# OpenVPNを使ったテレビ会議活動

2006/11/18

京都大学東南アジア研究所
木谷　公哉

kitani@cseas.kyoto-u.ac.jp

# テレビ会議システムって？

- 個人ベースの場合

  単体では数名レベル

  - 機材：PCにウェブカメラをつけ、後はソフト使えばいい。

    Skypeなどはセキュリティをほぼ無視できるので・・・いいのか？
    オンラインになってないと使えないよねー。接続確認の信憑性は？
    帯域制御できないよねー

- 会場ベースの場合

  単体で数十人以上の場合

  - 機材：ハードウェアを使うのがベスト。いずれにしても音声をいかにうまく拾えるか考えないと・・・。

    念のためソフトでつかえるものもほしいよな。
    帯域制御できるやつがいいな

# そこそこの会議で必要なのは？

- 機材運びと配置

  音響、映像、LAN、電源いずれもながーいケーブル必要！
- スケジュール調整

  国が違えば「時差」という大敵も！
- 人員配置

  人・・・意外と必要です
  - ネットワーク、テレビ会議機材、搬入・搬出、セッティング
  - プレゼン操作、相互連絡とか・・・・
- ネットワーク

  双方向通信ですから、双方の会場での調整が必要

# テレビ会議実体験

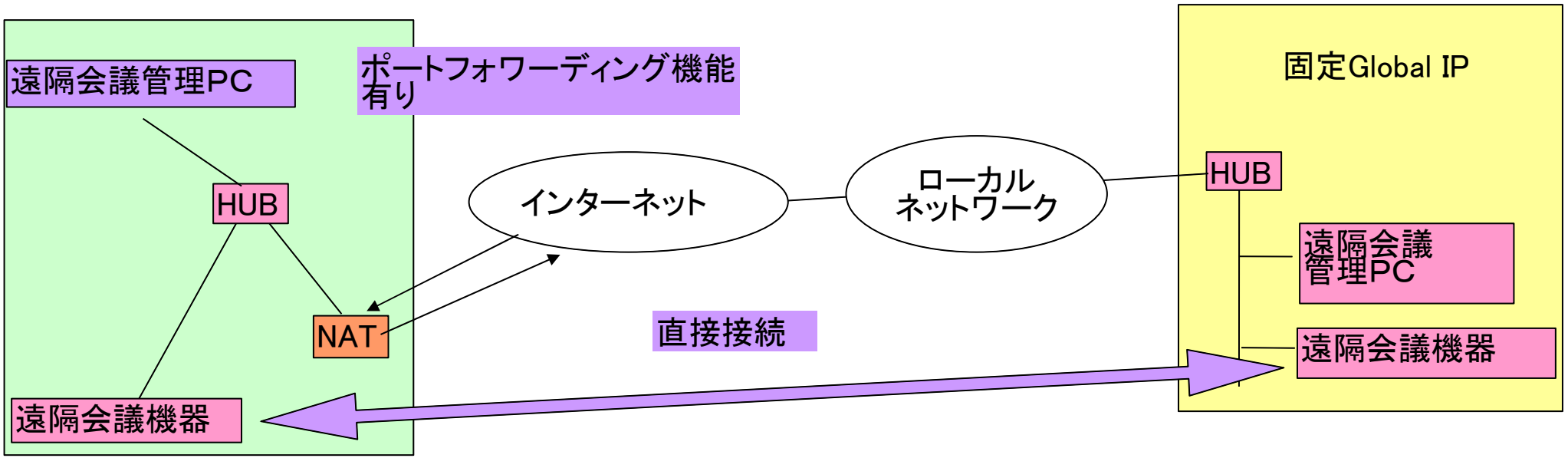
- 2006年6月　初めてのテレビ会議、さてどこから？ とりあえず機材購入必要だよね？
- 2006年7月　とりあえずベトナム、タイと日本間の接続実験に参加。VPNの必要性を痛感する
- 2006年8月　VPNをどう設計するか考え、テスト構築。いろいろためしてみる。
- 2006年9月中旬　29日のバンコク側開催場所のNATルータ破損連絡あり。期日までに交換予定だが、VPNが絶対必要だと感じる。
- 2006年9月20日　OpenVPNサーバを立ち上げ、試してみる。
- 2006年9月25日　連絡用IRCサーバ立ち上げ（一時利用）、OpenVPNサーバとクライアントのテストが一応終了。
- 2006年9月27日　バンコクに到着。交換されたNATルータにポートフォワーディング機能なし！ この時点でVPN接続することに決めた。
- 2006年9月29日　タイのバンコクと京大間でワークショップ。発表者はタイ側。冗長性の必要性を痛感する
- 2006年10月　冗長構成の設計と構築。一人で両側をある程度マネージメントできるように。
- 2006年11月10日　ベトナムのホテルと大阪市立大学学術情報総合センター10周年記念会場とちょろっと接続
- 2006年11月11日　ベトナムのホテル（GIS IDEAS2006国際会議）と京大時計台（京都大学国際シンポジウム）。

# なぜVPNが必要なの？

- 会場のセキュリティポリシー問題
  - 特定ポートを通過させてもらえない
    - FIREWALLやNAT設定変更不可
  - ウェブ認証が必要
    - 直接ハードを接続できない（PCで認証必要？）
  - 物理的に無理
    - ポートフォワーディングやUPnPなどの機能がないNATルータ
    - 多段NATルータで、どこまで対応してるかわからない
- 意思疎通できてる？　ー初めてのケースー
- イレギュラーな事態に巻き込まれる場合もある
  - ネットワークの故障、手違い

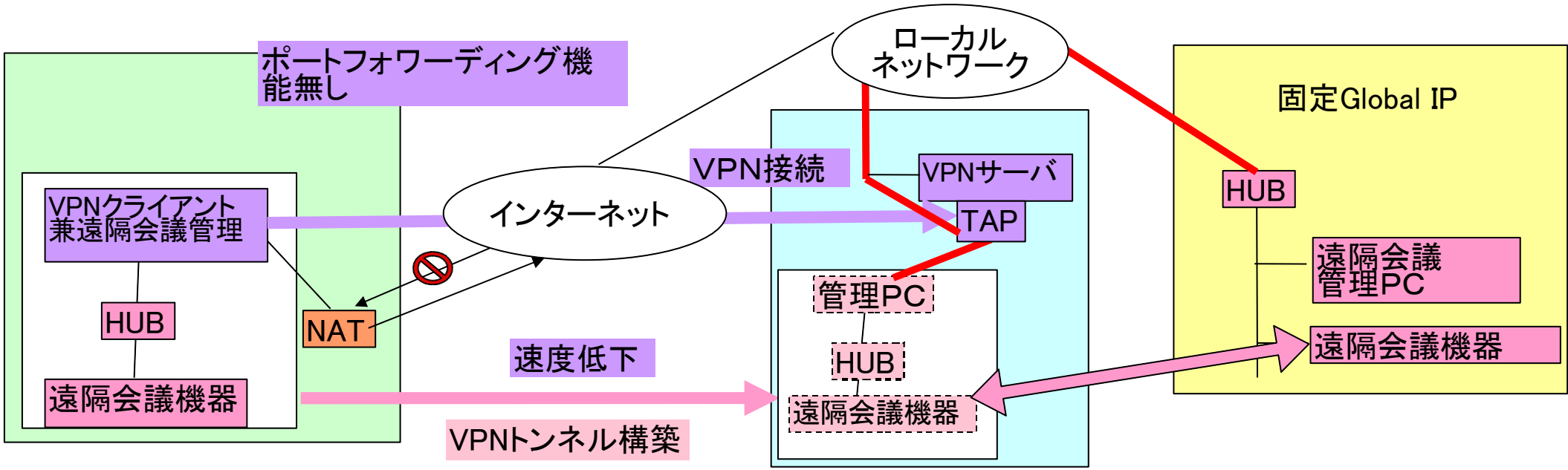
# ネットワーク構成（１）

- 方法1：　両側固定グローバルIP環境で直接接続する。（NATのポートフォワーディング機能を利用してもよい）



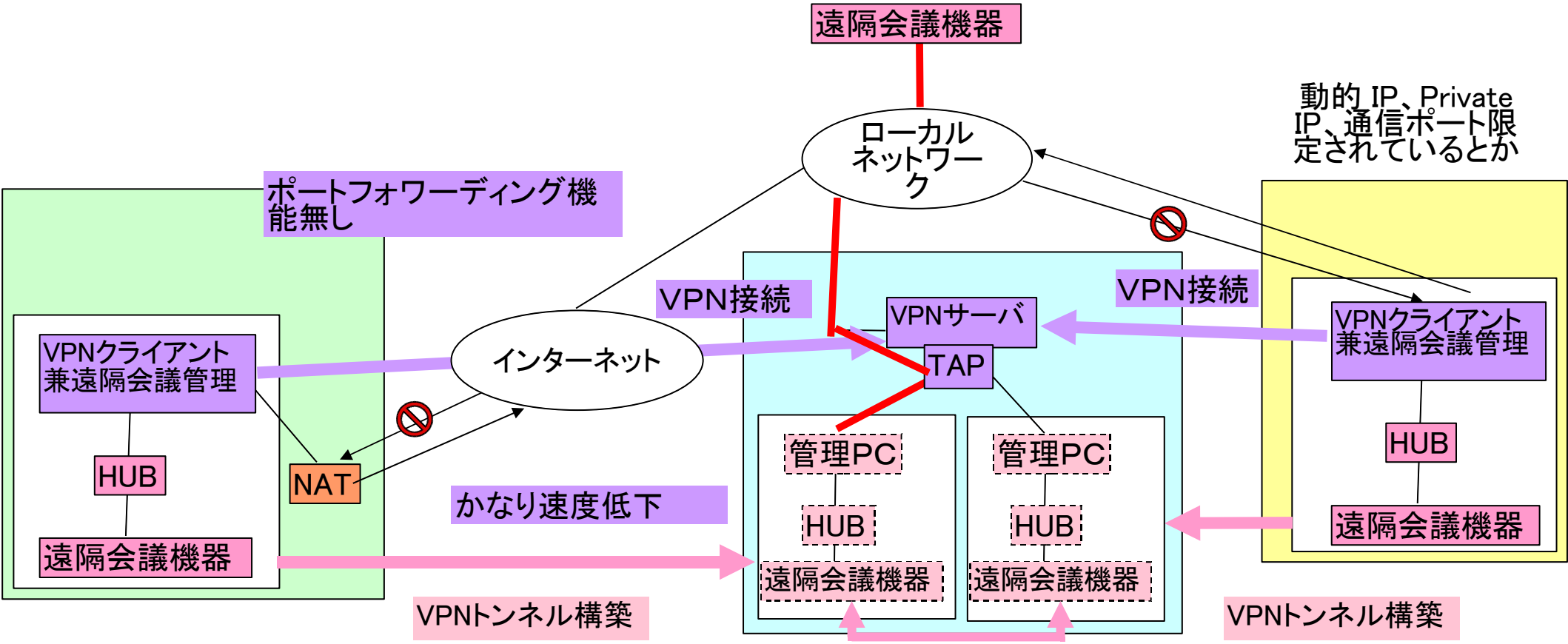
# ネットワーク構成（2）

- 方法2:　片側をVPN接続する

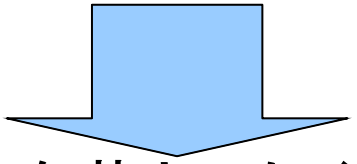


# ネットワーク構成（3）

- 方法3:　両側**VPN**接続する



# なんでOpenVPNなの？
## わがままな要求を満たせるのか！？



- 出来るだけ通信速度を落としたくない

  TCP over UDPがしたいよな
- 短期間でものにできるようにしたい

  与えられている時間、予算、機材が乏しい

  複雑な設計・設定は、構成理解とセットアップ、テストするまで時間かかるので却下。
- 短期使用とはいえ、一定のセキュリティは保ちたい
  - 接続のためのセキュリティだけでいい。
  - データは非暗号で十分
- ２、３ヶ月はテストしたい
- ブリッジ構成にしたい

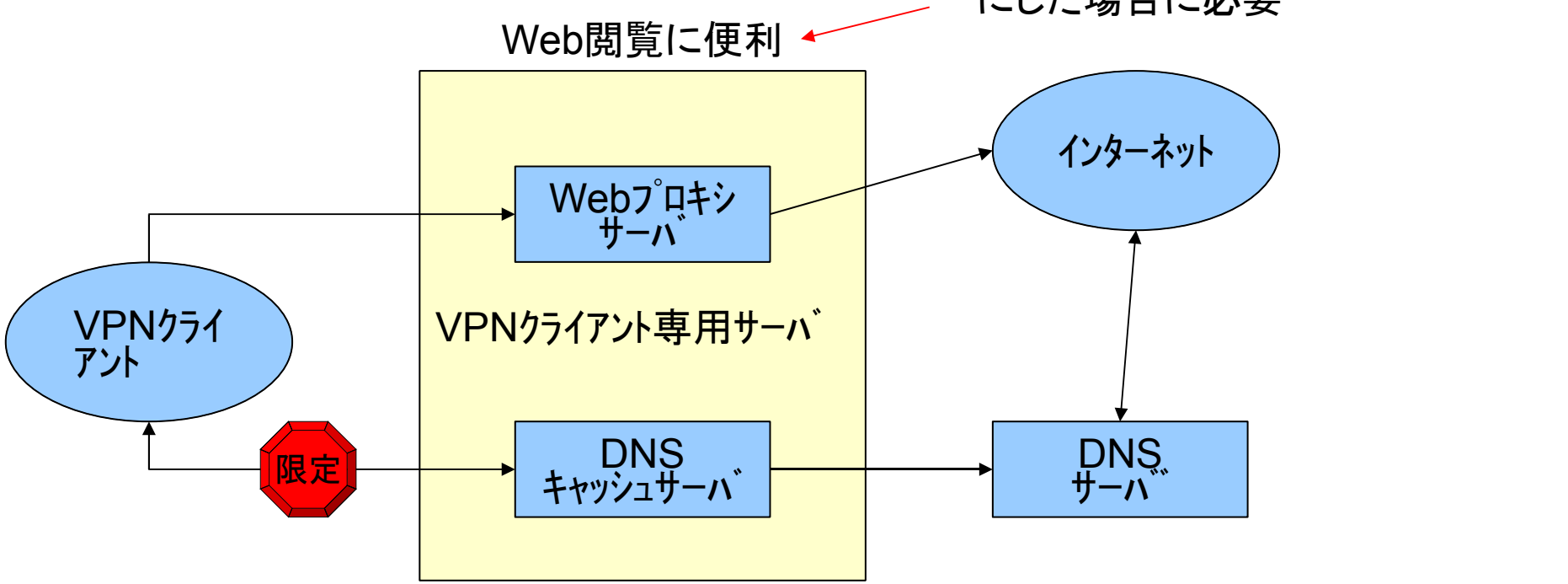
  できれば各種情報をクライアントに自動付与でしたいが・・・

# なんでOpenVPNなの？

## OpenVPNがｸﾗｲｱﾝﾄに自動付与できる情報

- ルーティング情報
- DNS情報
- TAPへのIP付与

  ブリッジ構成時は手動で設定必要
- WINS情報



バンコク事務所で哀愁漂う人形・・・・

日本から見るとこんな感じ
UP: 512kbps/ADSL, VPN接続

日本側だけでごちゃごちゃあるよ・・・

９月の日本側のワークショップ会場

2006.7.26　ベトナム側会場視察

とりあえず細長い会場だということはわかった・・・。でも使われていたので詳しくは・・・。

2006.11.11 こんな感じになった。

9月ワークショップ日本側

日本側はGlobal IP, バンコク側はVPN接続

帯域：256kbps

音声はクリアだが、映像は平均2秒、もっとも遅くて5秒程度のタイムラグ

バンコクから聴いて見た動画

9月ワークショップバンコク側


11月のシンポジウム（ベトナム側）
ベトナム側1Mbps/512kbps /ADSL専用回線

両側ともGlobal IP

帯域：384kbps

音声クリア、映像もほぼリアルタイム


双方のプレゼン画面を時々映像配信して同期

ベトナムから聴いて見た動画

11月のシンポジウム（日本側）
プレゼンの手動同期

税関で止められちゃった
ホテル出るとき、Please check out!と叫ばれた
15kg超えてたような。一人で持てる限界・・・。


VPN接続（ブリッジ構成）

# 意外と使えるOpenVPN

- WinXPならばサーバ、クライアント構築に1時間もかからない

  一度設定ファイルを作ってしまえば

  各種スクリプトも充実している

- そこそこのマシンでも安定稼動する

  １，２週間起動させっぱなしでも問題ない

- SFTP転送では、0.6倍程度の速度低下で済む
- ちょっとした設定でセキュリティもそれなりの強度になる。

# 参考URL

- 日本語翻訳
  http://freescitech.net/2/ovpn2_howto_ja.html

  セキュリティ強化
  - SSL認証（不正アクセス防止）
  - Tls-authによるHMAC署名（妨害防止）
  - "Man-in-the-Middle"攻撃の防止（成りすまし防止）

  障害対策
  - 負荷分散/障害迂回のための設定
- パターン例
  「OpenVPNで構築するリモートアクセス環境」で検索
  図を用いた概要や技術情報について取りまとめてある。

# OpenVPN実際の設定

# 即席OpenVPNサーバ例（ハード）WinXPの場合

- BIOS設定

  毎日深夜か早朝に電源オンに設定

  停電後の復電時の電源オン

- イーサネット二枚ざし

  1つは、ローカルネットから出られなくていい。リモートアクセスによるリモート管理のためだけ。

  特定IPからのみ、特定ポートのみを許諾するようさらに制限かけとけばいい。

- Firewallで必要なポートだけを許可する

  1194/udp だけとか。ICMPも通す必要はないけれど・・

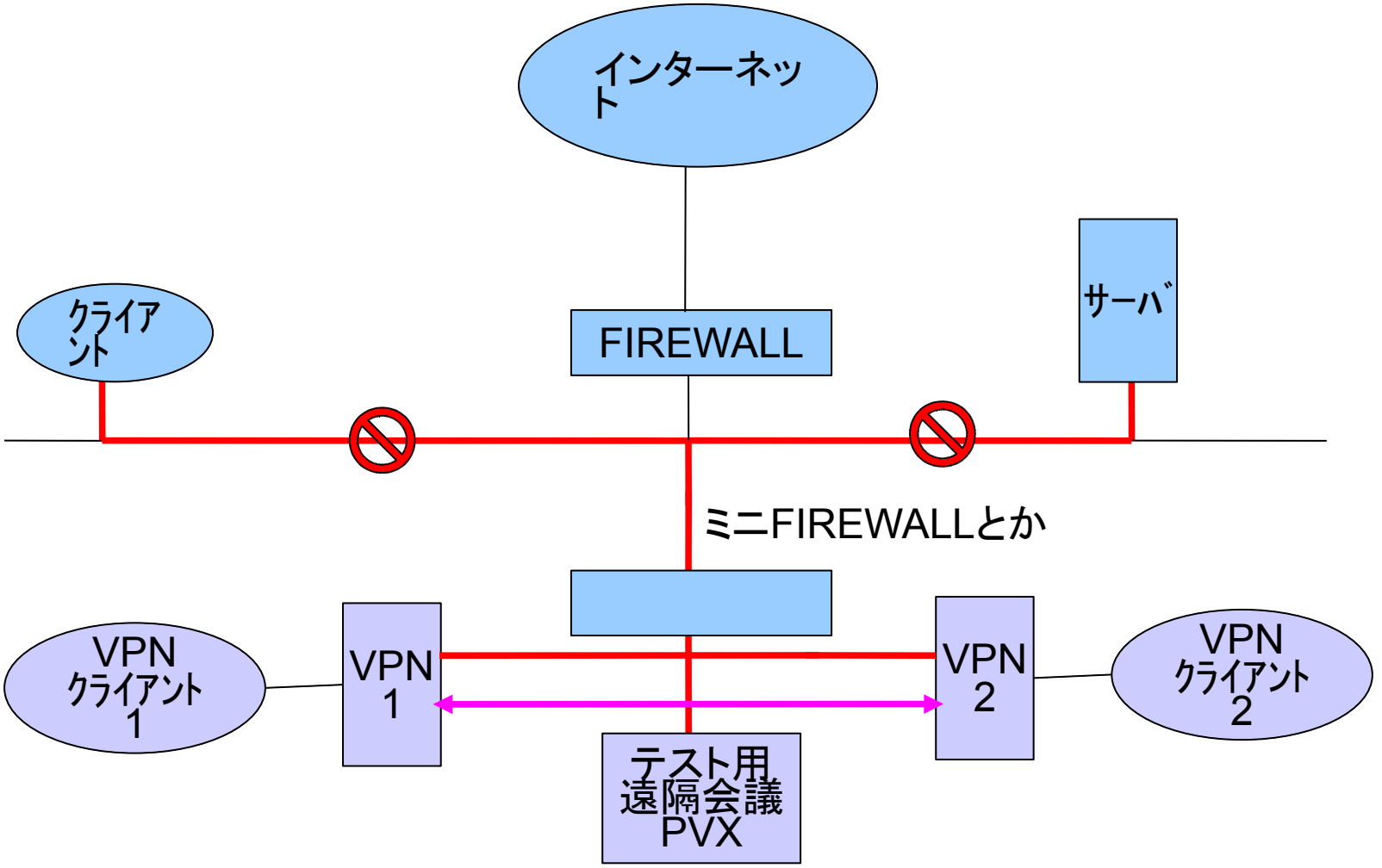
- 二つサーバ用意して相互補完する

  冗長性以外にサブに接続して、メインの2つ目のイーサネットを通じてメインをコントロールしたりとか。

# 即席OpenVPNサーバ例（ソフト）

- OpenVPNを自動起動させる。
- ソフトレベルのFirewallを入れて、OpenVPNが使うUDPポートのみあけておく
- TAPと外部ネットへの接続イーサネットをブリッジ接続する。
- 何日か動作させておいてもこけないかどうか、何度かチェック

# ローカルネットワーク構成例




互いにリモートアクセスできるように

# OpenVPNサーバ設定

- port 1194
- proto udp
- dev tap
- dev-node tap-win32
  TAPﾃﾞﾊﾞｲｽ名
- ca ..\\easy-rsa\\keys\\ca.crt
- cert ..\\easy-rsa\\keys\\server.crt
- key ..\\easy-rsa\\keys\\server.key
- dh ..\\easy-rsa\\keys\\dh1024.pem
- ifconfig-pool-persist ipp.txt
  clientのIP情報。
- push "redirect-gateway"
  通信経路をVPN接続先へ振る
- push "dhcp-option DNS AAA.BBB.CCC.FFF"
- server-bridge Server-IP Server-Netmask Client-Start-IP Client-End-IP

client-to-client
keepalive 10 120
persist-key
persist-tun
status openvpn-status.log
log  openvpn.log
log-append  openvpn.log
tls-auth ..\\easy-rsa\\keys\\ta.key 0
- UDPに署名

comp-lzo
- 圧縮

verb 3

# OpenVPNクライアント設定

- client
- dev tap
- dev-node tap-win32
  TAPﾃﾞﾊﾞｲｽ名
- proto udp
- remote AAA.BBB.CCC.DDD 1194
  remote AAA.BBB.CCC.EEE 1194
  ｻｰﾊﾞが複数ある場合は列挙
- resolv-retry infinite
- nobind

persist-key
persist-tun
ca ca.crt
cert client3.crt
key client3.key
ns-cert-type server
- ｻｰﾊﾞ証明確認

tls-auth ta.key 1
- UDPに署名

comp-lzo
- 圧縮

verb 3

# OpenVPNサーバで証明書作成

- インストールディレクトリ内の east-rsaを開く


1. clean-all.bat
   index.txt, serial. を生成
2. init-config.bat
   vat.bat, openssl.cnf作成
3. var.batの編集と実行
   簡単な環境変数。以下のバッチを動作させるために必要。
4. build-ca.bat
   CA作成
5. build-key-server.bat  server
   サーバ証明書作成
6. build-key.bat client1
   クライアント証明書作成
   出来たもの client1.key, client1.crtと、ca.crtをクライアントに渡せばいい。