オープンソースで始める「超」VPN 構築術 ～SUSE でセキュリティのお勉強～

はしもとまさ＠日本openSUSEユーザ会

In OpenSourceConference 2013 Kyoto

自己紹介

- 愛知県大府市在住。
- 日本openSUSEユーザ会の自称営業担当。
- 以前は名古屋某社のVPNルーターの開発に携わっていたり。（そんな会社あったっけ？）
- …実は文系出身のエンジニアです。。。

それでは気分を取り直して。。。

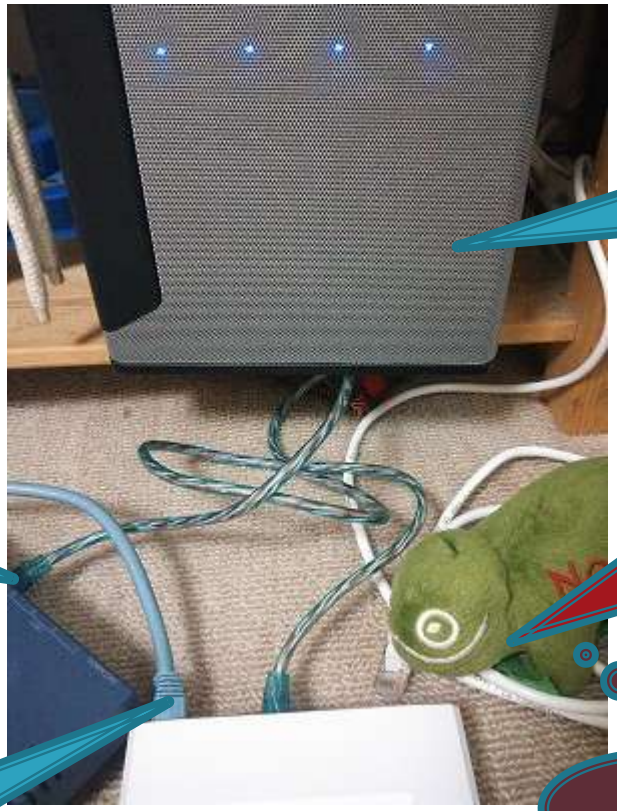
- 本日のお品書き。
  - VPNってそもそも何？
    - どんな場面で使用されるの？
    - どんなプロトコルが使われるの？
    - オープンソース以外ではどんなルーターがあるの？
  - openSUSE で VPN ルーターを構築しよう！
    - まずは YaST でさくっとルーター構築
    - スマホからもつながる VPN ルーターを構築しよう！

VPNってなんだ？

- 第1章

どうしてvpnが必要なの？

- たとえば、ちびぎーこくんはあることを思いついた。



暗号化されていない
ファイルサーバー

スイッチングハブ
の下にルーター

ファイルサーバーを
直接WANへ
接続しようとする
ちびぎーこくん

直接WANにささった
スイッチングハブ

これで外から
ファイルサーバーへ
アクセスできるはず！

これは・・・

暗号化されていないファイルサーバーを直接WANにさすとか、言語道断ですよね。

じゃ～どうすればいいの？

- SSH を使えばいいじゃないか！
  - ファイルサーバーも使いたいので却下。
- SCP でファイルサーバーみたいなことも出来るよね？
  - サービス毎にポート番号を開けるのはちょっと・・・。
    - SSH = 22
    - HTTP = 80
    - SSL = 443

    …とやっていたらキリがない！（セキュリティ的にもね）
- 外部から社内 LAN と同じネットワークへ接続したい！
  - そうすればポート番号も気にせずにサーバーが使えるはず。

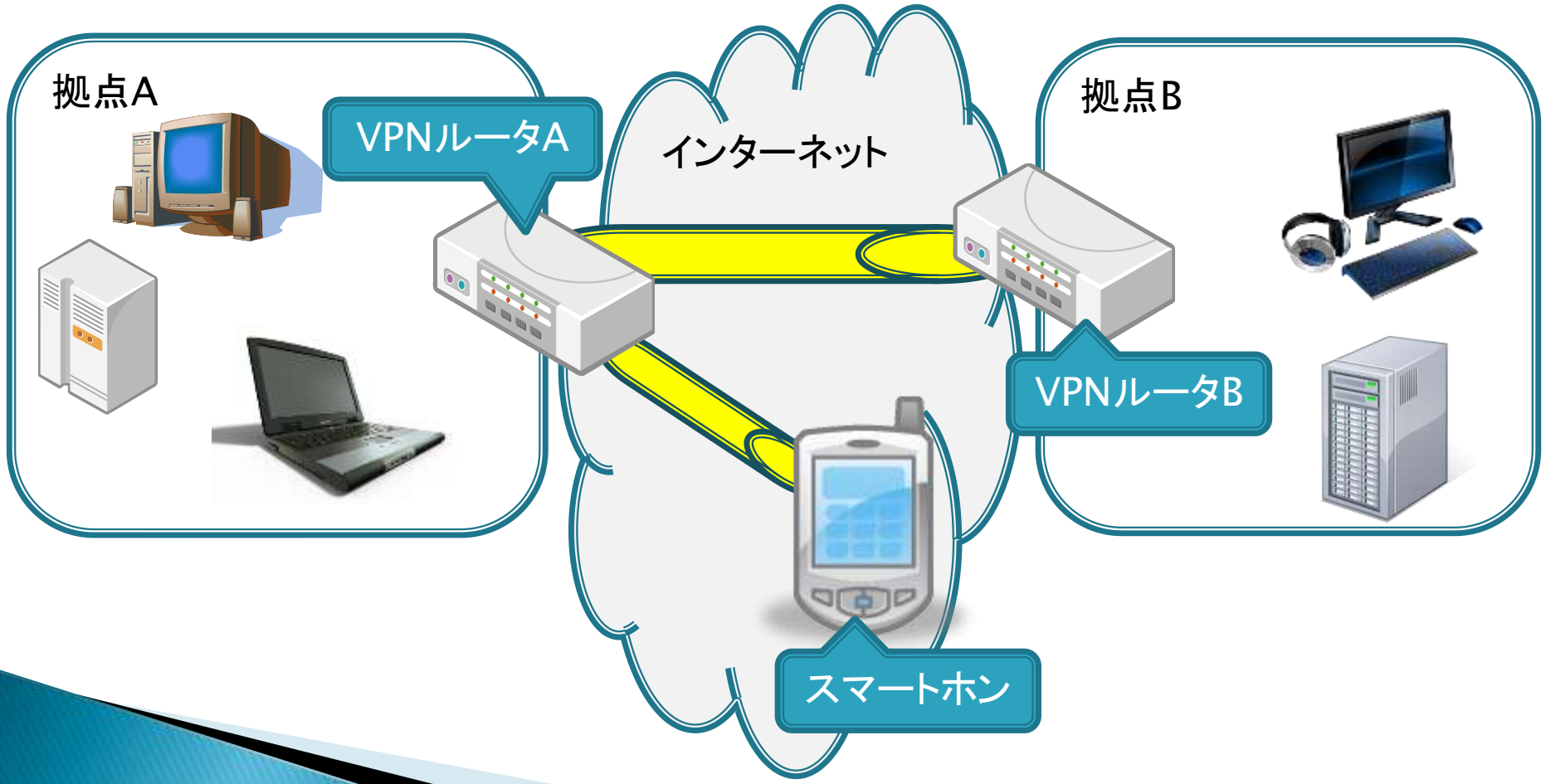
VPNについて。

- Virtual Private Networkの略。
  - Network (LAN) 間を接続する技術。
- 様々なプロトコルが使用される。
  - PPTP
  - IPsec
  - L2TP
  - OpenVPN
  - …

たとえば。

- こんなふうに接続します。

- 拠点間を同一ネットワークに
- スマートホンからもアクセス可能に



プロトコル！？

- いろいろあって、どう使い分けたら？？？
  - 自分が使っているルーターや端末を確認してみましょう！
  - 今時のスマートホンにもVPN接続機能はありますしね！
- Androidで使用できるVPNを調べてみると…。
  - PPTPとIPsec/L2TPが使えるみたい。
  - Android端末メーカーにも依りますけど。。。
- WindowsやLinuxではPPTPが使用できます。
  - 例えば、Yamaha製ルーターは、「Microsoft社製Windows OSのL2TP/IPsec接続はサポートしません。」と明記されています。やはり Windows は PPTP？（他のメーカーは調べてません。あしからず。。。）

1. PPTP

- メリット:
  - 非常に多くの端末で使用可能。(Windows, Linux …)
  - 鍵長が128ビットの暗号化のため、スピートが速い。
- デメリット:
  - 鍵長が128ビットのため、比較的容易に解読可能。
  - 認証方式もMS-CHAPv2が主に使われるが、脆弱性が既に発見されており、使用するべきではない。
- 総括:
  - 情報を盗まれても構わないVPNで使用するべき！
    - そんなVPNあるか～！？？

2. IPsec

- メリット:
  - 複数の暗号化方式、暗号鍵、セキュリティプロトコル等を利用できるため、非常にセキュリティを強固にすることが出来る。
- デメリット:
  - 暗号化方式、暗号鍵、セキュリティプロトコル等を、接続する側とされる側で全てを統一する必要があるため、かなり面倒。
  - 複雑な暗号化方式のため、PPTP と比べると遅い。
- 総括:
  - 拠点間接続向き。
    - 頑張れば仕様が特殊な市販ルーターでも、オープンソースルーターと接続可能ですよ！

3. IPsec/L2TP

- メリット:
  - L2TP 自体は暗号化機構を持っていないが、IPsec と併用することで、セキュリティを強固にすることが出来る。
- デメリット:
  - やっぱし遅い。
- 総括:
  - スマートホン向き。
    - L2TP 自体は実は古いプロトコルです。スマートホンブームにより、突然注目され始めたという経緯があります。

4. OpenVPN

- メリット:
  - OpenSSL のライブラリで暗号化が行われているため、それを利用してセキュリティを強固に出来る。
  - オープンソースのソフトウェアである。
- デメリット:
  - オープンソースのソフトウェア…のはずなのだけど、Android や iPhone 等には、デフォルトで接続ツールがインストールされていない。
- 総括:
  - Linux がクライアントとしてある場合は便利かも。。。

ところで・・・。

- オープンソースを使う以外で、VPNルーターはどんなものがあるの？
- やっぱし市販ルーターかな～？
  - 中古ルーターなら安く手に入る？
    - でも新機能満載ルーターは中古でも高い・・・。
- オープンソースは PC さえあれば構築可能！
  - しかも、プロトコルなども全て自分で自由に設定できます。
  - もちろんその知識も身につきますよね！

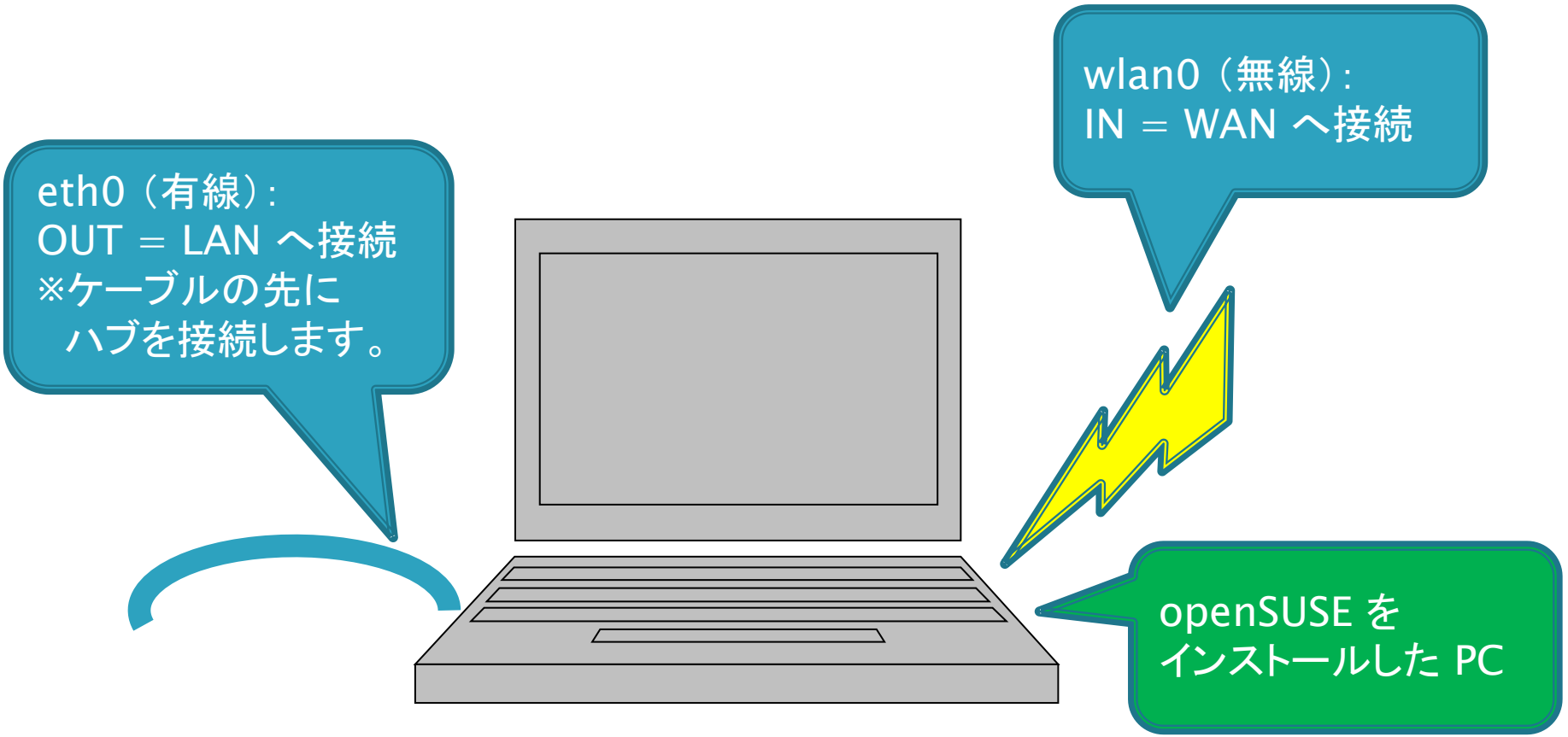
openSUSE でVPN ルーター構築

- 第2章

ちょっと待って！

- ふつ～の PC がルーターになんてすることできるの？
  - できます！
  - NIC が2つあれば、どうにかなります。

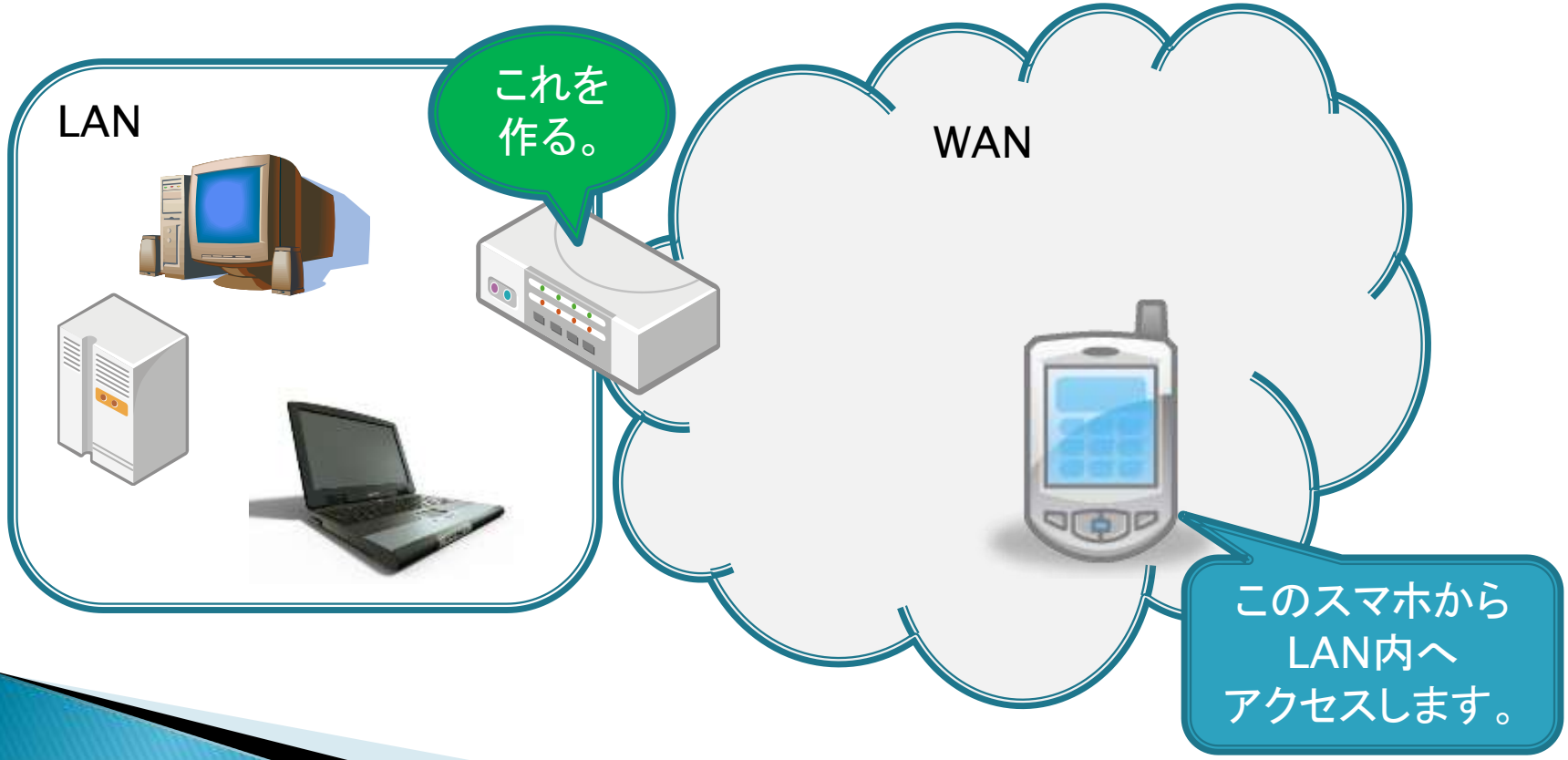
こうやります！



IN と OUT があれば他にも方法はあります。。。

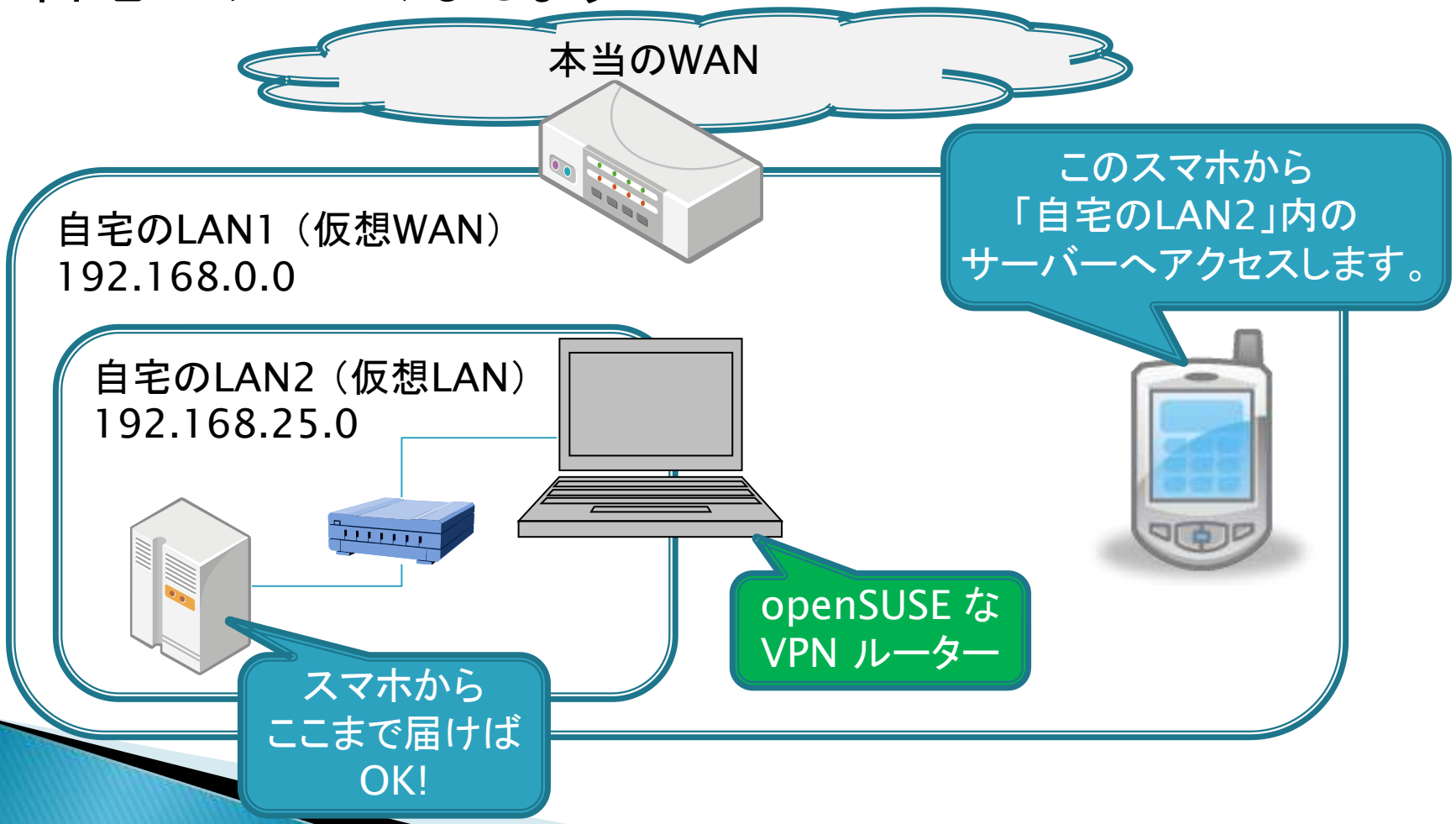
本日のお題。

- IPsec/L2TP ルーターを構築してみましょう！
  - 目標は、スマホから LAN 内へ接続できること。



実験環境？実は簡単です！

- 自宅でやってみましょう！

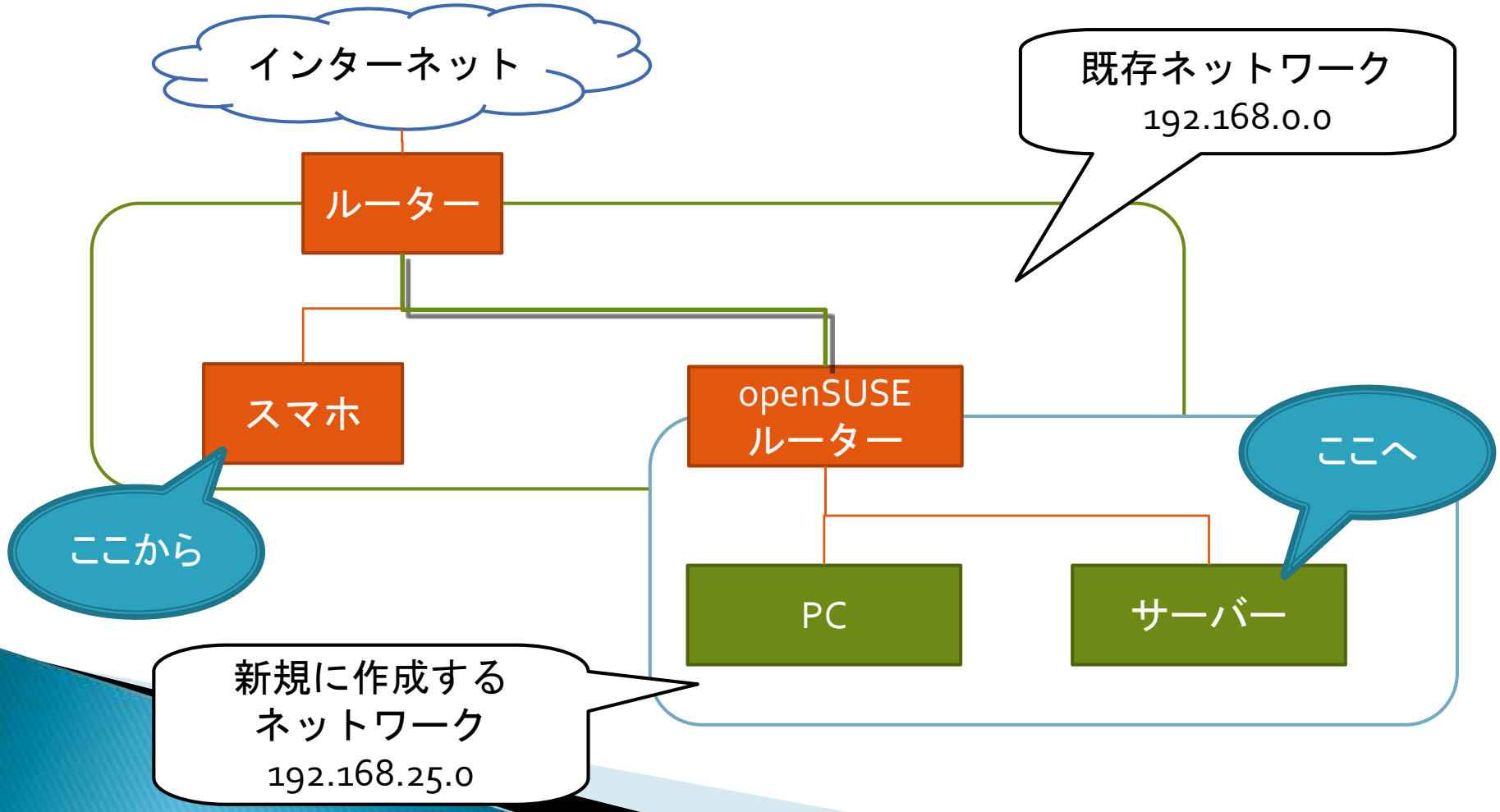


openSUSE って？

- ドイツ発祥の Linuxディストリビューションです。
- SUSE Linux Enterprise Server/Desktop のオープンソース版です。
  - 歴史があるので、昔から Linux 触ってる方はご存知な方が多いようです。
- openSUSE で覚えておきたい三種の神器。
  - YaST : Windows でいうところのコントロールパネル
  - OpenBuildService : パッケージ作成ツール
  - Geeko : SUSE のマスコット
- 合い言葉は「Have a lot of fun!」

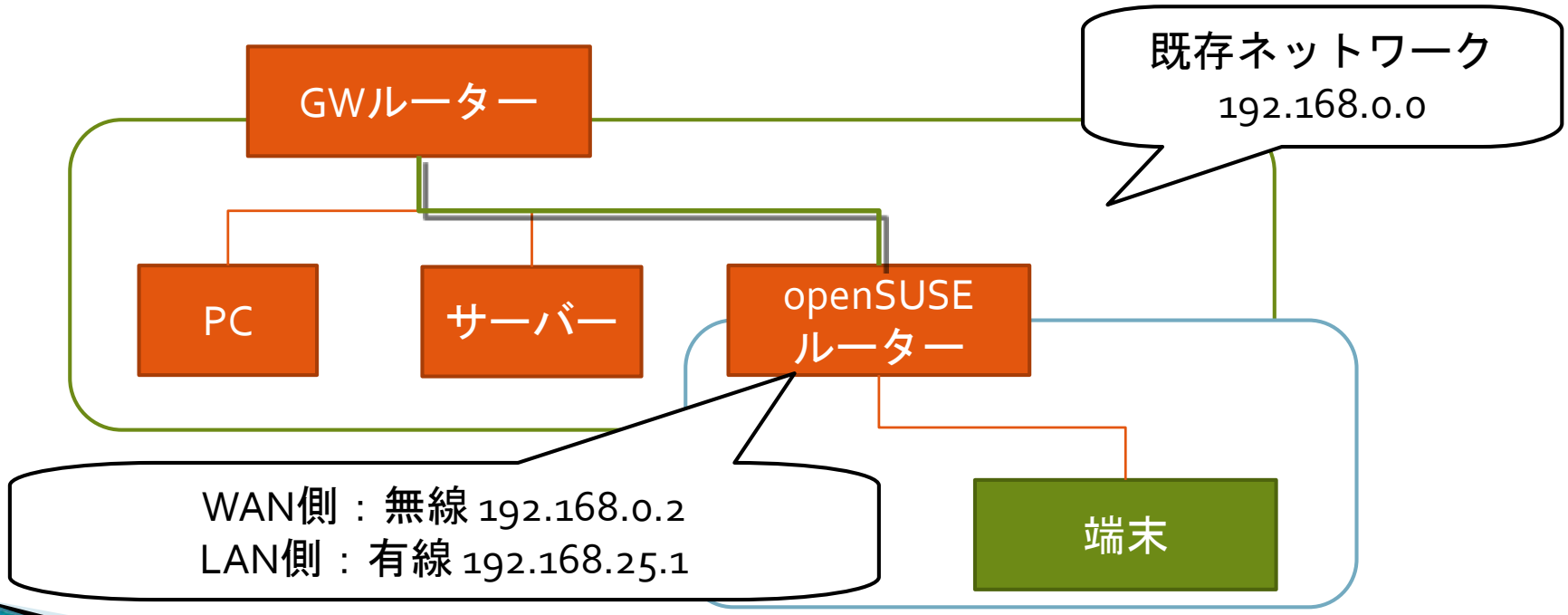
それではルーターを作ってみよう

- まずは実験用のネットワーク設計から。



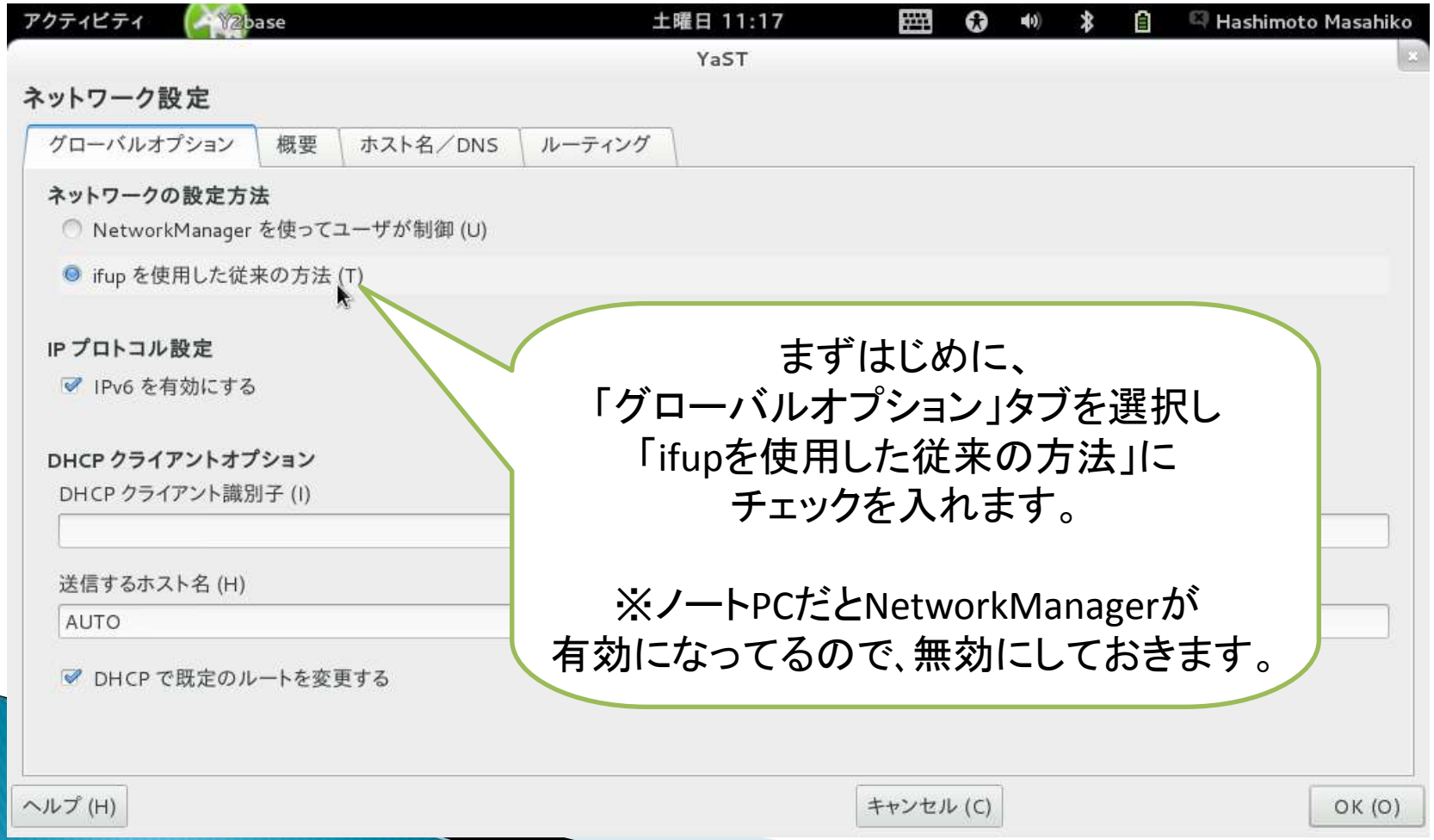
openSUSE ルーターのNIC設定

- 今回はノートPCを利用するので…
  - 有線:　eth0　＝　192.168.25.1
  - 無線:　wlan0　＝　192.168.0.2



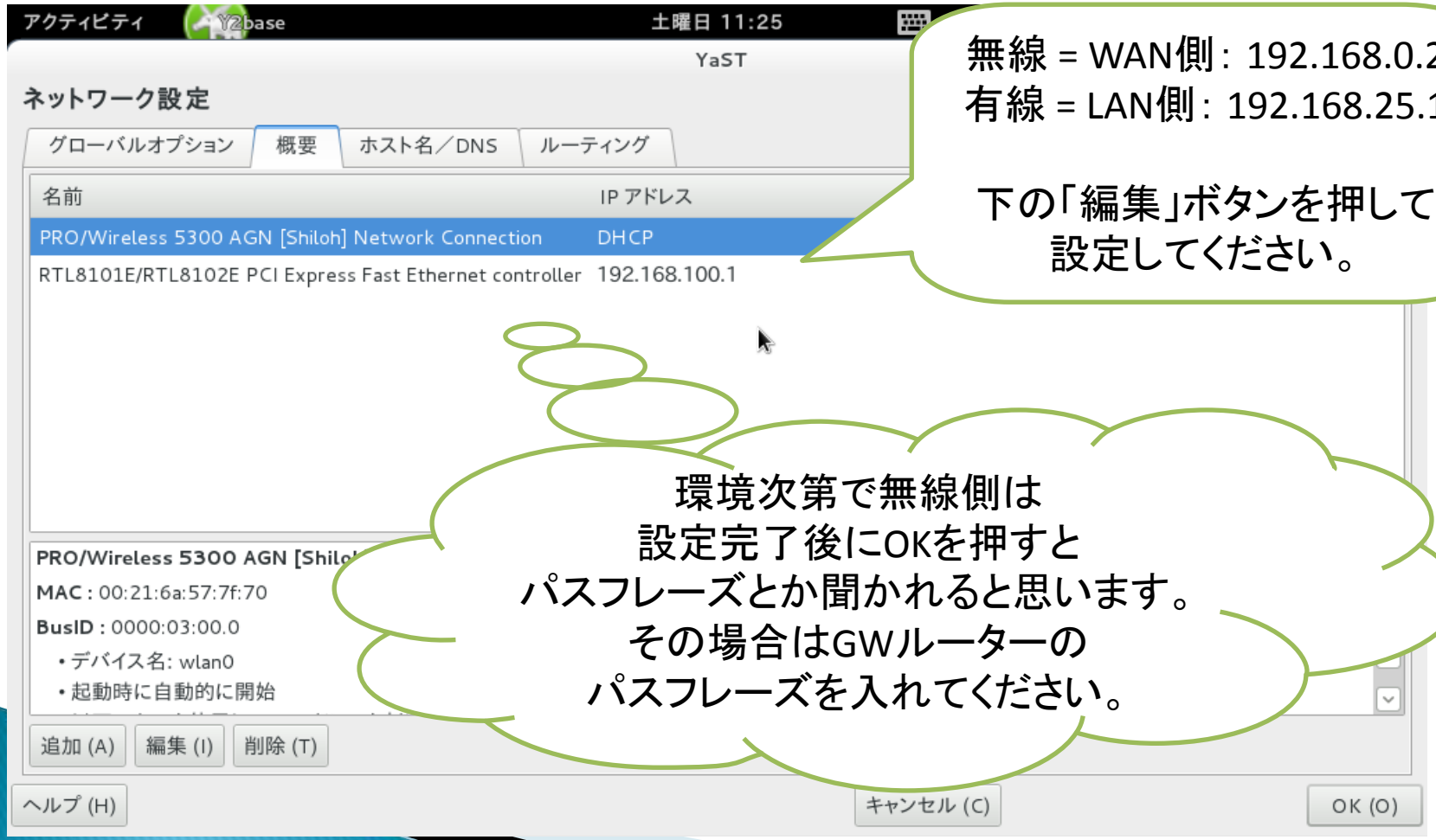
まずはYaSTでルーター構築。

- YaSTを起動して「ネットワークの設定」を開きます。



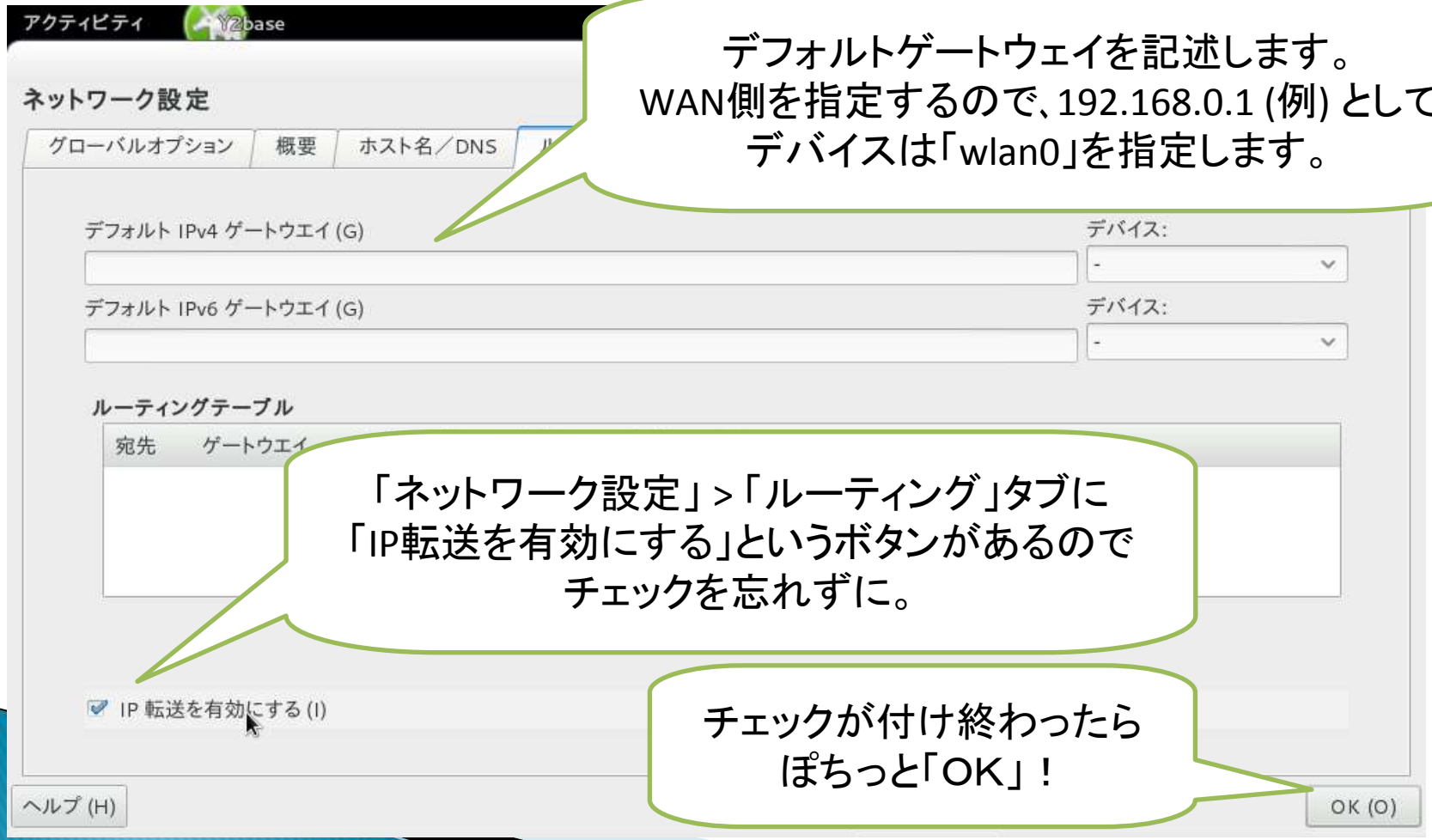
続いてIPアドレスの設定

- YaST だと楽々ですね！



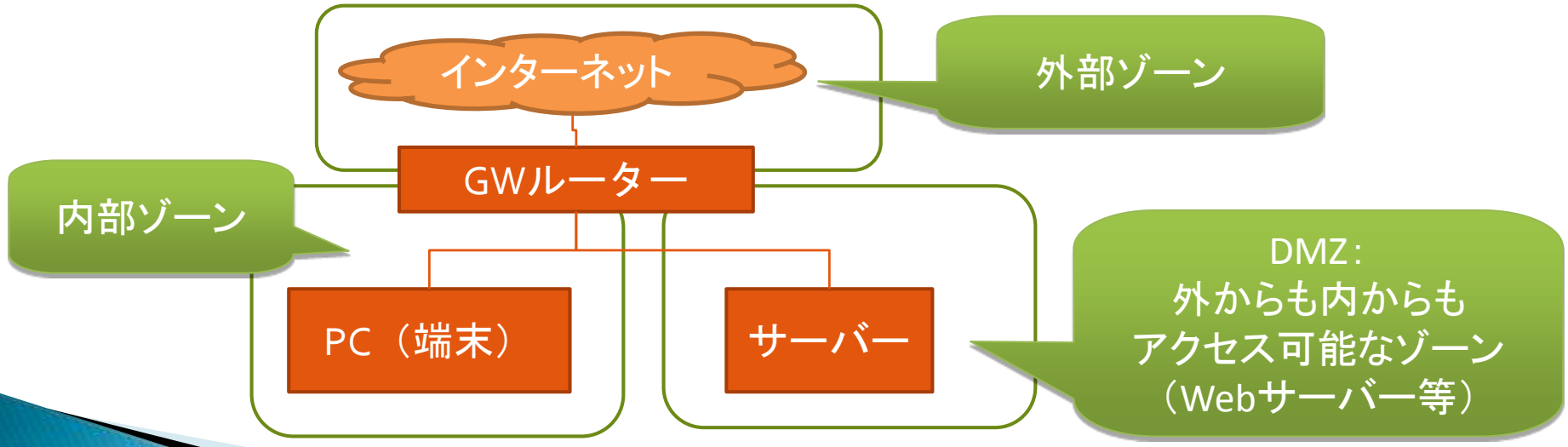
ルーティングの設定

- これも YaST であっという間に出来ます。



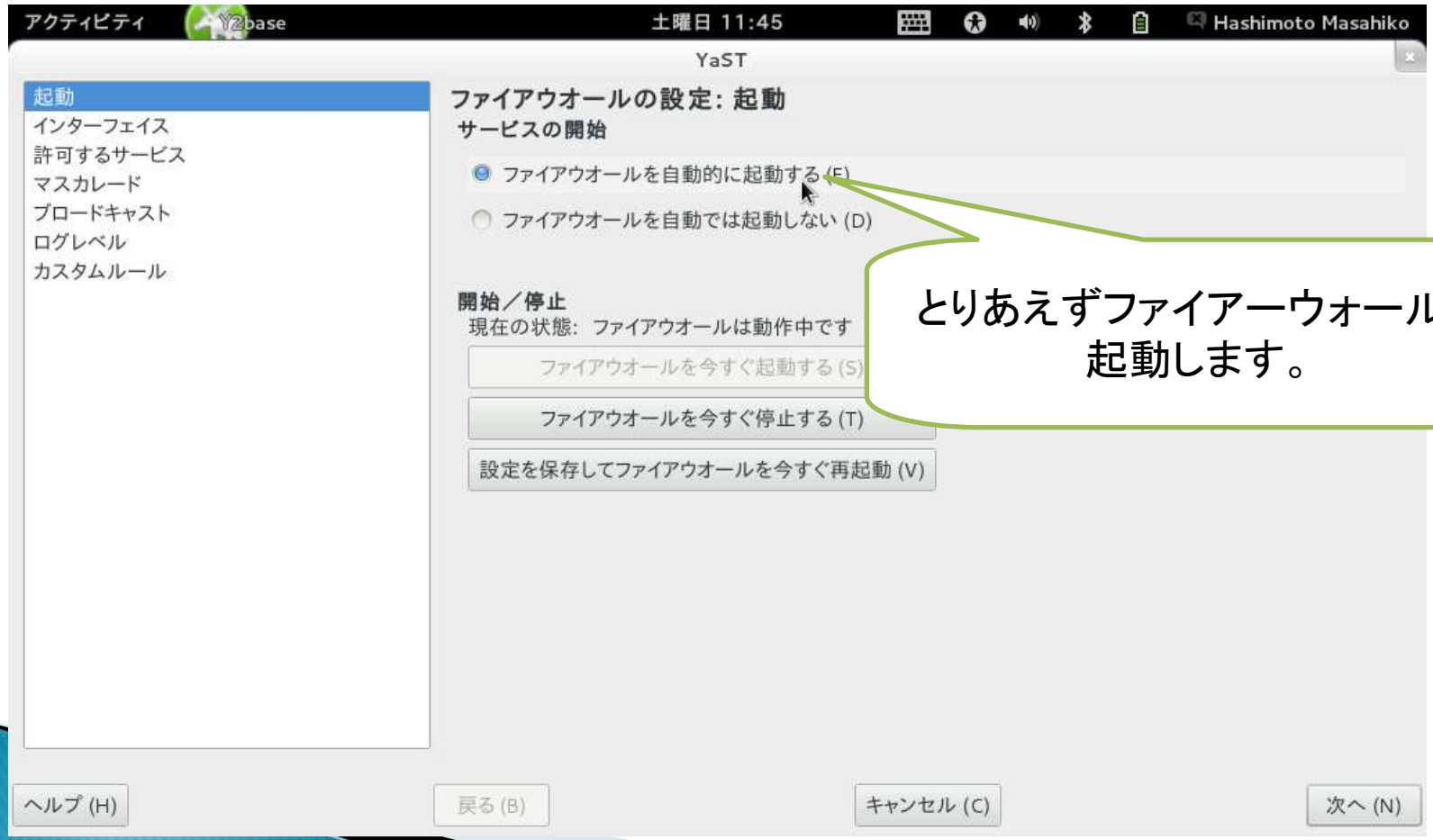
openSUSE のファイアーウォール

- openSUSE には3つの「ゾーン」があります。
  - 内部ゾーン： LANポート側
  - 外部ゾーン： WANポート側
  - 非武装ゾーン： DMZ



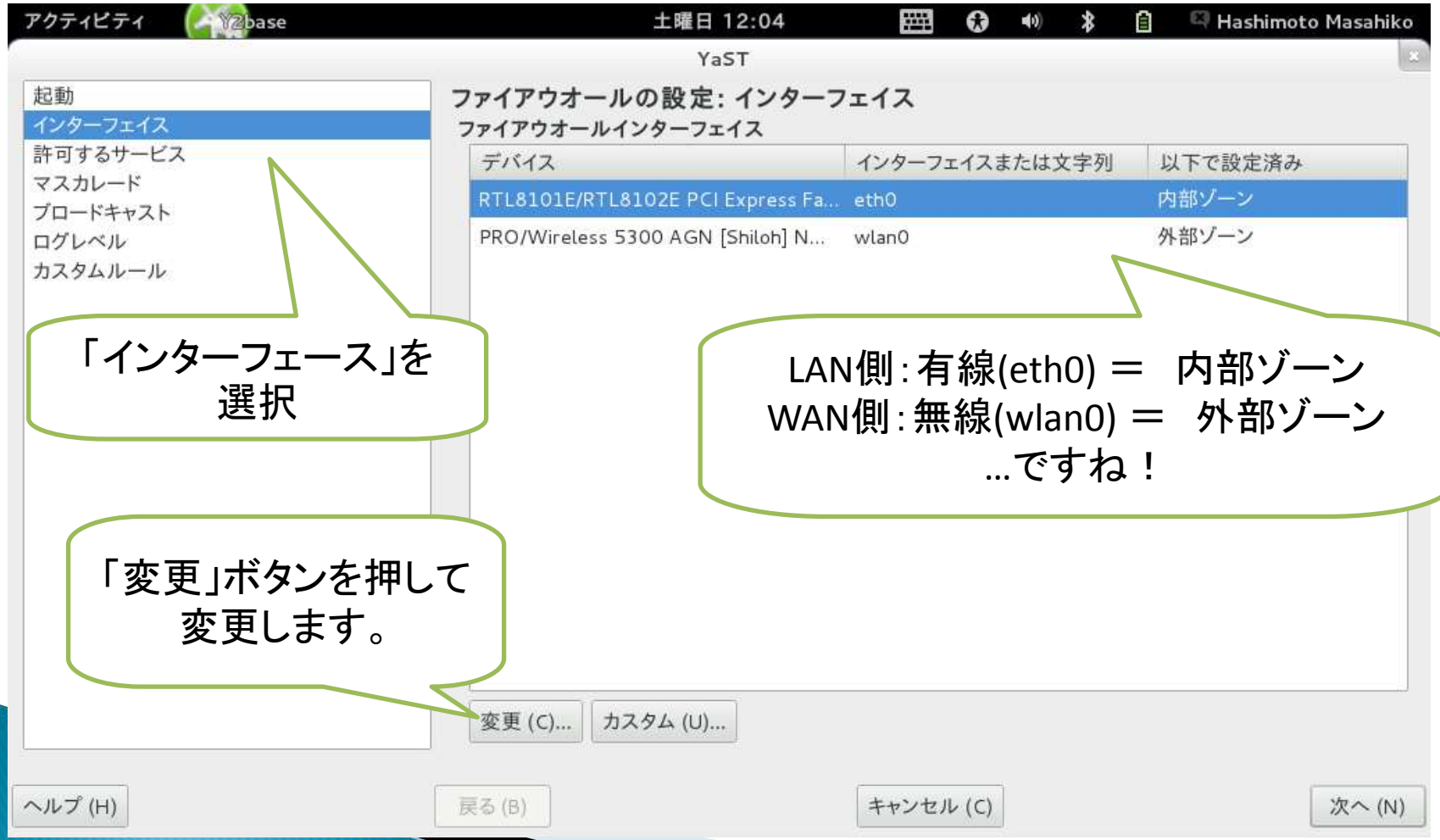
YaST でファイアーウォール設定

- YaST ＞「ファイアウォール」を起動しましょう！



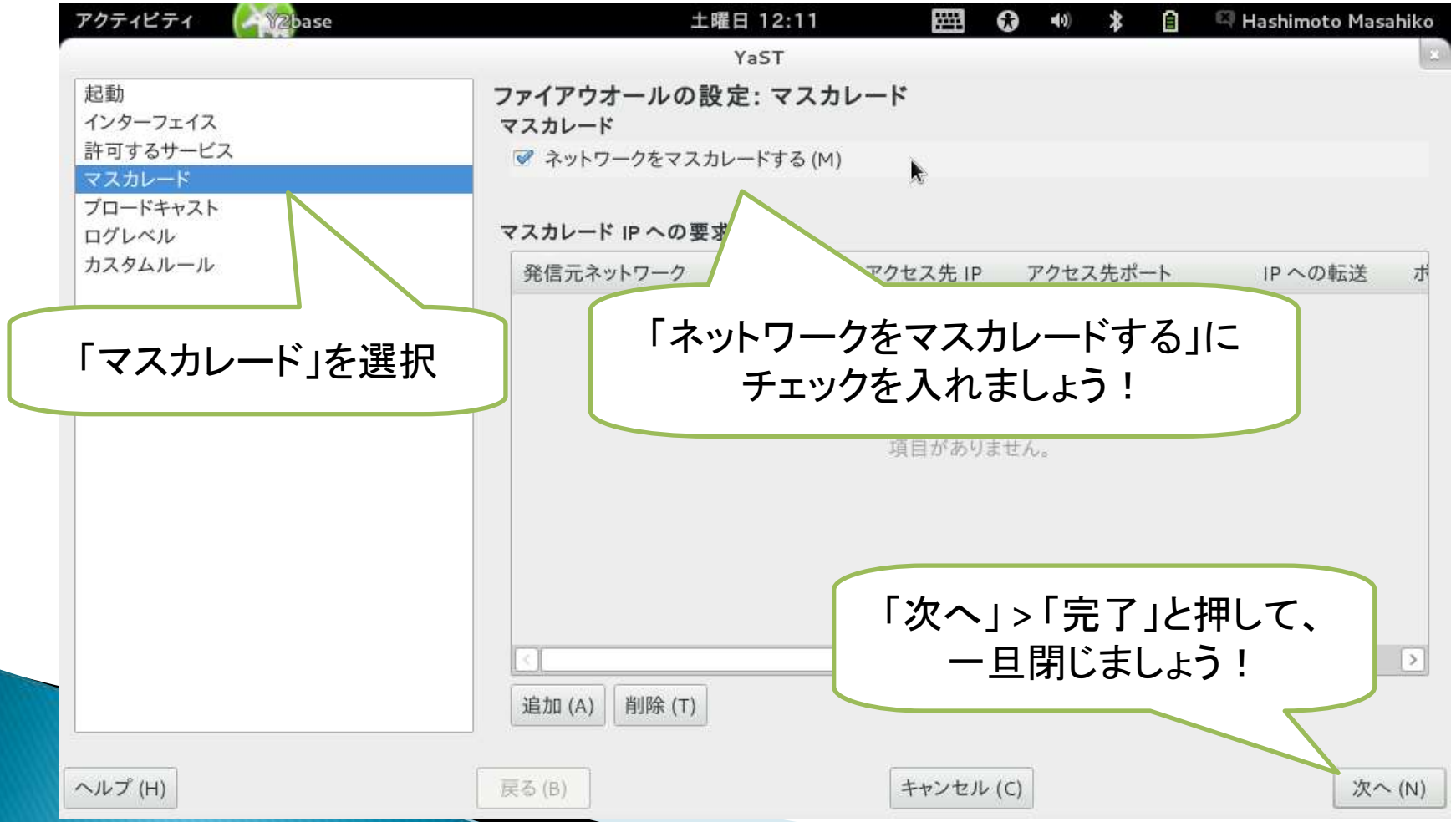
インターフェース＝NIC毎の設定

- 左メニューから「インターフェース」を選択します。



マスカレードの設定

- 左メニューから「マスカレード」を選択します。



ここまでで「ルーター」は完成！

- 後は有線(eth0)にスイッチングハブをつなげばOK!
- 単純なルーター構築だけなら、ここまでで完了です。
  - YaST なら面倒なネットワーク設定も楽々ですよね！
- YaST について詳しく知りたい方は、セミナー終了後にブースへお立ち寄りください。
  - もっといろんな使い方ができます！
  - Apache や Samba の設定も YaST からできますよ。

最後の砦、IPsec/L2TP！

- 使用するソフト:
  - StrongSwan：IPsec の実装
    - 他にも OpenSwan 等もありますが、openSUSE で標準リポジトリにあるのは、StrongSwan となります。
  - xl2tpd：L2TP の実装
    - こちらはほぼ一択かもしれません。StrongSwan と同様に、openSUSE の標準リポジトリにあります。
- どちらも、「YaST」–「ソフトウェア管理」から、パッケージを検索してインストールしてください。

StrongSwan の設定

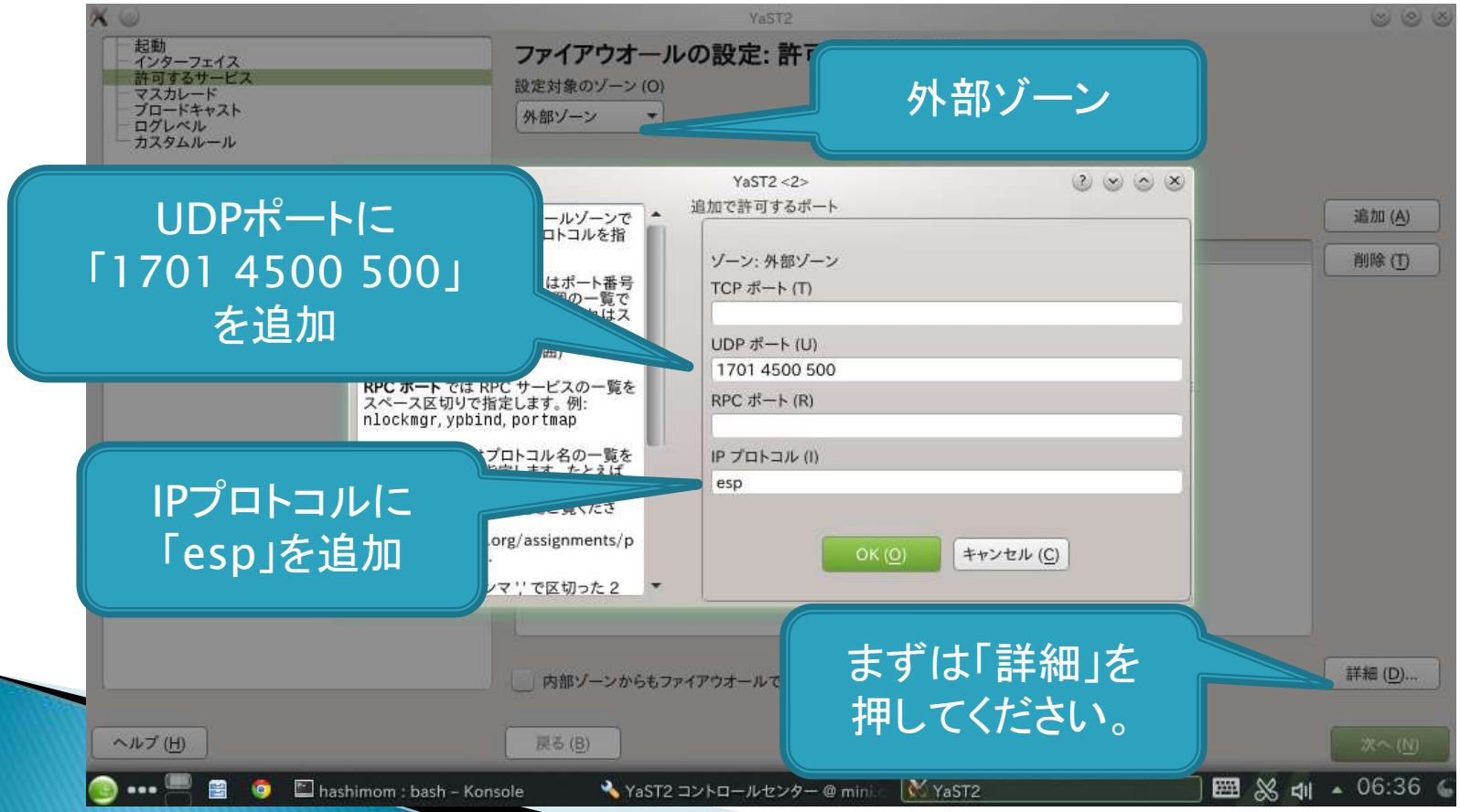
- 主な設定ファイルは3つ！
  - /etc/ipsec.conf：接続の設定
  - /etc/ipsec.secrets：認証の設定
  - /etc/strongswan.conf：StrongSwanの設定
    - strongswan.conf はそのままでも動作します。
- 一番はまりそうなこと。
  - ぐぐると様々な ipsec.conf 設定例が出てきますが、そのまま書くと動かないことが多いようです。
    - Ver5.0.0 から大きな仕様変更があったため。
    - Wiki（英語）を頑張って読みましょう！
    - http://wiki.strongswan.org/projects/strongswan/wiki

xl2tpd の設定

- 主な設定ファイルは3つ。
  - /etc/xl2tpd/xl2tpd.conf：接続の設定
  - /etc/ppp/options.xl2tpd：PPPの設定
  - /etc/ppp/chap.secrets：認証の設定（MS-CHAPv2）
    - IPsecで既に暗号化されているため、MS-CHAPv2の脆弱性も影響を受けません。（PPTP とは異なります）
- 一番はまりそうなこと。
  - 設定だけでは起動しない！
    - 原因を調べると「mkdir /var/run/xl2tpd/」と叩いてね！と書いてあるページを発見。←PC再起動毎に作成する必要あり！
      - …そんなオチかよ。。。（辿り着くまで2時間以上かかったorz

ファイヤウォールの設定も忘れずに

- 「YaST」–「ファイヤウォール」–「許可するサービス」を選択し、「外部ゾーン」の設定を変更します。



ここから先は設定「例」です。

- 自分の環境にあわせて、読み替えてください。
  - 実験してから利用することをオススメします。

/etc/ipsec.conf

```
config setup

conn L2TP
        authby=psk
        keyexchange=ikev1
        ike=aes256-sha1-modp2048,3des-sha1-modp2048!
        esp=aes256-sha1-modp2048,3des-sha1-modp2048!
        leftprotoport=17/1701
        right=%any
        rightprotoport=17/%any
        auto=add
```

IKE：
暗号鍵交換のための
プロトコル

ESP：
ペイロード部の暗号化

備考：
IKEv2にしてしまうと、Androidから接続できなくなるようです。
StrongSwan のパッチを当てれば解消される模様です。

/etc/ipsec.secrets

```
#
# ipsec.secrets
#
# This file holds the RSA private keys or the
PSK preshared secrets for
# the IKE/IPsec authentication. See the
ipsec.secrets(5) manual page.
#
192.168.0.2 %any : PSK "abcdefghijklmn"
```

Ipsecルーターの
WAN側IPアドレス

PSK:　事前共有鍵認証
その下の “abc～”が
事前共有鍵になります。

/etc/xl2tpd/xl2tpd.conf

```
[global]

[lns default]
ip range = 192.168.25.100-192.168.25.105
local ip = 192.168.25.1
require chap = yes
refuse pap = yes
require authentication = yes
ppp debug = yes
pppoptfile = /etc/ppp/options.xl2tpd
length bit = yes
```

クライアント側に付与する
IPアドレス

Ipsecルーターの
LAN側IPアドレス

/etc/ppp/options.xl2tpd

```
name l2tp
auth
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
logfile /var/log/xl2tpd.log
```

既に暗号化ずみのため
脆弱性の影響は受けません。

/etc/ppp/chap-secrets

```
# Secrets for authentication using CHAP
# client        server          secret          IP addresses

# INBOUND CONNECTIONS
hashimom        *       PASSWORD        *
```

ユーザ名

パスワード
※絶対に変えてね！！！

いかがでしたでしょうか

- 設定するポイントとして、信憑性のあるドキュメントを参考にするのが一番だと思います。
- 「なぜここはこうなっているの？」というのを理解しながら設定するのは、セキュアなサーバーを構築する基本ですよね！
  - ぐぐってコピペ！では、自分のためにもなりませんし、セキュリティ的にも高いものができるとは思えません。
- 「マスタリング TCP/IP IPsec編」も売っているので、それを参考にしてもよいと思います。
  - 別に回し者ではないけど・・・^^;

ご清聴、ありがとうございました
m(_ _)m