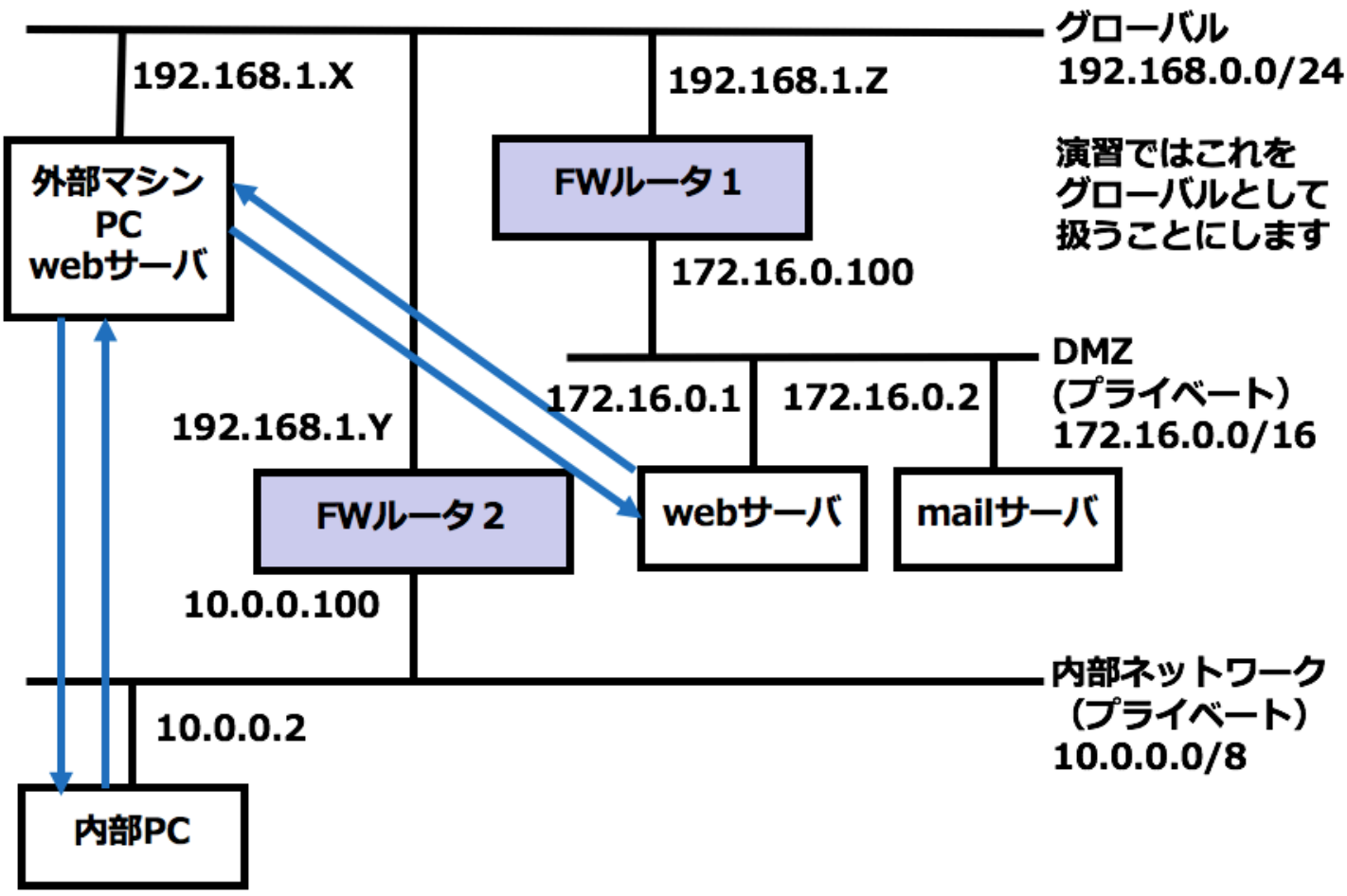
ネットワークセキュリティ演習

5回 ファイアーウォールの構築

演習レポートのURL

https://goo.gl/forms/rnpJEPoJpdnWWI8o2“

ネットワークの構成



前回の授業の影響を消す

確認

- gufwの影響を消す

```
gufw
```

gufwの画面でオフにする

- iptabelsの影響を消す

```
sudo iptables -L
```

ルールの削除とユーザチェーンの消去

```
sudo iptables -F
sudo iptables -X

sudo -t nat iptables -F
sudo -t nar iptables -X
```

確認

```
sudo iptables -L

udo iptables -t nat -L
```

各班で、マシンの役割決定とIPアドレスの設定

- 外部マシン
- FWルータ１
- FWルータ２
- webサーバ
- mailサーバ
- 内部PC

USB Ethernetの配布

ルータにそれぞれ USB Ethernet を１個ずつ接続する

- FWルータ１
- FWルータ２

USB Ethernetは、プライベート側のネットワークとする

それぞれUSB Ethernet にIPアドレスを設定する

デフォルトゲートウェイの設定に注意する！

デフォルトゲートウェイは、グローバル側NICのIPアドレスになる

ハブの配布と接続

ハブに名前をつける

- グローバル
- DMZ
- 内部ネットワーク

Linux PCをLANケーブルでハブと接続してネットワーク構成図のとおりのネットワーク構成にする

グローバルネットワークに接続されているマシンについては、インターネット接続を確認する

- 外部マシン
- FWルータ１
- FWルータ２

webサーバのセットアップ

apache2のインストールの確認

- 外部マシン
- webサーバ

について確認する

確認内容：ローカルでのブラウザからページが見えること

mail サーバのセットアップ

postfixのインストール

```
sudo apt install postfix
```

画面が出たら「インターネットサイト」を選択

mailコマンドのインストール

```
sudo apt install bsd-mailx
```

mailコマンドの確認

mail コマンドでメールを出してみる

```
mail kindai@localhost
Subject: test
test mail
.
Cc:
```

mailコマンドでメールを受信する

```
mail

Mail version 8.1.2 01/15/2001.  Type ? for help.
"/var/mail/hogeuser": 1 message 1 new
>N  1 hogeuser@sample.com   Fri Mar 24 12:32   14/429   test
& 1
Message 1:
From hogeuser@sample.com  Fri Mar 24 12:32:48 2017
X-Original-To: hogeuser@localhost
To: hogeuser@localhost
Subject: test
Date: Fri, 24 Mar 2017 12:32:48 +0900 (JST)
From: hogeuser@sample.com (hogeuser)

test mail

& q
Saved 1 message in /home/hogeuser/mbox
```

FWルータ１の設定

NICのインターフェース名を確認

```
ip addr
```

インターフェース名を記録する

- グローバル側　　「　　」
- プライベート側　「　　」

IPアドレスを記録する

- グローバル側　「　　」
- プライベート側　「　　」

DNATの設定

```
sudo iptables -t nat -A PREROUTING -d <グローバル側IPアドレス> -p tcp --dport 80 -j DNAT

sudo iptables -t nat -A PREROUTING -d <グローバル側IPアドレス>  -p tcp --dport 25 -j DNA
```

SNATの設定

```
sudo iptables -t nat -A POSTROUTING -o <グローバル側インターフェース名> -s <グローバル側IP
```

FWルータ１のapache2 を停止

```
sudo service apache2 stop
```

DMZのwebサーバの再確認

- webサーバマシンのindex.htmlファイルを修正する

```
sudo mv /var/www/html/index.html /var/www/html/index.html.org

sudo nano /var/www/html/index.html
```

```
<html>
<head></head>
<body>
<h1>__班DMZのwebサーバ
</body>
</html>
```

確認内容：ローカルでのブラウザからページが見えること

DNATの設定の確認

外部PCからDMZのwebサーバにアクセスする

URLをFWルータ１のIPアドレスにして、ページが見えれば成功

FWルータ２の設定

NICのインターフェース名を確認

```
ip addr
```

インターフェース名を記録する

- グローバル側　「　　」
- プライベート側　「　　」

IPアドレスを記録する

- グローバル側　「　　」
- プライベート側　「　　」

IP MASQUERADE の設定

```
sudo iptables -t nat -A POSTROUTING -o <グローバル側NIC名>
-j MASQUERADE
```

追加

FWルータ 1 にもIP MASQUERADEを設定

```
sudo iptables -t nat -A POSTROUTING -o <グローバル側NIC名>
-j MASQUERADE
```

演習レポートのURL

https://goo.gl/forms/rnpJEPoJpdnWWI8o2