



LPIC レベル3 303 Security ハンズオンセミナー

講師：株式会社びぎねっと

宮原 徹

tmiyahar@Begi.net

事前準備

1. クライアントの設定確認
 - NICに設定されたIPアドレスを確認
 - インターネットにアクセスできますか？
2. 実習環境はVMware Serverを利用
 - ルーターの代わりに仮想NATを使用
3. ゲストOSの導入
 - OSはCentOS 5.3
 - 仮想NATネットワークに接続
 - 仮想NATネットワークを10.0.0.0/8に設定
 - 仮想マシンのeth0を10.0.0.10/8に設定
4. 仮想NATのポート転送設定
 - クライアント サーバーにポート22を転送
 - クライアント サーバーにポート1194を転送



事前準備状態の確認

1. ゲストOSが起動できるか
2. ゲストOSにログインできるか
3. ゲストOSから外部のWebサイトが参照できるか
4. ホストOSからSSHで接続できるか
PuTTYをホストOSにインストール
ファイルコピー用にWinSCPをインストール



ポイント確認 OpenSSL



HTTPSの3つの役割

SSLを介したHTTPをHTTPSと呼ぶ

1. サーバーのなりすましを防ぐ

- 認証局(が電子署名したサーバー証明書)でサーバー自体の信頼性を保証する

2. 送受信されるデータの盗み見を防ぐ

- 共通鍵暗号で通信内容を暗号化する

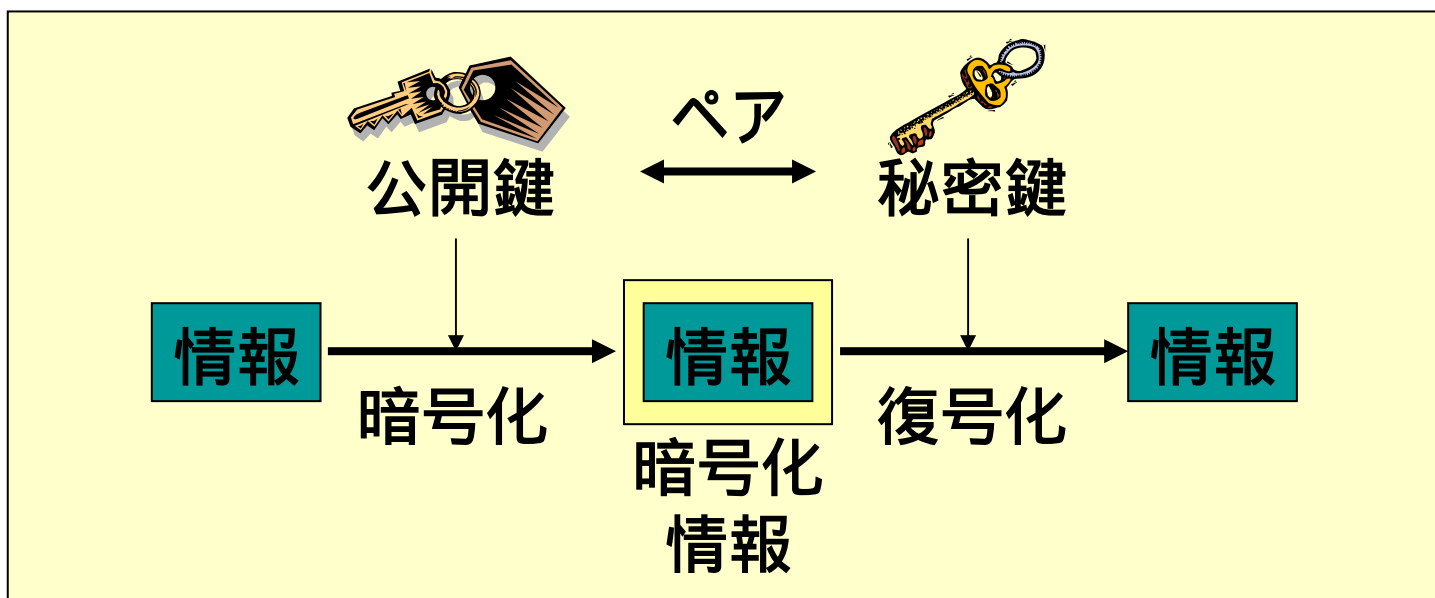
3. データの改ざんを防ぐ

- メッセージ認証コードでデータが改ざんされていないことを確認する



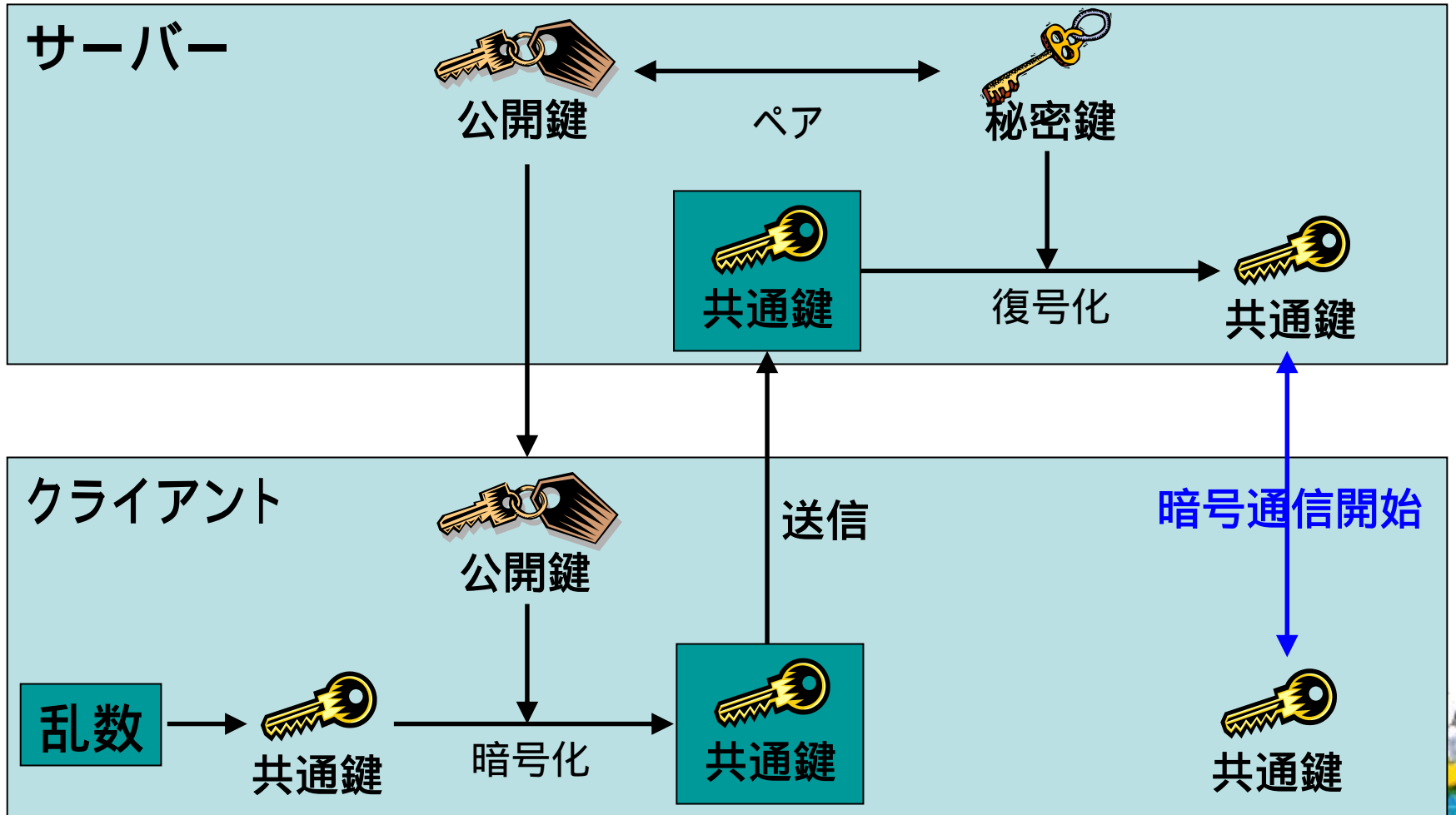
秘密鍵/公開鍵暗号の仕組み

- 秘密鍵と公開鍵はペアで生成される
- 公開鍵で暗号化された情報は、秘密鍵だけが復号化(元の情報を取り出す)できる

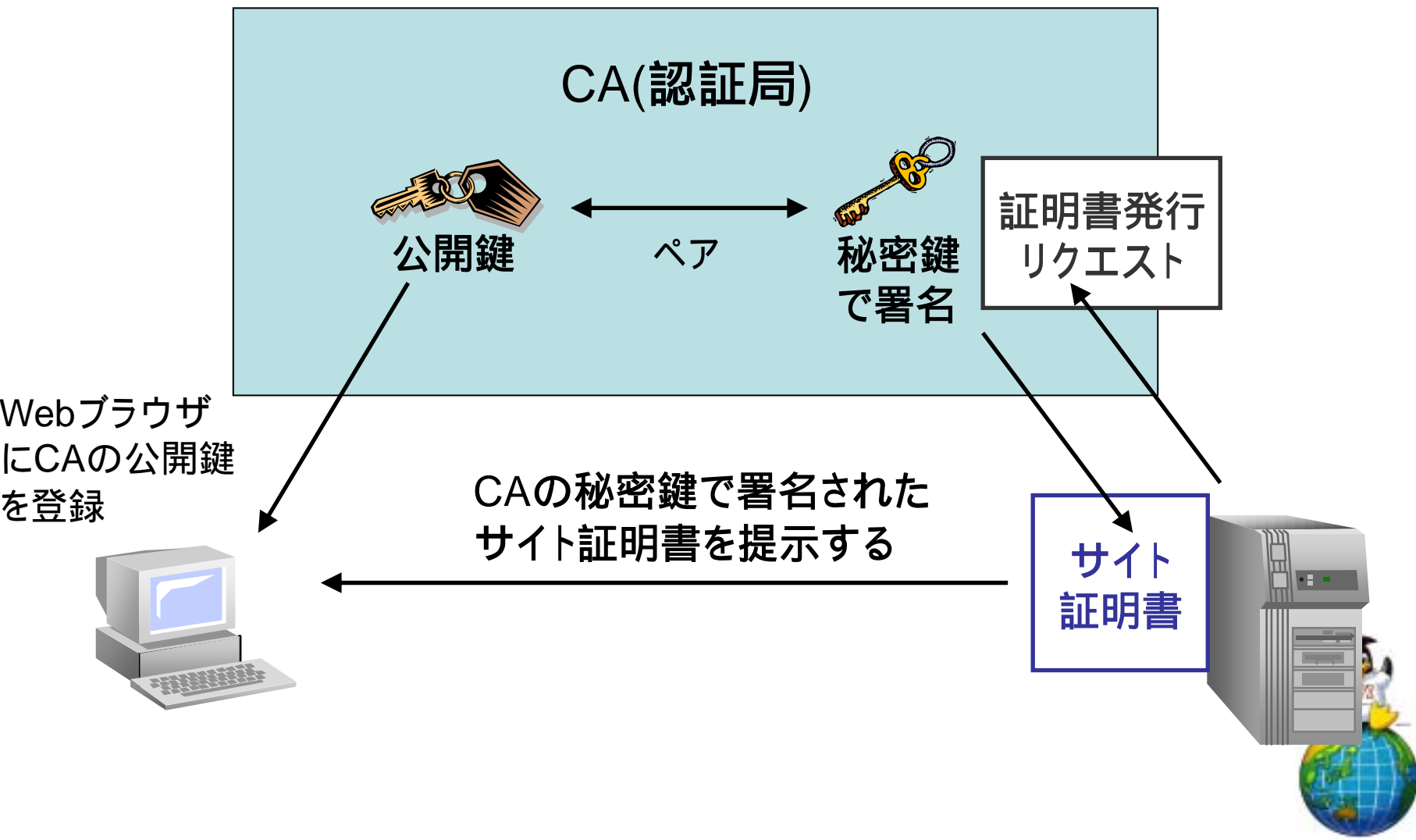


共通鍵を送る手順

～ 公開鍵暗号通信 ～



CAを介した信頼性の保証



HTTPSの提供に必要なもの

- Apacheのsslモジュール
- サーバーの公開鍵と秘密鍵
 - セッション開始時にクライアントから受信した共通鍵を復号化するため
- 認証局(CA)が電子署名したサイト証明書
 - 信頼できるサーバーである(なりすましではない)ことを確認できる
 - サーバーの運営主体やコンテンツの内容が信頼できるわけではない
 - 本人確認が甘いCAもあるので、信頼性が低い場合もある



HTTPSの設定手順

1. サーバーの秘密鍵の作成
2. CSR (Certificate Signing Request) の作成
3. CAにサイト証明書へ電子署名してもらう
4. Apacheの設定
 - ssl.confにヴァーチャルホストとして設定
 - ssl.confはデフォルトでhttpd.confから読み込まれるように設定されている
 - httpd.confそのものに記述する場合もある



ハンズオン実習

OpenVPN

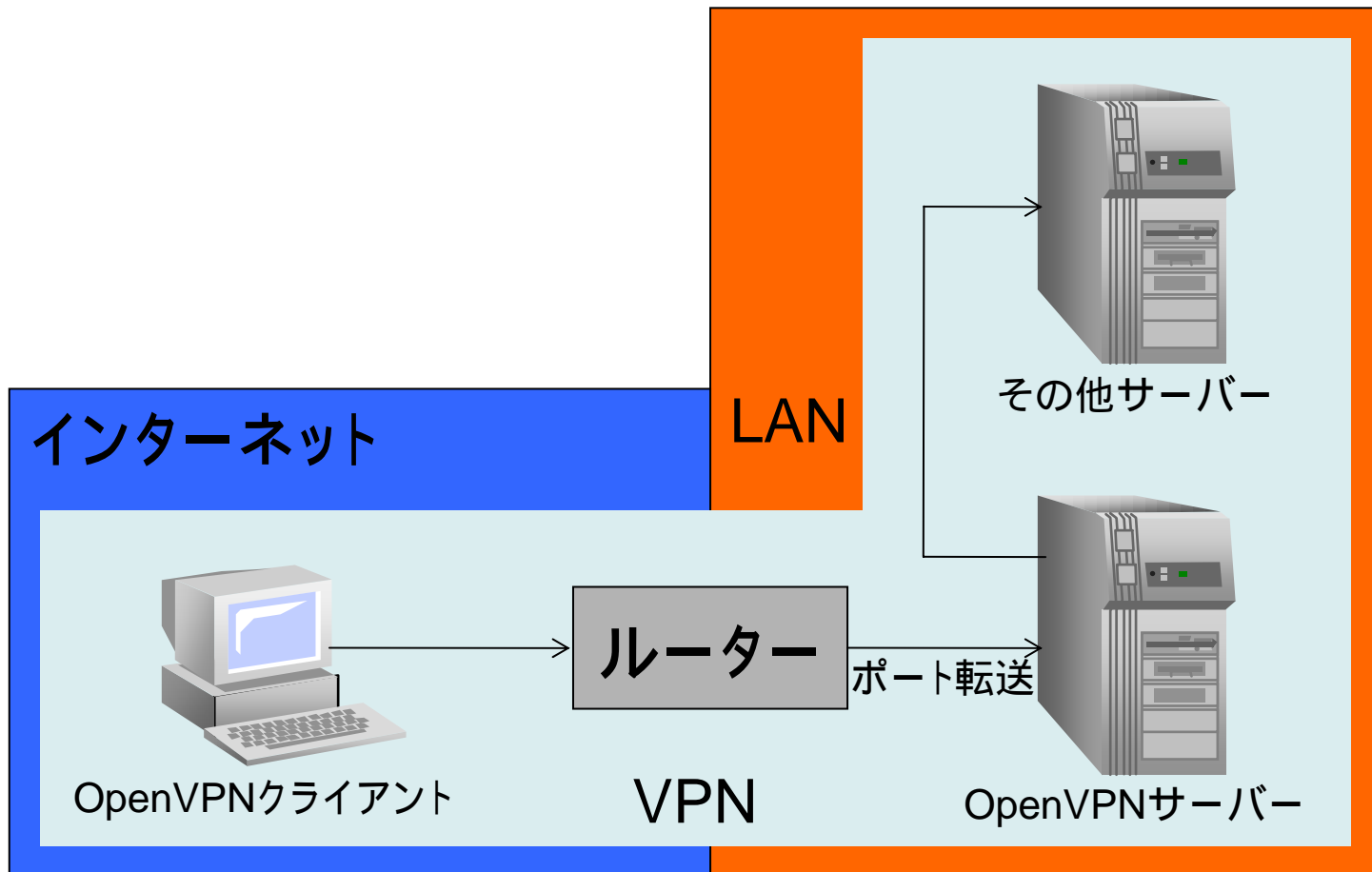


OpenVPN

- SSLを利用したSSL VPN
- GPLで提供されている
 - 非オープンな商用ライセンスも選択可能
- マルチOSサポート
 - Linux、Windows、各種BSD系OS、Solaris等
- 公開鍵認証やパスワード認証が可能



OpenVPNによるVPN構築例



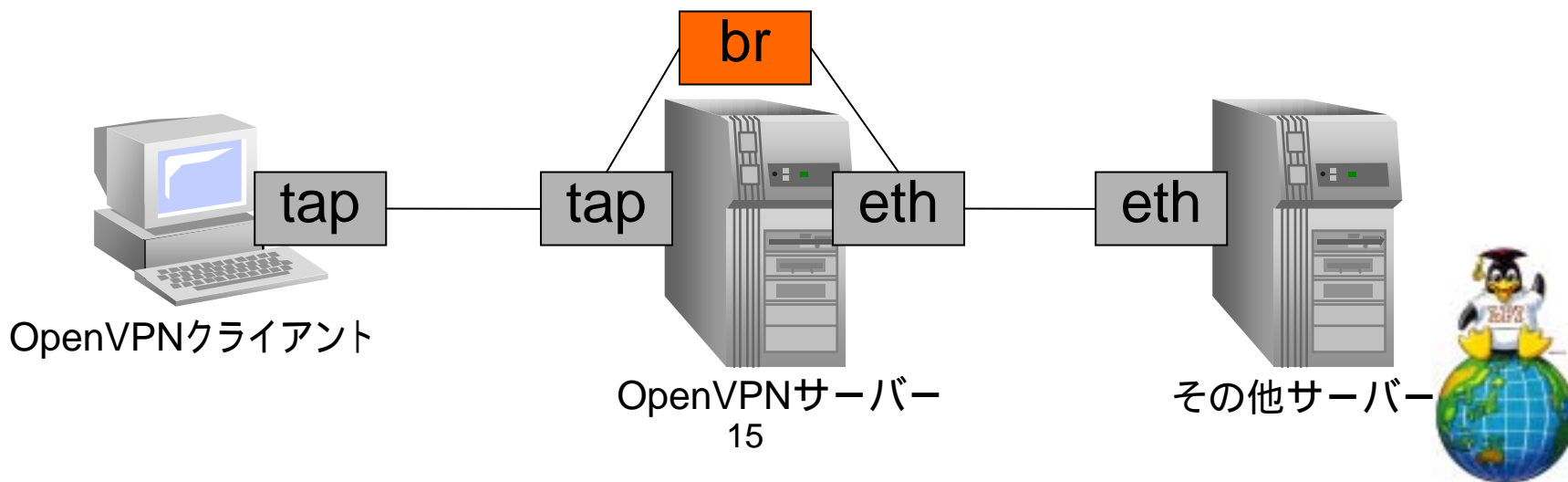
OpenVPN設定時のポイント

- ルーティングモードとブリッジモードがある
 - Windowsファイル共有のようにブロードキャストを使う場合はブリッジモードが楽
 - 今回はブリッジモードで設定
- OpenVPNサーバーとクライアントは別セグメント
 - 間にルーター等を入れてポート転送などを行う
- OpenVPNサーバーのNICは1つが良い
 - もちろん別NICとの間でのルーティングやNATも可能



tun/tapデバイスとブリッジ

- 仮想NIC tun/tapデバイス
 - カーネルモジュールが必要
 - tunはL3、tapはL2で動作
- tapデバイスとethデバイスをブリッジ接続



作業上の注意

- 時刻を合わせておく
 - CA作成前にNTPなどで時間を合わせておく
 - 時間がずれた状態で作業をするとやり直しになる
- OpenVPNサーバーの自動起動に注意
 - openvpnパッケージはOpenVPNサーバーを自動起動に設定する
 - ブリッジモードで使用する場合、ブリッジ設定スクリプトが別なので、ブリッジ無しで起動してしまう
 - 作業途中でシステムの再起動などを行った場合には要注意



OpenVPN サーバー構築手順

1. 必要なパッケージの導入
2. 各種認証関係ファイルの作成
 - CAの作成
 - サーバー証明書の作成
 - DHパラメータの作成
 - 証明書廃止リストの作成
 - TLS認証鍵の作成
3. ブリッジの設定
4. OpenVPNサーバーの設定



必要なパッケージの導入

1. bridge-utilsパッケージをインストール
 - ブリッジモードで設定する場合に必要
2. RPMforgeを使用可能にする
 - 手順は<https://rpmrepo.org/RPMforge/Using>を参照
3. openvpnパッケージをインストール
 - `# yum install openvpn`
 - lzo2パッケージも一緒にインストールされる



easy-rsaの導入

1. makeの実行でインストール可能

- インストール先として/etc/openvpn/easy-rsaを指定
- # cd /usr/share/doc/openvpn-*/easy-rsa/2.0/
- # make install DESTDIR=/etc/openvpn/easy-rsa

2. インストールの確認

- # cd /etc/openvpn/easy-rsa/



CAの作成

1. /etc/openvpn/easy-rsa/varsの修正

- export KEY_COUNTRY="JP"
- export KEY_PROVINCE="Tokyo"
- export KEY_CITY="Chiyodaku"
- export KEY_ORG="LPI-Japan"
- export KEY_EMAIL=info@lpi.or.jp

2. CAの作成

- # source vars
- # ./clean-all
- # ./build-ca

3. CAの証明書のコピー

- # cp keys/ca.crt /etc/openvpn/



サーバー証明書を作成

1. サーバー証明書の作成

- # ./build-key-server server
- チャレンジパスワードの設定は不要
- [y/n]が聞かれたら、yを入力(2回)

2. サーバー証明書のコピー

- # cp keys/server.crt /etc/openssl/
- # cp keys/server.key /etc/openssl/
- # chmod 600 /etc/openssl/server.key



DHパラメータの作成

1. DHパラメータの作成

– # ./build-dh

2. DHパラメータのコピー

– # cp keys/dh1024.pem /etc/openvpn/



証明書廃止リストの作成

1. openssl.cnfの修正(コメントアウト)
 - #[pkcs11_section]
 - #engine_id = pkcs11
 - #dynamic_path = /usr/lib/engines/engine_pkcs11.so
 - #MODULE_PATH = \$ENV::PKCS11_MODULE_PATH
 - #PIN = \$ENV::PKCS11_PIN
 - #init = 0
2. ダミーのクライアント証明書の作成と破棄
 - # ./build-key dummy
 - # ./revoke-full dummy
3. CRLのコピー
 - # cp keys/crl.pem /etc/openvpn/



静的暗号鍵の作成

- SSL/TLSのセキュリティ強化のための静的暗号鍵(事前共有鍵)を作成
 - 「HMACファイアーウォール」とも呼ばれる
 - サーバーとクライアントが同じ鍵を持っていないと接続が行えない
 - 詳細についてはマニュアルの--tls-authの記述を参照
1. `openvpn` コマンドに `--genkey` オプションをつけて実行
 - `# openvpn --genkey --secret /etc/openvpn/ta.key`



ブリッジの設定

1. ブリッジ設定スクリプトのコピー

- # cp /usr/share/doc/openvpn-2.0.9/sample-scripts/bridge-st* /etc/openvpn/
- chmod +x /etc/openvpn/bridge-st*

2. bridge-startスクリプトパラメータの編集

- eth_ip="10.0.0.10"
- eth_netmask="255.0.0.0"
- eth_broadcast="10.255.255.255"



OpenVPNサーバーの設定

1. 設定ファイルのコピー

- `cp /usr/share/doc/openvpn-2.0.9/sample-config-files/server.conf /etc/openvpn/`

2. 設定ファイル(server.conf)の修正

- TCPを使用
- tapデバイスとブリッジモードを使用
- 証明書関係ファイルは/etc/openvpnディレクトリに配置



OpenVPNサーバーの設定詳細

/etc/openvpn/server.conf

udpからtcpに変更

```
proto tcp  
;proto udp
```

#devはtap0とする。

```
dev tap0  
;dev tun
```

#証明書関係ファイルの指定

#デフォルトでは/etc/openvpn/を参照

```
ca ca.crt  
cert server.crt  
key server.key
```

#DHパラメータの指定

```
dh dh1024.pem
```

#サーバーのアドレス設定はコメントアウト

```
;server 10.8.0.0 255.255.255.0
```

#その代わりに、サーバーブリッジのコメントアウトを外し、修正

```
server-bridge 10.0.0.10 255.0.0.0 10.0.0.50 10.0.0.100
```

#コメントアウトを外す(1箇所のみ)

#/etc/openvpn/ccdのクライアント別設定ファイルを参照する

```
client-config-dir ccd
```

#コメントアウトを外す

```
client-to-client
```

```
duplicate-cn
```

tls-auth ta.key 0 ;サーバー側は0を設定。

#デーモンをnobody権限で実行する

```
user nobody
```

```
group nobody
```

#ログファイル等は必要に応じて設定

```
status /var/log/openvpn-status.log
```

```
log /var/log/openvpn.log
```

```
log-append /var/log/openvpn.log
```

#CRLの有効化設定を追加

```
crl-verify crl.pem
```



OpenVPNサーバーの起動

1. ブリッジの作成

- # cd /etc/openvpn
- # ./bridge-start

2. ブリッジの確認

- # brctl show
 - eth0とtap0がbr0に接続されていることを確認
- # ifconfig

3. OpenVPNサーバーの起動

- # service openvpn start



OpenVPNクライアントの設定

1. OpenVPNクライアントのインストール
2. クライアント証明書を作成
3. 各種証明書関連ファイルのコピー
4. クライアント設定ファイルを作成



OpenVPNクライアントのインストール

- OpenVPN GUI for Windows
 - <http://openvpn.se/>
- Tunnelblick
 - Mac OS X用OpenVPNクライアント
 - <http://code.google.com/p/tunnelblick/>



クライアント証明書を作成

1. CAの準備

- # cd /etc/openvpn/easy-rsa
- # source vars

2. クライアント証明書を作成(client1用)

- # ./build-key-pass client1
- パスフレーズを2回入力する
- [y/n]が聞かれたら、yを入力(2回)
- keysディレクトリにclient1.crtとclient1.keyが作成される



各種証明書関連ファイルのコピー

1. 認証に必要となる証明書関連ファイルをクライアントにコピー
 - 保存先は"C:¥Program Files¥OpenVPN¥config"
 - CA証明書
 - ca.crt
 - 静的暗号鍵
 - ta.key
 - クライアント証明書
 - client1.crt
 - client1.key



クライアント設定ファイルの例

```
pull
tls-client
dev tap
proto tcp-client
remote 接続先アドレス 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
ns-cert-type server
tls-auth ta.key 1
comp-lzo
verb 3
```

- ca CAの証明書
- cert クライアント証明書
- key クライアント秘密鍵
- tls-auth 静的暗号鍵 1
 - クライアントには1を設定
- 接続先アドレスはホストOSのNICに割り当てられたIPアドレス



その他の設定の意味

- proto
 - 使用するプロトコルを指定。UDP、またはTCPが選択できる。サーバーに合わせる。
- ns-cert-type server
 - サーバー証明書作成時に "nsCertType=server"と設定されていないサーバーと接続しない
 - build-key-serverスクリプトでは設定される



VPN接続の確認

1. Windowsクライアントのトレイアイコンを右クリックし、「Connect」を選択
2. 接続時のログは「View Log」で確認可能
3. サーバー・クライアント間でPING確認

