

フレッツ・VPN ワイド

セットアップガイド

東日本電信電話株式会社

- 本操作マニュアルの一部または全部を東日本電信電話株式会社の許可なく複製することを禁じます。
- 本マニュアルの内容は予告なく変更することがあります。
- 本マニュアルにおける製品に関する記述は、情報を提供する目的で書かれたもので、保証もしくは推奨するものではありません。
- Windows、Windows 11 は米国マイクロソフトコーポレーションの米国およびその他の国における登録商標です。
- その他の製品名などの固有名詞は、各メーカーの登録商標または商標です。
- 本文中の各社の登録商標または商標には、マークは表示していません。

目次

第1章 ご利用の前に

1-1 サービスの概要4
1-2 基本サービスプラン5
1-3 ユーザタイプ6
1-4 サービス利用例7
1-5 サービスの利用にあたって必要となる情報8

第2章 VPNの利用

2-1 VPN利用までの流れ12
2-2 設定方法	
Windows11の設定を用いたPPPoE及びPPPの設定13

第3章 トラブルが発生したら

3-1 VPN接続時のトラブル19
-----------------	---------

第4章 お問い合わせ先

4-1 お問い合わせ窓口一覧 21
4-2 パスワードを紛失した場合 22

第1章 ご利用の前に

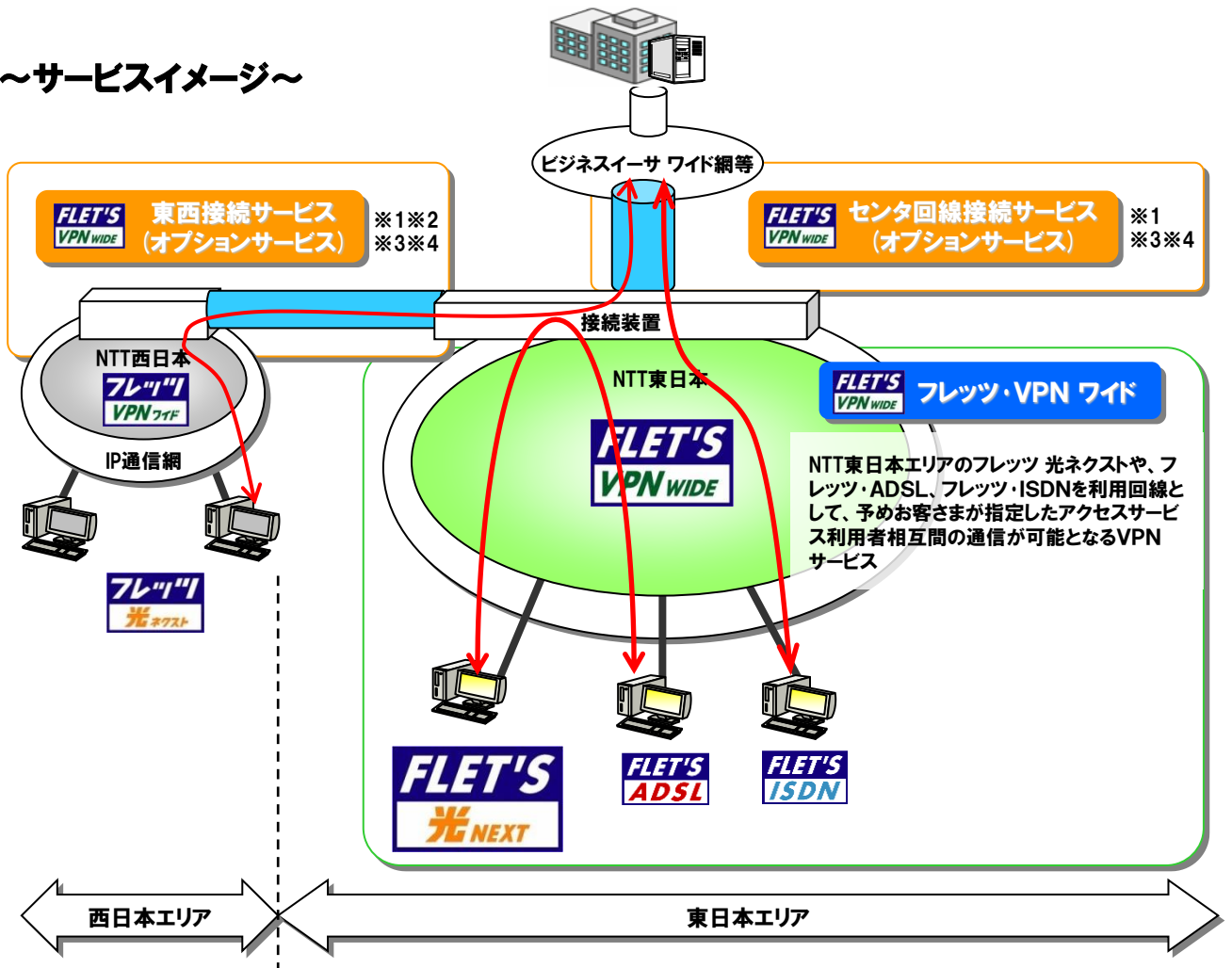
1-1 サービスの概要

フレッツ・VPN ワイドは、フレッツ 光ネクスト^{*}、フレッツ・ADSL、フレッツ・ISDN (以下、アクセスサービス) をご利用のお客さま間にて、簡易なプライベートネットワークの構築を実現する、ベストエフォート型サービスです。本サービスを利用することにより、同一プライベートネットワーク内のお客さま間でお互いの共有ファイルへのアクセス等をセキュアに行うことができます。

オプションサービスとして、お客さまのネットワークやサーバ等を接続可能である「センタ回線接続サービス」や、NTT西日本のフレッツ・VPN ワイドと接続可能である「東西接続サービス」をご利用いただくことで、より柔軟に様々な形態でのプライベートネットワークを構築することができます。又、「サポートオプション」により、フレッツ・VPN ワイドへのサポート機能を追加することが可能です。

※フレッツ 光ネクスト プライオ1、フレッツ 光ネクスト プライオ10、フレッツ 光ライト、フレッツ 光クロスはご利用できません。

～サービスイメージ～



※ **FLET'S VPN WIDE サポートオプション (オプションサービス)** 上記サービスイメージの他、フレッツ・VPN ワイドへのサポート機能追加を可能とする「サポートオプション」を提供しております。

※1 センタ回線接続サービス及び、東西接続サービス、サポートオプションをご利用の場合は、別途お申込みが必要です。

※2 東西接続サービスをご利用の場合は、NTT東日本とNTT西日本のそれぞれのフレッツ・VPN ワイド及び、東西接続サービスのお申込みが必要です。

※3 プラスプランをご利用いただく場合、センタ回線接続サービスおよび東西接続サービスは基本サービスお申込み (VPN開設) と同時に申し込みいただく必要があります。VPN開設後に東西接続サービスのお申込みはできません。

※4 プラスプランでは、センタ回線接続サービスと東西接続サービスを同時にご利用いただくことはできません。

図1-1 フレッツ・VPN ワイドの概要図

1-2 基本サービスプラン

基本サービスには「標準プラン」「プラスプラン」の2種類があります。以下、それぞれについて説明します。

	標準プラン	プラスプラン
プラン (拠点数)	プラン10 (10) プラン30 (30) プラン100 (100) プラン300 (300) プラン1000 (1000)	プラン10 プラス (10) プラン30 プラス (30) プラン100 プラス (100) プラン300 プラス (300) プラン1000 プラス (1000)
利用可能 アクセス サービス ※4	フレッツ 光ネクスト ファミリータイプ/ ファミリー・ハイスピードタイプ フレッツ 光ネクスト マンションタイプ/ マンション・ハイスピードタイプ フレッツ・ADSL フレッツ・ISDN	フレッツ 光ネクスト ビジネスタイプ フレッツ 光ネクスト ファミリータイプ/ ファミリー・ハイスピードタイプ/ギガファミリー・ス マートタイプ/ファミリー・ギガラインタイプ フレッツ 光ネクスト マンションタイプ/ マンション・ハイスピードタイプ/ギガマンション・ス マートタイプ/マンション・ギガラインタイプ/オフィ スタイプ・ファミリー/オフィスタイプ・マンション フレッツ・ADSL フレッツ・ISDN
利用可能 オプション サービス	センタ回線接続サービス 東西接続サービス サポートオプションサービス	センタ回線接続サービス※1※2 東西接続サービス※1※2 サポートオプションサービス
メリット	より低コストでネットワークを構築可能※3	フレッツ光 ネクスト ビジネスタイプ等を利用した 高速通信ネットワークを構築可能

※1 プラスプランをご利用いただく場合、センタ回線接続サービスおよび東西接続サービスは基本サービス
お申し込み (VPN開設) と同時に申し込みいただく必要があります。

※2 プラスプランでは、センタ回線接続サービスと東西接続サービスを同時にご契約いただくことはできません。

※3 標準プランとプラスプランでは、VPN管理者の月額利用料が異なります。

※4 フレッツ 光ネクスト プライオ1/ プライオ10、フレッツ 光ライト、フレッツ 光クロスはご利用できません。

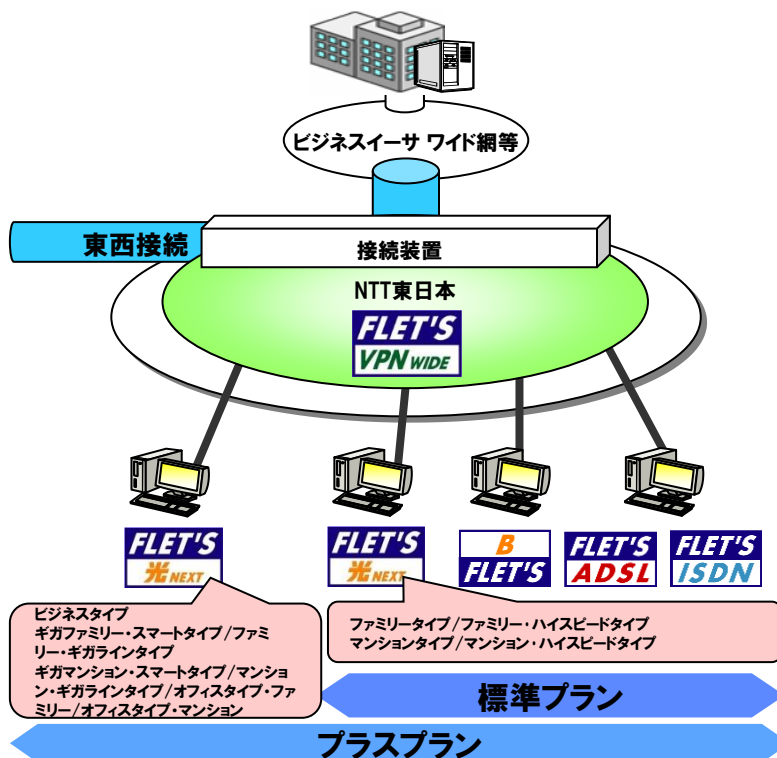


図1-2 フレッツ・VPN ワイドの基本サービス

1-3 ユーザタイプ

本サービス契約者には、VPN管理者とVPN参加者の2種類があります。以下、それぞれについて説明します。

VPN契約者	同一VPNを利用する本サービスの契約者です。 契約者の種別はVPN管理者とVPN参加者の2種類があります。	
	VPN 管理者	VPNの管理を行う契約者です。 カスタマコントロールを利用して、VPNの様々な設定を行うとともに、VPN参加希望者に対して、必要な情報の通知等を行っていただきます。 VPN管理者は、VPN内に1契約者のみであり、VPNを開設した契約者が初期のVPN管理者となります。 VPN管理者は、アクセスサービスとしてフレッツ 光ネクスト※、フレッツ・ADSL、フレッツ・ISDNをご利用することができます。 また、センタ回線接続サービス、東西接続サービス、サポートオプションは、VPN管理者のみが申込可能です。
	VPN 参加者	VPN管理者の承諾のもとVPNに参加するVPN契約者です。 VPN管理者より通知された情報によりVPNを利用することができます。 アクセスサービスとしてフレッツ 光ネクスト※、フレッツ・ADSL、フレッツ・ISDNをご利用することができます。

※フレッツ 光ネクスト プライオ1、フレッツ 光ネクスト プライオ10、フレッツ 光ライト、フレッツ 光クロスはご利用できません。

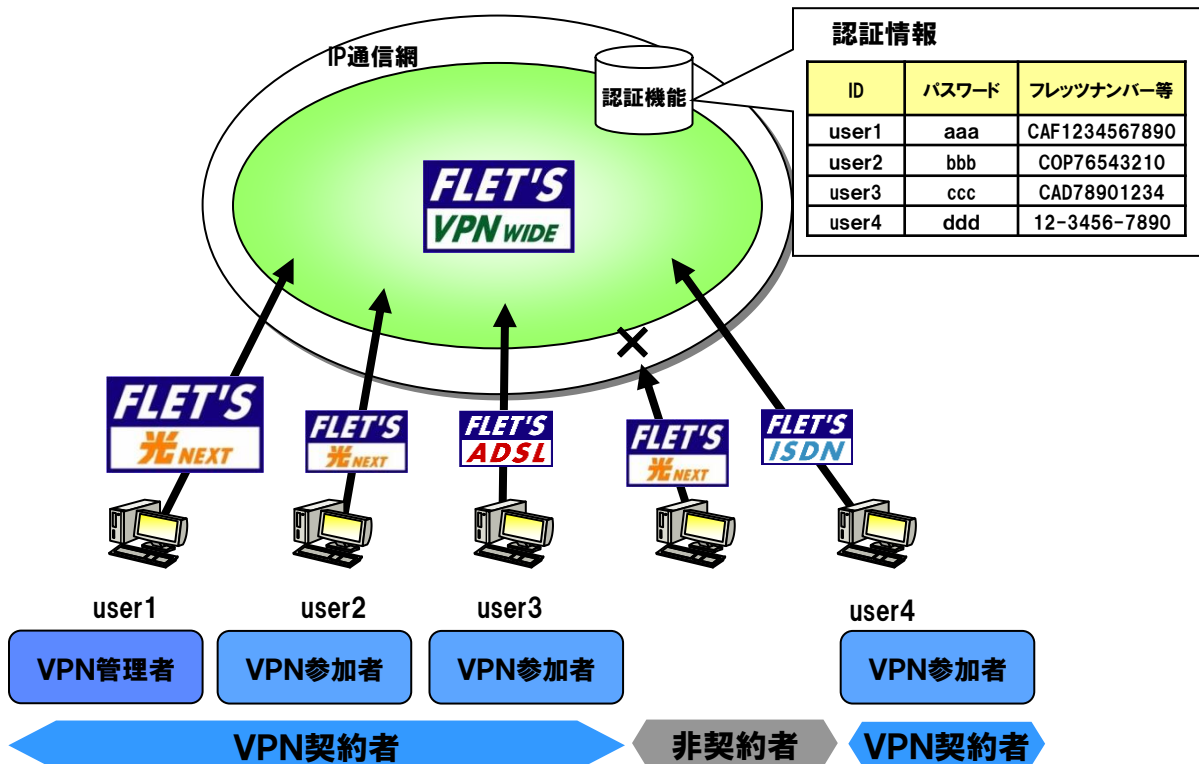


図1-3 VPN管理者とVPN参加者

1-4 サービス利用例

本サービスは、同一VPNを利用する契約者間のプライベートネットワークを提供するサービスです。お客様の利用環境次第で、さまざまな用途・方法での利用が可能です。

OSのネットワーク設定によるVPNの利用

オペレーティングシステム (OS) 等のネットワーク設定を行うことにより、各端末のフォルダ共有やサーバの共有を行います。

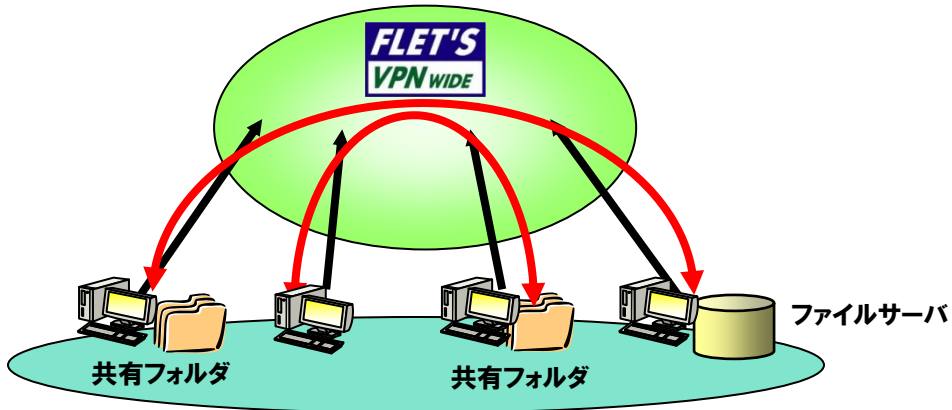


図1-4 オペレーティングシステム等のネットワーク設定によるファイル共有
(例: Windowsの共有設定等)

HTTPやFTP等のサーバによるVPNの利用

HTTPやFTPなどのTCP/IP上のプロトコルを利用したサーバを構築することにより、オペレーティングシステムの設定等を行うことなく情報の共有 (掲示板利用等) やファイルの共有 (アップロード/ダウンロード) を行うことが可能です。

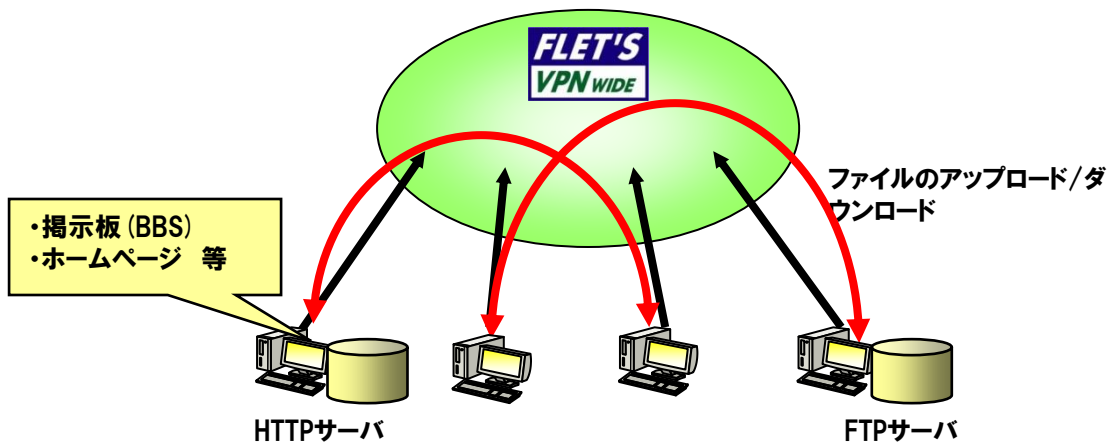


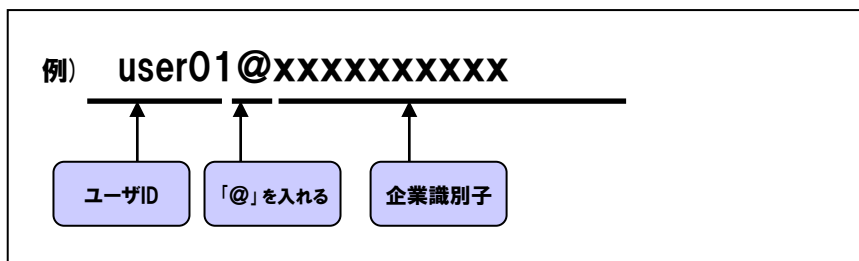
図1-5 HTTP/FTPサーバの構築

1-5 サービスの利用にあたって必要となる情報

本サービスを利用する際に必要となる情報は以下のとおりです。
これらの情報は、Web-SOの申込受付完了画面もしくは、開通のご案内に記載されています。VPN参加者は、一部の情報についてVPN管理者より通知してもらう必要があります。

ユーザ名

VPNへ接続する際に使用します。
VPN契約者のユーザID + @ + 企業識別子 で構成されます。



企業識別子

VPN開設時に、VPN毎にひとつ与えられる、VPNを識別するための文字列です。企業識別子は、VPN管理者がVPN参加者に通知する必要があります。

ユーザID

VPN契約者が利用するユーザIDです。VPNを利用する際、企業識別子と合わせて使用します。VPN参加者のユーザIDは、VPN管理者がVPN参加者に通知する必要があります。

パスワード

VPNへ接続する際の認証時に、ユーザ名と併せて使用します。

VPN管理者がVPN参加者に、通知する必要があります。なお、パスワードは、カスタマコントロールを利用して変更することが可能です。

IPアドレス / サブネットマスク

VPN契約者からのVPNへの接続の際に「ユーザID/パスワード/フレッツナンバーもしくは、発信者回線情報」による認証後、「IPアドレス/サブネットマスク」の払い出しを行います。

ユーザIDに対して、常に同一のIPアドレスを払い出すので、常に同じIPアドレスを利用してグループ内での通信を行うことが可能です。

VPN管理者は、ユーザIDごとにVPNで利用するIPアドレスを設定する必要があります。また、設定後の変更も可能です。

IPアドレスの付与方法には、「①端末型払い出し」と「②LAN型払い出し」の2つの方法があり、VPN契約者の利用環境等に合わせ、VPN管理者により設定を行なっていただく必要があります。

① 端末型払い出し

VPN参加者のユーザIDに対し、サブネットマスクに255.255.255.255を設定する場合、端末型払い出しとなります。VPN契約者に端末が接続されている場合等に利用します。

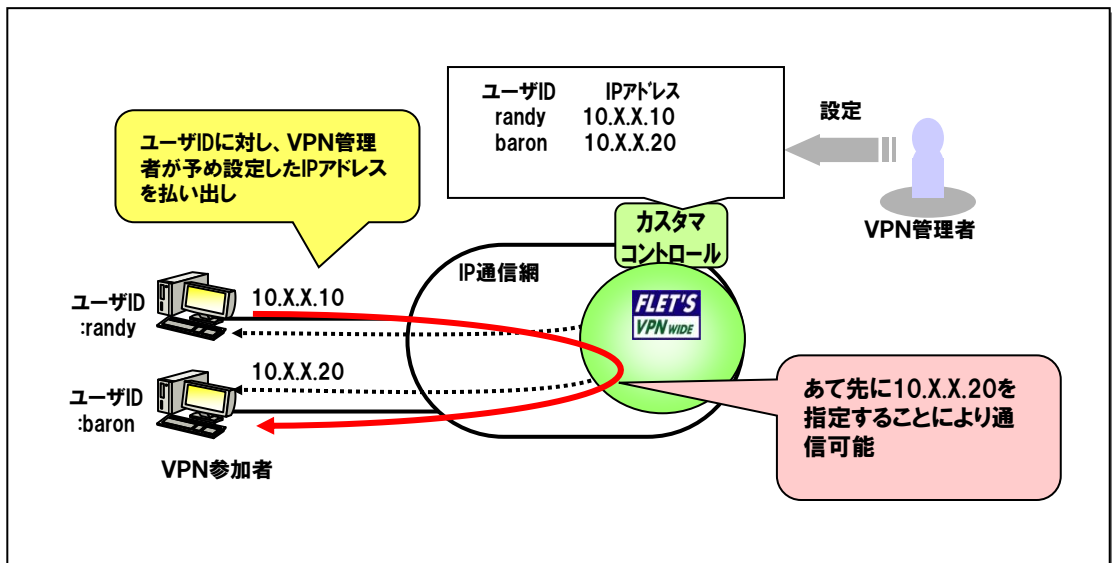


図1-6 端末型払い出し



設定上の注意点

IPアドレスの設定は、以下の点に注意して設定する必要があります。

- ①VPN内でIPアドレスが重複しないようご注意ください。
- ②以下のIPアドレス領域は、使用することができません。
 ※利用できないIPアドレス、サブネットマスクを、グループ参加者に払い出すIPアドレス、ならびにNW設定等に用いた場合、継続的に通信ができなくなる可能性がありますので、設定しないようご注意ください。

・0. 0. 0. 0
 ・10. 128. 0. 0～10. 128. 255. 255
 ・224. 0. 0. 0～239. 255. 255. 255 (クラスD)
 ・240. 0. 0. 0～255. 255. 255. 255 (クラスE)

- ③「端末型払い出し」に応じたサブネットマスク (255. 255. 255. 255) を設定するようご注意ください。

②LAN型払い出し

VPN参加者のユーザIDに対し、任意のサブネットマスク (255.255.255.255以外) を設定する場合、LAN型払い出しとなります。VPN契約者の環境にLANが接続されている場合等に利用し、LAN上の各端末をあて先として指定することが可能となります。

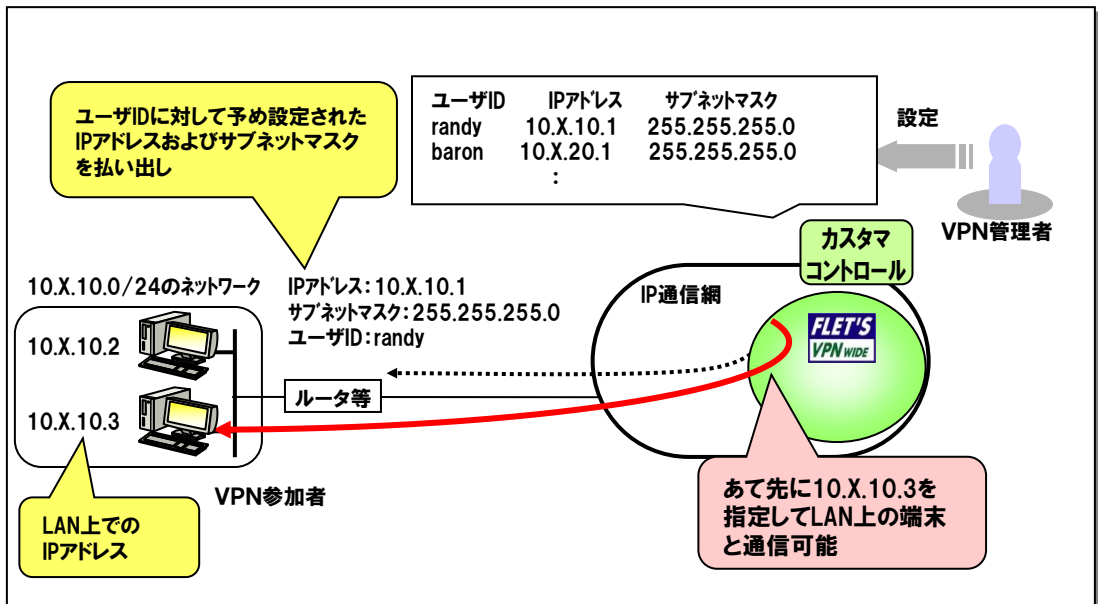


図1-7 LAN型払い出し



設定上の注意点

IPアドレスの設定は、以下の点に注意して設定する必要があります。

- ①グループ内でIPアドレス及びネットワークのアドレス体系が重複しないようご注意ください。

(参考1) IPアドレスが重複している場合の例

VPN参加者A	IPアドレス <u>192.168.1.1</u> サブネットマスク <u>255.255.255.0</u>
VPN参加者B	IPアドレス <u>192.168.1.1</u> サブネットマスク <u>255.255.255.0</u>

(参考2) ネットワークのアドレス体系が重複している場合の例

VPN参加者A	IPアドレス 192.168.129.30 サブネットマスク 255.255.255.224 ネットワーク範囲 <u>192.168.129.0~31</u>
VPN参加者B	IPアドレス 192.168.129.31 サブネットマスク 255.255.255.240 ネットワーク範囲 <u>192.168.129.16~31</u>

- ②以下のIPアドレスは使用できません。
(以下のIPアドレス領域を含むネットワークセグメントをLAN型払い出しとして設定することはできません。)
※利用できないIPアドレス、サブネットマスクを、グループ参加者に払い出すIPアドレス、ならびにNW設定等に用いた場合、継続的に通信ができなくなる可能性がありますので、設定しないようご注意ください。

ご利用いただけないIPアドレス領域

- ・0.0.0.0
- ・10.128.0.0~10.128.255.255
- ・224.0.0.0~239.255.255.255 (クラスD)
- ・240.0.0.0~255.255.255.255 (クラスE)

ご利用いただけないサブネットマスク

- ・0.0.0.0 ・128.0.0.0 ・192.0.0.0
- ・224.0.0.0 ・240.0.0.0 ・248.0.0.0
- ・252.0.0.0 ・254.0.0.0

第2章 VPNの利用

2-1 VPN利用までの流れ

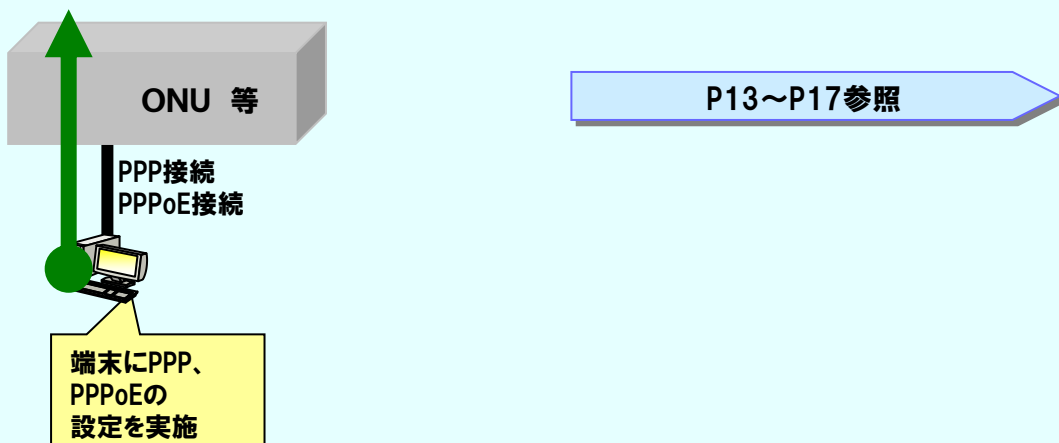
本サービスを利用するにあたっては、事前にVPNへの接続設定を実施する必要があります。設定については、パソコン等の端末に設定を行う方法とPPPoE対応ルータに設定を行う方法があり、お客さまのご利用環境により、設定手順が異なります。

◆ 本セットアップガイドでは、端末に設定を行いかつ端末型払出しで利用する場合についての手順について説明します。ルータ等を利用しLAN型払い出しにて利用する場合は、ご利用になるルータに添付されているマニュアル等を参照してください。

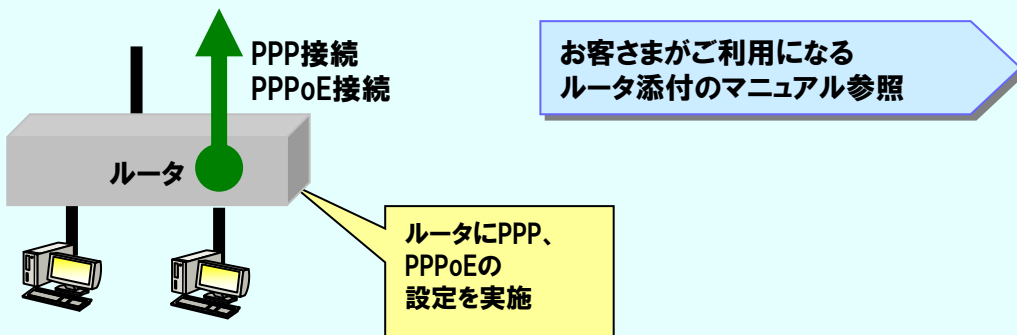
I. 事前設定 (P13~P17参照)

VPNへ接続するために必要な情報を確認し、事前設定を行います。

① 端末にPPP、PPPoE設定を行う方法



② ルータにPPP、PPPoE設定を行う方法



II. VPNへの接続例 (P18参照)

「I. 事前設定」で行った環境にて、VPNへの接続・切断を行います。

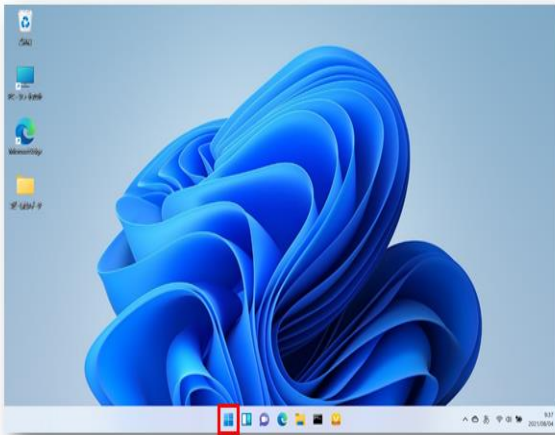
2-2 設定方法

① 端末での初回の接続

- ❖ ここではWindows 11の端末にて、アクセスサービスとフレッツ 光ネクスト、フレッツ・ADSLをご利用しているお客さまがPPPoE接続の設定を行う手順について説明します。
- ❖ 画面の表示内容については、お使いのパソコンやソフトウェアのバージョンなどにより、一部異なることがあります。

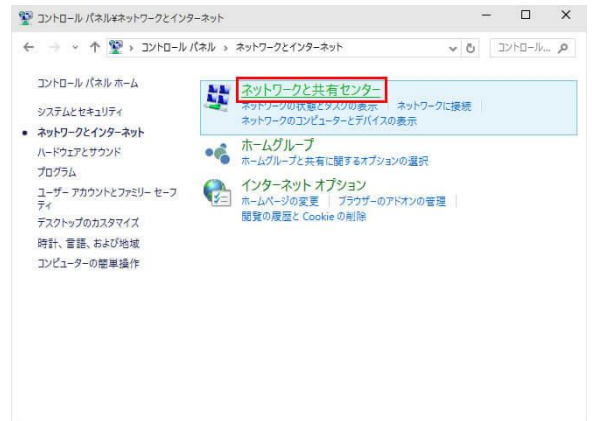
1

スタートボタン→「コントロールパネル」で検索します。



3

「ネットワークと共有センター」を選択します。



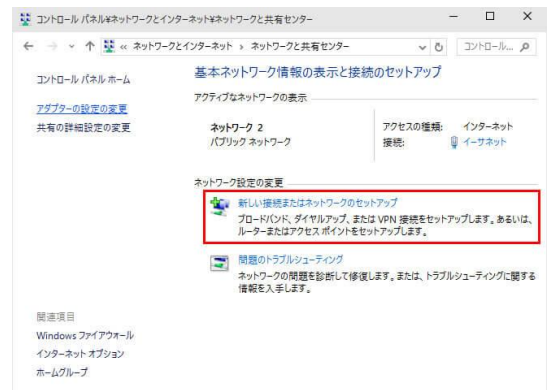
2

「ネットワークとインターネット」を選択します。



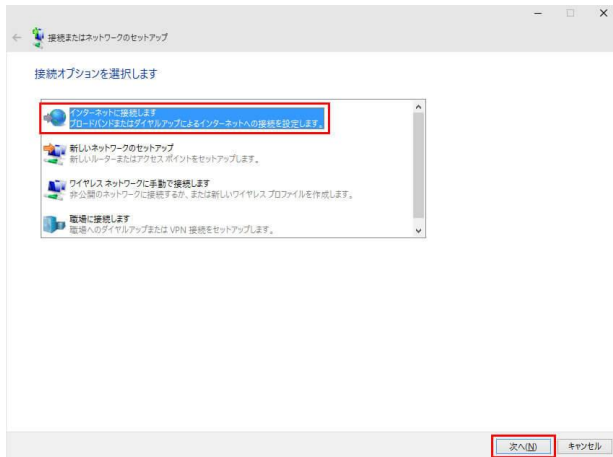
4

「新しい接続またはネットワークのセットアップ」を選択します。



5

[インターネットに接続します]を選択し、[次へ]を選択します。



7

[既にインターネットに接続しています]と表示された場合 [新しい接続をセットアップします]を選択します。



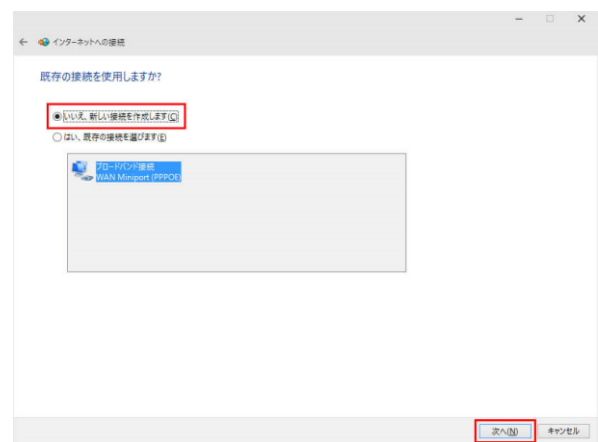
6

[ブロードバンド(PPPoE)(R)]を選択します。



8

[既存の接続を使用しますか?]&表示された場合 [いいえ、新しい接続を作成します]を選択すると、下記画面が表示されます。



9

必要な情報を入力し、[接続] を選択します。

インターネット サービス プロバイダー (ISP) の情報を入力します

ユーザー名(U): [ISP から付与されたユーザー名] 1

パスワード(P): [ISP から付与されたパスワード] 2

パスワードの文字を表示する(S)

このパスワードを記憶する(R) 3

接続名(N): ブロードバンド接続 4

このオプションによって、このコンピューターにアクセスがあるすべての人がこの接続を使えるようになります。

他の人がこの接続を使うことを許可する(A) 5

[ISP がありません](#)

接続(O) キャンセル

1 P8のユーザIDを入力します。

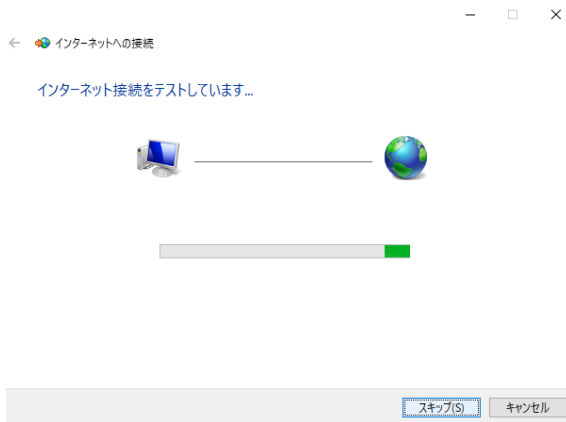
2 P8のパスワードを入力します。

3 チェックを入れると接続の都度パスワードを入力する必要がなくなります。

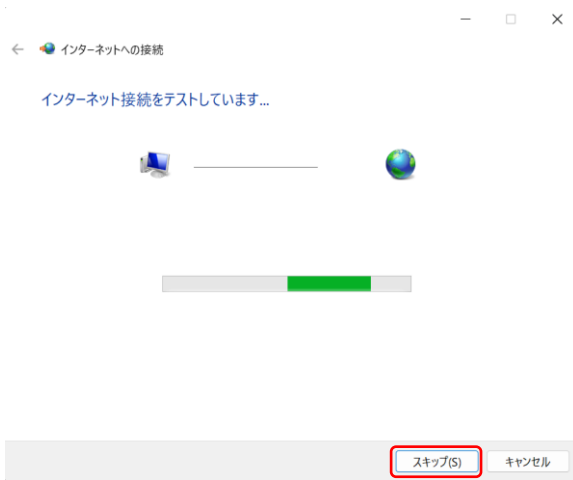
4 お客様にて自由に決めていただきます。

5 チェックを入れると1台のパソコンを複数のアカウントで利用する場合に、他のアカウントでもこの設定が有効になります。

10 VPN接続の認証テストが自動的に開始されます。



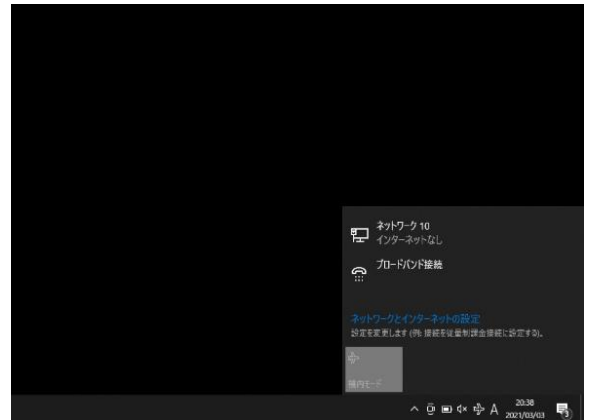
11 VPNおよび、インターネット接続の認証テストが開始されますが、【スキップ(S)】をクリックします。



12 ・「接続の使用準備ができました」と表示されますので、【閉じる(C)】をクリックします。



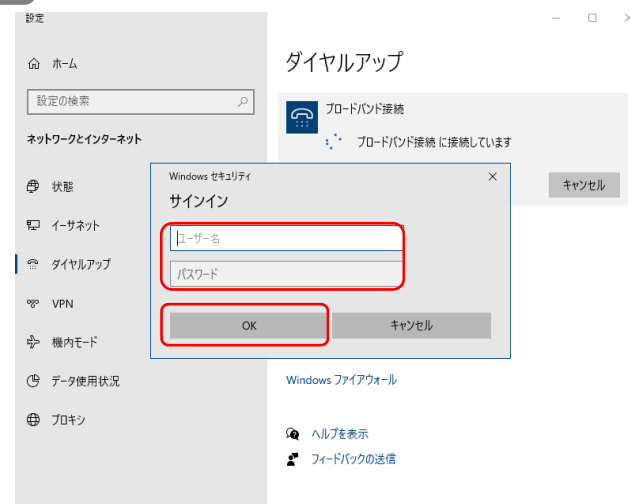
13 デスクトップ画面右下の「ネットワーク」のアイコンを右クリックし、「ネットワークとインターネットの設定」をクリックします。



14 1回目で設定したVPN接続用のアイコン(本マニュアル上は「ブロードバンド接続」)の【接続】をクリックします。



15 ユーザ名とパスワードを入力し、OKをクリックします。



16

接続済みになっていることを確認します。

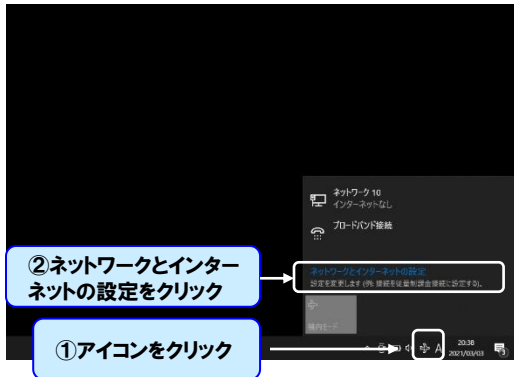


以上で、VPNへの接続は完了です。

② 端末での2回目以降の接続

- ❗ ここでは、Windows 11端末におけるVPNへの接続を行う手順について説明します。
- ❗ 画面の表示内容については、お使いのパソコンやソフトウェアのバージョンなどにより、一部異なることがあります。

1 デスクトップ画面右下の「ネットワーク」や「機内モード」のアイコンをクリックし、「ネットワークとインターネットの設定」をクリックします。



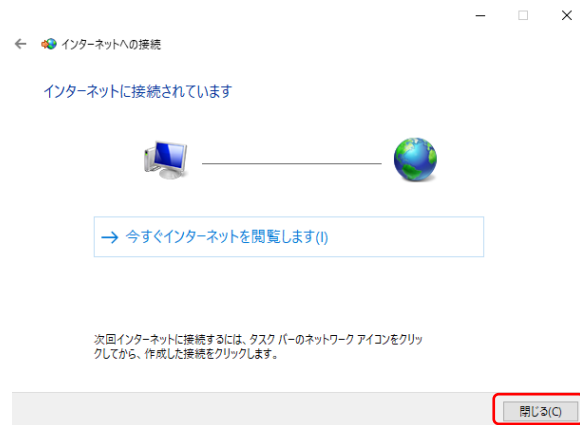
2 1回目で設定したVPN接続用のアイコン(本マニュアル上は「ブロードバンド接続」)の「接続」をクリックします。



3 ユーザ名とパスワードを入力し、OKをクリックします。



4 正常に接続されたことを確認後、【閉じる (C)】をクリックします。



5 接続済みになっていることを確認します。



以上で、VPNへの接続は完了です。

第3章 トラブルが発生したら

3-1 VPN接続時のトラブル

VPN契約者がPPP接続、PPPoE接続を行うときの主なトラブルについて説明します。パソコン上に表示されるエラーメッセージの内容に従って対処してください。

PPP接続の際の、主なエラーメッセージ

エラーメッセージ ①

ダイヤルアップ ネットワークによる接続を完了できませんでした。

エラー:691

ユーザ名またはパスワード、あるいはその両方が無効なため、このドメインにアクセスできませんでした。

【原因1】 ユーザ名が正しく入力されていない可能性があります。

【原因2】 パスワードが正しく入力されていない可能性があります。

◆P15手順6、P18手順11、P20手順12を参照し、設定内容をご確認ください

エラーメッセージ ②

ポートを開いています。

(パターン1) エラー676:電話回線はビジーです。

(パターン2) エラー678:リモートコンピュータが応答しませんでした。詳しい説明については、
{詳細}をクリックするか、ヘルプとサポートセンタでこのエラー番号を
検索してください。

(パターン3) エラー692:モデム(またはほかの接続デバイス)でハードウェア障害が発生しました。

【原因1】 アナログ信号で発信した可能性があります。

【原因2】 ターミナルアダプタとパソコン間で信号が認識されていない可能性があります。

【原因3】 モデム定義ファイルに誤りがある可能性があります。

◆配線やモデム定義ファイルについて再確認してください。

【原因4】 契約回線の電話番号から発信していない可能性があります。

◆ターミナルアダプタのデータポートの番号設定をご利用回線番号に変更してください。
※詳細は、ご利用のターミナルアダプタの取扱説明書を参考にされるか、製造元にご確認ください。

PPPoE接続の際の、主なエラーメッセージ

エラーメッセージ
③

エラー:678

リモートコンピュータが応答しませんでした。

【原因1】 LANケーブルが抜けている場合や、イーサネットアダプタが正常に動作していない可能性があります。

- ◆LANケーブルの正常性及び、接続が正しくされていることをご確認ください。
- ◆回線終端装置・VDSL装置等の再起動をお試しください。
- ◆ルータ経由で接続をしていないかご確認ください。
- ◆イーサネットアダプタのドライバが正常にインストールされているか、無効になっていないかなどをご確認ください。

エラーメッセージ
④

エラー:691

ユーザ名またはパスワード、あるいはその両方が無効なため、このドメインにアクセスできませんでした。
ユーザ名とパスワードを確認して再試行して下さい。

【原因1】 ユーザ名やパスワードの入力に誤りがある可能性があります。

- ◆P12手順3、P13手順3、P15手順6を参照し、設定内容をご確認ください。
- ◆接続プロファイルを作り直してください。

【原因2】 既にアクセスサービスからの接続が、最大接続数までご利用いただいている可能性があります。

- ◆現在の接続を切断していただき、再度接続を行ってください。

第4章 お問い合わせ先

4-1 お問い合わせ窓口一覧

お問い合わせは、NTT東日本公式ホームページにあるフレッツ・VPN ワイドに関するお問い合わせフォームで承っております。

サービス内容について

NTT東日本公式ホームページ上にあるお問い合わせフォームにてお問い合わせください。
<https://business.ntt-east.co.jp/support/vpnwide/>

故障について

開通のご案内もしくは、受付完了画面の記載のフレッツ・VPN ワイドサポートデスクにお問い合わせください。
もしくはNTT東日本公式ホームページ上にある故障に関するお問い合わせフォームにてお問い合わせください。
<https://business.ntt-east.co.jp/generic/trouble/vpnwide/form.html>

4-2 パスワードを紛失した場合

グループ契約者がパスワードを紛失した場合、以下の手続きを行う必要があります。

VPN管理者がパスワードを紛失した場合

VPN管理者がパスワードを紛失した場合は、カスタマコントロールによりパスワードを初期化する必要があります。

VPN参加者がパスワードを紛失した場合

VPN参加者がパスワードを紛失した場合は、VPN管理者へ連絡し、パスワードの初期化・変更を依頼する必要があります。

**フレッツ・VPN ワイド
セットアップガイド**

**発行日：2023年3月 第3.7版
発行：東日本電信電話株式会社**