CA Chorus™

サイト準備ガイド

バージョン 03.0.00、第 3 版

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™ for DB2 Database Management
- CA Chorus™ Infrastructure Management for Networks and Systems
- CA Chorus™ for Security and Compliance Management
- CA Chorus™ for Storage Management
- CA Chorus™ Software Manager (CA CSM)
- CA Common Services for z/OS （CA Common Services for z/OS）
- CA Datacom®/AD （CA Datacom/AD）
- CA Datacom/DB®
- CA Easytrieve
- CA Top Secret® for z/OS （CA Top Secret）

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

以下のリストでは、第 2 版以降行なわれた変更について詳述します。

ソフトウェア要件 (P. 27) -- CCS および CA CSM の FIXCAT 要件を明確にし、CA Datacom/AD MUF を作成するジョブの順序を修正しました。

以下のリストでは、第 1 版以降行なわれた変更について詳述します。

サンプル： IBM RACF でユーザを許可する (P. 55) -- 手順 1 で CA Chorus for DB2 Database Management 参照を修正しました。 それは現在 DB2DBA といいます。

サーバ要件 (P. 30) -- 改訂されたヒープ値と選択したすべてのディシプリンを持つ新しい例を追加しました。

ソフトウェア要件 (P. 27) -- ブラウザ要件と 1.12 以降に対する更新した IBM z/OS サポート を明確にしました。

以下のリストでは、以前「*インストール ガイド*」に表示されたコンテンツから変更した点について詳述します。

全般 -- システム プログラマおよびセキュリティ管理者が製品インストール日の前に完了できるタスクを識別するためにこのガイドを作成しました。

インストール処理の実行 (P. 10) -- このガイドおよび「*インストール ガイド*」を使用する方法について説明するためにこのトピックおよび図を追加しました。

導入前の計画 (P. 13) -- この新しいガイドおよび新しい HLQ 要件トピックを説明するためにこのトピックを更新しました。

セキュリティ管理者およびシステム プログラマのチェックリスト (P. 14) -- このガイドを使用する前に 2 つの役割が一致する必要がある詳細の概要を説明するためにこのトピックを追加しました。

セキュリティ ID の再利用に関する考慮事項 (P. 21) -- 2.0 および 2.5 のセキュリティ ID を再利用するクライアント用にこのトピックを追加しました。

システム要件 (P. 32) -- ヒープ メモリ要件を削除しました。

CA Chorus サーバ要件 (P. 30) -- ヒープ メモリ要件を改訂しこの新しいトピックに移動させました。

メモリ制限 (P. 31) -- このトピックを追加しました。

ソフトウェア要件 (P. 27)

- CCS Release 14.1 および CA Datacom/AD バージョン 14 要件を明確にし、IBM 64-bit SDK for z/OS、Java Technology Edition、Version 7 Release 0 Modification 0 Service **Release 2** (5655-W44) を更新しました（オプションの JZOS batch launcher を含む）。
- 必要な PTF が RO56614 であることを示すために CA CSM 要件を更新しました。
- CA Datacom/AD メンテナンスに使用する、FIXCAT ラベルを追加しました。

ターゲット ライブラリ (P. 33)

- CETJDATV、CETJSIDE、CETJZFS1 を削除しました。
- CETJJCL、CETJTOPN、CETJXML および TPV.AETJHFS に対する値を更新しました。

配布ライブラリ (P. 34)

- TPV.AETJJAR、AETJDATV および TPV.AETJSHSC を削除しました。
- AETJJCL、AETJOPTN、AETJXML および TPV.AETJHFS に対する値を更新しました。

ポート要件 (P. 35) -- 最大要求を 17 から 12 に更新しました。

（オプション）SMTP 電子メール要件 (P. 36) -- プラットフォーム設定中に後で使用する目的で収集できるデータを説明するためにこのトピックを追加しました。

USS Parmlib 要件 (P. 36) -- この設定を確認するコマンドを追加しました。

インストーラ セキュリティ権限 (P. 37) -- FSACCESS オプションを定義しました。

CA Chorus セキュリティ ジョブの実行 (P. 39) -- このトピックを追加し、このジョブが自動化する以前の手動トピックを削除しました。

CA Chorus で作業をユーザに許可する方法 (P. 44)

- このシナリオを「*Administration Guide*」からこのガイドに移動しました。
- CA Chorus Infrastructure Management for Networks and Systems および自動リフレッシュ リソースを追加しました。
- ユーザ ソフトウェア要件の確認を削除しました。この情報は、ソフトウェア要件 (P. 27) に表示されます。
- 「（オプション）EXPLAIN コマンドをによる Secondary Authorization ID の使用を許可する」を「*CA Chorus for DB2 Database Management サイト準備ガイド*」に移動しました。

z/OS UNIX System Services リソースへのアクセスを CA Chorus ユーザに許可する (P. 46) -- これらの設定がすでに存在するかどうかを確認するための事前確認手順を追加しました。

CA Chorus 用の CA CSM PassTicket の設定方法 (P. 58) -- ETJI095*x* セキュリティ ジョブで扱う手順を説明するためにこのシナリオを更新しました。

CA Chorus 用の CA CSM PassTicket の設定方法 (P. 58) -- このシナリオを追加しました。

サンプル： IBM RACF でユーザを許可する (P. 55) -- CAMFC に各ディシプリン リソースを追加するための新しい手順 1 を追加しました。

CA Chorus セキュリティ ジョブの実行 (P. 39) -- CA CSM ユーザのサブトピック用の PassTicket を追加するためにこのシナリオを更新しました。

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

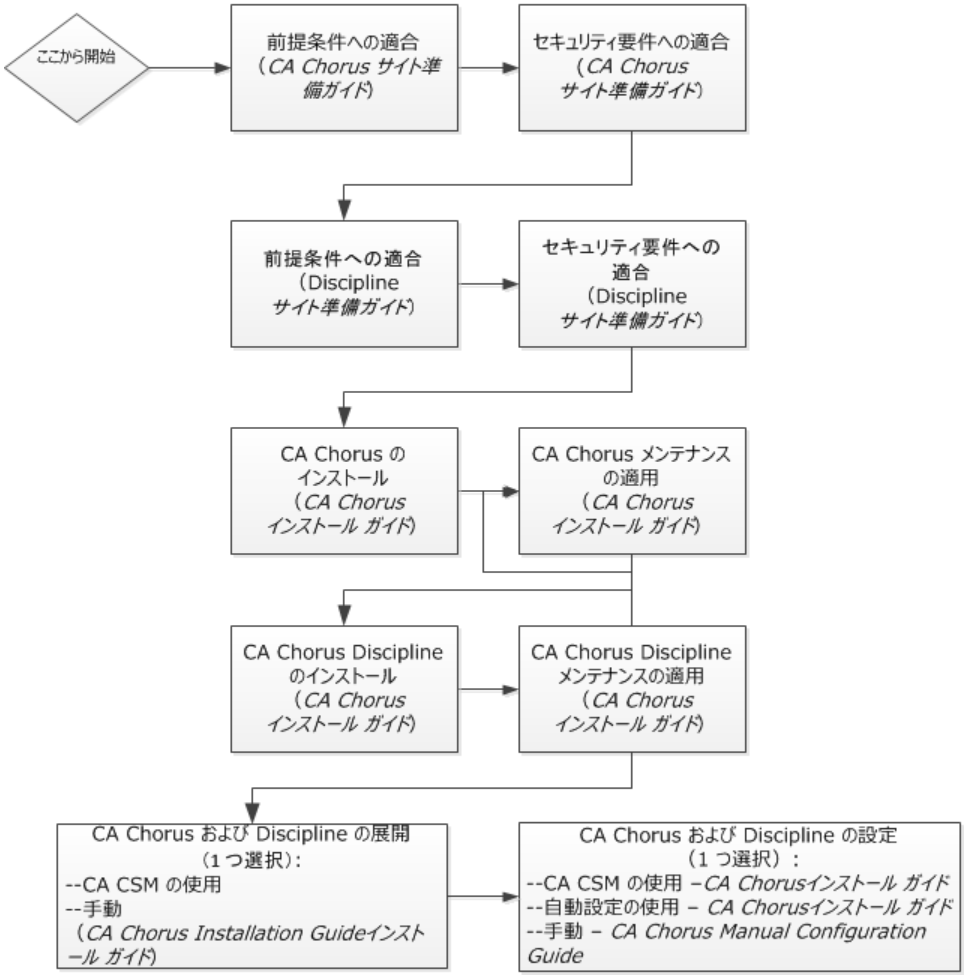
インストール処理の実行

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 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。

導入前の計画

CA Chorus インストールは、いくつかの領域の専門知識がある担当者を必要とする詳細なプロセスです。 インストールを開始する前に、以下の各チーム メンバに会い、各担当者のロールを確認することをお勧めします。

- z/OS のシステム プログラマ
- ストレージ管理者（DASD 割り当てに関して）
- アクセス許可およびセキュリティ設定のためのセキュリティ管理者
- DB2 および（または）CA Datacom/AD 設定のデータベース管理者

このミーティングについては、以下のアイテムを使用することを推奨します。

- セキュリティ管理者およびシステム プログラマのチェックリスト（P. 14）
- プラットフォームおよび適用可能なディシプリンの *サイト準備ガイド*
- *インストール ガイド*
- 適用可能なセキュリティ ジョブ ETJI095*x*。ここで x は CA ACF2 の場合は A、CA Top Secret の場合は T、および IBM RACF の場合は R に相当します。 これらのジョブは CA Chorus 製品ページにあります。

重要: チーム メンバ全員が自分のインストール責任について明確に理解するまで、インストールを開始しないでください。 そうしないと、インストールを完了する能力にタイムリーに影響する場合があります。

セキュリティ管理者およびシステム プログラマのチェックリスト

このセクション内の各テーブルでは、高レベルなインストールの詳細の概要を示します。 セキュリティ管理者およびシステム プログラマが各テーブルを一緒に確認することを推奨します。 確認後、一方がこのガイドおよび「*インストール ガイド*」で作業を開始する前に、管理者は特定の詳細に同意するか、または残りの点について認識している必要があります。

テーブル内のいくつかのエントリについては、同意済みの値を指定します。他のエントリについては、実装の詳細を調整するだけです。

重要: これらのチェックリスト内の作業を完了するまで、いかなる準備またはインストール手順も開始しないでください。たとえば、セキュリティ セットアップおよび製品設定用にこれらのテーブル内の値を必要とします。

セキュリティに関する考慮事項

下記のテーブルについて。

- セキュリティ シンボリックは & または % が頭につきます。 これらのシンボリックは、セキュリティ管理者が実行する ETJI095*x* セキュリティ ジョブに表示されます。

  %

  デフォルト値を示します。

  &

  値を確定する必要があることを示します。

- 網掛けセルは、値を記録する必要はないがこのガイドで作業を開始する前にこのコンテンツを確認する必要があることを示します。

ID または セキュリティ エンティティ	定義	値	シンボリック
CHORGRP	CA Chorus 管理グループ（オプション） デフォルト グループ名を指定します。		%CHORGRP
CHORUGRP	CA Chorus ユーザ グループ（オプション） リソースを個別のユーザにではなくグループに割り当てることで、管理が容易になるようにします。		&CHORUGRP
CA Chorus ディシプリン グループ	リソースを個別のユーザにではなくグループに割り当てることで、管理が容易になるようにします。 ユーザは、ジョブ機能に必要なディシプリン グループに接続されます。 サイトの命名標準および組織に従った名前を使用することをお勧めします。		&CHRD*x*GRP （ここで x はディシプリンを示します）

ID または セキュリティ エンティティ	定義	値	シンボリック
CHORADM	管理用（スターティッド タスクの所有者） ■ スターティッド タスクを所有します。 ■ OMVS セグメントを持っている必要があります。 ■ ユーザ用の PassTicket を生成するために使用されます。 **注**: ホーム ディレクトリは CA Chorus USS インストールと同じ場所にあることを推奨します。		%CHORADM

ID または セキュリティ エンティティ	定義	値	シンボリック
CHORTHD	補助ユーザ ■ ユーザがだれもログインしていない場合に、バックエンド機能にアクセスするためのユーザ ID としてのみ使用されます。 主に、設定データを取得するためにスタートアップ中に使用されます。 ■ PassTicket 生成で使用されます。 このユーザ ID は、ジョブまたはオンライン アクセスのために直接使用されることはありません。 このユーザ ID のパスワードへのアクセス権はだれも持つべきではありません。 RACF については、パスワードが必要です。 CA ACF2 または CA Top Secret はパスワードを使用しません。 ■ CHORJBOS は、CHORTHD 用の PassTicket を生成できる必要があります。また、CHORTHD には、適切なアプリケーション（APPLID）へのアクセス権を与える必要があります。 ■ 以下の項目を除いて、CA Chorus ユーザと同じセキュリティ権限を必要とします。 -- CAMFC -- CA Easytrieve レポート実行用の CETJOPTV CETJEZTR ■ いくつかのディシプリンは、バックエンド製品へアクセスするための CHORTHD 許可が必要となる場合があります。 詳細については、適用可能なディシプリンの「*サイト準備ガイド*」を参照してください。		%CHORTHD
インストーラ ID	インストーラのユーザ ID には新しい HLQ およびデータ セットへの更新アクセスが必要です。 インストールの後、更新権限は無効にできます。 完全な詳細については、「インストーラ セキュリティ権限 (P. 37)」を参照してください。		&INSTALLER

ID または セキュリティ エンティティ	定義	値	シンボリック
PassTicket	PassTicket リソースは CA Chorus プラットフォームによって必要とされます。 そのディシプリンは追加の PassTicket 定義を必要とします。 PassTicket アクセスはグループまたは個別の基準で定義されますか。 ■ グループは管理が容易で、おそらくより多くの分散化が可能になります。グループ権限は中央セキュリティに残りますが、ローカル(グループ)管理者はメンバシップを制御します。 ■ ユーザごとに明示的に表示されるアクセス権を持つ方がよいサイトもあります。		
	セキュリティ管理者は、各アプリケーションに対し KEYMASKED または SESSKEY の値を選択する必要があります。 ただし、それは保護する必要があるので、値はここでは入力されません。 同じ値をすべてのシステムでアプリケーションに使用する必要があります。		
	CHORWEBS： PassTicket がユーザに対して生成されるデフォルト アプリケーション ID。別の APPL を使用するつもりの場合は、その値を確認し記録します。		%CHORWEBS
	CSMAPPLM： クイック リンク モジュールから CA CSM を起動するユーザに対して PassTicket が生成されるデフォルト アプリケーション ID。 別の APPL を使用するつもりの場合は、その値を確認し記録します。 これらの手順は ETJI095*x* に存在しません。「CA CSM PassTicket の設定方法 (P. 58)」を参照してください。 クイック リンクとして CA CSM を追加していない場合は、このオプションを無視します。		&CSMAPPLM

ID または セキュリティ エンティティ	定義	値	シンボリック
CAMFC	CAMFC は、CA Chorus 専用のリソース クラスです。 クラスの名前およびエントリが修正されます。 プラットフォームは 1 つのエントリ CHORUS.SETTINGS.KNOWLEDGECENTER を有しています。Knowledge Center 内のユーザ ドキュメントを更新または保守するユーザのみが、このエントリを必要とします。 ディシプリンはそれぞれこのクラス内にエントリがあります。 ディシプリンのグループには、読み取りアクセスをそのディシプリンに対するエントリへ許可する必要があります。		
CAWEBSVR マスタ機能	CA Top Secret のみ: このマスタ機能へユーザを定義および追加する必要があります。		
プログラム制御（APF 許可）	スターティッド タスクの steplibs で命名されたデータ セットは、プログラム制御下にある必要があります。CA ACF2 または CA Top Secret を使用しているサイトについては、これらのライブラリが APF 認可される必要があります。		
	ランタイム環境用の HLQ を有するライブラリ ■ CETJPLD： CA Chorus ライブラリを含んでいます。 ■ CETJLOAD： CA Chorus ライブラリを含んでいます。 ■ CC2DLOAD： タイム シリーズ機能（TSF）ライブラリを含んでいます。		
	CA Datacom/AD 前提条件を満たす一部として、ライブラリ *datacomad_adthlq*.CAAXLOAD（CA Datacom/AD ロード ライブラリ）および *datacomad_adchlq*.CUSLIB（CA Datacom/AD カスタマイズ ライブラリ）が APF 認可される必要があります。		

ID または セキュリティ エンティティ	定義	値	シンボリック
	（IBM RACF のみ）非 CA Chorus ライブラリ CA Chorus によって使用されるライブラリは、たとえそれらが Linklist にあり、CA Chorus で明示的に指定されていない場合でも、プログラム制御にある必要があります。 これらのライブラリは、それらの製品がインストールされたとき、プログラム制御に追加されていた可能性がありますが、現在はシステム管理者がこの設定を確認する必要があります。 システム プログラマはサイト固有の名前を指定する必要があります。 ■ Java v7 m0 ライブラリ： &JAVALIB ■ CCS.CAW0LINK： CA CCS ライブラリ - リリース 14.1（リリース 2.5 CA Chorus 用） ■ TCPIP.SEZALOAD - ■ SYS1.CSSLIB： IBM からの A C++ ライブラリ		

詳細情報:

CA Chorus セキュリティ ジョブの実行 (P. 39)

セキュリティ ID の再利用に関する考慮事項

バージョン 3.0 セキュリティ ID 実装に関する以下の変更に注意します。バージョン 2.0 またはリリース 2.5 からセキュリティ ID を再利用する場合は、以下のオブジェクトを 3.0 の実装に追加します。 これらの変更に関連するサンプル コマンドを参照するには、適用可能な ETJI095*x* ジョブを参照してください。 このジョブでは、*x* は CA ACF2 には A、CA Top Secret には T、IBM RACF には R を使用します。

重要: バージョン 3.0 は、外部の CA Datacom/AD マルチユーザ機能（MUF）を必要とします。 そのため、MUF を実行するデータ セットを認識しておいてください。

CA ACF2

ユーザ ID CHORTHD： PassTicket を使用したログイン用のセカンダリ ログイン ID。

CAMFC： 新しい SETTINGS.AUTOREFRESH 機能用の CA Chorus プラットフォーム リソース。

ルール： CA Datacom/AD にカスタマイズされたライブラリ CUSLIB。

CA Chorus Software Manager クイック リンク（オプション）

CA Top Secret

ACID %CHORTHD： PassTicket を使用したログイン用のセカンダリ ログイン ID。

PROFILE %CHORUPF： CA Chorus ユーザ用のプロファイル（オプション）

CAMFC： 新しい SETTINGS.AUTOREFRESH 機能用の CA Chorus プラットフォーム リソース。

データ セット： CA Datacom/AD にカスタマイズされたライブラリ CUSLIB。

CA Chorus Software Manager クイック リンク（オプション）

IBM RACF

USERID %CHORTHD： PassTicket を使用したログイン用のセカンダリ ログイン ID。

GROUP %CHORUGRP： CA Chorus ユーザ用のグループ（オプション）

CAMFC： 新しい SETTINGS.AUTOREFRESH 機能用の CA Chorus プラットフォーム リソース。

データ セット： CA Datacom/AD にカスタマイズされたライブラリ CUSLIB。

特定のライブラリ用の一般的なデータ セット プロファイル

CA Chorus Software Manager クイック リンク（オプション）

詳細情報:

CA Chorus セキュリティ ジョブの実行 (P. 39)

データ セットの考慮事項

下記のテーブルについて。

- セキュリティ シンボリックは & または % が頭につきます。 これらのシンボリックは、セキュリティ管理者が実行する ETJI095*x* セキュリティ ジョブ (P. 39) に表示されます。

  %

  デフォルト値を示します。

  &

  値を確定する必要があることを示します。

- 網掛けセルは、値を記録する必要はないがこのガイドで作業を開始する前にこのコンテンツを確認する必要があることを示します。

データ セット	考慮事項	値	シンボリック
既存	データ セットが以前にユーザのセキュリティ製品で定義されていない場合、場合よっては CA Chorus ID によるアクセスを許可する前に、グループおよびプロファイルも定義する必要があります。		

データ セット	考慮事項	値	シンボリック
	TCP/IP スターティッド タスクの SYSTCPD DD ステートメントで命名されるようなライブラリのデータ セットまたはメンバは、CHORADM に使用可能である必要があります（読み取り専用）。このデータ セットはシステムによって変わります。		&TCPDATA
	Java v7 ライブラリは CHORADM および CHORUGRP に使用可能である必要があります（読み取り専用）。		&JAVALIB
	UNIX System Service（USS）Java Home ディレクトリは、CHORADM への読み取りアクセスが許可されている必要があります。 これには、マウントされたファイル システムへの読み取り FSACCESS も必要な場合があります（FSACCESS が使用可能な場合）。		@JAVA_HOME **注**: セキュリティのためにこの値は必要ありませんが、それにマウントされるデータ セットが必要な場合があります。
CA Chorus インストール データ セット	チームは、CA Chorus インストールに関する HLQ に同意する必要があります。 **注**: インストール HLQ はランタイム環境とは異なります。場合によっては、両方を定義する必要があります。デフォルト値はこれらのエントリに対して提供されません。 サンプル JCL は、ランタイム環境を確立するためのコマンドを提供します。		
	HLQ： インストール環境		なし
	HLQ： ランタイム環境		$CAI @RT_HLQ
ランタイム データ セット	CA Chorus 用の追加の HLQ		

データ セット	考慮事項	値	シンボリック
	VSAM データセット用の HLQ VSAM ファイルが特定の割り当て要件を持っているべきであることをサイト標準が示す場合、別の HLQ を VSAM データ セットに割り当てることができます。		$TSF
	データベース ファイル用の HLQ。CA Chorus によって使用される CA Datacom/AD データ ファイルを区別することもできます。これらのファイルは CA Chorus 専用に作成された MUF で使用されます。		$ADHLQ
CA Datacom/AD インストール データ セット	CA Chorus による使用については、以下のランタイム HLQ が必要です。詳細については、「*CA Datacom/AD インストール ガイド*」を参照してください。		
	CAAXLOAD を含む CA Datacom/AD システム ライブラリ。HLQ を記録します。		&ADTHLQ
	CA Chorus インスタンスに固有のライブラリ（CUSLIB）。 HLQ を記録します。		&ADCHLQ

スターティッド タスクの考慮事項

下記の表について。

- セキュリティ シンボリックは & または % が頭につきます。 これらのシンボリックは、セキュリティ管理者が実行する ETJI095*x* セキュリティ ジョブ (P. 39)に表示されます。

  %

  デフォルト値を示します。

  &

  値を確定する必要があることを示します。

網掛けセルは、値を記録する必要はないがこのガイドで作業を開始する前にこのコンテンツを確認する必要があることを示します。

注: ディシプリンは、また実行しそうなそれらの関連する製品のジョブまたはスターティッド タスクを必要とする場合もあります。 これらの項目については、それぞれの製品ガイドで説明します。

項目	定義	値	シンボリック
スターティッド タスク	CA Chorus には複数のスターティッド タスクと 1 つの生成されたタスクがあります。 サイト標準および基本設定に従ってそれらを命名することができます。 デフォルト名は次のとおりです。		
	CHORJBOS : JBoss サーバ CA Chorus アプリケーションをホストします。 JBoss はクロスプラットフォームで動作する、オープン ソースの Java ベース アプリケーション サーバです。 JBoss は、Java をサポートするあらゆるオペレーティング システム上で動作します。		CHORJBOS

項目	定義	値	シンボリック
	CA Datacom/AD マルチユーザ機能（MUF） MUF は、システムのマネージャで、データ用のオペレーティング システムとして機能的に働きます。 それはアプリケーションからリクエストを受信し、どのようにそれを処理するべきかを決定します。 それは、リクエストをサービスするために発生する必要があるアクティビティを調整します。CA Chorus のインストールへの前提条件として新しい専用の MUF を構築します。 作成する MUF 名を記録します。		&AD_MUF_STCID
	MUF OWNER： MUF スターティッド タスクを所有するユーザ ID。		&AD_MUF_OWNER
	CHORTSF： タイム シリーズ機能（TSF） TSF では、折れ線グラフ内のパフォーマンス データを表示できます。		%CHORTSF
	CHORTSFR： タイム シリーズ機能リレー タスク TSF データ リレーでは、リモート LPAR 上で収集されたデータを TSF に送信できます。		%CHORTSFR
	CHORJBOS は、CA DSI セキュリティ検証用の別のタスクを生成します。 このタスクに CHORJBOS に対して選択された名前とは別の名前をつけたい場合は、BPX.SUPERUSER および BPX.DAEMON 機能への CA Chorus 管理ユーザ ID 読み取りアクセス権を付与します。		

ソフトウェア要件

CA Chorus には、以下のソフトウェアが必要です。

- CA Technologies ソフトウェア - 以下のソフトウェアが必要です。
  - CAIRIM および CAMASTER サービス コンポーネントを含む CA Common Services for z/OS (CCS) Release 14.1、および CA Easytrieve Release 11.6。
  - 以下の FIXCAT ラベルを有する CCS メンテナンスをすべて適用します： CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0。

    CCS

    サービス コンポーネントは CCS を使用して配信されインストールされます。 他の CA Technologies 製品をサイトにインストールする場合は、これらのサービスおよびその他のサービスがインストールされることがあります。 これらのサービスがまだインストールされていない場合は、ここでインストールしてください。 これらのコンポーネントのインストールおよび設定の詳細については、CCS ドキュメント を参照してください。

    重要: CAMASTER アドレス空間が実行されている必要があります。それが実行している場合、以下のメッセージがメッセージの IPL 部分の一部として z/OS syslog にあります。
    CAMS101I CAMASTER INITIALIZATION COMPLETE.
    CAMASTER は、さまざまな CA 製品および CCS 用のシステム サービスおよびストレージ リソースを提供する解約不可能なスターティッド タスクです。 CAMASTER は、最小の CPU を使用し、停止または再起動はできません。

    注: CCS 前提条件を満たす一部として、CAW0LOAD ロード ライブラリが APF 認可される必要があります。

    CA Easytrieve

CCS Release 14.1 の前に、CA Easytrieve は Easytrieve Service CDX8E00 として提供されました。 CCS Release 14.1 をはじめとして、CA Easytrieve はスタンドアロンの pax インストールとして提供されます。 CA Easytrieve の単一のインストールは、CA Easytrieve の複数のインストールを必要とすることなく、CCS モードまたは完全な機能モードで稼働できます。 CCS 14.1 は、そのパッケージに CA Easytrieve Release 11.6 を同梱しています。CA Easytrieve 11.6 をすでにインストールしている場合は、CCS 14.1 とともに配布されるコピーをインストールする必要はありません。それらは同じものです。 CA Easytrieve Release 11.6 をインストールしていない場合は、「*CA Easytrieve Release 11.6 インストール ガイド*」の付録 B に記載されている手順に従ってください。

- CA Chorus Software Manager (CA CSM) Release 5.1 (RO56614)： CA Chorus をインストールするには CA CSM を使用する必要があります。
- 以下の FIXCAT ラベルを有する CA Datacom/AD メンテナンスをすべて適用します：
  CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0

  重要: CA CSM がシステム設定で製品固有のファイル システムを使用するように設定されていることを確認してください。 この設定を確認するには、CA CSM の［Settings］タブを使用します。［Software Installation］をクリックし、右ペインの［SIS Base Install-File System］をスクロールして、［Product Specific File System］が選択されていることを確認します。

  重要: CA Chorus は zFS ファイル システムのみをサポートします。HFS ファイル システムはサポートされていません。

- CA Datacom/AD バージョン 14

  注: CA Chorus は CA Datacom/DB をサポートしません。 CA Datacom/DB をインストールしている場合は、CA Datacom/AD をインストールし、CA Chorus をインストールするときにそれらのライブラリを参照します。

  - 完全な CA Datacom/AD のインストールおよび設定が必要です。「*CA Datacom/AD インストール ガイド*」を参照してください。
  - 以下の FIXCAT ラベルを有する CA Datacom/AD メンテナンスをすべて適用します：
    CA.ProductInstall-RequiredService.CA-Mainframe-Chorus.V3.0
  - CA Datacom Server を含む CA Datacom/AD コンポーネントをすべてインストールします（CA CSM インストール ウィザードから［Base Install + USS Client for DBSRV, FMID CAYTE02］を選択）。CA Datacom Server には、UNIX System Services（USS）下で実行する JDBC コンポーネントが含まれます。
  - 新規および空の CA Datacom/AD MUF: 以下のメンバを実行して、CA Datacom/AD MUF を構築する必要があります。インストール中に使用するために定義する MUF 名を記録します。 MUF を作成する正確な手順については、「*CA Datacom/AD Installation Guide*」内の INSTJCL メンバ トピックを参照してください。

    注: CA Datacom/AD 前提条件の一部として、ライブラリ *datacomad_adthlq*.CAAXLOAD（CA Datacom/AD ロード ライブラリ）および *datacomad_adchlq*.CUSLIB（CA Datacom/AD カスタマイズ ライブラリ）が APF 認可される必要があります。

    AXCUS00： インストール JCL データ セットを構築、入力、およびマス編集します。

    AXCUS01： CA Datacom/AD MUF 用のカスタマイズをすべて含んでいます。

    AXAPFADD： APF によりリスト化されるライブラリを動的に追加するための CA SYSVIEW の例を含んでいます。

    AXRIM01： PC CALLS をインストールします。

    AXNEW01： MUF が必要とするデータ セットを割り当てて入力します。

    AD14STRT： MUF を開始するサンプル JCL。

    AXIVP01： サンプル インストール検証 JOB。

注: ターゲット ランタイム ライブラリを共有できますが、MUF は共有できません。

- IBM ソフトウェア - 以下のソフトウェアが CA Chorus をインストールするシステムで利用可能である必要があります。
  - IBM z/OS 1.12 以上
  - IBM z/OS UNIX System Services (USS) support for zFS file systems
  - IBM z/OS システム ロガー
  - IBM 64-bit SDK for z/OS、Java Technology Edition、Version 7 Release 0 Modification 0 Service Release 2 (5655-W44)（オプションの batch launcher を含む）

    注: CA Chorus でバッチ レポートを生成するには、IBM 31-bit SDK for z/OS、Java Technology Edition、Version 7 Release 0 Modification 0（5655-W43）が必要です。 この機能は、CCS の CA Easytrieve サービス コンポーネントを使用します。
- 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められるようにします。

CA Chorus サーバ要件

CA Chorus は、各ディシプリンに対する以下の追加のヒープ要件を有する 2450MB のヒープメモリを必要とします。

- CA Chorus for DB2 Database Management 用に 200MB
- CA Chorus Infrastructure Management for Networks and Systems 用に 200MB
- CA Chorus for Security and Compliance Management 用に 100MB
- CA Chorus for Storage Management 用に 200MB

すべてのディシプリンを選択する場合は、最低 3150 MB の実ストレージを CA Chorus サーバが実行されている LPAR に割り当てます。デフォルト値です。

ヒープ メモリ サイズを増やすには、*chorus_runtime_hlq*.CETJOPTN の ENVETJ メンバで Java ヒープ サイズ（Java SDK オプション）設定を確認してください。 ヒープ範囲については、-Xms が開始値で、-Xmx が終了値です。

例

すべてのディシプリンを持つ CA Chorus は以下を必要とします： 2450MB + 200MB + 200MB + 200MB + 100MB = 3150MB

ストレージとセキュリティのディシプリンを持つ CA Chorus は以下を必要とします： 2450MB + 200MB + 100MB =2750 MB

メモリ制限

z/OS は、ジョブに対して指定される REGION= および MEMLIMIT= パラメータの値に基づくメモリ制限を設定します。 ただし、制限を無視するために使用できるインストール EXIT もあります。たとえば、IEFUJV、IEFUSI、IEALIMIT、JES2 Exit 6 または JES3 Exit IATUX03 などです。 GETMAIN リクエストが行われる場合、それは使用可能な制限内で満たされる必要があります。すなわち、制限内の隣接する空き容量は使用可能である必要があり、そうでないとリクエストは失敗します。

CA Chorus は、REGION=0M で実行されるように設計されています。 REGION=0M はデフォルトとして配布されます。 IBM は、「制限はありません」ということを意味するためにこのシナリオを定義します。 そのため、z/OS のデフォルト値がオーバーライドされない場合、標準以下のメモリ、標準以上だがバーを下回るメモリ、およびバーを上回るメモリはすべて割り当てに使用可能です。 REGION に対する他の値も、バーを下回るメモリの制限、バーを上回るメモリがないデフォルトをもたらします。 これらの場合にバーを上回るメモリを取得するには、MEMLIMIT に対するゼロ以外の値を指定する必要があります。

インストールは、SYS1.PARMLIB の SMFPRMxx メンバで MEMLIMIT に対するデフォルト値を指定できます。 値が指定されない場合、z/OS のデフォルトは MEMLIMIT（00000M）となり、バーを上回るメモリは使用可能ではありません（前述したように、REGION=0M が指定される場合を除く)。 MEMLIMIT=nnnnnM も JCL で JOB または EXEC ステートメントに指定できます。 JCL 内の値は、SMFPRMxx メンバからのデフォルトを常に無視します。 IEFUSI EXIST は、MEMLIMIT を無視するために使用できる唯一のものです。 アクティブなデフォルト値を検索するには、以下のコンソール コマンドを入力してアクティブな SMF オプションを表示します。

```
D SMF,O
```

システム要件

サイトが以下のシステム要件に取り組んでいることを確認します。

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。

ディスク

- CA Chorus 展開を実行するには、約 11,050 個のシリンダが必要です。
- インストールには約 5,300 個のシリンダが必要です。
- pax インストール ファイルを保持する zFS 上で、約 1,500 個のシリンダが必要です。

  注: インストールを完了した後、pax ファイルを削除して空き領域にできます。
- DASD 上のセカンダリ スペース割り当てが利用可能である必要があります。

注: タイム シリーズ機能に対するインストール後のディスク領域の推奨事項については、「*Administration Guide*」を参照してください。

ターゲット ライブラリ

以下のテーブルは、CA Chorus 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ています。

データ セット名	トラック数
CC2DEXEC	3000
CC2DLINK	15
CC2DLMD0	5
CC2DLOAD	750
CC2DLPA	4
CC2DMAC	20
CC2DSAMP	330
CC2DVSMI	2250
CETJDATA	15
CETJEXEC	600
CETJEZTR	10
CETJJCL	75
CETJLMDR	75
CETJLOAD	75
CETJMAC	20
CETJOPTN	30
CETJOPTV	5
CETJPLD	2250
CETJPROC	10
CETJSAMP	20
CETJVSMI	1425
CETJXML	750

データ セット名	トラック数
CETJZFS0（zFS ディレクトリ）	60000

注: CA CSM はマウント ポイント（それが以前に存在しない場合）を作成し、新しいファイル システムを自動的にマウントします。

配布ライブラリ

以下のテーブルは、CA Chorus 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ています。

データ セット名	トラック数
AC2DEXEC	3000
AC2DLOAD	750
AC2DMAC	20
AC2DMOD	750
AC2DSAMP	330
AC2DVSMI	2250
AETJDATA	15
AETJEXEC	600
AETJEZTR	10
AETJJCL	75
AETJLOAD	75
AETJMAC	20
AETJMODE	15
AETJMODR	75
AETJOPTN	30
AETJOPTV	5
AETJPLD	2250
AETJPROC	10
AETJSAMP	20

データ セット名	トラック数
AETJVSMI	1425
AETJXML	750
AETJZFS	9750
TPV.AETJHFS	14850

CA CSM 一時ストレージ要件

CA CSM のインストール中に、［User Settings］で指定されたオプション用に以下のストレージ要件が必要です。

- User Unpax Temporary Directory 用のディレクトリにマウントされる zFS 上に、約 1,000 個のシリンダ。
- GIMUNZIP Temporary Prefix 用に作成されたデータ セット用に、約 700 個のシリンダ。
- Temporary Data Set Prefix 用に作成されたデータ セット用に、約 300 個のシリンダ。

注: CA CSM は、一時展開ファイル システムを作成して CA Chorus 展開を処理するために、約 2,000 個のシリンダを必要とします。 これらの設定の詳細については、CA CSM 製品ドキュメントを参照してください。

ポート要件

CA Chorus には、JBoss サーバおよびタイム シリーズ機能（TSF）コンポーネント用のポート要件があります。

- CA DSI サーバおよび JBoss サーバ用の連続する 12 のポート。 JBoss ポートは、1 つの双方向 DSI（接続およびリスニング）ポートと、11 のサーバ（リスニング）ポートで構成されます。
- TSF 用の 3 つの一方向ポート。

  注: TSF インスタンスがリモート LPAR に使用されている場合、もう 2 つの一方向ポートがインスタンスに必要です。

これらのポートは後で JBoss サーバおよび TSF 設定中にインストール時に設定されます。

使用するつもりのポートが使用可能であることを確認するには、ネットワーク管理チームに相談してください。

（オプション）SMTP 電子メール要件

Investigator（CA Chorus インターフェース内にあります）では、パフォーマンス ポリシーを満たした際に通知されるように、電子メール アクションを指定できます。

たとえば、指定された時間間隔において製品へのログイン試行が失敗したユーザの数が *x* 人になったときに通知されるように Investigator でポリシーを作成することができます。その製品で SMTP を設定している場合は、ポリシー基準が満たされたことを知らせる電子メールを受信できます。そうすることでこのタイプの通知が自動化されます。

サイトでこの機能を使用する場合は、以下の情報を確認します。 この情報は後で CA Chorus を設定する場合に使用します。

SMTPHOST

SMTP メール サーバの名前/IP アドレス。

SMTPPORT

SMTP メール サーバのポート番号（1024 ～ 65535）。

USS Parmlib の要件

z/OS parmlib メンバ BPXPRM*xx* で、CA Chorus は MAXFILEPROC(64000) を必要とします。

設定を確認するには、MVS コンソールから以下のコマンドを入力します。

```
D OMVS,OPTIONS
```

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

インストール処理を開始する*前に*、CA Chorus 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.PFSCTL プロファイル

- z/OS：
  - CA Chorus 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。

外部セキュリティ製品によって実行される必要がある APF 許可およびその他のセキュリティ要件は、「*インストール ガイド*」記述されているように、CA Chorus 設定プロセス中に定義されます。 インストール パッケージからさまざまなジョブおよびメンバにアクセスする必要があるので、インストール中にそれらのタスクを完了します。

CA Chorus セキュリティ ジョブの実行

ETJI095*x* セキュリティ ジョブは、多くのセキュリティ要件を満たす方法を簡略化します。 セキュリティ ジョブは以下のように識別されます：ETJI095*x*、ここで x は CA ACF2 には A、CA Top Secret には T、IBM RACF には R を使用します。 これらのジョブは CA Chorus 製品ページにあります。

以下のリストでは、ジョブが取り組むセキュリティ要件について詳述します。

重要: この *トピックの最後*にある手順に進む前に、以下の概念資料を確認してください。

(CA Top Secret のみ)マスタ機能

CA Top Secret を使用している場合は、マスタ機能を定義し、CA Chorus スターティッド タスクと関連付けます。 マスタ機能として CAWEBSVR を使用します。 マスタ機能（MASTFAC キーワード）によって CAWEBSVR 機能にアクセスできます。 マスタ機能として機能を使用するには、まずシステム機能マトリックスでそれを CA Top Secret にユーザ機能として定義します。

重要: このタスクを 1 回のみ実行します。 CAWEBSVR を機能マトリックスに追加し、定義をアクティブにしている場合は、このタスクを繰り返さないでください。

その後、CA Chorus にアクセスするすべてのユーザ ACID 用に、CA Top Secret 機能 CAWEBSVR を許可します。

管理者ユーザ ID およびグループ ID

以下の条件が満たされるように、定義済みの UNIX System Services（USS）セグメントを有する 1 つのユーザ ID（デフォルトでは CHORADM）を使用して、CA Chorus を実行します。

- ユーザ ID には UID(0) でない有効な UID がある。
- デフォルトのシェルとしてシェルが指定されている（通常は /bin/sh）。
- ユーザ ID に有効な OMVS グループがある。

注: ホーム ディレクトリは CA Chorus インストール パスと同じであることを推奨します。

ETJI095*x* ジョブを実行すると、以下のセキュリティ ユーザ ID が作成されます。 デフォルト値が使用されない場合は、セキュリティ ジョブでの CHORADM および CHORGRP の発生をすべて変更します。

CHORADM

CA Chorus の実行に使用されるスターティッド タスク ユーザ ID。

CHORGRP

デフォルト グループ名。 このグループは、すべての関連するセキュリティ オブジェクト間の関係を作成します。

CHORTHD

アプリケーションに関連する PassTicket リクエスト用のユーザ ID。

注: CA Chorus スターティッド タスクのユーザ ID には、一意の USS UID および GID （ユーザ ID とグループ ID 番号）を使用する必要があります。 追跡を容易にするために、数的に一致する UID と GID を選択します。

重要: すべてのユーザ（インストールするユーザを含む）は、このメンバで指定されたグループへのアクセス権が必要です。 デフォルトのグループは CHORGRP です。

スターティッド タスク

ETJI095*x* ジョブを実行すると、以下のスターティッド タスクが定義されます。デフォルト値が表示されます。デフォルトの名前をスターティッド タスクに使用しない場合は、セキュリティ ジョブでの名前を変更します。

注: すべての CA Chorus タスクを、REGION=0M でスターティッド タスクとして実行することをお勧めします。 サイトで REGION=0M パラメータを制限している場合は、許可される最大の領域サイズで実行することをお勧めします。

your_muf_name

CA Chorus 用の CA Datacom/AD MUF と関連付けられるスターティッド タスク名。 この名前は、以前 MUF に割り当てた名前に依存します。

CHORTSF

タイム シリーズ機能（TSF）と関連付けられるスターティッド タスク名を指定します。

CHORTSFR

リモート TSF 設定と関連付けられるスターティッド タスク名。このスターティッド タスクは、TSF データ リレーが定義されている場合にのみ作成されます。

CHORJBOS

JBoss サーバと関連付けられるスターティッド タスク名。

リソース クラス

CA Chorus はクラス CAMFC でセキュリティ リソースを定義します。セキュリティ製品を使用して、それを定義します。 その後、場合に応じてユーザにディシプリン固有のリソースへの許可を割り当てます。 **注**: 必要なユーザ権限の詳細については、ディシプリン固有の「インストール ガイド」を参照してください。

一般ユーザ用の PassTicket

PassTicket は、ユーザが CA Chorus とそのサポートされたディシプリンが使用する z/OS コンポーネントおよび製品にアクセスするために必要です。 *PassTicket* は、特定のアプリケーションへのアクセスに使用できる、一時的にエンコードおよび暗号化された、ユーザ パスワードの代用です。 PassTicket は、生成後 10 分以内に使用する必要があります。

PassTicket を使用することで、z/OS コンポーネントおよび製品が、ネットワーク経由で z/OS パスワードを送信せずにユーザ ID を認証できるようになります。 この代わりに、ユーザは有効な z/OS ユーザ ID およびパスワードでの最初のログイン後に認証されます。 ユーザが z/OS コンポーネントにアクセスする機能を選択すると、以下のプロセスが発生します。

- CA Chorus Web サービスは、アクセス許可用の PassTicket を生成するために z/OS セキュリティ製品を呼び出します。
- PassTicket はユーザ リクエストと一緒にコンポーネント宛てに送信されますが、そのコンポーネントは別の z/OS システム上にある可能性があります。

  そのコンポーネントは、リクエストを処理する前に、パスワードの代用として PassTicket を使用し、z/OS セキュリティ製品を呼び出して、ユーザを認証します。

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 SRM、CA NetMaster NM for TCP/IP 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 ディシプリンに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、CA Chorus ユーザへのエントリ 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。

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 ディシプリン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。ユーザのサイトが以下の条件を満たしている場合、リモート システム上で追加のセキュリティ セットアップは必要ありません。

- z/OS 設定内のセキュリティ製品が共有セキュリティ データベースを使用しています。
- 1 つ以上のリモート システムを追加する場合、CA Chorus サーバ システム セットアップのみが必要です。

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 CSM ユーザ用の PassTicket

CA Chorus は PassTicket セキュリティを使用して、ユーザが別のユーザ ログインを必要とすることなく、クイック リンク モジュールから CA CSM を起動できるようにします。 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。 以下の要件に注意してください。

- CA Chorus インスタンスおよび CA CSM インスタンスが*別の*マシン上に存在する場合は、このジョブを実行した後に「CA Chorus 用の CA CSM PassTicket の設定方法 (P. 58)」にある該当する手順を完了してください。
- CA Chorus インスタンスおよび CA CSM インスタンスが*同じ*マシン上に存在する場合は、このジョブを実行した後に CA CSM passticket 設定が 1 つの例外を除いて完了します。 CA ACF2 を使用している場合は、「サンプル： CA ACF2 を使用した CA Chorus から CA CSM への接続用の PassTicket の設定 (P. 61)」にある 1 つの CA Chorus サーバ側と CA CSM 側の手順を完了します。

次の手順に従ってください:

1. 外部セキュリティ マネージャに適用される ETJI095*x* ジョブを取得します。 これらのジョブは CA Chorus 製品ページにあります。
2. メンバ ETJI095*x* の全体を確認します。
3. メンバ コメントに従ってジョブを編集します。
4. メンバをサブミットします。

   記述したセキュリティ要件が満たされます。
5. （CA Top Secret のみ）適用可能な CA Top Secret パラメータ ファイル（PARMFILE）に、以下の行を追加します。

   ```
   FACILITY(USERxx=NAME=CAWEBSVR)
   FACILITY(CAWEBSVR=PGM=********)
   FACILITY(CAWEBSVR=ACTIVE,SHRPRF,MULTIUSER,AUTHINIT)
   ```

   xx

   ユーザ機能番号。 システム上で、利用可能な任意のユーザ機能番号を使用できます。

詳細情報:

セキュリティに関する考慮事項 (P. 15)
セキュリティ ID の再利用に関する考慮事項 (P. 21)

CA Chorus での作業をユーザに許可する方法

セキュリティ管理者は、製品へのユーザ アクセス リクエストをすべて管理します。 CA Chorus については、セキュリティ管理者は以下のタスクを実行する必要があります。

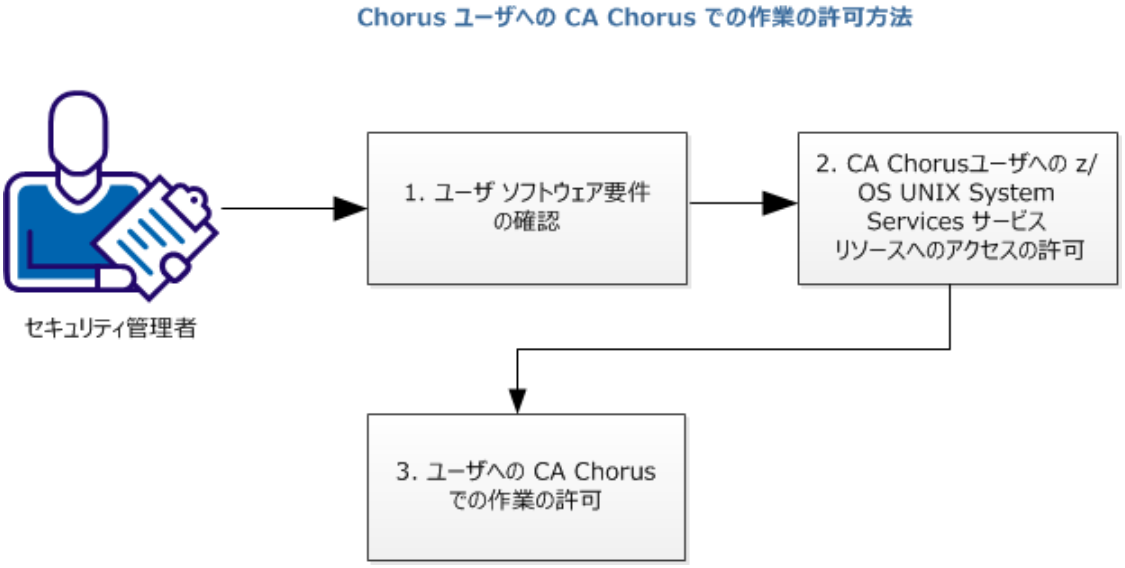
- 各ユーザの UNIX System Services（USS）環境を認可し確認します。
- CA Chorus およびそのサポートされたディシプリンで作業することをユーザに許可します。

注: CA Chorus はクラス CAMFC でセキュリティ リソースを定義します。アクセスを制限し、特定のユーザが製品にログインできないようにするために、CAMFC リソース クラスおよびユーザ アクセス許可を削除できます。

これらの権限を実行するには、セキュリティ管理者は CA ACF2、CA Top Secret または IBM RACF を使用します。

以下の図では、CA Chorus およびそのサポートされたディシプリンでユーザが作業することを許可するためのタスクについて説明しています。

注: 任意の順番でタスクを完了できますが、この図で表示される順番でタスクを実行することをお勧めします。



CA Chorus での作業をユーザに許可するには、以下のタスクを完了します。

1. ユーザ ソフトウェア要件の確認。 (P. 45)
2. z/OS UNIX System Services リソースへのアクセスを CA Chorus ユーザに許可する。 (P. 46)
3. CA Chorus での作業をユーザに許可する。 (P. 48)

ユーザ ソフトウェア要件の確認

- 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められるようにします。

USS リソースへのアクセスを CA Chorus ユーザに許可する

CA Chorus コンポーネントおよびディシプリンは、z/OS TCP/IP 通信サービスおよび z/OS UNIX System Services（USS）を使用します。 CA Chorus で作業する場合に z/OS USS リソースにアクセスできるように、各ユーザに対し OMVS セグメントを定義します。このアクセスを有効にするには、CA ACF2、CA Top Secret または IBM RACF を使用します。

z/OS USS リソースへのアクセスを CA Chorus ユーザに許可するには、以下のオプションが含まれる各ユーザに対し OMVS セグメントを定義します。

- デフォルト シェル プログラムの指定（PROGRAM または OMVSPGM）
- 数値の z/OS USS ユーザ ID（UID）

  注: ポリシーは、OMVS UID 番号を割り当てる目的でユーザのサイトに存在することもできます。 そうでない場合は、一意の番号を使用します。
- 数値の z/OS USS グループ ID（GID）

次の手順に従ってください:

1. ユーザが OMVS セグメントへのアクセス権があるかどうかを確認します。
   - CA ACF2:

     `LIST *userid* profile(all) section(all)`
   - CA Top Secret:

     `TSS LIST(*userid*) DATA(ALL)`
   - IBM RACF：

     `LISTUSER *userid* OMVS NORACF`

   ユーザがこのアクセス権を持っていない場合は、次の手順に移動します。
2. 各ユーザ ID（UID）と関連付けるホーム ディレクトリを作成します。

   たとえば、UID*nnn* に対して /u/name という名前のディレクトリをセットアップするには、OMVS UNIX シェルで以下のコマンドを発行します。

   ```
   mkdir /u/name
   chown nnn /u/name
   chmod 775 /u/name
   ```

3. 所有者およびディレクトリへのアクセスを確認します。

   ```
   ls -ld /u/name
   ```

   以下のサンプル結果が表示されます。

   drwxrwxr-x 2 **user** group 8192 Sep 31 14:58 **/u/name**

   太字部分は、正しい所有者および読み取り/書き込みのアクセス権が存在することを示します。

4. セキュリティ製品を使用して、OMVS セグメントを定義します。

   注: 有効なグループ レコードはこれらのコマンドを実行する前に存在する必要があります。

   - CA ACF2:

     CHANGE *userid* UID(*uid*) HOME(*path_name*) OMVSPGM(/bin/sh) GROUP(*ggggg*)

   - CA Top Secret:

     TSS ADD(*userid*) HOME(*path_name*) OMVSPGM(/bin/sh) UID(*uid*) GROUP(*ggggg*) DFLTGRP(*ggggg*)

   - IBM RACF：

     ALU *userid* OMVS(UID(*uid*) HOME(*path_name*) PROGRAM(/bin/sh)) GROUP(*ggggg*) DFLTGRP(*ggggg*)

     以下の構文変数が 3 つのセキュリティ製品すべてに適用されます。

     userid

     ユーザ ID を示します。

     path_name

     各ユーザ ID と関連付けるホーム ディレクトリを示します。

     uid

     ユーザ識別（UID）番号を示します。

     ggggg

     OMVS グループを示します。

5. OMVS セグメントのコンテンツを確認します。
   - CA ACF2:

     ```
     LIST userid profile(all) section(all)
     ```
   - CA Top Secret:

     ```
     TSS LIST(userid) DATA(ALL)
     ```
   - IBM RACF：

     ```
     LISTUSER userid OMVS NORACF
     ```

これでユーザは定義された OMVS セグメントがあるので USS にアクセスできます。そのセグメントは、ユーザが CA Chorus で作業するのに必要なものです。

CA Chorus で作業することをユーザに許可する

CA Chorus のサポートされたディシプリンへのアクセス許可を追加または削除できます。 これらの許可によって、ユーザは必要なディシプリンおよび機能にアクセスできるようになります。 CA Chorus は、必要なすべての許可に対して、リソース名高レベル修飾子 CHORUS を使用します。 CA Chorus は、ユーザが適用可能なリソースへの READ アクセスを持っているかを確認します。 また、Knowledge Center 内のコンテンツを管理し、自動リフレッシュ オプションを使用するための許可を変更できます。 そうするには、CA ACF2、CA Top Secret または IBM RACF の機能に従って CA Chorus で作業することをユーザに許可します。

- CA ACF2 でユーザを許可する（P. 49）
- CA Top Secret でユーザを許可する（P. 52）
- IBM RACF でユーザを許可する（P. 55）

注: Knowledge Center は、CA Chorus 内のすべてのドキュメント用のリポジトリです。 Knowledge Center コンテンツには、CA 製品ドキュメント、ユーザに生成されたドキュメント、Chicago-Soft MVS/Quick-Ref、Web サイトおよびサードパーティ ドキュメントへのリンクを含めることができます。

サンプル: CA ACF2 でユーザを許可する

CA Chorus にログインでき、特定のディシプリンを使用できるユーザを識別するためにこの手順を使用します。 さらに、ユーザに以下のタスクの実行を許可することができます。

- Knowledge Center 内のコンテンツへのインデックス付け。 コンテンツにインデックスを付けることで、ユーザはこのリポジトリからドキュメントを追加または削除することができます。
- 自動リフレッシュ オプションの使用。 このオプションは、バックエンド データが変更するたびに、CA Chorus UI に表示されるデータをリフレッシュします。

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の詳細については、「*CA ACF2 Administration Guide*」を参照してください。

ユーザ アクセス許可を定義するには、以下のコマンドを入力します。

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid1) SERVICE(READ)
ALLOW)
RECKEY CHORUS ADD(resource-name UID(uid-of-userid2) SERVICE(READ)
ALLOW)
...
RECKEY CHORUS ADD(resource-name UID(uid-of-useridn) SERVICE(READ)
ALLOW)
```

resource-name

ユーザがアクセスを許可される CA Chorus リソースを示します。

ROLE.DB2DBA

CA Chorus for DB2 Database Management 機能へのアクセスを制御します。CA Chorus Infrastructure Management for Networks and Systems は、CA Insight からのデータを提供しますが、リソースはこのディシプリンに必要ではありません。

ROLE.INFRASTRUCTURE

CA Chorus Infrastructure Management for Networks and Systems 機能へのアクセスを制御します。

ROLE.SECURITY

CA Chorus for Security and Compliance Management 機能（UI およびバッチ）へのアクセスを制御します。

ROLE.SDK*instance*

SDK へのアクセスを制御します。 CA Chorus は複数の SDK をサポートできます。 この名前を定義し共有するには、システム管理者およびアプリケーション開発者と連携します。 SDK をサポートするのに必要なファイルを構築するには、アプリケーション開発者がこの名前を使用することをお勧めします。 詳細については、「*Software Development Kit User Guide*」を参照してください。

instance

SDK 用のこのリソースを識別する英数文字列。

ROLE.STORAGE

CA Chorus for Storage Management 機能へのアクセスを制御します。

SETTINGS.KNOWLEDGECENTER

ユーザが Knowledge Center 内のコンテンツにインデックスを付けることができることを示します。

SETTINGS.AUTOREFRESH

ユーザが自動リフレッシュ オプションを使用できることを示します。

uid-of-userid1, uid_of_userid2, ..., uid_of_useridn

アクセスをリクエストする CA Chorus ユーザの UID を識別します。

READ

ユーザが READ アクセスを持っていることを示します。

ユーザは指定されたリソースへのアクセス権があり、CA Chorus にログインし、作業できます。

例

以下のコマンドがユーザ ABC1 に以下の機能を付与します。

- CA Chorus にログインします。
- CA Chorus for DB2 Database Management の機能を使用します。
- Knowledge Center 内のドキュメントを変更します。
- 自動リフレッシュ オプションの使用。

```
SET RESOURCE(MFC)
RECKEY CHORUS ADD(ROLE.DB2DBA UID(************ABC1) SERVICE(READ)
ALLOW)
RECKEY CHORUS ADD(SETTINGS.KNOWLEDGECENTER UID(************ABC1)
SERVICE(READ) ALLOW)
RECKEY CHORUS ADD(SETTINGS.AUTOREFRESH UID(************ABC1)
SERVICE(READ) ALLOW)
```

サンプル: CA Top Secret でユーザを許可する

CA Chorus にログインできるユーザを識別するためにこの手順を使用します。 さらに、ユーザに以下のタスクの実行を許可することができます。

- Knowledge Center 内のコンテンツへのインデックス付け。 コンテンツにインデックスを付けることで、ユーザはこのリポジトリからドキュメントを追加または削除することができます。
- 自動リフレッシュ オプションの使用。このオプションは、バックエンド データが変更するたびに、CA Chorus UI に表示されるデータをリフレッシュします。

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。

ユーザ権限をセットアップする際には、以下の点について考慮します。

- 単一レベルが 8 バイトより長いエンティティ名は、アスタリスク マスクの使用に向いていません。 浮動小数点マスクをお勧めします。
- プレフィクス許可を使用する場合は、ディシプリン ログイン自体だけでなく複数のコールに影響を与える場合があるので注意してください。

ユーザ アクセス許可を定義するには、以下のコマンドを入力します。

```
TSS PERMIT(acid1) CAMFC(resource-name) ACCESS(READ)
TSS PERMIT(acid2) CAMFC(resource-name) ACCESS(READ)
...
TSS PERMIT(acidn) CAMFC(resource-name) ACCESS(READ)
```

resource-name

ユーザがアクセスを許可される CA Chorus リソースを示します。

CHORUS.ROLE.DB2DBA

CA Chorus for DB2 Database Management 機能へのアクセスを制御します。CA Chorus Infrastructure Management for Networks and Systems は、CA Insight からのデータを提供しますが、リソースはこのディシプリンに必要ではありません。

CHORUS.ROLE.INFRASTRUCTURE

CA Chorus Infrastructure Management for Networks and Systems 機能へのアクセスを制御します。

CHORUS.ROLE.SECURITY

CA Chorus for Security and Compliance Management 機能（UI およびバッチ）へのアクセスを制御します。

CHORUS.ROLE.STORAGE

CA Chorus for Storage Management 機能へのアクセスを制御します。

CHORUS.ROLE.SDK*instance*

SDK へのアクセスを制御します。 CA Chorus は複数の SDK をサポートできます。 この名前を定義し共有するには、システム管理者およびアプリケーション開発者と連携します。 SDK をサポートするのに必要なファイルを構築するには、アプリケーション開発者がこの名前を使用することをお勧めします。 詳細については、「*Software Development Kit User Guide*」を参照してください。

instance

SDK 用のこのリソースを識別する英数文字列。

重要: SDK インスタンスには一意の名前を使用してください。 SDK インスタンスの名前が類似していると権限の適用を誤る可能性があるので注意してください。 たとえば、CHORUS.ROLE.SDKROLE1 と CHORUS.ROLE.SDKROLE123 には同じ権限があります。同じマスク制限は、文字および数字に適用されます。

CHORUS.SETTINGS.KNOWLEDGECENTER

ユーザが Knowledge Center 内のコンテンツにインデックスを付けることができることを示します。

CHORUS.SETTINGS.AUTOREFRESH

ユーザが自動リフレッシュ オプションを使用できることを示します。

acid1, acid2, ..., acidn

アクセスをリクエストする CA Chorus ユーザの ACID を示します。ACID はユーザまたはプロファイルになります。

READ

ユーザが READ アクセスを持っていることを示します。

ユーザは指定されたリソースへのアクセス権があり、CA Chorus にログインし、そこで作業できます。

例

以下のコマンドがユーザ ABC1 に以下の機能を付与します。

- CA Chorus にログインします。
- CA Chorus for DB2 Database Management の機能を使用します。
- Knowledge Center 内のドキュメントを変更します。
- 自動リフレッシュ オプションの使用。

```
TSS PERMIT(ABC1) CAMFC(CHORUS.ROLE.DB2DBA) ACCESS(READ)
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.KNOWLEDGECENTER)
ACCESS(READ)
TSS PERMIT(ABC1) CAMFC(CHORUS.SETTINGS.AUTOREFRESH) ACCESS(READ)
```

サンプル: IBM RACF でユーザを許可する

CA Chorus にログインできるユーザを識別するためにこの手順を使用します。 さらに、ユーザに以下のタスクの実行を許可することができます。

- Knowledge Center 内のコンテンツへのインデックス付け。 コンテンツにインデックスを付けることで、ユーザはこのリポジトリからドキュメントを追加または削除することができます。
- 自動リフレッシュ オプションの使用。このオプションは、バックエンド データが変更するたびに、CA Chorus UI に表示されるデータをリフレッシュします。

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 RACF の製品マニュアルを参照してください。

次の手順に従ってください:

1. 各ディシプリン リソースを CAMFC に追加します。

   注: この手順は機能ベースのリソース（たとえば自動リフレッシュ）には必要ではありません。 この手順を実行する必要があるのは一度のみです。 リソースを CAMFC に定義済みの場合は、手順 2 に進みます。

   ```
   RDEFINE CAMFC CHORUS.ROLE.discipline UACC(NONE)
   ```

   discipline

   DB2DBA

   INFRASTRUCTURE

   SECURITY

   STORAGE

   注: 各ディシプリン リソースの詳細な説明については、手順 2 を参照してください。

   適用可能なディシプリン リソースは CAMFC に割り当てられます。 これで、ユーザにディシプリンへのアクセスを与えることができます。

2. 以下のコマンドを入力することで特定のリソースへのユーザ アクセスを許可します。

   ```
   PERMIT resource-name ID(uid-of-userid1) AC(READ) CLASS(CAMFC)
   PERMIT resource-name ID(uid-of-userid2) AC(READ) CLASS(CAMFC)
   ...
   PERMIT resource-name ID(uid-of-useridn) AC(READ) CLASS(CAMFC)
   ```

   resource-name

   ユーザがアクセスすることを許可される CA Chorus リソースを識別します。

   CHORUS.ROLE.DB2DBA

   CA Chorus for DB2 Database Management 機能へのアクセスを制御します。CA Chorus Infrastructure Management for Networks and Systems は、CA Insight からのデータを提供しますが、リソースはこのディシプリンに必要ではありません。

   CHORUS.ROLE.INFRASTRUCTURE

   CA Chorus Infrastructure Management for Networks and Systems 機能へのアクセスを制御します。

CHORUS.ROLE.SECURITY

CA Chorus for Security and Compliance Management 機能（UI およびバッチ）へのアクセスを制御します。

CHORUS.ROLE.STORAGE

CA Chorus for Storage Management 機能へのアクセスを制御します。

CHORUS.ROLE.SDK*instance*

SDK ロールへのアクセスを制御します。CA Chorus は複数の SDK をサポートできます。この名前を定義し共有するには、システム管理者およびアプリケーション開発者と連携します。SDK をサポートするのに必要なファイルを構築するには、アプリケーション開発者がこの名前を使用することをお勧めします。詳細については、「*Software Development Kit User Guide*」を参照してください。

instance

SDK 用のこのリソースを示す英数文字列。

CHORUS.SETTINGS.KNOWLEDGECENTER

ユーザが Knowledge Center 内のコンテンツにインデックスを付けることができることを示します。

CHORUS.SETTINGS.AUTOREFRESH

ユーザが自動リフレッシュ オプションを使用できることを示します。

uid-of-userid1, uid_of_userid2, ..., uid_of_useridn

アクセスをリクエストする CA Chorus ユーザの UID を示します。

READ

ユーザに READ アクセス権限があることを示します。

3. CAMFC リソースに行なわれる変更をアクティブにします。

```
SETROPTS RACLIST(CAMFC) REFRESH
```

変更がアクティブになります。

ユーザは指定されたリソースへのアクセス権があり、CA Chorus にログインし、そこで作業できます。

例

以下のコマンドがユーザ ABC1 に以下の機能を付与します。

- CA Chorus にログインします。
- CA Chorus for Security and Compliance Management の機能を使用します。
- Knowledge Center 内のドキュメントを変更します。
- 自動リフレッシュ オプションの使用。

```
PERMIT CHORUS.ROLE.SECURITY ID(ABC1) AC(READ) CLASS(CAMFC)
PERMIT CHORUS.SETTINGS.KNOWLEDGECENTER ID(ABC1) AC(READ)
CLASS(CAMFC)
PERMIT CHORUS.SETTINGS.AUTOREFRESH ID(ABC1) AC(READ) CLASS(CAMFC)
SETROPTS RACLIST(CAMFC) REFRESH
```

（オプション）CA Chorus 用の CA CSM Passticket の設定方法

CA Chorus は PassTicket セキュリティを使用して、ユーザが追加のユーザ ログインを必要とすることなく、クイック リンク モジュールから CA CSM を起動できるようにします。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。

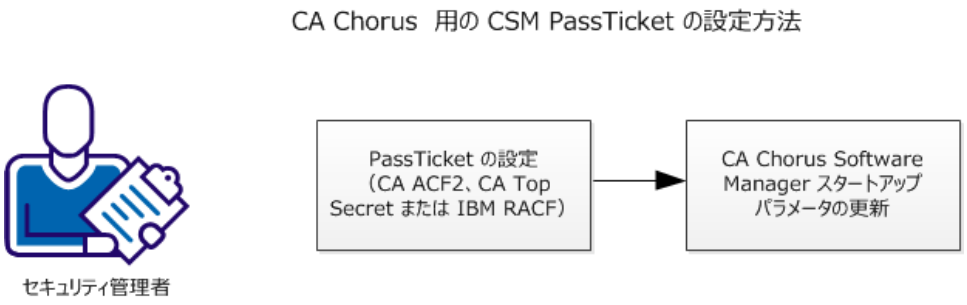
このシナリオは、ユーザが追加のユーザ ログインを必要とすることなく CA CSM を使用できるように、セキュリティ管理者およびシステム管理者が PassTicket を設定する方法について説明します。

重要: このシナリオ内の手順は、ユーザが ETJI095*x* セキュリティ ジョブを実行していると仮定しています。 まだの場合は、その手順を最初に完了してください。

PassTicket は、特定のアプリケーションへのアクセスに使用できる、一時的にエンコードおよび暗号化された、ユーザ パスワードの代用です。PassTicket は、生成後数分以内に使用される必要があります。PassTicket を使用することで、z/OS コンポーネントおよび製品が、ネットワーク経由で z/OS パスワードを送信せずにユーザ ID を認証できるようになります。 この代わりに、ユーザは有効な z/OS ユーザ ID およびパスワードでの最初のログイン後に認証されます。 ユーザが z/OS コンポーネントにアクセスする機能を選択すると、以下のプロセスが発生します。

- CA Chorus Web サービスは、アクセス許可用の PassTicket を生成するために z/OS セキュリティ製品を呼び出します。
- PassTicket はユーザ リクエストと一緒にコンポーネント宛てに送信されますが、そのコンポーネントは別の z/OS システム上にある可能性があります。
- そのコンポーネントは、リクエストを処理する前に、パスワードの代用として PassTicket を使用し、z/OS セキュリティ製品を呼び出して、ユーザを認証します。

注: 例は、CA ACF2、CA Top Secret および IBM RACF を使用して CA CSM への接続のための PassTicket を設定することを想定しています。 これらの例はガイドラインとして提供されます。CA ACF2 コマンドの使用に関する詳細情報については、「*CA ACF2 Administration Guide*」を参照してください。CA Top Secret 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*」 を参照してください。 IBM RACF の使用に関する詳細情報については、IBM のドキュメントを参照してください。



CA Chorus から CA CSM を起動し使用するには、以下のタスクを完了します。

1. PassTicket を使用できるようにセキュリティ システムを設定します。
   下記のオプションから *1* つ選択します。
   - CA ACF2 を使用した CA Chorus から CA CSM への接続用の PassTicket の設定 (P. 61)
   - CA Top Secret を使用した CA Chorus から CA CSM への接続用の PassTicket の設定 (P. 64)
   - IBM RACF を使用した CA Chorus から CA CSM への接続用の PassTicket の設定 (P. 65)
2. CA CSM スタートアップ パラメータを更新 (P. 68) します。

重要: CA Chorus で使用しているものと同じ CA CSM applid を使用していることを確認してください。

サンプル：CA ACF2 を使用した CA Chorus から CA CSM への接続用の PassTicket の設定

このサンプルでは、ETJI095*x* セキュリティ ジョブを実行した後に、セキュリティ管理者が CA Chorus から CA CSM へ接続するための PassTicket を設定する方法について説明します。

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 ACF2 for z/OS Administration Guide*」を参照してください。

この手順を行うには、CA Chorus サーバおよび CA CSM サーバでセキュリティをセットアップする必要があります。 以下の手順は、作業している場所と新しいサーバへユーザの焦点がシフトする時期が強調表示されます。 両方のサーバに適用される以下の定義に留意してください。

applid

CA Chorus クイック リンク モジュールの PassTicket 検証に使用されるアプリケーション ID を定義します。 *applid* を CA CSM applid に置換します。 CA CSM 設定の詳細については、「CA CSM スタートアップ パラメータの更新 (P. 68)」を参照してください。

デフォルト： CSMAPPLM

MULT-USE

同じ PassTicket を複数回を再利用できるようにします。

SSKEY

例で表示される値とは異なる、ランダムな 16 進数の 16 桁の形式でのアプリケーション用の暗号化鍵を定義します。

注：この例では、16 進数の 16 桁の完全なキー SESSKEY 値（8 バイトまたは 64 ビット キーを作成）を示しています。 各アプリケーション キーは設定内のすべてのシステム上で同一であり、その値は機密保護される必要があります。

CA Chorus サーバ側の手順

1. 個別のユーザに CA CSM へのアクセスを許可します。

   ```
   SET RESOURCE(SAF)
   RECKEY applid ADD(UID(chorus_userid) SERVICE(READ) ALLOW)
   F ACF2,REBUILD(SAF)
   ```

   chorus_userid

   クイック リンク モジュールによって CA CSM にアクセスする必要のあるユーザ。

   PassTicket は CA Chorus サーバ側で設定されます。

(オプション) CA CSM サーバ側の手順

注: 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。

重要: CA Chorus および CA CSM が同じマシン上にない場合は、手順 1 および 2 が必要です。 手順 3 はすべての状況で必要です。

1. CA CSM 接続アプリケーション セッション キーを定義します。

```
SET PROFILE(PTKTDATA) DIV(SSIGNON)
INSERT applid SSKEY(0123456789ABCDEF) MULT-USE
F ACF2,REBUILD(PTK),CLASS(P)
```

2. CA CSM ユーザの代わりに PassTicket を生成し評価するには、CA CSM スターティッド タスク ユーザ ID を許可します。

```
SET RESOURCE(PTK)
RECKEY IRRPTAUTH ADD(applid.- UID(uid-of-csm_stc_userid)
SERVICE(UPDATE,READ) ALLOW)
F ACF2,REBUILD(PTK)
```

uid_csm_stc_userid

CA CSM アプリケーション サーバ 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： MSMSERV

3. 個別のユーザに CA CSM へのアクセスを許可します。

```
SET RESOURCE(SAF)
RECKEY applid ADD(UID(uid-csm_userid) SERVICE(READ) ALLOW)
F ACF2,REBUILD(SAF)
```

PassTicket は CA CSM サーバ側で設定されます。

PassTicket セットアップを完了するには、「CA CSM スタートアップ パラメータの更新 (P. 68)」に移動します。

サンプル：CA Top Secret を使用した CA Chorus から CA CSM へ接続するための PassTicket の設定

このサンプルでは、ETJI095*x* セキュリティ ジョブを実行した後に、セキュリティ管理者が CA Chorus から CA CSM へ接続するための PassTicket を設定する方法について説明します。

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

この手順を行うには、CA Chorus サーバおよび CA CSM サーバでセキュリティをセットアップする必要があります。 以下の手順は、作業している場所と新しいサーバへユーザの焦点がシフトする時期が強調表示されます。 両方のサーバに適用される以下の定義に留意してください。

applid

CA Chorus クイック リンク モジュールの PassTicket 検証に使用されるアプリケーション ID を定義します。 *applid* を CA CSM applid に置換します。 CA CSM 設定の詳細については、「CA CSM スタートアップ パラメータの更新 (P. 68)」を参照してください。

デフォルト： CSMAPPLM

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許可を定義できます。

SESSKEY

例で表示される値とは異なる、ランダムな 16 進数の 16 桁の形式でのアプリケーション用の暗号化鍵を定義します。

注：この例では、16 進数の 16 桁の完全なキー SESSKEY 値（8 バイトまたは 64 ビット キーを作成）を示しています。 各アプリケーション キーは設定内のすべてのシステム上で同一であり、その値は機密保護される必要があります。

SIGNMULTI

同じ PassTicket を複数回再利用することを許可します。

CA Chorus サーバ側の手順

ETJI095*x* ジョブを実行したときに、このサーバ用の passticket を設定したことになります。

（オプション）CA CSM サーバ側の手順

重要: CA Chorus および CA CSM が同じマシン上にない場合は、この手順を完了します。

1. CA CSM 接続アプリケーション セッション キーを定義します。

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

2. CA CSM ユーザの代わりに PassTicket を生成し評価するには、CA CSM スターティッド タスク ユーザ ID を許可します。

   ```
   TSS PERMIT(csm_stc_userid) PTKTDATA(IRRPTAUTH.applid.) ACCESS(READ,UPDATE)
   ```

   csm_stc_userid

   CA CSM アプリケーション サーバ 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。

3. 適用可能な部門に applid を追加します。

   ```
   TSS ADDTO(department) APPLICATION(applid)
   ```

4. 個別のユーザに CA CSM へのアクセスを許可します。

   ```
   TSS PERMIT(csm_stc_userid) APPL(applid)
   ```

   PassTicket は CA CSM サーバ側で設定されます。

   PassTicket セットアップを完了するには、「CA CSM スタートアップ パラメータの更新 (P. 68)」に移動します。

サンプル: IBM RACF を使用した CA Chorus から CA CSM へ接続するための PassTicket の設定

このサンプルでは、ETJI095*x* セキュリティ ジョブを実行した後に、セキュリティ管理者が CA Chorus から CA CSM へ接続するための PassTicket を設定する方法について説明します。

注: この手順を開始する前に、PassTicket リソース（IRRPTAUTH）の PTKTDATA クラスおよび所有権が定義されていることを確認してください。

この手順を行うには、CA Chorus サーバおよび CA CSM サーバでセキュリティをセットアップする必要があります。 以下の手順は、作業している場所と新しいサーバへユーザの焦点がシフトする時期が強調表示されます。 両方のサーバに適用される以下の定義に留意してください。

applid

CA Chorus クイック リンク モジュールの PassTicket 検証に使用されるアプリケーション ID を定義します。 *applid* を CA CSM applid に置換します。 CA CSM 設定の詳細については、「CA CSM スタートアップ パラメータの更新 (P. 68)」を参照してください。

デフォルト： CSMAPPLM

KEYMASKED

サンプル構文の値と異なる値を使用して、アプリケーション用の暗号キーを定義します。

注: サンプル構文は、16 進数の 16 の完全なキー値（8 バイト キーまたは 64 ビット キーを作成）を示しています。 各アプリケーション キーは設定内のすべてのシステム上で同一であり、その値は機密保護される必要があります。

APPLDATA('NO REPLAY PROTECTION')

同じ PassTicket を複数回を利用できるようにします。

CA Chorus サーバ側の手順

ETJI095*x* ジョブを実行したときに、このサーバ用の passticket を設定したことになります。

(オプション) CA CSM サーバ側の手順

重要: CA Chorus および CA CSM が同じマシン上にない場合は、この手順を完了します。

1. CA CSM 接続アプリケーション セッション キーを定義します。

   ```
   SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
   RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(FEDCBA9876543210)) APPLDATA('NO
   REPLAY PROTECTION')
   ```

2. CA CSM ユーザの代わりに PassTicket を生成し評価するには、CA CSM スターティッド タスク ユーザ ID を許可します。

   ```
   SETROPTS GENERIC(PTKTDATA)
   RDEFINE PTKTDATA IRRPTAUTH.applid.* CLASS(PTKTDATA) UACC(NONE)
   PERMIT IRRPTAUTH.applid.* CLASS(PTKTDATA) ID(csm_stc_userid)
   ACCESS(READ,UPDATE)
   ```

   csm_stc_userid

   CA CSM アプリケーション サーバ 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: MSMSERV

3. 個別のユーザに CA CSM へのアクセスを許可します。

   ```
   RDEFINE APPL applid UACC(NONE)
   PERMIT applid CLASS(APPL) ID(csm_stc_userid) ACCESS(READ)
   SETROPTS CLASSACT(APPL)
   ```

4. PTKTDATA クラスをリフレッシュし、APPL クラスをアクティブにします。

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

   PassTicket は CA CSM サーバ側で設定されます。

   PassTicket セットアップを完了するには、「CA CSM スタートアップ パラメータの更新 (P. 68)」に移動します。

CA CSM スタートアップ パラメータの更新

この手順では、作成された CA CSM アプリケーション ID を使用してシステム管理者が CA CSM アプリケーション サーバを起動する方法について説明します。

次の手順に従ってください:

1. CA CSM アプリケーション ID を指定するために SAMPLIB (MSMLIB) メンバ内に以下のステートメントを追加します。

   `IJO="$IJO -DmsmApplid=`*`applid`*`"`

   applid

   PassTicket 検証に使用される CA CSM アプリケーション ID を定義して、サーバへの接続を認証します。

   デフォルト： CSMAPPLM

2. CA CSM アプリケーション サーバを再起動します。

   変更が有効になります。

これでユーザは、クイック リンク モジュールから CA CSM にアクセスできます。