7 接続認証

通常のイーサネットはホストのケーブル接続をすると無条件で接続を受け入れる。これに対して接続者をユーザー名・パスワードで確認してから受け入れる方法がある。図 7.1 で PC-A についてはルーターX との間で PPPoE 方式により認証接続を行い、また PC-B については Catalyst2940 スイッチが IEEE802.1x ポートベース認証を行うように設定する。IEEE802.1x 認証では CentOS に FreeRADIUS をインストールして認証サーバとした。PPPoE には認証サーバは使用しなかった。

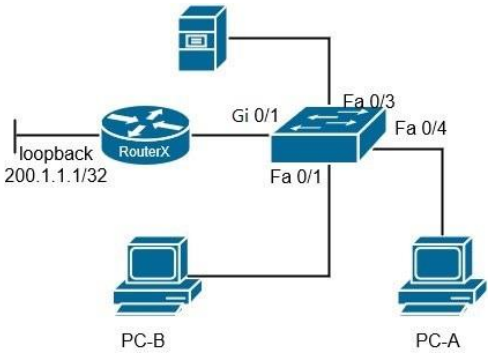

図 7.1 接続認証トポロジー図

そもそも、PPPoE（PPP over Ethernet）は、PPP（Point to Point Protocol）の認証機能などを、Ethernet 上でも利用できるようにしたプロトコルであり、RFC2516 で標準化されている。また、RADIUS（Remote Authentication Dial In User Service）は、ネットワーク上のユーザー認証プロトコルの 1 つで、現在では無線 LAN や有線 LAN でのネットワーク接続時のユーザー認証のプロトコルとしても利用されている。PC-A、PC-B ともに Windows の PC を使用した。図 7.2 に RouterX の設定を、図 7.3 にスイッチの設定を示す。

```
hostname PPPoE

username user password user

ip local pool POOL1 192.168.0.100 192.168.0.200

interface Loopback1

ip address 200.1.1.1 255.255.255.255

interface Virtual-Template1

mtu 1454

ip unnumbered Loopback1

peer default ip address pool POOL1

ppp authentication chap

bba-group pppoe PPPOE-GROUP1

virtual-template 1

interface GigabitEthernet 0/5

no ip address
```

図 7.2 RouterX の設定

```
aaa new-model
aaa session-id common
aaa group server radius ForDot1X
server-private 192.168.0.2 auth-port 1812 acct-port 1813 timeout 1 retransmit 1 key cisco
aaa authentication dot1x default group ForDot1X
dot1x system-auth-control
aaa authorization network default group ForDot1X if-authenticated

vlan 10
vlan 20

interface vlan 10
ip address 192.168.0.3 255.255.255.0
interface FastEthernet0/1
description ## AuthPort : eap ##
switchport mode access
dot1x port-control auto
spanning-tree portfast
interface GigabitEthernet0/1
description ## UplinkPort ##
switchport access vlan 10
spanning-tree portfast
```

図 7.3 Catalyst2940 の設定

RADIUS の設定としては、/etc/raddb/clients.conf に接続許可するネットワークと secret を追記し、/etc/raddb/users に新規ユーザとパスワードを追記した。

Windows の PC で有線 LAN にて IEEE802.1x 認証を行う場合、サービスから Wired AutoConfig を起動させる必要がある。次に、コントロールパネルのイーサネットのプロパティに認証というタブがあるので、選択し、「IEEE 802.1X 認証を有効にする」にチェックを入れた。認証の一番下にある「追加の設定」を選択し、「認証モードを指定する」の「資格情報の保存」ボタンを押して、RADIUS サーバに

設定したユーザー名とパスワードを登録する。すると、図 7.4 から図 7.5 のようにイーサネットの状態のメディアの状態が認証を試みていますから有効に変化する。

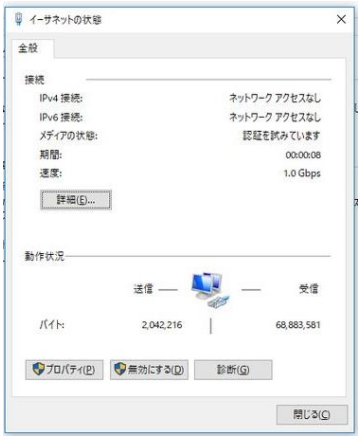

図 7.4 ユーザー登録前

図 7.5 ユーザー登録後

Windows の PC で PPPoE をする場合、コントロールパネルのネットワークとインターネットにある新しい接続またはネットワークのセットアップを選択。その後、PPPoE を選択してユーザー名・パスワードを入力する。接続が成功すれば、コマンドプロンプトで ipconfig の結果に、PPPoE の欄が図 7.7 のように追加される。

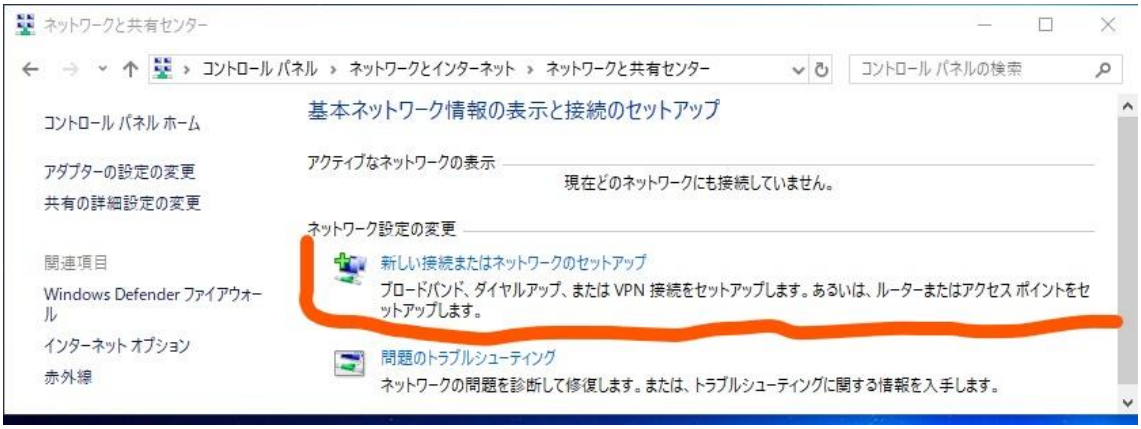

図 7.6 Windows で PPPoE を使用する

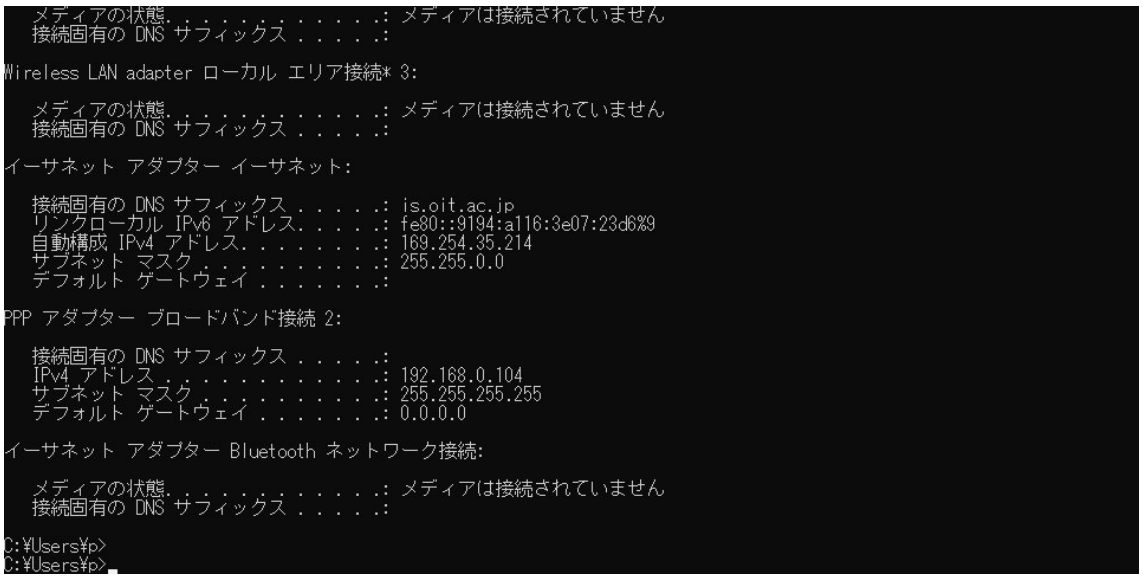

図 7.7 PPPoE が成功したときの ipconfig の結果