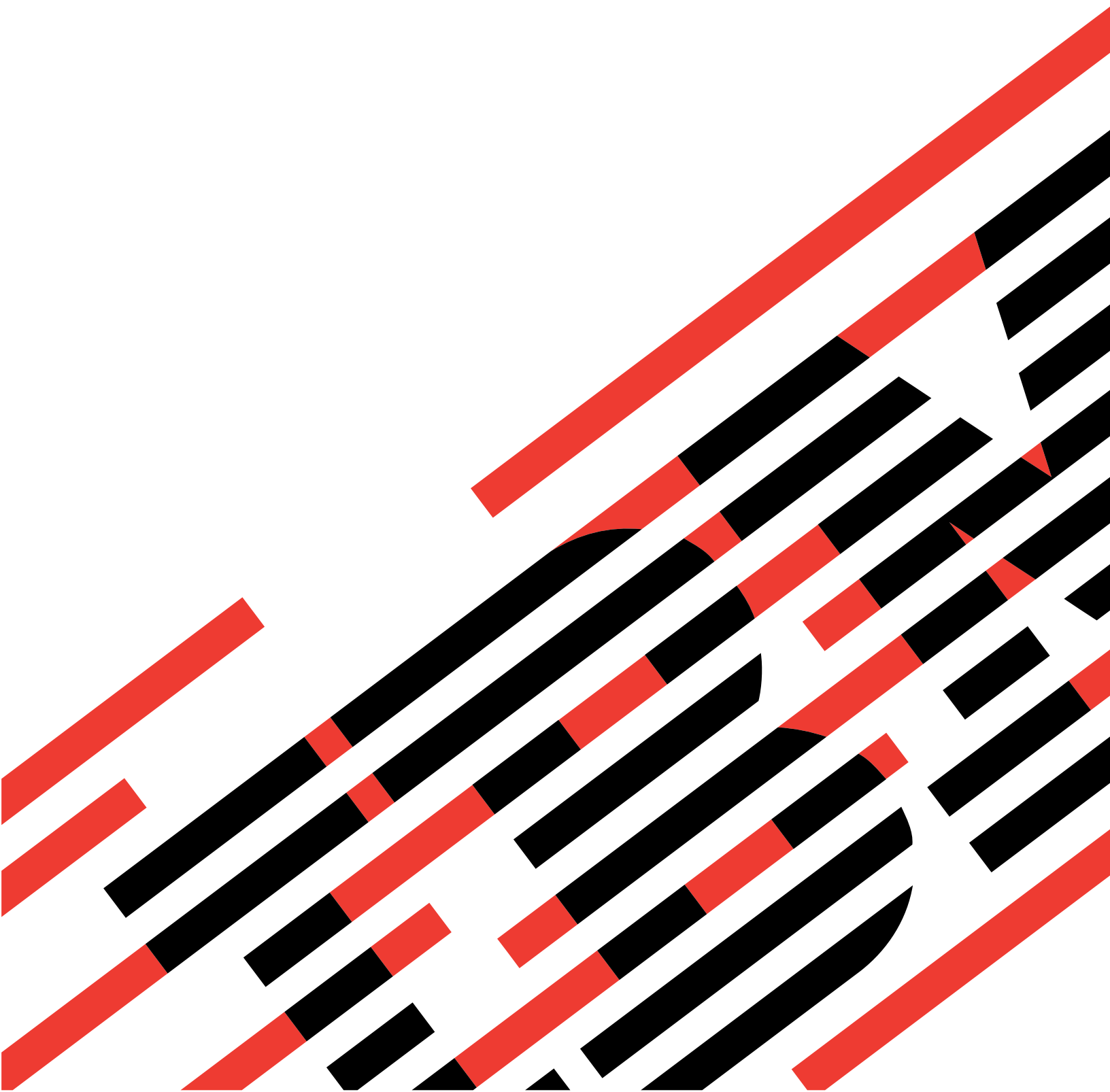




IBM Systems - iSeries

ネットワーキング: Telnet

バージョン 5 リリース 4







**IBM Systems - iSeries**

**ネットワーキング: Telnet**

バージョン 5 リリース 4

**ご注意**

本書および本書で紹介する製品をご使用になる前に、115 ページの『特記事項』に記載されている情報をお読みください。

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

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

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

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

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

(URL は、変更になる場合があります)

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

原 典： IBM Systems – iSeries  
Networking: Telnet  
Version 5 Release 4

発 行： 日本アイ・ピー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 2006.2

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

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

© Copyright International Business Machines Corporation 1998, 2006. All rights reserved.

© Copyright IBM Japan 2006

# 目次

<b>Telnet.</b> . . . . .	<b>1</b>	サーバー・セッションの終了 . . . . .	45
トピックの印刷 . . . . .	1	Device Manager ジョブの終了 . . . . .	45
Telnet のシナリオ. . . . .	1	Telnet 出口プログラムの使用 . . . . .	46
Telnet シナリオ：Telnet サーバーの構成 . . . . .	2	Telnet クライアントの管理 . . . . .	56
Telnet シナリオ：カスケード Telnet セッション . . . . .	4	クライアントからの Telnet サーバー機能の制御 . . . . .	57
Telnet シナリオ：SSL で保護された Telnet . . . . .	9	5250 Telnet クライアント・セッション . . . . .	58
Telnet サーバーの計画. . . . .	16	3270 Telnet クライアント・セッション . . . . .	60
仮想装置記述 . . . . .	16	VTxxx Telnet クライアント・セッション . . . . .	67
Telnet のセキュリティー . . . . .	17	カスケード Telnet セッションの確立 . . . . .	93
Telnet サーバーの構成. . . . .	22	Telnet クライアント・セッションの終了. . . . .	95
Telnet サーバーの開始. . . . .	23	Telnet の問題のトラブルシューティング. . . . .	96
仮想装置の数を設定する . . . . .	23	Telnet に関連した問題の判別 . . . . .	96
特定の装置に対する特権ユーザーを制限し、サイ ンオンの試行回数を制限する . . . . .	25	エミュレーション・タイプのトラブルシューティ ング . . . . .	100
セッション・キープアライブ・パラメーターを設 定する . . . . .	27	Telnet SSL サーバーのトラブルシューティング . . . . .	103
サブシステムに装置を割り当てる . . . . .	27	TRCTCPAPP サービス・プログラムの出力 . . . . .	108
QSYSWRK サブシステムを活動化する . . . . .	28	Telnet の問題の報告に必要な資料. . . . .	111
ユーザー・プロファイルを作成する . . . . .	29	自動生成される診断情報. . . . .	112
iSeries でサポートされているエミュレーション・ タイプ . . . . .	29	Telnet の関連情報 . . . . .	113
SSL で保護された Telnet . . . . .	35	<b>付録. 特記事項 . . . . .</b>	<b>115</b>
Telnet サーバーの管理. . . . .	43	プログラミング・インターフェース情報 . . . . .	116
Telnet 印刷装置セッションの構成 . . . . .	43	商標 . . . . .	116
		資料に関するご使用条件. . . . .	116



---

## Telnet

Telnet は、リモート・コンピューターにログオンし、ローカル・ネットワーク内で直接接続されているかのように、それを使用することができるプロトコルです。

ユーザーの目の前にあるマシン (通常は PC) またはシステムが Telnet クライアントになります。Telnet サーバーとは、クライアントの接続先のリモート・コンピューターです。IBM® eServer™ iSeries™ TCP/IP では Telnet のクライアントとサーバーの両方をサポートします。

Telnet の最も重要な機能の 1 つとして、クライアントとサーバーの間でデータ・ストリームの伝送をネゴシエーションする能力があります。このようなネゴシエーションにより、クライアントとサーバーのどちらでも、要求を開始したり、実行したりすることが可能になります。

要求をネゴシエーションし、それらを出力に変換するために、各種のエミュレーションを使用できます。iSeries Telnet の場合、優先されるタイプは 5250 エミュレーションです。iSeries Telnet は、3270 および VTxxx タイプのワークステーションに加えて、RFC 2877 (TN5250E) 印刷装置サポート・モードもサポートしています。このトピックでは、Telnet の概要を紹介し、iSeries サーバー上で Telnet を管理するのに役立つ情報を提供します。

注: コードのサンプルを使用すると、114 ページの『コードに関するライセンス情報および特記事項』の条件に同意したものとみなされます。

---

### トピックの印刷

この文書の PDF 版を参照用または印刷用にダウンロードし、表示することができます。


この文書の PDF 版を表示し、ダウンロードするには、「Telnet」を選択します。

### PDF ファイルの保存

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

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. PDF をローカルに保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「保存」をクリックする。

### Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、Adobe Reader がご使用のシステムにインストールされている必要があります。これは、Adobe Web サイト ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))  から無料でダウンロードできます。

---

### Telnet のシナリオ

このトピックでは、基本概念および構成タスクを導入するための Telnet の使用例を示しています。

以下の Telnet のシナリオでは、Telnet の構成と使用の方法について理解するために役立つ例が示されています。

## Telnet シナリオ : Telnet サーバーの構成

この構成シナリオでは、管理者が Telnet サーバーをカスタマイズする様子を示します。

### 状況

Ken Harrison は架空の会社 Culver Pharmaceuticals 社の新しい iSeries サーバーの管理者です。

### 目的

彼は以下の仕様に合わせて Telnet サーバーを構成する必要があります。

- 最大 100 の仮想装置が自動的に生成されるようにする
- 常にサインオン・ウィンドウを表示する。
- 特定の装置に対する特権ユーザーを制限する
- 各ユーザーを 1 装置セッションに限定する

### 前提条件および前提事項

このシナリオは、以下を想定しています。

- Culver Pharmaceuticals 社が、IBM OS/400® V5R2 オペレーティング・システムを稼働している iSeries サーバーを使用していること。
- TCP/IP が構成済みであること。
- Ken に IOSYSCFG 権限があること。

### 構成の詳細

1. Telnet サーバーを開始します。
  - a. iSeries ナビゲーターで、**iSeries サーバー** → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開します。
  - b. 右側区画の「サーバー名」列で、「Telnet」を見つけます。
  - c. 「状況」列に「開始済み」と表示されていることを確認します。
  - d. サーバーが実行していない場合には、「Telnet」を右クリックして、「開始」を選択します。
2. 仮想装置の数を設定します。
  - a. iSeries ナビゲーターで、**iSeries サーバー** → 「構成およびサービス」 → 「システム値」を選択します。
  - b. 右側区画で、「装置 (Devices)」を右クリックして「プロパティ」を選択します。
  - c. 「装置システム値 (Devices System Values)」ページで、「パススルー装置および Telnet」を使用可能にして、「装置の最大数 (Maximum number of devices)」を 100 に設定します。
3. Telnet サーバー・プロパティの構成
  - a. iSeries ナビゲーターで、**iSeries サーバー** → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」の順に選択します。



- b. 右側区画で、「Telnet」を右クリックして「プロパティ」を選択します。

表 1. Telnet のプロパティの設定

クリックするタブ	および ...
システム・サインオン	どちらかを選択します。 <ul style="list-style-type: none"> <li>特定の装置に対する特権ユーザーを制限する。</li> <li>各ユーザーを 1 装置セッションに限定する。</li> </ul>
リモート・サインオン	許可されるサインオンの試行回数、およびサインオンの最大試行回数に達した場合の処置を指定します。
リモート (Remote)	「リモート・サインオンに Telnet を使用」に、「常にサインオン画面を表示する」オプションを指定します。
タイムアウト	ジョブがタイムアウトに達したときに行うアクションを指定します。さらに、どれほどの時間が経過したら操作がタイムアウトになるかも指定できます。活動状態にないジョブと切断されたジョブの両方について情報を指定できません。

注: これらの設定値は、Telnet だけではなく iSeries サーバー上のすべての対話式装置およびジョブに適用されます。

4. サブシステムに装置を割り当てる。

文字ベースのインターフェースで、次のように入力します。

ADDWSE SBS(DQINTER) WRKSTNTYPE(\*ALL)

5. QSYSWRK サブシステムを活動化する。

QSYSWRK サブシステムの状況を検査します。

- iSeries サーバーの文字ベース・インターフェースで、WRKSBS (活動状態サブシステム処理) と入力します。
- 以下のシステムが表示されることを確かめます。
  - QSYSWRK
  - QINTER
  - QSPL

QSYSWRK サブシステムが活動状態でない場合には、以下のステップを完了します。

- iSeries サーバーの文字ベースのインターフェースで、STRSBS (サブシステム開始) と入力します。
  - サブシステム記述には **QSYSWRK**、ライブラリーには **QSYS** と入力して、**Enter** キーを押します。
  - ライブラリー **QSYS** のサブシステム名 **QINTER**、およびライブラリー **QSYS** のサブシステム名 **QSPL** についても同様に行います。
6. Telnet ユーザー・プロファイルの作成。
- iSeries ナビゲーターを開始して、iSeries サーバーを展開します。
  - 「ユーザーおよびグループ」を右クリックして、「新規ユーザー」を選択します。
  - ユーザー名、説明、およびパスワードを入力します。
  - ジョブ記述を指定するには、「ジョブ」をクリックしてからジョブ記述を入力します。
  - 「OK」をクリックします。

7. Telnet が実行していることを確認します。

Ken は 5250 エミュレーション・セッションを開始して、Telnet サーバーに接続します。

#### 関連概念

29 ページの『iSeries でサポートされているエミュレーション・タイプ』

iSeries で優先されるエミュレーションは 5250 エミュレーションです。ただし、iSeries では 3270 および VTxxx エミュレーションもサポートされています。

#### 関連タスク

22 ページの『Telnet サーバーの構成』

このトピックでは、さまざまなエミュレーション・タイプに対して Telnet サーバーを構成する方法について説明します。

## Telnet シナリオ：カスケード Telnet セッション

このシナリオでは、Telnet セッション中に別の Telnet セッションを開始する機能について示します。接続した後、システム要求値を使用してシステム間を移動できます。

このシナリオでは、ユーザーは複数のサーバーとの Telnet セッションを確立します。これをカスケード *Telnet* セッションと言います。この方式を使用することにより、ユーザーは、以下のことが可能になります。

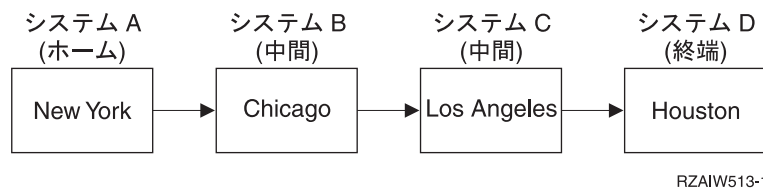
- ホーム・オフィスと Chicago との間に Telnet セッションを確立すること。
- 最初のセッションを終了しないで追加の Telnet サーバーに接続すること。
- セッション相互間を移動して、New York のシステム上にあるジョブに戻ること。

### 状況

Janice Lowe は、Culver Pharmaceuticals の販売部長です。彼女は New York のオフィスから接続して、Telnet を使用することにより Chicago のメイン・システムに接続します。Chicago にある Telnet サーバーとのクライアント・セッションを確立した後で、Janice は Los Angeles のオフィスからのファイルを処理する必要があることに気がきます。

### 目的

Janice は Chicago の Telnet クライアントを使用して、Los Angeles の Telnet サーバーに接続します。Los Angeles に接続しながら、Houston とのセッションを確立することを決めます。



この図は、Janice が確立する接続について示しています。彼女が New York から開始する iSeries サーバーは、ホーム・システムと呼ばれます。そこから彼女は Chicago の中間システム B に接続して、その後 Los Angeles の中間システム C に接続し、さらにそこから Houston の終端システム D に接続します。

### 前提条件および前提事項

このシナリオは、以下を想定しています。

- Telnet サーバーがすべてのシステム上で実行されていること。

- Janice がすべてのシステムにサインオン可能なこと。
- すべてのシステムが i5/OS™ またはそれ以降を実行している iSeries サーバーであること。

## 構成の詳細

Janice は以下のステップを完了して、Telnet システムに接続します。

1. New York システムから、STRTCPELN CHICAGO と入力します。
2. Chicago システムから、STRTCPELN LA と入力します。
3. Los Angeles システムから、STRTCPELN HOUSTON と入力します。

彼女は、Houston システムに接続した後、New York の (ホーム) システム上のタスクを完了したいと考えます。

1. システム要求キーを押します。
2. オプション 14 (ホーム・システムへ転送) を選択します。これにより、ニューヨークのシステム上の代替ジョブに戻ります。

New York システム上の作業を完了した後、彼女は以下のタスクを完了することで Houston システムに戻ることができます。

1. システム要求キーを押します。
2. オプション 15 (終端システムへ転送) を選択します。これにより、彼女は中間システムまたはホーム・システムから終端システムに移行します。

すべてのセッションからサインオフするには、SIGNOFF コマンドを使用します。これにより現行のセッションが終了して、ホーム・システムのサインオン画面に戻ります。

### 関連資料

93 ページの『カスケード Telnet セッションの確立』

Telnet セッションの内部から別の Telnet セッションを確立する方法について説明しています。カスケード・セッションを確立した後、異なるシステム間を移動できます。

94 ページの『複数のカスケード Telnet セッション間の移動』

カスケード Telnet セッションの開始後、SysRq キーを押して Enter を押すと、「システム要求」メニューが表示されます。

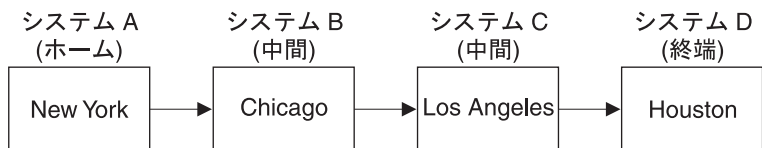
## システム要求処理のシナリオ

以下のシナリオは、複数のタイプのシステム間でシステム要求処理が実行される方法を示しています。

### シナリオ 1

すべてのサーバーが iSeries サーバーです。システム要求処理は正常に実行されます。

イメージは次の設定を示しています。New York にあるホーム・システム A は、Chicago にある中間システム B に接続しています。中間システム B は、Los Angeles にある中間システム C に接続し、中間システム C は、Houston にある終端システム D に接続しています。

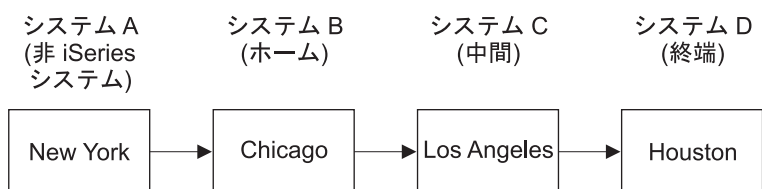


RZAIW513-1

## シナリオ 2

New York システムは 3270 または VTxxx Telnet を使用している非 iSeries サーバーです。

イメージは次の設定を示しています。New York にある非 iSeries サーバーのシステム A は、Chicago にあるホーム・システム B に接続しています。ホーム・システム B は、Los Angeles にある中間システム C に接続し、中間システム C は、Houston にある終端システム D に接続しています。



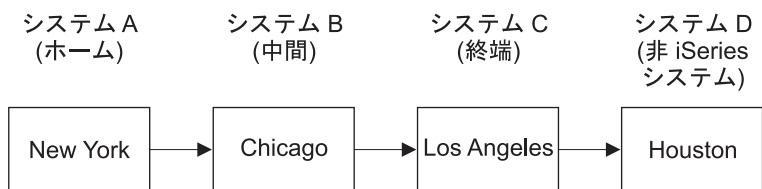
RZAIW516-1

システム要求処理はシナリオ 1 と同様に実行されますが、Chicago がホーム・システムと見なされる点が異なります。ホーム・システムに送信されるすべてのシステム要求は、Chicago システムで処理されます。

## シナリオ 3

Houston システムは 3270 または VTxxx Telnet を使用している非 iSeries サーバーです。

イメージは次の設定を示しています。New York にあるホーム・システム A は、Chicago にある中間システム B に接続しています。中間システム B は、Los Angeles にある中間システム C に接続し、中間システム C は、Houston にある非 iSeries サーバーの終端システム D に接続しています。



RZAIW517-1

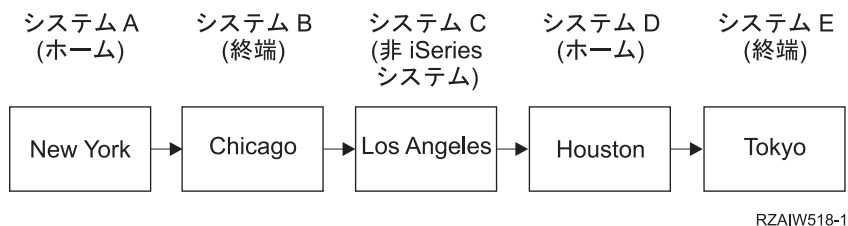
システム要求処理はシナリオ 1 と同様に実行されますが、Los Angeles がすべてのシステム要求処理の終端システムと見なされる点が異なります。「システム要求」キーを押してから実行キーを押すと、Los Angeles 用の「システム要求」メニューが表示されます。

## シナリオ 4

Los Angeles システムは 3270 または VTxxx Telnet を使用している非 iSeries サーバーです。

New York にあるホーム・システム A は、Chicago にある終端システム B に接続しています。終端システム B は、Los Angeles にある非 iSeries サーバー・システム C に接続しています。サーバー・システム

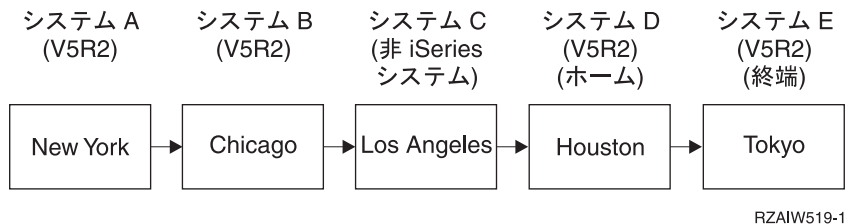
C は、Houston にあるホーム・システム D に接続し、ホーム・システム D は、Tokyo にある終端システム E に接続しています。



システム処理要求はシナリオ 1 と同様に実行されますが、Chicago システムがシステム要求処理の終端システムと見なされる点が異なります。「システム要求」キーを押してから実行キーを押すと、Chicago 用の「システム要求」メニューが表示されます。

システム要求を Tokyo システムに送りたい場合、Houston システムにある機能キーの 1 つを「システム要求」キーにマップすることができます。この機能をマップした場合、Tokyo システムは終端システムとなり、Houston はホーム・システムとなります。

イメージは次の設定を示しています。New York にあるシステム A は、Chicago にあるシステム B に接続しています。システム B は、Los Angeles にある非 iSeries サーバー C に接続しています。サーバー C は、Houston にあるホーム・システム D に接続し、ホーム・システム D は、Tokyo にある終端システム E に接続しています。



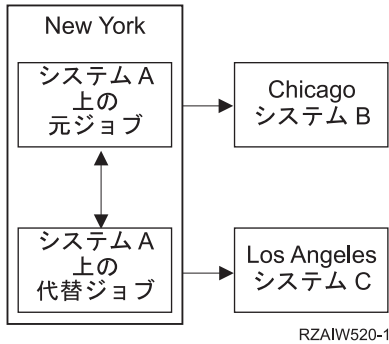
iSeries 3270 Telnet サーバーのマッピング機能の例が示すように、デフォルトのキーボード・マッピングは「システム要求」キーを 3270 PF11 キーとして識別します。iSeries 3270 Telnet クライアントの場合、F11 キーが 3270 PF11 キーにマップされます。Los Angeles システムが 3270 データ・ストリームを使用するシステムである場合、F11 を押すと Los Angeles システムが Houston システム上のシステム要求キーにマップされます。システム要求は Tokyo システムに伝送されて、Tokyo 用の「システム要求」メニューが表示されます。

注: VTxxx データ・ストリームを使用していてブロック・データと文字データとの間をマップしている場合には特に、このマップ機能は複雑です。

## グループ・ジョブの使用

このトピックでは、Telnet、代替ジョブ、およびグループ・ジョブを使用した複数システムでの作業について説明します。

Telnet と代替ジョブを使用すれば、ホーム・システムから複数のシステムにアクセスすることができます。以下の例を考慮してください。



Telnet が New York から Chicago へのセッションを確立します。また、Chicago システムに接続したまま、Los Angeles システムにアクセスするとします。システム要求オプション 11 を使用して、New York システムで代替ジョブを開始することができます。Los Angeles システムへのセッションを確立するには、Telnet コマンドを使用します。他のシステム (たとえば Houston ) に接続するには、Chicago システムまたは Los Angeles システムから別の Telnet セッションを開始します。

代替ジョブを使用する代わりに、グループ・ジョブを使用することができます。グループ・ジョブは、グループ内で同じワークステーション装置とユーザーに関連付けられた、最大で 16 ある対話式ジョブの 1 つです。グループ・ジョブをセットアップするには、以下のステップに従います。

1. グループ属性変更 (CHGGRPA) コマンドを使用して、現行ジョブをグループ・ジョブに変更します。  
CHGGRPA GRPJOB(home)
2. グループ・ジョブへの移行 (TFRGRPJOB) コマンドを使用して、Chicago システム用にグループ・ジョブを開始します。  
TFRGRPJOB GRPJOB(CHICAGO) INLGRPPGM(QCMD)
3. Chicago システムへの Telnet セッションを確立します。  
Telnet CHICAGO
4. ATTN キーを押して、ホーム・システムに戻ります。ATTN キーを押すと、「Telnet 制御機能の送信」メニューが表示されます。
5. 「Telnet 制御機能の送信」メニューの文字ベースのインターフェースで、以下のように入力します。  
TFRGRPJOB GRPJOB(home)  
  
これで、元のジョブに戻ります。

他のグループ・ジョブや Telnet セッションも同様に開始することができます。

TFRGRPJOB GRPJOB(\*SELECT) コマンドを使用すれば、必要なグループ・ジョブを選択することができます。たとえば、CHICAGO、LOSANGELES、HOUSTON、および TOKYO という名前を持つグループ・ジョブが開始する場合、TFRGRPJOB GRPJOB(\*SELECT) コマンドでは以下の画面が表示されます。

```

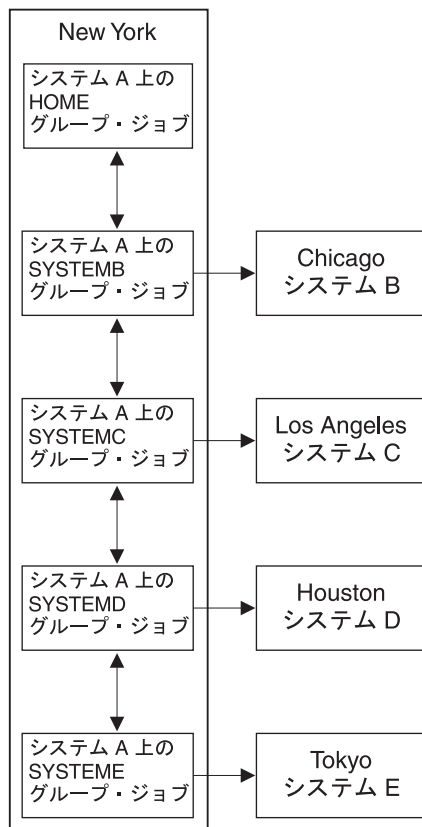
+-----+
|               グループ・ジョブへの移行               |
|                                                           |
|               システム :   SYS198               |
| 活動グループ・ジョブ . . . : HOME                 |
| テキスト . . . . . :                               |
| オプションを入力して、実行キーを押してください。   |
|   1= グループ・ジョブへの移行                       |
| -----抑止されたグループ・ジョブ-----          |
| Opt   グループ・ジョブ   テキスト                   |
|   TOKYO                                     |
|   HOUSTON                                    |
+-----+
  
```

```

-          LOSANGELES
-          CHICAGO
-
  終わり
  F3= 終了   F5= 最新情報   F6= 新しいグループ・ジョブの開始   F12= 取消し
+-----+

```

ここで、Telnet を使用して、適切なジョブから各システムとのセッションを確立することができます。以下の例は、グループ・ジョブ・シナリオを示しています。



RZAIW521-1

グループ・ジョブを終了するには、グループ・ジョブ終了 (ENDGRPJOB) コマンドを使用します。

Telnet セッション内で別のグループ・ジョブに切り替えるには、

1. ATTN キーを押します。
2. 文字ベースのインターフェースで TFRGRPJOB と入力します。

## Telnet シナリオ : SSL で保護された Telnet

Secure Sockets Layer (SSL) を使用して、iSeries 上の Telnet を保護できます。このシナリオでは、構成の例をステップバイステップで示します。

### 状況

Bob は、自宅で仲買業を始めようとしています。彼は大手商社の株式仲買人としての立場から退職しましたが、自宅から少数の得意先に仲買サービスの提供を続けたいと考えています。彼は小型の iSeries サーバーを使って事業を経営しています。そのサーバーから 5250 Telnet セッションを経由して、クライアントに対するアカウント・アクセスを行う計画です。Bob は現在、クライアントがそのアカウントに継続的に



アクセスして、自分の投資を管理できるようにする方法を模索しています。Bob はクライアントが 5250 Telnet セッションを使用してアカウントにアクセスするようにしたいと考えていますが、彼のサーバーおよびクライアントのセッションのセキュリティについて心配しています。iSeries サーバー Telnet セキュリティ・オプションについて検討した後、Bob は Secure Sockets Layer (SSL) を使用して、iSeries サーバーとクライアントとの間の 5250 Telnet セッションを流れるデータのプライバシーを保護することに決めます。

## 目的

このシナリオで Bob は、仲買業のクライアントから iSeries サーバー上の投資アカウントへの 5250 Telnet セッションを保護したいと考えます。Bob は SSL を使用可能にして、クライアント・データがインターネットを通過する際にそのプライバシーを保護したいと考えます。さらに、クライアント認証の証明書を使用可能にして、クライアントだけがそのアカウントにアクセスしていることをサーバーが検証できるようにしたいと考えます。SSL 用に Telnet サーバーを構成し、クライアントおよびサーバーの認証を使用可能にしたら、Bob は新しいアカウント・アクセス可能オプションをクライアントに提供し、アカウント・アクセス・セッションが保護されていることをクライアントに対して保証することができます。以下の目的を達成したら、Bob は新しいアカウント・アクセス可能オプションをクライアントに提供し、その 5250 Telnet セッションが保護されていることをクライアントに対して保証することができます。

- SSL で Telnet サーバーを保護する
- Telnet サーバーがクライアント認証できるようにする
- ローカル認証局 (CA) から専用証明書入手して、それを Telnet サーバーに割り当てる

## 詳細

このシナリオでは、仲介業務の設定は次のとおりです。

- iSeries サーバーは i5/OS バージョン 5 リリース 4 (V5R4) を実行し、5250 Telnet セッションを介した株主口座へのアクセスを提供します。
- i5/OS Telnet サーバー・アプリケーションが iSeries サーバー上で開始されます。
- Telnet サーバーは SSL を初期化して、QIBM\_QTV\_TELNET\_SERVER アプリケーション ID 内の証明書情報を検査します。
- Telnet 証明書構成が正しい場合、Telnet サーバーは SSL ポートでクライアント接続の listen を開始します。
- クライアントは Telnet サーバーへのアクセスを求める要求を開始します。
- Telnet サーバーは応答し、クライアントに証明書を提示します。
- クライアント・ソフトウェアは証明書を検証して、サーバーと通信している受け入れ可能で信頼できるソースであると確認します。
- Telnet サーバーはクライアント・ソフトウェアからの証明書を要求します。
- クライアント・ソフトウェアは Telnet サーバーへの証明書を示します。
- Telnet サーバーは証明書を検査して、クライアントがサーバーとの間に 5250 セッションを確立する権利があることを認めます。
- Telnet サーバーはクライアントとの間に 5250 セッションを確立します。

## 前提条件および前提事項

このシナリオは、以下を想定しています。

- iSeries サーバーが i5/OS バージョン 5 リリース 2 (V5R2) 以上を実行していること。



- TCP/IP が構成済みであること。
- Bob に IOSYSCFG 権限があること。
- Telnet サーバーが構成済みであること。
- Bob が SSL 使用可能化の計画の問題に取り組んでいること。
- Bob が iSeries サーバー上にローカル認証局を作成していること。

## タスク・ステップ

このシナリオをインプリメントするために、Bob が完了しなければならない 2 つのステップがあります。最初の一連のタスクでは、SSL の使用に合わせて iSeries サーバーをセットアップして、ユーザー認証のために証明書を要求します。もう一方の一連のタスクでは、Telnet クライアント上のユーザーが Bob の Telnet サーバーとの SSL セッションに参加して、ユーザー認証のための証明書を取得することを可能にします。

Bob は以下のタスク・ステップを実行して、このシナリオを完了します。

### Telnet サーバーのタスク・ステップ

このシナリオをインプリメントするために、Bob は iSeries サーバー上で以下のタスクを実行しなければなりません。

1. ポート制限を除去する
2. ローカル認証局を作成および操作する
3. クライアント認証の証明書を要求するように Telnet サーバーを構成する
4. Telnet サーバー上で SSL を使用可能にして開始する

### クライアント構成タスクのステップ

このシナリオをインプリメントするには、Bob の iSeries サーバー上の Telnet サーバーにアクセスする各ユーザーが以下のタスクを実行しなければなりません。

5. Telnet クライアントで SSL を使用可能にする
6. Telnet クライアントが認証のための証明書を提示できるようにする

これらのタスクは SSL およびクライアント認証を証明書によって実行するので、5250 Telnet セッションを使用する Bob のクライアントのアカウント情報へのアクセスが SSL で保護されることになります。

## 構成の詳細

このトピックでは、SSL で Telnet を保護するためのタスク・ステップについて説明します。

### ステップ 1: ポート制限を除去する

V5R1 より前のリリースでは、Telnet では Secure Sockets Layer (SSL) サポートが利用不能であったため、ポート制限が使用されていました。現在では、SSL、非 SSL、またはその両方を開始するかどうかを指定できるようになりました。したがって、ポート制限は不要になりました。以前のリリースでポート制限を定義した場合、SSL パラメーターを使用するためにはそのポート制限を除去する必要があります。

Telnet のポート制限の有無を判別して、それを除去することにより Telnet サーバーが SSL を使用できるように構成するには、以下のステップを行います。

1. 現行のポート制限を表示するには、iSeries ナビゲーターを開始して、**iSeries サーバー** → 「ネットワーク」を展開します。
2. 「**TCP/IP 構成**」を右クリックしてから、「**プロパティ**」を選択します。
3. 「**ポート制限**」タブをクリックして、ポート制限の設定値のリストを表示します。
4. 除去したいポート制限を選択します。
5. 「**除去**」をクリックします。
6. 「**OK**」をクリックします。

デフォルトでは、SSL セッションをポート 992、非 SSL セッションをポート 23 で開始する設定となっています。Telnet サーバーは Telnet のサービス・テーブル項目を使用して非 SSL ポートを取得し、Telnet-SSL を使用して SSL ポートを取得します。

## ステップ 2: ローカル認証局を作成および操作する

デジタル証明書マネージャー (DCM) を使用して iSeries サーバー上にローカル CA を作成して操作するには、以下のステップを行います。

1. DCM を開始します。
2. DCM のナビゲーション・フレームで、「**認証局 (CA) の作成 (Create a Certificate Authority (CA))**」を選択して一連のフォームを表示します。これらのフォームに示された手順に従って、ローカル CA を作成し、SSL のためのデジタル証明書の使用、オブジェクト署名、および署名検査に必要な他のタスクを完了することができます。
3. 表示されたすべてのフォームを完成させます。iSeries サーバー上にローカル CA を作成して操作するために実行する必要があるタスクごとにフォームがあります。これらのフォームを完成させることにより、以下を行うことができます。
  - a. ローカル CA 証明書のための秘密鍵を保管する方法を選択します。このステップが含まれるのは、IBM(R) 4758-023 PCI 暗号化コプロセッサが iSeries にインストールされている場合だけです。システムに暗号化コプロセッサがない場合、DCM は証明書とその秘密鍵をローカル CA 証明書ストアに自動的に保管します。
  - b. そのローカル CA の識別情報を指定します。
  - c. PC またはブラウザにローカル CA 証明書をインストールします。これにより、ソフトウェアがローカル CA を認識して、その CA が発行する証明書を妥当性検査することができるようになります。
  - d. ローカル CA のポリシー・データを選択します。
  - e. 新規のローカル CA を使用して、アプリケーションが SSL 接続のために使用できるサーバーまたはクライアント証明書を発行します。iSeries サーバーに IBM 4758-023 PCI 暗号化コプロセッサがインストールされている場合、このステップによりサーバーまたはクライアント証明書の秘密鍵を保管する方法を選択できるようになります。システムにコプロセッサがない場合、DCM は証明書とその秘密鍵を \*SYSTEM 証明書ストアに自動的に保管します。DCM はタスクの一部として \*SYSTEM 証明書ストアを作成します。
  - f. SSL 接続のためにサーバーまたはクライアント証明書を使用できるアプリケーションを選択します。

注: i5/OS Telnet サーバー (QIBM\_QTV\_TELNET\_SERVER) のアプリケーション ID を必ず選択してください。

- g. 新規のローカル CA を使用して、アプリケーションがオブジェクトにデジタル署名を行うために使用できるオブジェクト署名証明書を発行します。これによりオブジェクト署名証明書の管理に使用する \*OBJECTSIGNING 証明書ストアが作成されます。

注: このシナリオではオブジェクト署名証明書を使用しませんが、このステップを必ず完了してください。タスクのこの時点でキャンセルすると、タスクは終了してユーザーは SSL 証明書の構成を完了するために個々のタスクを実行する必要があります。

- h. ローカル CA をトラストさせたいアプリケーションを選択します。

注: i5/OS Telnet サーバー (QIBM\_QTV\_TELNET\_SERVER) のアプリケーション ID を必ず選択してください。

ガイド付きタスクのためのフォームを完成させた後、Telnet サーバーを構成してクライアント認証を要求することができます。

### ステップ 3: クライアント認証の証明書を要求するように Telnet サーバーを構成する

このサポートを活動化するため、システム管理者は SSL サポートの処理方法を指示します。iSeries ナビゲーターの「Telnet 汎用プロパティ」パネルを使用すれば、Telnet サーバーの始動時に SSL サポートまたは非 SSL サポート (あるいは両方のサポート) を開始するかどうかを指示できます。デフォルトでは SSL サポートおよび非 SSL サポートが常に開始します。

システム管理者は、システムにおけるすべての Telnet セッションで SSL クライアント認証を必須にするかどうかを指示できます。SSL が活動状態になっていてシステムがクライアント認証を必要とするとき、有効なクライアント証明書が存在することは、クライアントが信頼されていることを意味します。

クライアント認証の証明書を要求するように Telnet サーバーを構成するには、以下のステップを行います。

1. DCM を開始します。
2. 「証明書ストアの選択 (Select a Certificate Store)」をクリックします。
3. オープンする証明書ストアとして \*SYSTEM を選択して、「続行」をクリックします。
4. \*SYSTEM 証明書ストアのための適切なパスワードを入力して、「続行」をクリックします。
5. 左のナビゲーション・メニューが最新表示したら、「アプリケーションの管理 (Manage Applications)」を選択します。タスクのリストが表示されます。
6. 「アプリケーション定義の更新 (Update application definition)」タスクを選択します。一連のフォームが表示されます。
7. 「サーバー・アプリケーション (Server application)」を選択して、「続行」をクリックします。サーバー・アプリケーションのリストが表示されます。
8. アプリケーションのリストから、「i5/OS TCP/IP Telnet Server」を選択します。
9. 「アプリケーション定義の更新 (Update Application Definition)」をクリックします。
10. 表示される表で、「はい」を選択して、クライアント認証を要求します。
11. 「適用」をクリックします。「アプリケーション定義の更新 (Update Application Definition)」ページに、変更を確認するためのメッセージが表示されます。
12. 「完了」をクリックします。

クライアント認証のための証明書を要求するように Telnet サーバーを構成したので、SSL を Telnet サーバーで開始できます。

## ステップ 4: Telnet サーバー上で SSL を使用可能にして開始する

Telnet サーバーで SSL を使用可能にするには、以下のステップに従います。

1. iSeries ナビゲーターを開きます。
2. **iSeries** サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を拡張します。
3. 「Telnet」を右クリックします。
4. 「プロパティ」を選択します。
5. 「一般」タブを選択します。
6. SSL サポートのオプションのうちの 1 つを選択します。
  - 「セキュアのみ」 Telnet サーバーとの SSL セッションのみを許可する場合に選択します。
  - 「非セキュアのみ」 Telnet サーバーとの保護されたセッションを禁止する場合に選択します。SSL ポートへ接続しようとする試みは失敗します。
  - 「セキュアと非セキュアの両方」 Telnet サーバーとの保護されたセッションと保護されていないセッションの両方を許可します。

iSeries ナビゲーターを使用して Telnet サーバーを開始するには、以下のステップに従います。

1. **iSeries** サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を拡張します。
2. 右側区画の「サーバー名」列で、**Telnet** を見つけます。
3. 「状況」列に「開始済み」と表示されていることを確認します。
4. サーバーが実行していない場合には、「Telnet」を右クリックして、「開始」を選択します。

## ステップ 5: Telnet クライアントで SSL を使用可能にする

SSL セッションに参加するためには、Telnet クライアントは、Telnet サーバーが SSL セッションを確立するために提示する証明書を認識して受け入れることができなければなりません。Telnet クライアントがサーバーの証明書を認証するためには、iSeries の鍵データベース内に CA 証明書のコピーを保持していることが必要です。Telnet サーバーがローカル CA からの証明書を使用するとき、Telnet クライアントはローカル CA 証明書のコピーを取得して、それを iSeries の鍵データベースにインストールしなければなりません。

ローカル CA 証明書を iSeries から追加して、ローカル CA からの証明書を使用する Telnet サーバーと共に Telnet クライアントが SSL セッションに参加できるようにするには、以下のステップに従ってください。

1. iSeries ナビゲーターを開きます。
2. システムの名前を右マウス・ボタンでクリックします。
3. 「プロパティ」を選択します。
4. 「セキュア・ソケット」タブを選択します。

**注:** このタブは iSeries Client Encryption (128 ビット)、5722-CE3 の選択的なインストールを完了していない場合には表示されません。

5. 「ダウンロード」をクリックします。これにより、iSeries 認証局証明書が証明書鍵データベースに自動的にダウンロードされます。
6. 鍵データベースのパスワードを入力するようプロンプトが出されます。事前にデフォルトのパスワードを変更していなければ、ca400 と入力します。確認メッセージが表示されます。「OK」をクリックします。

ダウンロード・ボタンをクリックすると、IBM Toolbox for Java™ PC の鍵データベースを自動的に更新します。

## ステップ 6: Telnet クライアントが認証のための証明書を提示できるようにする

サーバーがローカル CA の発行する証明書を信頼するように指定して、そしてクライアント認証に証明書が必要であることを指定して、SSL を Telnet サーバーに構成しました。これで、ユーザーは接続を試行するたびに Telnet サーバーに有効で信頼できるクライアント証明書を提示する必要があります。

クライアント認証が機能するようになる前に、クライアントはローカル CA を使用して、Telnet サーバーへの認証の証明書を取得し、その証明書を IBM 鍵管理データベースにインポートする必要があります。

最初に、以下のステップに従ってクライアントは DCM を使用してユーザー証明書を取得しなければなりません。

1. DCM を開始します。
2. 左のナビゲーション・フレームで「**証明書の作成 (Create Certificate)**」を選択します。タスクのリストが表示されます。
3. タスク・リストから、「**ユーザー認証**」を選択して「**続行**」をクリックします。
4. 「**ユーザー認証**」フォームに記入します。記入する必要があるのは、「必要」とマーク付けされたフィールドだけです。「**続行**」をクリックします。
5. ブラウザーから、ブラウザーにロードする証明書を生成するよう要求されます。ブラウザーの指示に従います。
6. 「**ユーザー証明書の作成 (Create User Certificate)**」ページが再ロードされたら、「**証明書のインストール (Install Certificate)**」をクリックします。これにより、ブラウザーに証明書がインストールされます。
7. PC に証明書をエクスポートします。証明書をパスワード保護ファイルに保管しなければなりません。

注: エクスポート機能およびインポート機能を使用するには、Microsoft® Internet Explorer 5 または Netscape 4.5 が必要です。

次に、以下のステップに従って証明書を IBM 鍵管理データベースにインポートして、Telnet クライアントが認証のために使用できるようにしなければなりません。

クライアント証明書を作成した認証局を、PC の鍵データベースに追加しなければなりません。そうしないと、クライアント証明書をインポートできません。

1. 「**スタート**」 → 「**プログラム**」 → 「**IBM iSeries Access for Windows**」 → 「**iSeries Access for Windows Properties**」とクリックします。
2. 「**セキュア・ソケット**」タブを選択します。
3. 「**IBM 鍵管理 (IBM Key Management)**」をクリックします。
4. 鍵データベースのパスワードを入力するようプロンプトが出されます。事前にデフォルトのパスワードを変更していなければ、ca400 と入力します。確認メッセージが表示されます。「**OK**」をクリックします。
5. プルダウン・メニューから、「**個人用証明書 (Personal certificates)**」を選択します。
6. 「**インポート**」をクリックします。
7. 「**鍵のインポート (Import key)**」画面で、証明書のファイル名およびパスを入力します。「**OK**」をクリックします。



8. 保護ファイルのパスワードを入力します。これは DCM にユーザー証明書を作成したときに指定したパスワードと同じです。「OK」をクリックします。証明書が IBM 鍵管理内の個人用証明書に正常に追加されると、PC5250 エミュレーターまたはその他の Telnet アプリケーションを使用できるようになります。

これらのステップが完了すると、Telnet サーバーは Telnet クライアントとの間に SSL セッションを確立して、サーバーはクライアントが提示する証明書に基づいてユーザーを認証することができます。

### 関連タスク

デジタル証明書マネージャーの開始

37 ページの『証明書を Telnet サーバーに割り当てる』

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows®、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

---

## Telnet サーバーの計画

このトピックを使用して、システムに接続されたワークステーションに関連付ける仮想装置の数を判別します。また、このトピックでは、Telnet へのアクセスを制御したり妨げたりするためのセキュリティの手順も示されています。

Telnet サーバーを構成する前に、考慮しなければならないいくつかのセキュリティおよび操作上の性質があります。Telnet に自動構成させる仮想装置の数や、独自の仮想装置を作成するかどうかを決めておく必要があります。自動構成される仮想装置の数は、許可されるサインオンの試行回数に影響します。サインオンの試行回数が増えると、権限が与えられていないユーザーがサーバーにアクセスする可能性が増えることになります。Telnet サーバーが切断された接続を検出するようにするなど、セキュリティ上の他の方法も検討できます。

## 仮想装置記述

このトピックでは、仮想装置記述を構成して名前を付けることについて説明します。

Telnet は仮想装置記述を使用して、オープンな Telnet セッションに関するクライアント・ワークステーションの情報を保持します。仮想装置とは、リモート・システムに接続された物理ワークステーションとユーザーの間の接続を確立するために使用される装置記述です。仮想装置は物理装置 (表示装置または印刷装置) に関する情報をサーバー上のプログラムに提供します。サーバーは接続しているクライアント/サーバー・プロトコルを探し、仮想装置を指定します。指定された仮想装置を見つけられない場合、サーバーは登録済み出口プログラムで指定された仮想装置を探します。サーバーが仮想装置を見つけられない場合、ローカル・システム上の装置に類似した装置タイプおよびモデルに仮想装置記述を合わせようとします。

## 仮想制御装置および装置の Telnet 命名規則

i5/OS 標準によると、Telnet サーバーは、自動的に作成された仮想制御装置および装置を命名するために、以下の規則を使用します。

- 仮想制御装置の場合、サーバーは名前 QPACTL *nn* を使用します。ここで、*nn* は、01 以上の 10 進数です。
- 仮想装置の場合、サーバーは、名前 QPADEV *xxxx* を使用します。ここで、*xxxx* は 0001 から zzzzz の英数字 (母音を除く) です。
- 名前付き装置の場合、サーバーは仮想制御装置に QVIRCD *nnnn* の名前を付ける。

注:

1. i5/OS 命名規則の下では、仮想制御装置の名前は QPACTL *nm* である必要があります。
2. 仮想装置の名前は、QPADEV *xxxx* です。
3. ユーザーが作成した仮想装置には、QTCP ユーザー・プロファイル権限を認可する必要があります。
4. QAUTOVRT の \*REGFAC オプションを使用して、自動的に作成された仮想装置の命名規則を変更することができます。詳細については、『システム値』のトピックの『QAUTOVRT』を参照してください。

可能なサインオンの試行回数は、自動構成された仮想装置の数と共に増加します。サインオンの試行回数の合計は、可能なシステム・サインオン試行回数に作成可能な仮想装置の数を掛けたものです。サインオン・システム値によって、可能なサインオンの試行回数が決まります。

同じ装置タイプとモデルの仮想装置を選択すると、Telnet サーバーは、自動的に作成された既存の仮想装置のうちの使用可能なものを再利用します。一致する装置タイプとモデルがなくても、仮想装置がまだ使用可能であれば、ネゴシエーションされたクライアント装置とモデルに一致するように、その装置タイプとモデルが変更されます。これは、自動作成された仮想装置 (QPADEV *xxxx*) と名前付き装置の両方に当てはまります。

独自の装置を手動で作成することにした場合は、構成を容易に管理できるような命名規則を確立する必要があります。名前が i5/OS オブジェクト命名規則に従っていれば、希望する装置名および制御装置名をどれでも選択することができます。

仮想装置の作成手順については、『仮想装置の数の設定』を参照してください。

#### 関連概念

25 ページの『独自の仮想装置の作成』

カスタム名または自動生成された名前を持つ仮想装置を手動で作成することができます。

#### 関連タスク

23 ページの『仮想装置の数を設定する』

このトピックでは、Telnet サーバーの仮想装置の数の設定と、許可されるサインオンの試行回数を制限することについて説明します。

## Telnet のセキュリティー

このトピックでは、サーバー上の Telnet を保護する手順が示されています。

TCP 接続で Telnet を開始する際には、Telnet を介した iSeries サーバーへのユーザー・アクセスを許可したり拒否したりするための、セキュリティー上の手段を考慮する必要があります。たとえば、サインオン試行回数や、ユーザーが使用してサインオンできる装置の数の制限および制御を設ける必要があります。

### Telnet アクセスの防止

Telnet サーバーを使用する計画がない場合、このトピックのステップに従い、Telnet サーバーを使用不可にしてください。この手続きにより、自分の知らないうちにサーバーが使用されることを防止できます。

iSeries サーバーに Telnet を使用してアクセスされないようにする場合は、Telnet サーバーが実行されないようにする必要があります。Telnet が iSeries にアクセスしないようにするには、以下のタスクを完了してください。

## Telnet が自動的に開始しないようにする

TCP/IP の開始時に Telnet サーバー・ジョブが自動的に開始しないようにするには、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 サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と展開します。
2. 「Telnet」を右クリックして、「プロパティ」を選択します。
3. 「TCP/IP の開始時に開始する (Start when TCP/IP starts)」をクリアします。

## Telnet ポートにアクセスしないようにする

Telnet が開始しないようにするため、およびソケット・アプリケーションなどのユーザー・アプリケーションと iSeries が通常 Telnet 用に使用するポートとが関連付けられないようにするために、以下のステップに従ってください。

1. iSeries ナビゲーターを開始し、iSeries サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を展開します。
2. 「TCP/IP 構成」を右クリックしてから、「プロパティ」を選択します。
3. 「TCP/IP 構成プロパティ (TCP/IP Configuration Properties)」ウィンドウで、「ポート制限」タブをクリックします。
4. 「ポート制限」ページで、「追加」をクリックします。
5. 「ポート制限の追加」ページで、以下の値を指定します。
  - **ユーザー名 (User name):** iSeries で保護されているユーザー・プロファイル名を指定します。(保護されたユーザー・プロファイルとは、権限を借用するプログラムを所有せず、他のユーザーが知っているパスワードを持たないユーザー・プロファイルのことです。) ポートを特定のユーザーに制限することにより、他のすべてのユーザーは自動的に除外されます。
  - **開始ポート:** 23 (非 SSL TELNET の場合) または 992 (SSL TELNET の場合)
  - **終了ポート:** 23 (非 SSL TELNET の場合) または 992 (SSL TELNET の場合)
  - **プロトコル:** TCP

注: これらのポート番号は、「サービス・テーブル項目の処理」(WRKSRVTBLE) テーブルで、.Telnet-ssl の下に指定されます。それらは 23 と 992 以外のポートにマップされることがあります。制限するポートごとに、このプロセスを繰り返してください。Internet Assigned Numbers Authority (IANA) には、共通のポート番号割り当てに関する情報が示されています。

6. 「OK」をクリックして制限を追加します。
7. 「ポート制限」ページで「追加」をクリックして、ユーザー・データグラム・プロトコル (UDP)・プロトコルでも同じ手順を繰り返します。
8. 「OK」をクリックしてポート制限を保管してから、「TCP/IP 構成プロパティ」ウィンドウをクローズします。
9. ポート制限は次回 TCP/IP を開始したときから有効になります。ポート制限の設定時に TCP/IP が活動状態である場合、TCP/IP を終了してから再開始してください。

### 関連情報

Internet Assigned Numbers Authority (IANA)



## Telnet アクセスの制御

このトピックでは、Telnet サーバーが危害を被らないように保護するためのヒントが示されています。

以下は、Telnet クライアントがシステムにアクセスする際のセキュリティー上の考慮事項と提案です。

### クライアント認証

Telnet サーバーは、現在サポートされている SSL サーバー認証に加えて、クライアント認証もサポートしています。使用可能になっているなら、Telnet クライアントが Telnet SSL ポートに接続する際、iSeries Telnet サーバーはサーバー証明書とクライアント証明書の両方を認証します。Telnet SSL ポートに接続しようとする際に有効なクライアント証明書を送信しない Telnet クライアントは、表示または印刷装置セッションの確立に失敗します。V4R5 では、SSL クライアント認証をオンにする方法についての説明が PTF カバー・レター 5769-SS1-PTF SF61427 に記載されています。V5R1 以降は、デジタル証明書マネージャー (DCM) を使用して、SSL クライアント認証を使用可能または使用不可にすることができます。

### パスワードの保護

従来のクライアントとサーバーとの間で送信される場合、Telnet パスワードは暗号化されません。接続方式によっては、システムが回線盗聴によるパスワードの窃盗に対して無防備となっています。暗号化されたパスワードを交換するために TN5250E ネゴシエーションを使用する場合、Telnet パスワードは暗号化されます。そのような場合、サインオン画面をバイパスして、クリア・テキスト形式のパスワードをネットワーク上で伝送しないようにできます。TN5250E によって暗号化されるのはパスワードのみです。すべての通信を暗号化するには SSL が必要です。

注：電子機器を使用して回線をモニターすることを、多くの場合盗聴 と呼びます。

しかし、SSL Telnet サーバーと、SSL を使用可能な Telnet クライアントを使用するなら、パスワードを含むすべてのトランザクションが暗号化されて保護されます。Telnet SSL ポートは、WRKSRVTBLE エントリーの .Telnet-ssl の下で定義されています。これは、サインオンの試行回数を制限します。QMAXSIGN システム値が Telnet に適用されますが、仮想装置を自動的に構成するようにシステムをセットアップすると、このシステム値の効果が減少する可能性があります。QAUTOVRT システム値が 0 より大きな値であるとき、失敗した Telnet ユーザーは再接続して新規に作成された仮想装置に連結することができます。以下のいずれかの状態となるまで、これを続けることが可能です。

- すべての仮想装置が使用不可となり、システムが作成可能な新規の仮想装置の数を超過する。
- すべてのユーザー・プロファイルが使用不可となる。
- ハッカーがシステムへのサインオンに成功する。

仮想装置を自動的に構成すると、可能な Telnet の試行回数が倍加します。

注：仮想装置の制御を容易にするために、短時間だけ QAUTOVRT システム値を 0 よりも大きい値にした場合があります。自分で Telnet を使用してシステムに装置を作成させるか、または他のユーザーがシステムに十分な数の仮想装置を作成させるまで待ちます。その後、QAUTOVRT システム値を 0 に設定します。

Telnet の機能強化により、ハッカーがシステムに侵入しようとする試行回数を制限することができるようになりました。クライアントが Telnet セッションの開始を試行するたびにシステムによって呼び出される出口プログラムを作成することができます。出口プログラムは要求元の IP アドレスを受け取ります。短時間の間に同じ IP アドレスから一連の要求が来たことをプログラムが発見すると、プログラムはそのアドレ

スからの以降の要求を拒否して QSYSOPR メッセージ待ち行列にメッセージを送るなどの処置を行うようにすることができます。『Telnet 出口プログラム機能の概要』では、Telnet 出口プログラム機能について概説します。

注: あるいは、Telnet 出口プログラムを使用してロギングを行うこともできます。潜在的な侵入が試行されたかどうかをプログラムによって判別する代わりに、Telnet セッションを開始しようとする試行をロギング機能を使用してモニターすることができます。

## 活動状態にないセッションの終了

Telnet セッションは、システムの QINACTITV 処理に含められています。QINACTMSGQ システム値は、活動状態にないジョブのタイムアウト間隔が満了したときに非活動状態となる、対話的 Telnet セッションのアクションを定義します。QINACTMSGQ がジョブの切断を指示する場合、セッションは切断ジョブ機能をサポートしていなければなりません。サポートしていない場合、ジョブは切断されずに終了します。QPADEVxxxx という名前の装置記述の使用を続ける Telnet セッションは、ユーザーがそれらのジョブから切断されることを許可しません。それらのジョブからの切断が許可されないのは、ユーザーがどの装置記述に再接続されるかが予測できないからです。ジョブが切断されると、そのジョブが再接続されるときにユーザーのために同じ装置記述が必要になります。

## サインオン回数の制限

自動構成された仮想装置を使用している場合は、許可される Telnet サインオンの回数は増えます。iSeries ナビゲーターの装置システム値は、Telnet が作成できる仮想装置の数を定義します。

サインオン・システム値は、許可されるシステム・サインオンの回数を定義します。iSeries ナビゲーターでこの値を設定するための手順については、25 ページの『特定の装置に対する特権ユーザーを制限し、サインオンの試行回数を制限する』を参照してください。

## 強力なユーザー・プロファイルの制限

QLMTSECOFR システム値を使用して、\*ALLOBJ または \*SERVICE 特殊権限を持つユーザーを制限することができます。ユーザーまたは QSECOFR は、サインオンする装置に対する明示的な許可が必要です。そのため、QSECOFR がどの仮想装置に対する権限も持たないようにすることによって、\*ALLOBJ 特殊権限を持つユーザーが Telnet を使用してシステムにアクセスすることを防ぐことができます。\*ALLOBJ 特殊権限を持つすべての Telnet ユーザーを回避する代わりに、強力な Telnet ユーザーを位置ごとに制限することができます。Telnet 開始出口点を使用して、要求元の IP アドレスに基づいて特定の iSeries 装置記述をセッション要求に割り当てる出口プログラムを作成することができます。

## 位置による機能の制御

Telnet 要求の発生場所に基づいて、許可する機能やユーザーに表示するメニューを制御したい場合があります。QDCRDEVD API (アプリケーション・プログラミング・インターフェース) は、要求元の IP アドレスへのアクセスを可能にします。以下は、このサポートを使用するための提案事項です。

- この API をすべてのユーザーに対する初期プログラムで使用することができます (環境の中で Telnet の活動が重要である場合)。
- サインオンを要求したユーザーの IP アドレスに基づいて、ユーザーのためのメニューを設定したり、特定のユーザー・プロファイルに切り替えることもできます。
- Telnet 出口プログラムを使用して、要求元の IP アドレスに基づく決定を行うことができます。これにより、すべてのユーザー・プロファイルで初期プログラムを定義する必要はなくなります。たとえば、

ユーザーの初期メニューの設定、ユーザーの初期プログラムの設定、または Telnet セッションが実行するユーザー・プロファイルの設定を行うことができます。

さらに、ユーザーの IP アドレスにアクセスすることによって、ユーザーの IP アドレスに関連した印刷装置に動的に印刷することができます。QDCRDEVD API も印刷装置の IP アドレスおよび表示装置の IP アドレスを戻します。印刷装置には DEVD1100 フォーマット、表示装置には DEVD0600 フォーマットを選択してください。

## 自動サインオンの制御

Telnet は、ユーザー・プロファイル名とパスワードを Telnet セッション要求と共に送信することにより、iSeries Access for Windows のユーザーがサインオン画面をバイパスする機能をサポートしています。システムは QRMTSIGN (Remote sign-on) システム値の設定値を使用して、自動サインオンの要求を処理する方法について判別します。以下の表では、オプションを示しています。これらのオプションが適用されるのは、Telnet 要求にユーザー ID およびパスワードが含まれているときだけです。

表 2. QRMTSIGN システム設定のオプション

オプション	Telnet での QRMTSIGN の処理内容
*REJECT	自動サインオンを要求する Telnet セッションは許可されません。
*VERIFY	ユーザー・プロファイルとパスワードの組み合わせが有効であれば、Telnet セッションが開始します。 <sup>1</sup>
*SAMEPRF	ユーザー・プロファイルとパスワードの組み合わせが有効であれば、Telnet セッションが開始します。 <sup>1</sup>
*FRCSIGNON	システムはユーザー・プロファイルおよびパスワードを無視します。ユーザーにはサインオン画面が表示されます。

<sup>1</sup> 登録された Telnet 出口プログラムは、要求元に自動サインオンを許可するかどうかを (おそらく IP アドレスに基づいて) 選択することにより、QRMTSIGN の設定値を指定変更することができます。

この妥当性検査は、Telnet 出口プログラムの実行前に行われます。出口プログラムは、妥当性検査の結果を示す標識を受け取ります。出口プログラムは、その標識とは関係無くセッションを許可または拒否することができます。標識は、以下のいずれかの値を持ちます。

- 値 = 0、クライアント・パスワード / パスフレーズ (または Kerberos チケット) が妥当性検査されなかった、あるいは何も受信しなかった。
- 値 = 1、クライアントのクリア・テキスト・パスワード / パスフレーズが妥当性検査された。
- 値 = 2、クライアント暗号化パスワード / パスフレーズ (または Kerberos チケット) が妥当性検査された。

## 匿名サインオンの許可

Telnet 出口プログラムを使用して、.anonymous または .guest Telnet をシステムで使用することができます。出口プログラムにより、要求元の IP アドレスを検出できます。IP アドレスが組織の外部からのものであれば、Telnet セッションにシステムに対する制限された権限と特定のメニューを持つユーザー・プロファイルを割り当てることができます。サインオン画面をバイパスして、その訪問者が他のより強力なユーザー・プロファイルを使用する機会を持たないようにすることもできます。このオプションでは、ユーザーがユーザー ID とパスワードを入力する必要はありません。

## Telnet 出口プログラム機能の概要

Telnet セッションが開始するときと終了するときの両方に実行する、ユーザー作成の出口プログラムを登録することができます。以下は、出口プログラムを開始するときに行うことのできる事柄の例です。

- クライアント SSL 証明書を使用して、ユーザー・プロファイルを証明書に関連付け、サインオン画面をバイパスしてユーザー・プロファイルを Telnet セッションに割り当てることができます。
- サーバー (ローカル) IP アドレスを複数のホームを持つ iSeries サーバーで使用して、ネットワーク・インターフェース (IP アドレス) に基づいて接続を異なるサブシステムに経路指定することができます。
- ユーザーの IP アドレス、時刻、要求されたユーザー・プロファイル、装置タイプ (印刷装置など)、その他の既知の基準に基づいて、セッションを許可または拒否します。
- 特定の iSeries 装置記述をセッションに割り当てます。これにより、それらの装置を受け入れるようにセットアップされたサブシステムに対話式ジョブを経路指定することができます。
- キーボードや文字セットなど、特定の各国語値をセッションに割り当てます。
- 特定のユーザー・プロファイルをセッションに割り当てます。
- 要求元を自動的にサインオンします (サインオン画面は表示しません)。
- セッションの監査ロギングをセットアップします。

### 関連概念

24 ページの『仮想装置の自動構成』

設定された最大数までの範囲で、必要なだけ仮想装置を自動的に作成するよう Telnet サーバーを構成できます。

46 ページの『Telnet 出口プログラムの使用』

このトピックでは、Telnet サーバーで出口プログラムを使用するための情報について説明します。

### 関連タスク

デジタル証明書マネージャー (DCM)

27 ページの『セッション・キープアライブ・パラメーターを設定する』

TCP キープアライブ・パラメーターを使用すれば、プローブを送信して非活動セッションをテストする前に TCP プロトコルが許可する最大アイドル時間を設定することができます。

### 関連資料

装置システム値

サインオン・システム値

### 関連情報

テクニカル・スタジオ: Telnet エグジット・プログラム

---

## Telnet サーバーの構成

このトピックでは、さまざまなエミュレーション・タイプに対して Telnet サーバーを構成する方法について説明します。

Telnet の最も重要な機能の 1 つとして、クライアントとサーバーの間でオプションをネゴシエーションする能力があります。このようにオープンなネゴシエーションにより、クライアントとサーバーのどちらでも、要求を開始したり、実行したりすることが可能になります。要求をネゴシエーションし、それらのを出力に変換するために、各種のエミュレーション・タイプを使用できます。iSeries サーバーは、3270 タイプのワークステーションと VTxxx ワークステーションをサポートすることができますが、推奨されているタイプは 5250 エミュレーションです。



サポートされているいずれかのエミュレーション・タイプを使用するように Telnet サーバーを構成するには、以下のタスクを完了します。

Telnet を構成すると、Secure Sockets Layer (SSL) を使用して Telnet を保護することができます。

#### 関連概念

2 ページの『Telnet シナリオ : Telnet サーバーの構成』

この構成シナリオでは、管理者が Telnet サーバーをカスタマイズする様子を示します。

## Telnet サーバーの開始

このトピックでは、Telnet サーバーの開始について説明します。

活動状態になっている Telnet サーバーには、QSYSWRK サブシステムで実行しているジョブ (QTVTELNET および QTVDEVICE) のそれぞれに 1 つまたは複数のインスタンスがあります。

iSeries ナビゲーターを使用して Telnet サーバーを開始するには、以下のステップに従います。

1. **iSeries** サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を拡張します。
2. 右側区画の「サーバー名」列で、**Telnet** を見つけます。
3. 「状況」列に「開始済み」と表示されていることを確認します。
4. サーバーが実行していない場合には、「**Telnet**」を右クリックして、「**開始**」を選択します。

#### 次の手順:

初めて Telnet サーバーを構成する場合には、『仮想装置の数を設定する』に進みます。

#### 関連概念

45 ページの『サーバー・セッションの終了』

このトピックの説明に従って、Telnet セッションを終了します。Telnet セッションを終了すると、仮想装置が解放され、新しい Telnet セッションでこの装置を使えるようになります。

#### 関連タスク

28 ページの『QSYSWRK サブシステムを活動化する』

TCP/IP アプリケーションのサーバー・ジョブは、QSYSWRK サブシステムで開始しなければなりません。印刷装置のパススルー・セッションを開始するために、スプール・サブシステム QSPL が活動状態になっている必要があります。

41 ページの『Telnet サーバーで SSL を使用可能にする』

このトピックにより、Telnet サーバーで SSL を使用可能にする方法を理解できます。

104 ページの『システム状況の検査』

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

## 仮想装置の数を設定する

このトピックでは、Telnet サーバーの仮想装置の数の設定と、許可されるサインオンの試行回数を制限することについて説明します。

QAUTOVRT 装置システム値を使用して、Telnet サーバーが仮想装置および制御装置を自動的に構成設定することを可能にすることができます。また、自動的に開始される装置の数と、iSeries サーバーが自動的に構成する装置の最大数を指定できます。iSeries サーバーは、必要に応じて、一度に 1 つずつ、指定した限度まで装置を構成または作成します。

1. iSeries ナビゲーターで、iSeries サーバー → 「構成およびサービス」 → 「システム値」を選択します。
2. 右側区画で、「装置 (Devices)」を右クリックして「プロパティ」を選択します。
3. 「装置システム値 (Devices System Values)」ページで、「パススルー装置および Telnet」を使用可能にし、仮想装置の自動構成のためのオプションを選択します。オプションは次のとおりです。
  - 装置の最大数なし (No maximum number of devices) - 許可する装置数に制限を設けません。
  - 最大装置数 (1 から 32,500) - 自動的に構成される装置の最大数として、1 から 32500 の値を指定します。
  - 登録済み出口プログラムの実行 (Run registered exit program) - 仮想装置を選択したり、自動的に作成したりする必要があるとき、仮想装置選択 (QIBM\_QPA\_DEVSEL) 出口ポイントに登録されているプログラムを呼び出します。

その他のプログラミング情報および例については、テクニカル・スタジオ: Telnet エグジット・プログラムを参照してください。

#### 次の手順:

特定の装置に対する特権ユーザーを制限し、サインオンの試行回数を制限する

##### 関連概念

16 ページの『仮想装置記述』

このトピックでは、仮想装置記述を構成して名前を付けることについて説明します。

##### 関連資料

QAUTOVRT 装置システム値

## 仮想装置の自動構成

設定された最大数までの範囲で、必要なだけ仮想装置を自動的に作成するよう Telnet サーバーを構成できます。

iSeries ナビゲーターでは、QAUTOVRT 装置システム値を使用して、Telnet サーバーが仮想装置および制御装置を自動的に構成できます。また、自動的に開始される装置の数と、iSeries サーバーが自動的に構成する装置の最大数を指定できます。iSeries サーバーは、必要に応じて、一度に 1 つずつ、指定した限度まで装置を構成または作成します。

Telnet を使用して仮想装置を自動的に構成すると、Telnet サーバーは仮想装置を削除しません。また、セッションがクローズしても装置を削除しません。仮想制御装置に接続された装置の数が最大数を超過していても、サーバーは装置を削除しません。装置がすでに仮想制御装置上にある場合、Telnet サーバーはそれを使用できます。仮想装置が名前によって要求された場合、Telnet サーバーは、クライアント要求に一致するように既存の装置の属性を変更します。

サーバーで仮想装置の自動構成を許可したことがない場合、装置システム値の「装置の最大数」値は 0 です。使用中の装置数が「装置の最大数」を超えていると、Telnet 接続を試行しても失敗します。使用中の装置の状況は ACTIVE または SIGNON DISPLAY です。サインオンを試行すると、Telnet クライアント・セッションが終了して接続がクローズされたことを示すメッセージ (TCP2504) が戻されます。加えて、リモート iSeries サーバー内の QTCPIP ジョブからは、仮想装置を自動的に選択できないことを示すメッセージ (CPF8940) が戻されます。

「装置の最大数」を 10 に変更すると、次に Telnet 接続を試行したときに、Telnet サーバーで仮想装置が作成されます。Telnet サーバーがこの仮想装置を作成するのは、制御装置上の仮想装置数 (0) が「装置の

最大数」で指定された数 (10) よりも小さいためです。指定した数を再び 0 に変更しても、ユーザーによる次の Telnet 接続試行は成功します。iSeries サーバーが仮想装置を作成できないために Telnet 接続試行が失敗すると、Telnet サーバー上のシステム操作員メッセージ待ち行列に CPF87D7 メッセージが送られます。

注:

1. 仮想制御装置に接続された装置の数が「装置の最大数」を超えていても、Telnet サーバーは構成された仮想装置や名前付き装置を自動的に削除しません。
2. 装置システム値は、パススルー仮想装置と、QPACTLnn 制御装置に接続された Telnet 全画面仮想装置が自動構成されるかどうかを指定します。このシステム値は、QVIRCDnnnn 制御装置に接続された装置には影響しません。これは、これらの装置がデフォルトのシステム装置ではないためです。通常、QPADEVnnnn 装置は QPACTLnn 制御装置に接続され、NEWYORK001 などの名前付き装置は QVIRCDnnnn 制御装置に接続されます。

iSeries ナビゲーターでこの値を設定する方法については、23 ページの『仮想装置の数を設定する』を参照してください。

#### 関連概念

19 ページの『Telnet アクセスの制御』

このトピックでは、Telnet サーバーが危害を被らないように保護するためのヒントが示されています。

#### 関連資料

QAUTOVRT 装置システム値

## 独自の仮想装置の作成

カスタム名または自動生成された名前を持つ仮想装置を手動で作成することができます。

仮想制御装置と仮想装置を独自に作成することができます。独自の仮想装置を作成し、iSeries サーバーが装置名を自動選択できるようにする場合は、以下のルールに注意してください。

- 仮想制御装置の名前は QPACTL nn になります (nn は 01 以上の 10 進数)。
- 仮想装置の名前は QPADEV xxxx になります (xxxx は 0001 から ZZZZ までの英数字)。仮想装置の装置クラスは \*VRT です。仮想装置の位置は仮想制御装置の下にあります。

独自の装置を作成する場合、Telnet サーバーが使用する仮想装置記述の命名規則に精通している必要があります。独自の装置名を選択する (RFC 2877 クライアントまたは仮想端末 API を使用する) 場合、仮想制御装置の名前は QVIRCDnnnn (nnnn は 01 以上の 10 進数) となります。

#### 関連概念

16 ページの『仮想装置記述』

このトピックでは、仮想装置記述を構成して名前を付けることについて説明します。

## 特定の装置に対する特権ユーザーを制限し、サインオンの試行回数を制限する

サインオン・システム値は、ユーザーがサインオンできる装置の制約または制限、および許可されるシステム・サインオン試行回数の定義に使用されます。

### 特定の装置に対する特権ユーザーを制限する

i5/OS ライセンス・プログラムは、サインオン・システム値を使用して、ユーザーがサインオン可能な装置を制限します。全オブジェクト権限 (\*ALLOBJ) があれば、ユーザーはシステム上の任意のリソースにアク

セスできます。また、サービス特殊権限 (\*SERVICE) があれば、ユーザーはシステム上で特定のサービス機能を実行できます。たとえば、この種の権限を持つユーザーは、プログラムをデバッグして、表示および変更サービス機能を実行することができます。iSeries ナビゲーターを使用してこれらの値を設定するには、以下のステップに従います。

1. **iSeries サーバー** → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を選択します。
2. 右側区画で、「Telnet」を右クリックして「プロパティ」を選択します。
3. 「Telnet のプロパティ - システムのサインオン」ページで、以下のオプションを選択します。
  - **特定の装置に対する特権ユーザーを制限する。** この選択は、すべてのオブジェクト (\*ALLOBJ) およびサービス (\*SERVICE) 特殊権限を持つすべてのユーザーが、特定のワークステーションへの明示権限を必要とすることを示します。
  - **各ユーザーを 1 装置セッションに限定する。** この選択は、1 人のユーザーが 1 つのワークステーションのみでサインオンできることを示します。これにより、ユーザーがグループ・ジョブを使用できなくなったり、またはワークステーションでシステム要求を行うことができなくなったりするわけではありません。これにより、パスワードを共用されたり、装置が不在のままになる可能性が少なくなります。

## サインオン回数の制限

サインオン・システム値は、許可されるシステム・サインオンの回数を定義します。自動構成された仮想装置を使用している場合は、許可される Telnet サインオンの回数は増えます。これらの値を設定するには、以下のステップに従います。

1. iSeries ナビゲーターで、**iSeries サーバー** → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」の順に選択します。
2. 右側区画で、「Telnet」を右クリックして「プロパティ」を選択します。
3. 「Telnet のプロパティ」ページで、「システムのサインオン」タブをクリックします。
4. 「Telnet のプロパティ - システムのサインオン」ページで、許可されるサインオンの試行回数、およびサインオンの最大試行回数に到達した場合にとるアクションを指定することができます。
5. 「リモート」タブをクリックします。
6. 「Telnet のプロパティ - リモート・サインオン」ページで、「リモート・サインオンに Telnet を使用」のオプションを選択します。オプションは次のとおりです。
  - **常にサインオン画面を表示する** - すべてのリモート・サインオン・セッションに通常のサインオン処理が必要になります。
  - **サインオン画面をバイパスする** - システムはユーザーがサインオン・パネルをバイパスすることを許可します。ユーザーがシステムにサインオンすることには変わりはありませんが、サインオン画面は表示されません。

注: 「リモート・サインオンにパススルーを使用」が使用可能である場合、「リモート・サインオンにパススルーを使用」に指定する設定に基づいてオプションが自動的に選択されます。「パススルー」を選択する場合、Telnet は引き続きリモート・サインオンが可能です。

### 次の手順:

セッション・キープアライブ・パラメーターを設定する

#### 関連概念

サインオン・システム値



## セッション・キープアライブ・パラメーターを設定する

TCP キープアライブ・パラメーターを使用すれば、プローブを送信して非活動セッションをテストする前に TCP プロトコルが許可する最大アイドル時間を設定することができます。

セッションのアイドル期間がキープアライブ値を超えると、プロトコルはキープアライブ要求をリモート・クライアントに送信します。このアイドル期間は、iSeries ナビゲーターの Telnet プロパティにある「セッション・キープアライブ・タイムアウト (Session keep alive timeout)」パラメーター、または CHGTELNA コマンド内のパラメーターによって定義されます。セッションが非活動であると判別されると (キープアライブ・プローブに対するリモート・クライアントからの応答がない)、そのセッションは終了し、セッションに関連した仮想装置は仮想装置の空きプールに戻され、iSeries オペレーティング・システムは QDEVRCYACN システム値で設定されたアクションを、仮想装置上で実行されている対話式ジョブに対して実行します。このアクションは、名前付き仮想装置 (のみ) に対して影響を与えます。自動選択された仮想装置 (QPADEVxxxx) の場合、対話式ジョブは必ず終了します。

Telnet サーバーは、キープアライブ設定をデフォルトで 600 秒に定義します。

この設定は、サーバーの始動時に有効になります。セッション・キープアライブ・タイムアウト・パラメーターのほか、iSeries ナビゲーターの『ジョブ・システム値』内にあるタイムアウト・インターバル設定も確認することができます。このタイムアウト・パラメーターを使用すれば、iSeries オペレーティング・システムが QINACTMSGQ システム値で設定されたアクションを対話式ジョブに対して実行する前に、対話式ジョブがアイドル状態となっていることのできる時間を制限することができます。Telnet で接続された対話式ジョブの場合、\*DSCJOB のアクションが実行されるのは名前付き仮想装置の場合だけです。自動選択された仮想装置 (QPADEVxxxx) の場合、\*DSCJOB のアクションにより対話式ジョブが終了します。

iSeries ナビゲーターで Telnet のキープアライブ・パラメーターを設定するには、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 サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」の順に選択します。
2. 右側区画で、「Telnet」を右クリックして「プロパティ」を選択します。
3. 「Telnet プロパティ」ページで、「タイムアウト」タブをクリックします。
4. 「Telnet プロパティ - タイムアウト」ページで、ジョブがタイムアウトに達したときに実行するアクションを指定します。さらに、どれほどの時間が経過したら操作がタイムアウトになるかも指定できます。活動状態にないジョブと切断されたジョブの両方について情報を指定できます。

### 次の手順:

サブシステムに装置を割り当てる

#### 関連概念

19 ページの『Telnet アクセスの制御』

このトピックでは、Telnet サーバーが危害を被らないように保護するためのヒントが示されています。

#### 関連資料

非活動ジョブのシステム値

## サブシステムに装置を割り当てる

ユーザーが iSeries サーバーにサインオンするには、その前に、ワークステーションがサブシステムに対して定義されていなければなりません。たとえば、ワークステーションは Telnet サーバーによって選択、または自動作成された仮想表示装置であるかもしれません。

ワークステーション名またはワークステーション・タイプを、 iSeries サーバーのサブシステム記述で指定する必要があります。サブシステム記述の表示 (DSPSBSD) コマンドを使用して、サブシステムに対して定義されているワークステーション項目を調べます。

次のコマンドを使用して、すべてのワークステーション・タイプを QINTER という名前のサブシステムに追加することができます。

```
ADDWSE SBS(DQINTER) WRKSTNTYPE(*ALL)
```

印刷装置は常に QSPL スプーリング・サブシステムに経路指定されます。

サブシステムが活動状態になっている時に、ワークステーション項目の追加 (ADDWSE) コマンドを実行することができます。ただし、変更が直ちに反映される場合と、そうでない場合があります。サブシステムを終了してから再始動しなければならない場合もあります。

次の手順:

QSYSWRK サブシステムを活動化する

## QSYSWRK サブシステムを活動化する

TCP/IP アプリケーションのサーバー・ジョブは、QSYSWRK サブシステムで開始しなければなりません。印刷装置のパススルー・セッションを開始するために、スプール・サブシステム QSPL が活動状態になっている必要があります。

QSYSWRK サブシステムの状況を検査するには、以下のステップを完了します。

1. iSeries サーバーの文字ベース・インターフェースで、 WRKSBS (活動状態サブシステム処理) と入力します。
2. 以下のシステムが表示されることを確かめます。
  - QSYSWRK
  - QINTER
  - QSPL

QSYSWRK サブシステムが活動状態でない場合には、以下のステップを完了します。

1. iSeries サーバーの文字ベースのインターフェースで、 STRSBS (サブシステム開始) と入力します。
2. サブシステム記述には QSYSWRK、ライブラリーには QSYS と入力して、Enter キーを押します。
3. ライブラリー QSYS のサブシステム名 QINTER、およびライブラリー QSYS のサブシステム名 QSPL についても同様に行います。

対話式ジョブに使用するサブシステムがわからない場合は、iSeries の文字ベースのインターフェースで WRKSBSD \*ALL と入力します。「ワークステーションのタイプ」項目には、サブシステムに割り振られている装置が示されます。

次の手順:

ユーザー・プロファイルを作成する

### 関連タスク

23 ページの『Telnet サーバーの開始』

このトピックでは、Telnet サーバーの開始について説明します。

## ユーザー・プロファイルを作成する

Telnet サーバーでは、iSeries ナビゲーターを使用して Telnet ユーザー・プロファイルを作成できます。

Telnet ユーザー・プロファイルを作成するには、以下のステップを完了します。

1. iSeries ナビゲーターを開始して、**iSeries サーバー**を展開します。
2. 「**ユーザーおよびグループ**」を右クリックして、「**新規ユーザー**」を選択します。
3. ユーザー名、説明、およびパスワードを入力します。
4. ジョブ記述を指定するには、「**ジョブ**」をクリックしてからジョブ記述を入力します。
5. 「**OK**」をクリックします。

次の手順:

エミュレーション・タイプを選択および構成する

## iSeries でサポートされているエミュレーション・タイプ

iSeries で優先されるエミュレーションは 5250 エミュレーションです。ただし、iSeries では 3270 および VTxxx エミュレーションもサポートされています。

Telnet サーバーで使用するよう構成する、エミュレーション・タイプを選択してください。

### 関連概念

2 ページの『Telnet シナリオ : Telnet サーバーの構成』

この構成シナリオでは、管理者が Telnet サーバーをカスタマイズする様子を示します。

## Telnet サーバーを 5250 全画面モードに構成する

5250 全画面モードでは、Telnet クライアント・ユーザーは、iSeries 5250 全画面アプリケーションにサインオンして、これを実行することができます。

Telnet クライアント・セッションを確立するには、その前に以下のステップを完了する必要があります。

1. リモート・システム (Telnet を使用して接続するシステム) 上で、Telnet サーバーを開始します。
2. 仮想制御装置と仮想装置を自動構成するように iSeries サーバーを設定します。QTVTELNET および QTVDEVICE ジョブが QSYSWRK サブシステムで活動状態であることを確かめるには、以下のステップを完了します。
  - a. iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**実行管理機能**」を展開します。
  - b. 「**サブシステム**」を右クリックし、「**開く**」を選択します。
  - c. サブシステムが活動状態であることを確かめます。
3. QAUTOVRT システム値を確認します。これは自動構成された仮想装置を使用して一度にサインオンできる最大ユーザー数と等しいはずですが、QAUTOVRT は 0 から 32500 までの数値、および特殊値 \*NOMAX をサポートします。

## Telnet サーバーを 3270 全画面モードに構成する

Telnet クライアント・ユーザーは、3270 全画面モードを使用して、5250 全画面アプリケーションにサインオンしてこれを実行することができます。

サーバーは、5250 全画面アプリケーションとの間ではなく、3270 全画面アプリケーションをサポートする任意の Telnet クライアント・アプリケーションとの間で、3270 全画面サポートをネゴシエーションします。3270 全画面サポートをネゴシエーションするシステムの例は、IBM S/390<sup>®</sup> ファミリーです。

Telnet 5250 (TN5250) は、2 つのシステム間のデータ・ストリームを EBCDIC として送達します。3270 データ・ストリームは 5250 データ・ストリームに変換されるので、ワークステーション装置は、iSeries サーバーおよびアプリケーション・プログラムに対して、リモート 5251 表示装置として動作します。

Telnet サーバーの一般的な構成を完了した後、3270 全画面モードのサーバー・サポートを使用可能にするには、追加ステップがいくつかあります。全画面モードは、「行」モードと対比される「ブロック」モードです。「行」モードではデータが一行ごとに伝送されますが、「ブロック」または全画面モードでは一度に画面全体が伝送されます。

サポートされる 3270 装置機能については、31 ページの『サポートされる 3270 端末タイプ』を参照してください。

画面サイズ、キーボード・マッピング、カーソル選択キー、エラー・メッセージ、およびヌル文字などの 3270 全画面に関する考慮事項については、60 ページの『3270 Telnet クライアント・セッション』を参照してください。

Telnet サーバーを 3270 全画面モードに構成するには、以下のタスクを完了します。

1. 『QKBDTYPE システム値を検査する』
2. 『デフォルトのキーボード・マッピングを設定する』
3. 31 ページの『キーボード・マップの変更』
4. 31 ページの『メッセージ待ち行列の変更』

## QKBDTYPE システム値を検査する

iSeries Telnet サーバーは、仮想表示装置を自動的に作成するとき、QKBDTYPE システム値を使用して仮想装置のキーボード・タイプを判別します。

QKBDTYPE システム値による仮想装置の初期作成が失敗した場合、Telnet サーバーはキーボード値 USB を使用して装置の作成を試行します。USB を使用しての仮想表示装置の 2 回目の作成が失敗した場合、メッセージ (CPF87D7) がシステム操作員のメッセージ待ち行列に送られます。このメッセージは、システムが仮想装置を自動的に選択できないことを示しています。

## デフォルトのキーボード・マッピングを設定する

Telnet を使用して iSeries サーバーに接続された 3270 表示装置は、iSeries サーバーからは 5251 表示装置として認識されます。3270 表示装置のキーボードには、5251 と同等のキーボード・マップが関連付けられているので、5251 と同等の機能を iSeries サーバー上で実行することが可能です。

Telnet クライアント・システムのユーザーが 3270 全画面モードに最初にサインオンするとき、iSeries サーバーはデフォルトのキーボード・マップをユーザーの 3277、3278、または 3279 キーボードに自動的に割り当てます。これが生じないようにするには、ユーザー定義のキーボード・マップをユーザー・プロファイルのサインオン・プロシージャに含めてください。この結果、必要なマッピングが備えられるので、5250 と同等のキーボードで実行できるものと同じ機能のほとんどを 3270 キーボードによって実行できるようになります。

## キーボード・マップの表示

キーボード・マップの表示 (DSPKBDMAP) コマンドを使用して、現行のキーボード・マッピングを表示することができます。別の方法として、端末が 3270 エミュレーション・モードであるときに、「TCP/IP Telnet の構成」メニューのオプション 6 (3270 キーボード・マップの表示) を使用することもできます。

## キーボード・マップの変更

デフォルトのキーボード・マップに小変更を行いたい場合、キーボード・マップの変更 (CHGKBDMAP) コマンドを使用します。このコマンドは、「TCP/IP Telnet の構成」メニューのオプション 7 (3270 キーボード・マップの変更) によって使用できます。

新規のキーボード・マップを設定したい場合、キーボード・マップの設定 (SETKBDMAP) コマンドを使用します。このコマンドは、「TCP/IP Telnet の構成」メニューのオプション 7 (3270 キーボード・マップの変更) です。指定したキー割り当ては、これらのコマンドを再び使用して新規のキー割り当てを指定するか、またはサインオフするときまで有効です。

**注:** CHGKBDMAP と SETKBDMAP との違いは、次のとおりです。SETKBDMAP を使用すると、システムはデフォルトを適用してから SETKBDMAP に指定した変更を適用します。それに対して、CHGKBDMAP を使用すると、システムはデフォルトおよびこのセッション中に既に行われた変更を適用してから、CHGKBDMAP に指定した変更を適用します。

キーボード・マッピングの詳細については、65 ページの『Telnet サーバーの 3270 キーボード・マッピング』を参照してください。

## メッセージ待ち行列の変更

メッセージ待ち行列は、メッセージのメール・ボックスに似ています。iSeries サーバーにはメッセージを保持するためのメッセージ待ち行列がいくつかあり、それらは問題の発見および報告に役立つ情報を提供します。ワークステーション・メッセージ待ち行列が中断モードであるとき、3270 装置には 5250 表示装置に表示されるものと完全に同じ方法でメッセージが表示されます。中断モードでメッセージを受け取るには、メッセージ待ち行列の変更 (CHGMSGQ) コマンドに \*BREAK を指定しなければなりません。ワークステーションが中断モードではない場合、「メッセージ待ち行列にメッセージが届きました。(A message has arrived on a message queue.)」というメッセージを受け取ります。

このメッセージを検索してワークステーションの使用を続けるには、以下のステップに従います。

1. ヘルプ機能に割り当てられた機能キー、またはエラー・リセット機能に割り当てられた機能キーを押します。
2. メッセージの表示 (DSPMSG) コマンドを入力するか、またはシステム要求機能に割り当てられた機能キーを押してからオプション 4 (メッセージの表示) を選択して、待機中のメッセージを表示します。
3. ワークステーション・メッセージ待ち行列を中断モードに設定して、メッセージが届いたときにすぐに表示されるようにします。

## 表示装置の入力禁止ライトをリセットする

iSeries サーバーを 5250 タイプの端末から使用しているとき、特定の状況で特定のキーを押すと、入力が禁止されるようになります。このことが生じたとき、5250 端末は入力禁止ライトを表示します。

画面の右下の角に表示される 2 つのアスタリスクが、入力禁止ライトを示しています。キーボードが使用禁止になると、iSeries 機能キーにマップされているすべてのキーは無視されます。

キーボードをリセットするには、Enter キーを押すか、または iSeries リセット・キーにマップされているキーを押します。

### サポートされる 3270 端末タイプ:

このトピックでは、Telnet がサポートしている 3270 装置の機能を説明します。



ご使用の Telnet クライアント 3270 がサポートされている 3270 端末タイプとネゴシエーションを行っていることを確かめてください。以下の表では、サポートされる端末タイプを示しています。

表 3. フルスクリーン・ワークステーション・マッピング

装置タイプ	装置の機能
3277	この表示装置は汎用 3270 データ・ストリームをサポートしています。下線、明滅、反転イメージ、またはカラーなどの拡張属性はサポートされていません。
3278	この表示装置は、i5/OS データ記述仕様 (DDS) キーワードによって要求された場合に、明滅、反転イメージ、および下線などの拡張属性をサポートします。 注: 1. Telnet 3270 全画面モード (TN3270) の一部のクライアント・インプリメンテーションでは、拡張属性はサポートされません。 2. 3278-2-E 端末タイプとネゴシエーションを行う DBCS 端末はサポートされています。
3279	この表示装置は、カラー属性と、3278 装置について送信された拡張データ・ストリーム属性をサポートします。カラー属性は、DDS 属性を解釈することによって、(5292 フルカラー表示と同じ仕方)で明滅、高輝度、または DDS カラー・キーワードとして判別されます。

## Telnet サーバーを VTxxx 全画面モードに構成する

VTxxx サーバー・サポートを使用すれば、Telnet クライアント・ユーザーは、VTxxx 全画面サポートがネゴシエーションされていても、iSeries 5250 全画面アプリケーションにログオンして実行することができます。

Telnet クライアント・アプリケーションは、VTxxx 端末サポートをネゴシエーションできなければなりません。VTxxx 全画面モードがネゴシエーションされる時、iSeries Telnet サーバーは 5250 機能を VTxxx キーに (また、逆方向に) マップする処理を担当します。

iSeries Telnet サーバーは VTxxx クライアントをサポートしていますが、VTxxx 端末は文字モード装置なので、これは優先使用すべきモードではありません。iSeries サーバーはブロック・モード・システムです。ほとんどの Telnet インプリメンテーションは、iSeries Telnet サーバーに接続する際に使用すべき TN3270 または TN5250 クライアントをサポートしています。

一般に、VTxxx 端末上のキーが押されると、そのキーに関連した 16 進コードが即座に Telnet サーバーに伝送されます。Telnet は、そのキー・ストロークを処理してから、その文字を VTxxx 端末上の表示位置にエコーバックする必要があります。これにより、キー・ストロークごとに関連した大量のオーバーヘッドが発生します。対照的に、5250 および 3270 ブロック・モード装置は、アテンション識別コード (AID) キーが押されるまで、すべてのキー・ストロークをクライアント・システムでバッファリングします。AID キーが押されると、クライアントはバッファリングされた入力をサーバーで処理するために送ります。結果的に、ブロック・モード装置のほうがキー・ストロークごとのオーバーヘッドは少なくなり、一般に、VTxxx 端末などの文字モード装置よりも優れたパフォーマンスを示します。

VTxxx は、2 つのシステム間のデータを ASCII として送達します。

Telnet サーバーの一般的な構成を完了した後、VTxxx 全画面モードのサーバー・サポートを使用可能にするには、いくつかの追加ステップを完了する必要があります。

全画面モードは、「行」モードと対比される「ブロック」モードです。「行」モードではデータが一行ごとに伝送されますが、「ブロック」または全画面モードでは一度に画面全体が伝送されます。

VTxxx 全画面に関する考慮事項、エミュレーション・オプション、およびキー値については、67 ページの『VTxxx Telnet クライアント・セッション』を参照してください。

サーバーを VTxxx 全画面モードに構成するには、以下のタスクを完了します。

1. 『QKBDTYPE システム値を検査する』
2. 『デフォルトのキーボード・マップを設定する』
3. 34 ページの『デフォルトのネットワーク仮想端末タイプを設定する』
4. 34 ページの『ASCII/EBCDIC マッピング・テーブルを設定する』

## QKBDTYPE システム値を検査する

iSeries Telnet サーバーは、仮想表示装置を自動的に作成するとき、QKBDTYPE システム値を使用して仮想装置のキーボード・タイプを判別します。

QKBDTYPE システム値を使用しての仮想装置の初期作成が失敗した場合、Telnet サーバーはキーボード・タイプ値 USB を使用して装置の作成を再試行します。キーボード・タイプを作成する 2 回目の試行が失敗した場合、システムはメッセージ (CPF87D7) を QTCPIP ジョブ・ログに送ります。このメッセージは、システムが仮想装置を自動的に作成できないことを示しています。システムは、システム操作員のメッセージ待ち行列にもそのメッセージを送ります。

## デフォルトのキーボード・マップを設定する

Telnet セッションが VTxxx 全画面モード内でネゴシエーションするとき、システムはデフォルトのキーボード・マップを使用します。VTxxx のためのデフォルトのキーボード・マップを表示するには、VT キーボード・マップの表示 (DSPVTMAP) コマンドを使用します。VTxxx キーボード・マップを変更するには、VT キーボード・マップの変更 (CHGVTMAP) コマンドまたは VT キーボード・マップの設定 (SETVTMAP) コマンドを使用します。キーボード・マップに関する作業については、73 ページの『VTxxx のエミュレーション・オプション』を参照してください。

5250 機能の特殊な VTxxx キー値については、87 ページの『5250 機能別の VTxxx キー値』表を参照してください。

数字キーパッドの表は、通常の場合に数値、小数点、マイナス符号、およびコンマについて、コードを伝送する補助キーボード上のキーを示しています。

編集キーパッド表は、編集キーパッドのキーのコードを送信するキーワードを示しています。

VTxxx キーボードのキーは 5250 キーボードのキーと同じではないので、VTxxx キーと iSeries 機能との間にキーボード・マッピングが必要となります。iSeries サーバーは、VTxxx セッションが最初に確立されるときにデフォルトのキーボード・マッピングを割り当てます。場合によっては、複数のキーまたはキー・シーケンスが特定の iSeries サーバー機能にマップされることもあります。その場合、必要な iSeries サーバー機能を呼び出すために定義されているどのキーでも使用することができます。

注:

1. 各制御文字は、CTRL キーを押しながら英字キーの 1 つを押すことによって VTxxx キーボードから生成される 1 バイトの値です。シフトされた制御文字もシフト解除された制御文字も、同じ 16 進値を生成します。
2. エスケープ・シーケンスは、Esc キーに続いて必要な文字列を形成する複数の文字を押すことにより生成される、複数バイトのコードです。
3. iSeries サーバーは、エスケープ・シーケンス内のすべての英字について、大文字小文字の区別を無視します。エスケープ・シーケンス内の英字は、大文字によっても小文字によっても入力することができます。
4. iSeries サーバーの F1 から F12 の機能は、Esc キーおよびそれに続く VTxxx キーボードの最上段にあるキーの 1 つにマップされます。Esc キーおよびそれに続く VTxxx キーボードの最上段にあるシフトされたキーの 1 つは、F13 から F24 の機能にマップされます。
5. 一部の Telnet VTxxx クライアント・システムでは、Ctrl-S および Ctrl-Q をフロー制御の目的に使用します。これは一般に、XON/XOFF フロー制御と呼ばれます。XON/XOFF が使用可能となっているクライアント・システムを使用している場合、キーボード・マッピングに \*CTLS および \*CTLQ の値は使用しないでください。

## デフォルトのネットワーク仮想端末タイプを設定する

デフォルトのネットワーク仮想端末装置タイプ・パラメーターは、Telnet サーバーがサポートされている端末タイプの 1 つとネゴシエーションできないときに使用するモードを指定します。

デフォルトのネットワーク仮想端末装置タイプを \*VT100 または VT100/VT220 モードに設定するか、\*NVT に設定して ASCII ライン・モードにするためには、以下のステップに従ってください。

1. iSeries ナビゲーターを開始し、iSeries サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を展開します。
2. 「TELNET」を右クリックして、「プロパティ」を選択します。
3. 「一般」タブをクリックして、「デフォルトのネットワーク仮想端末装置」の隣で適切な値を選択します。
4. 「OK」をクリックします。

## ASCII/EBCDIC マッピング・テーブルを設定する

iSeries Telnet サーバーは、TCP/IP Telnet 属性内の CCSID パラメーターに基づいて、デフォルトの ASCII/EBCDIC および EBCDIC/ASCII マッピング・テーブルを使用します。デフォルトでは、DEC 各国間共通文字セット (\*MULTINAT) が使用されます。その他の 7 ビットおよび 8 ビットの ASCII CCSID、および 7 ビットの DEC 国別置き換え文字セットのいずれかを使用することもできます。

注: VT220 8 ビット・モードでは、マッピング・テーブルは使用できません。このモードでは、システムは DEC 置き換え文字セットを使用します。VT220 7 ビット・モードでは、マッピング・テーブルまたは DEC 置き換え文字セットのどちらかを使用できます。

デフォルトを変更する方法は 3 つあります。CCSID パラメーターを変更すること、VTxxx 発信テーブル (TBLVOUT) と着信テーブル (TBLVTIN) とで別の値を指定すること、または現行セッションのデフォルト・テーブルを変更することができます。

- テーブルの値を変更するには、以下のステップを完了してください。
  1. iSeries ナビゲーターを開始し、iSeries サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を展開します。
  2. 「TELNET」を右クリックして、「プロパティ」を選択します。



3. 「マッピング」タブをクリックします。
  4. 「指定されたマッピング・テーブルを使用」チェック・ボックスを選択して、「テーブル」をクリックします。
  5. 「発信マッピング・テーブルを使用」および「着信マッピング・テーブルを使用」チェック・ボックスを選択して、CCSID パラメーターを変更します。
  6. 「OK」をクリックします。
  7. 「OK」をクリックします。
- 現行セッションのデフォルト・テーブルを変更するには、VT マッピング・テーブルの設定 (SETVTTBL) コマンドを使用します。

このコマンドにアクセスする別の方法は、CHGTCPTELN コマンドのオプション 2 を使用することです。

#### 関連資料

83 ページの『数字キーパッド』

このトピックでは、通常の場合に数字、小数点 (.), マイナス符号 (-), およびコンマ (,) についてコードを伝送する、補助キーパッド上のキーをリストします。

85 ページの『編集キーパッド』

以下の表は、編集キーパッドのキーのコードを送信するキーを示しています。

## SSL で保護された Telnet

Secure Sockets Layer (SSL) プロトコルを使用すると、Telnet サーバー・アプリケーションと Telnet クライアントとの間で、通信セッションの一方または両方のエンドポイントで認証を行う、保護された接続を確立することができます。SSL では、クライアントとサーバー・アプリケーションが交換するデータのプライバシーと保全性も提供します。

#### 関連概念

Secure Sockets Layer (SSL)

#### 関連タスク

103 ページの『Telnet SSL サーバーのトラブルシューティング』

このトピックでは、システム SSL の戻りコードと一般的な SSL の問題を含む、SSL サーバーのトラブルシューティングについての詳細な情報が示されています。

## Telnet サーバー上での SSL の構成

このトピックを使用して、iSeries サーバーに SSL をセットアップします。

SSL でセッションを保護するように i5/OS Telnet サーバーを構成することができます。Telnet サーバーで SSL を使用可能にする際に考慮すべき最も重要な点として、クライアント・セッションに関する情報の機密性があります。情報が機密事項、もしくはプライベートである場合は、SSL を使用して iSeries Telnet サーバーを保護することをお勧めします。

Telnet サーバーに SSL を構成するには、以下のステップに従います。

1. Telnet SSL をサポートしてデジタル証明書を管理するために、以下のソフトウェアをインストールします。
  - TCP/IP Connectivity Utilities for iSeries、5722-TC1
  - デジタル証明書マネージャー、5722-SS1 - Boss Option 34
  - IBM HTTP Server for iSeries、5722-DG1
  - Developer Kit for Java、5722-JV1

2. 確実にポート制限を除去し、SSL を開始できるようにしてください。
3. 証明書を Telnet サーバーに割り当てる。
4. Telnet サーバーのクライアント認証を使用可能にする (オプションのステップ)。
5. Telnet サーバーで SSL を使用可能にする。
6. Telnet サーバーを開始します。

Telnet サーバーに関連した SSL の問題解決の詳細については、Telnet SSL サーバーのトラブルシューティングを参照してください。また、SSL 処理の仕組みが分かっていると、問題の起きた場所を判別するのに役立つことがあります。SSL 処理の詳細については、『SSL 初期化およびハンドシェイク』を参照してください。

#### 関連概念

41 ページの『SSL 初期化およびハンドシェイク』

このトピックでは、Telnet サーバー、クライアント、および SSL の間の相互作用に関する詳細を説明しています。

#### 関連タスク

103 ページの『Telnet SSL サーバーのトラブルシューティング』

このトピックでは、システム SSL の戻りコードと一般的な SSL の問題を含む、SSL サーバーのトラブルシューティングについての詳細な情報が示されています。

104 ページの『システム状況の検査』

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

#### ポート制限の除去:

V5R1 より前のリリースでは、Telnet では Secure Sockets Layer (SSL) サポートが利用不能であったため、ポート制限が使用されていました。現在では、SSL、非 SSL、またはその両方を開始するかどうかを指定できるようになりました。したがって、ポート制限は不要になりました。

以前のリリースでポート制限を定義した場合、SSL パラメーターを使用するためにはそのポート制限を除去する必要があります。ポート制限を除去するには、以下のステップに従ってください。

1. ポート制限をリストするには、以下のステップを完了します。
  - a. iSeries ナビゲーターを開始して、**iSeries サーバー** → 「ネットワーク」を展開します。
  - b. 「TCP/IP 構成」を右クリックしてから、「プロパティ」を選択します。
  - c. 「ポート制限」タブをクリックします。
2. ポート制限を除去するには、引き続き以下のステップを完了します。
  - a. 除去したいポート制限を選択します。
  - b. 「除去」をクリックします。
  - c. 「OK」をクリックします。

デフォルトでは、SSL をポート 992、非 SSL をポート 23 で開始する設定となっています。Telnet サーバーは Telnet のサービス・テーブル項目を使用して非 SSL ポートを取得し、Telnet-SSL を使用して SSL ポートを取得します。

#### 次の手順:

証明書を Telnet サーバーに割り当てる

## 関連タスク

『証明書を Telnet サーバーに割り当てる』

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

### 証明書を Telnet サーバーに割り当てる:

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

SSL を使用するように Telnet サーバーを構成するには、あらかじめシステムに前提条件となるプログラムをインストールし、デジタル証明書をセットアップしておかなければなりません。

1. IBM デジタル証明書マネージャー (DCM) を開始します。

注: DCM の使用中にフォームを完成する方法についてわからない場合は、ページ上部の疑問符 (?) を選択してオンライン・ヘルプにアクセスしてください。

2. ナビゲーション・フレームで「**証明書ストアの選択**」をクリックし、証明書ストアとして **\*OBJECTSIGNING** または **\*SYSTEM** を選択して開いてください。
3. 証明書ストアのパスワードを入力して「**続行**」をクリックします。
4. ナビゲーション・フレームが最新表示されたら、「**証明書の管理 (Manage Certificates)**」を選択してタスクのリストを表示します。
5. タスクのリストから「**証明書の割り当て (Assign certificate)**」を選択して、現在の証明書ストアの証明書リストを表示します。
6. リストから証明書を選択して「**アプリケーションに割り当て (Assign to Applications)**」をクリックし、現在の証明書ストアのアプリケーション定義のリストを表示します。
7. リストから Telnet を選択し「**続行**」をクリックします。ページ上には割り当ての選択を確認するメッセージ、または問題が生じた場合はエラー・メッセージが表示されます。

注: iSeries Access for Windows クライアント鍵データベースには、必要な認証局 (CA) の証明書のコピーがすべて含まれていなければなりません。この場合、CA 証明書は、Telnet サーバー・アプリケーションに割り当てた証明書用の鍵データベース内に存在する必要があります。鍵データベースは、ほぼすべての既知の共通 CA からコピーされた CA 証明書で事前構成されています。ローカル CA が発行した Telnet サーバーに証明書を割り当てることを選択した場合は、ローカル CA 証明書のコピーをクライアント鍵データベースに追加する必要があります。ローカル CA 証明書のコピーを追加する方法については、Telnet シナリオ: SSL での Telnet の安全性 - 構成の詳細の中の『ステップ 5: Telnet クライアントで SSL を使用可能にする』を参照してください。

i5/OS Telnet サーバーは、SSL 構成におけるオプションのコンポーネントとして、クライアント認証をサポートしています。クライアント認証は、サーバーがクライアントの身元を確かめるときに実行されます。これは、サーバー・アプリケーションに渡されたクライアント証明書を認証することによって行われます。

### 次の手順:

『Telnet サーバーのクライアント認証を使用可能にする (オプションのステップ)』または、『Telnet サーバーで SSL を使用可能にする』。

### 関連概念

前提条件のプログラム

11 ページの『構成の詳細』

このトピックでは、SSL で Telnet を保護するためのタスク・ステップについて説明します。

### 関連タスク

36 ページの『ポート制限の除去』

V5R1 より前のリリースでは、Telnet では Secure Sockets Layer (SSL) サポートが利用不能であったため、ポート制限が使用されていました。現在では、SSL、非 SSL、またはその両方を開始するかどうかを指定できるようになりました。したがって、ポート制限は不要になりました。

デジタル証明書のセットアップ

IBM デジタル証明書マネージャー (DCM) の開始

『Telnet サーバーのクライアント認証を使用可能にする』

Telnet サーバーは、Telnet クライアント証明書の認証をサポートしています。したがって、SSL ハンドシェイクの際、サーバーはクライアント用のサーバー証明書を生成するだけでなく、デジタル証明書マネージャー (DCM) の構成に応じて有効なクライアント証明書についてオプションで検査できます。

41 ページの『Telnet サーバーで SSL を使用可能にする』

このトピックにより、Telnet サーバーで SSL を使用可能にする方法を理解できます。

104 ページの『システム状況の検査』

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

### Telnet サーバーのクライアント認証を使用可能にする:

Telnet サーバーは、Telnet クライアント証明書の認証をサポートしています。したがって、SSL ハンドシェイクの際、サーバーはクライアント用のサーバー証明書を生成するだけでなく、デジタル証明書マネージャー (DCM) の構成に応じて有効なクライアント証明書についてオプションで検査できます。

DCM を使用すれば、Telnet セッションで SSL クライアント証明書を必須にするかどうかを構成できます。

このサポートを活動化するため、システム管理者は SSL サポートの処理方法を指示します。iSeries ナビゲーターの「Telnet 汎用プロパティ」パネルを使用すれば、Telnet サーバーの始動時に SSL サポートまたは非 SSL サポート (あるいは両方のサポート) を開始するかどうかを指示できます。デフォルトでは SSL サポートおよび非 SSL サポートが常に開始します。

システム管理者は、システムにおけるすべての Telnet セッションで SSL クライアント認証を必須にするかどうかを指示できます。SSL が活動状態になっていてシステムがクライアント認証を必要とするとき、有効なクライアント証明書が存在することは、クライアントが信頼されていることを意味します。

システムは、SSL 制御が達成された後、ネゴシエーションされた任意の RFC 2877 変数と Telnet ユーザー出口変数を適用します。

IBM DCM におけるアプリケーション指定を更新して、Telnet サーバーがクライアント認証を使用できるようにするには、以下のステップに従います。

1. IBM デジタル DCM を開始します。必要に応じて、証明書を入手または作成したり、あるいは認証システムをセットアップまたは変更したりします。証明書システムのセットアップについては、『デジタル証明書マネージャーの使用』を参照してください。
2. 「証明書ストアの選択 (Select a Certificate Store)」をクリックします。

3. 「\*SYSTEM」を選択します。「続行」をクリックします。
4. \*SYSTEM 証明書ストア用の適切なパスワードを入力します。「続行」をクリックします。
5. 左側のナビゲーション・メニューが再ロードされたら、「アプリケーションの管理 (Manage Applications)」を拡張します。
6. 「アプリケーション定義の更新 (Update application definition)」をクリックします。
7. 次のパネルで、「サーバー」アプリケーションを選択します。「続行」をクリックします。
8. 「i5/OS TCP/IP Telnet サーバー」を選択します。
9. 「アプリケーション定義の更新 (Update Application Definition)」をクリックします。
10. 表示される表で、「はい」を選択して、クライアント認証を要求します。
11. 「適用」をクリックします。
12. DCM は、「アプリケーション定義の更新 (Update Application Definition)」ページを再ロードし、確認メッセージを表示します。Telnet サーバー用のアプリケーション定義の更新が終了したら、「完了 (Done)」をクリックします。

Telnet アプリケーション用の証明書によってクライアント認証を使用可能にするためにクライアントが行う必要のある事柄の例については、『例: PC5250 セッションのクライアント認証を使用可能にする』を参照してください。

#### 次の手順:

Telnet サーバーで SSL を使用可能にする。

#### 関連タスク

37 ページの『証明書を Telnet サーバーに割り当てる』

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

IBM デジタル証明書マネージャー (DCM) の開始

41 ページの『Telnet サーバーで SSL を使用可能にする』

このトピックにより、Telnet サーバーで SSL を使用可能にする方法を理解できます。

#### 例: PC5250 セッションのクライアント認証を使用可能にする:

Telnet サーバー用に SSL を構成し、クライアント認証を使用するように指定すると、その後、ユーザーは接続しようとするたびに、Telnet サーバーに対して、有効で信頼できるクライアント証明書を提供するように要求されるようになります。

クライアントがユーザー証明書を作成して、これを IBM 鍵管理データベースにインポートしないと、クライアント認証は有効になりません。

#### DCM でユーザー証明書を作成する

1. IBM デジタル証明書マネージャー (DCM) を開始します。必要に応じて、証明書を入手または作成したり、あるいは認証システムをセットアップまたは変更したりします。証明書システムのセットアップについては、『デジタル証明書マネージャーの使用』を参照してください。
2. 「証明書の作成 (Create Certificate)」を拡張します。
3. 「ユーザー認証」を選択します。「続行」をクリックします。



4. 「ユーザー認証」フォームに記入します。記入する必要があるのは、「必要」とマーク付けされたフィールドだけです。「**続行**」をクリックします。
  5. ブラウザーから、ブラウザーにロードする証明書を生成するよう要求されます。ブラウザーの指示に従います。
  6. 「ユーザー証明書の作成 (Create User Certificate)」ページが再ロードされたら、「**証明書のインストール (Install Certificate)**」をクリックします。これにより、ブラウザーに証明書がインストールされます。
  7. PC に証明書をエクスポートします。証明書をパスワード保護ファイルに保管しなければなりません。
- 注: エクスポート機能およびインポート機能を使用するには、Microsoft Internet Explorer 5 または Netscape 4.5 が必要です。

### IBM 鍵管理に証明書をインポートする

1. 「スタート」 → 「プログラム」 → 「IBM iSeries Access for Windows」 → 「iSeries Access for Windows Properties」とクリックします。
2. 「セキュア・ソケット」タブを選択します。
3. 「IBM 鍵管理 (IBM Key Management)」をクリックします。
4. 鍵データベースのパスワードを入力するようプロンプトが出されます。事前にデフォルトのパスワードを変更していなければ、ca400 と入力します。確認メッセージが表示されます。「**OK**」をクリックします。
5. プルダウン・メニューから、「**個人用証明書 (Personal certificates)**」を選択します。
6. 「**インポート**」をクリックします。
7. 「**鍵のインポート (Import key)**」画面で、証明書のファイル名およびパスを入力します。「**OK**」をクリックします。
8. 保護ファイルのパスワードを入力します。これは、『DCM でユーザー証明書を作成する』のステップ 7 で作成したのと同じパスワードです。「**OK**」をクリックします。証明書が IBM 鍵管理内の個人用証明書に正常に追加されると、PC5250 エミュレーターまたはその他の Telnet アプリケーションを使用できるようになります。

### iSeries ナビゲーターから PC5250 エミュレーター・セッションを開始する

1. iSeries ナビゲーターを開きます。
2. Telnet 用のクライアント認証をセットアップしたシステムの名前を右クリックします。
3. 「**エミュレーターの表示 (Display emulator)**」を選択します。
4. 「**通信**」メニューから、「**構成**」を選択します。
5. 「**プロパティ**」をクリックします。
6. 「**接続**」ダイアログで、「**Secure Sockets Layer (SSL) を使用する**」を選択します。
7. 複数のクライアント証明書を持っている場合には、「**接続時に証明書を選択 (Select certificate when connecting)**」または「**デフォルトの使用**」のいずれかを選択し、使用するクライアント証明書を決定します。
8. 「**OK**」をクリックします。
9. 「**OK**」をクリックします。

#### 関連タスク

- IBM デジタル証明書マネージャー (DCM) の開始
- DCM の構成



## Telnet サーバーで SSL を使用可能にする:

このトピックにより、Telnet サーバーで SSL を使用可能にする方法を理解できます。

1. iSeries ナビゲーターを開きます。
2. **iSeries** サーバー → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を拡張します。
3. 「Telnet」を右クリックします。
4. 「プロパティ」を選択します。
5. 「一般」タブを選択します。
6. SSL サポートのオプションのうちの 1 つを選択します。

- **保護のみ (Secure only)**

Telnet サーバーとの SSL セッションのみを許可する場合に選択します。

- **非保護のみ (Non-secure only)**

Telnet サーバーとの保護されたセッションを禁止する場合に選択します。SSL ポートへ接続しようとする試みは失敗します。

- **保護と非保護の両方 (Both secure and non-secure)**

選択すると、Telnet サーバーとの保護されたセッションと無保護のセッションの両方を許可します。

## 次の手順:

### Telnet サーバーの開始

#### 関連タスク

37 ページの『証明書を Telnet サーバーに割り当てる』

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

38 ページの『Telnet サーバーのクライアント認証を使用可能にする』

Telnet サーバーは、Telnet クライアント証明書の認証をサポートしています。したがって、SSL ハンドシェイクの際、サーバーはクライアント用のサーバー証明書を生成するだけでなく、デジタル証明書マネージャー (DCM) の構成に応じて有効なクライアント証明書についてオプションで検査できます。

23 ページの『Telnet サーバーの開始』

このトピックでは、Telnet サーバーの開始について説明します。

## SSL 初期化およびハンドシェイク

このトピックでは、Telnet サーバー、クライアント、および SSL の間の相互作用に関する詳細を説明しています。

SSL 処理の仕組みが分かっていると、問題の起きた場所を判別するのに役立つことがあります。

## SSL 初期化中の動作

Telnet サーバーは、サーバーが開始するたびに SSL の初期化を試みます。初期化中に、Telnet サーバーは QIBM\_QTV\_TELNET\_SERVER アプリケーション内の認証情報を検査します。QSYSWRK サブシステム内に活動状態の QTVTELNET ジョブが複数あるなら、SSL 初期化に成功したことがわかります。ただ

し、Telnet プロパティの「一般」ページでフィールドを開始するサーバー・ジョブの数が 1 に設定されている場合、活動状態の QTVTELNET ジョブの数は当然 1 つだけです。

telnet-ssl ポートが制限されている場合、Telnet サーバーは SSL を初期化しません。Telnet サーバーは、TCP2550 メッセージ Access to port 992 is restricted を QTVTELNET ジョブ・ログおよび QSYSOPR メッセージ待ち行列に送信します。

証明書が不適切または有効期限切れであれば、初期化は失敗し、Telnet サーバーはメッセージ CPDBC nn を QTVTELNET ジョブ・ログに送信します。

QIBM\_QTV\_TELNET\_SERVER アプリケーション内に証明書が存在しないか、有効期限が切れた証明書が存在していても、Telnet サーバーは適切に SSL を初期化します。ただし、クライアントが Telnet サーバーへの接続を試みると、SSL ハンドシェイクが失敗します。Telnet サーバーはメッセージ CPDBC nn を QTVTELNET ジョブ・ログに送信します。

## SSL 再初期化中の動作

QIBM\_QTV\_TELNET\_SERVER アプリケーションの証明書が変更されると、DCM の変更が生じた場合に Telnet サーバーは SSL を再初期化します。つまり、有効期限が切れた証明書を復元したり、ユーザー証明書を追加または削除することができ、その場合に Telnet は変更を自動的に検出するということです。このプロセスは SSL 初期化と同じです。新しい Telnet SSL クライアント・セッションは、新しい証明書を使用します。すでに確立されていた Telnet SSL クライアント・セッションは、元の証明書を使用します。Telnet サーバーが終了して再始動すると、すべての Telnet SSL クライアント・セッションは新しい証明書を使用します。

SSL 再初期化が失敗すると、確立済み SSL セッションはサーバー開始時に初期化された元の証明書を使用し、新規のセッションは接続をブロックされます。次回 Telnet サーバーを開始する時、SSL 初期化は失敗しますが、活動状態の SSL listener は引き続き存在しています。しかし、DCM の変更の結果として Telnet サーバーの再初期化が正常に行われるまで、新規の SSL 接続は成功しません。

## SSL ハンドシェイク中の動作

Telnet SSL クライアントが TCP ポート 992 に接続して、サーバーとの間で SSL ネゴシエーションを試行する時、SSL ハンドシェイクが発生します。メッセージがサーバーに接続している間、開いているウィンドウのステータス・バーに状況番号または状況メッセージが表示されます。

SSL ハンドシェイクが失敗すると、Telnet セッションは確立されません。たとえば、Telnet SSL クライアント・ウィンドウにはサインオン画面が現れません。特定の状況番号または状況メッセージについては、Telnet SSL クライアントのユーザー・ガイドまたはオンライン・ヘルプを参照してください。

Telnet サーバーはメッセージ CPDBC nn を QTVTELNET ジョブ・ログに送信します。

### 関連タスク

35 ページの『Telnet サーバー上での SSL の構成』

このトピックを使用して、iSeries サーバーに SSL をセットアップします。

105 ページの『Telnet ジョブ・ログの検査』

SSL 初期化およびハンドシェイクが失敗すると、Telnet サーバーより CPDBC nn 診断メッセージが QTVTELNET ジョブへ送信されます。

---

## Telnet サーバーの管理

このトピックは、Telnet サーバーを処理し、出口プログラムを使用してユーザー・アクセスを制御する方法について説明します。

iSeries Telnet サーバーは、リモート Telnet クライアント・システム上の TCP/IP ユーザーが、iSeries サーバーにサインオンしてアプリケーションを実行することを許可します。iSeries Telnet サーバー・サポートは、リモート Telnet クライアント・アプリケーションとの間で様々な操作モードでのデータの伝送をネゴシエーションします。

Telnet サーバーおよびクライアント・アプリケーションとは、これらの操作モードをネゴシエーションします。ユーザーが使用できる機能は、ネゴシエーションされた端末タイプに依存します。

最小限のシステム値変更で、Telnet サーバーは TCP/IP の開始時に Telnet 接続をサポートすることができます。ASCII ライン・モード以外のすべての操作モードで、iSeries サーバーは Telnet 接続の確立時に iSeries サインオン画面を自動的に送信します。ASCII ライン・モードでは、データを表示する顧客アプリケーションが活動状態でなければなりません。

## Telnet 印刷装置セッションの構成

このトピックでは、ネットワーク上のリモート・ロケーションから iSeries サーバー上の印刷装置に接続するための手順を説明します。

Telnet 印刷装置エミュレーションを作動するには、仮想 iSeries 印刷装置 (3812 または 5553 装置となります) を作成する必要があります。そのような装置は、印刷装置セッションのために送信される、印刷装置データ・ストリームを生成するために必要です。Telnet 印刷で使用される印刷装置は、PC に接続したり、PC と同じネットワークに接続したりすることができます。Telnet 印刷装置セッションは、Telnet 印刷装置エミュレーションをサポートするシステム上のリモート Telnet クライアントとネゴシエーションします。

Telnet 印刷装置セッションは、2 つのシステム間で印刷装置のデータ・ストリームを (要求側クライアントのプリファレンスに応じて) EBCDIC または ASCII のいずれかとして送信します。

Telnet 印刷装置セッションは、Telnet を初期化すると直ちに活動状態になります。印刷機能にはユーザー・プロファイルやパスワードは必要ありません。しかしセキュリティのために必要であれば、Telnet 出口点プログラムを使用して印刷装置セッションが開始しないようにブロックすることもできます。

Telnet 印刷装置セッションの使用時は、すべての出力データが印刷装置書き出しプログラム待ち行列にプールされます。印刷装置に直接印刷することはできません。印刷装置ファイル・コマンドを使用して、印刷装置ファイルの作成 (CRTPRTF)、印刷装置ファイルの変更 (CHGPRTF)、および印刷装置ファイルの上書き (OVRPRTF) を実行する場合、デフォルトの SPOOL (\*YES) パラメーターを使用してください。また、Telnet は、印刷装置書き出しプログラムや出力待ち行列の名前を印刷装置名と同じ名前に設定します。

Telnet 印刷装置セッションをセットアップするには、以下のステップに従います。

1. TCP スタックが活動状態であることを確認します。活動状態ではない場合、STRTCP コマンドを発行して TCP スタックを開始します。
2. Telnet サーバーを開始します。
3. 仮想装置の数を設定します。
4. Telnet セッション・キープアライブ・パラメーターを設定します。

5. 仮想制御装置と仮想装置を作成します。
6. QSPL サブシステムを活動化します。
7. テスト印刷ファイルを使ってセットアップを検査します。
8. Telnet 印刷装置セッションによってファイルを印刷します。

注: QSYSWRK サブシステムは、TCP スタックが開始するときに開始します。

## Telnet 印刷装置セッションの要件

Telnet 印刷装置セッションの使用を検討している場合は、印刷装置セッション機能をサポートしているかどうか、Telnet クライアント製造販売元に確認してください。

印刷装置セッション機能をサポートするクライアントには以下のものがあります。

- IBM iSeries Access for Windows
- パーソナル・コミュニケーションズ
- IBM Host OnDemand

Telnet 印刷装置セッションは、次の汎用 EBCDIC 印刷装置をサポートします。

- IBM-3812-1 (1 バイト文字セット (SBCS) 用)
- IBM-5553-B01 (2 バイト文字セット (DBCS) 用)

iSeries ホスト印刷変換 (HPT) 機能を要求し、特定の製造タイプを選択することによって、いずれの汎用装置タイプを指定することもできます。iSeries Access for Windows をご使用の場合は、Printer Definition Table (PDT) または Graphical Device Interface (GDI) を使用して特定のハードウェアを定義できます。

iSeries サーバーはプリンター・データ・ストリームを ASCII で送ります。

### システム API の機能強化

システム API の装置記述の検索 (QDCRDEVD) は、Telnet クライアントの IP アドレスを提供します。表示装置 (\*DSP) および印刷装置 (\*PRT) 用に、ネットワーク・プロトコル、ネットワーク・プロトコル・アドレス、IP インターネット・アドレス (小数点付き 10 進数形式) などのいくつかのフィールドがあります。これらのフィールドは、クライアントの TCP/IP 接続に関するソケット・レベルの情報をアプリケーションに提供します。

### iSeries Access for Windows Telnet クライアントの Telnet サーバー印刷サポート:

IBM iSeries Access for Windows クライアントは、5250 全画面 Telnet クライアントのディスプレイ・エミュレーションと印刷装置エミュレーションの両方を提供します。

以下のうちのいずれかを選択して印刷装置セッションを開始します。

1. プログラム・スタート・メニューから、**iSeries Access for Windows** → 「**エミュレーター (Emulators)**」 → 「**セッションの開始または構成 (Start or Configure Session)**」
2. 接続先の iSeries サーバーの名前を選択します。
3. iSeries 仮想装置名を明示的に要求するには、ワークステーション ID フィールドを使用します。あるいは、フィールドをブランクのままにしておくと、Telnet サーバーは互換性のある仮想装置 (QPADDEVxxxx) を自動選択して、印刷装置の制御パネルにその名前を戻します。
4. エミュレーションのタイプを指定するには、以下のようにします。
  - a. 印刷装置を選択します。
  - b. セットアップ・ボックスをクリックして、「PC5250 プリンター・エミュレーションのセットアップ」画面を開始します。

フロント、iSeries メッセージ待ち行列、および HPT ホスト機能などをセットアップ画面から構成できます。HPT ホスト機能には、「iSeries 上での印刷データの ASCII 形式への変換」が含まれます。HPT を選択すると、印刷装置モデル、媒体トレイの選択オプションなど、他の構成項目も使用可能になります。また、自動再接続オプション、およびデフォルトの iSeries Telnet ポート番号 (23) を変更するオプションもあります。

セッションを終了するには、メニューバーから「通信」 → 「切断」をクリックします。

## サーバー・セッションの終了

このトピックの説明に従って、Telnet セッションを終了します。Telnet セッションを終了すると、仮想装置が解放され、新しい Telnet セッションでこの装置を使えるようになります。

iSeries サーバーに接続している場合、サインオフしても、Telnet サーバー・セッションが終了するとは限りません。仮想表示装置または印刷装置はまだ活動状態であり、別の Telnet セッションが使用することはできません。セッションを終了するには、Telnet クライアントをローカル・コマンド・モードにするための一連のキーを入力する必要があります。そうすれば、コマンドを入力してセッションを終了することができます。以下のキー・シーケンスを使用して、Telnet サーバー・セッションを終了します。

- iSeries サーバーから、**アテンション・キー**を押してから、オプション 99 (TELNET セッションの終了 - QUIT) を選択します。
- その他のほとんどのシステムからの場合は、ログオフします。

クライアントをコマンド・モードにするためのキーがわからない場合は、システム管理者に相談するか、または Telnet クライアントの資料を調べてください。

また、SIGNOFF コマンドの接続の終了 (ENDCNN) パラメーターを使用しても、システムをサインオフし、Telnet 接続を終了できます。たとえば、SIGNOFF ENDCNN(\*YES) を使用すると、クライアント・システムに戻ります (1 つの Telnet セッションしか確立されていない場合)。または直前のシステムに戻ります (複数の Telnet セッションが確立されている場合)。

### 関連タスク

23 ページの『Telnet サーバーの開始』

このトピックでは、Telnet サーバーの開始について説明します。

## Device Manager ジョブの終了

Device Manager ジョブを終了してから再始動する必要の生じることがあります (たとえば、プログラムに PTF を適用するとき)。このトピックでは、Device Manager ジョブを終了および再始動する手順を説明します。

Telnet を開始して停止すると Telnet サーバー・ジョブは終了しますが、Device Manager ジョブは終了しません。これは、常に (または、少なくとも次にシステムが再始動するまで) 実行されていない限りという Device Manager ジョブの性質によります。Device Manager ジョブをサイクルさせるには、特殊ステップ 2 (46 ページ) および 3 (46 ページ) を実行する必要があります。この後、Telnet を次に開始すると、Telnet は Device Manager ジョブが存在しないことに気づき、いくつかのジョブを実行しなければならないことを認識して、ジョブを開始します。Device Manager ジョブを終了するには、以下のステップを完了します。

1. 以下のステップを完了して、活動状態の Telnet サーバー・ジョブを終了します。
  - a. iSeries ナビゲーターを開始し、**iSeries サーバー** → 「ネットワーク」 → 「サーバー」 → 「TCP/IP」を展開します。



- b. 「Telnet」を右クリックして、「停止」を選択します。
2. 以下のステップを完了して、活動状態の Telnet Device Manager ジョブをすべて検索します。
  - a. iSeries ナビゲーターを開始し、iSeries サーバー → 「実行管理機能」を展開します。
  - b. 「活動ジョブ」を選択します。
  - c. QTVDEVICE を探します。
3. ステップ 2 で見付かったすべてのジョブを、右クリックして「削除 / 終了」を選択することによって終了します。すべてのジョブが終了するのを待ってから、次のステップを実行してください。
4. 「削除 / 終了」パネルで Telnet サーバーおよび Device Manager ジョブを開始します。

すべての Device Manager ジョブが終了した時点で終了途中だった Telnet 仮想装置は、次に再始動するまでアクセス不能になる可能性があります。

## Telnet 出口プログラムの使用

このトピックでは、Telnet サーバーで出口プログラムを使用するための情報について説明します。

出口プログラムを使用すれば、経験のあるプログラマーはアプリケーション内で実行されるカスタマイズされた処理を作成することができます。Telnet サーバーは、自身の出口点のいずれかに登録されたプログラムを検出すると、出口点で定義されたパラメーターを使用してそのプログラムを呼び出します。

出口点 は、制御を出口プログラムに渡すことが可能な、Telnet プログラム内の特定の点です。出口プログラム は、出口点が制御を渡すプログラムです。

出口点ごとに、出口点インターフェースと呼ばれる関連したプログラミング・インターフェースがあります。出口点はこのインターフェースを使用して、Telnet アプリケーションと出口プログラムとの間で情報を渡します。それぞれの出口点には固有の名前があります。それぞれの出口点インターフェースには、Telnet アプリケーションとカスタマー作成の出口プログラムとの間で情報を渡す方法を定義している、出口点形式名があります。

複数の異なる出口点が、同一の出口点インターフェースを共用することができます。その場合、複数の出口点が 1 つの出口プログラムを呼び出すことができます。

## 出口点のパフォーマンス

初期セッション要求に対する Telnet サーバーの応答時間には、サーバーが QIBM\_QTG\_DEVINIT 出口プログラムを呼び出し、処理し、戻すための時間が含まれます。ご使用の出口プログラムが大量の処理を行う場合、パフォーマンス上の影響が生じて、セッションが確立されるまで待つ時間が長くなることがあります。ユーザー出口プログラムのデフォルトの 60 秒のタイムアウト値を変更する場合には、ADDEXITPGM コマンドを使用して、タイムアウト値として読み取られるユーザー・データを追加することができます。以下の例では、PGMDTA パラメーターは、デフォルトの 60 秒のタイムアウト値を 10 秒にオーバーライドします。

```
ADDEXITPGM EXITPNT(QIBM_QTG_DEVINIT) FORMAT(INIT0100)
PGMNR(1) PGM(USEREXIT/DEVINIT2) REPLACE(*YES)
CRTEXTIPNT(*NO) PGMDTA(*JOB *CALC 10)
```

Telnet プログラムがサインオン画面または他の iSeries サーバー画面によって確立された後は、パフォーマンス上の影響はありません。その場合、出口プログラムは Telnet のパスに含まれなくなります。確立された Telnet セッションでは、QIBM\_QTG\_DEVINIT 出口プログラムによる遅延は生じません。



セッションの切断に関しては、ユーザーが感知できるようなパフォーマンス上の影響は生じません。切断するとは、端末エミュレーション・セッションを終了することであり、サインオフしてサインオン画面に戻ることはありません。切断した場合、QIBM\_QTG\_DEVTERM 出口プログラムが呼び出されて、セッションの切断処理が実行されます。これは接続が中断された後に行われるので、ユーザーが感知することはありません。

## 実行管理

Telnet 出口プログラムを使用することにより、主要な実行管理問題を解決することができます。それらの問題には、QPADEVxxxx 以外の装置記述を要求する能力、対話式仮想ワークステーション・ジョブの実行管理制御を可能にすること、およびそれらのジョブを特定のサブシステムにルーティングすることなどが含まれます。

## サブシステムのルーティングおよび装置名の選択

1 つのサブシステム (たとえば QBASE、QCMN、または QINTER など) は、300 を超えるユーザーにサービスを提供しないようにすることを、現在はお勧めします。

ユーザーは改良された Telnet 仮想装置名を利用して、対話式サブシステムが必要に応じて作業を細分できるよう構成できます。これは、ワークステーション項目の追加 (ADDWSE) コマンドを使用して行います。このコマンドによって、サブシステムによって仮想端末装置の特定名を割り振られる装置と割り振られない装置とを指定できます。

以下のコマンドによって、QINTER はすべての QPADEV\* ワークステーションを割り振ります。つまり、これらの装置はすべて QINTER サブシステムにルーティングされることになります。

```
ADDWSE SBS(DQINTER) WRKSTN(QPADEV*) AT(*SIGNON)
```

以下のコマンドによって、QINTER はすべての QPADEV\* ワークステーションを割り振りません。つまり、これらの装置は別のサブシステムに割り振ることが可能となります。

```
ADDWSE SBS(DQINTER) WRKSTN(QPADEV*) AT(*ENTER)
```

ユーザーは、作業を細分するために、独自の装置命名規則を考案することができます。たとえば、細分化の一例として、特定の装置を 2 つのロケーションにある各国語サポート (NLS) 関連のサブシステムにルーティングすることができます。

## 例

この例では、2 人のユーザーが Chicago および New York にいると想定します。それらのユーザーは、地理的な位置に応じて、iSeries のサブシステム CHICAGO または NEWYORK に割り当てられています。この例に含まれる特徴は、次のとおりです。

- Chicago の IP アドレスは、1.2.3.\* から開始します。
- New York の IP アドレスは、2.3.4.\* から開始します。
- すべての Chicago Telnet セッションが CHICAGO サブシステムで実行されるように、ユーザー出口プログラムが使用されます。出口プログラムは、1.2.3 からの Telnet 接続すべてに、'CHICAGO' で始まる仮想装置名を作成します。さらに、ユーザー出口プログラムは、2.3.4 からのすべての接続に 'NEWYORK' で始まる仮想装置名を作成します。
- ユーザー出口プログラムは、仮想装置名 'CHICAGO01' を IP アドレス 1.2.3.47 に割り当てます。プログラムは、仮想装置名 'NEWYORK01' を 2.3.4.48 からの IP アドレスに割り当てます。プログラムはルート名 'CHICAGO' に変数部分 ('01'、'02'など) を付加して、現行ユーザーに割り当てる前に、その装置が既に使用されていないかどうかを確認します。

仮想装置 CHICAGO01 がサブシステム Chicago に、および NEWYORK01 がサブシステム New York に結び付けられるように、ワークステーション項目を以下のようにセットアップします。

```
ADDWSE SBS(DQINTER) WRKSTN(CHICAGO*) AT(*ENTER)
ADDWSE SBS(DQINTER) WRKSTN(NEWYORK*) AT(*ENTER)
ADDWSE SBS(DCHICAGO) WRKSTN(CHICAGO*) AT(*SIGNON)
ADDWSE SBS(DNEWYORK) WRKSTN(NEWYORK*) AT(*SIGNON)
```

IBM は、お客様に、すべてのプログラム・コードのサンプルを使用することができる非独占的な著作使用権を許諾します。お客様は、このサンプル・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。

- | 強行法規に反する場合を除き、IBM、「プログラム」開発者および IBM ビジネス・パートナーは「プログラム」を特定物として現存するままの状態を提供し、「プログラム」または技術サポート（提供される場合）について、法律上の瑕疵担保責任を含め、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証を含む明示もしくは黙示のいかなる保証責任も負わないものとします。
- | いかなる場合においても、IBM、「プログラム」開発者および IBM ビジネス・パートナーは、その予見の有無を問わず発生した以下の損害については賠償責任を負いません。
  - | 1. データの喪失、または損傷。
  - | 2. 直接損害、特別損害、付随的損害、間接損害、または経済上の結果的損害
  - | 3. 逸失した利益、ビジネス上の収益、あるいは節約すべかりし費用
- | 国または地域によっては、法律の強行規定により、上記の責任の制限が適用されない場合があります。

#### 関連概念

19 ページの『Telnet アクセスの制御』

このトピックでは、Telnet サーバーが危害を被らないように保護するためのヒントが示されています。

## 装置初期設定出口プログラム

このプログラムによって、カスタム出口プログラムを、iSeries Telnet サーバー上の出口点に関連付けることができます。

Telnet サーバー・アプリケーションには、Telnet のサインオンおよび終了論理へのフックを可能にする出口点が組み込まれています。iSeries WRKREGINF（登録情報の処理）または ADDEXITPGM（出口プログラムの追加）コマンドを使用して、カスタム出口プログラムを出口点に関連付けることができます。Telnet サーバーは、自身の出口点のいずれかに登録されたプログラムを検出すると、出口点で定義されたパラメーターを使用してそのプログラムを呼び出します。これらのパラメーターには、IP アドレス、ユーザー名、および仮想装置名などが含まれます。次いで、カスタム出口プログラムが情報を処理します（たとえば、メッセージをログに記録して制御を Telnet サーバーに戻します）。戻り時に、出口プログラムはこのクライアントとオプションのユーザーまたはパスワードのオーバーライドを受け入れるべきか拒否すべきかをサーバーに伝えます。

各出口点には名前と出口点インターフェースがあります。出口点インターフェースは、Telnet サーバーが出口プログラムと交換する入出力パラメーターのリストです。Telnet サーバーには 2 つの出口点があります。

- QIBM\_QTG\_DEVINIT
- QIBM\_QTG\_DEVTERM

表 4. 必須パラメーター・グループ

番号	出口点のインターフェース	入力または出力	パラメーター
1	ユーザー記述情報	入出力	Char(*)
2	装置記述情報	入出力	Char(*)
3	接続記述情報	入力	Char(*)
4	環境オプション	入力	Char(*)
5	環境オプションの長さ	入力	Binary(4)
6	接続の許可	出力	Char(1)
7	自動サインオンを許可	出力	Char(1)

QSYSINC メンバー名: ETGDEVEX

出口点名: QIBM\_QTG\_DEVINIT

出口点形式の名前: INIT0100

Telnet サーバーでは、オプションで Telnet セッションで使用する装置名の選択や設定を行えます。また、Telnet クライアントが従来の装置初期設定をバイパスすることもできます。管理者は、新規の出口プログラムを使用して、これらの新規機能を制御できます。このプログラムは、クライアント・セッションが確立された直後にオプションで開始されます。この出口プログラムには、意思決定プロセスで使用するいくつかのパラメーターが提供されます。また、このプログラムによって、Telnet サーバーに戻る前にさまざまなパラメーターの設定や変更を行えます。オプションで、セッション終了の直前に開始される 2 番目の出口プログラムを登録することもできます。この 2 番目の出口プログラムは、セッション監査や仮想装置管理に使用できます。

#### Telnet 出口点の形式 INIT0100: 必須パラメーター・グループ:

このトピックでは、必須パラメーター・グループの詳細な定義について説明します。

##### ユーザー記述情報

入出力; CHAR(\*). 自動サインオン・プロセスの一部としてシステムが使用するユーザーに関する情報。

##### 装置記述情報

入出力; CHAR(\*). この Telnet セッションで使う装置の作成や変更システムが使用する情報。

##### 接続記述情報

入出力; CHAR(\*). 出口プログラムが使用できるクライアント接続に関する情報。

##### 環境オプション

入力; CHAR(\*). クライアントによってネゴシエーションされた RFC 2877 環境オプションをすべて含む配列。この形式は、クライアントから受信して RFC 2877 によって指定されたときのものとまったく同じです。配列は通常、環境変数名とその関連値の 1 つ以上の対から成ります。RFC の仕様では、常に各変数名の前に X'01' または X'03 のいずれかが指定されます。どちらが指定されるかは、RFC 2877 が定義した VAR であるか、またはアプリケーションが固有に定義した USERVAR であるかに依存します。値が VAR (または USERVAR) と関連する場合、その値は配列内で、RFC 1572 で定義された VALUE 文字 X'01' の次に現れます。この一連の VAR/VALUE の対は、ネゴシエーション・データの最大合計バイトの 1024 バイトまで繰り返されます。

RFC 2877 や、もっと一般的な Telnet ネゴシエーション RFC においても、VAR/USERVAR の変数名またはその関連値に制御文字を使用できます。これは、ESC 文字 X'02' と、ESC 文字自体

または Telnet IAC 制御文字がネゴシエーション・シーケンスに表示されるときに適用される規則を使用することによって、可能になります。制御文字のエスケープ規則については、RFC 1572 を参照してください。

環境オプション・バッファは、パスワードを含め、クライアントによるネゴシエーションを示しますが、Telnet は常に、機密漏れを避けるために、バッファ内のクリア・テキストまたは暗号化されたパスワードをオーバーレイします。

### 環境オプションの長さ

前の段落で参照されている環境オプションの長さ。通常は 1024 バイト。オプションのネゴシエーションは長さが未定義なので、環境オプション・バッファ内に収まるように、指定された長さを超えるネゴシエーションは切り捨てられます。

### 接続の許可

出力; CHAR(1)。すべての装置に適用され、クライアントの接続を許可するかどうかを Telnet サーバーに指示します。装置タイプが DISPLAY で、自動サインオンを使用可能にした場合、このクライアントは iSeries サーバーのサインオン・パネルをバイパスすることもできます。有効な値は以下のとおりです。

- 0 - クライアントからの要求を拒否する
- 1 - クライアントからの要求を受け入れる

### 自動サインオンの許可

出力; CHAR(1)。DISPLAY 装置タイプに適用され、この特定のクライアントの自動サインオン操作を許可するかどうかを Telnet サーバーに指示します。自動サインオンが許可された場合、このクライアントは iSeries サーバーのサインオン・パネルをバイパスできます。有効な値は以下のとおりです。

- 0 - クライアントからのアプリケーション要求を拒否する。システムは「ユーザー・プロファイル」、「現行<sup>®</sup>ライブラリー」、「呼び出すプログラム」、「初期メニュー」、および「装置名」出力パラメーターを無視します。
- 1 - クライアントのアプリケーション要求を受け入れる。出口プログラムが「ユーザー・プロファイル」、「現行ライブラリー」、「呼び出すプログラム」、「初期メニュー」、および「装置名」出力パラメーターを戻した場合に、システムはそれらが有効であると見なすことができます。

### INIT0100: ユーザー記述情報の形式:

自動サインオン・プロセスでは、ユーザーに関する情報が使用されます。

以下の表は、ユーザー記述情報の形式を示しています。

表 5. ユーザー記述情報の形式

10 進オフセット	16 進オフセット	タイプ	フィールド
0	0	INT(4)	ユーザー記述情報の長さ
4	4	CHAR(10)	ユーザー・プロファイル
14	E	CHAR(10)	現行ライブラリー
24	18	CHAR(10)	呼び出すプログラム
34	22	CHAR(10)	初期メニュー

## ユーザー記述情報フィールドの説明

### 現行ライブラリー

自動サインオン・フラグを使用可能にしたときに現行ライブラリーになるライブラリーの名前。このパラメーターはオプションですが、指定する場合は、左寄せした後、空白で埋めてください。有効な値は以下のとおりです。

#### ライブラリー名

システムが現行ライブラリーとして指定するライブラリーの名前

### 初期メニュー

自動サインオン・フラグを使用可能にしたときに表示される初期メニューの名前。有効な値は以下のとおりです。

#### メニュー名

表示されるメニューの名前

### ユーザー記述情報の長さ

ユーザー記述情報構造体の長さ

### 呼び出すプログラム

自動サインオン・フラグを使用可能にしたときにシステムが呼び出すプログラムの名前。このパラメーターはオプションですが、指定する場合は、左寄せした後、空白で埋めてください。有効な値は以下のとおりです。

#### プログラム名

システムが開始するプログラムの名前

### ユーザー・プロファイル

自動サインオン・フラグを使用可能にしたときにシステムがサインオン・プロシージャで使用するユーザー・プロファイル。このパラメーターはシステムに必須であり、左寄せした後、空白で埋める必要があります。

## INIT0100: 装置記述情報の形式:

このトピックでは、Telnet セッションで使用される装置の作成または変更方法について説明します。

以下の表は、このセッションに関連する装置の特性を記述する、装置記述情報の形式を示しています。

表 6. 装置記述情報の形式

10 進オフセット	16 進オフセット	タイプ	フィールド
0	0	CHAR(10)	装置名
10	A	CHAR(8)	装置の形式
18	12	CHAR(2)	予約済み
20	14	BINARY(4)	装置属性構造体へのオフセット
24	18	BINARY(4)	装置属性構造体の長さ
28	1C	CHAR(*)	装置属性構造体

## 装置記述情報フィールドの説明

**装置名** この Telnet セッションに関連付けられる特定の仮想装置。DISPLAY 装置の場合、装置の自動作成に関するシステム値 QAUTOVRT で指定されていれば、まだ存在していない装置はシステムによって自動作成され、オンに変更されます。PRINT 装置の場合、まだ存在していない装置はシス



テムによって自動作成されます。出口プログラムから値が提供されなければ、Telnet サーバーはデフォルトで従来の Telnet 仮想装置選択メソッドを使用します。この値は、有効な DISPLAY または PRINT 装置の記述名で、標準の i5/OS オブジェクト命名規則に従っていなければなりません。

### 装置の形式

この Telnet セッションに関連付けられる特定の仮想装置タイプ。現時点では、システムがサポートする表示装置だけです。

#### DSPD0100

表示装置を示します。システムは表示属性を戻します。

### 予約済み

将来の使用のために予約済み。

### 装置属性構造体へのオフセット

装置記述情報の最初から装置属性構造体の最初までのオフセット。

### 装置属性構造体の長さ

装置属性構造体に入っているユーザー・スペースの長さ。

### INIT0100: 表示装置記述情報の形式 (DSPD0100)

以下の表は、このセッションに関連する装置の特性を記述する、表示装置記述情報の形式を示しています。

表 7. 表示装置記述情報の形式 (DSPD0100)

10 進オフセット	16 進オフセット	タイプ	フィールド
0	0	CHAR(3)	キーボード ID
3	3	CHAR(1)	予約済み
4	4	BINARY(4)	コード・ページ
8	8	BINARY(4)	文字セット

## DSPD0100 フィールドの説明

### 文字セット

システムがこの対話式ジョブに使用する文字セットを指定します。有効な値は、各国語サポートで見付けることができます。同一のこのフィールドは、オープン仮想端末パス QTVOPNVT API の「Character set」パラメーターと同じです。

### コード・ページ

システムがこの対話式ジョブに使用するコード・ページを指定します。有効な値は、各国語サポートで見付けることができます。このフィールドは、オープン仮想端末パス QTVOPNVT API の「Code page」パラメーターと同じです。

### キーボード ID

システムがこの対話式ジョブに使用する 3 文字のキーボード ID を指定します。「Code page」および「Character set」パラメーターの一部としてオーバーライドされない限り、キーボード ID は、使用するコード・ページと文字セットを暗黙的に指定します。有効な ID は、各国語サポートで見付けることができます。このフィールドは、オープン仮想端末パス QTVOPNVT API の「keyboard Language type」パラメーターと同じです。

### 予約済み

将来の使用のために予約済み

### 関連資料



### INIT0100: 接続記述情報の形式:

このトピックでは、出口プログラムが使用できるクライアント接続についての情報を説明します。

以下の表は、このセッションでのクライアントおよび接続情報を記述する、接続記述情報の形式を示しています。

表 8. 接続記述情報の形式

10 進オフセット	16 進オフセット	タイプ	フィールド
0	0	INT(4)	接続記述情報の長さ
4	4	CHAR(20)	クライアント・インターネット・アドレス
24	18	CHAR(1)	妥当性検査されたクライアント・パスワード
25	19	CHAR(12)	ワークステーション・タイプ
39	27	CHAR(1)	Secure Socket Layer 接続
40	28	CHAR(20)	サーバー (ローカル) インターネット・アドレス
60	3C	CHAR(1)	クライアント認証レベル
61	3D	CHAR(3)	予約済み
64	40	INT(4)	クライアント証明書の有効な戻りコード
68	44	INT(4)	クライアント証明書へのオフセット
72	48	INT(4)	クライアント証明書の長さ

### 接続記述情報フィールドの説明

#### 接続記述情報の長さ

接続記述構造体の長さ

#### クライアント・インターネット・アドレス

これは、要求元クライアントの IP アドレス (またはタイプ構造体) であり、常に出口プログラムに提供されます。これらの新規フィールドのレイアウトは以下のとおりです。

表 9. クライアント IP アドレスのレイアウト

名前	サイズ	説明
sin_len	CHAR(1)	sockaddr_in 構造体のサイズ。
sin_family	CHAR(1)	ファミリーまたはプロトコル。 IP (バージョン 4) は hex 02 です。
sin_port	CHAR(2)	16 ビット符号なしポート番号。
sin_addr	CHAR(16)	4 バイト符号なしネットワーク・アドレス。

#### 妥当性検査されたクライアント・パスワード

Telnet がクライアントの暗号化されたパスワード (受信した場合) を妥当性検査したかどうかを指

定します。システムがこの値を設定するのは、TN5250E Clients が暗号化されたパスワードを妥当性検査用を送る場合です。パスワードは、サービス機能呼び出しを使用してチェックされます。これにより、出口プログラムは保護されたクライアント・サインオン処理を保証することができます。

- 値 = 0、クライアント・パスワード / パスフレーズ (または Kerberos チケット) が妥当性検査されなかった、あるいは何も受信しなかった。
- 値 = 1、クライアントのクリア・テキスト・パスワード / パスフレーズが妥当性検査された。
- 値 = 2、クライアント暗号化パスワード / パスフレーズ (または Kerberos チケット) が妥当性検査された。

#### ワークステーション・タイプ

クライアントが要求したワークステーション・タイプ。ワークステーションと印刷装置マッピングの表でリストされているインターネット仕様のいずれかです。

#### Secure Sockets Layer

接続が Secure Sockets Layer (SSL) 接続であるかどうかを示します。

- 0 - 接続は SSL を使用していません。
- 1 - 接続は SSL を使用しています。

#### サーバー・インターネット・アドレス

これは、ホスト (ローカル) ネットワーク・インターフェースの IP アドレス (またはタイプ構造体) であり、常に出口点プログラムに提供されます。これらの新規フィールドのレイアウトは以下のとおりです。

表 10. クライアント IP アドレスのレイアウト

名前	サイズ	説明
sin_len	CHAR(1)	sockaddr_in 構造体のサイズ
sin_family	CHAR(1)	プロトコル・ファミリー IP は hex 02 で、IPX は hex 06
sin_port	CHAR(2)	16 ビット符号なしポート番号
sin_addr	CHAR(16)	4 バイト符号なしネットワーク・アドレス

#### クライアント認証レベル

サーバーに接続するためにクライアント SSL 証明書が必要かどうかを示します。

- 0 - クライアント証明書は不要。
- 1 - 有効なクライアント証明書が必要。

#### クライアント証明書の有効な戻りコード

SSL ハンドシェイク操作におけるクライアント証明書の妥当性検査時に受信された戻りコードを示します。

#### クライアント証明書へのオフセット

Connection 構造体の最初からクライアント証明書の最初のバイトまでのオフセットを示します。

#### クライアント証明書の長さ

受信されたクライアント証明書の長さを示します。証明書が受信されなかった場合、この長さは 0 です。

#### 関連概念

100 ページの『エミュレーション・タイプのトラブルシューティング』  
このトピックでは、個々のエミュレーション・タイプ内の問題を判別するための、より具体的な情報が示されています。

## 装置終了出口プログラム

この装置終了出口プログラムにより、セッション終了情報をログに記録できます。

QIBM\_QTG\_DEVTERM 出口点は、Telnet クライアントが Telnet セッションを終了したときに発生します。これにより、顧客は、セッション終了情報をログに記録したり、装置のリセットまたは終結処置操作を実行したりできます。

以下の表に、QIBM\_QTG\_DEVTERM 出口点のパラメーターを示します。

QIBM_QTG_DEVTERM 出口点のパラメーターです。			
1	装置名	入力	Char(10)

QSYSINC メンバー名: NONE  
出口点名: QIBM\_QTG\_DEVTERM  
出口点形式の名前: TERM0100

Telnet サーバーでは、オプションで、終了した Telnet セッションに関連付けられた装置に関して、装置の停止、セッション監査アクティビティー、および仮想装置の管理を行えます。

## 必須パラメーター・グループ

装置名 入力; CHAR(10)。この Telnet セッションに関連付けられる特定の仮想装置。

## サンプル Telnet 出口プログラム

出口プログラムの作成を支援するサンプル Telnet 出口プログラムをダウンロードすることができます。

サーバーで Telnet 出口点を使用する際に役立つサンプル・プログラムが用意されています。

サンプル・ダウンロード・ファイルには、以下のリソースが含まれています。

### • Telnet 出口プログラム作成用 CL ユーティリティー・コード (TELCRT) のサンプル

このコードのサンプルを使用して、Telnet 出口プログラムを作成、インストール、または登録します。  
このコードは、i5/OS Command Language (CL) プログラム言語で作成されています。

### • Telnet 出口プログラム削除用 CL ユーティリティー・コード (TELDLT) のサンプル

このコードのサンプルを使用して、i5/OS システムから Telnet 出口プログラムをアンインストールおよび削除します。このコードは i5/OS CL プログラム言語で作成されています。

### • 初級 Telnet 初期設定出口プログラム (DEVINIT1) のサンプル

初級 Telnet 初期設定出口プログラム (DEVINIT1) は、Telnet クライアントを選別します。Telnet サーバーへの接続を許可するユーザーと許可しないユーザーを決定します。このサンプルは基礎的なものであり、Telnet 出口プログラムで使用できる他の多くの機能を利用するには設計されていません。上級 Telnet 出口プログラムは、それらの機能を利用するように設計されています。

まずは初級 Telnet 初期設定出口プログラムから始め、その内容を理解してから、仮想装置マッピングやその他の拡張機能の必要性に応じて上級 Telnet 初期設定出口プログラムに移行することをお勧めします。

## • 上級 Telnet 初期設定出口プログラム (DEVINIT2) のサンプル

上級 Telnet 初期設定 (ログオン) 出口プログラムは、アクセス・リスト MAP および DISALLOW を使用します。比較的単純な ALLOW リストの代わりに MAP リストを使用することで、上級初期設定プログラムでは初級版よりも多くの出口点インターフェースを活用することができます。これは、通常はクライアント・アクセス環境に見られる機能である、Telnet セッション設定の設定やオーバーライドを可能にします。セッション設定の例としては、以下のようなものがあります。

- そのセッションに対して特定の仮想端末を選択する
- サインオン・パネルを迂回する
- NLS サポートをセットアップする

## • Telnet 終了出口プログラム (DEVTERM) のサンプル

DEVTERM QCSRC は、切断メッセージをログに記録する単純なロギング・プログラムです。

これは、DEVINIT1 QCSRC および DEVINIT2 QCSRC 両プログラムの対となるプログラムです。このプログラムが記録する終了メッセージを初期化メッセージと組み合わせることによって、Telnet セッションの継続時間を判別することができます。

## Telnet 出口プログラムのサンプル・ファイル

ダウンロードする際、2 つのファイル・フォーマット ZIP および SAVF を選択することができます。どちらのフォーマットでも含まれているファイルは同じです。

.zip ファイルは PC と互換性のあるフォーマットです。 .zip ファイルを選択して PC にプログラムおよび情報ファイルをダウンロード後 unzip したら、それらのファイルを iSeries サーバーに転送してください。iSeries サーバーに転送後は、大部分のファイルを名前変更する必要があります。

.savf ファイルは i5/OS の保管ファイルです。このファイルを PC にダウンロードしてから、iSeries サーバーに転送してください。 iSeries に一時ライブラリーを作成し、このライブラリーに保管ファイルを転送できます。一時ライブラリーに保管ファイルを解凍し、readme ファイルの指示に従ってください。

希望のファイル・フォーマットのリンクをクリックして、「保管」をクリックします。

注: コードのサンプルを使用すると、114 ページの『コードに関するライセンス情報および特記事項』の条件に同意したものとみなされます。

- telnet.zip (924 KB)
- telnet.savf (5.45 MB)

---

## Telnet クライアントの管理

さまざまなエミュレーション・タイプを使用して Telnet クライアント・セッションを開始できます。また、カスケードされた Telnet セッションを確立する方法についても説明します。

iSeries Telnet クライアントを使用すれば、iSeries TCP/IP ユーザーは、Telnet サーバー・アプリケーションのあるリモート・システムにサインオンして、アプリケーションを使用することができます。Telnet を使用すると、リモート・コンピューターにログオンし、直接接続されているかのように、それを使用することができます。そして、プログラムの実行や構成の変更など、そのリモート・コンピューターを直接操作している場合に行える事柄を、すべて行うことができます。

Telnet により、ご使用のコンピューターはメインフレーム・コンピューターのワークステーションのように機能します。つまり Telnet を使用すると、ご使用のコンピューター (クライアント) は、リモート・コンピューター (Telnet サーバー) に直接接続された端末であるかのように機能します。つまり、端末をエミュレートします。

Telnet クライアントは RFC 2877 もサポートします。RFC 2877 クライアントは STRTCPTELN (TELNET) コマンドに指定するいくつかの新しいパラメーターによって、iSeries 上の Telnet サーバー仮想装置をより強力に制御できるようになりました。それらの新しいパラメーターは以下のとおりです。

表 11. STRTCPTELN コマンドの新規パラメーター

<ul style="list-style-type: none"> <li>• リモート仮想表示装置 (RMTVRTDSP)</li> <li>• リモート・ユーザー (RMTUSER)</li> <li>• リモート・パスワード (RMTPWD) (Telnet サーバーがサポートしている場合、新しい 128 バイトのパスワードのサポートを含む)</li> <li>• リモート・パスワード暗号化 (RMTPWENC) (DES7 および SHA1 暗号化を含む)</li> <li>• リモート初期プログラム (RMTINLPGM)</li> </ul>	<ul style="list-style-type: none"> <li>• リモート初期メニュー (RMTINLMNU)</li> <li>• リモート現行ライブラリー (RMTCURLIB)</li> <li>• リモート・キーボード・タイプ (RMTKBDTYPE)</li> <li>• リモート文字セット (RMTCHRSET)</li> <li>• リモート・コード・ページ (RMTCODPAG)</li> </ul>
---	--

## クライアントからの Telnet サーバー機能の制御

クライアント・セッションから、Telnet サーバー上のワークステーション処理を制御します。

iSeries Telnet クライアントには、クライアント・セッション中にシステム上でのワークステーションの処理を制御できるようにする制御機能があります。Telnet 制御機能を使用すると、すでに確立されたセッションに影響を与えるクライアントからサーバーへのコマンドを開始できます。

コマンド機能ごとに、iSeries サーバー名と TCP/IP 名がリストされます。

制御するサーバー機能を選択するには、「**Telnet 制御機能**」メニューにアクセスする必要があります。このメニューにアクセスするには、5250 キーボードで**アテンション**・キーを押します。

以下のリストでは、Telnet クライアント制御機能のそれぞれについて簡単に説明します。

**システムのプロセスへの割り込み 割り込みプロセスまたは IP:** この機能はサーバー上で開始しているプロセスの取り消し、割り込み、または中断を行います。たとえば、プロセスが永久ループになっていると思える場合、または意図せずにプロセスを開始してしまった場合に IP を使用できます。

**システムが非アクティブになった場合の接続状況の照会 接続状況の照会または AYT:** 接続状況の照会または AYT: この機能は、システムがまだ実行中であることを知らせるために、サーバーからメッセージを出します。システムが予期せずに長時間非活動状態になっているときに、この制御機能を使用できます。

**リモート出力がワークステーションに到達する前のリモート出力の破棄 リモート出力データの破棄または AO:** この機能によって、ワークステーションに出力を送信せずに、生成中の出力を持つプロセスの実行を完了することができます。この機能は、すでに作成されていてもワークステーションにはまだ表示されていないサーバー・システム出力を除去します。



システムとサーバー間のデータ経路のクリア データ経路のクリアまたは **SYNCH**: この機能は、ご使用のシステムとサーバー間のすべての文字 (ただし、Telnet コマンドは除く) を破棄します。ネットワークのフロー制御機構によって他の機能 (**IP**、**AO** など) がバッファに入れられる場合に、この機能を使用できません。

**Telnet セッションの終了 Telnet セッションの終了**または **QUIT**: この機能は、Telnet セッションを終了し、システム (リモート・システム) への TCP/IP 接続をクローズします。この機能は Telnet セッション中のいつでも要求できます。しかし、この機能を選択する前にリモート・システムをサインオフする必要があります。サインオフしない場合、Telnet プロトコルにはセッションの終了手順がないため、システムにサインオンしたままになります。

**リモート・ホストに対するアテンション・キー・オプションの使用** リモート・ホストに対する **ATTN** キー: アテンション・キーを押して、Telnet 制御機能メニューを表示します。

注:

1. このオプションは、5250 モードにのみ適用されます。
2. VTxxx モード (VT100 または VT220) を実行する場合、このメニューに 2 つの選択肢が加わりません。
  - VT100 セッションの場合、オプション 6 (VT100 基本キーボード・マップの変更) およびオプション 7 (VT100 代替キーボード・マップの変更)
  - VT220 セッションの場合、オプション 8 (VT220 基本キーボード・マップの変更) およびオプション 9 (VT220 代替キーボード・マップの変更)

#### 関連概念

『Telnet クライアント・セッションの開始』

このトピックを使用して、5250 Telnet クライアント・セッションを開始します。

60 ページの『3270 Telnet クライアント・セッションの開始』

このトピックでは、3270 エミュレーションを使用して Telnet クライアント・セッションを開始する方法を説明します。

67 ページの『VTxxx Telnet クライアント・セッションの開始』

VTxxx エミュレーションを使用して、Telnet クライアント・セッションを開始できます。

## 5250 Telnet クライアント・セッション

このトピックでは、このエミュレーション・タイプを使用して、Telnet サーバー・アプリケーションのあるリモート・システムにサインオンしてアプリケーションを使用する方法についての情報を示しています。

Telnet 5250 クライアント・サポートを使用すれば、iSeries は別のシステムにサインオンして、全画面 5250 アプリケーションにアクセスできます。5250 全画面サポートは、iSeries サーバー上で実行している Telnet サーバー・アプリケーション、または Telnet 5250 サーバーをサポートするシステムに限り、ネゴシエーションできます。リモート Telnet サーバー・アプリケーションとの間で 525x ワークステーション・サポートをネゴシエーションすることにより、5250 全画面サポートが活動化されます。

### Telnet クライアント・セッションの開始

このトピックを使用して、5250 Telnet クライアント・セッションを開始します。

注: Telnet セッションの開始相手となるリモート・システムの名前およびインターネット・アドレスを知っている必要があります。インターネット・アドレスおよびホスト名を表示するには、以下のステップを実行してください。



1. iSeries ナビゲーターを開始して、 **iSeries サーバー** → 「**ネットワーク**」を展開します。
2. 「**TCP/IP 構成**」をクリックしてから「**ホスト・テーブル**」をクリックして、インターネット・アドレスおよびホスト名を表示します。
1. iSeries コマンド行で STRTCPTELN コマンドを入力するか、または TELNET と入力して Enter を押しません。
2. リモート・システムの名前を入力し、オプション・パラメーターを使用する場合は F10 を押します。使用しない場合は、Enter を押します。

「**リモート・システム**」フィールドに \*INTNETADR と入力すると、「**インターネット・アドレス**」フィールドに入力するようサーバーがプロンプトを出します。

3. リモート・システムのインターネット・アドレスを入力し、オプション・パラメーターを使用する場合は F10 を押します。使用しない場合は、Enter を押します。画面にはインターネット・アドレス情報とオプション・パラメーターが表示されます。
4. デフォルトのパラメーター値を使用するには、**Enter** を押します。
5. 5250 全画面モード・セッションを開始する場合、以下のオプション・パラメーターも適用できます。
  - ホストのタイムアウト待ち (INZWAIT)
  - キーボードの言語タイプ (KBDTYPE)
  - リモート・ホスト・サーバー・アプリケーションのポート番号 (PORT)
  - リモート仮想表示装置 (RMTVRTDSP)
  - リモート・ユーザー (RMTUSER)
  - リモート・パスワード (RMPWD)
  - リモート・パスワード暗号化 (RMPWDENC)
  - リモート初期プログラム (RMTINLPGM)
  - リモート初期メニュー (RMTINLMNU)
  - リモート現行ライブラリー (RMTCURLIB)
  - リモート・キーボード・タイプ (RMTKBDTYPE)
  - リモート文字セット (RMTCHRSET)
  - リモート・コード・ページ (RMTCODPAG)

次に、リモート・システムのサインオン画面が表示されます。

#### 注:

1. STRTCPTELN コマンドで自動サインオン・パラメーター (RMTUSER、RMPWD、RMPWDENC) が入力されない場合や、これらのパラメーターが入力された際にエラーが生じた場合は、サインオン・パネルが表示されます。これらの値が正確に入力されれば、サインオン・パネルは表示されません。ユーザーのサインオンは自動的に行われ、そのユーザーに対して定義された初期パネルが表示されます。
2. さらに、次のことも当てはまります。
  - STRTCPTELN コマンドで、正確な RMTUSER、RMPWD、RMPWDENC パラメーターおよび正確な RMTINLPGM パラメーターが指定されている場合、ユーザーがサインオンされます。また、指定された初期プログラムも実行されます。
  - ただし、無効な RMTINLPGM が指定されている場合、ユーザーはサインオンされますが、「ジョブは異常終了しました (job ended abnormally)」というメッセージが表示されます。RMTINLMNU パラメーターが指定された場合にも、これと同じアクションが実行されます。

3. RMTURLIB パラメーターに関しても、正しい値が指定されていればユーザーはサインオンできません。さらに、ユーザー・プロファイルか STRTCPTELN コマンドのいずれかで定義された初期プログラムまたは初期メニュー、またはその両方が実行されます。それに加えて、現行ライブラリーもパラメーター値に設定されます。無効な RMTURLIB パラメーター値が指定されている場合、現行ライブラリー値が無効であることを示すメッセージがサインオン・パネルに表示されます。
4. また、上記のすべての項目に加えて、RMTKBDTYPE または RMTCHRSET または RMTCODPAG パラメーターに有効な値を指定すると、正常に自動サインオンされたときにこれらのパラメーターが有効になります。無効なサインオンが行われたときは、それらのパラメーターも無効になります。

注: システムが SOCKS サーバーを見付けられないか構成しない場合、あるいは SOCKS サーバーの使用中にエラーが起こった場合は、直接接続が確立されます。

## TN5250 画面サイズ

Telnet 5250 全画面モードは以下の画面サイズをサポートします。

- 全 5250 表示装置では、1920 文字 (24 x 80)
- 3180 モデル 2 と、3197 モデル D1、D2、W1、W2 と、3477 モデル FA、FC、FD、FE、FG、FW では、3564 文字 (27 x 132)

### 関連資料

57 ページの『クライアントからの Telnet サーバー機能の制御』

クライアント・セッションから、Telnet サーバー上のワークステーション処理を制御します。

93 ページの『カスケード Telnet セッションの確立』

Telnet セッションの内部から別の Telnet セッションを確立する方法について説明しています。カスケード・セッションを確立した後、異なるシステム間を移動できます。

## 3270 Telnet クライアント・セッション

3270 Telnet クライアント・セッションでは、このエミュレーション・タイプを使用して、Telnet サーバー・アプリケーションのあるリモート・システムにサインオンしてアプリケーションを使用する方法についての情報を提供しています。このセクションではさらに、3270 エミュレーションについての詳細も示しています。

3270 データ・ストリームは 5250 データ・ストリームに変換されるので、ワークステーション装置は、iSeries サーバーおよびアプリケーション・プログラムに対して、リモート 5251 表示装置として動作します。

### 3270 Telnet クライアント・セッションの開始

このトピックでは、3270 エミュレーションを使用して Telnet クライアント・セッションを開始する方法を説明します。

Telnet クライアントがリモート Telnet サーバー・アプリケーションとの間で 327x ワークステーション・サポートをネゴシエーションすると、システムは 3270 全画面モードを活動化します。Telnet クライアントは、(5250 ではなく) 3270 全画面アプリケーションをサポートする Telnet サーバー・アプリケーションとの間で、3270 全画面サポートをネゴシエーションします。リモート・システム・アプリケーションは、表示装置を制御します。表示される画面やデータの入力方法は、リモート・システムにローカル接続された他の 3270 装置の場合と同じです。

リモート・システム (Telnet を使用して接続するサーバー・システム) 上で、Telnet サーバーを開始する必要があります。

Telnet セッションの開始相手となるリモート・システムの名前およびインターネット・アドレスを知っている必要があります。インターネット・アドレスおよびホスト名を表示するには、以下のステップを実行してください。

1. iSeries ナビゲーターを開始して、**iSeries サーバー** → 「ネットワーク」を展開します。
2. 「**TCP/IP 構成**」をクリックしてから「**ホスト・テーブル**」をクリックして、インターネット・アドレスおよびホスト名を表示します。
1. STRTCPTELN コマンドを入力するか、コマンド行で TELNET と入力して Enter を押します。
2. リモート・システムの名前を入力します。オプション・パラメーターを使用する場合、F10 を押すか、Enter を押します。

「リモート・システム」名に \*INTNETADR と入力して Enter を押すと、「インターネット・アドレス」フィールドに入力を行うようサーバーがプロンプトを出します。

3. リモート・システムのインターネット・アドレスを入力します。オプション・パラメーターを使用する場合、F10 を押すか、Enter を押します。画面にはインターネット・アドレス情報とオプション・パラメーターが表示されます。
4. デフォルトのパラメーター値を使用するには、Enter を押します。Telnet サーバーへの接続が開始します。
5. 3270 全画面モード・セッションの間、以下のオプション・パラメーターも適用できます。
  - ホストのタイムアウト待ち (INZWAIT)
  - キーボードの言語タイプ (KBDTYPE)
  - ページ戻し (前ページ) キー (PAGEUP)
  - ページ送り (次ページ) キー (PAGEDOWN)
  - カーソル選択キー (CSRSLT)
  - 発信 3270 変換テーブル (TBL3270OUT)
  - 受信 3270 変換テーブル (TBL3270IN)
  - 数値ロック・キーボード (NUMLCK)
  - NULL の処理方法の変更 (NULLS)
  - リモート・ホスト・サーバー・アプリケーションのポート番号 (PORT)

次に、リモート・システムのサインオン画面が表示されます。

#### 関連概念

65 ページの『Telnet サーバーの 3270 キーボード・マッピング』

このトピックでは、3270 エミュレーションのサポートのためのキーボード・マッピングを説明していません。

62 ページの『3270 全画面の考慮事項』

3270 エミュレーションを使用するときには、以下の考慮事項を理解しておく必要があります。

#### 関連資料

57 ページの『クライアントからの Telnet サーバー機能の制御』

クライアント・セッションから、Telnet サーバー上のワークステーション処理を制御します。

## 3270 全画面の考慮事項

3270 エミュレーションを使用するときには、以下の考慮事項を理解しておく必要があります。

Telnet クライアントに 3270 全画面モードを使用するときには、以下の考慮事項に注意してください。

- 3270 画面サイズ
- 3270 カーソル選択キー
- 3270 エラー・メッセージ
- 3270 ヌル文字

## TN3270 画面サイズ

Telnet 3270 全画面モードの要件は、以下のとおりです。

- ネゴシエーションされた 3270 装置タイプに 1920 文字が必要な場合、iSeries Telnet クライアント・コードはクライアント端末として、任意の 5250 装置タイプから実行されます。
- ネゴシエーションされた 3270 装置タイプに 3564 文字が必要な場合、iSeries Telnet クライアント・コードにはクライアント端末として、3180 モデル 2、3197 モデル D1、D2、W1、W2、または 3477 モデル FA、FC、FD、FE、FG、または FW 5250 装置タイプのいずれかが必要です。
- 3180 モデル 2、3197 モデル D1、D2、W1、W2、または 3477 モデル FA、FC、FD、FE、FG、または FW 装置タイプがネゴシエーションされたとき、画面表示は 27x132 となります。以前のリリースでは、このサポートを受けるためにデータ域が必要とされました。
- 画面表示を 24x80 にするには、コマンド CRTDTAARA DTAARA(libname/QTVNO32785) TYPE(\*CHAR) VALUE('1') を実行します。

## TN3270 カーソル選択キー

カーソル選択キーのエミュレーションを選択した場合、既存のカーソル選択キーは使用不可となります。以下のパラメーターの 1 つを STRTCPTELN コマンドに指定すると、カーソル選択キーをエミュレートします。

表 12. カーソル選択キーをエミュレートするパラメーターの指定

パラメーター	値
前ページ (ロールダウン) キー	*CSRSLT
次ページ (ロールアップ) キー	*CSRSLT
カーソル選択キー	*F キー (*F1 から *F24 の機能キーを指定します)

## TN3270 メッセージ

Telnet 3270 全画面モードを使用しているとき、数種類のエラー・メッセージが表示されることがあります。

- キー入力エラーは、画面の左下角に明滅する 4 桁の数字として表示されます。メッセージについての詳細を表示するには、ヘルプ・キーまたは F1 (ヘルプ) を押します。エラーを修正できない場合は、System Operation を参照してください。
- システム・メッセージには、iSeries サーバーから発行された Telnet メッセージが含まれます。
- リモート・システムから送られたメッセージについては、リモート・システムの資料を参照してください。

## TN3270- ヌル文字の処理

3270 表示装置がデータ・ストリームを送信するとき、すべてのヌル文字は除去されます。STRTCPTELN コマンド上のヌル処理 (NULLS) パラメーターに、以下の値の 1 つを指定します。

### \*REMOVE

先頭および組み込みのヌル文字を除去します。

### \*BLANK

デフォルト値。先頭および組み込みのヌル文字をブランクに変更します。末尾のヌル文字は、どちらの値を指定した場合でも常に除去されます。たとえば、データが次のように構成されていると想定します (0 はヌルを表します)。

0x0yz000

デフォルトの \*BLANK で Telnet 3270 全画面を実行する 5250 表示装置から送られたデータ・ストリームには、次のコードが含まれることになります。

bxbyz

値 \*REMOVE で Telnet 3270 全画面セッションを実行する 3270 表示装置または 5250 表示装置から送られたデータ・ストリームには、次のコードが含まれることになります。

xyz

値 \*REMOVE は、以下の装置で有効です。

- ローカル接続した任意の表示装置
- リモート 5394 制御装置に接続された表示装置
- ワークステーション機能を使用しているパーソナル・コンピューター表示装置

### 関連概念

60 ページの『3270 Telnet クライアント・セッションの開始』

このトピックでは、3270 エミュレーションを使用して Telnet クライアント・セッションを開始する方法を説明します。

## 表示装置の使用

このトピックでは、Telnet 3270 全画面セッションで表示装置を使用する際のキーボードと表示の違いについて説明します。

Telnet 3270 全画面セッションで表示装置を使用する際は、キーボードと表示の違いを意識する必要があります。Telnet 3270 モードにおける他の考慮事項には、入力フィールドの数、エラー・メッセージ、およびセッションの終了があります。

## キーボードと文字セットの指定

STRTCPTELN コマンドのキーボード言語タイプ・パラメーターを使用してワークステーションに指定するキーボード言語タイプは、リモート接続されたワークステーションのキーボード言語タイプ・パラメーターと同じでなければなりません。一致しないキーボード言語タイプを指定すると、一部の文字が予期したとおりに表示されません。

## 5250 および 3270 キーボード

キーの位置と機能は、5250 キーボード (3196G、3180 Model 2、または 5291) と 3278 キーボードとで異なります。

注: 3270 全画面モードで稼働している Telnet クライアントの場合、3270 Clear 機能はデフォルトでキー・シーケンス Shift-Cmd-Backspace になっています。

System Operation for New Users には、以下のキーボードにおけるキーボードの違いが記載されています。

- IBM 拡張キーボード
- 122 キー・タイプライター型キーボード
- 5250 キーボード
- パーソナル・コンピューターまたはパーソナル・コンピューター IBM AT<sup>®</sup> コンピューター・スタイル・キーボード
- パーソナル・コンピューターまたはパーソナル・コンピューター AT 5250 スタイル・キーボード
- IBM 拡張パーソナル・コンピューター・キーボード

## パーソナル・コンピューター・キーボード

ご使用のパーソナル・コンピューターが iSeries Access for Windows Workstation Function (WSF) を使用している場合は、ワークステーション機能キー (WSFKEYS) コマンドを使用して 5250 キーボードのレイアウトを表示することができます。ワークステーション機能の構成 (CFGWSF) コマンドを使用すれば、スタイルを変更することができます。これらのコマンドについては、Client Access/400 for DOS with Extended Memory Setup で説明されています。ご使用のパーソナル・コンピューターが Workstation Function を使用していない場合は、適切な資料を参照して、キーボード・スタイルの表示や変更を行うエミュレーター (たとえば、OS/2<sup>®</sup> CM/2) を調べてください。

## TN3270--マイナス符号

STRTCPTELN コマンドの数値ロック・キーボード・パラメーターに値 \*YES を指定し、データ入力キーボードを使用しており、カーソルが「数字専用」フィールドにある場合、5250 マイナス符号を表示するには以下のタスクを完了してください。

1. Num (数字) キーを押します。
2. マイナス符号 (-) キーを押します。

3278 マイナス符号を表示するには、マイナス符号キーを押します。

## TN3270--次ページと前ページ

3270 アプリケーションの画面ですべての入力データ・フィールドを表示できない場合は、5250 次ページおよび前ページ・キーを使用すれば、画面上の入力フィールドの最大数を越えたときにデータを入力することができます。

また、STRTCPTELN コマンドでの使用を指定することにより、PF および PA 機能をページ・キーに割り当てることもできます。

5250 および 3270 画面では、カーソルは常に下線として表示されます。



## Telnet サーバーの 3270 キーボード・マッピング

このトピックでは、3270 エミュレーションのサポートのためのキーボード・マッピングを説明しています。

次の表は、様々な 5250 機能を実行するためのデフォルトの PF キー割り当てを示しています。キーボード・マップの表示 (DSPKBDMAP) コマンドを使用して、現行のキーボード・マッピングを表示することができます。または、端末が 3270 エミュレーション・モードであるときに、「TCP/IP Telnet の構成」メニューのオプション 6 (3270 キーボード・マップの表示) を使用することもできます。

表 13. デフォルトの PF キー割り当て

5250 機能キー	機能を選択するためのデフォルトの 3270 キー
ヘルプ	PF1
3270 のヘルプ	PF2
クリア	PF3
印刷	PF4
組み込み属性の表示	PF5
テスト要求	PF6
前ページ	PF7
次ページ	PF8
エラー・リセット	PF10 または実行キー
Sys Req	PF11
レコード後退	PF12
F1 から F12	PA1 を押してから、PF1 から PF12 のいずれかを押す
F13 から F24	PA2 を押してから、PF1 から PF12 または PF13 から PF24 (存在する場合) のいずれかを押す
制御	Erase EOF を押してから、フィールド・タブを押す
アテンション	3277 ではテスト要求を押してから、PA1 を押す。 3278/3279 では、ATTN キーを押す

次の CL プログラム例では、Telnet を使用して iSeries サーバーにアクセスする 327x タイプのワークステーション用にキーボード・マップを設定します。このプログラムは、iSeries 機能キーを 327x ワークステーションの同等の機能キーにマップします。3270 エミュレーション・モードではないワークステーションから CHGKBDMAP コマンドを実行しようとする、CPF8701 メッセージを受け取ります。そのメッセージをモニターすることによって、その状態が生じたときにプログラムの残りの部分が使用されないようにします。

```
PGM
MONMSG      MSGID(CPF8701 CPF0000)
CHGKBDMAP  PF1(*F1) PF2(*F2) PF3(*F3) PF4(*F4) PF5(*F5)
PF6(*F6) PF7(*DOWN) PF8(*UP) PF9(*F9)
PF10(*F10) PF11(*F11) PF12(*F12)
PA1PF1(*HELP) PA1PF2(*HLP3270)
PA1PF3(*CLEAR) PA1PF4(*PRINT)
PA1PF5(*DSPATR) PA1PF6(*TEST) PA1PF7(*F7)
PA1PF8(*F8) PA1PF9(*ATTN) PA1PF10(*RESET)
```

```
PA1PF11(*SYSREQ) PA1PF12(*BCKSPC)
```

```
ENDPGM
```

この CL ソースをライブラリー TCPLIB 内のファイル QCLSRC にメンバー CHGKBD として保管すれば、次のプログラムを使用して、CL プログラム CHGKBD をライブラリー TCPLIB 内に作成できます。

```
CRTCLPGM PGM(TCPLIB/CHGKBD) SRCFILE(TCPLIB/QCLSRC)
TEXT('Change the keyboard mapping for 327x terminals')
```

これにより、Telnet を使用して iSeries サーバーにアクセスしているすべてのユーザーがこの CHGKBD プログラムを使用することができます。さらに、CHGUSRPRF コマンドの初期プログラム・パラメーターに CHGKBD プログラムを指定することによって、サインオン時にこのプログラムを自動的に呼び出すこともできます。または、CHGKBD プログラムをプロファイルの初期プログラムによって呼び出すことも可能です。

## PC キーボード上の PA1 および PA2 キー

PA1 および PA2 キーは、PC キーボードにはありません。3270 エミュレーター内のキーボード・マップにより、これらの 3270 キーの機能が PC キーボード上に指定されます。

デフォルトの 3270 Telnet キーボード・マップでは、これらのキーが使用されます。そのため、3270 Telnet セッションを開始する前に、これらのキーがキーボード上のどこに存在するのかを知っていることは大切です。キーボードのマッピングを変更しないでセッションを開始する予定の場合、このことは特に大切です。ご使用のエミュレーターのマニュアルを参照して、これらの機能を実現するキーまたはキー・ストロークについて調べてください。

いくつかの 5250 キー・シーケンスではサポートされている 3270 キー・シーケンスが存在しないので、これらのキーボード・コマンドを 3270 上に設定することはできません。それらのキー・シーケンスは以下のとおりです。

- フィールド・プラス
- フィールド・マイナス
- すべての入力フィールドの消去

5250 制御キー機能を 3270 キーボードから実行するには、Erase EOF キーを使用してからタブ・キーを使用します。

## 特殊な状況

Telnet 3270 全画面モードを 3270 端末から使用しているとき、端末のデフォルト・マッピングが変更されるまで、PF1 から PF12 までのキーがキー・シーケンス PA1 PFx によってエミュレートされることがあります。そのため、「PF3 を押す」または「PF4 を押す」などの指示は、キーボード・マップを新規に作成するまで、「PA1 PF3 を押す」および「PA1 PF4 を押す」などと読み替えてください。

VM Telnet クライアントの場合のように、ホストに対してインストールされている Telnet クライアントによっては、PA1 を押したときに画面の下部に指示 TELNET command: が表示されることがあります。システムがこの指示を表示した場合には、PA1 と入力してから実行キーを押して、カーソルをコマンド入力行に移動してから目的の PF キーを押します。この場合、以下のコマンドが PF1 から PF12 をエミュレートします。

1. PA1 を押して、Telnet 指示 TELNET command を表示させる
2. PA1 と入力して、実行キーを押す
3. カーソルをコマンド入力行に移動する

#### 4. 目的の PF を押す

キーボードのマッピングについての詳細は、付録 D、『Telnet 3270 のキーボード・マッピング』を参照してください。

**注: ホスト・コマンド機能 (HCF)** は、System/370™、43xx、および 30xx ホスト・システムで使用可能な機能です。この機能により、ホスト・システム上のユーザーは iSeries サーバー上のアプリケーションを使用できるようになります。HCF を使用して iSeries サーバーに接続してから Telnet を使用してその iSeries サーバーから他の iSeries サーバーにサインオンした場合、3270 全画面モードのセッションとなります。キーボード・マップは、最初の HCF セッション用に 1 回、Telnet セッション用に 1 回の、合計 2 回行われます。通常と同じ方法で PF キーを使用するには、両方の iSeries サーバー上のキーボード・マッピングを変更しなければなりません。それぞれの iSeries サーバーで同じキーボード・マッピングを使用するように注意してください。

#### 関連概念

60 ページの『3270 Telnet クライアント・セッションの開始』

このトピックでは、3270 エミュレーションを使用して Telnet クライアント・セッションを開始する方法を説明します。

## VTxxx Telnet クライアント・セッション

VTxxx Telnet クライアント・セッションでは、このエミュレーション・タイプを使用して、Telnet サーバー・アプリケーションのあるリモート・システムにサインオンしてアプリケーションを使用する方法についての情報を提供しています。このセクションではさらに、VTxxx エミュレーションについての詳細も示しています。

Telnet VTxxx サポートを使用すれば、iSeries ユーザーは、システムにローカル接続された VTxxx 端末を使用しているかのように、非 iSeries サーバーにサインオンできます。Vtxxx クライアント・サポートによって、iSeries ユーザーは、Vtxxx バイト・ストリームをサポートする、TCP/IP ネットワーク中の任意のリモート・システムにサインオンできます。iSeries Telnet ユーザーは、VTxxx セッションと 5250 セッションの間の物理的な違いや操作上の違いを理解しておく必要があります。

### VTxxx Telnet クライアント・セッションの開始

VTxxx エミュレーションを使用して、Telnet クライアント・セッションを開始できます。

リモート・システム (Telnet を使用して接続するシステム) 上で、Telnet サーバーを開始する必要があります。

**注:** Telnet セッションの開始相手となるリモート・システムの名前およびインターネット・アドレスを知っている必要があります。インターネット・アドレスおよびホスト名を表示するには、以下のステップを実行してください。

1. iSeries ナビゲーターを開始して、**iSeries サーバー** → 「ネットワーク」を展開します。
  2. 「TCP/IP 構成」をクリックしてから「ホスト・テーブル」をクリックして、インターネット・アドレスおよびホスト名を表示します。
1. iSeries コマンド行で STRTCPTELN コマンドを入力するか、または TELNET と入力して **Enter** を押しします。
  2. リモート・システムの名前を入力するか、インターネット・アドレスを使う場合は \*INTNETADR と入力します。オプション・パラメーターを表示する場合は、F10 を押しします。使用しない場合は、**Enter** を押しします。

| 「リモート・システム」フィールドに \*INTNETADR と入力すると、「インターネット・アドレス」フィールドに入力を行うよう iSeriesがプロンプトを出します。

| 3. リモート・システムのインターネット・アドレスを入力します。オプション・パラメーターを使用する場合、**F10** を押すか、**Enter** を押します。画面にはインターネット・アドレス情報とオプション・パラメーターが表示されます。

| 4. デフォルトのパラメーター値を使用するには、**Enter** を押します。

| 5. VTxxx 全画面モード・セッションの間、以下のオプション・パラメーターも適用できます。

- | • 受信 ASCII 変換テーブル (TBLVTIN)
- | • 発信 ASCII 変換テーブル (TBLVTOUT)
- | • 特殊テーブル出力 (TBLVTDRAWO)
- | • 特殊テーブル入力 (TBLVTDRAWI)
- | • 選択オプション (VTOPT)
- | • 表示文字属性 (DSPCHRATTR)
- | • ページ・スクロール機能 (PAGE\_SCROLL)
- | • 返答機能 (ANSWERBACK)
- | • タブ・ストップ (TABSTOP)
- | • ホストのタイムアウト待ち (INZWAIT)
- | • コード化文字セット ID (CCSID)
- | • ASCII 操作モード (ASCOPRMODE)-- VT220 セッションの初期化だけに適用される (ネゴシエーションには影響しない)
- | • リモート・ホスト・サーバー・アプリケーションのポート番号 (PORT)
- | • 制御文字 (CTLCHAR)

| 注: リモート・システムの構成が不適切であると、予期しない文字が表示される場合があります。これが起きる場合、ワークステーション・タイプ値が VTxxx 全画面モード・ワークステーションに対して適切であるか検査します。また、set term コマンドを使用して、接続の全画面モードを変更することもできます。

| 次に、リモート・システムのサインオン画面が表示されます。

#### 関連概念

| 『VTxxx 全画面についての考慮事項』

| VTxxx エミュレーションを使用するときには、以下の考慮事項を理解しておく必要があります。

#### 関連資料

| 57 ページの『クライアントからの Telnet サーバー機能の制御』

| クライアント・セッションから、Telnet サーバー上のワークステーション処理を制御します。

| 74 ページの『VTxxx キー値』

| VTxxx キー値は、VTxxx エミュレーションのサポートのためのキーボード・マッピングを提供します。

| 81 ページの『VTxxx 各国語モード』

| VTxxx 各国語モードでは、7 ビットの文字セットのグループである、各国語置き換え文字セットがサポートされます。

## VTxxx 全画面についての考慮事項

VTxxx エミュレーションを使用するときには、以下の考慮事項を理解しておく必要があります。

エミュレーション・タイプの場合と同様、Telnet サーバーで VTxxx 全画面モードを使用する前には、特定の考慮事項を理解しておく必要があります。その考慮事項の中には、起こりうるエラー条件、表示ライント、そしてセキュリティーの問題が含まれます。VTxxx 全画面モードの使用方法の理解をより深めるには、それらの考慮事項に精通してください。

セキュリティー上の考慮事項に加えて、VTxxx 全画面モードを Telnet サーバーと共に使用する前に考慮の必要な他の多くの事柄があります。VTxxx 全画面モードを使用するときには、以下の考慮事項に注意してください。

- 『VTxxx 全画面モードのセキュリティーに関する考慮事項』
- 『VTxxx 全画面モードの Telnet および SNA 5250 のパススルーに関する考慮事項』
- 『VTxxx セッションのシステム要求処理』
- 70 ページの『5250 キーボードのエラー条件』
- 70 ページの『表示装置および VTxxx サポート』
- 70 ページの『操作方法の相違』
- 71 ページの『キーボードの特性』
- 72 ページの『画面の特性』
- 72 ページの『VTxxx の画面サイズ』
- 72 ページの『VTxxx の文字属性』

## VTxxx 全画面モードのセキュリティーに関する考慮事項

Telnet が仮想装置を自動的に構成すると、許可されるサインオンの試行回数は増えます。サインオンの試行回数は、許可されるシステム・サインオンの試行回数に実行可能な仮想装置の数を掛けた数に等しくなります。

QMAXSIGN システム値は、許可されるシステム・サインオンの試行回数を定義します。QAUTOVRT システム値は、Telnet が作成できる仮想装置の数を定義します。

## VTxxx 全画面モードの Telnet および SNA 5250 のパススルーに関する考慮事項

iSeries サーバーは 5250 パススルーをサポートします。5250 パススルーは Telnet と類似しています。ただしこれは TCP/IP ネットワークではなくシステム・ネットワーク体系 (SNA) プロトコル・ネットワーク上で稼働します。5250 パススルーは、Telnet と同じように、仮想表示装置を使用して物理装置に出力を送信します。5250 パススルーでは、Telnet の場合と同じように、iSeries サーバーは仮想装置を自動的に作成します。したがって、装置システム値は、5250 パススルーと Telnet の両方で自動構成される仮想装置の数を制御します。

## VTxxx セッションのシステム要求処理

VTxxx セッションのシステム要求処理は、通常の 5250 ワークステーションの場合と少し異なります。

5250 ワークステーションでシステム要求キーが押されると、画面の下部にシステム要求コマンド行が表示されます。Enter キーを押すと、「システム要求」メニューが表示されます。

VTxxx セッションでシステム要求機能呼び出すと、「システム要求」メニューが即時に表示されます。



## 5250 キーボードのエラー条件

一部のエラー条件では、5250 キーボードがロックされたり、エラー・コードがメッセージ行に表示されたりします。そのようなエラー条件の一つに、カーソルが入力フィールドにないときの入力があります。VTxxx セッションでは、このようなエラーが発生すると VTxxx ワークステーションでベルが鳴り、キーボードはアンロックの状態に保たれます。

5250 キーボードをロックし、5250 入力禁止ライトをオンにする iSeries アプリケーションもあります。ユーザーは、キーボードがアンロックされる前に取消キーを押さなければなりません。VTxxx セッションでは、5250 キーボードがロックされていると、キーが押されるたびに VTxxx 端末でベルが鳴ります。キーボードをアンロックするには、取消キーにマップされた VTxxx キーを押さなければなりません。デフォルトの VTxxx キーボード・マップでは、CTL-R キーが取消キーにマップされています。

## 表示装置および VTxxx サポート

システムが VTxxx サポートをネゴシエーションするとき、Telnet サーバーは最大で 80 桁 24 行の画面を送信します。VTxxx クライアント・システムでは、その画面は、5251 モデル 11 ワークステーションで表示されるのとはほぼ同じように表示されます。ただし、相違点がいくつかあります。

5251 ワークステーションでは、右側に表示ライトがあり、使用可能システム、メッセージ待ち中、キーボード・シフト、挿入モード、および入力禁止を示します。

VTxxx サーバー・サポートは、80 桁の 9 行目にアスタリスクを置くことによってシステムで使用可能なライトをエミュレートします。メッセージ待ち中、挿入モード、および入力禁止のライトの場合、アスタリスクは、80 桁の 11、13、15 行目に表示されます。アスタリスクが表示されると、それはその画面位置に表示されていた前の文字を上書きします。デフォルトでは、VTxxx サーバーは表示ライトを表示しません。表示ライトの切り替え機能にマップされたキー・シーケンスを入力することにより、表示ライトを使用可能にしたり使用不可にしたりすることができます。この機能のデフォルトのキー・シーケンスは ESC-T です。

### 注:

- VTxxx クライアントを使用して iSeries Telnet サーバーに接続するときは、挿入モードおよび入力禁止のライトが必ずしもここで説明したように表示されない場合があることに注意してください。5250 はローカル機能としてこの接続をサポートしますが、VTxxx にはその種の機能はありません。ただし、使用可能システムおよびメッセージ待ち中の表示ライトは正しく表示されます。
- 5251 画面は、桁区切り線として知られる画面属性をサポートします。**桁区切り線**とは、文字間に表示される縦線のことです。この行は文字スペースを消費しません。VTxxx ではこの種の属性はサポートされていません。iSeries アプリケーションが桁区切り線属性を使用する画面を生成すると、桁区切り線が VTxxx 下線属性にマップされた状態で、その画面は VTxxx クライアント・システム上に表示されます。

## 操作方法の相違

iSeries Telnet ユーザーは、VTxxx 端末と 5250 端末の間の物理的な違いや操作上の違いを理解しておく必要があります。

5250 はブロック・モードの端末です。5250 に入力されたデータはバッファに蓄積されて、AID (アテンション ID) キーが押されたときにだけ iSeries サーバーに送信されます。5250 キーボード上の AID キーは、機能を開始するキーです。以下のリストに 5250 キーボード上の AID キーを示します。

- クリア



- コマンド機能 1 から 24
- Enter/Rec Adv
- ヘルプ
- 印刷
- レコード後退機能
- ロールダウン (前ページ)
- ロールアップ (次ページ)

VTxxx 端末は、文字モードで稼働します。文字はキーが押されると即時にホストに伝送されます。

別の相違点は、データがディスプレイに届く方法です。システムは VTxxx 端末に 1 文字ずつ書き出すので、データが文字のストリームとして到着している様子が表示されます。5250 では、システムはデータをブロックごとに書き出すので、画面の全体または一部が一度に変更されます。

## キーボードの特性

5250 のカーソル移動キーは使用しないでください。その代わりに、\*CSRUP、\*CSRDOWN、\*CSRRIGHT、および \*CSRLEFT キーワードが関連付けられた機能キーを使用してください。デフォルトでは、これらはキー F13、F14、F15、および F16 です。5250 カーソル移動キーを使用すると、使用している VTxxx アプリケーションが予期したとおりに機能しないことがあります。これは、カーソル移動キーを使用してもその結果がリモート・システムに伝送されるのはアテンション識別コード (AID) キーが押されるときだからです。

たとえば、Telnet を使用して RS/6000<sup>®</sup> に接続し、VT220 エミュレーションを利用しているとき、SMIT コマンドによって AIX<sup>®</sup> へのメニューによるインターフェースが提供されます。このメニュー上では、\*CSRxx キーワードが関連付けられた機能キーを使用すれば、カーソル移動キーによって想定されている機能が実行されます。しかし 5250 のカーソル移動キーを使用した場合、カーソルは画面上を物理的に下に移動して SMIT オプションを正常に選択しますが、選択されたオプションは強調表示されません。キーの位置に関係なく、SMIT メニューの第 1 オプションが反転イメージによって強調表示されたままとなります。

iSeries キーボードに制御文字を入力する方法は、実際の VTxxx 端末に制御文字を入力する方法と異なります。VTxxx 端末では、制御キーを押しながら、制御機能が関連付けられた文字を押します。

iSeries Telnet サポートを使用しているとき、それと同等の操作を実行するためには、2 文字制御標識をタイプしてから、復帰なしの送信 (\*SENDWOCR) デフォルト機能が関連付けられた機能キー (F11 キー) を押します。たとえば、デフォルトのキーボード・マップおよびデフォルトの STRTCPTELN コマンド・パラメーターが有効であるとき、VTxxx での Control-C 機能を入力するためには、&C をタイプしてから F11 キーを押します。デフォルトのキーボード・マップを使用している場合、<F12> によってもこの機能を入力できます。使用しているアプリケーションによって <F12> が再マップされている場合のために、この例が示されて、\*SENDWOCR キーの原理を例示しています。

STRTCPTELN コマンドの CTLCHAR パラメーターを使用すれば、制御文字を示すために使用する文字を選択できます。デフォルトは、& です。&C の文字をタイプしたら、\*SENDWOCR 機能キーを押すまでの間に他のキーをタイプすることはできません。そうでないと、&C は制御文字として解釈されません。制御文字が伝送されるのは、\*SENDWOCR 機能キーが押されたときだけです。頻繁に使用される VTxxx 制御文字は、機能キーに割り当てることができます。Ctrl-C コマンドについての説明のための例を以下に示します。Telnet クライアントを使用して RS/6000 システムに接続しているとき、システムは通常 VT220 エミュレーションをネゴシエーションします。AIX において、Ctrl-C シーケンスは、PING などの長時間

実行されるコマンドを終了するために重要な文字列です。そのため、これを行う方法を RS/6000 コマンドを発行する前に知っておくことは大切です。デフォルトでは、その文字列は &C<F11> です。これらのキーを素早く入力する必要があること、および RS/6000 タスクがその入力を受け入れるまでに何回かの試行が必要な場合があることに、注意してください。

入力した文字を表示したくない場合は、\*HIDE 機能が関連付けられた機能キー (デフォルトのキーボード・マップでは F6) を押します。パスワードを入力するときには、この機能を使用してください。

タイプした文字を実行キーを押さないでリモート・システムに送信したい場合は、\*SENDWOCR 機能が関連付けられた機能キー (デフォルトのキーボード・マップでは F11) を押してください。

直前に入力したコマンドを再呼び出しできると、便利な場合が多くあります。iSeries サーバーでは、F9 がしばしばこの機能を提供します。AIX でこれを実現するには、コマンド `set -o vi` をタイプして実行キーを押します。その後、シーケンス `Esc-K` を使用してコマンドの検索を開始できます。VTxxx エミュレーションを使用しているときにデフォルトのキーボード・マップによってこの文字列を実行するには、シーケンス `<F5>k<F11>` を使用してください。Esc 文字によって、コマンドの検索が開始します。その後、k を使用して、さらに別のコマンドを検索します。このモードで実行しているとき、H は右、L は左、X は削除、I は挿入、および R は置換の各コマンドが適用されます。シーケンス `<F5>i<F11>` によって、この機能がオフに切り替わります。

## 画面の特性

カーソルの直前の位置にある文字は、常にブランクとして表示されます。実際の文字は内部的に保存されていて、カーソルが他の位置に移動して画面が最新表示されるときに、その文字が表示されます。

画面の第 1 行の第 1 列を使用する VTxxx アプリケーションは、iSeries Telnet クライアント・サポートを使用するとき動作が異なります。ほとんどの 5250 タイプの表示装置では、第 1 行の第 1 列に入力することができません。VTxxx アプリケーションが第 1 行の第 1 列にカーソルを表示させようとするとき、iSeries サーバーは自動的にカーソルを第 1 行の第 2 列に表示します。

アーキテクチャーの相違により、システムはサポートされていない特定のコマンドまたは文字列を無視します。例としては、ダウンストリーム・ロード可能文字セットがあります。

## VTxxx の画面サイズ

Telnet VTxxx 全画面モードは以下の画面サイズをサポートします。

- 3180 表示装置の場合：
  - 24 x 80 VTxxx 画面は 24 x 80 として表示されます。
  - 24 x 132 VTxxx 画面は 24 x 132 として表示されます。
- 5250 表示装置の場合：
  - 24 x 80 VTxxx 画面は 24 x 80 として表示されます。
  - 24 x 132 画面では、\*SHIFTDSP に割り当てられた機能キー (デフォルトのキーボード・マップでは F10) によって画面の情報を右または左に移動することが必要です。

## VTxxx の文字属性

VTxxx 端末は以下の属性をサポートしています。

- 明滅
- 太字

- 反転イメージ
- 下線
- 上記の属性の任意の組み合わせ

5250 データ・ストリームはこれらの属性をサポートしているため、5250 表示装置は VTxxx 属性のすべてを表示することができます。しかし、いくつかの制限もあります。

- 5250 データ・ストリームが同時にサポートできる文字属性は、3 つまでです。リモート・システムがすべての VTxxx 属性を同時に選択した場合、下線、明滅、および反転イメージ属性が表示されます。5250 表示装置は、下線、太字、および反転イメージの組み合わせを表示することはできません。VTxxx アプリケーションがこの組み合わせを選択した場合、下線および反転イメージが表示されます。
- 拡張属性をサポートしていない 5250 表示装置では、属性バイトがスペースを占有します。VTxxx 端末では、属性がスペースを占有することはありません。つまり、文字属性を選択した場合、5250 ディスプレイではすべてのデータが表示されていないことになります。文字属性を使用して表示する VTxxx データを受け取ると、5250 の属性バイトはデータの直前の位置をオーバーレイします。そこに表示されていた文字は、失われます。第 1 行の第 1 列に属性セットを使用して文字を表示しようとすると、その文字は表示されません。STRTPTELN コマンドに DSPCHRATTR(\*NO) を指定することによって、文字属性を表示しない設定を選択することができます。これにより、属性なしですべてのデータを表示できます。

注: 3477 表示装置などの拡張属性をサポートしている表示装置では、この制約事項は適用されません。

## VT100 キーボード標識

VT100 端末には、アプリケーションごとにプログラム可能な L1 標識があります。この標識は、iSeries Telnet サポートによってエミュレートされません。

### 関連概念

67 ページの『VTxxx Telnet クライアント・セッションの開始』

VTxxx エミュレーションを使用して、Telnet クライアント・セッションを開始できます。

96 ページの『Telnet に関連した問題の判別』

このトピックでは、サーバーの問題分析用フローチャートを含む診断情報、および Telnet の問題を報告するときに必要な資料のリストが示されています。

## VTxxx のエミュレーション・オプション

VTxxx エミュレーション・オプションは、VTxxx エミュレーション・タイプのカスタマイズ・オプションに関する情報を提供します。

Telnet サーバーで VTxxx 全画面モードを使用するとき、いくつかのオプション手順を行うことにより、エミュレーション・タイプを個人用に設定することができます。現行のキーボード・マップを表示してから、それを変更するかどうかを決めることができます。また、VT220 全画面モードを使用する際の制御文字を変更することもできます。

## VTxxx キーボード・マップの表示

現行のキーボード・マップを表示するには、VT キーボード・マップの表示 (DSPVTMAP) コマンドを使用します。このコマンドにはパラメーターがありません。iSeries サーバー機能にマップされた VTxxx キーが表示されます。

DSPVTMAP コマンドが有効なのは、VTxxx 全画面モードで実行されている iSeries Telnet サーバー・セッション内から呼び出される場合だけです。

DSPVTMAP と入力すると以下の画面が表示され、次ページキーを押すと追加画面が表示されます。

「TCP/IP Telnet の構成」メニューからオプション 3 を使用すれば、VT キーボード・マップを表示できます。

## VTxxx キーボード・マップの設定

デフォルトのキーボード・マップを変更するには、VT キーボード・マップの設定 (SETVTMAP) コマンドを使用します。(このコマンドは、「TCP/IP Telnet の構成」メニューのオプション 5 (VT キーボード・マップの設定 (Set VT keyboard map)) からでも使用できます。) ユーザー指定のパラメーターなしでこのコマンドを実行すると、指定された出荷時のデフォルトのキーボード・マップが復元されます。それぞれのパラメーターごとに、定義済み特殊値を 4 つまで指定できます。複数の iSeries サーバー機能を指定するために特殊値を使用することはできません。

## VTxxx キーボード・マップの変更

SETVTMAP と同様、VT キーボード・マップの変更 (CHGVTMAP) コマンドを使用すれば、VTxxx モードで iSeries Telnet サーバーに接続したときのキーボードのマッピングをカスタマイズできます。

SETVTMAP コマンドのパラメーターのデフォルトは、出荷時の値になります。一方、CHGVTMAP のパラメーターのデフォルトは、現行設定値になります。この違いを除いて、2 つのコマンドは同じです。

## VTxxx 自動折り返し

iSeries VTxxx サーバーでは、VTxxx クライアントで自動折り返し (autowrap) オプションがオンになっている必要があります。自動折り返しがオンになっている場合、文字が VTxxx の 80 桁目に書き込まれるとカーソルは次の行の 1 行目に移動します。このオプションの設定方法については、ご使用の VTxxx クライアントの資料を参照してください。

## VT220 の制御文字

VT220 8 ビット・エミュレーションがネゴシエーションされる場合、X'80' から X'9F' 文字の範囲は、DEC VT220 Programmer Reference Manual でアーキテクチャー定義されたとおり、C1 制御文字として保護されます。このとき、システムはデータ・ストリーム内のこれ以降の文字を、これらの文字の相対データとして解釈する可能性があります。システムが VT220 7 ビットまたは VT100 をネゴシエーションする場合、X'80' から X'F' の全範囲の文字を文字変換で使用できます。X'80' から X'9F' を C1 制御文字として解釈するのは、VT220 8 ビットの制御モードの場合だけにしてください。

これは特に各国語サポート (NLS) と関連があります。英語以外のいくつかの言語はこれらの値を言語固有の文字に使用するからです。そのような場合、VT220 8 ビット・エミュレーションは、期待通りに機能しない可能性があります。

### 関連資料

『VTxxx キー値』

VTxxx キー値は、VTxxx エミュレーションのサポートのためのキーボード・マッピングを提供します。

## VTxxx キー値

VTxxx キー値は、VTxxx エミュレーションのサポートのためのキーボード・マッピングを提供します。

VT100 および VT220 モードの両方におけるクライアント・セッション・サポートは、基本および代替キーボード・マップを提供します。VT220 モードの追加キーボード機能を利用するには、ご使用のキーボード・マップを保管しておくことができます。「VTxxx キーボード・マップの変更 (Change VTxxx Keyboard

Map)」画面で F6 キーを使用すれば、これらのキーボード・マップへのすべての変更点を以降のセッション用に保管することができます。データはユーザー・プロファイルに保管され、データは次に Telnet VTxxx エミュレーションが活動化されたときに自動的に適用されます。

「Telnet 制御機能の送信 (Send Telnet Control Functions)」メニューから選択するキーボード・オプションは、使用するキーボード・マップを決定します。図 2 から図 9 は、5250 AID キーに対応する VTxxx 機能を示しています。以下のリストは、オプション番号と対応図を示しています。

- 図 1 と 76 ページの図 2 はオプション 6 (「VT100 基本キーボード・マップの変更 (Change VT100 Primary Keyboard Map)」) を示しています。
- 76 ページの図 3 と 77 ページの図 4 はオプション 7 (「VT100 代替キーボード・マップの変更 (Change VT100 Alternate Keyboard Map)」) を示しています。
- 77 ページの図 5 と 78 ページの図 6 はオプション 8 (「VT220 基本キーボード・マップの変更 (Change VT220 Primary Keyboard Map)」) を示しています。
- 78 ページの図 7 と 79 ページの図 8 はオプション 9 (「VT220 代替キーボード・マップの変更 (Change VT220 Alternate Keyboard Map)」) を示しています。

「Telnet 制御機能の送信 (Send Telnet Control Functions)」メニューに表示されるオプションは、iSeries サーバーと Telnet サーバーの間でネゴシエーションされたサポートのレベルによって決まります。VT100 全画面モード・サポートが最初にネゴシエーションされた場合、メニューにはオプション 6 および 7 が表示されます。VT220 全画面モード・サポートが最初にネゴシエーションされた場合、メニューにはオプション 8 および 9 が表示されます。

注: VT100 の基本キーボード・マップと代替キーボード・マップのデフォルト値に違いはありません。

以下の図は、デフォルトのキーボード・マッピングを示しています。どの値も変更可能です。Enter キーを押した場合は、変更点が現行セッションについてのみ保管されます。F6 (保管) を押した場合は、変更点が永続的に保管され、次に VTxxx Telnet セッションを開始するまで有効になります。

```
+-----+
|                                     Change VT100 Primary Keyboard Map
| Type changes, press Enter:
| 5250 key          VT100 function
| Function Key 1 . . . *PF1
| Function Key 2 . . . *PF2
| Function Key 3 . . . *PF3
| Function Key 4 . . . *PF4
| Function Key 5 . . . *ESC
| Function Key 6 . . . *HIDE
| Function Key 7 . . . *TAB
| Function Key 8 . . . *CTLA
| Function Key 9 . . . *CTLB
| Function Key 10 . . *SHIFTDSP
| Function Key 11 . . *SENDWOCR
| Function Key 12 . . *CTLC
| Function Key 13 . . *CSRUP
| Function Key 14 . . *CSRDOWN
| Function Key 15 . . *CSRRIGHT
| Function Key 16 . . *CSRLEFT
|
|                                     More...
|
| F3=Exit  F6=Save  F12=Cancel
+-----+
```

図 1. Change VT100 primary keyboard map (画面 1)













**16 進データ:** 16 進ストリングを機能キーに割り当てることができます。機能キーを押すと、その 16 進データがリモート・システムに伝送されます。16 進データに復帰 (CR) および改行文字 (LF) は追加されません。データを入力してから機能キーを押すと、入力したデータに 16 進データが追加されてからリモート・システムに伝送されます。これにより、5250 キーボードに存在しない文字 (たとえば、大括弧) を入力することができます。16 進ストリングを割り当てするには、X に続けて引用符で囲まれた 16 進文字のストリング (たとえば、X'1A1A') を入力します。16 進データはリモート・システムに伝送される前にマップされません。

**ローカル iSeries 制御機能:** iSeries Telnet クライアント・セッションでローカルに処理されるキーワードを割り当てることができます。このような割り当てまたはマッピングを行うと、ASCII データ・ストリーム・トラフィックがリモート Telnet サーバー・セッションに伝送されない場合があります。これらのローカルな制御機能には、\*HIDE、\*SHIFTDSP、\*KEYPRI、および \*KEYALT があります。復帰なしの送信 (\*SENDWOCR) 機能もローカル機能ですが、この機能では ASCII データ・ストリームがリモート Telnet サーバー・セッションに伝送されます。

#### 関連概念

67 ページの『VTxxx Telnet クライアント・セッションの開始』

VTxxx エミュレーションを使用して、Telnet クライアント・セッションを開始できます。

#### 関連資料

73 ページの『VTxxx のエミュレーション・オプション』

VTxxx エミュレーション・オプションは、VTxxx エミュレーション・タイプのカスタマイズ・オプションに関する情報を提供します。

#### VTxxx の各国語サポート:

VTxxx 各国語サポートは、VTxxx エミュレーションを持つクライアントとサーバー間の文字マッピングを選択する代替方式を提供しています。

その方式は、以下のとおりです。

- コード化文字セット ID (CCSID)
- 各国間モード
- 各国語モード

これらの方式のどれも不適切な場合は、独自のユーザー定義マッピング・テーブルをセットアップして指定することができます。

**注:** VTxxx サポートは、1 バイト文字セット (SBCS) 言語のサブセットに制限されます。サポートされる言語のリストは、このセクションの後で示されます。サポートされるそれらの単一バイト言語の変換テーブルのいずれかを変更して、希望する単一バイト言語にマップできます。その後、クライアント Telnet を開始するための適切なパラメーターで識別できます。

モードの選択は、TCP/IP Telnet の開始 (STRTCPTLN) コマンドの CCSID パラメーターを使用して行います。このコマンドの受信 ASCII/EBCDIC テーブル (TBLVTIN)、および発信 EBCDIC/ASCII テーブル (TBLVTOUT) のパラメーターにより、ユーザー定義マッピング・テーブルが指定できます。それが不要ない場合、CCSID パラメーターで指定されたモードを使用することにより、デフォルト値の \*CCSID は文字マッピングが可能になります。

## VTxxx の各国間モード

各国間モードでは、DEC 各国間共通文字セットがサポートされます。これは、ヨーロッパの主要言語で使用されるほとんどの文字を含む 8 ビットの文字セットです。DEC 各国間共通文字セットには、ASCII 文字セットが含まれています。DEC 各国間共通文字セットはデフォルトで使用されます。

### VTxxx 各国語モード:

VTxxx 各国語モードでは、7 ビットの文字セットのグループである、各国語置き換え文字セットがサポートされます。

一度に使用できるのは、グループの 1 つの文字セットだけです。VT220 は、各国語モードの一部として、標準 7 ビット ASCII 文字セットもサポートします。VT220 端末は、以下の言語の 7 ビット ASCII 文字セットをサポートします。

- 英国英語
- デンマーク語
- オランダ語
- フィンランド語
- フランス語
- カナダ・フランス語
- ドイツ語
- イタリア語
- ノルウェー語
- スペイン語
- スウェーデン語
- スイス・フランス語 / スイス・ドイツ語
- 米国英語

各国語モードを使用するには、VTxxx 全画面モードで操作するときに受信 ASCII データを EBCDIC にマップし、発信 EBCDIC データを ASCII にマップするため、システムでマッピング・テーブルが必要です。

Telnet コマンドで CCSID パラメーターを使用して、各国語モード、つまり NLS マッピング・テーブルを選択します。

1 から 65553 の間の登録済み CCSID 値を表す数値を入力することは、適切なマッピング・テーブルを識別するための 1 つの方法です。*International Application Development* ブックには、登録済み CCSID の詳細が記載されています。

NLS マッピング・テーブルは、Telnet が最初に使用されるときにリモート・システムに動的に組み込まれます。このテーブルは DEC 各国語置き換え文字セットに基づきます。この文字セットは 7 ビットを基本とするので、文字セットに含まれるのは 1 つの国の固有文字だけです。DEC 各国間共通文字セットは 8 ビットを基本とするので、国グループの固有文字を含めることが可能です。

## テーブル・オブジェクトの識別

オブジェクトの処理コマンド WRKOBJ OBJ(QUSRSYS/Q\*) OBJTYPE(\*TBL) を使用すれば、テーブル・オブジェクト (\*TBL) を識別できます。





たとえば、QCHRID 697 285 (文字セット 697 コード・ページ 285) の英国英語システムで、CCSID(\*BRITISH) で Telnet を使用するメッセージ CPX8416 を使用する場合は、テーブル名は次のようになります。

- 発信 (EBCDIC/ASCII) Q285A06A5V
- 受信 (ASCII/EBCDIC) QA5V697285

## ユーザー定義マッピング・テーブル (ASCII モード)

各国間または NLS マッピング・テーブルがユーザーの要件を満たさない場合は、ユーザー定義文字マッピング・テーブルを作成し、それを使用できます。

STRTCPTELN コマンドの発信 (ASCII/EBCDIC) テーブル (TBLVTOUT) および受信 (ASCII/EBCDIC) テーブル (TBLVTIN) パラメーターを使用して、ユーザー定義マッピング・テーブルを指定することもできます。発信マッピング・テーブルまたは受信マッピング・テーブルのいずれかにのみユーザー定義マッピング・テーブルを指定し、指定しなかった方のものにデフォルト値を使用することもできます。

### 関連概念

67 ページの『VTxxx Telnet クライアント・セッションの開始』

VTxxx エミュレーションを使用して、Telnet クライアント・セッションを開始できます。

### 数字キーパッド:

このトピックでは、通常の場合に数字、小数点 (.), マイナス符号 (-), およびコンマ (,) についてコードを伝送する、補助キーパッド上のキーをリストします。

表 14. 補助キーパッド上のキー

キーワード	モード	送信される 16 進文字	制御文字の説明
*NUM0	VT52 モード	X'30' または X'1B3F70' <sup>1</sup>	数字キーパッドの 0 キー
*NUM0	VT100 または VT220 の 7 ビット・モード	X'30' または X'1B4F70' <sup>1</sup>	数字キーパッドの 0 キー
*NUM0	VT220 の 8 ビット・モード	X'30' または X'8F70' <sup>2</sup>	数字キーパッドの 0 キー
*NUM1	VT52 モード	X'31' または X'1B3F71' <sup>1</sup>	数字キーパッドの 1 キー
*NUM1	VT100 または VT220 の 7 ビット・モード	X'31' または X'1B4F71' <sup>1</sup>	数字キーパッドの 1 キー
*NUM1	VT220 の 8 ビット・モード	X'31' または X'8F71' <sup>2</sup>	数字キーパッドの 1 キー
*NUM2	VT52 モード	X'32' または X'1B3F72' <sup>1</sup>	数字キーパッドの 2 キー
*NUM2	VT100 または VT220 の 7 ビット・モード	X'32' または X'1B4F72' <sup>1</sup>	数字キーパッドの 2 キー
*NUM2	VT220 の 8 ビット・モード	X'32' または X'8F72' <sup>2</sup>	数字キーパッドの 2 キー
*NUM3	VT52 モード	X'33' または X'1B3F73' <sup>1</sup>	数字キーパッドの 3 キー
*NUM3	VT100 または VT220 の 7 ビット・モード	X'33' または X'1B4F73' <sup>1</sup>	数字キーパッドの 3 キー
*NUM3	VT220 の 8 ビット・モード	X'33' または X'8F73' <sup>2</sup>	数字キーパッドの 3 キー
*NUM4	VT52 モード	X'34' または X'1B3F74' <sup>1</sup>	数字キーパッドの 4 キー

表 14. 補助キーパッド上のキー (続き)

キーワード	モード	送信される 16 進文字	制御文字の説明
*NUM4	VT100 または VT220 の 7 ビット・モード	X'34' または X'1B4F74' <sup>1</sup>	数字キーパッドの 4 キー
*NUM4	VT220 の 8 ビット・モード	X'34' または X'8F74' <sup>2</sup>	数字キーパッドの 4 キー
*NUM5	VT52 モード	X'35' または X'1B3F75' <sup>1</sup>	数字キーパッドの 5 キー
*NUM5	VT100 または VT220 の 7 ビット・モード	X'35' または X'1B4F75' <sup>1</sup>	数字キーパッドの 5 キー
*NUM5	VT220 の 8 ビット・モード	X'35' または X'8F75' <sup>2</sup>	数字キーパッドの 5 キー
*NUM6	VT52 モード	X'36' または X'1B3F76' <sup>1</sup>	数字キーパッドの 6 キー
*NUM6	VT100 または VT220 の 7 ビット・モード	X'36' または X'1B4F76' <sup>1</sup>	数字キーパッドの 6 キー
*NUM6	VT220 の 8 ビット・モード	X'36' または X'8F76' <sup>2</sup>	数字キーパッドの 6 キー
*NUM7	VT52 モード	X'37' または X'1B3F77' <sup>1</sup>	数字キーパッドの 7 キー
*NUM7	VT100 または VT220 の 7 ビット・モード	X'37' または X'1B4F77' <sup>1</sup>	数字キーパッドの 7 キー
*NUM7	VT220 の 8 ビット・モード	X'37' または X'8F77' <sup>2</sup>	数字キーパッドの 7 キー
*NUM8	VT52 モード	X'38' または X'1B3F78' <sup>1</sup>	数字キーパッドの 8 キー
*NUM8	VT100 または VT220 の 7 ビット・モード	X'38' または X'1B4F78' <sup>1</sup>	数字キーパッドの 8 キー
*NUM8	VT220 の 8 ビット・モード	X'38' または X'8F78' <sup>2</sup>	数字キーパッドの 8 キー
*NUM9	VT52 モード	X'39' または X'1B3F79' <sup>1</sup>	数字キーパッドの 9 キー
*NUM9	VT100 または VT220 の 7 ビット・モード	X'39' または X'1B4F79' <sup>1</sup>	数字キーパッドの 9 キー
*NUM9	VT220 の 8 ビット・モード	X'39' または X'8F79' <sup>2</sup>	数字キーパッドの 9 キー
*NUMMINUS	VT52 モード	X'2D' または X'1B3F6D' <sup>1</sup>	数字キーパッドのマイナス・キー
*NUMMINUS	VT100 または VT220 の 7 ビット・モード	X'2D' または X'1B4F6D' <sup>1</sup>	数字キーパッドのマイナス・キー
*NUMMINUS	VT220 の 8 ビット・モード	X'2D' または X'8F6D' <sup>2</sup>	数字キーパッドのマイナス・キー
*NUMCOMMA	VT52 モード	X'2C' または X'1B3F6C' <sup>1</sup>	数字キーパッドのコンマ・キー
*NUMCOMMA	VT100 または VT220 の 7 ビット・モード	X'2C' または X'1B4F6C' <sup>1</sup>	数字キーパッドのコンマ・キー
*NUMCOMMA	VT220 の 8 ビット・モード	X'2C' または X'8F6C' <sup>2</sup>	数字キーパッドのコンマ・キー
*NUMPERIOD	VT52 モード	X'2E' または X'1B3F6E' <sup>1</sup>	数字キーパッドのピリオド・キー

表 14. 補助キーパッド上のキー (続き)

キーワード	モード	送信される 16 進文字	制御文字の説明
*NUMBERIOD	VT100 または VT220 の 7 ビット・モード	X'2E' または X'1B4F6E' <sup>1</sup>	数字キーパッドのピリオド・キー
*NUMBERIOD	VT220 の 8 ビット・モード	X'2E' または X'8F6E' <sup>2</sup>	数字キーパッドのピリオド・キー
*PF1	VT52 モード	X'1B50'	数字キーパッドの PF1 キー
*PF1	VT100 または VT220 の 7 ビット・モード	X'1B4F50'	数字キーパッドの PF1 キー
*PF1	VT220 の 8 ビット・モード	X'8F50' <sup>2</sup>	数字キーパッドの PF1 キード
*PF2	VT52 モード	X'1B51'	数字キーパッドの PF2 キー
*PF2	VT100 または VT220 の 7 ビット・モード	X'1B4F51'	数字キーパッドの PF2 キー
*PF2	VT220 の 8 ビット・モード	X'8F51' <sup>2</sup>	数字キーパッドの PF2 キード
*PF3	VT52 モード	X'1B52'	数字キーパッドの PF3 キー
*PF3	VT100 または VT220 の 7 ビット・モード	X'1B4F52'	数字キーパッドの PF3 キー
*PF3	VT220 の 8 ビット・モード	X'8F52' <sup>2</sup>	数字キーパッドの PF3 キード
*PF4	VT52 モード	X'1B53'	数字キーパッドの PF4 キー
*PF4	VT100 または VT220 の 7 ビット・モード	X'1B4F53'	数字キーパッドの PF4 キー
*PF4	VT220 の 8 ビット・モード	X'8F53' <sup>2</sup>	数字キーパッドの PF4 キード

<sup>1</sup> キーパッド数字モードのときは 1 文字が送信されます。キーパッド・アプリケーション・モードのときは 3 文字のシーケンスが送信されます。

<sup>2</sup> このシーケンスは、7 ビット・シーケンスを短くしたものです。これは、8 ビット・モード (リモート VT220 ホストまたはリモート VT220 サーバーによって呼び出せる) で操作している場合に表示されます。または、STRTCPTLN CL コマンドの ASCOPRMOD パラメーターで指定することもできます。

#### 関連概念

32 ページの『Telnet サーバーを VTxxx 全画面モードに構成する』

VTxxx サーバー・サポートを使用すれば、Telnet クライアント・ユーザーは、VTxxx 全画面サポートがネゴシエーションされていても、iSeries 5250 全画面アプリケーションにログオンして実行することができます。

#### 編集キーパッド:

以下の表は、編集キーパッドのキーのコードを送信するキーを示しています。

表 15. 編集キーパッドのキーのコードを送信するキー

キーワード	モード	送信される 16 進文字	制御文字の説明
*CSRUP	VT52 モード	X'1B41'	カーソル上移動キー

表 15. 編集キーパッドのキーのコードを送信するキー (続き)

キーワード	モード	送信される 16 進文字	制御文字の説明
*CSRUP	VT100 または VT220 の 7 ビットのカーソル・キー・モードのリセット	X'1B5B41'	カーソル上移動キー
*CSRUP	VT220 の 8 ビットのカーソル・キー・モードのリセット	X'9B41'	カーソル上移動キー
*CSRUP	VT100 または VT220 の 7 ビットのカーソル・キー・モードのセット	X'1B4F41'	カーソル上移動キー
*CSRUP	VT220 の 8 ビットのカーソル・キー・モードのセット	X'8F41'	カーソル上移動キー
*CSRDOWN	VT52 モード	X'1B42'	カーソル下移動キー
*CSRDOWN	VT100 または VT220 の 7 ビットのカーソル・キー・モードのリセット	X'1B5B42'	カーソル下移動キー
*CSRDOWN	VT220 の 8 ビット・モードのカーソル・キー・モードのリセット	X'9B42'	カーソル下移動キー
*CSRDOWN	VT100 または VT220 の 7 ビットのカーソル・キー・モードのセット	X'1B4F42'	カーソル下移動キー
*CSRDOWN	VT220 の 8 ビット・モードのカーソル・キー・モードのセット	X'8F42'	カーソル下移動キー
*CSRRIGHT	VT52 モード	X'1B43'	カーソル右移動キー
*CSRRIGHT	VT100 または VT220 の 7 ビットのカーソル・キー・モードのリセット	X'1B5B43'	カーソル右移動キー
*CSRRIGHT	VT220 の 8 ビットのカーソル・キー・モードのリセット	X'9B43'	カーソル右移動キー
*CSRRIGHT	VT100 または VT220 の 7 ビットのカーソル・キー・モードのセット	X'1B4F43'	カーソル右移動キー
*CSRRIGHT	VT220 の 8 ビットのカーソル・キー・モードのセット	X'8F43'	カーソル右移動キー
*CSRLEFT	VT52 モード	X'1B44'	カーソル左移動キー
*CSRLEFT	VT100 または VT220 の 7 ビットのカーソル・キー・モードのリセット	X'1B5B44'	カーソル左移動キー
*CSRLEFT	VT220 の 8 ビットのカーソル・キー・モードのリセット	X'9B44'	カーソル左移動キー

表 15. 編集キーパッドのキーのコードを送信するキー (続き)

キーワード	モード	送信される 16 進文字	制御文字の説明
*CSRLEFT	VT100 または VT220 の 7 ビットのカーソル・キー・モードのセット	X'1B4F44'	カーソル左移動キー
*CSRLEFT	VT220 の 8 ビットのカーソル・キー・モードのセット	X'8F44'	カーソル左移動キー
*FINDKEY	VT220 の 7 ビット・モード	X'1B5B317E'	編集キーパッドの Find キー
*FINDKEY	VT220 の 8 ビット・モード	X'9B317E' <sup>1</sup>	編集キーパッドの Find キー
*INSERTKEY	VT220 の 7 ビット・モード	X'1B5B327E'	編集キーパッドの Insert Here キー
*INSERTKEY	VT220 の 8 ビット・モード	X'9B327E' <sup>1</sup>	編集キーパッドの Insert Here キー
*REMOVEKEY	VT220 の 7 ビット・モード	X'1B5B337E'	編集キーパッドの Remove キー
*REMOVEKEY	VT220 の 8 ビット・モード	X'9B337E' <sup>1</sup>	編集キーパッドの Remove キー
*SELECTKEY	VT220 の 7 ビット・モード	X'1B5B347E'	編集キーパッドの Select キー
*SELECTKEY	VT220 の 8 ビット・モード	X'9B347E' <sup>1</sup>	編集キーパッドの Select キー
*PREVSCN	VT220 の 7 ビット・モード	X'1B5B357E'	編集キーパッドの Prev Screen キー
*PREVSCN	VT220 の 8 ビット・モード	X'9B357E' <sup>1</sup>	編集キーパッドの Prev Screen キー
*NEXTSCN	VT220 の 7 ビット・モード	X'1B5B367E'	編集キーパッドの Next Screen キー
*NEXTSCN	VT220 の 8 ビット・モード	X'9B367E' <sup>1</sup>	編集キーパッドの Next Screen キー

注: このシーケンスは、7 ビット・シーケンスを短くしたものです。これは、8 ビット・モード (リモート VT220 ホストまたはリモート VT220 サーバーによって呼び出せる) で操作している場合にのみ表示されます。または、STRTCPTELN CL コマンドの ASCOPRMOD パラメーターで指定することもできます。

#### 関連概念

32 ページの『Telnet サーバーを VTxxx 全画面モードに構成する』

VTxxx サーバー・サポートを使用すれば、Telnet クライアント・ユーザーは、VTxxx 全画面サポートがネゴシエーションされていても、iSeries 5250 全画面アプリケーションにログオンして実行することができます。

#### 5250 機能別の VTxxx キー値:

以下の表では、5250 機能別の VTxxx キー値について説明します。

表 16. 5250 機能別の VTxxx キー値

デフォルトの 5250 の機能	特殊値	VTxxx キー	16 進値 <sup>1</sup>
アテンション	*CTLA	<CTRL-A>	X'01'
アテンション	*ESCA	<ESC><A>	X'1B41'
バックスペース	*BACKSPC	<Backspace または CTRL-H>	X'08'
画面消去	*ESCC	<ESC><C>	X'1B43'
カーソル下	*CSRDOWN	<下矢印>	X'1B5B42'
カーソル左	*CSRLEFT	<左矢印>	X'1B5B44'
カーソル右	*CSRRIGHT	<右矢印>	X'1B5B43'
カーソル上	*CSRUP	<上矢印>	X'1B5B41'
削除	*DLT	<Delete>	X'7F'
削除	*RMV	<Remove>	X'1B5B337E' <sup>2</sup>
削除	*RMV	<Remove>	X'9B337E' <sup>3</sup>
複写	*ESCD	<ESC><D>	X'1B44'
実行	*RETURN	<Return または CTRL-M>	X'0D'
入力の消去	*CTLE	<CTRL-E>	X'05'
エラー・リセット	*CTLR	<CTRL-R>	X'12'
エラー・リセット	*ESCR	<ESC><R>	X'1B52'
フィールド前進	*TAB	<TAB または CTRL-I>	X'09'
フィールド・バックスペース	*ESCTAB	<ESC><Tab または CTRL-I>	X'1B09'
制御	*CTLK	<CTRL-K>	X'0B'
制御	*CTLX	<CTRL-X>	X'18'
制御	*ESCX	<ESC><X>	X'1B58'
フィールド・マイナス	*ESCM	<ESC><M>	X'1B4D'
ヘルプ	*CTLQST	<CTRL-?>	X'1F'
ヘルプ	*ESCH	<ESC><H>	X'1B48'
ホーム	*CTLO	<CTRL-O>	X'0F'
挿入	*ESCI	<ESC><I>	X'1B49'
挿入	*ESCDLT	<ESC><Delete>	X'1B7F'
挿入	*INS	<Insert Here>	X'1B5B327E' <sup>2</sup>
挿入	*INS	<Insert Here>	X'9B327E' <sup>3</sup>
改行	*ESCLF	<ESC> <Line Feed または CTRL-J>	X'1B0A'
次ページ (ロールアップ)	*CTLD	<CTRL-D>	X'04'
次ページ (ロールアップ)	*CTLF	<CTRL-F>	X'06'
次ページ (ロールアップ)	*NXTSCR	<Next Screen>	X'1B5B367E' <sup>2</sup>
次ページ (ロールアップ)	*NXTSCR	<Next Screen>	X'9B367E' <sup>3</sup>
前ページ (ロールダウン)	*CTLB	<CTRL-B>	X'02'
前ページ (ロールダウン)	*CTLU	<CTRL-U>	X'15'
前ページ (ロールダウン)	*PRVSCR	<Prev Screen>	X'1B5B357E' <sup>2</sup>



表 16. 5250 機能別の VTxxx キー値 (続き)

デフォルトの 5250 の機能	特殊値	VTxxx キー	16 進値 <sup>1</sup>
前ページ (ロールダウン)	*PRVSCR	<Prev Screen>	X'9B357E' <sup>3</sup>
印刷	*CTLP	<CTRL-P>	X'10'
印刷	*ESCP	ESC	X'1B50'
画面再描画	*CTLL	<CTRL-L>	X'0C'
画面再描画	*ESCL	<ESC><L>	X'1B4C'
システム要求	*CTLC	<CTRL-C>	X'03'
システム要求	*ESCS	<ESC><S>	X'1B53'
テスト要求	*CTLT	<CTRL-T>	X'14'
表示ライト切り替え	*ESCT	<ESC><T>	X'1B54'
F1	*ESC1	<ESC><1>	X'1B31'
F1	*F1	<F1> <sup>5</sup>	X'1B5B31317E' <sup>2</sup>
F1	*F1	<F1> <sup>5</sup>	X'9B31317E' <sup>3</sup>
F1	*PF1	<PF1>	X'1B4F50' <sup>2</sup>
F1	*PF1	<PF1>	X'8F50' <sup>3</sup>
F2	*ESC2	<ESC><2>	X'1B32'
F2	*F2	<F2> <sup>5</sup>	X'1B5B31327E' <sup>2</sup>
F2	*F2	<F2> <sup>5</sup>	X'9B31327E' <sup>3</sup>
F2	*PF2	<PF2>	X'1B4F51' <sup>2</sup>
F2	*PF2	<PF2>	X'8F51' <sup>3</sup>
F3	*ESC3	<ESC><3>	X'1B33'
F3	*F3	<F3> <sup>5</sup>	X'1B5B31337E' <sup>2</sup>
F3	*F3	<F3> <sup>5</sup>	X'9B31337E' <sup>3</sup>
F3	*PF3	<PF3>	X'1B4F52' <sup>2</sup>
F3	*PF3	<PF3>	X'8F52' <sup>3</sup>
F4	*ESC4	<ESC><4>	X'1B34'
F4	*F4	<F4> <sup>5</sup>	X'1B5B31347E' <sup>2</sup>
F4	*F4	<F4> <sup>5</sup>	X'9B31347E' <sup>3</sup>
F4	*PF4	<PF4>	X'1B4F53' <sup>2</sup>
F4	*PF4	<PF4>	X'8F53' <sup>3</sup>
F5	*ESC5	<ESC><5>	X'1B35'
F5	*F5	<F5> <sup>5</sup>	X'1B5B31357E' <sup>2</sup>
F5	*F5	<F5> <sup>5</sup>	X'9B31357E' <sup>3</sup>
F6	*ESC6	<ESC><6>	X'1B36'
F6	*F6	<F6>	X'1B5B31377E' <sup>2</sup>
F6	*F6	<F6>	X'9B31377E' <sup>3</sup>
F7	*ESC7	<ESC><7>	X'1B37'
F7	*F7	<F7>	X'1B5B31387E' <sup>2</sup>
F7	*F7	<F7>	X'9B31387E' <sup>3</sup>
F8	*ESC8	<ESC><8>	X'1B38'
F8	*F8	<F8>	X'1B5B31397E' <sup>2</sup>

表 16. 5250 機能別の VTxxx キー値 (続き)

デフォルトの 5250 の機能	特殊値	VTxxx キー	16 進値 <sup>1</sup>
F8	*F8	<F8>	X'9B31397E' <sup>3</sup>
F9	*ESC9	<ESC><9>	X'1B39'
F9	*F9	<F9>	X'1B5B32307E' <sup>2</sup>
F9	*F9	<F9>	X'9B32307E' <sup>3</sup>
F10	*ESC0	<ESC><0>	X'1B30'
F10	*F10	<F10>	X'1B5B32317E' <sup>2</sup>
F10	*F10	<F10>	X'9B32317E' <sup>3</sup>
F11	*ESCMINUS	<ESC><->	X'1B2D'
F11	*F11	<F11>	X'1B5B32337E' <sup>2</sup>
F11	*F11	<F11>	X'9B32337E' <sup>3</sup>
F12	*ESCEQ	<ESC><=>	X'1B3D'
F12	*F12	<F12>	X'1B5B32347E' <sup>2</sup>
F12	*F12	<F12>	X'9B32347E' <sup>3</sup>
F13	*ESCEXCL	<ESC><!>	X'1B21'
F13	*F13	<F13>	X'1B5B32357E' <sup>2</sup>
F13	*F13	<F13>	X'9B32357E' <sup>3</sup>
F14	*ESCAT	<ESC><@>	X'1B40'
F14	*F14	<F14>	X'1B5B32367E' <sup>2</sup>
F14	*F14	<F14>	X'9B32367E' <sup>3</sup>
F15	*ESCPOUND	<ESC><£>	X'1B23'
F15	*F15	<F15>	X'1B5B32387E' <sup>2</sup>
F15	*F15	<F15>	X'9B32387E' <sup>3</sup>
F16	*ESCDOLLAR	<ESC><\$>	X'1B24'
F16	*F16	<F16>	X'1B5B32397E' <sup>2</sup>
F16	*F16	<F16>	X'9B32397E' <sup>3</sup>
F17	*ESCPCT	<ESC><%>	X'1B25'
F17	*F17	<F17>	X'1B5B33317E' <sup>2</sup>
F17	*F17	<F17>	X'9B33317E' <sup>3</sup>
F18	*ESCCFX	<ESC><'>	X'1B5E' <sup>1</sup>
F18	*F18	<F18>	X'1B5B33327E' <sup>2</sup>
F18	*F18	<F18>	X'9B33327E' <sup>3</sup>
F19	*ESCAMP	<ESC><&>	X'1B26'
F19	*F19	<F19>	X'1B5B33337E' <sup>2</sup>
F19	*F19	<F19>	X'9B33337E' <sup>3</sup>
F20	*ESCAST	<ESC><*>	X'1B2A'
F20	*F20	<F20>	X'1B5B33347E' <sup>2</sup>
F20	*F20	<F20>	X'9B33347E' <sup>3</sup>
F21	*ESCLPAR	<ESC><(>	X'1B50'
F22	*ESCRPAR	<ESC><)>	X'1B51'
F23	*ESCUS	<ESC><_>	X'1B5F'

表 16. 5250 機能別の VTxxx キー値 (続き)

デフォルトの 5250 の機能	特殊値	VTxxx キー	16 進値 <sup>1</sup>
F24	*ESCPLUS	<ESC><+>	X'1B2B'
注 4 を参照	*FIND	<Find>	X'1B5B317E'
注 4 を参照	*FIND	<Find>	X'9B317E'
注 4 を参照	*SELECT	<Select>	X'1B5B347E'
注 4 を参照	*SELECT	<Select>	X'9B347E'

注:

- <sup>1</sup> - 他のものが指定されない場合、16 進値が VT100 モードになります。
- <sup>2</sup> - VT220 7 ビット制御モード。
- <sup>3</sup> - この VT キーにマップされる 5250 の機能キーはありません。
- <sup>4</sup> - F1 から F5 キーは、VT220 端末では使用できません。ただし、多くの VT220 エミュレーターは、F1 から F5 キーが押されたときに 16 進値を送信します。

#### VT220 ワークステーションの操作モード:

このトピックでは、システムが VT220 ワークステーション・タイプをネゴシエーションする場合にサポートされる複数の操作モードをリストします。

これらの操作モードは以下のとおりです。

- 7 ビット制御を持つ VT200 モードはデフォルトのモードで、標準 ANSI 機能を使用します。このモードは、8 ビット通信環境における一連の VT220 機能に 7 ビット制御を提供します。このモードは選択される文字セット・モードに応じて、DEC 各国間共通文字セットまたは各国語置き換え文字 (NRC) セットをサポートします。
- 8 ビット制御を持つ VT200 モードは標準 ANSI 機能を使用し、8 ビット通信環境における一連の VT220 機能に 8 ビット制御を提供します。このモードは選択される文字セット・モードに応じて、DEC 各国間共通文字セットまたは NRC セットをサポートします。
- VT100 モードは、標準 ANSI 機能を使用します。このモードでは、VT100 キーのキーボードの使用が制限されます。すべてのデータには 7 ビット制限があり、ASCII、NRC、または特殊図形文字だけが生成されます。
- VT52 モードは、DEC 専用機能 (ANSI ではない) を使用します。このモードでは、VT52 キーのキーボードの使用が制限されます。

VT220 モードがネゴシエーションされる場合、Telnet クライアントの初期操作モードは、TCP/IP Telnet の開始 (STRTCPTELN) コマンド、または TELNET コマンドの ASCII 操作モード (ASCOPRMOD) パラメーターを使用して選択されます。

#### VT220 の上段列の機能キー:

以下の表では、7 ビット・モードの VT220 キーボードの上段列にある機能キーのコードを送信するキーを説明します。

表 17. VT220 の上段列の機能キー

キーワード	送信される 16 進文字
*F6	X'1B5B31377E'
*F7	X'1B5B31387E'
*F8	X'1B5B31397E'
*F9	X'1B5B32307E'
*F10	X'1B5B32317E'
*F11	X'1B5B32337E'
*F12	X'1B5B32347E'
*F13	X'1B5B32357E'
*F14	X'1B5B32367E'
*F15 または *HELP	X'1B5B32387E'
*F16 または *DO	X'1B5B32397E'
*F17	X'1B5B33317E'
*F18	X'1B5B33327E'
*F19	X'1B5B33337E'
*F20	X'1B5B33347E'

以下の表では、8 ビット・モードの VT220 キーボードの上段列にある機能キーのコードを送信するキーを説明します。

キーワード	送信される 16 進文字
*F6	X'9B31377E'
*F7	X'9B31387E'
*F8	X'9B31397E'
*F9	X'9B32307E'
*F10	X'9B32317E'
*F11	X'9B32337E'
*F12	X'9B32347E'
*F13	X'9B32357E'
*F14	X'9B32367E'
*F15 または *HELP	X'9B32387E'
*F16 または *DO	X'9B32397E'
*F17	X'9B33317E'
*F18	X'9B33327E'
*F19	X'9B33337E'
*F20	X'9B33347E'

#### VT100 および VT220 制御文字キーワード:

以下のテーブルでは、VT100 および VT220 制御文字キーワードについて説明します。

表 18. VT100 および VT220 制御文字キーワード

制御文字の説明	CTRL キーを押しながら押すキー	キーワード	送信される 16 進文字
ヌル	スペース・バー	*NUL	X'00'
見出しの開始	A	*SOH,*CTLA	X'01'
テキストの開始	B	*STX,*CTLB	X'02'
テキストの終了	C	*ETX,*CTLC	X'03'
伝送の終了	D	*EOT,*CTLD	X'04'
問い合わせ	E	*ENQ,*CTLE	X'05'
確認	F	*ACK,*CTLF	X'06'
ベル	G	*BEL,*CTLG	X'07'
バックスペース	H	*BS,*CTLH	X'08'
水平タブ	I	*HT,*CTLI	X'09'
改行	J	*LF,*CTLJ	X'0A'
垂直タブ	K	*VT,*CTLK	X'0B'
用紙送り	L	*FF,*CTLL	X'0C'
復帰	M	*CR,*CTLM	X'0D'
シフトアウト	N	*SO,*CTLN	X'0E'
シフトイン	O	*SI,*CTLO	X'0F'
データ・リンク・エスケープ	P	*DLE,*CTLP	X'10'
装置制御 1	Q	*DC1,*CTLQ	X'11'
装置制御 2	R	*DC2,*CTLR	X'12'
装置制御 3	S	*DC3,*CTLS	X'13'
装置制御 4	T	*DC4,*CTLT	X'14'
否定の確認通知	U	*NAK,*CTLU	X'15'
同期信号	V	*SYN,*CTLV	X'16'
伝送ブロックの終了	W	*ETB,*CTLW	X'17'
直前の語または文字の取り消し	X	*CAN,*CTLX	X'18'
媒体の終了	Y	*EM,*CTLY	X'19'
置換	Z	*SUB,*CTLZ	X'1A'
エスケープ	[	*ESC	X'1B'
ファイル区切り	\	*FS	X'1C'
グループ分離	]	*GS	X'1D'
レコード分離	&eqv.	*RS	X'1E'
ユニット分離	?	*US	X'1F'
削除		*DEL	X'7F'

## カスケード Telnet セッションの確立

Telnet セッションの内部から別の Telnet セッションを確立する方法について説明しています。カスケード・セッションを確立した後、異なるシステム間を移動できます。

Telnet セッションの内部から別の Telnet セッションを開始できます。ホーム・システムは、使用している最初のクライアント・システムです。終端システムは、アクセスしている最後の Telnet サーバー・システムです。ホーム・システムから終端システムに至るまでにパススルーするシステムを、中間システムと言います。

## カスケード・セッションの開始

カスケード・セッションを開始するには、ホーム・システムにサインオンした後、クライアント・セッションを確立するステップを実行します。接続したいシステムごとに、このステップを繰り返します。

## サーバー・システムへの復帰

SIGNOFF コマンドはセッションを終了し、サーバー・システムのサインオン画面に戻ります。サーバー・システムにサインオンしたら、SIGNOFF コマンドは現行のサーバー・ジョブを終了し、サーバー・システムのサインオン画面に戻ります。

SIGNOFF コマンドの接続の終了 (ENDCNN) パラメーターを使用して、サーバー・システムをサインオフし、TELNET 接続を終了できます。signoff endcnn(\*yes) を使用すると、クライアント・システムの元のセッションに、複数の TELNET セッションを確立している場合は直前のセッションに戻ります。

### 注:

1. Telnet セッションを確立する対象となるシステムの数に制限はありません。
2. ホーム・システムは、システム要求入力行でシステム要求オプション 13 および 14 が入力された場合にそれを代行受信します。この機能は、サインオンできないシステムとの Telnet セッションを確立する場合に役立ちます。この場合、そのシステムのセッションを終了するには、次のステップを実行します。
  - システム要求キーを押します。
  - システム要求入力行で 13 (ホーム・システムでシステム要求を開始する (Start system request at home system)) を入力します。
  - システム要求メニューで 2 (前の要求を終了する (End previous request)) を入力します。

### 関連概念

4 ページの『Telnet シナリオ：カスケード Telnet セッション』

このシナリオでは、Telnet セッション中に別の Telnet セッションを開始する機能について示します。接続した後、システム要求値を使用してシステム間を移動できます。

58 ページの『Telnet クライアント・セッションの開始』

このトピックを使用して、5250 Telnet クライアント・セッションを開始します。

## 複数のカスケード Telnet セッション間の移動

カスケード Telnet セッションの開始後、SysRq キーを押して Enter を押すと、「システム要求」メニューが表示されます。

「システム要求」メニューでは、次のオプションが使用できます。

表 19. 「システム要求」メニューが提供するオプション

システム要求オプション	アクション	説明
10	クライアント・システムでのシステム要求の開始	直前のクライアント・システムの「システム要求」メニューを表示します。



表 19. 「システム要求」メニューが提供するオプション (続き)

システム要求オプション	アクション	説明
11	クライアント・システムへの転送	直前のクライアント・システムの代替ジョブに転送します。
13	ホーム・システムでのシステム要求の開始	中間システムまたは終端システムからホーム・システムの「システム要求」メニューに移動します。
14	ホーム・システムへの転送	中間システムまたは終端システムからホーム・システム上の代替ジョブに転送します。
15	終端システムへの転送	中間システムまたはホーム・システムから終端システムに転送します。

「システム要求」メニューをバイパスするには、SysRq キーを押してコマンド行で 10 を入力します。このショートカットが適用できるのは、iSeries サーバーの間の場合のみです。

### IBM 以外の Telnet クライアントの場合:

システム要求オプション 10、11、13、または 14 を使用しようとする、カスケード Telnet セッションが失われる場合があります。オプション 10 および 11 の場合、クライアント PC は直前のシステムです。オプション 13 および 14 の場合、クライアント PC はホーム・システムです。

ご使用の Telnet クライアントは、次の 2 つのテストに成功すれば互換性があります。

- オプション 13 または 14 の使用後、ホーム・システムに戻る。
- ホーム・システムからオプション 10 または 11 を使用する時、セッションが失われない。

非互換クライアントの場合、オプション 10、11、13、または 14 を使用する代わりに、以下のステップに従ってください。

1. システム要求オプション 11 を使用して、システムを前にさかのぼっていき、最後にホーム・システムに戻ります。ホーム・システムは、セッションの開始時に Telnet クライアントが接続した最初の iSeries です。
2. ホーム・システムから、システム要求オプション 1 を使用して、システムを順に進んでいきます。

#### 関連概念

4 ページの『Telnet シナリオ : カスケード Telnet セッション』

このシナリオでは、Telnet セッション中に別の Telnet セッションを開始する機能について示します。接続した後、システム要求値を使用してシステム間を移動できます。

## Telnet クライアント・セッションの終了

このトピックでは、Telnet セッションを完全に終了する方法について説明します。

iSeries サーバーに接続している場合、サインオフしても、Telnet サーバー・セッションが終了するとは限りません。セッションを終了するには、Telnet クライアントをローカル・コマンド・モードにするための一連のキーを入力する必要があります。そうすれば、コマンドを入力してセッションを終了することができます。次の表では、Telnet サーバー・セッションを終了するための一連のキーを示しています。

## Telnet クライアント・セッションの終了

- iSeries サーバーから、アテンション・キーを押してから、オプション 99 (TELNET セッションの終了 - QUIT) を選択します。
- その他のほとんどのシステムからの場合は、ログオフします。

クライアントをコマンド・モードにするためのキーがわからない場合は、システム管理者に相談するか、または Telnet クライアントの資料を調べてください。

また、SIGNOFF コマンドの接続の終了 (ENDCNN) パラメーターを使用しても、システムをサインオフし、Telnet 接続を終了できます。たとえば、SIGNOFF ENDCNN(\*YES) を使用すると、クライアント・システムに戻ります (1 つの Telnet セッションしか確立されていない場合)。または直前のシステムに戻ります (複数の Telnet セッションが確立されている場合)。

---

## Telnet の問題のトラブルシューティング

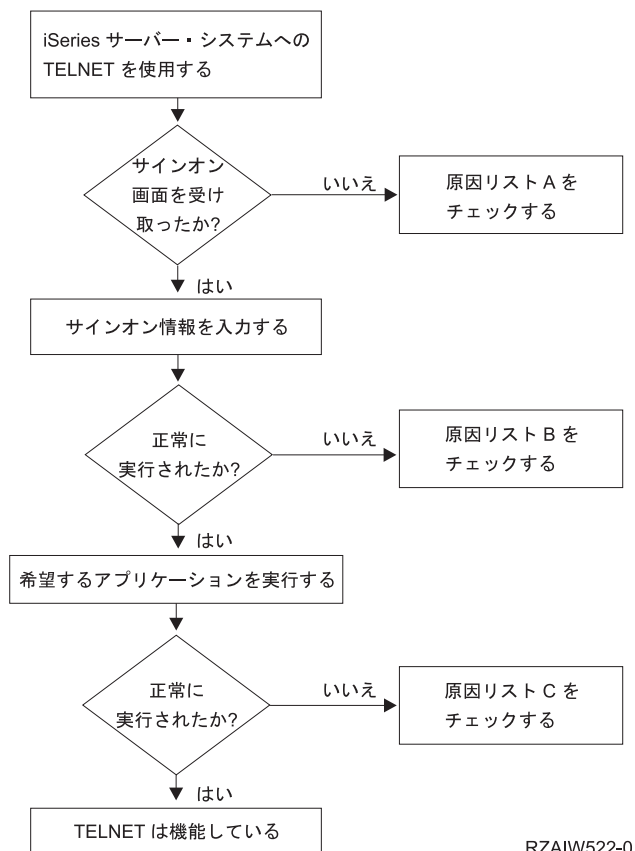
このトピックでは、Telnet の問題のトラブルシューティングや訂正に役立つ情報を示します。

これは完全なガイドではありませんが、最初の有用なステップとしての役割を果たします。

### Telnet に関連した問題の判別

このトピックでは、サーバーの問題分析用フローチャートを含む診断情報、および Telnet の問題を報告するときに必要な資料のリストが示されています。

一般的な TCP/IP 問題用のフローチャートを使用した後にこのフローチャートを使用してください。iSeries Telnet サーバーの使用時に問題が検出された場合は、このフローチャートを使用して原因を識別してください。フローチャートに続く原因リストは、潜在的な問題の識別に役立ちます。



## 原因リスト A

1. Telnet サーバー・ジョブが活動状態であることと、Telnet サービスが制限されていない有効なポートに割り当てられていることを確かめます。
  - a. QTVTELNET および QTVDEVICE ジョブが QSYSWRK サブシステムで活動状態であることを確かめるには、以下のステップを完了します。
    - 1) iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**実行管理機能**」を展開します。
    - 2) 「**活動ジョブ**」を右クリックして、QTVTELNET と QTVDEVICE が活動状態かどうかを調べます。活動状態である場合、ステップ 1c を続けます。
  - b. これらのジョブが活動状態でなければ、以下のステップを完了してこれらのジョブを開始します。
    - 1) iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」を展開します。
    - 2) 「**Telnet**」を右クリックして、「**開始**」を選択します。
  - c. 該当する Telnet サービスが有効なポートに割り当てられていることを確かめるには、以下のステップを完了します。
    - 1) iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」を展開します。
    - 2) 「**接続**」を右クリックし、「**開く**」を選択します。
    - 3) Telnet を探します。
  - d. 印刷装置の場合は、サブシステム QSPL が活動状態であることを確かめます。
  - e. ポート制約事項をチェックするには、メニュー CFGTCP を開いてオプション 4 (TCP/IP ポート制約事項の処理) を選択します。

2. iSeries サーバーの装置システム値が正しく設定されていて、Telnet サーバーが仮想装置を自動作成できるようにしていることを確かめます。
3. iSeries ナビゲーターで Ping ユーティリティを使用して、iSeries サーバーと Telnet クライアントの間のネットワーク接続が活動状態であることを確かめます。接続が活動状態でない場合は、ネットワーク管理者に問い合わせてください。
4. iSeries サーバー上において Telnet によって使用される仮想装置が、対話式 Telnet ジョブが実行されるサブシステムに定義されていることを確かめます。
  - a. サブシステムに定義されているワークステーション項目を参照するには、以下のステップを実行します。
    - 1) iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**実行管理機能**」を展開します。
    - 2) 「**サブシステム**」を右クリックし、「**開く**」を選択します。
  - b. ワークステーション項目の追加 (ADDWSE) コマンドを使用して、ワークステーションをサブシステムに定義します。たとえば、以下のコマンドを使用すれば、すべてのワークステーション・タイプが QINTER サブシステムの下で実行されるようにすることができます。

ADDWSE SBS(D(QINTER) WRKSTNTYPE(\*ALL)

5. 対話式サブシステム (QINTER) が活動状態であることを確かめます。対話式サブシステムが活動状態でない場合、Telnet 接続は失敗します。その状態では、問題を示すエラー・メッセージが QTVTELNET ジョブ・ログや QTVDEVICE ジョブ・ログに書き込まれることはありません。

サブシステムが活動状態であることを確かめるには、以下のステップを完了します。

- a. iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**実行管理機能**」を展開します。
  - b. 「**サブシステム**」を右クリックし、「**開く**」を選択します。
  - c. サブシステムが活動状態であることを確かめます。
6. VTxxx 全画面モードで操作している場合は、ローカル VTxxx クライアント構成で自動折り返しが指定されていることを確かめてください。自動折り返しがオンになっていれば、システムは自動的に行を 80 桁で折り返します。
  7. 登録情報の処理 (WRKREGINF) コマンドを使用して、出口点 QIBM\_QTG\_DEVINIT にフォーマット INIT0100 で登録されている Telnet 出口プログラムがないかどうかをチェックします。登録されたユーザー出口プログラムがある場合は、ジョブ名 QTVDEVICE の Telnet サーバー・ジョブ・ログで、そのプログラムに関連したエラーがないかどうかをチェックします。エラーが存在する場合は、出口プログラムでエラーを訂正するか、出口プログラムの除去 (RMVEXITPGM) コマンドによってその出口プログラムを除去します。
  8. クライアントが正しいポートを使用して Telnet に接続しようとしていることを確かめます。

Telnet サービスが割り当てられているポートを判別するには、以下のステップを完了します。

- a. iSeries ナビゲーターを開始し、**iSeries サーバー** → 「**ネットワーク**」 → 「**サーバー**」 → 「**TCP/IP**」を展開します。
  - b. 「**接続**」を右クリックし、「**開く**」を選択します。
  - c. Telnet を探します。
9. CFGTCP コマンドを使用して、クライアントが接続しようとしているポートが制限されていないことを確かめます。また、QTVTELNET ジョブ・ログで、使用しようとしているポートが制限されていることを示すメッセージがないかどうかを調べます。
  10. SSL Telnet を使用して接続しようとしている場合は、デジタル証明書マネージャー (DCM) といずれかの IBM Cryptographic Provider プログラムがインストールされていることを確かめます。これ

は、上記の項目への追加作業です。また、有効期限の切れていない有効な証明書が Telnet サーバー (QIBM\_QTV\_TELNET\_SERVER) に割り当てられていることを確かめます。

## 原因リスト B

1. 仮想表示装置に対する権限を確かめます。iSeries サーバーにサインオンしようとしたときにメッセージ CPF1110 を受信した場合は、仮想表示装置に対する権限がありません。iSeries Telnet サーバーが仮想装置を作成する際、ユーザー \*PUBLIC に認可される権限は QCRTAUT システム値によって判別されます。任意のユーザーが Telnet を使用してサインオンできるようにするには、このシステム値が \*CHANGE でなければなりません。
2. 機密保護担当者や \*SECOFR 権限を持っているユーザーは、QLMTSECOFR システム値が正しいことを確かめます。

## 原因リスト C

1. ワード処理の選択を確かめます。IBM OfficeVision® やフォルダーの処理 (WRKFLR) コマンドの使用時に問題が発生する場合は、Standard Editor の代わりに Office Adapted Editor を使用するよう構成を変更しなければならない場合があります。これを行うには、システム管理者に依頼して、ご使用のオフィス・ユーザー ID に関連した環境情報におけるワード処理の選択を変更してもらいます。
2. VTxxx 全画面モードで操作している場合は、ローカル VTxxx クライアント構成で自動折り返しが指定されていることを確かめてください。自動折り返しがオンになっていれば、システムは自動的に行を 80 桁で折り返します。
3. VTxxx セッションで文字が正しく表示されない場合は、セッションで正しいマッピング・テーブルが使用されていることを確かめます。
4. キーを押すたびに VTxxx クライアントがピープ音を出す場合は、キーボードがロックされている可能性があります。
5. QTVTELNET ジョブ・ログと QTVDEVICE ジョブ・ログで、iSeries サーバーに関するエラー・メッセージがないかどうかをチェックします。

### 関連概念

#### 装置システム値

68 ページの『VTxxx 全画面についての考慮事項』

VTxxx エミュレーションを使用するときには、以下の考慮事項を理解しておく必要があります。

## ホスト・サーバーの PING

iSeries ナビゲーターで Ping ユーティリティを使用して TCP/IP 接続をテストできます。

システムを PING するには、以下のステップを完了します。

1. iSeries ナビゲーターを開始して、**iSeries サーバー** → 「ネットワーク」を展開します。
2. 「TCP/IP 構成」を右クリックしてから、「ユーティリティ」を選択します。
3. 「PING」をクリックして、「PING」ダイアログ・ボックスを表示します。
4. 「PING」ボックスに、ホスト名 (たとえば、companyname.com) を入力します。
5. 「今すぐ PING」をクリックします。

「結果」ボックスにメッセージが表示されて、接続状況が示されます。

### 関連タスク

104 ページの『システム状況の検査』

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

## エミュレーション・タイプのトラブルシューティング

このトピックでは、個々のエミュレーション・タイプ内の問題を判別するための、より具体的な情報が示されています。

Telnet クライアントを開発する際は、適切なエミュレーション・ワークステーション・タイプをネゴシエーションすることが重要です。許可される機能はワークステーション・タイプによって異なります。以下のガイドは、ワークステーション・タイプとそのワークステーションの機能の理解に役立ちます。

### ワークステーション・タイプのネゴシエーションとマッピング

ワークステーションと印刷装置マッピングの表では、サーバーがクライアント・システムの物理表示装置と突き合わせる仮想表示装置のリストが示されています。

実行しているエミュレーション・パッケージがはっきりしない場合は、使用している仮想表示装置を判別する必要があります。これは、ジョブ処理 (WRKJOB) コマンドを使用すれば分かります。ジョブ名は最上部に表示されます。これは、ジョブに関連した仮想表示装置の名前です。デフォルトの命名規則は QPADEV xxxx です (xxxx は英数字)。

装置タイプを判別するには、以下のように入力します。

```
WRKCFGSTS *DEV QPADEVxxxx
```

装置の記述を処理することもできます。装置名の横に 8 (記述の処理) を入力してください。装置タイプが表示されます。次いで、装置タイプから、3270、5250、VT100、または VT220 の全画面モードで実行しているかどうかを判別することができます。

表 20. ワークステーションと印刷装置マッピング

サポートされるワークステーションと (モデル)	等価のタイプと (モデル)	インターネット仕様	説明
5251 (11)		IBM-5251-11	24 X 80 モノクロ・ディスプレイ
5291 (1)	5291 (2)	IBM-5291-1	24 X 80 モノクロ・ディスプレイ
5292 (2)		IBM-5292-2	24 X 80 カラー・グラフィックス・ディスプレイ: このワークステーション・タイプは、グラフィック・ワークステーション機能によってもエミュレートされます。
3196 (A1)	3196 (A1) 3196(B1) 3196 (B2) 3476 (EA)	IBM-3196-A1	24 X 80 モノクロ・ディスプレイ: このワークステーション・タイプは、モノクロ・ワークステーション機能によってもエミュレートされます。
3486 (BA)		IBM-3486-BA	24 X 80 モノクロ・ディスプレイ



表 20. ワークステーションと印刷装置マッピング (続き)

サポートされるワークステーションと (モデル)	等価のタイプと (モデル)	インターネット仕様	説明
3487(HA) <sup>2</sup>	3487 (HG) <sup>2</sup> 3487 (HW) <sup>2</sup>	IBM-3487-HA	24 X 80 モノクロ・ディスプレイ: このワークステーション・タイプは、モノクロ・ワークステーション機能によってもエミュレートされます。
3487 (HC) <sup>2</sup>		IBM-3487-HC	24 X 80 カラー・ディスプレイ: このワークステーション・タイプは、カラー・ワークステーション機能によってもエミュレートされます。
3179 (2)	3197 (C1) 3197 (C2) 3476 (EC)5292 (1)	IBM-3179-2	24 X 80 カラー・ディスプレイ: このワークステーション・タイプは、カラー・ワークステーション機能によってもエミュレートされます。
3180 (2)	3197 (D1) 3197 (D2) 3197 (W1) 3197 (W2)	IBM-3180-2	27 X 132 モノクロ・ディスプレイ
5555 (B01)	5555 (E01)	IBM-5555-B01	24 X 80 2 バイト文字セット (DBCS) モノクロ・ディスプレイ: このワークステーション・タイプは、DBCS 表示をサポートするワークステーション機能によってエミュレートされます。
5555 (C01)	5555 (F01)	IBM-5555-C01	24 x 80 DBCS カラー・ディスプレイ: このワークステーション・タイプは、DBCS 表示をサポートするワークステーション機能によってエミュレートされます。
5555 (G01)		IBM-5555-G01	24 X 80 2 バイト文字セット (DBCS) モノクロ・グラフィック・ディスプレイ: このワークステーション・タイプは、DBCS 表示をサポートするワークステーション機能によってエミュレートされます。

表 20. ワークステーションと印刷装置マッピング (続き)

サポートされるワークステーションと (モデル)	等価のタイプと (モデル)	インターネット仕様	説明
5555 (G02)		IBM-5555-G02	24 x 80 DBCS カラー・グラフィック・ディスプレイ: このワークステーション・タイプは、DBCS 表示をサポートするワークステーション機能によってエミュレートされます。
3477 (FC)		IBM-3477-FC	27 X 132 ワイド・スクリーン・カラー・ディスプレイ
3477 (FG)	3477 (FA) 3477 (FD) 3477 (FW)3477 (FE)	IBM-3477-FG	27 X 132 ワイド・スクリーン・モノクロ・ディスプレイ
3277 (0) <sup>3</sup>	3277 (DHCF)	IBM-3277-2	24 X 80 モノクロ・ディスプレイ
3277 (0) <sup>3,4</sup>	3278 (DHCF)	IBM-3278-2	24 X 80 モノクロ・ディスプレイ
3278 (0) <sup>3</sup>		IBM-3278-2-E <sup>5</sup>	24 x 80 モノクロ・ディスプレイ
3278 (0) <sup>3</sup>		IBM-3278-3	24 x 80 モノクロ・ディスプレイ
3278 (0) <sup>3</sup>		IBM-3278-4	24 x 80 モノクロ・ディスプレイ
3278 (0) <sup>3</sup>		IBM-3278-5	24 x 80 モノクロ・ディスプレイ
3279 (0) <sup>3</sup>	3279 (DHCF)	IBM-3279-2 IBM-3279-2-E <sup>5</sup>	24 X 80 モノクロ・ディスプレイ
3279 (0) <sup>3</sup>		IBM-3279-3	24 x 80 カラー・ディスプレイ
3812 (1)		IBM-3812-1	3812 印刷装置 (SBCS)
5553 (B01)		IBM-5553-B01	5553 印刷装置 (DBCS)
VT100 (*ASCII) <sup>6</sup>		DEC-VT100 VT100(7) VT102 DEC-VT102 DEC-VT200 DEC-VT220 VT200(7) VT220(7)	24 x 80 モノクロ ASCII ディスプレイ

**考慮事項:**

<sup>1</sup> 5555 (B01) と 5555 (C01) を除くすべての 5250 ワークステーションは、5251-11 ワークステーションとして稼働できます。

<sup>2</sup> このワークステーションは、24 x 80 または 27 x 132 に構成できます。ワークステーション・タイプ・パラメーター値を設定する前に、ワークステーションのモードを決定する必要があります。

<sup>3</sup> iSeries サーバーは、リモート 327x ワークステーションでは 24 X 80 画面だけをサポートしています。リモート 3277 (分散ホスト・コマンド機能 (DHCF) 版と通常版の両方) ワークステーションは IBM-3277-2 にマップされます。リモート 3278 ワークステーションは IBM-3278-2 にマップされます。リモート 3279 ワークステーションは IBM-3279-2 にマップされます。

<sup>4</sup> 一部の Telnet 3270 全画面 (TN3270) または 3278-2 エミュレーター・パッケージでは、構造化フィールド書き込みが正しくサポートされていません。このため、iSeries Telnet サーバー・インプリメンテーションでは、3278-2 タイプの装置が 3277-2 装置にマップされており、iSeries サーバーがこれらの TN3270 インプリメンテーションを処理できるようになっています。

<sup>5</sup> 拡張属性の強調表示はサポートされています。これには、下線、明滅、および反転表示が含まれます。3270 DBCS 処理もサポートされています。

<sup>6</sup> VT100 仮想装置は VT220 装置をサポートしています。

<sup>7</sup> VT100、VT200、および VT220 は、公式の端末タイプ名ではありません。ただし、一部のインプリメンテーションは、これらの名前を端末タイプ値として使用してネゴシエーションを行います。

#### 関連資料

53 ページの『INIT0100: 接続記述情報の形式』

このトピックでは、出口プログラムが使用できるクライアント接続についての情報を説明します。

## Telnet SSL サーバーのトラブルシューティング

このトピックでは、システム SSL の戻りコードと一般的な SSL の問題を含む、SSL サーバーのトラブルシューティングについての詳細な情報が示されています。

Telnet SSL サーバーの問題を識別するには、以下のステップに従います。

1. システム状況を検査して、適切なソフトウェアがインストールされていること、およびサーバーが開始済みであることを確認します。
2. ホスト・サーバーの PING を行って、TCP/IP が開始されていてネットワークが正常であることを確認します。
3. Telnet サーバーが開始済みであることを確認します。
4. NETSTAT \*CNN コマンドを使用して、活動状態の SSL 受話者が存在するかどうか検査します。
5. Telnet ジョブ・ログを検査して、SSL 戻りコードを探します。
6. 問題を解決するための提案について、SSL 戻りコードを参照してください。

不正確なデジタル証明書は、SSL で多くの問題を引き起こす可能性があります。デジタル証明書マネージャーを使用すると、認証局やシステム証明書を変更することができます。システム証明書が有効であることを確かめるには、デジタル証明書マネージャーの開始方法を参照の上、システム証明書を表示してください。

#### 関連概念

35 ページの『SSL で保護された Telnet』

Secure Sockets Layer (SSL) プロトコルを使用すると、Telnet サーバー・アプリケーションと Telnet クライアントとの間で、通信セッションの一方または両方のエンドポイントで認証を行う、保護された接続を確立することができます。SSL では、クライアントとサーバー・アプリケーションが交換するデータのプライバシーと安全性も提供します。

デジタル証明書

デジタル証明書マネージャーの開始

## 関連タスク

35 ページの『Telnet サーバー上での SSL の構成』

このトピックを使用して、iSeries サーバーに SSL をセットアップします。

## システム状況の検査

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

Telnet サーバーが SSL セッションを処理できる状態にあることを確認するには、以下のステップに従います。

1. Telnet SSL をサポートして証明書を管理するために必要な、以下のソフトウェアがインストールされていることを確認します。
  - TCP/IP Connectivity Utilities for iSeries、5722-TC1
  - デジタル証明書マネージャー、5722-SS1 - Boss Option 34
  - Cryptographic Access Provider、5722-AC x
  - IBM HTTP Server for iSeries、5722-DG1
  - Developer Kit for Java、5722-JV1
2. Telnet サーバー・アプリケーション QIBM\_QTV\_TELNET\_SERVER に証明書を関連付けることによって、保護された Telnet サーバーであることを検査します。
3. TCP/IP 接続とネットワークの状況を検査するために、ホスト・システムで PING を実行します。
4. Telnet サーバーが開始済みを確認します。
5. SSL 接続を許可するように Telnet サーバーが構成されているを確認します。

## 関連タスク

37 ページの『証明書を Telnet サーバーに割り当てる』

システム上の Telnet サーバーが SSL を使用できるようになったら、iSeries Access for Windows、またはその他の SSL を使用可能な Telnet クライアント (パーソナル・コミュニケーションズのエミュレーターなど) からシステムへ、保護された Telnet 接続を確立することができます。

99 ページの『ホスト・サーバーの PING』

iSeries ナビゲーターで Ping ユーティリティを使用して TCP/IP 接続をテストできます。

23 ページの『Telnet サーバーの開始』

このトピックでは、Telnet サーバーの開始について説明します。

35 ページの『Telnet サーバー上での SSL の構成』

このトピックを使用して、iSeries サーバーに SSL をセットアップします。

## 関連資料

106 ページの『SSL 戻りコード』

このトピックでは、SSL 初期化や SSL ハンドシェイクの際に発生しやすい問題に対するシステムの SSL 戻りコードをリストします。

## 活動状態の SSL 受話者が存在するかどうかの検査

このトピックでは、活動状態の SSL 受話者が存在するかどうかを検査する方法について説明します。

Telnet サーバーは活動状態で、接続試行を受け入れ可能な状態でなければなりません。活動状態の SSL 受話者が存在するかどうかを検査するには、以下のステップに従います。

1. iSeries 文字ベースのインターフェースで、NETSTAT \*CNN と入力して、「TCP/IP 接続状況の処理」画面を表示します。

2. 「ローカル・ポート」列で、telnet-ssl を表す telnet- ラベルを探します。フィールドの長さが十分でないため、telnet- のみが表示されます。
  - F22 キーを使用すると、「ローカル・ポート」フィールド全体を表示できます。
  - F14 キーを使用すると、ポート番号が表示されます。 telnet-ssl 項目のポートは 992 です。

「ローカル・ポート」列に telnet-ssl が見付からなければ、SSL の初期化は失敗したということです。この問題を修正する上で役立つ情報として、QSYSWRK サブシステムで実行している QTVTELNET ジョブ・ログの中の SSL 診断メッセージを調べてください。SSL の初期化が失敗した場合、実行される QTVTELNET ジョブは 1 つだけです。

#### 関連タスク

『Telnet ジョブ・ログの検査』

SSL 初期化およびハンドシェイクが失敗すると、Telnet サーバーより CPDBC nn 診断メッセージが QTVTELNET ジョブへ送信されます。

## Telnet ジョブ・ログの検査

SSL 初期化およびハンドシェイクが失敗すると、Telnet サーバーより CPDBC nn 診断メッセージが QTVTELNET ジョブへ送信されます。

Telnet ジョブ・ログを検査するには、以下のステップに従います。

1. iSeries ナビゲーターで、iSeries サーバー → 「ネットワーク」 → 「TCP/IP 構成」 → 「IPv4」を展開します。
2. 「接続」をクリックします。
3. 失敗しているクライアント・ワークステーションの IP アドレスを右クリックして、「ジョブ」を選択します。ジョブ名を書き留めます。
4. 「ジョブ管理」 → 「サーバーのジョブ」を展開します。
5. 「ジョブ名」列で、QTVTELNET を右クリックします。
6. 「ジョブ・ログ」を選択します。
7. 「メッセージ ID」列で、CPDBC nn メッセージを探します。

Telnet サーバー・ジョブに関して、以下の事柄に注意してください。

- SSL 受話者が初期化に失敗すると、QTVTELNET ジョブが 1 つだけ開始します。
- システムの再始動後に Telnet が開始すると、QTVDEVICE および QTVTELNET ジョブが開始します。
- Telnet サーバーが SSL 受話者を開始すると、同じ数の QTVTELNET および QTVDEVICE ジョブが開始します。
- ENDTCPSVR \*TELNET コマンドまたは ENDTCP コマンドを使用すると、QTVTELNET ジョブが終了します。
- QSYSWRK サブシステムが終了すると、QTVDEVICE ジョブが終了します。

#### 関連概念

41 ページの『SSL 初期化およびハンドシェイク』

このトピックでは、Telnet サーバー、クライアント、および SSL の間の相互作用に関する詳細を説明しています。

#### 関連タスク

104 ページの『活動状態の SSL 受話者が存在するかどうかの検査』

このトピックでは、活動状態の SSL 受話者が存在するかどうかを検査する方法について説明します。

## SSL 戻りコード

このトピックでは、SSL 初期化や SSL ハンドシェイクの際に発生しやすい問題に対するシステムの SSL 戻りコードをリストします。

以下の戻りコード表を参照する前に、次の点に注意してください。

- QTVTELNET ジョブ・ログの中で SSL 戻りコードを探す必要があります。
- 場合によっては、デジタル証明書マネージャー構成を使用して、認証局 (CA) 証明書やシステム証明書の問題を訂正する必要があります。
- Telnet SSL クライアント用に CA 証明書情報をコピーする時は、BEGIN CERTIFICATE および END CERTIFICATE という語を含む行を必ず含めてください。

### 一般的な戻りコード

表 21. 一般的な戻りコード

戻りコード	説明
-2	<p><b>SSL 処理に使用できるシステム証明書がありません。</b> Telnet サーバーは正常に SSL を初期化しましたが、SSL ハンドシェイクが失敗しました。SSL Telnet クライアント・ウィンドウにはサインオン・パネルが表示されません。QIBM_QTV_TELNET_SERVER アプリケーションに割り当てられたシステム証明書が存在しません。</p> <p>システム証明書を調べて、「Certificate Assigned」列の値が Yes であることを確認してください。値が No であれば、QIBM_QTV_TELNET_SERVER アプリケーション用のシステム証明書を作成してください。</p>
-4	<p><b>CA 証明書またはシステム証明書が不適切です。</b> システム証明書が専用ではなく、信頼されてもいません。サーバー証明書の Private Key フィールドおよび Trusted フィールドが不適切です。Telnet SSL クライアント・ウィンドウにはサインオン・パネルが表示されません。</p> <p>認証局 (CA) の情報を Telnet SSL クライアントに追加してください。iSeries Access for Windows を Telnet SSL クライアントとして使用している場合、『SSL 通信セッションのための公衆インターネット証明書の管理』を参照してください。それ以外の場合は、『専用 CA 証明書のコピーの取得』で手順を参照してください。</p>
-16	<p><b>対等システムが認識されません。</b> Telnet SSL クライアントが初めて SSL セッションの確立を試みる時、もっとも頻繁に生じるのがこの問題です。Telnet SSL クライアント・ウィンドウにはサインオン・パネルが表示されません。</p> <p>認証局 (CA) の認証情報を Telnet SSL クライアントに追加してください。</p>
-18	<p><b>システム証明書は自己署名されたものであり、サーバーはこれを CA 証明書として使用しています。</b> QIBM_QTV_TELNET_SERVER アプリケーションに割り当てられるシステム証明書は、信頼のおけるものであること、認証局の署名があること、および有効な時間枠内に使用されることが必要です。CA 証明書を作成して、それをシステム証明書に関連付ける必要があります。システム証明書が不適切であれば、Telnet サーバーは SSL を初期化しません。</p> <p>CA 証明書を作成して、それをシステム証明書と関連付けます。</p>
-23	<p><b>システム証明書は信頼のおける認証局によって署名されていません。</b></p> <p>QIBM_QTV_TELNET_SERVER アプリケーションに割り当てられるシステム証明書は、信頼のおけるものであること、認証局の署名があること、および有効な時間枠内に使用されることが必要です。</p> <p>CA 証明書を Trusted に変更します。その手順については、『DCM によるアプリケーションの管理』を参照してください。</p>



表 21. 一般的な戻りコード (続き)

戻りコード	説明
-24	CA 証明書の有効期間が満了しました。期限切れの証明書を使用しています。 Telnet SSL クライアント・ウィンドウにはサインオン・パネルが表示されません。  システム証明書の作成に使われた CA 証明書を更新します。
-93	SSL が使用できません。活動状態の SSL 受話者が存在しないため、 Telnet SSL クライアントがホストに接続できません。  Telnet SSL をサポートして証明書を管理するために必要なソフトウェアをインストールします。その方法については、システム状況の検査を参照してください。

### その他の SSL 戻りコード

以下の表にある SSL 戻りコードが報告された場合は、デジタル証明書マネージャーを使用して、デジタル証明書が次の要件を満たすことを確認してください。

- CA 証明書が有効で、有効期限が満了していないこと。
- Telnet サーバー・アプリケーション QIBM\_QTV\_TELNET\_SERVER の Certificate Assigned 列の値が Yes であること。
- 認証局がシステム証明書に署名していること。
- システム証明書が信頼のおけるものであること。
- システム証明書が、証明書に示された時間枠内で使用されていること。

表 22. その他の SSL 戻りコード

戻りコード	説明
-1	暗号が使用可能ではないか、指定されていません
-6	i5/OS はこのタイプの証明書をサポートしません
-10	SSL 処理でエラーが発生しました。ジョブ・ログの CPExxxx メッセージ (xxxx はソケット error 値) を検査してください。
-11	SSL が不正な形式のメッセージを受け取りました
-12	不正なメッセージ認証コードを受け取りました
-13	操作は SSL によってサポートされていません
-14	証明書シグニチャーが無効です
-15	不正な証明書です
-17	オブジェクトへのアクセス許可が拒否されました
-20	SSL 処理に必要な記憶域を割り振れません
-21	SSL は SSL セッション内で不適切な状態を検出しました
-22	SSL 接続に使われるソケットが閉じています
-25	証明書の日付形式が不適切です
-26	キーの長さがエクスポートに不適切です
-90	キー・リング・ファイルではありません
-91	キー・データベース内のパスワードの有効期限が満了しました
-92	証明書が無効、または出口プログラムによって拒否されました
-94	ジョブの SSL_Init() がまだ呼び出されていません
-95	SSL 初期化のキー・リングがありません

表 22. その他の SSL 戻りコード (続き)

戻りコード	説明
-96	SSL が使用不可です
-97	指定された暗号の組が無効です
-98	SSL セッションが終了しました
-99	SSL 処理中に不明な、または予期しないエラーが発生しました
-1010	AC2 および IP-SEC の使用時は二重暗号化を使用できません

### 関連タスク

デジタル証明書マネージャーの構成

アプリケーションに対する証明書割り当ての管理

SSL 通信セッションのための公開インターネット証明書の管理

ローカル CA の作成および運用

DCM によるアプリケーションの管理

104 ページの『システム状況の検査』

このトピックでは、システム状況の検査を実行するために学習する必要があるステップをリストします。

### 関連資料

専用 CA 証明書のコピーの取得

## TRCTCPAPP サービス・プログラムの出力

ユーザー・データ・フィールドを Telnet に設定して、VTM コンポーネント・トレースを実行できます。

TCP/IP アプリケーションのトレース (TRCTCPAPP) コマンドの場合、VTM コンポーネント・トレースはスプール・ファイルとして表示されます。このファイルは VTMTRACE と呼ばれ、ユーザー・データのフィールドが TELNET に設定されています。システムはこのファイルを、TRCTCPAPP \*TELNET \*OFF 呼び出しを実行するプロファイルのデフォルトの出力待ち行列に置きます。同時に、すべてのサーバー・ジョブのフライト・レコーダーが、ユーザー・データが QTVnnnnnn. に設定された QTOCTTRC と呼ばれるスプール・ファイルにダンプされます。

以下は、TRCTCPAPP \*OFF 呼び出しを実行するときに対話式ジョブのログに見られる例です。

```

-----+-----
                                コマンド入力                                SYSNAM03
                                                                要求レベル : 1
すべての前のコマンドおよびメッセージ :
> trctcpapp *telnet *off
Spooled printer file 1 opened for output.
  アプリケーション TELNET で形式設定された追跡データ : Spooled VTMTRACE
  user data 'TELNET' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017231' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017230' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017229' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017232' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017233' 。
  アプリケーション TELNET で形式設定された追跡データ : Spooled QTOCTTRC
  user data 'TV017234' 。

```

```

More...
コマンドを入力して、実行キーを押してください。
===>
F3= 終了   F4=プロンプト   F9= コマンドの複写   F10= 詳細なメッセージの除外
F11= 全面的表示   F12= 取消し   F13= 情報援助   F16=システム・メイン・メニュー

```

以下は、デフォルトの出力待ち行列で見られる例です。

```

-----
すべてのスプール・ファイルの処理
オプションを入力して、実行キーを押してください。
1= 送信  2= 変更  3= 保留  4= 削除  5= 表示  6= 解放  7= メッセージ
8= 属性  9= 印刷状況の処理

Opt   ファイル   ユーザー   装置／   ユーザー・   合計   現   コピー
      ファイル   ユーザー   待ち行列 データ   StS   ページ ページ
      VTTRACE   JEFF      JEFFSOUTQ TELNET      HLD   46    1
      QTOCTTRC  JEFF      JEFFSOUTQ TV017231    HLD   4     1
      QTOCTTRC  JEFF      JEFFSOUTQ TV017231    HLD   2     1
      QTOCTTRC  JEFF      JEFFSOUTQ TV017231    HLD   2     1
      QTOCTTRC  JEFF      JEFFSOUTQ TV017231    HLD   2     1
      QTOCTTRC  JEFF      JEFFSOUTQ TV017231    HLD   2     1

オプション 1, 2, 3, のパラメーターまたはコマンド
===>
F3=終了   F10=ビュー 4   F11=ビュー 2   F12=取り消し   F22=印刷装置
F24=キーの続き

```

VTMTRACE というファイルだけが作成されます。 SSL Telnet モードはサーバー上で操作可能で、1つ以上の QTOCTTRC ファイルを持つ場合があります。

以下は、QTOCTTRC ファイルの例です。このスプール・ファイルは、QTVDEVICE ジョブと対照を成す Telnet サーバー・ジョブ (QTVTELNET) です。

```

-----
スプール・ファイルの表示
ファイル . . . . : TV017231   ページ/行 1/6
制御 . . . . .   桁           1 - 78
検索 . . . . .
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
TRCTCPAPP Attributes
Application.....: Telnet Server
Buffer size (KB).....: 0
  (Default of 0 means 16MB buffer)
Trace full action.....: *WRAP
Job id.....: 017231/QTCP /QTVTELNET
Start date/time.....: Fri Dec 11 13:50:33 1998
End date/time.....: Fri Dec 11 14:08:34 1998
Trace buffer wrapped.....: No
Telnet Server Attributes
AutoStart server.....: 'Y'
Number servers.....: 2
Session keep alive timeout...: 0
Default NVT type.....: >*VT100<
Outgoing EBCDIC/ASCII table.: >*CCSID <
Incoming ASCII/EBCDIC table.: >*CCSID <
Coded character set id.....: 84542
Attributes version id.....: >V4R4M0 <
Trace_common buffer structure:
80000000 00000000 161A8753 14001074 |.....g.....| Byte 16

```

```

80000000 00000000 161A8753 14FFFE4 | .....g....U | Byte 48
80000000 00000000 161A8753 14005820 | .....g..... | Byte 80
00FFF000 00000084 F0F1F7F2 F3F1D8E3 | ..0....d017231QT | Byte 112
C3D74040 40404040 D8E3E5E3 C5D3D5C5 | CP QTVTELNE| Byte 144
E340C699 8940C485 8340F1F1 40F1F37A | T Fri Dec 11 13: | Byte 176
F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017 | Byte 208
F2F3F140 |231 | Byte 228
Flight Records:
qvtelnet: Job: QTVTELNET/QTCP/017231
(C) Copyright IBM Corporation, 1999
Licensed Material - Program Property of IBM.
Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Rel: V4R4M0 Vers: V4R4M0 PTR: P3684767
qvtelnet: Program QTVTELNET dated 04 December 1998 running
qvtelnet: Source file: qvtelnet.pIC
qvtelnet: Last modified: Wed Dec 9 11:57:40 1998
qvtelnet: Last compiled at 12:00:10 on Dec 9 1998
qvtelnet: Arguments passed: 1
qvtelnet: Time Started: Fri Dec 11 13:50:34 1998
qvtelnet: sigaction() for SIGUSR1 is EndClientSession()
qvtelnet: Set Telnet Server job identity for OpNav
qvtelnet: Need to setup SSL_Init_Application()
qvtelnet: SSL_Init_Application() successful
qvtelnet: Find Telnet Server control block
qvtelnet: Lock Telnet Server control block
qvtelnet: Open driver to stream
qvtelnet: First Telnet Server Job...

F3= 終了   F12= 取り消し  F19= 左   F20= 右   F24= キーの続き

```

以下は、別の QTOCTTRC ファイルの例です。これは、QTVTELNET サーバー・ジョブと対照を成す、Device Manager のスプール・ファイルです。

```

-----
                        スプール・ファイルの表示
ファイル . . . . . :      TV017230                ページ / 行   1/6
制御 . . . . .      :                               桁           1 - 78
検索 . . . . .      :                               桁           1 - 78
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
TRCTCPAPP Attributes
  Application.....: Telnet Server
  Buffer size (KB).....: 0
                      (Default of 0 means 16MB buffer)
  Trace full action.....: *WRAP
  Job id.....: 017230/QTCP /QTVDEVICE
  Start date/time.....: Fri Dec 11 13:50:33 1998
  End date/time.....: Fri Dec 11 14:08:39 1998
  Trace buffer wrapped.....: No
Telnet Server Attributes
  AutoStart server.....: Y
  Number servers.....: 2
  Session keep alive timeout.: 0
  Default NVT type.....: >*VT100<
  Outgoing EBCDIC/ASCII table.: >*CCSID <
5769TC1 V4R4M0 990521 TRCTCPAPP Output SysName Date-12/11/98 Time-14:08:32 Page-
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...
  Incoming ASCII/EBCDIC table.: >*CCSID <
  Coded character set id.....: 84542
  Attributes version id.....: >V4R4M0 <
Trace common buffer structure:
80000000 00000000 3DA86C25 5F001074 | .....y... | Byte 16
80000000 00000000 3DA86C25 5FFFFFFE4 | .....y..U | Byte 48
80000000 00000000 3DA86C25 5F002F64 | .....y... | Byte 80
00FFF000 00000084 F0F1F7F2 F3F0D8E3 | ..0....d017230QT | Byte 112
C3D74040 40404040 D8E3E5C4 C5E5C9C3 | CP QTVDEVIC| Byte 144
C540C699 8940C485 8340F1F1 40F1F37A | E Fri Dec 11 13: | Byte 176

```

```
F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 |50:33 1998QTV017| Byte 208
F2F3F040 |230 | Byte 228
Flight Records:
qvtvncsh: >>>> entry
(C) Copyright IBM Corporation, 1999.
Licensed Material - Program Property of IBM.
Refer to Copyright Instructions Form No. G120-2083
ProdId: 5769-SS1 Release: V4R4M0 Version: V4R4M0 PTR: P3684767
qvtvncsh: Program QTVTNCSSH dated 04 December 1998 running
qvtvncsh: iActiveLogLevel: 0
qvtvncsh: Source file: qvtvncsh.c
qvtvncsh: Last modified: Wed Dec 9 11:48:33 1998
qvtvncsh: Last compiled at 11:59:42 on Dec 9 1998
qvtvncsh: SignalHandler() registered with signal()
qvtvncsh: Arguments passed: 4
qvtvncsh: argc: 4
qvtvncsh: argv[0]: >QSYS/QTVTNCSSH<
qvtvncsh: argv[1]: ><
qvtvncsh: argv[2]: >lp<
qvtvncsh: argv[3]: >s<
SignalHandler: >>>> entry
SignalHandler: Caught signal SIGSEGV

F3= 終了   F12= 取り消し  F19= 左   F20= 右   F24= キーの続き
```

### 関連概念

『Telnet の問題の報告に必要な資料』

このトピックでは、Telnet の問題を報告する場合にサービス担当者に提供する必要がある情報をリストします。

## Telnet の問題の報告に必要な資料

このトピックでは、Telnet の問題を報告する場合にサービス担当者に提供する必要がある情報をリストします。

IBM に報告する問題には、サービス技術員の判断に応じて、以下の 1 つ以上の資料を含めることができます。

- Telnet サーバーのジョブ・ログ:
  - QTVTELNET ジョブ・ログ
  - QTVDEVICE ジョブ・ログ
- 問題のシナリオに関するいくつかの詳細事項。たとえば、
  - Telnet の接続元または接続先として使用しているリモート・ホストのタイプ (iSeries、zSeries<sup>®</sup>、または pSeries<sup>®</sup> サーバーなど)。この情報が特に役立つのは、カスケードされた Telnet 機能を使用している場合です。
  - Telnet に接続しようとしているクライアントのタイプ (IBM パーソナル・コミュニケーションズや iSeries Access for Windows など)。
- Telnet クライアントを実行している対話式ジョブのジョブ・ログ (Telnet クライアントが調査の対象となっている場合)。
- 障害の生じた対話式ジョブについての、ジョブのトレース (TRCJOB) 出力 (Telnet クライアントを実行している場合には特に重要)。

注: このトレースを開始するには、TRCJOB \*ON を使用します。その結果は、対話式ジョブ内の QPSRVTRC スプール・ファイルとなります。

- TCP/IP データのみを含む、障害に関する通信トレースを ASCII および EBCDIC の両方でフォーマットした資料。サービス技術員は、このトレース内にブロードキャスト・メッセージを含めるように指示することがあります。さらに、ネットワーク上に大量のトラフィックがあり、障害の生じたクライアントの IP アドレスが判明している場合、その特定の IP アドレスでトレースをフィルター操作しなければならないこともあります。
- 障害が生じた時点以後の、メジャー・コードが 0700 でマイナー・コードが 005x のライセンス内部コード (LIC) ログ。さらに、メジャー・コードが 0701 でマイナー・コードが 005x の LIC ログも、情報として役立つことがあります。必ずしも重要ではありません。
- 仮想端末管理機能 (VTM) LIC コンポーネント・トレース。このトレースを取得するには、TCP/IP アプリケーションのトレース (TRCTCPAPP) コマンド、またはシステム・サービス・ツールの開始 (STRSST) コマンドを使用します。TCP/IP アプリケーションのトレース (TRCTCPAPP) コマンドの使用方法に関する詳細は、TRCTCPAPP コマンドの説明を参照してください。

VTM LIC トレースを実行すると、パフォーマンスに影響が生じます。このコマンドを使用例のいくつかを、以下に示します。

- すべての VTM 活動をトレースするには、以下のようになります。  
TRCTCPAPP APP(\*TELNET) SET(\*ON)
- 装置名が判明しているとき、特定の装置上の活動をトレースするには、以下のようになります。  
TRCTCPAPP APP(\*TELNET) SET(\*ON) DEVD(devicename)
- クライアントの IP アドレスが判明しているとき、特定の装置上の活動をトレースするには、以下のようになります。  
TRCTCPAPP APP(\*TELNET) SET(\*ON) RMTNETADR(\*INET'www.xxx.yyy.zzz')
- トレースをオフにして、ファイル出力をスプールするには、以下のようになります。  
TRCTCPAPP APP(\*TELNET) SET(\*OFF)

注: このコマンドを実行する前に、問題に対してどのトレース・パラメーターを使用するかに関する詳細な指示を、サービス技術員から受けてください。これにより、問題に対して適切な情報を収集することができます。

#### 関連概念

108 ページの『TRCTCPAPP サービス・プログラムの出力』  
ユーザー・データ・フィールドを Telnet に設定して、VTM コンポーネント・トレースを実行できません。

## 自動生成される診断情報

Telnet サーバー・エラーの中には、自動的に診断情報を生成するものがあります。このセクションでは、その情報を検索する方法について説明されています。

Telnet サーバー内で特定のエラーが生じた場合、いくつかの診断情報が自動的に生成されることがあります。サービス技術員は Telnet サーバーの問題を適切に分析するために、この情報を必要とすることがあります。

Telnet または Device Manager のジョブが初期障害データ捕そく機能 (FFDC) エラーによって失敗した場合、WRKSPLF QTCP プロファイルの下にスプール・ファイルが見つかります。ジョブが FFDC エラーによって失敗した場合、失敗したジョブごとに 2 つのダンプが生成されます。1 つは DSPJOB \*PRINT を呼び出して作成されるダンプであり、もう 1 つは DSPJOBLOG \*PRINT を呼び出して作成されるダンプです。この方法により、ジョブ・ログおよびジョブ実行属性の両方をダンプして、ユーザー・データ・グ



ループおよびジョブ番号 ID の両方の出力を取得することができます。その結果、VTM コンポーネント・トレース出力と突き合わせることが可能になります。

合計 4 つのスパール・ファイルが見つかります。QTVTELNET ジョブのものが 2 つと QTVDEVICE ジョブのものが 2 つです。システムが FFDC エラーを検出すると、これらのスパール・ファイルが自動的に生成されます。以下の図に例を示します。

すべてのスパール・ファイルの処理

オプションを入力して、実行キーを押してください。

1=送信   2=変更   3=保留   4=削除   5=表示   6=解放   7=メッセージ  
8=属性   9=印刷状況の処理

OPT	ファイル	ユーザー	装置/ 待ち行列	ユーザー・ データ	ページ Sts	現 数	ページ HLD	コピー
	QPJOBLOG	QTCP	QEZJOBLOG		TV016868		HLD	4
	QPDSPJOB	QTCP	QPRINT		TV016868		HLD	7
	QPJOBLOG	QTCP	QEZJOBLOG		TV016955		HLD	3
	QPDSPJOB	QTCP	QPRINT		TV016955		HLD	7
	QPJOBLOG	QTCP	QEZJOBLOG		TV017231		HLD	3
	QPJOBLOG	QTCP	QEZJOBLOG		TV017232		HLD	3
	QPDSPJOB	QTCP	QPRINT		TV017232		HLD	7
	QPDSPJOB	QTCP	QPRINT		TV017231		HLD	7

オプション 1, 2, 3, のパラメーターまたはコマンド  
===>


F3=終了   F10=ビュー 4   F11=ビュー 2   F12=取り消し   F22=印刷装置  
F24=キーの続き

図 10. 「すべてのスパール・ファイルの処理」画面




## Telnet の関連情報

- | ここにリストされているものは、Telnet のトピックに関連する IBM Redbooks™ (PDF 形式) および Web
- | サイトにあります。どの PDF も表示または印刷可能です。

### IBM Redbooks

- **V4 TCP/IP for AS/400 : More Cool Things Than Ever**  (約 700 ページ) TCP/IP に関する広範囲にわたる情報を提供します。一般的なソリューションを例示するサンプル・シナリオと構成例も含まれています。

### Web サイト


- **Internet Engineering Task Force (IETF) Web サイト**  RFC 2877 5250 Telnet 機能拡張 (RFC 2877 5250 Telnet Enhancements)  などの Request for Comments (RFC) をご覧いただけます。
- **Internet Assigned Numbers Authority (IANA)**  には共通のポート番号割り当てに関する情報が示されています。

## PDF ファイルの保存

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

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. PDF をローカルに保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「保存」をクリックする。

## Adobe Reader のダウンロード

- | これらの PDF を表示または印刷するには、Adobe Reader がご使用のシステムにインストールされている
- | 必要があります。これは、Adobe Web サイト ([www.adobe.com/products/acrobat/readstep.html](http://www.adobe.com/products/acrobat/readstep.html))  から無料で
- | ダウンロードできます。

---

## コードに関するライセンス情報および特記事項

IBM は、お客様に、すべてのプログラム・コードのサンプルを使用することができる非独占的な著作使用权を許諾します。お客様は、このサンプル・コードから、お客様独自の特別のニーズに合わせた類似のプログラムを作成することができます。

- | 強行法規に反する場合を除き、IBM、「プログラム」開発者および IBM ビジネス・パートナーは「プログラム」を特定物として現存するままの状態を提供し、「プログラム」または技術サポート (提供される場合) について、法律上の瑕疵担保責任を含め、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証を含む明示もしくは黙示のいかなる保証責任も負わないものとします。
- | いかなる場合においても、IBM、「プログラム」開発者および IBM ビジネス・パートナーは、その予見の有無を問わず発生した以下の損害については賠償責任を負いません。
- | 1. データの喪失、または損傷
- | 2. 直接損害、特別損害、付随的損害、間接損害、または経済上の結果的損害
- | 3. 逸失した利益、ビジネス上の収益、あるいは節約すべかりし費用
- | 国または地域によっては、法律の強行規定により、上記の責任の制限が適用されない場合があります。

---

## 付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、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、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

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

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

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

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

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認できません。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をお願いします。

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。

---

## プログラミング・インターフェース情報

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

---

## 商標

以下は、IBM Corporation の商標です。

- | AIX
- | AS/400
- | eServer
- | IBM
- | iSeries
- | i5/OS
- | OfficeVision
- | OS/2
- | pSeries
- | Redbooks
- | System/370
- | zSeries

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

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

---

## 資料に関するご使用条件

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

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

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

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

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

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

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、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。









Printed in Japan