RICOH

ITKeeper Meraki スマートサービス

ご利用の手引き Ver3.5

ご使用の前に、本書を最後までよくお読みの上、正しくお使いください。また、本書が必要になったとき、すぐに利用できるように保管してください。

必ずお読みください

- 弊社が提供する、Meraki スマートサービスの取扱操作説明・管理操作説明・注意事項・制約事項を記述しています。
- ご契約者に提供する機器は、ご購入頂く機器によって異なります。
- お客様データの消失による損害、その他本サービスおよび使用説明書の使用または使用不能により生じた損害については、法令上賠償責任が認められる場合を除き、当社は一切その責任を負えませんのであらかじめご了承ください。
- サポート対応やメンテナンスなど、サービスの正常提供に必要な範囲で、お客様機器および、管理画面にログインさせていただくことがあります。
- お客様が追加、修正した情報、パスワードの管理などはお客様にてお願いいたします。
- お客様がご利用の ISP（インターネット サービス プロバイダー）の障害や、回線の障害時にはサービスをご利用いただけないことがあります。
- ブラウザは最新版をご利用ください。

おことわり

- 本書の内容の一部または全部を無断で複写することは禁止されております。
- 本書の内容は事前の予告なく変更されることがあります。
- 運用した結果の影響については責任を負いかねますので、ご注意ください。

目次

必ずお読みください 2
おことわり 3
目次 4
はじめに 5
　この本の読みかた 5
　　マークについて 5
無線 LAN および VPN の管理 6
　ユーザー管理ポータル画面にログインする 6
　　認証の強化と新しいセキュリティ機能について 7
　　二要素認証（SMS 認証）を設定する 8
　　二要素認証（SMS 認証）設定を確認する 9
　クライアント VPN ユーザー/無線 LAN ユーザーを新規追加する 10
　クライアント VPN ユーザー/無線 LAN ユーザーの情報を変更する 11
　クライアント VPN ユーザー/無線 LAN ユーザーを削除する 12
　DDNS 名を確認する 12
　パスワードを再設定する（パスワードを忘れた場合等） 13
VPN クライアント(L2TP/IPsec)を設定する（パソコン版） 16
　リモートアクセス設定ウィザードを実行する（パソコン版） 16
　プロパティを設定する（パソコン版） 17
　接続する（パソコン版） 19
　切断する（パソコン版） 21
動作を確認する（パソコン版） 22
　VPN 接続画面を起動する（パソコン版） 22
VPN クライアント(L2TP/IPsec)を設定する（iOS 版） 24
　L2TP を設定する（iOS 版） 24
　接続と切断を確認する（iOS 版） 25
VPN クライアント(L2TP/IPsec)を設定する（Android 版） 28
　L2TP を設定する（Android 版） 28
　接続を確認する（Android 版） 31
　切断を確認する（Android 版） 32
無線プロファイルを設定する（パソコン版） 34
　プロファイルを設定する（パソコン版） 34
　動作を確認する（パソコン版） 36
　手動による設定（パソコン版） 37
無線プロファイルを設定する（iOS 版） 40
　プロファイルを設定する（iOS 版） 40
　動作を確認する（iOS 版） 43
無線プロファイルを設定する（Android 版） 44
　プロファイルを設定する（Android 版） 44
　動作を確認する（Android 版） 47
無線ネットワーク全体の状況確認 48
　クライアント接続状況 48
　トラフィック分析 48
　イベントログ 49
　サマリーレポート 49
アクセスポイントの状況確認 51
　アクセスポイントの状況確認 51
Meraki 認証を使用する 52
　クライアントを設定する（Windows 版） 52
　クライアントを設定する（iOS 版） 59
　クライアントを設定する（Android 版） 60
お問い合わせ先 63
商標 64

はじめに

本書は、ITKeeper Meraki スマートサービスをご契約いただいたお客様で、ネットワーク管理者となられる方を対象とした、導入手順などを記述した使用説明書です。本書の構成は以下のとおりです。

無線 LAN および VPN の管理
無線 LAN ユーザーとクライアント VPN ユーザーに関する各種設定方法を説明します。

また、作業するときは以下を準備してください。
・　LAN ケーブル（ストレートケーブル）

この本の読みかた

マークについて

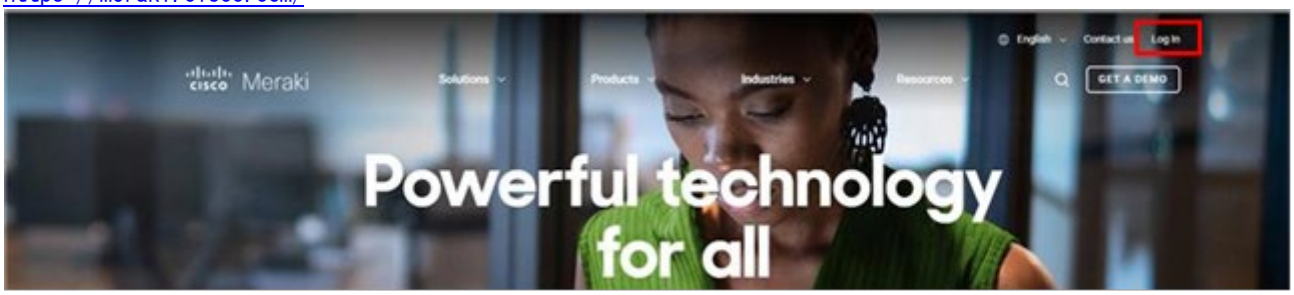
本書で使われているマークには次のような意味があります。

補足
操作するときに気を付けることや、操作を誤ったときの対処方法などを説明しています。
各タイトルの最後に記載しています。
[ ]
画面のキーや項目の名称を示します。

無線 LAN および VPN の管理

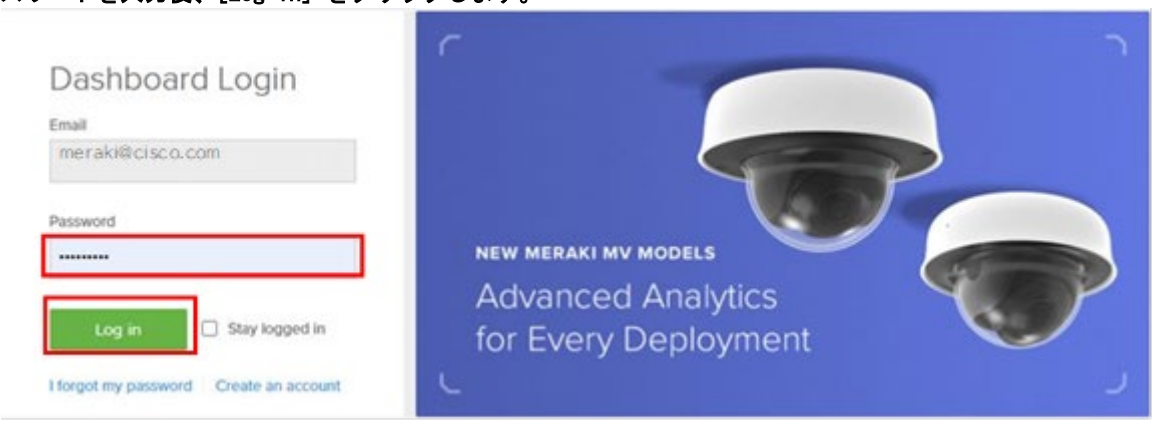
ユーザー管理ポータル画面にログインする

1. 以下の URL にアクセスします。下図画面が表示されたら、「Log In」をクリックします。
   https://meraki.cisco.com/

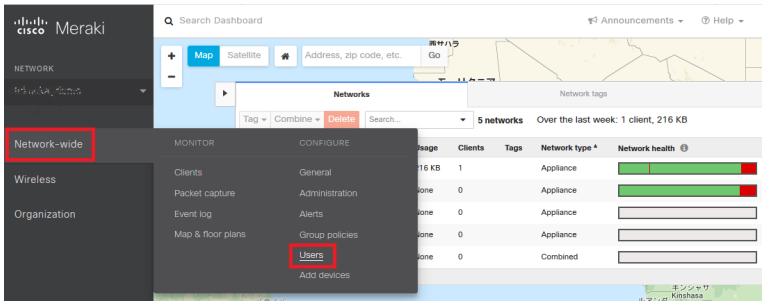


2. Email アドレスを入力後、[Next] をクリックします。

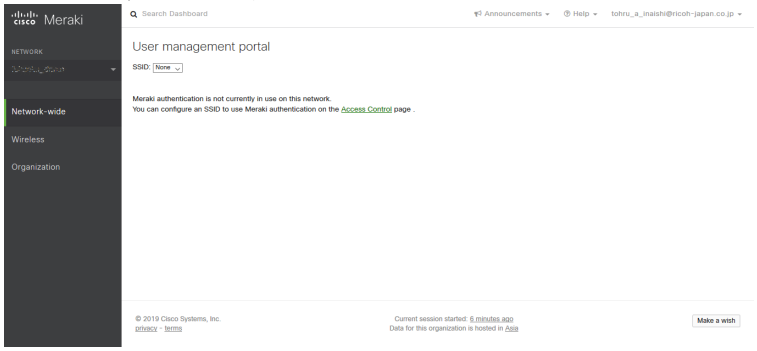
3. パスワードを入力後、[Log in] をクリックします。



4. 画面左のメニューで [Network-wide] にマウスオーバーし、[Users] をクリックします。



5. **以下の画面が表示されます。**



認証の強化と新しいセキュリティ機能について

2022 年 12 月以降、導入したセキュリティ機能では、以下のいずれかの条件を満たす場合に 6 桁のワンタイムパスワード(OTP) がログイン時に使用したメールアドレス宛に送信される追加の認証が行われるようになります。

- 不審なログイン試行を検知したとき
- ログイン対象の管理者がアクセス可能なネットワークにシステムマネージャーが含まれる場合

OTP はログイン画面で正しいパスワードが入力された際にも送信されることがあります。

なお、OTP を使用しない場合は、次項手順に沿って二要素認証(TFA)を設定してください。

詳しくは以下のリンクをご参照ください。

「認証の強化と新しいセキュリティ機能について」
https://documentation.meraki.com/General_Administration/Other_Topics/Authentication_Enhancements_and_New_Dashboard_Security_Features_jp

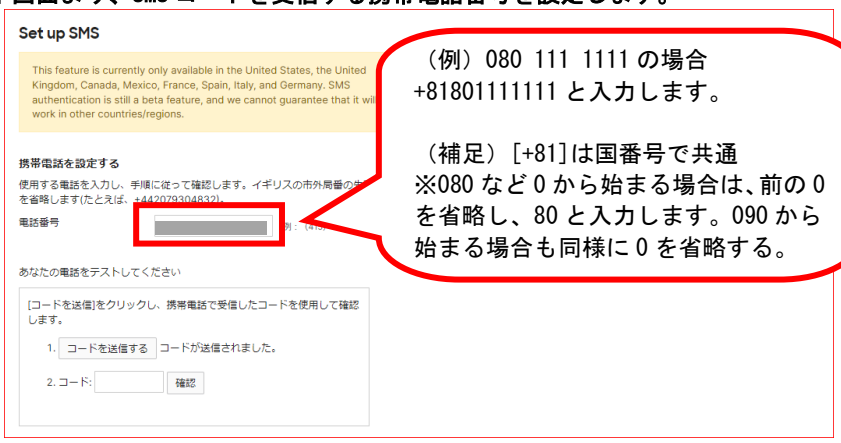
二要素認証（SMS 認証）を設定する

1. ダッシュボードにログイン後、ダッシュボード画面右にあるアカウント ID をクリックし、プロファイルを選択します。

2. 以下画面の二段階認証項目にある[二段階認証を設定する]をクリックします。

3. 以下画面の[Use SMS authentication instead]をクリックします。

4. **以下画面より、SMS コードを受信する携帯電話番号を設定します。**



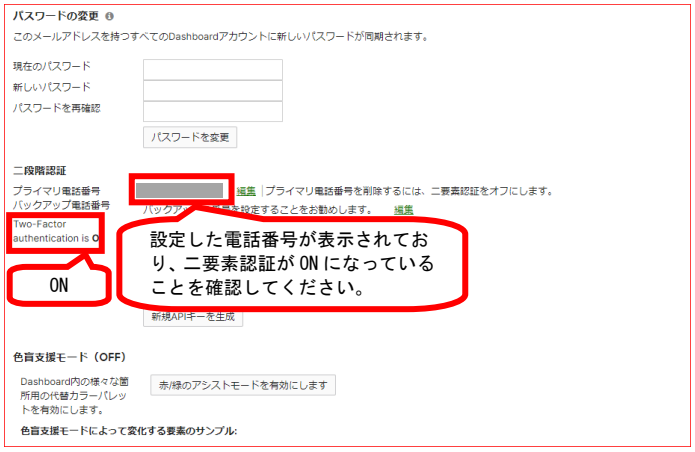
5. **以下画面より、SMS コードが送信されることを確認します。**

6. **以下画面より[コードを送信する]をクリックし、携帯電話に送信されたコードを[コード]欄に入力し、[確認]をクリックする。**

二要素認証（SMS 認証）設定を確認する

1. **ダッシュボードにログイン後、ダッシュボード画面右にあるアカウント ID をクリックし、プロファイルを選択します。**

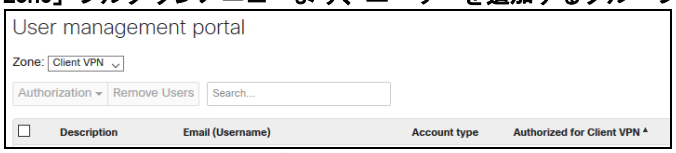
2. 以下画面の二段階認証項目にある[二段階認証を設定する]をクリックします。



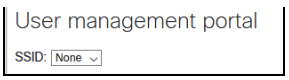
クライアント VPN ユーザー/無線 LAN ユーザーを新規追加する

※追加すると、登録したメールアドレス宛に CiscoMeraki よりメールが送信されます。

1. 「Zone」プルダウンメニューより、ユーザーを追加するグループ名を選びます。



※無線 LAN ユーザーの場合、以下の表記となります



- クライアントVPNユーザーのとき　：[Client VPN] を選択
- 無線LANユーザーのとき：対象のSSIDを選択

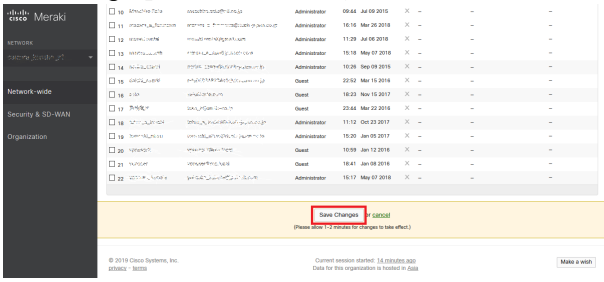
2. 画面右側にある [Add new user] をクリックします。

3. 各項目に入力し、[Create user] をクリックします。

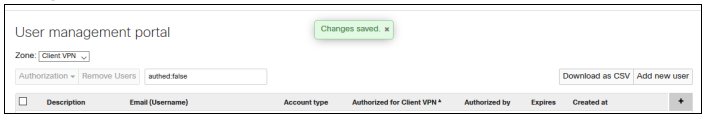
- Name　　：　追加するユーザー名を入力します。
- Email　　：　追加するユーザーのEmailアドレスを入力します。
- Password　　：　追加するユーザーのパスワードを入力します。[Generate] ボタンをクリックするとランダムパスワードが生成されます。
- Email new password to user　：　チェックしてユーザーを新規追加すると、「Email」に入力したアドレスにパスワードが通知されます。「Password」欄に入力すると表示されます。
- Authorized　：　[Yes] を選択するとユーザーIDで認証できます。
- Expires　　：　有効期限を指定します。初期値は [Never]（期限なし）です。「Authorized」欄で [Yes] を選択すると表示されます。

ユーザーが一覧画面に表示され、[Save Changes] 部分が黄色くなります。

4. **[Save Changes] をクリックします。**

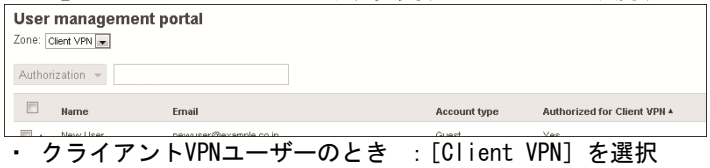


5. **「Changes saved.」と表示されます。**

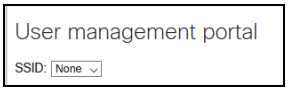


クライアント VPN ユーザー/無線 LAN ユーザーの情報を変更する

1. **「Zone」プルダウンメニューより、変更するユーザーが所属するグループ名を選びます。**

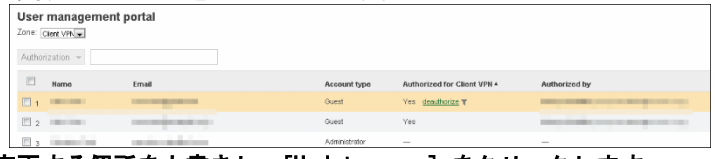


※無線 LAN ユーザーの場合、以下の表記となります

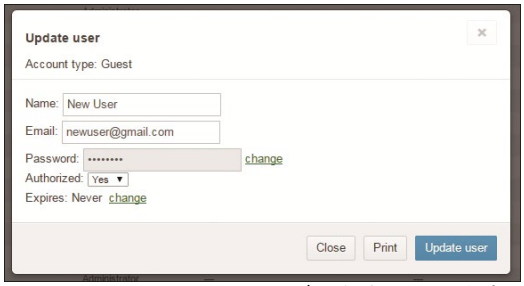


- クライアントVPNユーザーのとき　：[Client VPN] を選択
- 無線LANユーザーのとき：対象のSSIDを選択

2. **変更するユーザーをクリックします。**



3. **変更する個所を上書きし、[Update user] をクリックします。**

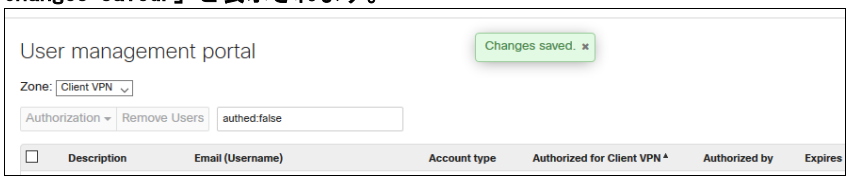


- Name　：　ユーザー名を入力します。
- Email　：　ユーザーのEmailアドレスを入力します。
- Password　：　ユーザーのパスワードを入力します。変更するときは［change］リンクをクリックします。
- Authorized　：　［Yes］を選択するとユーザーIDで認証できます。
- Expires　：　有効期限を指定します。変更するときは［change］リンクをクリックします。

更新したユーザーの情報が一覧画面画表示に表示され、［Save Changes］部分が黄色くなります。

4. **［Save Changes］をクリックします。**

5. **「Changes saved.」と表示されます。**

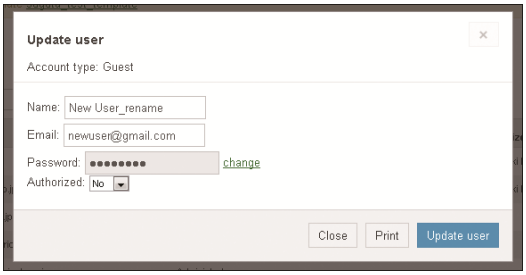


補足

- 「Account type」が「Guest」のユーザーの情報だけ変更できます。

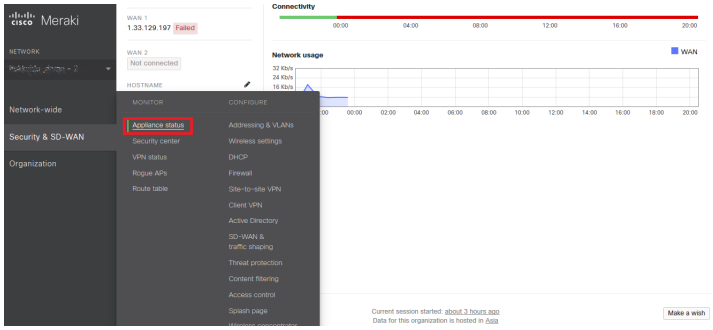
クライアント VPN ユーザー/無線 LAN ユーザーを削除する

お客様の権限ではユーザーを削除できません。
ユーザーを無効にするときは、「Authorized」を［No］に設定します。
また、「Name」、「Email」、「Password」を上書きして新規ユーザーに書き換えることができます。

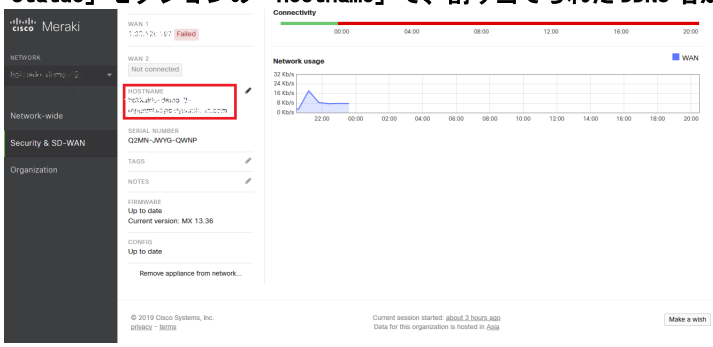


DDNS 名を確認する

1. **画面左のメニューで［Security appliance］にマウスオーバーし、［Appliance status］をクリックします。**

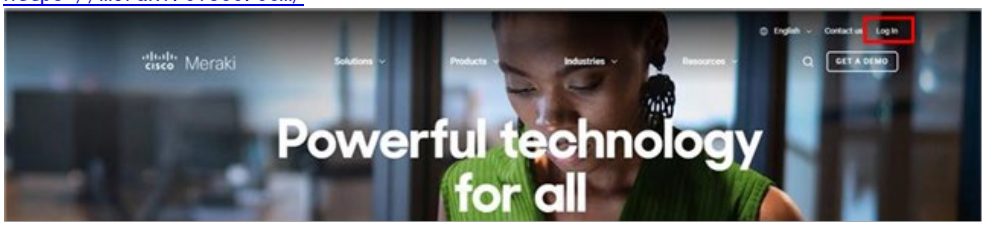


2. 「Status」セクションの「Hostname」で、割り当てられた DDNS 名が確認できます。



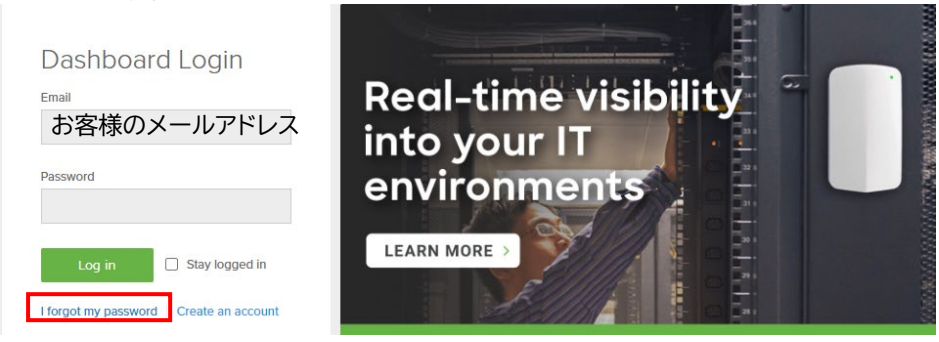
パスワードを再設定する（パスワードを忘れた場合等）

1. 以下の URL にアクセスします。下図画面が表示されたら、「Log In」をクリックします。
   https://meraki.cisco.com/

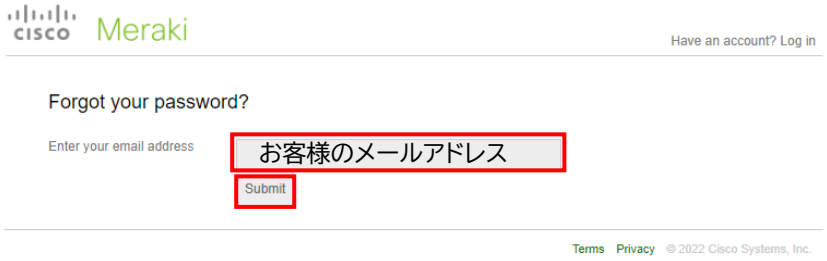


2. お客様のメールアドレスを入力し、「Next」をクリックします。

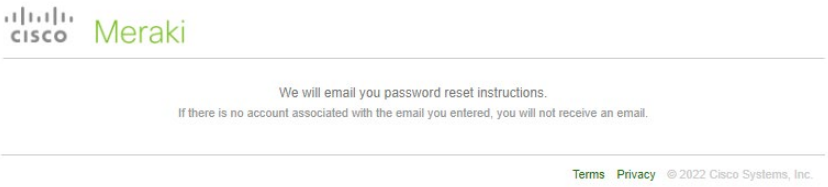
3. 「I forget my password」をクリックします。



4. **お客様のメールアドレスを入力し、「Submit」をクリックします。**



5. **以下画面が表示されたら、お客様ご自身のメールボックスをご確認ください。**

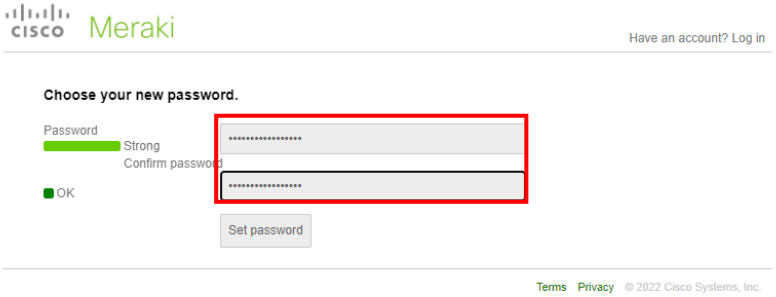


6. **以下タイトルのメールを開きます。**

送信元：Cisco Meraki - no Reply
タイトル：Cisco Meraki Password Reset

7. **メール中央部にあるリンクをクリックします。**

8. **新しいパスワードを入力します。**



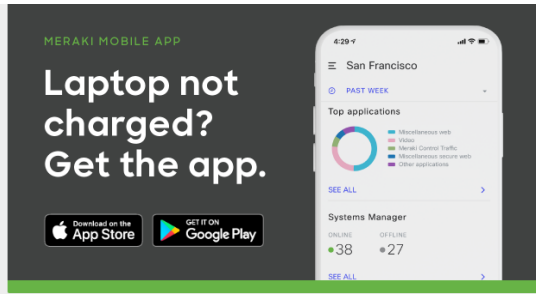
9. **ログイン画面が表示されます。設定は以上です。**

Dashboard Login

Email

Next

I forgot my email | Create an account



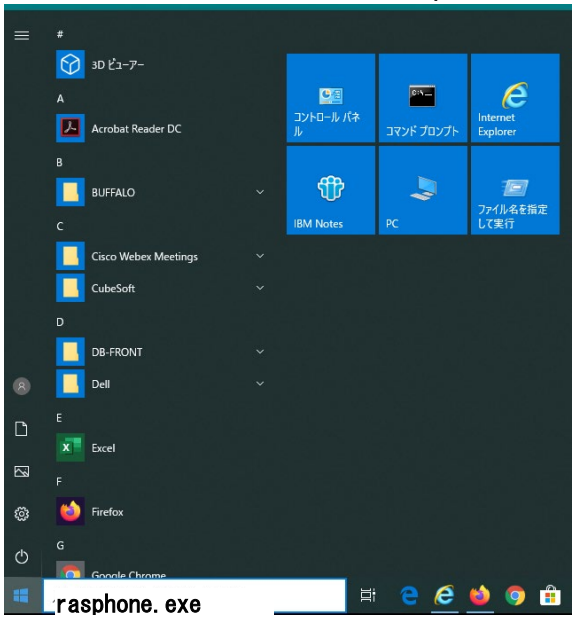
VPN クライアント(L2TP/IPsec)を設定する（パソコン版）

補足

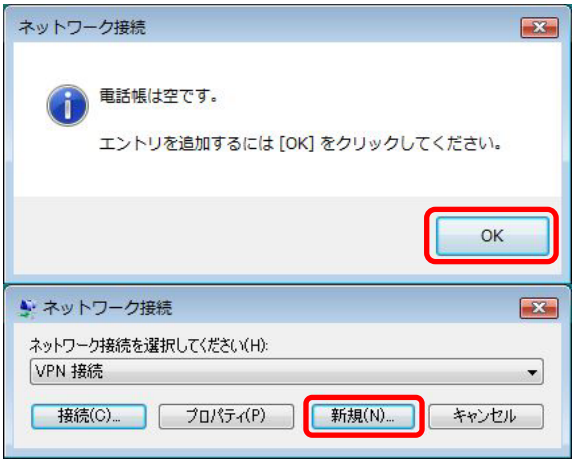
・本章は Windows 10 の画面で説明します。他のバージョンで画面が異なるときは適宜読み替えてください。

リモートアクセス設定ウィザードを実行する（パソコン版）

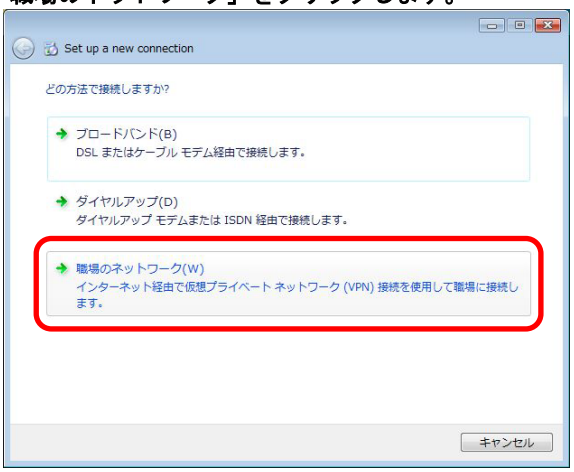
1. **スタートメニューの検索ボックスに「rasphone.exe」と入力し、エンターキーを押します。**



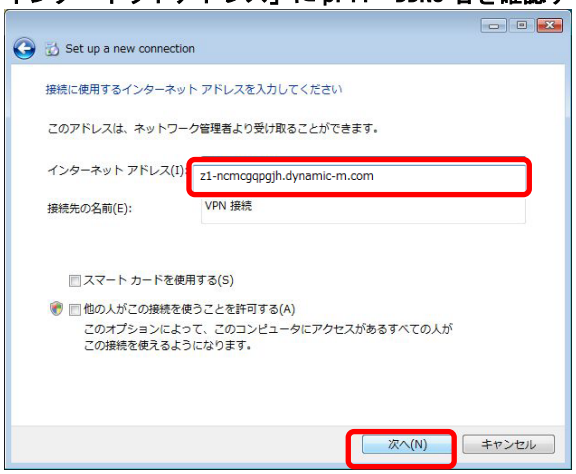
2. **以下のいずれかの画面が表示されます。**



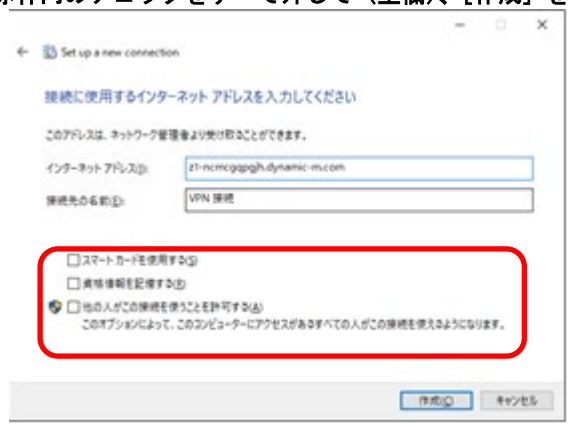
3. 「職場のネットワーク」をクリックします。



4. 「インターネットアドレス」に p.11「DDNS 名を確認する」で確認した「Hostname」を入力し、[次へ] をクリックします。



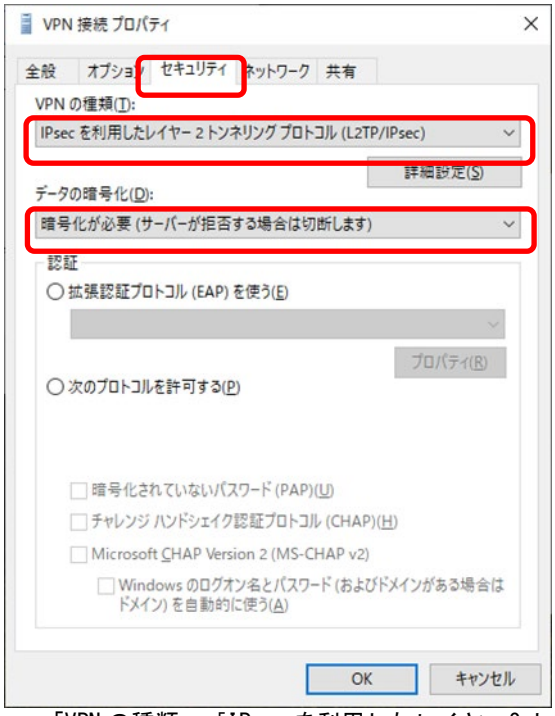
5. 赤枠内のチェックをすべて外して（空欄）、[作成] をクリックします。



6. [プロパティ] をクリックします。

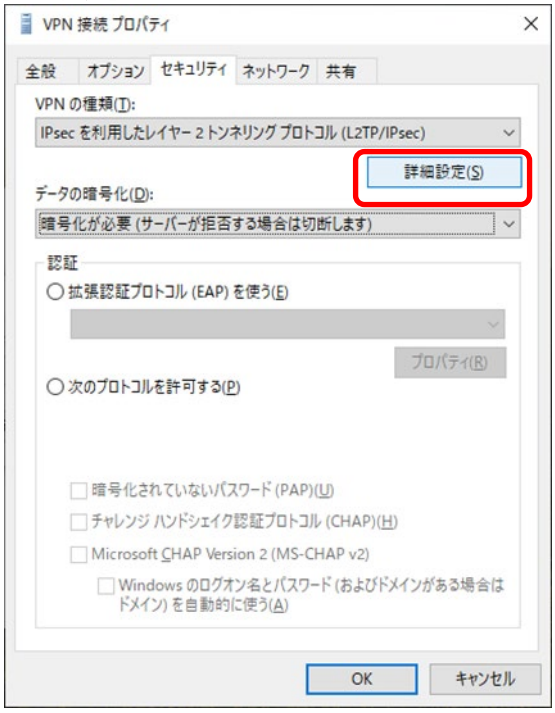
プロパティを設定する（パソコン版）

1. 「導入準備シート」にしたがって、プロパティを以下の通りに設定します。
2. [セキュリティ] タブをクリックし、以下のように設定します。

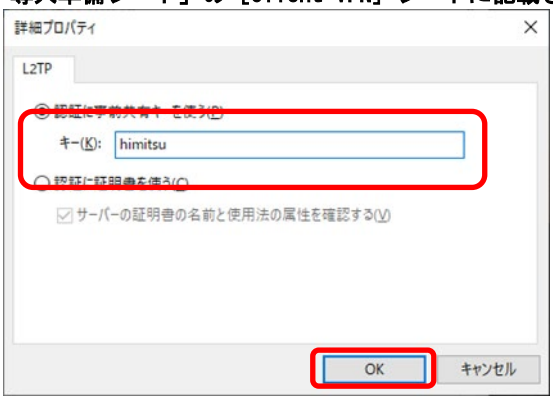


- 「VPN の種類」:[IPsec を利用したレイヤー2 トンネリングプロトコル（L2TP/IPSec)] を選択します。
- 「データの暗号化」:[暗号化が必要（サーバーが拒否する場合は切断します)] を選択します。

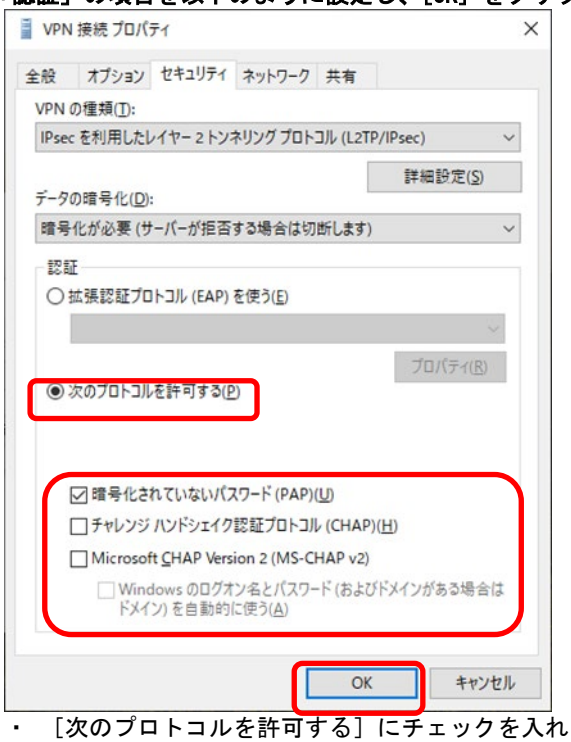
3. **[詳細設定] をクリックします。**



4. **「導入準備シート」の［Client VPN］シートに記載されている「事前共有鍵」を入力して、［OK］をクリックします。**



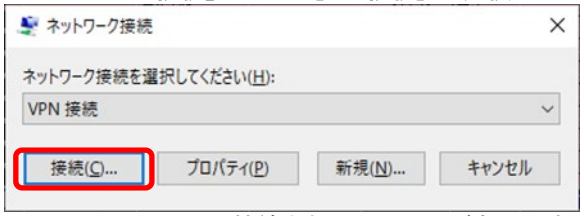
5. **「認証」の項目を以下のように設定し、［OK］をクリックします。**



・ ［次のプロトコルを許可する］にチェックを入れます。
・ ［暗号化されていないパスワード］だけにチェックを入れます。

接続する（パソコン版）

1. **「ネットワーク接続」画面で［VPN 接続］が選択されていることを確認して、［接続］をクリックします。**



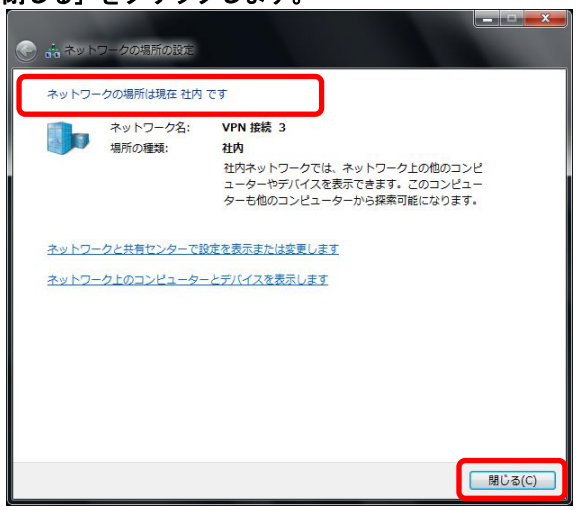
・ インターネットに接続されている必要があります。

2. **以下のとおりに項目を設定し、［接続］をクリックします。**

- 「ユーザー名」　：　「導入準備シート」の［users］シートに記載されている「電子メールアドレス」を入力します。
- 「パスワード」　：　設定したパスワードを入力します。
- 「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」　：　チェックを外します。

3. **以下の画面が表示されたときは、［社内ネットワーク］をクリックします。**

4. ［閉じる］をクリックします。



切断する（パソコン版）

1. タスクトレイのネットワークアイコン（または）をクリックします。

・Windows 10

アイコン(または、) をクリック後、表示されたメニューから、「目的とする VPN 接続先」をクリックし、続けて表示された画面で「目的とする VPN 接続先」をクリック後、「**切断**」をクリックします。

・Windows 8.1

アイコン(または、) をクリック後、「**接続済み**」をクリックし「**切断**」をクリックします。

動作を確認する（パソコン版）

補足

・本章は以下の各 OS の手順を参照し、VPN 接続画面を説明します。他のバージョンで画面が異なるときは適宜読み替えてください。

VPN 接続画面を起動する（パソコン版）

1. 各 OS の手順を参照し、VPN 接続画面を起動します。

・Windows 10

タスクトレイのネットワークアイコン( または、 ) をクリック後、表示されたメニューから、「目的とする VPN 接続先」をクリックし、続けて表示された画面で「目的とする VPN 接続先」をクリック後、「**接続**」をクリックします

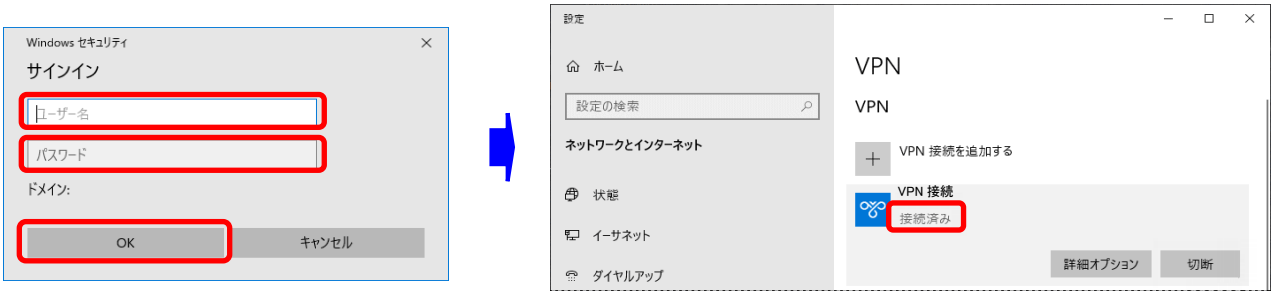
・Windows 8.1

タスクトレイのネットワークアイコン( または、 ) をクリック後、表示されたチャームから、「目的とする VPN 接続先」をクリックして表示を展開し、「**接続**」をクリック)します。

2. **VPN 接続に必要な認証情報を入力し、正常に接続されることを確認します。**

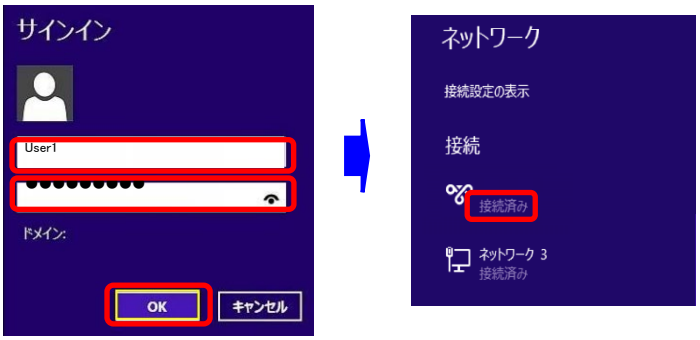
・Windows 10

VPN 接続に必要な認証情報を入力後「**OK**」をクリックし、正常に接続されたことを確認します。

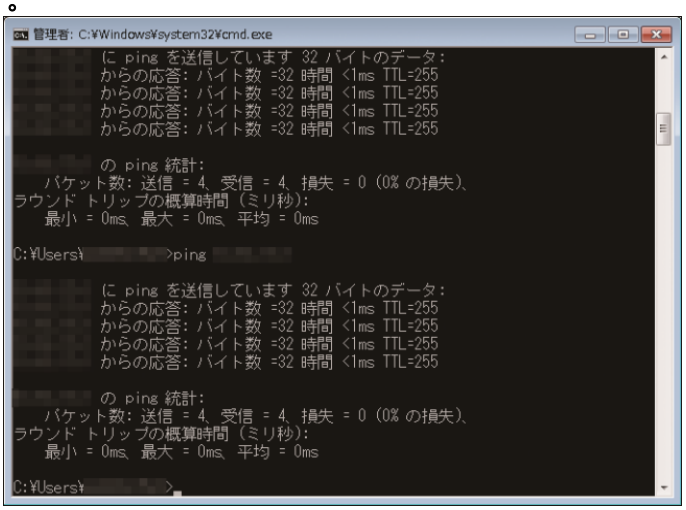


・Windows 8.1

VPN 接続に必要な認証情報を入力後「**OK**」をクリックし、正常に接続されたことを確認します。



3. コマンドプロンプトを開き、接続先機器の LAN 側の IP アドレス宛に ping コマンドを実行して、応答があることを確認します。



補足

・接続先機器の LAN 側の IP アドレスは、「導入準備シート」の[Addressing & VLANs]の IP アドレス設定に記載されています。

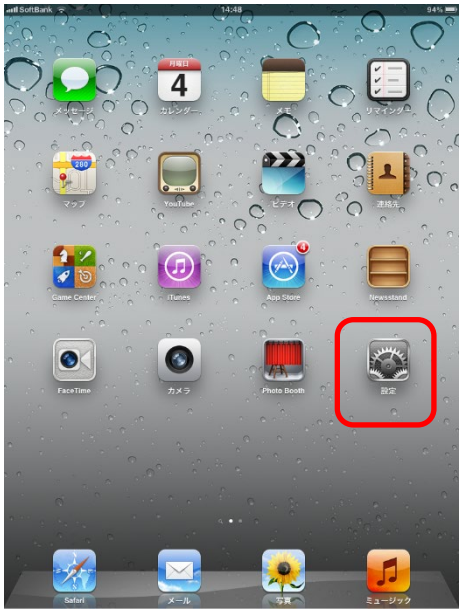
VPN クライアント(L2TP/IPsec)を設定する（iOS 版）

補足

・本章は iPad（iOS 7.0.3）の画面で説明します。他の機種や OS バージョンで画面が異なるときは適宜読み替えてください。

L2TP を設定する（iOS 版）

1. **接続先機器の設定および設置が完了していることを確認します。**
2. **［設定］をタップします。**



3. **［一般］をタップし、［VPN］をタップします。**

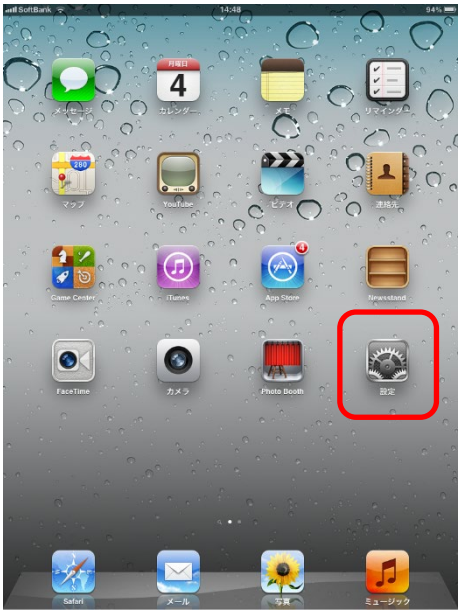
4. **［VPN 構成を追加］をタップします。**

5. **「L2TP」設定の各項目を入力し、［保存］をタップします。**

・説明　：　任意の内容を入力します。
・サーバ　：　p.11「DDNS 名を確認する」で確認した接続先機器の「Hostname」を入力します。
・アカウント　：　「導入準備シート」の［user］シートに記載されている電子メールアドレスを入力します。
・RSA SecureID　：　無効（OFF）に設定します。
・パスワード　：　入力しません。
・シークレット　：　「導入準備シート」の［Client VPN］シートに記載されている事前共有鍵を入力します。
・すべての信号を送信　：　有効（ON）に設定します。
・プロキシ　：　［オフ］を選択します。

接続と切断を確認する（iOS 版）

1. **［設定］をタップします。**



2. 「VPN」を［オン］にします。

3. 「パスワード」に設定済みのパスワードを入力し、[完了] をタップします。

4. 「一般」の「VPN」が [接続中] と表示されることを確認します。

5. 切断するときは、「設定」の「VPN」を [オフ] にします。

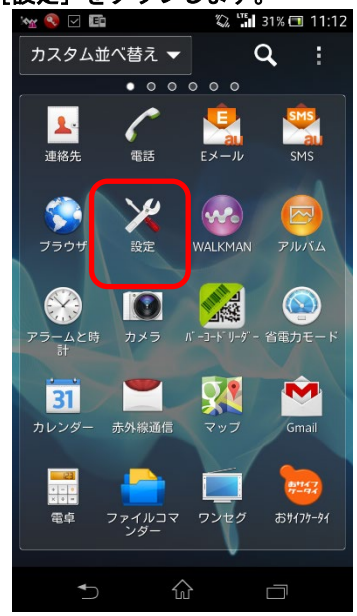
VPN クライアント(L2TP/IPsec)を設定する（Android 版）

補足

・本章は DoCoMo SO-03D の Android4.0 の画面で説明します。他の機種や OS バージョンで画面が異なるときは適宜読み替えてください。
・Android12 以降、L2TP/IPsec の接続設定ができないため、サポート対象外となります。

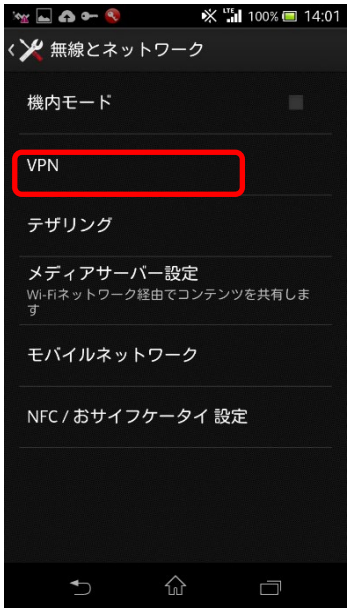
L2TP を設定する（Android 版）

1. **接続先機器の設定および設置が完了していることを確認します。**
2. **［設定］をタップします。**

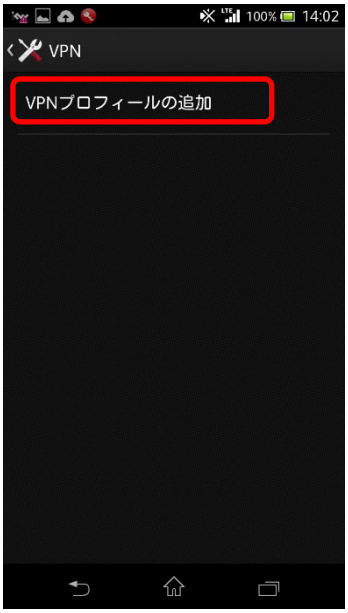


3. **［その他の設定］をタップします。**

4. **［VPN］をタップします。**



5. [VPN プロフィールの追加] をタップします。



6. **各項目を入力し、[保存] をタップします。**

・名前　　：任意の内容を入力します。
・タイプ　　：[L2TP/IPSec PSK] を選択します。
・サーバーアドレス　　：p.11「DDNS 名を確認する」で確認した接続先機器の「Hostname」を入力します。
・IPSec 事前共有鍵　　：「導入準備シート」の [Client VPN] シートに記載されている事前共有鍵を入力します。

7. **VPN プロフィールが追加されたことを確認します。**

接続を確認する（Android 版）

1. **接続する VPN プロフィールをタップします。**

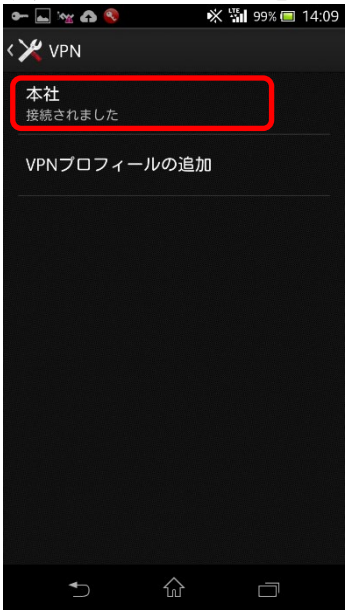
2. **各項目を入力し、[接続] をタップします。**

・ユーザー名　:「導入準備シート」の［user］シートに記載されている電子メールアドレスを入力します。
・パスワード　：設定済みのパスワードを入力します。
・「アカウント情報を保存する」: チェックを外します。

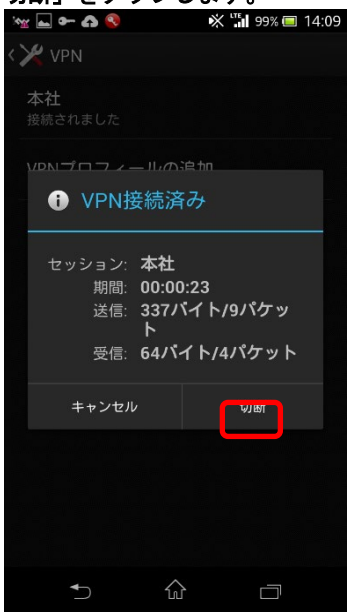
3. 「接続されました」と表示されることを確認します。

切断を確認する（Android 版）

1. 切断する VPN プロフィールをタップします。



2. 「切断」をタップします。


99% 14:09
VPN
本社
接続されました
VPN接続済み
セッション: 本社
期間: 00:00:23
送信: 337バイト/9パケット
受信: 64バイト/4パケット
キャンセル
切断

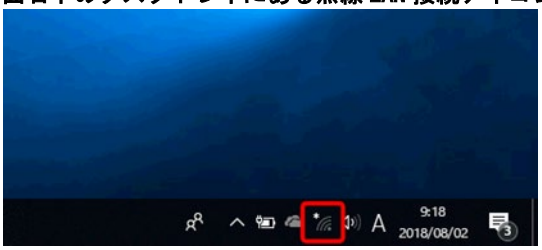
無線プロファイルを設定する（パソコン版）

補足

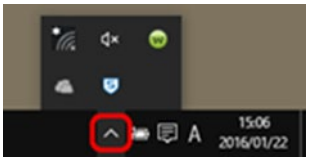
- 本章は Windows 10 の画面で説明します。他のバージョンで画面が異なるときは適宜読み替えてください。
- 無線 LAN アダプターによっては以下の手順通りに設定できません。そのようなアダプターは本サービスのサポート対象外となります。

プロファイルを設定する（パソコン版）

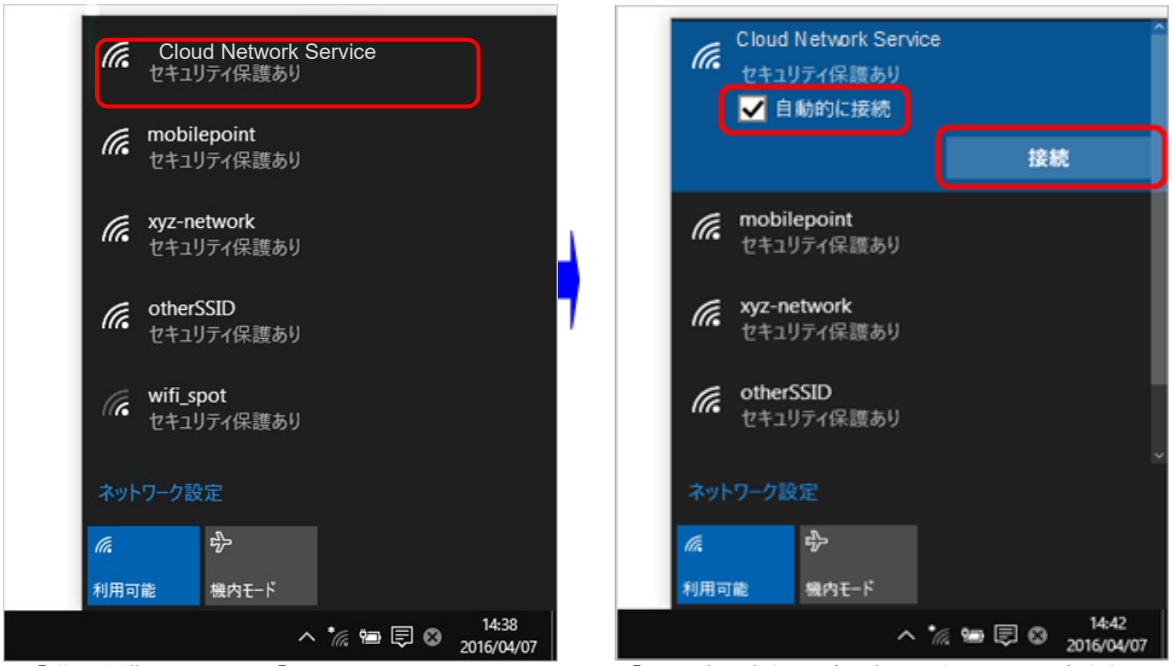
1. **パソコンに LAN ケーブルが接続されていないことを確認します。**
2. **パソコンに管理者権限を持つユーザーでログインします。**
3. **画面右下のタスクトレイにある無線 LAN 接続アイコンをクリックします。**



- タスクトレイにアイコンが表示されていないときは、三角形のアイコンをクリックして無線 LAN 接続アイコンを表示します。

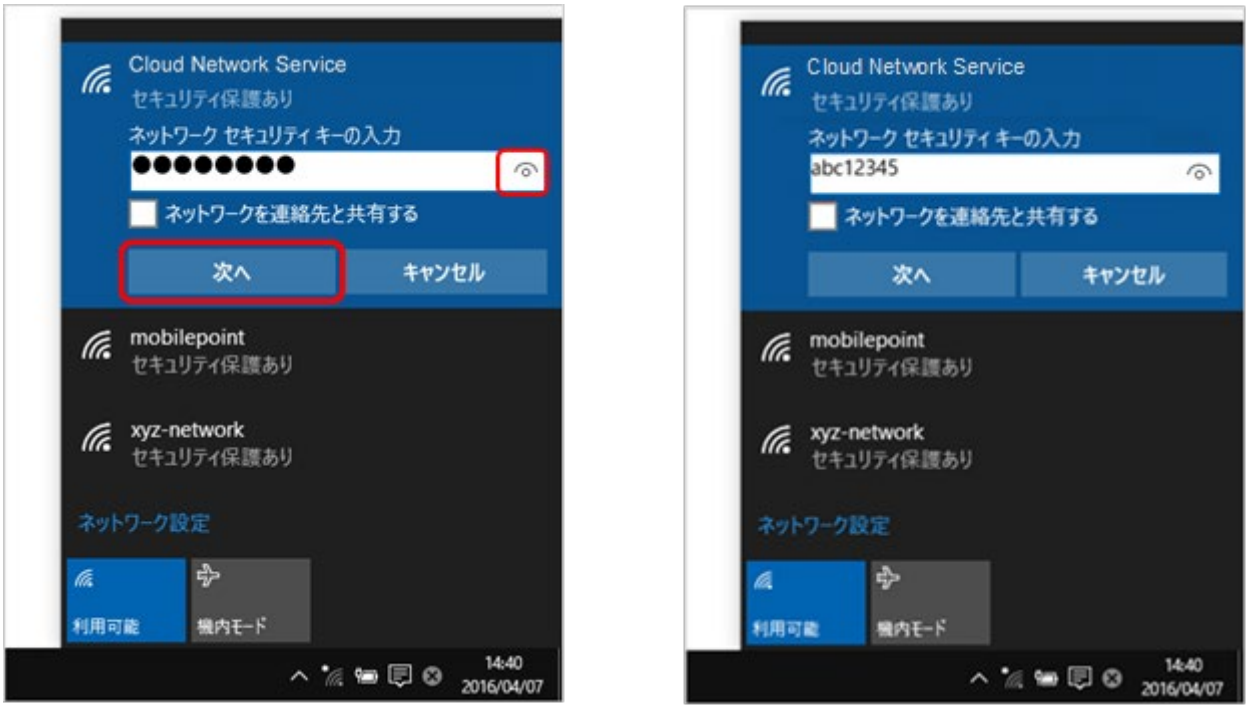


4. **接続するアクセスポイントの SSID を選択し、[接続] ボタンをクリックします。**

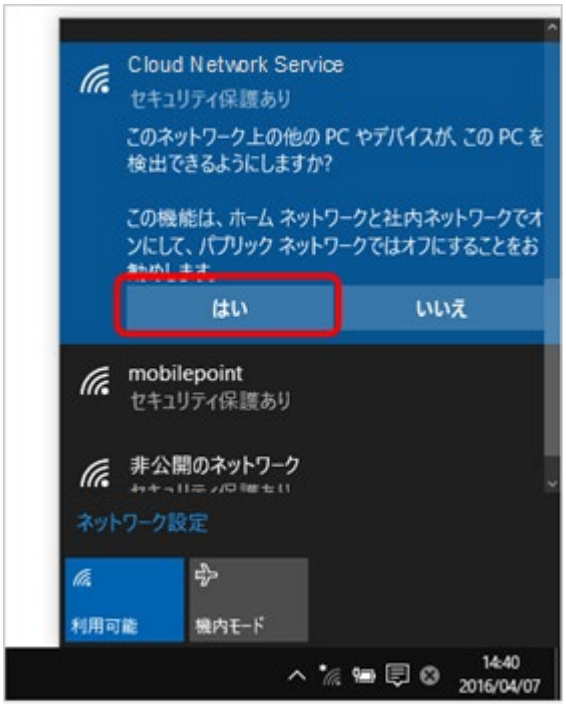


・「導入準備シート」の「Wireless settings シート」で「SSID 表示有無」が［表示しない］に設定されているときは、SSID が一覧に表示されません。p. 32「手動による設定（パソコン版）」の手順を参考に設定してください。

5. **「導入準備シート」の「Wireless settings シート」の「プリシェアードキー」欄に記載された文字列を入力し、[OK] をクリックします。（ を長押しするとパスワードが表示されます）**

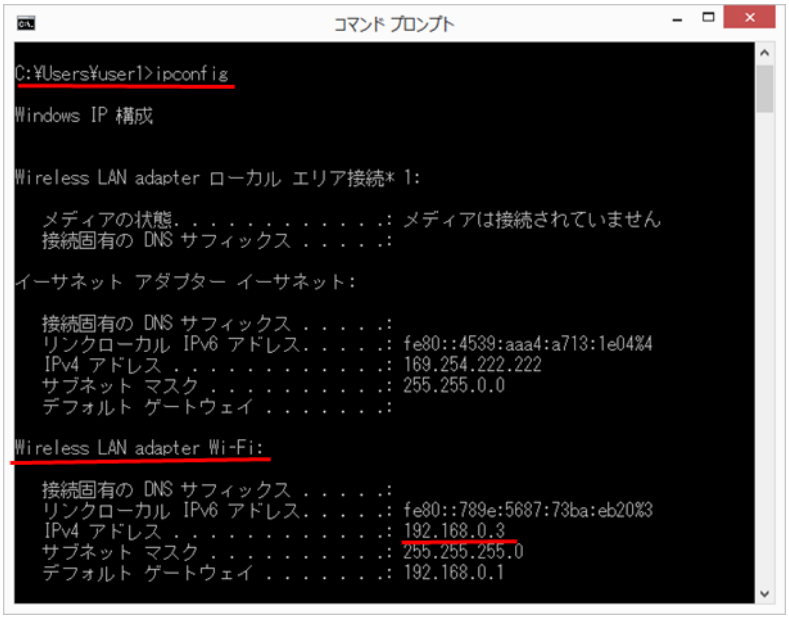


6. **以下の画面が表示されたときは、[はい] をクリックします。**



・※Windows 10 のバージョンによっては表示されない、表示が違うものもあります。

7. **コマンドプロンプトを起動し「ipconfig」と入力後、エンターキーを押します。**
   無線 LAN アダプターの項目に正しい IP アドレスが表示されることを確認します。



補足

・ 設定が必要な台数分、上記の手順を繰り返し実施します。
・ 手順 7 において、ネットワーク内に複数の LAN アダプターが存在するときは、無線 LAN アダプターの情報だけでなく、他の有線 LAN のアダプターなどの情報もあわせて表示されます。目的の無線 LAN アダプターの情報を確認してください。

動作を確認する（パソコン版）

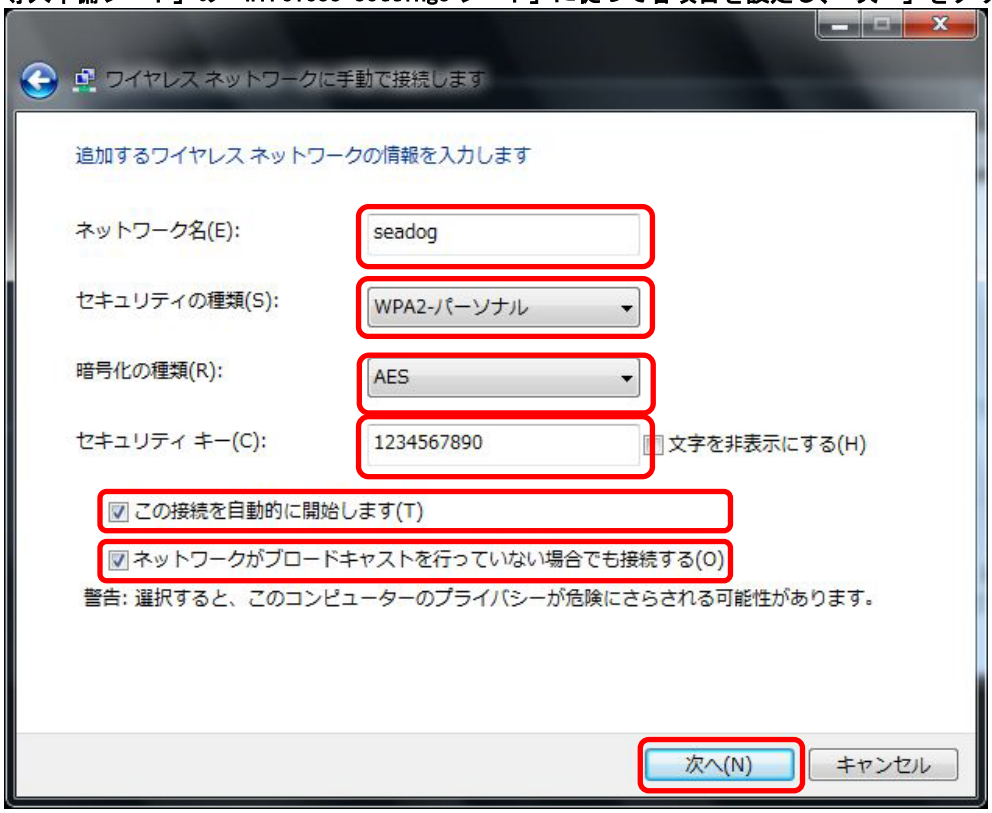
1. **PC に LAN ケーブルが接続されていないことを確認します。**
   ・ DHCP サーバーがない環境のときは、無線 LAN アダプターに適切な IP アドレスを設定します。
2. **ブラウザを起動し、アドレス欄に「http://ricoh.co.jp/」と入力してリコーのホームページが表示されることを確認します。**

手動による設定（パソコン版）

1. **［スタート］→［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］を開き［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。**

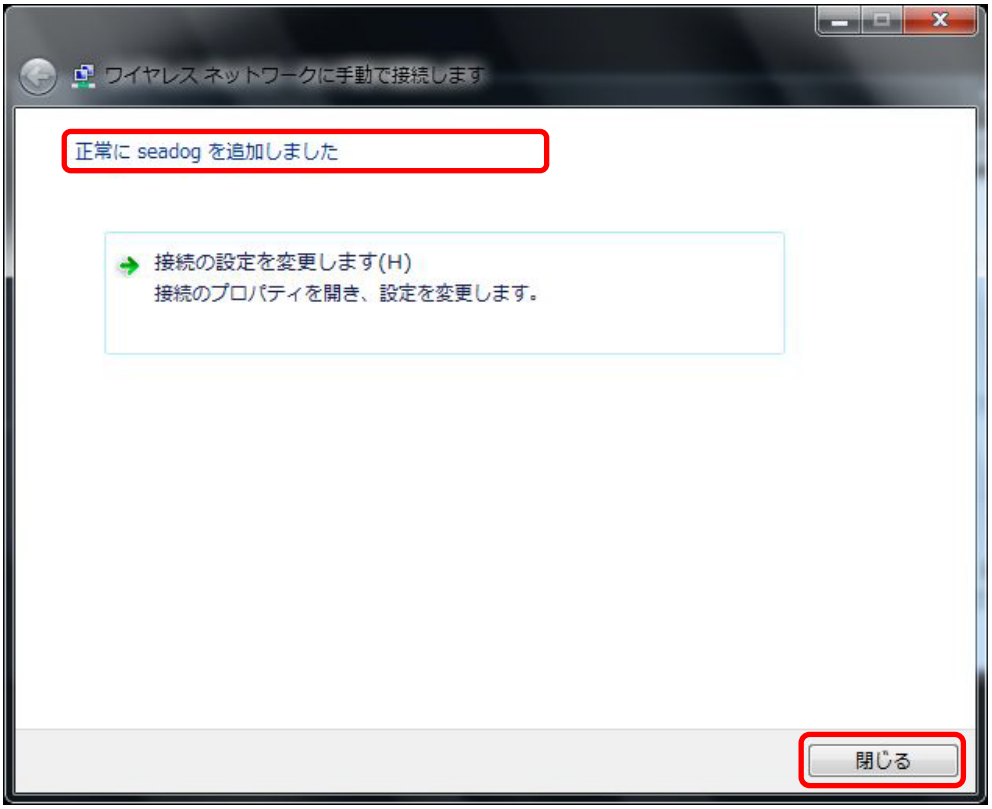
2. **［ワイヤレスネットワークに手動で接続します］を選択し、［次へ］をクリックします。**

3. **「導入準備シート」の「Wireless settings シート」に従って各項目を設定し、「次へ」をクリックします。**



・ネットワーク名　　：SSID 名を入力します。
・セキュリティの種類　　：暗号化方式に従って入力します。
・暗号化の種類　　：暗号化方式に従って入力します。
・セキュリティ　キー　　：プリシェアードキーを入力します。
・この接続を自動的に開始します　　：チェックを入れます。
・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：チェックを入れます。

4. **正常にネットワークが追加されたことを示すメッセージを確認し、［閉じる］をクリックします。**



5. 正常に Wi-Fi ネットワーク接続がされたことを確認します。

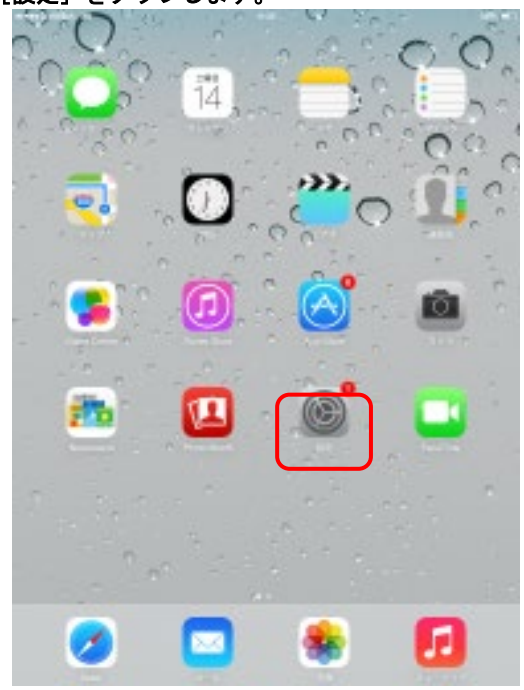
無線プロファイルを設定する（iOS 版）

補足

・本章は iPad（iOS 7.0.3）の画面で説明します。他の機種や OS バージョンで画面が異なるときは適宜読み替えてください。

プロファイルを設定する（iOS 版）

1. **接続先機器の設定および設置が完了していることを確認します。**
2. **［設定］をタップします。**

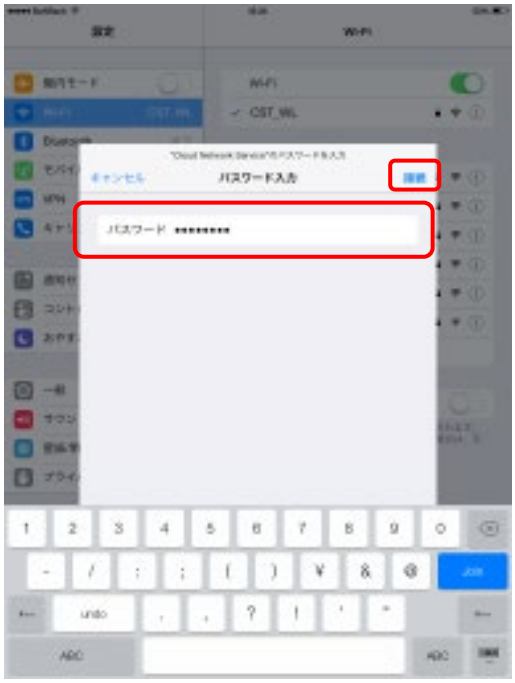


3. [Wi-Fi] をタップします。

4. 接続するアクセスポイントの SSID をタップします。

・「導入準備シート」の「Wireless settings シート」で「SSID 表示有無」が［表示しない］に設定されているときは、SSID が一覧に表示されません。接続するアクセスポイントを手動で追加し、設定してください。

5. 「導入準備シート」の「Wireless settings シート」の「プリシェアードキー」欄に記載された文字列を入力し、[接続] をタップします。



6. **接続した SSID の左にチェックがつき、画面上部に Wi-Fi アイコンが表示されていることを確認します。**

補足

・設定が必要な台数分、上記の手順を繰り返し実施します。

動作を確認する（iOS 版）

1. **ブラウザを起動し、アドレス欄に「http://ricoh.co.jp/」と入力してリコーのホームページが表示されることを確認します。**

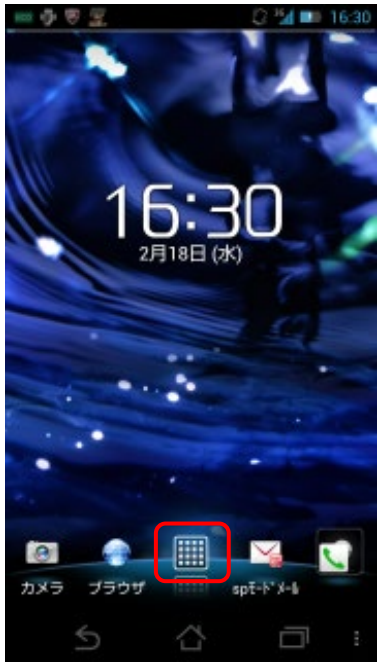
無線プロファイルを設定する（Android 版）

補足

・本章は DoCoMo P-06D の Android4.1 の画面で説明します。他の機種や OS バージョンで画面が異なるときは適宜読み替えてください。

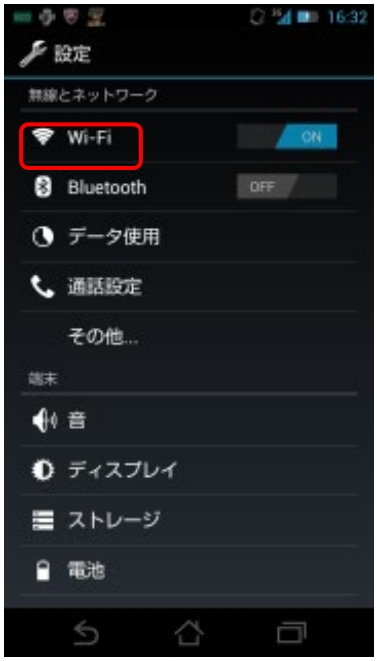
プロファイルを設定する（Android 版）

1. **接続先機器の設定および設置が完了していることを確認します。**
2. **アプリ一覧アイコンをタップします。**

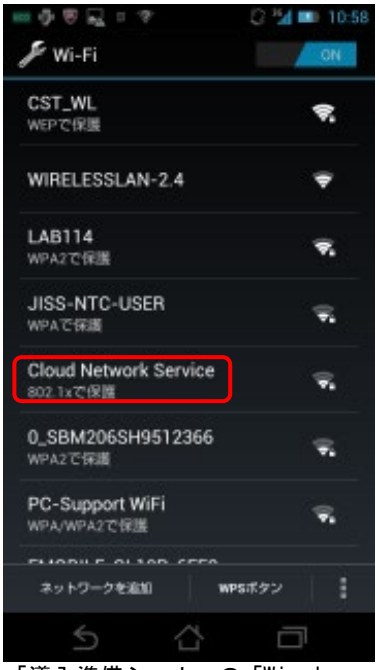


3. **[設定] をタップします。**

4. **[Wi-Fi] をタップし、Wi-Fi を ON にします。**



5. **接続するアクセスポイントの SSID をタップします。**



・「導入準備シート」の「Wireless settings シート」で「SSID 表示有無」が［表示しない］に設定されているときは、SSID が一覧に表示されません。接続するアクセスポイントを手動で追加し、設定してください。

6. 「パスワード」欄に、「導入準備シート」の「Wireless settings シート」の「プリシェアードキー」欄に記載された文字列を入力し、[接続] をタップします。

7. 目的のアクセスポイントが「接続済み」と表示されることを確認します。

補足

・設定が必要な台数分、上記の手順を繰り返し実施します。

動作を確認する（Android 版）

1. ブラウザを起動し、アドレス欄に「http://ricoh.co.jp/」と入力してリコーのホームページが表示されることを確認します。

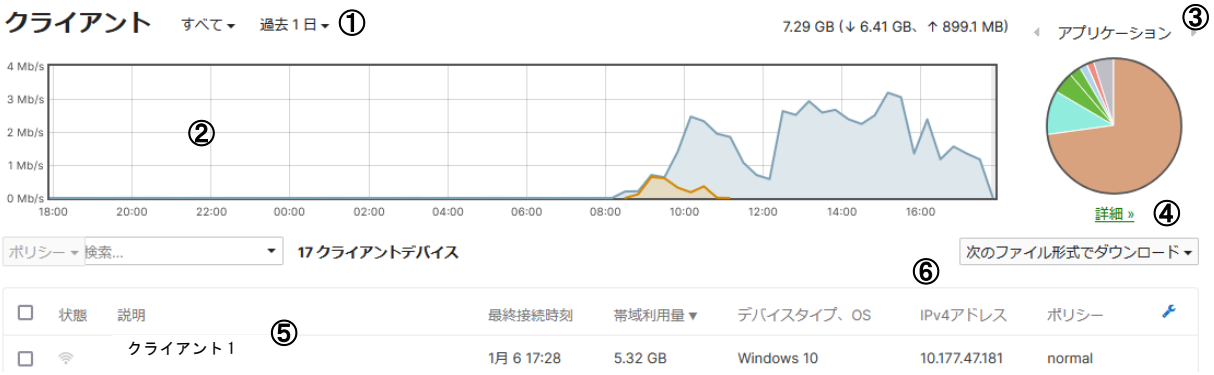
無線ネットワーク全体の状況確認

クライアント接続状況

無線ネットワークに接続しているクライアントの接続状況を確認できます。

1. **画面左のメニューで［ネットワーク全体］にマウスオーバーし、［クライアント］をクリックします。**

2. **以下の画面が表示され、クライアントの接続状況を確認できます。**

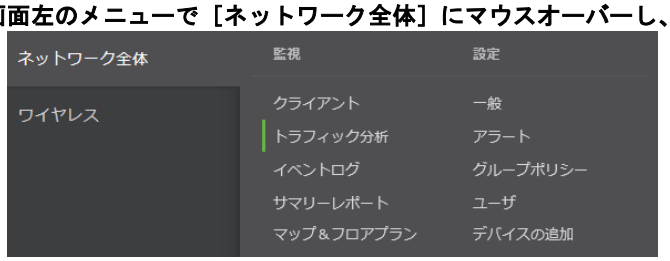


① 表示条件を指定 ［過去 1 日／2 時間／1 週間／1 か月］
② 時間帯別のトラフィック状況を表示
③ アプリケーションの使用状況を表示。 ▷ をクリックすると「ポート」、「HTTP コンテンツ」が選択可能
④ 「詳細」をクリックすることで上記③で選択した内容が確認できます。
⑤ クライアント毎の最終接続時間、帯域使用量、デバイスタイプなどを表示
⑥ 上記⑤の表示内容をファイル形式でダウンロード

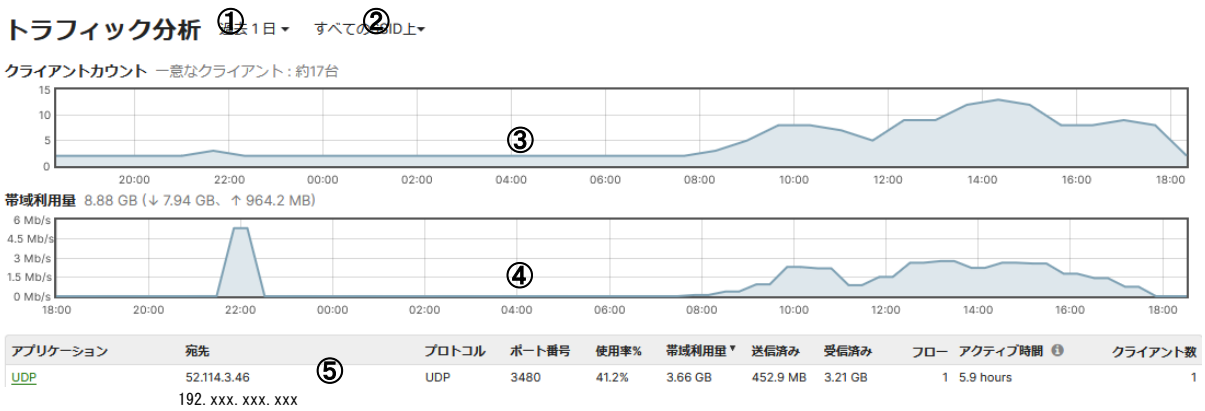
トラフィック分析

トラフィック状況を確認できます。

1. **画面左のメニューで［ネットワーク全体］にマウスオーバーし、［トラフィック分析］をクリックします。**



2. **以下の画面が表示され、トラフィック分析状況を確認できます。**



① 表示条件を指定 ［過去 1 日／2 時間／1 週間／1 か月］
② SSID を指定[すべての SSID、SSID 毎]
③ 時間帯別のクライアントの接続状況
④ 帯域利用量
⑤ アプリケーション毎の使用率、帯域帯域使用量などを表示

イベントログ

イベントログを確認できます。

1. **画面左のメニューで［ネットワーク全体］にマウスオーバーし、［イベントログ］をクリックします。**

2. **以下の画面が表示され、イベントログを確認できます。**

① イベントログの抽出条件を指定
② 上記①で抽出したイベントログをファイル形式でダウンロード
※上記③で表示しているイベントログのみのダウンロードとなります。複数ページに跨る場合はページ毎に ダウンロードする必要があります。
③ イベントログ内容を表示

サマリーレポート

サマリーレポートを確認できます。

1. **画面左のメニューで［ネットワーク全体］にマウスオーバーし、［イベントログ］をクリックします。**

2.　以下の画面が表示され、サマリーレポートを確認できます。

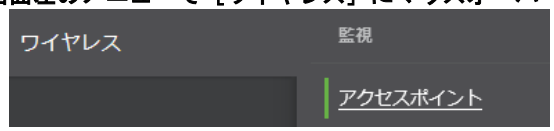
① ネットワーク名を指定
② SSID を指定
③ 上位の結果を表示[１／５／１０／２０／５０]
④ 表示内容をファイル形式でダウンロード
⑤ 以下のサマリーレポートが表示
　使用状況統計
　利用量の時間遷移
　クライアント統計
　利用量上位のクライアント

　※上記図にはありませんが以下内容も確認できます。
　データ転送量の多いデバイス
　デバイスモデル別使用量順位
　クライアント統計
　利用量上位のクライアントデバイスメーカー
　利用量上位の OS
　上位アプリケーションカテゴリ
　利用量上位のアプリケーション

アクセスポイントの状況確認

アクセスポイントの状況確認

1. **画面左のメニューで［ワイヤレス］にマウスオーバーし、［アクセスポイント］をクリックします。**



2. **以下の画面が表示され、アクセスポイントのオンライン数、オフライン数とアクセスポイント毎のコネクティビティを確認できます。**

3. **アクセスポイント毎のコネクティビティは上記①をクリックしすることにより以下内容を確認できます。**
   現在のトラフィック数
   現在のチャネル利用率
   デバイスの履歴データ

Meraki 認証を使用する

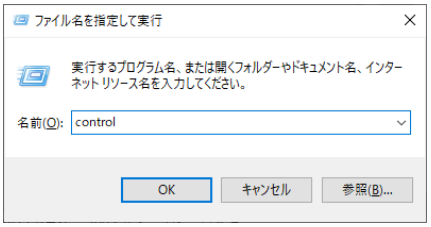
クライアントを設定する（Windows 版）

補足

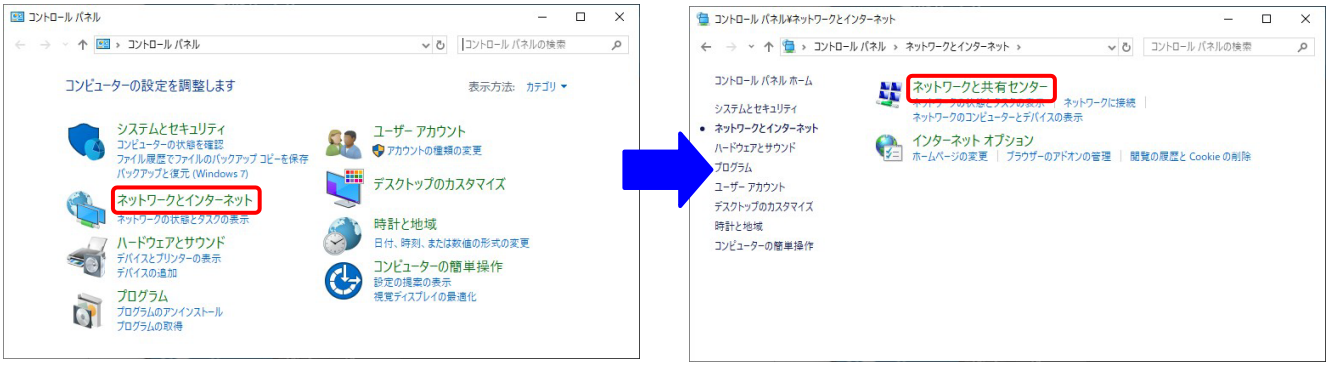
※Meraki 認証＝WPA2 Enterprise with Meraki Authentication

※暗号化方式で「WPA2 Enterprise with Meraki Authentication」が選択されている場合は、以下の手順を参考に設定をしてください。
※OS のバージョンにより表示される画面やメッセージが異なる場合があります。

1. [Windows]キー＋[R]キー押下し、ファイル名を指定して実行画面を表示させ、「**control**」と入力し、[OK]をクリックします。



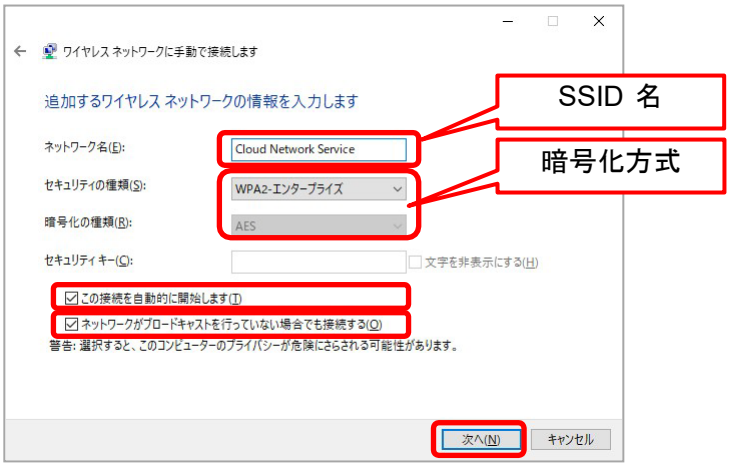
2. 「ネットワークとインターネット」をクリックし、「ネットワークと共有センター」をクリックします。



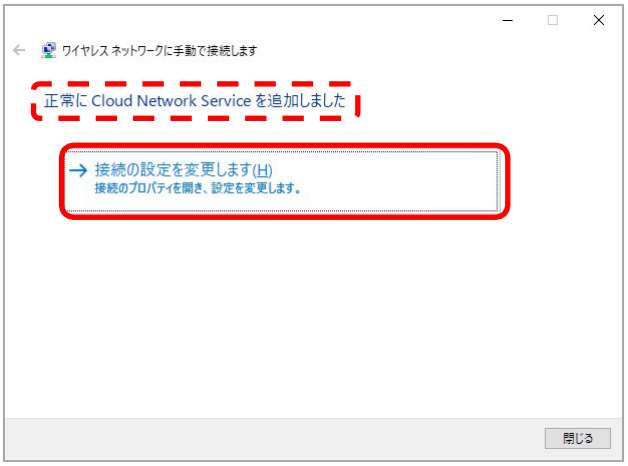
3. 「新しい接続またはネットワークのセットアップ」をクリックします。

4. 「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」をクリックします。

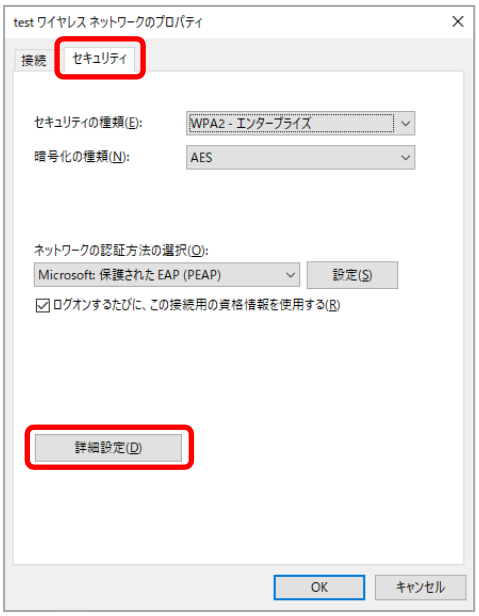
5. SSID 名、暗号化方式（WPA2 エンタープライズ）を入力し、「この接続を自動的に開始します」と「ネットワークがブロードキャストを行っていない場合でも接続する」の両方にチェックし、「次へ」をクリックします



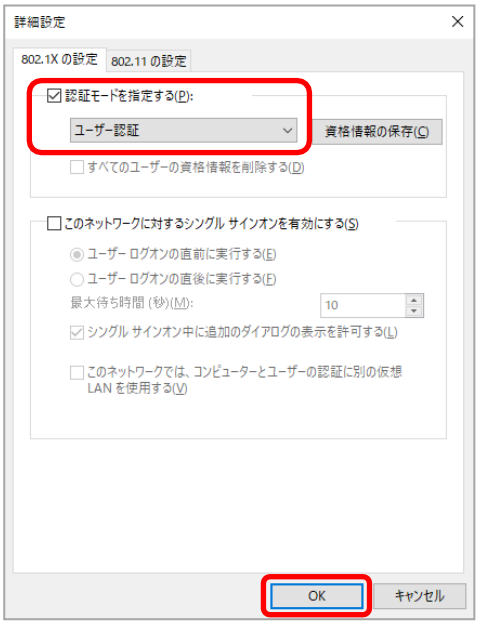
6. 「正常に xxx を追加しました」と表示されたことを確認したら、続けて「接続の設定を変更します」をクリックします。



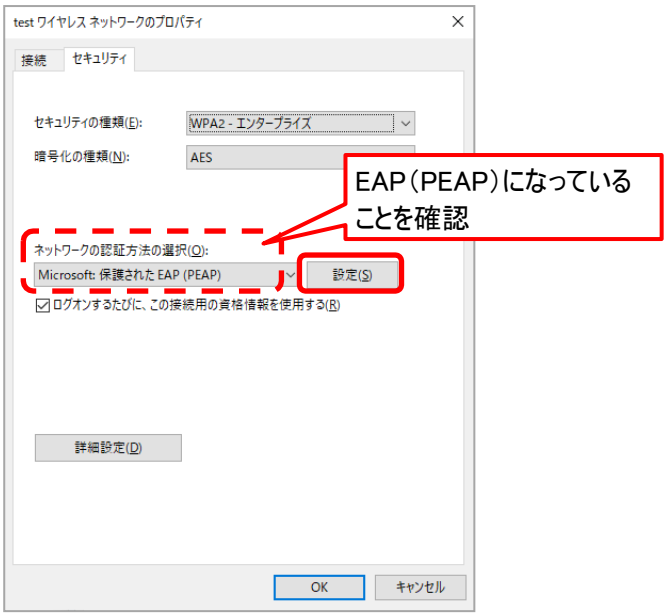
7. 「**セキュリティ**」タブを表示し、「**詳細設定**」をクリックします。



8. 「**802.1X　の設定**」タブで、「**認証モードを指定する**」にチェックを入れ、ドロップダウンから「**ユーザー認証**」を選択します。続けて「**OK**」をクリックします。

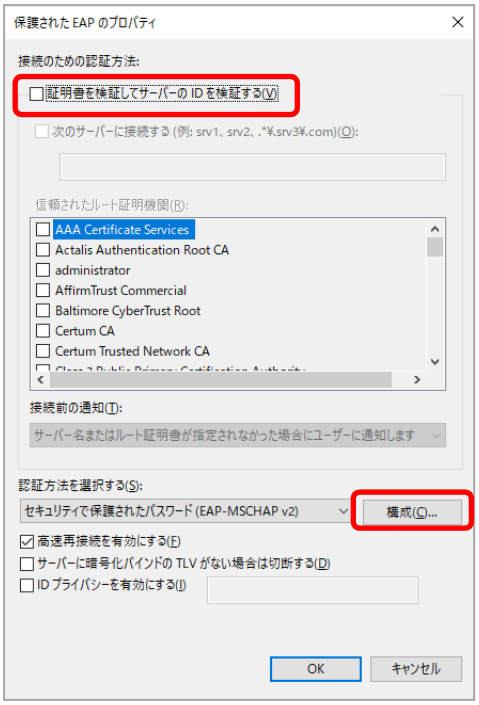


9. 1 つ前のウィンドウに戻ったら、「ネットワーク認証方法の選択」が「**EAP（PEAP）**」になっていることを確認し、「**設定**」をクリックします。

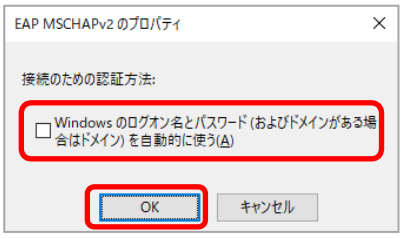


10. 「証明書を検証してサーバーの ID を検証する」のチェックを外し、「構成」をクリックします。

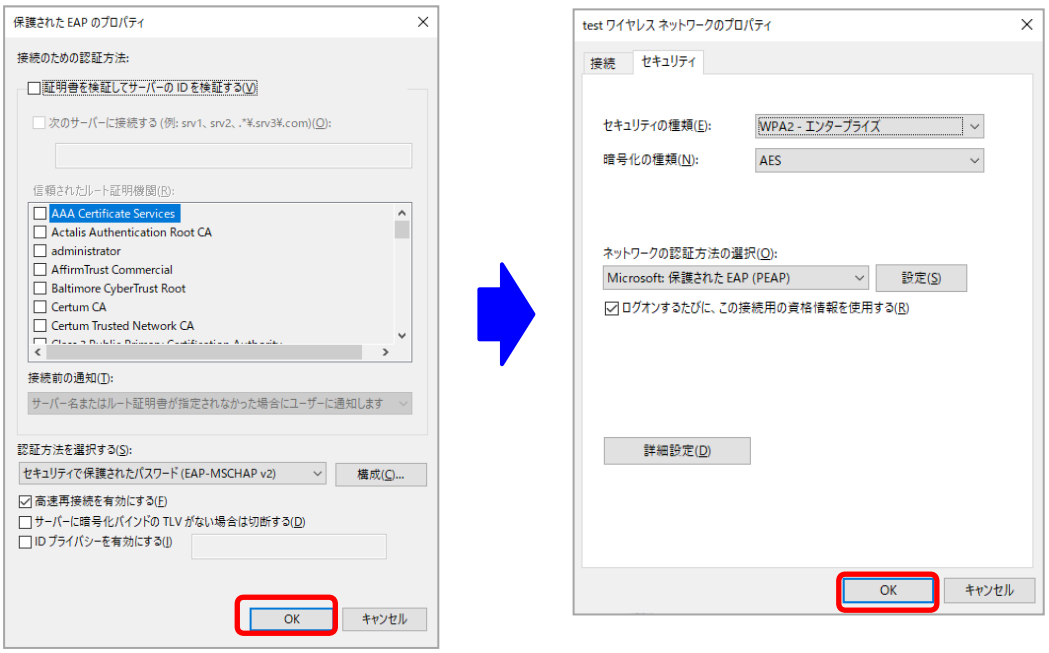
補足：サーバー証明書を検証する場合は、「Go Daddy Class 2　証明機関」と、「信頼されたルート証明機関」リストで http://valicert.com がチェックされていることを確認してください。



11. 「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」のチェックを外し、「OK」をクリックします。



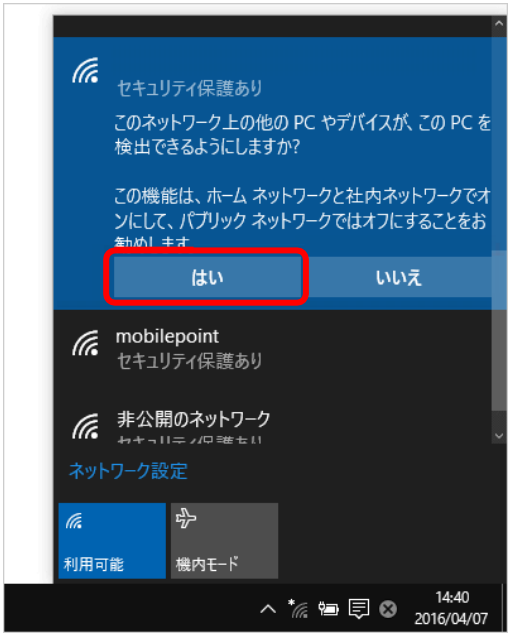
12. 「**OK**」を 2 回クリックしてウィンドウを閉じます。



13. 「**閉じる**」をクリックして、設定ウィザードを閉じます。

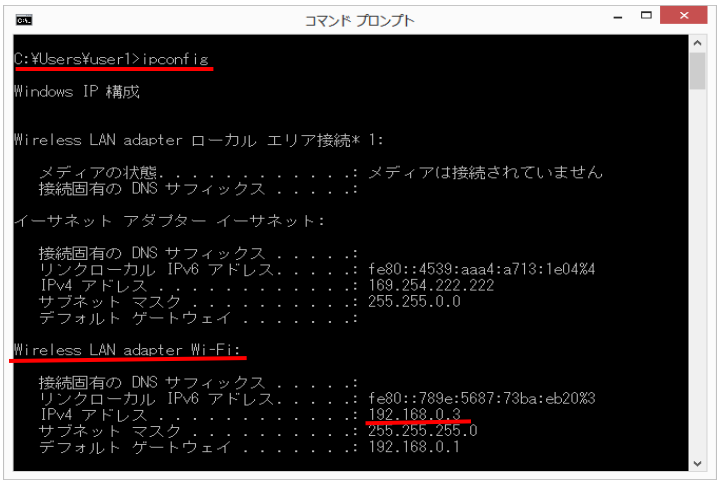
14. 画面右下の通知領域にある「**無線アイコン**」をクリックし、先ほど設定した「**SSID**」をクリックします。
「自動的に接続」にチェックが入っている状態で、「**接続**」をクリックします。（下左図）
サインイン画面が表示されたら、Meraki　認証用の「**ユーザ名**」と「**パスワード**」を入力し「OK」をクリックします。（下右図）

15. 以下の画面が表示された場合には、「**はい**」をクリックします。
※Windows 10 のバージョンによっては表示されない、表示が違うものもあります。正常に　WiFi　ネットワーク接続がされたことを確認します。



16. 正常に WiFi ネットワーク接続がされたことを確認します。

17. コマンドプロンプトを起動し「**ipconfig**」と入力後、[Enter]キーを押し、無線 LAN アダプタに意図した IP アドレスが割り当てされていることを確認します。



18. [対象のお客様 PC]に「**LAN ケーブル**」が接続されていないことを確認します。
※DHCP サーバーが無い環境の場合は、無線 LAN アダプタに適切な IP アドレスを設定します。

19. インターネットエクスプローラーを立ち上げ、アドレス欄に「**https://ricoh.co.jp/**」と入力してリコーのホームページが閲覧できることを確認します。

以上で、無線クライアント の動作確認は終了です。

クライアントを設定する（iOS 版）

補足

※Meraki 認証＝WPA2 Enterprise with Meraki Authentication

※暗号化方式で「WPA2 Enterprise with Meraki Authentication」が選択されている場合は、以下の手順を参考に設定をしてください。

1. ホーム画面で[設定] → ［Wi-Fi ］→ SSID の一覧画面で「**その他**」をタップします。

2. SSID、暗号化方式（WPA2 エンタープライズ）、Meraki 認証用のユーザ名とパスワードを入力し、「**接続**」をタップします。

3. 証明書画面が表示されます。[**信頼**] をタップします。続けて目的の SSID の左側に「**チェックマーク**」が表示(接続)されたことを確認します。

4. ブラウザを立ち上げ、アドレス欄に「**https://ricoh.co.jp/**」と入力してリコーのホームページが閲覧できることを確認します。

設定と確認は以上です。

クライアントを設定する（Android 版）

補足

※Meraki 認証＝WPA2 Enterprise with Meraki Authentication

※暗号化方式で「WPA2 Enterprise with Meraki Authentication」が選択されている場合は、以下の手順を参考に設定をしてください。
※設定画面や表示されるメニュー名は Android のバージョンによって変わることがあります。

1. ホーム画面で[アプリー覧]→[設定]→[Wi-Fi]の順にタップします。

2. 「**ネットワークを追加**」をタップ後、以下の内容に従って各項目を入力し、「**保存**」をクリックします。

SSID 名 802.1x
EAP※1PEAP
MSCHAPV2
システム証明書を使用※2
meraki.com※3

Meraki 認証用の
「ユーザ名」と「パスワード」

※1:「802.1x EAP」が無い場合は、「WPA/WPA2/WPA3-Enterprise」を選択
※2:Android 10　の場合は、「証明書なし」、Android 11 QPR1 以降は、「システム証明書を使用」を選択
※3:※2　　で「証明書なし」を選択した場合は、ドメイン入力欄は表示されません。「システム証明書を使用」を選択した場合は、「meraki.com」と入力

3. 目的の SSID に「**接続済み**」と表示されたことを確認します。

4. ブラウザを立ち上げ、アドレス欄に「**https://ricoh.co.jp/**」と入力してリコーのホームページが閲覧できることを確認します。

設定と確認は以上です。

お問い合わせ先

リコージャパン株式会社　IT コンタクトセンター

ご質問は以下のフリーダイヤルへのお電話にてお願いいたします。

フリーダイヤル	0120-025-361
受付時間	月曜～金曜　8:30　～　18:00
	（年末、年始、および株式会社リコーの定める休日を除く）

商標

Google および Google Chrome™ ブラウザは Google Inc. の商標です。

Mac OS は、米国および他の国々で登録された Apple Inc. の商標です。

Firefox、Thunderbird は Mozilla Foundation の商標です。

Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。

Microsoft、Windows、Windows Vista、Internet Explorer、Windows Live、Excel および Outlook Express は、米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。

- Windows Vista の製品名は以下のとおりです。

  Microsoft® Windows Vista® Ultimate

  Microsoft® Windows Vista® Business

  Microsoft® Windows Vista® Home Premium

  Microsoft® Windows Vista® Home Basic

  Microsoft® Windows Vista® Enterprise

- Windows 7 の製品名は以下のとおりです。

  Microsoft® Windows® 7 Starter

  Microsoft® Windows® 7 Home Premium

  Microsoft® Windows® 7 Professional

  Microsoft® Windows® 7 Ultimate

  Microsoft® Windows® 7 Enterprise

- Windows 8 の製品名は以下のとおりです。

  Microsoft® Windows® 8

  Microsoft® Windows® 8 Pro

  Microsoft® Windows® 8 Enterprise

- Windows 10 の製品名は以下のとおりです。

  Microsoft® Windows® 10

  Microsoft® Windows® 10 Pro

  Microsoft® Windows® 10 Enterprise

- Internet Explorer 8 の正式名称は Windows® Internet Explorer® 8 です。

Microsoft Corporation のガイドラインに従って画面写真を使用しています。

その他の製品名、名称は各社の商標または登録商標です。

JA (JP) 2022年1月 JMSS-0001