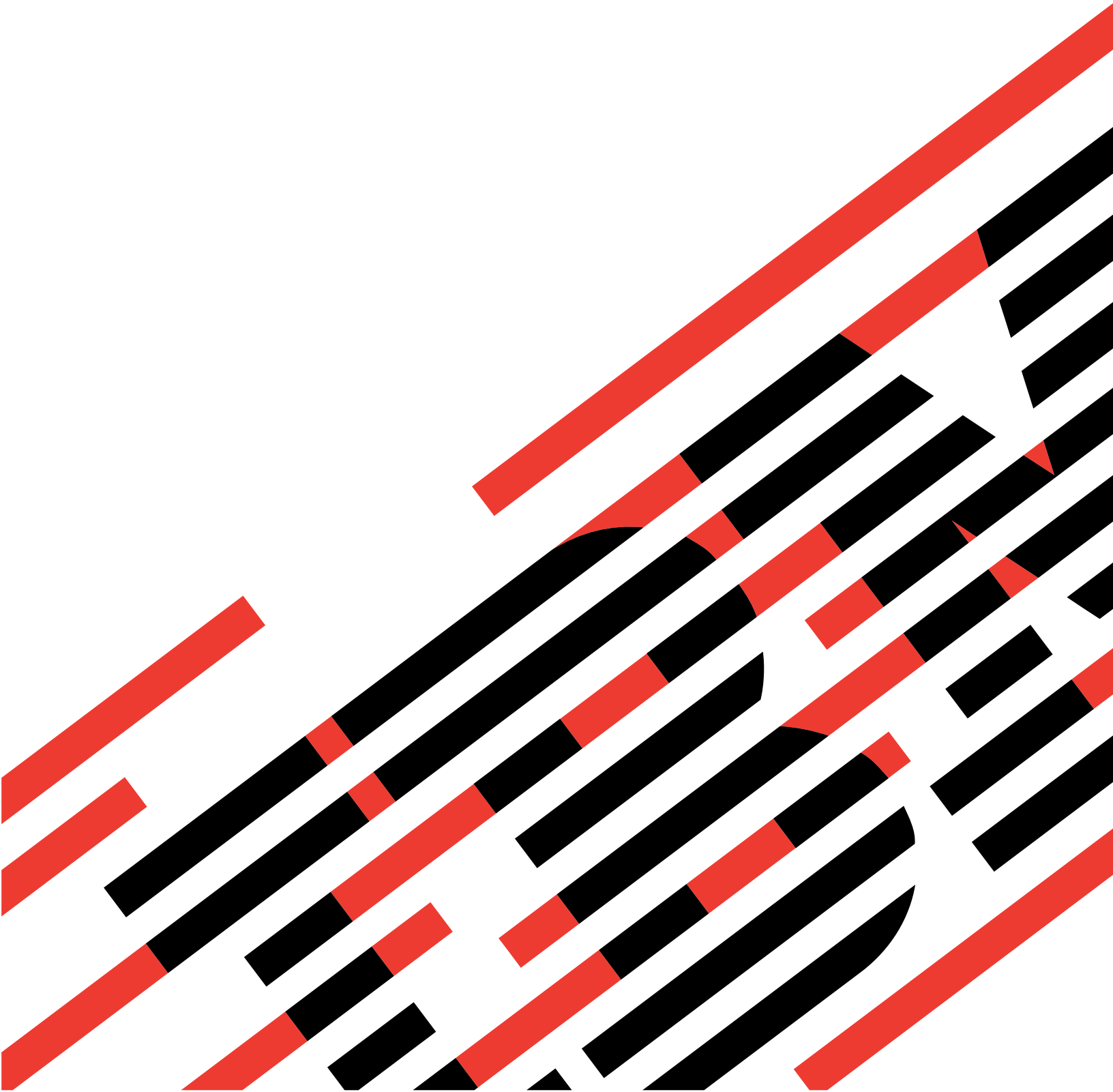
IBM

eserver

iSeries

VPN (仮想プライベート・ネットワーク)

バージョン 5 リリース 3



IBM

@server

iSeries

VPN (仮想プライベート・ネットワーク)

バージョン 5 リリース 3

お願い

本書および本書で紹介する製品をご使用になる前に、 79 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 (5722-SS1) のバージョン 5、リリース 3、モディフィケーション 2 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 モデルで稼動するとは限りません。また、CISC モデルでは稼動しません。

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： iSeries
Virtual private networking
Version 5 Release 3

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 2005.8

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

仮想プライベート・ネットワーク

仮想プライベート・ネットワーク (VPN) の使用により、企業は、インターネットなどの公衆ネットワークの既存のフレームワークの上に、その企業専用のイントラネットをセキュアに拡張することができます。VPN によって、企業は、ネットワーク・トラフィックを制御すると同時に、認証やデータ・プライバシーなどの重要なセキュリティー機能を提供することができます。

OS/400(R) VPN は、OS/400 の GUI (グラフィカル・ユーザー・インターフェース) である iSeries(TM) ナビゲーターの、オプションで導入可能な構成要素です。 これによって、ホストとゲートウェイ間の任意の組み合わせに対して、セキュアな終端間パスを構成することができます。 OS/400 VPN では、認証方式、暗号化アルゴリズム、その他の予防措置を採用することにより、その接続の 2 つのエンドポイント間で送信されるデータの安全性を確保します。

VPN は、TCP/IP 階層化通信スタック・モデルのネットワーク層で稼働します。具体的には、VPN では IP セキュリティー・アーキテクチャー (IPSec) オープン・フレームワークが使用されています。 IPSec は、インターネットに対する基本セキュリティー機能を提供し、さらに、堅固でセキュアな VPN の構築を可能にする柔軟な構造をも提供します。

VPN では、レイヤー 2 トンネリング・プロトコル (L2TP) VPN ソリューションもサポートしています。仮想回線とも呼ばれる L2TP 接続では、リモート・ユーザーに割り当てた IP アドレスを企業のサーバーで管理することができ、これによって、リモート・ユーザーにコスト効率のよいアクセスを提供します。さらに、IPSec と L2TP 接続を一緒に保護すると、システムやネットワークへのアクセスをセキュアに行うことができます。

VPN がネットワーク全体に与える影響を理解することは、重要です。計画と導入を適正に行うことは、成功するために不可欠な要素です。以下のトピックを参照して、VPN の動作と VPN の使用法に関する知識を確認することを、強くお勧めします。

2 ページの『V5R3 の新機能』
このトピックでは、本リリースでの新情報および、本リリースで大幅に変更された情報について説明しています。

3 ページの『トピックの印刷』
この情報のハードコピーが必要な場合は、ここに進んで PDF 文書を印刷してください。

3 ページの『VPN シナリオ』
基本 VPN 型とこれらの構成に必要なステップに精通するために、以下のシナリオを参照してください。

24 ページの『VPN の概念』
標準的な VPN テクノロジーについて、少なくとも基本知識は持っている必要があります。このトピックでは、VPN を実装する際に使用されるプロトコルについて、概念的な情報を提供しています。

35 ページの『VPN の計画』
VPN の使用を成功させるための最初のステップは計画です。このトピックでは、以前のリリースからの移行、セットアップ要件、およびユーザーの仕様に合わせてカスタマイズされた計画用ワークシートを生成する計画アドバイザーへのリンクに関する情報を提供しています。

41 ページの『VPN を構成する』
VPN の計画を終えた後、構成を開始することができます。このトピックでは、VPN を使用して実行が可能なことの概要とその方法について説明します。

51 ページの『VPN を管理する』
このトピックでは、活動中の VPN 接続を管理するために、実行できるさまざまなタスク (接続を変更したり、モニターしたり、あるいは削除したりする方法など) について説明します。

55 ページの『VPN のトラブルシューティング』
VPN 接続に関して何か問題が発生したときは、このトピックを参照してください。

77 ページの『VPN の関連情報』
VPN 情報および関連トピックの他のソースへのリンクに進んでください。

V5R3 の新機能

機能強化
バージョン 5 リリース 3 (V5R3) の仮想プライベート・ネットワーク (VPN) 機能に行われた機能強化としては、2 つの新しい ID タイプがあります。 VPN キー交換ポリシーおよび接続データ・エンドポイントを定義するときに選択できる 2 つの新しい ID タイプがあります。これらの ID タイプは、ローカル IP アドレスと IPv4 ホスト名です。追加情報については、iSeries(TM) ナビゲーターのオンライン・ヘルプを参照してください。

- **ローカル IP アドレス**
  この ID タイプ (ローカル IP アドレス) は、接続定義で Internet Key Exchange ポリシー用のローカル・キー・サーバー・タイプまたはローカル・データ・エンドポイントを定義するために選択できます。選択すると、VPN は使用可能な IPv4 アドレスを使用します。この ID タイプを使用する VPN 接続は、ポリシー・フィルターを使用してはなりません。さらに、ローカル・システムは接続のイニシエーターでなければなりません。
- **IPv4 ホスト名**
  この ID タイプ (IPv4 ホスト名) は、いくつかの異なるパラメーターを定義するために選択できます。
  - Internet Key Exchange ポリシー内のリモート・キー・サーバー ID タイプ
  - 接続のプロパティー内のリモート・アドレス ID
  - 接続グループのプロパティーのポリシー・フィルター定義

  IPv4 ホスト名は、ID タイプとして指定されたホスト名の IP アドレスになります。

VPN セキュリティー上の注意:
事前共用キーを認証に使用するときは、メインモード・ネゴシエーションの使用をお勧めします。よりセキュアな交換になるからです。事前共用キーとアグレッシブ・モード・ネゴシエーションを使用しなければならない場合は、パスワードを求めてディクショナリーをスキャンするアタックで解かれそうにないわかりにくい語を選択してください。キー交換を強制してメインモード・ネゴシエーションを使用する方法については、『事前共用キーを認証に使用するときの機密漏れ』を参照してください。 Internet Key Exchange ポリシーを作成または編集する場合、詳細については、iSeries ナビゲーターのオンライン・ヘルプも使用できます。

情報の強化
V5R3 VPN Information Center トピックに行われた変更としては、レイヤー 2 トンネリング・プロトコル (L2TP) 任意トンネルの概念を説明するビジュアル表示があります。 IPSec によって保護された L2TP 任

意トンネルに関するビジュアル表示を表示するには、以下のリンクを使用してください。これを行うには、Flash プラグイン  が必要です。あるいは、この表示の HTML 版を使用できます。

新規の情報または変更された情報の見分け方

技術上の変更が行われた個所を見分けることができるように、以下のイメージを使用しています。

-  イメージは、新規の情報または変更された情報が開始する位置を示しています。
-  イメージは、新規の情報または変更された情報が終了する位置を示しています。

このリリースの新機能または変更に関連した他の情報を見るには、「プログラム資料説明書」を参照してください。

トピックの印刷

この文書の PDF 版をダウンロードし、表示するには、『VPN (仮想プライベート・ネットワーク)』(約 857 KB) を選択します。

PDF ファイルの保管

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 を右クリックします (上のリンクを右クリックします)。
2. Internet Explorer を使用している場合は、「**対象をファイルに保存**」をクリックします。 Netscape Communicator を使用している場合は、「**リンクを名前を付けて保存**」をクリックします。
3. PDF を保管するディレクトリーを指定します。
4. 「**保存**」をクリックします。

Adobe Acrobat Reader のダウンロード

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 (www.adobe.com/products/acrobat/readstep.html)  からダウンロードできます。

VPN シナリオ

これらの基本接続タイプごとに、それぞれ関連する技術的詳細および構成の詳細を修得するには、以下のシナリオを検討してください。

- **4 ページの『VPN シナリオ: 基本的な事業所接続』**
  このシナリオでは、企業は、VPN ゲートウェイとして機能する 1 対の iSeries(TM) コンピューターを介して、遠隔地にある 2 部門のサブネット間に VPN を確立することを目的としています。
- **10 ページの『VPN シナリオ: 基本的な企業間接続』**
  このシナリオでは、企業は、企業の製造部門にあるクライアント・ワークステーションと、ビジネス・パートナーの供給部門にあるクライアント・ワークステーションとの間に、 VPN を確立することを目的としています。
- **15 ページの『VPN シナリオ: IPSec によって L2TP 任意トンネルを保護する』**
  このシナリオでは、IPSec によって保護された L2TP を使用する事業所ホストと共通オフィスの間の接続を示しています。事業所は動的に割り当てられた IP アドレスを持ち、一方共通オフィスは、静的で、グローバルにルーティング可能な IP アドレスを持っています。

- **22 ページの『VPN シナリオ: VPN のネットワーク・アドレス変換を使用する』**
  このシナリオでは、企業は、ビジネス・パートナーのうちの 1 社と、OS/400(R) VPN を使用して機密データを交換することを目的としています。また、企業のネットワーク構造のプライバシーをさらに保護するために、VPN NAT を使用して、ビジネス・パートナーがアクセスするアプリケーションをホストする iSeries のプライベート IP アドレスを隠します。

詳細な VPN シナリオ

VPN 構成のシナリオの詳細については、以下の他の情報のソースを参照してください。

- **シナリオ: セキュアで予測可能な結果 (VPN と QoS)**
  VPN と共に使用するサービス品質 (QoS) ポリシーを作成することができます。ここでは、両者が一緒に使用されている例が示されています。
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153**

  この IBM レッドペーパーでは、V5R1 VPN および Windows 2000 統合 L2TP および IPSec サポートを使用して VPN トンネルを構成するための、段階的なプロセスを示しています。
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  このレッドブックでは、VPN 概念を調べ、OS/400 で IP セキュリティー (IPSec) とレイヤー 2 トンネリング・プロトコル (L2TP) を使用したインプリメンテーションについて説明しています。
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  このレッドブックでは、IP フィルター、NAT、VPN、HTTP プロキシー・サーバー、SSL、DNS、メールの中継、監査、およびロギングなど、OS/400 システムで使用可能な統合ネットワーク・セキュリティー機能を探します。また、実際の例を通して、その使用法を説明します。

VPN シナリオ: 基本的な事業所接続

企業の要望は、自社の事業所間通信によって発生するコストを最小限にとどめることであると想定します。現在、企業はフレーム・リレー回線または専用回線を使用しています。しかし、内部の機密データを送信する手段として、より安価でセキュアな、グローバルにアクセスできる別の選択肢を検討することが必要です。インターネットを活用することによって、企業のニーズに合致した VPN (仮想プライベート・ネットワーク) を、容易に確立することができます。

企業も事業所も、インターネットでは VPN 保護を必要としますが、それぞれのイントラネット内部では、VPN 保護は必要ありません。イントラネットはトラステッドであると考えられるため、最も良い解決法は、ゲートウェイ間 VPN を構築することです。このケースでは、どちらのゲートウェイも、介在しているネットワークに直接接続されています。言い換えれば、これらはファイアウォールで保護されていない*境界*または *端* システムです。この例は、VPN の基本構成を設定するステップの概要説明として役立ちます。このシナリオでインターネット という用語に言及する場合は、 2 つの VPN ゲートウェイの間に介在しているネットワークを意味します。これは、会社独自の私設ネットワークの場合と、公衆のインターネットの場合がありえます。

注 (重要):
このシナリオでは、インターネットに直接接続されている iSeries(TM) セキュリティー・ゲートウェイを示しています。ファイアウォールが存在していない理由は、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するものではありません。実際には、インターネットに接続するときには、常にセキュリティー・リスクが伴うことを考慮する必要があります。このようなリスクを削減するためのさまざまな方式の詳細については、レッドブック「AS/400(R) Internet Security Scenarios: A Practical Approach」 (SG24-5954-00)  を参照してください。

利点

このシナリオには、以下のような利点があります。

- インターネットまたは既存のイントラネットを使用することにより、リモート・サブネット間の専用回線のコストを削減することができる。
- インターネットまたは既存のイントラネットを使用することにより、専用回線とそれに関連した装置の、導入および保守の複雑さを軽減することができる。
- インターネットの使用により、リモート・ロケーションを、世界中のほとんどどこにでも接続することができる。
- VPN の使用により、ユーザーは、接続のいずれの側からも、専用回線あるいは広域ネットワーク (WAN) 接続を使用して接続されているかのように、すべてのサーバーおよび資源にアクセスすることができる。
- 業界標準の暗号化および認証方式を使用することにより、あるロケーションから別のロケーションに渡される機密情報の、セキュリティーが確保される。
- 暗号鍵を動的かつ定期的に交換することにより、セットアップが単純化され、鍵がデコードされたり、セキュリティーが侵されたりするリスクが最小限に抑えられる。
- 個々のリモート・サブネットでプライベート IP アドレスを使用することにより、重要なパブリック IP アドレスをそれぞれのクライアントに割り振る必要がなくなる。

目的

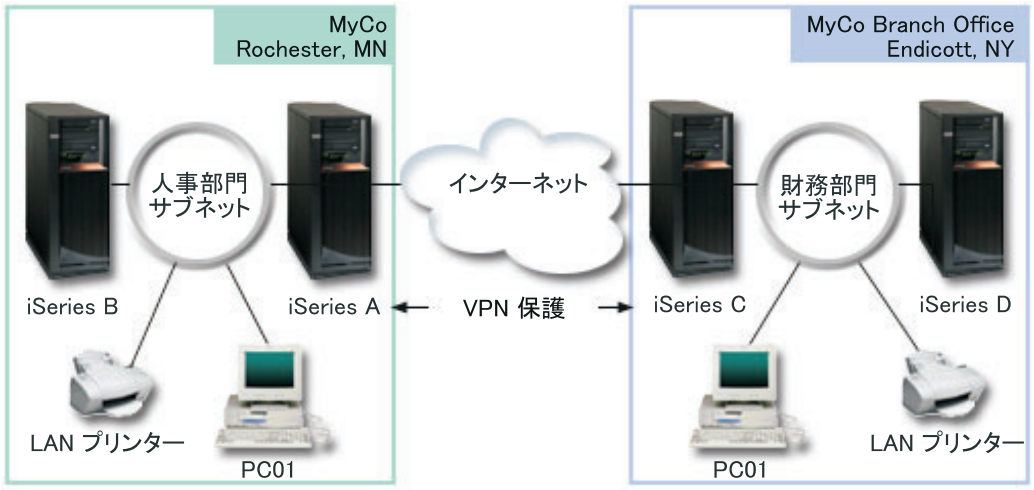
このシナリオでは、MyCo, Inc.が、1 対の iSeries サーバーを介して、人事部門のサブネットと財務部門のサブネットとの間に VPN を確立することを目的としています。 いずれのサーバーも、VPN ゲートウェイの役目をします。 VPN 構成に関して、ゲートウェイはキー管理を実行し、トンネルを通って流れるデータに IPSec を適用します。ゲートウェイは、接続のデータ・エンドポイントではありません。

このシナリオの目的は、次のとおりです。

- VPN は、人事部門のサブネット (Human Resources Subnet) と財務部門のサブネット (Finance Subnet) の間のすべてのデータ・トラフィックを保護しなければなりません。
- データ・トラフィックは、どちらかの部門のサブネットに到着したら VPN 保護を必要としません。
- 各ネットワーク上のすべてのクライアントおよびホストは、すべてのアプリケーションを含めて、他のネットワークに完全アクセスすることができます。
- ゲートウェイ・サーバーは、互いに通信することができ、互いのアプリケーションにアクセスすることができます。

詳細

次の図は、MyCo のネットワーク特性を示しています。



人事部門

- iSeries-A は、OS/400(R) バージョン 5 リリース 2 (V5R2) で稼働し、人事部門の VPN ゲートウェイとして機能します。
- サブネットは、10.6.0.0 (マスクは 255.255.0.0) です。このサブネットは、MyCo Rochester のサイトの VPN トンネルのデータ・エンドポイントを表しています。
- iSeries-A は、IP アドレス 204.146.18.227 でインターネットに接続します。これは、接続エンドポイントです。 つまり、iSeries-A は、キー管理を実行し、IP データグラムの着信および発信に IPSec を適用しています。
- iSeries-A は、IP アドレス 10.6.11.1 でそのサブネットに接続します。
- iSeries-B は、標準の TCP/IP アプリケーションを実行する人事部門サブネットの実動サーバーです。

財務部門

- iSeries-C は、OS/400 バージョン 5 リリース 2 (V5R2) で稼働し、財務部門の VPN ゲートウェイとして機能します。
- サブネットは、10.196.8.0 (マスクは 255.255.255.0) です。このサブネットは、MyCo エンディコットのサイトの VPN トンネルのデータ・エンドポイントを表しています。
- iSeries-C は、IP アドレス 208.222.150.250 でインターネットに接続します。これは、接続エンドポイントです。 つまり、iSeries-C は、キー管理を実行し、IP データグラムの着信および発信に IPSec を適用しています。
- iSeries-C は、IP アドレス 10.196.8.5 でそのサブネットに接続します。

構成作業

このシナリオに記載されている事業所接続を構成するには、次の各作業を完了しなければなりません。

1. TCP/IP 経路指定を検査して、この 2 つのゲートウェイ・サーバーがインターネット経由で互いに通信できることを確認する。これにより、各サブネットのホストが、リモート・サブネットにアクセスするためのそれぞれのゲートウェイに、適切に経路を定めているかどうかを確認できます。
   注: 経路指定については、このトピックの範囲外です。質問事項がある場合は、Information Center の『TCP/IP 経路指定および作業負荷の平準化』を参照してください。
2. 両システムの計画ワークシートとチェックリストを完成 (7ページ) させる。

3. 人事 VPN ゲートウェイ (iSeries-A) の VPN を構成 (8ページ) する。
4. 財務 VPN ゲートウェイ (iSeries-C) の VPN を構成 (9ページ) する。
5. VPN サーバーが開始 (9ページ) されていることを確認する。
6. 2 つのリモート・サブネット間の通信をテスト (9ページ) する。

構成の詳細

最初のステップを完了して、TCP/IP 経路指定が正しく機能し、ゲートウェイ・サーバーが通信可能であることを確認したら VPN の構成をいつでも開始できます。

ステップ 2: 計画ワークシートを完成する

次の計画チェックリストには、 VPN の構成を開始する前に必要な情報の種類が示されています。前提条件チェックリストの答えがすべて「はい」になってから、VPN のセットアップに進んでください。

注: これらのワークシートは、iSeries-A に適用され、iSeries-C の場合にもこのプロセスを繰り返します。必要に応じて IP アドレスをリバースしてください。

前提条件チェックリスト	答え
OS/400(R) のバージョンは、V5R2 (5722-SS1) 以降ですか。	はい
ディジタル証明書マネージャーのオプション (5722-SS1 オプション 34) は、導入してありますか。	はい
Cryptographic Access Provider (5722-AC2 または AC3) は、導入してありますか。	はい
iSeries(TM) Access for Windows(R) (5722-XE1) は、導入してありますか。	はい
iSeries ナビゲーターは、導入してありますか。	はい
iSeries ナビゲーターのネットワーク構成サブコンポーネントは、導入してありますか。	はい
TCP/IP 接続ユーティリティー OS/400 用 (5722-TC1) は、導入してありますか。	はい
サーバー・セキュリティー・データ保存 (QRETSVRSEC *SEC) のシステム値を、 1 に設定しましたか。	はい
iSeries で TCP/IP は構成されていますか (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・ネームなど)。	はい
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ますか。	はい
最新のプログラム一時修正 (PTF) を適用していますか。	はい
VPN トンネルが、IP パケット・フィルターを使用しているファイアウォールまたはルーターを横断する場合、ファイアウォールまたはルーター・フィルターの規則により、AH および ESP プロトコルはサポートされていますか。	はい
ファイアウォールまたはルーターは、IKE (UDP ポート 500)、AH プロトコル、および ESP プロトコルを許可するように構成されていますか。	はい
ファイアウォールは、IP 転送を使用可能にするように構成されていますか。	はい

VPN の構成に必要な情報	答え
作成している接続のタイプ	ゲートウェイ間
動的キー・グループに付ける名前	HRgw2FINgw
キーの保護に必要なセキュリティーとシステム性能のタイプ	平衡型
接続を認証するための証明書を使用していますか。 使用していない場合は、事前共用キーは何ですか。	いいえ topsecretstuff

VPN の構成に必要な情報	答え
ローカル・キー・サーバーの ID は、何ですか。	IP アドレス: 204.146.18.227
ローカル・データ・エンドポイントの ID は、何ですか。	サブネット: 10.6.0.0 マスク: 255.255.0.0
リモート・キー・サーバーの ID は、何ですか。	IP アドレス: 208.222.150.250
リモート・データ・エンドポイントの ID は、何ですか。	サブネット: 10.196.8.0 マスク: 255.255.255.0
接続を通過可能にしたいポートおよびプロトコル	任意
データの保護に必要なセキュリティーとシステム性能のタイプ	平衡型
接続が適用されるインターフェース	TRLINE

ステップ 3: iSeries-A で VPN を構成する

ワークシートの内容を使用して、以下の手順で iSeries-A に VPN を構成してください。

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**」を右クリックして、「**新規接続**」を選択し、「新規接続」ウィザードを開始する。
3. 「**ウェルカム**」ページで、このウィザードが作成するオブジェクトに関する情報を参照する。
4. 「**次へ**」をクリックして、「**接続名**」のページに移動する。
5. 「**名前**」フィールドに、HRgw2FINgw と入力する。
6. (オプション) この接続グループの記述を指定する。
7. 「**次へ**」をクリックして、「**接続シナリオ**」のページに移動する。
8. 「**ゲートウェイから別のゲートウェイに接続 (Connect your gateway to another gateway)**」を選択する。
9. 「**次へ**」をクリックして、「**Internet Key Exchange ポリシー**」のページに移動する。
10. 「**新しいポリシーの作成**」を選択してから、「**機密保護とパフォーマンスのバランス**」を選択する。
11. 「**次へ**」をクリックして、「**ローカル接続エンドポイントの証明書**」のページに移動する。
12. 接続の認証に証明書を使用しないよう指示するには、「**いいえ**」を選択する。
13. 「**次へ**」をクリックして、「**ローカル・キー・サーバー**」のページに移動する。
14. 「**ID のタイプ**」フィールドで、「**バージョン 4 IP アドレス**」を選択する。
15. 「**IP アドレス**」フィールドで、204.146.18.227 を選択する。
16. 「**次へ**」をクリックして、「**リモート・キー・サーバー**」のページに移動する。
17. 「**ID のタイプ**」フィールドで、「**バージョン 4 IP アドレス**」を選択する。
18. 「**ID**」フィールドに 208.222.150.250 と入力する。
19. 「**事前共用キー**」フィールドに topsecretstuff と入力する。
20. 「**次へ**」をクリックして、「**ローカル・データ・エンドポイント (Local Data Endpoint)**」のページに移動する。
21. 「**ID のタイプ**」フィールドで、「**IP バージョン 4 サブネット**」を選択する。
22. 「**ID**」フィールドに 10.6.0.0 と入力する。
23. 「**サブネット・マスク**」フィールドに 255.255.0.0 と入力する。
24. 「**次へ**」をクリックして、「**リモート・データ・エンドポイント (Remote Data Endpoint)**」のページに移動する。

25. 「**ID のタイプ**」フィールドで、「**IP バージョン 4 サブネット**」を選択する。
26. 「**ID**」フィールドに 10.196.8.0 と入力する。
27. 「**サブネット・マスク**」フィールドに 255.255.255.0 と入力する。
28. 「**次へ**」をクリックして、「**データ・サービス**」のページに移動する。
29. デフォルトを受け入れてから、「**次へ**」をクリックして、「**データ・ポリシー**」のページに移動する。
30. 「**新しいポリシーの作成**」を選択してから、「**機密保護とパフォーマンスのバランス**」を選択する。「**RC4 暗号化アルゴリズムを使用する**」を選択する。
31. 「**次へ**」をクリックして、「**適用できるインターフェース**」のページに移動する。
32. 「**回線 (Line)**」テーブルから **TRLINE** を選択する。
33. 「**次へ**」をクリックして、「**要約**」のページに移動する。ウィザードで作成されるオブジェクトを復習して、これらのオブジェクトが正しいことを確認してください。
34. 「**完了**」をクリックして、構成を完了する。
35. 「**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てから、「**はい、生成されたポリシー・フィルターを活動化します (Yes, activate the generated policy filters)**」を選択し、さらに「**他のすべてのトラフィックを許可 (Permit all other traffic)**」を選択する。「**OK**」をクリックして、構成を完了する。プロンプトが出されたときに、すべてのインターフェースでルールを活動化することを指定します。

これで、iSeries-A での VPN の構成は終了しました。次のステップは、財務部門 VPN ゲートウェイ (iSeries-C) での VPN の構成です。

ステップ 4: iSeries-C に VPN を構成する

iSeries-A の構成に使用したのと同じステップに従い、必要なら IP アドレスをリバースしてください。ガイダンスには、計画ワークシートを使用します。財務部門 VPN ゲートウェイの構成が終了すると、接続がオンデマンド 状態になります。つまり、この VPN 接続で保護する必要のある IP データグラムが送信された場合に、接続が開始されます。 VPN サーバーが開始されていない場合には、次のステップでこれらのサーバーを開始します。

ステップ 6: VPN サーバーを開始する

VPN サーバーを開始するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして、「**開始**」を選択する。

ステップ 7: テスト接続

両方のサーバーの構成が終了し、VPN サーバーが正常に開始された後で、リモート・サブネットが互いに通信可能であることを確認するために、接続のテストを行う必要があります。 この作業を行うには、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**」と展開する。
2. 「**TCP/IP 構成**」を右クリックして、「**ユーティリティー**」を選択してから「**PING**」を選択する。
3. 「**PING - iSeries-A**」ダイアログ・ボックスで、「**IP アドレスまたはホスト名**」フィールドに iSeries-C と入力する。
4. 「**PING**」をクリックして、iSeries-A から iSeries-C への接続を検査する。
5. 終了したら、「**クローズ**」をクリックする。

VPN シナリオ: 基本的な企業間接続

多くの企業では、フレーム・リレー回線または専用回線を使用することによって、その企業のビジネス・パートナー、子会社およびベンダーにセキュア通信を提供しています。残念ながら、こうした解決方法では、多くの場合、費用がかかり、地理的な制限があります。VPN により、経済的な専用通信を必要とする企業に新たな選択肢が提供されます。

製造会社に対する主要な部品供給元であると想定してください。製造会社の要求する日時に合わせて、特定の部品を特定の数量用意しておくことが重要であることから、常に製造会社の在庫状況と生産スケジュールに注意を払う必要があります。現在はこの業務を手作業で処理しているものの、手間と費用がかかり、さらに時々不正確でもあることが判明しています。現在よりも簡単、迅速、かつ効果的に製造会社と通信する方法を見つける必要があります。しかし、交換する情報の性質上、機密性および時間依存性を考慮する必要があるため、製造会社はその会社の Web サイト上でその情報を公開したり、対外向け月例報告書として配布したりすることは避けたいと考えています。インターネットを活用することによって、両社のニーズに合致した VPN (仮想プライベート・ネットワーク) を、容易に確立することができます。

目的

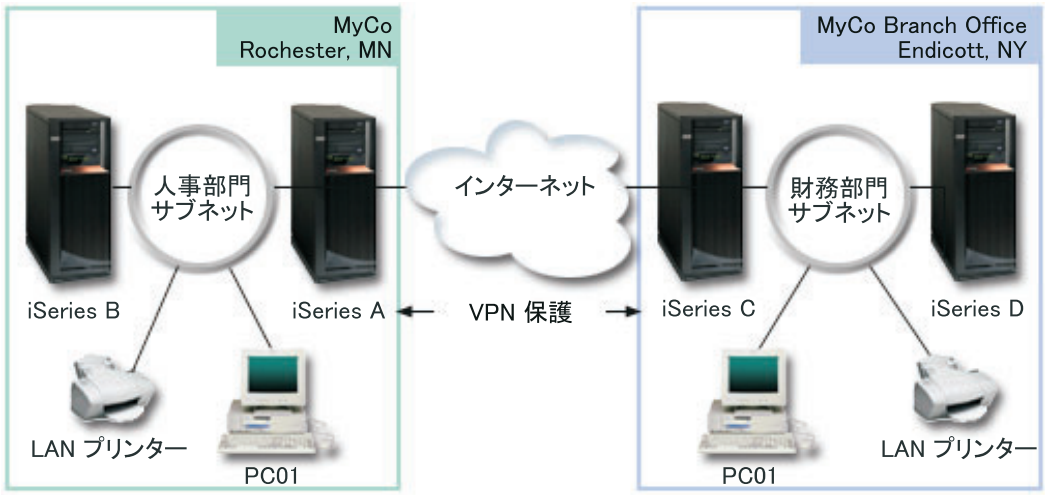
このシナリオで、MyCo という企業は、この企業の部品事業部にあるホストと、ビジネス・パートナーの 1 つである TheirCo の製造部門にあるホストとの間に、VPN を確立することを目的としています。

これらの 2 つの企業が共有している情報は、重要機密であるため、インターネットを介して移動している間は保護されていなければなりません。さらに、各ネットワークは、他のネットワークを非トラステッドと見なすため、いずれかの企業ネットワーク内にデータを何の配慮もなく流してはなりません。言い換えれば、どちらの企業でも終端間での認証、保全性、および暗号化が必要です。

注 (重要):
このシナリオは、例を挙げて、簡単なホスト間 VPN 構成を紹介することを意図したシナリオです。通常のネットワーク環境では、ファイアウォール構成、IP アドレッシングに関する要件、および他のネットワークとの間の経路指定も考慮する必要があります。

詳細

以下の図は、MyCo と TheirCo のネットワーク特性を示したものです。



MyCo 部品供給元ネットワーク

- iSeries-A は、OS/400(R) バージョン 5 リリース 2 (V5R2) で稼働します。
- iSeries-A の IP アドレスは 10.6.1.1 です。これは、接続エンドポイントであり、データ・エンドポイントでもあります。つまり、iSeries-A は IKE ネゴシエーションを実行し、IPSec を着信および発信 IP データグラムに適用します。これは、VPN を介して流れるデータのソースおよび宛先にもなります。
- iSeries-A は、サブネット 10.6.0.0 でマスク 255.255.0.0 にあります。
- iSeries-A のみが iSeries-C との接続を開始できます。

TheirCo 製造部門ネットワーク

- iSeries-C は、OS/400 バージョン 5 リリース 2 (V5R2) で稼働します。
- iSeries-C の IP アドレスは 10.196.8.6 です。これは、接続エンドポイントであり、データ・エンドポイントでもあります。つまり、iSeries-A は IKE ネゴシエーションを実行し、IPSec を着信および発信 IP データグラムに適用します。これは、VPN を介して流れるデータのソースおよび宛先にもなります。
- iSeries-C は、サブネット 10.196.8.0 およびマスク 255.255.255.0 にあります。

構成作業

このシナリオで説明している企業間接続を構成するには、以下の各作業を完了しなければなりません。

1. TCP/IP 経路指定を検査して、iSeries-A および iSeries-C がインターネット経由で互いに通信できることを確認する。これにより、各サブネットのホストが、リモート・サブネットにアクセスするためのそれぞれのゲートウェイに、適切に経路を定めているかどうかを確認できます。このシナリオの場合、以前持っていなかった可能性がある、プライベート・アドレスの経路指定を考慮する必要が出てくるので注意する必要があります。

   注: 経路指定については、このトピック内では説明しません。質問事項がある場合は、Information Center の『TCP/IP 経路指定および作業負荷の平準化』トピックを参照してください。
2. 両方のシステムの計画ワークシートおよびチェックリストを完成 (11ページ) させる。
3. MyCo の部品供給元ネットワークの iSeries-A に VPN を構成 (12ページ) する。
4. TheirCo の製造部門ネットワークの iSeries-C に VPN を構成 (13ページ) する。
5. 両方のサーバーのフィルター規則を活動化 (14ページ) する。
6. iSeries-A の接続を開始 (14ページ) する。
7. 2 つのリモート・サブネット間の通信をテスト (14ページ) する。

構成の詳細

最初のステップを完了して、TCP/IP 経路指定が正しく機能し、サーバーが通信可能であることを確認したら VPN の構成をいつでも開始できます。

ステップ 2: 計画ワークシートを完成する

次の計画チェックリストには、 VPN の構成を開始する前に必要な情報の種類が示されています。前提条件チェックリストの答えがすべて「はい」になってから、VPN のセットアップに進んでください。

注: これらのワークシートは、iSeries-A に適用され、iSeries-C の場合にもこのプロセスを繰り返します。必要に応じて IP アドレスをリバースしてください。

前提条件チェックリスト	答え
OS/400(R) のバージョンは、V5R2 (5722-SS1) 以降ですか。	はい

前提条件チェックリスト	答え
ディジタル証明書マネージャーのオプション (5722-SS1 オプション 34) は、導入してありますか。	はい
Cryptographic Access Provider (5722-AC2 または AC3) は、導入してありますか。	はい
iSeries(TM) Access for Windows(R) (5722-XE1) は、導入してありますか。	はい
iSeries ナビゲーターは、導入してありますか。	はい
iSeries ナビゲーターのネットワーク構成サブコンポーネントは、導入してありますか。	はい
TCP/IP 接続ユーティリティー OS/400 用 (5722-TC1) は、導入してありますか。	はい
サーバー・セキュリティー・データ保存 (QRETSVRSEC *SEC) のシステム値を、 1 に設定しましたか。	はい
iSeries で TCP/IP は構成されていますか (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・ネームなど)。	はい
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ますか。	はい
最新のプログラム一時修正 (PTF) を適用していますか。	はい
VPN トンネルが、IP パケット・フィルターを使用しているファイアウォールまたはルーターを横断する場合、ファイアウォールまたはルーター・フィルターの規則により、AH および ESP プロトコルはサポートされていますか。	はい
ファイアウォールまたはルーターは、IKE (UDP ポート 500)、AH、および ESP プロトコルを許可するように構成されていますか。	はい
ファイアウォールは、IP 転送を使用可能にするように構成されていますか。	はい

VPN の構成に必要な情報	答え
作成している接続のタイプ	ホスト間
動的キー・グループに付ける名前	MyCo2TheirCo
キーの保護に必要なセキュリティーとシステム性能のタイプ	最大
接続を認証するための証明書を使用していますか。 使用していない場合は、事前共用キーは何ですか。	はい
ローカル・キー・サーバーの ID は、何ですか。	IP アドレス: 10.6.1.1
ローカル・データ・エンドポイントの ID は、何ですか。	IP アドレス: 10.6.1.1
リモート・キー・サーバーの ID は、何ですか。	IP アドレス: 10.196.8.6
リモート・データ・エンドポイントの ID は、何ですか。	IP アドレス: 10.196.8.6
接続を通過可能にしたいポートおよびプロトコル	任意
データの保護に必要なセキュリティーとシステム性能のタイプ	最大
接続が適用されるインターフェース	TRLINE

ステップ 3: iSeries-A で VPN を構成する

ワークシートの内容を使用して、以下の手順で iSeries-A に VPN を構成してください。

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして、「**新規接続**」を選択し、「接続」ウィザードを開始する。
3. 「**ウェルカム**」ページで、このウィザードが作成するオブジェクトに関する情報を参照する。

4. 「**次へ**」をクリックして、「**接続名**」のページに移動する。
5. 「**名前**」フィールドに、MyCo2TheirCo と入力する。
6. (オプション) この接続グループの記述を指定する。
7. 「**次へ**」をクリックして、「**接続シナリオ**」のページに移動する。
8. 「**自分のホストを別のホストに接続**」を選択する。
9. 「**次へ**」をクリックして、「**Internet Key Exchange ポリシー**」のページに移動する。
10. 「**新しいポリシーの作成**」を選択してから、「**セキュリティーは最高、パフォーマンスは最低**」を選択する。
11. 「**次へ**」をクリックして、「**ローカル接続エンドポイントの証明書**」のページに移動する。
12. 接続の認証に証明書を使用することを示すには、「**Yes (はい)**」を選択する。次に、iSeries-A を表す証明書を選択します。
    注: 証明書を使用して、ローカル接続エンドポイントを認証したい場合は、まず、ディジタル証明書マネージャー (DCM) に証明書を作成しなければなりません。
13. 「**次へ**」をクリックして、「**ローカル接続エンドポイント ID**」のページに移動する。
14. ID のタイプとして、「**IP バージョン 4 アドレス**」を選択する。関連する IP アドレスは、10.6.1.1 です。この情報は、DCM で作成する証明書で再び定義されます。
15. 「**次へ**」をクリックして、「**リモート・キー・サーバー**」のページに移動する。
16. 「**ID のタイプ**」フィールドで、「**IP バージョン 4 アドレス**」を選択する。
17. 「**ID**」フィールドに 10.196.8.6 と入力する。
18. 「**次へ**」をクリックして、「**データ・サービス**」のページに移動する。
19. デフォルトを受け入れてから、「**次へ**」をクリックして、「**データ・ポリシー**」のページに移動する。
20. 「**新しいポリシーの作成**」を選択してから、「**セキュリティーは最高、パフォーマンスは最低**」を選択する。「**RC4 暗号化アルゴリズムを使用する**」を選択する。
21. 「**次へ**」をクリックして、「**適用できるインターフェース**」のページに移動する。
22. 「**TRLINE**」を選択する。
23. 「**次へ**」をクリックして、「**要約**」のページに移動する。ウィザードで作成されるオブジェクトを復習して、これらのオブジェクトが正しいことを確認してください。
24. 「**完了**」をクリックして、構成を完了する。
25. 「**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されます**」を選択して「**OK**」をクリックする。

次のステップは、iSeries-A だけがこの接続を開始できるように指定することです。これを実行するには、ウィザードで作成した、動的キー・グループ、MyCo2TheirCo のプロパティーをカスタマイズします。

1. VPN インターフェースの左側ペインの「**グループ別**」をクリックする。新規動的キー・グループ、MyCo2TheirCo が右側ペインに表示されます。このグループを右クリックして、「**プロパティー**」を選択します。
2. 「**ポリシー**」のページに進み、「**ローカル・システムが接続を開始します**」オプションを選択する。
3. 「**OK**」をクリックして、変更を保管する。

これで、iSeries-A での VPN の構成は終了しました。次のステップは、TheirCo の製造ネットワークの iSeries-C での VPN の構成です。

ステップ 4: iSeries-C に VPN を構成する

iSeries-A の構成に使用したのと同じステップに従い、必要なら IP アドレスをリバースしてください。ガイダンスには、計画ワークシートを使用します。 iSeries-C の構成を終了すると、「接続」ウィザードによりサーバーごとに作成されたフィルター規則を活動化しなければなりません。

ステップ 5: パケット・ルールを活動化する

ウィザードにより、この接続が正しく機能するために必要なパケット・ルールが自動的に作成されます。ただし、VPN 接続を開始できるようにするには、その前に、両方のシステムでこれらのパケット・ルールを活動化しなければなりません。 iSeries-A でこの作業を行うには、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**」と展開する。
2. 「**パケット・ルール**」を右クリックし、「**活動化**」を選択する。これにより、「**パケット・ルールの活動化 (Activate Packet Rules)**」ダイアログ・ボックスが開きます。
3. VPN で生成されたルールのみを活動化するのか、選択したファイルのみを活動化するのか、あるいは VPN で生成されたルールと選択したファイルの両方を活動化するのかを選択する。たとえば、VPN で生成されたルールに加えて、各種の PERMIT ルールや DENY ルールをインターフェースに適用したい場合には、VPN で生成されたルールと選択したファイルの両方の活動化を選択することができます。
4. 活動化させるルールのあるインターフェースを選択する。ここでは、「**すべてのインターフェース (All interfaces)**」を選択します。
5. ダイアログ・ボックス上で「**OK**」をクリックして、指定した 1 つまたは複数のインターフェースで規則の検査と活動化を実行することを確認します。「OK」をクリックすると、システムはそのルールに構文およびセマンティックのエラーがないかどうかを検査し、エディター下部のメッセージ・ウィンドウでその結果を報告します。特定のファイルおよび行番号に関連したエラー・メッセージは、エラーを右クリックし、「**行番号 (Go To Line)**」を選択すると、ファイル内のエラーを強調表示させることができます。
6. 上記のステップを繰り返して、iSeries-C でパケット・ルールを活動化する。

ステップ 6: 接続を開始する

iSeries-A の MyCo2TheirCo 接続を開始するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**iSeries-A**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. VPN サーバーが開始していない場合は、「**仮想プライベート・ネットワーク**」を右クリックして、「**開始**」を選択する。 これで、VPN サーバーが起動します。
3. 「**仮想プライベート・ネットワーク**」—>「**セキュア接続**」と展開する。
4. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
5. 「**MyCo2TheirCo**」を右クリックして、「**開始**」を選択する。
6. 「**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ると、状況が*アイドル* から*使用可能* に変更されます。接続が開始されるまでには数分を要する場合があるため、状況が*使用可能* に変わるまで定期的に最新表示されます。

ステップ 7: テスト接続

どちらのサーバーの構成も終了し、接続が正常に開始されたら、リモート・ホストが互いに通信可能になっていることを確認するために接続のテストを行う必要があります。この作業を行うには、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**」と展開する。
2. 「**TCP/IP 構成**」を右クリックして、「**ユーティリティー**」を選択してから「**PING**」を選択する。

3. 「**PING - iSeries-A**」ダイアログ・ボックスで、「**IP アドレスまたはホスト名**」フィールドに iSeries-C と入力する。
4. 「**PING**」をクリックして、iSeries-A から iSeries-C への接続を検査する。
5. 終了したら、「**クローズ**」をクリックする。

VPN シナリオ: IPSec によって L2TP 任意トンネルを保護する

ユーザーの企業が別の地方に小さな事業所を持っているとします。この事業所は、ある特定の営業日には 1 日中、企業イントラネット内にある iSeries(TM) に関する機密情報にアクセスしなければならない場合があります。企業は現在、事業所からの企業ネットワークへのアクセスを提供するために、高価な専用回線を使用しています。企業は、イントラネットにセキュアにアクセスできる体制は維持したいのですが、最終的には、専用回線に伴う費用を削減したい意向を持っています。レイヤー 2 トンネリング・プロトコル (L2TP) 任意トンネルを作成すれば、これを実行することができます。この任意トンネルは、企業ネットワークを拡張して、事業所を企業サブネットの一部であるかのように見せる働きをします。 VPN は、L2TP トンネル経由のデータ・トラフィックを保護します。

L2TP 任意トンネルを使用すると、遠隔地の事業所は、企業ネットワークの L2TP ネットワーク・サーバー (LNS) に、直接通じるトンネルを確立します。 L2TP アクセス集線装置 (LAC) の機能は、クライアント側にあります。このトンネルは、リモート・クライアントの、インターネット・サービス・プロバイダー (ISP) に対して透過的であるため、 L2TP のサポートには、ISP は必須ではありません。 L2TP の概念についてさらに詳しく知りたい場合は、29 ページの『レイヤー 2 トンネリング・プロトコル (L2TP)』を参照してください。

> **注 (重要):**
> このシナリオでは、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ています。ファイアウォールが存在していない理由は、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するものではありません。インターネットに接続するときには、常にセキュリティー・リスクが伴うことを考慮する必要があります。このようなリスクを削減するためのさまざまな方式の詳細については、レッドブック「AS/400(R) Internet Security Scenarios: A Practical Approach」(SG24-5954-00)  を参照してください。

目的

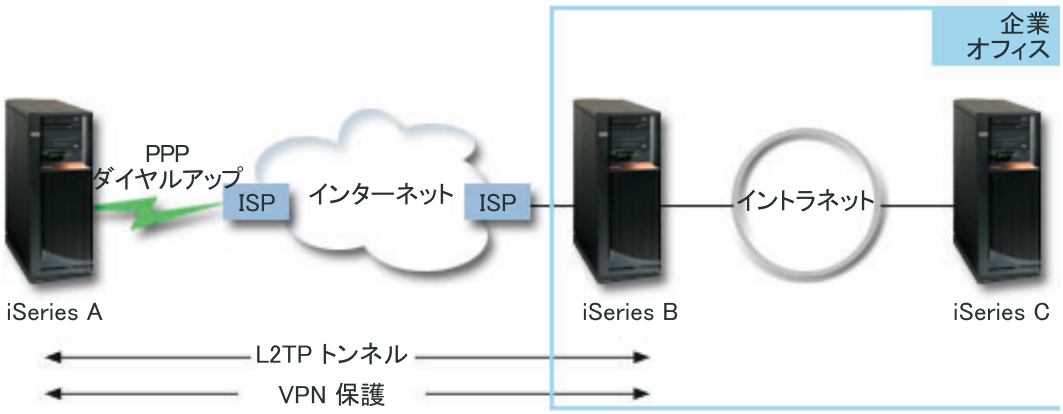
このシナリオでは、事業所の iSeries は、 VPN によって保護された L2TP トンネルを使ったゲートウェイ iSeries を介して企業ネットワークに接続します。

このシナリオの主な目的は、次のとおりです。

- 常に、事業所システムが企業オフィス (Corporate Office) への接続を開始する。
- 事業所システムが、企業ネットワークにアクセスする必要がある事業所ネットワークでの唯一のシステムである。すなわち、役割は、事業所ネットワークでのゲートウェイではなくホストのものです。
- 企業システムは、企業オフィス・ネットワークのホスト・コンピューターである。

詳細

以下の図は、このシナリオのネットワーク特性を示しています。



iSeries-A

- 企業ネットワークのすべてのシステム上の TCP/IP アプリケーションにアクセスできなければならない。
- 動的に割り当てられた IP アドレスをその ISP から受け取る。
- L2TP サポートを提供するように構成されていなければならない。

iSeries-B

- iSeries-A 上の TCP/IP アプリケーションにアクセスできなければならない。
- サブネットは、10.6.0.0 (マスクは 255.255.0.0) である。このサブネットは、社内サイトでの VPN トンネルのデータ・エンドポイントを表す。
- IP アドレスは 205.13.237.6 のインターネットに接続する。これは、接続エンドポイントです。 すなわち、iSeries-B はキー管理を実行し、IPSec 着信と発信の IP データグラムに適用されます。 iSeries-B は、IP アドレスが 10.6.11.1 のサブネットに接続します。

L2TP 用語では、 *iSeries-A* は L2TP の起動側として動作し、一方 *iSeries-B* は、L2TP ターミネーターとして動作します。

構成作業

TCP/IP 構成がすでに存在し、作動していると想定すると、以下の作業を完了しなければなりません。

1. iSeries-A で VPN を構成する (16ページ)。
2. iSeries-A 用 PPP 接続プロファイルおよび仮想回線を構成する (19ページ)。
3. 動的キー・グループを PPP プロファイルに適用する (20ページ)。
4. iSeries-B で VPN を構成する (20ページ)。
5. iSeries-B 用 PPP 接続プロファイルおよび仮想回線を構成する (20ページ)。
6. iSeries-A および iSeries-B でパケット・ルールを活動化する (21ページ)。
7. iSeries-A から接続を開始する (22ページ)。

構成の詳細

TCP/IP が正しく作動して iSeries(TM) サーバーが通信可能であることが検証された後、このシナリオで説明する接続の構成を開始することができます。

ステップ 1: iSeries-A 上で VPN を構成する

iSeries-A 上で VPN を構成するには、以下のステップに従ってください。

1. **Internet Key Exchange ポリシーを構成する**
   a. 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。
   b. 「**Internet Key Exchange ポリシー**」を右クリックして、「**新規 Internet Key Exchange ポリシー**」を選択する。
   c. 「**リモート・サーバー**」のページで、「**IP バージョン 4 アドレス**」を ID のタイプとして選択した後、「**IP アドレス**」フィールドに 205.13.237.6 を入力する。
   d. 「**関連**」のページで、「**事前共用キー**」を選択して、この接続では事前共用キーを使用してこのポリシーを認証することを示します。
   e. 「**キー**」フィールドに事前共用キーを入力する。事前共用キーは、パスワードのように扱ってください。
   f. ローカル・キー・サーバーの ID のタイプに「**キー ID**」を選択した後、「**ID**」フィールドでキー ID を入力する。たとえば、thisisthekeyid のようになります。ローカル・キー・サーバーには、事前に知ることのできない、動的に割り当てられた IP アドレスが存在することを忘れないでください。iSeries-A が接続を開始すると、iSeries-B はこの ID を使用して iSeries-A を識別します。
   g. 「**変形**」のページで、「**追加**」をクリックして、キー保護のために iSeries-A が iSeries-B に提案した変換を追加し、フェーズ 1 のネゴシエーションの開始時に IKE ポリシーが一致保護を使用するかどうかを指定する。
   h. 「**IKE ポリシー変形**」のページで、認証メソッドには**事前共用キー**を、ハッシュ・アルゴリズムには **SHA** を、および暗号化アルゴリズムには **3DES-CBC** を指定する。それから、Diffie-Hellman グループと IKE キー満了期間にはデフォルトを受け入れます。
   i. 「**OK**」をクリックして「**変形**」のページに戻る。
   j. 「**IKE アグレッシブ・モード・ネゴシエーション (一致保護なし)**」を選択する。

   » **注:** 事前共用キーとアグレッシブ・モード・ネゴシエーションを一緒に構成で使用しなければならない場合は、ディクショナリーをスキャンするアタックで解かれそうにないわかりにくいパスワードを選択してください。パスワードを定期的に変更することもお勧めします。«

   k. 「**OK**」をクリックして、構成を保管する。
2. **データ・ポリシーを構成する**
   a. VPN インターフェースから、「**データ・ポリシー**」を右クリックして、「**新規データ・ポリシー**」を選択する。
   b. 「**一般**」のページで、データ・ポリシーの名前を指定する。たとえば、l2tpremoteuser です。
   c. 「**提案**」のページに移動する。提案は、起動側および応答側のキー・サーバーが、 2 つのエンドポイント間の動的接続を確立する際に使用する、プロトコルのコレクションです。ユーザーは、複数の接続オブジェクトで、単一のデータ・ポリシーを使用することができます。ただし、すべてのリモート VPN キー・サーバーが、同じデータ・ポリシー・プロパティーを持っているとは限りません。したがって、1 つのデータ・ポリシーに、いくつかの提案を追加することができます。リモート・キー・サーバーとの VPN 接続を確立する場合は、起動側と応答側のデータ・ポリシーの提案が、少なくとも 1 つは一致していなければなりません。
   d. 「**追加**」をクリックして、データ・ポリシー提案を追加する。
   e. カプセル化モードに「**トランスポート**」を選択する。
   f. キーの有効期限値を指定する。
   g. 「**OK**」をクリックして「**提案**」のページに戻る。

h. 「**OK**」をクリックして、新規のデータ・ポリシーを保管する。

3. **動的キー・グループを構成する**

4.

a. VPN インターフェースから、「**セキュア接続**」を展開する。

b. 「**グループ別**」を右クリックして、「**新規動的キー・グループ**」を選択する。

c. 「**一般**」のページで、グループの名前を指定する。たとえば、l2tptocorp です。

d. 「**ローカルで開始された L2TP トンネルを保護する**」を選択する。

e. システムの役割には、「**システムが両方ともホストです**」を選択する。

f. 「**ポリシー**」のページに移動する。「**データ・ポリシー**」ドロップダウン・リストから、ステップ 2 で作成したデータ・ポリシー l2tpremoteuser を選択します。

g. 「**ローカル・システムが接続を開始します**」を選択して、 iSeries-B との接続を開始できるのは iSeries-A のみであることを示す。

h. 「**接続**」のページに移動する。「**このグループに次のポリシー・フィルターを生成**」を選択します。「**編集**」をクリックして、ポリシー・フィルターのパラメーターを定義します。

i. 「**ポリシー・フィルター - ローカル・アドレス**」のページで、 ID のタイプに「**キー ID**」を選択する。

j. ID には、キー ID thisisthekeyid を選択する。この ID は IKE ポリシーで定義されています。

k. 「**ポリシー・フィルター - リモート・アドレス**」のページに移動する。「**ID のタイプ**」ドロップダウン・リストから、「**IP バージョン 4 アドレス**」を選択します。

l. 「**ID**」フィールドで 205.13.237.6 を入力する。

m. 「**ポリシー・フィルター - サービス**」のページに進む。「**ローカル・ポート**」フィールドおよび「**リモート・ポート**」フィールドで、1701 を入力します。ポート 1701 は、L2TP の事前割り当てポートです。

n. 「**プロトコル**」ドロップダウン・リストから、「**UDP**」を選択する。

o. 「**OK**」をクリックして、「**接続**」のページに戻る。

p. 「**インターフェース**」のページに移動する。このグループが適用される任意の回線または PPP プロファイルを選択します。このグループにはまだ PPP プロファイルを作成していません。このプロファイルの作成後、このグループのプロパティーを編集して、次のステップで作成する PPP プロファイルにグループが適用されるようにします。

q. 「**OK**」をクリックして、動的キー・グループ l2tptocorp を作成する。

ここで、作成したばかりのグループに接続を追加する必要があります。

5. **動的キー接続を構成する**

a. VPN インターフェースから、「**グループ別**」を展開する。これで、iSeries-A 上で構成した動的キー・グループのリストが表示されます。

b. 「**l2tptocorp**」を右クリックして、「**新規動的キー接続**」を選択する。

c. 「**一般**」のページで、接続のオプション記述を指定する。

d. リモート・キー・サーバーでは、ID のタイプに「**IP バージョン 4 アドレス**」を選択する。

e. 「**IP アドレス**」ドロップダウン・リストから、205.13.237.6 を選択する。

f. 「**要求時に開始**」の選択を解除する。

g. 「**ローカル・アドレス**」のページに移動する。 ID のタイプに「**キー ID**」を選択した後、「**ID**」ドロップダウン・リストから thisisthekeyid を選択します。

h. 「**リモート・アドレス**」のページに移動する。 ID のタイプに「**IP バージョン 4 アドレス**」を選択します。
i. 「**ID**」フィールドで 205.13.237.6 を入力する。
j. 「**サービス**」のページに移動する。「**ローカル・ポート**」フィールドおよび「**リモート・ポート**」フィールドで、1701 を入力します。ポート 1701 は、L2TP の事前割り当てポートです。
k. 「**プロトコル**」ドロップダウン・リストから、「**UDP**」を選択する。
l. 「**OK**」をクリックして、動的キー接続を作成する。

これで、iSeries-A での VPN の構成は終了しました。次のステップは、iSeries-A 用 PPP プロファイルの構成です。

ステップ 2: iSeries-A 上で PPP 接続プロファイルおよび仮想回線を構成する

このセクションでは、iSeries-A 用 PPP プロファイルを作成するために実行しなければならないステップについて説明します。PPP プロファイルは、それに関連した物理的回線は持っていません。代わりに、仮想回線を使用します。これは、PPP トラフィックが L2TP トンネル経由で通過するためです。これに対し、VPN は L2TP トンネルを保護します。

iSeries-A 用 PPP 接続プロファイルを作成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**iSeries-A**」—>「**ネットワーク**」—>「**リモート・アクセス・サービス**」と展開する。
2. 「**発信元接続プロファイル**」を右クリックし、「**新規プロファイル**」を選択する。
3. 「**セットアップ**」のページで、プロトコル・タイプに「**PPP**」を選択する。
4. モード選択では、「**L2TP (仮想回線)**」を選択する。
5. 「**作動モード**」ドロップダウン・リストから、「**オンデマンド・イニシエーター (自発的トンネル)**」を選択する。
6. 「**OK**」をクリックして、「PPP プロファイルのプロパティー」のページに移動する。
7. 「**一般**」ページで、接続のタイプと宛先を識別する名前を入力する。この場合は、toCORP と入力します。指定する名前は、10 文字以下でなければなりません。
8. (オプション) プロファイルの記述を指定する。
9. 「**接続**」のページに移動する。
10. 「**仮想回線名**」フィールドで、ドロップダウン・リストから **tocorp** を選択する。この回線には、関連した物理インターフェースがないことを思い出してください。仮想回線は、この PPP プロファイルのさまざまな特性、たとえば最大フレーム・サイズ、認証情報、ローカル・ホスト名などを、記述します。「**L2TP 回線のプロパティー**」ダイアログ・ボックスが開きます。
11. 「**一般**」ページで、仮想回線の記述を入力する。
12. 「**認証**」ページに移動する。
13. 「**ローカル・ホスト名**」フィールドで、ローカル・キー・サーバーのホスト名 iSeriesA を入力する。
14. 「**OK**」をクリックして、新しい仮想回線の記述を保管し、「**接続**」のページに戻る。
15. 「**リモート・トンネル・エンドポイント IP アドレス**」フィールドに、リモート・トンネル・エンドポイント・アドレス 205.13.237.6 を入力する。
16. 「**IP-SEC 保護が必要**」を選択し、「**接続グループ名**」ドロップダウン・リストから、ステップ 1 で作成した動的キー・グループ l2tptocorp を選択する。
17. 「**TCP/IP 設定**」ページに移動する。
18. 「**ローカル IP アドレス**」セクションで、「**リモート・システムによる割り当て**」を選択する。

19. 「**リモート IP アドレス**」セクションで、「**固定 IP アドレス を使用**」を選択する。 10.6.11.1 と入力します。これは、サブネット内のリモート・システムの IP アドレスです。
20. 経路指定セクションで、「**追加の静的経路を定義**」を選択し、「**経路**」をクリックする。 PPP プロファイルに経路指定情報が提供されない場合は、 iSeries-A は、リモート・トンネル・エンドポイントに到達できるのみであり、 10.6.0.0 サブネット上の他のシステムには到達できません。
21. 「**追加**」をクリックして、静的経路項目を追加する。
22. サブネット 10.6.0.0、およびサブネット・マスク 255.255.0.0 を入力し、すべての 10.6.*.* トラフィックを、L2TP トンネル経由で経路指定する。
23. 「**OK**」をクリックして、静的経路を追加する。
24. 「**OK**」をクリックして、「経路指定」ダイアログ・ボックスをクローズする。
25. 「**認証**」ページに移動し、この PPP プロファイルのユーザー名とパスワードを設定する。
26. 「ローカル・システムの識別」セクションで、「**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します**」を選択する。
27. 「**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。
28. ユーザー名 iSeriesA とパスワードを入力する。
29. 「**OK**」をクリックして、PPP プロファイルを保管する。

ステップ 3: l2tptocorp 動的キー・グループを toCorp PPP プロファイルに適用する

PPP 接続プロファイルを構成した後、ユーザーが作成した動的キー・グループ l2tptocorp に戻り、PPP プロファイルと関連付ける必要があります。この作業を行うには、以下のステップに従ってください。

1. VPN インターフェースにナビゲートした後、「**セキュア接続**」—>「**グループ別**」と展開する。
2. 動的キー・グループ l2tptocorp を右クリックし、「**プロパティー**」を選択する。
3. 「**インターフェース**」のページに移動し、ステップ 2 で作成した PPP プロファイル toCorp に「**このグループを適用**」を選択する。
4. 「**OK**」をクリックして、l2tptocorp を PPP プロファイル toCorp を適用する。

ステップ 4: iSeries-B 上で VPN を構成する

iSeries-A の構成に使用したものと同じステップに従い、必要に応じて、IP アドレスと ID をリバースしてください。開始する前に、以下の他の事項を考慮事項に入れてください。

- iSeries-A でローカル・キー・サーバーに指定したキー ID で、リモート・キー・サーバーを識別する。たとえば、thisisthekeyid のようになります。
- *正確に* 同じ事前共用キーを使用する。
- 変形が、iSeries-A で構成したものと確実に一致させる。これを行わないと、接続は失敗します。
- 動的キー・グループの「一**般**」のページで、「**ローカルで開始された L2TP トンネルを保護する**」を指定しないでください。
- リモート・システムが接続を開始する。
- 接続が要求時に開始しなければならないことを指定する。

ステップ 5: iSeries-B 上で PPP 接続プロファイルと仮想回線を構成する

iSeries-B 用 PPP 接続プロファイルを作成するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**iSeries-B**」—>「**ネットワーク**」—>「**リモート・アクセス・サービス**」と展開する。
2. 「**受信側接続プロファイル**」を右クリックし、「**新規プロファイル**」を選択する。

3. 「**セットアップ**」のページで、プロトコル・タイプに「**PPP**」を選択する。
4. モード選択では、「**L2TP (仮想回線)**」を選択する。
5. 「**作動モード**」ドロップダウン・リストから、「**ターミネーター (ネットワーク・サーバー)**」を選択する。
6. 「**OK**」をクリックして「PPP プロファイルのプロパティー」ページに移動する。
7. 「**一般**」ページで、接続のタイプと宛先を識別する名前を入力する。この場合は、tobranch と入力します。指定する名前は、10 文字以下でなければなりません。
8. (オプション) プロファイルの記述を指定する。
9. 「**接続**」のページに移動する。
10. ローカル・トンネル・エンドポイントの IP アドレス 205.13.237.6 を選択する。
11. 「**仮想回線名**」フィールドで、ドロップダウン・リストから **tobranch** を選択する。この回線には、関連した物理インターフェースがないことを思い出してください。仮想回線は、この PPP プロファイルのさまざまな特性、たとえば最大フレーム・サイズ、認証情報、ローカル・ホスト名などを、記述します。「**L2TP 回線のプロパティー**」ダイアログ・ボックスが開きます。
12. 「**一般**」ページで、仮想回線の記述を入力する。
13. 「**認証**」ページに移動する。
14. 「**ローカル・ホスト名**」フィールドで、ローカル・キー・サーバーのホスト名 iSeriesB を入力する。
15. 「**OK**」をクリックして、新しい仮想回線の説明を保管し、「**接続**」のページに戻る。
16. 「**TCP/IP 設定**」ページに移動する。
17. 「**ローカル IP アドレス**」セクションで、ローカル・システムの固定 IP アドレス 10.6.11.1 を選択する。
18. 「**リモート IP アドレス**」セクションで、アドレス割り当て方式として「**アドレス・プール**」を選択する。開始アドレスを入力した後、リモート・システムに割り当てることができるアドレスの数を指定します。
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。
20. 「**認証**」ページに移動し、この PPP プロファイルのユーザー名とパスワードを設定する。
21. 「ローカル・システムの識別」セクションで、「**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します**」を選択する。 これで、「**ローカル・システム識別**」ダイアログ・ボックスが開きます。
22. 「**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。
23. ユーザー名 iSeriesB とパスワードを入力する。
24. 「**OK**」をクリックして、PPP プロファイルを保管する。

ステップ 6: パケット・ルールを活動化する

VPN により、この接続が正しく作動するために必要なパケット・ルールが自動的に作成されます。ただし、VPN 接続を開始できるようにするには、その前に、両方のシステムでこれらのパケット・ルールを活動化しなければなりません。 規則の活動化を行うには、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**」と展開する。
2. 「**パケット・ルール**」を右クリックし、「**ルールの活動化**」を選択する。これにより、「**パケット・ルールの活動化**」ダイアログ・ボックスが開きます。
3. VPN で生成されたルールのみを活動化するのか、選択したファイルのみを活動化するのか、あるいは VPN で生成されたルールと選択したファイルの両方を活動化するのかを選択する。たとえば、VPN で

生成されたルールに加えて、各種の PERMIT ルールや DENY ルールをインターフェースに適用したい場合には、VPN で生成されたルールと選択したファイルの両方の活動化を選択することができます。

4. 活動化させるルールのあるインターフェースを選択する。ここでは、「**全てのインターフェースと Point-to-Point フィルター ID 上のルールの活動化**」を選択します。
5. ダイアログ・ボックス上で「**OK**」をクリックして、指定した 1 つまたは複数のインターフェースで規則の検査と活動化を実行することを確認します。「OK」をクリックすると、システムはそのルールに構文およびセマンティックのエラーがないかどうかを検査し、エディター下部のメッセージ・ウィンドウでその結果を報告します。特定のファイルおよび行番号に関連したエラー・メッセージは、エラーを右クリックし、「**行に進む**」を選択すると、ファイル内のエラーを強調表示させることができます。
6. 上記のステップを繰り返して、iSeries-B でパケット・ルールを活動化する。

ステップ 7: 接続を開始する

最終ステップは接続の開始です。 L2TP 接続を開始する前に、L2TP ターミネーターが、起動側の要求に応答できるようにしておかなければなりません。必要なサービスがすべて開始済みであるのを確認してから、ターミネーター・サイドで PPP 接続を開始してください。以下のステップは、iSeries-B 上で PPP 接続を開始する方法を説明しています。

1. iSeries ナビゲーターで、「**iSeries-B**」—>「**ネットワーク**」—>「**リモート・アクセス・サービス**」と展開する。
2. 「**受信側接続プロファイル**」をクリックして、右側のペインで受信側プロファイルのリストを表示する。
3. 「tobranch」を右クリックして、「**開始**」を選択する。接続プロファイルの開始後、ウィンドウは、「**接続要求を待機中**」として、接続を最新表示します。これで、iSeries-B は、iSeries-A からの L2TP 接続要求に応じることができます。

iSeries-A 上で L2TP 接続を開始するには、以下のステップに従ってください。

1. iSeries ナビゲーターで、「**iSeries-A**」—>「**ネットワーク**」—>「**リモート・アクセス・サービス**」と展開する。
2. 「**発信元接続プロファイル**」をクリックして、右側のペインで発信元プロファイルのリストを表示する。
3. 「**toCORP**」を右クリックして、「**開始**」を選択する。接続プロファイルの開始後、ウィンドウは、「L2TP トンネルを設定中」として、接続を最新表示します。
4. F5 を押して、画面の最新表示を行う。 L2TP トンネルが正常に開始すれば、接続状況は「アクティブ」になります。

VPN シナリオ: VPN のネットワーク・アドレス変換を使用する

あなたが、ミネアポリスにある小規模な製造業のネットワーク管理者であるとします。ビジネス・パートナーの 1 つであるシカゴの部品業者が、あなたの企業とのインターネット経由での取引を増やしたいと考えています。あなたの企業では、特定の部品を必要なときに特定の数量用意しておくことが重要であるため、部品業者は、あなたの企業の在庫状況と生産スケジュールを知っておく必要があります。現在はこの業務を手作業で処理していますが、時間と費用がかかり、さらに時として不正確な場合もあることが判明しているため、別の方法を検討したいと考えています。

やり取りする情報は機密性が高く、時間の遅れが許されないものであるため、部品業者のネットワークとあなたの企業のネットワークとの間に VPN を作成することにしました。自社のネットワーク構造のプライバ

シーをさらに保護するために、部品業者がアクセスするアプリケーションをホストする iSeries(TM) のプライベート IP アドレスを隠す必要があるという結論に達しました問題は、それをどのようにして行うのかということです。

その答えが OS/400(R) VPN です。あなたの企業のネットワークにおける VPN ゲートウェイで接続定義を作成するためだけではなく、ローカルのプライベート・アドレスを隠すために必要なアドレス変換の提供にも、 OS/400 VPN を使用してください。従来型のネットワーク・アドレス変換 (NAT) では、VPN が機能するために必要なセキュリティー・アソシエーション (SA) で IP アドレスが変更されますが、VPN NAT は、接続の開始時に、接続にアドレスを割り当てることによって、SA 検証の前にアドレス変換を実行します。

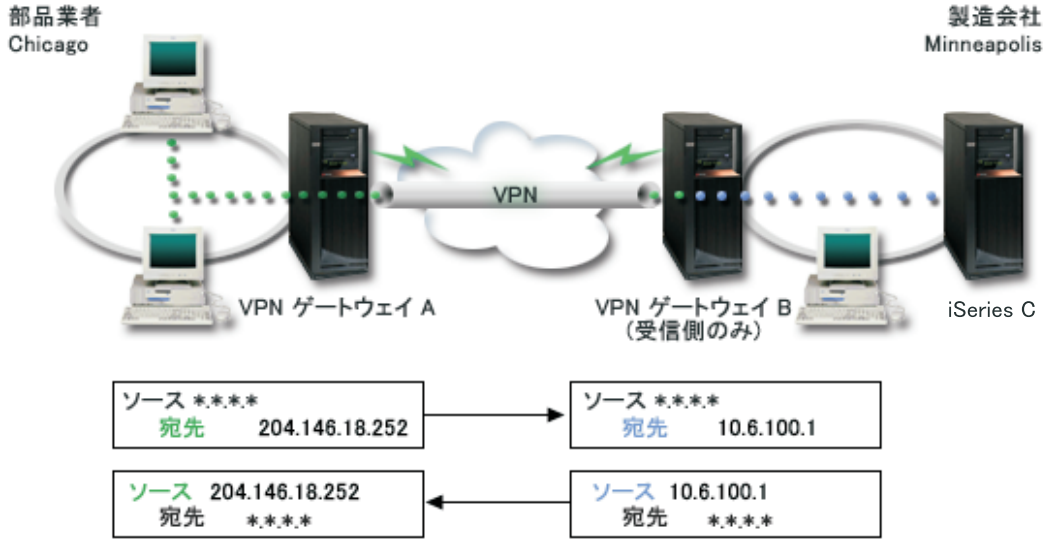
目的

このシナリオの目的は、次のとおりです。

- 部品業者のネットワーク内のすべてのクライアントが、製造会社内の単一ホスト iSeries にゲートウェイ間 VPN 接続を介してアクセスできるようにする。
- 製造会社のネットワーク内のホスト iSeries のプライベート IP アドレスを、VPN のネットワーク・アドレス変換 (VPN NAT) を使用してパブリック IP アドレスに変換することによって隠す。

詳細

次の図は、部品業者のネットワークと製造会社のネットワークの両方のネットワーク特性を表しています。



- VPN ゲートウェイ A は、常に VPN ゲートウェイ B との接続を開始するように構成されています。
- VPN ゲートウェイ A は、接続の宛先エンドポイントを 204.146.18.252 (iSeries-C に割り当てられた公衆アドレス) として定義しています。
- iSeries-C は、製造会社のネットワークで 10.6.100.1 というプライベート IP アドレスを所有しています。
- iSeries-C のプライベート・アドレス 10.6.100.1 に対応して、VPN ゲートウェイ B におけるローカル・サービス・プールで、204.146.18.252 という公衆アドレスが定義されています。
- VPN ゲートウェイ B はインバウンド・データグラムのために、iSeries-C の公衆アドレスを、そのプライベート・アドレスである 10.6.100.1 に変換します。 VPN ゲートウェイ B は、10.6.100.1 から戻されるアウトバウンド・データグラムを変換して、iSeries-C の公衆アドレス 204.146.18.252 に戻します。部

品業者のネットワーク内のクライアントについては、iSeries-C は 204.146.18.252 という IP アドレスを割り当てています。これらのクライアントには、アドレス変換が行われたことは分かりません。

構成作業

このシナリオで説明している接続を構成するには、以下の各作業を完了しなければなりません。

1. **VPN ゲートウェイ A** と **VPN ゲートウェイ B** との間で、基本ゲートウェイ間 VPN を構成する。
2. **VPN ゲートウェイ B** でローカル・サービス・プールを定義して、**iSeries-C** のプライベート・アドレスを 204.146.18.252 という公衆 ID で隠す。
3. ローカル・サービス・プールのアドレスを使用してローカル・アドレスを変換するように、**VPN ゲートウェイ B** を構成する。

VPN の概念

VPN (仮想プライベート・ネットワーク) では、いくつかの重要な TCP/IP プロトコルを使用して、データ・トラフィックを保護します。VPN 接続の仕組みをよりよく理解するためには、以下のプロトコルとその概念、および OS/400(R) VPN によるそのプロトコルと概念の使用方法を知っておかなければなりません。

- 25 ページの『IP セキュリティー (IPSec) プロトコル』
  IPSec は、ネットワーク層のセキュリティーを得るための、安定した永続的なベースを提供します。
- 28 ページの『キー管理』
  動的 VPN を使用すると、キー管理に Internet Key Exchange (IKE) を使用することにより、通信により一層のセキュリティーが提供されます。 IKE を使用すると、接続の両端にある VPN サーバーが、指定された間隔で新しいキーのネゴシエーションを行います。
- 29 ページの『レイヤー 2 トンネリング・プロトコル (L2TP)』
  VPN 接続を使用して、ネットワークとリモート・クライアント間の通信を保護する計画を立てる場合は、L2TP についても、十分に理解する必要があります。
- 30 ページの『VPN のネットワーク・アドレス変換』
  OS/400 VPN を使用すると、VPN NAT と呼ばれるネットワーク・アドレスネットワーク・アドレス変換を実行することができます。 VPN NAT は、IKE プロトコルと IPSec プロトコルを適用する前にアドレスを変換するという点で、従来の NAT と異なります。詳細については、このトピックを参照してください。
- 31 ページの『NAT 互換 IPSec』
  UDP カプセル化を使用すると、従来型の NAT デバイスを介して IPSec トラフィックを受け渡すことができます。 UDP カプセル化の詳細、および VPN 接続に UDP カプセル化を使用しなければならない理由については、このトピックを参照してください。
- 32 ページの『IP 圧縮 (IPComp)』
  IPComp は、データグラムを圧縮することによって IP データグラムのサイズを縮小し、 2 VPN パートナー間の通信パフォーマンスを向上させます。
- 33 ページの『VPN および IP フィルター操作』
  IP フィルター操作と VPN は密接に関係しています。事実、ほとんどの VPN 接続が正しく機能するには、フィルター規則が必要です。このトピックでは、VPN に必要なフィルター、および VPN に関するその他のフィルターの概念について説明します。

IP セキュリティー (IPSec) プロトコル

IPSec は、ネットワーク層のセキュリティーを得るための、安定した永続的なベースを提供します。また、現在使用中の暗号アルゴリズムのすべてをサポートし、より新しく、より強力なアルゴリズムにも適応することができます。 IPSec プロトコルは、次に示す主なセキュリティー上の問題を処理します。

データ起点認証
各データグラムの起点が要求の送信側であることを確認します。
データ保全性
データグラムの内容が、転送中、故意またはランダム・エラーのために変更されなかったことを確認します。
データ機密性
メッセージの内容を、通常は暗号化を使用して、隠します。
再生保護機能
侵入者がデータグラムを代行受信したり、それを後で再生したりできないことを保証します。
暗号キーおよびセキュリティー・アソシエーションの自動管理
手動での構成をほとんどあるいはまったく必要とせずに、拡張ネットワーク全体に VPN ポリシーを使用できることを保証します。

データが VPN 経由で流れるときに、VPN は、認証ヘッダー (AH) とカプセル化セキュリティー・ペイロード (ESP) の 2 つの IPSec プロトコルを使用して、データを保護します。 IPSec 使用可能性のもう 1 つの部分は、Internet Key Exchange (IKE) プロトコル、すなわちキー管理です。 IPSec はデータの暗号化を行いますが、IKE は、セキュリティー・アソシエーション (SA) の自動ネゴシエーション、暗号鍵の自動生成と最新表示をサポートします。

基本的な IPSec プロトコルを以下にリストします。

- 『認証ヘッダー』
- 27 ページの『カプセル化セキュリティー・ペイロード』
- 28 ページの『AH と ESP の組み合わせ』
- 28 ページの『キー管理』

Internet Engineering Task Force (IETF) では、Request for Comment (RFC) 2401、 *Security Architecture for the Internet Protocol* において、 IPSec を正式に定義します。この RFC は、インターネットの Web サイト http://www.rfc-editor.org で参照できます。

認証ヘッダー

認証ヘッダー (AH) プロトコルには、データ起点認証、データ保全性および再生保護の機能があります。ただし、AH はデータの機密性には対応していません。つまり、データはすべてプレーン・テキストで送信されます。

AH は、メッセージ確認コード (MD5 に似たコード) が生成するチェックサムによってデータ保全性を保証します。データ起点認証を保証するために、AH は、認証に使用するアルゴリズムに共用/秘密鍵を組み込みます。再生保護を保証するには、AH ヘッダー内の順序番号フィールドが使用されます。これら 3 つの異なる機能は、多くの場合一括して扱われ、**認証**として参照されることに注意してください。最も単純な言い方をすると、AH によって、データがその最終の宛先に向かう途中で改ざんされなかったことが保証されます。

IP データグラムは、AH によって可能な限り多く認証されますが、IP ヘッダー内の特定のフィールドの値は、受信側からは予測できません。AH は、**可変**フィールドと呼ばれるこれらのフィールドを、保護しません。ただし、IP パケットのペイロードは、AH によって常に保護されます。

Internet Engineering Task Force (IETF) は、Request for Comment (RFC) 2402、*IP Authentication Header* において、AH を正式に定義します。この RFC は、インターネットの Web サイト http://www.rfc-editor.org  で参照できます。

AH の使用法
AH は、トランスポート・モードまたはトンネル・モードの 2 つの方法で、適用することができます。トランスポート・モードでは、データグラムの IP ヘッダーは、最外部 IP ヘッダー、それに続く AH ヘッダー、およびデータグラムのペイロードから構成されます。 AH は、可変フィールド以外のすべてのデータグラムを認証します。ただし、データグラムに格納される情報はプレーン・テキスト形式で送信されるため、傍受されやすくなります。トランスポート・モードに必要な処理オーバーヘッドは、トンネル・モードの場合より減少しますが、セキュリティーの程度はトンネル・モードほど高くはありません。

トンネル・モードでは、新しい IP ヘッダーを作成して、それをデータグラムの最外部 IP ヘッダーとして使用します。 AH ヘッダーは、新しい IP ヘッダーの後に追加されます。元のデータグラム (IP ヘッダーおよび元のペイロード) は、最後尾に追加されます。 AH は、データグラム全体を認証します。これは、転送中にデータグラムに変更が加えられたかどうかを、応答側システムが検出できることを意味します。

セキュリティー・アソシエーションの一方の端がゲートウェイの場合は、トンネル・モードを使用してください。トンネル・モードでは、最外部 IP ヘッダーに書き込まれた送信元アドレスと宛先アドレスは、元の IP ヘッダーに書き込まれたアドレスと同じである必要はありません。たとえば、2 つのセキュリティー・ゲートウェイによって AH トンネルを動作させ、これらのゲートウェイが互いに接続しているネットワーク間でやり取りされる、すべてのトラフィックを認証する場合があります。実際に、これは非常に典型的な構成です。

トンネル・モードを使用する主な利点は、トンネル・モードでは、カプセル化された IP データグラムが全体的に保護されることです。さらに、トンネル・モードでは、プライベート・アドレスが使用できます。

AH の使用理由
多くの場合、データに必要なのは認証のみです。 27 ページの『カプセル化セキュリティー・ペイロード』プロトコルは、認証を実行できますが、 AH は ESP ほどにはシステム性能に影響を及ぼしません。 AH を使用するもう一つの利点は、AH はデータグラム全体を認証するという点です。一方、ESP は、先頭の IP ヘッダーや、ESP ヘッダーの前にあるその他の情報を認証しません。

その上、ESP を実施するには、強固な暗号アルゴリズムが必要です。強力な暗号化機能は、いくつかの国で制限されていますが、 AH には規制がなく、世界中で自由に使用することができます。

情報保護のために AH が使用するアルゴリズム
AH では、**ハッシュ式メッセージ認証コード (HMAC)** と呼ばれるアルゴリズムを使用します。特に、VPN では HMAC-MD5 または HMAC-SHA を使用します。 MD5 と SHA は、いずれも可変長入力データおよび秘密鍵を使用して、固定長出力データ (ハッシュ値と呼ばれる) を生成します。 2 つのメッセージのハッシュ値が一致した場合、これらのメッセージは同じものである可能性が非常に高くなります。 MD5 と SHA は、どちらもその出力のメッセージ長をエンコードしますが、 SHA の生成するハッシュ値の方が大きいため、 SHA の安全性の方が高いとされています。

Internet Engineering Task Force (IETF) では、Request for Comments (RFC) 2085、 *HMAC-MD5 IP Authentication with Replay Prevention* において、HMAC-MD5 を正式に定義しています。 Internet Engineering Task Force (IETF) では、Request for Comments (RFC) 2404、 *The Use of HMAC-SHA-1-96 within ESP and AH* において、 HMAC-SHA を正式に定義しています。これらの RFC は、インターネットの Web サイト http://www.rfc-editor.org  で参照できます。

カプセル化セキュリティー・ペイロード

カプセル化セキュリティー・ペイロード (ESP) プロトコルは、データ機密性機能を提供し、さらに、オプションとして、データ起点認証、データ保全性検査および再生保護の各機能を提供します。 ESP プロトコルと 25 ページの『認証ヘッダー』 プロトコルの違いは、 ESP は暗号化機能を提供するということです。一方、認証、保全性検査、再生保護の各機能は、どちらのプロトコルでも提供されます。ESP を使用する場合、双方の通信システムは、交換するデータの暗号化や暗号解除のために共用キーを使用します。

暗号化と認証の両方を使用することにした場合、応答側システムは最初にパケットを認証し、その最初のステップが正常に行われた場合は、続いて、暗号化解除に進みます。この種の構成をとることにより、処理オーバーヘッドだけでなく、サービス妨害アタックに対するもろさを低減します。

ESP の 2 つの使用法

ESP の適用方法には、トランスポート・モードまたはトンネル・モードの 2 つがあります。トランスポート・モードでは、ESP ヘッダーは、元の IP データグラムの IP ヘッダーのあとに追加されます。データグラムにすでに IPSec ヘッダーがある場合は、 ESP ヘッダーは IPSec ヘッダーの前に追加されます。 ESP トレーラーおよびオプションの認証データは、ペイロードのあとに追加されます。

トランスポート・モードでは、IP ヘッダーを認証することも、暗号化することもしません。このため、データグラムの転送中に潜在的な侵入者にアドレッシング情報をさらす恐れがあります。トランスポート・モードに必要な処理オーバーヘッドは、トンネル・モードの場合より減少しますが、セキュリティーの程度はトンネル・モードほど高くはありません。ほとんどの場合、ホストはトランスポート・モードで ESP を使用します。

トンネル・モードでは、新しい IP ヘッダーを作成して、これをデータグラムの最外部 IP ヘッダーとして使用します。 IP ヘッダーの次には、ESP ヘッダーと元のデータグラム (IP ヘッダーおよび元のペイロード) が続きます。 ESP トレーラーおよびオプションの認証データは、ペイロードに追加されます。暗号化と認証の両方を使用する場合は、元のデータグラムは新しい ESP パケットのペイロード・データになっているので、 ESP は元のデータグラムを完全に保護します。ただし、ESP は、新しい IP ヘッダーは保護しません。ゲートウェイは、ESP をトンネル・モードで使用する必要があります。

情報の保護のために ESP が使用するアルゴリズム

ESP では、双方の通信システムが、交換するデータの暗号化や暗号化解除に使用する対象鍵を使用します。送信側と受信側は、両者の間でセキュア通信を行う前に、このキーについて合意しておく必要があります。 OS/400(R) VPN では、暗号化にデータ暗号化規格 (DES)、Triple-DES (3DES)、RC5、RC4、または Advanced Encryption Standard (AES) を使用します。

Internet Engineering Task Force (IETF) では、Request for Comment (RFC) 1829、 *The ESP DES-CBC Transform* において、 DES を正式に定義しています。Internet Engineering Task Force (IETF) では、RFC 1851、 *The ESP Triple DES Transform* において、 3DES を正式に定義しています。これらの RFC およびその他の RFC は、インターネットの Web サイト http://www.rfc-editor.org で参照できます。

ESP では、HMAC-MD5 アルゴリズムおよび HMAC-SHA アルゴリズムを使用して、認証機能を提供します。 MD5 と SHA は、いずれも可変長入力データおよび秘密鍵を使用して、固定長出力データ (ハッシュ値と呼ばれる) を生成します。 2 つのメッセージのハッシュ値が一致した場合、これらのメッセージは同じものである可能性が非常に高くなります。 MD5 と SHA は、どちらもその出力のメッセージ長をエンコードしますが、 SHA の生成するハッシュ値の方が大きいため、 SHA の安全性の方が高いとされています。

Internet Engineering Task Force (IETF) では、Request for Comments (RFC) 2085、 *HMAC-MD5 IP Authentication with Replay Prevention* において、HMAC-MD5 を正式に定義しています。 Internet Engineering Task Force (IETF) では、Request for Comments (RFC) 2404、 *The Use of HMAC-SHA-1-96 within ESP and AH* において、 HMAC-SHA を正式に定義しています。これらの RFC およびその他の RFC は、インターネットの Web サイト http://www.rfc-editor.org  で参照できます。

AH と ESP の組み合わせ

VPN を使用すると、トランスポート・モードでのホスト間接続に、 AH と ESP を組み合わせて使用することができます。 これらのプロトコルを組み合わせると、IP データグラム全体が保護されます。 2 つのプロトコルを組み合わせることでセキュリティー・レベルは向上しますが、これに伴う処理オーバーヘッドの方が、セキュリティー・レベル向上のメリットを上回る場合があります。

キー管理

VPN サーバーは、ネゴシエーションの結果が正常なときにのみ、接続を保護するキーを再生成するため、侵入者はこの接続から情報を収集することがより困難になります。さらに、完全先行秘密性を使用すると、侵入者は、過去のキー生成情報をベースにして今後使用するキーを推論することができなくなります。

VPN キー・マネージャーは、IBM(TM) の Internet Key Exchange (IKE) プロトコルの実装プログラムです。 キー・マネージャーは、セキュリティー・アソシエーション (SA) の自動ネゴシエーション、ならびに暗号キーの自動生成と最新表示をサポートします。

セキュリティー・アソシエーション (SA) には、 IPSec プロトコルの使用に必要な情報が格納されています。たとえば、SA によって、アルゴリズムの種類、キーの長さと存続期間、参加者、カプセル化モードが識別できます。

暗号キーは、情報がその最終の宛先に問題なく到達するまで、文字どおり、情報に鍵を掛ける、つまり情報を保護する機能を持っています。

注: セキュアでプライベートな接続を確立するには、キーを保護されるように生成することが最も重要な要因です。キーが損なわれると、認証と暗号化がいかに強固でも、その労力は無駄になります。

キー管理のフェーズ

VPN キー・マネージャーでは、その実装時に 2 つの異なるフェーズを使用します。

フェーズ 1

フェーズ 1 では、ユーザーのデータ・トラフィックを保護するために、後続の 暗号キーの派生元となるマスター秘密鍵を設定します。 このことは、2 つのエンドポイント間でセキュリティーが保護されていない場合でも、当てはまります。VPN は、フェーズ 1 のネゴシエーションを認証するため、および後続のフェーズ 2 でのネゴシエーション時に流れる IKE メッセージを保護するキーを設定するために、RSA シグニチャー・モードまたは事前共用キーのいずれかを使用します。

事前共用キー は、128 文字までの長さの非単純ストリングです。接続の両端では、事前共用キーが一致している必要があります。事前共用キーを使用する利点は、その簡単さにあります。欠点は、IKE ネゴシエーションに先立って、共用されている秘密を (たとえば電話や登録済みメールを通じて) 外部に発信しなければならないことです。事前共用キーは、パスワードのように扱ってください。

RSA シグニチャー 認証は、事前共用キーより安全です。これは、このモードではディジタル証明書を使用して認証を与えているためです。 ディジタル証明書マネージャー (5722-SS1 オプション 34) を使用して、ディジタル証明書を構成しなければなりません。さらに、一部の VPN ソリューション

には、相互運用性のための RSA シグニチャーが必要です。たとえば、Windows(R) 2000 VPN は、RSA シグニチャーをデフォルトの認証方式として使用します。最後に、RSA シグニチャーには、事前共用キーよりも優れたスケーラビリティーが備わっています。ユーザーが使用する証明書は、両方のキー・サーバーが信頼する認証局が出した証明書でなければなりません。

フェーズ 2
一方、フェーズ 2 では、実際に交換されるアプリケーション・データを保護する、セキュリティー・アソシエーションとキーのネゴシエーションを行います。 この時点までは、実際に送信されるアプリケーション・データはないことに注意してください。フェーズ 1 は、フェーズ 2 の IKE メッセージを保護します。

フェーズ 2 のネゴシエーションが完了すると、VPN は、ネットワーク上および、ユーザーが接続用に定義したエンドポイント間で、セキュアな動的接続を確立します。 VPN でやり取りされるすべてのデータは、フェーズ 1 およびフェーズ 2 のネゴシエーション処理時に、キー・サーバーが承諾したセキュリティー・レベルおよび効率で転送されます。

通常、フェーズ 1 のネゴシエーションは、一日に一度ネゴシエーションされますが、フェーズ 2 のネゴシエーションは 60 秒ごとに、または 5 分に一度の頻度で更新されます。更新頻度を上げると、データのセキュリティー・レベルは向上しますが、システム性能が低下します。最も重要なデータを保護するときは、キー存続期間を短く設定してください。

iSeries(TM) ナビゲーターを使用して動的 VPN を作成する際には、 44 ページの『Internet Key Exchange (IKE) ポリシーを構成する』し、フェーズ 1 のネゴシエーションと 44 ページの『データ・ポリシーを構成する』を使用可能にして、フェーズ 2 のネゴシエーションを管理しなければなりません。オプションとして、「新規接続」ウィザードを使用することができます。このウィザードでは、VPN が正しく作動するために必要な、IKE ポリシーやデータ・ポリシーなどを含む、各構成オブジェクトが自動的に作成されます。

推奨参考文献
Internet Key Exchange (IKE) プロトコルおよびキー管理について、さらに詳しい情報を知りたい場合は、次に示す、Internet Engineering Task Force (IETF) の Request for Comments (RFC) を参照してください。

- RFC 2407、*The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408、*Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409、*The Internet Key Exchange (IKE)*

これらの RFC は、インターネットの Web サイト、 http://www.rfc-editor.org  で参照できます。

レイヤー 2 トンネリング・プロトコル (L2TP)

仮想回線とも呼ばれるレイヤー 2 トンネリング・プロトコル (L2TP) 接続では、リモート・ユーザーに割り当てた IP アドレスを、企業のネットワーク・サーバーで管理することができ、これによって、リモート・ユーザーに経済的なアクセスを提供します。さらに、IP セキュリティー (IPSec) と L2TP 接続を一緒に使用すると、システムやネットワークへのアクセスをセキュアに行うことができます。

L2TP は、任意トンネルと強制トンネルの 2 つのトンネル・モードをサポートします。この 2 つのトンネル・モードの主な違いは、エンドポイントです。任意トンネルでは、トンネルの終点はリモート・クライアントですが、強制トンネルでは ISP です。

L2TP の**強制トンネル**では、リモート・ホストが、インターネット・サービス・プロバイダー (ISP) への接続を開始します。続いて ISP が、リモート・ユーザーと企業ネットワークとの間に L2TP 接続を確立しま

す。接続は ISP によって確立されますが、VPN の使用によるトラフィックの保護方法は、ユーザーが決定します。 強制トンネルでは、ISP が LT2P をサポートしていなければなりません。

L2TP の**任意トンネル**では、接続はリモート・ユーザーが構築します。その一般的な方法は、L2TP トンネル・クライアントを使用するというものです。つまり、リモート・ユーザーは L2TP パケットを ISP に送信し、 ISP がそのパケットを、企業ネットワークに転送します。任意トンネルでは、ISP が L2TP をサポートしている必要はありません。 *15 ページの『VPN シナリオ: IPSec によって L2TP 任意トンネルを保護する』では、VPN によって L2TP を保護し、ゲートウェイ iSeries を介して会社のネットワークに接続するように事業所の iSeries(TM) を構成する方法の例を示しています。

» IPSec によって保護された L2TP 任意トンネルの概念に関するビジュアル表示を表示できます。これを行うには、Flash プラグイン が必要です。あるいは、この表示の HTML 版を使用できます。 «

L2TP は、実際には一種の IP カプセル化プロトコルです。 L2TP トンネルは、L2TP フレームを、ユーザー・データグラム・プロトコル (UDP) パケットの内部にカプセル化し、次にその UDP パケットを、 IP パケットの内部にカプセル化することによって作成されます。この IP パケットの送信元アドレスと宛先アドレスによって、接続のエンドポイントが定義されます。外部のカプセル化プロトコルは IP なので、IPSec プロトコルは複合 IP パケットに適用することができます。これにより、L2TP トンネルの範囲内でやり取りされるデータが保護されます。こうすると、認証ヘッダー (AH)、カプセル化セキュリティー・ペイロード (ESP)、および Internet Key Exchange (IKE) プロトコルを、直接適用することができます。

ユニバーサル・コネクションを介して、IBM (R) に接続する場合の L2TP の使用法の例については、『シナリオ: リモート PPP ダイヤルアップ接続を構成する』を参照してください。

VPN のネットワーク・アドレス変換

ネットワーク・アドレス変換 (NAT) は、プライベート IP アドレスを取り入れ、パブリック IP アドレスに変換します。この作業は、ネットワーク内のホストがインターネット (または他の共通ネットワーク) を介してサービスとリモート・ホストに同時にアクセスできるようにするときに、重要な共通アドレスを保存するのに役立ちます。

さらに、プライベート IP アドレスを使用すると、着信 IP アドレスが競合するようなことがあります。たとえば、別のネットワークと通信する必要があり、どちらのネットワークも 10.*.*.* というアドレスを使用している場合が考えられます。これは、アドレスが競合し、すべてのパケットが除去される原因になります。NAT をアウトバウンド・アドレスに適用することにより、この問題が解決されます。ただし、データ・トラフィックが VPN によって保護されている場合、従来型 NAT は作動しません。これは、従来型 NAT では、VPN が機能するために必要なセキュリティー・アソシエーション (SA) での IP アドレスを変更するためです。この問題を回避するために、VPN は VPN NAT という独自のバージョンのネットワーク・アドレス変換を提供しています。 VPN NAT は、接続の開始時に、接続にアドレスを割り当てることによって、SA 検証の前にアドレス変換を実行します。アドレスは、接続を削除するまで、その接続に関連付けられたままです。

注: 現時点では、FTP は VPN NAT をサポートしません。

どのように VPN NAT を使用すべきか

開始する前に考慮する必要がある VPN NAT には、異なる 2 つのタイプがあります。この異なる 2 つのタイプは、次のとおりです。

IP アドレスの競合を回避するための VPN NAT

このタイプの VPN NAT を使用すると、同じようなアドレッシング体系を持つネットワークまたはシ

ステム間に、 VPN 接続を構成したときに生じる可能性のある、 IP アドレスの競合を回避することができます。代表的な例は、2 つの企業が、指定されたプライベート IP アドレス範囲の 1 つを使用して VPN 接続を構築する場合です。たとえば、10.*.*.* を使用します。この種の VPN NAT の構成方法は、サーバーが VPN 接続の起動側か応答側かによって異なります。サーバーが接続開始側のときは、ローカル・アドレスを、 VPN 接続パートナーのアドレスと互換性を持つアドレスに変換することができます。サーバーが接続応答側のときは、VPN パートナーのリモート・アドレスを、ローカル・ アドレッシング体系と互換性を持つアドレスに変換することができます。このタイプのアドレス変換は、動的接続の場合にのみ構成してください。

ローカル・アドレスを隠すための VPN NAT
このタイプの VPN NAT は、主として、アドレスを、公に使用できるようにした別のアドレスに変換することによって、ローカル・システムの実際の IP アドレスを隠すために使用されます。 VPN NAT を構成すると、パブリック IP アドレスの 1 つ 1 つを、隠しアドレス・プールのいずれか 1 つに変換するように、指定することができます。これによって、複数のアドレスにわたって、個々のアドレスのトラフィックの負荷バランスをとることができます。ローカル・アドレスの VPN NAT では、サーバーがその接続に対する応答側として機能する必要があります。

以下の質問の答えが「はい」の場合は、ローカル・アドレスを隠すために VPN NAT を使用してください。

1. VPN を使用したアクセスを許可しているサーバーは、1 台以上ありますか。
2. システムの実際の IP アドレスについて柔軟性が必要ですか。
3. グローバルなルーティング可能な IP アドレスを 1 つ以上持っていますか。

シナリオ「*22 ページの『VPN シナリオ: VPN のネットワーク・アドレス変換を使用する』*」では、iSeries(TM) でローカル・アドレスを隠すために VPN NAT を構成する方法の例を示しています。

iSeries で VPN NAT をセットアップするための段階的な手順については、iSeries ナビゲーターの VPN インターフェースから使用可能なオンライン・ヘルプを参照してください。

NAT 互換 IPSec

問題: 従来型の NAT により VPN が中断される

ネットワーク・アドレス変換 (NAT) を使用すると、未登録のプライベート IP アドレスを登録済み IP アドレスのセットで隠すことができます。これは、社内ネットワークを外部ネットワークから保護するうえで役立ちます。 NAT を使用すると、多くのプライベート・アドレスを少数の登録済みアドレスのセットで表すことができるため、IP アドレス不足問題の緩和にも役立ちます。

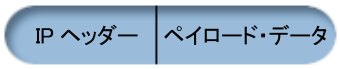
あいにく、従来型の NAT は IPSec パケットでは使用することができません。パケットが NAT デバイスを経由する際に、パケット内のソース・アドレスが変更され、パケットが無効となってしまうためです。このような場合、VPN 接続の受信側がパケットを廃棄し、VPN 接続のネゴシエーションは失敗します。

解決策: UDP カプセル化
簡潔に言うと、UDP カプセル化は、新規の (ただし複製の) IP/UDP ヘッダー内に IPSec パケットをラップします。新規 IP ヘッダー内のアドレスは、NAT デバイスを通過する際に変換されます。次に、パケットが宛先に到達すると、受信側によって追加ヘッダーが除去され、オリジナルの IPSec パケットが残されます。この IPSec パケットは、他のすべての妥当性検査にパスします。

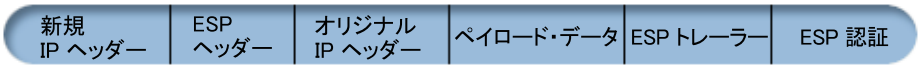
UDP カプセル化は、トンネル・モードまたはトランスポート・モードで IPSec ESP を使用する VPN にのみ適用することができます。さらに、V5R2 では、iSeries(TM) サーバーは UDP カプセル化に関してはクライアントとしてしか振る舞うことができません。つまり、UDP カプセル化されたトラフィックを開始する ことしかできません。

以下の図は、トンネル・モードにおける、UDP カプセル化された ESP パケットのフォーマットを表しています。

オリジナルの IPv4 データグラム



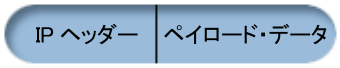
トンネル・モードでの IPSec ESP の適用後



UDP カプセル化の適用後

以下の図は、トランスポート・モードにおける、UDP カプセル化された ESP パケットのフォーマットを表しています。

オリジナルの IPv4 データグラム



トランスポート・モードでの IPSec ESP の適用後

UDP カプセル化の適用後

» パケットがカプセル化されると、iSeries は UDP ポート 4500 を介してそのパケットを VPN パートナーに送信します。通常は、VPN パートナーは、UDP ポート 500 を介して IKE ネゴシエーションを行います。ただし、キー・ネゴシエーション中に IKE が NAT を検出すると、後続の IKE パケットはソース・ポート 4500、宛先ポート 4500 を介して送信されます。このことは、適用できるどのフィルター規則においても、ポート 4500 が制限されていない必要があることも意味します。 IKE パケットでは UDP ペイロードの最初の 4 バイトがゼロに設定されているため、接続の受信側では、そのパケットが IKE パケットであるか、あるいは UDP カプセル化されたパケットであるかを判断することができます。接続が正しく機能するためには、接続の両側で UDP カプセル化がサポートされていなければなりません。 «

IP 圧縮 (IPComp)

IP ペイロード圧縮プロトコル (IPComp) は、データグラムを圧縮することによって IP データグラムのサイズを縮小し、 2 パートナー間の通信パフォーマンスを向上させます。意図は、通信の速度が低下しすぎ

たり、または混雑したリンクの場合に、通信全体のパフォーマンスを向上させることです。 IPComp にはセキュリティーが備わっておらず、VPN 接続を介して通信する場合には、AH 変換または ESP 変換のいずれかと一緒に使用しなければなりません。

Internet Engineering Task Force (IETF) は、Request for Comments (RFC) 2393、*IP ペイロード圧縮プロトコル (IPComp)* において、IPComp を正式に定義しています。この RFC は、インターネットの Web サイト、 http://www.rfc-editor.org  で参照できます。

VPN および IP フィルター操作

ほとんどの VPN 接続が正しく機能するには、フィルター規則が必要です。必要なフィルター規則は、構成しようとしている VPN 接続のタイプ、および制御対象となるトラフィックのタイプによって異なります。一般には、それぞれの接続ごとにポリシー・フィルターが用意されます。ポリシー・フィルターは、VPN を使用することができるアドレス、プロトコル、およびポートを定義します。さらに、Internet Key Exchange (IKE) プロトコルをサポートする接続では、通常、その接続を介した IKE 処理を許可するための規則が明示的に書かれています。

V5R1 以降のオペレーティング・システムでは、VPN はこれらのルールを自動的に生成することができます。可能な場合には、VPN にポリシー・フィルターを生成させるようにしてください。このようにすると、エラーを避けることができるだけでなく、iSeries(TM) ナビゲーターのパケット・ルール・エディターを使用して別のステップでルールを構成するという必要がなくなります。

当然ながら、例外も存在します。特定の状況に適用することのある、その他のあまり一般的でない VPN およびフィルター操作の概念と技法については、以下のトピックを参照してください。

- **『現行リリースへのポリシー・フィルターの移行』**
  オペレーティング・システムの V4R4 および V4R5 では、VPN パケット・ルールを別のステップとして構成しなければなりませんでした。 パケット・ルールは、VPN 構成の一部として自動的に生成されませんでした。このトピックでは、V4R4 および V4R5 のポリシー・フィルターを現行リリースに移行するための、特別な考慮事項と移行の方法について詳しく説明しています。
- **35 ページの『ポリシー・フィルターを使用しない VPN 接続』**
  VPN の接続エンドポイントが単一の特定な IP アドレスであり、システムでフィルター規則を作成または活動化せずに VPN を開始したい場合には、動的ポリシー・フィルターを構成することができます。このトピックでは、動的ポリシー・フィルターの使用を考慮すべき理由を説明し、また、その方法を概説しています。
- **35 ページの『暗黙的な IKE』**
  VPN のために IKE ネゴシエーションが行われるようにするためには、このタイプの IP トラフィックで UDP データグラムがポート 500 を通過できるように許可する必要があります。ただし、IKE トラフィックを許可するように明示されたフィルター規則がシステムに存在しない場合、システムは、IKE トラフィックが流れることを暗黙的に許可します。 iSeries でこれがどのように機能するのかについての詳細は、このトピックを参照してください。

現行リリースへのポリシー・フィルターの移行

オペレーション・システムの V4R4 および V4R5 では、iSeries(TM) ナビゲーターの「パケット・ルール」インターフェースで、VPN パケット・ルールを別のステップとして構成しなければなりませんでした。 パケット・ルールは、VPN 構成の一部として自動的に生成されませんでした。 V5R1 以降のオペレーティング・システムでは、VPN GUI はこれらのパケット・ルールを自動的に作成することができます。

V4R4 または V4R5 でポリシー・フィルター規則 (action=IPSEC の規則) を作成していて、現行リリースでもそれらの規則を使用する場合には、考慮する必要のある事項がいくつか存在します。あるいは、VPN

にポリシー・フィルター規則を生成させる としても、他の IP トラフィック (たとえば Telnet) が接続を通過できるようにするための規則を別途追加する必要があります。潜在的な構成エラーの回避に役立つ、以下の勧告に従ってください。

明確な理解のために: このトピックで *カスタマー* 規則ファイルと表記されている場合、iSeries ナビゲーターのパケット・ルール・エディターを使用して作成したあらゆる規則ファイルを指しています。この規則ファイルを、VPN が VPN 構成の一部として自動的に生成する *VPNPOLICYFILTERS.I3P* 規則ファイルと対比してください。

- V4R4 または V4R5 のいずれかより VPN 接続が構成されており、現行リリースで他の VPN 接続を構成することを計画していない場合は、現行のフィルター規則を活動化して、従来どおり接続を開始することができます。
- V4R4 または V4R5 のいずれかの VPN 接続が構成されていて、現行リリースでの新規 VPN 接続の構成を計画している場合は、「**ポリシー・フィルターの移行 (Migrate Policy Filters)**」ウィザードを使用します。このウィザードは、ユーザーの作成したパケット・ルール・ファイルからポリシー・フィルターを除去し、VPN が生成した VPNPOLICYFILTERS.I3P に同等のポリシー・フィルターを挿入します。このウィザードにアクセスするには、以下のステップに従ってください。
  1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして、「**ポリシー・フィルターの移行 (Migrate Policy Filters)**」を選択する。
  3. ウィザードが完了した後、「**完了**」をクリックする。
  4. ページまたはその中のいずれかのフィールドの記入方法についての質問がある場合は、「**ヘルプ**」をクリックする。
- VPN によりポリシー・フィルター規則を生成した場合で、VPN 以外のフィルター規則を追加する必要がある場合には、iSeries ナビゲーターのパケット・ルール・エディターを使用して、これらの規則を構成しなければなりません。これらの VPN 以外のフィルター規則のいずれかを VPN フィルターよりも前に置く必要がある場合には、そのセット名を `PREIPSEC` で始めてください。たとえば、`PREIPSECMYRULES` のようにします。これにより、システムが、フィルター規則を処理する順序を判別できるようになります。その他のすべての VPN 以外の規則のセット名には、`PREIPSEC` 接頭部を付けてはなりません。たとえば、`MORERULES` のようにします。
- 常に VPN がポリシー・フィルター規則を作成できるようにしてください。ただし、VPN 以外のフィルター規則がカスタマー規則ファイルに残っていなければなりません。これらの VPN 以外のフィルターのいずれかを、VPNPOLICYFILTERS.I3P 規則ファイルにあるポリシー・フィルターの前に置く必要がある場合には、セット名の先頭に `PREIPSEC` を追加する必要があることを忘れないでください。これにより、カスタマー規則と VPN を、ユーザーが意図したとおりに併用できるようになります。たとえば、VPN がポリシー・フィルター規則 (VPN セット) を生成した場合に、他の IP トラフィックがその接続を通過できるようにするために、追加規則 (ユーザー・セット) を付け加えたとします。これらの規則をシステムにロードすると、その順序は次のようになります。
  1. 名前が PREIPSEC で始まるユーザー・セット
  2. 名前が PREIPSEC で始まる VPN セット
  3. ACTION=IPSEC (ポリシー・フィルター) が指定された VPN セット
  4. ACTION=IPSEC (ポリシー・フィルター) が指定されたユーザー・セット
  5. その他の値が指定されたユーザー・セット
  6. その他の値が指定された VPN セット

EXPANDED.OUT ファイルをチェックして、マージされた出力ファイルの順序を表示します。EXPANDED.OUT は、カスタマー規則ファイルがあるディレクトリーに書き込まれます。

- iSeries ナビゲーターを使用することにより、以下のような活動化を選択することができます。
  - VPN により生成された規則ファイル VPNPOLICYFILTERS.I3P のみを活動化する
  - カスタマー規則ファイルのみを活動化する
  - VPN により生成された規則ファイルとカスタマー規則ファイルの両方を活動化する
- 個々のインターフェースごとにではなく、すべてのインターフェースでフィルター規則を活動化する。これは、フィルターがポリシー・フィルターを活動化し、正しい順序のポリシー・フィルターをも確実に設定するために役に立ちます。
- フィルター規則を活動化しようとする前に、フィルター規則を常に検査してください。検証がエラーなしで実行されたら、次に、EXPANDED.OUT をチェックして、規則の順序がユーザーの意図どおりであるかを確認します。このステップが完了したら、規則を活動化することができます。

ポリシー・フィルターを使用しない VPN 接続

ポリシー・フィルター規則は、VPN を使用できるアドレス、プロトコル、およびポートを定義し、接続を介して適切なトラフィックを送信します。場合によっては、ポリシー・フィルター規則を必要としない接続を構成することができます。たとえば、VPN 接続が使用するインターフェースに VPN 以外のパケット・ルールがあるため、そのインターフェースで活動中の規則を非活動化するのではなく、その接続に関するすべてのフィルターをシステムが動的に管理できるように VPN を構成することにしたと仮定します。このようなタイプの接続のポリシー・フィルターを、**動的ポリシー・フィルター**と呼びます。 VPN 接続で動的ポリシー・フィルターを使用するためには、その前に、以下のすべての条件が満たされていなければなりません。

- その接続はローカル・サーバーからのみ開始することができる。
- その接続のデータ・エンドポイントは単一システムでなければならない。つまり、サブネットあるいは一定範囲のアドレスにすることはできない。
- その接続に関するポリシー・フィルター規則をロードすることはできない。

接続がこの基準を満たす場合には、ポリシー・フィルターを必要としないように接続を構成することができます。この接続が開始されると、データ・エンドポイント間のトラフィックは、他のどのようなパケット・ルールがシステムにロードされていても、その接続を介して流れるようになります。

ポリシー・フィルターを必要としないように接続を構成するための段階的な手順については、VPN の オンライン・ヘルプを参照してください。

暗黙的な IKE

接続を確立するために、ほとんどの VPN では、IPSec 処理の前に Internet Key Exchange (IKE) ネゴシエーションが行われる必要があります。 IKE は事前割り当てポート 500 を使用するため、IKE が正しく動作するには、このタイプの IP トラフィックでポート 500 を UDP データグラムが通過できるようにする必要があります。 IKE トラフィックを許可するように明示されたフィルター規則がシステムに存在しない場合、IKE トラフィックが暗黙的に許可されます。 ただし、UDP ポート 500 トラフィックについて明示された規則は、活動状態のフィルター規則で定義されている内容に基づいて処理されます。

VPN の計画

計画の立案は、VPN ソリューションの最も重要な部分です。接続が正しく動作することを確認するには、複雑な決定を多数行う必要があります。以下の資源を使用して、VPN を確実に正常動作させるために必要なすべての情報を収集してください。

- 『VPN セットアップ要件』
  セットアップを始める前に、VPN を構築するための最低要件を満たしていることを確認してください。
- 『構築する VPN のタイプを決定する』
  VPN の使用方法を決定することは、計画を成功させる最初のステップの 1 つです。このトピックでは、構成可能なさまざまな接続タイプについて説明しています。
- **VPN 計画アドバイザーを使用する**
  計画アドバイザーは、ネットワークに関して質問し、その答えに基づいて、VPN の作成に関する提案を行います。
  注: VPN 計画アドバイザーは、Internet Key Exchange (IKE) プロトコルをサポートする接続にのみ使用してください。手動接続タイプの手動接続には、計画ワークシートを使用してください。
- 37 ページの『VPN 計画ワークシートを完成する』
  希望に応じて、VPN の使用計画についての詳細情報を収集するには、計画ワークシートを印刷して完成することができます。

VPN の計画が定まったら、41 ページの『VPN を構成する』を開始することができます。

VPN セットアップ要件

VPN を iSeries(TM) 上で、およびネットワーク・クライアントと共に正しく機能させるためには、iSeries およびクライアント PC で以下の要件を確実に満たしてください。

V5R2 iSeries の要件

- OS/400(R) バージョン 5 リリース 2 (5722-SS1) 以降
- ディジタル証明書マネージャー (5722-SS1 オプション 34)
- Cryptographic Access Provider (5722-AC2 または AC3)
- iSeries Access for Windows(R)(5722-XE1) および iSeries ナビゲーター
  - iSeries ナビゲーターのネットワーク構成要素
- サーバー・セキュリティー・データ保持 (QRETSVRSEC *SEC) のシステム値を 1 に設定すること
- TCP/IP の構成 (IP インターフェース、経路、ローカル・ホスト名、ローカル・ドメイン・ネームなど)

クライアントの要件

- iSeries に正しく接続され、TCP/IP 用に構成されている、Windows(R) 32 ビット版オペレーティング・システムを搭載したワークステーション
- 233 メガヘルツの処理装置
- Windows 95/98 クライアントの場合は、32 MB の RAM
- Windows NT(R) および 2000 クライアントの場合は、64 MB の RAM
- iSeries Access for Windows および iSeries ナビゲーターがクライアント PC に導入されていること
- IP セキュリティー (IPSec) プロトコルをサポートするソフトウェア
- リモート・ユーザーがシステムとの接続を確立するために L2TP を使用する場合は、 L2TP をサポートするソフトウェア

構築する VPN のタイプを決定する

VPN の使用方法を決定することは、計画を成功させる最初のステップの 1 つです。そのためには、ローカル・キー・サーバーとリモート・キー・サーバーが、接続で果たす役割を理解しておく必要があります。たとえば、*接続* エンドポイントと、データ ・エンドポイントとは、それぞれ異なる役割を持ちます。この両者には同じものが使用されているでしょうか、それとも別々のものが組み合わされて使用されているでしょ

うか。接続エンドポイントは、その接続のデータ・トラフィックの認証および暗号化 (あるいは暗号化解除) を行い、オプションで、Internet Key Exchange (IKE) プロトコルによる、キー管理を提供します。一方、データ・エンドポイントは、VPN を流れる IP トラフィック用の 2 つのシステム間の接続を定義します。たとえば、123.4.5.6 と 123.7.8.9 の間のすべての TCP/IP トラフィックなどです。通常は、接続エンドポイントとデータ・エンドポイントが異なる場合は、 VPN サーバーはゲートウェイの役目を果たします。両者が同じである場合は、VPN サーバーはホストとなります。

VPN の実装にはさまざまなタイプがありますが、大多数の業務上の要求に十分適合するのは、以下のものです。

ゲートウェイ間
両システムの接続エンドポイントは、データ・エンドポイントとは異なります。 IP セキュリティー (IPSec) プロトコルは、ゲートウェイ間を移動するトラフィックを保護します。ただし、IPSec は、内部ネットワーク内のゲートウェイの場合は、どちらの側でもデータ・トラフィックの保護は行いません。これは、事業所間の接続に共通のセットアップです。事業所のゲートウェイを超えて経路指定され、内部ネットワークに入ってくるトラフィックは、多くの場合トラステッドであると考えられるからです。

ゲートウェイ - ホスト間
IPSec は、ユーザーのゲートウェイとリモート・ネットワークのホストとの間のデータ・トラフィックを保護します。VPN は、ローカル・ネットワーク内のデータ・トラフィックは保護しません。それはトラステッドと考えられるためです。

ホスト - ゲートウェイ間
VPN は、ローカル・ネットワークのホストと、リモート・ゲートウェイとの間のデータ・トラフィックを保護します。 VPN は、リモート・ネットワークのデータ・トラフィックは保護しません。

ホスト間
ローカル・システムでもリモート・システムでも、接続エンドポイントはデータ・エンドポイントと同じです。 VPN は、ローカル・ネットワークのホストとリモート・ネットワークのホストとの間のデータ・トラフィックを保護します。このタイプの VPN は、終端間 IPSec の保護を提供します。

VPN 計画ワークシートを完成する

VPN の使用計画についての詳細情報を収集するには、 VPN 計画ワークシートを使用してください。この情報は、VPN の使用計画を適切に立てるために必要です。この情報を使用すると、VPN を構成することもできます。作成する接続のワークシートを選択してください。

- 38 ページの『動的接続の計画ワークシート』
  動的接続を構成する前に、このワークシートを完成してください。
- 39 ページの『手動接続の計画ワークシート』
  手動接続を構成する前に、このワークシートを完成してください。
- **VPN 計画アドバイザー**
  あるいはご希望に応じて、対話式計画および構成のガイダンスとしてアドバイザーを使用してください。計画アドバイザーは、ネットワークに関して質問し、その答えに基づいて、VPN の作成に関する提案を行います。

  注: VPN 計画アドバイザーは、動的接続の場合にのみ使用してください。手動接続タイプの手動接続には、計画ワークシートを使用してください。

同様のプロパティーを使って複数の接続を構築する場合は、 VPN のデフォルトの設定が可能です。構成したデフォルト値を持つ VPN プロパティー・シートが提供されます。つまり、同じプロパティーを何回も構成する必要はありません。 VPN デフォルトを設定するには、VPN メインメニューから、「**編集**」を選択して、次に、「**デフォルト**」を選択してください。

動的接続の計画ワークシート

動的 VPN 接続を構築するには、次のワークシートを完成させてください。ワークシートは、ユーザーが「新規接続」ウィザードを使用すると想定します。このウィザードによって、基本的なセキュリティー要件に基づいて VPN をセットアップすることができます。場合によっては、ウィザードによって構成される接続のプロパティーを更新する必要があります。たとえば、ジャーナル処理が必要であるか、または、TCP/IP が起動するたびに VPN サーバーを起動する必要があるかを決定します。この場合は、ウィザードによって作成された動的キー・グループまたは接続を右クリックして、「**プロパティー**」を選択します。

以下の各質問に答えてから、VPN のセットアップに進んでください。

前提条件チェックリスト	**答え**
OS/400(R) のバージョンは、V5R2 (5722-SS1) 以降ですか。	
ディジタル証明書マネージャーのオプション (5722-SS1 オプション 34) は、導入してありますか。	
Cryptographic Access Provider (5722-AC2 または AC3) は、導入してありますか。	
iSeries(TM) Access(5722-XE1) は、導入してありますか。	
iSeries ナビゲーターは、導入してありますか。	
iSeries ナビゲーターのネットワーク構成サブコンポーネントは、導入してありますか。	
TCP/IP 接続ユーティリティー OS/400 用 (5722-TC1) は、導入してありますか。	
サーバー・セキュリティー・データ保存 (QRETSVRSEC *SEC) のシステム値を、 1 に設定しましたか。	
iSeries で TCP/IP は構成されていますか (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・ネームなど)。	
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ますか。	
最新のプログラム一時修正 (PTF) を適用していますか。	
VPN トンネルが、IP パケット・フィルターを使用しているファイアウォールまたはルーターを横断する場合、ファイアウォールまたはルーター・フィルターの規則により、AH および ESP プロトコルはサポートされていますか。	
ファイアウォールまたはルーターは、IKE (UDP ポート 500)、AH プロトコル、および ESP プロトコルを許可するように構成されていますか。	
ファイアウォールは、IP 転送を使用可能にするように構成されていますか。	

動的 VPN 接続を構成するために必要な情報	**答え**
作成している接続のタイプ • ゲートウェイ間 • ホスト - ゲートウェイ間 • ゲートウェイ - ホスト間 • ホスト間	
動的キー・グループに付ける名前	

動的 VPN 接続を構成するために必要な情報	答え
キーの保護に必要なセキュリティーとシステム・パフォーマンスのタイプ • セキュリティー・レベルは高く、パフォーマンスは低い • セキュリティー・レベルとパフォーマンスのバランスを取る • セキュリティー・レベルは低く、パフォーマンスは高い	
接続を認証するための証明書を使用していますか。 使用していない場合は、事前共用キーは何ですか。	
ローカル・キー・サーバーの ID は、何ですか。	
ローカル・データ・エンドポイントの ID は、何ですか。	
リモート・キー・サーバーの ID は、何ですか。	
リモート・データ・エンドポイントの ID は、何ですか。	
データの保護に必要なセキュリティーとシステム・パフォーマンスのタイプ • セキュリティー・レベルは高く、パフォーマンスは低い • セキュリティー・レベルとパフォーマンスのバランスを取る • セキュリティー・レベルは低く、パフォーマンスは高い	

手動接続の計画ワークシート

次のワークシートを完成させて、キー管理に IKE を使用しない VPN (仮想プライベート・ネットワーク) 接続の作成に役立ててください。

以下の各質問に答えてから、VPN のセットアップに進んでください。

前提条件チェックリスト	答え
OS/400(R) のバージョンは、V5R2 (5722-SS1) 以降ですか。	
ディジタル証明書マネージャーのオプション (5722-SS1 オプション 34) は、導入してありますか。	
Cryptographic Access Provider (5722-AC2 または AC3) は、導入してありますか。	
iSeries(TM) Access(5722-XE1) は、導入してありますか。	
iSeries ナビゲーターは、導入してありますか。	
iSeries ナビゲーターのネットワーク構成サブコンポーネントは、導入してありますか。	
TCP/IP 接続ユーティリティー OS/400 用 (5722-TC1) は、導入してありますか。	
サーバー・セキュリティー・データ保存 (QRETSVRSEC *SEC) のシステム値を、 1 に設定しましたか。	
iSeries で TCP/IP は構成されていますか (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・ネームなど)。	
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ますか。	
最新のプログラム一時修正 (PTF) を適用していますか。	
VPN トンネルが、IP パケット・フィルターを使用しているファイアウォールまたはルーターを横断する場合、ファイアウォールまたはルーター・フィルターの規則により、AH および ESP プロトコルはサポートされていますか。	
ファイアウォールまたはルーターは、AH プロトコルと ESP プロトコルを許可するように構成されていますか。	
ファイアウォールは、IP 転送を使用可能にするように構成されていますか。	

手動 VPN の構成に必要な情報	答え
作成している接続のタイプ • ホスト間 • ホスト - ゲートウェイ間 • ゲートウェイ - ホスト間 • ゲートウェイ間	
接続に付ける名前は、何ですか。	
ローカル接続エンドポイントの ID は、何ですか。	
リモート接続のエンドポイントの ID は、何ですか。	
ローカル・データ・エンドポイントの ID は、何ですか。	
リモート・データ・エンドポイントの ID は、何ですか。	
この接続で可能なトラフィックのタイプ (ローカル・ポート、リモート・ポート、およびプロトコル) は、何ですか。	
この接続のアドレス変換は必要ですか。詳細は、 30 ページの『VPN のネットワーク・アドレス変換』を参照してください。	
トンネル・モードまたはトランスポート・モードを使用しますか。	
接続に使用する IPSec プロトコル (AH、ESP、または ESP による AH) の詳細は、25 ページの『IP セキュリティー (IPSec) プロトコル』を参照してください。	
接続に使用する認証アルゴリズム (HMAC-MD5 か HMAC-SHA か)	
接続に使用する暗号化アルゴリズム (DES-CBC か 3DES-CBC か) **注:** 暗号化アルゴリズムを指定するのは、 IPSec プロトコルとして ESP を選択した場合のみです。	
AH インバウンド・キー MD5 を使用する場合、このキーは 16 バイトの 16 進数ストリングです。 SHA を使用する場合、このキーは 20 バイトの 16 進数ストリングです。 インバウンド・キーは、リモート・サーバーのアウトバウンド・キーと正確に一致する必要があります。	
AH アウトバウンド・キー MD5 を使用する場合、このキーは 16 バイトの 16 進数ストリングです。 SHA を使用する場合、このキーは 20 バイトの 16 進数ストリングです。 アウトバウンド・キーは、リモート・サーバーのインバウンド・キーと正確に一致する必要があります。	
ESP インバウンド・キー DES を使用する場合、このキーは 8 バイトの 16 進数ストリングです。 3DES を使用する場合、このキーは 24 バイトの 16 進数ストリングです。 インバウンド・キーは、リモート・サーバーのアウトバウンド・キーと正確に一致する必要があります。	
ESP アウトバウンド・キー DES を使用する場合、このキーは 8 バイトの 16 進数ストリングです。 3DES を使用する場合、このキーは 24 バイトの 16 進数ストリングです。 アウトバウンド・キーは、リモート・サーバーのインバウンド・キーと正確に一致する必要があります。	

手動 VPN の構成に必要な情報	答え
インバウンド・セキュリティー・ポリシー指標 (SPI) インバウンド SPI は、4 バイトの 16 進数ストリングで、先頭バイトは 00 に設定されます。 インバウンド SPI は、リモート・サーバーのアウトバウンド SPI と正確に一致する必要があります。	
アウトバウンド SPI アウトバウンド SPI は、4 バイトの 16 進数ストリングです。 アウトバウンド SPI は、リモート・サーバーのインバウンド SPI と正確に一致する必要があります。	

VPN を構成する

VPN インターフェースでは、VPN 接続を構成するための、異なる複数の方法を提供しています。構成する接続のタイプと構成の方法を決めるには、以下の説明が役立ちます。

構成すべき接続のタイプ

動的接続は、 Internet Key Exchange (IKE) プロトコルを使用して、活動中の接続を保護するキーを動的に生成し、ネゴシエーションする接続です。動的接続を使用すると、キーが定期的に自動変更されるので、この接続でやり取りされるデータには、極めて高いレベルのセキュリティーが提供されます。その結果、侵入者がキーを盗む危険性が低下します。仮に盗んだとしても、キーを解読して使用し、キーが保護しているトラフィックの流れを変えたり、トラフィックを傍受したりする時間の確保が困難になります。

一方、**手動 (42ページ)** 接続は、IKE ネゴシエーションをサポートせず、したがって、自動キー管理もサポートしません。さらに、接続の両端でいくつかの属性を構成する必要がありますが、それらの属性は完全に一致しなければなりません。手動接続では、接続が活動中の間は最新表示または変更を行わない静的キーを使用します。手動接続に関連したキーを変更するには、その手動接続を停止する必要があります。このことをセキュリティー上のリスクであると考える場合は、その代わりに、動的接続を作成することもできます。

動的 VPN 接続の構成方法

VPN は、実際には、接続の特性を定義する構成オブジェクトのグループです。動的 VPN 接続では、これらのオブジェクトがそれぞれ正常に動作することが必要です。各 VPN 構成オブジェクトの構成方法に関する具体的な情報については、以下のリンク先を参照してください。

> **ヒント:**
> 43 ページの『「新規接続」ウィザードを使用して VPN 接続を構成する』
> 通常は、動的接続はすべて、「接続」ウィザードを使用して構築できます。このウィザードは、VPN が正しく作動するために必要な、パケット・ルールを含む各構成オブジェクトを自動的に作成します。ウィザードが VPN パケット・ルールを活動化するように指定した場合は、以下のステップ 6 (*接続を開始する*) はスキップできます。それ以外の場合は、ウィザードが VPN の構成を完了した後、パケット・ルールを活動化してからでなければ、接続は開始できません。

動的 VPN 接続の構成にウィザードを使用しない場合は、次のステップに従って構成を完了してください。

1. 43 ページの『VPN セキュリティー・ポリシーを構成する』
   動的接続すべてに対し、VPN セキュリティー・ポリシーを定義しなければなりません。 Internet Key Exchange (IKE) ポリシーおよびデータ・ポリシーは、IKE が、そのフェーズ 1 およびフェーズ 2 ネゴシエーションを保護する方法を指示します。
2. 45 ページの『VPN セキュア接続を構成する』
   接続のセキュリティー・ポリシーを定義したら、次に、セキュア接続を構成しなければなりません。動

的接続の場合は、セキュア接続オブジェクトには、動的キー・グループと動的キー接続が組み込まれます。**動的キー・グループ**は、 1 つまたは複数の VPN 接続の共通特性を定義するのに対し、**動的キー接続**は、対になったエンドポイント間の個々のデータ接続の特性を定義します。動的キー接続は、動的キー・グループに含まれています。

注: VPN インターフェースの、「**動的キー・グループ - 接続**」ページで、オプション、「**ポリシー・フィルターはパケット・ルールで定義される**」を選択した場合は、次の 2 ステップ、*パケット・ルールを構成する* と、*規則のインターフェースを定義する* のみを実行する必要があります。それ以外の場合は、これらの規則は VPN 構成の一部として作成され、ユーザーが指定するインターフェースに適用されます。

常に VPN インターフェースにポリシー・フィルター規則を作成させることをお勧めします。これを行うには、「**動的キー・グループ - 接続**」ページの、「**このグループに次のポリシー・フィルターを生成**」オプションを選択します。

3. 46 ページの『VPN パケット・ルールを構成する』
   VPN 構成が完了したら、接続を介してデータ・トラフィックをやり取りできるフィルター規則を作成し、適用しなければなりません。VPN の **IPSEC より前**の規則では、 IKE に接続のネゴシエーションができるように、指定されたインターフェース上の IKE トラフィックは、すべて許可されます。 **ポリシー・フィルター**規則は、それに関連した新規動的キー・グループを使用できるアドレス、プロトコル、ポートを定義します。

   V4R4 または V4R5 から移行を行っていて、既存の VPN 接続およびポリシー・フィルターを現行リリースで引き続き使用したい場合には、 33 ページの『現行リリースへのポリシー・フィルターの移行』を参照して、古いポリシー・フィルターと新しいポリシー・フィルターが意図したとおりに併用できるようにしてください。
4. 50 ページの『VPN フィルター規則のインターフェースを定義する』
   VPN 接続を使用可能にするために必要なパケット・ルールやその他の規則を構成した後、これらの規則が適用されるインターフェースを定義する必要があります。
5. 50 ページの『VPN パケット・ルールを活動化する』
   パケット・ルールのインターフェースを定義したら、接続を開始する前に、必ずそれらを活動化しなければなりません。
6. 51 ページの『VPN 接続を開始する』
   接続を開始するには、このタスクを完了します。

手動 VPN 接続の構成方法

手動接続とは、その名のとおり、VPN プロパティーをすべて (インバウンド・キーもアウトバウンド・キーも含めて)、手動で構成する必要がある接続のことです。手動接続の構成方法に関する特定の情報を表示するには、以下のリンクをたどってください。

1. 46 ページの『手動接続を構成する』
   手動接続では、接続の特性 (セキュリティー・プロトコル、接続とデータのエンドポイントなど) を定義します。

   注: VPN インターフェースの、「**手動接続 - 接続**」ページで、オプション、「**ポリシー・フィルターはパケット・ルールで定義される**」を選択した場合は、次の 2 ステップ、*ポリシー・フィルター規則を構成する* と、*規則のインターフェースを定義する* を完了すればよいだけです。それ以外の場合は、これらの規則は VPN 構成の一部として作成されます。

常に VPN インターフェースにポリシー・フィルター規則を作成させることをお勧めします。これを行うには、「**手動接続 - 接続**」ページの、「**データ・エンドポイントと一致するポリシー・フィルターを生成**」オプションを選択します。

2. 48 ページの『ポリシー・フィルター規則を構成する』
   手動接続の属性を構成した後、接続を介してデータ・トラフィックをやり取りできるポリシー・フィルター規則を作成し、適用しなければなりません。**ポリシー・フィルター**規則では、関連した接続を使用できるアドレス、プロトコル、ポートを定義します。
3. 50 ページの『VPN フィルター規則のインターフェースを定義する』
   VPN 接続を使用可能にするために必要なパケット・ルールやその他の規則を構成した後、これらの規則が適用されるインターフェースを定義する必要があります。
4. 50 ページの『VPN パケット・ルールを活動化する』
   パケット・ルールのインターフェースを定義したら、接続を開始する前に、必ずそれらを活動化しなければなりません。
5. 51 ページの『VPN 接続を開始する』
   ローカルに開始される接続を開始するには、このタスクを完了します。

「新規接続」ウィザードを使用して VPN 接続を構成する

「新規接続」ウィザードを使用すると、ホストとゲートウェイの任意の組み合わせで、仮想プライベート・ネットワーク (VPN) を構築することができます。たとえば、ホスト間、ゲートウェイ - ホスト間、ホスト - ゲートウェイ間、ゲートウェイ間などといった組み合わせで構築できます。

このウィザードは、VPN が正しく作動するために必要な、パケット・ルールを含む各構成オブジェクトを自動的に作成します。ただし、VPN に機能 (たとえば、ジャーナル処理や VPN 用のネットワーク・アドレス変換 (VPN NAT) など) を追加する必要がある場合は、該当する動的キー・グループまたは接続のプロパティー・シートを使用して、VPN をさらに調整する必要が生じることがあります。これを実行するには、接続が活動中の場合、まず接続を停止する必要があります。次に、動的キー・グループまたは接続を右クリックし、「**プロパティー**」を選択します。

始めに、VPN 計画アドバイザーを完成します。このアドバイザーは、VPN を作成するうえで必要となる、重要な情報を収集する方法を提供します。

「接続」ウィザードを使用して VPN を作成するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして、「**新規接続**」を選択し、このウィザードを開始する。
3. ウィザードを完了して、基本 VPN 接続を作成する。援助が必要な場合には、「**ヘルプ**」をクリックしてください。

VPN セキュリティー・ポリシーを構成する

VPN の使用方法を決定した後、VPN セキュリティー・ポリシーを定義する必要があります。特に、以下の作業を行う必要があります。

- 44 ページの『Internet Key Exchange (IKE) ポリシーを構成する』
  IKE ポリシーは、フェーズ 1 のネゴシエーション時に IKE が使用する認証と暗号化保護のレベルを定義します。 IKE フェーズ 1 は、後続のフェーズ 2 のネゴシエーションでやり取りされるメッセージを

保護するキーを確立します。手動接続を作成するときに、IKE ポリシーを定義する必要はありません。さらに、「新規接続」ウィザードを使用して VPN を作成する場合は、そのウィザードがユーザーに代わって IKE ポリシーを作成することができます。

- 『データ・ポリシーを構成する』
  データ・ポリシーは、VPN 経由でやり取りされるデータを保護する際の、認証または暗号化のレベルを定義します。通信システムは、Internet Key Exchange (IKE) プロトコルのフェーズ 2 のネゴシエーションの間は、これらの属性が一致しています。手動接続を作成するときに、データ・ポリシーを定義する必要はありません。さらに、「新規接続」ウィザードを使用して VPN を作成する場合は、その ウィザードがユーザーのためにデータ・ポリシーを作成することができます。

VPN セキュリティー・ポリシーの構成が終了した後、次に、 45 ページの『VPN セキュア接続を構成する』を構成しなければなりません。

Internet Key Exchange (IKE) ポリシーを構成する

IKE ポリシーは、 28 ページの『キー管理』 がフェーズ 1 のネゴシエーションの過程で使用する、認証または暗号化保護のレベルを定義します。 IKE フェーズ 1 は、後続のフェーズ 2 のネゴシエーションでやり取りされるメッセージを保護するキーを確立します。 VPN は RSA シグニチャー・モードまたは事前共用キーのいずれかを使用して、フェーズ 1 のネゴシエーションを認証します。キー・サーバーの認証にディジタル証明書を使用することを計画している場合は、最初に、ディジタル証明書マネージャー (5722-SS1 オプション 34) を使用してディジタル証明書を構成しなければなりません。 IKE ポリシーは、このポリシーを使用するリモート・キー・サーバーも識別します。

IKE ポリシーを定義するか、既存の IKE ポリシーを変更するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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. 新しいポリシーを作成するには、「**Internet Key Exchange ポリシー**」を右クリックして、「**新規 Internet Key Exchange ポリシー**」を選択する。既存のポリシーを変更するには、左側のペインで「**Internet Key Exchange ポリシー**」をクリックした後、右側のペインで変更したいポリシーを右クリックして、「**プロパティー**」を選択します。
3. それぞれのプロパティー・シートを完成する。ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. 「**OK**」をクリックして、変更を保管する。

» **注:** 事前共用キーを認証に使用するときは、メインモード・ネゴシエーションの使用をお勧めします。よりセキュアな交換になるからです。事前共用キーとアグレッシブ・モード・ネゴシエーションを使用しなければならない場合は、ディクショナリーをスキャンするアタックで解かれそうにないわかりにくいパスワードを選択してください。パスワードを定期的に変更することもお勧めします。詳細については、iSeries ナビゲーターのオンライン・ヘルプを使用してください。 «

データ・ポリシーを構成する

データ・ポリシーは、VPN 経由でやり取りされるデータを保護する際の、認証または暗号化のレベルを定義します。通信システムは、 28 ページの『キー管理』の、フェーズ 2 のネゴシエーションの間は、これらの属性が一致しています。

データ・ポリシーを定義するか、既存のデータ・ポリシーを変更するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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. 新しいデータ・ポリシーを作成するには、「**データ・ポリシー**」を右クリックして、「**新規データ・ポリシー**」を選択する。既存のデータ・ポリシーを変更するには、「**データ・ポリシー**」(左側のペインにある) をクリックした後、変更したいデータ・ポリシーを右クリックして (右側のペインで)「**プロパティー**」を選択する。
3. それぞれのプロパティー・シートを完成する。ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. 「**OK**」をクリックして、変更を保管する。

VPN セキュア接続を構成する

接続のセキュリティー・ポリシーを構成した後は、次に、セキュア接続を構成しなければなりません。動的接続の場合は、セキュア接続オブジェクトには、動的キー・グループと動的キー接続が組み込まれます。

動的キー・グループは、1 つ以上の VPN 接続の共通の特性を定義します。動的キー・グループを構成すると、同じポリシーを使用することができますが、データ・エンドポイントはグループ内の接続ごとに異なります。また動的キー・グループによって、リモート・システムが提案するデータ・エンドポイントが、前もって明確に分からない場合に、リモート起動側とのネゴシエーションを成功させることができます。これは、動的キー・グループのポリシー情報を、 IPSEC アクション・タイプのポリシー・フィルター規則と関連付けることによって実行されます。リモート起動側が提供する特定のデータ・エンドポイントが、IPSEC フィルター規則で指定される範囲内にある場合は、それらに、動的キー・グループで定義されるポリシーを適用することができます。

動的キー接続は、エンドポイントの組みの間の個々のデータ接続の特性を定義します。動的キー接続は、動的キー・グループに含まれています。 グループにある使用するポリシー接続について説明する動的キー・グループを構成したら、ローカルで開始する接続用に動的キー接続を作成する必要があります。

セキュア接続オブジェクトを構成するには、以下の作業を完了してください。

パート 1: 動的キー・グループを構成する

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**グループ別**」を右クリックして、「**新規動的キー・グループ**」を選択する。
3. ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. 「**OK**」をクリックして、変更を保管する。

パート 2: 動的キー接続を構成する

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」—>「**グループ別**」と展開する。
2. 「iSeries ナビゲーター」ウィンドウの左側のペインで、パート 1 で作成した動的キー・グループを右クリックして、「**新規動的キー接続**」を選択する。
3. ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. 「**OK**」をクリックして、変更を保管する。

これらのステップの完了後、接続が正しく作動するために必要パケット・ルールを 50 ページの『VPN パケット・ルールを活動化する』します。

注: ほとんどの場合、「**動的キー・グループ - 接続**」ページで「**このグループに次のポリシー・フィルターを生成**」オプションを選択して、VPN インターフェースが VPN パケット・ルールを自動的に生成できるようにしてください。ただし、「**ポリシー・フィルターはパケット・ルールで定義される**」オプションを選択した場合は、パケット・ルール・エディターを使用して 『VPN パケット・ルールを構成する』したうえで、その規則を活動化しなければなりません。

手動接続を構成する

手動接続とは、その名のとおり、VPN プロパティーをすべて手動で構成する必要がある接続のことです。さらに、接続の両端で、完全に 一致しなければならない要素を、いくつか構成する必要があります。たとえば、インバウンド・キーは、リモート・システムのアウトバウンド・キーと一致する必要があり、一致しない場合は、接続が失敗します。

手動接続では、接続が活動している間、更新または変更が行われない静的キーを使用します。手動接続に対応付けられたキーを変更するには、その手動接続を停止する必要があります。このことをセキュリティー上のリスクであり、接続の両端で Internet Key Exchange (IKE) プロトコルをサポートすると考える場合は、その代わりに、動的接続のセットアップを考慮する必要が生じる場合があります。

手動接続にプロパティーを定義するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」を右クリックして、「**新規手動接続**」を選択する。
3. それぞれのプロパティー・シートを完成する。ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. 「**OK**」をクリックして、変更を保管する。

注: ほとんどの場合、「**手動接続 - 接続**」ページで「**データ・エンドポイントと一致するポリシー・フィルターを生成**」オプションを選択して、VPN インターフェースが VPN パケット・ルールを自動的に生成できるようにしてください。ただし、「**ポリシー・フィルターはパケット・ルールで定義される**」オプションを選択する場合は、次に、手動で 48 ページの『ポリシー・フィルター規則を構成する』した後、それらを活動化しなければなりません。

VPN パケット・ルールを構成する

初めて接続を作成している場合は、VPN がユーザーに代わって自動的に VPN パケット・ルールを生成できるようにしてください。これは、「新規接続」ウィザードまたは VPN プロパティー・ページを使用して接続を構成することによって行うことができます。

iSeries(TM) ナビゲーターのパケット・ルール・エディターを使用して VPN パケット・ルールを作成する場合は、追加の規則も同様にこの方法で作成してください。逆に、VPN にポリシー・フィルター規則を生成させる場合には、追加のポリシー・フィルター規則をすべてこの方法で作成してください。

一般に、VPN は、IPSec より前のフィルター規則とポリシー・フィルター規則の 2 つのタイプのフィルター規則を必要とします。 iSeries ナビゲーターのパケット・ルール・エディターを使用してこれらの規則を構成する方法については、下記のトピックを参照してください。その他の VPN および IP フィルター操作オプションについては、『VPN の概念』トピックの 33 ページの『VPN および IP フィルター操作』セクションを参照してください。

- 47 ページの『IPSec より前のフィルター規則を構成する』
  IPSec より前の規則とは、IPSEC アクション・タイプが指定された規則の前に来る、ユーザーのシステム上の規則です。このトピックでは、IPSec より前の規則のなかで、VPN が正しく作動するために必要

なものについてのみ説明します。 この場合、IPSec より前の規則は、接続を介して IKE 処理を行うことができるようにする規則の組みです。 IKE によって、ユーザーの接続のために、動的キーの生成とネゴシエーションを行わせることができます。特定のネットワーク環境およびセキュリティー・ポリシーによって、他の IPSec より前の規則を追加する必要がある場合があります。

注: このタイプの、IPSec より前の規則の構成が必要となるのは、特定のシステムについて IKE を許可する他の規則がすでに存在する場合に限られます。 IKE トラフィックを許可するように明示されたフィルター規則がシステムに存在しない場合、IKE トラフィックが暗黙的に許可されます。

- 48 ページの『ポリシー・フィルター規則を構成する』
  ポリシー・フィルター規則は、VPN を使用できるトラフィックと、そのトラフィックに適用するデータ保護ポリシーを定義します。

始める前の考慮事項

インターフェースにフィルター規則を追加する場合は、システムはそのインターフェースにデフォルトの DENY 規則を自動的に追加します。つまり、明示的に許可されていないトラフィックはすべて拒否されます。この規則は見ることも変更することもできません。したがって、以前は動作していたトラフィックが、VPN フィルター規則を活動化して以降は原因不明で失敗する可能性があります。 インターフェース上で VPN 以外のトラフィックを許可したい場合は、これを許可するための明示的な PERMIT 規則を追加しなければなりません。

適切なフィルター規則を構成した後、その規則を適用する 50 ページの『VPN フィルター規則のインターフェースを定義する』し、次に、それらを 50 ページの『VPN パケット・ルールを活動化する』しなければなりません。

フィルター規則を正しく構成することは、重要です。正しく設定しない場合、iSeries を出入りするすべての IP トラフィックが、フィルター規則によってブロックされる可能性があります。これには、フィルター規則を構成するために使用する、iSeries ナビゲーターへの接続が含まれます。

フィルター規則によって iSeries ナビゲーターのトラフィックが許可されていない場合、 iSeries ナビゲーターは iSeries と通信することができません。 この状況になっていることが判明した場合は、オペレーション・コンソールなどの現在接続が持続されているインターフェースを使用して、 iSeries にログオンする必要があります。 RMVTCPTBL コマンドを使用して、このシステム上のすべてのフィルターを除去してください。このコマンドを使用すると、*VPN サーバーも終了および再始動します。そのあと、フィルターを構成して、サーバーを再度活動化します。

IPSec より前のフィルター規則を構成する

重要: このタスクは、VPN がポリシー・フィルター規則を自動的に生成しないように指定した場合にのみ実行してください。

一対の Internet Key Exchange (IKE) サーバーは、キーを動的にネゴシエーションして、最新の内容に更新します。 IKE は、事前割り当てポート 500 を使用します。 IKE が正しく動作するには、この IP トラフィックのポート 500 で、 UDP データグラムを使用可能にする必要があります。このためには、対になったフィルター規則 (1 つはインバウンド・トラフィック用、もう 1 つはアウトバウンド・トラフィック用) を作成し、接続が保護のために動的にキーをネゴシエーションするようにします。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右クリックして、「**ルール・エディター (Rules Editor)**」を選択する。これにより、パケット・ルール・エディターが開き、iSeries 用のフィルター規則および NAT 規則を作成または編集できるようになります。

3. 「ウェルカム」ウィンドウで「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. パケット・ルール・エディターから「**挿入**」—>「**フィルター (Filter)**」と選択する。
5. 「**一般**」ページで、VPN フィルター規則のセット名を指定する。少なくとも 3 つのセットを作成することをお勧めします。1 つ目は IPSec より前のフィルター規則用、2 つ目はポリシー・フィルター規則用、3 つ目は各種の PERMIT および DENY フィルター規則用です。 IPSec より前のフィルター規則が入っているセットには、 *preipsec* という接頭部を付ける必要があります。たとえば、preipsecfilters のようになります。
6. 「**アクション**」フィールドで、ドロップダウン・リストから、「**PERMIT**」を選択する。
7. 「**方向**」フィールドで、ドロップダウン・リストから「**OUTBOUND**」を選択する。
8. 「**ソース・アドレス名**」フィールドでは、最初のドロップダウン・リストから = を選択し、次に 2 番目のフィールドに、ローカル・キー・サーバーの IP アドレスを入力する。ローカル・キー・サーバーの IP アドレスは、IKE ポリシーで指定したものです。
9. 「**宛先アドレス名**」フィールドでは、最初のドロップダウン・リストから = を選択し、次に 2 番目のフィールドに、リモート・キー・サーバーの IP アドレスを入力する。リモート・キー・サーバーの IP アドレスも、IKE ポリシーで指定したものです。
10. 「**サービス**」ページで、「**サービス**」を選択する。これで、「**プロトコル**」、「**ソース・ポート**」、「**宛先ポート**」の各フィールドが、使用可能になります。
11. 「**プロトコル**」フィールドで、ドロップダウン・リストから、「**UDP**」を選択する。
12. 「**ソース・ポート**」の場合は、最初のフィールドで = を選択し、次に 2 番目のフィールドに 500 と入力する。
13. 「**宛先ポート**」でも、直前のステップを繰り返す。
14. 「**OK**」をクリックする。
15. INBOUND フィルターを構成するには、上記のステップを繰り返す。同じセット名を使用し、必要に応じてアドレスを変えてください。

注: 接続を介して IKE トラフィックを許可する場合、 IPSec より前のフィルターを 1 つだけ構成し、「**方向**」、「**ソース・アドレス名**」、「**宛先アドレス名**」の各フィールドに、ワイルドカード値 (*) を使用する方が、安全性には劣りますが簡単です。

次のステップは、 『ポリシー・フィルター規則を構成する』して、 VPN 接続が保護する IP トラフィックを定義することです。

ポリシー・フィルター規則を構成する

重要: このタスクは、VPN がポリシー・フィルター規則を自動的に生成しないように指定した場合にのみ実行してください。

ポリシー・フィルター規則 (action=IPSEC になっている規則) では、VPN を使用することができるアドレス、プロトコル、およびポートを定義します。 また、VPN 接続でトラフィックに適用されるポリシーの、識別も行います。ポリシー・フィルター規則を構成するには、以下のステップに従ってください。

注: IPSec より前の規則を構成した直後である場合 (動的接続の場合のみ)、パケット・ルール・エディターがまだオープンしています。その場合は、ステップ 4 から始めてください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。

2. 「**パケット・ルール**」を右クリックして、「**ルール・エディター (Rules Editor)**」を選択する。これにより、パケット・ルール・エディターが開き、iSeries 用のフィルター規則および NAT 規則を作成または編集できるようになります。
3. 「ウェルカム」ウィンドウで「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. パケット・ルール・エディターから「**挿入**」—>「**フィルター (Filter)**」と選択する。
5. 「**一般**」ページで、VPN フィルター規則のセット名を指定する。少なくとも 3 つのセットを作成することをお勧めします。1 つ目は IPSec より前のフィルター規則用、2 つ目はポリシー・フィルター規則用、3 つ目は各種の PERMIT および DENY フィルター規則用です。 たとえば、 `policyfilters` のように指定してください。
6. 「**アクション**」フィールドで、ドロップダウン・リストから、「**IPSEC**」を選択する。「**方向**」フィールドは、デフォルトで OUTBOUND になっていて、これを変更することはできません。このフィールドのデフォルトは OUTBOUND ですが、実際は両方向です。入力値のセマンティクスを明らかにするために、OUTBOUND と表示しているのです。たとえば、送信元の値はローカル値であり、宛先の値はリモート値です。
7. 「**ソース・アドレス名**」で、最初のフィールドで = を選択し、次に 2 番目のフィールドに、ローカル・データ・エンドポイントの IP アドレスを入力する。 IP アドレスまたは IP アドレスとサブネット・マスクの範囲は、「**定義済みアドレス**」機能を使用して、それらを定義してから指定することもできます。
8. 「**宛先アドレス名**」で、最初のフィールドで = を選択し、次に 2 番目のフィールドに、リモート・データ・エンドポイントの IP アドレスを入力する。 IP アドレスまたは IP アドレスとサブネット・マスクの範囲は、「**定義済みアドレス**」機能を使用して、それらを定義してから指定することもできます。
9. 「**ジャーナル処理**」フィールドで、必要なジャーナル処理レベルを指定する。
10. 「**接続名**」フィールドで、これらのフィルター規則が適用される接続の定義を選択する。
11. (オプション) 記述を入力する。
12. 「**サービス**」ページで、「**サービス**」を選択する。これで、「**プロトコル**」、「**ソース・ポート**」、「**宛先ポート**」の各フィールドが、使用可能になります。
13. 「**プロトコル**」、「**ソース・ポート**」、および「**宛先ポート**」の各フィールドで、そのトラフィックに該当する値を選択する。あるいは、ドロップダウン・リストからアスタリスク (*) を選択することもできます。これで、任意のプロトコルが、 VPN を使用する任意のポートを使用することが許可されます。
14. 「**OK**」をクリックする。

次のステップは、これらのフィルター規則が適用される 50 ページの『VPN フィルター規則のインターフェースを定義する』ことです。

注: インターフェースにフィルター規則を追加する場合、システムは自動的に、そのインターフェースにデフォルトの DENY 規則を追加します。つまり、明示的に許可されていないトラフィックはすべて拒否されます。この規則は見ることも変更することもできません。したがって、以前には動作していた接続が、VPN パケット・ルールを活動化して以降は原因不明のまま失敗してしまう、ということが発生する場合があります。インターフェース上で VPN 以外のトラフィックを許可したい場合は、これを許可するための明示的な PERMIT 規則を追加しなければなりません。

VPN フィルター規則のインターフェースを定義する

VPN 接続を使用可能にするために必要な VPN パケット・ルールおよびその他の規則を構成した後で、これらの規則が適用されるインターフェースを定義する必要があります。

VPN フィルター規則が適用されるインターフェースを定義するには、以下のステップに従ってください。

注: VPN パケット・ルールを構成した直後である場合は、「パケット・ルール」インターフェースはまだオープンされたままになっています。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右クリックして、「**ルール・エディター (Rules Editor)**」を選択する。これにより、パケット・ルール・エディターが開き、iSeries 用のフィルター規則および NAT 規則を作成または編集できるようになります。
3. 「ウェルカム」ウィンドウで「**新規パケット・ルール・ファイルの作成 (Create a new packet rules file)**」を選択し、「**OK**」をクリックする。
4. パケット・ルール・エディターで、「**挿入**」—>「**フィルター・インターフェース (Filter Interface)**」と選択する。
5. 「**一般**」のページで、「**回線名**」を選択した後、ドロップダウン・リストから、VPN パケット・ルールが適用される回線記述を選択する。
6. (オプション) 記述を入力する。
7. 「**フィルター・セット**」のページで、「**追加**」をクリックし、構成したばかりのそれぞれのセット名を追加する。
8. 「**OK**」をクリックする。
9. 規則ファイルを保管する。ファイルは、iSeries 上の統合ファイル・システムに、.i3p の拡張子を付けて保管されます。
   注: 次のディレクトリーにはファイルを保管しないでください。

   ```
   /QIBM/UserData/OS400/TCPIP/RULEGEN
   ```

   このディレクトリーはシステム専用です。 RMVTCPTBL *ALL コマンドを使用して、パケット・ルールを非活動化する必要がある場合、このコマンドを実行すると、上記ディレクトリー内のファイルはすべて削除されます。

フィルター規則のインターフェースを定義したら、VPN を開始する前に、必ずそれらを『VPN パケット・ルールを活動化する』しなければなりません。

VPN パケット・ルールを活動化する

VPN 接続を開始する前に、VPN パケット・ルールを活動化する必要があります。 VPN 接続がシステムで実行されている間は、パケット・ルールを活動化 (または非活動化) することはできません。このため、VPN フィルター規則を活動化する前に、それらのフィルター規則に関連した接続が活動状態ではないことを確認してください。

「新規接続」ウィザードを使用して VPN 接続を作成した場合には、関連したルールを自動的に活動化させるように選択することができます。指定したインターフェースのいずれかに、活動状態になっている他のパケット・ルールが存在する場合、それらのパケット・ルールは VPN ポリシーのフィルター規則によって置き換えられます。

VPN で生成された規則を、パケット・ルール・エディターを使用して活動化する場合には、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右クリックし、「**活動化**」を選択する。これにより、「**パケット・ルールの活動化 (Activate Packet Rules)**」ダイアログ・ボックスが開きます。
3. VPN で生成されたルールのみを活動化するのか、選択したファイルのみを活動化するのか、あるいは VPN で生成されたルールと選択したファイルの両方を活動化するのかを選択する。たとえば、VPN で生成されたルールに加えて、各種の PERMIT ルールや DENY ルールをインターフェースに適用したい場合には、VPN で生成されたルールと選択したファイルの両方の活動化を選択することができます。
4. 活動化させるルールのあるインターフェースを選択する。特定のインターフェースでの活動化、 2 地点間 ID での活動化、および、すべてのインターフェースとすべての 2 地点間 ID での活動化を選択することができます。
5. ダイアログ・ボックスで「**OK**」をクリックして、指定した 1 つまたは複数のインターフェースでルールの検査と活動化を実行することを確認する。「OK」をクリックすると、システムはそのルールに構文およびセマンティックのエラーがないかどうかを検査し、エディター下部のメッセージ・ウィンドウでその結果を報告します。特定のファイルおよび行番号に関連したエラー・メッセージは、エラーを右クリックし、「**行番号 (Go To Line)**」を選択すると、ファイル内のエラーを強調表示させることができます。

フィルター規則を活動化したら、 『VPN 接続を開始する』を開始することができます。

VPN 接続を開始する

以下の説明では、VPN 接続が正しく構成されていることを前提としています。 VPN 接続を開始するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. VPN サーバーが開始していない場合は、「**仮想プライベート・ネットワーク**」を右クリックして、「**開始**」を選択する。 これで、VPN サーバーが開始されます。
3. パケット・ルールが 50 ページの『VPN パケット・ルールを活動化する』ことを確認する。
4. 「**仮想プライベート・ネットワーク**」—>「**セキュア接続**」と展開する。
5. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
6. 開始する接続を右クリックして、「**開始**」を選択する。複数の接続を開始するには、開始したいそれぞれの接続を選択して右クリックし、「**開始**」を選択します。

VPN を管理する

以下のものを含む、すべての管理作業を処理するには、iSeries(TM) ナビゲーターの VPN インターフェースを使用します。

- 『VPN 接続を開始する』
  この作業を完了して、ローカルで開始する接続を開始します。
- 52 ページの『接続に使用するデフォルト属性を設定する』
  新しいポリシーと接続を作成するために使用するパネルにデフォルト値を提供します。セキュリティー・レベル、キー・セッション管理、キー存続期間、および接続の存続期間にデフォルトを設定することができます。

- 『エラー状態の接続をリセットする』
  エラー状態の接続は、リセットすることによって、アイドル状態に戻ります。
- 53 ページの『エラー情報を表示する』
  この作業を完了して、接続がエラー状態になった理由を判別する際に役立てます。
- 53 ページの『活動接続の属性を表示する』
  この作業を完了して、活動接続の状況と他の属性を検査します。
- 53 ページの『VPN サーバー・トレースを使用する』
  VPN サーバー・トレースを使用すると、VPN 接続マネージャーと VPN キー・マネージャーのトレースを構成、開始、停止、および表示することができます。この作業は、接続が活動であるときにトレースを表示できることを除き、文字ベースのインターフェースから TRCTCPAPP *VPN コマンドを使用するのに似ています。
- 54 ページの『VPN サーバー・ジョブ・ログを表示する』
  VPN キー・マネージャーおよび VPN 接続マネージャーのジョブ・ログを表示するには、この指示に従ってください。
- 54 ページの『VPN 接続を停止する』
  このタスクを完了して、活動接続を停止します。
- 54 ページの『セキュリティー・アソシエーション (SA) の属性を表示する』
  この作業を完了して、使用可能な接続に関連したセキュリティー・アソシエーション (SA) の属性を表示します。
- 54 ページの『VPN 構成オブジェクトを削除する』
  VPN ポリシー・データベースから VPN 構成オブジェクトを削除する前に、その構成オブジェクトが他の VPN 接続および接続グループに及ぼす影響を理解していることを確認してください。

接続に使用するデフォルト属性を設定する

新しい VPN オブジェクトを作成する際、さまざまなフィールドにデフォルトのセキュリティー値が提供されます。

ユーザーの VPN 接続にデフォルトのセキュリティー値を設定するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして、「**デフォルト**」を選択する。
3. ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。
4. それぞれのプロパティー・シートを完成後、「**OK** 」をクリックする。

エラー状態の接続をリセットする

エラー状態にある接続をリフレッシュするには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. リセットしたい接続を右クリックして、「**リセット**」を選択する。これで、接続がアイドル状態にリセットされます。エラー状態にある複数の接続をリセットするには、リセットしたいそれぞれの接続を選択して右クリックし、「**リセット**」を選択します。

エラー情報を表示する

エラーが発生した接続に関する情報を表示するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 表示したいエラーが発生している接続を右クリックし、「**エラー情報**」を選択する。

活動接続の属性を表示する

活動接続またはオンデマンド接続の現行属性を表示するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 表示したい活動接続またはオンデマンド接続を右クリックして、「**プロパティー**」を選択する。
4. 「**現行属性**」のページに移動し、接続の属性を表示する。

「iSeries ナビゲーター」ウィンドウからすべての接続の属性を表示することもできます。 デフォルトでは、状況、記述、および接続タイプの属性のみが表示されます。以下のステップに従って、表示されるデータの内容を変更することができます。

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 「**オプション**」メニューから、「**カラム**」を選択する。これにより、「iSeries ナビゲーター」ウィンドウで表示したい属性を選択するためのダイアログ・ボックスが開きます。

表示する列を変更する場合、変更内容は特定ユーザーや PC に固有のものではないが、システム規模のものである点に注意してください。

VPN サーバー・トレースを使用する

VPN サーバー・トレースを表示するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックし、「**診断ツール**」の後に「**サーバー・トレース**」を選択する。

VPN キー・マネージャーと VPN 接続マネージャーに生成させるトレースのタイプを指定するには、以下のステップに従ってください。

1. 「**仮想プライベート・ネットワーキング・トレース**」ウィンドウで、  (オプション) をクリックする。
2. 「**接続マネージャー**」のページで、接続マネージャー・サーバーに実行させるトレースのタイプを指定する。
3. 「**キー・マネージャー**」のページで、キー・マネージャーに実行させるトレースのタイプを指定する。
4. ページまたはそのページの任意のフィールドの記入方法について質問がある場合は、「**ヘルプ**」をクリックしてください。

5. 「**OK**」をクリックして、変更を保管する。
6.  (開始) をクリックして、トレースを開始する。  (最新表示) を定期的にクリックして、最新のトレース情報を表示します。

VPN サーバー・ジョブ・ログを表示する

VPN キー・マネージャーまたは VPN 接続マネージャーのいずれかの現行ジョブ・ログを表示するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」を右クリックして「**診断ツール**」を選択した後、表示したいサーバー・ジョブ・ログを選択する。

セキュリティー・アソシエーション (SA) の属性を表示する

使用可能な接続に関連したセキュリティー・アソシエーション (SA) の属性を表示すること。この作業を行うには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 該当する活動接続を右クリックし、「**セキュリティー・アソシエーション**」を選択する。表示されたウィンドウを使用すると、特定の接続に関連したそれぞれの SA のプロパティーを表示することができます。

VPN 接続を停止する

活動接続またはオンデマンド接続を停止するには、以下のステップに従ってください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 停止したい接続を右クリックして、「**停止**」を選択する。複数の接続を停止するには、停止したいそれぞれの接続を選択して右クリックし、「**停止**」を選択します。

VPN 構成オブジェクトを削除する

VPN ポリシー・データベースから VPN 接続を削除する必要性を確信している場合は、以下のステップを実行してください。

1. iSeries(TM) ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 「**すべての接続**」をクリックして、右側のペインに接続のリストを表示する。
3. 削除する接続を右クリックして、「**削除**」を選択する。

VPN のトラブルシューティング

VPN は複雑で変化の激しいテクノロジーであり、少なくとも、標準 IPSec テクノロジーの基本的な知識を必要とします。また、VPN を適正に動作させるには、いくつかのフィルター規則が必要となることから、IP パケット・ルールに精通している必要もあります。 この複雑さのために、しばしば、 VPN 接続に関してトラブルが発生する場合があります。 VPN のトラブルシューティングは、常に簡単な作業であるとは限りません。ユーザーは、システムおよびネットワーク環境ばかりでなく、その環境の管理に使用される構成要素まで理解していなければなりません。以下のトピックでは、VPN の使用中に発生する可能性があるさまざまな問題について、そのトラブルシューティングの方法に関するヒントを提供します。

- 『VPN のトラブルシューティング入門』
  ここでは、VPN 接続の問題の検出と訂正を開始します。
- 56 ページの『一般的な VPN の構成エラーとその修正方法』
  このトピックでは、ごく一般的なユーザー・エラーを取り上げ、可能な解決策を提供します。
- 63 ページの『QIPFILTER ジャーナルを使用して行う VPN のトラブルシューティング』
  このトピックでは、VPN フィルター規則に関する情報を提供しています。
- 65 ページの『QVPN ジャーナルを使用して行う VPN のトラブルシューティング』
  このトピックでは、IP トラフィックおよび IP 接続に関する情報を提供します。
- 68 ページの『VPN ジョブ・ログを使用して行う VPN のトラブルシューティング』
  このトピックでは、VPN が使用するさまざまなジョブ・ログについて説明しています。
- 75 ページの『OS/400 通信トレースを使用して行う VPN のトラブルシューティング』
  このトピックでは、通信回線でデータをトレースする方法について説明します。

VPN のトラブルシューティング入門

VPN の問題分析を開始するには、次のようないくつかの方法があります。

1. 最新のプログラム一時修正 (PTF) を適用していることを、常に確認してください。
2. 最低限の 36 ページの『VPN セットアップ要件』を満たしていることを、確認してください。
3. ローカル・システムとリモート・システムの両方で、「53 ページの『エラー情報を表示する』」ウィンドウまたは 68 ページの『VPN ジョブ・ログを使用して行う VPN のトラブルシューティング』 に表示されるエラー・メッセージを検討します。実際に、VPN 接続の問題をトラブルシューティングしている場合には、接続の両端で調べる必要がよくあります。さらに、検査しなければならない 4 つのアドレスがあることを考慮に入れておく必要があります。すなわち、IPSec が IP パケットに適用されるアドレスであるローカル接続とリモート接続のエンドポイントと、 IP パケットのソースと宛先アドレスであるローカルとリモートのデータ・エンドポイントです。
4. 表示されたエラー・メッセージで、問題解決のための十分な情報が得られない場合は、 63 ページの『QIPFILTER ジャーナルを使用して行う VPN のトラブルシューティング』・ジャーナルをチェックします。
5. iSeries(TM) の 75 ページの『OS/400 通信トレースを使用して行う VPN のトラブルシューティング』からも、ローカル・システムが接続要求を受信または送信したかどうかについての一般情報を得ることができます。
6. TCP アプリケーションのトレース (TRCTCPAPP) コマンドは、問題を分離するまた別の方法を提供します。 IBM(R) サービスでは通常、TRCTCPAPP を使用して、接続の問題を分析するために、トレース出力を取得しています。

チェックするべきその他の項目

接続のセットアップ終了後にエラーが発生し、そのエラーがネットワークのどこで発生したかが分からない場合は、環境の複合度を削減してみてください。たとえば、VPN 接続のすべての部分を一度に調べる代わ

りに、 IP 接続そのものから始めてください。以下のリストは、VPN の問題分析を、最も単純な IP 接続から始めて、より複雑な VPN 接続に進めていく方法に関する基本的なガイドラインを提供するものです。

1. ローカル・ホストとリモート・ホストの間の IP 構成から開始します。ローカル・システムとリモート・システムの両方が通信に使用するインターフェースの IP フィルターをすべて除去します。ローカル・ホストからリモート・ホストに PING できますか?

   注: PING コマンドでプロンプトが出されることを忘れないでください。リモート・システム・アドレスを入力して追加のパラメーターに PF10 を使用してから、ローカルの IP アドレスを入力してください。これは、複数の物理インターフェースまたは論理インターフェースを使用する場合には、特に重要です。確実に、正しいアドレスが PING パケットで配置されるようにします。

   答えが**はい**である場合は、ステップ 2 に進んでください。答えが**いいえ**である場合は、IP 構成、インターフェース状況、経路指定項目をチェックしてください。構成が正しければ、通信トレースを使用して、たとえば、PING 要求がシステムから出ていることを確認してください。 PING 要求を送信しているのに応答がない場合は、問題はネットワークかリモート・システムにある可能性が最も高くなります。

   注: IP パケット・フィルター操作を実行する中間ルーター・ファイアウォールがあり、PING パケットのフィルター操作が行われている可能性があります。一般的には、PING は ICMP プロトコルを基にしています。 PING が正常の行われた場合は、接続が使用可能であることが分かります。 PING が失敗に終わった場合は、PING が失敗したことだけが分かります。 2 つのシステム間で別の IP プロトコル (Telnet または FTP など) を試行して、接続を検査することができます。
2. VPN のフィルター規則をチェックし、その規則が活動化されていることを確認してください。フィルター操作は正常に始まりますか。答えが**はい**である場合には、ステップ 3 に進んでください。答えが**いいえ**である場合には、「iSeries ナビゲーター」の「パケット・ルール」ウィンドウでエラー・メッセージをチェックしてください。任意の VPN トラフィックに対し、フィルター規則がネットワーク・アドレス変換 (NAT) を指定していないことを、確認してください。
3. 51 ページの『VPN 接続を開始する』。接続は正常に開始されますか。答えが**はい**である場合は、ステップ 4 に進んでください。答えが**いいえ**である場合は、QTOVMAN ジョブ・ログ、QTOKVPNIKE ジョブ・ログにエラーがないかどうか、チェックしてください。
   ユーザーが VPN を使用する場合、インターネット・サービス・プロバイダー (ISP) および、ネットワーク内の個々のセキュリティー・ゲートウェイは、認証ヘッダー (AH) プロトコルおよび、カプセル化セキュリティー・ペイロード (ESP) プロトコルをサポートしている必要があります。ユーザーが AH の使用を選択するか ESP の使用を選択するかは、 VPN 接続で定義する提案によって決まります。
4. VPN 接続を介してユーザー・セッションを活動化することができますか。答えが**はい**である場合は、VPN 接続は必要に応じて動作しています。答えが**いいえ**である場合は、パケット・ルール、VPN 動的キー・グルーおよび接続をチェックし、必要なユーザー・トラフィックを許可しないフィルター定義を探してください。

一般的な VPN の構成エラーとその修正方法

このセクションでは、VPN を使用する際に発生する比較的一般的な問題を説明し、その解決法のヒントへのリンクを提供します。

注: VPN を構成する際、ユーザーは実際には、複数の異なる構成オブジェクトを作成します。これらの各構成オブジェクトは、VPN が接続を使用可能にするために必要となります。 VPN GUI の用語では、これらのオブジェクトは、IP セキュリティー・ポリシーおよびセキュア接続です。そこで、この情報でオブジェクトというときには、 VPN の 1 つまたは複数の部分のことを指しています。

主なエラー・メッセージ

メッセージ	症状
58 ページの『VPN エラー・メッセージ: TCP5B28』	インターフェースに関するフィルター規則を活動化しようとすると、「TCP5B28 CONNECTION_DEFINITION オーダー違反です (order violation)」というメッセージが出ます。
58 ページの『VPN エラー・メッセージ: 項目が見つかりません』	VPN オブジェクトを右クリックして、「**プロパティー**」または「**削除**」を選択したときに、「**項目が見つかりません (Item not found)**」というメッセージが表示されます。
59 ページの『VPN エラー・メッセージ: パラメーター PINBUF は無効です』	接続を開始しようとしたときに、「**パラメーター PINBUF は無効です (PARAMETER PINBUF IS NOT VALID)...**」というメッセージが表示されます。
59 ページの『VPN エラー・メッセージ: 項目が見つかりません。リモート・キー・サーバー...』	動的キー接続で「**プロパティー**」を選択したとき、サーバーが指定されたリモート・キー・サーバーを見つけられないというエラーが表示されます。
60 ページの『VPN エラー・メッセージ: オブジェクトを更新できません』	動的キー・グループまたは手動接続のプロパティー・シートで、「**OK**」を選択すると、システムがオブジェクトを更新できないというメッセージが表示されます。
60 ページの『VPN エラー・メッセージ: キーを暗号化できません...』	QRETSVRSEC 値は 1 に設定されていなければならないため、システムがキーを暗号化できないというメッセージが表示されます。
60 ページの『VPN エラー・メッセージ: CPF9821』	iSeries(TM) ナビゲーターで、「IP ポリシー」コンテナーを展開またはオープンしようとしたときに、「CPF9821- QSYS ライブラリーのプログラム QTFRPRS は、許可されていません (CPF9821- Not authorized to program QTFRPRS in QSYS library)」というメッセージが表示されます。

ユーザーが陥る可能性のあるその他の問題

エラー	症状
61 ページの『VPN エラー: キーがすべてブランクである』	手動接続のプロパティーを表示したとき、事前共用キー、およびその接続のアルゴリズム・キーがすべてブランクです。
61 ページの『VPN エラー: パケット・ルールを使用する際、別のシステムのサインオンが表示される』	iSeries ナビゲーターで「パケット・ルール」インターフェースを初めて使用するときに、現行システム以外のシステムのサインオン画面が表示されます。
61 ページの『VPN エラー: 「iSeries ナビゲーター」ウィンドウの接続状況がブランクである』	「iSeries ナビゲーター」ウィンドウの「**状況**」の欄に値が表示されていない接続があります。
61 ページの『VPN エラー: 接続を停止したにもかかわらず接続の状況が使用可能のままである』	接続を停止した後も、引き続き、「iSeries ナビゲーター」ウィンドウに、接続が使用可能と表示されています。
61 ページの『VPN エラー: 暗号化の選択項目に 3DES がない』	IKE ポリシー変形、データ・ポリシー変形、あるいは手動接続を使用して作業しているときに、選択項目に 3DES 暗号化アルゴリズムがありません。

62 ページの『VPN エラー: 「iSeries ナビゲーター」ウィンドウに予期しない列が表示される』	VPN 接続の「iSeries ナビゲーター」ウィンドウに表示させたい列を設定したにもかかわらず、あとでウィンドウを見ると、それとは違う列が表示されている。
62 ページの『VPN エラー: 活動中のフィルター規則を非活動化できない』	フィルター規則の現行セットを非活動化しようとすると、結果ウィンドウに、「**活動中の規則の非活動化に失敗しました (The active rules failed to be deactivated)**」というメッセージが表示される。
62 ページの『VPN エラー: 接続のためのキー接続グループが変更される』	動的キー接続を作成する際に、リモート・キー・サーバー用の動的キー・グループと ID を指定します。その後、関連のある接続オブジェクトのプロパティーを表示すると、プロパティー・シートの「一般」のページに、リモート・キー・サーバーの識別コードは同じものが表示されますが、動的キー・グループは別のものとなっています。

VPN エラー・メッセージ: TCP5B28

症状:
特定のインターフェースでフィルター規則を活動化しようとしたときに、次のエラー・メッセージを受け取ります。

```
TCP5B28: CONNECTION_DEFINITION order violation
```

解決方法:
活動化しようとしているフィルター規則には、前回活動化された規則のセットとは異なる方法で配列された接続定義が含まれています。このエラーを解決するための最も簡単な方法は、特定のインターフェースではなく、**すべてのインターフェース**上の規則ファイルを活動化することです。

VPN エラー・メッセージ: 項目が見つかりません

症状:
「仮想プライベート・ネットワーク」ウィンドウでオブジェクトを右クリックして、「**プロパティー**」または「**削除**」を選択したときに、次のようなメッセージが表示されます。

解決方法:

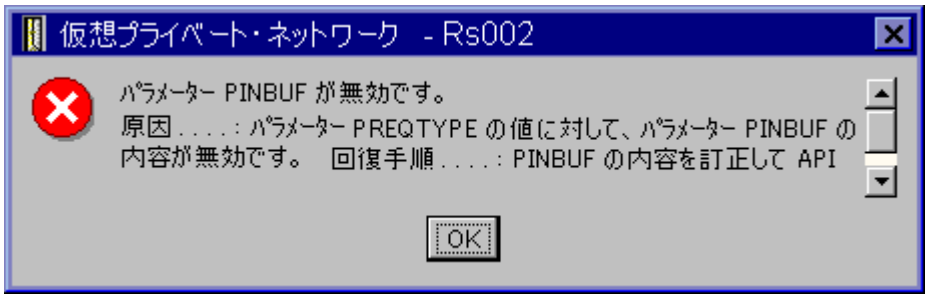
- オブジェクトを削除するかまたは名前変更した後、ウィンドウをまだ更新していない可能性があります。そのため、そのオブジェクトが、「仮想プライベート・ネットワーク」ウィンドウに、まだ表示されているのです。これを確かめるには、「**表示**」メニューから、「**最新表示**」を選択します。それでもまだ、「仮想プライベート・ネットワーク」ウィンドウにオブジェクトが表示されている場合は、このリストの次の項目に進んでください。
- そのオブジェクトのプロパティーを構成した際に、VPN サーバーと iSeries(TM) との間で通信エラーが発生した可能性があります。 「仮想プライベート・ネットワーク」ウィンドウに表示されるオブジェクト

の多くは、 VPN ポリシー・データベースの複数のオブジェクトに関連付けられます。つまり、通信エラーによって、データベース内の一部のオブジェクトが、 VPN のオブジェクトに関連付けられる場合があるということです。オブジェクトを作成または更新したときにはいつでも、同期が行われていないと、エラーが発生します。この問題を修正する唯一の方法は、エラー・ウィンドウで「**OK**」を選択することです。これで、エラーの出たオブジェクトのプロパティー・シートが立ち上がります。プロパティー・シートには、「名前」フィールドだけに値が入っています。他のフィールドはすべてブランクです(あるいはデフォルトが入っています)。そのオブジェクトの正しい属性を入力し、「**OK**」を選択して変更を保管してください。

- オブジェクトを削除しようとしたときにも同様のエラーが発生します。この問題を修正するには、エラー・メッセージ上で「**OK**」をクリックしたときに開く、ブランクのプロパティー・シートを完成させてください。そうすれば、VPN ポリシー・データベースへの失われたリンクが更新されます。これで、オブジェクトを削除することができます。

VPN エラー・メッセージ: パラメーター PINBUF は無効です

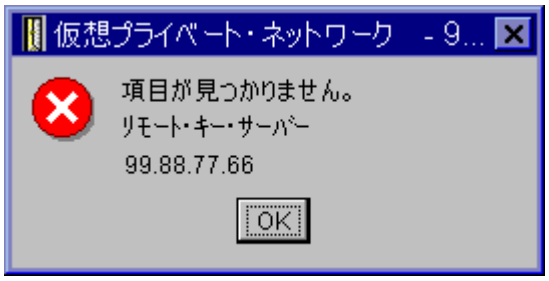
症状:
接続を開始しようとしたときに、次のようなメッセージが表示されます。



解決方法:
この状況は、ユーザーのシステム が、小文字が正しくマップしない特定のロケールを使用するように、設定されている場合に生じます。このエラーを修正するには、すべてのオブジェクトが必ず大文字のみを使用するようにするか、あるいはシステムのロケールを変更するかのいずれかの方法があります。

VPN エラー・メッセージ: 項目が見つかりません。リモート・キー・サーバー...

症状:
動的キー接続で「**プロパティー**」を選択したときに、次のようなメッセージが表示されます。

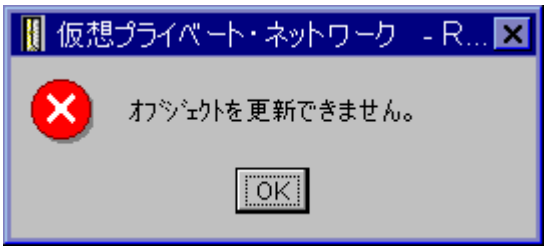


解決方法:
ある特定のリモート・キー・サーバー ID を使用して接続を構築し、その後、そのリモート・キー・サーバーを動的キー・グループから除去した場合に、この症状が発生します。このエラーを修正するには、エラー・メッセージ上で「**OK**」をクリックしてください。これで、エラー状態にある動的キー接続のプロパテ

ィー・シートが開きます。ここから、そのリモート・キー・サーバーを動的キー・グループに再度追加するか、または、別のリモート・キー・サーバー ID を選択することができます。プロパティー・シート上で「**OK**」をクリックして、変更を保管します。

VPN エラー・メッセージ: オブジェクトを更新できません

症状:
動的キー・グループまたは手動接続のプロパティー・シートで、「**OK**」を選択したときに、次のようなメッセージが表示されます。



解決方法:
活動中の接続が使用しているオブジェクトを、ユーザーが変更しようとした場合に、このエラーが発生します。接続が活動状態であるときにオブジェクトを変更することはできません。オブジェクトを変更するためには、該当する活動中の接続を識別した後、その接続を右クリックし、表示されたコンテキスト・メニューから「**停止**」を選択します。

VPN エラー・メッセージ: キーを暗号化できません...

症状:
次のようなエラー・メッセージが表示されます。

解決方法:
QRETSVRSEC はシステム値で、ユーザーのシステムが暗号化されたキーを保管できるかどうかを示しています。この値が 0 に設定されていると、事前共用キーと、手動接続でのアルゴリズム用のキーを、 VPN ポリシー・データベースに保管することができません。この問題を修正するには、ユーザーのシステムに 5250 エミュレーション・セッションを使用します。コマンド行で `wrksysval` と入力し、 **Enter** キーを押してください。リストから QRETSVRSEC を探して、その隣に 2 (変更) と入力します。次のパネルで 1 と入力し、 **Enter** キーを押してください。

VPN エラー・メッセージ: CPF9821

症状:
iSeries(TM) ナビゲーターで、「IP ポリシー」コンテナーを展開しようとしたときに、「`CPF9821- QSYS ライブラリーのプログラム QTFRPRS は、許可されていません (CPF9821- Not authorized to program QTFRPRS in QSYS library)`」というメッセージが表示されます。

解決方法:
パケット・ルールまたは VPN 接続マネージャーの現在の状況を検索するために、必要な権限がないことが考えられます。iSeries ナビゲーターのパケット・ルール機能にアクセスできるように *IOSYSCFG 権限を持っていることを確認してください。

VPN エラー: キーがすべてブランクである

症状:
事前共用キー、および手動接続用のアルゴリズム・キーがすべて、ブランクです。

解決方法:
システム値 QRETSVRSEC の設定が 0 に戻されると、必ずこの症状が発生します。このシステム値を 0 に設定すると、 VPN ポリシー・データベース内のキーはすべて削除されます。この問題を修正するには、システム値を 1 に設定して、すべてのキーを再入しなければなりません。この実行方法に関する詳細は、60 ページの『VPN エラー・メッセージ: キーを暗号化できません...』を参照してください。

VPN エラー: パケット・ルールを使用する際、別のシステムのサインオンが表示される

症状:
初めてパケット・ルールを使用するときに、現行システム以外のシステムのサインオンが表示されます。

解決方法:
パケット・ルールは、Unicode を使用して、統合ファイル・システムにパケット・セキュリティーを保管します。サインオンを追加すると、iSeries(TM) Access は、Unicode 用の適切な変換テーブルを獲得することができます。これを実行できるのは一度のみです。

VPN エラー: 「iSeries ナビゲーター」ウィンドウの接続状況がブランクである

症状:
「iSeries(TM) ナビゲーター」ウィンドウの「**状況**」の欄に値が表示されていない接続があります。

解決方法:
状況の値がブランクであるということは、接続が開始の過程にあることを示しています。つまり、接続はまだ実行されておらず、エラーが発生しているわけではありません。ウィンドウを最新表示すると、接続は、「エラー」、「使用可能」、「On-demand」、または「Idle」のいずれかの状況を表示します。

VPN エラー: 接続を停止したにもかかわらず接続の状況が使用可能のままである

症状:
接続を停止した後も、引き続き、「iSeries(TM) ナビゲーター」ウィンドウに、接続が使用可能と表示されています。

解決方法:
この症状は、通常、「iSeries ナビゲーター」ウィンドウが、まだ更新されていないために発生します。 したがって、ウィンドウには古い情報が表示されています。これを修正するには、「**表示**」メニューから、「**最新表示**」を選択してください。

VPN エラー: 暗号化の選択項目に 3DES がない

症状:
IKE ポリシー変形、データ・ポリシー変形、あるいは手動接続を使用して作業している際に、選択項目に 3DES 暗号化アルゴリズムがありません。

解決方法:
おそらく、Cryptographic Access Provider AC2 (5722-AC2) プロダクトのみがシステムに導入されており、Cryptographic Access Provider AC3 (5722-AC3) は導入されていないことが考えられます。 AC2 は、キーの長さに制限があるため、データ暗号化規格 (DES) の暗号化アルゴリズムしか考慮しません。

VPN エラー: 「iSeries ナビゲーター」ウィンドウに予期しない列が表示される

症状:
VPN 接続の「iSeries ナビゲーター」ウィンドウに表示させたい列を設定したにもかかわらず、あとでウィンドウを見ると、それとは違う列が表示されている。

解決方法:
表示する列を変更すると、その変更は、特定のユーザーまたは PC だけではなく、システム全体に及びます。したがって、だれかがウィンドウ上で列を変更すれば、その変更は、そのシステムで接続を表示するすべての人に影響を与えます。

VPN エラー: 活動中のフィルター規則を非活動化できない

症状:
フィルター規則の現行セットを非活動化しようとすると、結果ウィンドウに、「活動中の規則の非活動化に失敗しました (The active rules failed to be deactivated)」というメッセージが表示される。

解決方法:
通常、このエラー・メッセージは、少なくとも 1 つの VPN 接続が活動中であることを意味しています。状況が「使用可能」になっている接続を 1 つずつ停止しなくてはなりません。これを実行するには、活動中の接続をそれぞれ右クリックして、「**停止**」を選択します。これで、フィルター規則を非活動化できます。

VPN エラー: 接続のためのキー接続グループが変更される

症状:
動的キー接続を作成する際に、リモート・キー・サーバー用の動的キー・グループと ID を指定します。その後、関連のある接続オブジェクトの「**プロパティー**」を選択すると、プロパティー・シートの「**一般**」のページに、リモート・キー・サーバーの ID は同じものが表示されますが、動的キー・グループは別のものになっています。

解決方法:
ID は VPN ポリシー・データベースに保管される唯一の情報であり、動的キー接続のリモート・キー・サーバーを参照します。 VPN は、リモート・キー・サーバーのポリシーを検索する際、そのリモート・キー・サーバーの ID を含んでいる最初の動的キー・グループを検索します。したがって、これらの接続のいずれかのプロパティーを表示させると、VPN が検出したものと同じ動的キー・グループが使用されます。 動的キー・グループをそのリモート・キー・サーバーと対応付けたくない場合は、以下の項目のいずれかを実行してください。

1. 動的キー・グループからリモート・キー・サーバーを除去する。
2. VPN インターフェースの左側のペインで、「**グループ別 (By Groups)**」を展開し、希望する動的キー・グループを選択して、右側のペインに表示されている表の最上部にドラッグする。これで、VPN は、リモート・キー・サーバー用にこの動的キー・グループを最初にチェックするようになります。

QIPFILTER ジャーナルを使用して行う VPN のトラブルシューティング

QIPFILTER ジャーナルは QUSRSYS ライブラリーに配置され、そこには、フィルター規則のセットに関する情報に加えて、 IP データグラムが許可されたか拒否されたかという情報も、含まれています。ログ記録は、フィルター規則で指定するジャーナル処理オプションに基づいて、実行されます。

IP パケット・フィルター・ジャーナルを使用可能にする方法

QIPFILTER ジャーナルを活動化するには、iSeries(TM) ナビゲーターにあるパケット・ルール・エディターを使用してください。ログ記録機能は、個々のフィルター規則ごとに使用可能にしなければなりません。システムに出入りするすべての IP データグラムに、ログ記録を許可する機能はありません。

注: QIPFILTER ジャーナルを使用可能にするためには、フィルターを非活動にしなければなりません。

以下のステップは、特定のフィルター規則のジャーナル処理を使用可能にする方法を説明しています。

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**ネットワーク**」—>「**IP ポリシー**」と展開する。
2. 「**パケット・ルール**」を右クリックして、「**構成**」を選択する。これにより、「パケット・ルール」インターフェースが表示されます。
3. 既存のフィルター規則・ファイルを開く。
4. ジャーナル処理を希望するフィルター規則をダブルクリックする。
5. 「**一般**」のページで、上のダイアログ・ボックスにあるように、「**ジャーナリング**」フィールドで、「**FULL**」を選択する。これで、この特定のフィルター規則のログ記録が使用可能になります。
6. 「**OK**」をクリックする。
7. 変更したフィルター規則・ファイルを保管し、活動化する。

IP データグラムがフィルター規則の定義に一致する場合は、QIPFILTER ジャーナルに記入項目が作成されます。

QIPFILTER ジャーナルの使用方法

OS/400(R) は、ユーザーが初めて IP パケット・フィルター操作を活動化したときに、自動的にジャーナルを作成します。ジャーナルで項目ごとの詳細を表示させるには、画面上にジャーナル項目を表示させるか、出力ファイルを使用することができます。

ジャーナル項目を出力ファイルにコピーすると、 Query/400 や SQL のような照会ユーティリティーを使用して、その項目を簡単に表示させることができます。あるいは独自の HLL プログラムを作成して、出力ファイルの項目を処理することもできます。

次の例は、ジャーナル表示 (DSPJRN) コマンドの一例です。

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

以下のステップに従って、QIPFILTER ジャーナル項目を、出力ファイルにコピーしてください。

1. 複製オブジェクト作成 (CRTDUPOBJ) コマンドを使用して、システムが提供する出力ファイル QSYS/QATOFIPF のコピーを、ユーザー・ライブラリーに作成する。次の例は、CRTDUPOBJ コマンドの一例です。

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. ジャーナル表示 (DSPJRN) コマンドを使用して、 QUSRSYS/QIPFILTER ジャーナルから直前のステップで作成した出力ファイルに、項目をコピーする。

DSPJRN をコピーしようとする出力ファイルが存在していない場合は、システムがファイルを作成しますが、このファイルには、適切なフィールド記述が含まれていません。

注: QIPFILTER ジャーナルには、ジャーナル処理オプションが FULL に設定されているフィルター規則の、許可項目あるいは拒否項目しか含まれていません。たとえば、ユーザーが PERMIT フィルター規則のみをセットアップした場合、明示的に許可されていない IP データグラムは拒否されます。このような拒否されたデータグラムに関しては、ジャーナルに項目が追加されません。問題分析では、他のすべてのトラフィックを明示的に拒否し、 FULL ジャーナル処理を許可するフィルター規則を追加することができます。次に、拒否されたすべての IP データグラムに対して、ジャーナルで DENY 項目を取得します。パフォーマンス上の理由から、すべてのフィルター規則でジャーナル処理を使用可能にすることはお勧めしません。フィルター・セットをテストしたあとは、ジャーナル処理を、有用な項目サブセットに限定してください。

QIPFILTER 出力ファイルを説明する表については、『QIPFILTER ジャーナル・フィールド』を参照してください。

QIPFILTER ジャーナル・フィールド

次の表は、QIPFILTER 出力ファイルの各フィールドを説明したものです。

フィールド名	フィールド長	数値	記述	注記
TFENTL	5	Y	項目の長さ	
TFSEQN	10	Y	順序番号	
TFCODE	1	N	ジャーナル・コード	常に M
TFENTT	2	N	項目タイプ	常に TF
TFTIME	26	N	SAA タイム・スタンプ	
TFJOB	10	N	ジョブ名	
TFUSER	10	N	ユーザー・プロファイル	
TFNBR	6	Y	ジョブ番号	
TFPGM	10	N	プログラム名	
TFRES1	51	N	予約済み	
TFUSPF	10	N	ユーザー	
TFSYMN	8	N	システム名	
TFRES2	20	N	予約済み	
TFRESA	50	N	予約済み	
TFLINE	10	N	回線記述	TFREVT が U* の場合は *ALL、TFREVT が L* の場合はブランク、TFREVT が L の場合は回線名
TFREVT	2	N	規則イベント	規則がロードされている場合は L* または L、規則がアンロードされている場合は U*、アクション・フィルターに掛ける場合は A
TFPDIR	1	N	IP パケットの方向	O はアウトバウンド、I はインバウンド

フィールド名	フィールド長	数値	記述	注記
TFRNUM	5	N	規則番号	活動中の規則ファイルに規則番号を適用する
TFACT	6	N	実行されるフィルター・アクション	PERMIT、DENY、または IPSEC
TFPROT	4	N	トランスポート・プロトコル	1 は ICMP 6 は TCP 17 は UDP 50 は ESP 51 は AH
TFSRCA	15	N	送信元 IP アドレス	
TFSRCP	5	N	ソース・ポート	TFPROT= 1 (ICMP) の場合はガーベッジ
TFDSTA	15	N	宛先 IP アドレス	
TFDSTP	5	N	宛先ポート	TFPROT= 1 (ICMP) の場合はガーベッジ
TFTEXT	76	N	追加テキスト	TFREVT= L* または U* の場合は説明を含む

QVPN ジャーナルを使用して行う VPN のトラブルシューティング

VPN は、個別のジャーナルを使用して、IP トラフィックおよび接続に関する情報 (QVPN ジャーナルと呼ばれます) をログに記録します。 QVPN は、QUSRSYS ライブラリーに保管されます。ジャーナル・コードは M で、ジャーナル・タイプは TS です。ジャーナル項目を日常的に使用することは、まずありません。むしろ、トラブルシューティングの際、およびシステムやキーや接続が指定した方法で機能しているかどうかを検証する際に、その有効性が実感できます。たとえば、データ・パケットに何が起こっているかを知る場合に、ジャーナル項目が役立ちます。ジャーナル項目はまた、 VPN の現在の状況をユーザーに知らせる役目も果たしています。

VPN ジャーナルを使用可能にする方法

VPN ジャーナルを活動化するには、iSeries(TM) ナビゲーターの、仮想プライベート・ネットワーク・インターフェースを使用します。 すべての VPN 接続に対してログ記録を許可する機能はありません。したがって、ログ記録は、個々の動的キー・グループまたは手動接続ごとに使用可能にしなければなりません。

以下のステップは、特定の動的キー・グループまたは手動接続のジャーナル機能を使用可能にする方法を説明しています。

1. iSeries ナビゲーターで、「**ユーザー接続のサーバー**」—>「**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**」—>「**セキュア接続**」と展開する。
2. 動的キー・グループの場合は、「**グループ別**」を展開した後、ジャーナル処理を使用可能にしたい動的キー・グループを右クリックして、「**プロパティー**」を選択する。
3. 手動接続の場合は、「**すべての接続**」を展開した後、ジャーナル処理を使用可能にしたい手動接続を右クリックする。
4. 「**一般**」のページで、必要なジャーナル処理を選択する。 4 つのオプションから選択することができます。それは以下のようなものです。

None (なし)
この接続グループではジャーナル処理は行いません。
All (すべて)
すべての接続活動 (接続の開始または停止、キーの最新表示、 IP トラフィック情報など) で、ジャーナル処理を行います。
Connection Activity (接続活動)
接続の開始または停止などの接続活動に対して、ジャーナル処理を行います。
IP traffic (IP トラフィック)
この接続に関連したすべての VPN トラフィックで、ジャーナル処理を行います。ログ項目は、フィルター規則が呼び出されるたびに作成されます。システムは、IP トラフィック情報を QIPFILTER ジャーナルに記録します。このジャーナルは、QUSRSYS ライブラリーに配置されています。

5. 「**OK**」をクリックする。
6. 接続を開始して、ジャーナル処理を活動化する。

注: ジャーナル処理を停止するには、まず、接続が非活動であることを確認しなければなりません。接続グループのジャーナル処理状況を変更するには、活動中の接続がいずれも、その特定のグループに対応付けられていないことを確認する必要があります。

VPN ジャーナルの使用方法
VPN ジャーナルで項目ごとの詳細を表示させるには、画面上にジャーナル項目を表示させるか、出力ファイルを使用することができます。

ジャーナル項目を出力ファイルにコピーすると、 Query/400 や SQL のような照会ユーティリティーを使用して、その項目を簡単に表示させることができます。あるいは独自の HLL プログラムを作成して、出力ファイルの項目を処理することもできます。次の例は、ジャーナル表示 (DSPJRN) コマンドの一例です。

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

以下のステップを使用して、VPN ジャーナル項目を、出力ファイルにコピーしてください。

1. システムが提供する出力ファイル QSYS/QATOVSOF のコピーを、ユーザー・ライブラリーに作成する。これは、複製オブジェクト作成 (CRTDUPOBJ) コマンドを使用して、実行することができます。次の例は、CRTDUPOBJ コマンドの一例です。

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. ジャーナル表示 (DSPJRN) コマンドを使用して、 QUSRSYS/QVPN ジャーナルから直前のステップで作成した出力ファイルに、項目をコピーする。 DSPJRN をコピーしようとする出力ファイルが存在していない場合は、システムがファイルを作成しますが、このファイルには、適切なフィールド記述が含まれていません。

QVPN 出力ファイルのフィールドを説明する表については、『QVPN ジャーナル・フィールド』を参照してください。

QVPN ジャーナル・フィールド

次の表は、QVPN 出力ファイルの各フィールドを説明したものです。

フィールド名	フィールド長	数値	説明	注記
TSENTL	5	Y	項目の長さ	
TSSEQN	10	Y	順序番号	

フィールド名	フィールド長	数値	説明	注記
TSCODE	1	N	ジャーナル・コード	常に M
TSENTT	2	N	項目タイプ	常に TS
TSTIME	26	N	SAA 入力タイム・スタンプ	
TSJOB	10	N	ジョブの名前	
TSUSER	10	N	ジョブのユーザー	
TSNBR	6	Y	ジョブの番号	
TSPGM	10	N	プログラムの名前	
TSRES1	51	N	使用されていない	
TSUSPF	10	N	ユーザー・プロファイル名	
TSSYNM	8	N	システム名	
TSRES2	20	N	使用されていない	
TSRESA	50	N	使用されていない	
TSESDL	4	Y	特定のデータの長さ	
TSCMPN	10	N	VPN の構成要素	
TSCONM	40	N	接続名	
TSCOTY	10	N	接続タイプ	
TSCOS	10	N	接続状態	
TSCOSD	8	N	開始日付	
TSCOST	6	N	開始時刻	
TSCOED	8	N	終了日付	
TSCOET	6	N	終了時刻	
TSTRPR	10	N	トランスポート・プロトコル	
TSLCAD	43	N	ローカル・クライアント・アドレス	
TSLCPR	11	N	ローカル・ポート	
TSRCAD	43	N	リモート・クライアント・アドレス	
TSCPR	11	N	リモート・ポート	
TSLEP	43	N	ローカル・エンドポイント	
TSREP	43	N	リモート・エンドポイント	
TSCORF	6	N	更新時刻	
TSRFDA	8	N	次回最新表示の日付	
TSRFTI	6	N	次回最新表示の時刻	
TSRFLS	8	N	存続サイズの最新表示	
TSSAPH	1	N	SA フェーズ	
TSAUTH	10	N	認証タイプ	
TSENCR	10	N	暗号化タイプ	
TSDHGR	2	N	Diffie-Hellman グループ	
TSERRC	8	N	エラー・コード	

VPN ジョブ・ログを使用して行う VPN のトラブルシューティング

VPN 接続で問題に遭遇したときには、いかなる場合でも、ジョブ・ログを分析することをお勧めします。実際、エラー・メッセージおよび VPN 環境に関連したその他の情報を含むジョブ・ログが、いくつかあります。

接続の両サイドが iSeries(TM) サーバーである場合は、その両サイドのジョブ・ログを分析することが重要です。 動的接続の開始に失敗したときに、リモート・システムで何が起こっているのかが分かれば役立ちます。

VPN ジョブ、すなわち QTOVMAN および QTOKVPNIKE は、サブシステム QSYSWRK で実行されます。OS/400(R) iSeries ナビゲーターから、 54 ページの『VPN サーバー・ジョブ・ログを表示する』を行うことができます。

このセクションでは、VPN 環境で最も重要なジョブについて概説します。以下のリストは、ジョブ名と、そのジョブの使用目的の簡単な説明です。

QTCPIP
このジョブは、TCP/IP インターフェース全体を開始する基本ジョブです。 TCP/IP 全般に関して根本的な問題がある場合は、 QTCPIP ジョブ・ログを分析してください。

QTOKVPNIKE
QTOKVPNIKE ジョブは VPN キー管理機能のジョブです。 VPN キー管理機能は、UDP ポート 500 を listen し、Internet Key Exchange (IKE) プロトコルの処理を実行します。

QTOVMAN
このジョブは、VPN 接続の接続管理機能です。接続の試みが失敗するたびに、それに関連したジョブ・ログに『VPN 接続マネージャーのよくあるエラー・メッセージ』が入ります。

QTPPANSxxx
このジョブは、PPP ダイヤルアップ接続に使用されます。 PPP プロファイルで *ANS を定義する接続試行に応答します。

QTPPPCTL
これは、ダイヤルアウト接続のための PPP ジョブです。

QTPPPL2TP
これは、レイヤー 2 トンネリング・プロトコル (L2TP) 管理機能のジョブです。 L2TP トンネルの設定に問題がある場合は、このジョブ・ログのメッセージを検索してください。

VPN 接続マネージャーのよくあるエラー・メッセージ

このセクションでは、発生する可能性がある、VPN 接続マネージャーのよくあるエラー・メッセージのいくつかについて説明します。

概して、VPN 接続マネージャーでは、VPN 接続でエラーが発生すると QTOVMAN ジョブ・ログに 2 つのメッセージを記録します。 1 つめのメッセージは、エラーに関する詳細を説明します。 iSeries(TM) ナビゲーターで、エラーの発生した接続を右クリックして、「**エラー情報**」を選択し、これらのエラーに関する情報を表示することができます。

2 つめのメッセージでは、エラーの発生時にその接続で実行しようとしていたアクションについて説明します。たとえば、接続の開始または停止です。下記のメッセージ TCP8601、TCP8602 および TCP860A は、2 つめのメッセージの一般的な例です。

VPN 接続マネージャーのエラー・メッセージ

メッセージ	原因	回復方法
TCP8601 VPN 接続 [*接続名*] が開始できませんでした	以下の理由コードのいずれかにより、この VPN 接続を開始できませんでした。 *0* - 同じ VPN 接続名に関するジョブ・ログ内の前のメッセージにさらに詳細な情報があります。 *1* - VPN ポリシーの構成。 *2* - 通信ネットワークの失敗。 *3* - VPN キー・マネージャーが新しいセキュリティー・アソシエーションのネゴシエーションに失敗した。 *4* - この接続のリモート・エンドポイントが正しく構成されていない。 *5* - VPN キー・マネージャーが VPN 接続マネージャーへの応答に失敗した。 *6* - IP セキュリティー構成要素 VPN 接続のロード障害。 *7* - PPP コンポーネント障害。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. エラーを訂正して、要求を再試行する。 3. iSeries ナビゲーターを使用して 53 ページの『活動接続の属性を表示する』する。開始できなかった接続は、エラー状態になります。
TCP8602 エラーが発生し、VPN 接続 [*接続名*] が停止されました	指定された VPN 接続は、停止するように要求されましたが、以下の理由コードで、停止しなかったか、エラーで停止しました。 *0* - 同じ VPN 接続名に関するジョブ・ログ内の前のメッセージにさらに詳細な情報があります。 *1* - VPN 接続が存在しない。 *2* - VPN キー・マネージャーに関する内部通信障害。 *3* - IPSec コンポーネントに関する内部通信障害。 *4* - VPN 接続リモート・エンドポイントに関する通信障害。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. エラーを訂正して、要求を再試行する。 3. iSeries ナビゲーターを使用して 53 ページの『活動接続の属性を表示する』する。開始できなかった接続は、エラー状態になります。

メッセージ	原因	回復方法
TCP8604 VPN 接続 [*接続名*] の開始に失敗しました	以下の理由コードのいずれかにより、この VPN 接続の開始に失敗しました。 *1* - リモート・ホスト名を IP アドレスに変換できなかった。 *2* - ローカル・ホスト名を IP アドレスに変換できなかった。 *3* - VPN 接続に関連した VPN ポリシー・フィルター規則がロードされていない。 *4* - ユーザー指定のキー値が、関連したアルゴリズムに対して有効でない。 *5* - VP 接続の開始値が、指定されたアクションを許可していない。 *6* - VPN 接続のシステム上の役割が接続グループの情報と矛盾している。 *7* - 予約。 *8* - この VPN 接続のデータ・エンドポイント (ローカルおよびリモート・アドレスおよびサービス) が接続グループの情報と矛盾している。 *9* - ID のタイプが無効。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. エラーを訂正して、要求を再試行する。 3. iSeries ナビゲーターを使用して VPN ポリシー構成を検査または訂正する。この接続に関連した動的キー・グループに許容値が構成されていることを確認してください。
TCP8605 VPN 接続マネージャーが、VPN キー・マネージャーと通信できませんでした	VPN 接続マネージャーは、VPN キー・マネージャーのサービスにより、動的 VPN 接続のセキュリティー・アソシエーションを確立することを要求しています。 VPN 接続マネージャーは、VPN キー・マネージャーと通信できませんでした。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. NETSTAT OPTION(*IFC) コマンドを使用して、*LOOPBACK インターフェースが活動状態であることを検査する。 3. ENDTCPSVR SERVER(*VPN) コマンドを使用して、VPN サーバーを終了する。次に、STRTCPSRV SERVER(*VPN) コマンドを使用して、VPN サーバーを再始動する。 **注:** これにより、現行の VPN 接続はすべて終了されます。

メッセージ	原因	回復方法
TCP8606 VPN キー・マネージャーが、接続、 [*接続名*] に必要なセキュリティー・アソシエーションを確立できませんでした	VPN キー・マネージャーが、以下のいずれかの理由コードにより、必要なセキュリティー・アソシエーションを確立できませんでした *24* - VPN キー・マネージャーのキー接続認証に失敗した。 *8300* - VPN キー・マネージャーのキー接続ネゴシエーション中に障害が発生した。 *8306* - ローカル事前共用キーが見付からない。 *8307* - リモート IKE フェーズ 1 ポリシーが見付からない。 *8308* - リモート事前共用キーが見付からない。 *8327* - VPN キー・マネージャーのキー接続ネゴシエーションがタイムアウトになった。 *8400* - VPN キー・マネージャーの VPN 接続ネゴシエーション中に障害が発生した。 *8407* - リモート IKE フェーズ 2 ポリシーが見付からない。 *8408* - VPN キー・マネージャーの VPN 接続ネゴシエーションがタイムアウトになった。 *8500 または 8509* - VPN キー・マネージャーのネットワーク・エラーが発生した。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. エラーを訂正して、要求を再試行する。 3. iSeries ナビゲーターを使用して VPN ポリシー構成を検査または訂正する。この接続に関連した動的キー・グループに許容値が構成されていることを確認してください。
TCP8608 VPN 接続、[*接続名*] が NAT アドレスを取得できませんでした	この動的キー・グループまたはデータ接続が、ネットワーク・アドレス変換 (NAT) を 1 つまたは複数のアドレスで実行するように指定し、それが、可能性のある以下の理由コードのいずれかにより失敗しました。 *1* - NAT を適用するアドレスが単一 IP アドレスでない。 *2* - 使用可能なすべてのアドレスが使用済みである。	1. 追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. エラーを訂正して、要求を再試行する。 3. iSeries ナビゲーターを使用して VPN ポリシーを検査または訂正する。この接続に関連した動的キー・グループにアドレスの許容値が構成されていることを確認してください。

メッセージ	原因	回復方法
TCP8620 ローカル接続エンドポイントが使用できません	ローカル接続エンドポイントが使用できなかったため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. NETSTAT OPTION(*IFC) コマンドを使用して、ローカル接続エンドポイントが定義および開始されることを確認する。 3. エラーをすべて訂正して、要求を再試行する。
TCP8621 ローカル・データ・エンドポイントが使用できません	ローカル・データ・エンドポイントが使用できなかったため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. NETSTAT OPTION(*IFC) コマンドを使用して、ローカル接続エンドポイントが定義および開始されることを確認する。 3. エラーをすべて訂正して、要求を再試行する。
TCP8622 トランスポート・カプセル化はゲートウェイで許可されていません	ネゴシエーション・ポリシーでトランスポート・カプセル化モードが指定され、この接続がセキュリティー・ゲートウェイとして定義されているため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、この VPN 接続に関連付けられている VPN ポリシーを変更する。 3. エラーをすべて訂正して、要求を再試行する。
TCP8623 VPN 接続が既存の接続とオーバーラップします	既存の VPN 接続が既に使用可能であるため、この VPN 接続を使用可能にできませんでした。この接続のローカル・データ・エンドポイントは [*ローカル・データ・エンドポイント値*] で、リモート・データ・エンドポイントは [*リモート・データ・エンドポイント値*] です。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、ローカル・データ・エンドポイントおよびリモート・データ・エンドポイントがこの接続とオーバーラップしている、使用可能なすべての接続を表示する。 どちらの接続も必要な場合は、既存接続のポリシーを変更してください。 3. エラーをすべて訂正して、要求を再試行する。

メッセージ	原因	回復方法
TCP8624 関連ポリシー・フィルター規則の有効範囲内に VPN 接続がありません	定義されたポリシー・フィルター規則内にデータ・エンドポイントがないため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、この接続または動的キー・グループのデータ・エンドポイント制約事項を表示する。「**ポリシー・フィルターのサブセット (Subset of policy filter)**」または「**ポリシー・フィルターと一致するようにカスタマイズ (Customize to match policy filter)**」を選択している場合は、接続のデータ・エンドポイントをチェックします。これらは、この接続に関連付けられている IPSEC アクションおよび VPN 接続名を持つ活動状態のフィルター規則に適合していなければなりません。既存接続のポリシーまたはフィルター規則を変更して、この接続を使用可能にしてください。 3. エラーをすべて訂正して、要求を再試行する。
TCP8625 VPN 接続が ESP アルゴリズム検査に失敗しました	接続と関連した秘密鍵が不適切であるため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、この接続に関連付けられているポリシーを表示し、別の秘密鍵を入力する。 3. エラーをすべて訂正して、要求を再試行する。

メッセージ	原因	回復方法
TCP8626 VPN 接続エンドポイントがデータ・エンドポイントと同じではありません	ポリシーによりホストであると指定され、VPN 接続エンドポイントがデータ・エンドポイントと同じでないため、この VPN 接続を使用可能にできませんでした。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、この接続または動的キー・グループのデータ・エンドポイント制約事項を表示する。「**ポリシー・フィルターのサブセット (Subset of policy filter)**」または「**ポリシー・フィルターと一致するようにカスタマイズ (Customize to match policy filter)**」を選択している場合は、接続のデータ・エンドポイントをチェックします。これらは、この接続に関連付けられている IPSEC アクションおよび VPN 接続名を持つ活動状態のフィルター規則に適合していなければなりません。既存接続のポリシーまたはフィルター規則を変更して、この接続を使用可能にしてください。 3. エラーをすべて訂正して、要求を再試行する。
TCP8628 ポリシー・フィルター規則がロードされていません	この接続のポリシー・フィルター規則が活動状態ではありません。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、活動状態のポリシー・フィルターを表示する。この接続のポリシー・フィルター規則をチェックする。 3. エラーをすべて訂正して、要求を再試行する。
TCP8629 VPN 接続で IP パケットが欠落しました	この VPN 接続では、VPN NAT が構成されておらず、NAT アドレスに必要な設定が、使用可能な NAT アドレスを超えました。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. iSeries ナビゲーターを使用して、この VPN 接続に割り当てられる NAT アドレスの数を増やす。 3. エラーをすべて訂正して、要求を再試行する。

メッセージ	原因	回復方法
TCP862A PPP 接続の開始に失敗しました	この VPN 接続は PPP プロファイルに関連付けられています。この接続が開始されたときに、PPP プロファイルを開始しようとしましたが、障害が発生しました。	1. この接続に関する追加メッセージについて、 54 ページの『VPN サーバー・ジョブ・ログを表示する』をチェックする。 2. PPP 接続に関連したジョブ・ログをチェックする。 3. エラーをすべて訂正して、要求を再試行する。

OS/400 通信トレースを使用して行う VPN のトラブルシューティング

iSeries(TM) OS/400(R) は、ローカル・エリア・ネットワーク (LAN) や広域ネットワーク (WAN) インターフェースなどの、通信回線上のデータをトレースする機能を提供しています。 一般のユーザーが、トレース・データの内容をすべて理解することは難しいといえます。しかし、トレース項目を使用すれば、ローカル・システムとリモート・システムの間のデータ交換が、行われたかどうかを判別することができます。

通信トレースを開始する

通信追跡の開始 (STRCMNTRC) コマンドを使用して、ユーザーのシステム上で通信トレースを開始します。次の例は、STRCMNTRC コマンドの一例です。

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('VPN Problems')
```

以下のリストで、コマンド・パラメーターについて説明します。

CFGOBJ (構成オブジェクト)
トレース対象となる構成オブジェクトの名前。このオブジェクトは、回線記述、ネットワーク・インターフェース記述、ネットワーク・サーバー記述のいずれかです。

CFGTYPE (構成タイプ)
トレースされているのは、回線 (*LIN)、ネットワーク・インターフェース (*NWI)、ネットワーク・サーバー (*NWS) のいずれかです。

MAXSTG (バッファー・サイズ)
トレースのためのバッファー・サイズ。デフォルトは 128 KB に設定されています。有効範囲は 128 KB から 64 MB です。システム全体にわたるバッファー・サイズの実最大値は、システム・サービス・ツール (SST) 内で定義されます。したがって、STRCMNTRC コマンドで、SST で定義したよりも大きなバッファー・サイズを使用すると、エラー・メッセージが出る場合があります。すべての開始済み通信トレースで指定したバッファー・サイズの合計が、SST で定義したバッファー・サイズの最大値を超えてはいけないことを、覚えておいてください。

DTADIR (データの方向)
トレース対象となるデータ・トラフィックの方向。方向は、アウトバウンド・トラフィックのみ (*SND)、インバウンド・トラフィックのみ (*RCV)、両方向 (*BOTH) の 3 通りが考えられます。

TRCFULL (フル・トレース)
トレース・バッファーがフルである場合に生じること。このパラメーターには、可能な値が 2 つあります。デフォルトは *WRAP で、トレース・バッファーがフルの場合は、トレースは先頭に折り返されるという意味です。一番古いトレース・レコードが、収集された新規レコードによって上書きされます。

2 番目の値は *STOPTRC で、MAXSTG パラメーターで指定されたトレース・バッファーが、トレース・レコードでいっぱいになった場合は、そのトレースを停止させます。通常は必ず、バッファー・サイズを、すべてのトレース・レコードを保管できるだけの大きさに定義してください。トレースが折り返されると、重要なトレース情報が失われる可能性があります。断続的問題がしばしば発生する場合は、トレース・バッファーを十分な大きさに定義し、バッファーの折り返しが重要な情報を破棄することのないようにしてください。

USRDTA (トレース対称となるユーザー・バイト数)
データ・フレームのユーザー・データ部分でトレースされるデータの数を定義します。デフォルトでは、LAN インターフェースの場合、ユーザー・データの先頭の 100 バイトだけが取り込まれます。それ以外のインターフェースの場合はいずれも、ユーザー・データはすべて取り込まれます。フレームのユーザー・データに問題があると疑われる場合は、*MAX が指定されていることを確認してください。

TEXT (トレースの説明)
トレースを分かりやすく説明します。

通信トレースを停止する
特に指定しない限り、トレースは通常、トレース対象である状態が発生すると同時に停止します。トレースを停止するには、通信追跡の終了 (ENDCMNTRC) コマンドを使用してください。次のコマンドは、ENDCMNTRC コマンドの一例です。

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

このコマンドにはパラメーターが 2 つあります。

CFGOBJ (構成オブジェクト)
トレースが実行されている構成オブジェクトの名前。このオブジェクトは、回線記述、ネットワーク・インターフェース記述、ネットワーク・サーバー記述のいずれかです。

CFGTYPE (構成タイプ)
トレースされているのは、回線 (*LIN)、ネットワーク・インターフェース (*NWI)、ネットワーク・サーバー (*NWS) のいずれかです。

トレース・データを印刷する
通信トレースの停止後は、トレース・データを印刷する必要があります。このタスクを実行するには、通信追跡の印刷 (PRTCMNTRC) コマンドを使用します。トレース中は回線トラフィックがすべて取り込まれるので、出力生成のためのフィルター・オプションが、複数用意されています。スプール・ファイルをできるだけ小さくするようにしてください。そうすると、分析が、より速く、効率的にできます。 VPN 問題の場合は、IP トラフィックのみ、さらに可能なら、その中の特定の IP アドレスを、フィルターに掛けるようにしてください。特定の IP ポート番号上でフィルター操作をするというオプションもあります。次の例は、PRTCMNTRC コマンドの一例です。

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1')
    SLTPORT(500) FMTBCD(*NO)
```

この例で、トレースは IP トラフィック用に形式設定され、 IP アドレスのデータだけを含んでいます。ここでは、送信元または宛先のアドレスは 10.50.21.1 で、送信元または宛先の IP ポート番号は 500 です。

VPN 問題を分析する際に最も重要なコマンド・パラメーターだけを、以下で説明します。

CFGOBJ (構成オブジェクト)
トレースが実行されている構成オブジェクトの名前。このオブジェクトは、回線記述、ネットワーク・インターフェース記述、ネットワーク・サーバー記述のいずれかです。

CFGTYPE (構成タイプ)
トレースされているのは、回線 (*LIN)、ネットワーク・インターフェース (*NWI)、ネットワーク・サーバー (*NWS) のいずれかです。

FMTTCP (TCP/IP データのフォーマット設定)
TCP/IP および UDP/IP データのトレースをフォーマット設定するかどうか。 IP データのトレースをフォーマット設定する場合は、*YES を指定します。

TCPIPADR (アドレスによる TCP/IP データのフォーマット設定)
このパラメーターは、2 つの要素で構成されています。両方の要素で IP アドレスを指定すると、それらのアドレス間の IP トラフィックのみが印刷されます。

SLTPORT (IP ポート番号)
フィルターに掛ける IP ポート番号

FMTBCD (ブロードキャスト・データのフォーマット設定)
ブロードキャスト・フレームをすべて印刷するかどうか。デフォルトは「Yes」です。たとえばアドレス解決プロトコル (ARP) 要求を望まない場合は、 *NO を指定してください。これを行わないと、ブロードキャスト・メッセージが殺到する可能性があります。

VPN の関連情報

VPN 構成シナリオおよび説明に関する詳細については、以下の他の情報のソースを参照してください。

- **OS/400(R) V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries(TM) Server with Windows(R) 2000 VPN Clients, REDP0153**

  この IBM レッドペーパーでは、V5R1 VPN および Windows 2000 統合 L2TP および IPSec サポートを使用して VPN トンネルを構成するための、段階的なプロセスを示しています。
- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00**

  このレッドブックでは、VPN 概念を調べ、OS/400 で IP セキュリティー (IPSec) と Layer 2 Tunneling Protocol (L2TP) を使用したインプリメンテーションについて説明しています。
- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00**

  このレッドブックでは、IP フィルター、NAT、VPN、HTTP プロキシー・サーバー、SSL、DNS、メールの中継、監査、およびロギングなど、OS/400 システムで使用可能な統合セキュリティー機能を探します。また、実際の例を通して、その使用法を説明します。
- **Virtual Private Networking: Securing Connections**

この Web ページでは、最新の VPN ニュースについてのハイライト、最新の PTF のリスト、および関連するほかのサイトへのリンクを行っています。

- **その他のセキュリティー関連資料および Redbooks**
  ここで、オンラインで使用可能な情報に関連したセキュリティーのリストに進んでください。

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 を右クリックします (上のリンクを右クリックします)。
2. 「**リンクを名前を付けて保存**」(Netscape Navigator) または「**対象をファイルに保存**」(Internet Explorer) を選択します。
3. PDF を保管するディレクトリーを指定します。
4. 「**保存**」をクリックします。

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 (www.adobe.com/prodindex/acrobat/readstep.html)  からダウンロードできます。

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あり、米国以外の国においては本書で述べる製品、サービス、またはプログラムを提供しない場合があります。

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 49XA
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、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。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

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。

商標

以下は、IBM Corporation の商標です。
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus、Freelance、および WordPro は、IBM Corporation の商標です。

ActionMedia、LANDesk、MMX、Pentium および ProShare は、Intel Corporation の米国およびその他の国における商標です。

Microsoft、Windows、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。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

資料に関するご使用条件

お客様がダウンロードされる資料につきましては、以下の条件にお客様が同意されることを条件にその使用が認められます。

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。これらの資料は、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、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。

これらの資料の著作権はすべて、IBM Corporation に帰属しています。

お客様が、このサイトから資料をダウンロードまたは印刷することにより、これらの条件に同意されたものとさせていただきます。

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