画面で見るマニュアル

VPN接続BOX
BX-VP1シリーズ

ご注意　本製品を譲り受けた場合は、初期化してください

以前の設定が残っていると、以前本製品を使用していたユーザーが、あなたの構築したVPNネットワークにアクセスできる場合があります。
情報漏えいを防ぐため、必ず本製品を初期化してからご利用ください。
（「設定を初期化する方法」46ページ）

03版

もくじ

安全のために

お使いになる方への危害、財産への損害を未然に防ぎ、安全に正しくお使いいただくための注意事項を記載しています。ご使用の際には、必ず記載事項をお守りください。

▼ 警告および注意表示

危険	この表示の注意事項を守らないと、死亡または重傷を負う危険が生じます。
警告	この表示の注意事項を守らないと死亡または重傷を負うことがあります。
注意	この表示の注意事項を守らないと、けがをしたり周辺の物品に損害を与えたりすることがあります。

▼ 絵記号の意味

	禁止
	指示を守る

危険

本製品を修理・分解・改造しない

火災や感電、やけど、故障の原因になります。

警告

雷が鳴り出したら本製品や電源コードに触れない

感電の原因になります。

煙がでたり変な臭いや音がしたら、すぐに使用を中止する

コンセントから電源プラグを抜いてください。
そのまま使用すると火災・感電の原因になります。

ACアダプターや本製品をぬらしたり、水気の多い場所で使わない

火災・感電の原因になります。
・お風呂場、雨天、降雪中、海岸、水辺でのご使用は、特にご注意ください。
・水の入ったもの（コップ、花びんなど）を上に置かない。
・万一、ACアダプターや本製品がぬれてしまった場合は、絶対に使用しないでください。

本製品の周辺に放熱を妨げるような物を置かない

火災の原因になります。

本製品の小さな部品（ネジなど）を乳幼児の手の届くところに置かない

誤って飲み込み、窒息や胃などへの障害の原因になります。万一、飲み込んだと思われる場合は、ただちに医師にご相談ください。

故障や異常のまま、通電しない

本製品に故障や異常がある場合は、必ずパソコンから取り外し、コンセントから電源プラグを抜いてください。そのまま使用すると、火災・感電・故障の原因になります。

⚠ 警告（つづき）

電源について

ACアダプターや電源コードは、添付品または指定品のもの以外を使わない

電源コードから発煙したり火災の原因になります。

AC100V（50/60Hz）以外のコンセントにつながない

発熱、火災の恐れがあります。

電源コード、ACアダプターにものをのせたり、引っ張ったり、折り曲げ・押しつけ・加工などはしない

電源コードがよじれた状態や折り曲げた状態で使用しないでください。
電源コードの芯線(電気の流れるところ)が断線したり、ショートし、火災・感電の原因になります。

ゆるいコンセントにつながない

電源プラグは、根元までしっかりと差し込んでください。根元まで差し込んでもゆるみがあるコンセントにはつながないでください。発熱して火災の原因になります。

電源プラグを抜くときは電源コードを引っ張らない

電源プラグを持って抜いてください。
電源コードを引っ張ると電源コードに傷が付き、火災や感電の原因になります。

添付のACアダプターや電源コードは、他の機器につながない

添付の電源コードおよびACアダプターは本製品専用です。他の機器につなぐと、火災や感電の原因になります。

コンセントまわりは定期的に掃除する

長期間電源プラグを差し込んだままのコンセントでは、つもったホコリが湿気などの影響を受けて、火災の原因になります。（トラッキング現象）
トラッキング現象防止のため、定期的に電源プラグを抜いて乾いた布で電源プラグをふき掃除してください。

煙がでたり変な臭いや音がしたら、すぐにコンセントから電源プラグを抜く

そのまま使用すると火災・感電の原因になります。

じゅうたん、スポンジ、ダンボール、発泡スチロールなど、保温・保湿性の高いものの近くで使わない

火災の原因になります。

熱器具のそばに配線しない

電源コードの被覆が破れ、火災や感電、やけどの原因になります。

テーブルタップを使用する時は定格容量以内で使用する、たこ足配線はしない

テーブルタップの定格容量（「1500W」などの記載）を超えて使用すると、テーブルタップが過熱し、火災の原因になります。

⚠ 注意

本製品を踏まない

破損し、ケガの原因になります。特に、小さなお子様にはご注意ください。

長時間にわたり一定の場所に触れ続けない

使用中、使用直後に本体に長時間触れると、やけどの恐れがあります。

電源について

人が通行する場所に配線しない

足を引っ掛けると、けがの原因になります。

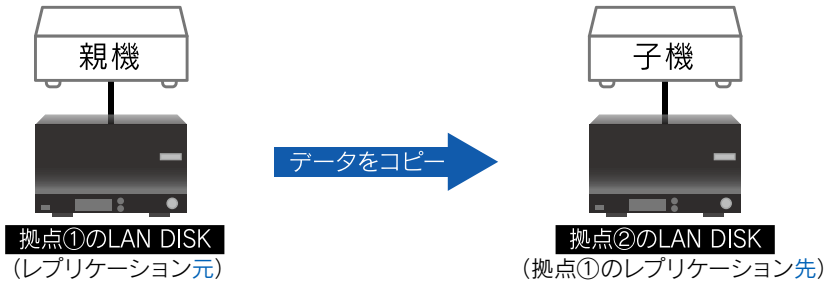
VPN接続

ご利用イメージ

接続例1

拠点①(本社など)のファイルサーバーのレプリカを、拠点②(支社など)に構築する場合

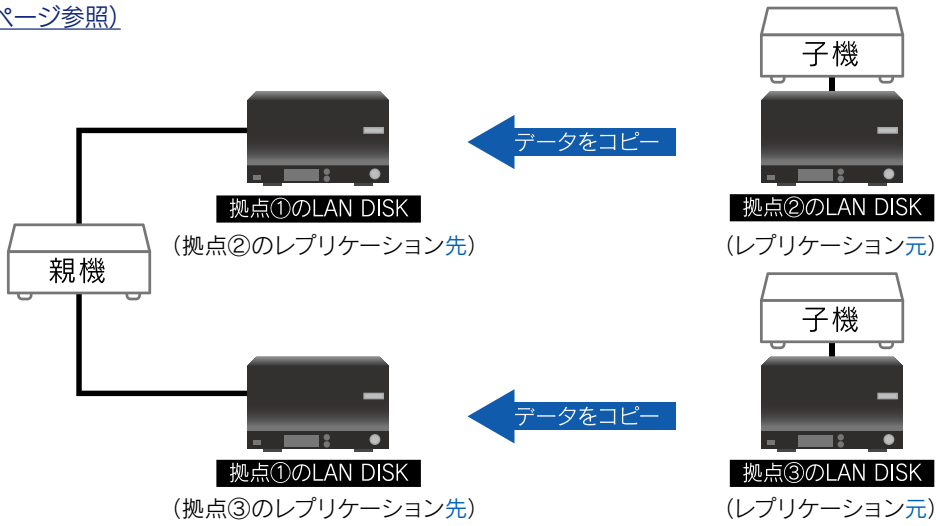
(「はじめてVPNを構築する方法」7 ページ参照)



接続例2

他拠点(支社など)のファイルサーバーのレプリカを、拠点①(本社など)に集約させる場合

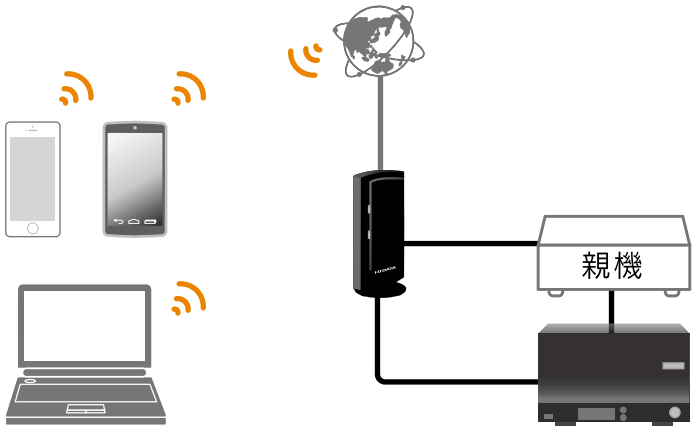
(「子機の増設方法」27 ページ参照)



接続例3

外出先の端末からVPN接続する場合

(「外出先の端末からVPN接続する方法」16 ページ参照)



はじめて VPN を構築する方法 （BX-VP1-S 接続例1 の場合）

ご注意　本製品ご利用前に以下の確認、準備をお願いします

- ホームネットワークチェッカーをダウンロードし、実行すると、VPN構築が可能なネットワーク環境（複数のルーターが設定されていないか等）かどうかを事前に診断できます。
  http://www.iodata.jp/r/4812
- ご利用のルーターが「IPsecパススルー」に対応しているかどうかご確認ください。（ルーターの取扱説明書参照）
- リモートレプリケーションを利用する場合は、十分なスループットを確保できる光回線をご使用ください。
- 準備するもの：ご利用になる伝送方式にあうLANケーブル2本
  - ・1000BASE-T通信時：カテゴリ5E以上のUTP、またはSTPケーブル
  - ・100BASE-TX通信時：カテゴリ5以上のUTP、またはSTPケーブル
  - ・10BASE-T通信時　：カテゴリ3以上のUTP、またはSTPケーブル
- 親機と子機の見分け方

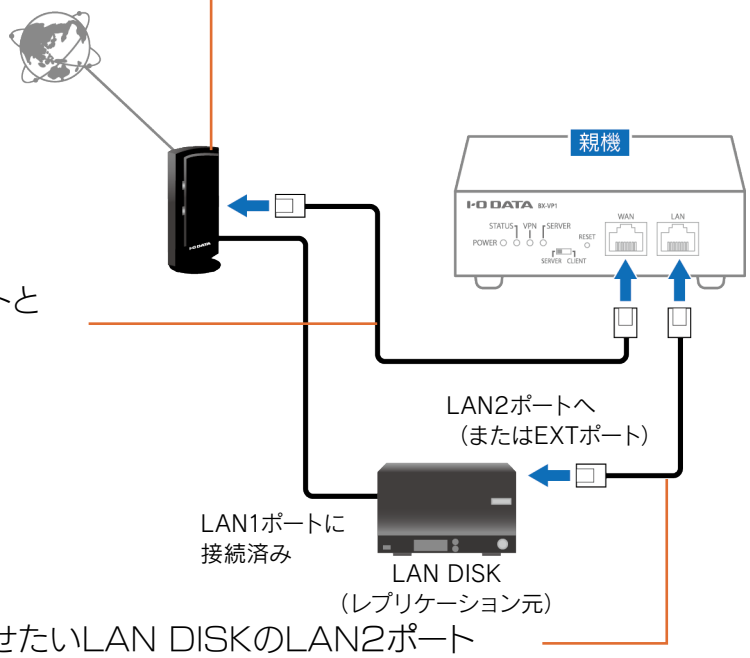
  SERVER/CLIENT切替スイッチの位置で見分けることができます。

  SERVER側：親機として使用時　　CLIENT側：子機として使用時

  ※ また、本体の天面には「親機」または「子機」と書かれたシールが貼られています。
- BX-VP1-Sは出荷時で親機と子機のペアリングが完了しています。子機を増設した場合や、本製品の初期化をおこなった場合は、VPN接続前にペアリングをおこなってください。（「1.親機とペアリングします」28 ページ）
- 本製品を利用すると、LAN DISKのNICチーミング機能は使用できません。あらかじめご了承ください。

1. 拠点①に親機を設置します

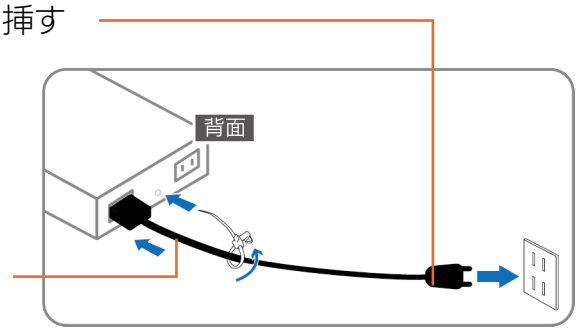
1 ルーターの「IPsecパススルー」を有効にする
（設定方法は、ご利用のルーターの取扱説明書参照）



2 LANケーブルで、ルーターのLANポートと
親機のWANポートをつなぐ

3 LANケーブルで、他拠点とVPN接続させたいLAN DISKのLAN2ポート
（またはEXTポート）と親機のLANポートをつなぐ

4 添付のACケーブルを、
親機のAC100V INコネクターと電源コンセントに挿す



5 添付のACケーブルクランプを、ACケーブルに巻き、
ACケーブルクランプ取り付け穴に挿して固定する

以上で、親機の設置は完了です。次に子機を設置します。
「2.拠点②に子機を設置します」10 ページへお進みください。

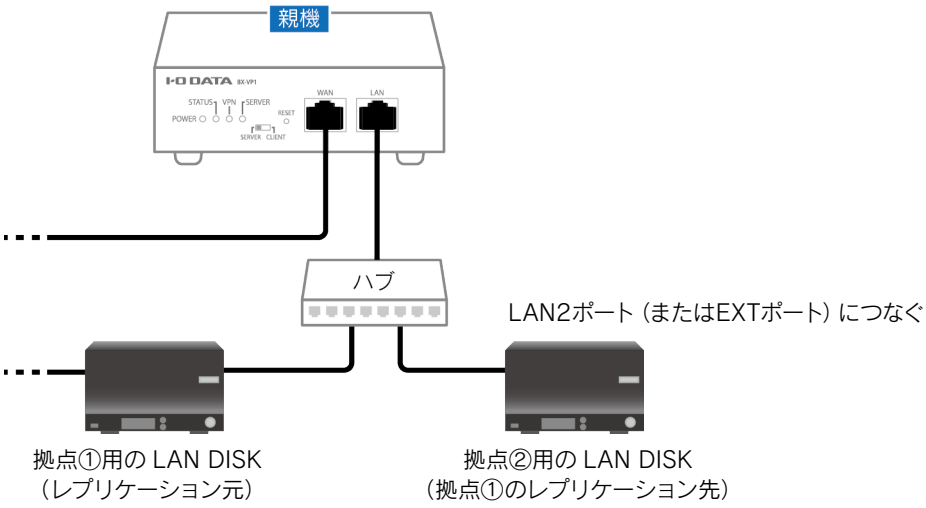
ご注意　レプリケーション元 LAN DISK にデータがある場合は、ローカル環境でのコピーをおすすめします

データの入っているLAN DISK（レプリケーション元）のリモートレプリケーションによる共有フォルダーの初回の同期には、時間がかかります。
また、ネットワーク環境に負荷がかかるため、通常の業務に支障が出る可能性があります。
拠点②にLAN DISK（レプリケーション先）を送る前に以下のようにつなぎ、ローカル環境にて同期をおこなうことをお勧めします。
【初回同期完了までの時間（目安）】
実効帯域60Mbps程度のインターネット回線において、データ容量1.0TBのファイルのレプリケーションをおこなった場合
＝約40時間

1　下図のように拠点②用のLAN DISKをつなぐ

2　LAN DISKのレプリケーションの設定をする

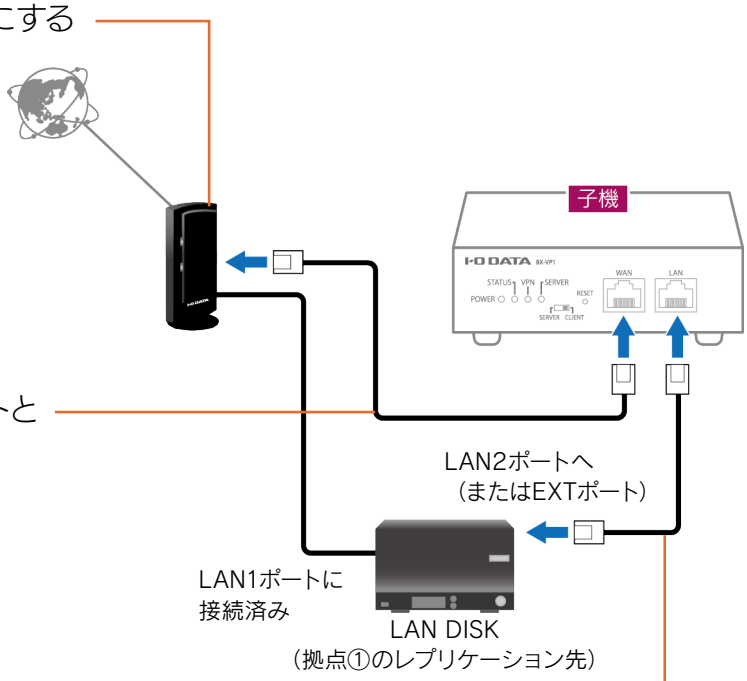
（設定方法は、ご利用のLAN DISKの取扱説明書参照）



以上で、LAN DISKの設定は完了です。
拠点①のLAN DISKは「1.拠点①に親機を設置します」8 ページの状態に戻します。
拠点②のLAN DISKは拠点②へ運び、設置をおこないます。（「2.拠点②に子機を設置します」10 ページ参照）

2. 拠点②に子機を設置します

1 ルーターの「IPsecパススルー」を有効にする
（設定方法は、ご利用のルーターの取扱説明書参照）



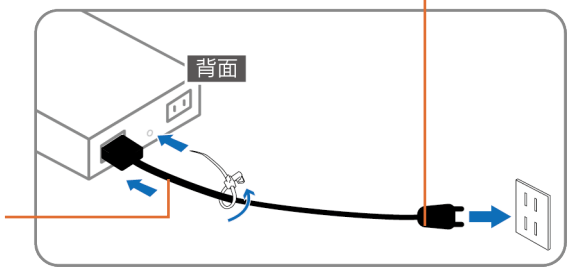
2 LANケーブルで、ルーターのLANポートと
子機のWANポートをつなぐ

3 LANケーブルで、他拠点とVPN接続させたいLAN DISKのLAN2ポート
（またはEXTポート）と子機のLANポートをつなぐ

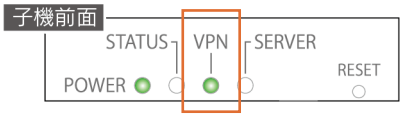
※ 本製品子機側に接続したLAN DISK（レプリケーション先）のIPアドレスは、「3.LAN DISKのレプリケーション設定をする」11 ページにしたがって設定してください。

4 添付のACケーブルを、
子機のAC100V INコネクターと電源コンセントに挿す

5 添付のACケーブルクランプを、ACケーブルに巻き、
ACケーブルクランプ取り付け穴に挿して固定する



6 子機のVPNランプが点灯していることを確認する



以上で、子機の設置は完了です。次にLAN DISKの設定をします。
「3.LAN DISKのレプリケーション設定をする」11 ページへお進みください。

VPN 対地数（本製品親機との接続可能数）

本製品子機：2台まで（※）
その他デバイスを含めて同時合計4台まで推奨
（※）本製品子機の配下に接続できるデバイスは、1台のみです。

3.LAN DISK のレプリケーション設定をする

接続例およびご利用のLAN DISKの手順例をご参照ください。

- 接続例1「拠点①（本社など）のファイルサーバーのレプリカを、拠点②（支社など）に構築する場合」12 ページ参照
- 接続例2「他拠点（支社など）のファイルサーバーのレプリカを、拠点①（本社など）に集約させる場合」14 ページ参照

以上で、VPN構築は完了です。
リモートレプリケーションやリモートアクセスをご利用ください。

ご注意　初回レプリケーションには時間がかかります

業務に支障が少ない時間帯におこなうか、ローカル環境にておこなうことをお勧めします。
（「ご注意　レプリケーション元LAN DISKにデータがある場合は、ローカル環境でのコピーをおすすめします」9 ページ参照）

レプリケーション先の指定は IP アドレスで設定してください

弊社製「HDL-Z シリーズ」にて DFS レプリケーションをご利用の場合、インターネット越しにアクティブディレクトリに参加する必要があります

ネットワーク管理者にご相談ください。

拠点①から拠点②の LAN DISK をリモートアクセスで設定する場合

HDL-Zシリーズでは、液晶モニター、キーボード、マウスをHDL-Zシリーズに接続して設定してください。
HDL-Zシリーズ以外では、親機のLANポートにハブをつなげて、LAN DISKとパソコンを接続して設定してください。

子機に接続した LAN DISK の IP アドレス

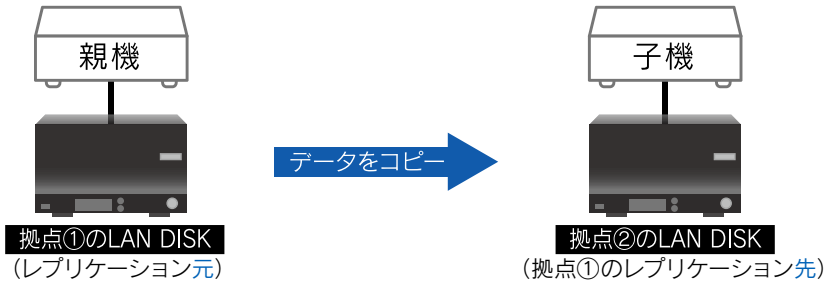
「192.168.88.110」または「192.168.88.111」に固定してください。
既にIPアドレスを固定していた場合は、上記のいずれかの値に変更してください。

親機に接続した LAN DISK の設定は、拠点①のルーターに接続しているパソコンからおこなえます

弊社製「HDL-Z シリーズ」にて arcserve Replication／High Availability（RHA）のスイッチオーバー機能：IP 移動、Sync with BE のネットワーク設定切替を利用する場合、本製品より割り当てる IP アドレスを変更する必要があります。

接続例1

拠点①(本社など)のファイルサーバーのレプリカを、拠点②(支社など)に構築する場合



レプリケーション元 LAN DISK は以下のいずれかの IP アドレスに固定してください

[192.168.88.11～192.168.88.99]
[192.168.88.112～192.168.88.254]

※ 上記は初期設定時のIPアドレスとなります。IPアドレスを変更した場合は、変更後に合わせてIPアドレスを固定してください。

レプリケーション先 LAN DISK の IP アドレスは［192.168.88.110］に固定してください

※ 上記は初期設定時のIPアドレスとなります。IPアドレスを変更した場合は、変更後に合わせてIPアドレスを固定してください。

例:HDL-XRシリーズの場合

1 レプリケーション先とレプリケーション元の両方のLAN DISKのEXTポートを有効にする

① LAN DISKのLAN1ポートから設定画面を開く

※ 管理者パスワードでログオンしてください。

② 設定画面の[詳細設定] → [基本設定] → [ネットワーク設定] よりEXTポートを有効にする

※ 上記①～②の操作をレプリケーション先とレプリケーション元の両方のLAN DISKでおこなってください。

③ レプリケーション元とレプリケーション先のLAN DISKのEXTポートのIPアドレスは、以下のように設定する

◆レプリケーション元のLAN DISK(拠点①):「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定する。

◆レプリケーション先のLAN DISK(拠点②):「192.168.88.110」に固定する。

※「IPアドレスを自動的に取得する(DHCP)」に設定した場合でも同様のIPアドレスになります。

2 レプリケーション先とレプリケーション元の両方のLAN DISKのレプリケーションの設定をする

※ LAN DISKの「画面で見るマニュアル」の「レプリケーション」をご参照ください。

※ レプリケーション先の設定を最初におこなってください。そのあと、レプリケーション元の設定をおこなってください。

▼「画面で見るマニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-xrmanual.pdf

例：HDL6-Hシリーズの場合

1 レプリケーション先のLAN DISKのLAN1ポートから設定画面を開く

① レプリケーション先のLAN DISKのLAN1ポートから設定画面を開く

② レプリケーション元とレプリケーション先のLAN DISKのIPアドレスは、以下のように設定する

◆レプリケーション元のLAN DISK（拠点①）：「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定する。

◆レプリケーション先のLAN DISK(拠点②)：「192.168.88.110」に固定する。

※「IPアドレスを自動的に取得する（DHCP）」に設定した場合でも同様のIPアドレスになります。

2 レプリケーション先とレプリケーション元の両方のLAN DISKのレプリケーションの設定をする

▼「パッケージ取扱説明書「レプリケーション」」参照

http://www.iodata.jp/lib/manual/pdf2/hdlh-replication-manual.pdf

例：HDL-Zシリーズの場合

1 レプリケーション先のLAN DISKのLAN1ポートからリモートデスクトップ接続でLAN DISKにアクセスする

下記マニュアル「IPアドレス設定」を参照し、レプリケーション元とレプリケーション先のLAN DISKのLAN2ポートのIPアドレスを以下のように設定する

◆レプリケーション元のLAN DISK（拠点①）：「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定する。

◆レプリケーション先のLAN DISK(拠点②)：「192.168.88.110」に固定する。

※「IPアドレスを自動的に取得する（DHCP）」に設定した場合でも同様のIPアドレスになります。

※ ネットワーク上で発見できない場合は、LAN DISKにディスプレイ、キーボード、マウスを接続して設定してください。

▼HDL-ZWLC2シリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwlc2_kanri_b-manu202101.pdf

▼HDL-ZWMC2シリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwmc2_kanri_b-manu202102.pdf

▼HDL-ZWSCシリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwsc_kanri_b-manu202008.pdf

2 レプリケーション元と先のLAN DISKにソフトをインストールし、レプリケーションの設定をする

▼arcserve Replication／High Availability（RHA）のマニュアルはこちら

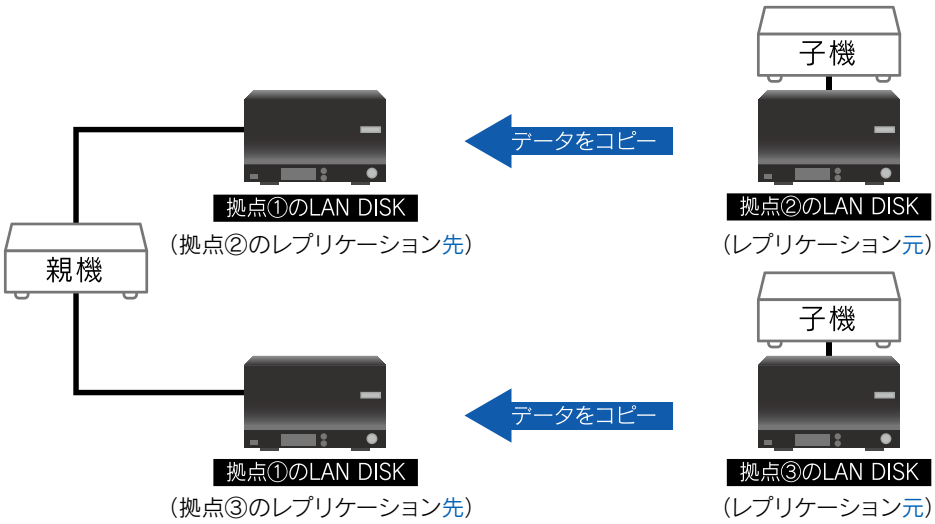
http://www.arcserve.com/jp/lpg/jpsupport/manual.aspx#a02

▼Sync with BEを使用したバックアップをおこなうには、こちらより無償ダウンロード

http://www.iodata.jp/solutions/syncwithbe/index.htm

接続例2

他拠点(支社など)のファイルサーバーのレプリカを、拠点①(本社など)に集約させる場合



レプリケーション先 LAN DISK は以下のいずれかの IP アドレスに固定してください

[192.168.88.11～192.168.88.99]
[192.168.88.112～192.168.88.254]

※ 上記は初期設定時のIPアドレスとなります。IPアドレスを変更した場合は、変更後に合わせてIPアドレスを固定してください。

レプリケーション元 LAN DISK は以下のいずれかの IP アドレスに固定してください

[192.168.88.110]または[192.168.88.111]

※ 上記は初期設定時のIPアドレスとなります。IPアドレスを変更した場合は、変更後に合わせてIPアドレスを固定してください。
※ ペアリング済み子機のLAN側DHCPクライアントリリースアドレスは、1台目が「192.168.88.110」、2台目が「192.168.88.111」となります。

例:HDL-XRシリーズの場合

1 レプリケーション先とレプリケーション元のすべてのLAN DISKのEXTポートを有効にする

① LAN DISKのLAN1ポートから設定画面を開く

※ 管理者パスワードでログオンしてください。

② 設定画面の[詳細設定] → [基本設定] → [ネットワーク設定] よりEXTポートを有効にする

※ 上記①～②の操作をリモートレプリケーションに使うすべてのLAN DISKでおこなってください。

③ レプリケーション先とレプリケーション元のLAN DISKのEXTポートのIPアドレスは、以下のように設定する

◆レプリケーション先のLAN DISK(拠点①):「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定する。

◆レプリケーション元のLAN DISK(拠点②と拠点③):「192.168.88.110」または「192.168.88.111」のいずれかに固定する。

※ ペアリング済み子機のLAN側DHCPクライアントリリースアドレスは、1台目が「192.168.88.110」、2台目が「192.168.88.111」となります。

2 レプリケーション先とレプリケーション元の両方のLAN DISKのレプリケーションの設定をする

※ LAN DISKの「画面で見るマニュアル」の「レプリケーション」をご参照ください。

※ レプリケーション先の設定を最初におこなってください。そのあと、レプリケーション元の設定をおこなってください。

▼「画面で見るマニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-xrmanual.pdf

例：HDL6-Hシリーズの場合

1 レプリケーション先とレプリケーション元の両方のLAN DISKのLAN1ポートから設定画面を開く

① レプリケーション先のLAN DISKのLAN1ポートから設定画面を開く

② レプリケーション先とレプリケーション元のLAN DISKのLAN2ポートのIPアドレスは、以下のように設定する

◆レプリケーション先のLAN DISK（拠点①）：「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定

◆レプリケーション元のLAN DISK(拠点②と拠点③)：「192.168.88.110」または「192.168.88.111」のいずれかに固定する。

※ ペアリング済み子機のLAN側DHCPクライアントリリースアドレスは、1台目が「192.168.88.110」、2台目が「192.168.88.111」となります。

2 レプリケーション先とレプリケーション元の両方のLAN DISKのレプリケーションの設定をする

▼「パッケージ取扱説明書「レプリケーション」」参照

http://www.iodata.jp/lib/manual/pdf2/hdlh-replication-manual.pdf

例：HDL-Zシリーズの場合

1 レプリケーション先とレプリケーション元のすべてのLAN DISKのLAN1ポートからリモートデスクトップ接続でLAN DISKにアクセスする

下記マニュアル「IPアドレス設定」を参照し、レプリケーション先とレプリケーション元のLAN DISKのLAN2ポートのIPアドレスを以下のように設定する

◆レプリケーション先のLAN DISK（拠点①）：「192.168.88.11～192.168.88.99」または「192.168.88.112～192.168.88.254」のいずれかに固定する。

◆レプリケーション元のLAN DISK(拠点②と拠点③)：「192.168.88.110」または「192.168.88.111」のいずれかに固定する。

※ ペアリング済み子機のLAN側DHCPクライアントリリースアドレスは、1台目が「192.168.88.110」、2台目が「192.168.88.111」となります。

※ ネットワーク上で発見できない場合は、LAN DISKにディスプレイ、キーボード、マウスを接続して設定してください。

▼HDL-ZWLC2シリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwlc2_kanri_b-manu202101.pdf

▼HDL-ZWMC2シリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwmc2_kanri_b-manu202102.pdf

▼HDL-ZWSCシリーズの場合：「管理マニュアル」参照

http://www.iodata.jp/lib/manual/pdf2/hdl-zwsc_kanri_b-manu202008.pdf

2 レプリケーション元と先のLAN DISKにソフトをインストールし、レプリケーションの設定をする

▼arcserve Replication／High Availability（RHA）のマニュアルはこちら

http://www.arcserve.com/jp/lpg/jpsupport/manual.aspx#a02

▼Sync with BEを使用したバックアップをおこなうには、こちらより無償ダウンロード

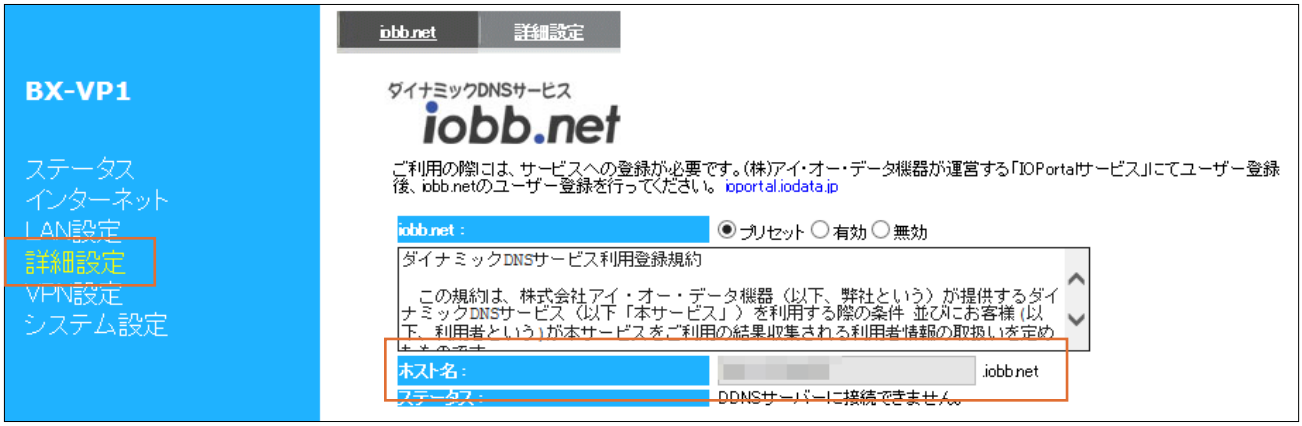
http://www.iodata.jp/solutions/syncwithbe/index.htm

外出先の端末から VPN 接続する方法

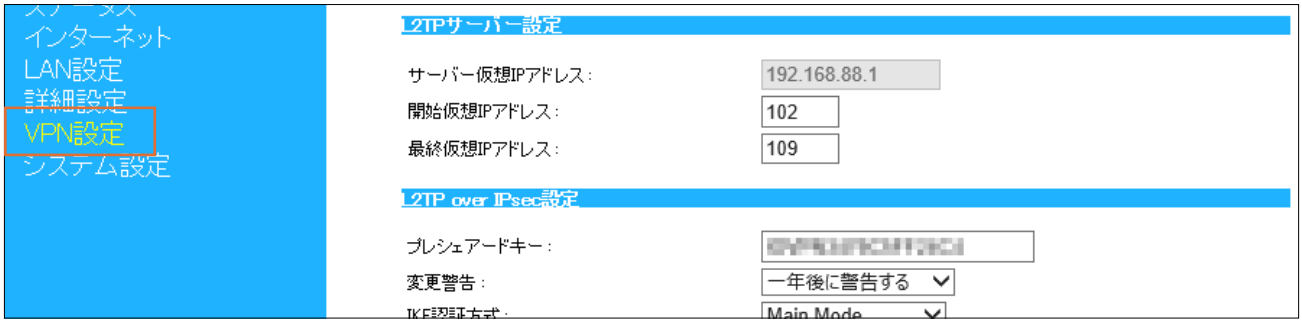
準備する

1 親機の設定画面を開く

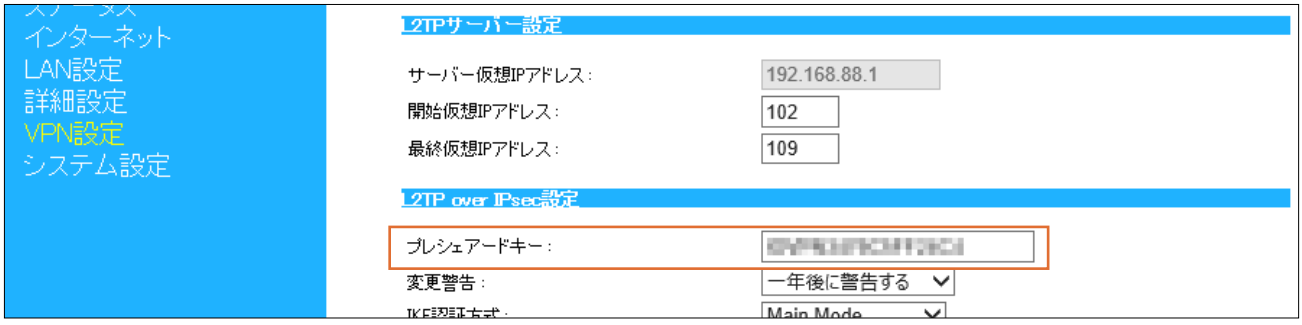
2 **Mac OS、Androidから接続する場合、**[詳細設定]メニューの[ホスト名]をメモする
(「設定画面の開き方」37 ページ参照)



3 [VPN設定]メニューを開く



4 **Mac OS、Androidから接続する場合、**「プレシェアードキー」をメモする

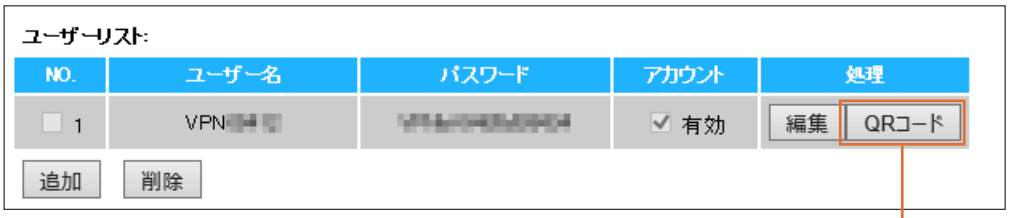


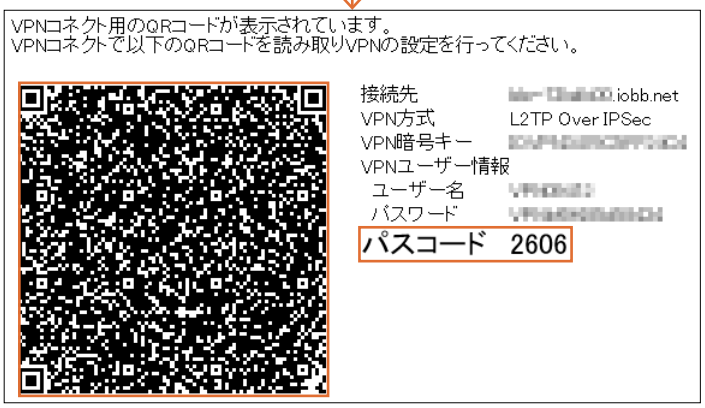
定期的にプレシェアードキーおよび設定画面のパスワードを変更してください

セキュリティ向上の為に、定期的にプレシェアードキーおよび設定画面のパスワードを変更することをお勧めします。(親機と子機ともに同じ内容で変更します。)(「プレシェアードキーの変更方法」40 ページ参照) (「パスワードの変更方法」42 ページ参照)

5 ユーザー情報を取得する

●**Windows、iOSから接続する場合、**接続するVPNユーザーの[QRコード]をクリックし、QRコードとパスコードを取得する（VPN環境設定アプリ『VPNコネクト』で使います）





QR コードとパスコードの配布

QRコードとパスコードは分けて配布することをおすすめします。
※QRコードは画像として表示されていますので、右クリックして印刷やコピーするのが便利です。

No.1 の VPN ユーザーのパスコードは、期限が来ると変更されます（初期値：毎曜日午前 4 時）

パスコードが変更になるたび、VPNコネクトによるVPN設定が必要です。
VPN設定をひんぱんに繰り返したくない場合は、新しいVPNユーザーを追加して、そのQRコードとパスコードをご利用ください。
※No.1のVPNユーザーのパスコード変更タイミングは、設定可能です。

設定方法によっては接続する VPN ユーザー名とパスコードが必要です（Windows 版のみ）

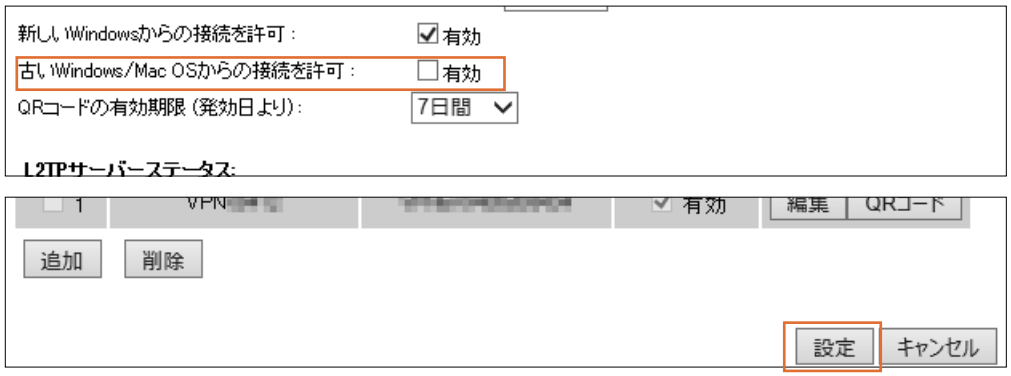
VPNコネクト Windows版ではQRコードを読み取る方法の他にも設定方法があります。
その方法では、VPNユーザー名とパスコードが必要になります。

●**Mac OS X、Androidから接続する場合、**接続するVPNユーザーの「ユーザー名」「パスワード」をメモする

No.1 の VPN ユーザーのパスワードは、期限が来ると変更されます（初期値：毎曜日午前 4 時）

パスワードが変更になるたび、VPN設定を変更する必要があります。
VPN設定をひんぱんに変更したくない場合は、新しいVPNユーザーを追加して、そのユーザー名とパスワードをご利用ください。
※No.1のVPNユーザーのパスワード変更タイミングは、設定可能です。

6 Windows Vista、Mac OS 10.6から接続する場合、[古いWindows/Mac OSからの接続を許可]の[有効]にチェックし、[設定]をクリックする



ご注意　本設定をおこなうとセキュリティが低下します

Windows Vista/Mac OS 10.6を接続したいとき以外は、本設定をしないことをおすすめします。
※本設定をおこなうと、IKEフェーズでの暗号化レベルが弱いものでも接続が可能な状態になります。

以上で準備は完了です。次にご利用のOSの設定をおこなってください。

Windows の場合

http://www.iodata.jp/lib/ で「VPNコネクト」を検索し、VPN環境設定アプリ『VPNコネクト』をダウンロードしてください。
その後の操作については、『VPNコネクト』のヘルプをご覧ください。

『VPN コネクト』を使わずに VPN の設定をする

お使いのWindowsにあったページをご覧ください。
「VPNコネクトを使わずにVPNを設定したい」65ページ参照

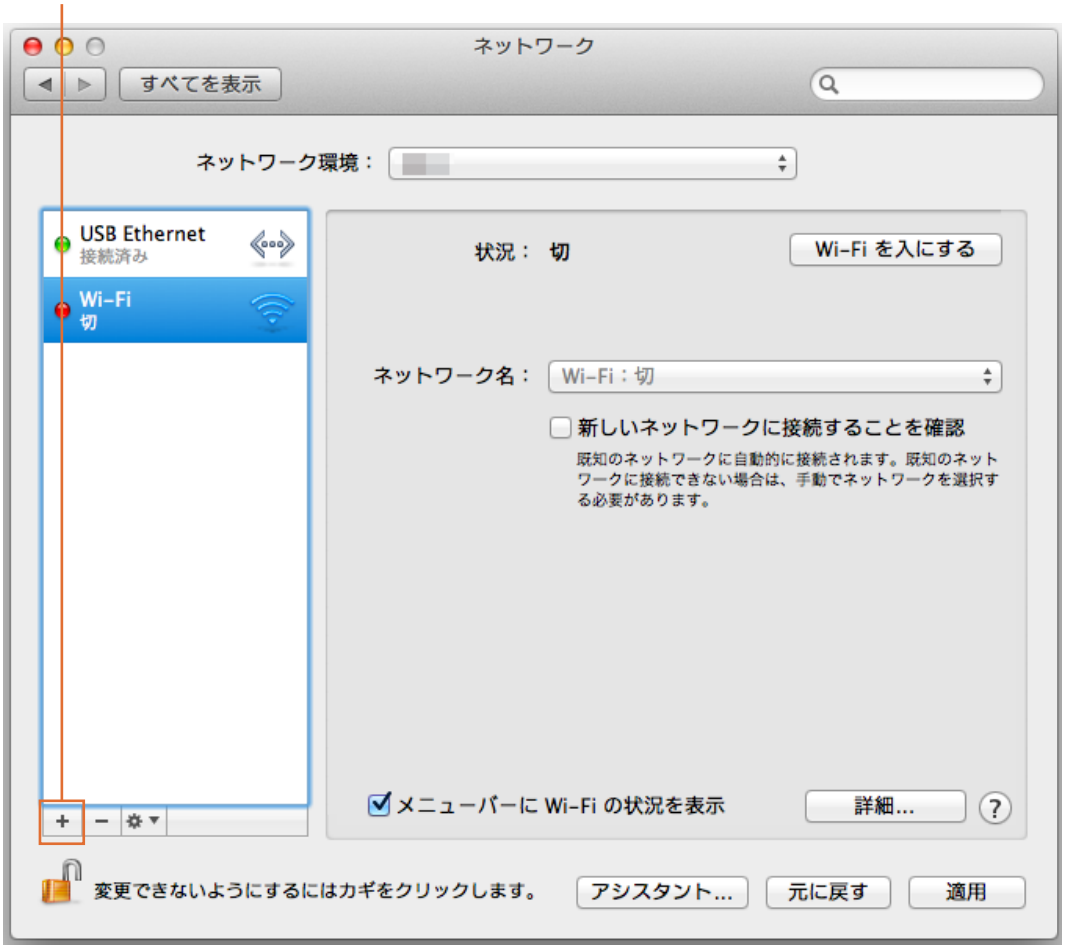
設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

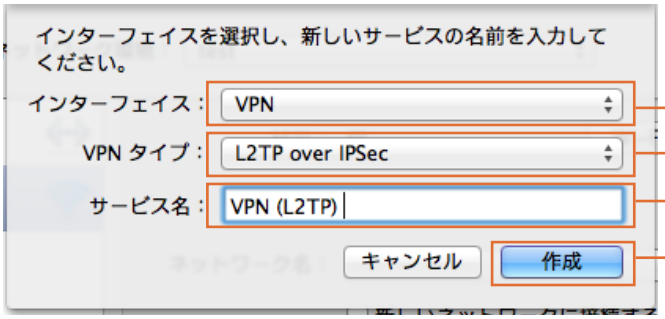
Mac OS X の場合

1 アップルメニューから[システム環境設定]→[ネットワーク]の順にクリック

2 ネットワーク画面のリスト下部の「＋」(追加)をクリック



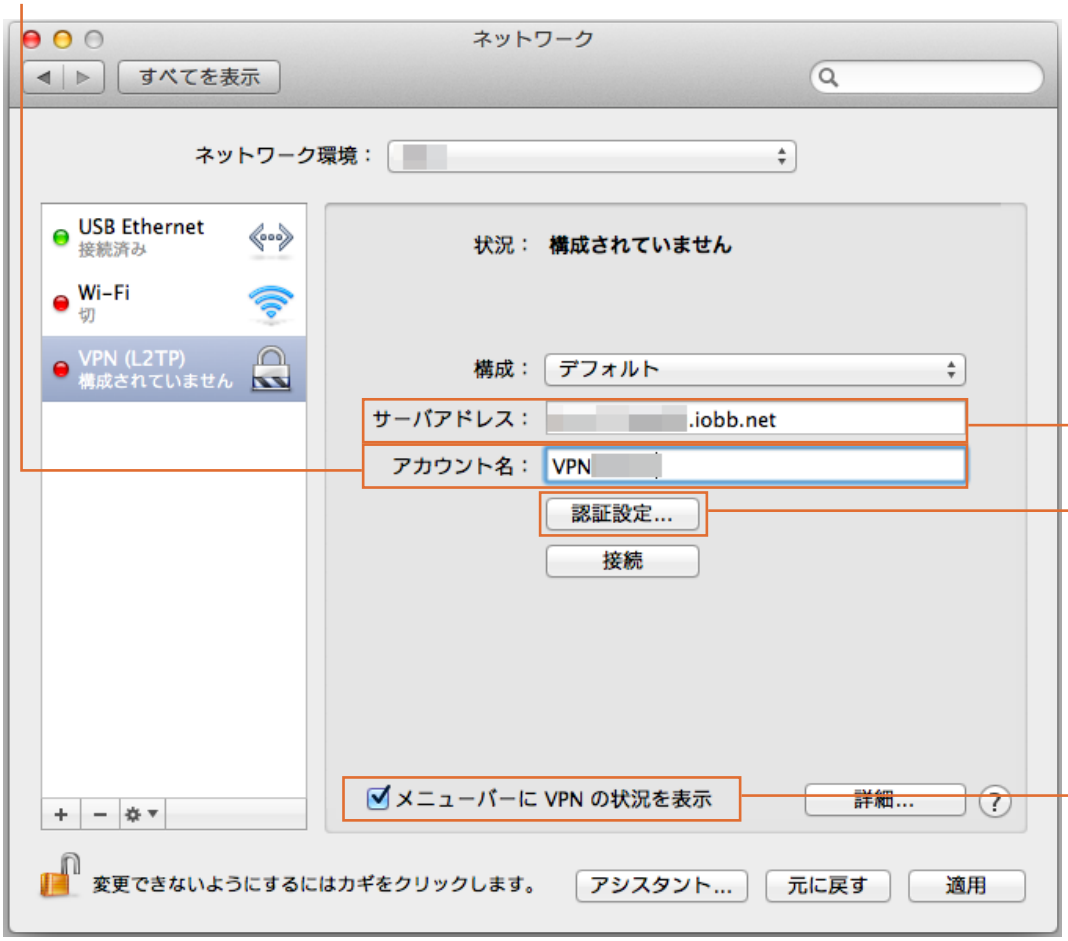
3



① インターフェイスは[VPN]を選択
② VPNタイプは[L2TP over IPSec]を選択
③ 任意のサービス名を入力
④ [作成]をクリック

4

① サーバアドレスに「準備する」16 ページで確認した[ホスト名]を入力
② アカウント名に「準備する」16 ページで確認した[ユーザー名]を入力

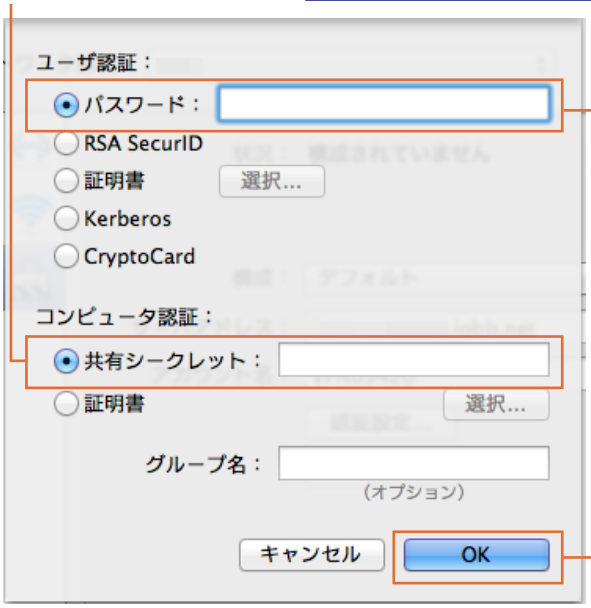


③ [認証設定]をクリック

④ [メニューバーにVPNの状況を表示]にチェック

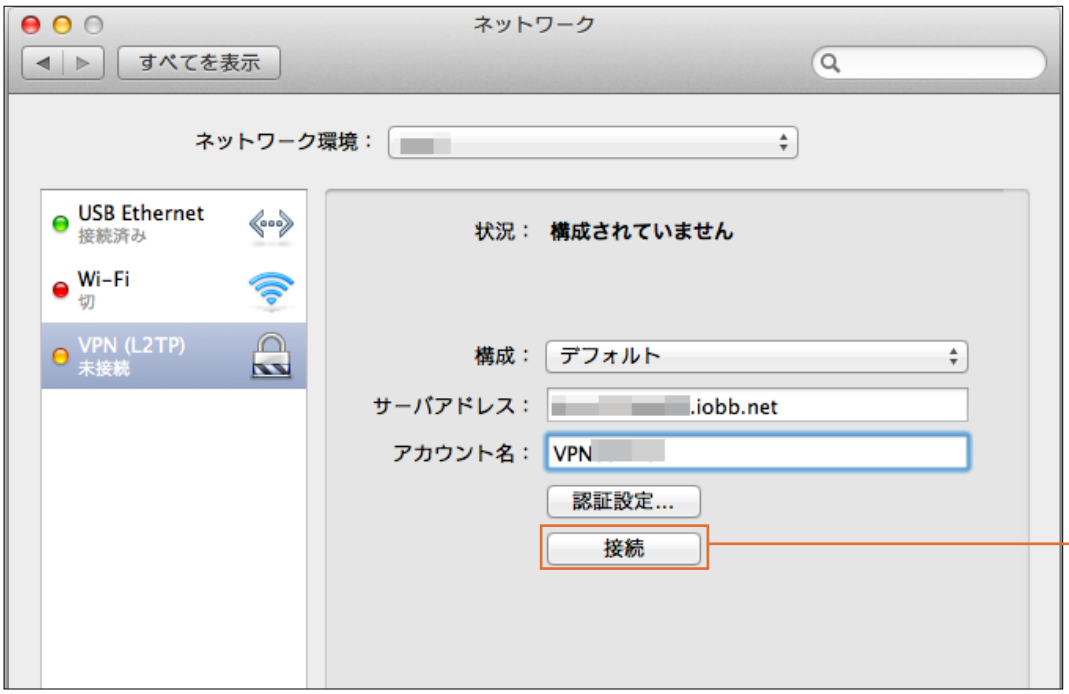
5

① パスワードに「準備する」16 ページで確認した[パスワード]を入力
② 共有シークレットに「準備する」16 ページで確認した[プレシェアードキー]を入力



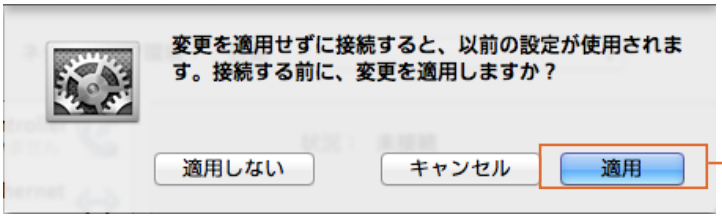
③ [OK]をクリック

6



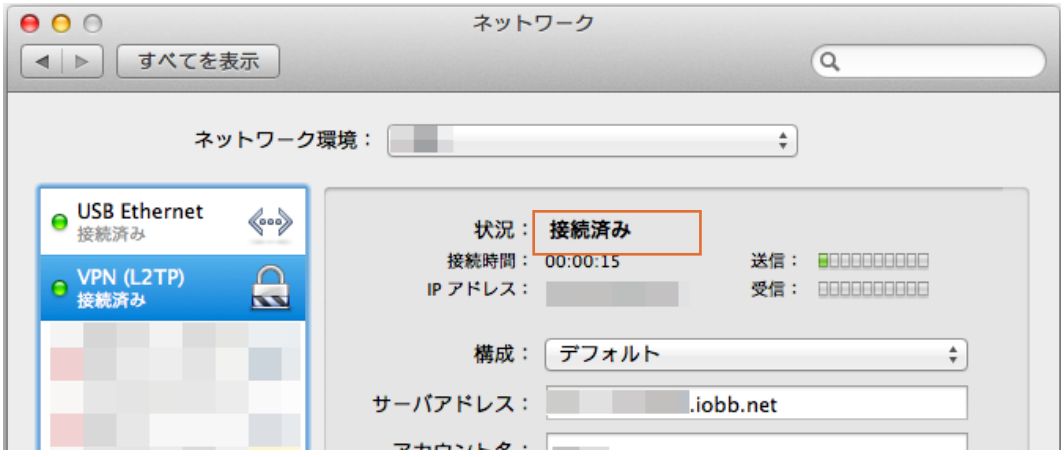
[接続]をクリック

7



[適用]をクリック

8 「接続済み」と表示されたことを確認



以上で設定は完了です。

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

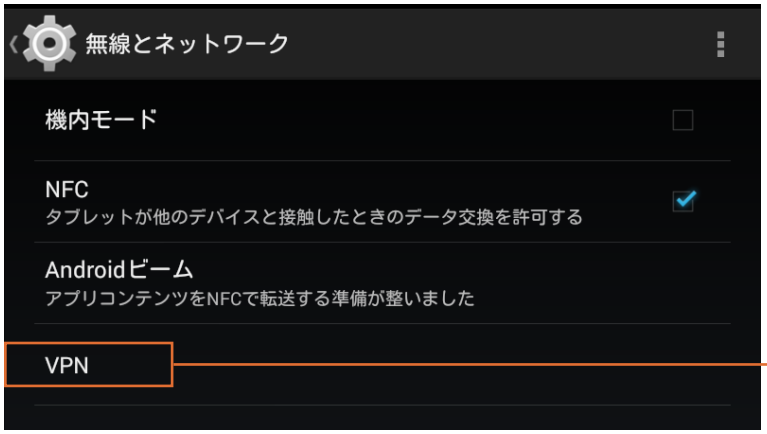
Android の場合

1 [設定] をタップ

2

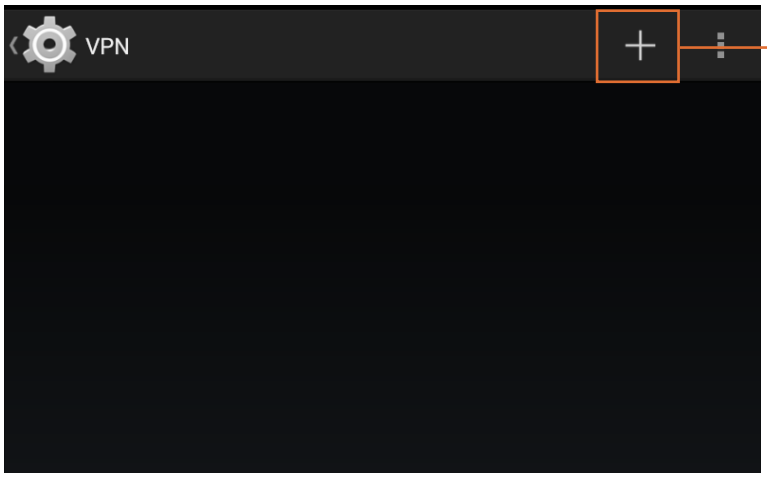
[その他]をタップ

3



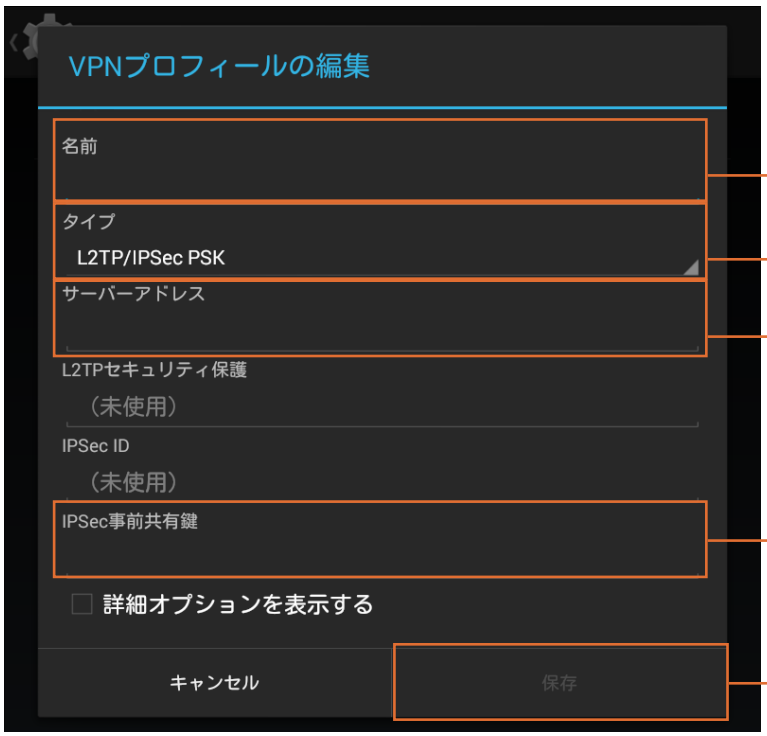
[VPN]をタップ

4



[+]をタップ

5



① 任意の名前を入力

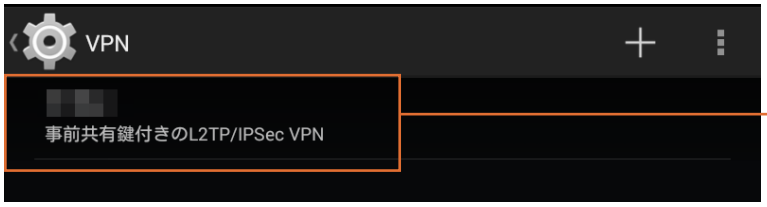
② [L2TP/IPSecPSK]を選択

③ 「準備する」16 ページで確認した[ホスト名]を入力

④ 「準備する」16 ページで確認した[プレシェアードキー]を入力

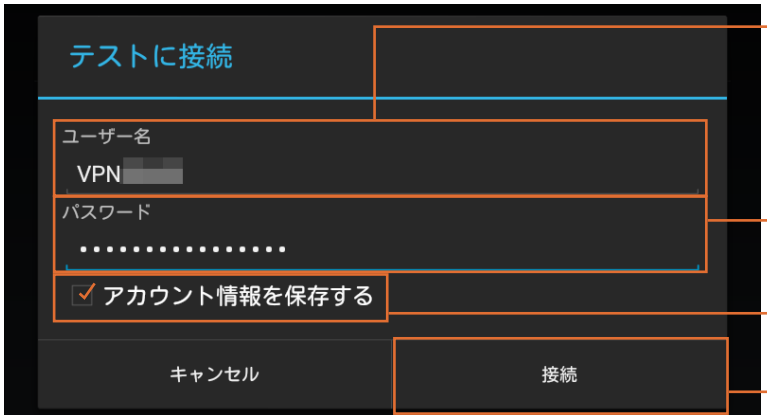
⑤ [保存]をタップ

6



保存した名前をタップ

7



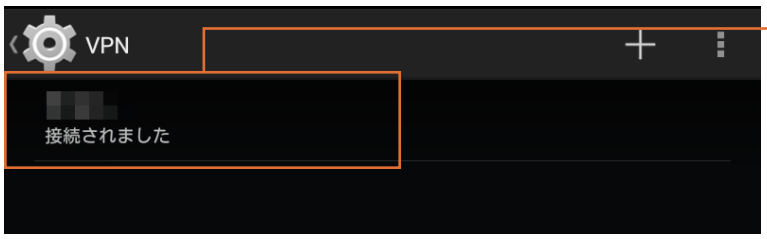
① 「準備する」16 ページで確認した[ユーザー名]を入力

② 「準備する」16 ページで確認した[パスワード]を入力

③ [アカウント情報を保存する]にチェック

④ [接続]をタップ

8



「接続されました」と表示されたことを確認

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

以上で設定は完了です。

iPhone/iPad の場合

VPN環境設定アプリ『VPNコネクト』を利用して、接続をおこなってください。

『VPN コネクト』を使わずに VPN の設定をする

こちらをご覧ください。

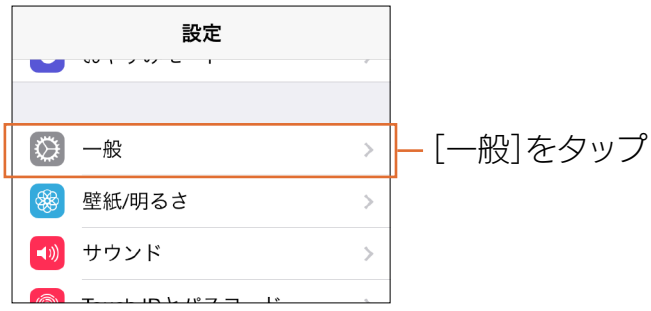
「iPhone/iPadの場合」78ページ参照

1 App Storeより『VPNコネクト』を検索し、インストールする

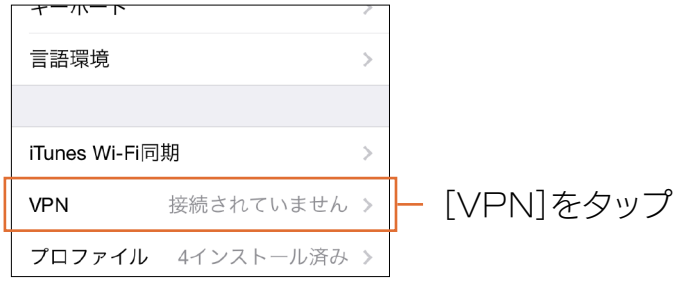
2 『VPNコネクト』を開き、画面の指示にしたがって設定する

※QRコード、パスコードについては、ネットワークの管理者に確認してください。

3 設定 をタップ



4



5

① [BX-VP…]をチェックする

② [オン]にする

③ [接続中]と表示されたことを確認

以上で設定は完了です。

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

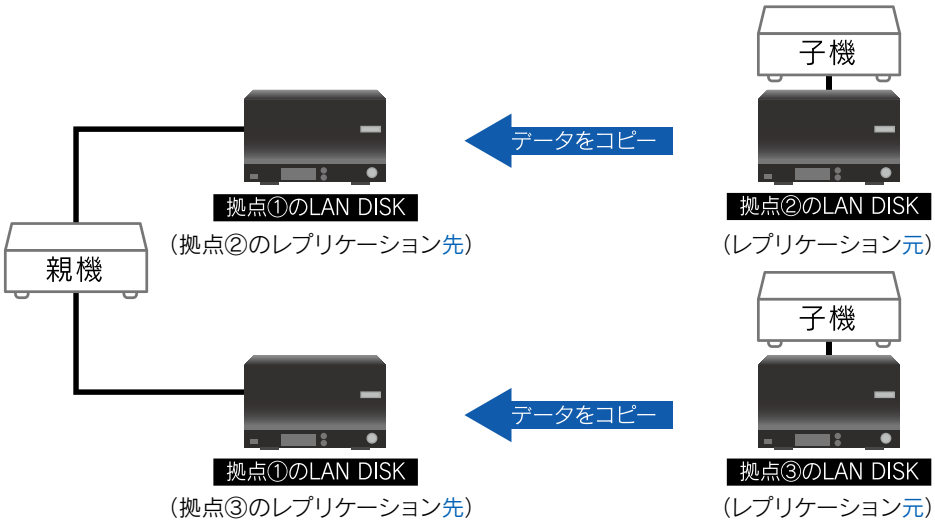
「VPN設定を削除したい」81ページ参照

子機の増設方法

接続例のご利用ケースで説明します。
すでに拠点①に「レプリケーション先LAN DISK」、拠点②に「レプリケーション元LAN DISK」が設置され、運用されていることを想定しています。

接続例2

他拠点(支社など)のファイルサーバーのレプリカを、拠点①(本社など)に集約させる場合



※ 本製品子機の配下に接続できるデバイスは、1台のみです。

ご注意

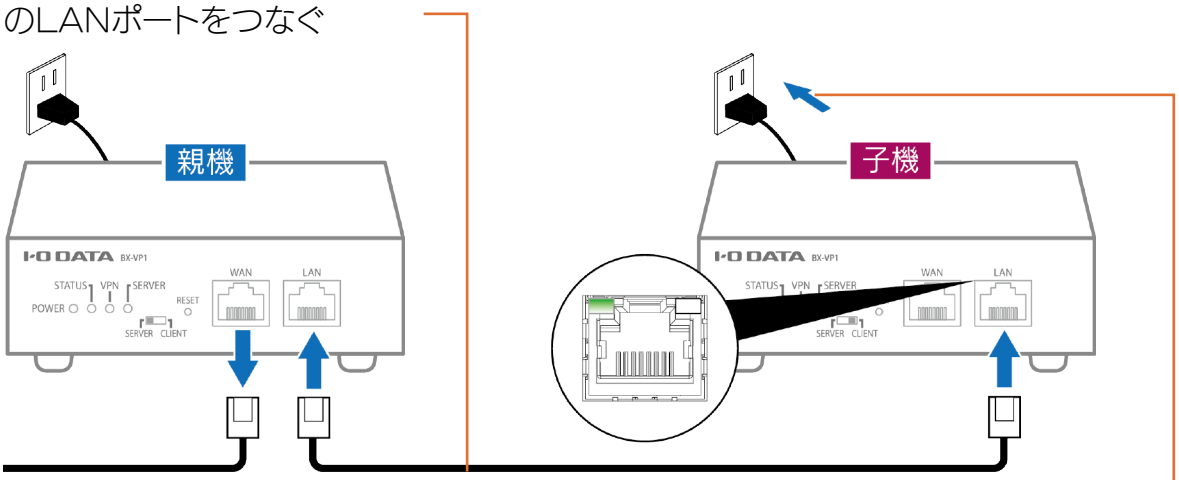
- 親機1台に対して子機は2台まで接続できます。
- ペアリング中はパソコン等から親機にVPN接続できません。

1. 親機とペアリングします

1 子機を親機の近くに置く

2 親機からLANケーブルをすべて取り外す（電源は入れたままにします）

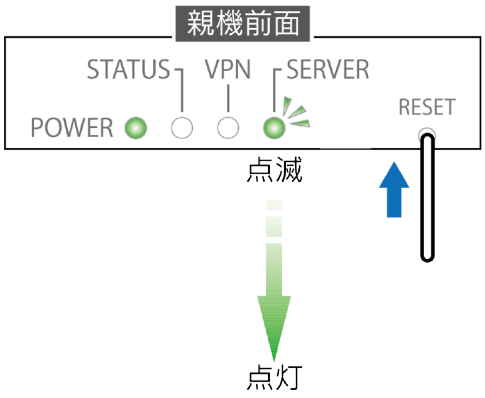
3 別のLANケーブルで、親機のLANポートと、子機のLANポートをつなぐ



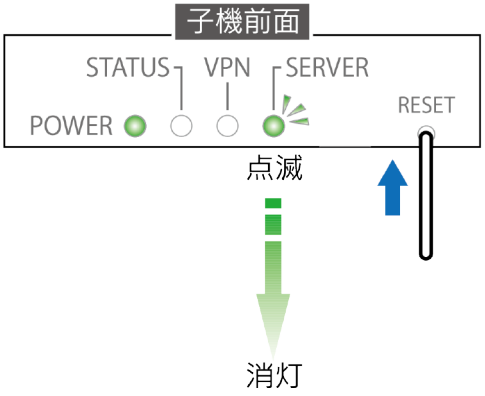
4 添付のACケーブルを、子機のAC100V INコネクターと電源コンセントに挿す

5 LINK/ACTランプが点灯したことを確認

6 ① 親機のRESETボタンをSERVERランプが点滅するまで長押し（約3秒）



② 子機のRESETボタンをSERVERランプが点滅するまで長押し（約3秒）



SERVER ランプが点滅したら、すぐに RESET ボタンから手を離してください

RESETボタンを10秒以上長押しすると、本製品は出荷時設定に戻ります。ご注意ください。

③ 親機のSERVERランプが点灯したことを確認

④ 子機のSERVERランプが消灯したことを確認

子機の SERVER ランプが消灯せず、速い点滅に変わった

ペアリングに失敗しています。もう一度手順1からやり直してください。

7 親機、子機ともにLANポートからLANケーブルを抜く

以上で、ペアリングは完了です。
次に設定画面でペアリングが正常に完了しているかどうかを確認します。

2. ペアリングが完了しているか確認します

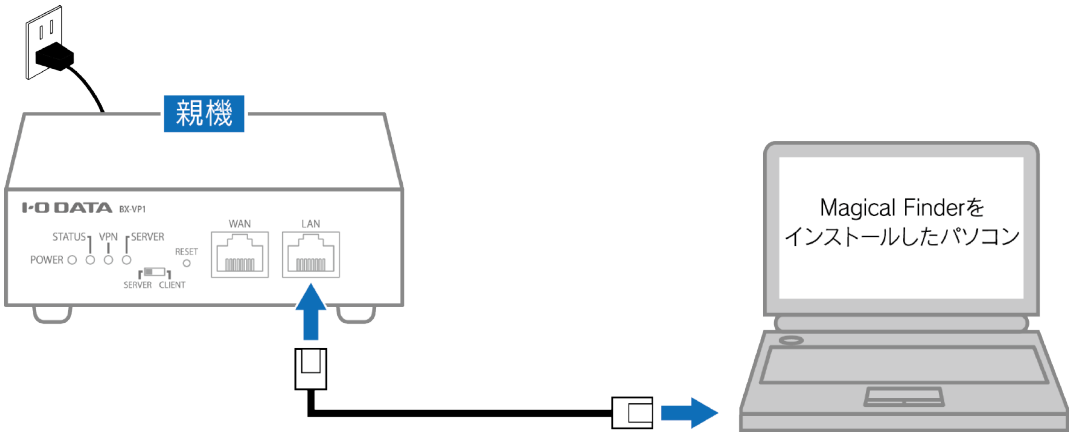
親機、子機ともに設定画面を開いて確認します。

1.Magical Finderをダウンロードする

設定画面を開くために設定アプリ「Magical Finder」(無料)をダウンロードし、利用します。
「設定画面の開き方」37 ページを参照し、ダウンロードしてください。

2.設定画面を開く

1 LANケーブルで、親機のLANポートと、パソコンのLANポートをつなぐ

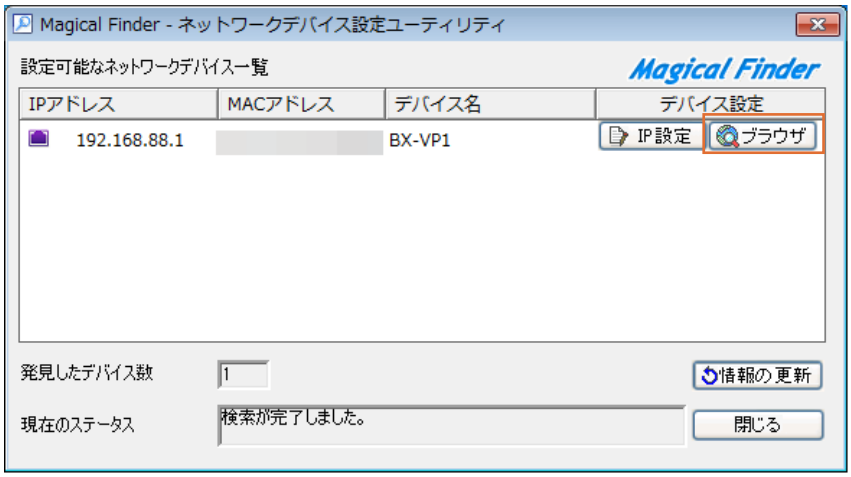


2 デスクトップ上にあるMagical Finderを起動する

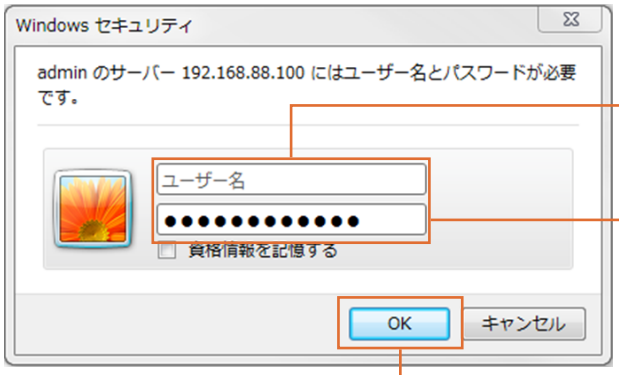
▼Windowsの場合
[mfinderXXX]フォルダを開き、[MagicalFinder.exe]をダブルクリック
※ “XXX” には数字が入ります。

▼Mac OSの場合
① [MagicalFinder for Mac XXX]→[Magical Finder]の順にダブルクリック
② インターネット上からのダウンロードファイルを開く場合の警告が表示された場合、[開く]をクリック
③ ご利用のパソコンに設定してあるパスワードを入力し、[OK]ボタンをクリック
※ “XXX” には数字が入ります。

3 親機のIPアドレスの ブラウザ （ブラウザ）ボタンをクリック



4



① [ユーザー名]は空欄のまま

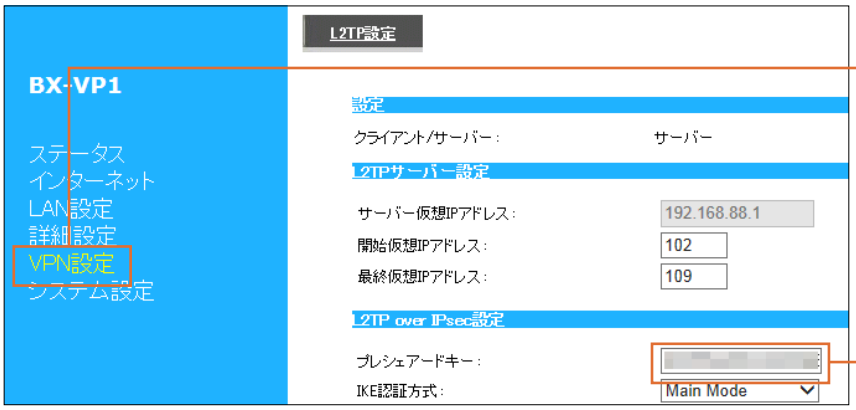
② [パスワード]に親機のMACアドレスを入力

※ MACアドレスはMagical Finderの画面、または親機底面に記載しています。
※ 半角大文字の英数字（12桁）を入力します。
※ パスワードは設定画面で変更できます。（「パスワード設定」57 ページ参照）

③ [OK]をクリック

3.プレシェアードキーを確認する

1



① [VPN設定]をクリック

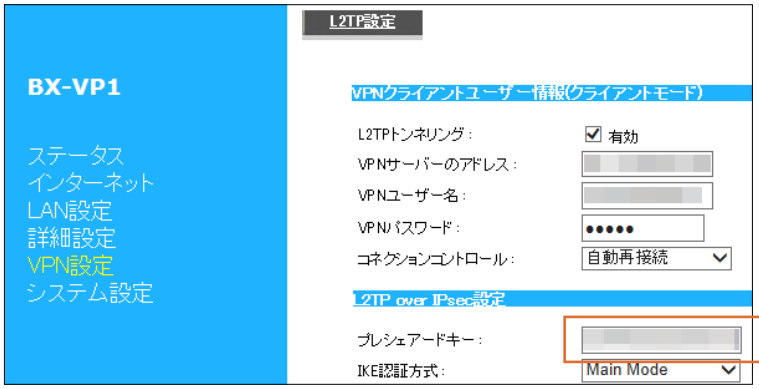
② [プレシェアードキー]をメモする

2 親機からLANケーブルを外す

3 「2.設定画面を開く」30 ページ参照の手順を、同様に子機でおこなう

4 ① [VPN設定]をクリック　② [編集]をクリック

5



[プレシェアードキー]をメモする

6 親機と子機のプレシェアードキーが同じかどうか確認する
⇒同じであればペアリング完了です。

親機と子機のプレシェアードキーが違う場合、ペアリングに失敗しています

再度、「1.親機とペアリングします」28 ページ参照の操作をおこなってください。

定期的にプレシェアードキーを変更してください

セキュリティ向上の為に、定期的にプレシェアードキーを変更することをお勧めします。(親機と子機ともに同じ内容で変更します。)
(「プレシェアードキーの変更方法」40 ページ参照)

7 子機のLANケーブル、電源コンセントを抜く

8 親機を元の状態に戻す(ルーター等とつなぎ直す)

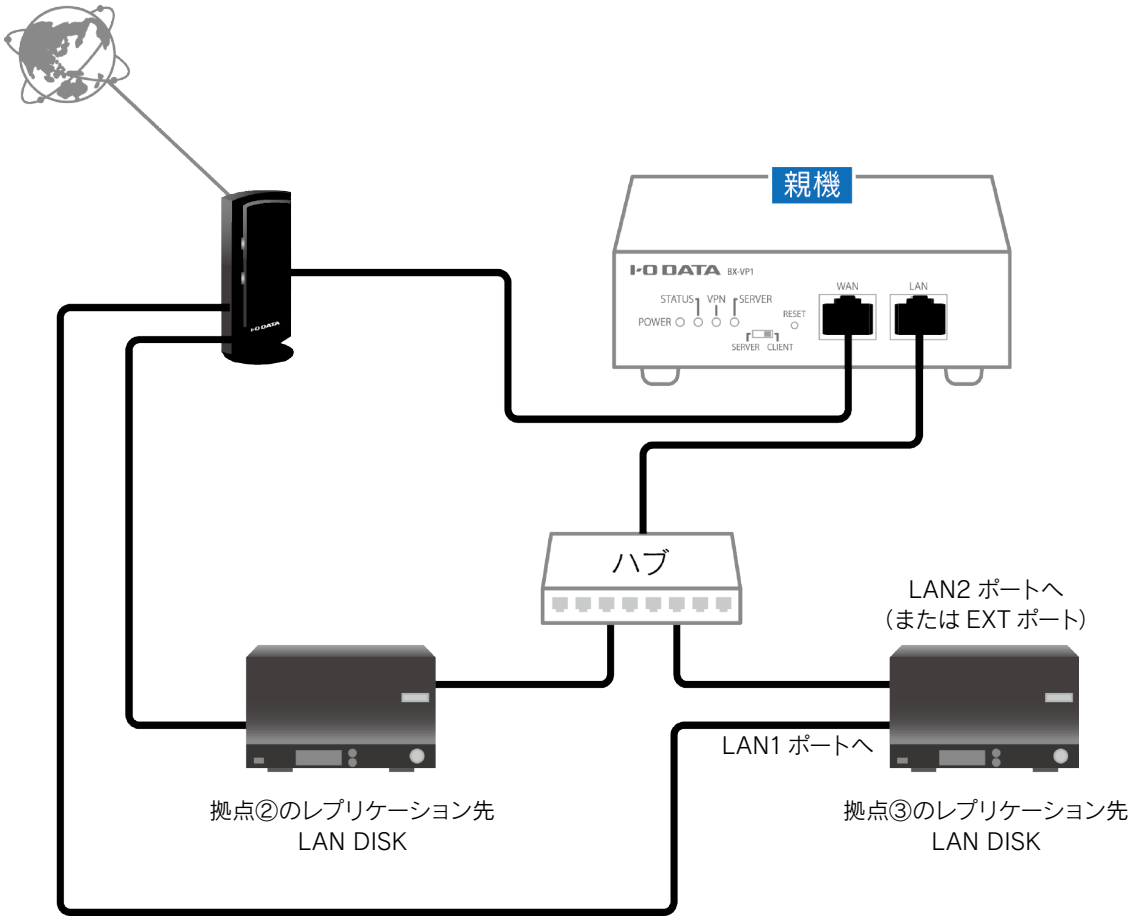
以上でペアリングは完了です。
「3.親機にLAN DISK(レプリケーション先)を増設する」33 ページへお進みください。

3.親機にLAN DISK（レプリケーション先）を増設する

1 下図のようにハブを介して、LAN DISKを追加接続する

※ LAN DISK（レプリケーション先）のIPアドレスは固定設定にしてください。
（設定方法は、ご利用のLAN DISKの取扱説明書（http://www.iodata.jp/lib/）参照）

※ 拠点③のレプリケーション先LAN DISKを設置しています。



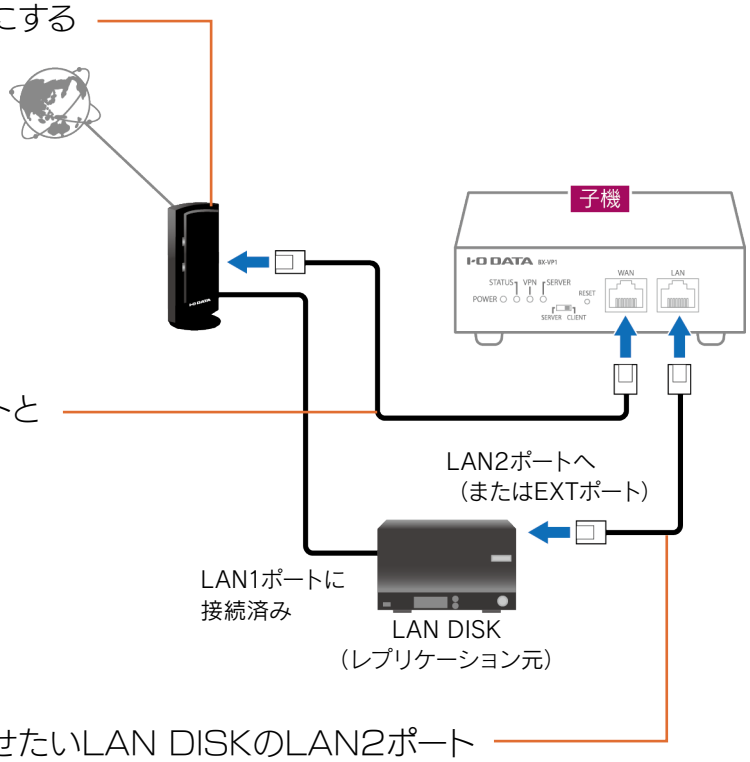
以上で、LAN DISKの増設は完了です。次に子機を設置します。

ご注意　初回レプリケーションには時間がかかります

業務に支障が少ない時間帯におこなうか、ローカル環境にておこなうことをお勧めします。
（「ご注意　レプリケーション元LAN DISKにデータがある場合は、ローカル環境でのコピーをおすすめします」9 ページ参照）

4. 拠点③に子機を設置します

1 ルーターの「IPsecパススルー」を有効にする
（設定方法は、ご利用のルーターの取扱説明書参照）

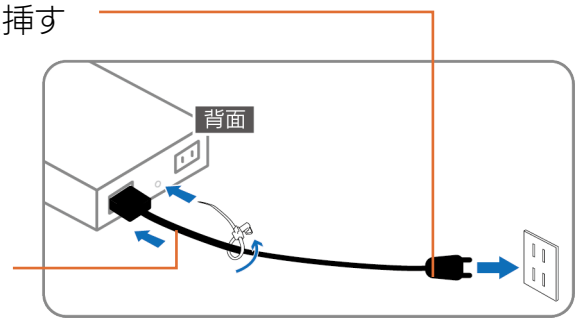


2 LANケーブルで、ルーターのLANポートと
子機のWANポートをつなぐ

3 LANケーブルで、他拠点とVPN接続させたいLAN DISKのLAN2ポート
（またはEXTポート）と子機のLANポートをつなぐ

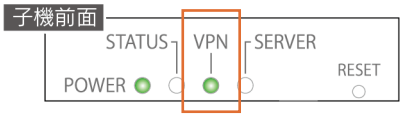
※ 本製品子機側に接続したLAN DISK（レプリケーション先）のIPアドレスは、「5.LAN DISKのレプリケーション設定をする」35 ページにしたがって設定してください。

4 添付のACケーブルを、
子機のAC100V INコネクターと電源コンセントに挿す



5 添付のACケーブルクランプを、ACケーブルに巻き、
ACケーブルクランプ取り付け穴に挿して固定する

6 子機のVPNランプが点灯していることを確認する



以上で、子機の設置は完了です。次にLAN DISKの設定をします。

VPN 対地数（本製品親機との接続可能数）

本製品子機：2台まで（※）
その他デバイスを含めて同時合計4台まで推奨
（※）本製品子機の配下に接続できるデバイスは、1台のみです。

【もくじ】へ

5.LAN DISK のレプリケーション設定をする

接続例2「他拠点（支社など）のファイルサーバーのレプリカを、拠点①（本社など）に集約させる場合」14 ページをご参照ください。

以上で、VPN構築は完了です。
リモートレプリケーションやリモートアクセスをご利用ください。

ご注意　初回レプリケーションには時間がかかります

業務に支障が少ない時間帯におこなうか、ローカル環境にておこなうことをお勧めします。
（「ご注意　レプリケーション元LAN DISKにデータがある場合は、ローカル環境でのコピーをおすすめします」9 ページ参照）

レプリケーション先の指定は IP アドレスで設定してください

弊社製「HDL-Z シリーズ」にて DFS レプリケーションをご利用の場合、インターネット越しにアクティブディレクトリに参加する必要があります

ネットワーク管理者にご相談ください。

拠点①から拠点②の LAN DISK をリモートアクセスで設定する場合

HDL-Zシリーズでは、液晶モニター、キーボード、マウスをHDL-Zシリーズに接続して設定してください。
HDL-Zシリーズ以外では、親機のLANポートにハブをつなげて、LAN DISKとパソコンを接続して設定してください。

子機に接続した LAN DISK の IP アドレス

「192.168.88.110」または「192.168.88.111」に固定してください。
既にIPアドレスを固定していた場合は、上記のいずれかの値に変更してください。

親機に接続した LAN DISK の設定は、拠点①のルーターに接続しているパソコンからおこなえます

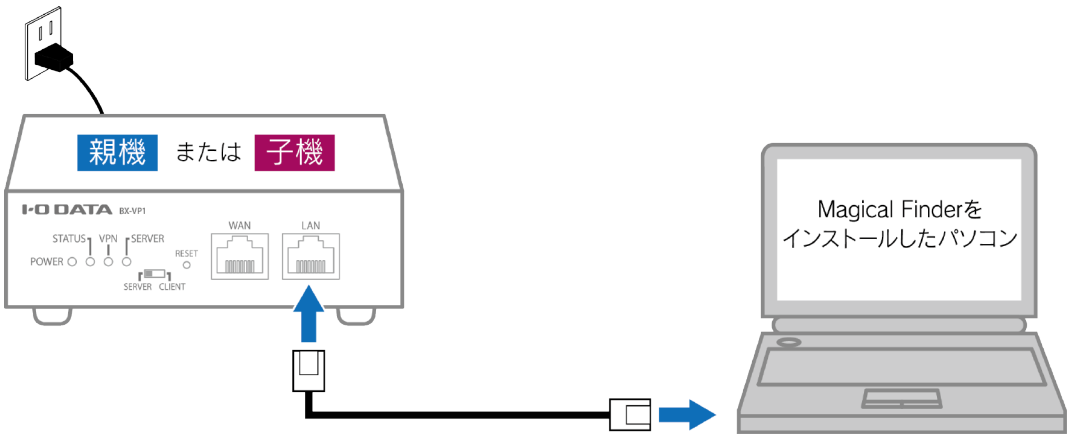
詳細設定

設定画面の開き方

設定画面では、本製品の詳細な設定や変更などがおこなえます。「Magical Finder」（無料）をダウンロードし、インストールして利用します。（Magical Finderは最新版をご利用ください。）

準備

1 LANケーブルで、親機または子機のLANポートと、パソコンのLANポートをつなぐ



以上で準備は完了です。
次に「Windowsの場合」38 ページまたは「Mac OSの場合」39 ページにお進みください。

Windows の場合

1

① Webブラウザー（Internet Explorerなど）から“http://www.iodata.jp/r/3022”にアクセス

② ご利用のOSを選択

2 [ダウンロード]をクリック

3 [実行]をクリック

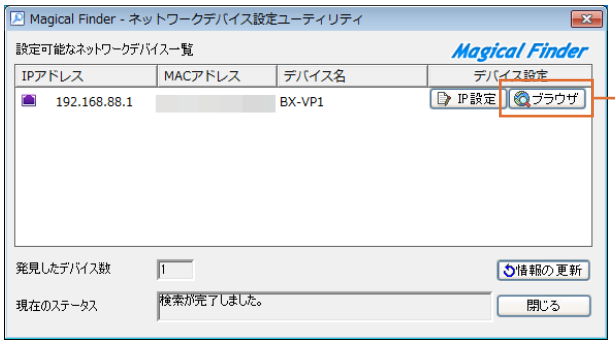
4 デスクトップ上にダウンロードした[mfinderXXX.exe]ファイルをダブルクリック

※ “XXX” には数字が入ります。

5 [mfinderXXX]フォルダを開き、[MagicalFinder.exe]をダブルクリック

※ “XXX” には数字が入ります。

6



本製品のIPアドレスの ブラウザ （ブラウザ）ボタンをクリック

7

① [ユーザー名]は空欄のまま

② [パスワード]に本製品のMACアドレスを入力

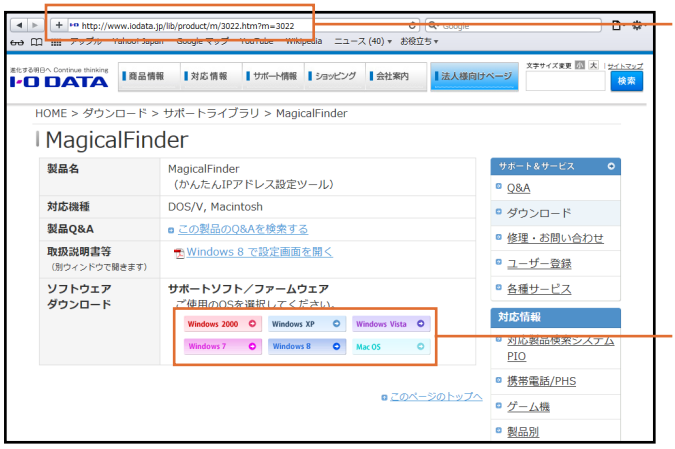
※ MACアドレスはMagical Finderの画面、または本製品底面に記載しています。
※ 半角大文字の英数字（12桁）を入力します。
※ パスワードは設定画面で変更できます。（「パスワード設定」57 ページ参照）

③ [OK]をクリック

以上で、設定画面が表示されます。
設定画面の詳細については、「設定画面のリファレンス」48 ページをご覧ください。

Mac OS の場合

1



① Webブラウザー（Internet Explorerなど）から“http://www.iodata.jp/r/3022”にアクセス

② ご利用のOSを選択

2 [Mac OS]を選択し、[ダウンロード]をクリック

3 Dockの[ダウンロード]→[MagicalFinder_for_Mac_XXX.dmg]ファイルの順にダブルクリック

※ “XXX” には数字が入ります。

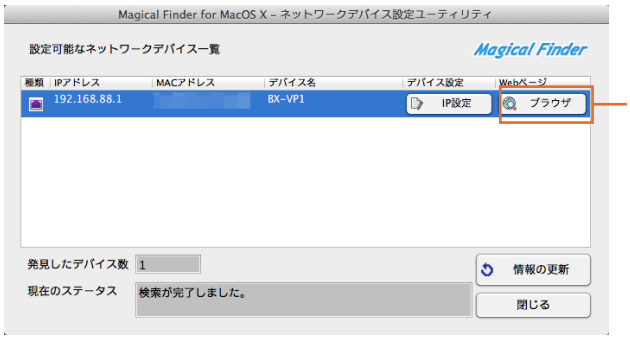
4 デスクトップ上にあるダウンロードした[MagicalFinder for Mac XXX]→[MagicalFinder]の順にダブルクリック

※ “XXX” には数字が入ります。

5 インターネット上からのダウンロードファイルを開く場合の警告が表示された場合、[開く]をクリック

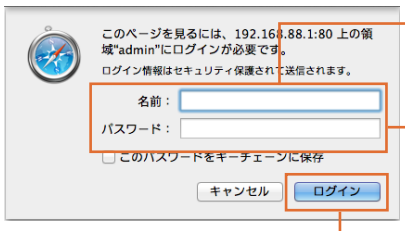
6 お使いのパソコンに設定してあるパスワードを入力し、[OK]をクリック

7



本製品のIPアドレスの ブラウザ （ブラウザ）ボタンをクリック

8



① [名前]は空欄のまま

② [パスワード]に本製品のMACアドレスを入力

※ MACアドレスはMagical Finderの画面、または本製品底面に記載しています。
※ 半角大文字の英数字（12桁）を入力します。
※ パスワードは設定画面で変更できます。（「パスワード設定」57 ページ参照）

③ [OK]をクリック

以上で、設定画面が表示されます。
設定画面の詳細については、「設定画面のリファレンス」48 ページをご覧ください。

プレシェアードキーの変更方法

セキュリティ向上の為に、定期的にプレシェアードキーを変更することをお勧めします。
親機と子機ともに同じ文字列で変更します。以下の操作を親機、子機の両方でおこなってください。

1 設定画面を開く(「設定画面の開き方」37 ページ参照)

2 ① [VPN設定]をクリック　② 子機の場合は、[編集]をクリック
（親機の場合は、手順3へ進む）

3 ① 任意の[プレシェアードキー]を入力する　② [設定]をクリック

※ 親機と子機ともに同じ文字列を入力してください。

⇒ 画面が元に戻るまでしばらくお待ちください。

4 本製品を元の接続状態に戻す（ルーター等とつなぎ直す）

5 まだプレシェアードキーを変更していない親機または子機で同様に、手順1から操作する

すべての親機、子機で同じプレシェアードキーに変更が完了したら、以上で設定は完了です。

プレシェアードキーを変更すると、VPN 接続していた端末は使用できなくなります

以下のいずれかの方法で接続してください。

- 設定画面の[VPN設定]メニューの[ユーザーリスト]にて[QRコード]をクリックして新しいQRコードを表示し、「VPNコネクト」アプリで読み込む（「VPN設定」52 ページ参照）
- 手動で接続する

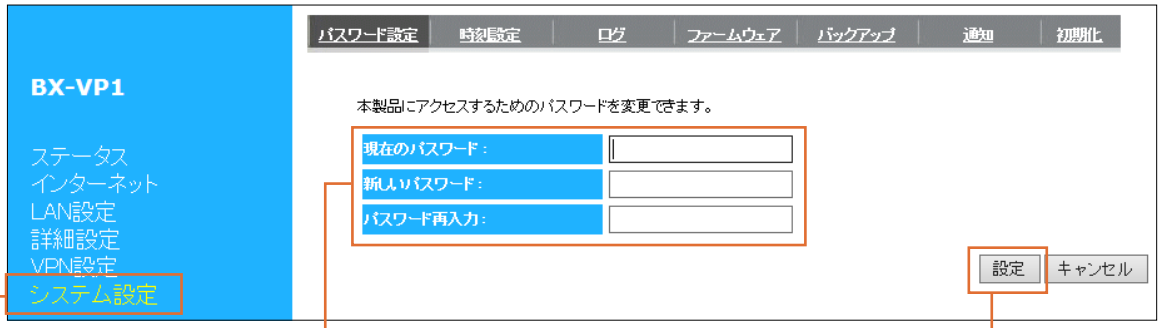
「VPNコネクトを使わずにVPNを設定したい」65ページ参照

パスワードの変更方法

セキュリティ向上の為に、設定画面のパスワードを変更することをお勧めします。
（設定画面のパスワードの出荷時設定は、本製品のMACアドレスです。）

1 設定画面を開く（「設定画面の開き方」37 ページ参照）

2 ① [システム設定]をクリック



② 入力する

③ [設定]をクリック

現在のパスワード	現在使用しているパスワードを入力します。 ※ パスワードの出荷時設定は親機または子機のMACアドレスです。 ※ MACアドレスはMagical Finderの画面、または本製品底面に記載しています。 ※ 半角大文字の英数字（12桁）を入力します。
新しいパスワード	変更するパスワードを入力します。
パスワード再入力	確認のため、[パスワード]と同じパスワードを入力します。

以上で設定画面のパスワードの変更は完了です。
次回、設定画面を開く際より、新しいパスワードを入力してください。

ファームウェアのバージョンアップ方法

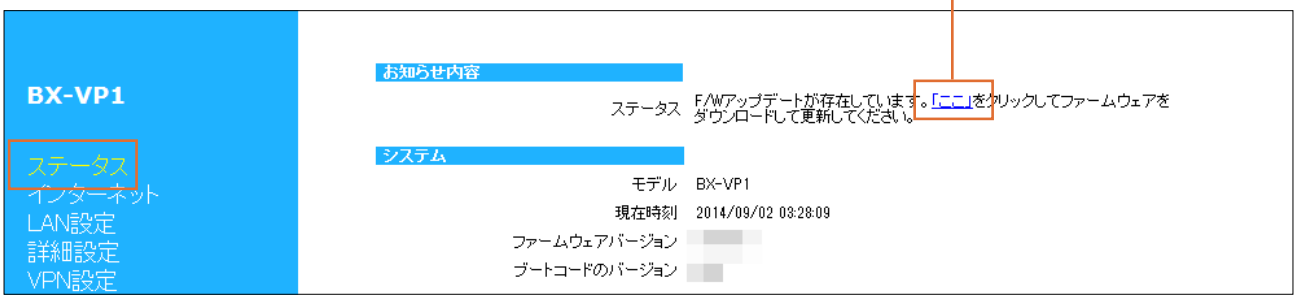
ファームウェアのバージョンアップは以下のいずれかの方法でおこなってください。

- ファームウェアの更新のお知らせを自動的に受け取り、更新内容を確認してからバージョンアップする方法（出荷時設定/「更新を確認してバージョンアップする方法」43 ページ参照）
- ファームウェアの更新を自動的に確認およびバージョンアップまでおこなう方法（「自動更新する方法」44 ページ参照）
- 弊社ホームページよりファームウェアの更新ファイルをダウンロードし、手動で更新する方法（「手動で更新する方法」45 ページ参照）

更新を確認してバージョンアップする方法

1 設定画面を開く（「設定画面の開き方」37 ページ参照）

2 [ステータス]の[お知らせ内容]に「F/Wアップデートが存在しています。…」のメッセージが表示されていたら、“「ここ」”をクリック



⇒ 自動的にファームウェアの更新ファイルのダウンロードおよびバージョンアップをおこないます。元の画面に戻るまで、しばらくお待ちください。

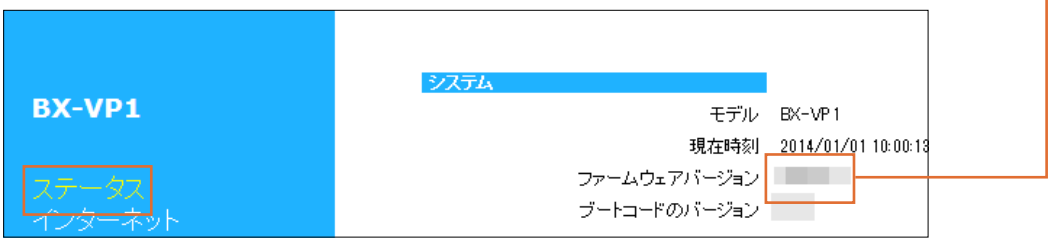
ご注意　ファームウェアのバージョンアップ中は絶対に本製品の電源を切らないでください

POWERランプ、STATUSランプの点滅中に本製品の電源を切らないでください。故障の原因となります。

ファームウェアの更新の自動確認は本体毎に月３回おこなわれます

ファームウェアの更新がある場合、STATUS ランプが点灯します

3 [ステータス]の[ファームウェアバージョン]が更新されていることを確認



以上で、ファームウェアの更新は完了です。

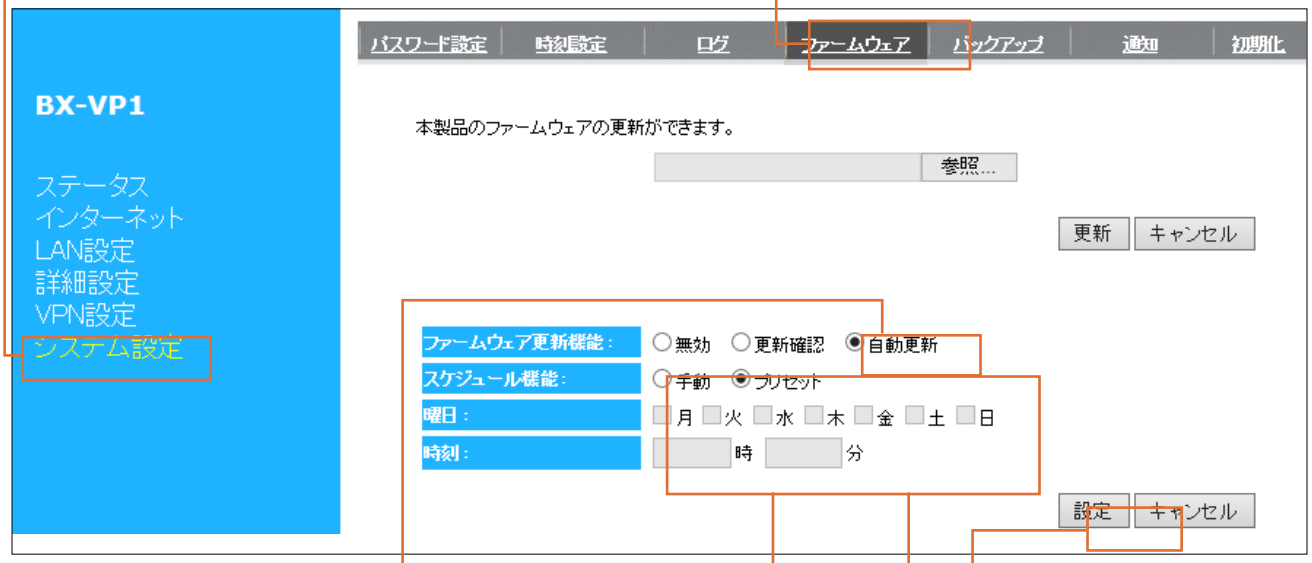
ご注意　ファームウェアのバージョンアップ中は本製品に VPN 接続できません

STATUSランプが消灯するまでお待ちください。

自動更新する方法

1 設定画面を開く(「設定画面の開き方」37 ページ参照)

2



③ [自動更新]にチェック

④ [プリセット]または[手動]を選択

⑤ [手動]を選択した場合は、ファームウェアの更新の確認をおこなう曜日、時刻を設定

⑥ [設定]をクリック

プリセットの場合、ファームウェアの更新の自動確認は本体毎に月３回おこなわれます

⇒ 元の画面に戻るまで、しばらくお待ちください。

以上で、設定は完了です。ファームウェアの更新が確認されると自動的にバージョンアップされます。

ご注意　ファームウェアのバージョンアップ中は絶対に本製品の電源を切らないでください

POWERランプ、STATUSランプの点滅中に本製品の電源を切らないでください。故障の原因となります。

ご注意　ファームウェアのバージョンアップ中は本製品に VPN 接続できません

STATUSランプが消灯するまでお待ちください。

手動で更新する方法

1 Webブラウザーに以下のURLを入力して最新のファームウェアファイルをダウンロードし、ファイルを解凍しておく

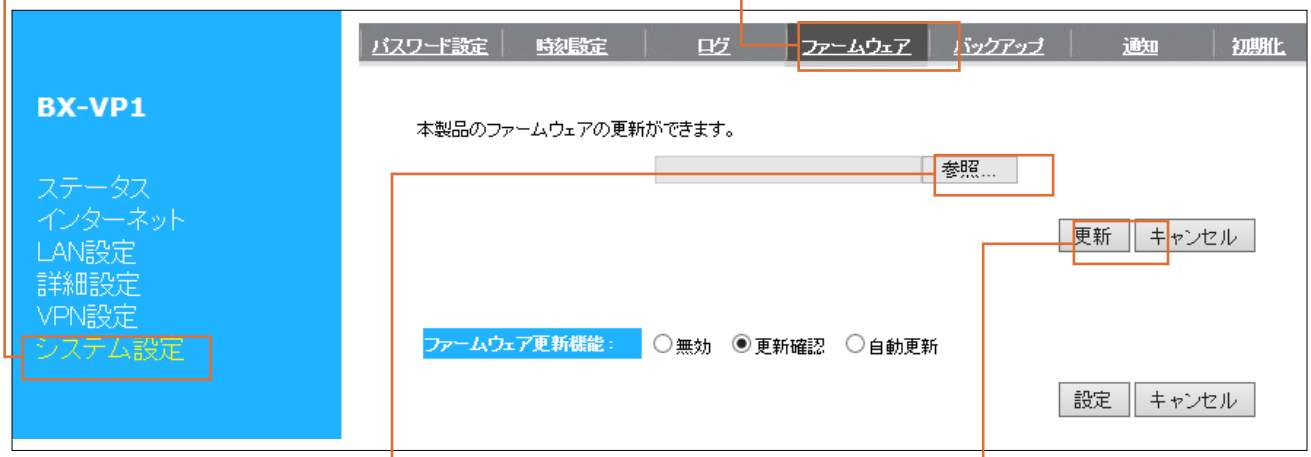
http://www.iodata.jp/lib/

（「BX-VP1-S」または「BX-VP1」を検索し、開く）

2 パソコンに常駐アプリケーションがある場合は、一時的に常駐を解除する（タスクトレイに常駐しているアイコンを右クリックして終了する）

3 設定画面を開く（「設定画面の開き方」37 ページ参照）

4 ① [システム設定]をクリック　② [ファームウェア]タブをクリック



③ [参照]をクリックし、手順1でダウンロードし解凍したファイル“BX-VP1_Vxxx.BIN”を選択

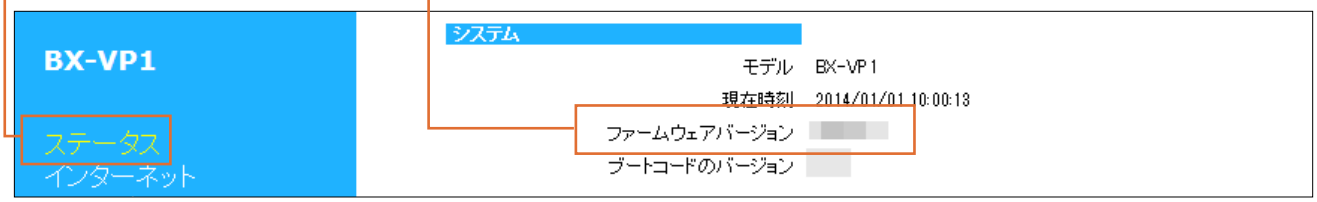
※ xxxには数字が入ります。

④ [更新]をクリック

⇒ 更新後、本製品を再起動します。元の画面に戻るまで、しばらくお待ちください。

※更新中は、絶対に本製品の電源を切らないでください。故障の原因となります。

5 ① [ステータス]をクリック　② [ファームウェアバージョン]が更新後のバージョンになっていることを確認



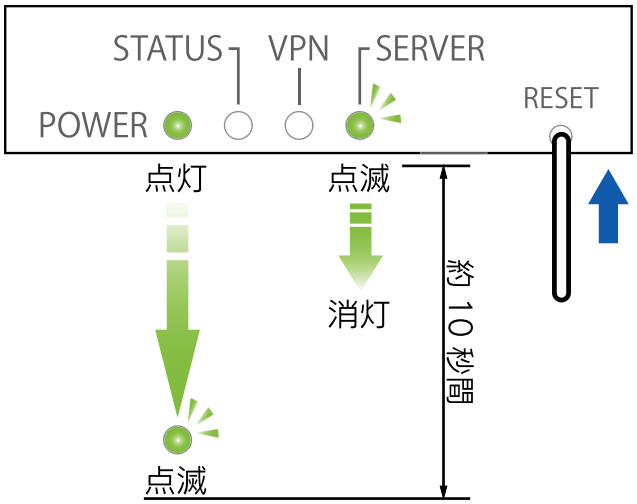
以上で、ファームウェアの更新は完了です。

設定を初期化する方法

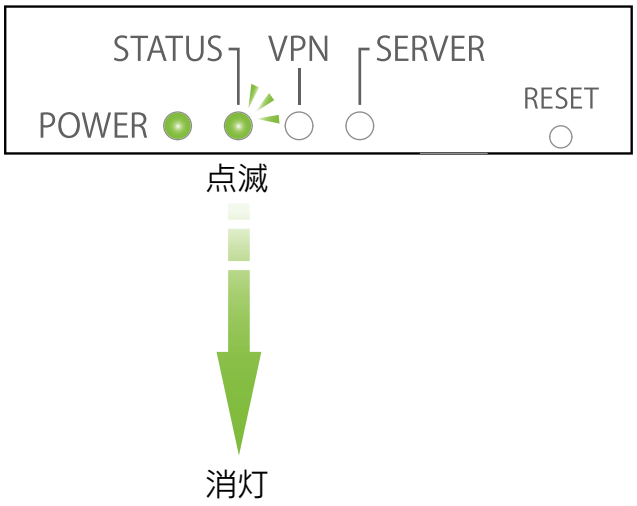
本製品の設定がすべて初期化されますので、ご注意ください。初期化方法は2通りあります。

RESET ボタンで戻す方法

1 SERVERランプが点滅→消灯になり、POWERランプが点灯→点滅になるまで、RESETボタンを長押し（約10秒間）



2 STATUSランプが点滅→消灯するまで待つ

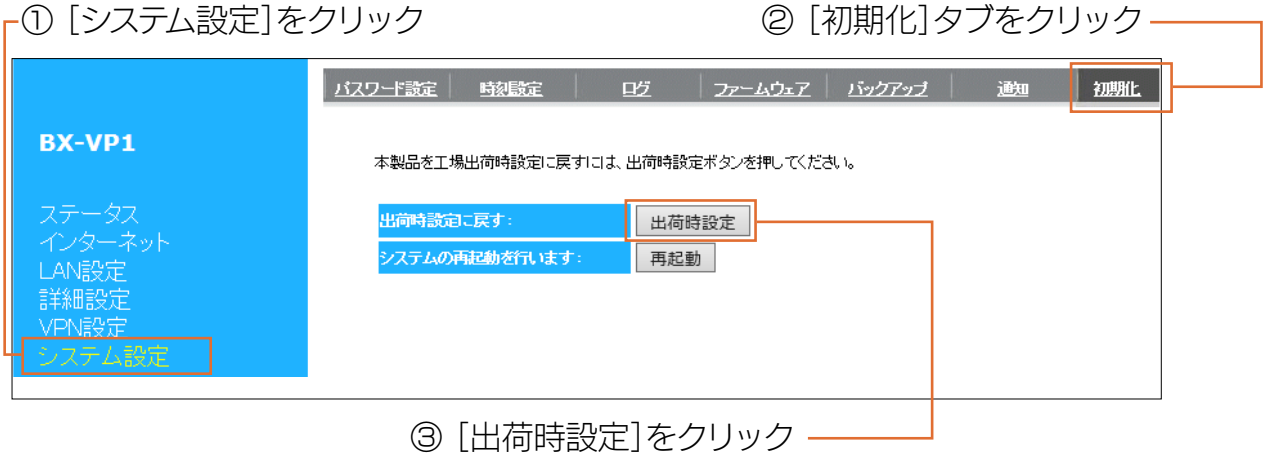


以上で初期化は完了です。
ペアリング情報も初期化されるため、再度本製品を使用する場合は親機と子機のペアリングをおこなってください。（「1.親機とペアリングします」28 ページ参照）

設定画面から戻す方法

1 設定画面を開く(「設定画面の開き方」37 ページ参照)

2 ① [システム設定]をクリック　② [初期化]タブをクリック



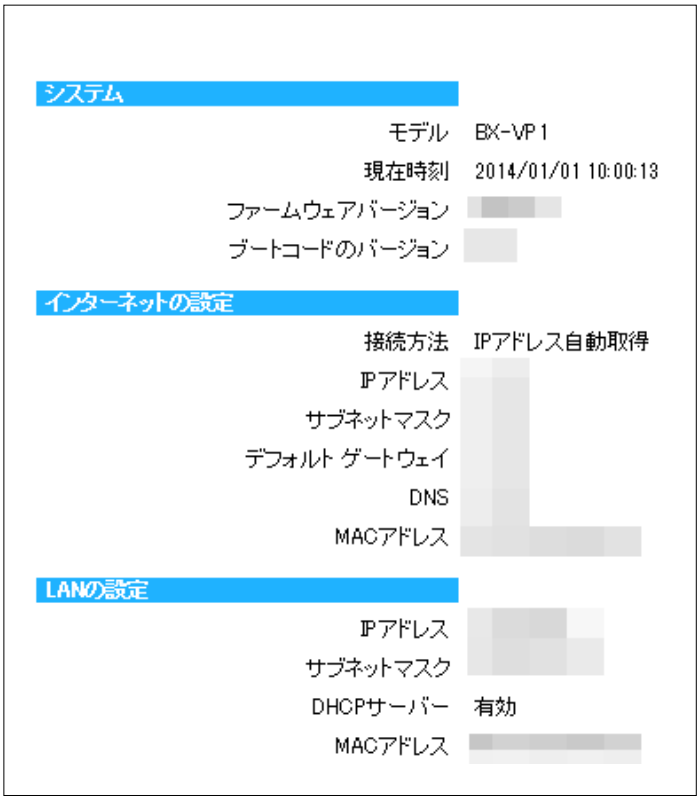
③ [出荷時設定]をクリック

⇒ 更新後、本製品を再起動します。元の画面に戻るまで、しばらくお待ちください。

※更新中は、絶対に本製品の電源を切らないでください。故障の原因となります。

以上で初期化は完了です。
ペアリング情報も初期化されるため、再度本製品を使用する場合は親機と子機のペアリングをおこなってください。(「1.親機とペアリングします」28 ページ参照)

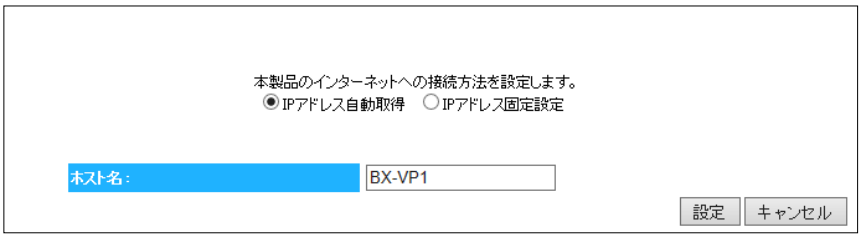
ステータス



システム	
モデル	本製品の型番を表示します。
現在時刻	現在時刻を表示します。
ファームウェアバージョン	本製品のファームウェアのバージョンを表示します。
ブートコードのバージョン	本製品のブートコードのバージョンを表示します。
インターネットの設定	
接続方法	インターネットの接続方法を表示します。
IPアドレス	インターネット側のIPアドレスを表示します。
サブネットマスク	インターネット側のサブネットマスクを表示します。
デフォルトゲートウェイ	インターネット側のゲートウェイアドレスを表示します。
DNS	使用するDNSを表示します。
MACアドレス	インターネット側のMACアドレスを表示します。
LANの設定	
IPアドレス	本製品のIPアドレスを表示します。
サブネットマスク	本製品のサブネットマスクを表示します。
DHCPサーバー	DHCPサーバーの状態を表示します。
MACアドレス	本製品のMACアドレスを表示します。

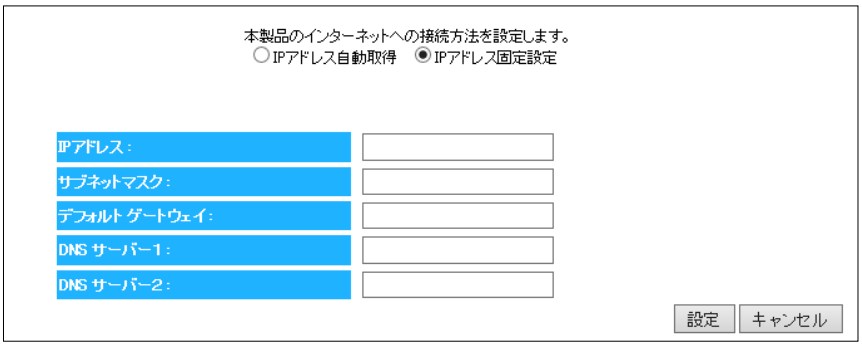
インターネット

- IPアドレス自動取得



ホスト名	ホスト名を入力します。

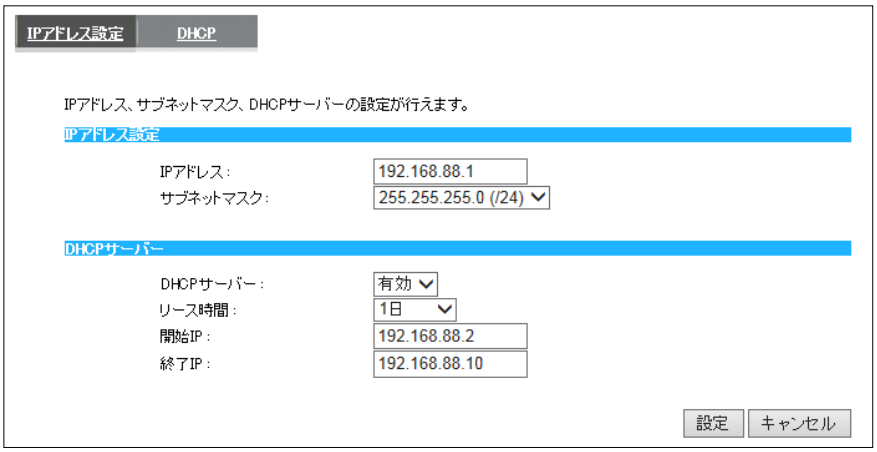
- IPアドレス固定設定



IPアドレス	プロバイダーから指定されたIPアドレスを入力します。
サブネットマスク	プロバイダーから指定されたサブネットマスクを入力します。
デフォルトゲートウェイ	プロバイダーから指定されたデフォルトゲートウェイを入力します。
DNSサーバー1	プロバイダーから指定されたDNSサーバーアドレスを入力します。
DNSサーバー2	

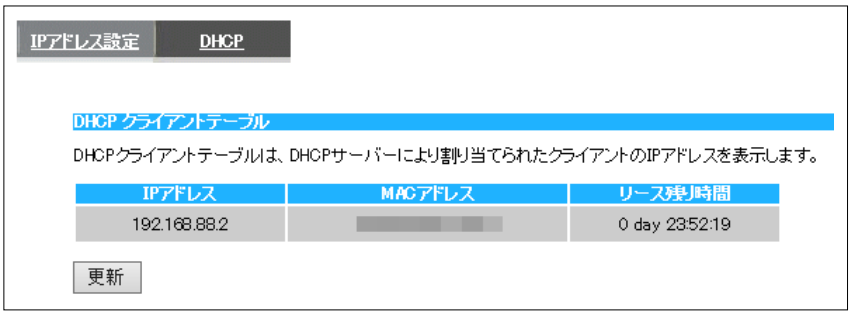
LAN 設定

IPアドレス設定



IPアドレス設定	
IPアドレス	本製品LAN側のIPアドレスを設定します。
サブネットマスク	本製品のサブネットマスクを表示します。 本製品のサブネットマスクは「255.255.255.0」で固定です。
DHCPサーバー	
DHCPサーバー	DHCPサーバー機能の[有効][無効]を選択します。[有効]にすると、本製品のLANポートに接続したパソコンのIPアドレスを自動的に割り当てます。
リース時間	IPアドレスを開放し、再取得する間隔を設定します。
開始IP	割り当てるIPアドレスの開始IPを設定します。
終了IP	割り当てるIPアドレスの終了IPを設定します。

DHCP

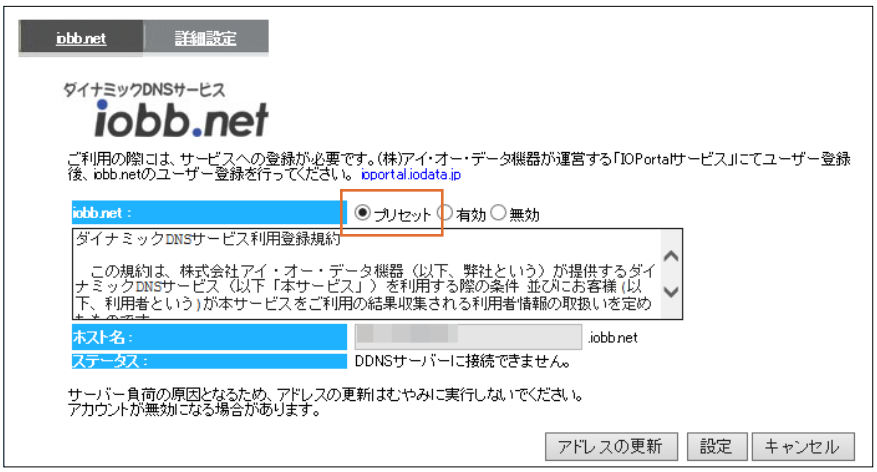


DHCPクライアントテーブル	
IPアドレス	割り当てられたIPアドレスを表示します。
MACアドレス	割り当てられたMACアドレスを表示します。
リース残り時間	IPアドレスを開放し、再取得するまでの時間を表示します。

詳細設定

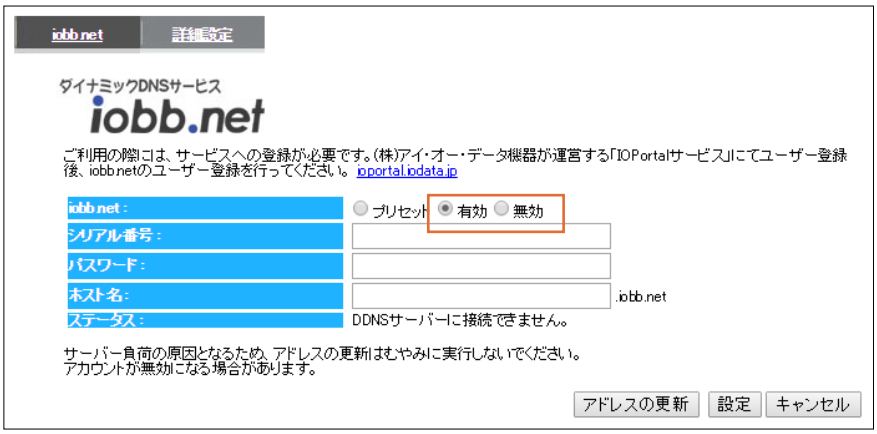
iobb.net（親機のみ表示）

- プリセットの場合



iobb.net	[プリセット]を選択します。
ホスト名	iobb.netに登録したホスト名を入力します。 xxxx.iobb.netの場合、「xxxx」のみ入力します。
ステータス	現在の状態が表示されます。

- 有効または無効の場合



iobb.net	[有効] [無効]を選択します。
シリアルナンバー	本製品のシリアル番号(S/N)(iobb.net登録に使用したもの)を入力します。 ※ 大文字英数字12桁 ※ シリアル番号(S/N)は ユーザーIDに該当します。 ※ 本製品のシリアル番号(S/N)は、本製品背面に貼られているシールにある英数字です。 (例:ABC1234567ZX)
パスワード	iobb.netに登録したパスワードを入力します。 ※ 使用可能な文字数は、6～8文字
ホスト名	iobb.netに登録したホスト名を入力します。 xxxx.iobb.netの場合、「xxxx」のみ入力します。
ステータス	現在の状態が表示されます。

詳細設定

EEE機能	有線LANの省電力モード(EEE:Energy Efficient Ehternet)の[有効] [無効]を選択します。 接続する機器により、通信がない場合に有線LANポートの切断処理がおこなわれますので、常時接続で処理をするような場合は、[無効]を選択してください。

VPN 設定

L2TP設定(親機の場合)

設定	
クライアント/サーバー	親機(サーバー)か子機(クライアント)かを表示します。
L2TPサーバー設定	
サーバー仮想IPアドレス	VPNサーバーのIPアドレスです。親機のLAN側アドレスと同じIPアドレスとなります。
開始仮想IPアドレス	VPNクライアントに割り振られるVPN上のIPアドレスの先頭のアドレスです。1～254の数値で設定します。
最終仮想IPアドレス	VPNクライアントに割り振られるVPN上のIPアドレスの最終のアドレスです。1～254の数値で設定します。

L2TP over IPsec設定		
プレシェアードキー	IPsec機器同士の認証用の事前暗号キー(1～20文字)です。 ※事前暗号キーは実際の暗号キーとは異なっています。	
変更警告	プレシェアードキーの変更を促すメッセージを表示するタイミングを設定します。	
IKE認証方式	IPsecのIKEプロトコルで使用するフェーズ1の認証方式を選択します。	
	Main Mode	接続をおこなうIPsec機器の認証設定を全く同じ設定にして、全ての認証ステップをおこなう方式。認証データは全て暗号化されているため、セキュアな方式になります。
	Agressive Mode	接続をおこなうIPsec(親機)に子機が認証方式を順々に試して認証ステップを減らすことにより、簡易な認証を可能にした方式。認証情報が一部暗号化されていませんが、再接続などの処理は高速におこなえます。

<table>
<tr><td>IKEプロトコル</td><td>IKEフェーズの認証、暗号化の設定を選択します。
<table>
<tr><td>暗号化方式</td><td>IKEプロトコル上の暗号化方式を選択します。
DES：IKEの通信をDES暗号化します。　AES-128：IKEの通信をAES 128bit暗号化します。
3DES：IKEの通信を3DES暗号化します。　AES-192：IKEの通信をAES 192bit暗号化します。
AES-256：IKEの通信をAES 256bit暗号化します。</td></tr>
<tr><td>認証方式</td><td>IKEプロトコル上の認証方式を選択します。
SHA1：認証データがSHA1がハッシュ暗号化されて通信されます。
MD5：認証データがMD5でハッシュ暗号化されて通信されます。
None：認証データが暗号化されません。</td></tr>
<tr><td>DHグループ</td><td>IKEプロトコル上のOakley 鍵交換手順を選択します。Oakley 鍵交換手順は公開鍵暗号を用いた鍵交換手順のアルゴリズムとパラメータのセットを定義したもので、アルゴリズムは大きく分けて Diffie-Hellman鍵共有 (DH-MODP) と楕円曲線暗号 (EC2N) の2種があります。本製品は、None(無効)、DH-MODPのGroup 1(768bit),Group 2(1024bit),Group 5(1536bit),Group 14(2048bit)をサポートしています。</td></tr>
</table></td></tr>
<tr><td>IPSecプロポーザル</td><td>IPsec通信の認証、暗号化の設定を選択します。
<table>
<tr><td>暗号化方式</td><td>IPsec上の暗号化方式を選択します。
DES：IKEの通信をDES暗号化します。　AES-128：IKEの通信をAES 128bit暗号化します。
3DES：IKEの通信を3DES暗号化します。　AES-192：IKEの通信をAES 192bit暗号化します。
AES-256：IKEの通信をAES 256bit暗号化します。</td></tr>
<tr><td>認証方式</td><td>IPsec上の認証方式を選択します。
SHA1：認証データがSHA1がハッシュ暗号化されて通信されます。
MD5：認証データがMD5でハッシュ暗号化されて通信されます。
None：認証データが暗号化されません。</td></tr>
<tr><td>PFSグループ</td><td>IKEフェーズ時に作成した鍵をそのまま使用した場合に、IKEのセキュリティ状態によって鍵が漏えいする可能性があるため、IPsec通信をおこなう場合にもOakley 鍵交換をおこなった鍵を使用することができます。
Oakley 鍵交換手順は公開鍵暗号を用いた鍵交換手順のアルゴリズムとパラメータのセットを定義したもので、アルゴリズムは大きく分けて Diffie-Hellman鍵共有 (DH-MODP) と楕円曲線暗号 (EC2N) の2種があります。
本製品は、None(無効)、DH-MODPのGroup 1(768bit),Group 2(1024bit),Group 5(1536bit),Group 14(2048bit)をサポートしています。
IPsec機器(子機)では本機能が対応されていない場合があります。</td></tr>
</table></td></tr>
<tr><td>カプセリング方式</td><td>IPsecのパケットのカプセリングをおこなう方法を選択します。
AH：AH (Authentication Header) は、認証および改竄防止機能を提供します。データは暗号化されません。
ESP：ESP (Encapsulated Security Payload) は Payload 部(IP ヘッダ、経路ヘッダ、ホップバイホップオプションヘッダを除いた部分)が暗号化されます。認証は提供されません。</td></tr>
<tr><td>Dead Peer Detection（DPD）</td><td>IPsec機器の接続相手とのセッション情報を確認し、無手順でセッションが切れているとなっている場合、セッションの情報を削除する機能です。
機能の[有効][無効]を選択できます。
タイムアウト時間：VPN上の最後の通信からのタイムアウト時間(60～3600)
遅延時間：通信相手から返答で許容できる遅延時間(10～3600)</td></tr>
<tr><td>新しいWindowsからの接続を許可</td><td>Windows 7以降のWindowsからの接続を許可する場合、選択してください。</td></tr>
<tr><td>古いWindows/Mac OSからの接続を許可</td><td>Windows Vista/Mac OS 10.6の接続を許可する場合、選択してください。
本オプションを選択した場合、IKEフェーズでの暗号化レベルが弱いものでも接続が可能な状態になります。
Windows Vista/Mac OS 10.6を接続したいとき以外は選択をしないことをお勧めします。</td></tr>
<tr><td>QRコードの有効期限（発効日より）</td><td>QRコードを使うことができる期限を設定します。
設定した期間が過ぎると、QRコードを利用できなくなります。</td></tr>
<tr><td colspan="2">L2TPサーバーステータス</td></tr>
<tr><td>ユーザー名</td><td>接続をしてきているL2TPのユーザー名を表示します。</td></tr>
<tr><td>ピアIP</td><td>接続をしているVPNクライアントのIPアドレスを表示します。</td></tr>
<tr><td>仮想IP</td><td>接続をしているVPNクライアントのVPN上のIPアドレスを表示します。</td></tr>
<tr><td>ピアコールID</td><td>接続をしているVPNクライアントとの接続IDを表示します。</td></tr>
<tr><td colspan="2">ユーザーリスト</td></tr>
<tr><td>ユーザー名</td><td>VPNユーザー名（1～20文字）</td></tr>
<tr><td>パスワード</td><td>VPNユーザーのパスワード（1～32文字）</td></tr>
<tr><td>アカウント</td><td>VPNユーザーのアカウントを有効にするかのチェックをします。</td></tr>
<tr><td>処理</td><td>[編集]ユーザー情報の編集（ユーザーアカウント設定）をします。
[QRコード]VPNコネクト用のユーザー情報とVPN情報の入ったQRコードを表示します。</td></tr>
</table>

- ユーザーアカウント設定（ユーザー情報の編集）

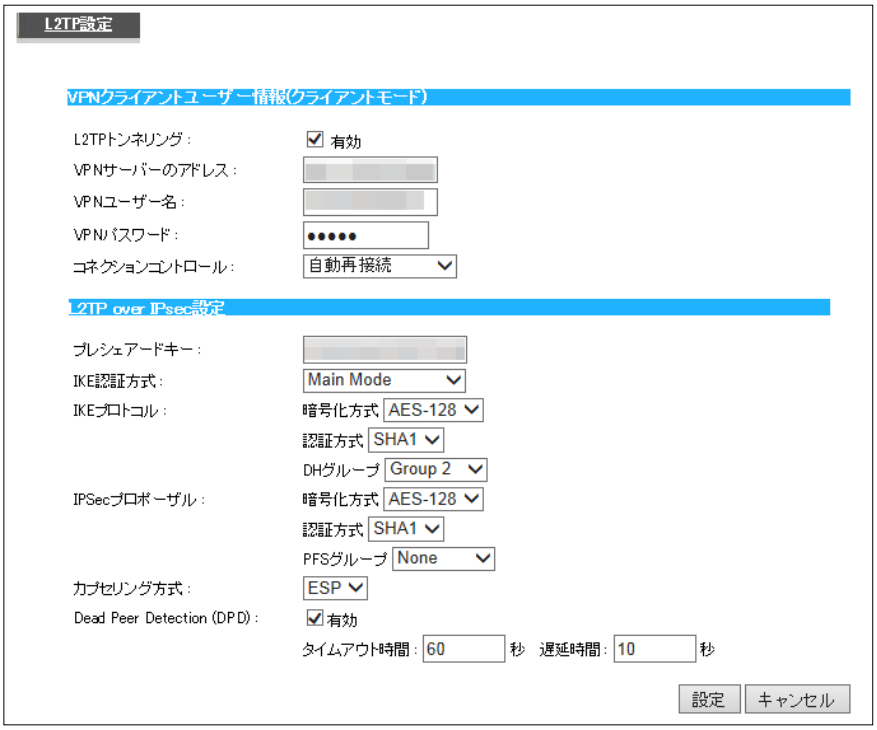
ユーザーアカウント設定	
ユーザー名	VPNユーザーのユーザー名を設定します。（1～20文字）
パスワード	VPNユーザーのパスワードを設定します。（1～32文字）
アカウント	VPNユーザーのアカウントを有効にするかのチェックをします。
ゲスト機能※	［有効］にすると、下で設定された曜日、時刻でパスワード（パスコード）が自動的に変更されます。
待ち受けポート番号※	ゲスト機能でVPNコネクトからの待ち受けを行うポート番号です。 上位ルーターがUPnPに対応していない場合、手動で本ポートのTCPを開放してください。
曜日※	パスワード（パスコード）が変更される曜日を設定します。
時刻※	パスワード（パスコード）が変更される時刻を設定します。

※NO.1のVPNユーザーを編集した場合のみ表示されます。NO.1のVPNユーザーは購入時すでに設定されています。

L2TP設定(子機の場合)

設定	
クライアント/サーバー	親機(サーバー)か子機(クライアント)かを表示します。
L2TPクライアント設定	
L2TPクライアントステータス	子機のVPNのステータスを表示します。[編集]をクリックすると編集画面を表示します。

- 編集画面



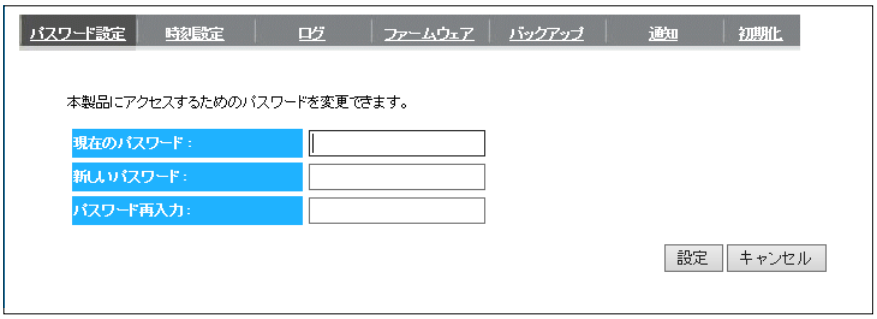
L2TPクライアント情報 (クライアントモード)	
L2TPトンネリング	L2TPトンネリングをおこなう場合、チェックしてください。
VPNサーバーのアドレス	接続を行うVPNサーバーのアドレス(1～32文字)を設定します。 URLまたは、IPアドレスを設定します。
VPNユーザー名	接続を行うVPNサーバーに登録されたユーザー名(1～20文字)を入力します。
VPNパスワード	接続をおこなうVPNサーバーに登録されたユーザーのパスワード(1～32文字)を入力します。
コネクションコントロール	VPN接続をおこなう方法を選択します。 自動再接続:自動で接続を再接続をおこない続けます。 オンデマンド接続:LAN側の子機からのアクセスがあった場合に接続処理をおこないます。 手動接続:手動で接続をおこないます。

L2TP over IPsec設定	
プレシェアードキー	IPsec機器同士の認証用の事前暗号キー(1～20文字)です。親機の設定に合わせてください。 ※事前暗号キーは実際の暗号キーとは異なっています。
IKE認証方式	IPsecのIKEプロトコルで使用するフェーズ1の認証方式を選択します。親機の設定に合わせてください。 Main Mode:接続をおこなうIPsec機器の認証設定を全く同じ設定にして、全ての認証ステップをおこなう方式。認証データは全て暗号化されているため、セキュアな方式になります。 Agressive Mode:接続をおこなうIPsec(親機)に子機が認証方式を順々に試して認証ステップを減らすことにより、簡易な認証を可能にした方式。認証情報が一部暗号化されていませんが、再接続などの処理は高速におこなえます。
IKEプロトコル	IKEフェーズの認証、暗号化の設定を選択します。 暗号化方式:IKEプロトコル上の暗号化方式を選択します。 AES-128:IKEの通信をAES 128bit暗号化します。 DES:IKEの通信をDES暗号化します。 AES-192:IKEの通信をAES 192bit暗号化します。 3DES:IKEの通信を3DES暗号化します。 AES-256:IKEの通信をAES 256bit暗号化します。 認証方式:IKEプロトコル上の認証方式を選択します。 SHA1:認証データがSHA1がハッシュ暗号化されて通信されます。 MD5:認証データがMD5でハッシュ暗号化されて通信されます。 None:認証データが暗号化されません。 DHグループ:IKEプロトコル上のOakley 鍵交換手順を選択します。Oakley 鍵交換手順は公開鍵暗号を用いた鍵交換手順のアルゴリズムとパラメータのセットを定義したもので、アルゴリズムは大きく分けて Diffie-Hellman 鍵共有 (DH-MODP) と楕円曲線暗号 (EC2N) の2種があります。本製品は、None(無効)、DH-MODPのGroup 1(768bit),Group 2(1024bit),Group 5(1536bit),Group 14(2048bit)をサポートしています。

<table>
<tr><td>IPSecプロポーザル</td><td>IPsec通信の認証、暗号化の設定を選択します。<table>
<tr><td>暗号化方式</td><td>IPsec上の暗号化方式を選択します。
DES：IKEの通信をDES暗号化します。
3DES：IKEの通信を3DES暗号化します。</td></tr>
<tr><td>認証方式</td><td>IPsec上の認証方式を選択します。
SHA1：認証データがSHA1がハッシュ暗号化されて通信されます。
MD5：認証データがMD5でハッシュ暗号化されて通信されます。
None：認証データが暗号化されません。</td></tr>
<tr><td>PFSグループ</td><td>IKEフェーズ時に作成した鍵をそのまま使用した場合に、IKEのセキュリティ状態によって鍵が漏えいする可能性があるため、IPsec通信をおこなう場合にもOakley 鍵交換をおこなった鍵を使用することができます。
Oakley 鍵交換手順は公開鍵暗号を用いた鍵交換手順のアルゴリズムとパラメータのセットを定義したもので、アルゴリズムは大きく分けて Diffie-Hellman鍵共有 (DH-MODP) と楕円曲線暗号 (EC2N) の2種があります。
本製品は、None(無効)、DH-MODPのGroup 1(768bit),Group 2(1024bit),Group 5(1536bit),Group 14(2048bit)をサポートしています。
IPsec機器(子機)では本機能が対応されていない場合があります。</td></tr>
</table></td></tr>
<tr><td>カプセリング方式</td><td>IPsecのパケットのカプセリングをおこなう方法を選択します。親機の設定に合わせてください。
AH：AH (Authentication Header) は、認証および改竄防止機能を提供します。データは暗号化されません。
ESP：ESP (Encapsulated Security Payload) は Payload 部(IP ヘッダ、経路ヘッダ、ホップバイホップオプションヘッダを除いた部分)が暗号化されます。認証は提供されません。</td></tr>
<tr><td>Dead Peer Detection
(DPD)</td><td>IPsec機器の接続相手とのセッション情報を確認し、無手順でセッションが切れているとなっている場合、セッションの情報を削除する機能です。
機能の[有効][無効]を選択できます。
タイムアウト時間：VPN上の最後の通信からのタイムアウト時間(60～3600)
遅延時間：通信相手から返答で許容できる遅延時間(10～3600)</td></tr>
</table>

システム設定

パスワード設定



現在のパスワード	現在使用しているパスワードを入力します。 ※ パスワードの出荷時設定は親機または子機のMACアドレスです。 ※ MACアドレスはMagical Finderの画面、または本製品底面に記載しています。 ※ 半角大文字の英数字(12桁)を入力します。
新しいパスワード	変更するパスワード(最大32文字)を入力します。
パスワード再入力	確認のため、[パスワード]と同じパスワードを入力します。

時刻設定

現在の日時情報	
日付	現在の日付を表示します。
時刻	現在の時刻を表示します。
日時の設定	
手動設定	手動で、現在の日付と時刻を設定します。
NTPサーバーから取得	時刻を入手するURLを選択します。

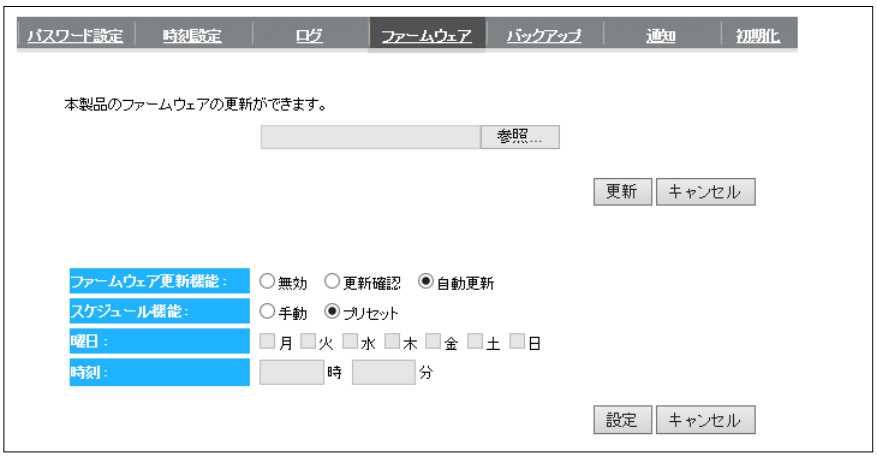
ログ

ログを表示します。表示されたログのファイル保存、削除、表示の更新がおこなえます。

ファームウェア

- 更新確認または無効の場合

- 自動更新の場合



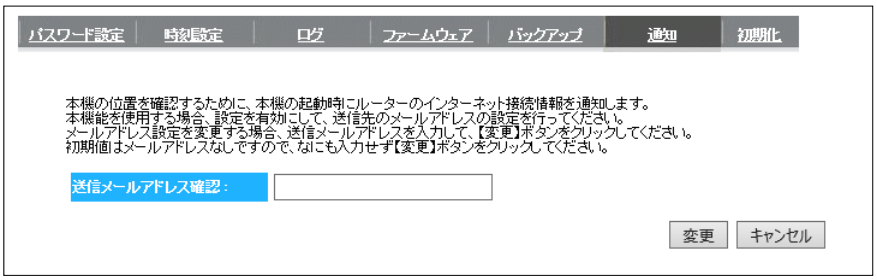
本製品のファームウェアの更新がおこなえます。 手動で更新する場合は、[参照]ボタンをクリックし、事前にダウンロードしたファームウェアファイルを指定して、[更新]をクリックします。		
ファームウェア更新機能	ファームウェアの更新方法を選択します。	
	無効	自動更新および自動で更新の確認はおこないません。
	更新確認 (出荷時設定)	自動でファームウェアの更新があるかどうか確認します。また、ファームウェアの更新がある場合は、確認画面を表示します。
	自動更新	自動でファームウェアの更新があるかどうか確認します。また、ファームウェアの更新がある場合は、自動的にファームウェアの更新を開始します。
スケジュール機能(自動更新の場合のみ)	[ファームウェアの更新機能]で[自動更新]を選択した場合に、更新を確認するスケジュールを設定します。 手動:更新を確認する曜日と時刻を設定します。 プリセット:月3回更新を自動で確認します。	

バックアップ

設定の保存	[保存]を押すと、本製品の各種設定情報をファイルに保存できます。 (保存先を選択し、[config.bin]ファイルを保存します。)
設定の復元	[設定の保存]で保存したファイルから本製品の各種設定情報を読み込み、復元します。 [参照]を押し、[設定の保存]で保存したファイルを読み込み、[復元]を押します。

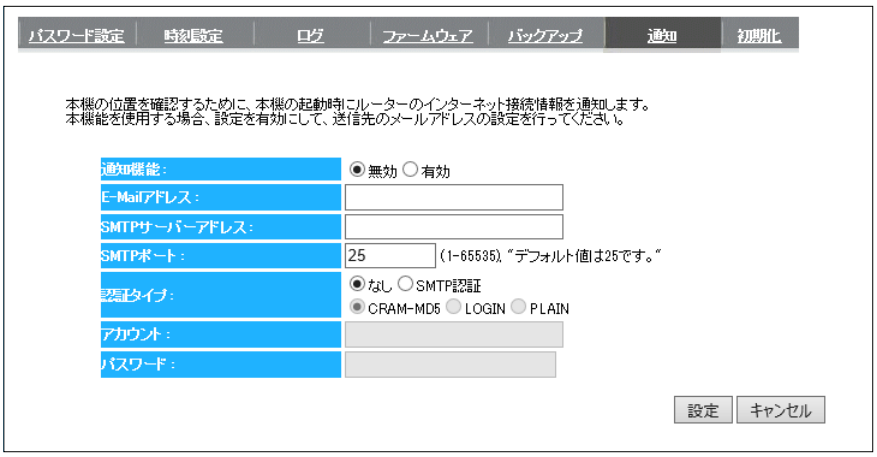
通知

- 送信メールアドレス確認



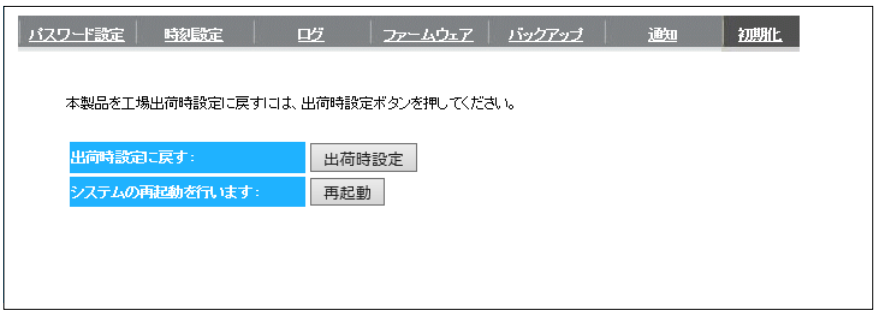
現在設定されている送信メールアドレスを入力し、[変更]をクリックすることでメールアドレスを設定できます。 ※初期値はメールアドレスなしです。 何も入力せずに[変更]をクリックすれば、メールアドレスを設定できます。

- メールアドレス設定



本製品が起動した時にグローバルIPアドレスが前回と異なる場合、設定したメールアドレスにインターネット接続状況を通知します。	
通知機能	[有効]にすると、インターネット接続状況を通知するようになります。
E-Mail アドレス	通知するメールアドレスを設定します。
SMTP サーバー アドレス	親機がメールを送信する際に利用するSMTPサーバーのアドレスを設定します。
SMTP ポート	SMTPサーバーと通信する際のポートを設定します。
認証タイプ	メール送信時の認証タイプを設定します。
アカウント	メールのアカウントを設定します。
パスワード	設定したアカウントのパスワードを設定します。

初期化

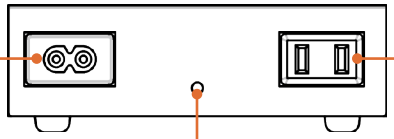


出荷時設定に戻す	[出荷時設定]を押すと、本製品の各種設定情報が出荷時設定に戻り、ペアリング情報が初期化されます。 再度本製品を使用する場合は、以下のいずれかをおこなってください。 ・親機と子機のペアリングをおこなう。 ・初期化前に[バックアップ]メニューから親機、子機の設定の保存をおこなっておき、初期化後、設定の復元をおこなう。
システムの再起動を行います	本製品を再起動します。 ※数分かかる場合があります。

仕様

各部の名前と機能

▼背面



AC100V IN コネクター

添付のACケーブルを接続します。

AC ケーブルクランプ取り付け穴

AC100V 最大 200W 非連動コネクター

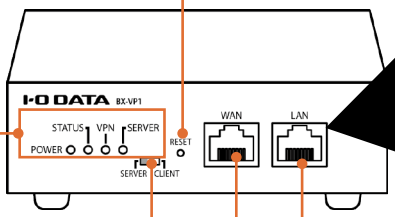
サービスコンセントです。

> 最大200W以内で使用し、たこ足配線はしないでください
>
> 200Wを超えて使用すると、過熱し、火災の原因になります。

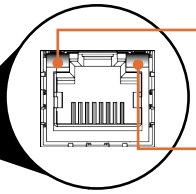
RESET ボタン

約3秒長押し：親機と子機間でペアリングをおこないます。
約10秒以上長押し：出荷時設定に戻します。
（「RESETボタンで戻す方法」46 ページ参照）

▼前面



▼ポート拡大図



LINK/ACT ランプ

緑点灯：機器を接続状態
緑点滅：機器に通信中

GIGA ランプ

橙点灯：1000BASE-Tで機器と通信中

LAN ポート

ＶＰＮ接続させたいNASとつなぎます。
または本製品の親機と子機をペアリングする際に使用します。

WAN ポート

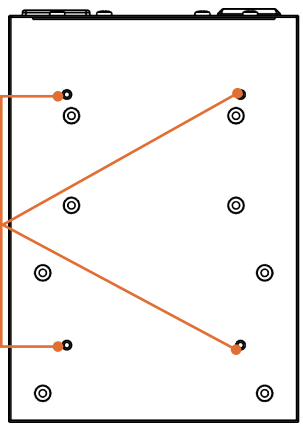
ルーターとつなぎ、本製品の親機と子機間でVPN接続します。

SERVER/CLIENT 切替スイッチ

スイッチを切り替え、電源を入れ直すと本製品のモードが切り替わります。
SERVER：親機として使用時
CLIENT：子機として使用時

ランプ	動作	概要
POWER	点灯	電源オン時
	点滅	設定初期化開始
	消灯	電源オフ時
STATUS	点灯	ファームウェアアップデートがあることのお知らせ
	遅い点滅	起動中
	速い点滅	設定初期化中
	消灯	通常動作時
VPN	点灯	親機と子機間でVPN接続中
	消灯	VPN接続していない状態
SERVER	点灯	親機として使用時
	遅い点滅	親機と子機間でペアリング中
	速い点滅	ペアリング失敗（子機のみ）
	消灯	子機として使用時

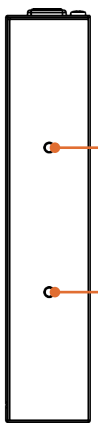
▼底面



マグネット取り付け位置

別売のマグネットキット「NB-OP/MAG」（4個入）を取り付けることができます。

▼側面



壁掛け用金具取り付けネジ穴

仕様

VPN接続方式	L2TP over IPSec
L2TP	L2TP v2、認証方式(MS-CHAP v2)、暗号化なし
IPSecトンネリング機能	パスフレーズ方式、IKE v1、カプセル方式(ESP、AH)、認証方式(なし、MD5、SHA1)、暗号化方式(※)(DES、3DES、AES 128bit、AES 192bit、AES 256bit)、DH Group(なし、1、2、5、14)、PFS(なし、1、2、5、14)、NAT Traversal (※)出荷時は、AES 128bitに設定されています。
VPN対地数 (本製品親機との接続可能数)	本製品子機:2台まで(※) その他デバイスを含めて同時合計4台まで推奨 (※)本製品子機の配下に接続できるデバイスは、1台のみです。
IPSecスループット	最大約108Mbps(当社実測値より)
VPNクライアントOS対応	Windows 10(32/64ビット版)、Windows 8.1(32/64ビット版)、Windows 8(32/64ビット版)、 Windows 7(32/64ビット版)、Windows Vista(32/64ビット版)、Mac OS X 10.6～10.10 iOS 6～8 Android 4.0～5.1
ネットワーク共通機能	DHCPクライアント(WAN側)、固定IP(WAN側)、iobb.net(DDNS)、UPnPクライアント、 VPNサーバーモード DHCPサーバー(8台まで)、 VPNクライアントモード DHCPサーバー(1台まで)
その他機能	ペアリング(VPNクライアントの自動設定)、VPNコネクト用QRコード表示、IEEE802.3az、Magical Finder対応、 Windows版NAT Traversal設定ツール、ファームウェア自動確認・更新機能
Web設定画面	Windows:Internet Explorer 9～11 Mac OS X:Safari 6～7
伝送方式	IEEE802.3ab(1000BASE-T) IEEE802.3u(100BASE-TX) IEEE802.3i(10BASE-T)
通信方式	CSMA/CD 全二重/半二重
伝送符号	1000BASE-T:8B1Q4 100BASE-TX:4B/5B+MLT-3 10BASE-T:マンチェスタ符号
LANポート	RJ-45×1ポート 「Auto MDI/MDI-X」「オートネゴシエーション」対応
WANポート	RJ-45×1ポート 「Auto MDI/MDI-X」「オートネゴシエーション」対応
電源	電源内蔵 / AC100V、50/60Hz
消費電力	最大5W
外形寸法	約120 (W) x170 (D) x35 (H) mm
本体質量	約550g
使用温度範囲	0～40℃
使用湿度範囲	20～80% (結露なきこと)
取得規格	VCCI Class-B RoHS指令準拠 電気通信事業法 設計認証

VPN 内の IP アドレスについて

VPN内、BX-VP1のLAN内のIPアドレスは、IPアドレス クラスA、B、Cともに同一セグメント254台まで設定が可能です。
BX-VP1は、工場出荷状態で192.168.88.xxxのセグメントとなります。
BX-VP1のLAN内の機器のIPアドレスを固定する場合、以下に記載されているアドレス以外の1～254のアドレスを設定してください。BX-VP1の子機LAN内の機器は、一台までの接続になります。

項目	IPアドレス
親機アドレス	192.168.88.1
ペアリング済み子機アドレス	192.168.88.100 (1台目) 192.168.88.101(2台目) ※工場出荷時設定は子機モードも192.168.88.1となります。
親機LAN側DHCPクライアントリリースアドレス	192.168.88.2～192.168.88.10
ペアリング済み子機LAN側DHCPクライアントリリースアドレス	192.168.88.110 (1台目) 192.168.88.111(2台目)
親機VPNサーバーリリースアドレス	192.168.88.102～192.168.88.109

困ったときには

困ったときには

参照したいトラブルの対処をご覧ください。

VPNランプが点灯しない

VPN構築にあたり、お使いのルーターの［IPsecパススルー］を有効にしてください。
お使いのルーターによっては、［IPsecパススルー］に対応していない場合があります。お使いのルーターのメーカーにお問合せください。

お使いのルーターの[IPsecパススルー]を有効にしても、VPNランプが点灯しない

お使いのルーターによっては、［IPsecパススルー］と［IPv6パススルー］の設定が共存できない場合があります。その場合、［IPv6パススルー］を無効に設定してください。詳しい設定方法は、お使いのルーターのメーカーにお問い合わせください。

通信が遅い(推奨の回線について)

ADSL回線やCATV回線、光ハイブリッド回線などをご利用の場合、下り方向の通信速度に対して、上り方向の通信速度を低く制限されている場合があります。
本製品の性能を発揮する上で十分なスループットが確保できる、光回線の利用をお勧めします。

推奨の同時接続台数は何台ですか?

本製品親機との接続可能数は、同時合計4台までを推奨しています。
本製品子機（※）は最大2台まで接続可能です。
接続先を増やす場合は、「BX-VP1」（増設用子機）をお買い求めください。子機を2台接続した場合、残り2台まで他デバイス（タブレットやパソコンなど）の接続が可能です。
※ 本製品子機の配下に接続できるデバイスは1台のみです。

VPNコネクトでQRコードを読み込めない

カメラの解像度やズーム可否によって、QRコードを読み込めないことがあります。
その場合、QRコードを150%ほどに拡大コピーしてお使いください。

昨日までVPN接続できていたのに、突然VPN接続できなくなった

VPNユーザーのパスワードが変わっています。管理者の方は設定用のQRコード（USBメモリー）とパスコードをご用意の上、VPNを利用する社員にご連絡ください。

VPN コネクトを使わずに VPN を設定したい

Windows 10の場合

1 「準備する」16ページを参照し、Mac OS X、Androidと同じ情報をメモする

2 「Windows用NAT-Traversal Configuration Tool」をダウンロードし、実行する

① http://www.iodata.jp/lib/より「BX-VP1」を検索し、製品ページを開く

② 「Windows用NAT-Traversal Configuration Tool」をダウンロードする

③ ダウンロードしたファイルを実行し、デスクトップ上に解凍してできた[WNATTSET]フォルダーを開き、[WNATTSet(.exe)]をダブルクリック

⑤ [IPSec NAT Traversalを有効にする]をクリック

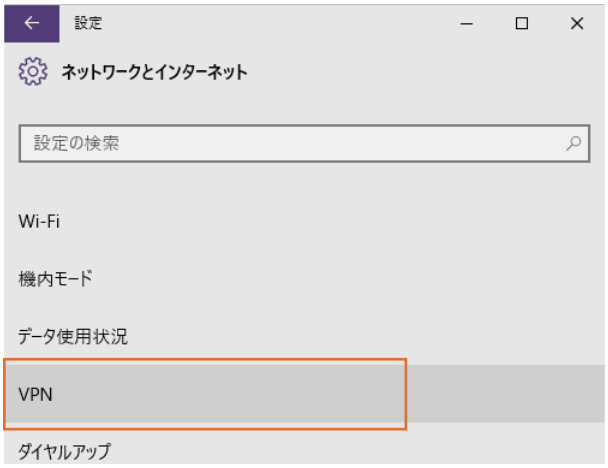
⑥ [設定変更に成功しました。・・・再起動を実行しますか]の画面で、[はい]をクリック

⇒ 自動的にパソコンを再起動します。

3 [スタート]→[設定]をクリック

4 [ネットワークとインターネット]をクリック

5 [VPN]をクリック



6 [VPN接続を追加する]をクリック

7 VPN接続について設定する

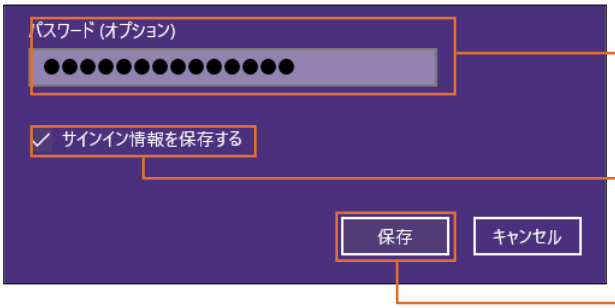
① [Windows(ビルトイン)]を選ぶ

② 「準備する」16ページで確認した[ホスト名]を入力

③ [IPsecを利用したレイヤー2 トンネリング プロトコル]を選ぶ

④ [ユーザー名とパスワード]を選ぶ

⑤ 「準備する」16ページで確認した[ユーザー名]を入力

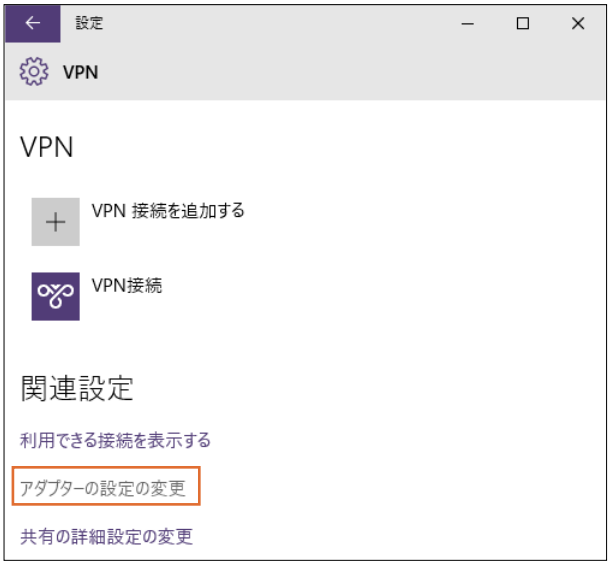


⑥「準備する」16ページで確認した[パスワード]を入力

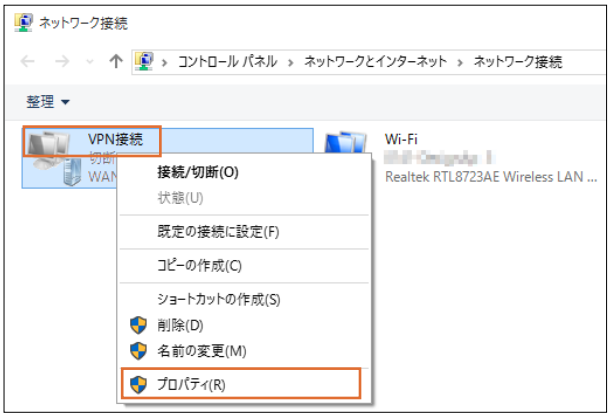
⑦[サインイン情報を保存する]をチェックする

⑧[保存]をクリック

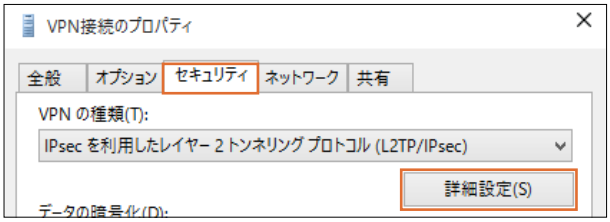
8 [アダプター設定の変更]をクリック



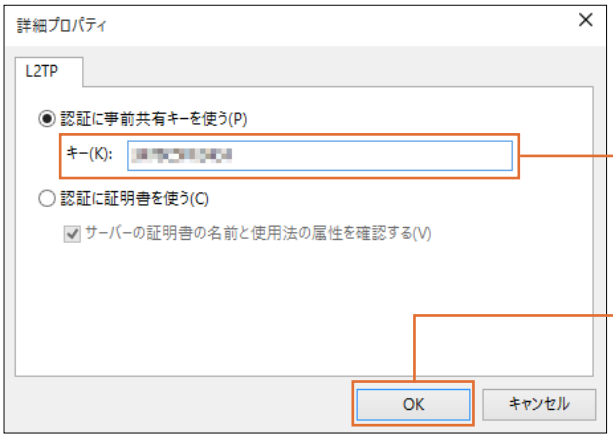
9 先ほど作ったVPN接続を右クリックし、[プロパティ]をクリック



10 [セキュリティ]タブの「VPNの種類」にある[詳細設定]をクリック



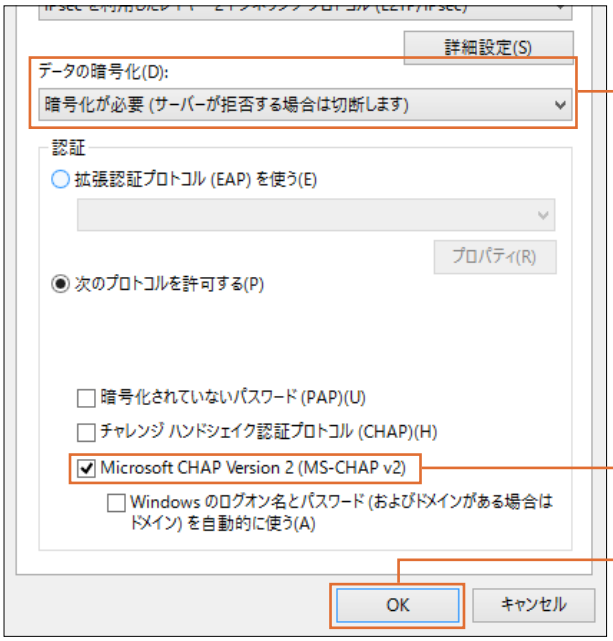
11



① 「準備する」16ページで確認した[プレシェアードキー]を入力

② [OK]をクリック

12

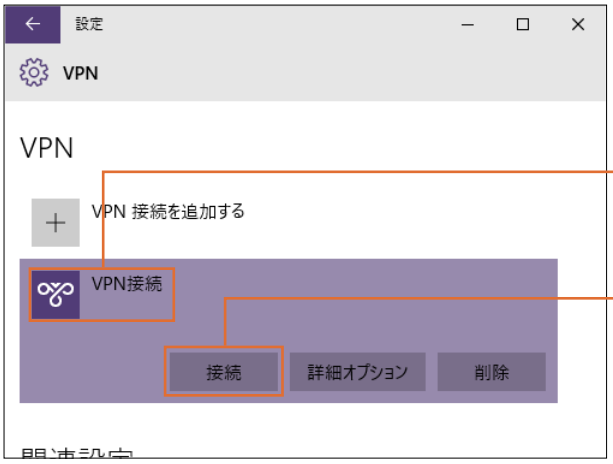


① [暗号化が必要]を選ぶ

② [Microsoft CHAP Version 2]を選ぶ

③ [OK]をクリック

13



① [VPN接続]をクリック

② [接続]をクリック

③ 「接続済み」と表示されたことを確認

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

以上で設定は完了です。

Windows 8の場合

1 「準備する」16ページを参照し、Mac OS X、Androidと同じ情報をメモする

2 「Windows用NAT-Traversal Configuration Tool」をダウンロードし、実行する

① http://www.iodata.jp/lib/より「BX-VP1」を検索し、製品ページを開く

② 「Windows用NAT-Traversal Configuration Tool」をダウンロードする

③ ダウンロードしたファイルを実行し、デスクトップ上に解凍してできた[WNATTSET]フォルダーを開き、[WNATTSet(.exe)]をダブルクリック

⑤ [IPSec NAT Traversalを有効にする]をクリック

⑥ [設定変更に成功しました。・・・再起動を実行しますか]の画面で、[はい]をクリック

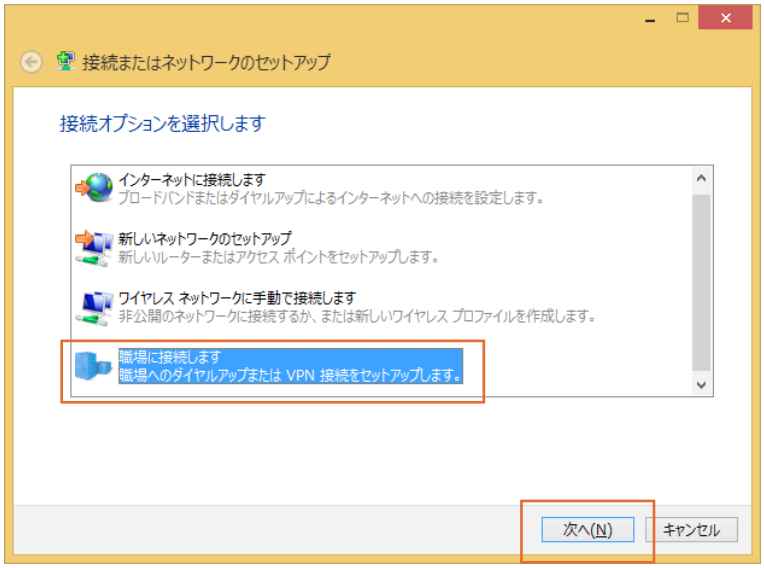
⇒ 自動的にパソコンを再起動します。

3 コントロールパネルを開く

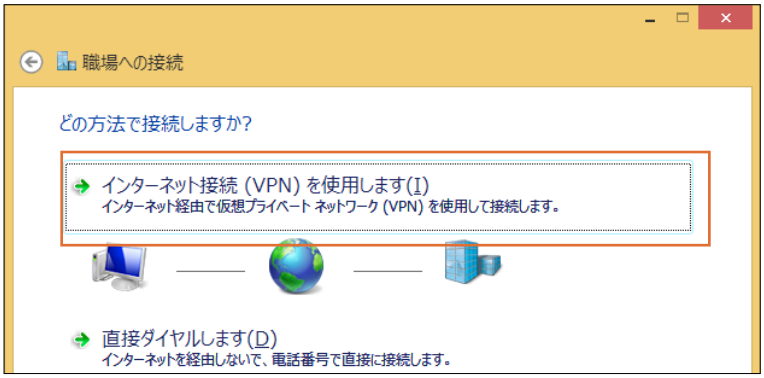
4 [ネットワークの状態とタスクの表示]をクリック

5 [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

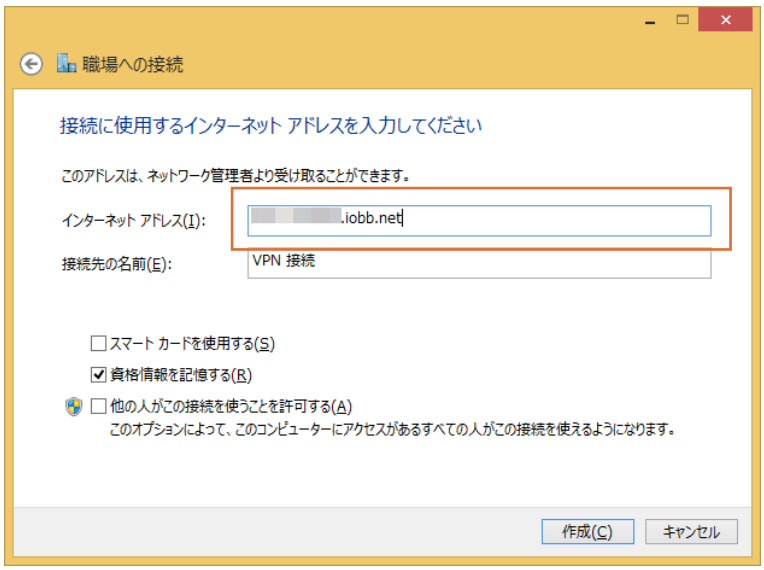
6 [職場に接続します]を選択し、[次へ]をクリック



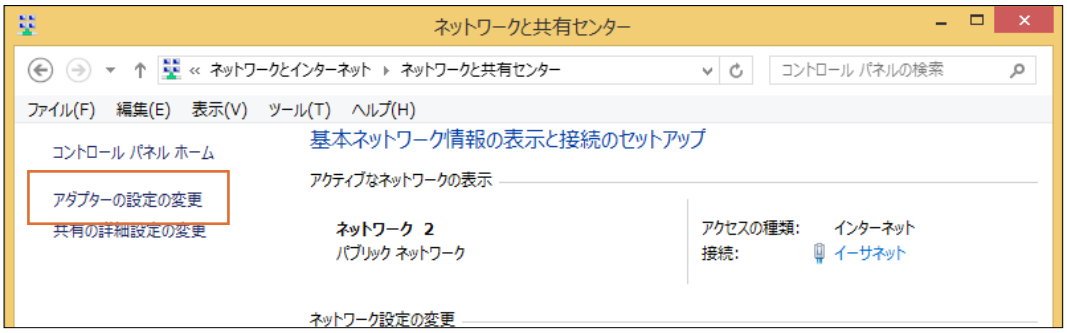
7 [インターネット接続(VPN)を使用します]をクリック



8 [インターネットアドレス]に「準備する」16ページで確認した[ホスト名]を入力し、[作成]をクリック

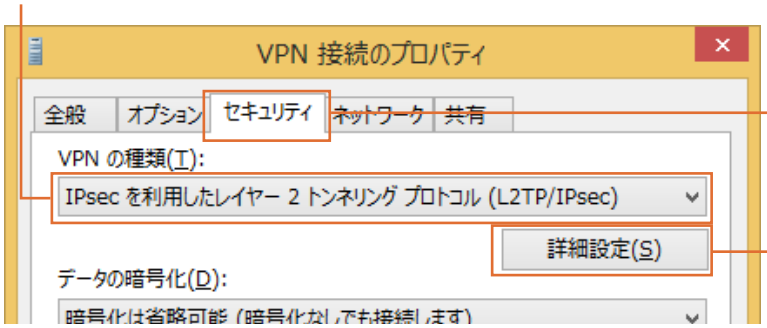


9 [アダプターの設定の変更]をクリック



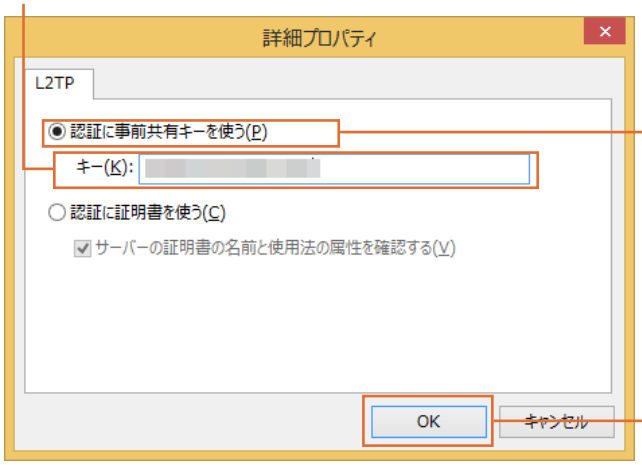
10 [VPN接続]を選択し、[この接続の設定を変更する]をクリック

11 ① [セキュリティ]タブをクリック ② [IPsecを利用した・・・(L2TP/IPsec)]を選択



③ [詳細設定]をクリック

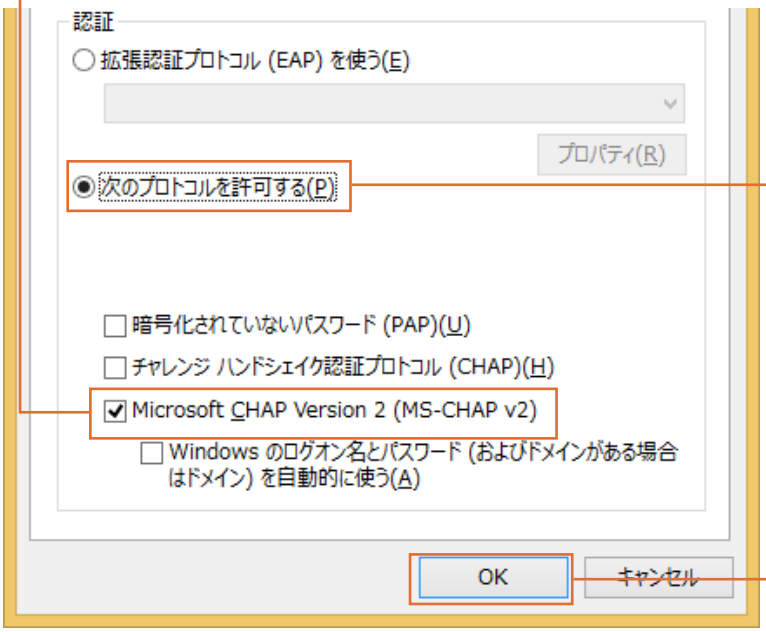
12 ① [認証に事前共有キーを使う]を選択 ② [キー]に「準備する」16ページで確認した[プレシェアードキー]を入力



③ [OK]をクリック

13

① [次のプロトコルを許可する]を選択
② [Microsoft CHAP Version 2(MS-CHAP v2)]にチェック



③ [OK]をクリック

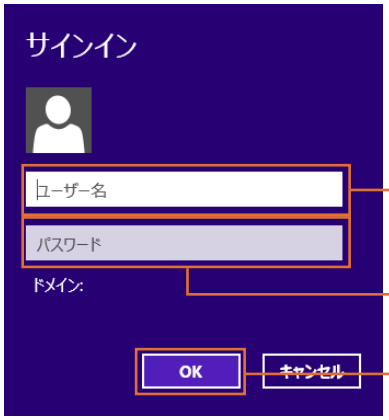
14

チャームバーから[設定]→無線のアイコンの順にクリック

15

① [VPN接続]をクリック
② [接続]をクリック

16



① 「準備する」16ページで確認した[ユーザー名]を入力

② 「準備する」16ページで確認した[パスワード]を入力

③ [OK]をクリック

17

「接続済み」と表示されたことを確認

以上で設定は完了です。

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

Windows 7/Vistaの場合

1 「準備する」16ページを参照し、Mac OS X、Androidと同じ情報をメモする

2 「Windows用NAT-Traversal Configuration Tool」をダウンロードし、実行する

① http://www.iodata.jp/lib/より「BX-VP1」を検索し、製品ページを開く

② 「Windows用NAT-Traversal Configuration Tool」をダウンロードする

③ ダウンロードしたファイルを実行し、デスクトップ上に解凍してできた[WNATTSET]フォルダーを開き、[WNATTSet(.exe)]をダブルクリック

⑤ [IPSec NAT Traversalを有効にする]をクリック

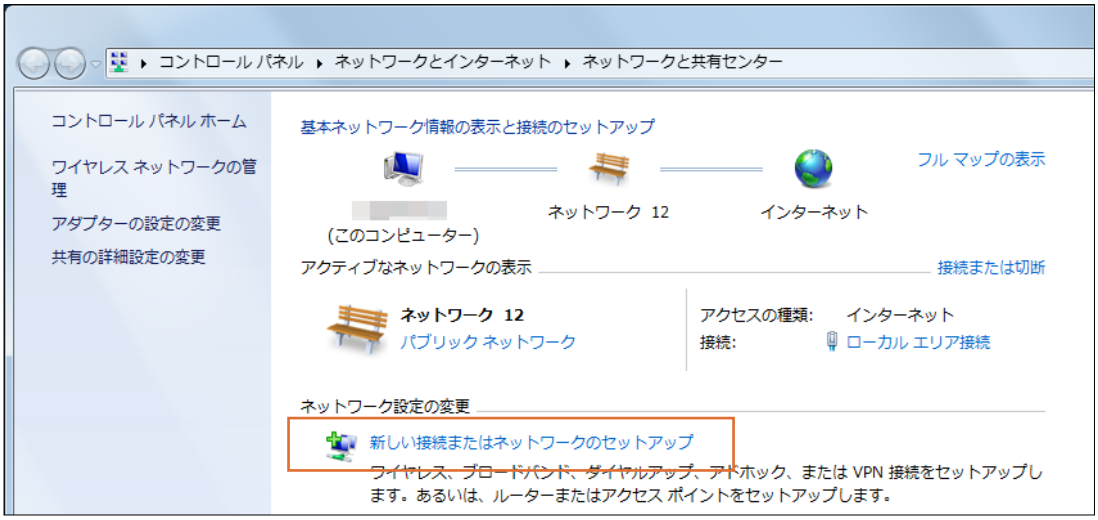
⑥ [設定変更に成功しました。・・・再起動を実行しますか]の画面で、[はい]をクリック

⇒ 自動的にパソコンを再起動します。

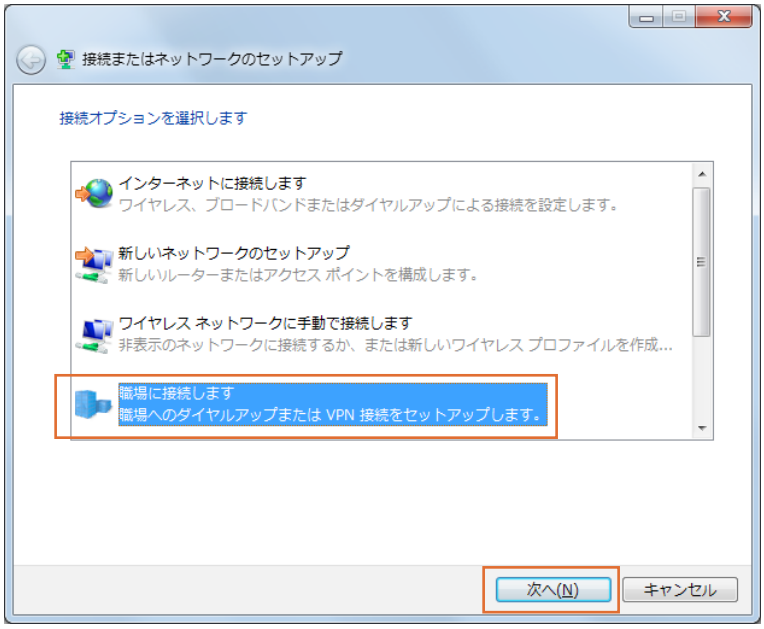
3 コントロールパネルを開く

4 [ネットワークの状態とタスクの表示]をクリック

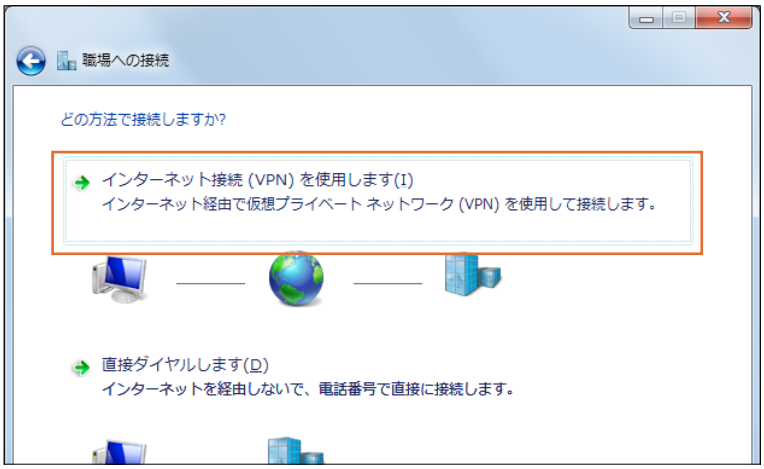
5 [新しい接続またはネットワークのセットアップ]をクリック



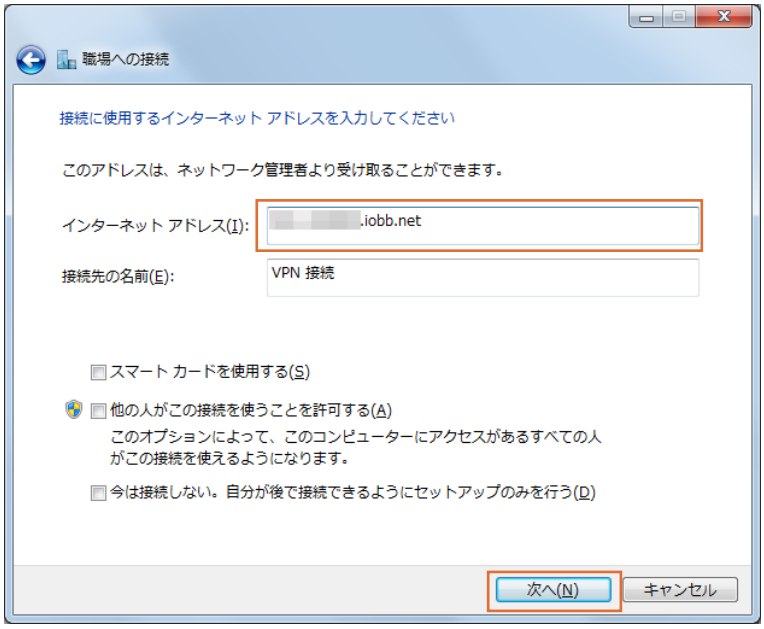
6 [職場に接続します]を選択し、[次へ]をクリック



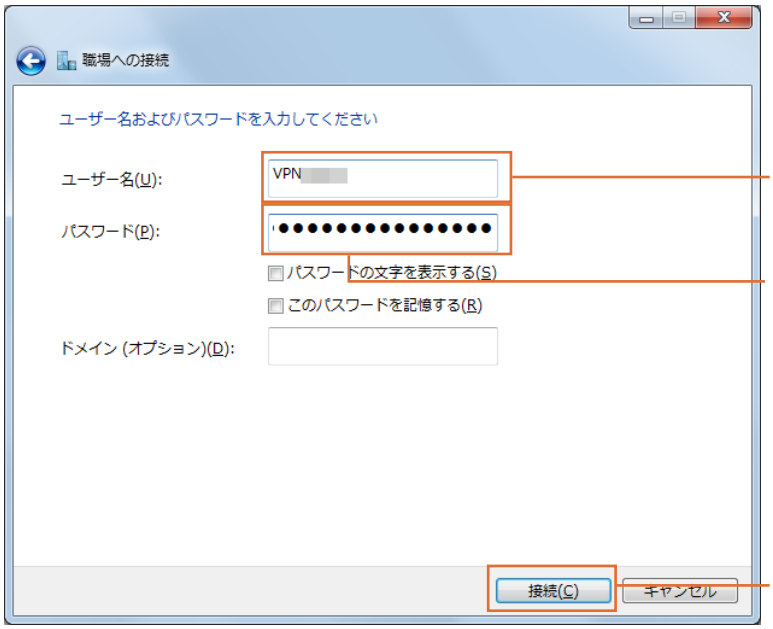
7 [インターネット接続(VPN)を使用します]をクリック



8 [インターネットアドレス]に[準備する]16ページで確認した[ホスト名]を入力し、[次へ]をクリック



9

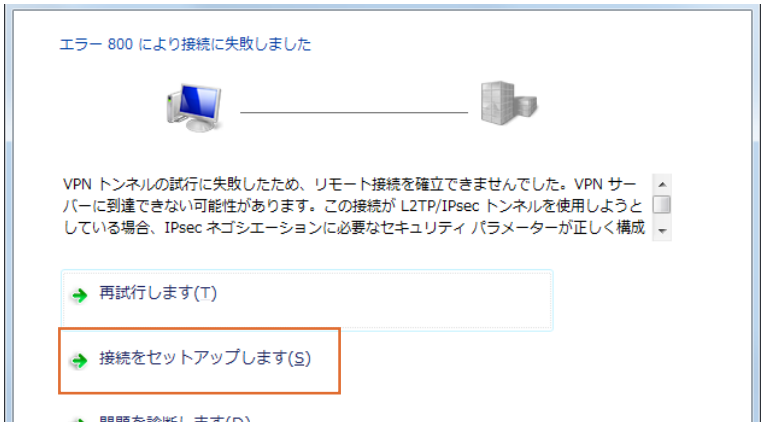


① [準備する]16ページで確認した[ユーザー名]を入力

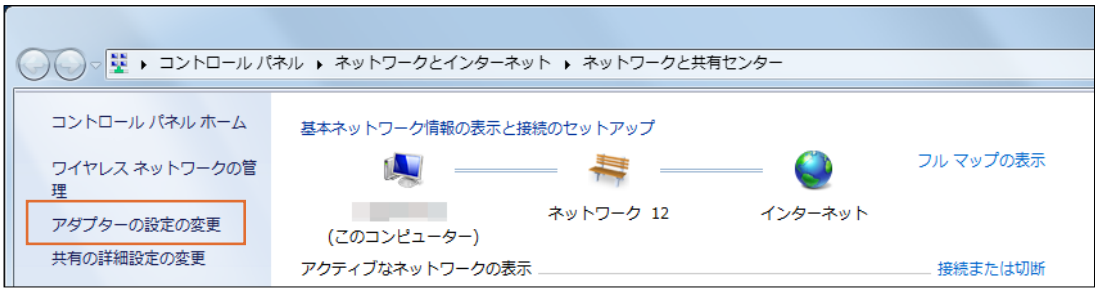
② [準備する]16ページで確認した[パスワード]を入力

③ [接続]をクリック

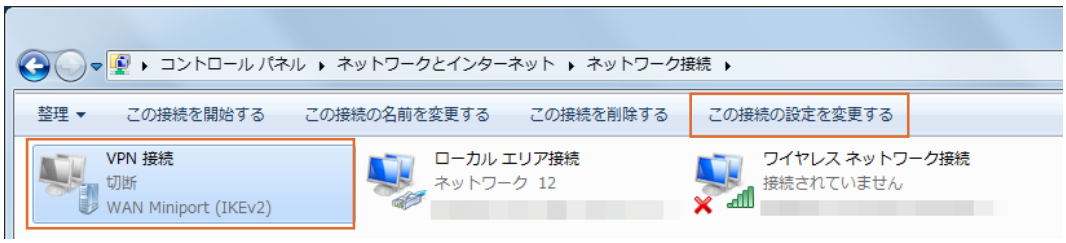
10 [接続をセットアップします]または[キャンセル]をクリック



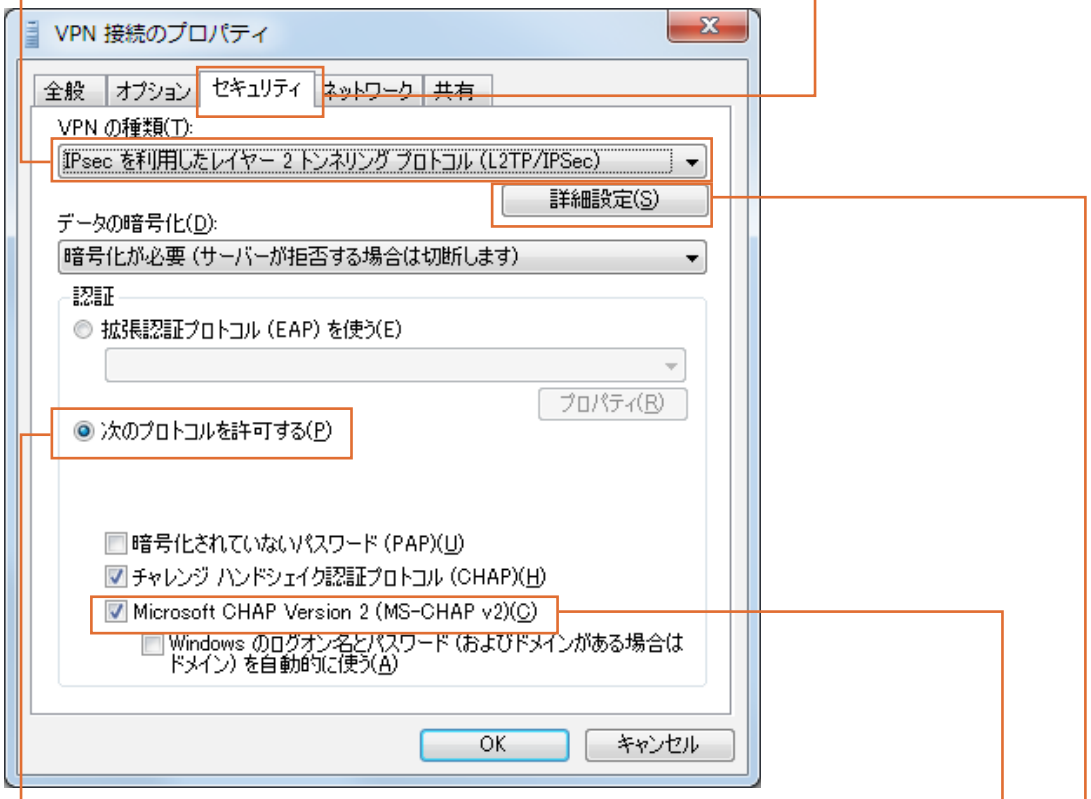
11 [アダプターの設定の変更]をクリック



12 [VPN接続]を選択し、[この接続の設定を変更する]をクリック



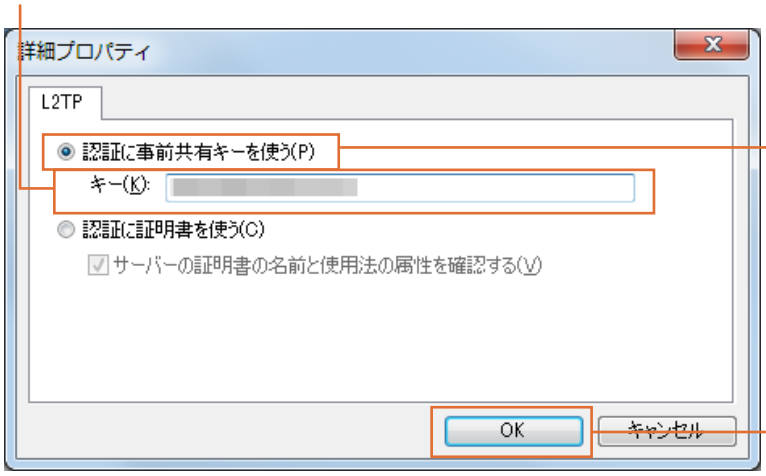
13 ① [セキュリティ]タブをクリック
② [IPsecを利用した・・・(L2TP/IPSec)]を選択



③ [次のプロトコルを許可する]を選択
④ [Microsoft CHAP Version 2(MS-CHAP v2)]にチェック
⑤ [詳細設定]をクリック

14

① [認証に事前共有キーを使う]を選択
② [キー]に「準備する」16ページで確認した[プレシェアードキー]を入力



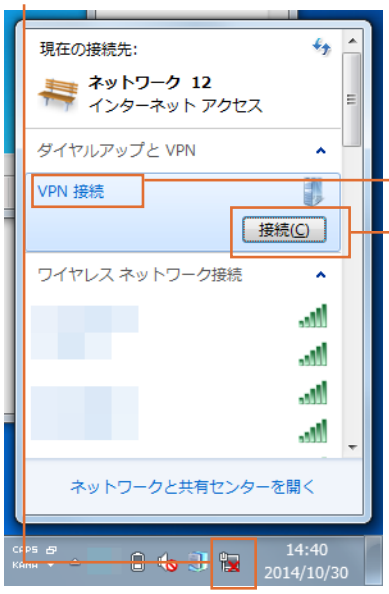
③ [OK]をクリック

15

VPN接続のプロパティ画面の[OK]をクリック

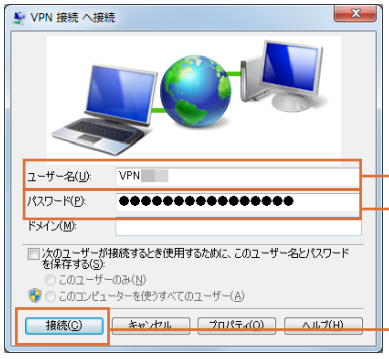
16

① 画面右下の通知領域の無線のアイコンをクリック



① [VPN接続]をクリック
② [接続]をクリック

17



① 「準備する」16ページで確認した[ユーザー名]を入力
② 「準備する」16ページで確認した[パスワード]を入力

③ [接続]をクリック

18

「接続済み」と表示されたことを確認

以上で設定は完了です。

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

iPhone/iPadの場合

1 「準備する」16ページを参照し、Mac OS X、Androidと同じ情報をメモする

2 設定 をタップ

3

[一般]をタップ

4

[VPN]をタップ

5

[VPN構成を追加]をタップ

6

① 任意の名前を入力

②「準備する」16ページで確認した[ホスト名]を入力

③「準備する」16ページで確認した[ユーザー名]を入力

④「準備する」16ページで確認した[パスワード]を入力

⑤「準備する」16ページで確認した[プレシェアードキー]を入力

⑥ [保存]をタップ

7

① [オン]にします
② [接続中]と表示されたことを確認

以上で設定は完了です。

設定したパソコンを譲渡・廃棄する場合は、VPN 設定を削除してください

「VPN設定を削除したい」81ページ参照

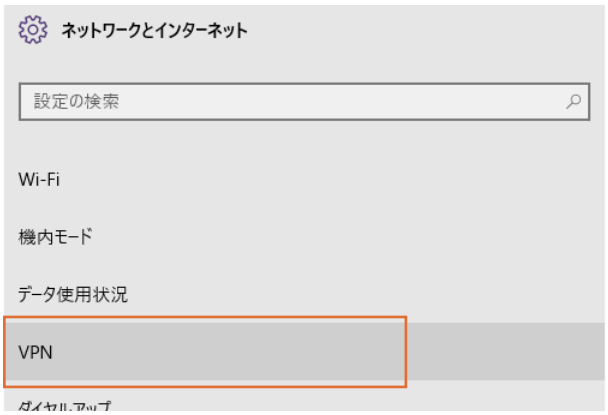
VPN 設定を削除したい

Windows 10の場合

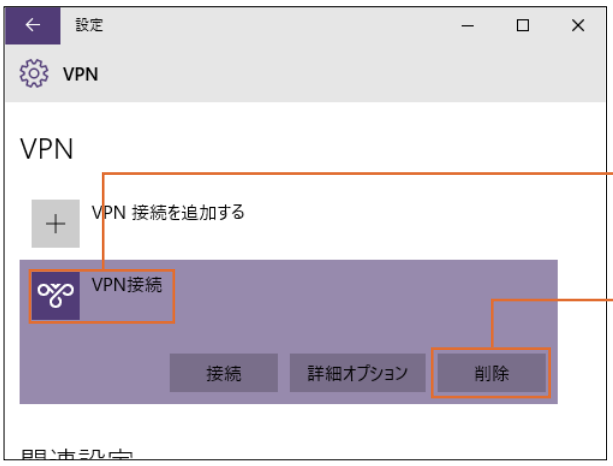
1 [スタート]→[設定]をクリック

2 [ネットワークとインターネット]をクリック

3 [VPN]をクリック



4

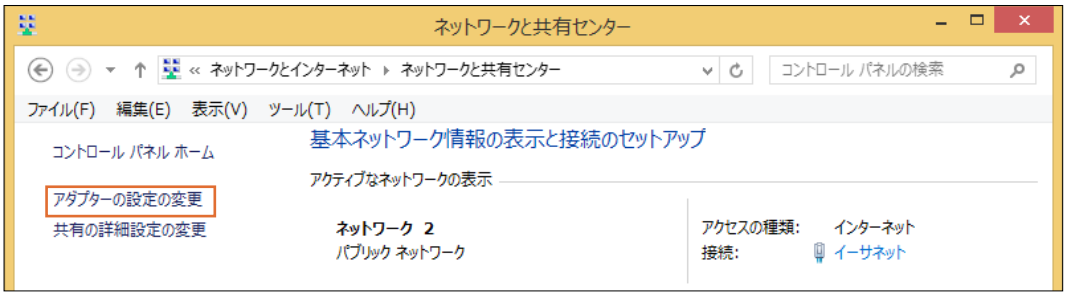


Windows 8/7/Vistaの場合

1 コントロールパネルを開く

2 [ネットワークの状態とタスクの表示]をクリック

3 [アダプターの設定の変更]をクリック

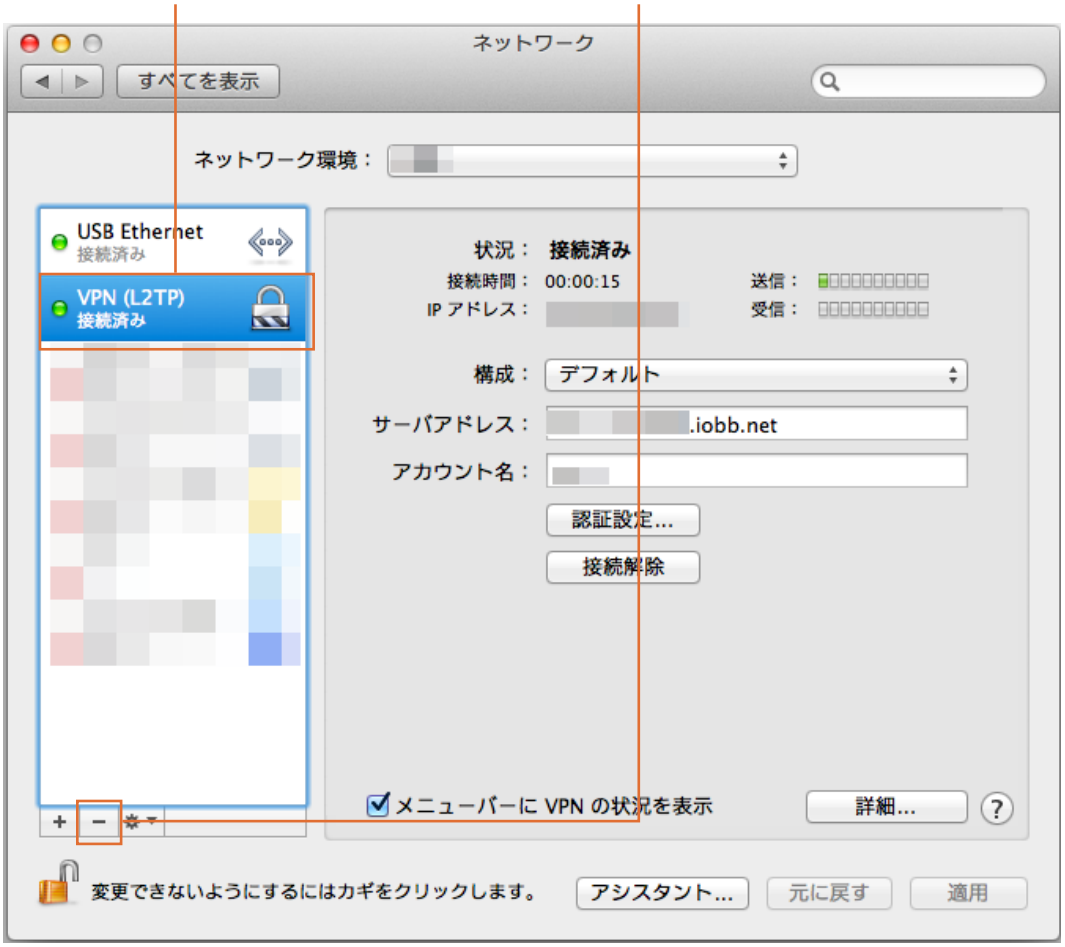


4 [VPN接続]を選択し、[この接続を削除する]をクリック

Mac OS Xの場合

1 アップルメニューから[システム環境設定]→[ネットワーク]の順にクリック

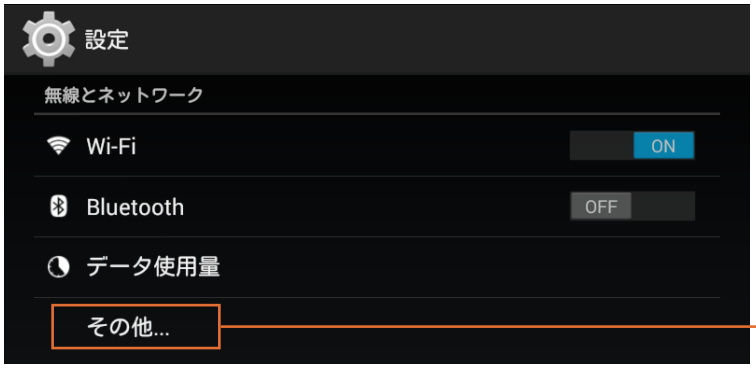
2 削除したいサービス名を選び、リスト下部の「－（削除）」をクリック



Androidの場合

1 [設定] をタップ

2

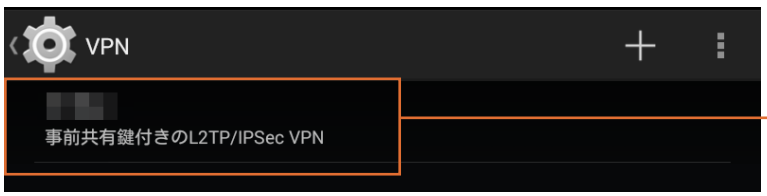


[その他]をタップ

3

[VPN]をタップ

4



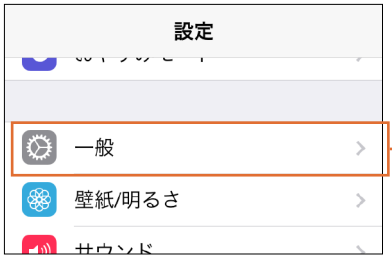
保存した名前をタップし続ける

5 [プロフィールを削除]または[ネットワークを削除]をタップ

iPhone/iPadの場合（VPNコネクトで設定した場合）

1 設定 をタップ

2



[一般]をタップ

3

[プロファイル]をタップ

4

[BX-VP1(xxxxxx)]をタップ

5

[プロファイルを削除]をタップ

iPhone/iPadの場合（VPNコネクトを使わずに設定した場合）

1 設定 をタップ

2

[一般]をタップ

3

[VPN]をタップ

4

削除したいVPN設定の[i]をタップ

5

画面一番下の[VPNを削除]をタップ

【もくじ】へ

お問い合わせについて

お問い合わせいただく前に、**以下をご確認ください**

- **マニュアルの「困ったときには」を参照** (64ページ参照)
- **サポートページのQ&Aを参照**
- **最新のソフトウェアをダウンロード**

http://www.iodata.jp/support/

それでも解決できない場合は、**サポートセンターへ**

電話：050-3116-3015
※受付時間　9：00～17：00　月～日曜日（年末年始・夏期休業期間をのぞく）
FAX：076-260-3360
インターネット： http://www.iodata.jp/support/

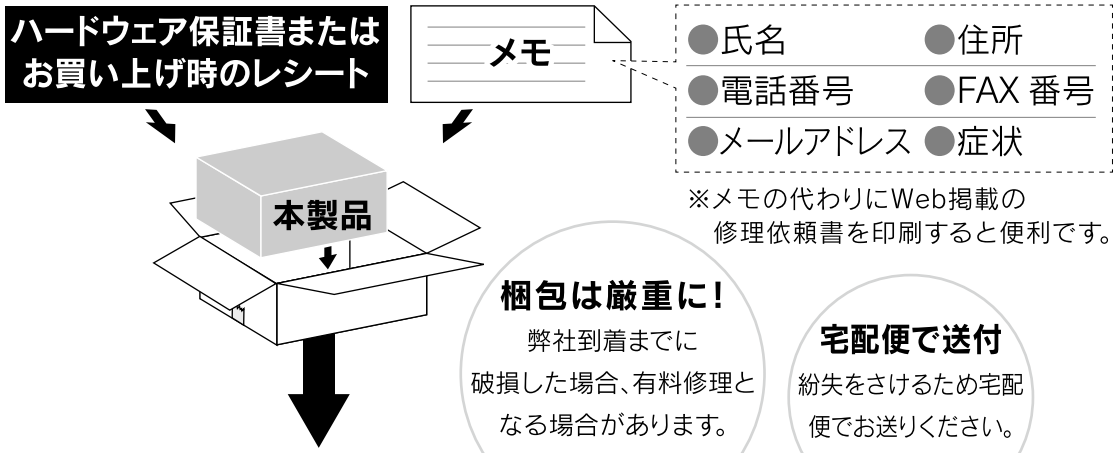
＜ご用意いただく情報＞
製品情報（製品名、シリアル番号など）、パソコンや接続機器の情報（型番、OSなど）

個人情報の取り扱いについて

個人情報は、株式会社アイ・オー・データ機器のプライバシーポリシー（http://www.iodata.jp/privacy.htm）に基づき、適切な管理と運用をおこないます。

修理について

修理を依頼される場合は、以下の要領でお送りください。



〒920-8513 石川県金沢市桜田町2丁目84番地
株式会社　アイ・オー・データ機器　修理センター 宛

- 送料は、発送時はお客様ご負担、返送時は弊社負担です。
- 有料修理となった場合は先に見積をご案内します。（見積無料）
  金額のご了承をいただいてから、修理をおこないます。
- 内部にデータがある場合、厳密な検査のため、内部データは消去されます。何卒、ご了承ください。
  バックアップ可能な場合は、お送りいただく前にバックアップしてください。弊社修理センターではデータの修復はおこなっておりません。
- お客様が貼られたシール等は、修理時に失われる場合があります。
- 保証内容については、ハードウェア保証規定に記載されています。
- 修理品を送る前に製品名とシリアル番号（S/N）を控えてください。

修理について詳しくは以下をご確認ください

http://www.iodata.jp/support/after/

【使用ソフトウェアについて】
本製品には、GNU General Public License (GPL2)に基づいたソフトウェアが含まれています。変更済みGPL 対象モジュール、GNU General Public License、及びその配布に関する条項については、弊社のホームページにてご確認ください。これらのソースコードで配布されるソフトウェアについては、弊社ならびにソフトウェアの著作者は一切のサポートの責を負いませんのでご了承ください。

【ご注意】
1) 本製品及び本書は株式会社アイ・オー・データ機器の著作物です。
したがって、本製品及び本書の一部または全部を無断で複製、複写、転載、改変することは 法律で禁じられています。
2) 本製品は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備や機器、兵器システムなどの人命に関る設備や機器、及び海底中継器、宇宙衛星などの高度な信頼性を必要とする設備や機器としての使用またはこれらに組み込んでの使用は意図されておりません。
これら、設備や機器、制御システムなどに本製品を使用され、本製品の故障により、人身事故、火災事故、社会的な損害などが生じても、弊社ではいかなる責任も負いかねます。設備や機器、制御システムなどにおいて、冗長設計、火災延焼対策設計、誤動作防止設計など、安全設計に万全を期されるようご注意願います。
3) 本製品は日本国内仕様です。本製品を日本国外で使用された場合、弊社は一切の責任を負いかねます。また、弊社は本製品に関し、日本国外への技術サポート、及びアフターサービス等を行っておりませんので、予めご了承ください。(This product is for use only in Japan. We bear no responsibility for any damages or losses arising from use of, or inability to use, this product outside Japan and provide no technical support or after-service for this product outside Japan.)
4) 本製品を運用した結果の他への影響については、上記にかかわらず責任は負いかねますのでご了承ください。

【商標について】
●記載されている会社名、製品名等は一般に各社の商標または登録商標です。