

# Windows10 における無線 LAN 接続設定例

(WLAN AutoConfig 使用 EAP-PEAP WPA2 版)

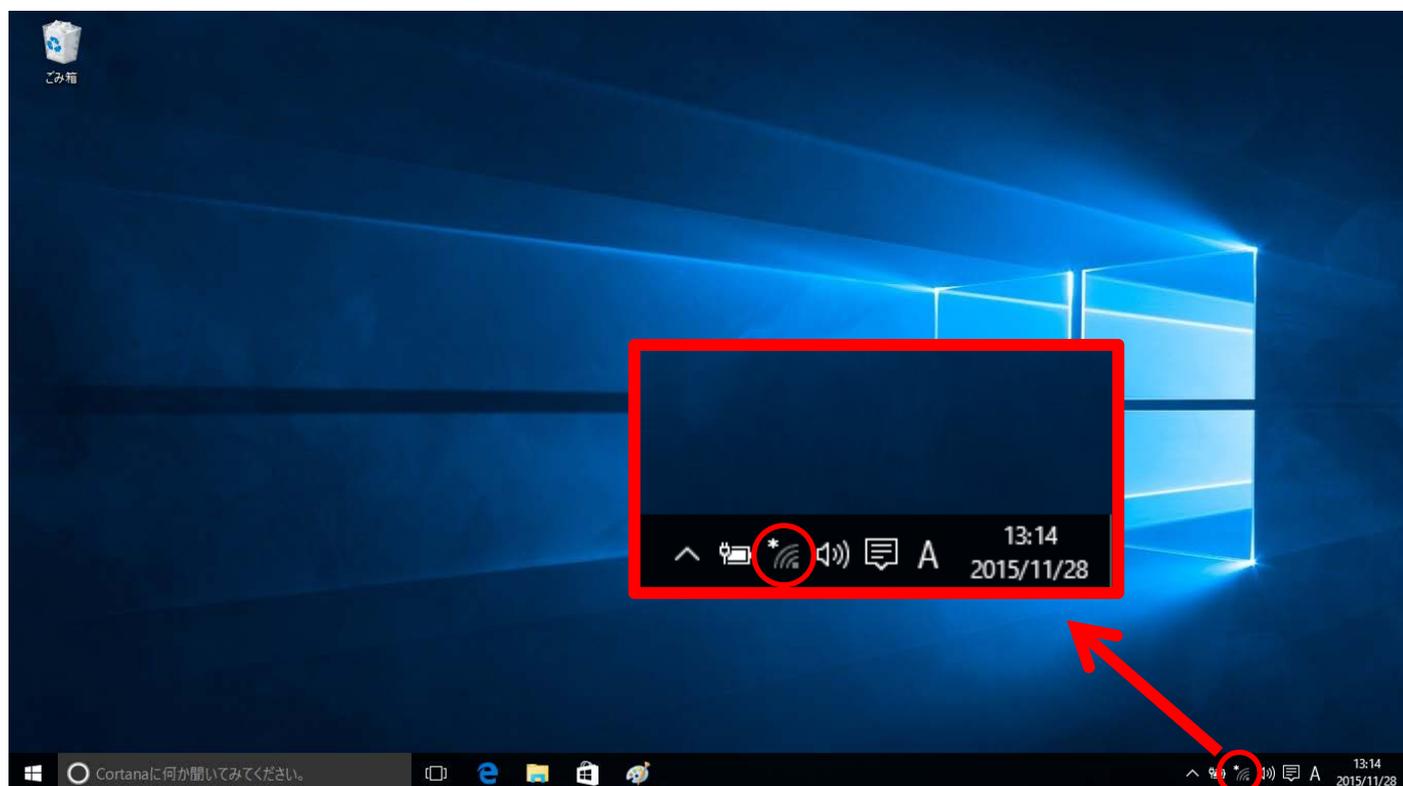
2016/01/26

## 1 はじめに

- 無線 LAN 環境を利用するには以下 2 点が必要です。
  - ・MNS アカウント(不明な場合は、MNS カウンタまでお問合せください)
  - ・無線 LAN カード(ノート PC やタブレット等に内蔵されていない場合、必要となります)
    - ※MNS カウンタでは「無線 LAN カード」の貸出は行っておりません
- 本ドキュメントで記載している設定例の環境
  - ・OS: Microsoft Windows 10 Pro build1511 以降
  - ・無線 LAN カード : PC 内蔵無線 LAN アダプター
- 本ドキュメントを読み進むための前提条件
  - ・無線 LAN カード(または内蔵無線 LAN アダプター)のデバイスドライバーが正しくインストールされ、無線 LAN カードが OS 上で正常動作していること。
  - ・使用可能なネットワーク名は mns80211genv02、ku24、ku52 です。  
ku24 または ku52 をご利用の際には、手順書内の「mns80211genv02」を適宜読み替えて設定を行ってください。

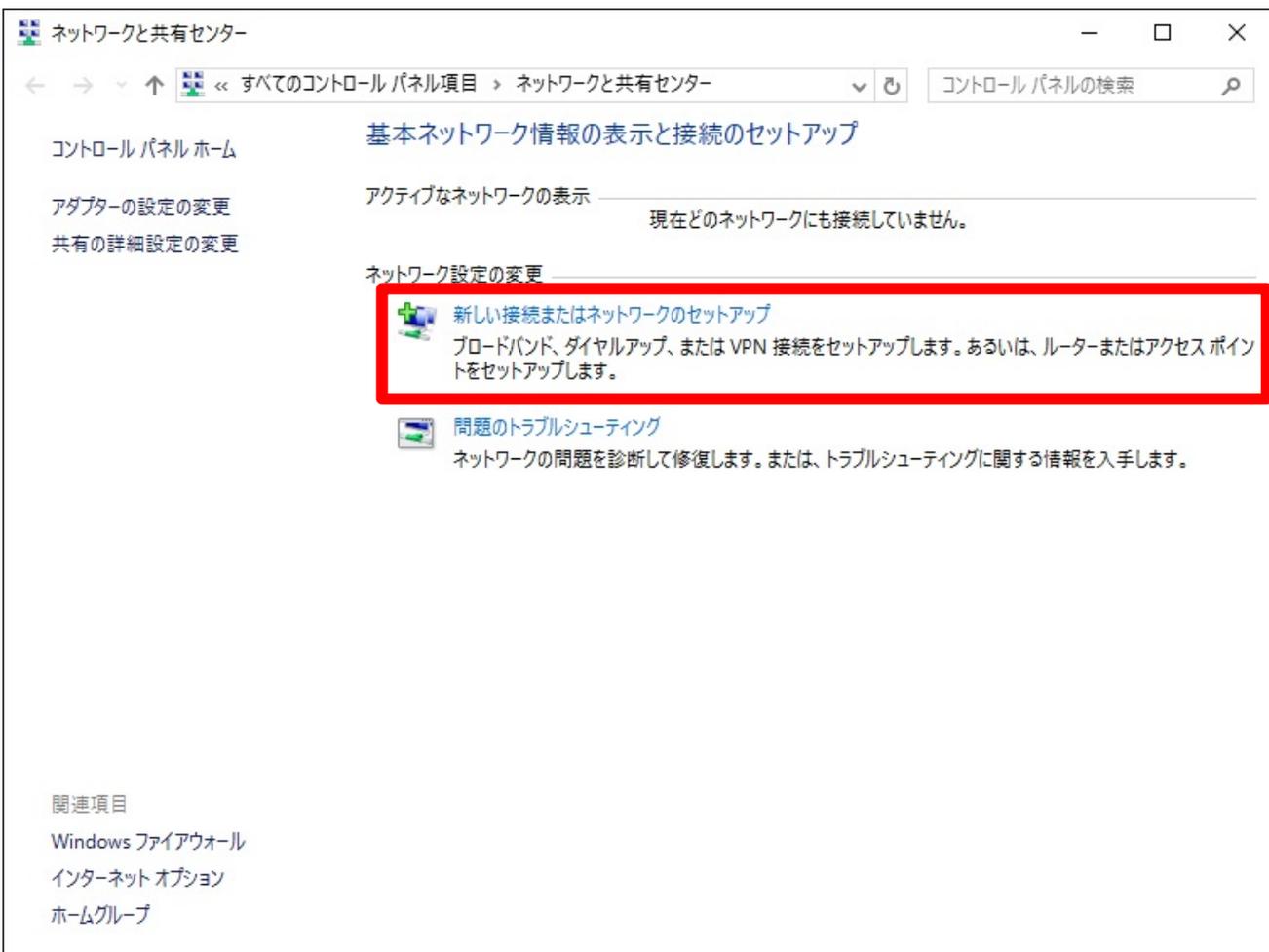
## 2 無線 LAN の設定

- ① スタート画面右下、タスクバーの通知領域にある「ワイヤレスネットワーク」のアイコン(  )をクリックします。





② 「ネットワークと共有センター」画面から「新しい接続またはネットワークのセットアップ」をクリックします。



- ③ 「ワイヤレスネットワークに手動で接続します」を選択し、[次へ(N)]をクリックします。



(次ページに続きます)

- ④ 下記画面が表示されたら各項目を以下のように設定し、[次へ(N)]をクリックします。
- ネットワーク名(E) : mns80211genv02(ku24/ku52)
  - セキュリティの種類(S) : WPA2 エンタープライズ
  - 暗号化の種類(R) : AES
  - 「 この接続を自動的に開始します(I)」のチェックを外す

← ワイヤレス ネットワークに手動で接続します

追加するワイヤレス ネットワークの情報を入力します

ネットワーク名(E): mns80211genv02

セキュリティの種類(S): WPA2-エンタープライズ

暗号化の種類(R): AES

セキュリティキー(Q):   文字を非表示にする(H)

この接続を自動的に開始します(I)

ネットワークがブロードキャストを行っていない場合でも接続する(O)

警告: 選択すると、このコンピューターのプライバシーが危険にさらされる可能性があります。

次へ(N) キャンセル

- ⑤ 「接続の設定を変更します(H)」をクリックします。

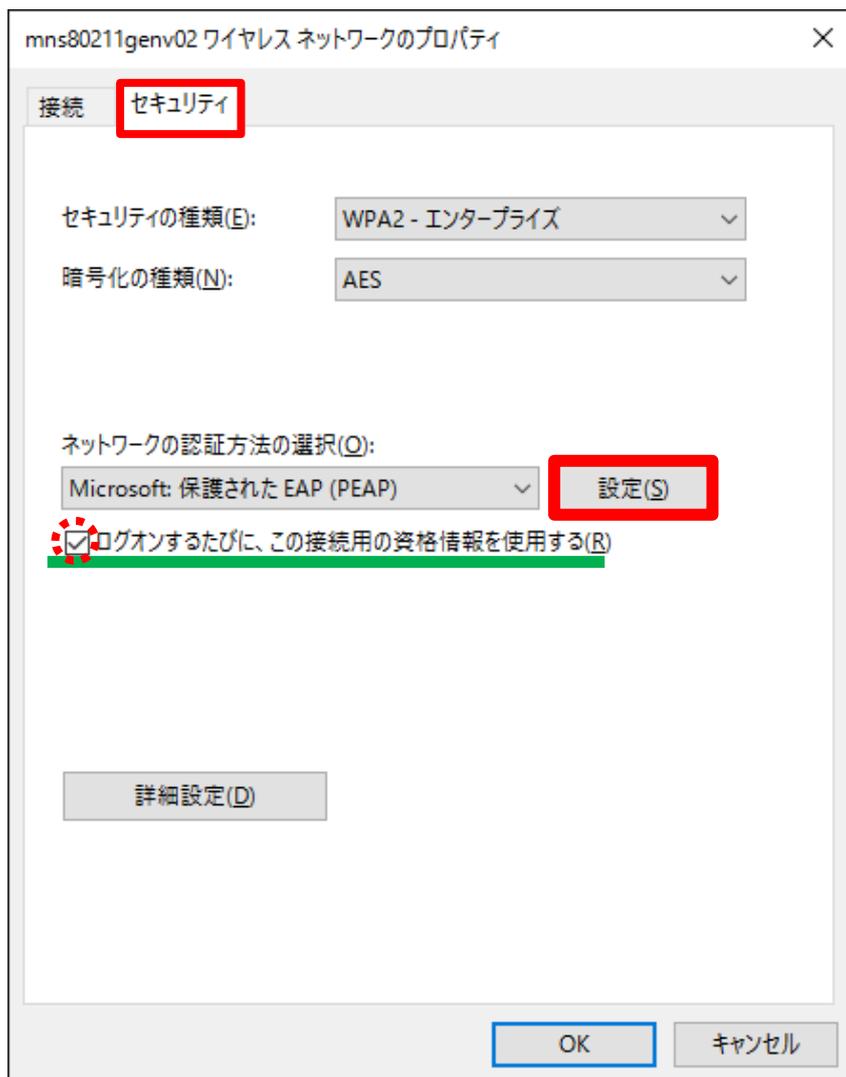
← ワイヤレス ネットワークに手動で接続します

正常に mns80211genv02 を追加しました

→ 接続の設定を変更します(H)  
接続のプロパティを開き、設定を変更します。

閉じる

- ⑥ 「mns80211genv02 ワイヤレスネットワークのプロパティ」が表示されます。[セキュリティ]タブを選択後、[設定(S)]ボタンをクリックします。



※「ログオンするたびに、この接続用の資格情報を使用する(R)」のチェックについて

- チェックあり：初回接続時のみ「MNS アカウント」の ID,パスワードの入力が必要(2 回目以降は入力不要)
- チェックなし：接続のたびに「MNS アカウント」の ID,パスワードの入力が必要（一台の PC を複数人で利用する場合はチェックを外し、利用者ごとに入力を行います）

- ⑦ 「保護された EAP のプロパティ」が表示されます。「 証明書を検証してサーバーの ID を検証する(V)」にチェックを付け、「信頼されたルート証明機関(R)」内の「 Baltimore CyberTrust Root」にチェックを付けます。ルート証明機関を選択後、「認証方法を選択する(S)」の[構成(C)]ボタンをクリックします。

保護された EAP のプロパティ

接続のための認証方法:

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)(O):

信頼されたルート証明機関(R):

- AddTrust External CA Root
- Baltimore CyberTrust Root
- Class 3 Public Primary Certification Authority
- DigiCert Global Root CA
- DigiCert High Assurance EV Root CA
- Equifax Secure Certificate Authority
- GlobalSign Root CA
- GTE CyberTrust Global Root

接続前の通知(I):

サーバーの ID を検証できない場合にユーザーに通知します

認証方法を選択する(S):

セキュリティで保護されたパスワード (EAP-MSCHAP v2)

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)

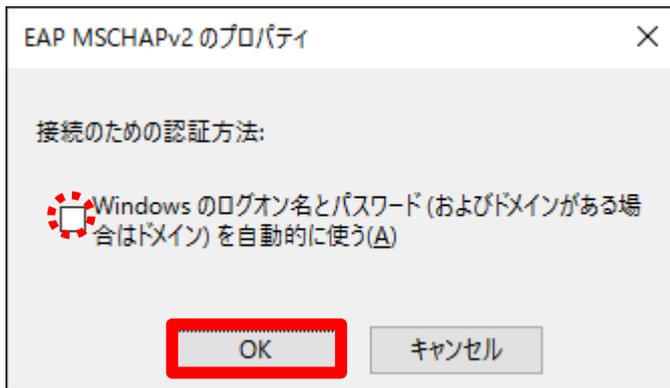
ID プライバシーを有効にする(I)

OK キャンセル

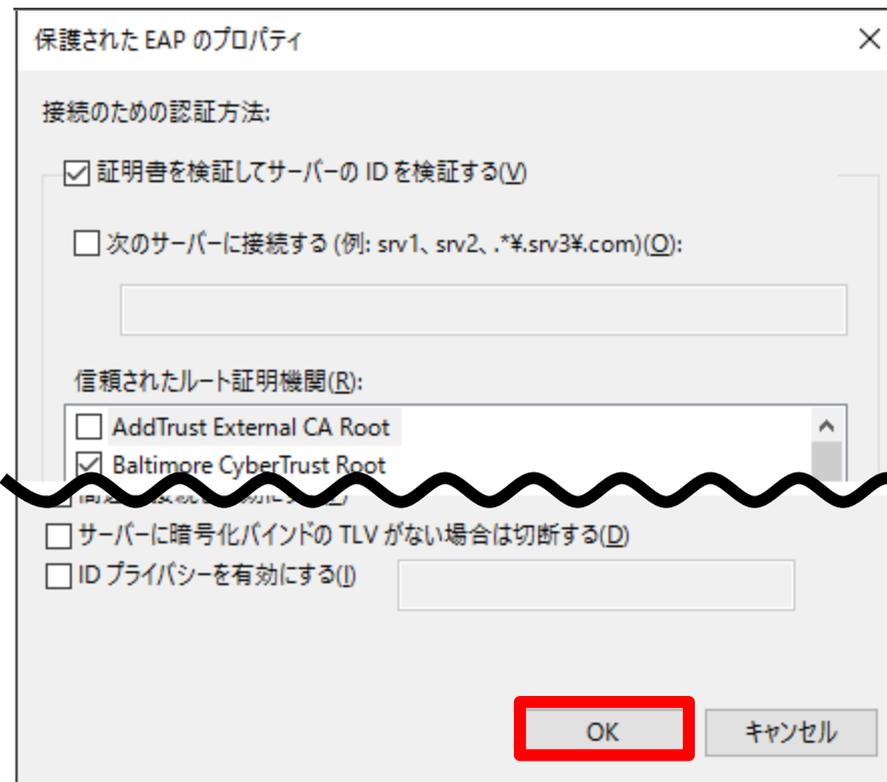
### 【重要】

この設定は不正なサーバーに接続しないためのものです。このチェックを外してしまうと、悪意のあるサーバーに自動的に接続する可能性があり、最悪の場合IDとパスワードが盗まれる危険性があります。重要なセキュリティ設定ですので、必ず外さないようにしてください。

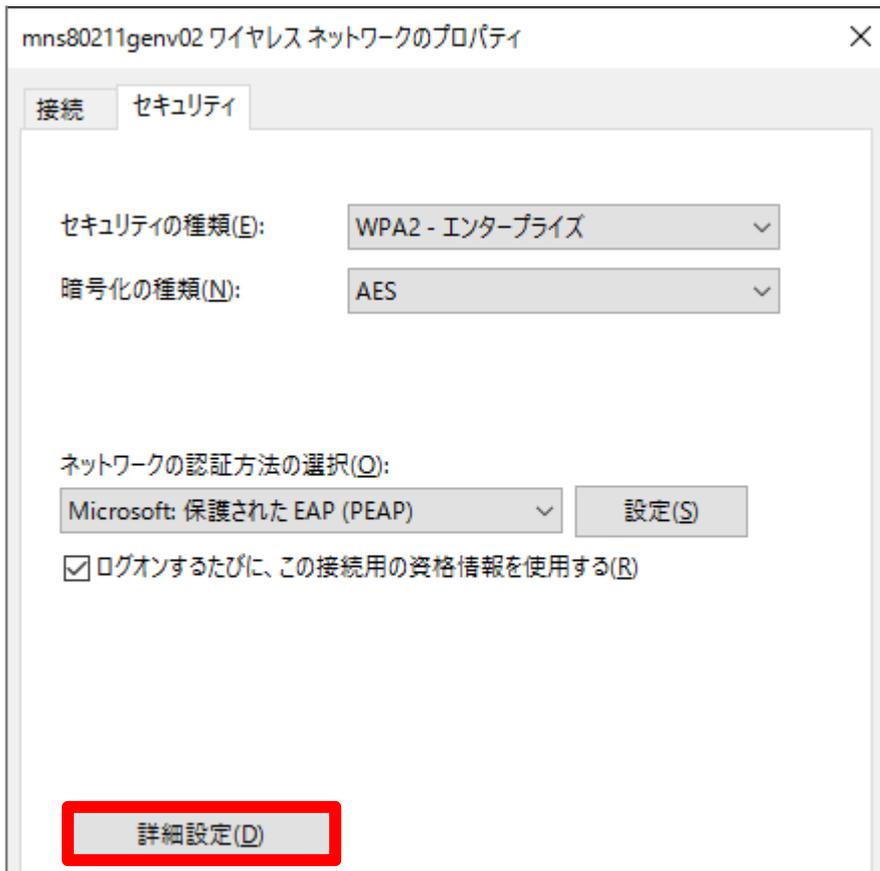
- ⑧ 「EAP MSCHAPv2 のプロパティ」が表示されます。「Windows のログオン名とパスワード(およびドメインがある場合はドメイン)を自動的に使う(A)」のチェックを外し、[OK]をクリックします。



- ⑨ 「保護された EAP のプロパティ」を[OK]で閉じます。



- ⑩ 「mns80211genv02 ワイヤレスネットワークのプロパティ」に戻りましたら、[詳細設定(D)]ボタンをクリックします。



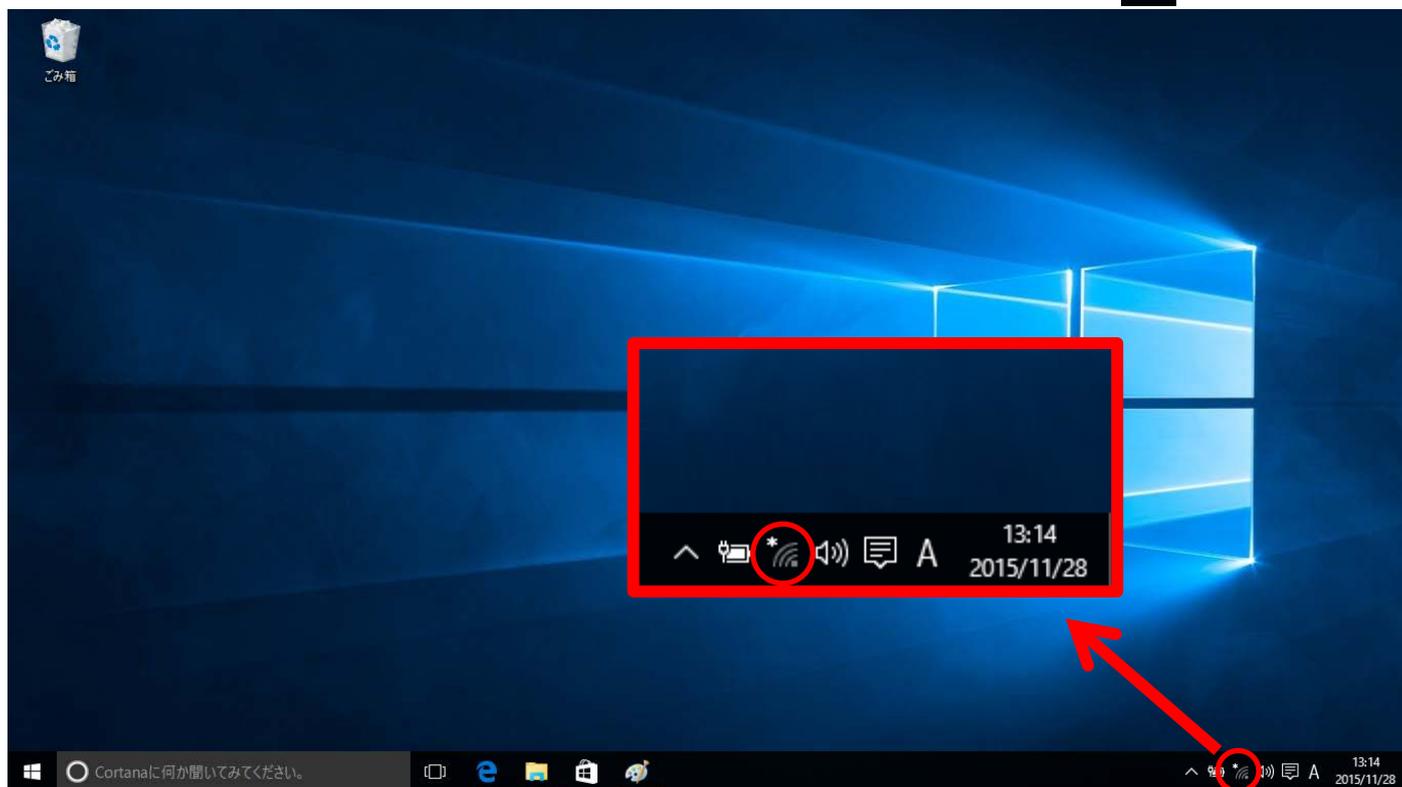
- ⑪ [802.1x の設定]タブを選択し、「 認証モードを指定する(P)」にチェックを付け、プルダウンリストより「ユーザー認証」を選択します。



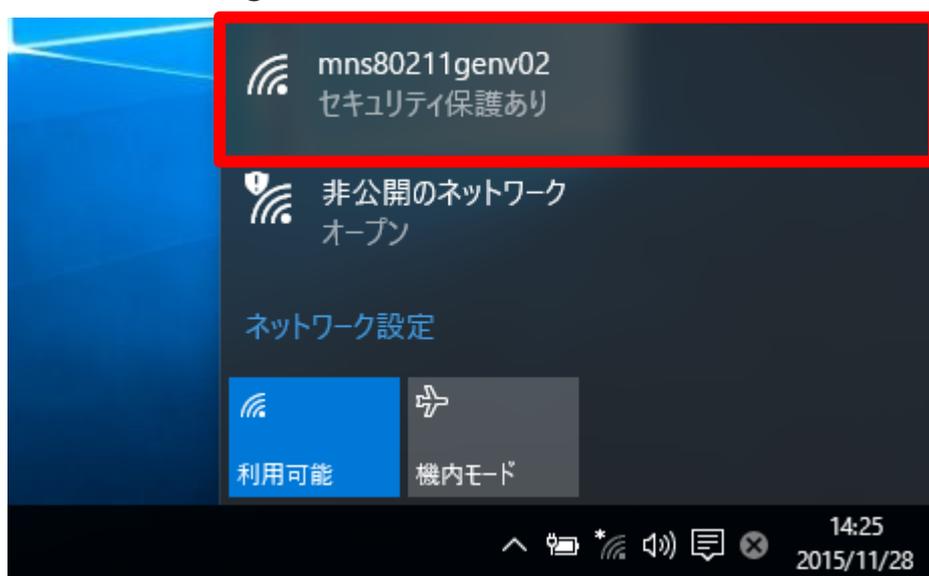
- ⑫ 最後に、「詳細設定」と「mns80211genv02 ワイヤレスネットワークのプロパティ」を[OK]で閉じれば設定完了です。

### 3 アクセスポイントへの接続

- ① スタート画面右下、タスクバーの通知領域にある「ワイヤレスネットワーク」のアイコン(  )をクリックします。

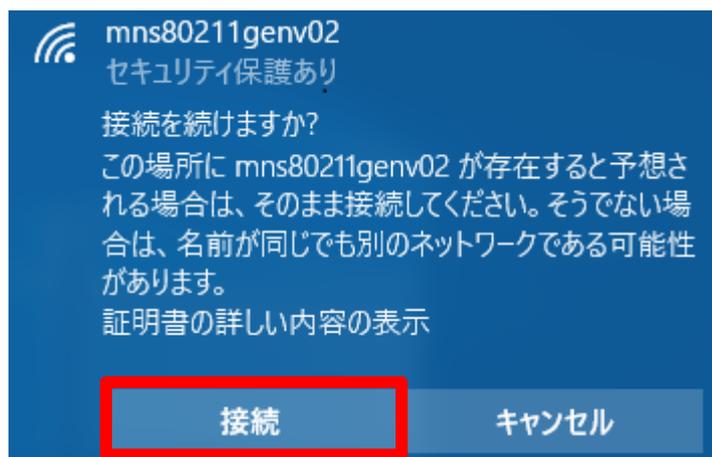


- ② 「mns80211genv02 セキュリティ保護あり」を選択します。





- ⑤ 「接続を続けますか？」というメッセージが表示された場合は、そのまま[接続]ボタンをクリックします。



- ⑥ 利用可能なワイヤレスネットワークの一覧に「mns80211genv02」が表示され、「接続済み、セキュリティ保護あり」と記載があれば接続完了です。

