ネットワーク講習

1 グローバル IP とプライベート IP

インターネットは接続先となる端末の所在を表すため，IP アドレスを用いているが，これはグローバル IP アドレスと呼ばれ世界中のネットワークに割り当てられる．また，グローバル IP アドレスは住所と同じように世界中で重複することはなく，グローバル IP アドレスを割り当てられた端末に対しては，世界中から宛先として通信することが可能である．

ここでは，ネットワークの疎通を確認する ping コマンドを使用してグローバル IP アドレスへの通信を確かめる．例として，小林研究室のグローバル IP アドレスである 158.217.77.225 に対して，ping コマンドを以下のように入力する．

```
# ping 158.217.77.225
PING 158.217.77.225 (158.217.77.225): 56 data bytes
64 bytes from 158.217.77.225: icmp_seq=0 ttl=64 time=2.701 ms
64 bytes from 158.217.77.225: icmp_seq=1 ttl=64 time=3.708 ms
64 bytes from 158.217.77.225: icmp_seq=2 ttl=64 time=3.807 ms
                    :
※終了は ctrl+c
```

ping コマンドの結果を確認するとグローバル IP アドレスに対して疎通確認することができる．

グローバル IP アドレスは，前述した通り世界中で重複することはなく，IP アドレスの割り当て個数は 32 桁の 2 進数で約 43 億のパターンが存在する．しかし，この個数は世界人口約 70 億人に対してインターネットを利用するデバイスが増加し続ける中でアドレスの枯渇が問題となっている．そこで，企業や家庭などの限られたエリアごとにネットワークを構成し，このネットワーク内はグローバル IP アドレスの代わりに，プライベート IP アドレスというものを用いて割り当てを行っている．

プライベート IP アドレスは，企業や家庭内などのローカルなネットワーク内でのみ有効なアドレスであり，各ネットワークごとに所属する端末間で自由にアドレスを設定することができる．これにより，各ネットワークごとに，プライベート IP アドレスを用いることで IP アドレスの割り当て個数を節約できる．しかし，プライベート IP アドレスは自由に設定されるため，インターネット上からは直接参照することができず，また，異なるネットワークに属する端末同士も直接通信することができない．プライベート IP アドレスを使用したネットワーク通信については後述する．

異なるネットワーク同士が通信できないことを確認してもらうため，ping コマンドを使用してプライベート IP アドレスから別のネットワークのプライベート IP アドレスに対して通信可能かどうかを確認する．例として，現在接続されている関西大学のネットワーク（kuwifi）から，小林研究室のネットワークで運用されるサーバである cririn のプライベート IP アドレス 10.1.3.10 に対して，ping コマンドを以下のように入力する．

```
# ping 10.1.3.10
PING 10.1.3.10 (10.1.3.10): 56 data bytes
ping: sendto: No route to host
```

結果を確認すると，宛先が見つからないため，プライベート IP アドレスには直接通信できないことが分かる．

上の例から異なるネットワークに属する端末同士は直接的に通信することができないことを確認したが，これにより，IP アドレスの節約に加え，他のネットワークと隔離されていることを利

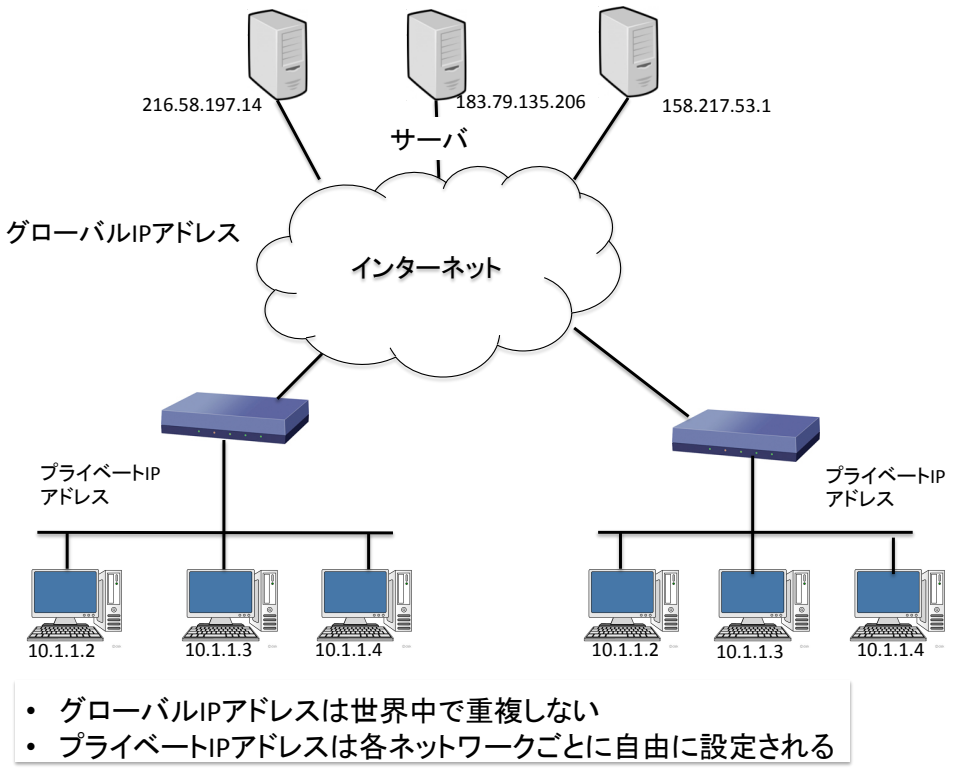

図 1: グローバル IP とプライベート IP

用して，セキュリティの確保を実現することができる．ネットワークを区切ることによる利点として，プライベート IP アドレスで構成されるネットワークは他のネットワークから切り離されるため，意図しないユーザからのアクセスを防ぐことができる．さらに，ネットワークに侵入する通信をファイアウォールなどを用いてフィルタリングすることで，ネットワーク全体のセキュリティを確保することができる．

2 ルータ

上の説明において，異なるネットワーク同士は直接通信できないと説明した．しかし，異なるネットワークであるはずのグローバル IP アドレスに対して ping コマンドにより疎通を確認することができた．また，私たちは日常においてインターネットを使用する際，無線 LAN などから設定されたプライベートアドレスを用いて，インターネット上に存在する Web サイトなどの Web サービスを利用している．これらのネットワークを越える通信はルータによって実現される．ルータは異なるネットワーク間においてデータを中継する機器であり，インターネットに接続されるルータは外側にグローバル IP アドレス，内側にプライベート IP アドレスを割り当てられる．このルータを用いることで，複数のネットワークで構成されるインターネット上においても，ルータが通信経路を中継することで目的の端末までデータを届けることができる（図 2）．こういった仕組みから，私たちはインターネット上の離れたネットワークに存在するサービスを利用することができる．実際に通信経路を確認するため，例としてネットワーク経路を調べる traceroute（tracert）コマンドを使用して関西大学のサーバまでの経路を確認する．

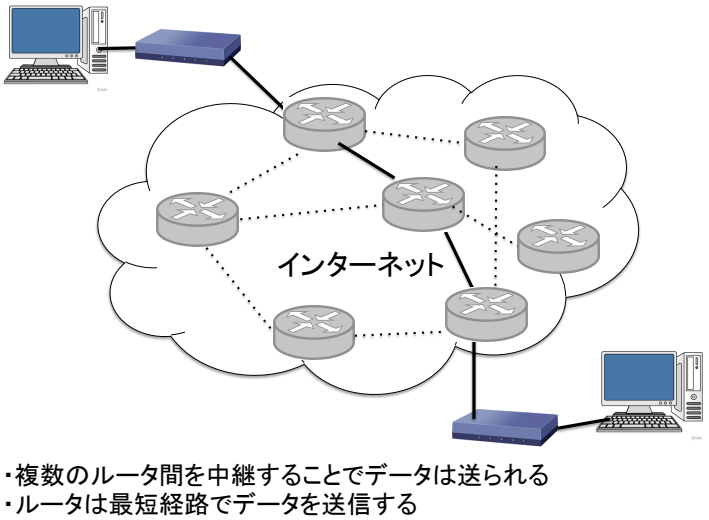

図 2: ルータによるデータの転送

Mac は以下のコマンドを入力する.

```
# traceroute sh.edu.kutc.kansai-u.ac.jp
traceroute to sh.edu.kutc.kansai-u.ac.jp (158.217.53.13), 64 hops max, 52
byte packets
 1  witccnt003.itc.kansai-u.ac.jp (172.29.70.203)  2.003 ms  0.975 ms  0.960
 ms
 2  172.29.143.254 (172.29.143.254)  2.111 ms  2.154 ms  2.371 ms
 3  158.217.103.254 (158.217.103.254)  3.114 ms  3.504 ms  2.996 ms
 4  172.17.5.240 (172.17.5.240)  4.834 ms  4.463 ms  4.421 ms
 5  158.217.4.1 (158.217.4.1)  4.249 ms  3.509 ms  3.742 ms
 6  sh.edu.kutc.kansai-u.ac.jp (158.217.53.13)  2.920 ms !Z  2.992 ms !Z
 4.961 ms
```

windows は以下のコマンドを入力する.

```
> traceroute sh.edu.kutc.kansai-u.ac.jp
sh.edu.kutc.kansai-u.ac.jp[158.217.53.13] へのルートをトレースしています
経由するホップ数は最大 30 です：
1     1ms    3ms     2ms   witccnt003.itc.kansai-u.ac.jp [172.29.70.203]
2     2ms    5ms     1ms   172.29.143.254
3     3ms    2ms     3ms   158.217.103.254
4     9ms    4ms     4ms   172.17.5.240
5     3ms    3ms     4ms   158.217.4.1
6     3ms    3ms     4ms   sh.edu.kutc.kansai-u.ac.jp [158.217.53.13]
トレースを完了しました。
```

traceroute（tracert）コマンドの結果から，宛先までの経路が中継されていることが確認できる.

3 ドメイン情報

前の説明で宛先に関西大学のドメインを指定したように，インターネット上のサービスを利用する際は IP アドレスを指定するより，アドレスに対応付けられたドメイン名を使用することが一般的である．また，このドメインについては，whois サービスにより所有先の情報を調べることができる．whois サービスは，登録者情報，ネームサーバホスト情報，担当者情報などを確認することができる．また，代表的なものとして，ANSI（ `http://whois.jprs.jp/` ）や JPRS（`http://whois.ansi.co.jp/`）などが Web サービスを提供している．(Unix 系 OS の場合，whois コマンドを使用することでも検索することができる．)

ドメイン情報を調べる whois サービスの検索方法を説明する．まず，インターネットブラウザから JPRS を検索し，検索結果から JPRS WHOIS /JPRS を選択する（図 3）．次に，ドメイン名登録情報検索に検索キーワードとして，関西大学のドメインである kansai-u.ac.jp を入力し，検索ボタンを押下する（図 4）．検索結果からドメインの登録情報を確認することができる（図 5）．

図 3: JPRS の検索

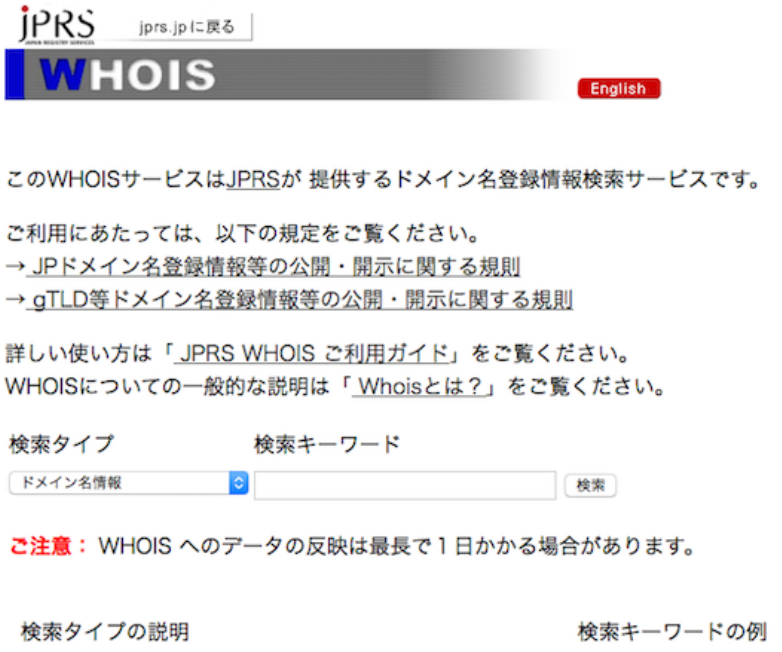

図 4: ドメイン名登録情報検索

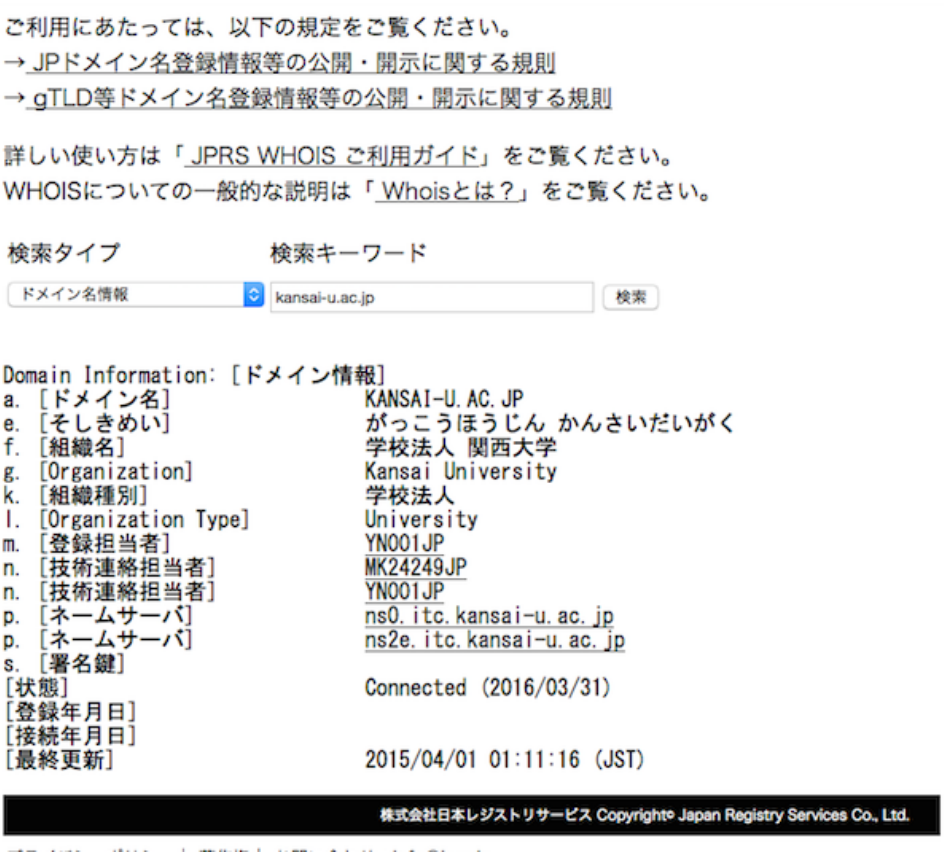

図 5: ドメイン情報結果

4 NAT と NAPT

ここでは，ルータの機能としてグローバル IP アドレスとプライベート IP アドレスの通信について説明する．

前述の IP アドレス枯渇問題から，プライベート IP アドレスの割り当てを説明したが，グローバル IP アドレスが振られるインターネット側からは，プライベート IP アドレスを認識することはできない．そこで，グローバルネットワークとプライベートネットワークの通信を可能にするため，ルータの NAT（Network Address Translation）機能を用いている．インターネットに繋がるルータには，外側にグローバル IP アドレス，内側にプライベート IP アドレスを割り当てられているが，NAT はこのグローバル IP アドレスとプライベート IP アドレスの変換を行う．

NAT の仕組みとして，プライベート IP アドレスが割り振られた端末が，インターネット上のグローバル IP アドレスと通信を行う場合について説明する．

まず，プライベート IP アドレスから送信があった場合，ルータは送信元となるプライベート IP アドレスはルータの外側にあるグローバル IP アドレスに変換する．そして，送信元がグローバル IP アドレスとなったデータは，インターネット上の宛先へと送信される．次に，インターネット上から送信元に対して返信があった場合は，変換された送信元であるルータの外側のアドレスに対して返信される．そして，返信を受け取ったルータは送信先を本来の送信元であるプライベート IP アドレスに転送することで，インターネット上との通信を可能にする．

このように，ルータが中継となってアドレスを変換することで，プライベート IP アドレスとグローバル IP アドレス間で通信を行うことを可能にする（図 6）．

しかし，NAT でのアドレス変換は一つのグローバル IP アドレスに対して，一つのプライベート IP アドレスを対応づけるため，グローバル側との通信は一つの端末のみに限られてしまう．そこで，NAT 機能の拡張として NAPT（Network Address Port Translation）の機能が用いられる．NAPT は，一つの端末しか接続できない問題に対応するため，ポート番号を用いる．ポート番号はサーバが提供するサービスを識別する番号である．このポート番号を端末ごとに割り当て，番号をもとに宛先の端末を識別することで，ポート番号を利用して複数の端末により通信を行うことが可能となる．

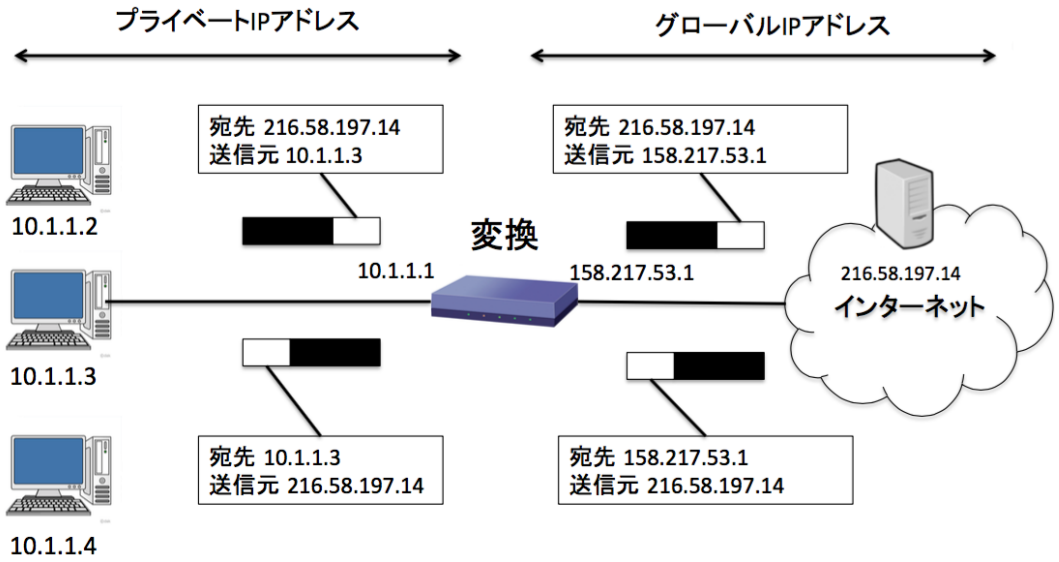

図 6: NAT によるアドレス変換

4.1 DHCP

ここまで，プライベート IP アドレスを利用した技術の説明をした．プライベート IP アドレスの使用に伴い，ネットワークで管理される端末数も増加し，IP アドレスの管理も大変になる．しかし，日常生活で利用する際に IP アドレスを設定する機会はほとんどない．多くの場合，実際の IP アドレスの設定は DHCP（Dynamic Host Configuration Protocol）により行われる．また，設定機能を持った機器を DHCP サーバと呼ぶ．これは，IP アドレスや DNS などのネットワーク情報を持っており，ネットワークに接続した端末に対して設定情報を提供する．また，端末がネットワークから離脱すると DHCP リソースを更新する．このように DHCP は，IP アドレスの割り当てなど，ネットワーク情報を自動的に管理することができる．

5 VPN（Virtual Private Network）

自宅など，外部のネットワークからゼミ内のプライベート IP アドレスが割り振られているマシンなどを操作する場合はネットワークが異なるため，直接的に利用することはできない．そこで VPN という技術を用いることで，異なるネットワーク同士を仮想的に同一のネットワークに属しているように見せかけ，異なるネットワークの端末と通信することができるようになる．

VPN による通信の仕組みとして，トンネリングによりネットワークを繋いでいる．トンネリングでは，もとの通信内容にヘッダが加えられ，加えられたヘッダにより通信内容はカプセル化される．このカプセル化を用いることで接続元でカプセル化を行い，接続先でカプセル化を解除し通信内容を取り出すことで，ネットワーク同士をトンネルで繋いだように見立てて使用することが可能となる．さらに，データをカプセル化する際は，データを暗号化することで安全にネットワークを越えて通信することが可能となる（図 7）．VPN で利用されるプロトコルには，IPsec/PPTP/L2TP/L2F/MPLS などがある．

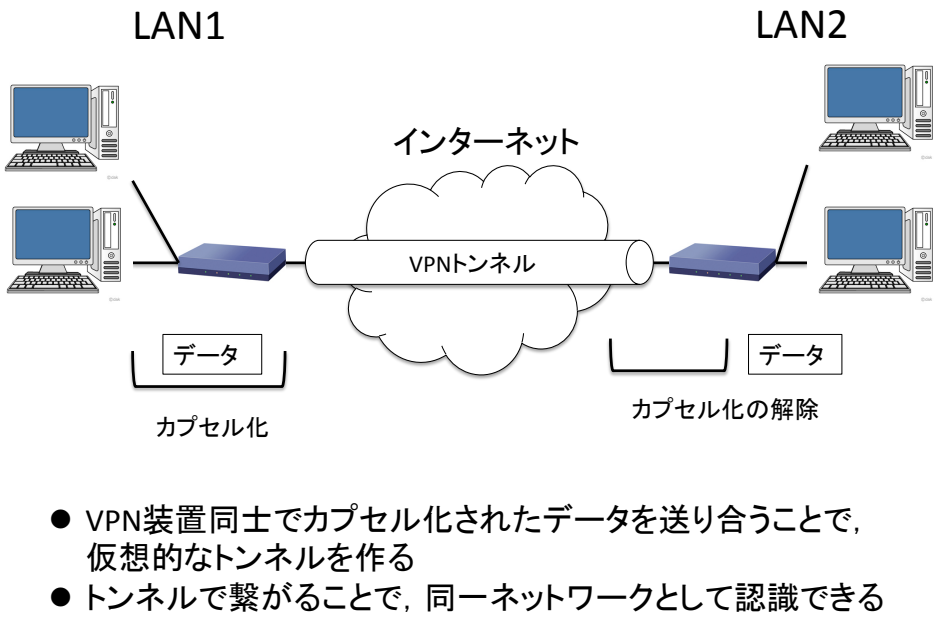

図 7: VPN の概要

5.1 小林ゼミの VPN

小林ゼミの VPN 環境において利用可能なプロトコルは L2TP Over IPSec と PPTP がある．Mac はいずれのプロトコルも利用することが可能である．ただし，L2TP Over IPSec は PPTP よりもセキュアなため前者の使用を推奨する．はじめに，VPN の設定に必要な情報を表 1 に示す．サーバアドレスは cririn.firefly.kutc.kansai-u.ac.jp と同じ 158.217.77.225 を使用する．アカウント名とパスワードは Xoops にログインする時と同じものを使用する．共有シークレットは口頭で伝える．

表 1: VPN 設定に必要な情報

項目	値
サーバアドレス	158.217.77.225
アカウント名	Xoops で使用するアカウント名
パスワード	Xoops で使用するパスワード
共有シークレット	******

5.2 VPN の設定（Mac の場合）

システム環境設定からネットワークを開く（図 8）．次に＋から新しいサービスを作成する．新たに表示されたウィンドウでインタフェースを VPN，VPN タイプを L2TP Over IPSec か PPTP を選択，サービス名は任意に入力して，作成を押す（図 9）．新しいサービスが作成されたので，そのサービスを選択した状態で設定を入力する．構成はデフォルト，サーバアドレスは 158.217.77.225, アカウント名を入力する．次に認証設定を押す．ここで L2TP over IPSec による VPN 構成の場合は，ユーザ認証でパスワード，コンピュータ認証で共有シークレットを入力する（図 10）．PPTP による VPN 構成の場合はパスワードを入力する．さらに PPTP の暗号化は自動（128 ビットまたは 40 ビット）にする．以上全ての項目を入力して，適応と接続を行う．またメニューバーに VPN の状況を表示をチェックすることで接続状態や接続時間が表示される．これは VPN 接続のショートカット機能も有しているのでチェックすることを推奨する（図 11）．

図 8: ネットワーク設定

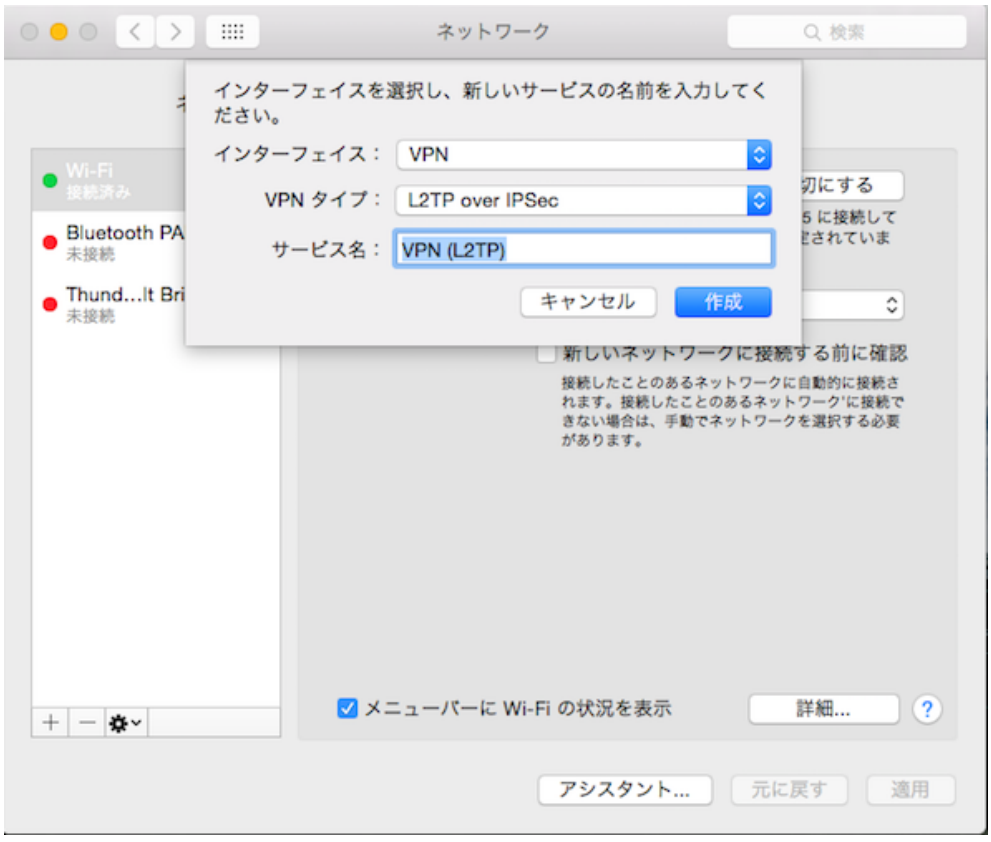

図 9: vpn サービスの作成

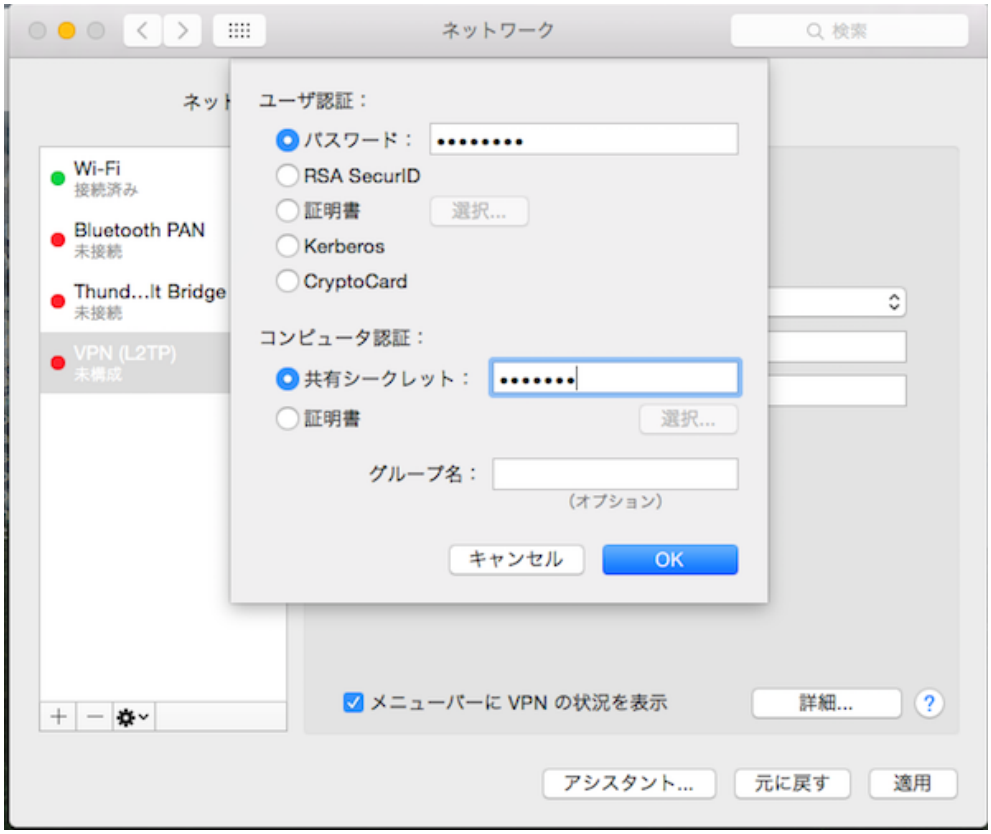

図 10: L2TP Over IPSec の認証設定

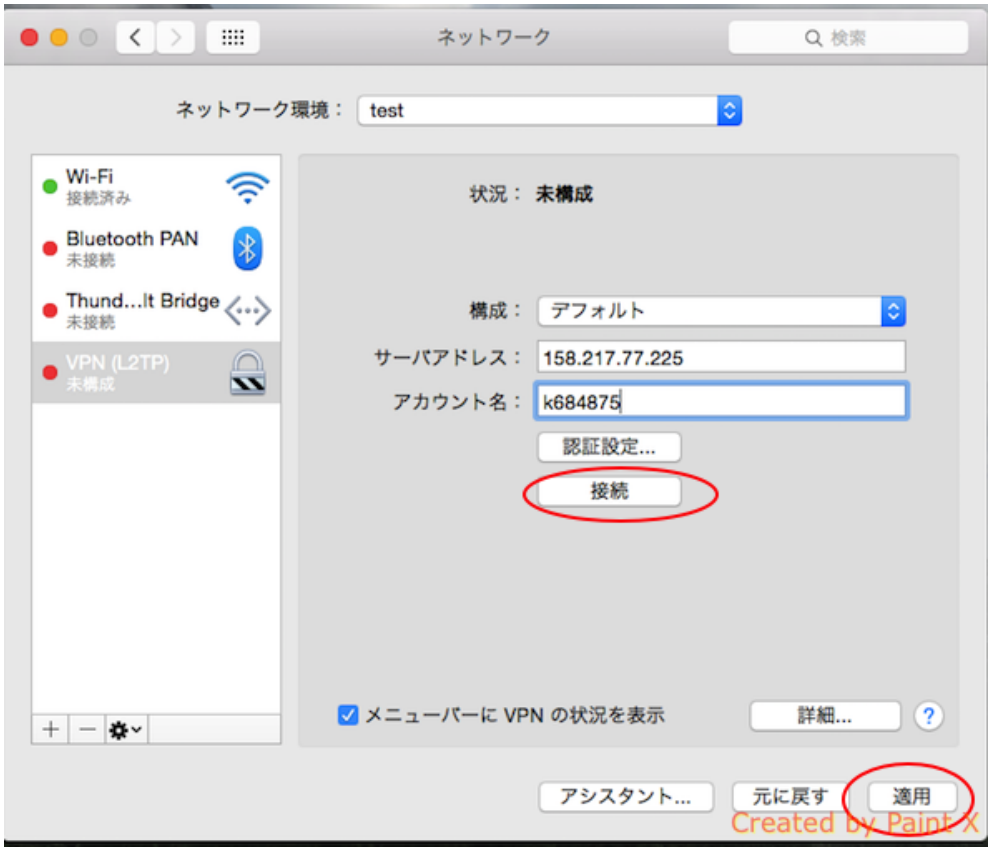

図 11: VPN の適応と接続

5.3 VPN の設定（Windows10 の場合）

ホーム画面左下の Windows アイコンから設定をクリックする（図 12）．開いたウィンドウからネットワークとインターネットを選択する（図 13）．次に，開いたメニュー左の VPN から VPN 接続を追加するを選択する（図 14）．VPN の設定ウィンドウについては，各項目に正しく入力する．それぞれ，VPN プロバイダーは windows（ビルトイン）．接続名は VPN．サーバ名またはアドレスには 158.217.77.225．VPN の種類は PPTP．ユーザ名とパスワードを入力し保存を押す（図 15）．ウィンドウを閉じると，関連設定のメニューにあるアダプターのオプションを変更を選択する（図 16）．作成した VPN 設定のアイコンが表示されるのを確認し，アイコンの上で右クリックからプロパティを選択（図 17）．セキュリティタブをクリックし，VPN の種類が PPTP になっているのを確認とデータの暗号化には暗号化が必要を選んで OK を押す（図 18）．最後に，ネットワークとインターネットのウィンドウから接続を選択し，接続中になっていることが確認できれば完了となる（図 19）．

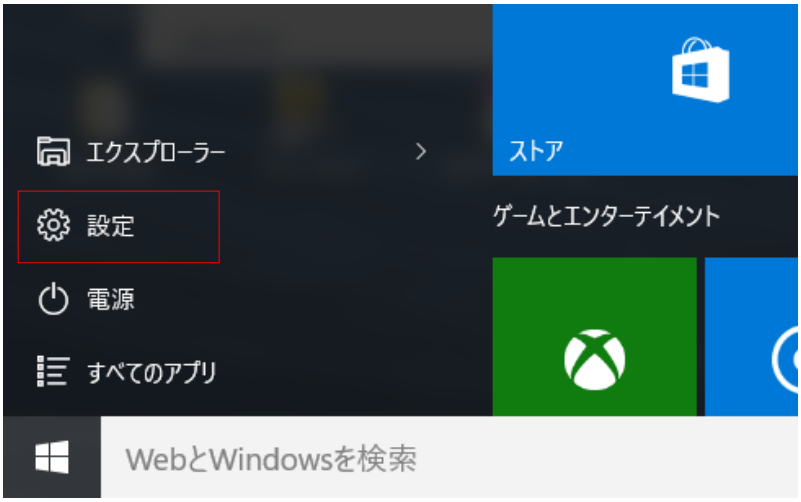

図 12: VPN の設定 1

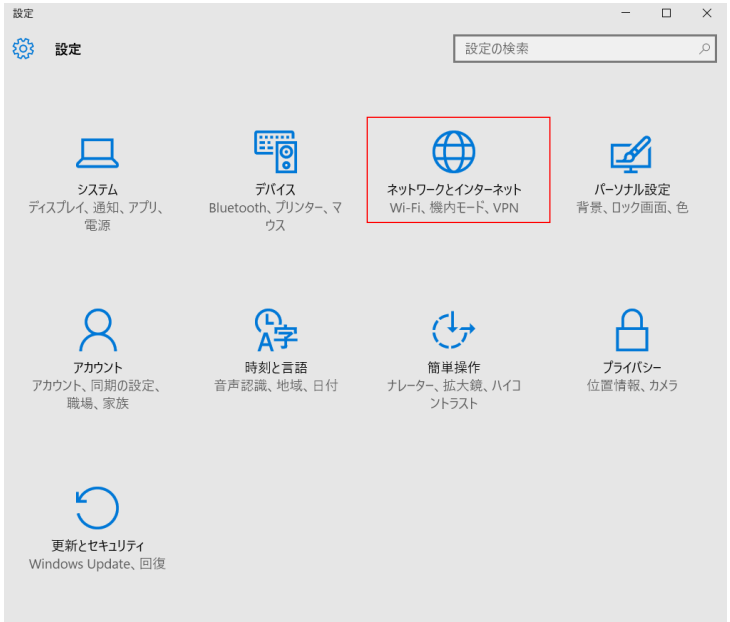

図 13: VPN の設定 2

図 14: VPN の設定 3

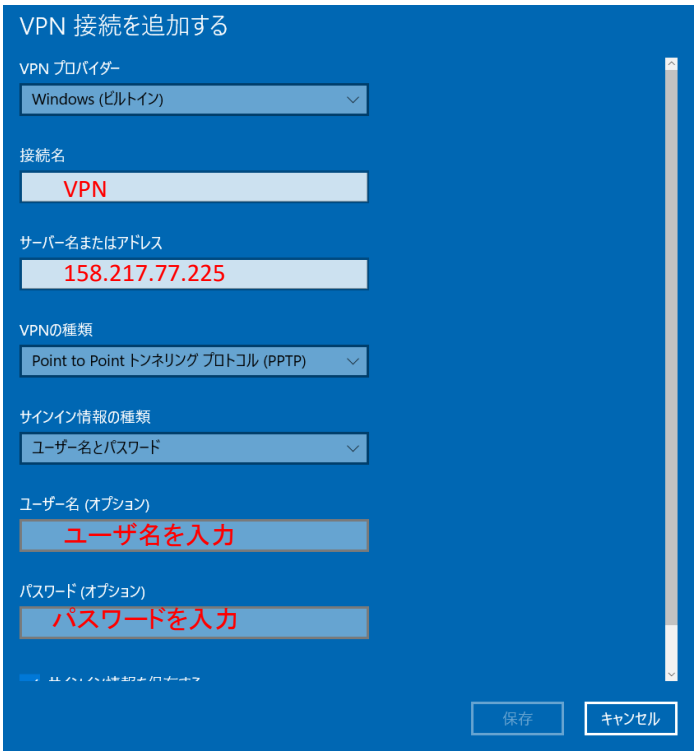

図 15: VPN の設定 4

図 16: VPN の設定 5

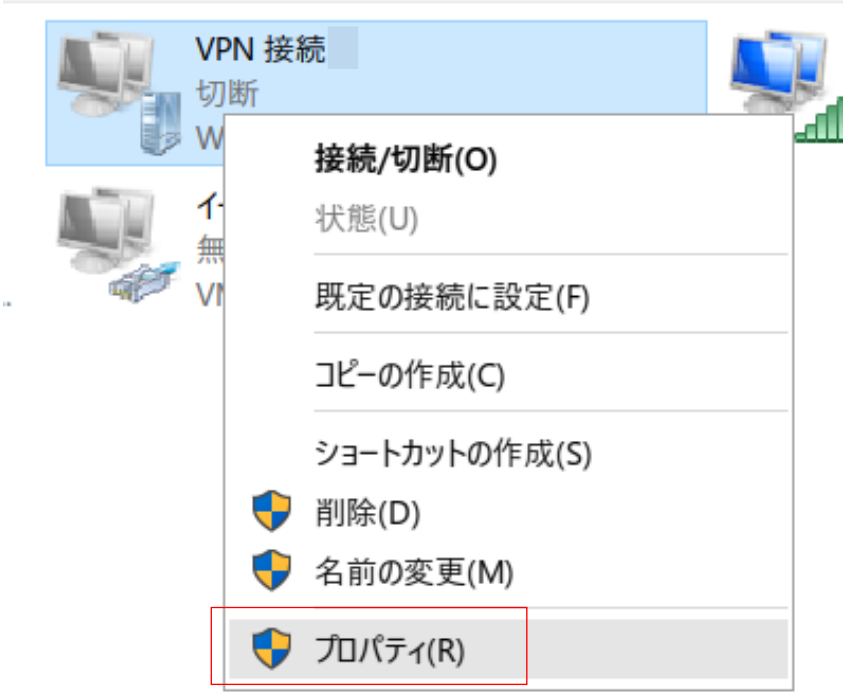

図 17: VPN の設定 6

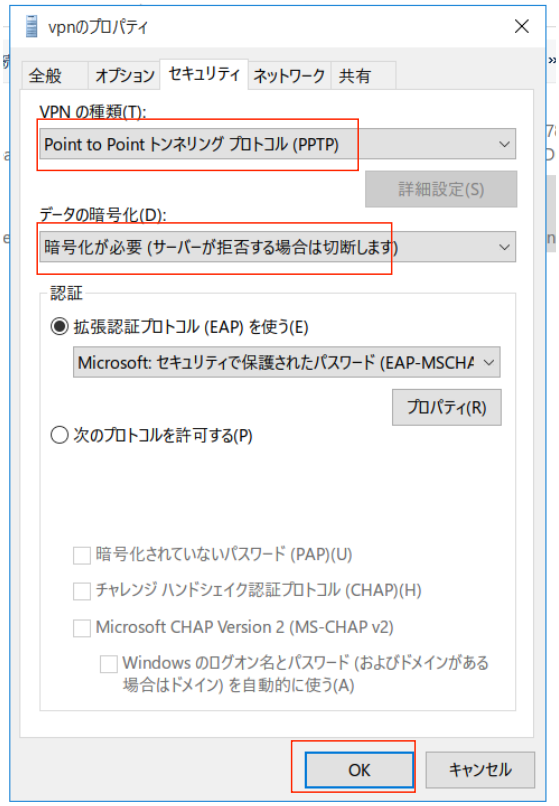

図 18: VPN の設定 7

図 19: VPN の設定 8

20XX 年 X 月 X 日　初版　　XX-XXXX　名無 権兵衛
20XX 年 Y 月 Y 日　第二版　YY-YYYY　John Smith