7 接続認証

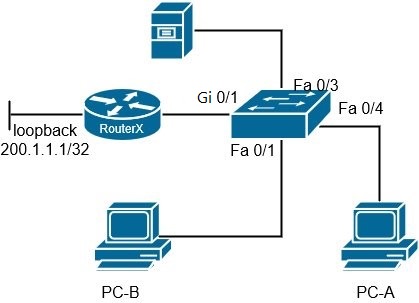
通常のイーサネットはホストのケーブル接続をすると無条件で接続を受け入れる。これに対して接続者をユーザー名・パスワードで確認してから受け入れる方法がある。図7.1でPC-AについてはルーターXとの間でPPPoE方式により認証接続を行い、またPC-BについてはCatalyst2940スイッチがIEEE802.1xポートベース認証を行うように設定する。IEEE802.1x認証ではCentOSにFreeRADIUSをインストールして認証サーバとした。PPPoEには認証サーバは使用しなかった。

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。

図7.2 RouterXの設定

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

pppoe enable group PPPOE-GROUP1

no shutdown

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。

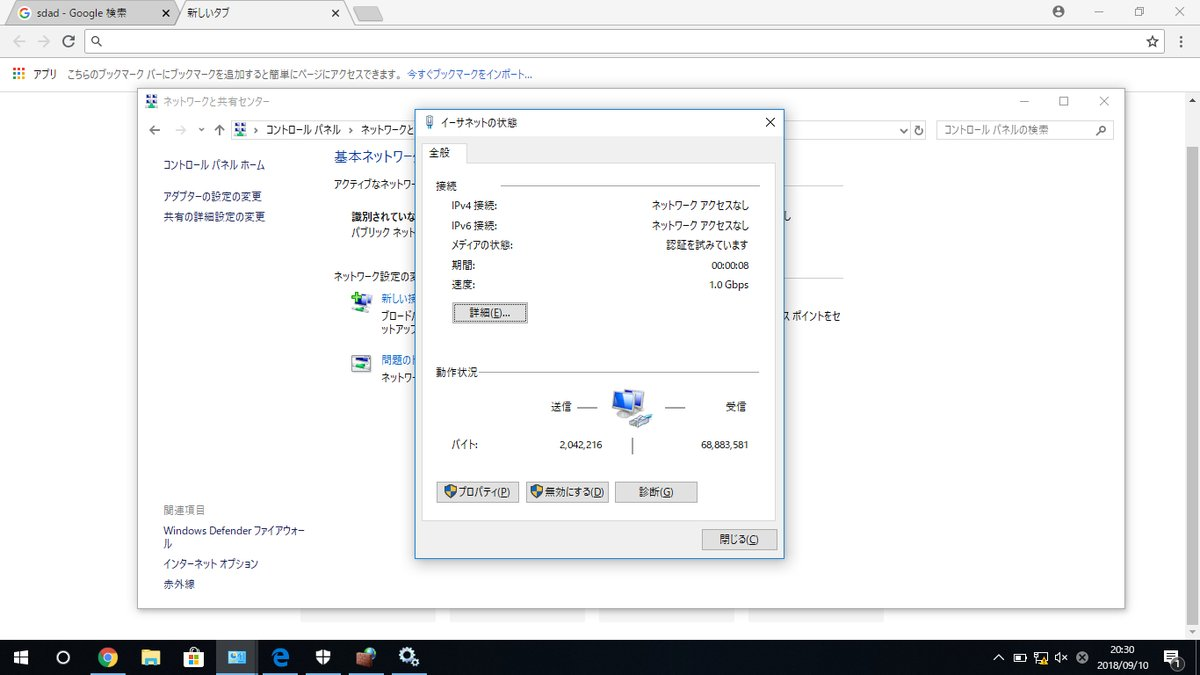


図7.4 ユーザー登録前

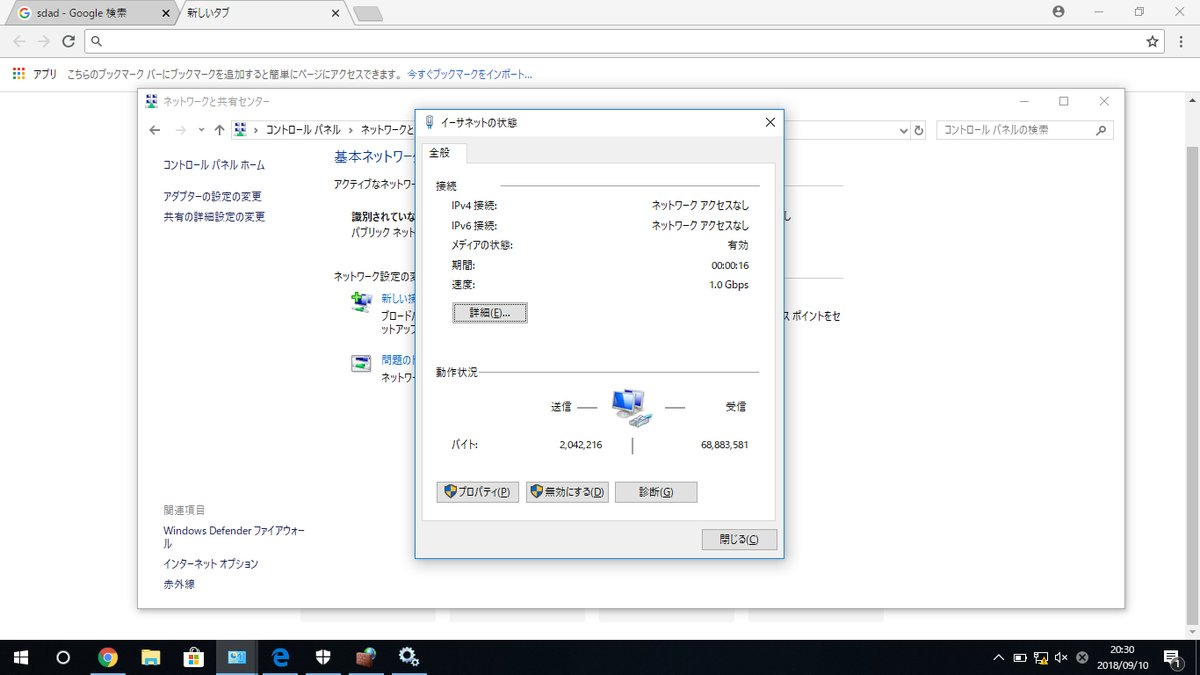


図7.5 ユーザー登録後

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。

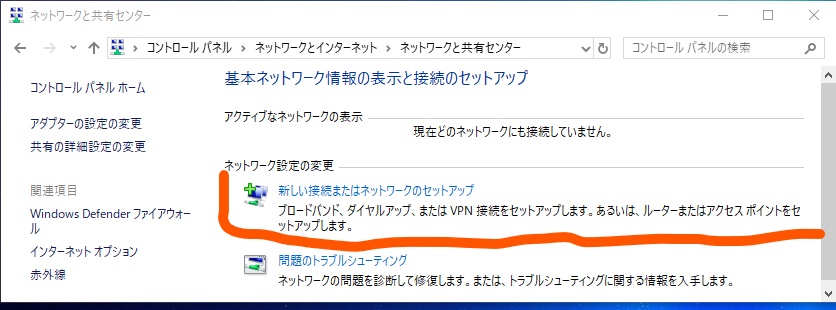


図7.6 WindowsでPPPoEを使用する

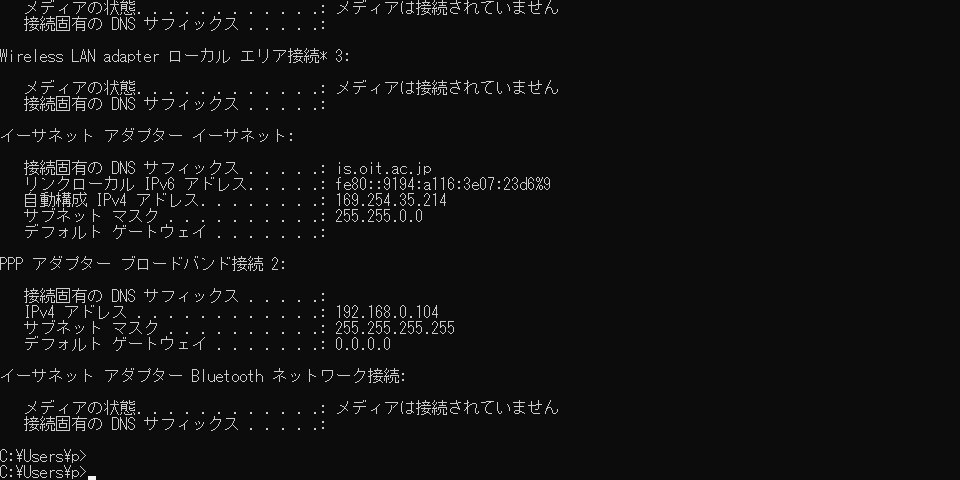


図7.7 PPPoEが成功したときのipconfigの結果