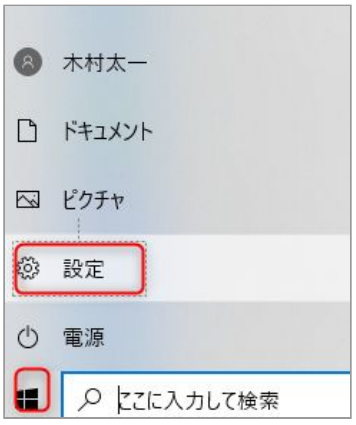
2020年4月13日

VPN（L2TP/IPsec）クライアント設定

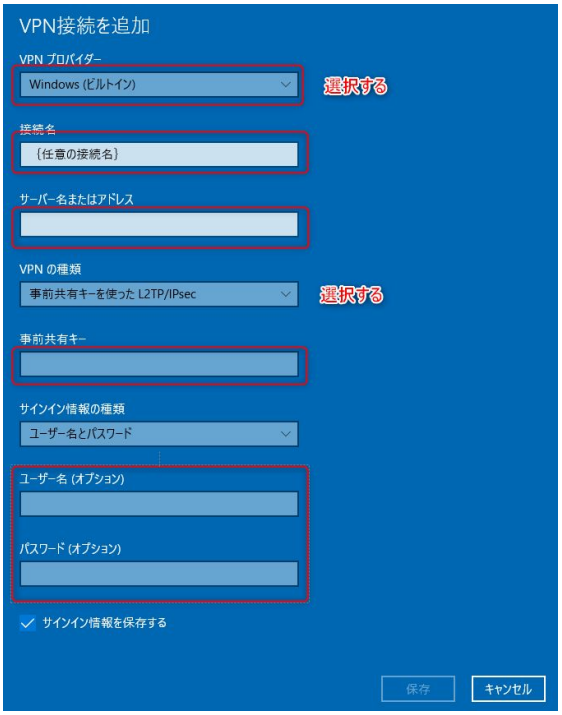
Windows10版

はじめからWindows10のモデルとアップグレードしたモデルだと設定方法が違います。
アップグレードしたモデルは「Windowsサービス」の動作の確認と、レジストリの変更が必要になることが多いです。

基本のVPN設定



スタートボタンより設定をクリックします。
設定画面が開くので、「ネットワークとインターネット」をクリック。
左メニューのVPNより「VPN接続を追加する」をクリックします。

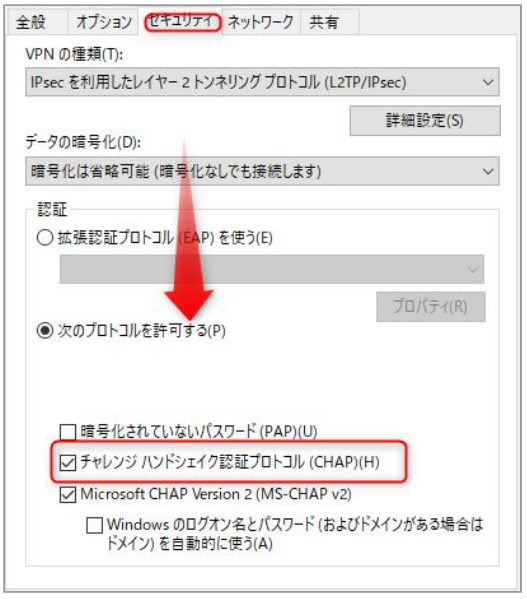


VPNプロバイダー：Windows(ビルトイン)
接続名：任意の接続名
サーバー名またはアドレス：

VPNの種類：事前共有キーを使ったL2TP/IPsec
事前共有キー：

サインイン情報の種類：ユーザー名とパスワード
ユーザー名：
パスワード：
（別途ご案内します）
こちらで基本設定は完了です。

認証のCHAPを有効にしているか確認

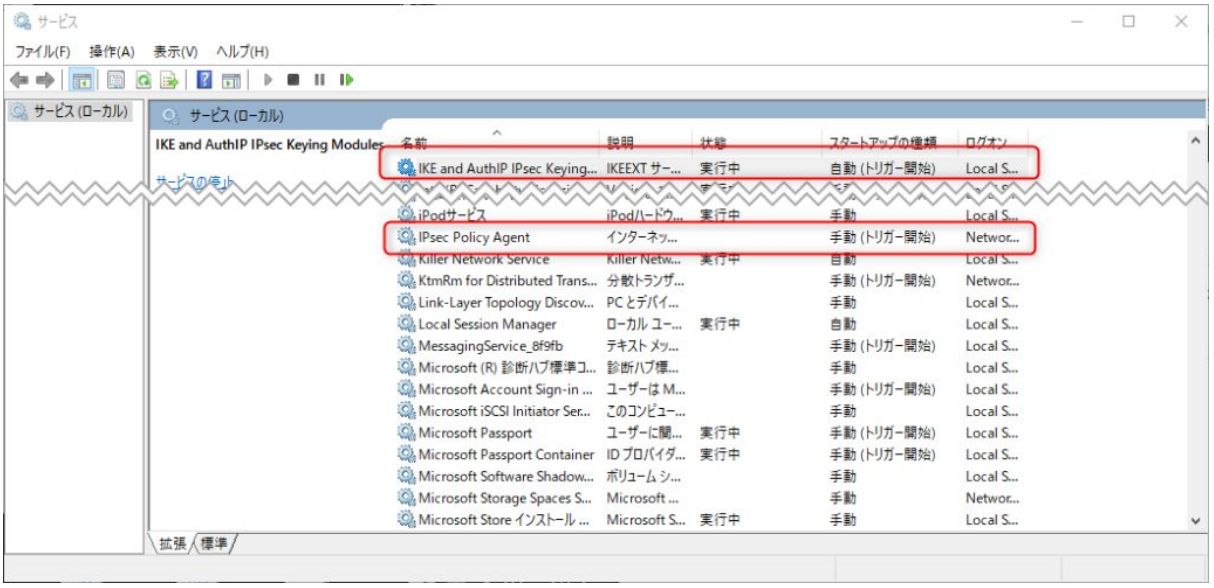


コントロールパネル＞ネットワークとインターネット＞ネットワークと共有センター＞（左メニュー）アダプターの設定の変更。

該当の接続を右クリック＞プロパティ。セキュリティタブの「チャレンジハンドシェイク認証プロトコル（CHAP）にチェックを入れる。

Windowsサービスの確認

IKE and AuthIP IPsec Keying ModulesとIPsec Policy Agentが起動しているか確認します。
【Win+R】で開いたウインドウに「services.msc」と入力して「OK」。サービス設定画面になるので、「IKE and AuthIP IPsec Keying Modules」、「IPsec Policy Agent」を探して、実行中になっていなければ、右クリックして「開始」を押す。



今後毎回手動で起動するのは面倒です。Windowsの起動時に起動させる場合は、右クリックして、プロパティーをクリック。「スタートアップの種類」の項目を「自動」に設定します。

レジストリの変更

1. 【Win+R】で開いたウインドウに「regedit」と入力
2. 「HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent」を右クリック。
3. 「新規」→「DWORD値（32ビット）」をクリック。
4. 「新しい値＃１」ができるので、右クリックして「名前の変更」をクリック。
5. 「AssumeUDPEncapsulationContextOnSendRule」と入力します。
6. 新しくできた「AssumeUDPEncapsulationContextOnSendRule 」を右クリックし、「修正」をクリックし「値のデータ」に「2」といれ、OKを押す。
7. パソコンを再起動。

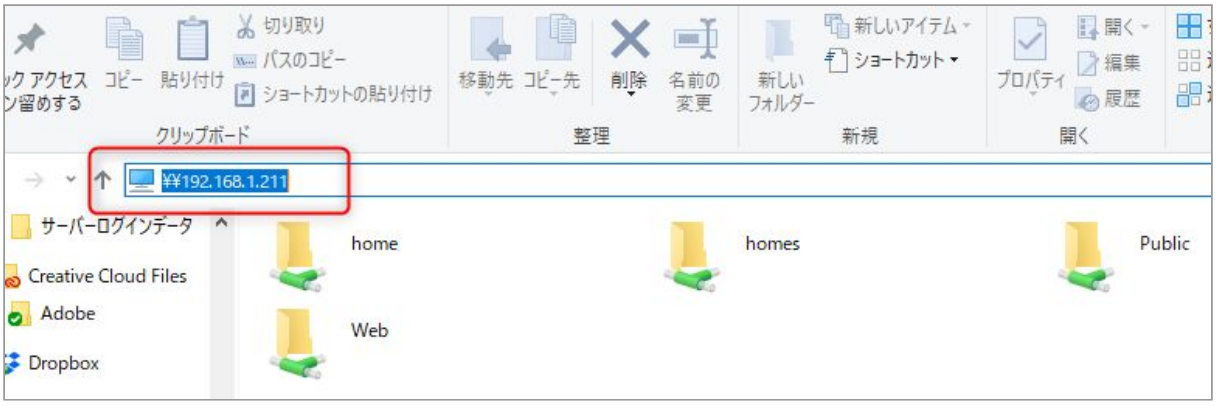
上記作業でもつながらない場合は、ルーターの設定を見直します。

ルーターの設定

IPsecパススルー機能が有効になっているか確認しましょう。

接続後

接続後はサーバーにアクセスできます。



エクスプローラーに直接IPアドレスを打つ「￥￥xxx.xxx.xxx.xxx」(￥は半角)