CA Chorus™ Software Manager

サイト準備ガイド

バージョン 06.0.00、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 ACF2™ for z/OS
- CA Chorus™
- CA Common Services for z/OS
- CA Database Management Solutions for DB2 for z/OS
- CA Datacom/MSM
- CA Distributed Security Integration for z/OS（CA DSI Server）
- CA PDSMAN® PDS Library Management（PDSMAN）
- CA Top Secret® for z/OS

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。

- 概要 -> CA CSM インストールを準備する方法 (P. 8)： プロセスを更新および効率化
- 要件とポートの確認 > ディスク領域の要件 (P. 11)： z/OS V2.1 内のユーティリティ プログラム IOEAGFMT の変更に関する重要な注意事項を追加
- 要件とポートの確認 > ソフトウェア要件 (P. 13)： セクションを更新
- セキュリティのセットアップ (P. 21)： 章を追加
- CA CSM Prerequisite Validator ユーティリティの使用 > インストールの準備 > Prerequisite Validator 要件の確認 (P. 30)： Java 要件を更新
- CA CSM Prerequisite Validator ユーティリティの使用 > ネイティブ USS コマンド プロンプトからの実行 > デフォルト プロパティの変更 (P. 32)： 既存パラメータを更新、新規パラメータを追加
- CA ACF2 for z/OS を使用して CA CSM のセキュリティをセットアップ (P. 41)：外部操作用の PassTicket のセットアップに関する情報が含まれるセクションを更新
- CA Top Secret for z/OS を使用して CA CSM のセキュリティをセットアップ (P. 55)： 外部操作用の PassTicket のセットアップに関する情報が含まれるセクションを更新
- IBM RACF を使用して CA CSM のセキュリティをセットアップ (P. 69)：外部操作用の PassTicket のセットアップに関する情報が含まれるセクションを更新

目次

第 1 章: 概要

このガイドでは、CA CSM バージョン 6.0 をインストールする前、または CA CSM を最新のバージョンにアップグレードする前に実行するべき準備について説明します。

このセクションには、以下のトピックが含まれています。

対象読者

このガイドは、「*インストール ガイド*」で説明されているインストールまたはアップグレード タスクを開始する前にシステム プログラマおよびセキュリティ管理者が完了できるタスクの詳細を示しています。 このサイト準備ガイドに従うことで、インストール手順を大幅に簡略化することができます。

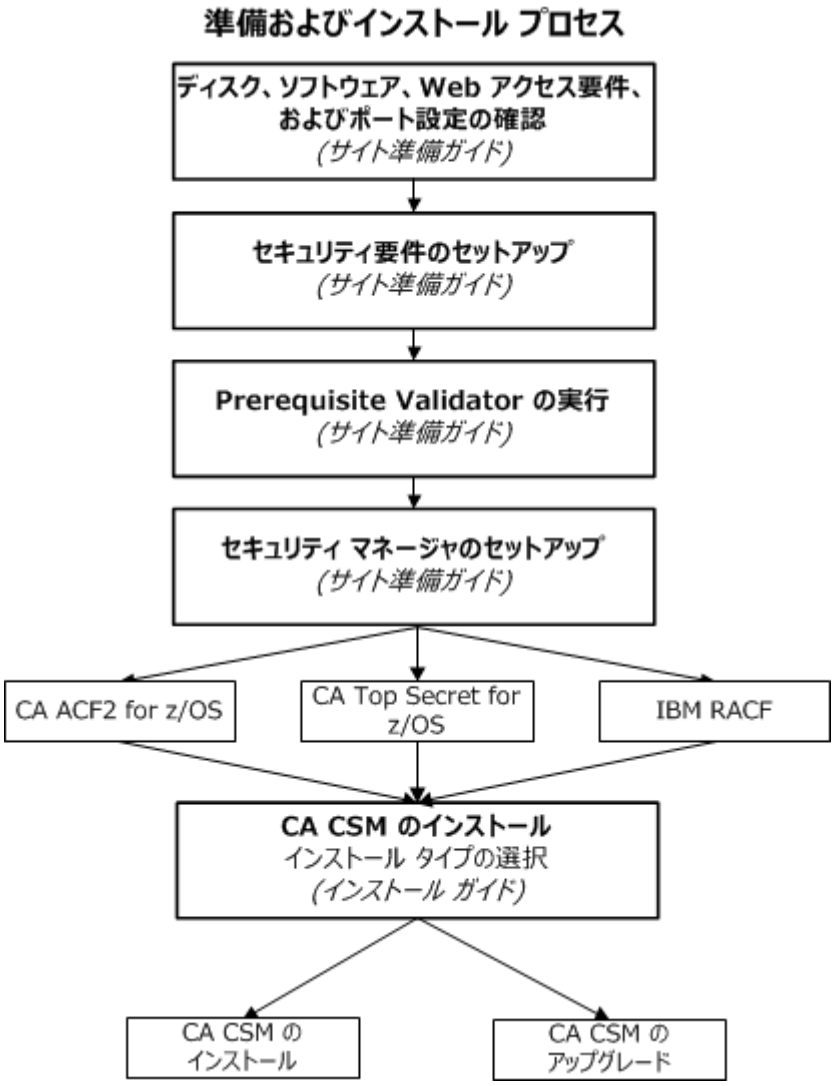
必要なスキル

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

CA CSM インストールを準備する方法

以下の図は、CA CSM の準備およびインストール プロセスの大まかな流れを示し、インストールを完了するためのガイドとなります。



CA CSM のインストールおよびアップグレードを準備するには、以下の手順に従います。

1. 「*サイト準備ガイド*」の記述に従いディスク要件、ソフトウェア要件、Web アクセス要件およびポート設定を確認します。
2. 「*サイト準備ガイド*」の記述に従い、セキュリティ要件をセットアップします。

3. 「*サイト準備ガイド*」の記述に従い、Prerequisite Validator ユーティリティを実行します。
4. 「*サイト準備ガイド*」の記述に従い、セキュリティ マネージャをセットアップします。
5. 「*インストール ガイド*」の記述に従い、CA CSM バージョン 6.0 をインストール、または CA CSM の既存のバージョンを バージョン 6.0 にアップグレードします。

第 2 章: 要件およびポートの確認

ディスク要件、ソフトウェア要件および Web アクセス要件が満たされ、TCP/IP ポートが設定されていることを確認します。

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 = 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。

    重要: z/OS V2.1 から開始して、IBM は、ユーティリティー プログラム IOEAGFMT（zFS データ セット フォーマッタ）が機能する方法を変更しました。ユーティリティは、IOEAGFMT の実行が許可される前にアクティブになる zFS カーネル アドレス空間を必要とします。サイトで zFS ファイル システムを使用する場合、zFS カーネル アドレス空間がアクティブであることを確認する必要があります。詳細については、IBM の「*z/OS Distributed File Services zFS Administration*」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。

- TSO 領域 = 143360 KB（最低でも）

- 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 の場合、各ターゲット システムにはそれぞれ、3390 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。

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、または バージョン 14.0 が必要です。

- CA CSM ドライビング 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、CETN600 が適用されていることを確認します。

  CA Common Services for z/OS リリース 14.1 またはバージョン 14.0 に CETN600 をインストールすると、それは CETN400 および CETN500 を置換します。

  注: すべての公開された CETN600 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。 CETN600 を適用しない場合、CA CSM は操作可能です。 ただし、Software Configuration Service（SCS）および Software Deployment Service（SDS）は使用不可能です。

- バージョン 14.0 に PTF RO40945、RO44235、RO44412 を適用します。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。

  リリース 14.1 に PTF RO53900 および RO53926 を適用します。

  重要: 指定された順序で PTF をリリース 14.1 に適用するか、または PTF 処理エラーを同時に回避します。

  CA Common Services for z/OS に CETN600 をインストールした後、バージョン 14.0 に RO64950 を適用するか、または SDS および SCS をサポートするために RO64952 をリリース 14.1 に適用します。

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

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）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: CA CSM ドライビング システムおよび SDS と SCS 用のすべてのターゲット システム上で、CAICCI が設定され、実行され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。

他にも CA Technologies ソフトウェア製品がある場合は、それらの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 に適用します。 または、PTF RO30898 を CA ACF2 for z/OS r15 に適用します。
- CA Top Secret for z/OS を使用する場合、PTF RO31780 を CA Top Secret for z/OS r14 に適用します。 または、PTF RO30836 を CA Top Secret for z/OS r15 に適用します。
- 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、最新公開の 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、ジョブのサブミットおよび処理に TSO を使用するように CA CSM インストール プロセスを設定できます。
- システムに少なくとも SMP/E V3R5 があること。
- システムに少なくとも IBM 64-bit Java SDK 1.7 for z/OS があること。 SR5 を使用することをお勧めします。

  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てください。 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 のリリースがリスト表示されます。 この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、それがサイトに適した設定である場合、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 へのアクセスに使用するコンピュータには、ご使用のメインフレームにアクセスできる Web ブラウザが必要です。CA CSM は以下のブラウザでテストされました。

- Mozilla Firefox 28
- Google Chrome 33
- Microsoft Internet Explorer 8、9 および 10

  注: Microsoft Internet Explorer のサポートされているバージョンについては、ドキュメント モードが Page Default に設定されていることを確認してください。 ドキュメント モードの詳細については、Microsoft Internet Explorer のユーザ ドキュメントを参照してください。

Mozilla Firefox を使用することをお勧めします。

お使いの Web ブラウザに 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。画面解像度がそれより低い場合、CA CSM Web ベース インターフェースが一部正しく表示されません。

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（MSMTC）は、使用中のランダムなファイルを設定しそのユーザ セッションの追跡を試みます。1 つのファイル作成されると、CA CSM はそれを使用します。 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（MSMTC）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 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 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。

Or

```
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。

第 3 章: セキュリティのセットアップ

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 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 プレフィクスに対してエイリアス 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。 このとき、切り替えられた SU ID には、オプション ファイルで指定された MVS データ セット修飾子に対する CREATE および MODIFY 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
- Java ロード モジュールがインストールされているデータ セットのメンバ JVMLDM76 （64 ビット Java 7.0 用）
- （オプション） SYS1.IDI.SIDIAUTH のメンバ IDIXCEE （オプションの EXIT として IDIXCEE を使用する場合のみ）

注: リソースを表示するには、RLIST コマンドを発行します。

プログラムを制御するために、IBM RACF を設定できます。 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される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、IOE.SIOELMOD（または同等のライブラリ）をプログラム制御に追加します。

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（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 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 アプリケーション サーバのユーザ ID には、UID(0) があると見込まれています。UID(0) のない CA CSM を設定する場合は、「*Administration Guide*」を参照してください。
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）
   - CA ACF2 for z/OS のみ： CA CSM を開始するユーザに対する MUSASS 許可
   - サイトで CA SAF HFS セキュリティを使用する場合は、以下のアクセス権を設定します。
     - BPX.CAHFS.SET.RLIMIT （READ 権限）
     - BPX.CAHFS.PTRACE（READ 権限）
     - BPX.CAHFS.MOUNT（READ 権限）

- BPX.CAHFS.UNMOUNT（READ 権限）
- BPX.CAHFS.CHANGE.FILE.MODE （READ 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。

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。

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。

次の手順に従ってください:

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)
     ```

   - IBM 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)
     ```

   - IBM 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
   ```

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。

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。

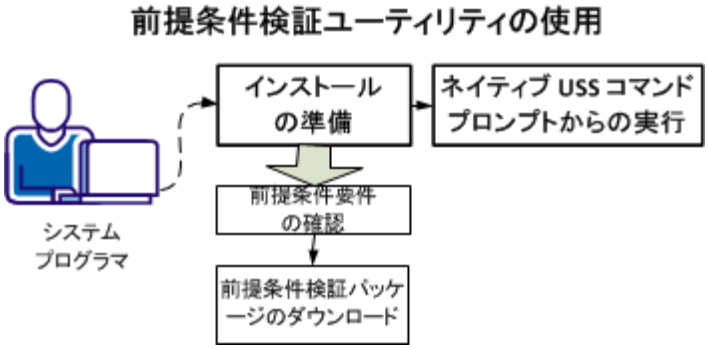
注: CA CSM は、CA CSM アプリケーション サーバ ID のセキュリティ コンテキストで GIMUNZIP を実行します。 SMP/E セキュリティがアクティブな場合、CA CSM アプリケーション サーバ ID には SAF FACILITY クラスの GIM.PGM.GIMUNZIP リソースへの READ アクセス権が必要です。

注: SAF チェックを有効にする方法の詳細については、「*Administration Guide*」を参照してください。

第 4 章: CA CSM Prerequisite Validator ユーティリティの使用

Prerequisite Validator ユーティリティを使用して、CA CSM をインストールする前に必要なセキュリティ権限がすべて整っていることを確認することができます。

インストール タスクを開始する前に、以下のタスクを実行して、必要な権限がすべて整っていることを確認します。



1. インストールの準備をします (P. 29)。
   a. Prerequisite Validator の要件を確認します (P. 30)。
   b. Prerequisite Validator 製品パッケージをダウンロードします (P. 30)。
2. ネイティブ USS コマンド プロンプトから実行します (P. 31)。

インストールの準備

このセクションでは、インストールを開始する前に実行するタスクについて説明します。

1. Prerequisite Validator の要件を確認します (P. 30)。
2. Prerequisite Validator 製品パッケージをダウンロードします (P. 30)。

Prerequisite Validator の要件の確認

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
- z/OS 用の IBM 64 ビット Java SDK 1.7
- 最小の TSO REGION サイズ 128 MB
- CA CSM の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 リソースへのアクセス権。

  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。

Prerequisite Validator 製品パッケージのダウンロード

Prerequisite Validator ユーティリティは CA サポート Online Web サイトで利用できます。

次の手順に従ってください:

1. CA サポート Online Web サイトに移動し、ログインして、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、最新のリリースを選択し、［Go］をクリックします。

   注: 製品リストで CA Chorus Software Manager が見つからない場合は、「*Don't see your product name below?*」のリンクをクリックします。

   製品ダウンロードの一覧が表示されます。
3. USS 環境内のディレクトリに Prerequisite Validator pax ファイル（CA CSM PRE VAL UTIL-ESD のみ）をダウンロードします。

ネイティブ USS コマンド プロンプトからの実行

z/OS システムでネイティブ USS コマンドを使用して、Prerequisite Validator ユーティリティを実行します。

次の手順に従ってください:

1. 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。
2. 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
   ```

3. 以下のコマンドを発行します。

   `pax -rvf file_name.pax.Z`

   file_name

   CA サポート Online Web サイトの Download Center からダウンロードした Prerequisite Validator ファイルの名前を指定します。例えば、DVD10155641E.pax.Z です。

   注: 完全な pax ファイル名およびその拡張子では、大文字と小文字が区別されます。 pax コマンドを発行する場合、大文字/小文字を正しく使用していることを確認してください。

   Bin フォルダのコンテンツが展開されます。

4. 以下のコマンドを発行します。

   ```
   cd Bin
   ```

5. （オプション）必要に応じて、デフォルトのプロパティ ファイルのパラメータ (P. 32)を修正します。
6. 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/J7.0_64
   ```

   使用許諾契約の画面が表示されます。

7. 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。

8. （オプション）デフォルトのファイル パラメータを変更した（P. 32）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のプロパティ 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 プロパティの変更

Prerequisite Validator ユーティリティの一部のパラメータには、デフォルトのプロパティが自動的に入力されています。

必要に応じて、サイト要件ごとにデフォルト プロパティ ファイル パラメータを変更します。

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。

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。収集されたホスト名が接続に失敗した場合、それを提供するように促されます。

注: このパラメータはデフォルトではコメントアウトされます。

ftp.port=

指定したホスト名または IP アドレス用の 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.stat.check.credential=

FTP quote STAT コマンドを発行する権限が必要かどうかを指定します。サイトに FTP quote STAT コマンドを発行する権限が必要な場合、「ftp.stat.check.credential=y」を指定します。 ユーティリティはユーザ ID とパスワードの入力を促すプロンプトを表示します。 コマンドは、ログに以下のように表示されます。

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

y を設定すると、ユーティリティはユーザ ID とパスワードの入力を促すプロンプトを表示します。

デフォルト： n

ftp.check=

FTP チェックを有効にするかどうかを指定します。 外部の CA Technologies FTP サーバへの接続 (P. 39)のチェックをアクティブにするには ftp.check=y を指定します。

デフォルト： y

ftp.proxy.enabled=

プロキシ サーバによる FTP チェックをアクティブにするかどうかを指定します。 プロキシ サーバによる FTP チェックをアクティブにするには ftp.proxy.enabled=y を指定します。

デフォルト： n

ftp.proxy.host=

プロキシ チェックが有効な場合、プロキシ サーバ（ホスト名または IP アドレス）を指定します。

ftp.proxy.port=

プロキシ チェックを有効にする場合は、ftp.proxy.host で定義したサーバのポート番号を指定します。

デフォルト： 21

ftp.proxy.credential.check=

プロキシ アクセスに認証情報が必要かどうかを指定します。 プロキシ サーバへのアクセス時に認証情報を要求するには、ftp.proxy.credential.check=y を指定します。

デフォルト： n

ftp.proxy.userid=

プロキシ サーバへのアクセス時に認証情報が要求される場合、プロキシ ユーザ ID を指定します。FTP プロキシ パスワードを求められます。

ftp.advanced.options=

プロキシの詳細オプションを使用するかどうかを指定します。 一連の ftp.proxy.FIRECMD オプションを定義するには、ftp.advanced.options=y を指定します。

デフォルト： n

以下のサンプルは、FTP プロキシ サーバにログインするためのコマンドの一例です。 複数のコマンドを使用する場合は、各コマンドにシーケンス番号を追加します。

```
ftp.proxy.FIRECMD.1=HOST;
ftp.proxy.FIRECMD.2=REMOTE_USER;@REMOTE_HOST; USER;
ftp.proxy.FIRECMD.3=REMOTE_PW;
ftp.proxy.FIRECMD.4=ACCT; PW;
```

ftp.proxy.FIRECMD.1=HOST;

プロキシ FTP ホスト サーバに接続するように Prerequisite Validator FTP クライアントに指示します。

ftp.proxy.FIRECMD.2=REMOTE_USER;@REMOTE_HOST; USER;

パラメータ ‘anonymous@ftp.ca.com *ftp.proxy.userid*’ を持つ FTP USER コマンドを送信するように FTP クライアントに指示します。

ftp.proxy.FIRECMD.3=REMOTE_PW;

一般的な電子メール アドレスを持つ FTP PASS コマンドを送信するように FTP クライアントに指示します。

ftp.proxy.FIRECMD.4=ACCT; PW;

プロンプトで入力したプロキシ パスワードを持つ FTP ACCT コマンドを送信するように FTP クライアントに指示します。

コマンドに以下のキーワードを使用することができます。

HOST

FTP プロキシ サーバの名前および IP 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 ftp.proxy.host オプションの値が代入されます。 FTP クライアントは、最初の接続にこの値を使用します。ftp.proxy.port の値も接続を確立するために使用されます。

USER

FTP プロキシの認証に使用する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 ftp.proxy.userid オプションの値が代入されます。

PW

FTP プロキシの認証に使用するパスワードを定義します。 このキーワードがあるとき、この値にはプロンプトで入力したプロキシ パスワードが代入されます。

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 CA Technologies FTP サーバに対する適切な FTP URL が代入されます。Prerequisite Validator ユーティリティではこれらの URL が提供されます。

REMOTE_USER

リモート サーバの認証に使用するユーザを定義します。 このキーワードがある場合、この値には「*anonymous*」が代入されます。

REMOTE_PW

リモート サーバの認証に使用するパスワードを定義します。このキーワードがある場合、この値には Prerequisite Validator ユーティリティにより指定された一般的な電子メール アドレスが代入されます。

ACCT

FTP プロキシ サーバに ACCT コマンドを発行するよう、FTP クライアントに指示します。このキーワードにより、付属パラメータが許可されます。 このパラメータは通常、PW キーワードが表すプロキシ パスワードです。

http.check=

HTTP Web サービス チェックをアクティブにするかどうかを指定します。HTTP Web サービス チェックをアクティブにするには http.check=y を指定します。

デフォルト： y

https.download.check=

HTTPS ファイル ダウンロードのチェックを有効にするかどうかを指定します。 HTTPS 接続チェックをアクティブにするには https.download.check=y を指定します。 HTTPS はファイルのダウンロードで FTP に代わるものです。

デフォルト： n

http.request.timeout=

リクエスト タイムアウト（秒）を指定します。

デフォルト: 3

http.connection.timeout=

タイムアウト後に HTTP 接続を確立するための試行回数を指定します。

デフォルト： 2

http.port=

HTTP 接続のポート番号を指定します。

デフォルト： 80

https.port=

HTTPS 接続のポート番号を指定します。

デフォルト： 443

http.proxy.enabled=

プロキシ サーバによる HTTP チェックをアクティブにするかどうかを指定します。 プロキシ サーバによる HTTP チェックをアクティブにするには http.proxy.enabled=y を指定します。

デフォルト： n

http.proxy.host=

プロキシ チェックが有効な場合、プロキシ サーバ（ホスト名または IP アドレス）を指定します。

デフォルト： myproxy.ca.com

http.proxy.port=

http.proxy.host で定義したサーバのポート番号を指定します。

デフォルト： 80

http.proxy.credential.check=

プロキシ アクセスに認証情報が必要かどうかを指定します。プロキシ サーバへのアクセス時に認証情報を要求するには、http.proxy.credential.check=y を指定します。

注: http.proxy.type=NTML の場合は、このパラメータを「y」に設定します。

デフォルト： n

http.proxy.type=

プロキシ サーバが NTLM 認証を使用するかどうかを指定します。プロキシ サーバで NTLM 認証の使用を有効にするには、「http.proxy.type=NTLM」を指定します。それ以外の場合、このパラメータを空白のままにします

http.domain=

プロキシ サーバで NTLM 認証（http.proxy.type=NTLM）を使用する場合は、NTLM ドメイン名を指定します。 NTLM 認証が使用されない場合、このパラメータは無視されます。

以下のサンプルは、プロキシ サーバを経由するためにユーザのサイトが外部 CA Technologies HTTP サーバへのリクエストを必要とする場合にパラメータを設定する方法の一例です。

```
http.proxy.enabled=yes
http.proxy.host=host_name_or_IP_address
http.proxy.port=80
http.proxy.credential.check=y
http.proxy.type=NTLM
http.domain=NTLM_domain_name
```

SafSecurityResourceAccess=

SAF を介して以下のリソースに対するユーザ アクセスを確認するかどうかを指定します。

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

リソース アクセス チェックを実行するには、「SafSecurityResourceAccess=y」を指定します。

デフォルト： y

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

注: デフォルト値を維持することをお勧めします。

MSMDSIPORTNO=

CA DSI Server 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

注: デフォルト値を維持することをお勧めします。

MSMConnectorRedirectPortNo=

リクエストのリダイレクト先のポート番号を指定します。リクエストが SSL ではないポートで受信され、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

注: デフォルト値を維持することをお勧めします。

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

検証用のカスタム FTP サーバの定義

デフォルトでは、Prerequisite Validator ユーティリティは以下の CA Technologies FTP サーバへの接続性を確認します。

- ftp.ca.com:21
- scftpd.ca.com:21
- ftpca.ca.com:21

Prerequisite Validator ユーティリティが接続を試行する FTP サーバのカスタム リストを指定し、ユーザのシステムに適切なネットワーク接続があるかどうかを判断できます。

次の手順に従ってください:

1. デフォルトのプロパティ ファイルを開き、以下を編集します。

   unpax_directory/Bin/lib/MSMSetupDefault.properties

2. FTP チェックがアクティブであることを確認します。

   ```
   ftp.check=y
   ```

3. 各 FTP サーバのホスト名およびポート番号を指定してユーティリティが接続する FTP サーバを入力します。

   ```
   ftp.check.host.1=hostname_1
   ftp.check.port.1=port_number_1
   ftp.check.host.2=hostname_2
   ftp.check.port.2=port_number_2
   ...
   ftp.check.host.n=hostname_n
   ftp.check.port.n=port_number_n
   ```

   たとえば、以下のサンプルを入力すると、Prerequisite Validator ユーティリティがポート 21 上の ftp.orders.ca.com およびポート 21 上の ftp.products.ca.com への接続性を確認します。

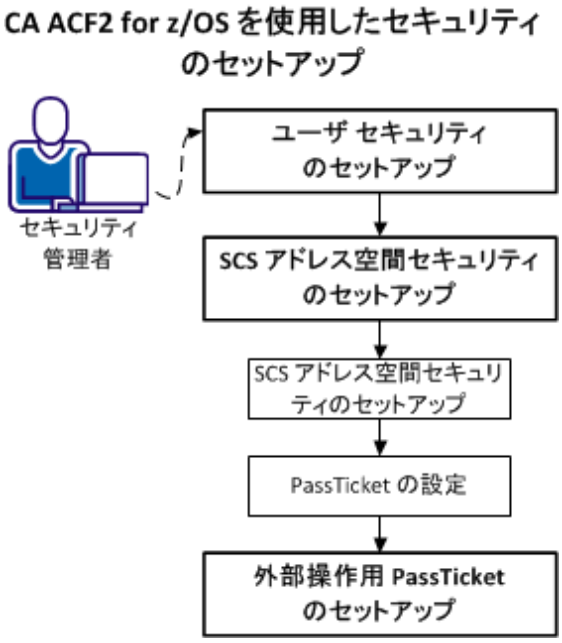
   ```
   ftp.check.host.1=orders.ca.com
   ftp.check.port.1=21
   ftp.check.host.2=products.ca.com
   ftp.check.port.2=21
   ```

4. デフォルトのプロパティ ファイルを保存します。

Prerequisite Validator ユーティリティでの作業が完了しました。 これで CA CSM のインストールを開始できます。

第 5 章: CA ACF2 for z/OS を使用した CA CSM のセキュリティのセットアップ

を使用して CA CSM のセキュリティをセットアップするには、以下のタスクを実行します CA ACF2 for z/OS:



1. ユーザのセキュリティをセットアップします (P. 42)。
2. Software Configuration Service (SCS) アドレス空間セキュリティをセットアップします (P. 47)。
   a. SCS アドレス空間セキュリティをセットアップします (P. 48)。
   b. PassTicket を設定します (P. 48)。
3. 外部操作用の PassTicket をセットアップします (P. 51)。

ユーザ セキュリティのセットアップ方法

ユーザ セキュリティをセットアップするには 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)
```

適切な CA CSM リソース プロファイルにユーザ権限を付与するには、各種役割について以下の例のコマンドを使用します。

- 管理者（P. 42）
- ユーザ（P. 44）
- 制限されたユーザ（P. 45）

例: 管理者用のセキュリティのセットアップ

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: ユーザ用のセキュリティのセットアップ

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: 制限されたユーザ用のセキュリティのセットアップ

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
```

SCS アドレス空間セキュリティをセットアップする方法

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。

セキュリティ セットアップ 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。

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。

設定 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。

PassTickets は、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 を確認するために使用されます。スターティッド タスク ID を確認することにより、リモート システムからアドレス空間への安全な接続が確立されます。

SCS アドレス空間セキュリティをセットアップするには

1. SCS アドレス空間セキュリティをセットアップします (P. 48)。
2. PassTickets を設定します (P. 48)。

SCS アドレス空間セキュリティのセットアップ

グローバル システム オプション（GSO）レコードを定義し、すべてのターゲット システム上のユーザ ID へのアクセスを許可するルールを定義します。

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別の名前が使用される場合があります。 デフォルトの SAF リソース クラス名を変更する場合は、MSMCPARM メンバ内の SAF クラス属性を更新します。

注: MSMCPARM メンバの詳細については、「*Administration Guide*」を参照してください。

次の手順に従ってください:

1. 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. ユーザ ID への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。

Pass Tickets の設定

設定 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。

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。.

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。

- 例： CA CSM アプリケーション サーバ用の PassTickets の設定（P. 49）
- 例： リモート システム上の SCS アドレス空間用の PassTickets の設定（P. 50）

例: CA CSM アプリケーション サーバ用の PassTickets 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。

次の手順に従ってください:

1. 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. MSMCAPPL PassTicket キー値への READ アクセスを有効にします。

```
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. PassTicket 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 PassTickets 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。

次の手順に従ってください:

1. 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. MSMCAPPL PassTicket キー値への READ アクセスを有効にします。

```
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. 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)
```

外部操作用の PassTicket のセットアップ方法

ユーザのパスワードを保存せずに、ユーザの代わりに CA CSM に外部操作を実行させるには、PassTicket を使用するように CA ACF2 for z/OS を設定します。

これにより、ユーザが以下のアクションを実行できます。

- 追加のユーザ ログインを必要とせずに、CA Chorus から CA CSM を起動する。

  注: CA Chorus の詳細については、CA Chorus のユーザ ドキュメントを参照してください。

- SMP/E 環境にインストールされている製品に対する自動メンテナンス更新（メンテナンスの受け入れと適用）のスケジュール。

重要: ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定するプロセスを完了するには、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。詳細については、「*保守更新を自動実行するための CA CSM の設定*」［User Documentation By Task］の下の CA CSM マニュアル選択メニューでおよび「*インストール ガイド*」を参照してください。

例: 外部操作用の PassTicket の設定

このサンプルでは、CA ACF2 for z/OS を使用して外部操作用の PassTicket を設定する方法を示します。

重要: CA CSM アプリケーション サーバ スターティッド タスク ユーザ ID の uid に RESTRICT 属性がある場合は、それに PTICKET 属性を追加します。

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

ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定する場合は、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。 詳細については、「*インストール ガイド*」および「*保守更新を自動実行するための CA CSM の設定*」を参照してください ［User Documentation By Task］の下の CA CSM マニュアル選択メニューで。

次の手順に従ってください:

1. CA CSM 接続アプリケーション セッション キーを定義します。

   ```
   SET PROFILE(PTKTDATA) DIVISION(SSIGNON)
   INSERT applid SSKEY(0123456789ABCDEF) MULT-USE
   ```

   applid

   外部操作の PassTicket 検証に使用されるアプリケーション ID を定義します。 *applid* を CA CSM applid で置換します。

   デフォルト： CHORWEBS

   SSKEY

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

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

   MULT-USE

   同じ PassTicket を複数回を再利用できるようにします。

2. CA CSM ユーザの代わりに PassTicket を生成および評価する権限を CA CSM スターティッド タスク ユーザ ID に付与します。

   ```
   SET RESOURCE(PTK)
   RECKEY IRRPTAUTH ADD(applid.- UID(uid_of_stc_userid) SERVICE(UPDATE,READ)
   ALLOW)
   ```

   uid_of_stc_userid

   CA CSM アプリケーション サーバ スターティッド タスク ユーザ ID の uid を指定します。 このユーザ ID は、任意のユーザに対して PassTicket の生成が可能である必要があります。

   デフォルト： MSMSERV

   applid

   PassTicket 検証に使用されたアプリケーション ID を定義して、サーバへの接続を認証します。 *applid* を CA CSM applid で置換します。

   デフォルト： CHORWEBS

3. 個別のユーザに CA CSM へのアクセスを許可します。

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

注: APPL クラスのタイプ コードを APL に変更するために GSO CLASMAP レコードを追加した場合は、TYPE として SAF ではなく APL を使用します。

uid_of_user

外部操作を実行する必要のあるユーザを定義します。

4. PTKTDATA レコード用のディレクトリを再構築します。

```
F ACF2,REBUILD(PTK),CLASS(P)
F ACF2,REBUILD(PTK)
```

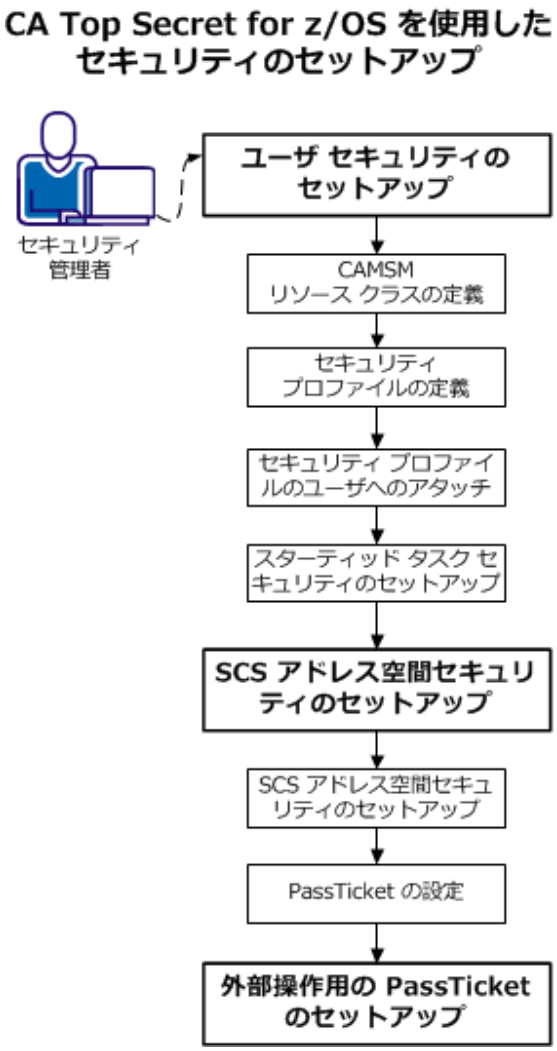
PassTicket が設定されます。

これで、CA ACF2 for z/OS を使用した CA CSM のセキュリティ セットアップは完了しました。

サイト準備が完了しました。システムが CA CSM をインストールする準備ができました。

第 6 章: CA Top Secret for z/OS を使用した CA CSM のセキュリティのセットアップ

を使用して CA CSM のセキュリティをセットアップするには、以下のタスクを実行します CA Top Secret for z/OS：



1. ユーザのセキュリティをセットアップします (P. 56)。
   a. CAMSM リソース クラスを定義します (P. 57)。
   b. セキュリティ プロファイルを定義します (P. 57)。
   c. ユーザにセキュリティ プロファイルをアタッチします (P. 59)。
   d. スターティッド タスク セキュリティをセットアップします (P. 60)。
2. Software Configuration Service (SCS) アドレス空間セキュリティをセットアップします (P. 47)。
   a. SCS アドレス空間セキュリティをセットアップします (P. 62)。
   b. PassTicket を設定します (P. 63)。
3. 外部操作用の PassTicket をセットアップします (P. 65)。

ユーザ セキュリティのセットアップ方法

CA CSM はリソース プロファイルを使用します 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別の名前が使用される場合があります。

ユーザ セキュリティをセットアップするには

1. CAMSM リソース クラスを定義します (P. 57)。
2. セキュリティ プロファイルを定義し、役割を設定します (P. 57)。
3. ユーザにプロファイルをアタッチします (P. 59)。
4. スターティッド タスク セキュリティをセットアップします (P. 60)。

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、CA Top Secret for z/OS に対するプロファイルを格納する 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別の名前が使用される場合があります。

次の手順に従ってください:

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. 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

各種役割にセキュリティ プロファイルを定義し、ユーザにプロファイルをアタッチすることができます。 各種役割について以下の例のコマンドを使用します。

- 管理者 (P. 58)
- ユーザ (P. 58)
- 制限されたユーザ (P. 59)

例: 管理者用のセキュリティのセットアップ

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: ユーザ用のセキュリティのセットアップ

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: 制限されたユーザ用のセキュリティのセットアップ

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。

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（MSMTC）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。

次の手順に従ってください:

1. 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。

SCS アドレス空間セキュリティをセットアップする方法

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。

セキュリティ セットアップは 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。

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。

設定 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。

PassTickets は、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 を確認するために使用されます。スターティッド タスク ID を確認することにより、リモート システムからアドレス空間への安全な接続が確立されます。

SCS アドレス空間セキュリティをセットアップするには

1. SCS アドレス空間セキュリティをセットアップします (P. 62)。
2. PassTickets を設定します (P. 63)。

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 で SCS アドレス空間用のセキュリティをセットアップします。

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別の名前が使用される場合があります。 デフォルトの SAF リソース クラス名を変更する場合は、MSMCPARM メンバ内の SAF クラス属性を更新します。

注: MSMCPARM メンバの詳細については、「*Administration Guide*」を参照してください。

次の手順に従ってください:

1. 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. CA CSM の部門別 ACID を作成します。

```
TSS CREATE(MSMDPT) NAME('CA CSM Department') TYPE(USER)
```

3. 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. 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. リソースがプロファイルにアクセスすることを許可します。

```
TSS PERMIT(SCSPRF1) CAMSM(SCSAS.CONNECT)   ACCESS(READ)
```

6. 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。

PassTickets を構成します。

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。

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。を設定します。

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。

- 例： CA CSM アプリケーション サーバ用の PassTickets の設定（P. 63）
- 例： リモート システム上の SCS アドレス空間用の PassTickets の設定（P. 65）

例: CA CSM アプリケーション サーバ用の PassTickets 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。

次の手順に従ってください:

1. 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. 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はこの部門に定義されます。 この所有権によって、部門管理者（またはそれ以上）は PassTicket の生成および検証の許可を定義できます。

3. CA CSM アプリケーション サーバ 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. 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。

次の手順に従ってください:

1. 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。

外部操作用の PassTicket のセットアップ方法

ユーザのパスワードを保存せずに、ユーザの代わりに CA CSM に外部操作を実行させるには、PassTicket を使用するように CA Top Secret for z/OS を設定します。

これにより、ユーザが以下のアクションを実行できます。

- 追加のユーザ ログインを必要とせずに、CA Chorus から CA CSM を起動する。

  注: CA Chorus の詳細については、CA Chorus のユーザ ドキュメントを参照してください。

- SMP/E 環境にインストールされている製品に対する自動メンテナンス更新（メンテナンスの受け入れと適用）のスケジュール。

重要: ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定するプロセスを完了するには、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。詳細については、「*保守更新を自動実行するための CA CSM の設定*」［User Documentation By Task］の下の CA CSM マニュアル選択メニューでおよび「*インストール ガイド*」を参照してください。

例: 外部操作用の PassTicket の設定

このサンプルでは、CA Top Secret for z/OS を使用して外部操作用に PassTicket を設定する方法を示します。

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

ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定する場合は、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。 詳細については、「*インストール ガイド*」および「*保守更新を自動実行するための CA CSM の設定*」を参照してください ［User Documentation By Task］の下の CA CSM マニュアル選択メニューで。

次の手順に従ってください:

1. CA CSM 接続アプリケーション セッション キーを定義します。

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

   applid

   外部操作の PassTicket 検証に使用されるアプリケーション ID を定義します。 *applid* を CA CSM applid で置換します。

   デフォルト： CHORWEBS

SESSKEY

例で表示される値とは異なる、ランダムな 16 桁の 16 進数形式のアプリケーション用暗号化キーを定義します。

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

SIGNMULTI

同じ PassTicket を複数回再利用できるようにします。

2. CA CSM スターティッド タスク ユーザ ID に、CA CSM ユーザに代わって、PassTicket の生成および評価を許可します。

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

stc_userid

CA CSM アプリケーション サーバ スターティッド タスク ユーザ ID を指定します。このユーザ ID は、任意のユーザに対して PassTicket の生成が可能である必要があります。

デフォルト： MSMSERV

applid

PassTicket 検証に使用されたアプリケーション ID を定義して、サーバへの接続を認証します。 *applid* を CA CSM applid で置換します。

デフォルト： CHORWEBS

3. 適用可能な部門に applid を追加します。

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

4. 個別のユーザに CA CSM へのアクセスを許可します。

```
TSS PERMIT(userid) APPL(applid)
```

userid

外部操作を実行する必要のあるユーザを定義します。

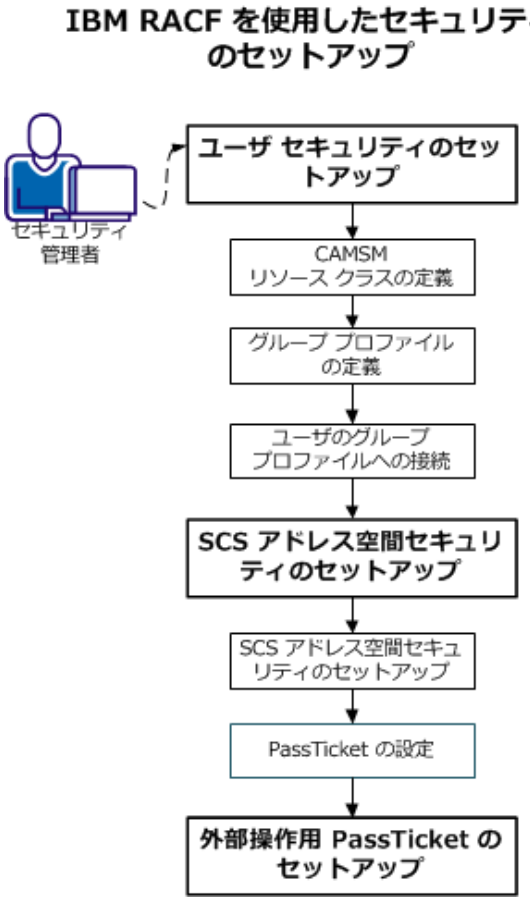
PassTicket が設定されます。

CA Top Secret for z/OS を使用した CA CSM 用のセキュリティ セットアップは完了しました。

サイト準備が完了しました。システムが CA CSM をインストールする準備ができました。

第 7 章: IBM RACF を使用した CA CSM のセキュリティのセットアップ

を使用して CA CSM のセキュリティをセットアップするには、以下のタスクを実行します IBM RACF：



1. ユーザのセキュリティをセットアップします (P. 70)。
   a. CAMSM リソース クラスを定義します (P. 71)。
   b. グループ プロファイルを定義します (P. 72)。
   c. グループ プロファイルにユーザを接続します (P. 75)。
2. Software Configuration Service (SCS) アドレス空間セキュリティをセットアップします (P. 47)。
   a. SCS アドレス空間セキュリティをセットアップします (P. 76)。
   b. PassTicket を設定します (P. 77)。
3. 外部操作用の PassTicket をセットアップします (P. 80)。

ユーザ セキュリティのセットアップ方法

CA CSM はリソース プロファイルを使用します 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別の名前が使用される場合があります。

ユーザ セキュリティをセットアップするには

1. CAMSM リソース クラスを定義します (P. 71)。
2. グループ プロファイルを定義します (P. 72)。
3. グループ プロファイルにユーザを接続します (P. 75)。

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、IBM RACF に対するプロファイルを格納する 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別の名前が使用される場合があります。

次の手順に従ってください:

1. SETROPTS 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. 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. 変更を終了させます。

   ```
   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。

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

グループ プロファイルの定義

各種役割用に適切なリソース プロファイルを含むグループ プロファイルを定義することができます。 グループ プロファイルにユーザを接続できます。

注: リソース プロファイルを使用して、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。

- 管理者 (P. 72)
- ユーザ (P. 73)
- 制限されたユーザ (P. 74)

例: 管理者用のセキュリティのセットアップ

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: ユーザ用のセキュリティのセットアップ

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: 制限されたユーザ用のセキュリティのセットアップ

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)
```

グループ プロファイルにユーザを接続する

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。

SCS アドレス空間セキュリティをセットアップする方法

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。

セキュリティ セットアップは 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。

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。

設定 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。

PassTickets は、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 を確認するために使用されます。 スターティッド タスク ID を確認することにより、リモート システムからアドレス空間への安全な接続が確立されます。

SCS アドレス空間セキュリティをセットアップするには

1. SCS アドレス空間セキュリティをセットアップします (P. 76)。
2. PassTickets を設定します (P. 77)。

SCS アドレス空間セキュリティのセットアップ

IBM RACF で SCS アドレス空間用のセキュリティをセットアップします。

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別の名前が使用される場合があります。 デフォルトの SAF リソース クラス名を変更する場合は、MSMCPARM メンバ内の SAF クラス属性を更新します。

注: MSMCPARM メンバの詳細については、「*Administration Guide*」を参照してください。

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. 71)場合、手順 1 ～ 4 をスキップできます。

次の手順に従ってください:

1. SETROPTS 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. 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. 汎用プロファイルの変更を有効にします。

   ```
   SETROPTS RACLIST(CDT) REFRESH
   ```
4. CAMSM クラスをアクティブにします。

   ```
   SETROPTS RACLIST(CAMSM) CLASSACT(CAMSM)
   ```
5. 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. ユーザにリソースを許可します。

   ```
   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、クラスを更新します。

   ```
   SETROPTS RACLIST(CAMSM) REFRESH
   ```

PassTickets を構成します。

設定 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。

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。.

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。

- 例： CA CSM アプリケーション サーバ用の PassTickets の設定（P. 78）
- 例： リモート システム上の SCS アドレス空間用の PassTickets の設定（P. 79）

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。

次の手順に従ってください:

1. PassTicket クラスをアクティブにします。

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

2. 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. 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. CA CSM アプリケーション サーバに対する 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. PTKTDATA クラスを更新します。

   ```
   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。

次の手順に従ってください:

1. PassTicket クラスをアクティブにします。

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

2. 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. 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. PTKTDATA クラスを更新します。

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

外部操作用の PassTicket のセットアップ方法

ユーザのパスワードを保存せずに、ユーザの代わりに CA CSM に外部操作を実行させるには、PassTicket を使用するよう IBM RACF を設定します。

これにより、ユーザが以下のアクションを実行できます。

- 追加のユーザ ログインを必要とせずに、CA Chorus から CA CSM を起動する。

  注: CA Chorus の詳細については、CA Chorus のユーザ ドキュメントを参照してください。

- SMP/E 環境にインストールされている製品に対する自動メンテナンス更新（メンテナンスの受け入れと適用）のスケジュール。

重要: ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定するプロセスを完了するには、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。詳細については、「*保守更新を自動実行するための CA CSM の設定*」［User Documentation By Task］の下の CA CSM マニュアル選択メニューでおよび「*インストール ガイド*」を参照してください。

例: 外部操作用の PassTicket の設定

このサンプルでは、IBM RACF を使用して外部操作用の PassTicket を設定する方法を示します。

ユーザのパスワードを保存せずに、ユーザに代わって外部操作を実行するよう CA CSM を設定する場合は、CA CSM のインストール後に CA CSM スタートアップ パラメータを更新します。 詳細については、「*インストール ガイド*」および「*保守更新を自動実行するための CA CSM の設定*」を参照してください［User Documentation By Task］の下の CA CSM マニュアル選択メニューで。

次の手順に従ってください:

1. アプリケーションの PTKTDATA クラスでアプリケーション用のプロファイルを定義し、セッション キーを指定します。

   ```
   SETROPTS CLASSACT(PTKTDATA) RACLIST(PTKTDATA)
   RDEFINE PTKTDATA applid SSIGNON(KEYMASKED(0123456789ABCDEF)) APPLDATA('NO
   REPLAY PROTECTION') UACC(NONE)
   ```

   applid

   PassTicket 検証に使用されたアプリケーション ID を定義して、サーバへの接続を認証します。 *applid* を CA CSM applid で置換します。

   デフォルト： CHORWEBS

   KEYMASKED

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

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

   APPLDATA('NO REPLAY PROTECTION')

   同じ PassTicket を複数回再利用できるようにします。

   CA CSM セッション キーが定義されます。

   注: この例では、16 進数の 16 桁のセッション キー値（8 バイトまたは 64 ビット キーを作成）を示しています。 セッション キーを定義する場合、別の値を使用します。 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、その値は保護される必要があります。

2. CA CSM スターティッド タスク ユーザ ID に、CA CSM ユーザに代わって、PassTicket の生成および評価を許可します。

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

   stc_userid

   CA CSM アプリケーション サーバ スターティッド タスク ユーザ ID を指定します。このユーザ ID は、任意のユーザに対して PassTicket の生成が可能である必要があります。

   デフォルト： MSMSERV

   applid

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

   デフォルト： CHORWEBS

3. 個別のユーザに CA CSM へのアクセスを許可します。

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

   userid

   外部操作を実行する必要のあるユーザを定義します。

4. PTKTDATA クラスを更新します。

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

   PassTicket が設定されます。

これで、IBM RACF を使用した CA CSM のセキュリティ セットアップは完了しました。

サイト準備が完了しました。システムが CA CSM をインストールする準備ができました。