コンピュータ科学実験第1
ソフトウェア実験

第2週説明資料

重要な注意事項

- 課題5　lynx による https 接続の確認時，
  自己署名証明書の確認でエラーとなるが，
  machine3 側からと ICE 側からで挙動が異なる

SSLエラー: ホスト～が cert(CN～)と一致しません
続けますか？（y）と　続けますか？（n）

⇒　デフォルト値が異なるが，必ず y を入力
　　何も考えずに Enter では終了する！

重要な注意事項 (2)

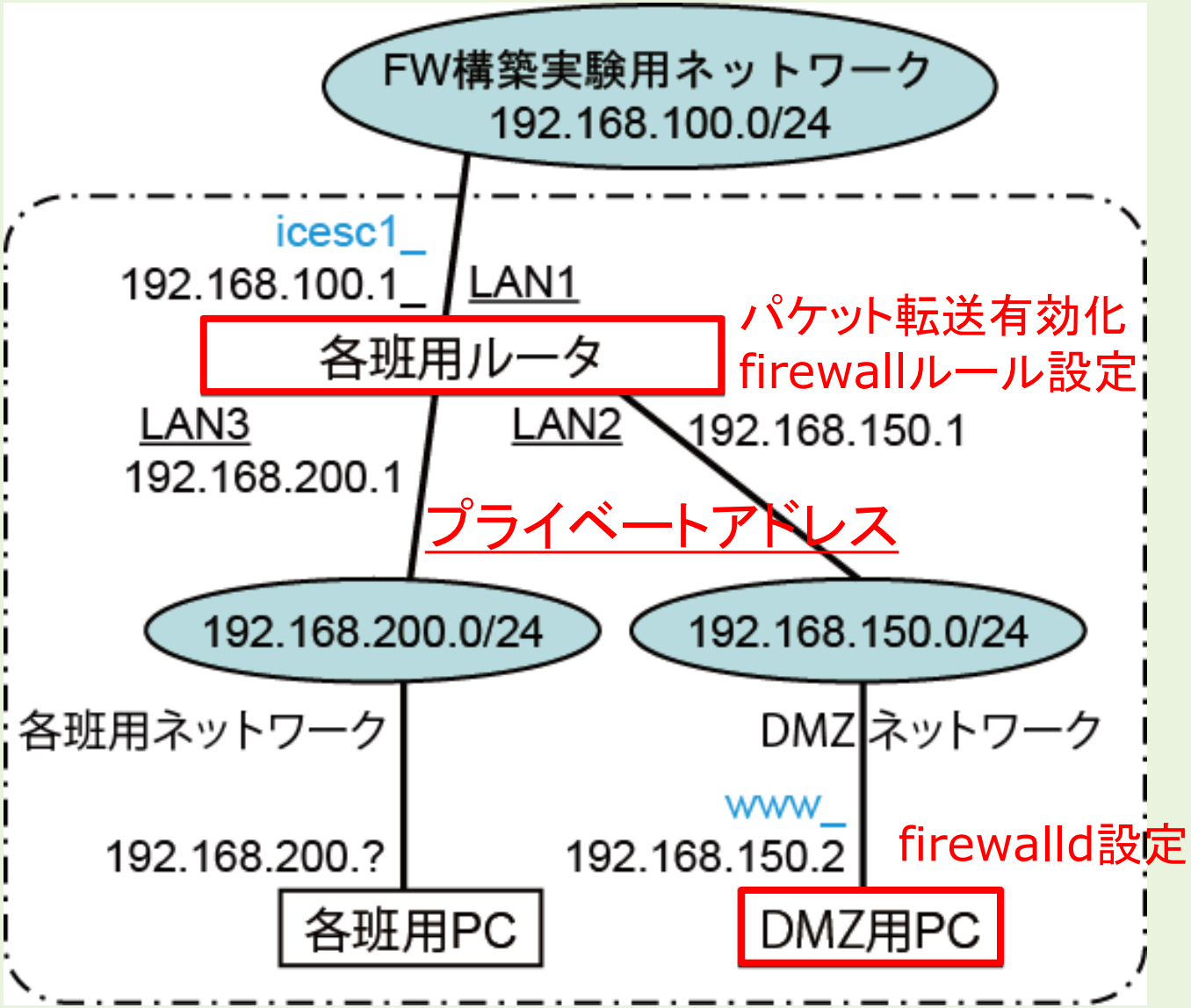
- 課題5の4 設定ファイル ssl.conf の修正
  （指導書 P.78）
  既存の ssl.conf の該当する3行のみを修正

```
SSLProtocol +TLSv1.2
SSLCertificateFile /etc/pki/tls/certs/server.crt
SSLCertificateKeyFile /etc/pki/tls/certs/server.key
```

  他の行は修正する必要がないので注意！

- machine2, machine3 は DNS に未登録
  IPアドレスを利用

課題4の目的（ルータとWEBサーバのfirewallを設定）



OSI 参照モデル（指導書第2章 P.2～）

			具体例
第7層	アプリケーション層	どのような通信サービスを行い，何を実現するか？	HTTP, SMTP
第6層	プレゼンテーション層	どのような表現形式で送るか？	HTTP, SMTP
第5層	セッション層	どのような対話モードで送るか？	
第4層	トランスポート層	相手に正確に届いたかどうかの確認方法は？	TCP, UDP
第3層	ネットワーク層	相手の識別アドレスは？ 通信網をどう使うのか？	IP, ARP, ICMP
第2層	データリンク層	伝送路の確保と端末の識別方法は？	イーサネット
第1層	物理層	伝送路に情報を送る媒体，方法は？	

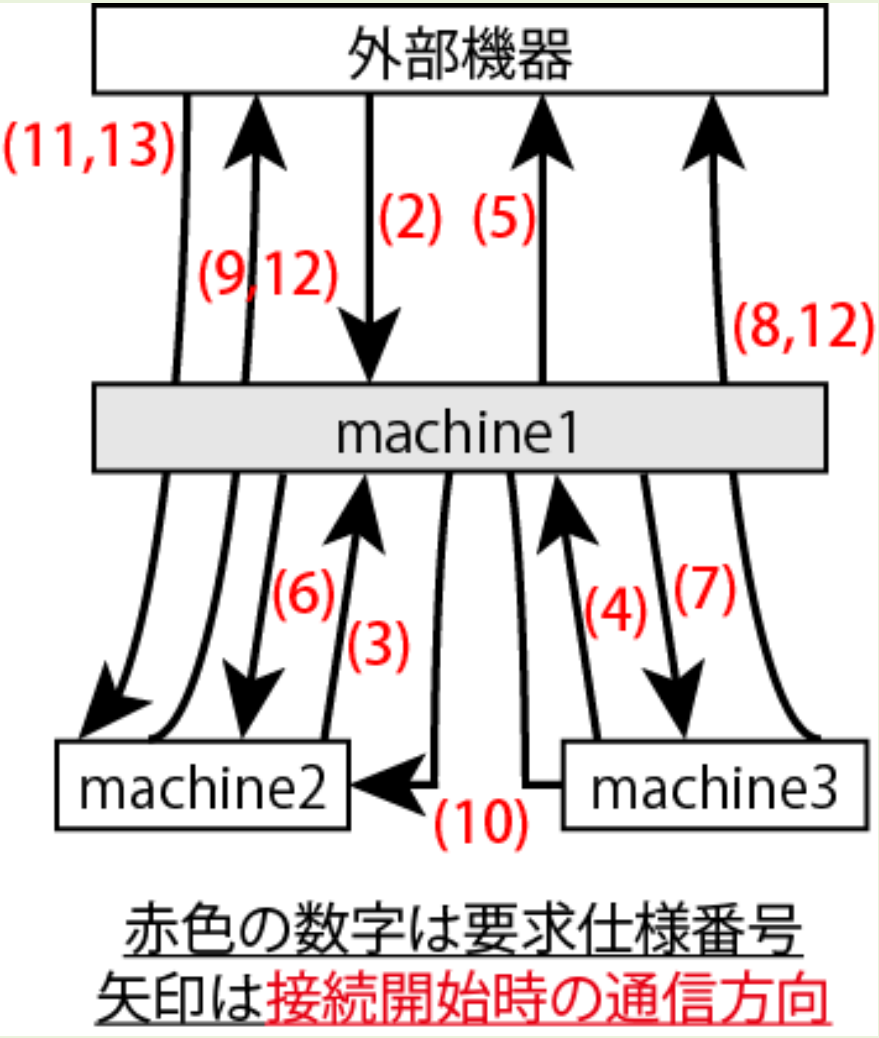
クライアントサーバ方式における通信の特徴

- クライアント側から通信を開始
- サーバ側のポート番号・プロトコルは既知
- クライアント側のポート番号は未定

サービス内容＝TCP, IPパケットヘッダで判断可能
IPアドレス，ポート番号，TCP/UDP/ICMP

firewall（での許可・拒否）はクライアント側からの
最初のパケットを適切に許可・拒否すれば良い
（引き続くパケットは許可で良い）

課題4の内容 (1)（P.71～, P.80～）



machine1 要求仕様

1～8, 10 は設定済み

通信は双方向を考慮

課題4の内容 (2)

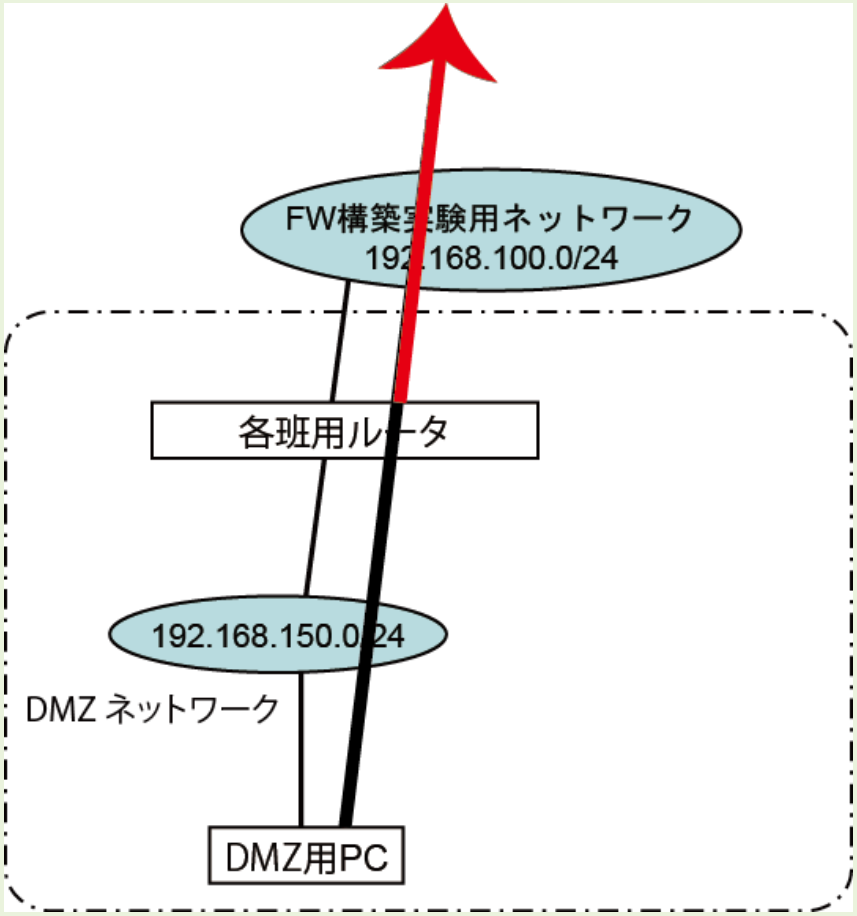
- 課題4 ファイアウォール構築 (iptables,firewalld)

  machine1 仕様の 1, 2～8, 10 はサンプルに実装済
  目的: FORWARD 9, 11 と NAT 12, 13 を設定する
  手順: 各仕様単位で, プロトコル単位で実装・動作確認

  1. 実装済み部分の動作確認
  2. 仕様 9, 12 SNAT (DMZ⇒外部)を実装・動作確認
     仕様 8, 12 SNAT (ローカル⇒外部) を参考
  3. 仕様 11 外部⇒DMZ, DNAT 13 を実装
     確認は課題5 WWWサーバ起動後
  4. machine2 は手順に従い, firewalld を設定する

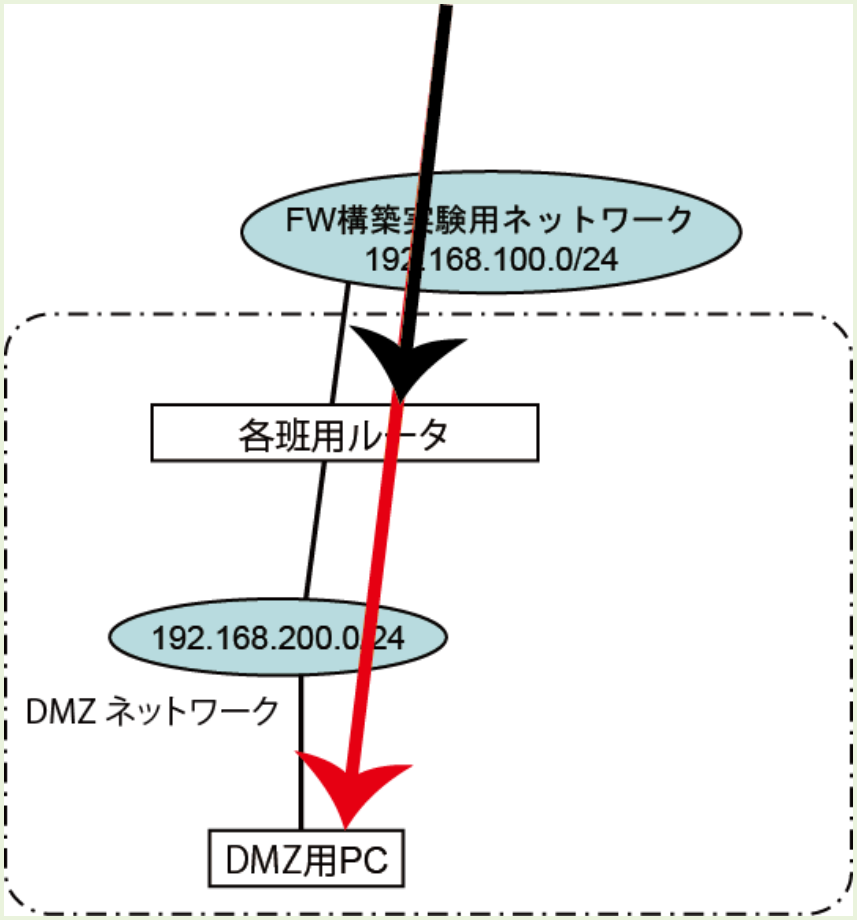
サンプルは設定のリセット用に保存しておくこと

SNAT (POSTROUTING)



外部ネットワークへの通信時に，
source をルータに変更
⇒ 戻りパケットはルータへ
⇒ ルータから各PCへ

DNAT (PREROUTING)



外部ネットワークからルータへの通信時に,

destination を変更

⇒ 外部からはルータがサーバ

課題4の内容 (3)

- firewall 設定の確認方法
  - ① DNS ⇒ host, dig, nslookup コマンド
  - ② SSH ⇒ ssh コマンド
  - ③ ping ⇒ ping コマンド（終了は Ctrl+C）
  - ④ http/https ⇒ lynx（CLI ブラウザ，終了は q）
    外部側からの確認は，端末からfirefoxでも可
    lynx の場合はサーバ証明書内容確認は諦める
- ICE WEB サーバは，http のみ
  https は情報学研究科の WEB サーバ
- 外部側からの確認は，
  接続テスト用PC icexs2 や ICE の機器を利用

課題5の内容

- 課題5 WWW サービスの設定
  1. Apache WWW サーバのインストール
  2. TLS 自己署名証明書の作成
     指導書 P.44～49 TLS の仕組みを理解
     - ① 秘密鍵の作成
     - ② CSR の作成(CSR 作成のための情報入力)
     - ③ 自分の秘密鍵で署名し，サーバ証明書の作成
  3. WWW サーバの設定と起動確認
     (lynx では証明書の内容は確認できない)

初回レポートについて

- 課題1～5（課題1～5で1ファイル）
  調査課題1～5（各1ページ以上，1～5で1ファイル）
- 実験結果：script の出力 ⇒ 必要な部分を編集
- 手順や結果は文章で説明
- iptables ファイル全文を添付しないこと
  今回作成した仕様に関係する部分のみ記載
- 注意事項 指導書 P.81～
- 今年度は成績〆切が厳密なため遅れないように

課題6

- HTML, CSS, SQL 等の知識が必要（⇒予習）
  指導書 P.87～ にサンプル sample.wsgi
- 各個人で WEB アプリケションを作成
- 課題5のWEBサーバが無くても,
  python のWEBサーバで実行可能
  指導書 P.88 参照