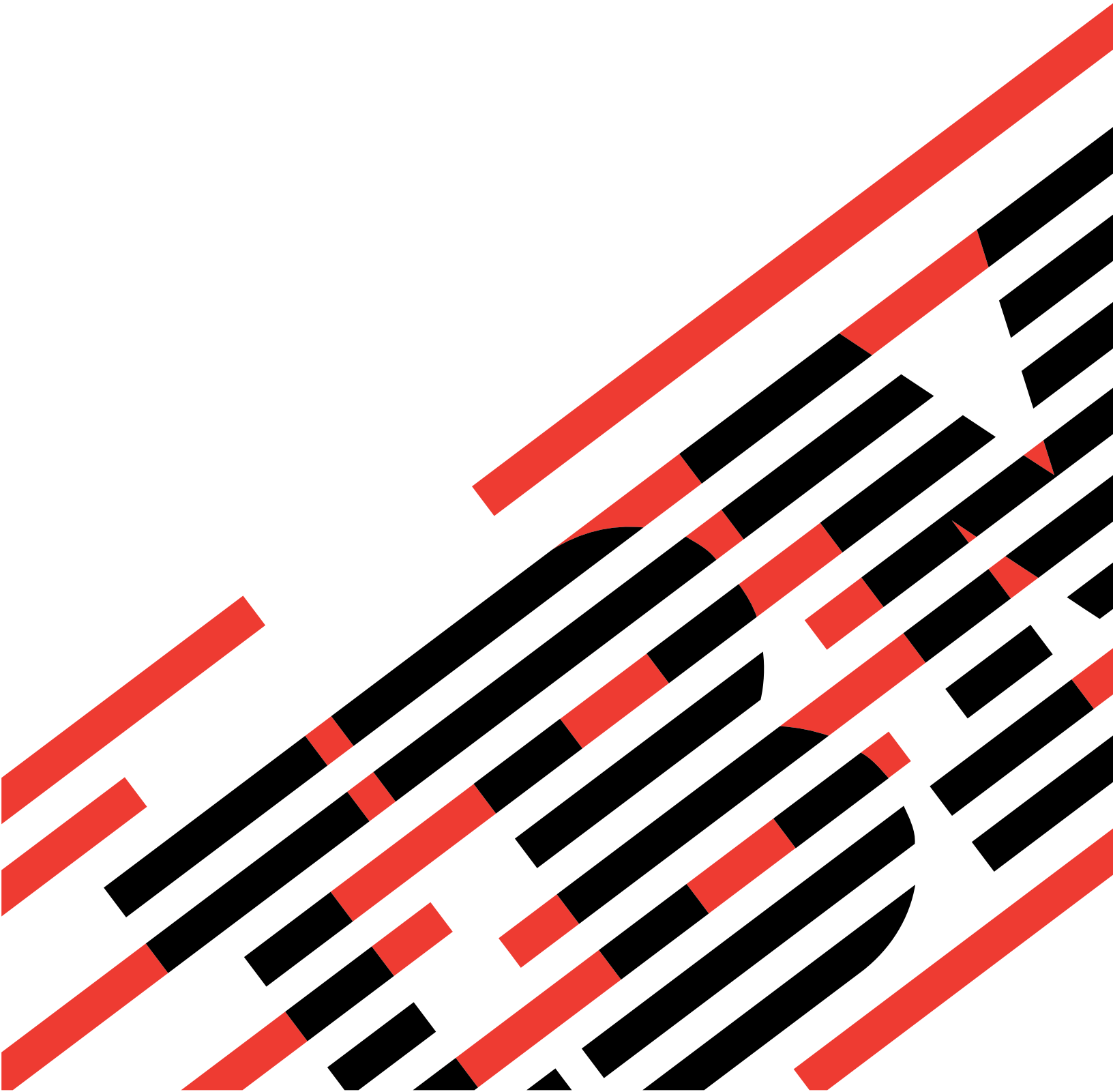
IBM

eserver

iSeries

リモート・アクセス・サービス: PPP 接続



IBM

@server

iSeries

リモート・アクセス・サービス: PPP 接続

目次

第 1 部 リモート・アクセス・サービス: PPP 接続

Point-to-Point Protocol (PPP) は、シリアル回線でデータを送信する際のインターネット標準です。これは、インターネット・サービス・プロバイダー (ISP) の間で最も広く利用されている接続プロトコルです。個々のコンピューターは PPP によってネットワークにアクセスすることができ、続いてそのネットワークがインターネットへのアクセスを提供します。 iSeries サーバーには、その広域ネットワーク (WAN) 接続の一部として TCP/IP PPP サポートが組み込まれています。

ロケーション間でデータの交換を行うには、PPP を使用して、iSeries サーバーとリモート・コンピューターを接続します。 iSeries サーバーに接続されたリモート・システムは、PPP を介して、サーバーと同じネットワークに属するリソースや他のマシンにアクセスできます。 iSeries サーバーを、PPP を使用してインターネットに接続するよう構成することもできます。 iSeries ナビゲーターのダイヤルアップ接続ウィザードは、 iSeries サーバーをインターネットまたは社内ネットワークに接続するプロセスのガイドとなります。

- 『V5R2 の新機能』では、このリリースでリモート・アクセス・サービスに加えられた更新について説明します。
- 『トピックの印刷』では、この情報の PDF 版をダウンロードしたり印刷したりする方法を示します。

リモート・アクセス・サービス: PPP 接続の理解

以下のトピックでは、iSeries 400 サーバーでのリモート・アクセス・サービスを簡潔に紹介します。ご使用のネットワーク用の PPP 環境を計画する際には、以下のトピックを参照することができます。

- 『**PPP シナリオ**』には、様々な接続における PPP のインプリメンテーション例があります。各例には説明が付けられ、PPP 接続を構成するためのサンプル値が示されています。
- 『**PPP の概念**』では、 PPP の概念、および PPP 接続のための iSeries 400 サーバー要件について説明します。
- 『**PPP の計画**』では、 PPP の概念、および PPP 接続のための iSeries 400 サーバー要件について説明します。

リモート・アクセス・サービス: PPP 接続の使用

以下のトピックでは、iSeries 400 サーバーにおける PPP 接続の構成と管理について説明します。

- 『**PPP の構成**』は、PPP 接続の構成ステップの概説です。
- 『**PPP の管理**』は、 PPP 接続の管理を行う際の手引きとして参照することができます。
- 『**PPP のトラブルシューティング**』では、基本的な PPP 接続エラーを説明し、関連したトラブルシューティング情報を示しています。

ここには、PPP に関するその他の情報もあります。このページには、関連した iSeries サーバーの役立つ情報へのリンクがあります。

第 1 章 V5R2 の新機能

V5R2 では、iSeries ナビゲーターを使って、 iSeries サーバーを起点とした PPP over Ethernet (PPPoE) 接続を確立することができます。このサポートは、物理イーサネット回線に結合された新しい PPPoE 仮想回線タイプを提供するものであり、 DSL に接続されたイーサネット LAN アダプターを使用して PPP 接続を確立します。 iSeries と ISP の間の接続がいったん開始されると、LAN 上の個々のユーザーは、 iSeries PPPoE 接続を介して ISP にアクセスすることができます。この新しい機能は、「発信元接続プロファイル」ダイアログまたはユニバーサル・コネクション・ウィザードを使用して、利用することができます。

詳しくは、『iSeries サーバーを PPPoE アクセス・コンセントレーターに接続する』を参照してください。

iSeries ナビゲーターになされたいくつかの追加により、PPP 接続の構成と管理がいっそう容易になりました。

- DHCP-WAN 構成ダイアログでは、DHCP-WAN クライアント・インターフェース用の IP アドレスを判別するために、 DHCP サーバーおよびクライアント・クライアントに自動的にコンタクトを取るようになります。このダイアログにアクセスするには、以下のようにします。
  - **「ネットワーク」→「リモート・アクセス・サービス」** を展開します。
  - **「リモート・アクセス・サービス」**を右マウス・ボタン・クリックします。
  - **「サービス」**を選択します。
  - **DHCP-WAN** タブを選択します。
- 改善された接続状況ダイアログには、 L2TP、L2TP マルチホップ、多重リンク、および PPP over Ethernet 接続について、接続の詳細が表示されるようになり、PPP 接続が管理しやすくなりました。
- 発信元および受信側のプロファイル、およびグループ・アクセス・ポリシーを作成する機能が、Task Pad に追加されました。
- 新規ダイヤル接続ウィザードおよびユニバーサル・コネクション・ウィザードは名前が変更されて、「新規インターネットまたは ISP ダイヤル接続 (New Internet or ISP Dial Connection)」および「新規 IBM ユニバーサル・コネクション (New IBM Universal Connection)」になりました。
- 着信呼び出しを待機する受信側接続プロファイルに割り当てられる PPP 回線およびモデムを、発信元接続プロファイルが「借りる」ことができるようになりました。発信元の接続は、接続終了時に PPP 回線およびモデムを受信側接続プロファイルに「戻し」ます。この新機能を使用可能にするには、PPP 回線構成ダイアログの「モデム」タブから**「動的リソース共用を使用可能にする (Enable dynamic resource sharing)」**オプションを選択します。 PPP 回線は、受信側シーバーおよび発信元の接続プロファイルの「接続」タブから構成できます。
- 回線プールの問題の可能性をなくすため、行プールのプロパティーは、使用中には変更できなくなりました。
- 「要求時起動側 (Initiator-on-demand)」および「要求時リモート・ダイヤル (Remote dial-on-demand)」動作モードは、 L2TP 接続を使用する発信元接続プロファイルから除去されました。

第 2 章 トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。
PDF ファイルを表示したり印刷したりするには、Adobe® Acrobat® Reader が必要です。これは、Adobe Web サイト (http://www.adobe.com/prodindex/acrobat/readstep.html)  からダウンロードできます。

PDF 版をダウンロードして表示するには、『リモート・アクセス・サービス: PPP 接続』  (約 986 KB、76 ページ) を選択します。

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューで、**「ファイル」**をクリックする。
3. **「名前を付けて保存」**をクリックする。
4. PDF を保存したいディレクトリーに進む。
5. **「保存」**をクリックする。

第 3 章 PPP シナリオ

PPP の機能と、ご使用のネットワークへの PPP 環境の実装方法を理解していただくため、ここでは、以下のようなシナリオを取り上げます。これらのシナリオは、PPP の基本的な概念を紹介するものであり、初心者であれ、熟達したユーザーであれ、タスクの計画と構成の前にここを参照するのは有益でしょう。

シナリオ: iSeries サーバーを PPPoE アクセス・コンセントレーターに接続する

多くの ISP は、PPPoE を使用する DSL 上の高速インターネット・アクセスを提供しています。 iSeries サーバーはこれらのサービス・プロバイダーに接続して、 PPP の利点を保持するブロードバンド接続を提供することができます。

シナリオ: リモート・ダイヤルイン・クライアントを iSeries サーバーに接続する

在宅勤務者やモバイル・クライアントなどのリモート・ユーザーは、会社のネットワークにアクセスしなければならなくなることがよくあります。こうしたダイヤルイン・クライアントは、PPP を使用して iSeries サーバーにアクセスできます。

シナリオ: モデムを使用してオフィス LAN をインターネットに接続する

普通、管理担当者は、従業員がインターネットにアクセスできるように、オフィス・ネットワークをセットアップします。 iSeries サーバーのインターネット・サービス・プロバイダー (ISP) への接続には、モデムが使用できます。 LAN に接続された PC クライアントは、 iSeries サーバーをゲートウェイとして用いて、インターネット通信を行うことができます。

シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する

モデムを使用することにより、2 つのリモート・ロケーション (本社と支社など) の間でデータの交換を行うことができます。 PPP を使って本社の iSeries サーバーと支社のもう 1 つの iSeries サーバーの間で接続を確立し、 2 つの LAN を接続することができます。

シナリオ: RADIUS NAS でダイヤルアップ接続を認証する

iSeries サーバー上で稼働する Network Access Server (NAS) は、ダイヤルイン・クライアントから別の RADIUS サーバーへ認証要求をルーティングすることができます。認証されると、RADIUS は IP アドレスとポートをユーザーに対して制御することもできます。

シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する

グループ・アクセス・ポリシーによって、接続のためのそれぞれのユーザー・グループを識別し、なんらかの共通の接続属性およびセキュリティー設定をグループ全体に適用することができます。 IP フィルター操作と組み合わせることにより、ネットワーク上の特定の IP アドレスへのアクセスを、許可したり制限したりすることができます。

シナリオ: PPP と DHCP を単一の iSeries サーバーに設置する

ダイヤルイン・クライアントやリモート・ユーザーは、 PPP を使用して、会社のネットワーク内の 1 つの iSeries サーバーにアクセスすることができます。同じ iSeries 上の DHCP 広域ネットワーク (WAN) クライアントにより、リモート・ユーザーは LAN 接続のユーザーと同じサービスを使用して、動的に割り当てられる IP アドレスを取得することができます。

シナリオ: DHCP と PPP を別個の iSeries サーバーに設置する

セキュリティーの配慮や、ネットワークの物理レイアウトのため、多くの企業ではネットワーク・サービスを分割し、別々のサーバーに分散します。このシナリオでは、PPP サーバーと DHCP サーバーを分けるという、さらに入り組んだ事柄について扱います。このセットアップによって、リモート・ユーザーは、前のシナリオと同様に、会社のネットワークにダイヤルインしたりアクセスしたりすることができます。

シナリオ: PPP と VPN: VPN が保護する L2TP 任意トンネル

支社は、レイヤー 2 トンネリング・プロトコル (L2TP) を通して本社に接続することができます。 L2TP 任意トンネルは、仮想 PPP リンクを確立します。事実上、L2TP は本社のネットワークを拡張して、支社が本社のサブネットの一部であるかのようにします。 VPN は、L2TP トンネルを介したデータ・トラフィックを保護します。

シナリオ: iSeries サーバーを PPPoE アクセス・コンセントレーターに接続する

状況: ビジネスでもっと速いインターネット接続が必要とされるため、地元の ISP による DSL サービスに関心があります。初期調査の後、ISP が PPPoE を使用してそのクライアントに接続していることがわかりました。この PPPoE 接続を使用して、iSeries サーバーを介したブロードバンド・インターネット接続を提供しようと思います。

図 1. PPPoE による iSeries サーバーから ISP への接続

ソリューション: iSeries サーバーを介して、 ISP への PPPoE 接続をサポートすることができます。iSeries サーバーは新しい PPPoE 仮想回線を利用します。これは、タイプ 2838 イーサネット・アダプターを使用するように構成された、物理イーサネット回線に結び付いています。この仮想回線は、イーサネット LAN 上の PPP セッション・プロトコルをサポートします。そのイーサネット LAN は、リモート ISP へのゲートウェイを提供する DSL に接続しています。これにより LAN 接続のユーザーは、iSeries サーバ

ーの PPPoE 接続を使用して、高速のインターネット・アクセスを実現できます。 iSeries と ISP の間の接続がいったん開始されると、LAN 上の個々のユーザーは、 iSeries サーバーに割り振られた IP アドレスを使用して、PPPoE 上で ISP にアクセスできます。追加のセキュリティーを提供するには、PPPoE 仮想回線にフィルター規則を適用して、特定の着信インターネット・トラフィックを制限することができます。

サンプル構成:

1. ISP とともに使用する接続装置を構成します。
2. iSeries サーバーで、発信元接続プロファイルを構成します。

   必ず、次の情報を入力してください。

   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: PPP over Ethernet
   - **動作モード**: 起動側 (Initiator)
   - **リンク構成**: 単一回線
3. 「新規 2 地点間プロファイルのプロパティー」の**「一般」**ページで、発信元プロファイルの名前と記述を入力します。この名前は、接続プロファイルと仮想 PPPoE 回線の両方を指します。
4. **「接続」**ページをクリックします。この接続プロファイルの名前に対応する **PPPoE 仮想回線名**を選択します。回線を選択した後、iSeries ナビゲーターは回線プロパティーのダイアログを表示します。
   a. **「一般」**ページで、PPPoE 仮想回線のわかりやすい説明を入力します。
   b. **「リンク」**ページをクリックします。物理回線名の選択リストで、 この接続で使用するイーサネット回線を選択し、**「開く」**をクリックします。あるいは、新しいイーサネット回線を定義する必要がある場合には、回線名を入力して**「新規」**をクリックします。 iSeries ナビゲーターはイーサネット回線のプロパティー・ダイアログを表示します。**注:** PPPoE には、タイプ 2838 のイーサネット・アダプターが必要です。
      1) **「一般」**ページで、イーサネット回線のわかりやすい説明を入力し、回線定義が適切なハードウェア・リソースを使用していることを確認してください。
      2) **「リンク」**ページをクリックします。物理イーサネット回線のプロパティーを入力します。詳しくは、イーサネット・カードの資料およびオンライン・ヘルプを参照してください。
      3) **「その他」**ページをクリックします。他のユーザーがこの回線に対して持つアクセス水準および権限を指定します。
      4) **「OK」**をクリックして、PPPoE 仮想回線のプロパティー・ページに戻ります。
   c. **「制限 (Limits)」**をクリックして LCP 認証のプロパティーを定義するか、または**「OK」**をクリックして「新規 2 地点間プロファイル」の**「接続」**ページに戻ります。
5. iSeries サーバーが自身の認証を行うことを ISP が求めている場合、または iSeries がリモート・サーバーの認証を行うようにしたい場合は、**「認証」**ページをクリックします。詳しくは、『システムの認証』を参照してください。
6. **「TCP/IP 設定 (TCP/IP Settings)」**ページをクリックし、この接続プロファイルの IP アドレス処理の各パラメーターを指定します。 LAN 接続のユーザーが、iSeries サーバーに割り振られた IP アドレスを使用して ISP に接続できるようにするには、**「アドレスを隠す (Hide addresses; Full masquerading)」**を選択します。
7. **「DNS」**ページをクリックし、 ISP が提供する DNS サーバーの IP アドレスを入力します。
8. 接続ジョブを実行するサブシステムを指定したい場合は、**「その他」**ページをクリックします。
9. **「OK」**をクリックしてプロファイルを完成させます。

外部 IP アドレスや iSeries リソースへのユーザー・アクセスの制限についての詳細は、 IP フィルター操作および グループ・アクセス・ポリシーを参照してください。

シナリオ: リモート・ダイヤルイン・クライアントを iSeries サーバーに接続する

状況: あなたは、会社のネットワークの管理担当者として、 iSeries サーバーとネットワーク・クライアントの両方を保守しなければなりません。あなたは、仕事場に来て問題の障害追及と修正を行うよりも、自宅のようなリモート・ロケーションから作業したいと思っています。会社には、インターネットに出て行くためのネットワーク接続がないので、あなたは PPP 接続を使用して iSeries サーバーにダイヤルインすることになるでしょう。また、あなたが現在所有しているモデムは、7852-400 ECS モデムだけであり、接続にはこのモデムを利用したいと思っています。

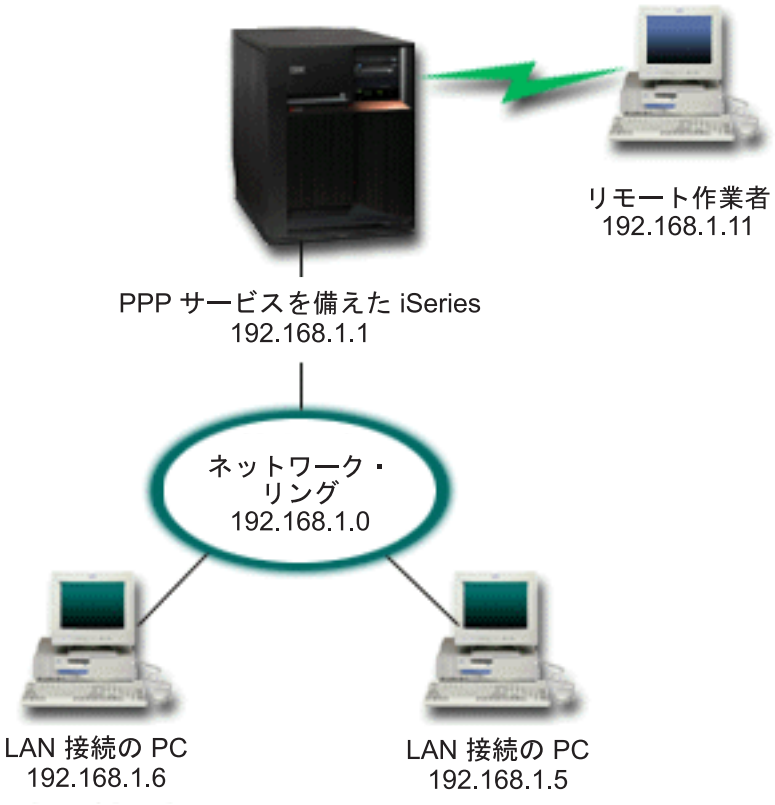


図 2. リモート・クライアントを iSeries サーバーに接続する

ソリューション: PPP を使用し、手持ちのモデムを用いて自宅の PC を iSeries サーバーに接続することができます。このタイプの PPP 接続に ECS モデムを使用するので、そのモデムが同期と非同期の両方のモードで構成されていることを確認する必要があります。上の図は、2 つの PC を持つ LAN に接続された、PPP サービスを備えた iSeries サーバーを示しています。リモート作業者は、iSeries サーバーにダイヤルインし、自らを認証して、作業ネットワーク (192.168.1.0) の一部となります。この場合、ダイヤルイン・ クライアントに静的な IP アドレスを割り当てるのは、非常に簡単です。

リモート作業者は、iSeries サーバーでの認証に CHAP-MD5 を使用します。 iSeries では MS_CHAP を使用することはできないので、PPP クライアントは、必ず CHAP-MD5 を使用するように設定されていなければなりません。

上に示したようにリモート作業者が会社のネットワークにアクセスできるようにしたい場合は、 TCP/IP スタックと PPP レシーバー・プロファイルで IP 転送をオンに設定する必要があります。また、IP ルーティングを正しく構成する必要もあります。ネットワーク内でリモート・クライアントが実行できるアクションを制限したり保護したりするには、 IP パケットを処理するためのフィルター規則を使用することができます。

ECS モデムが 1 度に処理できる接続は 1 つだけなので、上の図には、リモート・ダイヤルイン・クライアントが 1 つしかありません。同時に複数のダイヤルイン・クライアントが必要な場合は、『PPP の計画』セクションにあるハードウェアとソフトウェアの両方に関する考慮事項を参照してください。

サンプル構成:

1. ダイヤルアップ・ネットワーキングを構成し、リモート PC 上にダイヤルアップ接続を作成します。
2. iSeries サーバーで、受信側接続プロファイルを構成します。

   必ず、次の情報を入力してください。

   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: 応答
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。
3. 「新規 2 地点間プロファイルのプロパティー」の**「一般」**ページで、レシーバー・プロファイルの名前と記述を入力します。
4. **「接続」**ページをクリックします。適切な**回線**の**名前**を選択するか、新しい名前を入力し、**「新規」**をクリックして新規の回線を作成します。
   a. **「一般」**ページで、存在するハードウェア・リソースを強調表示し、「フレーム指示」に**「非同期」**を設定します。
   b. **「モデム」**ページをクリックします。名前選択リストから、**IBM 2772** モデムを選択します。
   c. **「OK」**をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
5. **「認証」**ページをクリックします。
   a. **「この iSeries サーバーがリモート・システムの識別を検査することが必要」**を選択します。
   b. **「妥当性検査リストを使用してローカルから認証」**を選択し、新規のリモート・ユーザーを妥当性検査リストに追加する。
   c. **「暗号化されたパスワード (CHAP-MD5) を許可」**を選択します。
6. **「TCP/IP 設定」**ページをクリックします。
   a. ローカル IP アドレス `192.168.1.1` を選択します。
   b. リモート・アドレスの場合は、開始アドレスが `192.168.1.11` である**「固定 IP アドレス」**を選択します。
   c. **「リモート・システムが他のネットワークにアクセスすること (IP 転送) を許可」**を選択します。
7. **「OK」**をクリックしてプロファイルを完成させます。

シナリオ: モデムを使用してオフィスの LAN をインターネットに接続する

状況: いま、あなたの会社が使用している会社のアプリケーションにおいて、ユーザーがインターネットにアクセスする必要が生じています。アプリケーションでは、大量のデータの交換は必要ないため、あなたは iSeries サーバーと LAN に接続された PC クライアントの両方を、モデムを使ってインターネットに接続できたらよいと思っています。この状況を次の図で説明します。

図 3. モデムを使用してオフィスの LAN をインターネットに接続する

ソリューション: ECS (または互換性のあるその他の) モデムを使用して iSeries をインターネット・サービス・プロバイダー (ISP) に接続することができます。 ISP への PPP 接続を確立するには、サーバー上に PPP 発信元プロファイルを作成する必要があります。

iSeries と ISP の間に接続を確立すると、LAN 接続 PC が、iSeries をゲートウェイとして使用して、インターネットと通信することができるようになります。発信元プロファイルでは、「アドレスを隠す」オプシ

ョンがオンになり、予約済みの IP アドレスを保持している LAN クライアントがインターネットと通信できるようになっていることを確認する必要があるでしょう。

iSeries とネットワークがインターネットに接続するにあたっては、セキュリティーのリスクを理解していなければなりません。利用している ISP についてよく研究してそのセキュリティー・ポリシーを理解し、サーバーとネットワークを保護するためのさらなる処置を講じてください。

このタイプの PPP 接続に ECS モデムを使用する場合は、そのモデムを非同期通信用に構成してください。インターネットの使用状況によっては、帯域幅が問題になることがあります。接続の帯域幅を増す方法についての詳細は、計画セクションを参照してください。

サンプル構成:

1. iSeries サーバーで、発信元接続プロファイルを構成します。

   必ず、次の情報を選択してください。

   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: ダイヤル
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。
2. 「新規 2 地点間プロファイルのプロパティー」の**「一般」**ページで、発信元プロファイルの名前と記述を入力します。
3. **「接続」**ページをクリックします。適切な回線名を選択するか、新しい名前を入力し、**「新規」**をクリックして新規の回線を作成します。
   a. 新規回線のプロパティーの**「一般」**ページで、存在するハードウェア・リソースを強調表示し、「フレーム指示」に**「非同期」**を設定します。
   b. **「モデム」**ページをクリックします。名前選択リストから、使用するモデムを選択します。
   c. **「OK」**をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
4. **「追加」**をクリックして、ISP サーバーに接続するのにダイヤルする電話番号を入力します。必須の接頭部を必ず含めるようにしてください。
5. **「認証」**ページをクリックし、**「リモート・システムがこの iSeries サーバーの識別を検査することを許可」**を選択します。認証プロトコルを選択し、必要なユーザー名やパスワードの情報を入力します。
6. 「TCP/IP 設定」ページをクリックします。
   a. リモートとローカルの両方の IP アドレスに対して、**「リモート・システムによる割り当て」**を選択します。
   b. **「リモート・システムをデフォルト経路として追加」**を選択します。
   c. **「アドレスを隠す」**をチェックし、内部 IP アドレスがインターネットに経路指定されないようにします。
7. **「DNS」**ページをクリックし、 ISP が提供する DNS サーバーの IP アドレスを入力します。
8. **「OK」**をクリックしてプロファイルを完成させます。

接続プロファイルを使用してインターネットに接続する場合は、「オペレーション・ナビゲーター」から、接続プロファイルを右マウス・ボタン・クリックして、**「開始」**を選択します。状況が**「活動中 (Active)」**に変われば接続は正常です。最新表示を行って表示を更新してください。

注: ネットワーク上のその他のシステムでも適切なルーティングが定義され、それらのシステムから出されるインターネットに向かう TCP/IP トラフィックが iSeries サーバーに送信されるようになっていることを確認する必要があります。

シナリオ: モデムを使用して会社のネットワークとリモート・ネットワークを接続する

状況: 支社と本社のネットワークが異なる 2 つのロケーションにあるとします。支社は、毎日、本社と接続して、データ入力アプリケーションのためのデータベース情報を交換する必要があります。データ交換量は、物理ネットワーク接続を購入するほどのものではないので、あなたは、モデムを使用して、必要な 2 つのネットワークを接続することに決めました。

図 4. モデムを使用して会社のネットワークとリモート・ネットワークを接続する

ソリューション: PPP では、上の図のように、各 iSeries サーバー間に接続を確立することで、2 つの LAN を接続することができます。ここでは、リモート・オフィスが本社への接続を開始するものと想定しましょう。あなたは、リモート iSeries 上に発信元プロファイルを構成し、本社のサーバー上にレシーバー・プロファイルを作成することになります。

リモート・オフィスの PC が、会社の LAN (192.168.1.0) にアクセスする必要がある場合は、本社のレシーバー・プロファイルの IP 転送をオンにする必要があります。また、IP アドレス・ルーティングが PC で使用できるようにする必要もあります (この例では、 192.168.2、192.168.3、192.168.1.6、および 192.168.1.5)。さらに、TCP/IP スタックの IP 転送も活動化しておく必要があります。このように構成することで、LAN の間の基本的な TCP/IP 通信が可能になります。セキュリティー要素や LAN の中のホスト名を決定する DNS についても考慮する必要があります。

サンプル構成:

1. リモート・オフィスの iSeries サーバーで、発信元接続プロファイルを構成します。
   必ず、次の情報を選択してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: ダイヤル
   - **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。
2. 「新規 2 地点間プロファイルのプロパティー」の**「一般」**ページで、発信元プロファイルの名前と記述を入力します。
3. **「接続」**ページをクリックします。適切な回線名を選択するか、新しい名前を入力し、**「新規」**をクリックして新規の回線を作成します。
   a. 新規回線のプロパティーの**「一般」**ページで、存在するハードウェア・リソースを強調表示し、「フレーム指示」に**「非同期」**を設定します。
   b. **「モデム」**ページをクリックします。名前選択リストから、使用するモデムを選択します。
   c. **「OK」**をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
4. **「追加」**をクリックして、本社の iSeries サーバーに接続するのにダイヤルする電話番号を入力します。必須の接頭部を必ず含めるようにしてください。
5. **「認証」**ページをクリックし、**「リモート・システムがこの iSeries サーバーの識別を検査することを許可」**を選択します。**「暗号化されたパスワードを使う (CHAP-MD5)」**を選択し、必要なユーザー名やパスワードの情報を入力します。
6. **「TCP/IP 設定」**ページをクリックします。
   a. ローカル IP アドレスとして、**「固定 IP アドレスを使用」**選択ボックスから、リモート・オフィスの LAN インターフェース (192.168.2.1) の IP アドレスを選択します。
   b. リモート IP アドレスに対し、**「リモート・システムによる割り当て」**を選択します。
   c. ルーティング・セクションで、**「リモート・システムをデフォルト経路として追加」**を選択します。
   d. **「OK」**をクリックして発信元プロファイルを完成させます。
7. 本社の iSeries サーバー上に、**受信側接続プロファイル**を構成します。
   必ず、次の情報を選択してください。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: 交換回線
   - **動作モード**: 応答

- **リンク構成**: これは、環境によって、単一回線または回線プールのいずれかになります。

8. 「新規 2 地点間プロファイルのプロパティー」の**「一般」**ページで、レシーバー・プロファイルの名前と記述を入力します。
9. **「接続」**ページをクリックします。適切な回線名を選択するか、新しい名前を入力し、**「新規」**をクリックして新規の回線を作成します。
   a. **「一般」**ページで、存在するハードウェア・リソースを強調表示し、「フレーム指示」に**「非同期」**を設定します。
   b. **「モデム」**ページをクリックします。名前選択リストから、使用するモデムを選択します。
   c. **「OK」**をクリックして「新規 2 地点間プロファイルのプロパティー」ページに戻ります。
10. **「認証」**ページをクリックします。
   a. **「この iSeries サーバーがリモート・システムの識別を検査することが必要」**をチェックします。
   b. 妥当性検査リストに新規リモート・ユーザーを追加します。
   c. 「CHAP-MD5」認証をチェックします。
11. **「TCP/IP 設定」**ページをクリックします。
   a. ローカル IP アドレスに、選択ボックスから、本社のインターフェースの IP アドレス (192.168.1.1) を選択します。
   b. リモート IP アドレスには、**「リモート・システムのユーザー ID を基にする」**を選択します。「ユーザー名によって定義されている IP アドレス」ダイアログが現れます。**「追加」**をクリックします。呼び出し元ユーザー名、IP アドレス、サブネット・マスクのフィールドに入力してください。このシナリオでは、次のように入力するのが適当でしょう。
      - 「呼び出し元ユーザー名」: `Remote_site`
      - 「IP アドレス」: `192.168.2.1`
      - 「サブネット・マスク」: `255.255.255.0`

      「OK」をクリックし、再度**「OK」**をクリックして「TCP/IP 設定」ページに戻ります。
   c. **「IP 転送」**を選択して、ネットワーク内のその他のシステムがこの iSeries サーバーをゲートウェイとして使用できるようにしてください。
12. **「OK」**をクリックしてレシーバー・プロファイルを完成させます。

シナリオ: RADIUS NAS でダイヤルアップ接続を認証する

状況: 会社のネットワークには、分散ダイヤルアップ・ネットワークから 2 台の iSeries サーバーにダイヤルインするリモート・ユーザーがいます。認証、サービス、およびアカウンティングを集中管理する方法として、 1 台のサーバーでユーザー ID とパスワードの妥当性検査のための要求を処理し、どの IP アドレスが自分たちに宛てられたものかを判別するようにします。

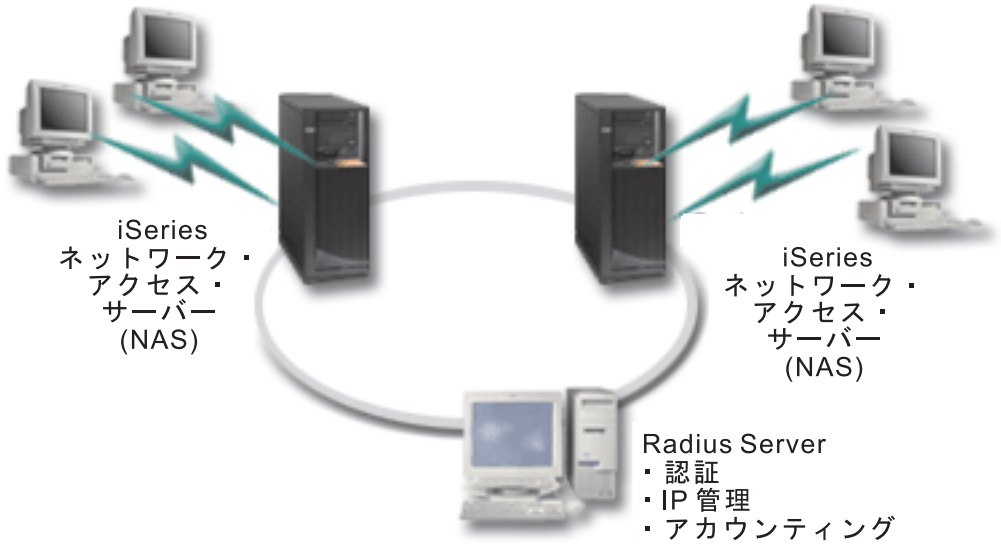


図 5. RADIUS サーバーによるダイヤルアップ接続の認証

ソリューション: ユーザーが接続を試行すると、 iSeries サーバーで稼働している Network Access Server (NAS) は、ネットワーク上の RADIUS サーバーに認証情報を転送します。 RADIUS サーバーは会社のネットワークのためのすべての認証確認を保守し、認証の要求と応答を処理します。ユーザーが妥当性検査される場合、相手側の IP アドレスを割り当てるように RADIUS サーバーを構成することもでき、 RADIUS サーバーはアカウンティングを活動化して、ユーザー・アクティビティーおよび使用状況を追跡することができます。 RADIUS をサポートするためには、iSeries 上に RADIUS NAS サーバーを定義する必要があります。

サンプル構成:

1. iSeries ナビゲーターで、**「ネットワーク」**を展開し、**「リモート・アクセス・サービス」**を右マウス・ボタン・クリックして、**「サービス」**を選択します。
2. **「RADIUS」** タブで、**「RADIUS ネットワーク・アクセス・サーバー接続を使用可能にする (Enable RADIUS Network Access Server connection)」**と、**「RADIUS を認証に使用可能にする (Enable RADIUS for authentication)」**を選択します。ご使用の RADIUS ソリューションによりますが、RADIUS ハンドル接続アカウンティングおよび TCP/IP アドレス構成を使用可能にすることもできます。
3. **「RADIUS NAS 設定 (RADIUS NAS settings)」**ボタンをクリックします。
4. **「一般」**ページで、このサーバーの説明を入力します。
5. 「認証サーバー」ページ (および、オプションで「アカウンティング・サーバー」ページでも)、**「追加」**をクリックして以下の情報を入力します。
   a. **「ローカル IP アドレス」**ボックスでは、 RADIUS サーバーとの接続に使用する iSeries インターフェース用の IP アドレスを入力します。
   b. **「サーバー IP アドレス」**ボックスでは、 RADIUS サーバー用の IP アドレスを入力します。
   c. **「パスワード」**ボックスでは、 RADIUS サーバーに対して iSeries サーバーを識別させるために使用するパスワードを入力します。

d. **「ポート」**ボックスでは、 RADIUS サーバーとの通信に使用する iSeries 上のポートを入力します。認証サーバーにはポート 1812 を、アカウンティング・サーバーにはポート 1813 を入力します。

6. **「OK」**をクリックします。
7. iSeries ナビゲーターで、**「ネットワーク」→「リモート・アクセス・サービス」**を展開します。
8. 認証用に RADIUS サーバーを使用する予定の接続プロファイルを選択します。 RADIUS サービスは、受信側接続プロファイルにのみ適用できます。
9. 「認証」ページで、**「この iSeries サーバーがリモート・システムの識別を検査することが必要」**を選択します。
10. **「RADIUS サーバーを使用してリモート側で認証 (Authenticate remotely using a RADIUS server)」**を選択します。
11. 認証プロトコルを選択します (EAP、PAP、または CHAP-MD5)。このプロトコルは RADIUS サーバーでも使用されていなければなりません。詳しくは、『システムの認証』を参照してください。
12. **「接続の編集とアカウンティングに RADIUS を使用する (Use RADIUS for connection editing and accounting)」**を選択します。
13. **「OK」**をクリックして、接続プロファイルへの変更を保管します。

RADIUS サーバーのセットアップも行う必要があります。これには、認証プロトコル、ユーザー・データ、パスワード、およびアカウンティング情報のサポートが含まれています。詳しくは、ご使用の RADIUS ベンダー資料を参照してください。

この接続プロファイルを使用してユーザーがダイヤルインすると、指定された RADIUS サーバーに iSeries は認証情報を転送します。ユーザーが妥当性検査された場合、接続は許可され、 RADIUS サーバー上のユーザーの情報で指定されている接続制限を使用することになります。

シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する

状況: ネットワークには、いくつかのグループの分散ユーザーがあり、それぞれのユーザーについて、社内 LAN 上で異なるリソースにアクセスする必要があります。データ入力ユーザーのグループは、データベースとその他のいくつかのアプリケーションへのアクセスが必要であり、一方、ビジネス・パートナーは、HTTP、FTP、および Telnet サービスへのダイヤルアップ・アクセスが必要になるものの、セキュリティーの理由から、他の TCP/IP サービスまたはトラフィックにアクセスすることは許可されません。それぞれのユーザーについて詳細に渡る接続属性および許可を定義するのは労力の重複であり、この接続のすべてのユーザーに対してネットワーク制限を提供するなら、十分な制御を提供できなくなります。このサーバーに定期的にダイヤルするユーザーで構成されるいくつかの特定のグループについて、接続設定および許可を定義できるような方法が必要でしょう。

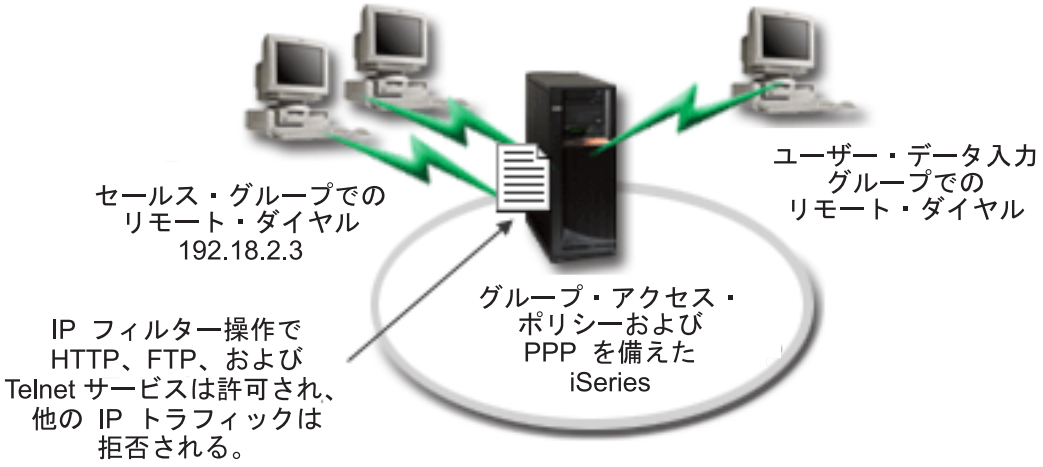


図 6. グループ・ポリシー設定に基づいて接続設定をダイヤルアップ接続に適用する

ソリューション: 2 つの異なるユーザーのグループにそれぞれ固有の IP フィルター制限を適用する必要があります。これを達成するには、グループ・アクセス・ポリシーおよび IP フィルター規則を作成します。グループ・アクセス・ポリシーは IP フィルター規則を参照するので、最初にフィルター規則を作成する必要があります。この例では、PPP フィルターを作成して、「ビジネス・パートナー」グループ・アクセス・ポリシーについての IP フィルターを組み込む必要があります。これらのフィルター規則は HTTP、FTP、および Telnet サービスを許可するものの、 iSeries サーバーを介したその他のすべての TCP/IP トラフィックおよびサービスへのアクセスは制限します。このシナリオでは、セールス・グループで必要なフィルター規則のみ示します。ただし、「データ入力」グループに類似したフィルターを設定することもできます。

最後に、グループ・アクセス・ポリシーを (グループごとに 1 つずつ) 作成して、グループを定義する必要があります。グループ・アクセス・ポリシーを使用すると、共通接続属性をユーザーのグループに定義することができます。 iSeries サーバーでグループ・アクセス・ポリシーを 妥当性検査リストに追加することにより、認証プロセスの際にこれらの接続設定を適用できます。このグループ・アクセス・ポリシーは、ユーザーのセッションにいくつかの設定を指定します。これには、IP アドレスを制限する IP フィルター規則を適用する機能、およびセッション中にユーザーが使用できる TCP/IP サービスが含まれます。

サンプル構成:

1. このグループ・アクセス・ポリシーの許可および制限を指定する PPP フィルター ID および IP パケット・フィルターを作成します。 IP フィルターについての詳細は、 IP パケット規則 (フィルター操作および NAT) を参照してください。
   a. iSeries ナビゲーターで、**「ネットワーク」→「リモート・アクセス・サービス」**を展開します。
   b. **「受信側接続プロファイル」**をクリックし、この接続の接続プロファイルを右マウス・ボタンでクリックしてから、**「プロパティー」**を選択します。
   c. **「TCP/IP 設定」**タブを選択してから、**「拡張」**を選択します。
   d. **「IP パケット規則をこの接続に使用」**を選択してから、**「規則ファイルの編集 (Edit Rules File)」**をクリックします。これにより、IP パケット規則エディターが始動し、 PPP フィルター・パケット規則ファイルがオープンします。
   e. **「挿入 (Insert)」**メニューをオープンしてから、**「フィルター (Filters)」**を選択して、フィルター・セットを追加します。**「一般」**タブを使用してフィルター・セットを定義し、**「サービス」**タブを使用して、HTTP などの、許可するサービスを定義します。以下のフィルター・セット、

″services_rules″ では、HTTP、FTP、および Telnet サービスが使用可能です。フィルター規則には、暗黙的デフォルト否定ステートメントが組み込まれ、明示的に許可されていない任意の TCP/IP サービスまたは IP トラフィックを制限します。

注: 以下の例の IP アドレスは、グローバル経路指定が可能であり、例としてのみ使用できます。

```
###The following 2 filters will permit HTTP (Web browser) traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 80 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        80 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = * SRCADDR =  %
        * DSTADDR = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS =  %
        NONE JRN = OFF

###The following 4 filters will permit FTP traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 21 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        21 FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.18.2.3 PROTOCOL = TCP DSTPORT = 20 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.18.2.3 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT =  %
        20 FRAGMENTS = NONE JRN = OFF

###The following 2 filters will permit telnet traffic in & out of the system.

FILTER SET services_rules ACTION = PERMIT DIRECTION = INBOUND SRCADDR  %
        = * DSTADDR = 192.54.5.1 PROTOCOL = TCP DSTPORT = 23 SRCPORT  %
        = * FRAGMENTS = NONE JRN = OFF

FILTER SET services_rules ACTION = PERMIT DIRECTION = OUTBOUND SRCADDR  %
        = 192.54.5.1 DSTADDR = * PROTOCOL = TCP DSTPORT = * SRCPORT  %
        = 23 FRAGMENTS = NONE JRN = OFF
```

f. **「挿入 (Insert)」**メニューをオープンしてから、**「フィルター・インターフェース (Filter Interface)」**を選択します。フィルター・インターフェースを使用して PPP フィルター ID を作成し、定義したフィルター・セットを組み込みます。

   1) 「一般」タブで PPP フィルター ID に

      ```
      permited_services
      ```

      と入力します。

   2) **「フィルター・セット」**タブで、フィルター・セット **services_rules** を選択してから、**「追加」**をクリックします。

   3) 「OK」をクリックします。規則ファイルに以下の行が追加されます。

      ```
      ###The following statement binds (associates) the 'services_rules' filter set with the
      PPP filter ID "permitted_services." This PPP filter ID
      can then be applied to the physical interface associated with a PPP connection profile
      ```

```
or Group Access Policy.

FILTER_INTERFACE PPP_FILTER_ID = permited_services SET = services_rules
```

g. 変更を保管し、終了します。後でこの変更を元に戻す必要が生じた場合には、文字ベースのインターフェースを使用して次のコマンドを入力します。

```
RMVTCPTBL
```

これで、サーバー上のすべてのフィルター規則および NAT を除去できます。

h. **「拡張 TCP/IP 設定 (Advanced TCP/IP settings)」**ダイアログでは、**「PPP フィルター ID (PPP filter identifier)」**ボックスをブランクにし、**「OK」**をクリックして終了します。後で、この接続プロファイルにではなく、グループ・アクセス・ポリシーに、この作成したばかりのフィルター ID を適用する必要があります。

2. このユーザー・グループに新規のグループ・アクセス・ポリシーを定義します。グループ・アクセス・ポリシーのオプションについての詳細は、『グループ・アクセス・ポリシーの構成』を参照してください。
   a. iSeries ナビゲーターで、**「ネットワーク」→「リモート・アクセス・サービス」>「受信側接続プロファイル」**を展開します。
   b. 「グループ・アクセス・ポリシー」アイコンを右マウス・ボタン・クリックしてから、「新規グループ・アクセス・ポリシー」を選択します。 iSeries ナビゲーターは、「新規グループ・アクセス・ポリシー」定義ダイアログを表示します。
   c. 「一般」ページで、「グループ・アクセス・ポリシー」に名前および説明を入力します。
   d. **「TCP/IP 設定」**ページで以下のようにします。
      - **「この接続に IP パケット規則を使用する (Use IP packet rules for this connection)」**を選択し、 PPP フィルター ID **permitted_services** を選択します。
   e. **「OK」**を選択し、グループ・アクセス・ポリシーを保管します。
3. このグループに関連付けられるユーザーにグループ・アクセス・ポリシーを適用します。
   a. これらのダイヤルアップ接続を制御する受信側接続プロファイルを選択します。
   b. 受信側接続プロファイルの**「認証」**ページでは、ユーザーの認証情報を含む妥当性検査リストを選択してから、**「開く」**をクリックします。
   c. セールス・グループで、グループ・アクセス・ポリシーを適用させたいユーザーを選択してから、**「開く」**をクリックします。
   d. **「グループ・ポリシーをユーザーに適用する」**をクリックしてから、ステップ 2 で定義されたグループ・アクセス・ポリシーを選択します。
   e. それぞれのセールス・ユーザーごとに繰り返します。

PPP 接続を介したユーザーの認証についての詳細は、 『システムの認証』を参照してください。

第 4 章 PPP の概念

iSeries サーバーをリモート・ネットワーク、クライアント PC、他の iSeries または ISP に接続するには、PPP を使用できます。このプロトコルを十分に使用するには、このプロトコルの機能および iSeries サポートの両方を理解しなければなりません。詳細については、以下のトピックを参照してください。

PPP とは?
2 地点間プロトコル (PPP) は、 1 つのコンピューターから別のコンピューターに接続するのに使用される TCP/IP プロトコルです。詳細な定義は、このトピックを参照してください。

接続プロファイル
2 地点間接続プロファイルは、特定の PPP 接続のパラメーターおよびリソースのセットを定義します。これらのパラメーターを使用するプロファイルを開始すると、ダイヤルアウト (発信) または PPP 接続の listen (受信) ができます。

グループ・アクセス・ポリシー
これらのポリシーは、ユーザーのグループについて、接続のセットおよびセキュリティー属性を定義します。ご使用のシステムでこれらを定義することについての詳細は、このトピックを参照してください。

PPP とは?

コンピューターは、**PPP**、つまり **2 地点間プロトコル**を使用し、電話回線を通してインターネット上の通信を行います。 PPP 接続は、2 つのシステムが電話回線を通して物理的に接続したときに存在することになります。 1 つのシステムを他のシステムに接続するには、PPP を使用することができます。たとえば、支社と本社の間に PPP 接続が確立されると、これらのオフィスはどちらも、ネットワークを介してもう一方のオフィスにデータを転送できるようになります。

PPP はインターネット標準です。これは、インターネット・サービス・プロバイダー (ISP) の間で最も広く利用されている接続プロトコルです。 ISP へは PPP を使用して接続することができ、ISP によってインターネットへの接続が可能になります。

PPP は、メーカーの異なるリモート・アクセス・ソフトウェア間の相互運用を可能にしています。 PPP ではまた、複数のネットワーク通信プロトコルが同じ物理通信回線を使用することもできます。

PPP プロトコルについては、以下の Request For Comment (RFC) 標準が記述しています。 RFC の詳細については、http://www.rfc-editor.org を参照してください。

- RFC1661 Point-to-Point Protocol
- RFC1662 PPP on HDLC-like framing
- RFC1994 PPP CHAP

接続プロファイル

V5R2 は 2 つのタイプのプロファイルを使用して、 PPP 接続または接続のセットについて、特性のセットを定義できるようにします。

- **発信元接続プロファイル**は、ローカル iSeries サーバーから発信されて、リモート・システムによって受信される 2 地点間接続です。アウトバウンド接続は、このオブジェクトを使用して構成することができます。

- **受信側接続プロファイル**は、リモート・システムから発信されて、ローカル iSeries サーバーによって受信される 2 地点間接続です。インバウンド接続は、このオブジェクトを使用して構成することができます。

接続プロファイルは、PPP 接続の働きを定義しています。接続プロファイル内の情報には、以下の質問の答えがあります。

- どのタイプの接続プロトコルを使用しますか (PPP それとも SLIP ですか)。
- iSeries サーバーは、ダイヤルアウトによってその他のコンピューターと接触しますか (発信元ですか)。それとも、他のシステムからの呼び出しを受信待機しますか (受信側ですか)。
- 接続ではどの通信回線を使用しますか。
- iSeries サーバーはどのように、使用する IP アドレスを決定しますか。
- iSeries サーバーはどのように他のシステムを認証しますか。 iSeries サーバーはどこに認証情報を保管しますか。

接続プロファイルは、以下の詳細事項を論理的に表したものです。

- 回線およびプロファイル・タイプ
- 多重リンク設定
- リモート電話番号およびダイヤル・オプション
- 認証
- TCP/IP 設定: IP アドレスおよびルーティング、および IP フィルター
- 実行管理機能および接続カスタマイズ
- ドメイン・ネーム・サーバー

iSeries は、接続プロファイル内にこれらの構成情報を保管します。この情報は、 iSeries サーバーが他のコンピューター・システムとの PPP 接続を確立するのに必要なコンテキストを示しています。接続プロファイルには、次の情報が含まれます。

- **プロトコル・タイプ**。 PPP か SLIP を選択することができます。 IBM は、可能な限り PPP を使用するようお勧めします。
- **モード選択**。この接続プロファイルにおける接続タイプと動作モードです。

  接続タイプは、接続で使用する回線のタイプと、それらが**ダイヤル** (発信元) なのか、もしくは**応答** (受信側) なのかを指定します。以下の接続タイプの中から選択することができます。

  – 交換回線
  – 専用 (占有) 回線
  – L2TP (仮想回線)
  – PPPoE (仮想回線)

  PPPoE は、発信元接続プロファイルにのみサポートされています。
- **動作モード**。使用可能な動作モードは、接続のタイプにより異なります。以下の表を参照してください。

発信元接続プロファイルについては、この表を参照してください。

表 1. 発信元接続プロファイルに使用できる動作モード

接続タイプ	使用できる動作モード
交換回線	– ダイヤル – ダイヤル・オンデマンド (ダイヤルのみ) – ダイヤル・オンデマンド (応答可能な専用ピア) – ダイヤル・オンデマンド (リモート・ピア使用可能)
専用回線	発信元
L2TP	– 発信元 – マルチホップ発信元 – リモート・ダイヤル
PPP over Ethernet	発信元

受信側接続プロファイルについては、以下の表を参照してください。

表 2. 受信側接続プロファイルに使用できる動作モード

接続タイプ	使用できる動作モード
交換回線	応答
専用回線	終端側
L2TP	終端側 (ネットワーク・サーバー)

- **リンク構成**。これは、この接続で使用する回線サービスのタイプを指定します。

  この選択肢は、選択するモード選択のタイプによって異なります。交換回線と専用回線には、以下のいずれかを選択することができます。

  – 単一回線
  – 回線プール
  – 統合 ISDN 回線

  他の接続タイプ (専用、L2TP、PPPoE) すべてについては、回線サービス選択は、単一回線だけです。

グループ・ポリシー・サポート

グループ・ポリシー・サポートは、ネットワーク管理者が、リソースの管理に役立つ、ユーザーを基本としたグループ・ポリシーを定義したり、個々のユーザーが PPP や L2TP セッションを用いてネットワークにログインするときに、アクセス制御ポリシーを割り当てたりすることを可能にしています。この概念では、ユーザーを、特定の 1 つのユーザー・クラスに所属するものとして認識することができます。そして、このクラスには、それぞれ独自の固有なポリシーがあります。それぞれの固有なグループ・ポリシーにより、多重リンク・バンドル内に含めることのできるリンク数などのリソース限界や、IP 転送などの属性や、適用する IP パケット・フィルター規則のセットの指定を定義することができます。グループ・ポリシー・サポートの適用により、ネットワーク管理者は、たとえば、Work_at_Home グループを定義することができます。この Work_at_Home グループは、そのクラスのユーザーにネットワークへの完全アクセスを許可するのに対し、 Vendor_Workers グループのサービスのセットは、これよりも制限されています。

例については、シナリオ: グループ・アクセス・ポリシーおよび IP アドレス・フィルターを使用してリソースへのユーザー・アクセスを管理するを参照してください。

第 5 章 PPP の計画

PPP 接続を作成および管理するには、iSeries サーバーでの PPP サポートおよび接続代替の両方について、そしてビジネスで使用する数多くのネットワーキングおよびセキュリティー計画について精通している必要があります。以下のトピックは、iSeries PPP 接続で使用可能なオプションおよび要件に精通するのに役立ちます。

ソフトウェアおよびハードウェア要件
iSeries ナビゲーター V4R4 以降で PPP 接続をサポートします。他の要件のリストは、このトピックを参照してください。

接続の選択肢
iSeries は、アナログ電話回線またはディジタル電話回線から、専用接続または分割 T1 接続までの、あらゆるメディアでの PPP 接続をサポートします。サポートされる接続オプションについての詳細は、このトピックを参照してください。

接続機器
iSeries サーバーは、 PPP 接続の処理に、モデム、ISDN ターミナル・アダプター、トークンリング・アダプター、イーサネット・アダプター、または CSU/DSU 装置を使用します。サポートされるハードウェアについての情報は、このトピックを参照してください。

IP アドレス処理
PPP 接続には、 IP アドレス割り当ておよび接続中の IP パケット・フィルター操作のオプションがいくつかあります。これらのオプションの説明は、このトピックを参照してください。

システムの認証
iSeries は、妥当性検査リストとパスワードの交換、あるいは RADIUS サーバーを使用して、ダイヤルアップ接続を認証することができます。また、接続先のシステムに認証情報を提供することもします。認証オプションの説明は、このトピックを参照してください。

帯域幅に関する考慮事項
iSeries は、PPP 接続に多重リンク・プロトコルをサポートします。こうすると、単一の接続で複数のアナログ電話回線を使用して、帯域幅を大きくすることができます。このサポートの概要は、このトピックを参照してください。

ソフトウェアおよびハードウェア要件

PPP 環境には、PPP をサポートする 2 つ以上のコンピューターが必要です。それらコンピューターの 1 つである iSeries サーバーは、発信元と受信側のいずれにもなります。リモート・システムがアクセスできるようにするため、iSeries サーバーは以下の要件を満たしている必要があります。

- TCP/IP サポートのある**オペレーション・ナビゲーター** リリース 4 バージョン 4 (V4R4) 以上
- 次の 2 つの接続プロファイルのうちのいずれか。
  - アウトバウンド PPP 接続を処理するための発信元接続プロファイル
  - インバウンド PPP 接続を処理するための受信側接続プロファイル
- iSeries ナビゲーターとともに **iSeries Access for Windows (95/98/NT/Millenium/2000/XP)** がインストールされている PC ワークステーション・コンソール
- インストール済みのアダプター

  次のアダプターの中から 1 つを選択することができます。
  - 2699*: 2 回線通信アダプター
  - 2720*: PCI WAN/平衡型 IOA

- 2721*: PCI 2 回線通信アダプター
- 2745*: PCI 2 回線通信アダプター (IOA 2721 に代わるものです)
- 2742*: 2 回線 IOA (IOA 2745 に代わるものです)
- 2750: PCI ISDN V.90 基本速度インターフェース U IOA (2 線式インターフェース)
- 2751: PCI ISDN V.90 基本速度インターフェース U IOA (4 線式インターフェース)
- 2761: 8 ポート・アナログ・モデム IOA
- 2771: 2 ポート WAN IOA (ポート 1 上には V.90 組み込みモデムが、ポート 2 上には通信インターフェースがある)。 2771 アダプターのポート 2 を使用するには、外部モデムか、適切なケーブルが付いた ISDN ターミナル・アダプターが必要です。
- 2772: 2 ポート V.90 組み込みモデム WAN IOA
- 2838: PPPoE 接続用のイーサネット・アダプター
- 2793*: 2 ポート WAN IOA (ポート 1 上には V.92 組み込みモデムが、ポート 2 上には標準通信インターフェースがある)。 2793 アダプターのポート 2 を使用するには、外部モデムか、適切なケーブルが付いた ISDN ターミナル・アダプターが必要です。これは、IOA モデル 2771 に代わるものです。
- 2805: 4 ポート WAN IOA (V.92 アナログ・モデム内蔵)。これは、モデル 2761 および 2772 に代わるものです。

* これらのアダプターには、外部 V.90 モデム (またはこれ以降) か、 ISDN ターミナル・アダプター、および RS232 または互換ケーブルが必要です。

- 接続タイプと回線に応じて、以下のうちのいずれか:
  - 外部または内部モデムか、 チャネル・サービス・ユニット (CSU)/データ・サービス装置 (DSU)
  - サービス総合ディジタル網 (ISDN) ターミナル・アダプター
- インターネットに接続しようと考えている場合、インターネット・サービス・プロバイダー (ISP) のダイヤルアップ・アカウントを用意する必要があります。必要な電話番号とインターネット接続のための情報を ISP から入手する必要があります。

接続の選択肢

PPP は、シリアル 2 地点間リンクを介してデータグラムを送信することができます。 PPP は、2 地点間通信を標準化することによって、複数の取引先の装置と複数のプロトコルの相互接続を可能にしています。 PPP データ・リンク層は、同期と非同期の両方の 2 地点間通信リンクのデータグラムをカプセル化するのに、 HDLC のようなフレームを使用します。

PPP は広い範囲のリンク・タイプをサポートするのに対し、 SLIP は非同期のリンク・タイプしかサポートしません。 SLIP は一般に、アナログ・リンクに採用されます。ローカル電話会社の提供する、従来の遠隔通信サービスの機能やコストの規模は、広がっています。これらのサービスでは、顧客と中央局の間で、現存する電話会社の音声ネットワーク機構が使用されます。

PPP リンクは、ローカル・ホストとリモート・ホストの間の物理接続を確立します。接続されるリンクには、専用帯域幅があります。また、多様なデータ速度やプロトコルもあります。 PPP リンクでは、以下のような接続の選択肢の中から選択することができます。

- アナログ電話回線
- ディジタル・サービスと DDS
- Switched-56

- ISDN
- T1/E1 と分割 T1
- フレーム・リレー
- PPP 接続の L2TP (トンネリング) サポート
- PPP 接続のための PPPoE (DSL) サポート

アナログ電話回線

モデムを使用して専用回線や交換回線にデータを送信するアナログ接続は、2 地点間スケールの最下部に位置します。専用回線は、指定された 2 つのロケーション間の全時間接続ですが、交換回線は、標準の音声電話回線です。現在の最も高速なモデムは、圧縮なしの速度 56Kbps で作動します。しかし、無条件音声帯域電話回線の信号対ノイズ比率を考慮に入れると、この速度には至らないこともよくあります。

モデムの製造業者が主張する、高いビット / 秒 (bps) 率は、普通、それらのモデムが使用するデータ圧縮 (CCITT V.42bis) アルゴリズムによるものです。 V.42bis には、データ・ボリュームを 4 分の 1 に縮小する潜在能力がありますが、圧縮はデータに依存しているため、50 % に達することさえめったにありません。データが既に圧縮されたり暗号化されたりしている場合、 V.42bis を適用するとデータが大きくなることさえあります。 X2 や 56Flex は、アナログ電話回線の bps 率を 56k に伸ばします。これは、ハイブリッド・テクノロジーであり、 PPP リンクの一端をディジタルに、もう一方の端をアナログにする必要があります。さらに、56Kbps が適用されるのは、データをリンクのディジタル終端からアナログ終端へ移動するときだけです。このテクノロジーは、リンクのディジタル終端とハードウェアを自分のロケーションに備えている ISP に接続する場合に最適です。通常、V.24 アナログ・モデムへは、RS232 シリアル・インターフェースを介し、非同期プロトコルを用いて、最高で 115.2Kbps の速度で接続することができます。

V.90 標準により、K56flex/x2 の互換性の問題は排除されました。 V.90 標準は、モデム業界の x2 と K56flex の関係者による交渉の結果です。 V.90 テクノロジーは、公衆交換電話ネットワークをディジタル・ネットワークと見なすことによって、インターネットからコンピューターまでのデータの速さを 56Kbps にまで高めています。 V.90 テクノロジーは、アナログ・モデムが行うようにデータを変調するのではなく、それをディジタル式にエンコードするという点で、その他の標準とは異なっています。データ転送は非対称的な方式であるため、アップストリーム送信 (ほとんどの場合、必要な帯域幅がより小さい、コンピューターから中央側へのキー・ストロークやマウスによるコマンド) は、引き続き、最大 33.6Kbps の従来の速度で流れます。モデムから送信されるデータは、V.34 標準を鏡映するアナログ送信として送信されます。 V.90 の最高速度は、ダウンストリーム・データ送信でのみ利用されます。

V.92 標準は、アップストリーム速度を 48Kbps にまで上げることにより、V.90 を改善したものとなっています。加えて、ハンドシェーク・プロセスが改善されたために、接続時間を短くすることができ、「保留」機能をサポートするモデムは、電話回線が、着信呼び出しを受け入れる、あるいは、呼び出し待機を使用する間にも、接続したままでいることができます。

ディジタル・サービスと DDS

ディジタル・サービス

ディジタル・サービスにおいて、データは、送信側のコンピューターから、電話会社の中央局、遠距離プロバイダー、中央局をはるばる巡って、最後にディジタル形式の受信側のコンピューターに到着します。ディジタル信号は、アナログ信号よりも大きな帯域幅とより高い信頼性を提供しています。ディジタル信号システムには、ノイズ、可変回線の品質、信号減衰など、アナログ・モデムが処理しなければならない多くの問題がありません。

DDS

ディジタル・データ・サービス (DDS) は、最も基本的なディジタル・サービスです。 DDS リンクは、最大 56Kbps の固定速度で稼働する、専用の、永続的な接続です。また、このサービスは、一般に DS0 と呼ばれます。

DDS へは、アナログ・シナリオのモデムに代わる チャネル・サービス・ユニット / データ・サービス装置 (CSU/DSU) という特別なボックスを使用して接続することができます。 DDS には、物理制限がありますが、この制限は、主に CSU/DSU と電話会社の中央局との間の距離に関係したものです。 DDS は、距離が 30,000 フィートより小さいときに最もよく機能します。電話会社は、シグナル・エクステンダーを使用して、距離をこれより長くすることもできますが、このサービスには高いコストがかかります。 DDS は、同一の中央局からサービスを受ける 2 つのサイトの接続に最も適しています。別々の中央局にまたがる遠距離接続では、すぐに遠距離料金がかさんでしまうので、DDS は実用的ではありません。このような場合は、Switched-56 を使用するほうがよいでしょう。通常、DDS CSU/DSU へは、V.35、RS449、X.21 のうちのいずれかのシリアル・インターフェースを介し、同期プロトコルを使用して、56Kbps までの速度で接続することができます。

Switched-56

常時接続の必要がない場合は、一般に Switch-56 (SW56) と呼ばれる交換回線ディジタル・サービスを使用することによって経費を節約することができます。 SW56 リンクにおいて、DTE が CSU/DSU を経由してディジタル・サービスに接続するという点は、 DDS のセットアップに似ています。しかし、SW56 CSU/DSU には、ユーザーがリモート・ホストの電話番号を入力するためのダイヤリング・パッドが組み込まれています。 SW56 を使用する場合、ユーザーは、国内と国外のどこへでもダイヤルアップ・ディジタル接続を行うことができます。 SW56 呼び出しは、遠距離のディジタル・ネットワーク上で、ちょうど、ディジタル化音声呼び出しと同じように実行されます。 SW56 サービスでは、ローカル電話システムと同じ電話番号が使用され、使用料は、ビジネス音声呼び出しの料金と同じです。 SW56 は、北米のネットワークでのみ利用可能であり、これは、データの搬送しか行わない単一のチャネルに制限されます。 SW56 は、ISDN の使用が不可能な場所のための代替手段です。通常、SW56 CSU/DSU へは、V.35 か RS 449 のシリアル・インターフェースを介し、非同期プロトコルを使用して、56Kbps までの速度で接続することができます。 V.25bis 呼び出し / 応答ユニットにおいて、データと呼び出し制御は、単一のシリアル・インターフェース上を流れます。

ISDN

Switched-56 と同様に、ISDN でも、交換回線終端間ディジタル接続が可能です。しかし、その他のサーバーとは異なり、ISDN は、同一の接続で、音声とデータの両方を搬送することができます。 ISDN サービスには様々なタイプがありますが、中でも、基本インターフェース (BRI) は最も一般的です。 BRI は、顧客のデータを運ぶ 64Kbps の 2 つの B チャネルと、シグナル・データを運ぶ D チャネルで構成されています。 2 つの B チャネルをリンクして 128Kbps の結合速度を出すこともできます。区域によっては、電話会社が B チャネルをそれぞれ 56Kbps、もしくは、結合して 112Kbps に制限することがあります。また、顧客のロケーションは中央局交換から 18,000 フィート以内になければならないという物理制限もあります。この距離は、中継機器を使用して延長できます。 ISDN へは、ターミナル・アダプターと呼ばれる装置を用いて接続することができます。ほとんどのターミナル・アダプターには、テレホン・ジャックへの直接接続を可能にするネットワーク終端装置 (NT1) が組み込まれています。通常、ターミナル・アダプターは、非同期 RS232 リンクを介してユーザーのコンピューターに接続し、 AT コマンド・セットを使用して、従来のアナログ・モデムと同じように、セットアップや制御を行います。各ブランドには、ISDN に固有なパラメーターをセットアップするための独自の AT コマンド拡張機能があります。以前、ISDN ターミナル・アダプターの個々のブランドの間には、相互運用性の問題が数多く存在していました。これらの問題は、そのほとんどが、V.110 と V.120 での速度適応プロトコルの不一致と、 2 つの B チャネル用の結合方式によるものでした。

業界では、2 つの B チャネルをリンクするための PPP 多重リンクを備えた同期 PPP プロトコルへの関心が高まっています。いくつかのターミナル・アダプター製造業者は、ターミナル・アダプターに V.34 (アナログ・モデム) の機能を組み込んでいます。これを使用する場合、顧客は、ISDN サービスの音声 / データ同時機能を利用することにより、単一の ISDN 回線で、ISDN と従来のアナログ呼び出しのいずれをも処理することができます。また、この新しいテクノロジーより、ターミナル・アダプターを、56K(X2/56Flex) クライアントのためのディジタル・サーバー・サイドとして操作させることも可能となっています。

ISDN ターミナル・アダプターへは、RS232 シリアル・インターフェースで、非同期プロトコルを使用して、最大 230.4Kbps の速度で接続したいと思うのが普通かもしれません。しかし、RS232 を介する非同期の場合、iSeries サーバーの最大通信速度は 115.2Kbps です。そのため、多重リンク機能付きのターミナル・アダプターは未圧縮時に 14/16k バイトの通信が可能であるにもかかわらず、残念ながら最大バイト転送速度が 11.5k バイト / 秒に制限されてしまいます。ターミナル・アダプターの中には、RS232 を介する同期を 128Kbps でサポートするものがありますが、 RS232 を介する同期の場合における iSeries サーバーの最大通信速度は 64Kbps です。

iSeries サーバーには、V.35 において、230.4Kbps までの速度で非同期に動作する能力がありますが、ターミナル・アダプターの製造業者は、普通、そのような構成を提供していません。この問題は、RS232 を V.35 インターフェースに変換するインターフェース・コンバーターによって適切に解決されるかもしれませんが、 iSeries サーバーに関してこのアプローチはまだ評価が定まっていません。もう 1 つの解決策として考えられるのは、 V.35 インターフェース同期プロトコルを備えたターミナル・アダプターを 128Kbps の速度で使用することです。このクラスのターミナル・アダプターは存在するものの、同期多重リンク PPP を提供しているものはあまりないようです。

T1/E1 と分割 T1

T1/E1

T1 接続は、4 線式銅回線による 64 Kbps の時分割多重方式 (TDM) チャネルを 24 個束ねたものです。これによって、合計 1.544Mbps の帯域幅が実現されます。ヨーロッパと世界の他の地域では、E1 回線が 32 の 64Kbps チャネルを束ねており、その合計は 2.048Mbps です。 TDM では、事前割り当ての時間スロットを使用することにより、複数のユーザーで、ディジタル伝送メッセージを共用することができます。ディジタル PBX の多くは、PBX と電話会社の間に 24 組のワイヤーを敷設する代わりに、 1 つの回線で複数の呼線をインポートする T1 サービスを利用しています。音声とデータの間で T1 を共用できるという点を知っておくのは重要です。たとえば、電話サービスが T1 リンクの 24 のチャネルのサブセットの 1 つから提供されるようにし、他のチャネルはインターネット接続に残しておくことなどもできます。 T1 幹線が複数のサービス間で共用されている場合、 24 DS0 チャネルを管理するには、T1 多重化装置が必要です。データ専用の単一の接続では、回線をチャネル化しない (信号については TDM を実行しない) で稼働することができます。そのため、より単純な CSU/DSU 装置を使用することも可能です。通常、T1/E1 の CSU/DSU や多重化装置へは、V.35 か RS 449 シリアル・インターフェースを介し、同期プロトコルを使用して、64Kbps 〜 1.544Mbps か 2.048Mbps の倍数の速度で接続することができます。 CSU/DSU や多重化装置は、ネットワーク内のクロックを提供しています。

分割 T1

分割 T1 (FT1) では、顧客は、T1 回線の一部を 64Kbps 単位で借用することができます。どんなときであれ、顧客が使用している実際の帯域幅に対して、占有 T1 のコストがひどく高く思える場合は、FT1 が有用です。 FT1 では、自分が必要とするものに対してのみ支払いをすることになります。さらに、FT1 では、完全な T1 回線を使用している場合には利用できない機構を利用することができます。それは、電話会社の中央局にある多重方式 DS0 チャネルです。 FT1 回線のリモート・エンドは、電話会社が維持する

ディジタル・アクセス・クロス接続交換にあります。同一のディジタル交換を共用しているシステムは、DS0 チャネルを交換することができます。この方式は、自分のロケーションから電話会社のディジタル交換までの単一の T1 幹線を使用する ISP には一般的なものです。この場合は、FT1 サービスでは、複数のクライアントがサービスを受けることができます。通常、T1/E1 の CSU/DSU や多重化装置へは、 V.35 か RS 449 のシリアル・インターフェースを介し、同期プロトコルを使用して、64Kbps の倍数の速度で接続することができます。 FT1 では、ユーザーには、24 のチャネルのサブセットが事前に割り当てられています。 T1 多重化装置の構成では、ユーザーのサービス用に割り当てられている時間スロットだけを埋める必要があります。

フレーム・リレー

フレーム・リレーとは、ネットワークで、アドレス・フィールド (データ・リンク接続 ID) を基にフレームの経路指定を行ったり、経路や仮想接続を管理したりするためのプロトコルです。

米国のフレーム・リレー・ネットワークは、 T-1 (1.544 Mbps) と T-3 (45 Mbps) という速度のデータ転送速度をサポートしています。フレーム・リレーは、サービス提供者によって所有されている、現存の T-1 回線と T-3 回線を使用するための手段と考えることができます。電話会社の多くは、56 Kbps ～ T-1 の速度の接続を必要とする顧客のために、フレーム・リレーを提供しています。 (ヨーロッパにおけるフレーム・リレーの速度は 64 Kbps ～ 2 Mbps です。米国では、フレーム・リレーは比較的安価であることから、非常に普及しています) しかし、一部の地域では、ATM などの、より高速のテクノロジーがこれに取って代わっています。

PPP 接続の L2TP (トンネリング) サポート

レイヤー 2 トンネリング・プロトコル (L2TP) は、PPP を拡張するトンネル伝送プロトコルであり、要求元の L2TP クライアント (L2TP Access Concentrator または LAC) とターゲットの L2TP サーバー端点 (L2TP Network Server または LNS) とをつなぐリンク層トンネルをサポートします。 L2TP トンネルを使用すると、ダイヤルアップ・プロトコルの終端のロケーションと、ネットワークへのアクセスの可能なロケーションを分離できます。これが、L2TP が仮想 PPP と呼ばれるゆえんです。 L2TP は、Request For Comment 標準 RFC2661 として文書化されています。 RFC についての詳細は、http://www.rfc-editor.org にあります。 L2TP トンネルは、PPP セッション全体にわたることができますが、 2 セグメント・セッションの 1 セグメントにおいてのみ使用することもできます。これは、以下のような 4 つの異なるトンネル伝送モデルに代表されます。

- 任意トンネル
- 必須トンネル - 着信呼び出し
- 必須トンネル - リモート呼び出し
- L2TP マルチホップ接続

任意トンネル

任意トンネル・モデルでは、トンネルは、ユーザーが、通常は L2TP の使用可能なクライアントを使用して作成します。その結果として、ユーザーは L2TP パケットをインターネット・サービス・プロバイダー (ISP) に送信することになり、それらの L2TP パケットは、そこから LNS に転送されます。任意トンネル伝送では、ISP による L2TP のサポートは不要であり、 L2TP トンネルの起動側は、リモート・クライアントと同じシステム上に常駐します。このモデルでは、トンネルは、L2TP クライアントから LNS までの PPP 接続全体にわたります。

必須トンネル・モデル - 着信呼び出し

必須トンネル・モデルの着信呼び出しでは、ユーザーがアクションを起こさなくてもトンネルが作成され、ユーザーは何ら選択できるものはありません。これを行う場合、ユーザーは PPP パケットを ISP (LAC)

に送信することになり、 ISP (LAC) はこれらを L2TP にカプセル化して LNS にトンネル伝送します。必須トンネル伝送の場合は、ISP が L2TP を使用できなければなりません。このモデルでは、トンネルは、ISP と LNS の間の PPP セッションのセグメントにしか及びません。

必須トンネル・モデル - リモート・ダイヤル

必須トンネル・モデル - リモート・ダイヤルでは、ホーム・ゲートウェイ (LNS) が ISP (LAC) へのトンネルを開始し、 ISP に、PPP 応答クライアントへのローカル呼び出しを行うよう指示をします。このモデルは、リモート PPP 応答クライアントが ISP との間に永続的な確立済みの電話番号を所有している場合に使用することを意図しています。インターネットにおける所在が確立されている会社が、ダイヤルアップ・リンクを必要とするリモート・オフィスへの接続を確立しようとする場合は、このモデルの使用が期待されます。このモデルでは、トンネルは、LNS と ISP の間の PPP セッションのセグメントにしか及びません。

L2TP マルチホップ接続

L2TP マルチホップ接続は、クライアント LAC や LNS の代わりに L2TP トラフィックの宛先変更を行うための 1 つの手段となります。マルチホップ接続は、L2TP のマルチホップ・ゲートウェイ (L2TP の終端側プロファイルと起動側プロファイルをリンクするシステム) を使用して確立します。マルチホップ接続を確立するため、L2TP マルチホップ・ゲートウェイは、 LAC のセットへ向かう LNS として、また、提供されている LNS へ向かう LAC としての両方の役割を担います。クライアント LAC から L2TP マルチホップ・ゲートウェイへのトンネルが確立され、 L2TP マルチホップ・ゲートウェイとターゲット LNS との間にもう 1 つのトンネルが確立されます。クライアント LAC からの L2TP トラフィックは、 L2TP マルチホップ・ゲートウェイによってターゲット LNS に宛先変更され、ターゲット LNS からのトラフィックは、クライアント LAC に宛先変更されます。

PPP 接続のための PPPoE (DSL) サポート

DSL は、カスタマーの居場所と ISP プロバイダーとを結ぶ既存の銅線電話ケーブルを使って、より広い帯域幅を取得するのに使用されるテクノロジーのクラスを指します。また、単一の銅線電話線で、音声および高速データ・サービスを同時に行うことができます。モデム速度は、各種の圧縮その他の技法を使用することで、次第に速くなっているものの、現在の最高速度 (56 kbit/s) で、このテクノロジーの理論上の限界が近づいています。 DSL テクノロジーを使用すると、対より線を介して、中央オフィスから住宅、学校、または業務地への非常に高速の通信を提供できます。地域によっては、秒速 2 メガバイトもの速度が可能です。これは、現在の最速モデムの 30 倍以上の速さです。 PPPoE とは、Point to Point Protocol over Ethernet の略です。 PPP は、通常、ダイヤルアップ・モデム接続のようなシリアル通信で使用されます。多くの DSL インターネット・サービス・プロバイダーは、現在、PPP over Ethernet を使用しています。これは、ログインおよびセキュリティー機能が優れているためです。 DSL モデムとは何でしょうか? DSL「モデム」は、銅線電話回線のいずれかの終端に配置されて、コンピューター (または LAN) が DSL 接続でインターネットに接続できるようにする装置です。ダイヤルアップ接続とは異なり、通常は、専用電話回線を必要としません (POTS スプリッター・ボックスで、回線を同時に共用するようにします)。 DSL は、次世代のモデム技術と見なされています。 DSL モデムは、従来のアナログ・モデムに類似しているものの、スループットはかなり高くなります。

接続機器

PPP 環境では、次のような 3 種類の通信機器を使用することができます。

- モデム
- CSU/DSU
- ISDN ターミナル・アダプター

- タイプ 2838 イーサネット・アダプター (PPPoE 接続用)。

モデム

PPP 環境では、外部モデムと内部モデムの両方が使用できます。モデムで使用されるコマンド・セットは、たいていモデムの資料で説明されています。これらのコマンドは、モデムのリセットや初期設定を行ったり、リモート・システムの電話番号をダイヤルするようモデムに指示したりするのに用いられます。モデム・モデルは、それぞれ別個の初期化コマンド・ストリングを持つので、これらは、PPP 接続プロファイルで使用する前に定義する必要があります。内部モデムのモデム・ストリングの使用法については既に定義済みです。

iSeries サーバーには、多くの事前定義モデム・モデルがありますが、オペレーション・ナビゲーターを通して新しいモデルを定義することも可能です。既存の定義は、新しいタイプを定義する際の基本とすることができます。モデムが使用しているコマンドが分からない場合や、モデムの資料が手に入らない場合は、Generic Hayes モデム定義を開始してください。出荷時に事前定義されている定義を変更することはできませんが、既存の初期化コマンドやダイヤル・ストリングに、追加のコマンドを加えることは可能です。

PPP 接続を確立するには、 iSeries サーバーに付属しているエレクトロニック支援 (ECS) モデムを使用することができます。旧システムにおいて、ECS モデムは IBM 7852-400 外部モデムでした。新しいシステムでは、2771 か 2772 の内部モデムを ECS モデムとして使用することができます。

CSU/DSU

チャネル・サービス・ユニット (CSU) は、端末をディジタル回線に接続する装置です。データ・サービス装置 (DSU) は、通信回線に対して、保護機能や診断機能を実行する装置です。通常この 2 つの装置は、単一のユニット、CSU/DSU としてパッケージされています。

CSU/DSU は、非常に高性能で高価なモデムと考えることができます。この装置は、T-1 接続や T-3 接続の両方の終端に必要で、両方の終端の装置は、同じ製造業者のものにする必要があります。

ISDN ターミナル・アダプター

ISDN では、他のマルチメディア・アプリケーションに加え、音声、データ、およびビデオを任意に組み合わせたものを使った通信も可能にするディジタル接続が提供されます。

ターミナル・アダプターがご使用の iSeries サーバーでの使用に適しているかどうか確認してください。

- 『推奨される ISDN ターミナル・アダプター』には、使用に最適なターミナル・アダプターのリストがあります。
- 『ISDN ターミナル・アダプターに関する制約事項』には、 iSeries サーバーで検査済みの、種々の ISDN ターミナル・アダプターに関する情報と、それらについての簡潔な評価があります。

ターミナル・アダプターは、以下のステップに従って構成してください。

1. iSeries ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」** と展開します。
2. **「モデム」**を右ボタンでクリックし、**「新規モデム」**を選択します。
3. 「新規モデムのプロパティー」ダイアログ・ボックスで、「一般」タブのすべてのフィールド・ボックスに正しい値を入力します。必ず、ISDN ターミナル・アダプターを通信装置として指定してください。
4. **「ISDN パラメーター」**タブを選択します。

5. ターミナル・アダプターが必要とするプロパティーに合わせて、**「ISDN パラメーター」**タブの ISDN プロパティーを追加または変更します。

オペレーション・ナビゲーターを使用するサンプル手順については、 ISDN ターミナル・アダプターの構成の例を参照してしてください。

推奨される ISDN ターミナル・アダプター

お勧めする外部 ISDN ターミナル・アダプター、つまり ISDN モデムは、 **3Com/U.S. Robotics Courier I ISDN V.Everything** です。このモデムは、V.34 アナログ・モデム接続、V.90 (X2)、V.92、また iSeries サーバー上での発信および応答モードのどちらでも ISDN を介した多重リンク PPP をサポートします。さらに、ISDN PPP 接続経由の Challenge Handshake Authentication Protocol (CHAP) 認証を自動的にサポートします。また、ISDN ターミナル・アダプターとして、Zyxel Omni.net Plus TA、Zyxel Omni.net LCD plus TA、および ADtran ISU 2x64 Dual Port も使用できます。

- **iSeries サーバーから発信する接続**。レシーバーから発信された CHAP 呼び出しは、Courier I ターミナル・アダプターから応答される一方で、 iSeries サーバーに対してパスワード検証プロトコル (PAP) 認証が折衝されます。 PAP 応答は、ISDN 接続上には表示されません。
- **iSeries サーバーが応答する接続**。 iSeries サーバーの応答構成が、CHAP 呼び出しの認証を開くようになっている場合は、Courier I では、呼び出し側による CHAP 認証が義務づけられます。 iSeries サーバーが PAP の認証を開く場合、Courier I は PAP の認証を行います。

1999 より前の Courier I モデムを使用している場合、 ISDN 接続のパフォーマンスを可能なかぎり最大化するには、 Courier I モデムを V.35 ケーブルで iSeries サーバーに接続します。 RS-232 から V.35 へのモデム・ケーブルが Courier I モデムに付属していますが、旧型のこのケーブルには、オス・メスの誤った V.35 コネクターが付いています。取り替えを希望する場合は、3Com/US Robotics のカスタマー・サポートにご連絡ください。

注: 3Com/US Robotics によると、このターミナル・アダプターの V.35 バージョンは、既になくなっていますが、サード・パーティーの供給元からであれば、まだ多少提供されている可能性があります。 RS-232 接続では 115.2 Kb に制限されているために、iSeries 上でのパフォーマンスはいくらか低くなりますが、やはりまだ RS-232 バージョンを使用することをお勧めします。

V.35 と RS-232 を接続するアダプターは、Black Box Corporation からも入手できます。部品番号は FA-058 です。

iSeries サーバー上では必ず V.35 の回線速度を 230.4 Kbps に設定してください。

ISDN ターミナル・アダプターに関する制約事項

以下のターミナル・アダプターは、評価済みです。 iSeries サーバーに対する ISDN リモート接続の発信元としてのみお勧めします。

3Com Impact IQ ISDN:

このターミナル・アダプターは、次のような理由で iSeries サーバーにはお勧めしません。

- このターミナル・アダプターは V.34 アナログ・モデム接続をサポートしていません。ただし、外部 RJ-11 接続を行えばサポートすることがあります。
- このアダプターは現在、V.90 接続をサポートしません。
- 115200 bps より早い速度では iSeries サーバーに接続できないかもしれません。
- Challenge Handshake Authentication Protocol (CHAP) を自動的にサポートしません。ただし、S84=0 と設定すれば、iSeries サーバーの CHAP 認証を実行できます。

- iSeries サーバーは、データ・セット・レディー・シグナルのモニター時にいつ接続が終了したかを判別できません。この結果、システム・セキュリティーが損なわれる可能性があります。

Motorola BitSurfr Pro ISDN:

このターミナル・アダプターは、次のような理由で iSeries サーバーにはお勧めしません。

- このターミナル・アダプターは V.34 アナログ・モデム接続をサポートしていません。ただし、外部 RJ-11 接続を行えばサポートすることがあります。
- このアダプターは現在、V.90 接続をサポートしません。
- 115200 bps より早い速度では iSeries サーバーに接続できないかもしれません。
- CHAP 認証を自動的にサポートしません。ただし、@M2=C と設定すれば、iSeries サーバーの CHAP 認証を実行できます。
- 単一リンクおよび多重リンクの PPP 呼び出しのどちらにも自動的に応答することを許可しません。発信元のリモート・ターミナル・アダプターを、応答側ターミナル・アダプターと同じプロトコル (単一リンクまたは多重リンク) に設定する必要があります。
- iSeries サーバーのハードウェア・フロー制御メカニズムは、このターミナル・アダプターではうまく作動しないため、多重リンク PPP 接続を介して iSeries サーバーからデータを送信すると、パフォーマンスが低下することになります。

IP アドレス処理

PPP 接続では、接続プロファイルのタイプに従って、 IP アドレスを管理するための異なるいくつかのセットのオプションを使用できるようになっています。それによって PPP 接続のための IP アドレス管理は、既存のネットワーク体系とのシームレスな動作が可能です。ご使用のネットワークに IP アドレス・スキームを定義することについての詳細は、以下のトピックを参照してください。

- DHCP

  DHCP は、ご使用のネットワークの IP アドレス割り当てを集中管理できます。ここで、ネットワークに DHCP サービスをセットアップおよび管理する方法を調べてください。
- DNS

  DNS を使用すると、ホスト名および関連する IP アドレスを管理できます。ここで、ネットワークに DNS サービスをセットアップおよび管理する方法を調べてください。
- BOOTP

  BOOTP は、クライアント・ワークステーションをご使用の iSeries サーバーに関連付け、これらに IP アドレスを割り当てるのに使用されます。ここで、ネットワークに BOOTP サービスをセットアップおよび管理する方法を調べてください。
- IP パケット・フィルター

  IP フィルター規則ファイルを作成すると、特定の IP アドレスに対して制限されたユーザーおよびグループがアクセスできるようにします。ここで、IP フィルター・サポート、およびご使用のネットワークにこのオプションを実装する方法について調べてください。

PPP 接続プロファイルを構成する前に、ご使用の IP アドレス管理の戦略に精通していなければなりません。この戦略は、認証戦略、セキュリティーの考慮事項、および TCP/IP 設定を含め、構成プロセスでの数多くの決定に影響を与えます。

発信元接続プロファイル:

通常、発信元プロファイルに定義されるローカルとリモートの IP アドレスは、**「リモート・システムによる割り当て」**と定義されます。これによって、接続で使用される IP アドレスをリモート・システムの管理者が制御できるようになります。多くの ISP が追加料金で固定 IP アドレスを提供していますが、インターネット・サービス・プロバイダー (ISP) へのほとんどすべての接続はこの方法で定義されます。

ローカルまたはリモートの IP アドレスの固定 IP アドレスを定義する場合は、リモート・システムが、定義するアドレスを受け入れるように定義されていなければなりません。ローカル・アドレスを固定 IP アドレスとして定義し、リモート・アドレスがリモート・システムによって割り当てられるよう定義するのが、1 つの典型的な設定です。接続するシステムを同様の方法で定義して、接続の際、その 2 つのシステムが、リモート・システムのアドレスを知る手段として、互いのアドレスを交換するようにすることができます。これは、1 つのオフィスが一時的な接続のために他のオフィスを呼び出す場合には便利かもしれません。

もう 1 つの考慮事項は、IP アドレスのマスカレードを使用可能にするかどうかです。たとえば、iSeries サーバーが ISP を介してインターネットに接続している場合は、 iSeries サーバーの背後で接続されているネットワークもインターネットにアクセスすることができます。基本的に iSeries サーバーは、ISP が割り当てるローカル IP アドレスの背後のネットワーク上にあるシステムを IP アドレスを「隠し」て、すべての IP アドレスが iSeries サーバーからのものであるように見せかけます。この他、LAN 上のシステムと iSeries サーバーの両方に対する、ルーティングに関連した付加的な考慮事項もあります。 LAN 上のシステムのインターネット・トラフィックは iSeries サーバーに送信されるようにする必要があり、 iSeries サーバーでは、「リモート・システムをデフォルト経路として追加」ボックスを使用可能にする必要があります。

受信側接続プロファイル:

受信側接続プロファイルには、 IP アドレスの考慮事項やオプションが発信元接続プロファイルよりも多く存在します。 IP アドレスの構成方法は、ご使用のネットワークでの IP アドレス管理プラン、この接続に固有のパフォーマンスおよび機能の要件、およびセキュリティー・プランにより異なります。

ローカル IP アドレス

単一のレシーバー・プロファイルでは、固有 IP アドレスを定義するか、 iSeries サーバー上の既存のローカル IP アドレスを使用することができます。これは、PPP 接続の iSeries サーバー側の終端を示すアドレスとなります。同時に複数の接続をサポートするよう定義されているレシーバー・プロファイルには、既存のローカル IP アドレスを使用しなければなりません。事前に存在している有効なローカル IP アドレスがない場合は、この目的で仮想 IP アドレスを作成することができます。

リモート IP アドレス

リモート IP アドレスを PPP クライアントに割り当てるのに使用できるオプションは数多くあります。以下のオプションは、受信側接続プロファイルの**「TCP/IP」**ページで指定できます。

注: リモート・システムが、LAN の一部と見なされるようにしたい場合には、 IP アドレス・ルーティングを構成する際に、LAN 接続システム用のアドレス範囲内で IP アドレスを指定し、 IP 転送がこの接続プロファイルと iSeries システムの両方で使用可能にされていることを確認してください。

表 3. レシーバー・プロファイル接続の IP アドレス割り当てオプション

オプション	説明
固定 IP アドレス	リモート・ユーザーがダイヤルインするときに与えられる単一の IP アドレスを定義します。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) で、単一接続のレシーバー・プロファイルにのみ有効です。

表 3. レシーバー・プロファイル接続の IP アドレス割り当てオプション (続き)

オプション	説明
アドレス・プール	開始 IP アドレスと、追加で定義できる IP アドレスの数量範囲を指定します。接続するユーザーは、この定義の範囲内で、固有アドレスを与えられます。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) で、多重接続のレシーバー・プロファイルにのみ有効です。
RADIUS	リモート IP アドレスとそのサブネット・マスクは、Radius サーバーが決定します。これは、以下のものが定義されている場合にのみ有効です。 • リモート・アクセス・サーバーのサービス構成で、認証と IP アドレッシングのための Radius サポートが使用可能になっている。 • 認証が、受信側接続プロファイルで使用可能となり、 Radius によってリモートで認証されるように定義されている。
DHCP	リモート IP アドレスは、DHCP サーバーにより直接、あるいは DHCP リレーにより間接的に決定できます。これは、リモート・アクセス・サーバーのサービス構成で、 DHCP サポートが使用可能になっている場合にのみ有効です。これは、ホスト専用の IP アドレス (サブネット・マスクは 255.255.255.255) です。
リモート・システムのユーザー ID を基にする	リモート IP アドレスは、リモート・システムが認証されたときにこれに定義されたユーザー ID によって決まります。これによって管理者は、ダイヤルインするユーザーに別々の IP アドレス (とそのサブネット・マスク) を割り当てることができます。これはまた、これらそれぞれのユーザー ID に対して付加的な経路を定義し、既知のリモート・ユーザーに合わせて環境を調整することを可能にしています。この機能が適切に働くようにするには、認証を使用可能にする必要があります。
リモート・システムのユーザー ID に基づいて追加の IP アドレスを定義	リモート・システムのユーザー ID を基にしてアドレスを定義する場合は、このオプションを使用することができます。 IP アドレスの割り当て方式として**「ユーザー ID を基にする」**が定義されている場合は、このオプションが自動的に選択され (て使用され) ます。このオプションは、固定 IP アドレスとアドレス・プールのアドレス割り当て方式でも使用できます。リモート・ユーザーが iSeries サーバーに接続すると、そのユーザーに対して固有に定義されたリモート IP アドレスがあるかどうかを判別するための検索が実行されます。定義されている場合、接続には、そのアドレスとマスクと可能な経路の設定が使用されます。ユーザーが定義されていない場合、アドレスはデフォルトとなり、定義されている固定 IP アドレスか、その次に有効なアドレス・プール IP アドレスとなります。
リモート・システムが独自の IP アドレスを割り当てることを許可	このオプションでは、リモート・ユーザーが折衝した場合に、独自の IP アドレスを定義することができます。リモート・ユーザーが独自のアドレスを使用するための折衝を行わないなら、リモート IP アドレスは、定義されているリモート IP アドレス割り当て方式により決定されます。このオプションは初期状態では使用不可になっており、これを使用可能にするにあたっては、注意深い考慮が必要です。
IP アドレス経路指定	ダイヤルアップ・クライアントが、 iSeries が属する LAN 上で任意の IP アドレスにアクセスする必要がある場合、このクライアントおよび iSeries には、IP アドレス・ルーティングが適切に構成されていなければなりません。

IP パケット・フィルター

IP パケット・フィルターは、個々のユーザーがネットワークにログイン時に利用できるサービスを制限する機能です。パケット・フィルター操作では、IP アドレスとポートのいずれかまたはその両方を基にして、アクセスを「許可」または「否認」することができます。それぞれが独自の固有な PPP フィルター ID を持つパケット・フィルター規則のセットが複数定義されることによって、個々のポリシーが課されます。パケット・フィルター規則は、特定の受信側接続プロファイルに対して割り当てることもできますし、

フィルター規則を適用するグループ・ポリシーを使用することによって、そのカテゴリーのユーザーに対して割り当てることもできます。パケット・フィルター規則自体は、PPP ではなく、 iSeries ナビゲーターIP パケット規則の下で定義されています。詳細については、Information Center トピックの『IP パケット規則』を参照してください。

L2TP 接続の場合、 IP SEc フィルターを伴う VPN を使用してネットワーク・トラフィックを保護しなければなりません。詳細については、Information Center トピックの『VPN』を参照してください。

システムの認証

iSeries サーバーでの PPP 接続は、リモート・クライアントの iSeries へのダイヤルインと、 iSeries がダイヤルしている ISP またはその他のサーバーへの接続の両方を認証するためのオプションをいくつかサポートします。 iSeries は、認証情報の保守のためのいくつかの方式をサポートします。これは、認可されたユーザーおよび関連するパスワードのリストを含む iSeries での単純な妥当性検査リストから、ネットワーク・ユーザーの詳細に渡る認証情報を保守する RADIUS サーバーのサポートまでの広範囲に及びます。さらに、iSeries は、ユーザー ID およびパスワード情報の暗号化のためのオプションもいくつかサポートします。これには、単純なパスワード交換から、CHAP-MD5 との柔軟サポートが含まれます。ダイヤルアウト時に iSeries を妥当性検査するのに使用されるユーザー ID およびパスワードを含む、システム認証のためのプリファレンスは、 iSeries ナビゲーターの接続プロファイルの**「認証」**タブで指定できます。

妥当性検査および認証情報の保守についての詳細は、以下を参照してください。

- Remote Authentication Dial In User Service (RADIUS)
- 妥当性検査リスト

サポートされているパスワード認証プロトコルについての詳細は、以下を参照してください。

- Challenge Handshake Authentication Protocol (CHAP-MD5)
- Password Authentication Protocol (PAP)
- Extensible Authentication Protocol (EAP)

CHAP-MD5

Challenge Handshake Authentication Protocol (CHAP-MD5) は、認証システムおよび遠隔装置だけが認識する値を計算するためのアルゴリズム (MD-5) を使用します。 CHAP を使うと、ユーザー ID とパスワードが常に暗号化されるので、 PAP よりも安全なプロトコルと言えます。このプロトコルは、プレーバックおよび試行とエラーを繰り返すアクセス試行に効果的です。 CHAP 認証は、接続中に複数回発生することがあります。

認証システムは、ネットワークに接続しようとする遠隔装置に誰何 (すいか) を送信します。遠隔装置は、両方の装置が使用する共通アルゴリズム (MD-5) によって計算された値で応答します。認証システムは、その値を独自の計算結果と照合します。認証は、値が一致した場合に与えられます。一致しない場合、接続は終了します。

EAP

Extensible Authentication Protocol (EAP) は、第三者認証モジュールが PPP 実装と対話することを可能にしています。 EAP は、トークン (スマート) カード、Kerberos、公開鍵、 S/Key といった認証方式のための標準サポート・メカニズムを提供することによって PPP を拡張しています。 EAP は、第三者セキ

ュリティー装置による RAS 認証の拡大に対する高まる需要に答えるものです。 EAP は、ディクショナリー・アタックやパスワード解読を行うハッカーから、セキュア VPN を保護します。 EAP は PAP と CHAP をさらに改良しています。

EAP では、認証情報は、情報の中に組み込まれているのではなく、むしろ情報に付随していると言えます。そのため、リモート・サーバーは、情報の受け渡しを行う前に、必要な認証について折衝することができます。

iSeries サーバーは現在 CHAP-MD5 に相当するバージョンの EAP しかサポートしていません。しかし、リモート認証は、上で説明した付加的な認証方式のいくつかをサポートしている RADIUS サーバーを使用して行うことができます。

PAP

Password Authentication Protocol (PAP) は両方向ハンドシェークを使用して、対等システムに ID を確立する簡単な方法を提供します。ハンドシェークは、リンクの確立時に行われます。リンクが確立されたら、遠隔装置はユーザー ID とパスワードの組み合わせを認証システムに送信します。この組み合わせが正しいかどうかに応じて、認証システムは接続を継続したり終了したりします。

PAP 認証では、ユーザー名とパスワードを、クリア・テキスト形式でリモート・システムに送信する必要があります。 PAP の場合、ユーザー ID とパスワードは暗号化されないので、トレースが可能となり、ハッカー・アタックを受けやすくなります。この理由から、可能な場合はいつでも CHAP を使用してください。

RADIUS 概説

Remote Authentication Dial In User Service (RADIUS) は、分散ダイヤルアップ・ネットワーク内のリモート・アクセス・ユーザーのために、認証、アカウンティング、および IP を集中管理するサービスを提供するインターネット標準プロトコルです。

RADIUS クライアント・サーバー・モデルには、 RADIUS サーバーのクライアントとしての Network Access Server (NAS) 操作があります。 NAS としての役割を担う iSeries サーバーは、 RFC 2865 で定義されている RADIUS 標準プロトコルを使用し、指定された RADIUS サーバーに、ユーザーと接続の情報を送信します。

RADIUS サーバーは、受信したユーザーの接続要求に対して作動して、ユーザーを認証し、必要なすべての構成情報を NAS に返して、 NAS (iSeries サーバー) が認可済みのダイヤルイン・ユーザーに認可済みサービスを送達できるようにします。

RADIUS サーバーに届かない場合は、iSeries サーバーが代わりのサーバーに認証要求を発送します。これにより、グローバル企業は、どんなアクセス・ポイントが使用されていようと、コーポレート・ワイド・アクセスのための、固有なログイン・ユーザー ID を用いるダイヤルイン・サービスをユーザーに提供することができます。

RADIUS サーバーが認証要求を受信すると、 RADIUS サーバーが、ユーザー名とパスワード情報にアクセスするためのデータ・パケットを暗号化します。この情報は、サポートされている適切なセキュリティー・システムに渡されます。これには、UNIX パスワード・ファイル、Kerberos、市販のセキュリティー・システム、あるいは、カスタム開発のセキュリティー・システムなどがあります。 RADIUS サーバーは、IP アドレスなど、認証されたユーザーが利用を許可されているサービスを、iSeries サーバーに送り返します。 RADIUS アカウンティング要求は、同様の方法で処理されます。リモート・ユーザーのアカウンティング情報は、指定された RADIUS アカウンティング・サーバーに送信することができます。 RADIUS ア

カウンティング標準プロトコルは、RFC 2866 で定義されています。 RADIUS アカウンティング・サーバーは、受信したアカウンティング要求に対して作動し、 RADIUS アカウンティング要求の情報を記録します。 RADIUS 構成の例については、 RADIUS サーバーによるダイヤルアップ・ユーザーの認証のシナリオを参照してください。

妥当性検査リスト

妥当性検査リストは、リモート・ユーザーに関連したユーザー ID とパスワードの情報を保管するために使用されます。既存の妥当性検査リストを使用するか、受信側接続プロファイルの「認証」ページで独自に作成することができます。妥当性検査リスト項目には、ユーザー ID やパスワードに関連した認証プロトコル・タイプを示す必要があります。これは、**「暗号化されたパスワードが必要 (EAP または CHAP-MD5)」**か**「暗号化されていないパスワードが必要 (PAP)」**になります。

詳細については、オンライン・ヘルプを参照してください。

帯域幅に関する考慮事項 - 多重リンク

あるタスクを実行する際には、帯域幅を追加する必要が生じることがありますが、帯域幅の追加は、すべての場合に必要なものではありません。この場合、特殊なハードウェアや高価な通信回線を購入することは、適当ではないかもしれません。 PPP 多重リンク・プロトコル (MP) は、複数の PPP リンクをグループ化して 1 つの仮想リンクを形成できます。このように複数のリンクをまとめると、標準のモデムと電話回線を使用する場合の、2 つのシステム間の有効帯域幅の合計は増加します。 MP バンドルには最大 6 つのリンクを組み込むことができます。多重リンク接続を確立するには、 PPP リンクの両方の終端で多重リンク・プロトコルがサポートされている必要があります。多重リンク・プロトコルは、Request For Comment (RFC) 標準 RFC1990 として文書化されています。 RFC についての詳細は、http://www.rfc-editor.org にあります。

オンデマンド帯域幅:

物理リンクを動的に追加したり除去したりする機能を使用することによって、帯域幅が必要なときにだけ供給されるように、システムを構成することができます。このアプローチは、一般に「オンデマンド帯域幅」と呼ばれ、実際にこれを使用しているときは、追加の帯域幅の料金を支払うだけで済みます。「オンデマンド帯域幅」の利益を得るには、 MP バンドル内の現在使用可能な合計帯域幅の稼働率をモニターする能力の備わった対等回線が少なくとも 1 つ必要です。帯域幅の稼働率が、構成で定義された値を超えると、リンクがバンドルに加えられたり、バンドルからリンクが除去されたりします。対等回線は、Bandwidth Allocation Protocol を使用することにより、 MP バンドル内のリンクの追加と除去について折衝することができます。 PPP Bandwidth Allocation Protocol (BAP) と Bandwidth Allocation Control Protocol (BACP) は両方とも RFC2125 に記述されています。

第 6 章 PPP の構成

PPP を使用してセットアップして 2 地点間接続をセットアップするにあたっては、まず初めに PPP 環境の構成を行う必要があります。 PPP 環境のための構成情報は、以下のセクションで提供されています。

- 接続プロファイルの作成
- モデムの構成
- リモート PC の構成
- AT&T Global Network を介するインターネット・アクセスの構成
- 接続ウィザード
- グループ・アクセス・ポリシーの構成
- PPP 接続への IP パケット・フィルター規則の適用
- PPP 受信側接続プロファイルにおける RADIUS および DHCP サービスの使用可能化

接続プロファイルの作成

システム間に PPP 接続を構成するための最初のステップは、 iSeries サーバー上に接続プロファイルを作成することです。接続プロファイルは、以下の詳細事項を論理的に表したものです。

- 回線およびプロファイル・タイプ
- 多重リンク設定
- リモート電話番号およびダイヤル・オプション
- 認証
- TCP/IP 設定: IP アドレスおよびルーティング
- 実行管理機能および接続カスタマイズ
- ドメイン・ネーム・サーバー

「ネットワーク」ディレクトリーの下の**「リモート・アクセス・サービス」**には、以下のオブジェクトが含まれています。

- **「発信元接続プロファイル」**は、 iSeries サーバー (ローカル・システム) から発信されるアウトバウンド 2 地点間接続です。これらは、リモート・システムが受信する PPP 接続です。
- **「受信側接続プロファイル」**は、リモート・システムから発信されるインバウンド 2 地点間接続です。これらは、iSeries サーバー (ローカル・システム) が受信する PPP 接続です。
- **「モデム」**

接続プロファイルは、以下のステップに従って作成してください。

1. iSeries ナビゲーターで、ご使用のシステムを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」**と展開します。
2. 以下のいずれかのオプションを選択します。
   - **「発信元接続プロファイル」**を右マウス・ボタン・クリックして、 iSeries サーバーを、接続を開始するサーバーとして設定します。
   - **「受信側接続プロファイル」**を右マウス・ボタン・クリックして、 iSeries サーバーを、リモート・システムやユーザーからの着信接続を許可するサーバーとして設定します。
3. **「新規プロファイル」**を選択します。

4. **「新規 2 地点間接続プロファイルのセットアップ」**ページで、 プロトコル・タイプを選択します。
5. モードの選択を指定します。
6. リンク構成を指定します。
7. **「OK」**をクリックします。

   「新規 2 地点間プロファイルのプロパティー」ページが現れます。ご使用のネットワークに固有なその他の値を設定することもできます。より具体的な情報については、オンライン・ヘルプを参照してください。

プロトコル・タイプ: PPP または SLIP

2 地点間接続の作成に、どちらのプロトコル・タイプを選択したら良いのでしょうか。

PPP は、標準インターネット接続です。 PPP は、メーカーの異なるリモート・アクセス・ソフトウェア間の相互運用を可能にしています。 PPP ではまた、複数のネットワーク通信プロトコルが同じ物理通信回線を使用することもできます。

PPP は、2 地点間接続のプロトコルとして、SLIP の代わりに選択することができます。以下のような理由で、SLIP の Request for Comment (RFC) は、インターネット標準にはなりません。

- SLIP には、2 つのホストの間の IP アドレスを定義するための標準的な方針がありません。そのため、無番号ネットを使用することができません。
- SLIP には、エラー検出やエラー圧縮のサポートがありません。 PPP には、エラー検出やエラー圧縮が実装されています。
- PPP には両方向認証があるのに対し、SLIP にはシステム認証のサポートがありません。

SLIP は現在でも使用されており、まだ iSeries サーバー上でサポートされています。しかし、IBM は、2 地点間接続のセットアップの際は PPP を使用することをお勧めします。 SLIP には多重リンク接続のサポートはありません。 PPP には、SLIP より優れた認証があります。 PPP には、圧縮機能があるので、パフォーマンスもこちらのほうが優れています。

注: このリリースでは、 ASYNC の回線タイプが定義される SLIP 接続プロファイルのサポートがなくなっています。これらの接続プロファイルがある場合は、 PPP 回線タイプを使用する SLIP プロファイルか PPP プロファイルのいずれかにマイグレーションする必要があります。

モード選択

PPP 接続プロファイルにおけるモードの選択には、**接続タイプ**と**動作モード**の選択があります。選択するモードにより、新規 PPP 接続をサーバーでどのように使用するかが指定されます。

以下のステップに従って、選択するモードを指定してください。

1. 以下のいずれかの接続タイプを選択します。
   - 交換回線
   - 専用回線
   - L2TP (仮想回線)
   - PPPoE 回線
2. 新規の PPP 接続に適した動作モードを選択します。
3. 選択した接続タイプと動作モードを記録します。この情報は、PPP 接続の構成を始めるときに必要となります。

交換回線

電話回線上で接続を行う際に、以下のいずれかを使用する場合は、この接続タイプを選択してください。

- モデム (内部または外部)
- 内部 ISDN 基本速度インターフェース・アダプター
- 外部 ISDN ターミナル・アダプター

交換回線接続モードには、以下のような動作モードがあります。

- **応答**

  リモート・システムから iSeries サーバーにダイヤルできるようにするには、この動作モード・タイプを選びます。

- **ダイヤル**

  iSeries サーバーからリモート・システムにダイヤルできるようにするには、この動作モードを選びます。

- **ダイヤル・オンデマンド (ダイヤルのみ)**

  システムで TCP/IP トラフィックが検出された場合に、 iSeries サーバーからリモート・システムに自動的にダイヤルアウトできるようにするには、この動作モードを選びます。データ伝送が完了すると接続は終了し、ある特定の期間の間、TCP/IP トラフィックは発生しなくなります。

- **ダイヤル・オンデマンド (応答可能な専用対等回線)**

  この動作モードは、iSeries サーバーから専用リモート・システムの呼び出しに応答できるようにする場合に選択します。この動作モードを使うと、リモート・システムの TCP/IP トラフィックが検出されたときに、 iSeries サーバーからリモート・システムを呼び出すこともできるようになります。両方のシステムが iSeries サーバーで、この動作モードを使用している場合、両システム間の TCP/IP トラフィックはオンデマンドで流れるので、永続的な物理接続を行う必要はありません。この動作モードには専用リソースが必要です。動作モードが適正に機能するには、リモート対等回線がダイヤルインしなければなりません。

- **ダイヤル・オンデマンド (応答可能なリモート対等回線)**

  この動作モードは、リモート・システムにダイヤルまたは応答できるようにする場合に選択します。着信呼び出しを処理するには、この動作モードを指定する PPP 接続プロファイルから既存の応答プロファイルを参照しなければなりません。このタイプを選択すると、1 つの応答プロファイルを使って、1 つまたは複数のリモート対等回線からのすべての着信呼び出しを処理し、発信呼び出しごとに別々のダイヤル・オンデマンド・プロファイルを処理することができます。この動作モードでは、リモート対等回線からの着信呼び出しを処理するための専用リソースは必要ありません。

専用回線

この接続タイプは、ローカル iSeries サーバーとリモート・システムとを接続する専用回線の場合に使用します。専用回線を使用する場合、 2 つのシステムを接続するためのモデムや ISDN ターミナル・アダプターは必要ありません。

2 つのシステム間の専用回線は、相手固定回線または専用回線と見なされます。これは常時接続されています。専用回線接続の一方の端は起動側として構成され、もう一方の端は終端側として構成されます。

専用回線接続モードには、以下のような動作モードがあります。

- **終端側**

  この動作モードは、リモート・システムから専用回線を介して iSeries サーバーにアクセスできるようにする場合に選びます。この動作モードは専用回線の応答プロファイルを参照します。

- **起動側**

  iSeries サーバーが専用回線を介してリモート・サーバーにアクセスできるようにするには、この動作モードを使用します。この動作モードは専用回線のダイヤル・プロファイルを参照します。

L2TP (仮想回線)

この接続タイプは、レイヤー 2 トンネリング・プロトコル (L2TP) を使って複数のシステムを接続する場合に選択します。

L2TP トンネルを設定すると、iSeries サーバーとリモート・システムとの間に PPP 接続が作成されます。L2TP トンネル伝送と IP セキュリティー (IP-SEC) を一緒に使用すると、インターネットを介してデータを安全に送信、経路指定、および受信することができます。

L2TP (仮想回線) 接続モードには、以下のような動作モードがあります。

- **終端側**

  この動作モードは、リモート・システムから L2TP トンネルを介して iSeries サーバーに接続できるようにする場合に選びます。

- **起動側**

  iSeries サーバーから L2TP トンネルを介してリモート・システムに接続できるようにするには、この動作モードを選びます。

- **リモート・ダイヤル**

  iSeries サーバーが、L2TP トンネルを介して ISP に接続し、 ISP がリモート PPP クライアントにダイヤルするよう誘導できるようにするには、この動作モードを選択します。

- **マルチホップ起動側**

  iSeries サーバーでマルチホップ接続を確立できるようにするには、この動作モードを選択します。

  注: このマルチホップ起動側に関連した L2TP 終端側プロファイルでは、「マルチホップ接続を許可する (Allow multi-hop connection)」チェック・ボックスがチェックされ、 PPP 妥当性検査リストに、PPP ユーザー名とマルチホップ起動側プロファイルをリンクする項目が含まれている必要があります。

レイヤー 2 トンネリング・プロトコル (L2TP): L2TP は、PPP を拡張し、要求元の L2TP クライアントとターゲットの L2TP サーバー端点とをつなぐリンク層トンネルをサポートします。 L2TP トンネルを使用すると、ダイヤルアップ・プロトコルの終端のロケーションと、ネットワークへのアクセスの可能なロケーションを分離できます。

インターネット・サービス・プロバイダー (ISP) は仮想回線モードを使って、仮想プライベート・ネットワーク (VPN) を操作することもできます。 VPN が L2TP を運用する方法についてさらに詳しく知りたい場合は、 VPN で保護された L2TP 接続の構成を参照してください。

以下に、3 種類の L2TP のトンネリングのインプリメンテーション例をそれぞれ図で示します。

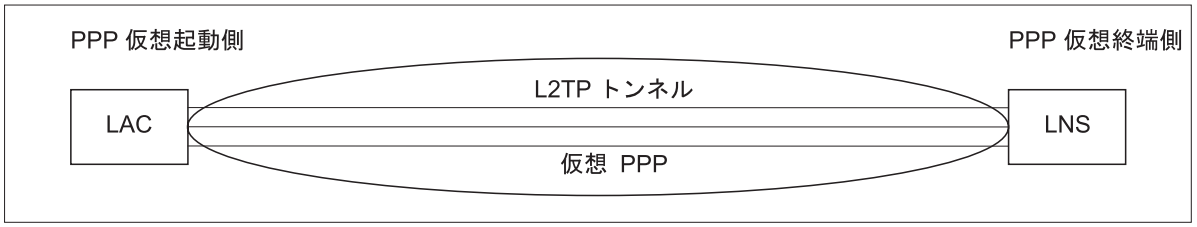


図 7. PPP 仮想起動側または PPP 仮想終端側

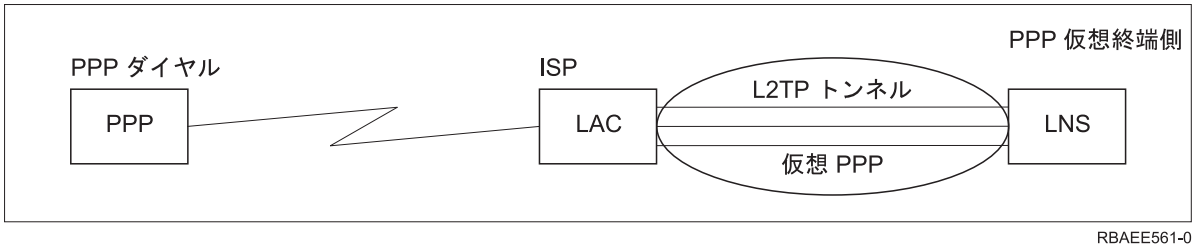


図 8. PPP ダイヤル起動側または PPP 仮想終端側

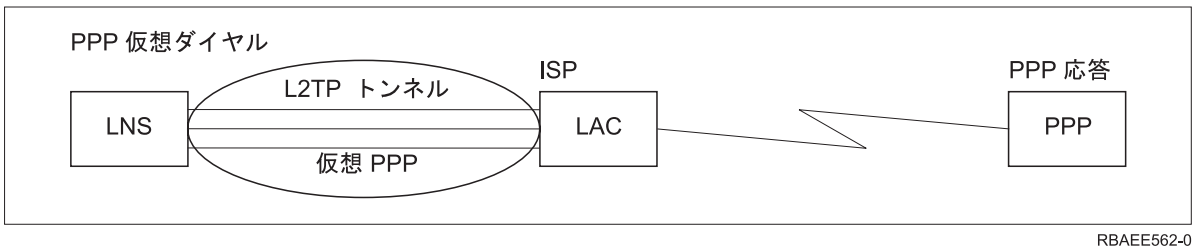


図 9. PPP 仮想ダイヤルまたは PPP 仮想応答

PPPoE 回線

PPPoE 接続は、仮想回線を使用し、タイプ 2838 イーサネット・アダプターを介して、 PPP データを DSL モデムに送信します。 DSL モデムもイーサネット・ベースの LAN に接続されており、ISP により提供されます。これにより、 iSeries サーバーからの PPP セッションを介した LAN ユーザーのための高速インターネット・アクセスが可能になります。 iSeries と ISP との間の接続が開始されたら、 LAN 上の個々のユーザーは、PPPoE 上で ISP との固有セッションを開始できます。

PPPoE 接続は、発信元接続プロファイルでのみ使用され、起動側動作モードを指定し、単一回線のみ使用します。

リンク構成

リンク構成は、接続の確立するために PPP 接続プロファイルが使用する回線サービスのタイプを定義します。回線サービスのタイプは、指定する接続タイプによって異なります。

- 単一回線
- 回線プール

- 統合 ISDN 回線

単一回線

アナログ・モデムに関連付けた PPP 回線を定義するには、この回線サービスを選びます。また、このオプションは、モデムを必要としない専用回線でも使います。 PPP 接続プロファイルでは、常に同じ iSeries サーバー通信ポート・リソースが使用されます。

望むなら、アナログ単一回線を、応答プロファイルとダイヤル・プロファイルとの間で「共用」に構成することができます。動的リソース共用は、リソースの使用可能度を拡張するために設計された新機能です。V5R2 以前は、モデム・リソースは、これを使用するプロファイルが開始されるとすぐにコミットされていました。これは、リソースが受動待ち状態の場合でも、セッションごとに 1 つのリソースにユーザーを制限することになっていました。現在では、特定のリソースがアクセスされる際に新しい共用規則が適用されるようになりました。これには、2 つのケースがあります。 1 番目は、ダイヤル・プロファイルが応答プロファイルよりも前に開始された場合です。 2 番目は、応答プロファイルがダイヤル・プロファイルよりも前に開始された場合です。前提として、リソース共用が使用可能にされていなければなりません。最初のケースでは、開始されたダイヤル・プロファイルは正常に接続します。後で開始された応答プロファイルは、回線が使用可能になるまで待機します。ダイヤル接続が終了したら、応答プロファイルは回線を要求し、開始します。 2 番目のケースでは、開始された応答プロファイルは、着信接続を待機します。着信接続が実行されないかぎり、後で開始されたダイヤル・プロファイルは、回線を「貸す」応答プロファイルから回線を「借り」ます。それから、発信接続が確立されます。接続が終了したら、ダイヤル・プロファイルは回線を応答プロファイルに戻します。この応答プロファイルは、再び着信接続を受け入れる準備をします。共用機能を使用可能にするには、交換回線の記述についてモデム・タブをクリックしてから、「動的リソース共用を使用可能にする (Enable Dynamic Resource Sharing)」を選択します。

単一回線サービスは、L2TP (仮想回線) および PPPoE (仮想回線) 接続タイプでも用いられます。 L2TP (仮想回線) 接続タイプでは、単一回線にハードウェア通信ポート・リソースは使用されません。言い換えるなら、L2TP 接続で使用される単一回線は、*仮想* 的であり、トンネルを確立するのに必要な物理ハードウェアはありません。 PPPoE 接続で使用される単一回線も、物理イーサネット回線を、リモート接続をサポートする PPP 回線であるかのように扱う機能を提供するという点で、仮想的です。 PPPoE 仮想回線は、物理イーサネット回線にバインドされて、イーサネット LAN 接続を介して DSL モデムへの PPP プロトコル・データ転送をサポートするのに使用されます。

回線プール

PPP が回線プールの回線を使用するように設定するには、この回線サービスを選択します。 PPP 接続が開始すると、iSeries サーバーは回線プールから未使用回線を選択します。ダイヤル・オンデマンド・プロファイルの場合、サーバーはリモート・システムの TCP/IP トラフィックを検出するまで回線を選択しません。

接続プロファイルの特定の回線記述を定義する代わりに、回線プールを使用することができます。回線プールには 1 つまたは複数の回線記述を指定できます。

回線プールを使用すれば、単一の接続プロファイルで複数の着信アナログ呼び出しと単一の発信アナログ呼び出しのいずれをも処理することができます。 PPP 接続が終了すると、回線は回線プールに戻されます。

回線プールを使用して同時に複数の着信アナログ呼び出しを処理する場合は、着信接続の最大数を指定する必要があります。これは、プロファイルの構成時に、**「新規 2 地点間プロファイルのプロパティー」**ダイアログの「接続」タブで設定できます。大きくなった帯域幅を使用する単一接続の回線プールを使用するには、多重リンク設定を使用してください。

回線プールを使用する利点:

- PPP 接続が開始するまで、これに回線リソースをコミットしません。

  特定の回線を使用する PPP 接続の場合、動的リソース共用が使用可能になっていない限り、回線が利用不能であれば、接続は終了します。回線プールを使用する接続の場合、プロファイルの開始時に回線プール内で少なくとも 1 回線は使用可能になっていなければなりません。

  さらに、リソースが共用として構成された (動的リソース共用を使用可能にする) 場合、特に発信接続について、リソースの可用性が向上します。
- 回線プールとともにダイヤル・オンデマンド・プロファイルを使用すれば、リソースをさらに効果的に使用できます。

  iSeries サーバーは、ダイヤル・オンデマンド接続の使用時にのみ回線プールから回線を選択します。この同じ回線は、また別の機会に、他の接続で使用することができます。
- より少ないリソースのサポートで、より多くの PPP 接続を確立することができます。

  たとえば、4 つの固有の接続タイプを必要とする環境がある場合でも、一定の時間に必要とする回線が 2 つだけであれば、回線プールを用いてこの環境を作動させることができます。 4 つのダイヤル・オンデマンド接続プロファイルを作成し、 2 つの回線記述を含んだ回線プールを個々のプロファイルに参照させます。個々の回線は 4 つの接続プロファイルすべてが使用できるので、2 つの接続をいつでも活動状態にすることができます。回線プールを使用すれば、4 つの別々の回線を持つ必要はありません。

  また、ご使用の環境が PPP クライアントと PPP サーバーとの間の組み合わせである場合、「単一回線」として使用される場合でも、「回線プール」に配置される場合でも、回線を共用する (動的リソース共用を使用可能にする) ことができます。最初に開始されたプロファイルは、接続がアクティブでないかぎり、リソースをコミットしません。たとえば、PPP サーバーが開始されており、着信接続を listen している場合、これは、使用している回線を、PPP サーバーから共用回線を開始して「借り」た PPP クライアントに「貸し」ます。

複数接続プロファイルのサポート

複数接続をサポートする 2 地点間接続プロファイルを使うと、1 つの接続プロファイルで、多数のディジタル、アナログ、または L2TP 呼び出しを処理することができます。これが便利なのは、複数のユーザーからの iSeries サーバーへの接続を可能にしたいが、各 PPP 回線を処理するために別個の 2 地点間接続を指定したくない場合です。この機能が特に便利なのは、1 つのアダプター、または 2750 および 2751 アダプターから 4 本の回線を使用できる 2805 型 4 ポート統合モデムの場合で、これによって 8 つの別々な ISDN B チャネル接続ができます。

複数接続プロファイルをサポートするアナログ回線の場合、指定された回線プール内の回線すべては最大接続数に達するまで使用されます。基本的に、回線プールに定義されている回線ごとに接続プロファイル・ジョブが 1 つずつ開始されます。すべての接続プロファイル・ジョブは、それぞれの回線での着信呼び出し待ちになります。

複数接続プロファイルのローカル IP アドレス:

複数接続プロファイルではローカル IP アドレスを使用できますが、そのアドレスは iSeries サーバー上で定義された既存の IP アドレスでなければなりません。既存のアドレスを選択するには、ローカル IP アドレスのプルダウン・リストを使用できます。 PPP プロファイルのローカル IP アドレスとして iSeries サーバーのローカル IP アドレスを選択すると、リモート・ユーザーはローカル・ネットワーク上のリソースにアクセスすることができます。また、リモート IP アドレス・プール内の IP アドレスが、ローカル IP アドレスと同じネットワーク内にあるように定義しなければなりません。

iSeries サーバーのローカル IP アドレスを持っていない場合、あるいはリモート・ユーザーによる LAN へのアクセスを望まない場合は、 iSeries サーバーの仮想 IP アドレスを定義しなければなりません。仮想 IP アドレスは、無回路インターフェースともいいます。 2 地点間プロファイルは、この IP アドレスをロ

ーカル IP アドレスとして使用できます。このアドレスは物理ネットワークに結合されていないため、iSeries サーバーに接続された他のネットワークにトラフィックを自動的に転送するわけではありません。

仮想 IP アドレスを作成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで使用しているサーバーを展開し、**「ネットワーク」→「TCP/IP 構成」→「IPV4」→「インターフェース」**の順にアクセスします。
2. **「インターフェース」**を右ボタンでクリックし、**「新しいインターフェース」→「仮想 IP」**を選択します。
3. インターフェース・ウィザードの指示に従って、仮想 IP インターフェースを作成します。仮想 IP アドレスが作成されると、2 地点間接続プロファイルはそのアドレスを使用できます。ご使用のプロファイルでアドレスを使用するには、「TCP/IP 設定」ページにある「ローカル IP アドレス」フィールドのプルダウン・リストを使用できます。

   注: 仮想 IP アドレスは、複数接続プロファイルを開始する前に活動状態にしておかなければなりません。そうしないと、プロファイルは開始しません。インターフェースの作成後にアドレスを活動化するには、インターフェース・ウィザードの使用時にアドレスを開始するためのオプションを選択します。

複数接続プロファイルのリモート IP アドレス:

複数接続プロファイルでは、リモート IP アドレスも使用できます。典型的な 1 つの接続 2 地点間プロファイルでは、1 つのリモート IP アドレスを指定できるだけです。このアドレスは、接続の確立時に呼び出し側システムに与えられます。複数の呼び出し元からの同時接続が可能になったので、リモート IP アドレス・プールを使って、開始のリモート IP アドレスを定義することに加え、呼び出し側システムに与えられる他の IP アドレスの範囲も定義します。

回線プールの制約事項:

複数接続用の回線プールを使用する際には、以下の制約事項が適用されます。

- 個々の回線は、一度に 1 つの回線プール内にしか置くことはできません。回線プールから回線を除去すると、その回線を別の回線プールで使用することができます。
- 回線プールを使用する複数接続プロファイルを開始する場合、回線プール内のすべての回線は、プロファイルに指定された最大接続数に達するまで使用されます。使用可能な回線がない場合、新しい接続はすべて失敗します。また、回線プール内に使用可能な回線がない状態で別のプロファイルが開始すると、そのプロファイルは終了します。
- 回線プールを持つ単一接続プロファイルを開始する場合、システムはその回線プールから 1 つの回線だけを使用します。同じ回線プールを使用する複数接続プロファイルを開始すると、回線プール内の残りの回線が使用可能になります。

リモート IP アドレス・プール: システムは、複数の着信接続に使われるすべての応答または終端の 2 地点間接続プロファイルに、リモート IP アドレス・プールを使用することができます。それには、L2TP、固有 ISDN、複数の最大接続数を持つ回線プールが含まれます。この機能により、システムは個々の着信接続に固有のリモート IP アドレスを割り当てることができます。

最初に接続するシステムは、「開始 IP アドレス」フィールドに定義されている IP アドレスを受信します。そのアドレスがすでに使用されている場合、「アドレスの数」の範囲内で次に使用可能な IP アドレスが付与されます。たとえば、開始 IP アドレスが 10.1.1.1 で、「アドレスの数」が 5 に定義されていると

仮定します。リモート IP アドレス・プール内で使用可能なアドレスは、10.1.1.1、10.1.1.2、10.1.1.3、10.1.1.4、および 10.1.1.5 になります。リモート IP アドレス・プールのアドレスに定義されるサブネット・マスクは、常に 255.255.255.255 になります。

リモート IP アドレス・プールを使用するときは、次の制約事項が適用されます。

- 複数の接続プロファイルが同じアドレス・プールを指定できます。ただし、そのプール内のすべてのアドレスが使われると、他の接続が終了してアドレスを未割り振りに戻さない限り、その後のすべての要求は拒否されます。
- 他の着信システムがプール内のアドレスを使えるようにすると同時に、一部のリモート・システムに特定のアドレスを割り振るには、以下のステップに従ってください。
  1. **「認証」**タブからリモート・システムの認証を使用可能にして、そのリモート・システムのユーザー名が認識できるようにします。
  2. 特定の IP アドレスを必要としないすべての着信接続要求に対して、リモート IP アドレス・プールを定義します。
  3. **「リモート・システムのユーザー ID に基づいて追加の IP アドレスを定義」**をチェックし、**「ユーザー名によって定義されている IP アドレス」**をクリックして、特定のユーザー用のリモート IP アドレスを指定します。

  リモート・ユーザーが接続するとき、 iSeries サーバーはそのユーザー用に特定の IP アドレスが定義されているかどうかを判別します。定義されている場合、その IP アドレスがリモート・システムに与えられます。定義されていない場合、リモート IP アドレス・プールのアドレスが返されます。

ISDN

ISDN ネットワーク接続に関連付けた PPP 回線を定義するには、この回線サービスを選びます。

ISDN を使用する利点:

- ISDN は、高速で円滑な通信を提供します。
- ISDN の目的は、単一のインターフェースと高速ディジタル・ネットワークを使って、すべてのタイプのデータを伝送するための汎用接続を提供することです。
- ISDN にはまた、交換回線接続での接続時間を高速化する機能があります。アナログ・モデムの接続は確立までに 30 秒ほどかかるのに対して、ISDN 接続はほんの数秒しかかかりません。

PPP 用のモデムの構成

アナログ PPP 接続の場合、外部モデム、内部モデム、または ISDN ターミナル・アダプターのいずれかを使用することができます。モデムには、アナログ接続機能 (専用および交換回線) が備わっています。大半の汎用モデムのモデム記述は iSeries サーバー用に定義されています。

モデム構成タスクには次のようなものがあります。

- 新規モデムを構成する
- モデムと回線記述を関連付ける
- モデムのコマンド・ストリングを設定する

新規モデムの構成

1. iSeries ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」**と展開します。

2. **「モデム」**を右ボタンでクリックし、**「新規モデム」**を選択します。
3. 「一般」タブで、すべてのフィールド・ボックスに正しい値を入力します。
4. **オプション:** 「追加パラメーター」タブをクリックして、ご使用のモデムに必要な初期化コマンドを追加します。
5. **「OK」**をクリックして項目を保管し、「新規モデムのプロパティー」ページをクローズします。

既存のモデム記述を使用できるかどうかを判別するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」**と展開します。
2. **「モデム」**を選択します。
3. 「モデム」リストを調べて、製造社名、モデル、およびモデムの構造を検討します。

   注: ご使用のモデムがデフォルト・リストに含まれていれば、残りのステップを実行する必要はありません。
4. ご使用のモデムによく似たモデム記述を右ボタンでクリックして、**「プロパティー」**を選択し、 コマンド・ストリングを調べます。
5. モデムの資料を調べて、モデムに合った特定のコマンド・ストリングを判別します。

   コマンド・ストリングがご使用のモデムの要件と一致していれば、デフォルトのモデム・プロパティーを使用します。一致しなければ、ご使用のモデムに合ったモデム記述を作成し、その記述を「モデム」リストに追加します。

モデム記述を作成するには、以下のステップに従ってください。

1. オペレーション・ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→「リモート・アクセス・サービス」** と展開します。
2. **「モデム」**を選択します。
3. 「モデム」リストから、**「$generic hayes」**を右ボタンでクリックし、**「これを基にした新規モデム」**を選択します。
4. **「新規モデム」**ダイアログで、ご使用のモデムが必要とする情報に合うように コマンド・ストリングを変更します。

モデムのコマンド・ストリングの設定

以下の表は、iSeries サーバーで定義されるモデムが使う、最小限のコマンド・ストリングのセットをリストしています。ご使用のモデムのユーザーズ・マニュアルには、これらと同等のコマンド・ストリングがあります。モデム記述では、製造元が推奨する設定値を使用してください。

モデムのプロパティー	**大半のモデムに該当するコマンド・ストリング**
工場設定値にリセットされたモデム	AT&F または AT&Z
モデムの初期設定:	
Verb の結果コードの表示	Q0 および V1
通常の CD または DTR モード	&C1 および &D2
エコー・モードのオフ	E0
搬送波検出用のデータ・セット作動可能 (DSR)	&S1
ハードウェア・フロー制御の使用可能化: (RTS/CTS)	
エラー訂正とオプションの圧縮の使用可能化 (V.42/V.42 bis)	

DTE-DCE 回線速度の、固定の 115.2 Kbps (またはモデムの最大値) での稼働の可能化	
(オプション) モデムがこの機能をサポートしない場合の非活動時間の使用可能化	
モデム応答モード:	
n リング後の応答	S0=*n* (ただし、n = 1 または 2)
m 秒後に搬送波 (接続) がない場合の切断	S7=*m*
モデムのダイヤル・タイプ	ATDT (トーン・ダイヤルの場合) または ATDP (パルス・ダイヤルの場合)

例: ISDN ターミナル・アダプターの構成

1. オペレーション・ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」** と展開します。
2. **「モデム」**を右ボタンでクリックし、**「新規モデム」**を選択します。
3. 「一般」タブで、すべてのフィールド・ボックスに正しい値を入力します。
4. **オプション:**「ISDN パラメーター」タブをクリックして、ご使用のモデムに必要な初期化コマンドを追加します。

   ISDN ターミナル・アダプターの場合、このリスト内のコマンドとパラメーターは、次のような条件の場合のみターミナル・アダプターに送信されます。
   - リスト内のコマンドまたはパラメーターが変更または追加されたとき
   - iSeries サーバーが実行する特定のエラー回復アクションの結果として

   したがって、これらのコマンドには以下の事柄を含め、それらに限定してください。
   - 電話会社から提供される ISDN の交換タイプとバージョンの設定
   - 電話会社から提供される電話番号と、サービス・プロファイル識別コード (SPID) の設定
   - 場合によって電話会社から提供される端末入力 ID (TEI) の設定
   - B チャネル・プロトコル (非同期から同期への PPP) の設定
   - パラメーターの長さを示すための改行を必要とする、可変長パラメーターをもつその他のモデム設定
   - システムをリセットまたは電源オフした後に復元できるようにするための、新規設定の保管と活動化
   - *U* インターフェース状況プローブ・コマンド (ATD*x*)。これは、ISDN 中央局交換との同期がいつとられたかを iSeries サーバーが判断するのに使います。 *x* は、# および * を含め、電話番号に使える任意の数字です。
5. **「追加」**をクリックし、追加のモデム・コマンドを追加します。これで、関連パラメーターを指定してもしなくても、モデム・コマンドと簡単な記述をコマンド・リストに追加できるようになりました。関連パラメーターを付けないで指定したどのコマンドにも、モデムに回線記述を関連付けたときにパラメーターを割り当てることができます。
6. **「OK」**をクリックして項目を保管し、「新規モデムのプロパティー」ページをクローズします。

モデムと回線記述を関連付ける

1. iSeries ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→「リモート・アクセス・サービス」→「発信元接続プロファイル」** または**「受信側接続プロファイル」**と展開します。
2. 以下のいずれかのオプションを選択します。

- 既存の接続プロファイルを処理する場合は、接続プロファイルを右マウス・ボタン・クリックして、**「プロパティー」**を選択します。
- 新規接続プロファイルを処理する場合は、新しい接続プロファイルを作成します。

3. 「新規 2 地点間プロファイルのプロパティー」ページから、**「接続」**タブを選択し、**「新規」**をクリックします。
   - リンク構成の名前を入力します。
   - **「新規」**をクリックして「新規回線のプロパティー」ダイアログ・ボックスを開きます。
4. 「新規回線のプロパティー」ダイアログ・ボックスから、**「モデム」**タブをクリックし、モデムをリストから選択します。選択されたモデムは、この回線記述に関連付けられます。内部モデムには、適切なモデム定義が既に選択されているはずです。詳細については、オンライン・ヘルプを参照してください。

V5R2 では、発信元接続プロファイルを構成して、着信呼び出しを待機する受信側接続プロファイルに割り当てられる PPP 回線およびモデムを「借りる」ようにすることができます。発信元の接続は、接続終了時に PPP 回線およびモデムを受信側接続プロファイルに「戻し」ます。この新機能を使用可能にするには、PPP 回線構成ダイアログの「モデム」タブから**「動的リソース共用を使用可能にする (Enable dynamic resource sharing)」**オプションを選択します。 PPP 回線は、レシーバーおよび発信元の接続プロファイルの「接続」タブから構成できます。

リモート PC の構成

Windows 32 ビット・オペレーティング・システムを実行している PC から iSeries サーバーへの接続を行うには、モデムがインストールされて、適切に構成されているかどうかを検査し、パーソナル・コンピューター上に TCP/IP と「ダイヤルアップ・ネットワーク」がインストールされていることを確認してください。

PC 上での「ダイヤルアップ・ネットワーク」の構成については、Microsoft Windows の資料を参照してください。必ず、次の情報を指定または入力してください。

- ダイヤルアップ接続のタイプは、必ず **PPP** にします。
- 暗号化パスワードを使用している場合は、必ず MD-5 CHAP を使用してください (iSeries サーバーでは MS-CHAP はサポートされていません)。 Windows のあるバージョンは、MD-5 CHAP を直接にはサポートしていなくても、 Microsoft の付加的な支援を受けることによって、そのように構成することができます。
- 暗号化されていない (保護されていない) パスワードを使用する場合は、自動的に PAP が使用されます。保護されていないその他のプロトコル・タイプは iSeries サーバーではサポートされません。
- 通常、IP アドレスは、リモート・システムが定義するか、この場合のように iSeries サーバーが定義します。代替 IP アドレス方式 (独自の IP アドレスを定義するものなど) の使用を計画している場合は、iSeries サーバーがそのアドレス方式を受け入れるよう構成されているかどうかを確認してください。
- ご使用の環境にとって適切であれば、DNS IP アドレスを追加してください。

AT&T Global Network を介するインターネット・アクセスの構成

IBM は、AT&T Global Network を介したインターネット・アクセスを提供します。このサービスを利用するには、「AT&T Global Network ダイヤル接続」ウィザードを使用して、交換ダイヤル PPP 接続プロファイルを構成し、AT&T Global Network にダイヤルすることができます。このウィザードは 8 つのパネルを順番に表示し、10 分ほどで完了します。ウィザードはいつでも取り消すことができ、既存のデータは保管されません。

AT&T Global Network 接続を使用できるアプリケーションには、次の 2 つのタイプがあります。
- **電子メール・サービス**: 単一の AT&T Global Network アカウントからメールを定期的に検索して iSeries サーバーに送信し、 Lotus Mail のユーザーまたはシンプル・メール転送プロトコル (SMTP) のユーザーに配布できるようにします。
- **ダイヤルアップ・ネットワーク**: AT&T Global Network とともに、他のダイヤルアップ・ネットワーク・アプリケーション (標準インターネット・アクセスなど) を使用します。

AT&T Global Network の接続プロファイルは、他の PPP 接続プロファイルと同じように保守します。

「AT&T Global Network ダイヤル接続」ウィザードを使用するには、以下のいずれかのアダプターが必要です。
- 2699: 2 回線通信アダプター
- 2720: PCI WAN/平衡型 IOA
- 2721: PCI 2 回線通信アダプター
- 2745: PCI 2 回線通信アダプター (IOA 2721 に代わるものです)
- 2761: 8 ポート・アナログ・モデム IOA
- 2771: 2 ポート WAN IOA (ポート 1 上には V.90 組み込みモデムが、ポート 2 上には通信インターフェースがある)。 2771 アダプターのポート 2 を使用するには、外部モデムか、適切なケーブルが付いた ISDN ターミナル・アダプターが必要です。
- 2772: 2 ポート V.90 組み込みモデム WAN IOA
- 2793: 2 ポート WAN IOA (ポート 1 上には V.92 組み込みモデムが、ポート 2 には標準通信インターフェースがある)。これは、2771 に代わるものです。
- 2805: 4 ポート WAN IOA (V.92 モデム内蔵)。これは、モデル 2761 および 2772 に代わるものです。

「AT&T Global Network ダイヤル接続」ウィザードを開始する前に、ご使用の環境について、以下のような情報を収集する必要があります。
- 電子メール・サービス・アプリケーションまたはダイヤルアップ・ネットワーキング・アプリケーションの場合は、 AT&T Global Network アカウント情報 (アカウント番号、ユーザー ID、およびパスワード)。
- 電子メール・サービス・アプリケーションの場合は、メール・サーバーおよびドメイン・ネーム・サーバーの IP アドレス。
- 単一回線接続の場合は、使用するモデムの名前。

「AT&T Global Network ダイヤル接続」ウィザードを開始するには、以下のステップに従ってください。
1. iSeries ナビゲーターで、ご使用のサーバーを展開し、**「ネットワーク」→「リモート・アクセス・サービス」** の順にアクセスします。
2. **「発信元接続プロファイル」**を右ボタンでクリックし、**「新規 AT&T Global Network ダイヤル接続」**を選択します。
3. 「AT&T Global Network ダイヤル接続」ウィザードが開始したら、**「ヘルプ」**をクリックして、パネルを完成させるための情報を調べます。

接続ウィザード

「新規ダイヤル接続 (New Dial Connection)」ウィザード

このウィザードは、ダイヤルアップ接続プロファイルを構成してインターネット・サービス・プロバイダー (ISP) つまりインターネットにアクセスするためのステップを示します。このウィザードを完了するには、ネットワーク管理者やインターネット・サービス・プロバイダー (ISP) からいくらかの情報を入手する必要がある場合があります。このウィザードについての詳細は、オンライン・ヘルプを参照してください。

ユニバーサル・コネクション・ウィザード

このウィザード選択は、エレクトロニック支援が IBM と接続するために使用するプロファイルを構成するためのステップを示します。エレクトロニック支援は、固有の iSeries サーバー・システム環境のモニターを行い、そのシステムと状況に対して個別設定された修正を使用するよう勧めます。このウィザードについての詳細は、オンライン・ヘルプを参照してください。

グループ・アクセス・ポリシーの構成

「受信側接続プロファイル」の下の**「グループ・アクセス・ポリシー」**フォルダーには、リモート・ユーザーのグループに設定する 2 地点間接続パラメーターを構成するためのオプションがあります。これは、リモート・システムが発信し、ローカル・システムが受信する 2 地点間接続にのみ適用されます。

新規グループ・アクセス・ポリシーの構成は、次のように行います。

1. オペレーション・ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→「リモート・アクセス・サービス」→「受信側接続プロファイル」**と展開します。
2. **「グループ・アクセス・ポリシー」**を右マウス・ボタン・クリックし、**「新規グループ・アクセス・ポリシー」**を選択します。
3. **「一般」**タブで、新規のグループ・アクセス・ポリシーの名前と記述を入力します。
4. **「多重リンク」**タブをクリックして、多重リンク構成をセットアップします。

   この多重リンク構成は、複数の物理回線を結合して 1 つのバンドルにすることを指定するものです。バンドルあたりのリンクの最大数は、1 ～ 16 になります。接続が行われるまでは、回線のタイプの設定が分からないため、デフォルト値は常に 1 です。特定のユーザーに対する多重リンク・プロトコルの機能を拡張したり、制限したりするには、グループ・アクセス・ポリシーを使用することができます。

   - **「バンドル当りの最大接続数」**では、 1 つの論理回線にしたいリンク (または回線) の最大数を指定します。回線の最大数は、このグループ・ポリシーを PPP プロファイル用のセッションに設定するときに有効な空き回線の数より大きくすることはできません。
   - リモート・システムが Bandwidth Allocation Protocol (BACP) をサポートしている場合にのみ接続が確立されるよう指定するには、**「帯域幅割り振りプロトコルが必要」**をチェックします。 BACP について折衝できない場合、単一リンクのみ許可されます。
5. **「TCP/IP 設定」**タブをクリックして、以下のものを有効にします。
   - リモート・システムが他のネットワークにアクセスすること (IP 転送) を許可

     このオプションは、IP 転送を行うか否かを指定するものです。これを選択する場合は、必ず iSeries サーバーをその接続のルーターとして使用できるようにしなければなりません。これを使用すれば、この iSeries サーバーに宛先指定されていないインターネット・プロトコル (IP) のデータグラムを、このシステムを介して接続されているネットワークに渡すことができます。これをブランクにすると、インターネット・プロトコル (IP) は、リモート・システムからのデータグラムのうち、宛先のアドレスがこの iSeries サーバーにとってローカルではないものを廃棄します。

     セキュリティーの理由で、IP 転送を行いたくない場合もあるかもしれません。それに反し、インターネット・サービス・プロバイダー (ISP) は普通、常に IP 転送を提供しています。これが有効になるのは、システム全域で IP データグラム転送が行える場合だけであることに注意してください。そう

でない場合は、たとえマークされていても無視されます。システム全域に渡る IP データグラム転送は、「TCP/IP のプロパティー」ページの「設定」タブから表示することができます。

- TCP/IP によるヘッダーの圧縮を要求する (Request TCP/IP header compression) (VJ)

  このオプションは、接続が確立された後に、インターネット・プロトコル (IP) によってヘッダー情報が圧縮されるようにするか否かを指定するものです。普通、圧縮を行うと、対話式トラフィックや低速のシリアル回線では特に、パフォーマンスが向上します。ヘッダーの圧縮は、RFC 1332 で定義されている Van Jacobson (VJ) 方式に従って行われます。 PPP では、接続が確立される際に、圧縮の折衝が行われます。接続のもう 1 つの終端で、VJ 圧縮がサポートされていない場合、 iSeries サーバーは、圧縮を用いない接続を確立します。

- この接続に IP パケット規則を使用する (Use IP packet rules for this connection)

  このオプションは、このグループ・ポリシーにフィルター規則を適用するか否かを指定するものです。フィルター規則を用いることで、ネットワーク内で許可される IP トラフィックを制御することができます。システムを保護するには、この IP パケット・フィルター操作コンポーネントを使用することができます。 IP パケット・フィルター操作コンポーネントは、ユーザーが指定する規則に従ってパケットのフィルター操作を行うことによって、システムを保護します。規則は、パケットのヘッダー情報に基づきます。

  IP パケット規則についての詳細は、 Information Center にある IP パケット・フィルター操作および NAT のトピックを参照してください。

例については、グループ・ポリシーおよび IP フィルターを使用してリソースへのユーザー・アクセスを管理するを参照してください。

リモート・アクセス・ユーザーへのグループ・ポリシーの適用:

新しい**受信側接続プロファイル**の 2 地点間プロパティーの設定を完了したならば、リモート・アクセス・ユーザーにグループ・アクセス・ポリシーを適用することができます。

リモート・アクセス・ユーザーへのグループ・ポリシーの適用は、次のように行います。

1. **「認証」**ページをクリックします。
2. **「この iSeries サーバーがリモート・システムの識別を検査することが必要」**をチェックします。
3. **「妥当性検査リストを使用してローカルから認証」**を選択します。
4. 既存の妥当性検査リストがある場合は、プルダウン・リストからそれを選択し、**「開く」**をクリックします。初めてこれを作成する場合は、新しい妥当性検査リストにつける名前を入力し、**「新規」**をクリックします。
5. **「追加」**をクリックして、新規ユーザーをその妥当性検査リストに追加します。
6. 「ユーザーの追加」ダイアログ・ボックスで、以下を実行します。
   - ユーザー名を定義する認証プロトコルを選択します。
   - ユーザー名とパスワードを入力します。

     注: セキュリティーのため、Challenge Handshake Authentication Protocol22314 (CHAP)、 Extensible Authentication Protocol (EAP)、 Password Authentication Protocol (PAP) に定義されるユーザーには、同じパスワードを使用しないようお勧めします。
   - **「グループ・ポリシーをユーザーに適用する」**をチェックし、プルダウン・リストからグループ・ポリシーを選択して**「開く」**をクリックします。

グループ・ポリシーのプロパティーを変更したり、既存のセットアップを処理したりすることもできます。**「OK」**をクリックして構成を完了し、「2 地点間プロファイルのプロパティー」ページに戻ります。

PPP 接続への IP パケット・フィルター規則の適用

Information Center の IP パケット・フィルター規則と NAT 規則 のトピックには、 PPP 接続プロファイルで参照できる IP パケット規則の作成方法についての解説があります。ご使用のネットワークで IP アドレスへのグループ・アクセスを制限するには、パケット規則ファイルを使用することができます。 PPP 接続を使用したフィルター規則ファイルの使用例については、『シナリオ: グループ・ポリシーおよび IP フィルターを使用してリソースへのリモート・ユーザー・アクセスを管理する』を参照してください。

既存の IP パケット・フィルター規則を使用する方法には、次の 2 つがあります。

- 接続プロファイル・レベルで
  1. **受信側接続プロファイル**の**「2 地点間プロファイルのプロパティー」**を完成させてから、「TCP/IP 設定」ページを選択して、**「拡張」**をクリックします。
  2. **「IP パケット規則をこの接続に使用」**をチェックして、プルダウン・リストから PPP フィルター ID を選択します。
  3. **「OK」**をクリックして PPP フィルターを接続プロファイルに適用します。
- ユーザー・レベルで
  1. 既存のグループ・アクセス・ポリシーを開くか、新規のグループ・アクセス・ポリシーを作成します。
  2. 「TCP/IP 設定」ページをクリックします。
  3. **「IP パケット規則をこの接続に使用」**をチェックして、プルダウン・リストから PPP フィルター ID を選択します。
  4. **「OK」**をクリックして PPP フィルターを適用します。

接続プロファイルにおける RADIUS および DHCP サービスの使用可能化

PPP 受信側接続プロファイルにおける RADIUS および DHCP サービスを使用可能にするには、次のように行います。

1. オペレーション・ナビゲーターで、使用しているサーバーを選択し、**「ネットワーク」→ 「リモート・アクセス・サービス」** と展開します。
2. **「リモート・アクセス・サービス」**を右マウス・ボタン・クリックし、**「サービス」**を選択します。
3. **「DHCP-WAN」**タブをクリックします。これにより、DHCP は自動的に使用可能になり、システムでどの DHCP サーバーおよびリレー・エージェント (ある場合) が稼働しているかを検出します。
4. RADIUS サービスを使用可能にするために、**「RADIUS」**タブをクリックします。
   a. **「RADIUS ネットワーク・アクセス・サーバー接続を使用可能にする」**を選択します。
   b. **「認証に RADIUS を使用可能にする (Enable RADIUS for authentication)」**を選択します。
   c. ご使用の RADIUS ソリューションに適用できる場合には、 RADIUS アカウンティングおよび TCP/IP アドレス構成を使用可能にすることもできます。
5. **「RADIUS NAS 設定 (RADIUS NAS settings)」**ボタンをクリックして、 RADIUS サーバーへの接続を構成します。
6. 「OK」をクリックして、iSeries ナビゲーターに戻ります。

RADIUS 構成の例については、 RADIUS サーバーによるダイヤルアップ・ユーザーの認証のシナリオを参照してください。

第 7 章 PPP の管理

iSeries サーバー上で実行できる PPP 管理タスクは以下のとおりです。

- 接続プロファイルのプロパティーの設定
- PPP 活動のモニター

PPP 接続プロファイルのプロパティーの設定

接続プロファイルを作成する際は、普通、「2 地点間接続プロファイルのセットアップ」ダイアログ・ボックスで、新規接続プロファイルのプロトコル、接続タイプ、動作モードを選択します。このダイアログ・ボックスで選択したものを入力すると、「接続プロファイルのプロパティー」シートが現れます。「2 地点間接続プロファイルのセットアップ 」ダイアログ・ボックスに指定する選択が、「接続プロファイルのプロパティー」シートのページの内容とタブの配列を決定します。発信元接続プロファイルのプロパティー・シートと受信側接続プロファイルのプロパティー・シートは異なります。

「新規 2 地点間プロファイルのプロパティー」ダイアログ・ボックスの各ページを完了する際は、以下の指針に従うことができます。各ページで選択する設定値は、実際の環境、および構成する接続タイプによって異なります。 iSeries ナビゲーターのオンライン・ヘルプには、ダイアログ・ボックスに表示されている各オプションの説明があります。詳細については、PPP の例と手順を参照してください。

PPP 活動のモニター

このページでは、オペレーション・ナビゲーターを使って、接続プロファイルおよびセッション・ログを表示する方法について説明します。

PPP 接続ジョブについて:

- 個々の PPP 接続ジョブの管理には、次のような 2 つの PPP 制御ジョブが用いられます。これらのジョブは、QSYSWRK サブシステムで実行します。
  - QTPPPCTL - 主要な PPP 制御ジョブ。各 PPP 接続ジョブは、このジョブで管理します。
  - QTPPPL2TP - L2TP サーバー。このジョブは、L2TP プロファイルが現在実行されている場合にのみ実行され、作成される L2TP トンネルを管理します。
- PPP 接続ジョブは、QTCP ユーザー・プロファイルの下で実行し、個々の PPP 接続の処理に使用されます。これらのジョブは、デフォルトでは、QUSRWRK サブシステムで実行しますが、その他のシステムで実行するように構成することもできます。次のような名前の 2 つの PPP 接続ジョブが使用されます。
  - QTPPPSSN - このジョブは、L2TP 以外のすべての PPP 接続の処理に使用されます。
  - QTPPPL2SSN ジョブは、QTPPPL2TP ジョブが L2TP トンネルとの折衝に成功した後に仮想 PPP データを処理します。
- SLIP 接続ジョブは、QTCP というユーザー名の下にある QSYSWRK サブシステムで実行されます。SLIP ジョブ名には、次の 2 つのタイプがあります。
  - QTPPDIAL*nn* はダイヤルアウト・ジョブです。ただし、*nn* は 1 から 99 までの任意の数字です。
  - QTPPANS*nn* はダイヤルイン・ジョブです。ただし、*nn* は 1 から 99 までの任意の数字です。

接続プロファイルの処理:

1. iSeries ナビゲーターで、ご使用のサーバーを展開し、**「ネットワーク」→「リモート・アクセス・サービス」** の順にアクセスします。**「発信元接続プロファイル」**か**「受信側接続プロファイル」**を選択します。
2. 「プロファイル」列で、任意の接続プロファイル名を右ボタンでクリックし、次のいずれかのオプションを選択します。
   - **「ジョブ」**を選ぶと、 QTPP*xxx* ジョブのジョブ・ログが開きます。
   - **「接続」**を選択すると、このプロファイルに関連したすべての接続の情報を表示するダイアログ・ボックスが開きます。この情報には、現行接続かその前の接続のいずれか、またはその両方の接続データが含まれます。各接続ごとのジョブの出力や接続の詳細を表示するオプションもあります。
   - **「プロパティー」**を選ぶと、接続の現行プロパティーを表示する「プロパティー」ページが開きます。

接続情報の表示:

1. iSeries ナビゲーターで、ご使用のサーバーを展開し、**「ネットワーク」→「リモート・アクセス・サービス」** の順にアクセスします。**「発信元接続プロファイル」**か**「受信側接続プロファイル」**を選択します。
2. 「プロファイル」列で、非活動状態を示さない任意の接続プロファイル名を右ボタンでクリックし、**「接続」**を選択して接続情報を表示します。

   このプロファイルの (現行および以前の) 接続がそれぞれ表示されます。この状況フィールドは、接続の現行状況を示します。各 PPP ジョブの状況に応じて、接続されているユーザーのユーザー ID、ローカルおよびリモート IP アドレス、 PPP ジョブの名前などといったその他の情報が表示されます。
3. ジョブ出力や接続の詳細を表示するには、「接続」を右マウス・ボタン・クリックします。すると、ボタンが使用可能になります。
4. ジョブ出力を表示する場合は、**「ジョブ」**をクリックします。「ジョブ・ログ」で、ジョブ名を右ボタンでクリックし、**「プリンター出力」**を選択します。接続セッション・ログとジョブ・ログ (終了済みのセッション用) の内容が表示されるようになります。
5. 接続の詳細を表示する場合は、**「詳細」**をクリックします。詳細は、現行で活動中の接続の詳細だけが表示されます。「詳細」ダイアログでは、特定の接続の追加接続情報を表示することができます。

iSeries サーバーからの PPP 出力の処理:

iSeries サーバーのコマンド行で PPP 出力のタイプ WRKTCPPTP を処理するには、次のように行います。

- (QTPPPCTL と QTPPPL2TP ジョブを含め) 活動中のすべての PPP ジョブを処理するには、 **F14** (活動中のジョブの処理) を押します。
- 特定の接続プロファイルのすべての出力を処理するには、そのプロファイルに **option 8** (出力の処理) を選択します。
- PPP プロファイル構成を印刷するには、そのプロファイルに **option 6** (印刷) を選択します。印刷出力にアクセスするには WRKSPLF コマンドを使用します。

接続状況:

接続プロファイル状況は、接続プロファイルのリスト内の各プロファイル用の**「状況」**フィールドに表示されます。この接続プロファイルは、発信元またはレシーバー・プロファイルのいずれかを選択した後に、**「ネットワーク」→「リモート・アクセス・サービス」**を選択してオープンできます。個々の接続の状況は、「接続」ダイアログを用いて表示されます。

1 次状況の記述	説明
接続要求を待機中	レシーバー・プロファイルが接続を待機している。
着信を待機中	サーバーが接続を待機している。
接続中	リモート・システムに接続中である。
アクティブ / 接続アクティブ	接続が行われ、ジョブが正常に実行されている。
非アクティブ	現在、この接続プロファイルについて実行されているジョブがない。
終了	情報が有効である。
マルチホップ・ターミネーターがマルチホップ起動側を開始中	マルチホップが進行中。
マルチホップ接続がアクティブ	マルチホップは正常に接続された。

2 次状況の記述	説明
モデムの初期化中	ダイヤルアップ接続の開始時にモデムを初期化している。
モデム接続の待機中	PPP サーバーは listen 状況にある。
xxx-xxxx をダイヤル中	ダイヤルアップ・クライアントによりダイヤルされる番号。
着信呼び出し検出	PPP サーバーが着信モデム呼び出しを検出した。
モデム接続済み	PPP ハンドシェークが正常に完了した。
操作可能	PPP 接続がアクティブである。
リンク終了	相手側により接続が終了した。
停止	プロファイルまたはジョブが終了した。
認証失敗	PPP 接続は、認証が失敗したために確立できなかった。
接続の無活動タイムアウト	PPP 接続は、無活動タイムアウトが原因で確立できなかった。
IP アドレスの折衝中	PPP 接続は、IP の折衝の問題が原因で終了した。
リモート・モデム無応答	PPP 接続は、相手からの応答がないために確立できなかった。
プロトコル拒否	PPP 接続は、NCP の折衝が失敗したために確立できなかった。
再試行失敗	PPP 接続は、再試行カウントを超えたために確立できなかった。
相手側より PPPoE セッション確認を受信	PPPoE 折衝は正常に完了した。
L2TP 呼び出し確立	L2TP トンネル・アップ・メッセージ

第 8 章 PPP のトラブルシューティング

プログラム一時修正 (PTF) とトラブルシューティングに関係のある現行の情報は、 iSeries サーバー TCP/IP ホーム・ページ で説明されています。このリンクをたどると、このトピックに含まれる情報の補足や変更に関する最新情報を参照できます。

PPP 接続の問題に直面した場合、このチェックリストを使用してエラー情報を収集することができます。このチェックリストは、エラーの徴候を確認して、PPP 接続の問題を解決するのに役立ちます。

1. 必要なサポート資料:
   - リモート・ホスト・タイプ、オペレーティング・システム、およびレベル
   - iSeries サーバー・ホスト・オペレーティング・システムのレベル
   - 障害が発生するセッションのジョブ・ログと接続ダイアログ・ファイル

     V5R1 では、ジョブ・ログと接続ダイアログの出力が、プロファイルと同じ名前で OUTQ に保管されます。
   - 接続スクリプト (実際の環境で使用している場合)
   - 接続障害の前後における接続プロファイルの状況
2. 推奨されるサポート資料:
   - 回線記述
   - 接続プロファイル

     プロファイル設定は、WRKTCPPTP のオプション 6 で印刷できます。
   - モデムのタイプおよびモデル
   - モデムのコマンド・ストリング
   - 通信のトレース

ITSO レッドブック TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190) には、次のような PPP 問題に関する詳しい説明があります。これには、詳細な問題解決情報もあります。

問題	ソリューション
モデムのハードウェア構成 ディップ・スイッチとその他のハードウェア設定の構成に誤りがある。	正しいフレーム指示タイプでモデムが構成されているかどうかを確認します。これは、*非同期* か *同期* のいずれかにすることができます。詳細については、モデムのマニュアルを参照してください。
モデムの AT コマンド 使用しようとしているモデムがオペレーション・ナビゲーターのモデムの事前定義リストに含まれていない。	新規モデムを作成します。
PPP のユーザーとパスワード PPP への接続を試行中に、ユーザー名とパスワードのエラーが発生する。	• ユーザー ID とパスワードが同じ大文字小文字で入力されているかを確認します。 • 対等回線で使用されている認証プロトコルが同一であるかを確認します。 • ある対等回線では PAP を使用しているのに、他の対等回線は CHAP として構成されているというようなことがないようにしてください。

問題	ソリューション
接続プロファイルを開始する PPP 回線 指定された PPP 回線が同じハードウェア・リソースによって使用されている。	同じハードウェア・リソースを使用している他の回線をオフに変更してください。
PPP プロトコル PPP プロトコルの構成ミスのために、接続エラーが発生することがある。	構成エラーのために、対等回線どうしが相互に通信できないような状況では、より低いレベルの PPP プロトコルを検査する必要があるかもしれません。 PPP ログまたは PPP ジョブのジョブ・ログに問題が表示されない場合は、通信トレース機能を使用してその問題を調査することができます。

第 9 章 PPP に関するその他の情報

PPP に関するその他の情報源:

- 最新のプログラム一時修正 (PTF) と PPP および L2TP に関する最新構成情報については、 iSeries server TCP/IP ホーム・ページ  の PPP リンクを参照してください。このリンクをたどると、**リモート・アクセス・サービス: PPP 接続**のトピックの補足や変更に関する最新情報を参照できます。
- ITSO レッドブック TCP/IP for iSeries server: More Cool Things Than Ever (SG24-5190)  には、TCP/IP のサービスと設定に関する詳しい説明があります。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12