

Windows 10 によるユーザー認証(802.1x)による 有線 LAN 利用方法

更新日:2020 年 11 月 19 日
筑波大学学術情報メディアセンター

注意

筑波大学構成員に限り再配布を認めます。

謝辞

この資料の作成には、数理物質系情報環境委員会の皆様にご協力いただきました。

概要

Window OS を用いて、有線 LAN により筑波大学の認証ネットワークに接続する際に必要となる設定を説明いたします。設定は、大きく 3 つのステップからなります。

1. Wired AutoConfig サービスを起動する。
2. (利用する有線 LAN 用の)ネットワークアダプタの設定を変更する。
3. ケーブルを接続して認証を行う。

なお、1と2は、1度設定するだけよいです。3については、ネットワークに接続する際に毎回行います。なお、3については、ユーザ名、PW を PC に記憶させることにより自動化することが可能ですが、その方法については、ここでは説明しません。

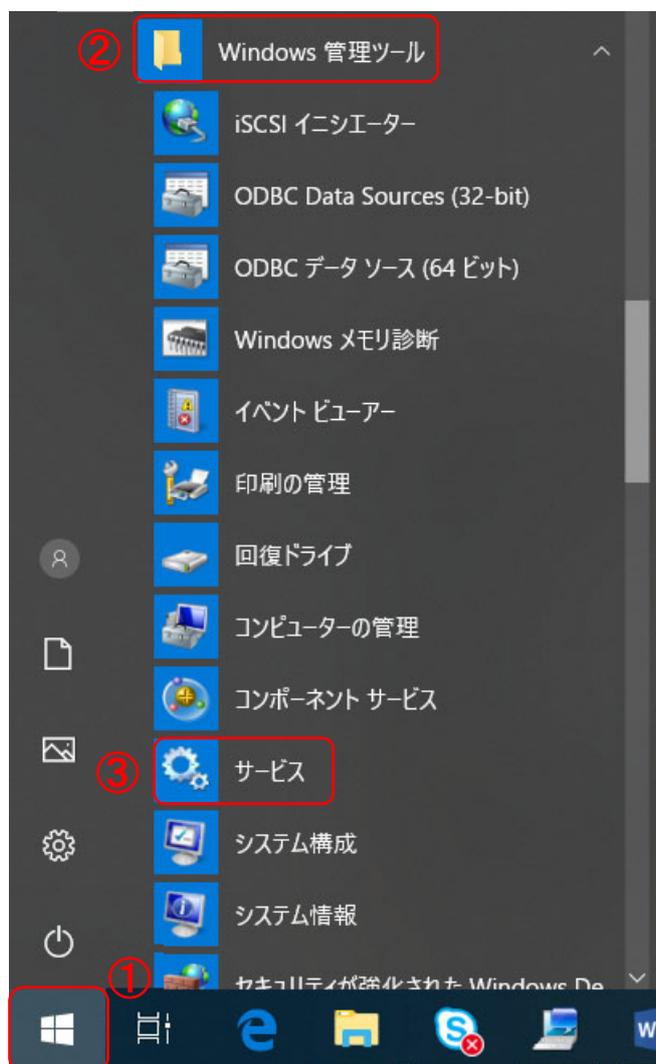
Wired AutoConfig サービスを起動する。

筑波大学の認証ネットワークで利用している 802.1x 認証を有線 LAN にて利用する場合には、Windows OS にて「Wired AutoConfig」を起動させる必要があります。このためには「サービス管理ツール」の中から設定を行います。ここでは、それらの手順を説明します。

1. 「サービス管理ツール」を起動する。

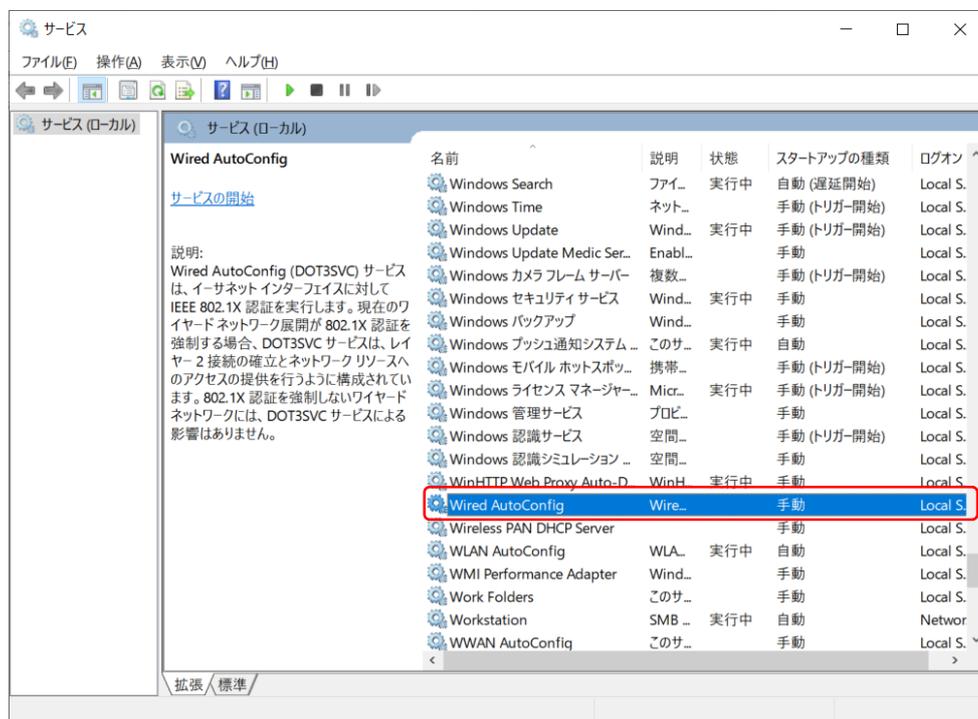
右の図を参考にして以下の1つを行うと「サービス管理ツール」を起動します。

- ① 「スタートメニュー」をクリックする。
- ② 「Windows 管理ツール」をクリックする。
- ③ 「サービス」をクリックする。



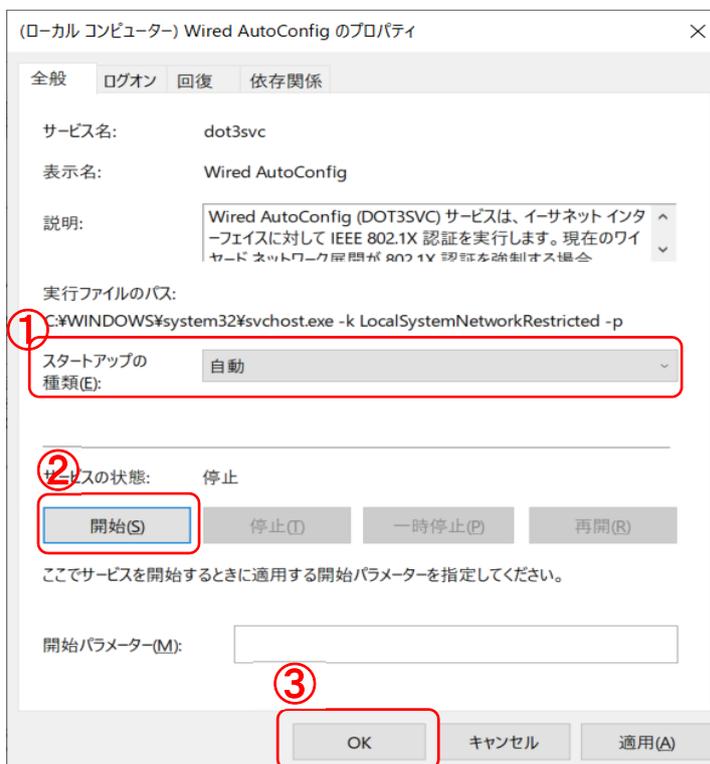
2. 「Wired AutoConfig」が起動されるように設定する。

2-1. サービス管理ツールの中から「Wired AutoConfig」を選択します。



2-2. 「Wired AutoConfig のプロパティの中で以下の 3 つを行って、「Wired AutoConfig」が自動で起動するようにします。

- ① 「スタートアップの種類」を「自動」にする。
- ② 「サービスの状態」を「開始」にする。
- ③ 「OK」をクリックする。



ネットワークアダプターの設定変更

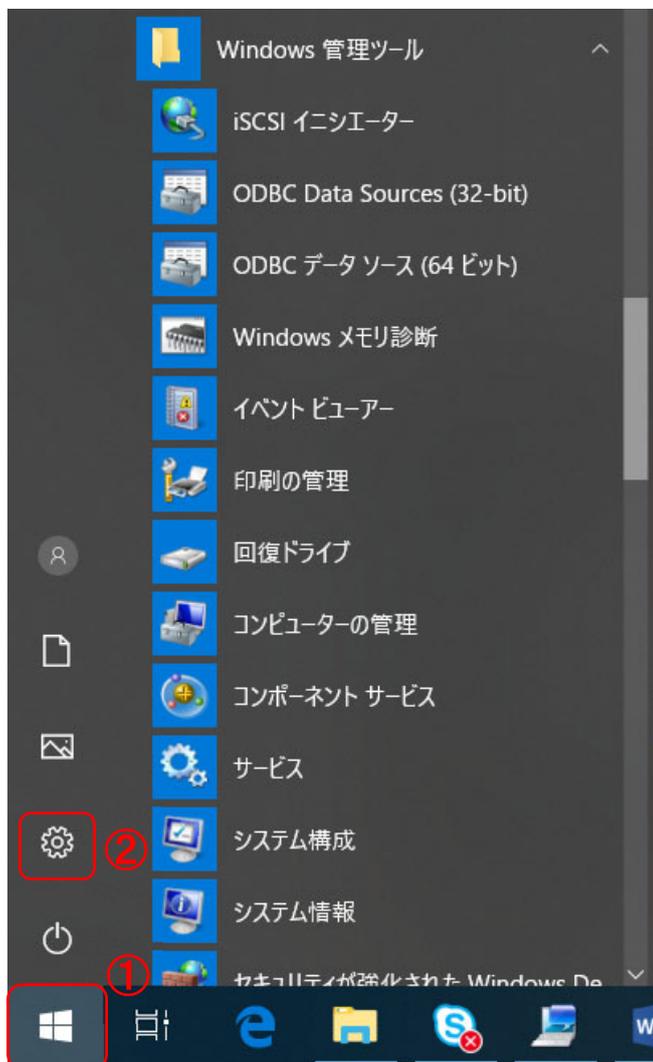
有線 LAN に接続する際に使用するネットワークアダプタの設定を変更します。そのために、ネットワークアダプタのプロパティ変更の画面を開き、その画面で変更作業を行います。ここではその順を説明します。

1. ネットワークアダプタのプロパティ変更画面を開く

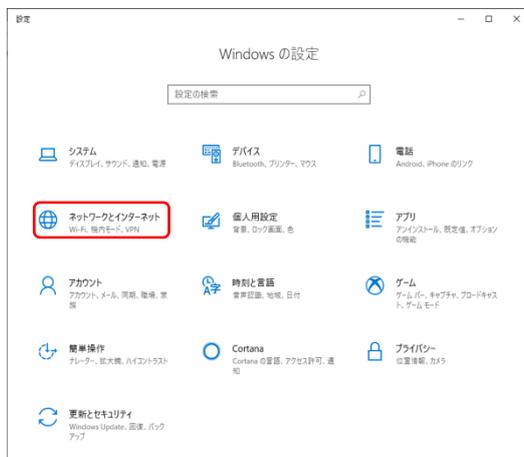
この方法はお使いの Windows のエディションにより異なりますので注意してください。ここでは、Pro の場合について説明します。他のエディションでの方法は各自で調べてください。

1. 「イーサネットのプロパティ」を開く

- ① 1.「スタートメニュー」を押す。
- ② 2.「設定」を押す。



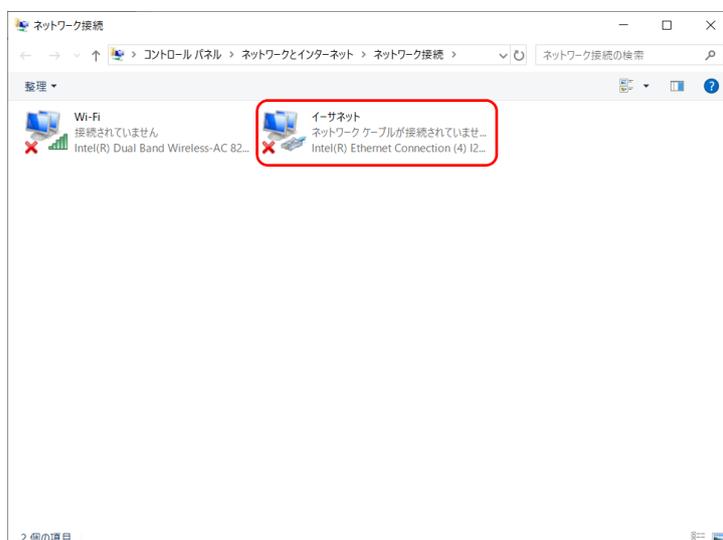
2. 「ネットワークとインターネット」を押す。



3. 「アダプターのオプションを変更する」を押す。

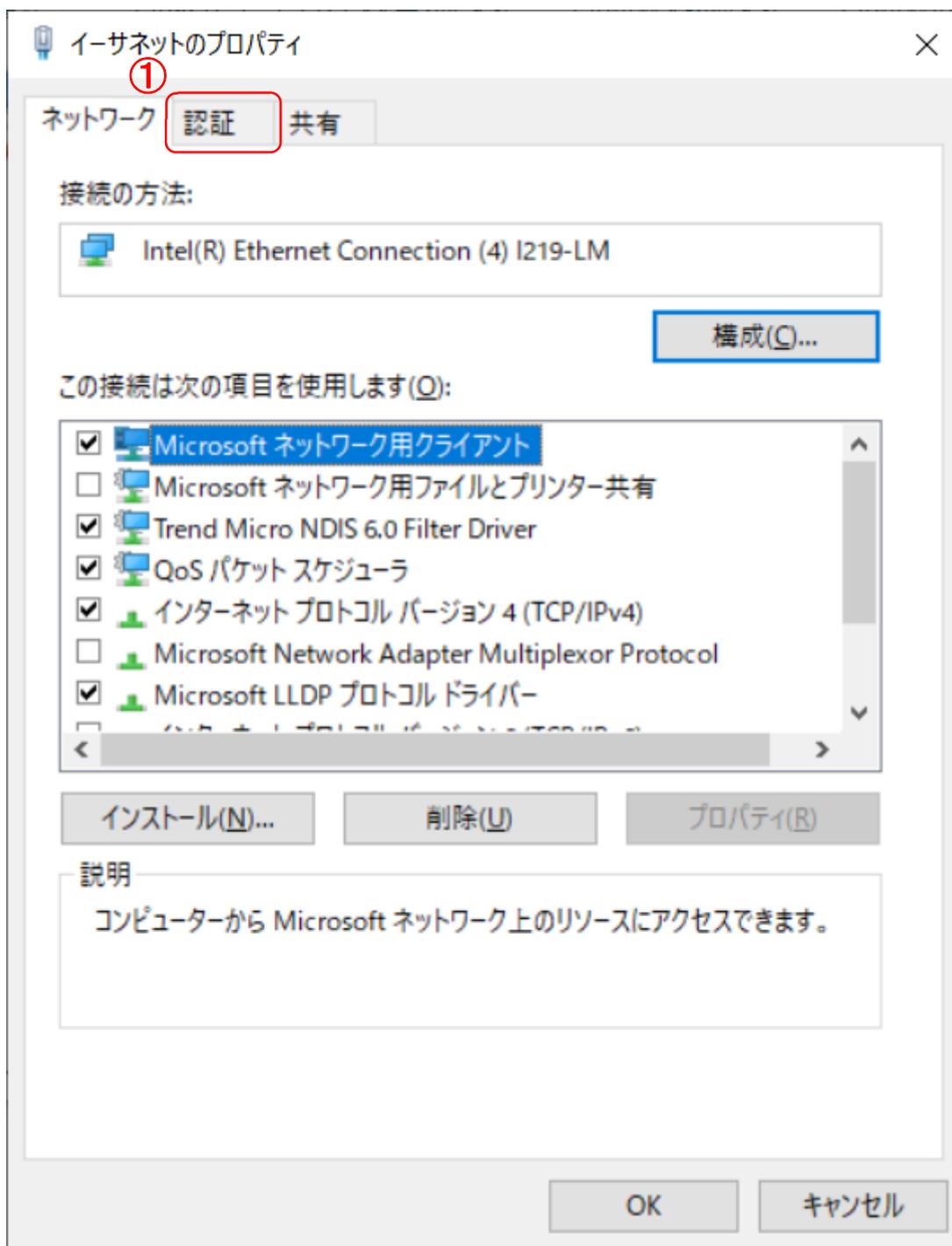


4. 利用するネットワークアダプターの設定を押す。(ここでは「イーサネット」)

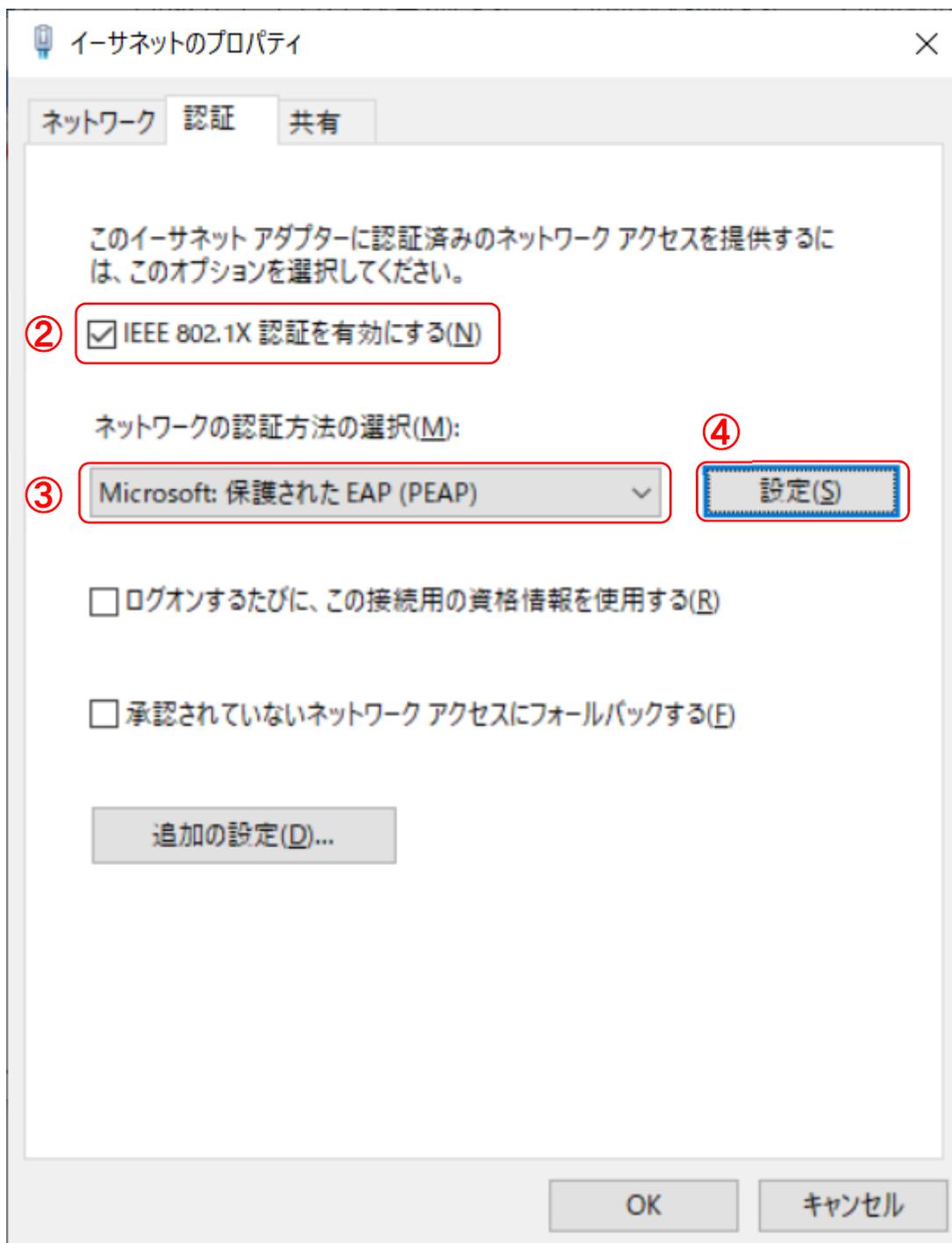


2 認証するように設定を変更する。

1. 「認証」タブを開く。



2. 「IEEE802.1X 認証を有効にする」をチェックする。
3. 「ネットワークの認証方法の選択」で「Microsoft: 保護された EAP(PEAP)」を選択する。
4. 「設定」をクリックする。(次のページの画面が表示される)



5. 「証明書を検証してサーバーの ID を検証する」のチェックを外す。
6. 「認証方法を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択する。
7. 「構成」をクリックする。(次のページの画面が表示される)

保護された EAP のプロパティ

接続のための認証方法:

⑤ 証明書を検証してサーバーの ID を検証する(V)

次のサーバーに接続する (例: srv1、srv2、.*¥.srv3¥.com)(Q):

信頼されたルート証明機関(R):

- AddTrust External CA Root
- AffirmTrust Commercial
- Baltimore CyberTrust Root
- Certum CA
- Certum Trusted Network CA
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- GlobalTrust Global Root

接続前の通知(I):

サーバーの ID を確認できない場合にユーザーに通知する

認証方法を選択する(S): ⑥

セキュリティで保護されたパスワード (EAP-MSCHAP v2) ⑦

構成(C)...

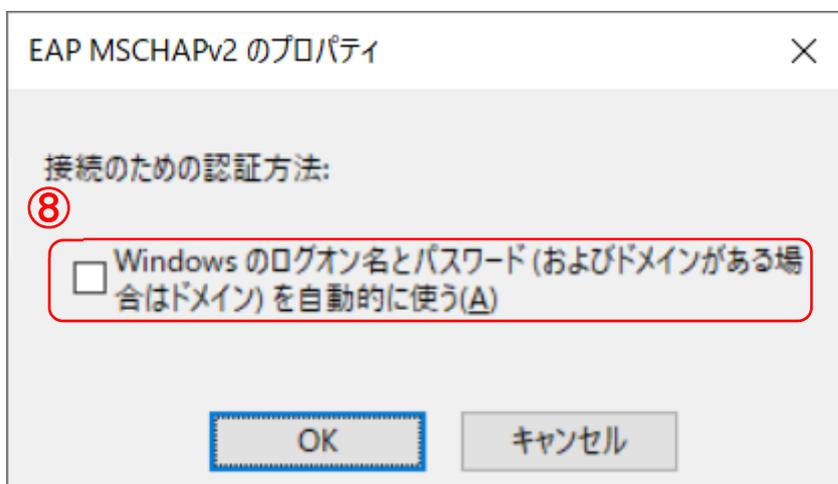
高速再接続を有効にする(E)

サーバーに暗号化バイン드의 TLV がない場合は切断する(D)

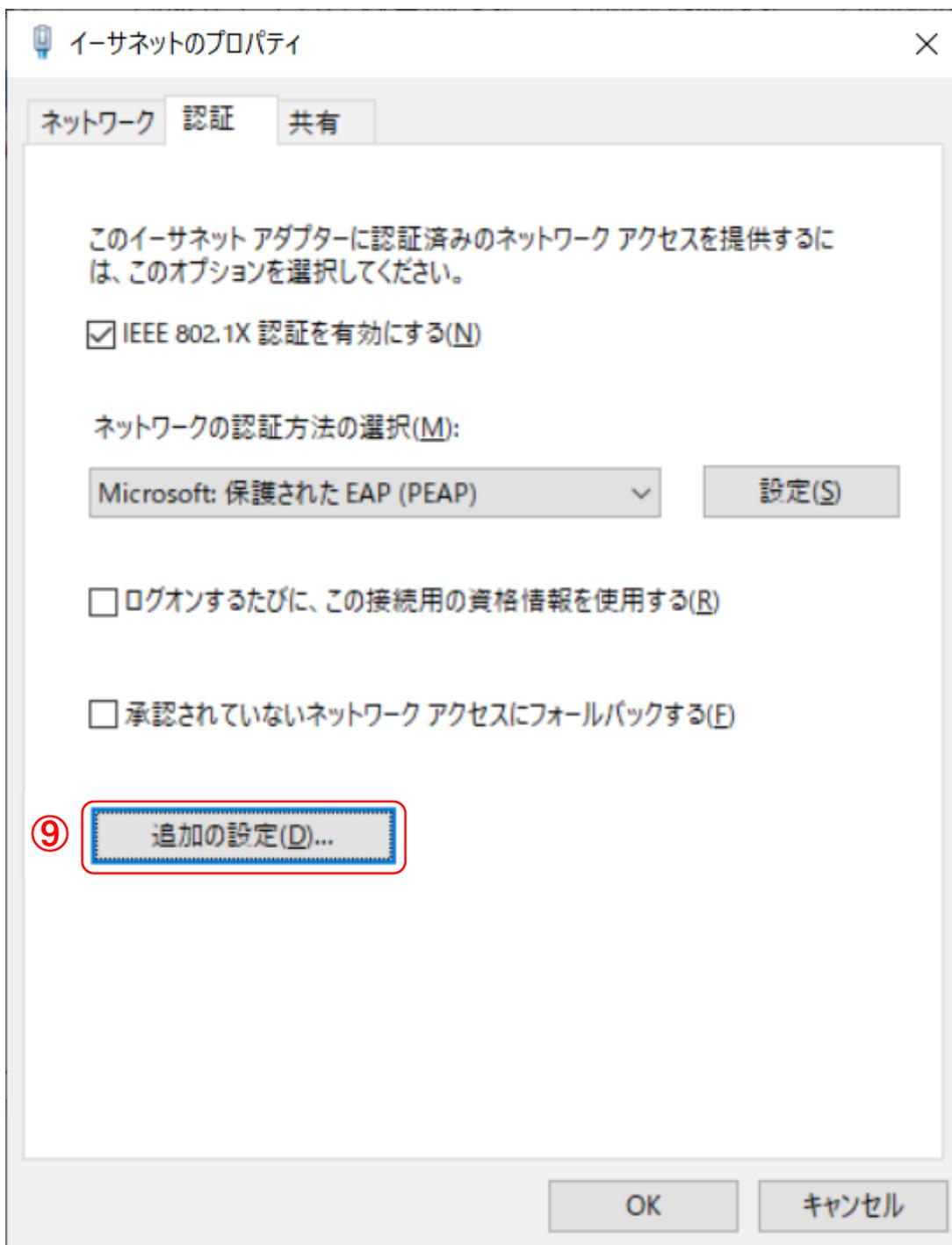
ID プライバシーを有効にする(I)

OK キャンセル

8. 「接続のための認証方法:」の「Windows のログオン名とパスワード(およびドメイン名がある場合はドメイン)を自動的に使う」のチェックを外す。その後 OK のボタンを押す。前の画面に戻りますが、そこでも OK のボタンを押す。



9. 「追加の設定」を押す。(次の画面が表示されます)



10. 「認証モードを指定する」をチェックし、ユーザー認証を選択する。その後 OK を押す。(次のページの画面に戻ります)

詳細設定

802.1X の設定

認証モードを指定する(P)

ユーザー認証

資格情報の保存(S)

すべてのユーザーの資格情報を削除する(L)

このネットワークに対するシングルサインオンを有効にする(S)

ユーザー ログオンの直前に実行する(E)

ユーザー ログオンの直後に実行する(E)

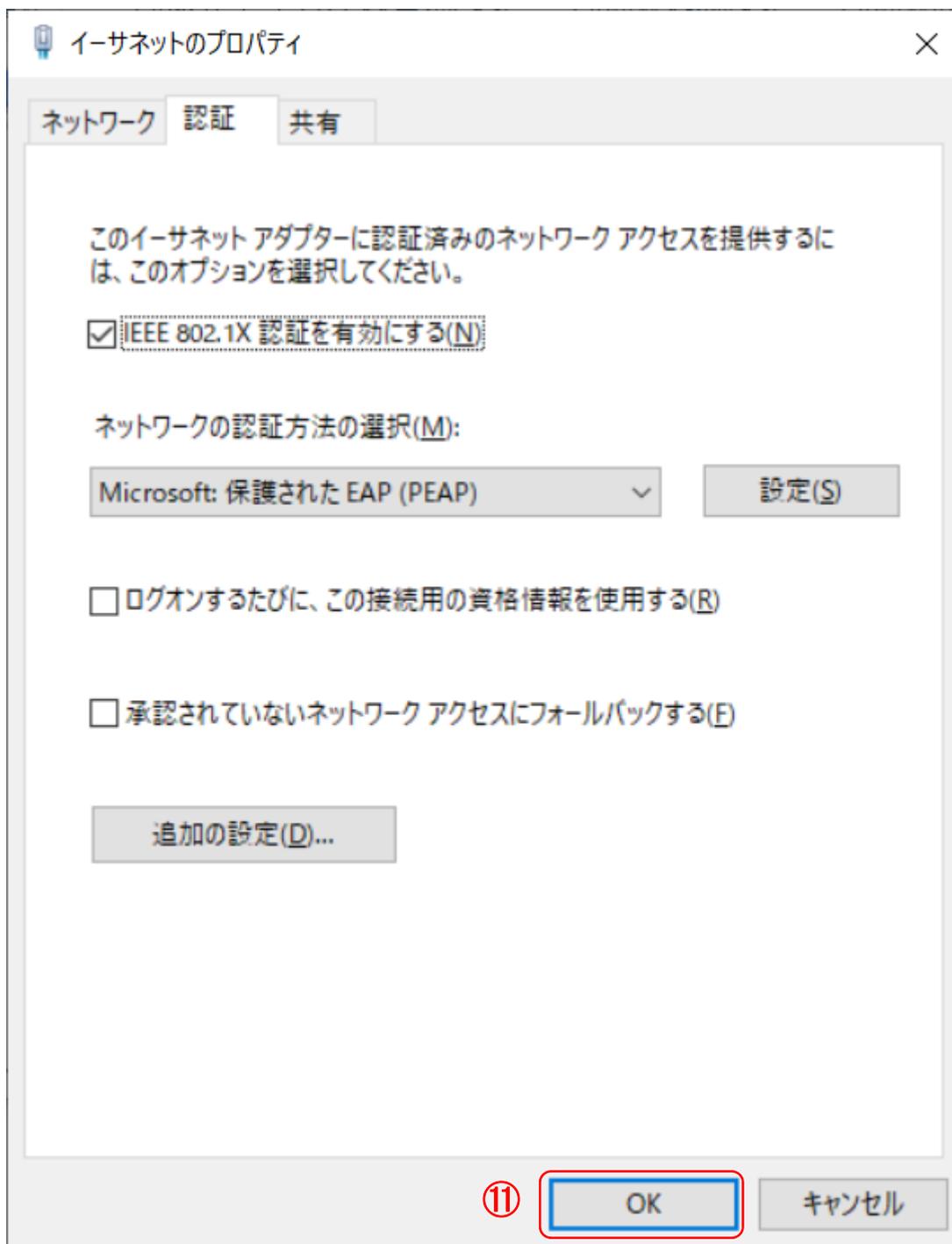
最大待ち時間 (秒)(M): 10

シングルサインオン中に追加のダイアログの表示を許可する(D)

このネットワークでは、コンピューターとユーザーの認証に別の仮想LANを使用する(V)

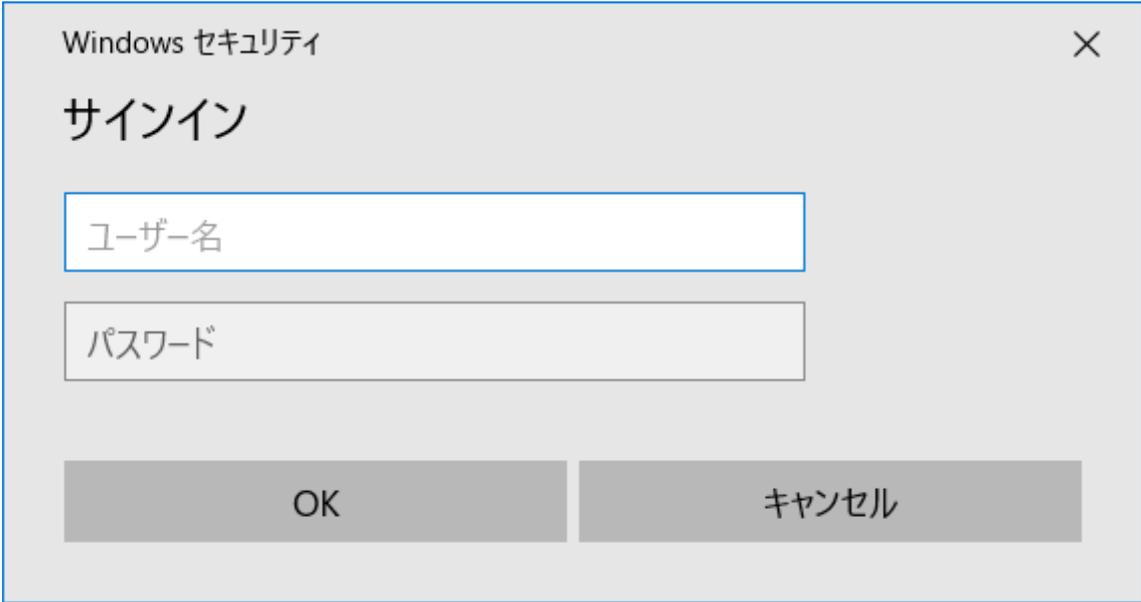
OK キャンセル

11. 「OK」をクリックする。(これで、ネットワークアダプタの設定は終了)



ケーブルを接続して認証を行う。

LAN ケーブルを PC に挿すと、以下の画面が表示され、ユーザー名とパスワードの入力を求められる。ユーザ名の部分に UTID-13を、パスワードのところに、統一認証パスワードを入力し、OK を押す。



The image shows a Windows Security dialog box titled "Windows セキュリティ" (Windows Security) with a close button (X) in the top right corner. Below the title is the heading "サインイン" (Sign in). There are two input fields: the first is labeled "ユーザー名" (User name) and the second is labeled "パスワード" (Password). At the bottom, there are two buttons: "OK" and "キャンセル" (Cancel).