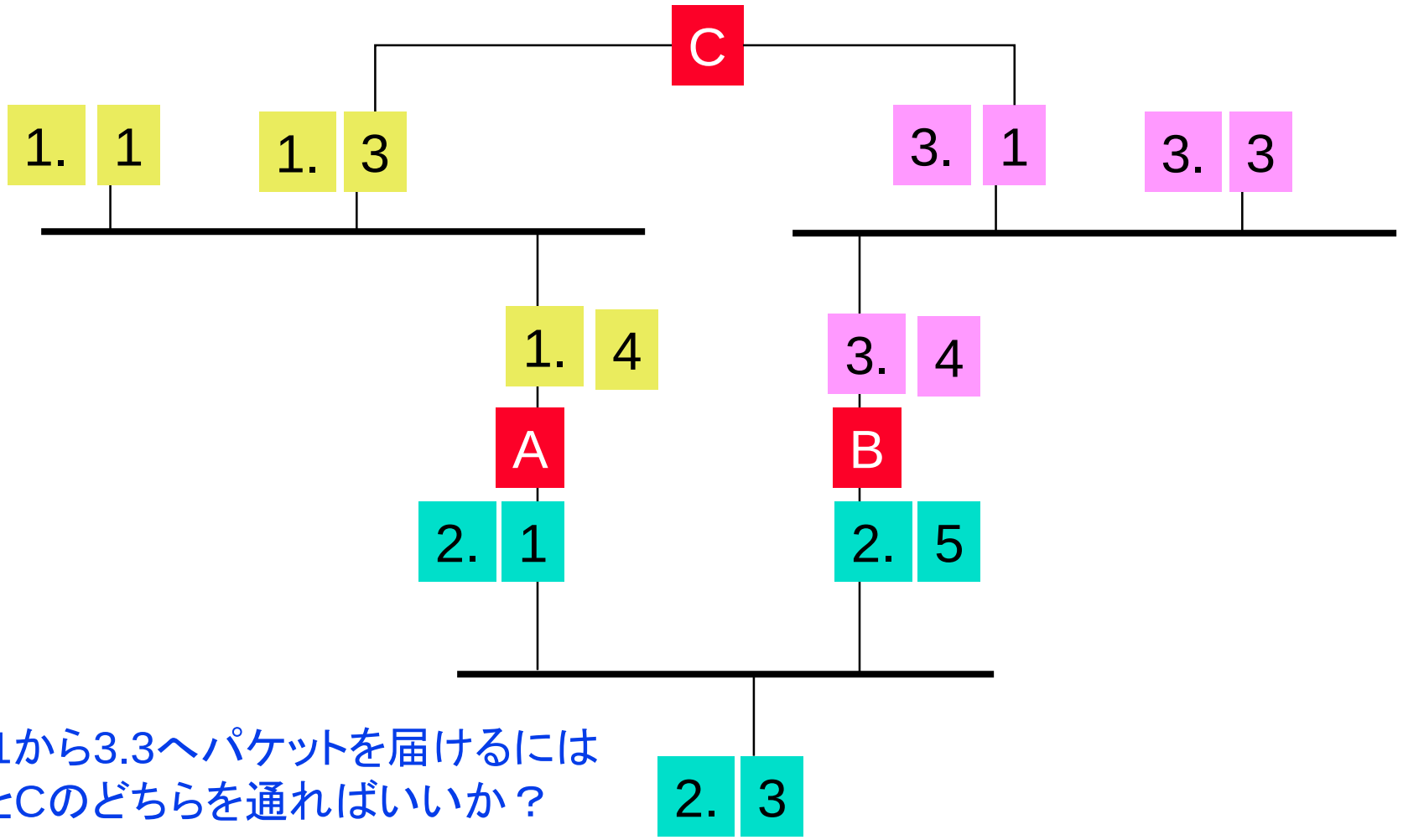


WAN



ID: identification (識別子)
Source: 送信元
Destination: 受信先

経路制御　routing (ルーティング)

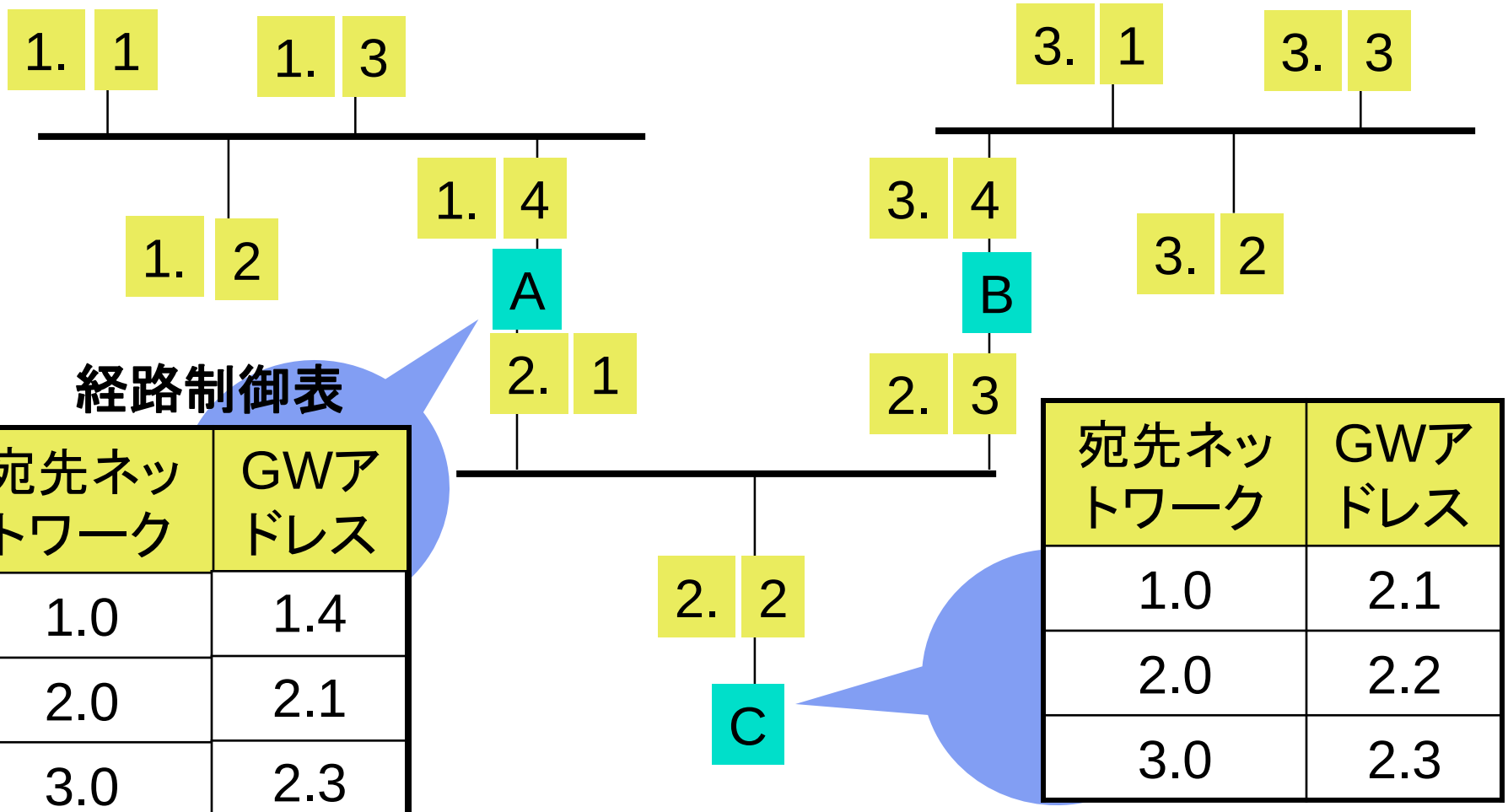


1.1から3.3へパケットを届けるには
AとCのどちらを通ればいいか？

経路制御

- 非適応（static 静的）
- 適応（adaptive 動的）
  - 中央集中型
    - » 最適な経路選択
    - » 障害に弱い，負荷の集中，規模の制約
  - 分散型
    - » ロバスト性（耐障害性）
    - » 経路選択の問題

ダイナミックルーティング



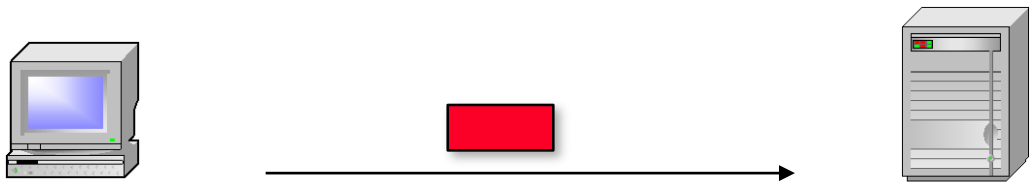
経路制御表

宛先ネットワーク	GWアドレス
1.0	1.4
2.0	2.1
3.0	2.3

宛先ネットワーク	GWアドレス
1.0	2.1
2.0	2.2
3.0	2.3

アクセス制御の条件

- TCP Connection
  - 送信元アドレス　source IP (sip)
  - 宛先アドレス　destination IP (dip)
  - 送信元ポート　source port (sp)
  - 宛先ポート　destination port (dp)
  - Flag　Ack, Syn



sip = 10.0.0.1
(sp = 2222)

dip = 20.0.0.2
dp = 80

1. Allow(許可)とdeny(拒否)

sip	dip	通過
10.0.0.0/8	10.0.0.0/8	drop
10.0.0.0/8	20.0.0.0/8	pass
20.0.0.0/8	10.0.0.0/8	pass
20.0.0.0/8	20.0.0.0/8	drop

- 1.
  - deny all
  - allow sip=10.0.0.0/8 dip=20.0.0.0/8
  - allow sip=20.0.0.0/8 dip = 10.0.0.0/8
- 2.
  - allow all
  - deny sip = 10.0.0.0/8 dip = 10.0.0.8/8
  - deny sip=20.0.0.0/8 dip=20.0.0.0/8

- どちらがよいか?

2. 重複するルール

sip	dip	sp	dp	通過
10	10	any	80	pass
10	10	any	53	pass
10	20	any	80	pass
10	20	any	53	drop
20	10	any	80	pass
20	10	any	53	pass
20	20	any	80	pass
20	20	any	53	drop

- 3.
  - deny all
  - allow sip=10 dip=10 dp=80
  - allow sip=10 dip=10 dp=53
  - allow sip=10 dip=20 dp=80
  - allow sip=20 dip=10 dp=80
  - allow sip=20 dip=10 dp=53
  - allow sip=20 dip=20 dp=80
- 4.
  - deny all
  - allow dp=
  - allow dip=

3. ルールの順序

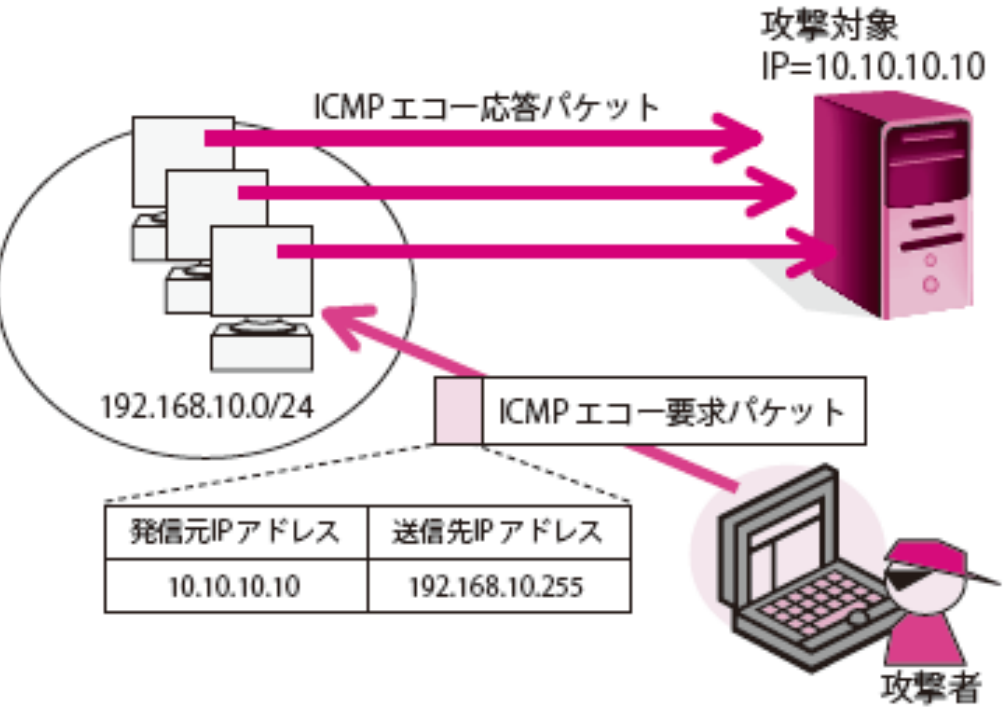
sip	dip	sp	dp	通過
10	10	any	80	
10	10	any	53	
10	20	any	80	
10	20	any	53	
20	10	any	80	
20	10	any	53	
20	20	any	80	
20	20	any	53	

- 6.
  1. allow all
  2. deny dp=80
  3. allow sip=10 dip=10
- 7.
  1. allow all
  2. allow sip=10 dip=10
  3. deny dp=80

❑ フィルタリング結果が変わるところはどこか？

DoSの防止

- Smurf攻撃



出典: 寺田,「情報処理」, Vol. 54, 2013

- Drop all ICMP packets going to a “broadcast” address (eg 130.207.255.255).

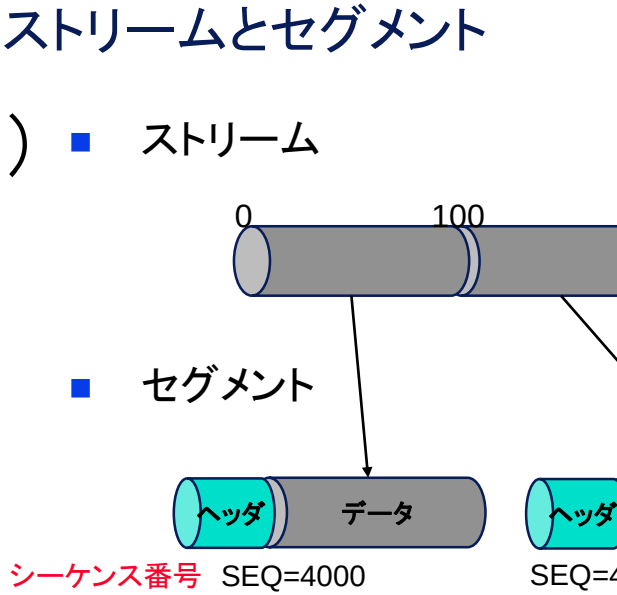
アクセス制御リスト ACLの例

- フィルタリングのルールを定めた表．条件とアクション（許可，拒否，遮断）

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

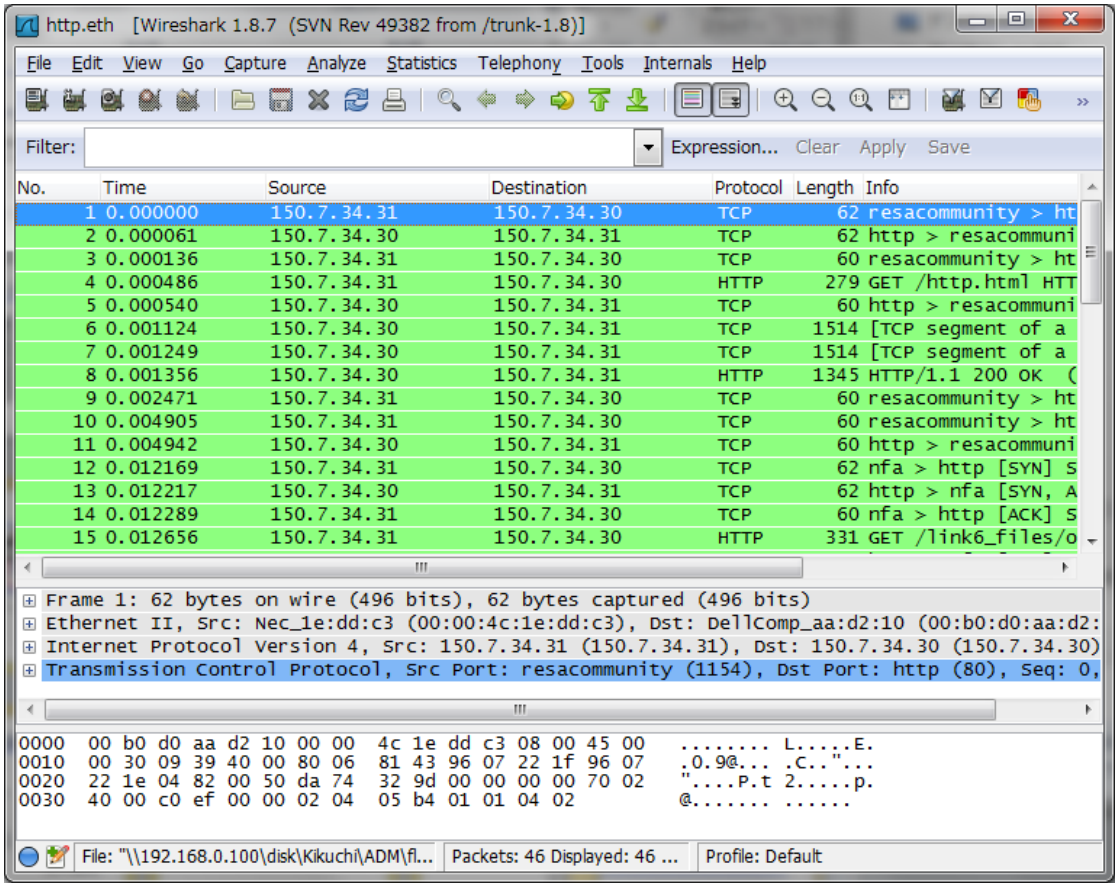
StatelessとStatefullフィルタリング

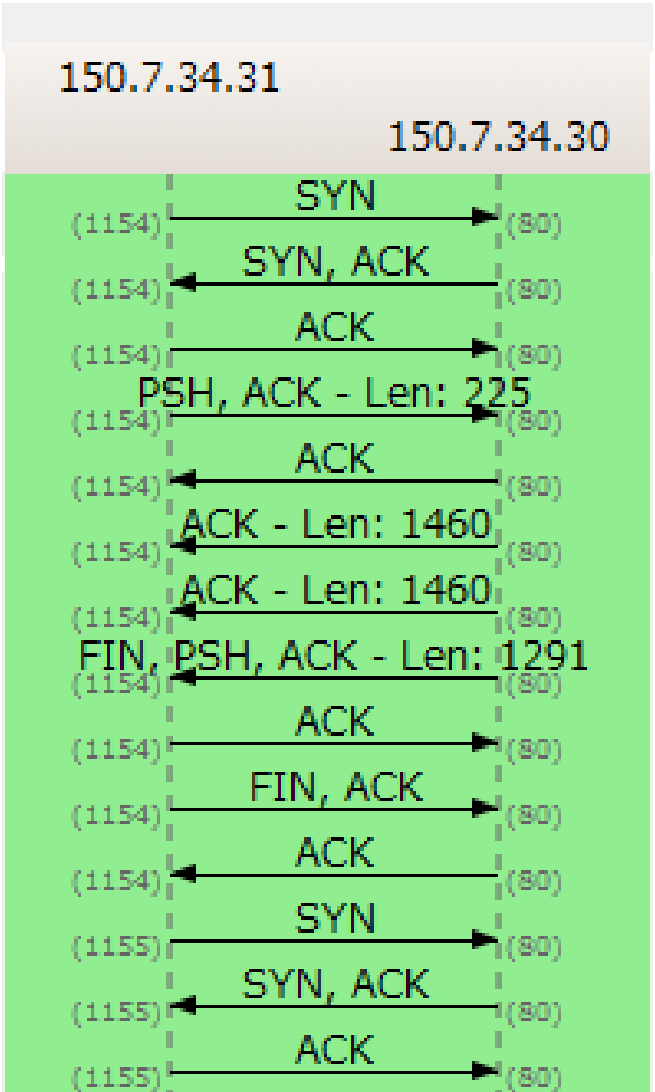
- TCPコネクションのフィルタリングの困難な点
  - 1. パケット通信（複数のパケットに分割される）
  - 2. inbound(内向き）とoutbound (外向き）の区別



- そこで，statefull (有限状態マシン）なフィルタリングの必要性

TCP stream の例 (HTTP)





Stateful パケットフィルタリング

- statefull packet filter
  - 次のルールは，TCP connectionが確立した後に意味がある

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

  - 通信路を追跡し，通信セットアップ (SYN)，終了(FIN)を判断し，通信路がinboundかoutboundかを判断する.

IDS 侵入検出システム

- IDS (Intrusion Detection System)
  - ネットワーク型・ホスト型
  - 不正検知型 (Misuse Detection)
    - » 不正侵入パターンとのマッチング
  - 異常検知型 (Anomaly Detection)
    - » 通常の行動との差異を検出
  - 課題
    - » フォルスネガティブ （不正なのに誤って検知されない）
    - » フォルス （正常なのに誤って検知される）

まとめ

- 脆弱なホストを探すために，ランダムなIPアドレスに向けて（　　）が行われる．
- ファイアウォールの主要な機能は，パケットフィルタンリグと（　　）と（　　）である．転送するアドレスブロックを指定した（　　）に基づいてパケットを転送する．
- TCP通信路をフィルタリングするには（　　）型のフィルタリングを行う必要．

課題

- 第2章 演習問題
  - 問1, 2, 3, 4