FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックの導入・運用

第 3 版

2021 年 8 月

古河電気工業株式会社

目次

商標について

1　はじめに

本書では、FITELnet F70M/F71M/F220M/F221M（以下、FITELnet）を利用した、「FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックの導入・運用」について記載します。

2　FUJITSU Security Solution アイソレーションゲートウェイサービス ルーターパックとは

本サービスは、WEB アイソレーション技術(Menlo Security)とルータ製品(FITELnet)を組み合わせてブラウザ経由のマルウェア感染を防ぐ、安心・手軽・安価にお使いいただけるサービスです。
全ての Web サイトのコンテンツを、マルウェアの有無に関わらず仮想環境上でクリーンな情報に変換するため、安心安全な Web アクセスが可能です。

3　サービスにおけるFITELnetの役割

図 1 に FITELnet を使ったサービスイメージを示します。クライアント PC を FITELnet に接続すると、クライアント PC は、FITELnet から DHCP で配布されるアドレス情報をもとに FITELnet に置かれているプロキシ設定情報（PAC ファイル）を取得します。このプロキシ設定情報に「分離・無害化サービス」の宛先情報が記載されており、その情報から、クライアント PC はインターネットアクセスをする際に「分離・無害化サービス」を通してアクセスします。

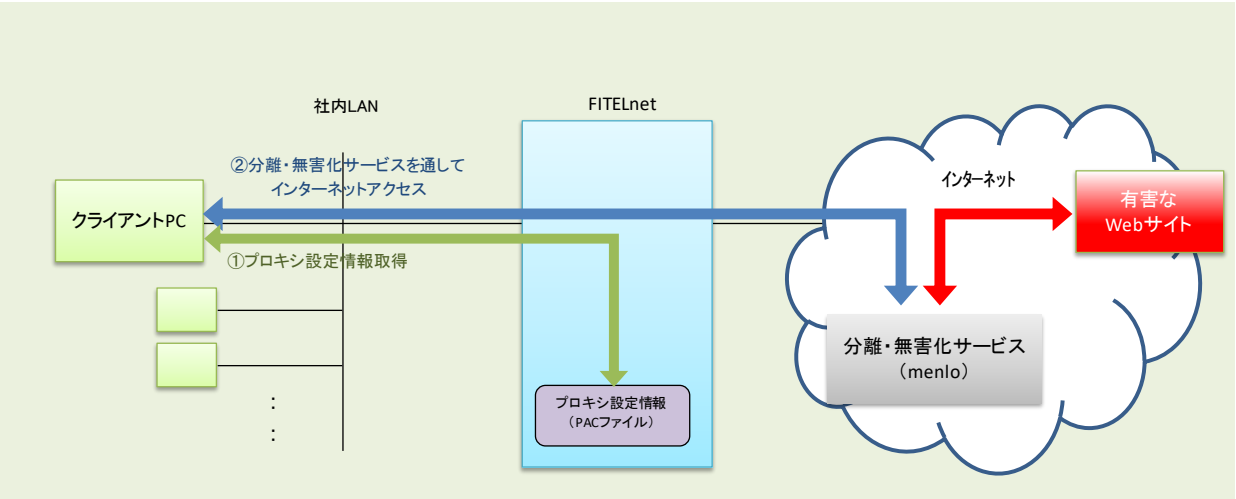


図 1 FITELnet を使ったサービスイメージ図

4　FITELnet構成例とコンフィグ

FITELnet を使った構成例を図 2 に示します。インターネット回線には Giga2/1 ポート(100.1.1.2)を通して接続され、社内ネットワーク(192.168.1.0/24)には Giga1/1 ポートを通して接続されています。本サービスはコンテナ機能を使用しており、プロキシ設定情報はコンテナ環境に置かれています。コンテナには 192.168.1.254 のアドレスが設定されており、Giga1/1 ポートを通してアクセスします。FITELnet の DHCP サーバ機能により、クライアント PC に IP アドレス等の払い出しが行われます。このタイミングでプロキシ設定情報のロケーション情報(URL)も一緒に通知されるため、クライアント PC はそのロケーション情報をもとにプロキシ設定情報を取得することが可能となります。Giga2/1 では NAT 変換を行い、パケットの送信元アドレス（LAN のアドレス）を Giga2/1 のインタフェースのアドレスに変換しています。

※Giga1/1(192.168.1.1)とコンテナアドレス(192.168.1.254)は工場出荷時にデフォルトで設定されています。Giga2/1 は工場出荷時には設定されておらず、お客様の環境に合わせて設定していただく必要があります。工場出荷時にデフォルトで設定された LAN 側アドレスをお客様環境に合わせて変更したい場合には、文末の付録 A を参照下さい。

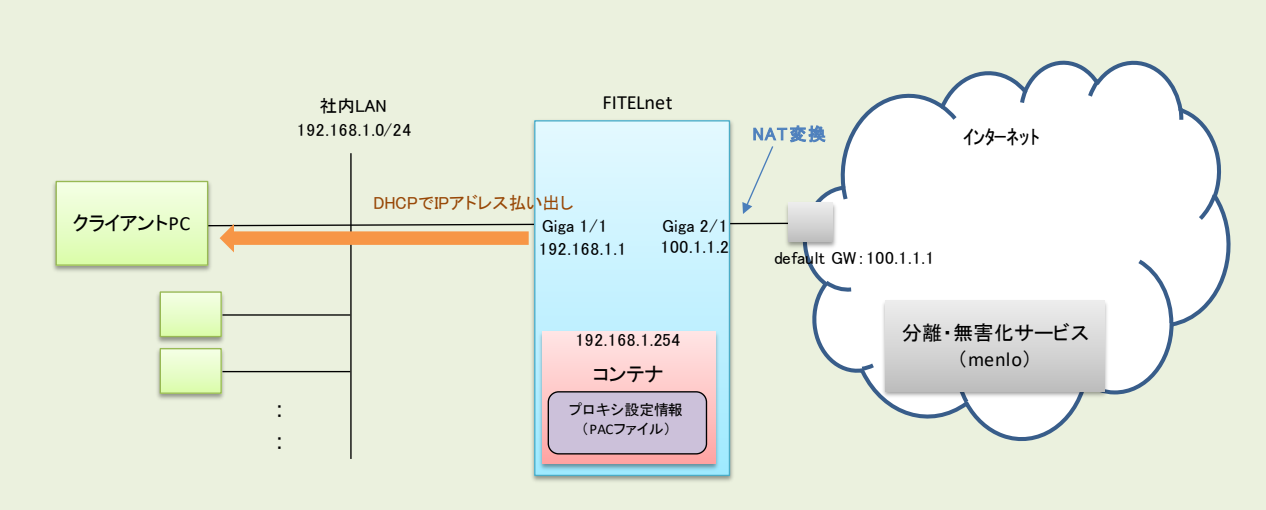


図 2 構成図

上記ネットワーク構成に合わせた FITELnet のコンフィグを以下に示します。

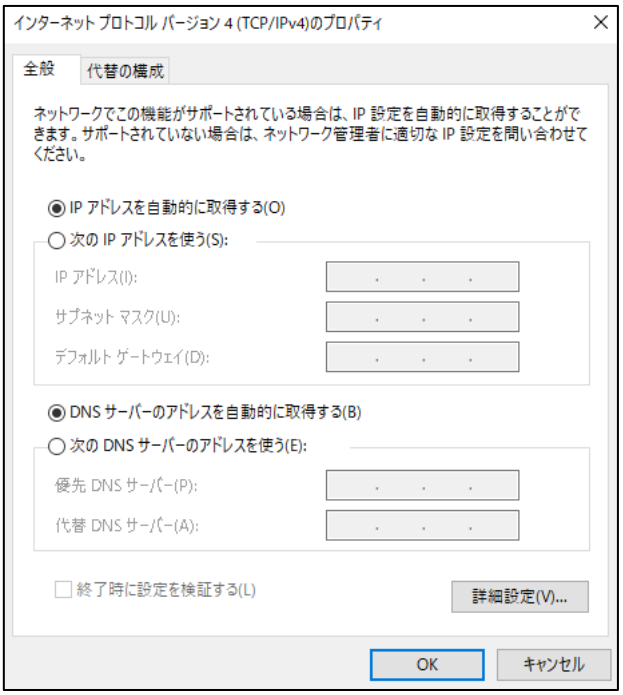
```
container enable                                    ←コンテナのサービスを有効にする設定
container device disk /mnt/pac_mainte drive uid 101 gid 101
!
container configuration                             ←コンテナの設定
 !
 interface 1                                          コンテナのinterface1をルータの
  bridge-group 1                                    ←bridge-group1(giga1/1)に紐づける設定
  ip address 192.168.1.254 255.255.255.0           ←コンテナアドレスの設定
  ip gateway 192.168.1.1                            ←コンテナのgeteway設定
 exit
```

```
 !
exit
 !
access-list 111 deny ip any any                          ←学習フィルタ設定
access-list 121 spi ip any any                           ←学習フィルタ設定
!
ip host fitelnet-container.fnsc.co.jp 192.168.1.254      ←コンテナアドレスにホスト名
!                                                          (fitelnet-container.fnsc.co.jp)登録
ip route 0.0.0.0 0.0.0.0 100.1.1.1                       ←デフォルトルートを設定
ip name-server 127.0.0.1
!
ip dhcp server-profile DHCP_SERVER_PROF                  ←DHCPサーバ機能のプロファイル
 address 192.168.1.2 192.168.1.101                       ←DHCP払い出しアドレスレンジ
 lease-time 3600                                         ←払い出し情報のリース時間(秒)
 dns 192.168.1.1
 gateway 192.168.1.1
 option 252 ascii http://fitelnet-container.fnsc.co.jp/pac/web_security.pac
exit                                                       ↑PACファイル置き場情報
!
ip nat list 1 192.168.1.0 0.0.0.255                      ←192.168.1.0/24 を list 1 と定義
!
hostname FITELnet
!
interface GigaEthernet 1/1
 vlan-id 1
 bridge-group 1
 channel-group 1
 container-use
exit
!
interface GigaEthernet 2/1
 vlan-id 21
 bridge-group 21
 channel-group 21
 ip access-group 111 in                                  ←WAN側からのアタックを防ぐための
 ip access-group 121 out                                   学習フィルタ設定
exit
!
interface Port-channel 1
 ip dhcp service server                                  ←giga1/1にDHCPサーバ機能を設定
 ip dhcp server-profile DHCP_SERVER_PROF                 ←DHCPサーバ機能のプロファイル名を指定
 ip address 192.168.1.1 255.255.255.0
 link-state always-up
exit
!
interface Port-channel 21
 ip address 100.1.1.2 255.255.255.0
 ip nat inside source list 1 interface                   ←list 1に含まれる送信元アドレスを
exit                                                       インタフェースのアドレスにNAT変換する
!
dns-server ip enable
!
proxydns domain 1 any * any static x.x.x.x               ←お客様環境に合わせてDNSサーバを指定
!                                                          して下さい(x.x.x.x の部分)
end
```

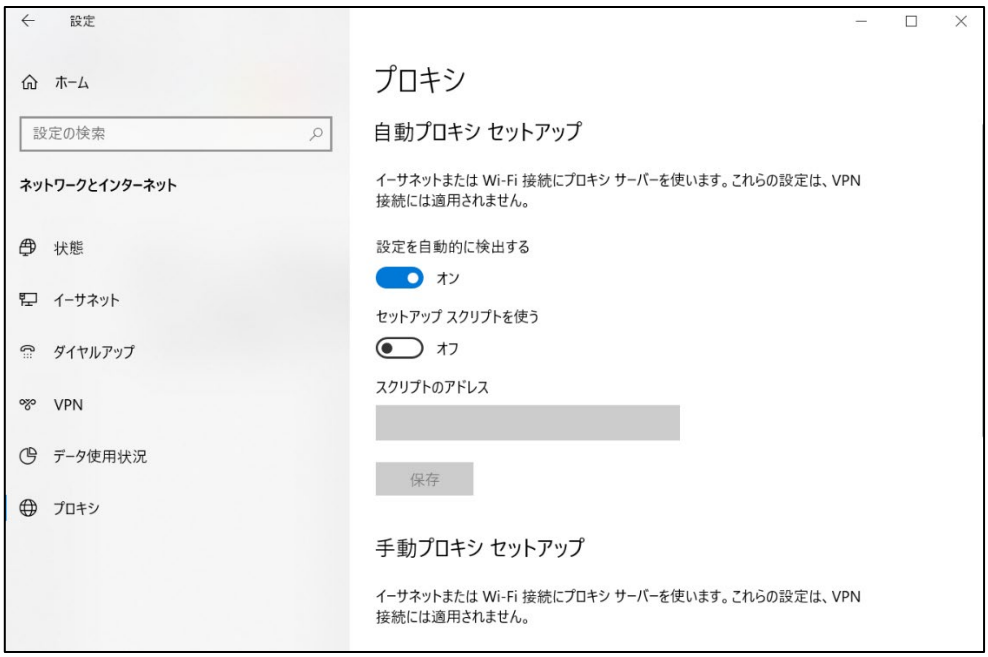
5　FITELnetへのクライアントPCの接続

※本手順実施前に、「分離・無害化サービス」のアカウントの取得と本サービスから提供される CA 証明書のインストールを行ってください。CA 証明書のインストール方法については、文末の付録 B を参照下さい。

前述のコンフィグが設定された FITELnet にクライアント PC を接続するにあたって、クライアント PC の接続ポートのネットワーク設定を”自動(DHCP)”に設定します。Windows10 を例に取ると、下図のインターネットプロトコル設定において、”IP アドレスを自動的に取得する”と”DNS サーバーのアドレスを自動的に取得する”を選択した状態になります。



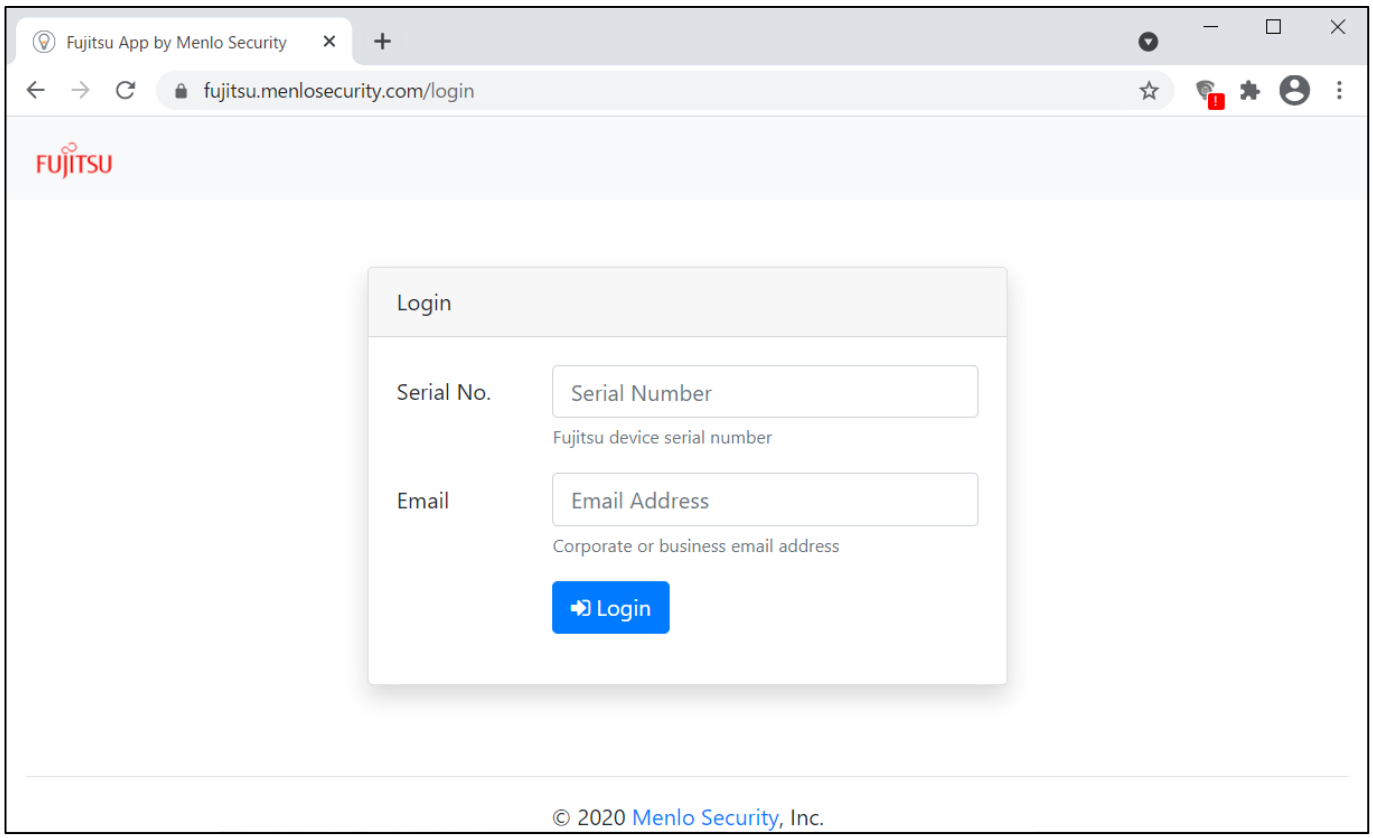
また、プロキシ設定において、”設定を自動的に検出する”をオンにして下さい。



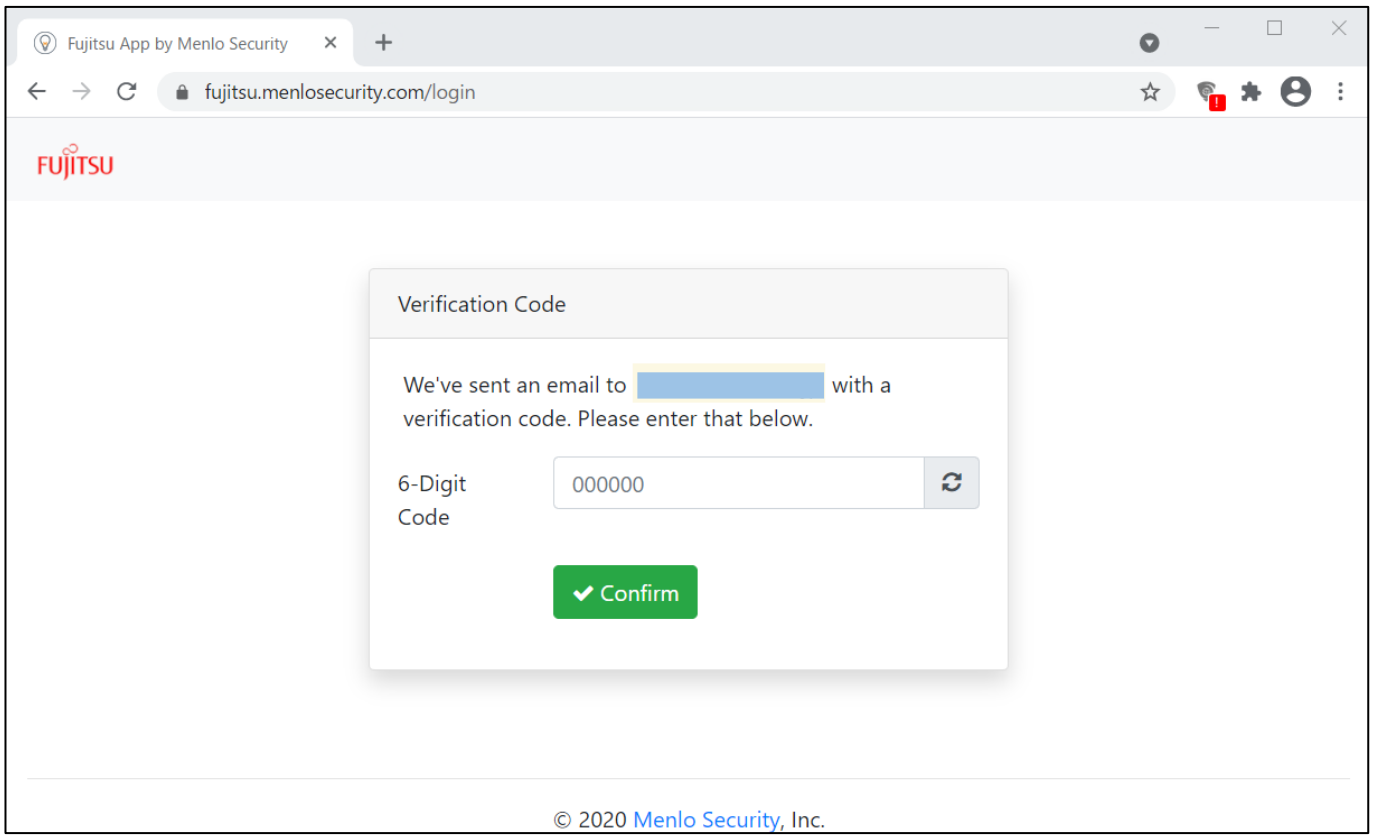
上記設定の後、クライアント PC を FITELnet の giga1/1 ポートのネットワークに接続します。

6　「分離・無害化サービス」を通したインターネットアクセス

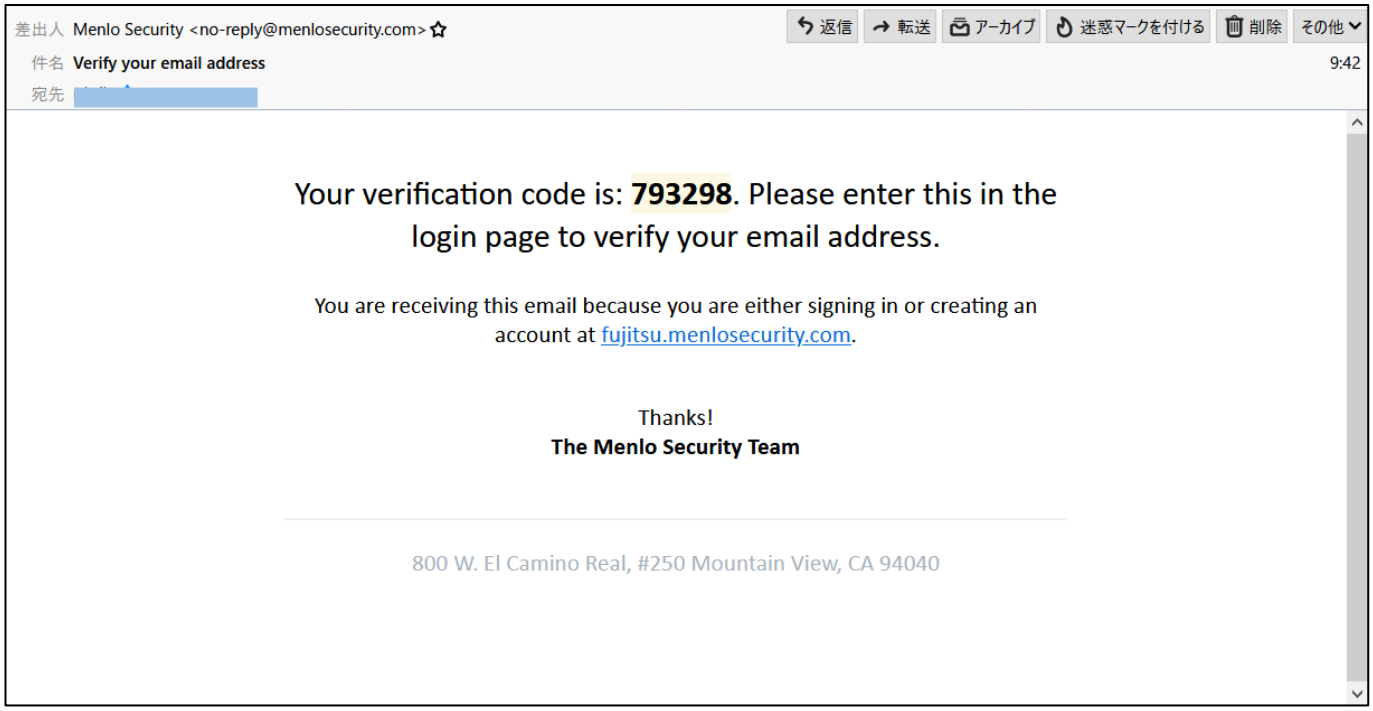
次に、接続したクライアント PC から「分離・無害化サービス」を通してインターネットへアクセスします。クライアント PC 上でウェブブラウザ(例では Google Chrome を使用)を立ち上げます。URL に試しに”www.furukawa.co.jp”を入力して古河電工のサイトへアクセスしようとすると、下記のような「分離・無害化サービス」の認証画面が表示されます。Serial No.に契約番号、Email に受信可能なメールアドレスを入力し、『Login』ボタンを押します。



6 桁のコードを入力する画面が表示されます。

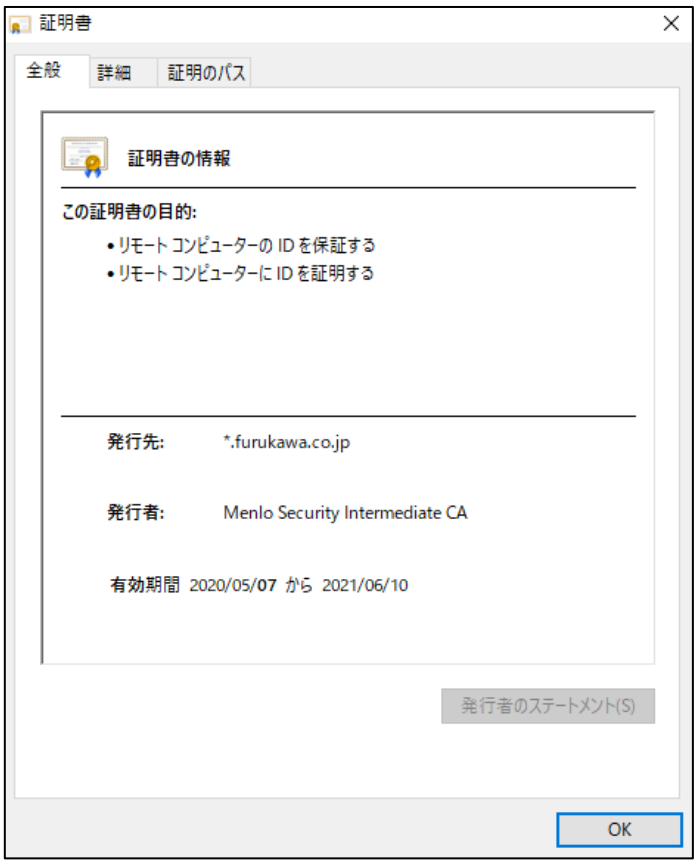


記入したメールアドレス宛にメーカより 6 桁の数字が送付されます。メールアドレスに記載されている 6 桁の数字を前述のコード入力画面に入力し、『Confirm』ボタンを押します。



認証が完了しホームページが表示されます。URL 横の鍵マークをクリックします。次に、表示された情報の中で”証明書”を選択しクリックします。

下記のような証明書情報が表示され、発行者が”Menlo Security Intermediate CA”になっていることが確認でき、「分離・無害化サービス」を通して表示されていることがわかります。



7　PACファイル管理機能

「分離・無害化サービス」を経由させないサイトへのアクセスがある場合は、FITELnet 上の PAC ファイルを編集して、特定のホスト・IP アドレス宛に対して「分離・無害化サービス」を経由させず直接通信させることが可能です。

PAC ファイルの編集は、クライアント PC から FITELnet の PAC ファイル管理ページへアクセスして行います。

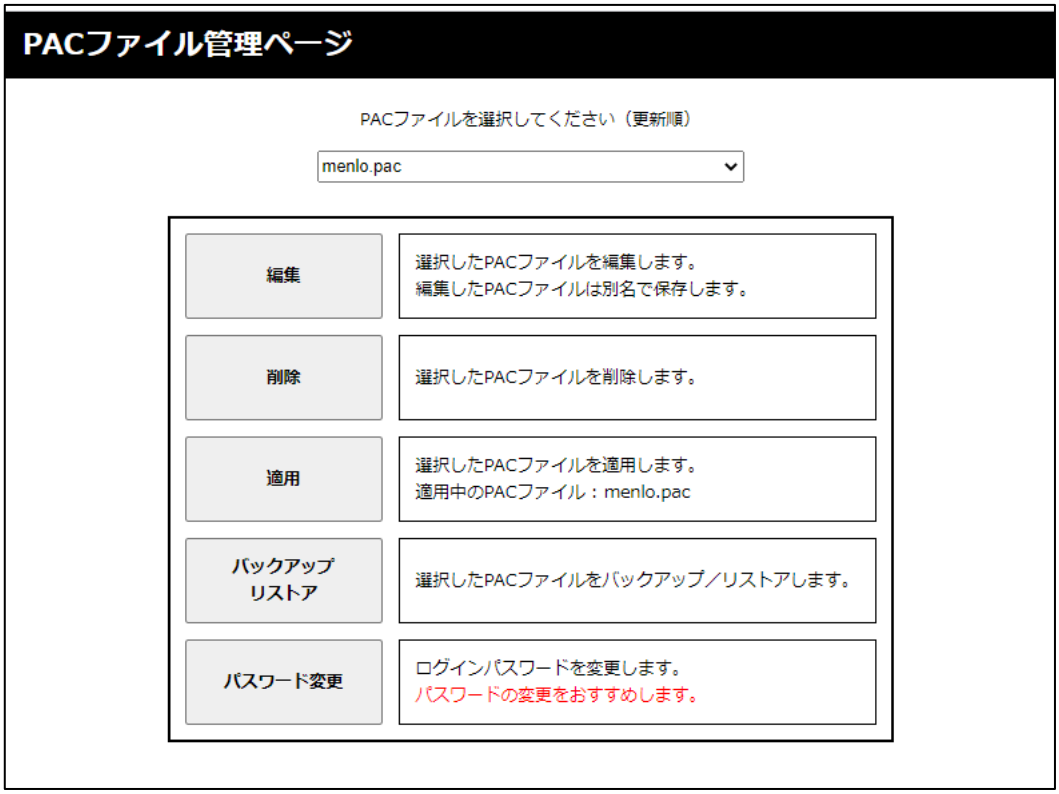
以降、PAC ファイル管理機能の利用方法についてご説明します。

7.1　PACファイル管理ページへのアクセス

PAC ファイル管理ページにアクセスするために、クライアント PC 上でブラウザを開き、URL に”http://fitelnet-container.fnsc.co.jp/cgi-bin/pac_mainte/index.cgi”を入力します。

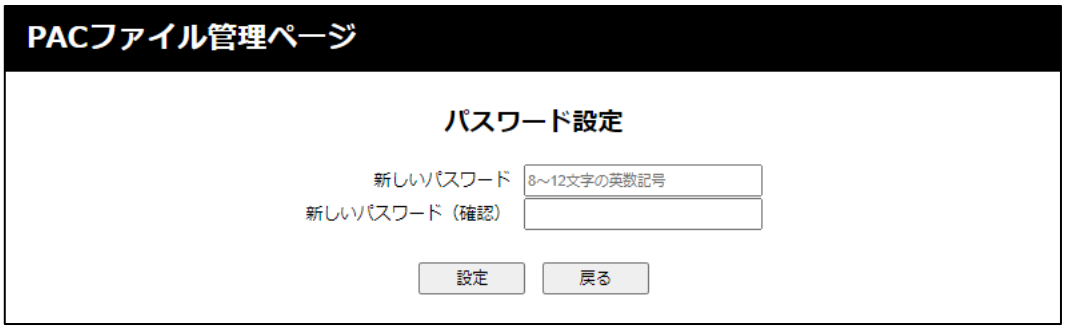
下記のようなログイン画面が表示されるので、ユーザー名とパスワードに”admin”を入力し『ログイン』ボタンを押してログインします。

次のような PAC ファイル管理メインページが表示されます。



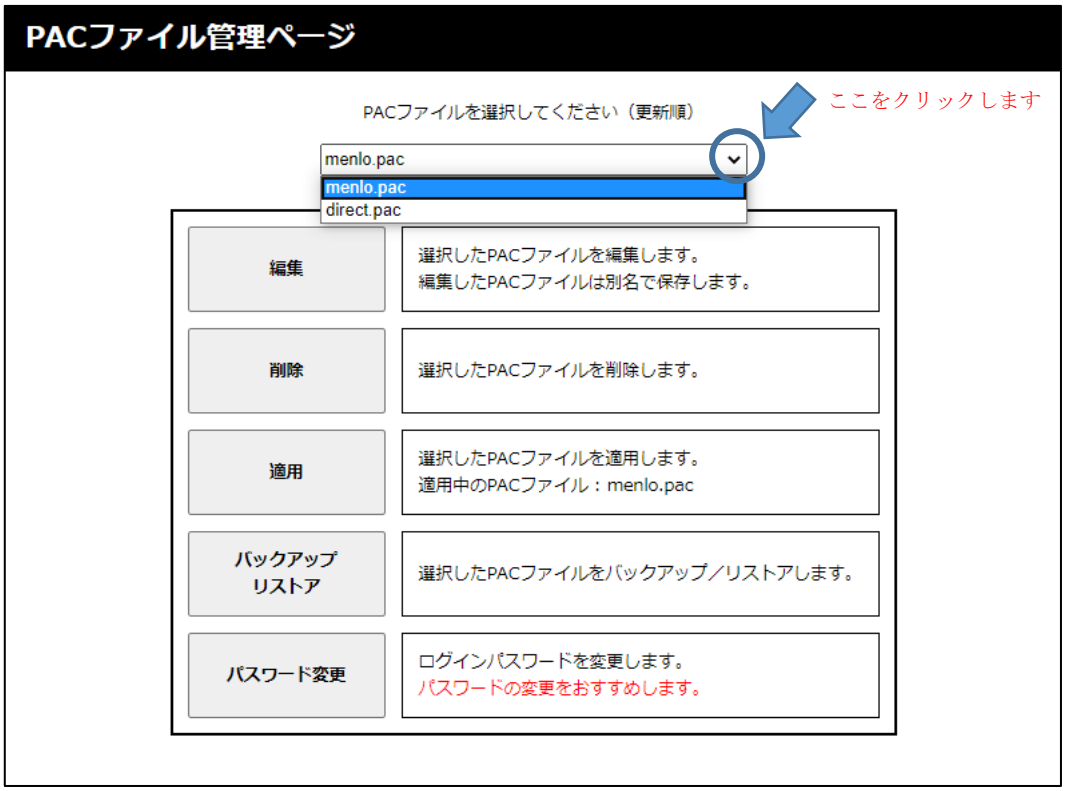
7.2　パスワード変更

初期パスワードを変更する場合は、『パスワード変更』ボタンを押し、新しいパスワードを設定して下さい。
パスワードは 8~12 文字の英数記号になります。



7.3 初期PACファイル

PAC ファイル管理メインページにおいて、上方のウインドウで編集する PAC ファイルを選択します。右端の∨をクリックすると初期の PAC ファイルがプルダウン表示されます。



初期の PAC ファイルは、下記の 2 種類存在します。

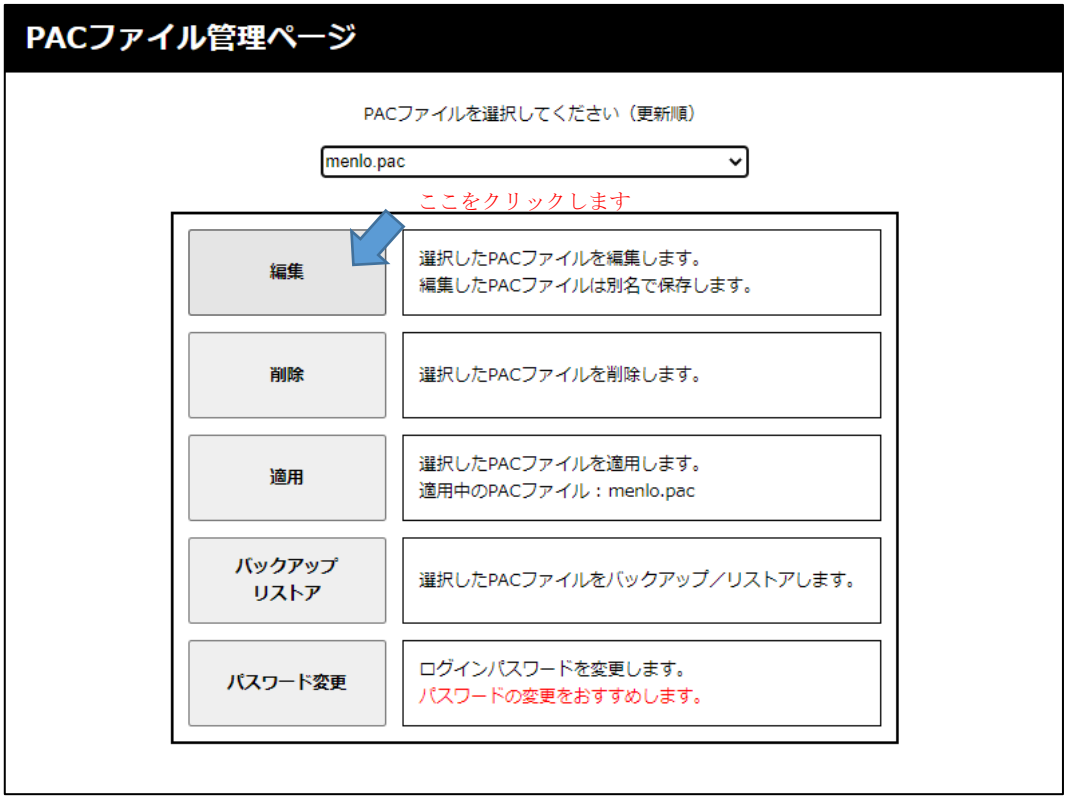
PAC ファイル名	説明
menlo.pac	「分離・無害化サービス」を使用するためにデフォルトで用意された PAC ファイル
direct.pac	「分離・無害化サービス」を使用しない設定の PAC ファイル ※全てのサイトに、「分離・無害化サービス」を経由せず直接アクセスする場合にご使用ください。

7.4 「分離・無害化サービス」を経由しないドメイン/IPアドレスの追加・削除

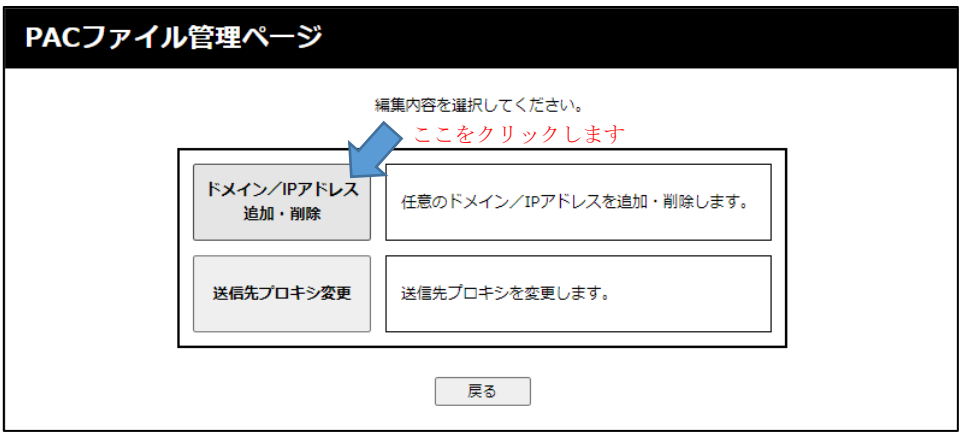
「分離・無害化サービス」を経由せず直接通信させるドメイン、IP アドレスを追加します。

PAC ファイル管理メインページにおいて"menlo.pac"を選択し、『編集』ボタンを押します。

※"direct.pac"への追加・削除の操作は行うことができません。



『ドメイン/IP アドレス 追加・削除』ボタンを押して先へ進みます。



ドメインを追加する場合は、『ドメイン』を選択します。

下のウインドウに追加したいドメインを記入(例では”example.com”を記入)し『追加』ボタンを押します。

追加したドメインが表示されます。※右端の『削除』ボタンを押すことで削除することができます。

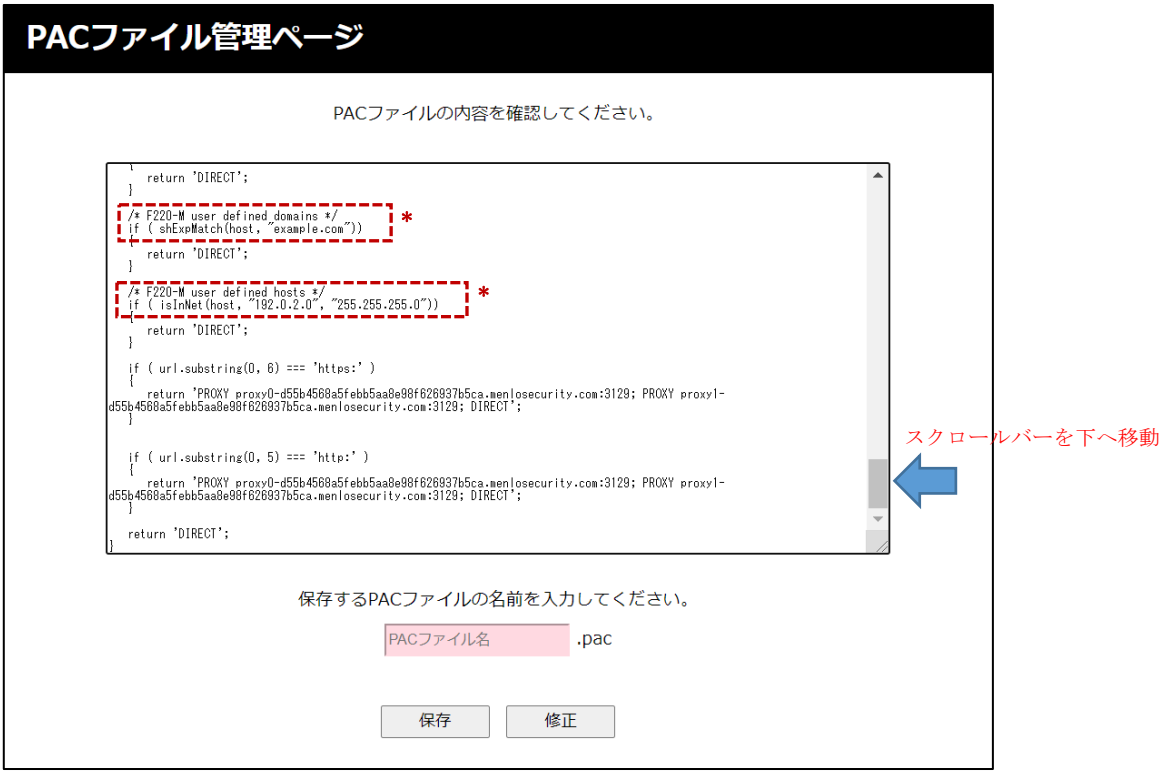
IP アドレスを追加したい場合は、『IP アドレス』を選択します。

下のウインドウに追加したい IP アドレスとサブネットマスクを入力(例では”192.0.2.0/255.255.255.0”を入力)し『追加』ボタンを押します。

追加した IP アドレスが表示されます。※右端の『削除』ボタンを押すことで削除することができます。

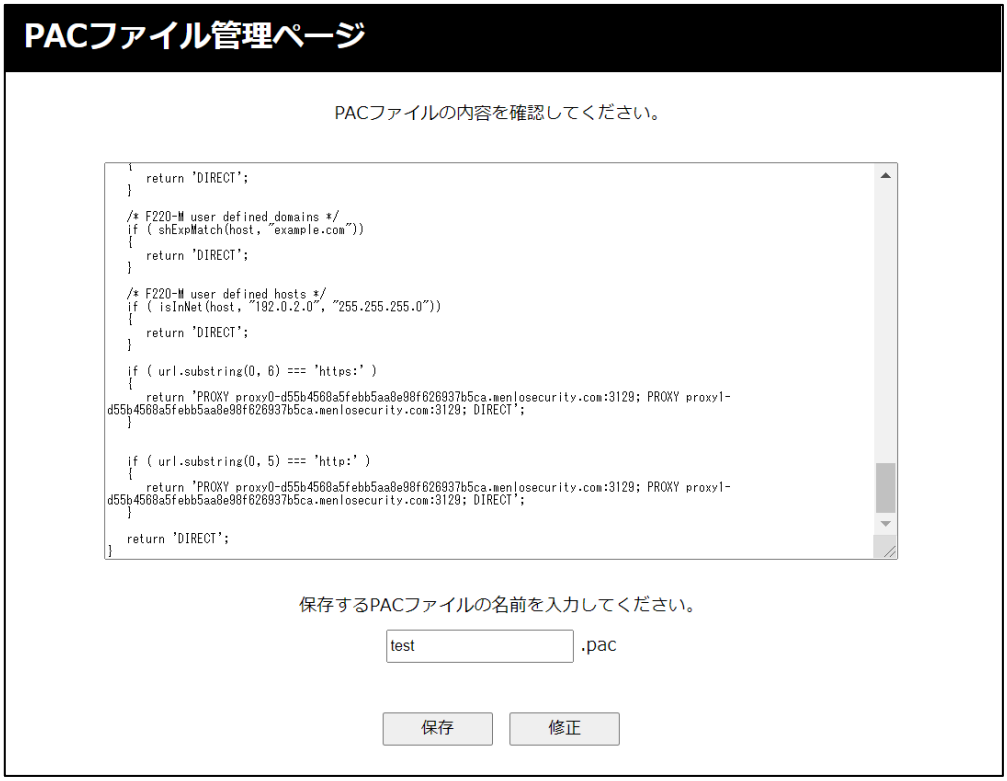
ドメインおよびIPアドレスの追加が完了したら、追加した情報を保存するために、下の『次へ』ボタンを押します。

追加した情報が書き込まれたPACファイルが表示されます。右端のスクロールバーを一番下に持っていくと、”F220-M user defined domains”の下に追加したドメイン(example.com)、” F220-M user defined hosts”の下に追加したIPアドレス(192.0.2.0/255.255.255.0)がmenlo.pacに追加されていることが確認できます。
※修正したい場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。

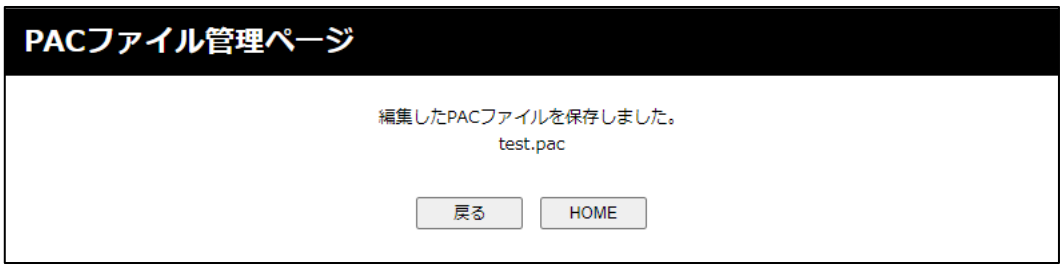


＊全ての機種で「F220-M」と表示されます。お使いの機種に読み替えてご使用ください。

保存する PAC ファイル名を記入(例では”test”を記入)して下の『保存』ボタンを押します。
※PAC ファイル管理メインページのプルダウンで表示された既存のファイル名では保存できませんのでご注意下さい。

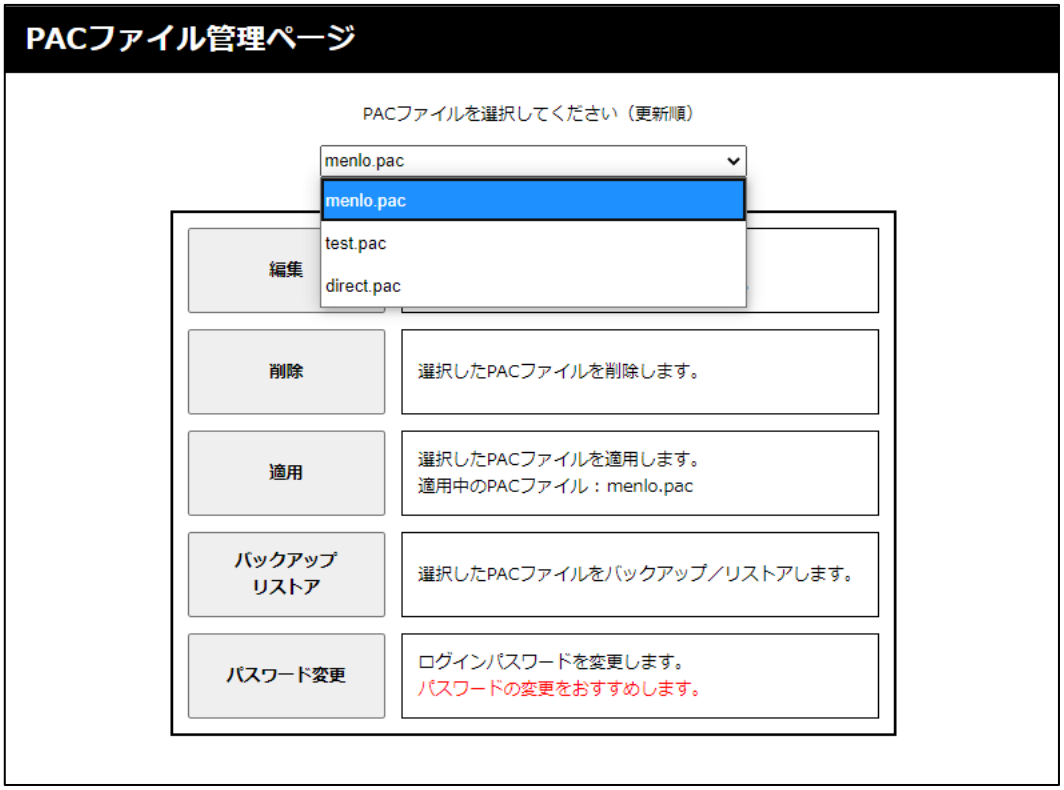


“test.pac”で保存が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。



保存したファイルは、PAC ファイル管理メインページのプルダウンで確認ができます。

※管理可能なファイル数は menlo.pac, direct.pac を含めて 10 ファイルまでです。11 ファイル以上のファイルを作成しようとした場合、エラーとなり作成できません。必要に応じて不要なファイルを削除してください。削除については、7.8 項でご説明します。

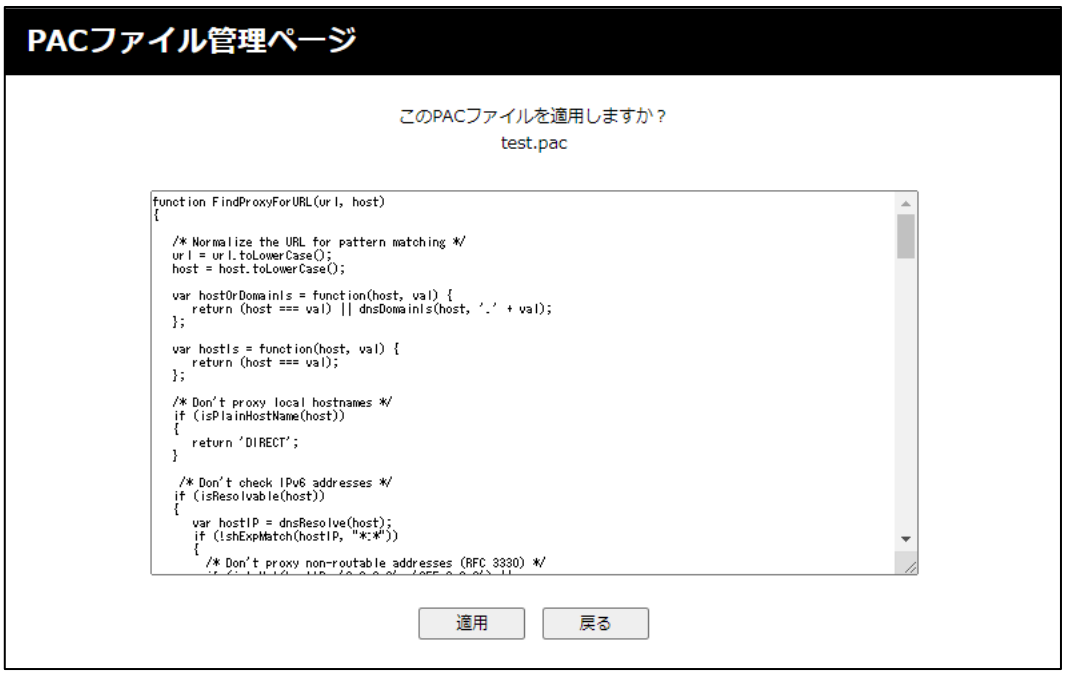


7.5 適用

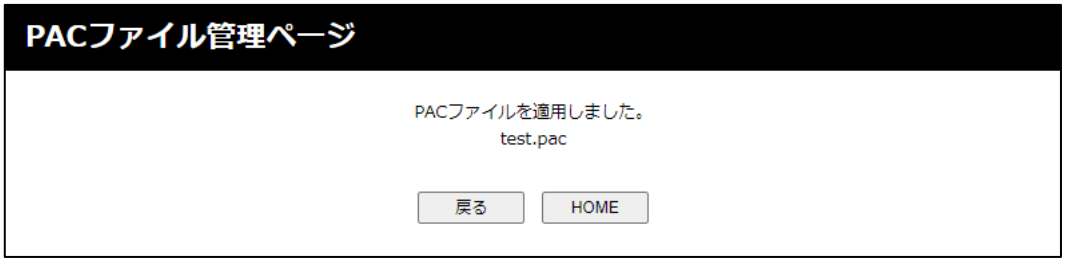
作成した PAC ファイルを適用します。

PAC ファイル管理メインページで適用するファイル名を選択(例では”test.pac”を選択)して、『適用』ボタンを押します。※初期状態では”menlo.pac”が適用されています。

確認画面で適用する PAC ファイルが表示されます。下の『適用』ボタンを押して適用します。

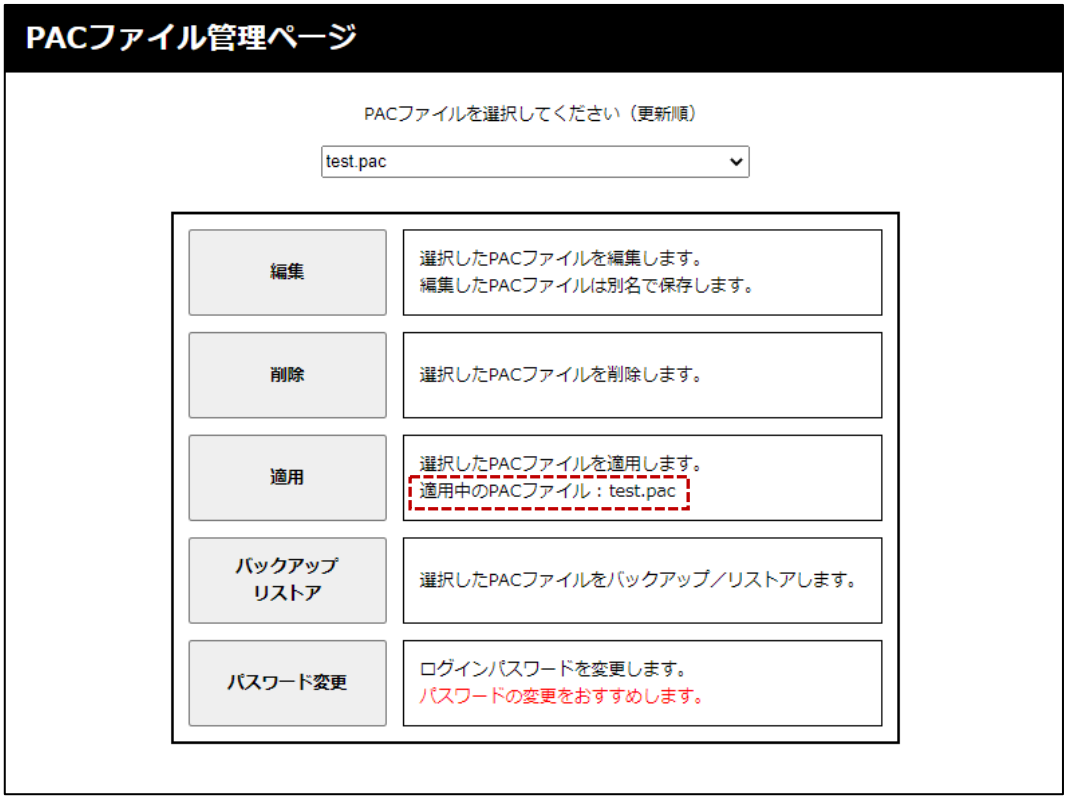


“test.pac”の適用が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。



PAC ファイル管理メインページに戻ると適用中のファイル名が”test.pac”になっています。

※”test.pac”がクライアント PC に反映されるのは、クライアント PC の DHCP リース更新時です（ブラウザによっては、ブラウザ起動時に PAC ファイル取得／反映します）。

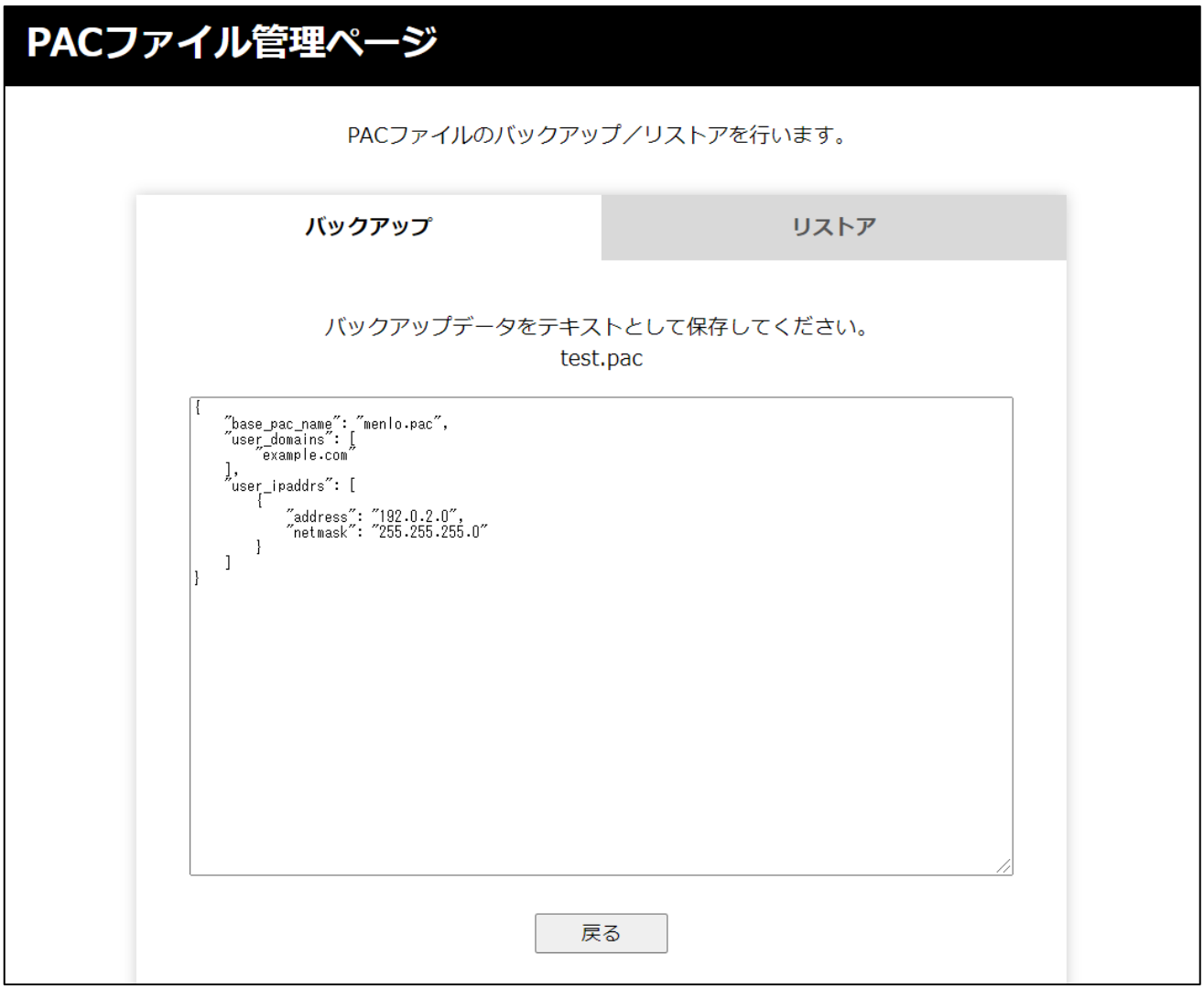


7.6 バックアップ

作成した PAC ファイルのバックアップデータを抽出することができます。

PAC ファイル管理メインページで抽出するファイル名を選択して(例では”test.pac”を選択)して『バックアップ リストア』ボタンを押します。

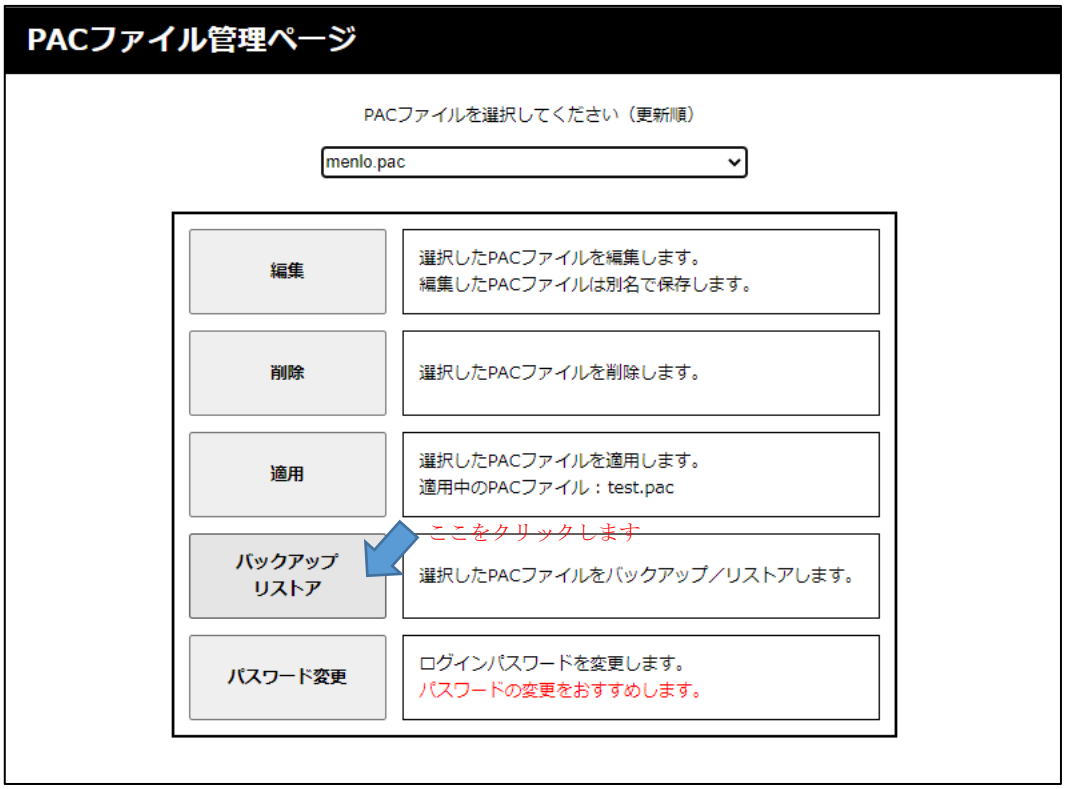
バックアップデータの表示画面に遷移して、”test.pac”のバックアップデータが表示されます。ここで表示される情報は”menlo.pac”に対してお客様が追加したドメイン・IP アドレスのみとなります。
下記の例では 7.4 項で追加したドメイン(example.com)と IP アドレス(192.0.2.0/255.255.255.0)が、それぞれバックアップデータの"user_domains"と"user_ipaddrs"の下に表示されています。
バックアップデータは、コピー&ペーストしてテキストファイル形式で保存して下さい。次のリストアコマンドで、保存したバックアップデータを使って PAC ファイルの復元が可能になります。
『戻る』ボタンで PAC ファイル管理メインページへ戻ります。



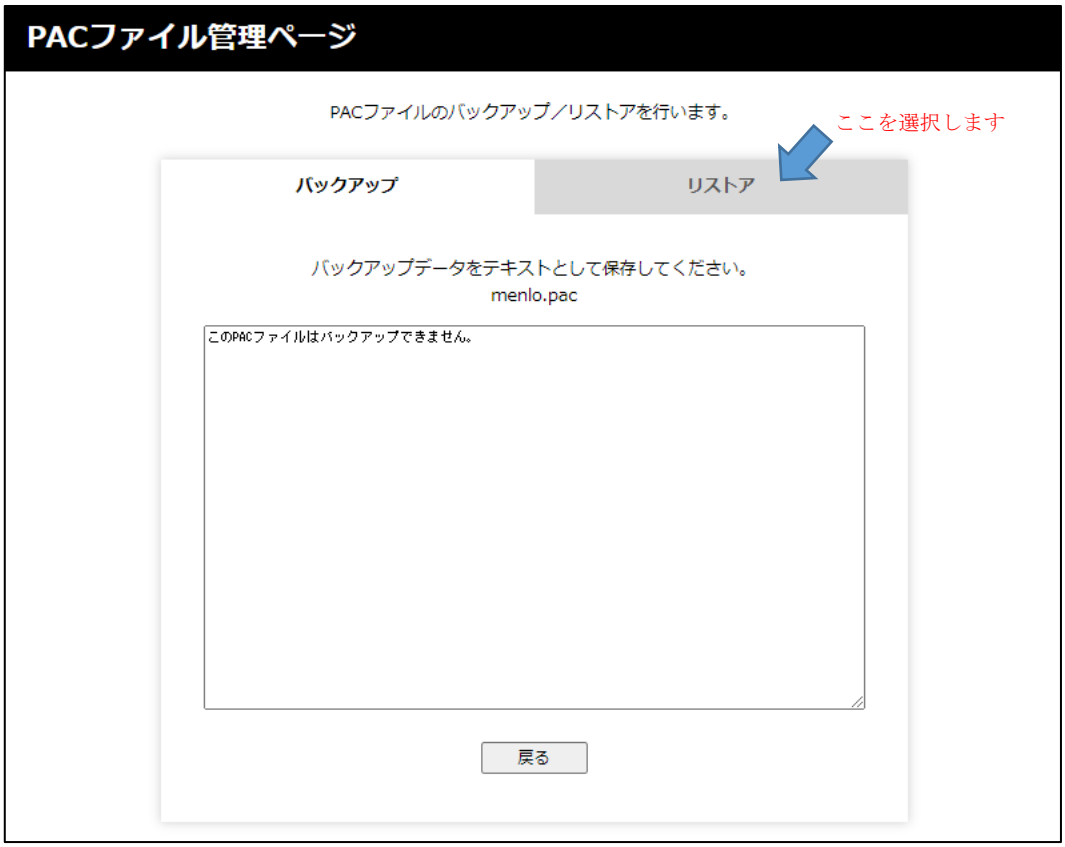
7.7　リストア

7.6 項のバックアップデータを使って、PAC ファイルを復元します。

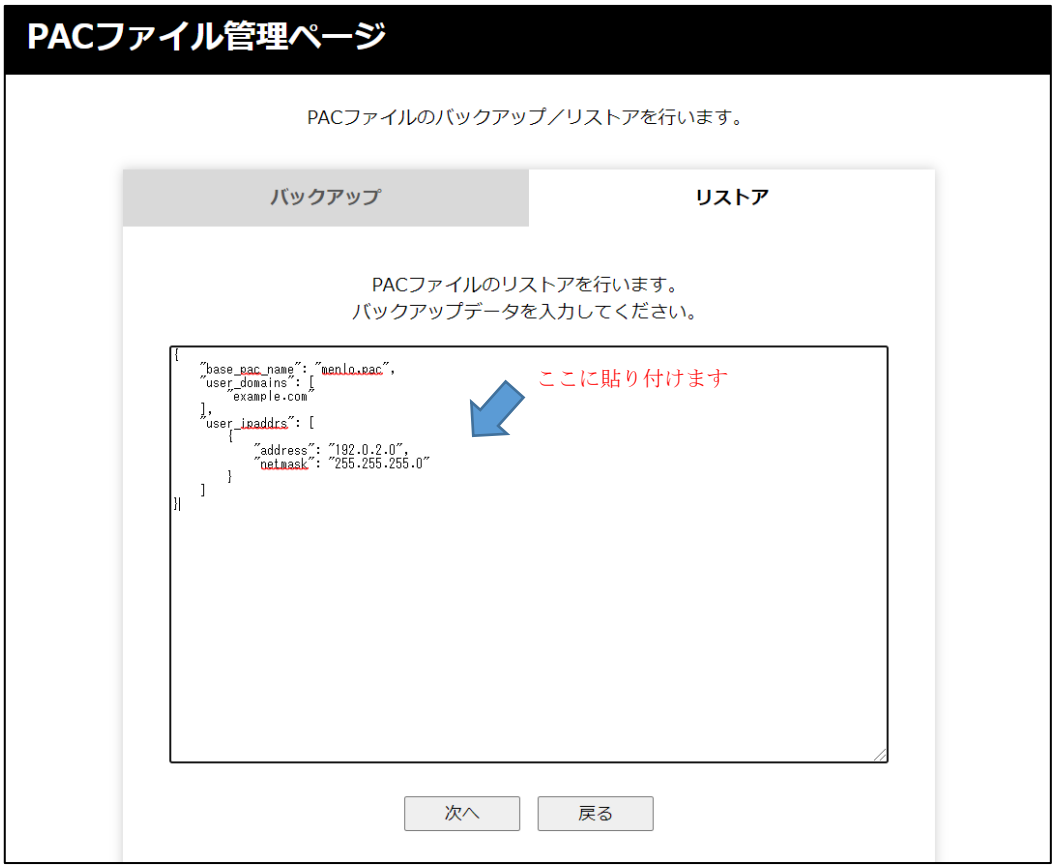
PAC ファイル管理メインページで menlo.pac を選択して『バックアップ リストア』ボタンを押します。



バックアップが選択された状態で確認ページに遷移するので、リストアを選択します。

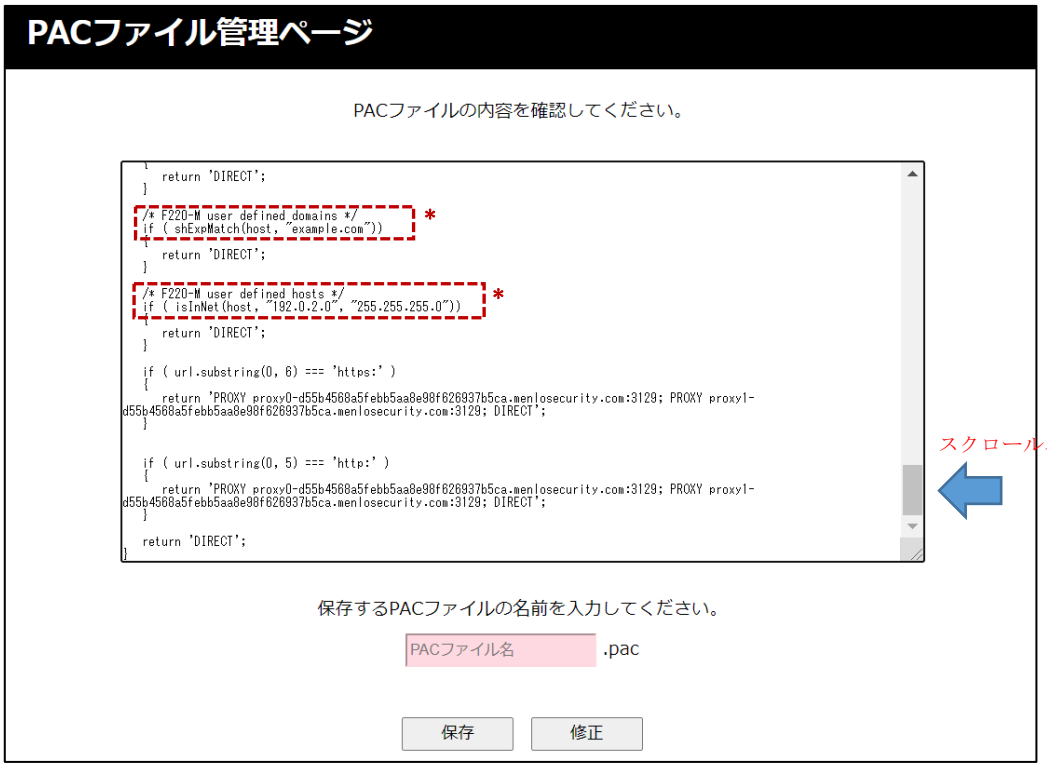


7.6 項で保存したバックアップデータをコピー&ペーストで下記のウインドウに貼り付けます。
PAC ファイルを復元するために下の『次へ』ボタンを押します。



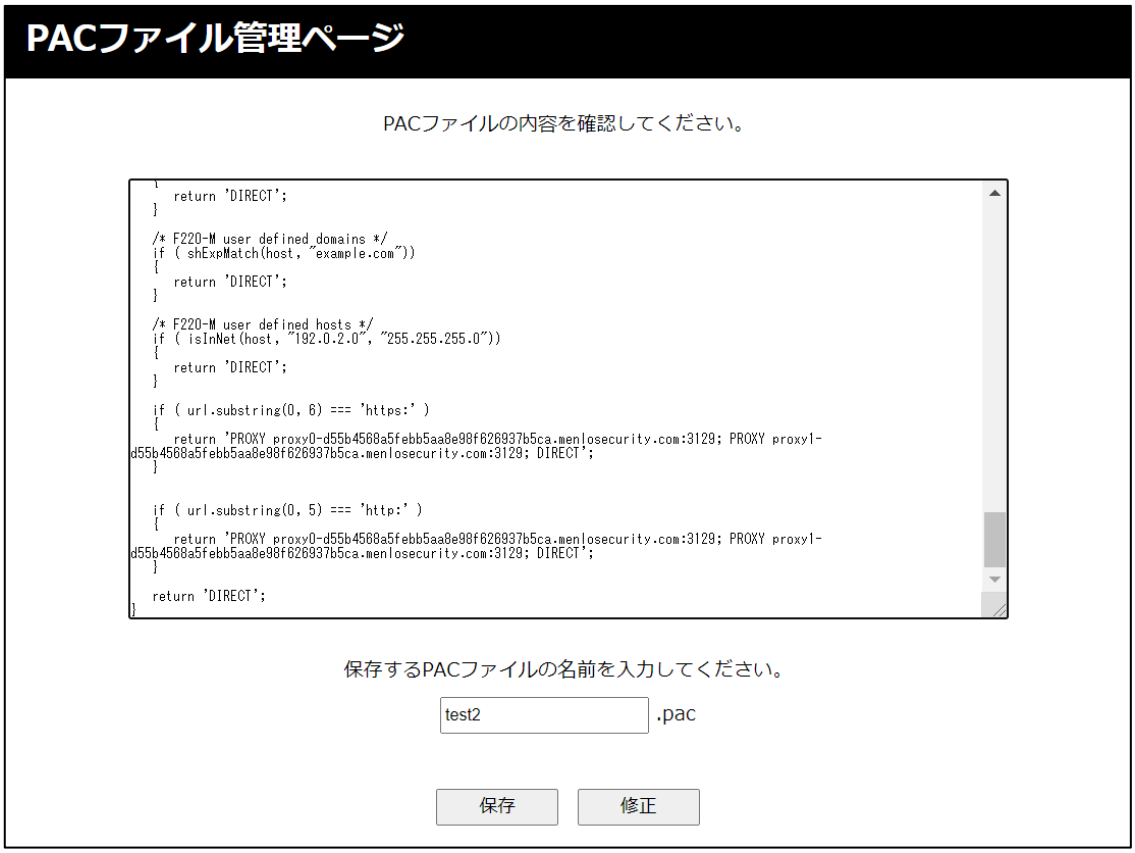
復元した PAC ファイルが表示されます。右端のスクロールバーを一番下に持っていくと、”F220-M user defined domains”の下に追加したドメイン(example.com)、” F220-M user defined hosts”の下に追加した IP アドレス(192.0.2.0/255.255.255.0)が確認できます。

※修正する場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。

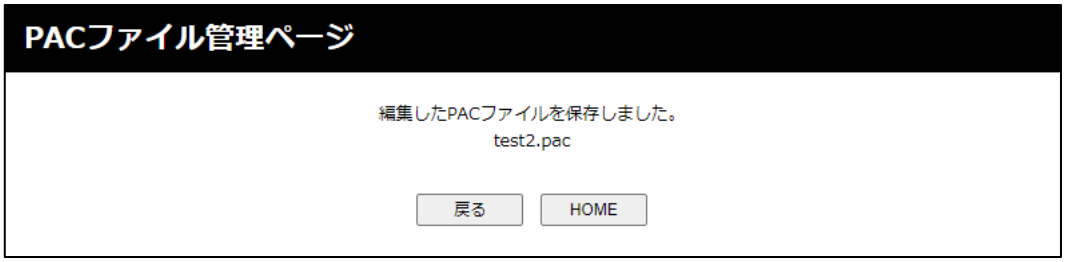


＊全ての機種で「F220-M」と表示されます。お使いの機種に読み替えてご使用ください。

保存する PAC ファイル名を記入(例では”test2”を記入)して下の『保存』ボタンを押します。
※既存のファイル名では保存できませんのでご注意下さい。



“test2.pac”というファイル名で復元が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。

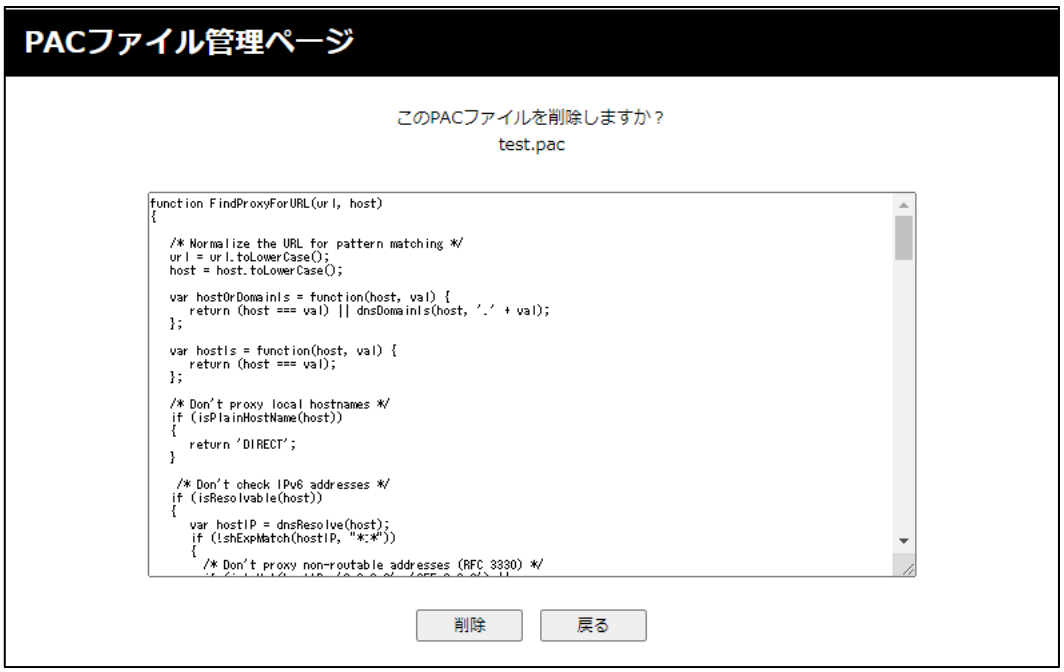


7.8 削除

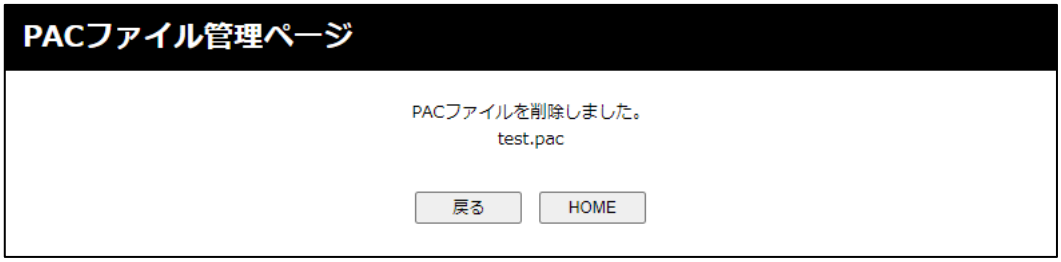
不要な PAC ファイルを削除する場合は、PAC ファイル管理メインページで削除するファイル名を選択して(例では”test.pac”を選択)して『削除』ボタンを押します。

※適用中のファイルや”menlo.pac”、”direct.pac”はエラーとなり削除できませんのでご注意下さい。

確認画面に削除する PAC ファイルが表示され、下の『削除』ボタンを押して削除します。



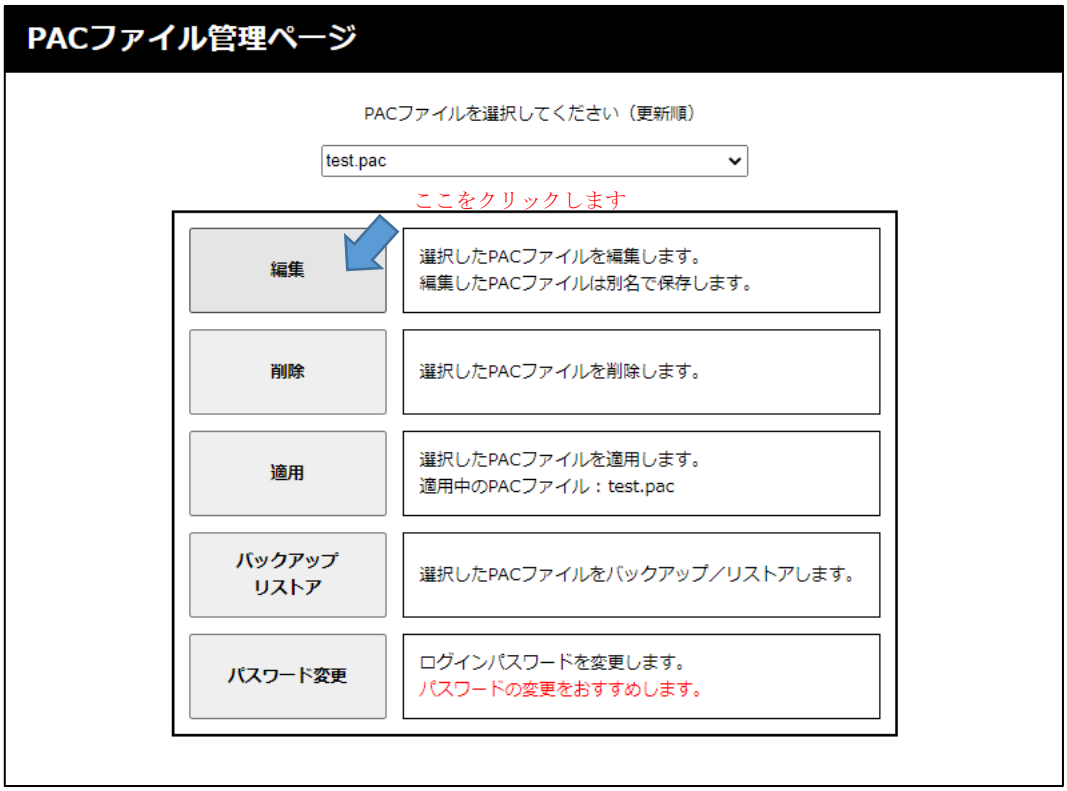
“test.pac”の削除が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。



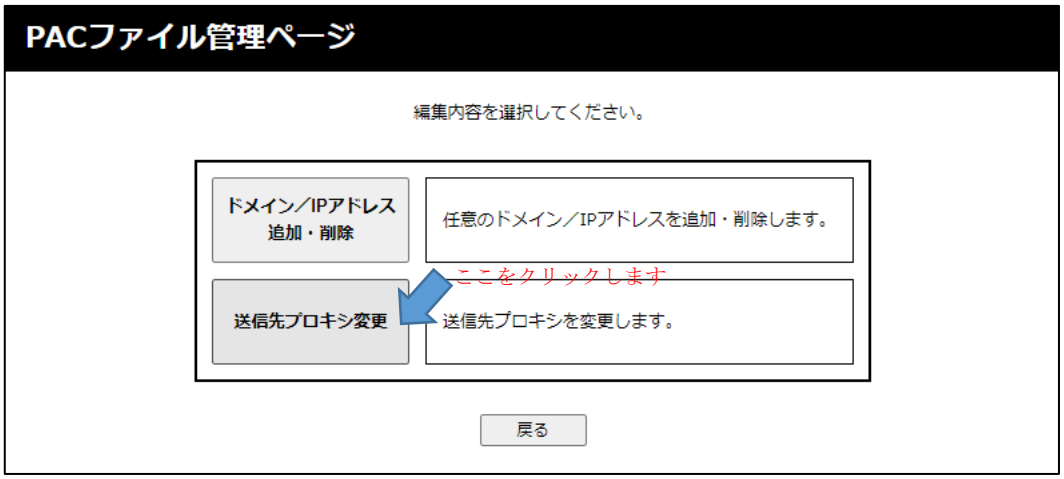
7.9　送信先プロキシ変更

PAC ファイルの送信先プロキシ情報を変更することも可能です。

PAC ファイル管理メインページで変更するファイル名を選択して(例では”test.pac”を選択)して『編集』ボタンを押します。※direct.pac はエラーとなり変更できませんのでご注意下さい。



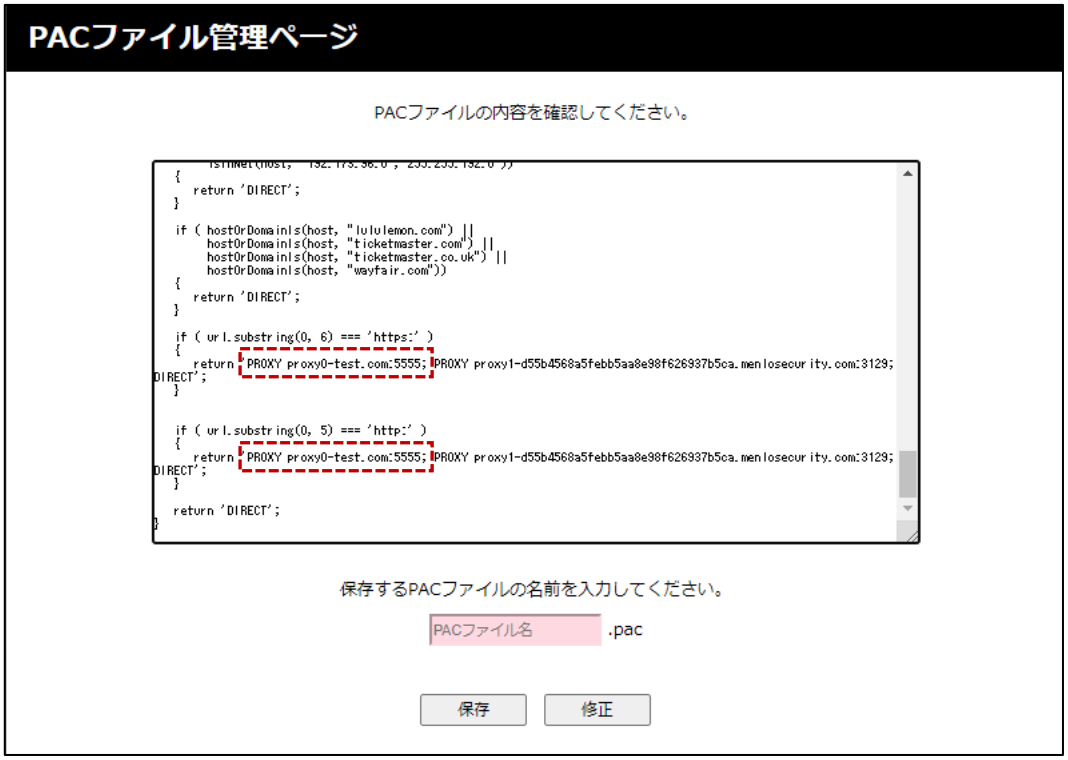
『送信先プロキシ変更』ボタンを押します。



送信先プロキシは２つ設定されており、どちらも変更可能です。

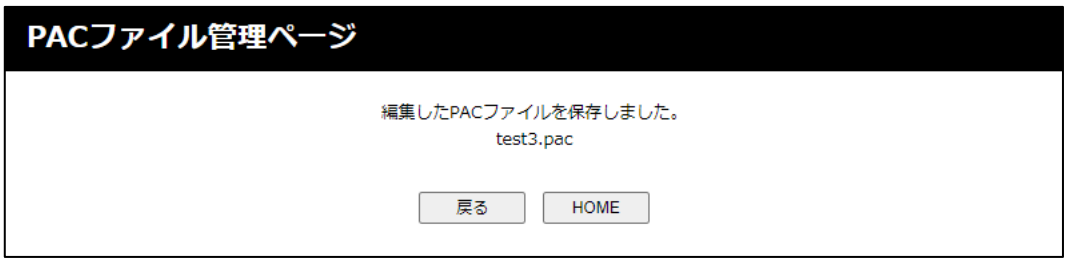
変更する送信先プロキシを記入（例では No1 を”proxy0-test.com：5555”に変更)し『次へ』ボタンを押します。

変更した PAC ファイルが表示されます。右端のスクロールバーを移動すると、No.1 のドメインが”proxy0-test.com：5555”に変更されていることが確認できます。
※修正したい場合は『修正』ボタンを押すことで前の画面に戻って修正が可能です。



保存する PAC ファイル名を記入(例では”test3”を記入)して下の『保存』ボタンを押します。
※既存のファイル名では保存できませんのでご注意下さい。

test3.pac で保存が完了しました。『HOME』ボタンで PAC ファイル管理メインページへ戻ります。



7.10 サポートブラウザ

本機能は、以下のブラウザで動作確認しています。

- Google Chrome(83)
- Firefox(77)
- Microsoft Edge(44.18362.449.0)
- Internet Explorer(11.719.18362.0)（※）
- Safari(13.1)

※Internet Explorer を使用される場合には、ブラウザの[設定](右上歯車マーク)＞[互換表示設定]にて「イントラネットサイトを互換表示で表示する」のチェックを外してご使用下さい。

8 注意事項

“reset clear コマンドによる初期化” や ”装置起動時の初期化 (RESET スイッチを押しながら装置を起動)” を実施された場合、本機能が全てクリアされ使用できなくなりますのでご注意下さい。

付録 A　LAN 側ネットワークをお客様環境に合わせて変更する方法

F F220M は工場出荷時に giga1/1 ポートは 192.168.1.1（192.168.1.0/24 のネットワーク）に、コンテナアドレスは 192.168.1.254 に設定してあります。これらのアドレスをお客様環境に合わせて変更する場合の変更箇所についてご説明します。

冒頭でご説明した F220M のコンフィグにおいて、下記赤枠で囲まれた部分の設定を、お客様ネットワークに合わせて変更をして下さい。

```
container enable
container device disk /mnt/pac_mainte drive uid 101 gid 101
!
container configuration
 !
 interface 1
  bridge-group 1
  ip address 192.168.1.254 255.255.255.0      ←お客様のネットワークに合わせてコンテナアドレスを
  ip gateway 192.168.1.1                        変更して下さい
 exit                    ↑変更後のgiga1/1のアドレスを設定して下さい
 !
exit
 !
access-list 111 deny ip any any
access-list 121 spi ip any any
!
ip host fitelnet-container.fnsc.co.jp 192.168.1.254
!                                              ↑お客様のネットワークに合わせてコンテナアドレスを
ip route 0.0.0.0 0.0.0.0 100.1.1.1               変更して下さい
ip name-server 127.0.0.1
!
ip dhcp server-profile DHCP_SERVER_PROF
 address 192.168.1.2 192.168.1.101          ←お客様のネットワークに合わせてDHCP払い出し
 lease-time 3600                               アドレスレンジを変更して下さい
 dns 192.168.1.1                            ←変更後のgiga1/1のアドレスを設定して下さい
 gateway 192.168.1.1                        ←変更後のgiga1/1のアドレスを設定して下さい
 option 252 ascii http://fitelnet-container.fnsc.co.jp/pac/web_security.pac
exit
!
ip nat list 1 192.168.1.0 0.0.0.255         ←お客様のネットワークに合わせて変更して下さい
!
hostname FITELnet
!
interface GigaEthernet 1/1
 vlan-id 1
 bridge-group 1
 channel-group 1
 container-use
exit
!
```

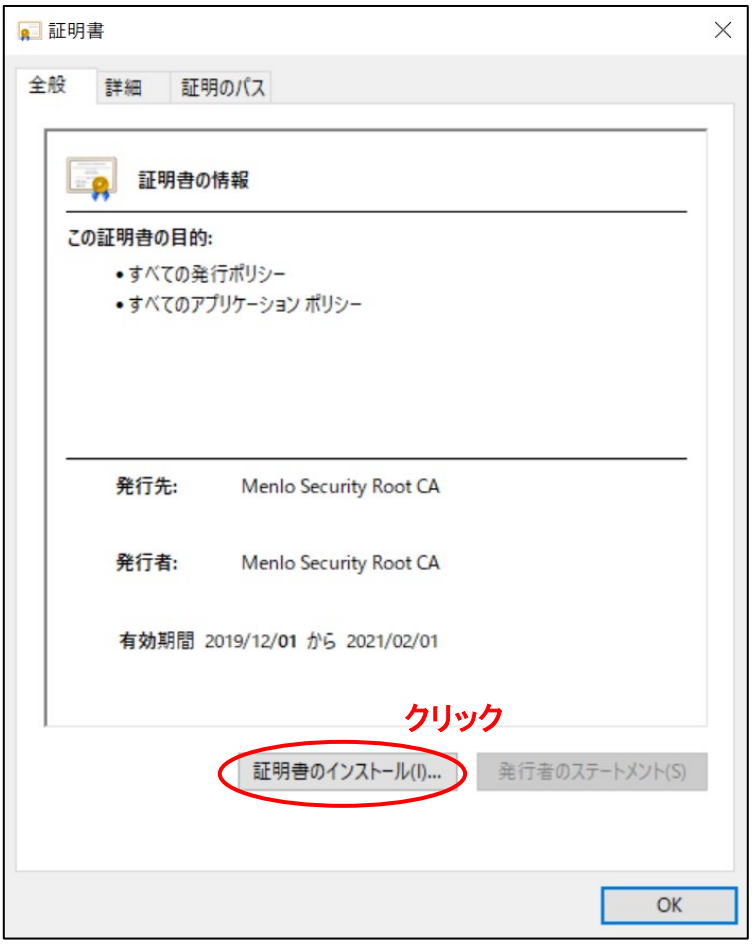
```
interface GigaEthernet 2/1
 vlan-id 21
 bridge-group 21
 channel-group 21
 ip access-group 111 in
 ip access-group 121 out
exit
!
interface Port-channel 1
 ip dhcp service server
 ip dhcp server-profile DHCP_SERVER_PROF
 ip address 192.168.1.1 255.255.255.0
 link-state always-up
exit
!
interface Port-channel 21
 ip address 100.1.1.2 255.255.255.0
 ip nat inside source list 1 interface
exit
!
dns-server ip enable
!
proxydns domain 1 any * any static x.x.x.x
!
end
```

←お客様のネットワークに合わせてgiga1/1のアドレスを変更して下さい

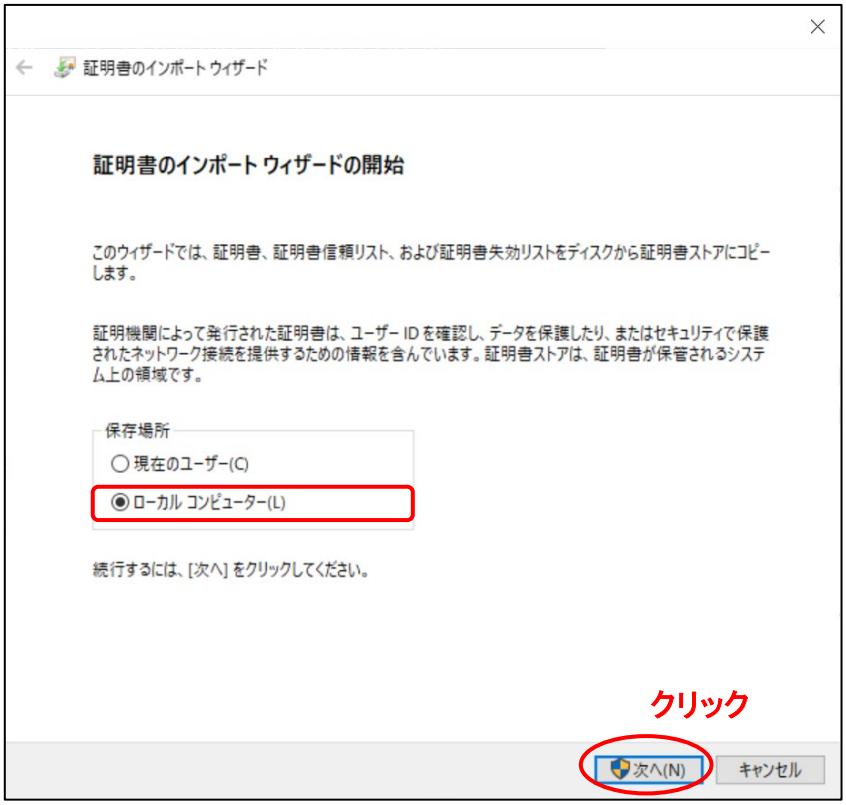
付録 B　Windows10 に CA 証明書をインストールする方法

入手した CA 証明書（例：MenloSecurityCACert2020.cer）をインストールするクライアント PC のデスクトップ上に置きダブルクリックします。

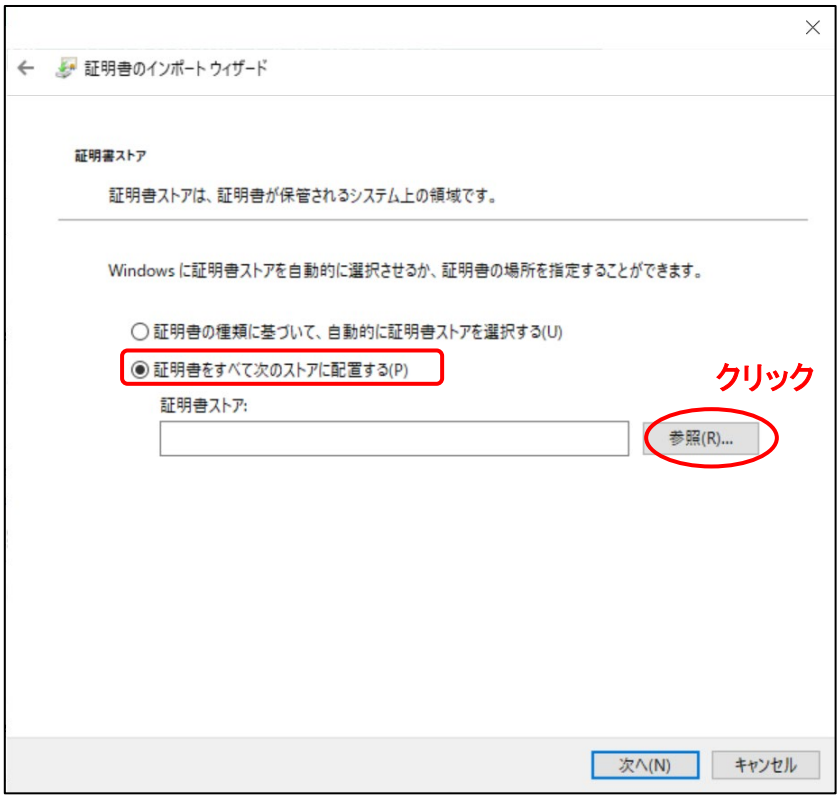
次の証明書ダイアログが表示されたら、『証明書のインストール』をクリックします。



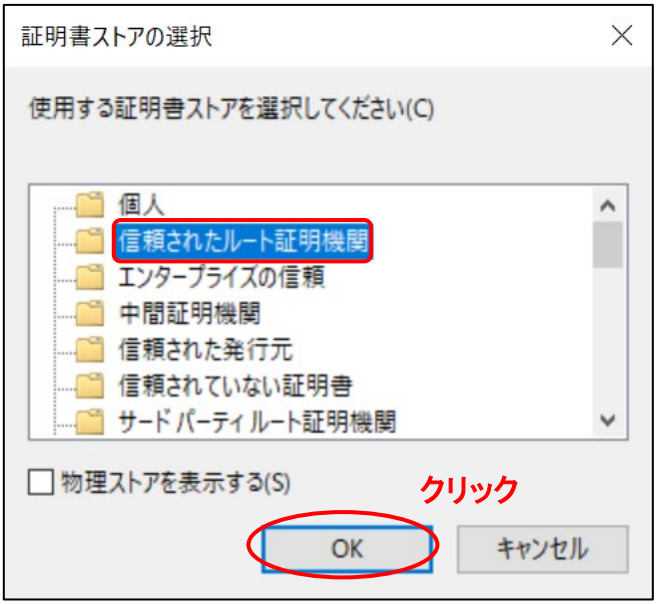
次の画面が表示されたら、保存場所『ローカルコンピュータ』を選択して『次へ』をクリックします。



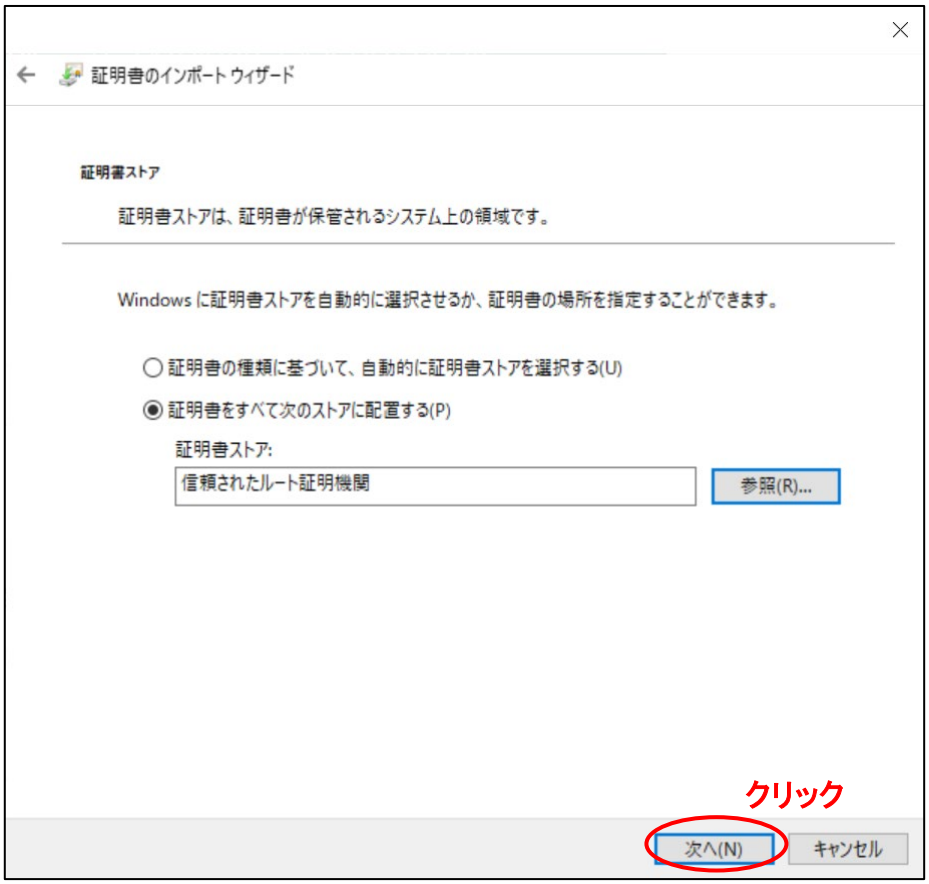
次の画面が表示されたら、『証明書をすべて次のストアに配置する』を選択して『参照』をクリックします。



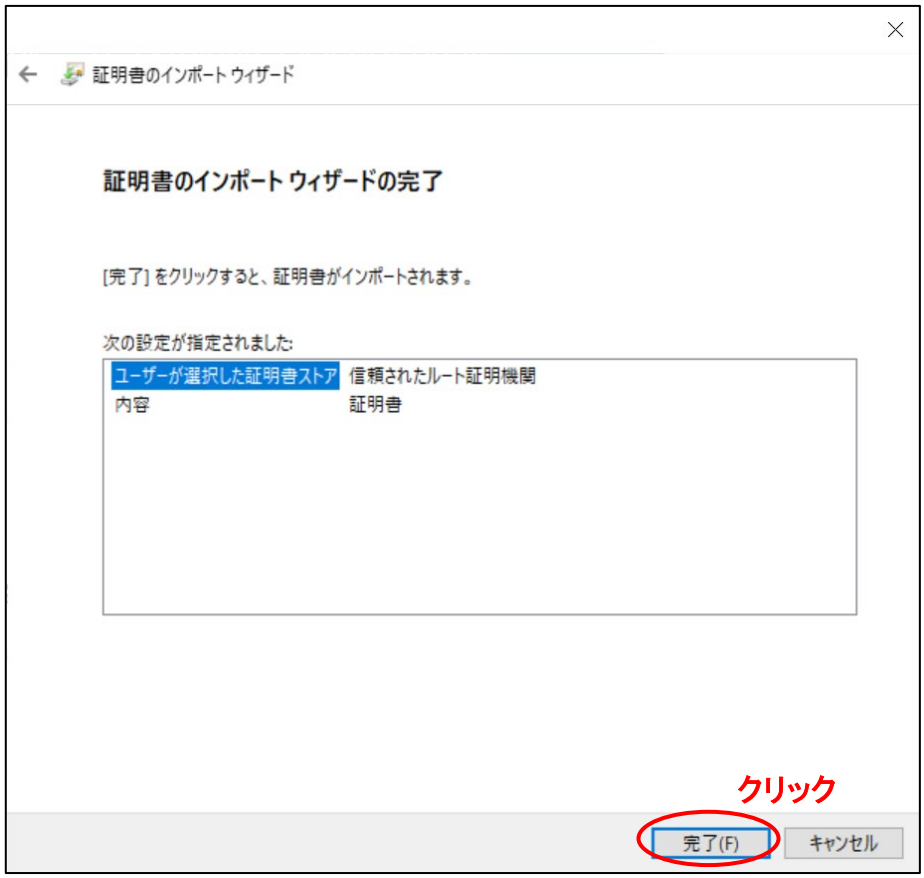
次の画面が表示されたら、『信頼されたルート証明機関』を選択して『OK』をクリックします。



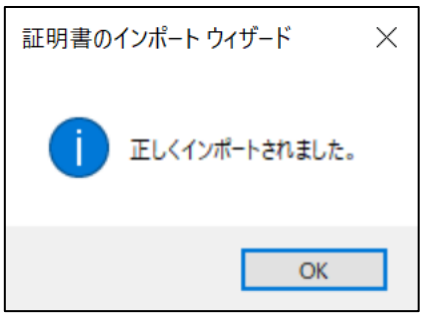
次の表示が確認できたら『次へ』をクリックします。



次の表示が確認できたら『完了』をクリックします。



『正しくインポートされました。』のメッセージが表示されれば完了です。



付録 C　リモートアクセス機能

リモート環境から F220M へアクセスし、分離・無害化サービスを利用する場合の設定方法についてご説明します。構成例を図 3 に示します。

クライアント PC と F220M は L2TP/IPsec でトンネル接続を行います。この時、クライアント PC には 192.168.1.102~192.168.1.200 の範囲のアドレスが払い出されます。トンネル接続後、ルータは PPP によりクライアント PC に DNS サーバアドレス（ルータ）情報を通知し、クライアント PC はプロキシ自動検出動作によりプロキシ設定情報である wpad.dat ファイル(PAC ファイルと同一)をコンテナから取得します。取得したプロキシ設定をもとに分離・無害化サービスを通したインターネットアクセスが可能になります。

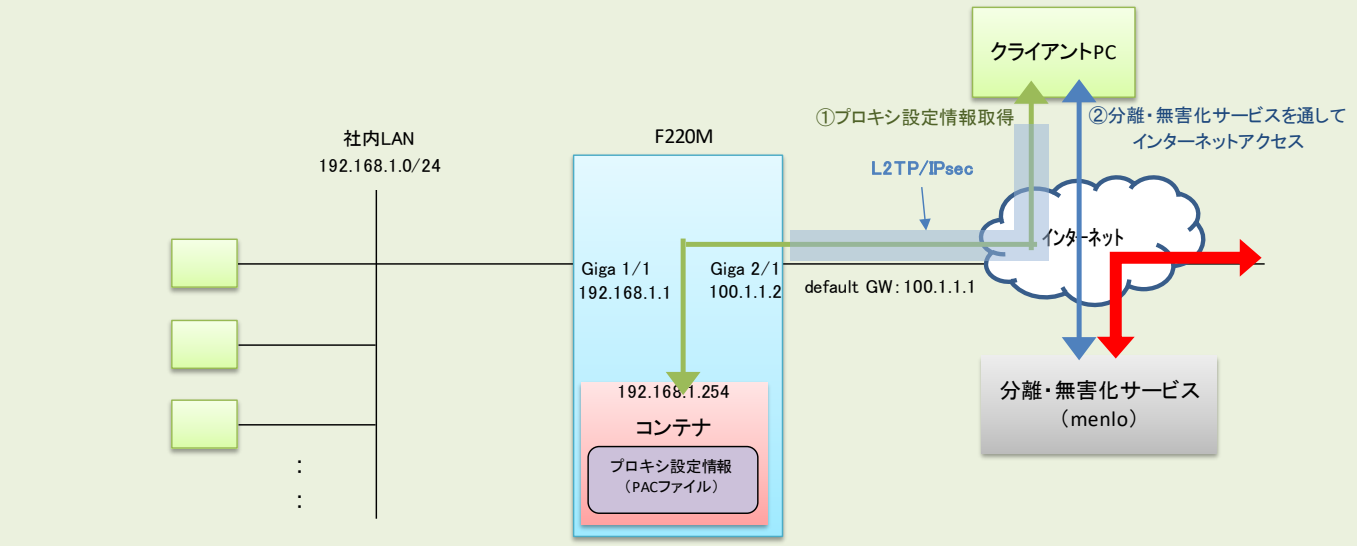


図 3 F220M リモートアクセス 構成図

次にリモートアクセス機能を実現するための F220M とクライアント PC の設定についてご説明します。

C-1　ルータ設定

F220M のコンフィグを以下に示します。前述(4 項)のコンフィグに赤字部分の設定が追加されています。

```
container enable                                          ←コンテナのサービスを有効にする設定
container device disk /mnt/pac_mainte drive uid 101 gid 101
!
container configuration
 !
 interface 1
  bridge-group 1
  ip address 192.168.1.254 255.255.255.0
  ip gateway 192.168.1.1
 exit
 !
exit
 !
access-list 100 permit udp any host 100.1.1.2 eq 500    ←フィルタ設定（ISAKMPパケット許可）
access-list 100 permit udp any host 100.1.1.2 eq 4500   ←フィルタ設定（ISAKMPパケット許可）
access-list 100 permit 50 any any                       ←フィルタ設定（ESPパケット許可）
```

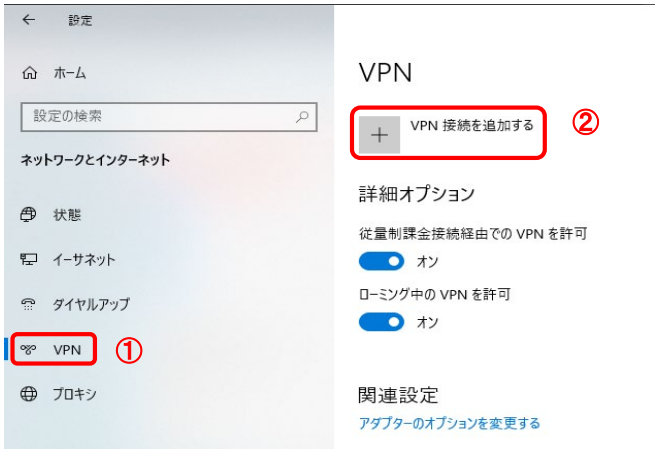
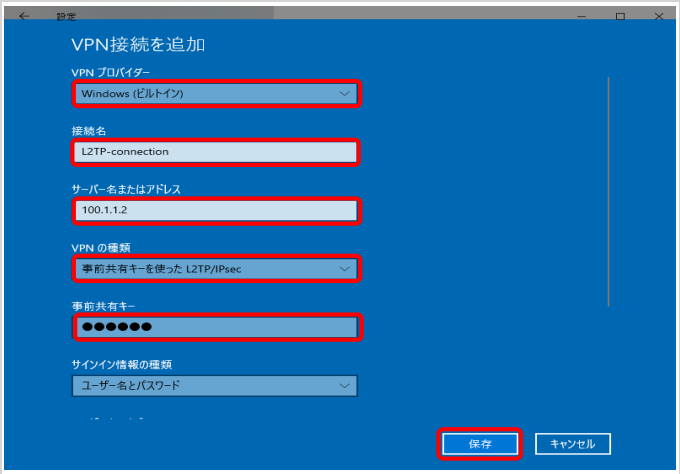
```
access-list 111 deny ip any any                          ←学習フィルタ設定
access-list 121 spi ip any any                           ←学習フィルタ設定
!
ip host fitelnet-container.fnsc.co.jp 192.168.1.254      ←コンテナアドレスにホスト名
ip host wpad.example.com 192.168.1.254                   (fitelnet-container.fnsc.co.jp)登録
!
ip route 0.0.0.0 0.0.0.0 100.1.1.1                       ←デフォルトルートを設定
ip name-server 127.0.0.1
ip local pool POOL1 192.168.1.102 192.168.1.200          ←L2TP/PPPにより通知するアドレス範囲
!                                                          の確定
ip dhcp server-profile DHCP_SERVER_PROF                  ←DHCPサーバ機能のプロファイル
 address 192.168.1.2 192.168.1.101                       ←DHCP払い出しアドレスレンジ
 lease-time 3600                                         ←払い出し情報のリース時間(秒)
 dns 192.168.1.1
 gateway 192.168.1.1
 option 252 ascii http://fitelnet-container.fnsc.co.jp/pac/web_security.pac
exit                                                     ↑PACファイル置き場情報
!
ip nat list 1 192.168.1.0 0.0.0.255                      ←192.168.1.0/24 を list 1 と定義
!
aaa authentication ppp LOCAL_AUTH local-group LOCAL_GROUP
!                                                        ↑PPPoEセッションの認定方式を設定
aaa local group LOCAL_GROUP                              ←クライアントデータベース設定モード
 username user1 password secret1                         ←接続を許可するユーザ名/パスワード設定
exit
!
hostname FITELnet
!
crypto ipsec policy IPSECPOL_1                           ←IPsecポリシー設定(Phase2)
 mode transport
 set security-association lifetime seconds 86400
 set security-association transform-keysize aes 128 256 256
 set ip df-bit 0
 set ip fragment post
 set udp-encapsulation nat-t keepalive interval 30 always-send
exit
!
crypto isakmp keepalive always-send                      ←DPD設定
crypto isakmp log sa detail
crypto isakmp log session detail
crypto isakmp log negotiation-fail detail
!
crypto isakmp policy ISAPOL_1                            ←ISAKMPポリシー設定(Phase1)
 authentication pre-share
 encryption aes
 encryption-keysize aes 256 256 256
 group 1 2 5 14 15
 lifetime 86400
 hash sha
 initiate-mode main
exit
```

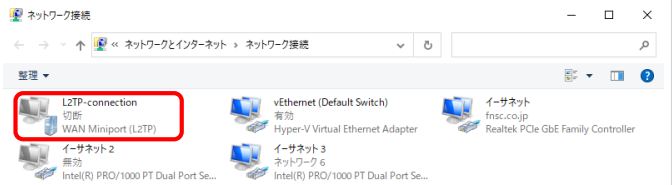
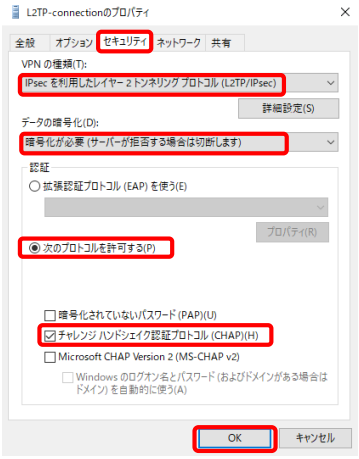
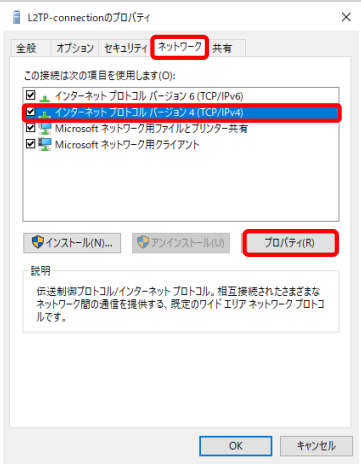
```
!
crypto isakmp profile ISAPROF_001                    ←ISAKMPプロファイル設定
 set isakmp-policy ISAPOL_1                          ←ISAKMPポリシーを指定
 set ipsec-policy IPSECPOL_1                         ←IPsecポリシーを指定
 ike-version 1                                       ←IKEバージョンを指定
 local-key secret                                    ←Pre-shared Keyを指定
exit
!
crypto map MAP_001 ipsec-isakmp dynamic              ←crypto MAP設定
 set isakmp-profile ISAPROF_001                      ←セレクタを指定
exit
!
interface GigaEthernet 1/1
 vlan-id 1
 bridge-group 1
 channel-group 1
 container-use
exit
!
interface GigaEthernet 2/1
 vlan-id 21
 bridge-group 21
 channel-group 21
 ip access-group 100 in                              ←ISAKMP、ESPを通す設定
 ip access-group 111 in                              ←WAN側からのアタックを防ぐための
 ip access-group 121 out                               学習フィルタ設定
exit
!
interface Port-channel 1
 ip dhcp service server                              ←giga1/1にDHCPサーバ機能を設定
 ip dhcp server-profile DHCP_SERVER_PROF             ←DHCPサーバ機能のプロファイル名を指定
 ip address 192.168.1.1 255.255.255.0
 ip proxy-arp                                        ←proxy-arp動作を行う設定
 link-state always-up
exit
!
interface Port-channel 21
 ip address 100.1.1.2 255.255.255.0
 ip nat inside source list 1 interface               ←list 1に含まれる送信元アドレスを
exit                                                   インタフェースのアドレスにNAT変換する
!
dns-server ip enable
!
proxydns domain 1 any * any static x.x.x.x           ←お客様環境に合わせてDNSサーバを指定
!                                                      して下さい(x.x.x.x の部分)
end
```

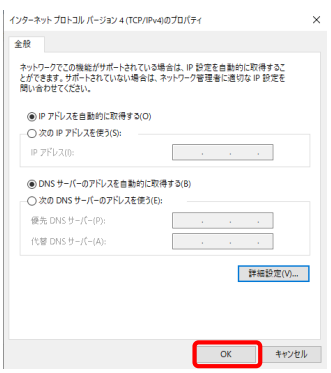
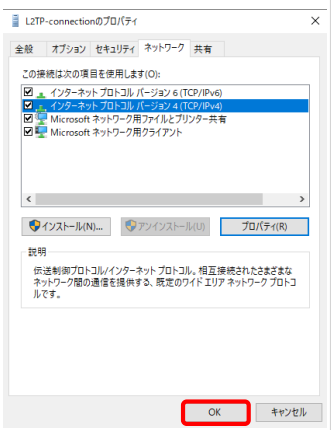
C-2　クライアント PC 設定

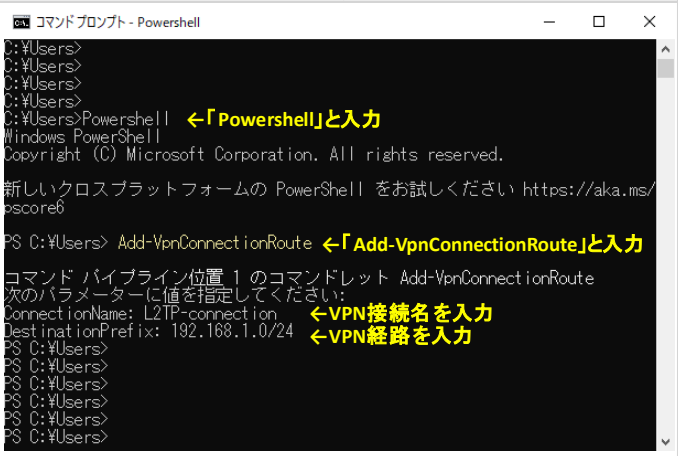
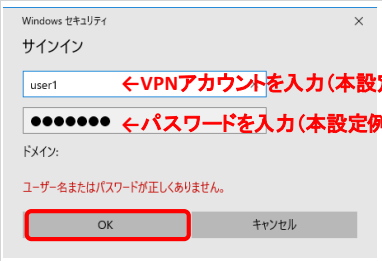
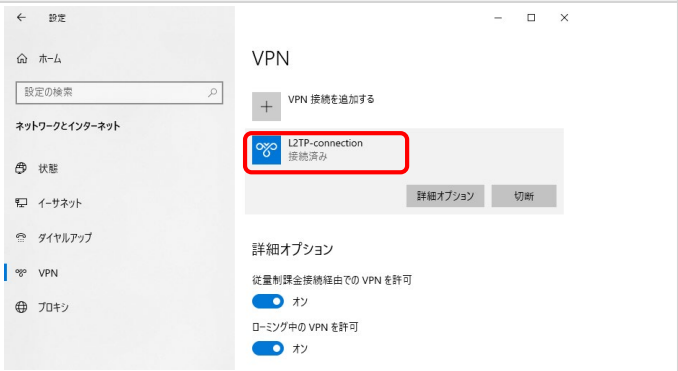
クライアント PC の設定手順は次のようになります。

※windows10 を例にご説明します。

手順	設定内容	画面表示
1	①Windows10左下のスタートボタンをクリックします。 ②「設定」を選択します。	
2	「設定」のメニュー画面が表示されたら、「ネットワークとインターネット」を選択して、次を実行します。 ①左側のメニューで「VPN」を選択します。 ②右のような画面が表示されたら「VPN接続を追加する」をクリックします。	
3	右の画面が表示されますので、以下の5つの情報を入力もしくは確認します。 1) VPNプロバイダー: 「Windows(ビルトイン)」と表示されていることを確認します。 2) 接続名：任意の名前を入力します。 3) サーバ名またはアドレス：お使いの環境に合わせて接続先のサーバー名もしくはアドレスを入力します。本設定例ではFITELnet装置のWAN側アドレス(100.1.1.2)となります。 4) VPNの種類: 「事前共有キーを使ったL2TP/IPsec」を選択します。 5) 事前共有キー：事前共有キー(Pre-shared Key)の文字列を入力します。設定例では「secret」です。 上記5つの情報を入力したら、右下の「保存」をクリックしてください。	
4	手順2の画面が再び表示されますので、手順3で追加した接続名が表示されることを確認します。	

手順	設定内容	画面表示
5	「ネットワークとインターネット」のメニューで「イーサネット」を選択します。「アダプターのオプションを変更する」をクリックします。	
6	手順3で追加したVPN接続名を右クリックして、プロパティをクリックします。	
7	プロパティのセキュリティタブを開き、以下を選択して、OKをクリックします。 1)VPNの種類: IPsecを利用したレイヤー2トンネリングプロトコル(L2TP/IPsec) 2)データの暗号化:暗号化が必要 3)認証:次のプロトコルを許可する チャレンジハンドシェイク認証プロトコル(CHAP)	
8	プロパティのネットワークタブを開き、「インターネットプロトコルバージョン4」をチェックして、プロパティをクリックします。	

手順	設定内容	画面表示
9	詳細設定をクリックします。	
10	「リモートネットワークでデフォルトゲートウェイを使う」のチェックを外して、DNSタブを開きます。	
11	「この接続のDNSサフィックス」のところに「example.com」と入力して、OKをクリックします。	
12	インターネットプロトコルバージョン4のプロパティに戻りましたら、OKをクリックします。 VPN接続名のプロパティに戻りましたら、OKをクリックします。	 

手順	設定内容	画面表示
13	コマンドプロンプトにてPowershellを実行して、右の画面のようにVPN接続先の経路情報を登録します。本設定例では、FITELnet装置のLAN側のホストと通信するために、192.168.1.0/24を登録します。	
14	設定＞ネットワークとインターネット　のメニューでVPN接続を選択して、手順3で追加したVPN接続名を選択して、「接続」をクリックします。	
15	VPNアカウントとパスワードを入力して、OKをクリックします。	
16	「接続済み」の表示が確認されたら、接続完了です。	

上記設定後、L2TP トンネル接続した状態で、前述 6 項の手順を行うことで分離・無害化サービスを通したインターネットアクセスが可能となります。

以上