
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

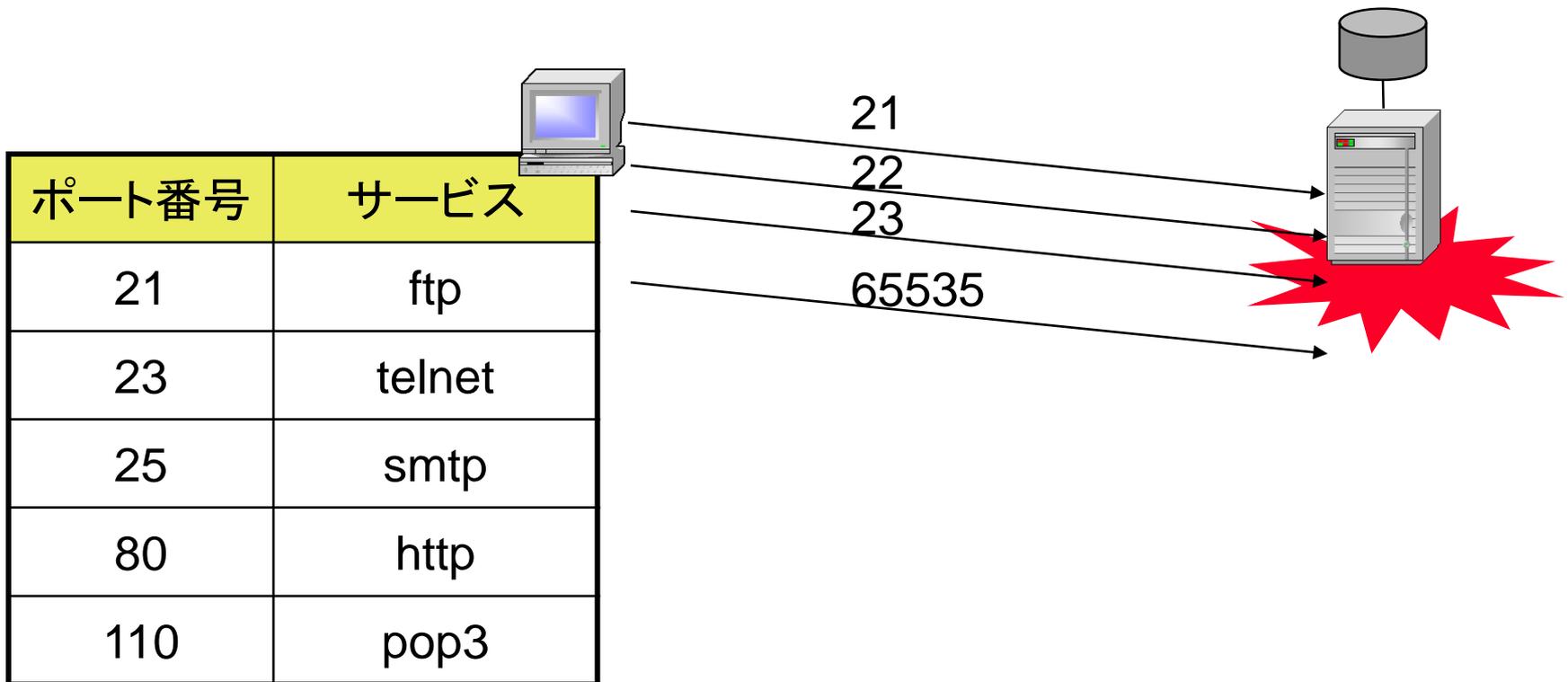
講義内容

- 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



TCPとUDP

■ TCP

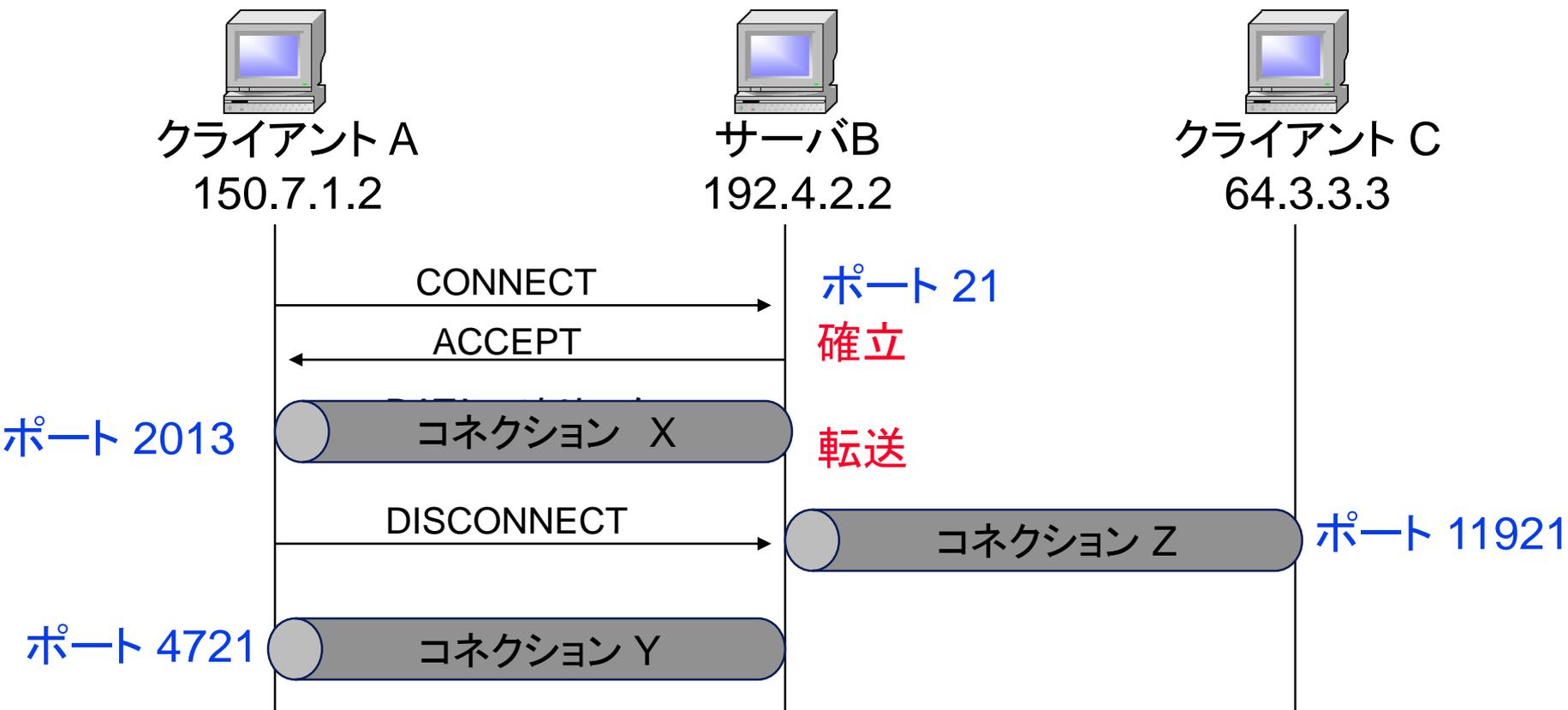
- Transmission Control Protocol
- **信頼性**のあるストリーム
 - » 再送と通信順序の保証
- コネクション・バーチャルサーキット

■ UDP

- User Datagram Protocol
- コネクションレス

トランスポート層	TCP	UDP
ネットワーク層	IP	
データリンク層	Ethernet / FDDI	

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

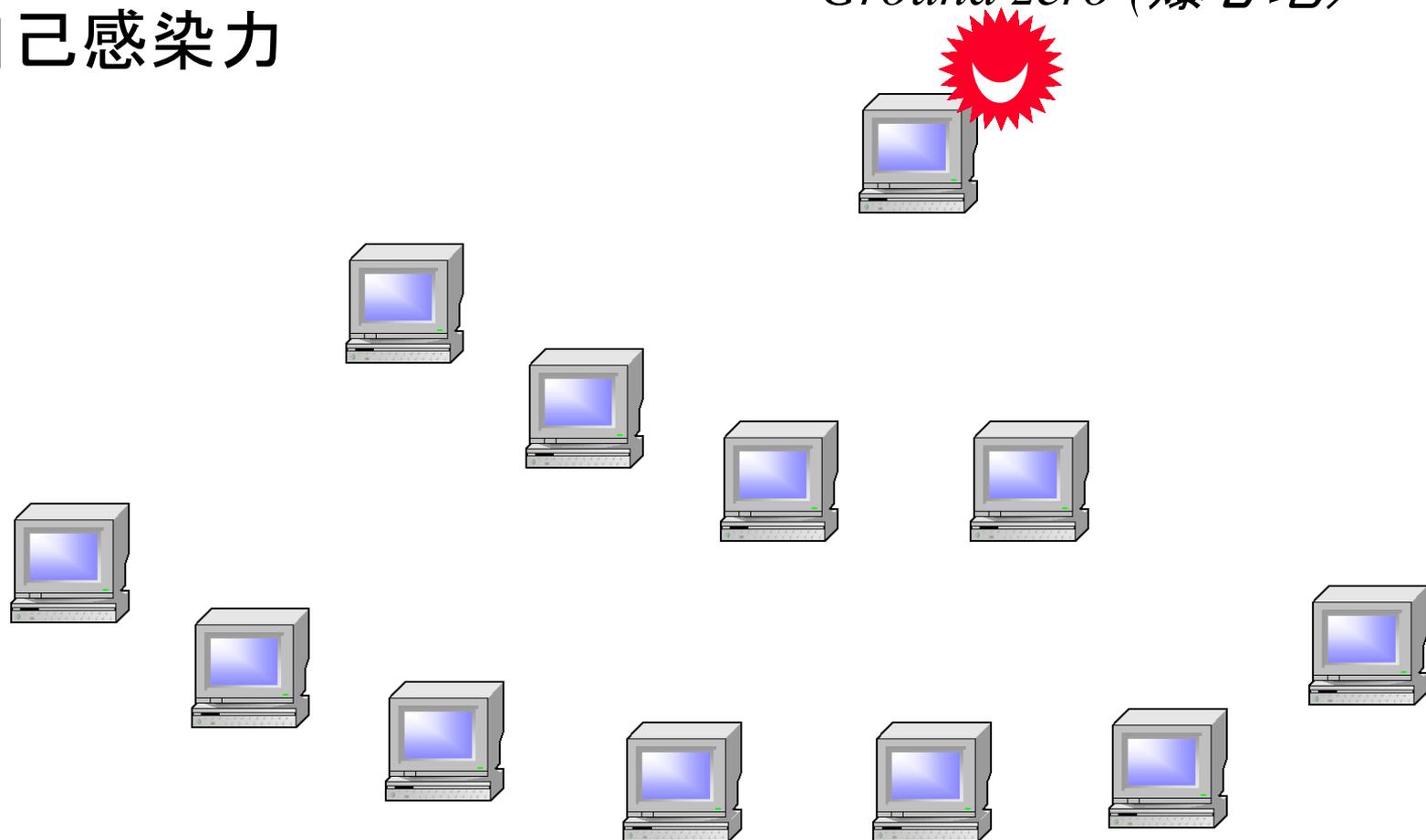
nmap 実行例

```
# 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

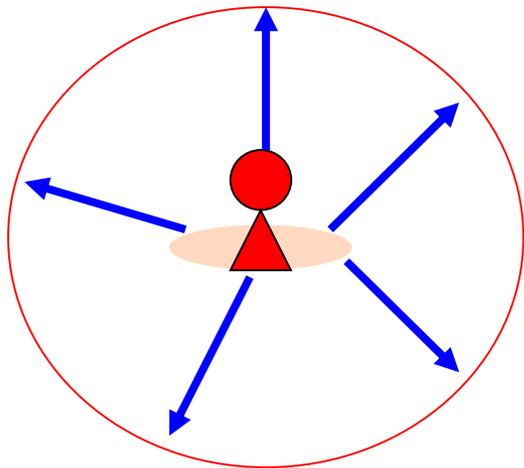
- 自己感染力

Ground zero (爆心地)



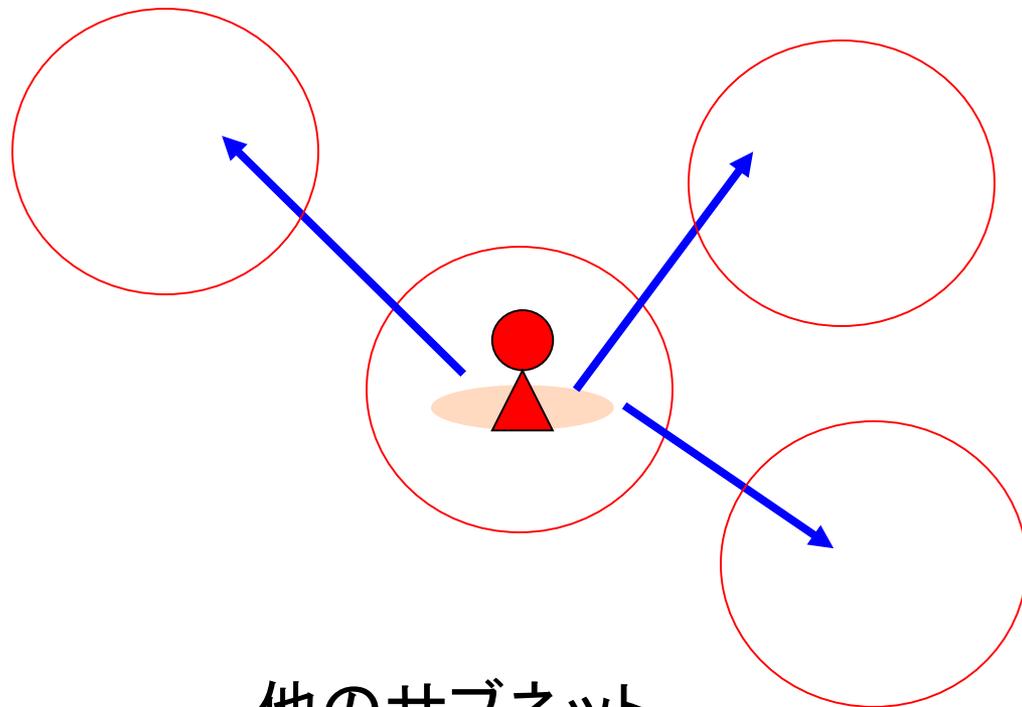
探索の戦略

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
 - 最初の本格的なワーム
 - 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>

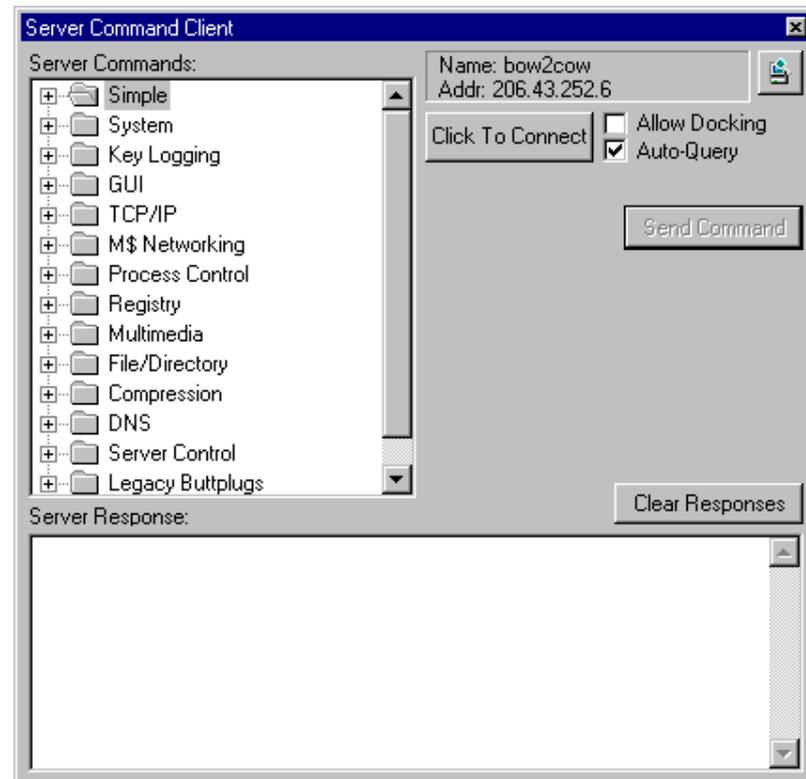
W32.Blaster.worm ローカル型

- 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)



2. バックドア（裏口）

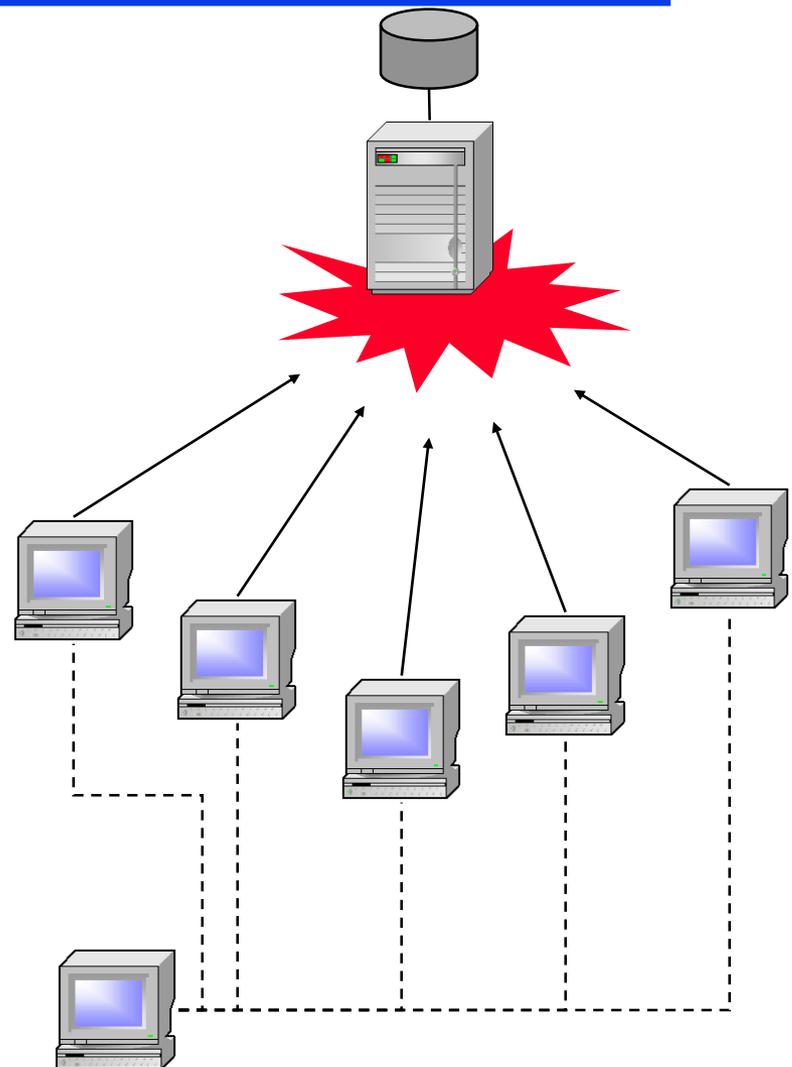
- Back Orifies (BO2k)
 - Win2000用遠隔操作
 - トロイの木馬
 - 攻撃先にインストール
 - 遠隔インストール, ネットワーク管理, リブート, DNS設定, プロセス制御, e.t.c.
 - 他のホストへの攻撃(踏み台)



3. ボットネット

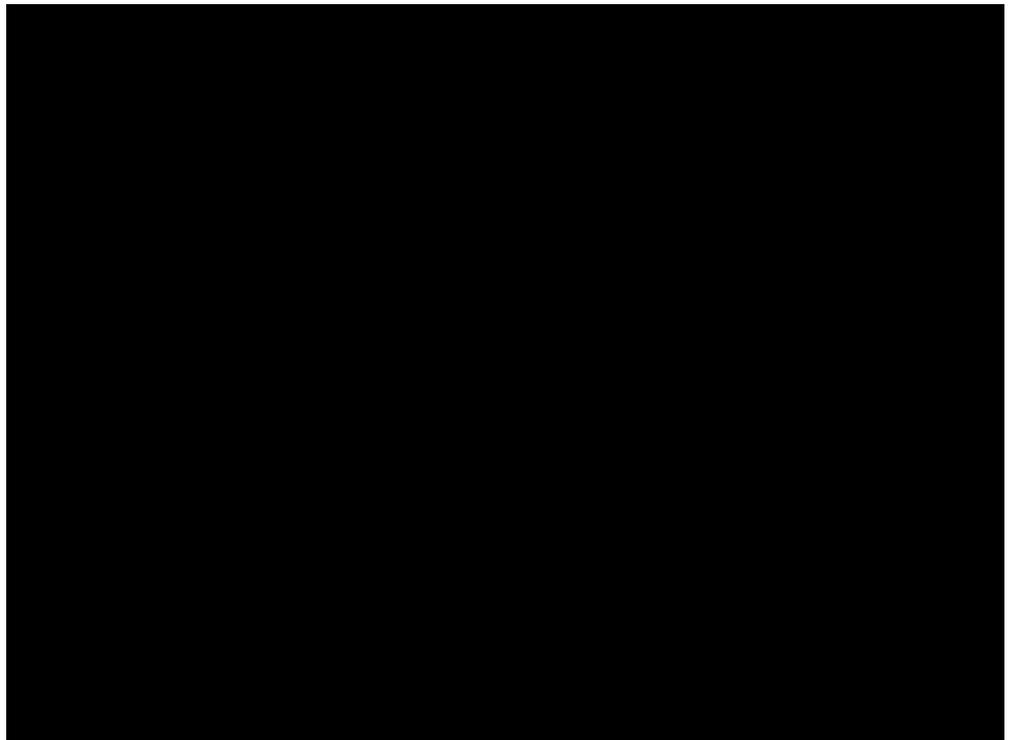
■ 新種ウイルス

- IRC制御のトロイの木馬型
- 「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)

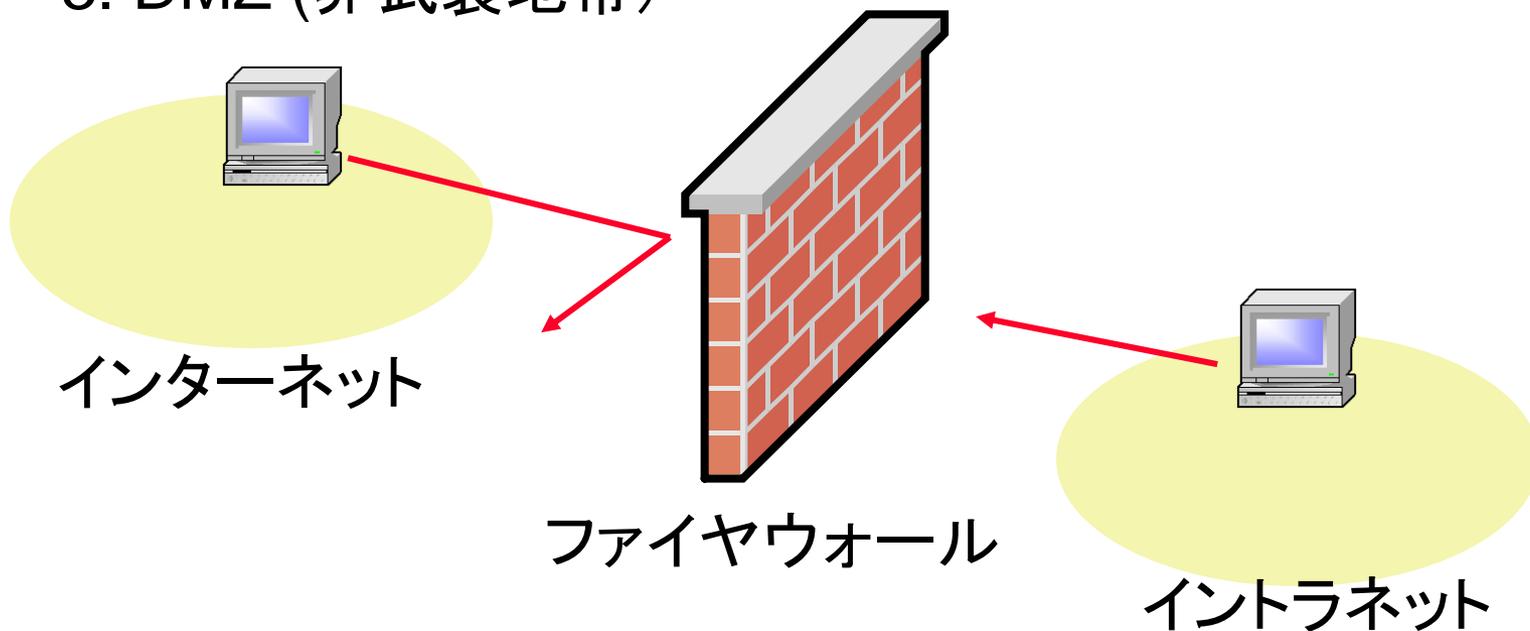


2. ファイアウォール

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)



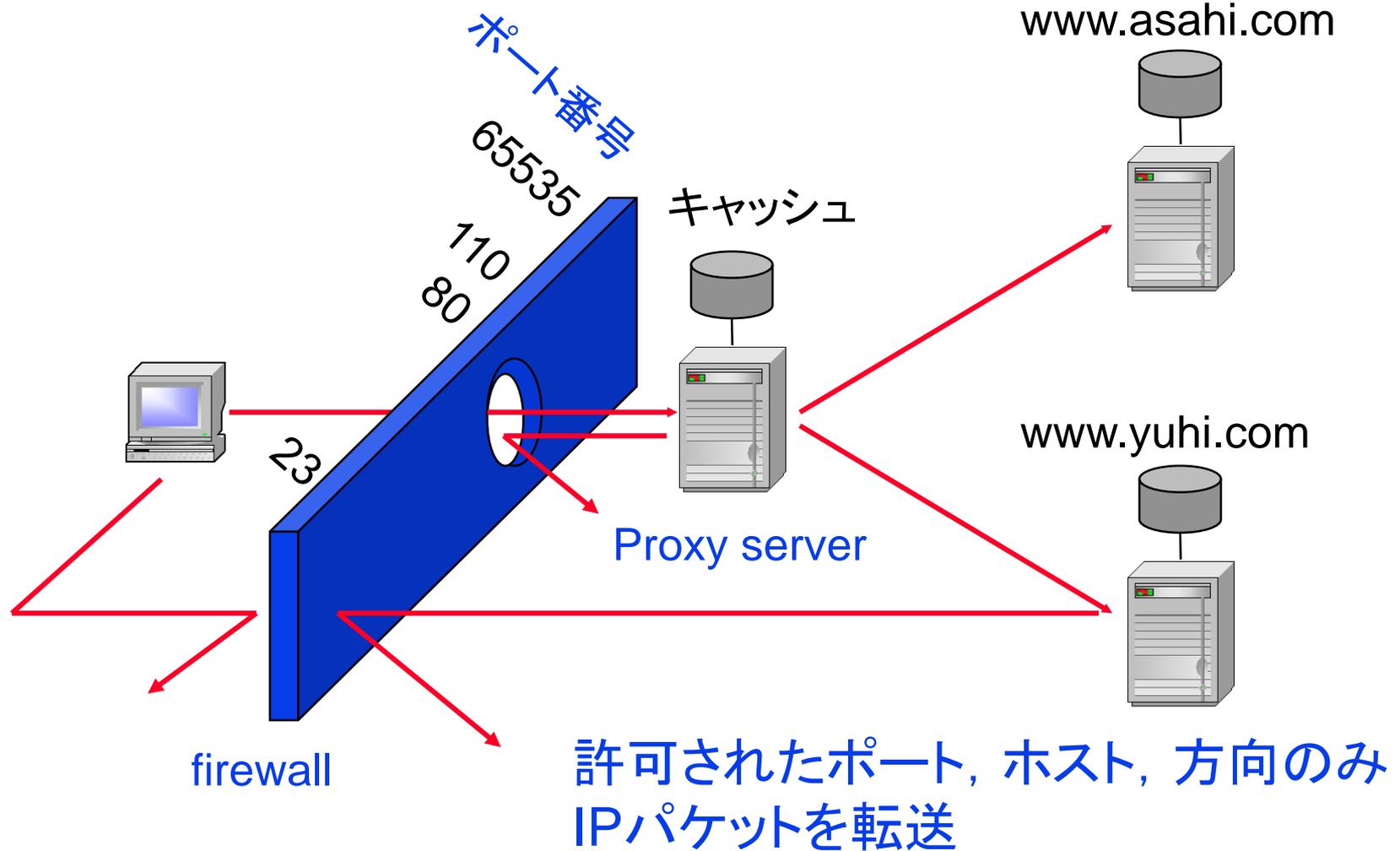
ファイヤウォール

- 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

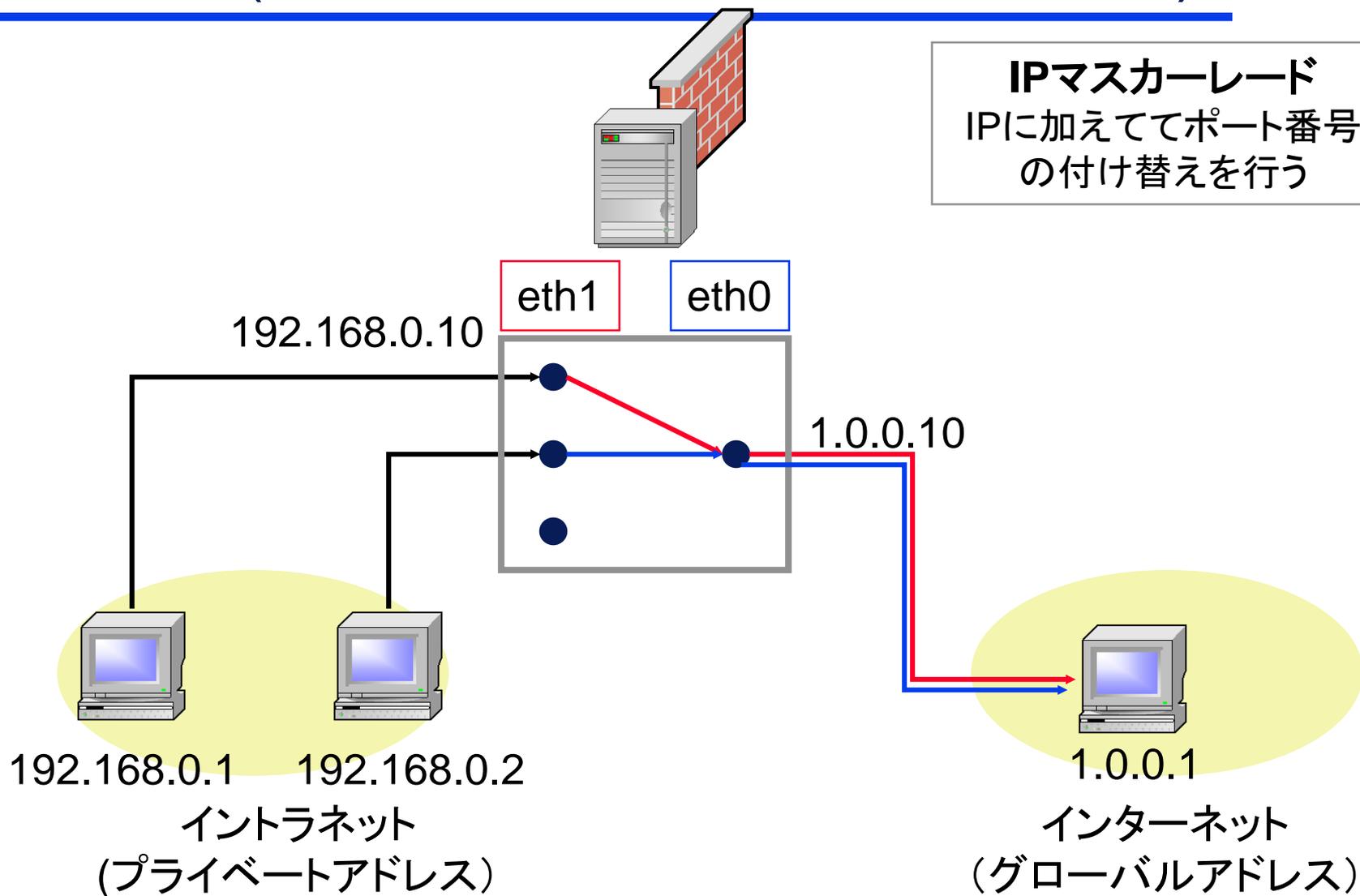
The screenshot shows the Japanese version of the Check Point website for FireWall-1. The browser title is "チェック・ポイント・ソフトウェア・テクノロジーズ: FireWall-1 - Microsoft Internet Explorer". The address bar shows "http://www.checkpoint.co.jp/products/". The page features the Check Point logo and the tagline "The World's Most Intelligent Security Solutions. We Secure the Internet." with navigation links for "Perimeter", "Internal", and "Web". A top navigation bar includes "TOP", "製品情報", "セキュリティ情報", "サービス", "イベント情報", "パートナー", "プレスリリース", "会社概要", and "MyAccount". The main content area is titled "FireWall-1" and "境界セキュリティ" (Boundary Security). It describes FireWall-1 as the industry's most effective firewall security, highlighting its use of INSPECT technology for high performance and flexibility. A sidebar on the left lists product categories like "Perimeter Security", "Internal Security", and "Web Security". A right sidebar contains a "CONTACT" section with links for "製品に関する問い合わせ" and "パートナー検索", and a "製品情報" section with links for "NGX 情報センター", "データシート [PDF]", "サポート・プラットフォーム", "チェック・ポイント Cisco /Juniper に勝つ [PDF]", and "サポートしているアプリケーション [英語版・PDF]".

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

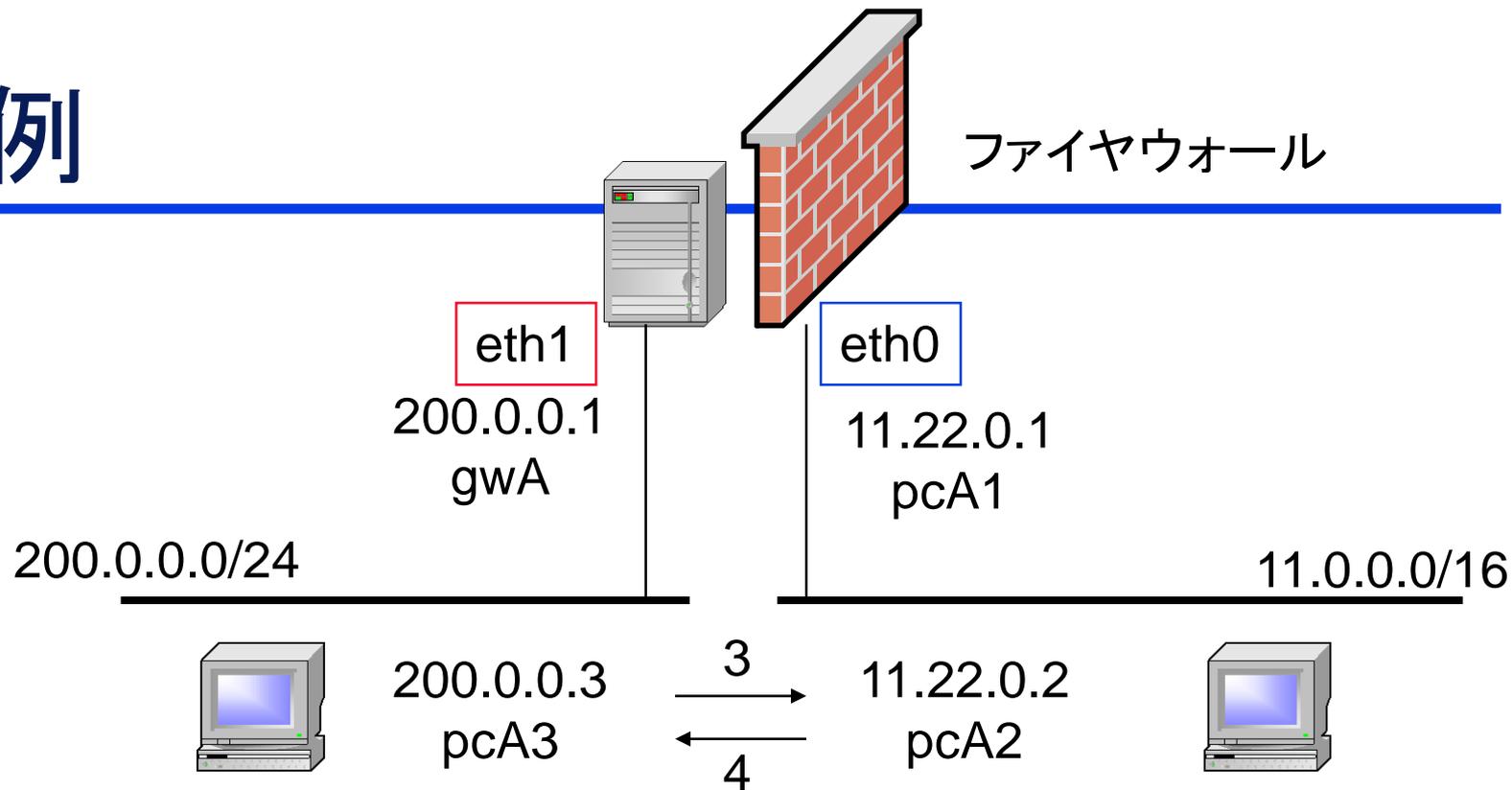
1. パケットフィルタリング



2. NAT(Network Address Translation)



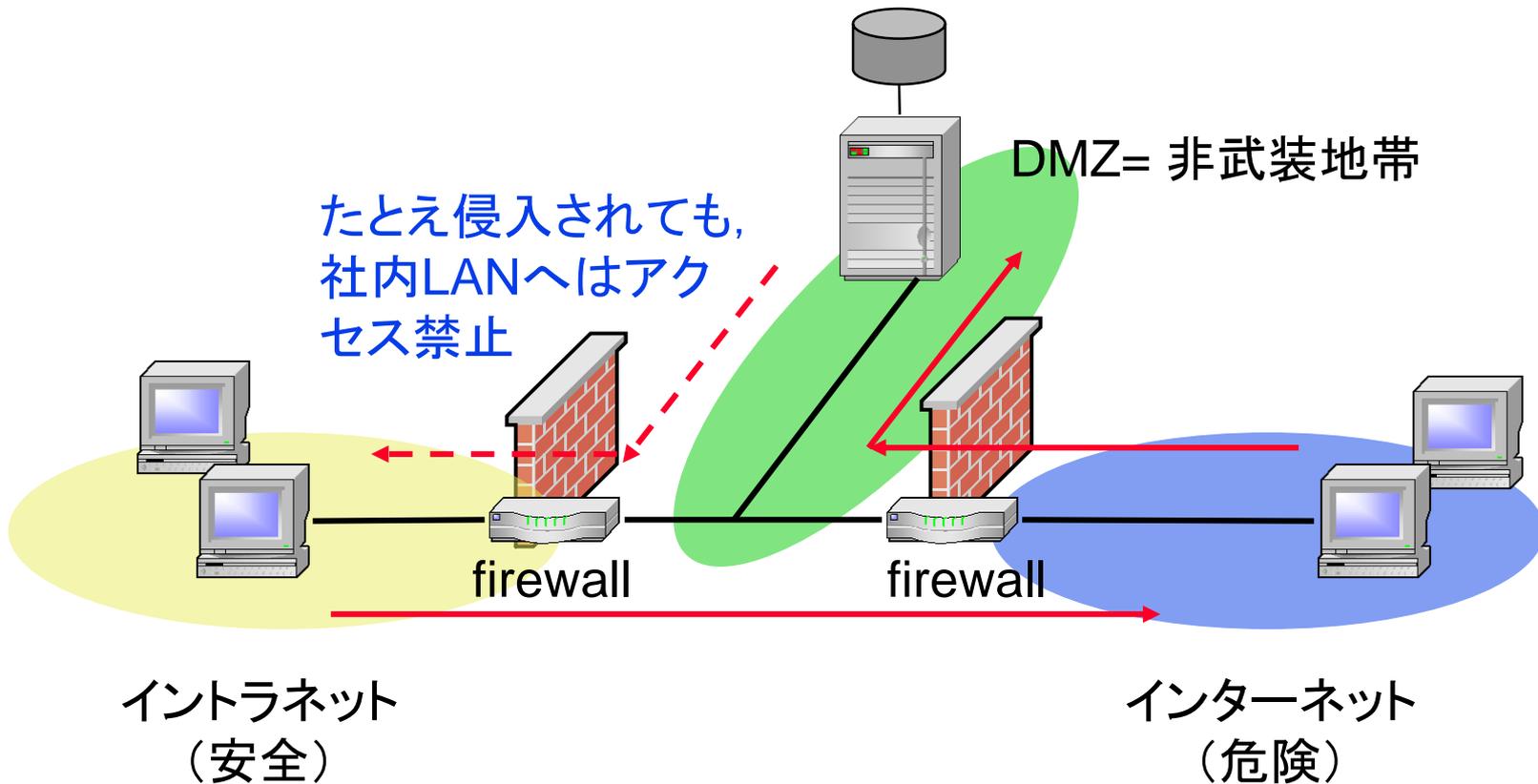
例



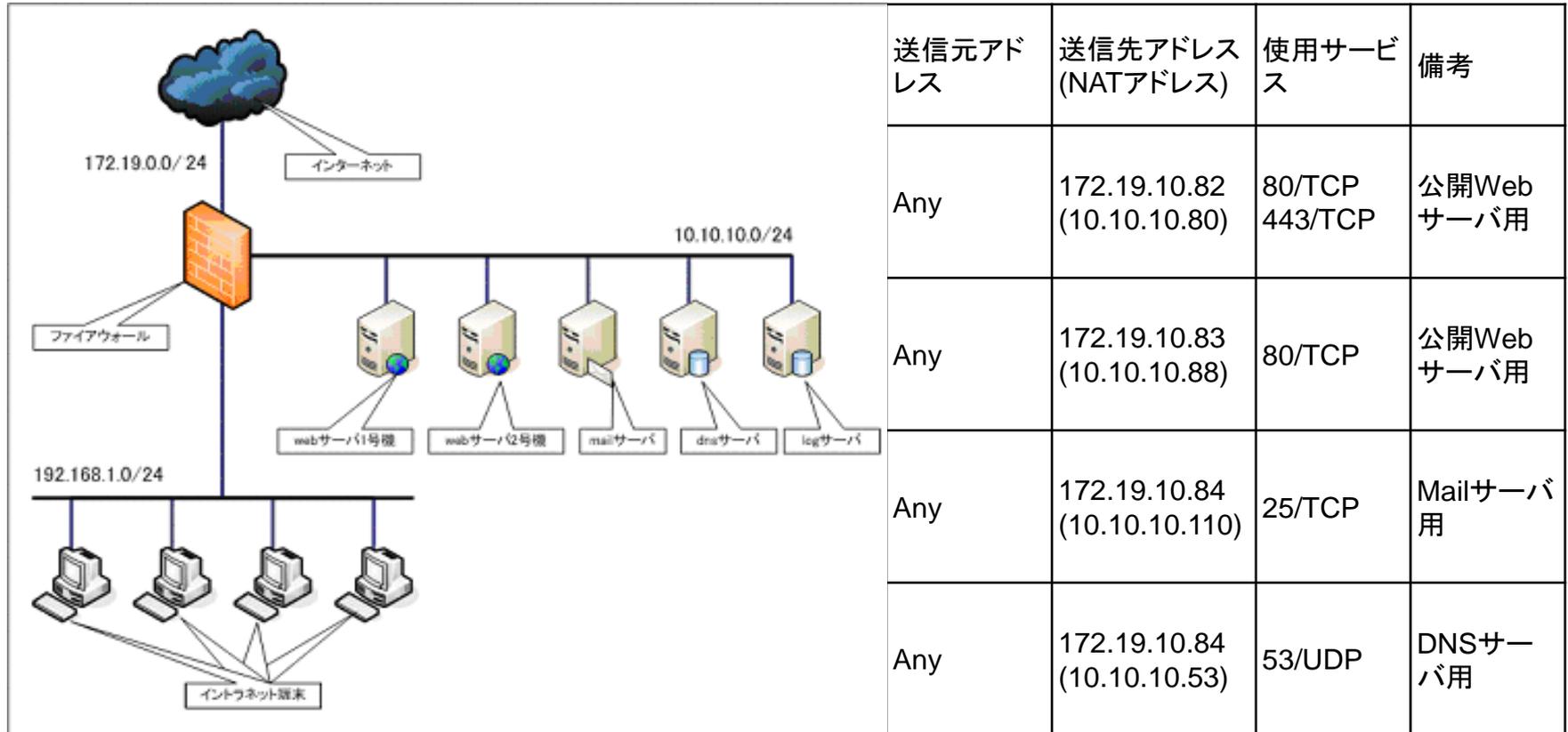
実行元	コマンド	pcA4 (内側) でのEthereal		pcA2 (外側) でのEthereal	
pcA3	ping pcA2	200.0.0.3	11.22.0.2	11.22.0.1	22.22.0.2

3. DMZ demilitarized zone

社外公開用ウェブサーバ



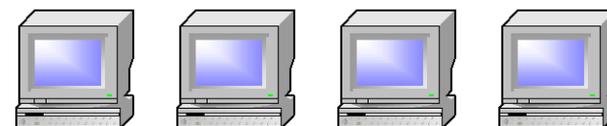
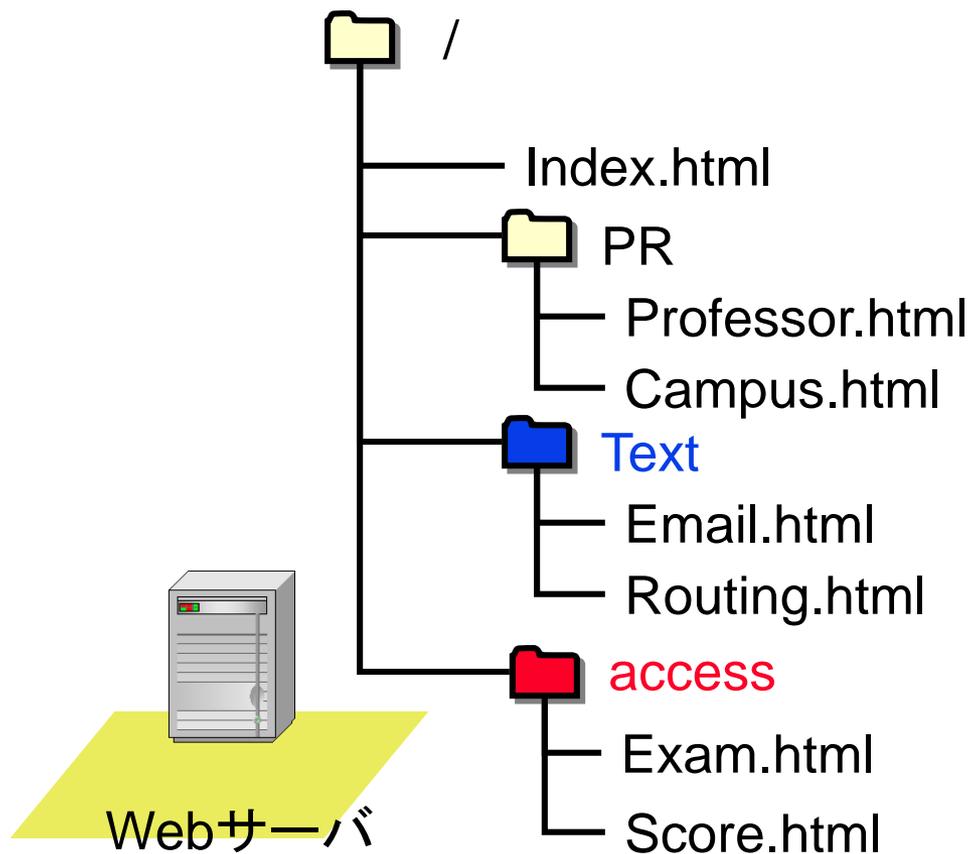
ポリシー設計の例 (Internet→DMZ)



3. 経路制御とアクセス制御

アクセス制御の例

http://www.imedia.com



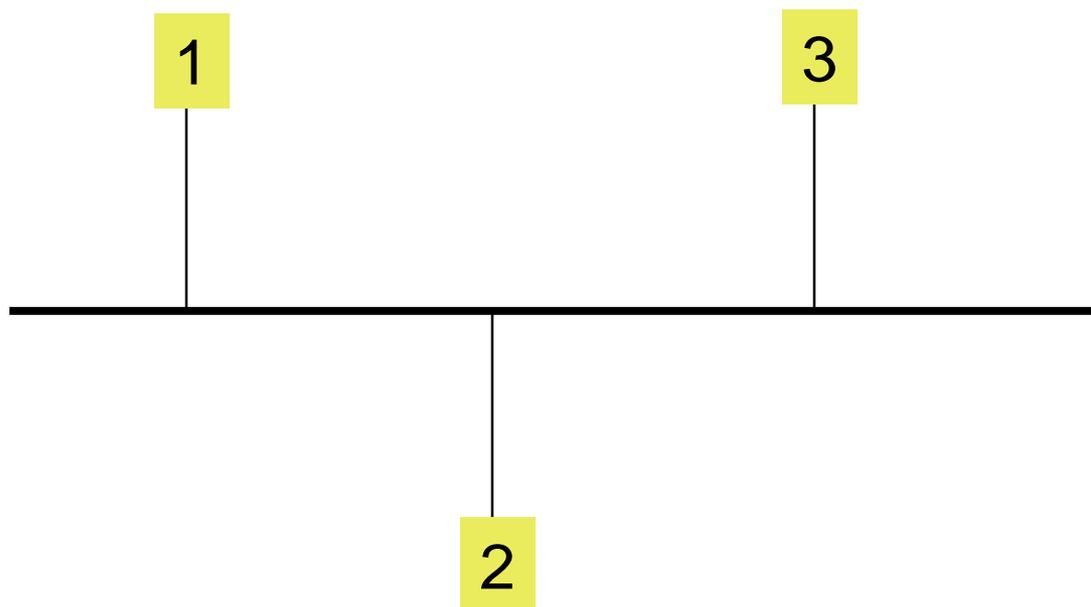
学外 学生 院生 教員

○	○	○	○
×	○	○	○
×	×	×	○

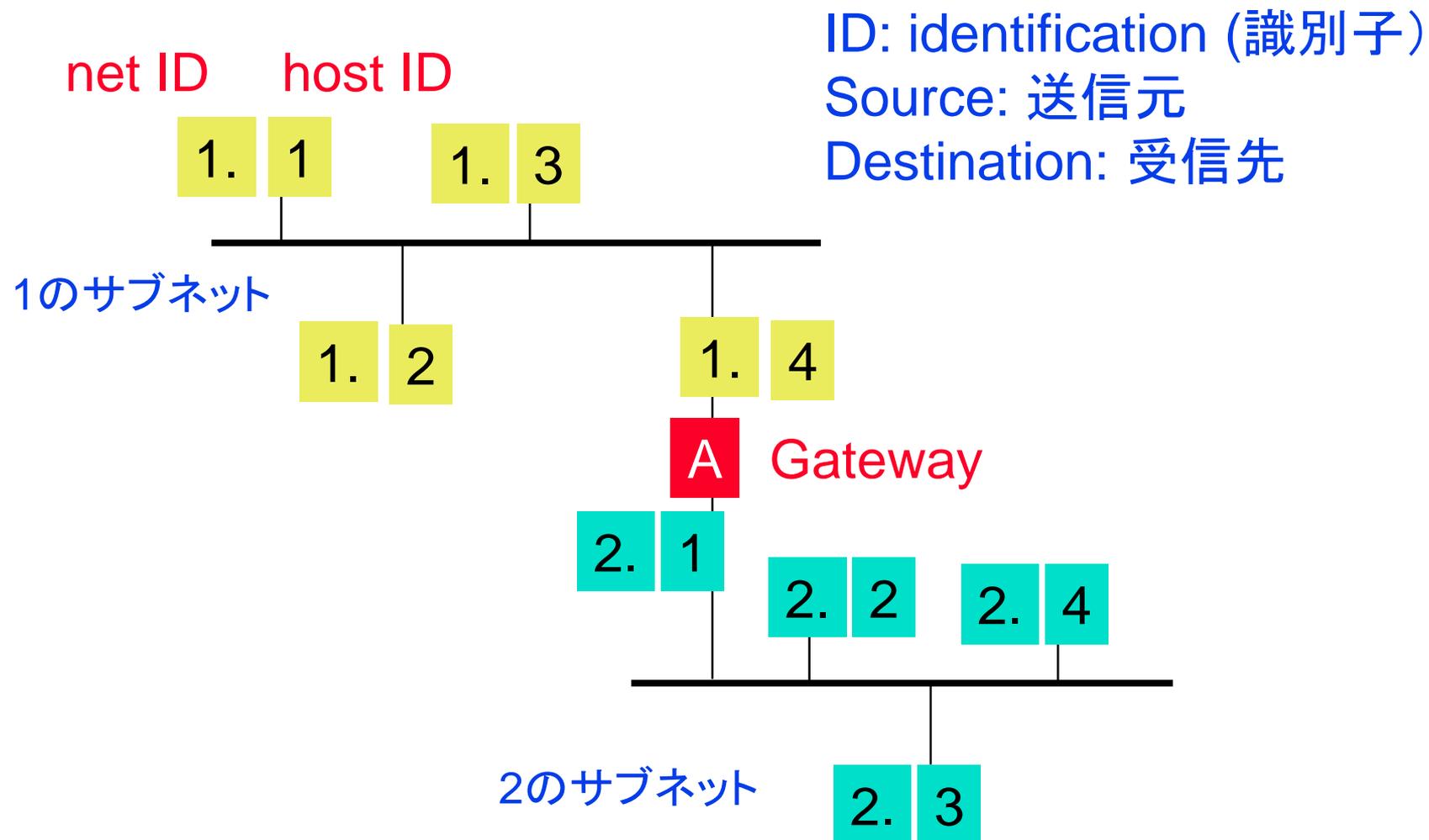
アクセス制御技術

- 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.

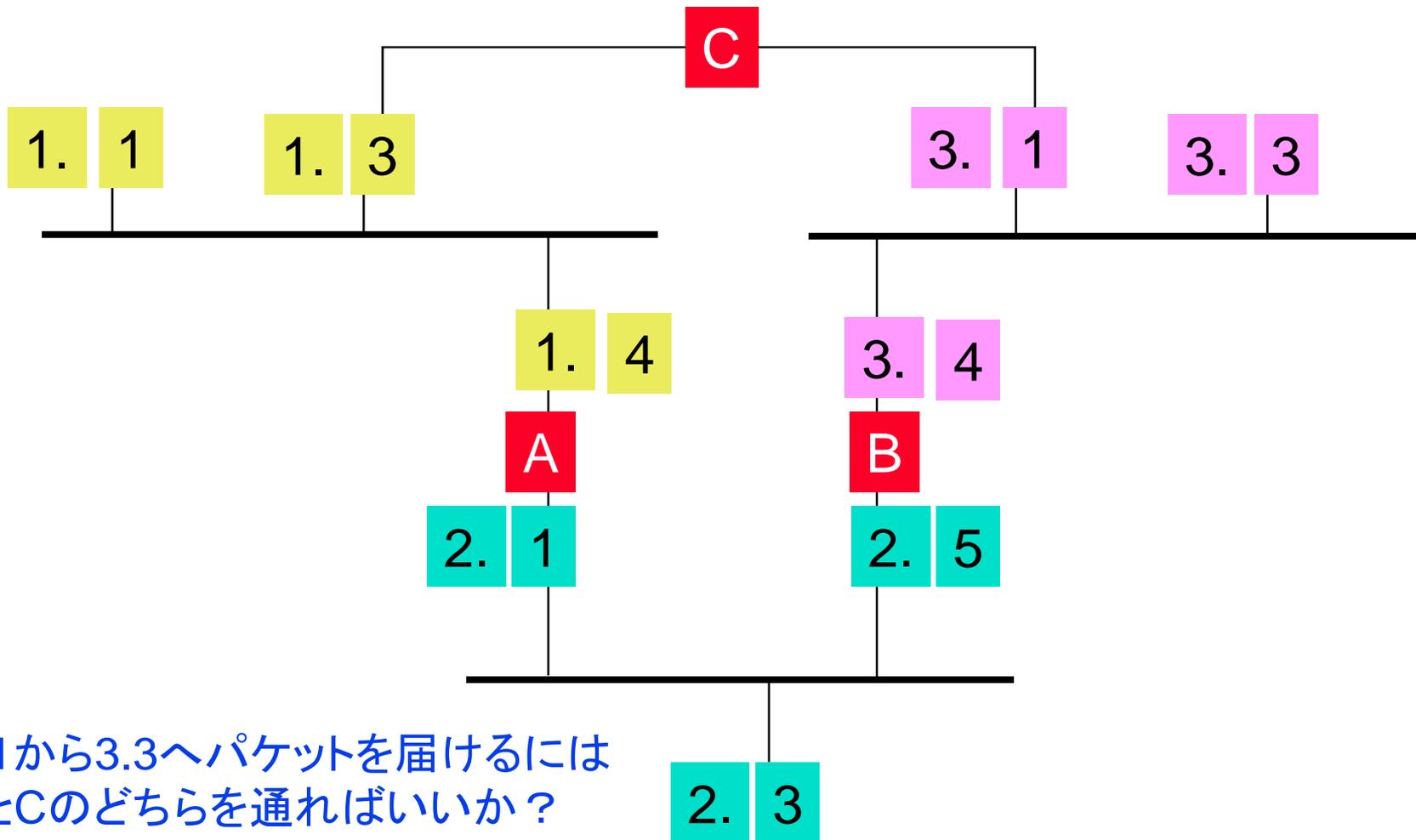
LAN



WAN



経路制御 routing (ルーティング)

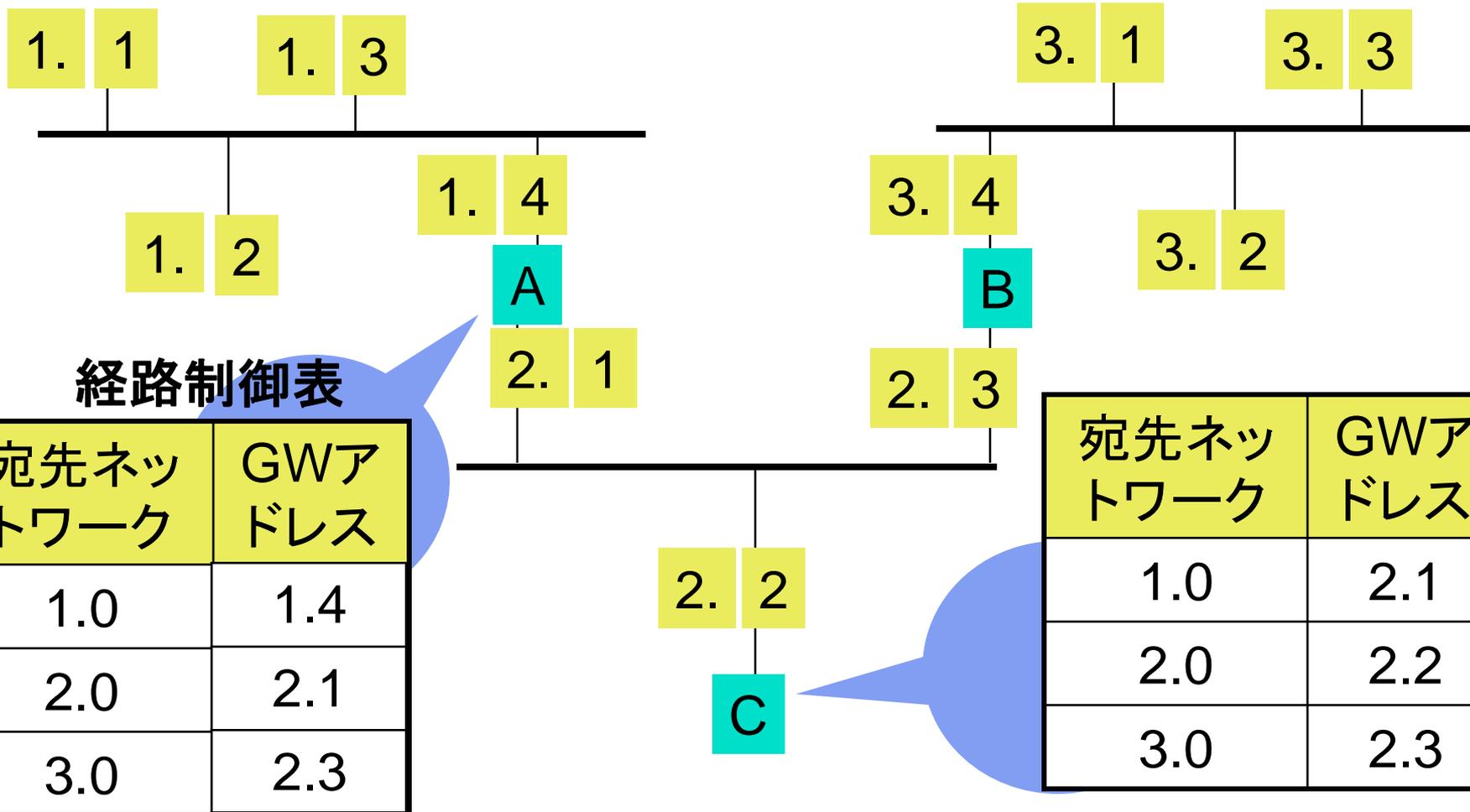


1.1から3.3へパケットを届けるには
AとCのどちらを通ればいいのか？

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

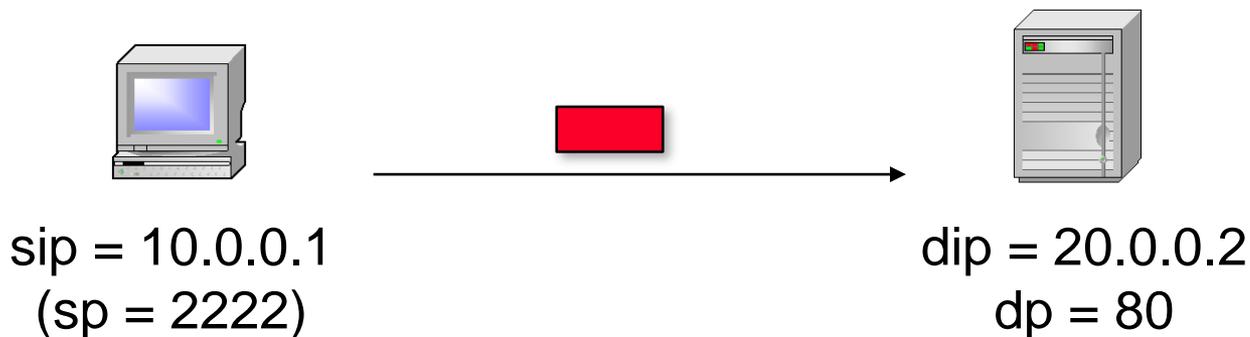
ダイナミックルーティング



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



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=

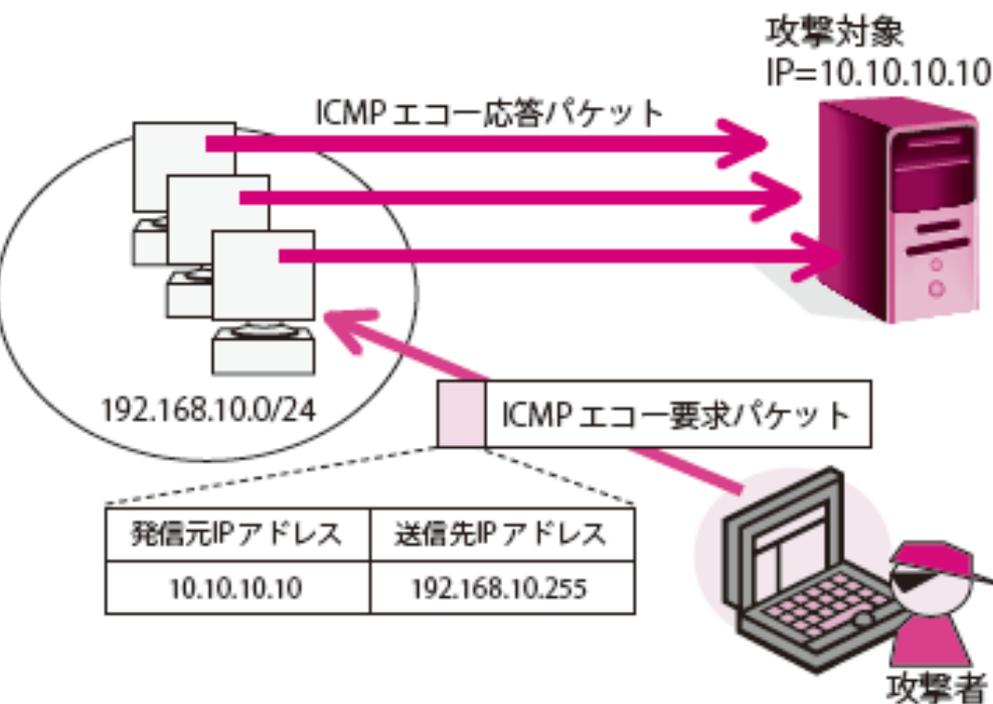
3. ルールの順序

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



- 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

ストリームとセグメント

■ ストリーム



■ セグメント



シーケンス番号 SEQ=4000



SEQ=4000

■ そこで、statefull (有限状態マシン)なフィルタリングの必要性

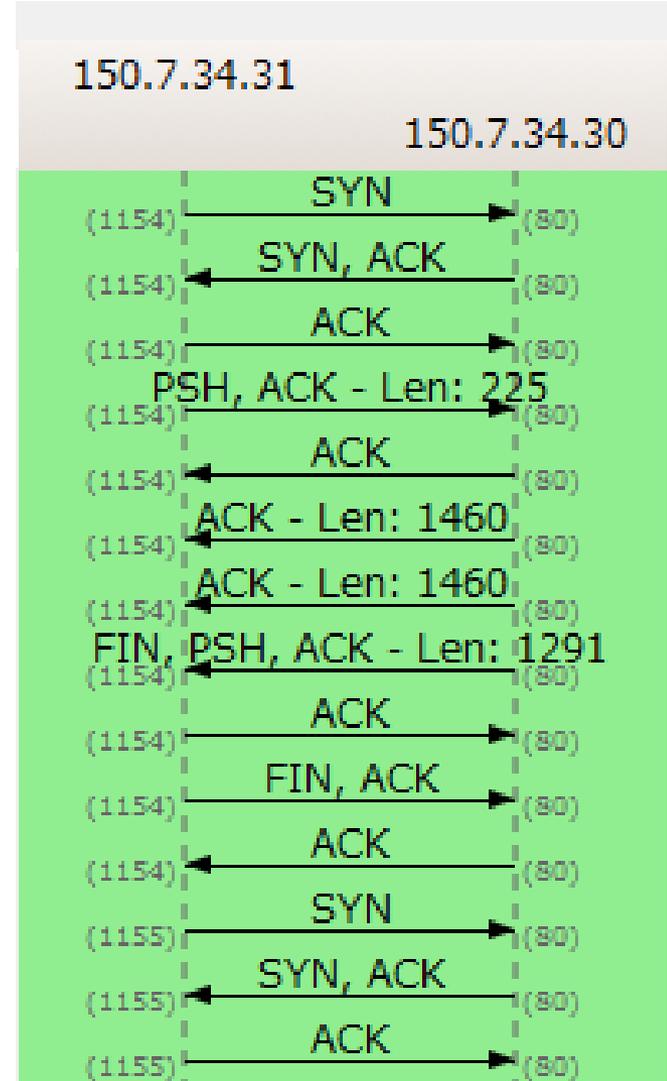
TCP stream の例 (HTTP)

Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8) showing a capture of an HTTP stream. The interface includes a menu bar, toolbar, filter field, and a packet list table. The packet list table shows 15 packets, including SYN, GET, and ACK messages. The packet details pane shows the structure of the first packet (Frame 1), including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields. The packet bytes pane shows the raw hex and ASCII data of the first packet.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	150.7.34.31	150.7.34.30	TCP	62	resacomunity > ht
2	0.000061	150.7.34.30	150.7.34.31	TCP	62	http > resacomuni
3	0.000136	150.7.34.31	150.7.34.30	TCP	60	resacomunity > ht
4	0.000486	150.7.34.31	150.7.34.30	HTTP	279	GET /http.html HTT
5	0.000540	150.7.34.30	150.7.34.31	TCP	60	http > resacomuni
6	0.001124	150.7.34.30	150.7.34.31	TCP	1514	[TCP segment of a
7	0.001249	150.7.34.30	150.7.34.31	TCP	1514	[TCP segment of a
8	0.001356	150.7.34.30	150.7.34.31	HTTP	1345	HTTP/1.1 200 OK (
9	0.002471	150.7.34.31	150.7.34.30	TCP	60	resacomunity > ht
10	0.004905	150.7.34.31	150.7.34.30	TCP	60	resacomunity > ht
11	0.004942	150.7.34.30	150.7.34.31	TCP	60	http > resacomuni
12	0.012169	150.7.34.31	150.7.34.30	TCP	62	nfa > http [SYN] S
13	0.012217	150.7.34.30	150.7.34.31	TCP	62	http > nfa [SYN, A
14	0.012289	150.7.34.31	150.7.34.30	TCP	60	nfa > http [ACK] S
15	0.012656	150.7.34.31	150.7.34.30	HTTP	331	GET /link6_files/o

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
Ethernet II, Src: Nec_1e:dd:c3 (00:00:4c:1e:dd:c3), Dst: DellComp_aa:d2:10 (00:b0:d0:aa:d2:10)
Internet Protocol Version 4, Src: 150.7.34.31 (150.7.34.31), Dst: 150.7.34.30 (150.7.34.30)
Transmission Control Protocol, Src Port: resacomunity (1154), Dst Port: http (80), Seq: 0,

```
0000 00 b0 d0 aa d2 10 00 00 4c 1e dd c3 08 00 45 00  ....L....E.  
0010 00 30 09 39 40 00 80 06 81 43 96 07 22 1f 96 07  .0.9@...C..."  
0020 22 1e 04 82 00 50 da 74 32 9d 00 00 00 00 70 02  "....P.t 2.....p.  
0030 40 00 c0 ef 00 00 02 04 05 b4 01 01 04 02      @.....
```



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、パケットフィルタリングと()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