
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 7 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 7 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 7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 7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 7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 7)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。

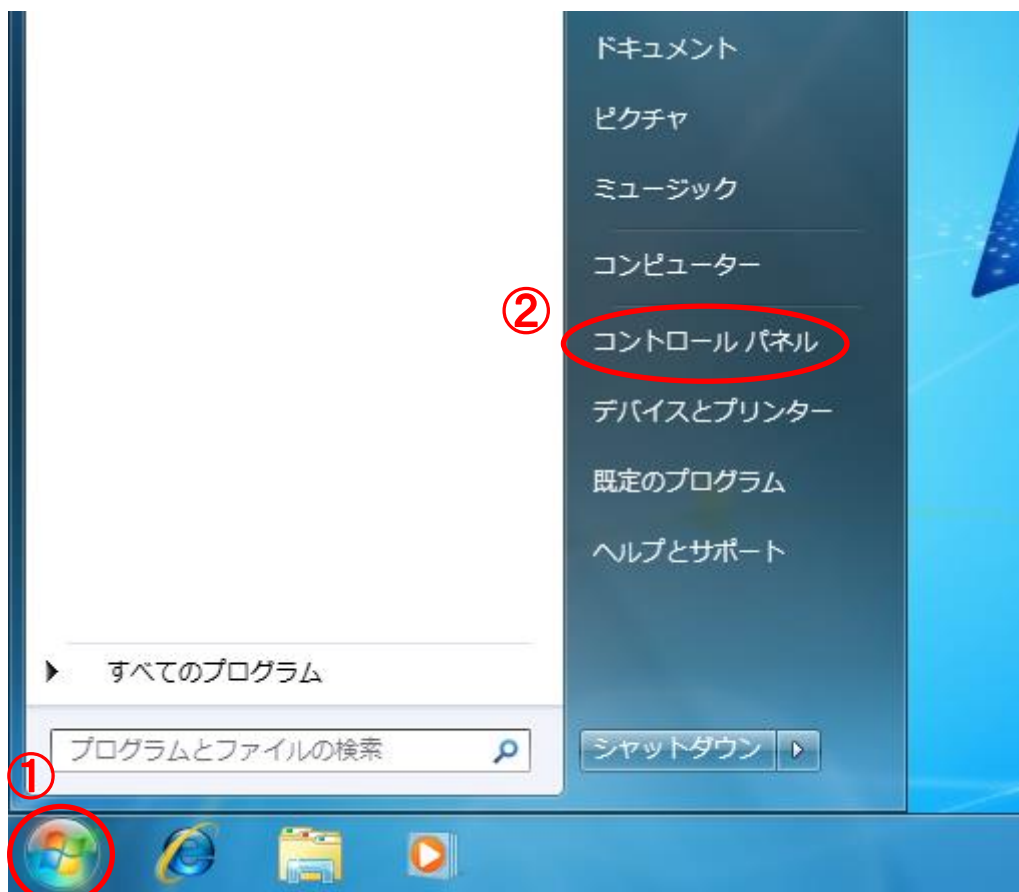
なお、ご利用 PC 側の詳細な設定方法については、Microsoft Windows 7 のマニュアルなどをご覧ください。

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 7 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 7 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

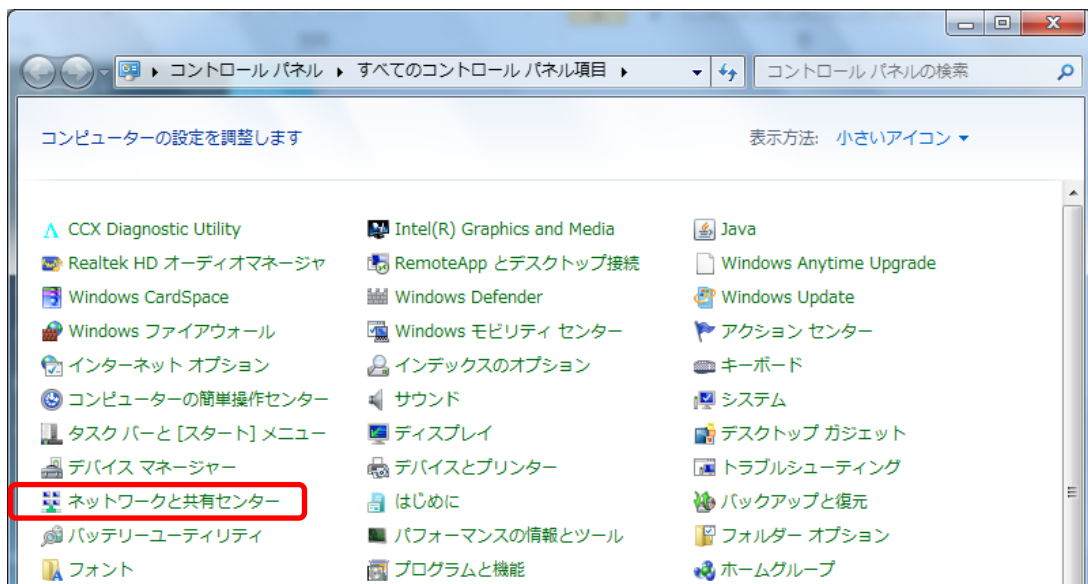
1. Window 画面左下の「スタート」ボタンをクリックし、「コントロールパネル」を選択します。



2. 「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。

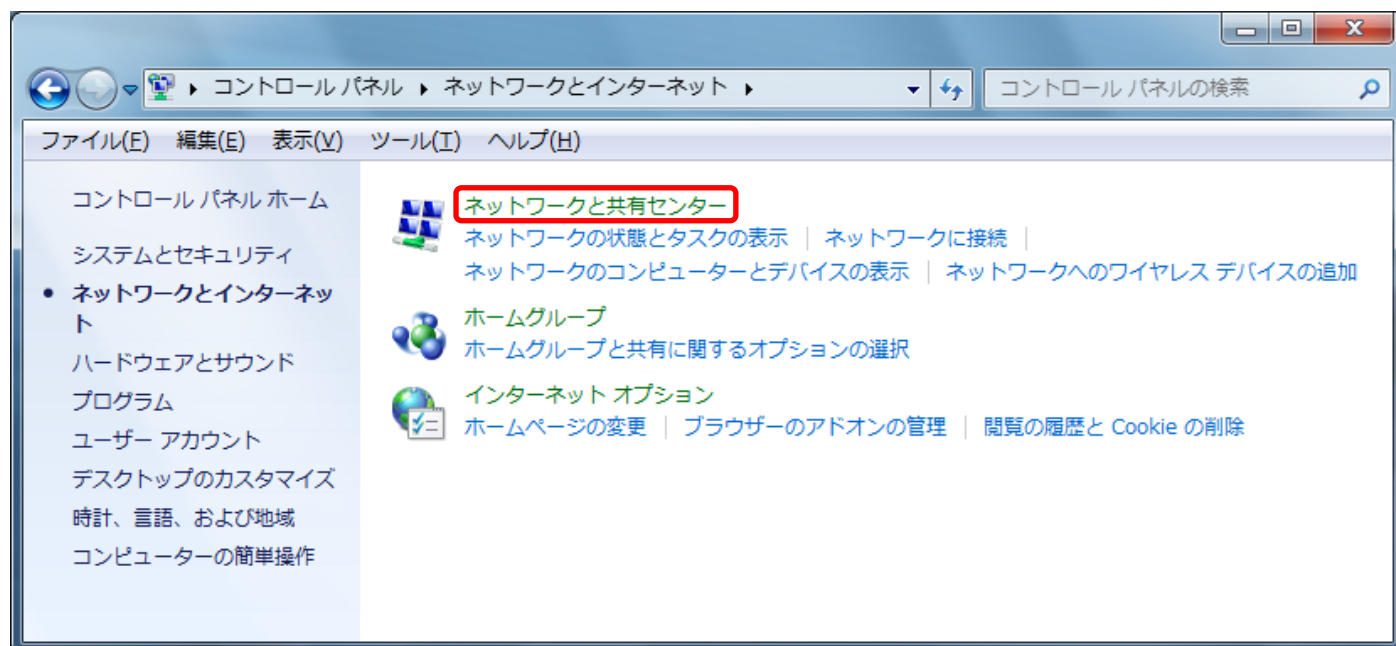


※「コントロールパネル」のダイアログが下記のように詳細項目に分かれて表示された場合は、「ネットワークと共有センター」をクリックします。



Note – 上記のように、詳細項目から「ネットワークと共有センター」をクリックした場合は、手順「3」を省略して手順「4」に進んでください。

3. 「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。



4. 「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。

ネットワーク設定の変更



新しい接続またはネットワークのセットアップ

ワイヤレス、ブロードバンド、ダイヤルアップ、アドホック、または VPN 接続をセットアップします。あるいは、ルーターまたはアクセス ポイントをセットアップします。



ネットワークに接続

ワイヤレス (無線)、ワイヤード (有線)、ダイヤルアップ、または VPN ネットワーク接続を確立または再確立します。



ホームグループと共有に関するオプションを選択する

他のネットワーク コンピューター上にあるファイルやプリンターを利用します。または、共有設定を変更します。



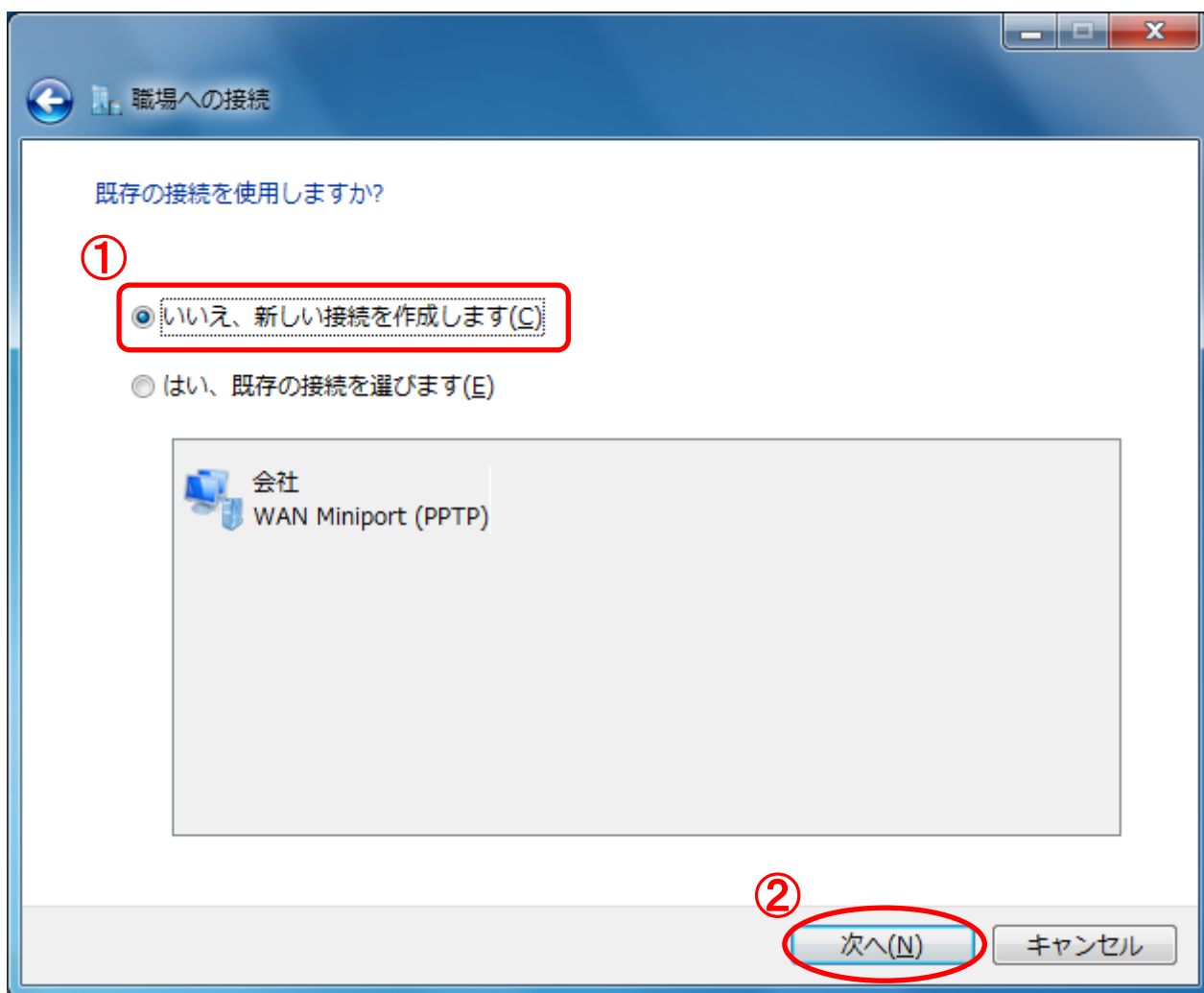
問題のトラブルシューティング

ネットワークの問題を診断して修復します。または、トラブルシューティングに関する情報を入力します。

5. 「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。



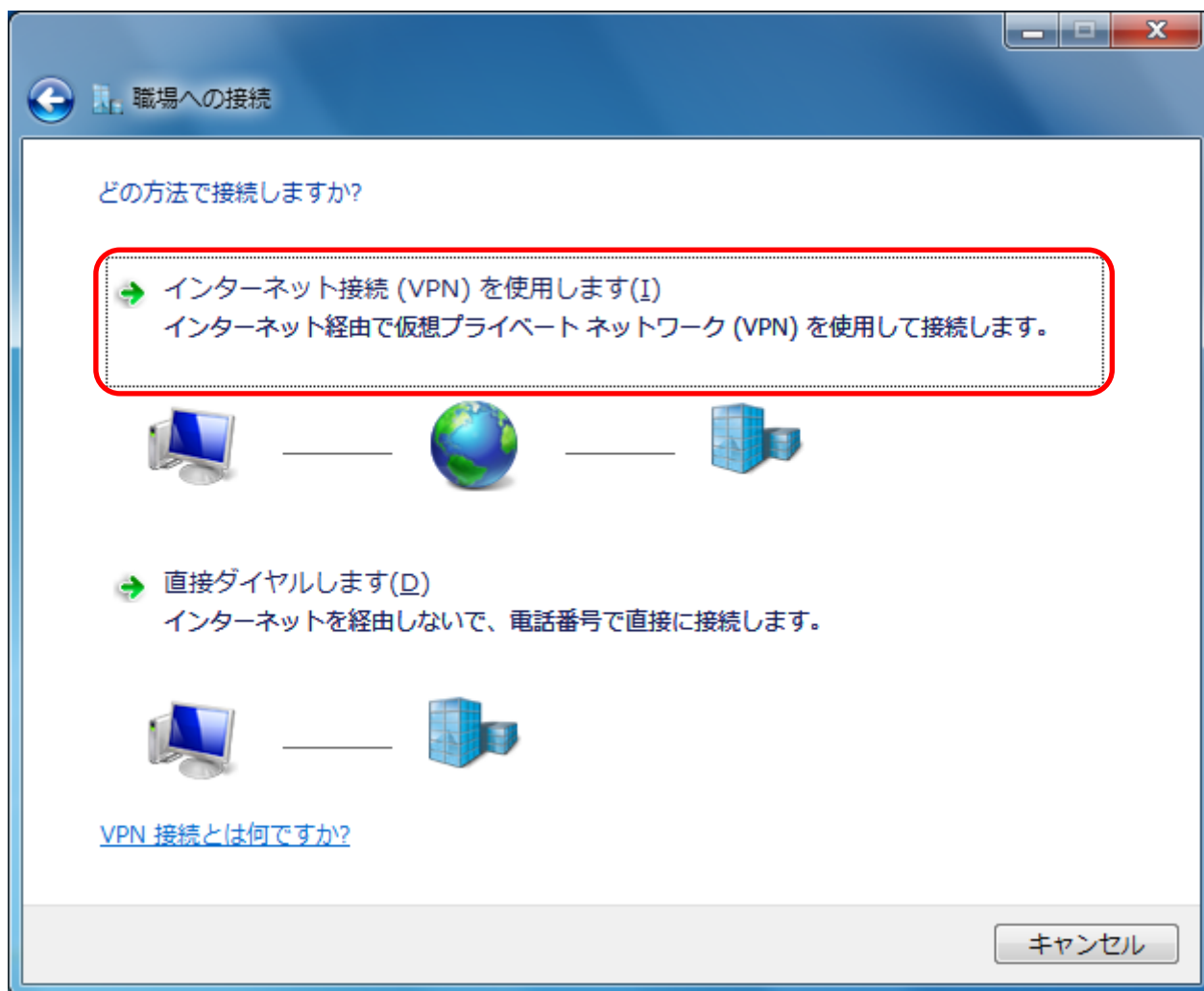
6. 「職場への接続」のダイアログが開きますので、「いいえ、新しい接続を作成します(C)」を選択して「次へ(N)」をクリックします。



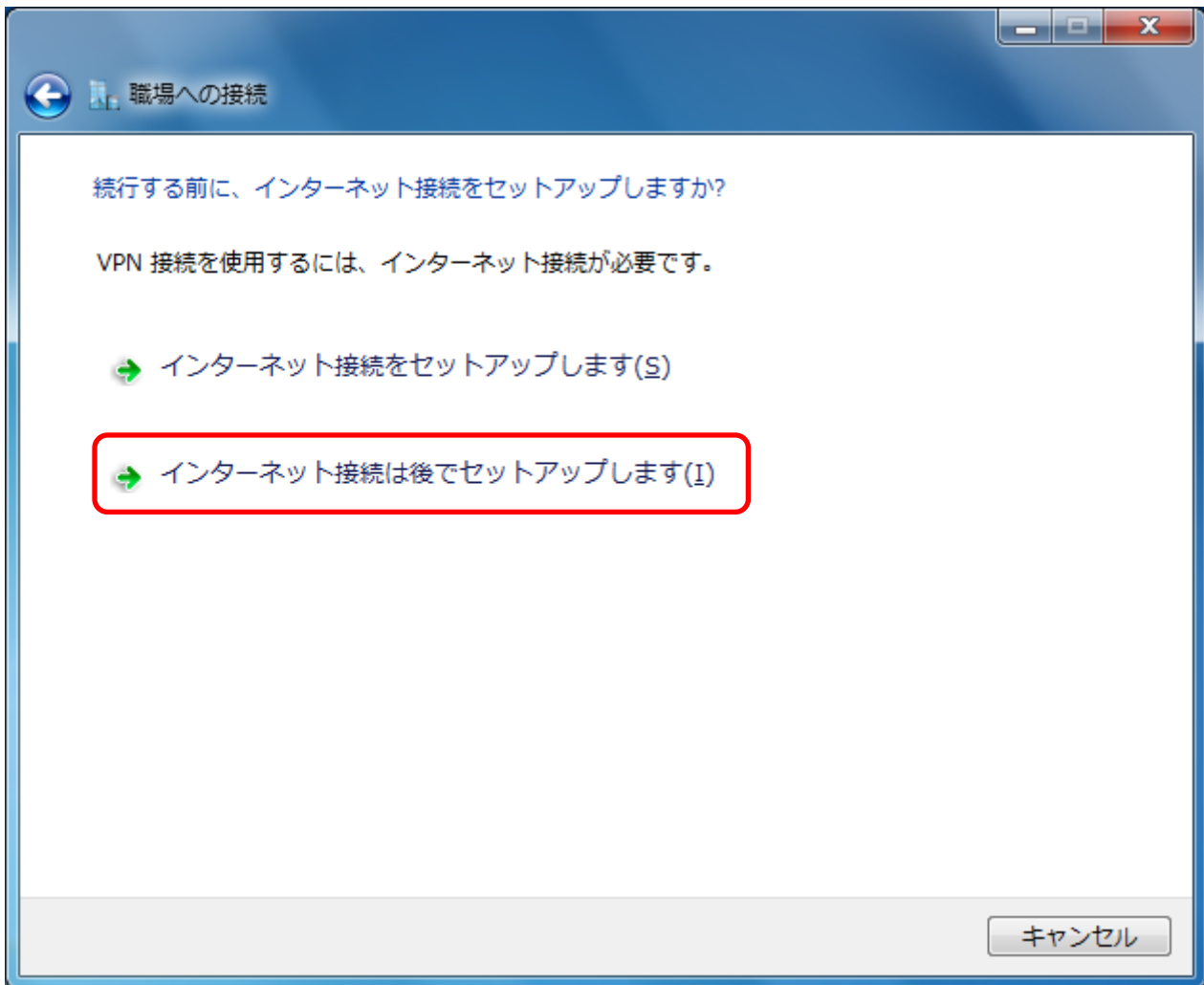
Note – 既存の接続が作成されていない場合などは、この画面が表示されず、次の画面が表示される場合があります。

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。

7. 「インターネット接続(VPN)を使用します(I)」を選択します。



8. 「インターネット接続は後でセットアップします(I)」を選択します。



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、P.12 の画面が表示される場合があります。

9. 「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「次へ(N)」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 vpn1	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 vpn2	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

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。

①

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)

☐ 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。

☒ 今は接続しない。自分が後で接続できるようにセットアップのみを行う(D)

②

次へ(N) キャンセル

10. 【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(U)」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(P)」に入力し「作成(C)」をクリックします。

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

職場への接続

① ユーザー名およびパスワードを入力してください

ユーザー名(U):

パスワード(P):

☐ パスワードの文字を表示する(S)

☐ このパスワードを記憶する(R)

ドメイン (オプション)(D):

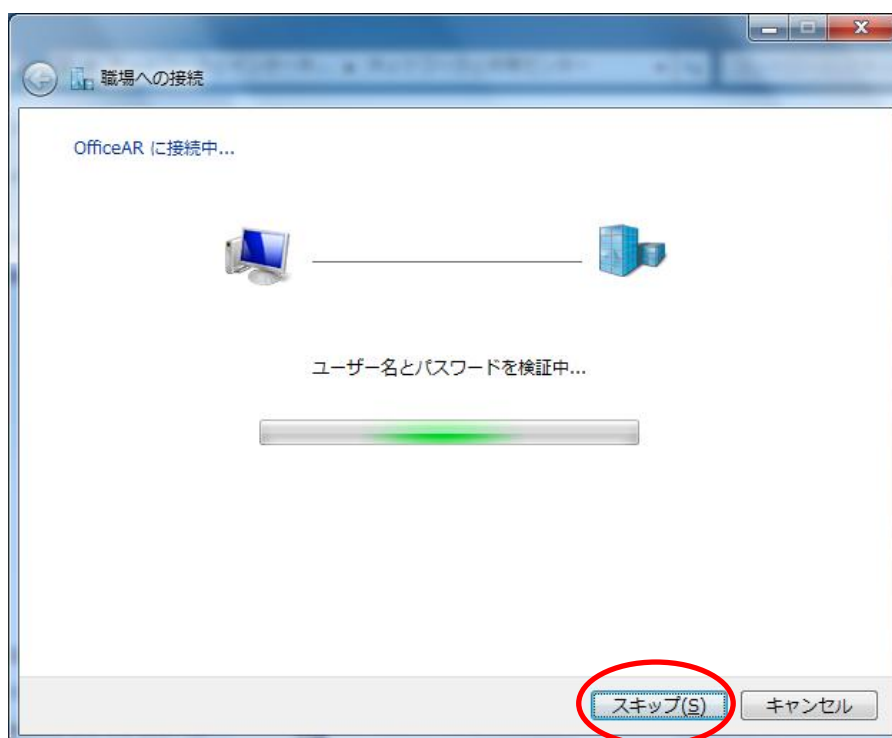
「接続(C)」と表示される場合があります。
その時は「接続(C)」ボタンをクリックしてください。

②

11. 「接続の使用準備ができました」の画面が開きますので、「閉じる(C)」をクリックします。



Note – P.13 で「接続(C)」ボタンをクリックした場合は、次のように「スキップ(S)」ボタンをクリックしてください。

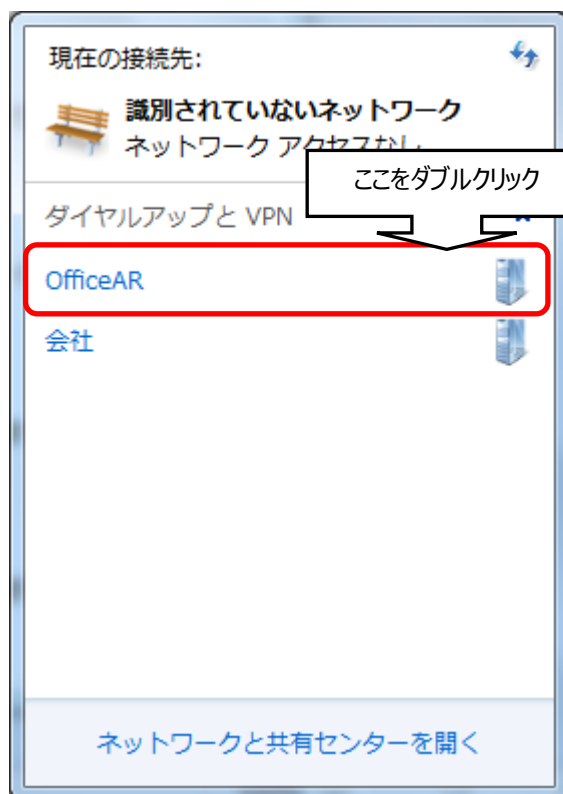


12. 再度 P.4~7 の手順を行い「ネットワークと共有センター」のダイアログが開きましたら、「接続または切断」をクリックします。



13. 「現在の接続先」のダイアログが開きますので、接続先の一覧から P.12 で任意の名前で作成した「接続先の名前」(※)を選んでダブルクリックします。

※本手順書では例として「OfficeAR」と入力しています

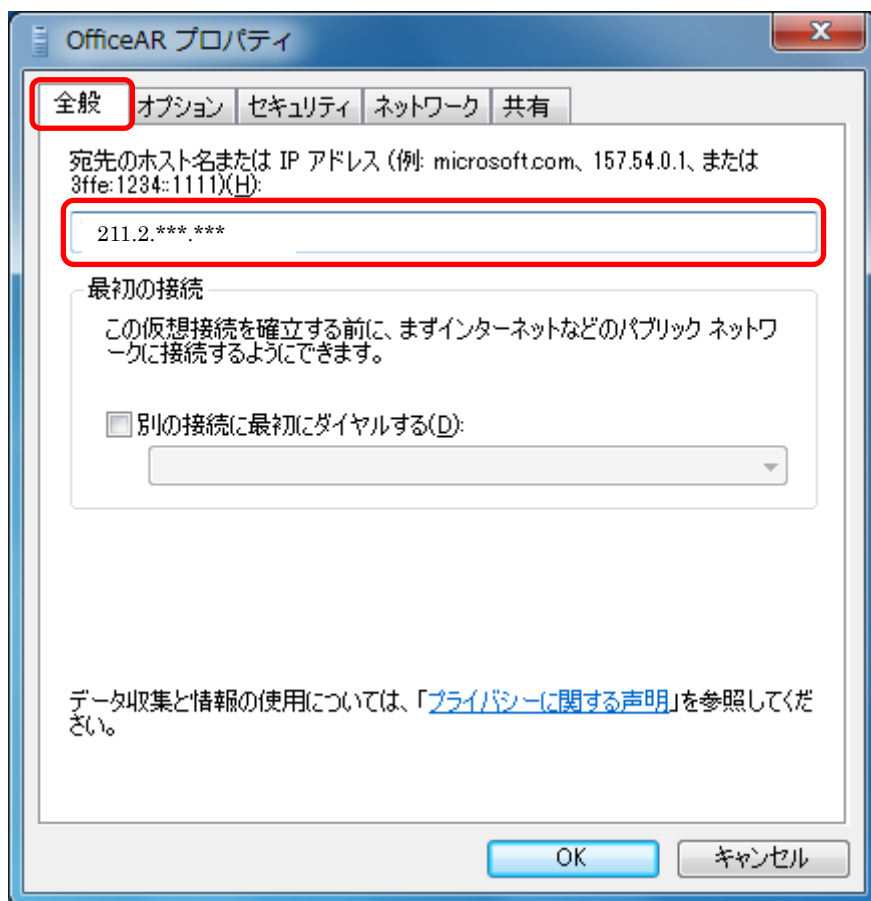


14. 「OfficeAR へ接続」のダイアログが開きますので、「プロパティ」をクリックします。

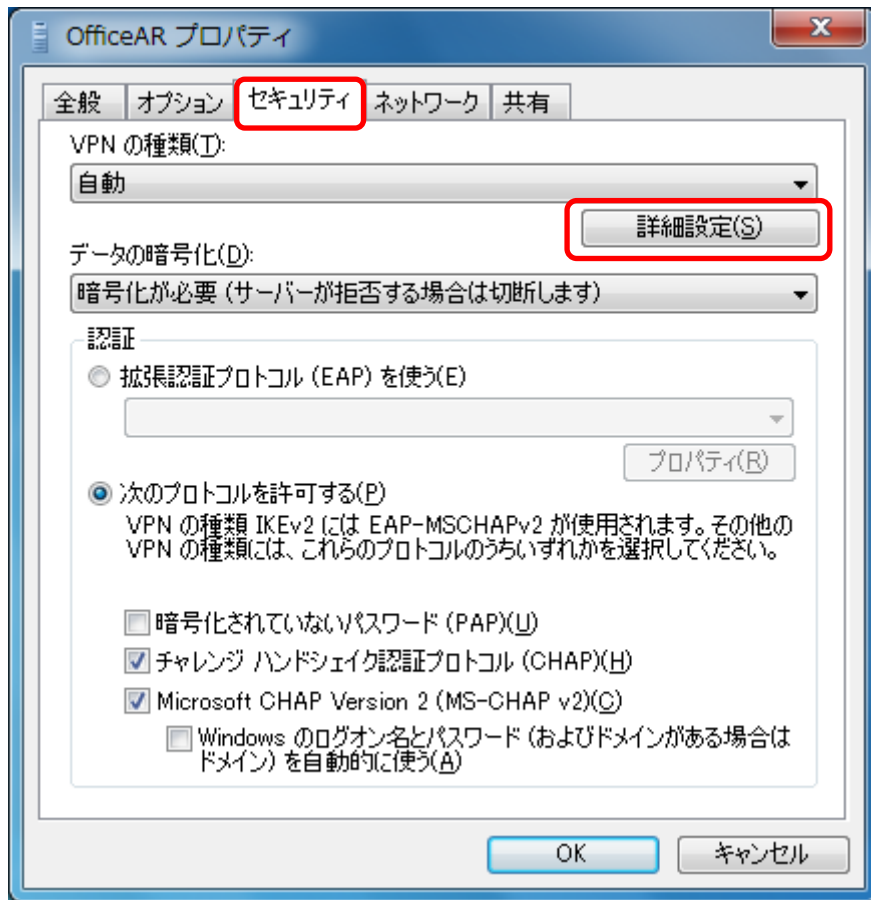


15. 「OfficeAR プロパティ」のダイアログが開きますので、「全般」のタブに、P.12 で入力した GW アドレスが入力されていることを確認します。

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 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



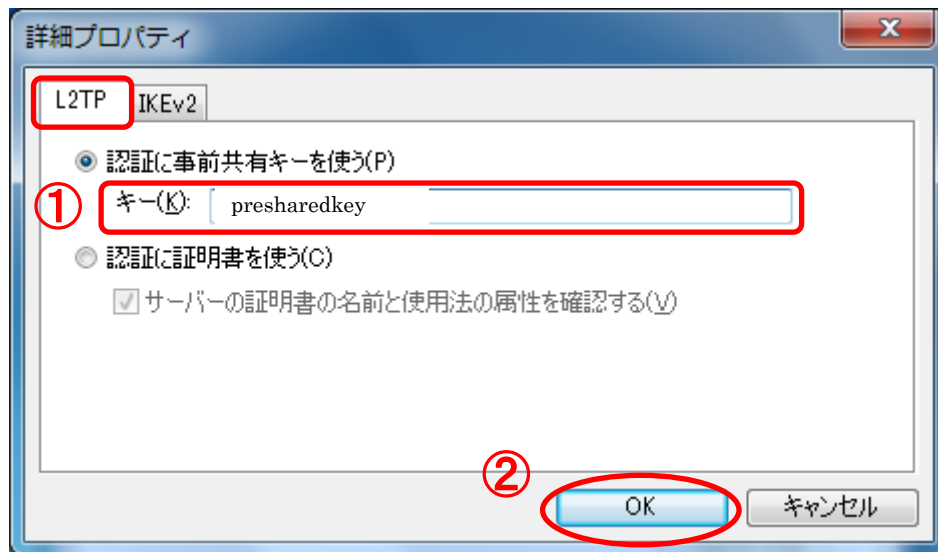
16. 「セキュリティ」タブを開き、「詳細設定(S)」をクリックします。



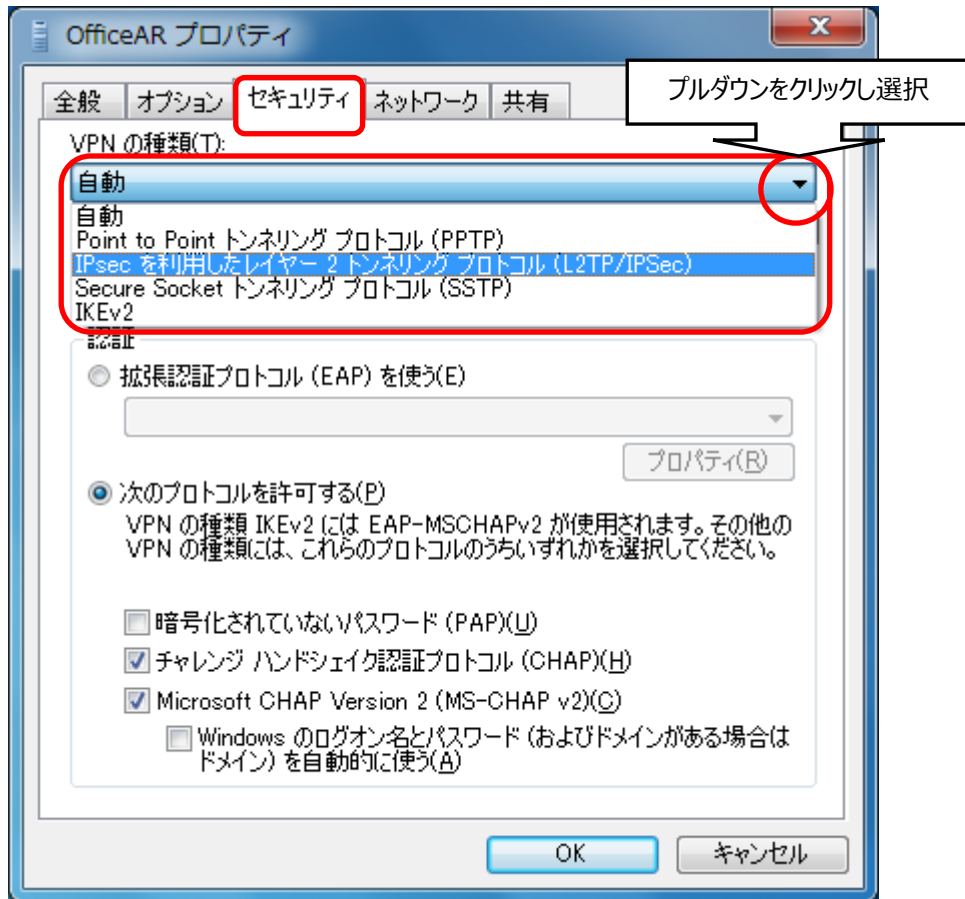
17.「詳細プロパティ」ダイアログが開きますので、「L2TP」タブの「認証に事前共有キーを使う(P)」にチェックを入れ、「キー(K)」に【AI 人物検索サービス(クラウド監視カメラパッケージ)開通案内】の基本情報「事前共有キー」を入力し、「OK」をクリックします。

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。

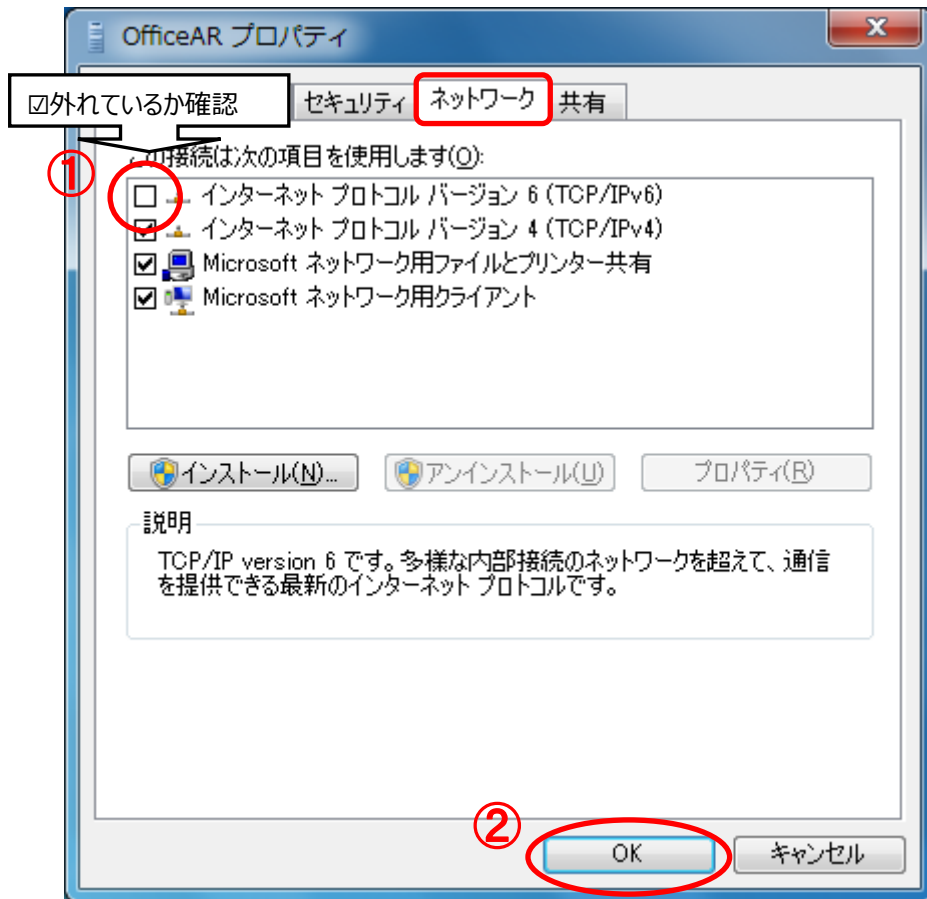
GWアドレス 211.2.***.***	事前共有キー presharedkey
管理端末接続用VPN ログインID ① vpnid1	管理端末接続用VPNログインパスワード ① vpnpass1
管理端末接続用VPN ログインID ② vpnid2	管理端末接続用VPNログインパスワード ② vpnpass2



18. 「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。



19. 「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。



20. 「OfficeAR へ接続」のダイアログに戻ったら、【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(U)」に「管理端末接続用 VPN パスワード①または②」を「パスワード(P)」に入力し、「接続(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 vpn1	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 vpn2	管理端末接続用VPNログインパスワード ② vpnpass2



The image shows a Windows-style dialog box titled "OfficeAR へ接続". It features a graphic of a laptop, a globe, and a desktop monitor connected by a green line. Below the graphic, there are input fields for "ユーザー名(U):", "パスワード(P):", and "ドメイン(M):". To the right of these fields, there are labels: "管理端末接続用 VPN ログイン ID①または②入力" for the username and "管理端末接続用 VPN ログインパスワード①または②入力" for the password. Below the input fields, there is a checkbox labeled "次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する(S):". Under this checkbox, there are two radio button options: "このユーザーのみ(N)" and "このコンピューターを使うすべてのユーザー(A)". At the bottom of the dialog, there are four buttons: "接続(C)", "キャンセル", "プロパティ(O)", and "ヘルプ(H)". The "接続(C)" button is circled in red, and a red circle with the number "2" is next to it. A red circle with the number "1" is next to the username input field.

21. 再度 P.16 の手順で「現在の接続先」を開き、P.13 で任意の名前で作成した「接続先の名前」(※)が「接続済み」と表示されれば、接続完了です。

※本手順書では例として「OfficeAR」と入力しています

