

# LANSA コミュニケーションセットアップガイド (LANSA ワークステーション製品)

- [始めに](#)
- [ワークステーションの構成](#)
- [IBM i の構成](#)
- [Linux の構成](#)
- [通信エラーコード](#)
- [複数のリスナー・ジョブを実行する](#)
- [トラブルシューティング](#)

エディション日付: 2013年2月18日

© 2013 LANSА

## 1. 始めに

1.1 LANSAX通信エクステンションとは？

1.2 ソフトウェア要件

1.3 暗号化の利用

1.4 コンポーネント

1.5 設定の概要

1.6 Lroute.dat の拡張機能

注: このLANSAX通信機能を利用するために現在の LANSAX機能や I/O モジュールを変更する必要はありません。

既存の LANSAX 通信ユーザーは「[1.6 Lroute.dat の拡張機能](#)」を参照して下さい。

## 1.1 LANSA通信エクステンションとは？

LANSAの通信エクステンションは、IMB i、WindowsやLinusのホストへの通信方法としてTCP/IP（ソケット）を使用することを可能にします。これらのエクステンションは、APPCインターフェースを経由してソケット・インターフェースにアクセスすることにより、LANSAワークステーション製品に対して、ネイティブなTCP/IPソケットのサポートを提供します。

ホスト上では、これらのエクステンションは、要求されたトランザクション・プログラム（TP）を呼び出し、呼び出されたTPをクライアントによって提供されるユーザー名とパスワードのもとで実行します。そのことによって、クライアントの接続要求を処理するための"ソケット・リスナー"を提供します。ホスト上では、各トランザクション・プログラムは、それぞれのジョブを実行します。これは、セッション・ジョブと言われています。

リスナーは暗号化を可能にすることで通信回線の機密保護の有無を決定できます。省略値は暗号化しないに設定されています。この設定は「[機密密保護設定](#)」に説明されている暗号化アルゴリズムのひとつを選択することによって変更できます。

## 1.2 ソフトウェア要件

### **IBM i**

TCP/IPサポートは、i5/OS によって提供されています。IBMのドキュメントに掲載されている手順に従ってTCP/IPを構成し、STRTCPコマンドを使用してTCPを開始してください。

### **ワークステーション・クライアントおよびホスト**

MS Windows のインストール時にTCP/IPをインストール、構成できます。インストールが終了したら、ワークステーションからホストに"ping"を実行し、その構成をテストしてください。このpingユーティリティは全てのTCP/IPのインプリメンテーションで提供されているもので、2つのノード間のエコー・テストを実行します。

### **Linux**

全てのバージョンのLinux でTCP/IP サポートが提供されています。

## 1.3 暗号化の利用

LANSA通信エクステンションは暗号化アルゴリズムの選択を可能にし、クライアントとホスト間のデータ伝送の暗号化を行ないます。

暗号化アルゴリズムの選択はリスナー・レコード構成内で行ないます。詳細については「LANSA/AD ユーザーガイド」内の「LANSA通信エクステンション・リスナー・レコード」を参照してください。

注: 暗号化アルゴリズムが選択された場合、リスナー・ジョブは選択された暗号アルゴリズムをサポートするクライアントからの要求のみ受け付けます。

暗号化をサポートしないLANSA通信エクステンション（バージョン1.x）以前のバージョンがクライアントにある場合は\*NONEを選択しているクライアントからの接続要求のみ受け付けます。

暗号化データは速度や処理資源の使用に影響を与えます。機密保護要件に関連して速度と機密保護のトレード・オフを行う必要があります。ホストへの暗号および非暗号接続が出来るようにする場合は、ふたつのリスナー・ジョブを構成してください。方法については「[複数のリスナー・ジョブを実行する。](#)」を参照してください。

### バージョンの互換性

暗号化機能を使用する場合は、クライアントおよびホストが同一バージョンのLANSA通信エクステンションを実行しなければなりません。バージョン9.0かそれ以降。

暗号化以前のバージョンで実行しているクライアントは暗号化可能ホストを暗号化不可の状態にすることで接続できます。（バージョン9.0かそれ以前）

バージョン9.0以前のバージョンで実行しているクライアントが暗号化可能のホストに接続を試みた場合、接続要求は拒否されホストに診断メッセージがロギングされます。

暗号化可能バージョンを実行しているクライアント（バージョン9.0かそれ以降）がバージョン9.0以前で実行中のホストに接続を行おうとする場合、ホストは要求を拒否します。そしてクライアントはバージョン9.0以前の要求を使用して接続するよう要求します。またIBM i ホスト上に接続要求が成功しない旨のジョブログが作成されます。これを避けるには

ホストをバージョン9.0にアップグレードしてください。

## 1.4 コンポーネント

### ホスト・コンポーネント

ホスト上でこれらのエクステンションをサポートするメイン・プログラムは、以下のとおりです：

	<b>IBM i</b>	<b>Visual LANSA</b>	<b>Linux</b>
リスナー	LCOLIST	LCOLIST.EXE	プログラム ライブラリ lcolist
トランザクション・プログラム・エン트리	LCOTP	LCOTP.EXE	プログラム ライブラリ lcotp
CPIC マネージャ	LCOMGR40	LCOMGR32.DLL	Lcomgr shared library
ソケット IPC	LCOSCK40	LCOSCK32.DLL	lcosck shared library
通信ルーティング・サポート	LCOCROUT	N/A	N/A
アドミニストレーション	LANSA CONFIGURE	LCOADM32.EXE	N/A
DES	LCOEDES	LCOEDES.DLL	
TWOFISH	LCOETWF	LCOETWF.DLL	

これらのプログラムは、リモート・セッション・リクエストをサポートするCS Builder/サーバー・プログラムによって使用されます。TCP/IPを実行するために、既存のLANSAファンクションおよびI/Oモジュールを変更する必要はありません。

リスナー・プログラム (LCOLIST) は、指定されたポート番号あるいはパイプでリモート・セッションからの接続要求を待つコンポーネントです。リスナーは、接続要求を受け取ると、セッション・ジョブへ接続を転送します。そのエン트리・ポイントは、トランザクション・プログ

ラム・エントリー (LCOTP) です。通信レイヤーは、CPICマネジャ、IPCモジュール、IBM i 上では通信ルーティング・サポート (COCROUT) によって提供されます。

## ワークステーション・コンポーネント

クライアント・ワークステーション上のコンポーネントは、アドミニストレーション・ユーティリティ、すなわち、APPCインターフェースDLL (CPICマネジャ) とWindowsソケット (Winsock) のインターフェースDLL (IPCモジュール) から構成されています。これらのモジュールは、LANSAのセットアップの間にインストールされます。

32ビットWindows上でのこれらのモジュールのファイル名は、以下のとおりです：

アドミニストレーション・ユーティリティ	LCOADM32.EXE
CPIC マネジャ	LCOMGR32.DLL
ソケット IPC モジュール	LCOSCK32.DLL
DES 暗号化アルゴリズムモジュール	LCOEDES.DLL
TwoFish 暗号化アルゴリズム	LCOETWF.DLL

## 1.5 設定の概要

### IBM i ホストでのTCP/IP 設定

1. IBM i TCP/IP のソフトウェアを構成する。
2. ワークステーションのTCP/IP ソフトウェアをインストールし、構成する。
3. IBM i TCP/IP のパラメータを指定する。
4. ワークステーションの通信エクステンションのパスとオプションを指定する。

### Visual LANSA ホストでのTCP/IP 設定

1. TCP/IP のソフトウェアをクライアントとホスト両方にインストールし、構成する。
2. ホストでワークステーションの通信エクステンションのリスナーオプションを指定する。
3. ワークステーションの通信エクステンションのパスとオプションをクライアントとホスト両方で指定する。

### Linux ホストでのTCP/IP 設定

1. TCP/IP をLinux サーバーで構成する。
2. ワークステーションのTCP/IP ソフトウェアをインストールし、構成する。
3. ホストで通信エクステンションのリスナーオプションを指定する。
4. ワークステーションの通信エクステンションのパスとオプションをクライアントで指定する。

## 1.6 Lroute.dat の拡張機能

新しいユーザーはこのメモを読む必要はありません。

LANSA V10.7以降、以前はlroute.datファイルにあったリスナーレコードがListen.datという新しいファイルから読み込まれます。lroute.datからリスナーレコードを取り除いたことにより、全てのLANSA構成でlroute.datファイルを共有できるようになりました。（それぞれの構成ごとに独自のポート番号を持つListen.datのコピーをして下さい）

下位互換性を保つために、リスナーレコードはlroute.datからは削除されません。

Listen.dat という新しいファイルはLANSAのインストールもしくはアップグレードの際に作成されます。

複数の構成 – クライアント / サーバー

以下の例にも示されている通り、クライアントとサーバーの構成とバージョンにより、lroute.datの要求が若干異なります。

LANSA v 10.7 以降のバージョンでは、クライアントとサーバーの両方からそれぞれのLANSA構成のLroute.datを共有できます。

LANSA V10.7 以前のバージョンでは、Lroute.dat ファイルは全ての構成で共有することが可能でしたが、リスナーはいずれの時でも1つしか実行できませんでした。

クライアント PC

この例ではクライアントPC側で全ての構成およびバージョンで同じlroute.datを共有することが可能です:

```
LANSAV10\Connect
  \Open
  \LANSA
  \X_WIN95
LANSAV10_7\Connect
  \Open
  \LANSA
  \X_WIN95
LANSAV9\Connect
  \LANSA
  \X_WIN95
LANSAclient\Connect
```

## サーバー PC

サーバー側では全ての構成およびバージョン間でroute.dat を共有出来るわけではありません。以下の例では、全てのV10.7以前のバージョンのサーバーが同時に実行されていますが、それぞれの構成には独自のroute.dat が必要です。

V 10.7以降のバージョンのみが1つのroute.dat を何のコンフリクトもなく共有することが可能です。

**LANSAV10\Connect**

**\Open**

**\LANSA**

**\X\_WIN95**

**LANSAV10\_7\Connect**

**\Open**

**\LANSA**

**\X\_WIN95**

**LANSAV11\Connect**

**\Open**

**\LANSA**

**\X\_WIN95**

**LANSAV9\Connect**

**\LANSA**

**\X\_WIN95**

## 複数の Web インスタンス (マルチホーミング)

このroute.dat の変更によりISAPI プラグインの構成に問題が起こることはありません。これは1つのシステムにアクティブなISAPI プラグインのコピーは1つしかないからです。ISAPI プラグインはLANSA通信エクステンションのクライアント側にあり、他の構成と共にシステム上でroute.dat を共有する、もしくはISAPI 構成の接続ディレクトリの中で独自のroute.dat を持つことも可能です。

## 2. ワークステーションの構成

LANSAコミュニケーション管理機能はワークステーション構成を指定したり、必要に応じログやトレース機能のオン・オフの設定をします。

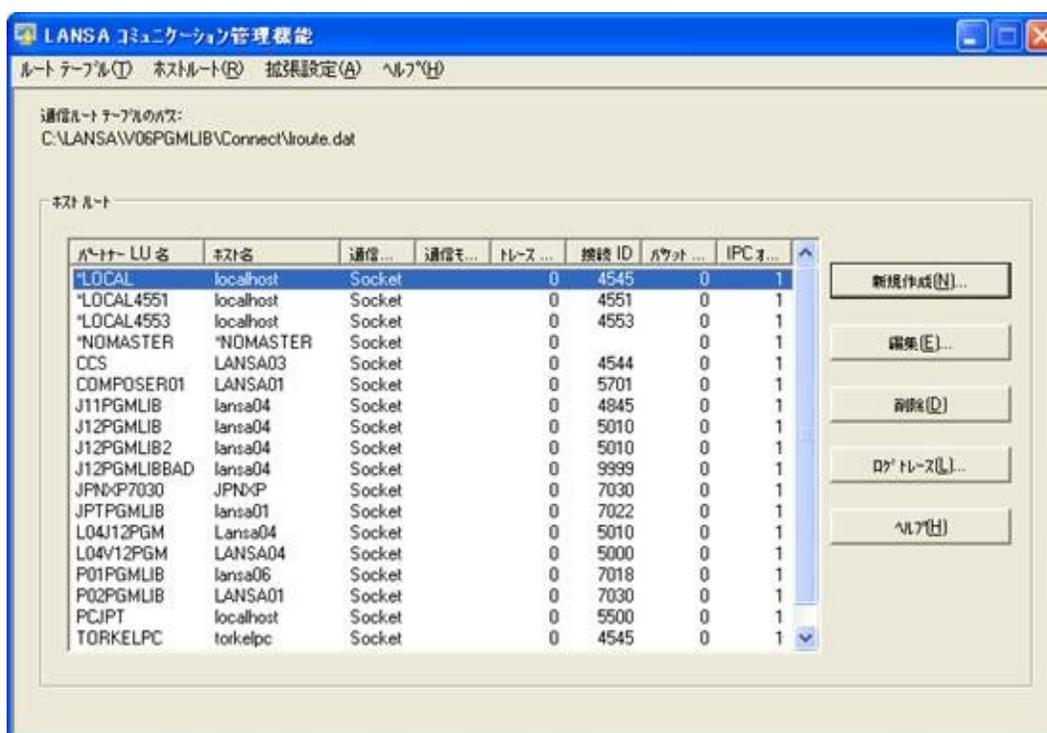
LANSA OpenあるいはVisual LANSАのインストールの際に、[LANSA通信エクステンション]のオプションを選択すると、LANSA通信エクステンション管理機能ユーティリティがインストールされます。最初のインストールの際にこのオプションを選択しなかった場合は、LANSAのインストールを行い、上記のステップを再度行うことでインストールすることができます。

このコミュニケーション管理機能は、クライアント・システムとVisual LANSАホスト・システムの両方で使用されます。

## 2.1 LANSACOMMUNICATIONS管理機能を開始する

LANSACOMMUNICATIONS管理機能を開始するには、[LANSACOMMUNICATIONSプログラム・グループ]あるいは[スタート]メニューから[LANSACOMMUNICATIONS管理機能]のアイコンを選択してください(LCOADM16.EXEあるいはLCOADM32.EXEが実行されます)。

LANSACOMMUNICATIONSエクステンションを使用するには、接続したい1つのホストあるいは複数のホストへのルートを定義する必要があります。この情報は、通信ルートテーブル・ファイル(route.dat)に保管されます。このタスクは管理機能のメイン・ウィンドウから始めます。



### [通信ルートテーブルのパス]

使用される通信ルートテーブルのパス名です。

### [ホストルート]

管理機能のメイン・ウィンドウには今まで設定されたホストルートのリストもしくは新しくLANSACOMMUNICATIONSをインストールした場合は省略値のホストルートが表示されます。

ホストルート情報を新たに追加するもしくは修正するには、管理機能のメイン・ウィンドウで、以下に示された該当するボタンを選択してください。

### [新規作成(N)]

「[2.2 ホストルートの追加あるいは変更](#)」に説明されているホストまたはルートを追加するためのホストルート情報のウィンドウを開きます。

### [編集(E)]

変更するルートを反転表示させて選択し、[編集(E)]ボタンを押してください。詳しくは「[2.2 ホストルートの追加あるいは変更](#)」を参照して下さい。

### [削除(D)]

削除したいホストまたはルートを反転表示させて選択し、[削除(D)]ボタンを押してください。

### ログとトレース

どのようにしてログやトレースを開始するかは、ログやトレースしたい内容によります。以下のどちらかになります。

- ホストルート - リストの中からルートを反転表示させて選択し、[ログとトレース] ボタンを押します。詳細は「[2.7 ログとトレースのオプション設定](#)」を参照して下さい。

または:

- モジュール - [拡張設定]メニューから [モジュール ログとトレース ...] を選択します。モジュールを監視するには、「[2.4 モジュールのログおよびトレース](#)」を参照して下さい。

## 2.2 ホストルートの追加あるいは変更

メインウィンドウで[新規作成(N)]あるいは[編集(E)]のボタンを選択すると、以下の画面が表示されます。



省略値のTCPホスト名とポート番号をペアフォーマットで利用している場合、このホストルート情報ダイアログ・ボックスで作成されるルートレコードは必要ありません。

ホスト名の省略値はlocalhost、ポート番号は4560です。(ホスト名はlocalhost:4560と設定するだけで呼び出せます。)

省略値のホストルートを使用していない場合は、このダイアログ・ボックスでオプションを引き続き設定して下さい。:

[TCPホスト名/ポートアドレスに、生成されたLU名を使用してください。]

TCPホスト名 /ポート番号のペアフォーマットで生成されたLU名を利用する場合はこのオプションを選択して下さい。

[パートナー LU名]

接続先のホスト名。LANSA Openでは、LceUseSystemの呼び出しで使用される名前です。

ヒント

IBM i システムを定義する場合は、2つの異なるパートナーLU名で定義しておくとも時間の節約になるかもしれません。例えば、IBM i のLU名がMYHOSTだとすると、MYHOSTおよびAPPN.MYHOSTというLU名で定義しておきます。この2つのエントリーは、名前以外の全ての面において同一のものであります。このアプローチを使用することによって、アプリケーションは、短い名前MYHOSTともっと正式な名前APPN.MYHOSTの両方を使用することができます。例えば、Visual LANSAのホスト・モニターは、常に正式名称であるAPPN.MYHOSTを使用します。ですから、この正式名称を指定しておかないと、Visual LANSAのホスト・モニターをスタートさせることができません。一方で、短い名前MYHOSTも使用できるようにしておけば、他のアプリケーションを使用する際、覚えやすいというメリットがあります。

#### [ホスト名 (アドレス)]

通信方法が必要とするフォーマットで表現されたホストへのアドレス。

これは、同じドメインのホストに対する単純なホスト名（上図において示されているように"ホスト・ドメイン名"というフルパス指定）です。IPアドレスでは、nnn.nnn.nnn.nnnというフォーマットになります。名前が指定される際、（IPアドレスに対する）名前の分析は、基礎となるTCP/IPプロトコル・スタックによって行われるということに注意してください。このため、TCP/IPプロトコル・スタックに関する知識が必要です。

Named Pipeは、Windows NTホストのコンピュータ名です。

#### [通信手段]

現在のところ、以下のオプションのみが有効です：

- Socket

#### オプション

以下のオプションを空白にしておくと、省略値が適用されます。

#### [接続ID]

標準ではないポート番号を提供するため、TCP/IPソケットで使用するものです。ホスト上のリスナー・コンポーネントも、このポート番号上で使用できるよう構成されていなければなりません。省略値は4545です。

#### [通信モジュール]

ブランクにしておいてください。

APPCパス・スルーを使用している場合は、APPCへの呼び出しを処理するDLL名を指定してください（例：Microsoft SNA Server 16ビットに対しては、WINCPIC.DLL。Microsoft SNA Server 32ビットに対しては、WCPIC32.DDL）。

#### [Maxl\_Field(パケット・サイズ)]

内部的に使用される送信バッファの大きさを決定することによって、APPCパケットの大きさをシミュレートします。省略値は、1024+ヘッダー・サイズです。このパラメータを省略値のままにしておき、特殊な状況に対する構成はネットワークの専門家に設定してもらうことをお勧めします。

#### [TCP\_NODELAY TCP/IP ソケットオプション]

ネーグルのアルゴリズムを無効にし、小さなデータパケットをリモートホストにすぐに送ることができます。

ネーグルのアルゴリズムでは複数の送信要求を小さなデータバッファ内に結合させ、前回のデータ・パケット送信が受信されたとのリモートホストからの確認をした後に送信します。これはTCP/IP ソケットの省略値として有効になっています。

LANSA 通信エクステンションは独自のデータバッファを導入しているため、このネーグルのアルゴリズムは必要ありません。

#### [Ipv6 を使用する]

インターネットプロトコルVersion 6 のサポートを有効にするためにはこのオプションを選択して下さい。このオプションにより、IPv4 と IPv6 の両方のネットワークでアプリケーションが作動できるようになります。

注: IPv6 はWindows XP/2003 以降のバージョンでのみサポートされません。

#### lroute.dat ファイルを生成

入力が全て終了したら、OK ボタンを押して下さい。lroute.dat ファイルが生成されます。

lroute.dat ファイルは絶対に手動で変更しないで下さい。変更が必要な場合は、このダイアログ・ボックスを利用して下さい。

## 2.3 Visual LANSAリスナーの構成

Visual LANSAをインストールする際、Visual LANSAサーバー・システムのインストールを選択し、通信方法としてTCP/IPを選択した場合は、"LConnect Services"という名前の通信エクステンション・リスナーが（Windows serviceとして）インストールされます。

このサービスがシステム上にインストールされると、管理機能ユーティリティにおいて、[拡張設定]メニューの下にサブメニュー[リスナー(L)...]が追加されます。

このオプションを選択することにより、Visual LANSAシステム上で、リスナー・サービスを開始および停止することができるようになります。リスナーは、接続するワークステーションに対して実行されている必要があります

[拡張設定]メニューから[リスナー(L)...]を選択すると、以下のようなダイアログ・ボックスが表示されます。



### [リスナー開始/停止]ボタン

通信手段を選択し、このボタンを押すとWindows serviceとして実行されているリスナー（LConnect Services）を開始または停止できます。ウィンドウのタイトル・バーには、このサービスが現在実行されているか、停止されているかが表示されます。

このリスナーの詳細を変更するには「[\[リスナーの通信手段の選択\]](#)」を参照して下さい。

#### [ログトレース]ボタン

トレースやログのどちらか一方または両方を使用可能あるいは使用不可にするには、このボタンを選択してください。詳細については、まず初めに「[2.4 モジュールのログおよびトレース](#)」、次に「[2.7 ログとトレースのオプション設定](#)」を参照して下さい。

#### [機密保護]ボタン

このボタンを選択して、使用可能、使用不可、または暗号化を選択してください。詳細は「[2.5 機密保護設定](#)」を参照してください。

#### [WDTM 設定]ボタン

Windows デスクトップヒープ管理 (Windows Desktop Heap Management) 設定画面 ([2.6 WDTM 設定](#)) にアクセスする場合はこのボタンを押して下さい。これはWindows サーバー上で実行されるweb ジョブやLANSA Open のセッションの数をコントロールするものです。

#### [リスナーの通信手段の選択]

リスナーに関する詳細を変更する場合は、適切な方法をリストから選択し、以下の内容を入力して下さい。

#### [リスナーのスレッド数]

この数は、接続要求をサポートするために、リスナーが開始するスレッドの数を決定するものです。通常は、1か2で十分ですが、負荷が重い場合は、もっと増やすこともできます。ブランクあるいは0の場合は、この通信方法は接続要求を受け取りません。

#### [オプション]

次のオプションがブランクの場合は省略値が使用されます。

#### [接続ID]

標準ではないポート番号を提供するため、TCP/IPソケットで使用するものです。ホスト上のリスナー・コンポーネントも、このポート番号上で使用できるよう構成されていなければなりません。省略値は4545です。

#### [通信モジュール]

ブランクにして下さい。このオプションは将来の使用のために留保されています。

#### [TCP\_NODELAY TCP/IP ソケットオプション]

ネーグルのアルゴリズムを無効にし、小さなデータパケットをリモート

ホストにすぐに送ることができます。

ネーグルのアルゴリズムでは複数の送信要求を小さなデータバッファ内に結合させ、前回のデータ・パケット送信が受信されたとのリモートホストからの確認をした後に送信します。これはTCP/IP ソケットの省略値として有効になっています。

LANSA 通信エクステンションは独自のデータバッファを導入しているため、このネーグルのアルゴリズムは必要ありません。

### **[IPv6を使用する]**

インターネットプロトコルVersion 6 のサポートを有効にするためにはこのオプションを選択して下さい。このオプションにより、IPv4 と IPv6 の両方のネットワークでアプリケーションが作動できるようになります。

注: IPv6 はWindows XP/2003 以降のバージョンでのみサポートされません。

### **[SO\_KEEPALIVE TCP/IP ソケットオプション]**

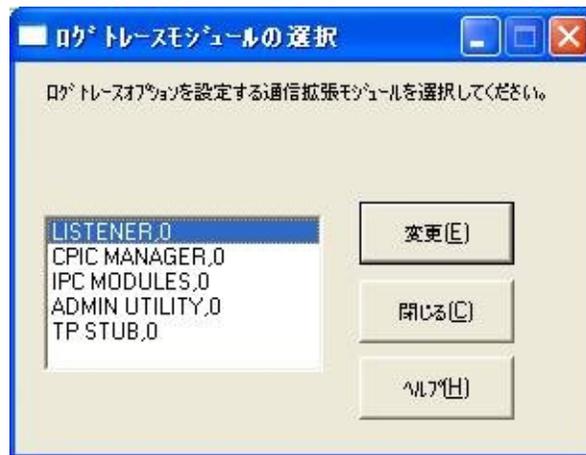
TCP/IP ソケットのオプションをキープアライブにするためにはこのオプションを選択して下さい。

アプリケーションによってはTCP/IPのプロバイダーにソケットオプションをSO\_KEEPALIVE にしてTCPの接続をキープアライブパケットが有効な状態にするよう要求する場合があります。このキープアライブオプションの結果、接続が切れた場合はソケットで進行中の全ての要求に対してエラーコードWSAENETRESET が戻されます。またそれに続く要求は全てWSAENOTCONN となります。

## 2.4 モジュールのログおよびトレース

ログとトレースのオプションに関する詳細は、「[2.7 ログとトレースのオプション設定](#)」を参照してください。

メイン・ウィンドウからモジュールのログとトレースを開始するには、管理機能メイン・ウィンドウの[拡張設定]メニューから[モジュール ログ トレース ...]を選択してください。



ログ・トレースモジュールの選択のダイアログ・ボックスのウィンドウにリストアップされているモジュールから、ログあるいはトレースを実行するモジュールを選択してください。

クライアントのワークステーションに対して有効なオプションは、以下のとおりです：

- CPIC MANAGER
- IPC MODULES
- ADMIN UTILITY.

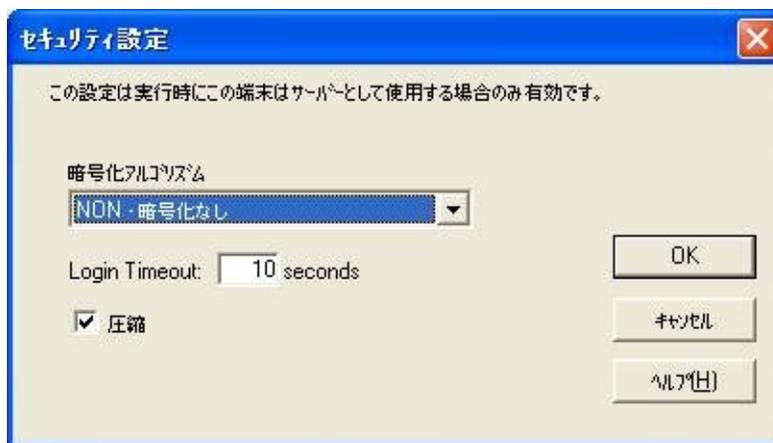
このリストにおけるその他のオプションは、リスナーを使用する際、ホストが使用するためのものです。

[変更(E)]を選択すると、[ログ・トレース情報]画面が表示されます。

注：IBM i のログおよびトレース機能は、『LANSA/AD ユーザーガイド』にある通り、IBM i 上で構成されています。この機能とは関係ありません。

## 2.5 機密保護設定

リスナー情報ダイアログ上の[機密保護]ボタンを押すと、このダイアログが開きます。（リスナー情報ダイアログにたどり着くには、管理機能メイン・ウィンドウの[拡張設定]メニューから[リスナー]を選択します。）。LANSA通信エクステンションのサーバー側は通信回線が機密保護か非機密保護回線を判断します。



### [暗号化アルゴリズム]

暗号化アルゴリズムは、転送データを暗号化するために使用されます。オプションは以下の通りです。

- NON - 暗号化なし。LANSA通信エクステンションの以前のリリースと互換性があります。
- DES ( Data Encryption Standard algorithm ) - 標準の暗号化 (DES )。データ暗号化標準アルゴリズム。この標準は1981年にANSIによって適用されました。DESはブロック暗号で、64ビット・ブロックを暗号化します。キーの長さは64ビットです。
- TWF ( Twofish cryptographic algorithm ) - Twofish 暗号化アルゴリズム (TWF)。TWOFISHは128ビット・ブロック暗号です。可能なキーの長さは、128、192、256ビットです。しかしながら、アメリカの制限の影響でLANSAでは128ビットのキーのみ使用します。TWOFISH暗号アルゴリズム。Advanced Encryption Standard ( AES、高度暗号化標準 ) として知られる新しい暗号化標準の最後の5項目のうちの1つです。この標準はNIST ( National Institute of Standards and Technology ) によって紹介されました。©Counterpane Internet Security Inc

### [圧縮]

このオプションを選択して、接続中の圧縮可能および圧縮不可を指定し

ます。

暗号化や圧縮アルゴリズムを使用すると、通信セッションにおいて、より多くのCPUサイクルが消費されます。

## 2.6 WDTM 設定

Windows デスクトップのヒープ管理 (Windows Desktop Heap Management, WDTM) 設定はWindows サーバーのオペレーションの性能をコントロールし、負荷が大きい場合のサーバーシステムの動きを細かく調整するために利用されます。この設定はWindows システム全体に影響を及ぼし、Windows データ/アプリケーションサーバーに接続している時のみ有効です。

この設定は通常修正する必要はありません。もし修正が必要な場合はWindows のパフォーマンスや安定性に影響を及ぼす場合があります。  
変更をする場合は必ず権限を与えられたWindows 管理者が行って下さい。また以下の注意事項を読み、理解してから行ってください。



**Windows デスクトップのヒープ管理に関する重要事項:**

忘れないで下さい: Windows デスクトップヒープ管理のパラメータは Windows システム全体に影響を及ぼします。通常は変更する必要はありません。

出荷時の省略値では合計約800個のWeb ジョブまたはLANSA Open

(V10.0 またはそれ以降のバージョン) のセッションのが同じWindows システム上で同時に実行できるようになっています。ほとんどの場合それ以上のWeb ジョブまたはLANSA Open のセッションを実行する必要はありません。もし変更が必要な場合は、必ずWindows の管理者が管理者グループのアカウントでログインして行って下さい。また事前に現地のLANSA 代理店に連絡して下さい。

これらのパラメータは ( LANSA for the Web アドミニストレータの同時ユーザー最大値設定とは違って ) 同じWindows システム上で実行されるWeb ジョブやLANSA Open セッション の上限を強いるものではありません。Web ジョブを800 以下に制限する場合は、Web アドミニストレータの最大同時ユーザー数設定を利用して下さい。

デスクトップヒープパラメータは実行中のWeb ジョブとLANSA Open セッションの数が示された制限より少ない場合、つまり省略値の時はWindows システム上のWeb ジョブまたはLANSA Openセッションの同時実行数が合計約800個未満の時にシステムの安定性を高めるために設計されました。これはWindows システムが主に実行中のWeb ジョブとLANSA Open セッション専用のものであれば、システムの安定性に深刻な影響を与えることはありません。Web ジョブとLANSA Open セッションの数がその数に達し、さらに別の要求がなされた場合、Visual LANSA (v10.0 以降のバージョン) はその要求を処理し、さらに多くのWeb ジョブやLANSA Open セッションを作成しようとします。(最大同時ユーザー設定で許可されているので) こういった場合にシステムリソースが低くなり、システムの安定性が損なわれる恐れがあります。

Windows システムが省略値の制限以上のWeb ジョブやLANSA Open セッションを実行できる性能のものであれば、(以下に示されている負荷限界の計算で決定されます) このパラメータを変更することによりシステムの安定性を高めることができます。省略値の800やそれ以下のWeb ジョブやLANSA Open セッションをかるうじて実行できるようなWindows システムの場合は、制限値を増やしたとしても、より多くのWeb ジョブやLANSA Open セッションを確実に実行させることを保証するものではありません。反対にこの場合は、制限値と最大同時ユーザー設定を下げるによりシステムの安定性を高めることができます。

#### 負荷制限の計算

同時に実行できるWeb ジョブとLANSA Open セッションの実際の数ハードの構成やアプリケーションに依存しています。パラメータを変更する前にまずWindows システムに最も最適な負荷制限を計算する必要があります。

実際の推定負荷制限を決める際には外的要因も考慮にいれなければなりません。例えばWindows システムでWindows バッチジョブを実行している場合、この制限テストを行う際にはそれらのジョブもアクティブな状態でなければなりません。

実際の負荷制限を計算するには:

1. Windowsデスクトップの数設定を変更し、Web ジョブとLANSA Open セッションの数を増やします。例えば3000 だとすると、それぞれの Visual LANSA は最大でも1500 のWebジョブしかサポートしないので、これをテストするには複数のVisual LANSA をインストールする必要があります。
2. システムが不安定になり始める、つまりレスポンスタイムが遅くなったり、ジョブがハングアップしたりなどの状態になるまでWeb ジョブとLANSA Open セッションの数を増やし続けて下さい。その時点で Web ジョブとLANSA Open セッションの数をメモに書きます。この数が実際のWindows システムの負荷制限となります。
3. この実際の負荷制限に基づき、(それ以下の)最適な負荷制限を予測します。
4. 予測した制限値に従ってWindowsデスクトップの数 の拡張オプションパラメータを変更します。

重要事項:

- これらのパラメータは同一のWindows システム上で同時に実行されている全てのVisual LANSA システム (V10.0 バージョン以降) で利用され、共有されます。
- これらのパラメータは同一のWindows システム上で同時に実行されている全てのLANSA Open セッション (V10.0 バージョン以降) でも利用され、共有されます。参考までに、LANSA Open を利用している時はLANSA for the Web アドミニストレータ内からこれらの設定にアクセスすることができます。
- LANSA システムのプロセスやリスナーサービス(V10.0 バージョン以降)、例えばW3\_P1200 や LCOTP などがWindows システム上で実行されている場合、全てのプロセスとリスナーサービスが終了され再起動されない限り、これらのパラメータはWindows 上では有効となりません。必ず全てのシステムとリスナーサービスを終了させてからこれらのプロセスやサービスを再起動させて下さい。

変更されたパラメータを有効にする方法

1. LANSA for the Web アドミニストレータを利用して同じシステム上で

同時に実行されている全てのLANSAのWeb ジョブ(V10.0 以降のバージョン) を終了させます。

2. 同じシステム上で同時に実行されている全てのLANSA Open セッション(V10.0 以降のバージョン)を閉じます。LANSA for the Web アドミニストレータ、LANSA Web ファンクションエディタやIIS Plug-in はLANSA Open セッションを使用していますので、実行中のLANSA for the Web アドミニストレータ、LANSA Web ファンクションエディタのアプリケーションも閉じて、IIS Plug-in を利用している全てのWeb サーバーも同じWindows システムに接続されていますので、終了させる必要があります。
3. 同じWindows システムに接続されている全てのWeb サーバーを終了させます。
4. 同じWindows システムで実行されている全てのリスナーサービス(V10.0 バージョン以降) を終了させます。
5. 同じWindows システムで実行されている全てのリスナーサービス(V10.0 バージョン以降) を再起動します。
6. 同じWindows システムに接続されている全てのWeb サーバーを再起動します。
7. エンドユーザーから要求されているWeb ジョブやLANSA Open セッションを再起動します。

## 2.7 ログとトレースのオプション設定

「[2.1 LANSACOMMUNICATIONS管理機能を開始する](#)」で説明されているように、ダイアログ・ボックスで[編集(E)]を選択すると、ログ・トレース情報のダイアログ・ボックスが開きます。

ログは、追跡したいノーマル・イベントの記録を可能にします。

トレースは、トラブル・シューティングの目的のため、記録された詳細情報の意味を明らかにします。

必要に応じてログかトレースのどちらか、または両方を設定することができます。

トレースあるいはログ・オプションをオンにすると、パフォーマンスに影響を与えます。この影響は最小限にとどまる場合もありますが、ワークステーションのハードウェアおよびソフトウェア構成により異なります。

ログ・トレースオプション共に、パフォーマンスに影響を及ぼします。通常のイベントを記録する時には、ログオプションを使用してください。問題追及をする時のみトレースオプションを使用してください。

ログ

接続       接続要求

OK  
キャンセル  
ヘルプ(H)

トレース

エラー       外部 IPC 呼び出し       IPC テキスト  
 リスナー・メッセージ       CPIC 呼び出し       内部 IPC 呼び出し  
 CPICメッセージ       システム情報       暗号化設定情報

標準の選択      全て選択      全て解除

ログ・トレースファイル

このファイル情報は、全ての LANSACOMMUNICATIONS 通信のログ・トレースオプションに適用されます。

省略値のパスを使用する

ログファイルパス: C:\LANSACOMMUNICATIONS\MSSQL Master V1      ログファイル最大サイズ: 2097152  
トレースファイルパス: C:\LANSACOMMUNICATIONS\MSSQL Master V1      トレースファイル最大サイズ: 2097152

ログおよび / あるいはトレースは、以下のものに対して設定することができます :

- ホストルート パートナー LU名によって識別される特定のルートとコミュニケーション管理機能メインウィンドウのホストルートリストから選択されたもの
- ソフトウェアモジュール 例えば CPIC マネージャなど。コミュニケーション管理機能のメインウィンドウの[拡張設定]メニューから[モジュール ログ トレース ...]ダイアログで選択されたもの

選択されたルートやモジュールはログトレース情報ダイアログのタイトルバー上に表示されます。

## ログ

### [接続]

将来の使用のために留保されています。

### [接続要求]

現在の接続要求の明細を記録する際にこのオプションを選んでください。

## トレース

以下の各アイテムのかっこの中の数字が、通信ルートテーブル・ファイルにおけるアイテムをトレースするため、自動的に設定に追加される値です。

### [エラー] (1)

エラー情報をトレースします。これは、致命的なエラーだけでなく、通信中に発生したノーマルと思われるエラーからも構成されています。致命的なエラーも、常にログ・ファイルに書き込まれます。

### [リスナー・デバッグ] (8)

将来の使用のために留保されています。

注：このオプションが使用される場合は、ホストマシン上でユーザは管理者権限が必要です。それ以外の場合、kernel32.dllでエラーが発生する場合があります。

### [CPIC データ] (1024)

通信エクステンションが呼び出された時に送信および受信されたデータをトレースします。

### [外部IPC呼び出し] (512)

基礎となる通信へのAPIコールおよびオペレーティング・システムへのいくつかのコールをトレースします。

#### [CPIC 呼び出し] (4096)

通信エクステンションのCPI-CマネージャへのAPI (CPI-C) コールをトレースします。

#### [システム情報] (2)

DLLがロードしたおよびロードしないイベントといった基本的な情報をトレースします。

#### [IPC データ] (2048)

基礎となる通信 (例: TCP/IPソケット) が呼び出された時に送信および受信されたデータをトレースします。

#### [内部IPC呼び出し] (8192)

通信エクステンションのIPCモジュールに対するAPIコールをトレースします。

#### [暗号情報] (16384)

暗号化通信モジュールが使用されている暗号化APIコールをトレースします。

#### [ホストのトレース] (32768)

このルートレコードが接続されている間トレースフラグがホストに送られます。ホストはこの通信セッションの間トレースフラグを利用します。

標準オプションを復元するには"標準の選択" ボタンを押して下さい。  
全てのオプションをオンにするには"全て選択"ボタンを押して下さい。  
全てのオプションを解除する場合は"全て解除"ボタンを押して下さい。

#### ログトレースファイル

このログトレースファイル設定は一般的な設定を行うもので、特定のルートやモジュールに限られたものではありません。

#### [省略値のパスを利用する]

省略値のパスを利用して複数の構成のための異なったトレースファイルを作成します。これはWindows プラットフォームのみです。

#### [ログファイルパス/最大サイズ]

ログのエントリーが記録されるファイル名および最大サイズ (バイト) を入力して下さい。ファイルサイズを0のままにしておくと、ファイル

サイズは無制限になります。

[トレースファイルパス/最大サイズ]

トレースファイルのエントリー用のファイル名および最大サイズ(バイト)を入力して下さい。最大ファイルサイズの省略値は0で、ファイルサイズが無制限になります。

## 2.8 Windows ワークステーションのセットアップ例

ここでは、TCP/IP通信エクステンションを使用して、CS Builder/サーバーで32ビット・アプリケーションを実行するWindows クライアントの構成に必要なステップを簡単に説明します。

この例では、クライアントはAS400PC1という名前のIBM i と通信を行います。

1. IBM i 上で、TCP/IPおよびLANSA通信エクステンションが実行されているかどうか、確認してください。
2. "コントロールパネル/ネットワーク"からWindows TCP/IPソフトウェアをインストールしてください。販売代理店の指示およびネットワーク管理者から提供される情報に従って、このソフトウェアを構成してください。
3. ワークステーション上とホスト上の両方でTCP/IPをインストールし、構成したら、ワークステーションからホストへ"ping"を実行することにより、構成のテストを行ってください。
4. CS Builder/サーバー for Windows をインストールしてください（LANSA通信エクステンションのオプションを含む）。
5. LANSAコミュニケーション管理機能（LCOADM32.EXE）を使用して、以下のステップで説明されているとおり、ホストのルートを指定してください。
6. LANSAコミュニケーション管理機能のメイン・ウィンドウで、"新規作成（N）"のボタンを選択し、"ホストルート情報"を表示してください。（これ以外にも、アクセラレーター・キーを使用して、該当する"編集"メニュー・アイテムを選択するか、あるいは、フォーカスが"ホストルート情報"にある間に挿入キーを押すことによって、この画面を表示することができます。）以下にある通りに情報を入力して下さい。

パートナー AS400PC1

LU名

ホスト名      ホストのアドレス。これは:  
- 同じドメインのホスト(AS400PC1) に対する単純なホスト名;

- "ホスト . ドメイン"というフルパス指定の名前;
- ネットワーク管理者から提供されたアドレスが  
nnn.nnn.nnn.nnn というフォーマットのIP アドレス

通信方法    Socket

その他の  
フィールド    省略値のまま

7. 終了したら OKボタンを押して下さい。

これで、32ビットのCS Builder/サーバー・アプリケーションは、ホスト AS400PC1との通信にTCP/IPソケット通信を使用できるようになりました。

### 3. IBM i の構成

ここでは、IBM i 上でTCP/IPを設定する時に使用する画面について説明しています。

#### 3.1 構成項目の処理

#### 3.2 オープン・システム・ユーティリティに関する考慮事項

#### 3.3 IBM i 上でリスナー・ジョブを実行する

### 3.1 構成項目の処理

IBM i 構成項目の設定方法については『LANSA/AD ユーザーガイド』を参照してください。

- LANSAX通信定義
- LANSAX通信エクステンション機能トレース・レコード
- LANSAX通信エクステンション・リスナー・レコード

### 3.2 オープン・システム・ユーティリティに関する考慮事項

IBM i 上では、セッション・ジョブはリスナー・ジョブを開始したユーザーのユーザー・プロフィールで前もって開始されています。接続要求を受け取ると、セッションをリクエストしたユーザー・プロフィールに変更されます。プログラムUD@CALL1を使用してLANSAファンクションを呼び出している場合は、ファイルDC@F28にあるアップデートされたソース番号を使用して、データ構造DC@IDSに現在のユーザーをロードしてください。

## 3.3 IBM i 上でリスナー・ジョブを実行する

### 3.3.1 リスナー・ジョブの開始

### 3.3.2 リスナー・ジョブの終了

#### サブシステムの設定

セッション・ジョブを実行するサブシステムを定義するため、LANSA 通信エクステンション定義で入力したジョブ記述のパラメータを使用してください。セッション・ジョブを実行するサブシステムは、実行したいと思っているだけの数のアクティブ・ジョブが可能なものでなければなりません。そうでないと、リスナーによって投入されたセッション・ジョブはキューに入れられ、接続要求を受け取ることができません。

#### 機密保護に関する考慮事項

セッション・ジョブは、リスナー・ジョブと同じユーザー・プロフィールのもとで開始されます。接続要求を受け取ると、セッション・ジョブは、リモート・セッションを要求するユーザーの"サインオン"を実行します。新しいユーザーがサインオンすると、ジョブは新しいユーザー・プロフィールのもとで実行されます（ライブラリ・リストは、新しいユーザーの初期ライブラリ・リストに変更されます）。

ユーザーのサインオンを実行するため、セッション・ジョブは、IBMが提供するAPIs QSYGETPH、QWTSETP、QSYRLSPHを使用します。プログラムLCOTPを所有するユーザー・プロフィールは、これらのAPIsの使用権限を持っていないとできません。

セッション・ジョブはサインオンしたユーザー・プロフィールのもとで実行されますが、初期のジョブ名は変更されないことに注意してください。セッション・ジョブを実行しているユーザーを識別するために、ジョブ名のユーザー・コンポーネントを信用してはいけません。セッション・ジョブの現在のユーザー属性を検索すべきです。これはLANSAによって処理されますが、非LANSAプログラムを使用している際は、そのことを知っておくべきでしょう。

### 3.3.1 リスナージョブの開始

TCP/IPを使用してリモート・セッションがIBM i に接続する前に、IBM i 上でリスナー・ジョブが開始されている必要があります。リスナー・ジョブは、通信ルートテーブルのリスナー・レコードにおいて指定されているポート番号で接続要求を待ちます。TCP/IPは、リスナー・ジョブが開始される前にアクティブになっていなければなりません。

リスナー・ジョブを開始するには、以下のLANSAリクエストを投入してください：

```
SBMJOB CMD(LANSA REQUEST(STRLISTEN) JOB(aaaaaaaaaa))
```

aaaaaaaaaaは、皆さんが選択したジョブ名です。

開始するLANSAシステムのリスナー・ジョブの従属関係を最小化した場合は、オプション・パラメータPARM01(\*UNLOCK)を使用します。このオプションが要求されると、リスナー・ジョブはデータエリアDC@A01にロックが発生しませんし、LANSAシステム・データ・ライブラリのファイルをオープンしたままにしません。このオプション付きのバッチ投入コマンドは次のようなリクエストになります。

```
SBMJOB CMD(LANSA REQUEST(STRLISTEN) PARM01(*UNLOCK)  
JOB(aaaaaaaaaa))
```

### 3.3.2 リスナージョブの終了

リスナー・ジョブを終了するには、そのリスナー・ジョブに対して、OPTION(\*IMMED)とともにENDJOBコマンドを発行してください。リスナー・ジョブは、すでに開始されているセッション・ジョブで使用されていないものを終了してから、シャット・ダウンします。

## 4. Linux 通信の構成

この章では、Linux サーバー上で、リスナーや通信ルートテーブルを構成する方法、リスナーを停止、開始、そのステータスをチェックする方法について説明します。

### 4.1 Linux 通信の構成ファイル

### 4.2 Linuxサーバー上でリスナー・ジョブを実行する

## 4.1 Linux 通信の構成ファイル

LANSAX for Linux は次の3つの構成ファイルを使って通信に必要な様々な条件を構成していきます。

- lansa.ini  
メインとなる構成ファイルで、別の構成ファイルの省略値のファイルロケーションを変更したり、共通のログ、トレースのパラメータを提供したりします。
- listen.dat  
リスナーの構成ファイルで、使用するTCPポート番号やログ、トレース用の様々なパラメータ、その他の設定が含まれています。
- lroute.dat  
通信ルートテーブルでホストルートやルートに関連したログ、トレースのパラメータ情報やその他の設定が含まれています。

これらのファイルはLANSAX for Linux インストーラーによってインストール時に作成され、インストールのルートディレクトリに置かれます。

環境変数LANSAXROOTが定義されたとすると、LANSAX通信はまずLANSAXROOTが指定したディレクトリにlansa.ini、listen.dat、lroute.datがあるか確認します。LANSAXROOTが定義されていない、もしくはこれらのファイルが見つからない場合は、次に/etcディレクトリを確認します。

注: インストーラーはシェルスクリプト {install\_root}/x\_lansa/bin/setenv.shを作成し、上級のユーザーがLANSAX for Linuxのシェルコマンドプロンプトに必要な環境変数を設定できるようにしています。例えば、setenv.shは省略値としてLANSAXROOTに {install\_root}を設定します。

[4.1.1 lansa.ini を使用して、省略値のファイル・ロケーションを変更する](#)

[4.1.2 リスナーを構成する](#)

[4.1.3 通信エクステンション・テーブルを構成する](#)

### 4.1.1 lansa.ini を使用して、省略値のファイル・ロケーションを変更する

省略値のファイル・ロケーション、パラメータあるいはサイズ（例えば最大ファイルサイズなど）を変更する必要がある場合は、テキストエディターを利用して{lansa\_root}/lansa.iniを編集して下さい。

LANSAs for Linuxを/lansaにインストールした場合、/lansa/lansa.iniが下の例のように作成されます。：

```
[Communications]
LicenceTable=/lansa/x_lansa/x_lickey.dat
ProcInfoFile=/lansa/lcoproc.ini
RouteTable=/lansa/lroute.dat
TraceFile=/lansa/log/lroute.trc
LogFile=/lansa/log/lroute.log
;TraceMaximum=65536
;LogMaximum=65536
;LogStateCheck=N
```

このファイルにはカスタマイズ可能な全てのファイルロケーションとその他のパラメータが記載されています。セミコロンで始まる行はコメント行です。つまり、セミコロンを使って簡単にパラメータを有効にしたり、無効にしたりすることができます。上の例ではTraceMaximumの省略値は現在コメント行になっています。

## 4.1.2 リスナーを構成する

LANSA for Linux インストーラーはリスナー用の構成ファイル {lansa\_root}/listen.dat をインストール時に作成します。インストーラーのポート番号が指定されていない場合は、4545 がポート番号として使用されます。

例えば、LANSA for Linux をディレクトリ/lansa にインストールしたとします。インストールにポートオプションを利用しない場合、/lansa/listen.dat ファイルは次のように作成されます。

- \* LANSA Communication Listener record File
- \* Comma Delimited, positional parameters.
- \* Empty parameters must have at least one space.
- \* Record Types (first character)
- \* L listener information
- \*L,Threads,IPCMethod,IPCModule,Trace,ConnectId,Compression,Algorithm,L,1,Socket, ,0,4545,1,Non,0,1,0

インストールにポートオプションを利用した場合は、代わりに指定されたポート番号が構成ファイルに書き込まれます。インストール時の詳細やオプションについては Linux 用のインストールガイドを参照して下さい。

インストール後にリスナーの設定をカスタマイズする必要がある場合は、テキストエディタで構成ファイルを編集することができます。ほとんどの設定が構成ファイルのコメントを見れば簡単に変更できるようになっています。

上級ユーザーの場合は上記の方法のほかに構成ファイルをWindows にコピーし、LANSA コミュニケーション管理機能を使って変更することも可能です。変更後は構成ファイルをコピーし、Linux サーバーに戻して下さい。LANSA for Windows インストール用の現在のlisten.dat を保存し、Linux 用の構成ファイルを変更した後に元に戻すことを忘れないようにして下さい。

### 4.1.3 通信エクステンション・テーブルを構成する

LANSA for Linux のインストーラは基本の通信ルートテーブル {lansa\_root}/lroute.dat をインストール時に作成します。このテーブルには同じインストールのリスナーにアクセスする際に使用されるLU名 \*LOCAL の1つのエントリーしか含まれていません。このエントリーのポート番号にはリスナーのポート番号と同じものが使われています。

例えば、LANSA for Linux をディレクトリ/lansa にインストールしたとします。インストールにポートオプションを利用しない場合、/lansa/lroute.datファイルは次のように作成されます。:

- \* LANSA Communication Routing Table File
  - \* Comma Delimited, positional parameters.
  - \* Empty parameters must have at least one space.
  - \* Record Types (first character)
  - \* R routing information
  - \* T module trace information
  - \*R,LUName,FullyQualName,IPCMethod,IPCModule,Trace,ConnectId,Packet
  - \*T,module identity,Trace
  - \*
- ```
R,*LOCAL,127.0.0.1,Socket, ,0,4545,0,1
```

インストール後にエントリーの設定をカスタマイズする必要がある場合は、テキストエディタでルートテーブルを編集することができます。ほとんどの設定がルートテーブルのコメントを見れば簡単に変更できるようになっています

ルートテーブルにエントリーを追加する必要がある場合、現在のエントリーをコピーし、コピーされたエントリーをカスタマイズすることで、ルートテーブルを変更することができます。

ルートテーブルに大幅な変更をする必要がある場合は、Windows の LANSA コミュニケーション管理機能のGUI を使えば編集しやすいです。

LANSA通信エクステンション・管理機能を使用して、Linuxサーバー上で使用するための通信ルートテーブルを作成あるいは保守することができます。LANSA/CS400リスナーがインストールされているWindowsサーバーの[拡張設定]メニューに[リスナー]オプションが表示され、管理機能を実行することができます。

1. Linux通信ルートテーブルのロケーションを決めてください(例: c:\temp\lroute.dat)。

2. 管理機能を開いて、"通信ルートテーブルのパス"を現在の設定から新しいロケーションに変更してください。"ホストルート"ウィンドウをクリックすると、省略値の通信ルートテーブルに定義されている"ホストルート"が消えるはずですが、Linuxサーバー上で"ホストルート"を構成する必要はありません。
3. 「[ワークステーションの構成](#)」の章で述べられている手順に従って、"モジュール・ログ"、"トレース"、"リスナー"を構成してください。この時、以下のポイントに注意してください：
  - [リスナーの開始]および[リスナーの停止]ボタンは、使用しないでください。これらのボタンは、Linuxサーバー上ではなく、Windowsサーバー上でリスナーを開始あるいは停止しようとしています。
  - ログとトレースファイルのパスは、変更しないでください。これは、Windowsサーバーのトレース・ファイルに対するパスを設定するものです。Linuxのパスを変更したい場合は、「[4.1.1 lans.iniを使用して、省略値のファイル・ロケーションを変更する](#)」を参照して下さい。
  - [リスナーのスレッド数]パラメータは、0か1でなければなりません。0か1以外の数は、全て1として扱われます。
4. "通信ルートテーブルのパス"をもとの設定に戻してください。
5. 新しいroute.datファイルをUNIX上の\etcディレクトリにコピーしてください。これは、必ず小文字でなければなりません。

## 4.2 Linuxサーバー上でリスナー・ジョブを実行する

Linuxサーバーには、lcolctlというリスナー制御ユーティリティがあります。このユーティリティ (lcolctl) により、リスナーが実行中であるか、リスナーが開始されているか、リスナーが停止されているかということを確認することができます。

このユーティリティを使用する前にシェルコマンドプロンプトを開始し、設定スクリプト {lansa\_root}/x\_lansa/bin/setenv.sh をロードして下さい。この設定スクリプトは標準シェルsh とbash の対象になります。他のシェルを利用する場合は、そのシェルに対してsetenv.sh を適用させて下さい。

標準シェルsh または bash を使用している場合、次のコマンドでLANSA for Linux を実行させるためのコマンドプロンプト環境を設定できます。:

```
. {lansa_root}/x_lansa/bin/setenv.sh
```

{lansa\_root} をLANSA for Linux インストールのディレクトリ、例えば/lansaに置き換えて下さい。設定スクリプトが LANSAXROOT や X\_RUN Y などの環境変数を設定します。この設定がLANSA forLinux をコマンドプロンプトで使用するにあたって重要な鍵となります。この設定スクリプトはまたコマンドパスや共有ライブラリのパスも更新します。

To start or stop the listener, you need to use a shell command prompt logged in as root. For other operations, you may log in as any user belongs to the group that owns the installation directory.

リスナーを開始するには、次のコマンドを使用して下さい。(ルートで実行して下さい。):

```
lcolctl start {port}
```

{port} はリスナーのポート番号です。インストーラーのポート番号を指定しなければ、省略値は4545 となります。現在のポート番号が分からない場合は、リスナーの構成ファイルlisten.dat. で確認できます。

例えば、リスナーのポート番号が4444 の場合は

```
lcolctl start 4444
```

となります。

リスナーを停止するには、これと似たコマンドを使用します。(ルートで実行して下さい):

## **lcolctl stop {port}**

例:

```
lcolctl stop 4444
```

リスナーが実行されているか確認するには次のコマンドを使用します。:

## **lcolctl show**

例えばインストールのリスナーが実行されている場合、次のような表示になります。:

```
Port PID SID  
4545 15489
```

これはリスナーが実行されていて、ポート番号4545 を見ていることを示します。また15489 は処理 I D です。SID 欄は現バージョンではもう使用されておらず、通常はブランクになっていることに注意して下さい。またLinux の標準ps コマンドを使ってシステム上で実行されている（使用中のインストールバージョン以外も含む）全てのリスナーを確認できます。例えば:

## **ps -ef | grep lco**

Linux サーバーでリスナーが実行されている場合、次のような表示になります。:

```
root 15489 1 0 Jul01 ? 00:00:00 /lansa/connect/lcolist: [monitor]  
root 15490 15489 0 Jul01 ? 00:00:00 /lansa/connect/lcolist: listening  
on port 4545
```

システム上で複数のリスナーが実行されている場合は上記のようなエントリーが見られます。

リスナーが停止していてもlcolctl stop コマンドを使用して適切に終了されていない場合は、例えばシステムのシャットダウンの一連処理の中で終了された場合など、lcolctl show コマンドがリスナーがまだ実行されていると誤って表示する可能性があります。lcolctl start コマンドを使って再度リスナーを開始しようとする、コマンドは以下のようなメッセージでエラーとなります。:

```
Port 4545 already in use
```

この場合、まず lcolctl stop コマンドを使用してから、lcolctl start コマンドで再度リスナーを開始して下さい。

## 5. 通信エラー・コード

通信エクステンションを使用している時にホストとクライアント間で通信エラーが発生した場合、TCP/IPソフトウェアから戻されるエラーは、標準のAPPCエラー・コードにマップされます。

よく経験するAPPCエラーコードは20, 6, 17です。通常、問題の原因を知るためには、このAPPCコードで十分です。簡単な解決策は以下の通りです。

| APPC<br>エラー<br>コード | 考えられる原因                                                                                |
|--------------------|----------------------------------------------------------------------------------------|
| 20                 | アプリケーションがリスナーに接続できなかったことを示します。リスナーが実行されているかチェックし、サーバーのリスナーポートにファイアウォールの問題がないかも確認して下さい。 |
| 6                  | ログイン確認時のエラーを示します。ユーザー名とパスワードが正しい場合はサーバーでLANSA通信のトレースを利用し、エラーの原因を確かめて下さい。               |
| 17                 | ログイン確認後、サーバー上で予期せぬエラーが生じたことを示します。サーバー上のジョブログ joblog/x_err.log で何が問題だったのかを確認して下さい。      |

この情報が十分でなく、問題が再現できる場合は、"エラー"トレースをオンにして、もとのエラーは何なのかということ突きとめる必要があります。(詳しくは、「[ログとトレース](#)」のセクションを参照してください。) "エラー"トレースをオンにすると、トレース・ファイルに以下のようなエントリーが現れます：

```
02/06/97 16:12:39 testw32(0xa2:0x9f):LCOSlapi:Error:COMM_Allocate  
Native Error:10061 CPIC Error:20 in connect
```

"Native Error"とは、通信ソフトウェアにより戻されたもとのエラーです。この例では、「ホストがソケット・ポート4545上での実行に必要な"リスナー"を実行していなかったため、"接続"要求でエラー・コード

10061 ( WSAECONNREFUSED ) が発生した」ということを表します。

以下の表は、WSAGetLastError() ( Winsock ) コールによって戻されるエラー・コードとそれらの説明をリストアップしたものです。これらのエラー番号は、全てのWindowsソケット準拠のインプリメンテーションを通じて一貫したものです。

| エラーコード | Windows ソケット・コード   | Berkeley 対応     | 説明   |
|--------|--------------------|-----------------|------|
| 10004  | WSAEINTR           | EINTR           | 標準 C |
| 10009  | WSAEBADF           | EBADF           | 標準 C |
| 10013  | WSEACCES           | EACCES          | 標準 C |
| 10014  | WSAEFAULT          | EFAULT          | 標準 C |
| 10022  | WSAEINVAL          | EINVAL          | 標準 C |
| 10024  | WSAEMFILE          | EMFILE          | 標準 C |
| 10035  | WSAEWOULDBLOCK     | EWOLDBLOCK      | 標準 C |
| 10036  | WSAEINPROGRESS     | EINPROGRESS     |      |
| 10037  | WSAEALREADY        | EALREADY        | BSD  |
| 10038  | WSAENOTSOCK        | ENOTSOCK        | BSD  |
| 10039  | WSAEDESTADDRREQ    | EDESTADDRREQ    | BSD  |
| 10040  | WSAEMSGSIZE        | EMSGSIZE        | BSD  |
| 10041  | WSAEPROTOTYPE      | EPROTOTYPE      | BSD  |
| 10042  | WSAENOPROTOOPT     | ENOPROTOOPT     | BSD  |
| 10043  | WSAEPROTONOSUPPORT | EPROTONOSUPPORT | BSD  |
| 10044  | WSAESOCKTNOSUPPORT | ESOCKTNOSUPPORT | BSD  |
| 10045  | WSAEOPNOTSUPP      | EOPNOTSUPP      | BSD  |
| 10046  | WSAEPFNOSUPPORT    | EPFNOSUPPORT    | BSD  |
| 10047  | WSAEAFNOSUPPORT    | EAFNOSUPPORT    | BSD  |
|        |                    |                 |      |

|       |                    |               |                                      |
|-------|--------------------|---------------|--------------------------------------|
| 10048 | WSAEADDRINUSE      | EADDRINUSE    | BSD                                  |
| 10049 | WSAEADDRNOTAVAIL   | EADDRNOTAVAIL | BSD                                  |
| 10050 | WSAENETDOWN        | ENETDOWN      | BSD                                  |
| 10051 | WSAENETUNREACH     | ENETUNREACH   | BSD                                  |
| 10052 | WSAENETRESET       | ENETRESET     | BSD                                  |
| 10053 | WSAECONNABORTED    | ECONNABORTED  | BSD                                  |
| 10054 | WSAECONNRESET      | ECONNRESET    | BSD                                  |
| 10055 | WSAENOBUFS         | ENOBUFS       | BSD                                  |
| 10056 | WSAEISCONN         | EISCONN       | BSD                                  |
| 10057 | WSAENOTCONN        | ENOTCONN      | BSD                                  |
| 10058 | WSAESHUTDOWN       | ESHUTDOWN     | BSD                                  |
| 10059 | WSAETOOMANYREFS    | ETOOMANYREFS  | BSD                                  |
| 10060 | WSAETIMEDOUT       | ETIMEDOUT     | BSD                                  |
| 10061 | WSAECONNREFUSED    | ECONNREFUSED  | BSD                                  |
| 10062 | WSAELOOP           | ELOOP         | BSD                                  |
| 10063 | WSAENAMETOOLONG    | ENAMETOOLONG  | BSD                                  |
| 10064 | WSAEHOSTDOWN       | EHOSTDOWN     | BSD                                  |
| 10065 | WSAEHOSTUNREACH    | EHOSTUNREACH  | BSD                                  |
| 10091 | WSASYSNOTREADY     |               | ネットワーク・サブシステムが使用できない                 |
| 10092 | WSAVERNOTSUPPORTED |               | WindowsソケットのDLLがこのアプリケーションをサポートしていない |

|       |                   |                |     |
|-------|-------------------|----------------|-----|
| 10093 | WSANOTINITIALISED |                |     |
| 11001 | WSAHOST_NOT_FOUND | HOST_NOT_FOUND | BSD |
| 11002 | WSATRY_AGAIN      | TRY_AGAIN      | BSD |
| 11003 | WSANO_RECOVERY    | NO_RECOVERY    | BSD |
| 11004 | WSANO_DATA        | NO_DATA        | BSD |

## 6. 複数のリスナー・ジョブを実行する

[6.1 IBM i ホスト](#)、[6.2 Linux ホスト](#)あるいは[6.3 Windows ホスト](#)上で、複数のリスナー・ジョブを実行することができます。

ここで述べるセットアップ手順は、2つのリスナー・ジョブを実行するためのものですが、さらに多くのリスナー・ジョブを実行する場合でも、手順は同じです。

## **6.1 IBM i ホスト**

6.1.1 別のリスナーの設定

6.1.2 追加のリスナーの作成

6.1.3 追加のリスナーのアップグレード

### 6.1.1 別のリスナーの設定

同じマシンに2つ目のLANSA システムをインストールした場合、そのシステム独自の通信構成を持つようになります。つまり、それぞれのLANSA システムに別々のリスナーがあるということです。この2番目のリスナーと最初にインストールされたLANSA システムのリスナー間でのコンフリクトを避けるためつぎの手順に従ってください。

1. 2つ目のLANSA システムのLANSA 通信記述 (構成項目 COMMS\_DEFINITIONSなど) を編集し、セッションのジョブ名の接頭辞を変更して下さい。これは必須ではありませんが、例えばどのリスナーから開始されたジョブセッションなのかを見分けやすくなります。
2. ジョブセッションのユーザー待ち行列を変更する場合は、他のリスナーに使用されていない固有の名前であることを確認して下さい。

## 6.1.2 追加のリスナーの作成

同一のLANSA システム上に2つのリスナーが必要になった場合(省略値プラス追加のリスナー)、2番目の構成を作成する必要があります。

2番目のリスナーが必要な理由として、例えば顧客によっては暗号化されたポートに接続する場合もあれば、暗号化されていないポートに接続する場合もあると思います。

2つのリスナーが確実に必要になった場合は、「[6.1.3 追加のリスナーのアップグレード](#)」に書かれてある通り、手動で追加のリスナーをアップグレードする必要があります。

同一のLANSA システム上に2つのリスナーを持つには以下の手順に従って下さい。:

1. 2番目のリスナーの構成オブジェクト(例: NEWCFGLIB)を保管するための新しい構成ライブラリを作成してください
2. 新しい構成ライブラリにデータ域LCOA01のコピーを作成してください。
3. 次のコマンドを実行してください。(出荷時のLANSA プログラムライブラリにあります。):

```
LCOAINST REQUEST(INSTALL) LIB(PPPPPPPPPP)
```

PPPPPPPPPP は新しい構成ライブラリの名前です。(例えば NEWCFGLIBなど)

4. エンターキーを一度押すと、追加のコマンドパラメータのプロントが出ます。省略値は現在のLANSA 構成から検索されます。:

OWNER: LANSA 通信ルートテーブルのオーナー

IFSPATH: ルートテーブルの IFS パス.

プロンプトの値が正しければ、エンターキーを一度押して下さい。LANSA システムをインストールもしくはアップグレードした後に LANSA 構成を変更している場合は、最新の値を入力してからエンターキーを押して下さい。このコマンドで省略値のつけられた新しいテーブルが作成されます。

5. 新しい構成ライブラリを現在実行しているジョブの現ライブラリ同様に設定します。これにはi5/OS コマンド CHGCURLIB を利用します。

6. LANSA 通信記述(構成項目COMMS\_DEFINITIONSなど)を編集します。画面の下のメッセージにどの構成オブジェクトが変更されているかが表示されます。ロックされている構成オブジェクトが新しい構成ライブラリからのものであることを確認して下さい。
7. ジョブセッション名の接頭辞を変更します。これは必須ではありませんが、例えばどのリスナーから開始されたジョブセッションなのかを見分けやすくなります。
8. ジョブセッションのユーザー待ち行列を変更します。この名前は同じマシン上の他のリスナーに使用されていない固有の名前でないといけません。
9. 新しい構成ライブラリが現ライブラリになるよう、2番目のリスナーが実行されるユーザープロファイルを変更して下さい。こうすることによってLANSA 通信エクステンションの構成がLANSAプログラムライブラリからではなく、新しい構成ライブラリから取り出されるのを確実にできます。
- 10.2番目のリスナーに接続しているユーザープロファイルも現ライブラリと同様、新しい構成ライブラリを持っている必要があります。
- 11.2番目のリスナージョブを提出して下さい。SBMJOB のUSER パラメータを使って上記の手順9で作成したユーザープロファイルを指名して下さい。

### 6.1.3 追加のリスナーのアップグレード

LANSA システムのアップグレードでは省略値のリスナー( LANSА プログラムライブラリに構成が保存されているもの)だけをアップグレードしますが、追加のリスナーのアップグレードは行われません。

LANSA システムの2番目(追加)のリスナーをアップグレードするには、次の手順に従って下さい。:

1. 以下のコマンドを実行して下さい。(出荷時の LANSА プログラムライブラリにあります):

**LCOAINST REQUEST(UPGRADE) LIB(PPPPPPPPPP)**

PPPPPPPPPP は2番目のリスナー構成ライブラリの名前です。

2. エンターキーを1度押すと、LANSА 通信ルートテーブルのオーナーのプロンプトが表示されます。
3. このプロンプトの値が正しければ、エンターキーをもう1度押して下さい。LANSА システムをインストールもしくはアップグレードした後にLANSА 構成を変更している場合は、現在のオーナー名を入力してからエンターキーを押して下さい。
4. 2番目のリスナーの構成ライブラリを現在のライブラリ同様に設定して下さい。
5. LANSА 構成記述を編集し、現在の構成を再確認して下さい。

## 6.2 Linux ホスト

それぞれのリスナー・ジョブは、1つのデータベースに接続されているクライアントからの接続要求のみを処理します。これは、全ての接続が、`lcolctl start`が実行された時から、rootユーザー(LANSAXROOT, ORACLE\_SID, など)の環境変数を受け継いでいるためです。データベースがその環境で設定されているため、リスナー・ジョブは、1つのデータベースしか処理できないのです。

1つのデータベースに複数のシステム区画を持つことができます。が、複数のデータベースが必要な場合は、各データベースに対してそれぞれ1つのリスナー・ジョブを実行する必要があります。複数のリスナー・ジョブを実行することは可能ですが、そのジョブが正しいデータベースに対して実行されるよう、セットアップには細心の注意を払わなければなりません。

- 通信ルートテーブル（省略値は `\etc\lroute.dat` です）をマニュアルで編集します。2番目のリスナーに対して、新しいIL（リスナー）レコードを追加してください。接続が使用する別々のTCP/IPポートを構成してください。
- 環境をrootユーザー用に設定してください。
- オプションで、`\etc\lansa.ini`を修正して、トレースおよびログ・ファイルに別々のパスを設定してください。詳しくは、「[lansa.iniを使用して、省略値のファイル・ロケーションを変更する](#)」を参照してください。
- コマンド・ラインにポート番号を指定することによって、2番目のリスナー・ジョブを開始してください。詳しくは、「[Linuxサーバー上でリスナー・ジョブを実行する](#)」を参照してください。

## 6.2.1 クライアント上でのセットアップ

各クライアント上で、新しいポート番号に接続するよう、接続IDを変更する必要があります。

## 6.3 Windows ホスト

複数のVisual LANSAシステムを1台のコンピュータ（Windows ServerのOSが好ましい）にインストールし、構成することが可能です。ここでは1台のサーバーに複数のVisual LANSAシステムをインストールする方法を説明します。

この例ではVisual LANSAシステムはそれぞれ別のデータベースを使用しており、リスナーはそれぞれのVisual LANSAシステムの通信を制御するために特定のポート番号で実行されるよう構成されます。

Visual LANSAをマスター/スレーブのサーバー構成でインストールする場合、LANSA通信ソフトはサブディレクトリCONNECTにインストールされます。

このインストールと構成の例ではVisual LANSAシステムの名前に一例として次の名前を使用しています。

- 最初の Visual LANSA システムの名前: Visual LANSA1
- 2番目のVisual LANSA システムの名前: Visual LANSA2

### 最初の *Visual LANSA* システムをインストールする

1. Visual LANSA1 システムはC:\Visual LANSA1 ディレクトリにインストールされます。
  - インストール中はリスナーを手動で開始するよう設定して下さい。\*
2. LANSA のメニューから[構成/管理]フォルダを選択し、[LANSA コミュニケーション管理機能]をスタートさせて下さい。
3. メニューオプション[拡張設定(A)]の[リスナー(L)...]よりリスナーポート番号を定義して下さい。Visual LANSA1 システムにはリスナーが同じポート番号に定義されます。例: 4550
4. Visual LANSA1 システムのホストルート情報の詳細を定義して下さい。
5. リスナーをテストして下さい。
  - リスナーを開始・停止し、サービスコンソールで実行されているサービスをよく監視して下さい。
  - 定義された LConnect サービスが実行されているはずです。

### 2番目の *Visual LANSA* システムをインストールする

1. Visual LANSA2 システムはC:\Visual LANSA2 ディレクトリにインストールされます。
  - インストール中はリスナーを手動で開始するよう設定して下さい。\*
2. LANSA のメニューから[構成/管理]フォルダを選択し、[LANSA コミュニケーション管理機能]をスタートさせて下さい。
3. メニューオプション[拡張設定(A)]の[リスナー(L)...]よりリスナーポート番号を定義して下さい。Visual LANSA2 システムにはリスナーが同じポート番号に定義されます。例: 4560
4. Visual LANSA2 システムのホストルート情報の詳細を定義して下さい。
5. リスナーを手動でスタートさせて下さい。サービスコンソールから *LConnect* サービスが監視できます。
6. 同一のマシンで実行されている2つのリスナーの動作をテストするには、両方のデータベースを同時に接続してみてください。

LANSA Web アドミニストレータ/ファンクションエディタやLANSA のクライアントがVisual LANSA1 と Visual LANSA2 システムに接続するようにインストールされている場合は、構成してから使用して下さい。

\*インストール時にリスナーを手動で開始するよう設定しなかった場合、リスナーのポート番号を変更する時にリスナーを停止し、開始させなければなりません。これが手動スタートに設定されているとリスナーを開始する前に停止させる必要はありません。しかしながら、手動スタートに設定されている場合、リスナーを使用する度に手動でスタートさせなければなりません。Windows サービスを通してこれを自動に変更することは可能です。

## 7. トラブルシューティング

### Windows

ルートテーブルが見つからない場合、以下のようなエラーが報告されます。:

Can't find lroute.dat (a Communication Extensions message)

または

Host route record can't be found (a Visual LANSA error)

LANSA 通信エクステンション管理機能を再起動させ、ルートレコードが正しいか確認して下さい。