

コネクティビティー 補足

バージョン 7



コネクティビティー 補足

バージョン 7



ご注意!

本書、および本書がサポートする製品をご使用になる前に、203ページの『付録B. 特記事項』にある一般的な情報を必ずお読みください。

本書において、日本では発表されていない IBM 製品（機械およびプログラム）、プログラミング、またはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのような IBM 製品、プログラミング、またはサービスを、日本で発表する意図があることを必ずしも示すものではありません。

本マニュアルについてご意見やご感想がありましたら

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

からお送りください。今後の参考にさせていただきます。

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.infocor.co.jp/ifc/books/>

をご覧ください。（URL は、変更になる場合があります）

原典：	Connectivity Supplement Version 7
発行：	日本アイ・ビー・エム株式会社
担当：	ナショナル・ランゲージ・サポート

第1刷 2000.2

この文書では、平成明朝体™W3、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™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 1995, 2000. All rights reserved.

Translation: © Copyright IBM Japan 2000

目次

本書について	v	データの表示	97
本書の構成	v	第3章 SNA を使用した DRDA ネットワーク での DB2 ユニバーサル・データベース (AS/400 版) の接続	99
本書の対象読者	vi	DB2 ユニバーサル・データベース (AS/400 版) インプリメンテーション	99
その他の情報源	vi	アプリケーション・リクエスターのセットア ップ	100
WWW の使用	vi	ネットワーク情報の提供	100
DRDA 関連資料	vi	機密保護の提供	107
DRDA サーバー関連資料	vii	データの表示	110
他の関連資料	viii	アプリケーション・サーバーのセットアップ ネットワーク情報の提供	112
第1章 DRDA ネットワークでの DB2 (MVS/ESA 版) の接続	1	機密保護の提供	113
DB2 (MVS/ESA 版)	2	データの表示	117
DB2 (MVS/ESA 版) インプリメンテーション	4	第4章 TCP/IP を使用した DRDA ネットワ ークでの DB2 ユニバーサル・データベース (AS/400 版) の接続	119
アプリケーション・リクエスターのセットア ップ	8	DB2 ユニバーサル・データベース (AS/400 版) 情報のまとめ	119
ネットワーク情報の提供	9	DB2 ユニバーサル・データベース (AS/400 版) DRDA TCP/IP サーバーの設定上および 使用上の考慮事項	120
機密保護の提供	21	DB2 ユニバーサル・データベース (AS/400 版) DRDA TCP/IP クライアントの設定上の 考慮事項	122
データの表示	28	TCP/IP を介した DRDA を使用する上での機 密保護の考慮事項	123
アプリケーション・サーバーのセットアップ ネットワーク情報の提供	28	第5章 DB2 ユニバーサル・データベース (AS/400 版) と DB2 ユニバーサル・デー タベースとの間のその他の考慮事項	125
機密保護の提供	30	第6章 DRDA ネットワークでの DB2 (VSE および VM 版) の接続	131
データの表示	44	DB2 (VM 版) 概説	131
第2章 DRDA ネットワークでの DB2 ユニバ ーサル・データベース (OS/390 版) の接続	45	アプリケーション・リクエスター通信フロ ーの例	134
DB2 ユニバーサル・データベース (OS/390 版)	46	アプリケーション・サーバー通信フローの 例	136
DB2 ユニバーサル・データベース (OS/390 版) インプリメンテーション	48		
追加機密保護拡張	52		
アプリケーション・リクエスターのセットア ップ	54		
ネットワーク情報の提供	55		
機密保護の提供	74		
データの表示	83		
アプリケーション・サーバーのセットアップ ネットワーク情報の提供	84		
機密保護の提供	85		
ネットワーク機密保護の提供	89		
データベース・マネージャー機密保護	92		
機密保護サブシステム	94		
	96		

DB2 (VM 版) インプリメンテーション	139	付録A. よく起こる接続問題	189
アプリケーションのプリプロセスまたは実行オプション	140	よくある DB2 接続問題	189
データベース・サーバー・マシンの開始オプション	143	SQL0965 または SQL0969	190
VM 環境でのアプリケーション・リクエストのセットアップ	144	CONNECT 時の SQL1338	190
ネットワーク情報の提供	145	CONNECT 時の SQL1403N	191
機密保護の提供	154	SQL5043N	191
データの表示	159	SQL30020	192
DB2 (VM 版) DRDA アプリケーション・リクエストを使用可能にするためのチェックリスト	161	SQL30060	193
VM 環境でのアプリケーション・サーバーのセットアップ	161	SQL30061	193
ネットワーク情報の提供	162	CONNECT 時の SQL30073 (戻りコード 119C)	194
機密保護の提供	165	SQL30081N (戻りコード 1)	195
データの表示	169	SQL30081N (戻りコード 2)	196
DB2 (VM 版) DRDA アプリケーション・サーバーを使用可能にするためのチェックリスト	170	SQL30081N (戻りコード 9)	196
DB2 (VSE 版) 概説	171	SQL30081N (戻りコード 10)	197
アプリケーション・サーバー通信フローの例	172	SQL30081N (戻りコード 20)	198
制限事項	174	SQL30081N (戻りコード 27)	198
アプリケーション・サーバー開始パラメーター	174	SQL30081N (戻りコード 79)	198
RMTUSERS パラメーター	174	SQL30081N (プロトコル固有のエラー・コード 10032)	199
SYNCPNT パラメーター	174	DB2 UDB DRDA AS で最も一般的な問題	200
VSE 環境でのアプリケーション・サーバーのセットアップ	175	CONNECT 時の通信エラー	200
ネットワーク情報の提供	175	CONNECT 時の DRDA エラー	200
機密保護の提供	182	CONNECT 時のデータベースが見つからないエラー	201
データの表示	185	APPC/SNA LU 6.2 を介した CONNECT 時の機密保護エラー	201
DB2 (VSE 版) DRDA アプリケーション・サーバーを使用可能にするためのチェックリスト	186	BIND 時のエラー	202
		付録B. 特記事項	203
		商標	206
		索引	209
		IBM と連絡をとる	215
		製品情報	215

本書について

本書は、種々の DB2 RDBMS 製品を、DRDA アプリケーション・リクエスターまたはアプリケーション・サーバーとして、インストール、構成するのに役立つ追加情報を記載しています。この情報は、以下の製品の設定を支援する目的で準備されました。

- DRDA アプリケーション・サーバー (AS) として実行される IBM DB2 ユニバーサル・データベース (UDB) バージョン 7 サーバー。
- IBM DB2 コネクト バージョン 7 アプリケーション・リクエスター (AR)。
- DRDA に準拠した他の製品。

本書に記載されている情報は、以下の解説書に記載されている情報の補足です。

- DB2 ユニバーサル・データベース エンタープライズ・エディション バージョン 7 についての概説およびインストール。
- DB2 ユニバーサル・データベース エンタープライズ拡張エディション バージョン 7 についての概説およびインストール。
- DB2 コネクト エンタープライズ・エディション バージョン 7 についての概説およびインストール。
- DB2 コネクト パーソナル・エディション バージョン 7 についての概説およびインストール。

ホスト製品 (DB2 ユニバーサル・データベース (OS/390 版)、DB2 ユニバーサル・データベース (AS/400 版)、および DB2 (VSE および VM 版)) に関する最新情報については、付属の資料を参照してください。

複数サイトで更新できるように DB2 同期点マネージャー (SPM) を構成する方法については、オンラインのインストールおよび構成 補足 を参照してください。

本書の構成

本書は次のように構成されています。

- 1ページの『第1章 DRDA ネットワークでの DB2 (MVS/ESA 版) の接続』
- 45ページの『第2章 DRDA ネットワークでの DB2 ユニバーサル・データベース (OS/390 版) の接続』

- 99ページの『第3章 SNA を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』
- 119ページの『第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』
- 125ページの『第5章 DB2 ユニバーサル・データベース (AS/400 版) と DB2 ユニバーサル・データベースとの間のその他の考慮事項』
- 131ページの『第6章 DRDA ネットワークでの DB2 (VSE および VM 版) の接続』
- 189ページの『付録A. よく起こる接続問題』
- 203ページの『付録B. 特記事項』

本書の対象読者

本書は DB2 ユニバーサル・データベースまたは DB2 コネクトをインストールした方で、前の節に示した見出しに関連してコネクティビティーについてさらにお知りになりたい方を対象にしています。

その他の情報源

この節では、他の役立つ情報源を紹介します。

WWW の使用

DB2 コネクト、DB2 ユニバーサル・データベース、およびその他の IBM ソフトウェア製品の最新情報を WWW で見つけることができます。ここでは、Technotes という形でまとめられた技術上のヒントだけでなく、最新の資料も含まれています。WWW でこの情報を見つけるためには、次のステップを実行してください。

1. ウェブ・ブラウザを次の URL に設定します。
`http://www.ibm.com/software/data/db2/library/`
2. 「DB2 ユニバーサル・データベース」を選択します。
3. たとえば、「DDCS」、「DRDA」、または「Connect」などのキーワードを使って「Technotes」を検索します。

DRDA 関連資料

以下の資料には関連情報が収められており、本書で参照することもあります。

資料番号	書名
SC88-7070	分散関係データベース体系 接続の手引き

資料番号	書名
N:SC26-4773	分散リレーショナル・データベース・ライブラリー 適用業務プログラミングの手引き
N:SC26-4782	分散関係データベース 問題判別の手引き
N:SC26-4650	分散リレーショナル・データベース ライブラリー 分散リレーショナル・データベースの計画
GC26-3195	<i>Distributed Relational Database Architecture Every Manager's Guide</i>
G321-5482	<i>IBM Distributed Data Management Architecture Level 3: Reference</i>

DRDA サーバー関連資料

関連する DRDA サーバー資料には、DB2 ユニバーサル・データベース (AS/400 版)、DB2 (OS/390 版)、および DB2 (VSE および VM 版) ライブラリーに含まれる以下の資料が含まれています。

資料番号	書名
SC88-5327	AS/400 分散データベース・プログラミング
SC88-5078	AS/400 SAA SQL/400 プログラマーの手引き
SC88-5002	AS/400 SAA SQL/400 解説書
GC21-8180	AS/400 Communications Configuration Reference
SC88-7377	DB2 (OS/390 版) 適用業務プログラミングおよび SQL の手引き
SC88-7378	DB2 (OS/390版) コマンド解説書
GC88-7385	DB2 (OS/390 版) インストレーションの手引き
SC88-7382	DB2 (OS/390 版) リモート DRDA リクエスター / サーバー 解説書
SC88-7381	DB2 (OS/390 版) SQL 解説書
SC88-7376	DB2 (OS/390 版) 管理の手引き
SC88-7384	DB2 (OS/390 版) ユーティリティーの手引きおよび解説書
SH88-7024	SQL/DS SQL 解説書 (VM、VSE)
SC26-3255	IBM SQL Reference

他の関連資料

資料番号	書名
SG24-2006	<i>Migrating to DB2 Universal Database Version 5</i>
SG24-2213	<i>DB2 for OS/390 Version 5 Performance Topics</i>
SG24-4893	<i>DB2 Meets NT</i>
SG24-4894	<i>The Universal Connectivity Guide to DB2</i>
SG24-4693	<i>Getting Started with DB2 Stored Procedures</i>
SG24-2212	<i>DRDA Support for TCP/IP in DB2 Universal Database for OS/390 V5.1 and DB2 Universal Database V5.0</i>
SC88-6725	<i>AIX CICS/6000 アプリケーション・プログラミング・ガイド</i>
SC88-6734	<i>AIX CICS/6000 カストマイゼーションおよび操作</i>
GD88-7250-00	<i>DB2 コネクト エンタープライズ・エディション (UNIX 版) 概説およびインストール</i>
GD88-7249-00	<i>DB2 コネクト エンタープライズ・エディション (OS/2 および Windows NT 版) 概説およびインストール</i>
GD88-7251-00	<i>DB2 コネクト パーソナル・エディション 概説およびインストール</i>
GG24-4155	<i>Distributed Relational Database Architecture: Using DDCS for AIX DRDA support with DB2 for MVS/ESA and DB2 Universal Database for AS/400</i>
GG24-4311	<i>Distributed Relational Database Architecture Cross Platform Connectivity and Application</i>
SC23-2443	<i>Encina for AIX Product Family Overview</i>

第1章 DRDA ネットワークでの DB2 (MVS/ESA 版) の接続

DB2 (MVS/ESA 版) は、MVS/XA および MVS/ESA システム用の IBM 関係データベース管理システムです。DB2 (MVS/ESA 版) バージョン 2 リリース 3 は、DB2 (MVS/ESA 版) で分散リレーショナル・データを、DRDA プロトコルをサポートする他の DBMS と共有する最初のリリースです。この章では、DB2 (MVS/ESA 版) がどのように分散関係データベース・システムをサポートするかを説明します。DB2 ユニバーサル・データベース (OS/390 版) で処理を行っている場合は、この章を飛ばして、45ページの『第2章 DRDA ネットワークでの DB2 ユニバーサル・データベース (OS/390 版) の接続』に進んでください。

この章では、DB2 (MVS/ESA 版) で以下の接続を構成することに関する情報に重点が置かれています。

1. DB2 コネクトからの接続 (28ページの『アプリケーション・サーバーのセットアップ』を参照)
2. DB2 ユニバーサル・データベース・サーバーへの接続 (8ページの『アプリケーション・リクエスターのセットアップ』を参照)

2 つの DB2 (MVS/ESA 版) システムを接続する方法、または DRDA 接続を DB2 (MVS/ESA 版) に定義する方法の詳細については、*IBM DB2 管理の手引き* の分散データベースの接続に関する説明を参照してください。

VTAM バージョン 4 リリース 2 の AnyNet 機能を使用すると、TCP/IP ネットワーク上で APPC を実行することができます。AnyNet 機能は、AnyNet/MVS (ホストで実行される) と AnyNet/2 (ワークステーションで実行され、ホストからダウンロードされる) から成り立っています。エンド・ユーザーは TCP/IP ネットワークの中で、どの APPC アプリケーションにでもアクセスできます。アプリケーションの側に変更の必要はありません。TCP/IP を介して APPC を使用すると、MVS/ESA 上のアプリケーション・プログラムは、MVS/ESA、OS/2、AIX/6000、または Windows 上の別の APPC アプリケーション・プログラムとの間で、AnyNet APPC を使って TCP/IP を介して通信できます。詳細については、*VTAM AnyNet Feature for V4R2 Guide to SNA over TCP/IP* を参照してください。

DB2 (MVS/ESA 版)

図1 は、DB2 (MVS/ESA 版) の単一コピーを実行している MVS システムを示しています。単一の MVS 上で DB2 (MVS/ESA 版) の複数のコピーを実行することも可能です。所定の MVS システム内の DB2 (MVS/ESA 版) のコピーを識別するため (または MVS/JES complex 内の DB2 (MVS/ESA 版) のコピーを識別するため)、各 DB2 システムにはサブシステム名 が与えられています。これは 1~4 文字の、MVS/JES complex 内で固有の文字列です。図1 では DB2 (MVS/ESA 版) のサブシステム名は xxxx です。3 つの MVS アドレス空間名の接頭部は、DB2 (MVS/ESA 版) のサブシステム名です。これらの 3 つのアドレス空間が DB2 (MVS/ESA 版) 製品を構成します。

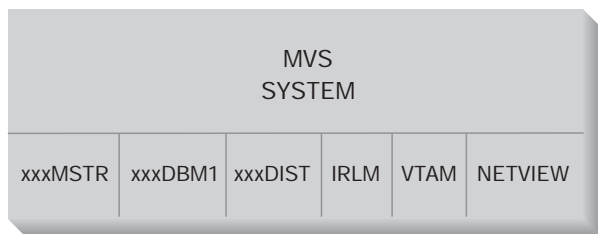


図1. DB2 (MVS/ESA 版) で使用される MVS アドレス空間

図1 は、DB2 (MVS/ESA 版) の分散データベース処理に関する MVS アドレス空間を示しています。これらのアドレス空間は、DB2 (MVS/ESA 版) ユーザーがローカル関係データベースにアクセスしたり、リモート DRDA システムと通信したりできるよう、協働します。各アドレス空間の目的は次のとおりです。

xxxxMSTR

DB2 (MVS/ESA 版) 製品のシステム・サービス・アドレス空間。DB2 (MVS/ESA 版) の始動と停止、DB2 (MVS/ESA 版) へのローカル・アクセスの制御を受け持ちます。

xxxxDBM1

データベース・サービス・アドレス空間。DB2 (MVS/ESA 版) によって制御される関係データベースへのアクセスを受け持ちます。ここでは、SQL アプリケーション・プログラムのためにデータベース資源への入出力が行われます。

xxxxDIST

DB2 (MVS/ESA 版) の、分散データベース機能を提供する部分。分散データベース機能 (DDF) とも言います。DDF は、分散データベース要求を受け取ると、必要なデータベース入出力を行えるよう、その要求を xxxxDBM1 に渡します。本書では DDF を詳細に説明します。

IRLM DB2 (MVS/ESA 版) が使用するロック・マネージャー。データベース資源へのアクセスを制御します。

VTAM MVS システム用の SNA コミュニケーション・マネージャー。DDF は、DB2 (MVS/ESA 版) のために分散データベース通信を行うのに VTAM を使用します。

NETVIEW

MVS システム上の、ネットワーク管理フォーカル・ポイント製品。分散データベースの処理中にエラーが発生すると、DDF は NetView ハードウェア・モニター・データベースにエラー情報 (警報 とも言う) を記録します。システム管理者は、ハードウェア・モニター・データベースに保管されたエラーを NetView を使って調べたり、あるいは警報条件が記録されると自動的に起動するコマンド・プロシーチャーを用意したりすることができます。

NetView は、VTAM 通信エラーの診断にも使用できます。詳細は、分散関係データベース [問題判別の手引き](#) を参照してください。

2ページの図1 には SQL アプリケーション・プログラムは示されていません。アプリケーション・プログラムが DB2 を使用して SQL ステートメントを発行する場合、このアプリケーション・プログラムを以下のいずれかの方法で DB2 (MVS/ESA 版) 製品と接続しなければなりません。

TSO TSO にログオンするバッチ・ジョブとエンド・ユーザーは、TSO 接続機能によって DB2 (MVS/ESA 版) と接続します。これは、SPUFI および大部分の QMF アプリケーションを DB2 (MVS/ESA 版) に接続するのに用いる手法です。

CICS/ESA

CICS/ESA アプリケーションが SQL 呼び出しを発行する場合、CICS/ESA 製品は CICS/ESA 接続インターフェースを使用して SQL 要求を DB2 (MVS/ESA 版) に経路指定します。

IMS/ESA

IMS/ESA の制御下で実行されるトランザクションは、IMS 接続インターフェースを使用して SQL ステートメントを DB2 (MVS/ESA 版) に渡し、これを処理します。

- DDF** 分散データ機能は、分散アプリケーションを DB2 (MVS/ESA 版) に接続します。
- CAF** 呼び出し接続機能を使用すると、ユーザー作成のサブシステムを直接 DB2 (MVS/ESA 版) に接続できます。

DB2 (MVS/ESA 版) インプリメンテーション

DRDA は、分散データベース管理システム機能のタイプを定義します。DB2 (MVS/ESA 版) V2R3 はリモート作業単位をサポートしています。リモート作業単位を使用すると、あるシステムで実行されているアプリケーション・プログラムは、1 つのリモート DBMS のデータにアクセスできます。そのときにはそのリモート DBMS が提供する SQL を使用します。DB2 (MVS/ESA 版) V3R1 は分散作業単位をサポートしています。分散作業単位を使用すると、あるシステムで実行されているアプリケーション・プログラムは、複数のリモート DBMS のデータにアクセスできます。そのときには各リモート DBMS が提供する SQL を使用します。DRDA で定義される分散のタイプの詳細については、分散関係データベース体系 接続の手引き を参照してください。

6ページの図2 に示されているとおり、DB2 (MVS/ESA 版) は 2 種類のアクセス方式を使用して、3 種類の分散データベース接続構成をサポートしています。

[1] システム主導アクセス では、DB2 (MVS/ESA 版) リクエスターを 1 つ以上の DB2 (MVS/ESA 版) サーバーに接続できます。DB2 (MVS/ESA 版) リクエスターとサーバーとの間に確立される接続は、DRDA で定義されたプロトコルに適合しないため、非 DB2 (MVS/ESA 版) 製品を DB2 (MVS/ESA 版) に接続するには使用できません。このタイプの接続は、3 つの部分からなる名前または別名をアプリケーションにコーディングすることによって確立されます。

[2] アプリケーション主導アクセス では、DB2 (MVS/ESA 版) リクエスターまたは非 DB2 (MVS/ESA 版) リクエスター (DB2 コネクトなど) を、1 つ以上の DB2 (MVS/ESA 版) アプリケーション・サーバーまたは非 DB2 (MVS/ESA 版) アプリケーション・サーバー、たとえば DB2 ユニバーサル・データベースや DB2 ユニバーサル・データベース (AS/400 版) などに接続できます。アプリケーション・リクエスターに一度に接続できるアプリケーション・サーバーの数は、アプリケーション・リクエスターの DB2 (MVS/ESA 版) のレベルに応じて異なります。アプリケーション・リクエスターが DB2 (MVS/ESA 版) V2R3 であれば、一度に 1 つだけアプリケーション・サーバーを接続できます。このタイプの接続は、SQL CONNECT ステートメントをアプリケーションにコーディングすることに

よって確立されます。アプリケーション・リクエスターが DB2 (MVS/ESA 版) V3R1 であれば、一度に 1 つ以上のアプリケーション・サーバーを接続できます。

[3] アプリケーション主導およびシステム主導アクセスを一緒に使用して接続を確立できます。

2 次サーバー という用語は、アプリケーション・サーバーのサーバーとして機能するシステムを指して用いられます。

構成の中に含まれるすべてのシステムが 2 フェーズ・コミットをサポートしている場合、分散作業単位 (複数サイト読み取りと複数サイト更新) がサポートされます。すべてのシステムが 2 フェーズ・コミットをサポートしているわけではない場合、作業単位内での更新は、2 フェーズ・コミットをサポートしない単一のサイト、または 2 フェーズ・コミットをサポートするサイトのサブセットのいずれかに制限されます。

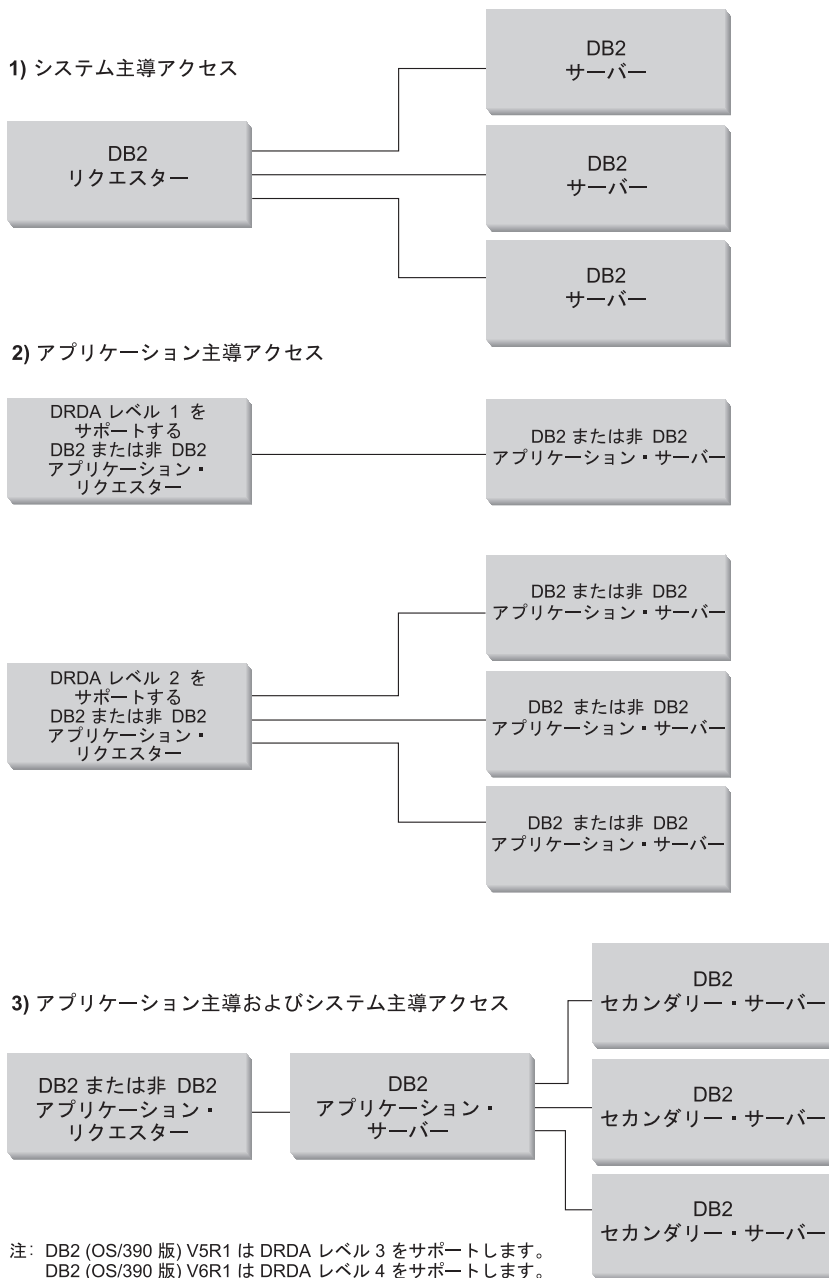


図 2. DB2 (MVS/ESA 版) 分散接続

6 DB2 コネクティビティー 補足

表1 は、DB2 (MVS/ESA 版) 分散データベースの接続タイプを比較したものです。

表1. DB2 (MVS/ESA 版) 分散データベースの接続の比較

[1] システム主導アクセス	[2] アプリケーション主導アクセス (すべてのシステムが 2 フェーズ・コミットをサポートする場合)	[3] アプリケーション主導およびシステム主導アクセス
すべてのパートナーが DB2 (MVS/ESA 版) システムでなければならぬ。	任意の 2 つの DRDA システムを相互接続できる。	アプリケーション・リクエスターは任意の DRDA システムでかまわないが、サーバーは DB2 (MVS/ESA 版) システムでなければならぬ。
複数のパートナーに直接接続できる。	複数のパートナーに直接接続できる。	アプリケーション・リクエスターは直接アプリケーション・サーバーに接続できる。アプリケーション・サーバーは複数の DB2 (MVS/ESA 版) 2 次サーバーに接続できる。
各 SQL アプリケーションは、各サーバーと複数の APPC 会話を行うことができる。	各 SQL アプリケーションは、各サーバーと 1 つの APPC 会話を行うことができる。	SQL アプリケーションは、各サーバーと 1 つの APPC 会話を行うことができる。DB2 (MVS/ESA 版) アプリケーションは、アプリケーションの各サーバーと複数の APPC 会話を確立できる。
1 コミットの範囲内でローカル資源とリモート資源の両方にアクセスできる。	1 コミットの範囲内でローカル資源とリモート資源の両方にアクセスできる。	アプリケーション・リクエスターとアプリケーション・サーバーはローカル・データとリモート・データにアクセスできる。
大規模な照会、および複数の照会を同時に行う場合に効果的。	1 コミットの範囲内で実行回数がわずかな SQL ステートメントの場合に効果的。	アプリケーション・リクエスターとアプリケーション・サーバー間の接続は [2] と同様に動作し、2 次サーバー接続は [1] と同様に動作する。
静的または動的 SQL をサポートできるが、コミットの範囲内で最初に静的 SQL を実行するとき、サーバーは静的 SQL を動的にバインドする。	静的または動的 SQL を発行できる。	アプリケーション・リクエスターとアプリケーション・サーバーは静的または動的 SQL を発行できる。2 次サーバーは静的または動的 SQL をサポートしているが、コミットの範囲内で最初に静的 SQL を実行するとき、静的 SQL を動的にバインドする。

表 1. DB2 (MVS/ESA 版) 分散データベースの接続の比較 (続き)

[1] システム主導アクセス	[2] アプリケーション主導アクセス (すべてのシステムが 2 フェーズ・コミットをサポートする場合)	[3] アプリケーション主導およびシステム主導アクセス
SQL INSERT、DELETE、UPDATE ステートメント、および SELECT をサポートするステートメントに制限されている。	システムがサポートしているステートメントであれば、どれも使用できる。	アプリケーション・サーバーはすべての SQL をサポートしている。2 次サーバーは DML SQL だけをサポートしている (CREATE または ALTER など)。

アプリケーション・リクエスターのセットアップ

DB2 (MVS/ESA 版) では、DB2 (MVS/ESA 版) 分散データ機能 (DDF) の重要な部分として DRDA アプリケーション・リクエスターを実装しています。DDF は、ローカルな DB2 (MVS/ESA 版) データベース管理機能とは別個に停止させることができますが、ローカルな DB2 (MVS/ESA 版) データベース管理サポートなしに実行させることはできません。

アプリケーション・リクエスターとして動作している場合、DB2 (MVS/ESA 版) はシステム上で実行されているアプリケーションを、DRDA アプリケーション・サーバー機能が実装されているリモート DB2 ユニバーサル・データベース、DB2 (MVS/ESA 版)、DB2 ユニバーサル・データベース (OS/390 版)、DB2 ユニバーサル・データベース (AS/400 版)、および DB2 (VSE および VM 版) の各データベース・サーバーに接続できます。

DB2 (MVS/ESA 版) アプリケーション・リクエスターを使用して分散データベースにアクセスするには、以下のようにしてください。

- 9 ページの『ネットワーク情報の提供』 - アプリケーション・リクエスターは、RDB_NAME 値を受け入れ、それらの値を SNA NETID.LUNAME 値に変換する必要があります。DB2 (MVS/ESA 版) は、DB2 (MVS/ESA 版) 通信データベースを使用して、RDB_NAME および対応するネットワーク・パラメーターを登録します。通信データベースによって、DB2 (MVS/ESA 版) アプリケーション・リクエスターは分散データベース要求を行うときに、必要な SNA 情報を VTAM に渡すことができます。
- 21 ページの『機密保護の提供』 - リモート・データベース要求がアプリケーション・サーバーによって受け入れられるようにするには、アプリケーション・リクエスターがサーバーに必要な安全保護情報を提供しなければなりま

せん。DB2 (MVS/ESA 版) は通信データベースと RACF を使用して、必要なネットワーク機密保護情報を提供します。

- 28ページの『データの表示』 - アプリケーション・リクエスターの CCSID がアプリケーション・サーバーと互換性があることを確認する必要があります。

ネットワーク情報の提供

分散データベース環境の処理の大部分では、ネットワーク内の他の場所との間でメッセージを交換することが必要です。このプロセスが正しく実行されるようにするには、以下のことを実行しなければなりません。

1. ローカル・システムの定義
2. リモート・システムの定義
3. 通信の定義
4. RU サイズおよび歩調合わせの設定

ローカル・システムの定義

ネットワーク内の各プログラムには NETID および LU 名が割り当てられているため、DB2 (MVS/ESA 版) アプリケーション・リクエスターがネットワークに接続するときには NETID.LUNAME 値が必要です。DB2 (MVS/ESA 版) アプリケーション・リクエスターはローカルの DB2 (MVS/ESA 版) データベース管理システムに統合されるため、アプリケーション・リクエスターには RDB_NAME も必要です。DB2 (MVS/ESA 版) のマニュアルでは、DB2 (MVS/ESA 版) は RDB_NAME をロケーション名と呼んでいます。

DB2 (MVS/ESA 版) アプリケーション・リクエスターを SNA ネットワークに定義するには、次のようにします。

1. DB2 (MVS/ESA 版) システムの LU 名を選択する。DDF が始動すると、DB2 (MVS/ESA 版) システムの NETID が VTAM から自動的に取得されます。
2. DB2 (MVS/ESA 版) のブートストラップ・データ・セット (BSDS) に LU 名とロケーション名を定義する (DB2 (MVS/ESA 版) ではロケーション名は 16 文字までに制限されています)。
3. 選択した LU 名を VTAM に登録するため、VTAM APPL 定義を作成する。

DDF BSDS の構成: DB2 (MVS/ESA 版) は始動処理中に BSDS を読み取って、システム・インストール・パラメーターを取得します。BSDS に保管されるレコードの 1 つは DDF レコード と呼ばれるものです。そのように呼ばれ

るのは、VTAM に接続するとき、その中に収められている情報を DDF が使用するからです。この情報は次のものから構成されます。

- DB2 (MVS/ESA 版) システムのロケーション名
- DB2 (MVS/ESA 版) システムの LU 名
- DB2 (MVS/ESA 版) システムが VTAM に接続するときに使用されるパスワード

以下の 2 つの方法で、DDF BSDS 情報を DB2 (MVS/ESA 版) に指定できます。

- DB2 (MVS/ESA 版) を最初にインストールするときに、DDF インストール・パネル DSNTIPR を使用して、必要な DDF BSDS 情報を指定する。ここではインストール・パラメーターの多くについては説明しません。DB2 (MVS/ESA 版) を VTAM に接続する方法を知る方が重要だからです。図3は、インストール・パネルを使ってロケーション名 SYDNEY、LU 名 LUDBD1、およびパスワード PSWDBD1 を DB2 (MVS/ESA 版) BSDS に記録する方法を示しています。

```
1 DDF STARTUP OPTION  ==> AUTO      NO (DDF not startable),
                                AUTO (automatic start up), or
                                COMMAND (start by command)
2 DB2 LOCATION NAME   ==> SYDNEY    The name other DB2s use to
                                refer to this DB2
3 DB2 NETWORK LUNAME  ==> LUDBD1    The name VTAM uses to refer to this DB2
4 DB2 NETWORK PASSWORD ==> PSWDBD1 Password for connecting to other DB2s
5 RLST ACCESS ERROR   ==> NOLIMIT   Action on non-local RLST access error
                                NOLIMIT - Run without limit
                                NORUN - Do not run at all
                                1-50000000 - Limit in CPU service units
PRESS: ENTER to continue  END to exit  HELP for more information
```

図3. DB2 (MVS/ESA 版) インストール・パネル DSNTIPR

- DB2 (MVS/ESA 版) のインストールが済んでいる場合は、ログ目録変更ユーティリティ (DSNJU003) を使用して BSDS の情報を更新する。
11 ページの図4 には、BSDS を更新して、ロケーション名を SYDNEY に、LU 名を LUDBD1 に、パスワードを PSWDBD1 にする方法が示されています。

```

//SYSADMB JOB , 'DB2 2.3 JOB', CLASS=A
//*
//*      CHANGE LOG INVENTORY:
//*      UPDATE BSDS WITH
//*          - DB2 LOCATION NAME FOR SYDNEY
//*          - VTAM LUNAME (LUDBD1)
//*          - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB DD DISP=SHR, DSN=DSN230.DSNLOAD
//SYSUT1 DD DISP=OLD, DSN=DSNC230.BSDS01
//SYSUT2 DD DISP=OLD, DSN=DSNC230.BSDS02
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
DDF LOCATION=SYDNEY, LUNAME=LUDBD1, PASSWORD=PSWDBD1
//*
```

図4. ブートストラップ・データ・セット DDF 定義の例

DDF が (DB2 (MVS/ESA 版) の始動に伴って自動的に、あるいは DB2 (MVS/ESA 版) の START DDF コマンドによって) 始動すると、DDF は VTAM に接続し、LU 名とパスワードを VTAM に渡します。VTAM は、LU 名とパスワード (VTAM パスワードが必要な場合) を DB2 (MVS/ESA 版) システムの VTAM APPL ステートメントで定義された値と照合することによって、DB2 (MVS/ESA 版) システムを認識します。VTAM パスワードは、指定された LU 名を DB2 (MVS/ESA 版) が VTAM 上で使用する許可を得ているかどうかを検査するために使用されます。VTAM パスワードはネットワークの中を伝送されることはありませんし、ネットワーク内の他のシステムを DB2 (MVS/ESA 版) に接続するために使用されることもありません。

VTAM がパスワードを必要としない場合は、ログ目録変更ユーティリティーで PASSWORD= キーワードを省略してください。このキーワードを指定しないということは、VTAM パスワードが不要であるということです。

VTAM APPL 定義の作成: VTAM LU 名とパスワードを DB2 (MVS/ESA 版) に定義したら、次にこれらの値を VTAM に登録する必要があります。VTAM では、ローカル LU 名を定義するのに APPL ステートメントを使用します。12ページの図5 は、LU 名 LUDBD1 を VTAM に定義する方法を示しています。

```

DB2APPLS VBUILD TYPE=APPL
*
*-----*
*
*          APPL DEFINITION FOR THE SYDNEY DB2 SYSTEM          *
*
*-----*
*
LUDBD1  APPL  APPC=YES,                                X
           AUTH=(ACQ),                                X
           AUTOSSES=1,                                X
           DMINWNL=10,                                X
           DMINWNR=10,                                X
           DSESLIM=20,                                X
           EAS=9999,                                  X
           MODETAB=RDBMODES,                          X
           PRTCT=PSWDBD1,                              X
           SECACPT=ALREADYV,                          X
           SRBEXIT=YES,                                X
           VERIFY=NONE,                               X
           VPACING=2,                                  X
           SYNCLVL=SYNCPT,                            X
           ATNLOSS=ALL                                X

```

図 5. DB2 (MVS/ESA 版) APPL 定義のサンプル

VTAM APPL ステートメントでは多くのキーワードを使用できます。キーワードの意味は、*DB2 管理の手引き* に詳細に説明されています。ここでは本書の内容に関係のあるキーワードだけを説明します。図5 に関するキーワードを以下に説明します。

LUDBD1

VTAM は、LU 名として APPL ステートメント・ラベルを使用します。この場合、LU 名は LUDBD1 です。APPL の構文では、完全な NETID.LUNAME の値を指定することができません。VTAM APPL ステートメントに NETID 値は指定されません。各アプリケーションには VTAM システムの NETID が自動的に割り当てられるからです。

AUTOSSES=1

APPC セッション数変更 (CNOS) が発行されるときに自動的に開始する SNA 回線争奪勝者セッションの数。VTAM CNOS 処理が失敗した場合に DB2 (MVS/ESA 版) に通知するため、AUTOSSES には非ゼロ値を指定する必要があります。

任意の 2 つの分散データベース・パートナー間のすべての APPC セッションを自動的に開始する必要はありません。AUTOSSES 値が回線争

奪勝者の限度 (DMINWNL) より小さい場合には、分散データベース・アプリケーションが必要とするまで、VTAM は残りの SNA セッションの開始を遅らせます。

DMINWNL=10

この DB2 (MVS/ESA 版) システムが回線争奪勝者となるセッションの数。DMINWNL パラメーターは CNOS 処理の省略時値ですが、DB2 (MVS/ESA 版) 通信データベースの SYSIBM.SYSLUMODES 表に行を追加することにより、任意のパートナーに合わせてオーバーライドできます。

DMINWNR=10

パートナー・システムが回線争奪勝者となるセッションの数。DMINWNR パラメーターは CNOS 処理の省略時値ですが、DB2 (MVS/ESA 版) 通信データベースの SYSIBM.SYSLUMODES 表に行を追加することにより、任意のパートナーに合わせてオーバーライドできます。

DSESLIM=20

DB2 (MVS/ESA 版) と特定のモード・グループ名の別の分散システムとの間に確立できるセッションの合計数 (勝者および敗者セッション)。DSESLIM パラメーターは CNOS 処理の省略時値ですが、DB2 (MVS/ESA 版) 通信データベースの SYSIBM.SYSLUMODES 表に行を追加することにより、任意のパートナーに合わせてオーバーライドできます。

パートナーが DSESLIM、DMINWNL、または DMINWNR パラメーターで要求されたセッションの数をサポートできない場合には、CNOS 処理はパートナーが受け入れ可能なこれらのパラメーターの新しい値を折衝します。

EAS=9999

この VTAM LU で必要とされるセッションの合計数の見積もり。

MODETAB=RDBMODES

各 DB2 (MVS/ESA 版) モード名が存在する VTAM MODE 表を指定します。

PRTCT=PSWDBD1

DB2 (MVS/ESA 版) が VTAM への接続を試行するときに使用される VTAM パスワードを指定します。PRTCT キーワードを省略する場合、パスワードは不要であり、DB2 (MVS/ESA 版) のログ目録変更ユーティリティから PASSWORD= キーワードを省略する必要があります。

SECACPT=ALREADYV

リモート・システムから分散データベース要求を受け取ったときにこの DB2 (MVS/ESA 版) システムが受け入れる、最大の SNA 会話レベル機密保護値を指定します。ALREADYV キーワードは、この DB2 (MVS/ESA 版) システムが、この DB2 (MVS/ESA 版) システムにデータを要求する他の DRDA システムから、以下の 3 つの SNA セッション機密保護オプションを受け入れることができることを示しています。

- SECURITY=SAME (リクエスターのユーザー ID だけを含む検査済みの要求)。
- SECURITY=PGM (リクエスターのユーザー ID およびパスワードを含む要求)。
- SECURITY=NONE (機密保護情報を含めないようにする要求)。DB2 (MVS/ESA 版) は、SECURITY=NONE と指定された DRDA 要求を拒否します。

各 DB2 (MVS/ESA 版) パートナーの SNA 会話機密保護レベルは DB2 (MVS/ESA 版) 通信データベース (SYSIBM.SYSLUNAMES 表の USERSECURITY 列) から取られるため、常に SECACPT=ALREADYV と指定するのが最良です。SECACPT=ALREADYV を指定すると、USERSECURITY の値を柔軟に選択できるようになります。

VERIFY=NONE

この DB2 (MVS/ESA 版) システムで必要な SNA セッション機密保護の (パートナー LU 検査) レベルを識別します。NONE 値は、パートナー LU 検査が必要ではないことを示しています。

DB2 (MVS/ESA 版) では、VERIFY キーワードの選択に制限はありません。信頼性の低いネットワークの場合は VERIFY=REQUIRED をお勧めします。VERIFY=REQUIRED を指定すると、パートナー LU 検査を実行できないパートナーを VTAM が拒否することになります。VERIFY=OPTIONAL を選択すると、VTAM はサポートを提供するパートナーにのみパートナー LU 検査を実行します。

VPACING=2

VTAM の歩調合わせカウントを 2 に設定します。

SYNCLVL=SYNCPT

DB2 (MVS/ESA 版) が 2 フェーズ・コミットをサポートできることを示します。VTAM は、この情報を使用して、パートナーに 2 フェーズ・コミットが使用可能であることを通知します。このキーワー

ドを指定すると、パートナーが 2 フェーズ・コミットをサポートできる場合に、DB2 (MVS/ESA 版) は自動的に 2 フェーズ・コミットを使用します。

ATNLOSS=ALL

VTAM セッションが終了するたびに DB2 (MVS/ESA 版) が通知を受ける必要があることを示します。これにより、DB2 (MVS/ESA 版) は必要なときに SNA 再同期を実行することになります。

DSESLIM、DMINWNL、および DMINWNR により、すべてのパートナーに当てはまる、省略時の VTAM セッション限度を確立できます。特殊なセッション限度要件があるパートナーの場合は、SYSIBM.SYSLUMODES 表を使って省略時のセッション限度をオーバーライドできます。たとえば、OS/2 システムに適した VTAM 省略時セッション限度を指定する場合、他のパートナーに適したセッション限度を定義する行を SYSIBM.SYSLUMODES 表に作成できません。次のサンプル値を考慮してください。

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

これらのパラメーターにより、各パートナーは、自分が回線争奪勝者であるセッションを最大 4 つまで DB2 (MVS/ESA 版) との間で作成できるようになります。OS/2 は DB2 (MVS/ESA 版) と LU 6.2 会話を作成するので、OS/2 を回線争奪勝者としても大幅なパフォーマンスの向上は望めません。OS/2 は、使用可能な回線争奪勝者セッションを持っている場合、新しい LU 6.2 会話を開始する許可を求める必要はありません。

リモート・システムの定義

DB2 (MVS/ESA 版) アプリケーションがリモート・システムからデータを要求するとき、DB2 (MVS/ESA 版) は通信データベース表を検索して、リモート・システムに関する情報を探します。次の情報が含まれます。

- LU 名と TPN
- リモート・サイトで必要なネットワーク機密保護情報
- リモート・サイトとの通信に使用されるセッション限度とモード名

通信データベースは、DB2 (MVS/ESA 版) システム管理者が管理する、SQL 表のグループです。DB2 (MVS/ESA 版) システム管理者は、使用される可能性のある各 DRDA パートナーを記述する行を通信データベースに挿入するのに、SQL を使用する必要があります。通信データベースは以下の 5 つの表から構成されています。

1. SYSIBM.SYSLOCATIONS

DB2 (MVS/ESA 版) は、この表を使って、DB2 (MVS/ESA 版) アプリケーションが選択した各 RDB_NAME の LU 名と TPN 値を判別します。列は次のとおりです。

LOCATION

リモート・システムの RDB_NAME。DB2 (MVS/ESA 版) では RDB_NAME 値が 16 バイトまでに制限されていて、DRDA で定義されている 18 バイトという制限より 2 バイト短くなっています。

LOCTYPE

現在使用されていません。ブランクにする必要があります。

LINKNAME

リモート・システムの LU 名。

LINKATTR

リモート・システムの TPN。リモート・システムが DB2 (MVS/ESA 版) システムである場合、またはリモート・システムが省略時の DRDA TPN 値 (X'07F6C4C2') を使用する場合、TPN に空ストリングを指定できます。DB2 (MVS/ESA 版) が自動的に正しい値を選択するためです。

リモート・システムが省略時値以外の TPN 値を必要とする場合、ここでその値を指定してください。

2. SYSIBM.SYSLUNAMES

この表は、リモート・システムのネットワーク属性を定義します。列は次のとおりです。

LUNAME

リモート・システムの LU 名。

SYSMODENAME

DB2 (MVS/ESA 版) 2 次サーバー・サポート (システム主導アクセス) 用の、DB2 (MVS/ESA 版) 同士のシステム間 会話を確立するのに使用される、VTAM ログオン・モード名。この列をブランク値にすると、DB2 (MVS/ESA 版) システム会話に IBMDB2LM が使用されることとなります。

USERSECURITY

この DB2 (MVS/ESA 版) システムがリモート・システムのサーバ

1. この TPN 値は現時点で DB2 (VM 版) に適用されます。

ーとして機能する場合の、リモート・システムのネットワーク機密保護受け入れに関する必須オプション (インバウンド機密保護 要件)。

ENCRYPTPSWDS

このパートナーとのパスワード交換を暗号化するかどうか。暗号化パスワードは、DB2 (MVS/ESA 版) リクエスターおよびサーバーでのみサポートされます。

MODESELECT

SYSIBM.SYSMODESELECT 表を使用し、要求を出したエンド・ユーザーとアプリケーションに基づいて VTAM ログオン・モード項目 (モード名) を選択するかどうかを決定します。この列に 'Y' が入っている場合、SYSIBM.SYSMODESELECT 表を使用して、各アウトバウンド分散データベース要求のモード名を取得します。

MODESELECT に 'Y' 以外の値が入っている場合、システム主導アクセス要求にモード名 IBMDB2LM が使用され、DRDA 要求にモード名 IBMRDB が使用されます。

モード名に関連した VTAM サービス・クラス (COS) を指定することにより、MODESELECT 列を使って分散データベース要求を優先順位付けすることが可能になります。

USERNAMES

必要な come-from 検査とユーザー ID 変換のレベル。この列は、リモート・パートナーからデータを要求するときこの DB2 (MVS/ESA 版) サブシステムが使用する機密保護パラメーターも指定します (アウトバウンド機密保護 要件)。USERNAMES の値は I、O、または B のいずれかとすることができま

3. SYSIBM.SYSLUMODES

この表は、パートナー・システムごとに LU 6.2 セッション限度 (CNOS 限度) を定義するために使用されます。列は次のとおりです。

LUNAME

リモート・システムの LU 名。

MODENAME

制限を指定する対象となる VTAM ログオン・モードの名前。MODENAME 列にブランク値を指定すると、IBMDB2LM に省略時解釈されます。

CONVLIMIT

このログオン・モードの場合の、ローカルな DB2 (MVS/ESA 版)

とりモート・システム間のアクティブな会話の最大数。この値は、このログオン・モードのための VTAM APPL 定義ステートメントの DSESLIM パラメーター (DB2 (MVS/ESA 版) の省略時の VTAM セッション限度を指定する) をオーバーライドするために使用されます。

CONVLIMIT に指定された値は、CNOS 中に DMINWNR および DMINWNL 値を CONVLIMIT/2 に設定するために使用されます。

AUTO DDF の始動時に CNOS 処理とセッションの事前割り振りを自動的に開始させるか、このログオン・モードを介して LU 名への最初の参照が行われるまで据え置くかを指定します。

4. **SYSIBM.SYSMODESELECT**

この表により、エンド・ユーザーおよび DB2 (MVS/ESA 版) アプリケーションごとに異なるモード名を指定できるようになります。各 VTAM モード名にはサービス・クラス (COS) を関連付けることができるので、この表を使って、AUTHID、PLANNAME、および LUNAME の組み合わせに基づいて、分散データベース・アプリケーションにネットワーク伝送優先順位を割り当てることができます。列は次のとおりです。

AUTHID

DB2 (MVS/ESA 版) ユーザーの許可 ID (ユーザー ID)。省略時値はブランクです。これは、指定されたログオン・モード名をすべての許可 ID に当てはめることを意味します。

PLANNAME

リモート・データベース・システムへのアクセスを要求しているアプリケーションに関連したプラン名。省略時値はブランクです。これは、指定されたログオン・モード名をすべてのプラン名に当てはめることを意味します。BIND PACKAGE コマンドで使用されるプラン名は DSNBIND です。

LUNAME

リモート・データベース・システムと関連した LU 名。

MODENAME

分散データベース要求を指定のリモート・システムに経路指定するときに使用される VTAM ログオン・モードの名前。省略時値はブランクです。これは、システム主導アクセス会話には IBMDB2LM を使用し、DRDA 会話には IBMRDB を使用することを意味します。

5. **SYSIBM.SYSUSERNAMES**

この表は、パスワード、名前変換、および come-from 検査を指定することによって、エンド・ユーザー名を管理するために使用します。DB2 (MVS/ESA 版) はエンド・ユーザー名を許可 ID として参照します。他の製品の大部分は、この名前をユーザー ID として参照します。

この表を使用すると、SNA ユーザー ID および DB2 (MVS/ESA 版) 許可 ID に別の名前を使用するよう、名前変換を行うことができます。名前変換処理は、リモート・システムへの要求 (アウトバウンド 要求) のため、およびリモート・システムから送られてくる要求 (インバウンド 要求) のために、行うことができます。パスワードが暗号化されていない場合、ユーザー ID とパスワードの両方をリモート・サイトに送るときに、この表はエンド・ユーザーのパスワードの情報源となります。列は次のとおりです。

TYPE 行の使用法の説明 (アウトバウンドまたはインバウンド用の名前変換を記述した行か、それとも come-from 検査要求を記述した行か)。

AUTHID

アウトバウンド名前変換の場合、これは変換対象の DB2 (MVS/ESA 版) 許可 ID。インバウンド名前変換の場合、これは変換対象の SNA ユーザー ID。どちらの場合でも、空白の AUTHID 値はすべての許可 ID またはユーザー ID にあてはまりません。

LUNAME

この行があてはまるリモート・システムの LU 名。空白の場合、NEWAUTHID 値はすべてのシステムにあてはまります。

NEWAUTHID

新しいエンド・ユーザー名 (SNA ユーザー ID または DB2 (MVS/ESA 版) 許可 ID)。空白を指定すると、ID の変換が不要であることを示すものとなります。

PASSWORD

パスワードが暗号化されない場合 (SYSIBM.SYSLUNAMES で ENCRYPTPSWDS = 'N' の場合)、割り当て会話で使用されるパスワード。パスワードが暗号化される場合、この列は無視されます。

通信の定義

VTAM は MVS システム用のコミュニケーション・マネージャーです。

VTAM は DB2 (MVS/ESA 版) から LU 6.2 verb を受け入れ、これらの verb を LU 6.2 データ・ストリームに変換して、ネットワーク経由で送信できるよ

うにします。VTAM が DB2 (MVS/ESA 版) 通信データベースで定義されているパートナー・アプリケーションと通信するためには、VTAM に以下の情報を提供しなければなりません。

- 各サーバーの LU 名。

DB2 (MVS/ESA 版) が VTAM と通信するときには、必要な宛先を識別するための LU 名 (NETID.LUNAME ではない) だけを VTAM に渡す許可が DB2 (MVS/ESA 版) に与えられています。DB2 (MVS/ESA 版) から渡される LU 名の値から VTAM が NETID と LU 名の両方を判別できるようにするためには、ローカル VTAM システムが認識している LU 名の中で、この LU 名が固有のものである必要があります。LU 名が企業の SNA ネットワーク全体に渡って固有のものであるなら、VTAM の資源定義の処理は大幅に単純化されます。ただし、これは必ずしも可能であるとは限りません。LU 名が SNA ネットワークの中で固有のものでないなら、VTAM の LU 名変換を使用して、固有でない LU 名のために NETID.LUNAME の正しい組み合わせを構築する必要があります。この処理については、VTAM ネットワーク導入の手引き (MVS/ESA) の『資源名変換』で説明されています。

リモート LU 名を定義するために用いられる VTAM の定義の配置と構文は、リモート・システムが論理的および物理的にどのようにローカル VTAM システムに接続されているかに応じて異なります。

- 各モード名の RU サイズ、歩調合わせウィンドウ・サイズ、およびサービス・クラス。通信データベースに指定されているモード名ごとに、VTAM モード表に項目を作成します。IBMRDB と IBMDB2LM を定義する必要もあります。
- LU 検査アルゴリズム用の VTAM および RACF プロファイル (パートナー LU 検査を使用する予定の場合)。

RU サイズおよび歩調合わせの設定

定義する VTAM モード表によって、RU サイズと歩調合わせカウントが指定されます。これらの値を正しく定義できていないと、すべての VTAM アプリケーションに悪影響を与える可能性があります。

RU サイズ、セッション限度、および歩調合わせカウントを選択した後、これらの値が既存の VTAM ネットワークに与える影響を考慮することは非常に重要です。新しい分散データベース・システムをインストールするときには、以下の項目を復習してください。

- VTAM CTC 接続には、MAXBFRU パラメーターが RU サイズ + 29 バイト (VTAM が SNA 要求ヘッダーおよび伝送ヘッダーに追加する分) を処理

するのに十分の大きさであることを確認してください。MAXBFRU は 4K バイト単位で計測されます。それで、MAXBFRU は少なくとも 2 でなければ 4K RU に適合しません。

- NCP 接続では、MAXDATA が RU サイズ + 29 バイトを処理できる十分な大きさであることを確認してください。4K の RU サイズを指定する場合、MAXDATA は最低 4125 でなければなりません。

NCP MAXBFRU パラメーターを指定する場合には、RU サイズに 29 バイトを加えた大きさが入る値を選択してください。NCP では、MAXBFRU パラメーターによって、PIU を保持するのに使用できる VTAM I/O バッファの数を定義します。IOBUF バッファ・サイズを 441 と選択する場合、10*441 は 4096+29 より大きいため、MAXBFRU=10 は 4K RU を正しく処理します。

- 分散関係データベース体系 接続の手引き では、VTAM IOBUF プールに対する分散データベースの影響を査定する方法について説明されています。IOBUF プール資源を使用しすぎている場合、VTAM パフォーマンスはすべての VTAM アプリケーションで低下します。

機密保護の提供

リモート・システムが SQL アプリケーションに代わって分散データベース処理を実行する場合には、アプリケーション・リクエスト、アプリケーション・サーバー、およびそれらに接続しているネットワークの機密保護要件を満たさなければなりません。これらの要件は、以下のカテゴリーのいくつかに分けられます。

- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護
- データ表示

エンド・ユーザー名の選択

MVS システムでは、エンド・ユーザーに 1~8 文字のユーザー ID が割り当てられます。このユーザー ID 値は、特定の MVS システムで固有でなければなりません。SNA ネットワーク全体で固有でなくてもかまいません。たとえば、NEWYORK システムで JONES というユーザーがいて、DALLAS システムでまた JONES というユーザーがいてもかまいません。この 2 人のユーザーが同一の人であれば、対立は起きません。しかし、DALLAS の JONES が NEWYORK の JONES とは別人の場合、SNA ネットワーク (およびそのネットワークの分散データベース・システム) は、NEWYORK の JONES と

DALLAS の JONES とを区別できません。この状況を訂正しない場合には、DALLAS の JONES は NEWYORK システムの JONES に与えられた特権を使用できます。

名前の対立を解消するため、DB2 (MVS/ESA 版) はエンド・ユーザー名前変換のサポートを提供します。DB2 (MVS/ESA 版) アプリケーション・リクエスターでアプリケーションが分散データベース要求を行うとき、通信データベースでアウトバウンド名前変換が必要であると指定されていれば、DB2 (MVS/ESA 版) は名前変換を実行します。アウトバウンド名前変換が選択されていると、DB2 (MVS/ESA 版) は必ず各アウトバウンド分散データベース要求と一緒にパスワードを強制的に送信します。

DB2 (MVS/ESA 版) のアウトバウンド名前変換は、SYSIBM.SYSLUNAMES 表の USERNAMES 列を 'O' または 'B' に設定すると活動化されます。USERNAMES を 'O' に設定すると、アウトバウンド要求でエンド・ユーザー名前変換が実行されます。USERNAMES を 'B' に設定すると、インバウンド要求とアウトバウンド要求の両方でエンド・ユーザー名前変換が実行されません。

DB2 (MVS/ESA 版) の許可は、エンド・ユーザーのユーザー ID および DB2 (MVS/ESA 版) プランまたはパッケージ所有者のユーザー ID に依存しているため、エンド・ユーザー名前変換処理は、エンド・ユーザーのユーザー ID、プラン所有者のユーザー ID、およびパッケージ所有者のユーザー ID に対して実行されます。² 名前変換処理に際しては、SYSIBM.SYSUSERNAMES 表の中で、次のパターン (TYPE.AUTHID.LUNAME) に一致する行が、次の順番で探索されます。

1. O.AUTHID.LUNAME - 特定のエンド・ユーザーから特定のパートナー・システムへの変換規則。
2. O.AUTHID.blank - 特定のエンド・ユーザーから任意のパートナー・システムへの変換規則。
3. O.blank.LUNAME - 任意のユーザーから特定のパートナー・システムへの変換規則。

一致する行が見つからないと、DB2 (MVS/ESA 版) は分散データベース要求を拒否します。行が見つかり、NEWAUTHID 列の値が許可 ID として使用されます (ブランクの NEWAUTHID 値は、元の名前を変換しないで使用することを意味します)。

2. 要求が DB2 (MVS/ESA 版) サーバーに送信される場合は、名前変換がパッケージ所有者とプラン所有者に対しても実行されます。パッケージ所有者とプラン所有者の名前がパスワードに関連付けられることはありません。

前述の例を考慮してみましょう。NEWYORK の JONES が DALLAS に分散データベース要求を出す場合、この JONES に別の名前 (NYJONES) を与えたものとします。この例において、JONES が使用するアプリケーションは DSNPLAN (DB2 (MVS/ESA 版) プラン所有者) の所有で、DALLAS に送信を行うときにこのユーザー ID の変換は不要であるものとします。名前変換規則を通信データベースに指定するのに必要な SQL ステートメントを図6 に示します。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', '0');
INSERT INTO SYSIBM.SYSLOCATIONS
  (LOCATION, LOCTYPE, LINKNAME, LINKATTR)
VALUES ('DALLAS', ' ', 'LUDALLAS', '');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

図6. アウトバウンド名前変換用 SQL

結果として通信データベースの表がどのようになるかを 24ページの図7 に示します。

NEWYORK.SYSIBM.SYSLOCATIONS			
LOCATION	LOCTYPE	LINKNAME	LINKATTR
DALLAS		LUDALLAS	

NEWYORK.SYSIBM.SYSLUNAMES					
LUNAME	SYSMODENAME	USERSECURITY	ENCRYPTPSWDS	MODESELECT	USERNAMES
LUDALLAS		A	N	N	O

NEWYORK.SYSIBM.SYSUSERNAMES				
TYPE	AUTHID	LUNAME	NEWAUTHID	PASSWORD
0	JONES	LUDALLAS	NYJONES	JONESPWD
0	DSNPLAN	LUDALLAS		PLANPWD

図7. アウトバウンド名前変換

ネットワーク機密保護

アプリケーション・リクエスターがリモート・アプリケーションを示すエンド・ユーザー名を選択した後は、そのアプリケーション・リクエスターは必要なネットワーク機密保護情報を提供しなければなりません。LU 6.2 は、主に3つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護。VTAM APPL ステートメントの VERIFY キーワードによって制御されます。セッション・レベル機密保護の指定方法についての詳細は、12ページの図5を参照してください。
- 会話レベル機密保護。SYSIBM.SYSLUNAMES 表の内容によって制御されます。
- データ暗号化。VTAM 3.4 以降のリリースでのみサポートされています。

アプリケーション・サーバーの責任でデータベース資源を管理するため、アプリケーション・サーバーは、どのネットワーク機密保護にアプリケーション・リクエストが必要かを指示します。各アプリケーション・サーバーの会話レベル機密保護要件を `SYSIBM.SYSLUNAMES` 表に記録する必要があります。そのためには `SYSIBM.SYSLUNAMES` 表の `USERNAMES` を、アプリケーション・サーバーの要件を反映するように設定します。

SNA 会話機密保護オプションは以下のとおりです。

SECURITY=SAME

これは検査済みの機密保護とも言います。それは、エンド・ユーザーのユーザー ID だけがリモート・システムに送信されるためです (パスワードは送信されません)。このレベルの会話機密保護は、`SYSIBM.SYSLUNAMES` の `USERNAMES` 列に 'O' または 'B' が入っていない場合に使用してください。

DB2 (MVS/ESA 版) ではエンド・ユーザー名前変換がアウトバウンド会話機密保護に関連付けられているので、アウトバウンド・エンド・ユーザー名前変換が活動化されている場合に `SECURITY=SAME` を使用することはできません。

SECURITY=PGM

このオプションを使用すると、エンド・ユーザー ID とパスワードが妥当性検査のためにリモート・システムに送信されます。この機密保護オプションは、`SYSIBM.SYSLUNAMES` 表の `USERNAMES` 列に 'O' か 'B' のいずれかが入っている場合に使用してください。

`SYSIBM.SYSLUNAMES` 表に指定されているオプションに応じて、DB2 (MVS/ESA 版) は 2 つの異なる情報源からユーザーのパスワードを取得します。

- 暗号化されていないパスワードは、`SYSIBM.SYSUSERNAMES` 表の `PASSWORD` 列から取得されます。`SYSIBM.SYSLUNAMES` の `ENCRYPTPSWDS` 列が 'Y' に設定されていない場合、DB2 (MVS/ESA 版) は `SYSIBM.SYSUSERNAMES` 表からパスワードを抽出します。この情報源から取得したパスワードは、どの DRDA アプリケーション・サーバーに対しても送信できます。

26ページの図8 では、SMITH と JONES のパスワードを定義しています。この例の `LUNAME` 列はブランクなので、これらのパスワードは SMITH または JONES がアクセスしようとするどのリモート・システムでも使用できます。

```

INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'SMITH', ' ', ' ', 'SMITHPWD');

```

図8. リモート・サイトへのパスワード送信

- SYSIBM.SYSLUNAMES の ENCRYPTPSWDS 列に 'Y' が入っている場合、暗号化パスワードがリモート・サイトに送信されます。暗号化パスワードは RACF (または RACF と同等の製品) から抽出され、別の DB2 (MVS/ESA 版) システムによってのみ解釈できます。DB2 (MVS/ESA 版) 以外のシステムと通信している場合は、ENCRYPTPSWDS を 'Y' に設定しないでください。

DB2 (MVS/ESA 版) は SYSIBM.SYSUSERNAMES 表を探索して、リモート・システムに送信するユーザー ID (NEWAUTHID 値) を判別します。変換されたこの名前は、RACF のパスワード抽出のために使用されます。名前を変換したくない場合は、名前を変換しないで送信するための行を SYSIBM.SYSUSERNAMES の中に作成する必要があります。図9 は、エンド・ユーザー名 (ユーザー ID) を変換せずに要求を LUDALLAS と LUNYC に送信できるようにします。

```

INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUDALLAS', ' ', ' ');

```

図9. リモート・サイトへの暗号化パスワードの送信

SECURITY=NONE

DRDA はこのオプションをサポートしていないため、DB2 (MVS/ESA 版) ではこの機密保護オプションを使用できません。

データベース・マネージャー機密保護

アプリケーション・リクエスターが分散データベースの機密保護に貢献できる 1 つの方法は、前に 21 ページの『エンド・ユーザー名の選択』で説明されたように、アウトバウンド・ユーザー名前変換です。アウトバウンド・ユーザー名前変換を使用すると、要求を出しているユーザーおよびアプリケーションの ID に従って、各アプリケーション・サーバーへのアクセスを制御できます。その

他に、DB2 (MVS/ESA 版) アプリケーション・リクエスターが分散システムの機密保護に貢献できる方法には以下のものがあります。

リモート・アプリケーションのバインド

エンド・ユーザーはアプリケーション・サーバーのリモート・アプリケーションを、DB2 (MVS/ESA 版) BIND PACKAGE コマンドを使ってバインドします。DB2 (MVS/ESA 版) は、リクエスターでの BIND PACKAGE コマンドの使用を制限しません。ただし、エンド・ユーザーは、リモート・パッケージが DB2 (MVS/ESA 版) プランに組み込まれるまで、このパッケージを使用できません。DB2 (MVS/ESA 版) は、BIND PLAN コマンドの使用を制限します。エンド・ユーザーは、DB2 (MVS/ESA 版) GRANT ステートメントで BIND または BINDADD 特権を与えられないかぎり、リモート・パッケージをプランに追加することができません。

パッケージをバインドするときは、ENABLE/DISABLE オプションを使用して、パッケージを TSO、CICS/ESA、IMS/ESA、またはリモート DB2 (MVS/ESA 版) サブシステムから使用できるかどうかを指定してください。

リモート・アプリケーションの実行

DB2 (MVS/ESA 版) エンド・ユーザーがリモート・アプリケーションを実行するには、そのアプリケーションに関連した DB2 (MVS/ESA 版) プランを実行する権限がエンド・ユーザーになければなりません。DB2 (MVS/ESA 版) プランの所有者には、自動的にそのプランの実行権限が与えられます。他のエンド・ユーザーは、DB2 (MVS/ESA 版) GRANT EXECUTE ステートメントで、プランの実行権限を与えてもらうことができます。このようにして、分散データベース・アプリケーションの所有者は個々のユーザー・ベースでアプリケーションの使用を制御できます。

機密保護サブシステム

MVS システムの外部機密保護サブシステムは RACF、および RACF と互換性のあるインターフェースを備えた同等の製品により提供されます。DB2 (MVS/ESA 版) アプリケーション・リクエスターには、外部の機密保護サブシステムを直接呼び出すことはありません。ただし、24ページの『ネットワーク機密保護』で説明された暗号化パスワード・サポートは例外です。しかし、以下の状況ではアプリケーション・リクエスターで外部機密保護サブシステムが間接的に使用されます。

- エンド・ユーザーと DB2 (MVS/ESA 版) との接続を受け持つ製品が、エンド・ユーザーの ID (ユーザー ID およびパスワード) の妥当性検査をするた

めに外部機密保護サブシステムを使用する場合。これは、エンド・ユーザーが DB2 (MVS/ESA 版) に接続する前に生じます。前述のとおり、CICS/ESA、TSO、および IMS/ESA は、エンド・ユーザーを DB2 (MVS/ESA 版) に接続する製品の一部です。

- SNA セッション・レベル機密保護を (DB2 (MVS/ESA 版) VTAM APPL ステートメントの VERIFY キーワードによって) 使用する場合、VTAM により外部機密保護サブシステムが呼び出されて、リモート・システムの ID が妥当性検査されます。

データの表示

DB2 (MVS/ESA 版) は、省略時のインストール・システム・コード化文字セット ID (CCSID) が 500 の状態で出荷されています。この省略時値はおそらく、ご使用のインストール・システムでは正しくない でしょう。

DB2 (MVS/ESA 版) をインストールするときには、インストール・システムの CCSID を、ご使用のサイトの入力装置が生成して DB2 (MVS/ESA 版) に送る文字の CCSID に設定する必要があります。通常、この CCSID はご使用になる言語によって決定されます。インストール・システムの CCSID が間違っていると、文字変換の結果が誤ったものになります。国別または言語別のサポートされる CCSID のリストについては、*DB2 コネクト 使用者の手引き* を参照してください。

ご使用の DB2 (MVS/ESA 版) サブシステムが、各アプリケーション・サーバーの CCSID を DB2 (MVS/ESA 版) サブシステムのインストール・システムの CCSID に変換できるかどうか確認する必要があります。変換元 CCSID と変換先の CCSID の一般的な組み合わせについては、DB2 (MVS/ESA 版) に変換テーブルが用意されていますが、可能なすべての組み合わせに対応しているわけではありません。必要であれば、使用可能な変換テーブルと変換ルーチンのセットを追加できます。DB2 (MVS/ESA 版) 文字変換の詳細については、*DB2 管理の手引き* を参照してください。

アプリケーション・サーバーのセットアップ

DB2 (MVS/ESA 版) のアプリケーション・サーバー・サポートによって、DB2 (MVS/ESA 版) は DRDA アプリケーション・リクエスターのサーバーとして機能することができます。DB2 (MVS/ESA 版) アプリケーション・サーバーに接続されたアプリケーション・リクエスターは、以下のものとして機能することができます。

- DB2 (MVS/ESA 版) リクエスター。

- AIX、HP-UX、OS/2、SCO、Solaris、Linux、Windows 9x、または Windows NT 上で実行できる DB2 コネクト バージョン 7。
- DB2 コネクト・サポートが使用できる DB2 ユニバーサル・データベース エンタープライズ・エディション バージョン 7 または DB2 ユニバーサル・データベース エンタープライズ拡張エディション。
- 分散データベース接続サービス (DDCS) バージョン 2 リクエスター。
AIX、HP-UX、OS/2、Solaris、Windows 3.1、Windows 3.11 for Workgroups、Windows 95、または Windows NT、および SCO、SGI、または SINIX 上で実行できます。
- OS/400 リクエスター。
- DB2 (VM 版) リクエスター。
- DRDA アプリケーション・リクエスター・プロトコルをサポートする他のすべての製品。

DB2 (MVS/ESA 版) アプリケーション・サーバーに接続されたアプリケーション・リクエスターの場合、DB2 (MVS/ESA 版) アプリケーション・サーバーは以下のようにデータベース・アクセスをサポートします。

- アプリケーション・リクエスターは、DB2 (MVS/ESA 版) アプリケーション・サーバーに保管された表にアクセスすることが許されています。アプリケーション・リクエスターが DB2 (MVS/ESA 版) アプリケーション・サーバーでパッケージを作成してからでなければ、アプリケーションを実行することはできません。DB2 (MVS/ESA 版) アプリケーション・サーバーは、実行時にアプリケーションの SQL ステートメントを探すのにこのパッケージを使用します。
- アプリケーション・リクエスターは DB2 (MVS/ESA 版) アプリケーション・サーバーに、DRDA リクエスターとサーバーとの接続が 2 フェーズ・コミット処理をサポートしない場合、アクセスが読み取り専用で制限されることを知らせることができます。たとえば、CICS フロントエンドの付いた DB2 (MVS/ESA 版) V2R3 リクエスターは、更新が許可されていないということを DB2 (MVS/ESA 版) アプリケーション・サーバーに通知できます。
- アプリケーション・リクエスターはさらに、システム主導アクセスを使用するネットワーク内の他の DB2 (MVS/ESA 版) システムに保管されているテーブルへのアクセスを許可されることもあります。システム主導アクセスによって、アプリケーション・リクエスターが単一の作業単位で複数のデータベース・システムに接続を確立できるようになります。

ネットワーク情報の提供

DB2 (MVS/ESA 版) アプリケーション・サーバーが適正に分散データベース要求を処理するためには、次のステップを踏む必要があります。

1. アプリケーション・サーバーをローカルのコミュニケーション・マネージャーに定義する。
2. 使用される可能性のある各 2 次サーバーの宛先を定義し、DB2 (MVS/ESA 版) アプリケーション・サーバーが SQL 要求を最終的な宛先に再経路指定できるようにする。
3. 必要な機密保護を提供する。
4. データ表示を提供する。

アプリケーション・サーバーを定義する

アプリケーション・サーバーが分散データベース要求を受信するためには、これをローカルなコミュニケーション・マネージャーに定義し、固有の RDB_NAME 名を割り当てる必要があります。アプリケーション・サーバーを正しく定義するには、次のステップを踏む必要があります。

1. DB2 (MVS/ESA 版) アプリケーション・サーバーが使用する LU 名と RDB_NAME を選択する。これらの名前を DB2 (MVS/ESA 版) と VTAM に記録するプロセスは、9ページの『ローカル・システムの定義』に説明されているプロセスと同じです。DB2 (MVS/ESA 版) のために選択する RDB_NAME を、アプリケーション・サーバーへのコネクティビティーが必要なすべてのエンド・ユーザーおよびアプリケーション・リクエスターに供給しなければなりません。
2. アクセスの必要なアプリケーション・リクエスターごとに NETID.LUNAME 値を DB2 (MVS/ESA 版) アプリケーション・サーバーに登録して、アプリケーション・リクエスターが SNA 要求を DB2 (MVS/ESA 版) サーバーに経路指定できるようにします。アプリケーション・リクエスターがダイナミック・ネットワーク・ルーティングを実行できる場合でも、そのようにしてください。アプリケーション・リクエスターは NETID.LUNAME を知らないとダイナミック・ネットワーク・ルーティングを使用できないからです。
3. DRDA 省略時 TPN (X'07F6C4C2') を各アプリケーション・リクエスターに指定します。DB2 (MVS/ESA 版) が自動的にこの値を使用するためです。
4. アプリケーション・リクエスターで要求された各モード名ごとに、VTAM モード表に項目を作成します。これらの項目は、各モード名の RU サイズ、歩調合わせウィンドウ・サイズ、およびサービス・クラスを記述します。
5. DB2 (MVS/ESA 版) アプリケーション・サーバーに接続するアプリケーション・リクエスターに、セッション限度を定義します。VTAM APPL ステ

ートメントは、すべてのパートナー・システムにあてはまる省略時のセッション限度を定義します。特定のパートナーに対して固有の省略時値を設定したい場合は、通信データベース (CDB) の SYSIBM.SYSLUMODES 表を使用できます。

VTAM ネットワークを調べる方法については、20ページの『RU サイズおよび歩調合わせの設定』を参照してください。

6. DB2 (MVS/ESA 版) アプリケーション・サーバーへの接続が許可されたアプリケーション・リクエスターを識別するための項目を DB2 (MVS/ESA 版) CDB に作成します。ネットワーク内のアプリケーション・リクエスター用に CDB 項目を定義する 2 つの基本的な方法は、以下のとおりです。
 - a. CDB で特に記述されていない、任意の LU に使用する省略時値を指定する行を SYSIBM.SYSLUNAMES に挿入できます (省略時の行は LUNAME 列がブランクです)。この方法では、ネットワーク内のいくつかの LU に対しては特定の属性を与え、一方、他のすべての LU については省略時値を設定できます。

たとえば、DALLAS システム (別の DB2 (MVS/ESA 版) システム) には検査済み分散データベース要求 (LU 6.2 SECURITY=SAME) を送信することを許可する一方で、データベース・マネージャー・システムにはパスワードを送信させるということができます。さらに、特にデータベース・マネージャー・システムが多数ある場合などは、システムごとに CDB に項目を作成したくない場合もあります。図10 では、DALLAS システムに対して SECURITY=SAME を指定する一方、他のすべてのリクエスターに対しては SECURITY=PGM にさせるために CDB を使用する方法を示します。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

図 10. アプリケーション・リクエスター接続の省略時値の確立

- b. CDB を次のいずれかに設定することにより、CDB を使用してネットワーク内の各アプリケーション・リクエスターに個別に許可を与えることができます。
 - SYSIBM.SYSLUNAMES 中に省略時の行を記録しないようにする。省略時の行 (LU 名がブランクの行) が存在しない場合、DB2 (MVS/ESA 版) は、接続しようとする各アプリケーション・リクエ

ターの LU 名を含んだ SYSIBM.SYSLUNAMES 中の行を必要とします。対応する行が CDB に見つからない場合、アプリケーション・リクエストはアクセスを拒否されます。

- SYSIBM.SYSLUNAMES に、come-from 検査が必要であることを指定した省略時の行を記録する (USERNAMES 列を 'I' または 'B' に設定)。これにより、37ページの『Come-From 検査』で説明されているように、DB2 (MVS/ESA 版) はアクセスをアプリケーション・リクエストおよび SYSIBM.SYSUSERNAMES 表で定義されたエンド・ユーザーに限定します。名前変換規則が SYSIBM.SYSLUNAMES 中にブランク LU 名の行を必要とするものの、この行の使用によって DB2 (MVS/ESA 版) が DB2 (MVS/ESA 版) アプリケーション・サーバーへの無制限なアクセスを許可するにはしたくない場合、この方法を使用できます。

図11 では、LUNAME 列にブランクの行はないため、DB2 (MVS/ESA 版) は LUDALLAS または LUNYC 以外の LU へのアクセスをすべて拒否します。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

図 11. 個々のアプリケーション・リクエスト接続の識別

2 次サーバーの定義

DB2 (MVS/ESA 版) では、DRDA に定義したデータベース・サーバーを実装していません。その代わりに、DB2 (MVS/ESA 版) では 2 次サーバーを使用できます。これは、システム主導アクセスを使って単一の作業単位の範囲で複数の DB2 (MVS/ESA 版) システムにアクセスすることを可能にします。

SQL の相違: システム主導アクセスで主導サポートされる SQL は、DRDA リモート作業単位の場合と大いに異なります。

- 2 次サーバーへの接続を確立する場合、SQL CONNECT ステートメントを使用しません。その代わりに、3 つの部分からなる SQL オブジェクト名を指定してサーバーにアクセスします。たとえば、次の SQL ステートメントは CHICAGO というシステム主導アクセス・サーバーに経路指定されます。

```
SELECT * FROM CHICAGO.USER.TABLE;
```

- SQL DDL ステートメント (CREATE など) は許可されていません。

- システム主導アクセスではリモート・バインド (BIND PACKAGE など) をサポートしていません。したがって、アプリケーションを実行する前に、アプリケーションをシステム主導アクセス・サーバーでバインドする必要はありません。
- 2 次サーバーに送信する SQL ステートメントは静的でも動的でもかまいませんが、すべてのステートメントは動的に発行されます。これは、2 次サーバーがアプリケーションの SQL ステートメントを含んだプランまたはパッケージを持っておらず、サーバーがデータベース・アクセス・パスを前もって選択することが不可能であるためです。
- 単一の SQL アプリケーションは、複数の 2 次サーバーに同時にアクセスできます。
- 所定のコミットの範囲内で、複数の DB2 (MVS/ESA 版) システムを SQL の更新のターゲットとすることができます。
- アプリケーションは、単一のコミットの範囲内で 2 次サーバーへの複数の LU 6.2 会話を使用できます。DB2 (MVS/ESA 版) アプリケーション・サーバーは通常、読み取り専用の SQL 照会ごとに 1 つの LU 6.2 会話を作成します。これにより、2 次サーバーは SQL アプリケーションの FETCH 要求を前もって予測し、アプリケーションが実際に要求を出す前に応答セットを送信できるようになります。

SQL オブジェクト名: DB2 (MVS/ESA 版) アプリケーション・サーバーは、SQL 要求を受け取るとオブジェクト名を調べて、オブジェクトがネットワークのどこに位置しているかを判別します。DB2 (MVS/ESA 版) は、1 つの部分からなる SQL オブジェクト名、2 つの部分からなる SQL オブジェクト名、3 つの部分からなる SQL オブジェクト名のいずれも受け入れます。それぞれ名前形式は次のようになります。

objectname DB2 (MVS/ESA 版) の表、視点、シノニム、別名の名前を指定します。

authid.objectname オブジェクトの所有者とオブジェクト名を指定します。

location.authid.objectname 所有者のシステム、所有ユーザー、およびオブジェクトの名前を指定します。

ロケーション名 (3 つの部分からなるオブジェクト名の最初の部分) がローカルな DB2 (MVS/ESA 版) システムの RDB_NAME と一致する場合、要求はローカルな DB2 (MVS/ESA 版) オブジェクトを識別します。

ロケーション名がローカルな DB2 (MVS/ESA 版) システムの RDB_NAME と一致しない場合、DB2 (MVS/ESA 版) アプリケーション・サーバーは、シス

システム主導アクセスを使用して、ロケーション名によって識別されるシステムに要求を再経路指定します。システム主導アクセスは DB2 (MVS/ESA 版) システム間でのみサポートされるため、ターゲット・システムは別の DB2 (MVS/ESA 版) システムでなければなりません。システム主導アクセスはリモート・バインド機能をサポートしないため、アプリケーションを実行前にサーバーでバインドする必要はありません。35ページの図12 は、DB2 (MVS/ESA 版) が SQL オブジェクト名を解決するのに使用するプロセスを要約しています。

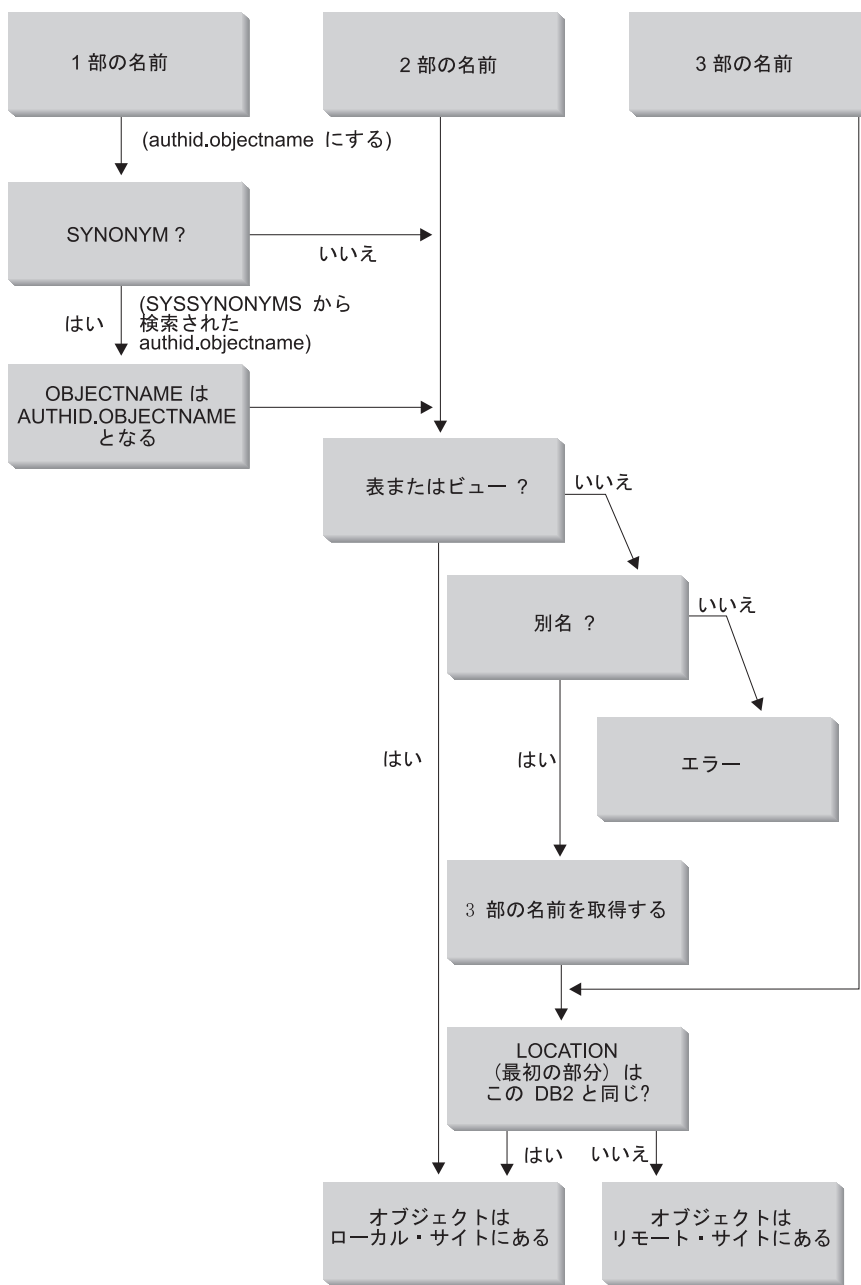


図 12. DB2 (MVS/ESA 版) SQL オブジェクト名の解決

サーバー定義: DB2 (MVS/ESA 版) アプリケーション・サーバーが SQL を再経路指定する場合、CDB および VTAM に各 2 次サーバーを定義する必要があります。定義のプロセスは、15ページの『リモート・システムの定義』に説明されているプロセスとよく似ています。2 次サーバーを接続するには、次の手順に従ってください。

1. 各サーバーの RDB_NAME と LU 名値を CDB および VTAM に記録する。システム主導アクセスで使用される TPN 値は、DRDA の省略時値と異なります。しかし、DB2 (MVS/ESA 版) は自動的に正しい値を選択するので、この相違は重要ではありません。
2. 2 次サーバーごとに機密保護要件を SYSIBM.SYSLUNAMES に定義する。このプロセスについては、21ページの『機密保護の提供』に説明されています。
3. DB2 (MVS/ESA 版) アプリケーション・サーバーと 2 次サーバーの間で使用されるモード名 (複数の場合もある) を定義し、これらのモード名を VTAM モード表に入れる。省略時解釈モード名は IBMDB2LM です。
4. 各 2 次サーバーのセッション限度を定義する。セッション限度を確立するためのプロセスは、9ページの『ローカル・システムの定義』に説明されているプロセスと同じです。しかし、システム主導アクセスの場合、SQL アプリケーションごとに複数の会話を確立できます。システム主導アクセス接続の場合は、DRDA 接続の場合に比べてセッション限度を高く設定する必要がありますかもしれません。システム主導アクセス・アプリケーションに必要な LU 6.2 セッションの数を計算する方法の詳細については、DB2 管理の手引きの『分散データベース』を参照してください。

データベース資源の所有者として、2 次サーバーはそこにある SQL オブジェクトのデータベース機密保護を制御します。ただしこの責任は、要求を出す DB2 (MVS/ESA 版) アプリケーション・サーバーと共有されます。サーバーは SQL オブジェクトに対するアクセスを次のように制御します。

- 2 次サーバーは DB2 (MVS/ESA 版) プランのコピーを持っていないので、エンド・ユーザーが要求側のシステム (アプリケーション・サーバー) でパッケージを実行する許可を得ているかどうかの検査は、要求側の DB2 (MVS/ESA 版) アプリケーション・サーバーに依存します。
- 静的 SQL ステートメントは 2 次サーバーで動的に実行されますが、そのときには、要求側の DB2 (MVS/ESA 版) アプリケーション・サーバーで DB2 (MVS/ESA 版) パッケージの所有者に付与されている特権が使用されます。
- 動的 SQL ステートメントはアプリケーション・リクエスターでエンド・ユーザーに与えられた特権を使用して実行されます。

機密保護の提供

アプリケーション・リクエスターが分散データベース要求を DB2 (MVS/ESA 版) アプリケーション・サーバーに向けるときには、以下の機密保護上の考慮事項が関係します。

- come-from 検査
- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護

Come-From 検査

DB2 (MVS/ESA 版) アプリケーション・サーバーがエンド・ユーザー名をアプリケーション・リクエスターから受け取る場合、アプリケーション・サーバーは指定されたアプリケーション・リクエスターから受け取るエンド・ユーザー名を制限できます。これは *come-from* 検査を使用することで行えます。

come-from 検査を使用すると、アプリケーション・サーバーは、所定のユーザー ID が特定のパートナーだけに使用されるよう指定できます。たとえば、アプリケーション・サーバーは JONES を DALLAS だけ「から来る (*come-from*)」よう制限できます。(DALLAS 以外の) 別のアプリケーション・リクエスターが名前 JONES をアプリケーション・サーバーに送ろうとする場合、アプリケーション・サーバーはその名前が適正なネットワーク・ロケーションから来なかったために要求を拒否できます。

DB2 (MVS/ESA 版) は *come-from* 検査をインバウンド・エンド・ユーザー名前変換の一部として実装しています。これについては次の節で説明します。

エンド・ユーザー名の選択

アプリケーション・リクエスターによって渡されるユーザー ID は、SNA ネットワーク全体で一意ではないことがあります。DB2 (MVS/ESA 版) アプリケーション・サーバーはインバウンド名前変換を実行して、SNA ネットワーク全体を通じて固有なエンド・ユーザー名を作成する必要があるかもしれません。同様に、DB2 (MVS/ESA 版) アプリケーション・サーバーはアウトバウンド名前変換を実行して、アプリケーションに関係する 2 次サーバーに対して固有なエンド・ユーザー名を与える必要があるかもしれません。(アウトバウンド・エンド・ユーザー名前変換については、21ページの『機密保護の提供』を参照してください。)

インバウンド名前変換は、SYSIBM.SYSLUNAMES 表の USERNAMES 列を 'I' (インバウンド変換) または 'B' (インバウンドおよびアウトバウンド両方の

変換) に設定することにより、使用可能にできます。インバウンド名前変換が有効であるとき、DB2 (MVS/ESA 版) はアプリケーション・リクエスターによって送られたユーザー ID を変換して、DB2 (MVS/ESA 版) は所有者の名前を立案します (アプリケーション・リクエスターが別の DB2 (MVS/ESA 版) システムである場合)。

アプリケーション・リクエスターがユーザー ID およびパスワードの両方を APPC ALLOCATE verb に関して送る場合、ユーザー ID およびパスワードはユーザー ID が変換される前に妥当性検査されます。

SYSIBM.SYSUSERNAMES の PASSWORD 列は、パスワード妥当性検査には使用されません。代わりに、ユーザー ID とパスワードが妥当性検査のため、外部機密保護システム (RACF または RACF と同等の製品) に送られます。

ALLOCATE verb の着信ユーザー ID が検査されるとき、DB2 (MVS/ESA 版) は許可出口ルーチンを持ちます。これは、2 次 AUTHID のリストを提供し、追加の機密保護検査を実行するために使用できます。詳細については、*DB2 管理の手引き* を参照してください。

インバウンド名前変換処理は SYSIBM.SYSUSERNAMES 表の中の行を検索しますが、これは以下の優先順位リスト (TYPE.AUTHID.LUNAME) のうちのパターンの 1 つと一致しなければなりません。

1. I.AUTHID.LUNAME — 特定のアプリケーション・リクエスターからの特定のエンド・ユーザー
2. I.AUTHID.blank — 任意のアプリケーション・リクエスターからの特定のエンド・ユーザー
3. I.blank.LUNAME — 特定のアプリケーション・リクエスターからの任意のエンド・ユーザー

行が検出されない場合、リモート・アクセスは拒否されます。行が検出されると、リモート・アクセスが許可され、エンド・ユーザー名は NEWAUTHID 列で与えられた値に変換されます。NEWAUTHID 値がブランクの場合は名前が変更されないことを示します。任意の DB2 (MVS/ESA 版) 資源に対する許可の検査 (たとえば、SQL 表特権) が、DB2 (MVS/ESA 版) により、元のユーザー名ではなく変換されたエンド・ユーザー名に対して実行されます。

DB2 (MVS/ESA 版) アプリケーション・サーバーがアプリケーション・リクエスターからエンド・ユーザー名を受け取る場合、DB2 (MVS/ESA 版) インバウンド名前変換機能を使用することによって以下のいくつかの目的が達成されます。

- エンド・ユーザー名を固有のものに変更できる。たとえば、以下の SQL ステートメントは、NEWYORK アプリケーション・リクエスター (LUNAME LUNYC) のエンド・ユーザー名 JONES を異なった名前 (NYJONES) に変換します。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
  VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', '');
```

- エンド・ユーザー名を変更して、エンド・ユーザーのグループをすべて単一の名前で表現できる。たとえば、NEWYORK アプリケーション・リクエスター (LUNAME LUNYC) からのすべてのユーザーをユーザー名 NYUSER で表現したいとします。そうすると、NYUSER という名前に対して SQL 特権を認可することにより、NEWYORK のユーザーに付与する SQL アクセスを制御できるようになります。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
  VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', 'NYUSER', '');
```

- 特定のアプリケーション・リクエスターから送られてくるエンド・ユーザーを制限することができます。エンド・ユーザー名前変換のこの使用法により、37ページの『Come-From 検査』で説明した come-from 検査を実行できます。たとえば、以下の SQL ステートメントは NEWYORK アプリケーション・リクエスターのエンド・ユーザーとして SMITH および JONES だけを許可します。その他の名前は、SYSIBM.SYSUSERNAMES 表にリストされていないため、アクセスが拒否されます。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
  VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');
```

- DB2 (MVS/ESA 版) アプリケーション・サーバーへの接続が許可されるアプリケーション・リクエスターを制限できます。これは come-from 検査のさらにもう 1 つの機能です。以下の例では、NEWYORK アプリケーション・

リクエスター (LUNYC) または CHICAGO アプリケーション・リクエスター (LUCHI) によって送られるエンド・ユーザーだけが受け入れられます。省略時の SYSIBM.SYSLUNAMES 行がすべてのインバウンド要求に対してインバウンド名前変換を指定しているため、その他のアプリケーション・リクエスター名はアクセスを拒否されます。

```
INSERT INTO SYSIBM.SYSLUNAMES
  (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
VALUES (' ', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUCHI', ' ', ' ');
```

ネットワーク機密保護の提供

LU 6.2 は、主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護
- 会話レベル機密保護
- 暗号化

24ページの『ネットワーク機密保護』では、DB2 (MVS/ESA 版) でのセッション・レベル機密保護および暗号化について説明しています。DB2 (MVS/ESA 版) アプリケーション・サーバーは、DB2 (MVS/ESA 版) アプリケーション・リクエスターとまったく同様に、セッション・レベルの機密保護および暗号化を使用します。

残りのネットワーク機密保護の考慮事項は、SNA 会話レベル機密保護だけです。会話レベル機密保護のいくつかの面は DB2 (MVS/ESA 版) アプリケーション・サーバー独自のものです。DB2 (MVS/ESA 版) アプリケーション・サーバーはネットワーク機密保護において 2 つの異なった役割を果たします。

- 2次サーバーへのリクエスターとして、DB2 (MVS/ESA 版) アプリケーション・サーバーは 2次サーバーが必要とする SNA 会話レベル機密保護パラメーターを含んだ APPC 要求を発行する責任があります。DB2 (MVS/ESA 版) アプリケーション・サーバーは SYSIBM.SYSLUNAMES 表の SYSUSERNAMES 列、および SYSIBM.SYSUSERNAMES 表を使用して、各 2次サーバーごとに SNA 会話レベル機密保護要件を定義します。これらの定義の詳細については、24ページの『ネットワーク機密保護』で説明した内容と同一です。
- アプリケーション・リクエスターのサーバーとして、DB2 (MVS/ESA 版) アプリケーション・サーバーはアプリケーション・リクエスターの SNA 会

話レベル機密保護要件を指定します。 DB2 (MVS/ESA 版) は SYSIBM.SYSLUNAMES 表の USERSECURITY 列を使用して、ネットワーク内の各アプリケーション・リクエスターに必要な会話機密保護を判別します。以下の値が USERSECURITY 列で使用されます。

C これは、 DB2 (MVS/ESA 版) には分散データベースごとにアプリケーション・リクエスターがユーザー ID およびパスワード (LU 6.2 SECURITY=PGM) を送る必要があることを示しています。 SYSIBM.SYSLUNAMES の ENCRYPTPSWDS 列に 'Y' が含まれる場合、 DB2 (MVS/ESA 版) はパスワードが RACF 暗号化形式で準備されている (これは DB2 (MVS/ESA 版) アプリケーション・リクエスターの場合にのみ可能) と想定します。 ENCRYPTPSWDS 列が 'Y' でない場合、 DB2 (MVS/ESA 版) はパスワードが標準 LU 6.2 形式 (EBCDIC 文字表示) になっているものとみなします。どちらの場合でも、 DB2 (MVS/ESA 版) はユーザー ID とパスワード値を妥当性検査のために機密保護サブシステムに渡します。 APPC ユーザー ID とパスワード検査を行える機密保護サブシステムが必要となります。たとえば、RACF には APPC ユーザー ID とパスワードの検査を行う機能があります。機密保護サブシステムがユーザー ID とパスワードの対を拒否した場合、分散データベース・アクセスは拒否されます。

その他の値

これは、アプリケーション・リクエスターが検査済みユーザー ID (LU 6.2 SECURITY=SAME) またはユーザー ID とパスワード (LU 6.2 SECURITY=PGM) のいずれかを送信できることを示しています。ユーザー ID とパスワードが送信されると、 DB2 (MVS/ESA 版) はそれらを 'C' について上記で述べたのと同様の方法で処理します。要求がユーザー ID のみを含んでいる場合、インバウンド・ユーザー ID が管理されるために SYSUSERNAMES 表が使用されるのでない限り、機密保護サブシステムが呼び出されて、ユーザーの認証がなされます。

機密保護違反が検出された場合、 LU 6.2 は DB2 (MVS/ESA 版) アプリケーション・サーバーが SNA 機密保護違反センス・コード (080F6051'X) をアプリケーション・リクエスターに送るようにします。このセンス・コードは障害の原因を示すものではないので、 DB2 (MVS/ESA 版) は 2 つの方式で分散機密保護違反の原因を記録します。

- DSNL030I メッセージを生成する。これには、リクエスターの LUWID、および障害を記述する DB2 理由コードが示されます。DSNL030I には (分かる場合には) AUTHID も含まれます。これは拒否されたアプリケーション要求から送信されたものです。
- NETVIEW ハードウェア・モニター・データベースにアラートが記録される。この中には、DSNL030I メッセージに示されるのと同じ情報が収められます。

データベース・マネージャー機密保護

データベース資源の所有者として、DB2 (MVS/ESA 版) アプリケーション・サーバーは、そこにある SQL オブジェクトに対してデータベース機密保護機能を制御します。DB2 (MVS/ESA 版) が管理するオブジェクトへのアクセスは、特権によって制御されます。これは、DB2 (MVS/ESA 版) 管理者または個々のオブジェクトの所有者によって、ユーザーに与えられます。DB2 (MVS/ESA 版) アプリケーション・サーバーが制御する 2 つの基本的なオブジェクトのクラスは以下のとおりです。

- **パッケージ** — 個々のエンド・ユーザーは、DB2 (MVS/ESA 版) GRANT ステートメントを使用して、パッケージの作成、置換、実行を行う権限を持っています。エンド・ユーザーがパッケージを所有する場合、そのユーザーは自動的にパッケージの実行または置換を行うことができます。他のエンド・ユーザーは DB2 (MVS/ESA 版) アプリケーション・サーバーの GRANT ステートメントで、パッケージを実行するよう許可を受ける必要があります。USE は、個々のエンド・ユーザーまたは PUBLIC に認可することができます。PUBLIC は、パッケージの実行をすべてのエンド・ユーザーに許可します。

アプリケーションが DB2 (MVS/ESA 版) にバインドされる時、パッケージにはアプリケーション・プログラムに含まれる SQL ステートメントが含まれています。これらの SQL ステートメントは以下のように分けられます。

静的 SQL

静的 SQL は、SQL ステートメントおよびそのステートメントにより参照される SQL オブジェクトが、アプリケーションが DB2 (MVS/ESA 版) にバインドされる時に認識されることを意味します。パッケージの作成者は、パッケージ内のそれぞれの静的 SQL ステートメントを実行する権限を持っていない限りなりません。

エンド・ユーザーがパッケージを実行する権限を与えられるとき、そのユーザーはパッケージに含まれる各静的 SQL ステートメントを実行する権限を自動的に与えられます。それで、実行されるパッケ

ージに静的 SQL ステートメントしか含まれていない場合には、エンド・ユーザーは DB2 (MVS/ESA 版) 表特権を必要としません。

動的 SQL

動的 SQL は、プログラムが実行するまで認識されない SQL ステートメントのことです。言い換えると、SQL ステートメントはプログラムによって作成され、SQL PREPARE ステートメントを使用して DB2 (MVS/ESA 版) に動的にバインドされます。エンド・ユーザーが動的 SQL ステートメントを実行するとき、そのユーザーには SQL ステートメントを実行するために必要な表特権がなければなりません。プランまたはパッケージが作成されるときに SQL ステートメントが認識されないため、エンド・ユーザーにはパッケージ所有者により必要な権限が自動的に与えられません。

- **SQL オブジェクト** — これは表、視点、シノニム、または別名です。DB2 (MVS/ESA 版) ユーザーには、個々の SQL オブジェクトを作成、削除、変更、または読み取る権限の各種のレベルを認可できます。この権限は、静的 SQL ステートメントをバインドしたり、動的 SQL ステートメントを実行するために必要です。

パッケージを作成するとき、DISABLE/ENABLE オプションによって、どの DB2 (MVS/ESA 版) 接続タイプがパッケージを実行できるか制御することができます。RACF および DB2 (MVS/ESA 版) 機密保護出口ルーチンを使用して、エンド・ユーザーに選択的に DDF の使用を許可できます。RLF を使用して、リモート・バインドおよび動的 SQL 実行のプロセッサ時間を制限できます。

MYPKG という名前の DB2 (MVS/ESA 版) パッケージについて考慮します。これは JOE が所有しているものとします。JOE は SAL に対して、DB2 (MVS/ESA 版) GRANT USE ステートメントを発行することにより、このパッケージの実行を許可できます。SAL がこのパッケージを実行すると、以下の事柄が発生します。

- DB2 (MVS/ESA 版) は SAL がこのパッケージに対する USE 権限を与えられているかどうか検査します。
- JOE はパッケージの作成に必要な SQL オブジェクト特権を持っているので、SAL はパッケージ中のすべての静的 SQL ステートメントを発行することができます。
- パッケージが動的 SQL ステートメントを含んでいる場合は、SAL は自分自身の SQL 表特権を持っている必要があります。たとえば、SAL は JOE.TABLE5 への読み取りアクセスを認可されていない限り、SELECT * FROM JOE.TABLE5 を発行することはできません。

機密保護サブシステム

DB2 (MVS/ESA 版) アプリケーション・サーバーの機密保護サブシステム (RACF または RACF と同等の製品) の使用法は、SYSIBM.SYSLUNAMES 表でインバウンド名前変換機能をどのように定義したかに応じて異なります。

- USERNAMES 列に 'I' または 'B' を指定した場合、インバウンド名前変換はアクティブになり、DB2 (MVS/ESA 版) は DB2 (MVS/ESA 版) 管理者がインバウンド名前変換を使用してシステム機密保護制約を部分的に実施するものとみなします。外部機密保護サブシステムが呼び出されるのは、アプリケーション・リクエスターがユーザー ID およびパスワードの両方を含む要求を送る場合だけです。APPC ユーザー ID とパスワード検査を行える機密保護サブシステムが必要となります。たとえば、RACF には APPC ユーザー ID とパスワードの検査を行う機能があります。

アプリケーション・リクエスターからの要求にユーザー ID (SECURITY=SAME) だけが含まれる場合、外部機密保護システムはまったく呼び出されません。インバウンド名前変換の規則によって、どのユーザーに DB2 (MVS/ESA 版) アプリケーション・サーバーへの接続が許可されているかが定義されているからです。

- 'I' または 'B' 以外の値が USERNAMES 列に指定されていた場合、以下の機密保護サブシステム検査が実行されます。
 - 分散データベース要求をアプリケーション・リクエスターから受け取った場合、DB2 (MVS/ESA 版) は外部機密保護システムを呼び出して、エンド・ユーザーのユーザー ID (供給された場合にはパスワードも) の妥当性検査を行います。
 - 外部機密保護システムが呼び出されて、エンド・ユーザーが DB2 (MVS/ESA 版) サブシステムへの接続を許可されているかどうか検査されます。
- どちらの場合も、許可出口ルーチンが駆動されて、2 次許可 ID のリストが与えられます。詳細については、DB2 管理の手引きを参照してください。

データの表示

ご使用の DB2 (MVS/ESA 版) サブシステムが、各アプリケーション・リクエスターの CCSID を DB2 (MVS/ESA 版) サブシステムのインストール・システムの CCSID に変換できるかどうか確認する必要があります。詳細については、28ページの『データの表示』を参照してください。

第2章 DRDA ネットワークでの DB2 ユニバーサル・データベース (OS/390 版) の接続

DB2 ユニバーサル・データベース (OS/390 版) は、OS/390 用の IBM 関係データベース管理システムです。この章は以前のリリースにはあてはまりません。1ページの『第1章 DRDA ネットワークでの DB2 (MVS/ESA 版) の接続』を参照してください。

この章では、(DB2 コネクトのような) DRDA アプリケーション・リクエスターが DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに接続する方法、および、他のシステム上の DB2 ユニバーサル・データベースのような DRDA アプリケーション・サーバーと通信できるように DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターを設定する方法を説明します。

この章では、SNA 接続を使用して非類似 DRDA システムを DB2 ユニバーサル・データベース (OS/390 版) に接続することに関する情報に重点が置かれています。しかし、DB2 ユニバーサル・データベース for OS/390 バージョン 5 では (AnyNet を使用しない) ネイティブな TCP/IP 接続を使用するデータベース通信のためのサポートも導入されているので、TCP/IP 接続の使用についてもある程度取り上げます。設定の使用方法および TCP/IP の使用方法に関する詳細は、*DB2 ユニバーサル・データベース (OS/390 版) インストレーションの手引き*、および *DRDA Support for TCPIP with DB2 Universal Database for OS/390 and DB2 Universal Database* を参照してください。

2 つの DB2 ユニバーサル・データベース (OS/390 版) システムを接続する方法、または DRDA 接続を DB2 ユニバーサル・データベース (OS/390 版) に定義する方法の詳細については、*DB2 ユニバーサル・データベース (OS/390 版) 管理の手引き* で分散データベースの接続に関する説明を参照してください。

注:

1. VTAM バージョン 4 リリース 2 の AnyNet 機能を使用すると、TCP/IP ネットワーク上で APPC を実行することができます。しかし、DB2 ユニバーサル・データベース for OS/390 V5.1 のユーザーは、TCP/IP を介した AnyNet APPC フィーチャーではなく、ネイティブの TCP/IP サポートを使用するようお勧めします。

2. この章には、DCE の使用についての情報は含まれていません。

DB2 ユニバーサル・データベース (OS/390 版)

図13 に、DB2 ユニバーサル・データベース (OS/390 版) の単一コピーを実行する OS/390 システムを示します。単一のシステムで、DB2 ユニバーサル・データベース (OS/390 版) の複数のコピーを実行することも可能です。所定のシステム内の DB2 ユニバーサル・データベース (OS/390 版) のコピーを識別するため (または JES complex 内の DB2 ユニバーサル・データベース (OS/390 版) のコピーを識別するため)、各 DB2 システムにはサブシステム名 が与えられています。これは 1~4 文字の、JES complex 内で固有の文字列です。図13 では DB2 ユニバーサル・データベース (OS/390 版) のサブシステム名は xxxx です。OS/390 アドレス空間のうちの 3 つについては、接頭部に DB2 ユニバーサル・データベース (OS/390 版) サブシステム名が付けられています。これらの 3 つのアドレス空間が DB2 ユニバーサル・データベース (OS/390 版) 製品を構成します。

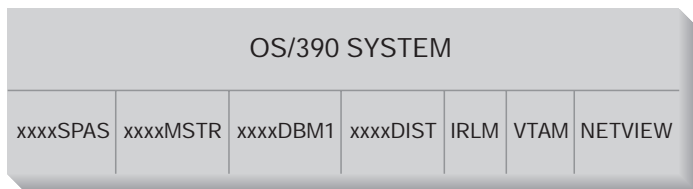


図13. DB2 ユニバーサル・データベース (OS/390 版) で使用される OS/390 アドレス空間

図13 は、DB2 ユニバーサル・データベース (OS/390 版) の分散データベース処理に関する OS/390 アドレス空間を示しています。これらのアドレス空間は、DB2 ユニバーサル・データベース (OS/390 版) ユーザーがローカル関係データベースにアクセスしたり、リモート DRDA システムと通信したりできるように、協働します。各アドレス空間の目的は次のとおりです。

xxxxSPAS

DB2 ストアード・プロシージャ・アドレス空間。

xxxxMSTR

DB2 ユニバーサル・データベース (OS/390 版) 製品のシステム・サービス・アドレス空間。DB2 ユニバーサル・データベース (OS/390 版)

の始動と停止、DB2 ユニバーサル・データベース (OS/390 版) へのローカル・アクセスの制御を受け持ちます。

xxxxDBM1

データベース・サービス・アドレス空間。DB2 ユニバーサル・データベース (OS/390 版) によって制御される関係データベースへのアクセスを受け持ちます。ここでは、SQL アプリケーション・プログラムのためにデータベース資源への入出力が行われます。

xxxxDIST

DB2 ユニバーサル・データベース (OS/390 版) の、分散データベース機能を提供する部分。分散データ機能 (DDF) とも言います。DDF は、分散データベース要求を受け取ると、必要なデータベース入出力を行えるよう、その要求を xxxxDBM1 に渡します。

IRLM DB2 ユニバーサル・データベース (OS/390 版) が使用するロック・マネージャー。データベース資源へのアクセスを制御します。

VTAM IBM Communications Server for OS/390 の SNA 機能 (VTAM)。DDF は SNA または TCP/IP を使用して、DB2 ユニバーサル・データベース (OS/390 版) のために分散データベース通信を行います。この図では、TCP/IP アドレス空間は示されていません。

NETVIEW

OS/390 システム上の、ネットワーク管理フォーカル・ポイント製品。分散データベースの処理中にエラーが発生すると、DDF は NetView ハードウェア・モニター・データベースにエラー情報 (警報 とも言う) を記録します。システム管理者は、ハードウェア・モニター・データベースに保管されたエラーを NetView を使って調べたり、あるいは警報条件が記録されると自動的に起動するコマンド・プロシーチャーを用意したりすることができます。

NetView は、VTAM 通信エラーの診断にも使用できます。詳細は、分散関係データベース 問題判別の手引き を参照してください。

46ページの図13 には SQL アプリケーション・プログラムは示されていません。アプリケーション・プログラムが DB2 を使用して SQL ステートメントを発行する場合、このアプリケーション・プログラムを以下のいずれかの方法で DB2 ユニバーサル・データベース (OS/390 版) 製品と接続しなければなりません。

TSO TSO にログオンするバッチ・ジョブとエンド・ユーザーは、TSO 接続機能によって DB2 ユニバーサル・データベース (OS/390 版) と接

続します。これは、SPUFI および大部分の QMF アプリケーションを DB2 ユニバーサル・データベース (OS/390 版) に接続するのに用いる手法です。

CICS/ESA

CICS/ESA アプリケーションが SQL 呼び出しを発行する場合、CICS/ESA 製品は CICS/ESA 接続インターフェースを使用して SQL 要求を DB2 ユニバーサル・データベース (OS/390 版) に経路指定します。

IMS/ESA

IMS/ESA の制御下で実行されるトランザクションは、IMS 接続インターフェースを使用して SQL ステートメントを DB2 ユニバーサル・データベース (OS/390 版) に渡し、これを処理します。

DDF 分散データ機能は、分散アプリケーションを DB2 ユニバーサル・データベース (OS/390 版) に接続します。

CAF 呼び出し接続機能を使用すると、ユーザー作成のサブシステムを直接 DB2 ユニバーサル・データベース (OS/390 版) に接続できます。

DB2 ユニバーサル・データベース (OS/390 版) インプリメンテーション

DRDA は、分散データベース管理システム機能のタイプを定義します。DB2 ユニバーサル・データベース (OS/390 版) はリモート作業単位をサポートしています。リモート作業単位を使用すると、あるシステムで実行されているアプリケーション・プログラムは、1 つのリモート DBMS のデータにアクセスできます。そのときにはそのリモート DBMS が提供する SQL を使用します。

DB2 ユニバーサル・データベース (OS/390 版) は、分散作業単位もサポートしています。分散作業単位を使用すると、あるシステムで実行されているアプリケーション・プログラムは、複数のリモート DBMS のデータにアクセスできます。そのときには各リモート DBMS が提供する SQL を使用します。

DRDA で定義される分散のタイプの詳細については、分散関係データベース体系 *接続の手引き* を参照してください。

50ページの図14 に示されているとおり、DB2 ユニバーサル・データベース (OS/390 版) は 2 種類のアクセス方式を使用して、3 種類の分散データベース接続構成をサポートしています。

[1] システム主導アクセス (DB2 ユニバーサル・データベース (OS/390 版) プライベート・プロトコル を使用するアクセスとしても知られている) により、DB2 ユニバーサル・データベース (OS/390 版) リクエストは 1 つ以上の DB2 ユニバーサル・データベース (OS/390 版) サーバーに接続

することができます。DB2 ユニバーサル・データベース (OS/390 版) リクエスターとサーバーとの間に確立される接続は、DRDA で定義されたプロトコルに適合しないため、非 DB2 ユニバーサル・データベース (OS/390 版) 製品を DB2 ユニバーサル・データベース (OS/390 版) に接続するには使用できません。このタイプの接続は、3 つの部分からなる名前または別名をアプリケーションにコーディングすることによって確立されます。

[2] アプリケーション主導アクセス では、DB2 ユニバーサル・データベース (OS/390 版) リクエスターまたは非 DB2 ユニバーサル・データベース (OS/390 版) リクエスター (DB2 コネクトなど) を、1 つ以上の DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーまたは非 DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバー、たとえば DB2 ユニバーサル・データベースや DB2 ユニバーサル・データベース (AS/400 版) などに接続できます。アプリケーション・リクエスターに一度に接続できるアプリケーション・サーバーの数は、アプリケーション・リクエスターの DB2 ユニバーサル・データベース (OS/390 版) のレベルに応じて異なります。アプリケーション・リクエスターが DB2 (MVS/ESA 版) V2R3 であれば、一度に 1 つだけアプリケーション・サーバーを接続できます。このタイプの接続は、SQL CONNECT ステートメントをアプリケーションにコーディングすることによって確立されます。アプリケーション・リクエスターが DB2 (MVS/ESA 版) V3R1 以降であれば、一度に 1 つ以上のアプリケーション・サーバーを接続できます。

[3] アプリケーション主導およびシステム主導アクセスを一緒に使用して接続を確立できます。DRDA とシステム主導記憶域を同一のスレッドの中で使用して接続することはできません。

2 次サーバー という用語は、アプリケーション・サーバーのサーバーとして機能するシステムを指して用いられます。

構成の中に含まれるすべてのシステムが 2 フェーズ・コミットをサポートしている場合、分散作業単位 (複数サイト読み取りと複数サイト更新) がサポートされます。すべてのシステムが 2 フェーズ・コミットをサポートしているわけではない場合、作業単位内での更新は、2 フェーズ・コミットをサポートしない単一のサイト、または 2 フェーズ・コミットをサポートするサイトのサブセットのいずれかに制限されます。

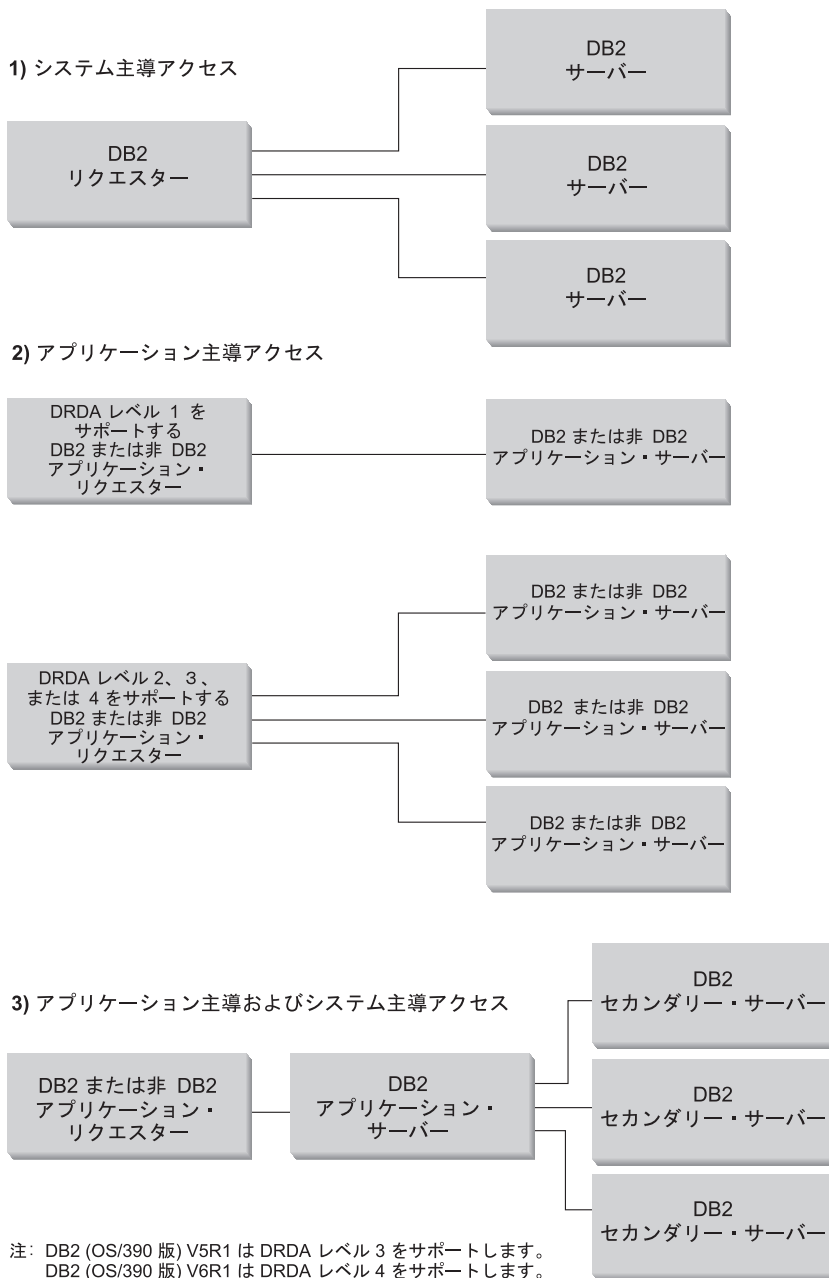


図 14. DB2 ユニバーサル・データベース (OS/390 版) 分散接続

表2 は、DB2 ユニバーサル・データベース (OS/390 版) 分散データベースの接続タイプを比較したものです。

表2. DB2 ユニバーサル・データベース (OS/390 版) 分散データベースの接続の比較

[1] システム主導アクセス	[2] アプリケーション主導アクセス (すべてのシステムが 2 フェーズ・コミットをサポートする場合)	[3] アプリケーション主導およびシステム主導アクセス
すべてのパートナーが DB2 ユニバーサル・データベース (OS/390 版) システムでなければならない。	任意の 2 つの DRDA システムを相互接続できる。	アプリケーション・リクエスターは任意の DRDA システムでかまわないが、サーバーは DB2 ユニバーサル・データベース (OS/390 版) システムでなければならない。
複数のパートナーに直接接続できる。	複数のパートナーに直接接続できる。	アプリケーション・リクエスターは直接アプリケーション・サーバーに接続できる。アプリケーション・サーバーは複数の DB2 ユニバーサル・データベース (OS/390 版) 2 次サーバーに接続できる。
各 SQL アプリケーションは、各サーバーと複数の会話を行うことができる。	各 SQL アプリケーションは各サーバーと 1 つの会話ができる。	SQL アプリケーションは、各サーバーと 1 つの会話を行うことができる。DB2 ユニバーサル・データベース (OS/390 版) アプリケーションは、アプリケーションの各サーバーと複数の会話を確立できる。
1 コミットの範囲内でローカル資源とリモート資源の両方にアクセスできる。	1 コミットの範囲内でローカル資源とリモート資源の両方にアクセスできる。	アプリケーション・リクエスターとアプリケーション・サーバーはローカル・データとリモート・データにアクセスできる。
大規模な照会、および複数の照会を同時に行う場合に効果的。	1 コミットの範囲内で実行回数が増える SQL ステートメントの場合に効果的。	アプリケーション・リクエスターとアプリケーション・サーバー間の接続は [2] と同様に動作し、2 次サーバー接続は [1] と同様に動作する。
静的または動的 SQL をサポートできるが、コミットの範囲内で最初に静的 SQL を実行するとき、サーバーは静的 SQL を動的にバインドする。	静的または動的 SQL を発行できる。	アプリケーション・リクエスターとアプリケーション・サーバーは静的または動的 SQL を発行できる。2 次サーバーは静的または動的 SQL をサポートしているが、コミットの範囲内で最初に静的 SQL を実行するとき、静的 SQL を動的にバインドする。

表 2. DB2 ユニバーサル・データベース (OS/390 版) 分散データベースの接続の比較 (続き)

[1] システム主導アクセス	[2] アプリケーション主導アクセス (すべてのシステムが 2 フェーズ・コミットをサポートする場合)	[3] アプリケーション主導およびシステム主導アクセス
SQL INSERT、DELETE、UPDATE ステートメント、および SELECT をサポートするステートメントに制限されている。	システムがサポートしているステートメントであれば、どれも使用できる。	アプリケーション・サーバーはすべての SQL をサポートしている。2 次サーバーは DML SQL だけをサポートしている (CREATE または ALTER など)。

追加機密保護拡張

拡張機密保護コード

DB2 ユニバーサル・データベース for OS/390 バージョン 5.1 よりも前のバージョンでは、ユーザー ID またはパスワードを指定した接続要求が失敗した場合、SQL30082 理由コード 0 が返されるものの、問題となっている点に関して他の指示は出されませんでした。

DB2 ユニバーサル・データベース for OS/390 バージョン 5.1 は機能が拡張され、拡張機密保護コードをサポートするようになりました。拡張機密保護を指定すると、理由コードのほかに (PASSWORD EXPIRED) などの診断が追加されません。

これを活用するには、DB2 ユニバーサル・データベース (OS/390 版) の拡張機密保護用に ZPARM インストール・パラメーターの値を YES に設定する必要があります。EXTSEC=YES に設定するには、DB2 ユニバーサル・データベース (OS/390 版) のインストール・パネル DSN6SYSP を使用します。これを設定するために、DDF パネル 1 (DSNTIPR) を使用することもできます。省略時値は EXTSEC=NO です。パスワードの有効期限が切れた場合、PC、UNIX、Apple Macintosh、および DB2 コネクトを使用している Web アプリケーションはエラー・メッセージ SQL01404 を受け取ります。

検査済みの TCP/IP 機密保護

DB2 ユニバーサル・データベースの機密保護オプション

AUTHENTICATION=CLIENT をサポートさせたい場合、DB2 ユニバーサル・データベース (OS/390 版) のインストール・パネル DSNTIP4 (DDF パネル 2) を使用して、検査済みの TCP/IP 機密保護を YES に設定します。

デスクトップ ODBC および Java アプリケーションの機密保護

ワークステーション ODBC および Java アプリケーションは動的 SQL を使用します。この動的 SQL はインストールの際に機密保護上の問題の原因となることがあります。DB2 ユニバーサル・データベース (OS/390 版) は、所有者とバインダーの両方の権限で動的 SQL を実行できる、新しいバインド・オプション DYNAMICRULES(BIND) を導入しています。DYNAMICRULES を DB2 コネクトを介して指定する方法については、[コマンド解説書](#) を参照してください。

DB2 ユニバーサル・データベースおよび DB2 コネクトには、DB2CLI.INI 構成ファイル内に新しい CLI/ODBC 構成パラメーター CURRENTPACKAGESET があります。これは適切な特権を持つスキーマ名に設定することが必要です。SQL SET CURRENT PACKAGESET schema ステートメントは、アプリケーションの各接続ごとに自動的に出されます。

DB2CLI.INI を更新するためには、ODBC マネージャーを使用します。詳しくは、[インストールおよび構成 補足](#) を参照してください。

パスワード変更サポート

SQL CONNECT ステートメントがユーザー ID のパスワードの有効期限が切れていることを示すメッセージを戻す場合、DB2 コネクトのバージョン 5.2 以降では TSO にサインオンしなくてもパスワードを変更できるようになっています。DRDA から、DB2 ユニバーサル・データベース (OS/390 版) はパスワードを変更できます。

旧パスワードと新規パスワード、および確認用パスワードを入力する必要があります。DB2 コネクト エンタープライズ・エディションのサーバーで指定された機密保護が DCS である場合、パスワード変更の要求は DB2 ユニバーサル・データベース (OS/390 版) データベース・サーバーに送られます。指定した機密保護が SERVER である場合、DB2 コネクト・サーバーのパスワードは変更されます。

他の利点は、LU を別々に定義する必要がないということです。追加情報は、DB2 コネクト エンタープライズ・エディションの[概説](#)および[インストール](#)の資料を参照してください。

アプリケーション・リクエスターのセットアップ

DB2 ユニバーサル・データベース (OS/390 版) では、DB2 ユニバーサル・データベース (OS/390 版) 分散データ機能 (DDF) の重要な部分として DRDA アプリケーション・リクエスターを実装しています。DDF は、ローカルな DB2 ユニバーサル・データベース (OS/390 版) データベース管理機能とは別個に停止させることができますが、ローカルな DB2 ユニバーサル・データベース (OS/390 版) データベース管理サポートなしに実行させることはできません。

アプリケーション・リクエスターとして動作している場合、DB2 ユニバーサル・データベース (OS/390 版) はシステム上で実行されているアプリケーションを、DRDA アプリケーション・サーバー機能が実装されているリモート DB2 ユニバーサル・データベース、DB2 (MVS/ESA 版)、DB2 ユニバーサル・データベース (OS/390 版)、DB2 ユニバーサル・データベース (AS/400 版)、および DB2 (VSE および VM 版) の各データベース・サーバーに接続できます。

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターを使用して分散データベースにアクセスするには、以下のようしてください。

- 55ページの『ネットワーク情報の提供』－ アプリケーション・リクエスターは、RDB_NAME 値を受け入れ、それらの値を SNA NETID.LUNAME または TCP/IP アドレス値に変換できる必要があります。DB2 ユニバーサル・データベース (OS/390 版) は、DB2 ユニバーサル・データベース (OS/390 版) 通信データベース (CDB) を使用して、RDB_NAME および対応するネットワーク・パラメーターを登録します。CDB によって、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターは SNA 接続または TCP/IP 接続のいずれかを介して分散データベース要求を行うときに必要な情報を通信サーバーに渡すことができます。
- 74ページの『機密保護の提供』－ リモート・データベース要求がアプリケーション・サーバーによって受け入れられるようにするには、アプリケーション・リクエスターがサーバーに必要な安全保護情報を提供しなければなりません。DB2 ユニバーサル・データベース (OS/390 版) は CDB、DCE、RACF、または他の機密保護サブシステムを使用して、必要なネットワーク機密保護情報を提供します。
- 83ページの『データの表示』－ アプリケーション・リクエスターの CCSID がアプリケーション・サーバーと互換性があることを確認する必要があります。

ネットワーク情報の提供

分散データベース環境の処理の大部分では、ネットワーク内の他の場所との間でメッセージを交換することが必要です。このプロセスが正しく実行されるようにするには、以下のことを実行しなければなりません。

1. ローカル・システムの定義
2. リモート・システムの定義
3. 通信の定義 (SNA または TCP/IP 接続用)
4. RU サイズおよび歩調合わせの設定 (SNA 接続の場合のみ)

『ローカル・システム (SNA) の定義』または62ページの『ローカル・システム (TCP/IP) の定義』を参照してください。

ローカル・システム (SNA) の定義

SNA ネットワーク内の各プログラムには NETID および LU 名が割り当てられているため、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターがネットワークに接続するときには NETID.LUNAME 値 (VTAM を介して割り当てられる) が必要です。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターはローカルの DB2 ユニバーサル・データベース (OS/390 版) データベース管理システムに統合されるため、アプリケーション・リクエスターには RDB_NAME も必要です。DB2 ユニバーサル・データベース (OS/390 版) のマニュアルでは、DB2 ユニバーサル・データベース (OS/390 版) は RDB_NAME をロケーション名と呼んでいます。

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターを SNA ネットワークに定義するには、次のようにします。

1. DB2 ユニバーサル・データベース (OS/390 版) システムの LU 名を選択する。DDF が始動すると、DB2 ユニバーサル・データベース (OS/390 版) システムの NETID が VTAM から自動的に取得されます。
2. DB2 ユニバーサル・データベース (OS/390 版) のブートストラップ・データ・セット (BSDS) に LU 名とロケーション名を定義する (DB2 ユニバーサル・データベース (OS/390 版) ではロケーション名が 16 文字に制限されます。)
3. 選択した LU 名を VTAM に登録するため、VTAM APPL 定義を作成する。
4. 拡張機密保護が「YES」に設定されていることを確認してください。52ページの『追加機密保護拡張』を参照してください。

DDF BSDS の構成: DB2 ユニバーサル・データベース (OS/390 版) は始動処理中に BSDS を読み取って、システム・インストール・パラメーターを取得します。BSDS に保管されるレコードの 1 つは *DDF* レコード と呼ばれるものです。そのように呼ばれるのは、VTAM に接続するとき、その中に収められている情報を DDF が使用するからです。この情報は次のものから構成されません。

- DB2 ユニバーサル・データベース (OS/390 版) システムのロケーション名
- DB2 ユニバーサル・データベース (OS/390 版) システムの LU 名
- DB2 ユニバーサル・データベース (OS/390 版) システムが VTAM に接続するときを使用されるパスワード

以下の 2 つの方法で、DDF BSDS 情報を DB2 ユニバーサル・データベース (OS/390 版) に指定できます。

- DB2 ユニバーサル・データベース (OS/390 版) を最初にインストールするときは、DDF インストール・パネル DSNTIPR を使用して、必要な DDF BSDS 情報を指定する。DB2 ユニバーサル・データベース (OS/390 版) を VTAM に接続する方法を知る方が重要なので、ここではインストール・パラメーターの多くについては説明しません。57ページの図15 は、インストール・パネルを使ってロケーション名 NEW_YORK3、LU 名 NYM2DB2、およびパスワード PSWDBD1 を DB2 ユニバーサル・データベース (OS/390 版) BSDS に記録する方法を示しています。

```

                                DISTRIBUTED DATA FACILITY                                =
==> _
Enter data below:
1 DDF STARTUP OPTION  ==> AUTO      NO, AUTO, or COMMAND
2 DB2 LOCATION NAME  ==> NEW_YORK3  The name other DB2s use to
                                refer to this DB2
3 DB2 NETWORK LUNAME ==> NYM2DB2  The name VTAM uses to refer to this DB2
4 DB2 NETWORK PASSWORD ==> PSWDBD1  Password for DB2's VTAM application
5 RLST ACCESS ERROR  ==> NOLIMIT  NOLIMIT, NORUN, or 1-5000000
6 RESYNC INTERVAL    ==> 3        Minutes between resynchronization period
                                (ACTIVE or INACTIVE) Status of a
7 DDF THREADS        ==> ACTIVE    database access thread that commits or
                                rolls back and holds no database locks
                                or cursors
8 DB2 GENERIC LUNAME ==>          Generic VTAM LU name for this DB2
                                subsystem or data sharing group
9 IDLE THREAD TIMEOUT ==> 120      0 or seconds until dormant server ACTIVE
                                thread will be terminated (0-9999)
10 EXTENDED SECURITY  ==> YES      Allow change password and descriptive
                                security error codes. YES or NO.
PRESS: ENTER to continue RETURN to exit HELP for more information

```

図 15. DB2 ユニバーサル・データベース (OS/390 版) インストール・パネル DSNNTIPR

- DB2 ユニバーサル・データベース (OS/390 版) のインストールが済んでいる場合は、ログ目録変更ユーティリティ (DSNJU003) を使用して BSDS の情報を更新する。

58ページの図16 には、BSDS を更新して、ロケーション名を NEW_YORK3 に、LU 名を NYM2DB2 に、パスワードを PSWDBD1 にする方法が示されています。

```

//SYSADMB JOB , 'DB2 5.1 JOB', CLASS=A
//*
//*      CHANGE LOG INVENTORY:
//*      UPDATE BSDS WITH
//*          - DB2 LOCATION NAME FOR NEW_YORK3
//*          - VTAM LUNAME (NYM2DB2)
//*          - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB DD DISP=SHR, DSN=DSN510.DSNLOAD
//SYSUT1 DD DISP=OLD, DSN=DSNC510.BSDS01
//SYSUT2 DD DISP=OLD, DSN=DSNC510.BSDS02
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
      DDF LOCATION=NEW_YORK3, LUNAME=NYM2DB2, PASSWORD=PSWDBD1
//*
```

図 16. ブートストラップ・データ・セット DDF 定義 (VTAM 用) の例

DDF が (DB2 ユニバーサル・データベース (OS/390 版) の始動に伴って自動的に、あるいは DB2 ユニバーサル・データベース (OS/390 版) の START DDF コマンドによって) 始動すると、DDF は VTAM に接続し、LU 名とパスワードを VTAM に渡します。VTAM は、LU 名とパスワード (VTAM パスワードが必要な場合) を DB2 ユニバーサル・データベース (OS/390 版) システムの VTAM APPL ステートメントで定義された値と照合することによって、DB2 ユニバーサル・データベース (OS/390 版) システムを認識します。VTAM パスワードは、指定された LU 名を DB2 ユニバーサル・データベース (OS/390 版) が VTAM 上で使用する許可を得ているかどうかを検査するために使用されます。VTAM パスワードはネットワークの中を伝送されることはありませんし、ネットワーク内の他のシステムを DB2 ユニバーサル・データベース (OS/390 版) に接続するために使用されることもありません。

VTAM がパスワードを必要としない場合は、ログ目録変更ユーティリティで PASSWORD= キーワードを省略してください。このキーワードを指定しないということは、VTAM パスワードが不要であるということです。

VTAM APPL 定義の作成: VTAM LU 名とパスワードを DB2 ユニバーサル・データベース (OS/390 版) に定義したら、次にこれらの値を VTAM に登録する必要があります。VTAM では、ローカル LU 名を定義するのに APPL ステートメントを使用します。59ページの図17 は、LU 名 NYM2DB2 を VTAM に定義する方法を示しています。

```

DB2APPLS VBUILD TYPE=APPL
*
*-----*
*
*          APPL DEFINITION FOR THE NEW_YORK3 DB2 SYSTEM
*
*-----*
*
NYM2DB2  APPL  APPC=YES,                X
            AUTH=(ACQ),                 X
            AUTOSSES=1,                  X
            DMINWNL=10,                  X
            DMINWNR=10,                  X
            DSESLIM=20,                  X
            EAS=9999,                    X
            MODETAB=RDBMODES,            X
            PRTCT=PSWDBD1,               X
            SECACPT=ALREADYV,            X
            SRBEXIT=YES,                  X
            VERIFY=NONE,                  X
            VPACING=2,                    X
            SYNCLVL=SYNCPT,              X
            ATNLOSS=ALL                   X

```

図 17. DB2 ユニバーサル・データベース (OS/390 版) の VTAM APPL 定義のサンプル

VTAM APPL ステートメントでは多くのキーワードを使用できます。キーワードの意味は、*DB2 ユニバーサル・データベース (OS/390 版) 管理の手引き* に詳しく説明されています。ここでは本書の内容に関係のあるキーワードだけを説明します。図17 に関係するキーワードを以下に説明します。

NYM2DB2

VTAM は、LU 名として APPL ステートメント・ラベルを使用します。この場合、LU 名は NYM2DB2 です。APPL の構文では、完全な NETID.LUNAME の値を指定することができません。VTAM APPL ステートメントに NETID 値は指定されません。各アプリケーションには VTAM システムの NETID が自動的に割り当てられるからです。

AUTOSSES=1

APPC セッション数変更 (CNOS) が発行されるときに自動的に開始する SNA 回線争奪勝者セッションの数。VTAM CNOS 処理が失敗した場合に DB2 ユニバーサル・データベース (OS/390 版) に通知するため、AUTOSSES には非ゼロ値を指定する必要があります。

任意の 2 つの分散データベース・パートナー間のすべての APPC セッションを自動的に開始する必要はありません。AUTOSSES 値が回線争

奪勝者の限度 (DMINWNL) より小さい場合には、分散データベース・アプリケーションが必要とするまで、VTAM は残りの SNA セッションの開始を遅らせます。

DMINWNL=10

この DB2 ユニバーサル・データベース (OS/390 版) システムが回線争奪勝者となるセッションの数。DMINWNL パラメーターは CNOS 処理の省略時値ですが、DB2 ユニバーサル・データベース (OS/390 版) CDB 中の SYSIBM.LUMODES 表に行を追加することにより、所定の任意のパートナーに合わせてオーバーライドすることができます。

DMINWNR=10

パートナー・システムが回線争奪勝者となるセッションの数。DMINWNR パラメーターは CNOS 処理の省略時値ですが、DB2 ユニバーサル・データベース (OS/390 版) CDB 中の SYSIBM.LUMODES 表に行を追加することにより、所定の任意のパートナーに合わせてオーバーライドすることができます。

DSESLIM=20

DB2 ユニバーサル・データベース (OS/390 版) と特定のモード・グループ名の別の分散システムとの間に確立できるセッションの合計数 (勝者および敗者セッション)。DSESLIM パラメーターは CNOS 処理の省略時値ですが、DB2 ユニバーサル・データベース (OS/390 版) CDB 中の SYSIBM.LUMODES 表に行を追加することにより、所定の任意のパートナーに合わせてオーバーライドすることができます。

パートナーが DSESLIM、DMINWNL、または DMINWNR パラメーターで要求されたセッションの数をサポートできない場合には、CNOS 処理はパートナーが受け入れ可能なこれらのパラメーターの新しい値を折衝します。

EAS=9999

この VTAM LU で必要とされるセッションの合計数の見積もり。

MODETAB=RDBMODES

各 DB2 ユニバーサル・データベース (OS/390 版) モード名が存在する VTAM MODE 表を指定します。

PRTCT=PSWDBD1

DB2 ユニバーサル・データベース (OS/390 版) が VTAM への接続を試行するときに使用される VTAM パスワードを指定します。PRTCT キーワードを省略する場合、パスワードは不要であり、DB2 ユニバーサル・データベース (OS/390 版) のログ目録変更ユーティリティから PASSWORD= キーワードを省略する必要があります。

SECACPT=ALREADYV

リモート・システムから分散データベース要求を受け取ったときにこの DB2 ユニバーサル・データベース (OS/390 版) システムが受け入れる、最大の SNA 会話レベル機密保護値を指定します。ALREADYV キーワードは、この DB2 ユニバーサル・データベース (OS/390 版) システムが、この DB2 ユニバーサル・データベース (OS/390 版) システムにデータを要求する他の DRDA システムから、以下の 3 つの SNA セッション機密保護オプションを受け入れることができることを示しています。

- SECURITY=SAME (リクエスターのユーザー ID だけを含む検査済みの要求)。
- SECURITY=PGM (リクエスターのパスワードまたはパスチケットを含む要求)。
- SECURITY=NONE (機密保護情報を含めないようにする要求)。DB2 ユニバーサル・データベース (OS/390 版) は、SECURITY=NONE と指定された DRDA 要求を拒否します。

各 DB2 ユニバーサル・データベース (OS/390 版) パートナーに対する SNA 会話機密保護レベルは、DB2 ユニバーサル・データベース (OS/390 版) CDB (SYSIBM.LUNAMES 表の USERSECURITY 列) から取られているので、常に SECACPT=ALREADYV を指定するのが最善の方法です。SECACPT=ALREADYV を指定すると、USERSECURITY の値を柔軟に選択できるようになります。

VERIFY=NONE

この DB2 ユニバーサル・データベース (OS/390 版) システムで必要な SNA セッション機密保護の (パートナー LU 検査) レベルを識別します。NONE 値は、パートナー LU 検査が必要ではないことを示しています。

DB2 ユニバーサル・データベース (OS/390 版) では、VERIFY キーワードの選択に制限はありません。信頼性の低いネットワークの場合は VERIFY=REQUIRED をお勧めします。VERIFY=REQUIRED を指定すると、パートナー LU 検査を実行できないパートナーを VTAM が拒否することになります。VERIFY=OPTIONAL を選択すると、VTAM はサポートを提供するパートナーにのみパートナー LU 検査を実行します。

VPACING=2

VTAM の歩調合わせカウントを 2 に設定します。

SYNCLVL=SYNCPT

DB2 ユニバーサル・データベース (OS/390 版) が 2 フェーズ・コミットをサポートできることを示します。VTAM は、この情報を使用して、パートナーに 2 フェーズ・コミットが使用可能であることを通知します。このキーワードを指定すると、パートナーが 2 フェーズ・コミットをサポートできる場合に、DB2 ユニバーサル・データベース (OS/390 版) は自動的に 2 フェーズ・コミットを使用します。

ATNLOSS=ALL

VTAM セッションが終了するたびに DB2 ユニバーサル・データベース (OS/390 版) が通知を受ける必要があることを示します。これにより、DB2 ユニバーサル・データベース (OS/390 版) は必要なときに SNA 再同期を実行することになります。

DSESLIM、DMINWNL、および DMINWNR により、すべてのパートナーに当てはまる、省略時の VTAM セッション限度を確立できます。特殊なセッション限度要件があるパートナーの場合は、SYSIBM.LUMODES 表を使って省略時のセッション限度をオーバーライドできます。たとえば、OS/2 システムに適した VTAM 省略時セッション限度を指定する場合、他のパートナーに適したセッション限度を定義する行を SYSIBM.LUMODES 表に作成できます。次のサンプル値を考慮してください。

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

これらのパラメーターにより、各パートナーは、自分が回線争奪勝者であるセッションを最大 4 つまで DB2 ユニバーサル・データベース (OS/390 版) との間で作成できるようになります。OS/2 は DB2 ユニバーサル・データベース (OS/390 版) と LU 6.2 会話を作成するので、OS/2 を回線争奪勝者としても大幅なパフォーマンスの向上は望めません。OS/2 は、使用可能な回線争奪勝者セッションを持っている場合、新しい LU 6.2 会話を開始する許可を求める必要はありません。

ローカル・システム (TCP/IP) の定義

読者の便宜のために、この節では DB2 コネクト エンタープライズ・エディション (OS/2 および Windows NT 版) 概説およびインストールを要約していません。詳細については、DB2 ユニバーサル・データベース (OS/390 版) インストールレーションの手引き、および *DRDA Support for TCP/IP with DB2 Universal Database for OS/390 and DB2 Universal Database* を参照してください。

DB2 ユニバーサル・データベース (OS/390 版) との TCP/IP 通信を定義するためのステップは以下のとおりです。

1. TCP/IP 通信は DB2 ユニバーサル・データベース (OS/390 版) およびパートナー・システム上で確立されている必要があります。
2. 2 つの適切な TCP/IP ポート番号がネットワーク管理者から割り当てられている必要があります。省略時では DB2 ユニバーサル・データベース (OS/390 版) は、データベース接続にポート番号 446 を、再同期要求 (2 フェーズ・コミット) にポート番号 5001 を使用します。
3. リモート・アプリケーション・サーバーまたはアプリケーション・リクエスターは、DB2 ユニバーサル・データベース (OS/390 版) として同一のポート番号 (またはサービス名) を使用する必要があります。
4. TCP/IP がすでに検査済みの機密保護オプションを「YES」に設定していることを確認してください。52ページの『追加機密保護拡張』を参照してください。
5. DB2 ユニバーサル・データベース (OS/390 版) BSDS は、追加のパラメーターを組み込んでいる必要があります。図18 は、TCP/IP 通信を使用可能にするために必要な追加パラメーターを強調しています。

```
//SYSADMB JOB , 'DB2 5.1 JOB', CLASS=A
/**
/**      CHANGE LOG INVENTORY:
/**      UPDATE BSDS WITH
/**          - DB2 LOCATION NAME FOR NEW_YORK3
/**          - VTAM LUNAME (NYM2DB2)
/**          - DB2/VTAM PASSWORD
/**
/**          - GENERIC LU NAME
/**          - TCP/IP PORT FOR DATABASE CONNECTIONS
/**          - TCP/IP PORT FOR RESYNCH OPERATIONS
/**
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB DD DISP=SHR, DSN=DSN510.DSNLOAD
//SYSUT1 DD DISP=OLD, DSN=DSNC510.BSDS01
//SYSUT2 DD DISP=OLD, DSN=DSNC510.BSDS02
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
DDF      LOCATION=NEW_YORK3, LUNAME=NTYM2DB2, PASSWORD=PSWDBD1,
          GENERICLU=name, PORT=446, RESPORT=5001
/*
/**
```

図18. ブートストラップ・データ・セット DDF 定義 (TCP/IP 用) の例

リモート・システムの定義

DB2 ユニバーサル・データベース (OS/390 版) アプリケーションがリモート・システムからのデータを要求する場合、通信データベース (CDB) 表が検

索されて、リモート・システムについての情報が検出されます。CDB は SQL 表のグループであり、DB2 ユニバーサル・データベース (OS/390 版) システム管理者が管理します。DB2 ユニバーサル・データベース (OS/390 版) システム管理者は、SQL を使用して CDB に行の挿入を行うことにより、使用される可能性のある各 DRDA パートナーを記述することができます。CDB およびその使用方法に関する完全な説明は、DB2 ユニバーサル・データベース (OS/390 版) SQL 解説書、および DB2 ユニバーサル・データベース (OS/390 版) インストレーションの手引き を参照してください。

CDB を参照し、以下の情報を探索します。

- LU 名と TPN (SNA 接続用)
- TCP/IP アドレス情報 (アウトバウンド TCP/IP SNA 接続の場合のみ必要)
- リモート・サイトで必要なネットワーク機密保護情報
- リモート・サイトとの通信に使用されるセッション限度とモード名 (SNA 接続用)

通信データベースにデータを読み込む: インバウンド TCP/IP データベース接続のみを使用する場合は、CDB の更新は必要ありません。それで、DB2 ユニバーサル・データベース (OS/390 版) を TCP/IP サーバーとしてのみ使用する計画であるなら、CDB にデータを読み込む必要はなく、省略時値を使用できます。しかしながら、インバウンド SNA 接続を使用する場合は、SYSIBM.LUNAMES に少なくとも 1 つのブランク行を含める必要があります。たとえば、任意の着信 DB2 コネクト LU からの SNA データベース接続要求を受け入れられるようにするには、以下のような SQL コマンドを使用します。

```
INSERT INTO SYSIBM.LUNAMES (LUNAME) VALUES ('      ')
```

DB2 ユニバーサル・データベース (OS/390 版) をリクエスターとして使用する場合は、CDB は常に更新する必要があります。SYSIBM.LOCATIONS 表、および SYSIBM.LUNAMES 表 (SNA 接続の場合) または SYSIBM.IPNAMES 表 (TCP/IP 接続の場合) のどちらかに行を挿入する必要があります。

さらに、SNA 接続用のインバウンド機密保護要件またはインバウンド・ユーザー ID 変換を制御したい場合は、追加の CDB 更新が必要となります。追加の例は以下の解説を参照してください。74ページの『機密保護の提供』は、アプリケーション・リクエスターを設定するときにユーザー機密保護を定義する方法を示しています。そして、89ページの『機密保護の提供』はアプリケーション・サーバーの設定について説明しています。

DB2 ユニバーサル・データベース (OS/390 版) 管理の手引き では、CDB 表を更新するための要件がより詳細に説明されています。CDB にデータを読み込んだ後、リモート・システム上のデータにアクセスする照会を書き込むことができます。DB2 ユニバーサル・データベース (OS/390 版) インストール・インストラクションの手引き にも CDB の更新に関する詳細な情報があります。

通信データベースが要求を処理する方法: 要求を送信するとき、DB2 ユニバーサル・データベース (OS/390 版) は SYSIBM.LOCATIONS カタログ表の LINKNAME 列を使用して、どのネットワーク・プロトコルをアウトバウンド・データベース接続に使用すべきかを決定します。VTAM 要求を受け取るには、DB2 ユニバーサル・データベース (OS/390 版) インストール・パネル DSNTIPR 中の LUNAME を選択する必要があります。TCP/IP 要求を受け取るには、DB2 ユニバーサル・データベース (OS/390 版) インストール・パネル DSNTIP5 中の、DRDA ポートと再同期ポートを選択する必要があります。TCP/IP はサーバーのポート番号を使用して、ネットワーク要求を正しい DB2 サブシステムに渡します。

SYSIBM.IPNAMES 表の LINKNAME 列に値が存在する場合、TCP/IP が DRDA 接続のために使用されます。値が SYSIBM.LUNAMES 表にある場合は、SNA が使用されます。SYSIBM.LUNAMES と SYSIBM.IPNAMES の両方に同一の名前がある場合は、そのロケーションに接続するために TCP/IP が使用されます。

注: リクエスターが SNA および TCP/IP プロトコルの両方を使用して、与えられたロケーションに接続することはできません。たとえば、ユーザーの SYSIBM.LOCATIONS で LINKNAME に LU1 が指定されていて、LU1 が SYSIBM.IPNAMES および SYSIBM.LUNAMES 表の両方で定義されている場合、このリクエスターから LU1 への接続には TCP/IP が使用される唯一のプロトコルとなります。

通信データベース表: CDB は以下の表で構成されています。

1. SYSIBM.LOCATIONS

この表によって DB2 ユニバーサル・データベース (OS/390 版) は、アウトバウンド要求用 DB2 ユニバーサル・データベース (OS/390 版) アプリケーションが選択した各 RDB_NAME にアクセスするのに必要となる SNA または TCP/IP アドレス情報を判別することができます。列は次のとおりです。

LOCATION

リモート・システムの RDB_NAME。DB2 ユニバーサル・データ

ベース (OS/390 版) では RDB_NAME 値が 16 バイトまでに制限されていて、DRDA で定義されている 18 バイトという制限より 2 バイト短くなっています。

LINKNAME

リモート・システムの LU 名または TCP/IP 属性。

PORT TCP/IP ポート名またはサービス名情報 (DRDA の省略時ポート名は 446)。

TPN リモート・システムの APPC トランザクション・プログラム名 (TPN)。リモート・システムが DB2 ユニバーサル・データベース (OS/390 版) システムである場合、またはリモート・システムが省略時の DRDA TPN 値 (X'07F6C4C2') を使用する場合は、DB2 ユニバーサル・データベース (OS/390 版) が自動的に正しい値を選択するため、TPN に空ストリングが使用されます。

リモート・システムが省略時値以外の TPN 値を必要とする場合、ここでその値を指定してください。

2. SYSIBM.LUNAMES

この表では、SNA 接続を使用して接続されるリモート・システムのネットワーク属性を定義します。列は次のとおりです。

LUNAME

リモート・システムの LU 名。

SYSMODENAME

DB2 ユニバーサル・データベース (OS/390 版) の 2 次サーバー・サポート (システム主導アクセス) のための DB2 ユニバーサル・データベース (OS/390 版) - DB2 ユニバーサル・データベース (OS/390 版) システム間 会話を確立するために使用される VTAM ログオン・モード名。この列をブランク値にすると、DB2 ユニバーサル・データベース (OS/390 版) システム会話に IBMDB2LM が使用されることとなります。

SECURITY_IN

この DB2 ユニバーサル・データベース (OS/390 版) システムがリモート・システムのサーバーとして機能する場合の、リモート・システムのネットワーク機密保護受け入れに関する必須オプション (インバウンド機密保護 要件)。以下の値を取ることができます。

- **V** はオプションが「検査」であることを示します。着信接続要求が次のうちの 1 つを含んでいる必要があります。ユーザー ID とパスワード、ユーザー ID と RACF パスチケット、あるいは DCE 機密保護チケット。
- **A** はオプションが「検査済み」であることを示します。要求はパスワードを必要としませんが、パスワードを送信する場合は検査されます。このオプションでは、次のうちのどれかを含んでいる場合、着信接続要求が受け入れられます。ユーザー ID、ユーザー ID とパスワード、ユーザー ID と RACF パスチケット、あるいは DCE 機密保護チケット。

USERNAMES 列に 'I' または 'B' が含まれている場合、ユーザー ID のみを含んでいる着信接続要求を検査するために RACF が呼び出されることはありません。

SECURITY_OUT

この DB2 ユニバーサル・データベース (OS/390 版) システムがリモート・システムのリクエスターとして機能する場合の、リモート・システムのネットワーク機密保護受け入れに関する必須オプション (アウトバウンド機密保護 要件)。以下の値を取ることができます。

- **A** はオプションが「検査済み」であることを示します。アウトバウンド接続要求は許可 ID を含んでおり、パスワードはありません。アウトバウンド要求のために使用される許可 ID は、USERNAMES 列の値に応じて、DB2 ユーザーの許可 ID または変換済み ID のどちらかになります。
- **R** はオプションが「RACF パスチケット」であることを示します。アウトバウンド接続要求はユーザー ID と RACF パスチケットを含んでいます。サーバーの LU 名 は、RACF パスチケット・アプリケーション名として使用されます。
アウトバウンド要求のために使用される許可 ID は、USERNAMES 列の値に応じて、DB2 ユーザーの許可 ID または変換済み ID のどちらかになります。
- **P** はオプションが「パスワード」であることを示します。アウトバウンド接続要求は許可 ID およびパスワードを含んでいます。パスワードは ENCRYPTPWDS 列で指定された値に応じて、SYSIBM.USERNAMES 表または RACF から取得されます。USERNAMES 列では 'B' または 'O' を指定する必要があります。

ENCRYPTPSWDS

このパートナーとのパスワード交換を暗号化するかどうか。暗号化パスワードは、DB2 ユニバーサル・データベース (OS/390 版) リクエスターおよびサーバーでのみサポートされます。

MODESELECT

SYSIBM.MODESELECT 表を使用し、要求を出したエンド・ユーザーとアプリケーションに基づいて VTAM ログオン・モード項目 (モード名) を選択するかどうかを決定します。この列に 'Y' が入っている場合、SYSIBM.MODESELECT 表を使用して、各アウトバウンド分散データベース要求のモード名を取得します。

MODESELECT に 'Y' 以外の値が入っている場合、システム主導アクセス要求にモード名 IBMDB2LM が使用され、DRDA 要求にモード名 IBMRDB が使用されます。

モード名に関連した VTAM サービス・クラス (COS) を指定することにより、MODESELECT 列を使って分散データベース要求を優先順位付けすることが可能になります。

USERNAMES

必要な come-from 検査とユーザー ID 変換のレベル。この列は、リモート・パートナーからデータを要求するときこの DB2 ユニバーサル・データベース (OS/390 版) サブシステムが使用する機密保護パラメーターも指定します (アウトバウンド機密保護 要件)。

USERNAMES は、I、O、または B (インバウンドのみ、アウトバウンドのみ、または両方) の値を取ることができます。

GENERIC

DB2 ユニバーサル・データベース (OS/390 版) が LU 名に実際の名前、または一般名のどちらを使用するかを示します。

3. SYSIBM.LUMODES

この表は、APPC (SNA) 接続を使用するパートナー・システム用に、VTAM に LU 6.2 セッション制限 (CNOS 制限) を設けるために使用されます。列は次のとおりです。

LUNAME

リモート・システムの LU 名。

MODENAME

制限を指定する対象となる VTAM ログオン・モードの名前。

MODENAME 列にブランク値を指定すると、IBMDB2LM に省略時解釈されます。

CONVLIMIT

このログオン・モードの場合の、ローカルな DB2 ユニバーサル・データベース (OS/390 版) とリモート・システム間のアクティブな会話の最大数。この値は、このログオン・モードのための VTAM APPL 定義ステートメントの DSESLIM パラメーター (DB2 ユニバーサル・データベース (OS/390 版) の省略時の VTAM セッション限度を指定する) をオーバーライドするために使用されます。

CONVLIMIT に指定された値は、CNOS 中に DMINWNR および DMINWNL 値を CONVLIMIT/2 に設定するために使用されます。

4. SYSIBM.MODESELECT

この表により、エンド・ユーザーおよび DB2 ユニバーサル・データベース (OS/390 版) アプリケーションごとに異なるモード名を指定できるようになります。これは SNA 接続でのみ使用されます。各 VTAM モード名にはサービス・クラス (COS) を関連付けることができるので、この表を使って、AUTHID、PLANNAME、および LUNAME の組み合わせに基づいて、分散データベース・アプリケーションにネットワーク伝送優先順位を割り当てることができます。列は次のとおりです。

AUTHID

DB2 ユニバーサル・データベース (OS/390 版) ユーザーの許可 ID (ユーザー ID)。省略時値はブランクです。これは、指定されたログオン・モード名をすべての許可 ID に当てはめることを意味します。

PLANNAME

リモート・データベース・システムへのアクセスを要求しているアプリケーションに関連したプラン名。省略時値はブランクです。これは、指定されたログオン・モード名をすべてのプラン名に当てはめることを意味します。BIND PACKAGE コマンドで使用されるプラン名は DSNBIND です。

LUNAME

リモート・データベース・システムと関連した LU 名。

MODENAME

分散データベース要求を指定のリモート・システムに経路指定するとき使用される VTAM ログオン・モードの名前。省略時値はブランクです。これは、システム主導アクセス会話には IBMDB2LM を使用し、DRDA 会話には IBMRDB を使用することを意味します。

5. SYSIBM.USERNAMES

この表は、パスワード、名前変換、および come-from 検査を指定することによって、エンド・ユーザー名を管理するために使用します。DB2 ユニバーサル・データベース (OS/390 版) はエンド・ユーザー名を許可 ID として参照します。他の製品の大部分は、この名前をユーザー ID として参照します。

この表で、ユーザーはユーザー名変換を使用して、ユーザー ID 接続および DB2 ユニバーサル・データベース (OS/390 版) 許可 ID として異なった値を使用するように強制することができます。名前変換処理は、リモート・システムへの要求 (アウトバウンド 要求) のため、およびリモート・システムから送られてくる要求 (インバウンド 要求) のために、行うことができます。パスワードが暗号化されていない場合、ユーザー ID とパスワードの両方をリモート・サイトに送るときに、この表はエンド・ユーザーのパスワードの情報源となります。列は次のとおりです。

TYPE 行の使用法の説明 (アウトバウンドまたはインバウンド用の名前変換を記述した行か、それとも come-from 検査要求を記述した行か)。

I はインバウンド接続を示し、**O** はアウトバウンド接続を示します。

TCP/IP 接続には "O" を使用してください。(インバウンド ID 変換と come-from 検査は TCP/IP 要求に対してはなされません。)

AUTHID

アウトバウンド名前変換の場合、これは変換対象の DB2 ユニバーサル・データベース (OS/390 版) 許可 ID。インバウンド名前変換の場合、これは変換対象の SNA ユーザー ID。どちらの場合でも、ブランクの AUTHID 値はすべての許可 ID またはユーザー ID にあてはまります。

LINKNAME

この行と関連した VTAM または TCP/IP ネットワーク・ロケーションを識別します。この列がブランク値の場合、この名前変換規則があらゆる TCP/IP または SNA パートナーに適用されることを示します。

非ブランクの LINKNAME が指定されていれば、次の条件のうちの 1 つまたは両方が真である必要があります。

- SYSIBM.LUNAMES の中に、LUNAME が SYSIBM.USERNAMES の LINKNAME 列で指定された値と一致する行が存在する。この行は、この名前変換規則と関連した VTAM サイトを指定します。

- **SYSIBM.IPNames** の中に、 **LINKNAME** が **SYSIBM.USERNames** の **LINKNAME** 列で指定された値と一致する行が存在する。この行は、この名前変換規則と関連した TCP/IP ホストを指定します。
インバウンド名前変換および **come-from** 検査は、TCP/IP クライアントに対しては実行されません。

NEWAUTHID

新しいエンド・ユーザー名 (SNA ユーザー ID または DB2 ユニバーサル・データベース (OS/390 版) 許可 ID)。ブランクを指定すると、ID の変換が不要であることを示すものとなります。

PASSWORD

パスワードが暗号化されない場合 (**SYSIBM.LUNAMES** で **ENCRYPTPSWDS = 'N'** の場合)、割り当て会話で使用されるパスワード。パスワードが暗号化される場合、この列は無視されます。

6. **SYSIBM.IPNames**

この表は、TCP/IP ノードのために使用されます。

LINKNAME

この列で指定された値は、 **SYSIBM.LOCATIONS** の **LINKNAME** 列で指定された値と一致していなければなりません。

SECURITY_OUT

この列では、**DRDA** 機密保護オプションを定義します。これはローカル **DB2 SQL** アプリケーションが、この TCP/IP ホストに関連した任意のリモート・サーバーに接続するとき使用されます。

- **A** はオプションが「検査済み」であることを示します。アウトバウンド接続要求は許可 ID を含んでおり、パスワードはありません。アウトバウンド要求のために使用される許可 ID は、**USERNames** 列の値に応じて、DB2 ユーザーの許可 ID または変換済み ID のどちらかになります。
- **R** はオプションが「**RACF** パスチケット」であることを示します。アウトバウンド接続要求はユーザー ID と **RACF** パスチケットを含んでいます。 **LINKNAME** 列で指定された値は、リモート・サーバー用の **RACF** パスチケット・アプリケーション名として使用されます。
アウトバウンド要求のために使用される許可 ID は、**USERNames** 列の値に応じて、DB2 ユーザーの許可 ID または変換済み ID のどちらかになります。

- **P** はオプションが「パスワード」であることを示します。アウトバウンド接続要求は許可 ID およびパスワードを含んでいます。パスワードは SYSIBM.USERNAMES 表から取得されます。USERNAMES 列では "O" を指定する必要があります。

USERNAMES

この列はアウトバウンド許可 ID 変換を制御します。アウトバウンド変換は、許可 ID が DB2 からリモート・サーバーに送信されたときに実行されます。

- **O** はアウトバウンド ID が変換対象となっていることを示します。SYSIBM.USERNAMES 表の行が ID 変換を実行するために使用されます。インバウンド ID については、変換または "come-from" 検査は実行されません。
- ブランクの項目は、変換が生じないことを示します。

IPADDR

この列はリモート TCP/IP ホストの IP アドレスまたはドメイン名を含んでいます。IPADDR 列は以下のように指定する必要があります。

- IPADDR が小数点で区切られた 4 個の数値を含む左ざろえの文字列を含んでいる場合、DB2 はその値を小数点付き 10 進数形式の IP アドレスと解釈します。たとえば、'123.456.78.91' は小数点付き 10 進数 IP アドレスとして解釈されます。
- それ以外のすべての値は、TCP/IP gethostbyname ソケット呼び出しで解決することができる、TCP/IP ドメイン名として解釈されます。TCP/IP ドメイン名は、大文字小文字の区別を行いません。

通信の定義 (SNA)

VTAM は、OS/390 システム用のコミュニケーション・マネージャーです。VTAM は DB2 ユニバーサル・データベース (OS/390 版) から LU 6.2 verb を受け入れ、これらの verb をユーザーがネットワーク上で送信可能な LU 6.2 データ・ストリームに変換します。VTAM が DB2 ユニバーサル・データベース (OS/390 版) CDB で定義されたパートナー・アプリケーションと通信するためには、以下の情報を VTAM に提供しなければなりません。

- 各サーバーの LU 名。

DB2 ユニバーサル・データベース (OS/390 版) が VTAM と通信するときは、望む宛先を識別するために (NETID.LUNAME ではなく) LU 名だけを

VTAM に渡すことができます。DB2 ユニバーサル・データベース (OS/390 版) から渡される LU 名の値から VTAM が NETID と LU 名の両方を判別できるようにするためには、ローカル VTAM システムが認識している LU 名の中で、この LU 名が固有のものである必要があります。LU 名が企業の SNA ネットワーク全体に渡って固有のものであるなら、VTAM の資源定義の処理は大幅に単純化されます。ただし、これは必ずしも可能であるとは限りません。LU 名が SNA ネットワークの中で固有のものでないなら、VTAM の LU 名変換を使用して、固有でない LU 名のために NETID.LUNAME の正しい組み合わせを構築する必要があります。この処理については、VTAM ネットワーク導入の手引き (MVS/ESA) の『資源名変換』で説明されています。

リモート LU 名を定義するために用いられる VTAM の定義の配置と構文は、リモート・システムが論理的および物理的にどのようにローカル VTAM システムに接続されているかに応じて異なります。

- 各モード名の RU サイズ、歩調合わせウィンドウ・サイズ、およびサービス・クラス。CDB 中で指定された各モード名ごとに、VTAM モード表に項目を作成します。IBMRDB と IBMDB2LM を定義する必要もあります。
- LU 検査アルゴリズム用の VTAM および RACF プロファイル (パートナー LU 検査を使用する予定の場合)。

RU サイズおよび歩調合わせの設定: 定義する VTAM モード表によって、RU サイズと歩調合わせカウントが指定されます。これらの値を正しく定義できていないと、すべての VTAM アプリケーションに悪影響を与える可能性があります。

RU サイズ、セッション限度、および歩調合わせカウントを選択した後、これらの値が既存の VTAM ネットワークに与える影響を考慮することは非常に重要です。新しい分散データベース・システムをインストールするときには、以下の項目を復習してください。

- VTAM CTC 接続には、MAXBFRU パラメーターが RU サイズ + 29 バイト (VTAM が SNA 要求ヘッダーおよび伝送ヘッダーに追加する分) を処理するのに十分の大きさであることを確認してください。MAXBFRU は 4K バイト単位で計測されます。それで、MAXBFRU は少なくとも 2 でなければ 4K RU に適合しません。
- NCP 接続では、MAXDATA が RU サイズ + 29 バイトを処理できる十分な大きさであることを確認してください。4K の RU サイズを指定する場合、MAXDATA は最低 4125 でなければなりません。

NCP MAXBFRU パラメーターを指定する場合には、RU サイズに 29 バイトを加えた大きさが入る値を選択してください。NCP では、MAXBFRU パ

ラメーターによって、PIU を保持するのに使用できる VTAM I/O バッファの数を定義します。IOBUF バッファ・サイズを 441 と選択する場合、10*441 は 4096+29 より大きいため、MAXBFRU=10 は 4K RU を正しく処理します。

- 分散関係データベース体系 接続の手引き では、VTAM IOBUF プールに対する分散データベースの影響を査定する方法について説明されています。IOBUF プール資源を使用しすぎている場合、VTAM パフォーマンスはすべての VTAM アプリケーションで低下します。

通信の定義 (TCP/IP)

この考慮事項については、以前に記述したとおりです (62ページの『ローカル・システム (TCP/IP) の定義』を参照してください)。

機密保護の提供

リモート・システムが SQL アプリケーションに代わって分散データベース処理を実行する場合には、アプリケーション・リクエスター、アプリケーション・サーバー、およびそれらに接続しているネットワークの機密保護要件を満たさなければなりません。これらの要件は、以下のカテゴリーのいくつかに分けられます。

- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護
- データ表示

エンド・ユーザー名の選択

OS/390 システムでは、エンド・ユーザーに 1~8 文字のユーザー ID が割り当てられます。このユーザー ID 値は、特定の OS/390 システムで固有でなければなりません。ネットワーク全体で固有でなくてもかまいません。たとえば、NEWYORK システムで JONES というユーザーがいて、DALLAS システムでまた JONES というユーザーがいてもかまいません。この 2 人のユーザーが同一の人であれば、対立は起きません。しかし、DALLAS の JONES が NEWYORK の JONES とは別人の場合、SNA ネットワーク (およびそのネットワークの分散データベース・システム) は、NEWYORK の JONES と DALLAS の JONES とを区別できません。この状況を訂正しない場合には、DALLAS の JONES は NEWYORK システムの JONES に与えられた特権を使用できます。

名前の対立を解消するため、DB2 ユニバーサル・データベース (OS/390 版) はエンド・ユーザー名前変換のサポートを提供します。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターでアプリケーションが分散データベース要求を行うとき、通信データベースでアウトバウンド名前変換が必要であると指定されていれば、DB2 ユニバーサル・データベース (OS/390 版) は名前変換を実行します。アウトバウンド名前変換が選択されていると、DB2 ユニバーサル・データベース (OS/390 版) は必ず各アウトバウンド分散データベース要求と一緒にパスワードを強制的に送信します。

DB2 ユニバーサル・データベース (OS/390 版) のアウトバウンド名前変換は、SYSIBM.LUNAMES または SYSIBM.IPNAMES 表の USERNAMES 列を 'O' または 'B' に設定すると活動化されます。USERNAMES を 'O' に設定すると、アウトバウンド要求でエンド・ユーザー名前変換が実行されます。USERNAMES を 'B' に設定すると、インバウンド要求とアウトバウンド要求の両方でエンド・ユーザー名前変換が実行されます。

DB2 ユニバーサル・データベース (OS/390 版) の許可は、エンド・ユーザーのユーザー ID および DB2 ユニバーサル・データベース (OS/390 版) プランまたはパッケージ所有者のユーザー ID に依存しているため、エンド・ユーザー名前変換処理は、エンド・ユーザーのユーザー ID、プラン所有者のユーザー ID、およびパッケージ所有者のユーザー ID に対して実行されます。³ 名前変換処理に際しては、SYSIBM.USERNAMES 表から以下の順序で以下のパターン (TYPE.AUTHID.LINKNAME) に一致する行が探索されます。

1. O.AUTHID.LINKNAME - 特定のエンド・ユーザーの特定のパートナー・システムへの変換規則。
2. O.AUTHID.blank - 特定のエンド・ユーザーから任意のパートナー・システムへの変換規則。
3. O.blank.LINKNAME - 任意のユーザーの特定のパートナー・システムへの変換規則。

一致する行が見つからないと、DB2 ユニバーサル・データベース (OS/390 版) は分散データベース要求を拒否します。行が見つかると、NEWAUTHID 列の値が許可 ID として使用されます (ブランクの NEWAUTHID 値は、元の名前を変換しないで使用することを意味します)。

3. 要求が DB2 ユニバーサル・データベース (OS/390 版) サーバーに送信される場合は、名前変換がパッケージ所有者とプラン所有者に対しても実行されます。パッケージ所有者とプラン所有者の名前がパスワードに関連付けられることはありません。

前述の例を考慮してみましょう。NEWYORK の JONES が DALLAS に分散データベース要求を出す場合、この JONES に別の名前 (NYJONES) を与えたものとします。この例において、JONES が使用するアプリケーションは DSNPLAN (DB2 ユニバーサル・データベース (OS/390 版) プラン所有者) の所有で、DALLAS に送信を行うときにこのユーザー ID の変換は不要であるものとします。CDB に名前変換規則を指定するのに必要な SQL ステートメントを図19 に示します。

```
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_OUT, ENCRYPTPSWDS, MODESELECT, USERNAMES)
  VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', '0');
INSERT INTO SYSIBM.LOCATIONS
  (LOCATION, LINKNAME, LINKATTR)
  VALUES ('DALLAS', 'LUDALLAS', '');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('0', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('0', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

図19. アウトバウンド名前変換用 SQL (SNA)

結果として得られる CDB 表を 77ページの図20 に示します。

NEWYORK.SYSIBM.LOCATIONS			
LOCATION	LINKNAME	PORT	TPN
DALLAS	LUDALLAS		

NEWYORK.SYSIBM.LUNAMES						
LUNAME	SYSMODENAME	SECURITY-IN	SECURITY-OUT	ENCRYPTPSWDS	MODESELECT	USERNAMES
LUDALLAS			A	N	N	O

NEWYORK.SYSIBM.USERNAMES				
TYPE	AUTHID	LINKNAME	NEWAUTHID	PASSWORD
0	JONES	LUDALLAS	NYJONES	JONESPWD
0	DSNPLAN	LUDALLAS		PLANPWD

図 20. アウトバウンド名前変換

78ページの図21 に、SNA 接続を使用して DB2 ユニバーサル・データベース DRDA AS に接続するためのより簡単な例を示します。

```

INSERT INTO SYSIBM.LUNAMES (LUNAME,
                            SECURITY_OUT,
                            ENCRYPTPSWDS,
                            USERNAMES)
        VALUES ('NYX1GW01','P','N','0');
INSERT INTO SYSIBM.LOCATIONS (LOCATION,LINKNAME,TPN)
        VALUES('TASG6',
                'NYX1GW01','NYSERVER');
INSERT INTO SYSIBM.USERNAMES (TYPE,AUTHID,LINKNAME,NEAUTHID,PASSWORD)
        VALUES ('0','          ','NYX1GW01','SVTDBM6','SG6JOHN');

```

図 21. アウトバウンド名前変換用 SQL (SNA 用の簡単な例)

79ページの図22 に TCP/IP 接続を使用して DB2 ユニバーサル・データベース DRDA AS に接続するための簡単な例を示します。


```

-- DB2 for Solaris1 - UNIX
DELETE FROM SYSIBM.IPNAMES WHERE LINKNAME = 'SOLARIS1' ;
INSERT INTO SYSIBM.IPNAMES ( LINKNAME
                             , SECURITY_OUT
                             , USERNAMES
                             , IBMREQD
                             , IPADDR)
VALUES ( 'SOLARIS1'
        , 'P'
        , 'O'
        , 'N'
        , '9.21.45.4')
;
INSERT INTO SYSIBM.LOCATIONS ( LOCATION
                               , LINKNAME
                               , IBMREQD
                               , PORT
                               , TPN)
VALUES ( 'TCPDB1'
        , 'SOLARIS1'
        , 'N'
        , '30088'
        , '')
;
INSERT INTO SYSIBM.USERNAMES ( TYPE
                               , AUTHID
                               , LINKNAME
                               , NEWAUTHID
                               , PASSWORD
                               , IBMREQD)
VALUES ( 'O'
        , ''
        , 'SOLARIS1'
        , 'svtdbm5'
        , 'svt5dbm'
        , 'N')
;

```

図 22. アウトバウンド名前変換用 SQL (TCP/IP 用の簡単な例)

ネットワーク機密保護

アプリケーション・リクエスターがリモート・アプリケーションを示すエンド・ユーザー名を選択した後は、そのアプリケーション・リクエスターは必要なネットワーク機密保護情報を提供しなければなりません。

SNA 接続では、LU 6.2 は主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護。VTAM APPL ステートメントの VERIFY キーワードによって制御されます。セッション・レベル機密保護の指定方法についての詳細は、59ページの図17を参照してください。

- 会話レベル機密保護。 SYSIBM.LUNAMES 表の内容によって制御されます。
- データ暗号化。 VTAM 3.4 以降のリリースでのみサポートされています。

アプリケーション・サーバーの責任でデータベース資源を管理するため、アプリケーション・サーバーは、どのネットワーク機密保護にアプリケーション・リクエストが必要かを指示します。各アプリケーション・サーバーの会話レベル機密保護要件を SYSIBM.LUNAMES 表または SYSIBM.IPNAMES 表に記録する必要があります。そのためには USERNAMES 列を、アプリケーション・サーバーの要件を反映するように設定します。

SNA 会話機密保護オプションは以下のとおりです。

SECURITY=SAME

これは検査済みの機密保護とも言います。それは、エンド・ユーザーのユーザー ID だけがリモート・システムに送信されるためです (パスワードは送信されません)。このレベルの会話機密保護は、SYSIBM.LUNAMES の USERNAMES 列に 'O' または 'B' が入っていない場合に使用してください。

DB2 ユニバーサル・データベース (OS/390 版) ではエンド・ユーザー名前変換がアウトバウンド会話機密保護に関連付けられているので、アウトバウンド・エンド・ユーザー名変換が活動化されている場合に SECURITY=SAME を使用することはできません。

SECURITY=PGM

このオプションを使用すると、エンド・ユーザー ID とパスワードが妥当性検査のためにリモート・システムに送信されます。この機密保護オプションは、SYSIBM.LUNAMES 表の USERNAMES 列に 'O' か 'B' のいずれかが入っている場合に使用してください。

SYSIBM.LUNAMES 表に指定されているオプションに応じて、DB2 ユニバーサル・データベース (OS/390 版) は 2 つの異なる情報源からユーザーのパスワードを取得します。

- 暗号化されていないパスワードは、SYSIBM.USERNAMES 表の PASSWORD 列から取得されます。SYSIBM.LUNAMES の ENCRYPTPSWDS 列が 'Y' に設定されていない場合、DB2 ユニバーサル・データベース (OS/390 版) は SYSIBM.USERNAMES 表からパスワードを抽出します。この情報源から取得したパスワードは、どの DRDA アプリケーション・サーバーに対しても送信できます。

図23 では、SMITH と JONES のパスワードを定義しています。この例の LUNAME 列はブランクなので、これらのパスワードは SMITH または JONES がアクセスしようとするどのリモート・システムでも使用できます。

```
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'SMITH', ' ', ' ', 'SMITHPWD');
```

図23. リモート・サイトへのパスワードの送信 (SNA)

- SYSIBM.LUNAMES の ENCRYPTPSWDS 列が 'Y' を含んでいる場合、暗号化パスワードはリモート・サイトに送信されます。暗号化パスワードは RACF (または RACF と同等の製品) から抽出され、別の DB2 ユニバーサル・データベース (OS/390 版) システムによってのみ解釈できます。DB2 ユニバーサル・データベース (OS/390 版) 以外のシステムと通信している場合は、ENCRYPTPSWDS を 'Y' に設定しないでください。

DB2 ユニバーサル・データベース (OS/390 版) は SYSIBM.USERNAMES 表を探索して、リモート・システムに送信するユーザー ID (NEWAUTHID 値) を判別します。変換されたこの名前は、RACF のパスワード抽出のために使用されます。名前を変換したくない場合は、名前を変換しないで送信するための行を SYSIBM.USERNAMES の中に作成する必要があります。図24 は、エンド・ユーザー名 (ユーザー ID) を変換せずに要求を LUDALLAS と LUNYC に送信できるようにします。

```
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUDALLAS', ' ', ' ');
```

図24. リモート・サイトへの暗号化パスワードの送信 (SNA)

SECURITY=NONE

DRDA はこのオプションをサポートしていないため、DB2 ユニバーサル・データベース (OS/390 版) ではこの機密保護オプションを使用できません。

データベース・マネージャー機密保護

アプリケーション・リクエスターが分散データベースの機密保護に貢献できる 1 つの方法は、前に 74 ページの『エンド・ユーザー名の選択』で説明されたように、アウトバウンド・ユーザー名前変換です。アウトバウンド・ユーザー名前変換を使用すると、要求を出しているユーザーおよびアプリケーションの ID に従って、各アプリケーション・サーバーへのアクセスを制御できます。その他に、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターが分散システムの機密保護に貢献できる方法には以下のものがあります。

リモート・アプリケーションのバインド

エンド・ユーザーはアプリケーション・サーバーのリモート・アプリケーションを、DB2 ユニバーサル・データベース (OS/390 版) BIND PACKAGE コマンドを使ってバインドします。DB2 ユニバーサル・データベース (OS/390 版) は、リクエスターでの BIND PACKAGE コマンドの使用を制限しません。ただし、エンド・ユーザーは、リモート・パッケージが DB2 ユニバーサル・データベース (OS/390 版) プランに組み込まれるまで、このパッケージを使用できません。DB2 ユニバーサル・データベース (OS/390 版) は、BIND PLAN コマンドの使用を制限します。エンド・ユーザーは、DB2 ユニバーサル・データベース (OS/390 版) GRANT ステートメントで BIND または BINDADD 特権を与えられないかぎり、リモート・パッケージをプランに追加することができません。

パッケージをバインドするときは、ENABLE/DISABLE オプションを使用して、パッケージを TSO、CICS/ESA、IMS/ESA、またはリモート DB2 ユニバーサル・データベース (OS/390 版) サブシステムから使用できるかどうかを指定してください。

リモート・アプリケーションの実行

DB2 ユニバーサル・データベース (OS/390 版) エンド・ユーザーがリモート・アプリケーションを実行するには、そのアプリケーションに関連した DB2 ユニバーサル・データベース (OS/390 版) プランを実行する権限がエンド・ユーザーになければなりません。DB2 ユニバーサル・データベース (OS/390 版) プランの所有者には、自動的にそのプランの実行権限が与えられます。他のエンド・ユーザーは、DB2 ユニバーサル・データベース (OS/390 版) GRANT EXECUTE ステートメントで、プランの実行権限を与えてもらうことができます。このようにして、分散データベース・アプリケーションの所有者は個々のユーザー・ベースでアプリケーションの使用を制御できます。

機密保護サブシステム

OS/390 システムの外部機密保護サブシステムは、通常、 RACF または RACF と互換性のあるインターフェースを備えた他の製品により提供されます。 DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターには、外部の機密保護サブシステムを直接呼び出すことはありません。ただし、79ページの『ネットワーク機密保護』で説明された暗号化パスワード・サポートは例外です。しかし、以下の状況ではアプリケーション・リクエスターで外部機密保護サブシステムが間接的に使用されます。

- エンド・ユーザーと DB2 ユニバーサル・データベース (OS/390 版) との接続を受け持つ製品が、エンド・ユーザーの ID (ユーザー ID およびパスワード) の妥当性検査をするために外部機密保護サブシステムを使用する場合。これは、エンド・ユーザーが DB2 ユニバーサル・データベース (OS/390 版) に接続する前に生じます。前述のとおり、CICS/ESA、TSO、および IMS/ESA は、エンド・ユーザーを DB2 ユニバーサル・データベース (OS/390 版) に接続する製品の一部です。
- SNA セッション・レベル機密保護を (DB2 ユニバーサル・データベース (OS/390 版) VTAM APPL ステートメントの VERIFY キーワードによって) 使用する場合、VTAM により外部機密保護サブシステムが呼び出されて、リモート・システムの ID が妥当性検査されます。

データの表示

DB2 ユニバーサル・データベース (OS/390 版) は、省略時のインストール・システム・コード化文字セット ID (CCSID) が 500 の状態で出荷されています。この省略時値はおそらく、ご使用のインストール・システムでは正しくないでしょう。

DB2 ユニバーサル・データベース (OS/390 版) をインストールするときには、インストール・システムの CCSID を、ご使用のサイトの入力装置が生成して DB2 ユニバーサル・データベース (OS/390 版) に送る文字の CCSID に設定する必要があります。通常、この CCSID はご使用になる言語によって決定されます。インストール・システムの CCSID が間違っていると、文字変換の結果が誤ったものになります。国別または言語別のサポートされる CCSID のリストについては、*DB2 コネクト 使用者の手引き* を参照してください。

ご使用の DB2 ユニバーサル・データベース (OS/390 版) サブシステムが、各アプリケーション・サーバーの CCSID を DB2 ユニバーサル・データベース (OS/390 版) サブシステムのインストール・システムの CCSID に変換できるかどうか確認する必要があります。変換元 CCSID と変換先の CCSID の一般的な組み合わせについては、DB2 ユニバーサル・データベース (OS/390 版)

に変換テーブルが用意されていますが、可能なすべての組み合わせに対応しているわけではありません。必要であれば、使用可能な変換テーブルと変換ルーチンのセットを追加できます。DB2 ユニバーサル・データベース (OS/390 版) 文字変換の詳細については、DB2 ユニバーサル・データベース (OS/390 版) 管理の手引き を参照してください。

アプリケーション・サーバーのセットアップ

DB2 ユニバーサル・データベース (OS/390 版) のアプリケーション・サーバー・サポートによって、DB2 ユニバーサル・データベース (OS/390 版) は DRDA アプリケーション・リクエスターのサーバーとして機能することができます。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに接続されたアプリケーション・リクエスターは、以下のものとして機能することができます。

- DB2 ユニバーサル・データベース (OS/390 版) リクエスター
- DB2 コネクト
- DB2 コネクト・サポートが使用できる DB2 ユニバーサル・データベース エンタープライズ・エディションまたは DB2 ユニバーサル・データベース エンタープライズ拡張エディション。
- DB2 バージョン 2 リクエスター。AIX、HP-UX、OS/2、Solaris、Windows 3.1、Windows 3.11 for Workgroups、Windows 95、または Windows NT、および Macintosh、SCO、SGI、または SINIX 上で実行できます。分散データベース接続サービス (DDCS) マルチ・ユーザー・ゲートウェイ・バージョン 2.3、DDCS 単一ユーザー・バージョン 2.3、および DDCS (Windows 版) バージョン 2.4 には、この機能があります。
- OS/400 リクエスター。
- DB2 (VM 版) リクエスター。
- DRDA アプリケーション・リクエスター・プロトコルをサポートする任意の製品。

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに接続されたアプリケーション・リクエスターの場合、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは以下のようにデータベース・アクセスをサポートします。

- アプリケーション・リクエスターは、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに保管された表にアクセスすることが許されています。アプリケーション・リクエスターが DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーでパッケージを

作成してからでなければ、アプリケーションを実行することはできません。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは、実行時にアプリケーションの SQL ステートメントを探すのにこのパッケージを使用します。

- アプリケーション・リクエスターは DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに、DRDA リクエスターとサーバーとの接続が 2 フェーズ・コミット処理をサポートしない場合、アクセスが読み取り専用で制限されることを知らせることができます。たとえば、CICS フロントエンドを持つ DDCS V2R3 リクエスターは、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに対して、更新は許可されないことを通知できます。
- アプリケーション・リクエスターはさらに、システム主導アクセスを使用するネットワーク内の他の DB2 ユニバーサル・データベース (OS/390 版) システムに保管されているテーブルへのアクセスを許可されることもあります。システム主導アクセスによって、アプリケーション・リクエスターが単一の作業単位で複数のデータベース・システムに接続を確立できるようになります。

ネットワーク情報の提供

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーが適正に分散データベース要求を処理するためには、次のステップを踏む必要があります。

1. アプリケーション・サーバーをローカルのコミュニケーション・マネージャーに定義する。
2. 使用される可能性のある各 2 次サーバーの宛先を定義し、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーが SQL 要求を最終的な宛先に再経路指定できるようにする。
3. 必要な機密保護を提供する。
4. データ表示を提供する。

アプリケーション・サーバー (SNA) を定義する

アプリケーション・サーバーが分散データベース要求を受信するためには、これをローカルなコミュニケーション・マネージャーに定義し、固有の RDB_NAME 名を割り当てる必要があります。以下の説明は SNA 接続と関連しています。アプリケーション・サーバーを正しく定義するには、次のステップを踏む必要があります。

1. DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーが使用する LU 名と RDB_NAME を選択する。これらの名前を DB2 ユ

ユニバーサル・データベース (OS/390 版) と VTAM に記録するプロセスは、55ページの『ローカル・システム (SNA) の定義』に説明されているプロセスと同じです。DB2 ユニバーサル・データベース (OS/390 版) のために選択する RDB_NAME を、アプリケーション・サーバーへのコネクティビティーが必要なすべてのエンド・ユーザーおよびアプリケーション・リクエスターに供給しなければなりません。

2. アクセスに必要なアプリケーション・リクエスターごとに NETID.LUNAME 値を DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに登録して、アプリケーション・リクエスターが SNA 要求を DB2 ユニバーサル・データベース (OS/390 版) サーバーに経路指定できるようにします。アプリケーション・リクエスターがダイナミック・ネットワーク・ルーティングを実行できる場合でも、そのようにしてください。アプリケーション・リクエスターは NETID.LUNAME を知らないダイナミック・ネットワーク・ルーティングを使用できないからです。
3. DRDA 省略時 TPN (X'07F6C4C2') を各アプリケーション・リクエスターに指定します。DB2 ユニバーサル・データベース (OS/390 版) が自動的にこの値を使用するためです。
4. アプリケーション・リクエスターで要求された各モード名ごとに、VTAM モード表に項目を作成します。これらの項目は、各モード名の RU サイズ、歩調合わせウィンドウ・サイズ、およびサービス・クラスを記述します。
5. DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに接続するアプリケーション・リクエスターに、セッション限度を定義します。VTAM APPL ステートメントは、すべてのパートナー・システムにあてはまる省略時のセッション限度を定義します。特定のパートナーに対して固有の省略時値を設定したい場合は、通信データベース (CDB) の SYSIBM.LUMODES 表を使用できます。
VTAM ネットワークを調べる方法については、73ページの『RU サイズおよび歩調合わせの設定』を参照してください。
6. DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーへの接続が許可されたアプリケーション・リクエスターを識別するための項目を DB2 ユニバーサル・データベース (OS/390 版) CDB に作成します。ネットワーク内のアプリケーション・リクエスター用に CDB 項目を定義する 2 つの基本的な方法は、以下のとおりです。
 - a. CDB で特に記述されていない、任意の LU に使用する省略時値を指定する行を SYSIBM.LUNAMES に挿入できます (省略時の行は LUNAME

列がブランクです)。この方法では、ネットワーク内のいくつかの LU に対しては特定の属性を与え、一方、他のすべての LU については省略時値を設定できます。

たとえば、DALLAS システム (別の DB2 ユニバーサル・データベース (OS/390 版) システム) には検査済み分散データベース要求 (LU 6.2 SECURITY=SAME) を送信することを許可する一方で、データベース・マネージャー・システムにはパスワードを送信させるということができます。さらに、特にデータベース・マネージャー・システムが多数ある場合などは、システムごとに CDB に項目を作成したくない場合があります。図25 では、DALLAS システムに対して SECURITY=SAME を指定する一方、他のすべてのリクエスターに対しては SECURITY=PGM にさせるために CDB を使用する方法を示します。

```
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

図 25. アプリケーション・リクエスター接続の省略時値の確立 (SNA)

- b. CDB を次のいずれかに設定することにより、CDB を使用してネットワーク内の各アプリケーション・リクエスターに個別に許可を与えることができます。
 - SYSIBM.LUNAMES 中に省略時の行を記録しないようにする。省略時の行 (LU 名がブランクの行) が存在しない場合、DB2 ユニバーサル・データベース (OS/390 版) は、接続しようとする各アプリケーション・リクエスターの LU 名を含んだ SYSIBM.LUNAMES 中の行を必要とします。対応する行が CDB に見つからない場合、アプリケーション・リクエスターはアクセスを拒否されます。
 - SYSIBM.LUNAMES に、come-from 検査が必要であることを指定した省略時の行を記録する (USERNAMES 列を 'I' または 'B' に設定)。これにより、89ページの『Come-From 検査』で説明されているように、DB2 ユニバーサル・データベース (OS/390 版) はアクセスをアプリケーション・リクエスターおよび SYSIBM.USERNAMES 表で定義されたエンド・ユーザーに限定します。名前変換規則が SYSIBM.LUNAMES 中にブランク LU 名の行を必要とするものの、この行の使用によって DB2 ユニバーサル・データベース (OS/390

版) が DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーへの無制限なアクセスを許可するようにはしたくない場合、この方法を使用できます。

図26 では、LUNAME 列にブランクの行はないため、DB2 ユニバーサル・データベース (OS/390 版) は LUDALLAS または LUNYC 以外の LU へのアクセスをすべて拒否します。

```
INSERT INTO SYSIBM.LUNAMES
(LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
(LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

図 26. 個々のアプリケーション・リクエスター接続の識別 (SNA)

アプリケーション・サーバー (TCP/IP) を定義する

アプリケーション・サーバーが TCP/IP 接続上で分散データベース要求を受信するためには、アプリケーション・サーバーをローカル TCP/IP サブシステムに定義し、固有の RDB_NAME を割り当てる必要があります。さらに、DB2 ユニバーサル・データベース (OS/390 版) ブートストラップ・データ・セットは必要なパラメーターを含んでいなければなりません。そして、DB2 ユニバーサル・データベース (OS/390 版) 通信データベース (CDB) に更新が必要な場合もあります。

1. AS での TCP/IP のセットアップについては、DB2 ユニバーサル・データベース (OS/390 版) インストレーションの手引きを参照してください。AR のセットアップ方法については、DB2 コネクト エンタープライズ・エディション (OS/2 および Windows NT 版) 概説およびインストール、および DB2 コネクト パーソナル・エディション 概説およびインストールに説明されています。
2. ブートストラップ・データ・セット定義の例を 63ページの図18 に示します。
3. インバウンド・データベース接続のみを使用する場合は、CDB の更新は必要ありません。それで、DB2 ユニバーサル・データベース (OS/390 版) をサーバーとしてのみ使用する計画であるなら、CDB にデータを読み込む必要はなく、省略時値を使用できます。以下に SYSIBM.IPNAMES を更新する簡単な方法を示します。

TCP/IP ノードへのインバウンド・データベース接続要求を許可したい場合、SQL コマンドを使用して以下のようにこの表を更新することができます。

```
INSERT INTO SYSIBM.IPNAMES (LINKNAME) VALUES('      ')
```

機密保護の提供

アプリケーション・リクエスターが分散データベース要求を DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーに向けるときには、以下の機密保護上の考慮事項が関係します。

- come-from 検査
- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護

Come-From 検査

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーがエンド・ユーザー名をアプリケーション・リクエスターから受け取る場合、アプリケーション・サーバーは指定されたアプリケーション・リクエスターから受け取るエンド・ユーザー名を制限できます。これは *come-from* 検査を使用することで行えます。come-from 検査を使用すると、アプリケーション・サーバーは、所定のユーザー ID が特定のパートナーだけに使用されるよう指定できます。たとえば、アプリケーション・サーバーは JONES を DALLAS だけ「から来る (come-from)」よう制限できます。(DALLAS 以外の) 別のアプリケーション・リクエスターが名前 JONES をアプリケーション・サーバーに送ろうとする場合、アプリケーション・サーバーはその名前が適正なネットワーク・ロケーションから来なかったために要求を拒否できます。

DB2 ユニバーサル・データベース (OS/390 版) は come-from 検査をインバウンド・エンド・ユーザー名前変換の一部として実装しています。これについては次の節で説明します。

注: インバウンドおよび come-from 検査は TCP/IP インバウンド要求に対してなされます。

エンド・ユーザー名の選択

アプリケーション・リクエスターによって渡されるユーザー ID は、SNA ネットワーク全体で一意ではないことがあります。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーはインバウンド名前変換を実行して、SNA ネットワーク全体を通じて固有なエンド・ユーザー名を作成する必要があるかもしれません。同様に、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーはアウトバウンド名前変換を実行し

て、アプリケーションに関係する 2 次サーバーに対して固有なエンド・ユーザー名を与える必要があるかもしれません。(アウトバウンド・エンド・ユーザー名前変換については、74 ページの『機密保護の提供』を参照してください。)

インバウンド名前変換は、SYSIBM.LUNAMES または SYSIBM.IPNAMES 表の USERNAMES 列を 'I' (インバウンド変換) または 'B' (インバウンドおよびアウトバウンド両方の変換) に設定することにより、使用可能にできます。インバウンド名前変換が有効であるとき、DB2 ユニバーサル・データベース (OS/390 版) はアプリケーション・リクエスターによって送られたユーザー ID を変換して、DB2 ユニバーサル・データベース (OS/390 版) は所有者の名前を立案します (アプリケーション・リクエスターが別の DB2 ユニバーサル・データベース (OS/390 版) システムである場合)。

アプリケーション・リクエスターがユーザー ID およびパスワードの両方を APPC ALLOCATE verb に関して送る場合、ユーザー ID およびパスワードはユーザー ID が変換される前に妥当性検査されます。SYSIBM.USERNAMES の PASSWORD 列は、パスワード妥当性検査には使用されません。代わりに、ユーザー ID とパスワードが妥当性検査のため、外部機密保護システム (RACF または RACF と同等の製品) に送られます。

ALLOCATE verb の着信ユーザー ID が検査されるとき、DB2 ユニバーサル・データベース (OS/390 版) は許可出口ルーチンを持ちます。これは、2 次 AUTHID のリストを提供し、追加の機密保護検査を実行するために使用できます。詳細については、DB2 ユニバーサル・データベース (OS/390 版) 管理の手引きを参照してください。

インバウンド名前変換処理は SYSIBM.USERNAMES 表の中の行を検索しますが、これは以下の優先順位リスト (TYPE.AUTHID.LINKNAME) のうちの 1 つのパターンと一致しなければなりません。

1. I.AUTHID.LINKNAME - 特定のアプリケーション・リクエスターからの特定のエンド・ユーザー
2. I.AUTHID.blank - 任意のアプリケーション・リクエスターからの特定のエンド・ユーザー
3. I.blank.LINKNAME - 特定のアプリケーション・リクエスターからの任意のエンド・ユーザー

行が検出されない場合、リモート・アクセスは拒否されます。行が検出されると、リモート・アクセスが許可され、エンド・ユーザー名は NEWAUTHID 列で与えられた値に変換されます。NEWAUTHID 値がブランクの場合は名前が変更されないことを示します。任意の DB2 ユニバーサル・データベース

(OS/390 版) 資源に対する許可の検査 (たとえば、SQL 表特権) が、DB2 ユニバーサル・データベース (OS/390 版) により、元のユーザー名ではなく変換されたエンド・ユーザー名に対して実行されます。

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーがアプリケーション・リクエスターからエンド・ユーザー名を受け取る場合、DB2 ユニバーサル・データベース (OS/390 版) インバウンド名前変換機能を使用することによって以下のいくつかの目的が達成されます。

- エンド・ユーザー名を固有のものに変更できる。たとえば、以下の SQL ステートメントは、NEWYORK アプリケーション・リクエスター (LUNAME LUNYC) のエンド・ユーザー名 JONES を異なった名前 (NYJONES) に変換します。

```
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', '');
```

- エンド・ユーザー名を変更して、エンド・ユーザーのグループをすべて単一の名前で表現できる。たとえば、NEWYORK アプリケーション・リクエスター (LUNAME LUNYC) からのすべてのユーザーをユーザー名 NYUSER で表現したいとします。そうすると、NYUSER という名前に対して SQL 特権を認可することにより、NEWYORK のユーザーに付与する SQL アクセスを制御できるようになります。

```
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUNYC', 'NYUSER', '');
```

- 特定のアプリケーション・リクエスターから送られてくるエンド・ユーザーを制限することができます。エンド・ユーザー名前変換のこの使用法により、89ページの『Come-From 検査』で説明した come-from 検査を実行できます。たとえば、以下の SQL ステートメントは NEWYORK アプリケーション・リクエスターのエンド・ユーザーとして SMITH および JONES だけを許可します。その他の名前は、SYSIBM.USERNAMES 表にリストされていないため、アクセスが拒否されます。

```
INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
```

```

INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');

```

- DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーへの接続が許可されるアプリケーション・リクエスターを制限できます。これは come-from 検査のさらにもう 1 つの機能です。以下の例では、NEWYORK アプリケーション・リクエスター (LUNYC) または CHICAGO アプリケーション・リクエスター (LUCI) によって送られるエンド・ユーザーだけが受け入れられます。省略時の SYSIBM.LUNAMES 行がすべてのインバウンド要求に対してインバウンド名前変換を指定しているため、その他のアプリケーション・リクエスターはアクセスを拒否されます。

```

INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
  MODESELECT, USERNAMES)
  VALUES (' ', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUCI', ' ', ' ');

```

ネットワーク機密保護の提供

SNA 接続では、LU 6.2 は主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護
- 会話レベル機密保護
- 暗号化

79ページの『ネットワーク機密保護』では、DB2 ユニバーサル・データベース (OS/390 版) でのセッション・レベル機密保護および暗号化について説明しています。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターとまったく同様に、セッション・レベルの機密保護および暗号化を使用します。

残りのネットワーク機密保護の考慮事項は、SNA 会話レベル機密保護だけです。会話レベル機密保護のいくつかの面は DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバー独自のものです。DB2 ユニバーサ

ル・データベース (OS/390 版) アプリケーション・サーバーはネットワーク機密保護において 2 つの異なった役割を果たします。

- 2 次サーバーへのリクエスターとして、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは 2 次サーバーが必要とする SNA 会話レベル機密保護パラメーターを含んだ APPC 要求を発行する責任があります。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは SYSIBM.LUNAMES 表の USERNAMES 列、および SYSIBM.USERNAMES 表を使用して、各 2 次サーバーごとに SNA 会話レベル機密保護要件を定義します。これらの定義の詳細については、79 ページの『ネットワーク機密保護』で説明した内容と同一です。
- アプリケーション・リクエスターのサーバーとして、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーはアプリケーション・リクエスターの SNA 会話レベル機密保護要件を指定します。DB2 ユニバーサル・データベース (OS/390 版) は SYSIBM.LUNAMES 表の USERSECURITY 列を使用して、ネットワーク内の各アプリケーション・リクエスターに必要な会話機密保護を判別します。以下の値が USERSECURITY 列で使用されます。

C これは、DB2 ユニバーサル・データベース (OS/390 版) には分散データベースごとにアプリケーション・リクエスターがユーザー ID およびパスワード (LU 6.2 SECURITY=PGM) を送る必要があることを示しています。SYSIBM.LUNAMES の ENCRYPTPSWDS 列に 'Y' が含まれる場合、DB2 ユニバーサル・データベース (OS/390 版) はパスワードが RACF 暗号化形式で準備されている (これは DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・リクエスターの場合にのみ可能) と想定します。ENCRYPTPSWDS 列が 'Y' でない場合、DB2 ユニバーサル・データベース (OS/390 版) はパスワードが標準 LU 6.2 形式 (EBCDIC 文字表示) になっているものとみなします。どちらの場合でも、DB2 ユニバーサル・データベース (OS/390 版) はユーザー ID とパスワード値を妥当性検査のために機密保護サブシステムに渡します。APPC ユーザー ID とパスワード検査を行える機密保護サブシステムが必要となります。たとえば、RACF には APPC ユーザー ID とパスワードの検査を行う機能があります。機密保護サブシステムがユーザー ID とパスワードの対を拒否した場合、分散データベース・アクセスは拒否されます。

その他の値

これは、アプリケーション・リクエスターが検査済みユーザー ID (LU 6.2 SECURITY=SAME) またはユーザー ID とパスワード (LU

6.2 SECURITY=PGM) のいずれかを送信できることを示しています。ユーザー ID とパスワードが送信されると、DB2 ユニバーサル・データベース (OS/390 版) はそれらを 'C' について上記で述べたのと同様の方法で処理します。要求がユーザー ID のみを含んでいる場合、インバウンド・ユーザー ID が管理されるために SYSUSERNAMES 表が使用されるのでない限り、機密保護サブシステムが呼び出されて、ユーザーの認証がなされます。

機密保護違反が検出された場合、LU 6.2 は DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバー が SNA 機密保護違反センス・コード ('080F6051'X) をアプリケーション・リクエスターに送るようにします。このセンス・コードは障害の原因を示すものではないので、DB2 ユニバーサル・データベース (OS/390 版) は 2 つの方式で分散機密保護違反の原因を記録します。

- DSNL030I メッセージを生成する。これには、リクエスターの LUWID、および障害を記述する DB2 理由コードが示されます。DSNL030I には (分かる場合には) AUTHID も含まれます。これは拒否されたアプリケーション要求から送信されたものです。
- NETVIEW ハードウェア・モニター・データベースにアラートが記録される。この中には、DSNL030I メッセージに示されるのと同一の情報が収められます。

データベース・マネージャー機密保護

データベース資源の所有者として、DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーは、そこにある SQL オブジェクトに対してデータベース機密保護機能を制御します。DB2 ユニバーサル・データベース (OS/390 版) が管理するオブジェクトへのアクセスは、特権によって制御されます。これは、DB2 ユニバーサル・データベース (OS/390 版) 管理者または個々のオブジェクトの所有者によって、ユーザーに与えられます。DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーが制御する 2 つの基本的なオブジェクトのクラスは以下のとおりです。

- **パッケージ** — 個々のエンド・ユーザーは、DB2 ユニバーサル・データベース (OS/390 版) GRANT ステートメントを使用して、パッケージの作成、置換、実行を行う権限を持っています。エンド・ユーザーがパッケージを所有する場合、そのユーザーは自動的にパッケージの実行または置換を行うことができます。他のエンド・ユーザーは DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーの GRANT ステートメントで、パッケージを実行するよう許可を受ける必要があります。USE は、個々のエ

ンド・ユーザーまたは PUBLIC に認可することができます。PUBLIC は、パッケージの実行をすべてのエンド・ユーザーに許可します。

アプリケーションが DB2 ユニバーサル・データベース (OS/390 版) にバインドされるとき、パッケージにはアプリケーション・プログラムに含まれる SQL ステートメントが含まれています。これらの SQL ステートメントは以下のように分けられます。

静的 SQL

静的 SQL は、SQL ステートメントおよびそのステートメントにより参照される SQL オブジェクトが、アプリケーションが DB2 ユニバーサル・データベース (OS/390 版) にバインドされるときに認識されることを意味します。パッケージの作成者は、パッケージ内のそれぞれの静的 SQL ステートメントを実行する権限を持っていないければなりません。

エンド・ユーザーがパッケージを実行する権限を与えられるとき、そのユーザーはパッケージに含まれる各静的 SQL ステートメントを実行する権限を自動的に与えられます。それで、実行されるパッケージに静的 SQL ステートメントしか含まれていない場合には、エンド・ユーザーは DB2 ユニバーサル・データベース (OS/390 版) 表特権を必要としません。

動的 SQL

動的 SQL は、プログラムが実行するまで認識されない SQL ステートメントのことです。言い換えると、SQL ステートメントはプログラムによって作成され、SQL PREPARE ステートメントを使用して DB2 ユニバーサル・データベース (OS/390 版) に動的にバインドされます。エンド・ユーザーが動的 SQL ステートメントを実行するとき、そのユーザーには SQL ステートメントを実行するために必要な表特権がなければなりません。プランまたはパッケージが作成されるときに SQL ステートメントが認識されないため、エンド・ユーザーにはパッケージ所有者により必要な権限が自動的に与えられません。

- **SQL オブジェクト** - これは表、視点、シノニム、または別名です。DB2 ユニバーサル・データベース (OS/390 版) ユーザーには、個々の SQL オブジェクトを作成、削除、変更、または読み取る権限の各種のレベルを認可できます。この権限は、静的 SQL ステートメントをバインドしたり、動的 SQL ステートメントを実行するために必要です。

パッケージを作成するとき、DISABLE/ENABLE オプションによって、どの DB2 ユニバーサル・データベース (OS/390 版) 接続タイプがパッケージを実

行できるか制御することができます。 RACF および DB2 ユニバーサル・データベース (OS/390 版) 機密保護出口ルーチンを使用して、エンド・ユーザーに選択的に DDF の使用を許可できます。 RLF を使用して、リモート・バインドおよび動的 SQL 実行のプロセッサ時間を制限できます。

MYPKG という名前の DB2 ユニバーサル・データベース (OS/390 版) パッケージについて考慮します。これは JOE が所有しているものとします。 JOE は SAL に対して、 DB2 ユニバーサル・データベース (OS/390 版) GRANT USE ステートメントを発行することにより、このパッケージの実行を許可できます。 SAL がこのパッケージを実行すると、以下の事柄が発生します。

- DB2 ユニバーサル・データベース (OS/390 版) は SAL がこのパッケージに対する USE 権限を与えられているかどうか検査します。
- JOE はパッケージの作成に必要な SQL オブジェクト特権を持っているので、SAL はパッケージ中のすべての静的 SQL ステートメントを発行することができます。
- パッケージが動的 SQL ステートメントを含んでいる場合は、SAL は自分自身の SQL 表特権を持っている必要があります。たとえば、SAL は JOE.TABLE5 への読み取りアクセスを認可されていない限り、SELECT * FROM JOE.TABLE5 を発行することはできません。

機密保護サブシステム

DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーの機密保護サブシステム (RACF または RACF と同等の製品) の使用法は、SYSIBM.LUNAMES 表でインバウンド名前変換機能をどのように定義したかに応じて異なります。

- USERNAMES 列に 'T' または 'B' を指定した場合、インバウンド名前変換はアクティブになり、DB2 ユニバーサル・データベース (OS/390 版) は DB2 ユニバーサル・データベース (OS/390 版) 管理者がインバウンド名前変換を使用してシステム機密保護制約を部分的に実施するものとみなします。外部機密保護サブシステムが呼び出されるのは、アプリケーション・リクエスターがユーザー ID およびパスワードの両方を含む要求を送る場合だけです。APPC ユーザー ID とパスワード検査を行える機密保護サブシステムが必要となります。たとえば、RACF には APPC ユーザー ID とパスワードの検査を行う機能があります。

アプリケーション・リクエスターからの要求にユーザー ID (SECURITY=SAME) だけが含まれる場合、外部機密保護システムはまったく呼び出されません。インバウンド名前変換の規則によって、どのユーザーに DB2 ユニバーサル・データベース (OS/390 版) アプリケーション・サーバーへの接続が許可されているかが定義されているからです。

- 'I' または 'B' 以外の値が `USERNAMES` 列に指定されていた場合、以下の機密保護サブシステム検査が実行されます。
 - 分散データベース要求をアプリケーション・リクエスターから受け取った場合、`DB2 ユニバーサル・データベース (OS/390 版)` は外部機密保護システムを呼び出して、エンド・ユーザーのユーザー ID (供給された場合にはパスワードも) の妥当性検査を行います。
 - 外部機密保護システムが呼び出されて、エンド・ユーザーが `DB2 ユニバーサル・データベース (OS/390 版)` サブシステムへの接続を許可されているかどうか検査されます。
- どちらの場合も、許可出口ルーチンが駆動されて、2 次許可 ID のリストが与えられます。詳細については、`DB2 ユニバーサル・データベース (OS/390 版) 管理の手引き` を参照してください。

データの表示

ご使用の `DB2 ユニバーサル・データベース (OS/390 版)` サブシステムが、各アプリケーション・リクエスターの `CCSID` を `DB2 ユニバーサル・データベース (OS/390 版)` サブシステムのインストール・システムの `CCSID` に変換できるかどうか確認する必要があります。詳細については、83ページの『データの表示』を参照してください。

第3章 SNA を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続

OS/400 には、DB2 ユニバーサル・データベース (AS/400 版) (AS/400 システム用の IBM 関係データベース管理システム) が含まれています。

この章では、AS/400 システムがコネクティビティーをサポートするように構成する方法を説明します。

1. DB2 コネクト ワークステーションから (112ページの『アプリケーション・サーバーのセットアップ』を参照)
 2. DB2 ユニバーサル・データベース・サーバーへ (100ページの『アプリケーション・リクエスターのセットアップ』を参照)
- 2 つの AS/400 システムを接続することについての詳細は、AS/400 分散データベース・プログラミングを参照してください。

DB2 ユニバーサル・データベース (AS/400 版) バージョン 4.2 では、TCP/IP を使用した DRDA 通信がサポートされるようになりました。このトピックについての情報のメイン・ソースは、AS/400 分散データベース・プログラミングであり、必須ステップのまとめがこのマニュアルに基づいて 119ページの『第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』に示されています。ここでの指針は、この章に示されている指針と同じですが、ネットワーク構成タスクはずっと簡単です。

DB2 ユニバーサル・データベース (AS/400 版) インプリメンテーション

この章では、DB2 ユニバーサル・データベース (AS/400 版) がどのように分散データベース・システムをサポートするかを説明します。OS/400 バージョン 2 リリース 1 モディフィケーション 1 ライセンス・プログラムでは、DRDA リモート作業単位をサポートしていましたが、OS/400 バージョン 3 リリース 1 で、DRDA 分散作業単位 (DUOW) のサポートが追加されました。このサポートは、OS/400 オペレーティング・システムの一部です。これにより、DRDA サポートを使用する際、または組み込み SQL を使用してプログラムを実行する際に、DB2 ユニバーサル・データベース (AS/400 版) の照会マネージャーおよび SQL 開発者キットを使用する必要はなくなりました。

アプリケーション・リクエスターのセットアップ

AS/400 システムでは、OS/400 オペレーティング・システムの重要な部分として DRDA アプリケーション・リクエスター・サポートを実装しています。アプリケーション・リクエスターは OS/400 オペレーティング・システムの一部であるため、オペレーティング・システムが活動中のときは常に活動中です。このことは DB2 ユニバーサル・データベース (AS/400 版) のアプリケーション・サーバーのサポートに関しても同様です。

DB2 ユニバーサル・データベース (AS/400 版) がアプリケーション・リクエスターとして機能するとき、これは DRDA をサポートするアプリケーション・サーバーには接続できません。DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・リクエスターが分散データベース・アクセスを提供するためには、以下の方法を知らなければなりません。

- ネットワーク情報の提供
- 機密保護の提供
- データの表示

ネットワーク情報の提供

アプリケーション・リクエスターは、関係データベース名を受け入れ、それをネットワーク・パラメーターに変換できなければなりません。AS/400 システムは、関係データベース・ディレクトリーを使用して、関係データベース名および対応するネットワーク・パラメーターを登録します。このディレクトリーにより、AS/400 アプリケーション・リクエスターは、分散データベース・ネットワークで通信を確立するのに必要なネットワーク情報を渡すことができます。

分散データベース環境の処理の大部分では、ネットワーク内の他の場所との間でメッセージを交換することが必要です。SNA 環境でこのプロセスが正しく実行されるようにするには、以下のことを実行しなければなりません。

- ローカル・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義
- リモート・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義
- 通信の DB2 ユニバーサル・データベース (AS/400 版) への定義

ローカル・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義

分散データベース・ネットワークのアプリケーション・リクエスターには、それぞれにローカル関係データベース用の関係データベース・ディレクトリー項目と、アプリケーション・リクエスターがアクセスする各リモート関係データベースの項目がなければなりません。分散データベース・ネットワークでアプリケーション・サーバーとしてのみ機能している AS/400 システムは、それぞれにローカル関係データベース用の関係データベース・ディレクトリー項目がなければなりません。関係データベース・ディレクトリーについての詳細は、AS/400 分散データベース・プログラミング を参照してください。

ローカル・システムを定義するには、リモート・ロケーション名 *LOCAL を関係データベース・ディレクトリーに追加することにより、ローカル・データベースに命名します。これを行うには、関係データベース・ディレクトリー項目の追加 (ADDRDBDIRE) コマンドを使用します。次に、ADDRDBDIRE コマンドの例を示します。ここで、アプリケーション・リクエスターの名前は ROCHESTERDB とします。

```
ADDRDBDIRE RDB(ROCHESTERDB) RMTLOCNAME(*LOCAL)
```

関係データベース・ディレクトリー・コマンドについての詳細は、AS/400 分散データベース・プログラミング を参照してください。

注: 最新バージョンの OS/400 では、ローカル RDB 名項目が必要なときにまだ作成されていない場合は、自動的に作成されます。ネットワーク属性でのシステム名が、ローカル RDB 名として使用されます。

リモート・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義

分散 DB ネットワーク内の各アプリケーション・サーバーの RDB ディレクトリー内には、ローカル項目がなければなりません。加えて、各リモート・データベースの項目が各アプリケーション・リクエスターの RDB ディレクトリーになければなりません。これらの項目を作成するには、以下のようにします。

- ADDRDBDIRE または WRKRDBDIRE コマンドを使用して、関係データベース・ディレクトリーに各リモート・データベースの項目を追加し、リモート・データベースをローカル・データベースに定義する。SNA 接続用に指定する情報には以下のものが含まれます。
 - リモート・データベース名
 - データベースのリモート・ロケーション名
 - ローカル・ロケーション名

- 通信を確立するために使用されるモード名
- リモート・ネットワーク識別子
- 通信に使用される装置の名前
- リモート・データベースのトランザクション・プログラム名

ほとんどの場合、必要な情報はリモート・データベース名およびリモート・ロケーション名だけです。⁴ リモート・ロケーション名だけが指定されていると、残りのパラメーターには省略時値が使用されます。システムは、リモート・ロケーション名を使用して装置の記述を選択します。

複数の装置記述に同一のリモート・ロケーション名が含まれていて、特定の装置記述が必要な場合、関係データベース・ディレクトリー項目のローカル・ロケーション名およびリモート・ネットワーク識別子の値が、装置記述の値と適合していなければなりません。複数の装置記述に同一のリモート・ロケーション名が使用されると、装置記述の選択が困難になることがあります。混乱を防ぐためには、各装置説明で固有のリモート・ロケーション名を使用してください。リモート・データベースのトランザクション・プログラム名の省略時値は、DRDA の省略時値のトランザクション・プログラム名 'X'07F6C4C2' になります。

関係データベース・ディレクトリー内の通信情報は、リモート・システムとの会話を確立するために使用されます。

TCP/IP 接続 (DB2 ユニバーサル・データベース (AS/400 版) バージョン 4.2 でサポートされている場合) には、リモート・データベース名および関連する IP アドレスだけがが必要です。119ページの『第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』を参照してください。

SNA 通信の定義

この節では、拡張対等通信ネットワーク機能 (APPN) を使用した、AS/400 システムでの通信の構成を説明します。また、AS/400 システムは、拡張プログラム間通信 (APPC) 構成を許可します。これは、ネットワーク経路指定サポートを提供しません。AS/400 分散データベースは、どちらの構成でも機能します。APPC 構成の詳細については、OS/400 通信構成 を参照してください。

4. OS/400 の「ロケーション名」は、VTAM の「LU 名」と同義です。「リモート・ロケーション名」とは、「パートナーまたはリモート LU 名」のことです。

AS/400 での AnyNet サポートの使用により、APPC アプリケーションは伝送制御プロトコル / インターネット・プロトコル (TCP/IP) ネットワークでの実行ができるようになります。以下の節の例には、DDM、システム・ネットワーク体系 (SNA) 配布サービス、アラート、および 5250 表示ステーション・パススルーが含まれています。これらのアプリケーションは、DRDA と一緒に使用すれば、いくらかの構成を追加するだけで、変更なく TCP/IP ネットワークで実行できます。AnyNet サポートを指定するには、CRTCTLAPPC コマンドの LINKTYPE パラメーターに *ANYNW を指定します。

TCP/IP の APPC についての詳細は、OS/400 通信構成 および OS/400 TCP/IP 構成および解説書を参照してください。(DB2 ユニバーサル・データベース (AS/400 版) バージョン 4.2 では、DRDA 通信用のネイティブ TCP/IP サポートが備わっています。119ページの『第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』を参照してください)

APPN は、ネットワーク・サポートを提供します。これにより AS/400 システムは、従来メインフレームにより提供されていたネットワーク・サポートを必要とせずにシステムのネットワークに参加および制御できます。AS/400 システムの APPN サポートを構成するには、以下のステップを実行します。

1. ネットワーク属性の変更 (CHGNETA) コマンドを使用してネットワーク属性を定義する。

ネットワーク属性には以下のものが含まれています。

- ローカル・システム名
- APPN ネットワークでのシステムの名前
- ローカル・ネットワーク識別子
- ネットワーク・ノード・タイプ
- マシンがエンド・ノードの場合、AS/400 システムが使用するネットワーク・サーバーの名前
- AS/400 がエンド・ノードの場合、ネットワーク制御ポイント

2. 回線記述を作成する。

回線記述は、AS/400 システムとネットワークとの間で使用される物理回線接続およびデータ・リンク・プロトコルについて記述します。以下のコマンドを使用して回線記述を作成してください。

- 回線記述の作成 (Ethernet) (CRTLINETH)
- 回線記述の作成 (SDLC) (CRTLINS DLC)
- 回線記述の作成 (トークンリング) (CRTLINTRN)

- 回線記述の作成 (X.25) (CRTLINX25)

3. 制御装置の記述を作成する。

制御装置の記述は、ネットワークでの隣接システムを記述します。制御装置の記述を作成するときには、APPN(*YES) を指定して、APPN サポートを使用することを指示してください。以下のコマンドを使用して制御装置の記述を作成してください。

- 制御装置の記述の作成 (APPC) (CRTCTLAPPC)
- 制御装置の記述の作成 (SNA HOST) (CRTCTLHOST)

トークンリングまたは Ethernet 回線の記述の AUTOCTRL パラメーターが *YES に設定されている場合には、システムがトークンリングまたは Ethernet 回線でセッション開始要求を受信するときに、制御装置の記述が自動的に作成されます。

4. サービス・クラスの記述を作成する。

サービス・クラスの記述を使用して、通信経路 (伝送グループ) を選択し、伝送の優先順位を決めます。システムにより 5 つのサービス・クラスの記述が提供されます。

#CONNECT

省略時サービス・クラス。

#BATCH

バッチ・ジョブ用のサービス・クラス。

#BATCHSC

#BATCH と同じですが、少なくともパケット交換ネットワークのデータ・リンク機密保護が必要です。パケット交換ネットワークでは、ネットワークでデータが常に同じパスに従うとは限りません。

#INTER

対話式通信用に調整済みのサービス・クラス。

#INTERSC

#INTER と同じですが、少なくともパケット交換ネットワークのデータ・リンク機密保護が必要です。

サービス・クラスの作成 (CRTCOSD) コマンドを使用して、他のサービス・クラスの記述を作成します。

5. モード記述を作成する。

モード記述では、セッションの特性や、ローカル・セッションとリモート・セッションとの間で許可される値を折衝するために使用されるセッションの

数が示されます。モード記述は、会話に使用されるサービス・クラスも指し示します。いくつかの定義済みモードがシステムに付属しています。

BLANK

システムが出荷されるときにネットワーク属性で指定される省略時モード名。

#BATCH

バッチ・ジョブ用に調整済みのモード。

#BATCHSC

#BATCH と同じ。関連するサービス・クラスの記述に、少なくとも 1 つの packets 交換ネットワークのデータ・リンク機密保護が必要な点だけが異なる。

#INTER

対話式通信用に調整済みのモード。

#INTERSC

#INTER と同じ。関連するサービス・クラスの記述に、少なくとも 1 つの packets 交換ネットワークのデータ・リンク機密保護が必要な点だけが異なる。

IBMRDB

DRDA 通信用に調整済みのモード。

モード記述の作成 (CRTMODD) コマンドを使用して、他のモード記述も作成できます。

6. 装置記述を作成する。

装置記述では、ローカル・システムとリモート・システムとの間の論理接続の特性が提供されます。AS/400 システムが APPN を使用するホスト・システムに対して、独立論理単位 (LU) として稼働している場合には、手操作で装置記述を作成する必要はありません。AS/400 システムは装置記述を自動的に作成し、セッションが確立されるときに適切な制御装置の記述に結び付けます。AS/400 システムが従属 LU の場合には、装置記述の作成 (CRTDEVAPPC) コマンドを使用して、装置記述を手操作で作成しなければなりません。装置記述では、APPN が使用されていることを示すために APPN(*YES) を指定してください。

7. APPN ロケーション・リストを作成する。

追加のローカル・ロケーション (他のシステムでは LU と呼ばれる) または APPN にリモート・ロケーションの特殊な特性が必要な場合には、APPN ロケーション・リストを作成しなければなりません。ローカル・ロケーション名は、ネットワーク属性で指定される制御ポイント名です。AS/400 シス

テムに追加のロケーションが必要な場合には、APPN ローカル・ロケーション・リストが必要です。リモート・ロケーションの特殊な特性の例は、ローカル・ロケーションのあるネットワークとは別のネットワークにリモート・ロケーションがある場合です。この状況の場合には、APPN リモート・ロケーション・リストが必要です。構成リストの作成 (CRTCFGL) コマンドを使用して APPN ロケーション・リストを作成してください。

8. 通信を活動化 (有効化) する。

構成の変更 (VRYCFG) コマンドまたは構成状況での作業 (WRKCFGSTS) コマンドを使用して、通信記述を活動化できます。回線記述が活動化すると、その回線に接続する適切な制御装置およびデバイスも活動化します。各接続の状況を表示するには、WRKCFGSTS コマンドも利用できます。

9. RU サイズおよび歩調合わせ

RU サイズおよび歩調合わせは、モード記述で指定されている値により制御されます。モード記述を作成するとき、RU サイズと歩調合わせの両方に省略時値が提供されます。省略時値は、分散データベースを含むほとんどの環境の AS/400 見積値です。省略時値が RU サイズで採用されると、AS/400 システムは最善の値を使用するように見積もります。AS/400 システムが適応歩調合わせをサポートしている他のシステムと通信している場合には、指定される歩調合わせ値は始点のみです。歩調合わせは、送信されるデータを処理するシステムの能力に従って、それぞれのシステムで調整されます。適応歩調合わせをサポートしないシステムでは、歩調合わせ値はセッション開始に折衝され、セッションの途中には変化しません。詳細については、OS/400 通信構成 を参照してください。

注:

1. 制御装置記述は、IBM ネットワーク制御プログラムおよび仮想記憶通信アクセス方式 (NCP/VTAM) の物理装置 (PU) マクロと同等です。
2. 装置記述は、NCP/VTAM の論理装置 (LU) マクロと同等です。装置記述には、コミュニケーション・マネージャー/2 1.1 パートナー LU プロファイルに保管されている情報に類似した情報が含まれています。
3. モード記述は、NCP/VTAM のモード表およびコミュニケーション・マネージャー伝送サービスのモード・プロファイルと同等です。

ネットワーク・サポートの構成およびロケーション・リストを使用した作業についての詳細は、OS/400 通信構成 および APPN サポート を参照してください。システム構成を定義するための CL コマンドの使用についての例は、AS/400 分散データベース・プログラミング を参照してください。

機密保護の提供

リモート・システムが SQL アプリケーションに代わって分散データベース処理を実行する場合には、アプリケーション・リクエスター、アプリケーション・サーバー、およびそれらに接続しているネットワークの機密保護要件を満たさなければなりません。これらの要件は、以下のカテゴリの 1 つかそれ以上を含みます。

- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- AS/400 機密保護により強制される機密保護

エンド・ユーザー名の選択

AS/400 システムでは、エンド・ユーザーはシステムに固有な 1~10 文字のユーザー ID として割り当てられますが、ネットワークで固有である必要はありません。このユーザー ID は、接続が 2 つのデータベース間に確立されているときにリモート・システムに渡される ID です。ネットワーク内のシステムのユーザー ID 間の対立を避けるために、ネットワークに送信する前に衝突を解決するように、アウトバウンド名変換を使用してユーザー ID を変更します。しかし、サーバーでの潜在的な対立を解決するために、AS/400 システムがアウトバウンド名変換を提供することはありません。これらの対立は、AS/400 SQL CONNECT ステートメントに USER 文節および USING 文節を追加して使用する場合を除き、アプリケーション・サーバーで解決されなければなりません。USER は、アプリケーション・サーバーの有効な ID であり、USING はユーザーに対応するパスワードです。

ネットワーク機密保護

アプリケーション・リクエスターがリモート・アプリケーションを示すエンド・ユーザー名を選択した後は、必要な LU 6.2 ネットワーク機密保護情報を提供しなければなりません。LU 6.2 は、主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護。これは CRTDEVAPPC コマンドで LOCPWD キーワードにより制御されます。
- 会話レベル機密保護。これは OS/400 オペレーティング・システムにより制御されます。
- 暗号化。これは OS/400 オペレーティング・システムではサポートされていません。

セッション・レベル機密保護が、LU 間検査を介して提供されます。各 LU には、リモート LU のキーに適合するキーがあります。キーは、CRTDEVAPPC コマンドの LOCPWD キーワードで指定します。

アプリケーション・サーバーの責任でデータベース資源を管理するため、アプリケーション・サーバーは、どのネットワーク機密保護にアプリケーション・リクエスターが必要かを指示します。AS/400 機密保護管理者は、それぞれのアプリケーション・サーバーの機密保護要件を確認して、AS/400 アプリケーション・リクエスター・サポート以外には何も必要でないようにしなければなりません。

以下に示すのは、指定できる SNA 会話機密保護オプションです。

SECURITY=SAME

検査済み機密保護として知られているものです。アプリケーション・ユーザーのユーザー ID のみ、リモート・システムに送信されます。パスワードは送信されません。AS/400 バージョン 2 リリース 2 モディフィケーション 0 以前のバージョンでは、このレベルの会話機密保護のみ、AS/400 アプリケーション・リクエスターによりサポートされていました。

SECURITY=PGM

アプリケーション・ユーザーのユーザー ID とパスワードの両方も、妥当性検査のためにリモート・システムに送信されます。AS/400 バージョン 2 リリース 2 モディフィケーション 0 以前のバージョンでは、AS/400 アプリケーション・リクエスターはこの機密保護オプションをサポートしていませんでした。

SECURITY=NONE

AS/400 がアプリケーション・リクエスターの場合には、サポートされません。

データベース・マネージャー機密保護

AS/400 システムには、外部機密保護サブシステムがありません。すべての機密保護は、OS/400 オペレーティング・システムにより制御されています。これは次の節、『システム機密保護』で説明されています。

システム機密保護

プログラム、パッケージ、表、視点、および集合を含むシステム上のすべてのオブジェクトの認可は、OS/400 オペレーティング・システムが制御します。

アプリケーション・リクエスターはアプリケーション・リクエスターにあるオブジェクトへの許可を制御します。アプリケーション・サーバーでのオブジェ

クトの機密保護は、アプリケーション・リクエスターから送信されるユーザー ID に基づいて、アプリケーション・サーバーで制御されます。アプリケーション・サーバーに送信されるユーザー ID は、AS/400 アプリケーション・リクエスターのユーザーまたは AS/400 SQL CONNECT ステートメントの USER 文節で与えられるユーザー ID と関連しています。たとえば、CONNECT TO rdbname USER userid USING password になります。

オブジェクトの機密保護は、オブジェクト権限 CL コマンドを使用するか、SQL ステートメント GRANT および REVOKE を使用して管理できます。オブジェクト CL 権限コマンドには、オブジェクト権限の認可 (GRTOBJAUT) と、オブジェクト権限の取消 (RVKOBJAUT) が含まれています。これらのコマンドは、システムにあるどのオブジェクトにも実行できます。ステートメント GRANT および REVOKE は、SQL オブジェクト、つまり表、視点、およびパッケージでのみ有効です。その他のオブジェクト (プログラムや集合など) の許可を変更する必要がある場合には、GRTOBJAUT および RVKOBJAUT コマンドを使用してください。

権限の許可と取り消し: プログラム PGMA でユーザー USER1 に *USE 権限を認可するには、AS/400 システムで以下のコマンドを入力します。

```
GRTOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

この権限を取り消すには、以下のようにします。

```
RVKOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

*PGM は、この例ではオブジェクト・タイプを識別します。*SQLPKG はパッケージでの操作に、*LIB は集合に、そして *FILE は表に使用されます。

GRTOBJAUT および RVKOBJAUT は、ユーザーがプログラムやパッケージを作成しないようにするためにも使用されます。プログラムを作成するために使用される CRTSQLxxx コマンド (ここで、xxx = RPG、C、CBL、FTN、または PLI) から権限が取り消されると、ユーザーはプログラムを作成できません。権限が CRTSQLPKG コマンドに取り消される場合には、ユーザーはアプリケーション・リクエスターから、またはアプリケーション・サーバーでパッケージを作成できません。

たとえば、AS/400 システムに以下のコマンドを入力して、CRTSQLPKG コマンドについてユーザー USER 1 に *USE 権限を認可します。

```
GRTOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```


これは、アプリケーション・リクエスターでの `crtsqlpkg` の実行に影響を与えます。アプリケーション・サーバーでは、このコマンドを使用するとパッケージを作成できます。

この権限を取り消すには、以下のようにします。

```
RVKOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```

省略時許可の適用: オブジェクトが作成されると、省略時許可が与えられます。省略時には、表、視点、またはプログラムの作成者にはそれらのオブジェクトに対するすべての権限が与えられます。省略時に、それらのオブジェクトが入るライブラリーまたは集合に対する権限をパブリックが持っている場合、作成者がオブジェクトに対して持つのと同じ権限がパブリックにも与えられません。

システム機密保護についての詳細は、*AS/400 機密保護 解説書* を参照してください。

データの表示

DRDA をサポートしている製品は、受信しているシステムでなんらかの変換が必要な場合に、これを自動的に実行します。これが実行されるには、アプリケーション・リクエスターの `CCSID` 値が、受信システムによる変換用にサポートされる値でなければなりません。

アプリケーション・リクエスターでは、以下のことに関連して `CCSID` を考慮しなければなりません。

- ジョブの要求

OS/400 作業管理サポートは、ジョブ `CCSID` を、ユーザー・プロファイルで指定した `CCSID` に初期設定します。ユーザー・プロファイル `CCSID` の値が `*SYSVAL` の場合、作業管理サポートは `QCCSID` システム値から `CCSID` を取得します。システム値 `QCCSID` は、最初に `CCSID 65535` に設定されます。DB2 ユニバーサル・データベースからの接続要求を処理するジョブの `CCSID` に `65535` を設定した場合、その接続要求は失敗します。システム値 `QCCSID` を変更するとシステム全体が影響を受けるため、そのサーバー・ジョブが処理されているジョブ用のユーザー・プロファイルの `CCSID` を変更することをお勧めします。そのジョブ用のユーザー・プロファイルの `CCSID` を適切な値に設定してください。たとえば、US English の場合 `CCSID` は `37` に設定します。たいていの場合、接続先の AS/400 用の省略時のコード化文字セット識別子を使用するのが適切です。

ジョブ `CCSID` は、ジョブの変更 (`CHGJOB`) コマンドを使用して変更できます。また、後続のジョブについては、ユーザー・プロファイルの `CCSID` 値

を変更するには、ユーザー・プロファイルの変更 (CHGUSRPRF) コマンドを使用してください。ジョブについて有効になっている CCSID を参照するには、CL プログラムでは、ジョブ属性の検索 (RTVJOBA) コマンドを使用して現行ジョブ CCSID を取得してください。対話式には、ジョブの処理 (WRKJOB) コマンドを使用して、ジョブでの作業の画面で、オプション 2 「ジョブ定義属性の表示」を選択します。

- データベース物理ファイル

物理ファイルの作成 (CRTPF) またはソース物理ファイルの作成 (CRTSRCPF) コマンドに CCSID が明示的に指定されていない場合には、データベース物理ファイルは、ファイル作成時にジョブ CCSID を省略時値にとります。この省略時値はジョブ CCSID とは異なる場合があります。DB2 (AS/400 版) の V3R1 以前のものでは、この省略時値はジョブ CCSID でした。しかしジョブ CCSID の値は 65535 の場合が多かったため、DRDA を使用するには不適切でした。それ以降のバージョンではジョブ CCSID が 65535 に設定されることはありません。そのため、DRDA を経由した物理ファイルの CCSID としてより適切になりました。

ファイルの CCSID を表示するにはファイル記述の表示 (DSPFD) コマンドを、またファイルのフィールドの CCSID を表示するにはファイル・フィールド記述の表示 (DSPFFD) コマンドを使用できます。

物理ファイルの CCSID を変更するには、物理ファイルの変更 (CHGPF) コマンドを使用します。以下のいずれかの状況が存在する場合には、物理ファイルは常に変更できるとは限りません。

- 物理ファイル上に論理ファイルが定義されている場合。この場合は、以下の作業を行う必要があります。
 1. 論理ファイルおよび物理ファイルをアクセス・パスとともに保管する。
 2. 論理ファイルの権限のリストを印刷する (DSPOBJAUT)。
 3. 論理ファイルを削除する。
 4. 物理ファイルを変更する。
 5. 物理ファイル、論理ファイル、および変更された物理ファイルのアクセス・パスを復元する。
 6. 論理ファイルに私用権限を認可する (印刷したリストを参照)。
- ファイルまたはフィールドに、明示的に CCSID 値が割り当てられている場合。フィールド・レベルで割り当てられた CCSID を持つ物理ファイルを変更するには、物理ファイルを再作成し、ファイルの複写 (CPYF) コマンドで FMTOPT(*MAP) パラメーターを使用して新しいファイルにデータをコピーします。

- レコード形式はバージョン 3 リリース 1 よりも前の OS/400 のバージョンと共用です。

アプリケーション・サーバーのセットアップ

AS/400 システムでのアプリケーション・サーバー・サポートは、DRDA アプリケーション・リクエスターのサーバーとして機能することができます。DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバーに接続できるアプリケーション・リクエスターは、DRDA プロトコルをサポートする任意のクライアントです。

アプリケーション・リクエスターは、DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバーにローカルで保管された表にアクセスすることが許されています。アプリケーション・リクエスターは、SQL が実行できるようになる前に、DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバーでパッケージを作成しなければなりません。DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバーは、プログラム実行時にアプリケーションの SQL ステートメントを含むパッケージを使用します。

ネットワーク情報の提供

AS/400 アプリケーション・サーバーで分散データベース要求を処理する場合、RDB ディレクトリーでアプリケーション・サーバー・データベースに名前を付ける必要があります。SNA 通信では、アプリケーション・サーバー・システムを定義し、要求単位および応答単位のサイズと歩調合わせを設定します。DB2 ユニバーサル・データベース (AS/400 版) バージョン 4.2 でサポートされる TCP/IP 通信については、119ページの『第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』を参照してください。

アプリケーション・サーバー・データベースに命名する

アプリケーション・サーバー・データベース (アプリケーション・サーバー・ロケーションにある) は、アプリケーション・リクエスター・データベース (アプリケーション・リクエスター・ロケーションにある) を識別するのと同じ方法で名前を付けます。関係データベース・ディレクトリー項目の追加 (ADDRDBDIRE) コマンドを使用して、リモート・ロケーションとして *LOCAL を指定します。

アプリケーション・サーバーのネットワークへの定義

SNA を使用してアクセスする場合、アプリケーション・サーバーをネットワークに定義する方法は、アプリケーション・リクエスターをネットワークに定義する方法と同じです。アプリケーション・サーバーと、要求を送信するアプリケーション・リクエスターの両方を定義するには、回線、制御装置、デバイス、およびモードの記述を作成しなければなりません。ネットワークにアプリケーション・サーバーを定義する方法についての詳細は、101ページの『ローカル・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義』および 101ページの『リモート・システムの DB2 ユニバーサル・データベース (AS/400 版) への定義』を参照してください。AS/400 分散データベース・プログラミング も参照してください。

AS/400 アプリケーション・サーバー・データベースを開始するために使用されるトランザクション・プログラム名は、DRDA 省略時値 X'07F6C4C2' です。このトランザクション・プログラム名は、アプリケーション・サーバーを開始するために AS/400 システムで定義されます。TCP/IP で対応するパラメーターは、DB2/400 がそのプロトコルをサポートしている場合、ポートになります。DB2/400 は、サーバーとして通常 446 のウェルノウン・ポートを使用します。

RU サイズおよび歩調合わせの設定

分散データベース・ネットワークが既存のネットワークに影響を与えるかどうかを判断するためには、ネットワーク定義を再検討しなければなりません。これらの考慮事項は、アプリケーション・サーバーと、アプリケーション・リクエスターとは同一です。

機密保護の提供

アプリケーション・リクエスターが分散データベース要求を AS/400 アプリケーション・サーバーに向けるときには、以下の機密保護上の考慮事項が関係します。

- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- AS/400 機密保護

エンド・ユーザー名の選択

アプリケーション・リクエスターは、機密保護処理のためにユーザー ID をアプリケーション・サーバーに送信します。AS/400 アプリケーション・サーバ

ーで処理されているジョブは、このユーザー ID、またはいくつかのインスタンスでは省略時のユーザー ID を使用します。

固有でないユーザー ID またはシングル・ユーザー ID の下のグループ複数ユーザーの対立を解決するために、AS/400 アプリケーション・サーバーがインバウンド・ユーザー ID 変換を提供することはありません。アプリケーション・リクエスターから送信される各ユーザー ID は、アプリケーション・サーバー上に存在していなければなりません。機密保護をいくらか犠牲にしても着信要求を単一ユーザー ID にグループ化するには、リモート・ジョブ開始要求を制御しているサブシステムの通信項目に省略時ユーザー ID を指定します。AS/400e シリーズ CL 解説書にある ADDCMNE と CHGCMNE の説明を参照してください。

SNA ネットワーク機密保護

LU 6.2 は、主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護
- 会話レベル機密保護
- 暗号化 (AS/400 システムではサポートされていません)

DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバーは、DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・リクエスターとまったく同じ方法でセッション・レベル機密保護を使用します。

アプリケーション・サーバーは、会話に使用される SNA 会話レベルを制御します。APPC 装置記述の SECURELOC パラメーターまたは APPN リモート・ロケーション・リストの安全ロケーション値によって、会話にアプリケーション・リクエスターから何が受け入れられるかを判別します。

SNA 会話機密保護オプションは以下のとおりです。

SECURITY=SAME

検査済み機密保護として知られているものです。アプリケーション・ユーザーのユーザー ID だけがアプリケーション・サーバーに必要です。パスワードは送信されません。アプリケーション・サーバーでこのレベルの会話機密保護を使用するには、APPC 装置記述で SECURELOC パラメーターを *YES に設定するか、APPN リモート・ロケーション・リストの安全ロケーション値を *YES に設定します。

SECURITY=PGM

妥当性検査に、ユーザー ID とパスワードの両方がアプリケーション・サーバーに必須であるとして設定します。このレベルの会話機密保

護をアプリケーション・サーバーで使用するには、AS/400 サブシステム通信項目の省略時ユーザー ID を *NONE (省略時ユーザー ID なし) に設定し、SECURELOC パラメーターまたは安全ロケーション値を *NO に設定します。

SECURITY=NONE

アプリケーション・サーバーはユーザー ID もパスワードも必要としません。アプリケーション・サーバーの省略時ユーザー・プロファイルを使用して会話できます。このオプションを使用するには、サブシステム通信ディレクトリーで省略時ユーザー・プロファイルを指定し、SECURELOC パラメーターまたは安全ロケーションに *NO を指定します。

SNA/DS (SNA 配布サービス) には省略時ユーザー ID が必要です。そのため DRDA アプリケーション用の省略時ユーザー ID が必要ない場合のために、SNA/DS にはサブシステムがなければなりません。

着信開始ジョブ要求をグループ化して単一のユーザー ID にする方法については、113ページの『エンド・ユーザー名の選択』に説明されています。この方法では、アプリケーション・リクエスターから送信されたユーザー ID は検査されません。アプリケーション・サーバー・ジョブは省略時ユーザー ID で開始され、アプリケーション・サーバーから接続を開始したユーザーは、送信されたユーザー ID の許可が制限されている場合でも、アプリケーション・サーバーにアクセスを持ちます。これを実現するには、アプリケーション・サーバーを無保護ロケーションとして定義し、AS/400 サブシステムの通信項目に省略時ユーザー ID を指定し、そして、接続処理のときにのみユーザー ID を送信するようにアプリケーション・リクエスターを構成します。パスワードが送信されると、これに伴うユーザー ID が省略時ユーザー ID の代わりに使用されます。

AS/400 サブシステムの通信項目は、会話を開始するために使用された装置およびモード名によりそれぞれ区別されます。異なる省略時ユーザー ID を異なる装置 / モードの組に割り当てると、アプリケーション・サーバーと通信する方法によってユーザーがグループ化されます。

AS/400 システムは、分散データベースおよび分散ファイル管理にのみ使用できるネットワーク機密保護機能も提供しています。このタイプのシステム・アクセス用のネットワーク属性は、アクセスのすべての試行を拒否するか、個々のオブジェクトに基づいてシステムが機密保護を制御することを許可するかのどちらかになります。

TCP/IP ネットワーク機密保護

DB2 ユニバーサル・データベース (AS/400 版) バージョン 4.2 では、新しい CRTDDMTCPA というコマンドが提供されます。これを使用することにより、サーバーが TCP/IP 接続要求をパスワードなしで受け入れるかどうかを指定できるようになります。

データベース・マネージャー機密保護

機密保護はすべて、OS/400 機密保護機能により制御されます。

システム機密保護

AS/400 システムには、外部機密保護サブシステムがありません。すべての機密保護は、オペレーティング・システムの重要な部分である OS/400 機密保護機能により制御されます。プログラム、パッケージ、表、視点、および集合を含むシステムのすべてのオブジェクトの認可は、オペレーティング・システムが制御します。

アプリケーション・サーバーは、アプリケーション・サーバーにあるオブジェクトの認可を制御します。これらのオブジェクトの機密保護制御は、アプリケーション・サーバー・ジョブを開始するユーザー ID により異なります。このユーザー ID は、113ページの『エンド・ユーザー名の選択』で解説されているように判別されます。

オブジェクトの機密保護は、オブジェクト権限 CL コマンドを使用するか、SQL ステートメント GRANT および REVOKE を使用して管理できます。オブジェクト権限 CL コマンドには、オブジェクト権限の付与 (GRTOBJAUT) およびオブジェクト権限の取り消し (RVKOBJAUT) が含まれています。システムのどのオブジェクトにもこれらの CL コマンドを使用できます。SQL オブジェクト (表、視点、およびパッケージ) にのみ、ステートメント GRANT および REVOKE を使用してください。他のオブジェクト (プログラムや集合など) の許可を変更する必要がある場合には、GRTOBJAUT および RVKOBJAUT コマンドを使用してください。

オブジェクトがシステム上に作成されると、省略時の許可が与えられます。表、視点、およびパッケージを作成するユーザー ID には、すべての権限が与えられます。他のすべてのユーザー ID (パブリック) には、オブジェクトが作成された集合またはライブラリーに対して同一の権限が与えられます。

パッケージ内で静的または動的ステートメントにより参照されるオブジェクトへの権限は、パッケージ実行時に検査されます。パッケージの作成者に、参照されるオブジェクトへの権限がない場合には、パッケージが作成されるときに警告メッセージが戻されます。実行時には、パッケージを実行しているユーザ

ーがパッケージの作成者としての許可を受けます。パッケージの作成者に表を使用する許可があり、パッケージを実行しているユーザーに許可がない場合、ユーザーはパッケージ作成者の権限を受けて、表を使用できます。

システム機密保護についての詳細は、*AS/400 機密保護 解説書* を参照してください。

データの表示

DRDA をサポートしている製品は、アプリケーション・サーバーでなんらかの変換が必要な場合に、これを自動的に実行します。これが実行されるには、アプリケーション・サーバーの CCSID 値が、アプリケーション・リクエスターによる変換用にサポートされる値でなければなりません。

アプリケーション・サーバーでは、以下に関連して CCSID を考慮しなければなりません。

- 通信サブシステムでのサービス・ジョブ

ご使用のジョブの CCSID はアプリケーション・リクエスターと互換性がなければなりません。この CCSID は、接続を要求するユーザー ID のユーザー・プロファイルにより確立されます。OS/400 作業管理サポートは、ジョブ CCSID を、ユーザー・プロファイルの CCSID に初期設定します。ユーザー・プロファイルに CCSID が存在しない場合には、作業管理サポートはシステム値から CCSID (QCCSID) を取り出します。システム値 QCCSID は、最初に CCSID 65535 に設定されます。

DB2 ユニバーサル・データベース (AS/400 版) への要求を開始する前に、サインオンしてユーザー・プロファイルの変更 (CHGUSRPRF) を使用することにより、DRDA 要求を処理するジョブのユーザー・プロファイルに受け入れ可能な CCSID 値を割り当てる必要があります。

- SQL 集合

SQL 集合は、OS/400 ライブラリー・オブジェクト、ジャーナル、ジャーナル・レシーバーで構成されています。さらに、WITH DATA DICTIONARY 文節が CREATE COLLECTION ステートメントに指定された場合には、任意選択で IDDU データ・ディクショナリーも含まれます。これらのオブジェクトの一部に使用される物理および論理ファイルは、作成時にジョブ CCSID を省略時値として使用します。これらのファイルの CCSID 値をサポートしていないアプリケーション・リクエスターからデータ・ディクショナリーまたはカタログを照会すると、表示不能のデータまたは間違っただけのデータが表示されることがあります。あるいは、アプリケーション・リクエスターは CCSID 値がサポートされていないことを示すメッセージを出します。これを

訂正するには、他のシステムで受け入れられるジョブ CCSID 値を使用して新しい SQL 集合を作成しなければなりません。

ジョブ CCSID は、ジョブの変更 (CHGJOB) コマンドを使用して変更できます。また、後続のジョブについては、ユーザー・プロファイルの CCSID 値を変更するには、ユーザー・プロファイルの変更 (CHGUSRPRF) コマンドを使用してください。CL プログラムでは、ジョブ属性の検索 (RTVJOBA) コマンドを使用して現行ジョブ CCSID を取得してください。対話式には、ジョブの処理 (WRKJOB) コマンドを使用して、ジョブでの作業の画面で、オプション 2「ジョブ定義属性の表示」を選択します。

- DRDA を介してアクセスされる SQL 表とその他の DB2 ユニバーサル・データベース (AS/400 版) ファイル

SQL 表は、集合と同じ名前を持つライブラリー内にある DB2 ユニバーサル・データベース (AS/400 版) 物理ファイルに対応します。また、表の列は、物理ファイルのフィールド定義に対応します。表または列の CCSID 値は、アプリケーション・リクエスターと互換性がありません。この値を変更する方法については、110ページの『データの表示』を参照してください。ここでは、データベース物理ファイルの変更について説明されています。バージョン 3 リリース 1 以前の OS/400 のバージョンの CCSID に互換性がない主な原因は、多くのファイルまたは SQL 表に省略時解釈で CCSID 65535 のタグが付いていたことにあります。バージョン 3 リリース 1 以降のリリースでは、これらのファイルの CCSID は自動的に他の適切な値に変更されます。

第4章 TCP/IP を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続

この章では、AS/400 の設定方法を説明した *AS/400 分散データベース・プログラミング* に含まれている情報をまとめています。

- アウトバウンド TCP/IP 通信を使用した DRDA アプリケーション・リクエスターとして
- インバウンド TCP/IP 通信を使用した DRDA アプリケーション・サーバーとして

ここでの指針は、99ページの『第3章 SNA を使用した DRDA ネットワークでの DB2 ユニバーサル・データベース (AS/400 版) の接続』に示されている指針と同じですが、通信構成のステップはずっと簡単です。

注:

1. TCP/IP を使用した DRDA 通信の場合、データベース接続の省略時のポート番号は 446 です。
2. DB2 ユニバーサル・データベース (AS/400 版) バージョン 4 リリース 2 のインプリメンテーションでは、TCP/IP 通信を介した 2 フェーズ・コミット (分散作業単位) はサポートされていません。

DB2 ユニバーサル・データベース (AS/400 版) 情報のまとめ

AS/400 分散データベース・プログラミング の中の以下の節を読んで参照してください。

- 第 1 章. 分散リレーショナル・データベースと AS/400 システム
 - 分散リレーショナル・データベース処理
 - DRDA および CDRA サポート
- 第 3 章. AS/400 分散リレーショナル・データベースのための通信
 - TCP/IP 用の通信ネットワークの構成
- 第 4 章. AS/400 分散リレーショナル・データベースの機密保護
 - TCP/IP を使用した DRDA 機密保護
- 第 5 章. AS/400 分散リレーショナル・データベースのセットアップ
 - DRDA 用の実行管理機能の TCP/IP での使用
 - DRDA 用の TCP/IP サーバーのセットアップ

- 第 6 章. 分散リレーショナル・データベースの管理および操作の作業
 - TCP/IP サーバーの管理
- 第 8 章. 分散リレーショナル・データベースのパフォーマンス
 - DRDA のブロック化に影響を与える要因
- 第 9 章. 分散リレーショナル・データベースの問題の処理
 - TCP/IP の接続要求障害の処理
 - TCP/IP サーバー用のサービス・ジョブの開始
- 付録 B. DRDA を使用したプラットフォーム間アクセス

さらに、以下の点も知っておく必要があります。

- サーバーとリクエスターの TCP/IP ポート番号およびホスト名の情報。
- サーバーとリクエスターの CCSID およびコード・ページの情報。
- データベースに接続する際に必要なユーザー ID とパスワード情報。

DB2 ユニバーサル・データベース (AS/400 版) DRDA TCP/IP サーバーの設定上および使用上の考慮事項

DB2 ユニバーサル・データベース (AS/400 版) DRDA TCP/IP サーバーを設定する上での主な考慮事項は、サーバーが起動したことを確認することです。DRDA サーバー (DDM サーバーともいう) を起動するときの CL コマンドは、次のとおりです。

```
STRTCPSVR SERVER(*DDM)
```

DRDA サーバーを起動するには、TCP/IP サーバーの起動 (STRTCPSVR) コマンドを使用することもできます。この場合、パラメーターを指定しないか、SERVER パラメーターに *ALL を指定します。この CL コマンドを発行しておけば、TCP/IP を開始したときに DRDA サーバーは自動的に起動します。

```
CHGDDMTCPA AUTOSTART(*YES)
```

次の CL コマンドを発行することにより、サーバーが起動していることを確認できます。

```
WRKUSRJOB USER(QUSER) STATUS(*ACTIVE)
```

このコマンドを発行すると、ジョブのスクロール可能リストが表示されます。ページを下方向にスクロールしていくと、以下の情報を含む 2 行が見つかりません。

—	QRWTLSTN	QUSER	BATCH	ACTIVE
—	QRWTSRVR	QUSER	PJ	ACTIVE

(アクティブになっている事前開始サーバー・ジョブの数によっては、QRWTSRVR 行が繰り返し出てくともあります。)

QRWTLSTN 行が現われることは、DRDA と DDM の接続要求を listen するジョブがアクティブであることを意味します。このジョブは、接続要求が受信されたときに作業を QRWTSRVR ジョブ (複数可) ヘディスパッチします。

DRDA サーバーが起動したことを確認するための別の方法は、STRTCPSVR SERVER(*DDM) コマンドを発行して、'DDM TCP/IP server already active' メッセージを探すことです。

特定の接続に使用する事前開始ジョブの名前は、次のようにして DSPLOG コマンドを発行することにより見つけられます。

```
DSPLOG PERIOD(('15:55'))
```

ここで、指定した時刻は接続が行われた時刻よりも早くなっています。活動記録ログ項目のスクロール可能リストが表示されます。次のようにして、サーバー・ジョブの名前を含む項目を探してください。

```
DDM job 039554/QUSER/QRWTSRVR servicing user SRR on 03/30/98 at 15:57:38.
```

このジョブ名は、現在アクティブなジョブのジョブ・ログを見る際に役立ちます。さらに、問題判別のために現在アクティブなジョブ上でサービス・ジョブを開始する際、あるいは照会最適化プログラムのメッセージを表示する際にも役立ちます。上記の情報を使用して、サービス・ジョブを開始する際の CL コマンド例は、次のとおりです。

```
STRSRVJOB 039554/QUSER/QRWTSRVR
```

サービス・ジョブをデバッグ・モードにするには、次のようにして STRDBG コマンドを実行します。

```
STRDBG UPDPROD(*YES)
```

特定の状況では、DRDA サーバーはジョブをリサイクルしてジョブ・ログをクリアする前に、事前開始ジョブのジョブ・ログを保管します。これが行われるのは、深刻な障害が検出されたり、ジョブが (STRSRVJOB を使用して) 処理されている間に終了したりした場合です。

ジョブの終了後に、保管したジョブ・ログを見つけるには、次のコマンドを発行します。

```
WRKJOB userid/QPRTJOB
```

ここでユーザー ID は、接続を行ったときのユーザー ID (上記の例では SRR) の名前です。

これにより、ジョブを選択するときのジョブのリスト、あるいは 1 つのジョブのオプション・メニューが表示されます。オプション 4 の 'スプールされたファイルの処理 (Work with spooled files)' を選択して、保管したジョブ・ログを検索します。複数のファイルがスプールされている場合には、QPJOBLOG のファイル名のものが該当ファイルです。オプション 5 を選択すると、ジョブ・ログ・ファイルが表示されます。

デバッグしながらジョブを実行しているときに、サーバー・ジョブ・ログ内に表示される照会最適化プログラムのメッセージ・タイプの例として、次のものがあります。

```
CPI4329      Information 00      03/30/98  16:14:57  QQQIMPLE
              QSYS          3911      QSQOPEN   QSYS          09C4
Message . . . . : Arrival sequence access was used for file TBL2.
Cause . . . . . : Arrival sequence access was used to select
                  records from member TBL2 of file TBL2 in library SR. If file TBL2
                  in library SR is a logical file then member TBL2 of physical file
                  TBL2 in library SR is the actual file from which records are
                  being selected. A file name of *N for the file indicates it is a
                  temporary file. Recovery . . . . : The use of an access path may
                  improve the performance of the query if record selection is
                  specified. If an access path does not exist, you may want to
                  create one whose left-most key fields match fields in the record
                  selection. Matching more key fields in the access path with
                  fields in the record selection will result in improved
                  performance. Generally, to force the use of an existing access
                  path, specify order by fields that match the left-most key fields
                  of that access path. For more information refer to the DB2 for
                  AS/400 SQL Programming book.
```

DB2 ユニバーサル・データベース (AS/400 版) DRDA TCP/IP クライアントの設定上の考慮事項

DB2 ユニバーサル・データベース (AS/400 版)を、TCP/IP を介して DRDA アプリケーション・リクエスターとして使用する上での主な考慮事項は、次の節で説明される機密保護の考慮事項に加えて、リモート・アプリケーション・サーバーの RDB ディレクトリー項目を追加することです。これは、SNA 通信の使用に関して前の章で説明されたのと同様の方法で行われます。しかし、リモート LU 名およびトランザクション・プログラム名などの APPC パラメーターではなく、リモート・ホスト名か IP アドレス、そしてポート番号かサービス名という 2 つの TCP/IP パラメーターがあります。リモート・ロケーション・パラメーターの 2 番目の要素は、*SNA (省略時値) あるいは *IP (接続に TCP/IP を使用する) と指定することができます。

TCP/IP を介した DRDA を使用する上での機密保護の考慮事項

ネイティブの TCP/IP を介した DRDA では、通信装置、モード、保護ロケーション属性、および APPC 通信と関連付けられた会話機密保護レベルといった、OS/400 通信機密保護サービスおよび概念を使用しません。したがって、TCP/IP のための機密保護の設定は、それらとは全く異なるものとなります。

TCP/IP を介した DRDA の現在の DB2/400 インプリメンテーションでは、以下の 2 タイプの機密保護メカニズムがサポートされています。

1. ユーザー ID のみ
2. ユーザー ID とパスワード

DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバー (AS) の場合、省略時の機密保護はユーザー ID とパスワードです。つまり、システムをインストールしたら、インバウンド TCP/IP 接続要求には、サーバー・ジョブを実行するときのユーザー ID とパスワードが必要だということです。パスワードが必要でないことを指定するときには、CHGDDMTCPA コマンドを使用することができます。このような変更を行うときには、CHGDDMTCPA PWDRQD(*NO) と入力してください。このコマンドを使用するには、*IOSYSCFG 特殊権限が必要です。

DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・リクエスター (AR、またはクライアント) では、2 通りの方法によって、TCP/IP 接続要求でユーザー ID とともにパスワードを送信することができます。どちらの方法も使用しない場合、ユーザー ID だけが送信されます。

パスワードを送信する最初の方法は、SQL CONNECT ステートメントの USER/USING フォームを使用することです。次のような構文になります。

```
CONNECT TO rdbname USER userid USING 'password'
```

ここで、小文字の語は、適切な接続パラメーターです。組み込み SQL を使用するプログラムでは、ユーザー ID とパスワードの値は、ホスト変数に含めることができます。

TCP/IP を介した接続要求で送信するパスワードを指定する別の方法は、サーバー許可項目を使用することです。サーバー許可リストは、システム上の各ユーザー・プロファイルに関連付けられています。省略時にはリストは空ですが、ADDSVRAUTE コマンドを使用すると項目を追加できます。TCP/IP を介した DRDA 接続を試行するときには、DB2 ユニバーサル・データベース (AS/400 版) はサーバー許可リストを検査して、クライアント・ジョブを実行するときのユーザー・プロファイルを調べます。CONNECT ステートメント上の RDB

名と許可項目内の SERVER 名が一致している場合、接続のユーザー ID としてその項目内の関連付けられた USRID パラメーターが使用されます。また、その項目内に PASSWORD パラメーターが含まれている場合、そのパスワードも接続要求で送信されます。

ADDSVRAUTE コマンドを使用してパスワードを保管する場合には、QRETSVRSEC システム値が '1' に設定されていなければなりません。省略時値は '0' に設定されています。変更するには、次のように入力します。

```
CHGSYSVAL QRETSVRSEC VALUE('1')
```

ADDSVRAUTE コマンドの構文は次のとおりです。

```
ADDSVRAUTE USRPRF(user-profile) SERVER(rdbname) USRID(userid) PASSWORD(password)
```

USRPRF パラメーターでは、アプリケーション・リクエスター・ジョブを実行するときのユーザー・プロファイルを指定します。SERVER パラメーターではリモート RDB 名を指定し、USRID パラメーターではサーバー・ジョブを実行するときのユーザー・プロファイルを指定します。PASSWORD パラメーターでは、サーバーにあるユーザー・プロファイルのパスワードを指定します。

注: SERVER パラメーターの RDB 名を大文字で指定することは非常に重要です。

USRPRF パラメーターを省略すると、ADDSVRAUTE コマンドを実行するときのユーザー・プロファイルに省略時設定されます。USRID パラメーターを省略すると、USRPRF パラメーターの値に省略時設定されます。PASSWORD パラメーターを省略するか、QRETSVRSEC の値が 0 の場合、項目内にパスワードが保管されないため、その項目を使用して接続試行を行うと、使用される機密保護メカニズムはユーザー ID だけになります。

サーバー許可項目は、RMVSVRAUTE コマンドを使用して削除することができ、CHGSVRAUTE を使用して変更できます。これらのコマンドの完全な説明は、*AS/400 Command Reference* を参照してください。

RDB のサーバー許可項目が存在している場合で、CONNECT ステートメントの USER/USING 書式も使用している場合、後者が優先されます。

第5章 DB2 ユニバーサル・データベース (AS/400 版) と DB2 ユニバーサル・データベースとの間のその他の考慮事項

このセクションでは、DB2 ユニバーサル・データベース (AS/400 版) と DB2 共通サーバー バージョン 2 または DB2 ユニバーサル・データベースとの間の SQL 操作に適用される、その他の考慮事項をいくつかリストします。以降の説明は DB2 (OS/2 版) に関するものですが、多くの場合、他のプラットフォーム上の DB2 共通サーバー バージョン 2 および DB2 ユニバーサル・データベースにも類似の考慮事項が適用されます。

1. AS/400 では、表名は集合 (またはライブラリー名) により修飾され、DB2 ユニバーサル・データベース (AS/400 版) データベース (AS/400 ごとに 1 つのデータベース) に保管されます。しかし、PC 上では、表はユーザー ID (表の作成者) により修飾され、特定のデータベース (DB2 (OS/2 版) の入った PC には複数のデータベースを置くことが可能) に保管されます。
 - a. これは、照会される表の名前を集合名を指定せずに指定した場合、DB2 (OS/2 版) から (DB2 コネクトを経由して) DB2 ユニバーサル・データベース (AS/400 版) への照会では、(省略時の) 集合名として (AS/400 上の) ターゲット側のジョブのユーザー ID が使用されるということです。警告が出されるか、その表が見つからないかのいずれかになります。
 - b. これはまた、DB2 ユニバーサル・データベース (AS/400 版) から DB2 (OS/2 版) への照会では、照会に識別子が ('識別子.表名' の形式で) 指定されていない場合、表識別子が暗黙指定されるということでもあります。DB2 (OS/2 版) の表識別子 (AS/400 アプリケーション・リクエストで集合またはライブラリーとして指定されている) の省略時値は、この照会を作成したユーザーのユーザー ID になります。この場合も、警告が出されるか、実行中の照会はその表を見つけれられません。
 - c. 共通ユーザー ID を使用して、DB2 (OS/2 版) の OS/2 データベース および表を作成することができます。DB2 (OS/2 版) では DB2 ユニバーサル・データベース (AS/400 版) にあるような物理集合はありませんが、表識別子があります。これは作成者のユーザー ID です。
2. DB2 (OS/2 版) が DRDA プロトコルを使用するクライアントである場合、DB2 コネクト (または DDCS) が必要です。DB2 (OS/2 版) がサーバーとしてのみ使用されている場合、上記のものは必要ではありません。

3. DB2 コネクトを正しく構成することは非常に重要です。
 - a. DB2 (OS/2 版) および DB2 コネクトのレベルを必ず最新のものにします。入手可能な FixPak を適用してください (まだ行っていない場合)。
 - b. このマニュアルのインストールおよび構成に関する指示に従ってください。
4. APPC を使用している場合、PC 用に作成された制御装置および装置を使用して通信を適切に構成するには特別の注意が必要です。このとき、DB2 (OS/2 版) はアプリケーション・リクエスターまたはアプリケーション・サーバーとして使用されます。さらに、使用している通信プロトコルに関係なく、AS/400 が接続する DB2 (OS/2 版) データベースごとに RDB ディレクトリが必要になります。

APPC 通信を設定するには以下を行ってください。

- a. 装置および制御装置記述を自分で作成することができます。また、トークンリングがあって、かつ回線記述 AUTOCRTCLT パラメーターが *YES の場合、装置および制御装置記述をシステムに作成させることもできます。オプション 2「変更」を使用して、WRKLNDR コマンドを使用し回線記述を調べます。パラメーター 'Autocreate controller' に行き、AUTOCRTCLT 値を調べてください。

ご使用のシステムが制御装置を自動作成する場合、必要な制御装置記述の作成を開始できます。OS/2 のフォルダー CM/2 から、「通信の開始」でサブシステム管理を実行します。サブシステムから SNA サブシステムに対する詳細を調べます。そこで論理リンクを調べることができます。オープンし、目的のシステムへのリンクを活動化してそこで制御装置を自動作成します。そのうち装置記述が自動作成されます。

- b. システム間のネットワーク接続が機能するには、AS/400 の PC の装置と制御装置が ACTIVE である必要があります。制御装置記述で SWTDSC パラメーターを *NO に設定すれば、ACTIVE 制御装置は ACTIVE のままです。また、ONLINE パラメーターを *YES に設定すれば、IPL 時に制御装置は活動状態になります (装置記述の ONLINE パラメーターは *YES に設定しなければならない場合もあります)。制御装置記述のパラメーターを変更するためには、そのパラメーターが VARIED OFF でなければならず、制御装置の所有者 (CTLOWN パラメーター) が *USER に設定される必要があります。
- c. AS/400 が接続する各 DB2 (OS/2 版) の RDB ディレクトリに項目を追加する場合、ADDRDBDIRE コマンドを使用します。RDB 名は DB2 (OS/2 版) データベース名で、リモート・ロケーション名はそのワークステーションの名前です。

5. DB2 (OS/2 版) が使用している AS/400 上のすべての表 (物理ファイル) に対して、正しい CCSID 値 (米国の顧客の場合、通常は 37) が必要です。DSPFD を使用して CCSID 値を表示させ、CHGPF を使用して物理ファイルの CCSID を変更することができます。さらに、正しく接続するために、ジョブの CCSID、使用しているユーザー・プロファイルの CCSID、またはシステム CCSID 値 (QCCSID) (省略時値の 65535 の場合) のうちのいずれかを変更する必要があるかもしれません。通常、この変更を行うための最適の場所は、サーバー・ジョブが実行されているユーザー・プロファイル内です。
6. DB2 コネクトを使用して AS/400 と相互協調処理を行う前に、アプリケーション・プログラムおよび DB2 コネクト ユーティリティー用に SQL パッケージを作成する必要があります。
 - a. DB2 PREP コマンドを使用して、組み込み SQL の付いたアプリケーション・プログラム・ソース・ファイルを処理します。この処理を行うことにより、SQL ステートメント用のホスト言語呼び出しを含む、変更されたソース・ファイルが作成され、省略時には、現在接続しているデータベースの SQL パッケージが作成されます。
 - b. DB2 コネクト ユーティリティーを AS/400 DB2 サーバーにバインドするには以下のことを行ってください。

1)

```
CONNECT TO rdbname
```

2)

```
BIND path@DDCS400.LST BLOCKING ALL SQLERROR CONTINUE  
MESSAGES DDCS400.MGS GRANT PUBLIC
```

path@DDCS400.LST の path を省略時のパス C:¥SQLLIB¥BND¥ に置き換えるか、または省略時ロケーションにインストールしていない場合はご使用のローカル値と置き換えます。

注: リストの 3 番目のファイル上の DB2 ユニバーサル・データベース (AS/400 版) データベースから SQL コード -901 を避けるために OS/400 V3R1 では PTF SF23624 が必要です。

3)

```
CONNECT RESET
```

7. DB2 ユニバーサル・データベース (AS/400 版) から DB2 (OS/2 版) への対話式 SQL
 - a. セッション属性 NAMING(*SQL)、DATFMT(*ISO)、および TIMFMT(*ISO) を使用します。 *ISO 作業以外の他の形式 (ただしすべ

てではない)、および日付形式 (DATFMT) で使用される形式は、時刻形式 (TIMFMT) でも使用されなければなりません。

- b. AS/400 の COLLECTION と DB2 (OS/2 版) の表修飾子 (作成者のユーザー ID) との間の対応にご注意ください。SQL 操作については、この考慮事項のリストの項目 1 を参照してください。
 - c. 最初の対話式セッションで、コミットメント制御に必ず COMMIT(*CS) を指定しなければなりません。その後、(1) RELEASE ALL、(2) COMMIT、そして (3) CONNECT TO rdbname (特定のデータベースで 'rdbname' が置換される場所) を指定します。この時点で、GRANT EXECUTE ON PACKAGE QSQL400.QSQL0200 TO PUBLIC (または特定のユーザー) を入力できます。これにより、他のユーザーも対話式 SQL 用に PC 上で作成された SQL PKG を使用することができます。
8. DB2 (OS/2 版) にアクセスする AS/400 上に作成されたどのようなプログラムに関しても、以下の DB2 (OS/2 版) コマンドを使用することを忘れないでください。

a.

```
GRANT ALL PRIVILEGES ON TABLE table-name TO user
```

b.

```
GRANT EXECUTE ON PACKAGE package-name (usually the AS/400  
program name) TO user
```

場合によっては、ユーザーに 'PUBLIC' を指定することがあります。

9. V.2.1.1 以前の DB2 (OS/2 版) にアクセスする AS/400 アプリケーションの開発にあたっては、実際にはパッケージが作成されていないのに、CRTSQLxxx コマンドに対する応答として、SQL パッケージが PC で作成されたというメッセージ (SQL5057) が出されていました。これは DB2 (OS/2 版) の最新のレベルで修正されました。

さらに、DB2 (OS/2 版) のより以前のバージョンでは、ソース・メンバー記述のテキスト・フィールドに何か入っている OS/400 プログラムには、SQL パッケージは作成されませんでした。

10. DB2 (OS/2 版) の C 言語ストアード・プロシージャは、パラメーターとして argc および argv は使用することができません (タイプを main() にできません)。これは AS/400 ストアード・プロシージャとは異なります。この AS/400 ストアード・プロシージャは argc および argv を使用しなければなりません。DB2 (OS/2 版) ストアード・プロシージャに関しては、¥SQLLIB¥SAMPLES サブディレクトリーの例を参照してください。C サブディレクトリーの OUTSRV.SQC および OUTCLI.SQC を探してください。

11. DB2 (OS/2 版) のストアード・プロシージャ (AS/400 で呼び出される) では、プロシージャ名には大文字を使用してください。現在の AS/400 ではプロシージャ名は大文字に変換されます。しかし、これは、PC 上のプロシージャが小文字で同じプロシージャ名を持っている場合、検出されないということです。AS/400 のストアード・プロシージャには、必ず大文字を使用してください。
12. また、組み込み SQL に適切な PTF を適用していない場合、AS/400 から DB2 (OS/2 版) への CALL ステートメントは、プロシージャ名をホスト変数 (CALL :host-procedure-name(...)) に書き込んだ場合にのみ、実行されます。これを修正する V3R7 の PTF は SF35932 で、V3R2 の PTF は SF36535 です。
13. ストアード・プロシージャは、呼び出し側のプログラムと同じ活動化グループで実行するように作成された場合 (作成の正しい方法)、COMMIT を含むことができません。しかし、DB2 (OS/2 版) では、ストアード・プロシージャは COMMIT を含むことができます。しかしアプリケーションの設計者は、DB2 ユニバーサル・データベース (AS/400 版) の側にコミットが生じるという知識がないことを承知しなければなりません。

第6章 DRDA ネットワークでの DB2 (VSE および VM 版) の接続

SQL/DS (DB2 (VM 版)) バージョン 3 リリース 5 は、VM システムに、DRDA リモート作業単位アプリケーション・サーバーとアプリケーション・リクエスター・サポートの両方を提供します。SQL/DS (DB2 (VSE 版)) バージョン 3 リリース 5 は、VSE システムに、DRDA リモート作業単位アプリケーション・サーバー・サポートを提供します。

さらに、DB2 (VSE および VM 版) のバージョン 5 リリース 1 は、VM および VSE システムの両方に、DRDA 分散作業単位アプリケーション・サーバー・サポートを提供します。この章では、主に DB2 (VSE および VM 版) システムを異種のリモート DRDA システムに接続することについて説明します。DB2 (VSE および VM 版) の接続に関する詳細については、以下のマニュアルを参照してください。

- *VM/ESA 接続計画、管理および操作*
- *DB2 システム管理 (VM 版)*
- *DB2 システム管理 (VSE 版)*

DB2 (VM 版) 概説

それぞれの DB2 (VM 版) データベース・マネージャーは、1 つ以上のデータベースを同時に管理でき、通常はその時点で管理しているデータベースの名前で参照されます。関係データベース名は、内部接続された SNA ネットワークのセット内では固有です。

分散データベース処理に関する各種の DRDA および VM 構成要素について、以下に説明します。これらの構成要素を使用すると、DB2 (VM 版) データベース・マネージャーは、ローカル関係データベースにアクセスでき、SNA ネットワークでリモート DRDA システムと通信できます。

AVS APPC/VTAM サポート (AVS) は、VM アプリケーションが SNA ネットワークにアクセスできるようにする VM 構成要素です。これは、SNA で定義されている論理装置 (LU) 機能を提供します。LU は、VM 環境ではゲートウェイと呼ばれています。AVS は、グループ制御システムで VTAM アプリケーションとして実行します。これは、APPC/VM マクロ呼び出しを APPC/VTAM マクロ呼び出しに、またそ

の逆に変換します。APPC/VM は、AVS を使用してデータ・ストリームを経路指定および変換します。AVS の使用により、DB2 (VM 版) 要求はローカル VM システムとリモート SNA ロケーションとの間で経路指定されます。DB2 (VM 版) アプリケーションまたはデータベースが DB2 (VM 版) 以外のデータベースまたはアプリケーションと通信しているときには常に、AVS を使用しなければなりません。

アプリケーション・リクエスター側では、要求が送信される前に、AVS ゲートウェイを介して接続することがユーザーに許可されていなければなりません。アプリケーション・サーバー側では、AVS がユーザーの要求を渡す前に、受信している AVS ゲートウェイが DB2 (VM 版) サーバー・マシンに接続するように許可されていなければなりません。許可は、適切な IUCV ディレクトリー制御ステートメントを、ユーザー・マシン、データベース・マシン、送信側および受信側の AVS マシンに提供することによって行われます。これを行う方法についての詳細は、*VM/ESA 接続計画、管理および操作* を参照してください。

APPC/VM

APPC/VM は、SNA により定義される LU 6.2 機能セットのサブセットを提供する VM アセンブラー・レベル API です。分かりやすく言うと、APPC/VM は DB2 (VM 版) アプリケーションがローカルおよびリモート・データベースの接続や処理を可能にする LU 6.2 verb を提供します。APPC/VM によりサポートされる LU 6.2 verb は、*VM/ESA CP プログラミング・サービス* にリストされています。

通信ディレクトリー

通信ディレクトリーは、ローカル VM アプリケーション・リクエスターとアプリケーション・サーバーとの間に APPC 会話を確立するとき特定の役割を果たす CMS NAMES ファイルです。ディレクトリーは、ターゲット・サーバーとの APPC 会話の経路指定および確立に関する必要な情報を提供します。この情報には、LU 名、TPN、機密保護、モード名、ユーザー ID、パスワード、およびデータベース名などの項目が含まれます。

DB2 (VM 版) は、COMDIR タグ `:dbname` を使用して、RDB_NAME を対応する経路指定データに解決します。

この特殊ファイルおよび通信機能に関しては、*VM/ESA 接続計画、管理および操作* で説明されています。

CRR 整合資源回復 (CRR) は、保護資源の更新のコミットまたはバックアウ

トを調整する VM 機能です。分散アプリケーションは、CRR と協力して、保護会話を使用し分散トランザクション資源保全性を確保します。

CRR 回復サーバー

CRR 回復サーバーは CRR の構成要素であり、それぞれの仮想計算機で稼働します。これは、同期点ログ記録および再同期機能の実行を担当するものです。

GCS グループ制御システムは VM 構成要素であり、以下のものから成ります。

- 仮想計算機で実行する共用セグメント
- 多数の仮想計算機を 1 つのグループにまとめ、その操作を監視する仮想計算機監視プログラム
- 以下のプログラム製品間のインターフェース
 - 仮想リモート通信アクセス方式 (VTAM)
 - APPC/VTAM サポート (AVS)
 - リモート・スプーリング通信サブシステム (RSCS)
 - 制御プログラム (CP)

GCS は、VM 環境での AVS のような VTAM アプリケーションの実行を監視します。GCS の監視のもとで稼働する仮想計算機は、CMS を使用しません。

資源アダプター

資源アダプターは、ご使用の仮想計算機にあり、ご使用のアプリケーションが DB2 (VM 版) サーバーへのアクセスを要求できるようにする DB2 (VM 版) の論理部分です。DRDA アプリケーション・リクエスト機能は、リソース・アダプターに統合されています。

TSAF 透過サービス・アクセス機能は、相互接続された VM システム間に通信サポートを提供する VM 構成要素です。TSAF コレクションには 8 個までの VM システムが参加できます。これは、VM ローカル・エリア・ネットワーク (または広域ネットワーク) と類似したものと考えることができます。参加しているそれぞれの VM システムでは、TSAF 仮想計算機が作動可能でなければなりません。TSAF コレクション内では、すべてのユーザー ID および資源 ID は固有です。

DB2 (VM 版) は TSAF を使用して、TSAF コレクション内での他の DB2 (VM 版) マシンへの分散データベース要求を経路指定します。ローカル VM システムに AVS 仮想計算機がない場合、DB2 (VM 版) は TSAF を使用して DRDA 要求を AVS 仮想計算機のある VM シス

テムに経路指定します。AVS を使用すると、要求を他の TSAF コレクションおよび非 DB2 (VM 版) システムに転送できます。

TSAF コレクションは、SNA ネットワークでは 1 つ以上の論理装置として表示されます。TSAF コレクションでグローバルとして定義された資源は、コレクション内のどこにあるリモート APPC プログラムからでもアクセスできます。

一般に、TSAF コレクションは独立型で機能し、VTAM および SNA ネットワークから独立しています。しかし、これは AVS および VTAM と協働して、グローバル資源が SNA ネットワーク内のどこにあるリモート APPC プログラムからもアクセスできるようにします。これには、AVS マシンおよび VTAM マシンが TSAF メンバーの 1 つかそれ以上で作動していなければなりません。TSAF に関しては、VM/ESA 接続計画、管理および操作 で説明されています。

VTAM 仮想リモート通信アクセス方式 (VTAM) は、接続のネットワーク通信サポートを提供します。DB2 (VM 版) は、AVS を介して VTAM サービスを使用して、接続の経路指定をし、リモート DRDA システムに要求します。VTAM は、SNA ネットワークにアクセスするリモート要求にのみ 使用されます。

***IDENT**

AVS および TSAF はトランザクション・プログラム名 (TPN) を使用して、TSAF および AVS を介して接続された VM システム間の要求を経路指定します。TPN は SNA 登録された TPN または有効な英数字名にできます。VM は、TPN 値を資源 ID として参照します。DB2 (VM 版) サーバーがリモート DRDA システムにアクセスできるようにするには、DB2 (VM 版) サーバーは VM IDENTIFY (*IDENT) システム・サービスを使用して、サーバー自身をグローバル資源 ID (TPN) のマネージャーとして定義します。サーバーがグローバル資源として識別された後で、受信した TPN が資源 ID と一致した場合、TSAF および AVS は DRDA 要求を DB2 (VM 版) サーバーへ経路指定できます。

アプリケーション・リクエスター通信フローの例

以下の例は、VM アプリケーション・リクエスターとリモート DRDA サーバーとの通信が確立される上での各構成要素の役割を示しています。135ページの図27には、アプリケーション・リクエスターが AVS に接続し、VTAM を使用して SNA ネットワークにアクセスする方法について示されています。リ

モート資源へのアクセスは、ローカル DB2 (VM 版) アプリケーション・サーバーを介して経路指定されるのではありません。

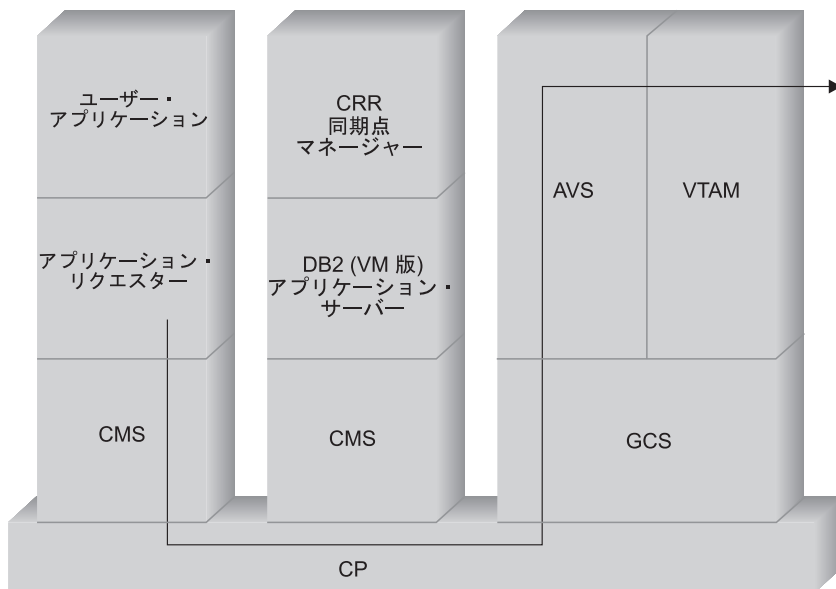


図 27. リモート資源へのアクセス要求

TSAF コレクションで実行している DRDA (VM 版) アプリケーション・リクエスターが、DRDA アプリケーション・サーバーにより管理されているリモート・データにアクセスするとします。これは、当然のことながら、TSAF マシンがアプリケーション・リクエスターがある VM ホストで操作されているということです。また、AVS 構成要素および VTAM マシンはこの TSAF コレクションの VM システムで運用されています。AVS および VTAM は、アプリケーション・リクエスターおよびアプリケーション・サーバーと同じシステムにもあります。

VTAM マシンの開始後は、ローカル AVS ゲートウェイを SNA ネットワークに定義し、1 つまたは複数のセッションを後で会話を確立するために使用するよう活動化します。

AVS マシンの開始後は、ローカル AVS ゲートウェイと潜在的なパートナー LU とのセッション限度を折衝します。

アプリケーション・サーバーは活動状態の場合も、そうでない場合もあります。操作員は、同種または異種アプリケーション・リクエスターからの要求を処理できるようになる前に、これを開始しなければなりません。

アプリケーション・リクエスターは APPC/VM CONNECT ステートメントを出して、アプリケーション・サーバーとの LU 6.2 会話を確立します。CONNECT 機能は CMS 通信ディレクトリーを使用して、関係データベース名を、SNA ネットワークでのアプリケーション・サーバーのアドレスを構成する関連 LU 名および TPN に解決します。CMS 通信ディレクトリーは、許可の目的でリモート側に渡すユーザー ID およびパスワードなどの会話機密保護のレベルおよび機密保護トークンも判別します。SECURITY=PGM が使用された場合、アプリケーション・リクエスターはユーザー ID およびパスワードをアプリケーション・サーバーに渡さなければなりません。ユーザー ID およびパスワードは、CMS 通信ディレクトリー内か、またはアプリケーション・リクエスター・ユーザーの CP ディレクトリーで定義された APPCPASS レコードに指定できます。SECURITY=SAME が使用された場合、アプリケーション・リクエスター・ユーザーの VM ログオン ID のみアプリケーション・サーバーに送信され、他のパスワードは必要ではなくなります。

たとえば、SECURITY=SAME を使用すると、ホストは AVS マシンがローカルで稼働しているかどうかを確認します。SECURITY=SAME を使用しない場合、ホストはアプリケーション・リクエスターとローカル TSAF マシンとの接続を確立します。ローカル TSAF マシンは、AVS マシンの TSAF コレクションで他の TSAF マシンをポーリングしてから、それとの接続を確立します。

TSAF コレクションの AVS 構成要素は、APPC/VM 接続要求を APPC/VTAM 同等機能呼び出しに変換します。それから、AVS は既存のセッションを使用するか、そのゲートウェイ (LU) とリモート LU との間に新しいセッションを割り当てます。次いで、AVS がリモート LU との会話を確立し、それに LU 名、TPN、機密保護レベル、およびユーザー ID を渡します。リモート LU も VM システムである場合には、セッションおよび会話は、システムで稼働している AVS 構成要素により制御されます。

アプリケーション・サーバー通信フローの例

以下の例は、各構成要素がアプリケーション・リクエスターとローカル DB2 (VM 版) DRDA サーバーとの通信の確立において果たす役割を示しています。137ページの図28には、VTAM がインバウンド接続を特定の AVS ゲートウェイへ、さらにアプリケーション・サーバーへ、経路指定する様子が示されています。

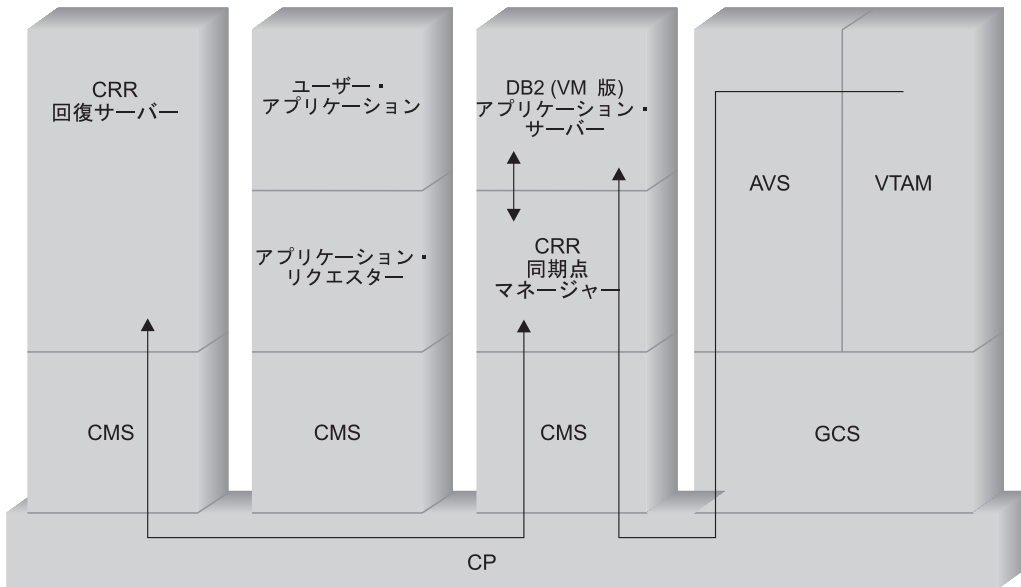


図 28. リモート資源へのアクセスの獲得

DB2 (VM 版) アプリケーション・サーバーが TSAF コレクションで運用されているとします。これは、当然のことながら、TSAF マシンがアプリケーション・リクエスターがある VM ホストで運用されているということです。また、AVS 構成要素および VTAM マシンはこの TSAF コレクションの VM システムで運用されています。AVS および VTAM は、アプリケーション・リクエスターおよびアプリケーション・サーバーと同じシステムにもあります。

VTAM マシンの開始後は、ローカル AVS ゲートウェイを SNA ネットワークに定義し、1 つまたは複数のセッションを後で会話を確立するために使用するよう活動化します。

AVS マシンの開始後は、ローカル AVS ゲートウェイと潜在的なパートナー LU とのセッション限度を折衝します。

アプリケーション・サーバーは活動状態の場合も、そうでない場合もあります。操作員は、同種または異種アプリケーション・リクエスターからの要求を処理できるようになる前に、これを開始しなければなりません。アプリケーション・サーバーが開始してから、*IDENT サービスを使用して、ホスト VM システムを管理する資源 ID を登録します。各登録では、VM システムにより管理される内部資源表に項目を作成します。

ローカル AVS 構成要素がパートナー LU とのセッションを確立した後、会話を受け入れ、TPN、ユーザー ID、パスワードを VM ホストに渡し、妥当性検査を行います。VM は、内部資源表で TPN を検索します。この表には、*IDENT システム・サービスを介して登録された各資源 ID の項目が含まれています。TPN 検索が成功すれば、VM はユーザー ID およびパスワードをそのディレクトリー、または RACF (もしくは同様の機密保護製品) を使用して妥当性検査を行います。妥当性検査が成功すると、AVS はアプリケーション・サーバーへの接続を確立し、データベース許可の目的でこれにユーザー ID を渡します。

表検索が不成功に終わった場合には、AVS は TPN が TSAF コレクションの他の VM システムにあるとして、ローカル TSAF マシンへの接続を確立し、これにユーザー ID、パスワード、TPN を渡します。TSAF マシンは、TSAF コレクションにある他方の TSAF マシンをポーリングします。これらのマシンのいずれかが、資源表に TPN があることを認識すると、ローカル TSAF マシンはリモート TSAF マシンに接続し、これにユーザー ID およびパスワードを渡し、その VM ディレクトリーによってそれらが検査されるようにします。妥当性検査が成功した場合、リモート TSAF マシンはアプリケーション・サーバーに接続し、ユーザー ID をデータベース許可のために渡します。

アプリケーション・リクエスターが DRDA 分散作業単位サポートを利用しようとする場合、DB2 (VM 版) アプリケーション・サーバーと、保護会話 (SYNCLEVEL=SYNCPPT など) を確立します。CMS が DB2 (VM 版) との接続を表示する前に、DB2 (VM 版) は DB2 (VM 版) マシン上での保護会話のために CMS 作業単位を作成します。その後 DB2 (VM 版) は、リクエスターの作業を実行する場合はいつでも、この CMS 作業単位を使用します。DB2 (VM 版) がリクエスターの作業を始めるときに、DB2 (VM 版) は CRR 同期点管理プログラムを使用して、この CMS 作業単位を登録します。そして、DB2 が保護会話で "take commit" または "take rollback" という指示を受け取った場合、それらの指示は CRR 同期点管理プログラムに作業単位をコミットまたはロールバックするように求めています。その後、CRR 同期点管理プログラムは CRR 回復サーバーに必要な時に同期点ログの記録を行うように要求し、コミットまたはロールバックを行います。

接続の経路指定の複雑さによっては、アプリケーション・リクエスターとアプリケーション・サーバーとの APPC 会話に他のシステムが関係してくる場合もあります。しかし、中間接続はすべて VM により管理され、アプリケーション・リクエスターやユーザー・アプリケーションからは見えません。APPC/VM インターフェースによって、DB2 (VM 版) アプリケーション・サーバーは以下の場所にある APPC アプリケーションと通信します。

- 同一の VM システム
- 異なる VM システム
- AVS および VTAM が稼働している SNA ネットワークの VM システム
- AVS および VTAM が稼働している、異なる TSAF コレクションでの VM システム
- LU 6.2 プロトコルをサポートする SNA ネットワークでの非 VM システム
- LU 6.2 プロトコルをサポートする SNA ネットワークでの非 IBM システム

DB2 (VM 版) インプリメンテーション

140ページの図29 に図示されているように、VM アプリケーションは DB2 VM アプリケーション・リクエスター (資源アダプター) を介して DB2 (VM 版) または DRDA アプリケーション・サーバー・データベースにアクセスしなければなりません。DB2 (VM 版) アプリケーション・サーバー・データベースは、任意の DB2 (VM 版) または DRDA アプリケーション・リクエスターから SQL 要求を受け取ることができます。

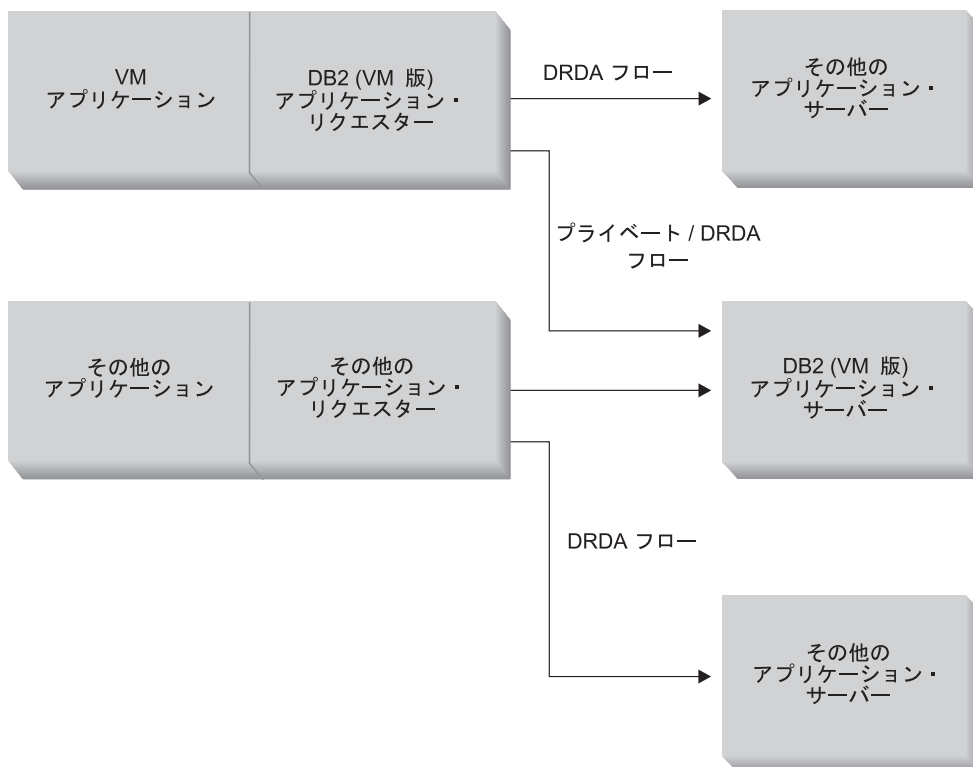


図 29. DB2 (VM 版) アプリケーション・リクエスターおよびアプリケーション・サーバー

アプリケーションのプリプロセスまたは実行オプション

DB2 (VM 版) は、ユーザーおよびデータベース管理者が分散データベース・サポートを使用可能にできる 3 つの処理オプションを SQLINIT コマンドにサポートしています。ユーザーは、アプリケーションをプリプロセスまたは実行する前に以下のいずれかの SQLINIT オプションを指定できます。

PROTOCOL(SQLDS)

プライベート SQLDS プロトコルの使用を要求します。これは、省略時オプションです。これは、ローカルまたはリモート環境で、DB2 (VM 版) アプリケーション・リクエスターとサーバーとの間で使用できます。DB2 (VM 版) アプリケーションは、リクエスターが同じ CCSID をサーバーとして使用することを前提とします。SQLINIT を

介してリクエスターにより設定された CCSID 省略時値⁵は無視され、どの LU 6.2 LUWID も会話と関連していません。DB2 (VM 版) システムしか使用しておらず、どこでも同じ省略時 CCSID を使用している場合には、この方法が最も効果的といえます。

PROTOCOL(AUTO)

DB2 (VM 版) アプリケーション・リクエスターに、アプリケーション・サーバーが同種システムか異種システムかを判別するように要求します。それから、同種システムにはプライベート SQLDS プロトコル、異種システムには DRDA プロトコルの使用を自動的に選択します。これは、同種 (ローカルおよびリモート) システムと異種システムとの間で使用できます。アプリケーション・サーバーが PROTOCOL=SQLDS で設定されていない場合には、アプリケーション・リクエスターとサーバーは異なる CCSID 省略時値を持つことができます。要求および応答は、適切に変換されます。AUTO は、以下のいずれかの場合に勧められるオプションです。

- 同種および異種システムの両方にアクセスする必要がある場合
- CCSID 省略時値がリクエスターおよびサーバーで異なる場合 (そしてアプリケーション・サーバーの PROTOCOL オプションが SQLDS ではない場合)
- タスクを起点サイトまで容易に追跡できるようにするために、各会話に関連する LU 6.2 LUWID が必要な場合。ご使用の分散データベース・ネットワークで数多くのリモート DB2 (VM 版) を管理している場合には、これは役に立ちます。

PROTOCOL(DRDA)

DB2 (VM 版) アプリケーション・リクエスターが DRDA プロトコルだけを使用して、アプリケーション・サーバーと通信するようにします。このオプションは、同種 (ローカルおよびリモート) システムと異種システムとの間で使用できます。アプリケーション・サーバーが同種システムの場合には、DRDA プロトコルが 2 つの DB2 (VM 版) システムの間で使用されます。アプリケーション・リクエスターとアプリケーション・サーバーとは CCSID 省略時値が異なります。要求および応答は、適切に変換されます。このオプションは 2 つの DB2 (VM 版) システムの間でテスト用に、またはある種のアプリケーション用に使用できます。つまり、DRDA プロトコルを使用するとデータの送受

5. DB2 (VM 版) では、アプリケーション・リクエスターおよびアプリケーション・サーバーはそれぞれ SQLINIT および SQLSTART に CHARNAME オプションを指定して省略時 CCSID を指定します。CHARNAME は、適切な CCSID に内部でマップされる記号名です。

信に、より大きなバッファ・サイズが使えるためにスループットが向上する場合があるので、その種のアプリケーションに使用できます。

表3 では、DB2 (VM 版) アプリケーション・リクエスターの SQLINIT 処理オプションの機能特性が比較されています。

表3. DB2 (VM 版) アプリケーション・リクエスター SQLINIT 処理オプションの比較

[SQLDS]	[AUTO]	[DRDA]
両パートナーとも DB2 (VM 版) システムでなければなりません。	どの DRDA システムにも接続しません。	どの DRDA システムにも接続します。
TSAF または AVS/VTAM を介してローカルにパートナーと通信できます。	DB2 (VM 版) システムとローカルに通信できます。また、TSAF か AVS を介してリモート DB2 (VM 版) と通信できます。異種システムでは、AVS を介して通信しなければなりません。	DB2 (VM 版) システムとローカルに通信できます。また、TSAF か AVS を介してリモート DB2 (VM 版) と通信できます。異種システムでは、AVS を介して通信しなければなりません。
静的、動的、および拡張動的 SQL をサポートします。	静的、動的、および拡張動的 SQL をサポートします。	静的、動的、および拡張動的 SQL をサポートします。 ⁶
アプリケーション・リクエスターの SQLINIT で定義された CCSID は、DB2 (VM 版) アプリケーション・サーバーにより無視されます。	アプリケーション・リクエスターについて SQLINIT で定義された CCSID が DB2 (VM 版) アプリケーション・サーバーで適用され、適切な会話が実行されます (アプリケーション・サーバーが AUTO に設定されている場合)。	アプリケーション・リクエスターについて SQLINIT で定義された CCSID が DB2 (VM 版) アプリケーション・サーバーで適用され、適切な会話が実行されます。
固定 8K ブロック・サイズ; OPEN 呼び出しは行を戻さない; アプリケーション・リクエスターがカーソルを明示的にクローズする必要がある。	DB2 (VM 版) から DB2 (VM 版) では SQLDS 方式。その他は DRDA 方式。	可変 1K ~ 32 K ブロック・サイズ; よりコンパクトなデータ・パッケージング; OPEN 呼び出しは行の 1 ブロックを戻す; アプリケーション・サーバーが暗黙的にカーソルをクローズするため、アプリケーション・リクエスターは CLOSE 送信する必要がない。
固定 8K ブロック・サイズを使用している時には、カーソル INSERT および PUT を使用して行のブロックを挿入できます。	DB2 (VM 版) から DB2 (VM 版) では SQLDS 方式。その他は DRDA 方式。	PUT は正規の単一行挿入に変換され、一度に一行ずつ送信されます。

6. 拡張動的 SQL は、静的または動的のステートメントに変換されることにより DRDA フローでサポートされています。いくつかの制限が適用されます。

表3. DB2 (VM 版) アプリケーション・リクエスター *SQLINIT* 処理オプションの比較 (続き)

すべての DB2 (VM 版) 固有コマンドがサポートされます。	DB2 (VM 版) から DB2 (VM 版) では <i>SQLDS</i> 方式。その他は <i>DRDA</i> 方式。	DB2 (VM 版) オペレーター・コマンド、一部の DB2 (VM 版) ステートメント、およびいくつかの <i>ISQL</i> と <i>DBSU</i> コマンドはサポートされません (<i>DB2</i> サーバー (<i>VSE</i> および <i>VM</i> 版) <i>SQL</i> 解説書を参照)。
<i>LUWID</i> はサポートされません。	<i>LUWID</i> がサポートされます。	<i>LUWID</i> がサポートされます。

データベース・サーバー・マシンの開始オプション

ここでは、データベース・サーバー・マシンを開始させるさまざまなオプションについて説明します。

PROTOCOL パラメーター

データベース管理者は、データベース・サーバー・マシンを開始するときに、*PROTOCOL* パラメーターで以下のいずれかのオプションを指定できます。

SQLDS

アプリケーション・サーバーが DB2 (VM 版) アプリケーション・リクエスターまたは *VSE* ゲスト共有を利用している DB2 (*VSE* 版) アプリケーション・リクエスターのサポートだけを提供する場合の、省略時または推奨されるオプション。アプリケーション・サーバーはプライベート (*SQLDS*) フローだけを使用します。

アプリケーション・サーバーはアプリケーション・リクエスターによって選択される処理オプションに影響されます。DB2 (VM 版) リクエスターが *PROTOCOL(SQLDS)* を指定する場合、DB2 (VM 版) サーバー上の処理はプライベート・フローを使用して通常通り続けられます。DB2 (VM 版) が *PROTOCOL(AUTO)* を指定すると、DB2 (VM 版) サーバーはプライベート・フローを切り替えるよう、リクエスターに通知します。アプリケーション・リクエスターとアプリケーション・サーバーとの間で *CCSID* 情報は交換されません。アプリケーション・サーバーは、アプリケーション・リクエスター *CCSID* がアプリケーション・サーバー *CCSID* と同じであるとして処理します。DB2 (VM 版) リクエスターが *PROTOCOL(DRDA)* を指定すると、会話は終了します。DB2 (VM 版) と DB2 (*VSE* 版) 以外のアプリケーション・リクエスターが DB2 (VM 版) サーバーにアクセスしようとする、会話は終了します。

AUTO アプリケーション・サーバーがプライベート・プロトコルと *DRDA* プ

ロトコルの両方にサポートを提供する必要がある場合に推奨されるオプション。PROTOCOL(SQLDS) または PROTOCOL(AUTO) を指定した DB2 (VM 版) アプリケーション・リクエスターはプライベート・フローで通信を行います。SQLDS を指定したアプリケーション・リクエスターでは、CCSID 情報は全く交換されず、アプリケーション・サーバーは、アプリケーション・リクエスター CCSID がアプリケーション・サーバー CCSID と同一であると想定します。AUTO を指定したリクエスターでは、CCSID 情報が交換され、要求および応答の CCSID 会話は正しく実行されます。DB2 (VM 版) 以外のリクエスター、または PROTOCOL(DRDA) を指定する DB2 (VM 版) リクエスターは、DRDA フローが必要です。

SYNCPNT パラメーター

このパラメーターは、同期点管理プログラム (SPM) が DRDA-2 マルチ・サイト読み込み、マルチ・サイト書き込み分散作業単位活動を調整するために使用されるかどうかを指定します。

Y を指定すれば、サーバーは同期点管理プログラムを使い (可能な場合)、2 フェーズ・コミットおよび再同期活動を調整します。N を指定すれば、アプリケーション・サーバーは 2 フェーズ・コミットを実行するために SPM を使用しません。N が指定された場合、アプリケーション・サーバーはマルチ・サイト読み込み、マルチ・サイト書き込み分散作業単位に限定され、シングル書き込みサイトになる場合があります。Y が指定された場合、アプリケーション・サーバーは検索マネージャーが利用不能であることを見つけ、その後サーバーは N が指定されたものとして操作されます。

PROTOCOL=AUTO のときの省略時値は SYNCPNT=Y です。

PROTOCOL=SQLDS のとき、SYNCPNT パラメーターは N に設定されます。

VM 環境でのアプリケーション・リクエスターのセットアップ

DB2 (VM 版) には、DRDA アプリケーション・リクエスター・サポートが、アプリケーションのあるエンド・ユーザーの仮想計算機上に存在するリソース・アダプターの統合部分として実装されています。ローカルのデータベース・マネージャーの仮想計算機がアクティブではないときでも、アプリケーション・リクエスター・サポートを使用できます。DRDA アプリケーション・リクエスター・サポートは、PROTOCOL(AUTO) または PROTOCOL(DRDA) を指定して SQLINIT EXEC を実行することにより活動化できます (140ページの『アプリケーションのプリプロセスまたは実行オプション』を参照)。

アプリケーション・リクエスターとして動作する場合、DB2 (VM 版) は DB2 (VM 版) アプリケーション・サーバーまたは DRDA アーキテクチャーをサポートする他の製品サーバーに接続できます。DB2 (VM 版) アプリケーション・リクエスターを使用して分散データベースにアクセスするには、以下のようになる方法を知っている必要があります。

- 『ネットワーク情報の提供』。アプリケーション・リクエスターは、RDB_NAME 値を受け入れ、それらを SNA NETID.LUNAME 値に変換する必要があります。DB2 (VM 版) は、CMS 通信ディレクトリーを使用して RDB_NAME とそれに対応するネットワーク・パラメーターをカタログします。通信ディレクトリーによって、アプリケーション・リクエスターは分散データベース要求を出すときに、必要な SNA 情報を VTAM に渡すことができます。
- 154ページの『機密保護の提供』。アプリケーション・サーバーがリモートのデータベース要求を受け入れるためには、アプリケーション・リクエスターはアプリケーション・サーバーの要求する安全保護情報を提供しなければなりません。DB2 (VM 版) は、通信ディレクトリーおよび CP ディレクトリーをアプリケーション・リクエスターの側で使用し、CP ディレクトリーまたは RACF をアプリケーション・サーバーの側でオプションとして使用して、分散データベース要求を出すときに必要なネットワーク安全保護情報を提供します。
- 159ページの『データの表示』。アプリケーション・リクエスターには、アプリケーション・サーバーと互換性のある CCSID がなければなりません。

ネットワーク情報の提供

分散データベース環境の処理の多くで、ネットワーク内の他の場所との間でメッセージが交換される必要があります。この処理を正しく実行するために、以下のステップに従ってください。

1. ローカル・システムの定義
2. リモート・システムの定義
3. 通信サブシステムの定義
4. RU サイズおよび歩調合わせの設定
5. DB2 (VM 版) アプリケーション・リクエスターの準備

ローカル・システムの定義

DB2 (VM 版) アプリケーション・リクエスターと DB2 (VM 版) アプリケーション・サーバーは、互いに独立しています。DB2 (VM 版) アプリケーション・リクエスターは、ローカルまたはリモート・アプリケーション・サーバーへの接続要求を直接指示します。しかし、インバウンド接続要求の宛先として

それ自身を定義することはありません。DB2 (VM 版) アプリケーション・サーバーだけがインバウンド接続要求を受け入れる (または拒否する) ことができます。そのため、DB2 (VM 版) アプリケーション・リクエスターは、DB2 ユニバーサル・データベース (OS/390 版) がするように RDB_NAME および TPN を自分で識別することはできません。

以下のように、DB2 (VM 版) アプリケーション・リクエスターを SNA ネットワークに定義してください。

1. VTAM APPL 定義ステートメントを使用して、AVS ゲートウェイ名を定義する。

アプリケーション・リクエスターはゲートウェイ名 (たとえば、LU 名) を定義し、アウトバウンド要求をネットワークに経路指定できるようにしてなければなりません。図30 には、この例が示されています。これらのステートメントは、VTAM 仮想計算機にあります。VTAM が開始すると、ゲートウェイはネットワークに識別されますが、制御 AVS 仮想計算機が開始するまで活動状態にはなりません。各 AVS 仮想計算機は、複数のゲートウェイを VM ホストに定義できます。

```

VBUILD TYPE=APPL
*****
*
*   Gateway Definition for Toronto DB2 for VM System   *
*
*****
TORGATE  APPL  APPC=YES,                X
            AUTHEXIT=YES,              X
            AUTOSES=1,                  X
            DMINWNL=10,                 X
            DMINWNR=10,                 X
            DSESLIM=20,                 X
            EAS=9999,                   X
            MAXPVT=100K,                 X
            MODETAB=RDBMODES,           X
            PARSESS=YES,                 X
            SECACPT=ALREADYV,           X
            SYNCLVL=SYNCPT,             X
            VPACING=2

```

図 30. AVS ゲートウェイ定義の例

以下のリストに、本書のトピックにあてはまる VTAM APPL ステートメント・キーワードを説明します。(VTAM APPL ステートメントはここに説明したものよりもっと多くのキーワードをサポートしています。)

TORGATE

VTAM は、ゲートウェイ (LU) 名として APPL ステートメント・

ラベルを使用します。146ページの図30では、ゲートウェイ TORGATE が定義されています。VTAM APPL ステートメントは NETID を指定しません。NETID は、VTAM システムのすべての VTAM アプリケーションに自動的に割り当てられます。

AUTOSES=1

ゲートウェイ TORGATE は、APPC セッション数変更 (CNOS) コマンドを出すときに、1つの SNA 回線争奪勝者セッションが自動的に開始することを指定します。CNO 処理が失敗したときに AVS がすべての場合に通知を受けるように、AUTOSES に非ゼロ値を提供しなければなりません。任意の2つの分散データベース・パートナー間のすべての APPC セッションを自動的に開始する必要はありません。AUTOSES 値が回線争奪勝者の限度 (DMINWNL) より小さい場合には、分散データベース・アプリケーションが必要とするまで、VTAM は残りのセッションの開始を遅らせます。

DMINWNL=10

ゲートウェイ TORGATE は、この DB2 (VM 版) システムが少なくとも10個のセッションでの回線争奪勝者であることを指定します。CNOS 処理は DMINWNL パラメーターを省略時値として使用しますが、AVS 仮想計算機から AGW CNOS コマンドを出すことによって、所定のパートナーでこれを一時変更することができます。

DMINWNR=10

ゲートウェイ TORGATE は、このパートナー・システムが少なくとも10個のセッションでの回線争奪勝者であることを指定します。CNOS 処理は DMINWNR パラメーターを省略時値として使用しますが、AVS 仮想計算機から AGW CNOS コマンドを出すことによって、指定パートナーでこれを一時変更することができます。

DSESLIM=20

ゲートウェイ TORGATE と特定のモード・グループ名のすべてのパートナー分散システムとの間に許可されているセッション (勝者と敗者の両方) の合計数は、20 です。CNOS 処理は DSESLIM パラメーターを省略時値として使用しますが、AVS 仮想計算機から AGW CNOS コマンドを出すことによって、指定パートナーでこれを一時変更することができます。パートナーが DSESLIM、DMINWNL、または DMINWNR パラメーターにより指定されたセ

セッションの数をサポートできない場合には、CNOS 処理はパートナーが受け入れ可能なこれらのパラメーターの新しい値を折衝します。

EAS=9999

この VTAM LU で必要とされるセッションの合計数の見積もり。

MODETAB=RDBMODES

VTAM モード表の名前は、RDBMODES です。この表には、このゲートウェイが他の分散データベース・パートナーと通信するために使用できるすべてのモード名が含まれています。

SECACPT=ALREADYV

これは機密保護受諾パラメーターであり、リモート・パラメーターから分散データベース要求で提示されたときにこのゲートウェイがサポートする最高の APPC 会話機密保護レベルを識別します。SECACPT=ALREADYV をお勧めします。ALREADYV オプションは以下の機密保護レベルをサポートします。

- SECURITY=NONE、機密保護情報を含めないようにする要求。DB2 (VM 版) は、この機密保護レベルを使用して DRDA 要求を拒否します。
- SECURITY=PGM、リクエスターのユーザー ID およびパスワードを含む要求。DB2 (VM 版) は、この機密保護レベルを使用して DRDA 要求を受け入れます。
- SECURITY=SAME は、リクエスターのユーザー ID だけを含む検査済みの要求を指示します。

SYNCLVL=SYNCPT

SYNCLVL パラメーターは AVS の同期サポート・レベルを指定します。SYNCPT の値は NONE、CONFIRM および SYNCPT の同期レベルがサポートされていることを示しています。AVS ゲートウェイが DB2 (VM 版) サーバーの DRDA-2 分散作業単位活動で使用される場合は、値として SYNCPT を指定してください。分散作業単位活動が行われない場合は、CONFIRM (NONE および CONFIRM がサポートされているが、SYNCPT がサポートされていない) を指定してください。

VERIFY=NONE

この DB2 (VM 版) システムで必要な SNA セッション機密保護の (パートナー LU 検査) レベルを識別します。NONE 値は、パートナー LU 検査が必要ではないことを示しています。

DB2 (VM 版) は VERIFY キーワードの選択を制限することはありませんが、実行中の VTAM バージョンはこの選択に影響を与えることがあります。信頼性に欠けるネットワークでは、DB2 (VM 版) は VERIFY=REQUIRED をコーディングすることをお勧めします。VERIFY=OPTIONAL を選択すると、VTAM はサポートを提供するパートナーにのみパートナー LU 検査を実行します。VERIFY=REQUIRED を指定すると、パートナー LU 検査を実行できないパートナーを VTAM が拒否することになります。

VPACING=2

このパラメーターは、パートナー LU とこのゲートウェイとの間で使用されるセッション歩調合わせカウントを設定します。セッション歩調合わせは、分散データベース・システムにたいへん重要です。

2. ゲートウェイを活動化します。

ゲートウェイの活動化は、DB2 (VM 版) アプリケーション・リクエスターと同じホスト (または同じ TSAF コレクションにある他のホスト) で稼働している AVS 仮想計算機から実行されます。AVS マシンのプロファイルに AGW ACTIVATE GATEWAY GLOBAL コマンドを含めるか、このコマンドを AVS マシン・コンソールから対話式に出して、AVS が開始するたびにゲートウェイが自動的に使用できるようにしてください。

3. ゲートウェイとその各パートナー LU との間のセッションの数を折衝するには、AGW CNOS コマンドを使用してください。

AVS ゲートウェイ・マシンの CP ディレクトリーでの MAXCONN 値が、必要なセッションの合計数をサポートするのに十分な大きさであることを確認してください。

AGW DEACTIVE GATEWAY コマンドを AVS 仮想計算機から出しそのゲートウェイを使用不可にします。ゲートウェイ定義はそのままになります。AGW ACTIVATE GATEWAY GLOBAL コマンドを使用すれば、この時点でゲートウェイは再び使用可能になります。

AVS コマンド形式についての詳細は、VM/ESA 接続計画、管理および操作を参照してください。

4. インストール時に VTAM NETID が DB2 (VM 版) DBMS に定義されたことを確認してください。

アプリケーション・リクエスターが存在するホスト (または同じ TSAF コレクション内の他のホスト) の NETID は、要求がネットワークに入れられるときに VTAM によって提供されます。NETID は CMS ファイル SNA NETID に保管されて、アプリケーション・リクエスターによってアクセス

される DB2 (VM 版) 実動ディスク内に存在します。アプリケーション・リクエスターはこの NETID を、会話ごとに送られる LUWID の生成に使用します。

リモート・システムの定義

VTAM が望ましいネットワーク宛先を位置指定できるような LU 名を登録することにより、リモート・システムを定義しなければなりません。AVS が開始すると、リモート・システムはグローバル・ゲートウェイ名 (LU 名) を識別します。この名前は SQL 要求を VTAM へのネットワークに経路指定するのに利用できます。インバウンド要求とアウトバウンド要求の両方が適切な LU 名に経路指定されるためには、ゲートウェイ名は、ローカル VTAM システムにより認識される LU のセット内で固有でなければなりません。これは、ユーザー・ネットワークを通してゲートウェイ名の固有性を確認する最善の方法です。これにより、VTAM 資源定義プロセスが単純になります。

DB2 (VM 版) アプリケーションがリモート・システムからデータを要求すると、DB2 (VM 版) は CMS 通信ディレクトリーでリモート・システムに関する以下の情報を検索します。

- ゲートウェイ名 (ローカル LU 名)
- リモート LU 名
- リモート TPN
- アプリケーション・サーバーで必要な会話機密保護レベル
- アプリケーション・サーバーでアプリケーション・リクエスターを識別するユーザー ID
- アプリケーション・サーバーでアプリケーション・リクエスターを許可するパスワード
- アプリケーション・サーバーと通信するために使用するセッションの特性を記述するモード名
- RDB_NAME

CMS 通信ディレクトリーは、ファイル・タイプ NAMES の CMS ファイルであり、DB2 (VM 版) システム管理者により作成および管理されます。管理者として、XEDIT を使用してこのファイルを作成し、おのおのの潜在的な DRDA パートナーを識別するために適切な項目を追加できます。ディレクトリーの各項目は、タグとそれに関連する値のセットです。151ページの図31は、項目の例を示しています。検索が実行されると、一致が見つかるかファイルの終了に達するまで、ファイルの各項目の :dbname タグ値と検索キーが比較されます。151ページの図31の例では、トロントの販売責任者は

MONTREAL_SALES データベースからデータをリモート・アクセスしてモン
トリオール支店の月別販売報告書を作成したいとします。

```
SCOMDIR NAMES A1 V 132 Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001 :nick.MTLSALES
00002 :tpn.SALES
00003 :luname.TORGATE MTLGATE
00004 :modename.BATCH
00005 :security.PGM
00006 :userid.SALESMGR
00007 :password.GREATMTH
00008 :dbname.MONTREAL_SALES
00009
```

図 31. CMS 通信ディレクトリーの項目の例

:tpn タグは、アプリケーション・サーバーを活動化するトランザクション・プログラム名を識別します。 :luname タグの最初の部分で、SNA ネットワークへのアクセスを得るために使用される AVS ゲートウェイ (ローカル LU) を識別します。2 番目の部分はリモート LU 名を識別します。:modename タグは、ローカル LU とリモート LU との間に割り当てられるセッションの特性を定義する VTAM モードを識別します。要求単位 (RU) サイズ、歩調合わせ、およびサービス・クラス (COS) はそのような特性の例です。:security タグは、アプリケーション・リクエストをアプリケーション・サーバーに接続する会話で使用する機密保護のレベルを示します。

CMS 通信ディレクトリーは、特定の VM システム内のすべてのアプリケーション・リクエストからアクセス可能な共通システム・ディスク上にあります。VTAM を介したリモート・アクセスに必要なプログラムまたは製品は、CMS 通信ディレクトリーを使用できます。

2 つのレベルの CMS 通信ディレクトリーにアクセスできます。システム・レベルおよびユーザー・レベルです。たとえば、システム・レベルのディレクトリーを、特定の VM システム内のすべてのアプリケーション・リクエストからアクセス可能な共通システム・ディスク上に作成できます。また、自分のユーザー・レベル・ディレクトリーを作成して、既存の項目を一時変更したり、システム・レベル・ディレクトリーにはない新しい項目を導入することもできます。ユーザー・レベル・ディレクトリーが最初に検索されます。検索に失敗した場合には、システム・レベル・ディレクトリーが検索されます。システム・レベル・ディレクトリーは、ユーザー・レベル・ディレクトリーの拡張です。これは、ユーザー・レベル・ディレクトリーに値が見つからない場合にのみ検索されます。

これらのディレクトリーはそれぞれ、`CMS SET COMDIR` コマンドによってアプリケーションに識別され、活動化されます。たとえば、以下のコマンド順序を使用して、システムおよびユーザー・レベル・ディレクトリー (それぞれ S および A ミニディスクにある) を識別できますが、検索にはシステム・レベル・ディレクトリーだけを活動化するよう選択します。

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S
SET COMDIR FILE USER UCOMDIR NAMES A
SET COMDIR OFF USER
```

CMS 通信ディレクトリーについては、*VM/ESA 接続計画、管理および操作* で詳細に説明されています。`CMS SET COMDIR` コマンドについては、*VM/ESA CMS コマンド解説書* で説明されています。

通信サブシステムの定義

VM 環境では、構成要素の組み合わせによって通信管理を実行します。異種 DRDA システム間の通信に関連する構成要素は、APPC/VM、CMS 通信ディレクトリー、TSAF、AVS、および VTAM です。

APPC/VM は、DB2 (VM 版) アプリケーション・リクエスターが通信サービスを要求するときに使用する LU 6.2 アセンブラー・レベルの API です。CMS 通信ディレクトリーは、分散パートナー・システムの経路指定および機密保護情報を提供します。AVS はゲートウェイを活動化し、アウトバウンド APPC/VM フローを APPC/VTAM フローに、インバウンド APPC/VTAM フローを APPC/VM フローに変換できます。

APPC/VM、TSAF、および AVS は、適切な DRDA パートナーに要求を経路指定する上で、CMS 通信ディレクトリー、VTAM、および *IDENT に依存しています。

VTAM が CMS 通信ディレクトリーで識別されるパートナー・アプリケーションと通信するためには、以下の情報を提供しなければなりません。

1. 各アプリケーション・リクエスターおよびアプリケーション・サーバーの LU 名を VTAM に定義します。リモート・システムが論理的および物理的に VTAM システムに接続されている状態により、これらの定義の配置および構文は異なります。
2. CMS 通信ディレクトリーで指定される各モード名の VTAM モード表に項目を作成します。これらの項目には、特定のモード名の要求単位 (RU) サイズ、歩調合わせサイズ、およびサービスのクラスを説明します。
3. パートナー LU 検査を使用する場合には (セッション・レベル機密保護)、検査アルゴリズムに VTAM および RACF プロファイル (または同等のもの) を提供してください。

AVS セッション限度の考慮事項: アプリケーション・リクエスターが AVS を使用してリモート・アプリケーション・サーバーと通信するときに、接続が開始されます。この接続が原因で確立されたセッション限度を超えると、セッションが利用可能になるまで、AVS は接続を保留状態に据え置きます。セッションが利用可能になると、AVS はセッションに保留の接続を割り当て、制御はユーザー・アプリケーションに戻されます。この状況を回避するため、セッション限度を増やしてさらに接続できるようにピーク時の使用を計画してください。AVS マシンの CP ディレクトリーでの MAXCONN 値が、APPC/VM 接続によるピーク時の使用をサポートするのに十分な大きさであることを確認してください。

RU サイズおよび歩調合わせの設定

VTAM モード表で定義する項目によって、要求単位 (RU) サイズおよび歩調合わせカウントを指定します。これらの値を正しく定義できていないと、すべての VTAM アプリケーションに悪影響を与える可能性があります。

要求単位 (RU) サイズ、セッション限度、および歩調合わせカウントを選択した後、これらの値が既存の SNA ネットワークに与える影響を考慮してください。新しい分散データベース・システムをインストールするときには、以下の項目を復習してください。

- VTAM CTC 接続には、MAXBFRU パラメーターが RU サイズ + 29 バイト (VTAM が SNA 要求ヘッダーおよび伝送ヘッダーに追加する分) を処理するのに十分な大きさであることを確認してください。MAXBFRU は 4K バイト単位で計測されます。それで、MAXBFRU は少なくとも 2 でなければ 4K RU に適合しません。
- NCP 接続では、MAXDATA が RU サイズ + 29 バイトを処理できる十分な大きさであることを確認してください。4K の RU サイズを指定する場合、MAXDATA は最低 4125 でなければなりません。

NCP MAXBFRU パラメーターを指定する場合には、RU サイズに 29 バイトを加えた大きさが入る値を選択してください。NCP では、MAXBFRU パラメーターによって、PIU を保持できる VTAM I/O バッファの数を定義します。IOBUF バッファ・サイズを 441 と選択する場合、 10×441 は $4096 + 29$ より大きいため、MAXBFRU=10 は 4K RU を正しく処理します。

- ご使用の分散データベースの査定する方法については、分散関係データベース体系 接続の手引き を参照してください。IOBUF プール資源を使用しすぎている場合、VTAM パフォーマンスはすべての VTAM アプリケーションで低下します。

DB2 (VM 版) アプリケーション・リクエスターの準備

DB2 (VM 版) アプリケーション・リクエスターでは、DRDA サポートがインストールされていない場合があります。以下のステップに従って、DRDA 通信用に DB2 (VM 版) アプリケーション・リクエスターを準備してください。

1. ARISDBMA exec を使用して、DRDA サポートをインストールします。
 - リクエスターとサーバーのサポートをインストールする場合、
"ARISDBMA DRDA(ARAS=Y)" を使用します。
 - リクエスターのサポートのみをインストールする場合、"ARISDBMA DRDA(AR=Y)" を使用します。

詳細については、DB2 システム管理 (VM 版) を参照してください。

2. ARISDBMA を出したあとに、DB2 (VM 版) ARISQLLD LOADLIB を再作成します。詳細については、DB2 システム管理 (VM 版) の『DRDA 環境の使用』の章を参照してください。

機密保護の提供

リモート・システムが SQL アプリケーションに代わって分散データベース処理を実行する場合には、アプリケーション・リクエスター、アプリケーション・サーバー、およびそれらに接続しているネットワークの機密保護要件を満たさなければなりません。これらの要件は、以下のカテゴリーのいくつかに分けられます。

- エンド・ユーザー名の選択
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護

エンド・ユーザー名の選択

SQL および LU 6.2 では、エンド・ユーザーには 1~8 文字のユーザー ID が割り当てられます。このユーザー ID 値は、特定のオペレーティング・システムで固有でなければなりません。SNA ネットワーク全体で固有でなければならぬわけではありません。たとえば、TORONTO システムで JONES というユーザーがいて、MONTREAL システムでまた JONES というユーザーがいてもかまいません。この 2 人のユーザーが同一の人であれば、対立は起きません。しかし、TORONTO の JONES が MONTREAL の JONES と同一人物でない場合、SNA ネットワーク (およびそのネットワークの分散データベース・システム) は、TORONTO の JONES と MONTREAL の JONES とを識別できません。この状況を避けるための処置をとらない場合には、TORONTO の JONES は MONTREAL の JONES に与えられた特権を使用できます。この逆のことも起こります。

名前の対立を解消するため、DB2 (VM 版) はエンド・ユーザー名変換のサポートを提供します。しかし、システムはユーザー ID の変換を強制しません。システム強制変換が必要な場合は、アプリケーション・サーバーで適切なインバウンド変換が実行されていることを確認しなければなりません。

アウトバウンド変換 は、CMS 通信ディレクトリーを使用して実行されます。CMS 通信ディレクトリーの項目に、:security.PGM を指定しなければなりません。この場合には、:userid および :password タグに対応する値が接続要求でのリモート・サイト (アプリケーション・サーバー) に流れます。

図32 に示されている項目を作成すると、ローカル (TORONTO) システムの JONES という ID のユーザーが MONTREAL システムの MONTREAL_SALES_DB アプリケーション・サーバーに接続したときに、ユーザー ID JONEST にマップされます。このようにして、ユーザー ID のあいまいさが解消されます。

```
UCOMDIR NAMES A1 V 132 Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001 :nick.MTLSALES
00002 :tpn.SALES
00003 :luname.TORLU MTLGATE
00004 :modename.BATCH
00005 :security.PGM
00006 :userid.JONEST
00007 :password.JONESPW
00008 :dbname.MONTREAL_SALES_DB
00009
```

図 32. アウトバウンド名前変換

ネットワーク機密保護

リモート・サイト (アプリケーション・サーバー) でアプリケーション・リクエストを表すエンド・ユーザー名を選択した場合、アプリケーション・リクエストは、必要な LU 6.2 ネットワーク機密保護情報を提供しなければなりません。LU 6.2 は、主に 3 つのネットワーク機密保護機構を提供します。

- セッション・レベル機密保護。VTAM APPL ステートメントに VERIFY パラメーターを使用して指定されます。
- 会話レベル機密保護、CMS 通信ディレクトリーで指定されます。
- 暗号化。

アプリケーション・サーバーにはデータベース資源を管理する責任があるので、アプリケーション・サーバーは、どのネットワーク機密保護メカニズムをアプリケーション・リクエストが提供しなければならないかを指示します。

:security タグに適切な値を設定して、アプリケーション・リクエスターの通信ディレクトリーにアプリケーション・サーバーの機密保護要件を記録しなければなりません。

DRDA によりサポートされる SNA 会話レベル機密保護オプションは、以下のとおりです。

SECURITY=SAME

これは、検査済みの機密保護としても知られています。それは、エンド・ユーザーの ID (ログオン ID) だけがリモート・システムに送信されるためです。パスワードは送信されません。このレベルの会話機密保護は、アプリケーション・サーバー用にアプリケーション・リクエスターの通信ディレクトリーで :security.SAME が指定された場合に、使用されます。このオプションが使用されているときには、アウトバウンド・エンド・ユーザー名変換は実行されません。リモート DRDA サイトに送信されるユーザー ID は、CMS ユーザーのログオン ID です。CMS 通信ディレクトリーの :userid タグは、:security.SAME では無視されます。

SECURITY=PGM

このオプションを使用すると、エンド・ユーザー ID とパスワードの両方が妥当性検査のためにリモート・システム (アプリケーション・サーバー) に送信されます。この機密保護オプションは、アプリケーション・リクエスターの CMS 通信ディレクトリー項目に :security.PGM が指定されるときに使用されます。このオプションが使用されているときには、アウトバウンド・エンド・ユーザー名変換が実行されます。

DB2 (VM 版) は、パスワード暗号化をサポートしません。このパスワードは :password タグに指定することもできますし、エンド・ユーザーの CP ディレクトリー項目に APPCPASS ディレクトリー・ステートメントを使用して保管することもできます。パスワードの機密保護を最高にしたい場合には、APPCPASS ステートメントをお勧めします。パスワードが CMS 通信ディレクトリー項目に指定されていない場合、ユーザーのシステム (VM) ディレクトリーで APPCPASS ステートメントが探索されます。

APPCPASS ステートメント: VM で提供される APPCPASS ステートメントは、アプリケーション・リクエスターがアプリケーション・サーバーへの接続に使用するユーザー ID およびパスワードの機密保護を最大にします。以下のいずれかの方法で機密保護情報を保管できるという点で、APPCPASS には柔軟性があります。

- **ユーザー ID およびパスワード。**この場合、CMS 通信ディレクトリーの :userid および :password タグがブランクに設定されていなければなりません。
- **ユーザー ID のみ。**この場合、CMS 通信ディレクトリーの :userid タグはブランクに設定されていなければならず、 :password タグにはユーザーのパスワードが設定されていなければなりません。
- **パスワードのみ。**この場合、CMS 通信ディレクトリーの :password タグはブランクに設定されていなければならず、 :userid タグにはユーザーの ID が設定されていなければなりません。

図33 では、ユーザー ID がユーザーの通信ディレクトリーに保管されており、パスワードがユーザーの VM ディレクトリー項目に保管されている場合の例を示しています。通信ディレクトリー項目では、ユーザー ID は MTLSSOU に設定されていますが、パスワードは設定されていません。パスワードは、ユーザーの VM ディレクトリー項目に保管されています。

```
UCOMDIR NAMES AI V 132 Trunc=132 Size=8 Line=1 Col=1 Alt=8
====>
00001 :nick.MTLSSALES
00002 :tpn.SALES
00003 :luname.TORGATE MTLGATE
00004 :modename.BATCH
00005 :security.PGM
00006 :userid.MTLSSOU
00007 :password.
00008 :dbname.MONTREAL_SALES_DB
00009
```

図 33. パスワードなしの通信ディレクトリー項目の例

APPC/VM がアプリケーション・リクエストとアプリケーション・サーバーとの間の接続を会話 SECURITY=PGM を使用して開始するとき、 :userid および :password タグの値が読み取られてアプリケーション・サーバーに渡されます。これらのタグの一方または両方がブランクに設定されている場合には、ユーザーの VM ディレクトリー項目で欠落情報を探索します。この場合、以下のように VM ディレクトリー項目に APPCPASS ステートメントがなければなりません。

```
APPCPASS TORGATE MTLGATE MTLSSOU Q6VBN8XP
```

このステートメントは APPC/VM に、(ローカルの) AVS ゲートウェイ TORGATE を介して接続を要求しているユーザー (アプリケーション・リクエスト)、 MTLGATE という名前のパートナー LU、およびユーザー ID

MTLSOU がパスワード Q6VBN8XP をアプリケーション・サーバーに送る必要があることを伝えます。このユーザーは、アプリケーション・サーバーで 2 つの識別子で識別されます。

VM ディレクトリーに APPCPASS ステートメントを配置することは、エンド・ユーザーのタスクではありません。エンド・ユーザーは、これを実行するように VM システム・プログラマーに要求しなければなりません。

会話レベル機密保護および APPCPASS ステートメントについての詳細は、*VM/ESA 接続計画、管理および操作* を参照してください。

データベース・マネージャー機密保護

DRDA 内の全体的な分散データベース機密保護フレームワークの一部として、アプリケーション・リクエスターはどのエンド・ユーザーに分散データベース要求を出すことを許可するかを制御する役割を果たします。DB2 (VM 版) では、アプリケーション・リクエスターは以下の 3 つの方法で分散データベースの機密保護に貢献します。

アウトバウンド・ユーザー名変換

アウトバウンド・ユーザー名変換を使用すると、要求しているエンド・ユーザーの ID にしたがって、特定のアプリケーション・サーバーへのアクセスを制御できます。DB2 (VM 版) は、リモート・サイトに要求を送信する前にエンド・ユーザーの名前を変換しようとします。ただし、VM アプリケーション・リクエスターのユーザーが CMS ユーザー通信ディレクトリーを使用してアウトバウンド変換を上書きする可能性があるため、最良の方法は、アプリケーション・サーバーが come-from 検査およびインバウンド変換を行うようにすることです。

アプリケーション・プリプロセス

エンド・ユーザーは、特定のアプリケーション・サーバーへのリモート・アプリケーションをプリプロセスします。これは、DB2 (VM 版) の SQLPREP EXEC またはデータベース・サービス・ユーティリティー (DBSU) RELOAD PACKAGE コマンドを使用して行います。DB2 (VM 版) は、これらのサービスの使用を制限しません。エンド・ユーザーがアプリケーションをプリプロセスするとき、そのユーザーが結果のパッケージを所有します。

アプリケーション実行

DB2 (VM 版) エンド・ユーザーがリモート・アプリケーションを実行するには、特定のアプリケーションに関連したリモート・パッケージを実行するためにエンド・ユーザーにリモート・サイト (アプリケーション・サーバー) での権限がなければなりません。パッケージの作成者

(所有者) には、パッケージを実行する権限が自動的に与えられます。他のエンド・ユーザーは、DB2 (VM 版) GRANT EXECUTE ステートメントでパッケージを実行する権限を得られます。このようにして、分散データベース・アプリケーションの所有者は個々のユーザー・ベースでアプリケーションの使用を制御できます。

機密保護サブシステム

VM システムの外部機密保護サブシステムは RACF か、RACF と互換性のあるインターフェースを備えた同等の製品のいずれかにより提供されます。DB2 (VM 版) アプリケーション・リクエスターは外部機密保護サブシステムと直接やり取りしません。外部機密保護サブシステムは、会話レベル機密保護のパスワードを提供するためには使用されません。セッション・レベル機密保護を使用することを選択すると、VTAM により外部機密保護サブシステムが呼び出されてパートナー LU の検証中にリモート LU 名の ID が妥当性検査されます。

データの表示

アプリケーション・リクエスターには、適切な省略時 CHARNAME および CCSID 値がなければなりません。適切な値を選択すると、文字データ表記の安全性が確保され、CCSID 会話に関連するパフォーマンス・オーバーヘッドを減少させます。

たとえば、ご使用の DB2 (VM 版) アプリケーション・リクエスターがコード・ページ 37 および米国英語の文字セット 697(CP/CS 37/697) で生成された場合、アプリケーション・リクエスターは省略時 CHARNAME を ENGLISH に設定しなければなりません。CP/CS 37/697 が 37 の CCSID に対応し、これは ENGLISH の CHARNAME に対応するからです。

新しくインストールされたか移行されたシステムの省略時 CHARNAME は INTERNATIONAL であり、CCSID は 500 です。これはおそらく、ご使用のインストール・システムでは正しくないでしょう。現行の省略時 CCSID の値を表示するには、以下のコマンドを使用してください。

SQLINIT QUERY

アプリケーション・リクエスターでは適切な CCSID でも、アプリケーション・サーバーの変換テーブルにはサポートされていない場合があります。この場合には、以下のいずれかを実行して接続を確立できます。

- アプリケーション・サーバーが CCSID 変換テーブルを更新するようにして、アプリケーション・リクエスターの省略時 CCSID とアプリケーション・サーバーの省略時 CCSID との変換をサポートするようにします

(CCSID 変換サポートの追加方法についての詳細は、アプリケーション・サーバー製品の資料を参照してください)。

- アプリケーション・リクエスターの省略時 CCSID を、アプリケーション・サーバーによりサポートされるものに変更する。これが原因でデータ保全性の問題が発生することがあるため、結果に注意を払う必要があります。このような結果の例を、以下に示します。

アプリケーション・リクエスターは、CP/CS 37/697 で定義された制御プログラムを使用します。アプリケーション・サーバーは CCSID 37 からの変換をサポートしませんが、CCSID 285 (これは SQL/DS 用の CHARNAME UK-ENGLISH です) からの変換はサポートしています。

アプリケーション・リクエスターが変更されて UK-ENGLISH の省略時 CHARNAME (そして CCSID は 285) を使用するようになると、データの保全性は保たれません。たとえば、アプリケーション・サーバーで英国ポンド記号 (£) が表示される場所では、アプリケーション・リクエスターはドル記号 (\$) を表示します。他の文字も異なる場合があります。

DB2 (VM 版) アプリケーション・リクエスターの CCSID 値を変更するには、SQLINIT EXEC の CHARNAME パラメーターを指定しなければなりません。詳細については、DB2 システム管理 (VM 版) を参照してください。

アプリケーション・サーバーでは適切な CCSID 値でも、アプリケーション・リクエスターの変換テーブルにはサポートされていない場合があります。この場合には、以下のいずれかを実行して接続を確立できます。

- アプリケーション・リクエスターにより使用される変換テーブルを更新して、アプリケーション・サーバーの省略時 CCSID とアプリケーション・リクエスターの省略時 CCSID との間の変換をサポートするようにします。SYSTEM.SYSSTRINGS システム表を更新する方法については、DB2 システム管理 (VM 版) を参照してください。この表を使用して CMS ファイル ARISSTR MACRO を作成します。このファイルは、CCSID 変換サポート用にアプリケーション・リクエスターで使用されます。
- アプリケーション・サーバーがその省略時 CCSID を変更するようにします。これは、アプリケーション・サーバーの省略時 CCSID を選択する場合の影響を考慮して適切な場合にだけ実行してください。アプリケーション・サーバーの省略時 CCSID は、それに接続しているすべてのアプリケーション・リクエスター、アプリケーション・サーバーで使用されている操作員端末、およびアプリケーション・サーバーで表に保管されているデータに影響を与えます。

DB2 (VM 版) DRDA アプリケーション・リクエスターを使用可能にするためのチェックリスト

以下のチェックリストは DRDA 通信用の DRDA アプリケーション・リクエスターを使用可能にするためのステップを要約したものです。初めに次のような前提事項があります。まず、VM システムがテレプロセッシング・アクセス方式として ACF/VTAM を使用してインストールされていること、そして、リモート・システムとの通信に必要な VTAM 定義 (NCP 定義など) がすでに完了していることです。

1. ローカル AVS ゲートウェイを VTAM に定義する。
2. ARISDBMA exec を使用して、DRDA サポートを DB2 (VM 版) アプリケーション・リクエスターにインストールする。
3. CMS 通信ディレクトリーを設定して、必要な APPCPASS ステートメントをアプリケーション VM マシンの VM ディレクトリーに追加する。SET COMDIR CMS コマンドを使用して、通信ディレクトリーを使用可能にします。
4. VTAM および AVS を始動して、VM アプリケーションが SNA ネットワークを介してリモート通信できるようにする。
5. SQLINIT exec を出して、DBNAME、PROTOCOL および CHARNAME パラメーターを指定します。これらのパラメーターは省略時データベース、使用しているプロトコルおよび CCSID を示しています。
6. リモート・サーバーでアプリケーションを準備する。

VM 環境でのアプリケーション・サーバーのセットアップ

DB2 (VM 版) のアプリケーション・サポートによって、DB2 (VM 版) は DRDA アプリケーション・リクエスターのサーバーとして機能することができます。DB2 (VM 版) アプリケーション・サーバーに接続されているアプリケーション・リクエスターは以下のいずれかです。

- DB2 (VM 版) リクエスター。
- DB2 ユニバーサル・データベース (OS/390 版) リクエスター。
- OS/400 リクエスター。
- DB2 (AIX 版) リクエスター。
- DB2 ファミリー・アプリケーション (DB2 コネクトを含む)、または DRDA アプリケーション・リクエスター・プロトコルをサポートする他の製品は、DB2 (VM 版) アプリケーション・サーバーと接続することができます。

DB2 (VM 版) アプリケーション・サーバーに接続しているアプリケーション・リクエスターでは、DB2 (VM 版) アプリケーション・サーバーによって、DB2 (VM 版) アプリケーション・サーバーにローカルで保管されているデータベース・オブジェクト (表など) にアクセスできます。アプリケーション・リクエスターは、接続が確立される前に、アプリケーションの SQL ステートメントが含まれるパッケージを、DB2 (VM 版) アプリケーション・サーバーに作成しなければなりません。

DB2 (VM 版) アプリケーション・サーバーが分散データベース要求を処理するためには、以下のステップを行ってください。

1. アプリケーション・サーバーをローカル通信サブシステムに定義する。
2. 必要な機密保護を提供する。
3. データ表示を提供する。

ネットワーク情報の提供

アプリケーション・サーバーを定義する

アプリケーション・サーバーが分散データベース要求を受信するためには、アプリケーション・サーバーをローカル通信サブシステムに定義し、固有の RDB_NAME 名を割り当てます。

以下のステップを実行して、アプリケーション・サーバーを定義してください。

1. DB2 (VM 版) アプリケーション・サーバーを SNA ネットワークに定義する。DB2 (VM 版) アプリケーション・サーバーにゲートウェイ名および RDB_NAME を選択した後に、145ページの『ネットワーク情報の提供』で説明されている手順に従ってください。DB2 (VM 版) に対して選択する RDB_NAME は、DB2 (VM 版) アプリケーション・サーバーへの接続が必要なすべてのユーザー (アプリケーション・リクエスター) に提供されていなければなりません。

NETID は始動パラメーターとして VTAM に定義されており、アプリケーション・リクエスターからのすべての分散要求は正確にこのパラメーターに経路指定されます。DB2 (VM 版) アプリケーション・サーバーは NETID を設定しません。

DB2 (VM 版) アプリケーション・サーバーは、アプリケーション・リクエスターからのインバウンド分散要求を経路指定するゲートウェイを判別しません。アプリケーション・リクエスターが常にそれを制御します。DB2 (VM 版) アプリケーション・リクエスターの場合、CMS 通信ディレクターが :luname および :tpn タグを使用してそれを指定します。

DB2 (VM 版) アプリケーション・サーバーが分散作業単位活動をサポートするために、アプリケーション・リクエスターは、SYNCLVL=SYNCPT パラメーターを使用して VTAM に定義されている AVS ゲートウェイを選択していなければなりません。必ず AVS ゲートウェイを定義して、分散作業単位をサポートするようにしてください。

2. CRR 回復サーバーを作成します。これは、VM システムで DB2 (VM 版) アプリケーション・サーバーの分散作業単位を管理するために使用されます。これを行うために、VM/ESA 導入の手引きで説明されている IBM 提供のサーバーおよびファイルのインストール後のロードを行ってください。このステップには、CRR サーバー (VMSERVER) および CRR ファイル・プール (VMSYSR) を定義することも含まれます。CRR 回復サーバーを開始した時に、LUNAME を指定してください。これは SYNCLVL=SYNCPT が指定される AVS ゲートウェイの名前と同じです。
3. アプリケーション・サーバー・マシンの CP ディレクトリーに IUCV *IDENT ステートメントがあることを確認してください。これは、サーバーをグローバル資源として識別します。
4. アプリケーション・リクエスターが要求する各モード名ごとに、VTAM モード名表に項目を作成します。これらの項目には、特定のモード名のセッション特性 (RU サイズなど)、歩調合わせカウント、およびサービス・クラスを記述します。
5. DB2 (VM 版) アプリケーション・サーバーに接続するアプリケーション・リクエスターにセッション限度を定義します。VTAM APPL ステートメントは、すべてのパートナー・システムに省略時セッション制限を定義します。特定のパートナーの固有の省略時値を確立するには、アプリケーション・サーバー・サイトで稼働している AVS 仮想計算機から AGW CNOS コマンドを使用してください。(セッション限度は、通常アプリケーション・リクエスターにより要求されます。)
RU サイズ、セッション限度、および歩調合わせカウントを選択した後は、VTAM IOBUF プールに与えるこれらの値の影響を考慮してください。

サーバー名の RESID へのマッピング: 資源 ID (RESID) は、トランザクション・プログラム名の VM 用語です。VM 環境では、これは一般に 8 バイト以下の長さの英数字名で定義されます。管理を簡潔にするために、通常は RESID をサーバー名と同一にして定義します。164ページの図34に、RESID 名前ファイルの例を示します。

```

RESID NAMES A1 V 132 Trunc=132 Size=4 Line=1 Col=1 Alt=3
====>
00001 :nick.MTLTPN
00002 :dbname.MONTREAL_SALES_DB
00003 :resid.SALES
00004

```

図 34. RESID 名前ファイルの例

この `dbname` および `RESID` を (TPN として) 定義する通信ディレクトリー項目についての詳細は、157ページの図33を参照してください。アプリケーション・サーバー名を `RESID` と同じにできない場合、DB2 (VM 版) アプリケーション・サーバーは `RESID NAMES` を使用して、マッピングを行います。このマッピングは、以下の場合に必要です。

- サーバー名と異なる `RESID` を使用する。
- 8 バイトより長いサーバー名を使用する。
- 4 バイト 16 進値 (省略時 `DRDA TPN X'07F6C4C2'` など) を使って `RESID` を使用する。

インストール時には、省略時解釈では `SQLDBINS EXEC` で指定されたサーバー名を `RESID` として使用します。`RESID NAMES` ファイルにマッピング項目を作成するには、`SQLDBINS` に `RESID` パラメーターを指定します。

`SQLSTART DB(server_name)` を使用してデータベースを開始する場合、DB2 (VM 版) は対応する `RESID` を見つけて、これが VM の制御対象の資源であるということを VM に伝えます。項目が `RESID NAMES` ファイルに見つからない場合には、DB2 (VM 版) は `RESID` がサーバー名と同一であると想定して、VM にそのように伝えます。詳細については、*DB2 システム管理 (VM 版)* を参照してください。

DB2 (VM 版) アプリケーション・サーバーの準備および開始

DB2 (VM 版) アプリケーション・サーバーが、DRDA サポートをインストールしていない場合があります。以下のステップに従って、DRDA 通信用に DB2 (VM 版) アプリケーション・サーバーを準備します。

1. `ARISDBMA exec` を使用して、DRDA サポートをインストールします。
 - リクエスターとサーバーのサポートをインストールする場合、`"ARISDBMA DRDA(ARAS=Y)"` を使用します。
 - サーバーのみのサポートをインストールする場合、`"ARISDBMA DRDA(AS=Y)"` を使用します。

詳細については、*VM/ESA System Administration* を参照してください。

2. ARISDBMA を出したあとに、DB2 (VM 版) ARISQLLD LOADLIB を再作成します。詳細については、DB2 システム管理 (VM 版) の『DRDA 環境の使用』の章を参照してください。

機密保護の提供

アプリケーション・リクエスターが分散データベース要求を DB2 (VM 版) アプリケーション・サーバーに向けるときには、以下の機密保護上の考慮事項が関係します。

- インバウンド・エンド・ユーザー名前変換
- ネットワーク機密保護パラメーター
- データベース・マネージャー機密保護
- 外部機密保護サブシステムによって課される機密保護

エンド・ユーザー名

SQL および LU 6.2 では、エンド・ユーザーには 1~8 バイトのユーザー ID が割り当てられます。このユーザー ID は特定のオペレーティング・システムでは固有でなければなりません、SNA ネットワーク全体で固有である必要はありません。命名の対立を解消するため、DB2 (VM 版) は AVS により提供されたユーザー ID 変換機能を任意選択で使用できます。このとき、以下の条件を満たしていなければなりません。

- DB2 (VM 版) アプリケーション・サーバーは、VM/ESA 環境で実行してください。
- インバウンド接続要求が AVS ゲートウェイを介して経路指定されていること。
- パートナー・アプリケーション・リクエスターは、会話 SECURITY=SAME (SNA 用語で検査済み ともいう) を使用しなければなりません。

SECURITY=SAME オプションを使用して AVS を介して接続が経路指定される場合、AVS ユーザー ID 変換が必要になります。AGW ADD USERID コマンドは、AVS マシンから出されますが、特定のリモート LU または AVS ゲートウェイから接続しているユーザーへの機密保護許可を提供しなければなりません。マッピングが、SECURITY=SAME を使用して接続するすべてのインバウンド LU およびユーザー ID に対して存在しなければなりません。コマンドには柔軟性があり、すべてのユーザー ID を特定の LU から受け入れることも、すべてのリモート LU から包括的に受け入れることもできます。あるいは、特定の LU から特定のセットのユーザー ID だけを受け入れることもできます。

AGW ADD USERID コマンドを使用してインバウンド (検査済み) ユーザー ID をローカル AVS マシンで許可した場合は、妥当性検査はホストにより実行されません。つまり、権限を受けた ID はホストになければならないわけではなく、いずれにしても接続は受け入れられます。

現行の AVS ユーザー ID 許可は以下の 2 つの方法で変更できます。

- AGW STOP コマンドを使用して、AVS を停止します。これにより、ユーザー ID 許可を全体的に白紙に戻します。
- AGW DELETE USERID コマンドを使用して、ユーザー ID を削除します。

たとえば、異なる都市の同一のユーザー ID を例にして、AVS 変換機能が名前の対立を解決する方法を示します。トロントのシステムに JONES という ID のユーザーがおり、モントリオールのシステムにも同一の ID のユーザーがいるとします。モントリオールの JONES が、トロントのシステムにあるデータにアクセスしたい場合、トロントのシステムの以下のアクションによって命名の対立を解消し、モントリオールの JONES がトロントの JONES に授与された特権を使用しないようにします。

1. AVS 操作員は AGW ADD USERID コマンドを使用して、モントリオールのユーザーの ID をローカル・ユーザー ID に変換しなければなりません。たとえば、操作員が AGW ADD USERID MTLGATE JONES MONTJON を出すと、モントリオールのユーザーはトロントのシステムでは MONTJON として認識されます。モントリオールの他のすべてのユーザーが接続 (リモート LU MTLGATE を介した接続) を許可されており、さらにローカルではリモート・ユーザー ID で認識されている場合には、操作員はコマンド AGW ADD USERID MTLGATE * = を出さなければなりません。これらの AVS コマンドを AVS プロファイルに追加して、AVS が始動したときに自動的に実行できるようにすることもできます。
2. DBA は DB2 (VM 版) GRANT コマンドを使用して、変換されたユーザー ID (この特定のケースでは MONTJON) に対して特権のセットを授与しなければなりません。

これらの処置はモントリオールのシステムでも実行でき、トロントの JONES がモントリオールのシステムのリモート・データにアクセスするときに、モントリオールの JONES に授与された特権を使用しないようにすることができます。

ユーザー ID 変換をサポートする AVS コマンドは、*VM/ESA 接続計画*、*管理および操作* で説明されています。

ネットワーク機密保護

LU 6.2 は、主に 3 つのネットワーク機密保護機能を提供します。

- セッション・レベル機密保護
- 会話レベル機密保護
- 暗号化

DB2 (VM 版) のセッション・レベル機密保護を指定する方法についての詳細は、155ページの『ネットワーク機密保護』を参照してください。DB2 (VM 版) アプリケーション・サーバーは DB2 (VM 版) アプリケーション・リクエストと同様の方法で、セッション・レベル機密保護を使用します。

アプリケーション・リクエストは、検査済みユーザー ID (SECURITY=SAME) またはユーザー ID とパスワード (SECURITY=PGM) のいずれかを送信できます。ユーザー ID とパスワードが送信された場合、CP、RACF、または同等のものがこれらをアプリケーション・サーバー・ホストの VM ディレクトリーによって検査します。妥当性検査に失敗すると、接続要求が拒否されます。そうでなければ、受け入れられます。要求にユーザー ID しか含まれていない場合、DB2 (VM 版) はユーザー ID の妥当性検査をしないで要求を受け入れます。

注: VM/ESA は暗号化をサポートしないため、DB2 (VM 版) は暗号化機能を提供しません。

データベース・マネージャー機密保護

DB2 (VM 版) アプリケーション・サーバーは、VM から受け取ったユーザー ID にデータベースへアクセスする CONNECT 権限があるかどうかを検査し、この権限がない場合には接続を拒否します。

データベース資源の所有者として、DB2 (VM 版) アプリケーション・サーバーは、そこにある SQL オブジェクトに対してデータベース機密保護機能を制御します。DB2 (VM 版) により制御されるオブジェクトへのアクセスは特権のセットを使用して制御されます。この特権は、DB2 (VM 版) システム管理者または特定のオブジェクトの所有者により授与されます。DB2 (VM 版) アプリケーション・サーバーは、2 つのクラスのオブジェクトを制御します。

- **パッケージ:** 個々のエンド・ユーザーは、DB2 (VM 版) GRANT ステートメントを使用して、パッケージの作成、置換、実行を行う権限を持っています。ユーザーがパッケージを作成するとき、そのユーザーはパッケージを実行または置換するように自動的に許可されます。他のエンド・ユーザーは GRANT EXECUTE ステートメントを使用して、DB2 (VM 版) アプリケーション・サーバーでパッケージを実行するように個々に許可を受けなければな

りません。RUN 特権は、個々のエンド・ユーザーまたは PUBLIC に授与することができます。PUBLIC は、パッケージの実行をすべてのエンド・ユーザーに許します。

アプリケーションが DB2 (VM 版) でプリプロセスされる時は、パッケージにはアプリケーション・プログラムにある SQL ステートメントが含まれています。これらの SQL ステートメントは以下のように分けられます。

- **静的 SQL:** これは、SQL ステートメントおよびそのステートメントにより参照される SQL オブジェクトが、アプリケーションのプリプロセス時に認識されることを意味します。パッケージの作成者は、パッケージ内のそれぞれの静的 SQL ステートメントを実行する権限を持っていない限りなりません。

エンド・ユーザーがパッケージを実行する特権を与えられるとき、そのエンド・ユーザーはパッケージに含まれる各静的 SQL ステートメントを実行する権限を自動的に持ちます。それで、パッケージに静的 SQL ステートメントしか含まれていない場合には、エンド・ユーザーには DB2 (VM 版) 表特権の必要はありません。

- **動的 SQL:** パッケージが実行するまで認識されない SQL ステートメントのことです。SQL ステートメントはプログラムにより作成され、SQL PREPARE ステートメントまたは EXECUTE IMMEDIATE ステートメントを使用して、動的に DB2 (VM 版) にプリプロセスされます。エンド・ユーザーが動的 SQL ステートメントを実行するとき、そのユーザーには SQL ステートメントを実行するために必要な表特権がなければなりません。パッケージが作成されるときに SQL ステートメントが認識されないため、エンド・ユーザーにはパッケージ所有者により必要な権限が自動的に与えられません。

- **SQL オブジェクト:** 表、視点、および同義語のことです。DB2 (VM 版) ユーザーには、個々の SQL オブジェクトを作成、削除、変更、または読み取る権限の各種のレベルを授与できます。この権限は、静的 SQL ステートメントをプリプロセスしたり、動的 SQL ステートメントを実行するために必要です。

機密保護サブシステム

DB2 (VM 版) アプリケーション・サーバーによるこのサブシステムの使用は、任意選択です。アプリケーション・サーバーがアプリケーション・リクエスト LU 名の識別項目を検査する必要がある場合には、VTAM が機密保護サブシステムを呼び出してパートナー LU 検査交換を実行するようにします。DB2 (VM 版) アプリケーション・サーバーがインバウンド分散データベース要求を受信するために使用するゲートウェイの VTAM APPL ステートメント

の VERIFY パラメーターで指定されている値にしたがって、パートナー LU 検査を実行するかどうかが決まります。

機密保護サブシステムを CP によって呼び出して、アプリケーション・リクエスターから送信されたユーザー ID およびパスワードを妥当性検査することもできます。機密保護サブシステムが RACF であり RACF システム・プロファイルがない場合は、妥当性検査は RACF により実行されます。RACF システム・プロファイル (たとえば RACFPROF) がある場合、以下の指示に従って RACF からこの妥当性検査を要求してください。

```
RALTER VMXEVENT RACFPROF DELMEM (APPCPWL/NOCTL
RALTER VMXEVENT RACFPROF ADDMEM (APPCPWL/CTL
SETEVENT REFRESH RACFPROF
```

データの表示

インストールには、最も適切な省略時 CHARNAME および CCSID を選択しなければなりません。最も適切な値を使用すると、文字データ表記の保全性を確保し、CCSID 会話に関連したパフォーマンス・オーバーヘッドを減少させます。

たとえば、ご使用の DB2 (VM 版) アプリケーション・サーバーが、端末制御機構がコード・ページ 37 および米国英語の文字セット 697(CP/CS 37/697) で生成されるローカル・ユーザーにのみアクセスされる場合は、アプリケーション・サーバーの省略時 CHARNAME を ENGLISH に設定してください。CP/CS 37/697 が 37 の CCSID 対応し、これは ENGLISH の CHARNAME に対応するからです。

不必要な CCSID 変換を減らすため、アプリケーション・サーバーの省略時 CCSID を、アプリケーション・サーバーに最も頻繁にアクセスするアプリケーション・リクエスターの CCSID と同じにするように選択してください。

これら 2 つの目標が対立する場合の例を次に示します。

- アプリケーション・サーバーに、5 つ未満のローカル (VM アプリケーション・リクエスターでは、プロトコル・パラメーターは SQL/DS に設定される) のアプリケーション・リクエスターがあり、アプリケーション・サーバーに DRDA プロトコルを使用してアクセスする数多くの (100 ほどの) アプリケーション・リクエスターがあるとします。ローカルのアプリケーション・リクエスターには、CP/CS 37/697 で定義されたコントローラーがあります。リモートのアプリケーション・リクエスターは、CCSID 285 を使用します。

アプリケーション・サーバーの省略時 CHARNAME が ENGLISH に設定されている場合には、これによりローカル・アプリケーション・リクエストのデータ安全性が保持されますが、CCSID 変換オーバーヘッドがすべてのリモート・アプリケーション・リクエストに及びます。

アプリケーション・サーバー省略時 CHARNAME が UK-ENGLISH に設定されている場合、すべてのリモート・アプリケーション・リクエストが CCSID 変換オーバーヘッドによって損害を受けることを避けることができます。しかし、ローカル・アプリケーション・リクエストでデータ安全性の問題 (ある文字がローカル・アプリケーション・リクエストで表示されない) が生じます。たとえば、英国ポンド記号はドル記号として表示されません。

システムの現行の CCSID を表示するには、SYSTEM.SYSOPTIONS 表を照会します。アプリケーション・サーバーの省略時 CCSID は、通常 CCSIDMIXED の値です。この値がゼロの場合、システムの省略時 CCSID は CCSIDSBBCS の値です。この表の CHARNAME、CCSIDSBBCS、CCSIDMIXED、および CCSIDGRAPHIC 値は、データベースが開始されるたびに、システム省略時値として使用されている値に更新されます。この表の値は、常にシステム省略時値とは限りません。勧められていませんが、DBA 権限のあるユーザーが、これらの値を変更した可能性があります。アプリケーション・サーバーの省略時 CCSID を変更するには、アプリケーション・サーバーが次に始動するときに、SQLSTART EXEC の CHARNAME パラメーターを指定しなければなりません。詳細については、*VM/ESA System Administration* を参照してください。

新しくインストールされたデータベースでは、アプリケーション・サーバーの省略時 CHARNAME は INTERNATIONAL であり、アプリケーション・サーバーの省略時 CCSID は 500 です。これはおそらく、ご使用のシステムでは正しくないでしょう。移行システムの省略時 CHARNAME は ENGLISH であり、省略時 CCSID は 37 です。

DB2 (VM 版) DRDA アプリケーション・サーバーを使用可能にするためのチェックリスト

以下のチェックリストは DRDA 通信用の DRDA アプリケーション・サーバーを使用可能にするためのステップを要約したものです。初めに次のような前提事項があります。まず、VM システムがテレプロセッシング・アクセス方式として ACF/VTAM を使用してインストールされていること、そして、リモート・システムとの通信に必要な VTAM 定義 (NCP 定義など) がすでに完了していることです。

1. ローカル AVS ゲートウェイを VTAM に定義する。
2. CRR 回復サーバーを作成する。CRR 回復サーバーが指定する LUNAME が、SYNCLVL=SYNCPNT 会話を処理する AVS ゲートウェイの名前と必ず一致するようにしてください。
3. ARISDBMA exec を使用して、DRDA サポートを DB2 (VM 版) アプリケーション・サーバーにインストールする。
4. IUCV *IDENT ステートメントを VM サーバー・マシンの CP ディレクトリーに追加して、グローバル資源として識別できるようにする。
5. ローカル・ユーザー ID およびパスワードを、リモート・アプリケーション・リクエスターが使用する CP に定義する。必要な場合、AVS AGW ADD USERID コマンドを使用して、リモート・ユーザー ID をローカル VM ユーザー ID にマップしてください。
6. アプリケーション・リクエスターが要求する各モードごとに、VTAM モード名表に項目を作成する。
7. VTAM および AVS を始動して、VM アプリケーションが SNA ネットワークを介してリモート通信できるようにする。
8. アプリケーション・リクエスターがあるすべてのパートナー・システムにセッション限度を設定する。
9. DBNAME、PROTOCOL および SYNCPNT パラメーターを入力して、DB2 (VM 版) アプリケーション・サーバーを始動する。データベース・マネージャーが始動している場合、そのデータベース・マネージャーは必ず GLOBAL として識別されるようにしてください。
10. DB2 (VM 版) アプリケーション・サーバーにアプリケーションを準備する。

DB2 (VSE 版) 概説

VSE/ESA 操作環境では、DB2 (VSE 版) は DRDA 環境でアプリケーション・サーバー機能を提供します。アプリケーション・リクエスター機能は提供されていません。分散データベース処理に関する各種の DB2 (VSE 版) および VSE の構成要素について、この節で説明します。これらの構成要素を使用すると、DB2 (VSE 版) データベース管理システムは、SNA ネットワークでリモート DRDA アプリケーション・リクエスターと通信できます。

CICS(ISC)

顧客情報管理システム (CICS) システム間通信の構成要素は、DB2 (VSE 版) アプリケーション・サーバーに SNA LU 6.2 (APPC) 機能を提供します。

CICS(SPM)

CICS 同期点マネージメントの構成要素は、DB2 (VSE 版) 分散作業単位サポートには不可欠です。CICS 同期点マネージメントの構成要素は、同期点参加プログラムとして動作し、VSE/ESA システムで 2 フェーズ・コミット活動の調整を担当します。

CICS(TRUE)

CICS タスク関連ユーザー出口は、CICS 同期点管理プログラムを使用したインターフェースへの AXE トランザクションによって使用される、インターフェースです。

ACF/VTAM

CICS(ISC) は、リモート・システムを使用して、LU から LU へのセッションの設定およびバインドを行います。DB2 (VSE 版) は LU 6.2 基本会話をこれらのセッションで使用してリモート DRDA アプリケーション・リクエスターと通信します。

AXE APPC-XPCC-交換トランザクションは、リモート DRDA アプリケーション・リクエスターにより活動化される CICS トランザクションです。これは、CICS LU 6.2 サポートおよび VSE XPCC 機能を使用して、リモート・アプリケーション・リクエスターと DB2 (VSE 版) アプリケーション・サーバーとの間の DRDA データ・ストリームを経路指定します。

DBNAME ディレクトリー

DBNAME (データベース名) ディレクトリーは、会話の割り当て用の着信要求を、着信 TPN により識別される判別済みのアプリケーション・サーバーにマップします。詳細は、*SQL/DS システム管理 (VSE)* を参照してください。

XPCC 区画間通信制御は、VSE 区画間のデータ転送を提供する VSE マクロ・インターフェースです。

アプリケーション・サーバー通信フローの例

173ページの図35 は、DB2 (VSE 版) アプリケーション・サーバーとリモートのアプリケーション・リクエスターとの通信が確立される上での各構成要素の役割を示しています。

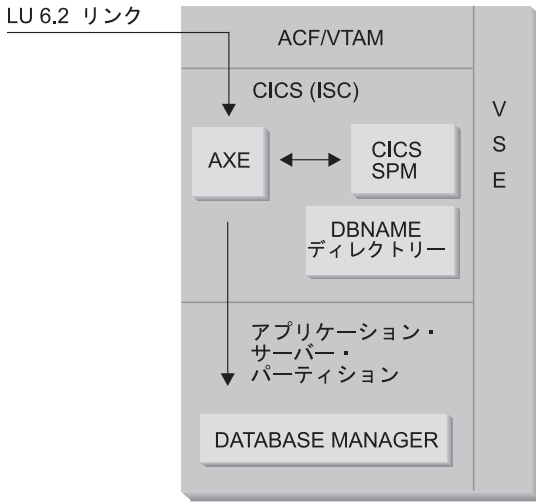


図 35. アプリケーション・サーバーへのアクセスの取得

アプリケーション・リクエスターは、特定の LU 名およびトランザクション・プログラム名 (TPN) を使用して APPC ALLOCATE verb を出し、アプリケーション・サーバーとの LU 6.2 会話を確立します。この LU 名を使用して、VTAM を介した ALLOCATE 要求の CICS への経路指定を行います。ALLOCATE verb を受信した上で、CICS は AXE トランザクションが TPN を使用して定義されていることを確認し、CICS サインオンを実行します。CICS 接続の会話機密保護レベルが VERIFY の場合、ユーザー ID とパスワードの両方がアプリケーション・リクエスターに要求され、サインオンで使用されます。接続が受け入れられるように、CICS サインオン・テーブル (DFHSNT) はこのユーザー ID とパスワードを使用して更新しなければなりません。機密保護レベルが IDENTIFY に設定されている場合は、ユーザー ID のみが必要です。CICS は機密保護チェックをリモート・システムに委託します。機密保護チェックが成功した場合は、CICS は AXE トランザクションを開始して、アプリケーション・リクエスターとアプリケーション・サーバーとの間の要求および応答を経路指定します。また、アプリケーション・リクエスターが使用する TPN には、DB2 (VSE 版) DBNAME ディレクトリーで定義された項目も必要です。このディレクトリーは VSE システムで操作している DB2 (VSE 版) サーバーを示しています。

アプリケーション・リクエスターが分散作業単位サポートを利用しようとする場合、APPC ALLOCATE verb に SYNCPT の SYNCLVL を指定します。AXE トランザクションが開始されると、CICS を照会し、会話の SYNCLVL を判別します。SYNCPT の場合、以下を行います。

- 必要な場合、AXE トランザクションは TRUE を使用可能にして、CICS 同期点管理プログラムと通信できるようにする。
- CICS 同期点管理プログラムに作業論理単位を登録する。

制限事項

VM の場合とは異なり、DB2 (VSE 版) アプリケーション・サーバーは、リモート・アプリケーション・リクエスターから DRDA フローを受け入れます。私用プロトコルはサポートされていません。結果として、VM アプリケーション・リクエスターは PROTOCOL=SQLDS では VSE サーバーにアクセスできません。

DB2 (VSE 版) DRDA サーバーは、VSE ゲスト共有を使用してリモート・アプリケーション・リクエスターからの要求を DB2 (VM 版) サーバーへ経路指定することはできません。このような要求は、DB2 (VM 版) DRDA サーバーに直接送信すべきです。

アプリケーション・サーバー開始パラメーター

RMTUSERS パラメーター

データベース管理者はアプリケーション・サーバーの始動時に RMTUSERS パラメーターを指定して、サーバーに接続できるリモート・アプリケーション・リクエスターの最大数を設定できます。これは、DB2 (VM 版) データベース・サーバー・マシンの VM ディレクトリーの MAXCONN 値と類似しています。このパラメーターを使用すると、ローカルとリモートの処理の作業負荷の平衡が保たれます。

RMTUSERS 値が (NCUSER で定義された) 使用可能な DB2 (VSE 版) エージェントの数より大きい場合、一部のリモート・ユーザーは、DB2 (VSE 版) エージェントが要求をサービスするのを待機しなければなりません。通常、DB2 (VSE 版) エージェントは、論理作業単位 (LUW) の最後で待機ユーザーに再割り当てされます。DB2 (VSE 版) アプリケーション・サーバーは、会話の終了まで複数 LUW についてリモート・ユーザーが DB2 VSE エージェントを保持するのを認める、特権アクセスをサポートしています。

SYNCPNT パラメーター

このパラメーターは、同期点管理プログラム (SPM) が DRDA-2 マルチ・サイト読み込み、マルチ・サイト書き込み分散作業単位活動を調整するために使用されるかどうかを指定します。

Y を指定すれば、サーバーは同期点管理プログラムを使い (可能な場合)、2 フェーズ・コミットおよび再同期活動を調整します。N を指定すれば、アプリケーション・サーバーは 2 フェーズ・コミットを実行するために SPM を使用しません。N が指定された場合、アプリケーション・サーバーはマルチ・サイト読み込み、マルチ・サイト書き込み分散作業単位に限定され、シングル書き込みサイトになる場合があります。Y が指定された場合、アプリケーション・サーバーは検索マネージャーが利用不能であることを見つけ、その後サーバーは N が指定されたものとして操作されます。

RMTUSERS が 0 より大きい場合、省略時値は SYNCNT=Y です。
RMTUSERS=0 のとき、SYNCNT パラメーターは N に設定されます。

VSE 環境でのアプリケーション・サーバーのセットアップ

DB2 (VSE 版) のアプリケーション・サポートによって、DB2 (VSE 版) は DRDA アプリケーション・リクエスターのサーバーとして機能することができます。DB2 (VSE 版) アプリケーション・サーバーに接続できるアプリケーション・リクエスターは以下のいずれかです。

- DB2 (VM 版) リクエスター。
- DB2 ユニバーサル・データベース (OS/390 版) リクエスター。
- DB2 リクエスター。
- OS/400 リクエスター。
- DB2 ファミリー・アプリケーション (DB2 CONNECT を含む)、または DRDA アプリケーション・リクエスター・プロトコルをサポートする他の製品は、DB2 (VSE 版) アプリケーション・サーバーと接続することができます。

ネットワーク情報の提供

ネットワーク接続を VSE アプリケーション・サーバーに接続するには、以下のステップが必要です。

1. リモート・システムへ CICS LU 6.2 セッションを確立する
2. アプリケーション・サーバーを定義する

CICS LU 6.2 セッションの確立

DB2 (VSE 版) アプリケーション・サーバーは、CICS LU 6.2 リンクを介してアプリケーション・リクエスターと通信します。この目的で使用される CICS 区画には、アプリケーション・リクエスターのあるリモート・システム

への LU 6.2 リンクがなければなりません。CICS/VSE 相互通信の手引きには、リモート・システムとの CICS LU 6.2 リンクを定義および確立することについての詳細が説明されています。

LU 6.2 通信の CICS インストールおよび資源定義:

1. ISC に必要なモジュールをインストールします。

SIT または初期化一時変更を使用して、以下のモジュールをご使用のシステムに組み込まなければなりません。

- EXEC インターフェース・プログラム (EXEC=YES を指定するか省略時値を許可する)。
- システム間通信プログラム (ISC=YES を指定)。
- DFHSG PROGRAM=TCP により生成される端末管理プログラム。
ACCMETH=VTAM、CHNASSY=YES、および VTAMDEV=LUTYPE6 を指定するバージョンが必要です。

2. CICS Restart Resynchronization Support をインストールします。

CICS Restart Resynchronization Support が使用できない場合、CICS システムがインストールされているときは、以下の CICS 表を更新して、CICS Restart Resynchronization 機能を使用可能にしてください。

DFHJCT	Journal Control Table A journal used for the CICS system log must be defined in the DFHJCT specifying JFILEID=SYSTEM in a DFHJCT TYPE=ENTRY macro.
DFHPCT	Program Control Table To generate the DFHPCT entry to use the CICS Restart Resynchronization capability, enter: DFHPCT TYPE=GROUP, FN=RMI
DFHPPT	Processing Program Table To generate the DFHPPT entry to use the CICS Restart Resynchronization capability, enter: DFHPPT TYPE=GROUP, FN=RMI
DFHSIT	System Initialization Table. The DFHSIT macro must include the JCT parameter. Specify JCT=YES or JCT=(jj<,...>) where jj is the SUFFIX parameter value specified in the DFHJCT TYPE=INITIAL macro defining the CICS system log journal data set.

3. CICS を VTAM (VSE 版) に定義します。

LU 6.2 接続をサポートする場合、CICS を VTAM アプリケーション大ノードとして VTAM (VSE 版) に定義しなければなりません。VTAM APPL ステートメントにコード化されるアプリケーション大ノードは、APPLID パラメーターにより SIT に指定された CICS 区画の APPLID です。これは、CICS システムを識別するために VTAM で使用される (そして CICS の通信相手により使用される) LU 名です。

図36 を参照してください。

```
VBUILD TYPE=APPL
*****
*
* LU Definition for Toronto VSE SQL/DS System
*
*****
VSEGATE APPL ACBNAME=VSEGATE,
          AUTH=(ACQ,SPO,VPACE),
          APPC=NO,
          SONSCIP=YES,
          ESA=30
          MODTAB=RDBMODES,
          PARSESS=YES,
          VPACING=0
```

図 36. CICS 用の VTAM APPL 定義例

AUTH=(ACQ,SPO,VPACE)

ACQ は、CICS が LU 6.2 セッションを獲得することを許可します。

SPO は、CICS が MODIFY vtamname USERVAR コマンドを出すことを許可します。

VPACE は、システム間フローの歩調合わせを許可します。

ESA=30

このオプションは、CICS がセッションを確立できるネットワーク・アドレス可能単位の数を指定します。この数には、この CICS システム用の並列セッションの合計数が含まれていなければなりません。

PARSESS=YES

LUTYPE6 並列セッション・サポートを指定します。

SONSCIP=YES

セッション故障通知 (SON) サポートを指定します。SON は、特定の場合に、CICS が障害のあるセッションを操作員の介入を必要とせずに回復するようにします。

APPC=NO

これは CICS が VTAM マクロを使用するのに必要です。CICS は、APPCCMD マクロ命令を出しません。

注: APPC=NO が指定されているため、SYNCLVL=SYNCPT は必要ありません。CICS は分散作業単位に関するすべての SYNCPT 同期点レベルの活動を管理します。

4. LU 6.2 プロトコルを使用してリモート・システムへのリンクを定義します。

a. すべてのリモート LU を CICS に定義する。

オンライン資源定義 (RDO) において CEDA DEFINE CONNECTION コマンドを使用してすべてのリモート LU を定義します。

- NETNAME パラメーターのリモート LU 名を指定する。
- PROTOCOL=APPC を指定して、LU6.2 プロトコルが使用されていることを確認する。
- AUTOCONNECT=YES および INSERVICE=YES を指定して、インストール時に、接続が自動的に行われ、セッションが自動的に確立されるようにする。
- ATTACHSEC パラメーターを使用して、会話レベル機密保護を指定する。ATTACHSEC=IDENTIFY は、DRDA で必要な最小機密保護レベルです。
- BINDPASSWORD パラメーターを使用して、セッション・レベル機密保護を指定する。省略時解釈では、セッション・レベル機密保護はありません。

会話およびセッション・レベル機密保護に関する詳細は、182ページの『機密保護の提供』を参照してください。

b. リモート・システムで LU 6.2 セッションのグループを定義する。

上記の定義済みの各接続ごとに、CEDA DEFINE SESSIONS コマンドを使用して、LU へのリンクごとのパラレル・セッションのグループを定義します。

- CONNECTION パラメーターの接続の名前 (上記で定義した) を指定する。
- MODENAME パラメーターの VTAM ログモード表項目を指定する。
- MAXIMUM パラメーターを使用して、以下を指定する。
 - セッションの最大数
 - 回線争奪勝者としてサポートされているセッションの最大数

DRDA アプリケーション・リクエスターの通信ソフトウェア (たとえば、IBM Communications Server for OS/2) が使用する値を指定する。

より大きな数で SENDSize および RECEIVESize を定義すると、データ伝送率は上がりますが、ネットワーク上でより多くの仮想記憶域が必要になります。SNA ネットワークのすべての層がサポートしているサイズは、4 K バイトです。そのため、DRDA サーバーが設定された時に、送信および受信バッファのサイズを 4 K バイトに設定してください。接続がリモート・ユーザーから正常に行われた場合、これらのパラメーターを調整して、最適値に決定してください。

- c. ユーザー ID およびパスワードを CICS に設定する。

CICS サインオン・テーブル (DFHSNT) にすべてのユーザーを定義します。CICS ターミナルで CESN ログオンを実行することにより、ユーザー ID の妥当性を検査することができます。ローカル・サインオンは成功しなければなりません。

- d. CEDA DEFINE PROGRAM コマンドを使用して、ロード・モジュール (フェーズ) を CICS に定義する。

- 1) ARICAXED - AXE トランザクション
- 2) ARICDIRD - DBNAME ディレクトリー、およびサーチ・ルーチン
- 3) ARICDAXD - DAXP および DAXT トランザクション・ハンドラー
- 4) ARICDEBD - CICS TRUE サポート使用可能性ハンドラー
- 5) ARICDRAD - CICS TRUE そのもの
- 6) ARICDR2 - DR2DFLT 制御ブロック

上記のそれぞれに、LANGUAGE=ASSEMBLER オプションを指定する必要があります。

- e. アプリケーション・リクエストで指定した TPN ごとに、CEDA DEFINE TRANSACTION コマンドを指定する。

- TRANSACTION パラメーターを使用して、TPN を指定する。
- PROGRAM=ARICAXED を指定して、フェーズを指定する。
- XTRANID パラメーターを使用して、2 番目の 16 進数トランザクション名を指定する。

この時、PROGRAM=ARICDAXD を指定して、DAXP および DAXT トランザクションの定義も行う。

定義の例: サンプル定義については、分散関係データベース体系 接続の手引きを参照してください。

アプリケーション・サーバーを定義する

1. DB2 (VSE 版) DBNAME ディレクトリーを更新します。

CEDA DEFINE TRANSACTION コマンドを使用して、これまでに定義された各トランザクションの項目を DBNAME ディレクトリーに追加します。LU 6.2 セッションが確立されると、リモート・アプリケーション・リクエスターは DB2 (VSE 版) アプリケーション・サーバーとの会話を開始できます。これは、TPN (トランザクション・プログラム名) を指定して、アプリケーション・サーバーとの LU 6.2 会話を割り当てることにより行います。この TPN は、DB2 (VSE 版) サーバーへのまたはこのサーバーからの要求を経路指定する AXE トランザクションの CICS トランザクション ID でなければなりません。TPN がアプリケーション・リクエスターからアクセスされるためには、TPN は、DB2 (VSE 版) サーバーにマップされる DB2 (VSE 版) DBNAME ディレクトリーになければなりません。DB2 (VSE 版) データベース管理者の責任で、DBNAME ディレクトリーを更新したり、リモート・ユーザーに TPN からサーバーへのマッピングを通知します。

TPN とそれに対応するサーバー名 (DBNAME ディレクトリーで定義されているデータベース名) の両方が、アプリケーション・リクエスターで識別されていなければなりません。

- アプリケーション・リクエスターは TPN を使用して、AXE ルーター・トランザクションを開始します。
 - アプリケーション・リクエスターは、初期 DRDA フローのサーバー名を引用して、ターゲット・データベース名とします。DB2 (VSE 版) サーバーはこのサーバー名を使用して、アプリケーション・リクエスターが正しいサーバーをアクセスしていることを確認します。サーバー名が一致しないと、アプリケーション・リクエスターによるサーバーへのアクセスが拒否されて、アプリケーション・リクエスターは会話を終了します。
2. プロシージャ ARISBDID を使用して、DBNAME ディレクトリー (メンバー ARISDIRD.A) を作成およびアセンブルします。

詳細については、DB2 システム管理 (VSE 版) を参照してください。

DB2 (VSE 版) アプリケーション・サーバーの準備および開始

1. AXE トランザクションは、ARIAXELG という名前の CICS 一時保管待ち行列であるエラー・ログを保持します。このエラー・ログには、通信問題および DRDA セッションの異常終了を記録した有用なエラー・メッセージが含まれています。CICS TST を使用して、このログを「回復可能」として定義してください。
2. プロシージャ ARIS342D を実行して、DRDA アプリケーション・サーバー・サポートをインストールします。

3. 必要な場合、DAXP トランザクションを発行して、省略時パスワードおよび言語を指定します。これらは CICS TRUE サポートが特定のサーバーで使用可能な時に使われます。詳細については、DB2 操作解説書 (VSE 版) を参照してください。
4. DBNAME、RMTUSERS、および SYNCNT パラメーターを使用して、DB2 (VSE 版) を開始する。
 - 使用される DBNAME は、DBNAME ディレクトリーで定義されなければなりません。
 - RMTUSERS パラメーターは、ゼロであってはなりません。
 - SYNCNT=Y を指定して、分散作業単位サポートを使用可能にする。
5. すべてのリモート・ユーザーは、異なるレベルの許可で DB2 (VSE 版) サーバーにより許可されていなければなりません。詳細については、DB2 データベース管理 (VSE 版) を参照してください。

問題判別:

- アプリケーション・リクエスターが、有効な TPN (DBNAME ディレクトリーで定義される TPN) を使用してパートナー CICS の到達に成功した場合には、AXE トランザクションが開始されます。プログラム ARICAXED での使用回数は、1 つずつ増加します (CEMT I PR(ARICAXED) を出して確認)。
- CICS サインオン・テーブルでリモート・ユーザー ID が確立されていることを確認するには、リモート・ユーザーのユーザー ID とパスワードで CESN トランザクションを使用してローカル・サインオンを実行します。ローカル・サインオンは成功しなければなりません。
- DB2 (VSE 版) サーバーが実行され、アプリケーションが初めに DRDA-2 分散作業単位活動を処理する場合、サーバーへの TRUE サポートが自動的に使用可能になります。TRUE サポートが正常に使用可能になったという、メッセージ ARI0187I を調べてください。しかし、TRUE を使用可能中にエラーが起きたという、メッセージ ARI0190E が表示された場合、コンソールで以前のエラー・メッセージを調べてください。
- ご使用の DRDA アプリケーション・プログラムがセンス・コード X'08063426' または X'FFFE0101' を受け取った場合、CICS はセッションの外で実行しているということです。すべてのセッションが使用されているか、アンバインドされる予定でありながら、UNBIND が完了されていない場合、CICS はセッションの外でも実行される場合があります。所要時間の短い同時着信トラン

ザクションがたくさんある場合、CICS はセッションの外で実行される場合があります。この場合、UNBIND される予定でありながら、まだ UNBIND が完了していないセッションに応じて、CEDA DEFINE SESSIONS MAXIMUM で指定するセッション数を増やしてください。

機密保護の提供

DB2 (VSE 版) アプリケーション・サーバーは、システム間通信の機密保護の点で CICS に依存しています。CICS はいくつかのレベルの機密保護を提供します。

- バインド実行時機密保護

SNA LU 6.2 セッション・レベル LU 間妥当性検査を CICS で実現したものです。バインド実行時機密保護の実施は、LU 6.2 体系では任意選択です。アプリケーション・サーバーの側では、アプリケーション・リクエスターへの接続を定義するときに CEDA DEFINE CONNECTION コマンドで BINDPASSWORD を指定することにより、この機能を使用可能にすることができます。アプリケーション・リクエスター上で、アプリケーション・リクエスターにサービスを提供するパートナー LU はバインド実行時の機密保護もサポートして、パートナー LU 検査のために同じパスワードを使用しなければなりません。

権限のないリモート・システムが CICS を使用してセッションを確立 (バインド) するのを阻止するために、バインド実行時機密保護を使用できます。

- リンク機密保護

リンク機密保護を使用して、リモート・システム (およびそれに常駐する DRDA アプリケーション・リクエスター) が特定のセットの AXE トランザクションだけに接続するように制限できます。

たとえば、2 つの AXE トランザクションを定義できるとします。AXE2 は機密保護キー 2 で、AXE3 は機密保護キー 3 で定義します。リモート・システムからのアプリケーション・リクエスターは、操作員機密保護 3 と割り当てることができ (たとえば、CEDA DEFINE SESSION コマンドで OPERSECURITY パラメーターを使用)、これで AXE3 だけに接続を許可できます。AXE2 が優先アクセスを有している間は、AXE3 はサーバーへの優先アクセスを持つことはできません。リモート・アプリケーション・リクエスターによるアプリケーション・サーバーへの特権アクセスについての詳細は、DB2 システム管理 (VSE 版) を参照してください。

リンク機密保護を使用可能にする方法については、CICS/VSE 相互通信の手引きを参照してください。

- ユーザー機密保護

エンド・ユーザーに妥当性検査を提供する SNA LU 6.2 会話レベル機密保護を CICS で実現したものです。

ユーザー機密保護は、会話を開始する要求を受け入れる前に、CICS サインオン・テーブル (DFHSNT) でユーザー ID の妥当性検査をします。たとえば、CICS サインオン・テーブルに定義されていない DRDA アプリケーション・リクエスターは、AXE トランザクションに接続して DB2 (VSE 版) サーバーとの会話を開始するように許可されていません。リモート・システムのユーザー機密保護レベルは、ATTACHSEC パラメーターを使用して CEDA DEFINE CONNECTION コマンドで選択できます。接続機密保護の 3 つのレベルは以下のとおりです。

- LOCAL。DRDA ではサポートされていません。
 - IDENTIFY。LU 6.2 用語では、SECURITY=SAME (または検査済み) と同じです。この機密保護レベルでは、CICS は、会話を DB2 (VSE 版) サーバーに割り当てるのを許可する前に、リモート・システムがそのユーザーを検査するように『委託』します。CICS サインオン・プロセスには、ユーザー ID だけが必要です。しかし、パスワードも渡された場合は、CICS はパスワードを使ってサインオンを実行します。
 - VERIFY。LU 6.2 用語では、SECURITY=PGM と同じです。この機密保護レベルでは、CICS は、会話を割り当てるときにリモート・システムがユーザー ID とパスワードの両方を送信することを要求し、パスワードが提供されない場合には接続を拒否します。
- SNA LU 6.2 セッション・レベル強制暗号。サポートされていません。

アプリケーション・サーバーの責任でデータベース資源を管理するので、アプリケーション・リクエスターがどのネットワーク機密保護メカニズムを提供しなければならないかを、アプリケーション・サーバーが指示します。たとえば、DB2 (VM 版) アプリケーション・リクエスターでは、184ページの図37に示されているとおり、適切な値を :security タグに設定して、アプリケーション・サーバーの会話レベル機密保護要求をアプリケーション・リクエスターの通信ディレクトリーに記録しなければなりません。

```
:nick.VSE1      :tpn.TOR3
                 :luname.TORGATE VSEGATE
                 :modename.IBMRDB
                 :security.PGM
                 :userid.SALESMGR
                 :password.PROFIT
                 :dbname.TORONTO3
```

Where: TOR3 - AXE transaction ID mapped to database TORONTO3.
TORGATE - VM/APPC gateway.
VSEGATE - APPLID of the CICS/VSE partition serving as gateway to TORONTO3.
SALESMGR/PROFIT - USERID/PASSWORD defined in the DFHSNT of VSEGATE, and authorized in TORONTO3
TORONTO3 - The name specified on the DBNAME startup parameter when the DB2 for VSE application server was started (or the name of the default database determined by the DBNAME Directory if DBNAME was omitted at startup).

図 37. CMS 通信ディレクトリー項目の例

データベース・マネージャー機密保護

ユーザー ID 変換は、VSE アプリケーション・サーバーでサポートされていません。CICS は、リクエスターから直接伝送されたユーザー ID を使用します。

アプリケーション・リクエスターにより開始された後、AXE トランザクションは CICS からユーザー ID を抽出し、これを DB2 (VSE 版) サーバーに渡します。データベース資源で必要なレベルのユーザー権限を設定するには、ユーザー ID を DB2 (VSE 版) カタログ SYSTEM.SYSUSERAUTH に更新しなければなりません。

DB2 (VSE 版) アプリケーション・サーバーは CICS により指定されたユーザー ID にデータベースへアクセスするための CONNECT 権限があるかどうかを検査し、権限がない場合には接続を拒否します。

データベース資源の所有者として、DB2 (VSE 版) アプリケーション・サーバーは、そこにある SQL オブジェクトに対してデータベース機密保護機能を制御します。DB2 (VSE 版) により制御されるオブジェクトへのアクセスは特権のセットを使用して制御されます。この特権は、DB2 (VSE 版) システム管理者または特定のオブジェクトの所有者により認可されます。DB2 (VSE 版) アプリケーション・サーバーは、2 つのクラスのオブジェクトを制御します。

- **パッケージ:** 個々のエンド・ユーザーは、DB2 (VSE 版) GRANT ステートメントを使用して、パッケージの作成、置換、実行を行う権限を持っています。

す。ユーザーがパッケージを作成するとき、そのユーザーはパッケージを実行または置換するように自動的に許可されます。他のエンド・ユーザーは `GRANT EXECUTE` ステートメントを使用して、DB2 (VSE 版) アプリケーション・サーバーでパッケージを実行するように個々に許可されなければなりません。RUN 特権は、個々のエンド・ユーザーまたは PUBLIC に授与することができます。PUBLIC は、パッケージの実行をすべてのエンド・ユーザーに許します。

アプリケーションが DB2 (VSE 版) でプリプロセスされる時、パッケージにはアプリケーション・プログラムにある SQL ステートメントが含まれています。これらの SQL ステートメントは以下のように分けられます。

- **静的 SQL:** これは、SQL ステートメントおよびそのステートメントにより参照される SQL オブジェクトが、アプリケーションのプリプロセス時に認識されることを意味します。パッケージの作成者は、パッケージ内のそれぞれの静的 SQL ステートメントを実行する権限を持っていない限りなりません。

エンド・ユーザーがパッケージを実行する特権を与えられるとき、そのユーザーはパッケージに含まれる各静的 SQL ステートメントを実行する権限を自動的に持ちます。それで、パッケージに静的 SQL ステートメントしか含まれていない場合には、エンド・ユーザーは DB2 (VSE 版) 表特権の必要はありません。

- **動的 SQL:** パッケージが実行するまで認識されない SQL ステートメントのことです。SQL ステートメントはプログラムにより作成され、SQL PREPARE ステートメントまたは EXECUTE IMMEDIATE ステートメントを使用して、動的に DB2 (VSE 版) にプリプロセスされます。エンド・ユーザーが動的 SQL ステートメントを実行するとき、そのユーザーには SQL ステートメントを実行するために必要な表特権がなければなりません。パッケージが作成される時に SQL ステートメントが認識されないため、エンド・ユーザーにはパッケージ所有者により必要な権限が自動的に与えられません。

- **SQL オブジェクト:** 表、視点、および同義語のことです。DB2 (VSE 版) ユーザーには、個々の SQL オブジェクトを作成、削除、変更、または読み取る権限の各種のレベルを授与できます。この権限は、静的 SQL ステートメントをプリプロセスしたり、動的 SQL ステートメントを実行するために必要です。

データの表示

169ページの『データの表示』を参照してください。

DB2 (VSE 版) DRDA アプリケーション・サーバーを使用可能にするためのチェックリスト

以下のチェックリストは DRDA アプリケーション・サーバーを使用可能にするためのステップを要約したものです。初めに次のような前提事項があります。まず、VSE システムがテレプロセッシング・アクセス方式として ACF/VTAM を使用してインストールされていること、そして、リモート・システムとの通信に必要な VTAM 定義 (NCP 定義など) がすでに完了していることです。

1. CICS ISC サポートおよび Restart Resynchronization サポートをインストールする。
2. CICS を VTAM (VSE 版) に定義します。
3. IBMRDB 項目で VTAM LOGMODE 表をアセンブルします。
4. すべてのリモート・ユーザー ID およびパスワードを定義して CICS サインオン・テーブルをアセンブルします。
5. 正しい SIT 情報で CICS を開始します。
 - ISC=YES
 - TST=YES、DFHTST で RECOVERABLE として定義されアセンブルされた ARIAXELG
 - APPLID=LU 名 (VTAM APPL ステートメントで定義)
6. リモート・システムを CICS に定義します (RDO が使用できます)。
 - CEDA DEF CONNECTION
 - CEDA DEF SESSION
 - CEDA DEF PROGRAM
 - CEDA DEF TRANSACTION

これらのステートメントには、1 つのグループ (たとえば、IBMG) のもとにすべての定義がなければなりません。CEDA INSTALL GROUP(IBMG) でグループをインストールします。
7. DBNAME ディレクトリーを更新します (ARISDIRD.A)。
 - ディレクトリーにリストされたすべての TPN を CICS に定義します。CICS に定義された TPN は使用できません。
 - 有効な TPN で、ディレクトリーに各 DB2 (VSE 版) DRDA アプリケーション・サーバーを定義します。
8. プロシージャー ARISBDID を実行して、更新された DBNAME ディレクトリーをアセンブルします。
9. DB2 (VSE 版) サーバーを準備します。

- プロシージャー ARIS342D を実行して、DRDA サポートをインストールします。
 - オンライン DB2 (VSE 版) アプリケーション (たとえば、ISQL) が CICS 区画から実行されている場合には、CICS SIT 表に指定されている CICS APPLID でスケジュール権限を認可します。
 - すべてのリモート・ユーザーに権限を授与します。
10. 必要な場合、DAXP CICS トランザクションを実行します。
 11. 正しい RMTUSERS パラメーターを使用して (任意選択で、DBNAME パラメーターおよび SYNCNT パラメーターも使用) DB2 (VSE 版) を開始します。
 12. VSE DRDA アプリケーション・サーバーでアプリケーションを準備します。

付録A. よく起こる接続問題

この付録では、DB2 コネクトと DB2 UDB DRDA-AS の使用時に、DB2 UDB ワークステーションの DB2 コネクトで生じる接続問題の一般的な症状をリストしています。

- 『よくある DB2 接続問題』
- 200ページの『DB2 UDB DRDA AS で最も一般的な問題』

この情報は、問題解決のプロセスを支援する目的で準備されました。メッセージ解説書、問題判別の手引き、および DB2 コネクト 使用者の手引き も参照してください。

よくある DB2 接続問題

この節では、DB2 コネクトの使用時に接続問題が生じたときの最も一般的な症状をリストします。どの場合でも、以下の形式で示されます。

- 表示されたメッセージに関連した、メッセージ番号と戻りコード (またはプロトコル固有の戻りコード) の組み合わせ。各メッセージと戻りコードの組み合わせには、個別のヘッダーがあり、このヘッダーはメッセージ番号順、その後に戻りコードの順で並べられます。
- 症状が示されます。通常は、サンプル・メッセージのリスト形式で示されます。
- 解決方法が提示されます。エラーの推定原因が示されます。場合によっては、複数の解決方法が提示されることがあります。

注:

1. ご使用の製品の概説およびインストールの資料や、推奨されるソフトウェア修正レベルについての最新の情報を収めた最新のリリース情報を参照してください。
2. APPC 通信に固有のメッセージと戻りコードの組み合わせの場合、SNA センス・コードも表示されます。今のところ、特定のメッセージと関連した SNA センス・コード情報は、SNA サブシステムから入手する必要があります。

システム・ログを見ていくと、SNA センス・コードを見られます。これが当てはまるかどうかは、使用する SNA サブシステムによって異なります。

状況によっては、SNA トレースをアクティブにして問題を再現し、センス・コード情報を入手しなければならないこともあります。

3. ゲートウェイという用語は、DB2 コネクト エンタープライズ・エディションを指しています。

SQL0965 または SQL0969

症状

DB2 ユニバーサル・データベース (AS/400 版)、DB2 ユニバーサル・データベース (OS/390 版)、DB2 (MVS/ESA 版)、および DB2 (VM および VSE 版) からのさまざまな異なる戻りコードとともに、メッセージ SQL0965 および SQL0969 が発行されます。

いずれかのメッセージが出された場合、そのメッセージを発行したデータベース・サーバー製品の資料で、元の SQL コードを調べる必要があります。

解決方法

ホスト・データベースから受信された SQL コードを変換できません。そのエラー・コードに基づいて問題を訂正してから、失敗したコマンドを再発信してください。

CONNECT 時の SQL1338

症状 / 原因

記号宛先名が定義されていないか、適切に定義されていません。

たとえば、これは APPC ノードを使用していて、DB2 ノード・ディレクトリーに指定した記号宛先名がローカル APPC 通信サブシステム構成の CPI-C 項目と一致しない場合に、生じることがあります。

別の原因として、複数の SNA スタックをマシンにインストールしてあることもあります。PATH と LIBPATH を検査して、使用したいスタックがまず最初に参照されることを確認する必要があるかもしれません。

解決方法

1. DB2 ノード・ディレクトリー項目に指定した CPIC サイド情報のプロファイル名が、SNA 構成と一致するようにします (大文字小文字を区別します)。
2. PATH と LIBPATH を検査して、使用したい SNA スタックがまず最初に参照されることを確認する必要があるかもしれません。

CONNECT 時の SQL1403N

症状

SQL1403N 指定されたユーザー名とパスワードのいずれか、またはその両方が正しくありません。

解決方法

1. DB2 コネクト・ワークステーションで認証に失敗します。ユーザーが DB2 コネクト・ワークステーションで認証されるようになっていないかを判別してください。

認証されるようになっていない場合、必要であれば CONNECT ステートメントに正しいパスワードを指定してあるか確認してください。

認証されるようになっていない場合、システム・データベース・ディレクトリー項目は、AUTHENTICATION SERVER (AUTHENTICATION を明示的に指定していない場合は、これが省略時値) を使用して不正にカタログ化されています。この場合、AUTHENTICATION DCS または CLIENT を使用して、項目を再カタログ化してください。

2. ターゲット・サーバー・データベースへ送信するときに使用できないパスワードです。システム・データベース・ディレクトリー項目が AUTHENTICATION DCS を使用してカタログされている場合は、パスワードを DB2 クライアントからターゲット・サーバー・データベースに送信する必要があります。特定のプラットフォーム、たとえば AIX などでは、パスワードは CONNECT ステートメントに指定してある場合に限り、入手することができます。

SQL5043N

症状

1 つまたは複数の通信プロトコルに対するサポートが正常に開始できませんでした。ただし、コアとなるデータベース・マネージャーの機能は正常に開始されました。

おそらく、TCP/IP プロトコルが DB2 コネクト・ゲートウェイで開始されていません。以前に成功したクライアント接続がまだ残っている可能性があります。

diaglevel = 4 の場合、db2diag.log に同様の項目が含まれている可能性があります。たとえば次のようになります。

```
1997-05-30-14.09.55.321092 Instance:svtdbm5 Node:000
PID:10296(db2tcpcom) Appid:none
common_communication sqlcctcpconnmgr_child Probe:46
DIA3205E Socket address "30090" configured in the TCP/IP
services file and
required by the TCP/IP server support is being used by another
process.
```

解決方法

この警告は、DB2 コネクト (リモート・クライアントのゲートウェイとして動作している) が 1 つまたは複数のクライアント通信プロトコルを処理する際に問題が発生していることを示しています。これらのプロトコルは TCP/IP、APPC その他のものであり、このメッセージは通常、DB2 コネクトに定義されているこれらの通信プロトコルのいずれかが正しく構成されていないことを示しています。

DB2COMM プロファイル変数が定義されていないか、不正に定義されていることが原因かもしれません。一般に、問題は DB2COMM 変数と、データベース・マネージャー構成で定義した名前 (たとえば、svccname、nname、または tpname) との間のミスマッチの結果です。

可能性のあるシナリオとして 1 つあげられるのは、以前に成功した接続がそのままになっており、構成が変更されていないのに、SQL5043 エラー・メッセージを受け取ってしまったというものです。これは、TCP/IP プロトコルの使用時にリモート・システムが何らかの理由で接続を異常終了したときに発生する可能性があります。異常終了する場合、接続をクライアント上に残しておくことができるので、下記のコマンドを発行して介入しなくても、接続を復元することができます。

一番多いのは、ゲートウェイに接続しているクライアントの 1 つが TCP/IP ポート上でハンドルを持ったままになるというケースです。ゲートウェイに接続している各クライアント・マシン上で、以下を発行します。

1. db2 terminate
2. db2stop

SQL30020

症状

SQL30020N 後続のコマンドまたは SQL ステートメントの正常な実行に影響を与える分散プロトコル・エラーのために、実行が失敗しました。

解決方法

このエラーが発生したら、サービス担当者に連絡してください。

db2dump ディレクトリーに ffdc ダンプ (pid.000) があるかどうか調べてください。ある場合は、このダンプ・ファイルを db2fdump によってフォーマットし、結果ファイルで "ERROR" を調べてください。そこに MVS ABEND がリストされている可能性があります。その場合、MVS コンソールで詳細を調べ、DB2 for MVS Messages and Codes の資料で異常終了コードを調べてください。

SQL30060

症状

SQL30060N "<authorization-ID>" が、処理 "<operation>" を実行する権限を持っていません。

解決方法

DB2 (MVS 版) または DB2 (OS/390 版) への接続時に、通信データベース (CDB) 表が正しく更新されていません。次を参照してください。

- DB2 コネクト 概説およびインストール

SQL30061

症状

誤ったホストまたは AS/400 データベース・サーバー・ロケーションに接続しています。ターゲット・データベースが見つかりません。

解決方法

DCS ディレクトリー項目に誤ったサーバー・データベース名を指定した可能性があります。これが生じた場合、SQLCODE -30061 がアプリケーションに戻されます。

DB2 ノード、データベース、および DCS ディレクトリー項目を調べてください。DCS ディレクトリー項目の宛先データベース名のフィールドは、プラットフォームに基づいたデータベースの名前に対応していなければなりません。たとえば、DB2 ユニバーサル・データベース (OS/390 版) データベースの場合、使用する名前はブートストラップ・データ・セット (BSDS) の "LOCATION=locname" フィールドで使用した名前と同じでなければなりません。これは、分散データ機能 (DDF) を開始するときの DSNL004I メッセージにも示されています (LOCATION=location)。

ご使用の DB2 コネクト 概説およびインストール の資料には、DB2 カタログの更新方法を示す例が収められています。SNA 構成を説明する各章の

『DB2 ディレクトリーの更新』を参照するか、『ホストおよび AS/400 データベースでの DB2 コネクトの構成』の章の『TCP/IP 接続の構成』を参照してください。

APPC または APPN ノードへの正しいコマンドは次のとおりです。

```
db2 catalog appc node <node_name> remote <sym_dest_name> security program
db2 catalog dcs database <local_name> as <real_db_name>
db2 catalog database <local_name> as <alias> at node <node_name>
authentication dcs
```

TCP/IP ノードへの正しいコマンドは次のとおりです。

```
db2 catalog tcpip node <node_name> remote <host_name_or_address>
server <port_no_or_service_name>
db2 catalog dcs database <local_name> as <real_db_name>
db2 catalog database <local_name> as <alias> at node <node_name>
authentication dcs
```

その後にデータベースへ接続するには、次のコマンドを発行します。

```
db2 connect to <alias> user <user_name> using <password>
```

CONNECT 時の SQL30073 (戻りコード 119C)

症状

メッセージ SQL30073 は戻りコード 119C とともに発行されます。これが発行されるのは、ターゲット・サーバー・データベースが DB2 クライアント (DB2 コネクトを使用する) のコード・ページをサポートしていない場合です。このコード・ページは、DB2 クライアントが実行されている操作環境の構成から派生します。

詳しくは、[管理の手引き](#) を参照してください。

解決方法

この問題は、ターゲット・サーバー・データベース・システムに修正ファイルをインストールすることにより、解決できることもあります。適切なサービス部門に連絡して、この症状に適した修正ファイルを入手し、それを適用してください。

一時的な作業環境として、ユーザーは DB2CODEPAGE 環境変数を設定することにより、省略時のコード・ページをオーバーライドすることができます。ロケールを調べるか、DB2CODEPAGE=850 を設定してください。

UNIX プラットフォームでは、LANG 環境変数を別の値に設定することにより、別のコード・ページに切り替えることができます。

SQL30081N (戻りコード 1)

症状

症状は、次のメッセージと SNA センス・コードです。

```
db2 connect to <database name> user <userid>
Enter password for <userid>:
SQL30081N A communication error has been detected.
Communication protocol
being used: "APPC". Communication API being used: "CPI-C".
Location where
the error was detected: "". Communication function detecting
the error:
"cmallc". Protocol specific error code(s): "1", "*",
"0x10030021".
SQLSTATE=08001
```

解決方法

この例では、センス・コードは 10030021 です。

このエラー・メッセージと関連する最も一般的なセンス・コード、およびそれぞれの場合の提案されている解決方法は、以下のとおりです。

1.

SQL30081N with return code 1 and sna sense code 0877002C

正しくないネットワーク名を指定しています。

2.

SQL30081N with return code 1 and SNA sense code ffff0003

正しくない MAC アドレスを指定しているか、SNA リンクがアクティブではありません。

3.

SQL30081N with return code 1 and SNA sense code 10030021

LU タイプのミスマッチがあります。

4.

SQL30081N with return code 1 and SNA sense code 084B6031

DSNZPARM の MAXDBAT (DB2 (MVS 版) または DB2 (OS/390 版) ホスト) は、0 に設定されます。

他の提案:

1. ローカル LU プロファイルを作成しているときに、その LU を省略時の LU として定義します。たとえば、CM/2 の「SNA 機能 (SNA Feature)」リスト・パネルでは、以下のいずれかを行います。
 - 「このローカル LU を省略時 LU 別名として使用する (Use this local LU as your default local LU alias)」チェック・ボックスにチェックマークを付ける。
 - DB2 コネクト エンタープライズ・エディション・ゲートウェイ・システムのプロファイルまたは環境変数 APPCLU をローカル LU 名に設定する。OS/2 システムでは CONFIG.SYS を編集することにより、Windows NT システムではコントロール・パネルによってこの作業を行うことができます。
2. DB2 コネクト・ゲートウェイで SNA が開始していることをチェックします。
3. DB2 (MVS 版) または DB2 (OS/390 版) を使用している場合、分散データ機能 (DDF) アドレス空間が開始されており、DB2 が実行中であることを確認します。

SQL30081N (戻りコード 2)

症状

戻りコード 2 および SNA センス・コード 08120022 であるメッセージ SQL30081N を受け取ります。

解決方法

NCP (リンクのホスト端) の NUMILU パラメーターは、省略時値 (0) に設定されている可能性があります。このことを確認してください。再試行前、あるいは変更を有効にした後、必要であれば NCP 定義を変更します。

SQL30081N (戻りコード 9)

症状

症状は次のメッセージです (この場合は、SNA センス・コードは必要ありません)。

```
db2 connect to <database> user <userid>
SQL30081N  A communication error has been detected.
Communication protocol
being used: "APPC".  Communication API being used: "CPI-C".
Location where
the error was detected: ".  Communication function detecting
```

```
the error:
"cmsend". Protocol specific error code(s): "9", "*",
"0x10086021".
SQLSTATE=08001
```

解決方法

問題は、DB2 コネクト・システム上でトランザクション・プログラム名 (TPNAME) が正しく定義されていないことにあります。たとえば、ご使用の SNA 構成は更新してあっても、DB2 コネクト・ゲートウェイで検証されていない場合があります。詳細は、DB2 コネクト エンタープライズ・エディション (OS/2 および Windows NT 版) 概説およびインストール、または DB2 コネクト パーソナル・エディション 概説およびインストール の資料を参照してください。

SQL30081N (戻りコード 10)

症状

症状は次のメッセージです (SNA センス・コードは必要ありません)。

```
SQL30081N A communication error has been detected.
Communication protocol
being used: "APPC". Communication API being used: "CPI-C".
Location where
the error was detected: ". Communication function detecting
the error:
"cmrcv". Protocol specific error code(s): "10", "*", "*".
SQLSTATE=08001
```

解決方法

DB2 を正しくインストールしたことを確認してください。

DB2 コネクト (OS/2 版) ゲートウェイを使用している場合は、TP 名が正しく定義されていないと次のように表示されます。

```
Protocol specific error code(s): "10", "*", "0x084C0000".
SQLSTATE=08001
```

たとえば CM/2 では、この場合次のように定義する必要があります。

```
Transaction program name      = 'tpname'      (user defined)
OS/2 program path and file name = notused
```

および (次の CM/2 構成画面)

```
Presentation type - background
Operation type - Queued, operator preloaded
```

SQL30081N (戻りコード 20)

症状

```
SQL30081N A communication error has been detected.  
Communication protocol  
being used: "APPC". Communication API being used: "CPI-C".  
Location where  
the error was detected: "". Communication function detecting  
the error:  
"xcstp". Protocol specific error code(s): "20", "*", "*".  
SQLSTATE=08001
```

解決方法

DB2 コネクト・システムで SNA サブシステムが開始していることを確認します。

SQL30081N (戻りコード 27)

症状

戻りコード 27 および SNA センス・コード 800Axxxx であるメッセージ SQL30081N を受け取ります。

解決方法

VTAM パス情報単位 (PIU) が大きすぎます。

SQL30081N (戻りコード 79)

症状

```
SQL30081N A communication error has been detected.  
Communication protocol  
being used: "TCP/IP". Communication API being used: "SOCKETS".  
Location  
where the error was detected: "". Communication function  
detecting the error:  
"connect". Protocol specific error code(s): "79", "*", "*".  
SQLSTATE=08001
```

解決方法

このエラーは、リモート・クライアントが DB2 コネクト・ゲートウェイへの接続に失敗した場合に発生する可能性があります。さらに、DB2 コネクト・ゲートウェイからホストへの接続時にも発生することがあります。

1. DB2COMM プロファイル変数が、DB2 コネクト・ゲートウェイで正しく設定されていない可能性があります。このことを確認してください。たとえば、

DB2 エンタープライズ拡張エディションを AIX 上で実行している場合は、コマンド `db2set db2comm=tcpip` が `sqllib/db2profile` に存在していなければなりません。

2. DB2 クライアントと DB2 コネクト・ゲートウェイで、TCP/IP サービス名またはポート番号 (あるいはその両方) の仕様間にミスマッチがある可能性があります。両方のマシンで、TCP/IP `services` ファイル内の項目を確認してください。
3. DB2 コネクト・ゲートウェイで DB2 が開始していることをチェックします。次のコマンドを使用して、データベース・マネージャー構成の `diaglevel` を 4 に設定してください。

```
db2 update dbm cfg using diaglevel 4
```

DB2 を停止して再始動したら、`db2diag.log` ファイルを参照して、DB2 TCP/IP 通信が開始していることをチェックします。次のような出力が含まれているはずです。

```
1998-02-03-12.41.04.861119 Instance:svtdbm2 Node:00
PID:86496(db2sysc) Appid:none
common_communication sqlcctcp_start_listen Probe:80
DIA3000I "TCP/IP" protocol support was successfully started.
```

SQL30081N (プロトコル固有のエラー・コード 10032)

症状

```
SQL30081N A communication error has been detected.
Communication protocol
being used: "TCP/IP". Communication API being used: "SOCKETS".
Location
where the error was detected: "9.21.85.159". Communication
function detecting
the error: "send". Protocol specific error code(s): "10032",
"*", "*".
SQLSTATE=08001
```

解決方法

このエラー・メッセージは、TCP/IP 通信に失敗したマシンから切断しようとするときに受け取ることがあります。TCP/IP サブシステムの問題を修正してください。

問題を修正する方法は、ほとんどのマシンでは、そのマシンの TCP/IP プロトコルを再始動することになります。マシン全体を再生しなければならないこともあります。

DB2 UDB DRDA AS で最も一般的な問題

この節では、DB2 UDB DRDA AS の使用時に最も生じやすい問題のシナリオをリストします。

CONNECT 時の通信エラー

DB2 UDB の終端で以下のものが正しく設定されていることを確認してください。

APPC/SNA LU 6.2

1. SNA 構成

必要であれば、TP 名を構成されていることを確認してください。

同様に、DRDA AR から機密保護 SAME を使用する場合、それが DRDA AR LU で使用可能になっていることを確認してください。

2. データベース・マネージャー構成の TPNAME パラメーター

3. 組み込み APPC に設定された環境変数 DB2COMM

警告が出されずに db2start が完了したことを確認してください。

TCP/IP

1. サービス・ファイル

2. データベース・マネージャー構成の SVCENAME パラメーター

3. 組み込み TCP/IP に設定された環境変数 DB2COMM。警告が出されずに db2start が完了したことを確認してください。

CONNECT 時の DRDA エラー

APPC/SNA LU 6.2

SNA Server for AIX が使用中である場合、`~/sqlib/adm/db2sysc` 実行可能ファイルのグループ名が、SNA 構成の「SNA システムのデフォルト (SNA System Defaults)」プロファイルの「トラステッド・グループ名 (Trusted group names)」フィールドに含まれていることを確認してください。

TCP/IP

DRDA AR が DB2 (OS/390 版) である場合は、APAR PQ05771/PTF UQ06843 と APAR PQ07537/PTF UQ09146 が適用されていることを確かめてください。

CONNECT 時のデータベースが見つからないエラー

ターゲット DB2 UDB データベースのデータベース別名を使用して DRDA AR が構成されていることを確認してください。

APPC/SNA LU 6.2 を介した CONNECT 時の機密保護エラー

DRDA AR からの接続が APPC/SNA LU 6.2 経由である場合、DB2 UDB データベース・マネージャー構成内の AUTHENTICATION 設定について特別な考慮事項があります。機密保護エラーが生じる場合、データベース・マネージャー構成の AUTHENTICATION 設定が次のように正しく設定されていることを確認してください。

1. クライアント

この設定では、機密保護 SAME と PROGRAM 接続の両方が動作します。

2. サーバー

この設定では、SNA サーバーを使用した AIX 上の DB2 UDB DRDA AS、および CS/2 V4 (SPM 構成済み) を使用した OS/2 上の DB2 UDB DRDA AS への機密保護 PROGRAM 接続だけが動作します。

3. DCS

DB2 UDB バージョン 7 DRDA AS では、AUTHENTICATION DCS が使用できるようになっています。この設定では、DRDA クライアントからの APPC 接続に機密保護 SAME (パスワード不要) を使用し、他のすべてのクライアント要求に SERVER 認証 (パスワードが必要) を強制することができます。

この設定では、次のものが動作します。

- a. SNA サーバーを使用した AIX 上の DB2 UDB DRDA AS、および CS/2 V4 (SPM 構成済み) を使用した OS/2 上の DB2 UDB DRDA AS
Security SAME
- b. CM/2 1.11 を使用した OS/2、Windows NT、および Sun Solaris 上の DB2 UDB DRDA AS
Security SAME or PROGRAM

通信サブシステムによっては、DB2 UDB への着信パスワードを公開していないため、このような違いがでてきます。

BIND 時のエラー

DRDA AS によって指定されたバインド・オプションがサポートされていない場合、SQLCODE -4930 が示された SQLCA が戻されることがあります。

「SQLERRMC」フィールドには、エラーを引き起こしたバインド・オプションについての情報が含まれています。

付録B. 特記事項

本書において、日本では発表されていない IBM 製品 (機械およびプログラム)、プログラミングまたはサービスについて言及または説明する場合があります。しかし、このことは、弊社がこのような IBM 製品、プログラミングまたはサービスを、日本で発表する意図があることを必ずしも示すものではありません。本書で、IBM ライセンス・プログラムまたは他の IBM 製品に言及している部分があっても、このことは当該プログラムまたは製品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。これらのプログラムまたは製品に代えて、IBM の知的所有権を侵害することのない機能的に同等な他社のプログラム、製品またはサービスを使用することができます。ただし、IBM によって明示的に指定されたものを除き、これらのプログラムまたは製品に関連する稼働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 および他社は、本書で説明する主題に関する特許権 (特許出願を含む)、商標権、または著作権を所有している場合があります。本書は、これらの特許権、商標権、および著作権について、本書で明示されている場合を除き、実施権、使用権等を許諾することを意味するものではありません。実施権、使用権等の許諾については、下記の宛先に、書面にてご照会ください。

〒106-0032 東京都港区六本木 3 丁目 2-31
AP 事業所
IBM World Trade Asia Corporation
Intellectual Property Law & 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ます。

本書に含まれる情報には、技術的に不正確なもの、または誤植が含まれる場合があります。これらに対する変更は、定期的に行われます。これらの変更は、資料の改訂版に含まれます。IBM は、本書で説明している製品、プログラムに対して、予告なく改良、変更を加える場合があります。

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、お客様になんら義務も負わせない適切な方法で、使用もしくは配布することがあります。

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 Canada Limited
Office of the Lab Director
1150 Eglinton Ave. East
North York, Ontario
M3C 1H7
CANADA

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

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

本書に含まれるパフォーマンス・データは、制御された環境下で決定されています。したがって、その他の稼働環境で得られる結果とは、かなり異なる可能性もあります。一部の測定値は、開発中のシステムを使用している場合があり、これらの測定値が一般的に提供可能なシステムで同様の数値になることを保証するものではありません。さらに、一部の測定値が推定されたものもあります。実測値と異なる場合があります。本書のユーザーは、使用される特定の環境での該当データを確認してください。

IBM 以外の製品については、当該製品の提供者から直接、出版されている資料または一般公開されている情報から入手しました。IBM は、これらの製品についてはテストを行っておらず、これらの IBM 以外の製品に関する性能、互換性またはその他の主張について確認することはできません。IBM 以外の製品の機能に対する質問は、それぞれの製品提供者にお問い合わせください。

IBM の将来の方向性または意図については、予告なしに変更または中止する場合があります。IBM の目的および目標のみを示しているものです。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれていますが、これは説明に具体性を与えるために記載されたものであり、それらの例には、個人、企業、ブランドの、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。それらの名前はすべて架空のものであり、また名称や住所が類似する企業が実在しても、それは偶然に過ぎません。

著作権：

本書に含まれる情報には、サンプル・アプリケーション・プログラムがソース言語の形式で含まれており、様々な、オペレーティング・プラットフォームでのプログラミング技法を示しています。お客様は、これらのサンプル・プログラムが書かれているオペレーティング・プラットフォームでアプリケーション・プログラミング・インターフェースが実行可能となるためのアプリケーション・プログラムを開発、使用、販売または配布もしくは転送する目的のためだけに、サンプル・プログラムを、IBM に対する別途料金を支払うことなく、複製、変更、配布または転送することができます。これらのサンプルは、すべての条件下で十分にテストを行っていません。したがって、IBM は、これらのプログラムの信頼性、実用性または機能について、いかなる保証も負いません。

サンプル・プログラムまたはその改変版の複製物には、全部複製か部分複製かを問わず、次の著作権表示を必ず行うものとします。

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

商標

本書中でアスタリスク (*) を付けて表記されている次のものは、 IBM Corporation の商標です。

ACF/VTAM	IBM
AISPO	IMS
AIX	IMS/ESA
AIX/6000	LAN DistanceMVS
AIXwindows	MVS/ESA
AnyNet	MVS/XA
APPN	Net.Data
AS/400	OS/2
BookManager	OS/390
CICS	OS/400
C Set++	PowerPC
C/370	QBIC
DATABASE 2	QMF
DataHub	RACF
DataJoiner	RISC System/6000
DataPropagator	RS/6000
DataRefresher	S/370
DB2	SP
DB2 Connect	SQL/DS
DB2 Extenders	SQL/400
DB2 OLAP Server	System/370
DB2 Universal Database	System/390
Distributed Relational Database Architecture	SystemView
DRDA	VisualAge
eNetwork	VM/ESA
Extended Services	VSE/ESA
FFST	VTAM
First Failure Support Technology	WebExplorer
	WIN-OS/2

次のものは、他社の商標または登録商標です。

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

Java、Java に関連するすべての商標およびロゴ、および Solaris は、米国ならびに他の国における Sun Microsystems, Inc. の商標または登録商標です。

Tivoli および NetView は、米国ならびに他の国における Tivoli Systems Inc. の商標です。

UNIX は、The Open Group がライセンスしている米国およびその他の国における登録商標です。

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

索引

日本語、数字、英字、特殊文字の順に配列されています。なお、濁音と半濁音は清音と同等に扱われています。

[ア行]

- アウトバウンド名前変換
 - DB2 アプリケーション・リクエスト 22, 75
 - SQL/DS アプリケーション・リクエスト 155
- アプリケーション主導アクセス 4, 48
- アプリケーション・サーバー
 - 資料 vii
- アプリケーション・サーバー、
 - DB2 28, 30, 37, 40, 42, 44, 84, 97
 - インバウンド名前変換 37, 89
 - 機密保護
 - エンド・ユーザー名 37, 89
 - サブシステム 44, 96
 - データベース・マネージャー 42, 94
 - ネットワーク 40, 92
 - システム主導アクセス 32
 - データ表示 44, 97
 - データベース・マネージャー機密保護 42, 94
 - ネットワーク情報 30, 85
 - 2次サーバー 32
 - come-from 検査 37, 89
- アプリケーション・サーバー、
 - OS/400 112, 117
 - エンド・ユーザー名 113
 - 機密保護 113
 - 説明 113
 - データ表示 117
 - ネットワーク情報 112
- アプリケーション・サーバー、
 - OS/400 112, 117 (続き)
 - リモート・データベースの命名 112
 - RU サイズの設定 113
- アプリケーション・サーバー、
 - SQL/DS VM 161
 - インバウンド名前変換 165
 - エンド・ユーザー名 165
 - 機密保護
 - データベース・マネージャー 167
 - ネットワーク 167
 - 説明 162
 - データ表示 169
 - ネットワーク情報 162
- アプリケーション・サーバー、
 - SQL/DS VSE 175, 187
 - 機密保護
 - データベース・マネージャー 184
 - バインド実行時 182
 - ユーザー 182
 - リンク 182
 - 説明 179
 - ネットワーク情報 175
- アプリケーション・リクエスト、
 - DB2 8, 15, 20, 21, 24, 26, 27, 28, 54, 63, 73, 74, 84 (続き)
 - 機密保護
 - エンド・ユーザー名 21, 74
 - サブシステム 27, 83
 - データベース・マネージャー 26, 82
 - ネットワーク 24, 79
 - 通信サブシステム 19, 72
 - データ表示 28, 83
 - 歩調合わせ 20, 73
 - リモート・システム定義 15, 63
 - ローカル・システム定義 9
- アプリケーション・リクエスト、
 - DB2 8, 15, 20, 21, 24, 26, 27, 28, 54, 63, 73, 74, 84 (続き)
 - ローカル・システム定義 (VTAM) 55
 - RU サイズの設定 20, 73
- アプリケーション・リクエスト、
 - OS/400 100, 112
 - 機密保護 107
 - 通信定義 102
 - データ表示 110
 - ネットワーク情報 100
 - 歩調合わせ 106
 - RU サイズの設定 106
- アプリケーション・リクエスト、
 - SQL/DS VM 144, 161
 - 機密保護
 - エンド・ユーザー名 154
 - サブシステム 159
 - データベース・マネージャー 158
 - ネットワーク 155
 - 通信サブシステム 152
 - データ表示 159
 - ネットワーク情報 145
 - 歩調合わせ 153
 - リモート・システム定義 150
 - ローカル・システム定義 145
 - AVS セッション限度考慮事項 153
 - RU サイズの設定 153
- インバウンド名前変換
 - DB2 アプリケーション・サーバー 37, 89
 - SQL/DS、VM アプリケーション・サーバーの 165
- エンド・ユーザー名 21, 37, 74
- アプリケーション・サーバー
 - OS/400 113
 - SQL/DS、VM での 165

エンド・ユーザー名 21, 37, 74 (続き)
アプリケーション・リクエスター
DB2 21, 74
OS/400 107
SQL/DS、VM での 154
DB2 37, 89
オブジェクト名の解決、DB2 36

[カ行]

解決、オブジェクト名、DB2 36
回線記述の作成 103
関係データベース・ディレクトリー、OS/400
項目情報 101
説明 101
関係データベース・ディレクトリー・コマンドの追加
(ADDRDBDIRE) 101
機密保護 21, 24, 26, 27, 37, 40, 42, 44, 74
アプリケーション・サーバー
DB2 サブシステム 44, 96
DB2 データベース・マネージャー 42, 94
OS/400 エンド・ユーザー名 113
SQL/DS データベース・マネージャー 167
SQL/DS、VM サブシステムの 168
アプリケーション・リクエスター
DB2 サブシステム 27, 83
DB2 データベース・マネージャー 26, 82
DB2 ネットワーク 24, 79
OS/400 データベース・マネージャー 108
SQL/DS データベース・マネージャー 158
エンド・ユーザー名
DB2 アプリケーション・サーバー 37, 89
DB2 アプリケーション・リクエスター 21, 74

機密保護 21, 24, 26, 27, 37, 40, 42, 44, 74 (続き)
エンド・ユーザー名 (続き)
OS/400 アプリケーション・リクエスター 107
SQL/DS アプリケーション・リクエスター 154
処理
DB2 アプリケーション・サーバー 37, 89
SQL/DS、VM アプリケーション・サーバーの 165
ネットワーク
DB2 アプリケーション・サーバー 40, 92
DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバー 114
OS/400 アプリケーション・リクエスター 107
SQL/DS アプリケーション・リクエスター 155
SQL/DS、VM アプリケーション・サーバーの 167
come-from 検査、DB2 での 37, 89
OS/400 システム 108
SQL/DS サブシステム 159
グループ制御システム (GCS) 133
交換、メッセージ
DB2 9, 55
構成についての考慮事項
パスワード変更 53
構成リストの作成 106

[サ行]

サービス・クラス
作成 104
OS/400 記述 104
資源アダプター、VM 133
システム機密保護、OS/400 108
システム主導アクセス 4, 48
処理
オプション、DB2 7, 51
省略時許可、AS/400 110

資料
アプリケーション・サーバー vii
AS/400 vii
DRDA vii
MVS vii
OS/400 vii
SQL/DS vii
VM vii
VSE vii
制御装置の記述の作成 104
整合資源回復 (CRR) 133
整合資源回復 (CRR) サーバー 133
静的 SQL 42, 95
セッション
限度、システム主導アクセス 36
限度、VM での SQL/DS 153
接続 51
システム主導アクセス・サーバー 36
タイプ
DB2 分散データベース 7, 51
VM 分散データベースでの SQL/DS 140
接続機密保護のレベル 183
装置記述の作成 105

[タ行]

通信 15, 16, 17, 18, 19, 64, 66, 68, 69, 71
サブシステム
DB2 アプリケーション・リクエスター 19, 72
OS/400 アプリケーション・リクエスター 102
データベース表、DB2
SYSIBM.IPNAMES 71
SYSIBM.LOCATIONS 64
SYSIBM.LUMODES 68
SYSIBM.LUNAMES 66
SYSIBM.MODESELECT 69
SYSIBM.SYSLOCATIONS 15
SYSIBM.SYSLUMODES 17
SYSIBM.SYSLUNAMES 16
SYSIBM.SYSMODESELECT 18
SYSIBM.SYSUSERNAMES 18
SYSIBM.USERNAMES 69

通信 15, 16, 17, 18, 19, 64, 66, 68, 69, 71 (続き)

ディレクトリー、VM 環境 132, 150

フロー、SQL/DS VSE 172

VM フローの例 135

データ表示

DB2 アプリケーション・サーバー 44, 97

DB2 アプリケーション・リクエスト 28, 83

OS/400 アプリケーション・サーバー 117

OS/400 アプリケーション・リクエスト 110

SQL/DS アプリケーション・リクエスト 159

SQL/DS、VM アプリケーション・サーバーの 169

データベース名ディレクトリー 172

データベース・マネージャー機密保護

DB2 アプリケーション・サーバー 42, 94

DB2 アプリケーション・リクエスト 26, 82

OS/400 アプリケーション・リクエスト 108

SQL/DS アプリケーション・リクエスト 158

SQL/DS、VM アプリケーション・サーバーの 167

透過サービス・アクセス機能 (TSAF) 133

動的 SQL 42, 95

CURRENTPACKAGESET 53

[ナ行]

ネットワーク機密保護

DB2 アプリケーション・サーバー 40, 92

DB2 アプリケーション・リクエスト 24, 79

ネットワーク機密保護 (続き)

DB2 ユニバーサル・データベース (AS/400 版) アプリケーション・サーバー 114

SQL/DS アプリケーション・リクエスト 155

SQL/DS、VM アプリケーション・サーバーの 167

ネットワーク情報

DB2 アプリケーション・サーバー 30, 85

OS/400 アプリケーション・サーバー 112

OS/400 アプリケーション・リクエスト 100

SQL/DS VSE アプリケーション・サーバー 175

SQL/DS アプリケーション・リクエスト 145

SQL/DS、VM アプリケーション・サーバーの 162

ネットワーク属性の変更コマンド 103

[ハ行]

パッケージ

DB2 アプリケーション・サーバー機密保護 42, 94

SQL/DS データベース・マネージャー機密保護 167, 185

分散作業単位

アプリケーション主導アクセス 4, 48

システム主導アクセス 4, 48

分散データベース

アクセス、DB2 アプリケーション・リクエスト 8, 54

DB2 接続 4, 48

歩調合わせ 20, 73

カウント

DB2 アプリケーション・リクエスト 20, 73

OS/400 アプリケーション・サーバー 113

OS/400 アプリケーション・リクエスト 106

歩調合わせ 20, 73 (続き)

カウント (続き)

SQL/DS アプリケーション・リクエスト 153

[マ行]

命名、リモート・データベースの、OS/400 112

メッセージ

交換、DB2 9, 55

モード記述の作成 105

[ラ行]

リモート作業単位

DB2 接続 4, 49

例

権限の認可、OS/400 109

ADDRDBDIRE コマンド 101

AVS ゲートウェイ定義 146

CMS 通信ディレクトリー項目 184

DB2 VTAM APPL ステートメント 12, 59

VM comdir 項目 157

VM 通信フローの例 135

ローカル・システム

定義、DB2 9

定義、DB2 (VTAM) 55

SQL/DS アプリケーション・リクエスト 145

ローカル・データベースの命名、

OS/400 101

[数字]

2 次サーバー 5, 32, 49

A

ACF/VTAM 172

ALREADYV ステートメント 148

APPCPASS ステートメント 156

APPC/VM サポート 132

APPC/VTAM サポート 131

APPL ステートメント
DB2 の例 12, 59
SQL/DS 例 146
APPN (拡張対等通信ネットワークキ
ング機能)
ロケーション・リストの作成
105
AS/400
資料 vii
AUTHENTICATION=CLIENT 52
AVS
セッション限度の考慮事項 153
VM の構成要素 131
AXE 172

B

BSDS (ブートストラップ・データ・
セット) の更新 10, 57

C

CCSID (コード化文字セット識別コー
ド)
DB2 の省略時値 28, 83
OS/400 省略時値 110
CHARNAME 141, 159, 169
CHGNETA コマンド 103
CICS LU 6.2 セッション 175
CICS(ISC) 171
CLI/ODBC アプリケーション
CURRENTPACKAGESET 53
CMS 通信ディレクトリー
機密保護 157
RDB_NAME のカタログ 150
comdir
項目例 157
CMS 150
VM 132
come-from 検査
DB2 アプリケーション・サーバ
ー 37, 89
CRTCFGL コマンド 106
CRTCOSD コマンド 104
CRTCTLAPPC コマンド 104
CRTCTLHOST コマンド 104
CRTDDMTCPA コマンド 116

CRTDEVAPPC コマンド 105
CRTLINETH コマンド 103
CRTLINS DLC コマンド 103
CRTLINTRN コマンド 103
CRTLINX25 コマンド 103
CRTMODD コマンド 105
CURRENTPACKAGESET 53

D

DB2 LINKNAME 表 15, 64
DB2 ユニバーサル・データベース
(AS/400 版)
ネイティブ TCP/IP 接続 103
TCP/IP 接続のセットアップ 102
DB2 ユニバーサル・データベース
(OS/390 版)
検査済みの TCP/IP 52
DYNAMICRULES(BIND) 53
DBNAME ディレクトリー 172
DDF レコード 10, 56
DRDA
資料 vi
DRDA サーバー
資料 vii

G

GCS (グループ制御システム) 133

I

IDENT 134

L

LINKNAME 表 15, 64

M

MVS
資料 vii
MVS (多重仮想記憶)、DB2 アドレス
空間 2, 46

O

ODBC アプリケーション
CURRENTPACKAGESET 53

OS/400
資料 vii
通信の活動化 106
ネットワーク属性 103

R

RDB_NAME
CMS 通信ディレクトリー 150
RELOAD PACKAGE コマンド 158
RESID NAMES ファイル
SQL/DS、VM での 163
RESID (TPN) 163
RU サイズの設定
DB2 アプリケーション・リク
エスター 20, 73
OS/400 アプリケーション・サー
バー 113
OS/400 アプリケーション・リク
エスター 106
SQL/DS アプリケーション・リク
エスター 153

S

SET CURRENT PACKAGESET 53
SQL 解説資料 vii
SQL (構造化照会言語) 32, 33
オブジェクト、DB2 機密保護
43, 95
オブジェクト、SQL/DS データベ
ース・マネージャー機密保護
168, 185
静的 42, 95
動的 42, 95
DB2 2 次サーバー
オブジェクト名 33
相違 32
SQLINIT 140
SQL/DS
資料 vii
SQL/DS VM
処理オプション
PROTOCOL 140
SQL/DS VSE
CICS LU 6.2 セッション 175

SYSIBM.IPNAMES 表 71
SYSIBM.LOCATIONS 表 64
SYSIBM.LUMODES 表 68
SYSIBM.LUNAMES 表 66
SYSIBM.MODESELECT 表 69
SYSIBM.SYSLOCATIONS 表 15
SYSIBM.SYSLUMODES 表 17
SYSIBM.SYSLUNAMES 表 16
SYSIBM.SYSMODESELECT 表 18
SYSIBM.SYSUSERNAMES 表 18
SYSIBM.USERNAMES 表 69

T

TCP/IP

機密保護、AS/400 116
検査済みの機密保護 52
DRDA 用のウェルノウン・ポート
446 113

TPN (トランザクション・プログラム
名)

DB2 SYSIBM.LOCATIONS 表
64

DB2 SYSIBM.SYSLOCATIONS
表 15

DRDA 省略時値、OS/400 102
OS/400 アプリケーション・サー
バー 113

SQL/DS、VM RESID での 163

TSAF (透過サービス・アクセス機
能) 133

V

VM

資源アダプター 133

資料 vii

通信ディレクトリー
(comdir) 132

ディレクトリー項目 157

DRDA 構成要素 131

VRYCFG コマンド 106

VSE

資料 vii

VTAM 12, 15, 59, 62

機密保護オプション 148

APPL ステートメント

省略時セッション限度 15, 62

VTAM 12, 15, 59, 62 (続き)

APPL ステートメント (続き)

DB2 の例 12, 59

VM の SQL/DS で使用される

パラメーター 146

DRDA、役割 134

W

WRKCFGSTS コマンド 106

X

XPCC 172

IBM と連絡をとる

技術上の問題がある場合は、時間をとって「問題判別の手引き」に定義されている処置を検討し、それらの提案を実行した後で、DB2 顧客サービスに連絡をとってください。この資料には、DB2 顧客サービスがお客さまを支援するために必要とする情報が説明されています。

製品情報

以下の情報は英語で提供されます。内容は英語版製品に関する情報です。

<http://www.ibm.com/software/data/>

DB2 World Wide Web ページには、ニュース、製品説明、研修スケジュールなどの DB2 に関する最新情報が提供されています。ただし提供されている情報は英語です。

<http://www.ibm.com/software/data/db2/library/>

「DB2 Product and Service Technical Library」では、よくされる質問 (FAQ)、修正内容、資料、および最新の DB2 技術情報などの情報へのアクセスが提供されています。

注: この情報のご提供は英語のみとなりますのでご注意ください。

<http://www.elink.ibm.com/pbl/pbl/>

「International Publications」注文用 Web サイトでは、マニュアルの注文方法についての情報を提供しています。ただし、提供されている情報は英語です。

<http://www.ibm.com/education/certify/>

IBM の「Professional Certification Program」Web サイトでは、DB2 を含むさまざまな IBM 製品の認証テストの情報を提供しています。ただし、提供されている情報は英語です。

<ftp.software.ibm.com>

匿名でログオンしてください。ディレクトリー /ps/products/db2 には、DB2 および多数の他製品に関連したデモ、修正プログラム、情報、およびツールがあります。ただし、提供されている情報は英語です。

comp.databases.ibm-db2, bit.listserv.db2-l

これらのインターネット・ニュースグループは、ユーザーが DB2 製品に関する自分の経験について話し合うために利用できます。ただし、提供されている情報は英語です。

CompuServe: GO IBMDB2

このコマンドを入力すると、IBM DB2 Family forum にアクセスできます。すべての DB2 製品が、このフォーラムでサポートされています。ただし、提供されている情報は英語です。

米国以外の国で IBM に連絡する方法については、*IBM Software Support Handbook* の Appendix A を参照してください。この資料にアクセスするには、Web ページ: <http://www.ibm.com/support/> にアクセスし、ページの最下部にある「IBM Software Support Handbook」リンク・ボタンを選択します。

注: 国によっては、IBM が承認している販売業者が、IBM サポート・センターの代わりにそれら販売業者のサポート・センターに連絡する場合があります。



Printed in Japan

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