# 京都大学における IKEv2 サービスの構築

針木 剛 [1)]

1) 京都大学 企画・情報部

hariki.tsuyoshi.3r@kyoto-u.ac.jp

# IKEv2 service construction in Kyoto University

HARIKI Tsuyoshi[1)]

1) Information Dept., Kyoto Univ.

**概要**

京都大学では新たな VPN サービスとして IKEv2 サービスを開始した。サービス開始にあたり幾つかの VPN 技術を比較検討し IKEv2 の新サービス構築を選択した。本稿では構築時の技術課題とその解決のために得られた知見の情報共有を目的として詳細内容をまとめる。

## 1 はじめに

現在京都大学では学外からの安全な通信経路の提供を目的として幾つかの VPN サービスを提供している。VPN サービスを提供し始めた 2005 年度当時 Windows 端末で安定動作が可能であった PPTP サービスを選択し、学内限定の事務手続きサイトや接続元が大学の IP アドレスに限定される電子ジャーナルの閲覧など多くの教職員や学生など学内関係者に利用されてきた。

一方で PPTP 接続時の GRE プロトコルが利用者環境によって制限されている場合もあり、その代替策として 2012 年度に TCP のみで利用できる SSTP サービス及び OpenVPN サービスを開始した。

その後 PPTP サービスは安定運用を継続しながら、研究室や事務室などの閉じた VLAN(以下研究室 VLAN とする) へ直接接続できる機能や国立情報学研究所 (NII) のクライアント証明書による TLS 認証に対応する機能 [1] の追加など適宜改善を行い、2015 年度には年間 220 万件を超える接続数があり大学として不可欠な情報サービスに成長した。しかしながら Apple 社が 2016 年 9 月に提供する新しい iOS や macOS で PPTP を非サポートとする通知があり、これに伴い PPTP に代わる新たな VPN サービスの検討を行った。

## 2 学内ネットワーク環境

京都大学では図 1 にあるように学内関係者が研究室 VLAN でパソコンやプリンタを利用するためのプライベートアドレス「KUINS-III」と、学外への通信や学外公開のためのグローバルアドレス「KUINS-II」を運用している。教職員は希望に応じて「KUINS-DB」[2] と呼ばれる Web フォームからそれらを利用申請し、申請内容を保存したデータベースの内容を適宜ネットワーク機器の設定に反映することで運用を行っている。また大学を地理的に 10 構内に分割し各構内にメインの L3 スイッチを配置し大学全体を束ねるルータでそれぞれのルーティングを管理する構成となっている。各構内で利用する VLAN 数が多いため構内メインの L3 スイッチごとに独立した VLAN 番号を割り当てている。そのため VLAN 番号とは別に学内で一意の値となる「VLAN 管理番号」を別途割り当てて「KUINS-DB」で管理している。

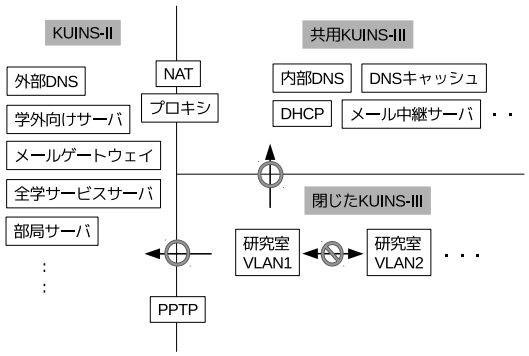


図 1 京都大学 IP アドレス利用

図 1 にあるように PPTP サーバは複数の NIC で、学外から接続を受け付けるための KUINS-II と

PPTP クライアントに割り当てる KUINS-III、さらに一部の各研究室 VLAN の KUINS-III を持っている。PPTP サーバで研究室 VLAN へ接続したい利用者は「KUINS-DB」から当該 VLAN に接続可能な全学アカウントを登録申請し、その情報を定期的に PPTP サーバに反映している。

## 3　VPN サービス比較検討

PPTP 代替サービスを検討するため、現在提供中のサービス PPTP、SSTP、OpenVPN に加えて新たに L2TP/IPsec、IKEv2 を対象にそれぞれの優位点の比較を行った。

表 1 に利用者のネットワーク環境で通す必要のあるプロトコルやポート番号をまとめた。PPTP は GRE が必要となるため利用者環境で制限されている場合があり、そのような利用者の受け皿として TCP だけで動作する SSTP と OpenVPN という位置付けでサービス提供をしている。L2TP/IPsec と IKEv2 は IPsec であるため ESP が必要だがこれは UDP/4500 で代替可能である。

表 1　VPN に必要なプロトコルやポート番号比較

| | |
|---|---|
| PPTP | △ (1703/TCP と GRE) |
| SSTP | ◎ (443/TCP) |
| OpenVPN | ○ (1194/UDP または TCP) |
| L2TP/IPsec | ○ (500/UDP と (ESP または 4500/UDP)) |
| IKEv2 | ○ (500/UDP と (ESP または 4500/UDP)) |

また表 2 に標準 OS での対応一覧をまとめた。利用者の手間を最小限にするために極力クライアント OS 標準対応しているものが望ましい。SSTP と OpenVPN は標準 OS でのサポートが不足しており、メインではなく従来通り補助的なサービスとしての提供すべきと判断した。

表 2　VPN クライアント OS 標準対応比較

| | Windows | macOS | iOS | Android |
|---|---|---|---|---|
| PPTP | ○ | × | × | ○ |
| SSTP | ○ | × | × | × |
| OpenVPN | △*1 | △*1 | △*1 | △*1 |
| L2TP/IPsec | ○ | ○ | △*2 | ○ |
| IKEv2 | ○ | ○ | ○ | △*1 |

*1 別途アプリが必要 *2 クライアント証明書認証不可

また macOS と iOS では標準が IKEv2 に変わり一方で L2TP/IPsec は iOS でクライアント証明書非対応のままである点から、今後は IKEv2 を推奨するように見える。比較的新しいプロトコルのため Android は標準非対応だが将来的な対応を期待して IKEv2 を選択した。

## 4　システム構築

### 4.1　システムの動作詳細

新規構築する IKEv2 サービスでのネットワーク利用方法を図 2 に示す。利用者のクライアント PC から IKEv2 サーバの KUINS-II へのアクセスに対し、IKEv2 サーバは自サーバ内の radius サービスに問い合わせ全学アカウントとパスワード認証または NII のクライアント証明書認証を行い、承認されるとクライアント PC に KUINS-III アドレスを割り当てる。

IKEv2 サーバでは予め割当 KUINS-III のセグメントに対し下記のようなルーティング及び NAT を設定しておく。

- 学外へのアクセスは KUINS-II の NIC を経由し SNAT して接続
- 学内へのアクセスは KUINS-III の NIC を経由してそのまま接続

これにより学外へは KUINS-II、学内へは割当 KUINS-III からのアクセスとなる。

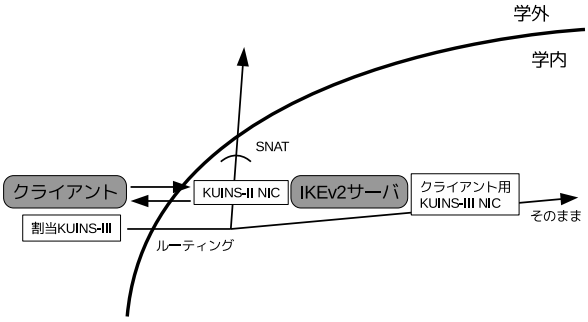


図 2　一般的なネットワーク利用方法

また図 3 に IKEv2 サービスで研究室 VLAN への接続を試みた場合のネットワーク利用方法を示す。利用者は全学アカウントに VLAN 管理番号を付与した ID により認証を行う。radius サービスで承認され、なおかつ KUINS-DB から定期的に取得している ID と VLAN 許可リストに符合した場合には、当該クライアント KUINS-III に限り以下のようなルーティングに変更する。

- 学内へのアクセスは研究室 VLAN の KUINS-III の NIC を経由して SNAT して接続

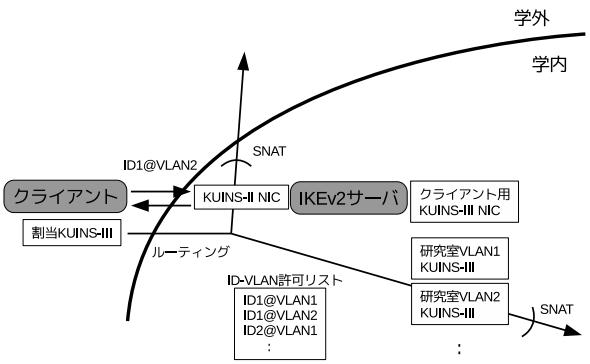


図 3　研究室 VLAN 接続のネットワーク利用方法

ここで利用者に対し各研究室 VLAN の KUINS-III ではゲートウェイアドレスを含む幾つかの IP アドレスが利用不可である旨通知済みである。研究室 VLAN のブロードキャストアドレスの 2 つ前も利用不可としたアドレスの 1 つで、このアドレスを事前に IKEv2 サーバに割り当てておく。予め送信元アドレスが割当 KUINS-III でこのインターフェースから出力されるパケットは SNAT するような設定としておく。これにより学外へは一般利用と同様の KUINS-II だが、学内へは研究室 VLAN のブロードキャストアドレスの 2 つ前の KUINS-III に変換されアクセスするようになり、当該研究室 VLAN への接続が可能となる。また当該研究室 VLAN のネットワークアドレスに制限された各種電子リソースへのアクセスも可能となる。

### 4.2　サーバのシステム構成と各種設定

構築した IKEv2 サーバのシステム構成を表 3 に示す。全て RHEL7 標準または EPEL 拡張パッケージを用いて構成している。

表 3　IKEv2 サーバのシステム構成

| 機能 | ソフトウェア名 | バージョン |
|---|---|---|
| OS | Linux | 3.10.0 |
| IKEv2 | strongswan | 5.4.0 |
| radius | freeradius | 3.0.4 |
| ルーティング | iproute2 | 3.10.0 |
| SNAT と | iptables | 1.4.21 |
| IP フォワード | firewalld | 0.3.9 |

サーバは仮想マシンで構築し KUINS-II、クライアント用 KUINS-III 及び各構内のメインスイッチにより QinQ に集約された研究室 VLAN を引き込み NIC に適切な IP アドレスを設定する。ここで仮の設定例を表 4 にまとめる。ens1 は KUINS-II のグローバルアドレスとして、ens2 はクライアント用 KUINS-III、VLAN 番号が付与された ens3 は研究室 VLAN の KUINS-III アドレスとしている。研究室 VLAN のルーティング名には VLAN 管理番号を使用した。

表 4　ネットワークインターフェース例示

| デバイス | IP アドレス | ゲートウェイ | ルーティング |
|---|---|---|---|
| ens1 | 192.0.2.1 | 192.0.2.254 | gwk2 |
| ens2 | 10.1.0.251 | 10.1.0.254 | gwk3 |
| ens3.1 | 10.2.0.253 | 10.2.0.254 | gw123456 |
| ens3.2 | 10.2.1.253 | 10.2.1.254 | gw123457 |
| : | : | : | : |

デフォルトゲートウェイは KUINS-II のゲートウェイアドレスとしているが各 NIC のゲートウェイも同様にルーティングテーブルに設定する。具体的には設定 1 による。

設定 1　ルーティング設定

```
--/etc/sysconfig/network-scripts/route-ens2--
10.1.0.0/24 dev ens2 src 10.1.0.251 table gwk3
default via 10.1.0.254 table gwk3

--/etc/sysconfig/network-scripts/route-ens3.1--
10.2.0.0/24 dev ens3.1 src 10.2.0.253 table gw123456
default via 10.2.0.254 table gw123456

--/etc/sysconfig/network-scripts/route-ens3.2--
10.2.1.0/24 dev ens3.2 src 10.2.1.253 table gw123457
default via 10.2.1.254 table gw123456

--/etc/iproute2/rt_tables--
200     gwk3
123456 gw123456
123457 gw123457
```

さらにデフォルトのルーティングルールを追加設定しておく。VPN クライアントから学内へのルーティング VPN クライアントのセグメントのゲートウェイに向かうように設定しておく。ここで優先順位はデフォルトのルーティング (32766) よりは高い値に設定するが、新しいルールが上位に追加しやすいようになるべく低い値 (30001) とする。

設定 2　ルーティングルール設定

```
--/etc/sysconfig/network-scripts/rule-ens2--
from 10.1.0.0/24 to [全学内] table gwk3 priority 30001
```

また SNAT の設定も事前に設定しておく。設定 3 の 4 行目最初の設定は VPN クライアントが学外接続するための KUINS-II への変換であり、それ以下は各研究室 VLAN へ接続するための研究室 KUINS-III への変換となっている。

設定 3　SNAT 設定

```
--/etc/firewalld/direct.xml--
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.1.0.0/24 -o ens1 -j SNAT --to-source 192.0.2.1</
        rule>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.1.0.0/24 -o ens3.1 -j SNAT --to-source
        10.2.0.253</rule>
  <rule priority="0" table="nat" ipv="ipv4" chain="POSTROUTING"
        >-s 10.1.0.0/24 -o ens3.2 -j SNAT --to-source
        10.2.1.253</rule>
  :
</direct>
```

次に strongswan を動作させるためのカーネルパラメータを設定 4 のように設定する。

設定 4　カーネルパラメータ設定

```
--/etc/sysctl.conf--
net.ipv4.ip_forward = 1
net.ipv4.ip_no_pmtu_disc = 1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
```

strongswan の設定を設定 5 にまとめる。クライアントの認証は同じサーバ内の radius サービスで行う。freeradius の設定は割愛するが全学アカウントへの LDAP でのパスワード認証と NII クライアント証明書を用いた TLS 認証を設定しておく。TLS 認証の際の注意点として Subject から他大学で発行された証明書は拒否するような設定が必要となる。また strongswan の追加ルーティングは利用しない設定とし、未使用で空となったルールの優先順位も新しく追加するルールのために値を下げておく (30000)。

設定 5　strongswan の設定

```
--/etc/strongswan/ipsec.conf--
conn %default
        keyexchange=ikev2
conn kuins
        auto=add
        left=192.0.2.1
        leftsubnet=0.0.0.0/0
        leftauth=pubkey
        leftcert=[証明書ファイル名]
        leftfirewall=yes
        leftid=[サーバFQDN]
        leftsendcert=always
        right=%any
        rightsourceip=10.1.0.10-10.1.0.250
        rightauth=eap-radius
        rightsendcert=never
        eap_identity=%any

--/etc/strongswan/ipsec.secrets--
: RSA [秘密鍵ファイル名]

--/etc/strongswan/strongswan.d/charon.conf--
charon {
    dns1 = [DNSキャッシュサーバアドレス1]
    dns2 = [DNSキャッシュサーバアドレス2]
    install_routes = no
    routing_table_prio = 30000
}

--/etc/strongswan/strongswan.d/charon/eap-radius.conf--
eap-radius {
    load = yes
    servers {
      server1 {
        address = 127.0.0.1
        secret = [secret]
      }
    }
}
```

最後に接続時と切断時に動作する strongswan の updown スクリプトの up-client にルーティングルール追加の設定 6 を追加する。ここで$USERLIST のファイル内には KUINS-DB で申請された全学アカウント@ VLAN 管理番号の一覧が記述されており、定期的に更新している。これにより$USERLIST に登録済みの ID で認証があった場合は VPN クライアント IP アドレスに対しルーティングルールが新たに追加されその VLAN 管理番号の研究室への接続が可能になる。また down-client には反対にルールを削除するスクリプトを追加しておく。

設定 6　updown スクリプトへの追加

```
#
# VLAN gateway setup
if expr "$PLUTO_XAUTH_ID" : '^.\+@[0-9]\+$' > /dev/null
then
  VLANGW=`grep "^$PLUTO_XAUTH_ID$" $USERLIST | cut -d@ -f2`
  if [ $VLANGW ]
  then
    ip rule add from $PLUTO_PEER_CLIENT to [全学内] lookup
          gw$VLANGW
    logger -t $TAG -p $FAC_PRIO \
      "added ip rule gw$VLANGW from $PLUTO_PEER_CLIENT by
            $PLUTO_XAUTH_ID"
  else
    logger -t $TAG -p $FAC_PRIO \
      "$PLUTO_XAUTH_ID VLAN and ID pair is not valid"
  fi
fi
```

## 5　構築時の問題

今回の構築時に下記の問題が発生し対応した。

- VPN 接続後に特定の学内サイトだけ閲覧不可となる現象が発生し、これは設定 4 のカーネルパラメータ net.ipv4.ip_no_pmtu_disc で Path MTU Discovery を有効にすることで解決できた。特定サイトからのパケットは IKEv2 サーバまで届くことは確認できたため、最後に UDP にのせてクライアントへ届ける際にフレームサイズが大きく届かなかったことが原因かと思われる。
- macOS や iOS クライアントで接続すると 8 分で接続断となってしまう現象が発生したが、これは暗号強度を別途指定していたことが原因で、より強度の高い strongswan のデフォルト値に戻すことで解決できた。

## 6　まとめ

- VPN サービスを比較検討した結果、新たに IKEv2 サービスを選択しシステム構築を行った。
- パスワード認証とクライアント証明書認証の両者をサポートし、更に各研究室 VLAN へ直接接続できる機能も実装した。
- Apple 社の新 OS での PPTP 停止時期にあわせて 2016 年 9 月よりサービスの提供を開始した。

## 参考文献


[1] NII 学術情報基盤オープンフォーラム 2016
「京都大学でのクライアント証明書の利用サービスと学内申請受付システムの紹介」古村隆明 2016 年

[2] 第 34 回全国共同利用情報基盤センター研究開発連合発表会
「京都大学学術情報ネットワークシステム接続機器管理システム（KUINS-DB）の更新」高見好男, 平田光英, 富浦雅雄, 西村知子, 四方敏明, 宮崎修一, 古村隆明, 岡部寿男 2012 年