IBM Systems - iSeries

ネットワーキング
ネットワーク・シナリオ

バージョン 5 リリース 4

IBM Systems - iSeries

ネットワーキング
ネットワーク・シナリオ

バージョン 5 リリース 4

ご注意

本書および本書で紹介する製品をご使用になる前に、 45 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS® (プロダクト番号 5722-SS1) のバージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： IBM Systems - iSeries
Networking
Network Scenarios
Version 5 Release 4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

目次

ネットワーク・シナリオ

ネットワーキングというテーマには、膨大な量の情報が含まれます。このトピックは、ネットワーキングに関する基本的な情報を提供することではなく、特定のネットワーキング環境で使用される iSeries™ テクノロジーの例を提供することを目的としています。以下のシナリオは、iSeries サーバーで使用可能なネットワーク・サービスおよびアプリケーションの活用方法を明示することを意図しています。

トピックの印刷

この情報の PDF を表示および印刷する場合に使用します。

この文書の PDF 版を表示またはダウンロードするには、「ネットワーク・シナリオ」を選択します。

次の関連トピックの 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。

- TCP/IP セットアップ には次のトピックが含まれています。
  - Internet Protocol バージョン 6 (IPv6)
  - TCP/IP セットアップの計画
  - TCP/IP のインストール
  - TCP/IP の構成
  - TCP/IP のカスタマイズ
  - 仮想イーサネットを介した TCP/IP 技法
- リモート・アクセス・サービス には、以下のトピックが含まれています。
  - PPP シナリオ
  - PPP の概念
  - PPP の計画
  - PPP の構成
  - PPP の管理
  - PPP のトラブルシューティング
- 仮想プライベート・ネットワーク には、以下のトピックが含まれています。
  - VPN シナリオ
  - VPN の概念
  - VPN の計画
  - VPN の構成
  - VPN の管理
  - VPN のトラブルシューティング
- TCP/IP トラブルシューティング には、以下のトピックが含まれています。
  - 対話式トラブルシューター
  - トラブルシューティング・ツールおよび手法
  - 特定のアプリケーションに関連する問題のトラブルシューティング

PDF ファイルの保存

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 ファイルを右マウス・ボタンでクリックする。(リンク上を右マウス・ボタンでクリックする。)
2. PDF をローカル側に保存するオプションをクリックする。
3. PDF を保管するディレクトリーを指定する。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Reader をご使用のシステムにインストールする必要があります。Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から無料のコピーをダウンロードできます。

ネットワーク計画ワークシート

ネットワーキングの基本的な考慮事項については、このワークシートをお読みください。

このワークシートは、ネットワーク計画のリサーチを行う際の補足用として使用してください。各シナリオには、ネットワーク環境についての前提条件と前提事項を含む、これと同様の表が含まれています。以下の表は、すべての環境に対するあらゆるネットワーク設計を網羅しているわけではありませんが、ユーザーの環境について検討するための基本を示しています。例えば、これらのシナリオに取り組む前に、サーバーの可用性、パフォーマンス、機能などを考慮する必要があります。

サーバー・ワークシート	**回答**
サーバー・モデルを記録してください。	
オペレーティング・システムのバージョンを記録してください。	
論理区分化された環境を理解し、文書化してください。	
iSeries サーバーに接続する必要のあるクライアントを決定してください。	
インストールされている通信アダプターのタイプを記録してください。イーサネット、トークンリング、およびその他の詳細は、「ネットワーク通信」を参照してください。	
通信リソース名を記録してください。	
iSeries サーバーの IP アドレスを記録してください。	
iSeries サーバーのサブネット・マスクを記録してください。	
ゲートウェイ・アドレスを記録してください。	
ホスト名とドメイン名を記録してください。	
ドメイン・ネーム・サーバーの IP アドレスを記録してください。	

ネットワーク・ワークシート	**回答**
明確なネットワークの目標を設定しください。	
ユーザーは誰で、その要件は何ですか ?	
それらの要件をサポートするのは、どのアプリケーションですか ?	
これらのアプリケーションではどの程度のパフォーマンスが要求されますか ?	

ネットワーク・ワークシート	回答
必要なプロトコルは何ですか ? 相互運用性に留意してください。ほとんどのネットワークでは TCP/IP を使用しますが、他のプロトコルも使用できます。詳細は、「ネットワーク通信」を参照してください。	
一部のアプリケーションの優先順位を、ほかのものより高くする必要がありますか ?	
アプリケーションは遅延やパケット・ロスの影響を受けやすいですか ?	
特定のセキュリティーを必要とするアプリケーションはどれですか ? セキュリティー計画を、ネットワーク計画に組み込んでください。ネットワーク・セキュリティーの計画に関する資料は、「eServer™ Security Planner」を参照してください。	
このネットワークの規模は今後拡大しますか ? また、それはいつ頃ですか ? 必ず、基本的なネットワーク体系におけるセキュリティーを考慮してください。	
LAN 用としてどのテクノロジーを使用しますか ?	
ネットワークに接続するその他の装置は何ですか ?	
ネットワークの図を描いてください。	

関連資料

5 ページの『計画ワークシートを検討する』

シナリオ: LAN と通信するように iSeries をセットアップする

ネットワーク管理者は、ローカル・エリア・ネットワーク (LAN) に新しい iSeries サーバーを追加します。このシナリオでは、ネットワーク管理者に、LAN と通信するように iSeries サーバーをセットアップする際の前提条件と、その手順を提供します。

設定

ユーザーは、Sampson Organic Produce という、小規模な卸売業者のネットワーク管理者であると想定します。顧客には、有機栽培の高品質な農産物を求める地域の食料品店や個人の家庭が含まれています。これまでに会社は成長を続けてきており、在庫をより効率的に管理するために、最近新しい iSeries サーバーを購入しました。従来、リソースと主要なビジネス・アプリケーションは、個々のワークステーションに保管されていました。ビジネスが変化するにつれ、これらのアプリケーションのデータをより簡単に共用できるようにする必要があることが明らかになりました。例えば、電話で注文を受ける従業員には、製品が出荷可能かどうかを確認するために、より速く在庫をチェックする手段が必要です。これまでは、在庫データベースにアクセスできる従業員に問い合わせている間、顧客を待たせていました。

ユーザーは、新しいサーバー上に、これらの主要なビジネス・アプリケーションのすべてを統合することを計画しています。新しいサーバーに必要なハードウェア計画とセットアップ・タスクはすべて、すでに完了しています。通信とネットワーキングは調査済みで、イーサネットによるローカル・エリア・ネットワーク (LAN) を作成することが決定されています。

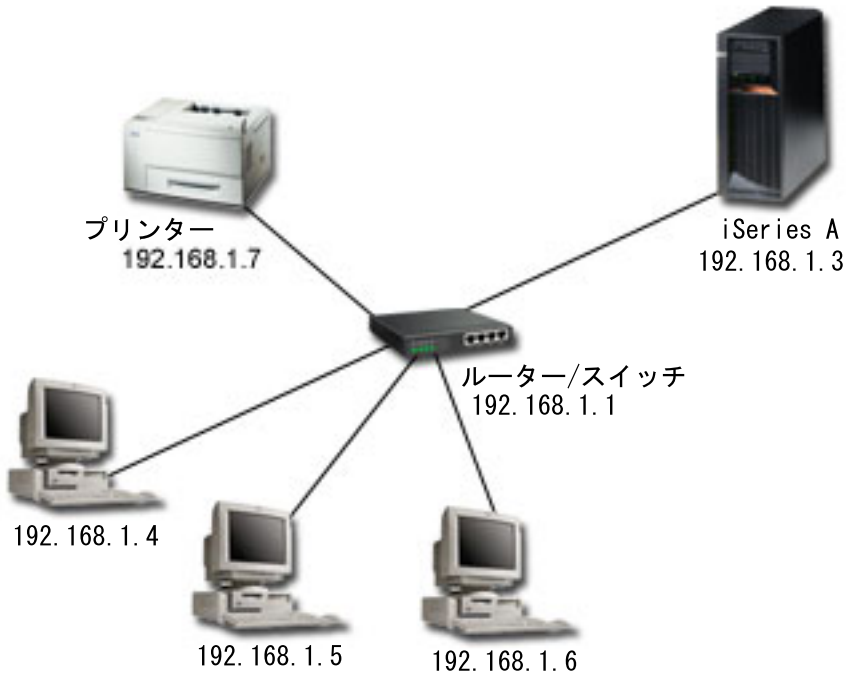
目的

LAN にサーバーを追加すると、以下の目的を達成することができます。

- LAN と通信するように iSeries をセットアップする。
- LAN 用のプリンターをセットアップする。
- サーバー上に保管されているデータを確実に保護する。
- 他のホストと通信する TCP/IP サービスを定める。

詳細

次の図は、ルーターに接続されている iSeries サーバーを示しています。ルーターには 3 台のワークステーションと 1 台のプリンターも接続されており、Sampson Organic Produce という名称の小規模な架空の会社のネットワークを表しています。



- iSeries A は OS/400® バージョン 5 リリース 2 (V5R2) 上で稼働し、関連するすべてのビジネス・アプリケーションが含まれています。
- iSeries A の IP アドレスは 192.168.1.3 です。
- iSeries A のサブネット・マスクは 255.255.255.128 です。
- ワークステーション 1 の IP アドレスは 192.168.1.4 です。
- ワークステーション 2 の IP アドレスは 192.168.1.5 です。
- ワークステーション 3 の IP アドレスは 192.168.1.6 です。
- プリンター の IP アドレスは 192.168.1.7 です。
- ネットワーク内のルーターの IP アドレスは 192.168.1.1 です。

ヒント: 外部ネットワーク接続を計画していない場合は、ルーターまたはスイッチの代わりにハブを使用することもできます。

前提条件および前提事項

このシナリオでは、このネットワーク環境で以下の前提条件がすでに満たされていると仮定しています。

- ネットワークのためのすべての配線とハードウェアのセットアップがすでに完了している。
- ルーターを使用する場合は、ルーターが構成済みである。ハブまたはスイッチを使用する場合、構成は必要ありません。

構成のステップ

以下のタスクを完了してください。各ステップの後に、次のタスクへのリンクがあります。

計画ワークシートを検討する

綿密な計画を立てた後、ネットワーク管理者は以下の質問に回答しました。これらの質問は、このシナリオで示されているタスクに直接影響を及ぼします。ブランクの表 (独自のワークシートを作成する場合) については、『2 ページの『ネットワーク計画ワークシート』』を参照してください。

サーバー・ワークシート	回答
サーバーのサイズを記録してください。	モデル 820
オペレーティング・システム (1 つまたは複数) を記録してください。	i5/OS™
現在の論理区分化された環境を理解し、文書化してください。	論理区画なし
iSeries に接続する必要のあるクライアントを決定してください。	IBM® @server ® iSeries Access for Windows® (iSeries ナビゲーターを組み込んだもの)。
インストールされている通信アダプターのタイプを記録してください。	イーサネット
通信リソース名を記録してください。	cmn01
iSeries サーバーの IP アドレスを記録してください。	192.168.1.3
iSeries サーバーのサブネット・マスクを記録してください。	255.255.255.128
ゲートウェイ・アドレスを記録してください。	192.168.1.1
ホスト名とドメイン名を記録してください。	iseriesa.sampson.com
ドメイン・ネーム・サーバーの IP アドレスを記録してください。	この LAN は別のネットワークに接続されていないため、DNS は必要ありません。この会社は、ネットワーク上のすべてのシステムのホスト・テーブル項目を追加しました。

ネットワークの前提事項	会社の決定
ユーザーは誰で、その要件は何ですか ?	顧客の注文を取る 3 つのエリア。
それらの要件をサポートするのは、どのアプリケーションですか ?	Web ベースではない社内受注アプリケーション。
必要なプロトコルは何ですか ? 相互運用性に留意してください。	TCP/IP
アプリケーションは遅延やパケット・ロスの影響を受けやすいですか ?	いいえ
ご使用のアプリケーションにはセキュリティーに関する特定の考慮が必要ですか ?	基本的なシステム・セキュリティー。詳細はシナリオに組み込みます。
このネットワークの規模は今後拡大しますか ? また、それはいつ頃ですか ? 必ず、基本的なネットワーク体系におけるセキュリティーを考慮してください。	はい。時期は確かではありません。
ネットワークに接続するその他の装置は何ですか ?	プリンター — IBM Infoprint® 40

ネットワークの前提事項	会社の決定
ネットワークの図を描いてください。	シナリオの図を参照してください。

関連概念

2 ページの『ネットワーク計画ワークシート』
ネットワーキングの基本的な考慮事項については、このワークシートをお読みください。

TCP/IP Connectivity Utilities ライセンス・プログラムをインストールする

1. TCP/IP 用のインストール・メディアをサーバーに挿入する。このサーバーは、インストール・メディアとして CD-ROM 装置を使用します。
2. コマンド行に `GO LICPGM` と入力してから、Enter を押して、「ライセンス・プログラムの処理」画面にアクセスする。
3. 「ライセンス・プログラムの処理」画面で、オプション 11 (ライセンス・プログラムの導入) を選択する。ライセンス・プログラムと、そのオプションの機能の一覧が表示されます。
4. 57xxTC1 (TCP/IP Connectivity Utilities for iSeries)、57xxCM1 (Communications Utilities)、および 57xxXE1 (iSeries Access for Windows) の横の「オプション」欄に 1 (導入) と入力する。Enter を押します。「ライセンス・プログラムの導入の確認」画面に、導入するよう選択したライセンス・プログラムが表示されます。
5. Enter で確認する。
6. ネットワーク管理者は、「導入オプション」画面で、下記の選択項目を入力する。
   - 導入装置: QOPT (これは CD-ROM 装置から導入する場合です。)
   - 導入するオブジェクト: プログラムと言語の両方のオブジェクト。
   - 自動再始動: はい (導入が正常に完了した後で、システムを自動的に再始動するかどうかを決定します)。

   TCP/IP Connectivity Utilities が正常に導入されると、「ライセンス・プログラムの処理」メニューか「サインオン (Sign On)」画面のいずれかが表示される。
7. オプション 50 (メッセージのログの表示) を選択して、ライセンス・プログラムが正常に導入されたかどうかを調べる。

TCP/IP の構成

1. コマンド行で、`WRKHDWRSC *CMN` と入力して、「通信資源の処理」メニューを表示する。
2. イーサネット・ポートの通信リソースの横に `5` と入力し、Enter を押します。
3. 「構成記述の処理」メニューで 1 と入力し、Enter を押す。
4. 「回線記述の作成 (イーサネット) (CRTLINETH)」メニューが表示される。
5. 「**回線記述**」フィールドで、回線の記述を入力する。この例では、ネットワーク管理者は `Eth01` を選択しました。
6. 「**回線速度**」および「**二重**」フィールドに情報を入力する。これらの値は、iSeries に接続しているスイッチ上のポートと一致させてください。この例では、100M および *HALF が使用されます。Enter を押します。
7. F10 を押して、追加のパラメーターを表示する。これらのパラメーターを表示するには、次ページ・キーを押す必要がある場合もあります。

8. 「リンク速度」フィールドを、前に入力した「回線速度」と一致するように変更する (この例では、100M)。
9. その他のすべてのデフォルト値を受け入れて、Enter を押す。
10. F3 を押して、「通信資源の処理」メニューに戻る。
11. もう一度 F3 を押して、「コマンド入力」メニューに戻る。
12. コマンド行に CFGTCP と入力して、「TCP/IP の構成」メニューを表示する。
13. 「TCP/IP の構成」メニューで、オプション 1 (TCP/IP インターフェースの処理) を選択する。
14. オプション 1 (追加) を選択して「TCP/IP インターフェースの追加」画面を表示するために、 Enter を押す。
15. 以下の値を入力して新しい TCP/IP インターフェースを作成し、Enter を押す。
    - インターネット・アドレス: 192.168.1.3
    - 回線記述: Eth01
    - サブネット・マスク: 255.255.255.128

    重要: これらのアドレスは、例示のみを目的としています。実際のネットワークに合った値を入力する必要があります。
16. F3 を押して、「TCP/IP の構成」メニューに戻る。
17. 「TCP/IP の構成」メニューで、オプション 2 (TCP/IP 経路の処理) を選択する。
18. オプション 1 (追加) を選択して「TCP/IP 経路の追加 (ADDTCPRTE)」画面に進むために、 Enter を押す。
19. 以下の値を入力して経路を作成し、Enter を押す。
    - 経路宛先: *DFTROUTE
    - サブネット・マスク: *NONE
    - 次のホップ: 192.168.1.1

    注: 別のネットワークに接続していない場合、この経路は必要ありません。この会社は将来インターネットに接続することが分かっているため、ここでこれを追加します。
20. 「TCP/IP の構成」メニューでオプション 10 (TCP/IP ホスト・テーブル項目の処理) を選択し、 Enter を押す。
21. オプション 1 (追加) を選択して「TCP/IP ホスト・テーブル項目の追加」画面を表示するために、 Enter を押す。
22. 以下の値を入力してホスト・テーブル項目を追加し、Enter を押す。
    - IP アドレス: 192.168.1.3
    - ホスト名: iseriesa.sampson.com
    - 名前: iseriesa
23. ネットワーク上の各システムで、 ステップ 22 を繰り返す。サーバーがドメイン・ネーム・システム (DNS) として構成されていないため、各システムがホスト・テーブル項目をもつ必要があります。例えば、iSeries A がワークステーション 1 (192.168.1.4/wstn1) と通信するためには、次のホスト・テーブル項目を新たに追加します: **IP アドレス**: 192.168.1.4、**ホスト名**: wstn1.sampson.com、**名前**: wstn1。ご使用のネットワーク環境においてこのような構成が現実的でない場合は、Information Center の DNS 構成のトピックを参照してください。
24. コマンド行で STRTCP と入力し、TCP/IP を開始します。これにより、インターフェースと回線も開始されます。

TCP/IP をテストする

TCP/IP Connectivity Utilities ライセンス・プログラムを正常にインストールし、iSeries システム上で TCP/IP を構成した後、TCP/IP 接続をテストする必要があります。

ネットワークへの TCP/IP 接続をテストするには、以下のようにします。

1. 各ワークステーション上で TCP/IP 通信が構成され、開始されていることを確認する。ご使用のワークステーションのベンダーから提供された資料を使用してください。
2. ワークステーション 1 でコマンド・プロンプトを開き、`ping 192.168.1.3` と入力する。パケットが iSeries A に送信されたことを確認するメッセージを受け取る場合があります。これは、ワークステーションがサーバーにアクセスできることを確認するためのメッセージです。ネットワークへの接続が失敗すると、 Information Center の TCP/IP トラブルシューティングのトピックで詳細を参照できます。

ワークステーションに iSeries Access for Windows をインストールして構成する

ライセンス・プログラム (LP) のインストール手順の実行中に、Sampson Organic Produce はサーバー上に iSeries Access for Windows 用の LP をインストールしました。 iSeries ナビゲーター (iSeries Access for Windows のコンポーネント) を使用するには、パーソナル・コンピューターにクライアントをインストールする必要もあります。ご使用の PC にクライアントをインストールする方法の詳細については、 iSeries Access for Windows の説明を参照してください。

LAN 上にプリンターを構成する

オフィスの LAN に接続された共通のプリンターをユーザーが共用できるようにして、ユーザーに印刷サービスを提供する必要もあります。このネットワークにあるプリンターは、Simple Network Management Protocol (SNMP) と互換性があります。iSeries システムをプリント・サーバーとして使用して、LAN 上で、印刷ジョブを管理しこのプリンターに送信します。このプリンターは、ネットワーク・アダプターによって LAN に接続されています。

iSeries サーバーを、印刷ジョブを管理するプリント・サーバーとしてセットアップするには、以下のステップを実行します。

1. プリンターを構成する
   a. すべてのケーブル接続が完了していることを確認する。
   b. プリンターが、プリンターの説明書に従ってセットアップされていることを確認する。
   c. プリンターの制御パネルで、「ポートのタイムアウト (Port Timeout)」を 300 (5 分) に設定する。このタイマーは、プリンターが最後のページを印刷するまで待機する時間を秒単位 (5 から 300) で制御します。タイマーは、印刷のためのコマンドによって終了しません。
2. 印刷装置記述を作成する
   a. 文字ベースのインターフェースから `CRTDEVPRT` と入力して、印刷装置記述を作成する。印刷装置記述は、プリンターが LAN に直接接続されているときに作成する必要があります。
   b. 「装置記述の作成 (印刷装置)」画面で、以下のパラメーターを入力する。

      ヒント: 適宜 F10 と Enter を押して、すべてのパラメーターを表示する必要があります。下にリストされていないパラメーターについては、画面に表示されるデフォルト値を受け入れることができます。各パラメーターの詳細説明については、iSeries Information Center の CL コマ

ンド検索プログラムを使用してください。 CRTDEVPRT コマンドを名前で検索し、装置記述の作成 (印刷装置) (CRTDEVPRT) コマンドを選択します。

- 装置記述: PRINTER1
- 装置クラス: *LAN
- 装置タイプ: 3812
- 装置型式: 1
- LAN 接続機構: *IP
- ポート番号: 2501
- 用紙送り: *AUTOCUT
- 印刷装置・エラー・メッセージ: *INFO
- メーカーのタイプおよび型式: *IBM4340
- 用紙入れ 1: *LETTER
- 用紙入れ 2: *LETTER
- エンベロープ・ソース: *NONE
- 名前またはアドレス: 192.168.1.7
- ユーザー定義オプション: *IBMSHRCNN
- システム・ドライバー・プログラム: *IBMSNMPDRV
- テキスト記述: IBM IP40 用、*LAN 3812 SNMP 装置記述

c. コマンド行から VRYCFG と入力して、PRINTER1 の構成をオンに構成変更する。

d. 「構成変更 (VRYCFG)」画面で、以下の項目を入力する。

- 構成オブジェクト: PRINTER1
- タイプ: *DEV
- 状況: *ON

e. これらのフィールドに入力し、Enter を押す。

f. コマンド行で STRPRTWTR と入力し、印刷装置書き出しプログラムを開始する。

g. 「印刷装置書き出しプログラムの開始 (STRPRTWTR)」画面で、「**プリンター (Printer)**」フィールドに PRINTER1 と入力する。Enter を押します。

3. プリンター接続をテストする

a. プリンターの電源が入っており、作動可能であることを確認する。

b. WRKWTR (すべてのプリンターを処理するコマンド) と入力して、印刷装置の状況が STR であることを確認する。

c. ping 192.168.1.7 と入力して、iSeries A がプリンターと通信できることを確認する。 システムがプリンターに接続されていることを示す確認メッセージが表示されます。

関連資料

CL コマンド検索プログラム

ネットワーク接続をテストする

ネットワーク用のプリンター構成が完了したら、ネットワーク内のすべての接続をテストする必要があります。

ネットワーク内のすべての接続をテストするには、以下のステップを実行してください。

1. コマンド行から ping xx.xx.xx.xx と入力する。ここで、*xx.xx.xx.xx* はワークステーションとプリンターのそれぞれの IP アドレスです。
2. 各ワークステーションのコマンド・プロンプトから ping xx.xx.xx.xx と入力する。ここで、*xx.xx.xx.xx* は iSeries サーバーとプリンターの IP アドレスです。

   ヒント: 各ワークステーション上で新しいプリンターを構成し、それぞれのホスト・テーブルにプリンターの IP アドレスを追加する必要があります。
3. **任意:** 次の指示に従ってテスト・ページを印刷する。
   a. iSeries ナビゲーターから、「**基本操作**」 → 「**プリンター出力**」を選択する。
   b. 右側のペインで出力名を右マウス・ボタン・クリックし、「**オープン**」を選択して出力を表示する。
   c. ビューアーから、「**ファイル**」 → 「**印刷**」を選択する。
   d. 印刷オプションを選択し、「**印刷**」をクリックする。このページがプリンターに送信されます。

これらの接続が機能しなかった場合、Sampson Organic のネットワーク管理者は TCP/IP トラブルシューティングを使用して問題を突き止めることができます。

iSeries サーバーの保護

このトピックの推奨事項は、Sampson Organic Produce Company 用として IBM eServer Security Planner によって生成されたものです。IBM eServer Security Planner を実行して、これらの詳細を検討してください。

ヒント: 以下の推奨事項には、これらのシステム値に関するセキュリティー値と運用上の考慮事項の詳細説明は含まれていません。

表 1. 全体的なセキュリティーの推奨事項

システム値	推奨値
QSECURITY	40
QINACTITV	60
QINACTMSGQ	*DSCJOB
QDSCJOBITV	240
QSHRMEMCTL	1 (はい)
QRETSVRSEC	1 (はい)
QRMTSRVATR	0 (いいえ)
QRMTIPL	*NONE

表 2. パスワード・ポリシーの推奨事項

システム値	推奨値
QPWDLVL	0
QPWDEXPITV	90
QPWDMINLEN	8
QPWDRQDDIF	8
QPWDLMTCHR	*NONE
QPWDLMTAJC	0 (許可)
QPWDLMTREP	0 (文字を繰り返すことができる)

表 2. パスワード・ポリシーの推奨事項 (続き)

システム値	推奨値
QPWDPOSDIF	0 (いいえ)
QPWDRQDDGT	1 (はい)
QPWDVLDPGM	*NONE

表 3. サインオン・ポリシーの推奨事項

システム値	推奨値
QDSPSGNINF	1 (はい)
QLMTDEVSSN	0 (いいえ)
QLMTSECOFR	1 (はい)
QMAXSIGN	3
QMAXSGNACN	2 (ユーザー・プロファイルを使用不可にする)
QRMTSIGN	*FRCSIGNON (常にサインオンを表示する)

表 4. 復元ポリシーの推奨事項

システム値	推奨値
QALWOBJRST	*ALWPTF
QVFYOBJRST	3
QFRCCVNRST	3

表 5. 監査ポリシーの推奨事項

システム値	推奨値
QAUDCTL	*AUDLVL、*OBJAUD、*NOQTEMP
QAUDCTL	*NONE
注: 監査報告書は月 1 回でスケジュールされます。	

関連タスク

『システム・セキュリティーの推奨事項をインプリメントする』

関連資料

セキュリティー参照

セキュリティー・プランナー

関連情報

i5/OS システム値検索プログラム

システム・セキュリティーの推奨事項をインプリメントする

iSeries サーバーに保管されている資産を保護するため、 Sampson Organic Produce は、IBM eServer Security Planner を使用しました。これは、システム環境に基づいて動的な推奨事項のセットを作成する、対話式の計画ツールです。このツールにアクセスするには、IBM eServer Security Planner を参照してください。Sampson Organic Produce の管理者が Security Planner で生成したセキュリティーに関する推奨事項は、ユーザーが自身のセキュリティー設定をインプリメントする際の例として使用することができます。

iSeries A にセキュリティーをインプリメントするには、以下のステップを実行してください。

1. iSeries ナビゲーターで、「**iSeries A**」を展開し、「**セキュリティー**」を右マウス・ボタン・クリックして「**構成**」を選択する。
2. 「ウェルカム」ページで、「**次へ**」をクリックする。
3. 「**普通**」を選択して、全般的なセキュリティー・ポリシーを記述する。「**次へ**」をクリックします。
4. 「**ビジネス・アプリケーションの実行**」を選択して、サーバーの使用方法を記述する。「**次へ**」をクリックします。
5. 「**いいえ**」を選択し、「**次へ**」をクリックする。
6. APPC の使用に対して「**いいえ**」を選択し、「**次へ**」をクリックする。
7. 「**はい**」を選択して TCP/IP を使用することを指定し、「**次へ**」をクリックする。
8. 「**いいえ**」を選択してインターネットに接続しないことを指定し、「**次へ**」をクリックする。
9. 「**いいえ**」を選択し、「**次へ**」をクリックする。
10. 「**いいえ**」を選択して、IBM iSeries NetServer™ を使用しないことを指定する。「**次へ**」をクリックします。
11. 「**いいえ**」を選択し、「**次へ**」を 2 回クリックします。
12. 「**はい**」を選択して、サーバーのセキュリティー関連のアクションを監査する。「**次へ**」をクリックします。
13. 「**はい**」を選択して、システムのセキュリティーをモニターするレポートをスケジュールする。「**次へ**」をクリックします。
14. これらのレポートのスケジューリングとして「**月に一度**」を選択する。「**次へ**」をクリックします。
15. セキュリティーに関する推奨事項を見直すには、「**詳細**」をクリックする。セキュリティーの値は、該当するセキュリティー管理を解除することによって変更することができます。「**OK**」をクリックします。次に「**次へ**」をクリックします。
16. 管理者およびユーザー情報レポートを保管するディレクトリーを指定する。「**次へ**」をクリックします。これらのレポートのそれぞれを見直すことができます。
17. もう一度「**次へ**」をクリックする。
18. 「**はい、今すぐ変更を行います**」を選択し、「**完了**」をクリックする。これで、iSeries A のセキュリティー構成が完了しました。

関連資料

10 ページの『iSeries サーバーの保護』

セキュリティー・プランナー

TCP/IP サービス、アプリケーション、およびプロトコルを調査する

Sampson Organic Produce が将来インプリメントできる TCP/IP サービスは、そのほかにも多数あります。最も一般的なユーティリティーは、Telnet と FTP です。さらに、印刷、TCP/IP アプリケーション、プロトコル、サービス、および iSeries Navigator の追加機能について詳しく知ることができます。

関連資料

TCP/IP アプリケーション、プロトコル、およびサービス

印刷

シナリオ: リモート接続を使用可能にする

会社に 1 つの営業所があり、そこに所属する数名の外勤の営業スタッフが iSeries サーバーに接続する必要があるとします。また、別の都道府県にある本社オフィスにも接続します。これらの地域間で送信される会社の情報は機密情報であるため、インターネットを介して送信する場合の情報保護面に不安があります。このシナリオを使用して、リモート・クライアントおよびサーバーへの接続を構成します。

設定

数人の外勤の営業スタッフを管理する営業所のネットワーク管理者の場合を想定します。また、別の都道府県にある本社オフィスとの作業も行います。外勤の営業スタッフと本社オフィスは、両方とも営業所の内部ネットワークにアクセスする必要があります。しかし、情報をインターネットを介して送信する際の情報の保護に関して、不安があります。

本社オフィスは、顧客の口座や請求書のような機密情報へのアクセスを頻繁に必要とします。外勤の営業スタッフは、Point-to-Point Protocol (PPP) を介してインターネット・サービス・プロバイダー (ISP) にダイヤルアップすることによって、営業所に情報を送信します。外勤の営業スタッフは機密情報も送信するため、この通信でのデータ保全性とプライバシーを確保する必要があります。クレジット・カード番号や顧客の連絡先などの機密情報は、インターネットには公開しないようにする必要があります。両方のユーザー・グループに対するオプションをリサーチした結果、本社オフィスへの接続を保護するためには仮想プライベート・ネットワーク (VPN) を使用し、外勤の従業員に対しては、VPN によって保護されたレイヤー 2 トンネリング・プロトコル (L2TP) を使用することを決定しました。

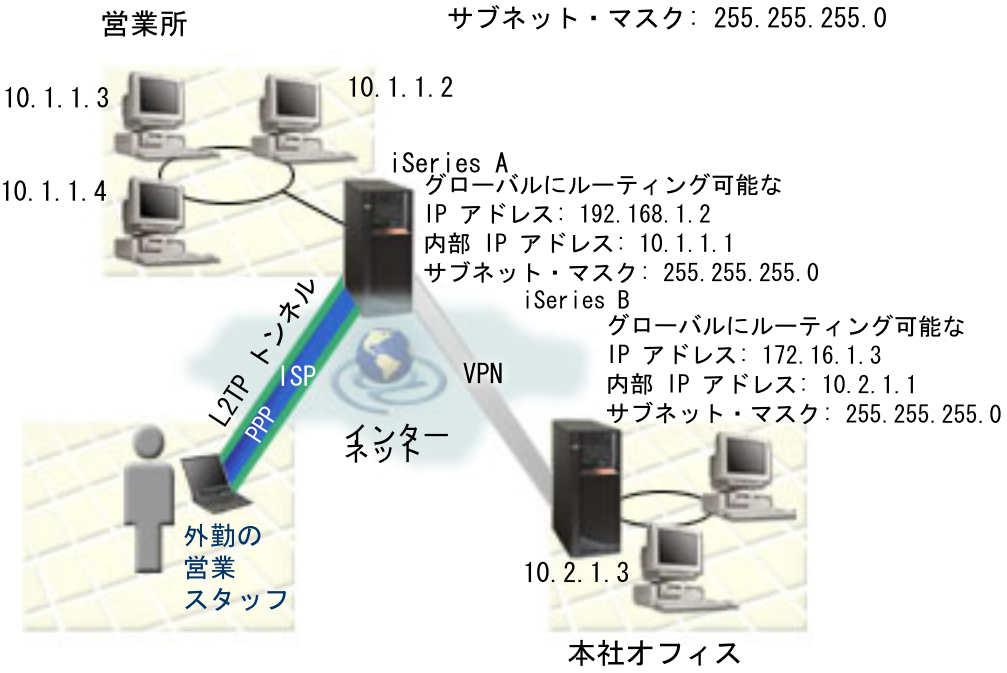
目的

MyCo, Inc の管理者には以下の目的があります。

- 外勤の営業スタッフと本社オフィスにアクセスを提供する。
- 既存の iSeries サーバーを使用して、これらの目標に対応する。
- 外勤の営業スタッフと本社オフィスがこの営業所のネットワークにアクセスできるようにする。

詳細

以下のネットワーク・トポロジーは、営業所と本社オフィス、および外勤の営業スタッフの間の接続を示しています。営業所への接続は、VPN によって保護されています。図に続く、このネットワークの各部についての説明は、構成の詳細を示します。



営業所

- iSeries A は OS/400 バージョン 5 リリース 2 (V5R2) 上で稼働し、関連するすべてのビジネス・アプリケーションが含まれています。
- iSeries A は、この営業所の VPN 接続のゲートウェイとして機能します。
- iSeries A は、グローバルに経路指定が可能な IP アドレス 192.168.1.2 を持っています。

  重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレス体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
- サブネット・マスクは 255.255.255.0 です。
- iSeries A は、IP アドレス 10.1.1.1 でそのサブネットに接続します。
- 営業所の内部ネットワークでは、すべての PC が、iSeries A をポイントするデフォルトの経路で構成されています。
- iSeries A の完全修飾ホスト名は iseriesa.myco.min.com です。
- iSeries A および B は、両方とも接続を開始することができます。
- 外勤の従業員は、範囲が 10.1.1.100 から 10.1.1.150 の IP アドレスのプールを使用します。

本社オフィス

- iSeries B は OS/400 バージョン 5 リリース 2 (V5R2) 上で稼働し、関連するすべてのビジネス・アプリケーションが含まれています。
- iSeries B は、本社オフィスの VPN 接続のゲートウェイとして機能します。
- iSeries B は、グローバルに経路指定が可能な IP アドレス 172.16.1.3 を持っています。

  重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。

- サブネット・マスクは 255.255.255.0 です。
- iSeries B は、IP アドレス 10.2.1.1 でそのサブネットに接続します。
- 本社オフィスの内部ネットワークでは、すべての PC が、iSeries B をポイントするデフォルトの経路で構成されています。
- iSeries B の完全修飾ホスト名は iseriesb.myco.wis.com です。

外勤の営業スタッフ

- Microsoft® Windows XP オペレーティング・システムを搭載したラップトップ。
- 外勤の従業員は、範囲が 10.1.1.100 から 10.1.1.150 の IP アドレスのプールを使用します。

前提条件および前提事項

このシナリオでは、営業所と本社オフィスの間の VPN 構成例を示します。また、外出中の営業スタッフが営業所に接続するための、リモート・アクセスの構成方法も示します。このシナリオは、いくつかの前提条件のステップがすでに完了してテスト済みであり、これらの構成のステップを始める前に運用可能になっていることを前提としています。このシナリオでは、以下の前提条件が満たされていることを前提としています。

1. 以下のライセンス・プログラムが確実にインストールされていること。
   - OS/400 バージョン 5 リリース 2 (5722-SS1)
   - ディジタル証明書マネージャー (5722-SS1 オプション 34)

     注: このシナリオでは、両方のシステムに DCM がインストール済みであるものの、いずれのシステムでも構成されていないと想定しています。
   - TCP/IP Connectivity Utilities for i5/OS (5722-TC1)
   - IBM HTTP Server for iSeries (5722-DG1)
   - IBM eServer iSeries Access for Windows (5722-XE1) および iSeries Navigator
   - IBM Developer Kit for Java™ (5722-JV1)
   - システムに最新の PTF が確実にインストールされている。
2. 以下のサーバー・セットアップが完了済みであること。
   - TCP/IP は、IP インターフェース、経路、ローカル・ホスト名、およびローカル・ドメイン・ネームを含めて、構成済みである必要がある。
   - 基本的なシステム・セキュリティーが構成済みで、テスト済みである。
   - iSeries ナビゲーターのネットワーク・コンポーネントがインストール済みである。
   - サーバー・セキュリティー・データの保存 (QRETSVRSEC *SEC) のシステム値が、1 に設定されている。
   - 共用メモリー (QSHRMEMCTL) のシステム値が 1 に設定されている。
   - 必要なエンドポイント間で通常の TCP/IP 通信が確立されている。
3. 外勤の従業員が使用する PC で以下の要件が満たされていること。
   - Windows 32 ビットオペレーティング・システムを搭載した Windows XP クライアントが、iSeries サーバーに適切に接続され、TCP/IP 用に構成されている。
   - 233 Mhz のプロセッサー。
   - Windows XP クライアントには 64 MB の RAM が搭載されている必要がある。
   - iSeries Access for Windows および iSeries ナビゲーターがクライアント PC にインストールされている。

- ソフトウェアは、IP セキュリティー (IPSec) プロトコルをサポートする必要がある。
- ソフトウェアは、レイヤー 2 トンネリング・プロトコル (L2TP) をサポートする必要がある。
- ISP への接続が確立されている。

上記の前提条件に加え、両方のネットワークで、それぞれのネットワーク上でのフィルター・ルールのセットアップと活動化、経路指定の構成、および IP アドレッシング体系の設定が済んでいることを前提とします。これらのタスクが完了していない場合は、『IP フィルター処理およびネットワーク・アドレス変換 (NAT)、および TCP/IP 経路指定およびワークロード・バランシング』のトピックを参照してください。

ヒント: このシナリオは、インターネットに直接接続されている iSeries セキュリティー・ゲートウェイを示します。ファイアウォールを使用していないのは、シナリオを単純化するためです。ファイアウォールを使用する必要がないことを意味しているわけではありません。実際には、インターネットに接続する場合に常に生じるセキュリティー上のリスクを考慮する必要があります。セキュリティー・リスクを減らすためのさまざまな方法の詳細については、 AS/400® インターネット・セキュリティー・シナリオ: 実践的アプローチ (AS/400 Internet Security Scenarios: A Practical Approach)


を参照してください。

関連資料

IP フィルター操作およびネットワーク・アドレス変換 (NAT)

TCP/IP 経路指定およびワークロード・バランシング

AS/400 インターネット・セキュリティー・シナリオ: 実践的アプローチ (AS/400 Internet Security Scenarios: A Practical Approach) SG24-5954-00

DCM シナリオ

VPN シナリオ

PPP シナリオ

ディジタル証明書マネージャーを使用して認証局をセットアップする

認証局 (CA) をセットアップする前に、営業所の管理者は、いくつかの計画タスクが完了済みであることを確認する必要がありました。以下のタスクを実行する前に、このシナリオのすべての前提条件が満たされていることを確認してください。

ディジタル証明書マネージャーの計画ワークシートを作成する

綿密な計画を立てた後、MyCo, Inc は、ビジネス・パートナーに発行するディジタル証明書をセットアップするのに役立つ、以下の計画ワークシートを作成します。

表 6. ディジタル証明書マネージャー (DCM) を使った認証局 (CA) の作成のための計画ワークシート

質問	回答
証明書の公開鍵と秘密鍵の生成に使用する予定の鍵のサイズは ?	1024
証明書ストアのパスワードは何ですか ?	secret **重要:** このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。

表 6. ディジタル証明書マネージャー (DCM) を使った認証局 (CA) の作成のための計画ワークシート (続き)

質問	回答
認証局の名前は何ですか ?	mycoca
あなたの組織の名前は何ですか ?	myco
認証局を有効とする期間は、何日間ですか ?	1095 (3 年)
ご使用のブラウザーは何ですか ?	Windows Internet Explorer バージョン 6.0
ネットワーク上のユーザーに証明書を発行しますか ?	いいえ

表 7. iSeries A のサーバー証明書の計画ワークシート

質問	回答
証明書の公開鍵と秘密鍵の生成に使用する予定の鍵のサイズは ?	1024
証明書ストアのパスワードは何ですか ?	secret **重要:** このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。
証明書ラベルの名前は何ですか ?	mycocert
証明書の共通名は何ですか ?	mycocert
あなたの組織の名前は何ですか ?	MyCo, Inc
iSeries サーバーの IP アドレスは何ですか ?	192.168.1.2 **重要:** このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
iSeries サーバーの完全修飾ホスト名は何ですか ?	iseriesa.myco.min.com

表 8. iSeries B のサーバー証明書の計画ワークシート

質問	回答
証明書の公開鍵と秘密鍵の生成に使用する予定の鍵のサイズは ?	1024
証明書ラベルの名前は何ですか ?	corporatecert
証明書の共通名は何ですか ?	corporatecert
証明書ストアのパスとファイル名は何ですか ?	/tmp/iseriesb.kdb

表 8. iSeries B のサーバー証明書の計画ワークシート (続き)

質問	回答
証明書ストアのパスワードは何ですか ?	secret2 **重要:** このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。
サーバー証明書の共通名は何ですか ?	corporatecert
この証明書を所有する組織の名前は何ですか ?	MyCo, Inc
iSeries サーバーの IP アドレスは何ですか ?	172.16.1.3 **重要:** このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
iSeries サーバーの完全修飾ホスト名は何ですか ?	iseriesb.myco.wis.com

iSeries A 上で IBM HTTP Server for iSeries を始動する

ディジタル証明書マネージャー (DCM) インターフェースにアクセスするには、以下のタスクを実行することによって、HTTP Server の管理インスタンスを開始する必要があります。

1. iSeries A から、文字ベース・インターフェースにサインオンする。
2. コマンド・プロンプトで、`strtcpsvr server(*HTTP) httpsvr(*admin)` と入力する。これにより HTTP Server の管理サーバーが始動します。

iSeries A を認証局として構成する

1. Web ブラウザーで、`http://iseriesa:2001` と入力する。これにより、ディジタル証明書マネージャー (DCM) インターフェースにアクセスするための「iSeries タスク・ページ (iSeries Task Page)」が起動します。
2. ご使用の iSeries A ユーザー・プロファイル名およびパスワードを使ってログオンする。
3. 「**ディジタル証明書マネージャー**」をクリックする。
4. 左側のナビゲーション区画から、「**認証局 (CA) の作成 (Create a Certificate Authority (CA))**」を選択する。
5. 「認証局 (CA) の作成 (Create a Certificate Authority (CA))」ページの以下の必須フィールドに、DCM 計画ワークシートの情報を入力する。
   - **鍵のサイズ:** 1024
   - **証明書ストアのパスワード:** secret
   - **確認パスワード:** secret

重要: このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。

- **認証局の名前:** mycoca
- **組織名:** MyCo, Inc
- **都道府県:** min
- **国または地域:** us
- **認証局の有効期間 (2 から 7300):** 1095

6. 「**継続**」をクリックする。
7. 「**ローカル CA 証明書のインストール (Install Local CA certificate)**」ページで、「**続行**」をクリックする。
8. 「**認証局 (CA) のポリシー・データ (Certificate Authority (CA) Policy Data)**」ページで、以下のオプションを選択する。
   - **ユーザー証明書の作成を許可する (Allow creation of user certificates):** はい
   - **この認証局が発行する証明書の有効期間 (1 から 2000) (Validity period of certificates that are issued by this Certificate Authority (1-2000)):** 365
9. 「受け入れ済みポリシー・データ (Policy Data Accepted)」ページで、表示されるメッセージを読み、「**続行**」をクリックして、デフォルトのサーバー証明書ストア (*SYSTEM) と、認証局 (CA) によって署名されたサーバー証明書を作成する。確認メッセージを読み、「**続行**」をクリックします。
10. 「サーバーまたはクライアント証明書の作成 (Create a Server or Client Certificate)」ページで、以下の情報を入力する。
    - **鍵のサイズ:** 1024
    - **証明書ラベル:** mycocert
    - **証明書ストアのパスワード:** secret
    - **確認パスワード:** secret

      重要: このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。
    - **共通名:** mycocert
    - **組織名:** myco
    - **都道府県:** min
    - **国または地域:** us
    - **IP バージョン 4 アドレス:** 192.168.1.2

      注: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
    - **完全修飾ドメイン・ネーム:** iseriesa.myco.min.com
    - **E メール・アドレス:** adminstrator@myco.min.com
11. 「**継続**」をクリックする。
12. 「アプリケーションの選択 (Select Application)」ページで、「**続行**」をクリックする。

ヒント: 「VPN 新規接続」ウィザードにより、今作成した証明書が自動的に i5/OS VPN Key Manager アプリケーションに割り当てられてます。この証明書を使用するその他のアプリケーションが

ある場合は、そのアプリケーションをこのページで選択することができます。このシナリオでは VPN 接続でしかこの証明書を使用しないため、その他のアプリケーションを選択する必要はありません。

13. 「アプリケーションの状況 (Application Status)」ページで、表示されるメッセージを読み、「**キャンセル (Cancel)**」をクリックする。これにより、作成した変更内容が受け入れられます。

    注: 証明書ストアを作成して、オブジェクトの署名に使用する証明書を含める場合は、「**続行**」をクリックする。

14. DCM インターフェースが最新表示されたら、「**証明書ストアの選択 (Select a Certificate Store)**」を選択する。
15. 「証明書ストアの選択 (Select a Certificate Store)」ページで ***SYSTEM** を選択する。「**継続**」をクリックします。
16. 「証明書ストアおよびパスワード (Certificate Store and Password)」ページで `secret` と入力する。「**継続**」をクリックします。
17. 左側のナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択する。
18. 「アプリケーションの管理 (Manage Applications)」ページで「**CA トラスト・リストの定義 (Define CA trust list)**」を選択する。「**継続**」をクリックします。
19. 「CA トラスト・リストの定義 (Define CA Trust List)」ページで「**サーバー**」を選択する。「**継続**」をクリックします。
20. 「**i5/OS VPN Key Manager**」を選択する。「**CA トラスト・リストの定義 (Define CA Trust List)**」をクリックします。
21. 「CA トラスト・リストの定義 (Define CA Trust List)」ページで「**LOCAL_CERTIFICATE_AUTHORITY**」を選択する。「**OK**」をクリックします。

iSeries B のサーバー証明書を作成する

1. 左側のナビゲーション区画で、「**証明書の作成 (Create Certificate)**」をクリックし、「**別の iSeries 用のサーバーまたはクライアント証明書 (Server or client certificate for another iSeries)**」を選択する。
2. 「**継続**」をクリックする。
3. 「別の iSeries 用のサーバーまたはクライアント証明書の作成 (Create Server or Client Certificate for another iSeries)」ページで「**V5R2**」を選択する。これは iSeries B のリリースのレベルです。「**続行**」をクリックします。
4. 「サーバーまたはクライアント証明書の作成 (Create a Server or Client Certificate)」ページで、以下の情報を入力する。
   - **鍵のサイズ:** 1024
   - **証明書ラベル:** corporatecert
   - **証明書ストアのパスとファイル名:**/tmp/iseriesb.kdb
   - **証明書ストアのパスワード:** secret2
   - **確認パスワード:** secret2

     注: このシナリオで使用されるすべてのパスワードは、例示のみを目的としています。実際の構成では、これらのパスワードは使用しないでください。

   - **共通名:** corporatecert
   - **組織名:** MyCo, Inc

- **都道府県:** wis
- **国または地域:** us
- **IP バージョン 4 アドレス:** 172.16.1.3

  重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
- **完全修飾ホスト名:** iseriesb.myco.wis.com
- **E メール・アドレス:** adminstrator@myco.wis.com

5. 「**継続**」をクリックする。iSeries A で iSeries B 用のサーバー証明書が 作成されたことを確認するメッセージが表示されます。営業所のネットワークの管理者は、これらのファイルを、暗号化した E メールを使用して本社オフィスの管理者に送信します。本社オフィスの管理者は、この時点で証明書ストア (.KDB) ファイルと要求 (.RDB) ファイルを iSeries B に移動して、名前変更する必要があります。本社オフィスの管理者はこれらのファイルを、バイナリー FTP を使用して統合ファイル・システム (IFS) 内の /QIBM/USERDATA/ICSS/CERT/SERVER ディレクトリーに移動する必要があります。これが完了した後、管理者は、該当のディレクトリーにあるこれらのファイルを名前変更する必要があります。

iSeries B 上の .KDB および .RDB ファイルの名前を変更する

*SYSTEM 証明書ストアは iSeries B には存在しないため、本社ネットワークの管理者は、iseriesb.kdb および iseriesb.RDB ファイルを DEFAULT.KDB および DEFAULT.RDB に名前変更する必要があります。このようにすることにより、これらの転送されたファイルは、iSeries B で *SYSTEM 証明書ストアとして使用されます。

1. iSeries ナビゲーターで、「**iSeries B**」 → 「**ファイル・システム**」 → 「**統合ファイル・システム**」 → 「**Qibm**」 → 「**UserData**」 → 「**ICSS**」 → 「**Cert**」 → 「**Server**」を展開し、ファイル iseriesb.kdb および iseriesb.RDB がこのディレクトリーにリストされていることを確認する。
2. コマンド行で `wrklnk ('/qibm/userdata/icss/cert/server')` と入力する。
3. 「オブジェクト・リンクの処理」画面で、7 を選択して iseriesb.kdb ファイルを名前変更する。Enter を押します。
4. 「オブジェクト名変更」画面で、「**新しいオブジェクト**」フィールドに `DEFAULT.KDB` と入力する。Enter を押します。
5. ステップ 3 とステップ 4 を繰り返して、iseriesb.RDB ファイルを DEFAULT.RDB に名前変更する。
6. iSeries ナビゲーターを最新表示し、「**iSeries B**」 → 「**ファイル・システム**」 → 「**統合ファイル・システム**」 → 「**Qibm**」 → 「**UserData**」 → 「**ICSS**」 → 「**Cert**」 → 「**Server**」を展開して、これらのファイルが変更されていることを確認する。 DEFAULT.KDB ファイルと DEFAULT.RDB ファイルがディレクトリー内にリストされている必要があります。

iSeries B 上の証明書ストアのパスワードを変更する

この時点で本社オフィスのネットワーク管理者は、DEFAULT.KDB および DEFAULT.RDB ファイルが作成されたときに作成された、新しい *SYSTEM 証明書ストアのパスワードを変更する必要があります。

注: *SYSTEM 証明書ストアのパスワードを変更する必要があります。パスワードを変更すると、そのパスワードは、アプリケーションが自動的にそれを回復し、証明書ストアを開いて証明書にアクセスできるように、隠されます。

1. ブラウザーで、http://iseriesb:2001 と入力する。「**証明書ストアの選択 (Select a Certificate Store)**」をクリックします。
2. 「***SYSTEM 証明書ストア (*SYSTEM Certificate Store)**」を選択し、パスワードとして secret2 と入力する。これは、営業所の管理者が iSeries B のサーバー証明書を作成したときに指定したパスワードです。「**継続**」をクリックします。
3. 左側のナビゲーション・フレームで「**証明書ストアの管理 (Manage Certificate Store)**」を選択し、「**パスワードの変更 (Change Password)**」を選択して「**続行**」をクリックする。
4. 「証明書ストアのパスワードの変更 (Change Certificate Store Password)」ページで、「**新規パスワード (New password)**」および「**パスワードの確認 (Confirm password)**」フィールドに coporatepwd と入力する。
5. 有効期限ポリシーとして「**パスワードは失効しない (Password does not expire)**」を選択する。「**継続**」をクリックします。確認ページが表示されます。「**OK**」をクリックします。
6. 「証明書ストアのパスワードの変更 (Change Certificate Store Password)」確認ページで、表示されるメッセージを読み、「**OK**」をクリックする。
7. 再ロードされた「証明書ストアおよびパスワード (Certificate Store and Password)」ページで、「**証明書ストア・パスワード (Certificate Store Password)**」フィールドに coporatepwd と入力する。「**継続**」をクリックします。

iSeries B 上の i5/OS VPN Key Manager の CA トラストを定義する

1. 左側のナビゲーション・フレームで、「**アプリケーションの管理 (Manage Applications)**」を選択する。
2. 「アプリケーションの管理 (Manage Applications)」ページで「**CA トラスト・リストの定義 (Define CA trust list)**」を選択する。「**継続**」をクリックします。
3. 「CA トラスト・リストの定義 (Define CA Trust List)」ページで「**サーバー**」を選択する。「**継続**」をクリックします。
4. 「**i5/OS VPN Key Manager**」を選択する。「**CA トラスト・リストの定義 (Define CA Trust List)**」をクリックします。
5. 「CA トラスト・リストの定義 (Define CA Trust List)」ページで「**LOCAL_CERTIFICATE_AUTHORITY**」を選択する。「**OK**」をクリックします。

これで、営業所と本社オフィスの管理者が VPN の構成を開始することができます。

営業所と本社オフィスの間の VPN 接続を構成する

以下のステップは、営業所の管理者が VPN 接続を構成する方法を示しています。

営業所と外勤の営業スタッフの間の VPN 接続の計画ワークシートを作成する

営業所の管理者は、VPN 計画アドバイザーを使用して動的な計画ワークシートを作成し、それを営業所と本社オフィスの間の VPN の構成に役立てました。 VPN 計画アドバイザーは、VPN のニーズについての特定の質問を行う、対話式ツールです。このツールは、ユーザーの回答に基づいて、VPN 接続を構成するときに使用できる、ユーザーの環境に合わせてカスタマイズされた計画ワークシートを生成します。
iSeries サーバー上で VPN を構成するときには、このワークシートを使用することができます。以下の各計画ワークシートは、VPN 計画アドバイザーによって生成されたもので、 iSeries ナビゲーターで「VPN 新規接続」ウィザードを使って VPN を構成するときに使用します。

表 9. 営業所と本社オフィスの間の VPN 接続の計画ワークシート

VPN ウィザードの質問内容	**VPN アドバイザーの推奨事項**
この接続グループの名前は ?	SalestoCorporate
作成する接続グループのタイプは ?	「**自分のゲートウェイを別のゲートウェイに接続**」を選択する
鍵の保護に使用したい Internet Key Exchange ポリシーは ?	「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンスは低い**」を選択する
証明書を使用しますか ? (Are you using certificates?)	「**はい**」を選択し、証明書として mycocert を選択する。**注:** この証明書は、iSeries A を認証局として構成するステップにおいて作成したものです。
ローカル接続エンドポイントを表す ID を選択してください。	選択した証明書に定義されている ID のタイプと ID のリストから、ID のタイプとして **IP バージョン 4 アドレス**、ID として **192.168.1.2** を選択する。**注:** このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
接続先のキー・サーバーの ID は ?	ID のタイプとして **IP バージョン 4 アドレス**、ID として **172.16.1.3** を選択する。**重要:** このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
この接続で保護されるデータのローカル・エンドポイントは ?	**ID のタイプ:** IP バージョン 4 サブネット **ID:** 10.1.1.0 **マスク:** 255.255.255.0

表 9. 営業所と本社オフィスの間の VPN 接続の計画ワークシート (続き)

VPN ウィザードの質問内容	VPN アドバイザーの推奨事項
この接続で保護されるデータのリモート・エンドポイントは ?	**ID のタイプ:** IP バージョン 4 サブネット **ID:** 10.2.1.0**マスク :** 255.255.255.0
この接続で保護されるデータのポートおよびプロトコルは ?	**ローカル・ポート:** 任意のポート**リモート・ポート**: 任意のポート**プロトコル:** 任意のプロトコル
データの保護に使用したいデータ・ポリシーは ?	「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンス は低い**」を選択する
この接続が適用されるローカル・システム上のインターフェースをチェックしてください。	• ETHLINE (営業所) • ELINE (本社オフィス)

関連資料

VPN 計画アドバイザー

iSeries A 上で VPN を構成する

VPN 接続の計画が完了したら、iSeries A を、VPN を使用して 2 つのネットワーク間でデータをセキュア送信するように構成することができます。

ヒント: 「VPN 新規接続」ウィザードを実行するときにすでに VPN サーバーが始動している場合、このウィザードは、先程作成した証明書ストアまたは証明書を自動的には検出しません。VPN サーバーが実行中の場合は、「VPN 新規接続」ウィザードを実行する前に、iSeries ナビゲーターで VPN サーバーを再始動する必要があります。

重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。

MyCo, Inc の管理者は、iSeries A での VPN の構成に、VPN 計画アドバイザーによって生成された計画ワークシートを使用しました。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」と展開する。
2. 「**仮想プライベート・ネットワーク**」を右マウス・ボタン・クリックし、「**新規接続**」を選択して「接続」ウィザードを開始する。このウィザードによって作成されるオブジェクトに関する情報については、「ウェルカム」ページをお読みください。
3. 「接続名」ページで、「**名前**」フィールドに `SalestoCorporate` と入力する。 オプションで、この接続グループの記述を指定します。「**次へ**」をクリックします。
4. 「接続シナリオ」ページで「**自分のゲートウェイを別のゲートウェイへに接続**」を選択する。「**次へ**」をクリックします。
5. 「Internet Key Exchange ポリシー」ページで、「**新規ポリシーの作成**」を選択してから、「**最高のセキュリティー、最低のパフォーマンス (Highest security, lowest performance)**」を選択する。「**次へ**」をクリックします。

6. 「ローカル接続エンドポイント用の証明書 (Certificate for Local Connection Endpoint)」ページで「**はい**」を選択し、証明書のリストから「**mycocert**」を選択する。「**次へ**」をクリックします。
7. 「ローカル接続エンドポイント ID (Local Connection Endpoint Identifier)」ページで、ID のタイプとして「**バージョン 4 IP アドレス (Version 4 IP address)**」を選択する。 関連する IP アドレスは 192.168.1.2 にしてください。この情報は DCM で作成する証明書に定義されています。「**次へ**」を 2 回クリックします。
8. 「リモート・キー・サーバー (Remote Key Server)」ページの「**ID のタイプ**」フィールドで「**バージョン 4 IP アドレス (Version 4 IP address)**」 を選択します。「**ID**」フィールドに 172.16.1.3 と入力します。これは、本社オフィスのネットワーク内の iSeries B の IP アドレスです。「**次へ**」をクリックします。
9. 「ローカル・データ・エンドポイント」ページで、 ID のタイプとして「**IP バージョン 4 サブネット**」を選択し、 ID として 10.1.1.0、マスクとして 255.255.255.0 と入力する。
10. 「リモート・データ・エンドポイント」ページで、 ID のタイプとして「**IP バージョン 4 サブネット**」を選択し、 ID として 10.2.1.0、マスクとして 255.255.255.0 と入力する。
11. 「データ・サービス」ページで、ローカル・ポートに「**任意のポート**」、リモート・ポートに「**任意のポート**」、およびプロトコルに「**任意のプロトコル**」を選択する。「**次へ**」をクリックします。
12. 「データ・ポリシー」ページで、「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンスは低い**」を選択する。「**次へ**」をクリックします。
13. 「適用できるインターフェース」ページで「**ETHLINE**」を選択して、「**次へ**」をクリックします。
14. 「要約」ページで、このウィザードによって作成されるオブジェクトを見直して、それらが正しいことを確認する。
15. 「**完了**」をクリックして、構成を完了する。「ポリシー・フィルターの活動化 」ダイアログ・ボックスが表示されたら、「**いいえ、パケット・ルールは後で活動化します**」を選択して、「**OK**」をクリックします。

iSeries B 上で VPN を構成する

本社オフィスの管理者は、必要に応じて IP アドレスを変えながら、iSeries A を構成したときに営業所の管理者が使用したステップと同じステップに従いました。作業の手引きとして計画ワークシートを使用してください。

この管理者が iSeries B の構成を終えた後、両方の管理者が両方のサーバーのフィルター・ルールを活動化することができます。

両方のサーバー上でフィルター・ルールを活動化する

このウィザードは、この接続が適切に機能するために必要なパケット・ルールを、自動的に作成します。ただし、VPN 接続を開始するためには、パケット・ルールを両方のシステムで活動化する必要があります。iSeries A でこれを行うには、以下の手順に従ってください。

注: フィルター・ルールを活動化した後で iSeries への接続を失った場合は、サーバー上で現在アクティブなフィルター・ルールを、すべて削除する必要があります。これを行うには、文字ベース・インターフェースから RMVTCPTBL (*ALL) コマンドを使用します。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右マウス・ボタン・クリックし、「**ルールの活動化**」を選択する。

3. 「パケット・ルールの活動化」ページで、「**VPN 生成ルールのみ活動化**」を選択し、これらのフィルター・ルールを活動化させる対象のインターフェースとして「**ETHLINE**」を選択する。「**OK**」をクリックします。
4. iSeries B でパケット・ルールを活動化するには、インターフェースとして ETHLINE ではなく ELINE を使用して、上記のステップを繰り返す。

VPN 接続の開始

SalestoCorporate 接続を iSeries A から開始するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」を展開する。
2. 「**仮想プライベート・ネットワーク**」を右マウス・ボタン・クリックしてから、「**開始**」を選択する。これで VPN サーバーが始動します。
3. 「**仮想プライベート・ネットワーク**」 → 「**セキュア接続**」を展開する。「**すべての接続**」をクリックして、右のペインに接続のリストを表示します。「**SalestoCorporate**」を右クリックしてから、「**開始**」を選択する。
4. 「**表示**」メニューから「**最新表示**」を選択する。接続が正常に開始された場合、状況が「アイドル」から「使用可能」に変わります。接続は開始するまで数分かかることがあるため、状況が「使用可能」に変わるまで、定期的に「**最新表示**」をクリックしてください。
5. iSeries B でこれらのステップを繰り返す。

エンドポイント間の VPN 接続をテストする

両方のサーバーの構成が終わり、接続が正常に開始されたら、接続性をテストして、リモート・ホストが相互に通信できることを確認する必要があります。

ヒント: 宛先がリモート・ネットワークのトラフィックについては、ローカル・クライアントに適切な経路が構成されていることを確認してください。

営業所内の Windows XP ワークステーションで、ネットワーク管理者は以下のステップを実行する必要があります。

1. コマンド・プロンプトから `ping 10.2.1.3` と入力する。これは、本社オフィスのネットワーク内のワークステーションのうちの 1 台の IP アドレスです。

   重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
2. これらのステップを繰り返し、今度は本社オフィスから営業所への接続性をテストする。

リモート・ユーザーへの VPN 接続を構成する

以下のタスクは、営業所の管理者が、外勤のスタッフへの VPN 接続を構成する方法を示しています。

営業所と外勤の営業スタッフの間の VPN 接続の計画ワークシートを作成する

営業所の管理者は、VPN 計画アドバイザーを使用して動的な計画ワークシートを作成し、それをサーバーおよびリモート・ワークステーションでの VPN の構成に役立てました。 VPN 計画アドバイザーは、VPN のニーズについての特定の質問を行う、対話式ツールです。このツールは、ユーザーの回答に基づいて、VPN 接続を構成するときに使用できる、ユーザーの環境に合わせてカスタマイズされた計画ワークシートを生成します。 iSeries サーバー上で VPN を構成するときには、このワークシートを使用することができ

ます。以下の各計画ワークシートは、VPN 計画アドバイザーによって生成されたもので、 iSeries ナビゲーターで「VPN 新規接続」ウィザードを使って VPN を構成するときに使用します。

表 10. 営業所と外勤の営業スタッフの間の VPN 接続の計画ワークシート

VPN ウィザードの質問内容	**VPN アドバイザーの推奨事項**
この接続グループの名前は ?	SalestoRemote
作成する接続グループのタイプは ?	「**自分のホストを別のホストに接続**」を選択する
鍵の保護に使用したい Internet Key Exchange ポリシーは ?	「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンスは低い**」を選択する
証明書を使用しますか ? (Are you using certificates?)	「**いいえ**」を選択する
この接続のローカル・キー・サーバーを表す ID を入力してください。	ID のタイプ: **IP バージョン 4 アドレス** IP アドレス :**192.168.1.2** **重要:** このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
接続先のキー・サーバーの ID は ?	ID のタイプ: **任意の IP アドレス 事前共有キー**: mycokey **注:** 事前共有キーは、i5/OS VPN が、接続の認証およびデータを保護する鍵の設定に使用する、32 文字のテキスト・ストリングです。通常、事前共有キーはパスワードと同様に扱います。
この接続で保護されるデータのポートおよびプロトコルは ?	**ローカル・ポート**: 1701 **リモート・ポート**: 任意のポート **プロトコル**: UDP
データの保護に使用したいデータ・ポリシーは ?	「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンスは低い**」を選択する
この接続が適用されるローカル・システム上のインターフェースをチェックしてください。	ETHLINE (営業所)

関連資料

VPN 計画アドバイザー

iSeries A の L2TP ターミネーター・プロファイルを構成する

リモート・ワークステーションへのリモート接続を構成します。これらのクライアントからインバウンド接続を受け入れるように、iSeries A をセットアップする必要があります。 iSeries A の L2TP ターミネーター・プロファイルを構成するには、以下のステップを実行してください。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**リモート・アクセス・サービス**」を展開する。
2. 「**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 A を、リモート・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、「**新規プロファイル**」を選択する。
3. 「**新規 Point-to-Point 接続プロファイルのセットアップ**」
   - **プロトコル・タイプ:** PPP
   - **接続タイプ:** L2TP (仮想回線)

     注: 「作動モード」フィールドに自動的に、「**ターミネーター (ネットワーク・サーバー)**」と表示されます。
   - **回線サービスのタイプ:** 単一回線
4. 「**OK**」をクリックする。これにより、「新規 Point-to-Point プロファイルのプロパティー」ページが立ち上がります。
5. 「新規 Point-to-Point プロファイルのプロパティー」ページで、「**名前**」フィールドに MYCOL2TP と入力する。「**OK**」をクリックします。
6. 「接続」タブで、「**ローカル・トンネル・エンドポイント IP アドレス**」に「**192.168.1.2**」を選択する。

   重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。
7. 「**仮想回線名**」に「**MYCOL2TP**」を選択する。「**OK**」をクリックします。これにより、「新規 L2TP 回線のプロパティー」ページが立ち上がります。
8. 「認証」ページで、ホスト名に「iseriesa」と入力する。「**OK**」をクリックします。これにより「接続」ページに戻ります。
9. 「接続」ページで以下のオプションを選択し、「**最大接続数**」に 25 と入力する。
10. 「認証」タブで、「**この iSeries サーバーはリモート・システムの ID を検索することが必要です。**」を選択する。
11. 「**妥当性検査リストを使用してローカル側で認証**」を選択する。
12. 「妥当性検査リスト名」フィールドに QL2TP と入力し、「**新規**」をクリックする。
13. 「妥当性検査リスト」ページで「**追加**」を選択する。
14. 各外勤の従業員について、ユーザー名とパスワードを追加する。「**OK**」をクリックします。
15. 「パスワードの確認」ページで、外勤の各従業員ごとにパスワードを再入力する。「**OK**」をクリックします。
16. 「TCP/IP 設定」ページで、「**ローカル IP アドレス**」に「10.1.1.1」を選択する。
17. 「**IP アドレス割り当て方式**」フィールドで「**アドレス・プール**」を選択する。
18. 「**開始 IP アドレス**」フィールドに 10.1.1.100 と入力し、「**アドレスの数 (Number of addresses)**」に対して 49 と入力する。

19. 「**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**」を選択する。「**OK**」をクリックします。

受信側接続プロファイルを開始する

iSeries A の L2TP 受信側接続プロファイルを構成した後、管理者は、リモート・クライアントからの着信要求を listen させるため、この接続を開始する必要があります。

注: QUSRWRK サブシステムが開始されていませんというエラー・メッセージを受け取る場合があります。このメッセージは、受信側接続プロファイルを開始するときに発生します。QUSRWRK サブシステムを開始するには、以下のステップを実行してください。

1. 文字ベース・インターフェースで `strsbs` と入力する。
2. 「サブシステム開始」画面で、「**サブシステム記述**」フィールドに `QUSRWRK` と入力する。

リモート・クライアント用の VPN を構成するには、以下のタスクを実行してください。

1. iSeries ナビゲーターで、「**表示**」メニューから「**最新表示**」を選択する。これにより、iSeries ナビゲーターのインスタンスが最新表示されます。
2. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**リモート・アクセス・サービス**」を展開する。
3. 「**受信側接続プロファイル**」をダブルクリックし、「**MYCOL2TP**」を右マウス・ボタン・クリックして「**開始**」を選択する。
4. 「**状況**」フィールドに「**接続要求を待機中 (Waiting for connection requests)**」と表示される。

iSeries A 上でリモート・クライアント用の VPN 接続を構成する

iSeries A の L2TP 受信側接続プロファイルを構成して開始した後、管理者は、リモート・クライアントと営業所のネットワークとの間の接続を保護するように VPN を構成する必要があります。

リモート・クライアント用の VPN を構成するには、以下のステップを実行してください。

重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」と展開する。
2. 「**仮想プライベート・ネットワーク**」を右マウス・ボタン・クリックし、「**新規接続**」を選択して「VPN 新規接続」ウィザードを開始する。このウィザードによって作成されるオブジェクトに関する情報については、「ウェルカム」ページをお読みください。
3. 「**次へ**」をクリックして、「接続名」ページに進む。
4. 「**名前**」フィールドで `SalestoRemote` と入力する。
5. **任意:** この接続グループの記述を指定します。「**次へ**」をクリックします。
6. 「接続のシナリオ」ページで「**自分のホストを別のホストに接続**」を選択する。「**次へ**」をクリックする。
7. 「Internet Key Exchange ポリシー」ページで、「**新規ポリシーの作成**」を選択してから、「**最高のセキュリティー、最低のパフォーマンス (Highest security, lowest performance)**」を選択する。「**次へ**」をクリックします。
8. 「ローカル接続エンドポイント用の証明書 (Certificate for Local Connection Endpoint)」ページで「**いいえ**」を選択する。「**次へ**」をクリックします。

9. 「ローカル鍵サーバー (Local Key Server)」ページで、ID のタイプとして「**バージョン 4 IP アドレス (Version 4 IP address)**」を選択する。関連する IP アドレスは 192.168.1.2 にしてください。「**次へ**」をクリックします。
10. 「リモート鍵サーバー (Remote Key Server)」ページの、「ID のタイプ」フィールドで「**任意の IP アドレス**」を選択する。「**事前共有キー (Pre-shared key)**」フィールドで mycokey と入力します。「**次へ**」をクリックします。
11. 「データ・サービス」ページで、ローカル・ポートに 1701 と入力し、リモート・ポートに 1701、およびプロトコルに UDP を選択する。「**次へ**」をクリックします。
12. 「データ・ポリシー」ページで、「**新規ポリシーの作成**」を選択してから、「**セキュリティーは高く、パフォーマンスは低い**」を選択する。「**次へ**」をクリックします。
13. 「適用できるインターフェース」ページで「**ETHLINE**」を選択して、「**次へ**」をクリックします。
14. 「要約」ページで、このウィザードによって作成されるオブジェクトを見直して、それらが正しいことを確認する。
15. 「**完了**」をクリックして、構成を完了する。「ポリシー・フィルターの活動化」ダイアログ・ボックスが表示されたら、「**いいえ、パケット・ルールは後で活動化します**」を選択します。「**OK**」をクリックします。

Windows XP クライアントからのリモート接続用の VPN ポリシーを更新する

このウィザードは、ほとんどの VPN 構成に使用できる標準的な接続を作成するため、Windows XP クライアントとの相互運用性を確保するためには、ウィザードによって生成されたポリシーを更新する必要があります。これらの VPN ポリシーを更新するには、以下のタスクを実行してください。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」 → 「**仮想プライベート・ネットワーク**」 → 「**IP セキュリティー・ポリシー**」と展開する。
2. 「**Internet Key Exchange ポリシー**」をダブルクリックし、「**任意の IP アドレス**」を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
3. 「変形」ページで「**追加**」をクリックする。
4. 「Internet Key Exchange ポリシー変形」ページで、以下のオプションを選択する。
   - **認証方式:** 事前共有キー
   - **ハッシュ・アルゴリズム:** MD5
   - **暗号化アルゴリズム:** DES-CBC
5. 「**OK**」をクリックする。
6. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」 → 「**仮想プライベート・ネットワーク**」 → 「**IP セキュリティー・ポリシー**」と展開する。
7. 「**データ・ポリシー**」をダブルクリックし、「**SalestoRemote**」を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
8. 「一般」ページで、「**Diffie-Hellman Perfect Forward Secrecy を使用**」を選択解除する。
9. 「提案」ページで「**追加**」をクリックする。
10. 「新規データ・ポリシー提案」ページで、以下のオプションを選択する。
    - **カプセル化モード:** トランスポート
    - **鍵の有効期限:** 15 分
    - **満了限界サイズ:** 100000
11. 「変形」ページで「**追加**」をクリックする。

12. 「データ・ポリシー変形」ページで、以下のオプションを選択する。
    - **プロトコル:** カプセル化セキュリティー・ペイロード (ESP)
    - **認証アルゴリズム:** MD5
    - **暗号化アルゴリズム:** DES-CBC
13. 「**OK**」をクリックする。

フィルター・ルールを活動化する

このウィザードは、この接続が適切に機能するために必要なパケット・ルールを、自動的に作成します。ただし、VPN 接続を開始するためには、パケット・ルールを両方のシステムで活動化する必要があります。

iSeries A のフィルター・ルールを活動化するには、以下の手順に従ってください。

重要: このシナリオで使用される IP アドレスは、例示のみを目的としています。これらのアドレスは IP アドレッシング体系を反映していないため、実際の構成では使用しないでください。これらのタスクを実行するときには、実際に使用する IP アドレスを使用してください。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」 → 「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右マウス・ボタン・クリックし、「**ルールの活動化**」を選択する。
3. 「パケット・ルールの活動化」ページで、「**VPN 生成ルールのみ活動化**」を選択し、これらのフィルター・ルールを活動化させる対象のインターフェースとして「**ETHLINE**」を選択する。「**OK**」をクリックします。

リモート・ユーザーが Windows XP ワークステーションを構成する前に、管理者は以下の情報を提供して、リモート・ユーザーが自分の側の接続をセットアップできるようにしてください。各リモート・ユーザーに、以下の情報を提供します。

- 事前共有キーの名前: `mycokey`
- iSeries A の IP アドレス: 192.168.1.2
- 接続のためのユーザー名とパスワード

注: これらは、管理者が L2TP ターミネーター・プロファイルの構成時中にユーザー名とパスワードを妥当性検査リストに追加したときに作成されたものです。

Windows XP クライアント上で VPN を構成する

MyCo, Inc のリモート・ユーザーは、以下のステップを実行して、自分のリモート Windows XP クライアントをセットアップする必要があります。

1. Windows XP の「**スタート**」メニューで、「**プログラム**」 → 「**アクセサリ**」 → 「**通信**」 → 「**新しい接続ウィザード**」と展開する。
2. 「新しい接続ウィザードの開始」ページで、概要情報を読む。「**次へ**」をクリックします。
3. 「ネットワーク接続の種類」ページで「**職場のネットワークへ接続する**」を選択する。「**次へ**」をクリックします。
4. 「ネットワーク接続」ページで「**仮想プライベート ネットワーク接続**」を選択する。「**次へ**」をクリックします。
5. 「接続名」ページで、「**会社名**」フィールドに 「営業所へ接続する (Connection to Branch office)」と入力する。「**次へ**」をクリックします。
6. 「パブリック ネットワーク」ページで、「**最初の接続にダイヤルしない**」を選択する。「**次へ**」をクリックします。

7. 「VPN サーバーの選択」ページで、「**ホスト名または IP アドレス**」フィールドに 192.168.1.2 と入力する。「**次へ**」をクリックします。
8. 「新しい接続ウィザードの完了」ページで、「**この接続へのショートカットをデスクトップに追加する**」をクリックする。「**完了**」をクリックします。
9. デスクトップ上に作成された「**MyCo への接続 (Connect Connection to MyCo)**」アイコンをクリックする。
10. 「MyCo への接続 (Connect Connection to MyCo)」ページで、管理者が提供したユーザー名とパスワードを入力する。
11. 「**次のユーザーが接続するとき使用するために、このユーザー名とパスワードを保存する**」および「**このユーザーのみ**」を選択する。「**プロパティ**」をクリックします。
12. 「**セキュリティ**」ページで、以下の「**セキュリティ オプション**」が選択されていることを確認する。
    - **標準**
    - **セキュリティで保護されたパスワードが必要**
    - **データの暗号化を必ず要求する**

    「**IPSec 設定**」をクリックします。
13. 「IPSec 設定 (IPSec Settings)」ページで「**認証に事前共有キーを使う**」を選択し、「**キー**」フィールドに mycokey と入力する。「**OK**」をクリックします。
14. 「ネットワーク」ページで、「**VPN の種類**」に「**L2TP IPSec VPN**」を選択する。「**OK**」をクリックします。
15. ユーザー名とパスワードを使ってサインオンし、「**接続**」をクリックする。

クライアント・サイドで VPN 接続を開始するには、接続ウィザードの完了後にデスクトップ上に表示されるアイコンをクリックします。

エンドポイント間の VPN 接続をテストする

iSeries A とリモート・ユーザーとの間の接続の構成が終わり、接続が正常に開始されたら、接続性をテストして、リモート・ホストが相互に通信できることを確認する必要があります。

接続性をテストするために、次のステップを実行します。

1. iSeries ナビゲーターで、「**iSeries A**」 → 「**ネットワーク**」と展開する。
2. 「**TCP/IP 構成**」を右マウス・ボタン・クリックし、「**ユーティリティー**」を選択して、「**PING**」を選択する。
3. 「**PING**」ダイアログで、「**IP アドレスまたはホスト名**」フィールドに 10.1.1.101 と入力する。

   注: 10.1.1.101 は、iSeries A の L2TP ターミネーター・プロファイルに指定されているアドレス・プールから (外勤の営業スタッフのクライアントに) 動的に割り当てられた IP アドレスを表します。
4. 「**PING**」をクリックして、iSeries A からリモート・ワークステーションへの接続性を検証する。「**OK**」をクリックします。

リモート・クライアントからの接続をテストするには、外勤の従業員が、Windows を実行するワークステーション上でこれらのステップを実行します。

1. コマンド・プロンプトから ping 10.1.1.2 と入力する。これは、本社オフィスのネットワーク内のワークステーションのうちの 1 台の IP アドレスです。
2. これらのステップを繰り返し、今度は本社オフィスから営業所への接続性をテストする。

シナリオ: 区画間通信用の仮想イーサネットを作成する

ユーザーが、小規模の会社のシステム管理者であると想定します。ユーザーは、4 つの論理区画に分割されたサーバーを使用します。 4 つのすべての論理区画間で通信できるようにする必要があります。IT 部門の費用とスペースに制限があるため、余分なイーサネット・カードとケーブルは購入しない予定です。

設定

ユーザーが、小規模の会社のシステム管理者であると想定します。ユーザーは、4 つの論理区画に分割されたサーバーを使用します。 4 つのすべての論理区画間で高速通信ができるようにする必要があり、その通信を外部 LAN に拡張する必要があります。LAN カード用に使用可能なハードウェアのカード・スロットの数が限られています。このため、追加の LAN カードを必要としないソリューションを見付ける必要があります。

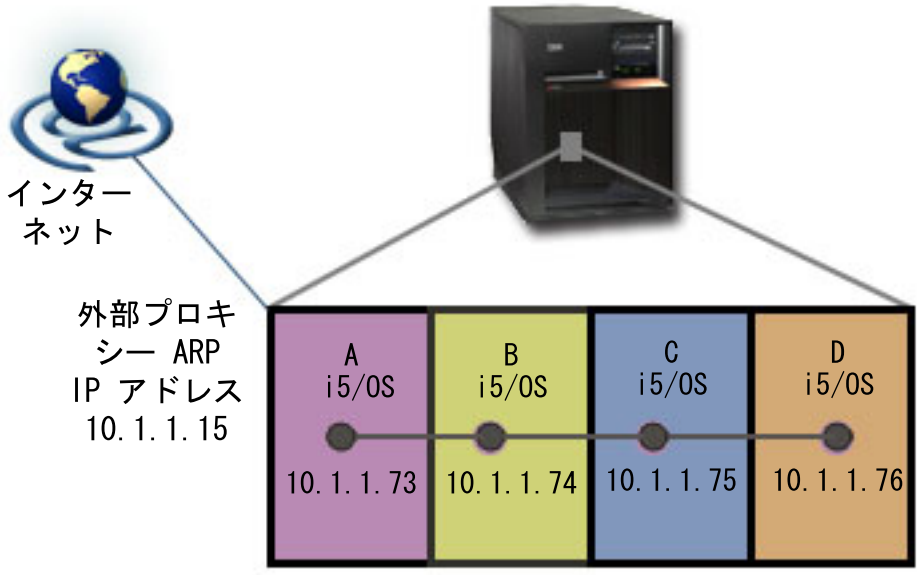
目的

この会社のシステム管理者として、以下の目的があります。

- 各論理区画間の通信が可能な仮想イーサネット・ネットワークを作成する。
- プロキシー ARP を使用して、この仮想イーサネット・ネットワークを外部 LAN に接続できるようにする。
- 必要な回線、インターフェース、および経路を構成する。

詳細

この図は、4 つの論理区画間での通信が可能で、かつ、プロキシー ARP を使用して仮想イーサネットと外部 LAN との間でデータを送信できる、仮想イーサネットを示しています。



論理区画

- 4 つの論理区画は、iSeries サーバー上に作成されています。
- それぞれの区画は、i5/OS バージョン 5 リリース 3 上で稼働します。
- 仮想 TCP/IP インターフェースが、以下の IP アドレスを使用して各区画に構成されています。
  - 区画 A の IP アドレスは 10.1.1.73 です。

– 区画 B の IP アドレスは 10.1.1.74 です。
– 区画 C の IP アドレスは 10.1.1.75 です。
– 区画 D の IP アドレスは 10.1.1.76 です。
- 外部プロキシー ARP インターフェースが、IP アドレス 10.1.1.15 を使用して、区画 A に構成されています。

前提条件および前提事項

セットアップ要件は以下のとおりです。
- i5/OS バージョン 5 リリース 3 以降が 1 次論理区画にインストールされていること
- IBM 270 および 8xx モデルのサーバー
- サーバー上の 4 つの論理区画 (LPAR)。1 次論理区画には、 i5/OS バージョン 5 リリース 3 以降がインストールされている必要があります。その他の論理区画には、i5/OS V5R3 または Linux® がインストールできます。

  このシナリオでは、論理区画のすべてが i5/OS を使用します。

構成のステップ

次の構成タスクを実行します。

関連資料

論理区画

論理区画が仮想イーサネットに参加できるようにする

仮想イーサネットを使用可能にするには、以下の手順に従ってください。
1. 1 次区画 (区画 A) のコマンド行で STRSST と入力し、Enter を押す。
2. 保守ツールのユーザー ID とパスワードを入力する。
3. 「システム保守ツール (SST)」画面で、オプション 5 (システム区画の処理) を選択する。
4. 「システム区画の処理」画面で、オプション 3 (区画構成の処理 (Work with partition configuration)) を選択する。
5. F10 (仮想イーサネットの処理 (Work with Virtual Ethernet)) を押す。
6. 1 次区画と 2 次区画の適切な欄に 1 と入力して、仮想イーサネットを介して区画がもう一方の区画と通信できるようにする。
7. 「システム保守ツール (SST)」を終了して、コマンド行に戻る。

イーサネット回線記述を作成する

仮想イーサネットをサポートするための新しいイーサネット回線記述を構成するには、以下の手順に従ってください。
1. 論理区画 A のコマンド行で、WRKHDWRSC *CMN と入力して Enter を押す。
2. 「通信資源の処理」画面で、該当する適切な仮想イーサネット・ポートの横でオプション 7 (資源明細の表示) を選択する。

   268C として表示されているイーサネット・ポートが、仮想イーサネット・リソースです。論理区画に接続されている各仮想イーサネットごとに 1 つあります。

3. 「資源明細の表示」画面で、スクロールダウンして、ポート・アドレスを見付ける。

   ポート・アドレスは、論理区画の構成時に選択した仮想イーサネットに対応します。
4. 「通信資源の処理」画面で、該当する仮想イーサネット・ポートの横でオプション 5 (構成記述の処理) を選択し、Enter を押す。
5. 「構成記述の処理」画面でオプション 1 (作成) を選択し、Enter を押して「回線記述の作成 (イーサネット) (CRTLINETH)」画面を表示する。
   a. 「*回線記述*」プロンプトで、VETH0 と入力する。これは任意ですが、VETH0 という名前は、論理区画を通信可能にするための「仮想イーサネット (Virtual Ethernet)」ページにある、番号付けされた欄に対応します。回線記述とそれに関連する仮想イーサネットで同じ名前を使用すれば、仮想イーサネット構成を簡単に把握することができます。
   b. 「*回線速度*」プロンプトで、1G と入力する。
   c. 「*二重*」プロンプトで *FULL と入力し、Enter を押す。
   d. 「*最大フレーム・サイズ*」プロンプトに対して 8996 と入力し、Enter を押す。

      フレーム・サイズを 8996 に変更することによって、仮想イーサネットでのデータの転送が向上します。

      回線記述が作成されたことを示すメッセージが表示されます。
6. 回線記述をオンに構成変更する。 WRKCFGSTS *LIN と入力し、VETH0 でオプション 1 (オンへの変更) を選択します。
7. ステップ 1 から 6 を繰り返す。ただし、これらのステップは論理区画 B、C、および D のコマンド行から実行して、各論理区画のイーサネット回線記述を作成します。

   回線記述の名前は任意ですが、仮想イーサネットと関連付けられた回線記述のすべてに、同じ名前を使用すると便利です。このシナリオでは、すべての回線記述に VETH0 という名前をつけています。

IP データグラム転送をオンにする

仮想イーサネットを外部 LAN に接続する区画で、IP データグラム転送をオンにする必要があります。 IP データグラム転送を使用すると、IP パケットをさまざまなサブネット間で転送することができます。このシナリオの場合は、区画 A で IP データグラム転送をオンにする必要があります。

IP データグラム転送をオンにするには、以下の手順に従ってください。

1. 区画 A のコマンド行で、CHGTCPA と入力して F4 を押す。
2. 「*IP データグラムの転送*」プロンプトで、*YES と入力する。

プロキシー ARP を使用可能にするインターフェースの作成

TCP/IP インターフェースを作成する前に、仮想イーサネットを物理 LAN に接続する方法を決定する必要があります。論理区画が外部 LAN 上のシステムと通信できるようにするには、TCP/IP トラフィックを仮想イーサネットと外部 LAN の間で移動できるようにする必要があります。仮想ネットワークと外部ネットワークを接続する方法として、プロキシー ARP、ネットワーク・アドレス変換 (NAT)、および TCP/IP 経路指定の 3 つがあります。このシナリオでは、プロキシー ARP 方式を使用します。このネットワーク・トラフィックを接続する 3 つの方法の詳細については、「仮想イーサネットを外部 LAN に接続する TCP/IP 技法」を参照してください。

TCP/IP インターフェースを作成してプロキシー ARP を使用可能にするには、以下のステップを実行してください。

1. ユーザーのネットワークでルーティング可能な IP アドレスの連続ブロックを取得する。

   この仮想イーサネットには合計 4 つの論理区画があるため、8 アドレスのブロックが必要です。ブロック内の最初の IP アドレスの 4 番目のセグメントが、8 で割り切れる必要があります。このブロックの最初と最後の IP アドレスはサブネット IP アドレスおよびブロードキャスト IP アドレスであり、使用できません。 2 番目のアドレスは論理区画 A の仮想 TCP/IP インターフェース用に使用することができ、3 番目、4 番目、および 5 番目のアドレスは、その他の各論理区画の TCP/IP 接続用に使用することができます。このシナリオの場合、IP アドレスのブロックは 10.1.1.72 から 10.1.1.79 で、サブネット・マスクは 255.255.255.248 です。

   また、外部 TCP/IP アドレス用の IP アドレスが 1 つ必要です。この IP アドレスは連続するアドレスのブロックには属していてはならず、かつ、同じオリジナルのサブネット・マスク 255.255.255.0 に含まれている必要があります。

2. 論理区画 A 用の i5/OS TCP/IP インターフェースを作成する。このインターフェースは、外部の、プロキシー ARP IP インターフェースとして知られています。

   このインターフェースを作成するには、以下のステップに従ってください。

   a. 論理区画 A のコマンド行で CFGTCP と入力し、Enter を押して「TCP/IP の構成」画面を表示する。
   b. オプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押す。
   c. オプション 1 (追加) を選択し、Enter を押して「TCP/IP インターフェースの追加 (ADDTCPIFC)」画面を表示する。
   d. 「IP アドレス」プロンプトで、10.1.1.15 と入力する。
   e. 「回線記述」プロンプトで、回線記述の名前 (ETHLINE など) を入力する。
   f. 「サブネット・マスク」プロンプトで、255.255.255.0 と入力する。

3. インターフェースを開始する。「TCP/IP インターフェースの処理」画面で、開始するインターフェースごとにオプション 9 (開始) を選択します。

関連資料

仮想イーサネットを 外部 LAN に接続する TCP/IP 技法

区画 A に仮想イーサネット・インターフェースを作成する

区画 A に仮想イーサネット・インターフェースを作成するには、以下のステップを実行します。

1. 論理区画 A のコマンド行で CFGTCP と入力し、Enter を押して「TCP/IP の構成」画面を表示する。
2. オプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押す。
3. オプション 1 (追加) を選択し、Enter を押して「TCP/IP インターフェースの追加 (ADDTCPIFC)」画面を表示する。
4. 「IP アドレス」プロンプトで、10.1.1.73 と入力する。
5. 「回線記述」プロンプトで、VETH0 と入力する。
6. 「サブネット・マスク」プロンプトで、255.255.255.248 と入力する。
7. 「関連したローカル・インターフェース」プロンプトで、10.1.1.15 と入力する。これにより、仮想イーサネット・インターフェースが外部インターフェースに関連付けられ、仮想イーサネット・インターフェース 10.1.1.73 と外部インターフェース 10.1.1.15 との間でプロキシー ARP を使用してパケットを転送できるようになります。

8. インターフェースを開始する。「TCP/IP インターフェースの処理」画面で、開始するインターフェースごとにオプション 9 (開始) を選択します。

区画 B に仮想イーサネット・インターフェースを作成する

区画 B に仮想イーサネット・インターフェースを作成するには、以下のステップを実行します。

1. 論理区画 B のコマンド行で CFGTCP と入力し、Enter を押して「TCP/IP の構成」画面を表示する。
2. オプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押す。
3. オプション 1 (追加) を選択し、Enter を押して「TCP/IP インターフェースの追加 (ADDTCPIFC)」画面を表示する。
4. 「IP アドレス」プロンプトで、10.1.1.74 と入力する。
5. 「回線記述」プロンプトで、VETH0 と入力する。
6. 「サブネット・マスク」プロンプトで、255.255.255.248 と入力する。
7. インターフェースを開始する。「TCP/IP インターフェースの処理」画面で、開始するインターフェースごとにオプション 9 (開始) を選択します。

区画 C に仮想イーサネット・インターフェースを作成する

区画 C に仮想イーサネット・インターフェースを作成するには、以下のステップを実行します。

1. 論理区画 C のコマンド行で CFGTCP と入力し、Enter を押して「TCP/IP の構成」画面を表示する。
2. オプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押す。
3. オプション 1 (追加) を選択し、Enter を押して「TCP/IP インターフェースの追加 (ADDTCPIFC)」画面を表示する。
4. 「IP アドレス」プロンプトで、10.1.1.75 と入力する。
5. 「回線記述」プロンプトで、VETH0 と入力する。
6. 「サブネット・マスク」プロンプトで、255.255.255.248 と入力する。
7. インターフェースを開始する。「TCP/IP インターフェースの処理」画面で、開始するインターフェースごとにオプション 9 (開始) を選択します。

区画 D に仮想イーサネット・インターフェースを作成する

区画 D に仮想イーサネット・インターフェースを作成するには、以下のステップを実行します。

1. 論理区画 D のコマンド行で CFGTCP と入力し、Enter を押して「TCP/IP の構成」画面を表示する。
2. オプション 1 (TCP/IP インターフェースの処理) を選択し、Enter を押す。
3. オプション 1 (追加) を選択し、Enter を押して「TCP/IP インターフェースの追加 (ADDTCPIFC)」画面を表示する。
4. 「IP アドレス」プロンプトで、10.1.1.76 と入力する。
5. 「回線記述」プロンプトで、VETH0 と入力する。
6. 「サブネット・マスク」プロンプトで、255.255.255.248 と入力する。
7. インターフェースを開始する。「TCP/IP インターフェースの処理」画面で、開始するインターフェースごとにオプション 9 (開始) を選択します。

経路を作成する

デフォルトの経路を作成して、パケットを仮想イーサネットの外部に送信できるようにするには、以下の手順に従ってください。

1. 区画 B のコマンド行で、CFGTCP と入力して Enter を押す。
2. オプション 2 (TCP/IP 経路の処理) を選択し、Enter を押す。
3. オプション 1 (追加) を選択して、Enter を押す。
4. 「経路宛先」プロンプトで、*DFTROUTE と入力する。
5. 「サブネット・マスク」プロンプトで、*NONE と入力する。
6. 「次のホップ」プロンプトで、10.1.1.73 と入力する。
7. 区画 C および D でステップ 1 から 6 を繰り返して、それらの各論理区画にデフォルトの経路を作成する。いずれの場合も、ネクスト・ホップ・アドレスとして 10.1.1.73 を指定します。

   これらの各論理区画からのパケットは、それぞれのデフォルトの経路を使用して、10.1.1.73 インターフェースへ仮想イーサネット上を移動します。 10.1.1.73 は外部プロキシー ARP インターフェース 10.1.1.15 に関連付けられているため、パケットはプロキシー ARP インターフェースを使用して仮想イーサネット外へ送信されます。

ネットワーク通信を検証する

PING コマンドを使用して、ネットワーク通信を検証してください。

- 区画 B、C、および D から、仮想イーサネット・インターフェース 10.1.1.73 および外部ホストを PING する。
- 外部 i5/OS ホストから、仮想イーサネット・インターフェース 10.1.1.73、10.1.1.74、10.1.1.75、および 10.1.1.76 をそれぞれ PING する。

関連資料

ping コマンド

シナリオ: L2TP を使用して論理区画間でモデムを共用する

4 つの論理区画にまたがる仮想イーサネットがセットアップされているとします。このシナリオを使用して、選択した論理区画でモデムを共用できるようにします。これらの論理区画は、共用モデムを使用して外部 LAN にアクセスします。

設定

ユーザーが、中規模の会社のシステム管理者であると想定します。コンピューター機器を入替える時期になっていますが、それよりもハードウェアを合理化したいと考えています。そこで、3 台の古いサーバーでの業務を 1 台の新しい iSeries サーバーに統合することによってこのプロセスを開始します。 iSeries サーバー上に 3 つの論理区画を作成します。新しい iSeries サーバーには 2793 内部モデムが付属しています。所有する入出力プロセッサー (IOP) のうち、PPP をサポートするものはこれだけです。また、古い 7852-400 エレクトロニック支援 (ECS) モデムも所有しています。

ソリューション

複数のシステムおよび区画は、ダイヤルアップ接続用に同じモデムを共用して、それぞれのシステムまたは区画が独自のモデムを持つ必要性をなくすことができます。これは、L2TP トンネルを使用し、発信呼び出

しを可能にする L2TP プロファイルを構成することによって実現できます。ネットワークでは、トンネルは仮想イーサネット・ネットワークおよび物理ネットワークを介して実行されます。物理回線はネットワーク上の別のサーバーに接続し、これもモデムを共用します。

詳細

以下の図は、このシナリオにおけるネットワーク特性を示しています。

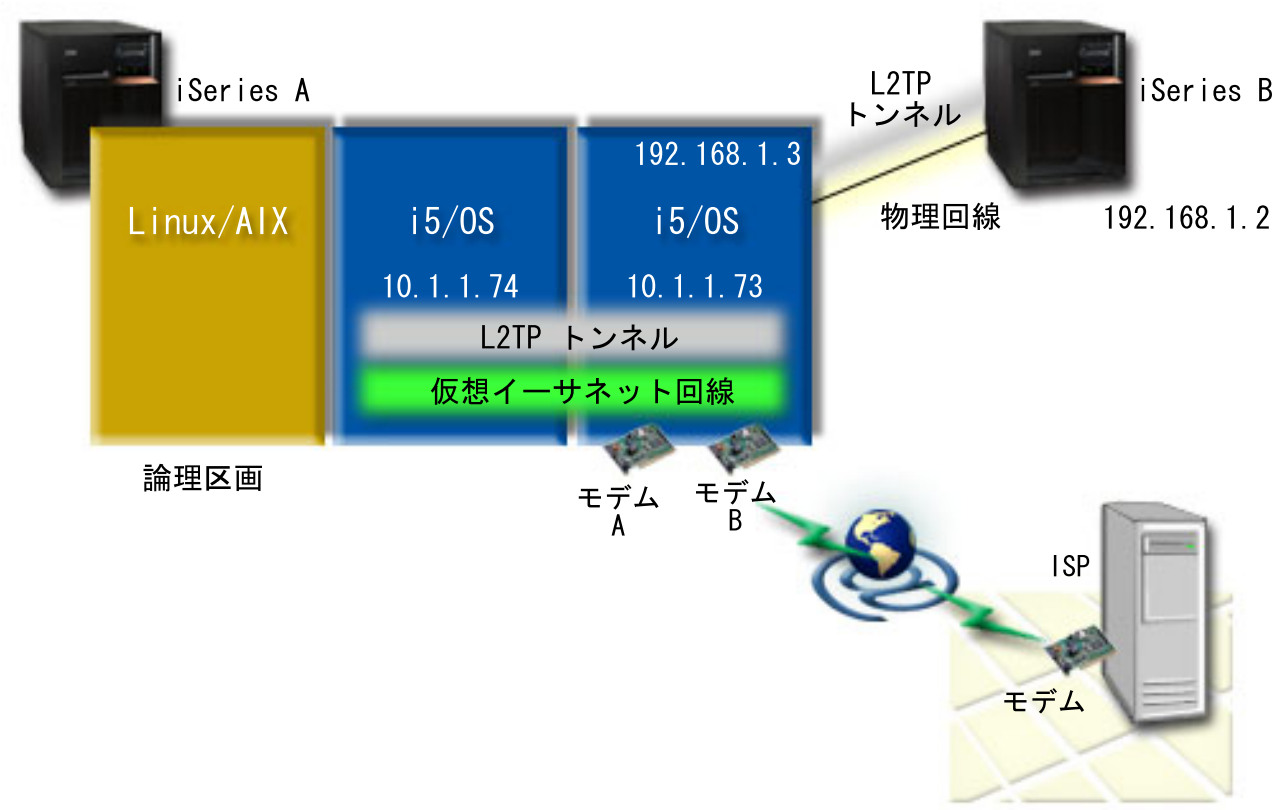


図 1. ダイヤルアップ接続用に同じモデムを共用する複数システム

前提条件および前提事項

iSeries-A のセットアップ要件は、以下のとおりです。

- i5/OS バージョン 5 リリース 3 以降が、ASYNC 対応モデムのある区画にインストール済みである。
- 区画を作成することができるハードウェア。
- iSeries Access for Windows および iSeries ナビゲーター (iSeries ナビゲーターの構成およびサービス・コンポーネント)、バージョン 5 リリース 3 以降
- サーバーには少なくとも 2 つの論理区画 (LPAR) が作成済みであること。モデムがある区画には、i5/OS バージョン 5 リリース 3 以降がインストールされている必要があります。その他の区画には、OS/400 V5R2、V5R3、Linux、または AIX® がインストールできます。このシナリオでは、各区画は i5/OS または Linux オペレーティング・システムのいずれかを使用しています。
- 区画間で通信するために仮想イーサネットが作成されていること。『シナリオ: 区画間通信用の仮想イーサネットを作成する』を参照してください。

iSeries-B のセットアップ要件は、以下のとおりです。

- iSeries Access for Windows および iSeries ナビゲーター (iSeries ナビゲーターの構成およびサービス・コンポーネント)、バージョン 5 リリース 2 以降

シナリオの詳細: L2TP を使用して論理区画間でモデムを共用する

前提条件を満たすと、L2TP プロファイルの構成を開始できます。

ステップ 1: モデムがある区画のすべてのインターフェース用の L2TP ターミネーター・プロファイルを作成する

すべてのインターフェース用のターミネーター・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、「*ご使用のサーバー*」 → 「**ネットワーク**」 → 「**リモート・アクセス・サービス**」を展開する。
2. 「**受信側接続プロファイル**」を右マウス・ボタン・クリックし、「**新規プロファイル**」を選択する。
3. 「セットアップ」ページで次のオプションを選択し、「**OK**」をクリックする。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: L2TP (仮想回線)
   - **作動モード**: ターミネーター (ネットワーク・サーバー)
   - **回線サービスのタイプ**: 単一回線
4. 「**新規プロファイル - 一般**」タブで、以下のフィールドに次のように入力する。
   - **名前**: toExternal
   - **記述**: ダイヤルアウトする受信側接続
   - 「**TCP によるプロファイルの開始 (Start profile with TCP)**」を選択。
5. 「**新規プロファイル - 接続**」タブで、以下のフィールドに次のように入力する。
   - **ローカル・トンネル・エンドポイント IP アドレス**: 任意
   - **仮想回線名**: toExternal。この回線には、関連した物理インターフェースはありません。仮想回線は、この PPP プロファイルのさまざまな特性を記述します。「L2TP 回線のプロパティー」ウィンドウがオープンします。「**認証**」タブをクリックし、サーバーのホスト名を入力します。「**OK**」をクリックして、「新規 PPP プロファイルのプロパティー」ウィンドウの「接続」タブに戻ります。
6. 「**発信呼び出しの確立可能**」をクリックする。「**発信呼び出しダイヤルのプロパティー**」ダイアログが表示されます。
7. 「発信呼び出しダイヤルのプロパティー」ページで、回線サービスのタイプを選択する。
   - **回線サービスのタイプ**: 回線プール
   - **名前**: dialOut
   - 「**新規**」をクリックする。「**新規回線プール・プロパティー**」ダイアログが表示されます。
8. 「新規回線プール・プロパティー」ウィンドウで、発信呼び出しを許可する回線とモデムを選択し、「**追加**」をクリックします。これらの回線を定義する必要がある場合は、「**新規回線**」を選択します。これらのモデムがある区画のインターフェースは、この回線プールからオープンしているあらゆる回線を使用しようとします。新規「回線プロパティー」ウィンドウが表示されます。
9. 「**新規回線プロパティー - 一般**」タブで、次のフィールドに情報を入力する。
   - **名前**: line1
   - **記述**: 回線プール用の最初の回線と最初のモデム (2793 内部モデム)
   - **ハードウェア・リソース**: cmn03 (通信ポート)

10. 他のすべてのタブでデフォルトを受け入れ、「**OK**」をクリックして「新規回線プール・プロパティー」ウィンドウに戻る。
11. 「新規回線プール・プロパティー」ウィンドウで、発信呼び出しを許可する回線とモデムを選択し、「**追加**」をクリックする。プールに対して 2793 モデムが選択されていることを確認します。
12. もう一度「**新規回線**」を選択して、 7852-400 ECS モデムを追加する。新規「回線プロパティー」ウィンドウが表示されます。
13. 「**新規回線プロパティー - 一般**」タブで、次のフィールドに情報を入力する。
    - **名前**: line2
    - **記述**: 回線プール用の 2 番目の回線と 2 番目のモデム (7852-400 外部 ECS モデム)
    - **ハードウェア・リソース**: cmn04 (V.24 ポート)
    - **フレーム指示**: 非同期
14. 「**新規回線プロパティー - モデム**」タブで、外部モデム (7852-400) を選択し、「**OK**」をクリックして「新規回線プール・プロパティー」ウィンドウに戻る。
15. 回線プールに追加する、使用可能なその他の回線をすべて選択し、「**追加**」をクリックする。この例では、上で追加した 2 つの新しいモデムが「*プール用に選択した回線*」フィールドの下にリストされていることを確認し、「**OK**」をクリックして「発信呼び出しダイヤルのプロパティー」ウィンドウに戻ります。
16. 「発信呼び出しダイヤルのプロパティー」ウィンドウで、「デフォルトの電話番号 (Default Dial Numbers)」を入力し、「**OK**」をクリックして「新規 PPP プロファイル・プロパティー (New PPP Profile Properties)」ウィンドウに戻る。

    注: これらの番号は、これらのモデムを使用して他のシステムによって頻繁に呼び出される、ご使用の ISP などの番号を指定することができます。他のシステムが電話番号に *PRIMARY または *BACKUP を指定している場合、ダイヤルされる実際の番号はここで指定した番号になります。他のシステムが実際の電話番号を指定している場合は、代わりにその電話番号が使用されます。
17. 「**TCP/IP 設定**」タブで、以下の値を選択する。
    - **ローカル IP アドレス**: なし
    - **リモート IP アドレス**: なし

    注: プロファイルを L2TP セッションの終了にも使用している場合は、iSeries サーバーを表すローカル IP アドレスを選択する必要があります。リモート IP アドレスには、サーバーと同じサブネットにあるアドレス・プールを選択することもできます。すべての L2TP セッションは、自身の IP アドレスをこのプールから取得します。その他の考慮事項については、「複数の接続プロファイルのサポート」を参照してください。
18. 「**認証**」タブで、すべてのデフォルト値を受け入れる。

これで、モデムがある区画の L2TP ターミネーター・プロファイルの構成が終了しました。次のステップでは、10.1.1.74 に L2TP リモート・ダイヤル - オリジネーター・プロファイルを構成します。

複数の接続プロファイルのサポート:

複数接続をサポートする Point-to-Point 接続では、デジタル、アナログ、または L2TP 呼び出しを扱う 1 つの接続プロファイルを持つことができます。

複数ユーザーが iSeries サーバーに接続する場合に、各 PPP 回線を扱う Point-to-Point 接続プロファイルを別々に指定したくないときにこれを使用すると便利です。この機能は、1 つのアダプターから 4 つの回線を使用する 2805 4 ポート内蔵モデムで特に有効です。

複数接続プロファイルがサポートされるアナログ回線の場合、接続の最大数まで、指定された回線プールのすべての回線が使用されます。基本的には、回線プールで定義された回線ごとに、別々の接続プロファイル・ジョブが開始されます。すべての接続プロファイル・ジョブは、それぞれの回線で着呼を待ちます。

複数接続プロファイル用のローカル IP アドレス

複数接続プロファイルにはローカル IP アドレスを使用できますが、このアドレスは、ご使用の iSeries サーバーで定義された既存 IP アドレスでなければなりません。ローカル IP アドレス・プルダウン・リストを使用して、既存 IP アドレスを選択できます。ローカル iSeries サーバー IP アドレスを PPP プロファイルのローカル IP アドレスとして選択すると、リモート・ユーザーがローカル・ネットワークのリソースにアクセスできるようになります。また、リモート IP アドレス・プールにある IP アドレスを、ローカル IP アドレスと同じネットワーク内に存在するアドレスとして定義する必要もあります。

ローカル iSeries サーバー IP アドレスがないか、リモート・ユーザーが LAN にアクセスできないようにする場合、iSeries サーバーに仮想 IP アドレスを定義する必要があります。仮想 IP アドレスは無線インターフェースとも呼ばれます。 Point-to-Point 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します。この IP 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自動的にトラフィックを転送することはありません。

仮想 IP アドレスを作成するには、以下のステップを実行します。

1. iSeries ナビゲーターでサーバーを展開し、「**ネットワーク**」 → 「**TCP/IP 構成**」 → 「**IPV4**」 → 「**インターフェース**」にアクセスする。
2. 「**インターフェース**」を右クリックし、「**新規インターフェース**」 → 「**仮想 IP**」と選択する。
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する。仮想 IP アドレスが作成されると、Point-to-Point 接続プロファイルはそれを使用できます。TCP/IP 設定ページのローカル IP アドレス・フィールドのプルダウン・リストを使用して、プロファイルに IP アドレスを指定できます。

   注: 仮想 IP アドレスをアクティブにしてから複数接続プロファイルを開始する必要があります。そうしないと、プロファイルを開始することができません。インターフェースの作成後に IP アドレスをアクティブにするには、インターフェース・ウィザードを使用するときに IP アドレスを開始するオプションを選択します。

複数接続プロファイル用のリモート IP アドレス・プール

複数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もできます。典型的な単一接続 Point-to-Point プロファイルでは、リモート IP アドレスを 1 つしか指定できず、接続が確立されるとこのアドレスが起呼システムに提供されます。複数の発呼者が同時に接続できるようになっているため、開始リモート IP アドレスおよび起呼システムに提供される一定範囲の追加 IP アドレスを定義するために、リモート IP アドレス・プールを使用します。

回線プールの制約事項

複数接続用回線プールを使用する際には、次の制約事項が適用されます。

- 1 つの回線プールには同時に 1 つの固有の回線しか存在できません。回線プールから特定の回線を削除すれば、その回線を別の回線プールで使用できます。
- 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と、プロファイルの接続最大数の値まで、回線プール内のすべての回線が使用されます。回線が存在しないと、すべての新規接続は失敗します。また、回線プールに回線が存在しない場合に別のプロファイルを開始すると、回線プールは終了します。

- 回線プールを持つ単一接続プロファイルを開始すると、システムは回線プールの 1 つの回線のみを使用します。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できるようになります。

ステップ 2: 10.1.1.74 に L2TP オリジネーター・プロファイルを構成する

L2TP オリジネーター・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、「**10.1.1.74**」 → 「**ネットワーク**」 → 「**リモート・アクセス・サービス**」を展開する。
2. 「**発信元接続プロファイル**」を右マウス・ボタン・クリックし、「**新規プロファイル**」を選択する。
3. 「セットアップ」ページで次のオプションを選択し、「**OK**」をクリックする。
   - **プロトコル・タイプ**: PPP
   - **接続タイプ**: L2TP (仮想回線)
   - **作動モード**: リモート・ダイヤル
   - **回線サービスのタイプ**: 単一回線
4. 「**一般**」タブで、以下のフィールドに次のように入力する。
   - **名前**: toModem
   - **記述**: モデムがある区画にアクセスする発信元接続
5. 「**接続**」タブで、以下のフィールドに次のように入力する。

   モデムへの**仮想回線名**: この回線には関連する物理インターフェースはありません。仮想回線は、この PPP プロファイルのさまざまな特性を記述します。「L2TP 回線のプロパティー」ウィンドウがオープンします。
6. 「**一般**」タブで、仮想回線の記述を入力する。
7. 「**認証**」タブで、区画のローカル・ホスト名を入力し、「**OK**」をクリックして「接続」ページに戻る。
8. 「**リモート電話番号**」フィールドで、*PRIMARY および *BACKUP を追加する。 これにより、このプロファイルが、モデムがある区画上のターミネーター・プロファイルと同じ電話番号を使用するようになります。
9. 「**リモート・トンネル・エンドポイント IP アドレス**」フィールドで、リモート・トンネル・エンドポイントのアドレス (10.1.1.73) を入力する。
10. 「**認証**」タブで、「**リモート・システムがこの iSeries サーバーの ID を検査することを許可します**」を選択する。
11. 「使用する認証プロトコル」の下で、「**暗号化パスワードが必要 (CHAP-MD5)**」を選択する。デフォルトでは、「**EAP を許可 (Allow extensible authentication protocol)**」も選択されています。

    注: プロトコルは、ダイヤル先のサーバーも使用するプロトコルと一致させてください。
12. ユーザー名とパスワードを入力する。

    注: ユーザー名とパスワードは、ダイヤル先のサーバー上で有効なユーザー名とパスワードと一致させる必要があります。
13. 「**TCP/IP 設定**」タブに進み、必須フィールドを確認する。
    - **ローカル IP アドレス**: リモート・システムによる割り当て
    - **リモート IP アドレス**: リモート・システムによる割り当て
    - **経路指定**: 追加の経路指定は不要

14. 「**OK**」をクリックして PPP プロファイルを保存する。

ステップ 3: 192.168.1.2 用に L2TP リモート・ダイヤル・プロファイルを構成する

ステップ 2 を繰り返します。ただし、リモート・トンネル・エンドポイント・アドレスを 192.168.1.3 (iSeries B の接続先の物理インターフェース) に変更してください。

注: これらは架空の IP アドレスであり、例示のみを目的としています。

ステップ 4: 接続をテストする

両方のサーバーの構成が終わったら、接続性をテストして、両方のシステムがモデムを共用して外部ネットワークに到達していることを確認する必要があります。これを行うには、以下の手順に従ってください。

1. L2TP ターミネーター・プロファイルがアクティブであることを確認する。
   a. iSeries ナビゲーターで、「**10.1.1.73**」 → 「**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**」と展開する。
   b. 右の画面区画で、必要なプロファイル (toExternal) を見付けて、「**状況**」フィールドが*活動状態* になっていることを確認する。「活動状態」になっていない場合は、プロファイルを右マウス・ボタン・クリックし、「**開始**」をクリックします。
2. 10.1.1.74 でリモート・ダイヤル・プロファイルを開始する。
   a. iSeries ナビゲーターで、「**10.1.1.74**」 → 「**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**」を展開する。
   b. 右の画面区画で、必要なプロファイル (toModem) を見付けて、「**状況**」フィールドが*活動状態* になっていることを確認する。「活動状態」になっていない場合は、プロファイルを右マウス・ボタン・クリックし、「**開始**」をクリックします。
3. iSeries B でリモート・ダイヤル・プロファイルを開始する。
   a. iSeries ナビゲーターで、「**192.168.1.2**」 → 「**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**」と展開する。
   b. 右側の区画で、作成したプロファイルを見付けて、「**状況**」フィールドが*活動状態* になっていることを確認する。「活動状態」になっていない場合は、プロファイルを右マウス・ボタン・クリックし、「**開始**」をクリックします。
4. 可能な場合には、ダイヤルした ISP またはその他の宛先を PING して、両方のプロファイルがアクティブであることを確認する。10.1.1.74 と 192.168.1.2 の両方から PING を試行します。
5. 別の方法として、「接続状況」をチェックすることもできる。
   a. iSeries ナビゲーターで、*「必要なサーバー (10.1.1.73 など)* → 「**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**」と展開する。
   b. 右側の区画で、作成したプロファイルを右マウス・ボタン・クリックし、「**接続**」を選択する。「接続状況」ウィンドウで、どのプロファイルがアクティブ、非アクティブ、接続中であるかなどを確認することができます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

この「ネットワーク・シナリオ」資料には、プログラムを作成するユーザーが IBM i5/OS のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

AS/400
eServer
e(ロゴ)server
i5/OS
IBM
IBM (ロゴ)
Infoprint
iSeries
NetServer
OS/400

Microsoft、Windows、Windows NT、Windows NT および Windows ロゴは、 Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

資料に関するご使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。 ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。この資料は、特定物として現存するままの状態で提供され、商品性の保証、第三者の権利の不侵害の保証、特定目的適合性の保証および法律上の瑕

疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

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