

CA Chorus™ for DB2 Database Management

サイト準備ガイド
バージョン 03.0.00、第 2 版



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、
(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されている CA ソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただし CA のすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CA に文書で証明する責任を負いません。

準拠法により認められる限り、CA は本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CA はお客様または第三者に対し責任を負いません。CA がかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者は CA です。

「制限された権利」のもとの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2013 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA ACF2™ for z/OS (CA ACF2)
- CA Chorus™ (CA Chorus)
- CA Chorus™ for DB2 Database Management (CA Chorus for DB2 Database Management)
- CA Chorus™ Infrastructure Management for Networks and Systems (CA Chorus Infrastructure Management)
- CA Chorus™ Software Manager (CA CSM)
- CA Common Services for z/OS (CA Common Services for z/OS)
- CA Compliance Manager for z/OS (CA Compliance Manager)
- CA Detector® for DB2 for z/OS (CA Detector)
- CA Insight™ Database Performance Monitor for DB2 for z/OS (CA Insight DPM)
- CA OPS/MVS® Event Management and Automation (CA OPS/MVS)
- CA Plan Analyzer® for DB2 for z/OS (CA Plan Analyzer)
- CA RC/Migrator™ for DB2 for z/OS (CA RC/Migrator)
- CA RC/Query® for DB2 for z/OS (CA RC/Query)
- CA RC/Update™ for DB2 for z/OS (CA RC/Update)
- CA Subsystem Analyzer for DB2 for z/OS (CA Subsystem Analyzer)
- CA Top Secret® for z/OS (CA Top Secret)
- CA Vantage™ Storage Resource Manager (CA Vantage)

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

マニュアルの変更点

以下のリストは、このガイドの初版以来に加えられた変更について説明しています。

[システム要件 \(P. 15\)](#) -- ヒープメモリ要件を削除し、特殊プロセッサ推奨事項を追加しました。

[サーバ要件 \(P. 33\)](#) - ヒープメモリ要件を更新し、ヒープサイズを変更するパラメータを示し、値は実際のストレージを表すことを示し、ヒープメモリ要件をこの新規トピックに移動しました。

[ソフトウェア要件 \(P. 13\)](#) - ブラウザサポートを明確にしました。

目次

第 1 章: 概要	9
第 2 章: 一般的な前提条件について	13
ソフトウェア要件.....	13
システム要件.....	15
ターゲット ライブラリ	15
配布ライブラリ.....	16
ポート要件.....	16
第 3 章: セキュリティ要件について	19
インストーラ セキュリティ 権限.....	19
ユーザ権限.....	21
(オプション) EXPLAIN コマンドでセカンダリ許可 ID 使用状況を承認する.....	24
スターティッドタスク権限.....	30
サーバ要件.....	33
PassTicket の構成.....	34
CA Chorus システム用の PassTicket 設定.....	35
CA Chorus システム用のサンプル PassTicket 設定.....	36
サンプル: CA ACF2 を使用して CA Chorus for DB2 Database Management PassTicket を設定.....	38
サンプル: CA Top Secret を使用して CA Chorus for DB2 Database Management PassTicket を設定.....	43
サンプル: RACF を使用して CA Chorus for DB2 Database Management PassTicket を設定.....	48
CA Chorus for DB2 Database Management 用の RRSAF 許可.....	53
サンプル: CA ACF2 を使用して RRSAF リソース許可を作成.....	54
サンプル: CA Top Secret を使用して RRSAF リソース許可を作成.....	55
サンプル: RACF を使用して RRSAF リソース許可を作成.....	56
第 4 章: 設定変更について	59
Xnet 設定の更新.....	59
CA Insight DPM 設定の更新.....	61

付録 A: パフォーマンスの向上 63

付録 B: CA Chorus for DB2 Database Management インストール ワークシート 65

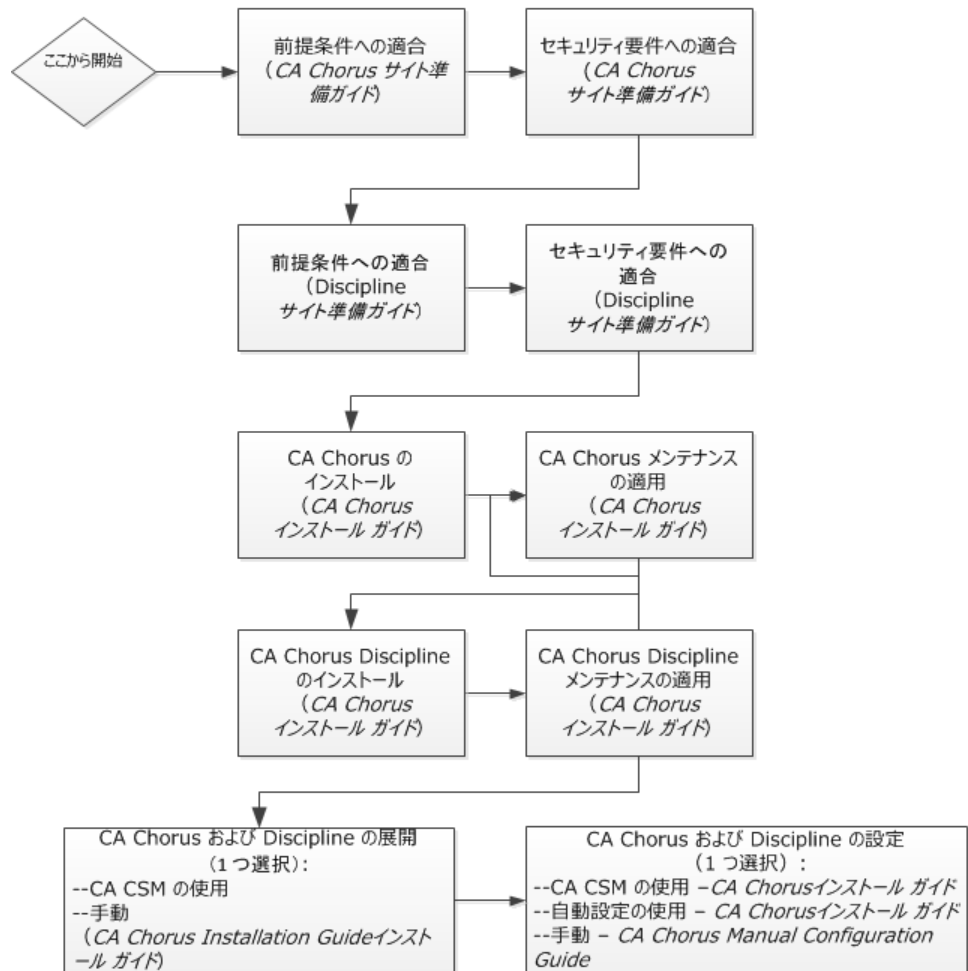
第 1 章：概要

このガイドは、「インストールガイド」で説明されているインストール、配備、および設定タスクを開始する前にシステム プログラマおよびセキュリティ管理者が実行できるタスクの詳細を示しています。以下の図は、CA Chorus およびディシプリンインストール、展開、および設定プロセス、および使用するガイドの高レベル概要を示しています。

重要: CA Chorus およびそのディシプリンをインストールするには、CA Chorus Software Manager を使用する必要があります。

注: ディシプリン「サイト準備ガイド」からの作業を示すボックスについては、インストールするディシプリンごとにこの手順を繰り返します。

インストールプロセスの仕組み



CA Chorus およびそのディシプリンのインストール、展開、および設定を行うには、以下の手順に従います。

1. 「CA Chorus サイト準備ガイド」で説明されているソフトウェア、システム、ポート、およびその他の前提条件を満たします。
2. 「CA Chorus サイト準備ガイド」で説明されているセキュリティ要件を満たします。
3. 適切なディシプリンの「サイト準備ガイド」で説明されているソフトウェア、システム、ポート、およびその他の前提条件を満たします。インストールするディシプリンごとにこの手順を繰り返します。
4. 適切なディシプリンの「サイト準備ガイド」で説明されているセキュリティ要件を満たします。インストールするディシプリンごとにこの手順を繰り返します。
5. 「CA Chorus インストールガイド」で説明されている CA CSM を使用して、CA Chorus および適用可能なディシプリンをインストールします。この手順には、SMP/E を使用した CA Chorus ソフトウェアの取得 (z/OS システムへのトランスポート) およびインストールが関連します。インストールプロセスにより CSI 環境が作成され、RECEIVE、APPLY、および ACCEPT SMP/E の手順が実行されます。ソフトウェアはカスタマイズされていません。
6. CA CSM または手動のプロセスを使用して、CA Chorus および適用可能なディシプリンを展開します。「CA Chorus インストールガイド」は両方のメソッドについて説明しています。

この手順により、ターゲットのライブラリが別のシステムや LPAR にコピーされます。

重要: CA CSM からの展開では、CA Chorus とディシプリンを同時に配備する必要があります。たとえば、CA Chorus、DBA、および Security をインストールした後、CA Chorus および DBA のみを展開する方法はサポートされていません。

重要: CA CSM Software Configuration Service を使用するには、CA CSM 展開が必要です。

7. CA Chorus およびディシプリンを設定します。この手順により、カスタマイズされたロードモジュールが作成され、CA Chorus ソフトウェアが実行可能状態に移行されます。以下の方法のいずれかで製品を設定できます。

注: 最初の 2 つの方法のいずれかをお勧めします。製品を設定するための最も効率的な方法です。

CA CSM

このメソッドでは、製品の設定にウィザードに基づく CA CSM ツールを使用できます。

「インストールガイド」には、このメソッド用の CA Chorus およびディシプリン手順が含まれます。

自動設定

この方法では、1 つのバッチ ジョブ (ETJICUST) と 1 つの設定ファイルを編集します。その後、Java プログラムは適切なメンバに変更を伝達します。次に、手動で各ジョブをサブミットします。このオプションでは、プラットフォームおよびディシプリンを同時に設定することをお勧めします。

「インストールガイド」には、このメソッド用の CA Chorus およびディシプリン手順が含まれます。

手動

この方法では、各設定ジョブの編集および実行を手動で行います。

この方法の場合、「*Manual Configuration Guide*」を使用して、CA Chorus およびそのディシプリンを設定します。

第 2 章: 一般的な前提条件について

この章は、CA Chorus for DB2 Database Management インストール、配備、および設定タスクを開始する前にシステム プログラマが完了する必要のあるすべてのタスクについて説明しています。

このセクションには、以下のトピックが含まれています。

[ソフトウェア要件 \(P. 13\)](#)

[システム要件 \(P. 15\)](#)

[ポート要件 \(P. 16\)](#)

ソフトウェア要件

CA Chorus for DB2 Database Management には、以下のソフトウェアが必要です。

注: CA Chorus の前提条件とセキュリティ要件をすでに満たしている必要があります。

- CA Technologies ソフトウェア
 - CA Chorus バージョン 3.0

初期サイト インストールについては、「*CA Chorus* インストール ガイド」に説明されているタイミングで CA Chorus およびディシプリンをインストールします。

既存の CA Chorus インスタンスにディシプリンをインストールしている場合、ディシプリンのバージョンが CA Chorus バージョンに一致することを確認します。

注: CA Chorus インストールの詳細については、「*CA Chorus* サイト 準備ガイド」および「*CA Chorus* インストールガイド」を参照してください。

- 以下の CA Database Management Solutions for DB2 for z/OS 製品で r15 以上

重要: これらの製品に対してすべての現在の CA Chorus FIXCAT 保守を適用します。

- CA Detector
- CA Insight DPM
注: CA Chorus Infrastructure Management がインストールされている場合、CA Insight DPM がすでにインストールされています。
- CA Plan Analyzer
- CA RC/Migrator
- CA RC/Query
- CA RC/Update
- CA Subsystem Analyzer
- 一般的なコンポーネント: Xmanager、Xnet Batch Processor、Object Framework Services (OFS) および CA Chorus DBA Services (FMID EU9/CHRDBM)

注: CA Chorus Infrastructure Management がインストールされている場合、Xmanager および Xnet がすでにインストールおよび設定されています。

注: これらの製品とコンポーネントのインストールの詳細については、CA Database Management Solutions for DB2 for z/OS の「インストールガイド」および「*Implementation Guide*」を参照してください。CA Chorus for DB2 Database Management と統合するためにこれらの製品の設定を更新する詳細については、このガイドの後の章を参照してください。

- IBM ソフトウェア
 - IBM DB2 V8 New Function Mode (NFM)、DB2 9、または DB2 10
 - Resource Recovery Services Attachment 機能 (RRSAF) を管理するための IBM Resource Recovery Services (RRS) for z/OS

注: RRSAF は CA Chorus for DB2 Database Management が使用する DB2 アタッチ機能です。DB2 システム用の RRS の実装の詳細については、IBM Resource Recovery Services のマニュアルを参照してください。

- 各ユーザに必要な PC ソフトウェア
 - Adobe Flash Player 9.0.124 以降
 - バージョン 3.0 のリリースで、CA Chorus は Microsoft Windows Internet Explorer 9 および Mozilla Firefox 13 ~ 19 をサポートします。新規ブラウザがリリースされた場合、当社はそれを検証し、[CA Chorus 製品ページ](#)の「推奨ドキュメント」に互換性を示します。
 - 注: CA Chorus は、最低 1024×768 の画面解像度を必要とします。画面解像度がこの要件を満たさない場合、全画面モード（ほとんどのブラウザでは F11）を使用して、表示にスクロールバーが含まれるようにします。

システム要件

ユーザのサイトが以下のシステム要件を満たしていることを確認します。

ディスク

CA Chorus for DB2 Database Management には約 251 トラック必要です。

注: インストールが正常に完了した後、ダウンロードおよび REL ファイルは自動的に削除されます。

プロセッサ

CA Chorus は z/OS 上で JavaVM 環境を使用します。従って、パフォーマンスを最適化し、リソースを有効に活用するために、専用のプロセッサを使用することを強くお勧めします。

ターゲット ライブラリ

以下の表に、CA Chorus for DB2 Database Management ターゲット ライブラリのデータセットスペース要件をトラック数で示します。

データセット名	トラック数
CE3KJCL	10
CE3KPARM	10
CE3KXML	10
CE3KZFS (zFS ディレクトリ)	750

注: CA CSM で zFS データ セットが作成されます。

配布ライブラリ

以下の表に、CA Chorus for DB2 Database Management 配布ライブラリのデータセットスペース要件をトラック数で示します。

データセット名	トラック数
AE3KJCL	10
AE3KPARM	10
AE3KXML	10
AE3KZFS (zFS ディレクトリ)	750

ポート要件

実行中の各 Xnet (実行マネージャ ネットワーク) サーバに対して、CA Chorus for DB2 Database Management に TCP/IP ポート指定および対応する接続定義が必要です。

Xnet 通信サーバ内のリスナプロセスは、このポートを使用して CA Chorus for DB2 Database Management のデータ ソース ハンドラ (DSH) から Xnet への接続を受け入れます。Xnet は、すべての CA Database Management 製品ソリューション for DB2 for z/OS に対して共有通信サブシステムを提供します。Xnet が開始されると、ポートがリスニングソケットにバインドされ、CA Chorus クライアントから接続が受信されます。

ポート番号は `your_db2tools_hlq.CDBASAMP` 内の `PXNPROC JCL` で指定されます。この値は通常、インストールされた CA Database Management Solutions for DB2 for z/OS のインストール後処理中にカスタマイズされます。CA Chorus for DB2 Database Management 設定中に DB2 サブシステム接続を定義するためにこの同じポート値を使用します。

ネットワーク管理チームに問い合わせ、使用予定のポートが利用可能であることを確認してください。

注: CA Chorus for DB2 Database Management 設定の詳細については、「CA Chorus Manual Configuration Guide」を参照してください。

詳細情報:

[Xnet 設定の更新](#) (P. 59)

第 3 章: セキュリティ要件について

このセクションには、以下のトピックが含まれています。

[インストーラセキュリティ権限 \(P. 19\)](#)

[ユーザ権限 \(P. 21\)](#)

[スターティッドタスク権限 \(P. 30\)](#)

[サーバ要件 \(P. 33\)](#)

[PassTicket の構成 \(P. 34\)](#)

[CA Chorus for DB2 Database Management 用の RRSAF 許可 \(P. 53\)](#)

インストーラセキュリティ権限

インストール処理を開始する前に、CA Chorus for DB2 Database Management インストーラ ユーザ ID に以下のセキュリティ権限が定義されていることを確認します。

- USS (UNIX System Services) :
 - zFS データ セットを操作する機能。この機能は、FSACCESS クラス内の適切なエンティティへの UPDATE 権限を必要とします。
 - FSACCESS では、ZFS ファイル システム コンテナ (つまりデータ セット) へのアクセスを確保できます。リソース名が ZFS ファイル システム名になります。
 - たとえば、OMVS.ZFS.WEBSRV.TOOLS という名前の ZFS ファイル システムを定義し、ディレクトリ内のファイルでディレクトリ U1 および U2 を作成した場合、ユーザが ZFS ファイル システム内のディレクトリ U1 および U2 へのアクセスを試みるとクラス FSACCESS のリソース OMVS.ZFS.WEBSRV.TOOLS のリソース確認が発生します。詳細については、適用可能なセキュリティ製品ドキュメントを参照してください。
 - 有効な OMVS 定義。
 - スーパーユーザ権限。
 - FACILITY クラス内の以下のリソースへの READ アクセス
 - BPX.SUPERUSER
 - BPX.FILEATTR.APF

- BPX.FILEATTR.PROGCTL
- BPX.FILEATTR.SHARELIB
- BPX.SERVER
- UNIXPRIV リソース クラスの SUPERUSER.FILESYS.PFSCPL プロファイル
- z/OS :
 - インストールデータセットおよびライブラリから作成、更新および実行する権限。
 - 外部セキュリティ マネージャ (CA ACF2、CA Top Secret または IBM RACF) データベースを操作するコマンドを実行する権限。
- DB2 では、インストーラは必要な製品 (CA Detector、CA RC/Migrator など) に対する以下のタスクを実行するために SYSADM 権限が必要です。
 - DB2 カタログおよび製品カスタマイズタスクを実行します (サンプルメンバは *your_db2tools_hlq.CDBASAMP* に置かれています)
 - *your_db2tools_hlq.CDBAPARM* 内のグローバルおよび製品固有の parmlib メンバを編集します。

ユーザ権限

以下の手順を実行して、CA Chorus for DB2 Database Management ユーザに CA Chorus での作業権限を付与します。

注: CA Chorus または別のディシプリンのインストールの準備の一部として手順をすでに完了している場合は、このディシプリンに対して再定義する必要はありません。

1. ユーザの z/OS UNIX System Services (USS) リソースへのアクセスを承認します。各ユーザに OMVS セグメントが定義されていることを確認します。これらのセグメントには、ホームディレクトリ、デフォルトシェルプログラム、UID、および GID またはグループなどがあります。

注: UID に HOME ディレクトリへの READ/WRITE アクセスがあることを確認します。サンプルコマンドについては、「CA Chorus サイト準備ガイド」を参照してください。

2. 以下のリソースに READ アクセスを定義して、CA Chorus for DB2 Database Management ユーザの CA Chorus リソースへのアクセスを承認します。
 - CHORUS.ROLE.DB2DBA - CA Chorus for DB2 Database Management データへのユーザアクセスを制御します。
 - CHORUS.SETTINGS.KNOWLEDGECENTER - Knowledge Center コンポーネントのドキュメントインデックス機能へのアクセスを制御します。
 - CHORUS.SETTINGS.AUTOREFRESH - 自動更新オプションへのユーザアクセスを制御します。

注: CA ACF2、CA Top Secret および IBM RACF コマンドのサンプルについては、「CA Chorus サイト準備ガイド」を参照してください。

3. (オプション) セカンダリ許可 ID リソース検証用の EXPLAIN リソース権限を作成します。このユーザ権限が必要となるのは、セカンダリ許可 ID が SQL ステートメントの DB2 EXPLAIN を実行するために使用される場合です。DBA Command Manager for DB2 モジュールでは、EXPLAIN 処理を実行するために、プライマリおよびセカンダリ ID を使用できます。セカンダリ許可 ID の使用は任意です。ただし、ユーザが SQL が参照するオブジェクトを所有しない場合、セカンダリ許可 ID の使用が役立つこともあります。

注: ユーザが CA Plan Analyzer のインストールおよび設定中にすでに EXPLAIN コマンド認可をセットアップしている場合でも、これらのリソース許可が CA Chorus for DB2 Database Management ユーザに対して定義される必要があります。CA Chorus for DB2 Database Management からの EXPLAIN は、Call Attachment 機能 (CAF) の代わりに DB2 RRSF を使用します。EXPLAIN リソース権限を作成する詳細については、「[セカンダリ許可 ID の使用の許可 \(P. 24\)](#)」を参照してください。CA ACF2、CA Top Secret、および IBM RACF 用のサンプルコマンドが提供されています。

4. <chorus-install-home>/config 内の db2tools.cfg ファイルへの READ アクセスを定義します。

注: このファイルはオブジェクトマイグレータ機能の CA Chorus for DB2 Database Management 設定中に作成されます。自動設定オプションを使用してこのファイルを設定する詳細については、「[CA Chorus インストールガイド](#)」を参照してください。このファイルを手動で設定する詳細については、「[CA Chorus Manual Configuration Guide](#)」を参照してください。

5. 以下の製品およびコンポーネントに対する特定のプランに対して DB2 EXECUTE 許可を付与します。
 - CA Detector
 - CA Insight DPM
 - CA Plan Analyzer
 - CA RC/Migrator
 - CA RC/Query
 - CA RC/Update
 - CA Subsystem Analyzer
 - 一般的な機能
 - Batch Processor
 - オブジェクトフレームワーク サービス (OFS)
 - CA Chorus OFS エージェント

注: Product Authorization Facility を使用して DB2 EXECUTE 権限を付与する詳細については、「*CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide*」を参照してください。

6. 以下のインストールデータセットおよびライブラリに READ アクセスを定義して、ユーザが JCL を実行してバッチ レポートを生成するのを許可します。
 - *your_chorus_hlq.CETJOPTV*
 - *your_chorus_hlq.CETJEZTR*

注: これらのデータセットは、「*CA Chorus インストールガイド*」で説明されているとおり CA Chorus インストール中に作成されます。

(オプション) EXPLAIN コマンドでセカンダリ許可 ID 使用状況を承認する

この手順は、CA Chorus for DB2 Database Management ユーザのみに適用されます。EXPLAIN 機能はこのディシプリンに固有です。

DB2 Command Manager 機能用の DBA では、プライマリおよびセカンダリ許可 ID を使用して、SQL ステートメントの DB2 EXPLAIN を実行できます。DB2 はユーザ許可 ID に基づいてユーザ アクセス許可を制御します。これには一連の権限が含まれます。ユーザはすべてプライマリ許可 ID を持ちます。セカンダリ許可 ID はオプションで、ユーザに対する追加の特権を含めることができます。この許可 ID は、SQL が参照するオブジェクトをユーザが所有しない場合に役立ちます。

セカンダリ許可 ID が EXPLAIN コマンドを実行するのに使用される場合、リソース確認がアクティブなセキュリティ製品に対して発行されます。この確認は、ユーザが別のユーザの代わりに EXPLAIN コマンドを実行する権限を持つことを検証します。このオプションをサポートするには、アクティブなセキュリティ製品を使用してユーザに対してリソース権限を作成します。リソース権限は、ユーザが別のプライマリ許可 ID を使用して EXPLAIN コマンドを実行することを許可します。ユーザがこのタイプのアクションの権限を持たない場合、セキュリティ製品はリクエストを拒否し、EXPLAIN レポートは生成されません。

このリソース権限は以下のように表示されます。

```
CADB2: CONNECT.EXPLAIN.pauthid
```

pauthid

ユーザが EXPLAIN に対して使用するプライマリ DB2 許可 ID を表します。

注: インストールおよび設定中にすでに EXPLAIN コマンド許可をセットアップしている場合でも、これらのリソース権限を CA Chorus for DB2 Database Management ユーザに対して定義してください。CA Chorus for DB2 Database Management からの EXPLAIN は、Call Attachment 機能 (CAF) の代わりに DB2 Resource Recovery Services Attachment 機能 (RRSAF) を使用します。

CA ACF2、CA Top Secret、または IBM RACF 内の機能に従って、ユーザがセカンダリ許可 ID を使用して EXPLAIN コマンドを実行することを許可します。

- CA ACF2 でセカンダリ許可 ID の使用状況を承認
- CA Top Secret でセカンダリ許可 ID の使用状況を承認
- IBM RACF でセカンダリ許可 ID 使用状況を承認

詳細情報:

[CA Chorus for DB2 Database Management 用の RRSAF 許可 \(P. 53\)](#)

CA ACF2 でセカンダリ許可 ID の使用状況を承認

この手順を使用して、ユーザが別のオブジェクト所有者の許可 ID を使用して EXPLAIN ステートメントを実行することを許可します。このアクセスなしには、ユーザは SQL が参照するオブジェクトの所有者でないかぎり、EXPLAIN コマンドを実行できません。

注: この手順のコマンドはサンプルです。これらのコマンドの使用の詳細については、「*CA ACF2 Administration Guide*」を参照してください。

以下の手順に従います。

1. 以下のコマンドを入力して、ビューを該当するシステムに設定します。

```
SET C(GSO) SYSID(sysid)
```

sysid

特定のシステムに CA ACF2 を持つどの GSO レコードが使用のために選択されるかを決定します。

ビューが適用可能なシステムに設定されます。

2. CLASMAP レコードに CADB2 リソースおよび CDB リソース タイプを挿入します。

```
INSERT CLASMAP.CADB2 ENTITYLN(entitylength) POSIT(value)
```

```
RESOURCE (CADB2) -
```

```
RSRCTYPE (CDB)
```

ENTITYLN *entitylength*

指定された SAF クラスのエンティティ長を指定します。この値により、クラス記述子テーブル (CDT) を使用する必要がなくなります。ゼロの値により、CA ACF2 は内部 CLASMAP 定義を検索します。ゼロでない値により、GSO CLASMAP が使用されます。結果として生じる CLASMAP レコード (GSO または内部) が RSRCTYPE および ENTITYLN に対して使用されます。結果として生じる ENTITYLN がゼロの場合、CA ACF2 は IBM のデフォルトの長さである 39 を割り当てます。

デフォルト : 0

POSIT 値

ビットテーブル内で確認されるビット値を指定して、RACROUTE 呼び出しが発行されない場合にクラスがアクティブかどうかを決定します。

カスタマ定義リソース クラスに対する有効な値は 19-56 および 128-527 です。

IBM 定義リソース クラスに対する有効な値は 0-18、57-127、および 528-1023 です。IBM クラスに対する POSIT 値は自動的に割り当てられます。これらの値をコーディングする必要はありません。コーディングする場合、この値は IBM に割り当てられた値に一致する必要があります。POSIT() のコーディングが許可され、IBM 定義値が代用されます。IBM リソース クラスおよび割り当てられた POSIT 値の完全なリストについては、IBM のドキュメント「z/OS Security Server RACROUTE マクロ解説書」を参照してください。

注: このフィールドの値が NULL またはデフォルトの場合は、CLASMAP レコードが表示されても表示されません。

リソースが挿入されます。

3. CLASMAP レコードをリフレッシュします。

```
F ACF2,REFRESH(CLASMAP),SYSID(sysid)
```

変更が実装されます。

4. ユーザが所有者の許可 ID を使用することを許可します。

```
SET RESOURCE(CDB)
```

```
RECKEY CADB2 ADD(CONNECT.EXPLAIN.pauthid UID(logonid) ALLOW)
```

pauthid

ユーザが DB2 EXPLAIN 処理で使用するプライマリ DB2 許可 ID を表します。

logonid

所有者の許可 ID へのアクセスを必要とするログオン ID (ユーザ) を指定します。

ユーザが所有者の許可 ID を使用するように設定されます。

5. CDB レコードをリフレッシュします。

```
F ACF2,REFRESH(CDB)
```

変更が実装されます。

ユーザはセカンダリ許可 ID で EXPLAIN コマンドを実行できます。加えて、ユーザは CA Chorus for DB2 Database Management で作業するアクセス権があります。

CA Top Secret でセカンダリ許可 ID の使用状況を承認

この手順を使用して、ユーザが別のオブジェクト所有者の許可 ID を使用して EXPLAIN ステートメントを実行することを許可します。このアクセスなしには、ユーザは SQL が参照するオブジェクトの所有者でないかぎり、EXPLAIN コマンドを実行できません。

以下の手順で、Resource Descriptor Table (RDT) には、CA Top Secret に識別されるすべての動的および事前定義済みリソースが含まれます。

注: この手順のコマンドはサンプルです。これらのコマンドの使用に関する詳細情報については、「CA Top Secret Command Functions Guide」および「CA Top Secret Control Options Guide」を参照してください。

以下の手順に従います。

1. 以下のコマンドの入力により RDT への CADB2 リソース クラスを追加します。

```
TSS ADDTO(RDT) RESCLASS(CADB2) RESCODE(XXXX)
```

XXXX

ユーザ定義の PIE リソースに使用可能な、101 ~ 13F の間の値を示します。

CADB2 リソースは RDT に追加されます。

2. リソース エンティティの所有権の獲得：

注: 部門に所有権を与えることをお勧めします。

```
TSS ADDTO(acid) CADB2(CONNECT.EXPLAIN)
```

acid

オブジェクトの所有者を指定します。SQL はこのオブジェクトを参照します。

CONNECT.EXPLAIN

EXPLAIN コマンド用のリソースを定義します。完全なエンティティは CONNECT.EXPLAIN.*pauthid* です。これはコマンド許可が確認されている ID です。

3. ユーザが許可 ID で EXPLAIN コマンドを実行することを許可します。

```
TSS PERMIT(acid) CADB2(CONNECT.EXPLAIN.pauthid)
```

acid

許可 ID にアクセスが必要なユーザまたはプロファイル ACID を指定します。

pauthid

ユーザが EXPLAIN に対して使用するプライマリ DB2 許可 ID を表します。

ユーザは許可 ID を使用することが許可されます。

ユーザはセカンダリ許可 ID で EXPLAIN コマンドを実行できます。加えて、ユーザは CA Chorus for DB2 Database Management で作業するアクセス権があります。

IBM RACF でセカンダリ許可 ID 使用状況を承認

この手順を使用して、ユーザが別のオブジェクト所有者の許可 ID を使用して EXPLAIN ステートメントを実行することを許可します。このアクセスなしには、ユーザは SQL が参照するオブジェクトの所有者でないかぎり、EXPLAIN コマンドを実行できません。

注: 以下のコマンドはサンプルです。これらのコマンドの使用の詳細については、IBM の製品マニュアルを参照してください。

以下の手順に従います。

1. 以下のコマンドを入力して、クラス記述子テーブル (CDT) をアクティブ化します。

```
SETROPTS CLASSACT(CDT) RACLIST(CDT)
```

CDT がアクティブになります。

2. CDT に CADB2 クラスを定義します。

```
RDEFINE CDT CADB2 UACC(NONE) -  
CDTINFO(DEFAULTUACC(NONE) FIRST(ALPHA) MAXLENGTH(42) -  
OTHER(ALPHA,NUMERIC,SPECIAL) -  
POSIT(value) RACLIST(REQUIRED))
```

CADB2 クラスが定義されます。

注: POSIT 値はサイト固有で、セキュリティ処理を制御するオプションフラグのセットを識別します。

3. CDT の更新

```
SETROPTS RACLIST(CDT) REFRESH
```

変更が実装されます。

4. CONNECT.EXPLAIN.pauthid CADB2 リソースを定義します。

```
RDEFINE CADB2 CONNECT.EXPLAIN.pauthid UACC(NONE)  
SETROPTS CLASSACT(CADB2) RACLIST(CADB2)
```

pauthid

ユーザが EXPLAIN に対して使用するプライマリ DB2 許可 ID を表します。

CADB2 リソースが定義されます。

5. 新規定義された CADB2 リソースに対してユーザを許可します。

```
PERMIT CONNECT,EXPLAIN.pauthid CLASS(CADB2) ID(user)  
ACCESS(EXECUTE)
```

user

所有者の許可 ID へのアクセスを必要とするユーザの ID を指定します。

ユーザが所有者の許可 ID を使用することが許可されます。

6. CADB2 リソース クラスを更新します。

```
SETROPTS RACLIST(CADB2) REFRESH
```

変更が実装されます。

ユーザはセカンダリ許可 ID で EXPLAIN コマンドを実行できます。加えて、ユーザは CA Chorus for DB2 Database Management で作業するアクセス権があります。

スターティッド タスク権限

CA Chorus (デフォルトで CHORADM) の実行に使用される、スターティッドタスク ユーザ ID は *your_db2tools_hlq.CDBALOAD* ライブラリのメンバを実行するために十分な権限を持っている必要があります。CHORADM は、CHORJBOS スターティッドタスクと関連付けられるユーザ ID または ACID を表します。CHORJBOS は、CA Chorus JBoss サーバと関連付けられるスターティッドタスク名です。

サンプル CA ACF2、CA Top Secret および RACF コマンドが提供されます。

注: CHORADM および CHORJBOS の詳細については、「CA Chorus サイト準備ガイド」を参照してください。

CA ACF2 コマンド

```
SET RULE RECKEY &DB2TOOL1 ADD(&DB2TOOLL.CDBALOAD UID(*****CHORADM)
R(A) E(A) )
```

&DB2TOOL1

CA Database Management Solutions for DB2 for z/OS 製品インストールの場所の高レベルインデックス（最初の修飾子）を指定します。

&DB2TOOLL

高レベル修飾子の残りを指定します。

たとえば、*your_db2tools_hlq* が CAID.DB2.R160 である場合は、&DB2TOOL1 を CAID に置換し、&DB2TOOLL を DB2.R160 に置換します。

注: サイト固有の基準を満たすために UID 値を確認し変更します。

CA Top Secret のコマンド

```
TSS PERMIT(CHORADM) DATASET(&DB2TOOLS.*) ACCESS(READ)
```

&DB2TOOLS

CA Database Management Solutions for DB2 for z/OS のインストールで使用される、高レベル修飾子を指定します。

CA Database Management Solutions for DB2 for z/OS に定義するセキュリティの一部として、この値は以下のようなコマンドを使用して部門に割り当てられている必要があります。

```
TSS ADDTO(&DBADEPT) DATASET(&DB2TOOLS)
```

&DBADEPT

DB2TOOLS リソースを所有する既存の部門を表します。

RACF コマンド

```
PERMIT '&DB2TOOLS.CDBALOAD' ID(CHORADM) ACCESS(EXECUTE)
```

重要: データセットプロフィール '&DB2TOOLS.CDBALOAD' が PERMIT コマンドを実行する前に存在する必要があります。CHORADM は、このプロフィールへの実行アクセス権を必要とします。

さらに、CA Chorus for DB2 Database Management は、CA Database Management Solutions for DB2 for z/OS のインストール後の処理中に作成される以下のスターティッド タスクを使用します。

- PTXMAN - Xmanager (実行マネージャ) スターティッド タスク。
- PXNPROC - Xnet (実行マネージャ ネットワーキング) スターティッド タスク。
- OFAPROC - Object Framework Services エージェント (OFA) スターティッド タスク。 CA Chorus for DB2 Database Management には以下が必要です。
 - USS 内の BPX.SERVER への READ アクセス。
 - RRSAF を使用して DB2 に接続するための、OFS エージェント スターティッド タスクに対する RRSAF リソース許可を作成します。

注: デフォルト値が表示されます。関連する製品に固有のタスクおよび DB2 カタログ カスタマイズ タスクを実行する詳細については、「*CA Database Management Solutions for DB2 for z/OS Implementation Guide*」を参照してください。これらのタスクの開始または停止に関する詳細については、「*CA Chorus Administration Guide*」を参照してください。

CA OPS/MVS が使用される場合、CA Chorus for DB2 Database Management は TPDTFEED スターティッド タスクも使用します。このタスクは、CA Chorus で Time Series 機能 (TSF) に CA Detector 収集データを自動的に提供するための CA Chorus for DB2 Database Management 設定処理中に作成されます。CA Chorus for DB2 Database Management には以下が必要です。

- CA Database Management Solutions for DB2 for z/OS インストールデータセットの高レベル修飾子への READ アクセス。
- CA Detector Time Series 機能 (TSF) 高レベル修飾子 (TPDTHLQ) への UPDATE アクセス。この値は、CA Chorus for DB2 Database Management 設定中に使用します。

注: TPDTFEED スターティッド タスクの詳細については、「*CA Chorus Manual Configuration Guide*」を参照してください。

注: 各スターティッド タスクに関連付けられたユーザ ID は定義された OMVS セグメントを持つ必要があります。これにより TCP/IP 処理が z/OS UNIX System Services (USS) にアクセスできるようになります。

詳細情報:

[CA Chorus for DB2 Database Management 用の RRSAF 許可 \(P. 53\)](#)

サーバ要件

サイトが以下のシステム要件を満たしていることを確認します。

実記憶域

CA Chorus for DB2 Database Management 用に 200 MB のヒープメモリ
および CA Chorus 用に 2450 MB のヒープメモリ。

注: ディシプリンがすべてインストールされている場合、3150 MB 必要です。デフォルト値です。CA Chorus および任意のディシプリンのインストールの後にヒープメモリサイズを増やすには、*your_chorus_hlq.CETJOPTN* の ENVETJ メンバの Java ヒープサイズ (Java SDK オプション) 設定を確認します。ヒープ範囲については、-Xms が開始値で、-Xmx が終了値です。

PassTicket の構成

PassTicket は、CA Chorus JBoss サーバに接続する CA Chorus の機能を使用する CA Chorus for DB2 Database Management ユーザに対して生成される必要があります。これらの機能には、レポート用の JCL 生成を有効にするレポート オプションと CA Chorus for DB2 Database Management の Object Migrator 機能が含まれます。また、PassTicket は、CA Chorus for DB2 Database Management に対して CA Database Management Solutions for DB2 for z/OS バックエンド要件 CA 製品およびコンポーネントから提供されるデータへのアクセスをユーザに許可するよう設定されている必要があります。CA Database Management Solutions for DB2 for z/OS によって、ユーザが特定のコンポーネントにアクセスするときに、サーバが生成した PassTicket が検証されます。

注: レポート オプションおよび Object Migrator ジョブは、CA Chorus JBoss サーバに対してネットワーク接続可能な任意のシステム上で実行できません。

重要: ユーザが異なる LPAR にまたがって実行している場合、Investigator で Object Migrator、DB2 DBA Command Manager、または Display Databases アクションを使用するために共有 DASD が必要です。

CA Chorus システム用の[サンプル設定](#) (P. 36)が提供されます。PassTicket を生成するためのガイドラインとして、サンプルの[CA ACF2](#) (P. 38)、[CA Top Secret](#) (P. 43)、および [IBM RACF](#) (P. 48) コマンドが提供されています。

注: サンプル コマンドの一部は、外部セキュリティ マネージャへのレポート オプションおよびオブジェクトマイグレータ ジョブ用の PassTicket 検証を定義するために、デフォルトのアプリケーション名 (CHORWEBS) を使用します。ただし、このアプリケーション名は設定可能です (8 文字以下の任意の大文字文字列を使用できます)。アプリケーション ID に CHORWEBS とは異なる値を使用する場合は、同じ値を使用するようにサンプル コマンドを更新します。さらに、CA Chorus のインストール後に同じ値を使用するように、*your_chorus_hlq*.CETJOPTN の ENVETJ メンバの CHORUS_APPL 環境変数を更新します。

CA Chorus システム用の PassTicket 設定

CA Chorus サーバによって、CA Chorus ディシプリンが使用するさまざまなバックエンド製品へのユーザのアクセスを許可する PassTicket が生成されます。ユーザが特定のコンポーネントにアクセスする際は、PassTicket がリクエストの検証のために生成されます。

CA Chorus PassTicket 設定には以下のシステムが含まれます。

- JBoss サーバ、および同じシステム上の CA Chorus ディシプリンに必要なバックエンド製品（CA Detector、CA Compliance Manager、CA Vantage など）を実行する 1 つの z/OS システム。このシステムのタイプは CA Chorus サーバシステムです。
- CA Chorus ディシプリンで必要な製品およびコンポーネントのみを実行する追加の z/OS システム。このシステムのタイプは CA Chorus リモートシステムと呼ばれます。

CA Chorus サーバシステムによって、すべての CA Chorus ユーザへのエントリのポイントが提供されます。その後、ユーザは、z/OS システムのユーザのネットワーク内で使用を許可されたすべての CA Chorus リモートシステムにアクセスできます。

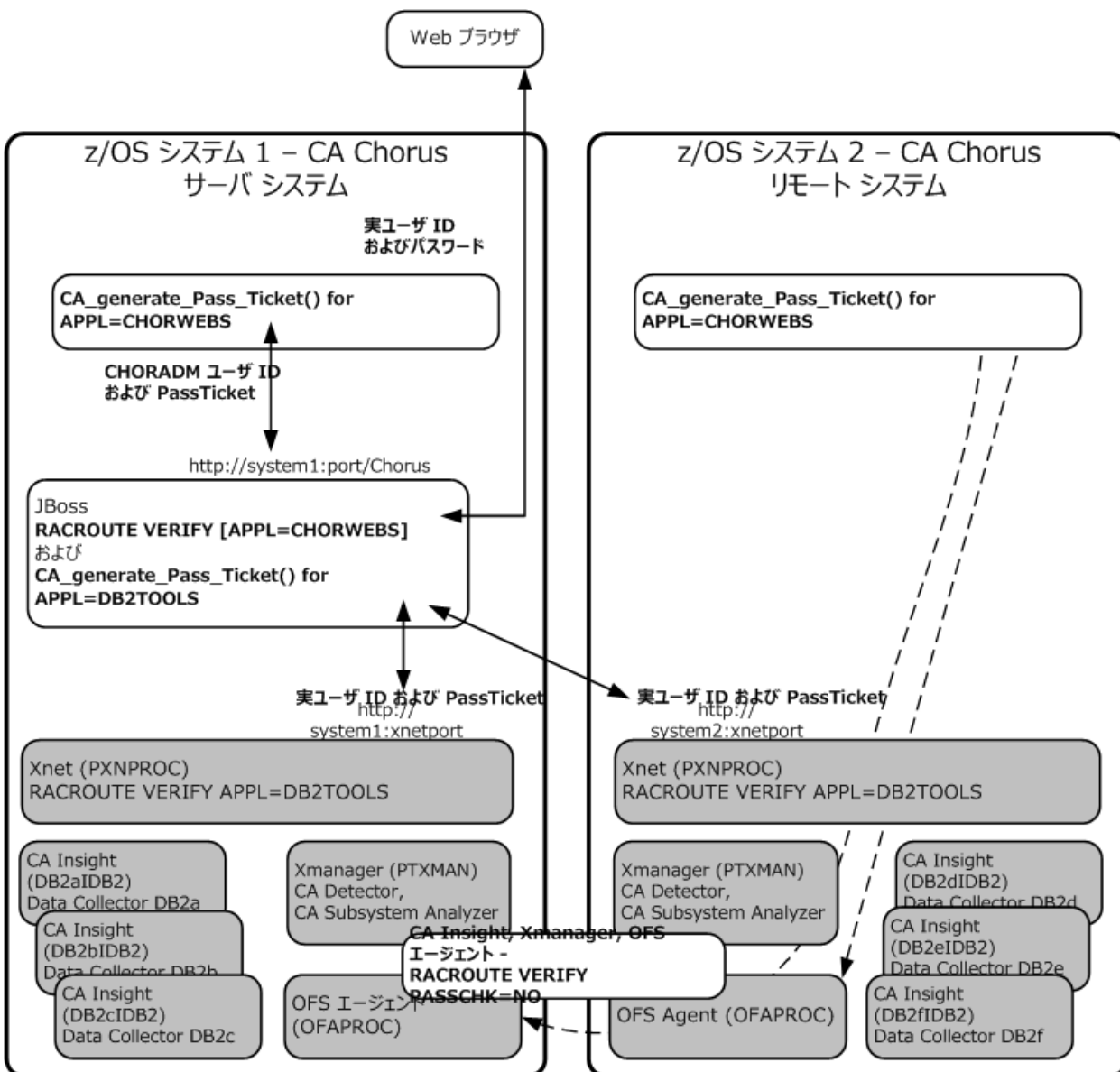
z/OS セキュリティ製品用の PassTicket 設定は、CA Chorus が使用するコンポーネントをホストする各 z/OS システム上で実行される必要があります。CA Chorus ロールに必要な接続の生成および検証を有効にするため、z/OS セキュリティ製品で PassTicket を設定します。以下の点に注意してください。

- CA Chorus サーバシステムおよびリモートシステムが、セキュリティデータベースを共有する場合、追加のセットアップは必要ではありません。
- 必要な製品およびコンポーネントがセキュリティデータベースを共有しないリモートシステムに存在する場合、追加のセキュリティセットアップがリモートシステム上で必要です。

CA Chorus システム用のサンプル PassTicket 設定

以下の図は、左側に CA Chorus サーバシステムを示し、右側に CA Chorus リモートシステムを示しています。この図の白いボックスは、サーバシステムにのみ必要な設定手順を表します。淡灰色のボックスは、CA Chorus サーバおよびリモートシステムに必要な設定手順を表します。これらの淡灰色の領域は、CA Chorus に必要な CA Technologies バックエンド製品の設定を表します。各領域には、共通コンポーネント名とカッコで囲まれた STC JCL 名があります。

通常、最初の CA Chorus インストールには、完全な CA Chorus サーバシステムがあります。CA Chorus サーバシステムには Web サーバ（白い四角）と、図の左側に書かれた製品（灰色の四角）が含まれます。CA Chorus サーバシステム用のセキュリティセットアップには、追加のリモートシステムに必要な定義のサブセットが含まれます。



z/OS セキュリティ製品で共有セキュリティ データベースが使用される場合、サーバシステム用のセキュリティセットアップ以上に、リモートシステム上に追加のセキュリティセットアップは必要ありません。サポート対象の CA Technologies バックエンド製品をセキュリティ データベースを共有しないシステムにインストールしている場合は、リモートシステム上でセキュリティ セットアップを実行します。

サンプル: CA ACF2 を使用して CA Chorus for DB2 Database Management PassTicket を設定

CA ACF2 を使用して、CA Chorus for DB2 Database Management 固有の PassTicket を設定できます。これは、CA Chorus サーバおよびリモートシステムへのアクセスを検証するために使用されます。CA Chorus サーバおよびリモートシステムについては、「PassTicket の設定」で説明しています。

注: これらの例はガイドラインとして提供されます。PassTicket 設定に精通しているセキュリティ管理者のみが、このプロセスを実行するようにしてください。これらのコマンドの使用に関する詳細情報については、「CA ACF2 for z/OS Administration Guide」を参照してください。

例: CA ACF2を使用して CA Chorus サーバシステム用の PassTicket を設定

以下の手順に従います。

1. 以下のコマンドを入力して、アプリケーションセッションキーを定義します。

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
INSERT DB2TOOLS SSKEY(0123456789ABCDEF) MULT-USE
INSERT CHORWEBS SSKEY(FEDCBA9876543210) MULT-USE
F ACF2,REBUILD(PTK),CLASS(P)
```

DB2TOOLS および CHORWEBS

PassTickets の検証に対して使用されるアプリケーション ID を定義します。DB2TOOLS および CHORWEBS はデフォルトアプリケーション ID です。

- DB2TOOLS は、CA Chorus UI および Quick Links モジュールから CA Database Management Solutions for DB2 for z/OS への CA Chorus for DB2 Database Management ユーザアクセスを認証します。
- CHORWEBS は、CA Chorus Investigator で Object Migrator 機能 (マイグレート) への CA Chorus for DB2 Database Management ユーザアクセスを認証します。このアプリケーション ID およびセッションキーは、CA Chorus プラットフォーム PassTicket 設定の一環としてすでに定義されている場合があります。

重要: SSKEY は 16 進数字を使用して暗号化キーを定義します (8 バイトまたは 64 バイトのキーを作成します)。この値は例として使用されています。サイト固有のキー値を使用してください。キーはそれぞれ設定内のすべてのシステム上で同じである必要があります。

MULT-USE

同じ PassTicket を複数回を再利用できるようにします。

CA Chorus for DB2 Database Management セッションキーが定義されます。

2. ユーザが DB2TOOLS アプリケーションと CHORWEBS アプリケーション用の PassTicket を生成できるようにします。

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(DB2TOOLS.- UID(uid-of-stc-userid)
SERVICE(UPDATE,READ) ALLOW)
RECKEY IRRPTAUTH ADD(DB2TOOLS.useridn UID(uid-of-useridn)
SERVICE(UPDATE,READ) ALLOW)
RECKEY IRRPTAUTH ADD(CHORWEBS.- UID(uid-of-stc-userid)
SERVICE(UPDATE,READ) ALLOW)
RECKEY IRRPTAUTH ADD(CHORWEBS.- UID(uid-of-ofa-stc-userid)
SERVICE(UPDATE,READ) ALLOW)
RECKEY IRRPTAUTH ADD(CHORWEBS.useridn UID(uid-of-useridn)
SERVICE(UPDATE,READ) ALLOW)
```

stc-userid

your_chorus_hlq.CETJJCL の ETJI095x で作成された、スターティッドタスク ユーザ ID を指定します。この ID は、任意のユーザのための PassTicket を生成できる必要があります。デフォルト：**CHORADM**。この ID は、「**CA Chorus サイト準備ガイド**」で説明されているとおり、CA Chorus セキュリティ設定中に作成されます。

useridn および *uid-of-useridn*

ユーザ ID および CA Chorus へのアクセスをリクエストしているユーザの UID を指定します。

ofa-stc-userid および *uid-of-ofa-stc-userid*

ユーザ ID および Object Migrator 機能に使用される Object Framework Services エージェント (OFA) スターティッドタスク (デフォルトでは OFAPROC) に関連付けられている UID を指定します。このスターティッドタスクは、「**CA Database Management Solutions for DB2 for z/OS Implementation Guide**」で説明されているような OFS エージェント (OFA) の設定中に作成されます。追加の設定が CA Chorus for DB2 Database Management で必要です。この設定は「**CA Chorus Manual Configuration Guide**」で説明されています。

各 UID の正確な値の取得については、セキュリティ管理者に相談してください。

注: すべてのユーザに対して一律に PassTicket の自動生成を行わない場合、以下のコマンド構文を使用して、個別のユーザにアクセス権を与えることができます。

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(DB2TOOLS.userid UID(uid-of-stc-userid)
SERVICE(UPDATE,READ) ALLOW)
RECKEY IRRPTAUTH ADD(CHORWEBS.userid UID(uid-of-stc-userid)
SERVICE(UPDATE,READ) ALLOW)
```

注: また、ACFNRULE ユーティリティプログラムを使用し、既存のルールにルール行を追加することもできます。このオプションの詳細については、「*CA ACF2 for z/OS Administration Guide*」を参照してください。

例: CA ACF2 を使用して CA Chorus リモートシステム用の PassTicket を設定

CA Technologies バックエンドの必要な製品およびコンポーネントがセキュリティ データベースを共有しないリモート システムに存在する場合、追加のセキュリティ セットアップが CA Chorus リモートシステム上で必要です。 リモートシステムは、バックエンド CA Technologies 製品およびコンポーネントを介して CA Chorus にデータを提供しており、JBoss サーバは実行していない任意の追加の z/OS システムです。

以下の手順に従います。

1. リモートシステムで DB2TOOLS セッション キーおよび CHORWEBS セッション キーを定義します。

```
SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
INSERT DB2TOOLS SSKEY(0123456789ABCDEF) MULT-USE
INSERT CHORWEBS SSKEY(FEDCBA9876543210) MULT-USE
F ACF2,REBUILD(PTK),CLASS(P)
```

2. (オプション) それぞれ CA Database Management Solutions for DB2 for z/OS および Object Migrator 機能へのアクセスを許可されている各ユーザに対し、DB2TOOLS アプリケーションへのアクセスを許可します。

注: この手順を実行するのは、DB2TOOLS アプリケーション リソースをすでに定義している場合のみです。APPL クラスのタイプコードを APL に変更するために GSO CLASMAP レコードを挿入した場合は、以下のコマンドで TYPE として SAF ではなく APL を使用します。

```
ACF
SET RESOURCE(SAF)
RECKEY DB2TOOLS ADD(UID(uid_of_stc_userid) SERVICE(READ) ALLOW)
RECKEY DB2TOOLS ADD(useridn UID(uid-of-useridn) SERVICE(READ)
ALLOW)
F ACF2,REBUILD(SAF)
```

3. リモートシステム上で Object Migrator 機能を利用可能なすべてのユーザに対して、CHORWEBS PassTicket キー値への UPDATE アクセスを有効にします。

```
SET RESOURCE(PTK)
RECKEY CHORWEBS ADD(useridn UID(uid-of-useridn) SERVICE(UPDATE)
ALLOW)
```

サンプル: CA Top Secret を使用して CA Chorus for DB2 Database Management PassTicket を設定

CA Top Secret を使用して、CA Chorus サーバおよびリモート システムに対して PassTicket を設定できます。CA Chorus サーバおよびリモート システムについては、「PassTicket の設定」で説明しています。

注: これらの例はガイドラインとして提供されます。PassTicket 設定に精通しているセキュリティ管理者のみが、このプロセスを実行するようにしてください。これらのコマンドの使用に関する詳細情報については、「*CA Top Secret for z/OS Control Options Guide*」を参照してください。

注: この手順では、PTKTDATA クラスおよび IRRPTAUTH リソースの所有権が定義されていると想定しています。

例: CA Top Secret を使用して CA Chorus サーバシステム用の PassTicket を設定

以下の手順に従います。

1. PassTickets を受理するためにホストおよびリモート システムをセットアップします。

- a. CA Chorus for DB2 Database Management によって使用されるアプリケーション リソースを定義し、所有権を割り当てます。

```
TSS ADDTO(department) APPLICATION(DB2TOOLS)
TSS ADDTO(department) APPLICATION(CHORWEBS)
```

department

既存の部門を特定します。アプリケーションはこの部門に対して定義されます。この所有権によって、部門管理者（またはそれ以上）は PassTicket の生成および検証の権限を定義できます。

DB2TOOLS および CHORWEBS

PassTickets の検証に対して使用されるアプリケーション ID を定義します。DB2TOOLS および CHORWEBS はデフォルトアプリケーション ID です。

* DB2TOOLS は、CA Chorus UI および Quick Links モジュールから CA Database Management Solutions for DB2 for z/OS への CA Chorus for DB2 Database Management ユーザアクセスを認証します。

* CHORWEBS は、CA Chorus Investigator で Object Migrator 機能（マイグレート）への CA Chorus for DB2 Database Management ユーザアクセスを認証します。このアプリケーション ID およびセッションキーは、CA Chorus プラットフォーム PassTicket 設定の一環としてすでに定義されている場合があります。

- b. 以下のコマンドを使用し、アプリケーション ID を定義して暗号化キーを割り当てるように Node Descriptor Table（NDT）を更新します。

```
TSS ADDTO(NDT) PSTKAPPL(DB2TOOLS) SESSKEY(0123456789ABCDEF)
SIGNMULTI
TSS ADDTO(NDT) PSTKAPPL(CHORWEBS) SESSKEY(FEDCBA9876543210)
SIGNMULTI
```

重要: SESSKEY は 16 進数字を使用して暗号化キーを定義します (8 バイトまたは 64 バイトのキーを作成します)。この値は例として使用されています。サイト固有のキー値を使用してください。キーはそれぞれ設定内のすべてのシステム上で同じである必要があります。

PassTicket は複数回再利用できます。

PassTicket を使用するすべてのシステムでは、ネットワークの上のすべてのノードに同一のアプリケーション名とセッション キーが必要です。

2. DB2TOOLS アプリケーション用の PassTicket 生成を有効にします。

```
TSS PERMIT(stc-userid) PTKTDATA(IRRPTAUTH.DB2TOOLS.)  
ACCESS(READ,UPDATE)  
TSS PERMIT(useridn) PTKTDATA(IRRPTAUTH.DB2TOOLS.useridn)  
ACCESS(READ,UPDATE)
```

stc-userid

your_chorus_hlq.CETJJCL の ETJI095x で作成された、スターティッドタスク ユーザ ID を指定します。この ID は、任意のユーザのための PassTicket を生成できる必要があります。デフォルト: CHORADM. この ID は、「CA Chorus サイト準備ガイド」で説明されているとおり、CA Chorus セキュリティ設定中に作成されます。

useridn

CA Chorus へのアクセスをリクエストしているユーザのユーザ ID を指定します。

この手順では、特定のユーザ向けの PassTicket の生成にセッション キー値を使用するための CA Chorus サーバ許可を与えます。

3. CA Database Management Solutions for DB2 for z/OS へのアクセスを許可されている各ユーザに対し、DB2TOOLS アプリケーションへのアクセスを許可します。

```
TSS PERMIT(stc-userid) APPLICATION(DB2TOOLS)  
TSS PERMIT(useridn) APPLICATION(DB2TOOLS)
```

この手順では、特定のユーザに対し、DB2TOOLS セッション キー値を使用して生成される PassTicket を検証する権限を含む CA Database Management Solutions for DB2 for z/OS へのアクセス権を与えます。

4. ユーザが CHORWEBS アプリケーションの PassTicket を生成することを許可します。

```
TSS PERMIT(stc-userid) PTKTDATA(IRRPTAUTH.CHORWEBS.)  
ACCESS(READ,UPDATE)  
TSS PERMIT(ofa-stc-userid) PTKTDATA(IRRPTAUTH.CHORWEBS.)  
ACCESS(READ,UPDATE)  
TSS PERMIT(useridn) PTKTDATA(IRRPTAUTH.CHORWEBS.useridn)  
ACCESS(READ,UPDATE)
```

stc-userid

your_chorus_hlq.CETJJCL の ETJI095x で作成された、スターティッドタスク ユーザ ID を指定します。この ID は、任意のユーザのための PassTicket を生成できる必要があります。デフォルト：**CHORADM**。このユーザは、CHORWEBS PassTicket へのアクセスを必要とします。

ofa-stc-userid

Object Migrator 機能に使用される Object Framework Services エージェント (OFA) スターティッドタスク (デフォルトでは OFAPROC) に関連付けられているユーザ ID を指定します。このスターティッドタスクは、「*CA Database Management Solutions for DB2 for z/OS Implementation Guide*」で説明されているような OFS エージェント (OFA) の設定中に作成されます。インストール後に CA Chorus for DB2 Database Management に追加の設定を行う必要があります。この設定は「*CA Chorus Manual Configuration Guide*」で説明されています。

useridn

CA Chorus へのアクセスをリクエストしているユーザのユーザ ID を指定します。

例: CA Top Secret を使用して CA Chorus リモートシステム用の PassTicket を設定

以下の手順に従います。

注: この手順では、PTKTDATA クラスおよび IRRPTAUTH リソースの所有権がすでに定義されていると想定しています。

1. 以下のコマンドを入力することで、DB2TOOLS アプリケーション リソースを定義して所有権を割り当てます。

```
TSS ADDTO(department) APPLICATION(DB2TOOLS)
```

2. CA Chorus PassTicket アプリケーションセッション キーを定義します。

```
TSS ADDTO(NDT) PSTKAPPL(DB2TOOLS) SESSKEY(FEDCBA9876543210)  
SIGNMULTI
```

```
TSS ADDTO(NDT) PSTKAPPL(CHORWEBS) SESSKEY(0123456789ABCDEF)  
SIGNMULTI
```

セッション キーが定義されます。

3. CA Database Management Solutions for DB2 for z/OS へのアクセスを許可されている各ユーザに対し、DB2TOOLS アプリケーションへのアクセスを許可します。

```
TSS PERMIT(userid1) APPLICATION(DB2TOOLS)
```

```
TSS PERMIT(userid2) APPLICATION(DB2TOOLS)
```

...

```
TSS PERMIT(useridn) APPLICATION(DB2TOOLS)
```

この手順では、特定のユーザに対し、DB2TOOLS セッション キー値を使用して生成される PassTicket を検証する権限を含む CA Database Management Solutions for DB2 for z/OS へのアクセス権を与えます。

4. Object Migrator 機能にアクセスするユーザに対して CHORWEBS アプリケーションへのアクセスを許可します。

```
TSS PERMIT(useridn) PTKTDATA(IRRPTAUTH.CHORWEBS.useridn)  
ACCESS(UPDATE)
```

サンプル: RACF を使用して CA Chorus for DB2 Database Management PassTicket を設定

IBM RACF を使用して、CA Chorus サーバおよびリモートシステムに対して PassTicket を設定できます。CA Chorus サーバおよびリモートシステムについては、「PassTicket の設定」で説明しています。

注: これらの例はガイドラインとして提供されます。PassTicket 設定に精通しているセキュリティ管理者のみが、このプロセスを実行するようにしてください。これらのコマンドの使用に関する詳細については、IBM RACF の製品マニュアルを参照してください。

注: Passticket 設定を開始する前に、PassTicket リソース IRRPTAUTH に対して PTKTDATA クラスおよび所有権が定義されていないことを確認します。それらが定義されている場合は、以下の手順 1 および手順 2 をスキップします。

例: IBM RACF を使用して CA Chorus サーバシステム用の PassTicket を設定

以下の手順に従います。

1. 以下のコマンドを入力して、DB2TOOLS アプリケーションを定義します。

```
RDEFINE APPL DB2TOOLS UACC(NONE)
SETROPTS CLASSACT(APPL)
```

注: 汎用ユーザ ID を実装する場合は、以下の追加のコマンドを指定します。

```
SETROPTS GENERIC(PTKTDATA)
```

2. 現在 PassTicket クラスがアクティブでない場合はアクティブにします。
SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)

3. アプリケーション用のプロファイルを定義し、セッション キーを指定します。

```
RDEFINE PTKTDATA DB2TOOLS SSIGNON(KEYMASKED(FEDCBA9876543210))
APPLDATA('NO REPLAY PROTECTION')
RDEFINE PTKTDATA CHORWEBS SSIGNON(KEYMASKED(0123456789ABCDEF))
APPLDATA('NO REPLAY PROTECTION')
```

DB2TOOLS および CHORWEBS

PassTickets の検証に対して使用されるアプリケーション ID を定義します。DB2TOOLS および CHORWEBS はデフォルトアプリケーション ID です。

- DB2TOOLS は、CA Chorus UI および Quick Links モジュールから CA Database Management Solutions for DB2 for z/OS への CA Chorus for DB2 Database Management ユーザアクセスを認証します。
- CHORWEBS は、CA Chorus Investigator で Object Migrator 機能（マイグレート）への CA Chorus for DB2 Database Management ユーザアクセスを認証します。このアプリケーション ID およびセッション キーは、CA Chorus プラットフォーム PassTicket 設定の一環としてすでに定義されている場合があります。

重要: KEYMASKED は 16 進数字を使用して暗号化キーを定義します（8 バイトまたは 64 バイトのキーを作成します）。この値は例として使用されています。サイト固有のキー値を使用してください。キーはそれぞれ、すべてのシステムの設定で同じである必要があります。

プロファイルとセッション キーが定義されます。

4. CA Database Management Solutions for DB2 for z/OS へのアクセスを許可されている各ユーザに対して、プロファイルを定義して DB2TOOLS PassTicket セッション キー値へのアクセスを許可します。

```
RDEFINE PTKTDATA IRRPTAUTH.DB2TOOLS.* UACC(NONE)
PERMIT IRRPTAUTH.DB2TOOLS.* ID(stc-userid) CLASS(PTKTDATA)
ACCESS(UPDATE)
```

stc-userid

your_chorus_hlq.CETJJCL の ETJI095x で作成された、スターティッド タスク ユーザ ID を指定します。この ID は、任意のユーザのための PassTicket を生成できる必要があります。デフォルト:

CHORADM. このユーザは、CHORWEBS PassTicket へのアクセスを必要とします。

この操作の代わりに、CA Chorus for DB2 Database Management 機能用のグループを作成できます。以下に例を示します。

```
ADDGROUP ETJDB2GR
CONNECT CHORUSR1 GROUP(ETJDB2GR)
CONNECT CHORUSR2 GROUP(ETJDB2GR)
...
CONNECT CHORUSRN GROUP(ETJDB2GR)
```

```
RDEFINE PTKTDATA IRRPTAUTH.DB2TOOLS.ETJDB2GR OWNER(stc-userid)
UACC(NONE)
PERMIT IRRPTAUTH.DB2TOOLS.ETJDB2GR ID(stc-user) AC(UPDATE)
CLASS(PTKTDATA)
```

この例では、ETJDB2GR で CA Chorus for DB2 Database Management ユーザ用のグループを定義し、CHORUSRx でグループに特定のユーザを定義し、RDEFINE コマンドでグループメンバに対して PassTicket 生成を有効にするためのリソースを定義し、PERMIT コマンドでグループメンバに対して JBoss サーバユーザの DB2TOOLS への PassTicket の生成を有効にします。

5. CA Database Management Solutions for DB2 for z/OS へのアクセスを許可されている各 CA Chorus for DB2 Database Management ユーザに対して、DB2TOOLS アプリケーションへのアクセスを許可します。

```
PERMIT DB2TOOLS CLASS(APPL) ID(stc-userid) ACCESS(READ)
PERMIT DB2TOOLS CLASS(APPL) ID(useridn)
```

useridn

アクセスをリクエストしているユーザのユーザ ID を指定します。

6. CHORWEBS アプリケーションを定義します。

```
RDEFINE APPL CHORWEBS UACC(READ)
SETROPTS CLASSACT(APPL)
```

注: この手順は CA Chorus インストールでの PassTicket 設定中にすでに実行されている場合があります。

7. CA Chorus for DB2 Database Management の Object Migrator 機能へのアクセスを許可されている各ユーザに対し、プロファイルを定義し、CHORWEBS PassTicket セッション キー値へのアクセスを許可します。

```
RDEFINE PTKTDATA IRRPTAUTH.CHORWEBS.* UACC(NONE)
PERMIT IRRPTAUTH.CHORWEBS.* CLASS(PTKTDATA) ID(stc-userid)
ACCESS(UPDATE)
```

stc-userid

「CA Chorus ユーザ ID の作成」で作成したスターティッドタスク ユーザ ID を参照します。このユーザ ID は、任意のユーザに対して PassTicket の生成が可能である必要があります。

注: この手順は CA Chorus インストールでの PassTicket 設定中にすでに実行されている場合があります。

8. Object Migrator スターティッドタスク ID に対して CHORWEBS PassTicket セッション キー値へのアクセスを許可します。

```
PERMIT IRRPTAUTH.CHORWEBS.* CLASS(PTKTDATA) ID(ofa-stc-userid)
ACCESS(UPDATE)
```

ofa-stc-userid

Object Migrator 機能に使用される Object Framework Services エージェント (OFA) スターティッドタスク (デフォルトでは OFAPROC) に関連付けられているユーザ ID を指定します。このスターティッドタスクは、「*CA Database Management Solutions for DB2 for z/OS Implementation Guide*」で説明されているような OFS エージェント (OFA) の設定中に作成されます。インストール後に CA Chorus for DB2 Database Management に追加の設定を行う必要があります。この設定は「*CA Chorus Manual Configuration Guide*」で説明されています。

9. Object Migrator 機能へのアクセスを許可されている各ユーザに対して、プロファイルを定義し、CHORWEBS PassTicket セッションキー値へのアクセスを許可します。

```
RDEFINE PTKTDATA IRRPTAUTH.CHORWEBS.useridn UACC(NONE)
PERMIT IRRPTAUTH.CHORWEBS.useridn CLASS(PTKTDATA) ID(useridn)
ACCESS(UPDATE)
```

10. CHORWEBS アプリケーションへのアクセスを許可します。

```
PERMIT CHORWEBS CLASS(APPL) ID(stc-userid) ACCESS(READ)
PERMIT CHORWEBS CLASS(APPL) ID(useridn)
```

注: この手順は CA Chorus インストールでの PassTicket 設定中にすでに実行されている場合があります。

11. 以下のコマンドで APPL クラスと PTKTDATA クラスをリフレッシュします。

```
SETROPTS RACLIST(APPL) REFRESH
SETROPTS RACLIST(PTKTDATA) REFRESH
```

例: IBM RACF を使用して CA Chorus リモートシステム用の PassTicket を設定

以下の手順に従います。

1. 以下のコマンドを入力して、DB2TOOLS アプリケーションを定義します。

```
RDEFINE APPL DB2TOOLS UACC(NONE)
SETROPTS CLASSACT(APPL)
```

2. 以下のコマンドを入力して PassTicket クラスをアクティブ化します。

```
SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
```

3. 以下のコマンドを入力して、アプリケーション用のプロファイルを定義し、セッションキーを指定します。

```
RDEFINE PTKTDATA DB2TOOLS SSIGNON(KEYMASKED(FEDCBA9876543210))
APPLDATA('NO REPLAY PROTECTION')
RDEFINE PTKTDATA CHORWEBS SSIGNON(KEYMASKED(0123456789ABCDEF))
APPLDATA('NO REPLAY PROTECTION')
```

セッションキーが定義されます。

4. CA Database Management Solutions for DB2 for z/OS へのアクセスを許可されている各ユーザに対し、DB2TOOLS アプリケーションへのアクセスを許可します。

```
PERMIT DB2TOOLS CLASS(APPL) ID(stc-userid) ACCESS(READ)
PERMIT DB2TOOLS CLASS(APPL) ID(userid1)
PERMIT DB2TOOLS CLASS(APPL) ID(userid2)
...
PERMIT DB2TOOLS CLASS(APPL) ID(useridn)
```

5. Object Migrator スターティッドタスク用の CHORWEBS PassTicket セッションキー値へのアクセスを許可します。

```
RDEFINE PTKTDATA IRRPTAUTH.CHORWEBS.* UACC(NONE)
PERMIT IRRPTAUTH.CHORWEBS.* CLASS(PTKTDATA) ID(ofa-stc-userid)
ACCESS(UPDATE)
```

6. Object Migrator 機能へのアクセスを許可されている各 CA Chorus for DB2 Database Management ユーザに対して、CHORWEBS PassTicket セッションキー値へのアクセスを許可します。

```
RDEFINE PTKTDATA IRRPTAUTH.CHORWEBS.userid UACC(NONE)
PERMIT IRRPTAUTH.CHORWEBS.userid CLASS(PTKTDATA) ID(userid)
ACCESS(UPDATE)
```

7. APPL クラスと PTKTDATA クラスをリフレッシュします。

```
SETROPTS RACLIST(APPL) REFRESH
SETROPTS RACLIST(PTKTDATA) REFRESH
```

CA Chorus for DB2 Database Management 用の RRSAF 許可

CA Chorus for DB2 Database Management では、Resource Recovery Services Attachment 機能 (RRSAF) 用のリソース許可が必要です。これは、DB2 システムに接続するユーザに対する接続許可の仕組みとして機能します。RRSAF 接続が試行されると、DB2 は呼び出し元に RRSAF を使用する権限があるかどうかを確認します。セキュリティ管理者は、Object Framework Services エージェント (OFA) アドレス空間に関連付けられた各スターティッドタスクに対するリソース許可を作成する必要があります。

CA Chorus for DB2 Database Management では、RRSAF をサポートするためにこの追加の手順が必要ですが、Call Attachment 機能 (CAF) を使用するレガシー CA Database Management Solutions for DB2 for z/OS では必要ありません。

注: RRSAF セキュリティ環境の RACF によるアクセスの管理の詳細については、「*IBM DB2 Administration Guide*」を参照してください。ここに CA ACF2 および CA Top Secret への RRSAF 許可のリコメンデーションの適用に役立つ一般的な概念が記載されています。RRSAF の IDENTIFY 機能の詳細については、「*IBM DB2 Application Programming and SQL Guide*」を参照してください。

CA ACF2、CA Top Secret、または IBM RACF を使用して RRSAF リソース許可を作成するための、サンプル コマンドが提供されています。このリソース許可は、CA Chorus for DB2 Database Management に接続する DB2 サブシステムで必要です。

注: これらのサンプル コマンドに関する詳細情報については、製品に固有のセキュリティ ドキュメントを参照してください。

サンプル: CA ACF2 を使用して RRSAF リソース許可を作成

スターティッドタスク ID (STC ID) が DB2 権限に対して Resource Recovery Services Attachment 機能 (RRSAF) を使用することを許可するには、この手順に従います。各サブシステムに対してこの許可を繰り返します。このアクセス権限がないと、STC ID のユーザは DB2 システムに接続できません。

注: この手順のコマンドはサンプルです。これらのコマンドの使用に関する詳細情報については、「*CA ACF2 for z/OS Administration Guide*」を参照してください。

以下の手順に従います。

1. 以下のコマンドを入力して、リソースを設定します。

```
SET RESOURCE(SAF)
```

```
SAF
```

リソース タイプを指定します。

このビューはリソースのビューです。

- RRSAF へのユーザ アクセスを許可します。

```
COMP
$KEY(DSNR) TYPE(SAF)
ssss.RRSAF UID(ofa_stc_id) ALLOW
END
STORE

ssss
```

サブシステム ID を指定します。

ofa_stc_id

Object Framework Services エージェント (OFA) スターティッドタスクに関連付けられた STC ID を指定します。デフォルトでは「OFAPROC」になります。

エージェントが許可されます。

- RRSAF セットアップを完了します。

```
F ACF2,REBUILD(SAF)
```

許可が完了します。

サンプル: CA Top Secret を使用して RRSAF リソース許可を作成

スターティッドタスク ID (STC ID) が DB2 権限に対して Resource Recovery Services Attachment 機能 (RRSAF) を使用することを許可するには、この手順に従います。各サブシステムに対してこの許可を繰り返します。このアクセス権限がないと、STC ID のユーザは DB2 システムに接続できません。

注: この手順のコマンドはサンプルです。これらのコマンドの使用に関する詳細情報については、「*CA Top Secret for z/OS Command Functions Guide*」および「*CA Top Secret for z/OS Control Options Guide*」を参照してください。

CA Top Secret を使用して RRSAF のリソース許可を作成する方法

1. 以下のコマンドを入力して、リソースの所有権を割り当てます。

注: サイトでこのタスクをすでに終了している場合、この手順は必要ありません。

```
TSS ADDTO(department_acid) DB2(DSNR.)  
department_acid
```

オブジェクトの所有者を指定します。このオブジェクトは SQL によって参照されます。

注: 通常は部門に所有権を与えることをお勧めします。

2. DB2 ユーザ許可を許可します。

```
TSS PERMIT(ofa_stc_id) DB2(DSNR.ssss.RRSAF)  
ofa_stc_id
```

Object Framework Services エージェント (OFA) スターティッドタスクと関連付けられた STC ID を指定します。デフォルトでは「OFAPROC」になります。

```
SSSS
```

サブシステム ID を指定します。

エージェントが許可されます。

サンプル: RACF を使用して RRSAF リソース許可を作成

スターティッドタスク ID (STC ID) が DB2 権限に対して Resource Recovery Services Attachment 機能 (RRSAF) を使用することを許可するには、この手順に従います。各サブシステムに対してこの許可を繰り返します。このアクセス権限がないと、STC ID のユーザは DB2 システムに接続できません。

注: 以下のコマンドはサンプルです。これらのコマンドの使用に関する詳細については、IBM の製品マニュアルを参照してください。

RACF を使用して RRSAF のリソース許可を作成する方法

注: サイトでこれらのタスクをすでに終えている場合、最初の 2 つの手順は必要ない場合があります。

1. (オプション) 以下のコマンドを入力して、**DSNR** にビューを設定します。

```
SETROPTS CLASSACT(DSNR)
```

このビューは **DSNR** のビューです。

2. (オプション) リソースを定義します。

```
RDEFINE DSNR DSNR.ssss.RRSAF UACC(NONE)
```

```
SSSS
```

サブシステム ID を指定します。

機能が定義されます。

3. 機能へのユーザアクセスを許可します。

```
PERMIT DSNR.ssss.RRSAF CLASS(DSNR) ID(ofa_stc_id)
```

```
ofa_stc_id
```

Object Framework Services エージェント (OFA) スターティッドタスクと関連付けられた **STC ID** を指定します。デフォルトでは「OFAPROC」になります。

エージェントが許可されます。

第 4 章：設定変更について

この章は、CA Chorus for DB2 Database Management にバックエンド製品を統合するために実行する必要がある設定タスクについて説明しています。

CA Chorus Infrastructure Management がインストールされている場合、以下のタスクがすでに完了しています。

- Xnet 設定を更新します。
- CA Insight DPM 設定を更新します。

このセクションには、以下のトピックが含まれています。

[Xnet 設定の更新](#) (P. 59)

[CA Insight DPM 設定の更新](#) (P. 61)

Xnet 設定の更新

Xnet (Execution Manager Networking) は、専用のアドレス空間でスタートアップタスクとして実行されます。Xnet は、CA Database Management Solutions for DB2 for z/OS 用の Execution Manager (Xmanager) アドレス空間で動作して、共有通信サブシステムを提供します。CA Database Management Solutions for DB2 for z/OS と CA Chorus for DB2 Database Management の間の通信を有効にするには、CA Chorus for DB2 Database Management と一緒に使用するよう Xnet 設定を更新する必要があります。

注: 「CA Database Management Solutions for DB2 for z/OS Implementation Guide」に記載されているように、Xnet のカスタマイズが完了したことを確認します。この確認には、カスタマイズ情報メンバの確認、Xnet ログファイルの割り当て、Xnet スタートアップタスク JCL の準備、Xnet スタートアップ設定の確認などが含まれます。

重要: Xnet 設定を更新する前に、CA Chorus for DB2 Database Management 用の PassTicket 設定が完了している必要があります。

以下の手順に従います。

1. `your_db2tools_hlq.CDBAPARM` の Xnet PXNPARM parmlib メンバを更新して、PassTicket のサポートに使用されるアプリケーション名 (APPL) を指定します。Xnet PXNPARM parmlib メンバの CMD エントリの前または後に、以下の行を挿入します。

PASSNAME (DB2TOOLS)

変更内容を保存します。

CA Chorus for DB2 Database Management ユーザ ログインの検証時に、PXNPARM が更新され、CA Database Management Solutions for DB2 for z/OS のアプリケーション名 (DB2TOOLS) が使用されます。

注: Xnet JCL プロシージャの INITPARM DD ステートメントで、PXNPARM スタートアップ パラメータ ファイルが選択されます。PASSNAME パラメータおよび Xnet の詳細については、「*CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide*」を参照してください。

2. Xnet スターティッドタスク (`your_db2tools_hlq.CDBASAMP` 内の PXNPROC) で、ポート、tcp、および xman ID を設定します。

PXNPROC が更新されます。

3. (オプション) スターティッドタスク プロシージャ (PTXMAN) で Xmanager の値として 0000 を使用している場合は、XMANID パラメータをリリースバージョンへ更新します。たとえば、CA Database Management Solutions for DB2 for z/OS r15 の場合は、XMANID=1500 を指定します。このパラメータは、Xnet スターティッドタスク プロシージャ (`your_db2tools_hlq.CDBASAMP` の PXNPROC) にあります。

PXNPROC が更新されます。

4. 以下のコマンドを入力して、各 Xnet 設定を再起動します。

S PXNPROC

メッセージに、Xnet スターティッドタスクが正常に初期化されたことが示されます。

CA Insight DPM 設定の更新

CA Insight DPM データの CA Chorus への転送を許可するため、CA Insight DPM データ コレクタ初期化パラメータを更新する必要があります。

注: CA Insight DPM データ コレクタは、CA Database Management Solutions for DB2 for z/OS のポストインストール処理中にセットアップされ設定されます。CA Insight DPM の設定に必要な手順の詳細については、「CA Database Management Solutions for DB2 for z/OS インストールガイド」、「CA Database Management Solutions for DB2 for z/OS 実装ガイド」、「CA Insight DPM システム リファレンスガイド」を参照してください。CA Insight DPM のベストプラクティスについては、「CA Database Management Solutions for DB2 for z/OS Best Practices Guide」を参照してください。

以下の手順に従います。

XNETAGT=YES を指定するように、CA Chorus 設定の各 DB2 サブシステムに対する CA Insight DPM データ コレクタ初期化パラメータを更新します。データ コレクタ初期化パラメータは `your_db2tools_hlq.SOURCE` の IDDCPRMS 内に存在します。

Xnet エージェントサブタスクは CA Insight DPM 初期化中に開始されます。また、CA Insight DPM が取得した XMANID 値を使用して、関連する Xmanager と Xnet のペアへの接続を定期的に試行します。CA Insight DPM は、CA Database Management Solutions for DB2 for z/OS の SETUPxx parmlib メンバの Xmanager グローバルパラメータから XMANID を取得します。

注: XNETAGT パラメータおよび CA Insight DPM データ コレクタの初期化の詳細については、「CA Insight DPM システム リファレンスガイド」を参照してください。Xmanager および Xnet の詳細については、「CA Database Management Solutions for DB2 for z/OS General Facilities Reference Guide」を参照してください。

付録 A: パフォーマンスの向上

統合バックエンド CA Database Management Solutions for DB2 for z/OS のパフォーマンスを CA Chorus for DB2 Database Management で改善するには、以下の DB2 カタログ テーブルでインデックスを作成します。

- SYSTABLES (DBNAME,TSNAME) 上のインデックス。
your_db2tools_hlq.CDBASRC (CATDTX08) のサンプル。
- SYSTABLES (TBCREATOR,TBNAME) 上のインデックス。
your_db2tools_hlq.CDBASRC (CATDTX09) のサンプル。このインデックスは、DB2 で推奨されるインデックス **DSNDTX03** です。
- *your_db2tools_hlq.CDBASRC*(CATDYX02) の
SYSSYNONYMS(TBNAME,TBREATOR).Sample 上のインデックス
- SYSRELS (IXNAME、IXOWNER) 上のインデックス
- SYSPACKAGE (NAME、COLLID) 上のインデックス
- SYSTABLESPACE (NAME) 上のインデックス
- SYSVIEWDEP (DCREATOR、DNAME) 上のインデックス。
your_db2tools_hlq.CDBASRC (CATGGX02) のサンプル。

多くのビュー、エイリアスなどがない場合、テーブルでは、SYSTABLES の TBNAME および TBCREATOR を使用するカーソルは、SYSIBM.DSNDTX03 インデックスに対して低いカーディナリティを持ちます。インデックスは、インデックス アクセス パスの代わりにテーブルスペース スキャンを使用します。

これらのインデックスを手動で更新するには、以下の手順を実行します。

1. インデックス DSNDTX03 に対する FIRSTKEYCARDF=200 および FULLKEYCARDF=2000 で SYSIBM.SYSINDEXES テーブルを更新します。

例: UPDATE SYSIBM.SYSINDEXES SET FIRSTKEYCARDF = 200, FULLKEYCARDF = 2000 WHERE NAME = 'DSNDTX03' AND CREATOR = 'SYSIBM';

2. Run RUNSTATS UPDATE(NONE).

動的なステートメント キャッシュが無効にされます。新規アクセス経路がインデックス DSNDTX03 に選択されます。

注: カタログで RUNSTATS を実行するときは常に、手動で FIRSTKEYCARDF と FULLKEYCARDF の値を更新し、前の手順を繰り返します。

付録 B: CA Chorus for DB2 Database Management インストール ワークシート

このワークシートを使用して、CA Chorus for DB2 Database Management インストールおよび設定中に指定される必要がある以下のデータ ソースからすべての必須インストールパラメータを収集します。

CA Database Management Solutions for DB2 for z/OS 設定情報

CA Chorus for DB2 Database Management をインストールおよび設定する場合、CA Database Management Solutions for DB2 for z/OS に関連する以下の情報が必要です。

展開した CA Database Management Solutions for DB2 for z/OS ターゲットライブラリの高レベル修飾子。この値(DB2TOOLS)は、*your_chorus_hlq*.CETJJCL の ETJVARs および ETJI095x メンバでも使用されます。(x は External Security Manager を表します。CA ACF2 には A、CA Top Secret には T、IBM RACF には R を使用します。

- スターティッドタスク ユーザ ID 値は以下のとおりです。
 - TPDTFEED - CA Detector ユーティリティプログラム。CA OPS/MVS が使用される場合、このタスクは CA Chorus 内の Time Series 機能コンポーネントに CA Detector データを提供します。
 - OFAPROC - CA Chorus for DB2 Database Management 内の DB2 オブジェクトマイグレーションに対する Object Framework Services エージェント (OFA)。
 - PTXMAN - Xmanager (実行マネージャ)。
 - PXNPROC - Xnet (実行マネージャ接続)。
- *your_db2tools_hlq*.PXNPROC JCL 内の PORT シンボリックに対する Xnet ポート値。DB2 サブシステムが CA Chorus for DB2 Database Management で定義されている場合、この値が指定されます。
your_chorusdba_hlq.CE3KJCL の E3KCFG10 を使用して、db2tools.cfg ファイルを更新します。*your_chorusdba_hlq*.CE3KPARAM の E3KCFG10 の PORT 値を指定します。

CA Chorus for DB2 Database Management 設定

以下の値が CA Chorus for DB2 Database Management の設定中に指定されます。

- JOB ステートメント設定 - &CAI (CA Chorus インストール データ セットが定義される *hlq*)。
- E3KCFG10 (*your_chorusdba_hlq*.CE3KPARM) のコンフェデレーション設定
 - TRACE - 初期設定処理中のトレースをアクティブにします。デフォルトは 0 です。有効範囲は 0 ~ 7 です。
 - REFRESH - 設定更新間の最低時間制限を秒単位で設定します。デフォルトは 60 です。有効な範囲は 60 ~ 300 です。
 - GLOBALAPPLID - CA Chorus for DB2 Database Management の使用に対して定義されるセキュリティ サブシステムで PassTicket 定義と関連付けられるアプリケーション名を指定します。デフォルトは DB2TOOLS です。この値はターゲット CA Database Management Solutions for DB2 for z/OS インストールに対する Xnet 開始パラメータで指定される PASSNAME() に一致する必要があります。セキュリティ サブシステム定義でそのアプリケーション名に割り当てられた実際の SESSKEY 値は、DSH z/OS システムおよび Xnet z/OS システムで同一である必要があります。Xnet が PassTicket が含まれる CA Chorus リクエストを受信すると、以下の処理が発生します。
 - Xnet はセキュリティ サブシステムを呼び出して、CA Database Management Solutions for DB2 for z/OS に対するユーザアクセス リクエストを認証します。
 - Xnet は、DSH によってユーザに対して生成された PassTicket を検証します。

注: TRACE、REFRESH および GLOBALAPPLID デフォルト値はほとんどのインスタンスで使用できます。

- CONFEDERATION1 から CONFEDERATION5 - コンフィデレーションとして知られる論理的なグループ化を作成するために、カンマ区切りの値 (CSV) 形式で Xnet 接続を識別します。CA Chorus for DB2 Database Management 設定内の各 Xnet サーバインストールに対してコンフィデレーション定義を追加: コンフィデレーションには、CA Chorus サーバと接続するのに必要な Xnet サーバ (conf)、TCP/IP ホストアドレス (host)、およびポート (port) が含まれます。APPLID が指定される場合、この値は GLOBALAPPLID 値をオーバーライドします。

例 :

```
# DEFAULT Confederation member definitions
conf=default host=system1.com port=1027
conf=default host=system2.com port=1027
#
# TEST Confederation member definitions
conf=test host=system1.com port=1229 Applid=DB2T00LS
conf=test host=system3.com port=6791 Applid=DB2T00LS
```