CA Chorus™ Software Manager

管理ガイド

リリース 5.1

第 1 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 Chorus™ Software Manager（CA CSM）
- CA Chorus™
- CA ACF2™ for z/OS
- CA Datacom®/DB
- CA Datacom/MSM
- CA Distributed Security Integration for z/OS（CA DSI Server）
- CA Top Secret® for z/OS
- CA Common Services for z/OS
- CA Allocate™ DASD Space and Placement（CA Allocate）
- CA Database Management Solutions for DB2 for z/OS
- CA Disk Backup and Restore（CA Disk）
- CA Easytrieve® Simplified Design System（CA Easytrieve）
- CA Panvalet®（CA Panvalet）
- CA Auditor for z/OS
- CA SMF Director
- CA View®
- CA PDSMAN® PDS Library Management（PDSMAN）
- CA SYSVIEW

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

以下のドキュメントの更新は、本書の前回のリリース以降に実施されました。

- 「インストールの準備」-「アップグレード タスク」-「アップグレード シナリオ (P. 31)」: CA MSM V5.0 から最新のバージョンにアップグレードするシナリオの追加
- 「インストールの準備」-「アップグレード タスク」-「アップグレード プロセス」 -「インストール後の処理 (P. 35)」 : 展開のスナップショットのクリーンアップに関する情報を追加
- 「インストールの準備」-「アップグレード タスク」-「アップグレード プロセス」 -「長期メンテナンス (P. 37)」 : msmtmp ディレクトリに関する情報の更新
- 「インストールの準備」 -「Prerequisite Validator」 -「Prerequisite Validator の要件 (P. 38)」 : 最新バージョンの CA CSM サポートの更新
- 「インストールの準備」 -「ディスク スペース要件 (P. 44)」 : 階層型ファイル システム (HFS) または zSeries ファイル システム (zFS) 空間用の割り当てを更新
- 「インストールの準備」-「ソフトウェア要件 (P. 45)」: 最新バージョンの CA CSM のサポートを更新
- 「インストールの準備」 -「Web アクセス要件 (P. 51)」 : sdownloads.ca.com を追加
- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」 -「CA CSM 機能のユーザ セキュリティのセットアップ (P. 62)」: SAF リソース クラス名に関する情報を追加
- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」 -「CA ACF2 for z/OS でのユーザ セキュリティのセットアップ (P. 64)」: SAF リソース クラス名に関する情報を追加
- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」 -「CA Top Secret for z/OS でのユーザ セキュリティのセットアップ (P. 69)」 : SAF リソース クラス名に関する情報を追加

- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」-「CA ACF2 for z/OS でのユーザ セキュリティのセットアップ」-「CA Top Secret for z/OS での CAMSM リソース クラスの定義 (P. 69)」：SAF リソース クラス名に関する情報を追加
- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」-「IBM RACF でのユーザ セキュリティのセットアップ (P. 72)」 ： SAF リソース クラス名に関する情報を追加
- 「インストールの準備」-「セキュリティ セットアップ」-「CA CSM アプリケーション サーバでのセキュリティのセットアップ」-「IBM RACF でのユーザ セキュリティのセットアップ」-「IBM RACF での CAMSM リソース クラスの定義 (P. 73)」 ： SAF リソース クラス名に関する情報を追加
- 「インストールの準備」 -「CA CSM 関連セキュリティ ID - OMVS セグメントおよびホーム ディレクトリ (P. 81)」 ： ホーム ディレクトリに関する情報を更新
- 「インストールの準備」 -「USS パスの設定詳細」 -「USS パスの設定 (P. 82)」 ： msmtmp ディレクトリの情報の削除、必要なスペースを更新
- 「CA CSM のインストールとセットアップ」 -「インストールとセットアップ オプションの指定」 -「ISPF UI Tool を使用したオプションの自動指定 (P. 90)」: ISPF コマンド ラインに関するメモを追加
- 「CA CSM のインストールとセットアップ」-「CA CSM のインストールとセットアップ (P. 92)」 ： トピックの再構成および更新
- 「CA CSM のインストールとセットアップ」-「CA CSM のインストールとセットアップ」 -「インストール ジョブ (P. 104)」 ： 再構成およびセクションの更新
- 「CA CSM のインストールとセットアップ」-「CA CSM のインストールと設定」-「UID (0) を使用しない CA CSM ユーザ ID の設定 (P. 108)」：手順の指示を更新
- 「CA CSM のインストールとセットアップ」-「CA CSM のインストールと設定」 -「展開のパス命名基準のオーバーライド」 ： 「ユーザ ガイド」にトピックを移動

- 「CA CSM のインストールとセットアップ」 -「CA CSM の開始」 -「出力記述子の設定 (P. 119)」： CA CSM サーバ スタートアップ JCL の出力記述子の設定についてのセクションを追加
- 「CA CSM のインストールとセットアップ」 -「既存インストール用の FTP 接続の設定 (P. 122)」: 既存インストールに対する FTP 設定には変更がない旨の記述を更新、元のトピックを削除
- 「CA CSM のインストールとセットアップ」 -「CETN500 を使用した CA Common Services のアップグレード (P. 133)」： サポート対象外になったため、CA Common Services for z/OS r11.0 からのアップグレード シナリオを削除
- 「CA CSM のインストールとセットアップ」 -「CETN500 を使用した CA Common Services のアップグレード (P. 133)」： ソフトウェア要件へのリンクを追加
- 「Post-Installation タスク」 -「IPL での CA Datacom/MSM SVC のロードのための CAIRIM セットアップ (P. 141)」 ： CA MSM r3.0 からのアップグレードに関する情報を削除
- 「Post-Installation タスク」-「CA CSM のバックアップとリカバリ」-「CA CSM のバックアップ方法 (P. 156)」 ： ファイル システムに関する情報を更新
- 「データベース管理」 -「データベース割り当ての管理」 -「JCL 割り当て調整 (P. 165)」 ： 新規インストールのジョブ名と詳細でセクションを更新
- 「CA CSM の実装およびステータス」-「実装チェックリスト」-「ネットワーク管理者 (P. 235)」 ： sdownloads.ca.com を追加
- 「CA CSM の実装およびステータス」 -「実装チェックリスト」 -「USS 管理者 (P. 238)」 ： ファイル システム構造の更新
- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード」 -「CA Datacom/MSM (P. 243)」 ： SVCNO キーワード セクションから CA MSM r3.0 からのアップグレードに関する情報を削除
- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード」 -「マウント ポイント マネージャ (P. 245)」 ： TempSpaceCleanupInterval キーワードを追加
- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード (P. 240)」 ： 製品取得サービス (PAS) セクションを削除

- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード」 -「ソフトウェア インストール サービス（P. 248）」： sisServerUnpaxTempDir キーワードを削除し、sisGimunzipTempPrefix に関する情報を更新
- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード」 -「セキュリティ（P. 251）」： safResourceClass キーワードを追加
- 「CA CSM の実装およびステータス」-「オプション ファイル キーワード」 -「CA CSM インストーラの実行制御パラメータ（P. 256）」： InstallSVC キーワード セクションから CA MSM r3.0 からのアップグレードに関する情報の削除
- 「CA CSM の実装およびステータス」-「USS ファイル システム」-「USS パスの設定詳細（P. 262）」： ファイル システム構造に関する情報の更新
- 「CA CSM の実装およびステータス」-「USS ファイル システム」-「USS パスの設定詳細」 -「単一ファイル システム（P. 265）」： ファイル システム構造に関する情報の更新
- 「CA CSM の実装およびステータス」-「USS ファイル システム」-「一時ファイル システムの使用（P. 267）」： CA CSM が一時ファイル システムを処理する方法について説明するトピックの追加
- 「CA CSM の実装およびステータス」 -「CA CSM データ セットとファイルシステム」-「CA CSM データ セット タイプ（P. 269）」: データ セット タイプの更新
- 「CA CSM の実装およびステータス」 -「CA CSM データ セットとファイルシステム」-「CA CSM ファイル システム（P. 270）」： システム パス詳細の更新
- 「CA CSM の実装およびステータス」 -「CA CSM 機能のセキュリティ」 -「リソース プロファイル（P. 279）」： ［Products」ツリー内の［Hide］メニュー アイテムへのアクセスを制御する、新規リソース ファイル SC.@HIDE を追加
- 「CA CSM の実装およびステータス」 -「CA CSM 機能のセキュリティ」 -「リソース プロファイル（P. 279）」: ［Task］タブ内の［Manage History］機能へのアクセスを制御し、許可されたユーザによるポリシーの作成、実行、削除の実行が可能になる、新しいリソース プロファイル TM.TASK.ARCHIVE を追加

- 「CA CSM の実装およびステータス」 - 「DBINIT および DBUPDATE の設定 (P. 287)」 : sisServerUnpaxTempDir および pasTemporaryDownloadDirectory の削除、GIMUNZIP 一時プレフィクスに関する情報の更新
- 「CA CSM の実装およびステータス」-「ジョブ割り当て詳細 (P. 299)」: インストール ジョブの新しい名前および最新の割り当て詳細を反映するため、セクションの更新
- 「トラブルシューティング」-「CA CSM アプリケーション サーバのタイムアウト (P. 312)」 : 新しいセクションの追加
- 「トラブルシューティング」 - 「z/OS V1.11 RSU 1106 環境の Software Configuration Service アドレス空間で ABEND が発生する」: 情報が古いため、セクションを削除

目次

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

概要

CA Chorus™ Software Manager（CA CSM）は、z/OS システム上の CA Technologies メインフレーム製品の管理を簡素化して統一するアプリケーションです。 製品が CA CSM サービスを採用することにより、業界のベスト プラクティスに沿った一般的な方法で、製品の取得、インストール、メンテナンス、展開、設定を実行できます。

CA CSM サービスを使用すると、製品の取得、インストール、展開、設定が簡素化されます。 またこれらのサービスにより、修正および推奨されるメンテナンスの取得と適用が、より簡単になります。 Web ベース インターフェースにより、より速く、より少ない失敗で製品のインストールとメンテナンスが可能になります。

注: CA CSM は、z/OS 用の CA Technologies メインフレーム製品のライセンス保持者で、メンテナンスを実行しているユーザに無償で提供されます。 CA CSM は、CA Technologies 製品を申請するのと同じライセンス条件の下で提供されます。 以降、関連する CA Technologies メインフレーム製品用のメンテナンス契約の期間、CA CSM メンテナンスも無償で提供されます。

本書の構成

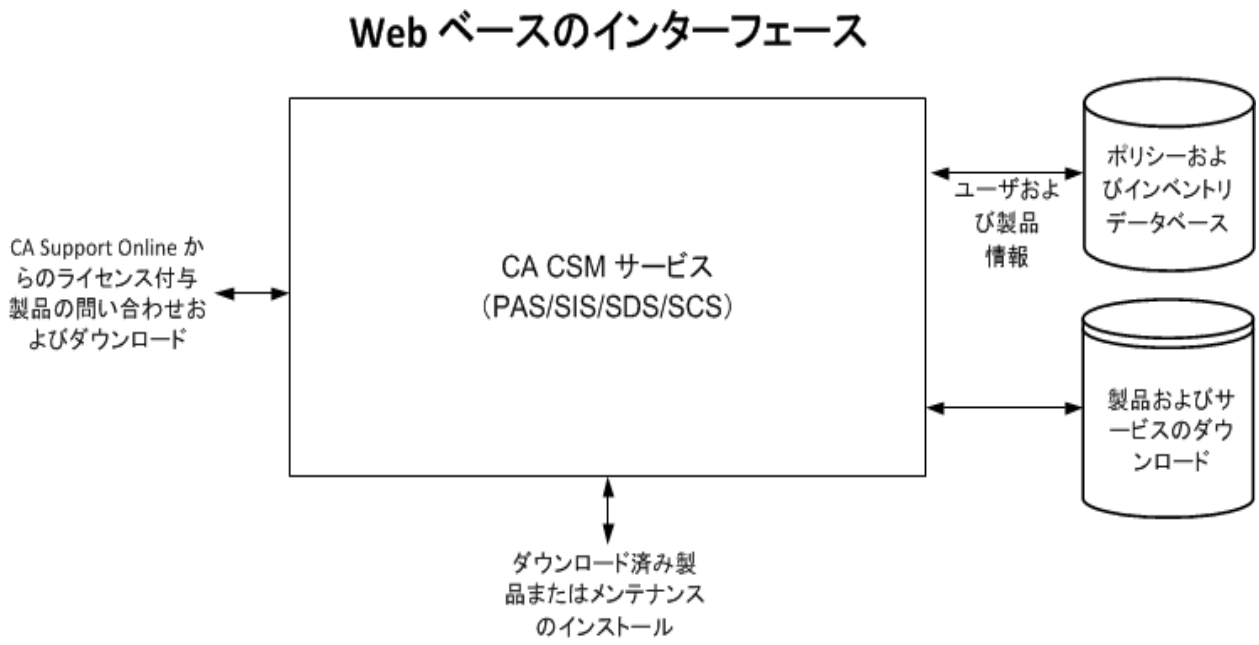
本書は、CA CSM の理解、そのインストールと設定、およびその管理についての情報を、以下のように説明します。

一般的な主題のエリア	章:
CA CSM の理解	第 1 章
CA CSM のインストールとセットアップ	第 2 ～ 4 章
CA CSM の管理	第 5 ～ 7 章、付録 A

CA CSM の動作の仕組み

CA CSM は、z/OS システム上でホストされたアプリケーション サーバ環境のアドレス空間で実行されるプログラムです。 通常、このシステムは SMP/E を使用して製品をインストールし、メンテナンスするための場所です。 このシステムは SMP/E 実行システムとして知られています。 CA CSM Web ベース インターフェースにより、コーディングや手動でバッチ ジョブのサブミットを行うことなく、SMP/E 処理の実行を動的に行うことができます。

以下の図は、主要なコンポーネントとデータ フローについて示しています。



CA CSM には以下の主要なコンポーネントがあります。

CA CSM サービス

以下のサービスを提供します。

製品取得サービス(PAS)

CA Technologies メインフレーム製品、プログラム一時修正(PTF)などのメインフレーム製品用サービスを簡単に取得できるようになります。 このサービスは、サイトにライセンスが付与されている製品に関する情報を取得し、ソフトウェア インベントリにそれらのライセンスを記録します。 インベントリは実行中のシステムでメンテナンスされます。サービスはまた、それらの製品用の LMP キー(ライセンス)もダウンロードできます。Web ベース インターフェースにより、利用可能なソフトウェアおよび修正のソフトウェア インベントリを参照し、それらを実行中のシステム内で利用できるようになります。

ソフトウェア インストール サービス（SIS）

実行中のシステムのソフトウェア インベントリ内の CA Technologies メインフレーム製品のインストールおよびメンテナンスを簡単にできるようになります。Web ベース インターフェースにより、ソフトウェア インベントリの参照と管理、またインストール タスクを自動化することが可能になります。 ダウンロードしたソフトウェア パッケージを参照し、実行中のシステムの SMP/E 環境の参照と管理を行うことができます。

Software Deployment Service（SDS）

実行中システムのソフトウェア インベントリから、CA Technologies メインフレーム製品の展開を円滑に行えるようにします。 このサービスにより、適切な転送メカニズムを備えたポリシー主導のインストール済み製品を、既知のトポロジ全体に展開できます。企業システム トポロジには、共有 DASD 環境、ネットワーク環境、および z/OS システムを含めることができます。 ポリシーは、メタデータ入力とユーザ指定の入力の組み合わせを表します。 メタデータ入力は、製品のコンポーネント部分を識別します。 ユーザ指定の入力は、展開する場所および名前などの展開基準を表します。

ソフトウェア構成サービス（SCS）

実行中システムのソフトウェア インベントリから、ターゲットの z/OS メインフレーム オペレーティング システムに対して、メインフレーム製品の設定を簡単に行えるようにします。SCS は、設定の作成プロセスと、設定を実行するための手動の手順をユーザに示します。 さらに、SCS には各ターゲットの z/OS システム上で動作するアドレス空間通信サービスも含まれています。

データベース

CA CSM が使用する情報を格納します。

ポリシー

CA Technologies メインフレーム製品をダウンロードして処理するための、サイトおよびユーザの情報を格納します。

インベントリ

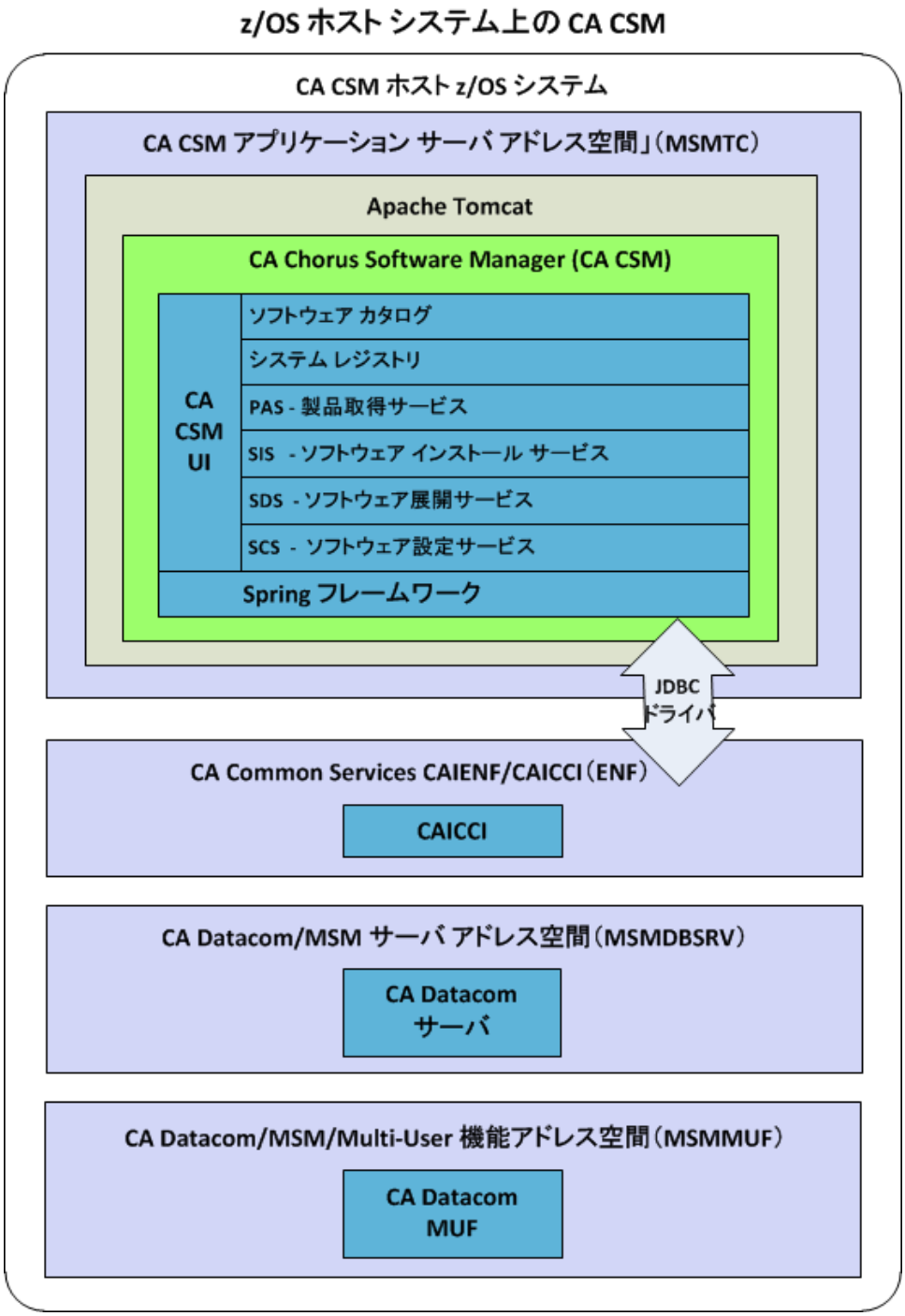
ユーザにライセンスが付与された CA Technologies メインフレーム製品に関する情報を格納します。

Web ベース インターフェース

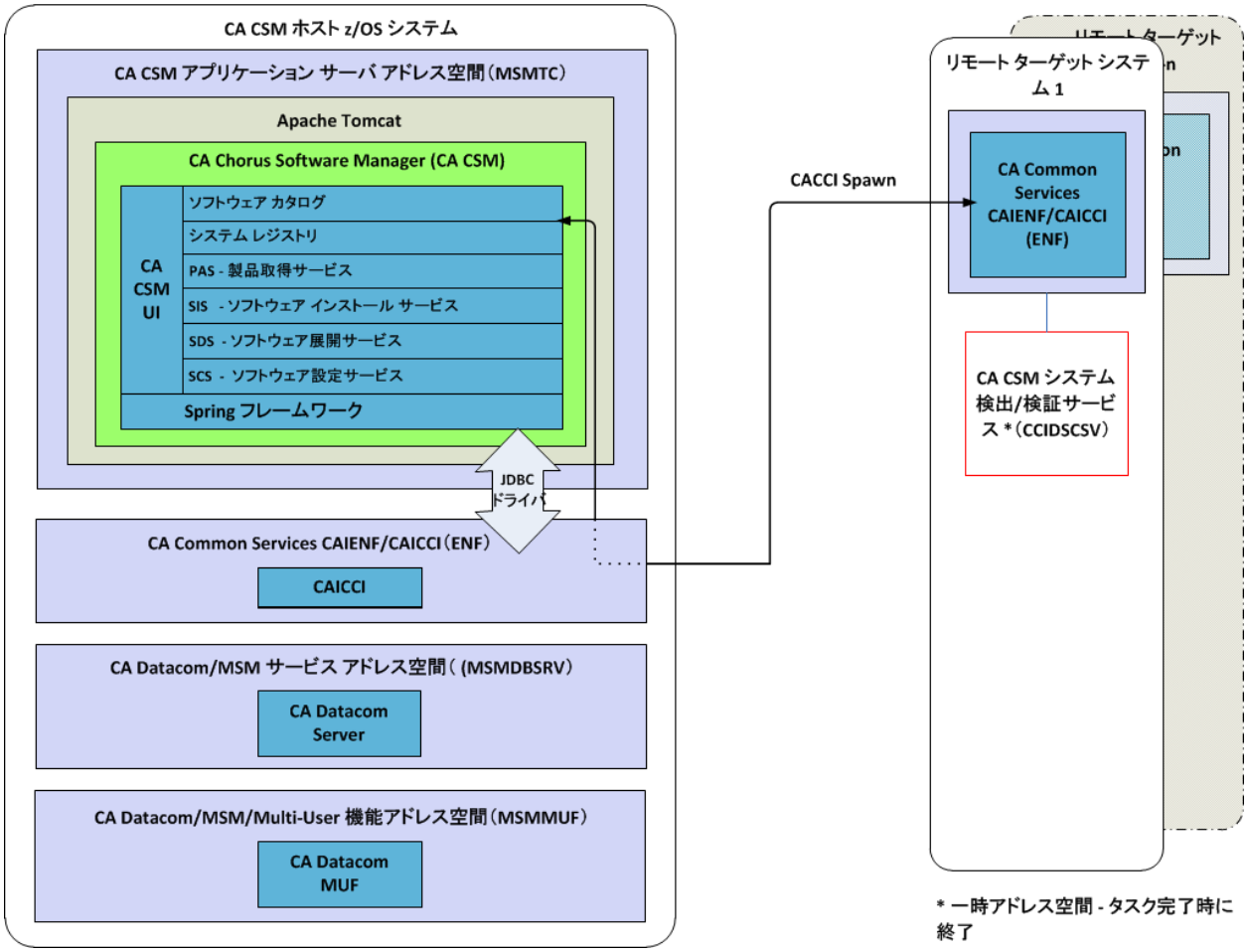
CA CSM カタログから取得した、CA Technologies メインフレーム製品の取得、インストール、メンテナンス、展開、設定、および SMP/E 環境の管理ができるようになります。 Web ベース インターフェースにはオンライン ヘルプが用意されており、CA CSM の使用方法に関する情報が提供されます。

CA CSM 運用アーキテクチャ図

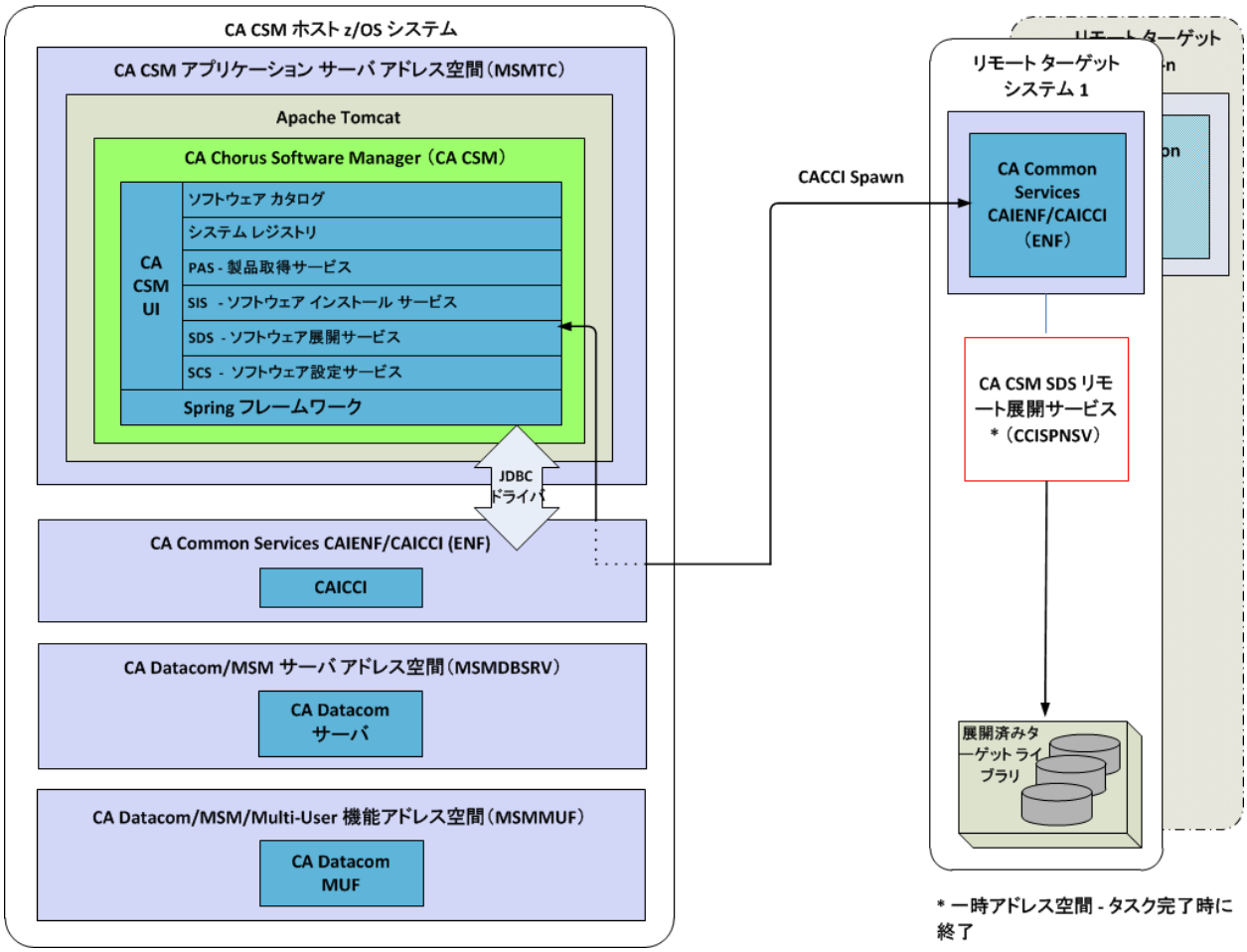
以下の図は、リモートおよびローカル システム上の CA Common Services for z/OS を使用した CA CSM の設定を示します。

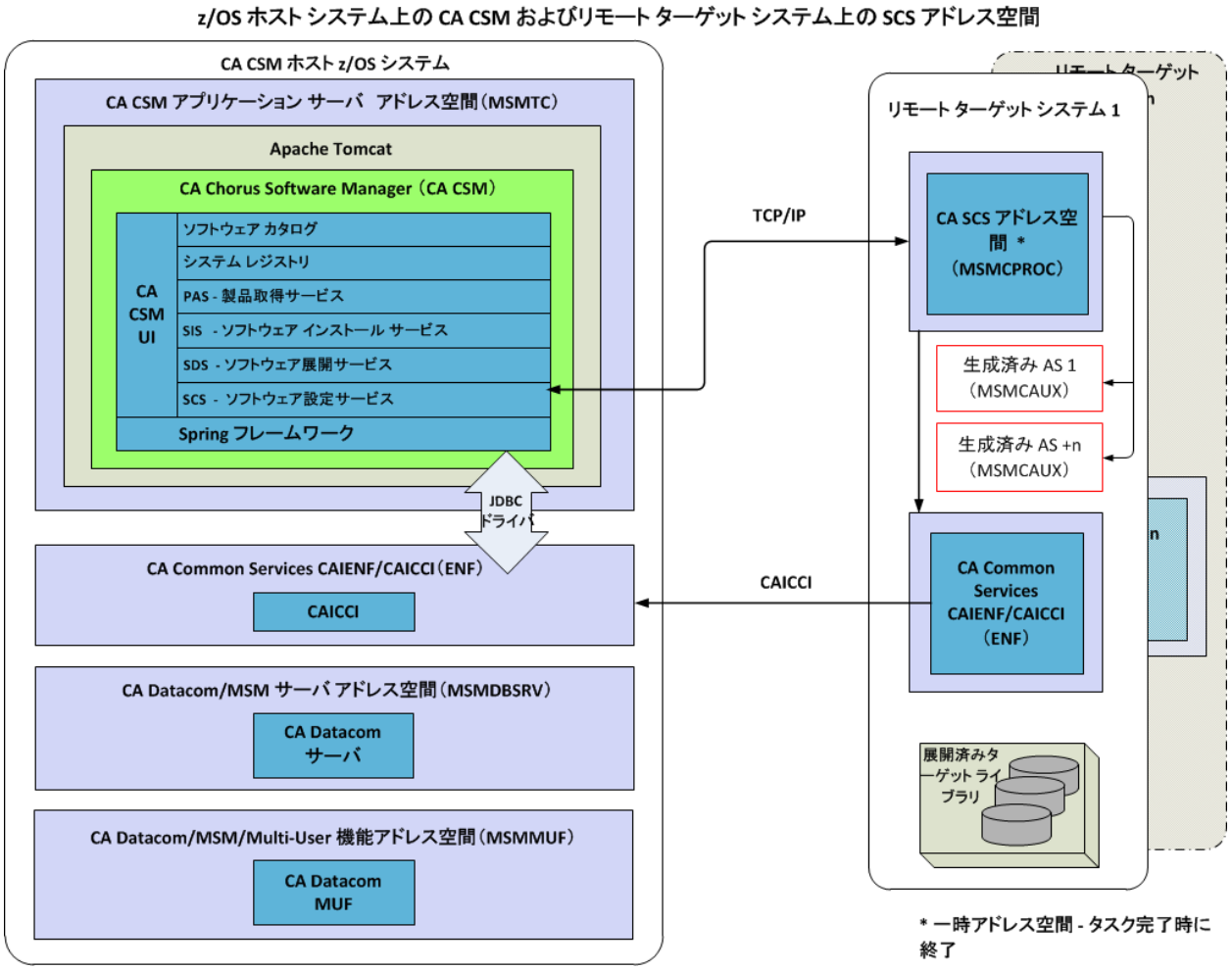


z/OS ホスト システム上の CA CSM およびリモート ターゲット システム上のシステム検出/検証サービス

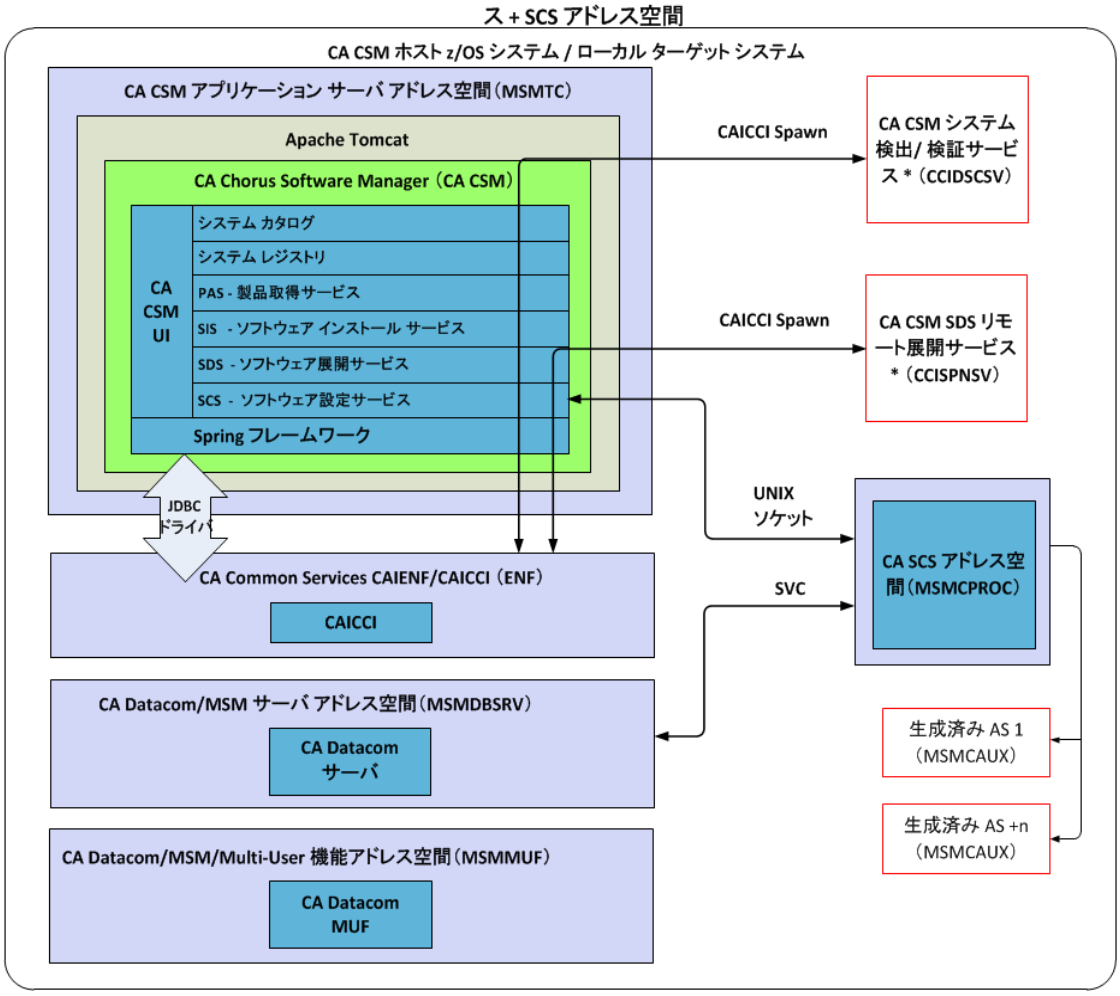


z/OS ホスト システム上の CA CSM およびリモート ターゲット システム上の SDS リモート展開サービス




z/OS ホスト システム上の CA CSM およびリモート ターゲット システム上の SCS アドレス空間
CA CSM ホスト z/OS システム
CA CSM アプリケーション サーバ アドレス空間(MSMTC)
Apache Tomcat
CA Chorus Software Manager (CA CSM)
CA CSM UI
ソフトウェア カタログ
システム レジストリ
PAS - 製品取得サービス
SIS - ソフトウェア インストール サービス
SDS - ソフトウェア展開サービス
SCS - ソフトウェア設定サービス
Spring フレームワーク
JDBC ドライバ
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
CA Datacom/MSM サーバ アドレス空間(MSMDBSRV)
CA Datacom サーバ
CA Datacom/MSM/Multi-User 機能アドレス空間(MSMMUF)
CA Datacom MUF
TCP/IP
リモート ターゲット システム 1
CA SCS アドレス空間 * (MSMCPROC)
生成済み AS 1 (MSMCAUX)
生成済み AS +n (MSMCAUX)
CA Common Services CAIENF/CAICCI (ENF)
展開済みターゲット ライブラリ
* 一時アドレス空間 - タスク完了時に終了

z/OS ホスト システム上の CA CSM およびローカル ターゲット システム上のシステム レジストリ検証サービス + SDS リモート展開サービス + SCS アドレス空間



ネットワーク フロー

CA CSM は以下のプロセスを使用し、ユーザを適切な CA Technologies Web サイトに直接接続し、ユーザはそこで CA Technologies ソフトウェアを管理できます。

1. HTTP プロトコル（http://*yourmainframe*: *yourport*/CSM など）を使用して、社内イントラネット（ローカルで接続された、または VPN でトンネルされた）から CA CSM に接続します。
   - システム プログラマがすべてのアクションを開始します。
   - ポートはインターネットに公開されません。
   - 通信はイントラネットの外からは開始されません。

2. CA CSM 製品取得サービス（PAS）は、以前に手動で Web サイトにアクセスするときに使用した以下のような方法と同じ方法を使用して、CA Technologies と通信します。

   HTTPS

   認証情報を渡し、適切な CA Technologies Web サイトから製品情報を取得します。

   FTP

   匿名 FTP を使用し、認証情報なしで CA FTP Services からお使いのメインフレーム システムにソフトウェア パッケージをダウンロードします。 CA CSM は以下のいずれかの場所にアクセスします。

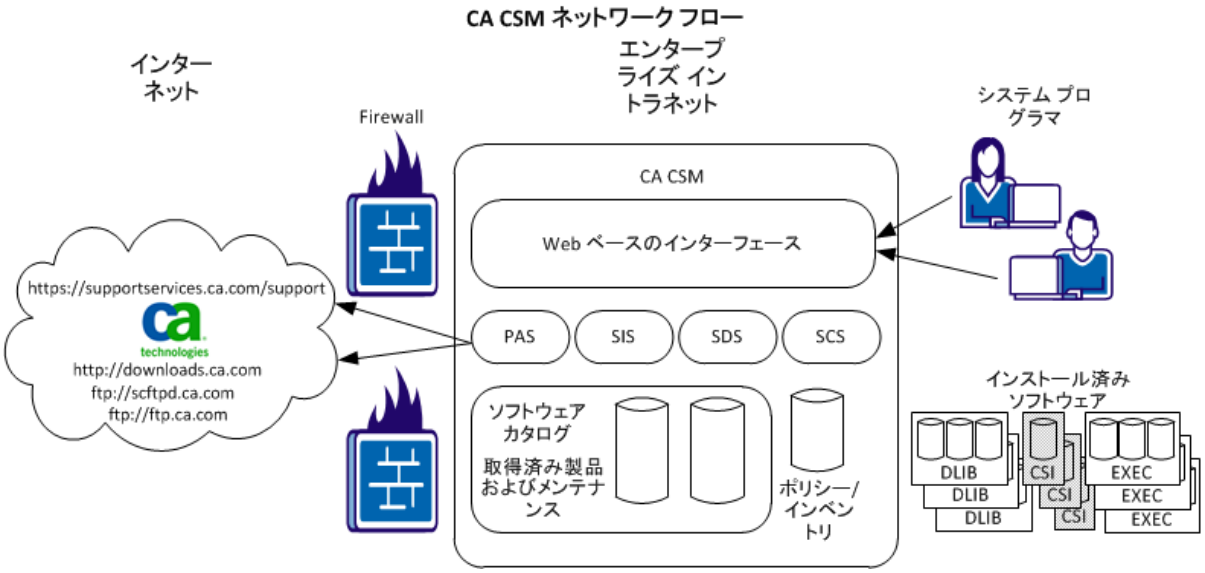
   - ftp://scftpd.ca.com
   - ftp://ftp.ca.com

注: 以下の情報は、CA Technologies でやりとりする唯一の暗号化されていないデータです。

- 匿名 FTP 用の電子メール アドレス（パスワードなし）
- CA Technologies 製品情報。基本インストール パッケージまたはソリューションのいずれか。

これらのデータは、プライバシー標準または暗号化標準の一部ではありません。

以下の図で、このプロセスを説明します。



Web ベース インターフェース

Web ブラウザから CA CSM にアクセスし、使用します。 Web ベース インターフェースにはオンライン ヘルプが用意されており、製品の取得、インストール、メンテナンス、展開、設定に関する情報が提供されています。

最初にログインすると、初期ページが表示され、以下の機能がタブ表示されます。

ソフトウェア ステータス

ユーザにメンテナンスとタスクの問題を警告します。

製品

製品パッケージのダウンロードやインストール、メンテナンスの APPLY など、CA Technologies 製品の管理ができます。

SMP/E 環境

SMP/E 環境の管理や製品のインストールができます。

展開

展開の作成、既存の展開の管理、設定の作成ができます。

構成

既存の構成を管理および実装できます。

システム レジストリ

システム レジストリの作成や、データ送信先のメンテナンスができます。

タスク

ユーザのアクティビティ（たとえばインストール タスク）をサポートする CA CSM タスクの管理ができます。

設定

CA CSM 用の設定（たとえばソフトウェアの取得）を定義します。

第 2 章: インストールの準備

このセクションには、以下のトピックが含まれています。

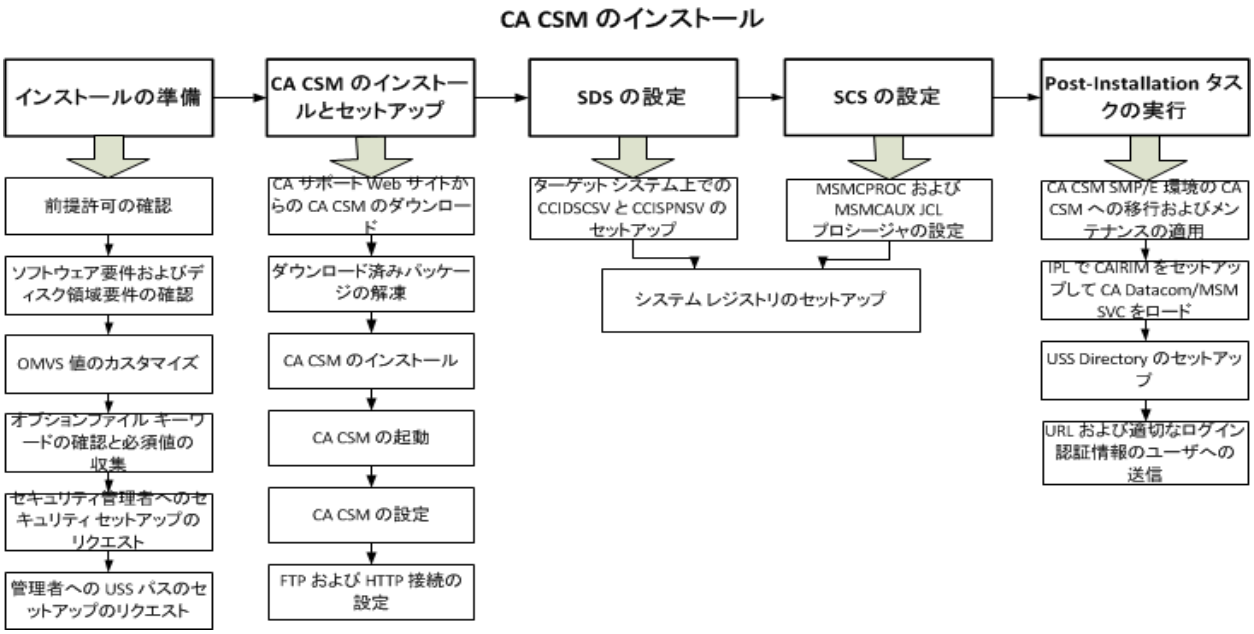
必要なスキル

本書で説明されるタスクの実行とは、以下のスキルが必要な作業の組み合わせです。

- z/OS UNIX System Services（USS）およびファイル システム。機能別の UNIX およびファイル システム環境をセットアップするため
- セキュリティ サーバ（たとえば CA ACF2 for z/OS、CA Top Secret for z/OS、IBM RACF）、またはお使いのセキュリティ製品。リソースにアクセス権を付与するため
- z/OS 用の Java
- CA Common Services for z/OS
- ネットワーク管理。製品パッケージを取得してダウンロードするためのアクセス権をセットアップするため

セットアップおよびインストール プロセスの仕組み

後の章で説明される CA CSM のセットアップおよびインストール プロセスは、以下の手順から構成されます。



1. 以下のタスクを実行し、インストールの準備をします。

   注: CA CSM の旧バージョンからアップグレードしている既存の CA CSM ユーザである場合は、このリストにあるタスクを実行する前に、アップグレード タスク (P. 30)を確認してください。

   a. すべての必要な前提許可 (P. 38)を満たしていることを確認します。

   b. CA CSM のソフトウェア要件 (P. 45)およびディスク スペース要件 (P. 44)を確認します。

   c. 必要に応じ、z/OS OMVS 値を設定します (P. 49)。

   d. オプション ファイル キーワード (P. 240)を確認し、必要な値を収集します。

   e. セキュリティ管理者に依頼し、必要なセキュリティをセットアップ (P. 53)します。

   f. USS 管理者に依頼し、USS パスをセットアップ (P. 82)します。

2. 以下のタスクを実行し、CA CSM のインストールおよびセットアップを行います。

   a. CA サポート Online Web サイトの Download Center から、お使いのシステムに CA CSM ソフトウェア パッケージをダウンロード (P. 87)します。

   b. ダウンロードしたパッケージを解凍します (P. 87)。

   c. ソフトウェアのインストール

      - インストールおよびセットアップ オプション ファイルをカスタマイズします (P. 89)。
      - セットアップ ユーティリティを実行します (P. 92)。ユーティリティは、CA CSM にアクセスするための URL（Uniform Resource Locator）もセットアップします。

   d. CA CSM を起動します (P. 114)。

   e. CA CSM を設定します (P. 120)。

   f. FTP と HTTP の接続を設定します (P. 122)。

3. Software Deployment Service（SDS）の設定

   a. 各ターゲット システムで CCIDSCSV と CCISPNSV をセットアップします (P. 143)。

   b. システム レジストリをセットアップします。

   注: システム レジストリをセットアップする方法の詳細については、「*ユーザ ガイド*」の「システム レジストリのセットアップ」の章を参照してください。

4. Software Configuration Service（SCS）の設定

   a. MSMCPROC (P. 184) および MSMCAUX (P. 185) JCL プロシージャを設定します。

   b. システム レジストリがセットアップされたことを確認します。

   注: システム レジストリをセットアップする方法の詳細については、「*ユーザ ガイド*」の「システム レジストリのセットアップ」の章を参照してください。

5. 以下のインストール後のタスクを実行します。
   a. CA CSM SMP/E 環境を CA CSM に移行し (P. 146)、利用可能なときにメンテナンスを適用 (P. 149)します。
   b. CAIRIM をセットアップして IPL 時に CA Datacom/MSM SVC をロードします (P. 141)。
   c. USS ディレクトリをクリーン アップします (P. 159)。
   d. URL および適切なログイン認証情報をユーザに伝えます。

詳細:

実装チェックリスト (P. 235)

アップグレード タスク

このセクションは、CA CSM の旧バージョンからアップグレードを行っている既存の CA CSM ユーザのみを対象としています。

重要: このセクションのトピックでは、必要な手順の概要のみが説明されています。 CA CSM を正常にアップグレードするためには、このトピックで言及されている詳細な手順をすべて完了してください。

最新のバージョンには CA Datacom/MSM および Apache Tomcat をはじめとする、組み込み済みの CA CSM コンポーネントの更新バージョンが含まれます。 アップグレード プロセスは新しい環境をセットアップし、データベースをアップグレードします。

セットアップ ユーティリティ

CA CSM の旧バージョンから取得する SMP/E のターゲット パスを使用して、MSMSetup.sh ユーティリティを使用したアップグレード プロセスを呼び出すことができます。

注: z/OS Telnet セッションまたは ISHELL コマンド シェルから、MSMSetup.sh ユーティリティを呼び出すことはできません。

MSMSetup.sh ユーティリティは以下のアクションを実行します。

- ユーティリティは新しい CA CSM SMP/E およびランタイム環境をセットアップします。
- ユーティリティは、データベースを旧バージョンの CA CSM から最新のバージョンに移行します。
- CA CSM メンテナンス展開ジョブをセットアップします。

重要: アップグレード プロセスは、CA CSM の旧バージョンにはまったく影響を与えません。 新しい CA CSM 環境は、アップグレードされたデータベースを使用してセットアップされます。 CA CSM を使用して管理される製品用の旧バージョンの CA CSM のマウント ポイントは、アップグレードの後も引き続き使用されます。

データベースの割り当て

CA CSM を最新のバージョンにアップグレードすると、CA CSM データベース（DBID 4000）のデータ セットにはディスク領域の概算容量が割り当てられます。 このディスク領域は、ほとんどの組織の作業量に対応できます。ですが、操作中にデータベースのディスク割り振りを増加させ (P. 162)、現行のボリューム増加に合わせることができます。

アップグレード シナリオ

CA CSM の最新バージョンには以下の変更が含まれます。

- CA Datacom/MSM と Apache Tomcat をはじめとする、組み込み済みの CA CSM コンポーネントの更新バージョン
- USS フォルダ構造および CA CSM コンポーネント名の変更
- 一部の CA CSM コンポーネントの削除および新しい CA CSM コンポーネントの追加

注: CA MSM の旧バージョンから r3.1 へのアップグレードはサポートされていません。 現在のバージョンをアンインストールし、最新バージョンを新規インストールとしてインストールする必要があります。

以下のアップグレード シナリオが考えられます。

CA CSM r3.1 の最新バージョンへのアップグレード

このシナリオでは、以下のアクションが実行されます。

- 4 つの z/OS データ セットが追加され、新しい CA Datacom/MSM データベース領域がサポートされます。
- 8 つの旧バージョンの CA Datacom/MSM データベース テーブルがコピー、再構成され、データがあれば変換されます。
- 50 の CA Datacom/MSM テーブルがそれぞれのデータベース領域に追加されます。
- 4 つのシステム レジストリ データベース テーブルに初期データが読み込まれます。
- 以下のデータベース テーブルに、追加データが追加されます。
  - IDC（IDCONTROL）
  - LIS（LISTTASKTYPE）

CA MSM V4.0 の最新バージョンへのアップグレード

このシナリオでは、以下のアクションが実行されます。

- 6 つの旧バージョンの CA Datacom/MSM データベース テーブルがコピー、再構成され、データがあれば変換されます。
- 6 つの既存の CA Datacom/MSM テーブルが削除されます。
- 12 の新しい CA Datacom/MSM テーブルがそれぞれのデータベース領域に追加されます。
- 以下のデータベース テーブルに、追加データが追加されます。
  - IDC（IDCONTROL）
  - LIS（LISTTASKTYPE）
- システム レジストリ テーブルが変更されたデータで置換されます。

CA MSM R4.1 の最新バージョンへのアップグレード

このシナリオでは、以下のアクションが実行されます。

- 11 の z/OS データ セットが追加され、新しい CA Datacom/MSM データベース領域がサポートされます。
- 4 つの旧バージョンの CA Datacom/MSM データベース テーブルがコピー、再構成され、データがあれば変換されます。

- 6 つの既存の CA Datacom/MSM テーブルが削除されます。
- 6 つの新しい CA Datacom/MSM テーブルがそれぞれのデータベース領域に追加されます。
- 以下のデータベース テーブルに、追加データが追加されます。
  - IDC（IDCONTROL）
  - LIS（LISTTASKTYPE）
- システム レジストリ テーブルが変更されたデータで置換されます。

CA MSM V5.0 の最新バージョンへのアップグレード

このシナリオでは、以下のアクションが実行されます。

- 6 つの既存の CA Datacom/MSM テーブルが削除されます。
- 6 つの新しい CA Datacom/MSM テーブルが追加されます。

アップグレード プロセス

アップグレード プロセスは、いかなる旧 CA Datacom/MSM データも更新または削除しません。 アップグレード プロセスは、現行の CA Datacom/MSM 環境のバックアップのみ行います。 この処理には、新しい（最新）バージョンの CA CSM 環境の作成と、バックアップされ変換された既存のデータ（CA CSM の旧バージョン）をその環境に読み込むことが含まれます。

アップグレードとして CA CSM をインストールする処理は、新規インストールでインストールする処理とほぼ同じです。 処理は以下の手順に分割できます。

- 計画と準備
- インストール
- インストール後の処理
- フォールバック
- 長期メンテナンス

計画と準備

CA CSM の必須要件を確認し、以下の手順を実行します。

1. Prerequisite Validator ユーティリティ (P. 38) を実行し、すべてのソフトウェア要件および必要な権限が設定されているかどうかを確認します。
2. CA Common Services for z/OS ソフトウェア要件を確認しセットアップします。
3. 以下のパラメータを要求し、セットアップします。
   - ディスクスペース要件 (P. 44)
   - Web アクセス要件 (P. 51)
   - TCP/IP ポートの予約 (P. 52)
   - SCS アドレス空間セキュリティ (P. 188)をはじめとするセキュリティ (P. 53)
   - USS パス (P. 82)
   - SDS アクセス用の権限および許可 (P. 79)

   注: CA CSM のアップグレードには、新しいディスク スペース要件 (P. 44)があります。

MSMSetup.sh ユーティリティは、オプション ファイルで指定された値に従って、CA CSM がアップグレードであるか、または新規インストールであるかを識別します。 アップグレードを実施している既存の顧客用に、追加の指示と手順が用意されています。

MSMSetup.sh ユーティリティにはコピー機能があります。この機能を使用し、旧バージョン用のオプション ファイルから最新のバージョンに対し、オプション ファイル キーワードの値をコピー (P. 101)することができます。

注: オプション ファイルのコピー機能およびアップグレードのインストール 処理はどちらも、旧バージョンの SMP/E ターゲット USS パス名を指定する必要があります。 各キーワードのアップグレードの詳細については、オプション ファイル キーワード (P. 240)を確認してください。

重要: アップグレード プロセスにより、新規の SMP/E およびランタイム環境が作成されます。 SMP/E のインストール (P. 240)およびランタイム (P. 242)のパラメータの旧バージョンの値を変更し、旧バージョンのファイルやフォルダに上書きしないようにする必要があります。

インストール

キーワードが正しく設定されていない場合、MSMSetup.sh プロセスは利用可能なインストール オプションから正しい値を選択するように求めるプロンプトを表示します。

スクリプトは、SMP/E のインストール (P. 240)、ランタイム (P. 242)およびデータベース (P. 242)のパラメータに対する旧バージョンの値が異なるかどうかを検証します。 アップグレードに関連するジョブおよび手順は、インストール モードに基づいて実行されます。

アップグレード プロセスは、まず旧バージョン用のデータベースをバックアップし、次に新バージョンのデータベースにその内容を移行します (P. 103)。

MSMSetup.sh は旧バージョンの詳細を検出し、アップグレード手順および旧バージョン固有の生成済みジョブを処理します。

MSMSetup.sh ユーティリティが正常に完了したら、生成されたサマリ レポートを読み、インストール後の手順を完了します。

インストール後の処理

サマリ レポートを確認し、インストール後の手順で表示される手順を完了し、次に最新の CA CSM アドレス空間を起動します。

CA CSM アップグレード インストール中に作成した CA CSM SMP/E 環境を (P. 146) CA CSM に移行し、CA CSM をメンテナンスします。 あるいは、最新のバージョンから CA CSM SMP/E 環境の旧バージョンを削除することもできます。 Web ベース インターフェースの［SMP/E Environments］タブをクリックし、次に［Remove SMP/E Environment from CA CSM］をクリックします。

その後、古い展開のスナップショットをクリーン アップし、システムの DASD 空間を解放します。

注: CA CSM SMP/E 環境の旧バージョンの削除の詳細について、または SMP/E 環境の削除については、「*ユーザ ガイド*」の「SMP/E 環境の管理」の章を参照してください。 展開のスナップショットのクリーン アップの詳細については、「*ユーザ ガイド*」の「製品の展開」の章を参照してください。

アップグレードが完了し、一貫して最新のバージョンを使用しているならば、以降あらゆる旧バージョンの CA CSM を使用しないことをお勧めします。

詳細:

長期メンテナンス (P. 37)

フォールバック

CA CSM の最新バージョンが正しく開始しない場合、CA CSM の旧バージョンを引き続き使用することもできます。

最新のバージョンを正常に実行できる場合、旧バージョンをこれ以降使用しないことをお勧めします。 最新の CA CSM アプリケーション サーバ (P. 329)名およびポート番号が旧バージョンのものと同じである場合、両方のバージョンを同時に実行することはできません。

旧 CA CSM のシステム ライブラリ（CXX、DBID 002 および 015）およびそれらに関連するデータ（DBID 4000）は、CA CSM アップグレード プロセス中に削除されません。 アップグレード プロセスは、新しいバージョンの CA CSM および旧バージョンの CA CSM の機能の実行を許可する、一意のライブラリおよびデータ セットを追加します。 アップグレード プロセスは旧バージョンのデータベースからデータをコピーして変換し、それを新しいバージョンに組み込みます。 新しいバージョンは、旧バージョンと同じファイル システム、および同じマウント ポイントを使用します。

アップグレードを実施し、最新のバージョンを使用しているとします。現在、旧バージョンを使用している場合、あるバージョンで加えた変更は、別のバージョンには一切反映されません。 旧バージョンのデータは、新しいバージョンのデータから分離されています。 最新のバージョンを使用した後に旧バージョンの CA CSM を使用しようとする場合には注意してください。

注: 新しいバージョンの利点と機能をすべて利用するため、アップグレード プロセスを完了した後、直ちに新しいバージョンを使用し始めることをお勧めします。

長期メンテナンス

何度か最新のバージョンを使用したら、旧バージョンのデータ セットとフォルダをクリーン アップし、DASD を解放することをお勧めします。 旧バージョンのコンテンツを削除する前に、MSMPWIPE ジョブをよく確認してください。

旧バージョンのマウントは、旧バージョンのインストールで単一のマウント ファイル システムまたは複数のマウント ファイル システムのどちらを優先して設定したかに応じて、システムから削除されます。

- 旧バージョンが単一のファイル システムでインストールされている場合、msminstall、msm、msmruntime、msmtmp、mpm フォルダは、1 つのマウント ファイル データ セットの下に作成されます。 その後、UNIX System Services（USS）から msminstall、msm および msmruntime フォルダを削除できます。
- 旧バージョンが複数のファイル システムでインストールされている場合、msminstall、msm、msmruntime、msmtmp、mpm フォルダは、個別のマウント ファイル データ セットを使用します。 USS から msminstall、msm、msmruntime フォルダを削除し、関連するマウント ファイル データ セットを削除し、もしあれば SYS1.PARMLIB（BPXPRM*xx*）から自動マウント エントリを削除できます。

注: リリース 5.1 以降、CA CSM は msmtmp ディレクトリを使用しません。最新のバージョンで、以前のバージョンからの msmtmp ファイル システムを再利用していない場合は、それを削除できます。 ファイル システム データ セットを削除し、SYS1.PARMLIB（BPXPRM*xx*）メンバから自動マウント エントリを削除します。

Prerequisite Validator

CA CSM Prerequisite Validator は、CA CSM をインストールする前に、ユーザが必要な権限をすべて所有しているかどうかを確認できるユーティリティです。

圧縮された CA CSM Prerequisite Validator の製品パッケージは、CA サポート Online Web サイトの Download Center の［CA Chorus Software Manager］ページで入手できます。他の CA CSM ファイルをダウンロードして解凍するのと同じ方法で、パッケージをダウンロードして解凍できます。

Prerequisite Validator 要件

このユーティリティを使用するには、以下の最小要件が必要です。

- z/OS の最新バージョンまたは直近の旧バージョン
- ユーザ用の OMVS セグメント
- Java

  システムに以下の IBM Java SDK for z/OS があること。

  - Java 6.0、ビルド 2.4、メンテナンス レベル SR9（31 ビットまたは 64 ビット）。
  - Java 6.0、ビルド 2.4、メンテナンス レベル SR10（31 ビットまたは 64 ビット）。
  - Java 6.0、ビルド 2.6、基本ビルド（31 ビットまたは 64 ビット）。

    注: Java 6.0、ビルド 2.6 は IBM Java 6.0.1 と同等です。Java 6.0 については、PTF UK56434、APAR PM08437、SDK6 SR8 をインストールします。
  - Java 6.0.1、ビルド 2.6、メンテナンス レベル SR1（31 ビットまたは 64 ビット）。
  - Java 7.0、ビルド 2.6（31 ビットまたは 64 ビット）。
- 最小の TSO REGION サイズ 128 MB
- CA CSM インストールに必要な SAF リソースを確認するための BPX.SERVER READ リソース アクセス権。

注: Prerequisite Validator ユーティリティは特定のリソースへのユーザアクセス権を検証しますが、汎用のユーザ アクセス権（たとえば CA Top Secret for z/OS 用の NORESCHK）は検証*しません*。 Prerequisite Verification レポートは、ユーザにリソースに対するアクセス権がないことを示すことがあります。

ネイティブの USS からの実行

Prerequisite Validator ユーティリティは、ネイティブの USS コマンド プロンプトから直接実行できます。

以下の手順に従います。

1. Prerequisite Validator pax ファイルを、お使いの USS 環境のディレクトリにダウンロードします。
2. お使いの z/OS システムで、ネイティブの USS コマンド プロンプトを開きます。
3. 以下のコマンドを使用して、Prerequisite Validator の pax ファイルをダウンロードしたディレクトリに移動します。

   ```
   cd path_where_Prerequisite_Validator_is_downloaded
   ```

   以下に例を示します。

   ```
   cd /u/users/MSMpre
   ```

4. 以下のコマンドを発行します。

   ```
   pax -rvf 51000068XU1.pax.Z
   ```

   注: Z サフィックスを含む完全な pax ファイル名では、大文字と小文字が区別されます。 pax コマンドを発行するシステムでは、ファイル名に大文字や小文字が正確に使用されていることを確認してください。必要に応じて、ファイル名を変更します。

   Bin フォルダのコンテンツが展開されます。

5. 以下のコマンドを発行します。

   ```
   cd Bin
   ```

6. （オプション） 必要に応じて、デフォルトのプロパティ ファイル パラメータ (P. 41)を修正します。

7. 以下のコマンドを発行して、ユーティリティを呼び出します。

   ```
   ./MSMVal.sh JavaHomePath
   ```

   以下に例を示します。

   ```
   ./MSMVal.sh /usr/lpp/java/J6.0
   ```

   使用許諾契約の画面が表示されます。

8. 使用許諾契約を確認し、F3 キーを押します。

   この契約への同意を促すメッセージが表示されます。

   「**Y**」と入力して、契約に同意します。

   ユーティリティは、ホスト名および IP アドレスをシステムから収集し、JESINTERFACELEVEL を確認するために FTP 接続を試行します。

9. （オプション） デフォルト ファイル パラメータを変更した (P. 41) 場合、または収集したホスト名で接続に失敗した場合、プロンプトの表示に応じてホスト名を入力します。 または、後のセクションで説明されるデフォルト プロパティ ファイルを使用して、この値を指定することもできます。

実行が成功すると、最後に Prerequisite Verification レポートが参照モードで表示され、以下のファイルが生成されます。

- MSMPre-RequisiteVerificationReport.txt
- MSMPre-RequisiteLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log

デフォルト値の設定

以下のファイルで、サイト要件ごとにデフォルト値を設定できます。

unpax_directory/Bin/lib/MSMSetupDefault.properties

このファイルには、以下のパラメータが含まれます。

ホスト名または IP アドレス

HOSTNAME=

システムのホスト名または IP アドレスを指定します。 Prerequisite Validator ユーティリティは、システムのホスト名または IP アドレスを使用して FTP 接続をテストし、JESINTERFACELEVEL 値を確認します。

ローカル ホスト FTP ポート

ftp.port=

指定したホスト名または IP アドレスの FTP ポート番号を指定します。 Prerequisite Validator ユーティリティは FTP 接続をテストし、JESINTERFACELEVEL 値を確認します。

デフォルト： 21

FTP コマンドを発行するための権限

ftp.stat.check.credential=

サイトに FTP 引用 STAT コマンドを発行する権限が必要な場合、ftp.stat.check.credential に y を指定します。 コマンドは以下のようにログに表示されます。

```
503 Login required, enter USER
```

y を設定すると、ユーティリティはユーザ ID とパスワードを求めるメッセージを表示します。

デフォルト： n

FTP リクエスト用のプロキシ サーバ

以下のパラメータは FTP プロキシ チェックに関連しています。 パラメータを **yes** に設定し、プロキシ経由での FTP チェックを有効にします。

```
ftp.proxy.enabled=
ftp.proxy.host=
ftp.proxy.port=
ftp.proxy.credential.check=
ftp.proxy.fireCmd.proxy_userid=
ftp.proxy.fireCmd.site=
ftp.proxy.fireCmd.acct=
ftp.advanced.session.options=
```

ユーティリティは、外部の CA Support FTP サーバへの接続を確認します。 サイトでこれらのリクエストを、プロキシ サーバを経由して送信する必要がある場合、これらのパラメータを以下の例のように変更します。

```
ftp.proxy.enabled=yes
ftp.proxy.host=host_name_or_IP_address
ftp.proxy.port=port_number
ftp.proxy.credential.check=n_or_y
```

ftp.proxy.credential.check が y の場合は、以下のパラメータを変更します。

```
ftp.proxy.fireCmd.proxy_userid=proxy_userid
```

以下のパラメータは、ユーザのプロキシ要件に基づいて変更できます。

```
ftp.proxy.fireCmd.site=
ftp.proxy.fireCmd.acct=
ftp.advanced.session.options=
```

HTTP リクエスト用のプロキシ サーバ

以下のパラメータは HTTP プロキシ チェックに関連します。 以下のパラメータを **yes** に設定し、プロキシ経由での HTTP チェックを有効にします。

```
http.proxy.enabled=
http.proxy.host=
http.proxy.port=80
http.proxy.credential.check=
http.proxy.type=
http.domain=
```

このユーティリティは、外部の CA Support HTTP サーバへの接続を確認します。サイトでこれらのリクエストを、プロキシ サーバを経由して送信する必要がある場合、これらのパラメータを以下の例のように変更します。

```
http.proxy.enabled=yes
http.proxy.host=company_proxy_name
http.proxy.port=80
http.proxy.credential.check=y_or_n
http.proxy.type=NTLM
http.domain=company_domain_name
```

SAF リソース アクセス権のチェック

```
SafSecurityResourceAccess=
```

ユーティリティは、以下のリソースに対するユーザ アクセス権を確認します。

```
BPX.SERVER(UPDATE)
BPX.FILEATTR.SHARELIB(READ)
BPX.FILEATTR.PROGCTL(READ)
BPX.FILEATTR.APF(READ)
```

SafSecurityResourceAccess に n を指定し、リソース アクセス権のチェックをオフにします。

デフォルト： y

MSMServerPortNo

```
MSMServerPortNo=
```

CA CSM への Web ベース アクセス用のアプリケーション サーバ HTTP ポートとして使用するポート番号を指定します。

デフォルト： 22120

MSMDSIPORTNO

CA DSI Server 用のポート番号を指定します。これは、セキュリティ機能を提供するために CA CSM によって内部的に使用されます。

デフォルト： 22130

MSMConnectorRedirectPortNo

リクエストがリダイレクトされるポート番号を指定します。 非 SSL ポートでリクエストが受信され、そのリクエストが SSL を必要とする転送保証を備えたセキュリティ制約に従う場合、リダイレクトが発生します。

デフォルト： 22140

MSMTomcatServerShutdownPortNo

CA CSM アプリケーション サーバがシャットダウン コマンドをリッスンするポート番号を指定します。

デフォルト： 22150

ディスク スペース要件

CA CSM には以下のディスク領域要件があります。

注: すべてのスペース割り振りは、3390 DASD を対象として記述されています。

- CA CSM をインストールおよびセットアップする場合の要件は以下のとおりです。
  - 階層型ファイル システム（HFS）または zSeries ファイル システム（zFS）スペース (P. 82) = 2500 シリンダ

    注: zFS ファイル システムの使用をお勧めします。HFS ファイル システムから zFS ファイル システムに移行する方法の詳細については、最新の「*IBM z/OS Migration*」を参照してください。
  - z/OS スペース = 2400 シリンダ

    このスペースには CA Datacom/MSM SMP/E 環境およびランタイム ライブラリが格納されます。 SMP/E 環境には CA Datacom/MSM、CA Datacom Server および CA CSM コンポーネントが格納されます。
  - SDS ルート スペース = 100 トラック（概算）

    Software Deployment Service（SDS）については、初期 DASD セットアップに対する DASD スペースの総量は、100 トラックです。 この量には CA CSM ホストの CA CSM および SDS スペースのみが含まれており、展開のスナップショット ファイル システムのためのスペースは含まれて*いません*。 追加のスペースが SDS のターゲット システム用に必要です。
  - SDS 展開スペース = 500 シリンダ

    SDS について、各ターゲット システムにはそれぞれ、3390 DASD 用に 500 シリンダが必要ですが、CA Database Management Solutions for DB2 for z/OS については 1500 シリンダが必要です。

- CA CSM を操作する場合の要件は以下のとおりです。

  初期設定の後、CA CSM は製品のダウンロードとメンテナンスに応じて、追加の HFS または zFS ファイルを割り当てます。 割り当てられるスペースの量は、製品の数とメンテナンス、および関連ファイルのサイズによって異なります。

詳細:

USS パスの設定 (P. 82)
USS ファイル システム (P. 262)

ソフトウェア要件

CA CSM には、以下の*最小*ソフトウェア要件があります。

CA Technologies ソフトウェア

お使いのシステムに、CA Common Services for z/OS リリース 14.1、バージョン 14 または r12 が必要です。

- CA CSM 実行システム、Software Deployment Service（SDS）および Software Configuration Service（SCS）用のすべてのターゲット システムに、CETN500（P. 133）が適用されていることを確認します。

  CA Common Services for z/OS r12 またはバージョン 14 に CETN500 をインストールすると、CETN500 は CETN300 または CETN400 を置換します。

  注: すべての公開された CETN500 メンテナンスを適用し、すべてのターゲット システムに展開し、HOLDDATA の手順が完了したことを確認します。 CETN500 を適用しない場合でも CA CSM は操作可能ですが、Software Configuration Service（SCS）および Software Deployment Service（SDS）を利用することはできません。

- PTF RO17488、RO19624、RO41046、RO42868、RO43995 を r12 に APPLY します。

  SDS を使用する予定がない場合は、PTF RO19624 および RO42868 をスキップできます。

  CAICCI 認証呼び出しに APPLID を渡す場合、PTF RO37409 を APPLY します。 PTF RO18999 も必須ですが、これは RO42868 の一部として自動的に APPLY されます。

- バージョン 14 に PTF RO40945、RO44235、RO44412 を APPLY します。

  SCS を使用する予定がない場合は、PTF RO44235 をスキップできます。

  CAICCI 認証呼び出しに APPLID を渡す場合、PTF RO30506、RO30937、RO33987 を APPLY します。

  CA Common Services for z/OS ロード ライブラリの CAW0LOAD および CAW0PLD（リリース 14.1 およびバージョン 14.0）または CAIPLD（r12）は、ジョブ制御言語（JCL）またはシステムの LINKLST を介して CA CSM にアクセスできる必要があります。 必要となるサービスは以下のとおりです。

  - CAICCI

    注: CAICCI を設定し、CAICCI を CA CSM 実行システムおよび SDS と SCS 用のすべてのターゲット システムで実行している必要があります。
  - CAIENF
  - CAIRIM
  - CA-C Runtime

注: CA Common Services for z/OS の詳細については、CA Common Services for z/OS のユーザ マニュアルを参照してください。

他の CA Technologies ソフトウェア製品がある場合は、製品用の必須メンテナンスが以下のようにインストールされていることを確認します。

- CA ACF2 for z/OS を使用する場合、PTF RO31548 を CA ACF2 for z/OS r14 に APPLY します。 または、PTF RO30898 を CA ACF2 for z/OS r15 に APPLY します。
- CA Top Secret for z/OS を使用する場合、PTF RO31780 を CA Top Secret for z/OS r14 に APPLY します。または、PTF RO30836 を CA Top Secret for z/OS r15 に APPLY します。
- SCS ターゲット システムで CA PDSMAN を使用する場合、PTF RO26804 を CA PDSMAN r7.6 に APPLY します。 または、PTF RO25866 を CA PDSMAN r7.7 に APPLY します。

IBM ソフトウェア

ユーザのシステムで以下の要件が満たされている必要があります。

- システムに z/OS の最新のバージョン、または最後の旧バージョンがあること。 IBM は、最近発表の GA バージョンおよび 1 つ前のバージョンをサポートします。
- システムは、JESINTERFACELEVEL 2 ステートメントで設定される FTP.DATA データ セットを備えた、z/OS Communications Server の TCP/IP プロトコル スイートを使用すること。 インストール ジョブが FTP によってサブミットされると、CA CSM インストール プロセスはジョブ ステータスと出力を取得するために、JESINTERFACELEVEL 2 ステートメントを要求します。 CA CSM を正常にインストールした後、JESINTERFACELEVEL をその前の値に戻すことができます。

  あるいは CA CSM インストール プロセスを設定し、ジョブのサブミットおよび処理に TSO を使用 (P. 259)できます。
- システムに少なくとも SMP/E V3R5 があること。
- システムに以下の IBM Java SDK for z/OS があること。
  - Java 6.0、ビルド 2.4、メンテナンス レベル SR9（31 ビットまたは 64 ビット）。
  - Java 6.0、ビルド 2.4、メンテナンス レベル SR10（31 ビットまたは 64 ビット）。
  - Java 6.0、ビルド 2.6、基本ビルド（31 ビットまたは 64 ビット）。

    注: Java 6.0、ビルド 2.6 は IBM Java 6.0.1.For Java 6.0、インストール PTF UK56434、APAR PM08437、SDK6 SR8 と同等です。
  - Java 6.0.1、ビルド 2.6、メンテナンス レベル SR1（31 ビットまたは 64 ビット）。
  - Java 7.0、ビルド 2.6（31 ビットまたは 64 ビット）。

このソフトウェアを SMP/E 以外のインストール可能な形式でダウンロードできます。 詳細については、次の Web サイトに移動し、ソフトウェアへのリンクをクリックします。 http://www-03.ibm.com/servers/eserver/zseries/software/java/。 この Web ページには、利用可能な IBM SDK のリリースが表示されます。 リリースのリンクから、より詳細な Web ページにリダイレクトされます。詳細ページは通常、*追加のインストール情報*用のテキストの中にリンクがあります。 このリンクから開くページから、CA CSM が使用する JZOS Batch Launcher 機能をカスタマイズするために有用な情報を取得できます。 たとえばこの情報を使用して、それがサイトで望ましい設定である場合、CA CSM 用の代替 JVM loadlib を作成することができます。

- Language Environment ライブラリの CEE.SCEERUN2 は、APF 許可されています。

PC ソフトウェア

CA CSM にアクセスするために使用するコンピュータには、少なくとも以下のいずれかの Web ブラウザが必要です。

- Microsoft Internet Explorer 7、8、9
- Mozilla Firefox 13、14、15、16

Mozilla Firefox を使用することをお勧めします。

お使いの Web ブラウザが CA CSM が実行されているサーバに対して有効な JavaScript および Cookie があることを確認します。

注: 画面解像度は 1024 × 768 ピクセル以上をお勧めします。 それより低い画面解像度の場合、CA CSM Web ベース インターフェースで正しく表示されない要素があります。

詳細:

CA Common Services コンポーネント要件 (P. 273)
CA CSM の起動 (P. 266)

z/OS 設定

CA CSM インストーラのユーティリティおよび CA CSM アプリケーション サーバを正常に実行するには、SYS1.PARMLIB（BPXPRM*xx*）で OMVS の制限を以下のように指定します。

MAXASSIZE(*nnnnn*)

2147483647 に設定します。

MAXCPUTIME(*nnnnn*)

最小で 20000 に設定します。

MAXFILEPROC(*nnnnn)*

最小で 10000 に設定します。

MAXTHREADS(*nnnnn)*

最小で 1000 に設定します。

MAXTHREADTASKS(*nnnnn*)

最小で 1000 に設定します。

注: 現在の設定を表示するには、以下のコマンドを発行します。

```
DISPLAY OMVS,OPTIONS
```

SETOMVS オペレータ コマンドを使用して、オペレーティング システムの IPL を実行せずに、これらの値を動的に変更することができます。 これらの値を動的に変更するには、以下のオペレータ コマンドを発行します。

```
SETOMVS MAXASSIZE=2147483647
SETOMVS MAXCPUTIME=20000
SETOMVS MAXFILEPROC=10000
SETOMVS MAXTHREADS=1000
SETOMVS MAXTHREADTASKS=1000
```

CSF の初期化

CA CSM アプリケーション サーバ (P. 329)（MSMTC (331以下のページで定義参照：)）は、ランダムのファイルを作成してユーザ セッションの追跡を試み、ファイルが作成されると CA CSM はそのファイルを使用します。このファイルの作成はプラットフォームに関係なく、基本の Apache Tomcat アプリケーションで実行されます。 このファイルが設定されない場合、CA CSM アプリケーションは、それ自身のロジックを使用してユーザ セッションを追跡します。 z/OS でランダムなファイルの作成を成功させるには、サイトに Integrated Cryptographic Services Facility（ICSF）プロセッサが取り付けられ、有効である必要があります。 サイトに ICSF プロセッサがない場合、CA CSM は以下の例のようなメッセージを発行し、初期化を続行します。

```
Aug 5, 2010 4:56:37 PM org.apache.catalina.session.ManagerBase setRandomFile
 WARNING: Failed to close randomIS.
```

ICSF プロセッサが有効な場合は、CA CSM アプリケーション サーバ (P. 329)（MSMTC (331以下のページで定義参照：)）を開始する前に、CSF アドレス空間を完全に初期化します。 CSF アドレス空間を初期化しない場合、CA CSM が失敗し、再試行も行いません。 リカバリするには、MSMTC (331以下のページで定義参照：) スターティッド タスクのリサイクルを実行してください。

LPAR に接続されている ICSF プロセッサがある場合は、システム自動化ソフトウェアを使用して、CSF スターティッド タスクを、MSMTC (331以下のページで定義参照：) スターティッド タスクを開始する前提条件として追加することをお勧めします。

CSF アドレス空間の初期化が成功した後、MSMTC スターティッド タスクのみを開始してください。 システム自動化ソフトウェアを設定し、以下の CSF 初期化メッセージを検索します。

CSFM001I ICSF INITIALIZATION COMPLETE

このメッセージは、CSF サービスが開始されたが利用可能ではないこと、また暗号キーがまだロードされていないことを通知します。

または

CSFM400I CRYPTOGRAPHY - SERVICES ARE NOW AVAILABLE.

このメッセージは、ICSF サービスが利用可能で、また暗号キーがロードされたことを通知します。

注: 詳細については、「*IBM z/OS Cryptographic Services PKI Services Guide and Reference*」（SA22-7693-12）を参照してください。

Web アクセス要件

ネットワーク管理者は、以下の Web サイトおよび FTP サイトへのアクセス権を設定する必要があります。

- supportservices.ca.com（HTTPS ポート番号 443 を使用）
- ftp.ca.com（FTP ポート番号 21 を使用）
- ftpca.ca.com（FTP ポート番号 21 を使用）

  注: CA CSM はこの FTP サーバを使用して、最小限の情報を収集します。この情報には、CA サポート Online Web サイトのサイト ID、製品、ユーザ ID などがあります。 サイトのアクセス ルールにより、これらの情報の収集を目的として確立された FTP 接続が拒否されることがあり、あるいはその他の理由により接続が確立できないことがあります。 その後も、CA CSM は引き続き稼働します。
- scftpd.ca.com（FTP ポート番号 21 を使用）

- ftpdownloads.ca.com（FTP ポート番号 21 を使用）
- supportftp.ca.com（FTP ポート番号 21 を使用）
- sdownloads.ca.com（HTTPS ポート番号 443 を使用）

  注: ［Settings］ページの［System Settings］ - ［Software Acquisition］で［Use HTTPS for Downloads］取得オプションを使用する場合、sdownloads.ca.com のみが必要です。 ポート 80 とポート 443 の両方に対して ca.com ドメインを許可する場合、sdownloads.ca.com を許可する必要はありません。

さらに、ネットワーク管理者は localhost のドメイン ネーム システム（DNS）エントリを定義する必要があります。

TCP/IP ポートの予約

以下の TCP/IP ポートを予約することをお勧めします。

- CA CSM アプリケーション サーバ HTTP ポート
- CA DSI Server ポート
- CA CSM アプリケーション サーバ リダイレクト ポート
- CA CSM アプリケーション サーバ シャットダウン ポート

ポートを予約するには、z/OS の TCP/IP プロファイル データ セットを更新します。

例

```
PORT      Application ID
22120 TCP MSMTC* ; CA CSM Application Server HTTP port
22130 TCP MSMTC* ; CA DSI server port
22140 TCP MSMTC* ; CA CSM Application server redirect port
22150 TCP MSMTC* ; CA CSM application server shutdown port
```

注: セキュリティ上の理由により、このセクションの例で表示されているアスタリスク（*）を使用せず、8 文字のアプリケーション ID を使用することをお勧めします。 **MSMTC** を 8 文字のジョブ名に変更するには、CA CSM スタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））を編集します。次に、z/OS の TCP/IP プロファイルデータ セットの **MSMTC*** を、同じ 8 文字のジョブ名に変更します。

CA CSM アプリケーション サーバに 5 文字の名前を使用する場合、CA DSI Server ポート番号の定義にはアスタリスク（*）を使用する必要があります。アプリケーション ID に追加されるシーケンス番号を一意にする必要があるためです。

詳細:

ポート、データ セットおよび USS ディレクトリ (P. 244)

セキュリティ セットアップ

CA CSM を正常に実装するため、セキュリティ管理者は以下の必要なセキュリティをセットアップする必要があります。

- CA CSM をダウンロード、インストール、セットアップするユーザに、必要なアクセス権を付与します。
- CA CSM アプリケーション サーバ（P. 329）（MSMTC（331以下のページで定義参照：）ジョブまたはスターティッド タスク）に関連付けられたユーザ ID に、必要なアクセス権を付与します。
- Web ベース インターフェースを使用して CA CSM にログインするユーザのセキュリティをセットアップします。

詳細:

ユーザの USS 許可のセットアップ (P. 58)
CA CSM 機能のユーザ セキュリティのセットアップ (P. 62)

CA CSM アプリケーション サーバでのセキュリティのセットアップ

このセクションのトピックでは、CA CSM アプリケーション サーバ (P. 329) 上で CA CSM のセキュリティをセットアップする方法について説明します。

CA CSM ダウンロード、インストール、セットアップのアクセス要件

CA CSM をダウンロード、インストール、セットアップするには、セキュリティ管理者はお使いのシステム上で、以下のアクセス権限を設定する必要があります。

1. CA CSM のダウンロードおよび実装のための UNIX System Services（USS）への以下のアクセス権。

   CA CSM 用に新規ファイル システムを作成しマウントする場合、以下の*いずれか*の権限が必要です。

   - サイトが CA SAF HFS セキュリティを使用する場合、BPX.CAHFS.CHANGE.FILE.ATTRIBUTES
   - サイトが CA SAF HFS セキュリティを使用*しない*場合、UID（0）または BPX.SUPERUSER 権限

   注: CA SAF HFS セキュリティは CA ACF2 for z/OS および CA Top Secret for z/OS の機能です。

2. CA CSM を実装するユーザのための、以下のデータ セットまたはライブラリへの UPDATE 権限

   - SYS*x*.PARMLIB
   - CA CSM アドレス空間を開始するために使用される、JCL ジョブを格納するプロシージャ ライブラリ（たとえば、SYS3.PROCLIB）
   - （オプション）CA CSM データ セットのプレフィクス用にエイリアス エントリを定義する場合のマスタ カタログ

3. CA CSM セットアップ ユーティリティと関連付けられたユーザ ID 用のアクセス権

   - UNIX に関連する、以下の FACILITY クラス プロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）
     - BPX.DAEMON（READ 権限）
     - BPX.SERVER（UPDATE 権限）
     - BPX.CONSOLE（READ 権限）
   - SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）

- SMP/E GIMUNZIP ハッシュ検証を実行するための CSFSERV クラス プロファイル、CSFOWH（READ 権限）へのアクセス許可
- オプション ファイル (P. 240)で指定された修飾子（CA CSM MVS SMP/E およびランタイム データ セット）用のデータ セットの作成および修正の許可

  注: ユーザ ID は BPX.SUPERUSER アクセス権を持つことができ、それを SUPERUSER に切り替えることができます。 その後、その切り替えられた SUPERUSER ID には、オプション ファイル (P. 240)で指定された MVS データ セット修飾子の作成および修正のアクセス権が必要です。
- IBM RACF を使用している場合、プログラム制御用の以下のデータ セットにアクセスします。
  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - メンバ IEANTCR、IEANTDL および SYS1.CSSLIB の IEANTRT
  - メンバ JVMLDM60（31 ビット Java 6.0 用）、または Java のロード モジュールがインストールされているデータ セットの JVMLDM66（64 ビット Java 6.0 用）。

    または
  - メンバ JVMLDM61（31 ビット Java 6.0.1 用）、または Java のロード モジュールがインストールされているデータ セットの JVMLDM67（64 ビット Java 6.0.1 用）。

    または
  - メンバ JVMLDM70（31 ビット Java 7.0 用）、または JVMLDM76（64 ビット Java 7.0 用）。
  - （オプション）オプションの EXIT として IDIXCEE を使用する場合にのみ、SYS1.IDI.SIDIAUTH のメンバ IDIXCEE。

  注: リソースを表示するには、RLIST コマンドを発行します。

  IBM RACF を制御プログラムに設定できます。 リソースが存在しない場合は、以下のコマンドを発行します。

  ```
  RDEFINE PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  以下に例を示します。

  ```
  RDEFINE PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

リソースが存在する場合は、以下のコマンドを発行します。

```
RALTER PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
```

以下に例を示します。

```
RALTER PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
```

注: データ セットの全メンバを制御済みプログラムとして設定するには、メンバ名をアスタリスク（*）で置換します。 以下に例を示します。

```
RDEFINE PROGRAM * ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
```

重要: zFS を使用する予定がある場合は、プログラム制御に IOE.SIOELMOD（または同等のライブラリ）を追加します。

CA CSM アプリケーション サーバに関連付けられたユーザ ID 用のアクセス要件

CA CSM を正常に操作するため、CA CSM アプリケーション サーバ (P. 329)（MSMTC (331以下のページで定義参照：) ジョブまたはスターティッド タスク）に関連付けられたユーザ ID には、以下のアクセス権限が必要です。

1. セキュリティ管理者は、CA CSM 用の UNIX System Services（USS）へのアクセス権を設定する必要があります。 CA CSM アプリケーション サーバ (P. 329) ユーザ ID には、読み取りおよび書き込みアクセス権がある有効なホーム ディレクトリを持った OMVS セグメントが必要です。

   CA CSM には、以下の*いずれか*の権限が必要です。

   - サイトが CA SAF HFS セキュリティを使用する場合、BPX.CAHFS.CHANGE.FILE.ATTRIBUTES
   - サイトが CA SAF HFS セキュリティを使用*しない*場合、UID（0）

   注: CA SAF HFS セキュリティは CA ACF2 for z/OS および CA Top Secret for z/OS の機能です。

2. セキュリティ管理者は、以下のアクセス権を設定する必要があります。

   - UNIX に関連する、以下の FACILITY クラスのプロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）

- BPX.SERVER（UPDATE 権限）
- BPX.CONSOLE（READ 権限）

■ SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）

注: SAF セキュリティを使用している場合は、以下のオプションを検討します。

- CSFSERV クラスがアクティブな場合、CA CSM アプリケーション サーバのこのリクエストを行うユーザ ID には CSFRNG と CSFDSV への READ アクセス権があることを確認します。
- APPL クラスがアクティブな場合、CA CSM アプリケーション サーバのこのリクエストを行うユーザ ID には OMVSAPPL リソースへの READ アクセス権があることを確認します。

注: CA CSM は、CA CSM アプリケーション サーバ ID のセキュリティ コンテキストで GIMUNZIP を実行します。SMP/E セキュリティがアクティブな場合、CA CSM アプリケーション サーバ ID には SAF FACILITY クラスの GIM.PGM.GIMUNZIP リソースへの READ アクセス権が必要です。

CA Top Secret for z/OS でのスターティッド タスク セキュリティのセットアップ

CA Top Secret for z/OS の下でスターティッド タスクとして CA CSM アプリケーション サーバ (P. 329)（MSMTC (331以下のページで定義参照：)）を実行する予定がある場合は、関連する設定を実行します。

以下の手順に従います。

1. 以下のコマンドを使用し、スターティッド タスクの機能を定義します。

   ```
   TSS MODIFY FACILITY(USERxx=NAME=MSM)
   TSS MODIFY FACILITY(MSM=MULTIUSER,SIGN(M))
   ```

   この機能を使用し、サーバにログインできるユーザを制御します。

   注: 詳細については、「*CA Top Secret for z/OS Control Options Guide*」を参照してください。

2. サーバを制御する ACID（ユーザ ID）を作成します。

   注: 詳細については、「*CA Top Secret for z/OS Command Functions Guide*」を参照してください。

3. STC テーブルにサーバ リージョンを定義します。

   STC エントリにはサーバ プロシージャ名および ACID が含まれます。

   注: 詳細については、「*CA Top Secret for z/OS Command Functions Guide*」を参照してください。

4. MASTFAC キーワードを使用し、手順 1 で定義した機能をサーバの ACID に追加します。

   注: 詳細については、「*CA Top Secret for z/OS Command Functions Guide*」を参照してください。

5. FACILITY キーワードを使用し、手順 1 で定義した機能を、サーバへのログオンを必要とする各ユーザに追加します。

   注: 詳細については、「*CA Top Secret for z/OS Command Functions Guide*」を参照してください。

ユーザの USS 許可のセットアップ

CA CSM のユーザには、USS へのアクセス権が必要です。 ユーザにはそれぞれ OMVS セグメントが必要です。 セキュリティ管理者は、これらのセグメントをセットアップする必要があります。

以下の手順に従います。

1. OMVS UID 番号を選択し、各ユーザ ID に関連付けます。 セキュリティ管理者が、OMVS UID 番号を割り当てるためのポリシーを保有している可能性があります。 そうでない場合は、一意の番号を使用します。

   注: OMVS UID 番号の詳細については、「*IBM UNIX System Services Planning*」を参照してください。

2. ユーザの OMVS セグメントを定義します。ユーザ ID には *uuuuuuu*、UID 番号には *nnn*、ホーム ディレクトリには *path_name* を指定し、以下のコマンドを入力します。

   - CA ACF2 for z/OS システムについては、以下のコマンドを入力します。

     ```
     SET PROFILE(USER) DIV(OMVS)
     INSERT uuuuuuu UID(nnn) HOME(path_name) OMVSPGM(/bin/sh)
     ```

   - CA Top Secret for z/OS システムについては、以下のコマンドを入力します。

     ```
     TSS ADD(uuuuuuu) HOME(path_name) OMVSPGM(/bin/sh) UID(nnn)
     GROUP(ggggggg)
     ```

   - RACF システムについては、以下のコマンドを入力します。

     ```
     ALU uuuuuuu OMVS(UID(nnn) HOME(path_name) PROGRAM(/bin/sh))
     ```

   注: OMVS セグメントには以下の構成要素が含まれている必要があります。

   - ホーム ディレクトリ（HOME）
   - ログイン シェル（PROGRAM または OMVSPGM）

3. 認可する各ユーザ ID に対してこの手順を完了したことを確認します。OMVS セグメントの内容を確認するには、以下のコマンドを入力します。

   - CA ACF2 for z/OS システムについては、以下のコマンドを入力します。

     ```
     SET PROFILE(USER) DIV(OMVS)
     LIST uuuuuu
     ```

   - CA Top Secret for z/OS システムについては、以下のコマンドを入力します。

     ```
     TSS LIST(uuuuuu) DATA(ALL)
     ```

   - RACF システムについては、以下のコマンドを入力します。

     ```
     LISTUSER uuuuuu OMVS NORACF
     ```

4. 各ユーザ ID と関連付けるホーム ディレクトリを選択します。 ホーム ディレクトリが存在し、UID にホーム ディレクトリの読み取りおよび書き込みアクセス権があることを確認してください。

   手順 2 に示されている UNIX ディレクトリ（*path_name*）を使用するか、カスタマイズされたホーム ディレクトリ名を使用できます。

   たとえば、UID*nnn* 用の /u/name という名前のディレクトリを設定するには、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
   ```

5. 以下のコマンドを使用して、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
   ```

   以下の結果が表示されます。

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

HTTPS を使用するための CA CSM の設定

この手順を使用して、ユーザ アクセスに HTTP ではなく HTTPS を使用するように、CA CSM を手動で設定します。

以下の手順に従います。

1. 以下の手順に従って、キーストアを生成します。

   a. OMVS セッションを開始し、以下のコマンドを入力します。

      ```
      keytool -genkey -alias tomcat -keyalg RSA
      ```

      プロンプトが表示されます。

      注: *keytool* は Java ライブラリにある Java のコマンドです。 これらのライブラリは、*/Customer-Java-Prefix/* java/J6.0.1/bin/ のような名前で、*Customer-Java-Prefix* はユーザ サイトでの Java USS のディレクトリ名です。 USS プロファイル パス変数にこのディレクトリ名を追加すると、コマンドを正常に実行できます。

   b. プロンプトに従って、キーストアのパスワードを記憶し、デフォルトのパスワードを保持するかどうかを尋ねるプロンプトが表示されたら、Enter キーを押します。

      デフォルトのキーストアは、自己署名証明書が 1 つあるホーム ディレクトリに作成されます。

c. （オプション）別の場所に作成する場合、/path/to/my/keystore の部分を自分のサイト固有情報に置き換えて、以下のコマンドを入力します。

```
keytool -genkey -alias tomcat -keyalg RSA ¥ -keystore /path/to/my/keystore
```

2. 以下の手順に従って、Apache Tomcat を設定します。

a. tomcat/conf に移動し、server.xml ファイルを開きます。

b. 以下のように、SSL コネクタの部分のコメントを解除するか、または置換します。

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
   <Connector port="30308" maxHttpHeaderSize="8192"
              maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
              enableLookups="false" disableUploadTimeout="true"
              SSLEnabled="true"
              keystorePass="tomcat"
              keystoreFile="/a/path/to/my/keystore/.keystoreFile"
              algorithm="IbmX509"
              acceptCount="100" scheme="https" secure="true"
              clientAuth="false" sslProtocol="TLS"
              sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1" /> "
```

c. ニーズに合わせて、ポートと keystoreFile のパラメータを変更します。

d. keystorePass が前の手順で指定したパスワードと必ず一致するようにしてください。

e. 標準的な HTTP コネクタでは、SSL コネクタで指定したものと同じ redirectPort を以下のように指定します。

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <Connector port="30305" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" redirectPort="30308"
               acceptCount="100"
               connectionTimeout="20000" disableUploadTimeout="true" />
    <!-- Note : To disable connection timeouts, set connectionTimeout
     value to 0 -->
```

3. Apache Tomcat を起動（または再起動）します。

4. TLS 暗号化を使用するために、以下のようにしてブラウザを有効にします。
   - Microsoft Internet Explorer を使用する場合は、［ツール］-［インターネット オプション］ -［詳細設定］の順にクリックし、［セキュリティ］の下の［TLS 1.0 を使用する］チェック ボックスをオンにします。
   - Mozilla Firefox を使用する場合は、［ツール］-［オプション］-［詳細］の順にクリックし、［暗号化］タブの［TLS 1.0 を使用する］チェック ボックスをオンにします。
5. ブラウザを再起動します。
6. HTTPS URL にアクセスします。

   注: お使いのブラウザから HTTPS URL に初めてアクセスすると、証明書を信頼することを確認するメッセージが表示されます。
7. ［Yes］をクリックし、信頼済みの証明書にこの証明書を追加します。

注: 詳細については、Web で「Apache Tomcat 6.0 Servlet/JSP Container」を参照してください。

CA CSM 機能のユーザ セキュリティのセットアップ

CA CSM は CAMSM リソース クラスのリソース プロファイル (P. 279)を使用し、Web ベース インターフェース上のリソースへのアクセス権を付与します。 これらのプロファイルを使用し、ユーザ セキュリティを設定します。 CA CSM 機能のセキュリティ チェックの有効化が予定されている場合、セキュリティ管理者はユーザが Web ベース インターフェースにアクセスする前に、セキュリティを設定する必要があります。

SAF リソース クラスのデフォルトの名前は CAMSM です。 CA CSM インストール中にそのリソース クラス名を変更できます。名前を変更するには、CA CSM オプション ファイル (P. 251)内の safResourceClass キーワードを編集します。

CA CSM をインストールしてセットアップした後に設定を変更する場合、SAMPLIB（MSMLIB）メンバ内の以下のステートメントを更新します。

```
IJO="$IJO-Dsaf.resource.class=saf_resource_class_name"
```

CA CSM オプション ファイル (P. 240)の safSecurity キーワードは、SAF リソースを使用して CA CSM へのアクセスをコントロールするかどうかを制御します。 CA CSM をインストールしてセットアップした後に設定を変更する場合、SAMPLIB（MSMLIB）メンバ内の以下のステートメントを更新します。 値が false の場合はセキュリティが無効になり、値が true の場合はセキュリティが有効になります。

```
IJO="$IJO -Dactivate.saf.manager=false_or_true"
```

重要: SAF セキュリティが有効化された CA CSM の開始に失敗 (P. 313)した場合、以下のエラーが CA CSM ジョブ ログで表示されます。

SafError - Error during DSI java open. RC=13

リソース プロファイルは、リソースへの細やかなアクセスを提供します。しかしながら、まず始めに 2 つの一般的なロールである管理者および一般ユーザ用のセキュリティを設定します。

以下の手順に従います。

1. リソース プロファイルを使用し、ユーザ セキュリティを設定します。

   ユーザはさまざまなロールに対してセキュリティ保護されます。

2. CA CSM アプリケーション サーバを再利用します。

   設定されたセキュリティが有効になります。

注: CA CSM の前に製品管理作業の実行で使用されていたのと同じ認証情報を使用することをお勧めします。 同じ認証情報を使用することで、CA CSM 内の TSO、BATCH、ISPF、SMP/E に対して、ユーザに確実に同じアクセス権限を持たせることができます。

ユーザ セキュリティ権限への変更を有効にするには、CA CSM アプリケーション サーバを再起動します。

詳細:

SAF セキュリティが有効な状態での CA CSM の開始に失敗する (P. 313)
CA CSM 機能のセキュリティ (P. 278)

CA ACF2 for z/OS でのユーザ セキュリティのセットアップ

CA ACF2 for z/OS では、CAMSM リソース クラスを使用してグローバル システム オプション（GSO）の CLASMAP レコードを作成し、適切な CA CSM リソース プロファイルにユーザ許可を付与します。

注: CAMSM は SAF リソース クラスのデフォルトの名前です。 お使いのシステムでは、CA CSM のインストールに応じて (P. 62)別の名前が使用される場合があります。

CLASMAP レコードを定義するには、以下の CA ACF2 for z/OS コマンドを発行します。

```
SET C(GSO)
INSERT CLASMAP.MSM ENTITYLN(246) MUSID() RESOURCE(CAMSM) RSRCTYPE(MSM)
```

CLASMAP レコードをリフレッシュするには、以下のコマンドを発行します。

```
F ACF2,REFRESH(CLASMAP),TYPE(GSO)
```

注: リソース プロファイル (P. 279)を使用して、CA CSM へのアクセスを拒否または許可します。

以下の例では、さまざまなロールのユーザに対してセキュリティをセットアップする方法を示します。

例: 管理者

ユーザ MSMUSR1 にすべてのアクションへのアクセス権を付与します。アクションには、システム設定の管理、システム レジストリ、方法、展開、設定、およびユーザ設定などがあります。

以下の CA ACF2 for z/OS コマンドを発行します。

```
SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(*****MSMUSR1)                    SERVICE(READ)     ALLOW


SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS.-    UID(*****MSMUSR1)      SERVICE(READ)     ALLOW
LMPKEY.-      UID(*****MSMUSR1)      SERVICE(READ)     ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION.-    UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION.-    UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
UID(*****MSMUSR1)     SERVICE(READ)     ALLOW

SET R(MSM)
COMPILE STORE
$KEY(TM) TYPE(MSM)
UID(*****MSMUSR1)     SERVICE(READ)     ALLOW
```

例: ユーザ

ユーザ MSMUSR2 にすべてのユーザ アクションに対するアクセス権を付与します。ただし、ユーザは環境内の SANDBOX システムのみにアクセスできます。 この設定を行ったユーザは、システムまたは他のユーザの設定の管理、システム レジストリの変更、または方法の作成を行うことはできません。 ユーザは、SANDBOX システムをターゲットとした展開を作成でき、他の CA CSM ユーザが定義した方法を使用できます。 ユーザは、定義済みシステム プロファイルの値を使用して SANDBOX リモート システムをターゲットとした設定を作成できますが、それらの設定を実行することはできません。

以下の CA ACF2 for z/OS コマンドを発行します。

```
SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(*****MSMUSR2)                       SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS.USER.-   UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
LMPKEY.-          UID(*****MSMUSR2)   SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION.-         UID(*****MSMUSR2)   SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION.-         UID(*****MSMUSR2)   SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
@DISPLAY.-        UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@PROFILE.DISPLAY  UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@SYSTEM.SANDBOX   UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
@DISPLAY.-        UID(*****MSMUSR2)   SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
@DISPLAY.-        UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@BUILD.-          UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@EXECUTE.-        UID(*****MSMUSR2)   SERVICE(READ)   ALLOW


SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
@DISPLAY.-        UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@ACTION.CREATE    UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
@ACTION.REMOVE    UID(*****MSMUSR2)   SERVICE(READ)   ALLOW
```

例: 制限されたユーザ

ユーザ MSMUSR3 に以下のアクションに対してのみアクセス権を付与します。

- 製品パッケージのダウンロード。
- CA CSM 以外でダウンロードされた製品パッケージのインストール。
- 既存の SMP/E 環境の CA CSM への移行。
- CA CSM からの SMP/E 環境のナレッジの削除。
- 独自の展開の作成と展開。
- プロファイル情報をはじめとする、システム レジストリ内のリモート システムの作成とメンテナンス。
- リモート システム上に準備された設定の実行。

以下の CA ACF2 for z/OS コマンドを発行します。

```
SET R(MSM)
COMPILE STORE
$KEY(LOGON) TYPE(MSM)
UID(*****MSMUSR3)                       SERVICE(READ)   ALLOW
```

```
SET R(MSM)
COMPILE STORE
$KEY(ADMIN) TYPE(MSM)
SETTINGS.USER.-      UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(SC) TYPE(MSM)
@ACTION.INSTPKG.-    UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(SMPE) TYPE(MSM)
@ACTION.MIGRATE.-    UID(*****MSMUSR3)   SERVICE(READ)   ALLOW
@ACTION.REMOVECSI.-  UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(SYSREG) TYPE(MSM)
                     UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(METHOD) TYPE(MSM)
@DISPLAY.-           UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(DEPLOY) TYPE(MSM)
@SELF.-              UID(*****MSMUSR3)   SERVICE(READ)   ALLOW

SET R(MSM)
COMPILE STORE
$KEY(CONFIG) TYPE(MSM)
@ACTION.IMPL         UID(*****MSMUSR3)   SERVICE(READ)   ALLOW
```

詳細情報:

CA ACF2 for z/OS での SCS アドレス空間セキュリティのセットアップ (P. 189)
CA ACF2 for z/OS PassTicket の例 (P. 192)

CA Top Secret for z/OS でのユーザ セキュリティのセットアップ

CA CSM はリソース プロファイル (P. 279)を使用し、Web ベース インターフェースのリソースへのアクセス権を付与するために リソース クラスは CAMSM です。CA Top Secret for z/OS では、さまざまなロールに対する適切なリソース プロファイルが含まれるセキュリティ プロファイルを定義し、そのセキュリティ プロファイルをユーザにアタッチすることができます。

注: CAMSM は SAF リソース クラスのデフォルトの名前です。 お使いのシステムでは、CA CSM のインストールに応じて (P. 62)別の名前が使用される場合があります。

以下の手順に従います。

1. お使いのセキュリティ製品で CAMSM リソース クラスを定義します。

   CAMSM リソース クラスが定義されます。
2. セキュリティ プロファイルを定義し、ロールを設定します。

   さまざまなロールのユーザに対し、プロファイルをアタッチできます。
3. ユーザにプロファイルをアタッチします。

   ユーザはさまざまなロールに対してセキュリティ保護されます。

詳細情報:

CA Top Secret for z/OS での SCS アドレス空間セキュリティのセットアップ (P. 189)
CA Top Secret for z/OS PassTicket の例 (P. 195)

CA Top Secret for z/OS での CAMSM リソース クラスの定義

CA CSM リソース プロファイルを使用する前に、お使いのセキュリティ製品へのプロファイルを含んだ CAMSM クラスを定義します。

注: CAMSM は SAF リソース クラスのデフォルトの名前です。 お使いのシステムでは、CA CSM のインストールに応じて (P. 62)別の名前が使用される場合があります。

以下の手順に従います。

1. 以下のコマンドを発行します。

```
TSS ADDTO(RDT) RESCLASS(CAMSM)
               ATTR(MASK) MAXLEN(246)
TSS REPL(RDT) RESCLASS(CAMSM)
                ACLST(READ=4000,UPDATE=8000,CONTROL=0400,NONE=0000)
                DEFACC(READ)
```

2. 以下のコマンドを発行して、CAMSM クラス内のリソース プロファイルを定義します。

```
TSS ADDTO(MSMDPT) CAMSM(LOGON)
TSS ADDTO(MSMDPT) CAMSM(ADMIN.)
TSS ADDTO(MSMDPT) CAMSM(SC.)
TSS ADDTO(MSMDPT) CAMSM(SMPE.)
TSS ADDTO(MSMDPT) CAMSM(SYSREG.)
TSS ADDTO(MSMDPT) CAMSM(METHOD.)
TSS ADDTO(MSMDPT) CAMSM(DEPLOY.)
TSS ADDTO(MSMDPT) CAMSM(CONFIG.)
TSS ADDTO(MSMDPT) CAMSM(TM.)
```

注: リソース プロファイル (P. 279)を使用して、CA CSM へのアクセスを拒否または許可します。

セキュリティ プロファイルの定義

以下の例では、さまざまなロールのセキュリティ プロファイルを定義します。

例: 管理者

すべてのアクションへのアクセス権を付与するプロファイル MSMPRF1 を定義します。 アクションには、システム設定の管理、システム レジストリ、方法、展開、設定、およびユーザ設定などがあります。

以下の CA Top Secret for z/OS コマンドを発行します。

```
TSS CREATE(MSMPRF1)    NAME('CA CSM ADMIN PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF1)    CAMSM(LOGON)   ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(ADMIN.)  ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(SC.)     ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(SMPE.)   ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(SYSREG.) ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(METHOD.) ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(DEPLOY.) ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(CONFIG.) ACCESS(READ)
TSS PERMIT(MSMPRF1)    CAMSM(TM.)     ACCESS(READ)
```

例: ユーザ

すべてのユーザ アクションへのアクセス権を付与するプロファイル MSMPRF2 を定義します。ただし、ユーザがアクセスできるのは、環境内の SANDBOX システムのみです。 この設定を行ったユーザは、システムまたは他のユーザの設定の管理、システム レジストリの変更、または方法の作成を行うことはできません。ユーザは、SANDBOX システムをターゲットとした展開を作成でき、他の CA CSM ユーザが定義した方法を使用できます。ユーザは、定義済みシステム プロファイルの値を使用して SANDBOX リモート システムをターゲットとした設定を作成できますが、それらの設定を実行することはできません。

以下の CA Top Secret for z/OS コマンドを発行します。

```
TSS CREATE(MSMPRF2) NAME('CA CSM USER PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF2) CAMSM(ADMIN.SETTINGS.USER)     ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(ADMIN.LMPKEY)            ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SC.@ACTION)              ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SMPE.@ACTION)            ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@DISPLAY)         ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@PROFILE.DISPLAY) ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(SYSREG.@SYSTEM.SANDBOX)  ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(METHOD.@DISPLAY)         ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(DEPLOY.)                 ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@DISPLAY)         ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@ACTION.CREATE)   ACCESS(READ)
TSS PERMIT(MSMPRF2) CAMSM(CONFIG.@ACTION.REMOVE)   ACCESS(READ)
```

例: 制限されたユーザ

以下のアクションのみへのアクセス権を付与するプロファイル MSMPRF3 を定義します。

- 製品パッケージのダウンロード。
- CA CSM 以外でダウンロードされた製品パッケージのインストール。
- 既存の SMP/E 環境の CA CSM への移行。
- CA CSM からの SMP/E 環境のナレッジの削除。
- 展開の作成と、それらの展開（それらが所有者である場合）。
- プロファイル情報をはじめとする、システム レジストリ内のリモート システムの作成とメンテナンス。
- リモート システム上に準備された設定の実行。

以下の CA Top Secret for z/OS コマンドを発行します。

```
TSS CREATE(MSMPRF3) NAME('CA CSM SMPE USER PROFILE') DEPT(MSMDPT) TYPE(PROFILE)
TSS PERMIT(MSMPRF3) CAMSM(ADMIN.SETTINGS.USER)      ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SC.@ACTION.INSTPKG)       ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SMPE.@ACTION.MIGRATE)     ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SMPE.@ACTION.REMOVECSI)   ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(SYSREG)                   ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(METHOD.@DISPLAY)          ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(DEPLOY.@SELF)             ACCESS(READ)
TSS PERMIT(MSMPRF3) CAMSM(CONFIG.@ACTION.IMPL)      ACCESS(READ)
```

ユーザへのセキュリティ プロファイルのアタッチ

ユーザにセキュリティ プロファイルをアタッチし、さまざまなロールの CA CSM アクションへのアクセス権をユーザに付与します。

ユーザにセキュリティ プロファイルをアタッチするには、たとえば以下のような TSO の CA Top Secret for z/OS コマンドを発行します。

```
TSS ADDTO(MSMUSR1) PROFILE(MSMPRF1)
TSS ADDTO(MSMUSR2) PROFILE(MSMPRF2)
TSS ADDTO(MSMUSR3) PROFILE(MSMPRF3)
```

この例では、以下の設定をセットアップします。

- MSMPRF1 プロファイルは、ユーザ MSMUSR1 にアクセス権を許可します。
- MSMPRF2 プロファイルは、ユーザ MSMUSR2 にアクセス権を許可します。
- MSMPRF3 プロファイルは、ユーザ MSMUSR3 にアクセス権を許可します。

IBM RACF でのユーザ セキュリティのセットアップ

CA CSM はリソース プロファイル (P. 279)を使用し、Web ベース インターフェースのリソースへのアクセス権を付与するために リソース クラスは CAMSM です。 IBM RACF では、さまざまなロールに対する適切なリソース プロファイルを含んだグループ プロファイルを定義し、ユーザをそのグループ プロファイルに結び付けることができます。

注: CAMSM は SAF リソース クラスのデフォルトの名前です。 お使いのシステムでは、CA CSM のインストールに応じて (P. 62)別の名前が使用される場合があります。

以下の手順に従います。

1. お使いのセキュリティ製品で CAMSM リソース クラスを定義します。

   CAMSM リソース クラスが定義されます。

2. グループ プロファイルを定義し、ロールを設定します。

   さまざまなロールのプロファイルにユーザを結びつけることができます。

3. ユーザをプロファイルに結びつけます。

   ユーザはさまざまなロールに対してセキュリティ保護されます。

詳細情報:

IBM RACF での SCS アドレス空間セキュリティのセットアップ (P. 191)
IBM RACF PassTicket の例 (P. 197)

IBM RACF での CAMSM リソース クラスの定義

CA CSM リソース プロファイルを使用する前に、お使いのセキュリティ製品へのプロファイルを含んだ CAMSM クラスを定義します。

注: CAMSM は SAF リソース クラスのデフォルトの名前です。 お使いのシステムでは、CA CSM のインストールに応じて (P. 62)別の名前が使用される場合があります。

以下の手順に従います。

1. STEROPTS LIST コマンドを発行して、エントリの CLASSACT および RACLIST の両方のリストに CDT リソースが表示されることを確認します。
2. 以下のコマンドを発行して、汎用プロファイルを定義します。

   ```
   RDEFINE CDT CAMSM UACC(NONE) CDTINFO(GENERIC,MAXLENGTH(246) POSIT(nnn)
   OTHER(ALPHA,NATIONAL,NUMERIC,SPECIAL) RACLIST(ALLOWED))
   ```

   nnn

   IBM の予約値と重複しない POSIT 番号を定義します。

   注: POSIT 番号の詳細については、「*IBM Server RACF Command Language Reference*」を参照してください。

   汎用プロファイルが定義されます。
3. 以下のコマンドを発行し、変更を確定します。

   ```
   SETROPTS RACLIST(CDT) REFRESH
   SETROPTS GENERIC(CAMSM) RACLIST(CAMSM) CLASSACT(CAMSM)
   ```

   変更が有効になり、CAMSM リソース クラスが IBM RACF に定義されます。

グループ プロファイルの定義

注: リソース プロファイル (P. 279)を使用して、CA CSM へのアクセスを拒否または許可します。

以下の例では、さまざまなロールのグループ プロファイルを定義します。

例: 管理者

すべてのアクションへのアクセス権を付与するプロファイル MSMPRF1 を定義します。 アクションには、システム設定の管理、システム レジストリ、方法、展開、設定、およびユーザ設定などがあります。

以下の IBM RACF コマンドを発行します。

```
ADDGROUP MSMPRF1 DATA( 'CA CSM ADMIN' )

RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.* UACC(NONE)
RDEFINE CAMSM SC.* UACC(NONE)
RDEFINE CAMSM SMPE.* UACC(NONE)
RDEFINE CAMSM SYSREG.* UACC(NONE)
RDEFINE CAMSM METHOD.* UACC(NONE)
RDEFINE CAMSM DEPLOY.* UACC(NONE)
RDEFINE CAMSM CONFIG.* UACC(NONE)
RDEFINE CAMSM TM.* UACC(NONE)


PERMIT LOGON CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT ADMIN.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SC.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SMPE.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT SYSREG.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT METHOD.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT DEPLOY.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT CONFIG.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
PERMIT TM.* CLASS(CAMSM) ID(MSMPRF1) ACCESS(READ)
```

例: ユーザ

すべてのユーザ アクションへのアクセス権を付与するプロファイル MSMPRF2 を定義します。ただし、ユーザがアクセスできるのは、環境内の SANDBOX システムのみです。 このプロファイルを持つユーザは、システムまたは他のユーザの設定の管理、システム レジストリの変更、または方法の作成を行うことはできません。 ユーザは、SANDBOX システムをターゲットとした展開を作成でき、他の CA CSM ユーザが定義した方法を使用できます。 ユーザは、定義済みシステム プロファイルの値を使用して SANDBOX リモート システムをターゲットとした設定を作成できますが、それらの設定を実行することはできません。

以下の IBM RACF コマンドを発行します。

```
ADDGROUP MSMPRF2 DATA(‘CA CSM USER’)

RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.SETTINGS.USER.* UACC(NONE)
RDEFINE CAMSM ADMIN.LMPKEY.* UACC(NONE)
RDEFINE CAMSM SC.@ACTION.* UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.* UACC(NONE)
RDEFINE CAMSM SYSREG.@DISPLAY UACC(NONE)
RDEFINE CAMSM SYSREG.@PROFILE.DISPLAY UACC(NONE)
RDEFINE CAMSM SYSREG.@SYSTEM.SANDBOX UACC(NONE)
RDEFINE CAMSM METHOD.@DISPLAY UACC(NONE)
RDEFINE CAMSM DEPLOY.* UACC(NONE)
RDEFINE CAMSM CONFIG.@DISPLAY UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.CREATE UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.REMOVE UACC(NONE)

PERMIT LOGON CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT ADMIN.SETTINGS.USER.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT ADMIN.LMPKEY.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SC.@ACTION.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SMPE.@ACTION.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SYSREG.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT SYSREG.@PROFILE.DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT METHOD.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT DEPLOY.* CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@DISPLAY CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@ACTION.CREATE CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
PERMIT CONFIG.@ACTION.REMOVE CLASS(CAMSM) ID(MSMPRF2) ACCESS(READ)
```

例: 制限されたユーザ

以下のアクションのみへのアクセス権を付与するプロファイル MSMPRF3 を定義します。

- 製品パッケージのダウンロード。
- CA CSM 以外でダウンロードされた製品パッケージのインストール。
- 既存の SMP/E 環境の CA CSM への移行。
- CA CSM からの SMP/E 環境のナレッジの削除。
- 展開の作成と、それらの展開（それらが所有者である場合）。
- プロファイル情報をはじめとする、システム レジストリ内のリモート システムの作成とメンテナンス。
- リモート システム上に準備された設定の実行。

以下の IBM RACF コマンドを発行します。

```
ADDGROUP MSMPRF3 DATA( 'CA CSM SMPE' )

RDEFINE CAMSM LOGON UACC(NONE)
RDEFINE CAMSM ADMIN.SETTINGS.USER.* UACC(NONE)
RDEFINE CAMSM SC.@ACTION.INSTPKG UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.MIGRATE UACC(NONE)
RDEFINE CAMSM SMPE.@ACTION.REMOVECSI UACC(NONE)
RDEFINE CAMSM DEPLOY.@SELF UACC(NONE)
RDEFINE CAMSM SYSREG.* UACC(NONE)
RDEFINE CAMSM METHOD.@DISPLAY UACC(NONE)
RDEFINE CAMSM CONFIG.@ACTION.IMPL UACC(NONE)

PERMIT LOGON CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT ADMIN.SETTINGS.USER.* CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SC.@ACTION.INSTPKG CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SMPE.@ACTION.MIGRATE CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SMPE.@ACTION.REMOVECSI CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT DEPLOY.@SELF CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT SYSREG.* CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT METHOD.@DISPLAY CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
PERMIT CONFIG.@ACTION.IMPL CLASS(CAMSM) ID(MSMPRF3) ACCESS(READ)
```

ユーザのグループ プロファイルへの結合

ユーザをグループ プロファイルに結びつけ、さまざまなロールの CA CSM アクションへのアクセス権をユーザに付与します。

ユーザをグループ プロファイルに結びつけるには、たとえば以下のように TSO で IBM RACF コマンドを発行します。

```
CONNECT MSMUSR1 GROUP(MSMPRF1)
CONNECT MSMUSR2 GROUP(MSMPRF2)
CONNECT MSMUSR3 GROUP(MSMPRF3)
```

この例では、以下の設定をセットアップします。

- MSMPRF1 プロファイルは、ユーザ MSMUSR1 にアクセス権を許可します。
- MSMPRF2 プロファイルは、ユーザ MSMUSR2 にアクセス権を許可します。
- MSMPRF3 プロファイルは、ユーザ MSMUSR3 にアクセス権を許可します。

ターゲット システムでのセキュリティのセットアップ

このセクションのトピックでは、ターゲット システム上で CA CSM 用のセキュリティをセットアップする方法について説明します。

詳細:

SCS アドレス空間セキュリティのセットアップ (P. 188)

SDS アクセス用の権限および許可

システム管理者は、利便性の向上のために、これらの要件を満たす必要があります。 CA CSM ホストはユーザ認証情報を基にして、出力を取得し削除する必要があります。したがって、読み取りおよび書き込み権限が必要です。

Software Deployment Service（SDS）および CA Common Services には、以下の領域でターゲット システムを使用しアクセスするための読み取りおよび書き込みアクセス権が必要です。

- リモート SDS はスクラッチ パッドとして SMP Work Directory（SMPDIRWK）を使用します。 PROC CCISPNSV を使用する GIMUNZIP と SDS は、スクラッチ パッドを使用します。許可を設定して、読み取り、書き込み、削除、実行に関して、ユーザに適切なアクセス権限を与える必要があります。 所有者の UID および GID は、展開ユーザにその作業ディレクトリ内で読み取り、書き込み、実行する許可を与えることができる必要があります。

  注: Started Task Class（STC）のみ、読み取りアクセス権が必要です。ユーザには読み取りおよび書き込みアクセス権が必要です。

- FTP およびランディング ディレクトリは、ターゲット システムの CA CSM 展開リモート サービスからアクセス可能で、アクセス許可はユーザ認証情報を基にしています。

  注: ユーザには読み取りおよび書き込みアクセス権が必要です。

- CCISPNSV スターティッド タスクに関連付けられたセキュリティ ID には、有効な OMVS セグメントが必要です。 CCISPNSV は、ターゲット システムのセキュリティ コンテキストで展開にユーティリティ機能を実行するタスクをアタッチします。

- マウント ポイントはディレクトリ パスで、そのパスには書き込み許可があり、またそのパスはターゲット システムに存在する必要があります。展開を実行するユーザ ID は、このディレクトリに対する書き込み許可を持っている必要があります。

  展開ユーザ ID は、マウント ディレクトリに対する書き込み許可を持っている必要があります。 展開ユーザ ID は、ターゲット システムで権限を付与されたマウントを持っている必要があります。

  注: マウント ユーザは UID(0) か、少なくとも、UNIXPRIV クラスで見つかる SUPERUSER.FILESYS.MOUNT リソースへの READ アクセス権を持っている必要があります。

リモート システム展開セキュリティ要件

SDS は、SMP/E GIMZIP プログラムに依存しています。展開操作を実行する場合、ユーザには CA CSM 実行中システムの GIM.PGM.GIMZIP SAF 機能クラス リソースへの READ アクセス権が必要です。 また、ユーザには CA CSM リモート システムの GIM.PGM.GIMUNZIP SAF 機能クラス リソースへの READ アクセス権が必要です。

SAF CSFSERV（Cryptographic Services Facility）クラスを使用している場合、CSFSERV クラス プロファイルの CSFOWH（READ 権限）を使用して、アクセス許可を設定する必要があります。 SMP/E GIMUNZIP は CSFSERV クラス プロファイルを使用し、サイトでの完全なデータ整合性を保証するための SHA-1 ハッシュ検証を実行します。

USS パーツおよび SUPERUSER 権限を使用した展開

ユーザが USS パーツを使用して展開をターゲット システムに作成し、UID に SUPERUSER 権限がある場合、GIMUNZIP は非 SUPERUSER の権限に対するものとは異なる方法で動作します。

注: CA CSM は CA CSM で定義する認証情報を使用し、Software Deployment Service（SDS）をターゲット システム上で作成します。

SUPERUSER 権限を使用した GIMUNZIP

UID に SUPERUSER 権限があるとき、GIMUNZIP は ROOT ユーザとして実行されます。GIMUNZIP が ROOT として作成するディレクトリにはすべて、ROOT の UID および GID があります。

展開の USS パーツ（所有者および許可）は、想定とは異なる可能性があります。ディレクトリ レベルで作成される USS アイテムを確認してください。必要に応じて SUPERUSER モードに切り替え、ターゲット システム上の USS パーツの結果にアクセスします。 展開済み製品のドキュメントや組織のガイドラインを使用し、所有者の UID および GID と許可を、必要に応じてリセットします。

SUPERUSER 権限を使用しない GIMUNZIP

GIMUNZIP は、常に ROOT に切り替わろうとします。切り替わることができない場合、GIMUNZIP は SMPOUT に情報メッセージを発行し、ユーザの UID および GID で稼働し続けます。

リモート展開サービス USS の考慮事項

Software Deployment Service（SDS）は z/OS UNIX のバッチ プログラムとして実行されます。 システムの CEEOPTXX メンバに MSGFILE（SYSPRINT）がある場合、MSGFILE を MSGFILE（SYSOUT,FBA,121,0,NOENQ）にオーバーライドするために、CCISPNSV 内の CEEOPTS DD が必要になります。 MSGFILE（SYSOUT,FBA,121,0,NOENQ）は、デフォルトで非 CICS です。

SCS アドレス空間アクセス用の権限および許可

特定のタスクを実行し、システムで実行されている SCS アドレス空間 (P. 181)を取得します。 SCS アドレス空間セキュリティ セットアップは、CA CSM 実行システムを含むすべてのターゲット システム上で実行されます。

CA CSM 関連セキュリティ ID - OMVS セグメントおよびホーム ディレクトリ

msmserv USS ディレクトリ パスが利用できない場合、CA CSM は稼働しません。 このホーム ディレクトリ パスを使用して、ユーザ ID をアプリケーション アドレス空間へ割り当てます。 この手順は、CA CSM が USS システムまたは別のアプリケーション ファイル システムをいっぱいにしてしまう可能性を防ぎます。 このアクションにより、CA CSM がその使用に割り当てられたファイル システムと確実に分離されます。

定義済みの有効な OMVS セグメントを持つユーザ ID は、CA CSM アドレス空間に割り当てられる必要があります。 この OMVS セグメントには、有効なホーム ディレクトリが定義される必要があります。 ユーザ ID を msmserv ディレクトリ用の USS パスのホーム ディレクトリに割り当てることをお勧めします。 デフォルトの USS ディレクトリ パスが使用される場合、このパスは /u/users/msmserv です。

注: 詳細については、お使いのセキュリティ製品についての、ユーザ ドキュメントを参照してください。

USS パスの設定

注: zFS ファイル システムの使用をお勧めします。 HFS ファイル システムから zFS ファイル システムに移行する方法の詳細については、最新の「*IBM z/OS Migration*」を参照してください。

ファイル システムを定義し、MOUNT ステートメントを使用して、SYS1.PARMLIB（BPXPRM*xx*）メンバのシステムの初期化でマウントすることができます。MSMSetup プロセスの一部として、SETUID オプションを持つファイル システムを指定します。

詳細:

USS ファイル システム (P. 262)

USS パス

CA CSM では、ダウンロード、インストールとセットアップ、および一般的な用途で HFS ファイル システムまたは zFS ファイル システムを使用できます。

注: zFS ファイル システムの使用をお勧めします。 HFS ファイル システムから zFS ファイル システムに移行する方法の詳細については、最新の「*IBM z/OS Migration*」を参照してください。

CA CSM をダウンロードしてインストールする前に、USS 管理者はこれらのファイル用のディレクトリ パスをセットアップする必要があります。 簡単なセットアップは、既存のファイル システムに 775 の許可を持つ 4 つの以下のようなディレクトリを作成することです。

/parent_path/msmserv/mpm
/parent_path/msmserv/*version_number*/msm
/parent_path/msmserv/*version_number*/msmruntime
/parent_path/msmserv/*version_number*/msminstall

ここで、「*parent_path*」は、以下のような、ユーザのサイトでプライマリ マウント ポイントまたはディレクトリとして定義された CA CSM 親パス名です。

/u/users/msmserv
/usr/lpp/msmserv
/cai/msmserv

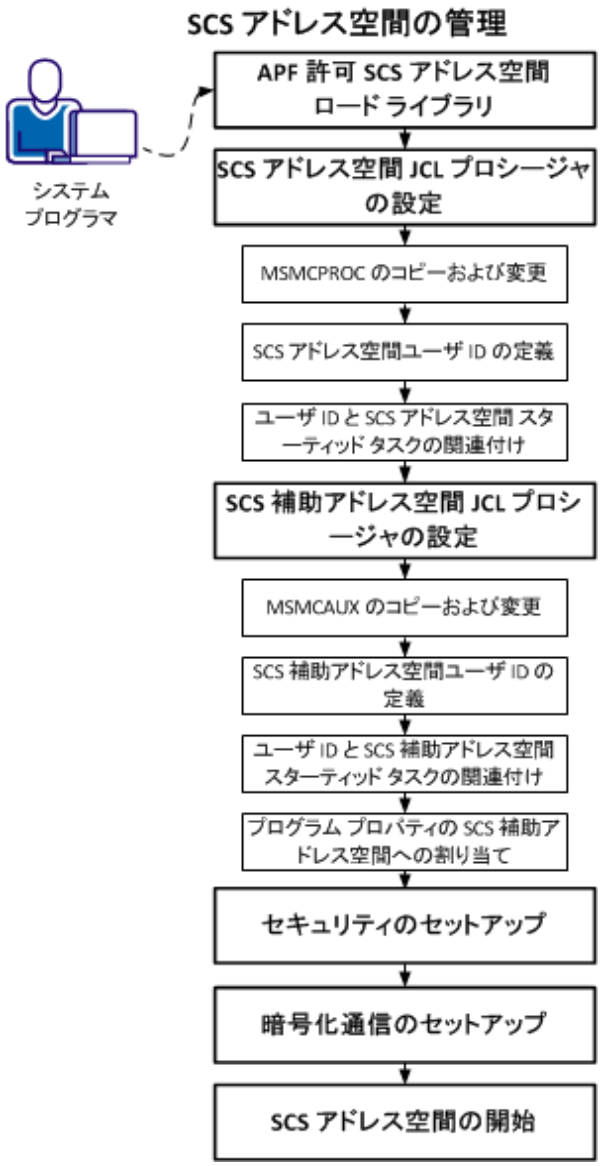
注: 親パスの最後の部分に /msmserv を使用することをお勧めしますが、ユーザ サイトの基準に応じて変更することもできます。

必要なスペースは 2500 シリンダです。

/u/users/msmserv/mpm は特別なパスで、CA CSM がスタートアップ中に割り当ててマウントするファイル システムのマウント ポイントとして機能します。

SCS アドレス空間の設定

以下のタスクを実行し、SCS アドレス空間をユーザの環境で実行します。



1. SCS アドレス空間ロード ライブラリに対して APF 許可します (P. 183)。
2. SCS アドレス空間 JCL プロシージャを設定します (P. 184)。
   a. MSMCPROC (P. 330) をシステム PROCLIB にコピーし、インストール環境に合わせて修正します。
   b. SCS アドレス空間用のユーザ ID を定義します。
   c. セキュリティ システムを使用して、ユーザ ID と SCS アドレス空間のスターティッド タスクを関連付けます。 SCS アドレス空間をスターティッド タスクとして開始している場合は、この手順を実行します。
3. SCS 補助アドレス空間 JCL プロシージャを設定します (P. 186)。
   a. MSMCAUX (P. 330) をシステム PROCLIB にコピーし､インストール環境に合うように修正します。
   b. SCS 補助アドレス空間用のユーザ ID (P. 187) を定義します。
   c. セキュリティ システムを使用して、ユーザ ID と SCS 補助アドレス空間スターティッド タスクを関連付けます。
   d. 特殊プログラム プロパティ (P. 187)を SCS 補助アドレス空間に割り当てます。
4. セキュリティをセットアップします (P. 188)。
5. 暗号化通信をセットアップします (P. 200)。
6. SCS アドレス空間を開始します (P. 208)。

第 3 章: CA CSM のインストールとセットアップ

このセクションには、以下のトピックが含まれています。

CA CSM ファイルのダウンロードと解凍

圧縮された CA CSM 製品パッケージは CA サポート Online Web サイトから入手できます。 CA CSM をインストールする前に、Prerequisite Validator ユーティリティ (P. 38)をダウンロードして実行します。

注: Prerequisite Validator は CA サポート Online Web サイトでも取得できます。 Prerequisite Validator および関連する情報を個別にダウンロードできます。

Prerequisite Validator ユーティリティを正常に実行した後、CA サポート Online Web サイトに戻り、完全な CA CSM パッケージをダウンロードできます。 その後、CA CSM をインストールできるようになります。

以下の手順に従います。

1. CA サポート Online Web サイトで［Download Center］に移動します。
2. ［Select a Product］フィールドに CA Chorus Software Manager を入力し、最新のバージョンを選択して［Select all components］チェック ボックスをオンにし、［Go］をクリックします。

   注: 製品リストに CA Chorus Software Manager が見つからない場合は、製品ページ上部の［Free Service］エリアに記載されている指示に従ってください。

   製品ダウンロードの一覧が表示されます。
3. ソフトウェア パッケージをダウンロードします。

ソフトウェア パッケージをダウンロードした後、インストール用のファイルを解凍し展開します。

重要: 解凍した CA CSM パッケージが、作業ボリュームや一時ボリュームではなく、恒久ストレージ ボリュームに格納されていることを確認してください。

以下の手順に従います。

1. CA CSM パッケージがダウンロードされたディレクトリに移動し、以下のコマンドを入力してパッケージを解凍します。

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   注: Z サフィックスを含む完全な pax ファイル名では、大文字と小文字が区別されます。 pax コマンドを発行するシステムでは、ファイル名に大文字や小文字が正確に使用されていることを確認してください。必要に応じて、ファイル名を変更します。

   MSMInstaller ディレクトリが作成され、パッケージはそのディレクトリ内に解凍されます。
2. サイトのデータ セットおよび USS ディレクトリの命名基準に適合するように、MSMInstaller ディレクトリの UNZIPJCL ファイルをカスタマイズします。 ジョブをサブミットして（たとえば、USS OMVS の z/OS シェル コマンドのサブミットを使用して）、正常に完了したことを出力で確認します。

   UNZIPJCL ジョブは、CA CSM インストール ファイルを格納する MSMSetup ディレクトリおよび MSMProduct ディレクトリを作成します。

- 以下のテキストを、MSMInstaller ディレクトリが作成された場所のパスで置換します。

  ```
  <-- YOUR USS HFS DIRECTORY -->
  ```

- 以下のテキストを、MSMSetup ディレクトリと MSMProduct ディレクトリを作成する場所のパスで置換します。

  ```
  <-- YOUR CA CSM USS HFS DIRECTORY -->
  ```

  注: <-- YOUR USS HFS DIRECTORY --> ディレクトリと <-- YOURCA CSM USS HFS DIRECTORY --> ディレクトリには、同じパスを設定することをお勧めします。

- **yourHLQ** を ISPF UI Tool データ セット用の高レベル修飾子で置換します。 高レベル修飾子の長さは、26 文字以下にする必要があります。

MSMSetup ディレクトリ、MSMProduct ディレクトリおよび CA CSM Installation ISPF UI ツール z/OS データ セットが作成され、CA CSM ファイルが展開されます。

注: UNZIPJCL ファイルを開くとき、警告メッセージが画面の一番下に表示されることがあります。 このメッセージは、末尾の空白がすべて UNZIPJCL ファイルから削除されることを示します。 末尾の空白を削除しても保持しても、ジョブの実行は影響を受けません。 このメッセージは無視してもかまいません。

インストールとセットアップ オプションの指定

CA CSM ファイルを展開したディレクトリ（…/MSMSetup）には、MSMSetupOptionsFile.properties オプション ファイルが格納されています。CA CSM セットアップ ユーティリティはこのファイルのコンテンツを使用し、CA CSM のインストールおよびセットアップ プロセスをカスタマイズします。 ファイルには設定済みの値が含まれています。 このファイルのコンテンツをカスタマイズし、ユーザの要件を反映させます。各オプションを以下の形式で指定します。

option_keyword=value

インストールとセットアップのオプションを手動で指定するには、EBCDIC 文字セット対応のテキスト エディタを使用して、オプション (P. 240)の確認とカスタマイズを行います。 たとえば、Interactive System Productivity Facility（ISPF）を使用します。 必要に応じて、サイトで他のチーム メンバと相談して値を収集します。

すでに CA CSM を使用している場合、USS シェル ユーティリティを実行して、以前のバージョンのオプション ファイルから現在のオプション ファイルに値をコピーする (P. 101)ことができます。

また、CA CSM Installation ISPF UI Tool (P. 90) を使用することもできます。このツールにより、サイトの値を取集し、ほとんどのオプション ファイル パラメータに事前入力することができます。必要に応じ、サイトのチーム メンバに依頼し、これらの事前入力された値を確認してください。

注: サイトで Storage Management Subsystem（SMS）の自動クラス選択 （ACS）を使用している場合、ACS はオプション ファイルのストレージ パラメータ値をオーバーライドします。

詳細:

オプション ファイル キーワード (P. 240)

ISPF UI ツールを使用したオプションの自動指定

CA CSM Installation ISPF UI Tool を使用し、オプションを自動的に指定することができます。 このツールにより、以下のタスクが実行できます。

- 大部分のパラメータに対するサイトの値の収集
- JCL を使用して必要な USS ファイル システムを作成し、CA CSM をインストールする前にこのオプション ファイルを編集する。

3270 エミュレータは、35 行までの ISPF ダイアログ ボックスがサポート可能である必要があります。

注: ISPF コマンド 来院をダイアログ ボックスの一番下に表示する設定が有効な場合、ISPF UI Tool で一部の ISPF ダイアログ ボックスが正しく表示されない場合があります。 その結果として、オプションが ISPF ダイアログ ボックスの一番下の、他のオプションとは違う場所に表示される場合があります。 こうした状況を回避するには、ISPF UI Tool を終了し、一時的にこのオプションを無効にしてから、UI Tool を起動します。 このオプションは、後で再度有効にできます。

以下の手順に従います。

1. TSO/ISPF オプション 6 に移動し、以下のコマンドを実行します。

   ```
   exec 'data_set_name(#RUNTOOL)'
   ```

   data_set_name

   UNZIPJCL を使用して展開した CA CSM Installation ISPF UI Tool z/OS データ セットの名前を定義します。

   例： CAI.MF20.MSMI.UITOOL

   メインの ISPF パネルが表示されます。

2. 1 を入力し、オプション ファイル パラメータに事前入力するためのサイトの値を収集します。

   Java のホーム パスおよび MSMSetup ディレクトリのパスを入力するように求めるプロンプトが表示されます。

   USS MSMSetup フォルダにあるプログラムはこのインターフェースから実行され、いくつかのパラメータに対するサイトの値を収集します。収集された値は、XML ファイルに保存されます。 このファイルを使用してオプション ファイル クエリを事前入力し、より簡単により速く CA CSM インストール オプション ファイルの編集を行うことができます。

3. 6 または 7 を入力し、オプション ファイルを編集します。

   このグループ内のオプションにより、サイトで収集した値でオプション ファイルを事前入力する、または ISPF エディタを使用して TSO からオプション ファイルを直接編集することができます。

事前入力されたサイトの値の使用

このオプション（オプション 6）を使用し、すべてのインストール オプション パラメータおよびそれらの事前入力された値を確認します。 値はすでにインストール セットにデフォルトで含まれており、編集と確認が簡素化されます。

- S から始まる値は、収集されたサイトの値を示します。
- D から始まる値は、製品のデフォルト値を示します。
- U から始まる値は、値が編集されたことを示します。

各パラメータの前に「**/**」を入力し、利用可能な値（S/D/U）を表示します。それらの値を選択して修正することもできます。

パラメータが複数のページに一覧表示されます。 すべてのパラメータを編集し確認した後に、前（Enter キーを押す）、後（PF3 キーを押す）に移動し、各画面を確認します。

ISPF UI ツールを使用して、すべてのパネルを編集し、確認します。その後ツールは、パスとコマンドを表示し、インストール スクリプトを呼び出します。

ISPF エディタの使用

このオプション（オプション 7）を使用し、TSO/ISPF から ISPF エディタを使用して、オプション ファイルを手動で編集します。

CA CSM インストーラが呼び出された後、パラメータの検証が失敗する場合、再度オプション ファイルを編集します。

CA CSM のインストールおよびセットアップ

CA CSM ファイルを展開するディレクトリ（.../MSMSetup）には、CA CSM をインストールおよびセットアップする MSMSetup.sh セットアップ ユーティリティが格納されています。

注: CA CSM は SMP/E がインストール済みで、使用できる状態の製品です。

このユーティリティは、オプション ファイルのコンテンツを使用して、全体の処理をカスタマイズします。このユーティリティは、Apache Tomcat アプリケーション サーバ、CA Datacom/MSM データベース、CA CSM サービス コンポーネント、Web ベース インターフェースをセットアップします。 このユーティリティは、CA CSM 用のランタイム環境を作成し、セットアップします。

ユーザが既存の CA CSM の顧客である場合、ユーティリティは新しい環境をセットアップします。 ユーティリティは、オプション ファイルの値に従って、旧バージョンのデータベースの移行も行います。

このユーティリティには、以前実行に失敗した後に再度呼び出された際に、インストールを続行するための再開メカニズムがあります。 このユーティリティでは、以前失敗した実行の最初からのインストールを選択することもできます。 再開モード中に、オプション ファイルのパラメータのいずれかが完了した手順に影響する場合、このユーティリティは強制的に最初からのインストールを開始します。

処理の始めに、ユーティリティはオプション パラメータに設定された値のデータ セットと USS フォルダが存在するかどうかをチェックします。それらが存在する場合、ユーティリティは前回のインストール ファイルに上書きするか、または上書きせずに処理を続行するかを尋ねるプロンプトを表示します。

ユーティリティは、オプション ファイルから渡されるポート番号が使用できるかどうかを確認します。 ポート番号が予約済みか、すでに使用中か、または他の理由で使用できない場合、ユーティリティは指定された値を使用してインストールを続行するかどうかを確認するプロンプトを表示します。

以下の情報を考慮します。

- CA CSM のインストールを開始する前に、TSO リージョン サイズが少なくとも 143360 KB であることを確認してください。
- MSMSetup.sh スクリプトを、TSO OMVS 環境（ネイティブの USS コマンド プロンプト）から直接呼び出します。
- z/OS Telnet セッションまたは ISHELL コマンド シェルから、MSMSetup.sh ユーティリティを呼び出すことはできません。
- MSMSetup.sh には、UID(0) または SUPERUSER 権限を持った userid が必要です。
- サイトに SMS ACS ルールがあり、POU から PDSE への変更を強制される場合、これらの設定によりインストール ジョブ CSMN5102（新規インストール用）または CSMU*xx*02（アップグレード用）が失敗します。MSMSetup.sh には、PDS データ セットとして作成される POU データ セットが必要です。
- JCL スペース割り当てを調整 (P. 165) する場合は、CA CSM インストーラを Manual モードまたは Review インストール モードで実行します。

以下の手順に従います。

1. ダウンロードした CA CSM パッケージからファイルを展開したこと (P. 87) を確認してください。

   MSMSetup および MSMProduct ディレクトリが存在し、CA CSM ファイルはそれらのディレクトリに展開されます。

2. MSMSetupOptionsFile.properties オプション ファイル (P. 240) を編集し、ファイルがサイトの要件に確実に一致するようにします。
   - すでに CA CSM を使用している場合、USS シェル ユーティリティを実行して、以前のバージョンのオプション ファイルから現在のオプション ファイルに値をコピーする (P. 101) ことができます。
   - アップグレード用 CA CSM のオプションの設定により、新しいバージョンへ現行のデータベースを移行します (P. 103)。
3. 必須 USS パス (P. 82) が利用可能であることを確認します。
4. userid に UID(0) を使用していることを確認します。そうでない場合は、su コマンドを発行して、UID(0) に切り替えます。

5. MSMSetup.sh セットアップ ユーティリティがあるディレクトリに移動し、たとえば OMVS から以下のようにユーティリティを実行します。

   ```
   sh MSMSetup.sh
   ```

   このユーティリティは、以下の存在を確認します。

   - 現在のパス内の MSMSetupOptionsFile.properties ファイル。
   - オプション ファイル内の有効な JAVAPATH パラメータ フィールド。
   - サポートされているバージョンの Java SDK がインストールされていること。

   注: セットアップ ユーティリティは対話型で、セットアップが完了するまでユーザの入力が要求されます。 出力は、MsminstallerLog*yyyy-mm-dd*,*hh-mm-ss*,*ttt*.log の形式で、MSMSetup ディレクトリのログ ファイルに書き込まれます。失敗した後にユーティリティを再実行する場合、ユーティリティは前回の実行に対して必要なクリーンアップ手順を実行します。

   ユーティリティに関する情報を示すパネルが表示されます。 その後、使用許諾契約の画面が表示されます。

   この使用許諾契約には、CA Technologies による製品取得アクティビティに関連する最小限の情報収集を可能にする許諾契約が含まれています。 この情報には、CA サポート Online Web サイトのサイト ID、製品、ユーザ ID などがあります。 サイトのアクセス ルールにより、これらの情報の収集を目的として確立された FTP 接続が拒否されることがあり、あるいはその他の理由により接続が確立できないことがあります。 その後も、CA CSM は引き続き稼働します。

   注: CA CSM の最新のバージョンに移行している場合は、CA CSM の旧バージョンがこの移行中に実行されていないことを確認してください。

6. 使用許諾契約を確認し、PF3 キーを押します。

   この契約への同意を促すメッセージが表示されます。

   注: 使用許諾契約が表示されない場合は、TSO OMVS ライブラリがユーザの TSO 環境に割り当てられていることを確認してください。

7. 「**Y**」と入力して、契約に同意します。

   （非 UID(0) のインストールのみ） UID(0) が割り当てられていない userid でインストーラ スクリプトを実行している場合、インストーラをすぐに停止して UID(0) が割り当てられている userid に切り替えるかどうかを確認するメッセージが表示されます。

注: UID が 0 以外の userid で実行するとエラーが発生する場合がありますが、ファイルはコピーされ、ファイルの属性と許可は修正されます。 これらのエラーは通常、その*操作が許可されていない*ことを示します。通常、インストーラ スクリプトはこのタイプのエラーを検知し、その結果、途中で失敗して終了します。 ほとんどの場合、UID(0) が割り当てられた userid でインストーラ スクリプトを再開すると、インストールは正常に再開し、完了します。

ただし、このタイプのエラーが検知されない場合があります。 そのような場合、インストーラ スクリプトを正常に再開するのは非常に困難です。解凍したファイル、インストールしたファイルをすべて削除し、最初からインストールをやり直す必要があります。

8. （非 UID(0) のインストールのみ） プロンプトの表示に応じ、Y（Yes）または N（No）を入力します。インストーラ スクリプトのプロンプトの表示に N（No）を入力してインストールを停止し、UID(0) が割り当てられた userid に切り替えることを強くお勧めします。 これは、スーパーユーザ モードで実行して行います。 スーパーユーザ モードで実行するには、OMVS コマンド プロンプトで su コマンドを発行し、次にインストーラ スクリプトを再実行します。

   Y（Yes）を入力すると、インストールは続行します。

9. ユーティリティをモニタし、システムおよびソフトウェアの前提条件が満たされていることを確認し、オプション ファイルの内容を検証します。

   （オプション）システムから取得した IP アドレスで接続できない場合は、バッチ ジョブを処理する FTP をサポートするホスト名または IP アドレスを指定します。

10. 以下のいずれかのインストール モードを指定して、CA CSM インストール ジョブを処理します。

    A

    Automatic モードでは、インストール ジョブはノンストップ モード（サブミットされたジョブがサブミット前に表示されない）で自動的にサブミットされます。

    R

    Review モードでは、サブミット前に各インストール ジョブの確認を促すプロンプトが表示されます。

    M

    Manual モードでは、セットアップ プロセスの後に各インストール ジョブを手動でサブミットします。

    注:

    - TSO を使用してインストール ジョブをサブミットする場合、インストーラは Manual モードでのみ実行されます。
    - インストーラは 17200 KB を超えるメモリを必要とする場合があります。
    - 以前に失敗したポイントの後で再起動した場合、以前に失敗したポイントから開始するか、または最初からインストールするかを選択するメッセージが表示されます。
    - インストール ジョブのサブミット用に FTP モードを選択していた場合、z/OS 認証情報の入力を促すメッセージが表示されます。

11. （FTP モードのみ）ユーザ ID を入力し、次にパスワードを入力します。

    ユーザ ID またはパスワードの入力が間違っていた場合、あと 2 回、認証情報を再入力することができます。 2 回目と 3 回目の試行の前に、Yes/No プロンプトが表示されます。

    Yes

    認証情報を再入力できます。

    No

    インストール手順を終了します。

    FTP 認証情報の検証が 3 回失敗すると、インストール プロセスは終了します。 この問題を解決したら、インストール スクリプトを再起動します。

このユーティリティは JOB ステートメント、JOBPARM ステートメント（JES2 環境の場合）、または確認および変更用の MAIN ステートメント（JES3 環境の場合）を表示します（必要な場合）。

12. Edit Job Card の質問に応じて、以下のいずれかの手順を実行します。
    - サイトに追加パラメータが必要ない場合は、「**N**」と入力します。インストールが続行します。
    - サイトに追加パラメータが必要な場合は、「**Y**」と入力します。JOB カードが編集モードで開きます。JOB カードを修正し、PF3 キーを押して変更を保存し、インストール プロセスを続行します。

      注: CA View がホスト システム上で実行されている場合は、以下のステートメントのコメントを解除します。次に、CA View のセットアップ時に SARINIT で使用された初期化パラメータに基づいて、それらのステートメントに入力します。
      - JOBCARD 内の OUTPUT ステートメント、SARPRT および JESPRT
      - SARPRT および JESPRT ステートメントの両方の CLASS オプション
13. ユーティリティをモニタし、すべての必須インストール ジョブがカスタマイズされていることを確認します。

    （オプション） Review インストール モードを選択した場合、インストール ジョブを 1 つずつ確認するように求めるプロンプトが表示されます。 ジョブを修正し、PF3 キーを押して変更を保存し、ジョブをサブミットします。
14. ユーティリティが CA CSM 用の SMP/E 環境を作成するのをモニタし、CA CSM コンポーネントをセットアップします。

    このユーティリティは以下の手順を実行します。
    - 以前に修正されたジョブを 1 つずつサブミットし、カスタマイズされた JCL をランタイム JCL PDS にコピーします。

      注: ジョブの実行が JobCompletionWaitMaxTime オプション ファイルのキーワードが指定する時間より長くかかる場合、ユーティリティはそのまま待機するかどうかを確認するメッセージを表示します。「**N**」と入力して、全インストール プロセスを終了します。
    - CA Datacom/MSM アドレス空間および接続プールを含む、CA Datacom/MSM 環境をカスタマイズします。

- server.xml および context.xml ファイル、ポート番号、接続プールおよびユーザ XML 設定などの Apache Tomcat 環境をカスタマイズします。
- ランタイム PROCLIB PDS 用の JCL をカスタマイズしてコピーします。
- ランタイム JCL PDS 用の JCL をカスタマイズしてコピーします。
- CAICCI インターフェース用の CA CSM を準備し、LIBCCI と LIBCCI6E モジュール、およびカスタマイズされたジョブ COPYCCI を、ランタイム JCL PDS メンバの COPYCCI にコピーします。 インストール プロセスの一環として COPYCCI ジョブを実行する必要はありません。 このジョブは、これらのモジュールを簡単に再ロードするために、必要に応じて提供されます。 たとえば、これらのモジュールがメンテナンス手順によって更新される場合、その更新を CA CSM ランタイムにコピーできます。

最後の手順が完了した後、ユーティリティはインストール サマリ レポート（MSMSummaryReport.txt）を表示します。 このレポートは MSMSetup ディレクトリに保存されます。このレポートには Web ブラウザから CA CSM にアクセスするのに必要な URL が記載されています。

セットアップ ユーティリティは処理を完了します。

15. サマリ レポート MSMSummaryReport.txt を確認し、CA CSM のインストール全体を完了するのに必要な、特定のインストール後ジョブをサブミットします。

    サマリ レポートで指定されているインストール ジョブ CSMN51*yy*（新規インストール (P. 104)を実行している場合）または CSMU*xxyy*（旧バージョンからアップグレードしている場合 (P. 106)）をサブミットします。 *xx* は、どのバージョンからアップグレードしているかのバージョン番号を示し、*yy* は、ジョブのシーケンス番号を示します。

    注: CA CSM インストーラが実行されているインストール モードにかかわらず、MSMSetup.sh の完了後に、インストール ジョブを手動でサブミットします。

16. JCL（MSMMUF）ジョブの STEPLIB 内の以下のライブラリが APF 許可されていることを確認します。
    - CAAXLOAD および CUSLIB CA Datacom/MSM ライブラリ
    - オプション ファイルの CCSdsn キーワードで指定される CA Common Services for z/OS ライブラリ

次回の IPL 実行後にもライブラリを APF 許可されたままにするには、そのライブラリを永続 APF リストに追加します。

注: オプション ファイルの AddAPFauthDSdyn キーワードの値が N の場合は、これらのライブラリを手動で APF 許可してください。

17. CA CSM アプリケーション サーバ（MSMTC ジョブまたはスターティッド タスク）に関連付けられたユーザ ID に、必要な USS アクセス権限があることを確認します。

    CA CSM ではファイル システムを作成してマウントできます。

18. ネットワーク設定が CA CSM に以下の Web サイトへのアクセスを許可していることを確認します。

    - supportservices.ca.com（HTTPS ポート番号 443 を使用）
    - ftp.ca.com（FTP ポート番号 21 を使用）
    - ftpca.ca.com（FTP ポート番号 21 を使用）

      注: CA CSM はこの FTP サーバを使用して、最小限の情報を収集します。 この情報には、CA サポート Online Web サイトのサイト ID、製品、ユーザ ID などがあります。サイトのアクセス ルールにより、これらの情報の収集を目的として確立された FTP 接続が拒否されることがあり、あるいはその他の理由により接続が確立できないことがあります。 その後も、CA CSM は引き続き稼働します。
    - scftpd.ca.com（FTP ポート番号 21 を使用）
    - ftpdownloads.ca.com（FTP ポート番号 21 を使用）
    - supportftp.ca.com（FTP ポート番号 21 を使用）
    - sdownloads.ca.com（HTTPS ポート番号 443 を使用）

      注: ［Settings］ページの［System Settings］-［Software Acquisition］で［Use HTTPS for Downloads］取得オプションを使用する場合、sdownloads.ca.com のみが必要です。ポート 80 とポート 443 の両方に対して ca.com ドメインを許可する場合、sdownloads.ca.com を許可する必要はありません。

    さらに、ネットワーク管理者は localhost のドメイン ネーム システム（DNS）エントリを定義する必要があります。

19. CA CSM を起動します (P. 114)。

    CA CSM が操作可能になります。

オプション ファイル キーワードのコピー

より容易で迅速なカスタマイズを行うため、以前のバージョンの CA CSM からキーワード値をコピーできます。

注: この手順は CA CSM の旧バージョンからアップグレードしているユーザのみを対象とし、またこれはオプションです。

以下の手順に従います。

1. MSMSetup.sh セットアップ ユーティリティが格納されているディレクトリに移動します。

   以下のいずれかの方法を使用して、旧バージョンの MSMPATH を検索することができます。

   - CA CSM Product Installed Path の旧バージョンのサマリ レポート（MSMSummaryReport.txt）の CA CSM Product Installed Path に指定されたパス
   - 旧バージョンの MSMSetup フォルダの MSMSetupOptionsFile.properties オプション ファイル内の MSMPATH キーワードに指定されたパス

2. ユーティリティを実行します。

   たとえば、以下のコマンドを使用して、USS OMVS からユーティリティを実行します。

   ```
   sh MSMSetup.sh copyOPT PreviousRelease.MSMPATH
   ```

   PreviousRelease.MSMPATH

   旧バージョンの CA CSM ターゲット ファイルがある場所のパスです。

   例： /u/users/msmserv/msm

   ユーティリティは、以下の場所で旧バージョンのオプション ファイルを探します。

   ```
   PreviousRelease.MSMPATH/CEGPHFS/MSMSetupOptionsFile.properties.
   ```

   このユーティリティは、利用可能なすべての値を旧バージョンのオプション ファイルから現在のオプション ファイルにコピーし、不足している対応するキーワードを設定します。

ユーティリティが完了すると、変更された MSMSetupOptionsFile.properties オプション ファイルが編集モードで表示されます。 サイトの要件に一致させるように、このファイルをカスタマイズできます。

重要: 旧バージョンのシステムに対するキーワード値と、旧バージョンの CA CSM ユーザ インターフェースのユーザ構成の設定を確認します。 移行中、オプション ファイルで指定された 2 つのキーワード（MVSHFSDsnPrefix および MountPath）は、旧バージョンと同じである必要があります。 他のすべてのシステムおよびユーザ設定のキーワードは、移行中に変更できます。

詳細:

オプション ファイル キーワード (P. 240)

データベースのアップグレード

注: このトピックは、CA CSM の旧バージョンからアップグレードしているユーザのみを対象としています。 セットアップ プロセスは移行ジョブを作成します。 ジョブは選択されたインストール モードに従って実行されます。

MSMSetupOptionsFile.properties オプション ファイルの PreviousRelease.MSMPATH オプション ファイル パラメータは、以前のアプリケーション インストール パスと同じ値で入力される必要があります。これを実施することで、移行ジョブが確実に自動生成されます。

旧バージョンから CA CSM を移行するとき、現行および以前の MSMSetupOptionsFile.properties の MVSHFSDsnPrefix および MountPath が、旧バージョンの CA CSM と同じ値であることを確認します。インストールの間、これらのパラメータが CA CSM のバージョン間で異なる場合、CA CSM インストーラは対応するプロパティに対するエラー メッセージを表示し、インストールを終了します。

注: 選択したインストール モードにかかわらず、2 つのインストール ジョブが実行されます。 最初のジョブは、旧インストール バージョンの CA CSM の CA Datacom/MSM データベース ファイルをバックアップし、2 番目のジョブは、CA CSM pax ファイルのコンテンツを解凍します。

以下のインストール モードをアップグレードの実行中に利用できます。

A

Automatic モードでは、インストール ジョブはノンストップ モード（サブミットされたジョブがサブミット前に表示されない）で自動的にサブミットされます。

R

Review モードでは、サブミット前に各インストール ジョブの確認を促すプロンプトが表示されます。

M

Manual モードでは、セットアップ プロセスの後に各インストール ジョブを手動でサブミットします。

インストール ジョブ

CA CSM セットアップ ユーティリティは、セットアップ プロセスの一部としてジョブをサブミットします。 CA CSM のコンテンツ（新規インストール用の CSMN5102 およびアップグレード用の CSMU*xx*02）を解凍するジョブは、インストール モードを問わず、デフォルトでセットアップ プロセスを使用してサブミットされます。 セットアップ プロセスは必要な設定を実行し、実行時パスを作成します。

注:

- インストール ジョブ CSMU*xx*01 は、既存のバージョンのデータをバックアップし、最新のバージョンに読み込むための変換データを準備します。 以前のバージョンの CA CSM からアップグレードする場合、インストール ジョブ CSMU*xx*01 は、すべてのインストール モードに対して最初にサブミットされます。Manual モードでは、スクリプトはインストール ジョブ CSMU*xx*01 および CSMU*xx*02 をサブミットします。
- Manual モードで実行している場合は、このセクションで示された順番でジョブをすべて実行します。

新規インストール用のインストール ジョブ

CA CSM の新規インストールを実行しているとき、以下のジョブが作成されます。

CSMN5101

このメンバは、アップグレード用のジョブ シーケンスと強制的に一致させるためのプレースホルダにすぎません。 これはジョブではなく、実行もできません。

CSMN5102（CA CSM 製品の解凍）

z/OS と USS コンテンツを解凍します。

CSMN5103（CA CSM SMP/E 環境のカスタマイズ）

SMP/E 環境データ セット UCLIN ステートメントを、オプション ファイルから提供されるサイト固有の値でカスタマイズします。

CSMN5104（CA Datacom/MSM データベース システム モジュールのアセンブルおよびリンクエディット）

CA Datacom/MSM システム ID モジュールを、オプション ファイルで提供されるサイト固有の値でアセンブルし、リンク エディットします。

CSMN5105（CA Datacom/MSM SVC のロード）

CAIRIM モジュールを実行し、CA Datacom/MSM SVC をロードします。

CSMN5106（CA Datacom/MSM データベース データ セットの割り当ておよびロード）

CA Datacom/MSM データベース データ セットを割り当ててロードします。

CSMN5107

このメンバは、アップグレード用のジョブ シーケンスと強制的に一致させるためのプレースホルダにすぎません。 これはジョブではなく、実行もできません。

CSMN5108（CA Datacom MUF の開始）

このジョブは CA Datacom/MSM MUF を開始します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。 ジョブ CSMN5108 は実行中のタスクです。 次のジョブをサブミットする前に、JES Active Queue を確認し、ジョブ CSMN5108 が実行中かどうかを判断します。

CSMN5109（新規にインストールされたデータベースのデータベース テーブルとバックアップの確認）

MSMDBSVS（CA Datacom/DB サーバ）および MSMTCSRV（Apache Tomcat）がアクティブではないことを確認します。

このジョブは CA Datacom/MSM データベース テーブルを確認し、最新の CA Datacom/MSM インストール データベースのバックアップを作成します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。

CSMN5110（CA Datacom MUF の停止）

このジョブは CA Datacom/MSM MUF を停止します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。

アップグレード用のインストール ジョブ

インストーラは、以下のルールに従って指定したインストールのタイプとインストール オプションに必要な、一意の JCL を生成します。

CSMU*xxyy*

xx

どのバージョンからアップグレードするかを示します.

yy

ジョブのシーケンス番号を表します。

たとえば、ユーザが CA MSM R4.1 からアップグレードしている場合、ジョブ番号は CSMU4101、CSMU4102、...、CSMU4110 になります。

現行の CA CSM データベースから最新バージョンの CA CSM へのアップグレードを実行している場合、以下のジョブが作成されます。

CSMU*xx*01（**既存の CA CSM データのバックアップ**）

既存の旧バージョンの CA Datacom/MSM データをバックアップします。

CSMU*xx*02（CA CSM **製品の解凍**）

z/OS と USS コンテンツを解凍します。

CSMU*xx*03（CA CSM SMP/E **環境のカスタマイズ**）

SMP/E 環境データ セット UCLIN ステートメントを、オプション ファイルから提供されるサイト固有の値でカスタマイズします。

CSMU*xx*04（CA Datacom/MSM **データベース システム モジュールのアセンブルおよびリンクエディット**）

CA Datacom/MSM システム ID モジュールを、オプション ファイルで提供されるサイト固有の値でアセンブルし、リンク エディットします。

CSMU*xx*05（CA Datacom/MSM SVC **のロード**）

CAIRIM モジュールを実行し、CA Datacom/MSM SVC をロードします。

CSMU*xx*06（CA Datacom/MSM **データベース データ セットの割り当ておよびロード**）

CA Datacom/MSM データベース データ セットを割り当ててロードします。

CSMU*xx*07（データ移行）

旧バージョンの CA Datacom/MSM データベースを最新のバージョンへ移行します。

CSMU*xx*08（CA Datacom MUF の開始）

このジョブは CA Datacom/MSM MUF を開始します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。ジョブ CSMU*xx*08 は実行中のタスクです。 次のジョブをサブミットする前に、JES Active Queue を確認し、ジョブ CSMU*xx*08 が実行中かどうかを判断します。

CSMU*xx*09（新規にインストールされたデータベースのデータベース テーブルとバックアップの確認）

MSMDBSVS（CA Datacom/DB サーバ）および MSMTCSRV（Apache Tomcat）がアクティブではないことを確認します。

このジョブはアップグレードしている CA CSM のバージョンに固有の要件と一致します。 すべてのバージョンにおいて、このジョブは CA Datacom/MSM データベース テーブルを確認し、最新の CA Datacom/MSM インストール データベースのバックアップを作成します。 ただし、最新のバージョンにアップグレードしている場合、このジョブにはアップグレードしている CA CSM バージョン固有の、追加の JCL 手順が含まれます。

このジョブが失敗する場合は、エラー メッセージを確認し、その問題の原因を突き止めます。状況を修正するために適切な処置を講じます。このジョブを再びサブミットする前に、以下の手順を実行します。

- CSMU*xx*10 JCL メンバをサブミットして、CA Datacom/MSM MUF を停止します。
- ジョブ CSMU*xx*07 を再びサブミットします。
- CSMU*xx*08 JCL メンバをサブミットして CA Datacom/MSM MUF を起動するか、または MSMMUF PROCLIB メンバを開始します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。

CSMU*xx*10（CA Datacom MUF の停止）

このジョブは CA Datacom/MSM MUF を停止します。

注: Automatic または Review モードで CA CSM インストーラを実行している場合でも、このジョブを手動で実行します。

UID(0) を使用しない CA CSM ユーザ ID の設定

CA CSM インストールが完了した後、実行中に UID(0) を使用せずに CA CSM を設定できます。

このセクションには、以下のトピックが含まれています。

前提条件 (P. 108)

CA Top Secret for z/OS の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 108)

CA ACF2 for z/OS の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 110)

IBM RACF の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 111)

前提条件

UID(0) を使用しないで CA CSM を実行するには、以下の要件が満たされていることを確認します。

- CA CSM アプリケーション サーバに関連付けられる CA CSM ユーザ ID は、0 以外の UID を持つ必要があります。
- CA CSM にログインする最初のユーザは、0 以外の UID を持つ必要があります。

  注: LJWK ディレクトリおよびマウント ポイントは、CA CSM ユーザ ID（*CA_CSM_USER_ID*）の代わりに、最初のユーザのユーザ ID を使用して作成されます。

CA Top Secret for z/OS の UID(0) を使用しない CA CSM ユーザ ID の設定

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 108)。
2. CA CSM のインストールが完了した後、お使いのセキュリティ システムで、たとえば GID 定義がある CACSMGRP のようなグループを作成し、以下の手順を実行します。
   a. CACSMGRP を DFLTGRP として各 CA CSM ユーザに追加します。
   b. CACSMGRP を DFLTGRP として CA CSM ユーザ ID に追加します。

3. 以下のコマンドを SUPERUSER 権限で発行し、所有者とグループを変更します。

```
chown -R CA_CSM_USER_ID MSMPATH
chgrp -R CACSMGRP MSMPATH
chown -R CA_CSM_USER_ID MountPath
chgrp -R CACSMGRP MountPath
chown -R CA_CSM_USER_ID RunTimeUSSPath
chgrp -R CACSMGRP RunTimeUSSPath
chown -R CA_CSM_USER_ID USSTempDwnldPath
chgrp -R CACSMGRP USSTempDwnldPath
```

   MSMPATH、MountPath、RunTimeUSSPath、USSTempDwnldPath (P. 240) には MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

   注: またこれらのコマンドを、MSMDEPLY ジョブを実行した後にも発行します。

4. 以下の手順を実行し、CA CSM ユーザ ID 用のパラメータを設定します。

   a. Facility STC を割り当てます。

   b. Master FAC に MSM を割り当てます。

      注: 割り当てる前に、Master FAC が存在する (P. 57)ことを確認してください。

   c. この MASTFAC を各 CA CSM ユーザに割り当てます。

5. 以下の必須 IBMFAC クラス許可を CA CSM ユーザ ID に割り当てます。

```
IBMFAC BPX.CONSOLE ACCESS(UPDATE)
IBMFAC BPX.SERVER  ACCESS(UPDATE)
IBMFAC BPX.FILEATTR.APF ACCESS(READ)
IBMFAC BPX.FILEATTR.PROGCTL ACCESS(READ)
IBMFAC BPX.FILEATTR.SHARELIB ACCESS(READ)
```

6. 以下の必須 UNIXPRIV クラス許可を CA CSM ユーザ ID に割り当てます。

```
UNIXPRIV SUPERUSER.FILESYS.CHANGEPERM ACCESS(READ)
UNIXPRIV SUPERUSER.FILESYS.MOUNT ACCESS(UPDATE)
```

7. 以下のオプションの SERVAUTH クラス許可を CA CSM ユーザ ID に割り当てます。

   ```
   SERVAUTH EZB.FTP ACCESS(READ)
   SERVAUTH EZB.STACKACCESS ACCESS(READ)
   ```

8. CA CSM 内の最初のタスクが完了した後、SUPERUSER 権限で以下のコマンドを発行します。

   ```
   chown -R CA_CSM_USER_ID MountPath
   chgrp -R CACSMGRP MountPath
   ```

   MountPath (P. 240) には、MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

CA ACF2 for z/OS の UID(0)を使用しない CA CSM ユーザ ID の設定

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 108)。
2. CA CSM のインストールが完了した後、お使いのセキュリティ システムで、GID 定義があるグループ（たとえば CACSMGRP）を作成し、以下の手順を実行します。
   a. CA CSM ユーザ ID を CACSMGRP のメンバとして定義します。
   b. 各 CA CSM ユーザを CACSMGRP のメンバとして定義します。
3. 以下のコマンドを SUPERUSER 権限で発行し、所有者とグループを変更します。

   ```
   chown -R CA_CSM_USER_ID MSMPATH
   chgrp -R CACSMGRP MSMPATH
   chown -R CA_CSM_USER_ID MountPath
   chgrp -R CACSMGRP MountPath
   chown -R CA_CSM_USER_ID RunTimeUSSPath
   chgrp -R CACSMGRP RunTimeUSSPath
   chown -R CA_CSM_USER_ID USSTempDwnldPath
   chgrp -R CACSMGRP USSTempDwnldPath
   ```

   MSMPATH、MountPath、RunTimeUSSPath、USSTempDwnldPath (P. 240) には MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

   注: またこれらのコマンドを、MSMDEPLY ジョブを実行した後にも発行します。

4. FACILITY リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のリソース名を定義します。

```
BPX.CONSOLE             UPDATE
BPX.SERVER              UPDATE
BPX.FILEATTR.APF        READ
BPX.FILEATTR.PROGCTL    READ
BPX.FILEATTR.SHARELIB   READ
```

5. UNIXPRIV リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のリソース名を定義します。

```
SUPERUSER.FILESYS.CHANGEPERM    READ
SUPERUSER.FILESYS.MOUNT         UPDATE
```

6. SERVAUTH リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のリソース名を定義します。

```
EZB.FTP           READ
EZB.STACKACCESS   READ
```

7. CA CSM 内の最初のタスクが完了した後、SUPERUSER 権限で以下のコマンドを発行します。

```
chown -R CA_CSM_USER_ID MountPath
chgrp -R CACSMGRP MountPath
```

MountPath (P. 240) には、MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

IBM RACF の UID(0) を使用しない CA CSM ユーザ ID の設定

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 108)。
2. CA CSM のインストールが完了した後、お使いのセキュリティ システムで、GID 定義があるグループ（たとえば CACSMGRP）を作成し、以下の手順を実行します。
   a. CA CSM ユーザ ID を CACSMGRP のメンバとして定義します。
   b. 各 CA CSM ユーザを CACSMGRP のメンバとして定義します。

3. 以下のコマンドを SUPERUSER 権限で発行し、所有者とグループを変更します。

```
chown -R CA_CSM_USER_ID MSMPATH
chgrp -R CACSMGRP MSMPATH
chown -R CA_CSM_USER_ID MountPath
chgrp -R CACSMGRP MountPath
chown -R CA_CSM_USER_ID RunTimeUSSPath
chgrp -R CACSMGRP RunTimeUSSPath
chown -R CA_CSM_USER_ID USSTempDwnldPath
chgrp -R CACSMGRP USSTempDwnldPath
```

   MSMPATH、MountPath、RunTimeUSSPath、USSTempDwnldPath (P. 240) には MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

   注: またこれらのコマンドを、MSMDEPLY ジョブを実行した後にも発行します。

4. FACILITY リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のプロファイルを定義します。

```
BPX.CONSOLE             UPDATE
BPX.SERVER              UPDATE
BPX.FILEATTR.APF        READ
BPX.FILEATTR.PROGCTL    READ
BPX.FILEATTR.SHARELIB   READ
```

5. UNIXPRIV リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のプロファイルを定義します。

```
SUPERUSER.FILESYS.CHANGEPERM    READ
SUPERUSER.FILESYS.MOUNT         UPDATE
```

6. SERVAUTH リソース クラスで、CA CSM ユーザ ID へのアクセス権限で以下のプロファイルを定義します。

```
EZB.FTP           READ
EZB.STACKACCESS   READ
```

7. CA CSM 内の最初のタスクが完了した後、SUPERUSER 権限で以下のコマンドを発行します。

```
chown -R CA_CSM_USER_ID MountPath
chgrp -R CACSMGRP MountPath
```

   MountPath (P. 240) には、MSMSetupOptionsFile.properties ファイルで参照した値を設定します。

SAMPLIB(MSMLIB) メンバのリモート システムの SYSUT3 および SYSUT4 用の UNIT パラメータの指定

IEBCOPY ユーティリティでは、SAMPLIB(MSMLIB) メンバ内にステートメントを追加することで、SYSUT3 および SYSUT4 DD ステートメントに対する特定の UNIT パラメータを指定できます。 Remote Deployment Service は、SYSUT3 および SYSUT4 の DD ステートメントを割り当てる際に、この方法で指定された UNIT パラメータを選択し、使用します。 ステートメントが定義されていない場合、Remote Deployment Service は、SYSUT3 および SYSUT4 の DD ステートメントを割り当てる際に、デフォルトの UNIT(SYSDA) を使用します。 パラメータを指定するには、以下のステートメントを追加します。

```
IJO="$IJO -Dmsmdutil.sysut3.unit=SYSALLDA"
IJO="$IJO -Dmsmdutil.sysut4.unit=SYSALLDA"
```

CA CSM アプリケーション サーバのマルチ TCP/IP スタック環境の TCP/IP スタックへのバインド

CA CSM がある LPAR に複数の TCP/IP スタックがあるとき、必要なスタックへの TCP/IP スタック親和性を確立します。 スタック親和性の確立により、すべてのソケット通信はそのスタックにバインドされます。

スタック親和性を確立するには、以下のいずれかのメソッドを選択します。

- 特定の TCPIP.DATA データ セットを指している CA CSM スタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に DD ステートメント SYSTCPD DD を追加します。 以下に例を示します。

  ```
  //SYSTCPD DD DSN=TCPIP.SEZAINST(TCPDATA),DISP=SHR
  ```

- 環境変数 _BPXK_SETIBMOPT_TRANSPORT を、CA CSM アプリケーション サーバの STDENV DD に関連付けられる *RunTimeMVSHLQPrefix*.SAMPLIB（MSMLIB）メンバに追加します。 以下に例を示します。

  ```
  export _BPXK_SETIBMOPT_TRANSPORT=stackname
  ```

- MSMSRV 手順の前に、CA CSM スタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に、追加の手順 AFFINITY を以下のように追加します。

  ```
  //AFFINITY EXEC PGM=BPXTCAFF,PARM=stackname
  ```

CA CSM の起動

CA CSM を起動する JCL メンバは、JCL データ セット（*RunTimeMVSHLQPrefix*.JCL）、または PROCLIB データ セット（*RunTimeMVSHLQPrefix*.PROCLIB）のいずれかにあります。 メンバの場所は、CA CSM のインストールおよびセットアップ プロセスのサマリ レポートで示されます。 これらのメンバをバッチ ジョブまたはスターティッド タスクとしてサブミットまたは開始できます。

CA CSM は、スタートアップ時および稼働中にファイルを割り当てます。サイトにファイル割り当てに影響する製品がある場合は、そのような処理を除外する DD ステートメントが、CA CSM アプリケーション サーバ (P. 329) を開始する JCL メンバ MSMTCSRV に含まれていることを確認してください。

注: CA CSM アプリケーション サーバ (P. 329)は、512 MB のデフォルト リージョン サイズを使用します。この値を変更する場合は、MSMTCSRV JCL メンバの REGSIZE パラメータを更新します。 また、以下のステートメントで、SAMPLIB(MSMLIB) メンバの Xmx 値を更新します。

```
IJO="-Xms128m -Xmx512m"
```

重要: 移行している場合は、旧バージョンの CA CSM からのアドレス空間が停止していることを確認します。 また、APLROOT、SCROOT、LJROOT、LJWK マウント ポイントを旧バージョンからマウント解除します。

以下の手順に従います。

1. MSMMUFS JCL メンバをサブミットするか、または MSMMUF PROCLIB メンバを開始します。

   CA Datacom/MSM/Multi-User 機能（MUF）アドレス空間が開始します。

   注: STEPLIB のすべてのデータ セットは、APF 許可される必要があります。

MUF が正常に開始すると、以下の例のようなメッセージが表示されます。

```
DB00215I - CA Datacom/DB r12 at service pack: SP0
DB00212I - CA Datacom SQL r12   at service pack: SP0
DB00226I - MULTI-USER ACTIVATED XCF SUPPORT (RIMF20,mufname)
DB00222I - MULTI-USER ACTIVATED CCI SUPPORT (caicci_sysid,mufname)
DB00201I - MULTI-USER ENABLED, CXX=cxx_name    MUFNAME=mufname SVC=svc_number
```

重要: ランタイム CUSMAC(DBDATIN1) メンバの MUF パラメータの値が、オプション ファイル（MSMSetupOptionsFile.properties）の MUFname キーワードの値と一致することを確認してください。一致しない場合、MUF を開始できません。

2. *初めて*最新の CA Datacom/MSM MUF を起動する場合、MSMDBSVS（CA Datacom/DB サーバ）および MSMTCSRV（アプリケーション サーバ）がアクティブではないことを確認してください。

3. MSMDBSVS JCL メンバをサブミットするか、または MSMDBSRV PROCLIB メンバを開始します。

   CA Datacom/MSM サーバ アドレス空間が開始します。

   サーバが正常に起動すると、以下の例のようなメッセージが表示されます。

   ```
   DB00101I - Started Job-MF2SRVR2 number-11326 CXX=CAMSM    Mufname=muf_name
   Svc=svc_number
   BPXM023I (USER01) DSV00049I-CA Datacom Server r11      INITIALIZED -server_name
   ```

4. MSMTCSRV JCL メンバをサブミットするか、または MSMTC PROCLIB メンバを開始します。

   CA CSM アプリケーション サーバ アドレス空間が開始します。

   サーバが正常に開始すると、以下のメッセージが STDOUT に表示されます。

   ```
   MSM0009I - CA CSM startup complete.
   ```

   スタートアップが失敗した場合、以下のメッセージが STDOUT に表示されます。

   ```
   MSM0010E - CA CSM startup failed.
   ```

   さらに、スタートアップの結果に応じて、以下のいずれかのメッセージがシステム コンソールに表示されます。

   ```
   MSM0009I CA CSM STARTUP COMPLETE
   MSM0010E CA CSM STARTUP FAILED
   ```

注: CA CSM アプリケーション サーバ (P. 329) リージョンのスタートアップ JCL には、コメント アウトされた SYSMDUMP DD ステートメントがあります。サイトの基準やシステムが、このダンプのスプール システムへの収集をサポートしている場合、この DD ステートメントのコメントを解除することで、失敗した場合のダンプを取得することができます。

CA CSM アプリケーション サーバ アドレス空間 (P. 329)が正常に開始されると、Web ブラウザから CA CSM にログインできます。

注:

- MSMDBSRV ジョブの初期化が完了し、BPXM023I メッセージが表示されるまで、MSMTCSRV ジョブを開始しないでください（手動、または自動化により）。
- CA CSM アプリケーション サーバを正常に起動した後、以下のメッセージが表示される場合は、無視してください。

  ```
  INFO: The APR based Apache Tomcat Native library which allows optimal performance in production environments was not found on the java library.path:
  ```

  CA CSM では、このライブラリのインストールは必要ありません。
- CA サポート からのリクエストがない限り、いかなる CA CSM アプリケーション サーバ スタートアップ JCL パラメータも変更しないでください。 変更した場合、CA CSM が操作できなくなる可能性があります。
- ユーザが既存の CA CSM 顧客で、データベースをアップグレードしている場合、初めて CA CSM を正常に起動した後に MSMTCSRV JCL メンバまたは MSMTC PROCLIB 内の DBUPDATE DD カードをコメントアウトします。
- CA Datacom/MSM サーバを再起動する場合は、CA CSM アプリケーション サーバを再起動します。

詳細:

CA CSM の停止 (P. 154)
CA CSM 機能のユーザ セキュリティのセットアップ (P. 62)

MUF メッセージ出力の設定

複数の CA Datacom/DB MUF リージョンを区別するため、DBDATIN1 メンバ内の MUFMSG パラメータを使用します。 このパラメータを設定し、ジョブ名、SVC 番号および SUBID の出力を指定します。これらのプロパティは、Multi-User 機能が発行したメッセージ、および Multi-User 機能との通信に関係のある一部のメッセージのメッセージ番号の前に付けます。

```
MUFMSG=YES,YES,YES
```

プレフィクス付きメッセージは、以下の形式で表示されます。

jobname:*svc_number*:*subid*:DB0*xxxx*I

FORCE_SVC MUF スタートアップ オプションを使用する場合、MUF は MUF と同じバージョンの最も数字が大きい Service Pack の、最も数字が小さい SVC 番号を選択します。

ただ 1 つの CA Datacom/DB MUF リージョンを実行する場合、このパラメータを変更して出力を無効にできます。出力を無効にするには、MUFMSG パラメータを以下のように設定します。

```
MUFMSG=NO,NO,NO
```

CA Datacom/MSM MUF スタートアップの IEC988I メッセージの有効化

CA CSM は、以下の情報を表示するオプションを提供します。

```
IEC988I jjj,sss,ddn{-#},dev,volser,dsn DATA SET NOT UNALLOCATED DURING
           CLOSE RCxx
```

アップグレードまたは新規インストール中にエラーとして解釈される可能性があるメッセージを可能な限り小さくするために、デフォルトでは CA CSM はこれらのメッセージの発行を行いません。

CA CSM を有効化し、コンソール ログおよびジョブ出力のメッセージを表示できます。

以下の手順に従います。

1. CA Datacom/MSM Multi-User 機能（MUF）スタートアップ メンバ CUSMAC（DBDATIN1）の検索
2. 以下のコントロール カードを検索します。

   ```
   PREVENT_IEC988 YES        PREVENT IEC988I MESSAGE
   ```

3. コントロール カードの前の列にアスタリスク（*）を直接挿入して、コントロール カードをコメントアウトします。

   コントロール カードは以下のように表示されます。

   ```
   *PREVENT_IEC988 YES          PREVENT IEC988I MESSAGE
   ```

4. CA CSM をリサイクルします。

   以下の順に CA CSM を停止し、次に逆順でそれを起動することで、CA CSM を再利用できます。

   a. MSMCPROC - SCS アドレス空間（利用可能な場合）
   b. MSMTCSRV - CA CSM アプリケーション サーバ
   c. MSMDBSVS - CA Datacom/MSM データベース（ジョブ メンバ MSMDBSVP を実行）
   d. MSMMUFS - CA Datacom/MSM MUF（ジョブ メンバ MSMMUFP を実行）

これらの変更を適用した後、コンソール ログに CA Datacom/MSM ユーティリティの open と close 機能を発行するジョブに対する IEC988I メッセージが表示される場合があります。このメッセージは、open と close 機能が CA Datacom/MSM データ セット（特に複数のエクステント ディスク割り振りにあるデータ セット）に対して実行されるごとに表示されます。

出力記述子の設定

CA CSM ポリシー ウィザードから出力記述子を選択できるようにするには、CA CSM サーバ スタートアップ JCL で出力記述子の値を指定する必要があります。CA CSM ランタイム JCL ライブラリで提供されるサンプル JCL の名前は MSMTCSRV で、CA CSM ランタイム PROCLIB ライブラリで提供されるサンプル JCL の名前は MSMTC です。 CA CSM スタートアップ JCL で複数の出力記述子を使用することができ、それによりウィザードからそれらの出力記述子のうちいずれか 1 つを選択することができます。 ポリシーが JES スプール オプションによって CA CSM タスク出力の処理に対して実行されるとき、選択された出力記述子が使用されます。 出力記述子は、それらが CA CSM スタートアップ JCL で指定される場合、このウィザードからのみ利用できます。

以下の例ではサイト固有の意味のある名前を使用して、出力記述子を示します。

```
//CAVIEW    OUTPUT  CLASS=9,FORMS=2UP
//CASPOOL   OUTPUT  CLASS=S
```

注: 出力記述子および OUTPUT JCL ステートメントのパラメータの詳細については、「*IBM z/OS MVS JCL Reference*」を参照してください。

CA CSM の[Notice and Consent]バナーの有効化

CA CSM をセットアップしてインストールした後、CA CSM にログインするごとに［Notice and Consent］バナーを表示するように設定できます。

CA CSM が初めて開始されるとき、MSMBanner.html という名前のファイルが以下のディレクトリに作成されます。

```
tomcat/webapps/MSM/
```

ファイルにはサンプルのバナーが含まれます。

以下の手順に従います。

1. 以下のディレクトリにサンプル ファイル MSMBanner.html をコピーします。

   ```
   tomcat/webapps/
   ```

2. （オプション）ファイルのコンテンツを修正し、それがユーザ組織の要件に一致するようにします。

   バナーが利用可能になり、次回ユーザが CA CSM にログインする時に表示されます。

   注: 以下の文字列内の CA CSM アクセス URL を変更しないでください。

   ```
   <a href="MSMMain.html">
   ```

CA CSM の設定

CA CSM をセットアップしてインストールした後、CA サポート Online Web サイトにアクセスして、製品を取得できるように設定します。 最初のログイン時に、CA CSM を設定を促すプロンプトが表示されます。

以下の手順に従います。

1. Web ブラウザを開き、アクセス先の URL を入力します。

   ログイン ページが表示されます。

   注: Notice and Consent バナーが表示される場合は、表示される情報を読み、その内容に同意してください。

2. z/OS のログイン ユーザ名およびパスワードを入力し、ログインします。

   初期ページが表示され、CA CSM を設定するように求めるプロンプトが表示されます。

   注: インターフェースの詳細については、ページの右上隅にあるオンライン ヘルプのリンクをクリックしてください。

3. 以下の設定を行います。

   - CA CSM が CA サポート Online Web サイトとの通信に使用するプロキシ

     プロキシが使用されない場合、CA CSM は HTTPS ポート番号 443 および FTP ポート番号 21 を使用します。

     重要: サイトでプロキシを使用する場合は、［User Settings, Software Acquisition］ページで、プロキシ認証情報を確認します。

   - ダウンロードされたソフトウェア パッケージ用の一時ディレクトリへの USS パス

     このディレクトリを指定しない場合、CA CSM は後で変更できるデフォルトの設定を使用して、USS パスを設定します。

   注: これらの設定は、［System Settings］ - ［Software Acquisition］ページでも行うことができます。

   ［Next］をクリックします。

   CA サポート Online Web サイトのアカウントを定義するように促すメッセージが表示されます。

4. ［New］をクリックします。

   CA サポート Online Web サイトで使用する認証情報の入力を促すメッセージが表示されます。

5. 認証情報を指定し、［OK］をクリックして［Next］をクリックします。

   ユーザ設定の確認を促すメッセージが表示されます。

   注: これらの設定は ［User Settings］ページで設定可能です。

6. 設定を変更するかデフォルトをそのまま使用し、［Finish］をクリックします。

   設定タスクの進捗状況を示すダイアログ ボックスが表示されます。［Show Results］をクリックすると、完了したタスクのアクションの詳細を表示できます。

7. ［Settings］タブをクリックし、他の設定を確認します。

CA CSM の設定が完了しました。 ユーザはログインし、メインフレーム製品のダウンロードが開始できます。

FTP および HTTP 接続の設定

このセクションでは、新規および既存の CA CSM インストール用の FTP 接続を設定する方法について、また HTTP 接続を設定する方法について説明します。

既存インストール用の FTP 接続の設定

旧バージョンの CA CSM から CA CSM リリース 5.1 にアップグレードするとき、FTP の設定変更はありません。

新規インストール用の FTP 接続の設定

このセクションでは、CA CSM をインストールした後に、FTP と HTTP の設定を設定する方法について説明します。

FTP セッションのオプション

CA CSM は Java ベースの FTP クライアントを使用します。 この FTP クライアントには、セッションの操作を制御するいくつかのオプションがあります。 FTP サーバにログインするとき、これらのオプションは認証サービスを提供する FTP プロキシに関連付けられているとは見なされません。

FTP セッションのオプションは、インストールされた CA CSM データ セット SAMPLIB（PASADVOP）で指定されます。 このデータ セットは XML ファイルで、利用可能なすべての FTP セッションのオプションを定義する FTPOPTIONS セクションがあります。 各オプションは FTP クライアントのデフォルトに設定されます。

<FTPOPTIONS> XML タグは、CA CSM が確立するすべての FTP 接続に対して読み込まれます。 タグが定義されていない、または空の場合、CA CSM FTP クライアントはこのセクションで示されているデフォルトを使用します。

FTP セッション設定用のコード構文のサンプルを以下に示します。

```
<FTPOPTIONS>key_1=value_1, key_2=value_2</FTPOPTIONS>
```

以下のキーを使用することができます。

- firewall.friendly
- verify.pasv.ip
- default.timeout
- default.port

firewall.friendly

firewall.friendly FTP オプションは、以下のようにデフォルトでは true に設定されます。

```
<FTPOPTIONS>firewall.friendly=true</FTPOPTIONS>
```

オプションをオーバーライドする場合のみ、このオプションを指定します。

firewall.friendly オプションは、パッシブ モードで動作する FTP を参照します。 パッシブ モードは、FTP サーバに FTP データ接続用のリスニング ポートを開くように指示します。 このオプションが false に設定される場合、FTP クライアントはサーバ用のリスニング ポートを開きます。

パッシブ モードがサポートされているかどうかをネットワーク管理者に問い合わせてください。 または、バッチ FTP プログラムを実行して、デフォルトが受け付けられるかどうかをテストできます。「*anonymous*」で FTP サーバにログインするステートメントの後に、QUOTE PASV を挿入します。

ジョブ出力は、以下のテキストを含むメッセージを表示します。

```
227 Entering Passive Mode (IP_address,FTP_server_code)
```

- このメッセージが表示される場合、firewall.friendly オプションを指定する必要はありません。
- このメッセージが表示されない場合は、QUOTE PASV を削除して、ジョブを再実行します。ジョブ出力は、以下のテキストを含むメッセージを表示するようになります。

  ```
  200 PORT command successful.
  ```

  このメッセージが表示された場合、firewall.friendly を false に設定します。

verify.pasv.ip

verify.pasv.ip FTP オプションは、以下のようにデフォルトでは true に設定されます。

```
<FTPOPTIONS>verify.pasv.ip=true</FTPOPTIONS>
```

オプションをオーバーライドする場合のみ、このオプションを指定します。

重要: ファイアウォールのサポート チームが強く依頼しない限り、このオプションをオーバーライドしないことをお勧めします。

ファイアウォールの実装の中には、PASV コマンドへの応答で FTP サーバから返される IP アドレスを遮断し変更するものもあります。この場合、CA CSM アプリケーション サーバ (P. 329)のログで以下のメッセージが表示されることがあります。

```
Host attempting data connection ip_address_1 is not same as server ip_address_2
```

ip_address_1

ファイアウォール サーバで変更された IP アドレスを示します。

ip_address_2

FTP サーバの IP アドレスを示します。

default.timeout

default.timeout FTP オプションは、以下のようにデフォルトでゼロ（0）に設定されます。

```
<FTPOPTIONS>default.timeout=0</FTPOPTIONS>
```

オプションをオーバーライドする場合のみ、このオプションを指定します。

このオプションの値はミリ秒で時間を指定します。デフォルト値 0 は無限タイムアウトとして解釈されます。いくつかの環境では、200 MB 以上のサイズの大きなファイルをダウンロードするときに、タイムアウトの問題が発生する場合があります。

たとえば、大きなファイルは OMVS の FTP コマンド ライン セッションを使用してダウンロードされます。データ転送が完了すると、後続の FTP コマンド（たとえば **ls**）が入力されます。 タイムアウトの条件を満たすと、以下のようなメッセージが表示されることがあります。

```
Connection to server interrupted or timed out. Waiting for reply.
```

このケースでは、CA CSM にこのメッセージが表示された場合、10000（10 秒を表す）の値を設定することでこの問題は解決します。

default.port

default.port オプションは、デフォルトでは 21 に設定されます。 このポートは FTP が使用する業界標準のデフォルト ポートです。 FTP プロキシ認証要件がない場合でも、このデフォルト ポートを変更するファイアウォールの実装がある場合があります。

```
<FTPOPTIONS>default.port=21</FTPOPTIONS>
```

ポート番号 21 を必要なポート番号に変更できます。

注: FTP プロキシ設定を有効にする場合、このオプションによる影響はありません。

詳細:

FTP プロキシ認証設定 (P. 125)

FTP プロキシ認証設定

CA CSM の FTP および HTTP プロキシ認証設定を必要に応じて設定できます。 CA CSM の FTP Java ベース クライアントには、設定可能な追加のセッション オプションがあります。 これらのオプションは FTP プロキシとは関連がありません。

CA CSM がインストールされると、PASADVOP という名前の PDS メンバが SAMPLIB データ セットに配置されます。 このメンバには、拡張 FTP および HTTP 設定が含まれる汎用テンプレートがあります。 メンバのデフォルト値を使用するか、または ISPF エディタを使用してそれらを修正し、ユーザの FTP および HTTP プロキシ認証要件に一致させることができます。

注:データ セットとメンバ名のような拡張設定は、CA CSMWeb ベース インターフェースの［System Settings］ - ［Software Acquisition］ページに表示されます。

お使いの FTP ファイアウォールにプロキシ サーバとポートの指定のみが必要な場合、これらの拡張設定を使用する必要はありません。

詳細:

FTP セッションのオプション (P. 122)

FTP 基本プロキシ設定

［System Settings］ - ［Software Acquisition］ページの［FTP Proxy］セクションの［Enable Proxy Settings］チェック ボックスのみをオンにすると、CA CSM は以下の 2 つの基本的な FTP プロキシ要件をサポートします。

- FTP プロキシ サーバ名およびポートを指定し、ユーザ認証情報は空白にします。CA CSM はプロキシ サーバに接続します。その後、CA CSM は、anonymous@ftp.ca.com パラメータを使用して FTP USER コマンドを送信し、CA サポート Online Web サイト用の ID をパスワードとして使用して、FTP PASS コマンドを送信します。

  注: ユーザ認証情報は、［User Settings］ - ［Software Acquisition］ページに表示されます。

- FTP プロキシ サーバ名とポートは FTP ユーザ認証情報を使用して指定されます。CA CSM は指定したプロキシ サーバに接続し、FTP コマンドの以下のシーケンスを送信して FTP サーバの認証を行い、ログインします。

  ```
  USER FTP_proxy_user_ID@ftp.ca.com
  PASS proxy_password
  USER anonymous
  PASS Support_Online_user_ID
  ```

注: ftp.ca.com が記述されている他のすべての CA FTP サーバに、同じシナリオが適用されます。

FTP 拡張プロキシ設定

FTP の基本的な設定がお使いの FTP プロキシの認証要件をサポートしない場合、FTP の拡張プロキシ設定を使用して、お使いの FTP に必要な FTP 認証およびログオンをカスタマイズできます。

すべての XML 要素は、以下のように親要素の <ADVOPTIONS></ADVOPTIONS> の間に指定される必要があります。

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;@REMOTE_USER;@REMOTE_HOST;</FIRECMD>
    <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  <FIREWALL>
</ADVOPTIONS>
```

FTP プロキシ設定用のコード構文のサンプルを以下に示します。

```
<FIREWALL>
  <FIRECMD>keyword;</FIRECMD>
<FIREWALL>
```

以下のキーワードを使用し、さまざまな FTP プロキシ認証スキームをサポートします。

HOST

FTP プロキシ サーバの名前を定義します。 このキーワードがあるとき、CA CSM はこの値に［System Settings］ - ［Software Acquisition］ページの［FTP Proxy Server］名に入力された値を代入します。 FTP クライアントは、最初の接続にこの値を使用します。

USER

有効なプロキシの認証のためのユーザを定義します。 このキーワードがあるとき、この値には［User Settings］ - ［Software Acquisition］ページの［FTP Proxy User］に入力された値が代入されます。

PW

有効なプロキシの認証のためのパスワードを定義します。 このキーワードがあるとき、この値には［User Settings］-［Software Acquisition］ページの［FTP Proxy Password］に入力された値が代入されます。

REMOTE_HOST

リモート サーバの FTP アドレスを定義します。このキーワードがあるとき、この値には適切な FTP URL が代入されます。

REMOTE_USER

リモート サーバの認証のためのユーザを定義します。このキーワードがあるとき、この値には「*anonymous*」が代入されます。

REMOTE_PW

リモート サーバの認証のためのパスワードを定義します。 このキーワードがあるとき、この値には CA サポート Online Web サイト用のユーザ ID が代入されます。

ACCT

FTP サーバに ACCT コマンドを発行するよう、CA CSM FTP クライアントに指示します。 このキーワードが実装され、付属パラメータが許可されるようになりました。 このパラメータは通常、PW キーワードで表されるプロキシのパスワードです。

セミコロン（;）の後にキーワードを続けます。 これらのキーワードを使用して、プロキシ認証の概略について説明します。 CA CSM は、［System Settings］ - ［Software Acquisition］ページからの実際の値を代入します。

詳細:

サンプル FTP 拡張設定 (P. 128)

サンプル FTP 拡張設定

IBM FTP プログラムを実行する z/OS 内のバッチ ジョブを実行して、拡張設定をセットアップすることをお勧めします。 FTP プロキシ認証スキームを、拡張設定が含まれるデータ セットに変換できます。

たとえば、FTP バッチ ジョブへの入力を以下に示します。

```
//INPUT DD *
proxy_host_URL_or_IP
anonymous@ftp.ca.com proxy_userid
Support_Online_user_id
ACCT proxy_password
/*
```

注:

- スペースを *proxy_userid* の前に入れます。
- ネットワーク管理者が引用符を要求する場合は、引用符で 2 番目の入力行を囲みます。

この場合、拡張設定データ セットを以下のように編集します。

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;@REMOTE_HOST; USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
    <FIRECMD>ACCT; PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

- HOST キーワードには、［System Settings］-［Software Acquisition］ページ上の［FTP Proxy Server］名に指定された FTP プロキシ名が代入されます。
- REMOTE_USER キーワードには「anonymous」が代入されます。
- USER キーワードには、［User Settings］ -［Software Acquisition］ページの［FTP Proxy］セクションのユーザに指定された値が代入されます。
- REMOTE_HOST キーワードには、適切な CA TechnologiesFTP サーバ URL が代入されます。
- ACCT キーワードは、CA CSM FTP クライアントに FTP サーバに ACCT コマンドを発行するように指示します。 このキーワードにより、付属パラメータが許可されます。 パラメータは通常、キーワード PW で示されるプロキシ パスワードですが、ネットワーク管理者が要求する内容によって異なります。
- CA CSM は REMOTE_USER キーワードに、［System Settings］-［Software Acquisition］ページの［CA Support Online Accounts］セクションで指定された、CA サポート Online Web サイトのユーザ ID を代入します。 PW キーワードには、［User Settings］-［Software Acquisition］ページの［FTP Proxy］セクションのパスワードに指定された値が代入されます。 これらの代入はすべて FIRECMD ステートメントで指定された順に連結されます。 アット記号（@）が、解決された文字列に指定されたとおりに挿入されます。

FTP 入力は、容易に FIRECMD 要素に変換されないこともあります。その場合、バッチ FTP ジョブの SYSOUT を使用することができます。 このセクションの初めに説明された //INPUT DD * バッチ ジョブを使用すると、特定の FTP コマンドを検索し、特定のシーケンスを確認することができます。

以下の SYSOUT は省略して表示しています。 FIRECMD ステートメントの作成に使用される、関連ステートメントが強調表示されています。

注: コメントは ==> で示されます。

```
EZA1450I IBM FTP CS V1R9
EZA1772I FTP: EXIT has been set.
    ==> The EZA1554I message shows the IP address of the FTP proxy server, and
    message 220 typically, but not always, displays the URL of the FTP proxy.
    Either of these can be specified in the CA CSM FTP Proxy settings as
    an IP address or the FTP proxy server name. This would translate to
    <FIRECMD> HOST;</FIRECMD>.
EZA1554I Connecting to:   123.456.789.1 port: 21.
220 Secure FTP server running on ftpproxyserver
    ==> The EZA1701I message indicates that the FTP USER command accepts a
    concatenated string to provide the FTP proxy user ID, the FTP user ID, and
    the actual FTP site to connect after the authentication is completed. This
    concatenated string would be translated as
    <FIRECMD>REMOTE_USERID;@USER;@REMOTE_HOST;</FIRECMD>.
EZA1459I NAME (123.456.789.1:ZOSUSERID):
EZA1701I >>> USER anonymous@proxy_userid@ftp.ca.com
    ==> Message 331 is an FTP proxy reply that indicates that the PASS command
    will accept a concatenated string to provide the passwords for both
    the FTP proxy server and the FTP server. As it does not specify which should
    be first, check the //INPUT DD * sample to see that the FTP server password
    is first (anonymous). Typically, but not always, if the user IDs are
    concatenated, the passwords are concatenated in the same order. That means,
    as in this case, the FTP user ID is first, therefore the FTP password is
    first. This concatenated string would be translated to
    <FIRECMD>REMOTE_PW;@PW;</FIRECMD>.
331 password: use password@password
EZA1789I PASSWORD:
EZA1701I >>> PASS
    ==> The following replies indicate the FTP proxy has successfully
    authenticated your FTP proxy credentials, and is logging in to the
    FTP server. The FTP server is acknowledging you have successfully
    logged in.
230-User proxy_userid authenticated by Secure FTP authentication
230-Connected to server. Logging in...
230-220 ftp.ca.com NcFTPd Server (licensed copy) ready.
230-331 User anonymous okay, need password.
230-230-You are user #18 of 4000 simultaneous users allowed.
```

SITE コマンドを使用する例を以下に示します。

```
<ADVOPTIONS>
  <FIREWALL>
    <FIRECMD>HOST;</FIRECMD>
    <FIRECMD>USER;</FIRECMD>
    <FIRECMD>PW;</FIRECMD>
    <FIRECMD>SITE;REMOTE_HOST;</FIRECMD>
    <FIRECMD>REMOTE_USER;</FIRECMD>
    <FIRECMD>REMOTE_PW;</FIRECMD>
  </FIREWALL>
</ADVOPTIONS>
```

FTP XML の制限

以下の制限が適用されます。

- CA CSM は、<FIRECMD> 要素内の実際のユーザ ID およびパスワードをサポートしません。
- CA CSM はプロキシのユーザ ID と FTP のユーザ ID（*匿名*）の連結、およびプロキシのパスワードと FTP のパスワード（CA サポート Online Web サイト用の ID）の連結をサポートします。 ただし、プロキシ ユーザ ID とプロキシ パスワードの連結、または CA サポート Online Web サイトの ID の「*anonymous*」はサポートされて*いません*。

  たとえば、以下がサポートされています。

  ```
  <FIRECMD>USER;@REMOTE_USER;</FIRECMD>
  <FIRECMD>PW;@REMOTE_PW;</FIRECMD>
  ```

  以下はサポートされて*いません*。

  ```
  <FIRECMD>USER;PW;</FIRECMD>
  <FIRECMD>REMOTE_USER;REMOTE_PW;</FIRECMD>
  ```

  この場合、個別の FIRECMD 要素にユーザ ID とパスワードを、たとえば以下のように配置します。

  ```
  <FIRECMD>USER;</FIRECMD>
  <FIRECMD>PW;</FIRECMD>
  <FIRECMD>REMOTE_USER;</FIRECMD>
  <FIRECMD>REMOTE_PW;</FIRECMD>
  ```

HTTP 接続設定の構成

注: CA CSM Web ベース インターフェース内の［User Settings］の［Software Acquisition］ページに、NTLM ドメインおよびユーザ情報を追加することをお勧めします。 または、ここで説明されているプロセスを使用することもできます。

HTTP 設定用のコード構文のサンプルを以下に示します。 すべての XML 要素は、以下のように親要素の <ADVOPTIONS></ADVOPTIONS> の間に指定される必要があります。

```
<ADVOPTIONS>
  <HTTPPROXY ntlmDomain="mydomain" ntlmVersion="1"> </HTTPPROXY>
</ADVOPTIONS>
```

詳細設定で、NTLM 認証を指定することができます。

XML 要素が必要になるのは、Microsoft Windows サーバが HTTP 認証を実行する場合のみです。 そうでない場合は、［System Settings］ -［Software Acquisition］ページで、HTTP プロキシ用の拡張設定データ セットを有効にしないことをお勧めします。

「ntlmDomain="*domainName*"」の設定は、Microsoft Windows サーバで実行されていて、NTLM 認証を採用している HTTP プロキシにのみ必要です。

NTLM v1（ntlmVersion="1" の設定）は、NTLM 認証が必要な場合のデフォルト設定です。 この設定はオプションで、値を省略するか、「1」（NTLM v1）または「2」（NTLM v2）を指定します。

CETN500 を使用した CA Common Services for z/OS のアップグレード

CETN500 は CA Common Services for z/OS の機能で、pax ファイル MSM50G0.pax.Z にパッケージ化されています。 このファイルには、CETN500 を既存の CA Common Services for z/OS SMP/E 環境（r12 またはバージョン 14）にインストールするための、RELFILES、SMP MCS、およびサンプル JCL が含まれています。 この機能をインストールし、CA CSM を使用して CA Common Services for z/OS に製品を設定します。 CETN500 はモジュールを CA Common Services for z/OS PDSE CAIPLD（r12）または CAW0PLD（バージョン 14）にインストールします。それは APF 許可され、LINKLIST 内にあることが必要です。 CETN500 は CA Common Services for z/OS リリース 14.1 に組み込まれます。

CETN500 をインストールする前に、ソフトウェア要件 (P. 45)を満たしていることを確認します。

注: SYSTEM REGISTRY VALIDATE アクションが必要とする System Discovery 機能は、CA Common Services for z/OS 用の CCS LOAD ライブラリ（CAILOAD CAW0LOAD）内にあります。

CETN500 は、CA Common Services for z/OS バージョン 14.0 に含まれる名前と互換性のある DDDEF 名を使用します。 さらに CETN500 は、お使いの CA Common Services for z/OS SMP/E 環境から CETN300 または CETN400 を削除して、それらと入れ替わります。 CETN500 には、Software Configuration Service（SCS）および Software Deployment Service（SDS）の共通コンポーネントの両方が含まれます。SDS を開始する前に、各ターゲット システム上で CCIDSCSV と CCISPNSV をセットアップします。

CA CSM を使用した r12 のアップグレード

CA Common Services for z/OS r12 を使用していて、CA Common Services for z/OS バージョン 14.0 またはそれ以降のバージョンにアップグレードできない場合、代わりに CA CSM を使用して、CA Common Services for z/OS r12 を CETN500 でアップグレードできます。

以下の手順に従います。

1. MSM50G0.pax.Z を USS ディレクトリにダウンロードします。ファイルをダウンロードするには、ファイルを CA Technologies ファイル サーバ ディレクトリからユーザの USS ディレクトリに直接 FTP 転送します。

   a. 以下の場所にある FTP サイトに接続します。

      ```
      ftp://ftp.ca.com
      ```

   b. 以下の認証情報を使用して、ftp.ca.com にログインします。

      ユーザ名： anonymous
      パスワード： *自分の電子メール アドレス*

   c. 以下のディレクトリに移動します。

      ```
      cd /CAproducts/ca90s/MSMCCS50/GA/CCS_r12/
      ```

   d. 以下の ESD 配布ファイルをバイナリ形式で、メインフレームの HFS ファイルにダウンロードします。

      ```
      bin
      get MSM50G0.pax.Z MSM50G0-CCSR12.pax.Z
      ```

   e. FTP セッションを終了します。

2. CA CSM にログインし、［SMP/E Environments］タブをクリックします。右ペインでお使いの CA Common Services for z/OS r12 SMP/E 環境を選択し、［Use as Working Set］をクリックします。

3. ［Products］タブをクリックし、左ペインの［Actions］リストの下の［Install External Package］をクリックします。表示される［Install External Package］ダイアログ ボックスで、pax ファイルの場所を以下のように入力し、［OK］をクリックします。

   ```
   /your_directory_path/MSM50G0-CCSR12.pax.Z
   ```

   ［Install External Package］ダイアログ ボックスが閉じ、［Base Installation］ウィザードが開き、［Welcome］の手順に進みます。

4. ［Next］をクリックして［Features］手順に進み、［Full Install］を選択し、［Next］をクリックします。

   ［Prerequisites］手順が表示されます。

5. 前提条件がない場合、［Next］をクリックしてこの手順をスキップします。

   ［SMP/E Environment］手順 1/3 が、［Create a New SMP/E Environment］や、既に作業セットにある SMP/E 環境のような複数のオプションで表示されます。

   注: SMP/E 環境定義が表示されない場合は、［Cancel］をクリックし、手順 1 で別の CA Common Services for z/OS r12 SMP/E 環境を選択してこの手順を再開します。 ［Create a New SMP/E Environment］をクリックしないでください。

6. CA Common Services for z/OS SMP/E 環境を選択し、［Next］を 2 回クリックし（［SMP/E Environment］手順 2/3 を更新することはできません）、［SMP/E Environment］手順 3/3 に進みます。

7. ワークの DDDEF パラメータを指定し、［Next］をクリックして［Target Zone］手順 1/3 に進みます。

8. CA Common Services for z/OS r12 インストールに関連付けられたゾーンを選択し、［Next］をクリックして［Target Zone］手順 2/3 に進みます。

   CA CSM は［Target Zone］手順 2/3 の下の部分に、SMS またはデータ セット ターゲット ライブラリ割り当てパラメータを表示します。

9. SMS またはデータ セット ターゲット ライブラリ割り当てパラメータを指定し、［Next］をクリックして［Target Zone］手順 3/3 に進みます。

   注: CA CSM がこれらのフィールドに事前入力する値を使用できます。それらの値は、CA Common Services for z/OS r12 をインストールしたときに設定した値です。

10. Secure Socket Library ターゲット ゾーン パラメータを指定します。

    以下のターゲット データ セットが表示されます。

    - CAW0SCST
    - CAW0XML0（何もインストールされていない、または CETN300 のみがインストールされている場合）

11. ［Next］をクリックし、［Distribution Zone］手順 1/3 に進みます。

12. CA Common Services for z/OS r12 インストールに関連付けられたゾーンを選択し、［Next］をクリックして［Distribution Zone］手順 2/3 に進みます。

13. SMS またはデータ セット配布ライブラリ割り当てパラメータを指定し、［Next］をクリックして［Distribution Zone］手順 3/3 に進みます。

    注: CA CSM がこれらのフィールドに事前入力する値を使用できます。それらの値は、CA Common Services for z/OS r12 をインストールしたときに設定した値です。

    以下の配布データ セットが表示されます。

    - AETNSCST
    - AETNEXP（何もインストールされていない、または CETN300 のみがインストールされている場合）
    - AETNJCL（何もインストールされていない、または CETN300 のみがインストールされている場合）
    - AETNSDF（何もインストールされていない、または CETN300 のみがインストールされている場合）
    - AETNXML0（何もインストールされていない、または CETN300 のみがインストールされている場合）
    - AETNOPTN（CETN300 も CETN400 もインストールされていない場合）
    - AETNPROC（CETN300 も CETN400 もインストールされていない場合）
    - AETNPLD（CETN300 も CETN400 もインストールされていない場合）

14. ［Next］をクリックして［Summary］手順に進み、インストール サマリを確認し、［Install］をクリックしてインストール プロセスを完了します。

CETN500 で配布されたロード モジュールに一致する CA Datacom/MSM SQL プランは、DDDEF CAW0EXP によって示されるライブラリ内にあり、MSMC*SQL という形式のメンバ名です。 CA CSM 用に CA Datacom/DB へプランをインポートするために使用されるサンプルの JCL は、CAW0JCL に示されるサンプルの JCL ターゲット ライブラリ内のメンバ MSMCXPLN として提供されます。

CA CSM を使用したバージョン 14 のアップグレード

CA Common Services for z/OS バージョン 14.0 を使用している場合、CA CSM を使用して、CETN500 でアップグレードできます。

重要: CETN500 をインストールする前に、RO44235 を APPLY して ACCEPT してください。 HOLDDATA で指示される手順に従い、必要なライブラリを割り当て、DDDEF エントリを追加します。RO44235 を ACCEPT した後、CA CSM から CA Common Services for z/OS バージョン 14.0 SMP/E 環境を削除し、CA CSM にそれを再移行します。 これにより、CA CSM は外部で追加された DDDEF エントリを認識します。

以下の手順に従います。

1. MSM50G0.pax.Z を USS ディレクトリにダウンロードします。 ファイルをダウンロードするには、ファイルを CA Technologies ファイル サーバ ディレクトリからユーザの USS ディレクトリに直接 FTP 転送します。
   a. 以下の場所にある FTP サイトに接続します。

      ```
      ftp://ftp.ca.com
      ```

   b. 以下の認証情報を使用して、ftp.ca.com にログインします。

      ユーザ名： anonymous
      パスワード： *自分の電子メール アドレス*

   c. 以下のディレクトリに移動します。

      ```
      cd /CAproducts/ca90s/MSMCCS50/GA/CCS_r14.0/
      ```

   d. 以下の ESD 配布ファイルをバイナリ形式で、メインフレームの HFS ファイルにダウンロードします。

      ```
      bin
      get MSM50G0.pax.Z MSM50G0-CCSR14.pax.Z
      ```

   e. FTP セッションを終了します。
2. CA CSM にログインし、［SMP/E Environments］タブをクリックします。 右ペインでお使いの CA Common Services for z/OS バージョン 14 SMP/E 環境を選択し、［Use as Working Set］をクリックします。

3. ［Products］タブをクリックし、左ペインの［Actions］リストの下の［Install External Package］をクリックします。 表示される［Install External Package］ダイアログ ボックスで、pax ファイルの場所を以下のように入力し、［OK］をクリックします。

   /your_directory_path/MSM50G0-CCSR14.pax.Z

   ［Install External Package］ダイアログ ボックスが閉じ、［Base Installation］ウィザードが開き、［Welcome］の手順に進みます。

4. ［Next］をクリックして［Features］手順に進み、［Full Install］を選択し、［Next］をクリックします。

   ［Prerequisites］手順が表示されます。

5. 前提条件がない場合、［Next］をクリックしてこの手順をスキップします。

   ［SMP/E Environment］手順 1/3 が、［Create a New SMP/E Environment］や、既に作業セットにある SMP/E 環境のような複数のオプションで表示されます。

   注: SMP/E Environment 定義が表示されない場合は、［Cancel］をクリックし、手順 1 で別の CA Common Services for z/OS バージョン 14 SMP/E 環境を選択してこの手順を再開します。 ［Create a New SMP/E Environment］をクリックしないでください。

6. CA Common Services for z/OS バージョン 14 SMP/E 環境を選択し、［Next］を 2 回クリックし（［SMP/E Environment］手順 2/3 を更新することはできません）、［SMP/E Environment］手順 3/3 に進みます。

7. ワークの DDDEF パラメータを指定し、［Next］をクリックして［Target Zone］手順 1/3 に進みます。

8. CA Common Services for z/OS バージョン 14 インストールと関連付けられたゾーンを選択し、［Next］をクリックして［Target Zone］手順 2/3 に進みます。

   CA CSM は［Target Zone］手順 2/3 の下の部分に、SMS またはデータ セット ターゲット ライブラリ割り当てパラメータを表示します。

9. SMS またはデータ セット ターゲット ライブラリ割り当てパラメータを指定し、［Next］をクリックして［Target Zone］手順 3/3 に進みます。

   注: CA CSM がこれらのフィールドに事前入力する値を使用できます。それらの値は、CA Common Services for z/OS バージョン 14 をインストールしたときに設定した値です。

10. ［Next］をクリックし、［Distribution Zone］手順 1/3 に進みます。

    注: RO44235 がインストールされているが、HOLDDATA で提供されるサンプル ジョブが実行されなかった、あるいは正しく実行されなかった場合、CAW0SCST データ セットが表示される場合があります。

11. CA Common Services for z/OS バージョン 14 インストールに関連付けられたゾーンを選択し、［Next］をクリックして［Distribution Zone］手順 2/3 に進みます。

12. SMS またはデータ セット配布ライブラリ割り当てパラメータを指定し、［Next］をクリックして［Distribution Zone］手順 3/3 に進みます。

    注: CA CSM がこれらのフィールドに事前入力する値を使用できます。それらの値は、CA Common Services for z/OS バージョン 14 をインストールしたときに設定した値です。

13. ［Next］をクリックして［Summary］手順に進み、インストール サマリを確認し、［Install］をクリックしてインストール プロセスを完了します。

    注: RO44235 がインストールされているが、HOLDDATA で提供されるサンプル ジョブが実行されなかった、あるいは正しく実行されなかった場合、AETNSCST データ セットが表示される場合があります。

CETN500 で配布されたロード モジュールに一致する CA Datacom/MSM SQL プランは、DDDEF CAW0EXP によって示されるライブラリ内にあり、MSMC*SQL という形式のメンバ名です。 CA CSM 用に CA Datacom/DB へプランをインポートするために使用されるサンプルの JCL は、CAW0JCL に示されるサンプルの JCL ターゲット ライブラリ内のメンバ MSMCXPLN として提供されます。

CETN500 DDDEF エントリ

CETN500 は以下の DDDEF 名を使用します。

ターゲット ゾーン	配布ゾーン	用途
CAW0PLD	AETNMOD	モジュール
CAW0JCL	AETNJCL	サンプル JCL
CAW0PROC	AETNPROC	サンプル PROCs
CAW0OPTN	AETNOPTN	オプションのメンバ

ターゲット ゾーン	配布ゾーン	用途
CAW0SDF	AETNSDF	サイド デッキ
CAW0EXP	AETNEXP	CA Datacom/MSM SQL プラン
CAW0XML0	AETNXML0	CA CSM SCS アドレス空間 XML
CAW0SCST	AETNSCST	SCS テンプレート

ターゲットの DDDEF CAW0XML0 のみが CETN500 に使用される一方、他のすべてのターゲットも CA Common Services for z/OS の他の機能によって使用されます。

第 4 章: インストール後のタスク

このセクションには、以下のトピックが含まれています。

IPL での CA Datacom/MSM SVC のロードのための CAIRIM セットアップ

CAIRIM サービスは、動的な一連の初期化ルーチン用の CA Common Services for z/OS の共通ドライバです。 CA CSM セットアップ ユーティリティは、現在の初期プログラム ロード（IPL）に CA Datacom/MSM スーパーバイザ コール（SVC）をロードします。 CAIRIM をセットアップし、各 IPL 中に SVC を自動的にロードします。

注: CA MSM r3.1 からアップグレードしている場合、別の SVC を使用する必要があります。ユーザが CA CSM の既存顧客で、CA MSM V4.0 あるいはそれ以降のバージョンから移行している場合、このパラメータ値は以前のバージョンと同じ値でかまいません。 CA Datacom Version 12.0 の既存インスタンスと同じ SVC を使用している場合、このタスクを実行する必要はありません。 このタスクは、その既存インスタンスに対してすでに実行済みです。

以下の手順に従います。

1. CAIRIM のスタートアップ プロシージャに、以下の*いずれか*のステートメントを追加します。

   - CA Datacom/MSM SVC のみをロードする場合は、以下のステートメントを使用します。

     ```
     //DBLIB DD DSN=run_time_caaxload,DISP=SHR
     ```

   - 既存の CA Datacom SVC とは異なる CA Datacom/MSM SVC をロードする場合は、以下のステートメントを使用します。

     ```
     //DBLIBx DD DSN=run_time_caaxload,DISP=SHR
     ```

   run_time_caaxload

   CAAXLOAD CA Datacom/MSM ライブラリの名前を指定します。

   x

   他の CAAXLOAD CA Datacom ライブラリと区別するために、ddname にサフィックスを指定します。

   制限： 英数で 1 ～ 3 文字

   IPL 実行時に CA Datacom/MSM SVC をロードするように CAIRIM サービスが設定されます。

2. STEPLIB に以下のステートメントを追加します。

   DSN=*run_time_caaxload*,DISP=SHR

   run_time_caaxload

   CAAXLOAD CA Datacom/MSM ライブラリの名前を指定します。

   注: この STEPLIB の一部であるすべてのデータ セットと同様に、CA Datacom/MSM CAAXLOAD ターゲット ライブラリは APF 許可される必要があります。

3. CAIRIM スタートアップ JCL プロシージャ（通常は CAS9 プロシージャ）によって参照される PARMLIB メンバに、以下の*いずれか*のステートメントを追加します。

   - CA Datacom/MSM SVC のみをロードする場合は、以下のステートメントを使用します。

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)   -
     PARM(Dsvc,DBSVCPR,TYP=3)
     ```

   - 既存の CA Datacom SVC とは異なる CA Datacom/MSM SVC をロードする場合は、以下のステートメントを使用します。

     ```
     PRODUCT(CA DATACOM) VERSION(BD12) INIT(DBRIMPR)   -
     PARM(Dsvc,DBSVCPR,TYP=3,L=x)
     ```

   svc

   CA CSM セットアップ ユーティリティ用のオプション ファイルで、SVCNO キーワードによって設定される SVC 番号を指定します。

各ターゲット システム上での CCIDSCSV と CCISPNSV のセットアップ

ロード モジュールおよび SDS 用のサンプル プロシージャは、有用な CA Common Services for z/OS の機能 CETN500 として提供されます。 CETN500 はすべてのサポートされた CA Common Services for z/OS で利用可能です。

注: CAICCI プロトコル サポートの改善についての詳細は、「*CA Common Services for z/OS Administration Guide*」および「*リリース ノート*」を参照してください。

CETN500 のインストールにより、必要に応じてターゲット システム上でアドレス空間 CCIDSCSV または CCISPNSV が作成されます。CCIDSCSV は、ユーザが CA CSM システム レジストリで起動する、すべての Validate アクションに対して開始されます。 CCISPNSV は、ユーザが Software Deployment Service (SDS) で起動する各 Deployment アクションに対して開始されます。CCIDSCSV および CCISPNSV は、それらに関連するタスクが完了した後に終了します。 システム検出モジュールは、CA Common Services for z/OS の基本 FMID、およびその関連する非 PDSE ロード ライブラリにあります。

以下の手順に従います。

1. 以下の CA Common Services for z/OS メンテナンスおよび機能がインストールされていることを確認します。

   CA Common Services for z/OS r12

   - CETN500
   - RO17488
   - RO19624

   CA Common Services for z/OS バージョン 14

   - CETN500

   さらに、これらのバージョンに関連付けられる任意の追加のメンテナンスを、利用可能になったときにインストールします。

   CETN500 は以下のいずれかの場所へモジュールをインストールします。

   - CA Common Services for z/OS r12 用の CAIPLD
   - CA Common Services for z/OS バージョン 14.0 以降用の CAW0PLD

2. 独立したファイル システム (HFS または zFS) を作成し、SMPDIRWK ディレクトリおよび SDS FTP ランディング ディレクトリを格納します。

   ETNI0100 には、zFS ファイル システムを作成するサンプル ジョブが用意されています。

3. 作成したファイル システムをマウントします。SMP/E SMPDIRWK ディレクトリおよび SDS FTP ランディング ディレクトリを、ファイル システム マウント ポイントの下に作成します。

   ETNI0200 には、マウント ポイントを作成して zFS ファイル システムをマウントし、SMP/E SMPDIRWK ディレクトリおよび SDS FTP ランディング ディレクトリを作成するサンプル ジョブが用意されています。

4. 以前に定義したファイル システムおよびマウント ポイントで、SYS1.PARMLIB 内の BPXPRM*xx* メンバが更新されることを確認します。
5. CAIENF プロシージャを修正し、CETN500 が提供する CAIOPTN ライブラリ メンバ MSMSPNPM を、SPNPARMS DD ステートメントに追加します。
6. CA CSM ホストで実行される CAICCI を指すノードと接続ステートメントが、ターゲット システムの CCIPARM ステートメントに存在することを確認します。 これらのノードと接続ステートメントにより、CA CSM ホストおよびすべてのターゲット システムに対する CAICCI ネットワーク接続が保証されます。

   注: CAICCI はプロトコル VTAM LU0、TCPIP、XCF を、システム間の接続パスに使用できます。 1 つまたは複数のプロトコル を使用して、組織のポリシー、手順および標準に最適になるように合わせます。 CAICCI Spawn Facility が CA CSM ホスト システムおよびターゲット システム CAIENF および CAICCI の両方でアクティブであることを確認します。
7. CCISPNSV および CCIDSCSV サンプル プロシージャを、CA Common Services for z/OS ターゲット ゾーン PROC ライブラリ（r12 用の CCS*hlq*.CAIPROC、およびバージョン 14.0 またはそれ以降のバージョン用の CCS*hlq*.CAW0PROC）から STC PROC ライブラリにコピーします。
8. CCISPNSV と CCIDSCSV プロシージャを修正し、組織の標準に合わせます。

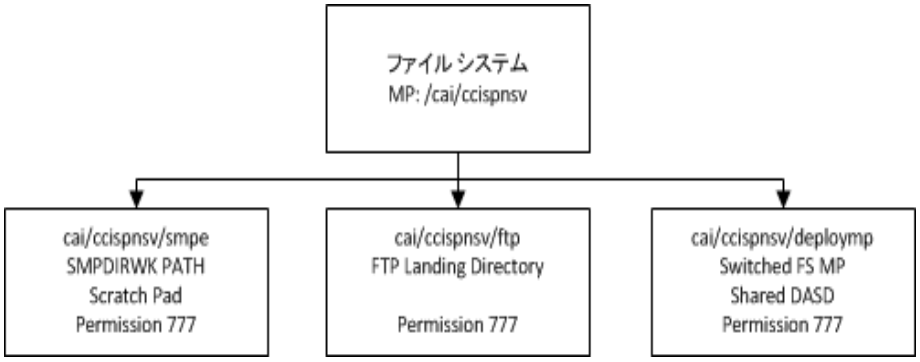
   - 手順 2 および 3 で実施したように、インストールしたファイル システムおよびマウント ポイントに、SMPDIRWK が正しくセットアップされたことを確認します。

     共有 DASD に切り替えたファイル システムを使用している場合、サブディレクトリをマウント ポイント ディレクトリとして作成する必要があります（たとえば、/cai/ccispnsv/msmMPm）。
   - SMPJHOME と SMPCPATH がシステムの Java ホーム ディレクトリおよびホーム SMP クラスを指していることを確認します。

   これらのプロシージャ名を変更できます。ただし、System Discovery の MSMD_DSC_APPLICATION、および SDS の MSMD-DPL_APPLICATION を参照する CAICCI SPAWN パラメータを、すべてのシステムで変更する必要があります。 CAICCI SPAWN パラメータは、SPNPARMS DD ステートメントにより参照される CAIOPTN ライブラリ メンバ MSMSPNPM で定義されています。

9. CCISPNSV プロシージャに関連付けられたユーザ ID に正しいセキュリティ アクセスおよび権限があることを確認します。 関連付けられたユーザ ID は、有効な OMVS セグメントおよび CAIENF と CAICCI 用のユーザ ID に関連付けられるすべてのセキュリティ アイテムを持つ必要があります。 CAIENF のユーザ ID、または自分で定義した ID を使用できます。
10. CA Common Services for z/OS ロード ライブラリが APF 許可されていることを確認します。

CCISPNSV サンプル ディレクトリ ツリー



メンテナンス

CA CSM をセットアップしてインストールした後、それを使用してそれ自体のメンテナンスを行うことができます。

CA CSM SMP/E 環境の CA CSM への移行

CA CSM インストール中に作成した SMP/E 環境を CA CSM に移行する必要があります。

以下の手順に従います。

1. ［SMP/E Environments］タブをクリックし、左側の［Actions］セクション内の［Migrate SMP/E Environment］リンクをクリックします。

   SMP/E 環境の指定を促すプロンプトが表示されます。

2. CA CSM のインストール中に作成した SMP/E 環境の名前を入力し、SMP/E 環境データ セット名を指定し、［Next］をクリックします。

   SMP/E 環境内の機能が表示されます。

3. 情報を確認し、［Next］をクリックします。

   ゾーンのリストが DDDEF の関連付けとともに表示されます。

4. ゾーンを確認し、［Next］をクリックします。

   DDDEF で指定されたパスにマウントされているものがある場合、そのファイル システムの一覧が表示されます。

5. ファイル システムを確認します。 管理する製品の USS ファイル システムとして追加するファイル システムがある場合は、それを選択します。 ［Next］をクリックします。

   移行された SMP/E 環境のゾーンが表示されます。

   注: 実在し、アクセス権があるゾーンのみが表示されます。

6. 各ゾーンのプレフィクスを指定し、［Next］をクリックします。 プレフィクスは、同じ SMP/E 環境への将来ベースのインストール中に、高レベル修飾子（HLQ）のデフォルトとしてのみ使用されます。 基本インストール中にこれらのデフォルトを必要に応じてオーバーライドできます。

   拡張オプションの一覧が表示されます。

   注: グローバル ゾーン用のプレフィクスは自動的に定義され、それを変更することはできません。

7. 利用可能なオプションの一覧を確認し、移行された SMP/E 環境に APPLY する以下のオプションを選択します。

   SMP/E 環境の作業セットへの追加

   移行した SMP/E 環境を作業セットに追加します。

8. ［Next］をクリックします。

   サマリ ページが表示されます。

9. 情報を確認し、［Migrate］をクリックします。

   注: ゾーン DDDEF 用の UCLIN ステートメントを参照するには、一番下の［Show UCLIN］をクリックします。

   タスクの進捗状況を示すダイアログ ボックスが表示されます。タスクが完了したら［Progress］タブの［Show Results］をクリックし、このダイアログ ボックスを閉じます。タスク出力ブラウザが表示され、アクションの詳細を確認できます。［Close］をクリックして、タスク出力ブラウザを閉じます。

   注: タスクが実行中の場合は、他のタスクを実行できます。［Hide］タブをクリックしてダイアログ ボックスを終了し、後で［Tasks］タブでタスクのステータスを表示できます。

   移行が正常に完了した後、SMP/E 環境および関連製品に関する情報は、CA CSM データベースに保存されます。 移行された環境が、左側の［SMP/E Environments］セクションのツリーに表示されます。

CA CSM へのメンテナンスの APPLY

重要: メンテナンスをダウンロードするには、［Product Acquisition Settings］ページで CA CSM ログイン ユーザ名を CA サポート Online Web サイトの登録ユーザと関連付ける必要があります。

以下の手順に従います。

1. 以下の手順を実行し、CA サポート Online Web サイトから取得した CA CSM メンテナンス情報でソフトウェア カタログを更新します。
   a. ［Products］タブに移動し、左側の［Available Products］パネル内で CA Chorus Software Manager を検索します。

      注: ツリーに CA Chorus Software Manager がない場合は、この処理に対し、CA CSM を使用してインストールできる製品のいずれかを使用します。これらの製品は CA CSM にコンポーネントとして反映されているため、メンテナンスもまたそこに反映されます。 詳細については、CA サポート Online Web サイトの CA CSM ページの「Recommended Reading」セクションで「CA Chorus Software Manager Enabled Products」を参照してください。

   b. CA Chorus Software Manager を右クリックし、［Update Product］を選択します。

      このタスクは、完了するのにある程度の時間がかかります。タスクが完了した後、ソフトウェアが正常に取得されたことを確認するメッセージが表示されます。

   c. ［Hide］をクリックして、メッセージを非表示にします。

   d. 右のパネルで CA CSM メンテナンスを検索します。

2. （オプション） 外部のメンテナンスを使用して、テストの修正を追加します。

   注: 外部から CA CSM にダウンロードしたテストの修正の APPLY およびメンテナンスの管理の詳細については、「*ユーザ ガイド*」の「*製品のメンテナンス*」の章を参照してください。

3. メンテナンスを確認し、APPLY します。

   CA CSM 用の SMP/E ターゲット ライブラリおよび USS パスのコンテンツが更新されます。 これらのライブラリとパスは、MSMSetupOptionsFile.properties オプション ファイルの TargetHLQ と MSMPATH キーワードを使用してセットアップされます。

   注: メンテナンスの APPLY および管理の詳細については、「*ユーザ ガイド*」の「*製品のメンテナンス*」の章を参照してください。

4. CA CSM を停止します (P. 154)。

   CA CSM は稼働を停止します。

5. CA CSM ランタイム ライブラリおよび USS パスに CA CSM のメンテナンスを展開します。それらは、MSMSetupOptionsFile.properties オプション ファイルの RunTimeMVSHLQPrefix と RunTimeUSSPath のキーワードを使用してセットアップされます。

   a. JCL(MSMDEPLY) ジョブのカスタマイズ JOB ステートメントを更新し、**deploy** を第 1 引数に指定します。

   b. ジョブをサブミットします。

6. CA CSM を起動します (P. 114)。

   メンテナンスされた CA CSM が操作可能になります。

重要: SMP/E ターゲット ライブラリと USS パス、およびランタイム ライブラリと USS パスを区別してください。 CA CSM はランタイム ライブラリおよび USS パスから実行されます。 メンテナンスを APPLY すると、SMP/E ターゲット ライブラリおよび USS パスのみが更新されます。 CA CSM を停止し、MSMDEPLY ジョブをサブミットして、ランタイム ライブラリおよび USS パスを更新する必要があります。 CA CSM を再起動すると、それらの更新は有効になります。

SQL プランの更新

CA Datacom/MSM SQL プランに影響する更新を適用する必要がある場合があります。 これらの SQL プランは、CA Common Services for z/OS メンテナンスとして提供されます。 CA Common Services for z/OS には、CA Datacom/DB MUF 環境のこれらの SQL プランの更新に使用できるサンプルの JCL メンバ MSMCXPLN が用意されています。

最新の SQL プランの実装

CA Common Services for z/OS SMP/E 環境のサンプル JCL ライブラリにあるメンバ MSMCXPLN はモデル化された JCL で、CA Datacom/MSM SQL プランの更新に使用することができます。 少なくとも 1 つのモジュール要素と、関連する SQL プラン要素が含まれる PTF を APPLY する場合は常に、この JCL を実行します。 ユーザは、PTF を APPLY するプロセス中に発生する ++HOLD 条件アクションにより、サンプルの JCL メンバ MSMCXPLN に修正と実行が必要であると通知されます。 ++HOLD コメントに示された以下の手順に従い、このメンバを適切に修正して実行します。

注: CETN500（MSMCCS 5.0）が CA Common Services for z/OS に存在する場合は、SQL プランが CA Datacom/MSM データベース リリース 5.1 および実行中の CA Common Services for z/OS ライブラリで同期されることを確認してください。DDDEF CAW0EXP で示される CA Common Services for z/OS ライブラリの、各 MSMC*SQL メンバに対し CA Common Services for z/OS JCL ライブラリから MSMCXPLN ジョブをサブミットします。

サンプル JCL のデータ セット リファレンス

適切なサンプル JCL ライブラリのデータ セット名を特定するには、DDDEF 要素 CAW0JCL を参照してください。

SQL プランのデータ セット リファレンス

適切な SQL プラン ライブラリのデータ セット名を特定するには、DDDEF 要素の CAW0EXP を参照してください。

旧バージョンからのコードを含んだ SCS アドレス空間での CA CSM リリース 5.1 の実行

CA CSM リリース 5.1 には CA MSM V4.0 の SQL プランがすべて含まれるとは限りません。 このことにより、旧バージョン（CETN400）の SCS アドレス空間に接続するとき、SQL -124 リターン コードを受け取る場合があります。

CA MSM V4.0 から CA CSM リリース 5.1 へのアップグレードが完了したら、このセクションで説明される以下の手順に従い、CETN400 ライブラリから SQL プランをインポートします。 手順では、CETN500 を CETN400 に読み替えます。 1 つ以上の CA CSM アドレス空間に接続する場合、それらのアドレス空間には引き続き旧バージョン（CETN400）のコードが含まれており、CA Common Services for z/OS を CETN500 にアップグレードできない場合は、この手順を実施します。

詳細:

CA CSM アドレス空間が正しく機能しない (P. 311)

CA CSM からのメンテナンスのバックアウト

APPLY した（しかし ACCEPT されていない）メンテナンスを、CA CSM からバックアウトできます。 CA CSM メンテナンスをバックアウトするとき、まず CA CSM リストア アクションを使用し、SMP/E ターゲット ライブラリと USS パスを更新します。 その後、CA CSM を停止し、MSMDEPLY ジョブをサブミットしてランタイム ライブラリと USS パスを更新する必要があります。 CA CSM を再起動すると、それらの更新は有効になります。

以下の手順に従います。

1. RESTORE アクションを使用してメンテナンスをバックアウトします。

   CA CSM 用の SMP/E ターゲット ライブラリおよび USS パスのコンテンツが更新されます。 これらのライブラリとパスは、MSMSetupOptionsFile.properties オプション ファイルの TargetHLQ と MSMPATH キーワードを使用してセットアップされます。

   注: メンテナンスのバックアウトの詳細については、「*ユーザ ガイド*」の「*Maintaining Products*」の章を参照してください。

2. CA CSM を停止します (P. 154)。

   CA CSM は稼働を停止します。

3. 更新された SMP/E ターゲット ライブラリと USS パスを CA CSM ランタイム ライブラリおよび USS パスのコンテンツに展開します。それらは、MSMSetupOptionsFile.properties オプション ファイルの RunTimeMVSHLQPrefix と RunTimeUSSPath のキーワードを使用してセットアップされます。

   a. JCL(MSMDEPLY) ジョブのカスタマイズ JOB ステートメントを更新し、*backout* を第一引数に指定します。

   b. ジョブをサブミットします。

4. CA CSM を起動します (P. 114)。

   CA CSM はメンテナンスなしで稼働可能になります。

フェイルセーフ バックアウト

まれに、CA CSM に対する不正なテスト修正により、CA CSM が稼働不能になることがあります。その問題を解決するため、MSMDEPLY ジョブを使用して CA CSM ランタイム ライブラリと USS パスを稼働可能な状態にリストアすることができます。第一引数に *backout* を指定して MSMDEPLY ジョブをカスタマイズし、サブミットします。ジョブが完了した後、CA CSM を再起動し、通常の手順に従って不正なテスト修正をバックアウトします。

MSMDEPLY ジョブに *deploy* を指定して実行すると、現行の CA CSM ランタイム ライブラリおよび USS パスのコピーが、展開の前に保存されます。MSMDEPLY ジョブに *backout* を指定して実行すると、CA CSM ランタイム ライブラリおよび USS パスの最後に保存されたコピーが展開されます。

重要: ただ 1 つの CA CSM ランタイム ライブラリおよび USS パスのコピーがメンテナンスされます。 MSMDEPLY ジョブに *deploy* を指定して実行するたびに、最後に保存したランタイム ライブラリおよび USS パスは、新しいコピーで置き換えられます。 MSMDEPLY ジョブに *backout* を指定して何度実行しても、複数保存されたコピーのバックアウトはできません。

CA CSM の停止

CA CSM を停止する場合（たとえばメンテナンス中など）、CA CSM の開始 (P. 114)とは逆の順序で CA CSM を停止します。

以下の手順に従います。

1. 以下の z/OS システム コマンドを入力します。

   ```
   P MSMTC
   ```

   CA CSM アプリケーション サーバ (P. 329)は正常に終了し、以下のメッセージがシステム コンソールに表示されます。

   ```
   MSM0011I CA CSM HAS TERMINATED SUCCESSFULLY
   ```

   注: このメッセージが表示されない場合、CA CSM は稼働停止に失敗しているため、以下のコマンドを使用して、強制的にシャットダウンする必要があります。

   ```
   F MSMTC,APPL=FORCESHUTDOWN
   ```

   強制シャットダウンが完了した後、以下のメッセージがシステム コンソールに表示されます。

   ```
   MSM0012W CA CSM TERMINATION WAS FORCED
   ```

   重要: 強制的にシャットダウンする場合、データの一部が失われる可能性があります。そのため、標準的な停止方法が作動しない場合のみ、この方法を使用してください。

   CA CSM アプリケーション サーバが停止した後、Tomcat ジョブが停止します。

2. MSMDBSVP JCL メンバをサブミットするか、または MSMDBSRP PROCLIB メンバを開始します。

   CA Datacom/MSM サーバが停止します。

3. MSMMUFP ジョブまたはスターティッド タスクをサブミットします。

   CA Datacom/MSM MUF が停止し、CA CSM は稼働停止します。

CA CSM のバックアップおよびディザスタ リカバリ

災害の場合に備え、CA CSM 環境の定期的なバックアップの実施をお勧めします。

ディザスタ リカバリの処理を開始する前に、CA CSM によって管理されるすべての SMP/E 環境およびデータ セットをバックアップします。

ディザスタ リカバリを実施するときは、以下の手順に従います。

1. CA CSM によって管理されるすべての SMP/E 環境をリカバリします。
2. CA CSM 自体をリカバリします。

CA CSM が最初にインストールされた環境と同一の環境に、CA CSM をリカバリさせる必要があります。 すなわち、リカバリ システムの以下の設定は、元のシステムのものと同じである必要があります。

- TCP/IP ポート、DASD、HLQ などのオペレーティング システム設定
- CA Datacom/MSM SVC
- CA CSM に必要な APF 許可データ セットの設定
- Java

  注: CA CSM がサポートするバージョンの Java である必要があります。
- TCP/IP 設定、ホスト名、IP アドレス、展開で指定されたシステムの CCI-ID

注:

- リカバリ システム用の SAF 設定には、CA CSM をセットアップしたときに使用した、すべての変更済み SAF 設定が含まれる必要があります。
- CA Datacom/DB ユーティリティ関数 DBUTLTY を使用した CA Datacom/MSM データベース データ領域の定期的なバックアップにより、お使いの製品へのアクセシビリティに影響を与える、スケジュールされたイベントまたはスケジュール外のイベント中の CA Datacom/MSM データを保護することができます。 データベースを再編成する方法の詳細については、「*Best Practices Guide*」を参照してください。

CA CSM のバックアップ方法

CA CSM のバックアップは、いくつかの手順で処理されます。

注: バックアップについては、ユーザのサイトと環境にとって適切な方法を選択し、使用してください。 バックアップの管理は、ディザスタ バックアップ ルーチンの一部である必要があります。

以下の手順に従います。

1. CA CSM アプリケーション サーバ (P. 329) を停止します。
2. 以下のオペレーティング システム設定をバックアップします。
   - ポート、DASD、HLQ などのオペレーティング システムの設定
   - Java

     注: CA CSM がサポートするバージョンの Java である必要があります。
   - TCP/IP
   - SAF

   注: CA Datacom/MSM SVC は同じものになることが想定され、APF 許可されたデータ セットのリストは保存されます。
3. 展開ファイル システム、ソフトウェア カタログ ファイル システムなどを表すデータ セットの一覧を取得します。 データ セットはマウント ポイント テーブルの MP_DATASET 列に格納されます。

   注: データ セットの一覧を取得するため、SQL ステートメントを実行する JCL をサブミット (P. 157)できます。
4. CA Datacom/MSM サーバおよび CA Datacom/MSM MUF を停止します。
5. 以下の CA CSM データ セットをバックアップします。
   - マウント ポイントを表すデータ セット (P. 262)

     これらのマウント ポイントに個別のファイル システムを割り当てなかった場合は、以下の手順に従います。

     a. 存在する場合には、以下のファイル システムでマウントされたすべてのファイル システムをマウント解除します。

```
/u/users/msmserv/msminstall
/u/users/msmserv/msm
/u/users/msmserv/msmruntime
/u/users/msmserv/mpm
```

b. /u/users/msmserv に相当するディレクトリ構造をバックアップします。

- マウントポイント テーブルから取得したすべてのデータ セット。
- オプション ファイル（MSMSetupOptionsFile.properties）で指定された HLQ（CSIHLQ、TargetHLQ、DlibHLQ、DatabaseHLQ、RunTimeMVSHLQPrefix）の下のすべてのデータ セット。

SQL ステートメントを実行する JCL

マウントポイント テーブルのコンテンツを検出する SQL ステートメントを実行するためにサブミットする JCL の例を以下に示します。

```
//*******************************************************************************
//*******************************************************************************
//*                                                                             *
//*JOBLIB DD DSN=HLQ.CUSLIB replace HLQ with HLQ of your CA CSM installation  *
//*          DSN=HLQ.CAAXLOAD replace HLQ with HLQ of your CA CSM installation*
//*                                                                             *
//*******************************************************************************
//*******************************************************************************
//B2UP     OUTPUT DEST=LOCAL,JESDS=ALL,DEFAULT=Y,
//         PAGEDEF=32D3,CHARS=GT20,FORMDEF=P2B111
//JOBLIB   DD DSN=HLQ.CUSLIB,
//         DISP=SHR
//         DD DSN=HLQ.CAAXLOAD,
//         DISP=SHR
//         DD DSN=SYSDEV.CCS.LINKLIB,
//         DISP=SHR
//         DD DSN=CEE.SCEERUN,DISP=SHR
//         DD DSN=CEE.AIGZMOD1,DISP=SHR
//*
//SQLEXEC  EXEC PGM=DBSQLPR,
//       PARM='prtWidth=1500,inputWidth=80'
//SYSUDUMP DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//STDOUT   DD  SYSOUT=*
//OPTIONS  DD  *
AUTHID=CASWMGT
/*
//SYSIN    DD  *
   SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
/*
```

JCL をサブミットしてマウントポイント テーブルのコンテンツを検出した後に受信する出力の一部を以下に示します。

```
Command Line Options
_____________________
INPUTWIDTH=80
PRTWIDTH=1500
Option File Options
____________________
AUTHID=CASWMGT
INPUT STATEMENT:
SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
MP_DATASET
VARCHAR(45)
_____________________________________________
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
...
```

入力ステートメントの後に返却されるデータ セットで、バックアップする必要があるものを以下に示します。

```
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
```

バックアップからの CA CSM のリカバリ方法

バックアップから CA CSM をリカバリするには、以下の手順に従います。

1. オペレーティング システム設定をリカバリします。
2. CA CSM データ セットをリカバリします。
3. CA CSM を起動します (P. 114)。

メンテナンスが理由で CA CSM が失敗する場合のリカバリ

CA CSM が依存するソフトウェアにメンテナンスを APPLY すると、CA CSM が失敗することがあります。また、CA CSM を使用してその問題を修正できない可能性があります。

- メンテナンスが CA CSM 自体に APPLY されている場合は、フェイルセーフ バックアウト メソッド (P. 153) を使用し、CA CSM を稼働可能な状況に戻します。
- CA CSM に影響する別の製品に属するソフトウェアにメンテナンスが APPLY されたことが原因で問題が発生する場合、SMP/E バッチ ジョブを使用して、新しい修正メンテナンスを APPLY する、またはメンテナンスをバックアウトして、CA CSM を再起動します。 この処理には CA CSM 自体への新しい修正メンテナンスの APPLY が含まれます。CA CSM 自体に新しい修正メンテナンスを APPLY する場合、CA CSM を再起動する前にメンテナンスを展開する必要があります。

USS ディレクトリのクリーン アップ

CA CSM インストール pax ファイルをダウンロードして処理した後は、USS ディレクトリからそのファイルを削除します。 これらのアクションにより、後続のダウンロードのためにファイル システムのディスク スペースが解放されます。 以下の項目を削除できます。

- pax ファイル
- pax コマンドで作成され、すべてのファイルが格納されたパッケージ固有のディレクトリ

注: 今後参照することに備え、SMP/E 以外のインストール データ セットを保持してください。

以下の手順に従います。

1. ダウンロードされたパッケージの USS ディレクトリに移動します。
2. 以下のコマンドを入力して、pax ファイルを削除します。

   `rm paxfile`

   paxfile

   ダウンロードした pax ファイルの名前を指定します。

3. 以下のコマンドを入力して、パッケージ固有のディレクトリを削除します。

   `rm -r package_specific_directory`

   package_specifc_directory

   pax コマンドによって作成されたディレクトリを指定します。

   注: TSO ISHELL を使用して pax ファイルおよびパッケージ固有のディレクトリに移動し、D 行コマンドを使用して、それらを削除することもできます。

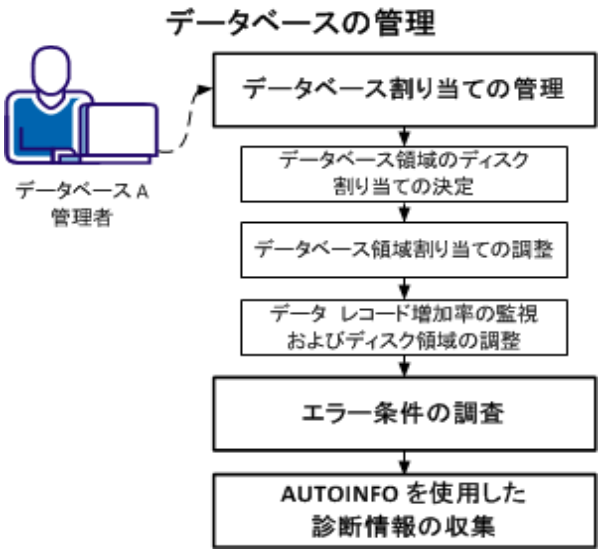
第 5 章: データベース管理

CA CSM には、CA CSM 用にカスタマイズされた CA Datacom/MSM の変形バージョンが用意されています。 これは CA Datacom/MSM として参照され、CA CSM はこの変形バージョンを基本のデータ リポジトリとして使用します。

このセクションには、以下のトピックが含まれています。

データベース管理プロセスの動作

以下の高レベル タスクを実行し、CA Datacom/MSM データベースを管理します。



1. 以下のようにして、データベース割り当てを管理します。
   a. 既存の CA CSM データベース領域に対し、現行のディスク割り振りを決定します (P. 163)。
   b. データベース スペースの割り振りを調整します (P. 165)。
   c. データ レコードの増加をモニタし、ディスク スペースを調整します (P. 166)。
2. エラーが発生した場合、エラーの状態を調査します (P. 172)。
3. AUTOINFO 機能を使用し (P. 174)、診断情報を収集します。

データベース割り当ての管理

以下のいずれかの状況により引き起こされる、ファイルがフルの状態が理由で、ディスク割り振りを増やす必要があることがあります。

- 製品更新の頻度の増加
- 新しい製品のインストール
- CA CSM のアップグレード

ユーザの CA Datacom/MSM データ領域とインデックスに対するディスク割り振りへの変更は、以下のいずれかの理由により発生した可能性があります。

- CA Datacom/MSM Dynamic Extend 関数の内部的自動実行
- CA Datacom/MSM DBUTLTY EXTEND 関数の手動実行
- 以下の作業の実行。
  - CA Datacom/MSM データ領域バックアップを実行した
  - 関連する CA Datacom/MSM データ領域データ セットを削除した
  - データ セットを再配置した
  - CA Datacom/MSM DBUTLTY INIT LOAD を実行し、データ領域を再ロードした

注: すべての CA CSM データベース データ セットのディスク割り振りが、少なくともサイトの現行の割り振りと同じであることを確認することをお勧めします。

ディスク割り振りを正しく管理するには、以下の手順を実行する必要があります。

1. 既存の CA CSM データベース データ セット用の現行のディスク割り振りを決定 (P. 163)します。
2. CA CSM アップグレードを開始する前に、CA Datacom/MSM ディスク スペースの割り振りを調整します (P. 165)。
3. CA CSM の稼働後、ある期間にわたってデータ レコードの増加をモニタし (P. 166)、その結果に基づき CA Datacom/MSM ディスク スペースを調節します。

既存の CA CSM データベース領域に対する現行のディスク割り振りの決定

この手順を使用し、サイトの現行のデータベース割り当てを決定し、CA CSM アップグレード ジョブ ストリームに適切な変更を加える準備ができます。

注: samplib データ セットの任意のジョブをサブミットする前に、この一連の手順を実行する必要があります。

以下の手順に従います。

1. CA Datacom/MSM がアクティブであることを確認します。

   a. 以下のオンライン コンソール コマンドを入力します。

      ```
      /F dbjobnm,STATUS
      ```

      dbjobnm

      CA CSM Multi-User 機能（MUF）の実行可能ジョブ名を指定します。

      コンソール DB ステータス コマンドが発行されます。 このコマンドの出力は、メインフレーム コンソールと、CA Datacom/MSM ジョブの SYSOUT クラスの JESMSGLG に表示されます。

      CA Datacom/MSM がアクティブな場合、以下の情報メッセージが表示されます。

      ```
      DB01327I - MULTI-USER AVAILABLE
      ```

   b. 必要に応じて、表示されるその他のメッセージに対する適切な処理を実行します。

   c. CA Datacom/MSM がアクティブでない場合、samplib データ セットからジョブ メンバ MSMMUFS をサブミットして、CA Datacom/MSM 環境を起動できます。

2. Directory（CXX）Space レポートを実行します。

   Directory（CXX） レポート サンプル JCL (P. 169) を使用し、CA CSM DBID 4000 用のスペース レポートを作成します。

   CA Datacom/MSM 領域に割り当てられたトラック数に関する情報、およびその他の重要なスペースの使用状況の情報が生成されます。 制御ステートメントのキーワードと値に TYPE=A を入力し、この情報を作成します。

   注: Directory（CXX） レポートの機能の詳細については、「*CA Datacom/DB DBUTLTY Reference Guide z/OS*」の「REPORT（Generate Reports）」の章を参照してください。本書の情報は、CA Datacom/MSM にも適用されます。

3. Directory（CXX）Space レポートの出力を確認し、ディスク スペースを分析します。

   注: Directory（CXX） レポート サンプル JCL (P. 169) を参照できます。

   レポートはデータ領域名（3 文字）を表示します。 各データ領域は、メインフレームのデータ セットと関連付けられます。データ領域名は、JCL の DD カードに表示される、関連するデータ領域のデータ セット名のサフィックスです。

4. 各データ領域の、パーセント フルおよび割り振り済みトラックの数を示します。

JCL 割り振り調整

任意の JCL ジョブ ストリームに対するディスク割り振りを調整する必要がある場合があります。

新規インストールについては、ジョブ CSMN5106 が、通常の CA CSM 使用状況に適した CA Datacom/MSM ディスクの初回割り振りを実行します。旧バージョンからのアップグレードについては、ジョブ CSMU*xx*06 が通常の CA CSM 使用状況に適している CA Datacom/MSM ディスクの初回割り振りを実行します。

xx

どのバージョンからアップグレードするかを示します.

計画された CA CSM の使用方法、および現在の DASD ディスク プール リソースに基づき、プライマリおよびセカンダリの CA Datacom/MSM ディスク スペースを調節してユーザのサイト要件に合わせる必要がある場合があります。 アップグレードを実行している場合は、新しいディスク割り振りが現在使用中の CA Datacom/MSM ディスク スペースと少なくとも等しいことを確認します。

MSMSetup.sh シェル スクリプトを実行するときにディスク スペース割り振りを調整するには、以下のいずれかを実行します。

- Review インストール モードの場合は、自動ジョブ サブミットの前に JCL をプレビューする場合は、プロンプトに対して **Y**（Yes）と入力します。
- Manual インストール モードの場合は、ジョブ サブミットの前に、*runtimeHLQ*.JCL データ セットを必要に応じて修正します。

以下のディスク割り振りが CA Datacom/MSM データ領域 XML、すなわちデータ セット *dbHLQ*.XML4000 で使用されます。*dbHLQ* は、CA Datacom/MSM データ セットの高レベル修飾子です。

- CA CSM 以外の製品の設定機能については、最小で 1 シリンダが必要です。
- CA CSM 製品設定の少量での使用については、最小で 300 シリンダが必要です。
- CA CSM 製品設定の大量の使用については、平均で最小 3,000 シリンダが必要です。

データ レコード増加のモニタおよびディスク スペースの調整

組織のディスク スペースを徐々に増加させる必要がある場合があります。

CA CSM の稼働後に、Directory（CXX）レポートを定期的に実行し、すべての期間で現在の Directory CXX レポートと履歴を比較して将来的な増加を予測し、それに応じて CA Datacom/MSM ディスク割り振りを調節できるようになります。

以下の方法を使用して、ディスク スペースを調整します。

- DBUTLTY EXTEND 関数 (P. 166)の使用。
- ディスク スペースの手動調整 (P. 167)。 この方法では、ユーザのデータをバックアップし、関連するデータ セットを削除し、データ セットを再度割り振って初期化し、データを再ロードすることが必要です。

DBUTLTY EXTEND 関数

DBUTLTY EXTEND 関数を使用し、データ領域またはインデックス領域で利用可能なスペースを増加させます。以下の目的のために、DBUTLTY EXTEND 関数を使用することができます。

- 将来の増加に対応する計画を立てるとき
- 領域またはインデックスがフルか、ほとんどフルのとき

DBUTLTY の EXTEND 関数は、既存のデータ領域またはインデックス領域を拡張し、取得したスペースをフォーマットします。 この関数はデータ領域やインデックス領域の制御レコードも更新し、CA Datacom/DB に追加スペースが利用可能であることを通知します。

注: EXTEND 関数を使用して領域のサイズを減少させることはできません。

EXTEND 関数が完了すると、システムにそれ以上の変更を加えることなく、新しい領域をすぐに使用できます。 EXTEND 関数の完了後に開始したすべてのジョブは、この新しく割り当てられたスペースを使用できます。

注: 詳細については、「*CA Datacom/DB DBUTLTY Reference Guide z/OS*」の「EXTEND（Extend Data or Index Areas）」の章を参照してください。

ディスク スペースの手動調整

手動でディスク スペースを調整するには、以下の手順を実行する必要があります。

- データのバックアップ
- 関連するデータ セットの削除
- データ セットの再割り振り
- 初期設定
- データの再ロード

以下の手順に従います。

1. Directory（CXX）レポートを実行し、現在のディスク割り振りを決定します（P. 163）。
2. CA CSM データベースの使用を必要とする、CA CSM アプリケーション サーバの起動や、CA CSM に関連付けられた CA Datacom/MSM サーバ リージョンなどの、すべてのアクティビティが停止されていることを確認します。

   以下の関連するアクションを実行し、CA CSM アプリケーション サーバおよび CA Datacom/MSM サーバを停止します。

   - 「**P MSMTC**」と入力して、CA CSM アプリケーション サーバを停止します。
   - MSMDBSVP JCL メンバまたは MSMDBSRP PROCLIB メンバをサブミットし、CA Datacom/MSM サーバを停止（一時停止）します。

3. CA Datacom/MSM がアクティブであることを確認します。
   a. 以下のオンライン コンソール コマンドを入力します。

      ```
      /F dbjobnm,STATUS
      ```

      dbjobnm

      CA CSM Multi-User 機能（MUF）の実行可能ジョブ名を指定します。

      コンソール DB ステータス コマンドが発行されます。 このコマンドの出力は、メインフレーム コンソールと、CA Datacom/MSM ジョブの SYSOUT クラスの JESMSGLG に表示されます。

      CA Datacom/MSM がアクティブな場合、以下の情報メッセージが表示されます。

      ```
      DB01327I - MULTI-USER AVAILABLE
      ```

   b. 必要に応じて、表示されるその他のメッセージに対する適切な処理を実行します。

   c. CA Datacom/MSM がアクティブでない場合、samplib データ セットからジョブ メンバ MSMMUFS をサブミットして、CA Datacom/MSM 環境を起動できます。

4. CA Datacom/MSM DBUTLTY BACKUP 関数を実行し、CA Datacom/MSM データベース（DBID 4000）をバックアップします。samplib データ セットのメンバ B4KBKUP を使用してモデル化し、バックアップ ジョブ ストリームを構築できます。

5. CA Datacom/MSM データベースのバックアップを正常に作成した後、TSO または IBM のユーティリティを使用して、関連する CA CSM データベース（DBID 4000）領域およびインデックス データ セットを削除します。

6. 以下のいずれかの方法を使用し、CA CSM データベース（DBID 4000）領域およびインデックス データ セットを、新しいディスク割り振りを使用して再度割り振ります。
   - TSO
   - IBM ユーティリティ
   - CA Datacom/MSM DBUTLTY INIT ジョブ ストリームの一部としてのインクルード データ セット名

7. DBUTLTY BACKUP 手順で実行された現在のバックアップを使用して、CA Datacom/MSM DBUTLTY INIT および LOAD 関数を実行します。 samplib データ セット内のメンバ B4KLOAD をコピーし、それをカスタマイズして CA CSM データベースをリストアできます。

   ディスク割り振りが調整され、サイトの CA CSM のアクティビティに対応するために必要なスペースが確保されます。

   注: 入力 DD カードを、前の手順で作成された現行のバックアップで必ず置換してください。

8. Directory（CXX）レポートを実行し、正常に変更されたことを確認します。

9. CA Datacom/MSM サーバおよび CA CSM アプリケーション サーバを起動します。

   CA CSM を使用して、通常稼働できます。

Directory（CXX）レポートのサンプル JCL

Directory のスペース使用率レポートを生成するコマンドを以下に示します。

```
//jobname（注参照）
// EXEC PGM=DBUTLTY,REGION=2M
//STEPLIB（注参照）
//CXX      DD DISP=SHR,DSN=RunTimeMVSHLQPrefix.cxx   Directory (CXX) data set
//SYSIN  DD * Command Input
REPORT AREA=CXX,DBID=4000,TYPE=A
```

注: ご自分の JCL を準備するためのガイドとして、このサンプル JCL を使用してください。 以下のガイドラインに準拠していることを確認します。

- *RunTimeMVSHLQPrefix.cxx* を、ユーザ サイトの CA Datacom/MSM CXX ディレクトリ用のメインフレームのデータ セット名で置換します。
- ステートメント内の小文字は、ユーザが入力する必要がある値を示します。
- 任意の JOB ステートメントをはじめとする、ユーザ サイト、およびインストール標準と仕様に対するすべてのステートメントをコーディングします。

- すべてのデータ セット名およびライブラリ名は、ユーザ サイトでのインストールの正しい名前で指定する必要があります。
- 多くの例において、REGION= または SIZE= のパラメータは、EXEC ステートメントで表示されます。 表示された値は、ほとんどのインスタンスで最適化されていますが、特定のニーズに対して値を調整することができます。

Directory CXX レポートのサンプル

```
CONTROL CARD(S)
                    .........1.........2.........3.........4.........5.........6.........7.........8
                      REPORT AREA=CXX,DBID=4000,TYPE=A

                    FUNCTION=REPORT
                       AREA=CXX
                       DBID=04000
                       TYPE=A
```

そのレポートは以下の内容を表示します。

- 入力されたコマンドそのもの。
- 発生した、および予測されるキーワードの分析。 エラーは、左側余白の注にフラグが付けられます。
- 構文処理に関連したメッセージ。

```
 DATACOM/AD                  DATA AREA SPACE UTILIZATION REPORT
-AREA DATA       TOTAL        TOTAL       TOTAL        USED    PERCENT    PARTIALLY  AREA REUSE
 NAME BASE      TRACKS      RECORDS      BLOCKS      BLOCKS  FULL   MAX  EMPTY BLKS    OPTION

 CXX               525          N/A       6,300         342     5     5         N/A  N/A
 IXX  4000         900          N/A      10,800       5,445    50    50         N/A  N/A
  AUD 4000       5,010      254,258      10,020       4,398    43    43           1  RANDOM
  INV 4000       3,000      148,724      18,000      14,538    80    80           0  RANDOM
  JNL 4000       1,125       91,359       6,750       5,182    76    76           0  RANDOM
  PCY 4000         510       34,573       6,120       2,449    40    40           1  RANDOM
  SCS 4000       2,010       59,111      12,060       1,136     9     9           1  RANDOM
  SDS 4000         750       16,809       4,500       3,145    69    69           1  RANDOM
  SRG 4000       1,005        1,616       6,030         142     2     2           1  RANDOM
  XML 4000      33,000       61,858      66,000      61,860    93    93           0  RANDOM
```

このレポートでは、以下の情報が提供されます。

AREA NAME および DATA BASE

その領域が含まれるデータベースの DATACOM-ID。 Directory（CXX）のサマリ統計は、常に最初の行に表示されます。

TOTAL TRACKS

その領域で使用される CA Datacom/MSM によって割り当てられ許容されるトラックの数。 割り当て済みトラック（ブロック）の実際の数がこれより多い場合は、EXTEND 関数を実行し、CA Datacom/MSM がスペースを利用できるようにします。

TOTAL RECORDS

データ領域について、その領域のレコード数。 メンテナンス処理中にシステム障害が発生した場合、この数は正確ではないことがあります。

TOTAL BLOCKS

その領域のブロック数。

USED BLOCKS

データがあるブロック数。 メンテナンス処理中にシステム障害が発生した場合、この数は正確ではないことがあります。

PERCENT FULL および MAX

パーセント フルは、使用済みブロックを総ブロックで割ることで計算されます。 値は偶数のパーセントでレポートされます。 少数は切り捨てられます。

*ハイウォーター マーク*と呼ばれることもある最大パーセンテージは、最大使用済みブロックを総ブロックで割ることで計算されます。 最大使用済みブロックの値は、内部で計算されます。 このパーセンテージは、以下の状況の FULL パーセンテージより大きくなります。

- すべてのレコードが、スペース管理オプション 1 または 3（ランダムまたはクラスタ）を使用して、データ ブロック内で削除されるとき

  注: データ領域スペース管理オプションの詳細については、「*CA Datacom/DB Database and System Administration Guide*」を参照してください。

- すべての Index エントリが Index ブロック内で削除されるとき

PARTIALLY EMPTY BLKS

その領域で最大のレコードを保持するための十分なスペースがあるブロックは、部分的に空であるとみなされます。 部分的に空のブロックが存在し、スペース再活用オプションが選択された場合、すべてのブロックにデータ（100 パーセント フル）があったとしても、レコードを引き続き追加できます。

AREA REUSE OPTION

データ領域に使用される、データ領域スペース管理オプションです。

注: CA サポート はこの情報を使用します。

データベース エラー条件

CA サポート に問い合わせすることなく、CA CSM Web ベース インターフェースから対処できるエラー状態もあります。 これらのエラーには、メッセージ詳細の中に以下のテキストが含まれています。

`UNEXPECTED ENGINE ERROR: n(o)`

n(*o*)

CA Datacom/MSM MUF エラーまたはリターン コードです。

エラーがここで説明されていない場合、AUTOINFO 関数 (P. 174)を使用して、CA サポート に問い合わせる前に診断情報を収集します。

MUF のキャンセルまたは異常終了

問題の状況:

以下のエラーが表示されます。

`UNEXPECTED ENGINE ERROR: 86(186)`

解決方法

CA Datacom/MSM MUF はキャンセルされたか、または異常終了しました。

MUF がキャンセルされた場合は、以下のアクションを実行し、MUF を再起動します。

1. 「**P** MSMTC」と入力し、CA CSM アプリケーション サーバを停止します。
2. MSMDBSVP JCL メンバまたは MSMDBSRP PROCLIB メンバを使用し、CA Datacom/MSM サーバを停止します。
3. MSMMUF JCL メンバまたは MSMMUFS PROCLIB メンバを使用し、MUF を開始します。
4. MSMDBSVS JCL メンバまたは MSMDBSRV PROCLIB メンバを使用し、CA Datacom/MSM サーバを開始します。
5. MSMTCSRV JCL メンバまたは MSMTC PROCLIB メンバを使用し、CA CSM アプリケーション サーバを開始します。

MUF が異常終了した場合は、AUTOINFO 関数 (P. 174)を使用して、CA サポート に問い合わせる前に診断情報を収集します。

データ領域がフル

問題の状況:

以下のエラーが表示されます。

```
UNEXPECTED ENGINE ERROR: 07(07)
```

解決方法:

CA Datacom/MSM MUF データベース データ領域がいっぱいです。 データベースを拡張してください。

インデックスがフル

問題の状況:

以下のエラーが表示されます。

```
UNEXPECTED ENGINE ERROR: 08(08)
```

解決方法:

CA Datacom/MSM MUF データベース インデックスがいっぱいです。 データベースを拡張してください。

AUTOINFO 関数

DBUTLTY AUTOINFO 関数は、MUF のメモリ、および選択した動的システム テーブルから診断情報を収集します。 出力は印刷形式で、CA サポート に送付可能な一連のデータ セットに書き込まれます。

AUTOINFO の実行方法

ターゲットの MUF と同じシステム上で DBUTLTY AUTOINFO 関数を実行します。MUF に問題が発生している間に、AUTOINFO を実行します。MUF が停止しているときに AUTOINFO を実行する場合、この関数は S000 U0004 条件コードで終了し、利用可能なデータがなかったことをユーザに通知します。

関数を実行するためのガイドとして、以下の JCL ステートメントを使用できます。 ステートメントをカスタマイズし、ユーザのサイトの要件に合わせます。

```
//job_card
//AUTOINFO EXEC PGM=DBUTLTY,REGION=6M
//STEPLIB  DD DSN=prefix.CUSLIB,DISP=SHR
//         DD DSN=prefix.CAAXLOAD,DISP=SHR
//TABLES   DD DSN=output_data_set,DISP=(NEW,CATLG,CATLG),
//         UNIT=SYSDA,SPACE=(TRK,(3,1),RLSE)
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
AUTOINFO DDNAME=TABLES
/*
//
```

第 6 章: 追加の管理タスク

このセクションには、以下のトピックが含まれています。

現在のユーザへのメッセージ送信

z/OS の修正コマンドを使用し、CA CSM Web ベース インターフェースにログインしている 1 人のユーザまたはすべてのユーザにメッセージを送信できます。 たとえば、メンテナンスのために CA CSM をシャットダウンする前に、CA CSM アプリケーション サーバにログインしているすべての CA CSM ユーザにメッセージを送信し、CA CSM がシャットダウンしようとしていることを知らせることができます。

現在ログインしているすべての CA CSM ユーザにメッセージを送信するには、以下のコマンドを入力します。

```
/F jobname,APPL=MSG,message text
```

注: 1 人のユーザにメッセージを送信するには、以下のように TSO ユーザ ID を追加します。

```
/F jobname,APPL=MSG,TSOuserID,message text
```

jobname

システムの CA CSM アプリケーション サーバの名前を指定します。

APPL=MSG

CA CSM アドレス空間に対して指定し、この修正リクエストをメッセージ送信リクエストとして処理します。

TSOuserID

（オプション） メッセージを送信する対象のユーザの TSO ユーザ ID を指定します。TSO ユーザ ID が指定されていない場合、メッセージはサーバに現在ログインしているすべてのユーザに送信されます。

メッセージ テキスト

メッセージの本体を指定します。自由形式のメッセージ テキストを入力し、CA CSM アプリケーション サーバにログインしているすべてのユーザに表示するか、または TSO ユーザ ID が指定されている場合は、1 人のユーザに表示します。

制限 : メッセージ テキスト自体に引用符を使用している場合でも、カンマを含めないでください。

詳細:

CA CSM の停止 (P. 154)

ユーザにメッセージを送信するサンプル JCL

以下のサンプル JCL は、CA CSM にログインしているすべてのユーザにメッセージを送信する方法、および DOEJON01 の TSO ユーザ ID を持つ 1 人の CA CSM ユーザにメッセージを送信する方法を示します。

Proclib メンバ INFORMSM は以下のとおりです。

```
//*******************************************************************************
//*****                                                                      *****
//*****  Send Message to CA CSM users                                       *****
//*****                                                                      *****
//*****  SERVER= is the number of the server to receive message.           *****
//*****  MSMMSG= is the message you want sent to the server user(s)        *****
//*****                                                                      *****
//*****  EXAMPLE JCL shown below how to send message to ALL users          *****
//*****                                                                      *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                        *****
//*****  //          EXEC INFORMSM,SERVER=2,                               *****
//*****  // MSMMSG='CA CSM - IS SHUTTING DOWN - RESTART REQUESTED'         *****
//*****                                                                      *****
//*****  EXAMPLE JCL shown below how to send message to a CA CSM User      *****
//*****                                                                      *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                        *****
//*****  //          EXEC INFORMSM,SERVER=2,                               *****
//*****  // MSMMSG='DOEJON01,TEST MESSAGE FROM JCL'                        *****
//*****                                                                      *****
//*******************************************************************************
//*
//INFORMSM  PROC  MSMMSG=,
//             SERVER=
//*
//OPSCMD   EXEC PGM=OPSCMD,PARM='F MF2T&SERVER.SRV,APPL=MSG,&MSMMSG.'
//*
//OPS$OPSP DD DUMMY         Direct request to production subsystem OPSP
//*
//INFORMSM  PEND
//*
```

メッセージを送信する JCL は以下のとおりです。

```
//INFORM5S  JOB (129300000),'Inform CA CSM user',
//        COND=(4,LT),
//        CLASS=A,
//        MSGCLASS=X,
//        NOTIFY=&SYSUID,
//        MSGLEVEL=(1,1)
//*
/*JOBPARM SYSAFF=MACHINE31
//*
// JCLLIB ORDER=(MF20.MSM.PROCLIB)
//*
//*********************************************************************
//*****                                                          *****
//*****  send message to CA CSM server user(s)                  *****
//*****                                                          *****
//*********************************************************************
//*
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server is closing down in fifteen minutes       '
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server will be restarted soon after             '
//
//*
// MSMMSG='DOEJON01, send a message to a user on a CA CSM server    '
//*
```

実行中タスクの確認

実行しているタスクがあるが、それらのタスクを開始したユーザがすでに CA CSM にログインしていない場合があります。 CA CSM を停止する前に、これらのタスクを把握し、それらを急に終了することによる影響について認識する必要があります。

以下の手順に従います。

1. CA CSM Web ベース インターフェースにログインし、［Tasks］タブをクリックし、［Current Tasks］サブタブが選択されていることを確認します。

   そのユーザのタスクのみを表示した［Tasks］ページが表示されます。

2. ［Show］ドロップダウン リストから［All tasks］を選択します。

   すべてのタスクが一覧表示されます。

3. タスクのステータスを確認し、Executing ステータスのタスクがある場合は、CA CSM を停止する前にそのタスクの所有者に連絡をとることを検討してください。

Java ホーム ディレクトリの再割り当て

Java の新しいマイナー バージョンを別のディレクトリにインストールして、古いバージョンを保存するときなど、Java ホーム ディレクトリを再割り当てすることがあります。Java ディレクトリを変更するとき、以下の場所の Java のパスを修正する必要があります。

- SAMPLIB（MSMLIB）メンバの JAVA_HOME 変数の値を変更します。

  例： 以下のサンプル SAMPLIB（MSMLIB）メンバの、*original_path* を新しいパスで置換します。

  ```
  export JAVA_HOME=original_path
  ```

- Java ホーム ディレクトリを指す CA CSM CSI の SMPJHOME DDDEF 値を変更します。CA CSM CSI は CSIHLQ.SMPCSI.CSI にあります。グローバル（GLOBAL）ゾーン、ターゲット（CAIT）ゾーン、および配布（CAID）ゾーンの SMPJHOME DDDEF 値を変更します。 UCLIN ステートメントを使用し、SMPJHOME DDDEF 値を変更します。

  例： この UCLIN ステートメントを使用して、ゾーンの変数を各ゾーン名（CAID、CAIT、GLOBAL）で置換することにより、すべての CA CSM CSI ゾーンの SMPJHOME DDDEF 値を変更します。

```
SET
BOUNDARY(zone).
UCLIN.
REP  DDDEF(SMPJHOME)
     PATH('new_path').
ENDUC.
```

注: ユーザが MSMTC ジョブを開始した後は、ジョブ ログ メッセージ内の JAVA_HOME パスは、CA CSM CSI 内の SMPJHOME DDDEF のパスと以下のように一致させる必要があります。

```
JVMJZBL1006I JAVA_HOME = new_path
```

- *MSMPATH*/CEGPHFS ディレクトリにある MSMSetupOptionsFile.properties オプション ファイル内の JAVAPATH オプションを変更します。

  例： 以下の MSMSetupOptionsFile.properties オプション ファイル のサンプルで、*original_path* を新しいパスで置換します。

  ```
  JAVAPATH=original_path
  ```

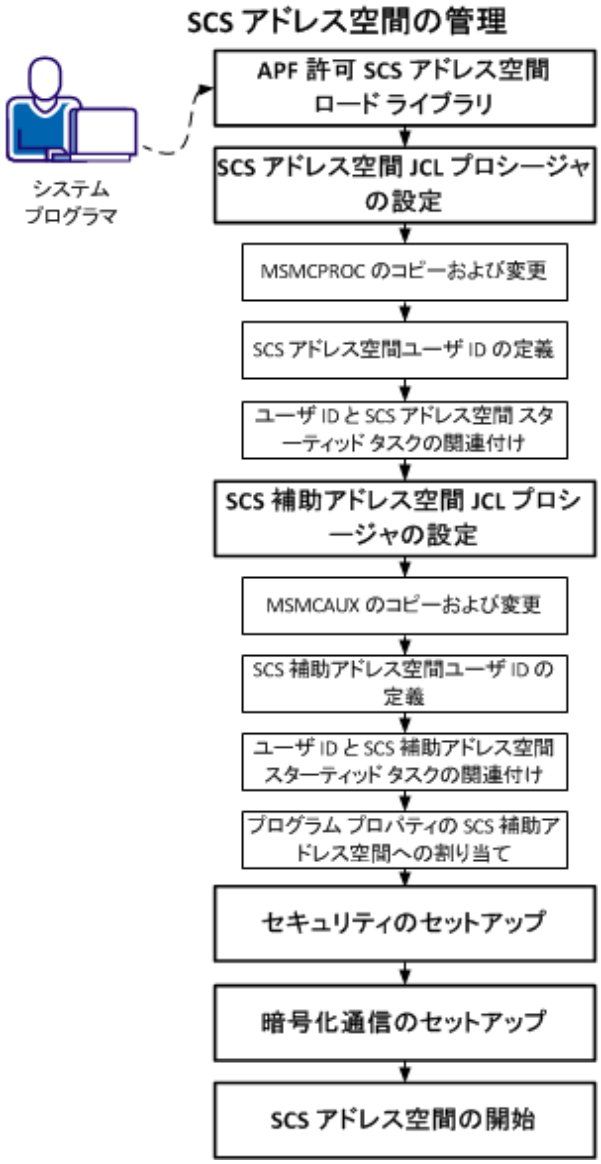
第 7 章: SCS アドレス空間管理

*SCS アドレス空間*は、特別に定義された場所で、出力およびコンソールのトラフィックを照会するためのシステム レジストリやコマンドが存在する、オペレーティングシステム内の場所です。 SCS アドレス空間は、ターゲットの z/OS システム間で設定を実装するのに必要なサービスおよび処理を提供します。SCS の処理をサポートするための各ターゲット システムは、SCS アドレス空間を実行する必要があります。

このセクションには、以下のトピックが含まれています。

SCS アドレス空間管理プロセスの動作

以下のタスクを実行し、SCS アドレス空間をユーザの環境で実行します。



1. SCS アドレス空間ロード ライブラリに対して APF 許可します (P. 183)。
2. SCS アドレス空間 JCL プロシージャを設定します (P. 184)。
   a. MSMCPROC (P. 330) をシステム PROCLIB にコピーし、インストール環境に合わせて修正します。
   b. SCS アドレス空間用のユーザ ID を定義します。
   c. セキュリティ システムを使用して、ユーザ ID と SCS アドレス空間のスターティッド タスクを関連付けます。 SCS アドレス空間をスターティッド タスクとして開始している場合は、この手順を実行します。
3. SCS 補助アドレス空間 JCL プロシージャを設定します (P. 186)。
   a. MSMCAUX (P. 330) をシステム PROCLIB にコピーし､インストール環境に合うように修正します。
   b. SCS 補助アドレス空間用のユーザ ID (P. 187) を定義します。
   c. セキュリティ システムを使用して、ユーザ ID と SCS 補助アドレス空間スターティッド タスクを関連付けます。
   d. 特殊プログラム プロパティ (P. 187)を SCS 補助アドレス空間に割り当てます。
4. セキュリティをセットアップします (P. 188)。
5. 暗号化通信をセットアップします (P. 200)。
6. SCS アドレス空間を開始します (P. 208)。

許可プログラム機能

重要: SCS アドレス空間のドキュメントでは、すべての SYS1.PARMLIB データ セットへの参照は、論理的な PARMLIB 連結で定義されている任意のデータ セットを示します。

許可プログラム機能（APF）を使用して、重要なシステム機能を使用するプログラムを特定します。 SCS アドレス空間は、APF 許可されたジョブ ステップとして開始される必要があります。SCS アドレス空間ロード ライブラリは､SCS アドレス空間が開始される各 z/OS システム上で APF 許可される必要があります。

確実に SCS アドレス空間を APF 許可されたジョブ ステップとして開始するには、SCS アドレス空間 STEPLIB 連結に含まれるすべてのライブラリを APF 許可します。 APF 許可されていない連結にライブラリを格納すると、ライブラリ連結全体がその APF 許可を失います。

APF リストは SYS1.PARMLIB メンバ PROG*xx* にあります。 このリストには、APF 許可されたライブラリの名前が含まれています。リスト内のエントリの順序は重要ではありません。

動的な形式で PROG*xx* メンバを使用する場合は、z/OS コマンド SET PROG=*xx* を発行できます。変更は次の IPL の前に有効になります。

注: APF リストの詳細については、「*IBM Initialization and Tuning Reference*」を参照してください。

MSMCPROC JCL プロシージャ

SCS アドレス空間は、MSMCPROC (P. 330) JCL プロシージャを使用します。このプロシージャを z/OS の START コマンドが使用するシステム PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。

以下のことが可能です。

- JCL EXEC ステートメントの PARM キーワード パラメータと共に使用できる、JCL EXEC ステートメントのパラメータ (P. 218) を指定します。
- 必要に応じて、任意の DD ステートメントを追加または変更します。MSMCPROC サンプル メンバは、必要な変更を示しています。

  注: MSMCPROC は SCS アドレス空間 JCL プロシージャの一般的な名前です。 ユーザのインストール環境に合わせて、名前を変更することができます。

お使いのシステムの z/OS UNIX System Services 環境が、SYS1.PARMLIB（BPXPRM*xx*）メンバの AF_INET6 ドメインで設定されていない場合は、SCS アドレス空間パラメータ メンバ MSMCPARM (P. 220) の TCP/IP パラメータを更新します。<TCPIP ipaddr="::" port="49152"/> を <TCPIP ipaddr = "0.0.0.0" port="49152"/> に変更します。

SCS アドレス空間用のセキュリティ システム ユーザ ID を定義します。ユーザ ID には、定義済みの OMVS セグメント、および SCS アドレス空間 JCL プロシージャが配置されたデータ セットに対する読み取りアクセス権が必要です。ユーザ ID には OMVS のスーパーユーザ権限は必要ありません。

SCS アドレス空間をスターティッド タスク、または開始されたジョブとして開始できます。

- SCS アドレス空間をスターティッド タスクとして開始するには、START（P. 208）コマンドを使用します。 お使いのセキュリティ システムを使用し、ユーザ ID と SCS アドレス空間のスターティッド タスクを関連付けます。
- SCS アドレス空間を開始されたジョブとして開始するには、バッチ ジョブ ストリーム内の MSMCPROC JCL プロシージャを実行します。JCL JOB ステートメントの USER パラメータを使用して、ユーザ ID と SCS アドレス空間の開始されたジョブを関連付けます。

補助アドレス空間

最初の補助アドレス空間は、SCS アドレス空間によって実行されたサービス リクエストから作成されます。 追加の補助アドレス空間は、必要に応じて作成されます。

補助アドレス空間は、同時設定リクエストのレベルに応じて、動的に作成、管理されます。 補助アドレス空間は、SCS アドレス空間の代わりにサービス リクエストを処理します。

SCS アドレス空間は、設定を実行しているユーザの代わりにサービス リクエストを実行します。 SCS アドレス空間は補助アドレス空間を作成し、それらがアクティブになったとき、補助アドレス空間に対してサービス リクエストをスケジュールします。 補助アドレス空間はリクエストを実行し、その結果は SCS アドレス空間に返されます。

補助アドレス空間の操作

SCS アドレス空間は必要に応じて自動的に補助アドレス空間を作成し、リクエストをスケジュールします。 補助アドレス空間は、SCS アドレス空間によって作成されたワークロード マネージャ（WLM）依存エンクレーブで実行されます。 スケジュールされているサービスがある場合、すべての SCS 補助アドレス空間はアクティブ状態のままになります。実行するリクエストがそれ以上ないとき、アクティブではない補助アドレス空間は停止します。

注: SCS アドレス空間は、処理される同時サービス リクエストの数に応じて、最大 20 までの数の補助アドレス空間を作成および管理します。

SCS アドレス空間パラメータを指定して、同時にアクティブな補助アドレス空間の最大数を 20 未満の数に制限できます。

補助アドレス空間に対して、自動化操作を実行する必要はありません。これは、SCS アドレス空間が動的にその操作を開始するからです。 非常に稀ですが、SCS アドレス空間が失敗すると、すべての補助アドレス空間は停止します。

インストールに関する考慮事項

CA CSM には MSMCAUX (P. 330) サンプル メンバが用意されています。補助アドレス空間は JCL プロシージャ MSMCAUX (P. 330) を使用します。このプロシージャを、z/OS START コマンドが使用するシステム PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。

必要に応じて、任意の DD ステートメントを追加または変更できます。MSMCAUX サンプル メンバは、その変更を説明します。

MSMCAUX プロシージャを手動で開始しないでください。 MSMCAUX プロシージャは SCS アドレス空間（MSMCPROC）によって開始されます。

注: MSMCAUX は補助アドレス空間 JCL プロシージャの一般的な名前です。ユーザのインストール環境に合わせて、名前を変更することができます。名前を変更する場合は、SCS アドレス空間パラメータ (P. 220)の AUX *procname* を更新します。

補助アドレス空間のユーザ ID

補助アドレス空間用のセキュリティ システム ユーザ ID を定義する必要があります。 このユーザ ID は、SCS アドレス空間に対して定義されたものと同じでかまいません。ユーザ ID は、補助のアドレス空間 JCL プロシージャによって割り当てられたデータ セットへの読み取りアクセス権が必要です。 補助アドレス空間のユーザ ID が SCS アドレス空間のユーザ ID と異なる場合、OMVS セグメントは必要ありません。

補助アドレス空間は、常にスターティッド タスクとして開始されます。セキュリティ システムを使用して、ユーザ ID と補助アドレス空間スターティッド タスクを関連付けます。

特殊プログラム プロパティ

特殊プログラム プロパティは要件であり、MSMCAUX PROC の EXEC PGM= JCL カードで指定されたプログラム MSMCAUX (P. 330) のシステムに割り当てられる必要があります。

MSMCAUX は、ストレージ保護キー 4 で実行するために、SYS1.PARMLIB の SCHED*xx* メンバに定義される必要があります。

ストレージ保護キー 4 で実行するように MSMCAUX を定義するには、以下のステートメントを使用します。

```
PPT PGMNAME(MSMCAUX) KEY(4) SYST PRIV
```

注: 特殊プログラム プロパティは、APF 許可されたライブラリ連結から取得されるプログラムにのみ割り当てられます。 すべての MSMCAUX PROC STEPLIB データ セットは、APF ライブラリ リストで正しく定義される必要があります。

特殊プログラム プロパティの定義の詳細については、「*IBM Initialization and Tuning Reference*」を参照してください。

SCS アドレス空間セキュリティのセットアップ

セキュリティのセットアップ (P. 53) は CA CSM で必要で、実行中のシステムでのみセットアップされます。SCS アドレス空間セキュリティをセットアップするには、CA CSM 実行システムを含む、すべてのターゲット システム上でセキュリティ セットアップを実行します。

SCS アドレス空間は、要求しているスターティッド タスクまたは開始されたジョブに割り当てられているユーザ ID を確認し、そのユーザ ID に接続を許可します。

注: 許可されていない CA CSM ユーザ ID には、選択したターゲット システムへのアクセスが拒否されます。

セキュリティ プロファイルが定義されていない場合、CA CSM は SCS アドレス空間に接続できません。アドレス空間内部からもアクセスできません。

セキュリティ管理者は CAMSM クラスの SCSAS.CONNECT（READ 権限）エンティティにアクセスする権限 この権限により、CA CSM アプリケーション サーバおよび SCS アドレス空間から SCS アドレス空間へ接続することができます。 を設定する必要があります。

使用されている 3 つの主要外部セキュリティ マネージャ（ESM）製品（CA ACF2 for z/OS、CA Top Secret for z/OS、または IBM RACF）のいずれかでセキュリティをセットアップします。

以下のトピックでは、CAMSM という名前のリソース クラスのエンティティ SCSAS.CONNECT へ READ アクセス権を設定するために、ルールをセットアップする方法について説明します。エンティティへの READ アクセス権を設定するルールのセットアップは、使用しているセキュリティ ソフトウェアによって異なります。

CA ACF2 for z/OS での SCS アドレス空間セキュリティのセットアップ

CA ACF2 for z/OS を使用して SCS アドレス空間にセキュリティをセットアップしている場合、グローバル システム オプション（GSO）レコードを定義し、ユーザ ID にアクセスを許可するルールを定義する必要があります。

以下の手順に従います。

1. 以下のコマンドを入力し、GSO レコードを定義します。

```
SET C(GSO)
INSERT CLASMAP.MSM ENTITYLN(246) MUSID() RESOURCE(CAMSM) RSRCTYPE(MSM)
```

2. 以下のコマンドを入力し、ユーザ ID にアクセスを許可するルールを定義します。

```
SET R(MSM)
COMPILE STORE
$KEY(SCSAS) TYPE(MSM)
CONNECT.-     UID(*****userid)                SERVICE(READ)     ALLOW
CONNECT.-     UID(*****userid2)               SERVICE(READ)     ALLOW
```

userid

SCS アドレス空間に割り当てられるユーザ ID を指定します。

userid2

CA CSM アプリケーション サーバ実行システムに割り当てられるユーザ ID を指定します。

CA Top Secret for z/OS での SCS アドレス空間セキュリティのセットアップ

CA Top Secret for z/OS を使用している場合、SCS アドレス空間でセキュリティをセットアップします。

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 クラスを RDT に追加します。

```
TSS ADDTO(RDT) RESCLASS(CAMSM) ATTR(MASK) MAXLEN(246)
TSS REPL(RDT) RESCLASS(CAMSM)
                ACLST(READ=4000,UPDATE=8000,CONTROL=0400,NONE=0000)
                DEFACC(READ)
```

2. 以下のコマンドを入力して、CA CSM の部門別 ACID を作成します。

```
TSS CREATE(MSMDPT) NAME('CA CSM Department') TYPE(USER)
```

3. 以下のコマンドを入力して、CAMSM クラス内のリソース プロファイルを定義します。

   ```
   TSS ADDTO(MSMDPT) CAMSM(SCSAS.CONNECT)
   ```

4. 以下のコマンドを入力して、CA Top Secret for z/OS プロファイルを作成します。

   ```
   TSS CREATE(SCSPRF1) NAME('CA CSM SCS AS PROFILE')
   DEPT(MSMDPT)   TYPE(PROFILE)
   ```

5. 以下のコマンドを入力して、リソースにプロファイルへのアクセス許可を与えます。

   ```
   TSS PERMIT(SCSPRF1) CAMSM(SCSAS.CONNECT)   ACCESS(READ)
   ```

6. 以下のコマンドを入力して、プロファイルを ACID に割り当てます。

   ```
   TSS ADDTO(userid) PROFILE(SCSPRF1)
   ```

   userid

   SCS アドレス空間に割り当てられるユーザ ID を指定します。

IBM RACF での SCS アドレス空間セキュリティのセットアップ

IBM RACF を使用している場合、SCS アドレス空間でセキュリティをセットアップします。

注: IBM RACF にすでに定義済みで有効化されている CAMSM リソース クラスがある (P. 73)場合、手順 1 ～ 4 をスキップできます。

以下の手順に従います。

1. STEROPTS LIST コマンドを発行して、エントリの CLASSACT および RACLIST の両方のリストに CDT リソースが表示されることを確認します。
2. 以下のコマンドを発行して、汎用プロファイルを定義します。

   ```
   RDEFINE CDT CAMSM UACC(NONE) CDTINFO(GENERIC,MAXLENGTH(246) POSIT(nnn)
   OTHER(ALPHA,NATIONAL,NUMERIC,SPECIAL) RACLIST(ALLOWED))
   ```

   nnn

   IBM の予約値と重複しない POSIT 番号を定義します。

   注: POSIT 番号の詳細については、「*IBM Server RACF Command Language Reference*」を参照してください。

   汎用プロファイルが定義されます。
3. 以下のコマンドを入力して、汎用プロファイルの変更を有効にします。

   ```
   SETROPTS RACLIST(CDT) REFRESH
   ```
4. 以下のコマンドを入力して、CAMSM クラスを有効にします。

   ```
   SETROPTS RACLIST(CAMSM) CLASSACT(CAMSM)
   ```
5. 以下のコマンドを入力して、CAMSM クラス内のリソース プロファイルを定義します。

   ```
   RDEFINE CAMSM SCSAS.CONNECT UACC(NONE)
   ```
6. 以下のコマンドを入力して、リソースをユーザに許可します。

   ```
   PERMIT SCSAS.CONNECT CLASS(CAMSM) ID(userid) ACCESS(READ)
   ```

   userid

   SCS アドレス空間に割り当てられるユーザ ID を指定します。
7. （オプション）CAMSM クラスが RACLISTed である場合は、以下のコマンドを入力して、そのクラスを更新します。

   ```
   SETROPTS RACLIST(CAMSM) REFRESH
   ```

PassTicket

PassTicket は、リモート システムから SCS アドレス空間へ接続するために、CA CSM アプリケーション サーバのスターティッド タスク ID の確認に使用されます。

CA CSM アプリケーション サーバを実行しているシステム、および SCS アドレス空間が実行されている各システム上で、PassTicket をセットアップする必要があります。

注: 有効な PassTicket を生成するには、CA CSM アプリケーション サーバが実行されているシステムで、リモート SCS アドレス空間用の値を使用します。 を、

PassTicket をセットアップするには、サーバおよびリモート ターゲット システムの両方で以下のコマンドを使用します。使用しているセキュリティ ソフトウェア（CA ACF2 for z/OS、CA Top Secret for z/OS または IBM RACF）に応じて設定する必要があります。

注: これらの例はガイドラインとして提供され、PassTicket の設定を十分理解しているセキュリティ管理者を対象としています。

CA ACF2 for z/OS PassTicket の例

CA ACF2 for z/OS を使用して、CA CSM アプリケーション サーバ用の PassTicket を設定し、リモート システムと通信することができます。

注: これらの例でのコマンド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 CSM アプリケーション サーバ用の PassTicket の設定

CA ACF2 for z/OS を使用し、CA CSM アプリケーション サーバを実行しているシステムの PassTicket を設定することができます。

以下の手順に従います。

1. 以下のコマンドを入力し、CA CSM アプリケーション サーバのセッション キーを定義します。

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

2. 以下のコマンドを入力し、MSMCAPPL PassTicket キー値への READ アクセス権を有効にします。

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

   stc-userid および *uid-of-stc-userid*

   CA CSM アプリケーション サーバのスターティッド タスクに関連付けられたユーザ ID および UID を指定します。

   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。

3. 以下のコマンドを入力して、PassTicket のセットアップを完了します。

   ```
   F ACF2,REBUILD(PTK),CLASS(P)
   F ACF2,REBUILD(PTK)
   ```

例: リモート システム上の SCS アドレス空間用の PassTicket の設定

CA ACF2 for z/OS を使用して、SCS アドレス空間を実行しているリモート システム上で PassTicket を設定できます。

以下の手順に従います。

1. 以下のコマンドを入力して、MSMCAPPL セッション キーを定義します。

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT MSMCAPPL SSKEY(0123456789ABCDEF) NOMULT-USE
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

2. 以下のコマンドを入力し、MSMCAPPL PassTicket キー値への READ アクセス権を有効にします。

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

   stc-userid および *uid-of-stc-userid*

   SCS アドレス空間に関連付けられたユーザ ID および UID を指定します。

   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。

3. 以下のコマンドを入力して、リモート システムの PassTicket のセットアップを完了します。

   ```
   F ACF2,REBUILD(PTK),CLASS(P)
   F ACF2,REBUILD(PTK)
   ```

CA Top Secret for z/OS PassTicket の例

CA Top Secret for z/OS を使用して、CA CSM アプリケーション サーバ用の PassTicket を設定し、リモート システムと通信することができます。

注: これらの例でのコマンド使用に関する詳細情報については、「*CA Top Secret for z/OS Administration Guide*」を参照してください。

例: CA CSM アプリケーション サーバ用の PassTicket の設定

CA Top Secret for z/OS を使用して、CA CSM アプリケーション サーバを実行しているシステムの PassTicket を設定することができます。

以下の手順に従います。

1. 以下のコマンドを入力して、PTKTDATA クラス（定義済みクラスではありません）を定義するリソース記述子テーブル（RDT）を更新します。

   ```
   TSS ADDTO(RDT) RESCLASS(PTKTDATA) RESCODE(n) ACLIST(ALL,READ,UPDATE) MAXLEN(37)
   ```

   注: PTKTDATA をプレフィクス付きリソース クラスにするために、RESCODE(*n*) を 101 ～ 13F の範囲で入力してください。

2. 以下のコマンドを入力して、PassTicket セッション キー（SESSKEY）リソースの部門へ所有権を割り当てます。

   ```
   TSS ADDTO(department) PTKTDATA(IRRPTAUTH)
   ```

   department

   既存の部門を指定します。 アプリケーションの所有権がこの部門に定義されます。この所有権により、部門管理者（またはより上位の職務者）が PassTicket の生成および検証の許可を定義できるようになります。

3. 以下のコマンドを入力して、CA CSM アプリケーション サーバの PassTicket セッション キーを定義します。

   ```
   TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

4. 以下のコマンドを入力して、CA CSM アプリケーション サーバのスターティッド タスク ユーザ用の CA CSM アプリケーション サーバ PassTicket セッション キー値へのアクセスを許可します。

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

   stc-userid

   CA CSM アプリケーション サーバに関連付けられたユーザ ID のアクセス要件 (P. 56)を定義した ACID を指定します。

例: リモート システム上の SCS アドレス空間用の PassTicket の設定

CA Top Secret for z/OS を使用して、SCS アドレス空間を実行しているリモート システム上で PassTicket を設定できます。

以下の手順に従います。

1. 以下のコマンドを入力し、SCS アドレス空間 PassTicket セッション キーを定義します。

   ```
   TSS ADDTO(NDT) PSTKAPPL(MSMCAPPL) SESSKEY(0123456789ABCDEF)
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

IBM RACF PassTicket の例

IBM RACF を使用して、CA CSM アプリケーション サーバ用の PassTicket を設定し、リモート システムと通信することができます。

注: これらの例でのコマンド使用に関する詳細情報については、「IBM RACF」ドキュメントを参照してください。

例: CA CSM アプリケーション サーバ用の PassTicket の設定

IBM RACF を使用して、CA CSM アプリケーション サーバを実行しているシステム上で PassTicket を設定できます。

以下の手順に従います。

1. 以下のコマンドを入力して、PassTicket クラスを有効化します。

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

2. 以下のコマンドを入力して、アプリケーション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 MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

3. 以下のコマンドを入力し、プロファイルを定義して、スターティッド タスク ユーザ ID に対して MSMCAPPL PassTicket セッション キー値へのアクセスを許可すると、その ID が SCS アドレス空間にアクセスできるようになります。

   ```
   RDEFINE PTKTDATA IRRPTAUTH.MSMCAPPL.stc-userid UACC(NONE)
   ```

   stc-userid

   CA CSM アプリケーション サーバ スターティッド タスクに関連付けられたユーザ ID を指定します。このユーザ ID には、そのユーザ ID 自体に対する PassTicket を生成する機能のみが必要です。

4. 以下のコマンドを入力して、CA CSM アプリケーション サーバ用の MSMCAPPL PassTicket セッション キー値へのアクセスを許可します。

   ```
   PERMIT IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) ID(stc-userid)
   ACCESS(READ,UPDATE)
   ```

5. 以下のコマンドを入力して、PTKTDATA クラスをリフレッシュします。

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

例: リモート システム上の SCS アドレス空間用の PassTicket の設定

IBM RACF を使用して、SCS アドレス空間を実行しているリモート システム上で PassTicket を設定できます。

以下の手順に従います。

1. 以下のコマンドを入力して、PassTicket クラスを有効化します。

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

2. 以下のコマンドを入力して、アプリケーション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 MSMCAPPL SSIGNON(KEYMASKED(0123456789ABCDEF)) UACC(NONE)
   ```

   MSMCAPPL

   CA CSM 設定プロセス中に使用される SCS アドレス空間 ID のセッション キーを定義します。 この名前は CA CSM のインストール時にオーバーライドされる可能性があるため、実際のアプリケーション名を反映した名前にする必要があります。

   注: この例では、16 進数の完全なセッション 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。 16 のランダムな 16 進数で構成されるようにキーを変更し、この例で示されている値とは異なるようにします。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、値は機密保護される必要があります。

3. 以下のコマンドを入力し、SCS アドレス空間スターティッド タスクのユーザ ID に対して MSMCAPPL PassTicket セッション キー値へのアクセスを許可します。

   ```
   RDEFINE IRRPTAUTH.MSMCAPPL.stc-userid CLASS(PTKTDATA) UACC(NONE)
   ```

   stc-userid

   SCS アドレス空間スターティッド タスクのユーザ ID を指定します。

4. 以下のコマンドを入力して、PTKTDATA クラスをリフレッシュします。

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

UNIX ソケットの要件

SCS アドレス空間は、UNIX ソケットを内部での通信に使用します。

ターゲット システムで以下の項目をセットアップします。

- BPXPRMxx PARMLIB メンバで AF_UNIX ドメインを定義します。
- /var/sock ディレクトリが UNIX ファイル システムに存在するか、もしくは MSMCPROC にそのディレクトリを作成する権限があることを確認します。
- MSMCPROC が /var/sock ディレクトリへの書き込み権限があることを確認します。

暗号化通信

SCS アドレス空間で暗号化通信を有効にするには、以下のいずれかの暗号化方式を設定する必要があります。

- IBM System Secure Socket Layer（SSL）
- IBM Application Transparent Transport Layer Security（AT-TLS）

Web ベース インターフェース リモート ホストから SCS アドレス空間に接続する場合、アドレス空間は System SSL または IBM AT-TLS の使用を検出します。 どちらの方式も検出されない場合、Web ベース インターフェースとの通信はクリア テキストで実行されます。

SSL 伝送のサポートの実装

SCS アドレス空間をセットアップして、以下の*いずれか*を使用します。

- 階層型ファイル システム（HFS）にあるキー ストア ファイルを使用した、IBM System Secure Socket Layer（SSL）ツールキット。

  注: シェル プロンプトで OMVS の下のプログラム *gskkyman* を実行します。このプログラムの実行により、HFS 上でキー ストア ファイルが作成され、自己署名の認証局証明書が生成され、サーバ証明書が生成されます。

- 外部セキュリティ マネージャ（ESM）

  注: お使いの ESM のコマンドを実行して、サーバ証明書を生成します。

キー ストア ファイルの作成

SSL を使用するために SCS アドレス空間をセットアップする際に、zFS または HFS 上でキー ストア ファイルを作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Create new database］を選択し、新しいキー ストア ファイルまたはデータベースへのパスおよびファイル名を入力します。

   注: パスとファイル名は、書き込み可能なパスおよびファイル名である必要があります。
3. データベース パスワードを入力し、パスワードの有効期限を日数で入力します。

   注: パスワードに有効期限を設けない場合は、ENTER キーを押します。
4. データベース レコード長に「**5000** 」を入力し、データベース モードに「**0**」を入力します。
5. キー データベースが作成されたことを伝える確認通知を待ちます。
6. ［Exit program］を選択します。

   キー ストア ファイルが作成されます。

自己署名の認証局証明書の作成

SSL を使用するために SCS アドレス空間をセットアップする際に、自己署名の認証局証明書を作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力し、データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
3. ［Create self-signed certificate］を選択します。
4. 1024 ビット RSA キーの認証局証明書を選択し、［SHA-512］を選択します。

   注: 1024 ビット RSA キーの認証局証明書を選択すると、認証局が作成されます。

5. 自己署名の認証局証明書のラベルを入力し、共有名を入力します。

   注: 共有名はラベルと同じでかまいません。

6. プロンプトに表示された、証明書の所有権に関するデータを入力します。 所有権には以下のものが含まれます。

   - 組織単位
   - 組織
   - 組織の国、都道府県、市町村

7. 証明書が有効な日数を入力し、「**0**」を入力して続行します。
8. 証明書が作成されるまで待機します。
9. ［Exit program］を選択します。

   自己署名の認証局証明書が作成されます。

サーバ証明書の作成

SSL を使用するために SCS アドレス空間をセットアップする際に、サーバ証明書を作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力し、データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。

3. ［Manage keys and certificates］を選択し、使用する認証局証明書の数を入力します。

   注: 事前に作成した数を使用することができます。

4. ［Create a Signed Certificate and Key］を選択し、1024 ビット RSA キーのユーザ証明書またはサーバ証明書を選択します。
5. サーバ証明書のラベルを入力し、共有名を入力します。

   注: 共有名はラベルと同じでかまいません。

6. プロンプトに表示された、証明書の所有権に関するデータを入力します。 所有権には以下のものが含まれます。
   - 組織単位
   - 組織
   - 組織の国、都道府県、市町村
7. 証明書が有効な日数を入力し、「**0**」を入力して続行します。
8. 証明書が作成されるまで待機します。
9. ［Exit program］を選択します。

   サーバ証明書が作成されます。

デフォルト証明書としてのサーバ証明書の設定

SSL を使用するために SCS アドレス空間をセットアップする際に、サーバ証明書をデフォルト証明書として設定できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースのパスを入力します。
3. データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
4. ［Manage keys and certificates］を選択し、サーバ証明書のラベルの数を入力します。
5. オプションを選択し、キーをデフォルトとして設定します。
6. ［Exit program］を選択します。

   サーバ証明書がデフォルト証明書として設定されます。

認証局証明書のエクスポート

SSL を使用するために SCS アドレス空間をセットアップする際に、認証局証明書をエクスポートできます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力します。
3. データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
4. ［Manage keys and certificates］を選択し、エクスポートする認証局証明書のラベルの数を入力します。
5. ［Export certificate to a file］を選択し、［Binary ASN.1 DER］を選択します。
6. 証明書をエクスポートするパス名およびファイルを入力し、Enter キーを押します。
7. ［Exit program］を選択します。

   認証局証明書がエクスポートされます。

データベース パスワードまたはキー ストア パスワードの stash ファイルへの格納

SSL を使用するために SCS アドレス空間をセットアップする際に、stash ファイルにデータベース パスワードまたはキー ストア パスワードを保存できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースのパスを入力します。

3. データベース パスワードを入力し、［Store Database Password］を選択します。

   database_*name*.sth ファイルは、データベース ファイルが格納されている場所に格納されます。

4. ［Exit program］を選択します。

   データベース パスワードまたはキー ストア パスワードが、stash ファイルへ保存されます。

Java キー データベースへの認証局証明書のインポート

SSL を使用するために SCS アドレス空間をセットアップする際に、認証局証明書を Java キー データベースへインポートできます。

以下の手順に従います。

1. Java SDK に付属の keytool プログラムをスーパーユーザ モードで実行します。
2. キー ストアのパスワードを入力します。

   デフォルト： changeit

3. 「yes」を入力し、証明書を信頼します。

   注: 証明書が正常に追加された場合、この設定は完了です。

   認証局証明書は Java キー データベースへインポートされます。

例: keytool プログラムの実行

keytool プログラムを実行する方法の例を以下に示します。

```
keytool -import -trustcacerts -file /path/to/exported/ca/certificate -keystore
$JAVA_HOME/lib/security/cacerts
```

System SSL 使用のセットアップ

SCS アドレス空間が System SSL を使用するには、PDSE メンバの GSKSSL が以下の 2 つの方法のうち 1 つを使用して、プログラムにアクセスできる必要があります。

- 動的 LPA（PROGxx メンバ）への *pdsename*.SIEALNKE という名前の PDSE の追加。

  注: System SSL のセットアップの詳細については、IBM の「*z/OS Cryptographic Service System Secure Sockets Layer Programming*」を参照してください。

- SCS アドレス空間を開始するのに使用される JCL プロシージャを含んだ PROCLIB メンバの修正。名前は一般的には MSMCPROC（P. 330）です。STEPLIB に DD ステートメントを追加し、*pdsename*.SIEALNKE への参照を組み込みます。

SCS アドレス空間設定 XML に移動し、アドレス空間内の SSL を有効にします。

認証局証明書およびサーバ証明書を作成したら、SCS アドレス空間用の *MSMCPARM* という名前のパラメータ ファイルを修正します (P. 220)。

デフォルト： MSMCPARM

XML ドキュメントに SSL タグを配置し、keyring 属性をキー ストアおよびデータベース ファイルに設定し、stashfile 属性を該当する stash ファイルに設定します。

XML ドキュメントの SSL 要素で keyring と stashfile を設定して SCS アドレス空間設定 XML を更新し、キーストア データベースおよびパスワードの stash ファイルを指すようにします。

AT-TLS 伝送サポートの実装

Application Transparent Transport Layer Security（AT-TLS）は z/OS のコンポーネントで、機密データを交換するが暗号化の手段が備わっていないアプリケーションに対し、暗号化サービスを提供します。 このサービスは、暗号化を行うための余計な API の呼び出しを追加することなく、アプリケーションに送信されるデータの暗号化を可能にします。

SCS アドレス空間で AT-TLS を使用するには、以下の作業を完了しておく必要があります。

- Communications Policy Agent の設定
- AT-TLS ポリシーの設定
- サーバ証明書および認証局証明書のインストール

注: IBM Policy Agent の詳細については、「*IBM z/OS V1R11 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*」を参照してください。

オペレータ通信インターフェース

z/OS オペレータ コマンドは、SCS アドレス空間の操作を制御するために使用されます。

オペレータ コマンドを発行できるユーザのグループを制御できます。 CA ACF2 for z/OS、CA Top Secret for z/OS または IBM RACF を使用し、一部またはすべてのコマンドの発行をユーザに許可または制限します。

オペレータ コマンドの使用を制御するには、SAF OPERCMDS クラスでプロファイルを作成します。

コマンドの説明文は、そのコマンドに対する権限の要件を説明します。ほとんどの場合、1 つ以上のレベルの権限が必要です。また、コマンドを発行するユーザには、指定されたすべてのアクセス権限が必要です。

SCS アドレス空間オペレータ コマンド

このセクションでは、SCS アドレス空間がサポートするコマンドを説明します。

START コマンド -- SCS アドレス空間を開始する

START コマンドは、SCS アドレス空間を開始します。 START または省略形の「S」を入力できます。 このコマンドを使用するには、*MVS.START.STC.procname* という名前の、SAF OPERCMDS クラス リソースに対する UPDATE 権限が必要です。

注: MSMCAUX プロシージャを手動で開始しないでください。 MSMCAUX プロシージャは SCS アドレス空間（MSMCPROC）によって開始されます。

START コマンドのガイドラインを以下に示します。

- START コマンドのパラメータ値は、JCL EXEC ステートメント PARM キーワードのパラメータ値をオーバーライドします。
- 2 つ以上のパラメータを持つキーワードは、カンマまたはスペースで区切る必要があります。
- 2 つ以上のサブパラメータを持つキーワードは、カンマまたはスペースで区切る必要があります。
- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（「/*」）でコメントを開始します。（オプション）コメント終了区切り文字（「*/」）でコメントを終了します。
- 不正に指定されたパラメータは無視されます。

このコマンドの構文は以下の通りです。

```
Start procname[,,,(start_parameters)][,REUSASID=YES][,PARMS='exec_parameters']
```

procname

SCS アドレス空間を開始するために使用される JCL プロシージャが含まれているシステム PROCLIB メンバの名前を指定します。 名前は一般的には MSMCPROC (P. 330) です。

,,,(*start parameters*)

（オプション） SCS アドレス空間用の START コマンド パラメータ (P. 218)を指定します。START コマンドのパラメータ値は、JCL EXEC ステートメントの PARM パラメータ値をオーバーライドします。

,REUSASID=YES

（オプション） z/OS が、再利用可能なアドレス空間識別子（ASID）を SCS アドレス空間に割り当てる必要があることを指定します。

,PARMS='*exec_parameters*'

（オプション） SCS アドレス空間の JCL EXEC ステートメントの PARM パラメータ (P. 218)を、指定したパラメータでオーバーライドすることを指定します。 指定する exec_parameter 値で、JCL EXEC ステートメントの PARM パラメータ値がオーバーライドされます。

例:SCS アドレス空間の開始

これらの例は、START コマンドを使用して、SCS アドレス空間を開始する方法を示しています。

```
S MSMCPROC,REUSASID=YES,PARMS='CONFIG(SCSPARMS)'

S MSMCPROC,,,(CONFIG(SCSPARMS)),REUSASID=YES
```

SCS アドレス空間の初期化

以下のメッセージを受信すると、SCS アドレス空間が初期化されます。

```
MSMC0002I SCS initialization complete. SYSNAME=system_name, CCINAME=CAICCI_name
```

以下のメッセージを受信すると、SCS アドレス空間は完全に稼働中になります。

```
MSMC0423I Task MSMCIENG database connection opened
MSMC0424I Task MSMCFCOM database connection opened
```

SCS アドレス空間が接続の待機中であることを確認するには、接続をリッスンし、以下のメッセージを探します。

```
MSMC0617I The SCS address space is now listening for connections on the UNIX socket
MSMC0618I The SCS address space is now listening for connections on the INET/INET6
socket, port nnnn
```

STOP コマンド - SCS アドレス空間の停止

STOP コマンドは、SCS アドレス空間の正常終了を開始します。 STOP または省略形の P を入力できます。 このコマンドを使用するには、CAMSMSCS.STOP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を設定する必要があります。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.STOP.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を設定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.STOP.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を設定します。

このコマンドの構文は以下の通りです。

```
stoP jobname
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 330) です。

例: SCS アドレス空間の停止

この例は、STOP コマンドを使用して SCS アドレス空間を停止する方法を示します。

```
P MSMCPROC
```

MODIFY コマンド - SCS アドレス空間を変更します

MODIFY コマンドを使用して、SCS アドレス空間の操作を制御します。MODIFY または省略形の F を入力できます。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.*procname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.*jobname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

以下の 3 つの MODIFY コマンドがあります。

- ABEND
- DUMP
- STOP

MODIFY コマンドの仕様を以下に示します。

- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（「/*」）でコメントを開始します。(オプション) コメント終了区切り文字(「*/」)でコメントを終了します。
- 2 つ以上の指定パラメータを持ったキーワード（オプション値がある各キーワード）は、カンマまたはスペースで区切る必要があります。
- 2 つ以上のサブパラメータを持つキーワードは、カンマまたはスペースで区切る必要があります。

  注: コメントがパラメータ文字列の最後にある場合、コメント終了区切り文字は省略可能です。

MODIFY ABEND コマンド - SCS アドレス空間の異常終了を開始する

MODIFY ABEND コマンドを使用して、SCS アドレス空間の異常終了を開始します。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.ABEND という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を設定する必要があります。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します

このコマンドの構文は以下の通りです。

```
modiFy jobname,ABEND
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 名前は一般的には MSMCPROC (P. 330) です。

例: MODIFY ABEND コマンドを使用して、SCS アドレス空間を修正する

この例は、MODIFY ABEND コマンドを使用して、SCS アドレス空間を修正する方法を示します。

```
F MSMCPROC,ABEND
```

MODIFY DUMP コマンド - SCS アドレス空間の SVC ダンプを収集する

MODIFY DUMP コマンドは、SCS アドレス空間の SVC ダンプを収集するために使用されます。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.DUMP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を設定する必要があります。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.*procname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.*jobname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

このコマンドの構文は以下の通りです。

```
modiFy jobname,DUMP[ASID(asid_list)]JOBNAME(job_list)[DSPNAME(dsp_list)]
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 330) です。

デフォルト： JOBNAME が指定されない場合は、SCS アドレス空間。

ASID（*asid_list*）

（オプション） ダンプに含める 1 つ以上のアドレス空間のアドレス空間識別子オペレータ入力 (P. 216)を指定します。

制限： 1 ～ 32767 の 10 進数の範囲または 1 ～ 7FFF の 16 進数の範囲

デフォルト： ASID パラメータが指定されない場合は、SCS アドレス空間。

JOBNAME(*job_list*)

ダンプに含める 1 つ以上のアドレス空間の名前を指定します。

注: *ジョブ名*には、疑問符（?）のような単一マスク文字を意味するものや、アスタリスク（*）のような 0 以上のマスク文字を意味する、ワイルドカード文字を含めることができます。

制限： 区切り記号または区切り文字で終了の場所が示された、引用符で囲まれた 1 ～ 8 文字の文字列（'abc' など）、または引用符で囲まれていない文字列（abc など）。

DSPNAME(*dsp_list*)

（オプション） ダンプに含める 1 つ以上のデータ空間のデータ空間識別子 (P. 217)を指定します。

デフォルト： DSPNAME が指定されない場合、SCS アドレス空間が所有するデータ空間。

注: JOBNAME と DSPNAME のパラメータでワイルド カード文字を使用すると、ダンプに含めるアドレス空間を複数選択できるようになります。

例: MODIFY DUMP コマンドを使用して、SCS アドレス空間および補助アドレス空間をダンプする

この例は、MODIFY DUMP コマンドを使用して、SCS アドレス空間と補助アドレス空間をダンプする方法を示します。

```
F MSMCPROC,DUMP JOBNAME(MSMCPROC,MSMCAUX)
```

MODIFY STOP コマンド - SCS アドレス空間の正常終了の開始

MODIFY STOP コマンドを使用して、SCS アドレス空間の正常終了を開始します。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.STOP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を設定する必要があります。

注: STOP コマンドと MODIFY STOP コマンドの実行結果はまったく同じになります。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

このコマンドの構文は以下の通りです。

```
modiFy jobname,STOP
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 330) です。

例: MODIFY STOP コマンドを使用して、SCS アドレス空間を修正する

この例は、MODIFY STOP コマンドを使用して、SCS アドレス空間を修正する方法を示します。

```
F MSMCPROC,STOP
```

SCS アドレス空間 ASID オペレータ入力の例

例

以下の例は、16 進数の数字（AF、0 ～ 9）で表現された SCS アドレス空間 ASID オペレータ入力値を示します。

X'nnnn'

以下の例は、10 進数の数字（0 ～ 9）で表現された SCS アドレス空間 ASID オペレータ入力値を示します。

ddddd

結合時に、以下のアドレス空間が 15 を超える場合、最初の 15 のアドレス空間のみがダンプに含まれます。

- SCS アドレス空間
- ASID パラメータで指定されるアドレス空間
- JOBNAME パラメータで指定されるアドレス空間
- DSPNAME パラメータで指定される、データ空間を所有するアドレス空間

SCS アドレス空間のデータ空間識別子の入力

有効なデータ空間識別子の入力指示子を以下に示します。

asid.name

ダンプに含める、所有するアドレス空間の 16 進数のアドレス空間識別子（ASID）、およびデータ空間の *data_space_name* を指定します。

制限： 1 ～ 7FFF の 16 進数の範囲（ASID）

デフォルト： SCS アドレス空間の ASID およびデータ空間

注: 指定する ASID 値の最初の文字は、10 進数である必要があります。所有するアドレス空間の ASID の最初の有効桁が、10 進数でない場合は、ゼロから始まる ASID を指定します。

jobname.name

ダンプに含める、所有するアドレス空間の *ジョブ名*および *data_space_name* を指定します。 *ジョブ名*には、疑問符（?）のような単一マスク文字を意味するものや、アスタリスク（*）のような 0 以上のマスク文字を意味する、ワイルドカード文字を含めることができます。

制限： 1 ～ 8 の引用符で囲まれていない文字

注: 256 を超えるデータ空間をダンプに含むことはできません。 パラメータでワイルド カード文字を使用すると、ダンプに含めるデータ空間を複数選択できるようになります。

ダンプに含まれていないアドレス空間がデータ空間を所有している場合、ASID のアドレス空間をダンプに含まれているアドレス空間のリストに追加します。 最大 15 のアドレス空間が許可されています。 アドレス空間の制限により、256 以上のデータ空間の指定はできません。

JCL EXEC ステートメント PARM キーワードおよび START コマンド パラメータ

SCS アドレス空間のパラメータは、パラメータ ライブラリ メンバで指定されます。時として、SCS アドレス空間パラメータは、アドレス空間のスタートアップ JCL の JCL EXEC ステートメントの PARM キーワード パラメータ、および SCS アドレス空間を開始するのに使用される START コマンドで指定されます。

JCL EXEC ステートメントの PARM キーワード パラメータ、および START コマンドで指定できるパラメータはまったく同じです。

これらの代替方法のいずれかを使用して SCS アドレス空間パラメータを指定する場合、以下のガイドラインを厳守する必要があります。

- START コマンドのパラメータ値は、JCL EXEC ステートメント PARM キーワードのパラメータ値をオーバーライドします。
- 2 つ以上のパラメータを持つキーワードは、カンマまたはスペースで区切る必要があります。
- 2 つ以上のサブパラメータを持つキーワードは、カンマまたはスペースで区切る必要があります。
- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（「/*」）でコメントを開始します。 オプションで、コメント終了区切り文字（「*/」）でコメントを終了します。
- 不正に指定されたパラメータは無視されます。

JCL EXEC ステートメントの PARM キーワード パラメータおよび START コマンドで使用されるパラメータを以下に示します。

CONFIG(*name)*

SCS アドレス空間設定パラメータが含まれるパラメータ ライブラリ メンバの名前を指定します。

制限： 1 ～ 8 文字の、引用符で囲んだ文字列（'abc' など）または囲んでいない文字列。 区切り記号または区切り文字で終了を示します。

デフォルト： CONFIG が指定されていない場合、MSMCPARM。

ROUTCDE(*routing code list*)

WTO メッセージに割り当てられる、経路指定コードまたは経路指定コードの範囲を指定します。

ダッシュ（-）で区切られた 2 つの値によって、経路指定コードの包括的な範囲を指定します。

指定された経路指定コードは、メッセージごとに定義された特定の経路指定コードに追加されます。

制限： 1 ～ 128

例： *ddd*（*d* は有効な 10 進数（0 ～ 9））

CASE(MIXED|UPPER)

WTO のメッセージを大小混合文字、または大文字のみを使用して書き込むことを指定します。

MIXED： WTO のメッセージを大文字と小文字の混合で書き込むことができます。

UPPER： WTO のメッセージは大文字を使用して書き込むことができます。

デフォルト： MIXED

DAE(YES|NO)

DAE ダンプ抑制を許可するか禁止するかを指定します。

YES： DAE ダンプ抑制は許可されます。

NO： DAE ダンプ抑制は禁止されます。

デフォルト： YES

パラメータ ライブラリ

SCS アドレス空間パラメータは、パラメータ ライブラリのメンバで設定パラメータとして指定されます。

パラメータ ライブラリは、SCS アドレス空間の JCL プロシージャ内の MSMPARM DD ステートメントに割り当てられたデータ セット、または複数のデータ セットです。

パラメータ ライブラリは、区分データ セットまたは区分データ セットの連結である必要があります。また各区分データ セットには可変長レコードが必要です。 各パラメータ ライブラリ メンバには、アドレス空間パラメータを指定し、さまざまな要素を含んだ XML ドキュメントがあります。

SCS アドレス空間の複数インスタンス用の共通設定パラメータを使用して簡素化するために、パラメータ ライブラリのメンバの設定パラメータに z/OS のシステム記号を含めることができます。

注: CA CSM には MSMCPARM パラメータ ライブラリ メンバが用意されており、そのメンバにはデフォルトの SCS アドレス空間パラメータが含まれています。

MSMCPARM メンバ

アドレス空間パラメータを指定する MSMCPARM メンバ ドキュメントに、以下の要素を含めることができます。

データ リカバリ パラメータ

データ リカバリ用のディスク記憶域の SCS アドレス空間の使用と関連するパラメータを設定します。 このパラメータは、リカバリ用に既存データを保存するために作成されたデータ セットを割り当てるときに使用されます。

データ リカバリ パラメータは、以下の属性を使用して指定されます。

dsnhlq

データ リカバリ用に作成されたデータ セットを割り当てるときに使用される、データ セット名の高レベル修飾子を指定します。

制限： 1 ～ 17 バイト。 値には静的および動的システム記号、およびインストールで定義された静的システム記号を含めることができます。

注: システム記号の一覧については、IBM の「*z/OS MVS Initialization and Tuning リファレンス*」を参照してください。

（オプション） *&SYSUID*

どのデータ セットがリカバリ用に作成されたかという設定リクエストを開始した CA CSM ユーザのユーザ ID を指定します。

制限： アンパサンド文字（&）は XML ドキュメントの属性値のため、リテラルとして指定できません。 この文字は、後続の文字を制御シーケンスに変換するために、文字列「*&*」を使用して変換する必要があります。

例： '&SYSNAME..MSM', dsnhlq='&SYSNAME..MSM'

デフォルト： &SYSUID..MSMDATA

単位

データ リカバリ用に作成された z/OS データ セットを割り当てるときに使用される、単位名を指定します。

制限： 1 ～ 8 バイト。

デフォルト： なし

volser

データ リカバリ用に作成されたデータ セットを割り当てるときに使用される、ボリューム シリアル番号を指定します。

制限： 1 ～ 6 バイト。 シリアル番号の文字は英文字、各国文字、またはハイフンである必要があります。

デフォルト： なし

mgmtclas

データ リカバリ用に作成されたデータ セットを割り当てるときに使用される、SMS 管理クラスを指定します。

制限： 1 ～ 8 バイト。 クラス名の先頭文字は、英文字または各国文字である必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： なし

storclas

データ リカバリ用に作成されたデータ セットを割り当てるときに使用される、SMS ストレージ クラスを指定します。

制限： 1 ～ 8 バイト。 クラス名の先頭文字は、英文字または各国文字である必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： なし

TCP/IP

CA CSM の他のコンポーネントと通信するために、SCS アドレス空間と TCP/IP 間のインターフェース用のアドレス空間パラメータを指定します。

TCP/IP パラメータは、以下の属性を使用して指定されます。

ipaddr

SCS アドレス空間が他の CA CSM コンポーネントからの TCP 接続要求を受け付けるインターフェースの IP アドレスを指定します。

制限： 標準のドット区切り 10 進表記法を使用した IPv4 アドレス。

（オプション）RFC 4291 の IPv6 アドレス体系で定義されている標準のテキスト フォームの 1 つを使用した IPv6 アドレス

例 1： 0.0.0.0

例 2： ::

注: IPv4 の未指定のアドレス 0.0.0.0 は、SCS アドレス空間がすべての IPv4 インターフェースからの TCP 接続要求を受け入れることを指示するために使用されます。 IPv6 の未指定のアドレス :: は、SCS アドレス空間がすべての IPv4 および IPv6 インターフェースからの TCP 接続要求を受け付けることを指示するために使用されます。

デフォルト： ::

port

SCS アドレス空間が、他の CA CSM コンポーネントからの TCP 接続要求をリッスンするために使用するポート番号を指定します。

制限： 最大ポート番号は 65535 で、数値である必要があります。

デフォルト： 49152

コンソール

z/OS コマンドの発行、コマンド応答の受信、非送信請求メッセージ トラフィックの受信を行う拡張 MCS コンソールの SCS アドレス空間の使用法に関係するパラメータを設定します。

コンソール パラメータは、以下の属性を使用して指定されます。

prefix

拡張 MCS コンソール名の作成に使用されます。

制限： 1 ～ 5 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： CAMSM

auth

拡張 MCS コンソールが z/OS コマンドを発行するための権限を指定します。

割り当てられた権限により、コンソールから入力できるコマンドが指定されます。 空白スペースまたはカンマで複数の値を区切ります。

コンソールから以下の値のうち 1 つ以上を入力します。

MASTER

コンソールがマスタ コンソールとして動作することを可能にし、そのコンソールがすべての MVS コマンドを発行します。

ALL

コンソールによる、システム制御コマンド、入力および出力コマンド、コンソール制御コマンドおよび情報提供コマンドの発行が可能になります。

SYS

コンソールによる、システム制御コマンドおよび情報提供コマンドの発行が可能になります。

IO

コンソールによる、入力および出力コマンド、および情報提供コマンドの発行が可能になります。

CONS

コンソールによる、コンソール制御コマンドおよび情報提供コマンドの発行が可能になります。

INFO

コンソールによる、情報提供コマンドの発行が可能になります。

デフォルト： INFO

注: SYS、IO および CONS は、任意の組み合わせで指定できます。 他はすべて、排他関係にあります。

特定の権限レベルでコンソールから入力できるコマンドについての詳細については、IBM の「*z/OS MVS System Commands Reference*」を参照してください。

注: セキュリティ製品の設定は、セキュリティ製品によって保護された z/OS コマンド用のコンソール コマンド権限設定をオーバーライドします。たとえば CA ACF2 for z/OS は、OPERCMDS クラスがアクティブの場合、コマンドを保護するためのプロファイルが定義されます。

SAF

System Authorization Facility（SAF）に対する SCS アドレス空間インターフェースに関連するパラメータを設定します。

SAF パラメータは以下の属性を使用して指定されます。

application

SCS アドレス空間に割り当てられるアプリケーション名を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： MSMCAPPL

requestor

サブシステムに存在する制御ポイント内で一意の制御ポイントを割り当てる、SCS アドレス空間に割り当てられる名前を指定します。

注: リクエスタ名を指定し、また IBM RACF がインストールされている場合、IBM RACF ルータ テーブルを、一致するエントリで更新する必要があります。 テーブルを更新しない場合、IBM RACF 処理が省略されます。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： なし

subsystem

SCS アドレス空間に割り当てられるサブシステム名、バージョンおよびリリース レベルを指定します。

注: サブシステム名を指定し、また IBM RACF がインストールされている場合、IBM RACF ルータ テーブルを、一致するエントリで更新する必要があります。 テーブルを更新しない場合、IBM RACF 処理が省略されます。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： なし

SSL

System SSL Cryptographic Services に対する SCS アドレス空間インターフェースと関連するパラメータを設定します。

SSL パラメータは以下の属性を使用して指定されます。

keyring

リモート システムからの暗号化データに使用される、キー リング データベース ファイルのパスとファイル名、または SCS アドレス空間に割り当てられたユーザ ID 用の CA ACF2 for z/OS、CA Top Secret for z/OS または IBM RACF などの外部セキュリティ マネージャで定義された SAF キー リングのラベルを指定します。

デフォルトの証明書を取得してクライアント側に送り、通信用の接続を保護する処理を開始するために使用されます。

デフォルト： なし

stashfile

keyring 属性がキー リング データベース ファイルのパスおよびファイル名に設定される場合、stashfile のパスおよびファイル名を指定します。

stashfile には、キー リング データベース ファイルにアクセスするためのパスワードが含まれています。

制限： keyring 属性がキー リング データベース ファイル名に設定されている場合は必須です。

デフォルト： なし

AUX

SCS AUX アドレス空間に関連付けるパラメータを設定します。

SCS AUX アドレス空間パラメータは、以下の属性を使用して指定されます。

procname

SCS AUX アドレス空間用のソース JCL を含んだ、JCL プロシージャ ライブラリ メンバの名前を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： MSMCAUX (P. 330)

jobname

SCS AUX アドレス空間に割り当てられるジョブ名を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字である必要があります。

デフォルト： ソース JCL がプロシージャの場合は、JCL プロシージャ ライブラリ メンバ名、またはソース JCL がジョブの場合は、JOB ステートメントに割り当てられるジョブ名。

reusasid

SCS AUX アドレス空間に対して、再利用可能な ASID を要求するかどうかを決定します。

SCS AUX アドレス空間は、以下のいずれかの値を受け取ります。

YES

DIAGxx PARMLIB メンバに REUSASID（YES）も指定されている場合、SCS AUX アドレス空間に再利用可能な ASID が割り当てられます。

NO

SCS AUX アドレス空間には、再利用可能な ASID は割り当てられません。

デフォルト： YES

注: CA Technologies 製品の設定で使用される製品またはプログラムに、再利用可能な ASID を使用するためのアップグレードが実行されていない場合、再利用可能な ASID を使用するとシステム 0D3 の異常終了（ABEND）が発生します。

ASID の再利用の詳細については、IBM の「*z/OS MVS Programming: Extended Addressability Guide*」を参照してください。

maxactive

同時にアクティブな SCS AUX アドレス空間の最大数を指定します。

制限： 1 ～ 20 の数字

デフォルト： 20

SCS アドレス空間メッセージ ログ（SCSLOG）

SCS アドレス空間メッセージ ログ（SCSLOG）は、SCS アドレス空間によって書き込まれる、すべてのメッセージの詳細ログです。

z/OS ハードコピー メッセージ ログに書き込まれる SCS アドレス空間メッセージは、SCSLOG にも書き込まれています。 さらに、SCSLOG にはより詳細なメッセージが書き込まれており、問題を診断するときに役に立ちます。従って、SCSLOG は SCS アドレス空間のアクティビティに関する、より完全な記録になります。

SCSLOG は、z/OS UNIX System Services（USS） の syslog デーモンを使用して実行されます。syslog デーモンは z/OS システム製品の一部です。このデーモンは、USS の syslogd コマンドを使用して明示的に開始される必要があります。

注: syslog デーモンの詳細については、IBM の「*z/OS Communications Server: IP Configuration*」および「*z/OS Communications Server: IP Configuration*」リファレンスを参照してください。

syslog デーモンの設定

設定ファイルにより、syslog デーモン（syslogd）の処理が制御されます。

デフォルト： `/etc/syslog.conf`

設定ファイル内のステートメントにより、ログ記録ルール、およびログメッセージの出力先が定義されます。syslog デーモン設定ファイルでログ記録ルールを定義し、特定の送信先に SCS アドレス空間メッセージを送信します。

ログ記録ルールはファシリティ名と優先度コードを使用して定義されます。 メッセージを生成するプログラムのユーザ ID およびジョブ名も、ログ記録ルールで指定することができます。

注: AUX アドレス空間のメッセージは、SCS アドレス空間で実行中のプロセスによって syslog デーモンに書き込まれています。 SCS アドレス空間のジョブ名用のログ記録ルールのみを定義してください。AUX アドレス空間のジョブ名用のログ記録ルールは必要ありません。

syslog デーモンに書き込まれたすべての SCS アドレス空間のメッセージは、ファシリティ名が「user」で書き込まれています。

syslog デーモンに書き込まれた各 SCS アドレス空間のメッセージは、以下のいずれかの優先度コードで書き込まれています。

info

この優先度コードのメッセージは、情報を提供するメッセージです。

warning

この優先度コードのメッセージは警告メッセージです。

error

この優先度コードのメッセージはエラー メッセージです。

crit

この優先度コードのメッセージは深刻なエラー メッセージです。

debug

この優先度コードのメッセージはデバッグ メッセージです。

例: syslog デーモンへのステートメントの追加

MSMCPROC という名前のジョブによって書き込まれたすべてのメッセージを、ファイル /tmp/syslogd/msmcproc.syslog に書き込めるようにするには、以下のステートメントを syslog デーモン設定ファイルに追加し、変更を有効化します。

```
#
#  CA CSM SCS message log(SCSLOG)
#
*.MSMCPROC.*.* /tmp/syslogd/msmcproc.scslog
```

syslog デーモン設定変更の有効化

syslog デーモン設定ファイルを更新した後、syslog デーモンに SIGHUP 信号を送信して、デーモンに設定ファイルを再度読み込ませ、修正したパラメータを有効化する必要があります。

USS の kill コマンドを使用して、SIGHUP 信号を送信します。

このコマンドの構文は以下の通りです。

```
kill -s SIGHUP pid
```

pid

syslog デーモンのプロセス ID を指定します。

デーモンの開始方法により異なりますが、syslog デーモンはファイルにデーモンのプロセス ID を保存するため、それをデーモンの再設定に使用できます。

- syslog デーモンが normal モード、または local-only モードで開始される場合、ファイル名は以下のとおりです。

  /etc/syslog.pid

- syslog デーモンが network-only モードで開始される場合、ファイル名は以下のとおりです。

  /etc/syslog_net.pid

syslog デーモンは、設定ファイルを再度読み込んだ後、設定で指定されたファイルにログ メッセージを追加し続けます。

注: syslog -c オプションが指定されない限り、syslog デーモンによって使用されるすべてのログ ファイルは、syslog デーモンが開始もしくは再設定される前に、z/OS UNIX ファイル システムに作成される必要があります。 -c オプションが指定される場合、syslog デーモンは存在していないログ ファイルを動的に作成します。

汎用トレース機能

SCS アドレス空間は汎用トレース機能（GTF）を使用し、診断用のデータを収集します。 GTF は z/OS システム製品の一部です。 GTF は、START GTF コマンドを発行して明示的に有効化する必要があります。

注: GTF の詳細については、「*IBM MVS Diagnosis Tools and Service Aids*」を参照してください。

GTF の開始

GTF を開始するには、START GTF コマンドを入力します。 IBM のプロシージャまたは GTF 開始用の内部プロシージャを使用して、GTF を開始できます。

注: 複数の GTF インスタンスを同時にアクティブにできます。各インスタンスは、スターティッド タスクとして、それ自身のアドレス空間で実行されます。

各 GTF のインスタンスには一意の識別子を割り当てることができ、その識別子は START GTF コマンドで指定されます。 この識別子により、GTF の特定のインスタンスの認識と制御が可能になります。 一意の識別子が指定されない場合、オペレーティング システムはトレース データ セットがあるデバイスのデバイス番号を割り当てます。

GTF がトレースするイベントは、オプションとして指定します。 SCS アドレス空間に対し、USRP と JOBNAMEP オプションを指定します。

USRP GTF オプションを指定した後、GTF はイベント識別子（EID）の一覧を求めるプロンプトが表示されます。

SCS アドレス空間は以下の EID を使用します。

301

SCS アドレス空間のインフラストラクチャ コンポーネント用の診断データを収集します。

302

SCS アドレス空間の通信サーバ コンポーネント用の診断データを収集します。

303

SCS アドレス空間の通信サーバ イベント API コンポーネント用の診断データを収集します。

304

SCS アドレス空間のコンテナ セクション コンポーネント用の診断データを収集します。

305

SCS アドレス空間の実装エンジン コンポーネント用の診断データを収集します。

306

SCS アドレス空間のサービス セクション コンポーネント用の診断データを収集します。

307

SCS アドレス空間のシステム情報エージェント コンポーネント用の診断データを収集します。

注: 不要な情報の出力を回避するには、USRP オプションを使用して GTF のトレース出力を制限します。

JOBNAMEP GTF オプションが指定されている場合、どのジョブ名に対するトレース出力を収集するかのリストを求めるプロンプトが表示されます。メインまたは補助の SCS アドレス空間の名前を指定します。一般的な名前は、順番に MSMCPROC (P. 330) および MSMCAUX です。

例

CA CSM には以下の GTF トレース オプションを含む MSMCGTFP サンプル メンバが用意されています。

```
TRACE=USRP,JOBNAMEP
USR=(301,302,303,304,305,306,307)
JOBNAME=(MSMCPROC,MSMCAUX)
END
```

GTF の停止

GTF を停止するには、STOP GTF コマンドを発行します。 START GTF コマンドの識別子を指定します。識別子が START GTF コマンドで指定されていない場合は、トレース データ セットがあるデバイスのデバイス番号で識別子を指定します。

付録 A: CA CSM の実装およびステータス

このセクションには、以下のトピックが含まれています。

実装チェックリスト

このセクションのチェックリストを使用し、それぞれのロールに関係するタスクが完了したことを確認します。

ネットワーク管理者

以下の Web サイトへのアクセス権を設定します。

- supportservices.ca.com（HTTPS ポート番号 443 を使用）
- ftp.ca.com（FTP ポート番号 21 を使用）
- ftpca.ca.com（FTP ポート番号 21 を使用）

  注: CA CSM はこの FTP サーバを使用して、最小限の情報を収集します。この情報には、CA サポート Online Web サイトのサイト ID、製品、ユーザ ID などがあります。 サイトのアクセス ルールにより、これらの情報の収集を目的として確立された FTP 接続が拒否されることがあり、あるいはその他の理由により接続が確立できないことがあります。 その後も、CA CSM は引き続き稼働します。
- scftpd.ca.com（FTP ポート番号 21 を使用）

- ftpdownloads.ca.com（FTP ポート番号 21 を使用）
- supportftp.ca.com（FTP ポート番号 21 を使用）
- sdownloads.ca.com（HTTPS ポート番号 443 を使用）

  注: ［Settings］ページの［System Settings］ - ［Software Acquisition］で［Use HTTPS for Downloads］取得オプションを使用する場合、sdownloads.ca.com のみが必要です。 ポート 80 とポート 443 の両方に対して ca.com ドメインを許可する場合、sdownloads.ca.com を許可する必要はありません。

さらに、ネットワーク管理者は localhost のドメイン ネーム システム（DNS）エントリを定義する必要があります。

セキュリティ管理者

1. 以下のデータ セットまたはライブラリへの UPDATE 権限を、CA CSM を実装するユーザに付与します。
   - SYS*x*.PARMLIB
   - CA CSM アドレス空間を開始するために使用される、JCL ジョブを格納するプロシージャ ライブラリ（たとえば、SYS3.PROCLIB）
   - （オプション）CA CSM データ セットのプレフィクス用にエイリアス エントリを定義する場合のマスタ カタログ
2. CA CSM セットアップ ユーティリティ MSMSetup.sh に関連付けられたユーザ ID に、以下のアクセス権を付与します。
   - USS へのアクセス権
   - UNIX に関連する、以下の FACILITY クラスのプロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）
     - BPX.SERVER（UPDATE 権限）
     - BPX.CONSOLE（READ 権限）
   - SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）

- SMP/E GIMUNZIP ハッシュ検証を実行するための CSFSERV クラス プロファイル、CSFOWH（READ 権限）へのアクセス許可
- オプション ファイル (P. 240)で指定された修飾子（CA CSM MVS SMP/E およびランタイム データ セット）用のデータ セットの作成および修正の許可

  注: ユーザ ID は BPX.SUPERUSER アクセス権を持つことができ、それを SUPERUSER に切り替えることができます。 その後、その切り替えられた SUPERUSER ID には、オプション ファイル (P. 240)で指定された MVS データ セット修飾子の作成および修正のアクセス権が必要です。
- IBM RACF を使用している場合、プログラム制御用の以下のデータ セットにアクセスします。
  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - メンバ IEANTCR、IEANTDL および SYS1.CSSLIB の IEANTRT
  - メンバ JVMLDM60（31 ビット Java 6.0 用）、または Java のロード モジュールがインストールされているデータ セットの JVMLDM66（64 ビット Java 6.0 用）。

    または
  - メンバ JVMLDM61（31 ビット Java 6.0.1 用）、または Java のロード モジュールがインストールされているデータ セットの JVMLDM67（64 ビット Java 6.0.1 用）。

    または
  - メンバ JVMLDM70（31 ビット Java 7.0 用）、または JVMLDM76（64 ビット Java 7.0 用）。
  - （オプション）オプションの EXIT として IDIXCEE を使用する場合にのみ、SYS1.IDI.SIDIAUTH のメンバ IDIXCEE。

  注: リソースを表示するには、RLIST コマンドを発行します。

  IBM RACF を制御プログラムに設定できます。 リソースが存在しない場合は、以下のコマンドを発行します。

  ```
  RDEFINE PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
  ```

  以下に例を示します。

  ```
  RDEFINE PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
  ```

リソースが存在する場合は、以下のコマンドを発行します。

```
RALTER PROGRAM member ADDMEM('hlq.libraryname'//NOPADCHK) UACC(READ)
```

以下に例を示します。

```
RALTER PROGRAM IEANTCR ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
```

注: データ セットの全メンバを制御済みプログラムとして設定するには、メンバ名をアスタリスク（*）で置換します。 以下に例を示します。

```
RDEFINE PROGRAM * ADDMEM('SYS1.CSSLIB'//NOPADCHK) UACC(READ)
```

重要: zFS を使用する予定がある場合は、プログラム制御に IOE.SIOELMOD（または同等のライブラリ）を追加します。

3. CA CSM アプリケーション サーバ（MSMTC ジョブまたはスターティッド タスク）に関連付けられたユーザ ID に、以下のアクセス権を付与します。
   - USS へのアクセス権
   - ファイル システムの作成およびマウント権限
   - UNIX に関連する、以下の FACILITY クラスのプロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）
     - BPX.SERVER（UPDATE 権限）
     - BPX.CONSOLE（READ 権限）
   - SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）
4. CA CSM ユーザ用の OMVS セグメントをセットアップします。

USS 管理者

以下の構造を使用し、USS パスをセットアップします。

```
/u/users/msmserv（プライマリ マウント ポイント）
     msminstall（1000 シリンダ）
     msm（750 シリンダ）
     msmruntime（750 シリンダ）
     mpm（CA CSM が使用するマウント ポイント）
```

Systems Programmer

1. 必須要件が満たされることを確認します。
2. オプション ファイル キーワードを確認し、必要な値を収集します。
3. CA CSM をダウンロードします。
4. 以下のように CA CSM を解凍します。

   ```
   pax -rvf 51000068X01.pax.Z
   ```

   注: Z サフィックスを含む完全な pax ファイル名では、大文字と小文字が区別されます。 pax コマンドを発行するシステムでは、ファイル名に大文字や小文字が正確に使用されていることを確認してください。必要に応じて、ファイル名を変更します。
5. UNZIPJCL をカスタマイズしてサブミットし、CA CSM 製品ファイルを展開します。
6. MSMSetupOptionsFile.properties ファイルをカスタマイズします。
7. MSMSetup.sh を実行します。
8. 以下のメンバを順番に使用して、CA CSM を開始します。
   - MSMMUFS JCL メンバまたは MSMMUF PROCLIB メンバ
   - MSMDBSVS JCL メンバまたは MSMDBSRV PROCLIB メンバ
   - MSMTCSRV JCL メンバまたは MSMTC PROCLIB メンバ
9. Web ブラウザを使用して CA CSM にアクセスし、初期設定を実行します。
10. CAIRIM をセットアップして IPL 時に CA Datacom/MSM SVC をロードします。
11. USS ディレクトリをクリーン アップします。
12. 製品の展開をサポートするため、各 CA Technologies 製品の展開アクティブ化要素が取得され、インストールされていることを確認してください。

    注: 製品の展開の詳細については、「*ユーザ ガイド*」の「*製品の展開*」の章を参照してください。

オプション ファイル キーワード

CA CSM セットアップ ユーティリティは、MSMSetup ディレクトリにある MSMSetupOptionsFile.properties オプション ファイルのコンテンツを使用して、CA CSM のインストールおよびセットアップ プロセスをカスタマイズします。

オプション ファイルは以下のようなキーワードを使用し、「*option_keyword=value*」の形式でオプションの値を指定します。

重要: オプション ファイルで使用されるキーワードは、CA CSM インストール セットアップ プロセスに固有のものです。 一部のキーワードの値は、この処理中に CA CSM で処理可能な値に変換されます。CA サポートから指示のない限り、CA CSM の他の領域の同様のキーワードに、これらの値を使用しないでください。

MSMProdPaxPath

展開された CA CSM ファイルのパスを指定します。この値は、UNZIPJCL ジョブの CA CSM 製品アーカイブ ID に対して定義されたパスです。

例： /u/users/msmserv/msminstall/MSMProduct

JAVAPATH

IBM Java SDK for z/OS コンポーネントのパスを指定します。

例： /usr/lpp/java/J6.0

SMP/E のインストール データ セットおよび場所の詳細

重要: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンの CA CSM に移行する場合、このセクションに示されているすべてのキーワードには一意の値を指定します。 新しいキーワード値は、以前のバージョンの CA CSM の値とは異なっている必要があります。

CSIHLQ

統合されたソフトウェア インベントリ（CSI）データ セット、および SMPPTS や SMPSTS などのその他の SMP/E データ セットのプレフィクス（高レベル修飾子）を指定します。

デフォルト： CAI

TargetHLQ

ターゲット データ セットのプレフィクスを指定します。

デフォルト： CSIHLQ の値

重要: TargetHLQ の値は RunTimeMVSHLQPrefix および DatabaseHLQ の値とは異なる必要があります。

TargetZoneName

SMP/E 環境のターゲット ゾーン名を指定します。

デフォルト： CAIT

DlibHLQ

配布データ セット用のプレフィクスを指定します。

デフォルト： CSIHLQ の値

重要: DlibHLQ の値は RunTimeMVSHLQPrefix および DatabaseHLQ の値とは異なる必要があります。

DlibZoneName

SMP/E 環境の配布ゾーン名を指定します。

デフォルト： CAID

MSMPATH (P. 266)

CA CSM をインストールする USS ディレクトリのパスを指定します。このディレクトリは CA CSM のルートになり、CA CSM セットアップ ユーティリティを実行するときに利用でき、書き込み可能である必要があります。

マウント ポイントを定義する必要があります。 必要なファイル システムのスペースは約 250 シリンダです。

ランタイム データ セットおよび場所の詳細

重要: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンの CA CSM に移行する場合、このセクションに示されているすべてのキーワードには一意の値を指定します。 新しいキーワード値は、以前のバージョンの CA CSM の値とは異なっている必要があります。

RunTimeMVSHLQPrefix

CA CSM ランタイム データ セット用のプレフィクスを指定します。これはターゲット データ セットのランタイム コピーです。

重要: RunTimeMVSHLQPrefix の値は TargetHLQ および DlibHLQ とは異なる必要があります。

RunTimeUSSPath (P. 266)

CA CSM ランタイムに使用する USS ディレクトリのパスを指定します。CA CSM セットアップ ユーティリティを実行するとき、このディレクトリが利用でき、書き込み可能である必要があります。

必要なスペースは約 750 シリンダです。

データベース データ セットおよび場所の詳細

DatabaseHLQ

インストール プロセス中に作成される CA Datacom データ セット用のプレフィクスを指定します。

デフォルト： RunTimeMVSHLQPrefix の値

重要: DatabaseHLQ の値は TargetHLQ および DlibHLQ とは異なる必要があります。

重要: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンの CA CSM への移行を計画している場合、このキーワードには一意の値を指定します。 新しいキーワード値は、以前のバージョンの CA CSM の値とは異なっている必要があります。

CA Datacom/MSM

MUFname

CA Datacom/MSM Multi-User 機能（MUF）の優先名を指定します。 CA Datacom はこの名前を使用し、MUF の複数インスタンスを区別します。サイトのシステムまたはシスプレックスに複数の MUF がある場合は、この名前が CAICCI Plex 内で一意であることを確認してください。

例： MSMR5MUF

制限： 8 文字

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

ServerName

CA Datacom/MSM サーバの優先名を指定します。 CA Datacom はこの名前を使用し、サーバの複数のインスタンスを区別します。 サイトのシステムやシスプレックスに複数の CA Datacom/MSM サーバがある場合は、この名前が CAICCI Plex 内で一意であることを確認します。

注: この名前は CAICCI Plex 全体で一意である必要があります。また、サーバ名およびアプリケーション ID はシスプレックス内で一意である必要があります。これらの値を一意にしておくことで、データベース サーバがスタートアップ中に失敗することを防ぐことができます。

例： MSMR5SRV

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

CXXNAME

CA Datacom/AD Directory が初期化されるときの識別子名を指定します。この値は CA Datacom DBUTLTY INIT CXX オプションの CXXNAME パラメータに使用されます。

制限： 8 文字

デフォルト： CAMSM

注: CXXNAME の命名規則の詳細については、「*CA Datacom/DB DBUTILTY Reference Guide*」を参照してください。

SVCNO

CA Datacom/MSM 用の SVC 番号を指定します。

注: CA Datacom r11 の実行中インスタンスが使用しているものと同じ SVC を使用しないでください。

制限： 200 ～ 255

注: CA MSM r3.1 からアップグレードしている場合、別の SVC を使用する必要があります。ユーザが CA CSM の既存顧客で、CA MSM V4.0 あるいはそれ以降のバージョンから移行している場合、このパラメータ値は以前のバージョンの値と同じでかまいません。

ポート、データ セットおよび USS ディレクトリ

注: CA CSM の既存バージョンをすでに使用していて、最新のバージョンへ移行する場合、このセクションで説明されているすべてのキーワード値は、旧バージョンの値と同じでかまいません。

MSMServerPortNo

（CA CSM アプリケーション サーバの HTTP ポート） CA CSM への Web ベース アクセスに使用するポート番号を指定します。

デフォルト： 22120

MSMDSIPORTNO

（CA DSI Server ポート） CA DSI Server のポート番号を指定します。CA CSM はこのポート番号を内部で使用して、セキュリティ機能を提供します。

デフォルト： 22130

MSMConnectorRedirectPortNo

（CA CSM アプリケーション サーバのリダイレクト ポート）リクエストがリダイレクトされるポート番号を指定します。 非 SSL ポートでリクエストが受信され、そのリクエストが SSL を必要とする転送保証を備えたセキュリティ制約に従う場合、リダイレクトが発生します。

デフォルト： 22140

MSMTomcatServerShutdownPortNo

（CA CSM アプリケーション サーバのシャットダウン ポート）CA CSM アプリケーション サーバ (P. 329)がシャットダウン コマンドをリッスンするポート番号を指定します。

デフォルト： 22150

詳細:

TCP/IP ポートの予約 (P. 52)

マウント ポイント マネージャ

MVSHFSDsnPrefix

ファイル システム データ セット名のプレフィクスを指定します。 この値は、Web ベース インターフェースの［Mount Point Management］ページの［Data Set Prefix］のデフォルトを設定します。 CA CSM 管理者はこの値をオーバーライドできます。

デフォルト： OMVSUSR.CAMSM

重要: 以前のバージョンから移行する場合は、このキーワードの値が以前のバージョンの値と同じであることを確認します。

MountPath (P. 266)

CA CSM が作業ファイルに使用できる USS ディレクトリのパスを指定します。セットアップ ユーティリティの実行時に、このディレクトリが利用可能である必要があります。 この値は、Web ベース インターフェースの［Mount Point Management］ページの［Application Root］フィールドのデフォルトを設定します。 CA CSM 管理者はこの値をオーバーライドできます。

重要: 以前のバージョンから移行する場合は、このキーワードの値が以前のバージョンの値と同じであることを確認します。

mpmAutomount

CA CSM が起動時にファイル システムをマウントするかどうかを指定します。

以下のオプションがあります。

- Y（Yes）
- N（No）

デフォルト： Y

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

USSFileSystemType

一時ファイル用にファイル システムとして HFS または zFS のどちらを使用するかを指定します。

値： HFS または ZFS

デフォルト： ???

注: zFS ファイル システムの使用をお勧めします。 HFS ファイル システムから zFS ファイル システムに移行する方法の詳細については、最新の「*IBM z/OS Migration*」を参照してください。

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

mpmAllocation

［Settings］タブの［Mount Point Management］ページで、ファイル システムに新しいデータ セットを割り当てるときに SMS を使用するかどうかを指定します。

以下のオプションがあります。

- SMS
- NONSMS

デフォルト： SMS

mpmStorageClass

Web ベース インターフェースの［Mount Point Management］ページで DASD の SMS ストレージ クラスを指定します。 この値は、製品インストールおよびメンテナンス時に使用されます。

mpmAllocation に SMS が設定されると、このパラメータが使用されます。 デフォルトのサイト設定を使用するには、このパラメータを空白のままにします。

デフォルト： サイト固有の SMS デフォルト設定

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

mpmMgmtClas

［Settings］タブの［Mount Point Management］ページでファイル システム データ セットに対する SMS 管理クラスを指定します。

mpmAllocation に SMS が設定されると、このパラメータが使用されます。 デフォルトのサイト設定を使用するには、このパラメータを空白のままにします。

mpmDataClas

［Settings］タブの［Mount Point Management］ページで、ファイル システム データ セットの SMS データ クラスを指定します。

mpmAllocation に SMS が設定されると、このパラメータが使用されます。 デフォルトのサイト設定を使用するには、このパラメータを空白のままにします。

mpmUnit

［Settings］タブの［Mount Point Management］ページでデータ セットを配置する DASD のタイプを指定します。

mpmAllocation に NONSMS が設定されると、このパラメータが使用されます。 値は空白でもかまいません。

mpmVolumeSer

Web ベース インターフェースの［Mount Point Management］ページで、DASD の NONSMS ボリューム シリアル番号を指定します。 この値は、製品インストールおよびメンテナンス時に使用されます。

mpmAllocation に NONSMS が設定されると、このパラメータが使用されます。 値は空白でもかまいません。 値を指定する場合、その値はオンライン ボリュームのボリューム シリアル番号である必要があります。

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

TempSpaceCleanupInterval

CA CSM が一時ワークスペースをクリーンアップする時間間隔を分単位で指定します。 値にゼロ（0）を指定すると、この機能が無効になります。

デフォルト： 60

制限： 1440

ソフトウェア インストール サービス

sisExecutorOutputStorclas

CA CSM ソフトウェア インストール サービスを使用した製品インストール中に一時データに使用する、プログラムを実行したデータ セットの SMS ストレージ クラスを指定します。

値は空白でもかまいません。

デフォルト： サイト固有の SMS デフォルト設定

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

sisExecutorOutputUnit および sisExecutorOutputVolser

一時データに使用する、プログラムを実行したデータ セットの DASD のタイプおよびボリューム シリアル番号を指定します。

値は両方とも空白でかまいません。 値を指定する場合、sisExecutorOutputVolser はオンライン ボリュームのボリューム シリアル番号である必要があり、また sisExecutorOutputUnit は有効なユニット デバイス タイプである必要があります。

sisGimunzipTempVolser

CA CSM ソフトウェア インストール サービスによる製品インストール中に一時データ セットに使用する、GIMUNZIP によって作成された DASD のボリューム シリアル番号（SMS または NONSMS 管理）を指定します。

値は空白でもかまいません。値を指定する場合、sisGimunzipTempVolser は、*（アスタリスク）にするか、またはオンライン ボリュームのボリューム シリアル番号である必要があります。

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

sisGimunzipTempPrefix

製品インストールおよびメンテナンス時に、GIMUNZIP 出力一時データ セット名として CA CSM が使用するプレフィクスを指定します。 作成された一時作業ファイルは、SMP/E で制御されたデータ セットではありません。 CA CSM は製品インストール プロセスで、それらのファイルを削除します。 これらのファイルは、製品を SMP/E 環境のグローバル ゾーンに RECEIVE する際に、SMP/E 処理の入力関連ファイルとして使用されます。

制限： 12 ～ 19 文字（*ジョブ名*に使用される文字数により異なる）

注: デフォルトの 6 文字の *ジョブ名*を使用する場合、GIMUNZIP 一時プレフィクスには 14 文字まで入力できます。

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

DATASETSUFFIX

製品インストールおよびメンテナンス時に、パッケージを格納するためにソフトウェア カタログに割り当てられたファイル システム データ セットの名前として CA CSM が使用する修飾子を指定します。 完全なデータ セット名は、次のような形式で表示されます。
MVSHFSDsnPrefix.DATASETSUFFIX*nnnn*

nnnn

CA CSM が修飾子に自動的に追加する、一意の数値識別子を表します。

デフォルト： CASC

制限： 4 文字

例

MVSHFSDsnPrefix = OMVSUSR.CAMSM

DATASETSUFFIX = CASC

完全なデータ セット名： OMVSUSR.CAMSM.CASC1234

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

sisExecutorServerDsnPrefix

製品インストールおよびメンテナンス時に、SMP/E の実行によって作成される一時出力ファイルを格納するためのデータ セット プレフィクスを指定します。 この値は空白でもかまいません。

デフォルト： *SAF_userid*

制限： 24 文字

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

セキュリティ

safSecurity

Web ベース インターフェース上のリソースに対してセキュリティ チェックを有効にするかどうかを指定します。

デフォルト： N

注: ユーザが CA CSM の既存バージョンをすでに使用していて、最新バージョンへ移行する場合、このパラメータ値は以前のバージョンと同じ値でかまいません。

safResourceClass

リソース プロファイルで CA CSM がセキュリティ ルールとして使用する SAF リソース クラス名を指定します。

デフォルト： CAMSM

SAF セキュリティ マネージャを無効にする場合、以下のパラメータを Apply します。

sysTaskDeleteOverrideEnabled

CA CSM ユーザにタスクを削除させるかどうかを指定します。

Y

任意のユーザが任意の完了タスクを削除できます。

N

ユーザは完了したタスクを削除できません。

デフォルト： N

SMP/E GIMUNZIP

HASH

SMP/E GIMUNZIP のハッシュ検証を実行するかどうかを指定します。

デフォルト： Y（推奨）

ハッシュ検証を実行する場合、以下のパラメータを Apply します。

ICSF

システムに Integrated Cryptographic Services Facility（ICSF）がインストールされているかどうかを指定します。

デフォルト： Y

ハッシュ検証を実行し、ICSF がインストールされていない場合、以下のパラメータを Apply します。

SMPCPATH

SMP/E Java アプリケーション クラスへのパスを指定します。

例： /usr/lpp/smp/classes

SMP/E GIMSMP

CSIVOL

CA CSM SMP/E データ セットを配置する DASD のボリューム シリアル番号を指定します。

デフォルト： *

SMS のデフォルト ボリュームを使用する場合は、「*」を指定します。

注: SmpeVOL に「*」を指定するが、サイトに SMS で指定されたデフォルトのボリュームも標準ボリュームもない場合、最初のインストール ジョブ（新規インストール用の CSMN5102、またはアップグレード用の CSMU*xx*02）が、CA CSM SMP/E 環境を割り当てる間に IDCAMS エラーで失敗する場合があります。そのシナリオでは、有効な SMS ボリュームまたは非 SMS のボリュームを指定し、インストーラを再実行します。

TargetVOL

CA CSM SMP/E ターゲット データ セットを配置する DASD のボリューム シリアル番号を指定します。

デフォルト： CSIVOL の値

SMS のデフォルト ボリュームを使用する場合は、「*」を指定します。

DlibVOL

CA CSM SMP/E 配布データ セットを配置する DASD のボリューム シリアル番号を指定します。

デフォルト： CSIVOL の値

SMS のデフォルト ボリュームを使用する場合は、「*」を指定します。

RuntimeVOL

CA CSM ランタイム データ セットを配置する DASD のボリューム シリアル番号を指定します。

値： 空白または *、または有効な SMS ボリュームまたは非 SMS ボリューム

SMS のデフォルト ボリュームを使用する場合は、「*」を指定します。

デフォルト： *

DatabaseVOL

インストール プロセス時に作成された CA Datacom データ セットを配置する DASD のボリューム シリアル番号を指定します。

値： 空白または *、または有効な SMS ボリュームまたは非 SMS ボリューム

SMS のデフォルト ボリュームを使用する場合は、「*」を指定します。

デフォルト： RuntimeVOL の値

TEMPUNIT

一時作業データ セット用の非公式のユニットを指定します。

デフォルト： SYSDA

SMP/E ストレージ

STORAGE

SMS に SMP/E 一時データ セットの管理を許可するかどうかを指定します。

値： SMS または NONSMS

SMS が使用される場合、以下のストレージ パラメータを Apply します。

注: サイトが SMS ACS を使用している場合、ACS はストレージ パラメータ値をオーバーライドします。

MGMTCLAS

一時 SMP/E データ セットに使用する SMS 管理クラスを指定します。管理クラスはさまざまなレベルの移行、バックアップおよびリテンション サービスを定義します。

STORCLAS

一時 SMP/E データ セットに使用する SMS ストレージ クラスを指定します。ストレージ クラスはさまざまなレベルのパフォーマンスと可用性サービスを定義します。

DATACLAS

一時 SMP/E データ セットに使用する SMS データ クラスを指定します。データ クラスはさまざまな割り振りのデフォルト設定を定義します。

NONSMS が使用される場合、以下のパラメータを Apply します。

UNIT および VOLUME

一時 SMP/E データ セットを配置する DASD のタイプおよびボリューム シリアル番号を指定します。

例： 3390 および DASD01

JVM

JVMdsn

JVM ロード モジュールが存在するデータ セット名を指定します。

例： SYS1.SIEALNKE

詳細:

ソフトウェア要件 (P. 45)

CA Common Services for z/OS

CCSdsn

CA Common Services for z/OS ターゲット ロード ライブラリの完全修飾名を指定します。 ライブラリは APF 許可される必要があります。

CCScaipdsedsn

CA Common Services for z/OS CAIPDSE データ セットの完全修飾名を指定します。

CCISSLPortNo

システムで設定された CA Common Services for z/OS CCITCP または CCISSL ポート番号を指定します。

以下のメッセージからこの値を検索できます。

```
CAS9850I CAICCI TCP/IP server ready. PORT port-number ADDR host_address
```

デフォルト： 1202

ENF SystemID

お使いのシステムの CA Common Services for z/OS CAICCI SYSID の値を指定します。

以下のコンソール メッセージから、この値を取得できます。

```
CAS9214I - CA-ENF Command: SYSID(caicci_sysid)
```

以下のオペレータ コマンドを発行し、値を取得します。

```
ENF DISPLAY,SYSID
```

インストール ジョブの処理

ActiveJES

z/OS システム上で使用される、ジョブ入力サブシステム（JES）のタイプを指定します。

デフォルト： JES2

値： JES2 または JES3

JOBNAME

JOB ステートメントで、インストールの一部としてサブミットされるすべてのジョブに対して使用されるジョブ名を指定します。

デフォルト： # で連結された、CA CSM セットアップ ユーティリティを実行するユーザの ID。

MSGCLASS

ジョブ ログ用の JES 出力クラスを指定します。 このクラスは、ログの処理方法（たとえば、後で確認するために保持する）を決定します。

デフォルト： X

CLASS

ジョブに使用する JES イニシエータ クラスを指定します。

デフォルト： A

ACCOUNT

JOB ステートメントで、すべてのジョブに対して使用する、ジョブ アカウンティング文字列を指定します。

例： ’1234,dept01,NY NY’

SYSAFF

ジョブを処理する対象のシステムを指定します。 キーワードには、JOBPARM SYSAFF パラメータの値を指定します。

特定のシステムの ID を指定できるため、ジョブがそのシステム上で処理されるようになります。 この機能を使用しない場合は、値を指定しないでください。

CA CSM インストーラの実行制御パラメータ

AddAPFauthDSdyn

CA CSM インストーラにより、APF 許可が必要な CA Datacom/MSM ジョブのデータ セットを、APF リストに動的に追加するかどうかを指定します。

Y

CA CSM インストーラによる CA Datacom/MSM データ セットの APF リストへの動的追加が可能になります。

N

CA Datacom/MSM データ セットを手動で追加します。

デフォルト： Y

InstallSVC

CA Datacom/MSM SVC をインストールする必要があるかどうかを指定します。

Y

CA CSM インストール プロセス中に、CA Datacom/MSM SVC をインストールします。

注: CA MSM r3.1 からアップグレードしている場合、別の SVC を使用する必要があります。 このパラメータを **Y** に設定します。

N

CA CSM インストール プロセス中に、CA Datacom/MSM SVC ロード プロセスをスキップします。

注: CA CSM の再インストール、あるいは CA MSM V4.0 またはそれ以降のバージョンからのアップグレードを行っており、サイトに利用可能な SVC がインストールされている場合、このパラメータを **N** に設定します。

デフォルト： Y

サイトのデフォルト

HOSTNAME

システムのホスト名または IP アドレスを指定します。 Prerequisite Validator ユーティリティはこのキーワードを使用して FTP 接続をテストし、JESINTERFACELEVEL 値を検証します。

MFASM

SMP/E が使用する、z/OS アセンブラ プログラムの名前を指定します。

デフォルト： ASMA90

MFZAP

モジュール、ロード モジュール、またはモジュール内の CSECT の変更をインストールするために使用される、システム ユーティリティ プログラムの名前を指定します。

デフォルト： IMASPZAP

MFLKED

使用するリンク エディット プログラムまたはプロシージャの名前を指定します。

デフォルト： IEWL

TCPdsn

TCPIP.DATA データ セットの名前を指定します。

例： TCPIP.TCPIP.DATA

注: この値は空白のままでもかまいません。Apache Tomcat のスタートアップ ジョブ（MSMTCSRV）中にエラーが発生する場合、MSMTCSRV の中の SYSTCPD DD カードのコメントを、診断用に外すことができます。

TCPIPLinkDSName

TCPIP Services SEZATCP データ セットの名前を指定します。 このデータ セットは z/OS Communications Server の一部です。 このデータ セットは通常はプログラムが制御し、z/OS リンクリスト（LNKLST）にあります。

デフォルト： TCPIP.SEZATCP

LangEnvLinkEditorDSN

Language Environment リンケージ エディタ データ セットの名前を指定します。

デフォルト： CEE.SCEELKED

C370linkEditDSN

C/370 リンケージ エディタ データ セットのデータ セット名を指定します。

デフォルト： CEE.SCEESPC

LangEnvSPCdsn

C/C++ Language ライブラリ関数データ セットの名前を指定します。

デフォルト： CEE.SCEESPC

CSSLibDSN

IBM Linkage Assist Library データ セットの名前を指定します。

デフォルト： SYS1.CSSLIB

SSLLIBRARY

System SSL ライブラリのデータ セット名を指定します。

デフォルト： SYS1.SIEALNKE

SysUtilitiesPath

mount や unmount などの、z/OS UNIX ユーティリティのパスを指定します。

デフォルト： /usr/sbin

CA CSM インストーラのデフォルト

job.submission.mode

CA CSM インストール スクリプト（installer/MSMSetup.sh）が、ジョブのサブミット、ステータスの確認、インストールの一部としてのリターン コードの検証に使用する方法を指定します。有効な値は、以下のとおりです。

FTP

インストール ジョブは、FTP を使用してサブミットされます。 前提条件は JESINTERFACELEVEL 2 です。

TSO

インストール ジョブは、TSO を使用してサブミットされます。 CA CSM インストーラは、Manual インストール モードでのみ実行されます。

デフォルト： FTP

注: ローカルの FTP が Secure FTP または FTP Secure の場合、CA CSM インストーラはこの機能をサポートしません。 job.submission.mode に TSO を指定し、CA CSM インストーラを実行します。

JobStatusCheckPollPeriod

CA CSM のインストールおよびセットアップ プロセス時にサブミットされたジョブのステータスをポーリングする間隔を秒単位で指定します。

デフォルト： 2

JobCompletionWaitMaxTime

ジョブの完了を待機する時間を秒単位で指定します。この時間が経過すると、続行するかどうかをユーザに確認するメッセージが表示されます。このフィールドにより、システムがビジーな場合に処理をキャンセルできるようになります。

デフォルト: 30

HTTP または HTTPS の設定

msm.ssl.secure.connection.enable

HTTP または HTTPS を使用するように、CA CSM を設定することができます。

Y

HTTPS を使用します。

N

HTTP を使用します。

デフォルト： N

msm.ssl.secure.connection.enable を Y に設定した場合、以下のパラメータのセットを指定し、CA CSM を設定して HTTPS を使用します。

注: これらのパラメータはすべてオプションです。インストーラは、インストール時にキーストア パスワードの入力を促すプロンプトを表示します。

first.name.and.last.name

URL ドメイン名を指定します。

例： www.your.domain

organization.name

組織名を指定します。

organization.unit.name

組織単位名を指定します。

city

市町村名を指定します。

state

都道府県名を指定します。

country.code

国名を指定します。

keystore.location

キーストアの場所を指定します。デフォルトの場所とは異なる USS の場所を使用する必要がある場合は、独自の値を指定します。

デフォルト： RunTimeUSSPath に作成されます

validity.period

生成されたキーストア証明書の有効期間を日数で指定します。

デフォルト： 365

移行

注: このキーワードは、ユーザが既存の CA CSM ユーザで、CA CSM の旧バージョンからアップグレードしている場合のみ適用されます。

PreviousRelease.MSMPATH

旧バージョンの CA CSM がインストールされている USS ディレクトリのパスを指定します。 このパスには、たとえば CEGPHFS、CEGPJAR などのフォルダがあります。

旧バージョンの CA CSM の MSMSetup フォルダにある、MSMSummaryReport.txt または利用可能なオプション ファイルを参照します。

例： PreviousRelease.MSMPATH=/u/users/msmserv/msm

CA CSM ソフトウェア展開生成手順エンティティ

以下のエンティティは、CA CSM ソフトウェア展開手順の中でインストールされます。これは CA Common Services for z/OS、CAIENF および CAICCI のコンポーネントに依存する機能です。

SMPCPATH

SMP/E Java アプリケーション クラスへのパスを指定します。

プリセット： /usr/lpp/smp/classes/

SMPJHOME

Java ホーム ディレクトリを指定します。

例： /sys/java31bt/v6r0mo/usr/lpp/java/J6.0/

注: 異なる Java ホーム ディレクトリがインストールされている場合は、そのディレクトリ名を使用します。

SMPDRIWK

このエンティティは 775 の許可で定義される必要があります。

プリセット： /cai/msm/ccispnsv/smpe

注: 手順では /cai/msm/ccispnsv/smpe に設定されていますが、これをユーザの社内標準に合わせる必要があります。

USS ファイル システム

このセクションでは、z/OS UNIX System Services（USS）およびファイル システムのセットアップに関する追加の情報を説明します。

USS パスの設定詳細

CA CSM では、ダウンロード、インストールとセットアップ、および一般的な用途で HFS ファイル システムまたは zFS ファイル システムを使用できます。

注: zFS ファイル システムの使用をお勧めします。 HFS ファイル システムから zFS ファイル システムに移行する方法の詳細については、最新の「*IBM z/OS Migration*」を参照してください。

CA CSM をダウンロードしインストールする前に、USS の管理者はこれらのファイル用のディレクトリ パス、またオプションでファイル システムを設定する必要があります。サイトのポリシーに応じて、単一のファイル システムまたは複数のファイル システムでパスをセットアップできます。

注: 複数のファイル システム構造を使用して USS ファイル システムをセットアップすることをお勧めします。

最小で、775 の許可を持つ 4 つのディレクトリが必要です。

稼働中、CA CSM は追加のファイル システムを動的に作成し、マウントします。 ファイル システムは起動中にマウントされ (P. 266)、製品およびメンテナンスとしてダウンロードされます。

zFS ファイル システムを動的に拡張するには、ファイル システムをマウントするときに AGGRGROW を指定します。 以下に例を示します。

```
MOUNT FILESYSTEM('yourHLQ.MSM.ZFS') -
     MOUNTPOINT('/parent_path/msmserv/version_number/msm')          -
     TYPE(ZFS)                                  -
     MODE(RDWR)                                 -
     PARM('AGGRGROW')
```

詳細については、IBM の「*Distributed File Service zFS Administration*」を参照してください。

CA CSM は以下の z/OS UNIX System Services（USS）ディレクトリ パス構造を使用します。

/parent_path/msmserv/mpm
/parent_path/msmserv/*version_number*/msm
/parent_path/msmserv/*version_number*/msmruntime
/parent_path/msmserv/*version_number*/msminstall

注: /mpm ディレクトリにはバージョン番号を含めないでください。 このディレクトリは複数の CA CSM バージョン間で共有される共通のディレクトリです。

/*parent_path*/msmserv/

ユーザのサイトでプライマリ マウント ポイント、またはディレクトリとしてサイトで定義される CA CSM 親パス名を以下のように指定します。

```
/u/users/msmserv
/usr/lpp/msmserv
/cai/msmserv
```

注: 親パスの最後の部分に /msmserv を使用することをお勧めしますが、ユーザ サイトの基準に応じて変更することもできます。

/*parent_path*/msmserv/mpm

CA CSM が割り当て、マウントするファイル システムのマウント ポイントを指定します。 このマウント ポイントは、ソフトウェア カタログのルート アプリケーション ファイル システムをマウントするのに CA CSM が使用するディレクトリです。 オプション ファイルの MountPath キーワードにこのパスを指定します。

注: ユーザが既存の CA CSM 顧客でアップグレードを行っている場合、このパスを作成する必要はありません。 アップグレード プロセスは、デフォルトで旧バージョンのパスを再利用します。

/*parent_path*/msmserv/*version_number*/msm

CA CSM 製品用のターゲット USS ファイルのディレクトリを指定します。ディレクトリのコンテンツは SMP/E によって管理されます。

スペース： 750,100 シリンダ

/*parent_path*/msmserv/*version_number*/msmruntime

CA CSM のランタイム ファイルを指定します。つまり、実行中の CA CSM アプリケーションは、このディレクトリから実行されます。オプション ファイルの RunTimeUSSPath キーワードにこのパスを指定します。

スペース： 750,100 シリンダ

/parent_path/msmserv/*version_number*/msminstall

ダウンロードされ解凍されたすべての CA CSM ファイルなど、CA CSM のインストール データ用のディレクトリを指定します。

スペース： 1000,100 シリンダ

注: インストールの完了後、このディレクトリは削除できます。

注: 複数バージョン CA CSM の USS パスをセットアップする方法の詳細については、「*Best Practices Guide*」を参照してください。

詳細:

オプション ファイル キーワード (P. 240)

単一ファイル システム

複数のファイル システム構造を使用して USS ファイル システムをセットアップすることをお勧めします。 ただし、USS ファイル システムを単一のファイル システムとして構成する必要がある場合は、必ずそのファイル システムに製品のインストールおよび稼働中の操作に必要なスペースがすべて含まれるようにしてください。

- サイトで定義される、以下のいずれかのような CA CSM 親パス名を使用します。

  ```
  /u/users/msmserv
  /usr/lpp/msmserv
  /cai/msmserv
  ```

  注: 親パスの最後の部分に /msmserv を使用することをお勧めしますが、ユーザ サイトの基準に応じて変更することもできます。

- 以下の必須ディレクトリを定義し、以下のような構造にします。

  /parent_path/msmserv/mpm
  /parent_path/msmserv/*version_number*/msm
  /parent_path/msmserv/*version_number*/msmruntime
  /parent_path/msmserv/*version_number*/msminstall

- 単一のファイル システムおよびマウント ポイントで UNIX BPXPRMxx 制御メンバを更新します。
- インストールが完了した後、ディレクトリ */parent_path*/msmserv/*version_number*/msminstall およびそのコンテンツを削除します。

CA CSM のインストールとセットアップ

MSMSetup.sh ユーティリティを実行する前に、CA CSM インストール用のマウント ポイントを定義する必要があります。 マウント ポイントには以下のディレクトリが含まれます。

- MSMSetupOptionsFile.properties の MSMPATH キーワードにより参照されるインストール ディレクトリ（たとえば、/u/users/msmserv/msminstall）
- MSMSetupOptionsFile.properties の RunTimeUSSPath キーワードにより参照されるランタイム ディレクトリ（たとえば、/u/users/msmserv/msmruntime）

CA CSM のダウンロード

CA CSM は pax ファイルとして提供されます。pax ファイルは、マウントされたファイル システムまたはディレクトリ（たとえば、/u/users/msmserv/msminstall）にダウンロードされ、インストールされます。ファイルの名前は、51000068X01.pax.Z です。ファイルを展開すると、新規ディレクトリが作成されます。

CA CSM の起動

このセクションでは、新規および既存の CA CSM インストールの CA CSM 起動プロセスについて説明します。

起動時に、CA CSM はファイル システムおよび USS ディレクトリを割り当ててマウントします。MSMSetup.sh を実行する前に、APLROOT ファイル システム用のマウント ポイント（たとえば、/u/users/msmserv/mpm）を定義します。 CA CSM はファイル システムを割り当て、そのファイル システムをこのマウント ポイントにマウントします。

注: MSMSetupOptionsFile.properties の MountPath キーワードは、APLROOT ディレクトリを指定します。 MSMSetup.sh は、SAMPLIB（DBINIT）メンバの mpmPath パラメータに、この値を読み込みます。 CA CSM を初めて開始するときは、DBINIT メンバが使用されます。 起動時に、この値はデータベースに格納されます。 Web ベース インターフェースで［Settings］タブの［Mount Point Management］ページの［Application Root］フィールドを使用して、値を変更できます。

APLROOT ファイル システムの下では、CA CSM は sdsroot、scroot、ljroot、tmproot の 4 つの USS ディレクトリを作成します。 USS ディレクトリ ljwk は、ljroot ディレクトリの下に作成されます。

以下のリストは、永続ファイル システムおよびそれらのマウント ポイントを示します。

- *mountpath* にマウントされた *hfs_prefix*.APLROOT（105,105 トラック）
- *mountpath*/ljroot/ljwk にマウントされた *hfs_prefix*.LJWK（2370,105 トラック）
- *mountpath*/sdsroot にマウントされた *hfs_prefix*.SDSROOT（105,105 トラック）

hfs_prefix

このプレフィクスは、MSMSetupOptionsFile.properties の MVSHFSDsnPrefix キーワードによって指定されます。 MSMSetup.sh は、SAMPLIB（DBINIT）メンバの mpmHlq パラメータに、この値を読み込みます。 起動時に、この値はデータベースに格納され、Web ベース インターフェースの［Settings］タブの［Mount Point Management］ページの［Data Set Prefix］フィールドを使用して値を変更できます。

tmproot USS ディレクトリは、CA CSM 稼働中に必要な一時ファイル システムを割り当ててマウントする (P. 267)ために使用されます。

CA CSM が起動時にファイル システムをマウントするかどうかを定義できます。 Web ベース インターフェースの［Settings］タブの［Mount Point Management］ページには、［Automount］オプションがあります。 オプションが有効な場合、CA CSM は管理するすべてのファイル システムを検索してマウントします。オプションが有効ではない場合、SYS*x*.PARMLIB の BPXPRM*xx* メンバを更新してマウント ポイントを管理します。

一時ファイル システムの使用

さらに、CA CSM は製品の取得、製品のインストール、および他のタスクの実行中に、必要に応じて一時ファイル システムを割り当てます。デフォルトでは、CA CSM は一時ファイル システムを 60 分間保持します。 ファイル システムが 60 分間のアイドル状態を続けた後、CA CSM は一時ファイル システムの割り当てを解除し、解放します。

ファイル システムの名前は、*hfs_prefix*.T*x* のような形式です。

x

7 文字以内の内部生成された数字です。

CA CSM は以下のパスに一時ファイルをマウントします。

mountpath/tmproot/MSM.*unique_number*.scratchpad

割り当てられマウントされたファイル システムを CA CSM が保持するタイム スロットを変更できます。 SAMPLIB（MSMLIB）メンバで、以下のパラメータに必要な分単位の数を設定し、CA CSM アプリケーション サーバを再起動します。

```
IJO="$IJO - DCSM_MPM.TEMPSPACE.MINIMUM.IDLE.MINUTES=60"
```

最小有効値は 60 です。ユーザが 60 未満にパラメータの値を設定した場合、CA CSM はそれを再度 60 に設定します。

このパラメータが 0 に設定される場合、CA CSM は実行中に一時スペースを割り当て、終了時にそれを解放します。

ソフトウェア カタログ

CA CSM は、ソフトウェア カタログが使用するためのファイル システムを必要に応じて割り当ててマウントします。 CA CSM は、これらのファイル システムを *mountpath*/scroot の下にマウントします。

ファイル システムの名前は、*hfs_prefix.suffixn* の形式です。

suffix

ファイル システム名の最後の部分を定義するもので、SAMPLIB（DBINIT）メンバの scDatasetPrefix パラメータによって指定されます。

n

4 文字以内の内部生成カウンタです。

詳細:

CA CSM の起動 (P. 266)

CA CSM データ セットとファイル システム

このセクションでは、CA CSM データ セットとファイル システムに関する追加の情報を説明します。

このセクションには、以下のトピックが含まれています。

CA CSM データ セット タイプ (P. 269)

CA CSM ファイル システム (P. 270)

CA CSM データ セット タイプ

CA CSM には 5 つのグループのデータ セットがあります。 グループは以下のタイプで構成されます。

アプリケーション ルート: *hlq*.APLROOT

このデータ セットはルートの USS ファイル システムとして使用され、CA CSM のディレクトリ構造を格納します。

一時領域: *hlq*.T*x*

これらのデータ セットは一時ファイル システムで、CA CSM 処理用の一時領域として使用されます。 これらのデータ セットは CA CSM 稼働中に必要に応じて割り当てられ、必要とされなくなったときに削除されます。

ログ ジャーナル: *hlq*.LJWK*x*

これらのデータ セットはタスクの出力結果を保存するために使用され、その内容は完了したタスク用の［Tasks］タブに表示されます。 CA CSM を使用してこの内容を削除するには、［Task］タブの［Delete Task］ボタンを使用します。

ソフトウェア カタログ: *hlq*.CASC*x*

これらのデータ セットはすべてのダウンロードされた製品およびメンテナンス パッケージを格納し、それらはソフトウェア カタログに表示されます。 サフィックスが CASC のデータ セットは通常、CASC のデフォルト値があります。 展開が完了または削除された後に、データ セットは削除されます。

注: 旧バージョンの CA CSM では、デフォルトのソフトウェア カタログ データ セットは、サフィックスが MSMT でした。

展開一時領域: *hlq*.SDSROOT

このデータ セットは一時ファイル システムで、CA CSM 展開処理用の一時領域として使用されます。データが必要なくなった後、CA CSM はこのファイル システムのコンテンツを削除します。 CA CSM をシャットダウンした後にコンテンツがそこに残っている場合、適切な USS ディレクトリからコンテンツを手動で削除でき、CA CSM に影響を与えることはありません。

展開: *hlq*.D*x*

これらのデータ セットは展開処理に使用され、展開データが含まれています。 CA CSM を使用してこのコンテンツを削除するには、［Deployment］タブの［Action］ドロップダウン リストから［Remove］を選択します。

重要: これらのデータ セットやコンテンツを、CA CSM の外部で、手動でデータ セットから削除しないでください。 手動でデータ セットを削除すると、タスク出力が失敗、または CA CSM が失敗します。

CA CSM ファイル システム

以下の表では、CA CSM が割り当てて使用するファイル システムを示します。 以下の用語が表で使用されています。

mpm

アプリケーション ルートへの UNIX パスを指定します。 mpm は、ファイル システムのマウント ポイント ディレクトリを指定します。 初期マウント ポイントは、CA CSM のインストール中に設定されます。

hlq

CA CSM によって割り当てられた新規ファイル システムに対して作成される、データ セット名の HLQ を指定します。

データ セット名（DSN）

このディレクトリにマウントされるファイル システムの DSN、またはこのディレクトリにマウントされているファイル システムがない場合には、このディレクトリを含むファイル システムの DSN を指定します。

標準サイズ

ファイル システムの標準サイズを指定します。この値は、そのパスにマウントされたファイル システムがあるパスに対してのみ指定します。

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm	*hlq*.APLROOT	Yes	アプリケーション ルート	CA CSM のメインのマウント ポイント ディレクトリ。 このディレクトリは *hlq*.APLROOT データ セットにあります。	14400 KB
mpm/ljroot	*hlq*.APLROOT	No	ログ ジャーナル ルート	ログ ジャーナル（タスク出力）用のルート ディレクトリ。	N/A
mpm/scroot	*hlq*.APLROOT	No	ソフトウェア カタログのルート	ソフトウェア カタログ（製品およびメンテナンス パッケージを格納） 用のルート ディレクトリ。	N/A
mpm/sdsroot	*hlq*.SDSROOT	Yes	展開のルート	展開パッケージ用のルート ディレクトリ。	158400 KB
mpm/ljroot/ljwk	*hlq*.LJWK	Yes	ログ ジャーナル	このディレクトリは *hlq*.LJWK データ セットにあります。	137760 KB
mpm/scroot/tmp	*hlq*.APLROOT	No	ソフトウェア カタログ	ソフトウェア カタログの一時ディレクトリが含まれるディレクトリ。	N/A

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm/scroot/tmp/tmp*x*	*hlq*.CASCn	Yes	ソフトウェア カタログ	ソフトウェア カタログの一時ディレクトリ。	400000 KB
mpm/scroot/DatabaseM	*hlq*.APLROOT	No	ソフトウェア カタログ	ソフトウェア カタログ データベースが含まれるディレクトリ。	N/A
mpm/scroot/DatabaseM/CA	*hlq*.APLROOT	No	ソフトウェア カタログ	すべてのベンダーのダウンロードが格納された、CA Technologies ベンダー ディレクトリ。	N/A
mpm/scroot/DatabaseM/CA/error_hold_data	*hlq*.APLROOT	No	ソフトウェア カタログ	ALL-HOLDDATA.txt ファイルが格納されるディレクトリ。 このファイルには、すべての CA Technologies 製品用の HOLDDATA が含まれます。	N/A
mpm/scroot/DatabaseM/CA/COMMONS	*hlq*.APLROOT	No	ソフトウェア カタログ	CA Common Services 用のインストールが格納されるディレクトリ。	N/A
mpm/scroot/DatabaseM/cars	*hlq*.CASCn	Yes	ソフトウェア カタログ	CA RS ファイルが格納されるディレクトリ。	4800 KB
mpm/scroot/DatabaseM/CA/MAINTENANCE	*hlq*.CASCn	Yes	ソフトウェア カタログ	すべてのメンテナンス パッケージが格納されるディレクトリ	4800 KB
mpm/scroot/DatabaseM/CA/*product_name*	*hlq*.CASCn	Yes	ソフトウェア カタログ	特定の製品用の製品ディレクトリ。	4800 KB

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm/scroot/DatabaseM/CA/*product_name*/*release*/*servicepack*/*packagename*/*date*	*hlq*.CASCn	Yes	ソフトウェア カタログ	製品ディレクトリに組み込まない、特定の製品パッケージ用のディレクトリ。	4800 KB
mpm/sdsroot/*deployment_ID*	*hlq*.Dn	Yes	Software Deployment Service（SDS）	ID *deployment_ID* で行う展開用に保存されたデータを格納するディレクトリ。このディレクトリは *hlq.deployment_ID* データセットにあります。	21024 KB
mpm/tmproot	*hlq*.APLROOT	Yes	一時領域	このディレクトリには、一時ファイル システム用の一時マウント ポイントが含まれます。	N/A
mpm/tmproot/MSM.*n*.scraptchpad	*hlq*.T*n*	Yes	一時領域	このディレクトリは一時ファイル システムのマウント ポイントとして機能し、CA CSM が製品の取得、製品のインストール、その他のタスクの実行中に、必要に応じて割り当てます。	57408 KB

CA Common Services コンポーネント要件

CA Common Services はオープンかつクロス プラットフォームのエンタープライズ マネジメント インフラストラクチャで、z/OS をはじめとする多くのオペレーティング システムで使用できます。 このインフラストラクチャは、CA Technologies の IT 管理ソリューション向けの共通サービスおよびイネーブリング テクノロジを提供します。

CA Common Services for z/OS

CA Common Services for z/OS には、CA Technologies の実装に共通の分散サービスと、z/OS に固有のソリューションが用意されています。 CA Common Services for z/OS は、複数の統一されたリソース ビューを作成するための共通のインターフェースとイベント サービスを提供します。

z/OS をホストとするこのエンタープライズ マネジメント アーキテクチャにより、Windows および UNIX プラットフォームで動作する CA Common Services for z/OS と同じように、管理する対象と範囲の選択肢が広がります。また CA Common Services for z/OS には、z/OS の統合管理の実現に欠かせないコンポーネントや機能も用意されています。

CA Common Services for z/OS は、z/OS UNIX System Services を基盤とするアプリケーションをサポートしています。CA Common Services for z/OS には、z/OS エージェントを実行するための Agent Technology インフラストラクチャも組み込まれています。

CA Common Services for z/OS により、以下のことが可能になります。

- メインフレームを他の分散プラットフォームと統合できます。
- Web サーバ、Java アプリケーション、UNIX アプリケーションなど、新たな z/OS ワークロードを管理できます。
- 既存の CA Technologies z/OS 管理ソリューションを使用してイベントを作成し、そのイベントを使って必要な結果が得られるエンタープライズ プラットフォームにイベントを送信することができます。
- 先進的なマネージャおよびエージェント テクノロジと CA Technologies 製品を併用することで、クリティカル リソースのモニタおよび管理を、企業全体で自動化し、高度なレベルで実現できます。

注: CA Common Services for z/OS の詳細については、CA Common Services for z/OS のユーザ マニュアルを参照してください。

ソフトウェア サービス

CA Common Services for z/OS ソフトウェア サービスは CA CSM に、さまざまな機能を実行するいくつかのソフトウェア コンポーネントを提供します。

CAICCI

CAICCI は、一般的な通信ソフトウェア層を、CA エンタープライズ アプリケーションに提供するソフトウェア コンポーネントです。 このソフトウェア層によって、プロトコルの指定、エラー リカバリ、およびシステム接続の確立がアプリケーションで行われないようにします。

CAIENF (Base)

CAIENF (Base) はソフトウェア コンポーネントで、製品ライン全体を対象としたテクノロジを利用し、CA Technologies のあらゆる z/OS アプリケーションに対して包括的なオペレーティング システム インターフェース サービスを提供します。 オペレーティング システムと CA Technologies ソフトウェアで生成されたイベント情報を標準インターフェースから制御できるようにすることで統合レベルが向上し、それにより複数の製品間インターフェースが単純化され、関連するメンテナンスが容易になります。

CAIRIM

CAIRIM は、すべての CA アプリケーションに対するオペレーティング システム環境を作成し、それらのアプリケーションを開始するソフトウェア コンポーネントです。 CAIRIM は、一連の動的初期化ルーチン用の共通ドライバです。ユーザ SVC、SMF EXIT、サブシステムなど、システム アプリケーションのインストール時に要求される一般的なインストール要件を不要にします。

CAIRIM の重要な 2 つの要素は、CAISSF と CA LMP です。

CAISSF

すべてのシステム リソース プロセスとアプリケーション リソース プロセスへの制御と監視アクセスのための外部セキュリティ機構が実現されます。 CAISSF は多くの CA エンタープライズ アプリケーションに統合されており、他の CA Common Services for z/OS サービスでも使用されます。 ユーザ サインイン、リソース アクセス制御、プロセス使用制御、違反行為の記録およびモニタのためのセキュリティ サービスを提供します。

CA LMP

CA LMP は、ライセンス ソフトウェアを監視する標準化された自動化アプローチを提供します。

CA-C Runtime

CA-C Runtime はサポート サービスのコンポーネントで、システムおよびリリースを問わずプログラムの実行を可能にする、C のランタイム機能を提供します。

FMID

CA CSM には、さまざまな機能を実行する CA Common Services for z/OS r12 またはバージョン 14.0 およびそれ以降のコンポーネントが必要です。 機能変更 ID（FMID）が、これらのコンポーネントに対して用意されています。

以下の表内の FMID は CA Common Services for z/OS r12 を基にしています。

FMID	コンポーネント
CAF3C00	CA-C Runtime
CAS9C00	CAIRIM
CAW1C00	CAIENF
CAW4C00	CAICCI （SSL を使用）

以下の表の FMID は、CA Common Services for z/OS バージョン 14.0 およびそれ以降のバージョンを基にしています。

FMID	コンポーネント
CAF3E00	CA-C Runtime
CAS9E00	CAIRIM
CAW1E00	CAIENF
CAW4E00	CAICCI （SSL を使用）

以下の表の FMID は CA Common Services for z/OS r12 およびバージョン 14.0 およびそれ以降のバージョンを基にしています。 これは CA Common Services for z/OS に依存する機能で、SDS と SCS に対してのみ使用されます。

FMID	コンポーネント
CETN500	CAICCI を使用する MSM Common Services

注: 完了する必要があるセットアップおよび設定の手順の詳細については、「*CA Common Services for z/OS インストール ガイド*」を参照してください。

CAICCI のセットアップ

注: CAICCI をまったくセットアップしていない場合は、この手順を使用します。 詳細については、「*CA Common Services for z/OS インストール ガイド*」を参照してください。

以下の手順に従います。

1. 以下の形式を使用し、CAIENF パラメータ ファイル内、または ENFPARMS に連結された個別の CCIPARM PDS メンバのどちらかで、CAICCI SYSID を定義します。

   `SYSID(sysid)`

   sysid

   CAICCI 識別子を指定します。

   制限： 8 文字

2. CAICCI データ収集モジュール（DCM） CAS9DCM3 を CAIENF パラメータ ファイルに定義します。 以下に例を示します。

   ```
   DCM(CAS9DCM3)         * ENF V1.0 CCI Event
   ```

CA CSM 機能のセキュリティ

CA CSM によって提供されるリソースとアクティビティの多くは、お使いの外部セキュリティ マネージャ（ESM）に定義されたセキュリティ プロファイルによって保護されます。 Web ベース インターフェースのアクションを実行しようとすると（たとえば、ログインまたは設定の変更）、CA CSM は関連するリソース プロファイルを使用して System Authorization Facility（SAF）を呼び出します。CA CSM リソース プロファイル (P. 279)は、CA CSM リソース クラスで定義されています。リソース プロファイルにより、サイトはさまざまなリソースやアクションへの権限を特定のユーザに付与し、少しの設定で汎用アクセス権を設定できるようになります。

リソース名

CA CSM は、リソースへのアクセス用の READ、UPDATE、CONTROL、ALTER を区別しません。 その代わりに、アクセス権はリソース名にエンコードされます。 リソースに対するアクセス権がある場合、リソース上の指定されたアクションを実行できます。

付与される権限レベルは重要ではありません。 リソースへのアクセスはバイナリ方式で管理されます。これはリソースにアクセスできる場合（READ、UPDATE、CONTROL、ALTER の任意の組み合わせ）、またはリソースにアクセスできない場合のどちらでも同じです。 たとえば、以下のリソース プロファイルは、［Settings］タブのシステム設定へのアクセスを制御します。

ADMIN.SETTINGS.SYSTEM

ユーザにシステム設定の表示と更新を許可します。

ADMIN.SETTINGS.SYSTEM.@DISPLAY

ユーザにシステム設定の表示を許可します。

ADMIN.SETTINGS.SYSTEM.@UPDATE

ユーザにシステム設定の更新を許可します。

@DISPLAY および @UPDATE プロファイルの両方があるリソースについては、@UPDATE プロファイルに対してのみのアクセス権の付与はエラーになります。 値を表示する権限がないため、たとえそのレベルのアクセス権が付与されているとしても、値を変更することはできません。

すべてのシステム設定は ADMIN.SETTINGS.SYSTEM の下に構成されるため、1 人以上のユーザに ADMIN.SETTINGS.SYSTEM プロファイルに対する権限を付与することで、すべてのシステム設定へのアクセス権を与えることができます。 これらのユーザは、CA CSM の管理の役割を担います。

ユーザ設定は ADMIN.SETTINGS.USER の下に構成されます。この設定は、CA CSM 内でユーザごとに別々に管理され、リソースの表示または更新のアクセス権は、リソース プロファイル内の @SELF 修飾子を使って管理されます。 たとえば、USER01 および USER02 ユーザ ID に ADMIN.SETTINGS.USER.@SELF.@DISPLAY および ADMIN.SETTINGS.USER.@SELF.@UPDATE プロファイルへの権限を付与することにより、ユーザは自分の Web ベース インターフェースの設定を更新できるようになります。 ただし、USER01 は、USER02 用の設定の表示や更新はできません。 ADMIN.SETTINGS.USER.@SELF へのアクセス権を、すべての CA CSM ユーザに付与することをお勧めします。

リソース プロファイル

セキュリティ ルールを使用してアクセスを許可または却下することによって、CA CSM の特定の一部を保護することができます。これを *リソース プロファイル*と呼びます。 リソース クラス CAMSM を使用し、これらのリソース プロファイルを関連するセキュリティ パッケージに作成します。

重要: ユーザに *.@UPDATE リソース プロファイルへのユーザ権限を付与する場合、それに対応する *@DISPLAY リソース プロファイルにもそのユーザ権限を付与する必要があります。

LOGON

CA CSM へのアクセス権を付与します。

ADMIN.SETTINGS

［Settings］タブ上のすべての設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.SYSTEM

すべてのシステム設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.SYSTEM.@DISPLAY

すべてのシステム設定への DISPLAY 権限を付与します。

ADMIN.SETTINGS.SYSTEM.@UPDATE

すべてのシステム設定への UPDATE 権限を付与します。

ADMIN.SETTINGS.USER.@SELF

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.USER.@SELF.@DISPLAY

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定への DISPLAY 権限を付与します。

ADMIN.SETTINGS.USER.@SELF.@UPDATE

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定への UPDATE 権限を付与します。

ADMIN.LMPKEY

［LMP Keys Browser］ページ上のリソースへのフル アクセス権を付与します。

ADMIN.LMPKEY.UPDTKEYS

［LMP Keys Browser］ページ上の［Update Keys］へのアクセス権を付与します。

ADMIN.LMPKEY.REFRSITE

［LMP Keys Browser］ページ上の［Refresh Site IDs］へのアクセス権を付与します。

CONFIG

［Configurations］タブ上のリソースへのフル アクセス権を付与します。

CONFIG.@DISPLAY

SCS に関係するリソースに表示専用アクセス権を付与します。

CONFIG.@ACTION.CREATE

SCS に関係するリソースの作成、または更新のためのフル アクセス権を付与します。

CONFIG.@ACTION.REMOVE

［Deployments］タブ上のリソースへのフル アクセス権を付与します。

CONFIG.@ACTION.IMPL

リモート システムの設定を実装するためのアクセス権を付与します。

DEPLOY

［Deployment］タブ上のリソースへのフル アクセス権を付与します。

DEPLOY.@DISPLAY

［Deployments］タブ上で提供される情報への読み取り専用権限を付与します。

DEPLOY.@SELF

展開の作成、システムとカスタム データ セットの割り当てを行う権限を付与します。同様に、CA CSM ユーザ ID が展開の所有者としてマークされている場合、展開のすべてのアクションの割り当てを行う権限を付与します。

DEPLOY.@BUILD

展開の作成、システムおよびカスタム データ セットの割り当てを行う権限を付与します。同様に、展開をプレビューする権限も付与します。

DEPLOY.@EXECUTE

スナップショットの実行、転送、展開、展開の確認を行う権限を付与します。

METHOD

すべての方法へのフル アクセス権を付与します。

METHOD.@DISPLAY

すべての方法への読み取りアクセス権を付与します。

METHOD.@SELF

ユーザが所有者として登録された方法のみに、フル アクセス権を付与します。

METHOD.@UPDATE

［Maintain Methodologies］ページ内から、方法を作成、編集、削除するためのアクセス権を付与します。 これは展開ビュー内の、方法の隣にある［Edit］ボタンを有効にするかどうかも制御します。

SC

［Products］タブ上のリソースへのフル アクセス権を付与します。

SC.@ACTION

［Products］タブ上のアクションへのフル アクセス権を付与します。

SC.@ACTION.UPDTCAT

［Products］タブ上のすべての［Update Catalog］アクションへのアクセス権を付与します。

SC.@ACTION.SHOWLMP

［Products］タブ上の［Actions］セクション内の［Show License Keys］アクションへのアクセス権を付与します。

SC.@ACTION.INSRTPRD

［Products］タブ上の［Actions］セクション内の［Add Product］アクションへのアクセス権を付与します。

SC.@ACTION.INSTPKG

［Products］タブ上の［Actions］セクション内の［Install External Package］アクションへのアクセス権を付与します。

SC.@HIDE

［Products］ツリーの［Hide Product］アクション、および［Products］タブ上の［Show Hidden Products］ダイアログ ボックスの［Show Products］ボタンへのアクセス権を付与します。

SIS.BASE.@SELF.WORKDD.@UPDATE

製品インストール中の作業 DDDEF の設定を更新するためのアクションにアクセス権を付与します。

SMPE.@ACTION

［SMP/E Environments］タブ上のアクションへのフル アクセス権を付与します。

SMPE.@ACTION.MIGRATE

SMP/E 環境を移行するためのアクションへのフル アクセス権を付与します。

SMPE.@ACTION.REMOVECSI.*csidatasetname*

［SMP/E Environments］ - ［SMP/E Environment Information］タブ上の［Remove SMP/E Environment from CA CSM］へのアクセス権を付与します。 このアクセス権は指定された SMP/E 環境用です。

.csidatasetname

ユーザが削除できる SMP/E 環境のデータ セット名を指定します。

この値には、1 つの SMP/E 環境に一致するフル ネーム、または複数の SMP/E 環境データ セット名に一致するプレフィクスを指定できます。

SYSREG

［System Registry］タブ上のリソースへのフル アクセス権を付与します。

SYSREG.@DISPLAY

すべての System Registry 値に表示権限を付与します。

注: このアクセス権で定義されたユーザは、すべてのパネル上のいかなる情報も作成、削除、更新できません。

SYSREG.@ACTION

［System Registry］タブ上のアクションへのフル アクセス権を付与します。

SYSREG.@ACTION.CREATE

［Create Non-Sysplex System］リンク、［Create Sysplex］リンク、［Create Shared DASD Cluster］リンク、［Create Staging System］リンクへのアクセス権を付与します。 また、［System Registry］ツリーの各プライマリ ノードの画面内の［Create］ボタンが有効になります。同様に、［Data Destinations］内の［Create］ボタンも有効になります。 Create 権限には、Update 権限も含まれます。

SYSREG.@ACTION.REMOVE

［System Registry］ツリーの各プライマリ ノードの内の［Actions］ボタンからの［Select check box］および［Remove item］へのアクセス権を付与します。

注: ユーザにこの権限がない場合、これらのアイテムは無効になっています。

SYSREG.@PROFILE

システム レジストリの各プライマリ ノード内のプロファイル情報へのフル アクセス権を付与します。プロファイル情報は、設定の作成または実装を行う組織内の CA CSM ユーザに適用することができます。このアクセス権が付与されていない場合、システムのプロファイル情報は Web ベース ユーザ インターフェース内に表示されません。

注: 実装が正しく行われなかった場合、この変更によりリモート システムの安定稼働に悪影響を与えるおそれがあります。 このプロファイルに対する権限を制限することをお勧めします。

SYSREG.@PROFILE.DISPLAY

システム レジストリの各システム ノードの内から、このアクセス権を持ったユーザはプロファイル内のいかなる値も修正する権限がありません。 これらのアイテムは表示されますが、すべての［Action］ボタンは無効になります。

SYSREG.@PROFILE.UPDATE

システム レジストリの各システム ノードの内から、プロファイルのオカレンスの作成、またはプロファイル内の任意の既存の値の更新を行うアクセス権を付与します。 システム レジストリがリソース ルール SYSREG@PROFILE.DISPLAY で保護されている場合、このアクセス ルールには任意のプロファイル情報の更新を可能にすることが必要です。

SYSREG.@SYSTEM

［System Registry］タブ内に定義されたすべてのシステムへのフル アクセス権を付与します。

SYSREG.@SYSTEM.*systemname*

［System Registry］タブ内の「システム名」へのアクセス権を付与します。 システムが CA CSM セッション内で作成され、特定のシステム レベル セキュリティが必要な場合、セキュリティ管理者は新しく定義されたシステムへのアクセス権を、それが CA CSM ユーザに見えるようになる前に付与する必要があります。 このレベルのセキュリティは、ユーザが利用可能な定義済みシステムの制御のみを行います。 定義済みシステムの情報を更新または削除する機能は、SYSREG.@ACTION.CREATE、SYSREG.@ACTION.REMOVE、SYSREG.@PROFILE.UPDATE リソースを使用して許可されます。

TM.TASK.ARCHIVE

［Task］タブ内の［Manage History］機能へのアクセス権を付与し、権限のあるユーザによるタスク アーカイブ ポリシーの作成、実行、削除を可能にします。

TM.TASK.@SELF.DELETE

ユーザ自身のタスクを削除するためのアクセス権を付与します。

TM.TASK.SYSTEM.DELETE

任意のタスクを削除するためのアクセス権を付与します。

SMP/E 処理中の SAF チェック

SMP/E コマンドを実行するすべての CA CSM 機能は、CA CSM にログインし、これらの機能を操作するユーザのセキュリティ コンテキスト内でこのチェックを行います。 CA CSM の機能により異なりますが、さまざまな SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

注: CA CSM は、CA CSM アプリケーション サーバ ID のセキュリティ コンテキストで GIMUNZIP を実行します。SMP/E セキュリティがアクティブな場合、CA CSM アプリケーション サーバ ID には SAF FACILITY クラスの GIM.PGM.GIMUNZIP リソースへの READ アクセス権が必要です。

SMP/E 環境の移行

カスタマ提供の JCL を使用して新しい DDDEF を移行済みの SMP/E 環境に追加する場合、ユーザには以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.CMD.SET
- GIM.CMD.UCLIN

基本製品のインストール

製品をインストールするには、以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.PGM.GIMUNZIP
- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RECEIVE
- GIM.CMD.APPLY
- GIM.CMD.ACCEPT

既存の SMP/E 環境に製品をインストールするときにエラーが発生する場合、CA CSM はインストールを開始する前に UNDO 操作を実行し、SMP/E 環境をその状態にリストアします。

CA CSM により実行された UNDO 操作のレベルにより異なりますが、以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RESTORE
- GIM.CMD.REJECT

メンテナンス管理

メンテナンスを管理するため、GIM.CMD.SET SAF 機能クラス リソースへの READ アクセス権が必要です。

その他の要件は、以下の特定のメンテナンス操作により異なります。

- メンテナンスをインストールするには、少なくとも以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。
  - GIM.CMD.RECEIVE
  - GIM.CMD.APPLY
- また、メンテナンスを ACCEPT するには、ユーザには GIM.CMD.ACCEPT SAF 機能クラス リソースへの READ アクセスが必要です。
- 1 つ以上のメンテナンス パッケージで基本の SMP/E コマンドを実行するには、ユーザには以下の対応する SAF 機能クラス リソースへの READ アクセス権が必要です。
  - GIM.CMD.RECEIVE（RECEIVE 操作用）
  - GIM.CMD.APPLY（APPLY 操作用）
  - GIM.CMD.ACCEPT（ACCEPT 操作用）
  - GIM.CMD.RESTORE（RESTORE 操作用）
  - GIM.CMD.REJECT（REJECT 操作用）

展開

SDS は、SMP/E GIMZIP プログラムに依存しています。展開操作を実行する場合、ユーザには CA CSM 実行中システムの GIM.PGM.GIMZIP SAF 機能クラス リソースへの READ アクセス権が必要です。 また、ユーザには CA CSM リモート システムの GIM.PGM.GIMUNZIP SAF 機能クラス リソースへの READ アクセス権が必要です。

DBINIT および DBUPDATE の設定

CA CSM を初めて起動する際に、DBINIT メンバ *RunTimeMVSHLQPrefix*.SAMPLIB（DBINIT）が使用されます。 CA CSM インストーラは、このメンバのコンテンツを設定します。

重要: CA サポート から要求された場合のみ、メンバのコンテンツを変更してください。 キーワードに設定された値の中には、CA CSM セットアップ オプション ファイルと *RunTimeMVSHLQPrefix*.SAMPLIB（DBINIT）メンバの間で異なるものもあります。 そのため、CA サポート からの指示に忠実に従うことが重要です。

DBINIT メンバは、CA CSM スタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））の DBINIT DD に割り当てられます。 これは CA CSM が初めて実行されるときのみ使用されます。

起動中、DBINIT メンバから取得した値はデータベースに格納されます。 1 回だけ設定できる値があります。 それらを変更することはできず、値を変更してもまったく効果がありません。 後で CA CSM Web ベース インターフェースを使用して、その他の値を修正できます。

Web ベース インターフェースを使用して修正できない値を変更するには、DBUPDATE DD (P. 296) を使用します。 DBUPDATE DD は、CA CSM の起動中に処理されます。

重要: CA サポート から要求された場合のみ、これらの値を更新してください。 それ以外の場合に更新すると、データの不整合が起こる可能性があります。

DBINIT と DBUPDATE のコンテンツはレコードで、# で始まるコメント、または以下の形式での値が設定されます。

```
setting=value
```

値は DBINIT または DBUPDATE 処理中には検証されません。

以下の設定がマウント ポイント マネージャで利用可能です。

mpmPath

CA CSM が作業ファイルに使用する、USS ディレクトリへのパスを定義します。セットアップ ユーティリティの実行時に、このディレクトリが利用可能である必要があります。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Application Root］フィールドを使用して変更できます。

注: この値を変更しても、既存のデータは新しいパスにコピーされません。 新しいパスが有効であることを確認します。

mpmHlq

ファイル システムの割り当てに使用されるプレフィクスを定義します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Data Set Prefix］フィールドを使用して変更できます。

制限： 40 文字

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmStorclas

［Settings］タブの［Mount Point Management］ページの SMS ストレージ クラスを定義します。

値は空白でもかまいません。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Storage Class］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmVolser

［Settings］タブの［Mount Point Management］ページで、対応する DASD のボリューム シリアル番号を定義します。

値は空白でもかまいません。 値を定義する場合、mpmVolser はオンライン ボリュームのボリューム シリアル番号である必要があります。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Storage Class］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmFilesystemType

ファイル システムの割り当てに使用されるファイル システム タイプを指定します。

以下のオプションがあります。

- HFS
- zFS

注: zFS ファイル システムの使用をお勧めします。

これらの値は Web ベース インターフェース、［Settings］タブの［System Settings］ - ［Mount Point Management］ページを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。 既存のデータ セットはそのまま残します。

mpmAutomount

CA CSM が起動中にすべてのファイル システムをマウントする必要があるかどうかを指定します。

以下のオプションがあります。

- true
- false

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Automount check］チェック ボックスを使用して変更できます。

mpmunit

［Settings］タブの［Mount Point Management］ページで、データ セットを配置する DASD のタイプを指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Unit］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmDataClas

［Settings］タブの［Mount Point Management］ページで、ファイル システム データ セットの SMS データ クラスを指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Data Class］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmMgmtClas

［Settings］タブの［Mount Point Management］ページでファイル システム データ セットに対する SMS 管理クラスを指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Storage Class］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmAllocation

［Settings］タブの［Mount Point Management］ページで、ファイル システムに新しいデータ セットを割り当てるときに SMS を使用するかどうかを指定します。

以下のオプションがあります。

- SMS
- NONSMS

mpmStorclas が定義されている場合、mpmAllocation は SMS として扱われます。 それ以外の場合、mpmAllocation は NONSMS として扱われます。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Use SMS or Use Non-SMS］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

以下の設定がソフトウェア カタログで利用可能です。

scDatasetPrefix

データ セット名のサフィックスを指定します。データ セットには内部生成カウンタもあります。

名前の形式は、以下のとおりです。

`mpmHlq.scDatasetPrefix`*n*

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ -［Software Catalog］ページの［Data Set Suffix］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

scRoot

CA サポート Online Web サイトから取得したパッケージを格納する、カスタマ サイトの Software Catalog データベースのルート ディレクトリを定義します。 ディレクトリは CA CSM のアプリケーション ルート、mpmPath と関連付けられています。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Root Directory］フィールドを使用して変更できます。

注: 新しいパスが有効なソフトウェア カタログのルートを指していることを確認してください。

scPrimBig

USS データベースの、製品またはリリース レベルで暗黙的にマウントされているデータ セットの初期量のデフォルト値を指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Primary Quantity］フィールドを使用して変更できます。

scSecBig

USS データベースの、製品またはリリース レベルで暗黙的にマウントされているデータ セットの増分量のデフォルト値を指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Secondary Quantity］フィールドを使用して変更できます。

以下の設定が CA DSI Server で利用可能です。

dsiHost

CA CSM がセキュリティ機能を提供するために内部で使用する、CA DSI Server のホスト名を指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

dsiPort

CA CSM がセキュリティ機能を提供するために内部で使用する、CA DSI Server のポート番号を指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

dsiConf

CA DSI Server 設定ファイルのパスを指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

以下の設定がソフトウェア インストール サービスで利用可能です。

sisGimunzipTempPrefix

製品のインストールとメンテナンス中に GIMUNZIP 出力一時データ セットを割り当てるために CA CSM が使用するプレフィクスを定義します。データ セットの名前は、*prefix.jobname.unpacked_file_name* のようになります。 作成された一時作業ファイルは、SMP/E で制御されたデータ セットではありません。 CA CSM は製品インストール プロセスで、それらのファイルを削除します。 これらのファイルは、製品を SMP/E 環境のグローバル ゾーンに RECEIVE する際に、SMP/E 処理の入力関連ファイルとして使用されます。

この値は Web ベース インターフェースで、［Settings］タブの［Software Installation］ページの［GIMUNZIP Temporary Prefix］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

制限： 12 ～ 19 文字（*ジョブ名*に使用される文字数により異なる）

注: デフォルトの 6 文字の *ジョブ名*を使用する場合、GIMUNZIP 一時プレフィクスには 14 文字まで入力できます。

sisExecutorServerDsnPrefix

実行されたプログラムによって使用される一時データ セット用のプレフィクスを定義します。

一時データ セットの名前は、以下の形式になります : *prefix*.R*n*.*ddname*（*n* は実行リクエスト番号です）。

この値は Web ベース インターフェースで、［Settings］タブの［Software Installation］ページの［Temporary Data Set Prefix］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

デフォルト： *userid*.CAMSM.*jobname*

制限： 24 文字

sisGimunzipTempVolser

インストール中に GIMUNZIP によって作成された一時データ セットに使用する DASD のボリューム シリアル番号を指定します。

この値は Web ベース インターフェースで、[Settings]タブの[Software Installation]ページの［GIMUNZIP Temporary VOLSER］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

制限： 1 ～ 6 文字の英数文字またはアスタリスク（*）。 アスタリスクを指定すると、自動クラス選択（ACS）ルーチンが許可する場合、SMS は新しい VSAM データ セット用のボリュームを割り当てます。

sisExecutorOutputStorclas

実行したプログラムが一時データ用に使用するデータ セットの SMS ストレージ クラスを指定します。

この値は Web ベース インターフェースで、[Settings]タブの[Software Installation]ページの［Storage Class field］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

sisExecutorOutputVolser

実行されたプログラムが一時データ用に使用するデータ セットに使用する DASD のボリューム シリアル番号を指定します。

この値は Web ベース インターフェースで、[Settings]タブの[Software Installation]ページの［VOLSER］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

制限： 1 ～ 6 文字の英数文字

sisExecutorOutputUnit

実行されたプログラムが一時データ用に使用するデータ セットを配置する DASD のタイプを指定します。

この値は Web ベース インターフェースで、[Settings]タブの[Software Installation]ページの［Unit］フィールド（［System Settings］と［User Settings］の両方）を使用して変更できます。

以下の設定が PAS コンポーネント キーに対して利用可能です。

PASAdvancedSettingsPDS

FTP プロキシの拡張設定のサンプルが格納されるメンバのデータ セットを定義します。

デフォルト： *RunTimeMVSHLQPrefix*.SAMPLIB

RunTimeMVSHLQPrefix

CA CSM ランタイム データ セットのプレフィクスを指定します。これはターゲット データ セットのランタイム コピーです。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

PASAdvancedSettingsMember

FTP プロキシの拡張設定のサンプルが格納され、FTP および HTTP どちらの拡張設定も設定できるメンバを定義します。

デフォルト： PASADVOP

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

以下の設定がタスク管理に対して利用可能です。

sysTaskDeleteOverrideEnabled

CA CSM 内のセキュリティ機能が無効なとき、すべての CA CSM ユーザが完了したタスクを削除できるようにします。

true

任意のユーザが任意の完了タスクを削除できます。

false

ユーザは完了したタスクを削除できません。

注: セキュリティ機能が CA CSM で有効な場合、タスクの削除はセキュリティ リソース (P. 279)によって管理されるため、このパラメータは無視されます。

デフォルト： なし

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

DBUPDATE DD を使用した値の修正

DBUPDATE DD を使用して CA CSM データベース内の入力値を修正するには、CA CSM のスタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に DBUPDATE DD を追加します。

以下の手順に従います。

1. *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバを作成します。
2. 修正する *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバ内の設定（P. 287）およびその値のみを追加します。
3. CA CSM のスタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバを指す DBUPDATE DD を追加します。
4. CA CSM アプリケーション サーバを再起動します。
5. *RunTimeMVSHLQPrefix*.JCL（MSMTCSRV）内の DBUPDATE DD をコメントアウトします。

ASCII 設定ファイル

tomcat/conf フォルダ内のすべてのファイルおよび tomcat/webapps/MSM フォルダ内のすべての設定ファイルは ASCII で保存されるため、標準的な方法ではこれらのファイルを編集できません。 このセクションでは、いくつかの ASCII ファイルを紹介し、それらを編集する方法について説明します。

ASCII ファイルの編集

いくつかのテキスト ファイルは、USS に ASCII で保存されます。 EBCDIC のようなファイルを開こうとすると、バイナリで表示されることがあります。

ASCII の要件は Java に起因するものです。Java は ASCII でのみ実行されます。USS (OMVS) は EBCDIC と同様に、ASCII のコードを実行できます。

注: OEDIT と ISHELL は EBCDIC 用であり、ASCII ファイルの編集には使用できません。

以下のいずれかの方法を使用して、ASCII モードのファイルを編集できます。

- USS からの ASCII ファイルを直接編集できる、サードパーティ製のユーティリティを使用します。
- 以下の手順で、ASCII ファイルをテキスト エディタでローカルで編集します。

  1. FTP を使用して、バイナリ モードでマシンにファイルをダウンロードします。そうすることで、エンコードが転送中に変更されません。
  2. そのファイルをお使いのマシン上でテキスト エディタで編集します。
  3. FTP を使用して、ファイルをバイナリで再度アップロードします。
- 以下の手順で、USS 内の ISPF UI Tool を使用して ASCII ファイルを編集します。

  1. ISPF プライマリ オプション メニューから［UTILITIES］を選択します。

     ［Utility Selection Panel］が開きます。
  2. ［Udlist］を選択します。

     ［z/OS UNIX Directory List Utility］が開きます。
  3. パス名を入力し、次に通常の USS コマンドを使用し、必要なディレクトリまでパスをたどります。
  4. ユーザをスーパーユーザにし、適切なファイル上で EA コマンドを入力します。

ファイルは読み取り可能な形式のため、更新することができます。

context.xml パラメータ

context.xml ファイル内の値を編集できます。 context.xml ファイルは ASCII ファイルのため、このファイルを編集する (P. 296)ときには、特別な操作が必要になります。

重要: ServerName の値を変更する場合、SAMPLIB(SRVLIB) メンバ内の対応する値も変更する必要があります。 SAMPLIB(SRVLIB) メンバでは、ServerName の値は SERVERNAME に対応しています。

ApplicationID の値を変更する場合、SAMPLIB(SRVLIB) メンバ、および SAMPLIB(SRVLIB) メンバ内の対応する値も変更する必要があります。 SAMPLIB(SRVLIB) メンバおよび SAMPLIB(SRVLIB) メンバの両方において、ApplicationID の値は APPLID に対応しています。

context.xml のサンプルを以下に示します。

```
url="jdbc:datacom:/ServerName=SRVMUF,SystemID=A31SENF, ApplicationID=SRVMUF,
HostPort=1202,ConnectType=CCI, HostName=AA01,UserID=SWMGRQA"
```

URL 文字列は以下のパラメータから構成されます。

ServerName

CA CSM アプリケーション サーバによって使用される CA Datacom/MSM サーバを定義します。

SystemID

CA CSM アプリケーション サーバによって使用されるシステムの CA-ENF CAICCI SYSID を定義します。

ApplicationID

CA Datacom/MSM サーバ名を定義します。

HostPort

ユーザのシステムで設定された CA CCITCP または CCISSL ポート番号を定義します（たとえば 1202）。

ConnectType

CA CSM アプリケーション サーバ (P. 329)と CA Datacom/MSM サーバ間の接続のタイプを定義します。 ConnectType は常に CCI を指定します。

HostName

お使いのシステムのホスト システムの名前または IP アドレスを定義します。

UserID

データベースにアクセスするために CA CSM によって使用される、ユーザ ID を定義します。

ジョブ割り当て詳細

このセクションでは、z/OS および USS の詳細、また CA CSM がインストールされた後に作成されるファイルおよびフォルダの詳細について説明します。

以下のジョブは、ユーザが CA CSM インストールまたはアップグレードのどちらを実行しているかに基づいてサブミットされます。 ジョブ名は、CSM*axxyy* の形式です。

a

新規インストール（N）か、アップグレード（U）かを表します。

xx

どのバージョンからアップグレードするかを示します 、または、新規インストールに対しては 51 を指定します。

yy

ジョブのシーケンス番号を表します。

このセクションには、以下のトピックが含まれています。

- CSMaxx02（P. 299）（新規インストールとアップグレード)
- CSMaxx06（P. 302）（新規インストールとアップグレード)
- CSMaxx09（P. 304）（新規インストールとアップグレード)
- CSMUxx01（P. 304）（アップグレードのみ)

CSMaxx02

以下の表は、このジョブが実行されるときに作成されるデータ セットおよび USS ファイルの一覧を示します。

注: シリンダの初期量の合計は、922/3390 DASD スペースです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<CSIHLQ>.SMPCSI.CSI	互換性なし	互換性なし	互換性なし	VSAM KSDS	互換性なし	互換性なし	互換性なし

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<CSIHLQ>.SMPCSI.CSI.DATA	CYLS	15		VSAM KSDS	互換性なし	互換性なし	互換性なし
<CSIHLQ>.SMPCSI.CSI.INDEX	CYLS	5		VSAM KSDS	互換性なし	互換性なし	互換性なし
<CSIHLQ>.SMPLOG	CYLS	6	5	PS	VB	510	6233
<CSIHLQ>.SMPLOGA	CYLS	6	5	PS	VB	510	6233
<CSIHLQ>.SMPLTS	CYLS	6	5	PO	U	0	6144
<CSIHLQ>.SMPMTS	CYLS	6	5	PO	FB	80	3120
<CSIHLQ>.SMPPTS	CYLS	102	100	PO	FB	80	27920
<CSIHLQ>.SMPSCDS	CYLS	10	5	PO	FB	80	3120
<CSIHLQ>.SMPSTS	CYLS	6	5	PO	FB	80	3120
<DatabaseHLQ>.MSM.ADCXX.BKP	CYLS	5	1	PS	VB	4088	4096
<DatabaseHLQ>.MSM.DB002.BKP	CYLS	10	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DB015.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.JNL4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PCY4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DatabaseHLQ>.MSM.SRG4000.BKP	CYLS	4	2	PS	VB	20480	27998
<DlibHLQ>.AAAXDATV	CYLS	88	1	PO	VB	31996	32000
<DlibHLQ>.AAAXHFS	CYLS	3	1	PO	VB	1028	6144
<DlibHLQ>.AAAXMAC	CYLS	15	1	PO	FB	80	32720
<DlibHLQ>.AAAXMOD0	CYLS	45	1	PO	U	0	6144
<DlibHLQ>.AAAXSAMP	CYLS	26	1	PO	FB	80	32720
<DlibHLQ>.AABDXML	CYLS	5	1	PO	VB	512	32760
<DlibHLQ>.AEG1JAR	CYLS	10	2	PO-E	VB	1028	6144
<DlibHLQ>.AEG1SHSC	CYLS	1	1	PO-E	VB	255	27998
<DlibHLQ>.AEGPHFS	CYLS	35	10	PO-E	VB	1028	6144
<DlibHLQ>.AEGPJAR	CYLS	127	10	PO-E	VB	1028	6144

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DlibHLQ>.AEGPJCL	CYLS	2	1	PO-E	FB	80	32720
<DlibHLQ>.AEGPPROC	CYLS	1	1	PO-E	FB	80	32720
<DlibHLQ>.AEGPSAMP	CYLS	1	1	PO-E	FB	80	32720
<MSMPATH>/CEG1JAR	互換性なし						
<MSMPATH>/CEG1SHSC	互換性なし						
<MSMPATH>/CEGPHFS	互換性なし						
<MSMPATH>/CEGPJAR	互換性なし						
<MSMPATH>/datacom/dbsrv	互換性なし						
<MSMPATH>/dsi	互換性なし						
<RunTimeMVSHLQPrefix>.CAAXLOAD	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO1	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO2	CYLS	50	5	PO	U	0	27998
<RunTimeMVSHLQPrefix>.CAAXMAC	TRKS	227	15	PO	FB	80	32720
<RunTimeMVSHLQPrefix>.CAAXSAMP	CYLS	26	1	PO	FB	80	32720
<RunTimeMVSHLQPrefix>.CUSLIB	CYLS	8	1	PO	U	0	6144
<RunTimeMVSHLQPrefix>.CUSMAC	TRKS	37	15	PO	FB	80	3120
<RunTimeMVSHLQPrefix>.DEPLOYIN	TRKS	2	1	PS	FB	80	27920

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<RunTimeMVSHLQPrefix>.JCL	TRKS	20	20	PO	FB	80	27920
<RunTimeMVSHLQPrefix>.PROCLIB	TRKS	16	15	PO	FB	80	27920
<RunTimeMVSHLQPrefix>.SYSPRINT	TRKS	19	5	PS	VB	510	3120
<RunTimeUSSPath>/dsi	互換性なし						
<RunTimeUSSPath>/tomcat	互換性なし						
<TargetHLQ>.CAAXDATV	CYLS	88	1	PO	VB	31996	32000
<TargetHLQ>.CAAXLOAD	CYLS	20	5	PO	U	0	27998
<TargetHLQ>.CAAXLPA	TRKS	12	6	PO	U	0	27998
<TargetHLQ>.CAAXMAC	CYLS	15	1	PO	FB	80	32720
<TargetHLQ>.CAAXSAMP	CYLS	26	1	PO	FB	80	32720
<TargetHLQ>.CABDXML	TRKS	5	5	PO	VB	512	32720
<TargetHLQ>.CUSLIB	CYLS	8	1	PO	U	0	6144
<TargetHLQ>.CUSMAC	TRKS	37	15	PO	FB	80	3120
<TargetHLQ>.CEGPJCL	CYLS	2	1	PO-E	FB	80	32720
<TargetHLQ>.CEGPPROC	CYLS	1	1	PO-E	FB	80	32720
<TargetHLQ>.CEGPSAMP	CYLS	1	1	PO-E	FB	80	32720

CSMaxx06

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの初期量の合計は、3390 DASD スペースの 2,445 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.A011007	CYLS	15	5	PS	F	4096	4096

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.A021007	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.AUD4000	CYLS	500	350	PS	F	27992	27992
<dbHLQ>.CBS1006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.CXX	CYLS	35	10	PS	F	4096	4096
<dbHLQ>.DD1002	CYLS	60	15	PS	F	4096	4096
<dbHLQ>.DDD015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.DDDIXX	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.DEL1020	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.FXX	CYLS	90	15	PS	F	32760	32760
<dbHLQ>.INV4000	CYLS	400	100	PS	F	8192	8192
<dbHLQ>.IXX002	CYLS	45	15	PS	F	4096	4096
<dbHLQ>.IXX006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX016	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.IXX017	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.IXX1000	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1006	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.IXX1007	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1018	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1019	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX1020	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.IXX4000	CYLS	120	30	PS	F	4096	4096
<dbHLQ>.JNL4000	CYLS	120	30	PS	F	8192	8192
<dbHLQ>.LXX	CYLS	90	15	PS	U	32760	32760
<dbHLQ>.MSG015	CYLS	15	15	PS	F	4096	4096
<dbHLQ>.PXX	CYLS	90	15	PS	U	0	0
<dbHLQ>.PCY4000	CYLS	35	15	PS	F	4096	4096
<dbHLQ>.SCS4000	CYLS	130	60	PS	F	8192	8192

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.SDS4000	CYLS	90	30	PS	F	8192	8192
<dbHLQ>.SIT015	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.SNP1019	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.SQ1016	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.SRG4000	CYLS	60	15	PS	F	8192	8192
<dbHLQ>.STA1018	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.SYS1000	CYLS	15	5	PS	F	4096	4096
<dbHLQ>.TTM017	CYLS	5	5	PS	F	4096	4096
<dbHLQ>.XML4000	CYLS	300	300	PS	F	27992	27992

CSMaxx09

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの初期量の合計は 3390 DASD スペースの 460 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<dbHLQ>.MSM.CXX.INSBKUP	CYLS	35	10	PS	VB	4088	4096
<dbHLQ>.MSM.DB002.INSBKUP	CYLS	60	15	PS	VB	4069	27998
<dbHLQ>.MSM.DB015.INSBKUP	CYLS	15	15	PS	VB	2309	27998
<dbHLQ>.MSM.DB4000.INSBKUP	CYLS	350	300	PS	VB	27988	27992

CSMUxx01

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

これは最初に実行するジョブです。

このジョブの内容は、アップグレードしているバージョン固有です。

初期量スペース割り振りは、関連する z/OS のジョブストリームで定義されている内容を反映した、十分な割り当て量である必要があります。 ただし、総量は現在の環境の使用状況に基づいて、実際に必要な量に調節されます。

以下は、CA MSM V5.0 から CA CSM リリース 5.1 にアップグレードしている場合に必要なデータ セットです。

注: シリンダの初期量の合計は、3390 DASD スペースの 1,060 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	4088	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	27988	27992
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	10	PS	VB	4069	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	2309	27988
<depDbHLQ>.PR.BEXCLINV	CYLS	200	200	PS	VB	27988	27992
<depDbHLQ>.PR.BEXCLJNL	CYLS	200	200	PS	VB	27988	27992
<depDbHLQ>.PR.BEXCLPCY	CYLS	200	200	PS	VB	27988	27992

以下は、CA MSM R4.1 から CA CSM リリース 5.1 にアップグレードしている場合に必要なデータ セットです。

注: シリンダの初期量の合計は、3390 DASD スペースの 985 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	4088	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	27988	27992
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	10	PS	VB	4069	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	2309	27988
<depDbHLQ>.PR.BEXCLSCS	CYLS	130	60	PS	VB	2371	27998
<depDbHLQ>.PR.BEXCLSDS	CYLS	50	25	PS	VB	5778	27998
<depDbHLQ>.PR.ESCSDUF	CYLS	50	25	PS	FB	64	25600

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.PR.ESDSC13	CYLS	50	25	PS	FB	12	24000
<depDbHLQ>.PR.ESDSC24	CYLS	50	25	PS	FB	1349	26980
<depDbHLQ>.PR.ESDSSYS	CYLS	15	15	PS	FB	1043	26075
<depDbHLQ>.PR.ESRGSR1	CYLS	15	15	PS	FB	517	32571
<depDbHLQ>.PR.NSCSDUF	CYLS	50	25	PS	FB	82	24600
<depDbHLQ>.PR.NSDSC13	CYLS	50	25	PS	FB	20	26000
<depDbHLQ>.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<depDbHLQ>.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

以下は、CA MSM V4.0 から CA CSM リリース 5.1 にアップグレードしている場合に必要なデータ セットです。

注: シリンダの初期量の合計は、3390 DASD スペースの 1,105 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.CXX.BACKUP	CYLS	35	10	PS	VB	20480	27998
<depDbHLQ>.DB4000.BACKUP	CYLS	350	300	PS	VB	20480	27998
<depDbHLQ>.DDDBBU.BACKUP	CYLS	60	15	PS	VB	20480	27998
<depDbHLQ>.DDDDBU.BACKUP	CYLS	15	15	PS	VB	20480	27998
<depDbHLQ>.PR.BEXCLSCS	CYLS	130	60	PS	VB	2371	27998
<depDbHLQ>.PR.BEXCLSDS	CYLS	50	25	PS	VB	5779	27998
<depDbHLQ>.PR.ESCSCNP	CYLS	30	15	PS	FB	801	24030
<depDbHLQ>.PR.ESCSDUF	CYLS	50	25	PS	FB	64	25600
<depDbHLQ>.PR.ESDSC13	CYLS	50	25	PS	FB	12	24000
<depDbHLQ>.PR.ESDSC23	CYLS	30	15	PS	FB	632	25280
<depDbHLQ>.PR.ESDSC24	CYLS	50	25	PS	FB	1250	27500
<depDbHLQ>.PR.ESDSSYS	CYLS	15	15	PS	FB	1043	26075
<depDbHLQ>.PR.ESRGSR1	CYLS	15	15	PS	FB	517	32571

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<depDbHLQ>.PR.NSCSCNP	CYLS	30	15	PS	FB	806	24180
<depDbHLQ>.PR.NSDSDUF	CYLS	50	25	PS	FB	82	24600
<depDbHLQ>.PR.NSDSC13	CYLS	50	25	PS	FB	20	26000
<depDbHLQ>.PR.NSDSC23	CYLS	30	15	PS	FB	634	25360
<depDbHLQ>.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<depDbHLQ>.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

以下は、CA MSM r3.1 から CA CSM リリース 5.1 にアップグレードする場合に必要なデータ セットです。

注: シリンダの初期量の合計は 1,110 シリンダです。

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DatabaseHLQ>.MSM.CXX.BACKUP	CYLS	35	10	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DB4000.BACKUP	CYLS	350	300	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DDDBBU.BACKUP	CYLS	60	15	PS	VB	20480	27998
<DatabaseHLQ>.MSM.DDDDBBU.BACKUP	CYLS	15	15	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PR.BEXCLSDS	CYLS	50	25	PS	VB	20480	27998
<DatabaseHLQ>.MSM.PR.ESDSC13	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC14	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC15	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC16	CYLS	30	15	PS	FB	8	27992
<DatabaseHLQ>.MSM.PR.ESDSC23	CYLS	30	15	PS	FB	630	27720
<DatabaseHLQ>.MSM.PR.ESDSC24	CYLS	50	25	PS	FB	1250	27500
<DatabaseHLQ>.MSM.PR.ESDSDAS	CYLS	30	15	PS	FB	329	27965
<DatabaseHLQ>.MSM.PR.ESDSSYS	CYLS	15	15	PS	FB	770	27720
<DatabaseHLQ>.MSM.PR.NSDSC13	CYLS	50	15	PS	FB	20	26000
<DatabaseHLQ>.MSM.PR.NSDSC14	CYLS	30	15	PS	FB	13	27989

Name	Space Units	Pri Qty	Sec Qty	Dsorg	Recfm	Lrecl	Blksize
<DatabaseHLQ>.MSM.PR.NSDSC15	CYLS	30	15	PS	FB	13	27989
<DatabaseHLQ>.MSM.PR.NSDSC16	CYLS	30	15	PS	FB	13	27989
<DatabaseHLQ>.MSM.PR.NSDSC23	CYLS	30	15	PS	FB	634	25360
<DatabaseHLQ>.MSM.PR.NSDSC24	CYLS	50	25	PS	FB	1370	27400
<DatabaseHLQ>.MSM.PR.NSDSDAS	CYLS	30	15	PS	FB	331	27804
<DatabaseHLQ>.MSM.PR.NSDSSYS	CYLS	15	15	PS	FB	1060	26500

付録 B: トラブルシューティング

この付録が提供する、よくある質問およびトラブルシューティングの情報を使用し、CA CSM を使用するときに起こりうる問題の識別および解決ができるようになります。この付録には CA CSM エラー メッセージは含まれていません。

注: CA CSM メッセージの完全なリストについては、「*メッセージ リファレンス ガイド*」を参照してください。

SMP/E 内のメンテナンスの ACCEPT または RESTORE が失敗する

問題の状況:

SMP/E 環境でメンテナンスを ACCEPT または RESTORE しようとすると、タスクが失敗し、また SPMOUT がエラー メッセージのレポートを出力します。

- メンテナンスの ACCEPT に対し、以下のエラー メッセージが出力される場合があります。

  GIM51702S ** THE ACCEPT COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

- メンテナンスの RESTORE に対し、以下のエラー メッセージが出力される場合があります。

  GIM51702S ** THE RESTORE COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

理由:

実行しているアクションにより異なりますが、理由は以下のいずれかによるものです。

- メンテナンスを ACCEPT する場合、更新される配布ゾーンと関連するターゲット ゾーンが SMP/E 環境に存在しない、または関連するターゲット ゾーンが存在しません。
- メンテナンスを RESTORE する場合、更新されるターゲット ゾーンと関連する配布ゾーンが SMP/E 環境に存在しない、または関連する配布ゾーンが存在しません。

解決方法:

- 以下の例のような手順でバッチ ジョブをサブミットし、更新される配布ゾーンに関連する不足したターゲット ゾーンを追加するか、または既存のターゲット ゾーンを定義します。

```
SET
   BOUNDARY(distribution_zone_name) .
UCLIN .
ADD DLIBZONE(distribution_zone_name)
  RELATED(target_zone_name) .
ENDUCL .
```

- 以下の例のような手順でバッチ ジョブをサブミットし、更新されるターゲット ゾーンに関連する不足した配布ゾーンを追加するか、または既存の配布ゾーンを定義します。

```
SET
   BOUNDARY(target_zone_name) .
UCLIN .
ADD TARGETZONE(target_zone_name)
  RELATED(distribution_zone_name) .
ENDUCL .
```

CA CSM アドレス空間が正しく機能しない

症状:

SCS アドレス空間が正しく機能しません。また、ログに以下のようなメッセージが表示されます。

```
MSMC0501E SQL PREPARE VERSIONSTMT for task MSMCJTSK failed, SQLCODE=-124,
SQLSTATE=51002, RETCODE=,
                              IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST
MSMC0501E SQL ROLLBACK for task MSMCJTSK failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST


MSMC0501E SQL PREPARE_DEPUNIT for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0501E SQL ROLLBACK for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
```

さらに、以下のようなメッセージが表示されます。

```
MSMC0401E EVTINIT for task MSMCIES0 failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCIENG failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCCEVH failed, RETCODE=X'00000020'
```

原因:

CA Datacom/MSM データベース内の SQL プランが最新ではありません。

解決方法:

CA Datacom/MSM データベース内の SQL プランを更新し、同期します。

詳細:

SQL プランの更新 (P. 150)

CA CSM アプリケーション サーバのタイムアウト

症状:

メンテナンス パッケージの一覧を選択して表示すると、以下のメッセージが表示されます。

```
Reading maintenance packages from Software Catalog
```

その後、以下のエラー メッセージが表示されます。

```
The call failed on the server; see server log for details
```

MSMTC ジョブのログに、以下のメッセージが表示されます。

```
SEVERE: Exception while dispatching incoming RPC call
Throwable occurred: java.net.SocketTimeoutException: Read timed out
at java.net.SocketInputStream.read(SocketInputStream.java:140)
```

この問題は、Microsoft Internet Explorer で CA CSM の作業を行っているときのみ発生します。

原因:

CA CSM は大量のデータ表示に失敗します。

解決方法:

必要に応じ、以下の手順を実行します。

1. 表示する表の行数を確認します。 この数は、［Settings］タブの［User Settings］ -［User Preferences］ページの［Table Rows］フィールドで定義されます。 行の数が 250 の場合は、それをより低い値（たとえば 50 または 100）に設定します。

2. 表の行数を 250 のまま維持する必要がある理由がある場合は、CA CSM アプリケーション サーバのタイムアウト パラメータを更新します。

   tomcat/conf ディレクトリにある server.xml ファイルで、以下の行を検索します。

   ```
   connectionTimeout="20000"
   ```

   このパラメータは、TCP/IP スタックが着信パケットを待機する時間（ミリ秒）を定義します。 このパラメータを、より大きな値（たとえば、180000）に設定します。 次に、CA CSM アプリケーション サーバを再起動し、変更を有効にします。

   注: server.xml ファイルは、ASCII で保存されます。

詳細:

ASCII ファイルの編集 (P. 296)

SAF セキュリティが有効な状態での CA CSM の開始に失敗する

症状:

SAF セキュリティが有効な状態で、CA CSM が失敗します。 RC=13 または RC=15 の SafError がジョブのログに表示されます。 ログは以下の例のようなエラー メッセージを表示します。

```
FATAL (main) 2012-06-13 14:12:37,056 (SafManagerImpl.java:434):SafManager-
initialize
DSI():Return code from DDSI_java_open is higher than zero.RC=13
FATAL (main) 2012-06-13 14:12:37,067 (SystemManager.java:491):
com.ca.mf20.zos.services.saf.errors.SafError: null

Additional Diagnostic Data:
Error during DSI java open. RC=13
Path to 'dsi.conf': /u/users/msmr51/msmruntime/dsi/dsi.conf
BEGINNING OF 'dsi.conf' :
This is the DSI Server component configuration file
host localhost
port 22130
TLSKeyringFile /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.kdb
TLSKeyringStash /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.sth
TLSKeyLabel "Cert for SelfSigned Server"
TLSVerifyClient ON
END OF 'dsi.conf'
```

```
DSI parameters from table USERCONFIG in database:
Required parameters are marked with (*):
KEY:            DEFAULT_VALUE:  VALUE
*dsiPort:       22130:          22130
*dsiHost:       localhost:      localhost
*dsiConf:       N/A:            /u/users/msmr51/msmruntime/dsi/dsi.conf
>dsiKdb:        N/A:            Uninitialized
>dsiSth:        N/A:            Uninitialized
>dsiLabel:      N/A:            Uninitialized
>dsiVerPeer:    N/A:            false
```

解決方法:

必要に応じて、以下の手順を実行します。

- localhost エントリがユーザの DNS で定義されているかどうかを確認します。 以下の USS コマンドを発行します。

  ```
  oping localhost
  ```

  コマンドによりエラー メッセージ（EZZ3111I Unknown host 'localhost'）が返される場合、localhost エントリが定義されていません。この場合、以下のいずれかのアクションを実行します。

  - ネットワーク管理者に依頼し、ユーザの DNS に localhost エントリを定義します。
  - USERCONFIG データベース テーブルおよび dsi.conf で、dsiHost エントリを 127.0.0.1 に設定します (P. 296)。

- dsi.conf ファイル内の host および port パラメータが、USERCONFIG データベース テーブルの dsiHost および dsiPort のパラメータと同じであることを確認します。 host と dsiHost、および port と dsiPort のパラメータが異なる場合は、dsi.conf ファイルまたはデータベース エントリ (P. 296)のいずれかを更新します。 dsi.conf ファイルのコンテンツ、USERCONFIG データベース テーブルの CA DSI Server パラメータ、および dsi.conf ファイルへのパスが、エラー メッセージに表示されます。

- CA DSI Server のポート（port および dsiPort）が開放されていることを確認します。 以下の USS コマンドを発行します。

  ```
  onetstat -P port_number
  ```

  以下に例を示します。

  ```
  onetstat – P 22130
  ```

  このコマンドによって空の表が返される場合、ポートは開放されています。

- CA DSI Server のポートが CA CSM 用に予約済みかどうかを確認します。以下の USS コマンドを発行します。

  ```
  onetstat -o
  ```

  このコマンドは、予約済みポートの一覧を表示します。 CA DSI Server ポートが表示されない場合、CA DSI Server ポートを予約する (P. 52)ことをお勧めします。

CA CSM が例外で失敗する

問題の状況:

CA CSM が、たとえば以下のような例外で失敗します。

```
MSM0008E - System startup failed - please see error output for further information.
Fatal error that has stopped the startup was: or
g.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online in
Session(connect)).

MSM0010E - CA CSM startup failed.

FATAL (main) 2011-01-12 15:05:15,098 (SystemManager.java:333): java.lang.Error:
org.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online in
Session(connect))
```

理由:

SAMPLIB(SRVLIB) メンバおよび context.xml ファイル双方において、CA Datacom/MSM サーバの ServerName、または ApplicationID が一致しません。

解決方法:

context.xml または SAMPLIB(SRVLIB) のいずれかの ServerName または ApplicationID を変更し (P. 297)、それらが一致するようにします。

SMP/E 環境の移行が、SMP/E Environment Migration ウィザードの［SMP/E Environment Functions］手順で失敗する

症状:

SMP/E 環境の移行が、ウィザードの［SMP/E Environment Functions］手順で失敗します。または以下のいずれかのメッセージが表示されます。

- SMP/E Environment Migration ウィザードで、以下のメッセージが表示されます。

  ```
  MMR0005S - An error occurred during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so was not found. MMI0084S - Initialization of CAGIMAPI address space failed.
  ```

- MSMTC ジョブのログで、以下のいずれかのメッセージが表示されます。

  ```
  .1299171650. CGIMAPIExtractor_ForkStub: Exception occurred during Initialize() processing: mcCagimapiHandshake
  ```

  ```
  .1299171650. CGIMAPIExtractor_ForkStub: Exception text: Initialization of CAGIMAPI address space failed.
  ```

  ```
  An exception has occurred during native_initialize(): MMI0101S - A serious error has occurred while initializing GIMAPI Extractor.
  ```

  ```
  ERROR (http-17310-5) 2011-03-03 14:49:43,895 (DataExtractionDriver_Jni.java:305): Initialization of DataExtractionDriver_Jni has failed.
  ```

  ```
  INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206): A new message was read and enqueued in the message log: MMR0005S - An error occurred during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so was not found.  at ./CGIMAPIExtractionLibrary.C:51
  ```

  ```
  INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206): A new message was read and enqueued in the message log: MMI0084S - Initialization of CAGIMAPI address space failed. At ./CGIMAPIExtractor_ForkStub.C:430
  ```

原因:

CA CSM は共有オブジェクト ファイル（DLL）をロードできません。ファイルに必要な属性がないのが理由です。 すべてのファイルには、以下の属性が必要です。

+p、+s、+r、+x

libcci.so ファイルには、以下の属性も必要です。

+a

解決方法:

.so ファイルおよび .dll ファイルを確認し、属性および権限が正しいことを確認します。 必要な属性および権限を、それらが不足しているファイルに追加します。

1. 以下のコマンドを使用し、…/tomcat/lib ディレクトリ内のすべての .so ファイルおよび .dll ファイルの属性および権限を確認します。

   ```
   ls – E  *.so *.dll
   ```

   以下の例のような結果が表示されます。

   ```
   -rwxr-xr-x  aps-  1 USERID  GROUPID   233472 Aug 17  2010 libcci.so
   ```

2. 以下のコマンドを使用し、共有オブジェクト ファイルの属性を修正します。

   ```
   extattr attribute filename
   ```

   たとえば、+a 属性を libcci.so ファイルに追加するには、以下のように入力します。

   ```
   extattr +a libcci.so
   ```

3. 以下のコマンドを使用し、アクセス権限を修正します。

   ```
   chmod attribute filename
   ```

   たとえば、+r 権限を libcci.so ファイルに追加するには、以下のように入力します。

   ```
   chmod +r libcci.so
   ```

[Tasks]タブの[Delete Task]ボタンが無効

問題の状況:

［Tasks］タブからタスクを削除できません。また［Delete Task］ボタンが無効です。

理由:

タスクを削除するためのアクセス権がありません。

解決方法:

CA CSM のセキュリティ機能が有効かどうかを確認し、以下のいずれかを実行します。

- セキュリティ機能が有効な場合は、以下のリソース プロファイルが作成されていることを確認します。

  TM.TASK.@SELF.DELETE

  ユーザ自身のタスクを削除するためのアクセス権を付与します。

  TM.TASK.SYSTEM.DELETE

  任意のタスクを削除するためのアクセス権を付与します。

- セキュリティ機能が無効な場合は、CA CSM オプション ファイルで以下のオプションが指定されていることを確認します。

  sysTaskDeleteOverrideEnabled=Y

  sysTaskDeleteOverrideEnabled

  CA CSM ユーザにタスクを削除させるかどうかを指定します。

  Y

  任意のユーザが任意の完了タスクを削除できます。

  N

  ユーザは完了したタスクを削除できません。

  デフォルト： N

SMPOUT の展開で、GIMUNZIP メッセージが表示される

問題の状況:

展開タスクの SMPOUT レポートで、メッセージ GIM69158I が表示されます。

理由:

このメッセージは、展開を実行するユーザに UNIX SUPERUSER 属性がないか、または権限が割り当てられていないときに表示されます。 ターゲット システムの GIMUNZIP の動作は、SUPERUSER 属性の存在に影響を受けます。

解決方法:

これは情報を提供するメッセージです。

注: このメッセージに関連する特定のリターン コードまたは理由コードの詳細については、「*IBM SMP/E Messages and Codes*」を参照してください。

一時データ セットおよび RELFILE データ セットの動的割り当てエラー

問題の状況:

一時データ セットと RELFILE データ セットの動的な割り当てエラーが発生します。

理由:

HLQ オプションが、使用が許可されていない値に設定されています。

解決方法:

HLQ オプションを、使用が許可されている値に変更します。

ソフトウェア インストール中の MACLIB ライブラリの動的な割り当てが失敗する

問題の状況:

製品インストール中に SMP/E 環境を作成すると、メッセージ ログに以下のエラーが表示されます。

```
Dynamic allocation of input data set member SYS1.MACLIB(GIMZPOOL) failed. DD: ZP3 RC:
4 Error code: 0x1708 Info code: 0x2.
```

理由:

CA CSM がデフォルトの MACLIB ライブラリ、SYS1.MACLIB を見つけることができません。 たとえば、ライブラリの名前が変更されたことなどが理由です。

解決方法:

SAMPLIB (MSMLIB) メンバで、新しい Java ランタイム オプション maclib.dsn 変数を定義します。新しいデータ セット名が 38 文字を超えていないことを確認してください。

例:

```
IJO="$IJO -Dmaclib.dsn=CUSTOM.MACLIB"
```

不正な製品更新成功ステータス

問題の状況:

CA CSM は、Succeeded ステータスで製品更新を完了しますが、ソフトウェア カタログが更新されていません。

注: HTTP ダウンロードがアクティブなとき、この問題は発生しません。

理由:

Pax と ESD の製品ファイルは、即時ダウンロードが利用できないことがあります。この問題が発生すると、CA CSM は Web ページ上でこれらのファイルを利用できるようにする Request Product PrePackage 処理を開始し、処理が完了するとユーザに電子メールを送信します。CA サポート Online Web サイトの内部的な変更が理由で、CA CSM は CA CSM Build 442 PTF 5EGP442、またはそれ以降のバージョンがインストールされないかぎり、Request Product PrePackage 処理を開始しません。

解決方法:

CA CSM Build 442 PTF 5EGP442 またはそれ以降のバージョンがインストールされていることを確認してください。

GIM54701S ** ALLOCATION FAILED FOR SMPJHOME

問題の状況:

メンテナンス パッケージを APPLY すると、以下の SMP/E エラー メッセージが表示されます。

```
GIM54701S ** ALLOCATION FAILED FOR SMPJHOME - IKJ56228I PATH
/sys/java31bt/v6r0m0/usr/lpp/java/J6.0 NOT IN CATALOG OR CATALOG CAN NOT BE ACCESSED.
```

注: CA CSM が必須パスを指定しないため、Java ホーム パスが、旧メッセージの Java ホーム パスとは異なっている可能性があります。

理由:

メンテナンス パッケージを APPLY した SMP/E 環境で、SMPJHOME DDDEF が正しく設定されていません。

解決方法:

SMP/E 環境の SMPJHOME DDDEF を変更します。

- SMPJHOME DDDEF が CA CSM SMP/E 環境で正しく設定されていない場合、UCLIN ステートメントを使用し、CA CSM SMP/E 環境の SMPJHOME DDDEF を修正します。 (P. 179)
- SMPJHOME DDDEF が別の SMP/E 環境で正しく設定されていない場合は、UCLIN ステートメントを使用し、SMP/E 環境内のすべてのゾーンでの SMPJHOME DDDEF を修正します (P. 179)。

SMP/E が生成したデータ セットで I/O エラーが発生する

症状:

製品のインストール、またはメンテナンス パッケージの管理を行おうとすると、タスク出力がある 1 つ以上の手順がタスクに不足しています。これらの手順は、SMPLIST、SMPPRINT、SYSPRINT、SYSTERM のタイプである可能性があります。 MSMTC ジョブのログで以下のエラー メッセージが表示されます。

```
Errno2: -1070137335, ErrorCode: 0, FeedbackFdbk: 0, FeedbackFtncd: 0,
FeedbackRc: 0, LastOp: 3, ErrnoMsg: EDC5066I A read system error was detected.
```

原因:

CA CSM は、作成したタスク出力の一時データ セットの 1 つの読み込みに失敗すると、それ以上の読み込みができません。

解決方法:

以下を実行してください。

1. SAMPLIB（MSMLIB）データ セット メンバに以下のパラメータを含めます。

   ```
   IJO="$IJO -DWriteEmptyRecordMVS=true"
   ```

2. CA CSM アプリケーション サーバを再起動します。

MSMTC が RC=100 で失敗する

問題の状況:

ジョブが開始された後、MSMTC ジョブが RC=100（MAXCC=100）で失敗します。

以下に例を示します。

```
04.30.18 JOB00480 $HASP165 MSMTC    ENDED AT SYSSERV1  MAXCC=100 CN(INTERNAL)
```

STDMSG 出力には以下のメッセージが表示されます。

```
JVMJZBL2007E Stack trace follows:
java.lang.NoClassDefFoundError: org.apache.catalina.startup.Bootstrap
Caused by: java.lang.ClassNotFoundException: org.apache.catalina.startup.Bootstrap
```

注: STDMSG 出力は、MSMTC のジョブ ログの一部ではない場合があります。この出力は RunTimeMVSHLQPrefix.JCL（MSMTCSRV）の以下のステートメントによって管理されます。

```
//   ARGS=' start 1>stdout 2>stdERR',   <-- Args to Java class
```

ARGS が ''（空）の場合、STDMSG は作成されています。

理由:

MSMTC ジョブの最初の手順は、RunTimeUSSPath/Tomcat に配置された CA CSM アプリケーション サーバ (P. 329)を開始することです。

RunTimeUSSPath が空のとき、この手順は RC=100 で失敗します。
RunTimeUSSPath が空になる理由の 1 つに、このフォルダに属するファイル システムがマウントされていないことが考えられます。

解決方法:

- RunTimeUSSPath にファイル システムをマウントし、他のファイル システムも正しくマウントされていることを確認します。
- CA サポートにお問い合わせください。

CA CSM にアクセスするとき、No Ticket エラー メッセージが表示される

症状:

Web ブラウザを使用して CA CSM にアクセスしようとすると、No Ticket エラー メッセージをはじめとする複数のエラー メッセージが表示されます。そしてアクセスは失敗します。

原因:

Cookie がお使いの Web ブラウザで許可されていません。

解決方法:

お使いの Web ブラウザで Cookie を許可します。

サイトの標準が Cookie の使用を制限している場合、CA CSM アクセス URL を信頼済みサイトに追加します。

注: Cookie を許可する方法、および信頼済みサイトへの URL の追加方法の詳細については、お使いの Web ブラウザのユーザ ドキュメントを参照してください。

製品リストの更新が失敗する

症状:

製品リストを更新すると、以下のようなメッセージが表示されます。

```
IO Error was detected during PAS processing.
Additional Diagnostic Data:
IO Exception Error.(UnknownHostException) Error encountered while
accessing the following URL:
https://supportservices.ca.com/support
supportservices.ca.com
Please review your http proxy settings and validate that your system has network
connectivity to the above URL.
```

解決方法:

CA CSM アプリケーション サーバが正しい TCP/IP スタックを使用していることを確認します。 必要に応じ、CA CSM アプリケーション サーバのスタートアップ ジョブ（MSMTCSRV）、またはアプリケーション サーバのスターティッド タスクの SYSTCPD DD カードのコメントを解除します。

```
//SYSTCPD DD DSN=VTAM.TCPIP.TCPIP.DATA,
//           DISP=SHR
```

SMP/E の APPLY または ACCEPT 処理が失敗する

問題の状況:

SMP/E の APPLY または ACCEPT 処理が、ターゲットまたは配布ライブラリの空きディレクトリ ブロックの不足により、失敗します。

理由:

PDSMAN のような製品がインストールされ、PDS ディレクトリ ブロックがデフォルトよりも多くのスペースを占有する方法で設定されています。この特定の PDS データ セットが、空きのディレクトリ ブロックを使い果たしています。

解決方法:

PDS ディレクトリ ブロックの増加パーセンテージを変更します。

以下の手順に従います。

1. 以下のコマンドを使用して、MSMTC アドレス空間をシャットダウンします。

   ```
   P MSMTC
   ```

2. STDENV スタートアップ スクリプトで、MSMTC STC プロシージャの STDENV DDNAME が指しているデータ セットの、msm.pds.dirblk.percentage の変数を指定します。または、変数の値を増やすことができます。

   ```
   IJO="$IJO – Dmsm.pds.dirblk.percentage=25”
   ```

3. 以下のコマンドを使用して、MSMTC アドレス空間を開始します。

   ```
   S MSMTC
   ```

4. 失敗したタスクを再試行します。

MSMLOG ファイルで Tomcat エラーが発生する

問題の状況:

CA CSM Tomcat MSMLOG ファイルで、以下のエラー メッセージが表示されます。

```
WARNING: Error reading /dev/urandom
Throwable occurred: java.io.FileNotFoundException: /dev/urandom (EDC5157I An
internal error has occurred.)
 at java.io.FileInputStream.<init>(FileInputStream.java:112)
```

理由:

このメッセージは、PTF RO21996 が CA CSM r2.0（FMID CEG1200）にインストールされ、CA CSM Tomcat セッションを実行している z/OS システム上で、IBM Integrated Cryptographic Service Facility（ICSF）が開始されていない場合にのみ表示されます。

解決方法:

このメッセージが表示されても、CA CSM のパフォーマンスには全く影響しません。また CA CSM は引き続き機能します。 dev/urandom が実行されており、CA CSM と互換性があることを確認する場合は、以下のコマンドを使用します。

```
$ cat </dev/urandom | head -c12 | od -X
```

コマンドを実行すると、エラーのないランダム データが返ってきます。以下に例を示します。

```
0000000000          60621BCF        8AAD1F12        8944D619
0000000014
```

デバイスが動作していない場合、警告メッセージが表示されます。 以下に例を示します。

```
FSUM7343 cannot open "/dev/urandom" for input: EDC5157I An internal error
has occurred.
0000000000
```

このエラー メッセージが表示される場合は、/dev/random デバイスを再設定し、コマンドがこのデバイスから正常に読み取れるようにします。

注: /dev/random デバイスの詳細については、IBM の「*z/OS V1R10.0 UNIX System Services Planning*」（GA22-7800-14）を参照してください。

MSMLOG ファイルの Tomcat の起動時エラー

症状:

CA CSM Tomcat が起動中に失敗し、CA CSM Tomcat MSMLOG ファイルに以下のエラー メッセージが表示されます。

```
SEVERE: StandardServer.await: create[22150]:
Throwable occurred: java.net.BindException: EDC8116I Address not available.
             at java.net.PlainSocketImpl.socketBind(Native Method)
             at java.net.PlainSocketImpl.bind(PlainSocketImpl.java:384)
             at java.net.ServerSocket.bind(ServerSocket.java:331)
```

原因:

localhost Domain Name System（DNS）エントリが、ローカルの DNS に定義されていません。

解決方法:

ネットワーク管理者は、localhost の DNS エントリを定義する必要があります。

用語集

CA CSM アプリケーション サーバ

*CA CSM アプリケーション サーバ*は、CA CSM アプリケーション コードをサポートする CA CSM Tomcat のリージョンです。

CA Datacom/MSM サーバ

*CA Datacom/MSM サーバ*は、ワークステーション ベースのアプリケーションが CA Datacom/MSM データベースを使用できるようにするサーバです。

CA Recommended Service（CA RS）

*CA Recommended Service（CA RS）*は、メインフレーム統合システム テスト環境でテスト済みのメンテナンス パッケージ セットです。 CA RS メンテナンスをインストールして、ご使用の製品を常に最新の状態に保持しておくことをお勧めします。新しい CA RS メンテナンスが利用可能であるかどうかを知るには、その CA RS レベルに対して公開されたメンテナンスの一覧を示す CA RS ファイルをすべて自動または手動でダウンロードする必要があります。

CAICCI システム ID

CAICCI システム ID は、CAICCI ネットワークの一部であるシステムの一意の名前です。 これを指定しない場合、CA CSM は検証アクションを使用してそれを取得します。

FIXCAT

FIXCAT（修正カテゴリ）は、メンテナンス パッケージを PTF の 1 つ以上のカテゴリ（たとえばインストール、関数、z/OS バージョンまたは通信）に関連付けます。

FTP ポート

*FTP ポート*は、ファイルが転送される接続のポイントです。 デフォルトは 21 です。

Gen Level

Gen Level は、製品のリリース レベルの下の左ペインの製品リスト内で最も内側に位置するレベルです。 左ペインで Gen Level を選択すると、利用可能な基本インストール パッケージおよびその他製品コンポーネントが右ペインに表示されます。アイコン  の後に、Gen Level が表示されます。

詳細:

製品 (P. 334)
リリース (P. 338)

GIMUNZIP ボリューム

*GIMUNZIP ボリューム*は、CA CSM のデータ送信先の設定で、GIMUNZIP 制御ファイルを使用してデータ セットを特定のボリューム上に解凍するため、GIMUNZIP を向く GIMUNZIP ボリュームを指定します。 この設定は、CA CSM によって展開され、コピーされるライブラリが、ターゲット システムの特定のボリュームを向くようするための環境上のセットアップが必要なときに使用してください。

GIMZIP

GIMZIP は IBM のユーティリティで、*z* のサフィックスを持つソフトウェアのポータブル パッケージを作成します。

MSM Common Services

MSM Common Services（CETN500）は、Software Deployment Service（SDS）および Software Configuration Services（SCS）で構成される、 CA Common Services for z/OS の有用なコンポーネントです。

MSMCAUX

MSMCAUX は JCL プロシージャで、補助アドレス空間を開始するために使用されます。 CA CSM が使用する CA Common Services for z/OS には、CCS CAIPROC（CCShlq.CAIPROC）ライブラリのメンバ MSMCAUX にサンプル プロシージャが用意されています。このプロシージャを、z/OS START コマンドが使用するシステム PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。MSMCAUX サンプル メンバは、必要な変更を説明します。MSMCAUX プロシージャを手動で開始しないでください。 MSMCAUX プロシージャは SCS アドレス空間（MSMCPROC）によって開始されます。

MSMCPROC

MSMCPROC は JCL プロシージャで、SCS アドレス空間を開始するために使用されます。 CA CSM が使用する CA Common Services for z/OS には、CCS CAIPROC（CCShlq.CAIPROC）ライブラリのメンバ MSMCPROC にサンプル プロシージャが用意されています。 このプロシージャを z/OS START コマンドが使用するシステムの PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。 MSMCPROC サンプル メンバは、必要な変更を示しています。

MSMTC

MSMTC は、CA CSM アプリケーション サーバ (P. 329)に関連付けられたジョブ ストリームまたはスターティッド タスクです。

SCS アドレス空間

*SCS アドレス空間*は、特別に定義された場所で、出力およびコンソールのトラフィックを照会するためのシステム レジストリやコマンドが存在する、オペレーティングシステム内の場所です。 SCS アドレス空間は、ターゲットの z/OS システム間で設定を実装するのに必要なサービスおよび処理を提供します。SCS の処理をサポートするための各ターゲット システムは、SCS アドレス空間を実行する必要があります。

SCS アドレス空間ポート

*SCS アドレス空間ポート*は、そこを経由してクライアントがアドレス空間と通信する、接続のポイントです。 デフォルトは 49152 です。

UNIX System Services（USS）ファイル

z/OS システム用の *UNIX System Services（USS） ファイル*については、3 つのタイプのファイル システム、すなわち HFS（階層型ファイル システム）、zFS（zSeries ファイル システム）、および NFS（ネットワーク ファイル システム）があります。 USS ファイルは、これらのファイル システムの任意の 1 つ、または組み合わせであり、単一のスラッシュ（/）によって表されるルート ディレクトリから始まります。

VOLSER

VOLSER はボリューム シリアル番号で、明示的なボリュームにデータを配置します。

zFS 候補ボリューム

環境セットアップで、zFS コンテナ データ セットを指定したボリュームに送信するように指示されるときは、*zFS 候補ボリューム*を使用することができます。

オプション変数

*オプション変数*には、値は必須ではありません。 いくつかのオプション変数については、確認する必要があります。

解決済み変数

*解決済み変数*には値が含まれ、確定されています（必要に応じ）。 解決済み変数を修正できます。

確認

展開が完了したことを*確認します*。 これはユーザの最終アクションです。確認されるまで、展開は完了しません。 確認した後、展開は確認済み展開リストに移動します。

カスタム データ セット

*カスタム データ セット*は、z/OS データ セットまたは USS パーツのパスのいずれかを含むデータ セットです。

管理対象製品 USS ファイル システム

*管理対象製品 USS ファイル システム*は、CA CSM の制御下で SMP/E 環境によって使用される USS ファイル システムの集まりです。 CA CSM は、基本インストール中、およびオプションで SMP/E 環境の移行中に、管理対象製品 USS ファイル システムを作成します。

共有 DASD クラスタ

*共有 DASD クラスタ*システムは、DASD を共有するシステムのセットで、シスプレックスおよび非シスプレックス システムから構成することができます。ステージング システムを共有 DASD クラスタの一部にすることはできません。

検証

ユーザがシステムの［System Registry Page］上のシスプレックス システム、非シスプレックス システム、共有 DASD クラスタに対する［Actions］ドロップ ダウンで［Validate］ボタンを選択すると、*検証*プロセスが開始されます。 これによって、CAICCI 検証サービスを使用したバックグラウンド セキュリティ手順が開始され、このシステムが検証されます。

作業セット

*作業セット*とは、作業をする SMP/E 環境で使用される選択したグループのことです。 先々で表示される情報は、作業セットを基にしています。 たとえば、メンテナンス情報は、作業セットに対して表示されます。 この情報は、作業セットの外の環境には、表示されません。

資源

*資源*は、システムの物理的コンポーネントまたは仮想コンポーネントです。資源にはデータ セット、パラメータ設定、ライブラリ、ファイル、オペレータ コマンドが含まれます。 ダミー リソースは設定のビルド中または実装プロセス中に使用される一時資源で、または、トラッキング用のプレースホルダとして機能します。

システム レジストリ

*システム レジストリ*は、すべての CA CSM 管理製品が共有する変数データのリポジトリです。システム レジストリ リポジトリには、CA CSM に定義され、展開と設定のターゲットとして選択されるシステムに関する情報が格納されます。 非シスプレックス、シスプレックス、共有 DASD クラスタおよびステージング システムを作成できます。登録したシステムを保持、検証、表示、削除することができ、また失敗した検証を調査できます。

シスプレックス

シスプレックス（SYStem comPLEX）は IBM のメインフレーム システム複合体で、1 つ以上の物理システム上で動作する単一の論理システムです。シスプレックスを構成する各物理システムは、しばしば「メンバ」システムと呼ばれます。

自動 ID

自動 ID は、MSMID 変数の値です。 これはスナップショットの一部で、すべての展開に対して一意の値です。

集約パッケージ

*集約パッケージ*は、単一のメンテナンス パッケージを複数集めて構成されたファイルです（ネストされたパッケージ）。

シンボリック置換

*シンボリックの置換*または変換は CA CSM よって実行されるプロセスで、データ セット名マスクと Directory Path で指定されたマスク値を、変換時のシンボリック変数の内容に基づく実際の名前に解決します。 CA CSM シンボルは、シンボル リストに定義されています。 各シンボルはアンパサンド（&）で始まり、ピリオド（.）で終了します。 たとえばシンボル &LYYMMDD. は、アンパサンドと最後のピリオドを含め、変換時の値で置き換えられます。 最後のピリオドは重要です。これは、シンボリック名の一部とみなされます。

ステージング システム

*ステージング システム*は仮想システムで、CA CSM 実行システムがあるコンピュータに展開します。ステージング システムを使用するには、CA CSM 実行システムが CA CSM システム レジストリに登録されている必要があります。 ステージング システムは、展開のテストおよび展開全般について学習する上で有用です。 また、ターゲット システムがファイアウォールの外側にある場合でも使用できます。 たとえば、ステージング システムに展開し、その後展開をテープに手動でコピーします。

ストレージ クラス

*ストレージ クラス*は SMS 管理のデータ セットおよびオブジェクトにのみ適用されます。 ストレージ クラスにより、異なるレベルのパフォーマンスと可用性サービスを、データ セットに定義できるようになります。 ストレージ クラスを使用し、データ セットやオブジェクトに必要なサービス レベルと、その物理的特性を分離できます。ストレージ クラスにより、動的キャッシュ管理、順次データ セット ストライピング、および同時コピーの属性のような情報が提供されます。
ストレージ クラスは、SMS 管理のデータ セットまたはオブジェクトにする、データ セットまたはオブジェクトを持つストレージ クラスの集合です。 このため、動的キャッシュ管理や順次データ セット ストライピングのような機能は、SMS 管理のデータ セットのみに適用されます。 SMS 管理または非 SMS 管理のデータ セットがある可能性があります。 オブジェクトは SMS 管理される必要があります。

スナップショット

*スナップショット*は、CA CSM が IBM のユーティリティ GIMZIP を使用して作成する、ターゲット ライブラリのセットのコピーです。 CA CSM は GIMZIP を使用して、APPLY されたメンテナンスのリストをはじめとする、これらのライブラリの圧縮アーカイブを作成します。 このアーカイブ作成処理中、アーカイブ済みデータの整合性を保証するために、SMP/E 環境はロックされます。

製品

*製品*は、ベンダーの下の左ペイン内の製品リスト内のレベルです。 左ペインで製品を選択すると、右ペインに製品リリースが表示されます。 アイコン  の後に製品が表示されます。

詳細:

Gen Level (P. 329)
リリース (P. 338)

製品取得サービス（PAS）

製品取得サービス（PAS）を使用すると、メインフレーム製品とそのサービス（プログラム一時修正（PTF）など）を簡単に取得できます。 PAS は、ユーザのサイトにライセンスされている製品に関する情報を取得します。次に、PAS はそれらのライセンス情報を、ユーザの実行システムでメンテナンスされているソフトウェア インベントリに記録します。

接続システム

*接続システム*は、展開をどのシステム上で解凍するかを定義します。 つまり、解凍処理を実行するために、どのシステム CAICCI を生成するかが定義されます。

設定

*設定*は、展開済みソフトウェアをカスタマイズし、それをユーザの環境で使用可能にするために作成する、CA CSM のオブジェクトです。 設定にはユーザの環境に固有のプロファイル、変数およびリソースが含まれます。

設定カテゴリ

*設定カテゴリ*は構成用の変数の集まりです。 最上位ルート レベルは、すべてのカテゴリおよび変数を含んだカテゴリです。

ソフトウェア インストール サービス（SIS）

*ソフトウェア インストール サービス（SIS）*によって、実行システムのソフトウェア インベントリでのメインフレーム製品のインストールおよびメンテナンスが容易になります。 簡略化される操作には、ダウンロード済みソフトウェア パッケージの参照、実行システムでの SMP/E 統合ソフトウェア インベントリの管理、およびインストール タスクの自動化などがあります。

ソフトウェア構成サービス（SCS）

*ソフトウェア構成サービス（SCS）*によって、実行システムのソフトウェア インベントリからターゲットの z/OS オペレーティング システムへのメインフレーム製品の設定が容易になります。

ソフトウェア展開サービス（SDS）

*ソフトウェア展開サービス（SDS）*によって、実行システムのソフトウェア インベントリからターゲット システムへのメインフレーム製品の展開が容易になります。 簡略化される操作には、既知のトポロジ全体での適切な転送メカニズムによる、ポリシー準拠のインストール済み製品の展開などがあります。

タスク出力ブラウザ

*タスク出力ブラウザ*は、完了したタスクの詳細を表示します。

ディレクトリ パス

*ルートのディレクトリ パス*は、FTP サーバがアクセスを許可された基本のディレクトリです。 FTP サーバはこのディレクトリ、およびそのサブディレクトリにファイルを作成し、そこからのファイルの読み取りを許可されます。 ディレクトリ パスは USS パス名です。これは、スラッシュ（/）で区切られた 1 つ以上のディレクトリ リーフで構成されます。また、最大入力長は、スラッシュを含めて 255 文字です。 ディレクトリ パスが変換されるとき、最大長は 255 文字になります。

データ宛先

システムごとに*データ宛先*を定義する必要があります。 データ宛先は、転送データをリモート システムに転送するためにどのテクニックを使用するかを CA CSM に指示する方法です。 データ宛先は、非シスプレックス システム、シスプレックス システム、および共有 DASD クラスタに割り当てられます。 データ宛先は名前付きオブジェクトで、システム レジストリ内の複数のエンティティに割り当てられる場合があります。また、データ宛先自身の独立したメンテナンス ダイアログ ボックスがあります。

データ セット名マスク

*データ セット名マスク*は、各データ セットを識別する一意の名前です。これは、ピリオドで区切られた 1 つ以上の修飾子で構成され、ピリオドを含めた最大入力長は 64 文字です。 データ セット名マスクを変換するとき、ピリオドを含めた最大長は 44 文字です。

展開

*展開*機能により、スナップショット、転送、展開のアクションが 1 つのアクションに集約され、社内中のシステムに CA CSM 製品をコピーすることが可能になります。 たとえば、共有 DASD にコピーし、または FTP を経由して、1 つまたは多数の製品を 1 つまたは多数のシステムに送信できます。

展開

*展開*では、ライブラリおよびデータ セットを展開できます。 このプロセスでは、SMP/E に定義されたターゲット ライブラリおよびユーザ データ セットを、共有 DASD およびネットワーク環境の両方にコピーします。

転送

*転送*機能により、FTP 経由で組織全体のシステムに製品をコピーすることができ、今後の展開に備えることができます。

統一資源識別子（URI）

*統一資源識別子（URI）*は、インターネット上の名前またはリソースを識別するために使用される文字列です。 この識別子により、特定のプロトコルを使用したリソースの表現との対話が、ネットワーク間で（通常は、World Wide Web）可能になります。 具体的な構文法および関連するプロトコルを指定するスキームにより、各 URI が定義されます。
共有 DASD クラスタまたはシスプレックスについては、URI は接続システムの URI である必要があります。

トポロジ

企業システム *トポロジ*には、共有 DASD 環境、ネットワーク環境、および z/OS システムを含めることができます。

非シスプレックス

*非シスプレックス*は、シスプレックスまたはモノプレックス システムの一部ではない、スタンドアロンの z/OS システムです。

ファイル転送プロトコル（FTP）

*ファイル転送プロトコル（FTP）*は、ネットワーク上のあるコンピュータから別のコンピュータにファイルを転送するためのプロトコルです。

プレビュー

*プレビュー*では、展開は名前で識別され、製品、システム、転送方法、ターゲット ライブラリ（ソース、ターゲット、解決を含む）、および SMP/E の環境とスナップショットが簡潔に表示されます。

プロファイルおよびプロファイル オカレンス

*プロファイル*は、サブシステムまたはコンポーネントに属する変数の集まりです。 *プロファイル オカレンス*は、特定のシステム用にカスタマイズされたバージョンのプロファイルです。1 つのシステムに同じプロファイル用の複数のプロファイル オカレンスを持つことができます。

方法

*方法*とは、ターゲット システム上でデータ セットが命名されるプロセスです。 方法は、展開の*方法*を提供します。 方法は説明がある名前付きオブジェクトで、個別の展開に割り当てられます。

ポリシー

CA CSM の*ポリシー*は、（1）製品のコンポーネント部分を識別するメタデータの入力、および（2）展開基準（展開する場所および名前など）を識別するユーザ入力の組み合わせを表します。

モノプレックス

*モノプレックス*は、ただ 1 つのメンバ システムと、最小の単一のカップリング ファシリティを持つシスプレックスです。 現在、モノプレックスはシスプレックスと同じ方法でトラックされます。違いは、Web ベース インターフェースで表示されるシスプレックス名が、実際のモノプレックスのシステム名であることです。

ランディング ディレクトリ

*ランディング ディレクトリ*はデータが展開中に一時的に配置される場所です。

リリース

*リリース*は、製品の下の左ペインの製品リスト内のレベルです。 左ペインのリリースを選択すると、右ペインにメンテナンス パッケージが表示されます。 アイコン の後にリリースが表示されます。

詳細:

Gen Level (P. 329)
製品 (P. 334)

索引

S

U

V

X

Z

あ

か

さ

た

は

ま

や

ら