
AI人物検索サービス クラウド監視カメラパッケージ

リモート接続設定手順書

Windows 8 版

Ver1.0

NTT コミュニケーションズ株式会社

目次

1. はじめに	2
2. 実施前ご確認事項.....	2
3. VPN 接続設定手順について (IPsec 接続設定手順)	3
4. リモート接続設定方法.....	4

*Microsoft、Windows 8 は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。

*本手順書に掲載しているスクリーンショットは、マイクロソフトの許可を得て使用しています。

1. はじめに

- 本資料はNTTコミュニケーションズ(以下NTTコム)が提供する AI人物検索サービス(クラウド監視カメラパッケージ)リモート接続のご利用に関する手順書です。
- 今後、本手順書は予告なく変更される可能性があります。
- Microsoft Windows 8標準のソフトウェアを利用した接続手順です。
- 本手順書を利用したことにより、深刻な問題が発生することがあります。最悪の場合には再インストールが必要です。本手順書を使用したことにより発生した問題に関しては、一切責任を負わないものとします。本手順書は、自己の責任においてご使用ください。

2. 実施前ご確認事項

※作業開始前に必ずお読みください※

- 作業実施はご利用PCの**管理者権限**で行うようにしてください。
- 作業実施前にすべてのプログラムを終了させてください。終了させない場合、作業中のデータが失われる場合があります。
- 本手順書は、ご利用PCからインターネットに接続できる環境を前提にしております。
- 本手順書は断わりがない場合、Microsoft Windows 8を使用して作成しております。
ご利用PCのOS／画面カスタマイズ内容によっては手順書内の画像が一部異なる場合がございます。
- ユーザー アカウント制御 (UAC)画面が表示された場合には、「許可」または「続行」、「はい」ボタンをクリックしてください。
- 設定の際には【AI人物検索サービス(クラウド監視カメラパッケージ)開通案内】をお手元にご用意ください。
- ボタンのクリックや入力操作が複数回の場合、操作順序として「①」「②」・・・と画面イメージに記入していますので、記入された数字の順序に沿って、操作してください。
- マウスとキーボードでの操作を前提としております。また、特に指定がない場合、「クリックする」は、マウスの左ボタンのクリックを指します。

Microsoftの制限により、Windows 8については、次手順を実施する必要がある場合があります。

次は参考手順となりますので詳細はMicrosoftに確認ください。

NTTコムでは次に関する一切の責任を持ちません。

※下記手順は(<http://support.microsoft.com/kb/926179/ja>)より抜粋しております。

(文書番号: 926179 - 最終更新日: 2013年9月3日 - リビジョン: 5.0)

- 1.[スタート] ボタンをクリックし、[ファイル名を指定して実行] をクリックします。[名前] ボックスに regedit と入力し、[OK] をクリックします。
- 2.次のレジストリ サブキーを見つけてクリックします。
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥PolicyAgent
3. [編集] メニューで、新規作成をポイントし、[DWORD (32 ビット) 値] をクリックします。
- 4.[新しい値 #1] ボックスで AssumeUDPEncapsulationContextOnSendRule と入力し、Enter キーを押します。 ※既に登録している場合は登録済のキーを使用してください。
- 5.[AssumeUDPEncapsulationContextOnSendRule] を右クリックし、[変更] をクリックします。
- 6.[値のデータ] ボックスに次のいずれかの値を入力します。
※「2」に設定して接続できることを確認しておりますが、環境により異なる可能性があります。
 - ・0 (デフォルト) : 値 0 (ゼロ) を入力すると、Windows は、ネットワーク アドレス変換器の外側に配置されているサーバーに対してセキュリティ アソシエーションを確立できないように構成されます。これは既定値です。
 - ・1 : 値 1 を入力すると、Windows は、ネットワーク アドレス変換器の外側に配置されているサーバーに対してセキュリティ アソシエーションを確立できるように構成されます。
 - ・2 : 値 2 を入力すると、Windows Vista ベースまたは Windows Server 2008 ベースの VPN クライアントコンピュータとサーバーの両方が、NAT デバイスの背後にあるセキュリティ アソシエーションを確立できるように Windows を構成します。
- 7.[OK] をクリックし、レジストリ エディタを終了します。
- 8.コンピュータを再起動します。

3. VPN 接続設定手順について (IPsec 接続設定手順)

- 参考として、VPN クライアント(Windows 8)の設定手順について簡単に述べます。

ここでは、すでにご利用 PC 側でインターネットアクセスの設定が完了しており、IP を使ってルーターに到達可能な状態にあると仮定しています。

本例では NAT-T を使用するため、ルーターまでの経路上に NAT 機器が存在していてもかまいません。

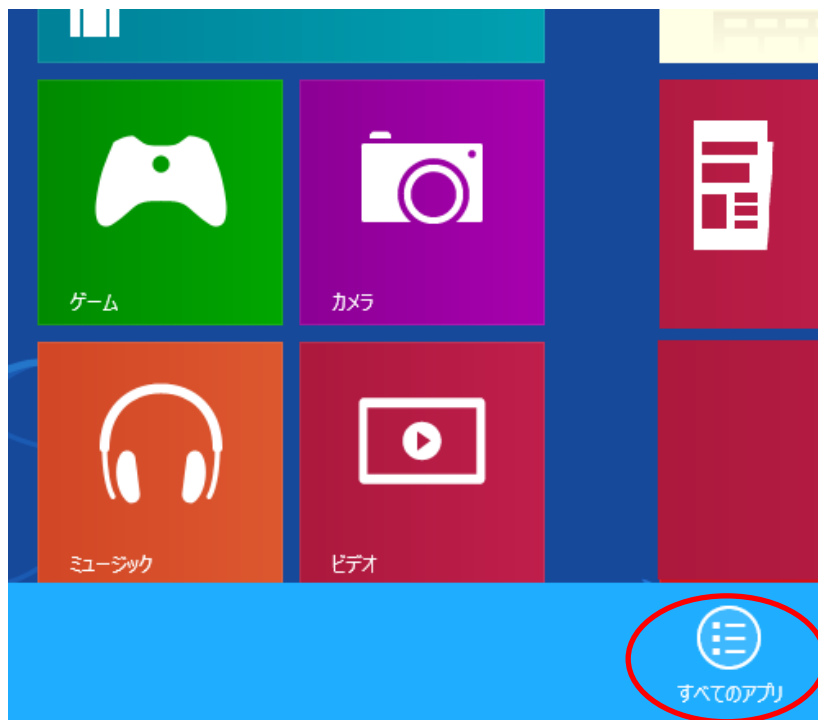
なお、ご利用 PC 側の詳細な設定方法については、Microsoft Windows 8 のマニュアルなどをご覧ください。

Note - 本設定例は、NAT-Traversal を利用したリモートアクセス型 IPsec VPN の一構成例であり、Microsoft Windows 8 との接続性を保証するものではありません。

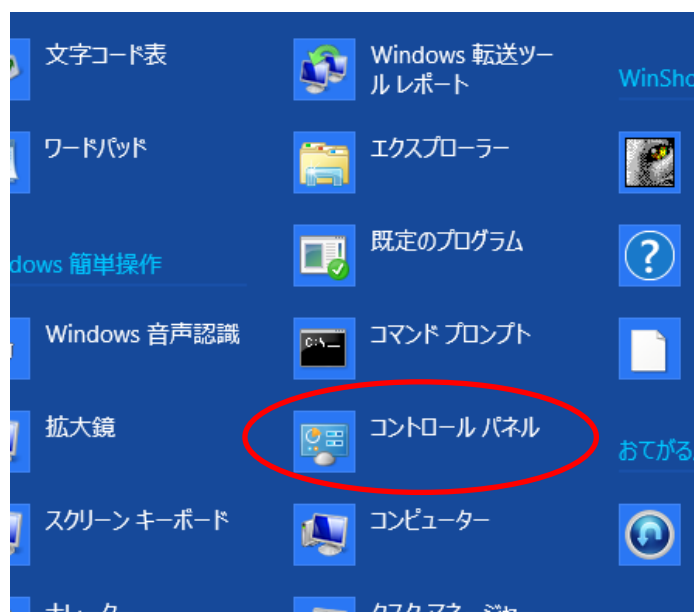
Note - 次に述べる手順は一例です。サービスパックや修正プログラムの適用状況、環境設定の仕方などによっては、次の手順で接続できない可能性もあります。詳しくは、Microsoft Windows 8 のマニュアルなどをご参照ください。

4. リモート接続設定方法

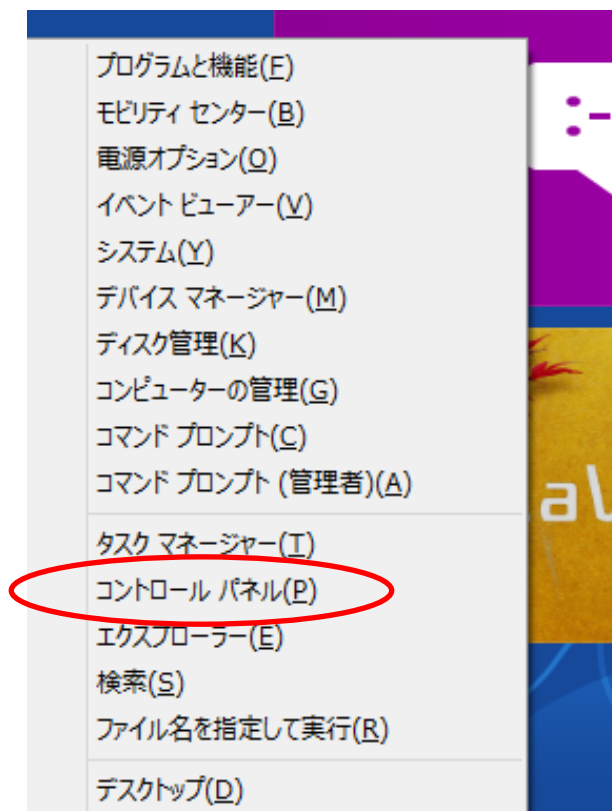
1. 「すべてのアプリ」を選択し、すべてのアプリケーションのメニューを開きます。



2. インストールされているすべてのアプリケーションのアイコンが表示されるので、その中から「コントロールパネル」を選択します。



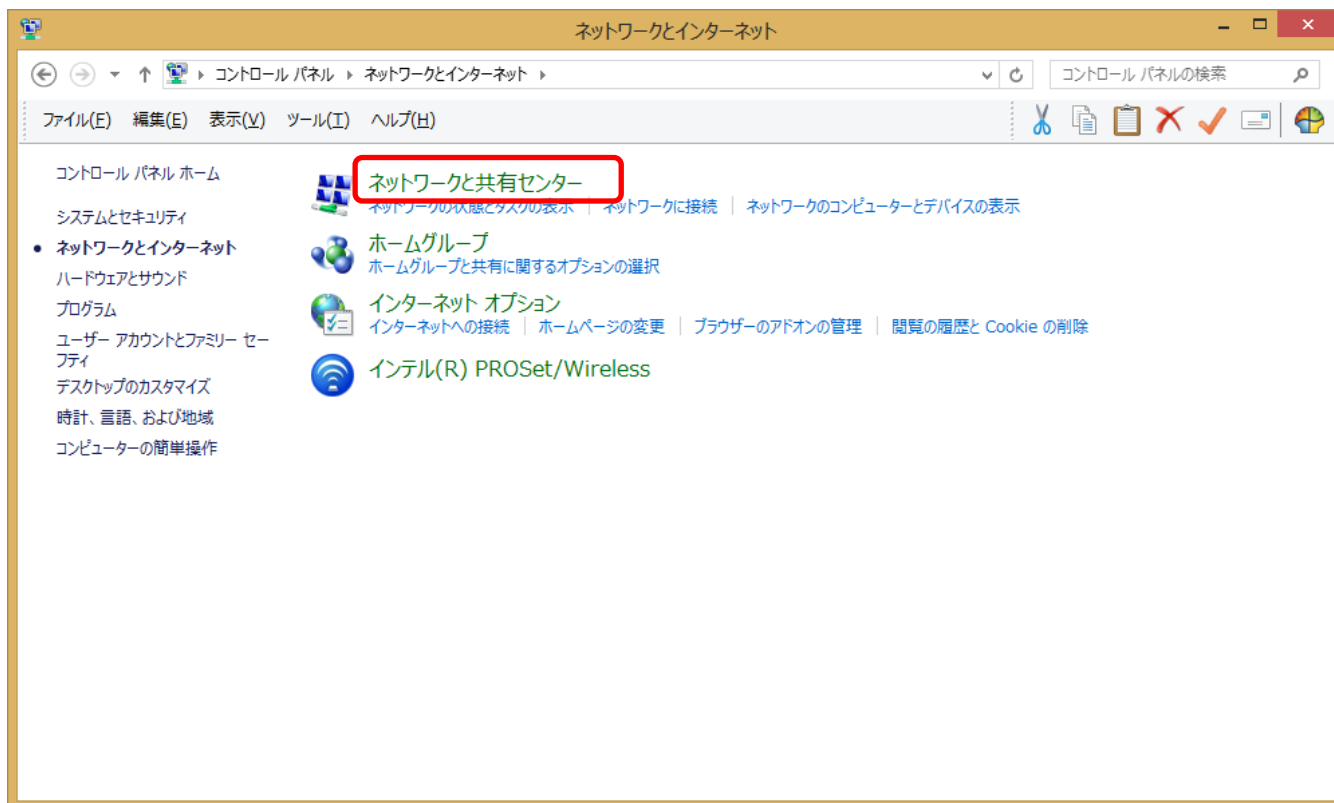
または「Windows キー」 + 「x」で開くメニューから、「コントロールパネル」を選択することもできます。



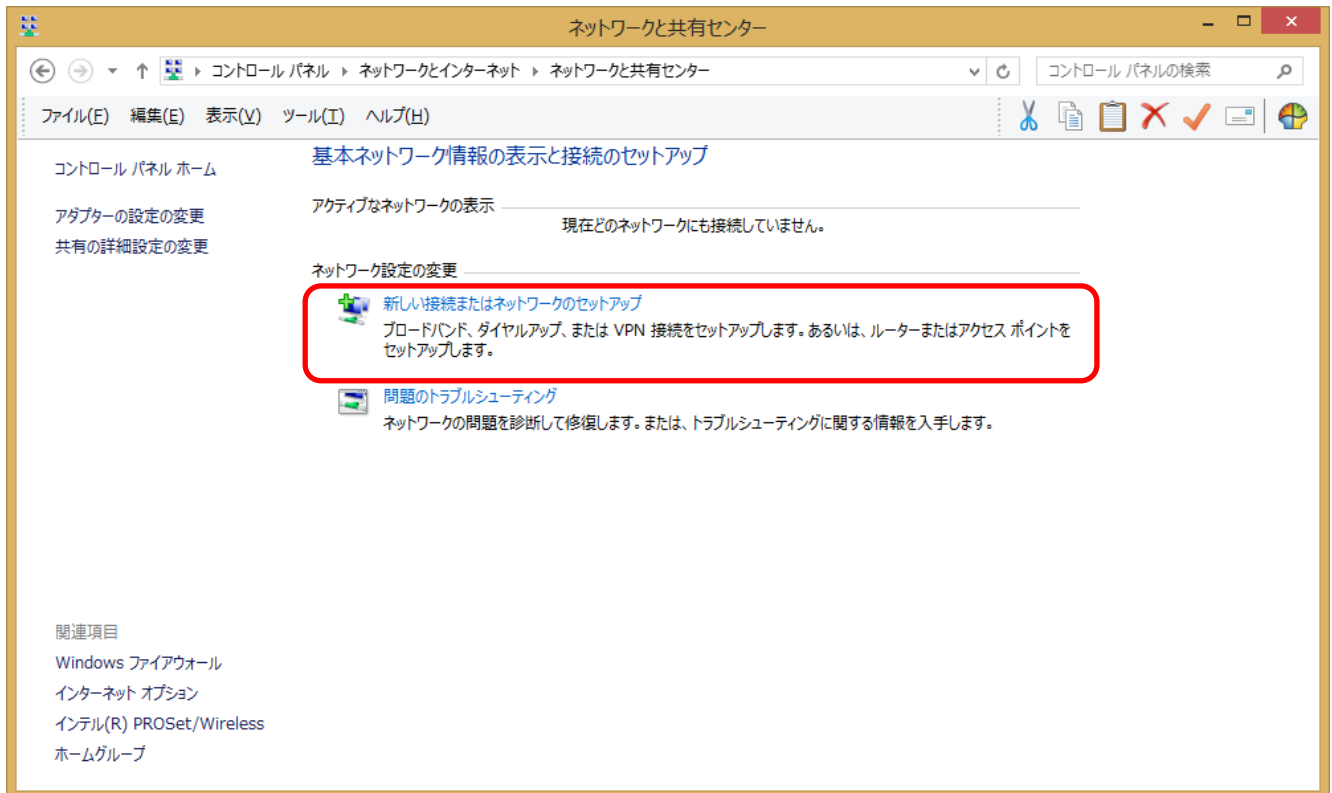
3. 「コントロールパネル」のダイアログが開きますので、「ネットワークとインターネット」をクリックします。



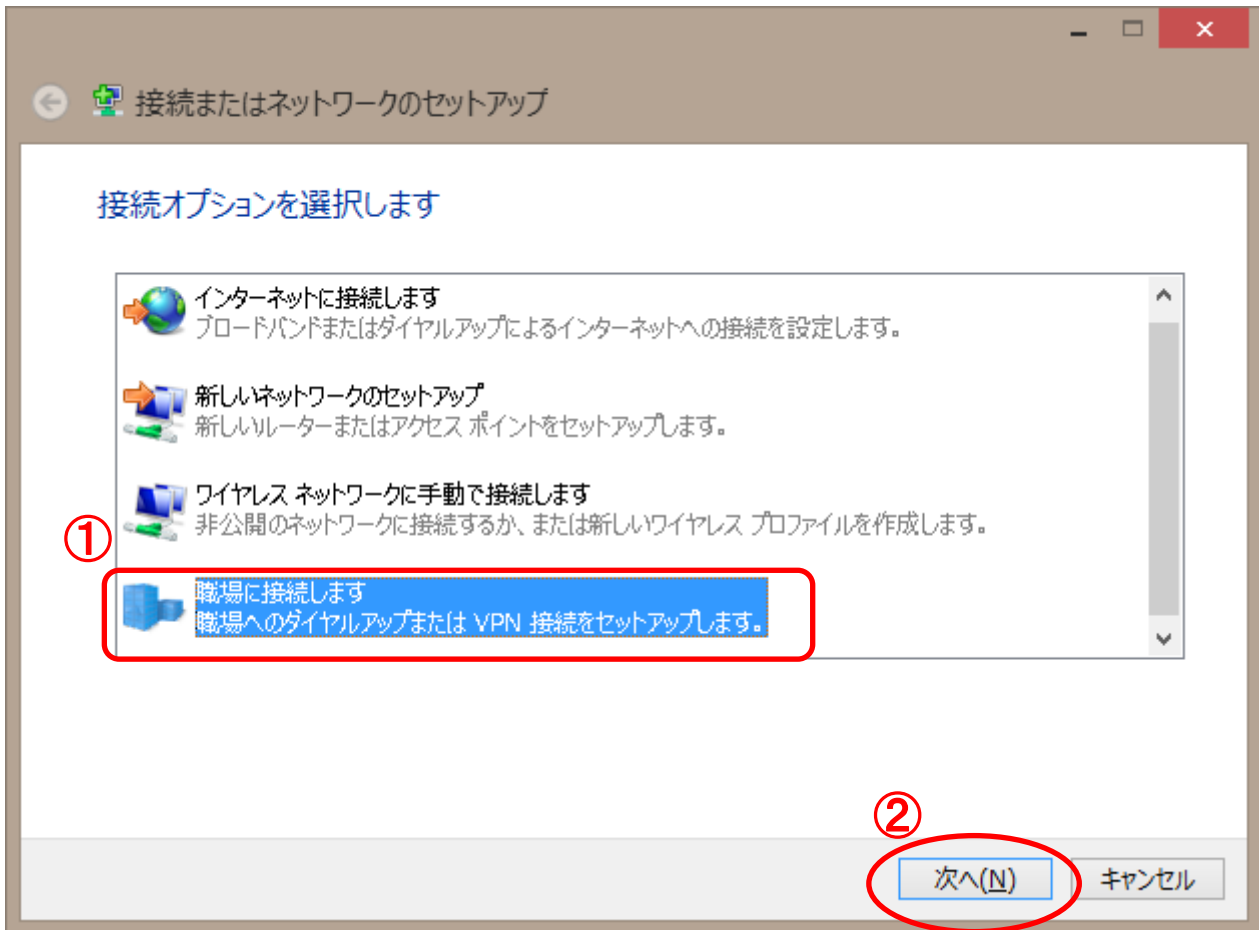
4. 「ネットワークとインターネット」のダイアログが開きますので、「ネットワークと共有センター」をクリックします。



5. 「ネットワークと共有センター」のダイアログが開きますので、「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。



6. 「接続またはネットワークのセットアップ」のダイアログが開きますので、「職場に接続します」を選択し、「次へ(N)」をクリックします。



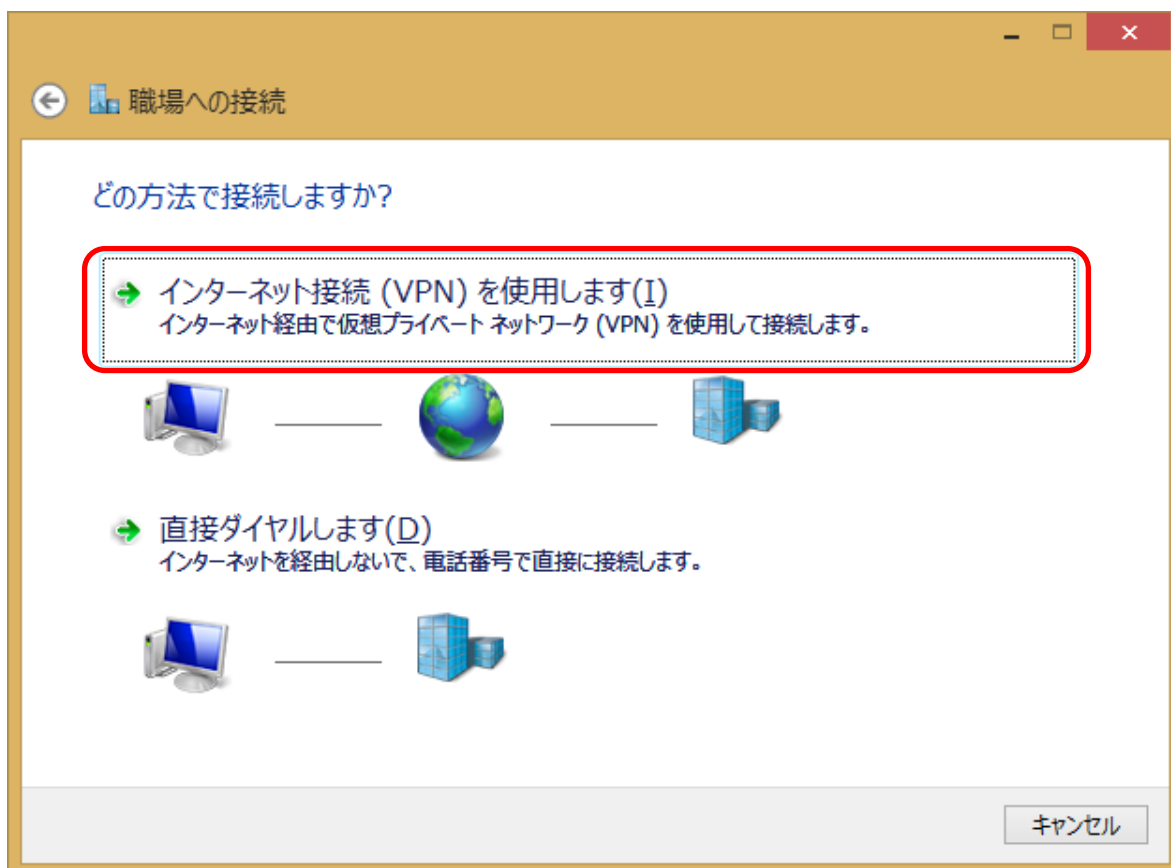
- 7.「職場への接続」のダイアログが開きますので、「いいえ、新しい接続を作成します(C)」を選択して「次へ (N)」をクリックします。



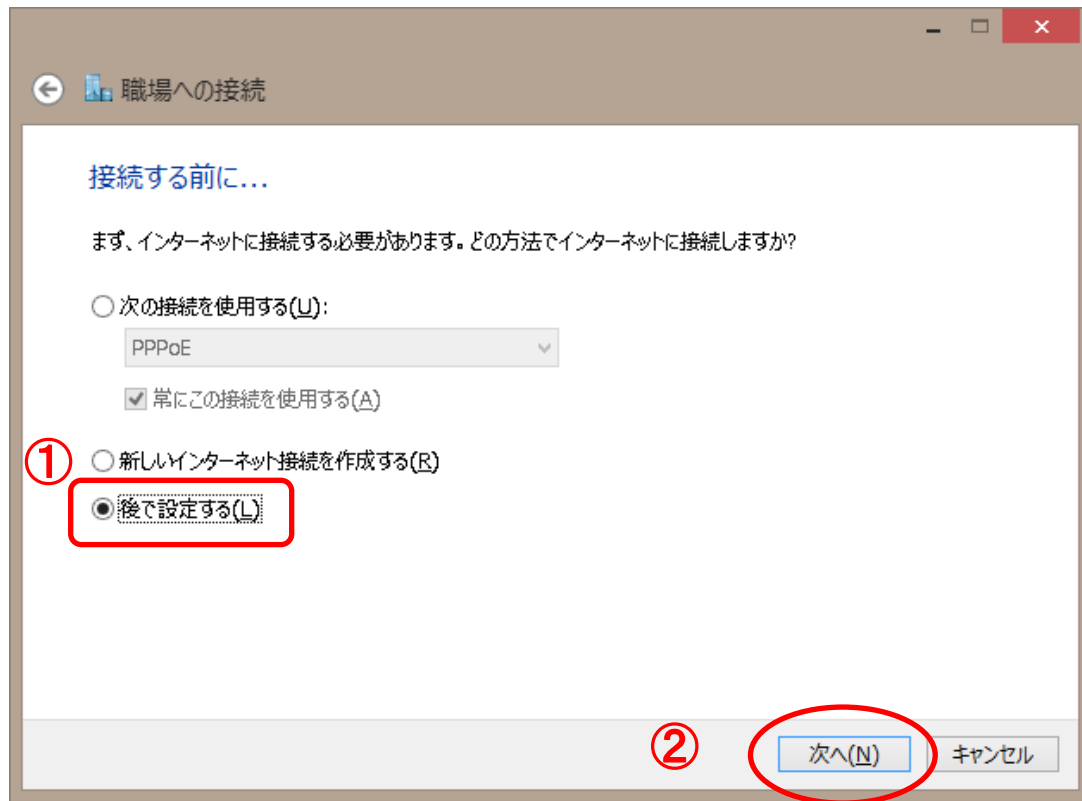
Note – 既存の接続が作成されていない場合などは、この画面が表示されず、次の画面が表示される場合があります。

Note – 開いたときに、既存の接続が選択されていることがあります。

8. 「インターネット接続(VPN)を使用します(I)」を選択します。



9. 「後で設定する (L)」を選択し「次へ (N)」をクリックします。



Note - PC から直接インターネットに接続する場合は、ご使用環境に適した設定を行ってください。

Note - インターネット接続がすでに行われている場合などは、この画面が表示されず、次の画面が表示される場合があります。

10.「インターネットアドレス(I)」に【AI 人物検索サービス(クラウド監視カメラパッケージ)開通案内】の基本情報から「GW アドレス」を入力、「接続先の名前」には任意の名前(※)を入力し「作成(C)」をクリックします。

※本手順書では例として「OfficeAR」と入力しています

GWアドレス 211.2.***.***	事前共有キー presharedkey
管理端末接続用VPN ログインID ① vpn1d1	管理端末接続用VPNログインパスワード ① vpnpass1
管理端末接続用VPN ログインID ② vpn1d2	管理端末接続用VPNログインパスワード ② vpnpass2

職場への接続

接続に使用するインターネット アドレスを入力してください

① このアドレスは、ネットワーク管理者より受け取ることができます。

インターネット アドレス(I):
211.2.***.***
GW アドレス 入力

接続先の名前(E):
OfficeAR
任意の名前 入力

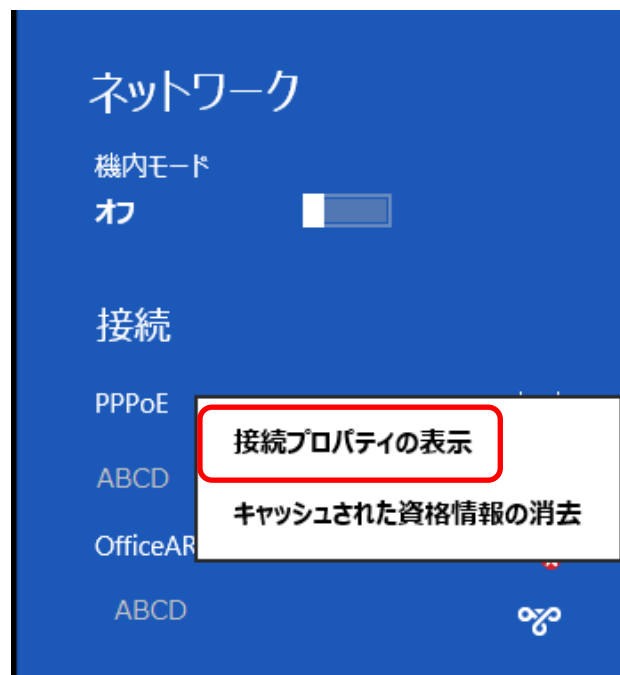
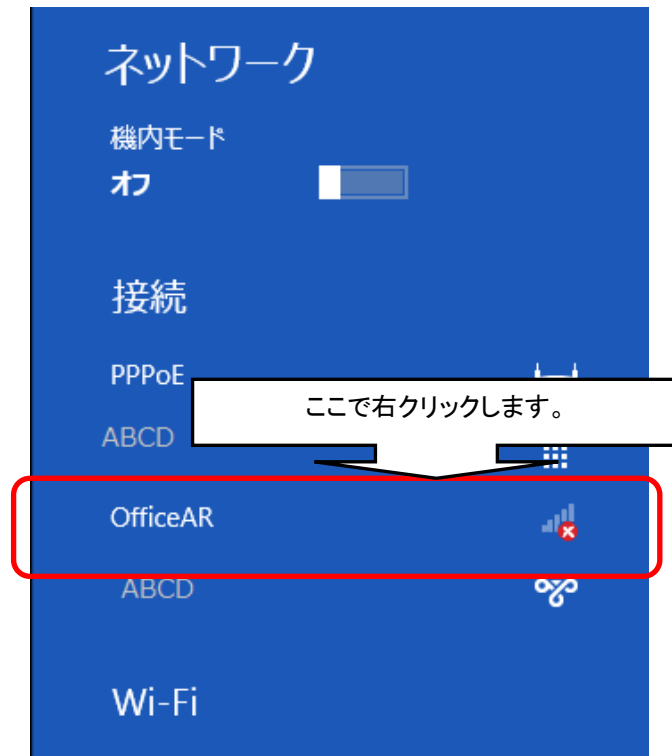
☐ スマートカードを使用する(S)
☐ 資格情報を記憶する(R)
☒ 他の人がこの接続を使うことを許可する(A)
このオプションによって、このコンピューターにアクセスがあるすべての人がこの接続を使えるようになります。

②

作成(C)
キャンセル

11.「ネットワーク」画面が開きますので、「接続」の一覧に P.13 で任意の名前で作成した「接続先の名前 (E)」(※)が表示されていることを確認し、マウスを右クリックし、メニューを表示します。表示されたメニューから、「接続プロパティの表示」をクリックします。

※本手順書では例として「OfficeAR」と入力しています



12.「OfficeAR」のダイアログが開きますので、「全般」のタブに、P.13 で入力した GW アドレスが入力されていることを確認します。

GWアドレス 211.2.***	事前共有キー presharedkey
管理端末接続用VPN ログインID ① vpnid1	管理端末接続用VPNログインパスワード ① vpnpass1
管理端末接続用VPN ログインID ② vpnid2	管理端末接続用VPNログインパスワード ② vpnpass2

OfficeARのプロパティ

全般 オプション セキュリティ ネットワーク 共有

宛先のホスト名または IP アドレス (例: microsoft.com、157.54.0.1、または 3ffe:1234::1111)(H):

211.2.***.***

最初の接続

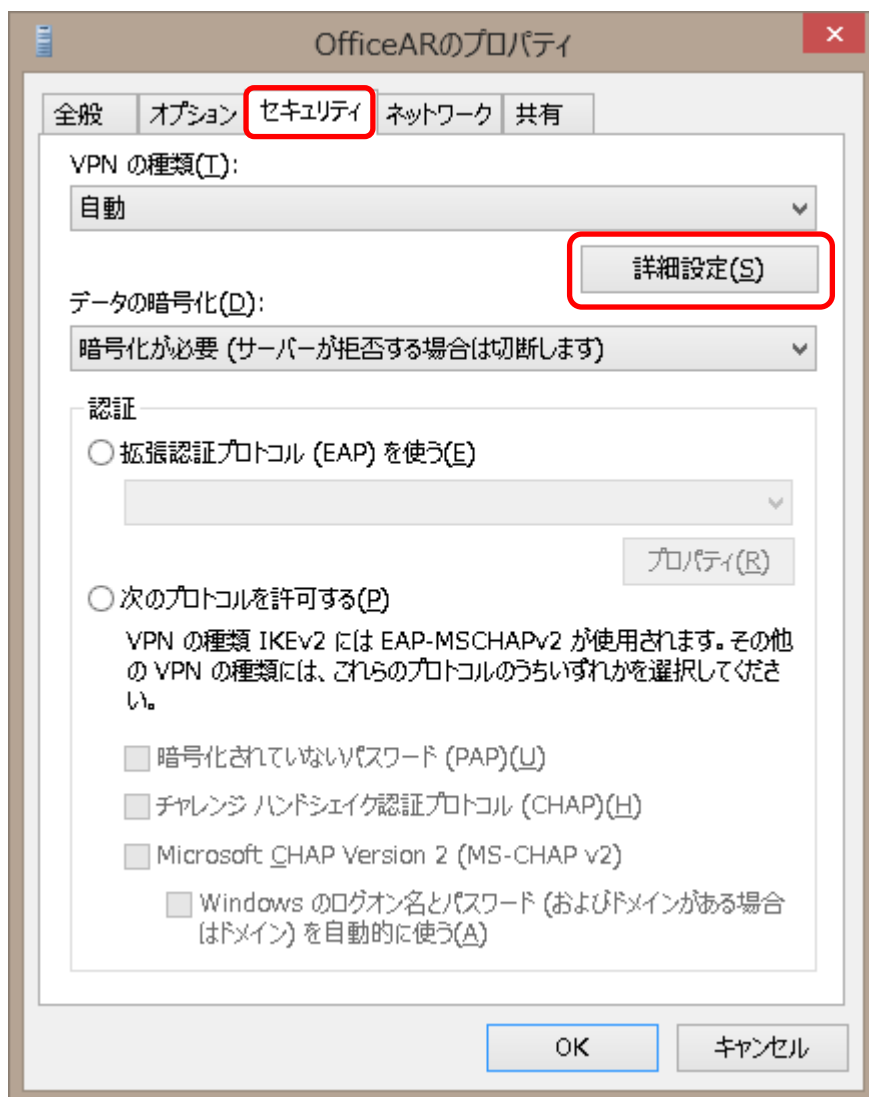
この仮想接続を確立する前に、まずインターネットなどのパブリック ネットワークに接続することができます。

☐ 別の接続に最初にダイヤルする(D):

プライバシーに関する声明

OK キャンセル

13.「セキュリティ」タブを開き、「詳細設定(S)」をクリックします。



14.「詳細プロパティ」ダイアログが開きますので、「L2TP」タブの「認証に事前共有キーを使う(P)」にチェックを入れ、「キー(K)」に【AI 人物検索サービス(クラウド監視カメラパッケージ)開通案内】の基本情報「事前共有キー」を入力し、「OK」をクリックします。

クリックすると、「詳細プロパティ」のダイアログが閉じます。

GWアドレス 211.	事前共有キー presharedkey
管理端末接続用VPN ログインID ① vpnic.	管理端末接続用VPNログインパスワード ① vpnpass1
管理端末接続用VPN ログインID ② vpnic.	管理端末接続用VPNログインパスワード ② vpnpass2

詳細プロパティ

L2TP

①

☒ 認証に事前共有キーを使う(P)
 キー(K): presharedkey

☐ 認証に証明書を使う(C)
☒ サーバーの証明書の名前と使用法の属性を確認する(V)

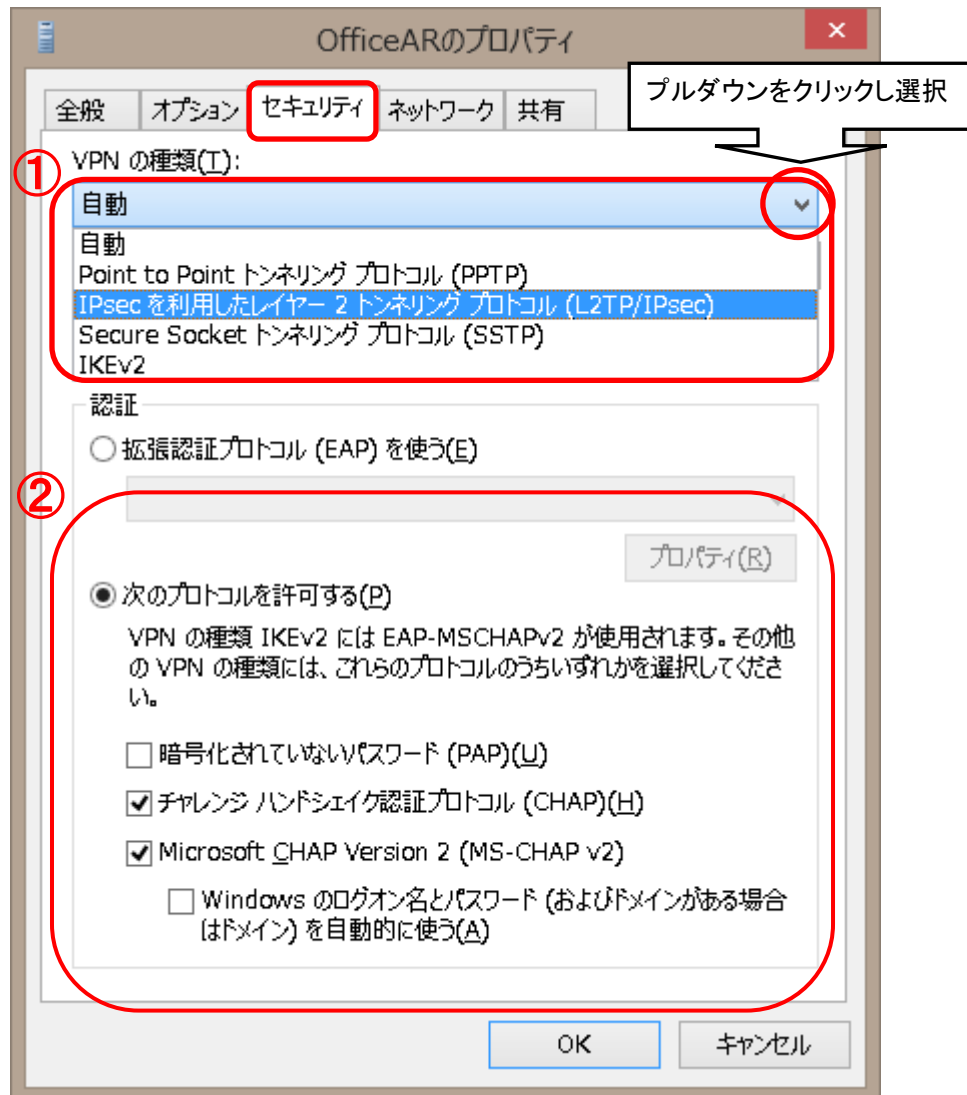
②

OK

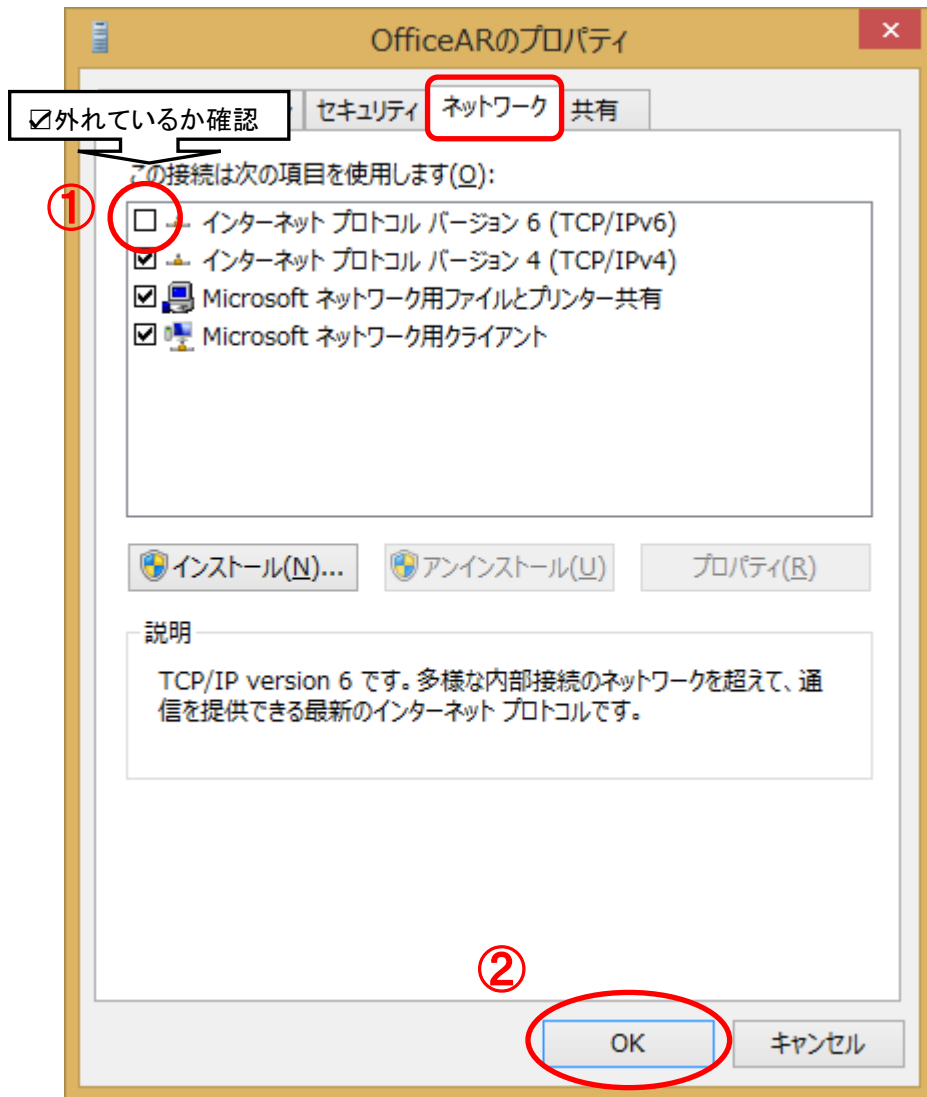
キャンセル

15.「セキュリティ」タブの「VPN の種類(T)」のプルダウンから、「IPsec を利用したレイヤー 2 トンネリング プロトコル(L2TP/IPsec) 」を選択します。

「認証」から「次のプロトコルを許可する(P)」にチェックを入れ、「チャレンジハンドシェイク認証プロトコル (CHAP)(H)」、「Microsoft CHAP Version 2(MS-CHAP v2)」にチェックを入れます。



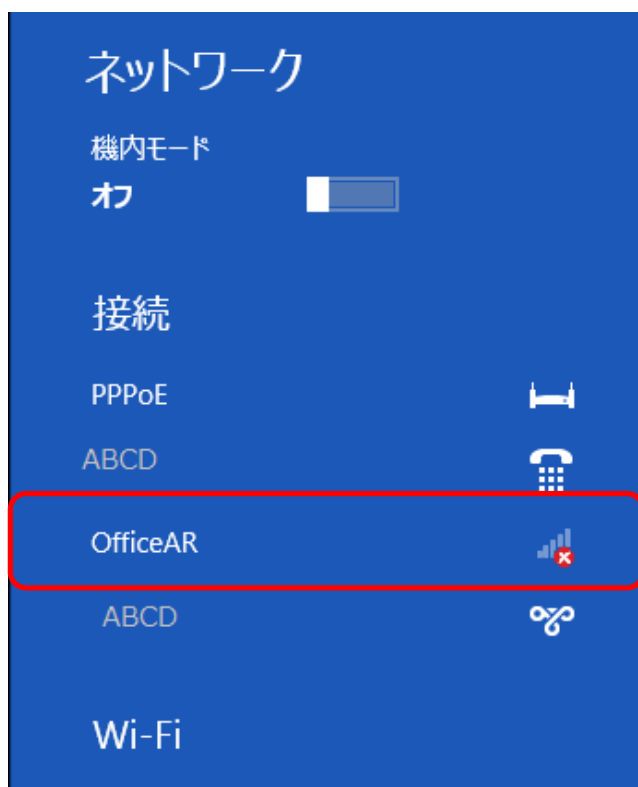
- 16.「ネットワーク」タブを開き、「インターネットプロトコルバージョン 6(TCP/IPv6)」の設定を確認します。
 チェックが入っていれば、チェックを外します。
 「OK」をクリックして、プロパティのダイアログが終了します。



17. 以上で設定は完了です。

「ネットワーク」に戻ったら、「接続」の一覧に P.13 で任意の名前で作成した「接続先の名前 (E)」(※) をクリックします。


※本手順書では例として「OfficeAR」と入力しています



- 18.「ネットワーク認証」画面が開きますので、「ユーザー名」「パスワード」に【AI 人物検索サービス(クラウド監視カメラパッケージ)開通案内】の基本情報から「管理端末接続用 VPN ログイン ID①または②」を「ユーザー名」に「管理端末接続用 VPN ログインパスワード①または②」を「パスワード」に入力し「OK」をクリックすると、接続が開始されます

GWアドレス 211.2.***.***	事前共有キー presharedkey
管理端末接続用VPN ログインID ① vpn1d1	管理端末接続用VPNログインパスワード ① vpnpass1
管理端末接続用VPN ログインID ② vpn1d2	管理端末接続用VPNログインパスワード ② vpnpass2

ネットワーク認証



ユーザー名

管理端末接続用 VPN ログイン ID①または②入力

パスワード

管理端末接続用 VPN ログインパスワード①または②入力

ドメイン:

OK

キャンセル

19. 下記のように、「接続済み」と表示されれば、接続完了です。

