CA Chorus™ Software Manager

インストール 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 Common Services for z/OS
- CA Database Management Solutions for DB2 for z/OS
- CA Datacom®/DB
- CA Datacom/MSM
- CA Disk Backup and Restore（CA Disk）
- CA Distributed Security Integration for z/OS（CA DSI Server）
- CA View®

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。

- CA CSM をインストールする方法（P. 9）： プロセスおよび手順を更新
- CA CSM をアップグレードする方法（P. 55）： プロセスおよび手順を更新
- オプション ファイル ワークシート（P. 89）：「*Administration Guide*」から移動された情報で更新
- アップグレード シナリオ（P. 121）： 付録を追加

目次

第 1 章: 概要

このガイドでは、CA CSM バージョン 6.0 のインストール方法、または CA CSM を最新のバージョンにアップグレードする方法について説明します。

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

このガイドでは、CA CSM をインストールまたはアップグレードするためにシステム プログラマが完了できるタスクの詳細について説明します。

インストール処理の実行

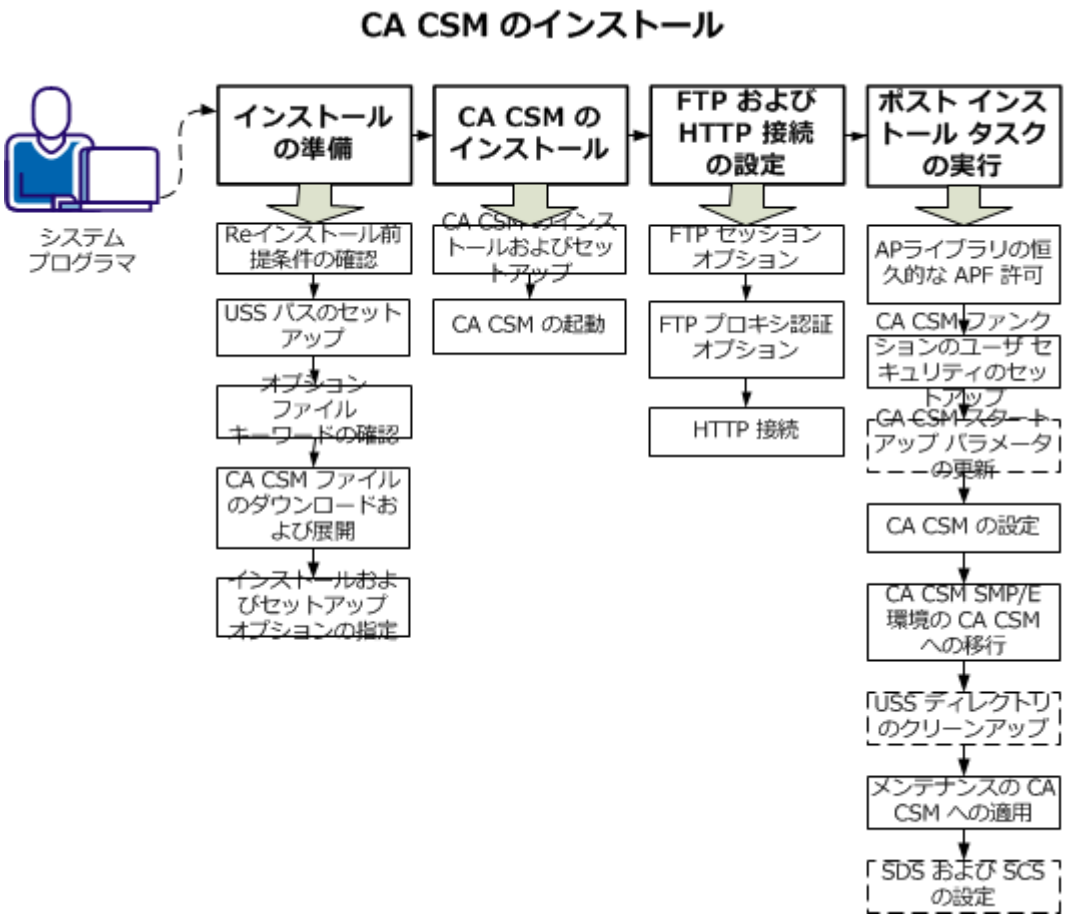
以下のアクションの*いずれか*を実行します。

- CA CSM をインストールしていない場合は、CA CSM バージョン 6.0 をインストールします (P. 9)。
- CA CSM の旧バージョンをインストールしている場合は、CA CSM をバージョン 6.0 にアップグレードします (P. 55)。

「*サイト準備ガイド*」に記載されているセキュリティ作業および前提条件作業をすべて完了するまで続行しないでください。

第 2 章: CA CSM のインストール方法

CA CSM をインストールするには、以下のタスクを実行します。



1. インストールの準備をします。
   a. インストールの前提条件を確認します (P. 11)。
   b. USS パスをセットアップします (P. 13)。
   c. オプション ファイル キーワードを確認します (P. 15)。
   d. CA CSM ファイルをダウンロードして解凍します (P. 16)。
   e. インストールおよびセットアップ オプションを指定します (P. 18)。

2. CA CSM をインストールします。
   a. CA CSM をインストールしてセットアップします (P. 22)。
   b. CA CSM を起動します (P. 31)。
3. FTP および HTTP 接続を設定します。
   a. FTP セッション オプション (P. 33)。
   b. FTP プロキシの設定 (P. 37)。
   c. HTTP プロキシの設定 (P. 44)。
4. 以下のインストール後のタスクを実行します。
   a. ライブラリを永続的に APF 許可します (P. 45)。
   b. CA CSM 機能のユーザ セキュリティをセットアップします (P. 46)。
   c. （オプション）CA CSM スタートアップ パラメータを更新します (P. 46)。
   d. CA CSM を設定します (P. 47)。
   e. CA CSM SMP/E 環境を CA CSM に移行します (P. 49)。
   f. （オプション）USS ディレクトリをクリーンアップします (P. 50)。
   g. CA CSM にメンテナンスを APPLY します (P. 52)。
   h. （オプション）SDS および SCS を設定します (P. 54)。

これらのタスクを完了した後、CA CSM のインストールを完了します。 これで、URL と適切なログイン認証情報をユーザに伝え、CA CSM の使用を開始することができます。

インストールの準備

このセクションでは、CA CSM の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。

インストールの前提条件の確認

CA CSM のインストールを開始する前に、以下のアクションを実行します。

1. Prerequisite Validator ユーティリティを使用して、前提許可をすべて満たしていることを確認します。
2. UID(0) または SUPERUSER 権限を持った userid を使用することを確認します。
3. ディスク スペース要件を確認します。
   - 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
   - TSO 領域 = 143360 KB（最低でも）
   - z/OS スペース = 2400 シリンダ
   - DASD スペース = 100 トラック
   - 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
4. ソフトウェア要件を確認します。
   - CA ソフトウェア -- システムには CA Common Services for z/OS リリース 14.1 またはバージョン 14.0 がインストールされている必要があります。
   - IBM ソフトウェア -- システムは以下の要件を満たしている必要があります。
     - z/OS の最新バージョンまたは直近の旧バージョン
     - JESINTERFACELEVEL 2 ステートメントで設定された FTP.DATA データ セットを持つ z/OS Communications Server の TCP/IP プロトコル スイート
     - SMP/E V3R5 以上
     - IBM 64-bit Java SDK 1.7 for z/OS、SR5 を使用することをお勧めします。

- 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。

5. 以下の Web サイトへの Web アクセス要件を確認します。
   - supportservices.ca.com
   - ftp.ca.com
   - ftpca.ca.com
   - scftpd.ca.com
   - ftpdownloads.ca.com
   - supportftp.ca.com
   - sdownloads.ca.com
6. 以下の z/OS OMVS 値をカスタマイズします。
   - MAXASSIZE（2147483647）
   - MAXCPUTIME（20000）
   - MAXFILEPROC（10000）
   - MAXTHREADS（1000）
   - MAXTHREADTASKS（1000）
7. 以下のシステムで、セキュリティをセットアップします。
   - CA CSM アプリケーション サーバ
   - ターゲット システム
8. アドレス空間 ACID のホーム ディレクトリを設定します。

注: 詳細については、「サイト準備ガイド」を参照してください。

USS パスのセットアップ

CA CSM は、ダウンロード、インストール、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。

MOUNT ステートメントを使用して、SYS1.PARMLIB（BPXPRM*xx*）メンバ内のシステム初期化時にマウントするファイル システムを定義することができます。

CA CSM をダウンロードしてインストールする前に、これらのファイル用にディレクトリ パスをセットアップし、またオプションでファイル システムを設定します。 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。ただし、サイトの標準で必要な場合は、単一のファイル 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できます。

最小で、775 の許可を持つ 4 つのディレクトリが必要です。 必要なスペースは 2500 シリンダです。

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、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')
```

注: 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

/*parent_path*/msmserv/

プライマリ マウント ポイントとしてユーザの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

操作中に CA CSM が割り当ておよび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。

/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共通ディレクトリで複数の CA CSM バージョン間で共有されます。

注: 同じシステム上で CA CSM の複数のインスタンスを実行する予定がある場合は、これらのインスタンス用の /mpm ディレクトリは異なっている*必要*があります。

/*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 シリンダ（プライマリ）、100 シリンダ（セカンダリ）

/*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 シリンダ（プライマリ）、100 シリンダ（セカンダリ）

/*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 シリンダ（プライマリ）、100 シリンダ（セカンダリ）

注: インストールの完了後に、このディレクトリを削除できます。

注: 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。

オプション ファイル キーワードの確認

CA CSM のインストールを開始する前に、オプション ファイル ワークシート (P. 89)を使用することをお勧めします。 オプション ファイル キーワードを確認し、それらのキーワードに対する、自社のサイトに固有の値を収集します。 インストール用のキーワードが必要になります。

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。

次の手順に従ってください:

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。

インストール用のファイルを解凍し抽出する準備ができました。

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。

次の手順に従ってください:

1. CA CSM パッケージがダウンロードされるディレクトリに移動し、パッケージを解凍します。

   ```
   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インストーラ ファイルの名前を指定します。例えば、DVD10155349E.pax.Z。

   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。

   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。

   UNZIPJCL ファイルを編集します。

   - JOB カードで、サイトの要件に従って適切な JOB ステートメント パラメータを更新します。
   - 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。
   - （オプション）ファイルで提供される手順に従ってサイトが必要とするその他の更新を行います。

   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。

インストールおよびセットアップ オプションの指定

CA CSM ファイルを抽出したディレクトリ .../MSMSetup には、MSMSetupOptionsFile.properties オプション ファイルが含まれています。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。

このファイルのコンテンツをカスタマイズして、ユーザの要件を反映する*必要があります*。 説明に「required」とマークされているオプションは必須です。

手動で (P. 18)、または ISPF UI ツールを使用して (P. 19)、インストールおよびセットアップ オプションを指定できます。

注: PTF RO60802 が適用されていて CA Allocate を使用する場合、ボリューム シリアル番号パラメータの値としてボリューム プール名を指定できます。 シリアル番号パラメータは次のとおりです： CSIVOL、TargetVOL、DlibVOL、RuntimeVOL および DatabaseVOL。

手動によるオプションの指定

インストールおよびセットアップ 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、MSMSetupOptionsFile.properties ファイル内のオプションを確認し、カスタマイズします。 たとえば、対話式システム生産性向上機能（ISPF）を使用できます。 必要に応じて、サイトの他のチーム メンバと相談して値を収集します。

ISPF UI ツールを使用したオプションの指定

CA CSM Installation ISPF UI ツールを使用できます。このツールにより、サイトの値を収集し、オプション ファイル パラメータの一部を事前入力することができます。 それでも、サイトで他のチーム メンバと相談して、これらの事前入力値を確認する必要がある場合があります。

注: サイトでストレージ管理サブシステム (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。

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。 このツールを使用して、以下のタスクを実行できます。

- 一部のパラメータのサイト値を収集します
- オプション ファイルを編集します
- 必要な USS ファイル システムを作成するための JCL を提供します

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。

次の手順に従ってください:

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/lib 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 ユーティリティを呼び出します。

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

このセクションでは、CA CSM をインストールするために実行するタスクについて説明します。

MSMSetup.sh インストール ユーティリティでは、オプション ファイル MSMSetupOptionsFile.properties のコンテンツを使用して、プロセス全体を調整します。 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。

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 ファイルを上書きするか、またはインストールを終了するかを選択するプロンプトを表示します。

キーワードが正しく設定されていない場合、MSMSetup.sh はエラーのあるオプションのリストを表示して処理を終了します。 オプションの値を修正して、MSMSetup.sh を再実行してください。

インストール プロセスが失敗した場合、失敗した時点から再開するか、またはインストール プロセスを最初から開始することができます。 以前に失敗した実行を解決する際に、オプション ファイル MSMSetupOptionsFile.properties 内のキーワードを更新した場合、インストールを最初から開始する必要があります。 そうしないと、新しいキーワードが処理されません。

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。

CA CSM のインストールおよびセットアップ

CA CSM ファイルを抽出するディレクトリ .../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 ユーティリティが含まれています。

MSMSetup.sh ユーティリティを、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。

ご使用のサイトに、PDSE に対して POU を強制実行する SMS ACS ルールがある場合、これらの設定によりインストール ジョブ CSMN6001 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。

次の手順に従ってください:

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. 16）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. 必須 USS パス（P. 13）が利用可能であることを確認します。
3. 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。

4. OMVS から 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、以下の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、以下のステートメントが真であることを確認します。

   - MSMSetupOptionsFile.properties ファイルが現在のパス内にあること。
   - オプション ファイル内の JAVAPATH パラメータ フィールドが有効であること。
   - 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、最初に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.

5. 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（特に OMVS obrowse コマンド）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。

6. 「**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 でインストール ユーティリティ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、インストール ユーティリティ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 でインストール ユーティリティを再開すると、インストールは正常に再開して完了します。

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、インストール ユーティリティ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。

7. （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。インストール ユーティリティの表示に 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、次にインストール ユーティリティを再実行します。

   Y（Yes）を入力すると、インストールは続行します。

8. 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。

9. 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、各インストール ジョブの確認を求めるプロンプトが表示されます。 その後、インストール ジョブは自動的にサブミットされます。 このモードでは、JCL スペースの割り振りを調節 (P. 74)できます。

   M

   Manual モードでは、ジョブ CSMN6001 の確認および編集を求めるプロンプトが表示されます。 ISPF 環境でのセットアップ処理の後に、JCL ライブラリから残りの各インストール ジョブを手動でサブミットします。このモードでは、JCL スペースの割り振りを調節 (P. 74)できます。

   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。
   - インストーラで必要なメモリは 17200 KB を超える場合があります。

   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）を必要な場合に表示します。

10. 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 ステートメントが編集モードで開きます。 JOB ステートメントを修正し、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。

11. 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。

12. （FTP ジョブ サブミット 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 ユーティリティを再起動します。

13. 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。

14. 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。
15. （Manual モードのみ）このサマリ レポートで指定されているように、インストール ジョブ CSMN60yy（P. 28）をサブミットします。 *yy* は、ジョブのシーケンス番号を示します。
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 (P. 45)。

    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。

    - 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。

    CA CSM が操作可能になります。

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 の内容を解凍する CSMN6001 ジョブは、インストール モードにかかわらず、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: 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。

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。

CSMN6001（CA CSM 製品の解凍）

z/OS と USS コンテンツを解凍します。

CSMN6002

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。

CSMN6003（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。

CSMN6004（CA Datacom カスタム データ セットの作成）

CA Datacom/MSM IDCUSIB をアセンブルおよびリンク エディットします。また、CUSMAC parmlib メンバを初期化します。

CSMN6005（クエリ CA Datacom PC の初期化）

CA Datacom 用にロードされた初期化済みプログラム コール（PC）のレポートに対して CA Common Services for z/OS CAIRIMU ユーティリティを実行します。

CSMN6006（CA Datacom/MSM PS ルーチンのロード）

CAIRIM モジュールを実行し、CA Datacom/MSM PC ルーチンをロードします。

CSMN6007（CA Datacom/MSM データベース システム データ セットの割り振りおよび初期化）

CA Datacom/MSM データベース システム環境データ セットの割り振りと初期化を実行します。

CSMN6008（CA Datacom MUF の開始）

CA Datacom/MSM MUF を開始します。

CSMN6009（CA Datacom/MSM 固有の製品データベースの割り振りおよび初期化）

CA Datacom/MSM 固有の製品データベースの割り振りおよび初期化を実行し、テーブルを確認します。

CSMN6010（CA Datacom MUF の停止）

CA Datacom/MSM MUF を停止します。

データベース割り振りの調整

場合によって、計画された CA CSM の使用（SCS 機能を含む）、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 スペース割り振りを JCL ジョブ ストリームに調節する必要があります。

ジョブ CSMN6009 は、CA CSM の通常使用に適した CA Datacom/MSM ディスクの初回割り振りを実行します。

MSMSetup.sh インストール ユーティリティ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、以下のアクション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。

- 製品の設定に CA CSM 機能を使用していない場合は、最低 1 つのシリンダで十分です。
- 製品の設定に少量の CA CSM 機能を使用している場合は、最低 300 のシリンダが必要です。
- 製品の設定に平均量から大量の CA CSM 機能を使用している場合は、最低 3,000 のシリンダが必要です。

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 レポートに示されます。 これらのメンバのいずれかをサブミットまたは開始して、バッチ ジョブまたはスターティッド タスクとして実行できます。

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 サーバを開始する MSMTCSRV JCL メンバ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 サーバは、768 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、SAMPLIB(MSMLIB) メンバの以下のステートメントで、Xmx 値を更新します。

```
IJO="-Xms128m -Xmx768m -Xss768m"
```

次の手順に従ってください:

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 Facility（MUF）アドレス空間が開始されます。

   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。

   ```
   DB00226I - MULTI-USER ACTIVATED XCF SUPPORT
   DB00222I - MULTI-USER ACTIVATED CCI SUPPORT
   DB00201I - MULTI-USER ENABLED, CXX=cxx_name  MUFNAME=muf_name   AD
   ```

2. 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。

   ```
   DSV00049I-CA Datacom Server Version 14.0 INITIALIZED –server_name
   ```

3. 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 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 CSM アプリケーション サーバのスタートアップ JCL パラメータは、CA サポートによって要求された場合を除いて、一切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。
- 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。

FTP および HTTP 接続の設定

このセクションでは、CA CSM のインストールに使用する FTP および HTTP 接続の設定方法について説明します。

注: 開始する前に、CA Support Online アカウントがあることを確認します。これは、［System Settings］の［Software Acquisition］ページで確認できます。

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 サーバへのログイン時に、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 *RunTimeMVSHLQPrefix*.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か空である場合、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値を使用します。

以下の例は、FTP セッション設定用のコード構文のサンプルです。

```
<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

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

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

このオプションを指定するのは、このオプションをオーバーライドする場合のみです。

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、デフォルト値が使用可能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。

ジョブ出力には、以下のテキストを含むメッセージが表示されます。

```
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。 ジョブ出力に以下のテキストを含むメッセージが表示されるようになりました。

  ```
  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、デフォルトでは以下のように true に設定されます。

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

このオプションを指定するのは、このオプションをオーバーライドする場合のみです。

重要: ファイアウォールのサポートでどうしても必要な場合を除き、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。

ファイアウォールには、PASV コマンドへの応答として FTP サーバから返される IP アドレスをインターセプト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 サーバのログに以下のメッセージが表示される場合があります。

```
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>
```

このオプションを指定するのは、このオプションをオーバーライドする場合のみです。

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 プロキシ認証方式がなくても、このデフォルト ポートを変更するファイアウォールが実装されている場合があります。

```
<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しても、このオプションによる影響はありません。

control.keep.alive.timeout

キープアライブ パケット(ノーオペレーション パケット)により、ルータが大きなファイルの転送中に一定期間非アクティブになり制御接続を閉じることが回避されます。 control.keep.alive.timeout オプションでは、キープアライブ パケットが送信される頻度（*x* 秒ごと）を指定します。

control.keep.alive.timeout オプションはデフォルトでは指定されていません（キープアライブ パケットは送信されません）。 このオプションをキープアライブ パケットを送信する必要がある頻度（秒単位）に設定できます。たとえば、ファイル ダウンロード方法によって 5 分（300 秒）ごとにキープ アライブ パケットを送信させるには、*RunTimeMVSHLQPrefix*.SAMPLIB （PASADVOP）データ セットに以下のステートメントを追加します。

```
<FTPOPTIONS>control.keep.alive.timeout=300</FTPOPTIONS>
```

詳細情報:

FTP プロキシ設定 (P. 37)

FTP プロキシ設定

FTP 基本プロキシ設定

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

- ユーザ認証情報を使用しない（P. 37）
- ユーザ認証情報を使用する（P. 38）

ユーザ認証情報を使用しない設定

次の手順に従ってください:

1. ［Settings］タブで、［System Settings］ - ［Software Acquisition］に移動します。
2. ［FTP Proxy］セクションで、［Enable Proxy Settings］チェック ボックスをオンにして、FTP プロキシ ポートおよびアドレスを指定します。
3. ［Apply］をクリックします。

   変更が有効になります。
4. ［User Settings］ - ［Software Acquisition］に移動します。
5. ［FTP Proxy］セクションで、ユーザ名およびパスワードが指定されていないことを確認します。 指定されている場合は、それらを両方とも削除して［Apply］をクリックします。

   変更が有効になります。

CA CSM は以下のコマンドを送信します。

- anonymous@ftp.ca.com パラメータを使用した FTP USER コマンド
- 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た FTP PASS コマンド

ユーザ認証情報を使用する設定

次の手順に従ってください:

1. ［Settings］タブで、［System Settings］ - ［Software Acquisition］に移動します。
2. ［FTP Proxy］セクションで、［Enable Proxy Settings］チェック ボックスをオンにして、FTP プロキシ ポートおよびアドレスを指定します。
3. ［Apply］をクリックします。

   変更が有効になります。
4. ［User Settings］ - ［Software Acquisition］に移動します。
5. ［FTP Proxy］セクションで、FTP プロキシ サーバ用のユーザ名およびパスワードを指定します。
6. ［Apply］をクリックします。

   変更が有効になります。

CA CSM は指定されたプロキシ サーバに接続し、認証およびログインのために FTP サーバに以下の一連の FTP コマンドを送信します。

```
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 の基本設定がお使いの FTP プロキシ認証方式をサポートしていない場合、FTP 拡張プロキシ設定を使用して、FTP プロキシに必要な FTP 認証およびログオンをカスタマイズできます。 これらの拡張設定は、PASADVOP という名前の PDS メンバに格納されます。 CA CSM がインストールされると、PASADVOP は *RunTimeMVSHLQPrefix*.SAMPLIB データ セットに配置されます。 PASADVOP の現在の場所を確認するには、［System Settings］ - ［Software Acquisition］ページの［FTP Proxy］-［Advanced Settings Data Set］内を参照します。このメンバには、拡張 FTP 設定を含む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、お使いの FTP および HTTP プロキシ認証方式に一致するように、ISPF エディタを使用してそれらを修正することができます。

PASADVOP メンバの例

すべての XML 要素を <ADVOPTIONS></ADVOPTIONS> のタグ間に指定する必要があります。

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

以下の例は、FTP プロキシ設定用のコード構文のサンプルです。

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

以下のキーワードを使用して、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］ページで指定された［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］ページで指定された［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。

セミコロン（;）をキーワードの後に続けます。 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。

詳細情報:

FTP 拡張設定の定義 (P. 40)

FTP 拡張設定の定義

IBM FTP プログラムを実行する z/OS でバッチ 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のサンプルに示します。

```
//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 番目の入力行を囲んでもかまいません。

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 パスワードであり、ネットワーク管理者の要求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した //INPUT DD * バッチ ジョブを使用して、特定の FTP コマンドを検索し、特定のシーケンスを確認します。

以下の SYSOUT は省略して表示しています。 リストでは、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.
```

以下のサンプルは SITE コマンドを使用する例です。 サーバではこのコマンドを使用して、ファイル転送に必須であるが、コマンドとしてプロトコルに含めるほど一般的ではない、システム固有のサービスを提供します。

```
<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 拡張プロキシ設定の制限

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、以下のサンプルがサポートされています。

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

  以下のサンプルはサポートされて*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 プロキシ設定。

サイトの設定に応じて以下のシナリオが考えられます。

HTTP プロキシ サーバを使用しない場合、HTTP 接続設定は完了しています。

認証を使用しない HTTP プロキシ サーバ

次の手順に従ってください:

1. ［Settings］タブで、［System Settings］ - ［Software Acquisition］に移動します。
2. ［HTTP Proxy］セクションで、［Enable Proxy Settings］チェック ボックスをオンにして、HTTP プロキシ ポートおよびアドレスを指定します。
3. ［Apply］をクリックします。

   変更が有効になります。
4. ［User Settings］ - ［Software Acquisition］に移動します。
5. ［HTTP Proxy］セクションで、ユーザ名およびパスワードが指定されていないことを確認します。 指定されている場合は、それらを両方とも削除して［Apply］をクリックします。

   変更が有効になります。

基本認証を使用する HTTP プロキシ サーバ

次の手順に従ってください:

1. ［Settings］タブで、［System Settings］ - ［Software Acquisition］に移動します。
2. ［HTTP Proxy］セクションで、［Enable Proxy Settings］チェック ボックスをオンにして、HTTP プロキシ ポートおよびアドレスを指定します。
3. ［Apply］をクリックします。

   変更が有効になります。
4. ［User Settings］ - ［Software Acquisition］に移動します。
5. ［HTTP Proxy］セクションで、HTTP プロキシ サーバ用のユーザ名およびパスワードを指定します。
6. ［Apply］をクリックします。

   変更が有効になります。

NTLM 認証を使用する HTTP プロキシ サーバ

次の手順に従ってください:

1. ［Settings］タブで、［System Settings］ - ［Software Acquisition］に移動します。
2. ［HTTP Proxy］セクションで、［Enable Proxy Settings］チェック ボックスをオンにして、HTTP プロキシ ポートおよびアドレスを指定します。
3. ［Apply］をクリックします。

   変更が有効になります。
4. ［User Settings］ - ［Software Acquisition］に移動します。
5. ［HTTP Proxy］セクションで、HTTP プロキシ サーバ用の NTML ドメイン、ユーザ名およびパスワードを指定します。 以下のサンプルは、NTML ドメインおよびユーザ名を指定する例です。

   ```
   mydomain¥user1
   ```
6. ［Apply］をクリックします。

   変更が有効になります。

インストール後のタスクの実行

このセクションでは、CA CSM のインストールの完了後に実行するタスクについて説明します。

永続的な APF 許可ライブラリ

MUF を APF 許可されたジョブ ステップとして確実に開始するには、MUF STEPLIB 連結に含まれるすべてのライブラリを APF 許可します。

メンバ PROG*xx* の APF リストに以下のライブラリを追加します。

- 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

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。

CA CSM 機能のユーザ セキュリティのセットアップ

CA CSM が提供するリソースおよび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。

注: CA CSM 機能のセキュリティの詳細については、「管理ガイド」を参照してください。

CA CSM スタートアップ パラメータの更新

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 スタートアップ パラメータを更新します。

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。

次の手順に従ってください:

1. PassTicket を外部操作に使用するようにセキュリティ マネージャ（CA ACF2 for z/OS、CA Top Secret for z/OS、または IBM RACF）を設定済みであることを確認してください。

   注: PassTicket の設定の詳細については、「*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「*サイト準備ガイド*」を参照してください。

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

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

   applid

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

   デフォルト： CHORWEBS

3. CA CSM アプリケーション サーバを再起動します。

   変更が有効になります。

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。

次の手順に従ってください:

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: 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。

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 に移行します。

次の手順に従ってください:

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 環境の指定を求める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 環境のゾーンがリスト表示されます。

   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、ユーザが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、下にある［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。

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。 以下のエンティティを削除できます。

- 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。

次の手順に従ってください:

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_specfic_directory

   pax コマンドで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。

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。

次の手順に従ってください:

1. CA サポート Online Web サイトの CA CSM メンテナンス情報によってソフトウェア 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 セクションに掲載されている <productname >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］をクリックします。

      メッセージは非表示になります。

   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: テスト修正の適用および CA CSM の外部でダウンロードされたメンテナンスの管理の詳細については、オンライン ヘルプ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、オンライン ヘルプを参照してください。

4. CA CSM を停止します。

   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。 ライブラリおよび USS パスは、MSMSetupOptionsFile.properties オプション ファイルの RunTimeMVSHLQPrefix と RunTimeUSSPath 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。

   CA CSM とそのメンテナンス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。

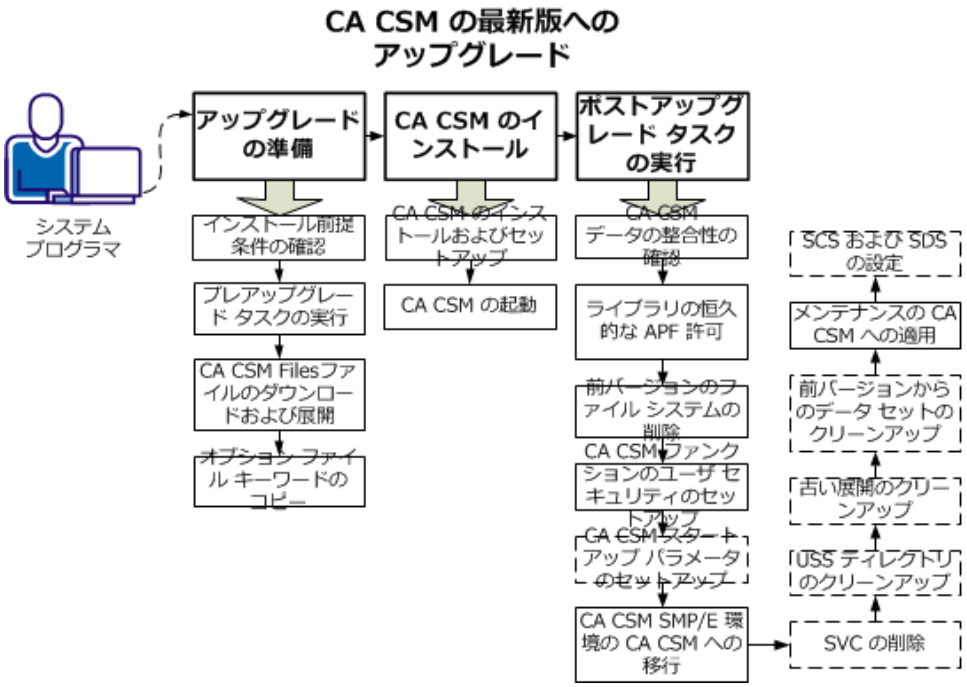
SDS および SCS の設定

CA CSM を使用して製品を展開および設定する予定の場合は、ソフトウェア展開サービス（SDS）およびソフトウェア設定サービス（SCS）を設定します。

注: SDS および SCS の構成に関する詳細については、「*CA CSM での SDS および SCS の構成*」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。

第 3 章: CA CSM をアップグレードする方法

CA CSM をアップグレードするには、以下のタスクを実行します。



1. アップグレードの準備を行います。
   a. インストールの前提条件を確認します (P. 57)。
   b. アップグレード前のタスクを実行します (P. 59)。
   c. CA CSM ファイルをダウンロードして解凍します (P. 16)。
   d. オプション ファイル キーワードをコピーします (P. 62)。
2. CA CSM をインストールします。
   a. CA CSM をインストールしてセットアップします (P. 65)。
   b. CA CSM を起動します (P. 76)。
3. アップグレード後のタスクを実行します。
   a. CA CSM のデータ整合性を確認します (P. 79)。
   b. ライブラリを永続的に APF 許可します (P. 45)。
   c. 以前のバージョンのファイル システムを削除します (P. 79)。

d. CA CSM 機能のユーザ セキュリティをセットアップします (P. 46)。

e. （オプション）CA CSM スタートアップ パラメータを更新します (P. 46)。

f. CA CSM SMP/E 環境を CA CSM に移行します (P. 49)。

g. （オプション）HTTP 接続を設定します (P. 83)。

h. （オプション） SVC を削除します (P. 83)。

i. （オプション）USS ディレクトリをクリーンアップします (P. 50)。

j. （オプション）古い展開をクリーンアップします (P. 84)。

k. （オプション）旧バージョンからのデータ セットをクリーンアップします (P. 84)。

l. CA CSM にメンテナンスを APPLY します (P. 52)。

m. （オプション）SDS および SCS を設定します (P. 54)。

これらのタスクを完了した後、最新のバージョンへの CA CSM のアップグレードを完了します。 CA CSM の使用を開始できます。

注: アップグレード プロセスは、CA CSM の旧バージョン内のデータ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。最新バージョンの CA CSM を正常に実行できる場合は、旧バージョンをこれ以上使用しないでください。

アップグレードの準備

このセクションでは、CA CSM のアップグレードの準備のために実行するタスクについて説明します。

インストールの前提条件の確認

CA CSM のアップグレードを開始する前に、以下の手順を実行します。

1. Prerequisite Validator ユーティリティを使用して、前提許可をすべて満たしていることを確認します。
2. UID(0) または SUPERUSER 権限を持った userid を使用することを確認します。
3. ディスク スペース要件を確認します。
   - 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
   - TSO 領域 = 143360 KB（最低でも）
   - z/OS スペース = 2400 シリンダ
   - DASD スペース = 100 トラック
   - 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
4. ソフトウェア要件を確認します。
   - CA ソフトウェア -- システムには CA Common Services for z/OS リリース 14.1 またはバージョン 14.0 がインストールされている必要があります。
   - IBM ソフトウェア -- システムは以下の要件を満たしている必要があります。
     - z/OS の最新バージョンまたは直近の旧バージョン
     - JESINTERFACELEVEL 2 ステートメントで設定された FTP.DATA データ セットを持つ z/OS Communications Server の TCP/IP プロトコル スイート
     - SMP/E V3R5 以上
     - IBM 64-bit Java SDK 1.7 for z/OS、SR5 を使用することをお勧めします。

- 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。

5. 以下の Web サイトへの Web アクセス要件を確認します。
   - supportservices.ca.com
   - ftp.ca.com
   - ftpca.ca.com
   - scftpd.ca.com
   - ftpdownloads.ca.com
   - supportftp.ca.com
   - sdownloads.ca.com
6. 以下の z/OS OMVS 値をカスタマイズします。
   - MAXASSIZE（2147483647）
   - MAXCPUTIME（20000）
   - MAXFILEPROC（10000）
   - MAXTHREADS（1000）
   - MAXTHREADTASKS（1000）
7. 以下のシステムで、セキュリティをセットアップします。
   - CA CSM アプリケーション サーバ
   - ターゲット システム
8. アドレス空間 ACID のホーム ディレクトリを設定します。

注: 詳細については、「サイト準備ガイド」を参照してください。

アップグレード前のタスクの実行

CA CSM のアップグレードを開始する前に、以下のタスクを実行します。

1. CA CSM の Web ベース インターフェースで、［Settings］タブに移動し、［System Settings］の下の［Mount Point Management］をクリックし、［Unmount at Shutdown］を選択します。［Apply］をクリックします。
2. 以前の CA CSM のバージョンの CA CSM アドレス空間をシャットダウンします。
3. ファイル システムの設定に応じて、以下のいずれかのオプションを選択します。
   - 単一の CA CSM ファイル システムの設定の場合
     a. 以前のバージョンの CA CSM ファイル システムをマウント解除します。
     b. CA CSM ファイル システムを作成し、以前のバージョンのマウント ポイント（つまり、/u/users/msmserv）でそれをマウントします。
     c. 次のディレクトリを作成します： mpm、msm、msmruntime、msminstall。
     d. 以前のバージョン用の新しいマウント ポイントを作成します: /u/users/msmserv/*previous_version_number*。 パス ノード *previous_version_number* は、英字 1 文字に 2 桁の数字が続く形式（たとえば V50）である必要があります。
     e. 手順 3d で作成したこの新しいマウント ポイントに CA CSM の以前のバージョンのファイル システムをマウントします。
     f. /u/users/msmserv/*previous_version_number*/msm/CEGPHFS/MSMSetupOptionsFile.properties オプション ファイル内の次のパラメータを編集して、新しいバージョンのディレクトリ パスをポイントします。

     ```
     MSMPATH=/u/users/msmserv/previous_version_number/msm
     RunTimeUSSPath=/u/users/msmserv/previous_version_number/msmruntime
     ```

   - 複数の CA CSM ファイル システムの設定の場合
     a. 次の新しいバージョンのディレクトリを作成します。

     ```
     /u/users/msmserv/version_number/msm
     /u/users/msmserv/version_number/msmruntime
     /u/users/msmserv/version_number/msminstall
     ```

b. 次の新しいバージョンのファイル システムを作成します：msm、msmruntime、および msminstall。

c. ファイル システムを新しいバージョンのディレクトリ、/u/users/msmserv/*version_number*/msm、/u/users/msmserv/*version_number*/msmruntime、および /u/users/msmserv/*version_number*/msminstall でマウントします。

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。

次の手順に従ってください:

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。

インストール用のファイルを解凍し抽出する準備ができました。

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。

次の手順に従ってください:

1. CA CSM パッケージがダウンロードされるディレクトリに移動し、パッケージを解凍します。

   ```
   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インストーラ ファイルの名前を指定します。例えば、DVD10155349E.pax.Z。

   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。

   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。

   UNZIPJCL ファイルを編集します。

   - JOB カードで、サイトの要件に従って適切な JOB ステートメント パラメータを更新します。
   - 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。
- （オプション）ファイルで提供される手順に従ってサイトが必要とするその他の更新を行います。

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。

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。

重要: MSMSetupOptionsFile.properties オプション ファイル内のキーワード PreviousRelease.MSMPATH が、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ていることを確認してください。 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。

次の手順に従ってください:

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。

3. 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。

   現在のバージョンのオプション ファイル内にあるキーワード MVSHFSDsnPrefix および MountPath が、旧バージョンのオプション ファイル内にある値と同じであることを確認してください。 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。 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。

オプション ファイル キーワードの更新

MSMSetup ディレクトリにある MSMSetupOptionsFile.properties オプション ファイルが更新されました。

追加キーワード

以下のキーワードが追加されました。

Applid

CA Datacom/MSM アプリケーションに対して CA Datacom Server を識別するために使用する名前を指定します。

PROTOCOL

CA CSM と CA Datacom Server 間のデータ転送に使用する通信プロトコルを指定します。

TCPIP_HOST

CA Datacom Server が CA CSM からの受信 TCP/IP データ トラフィックをリスンするホスト名または IP アドレスを指定します。

TCPIP_PORT

CA Datacom Server が CA CSM からの 受信 TCP/IP データ トラフィックをリスンするポート番号を指定します。

TCPIP_CONNECT_QUEUE

CA Datacom Server がすぐに処理できる CA CSM からの TCP/IP データベース リクエストの数を指定します。

削除されたキーワード

以下のキーワードが削除されました。

- MUFName
- SVCNO
- InstallSVC
- C370linkEditDSN

他の更新

CA CSM では、CA Datacom/MSM Multi-User Facility CXX 名は、最大 7 文字の一意の英数字である必要があります。 この名前は CXXNAME キーワードとして定義されます。 サイトが複数の MUF を実行をしている場合は、CA CSM の MUF CXX 名が他のすべての MUF とは異なることを確認します。

詳細情報:

オプション ファイル ワークシート (P. 89)

CA CSM のインストール

このセクションでは、CA CSM の最新バージョンにアップグレードするために実行するタスクについて説明します。

MSMSetup.sh インストール ユーティリティでは、オプション ファイル MSMSetupOptionsFile.properties のコンテンツを使用して、プロセス全体を調整します。 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。

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。

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 ファイルを上書きするか、またはインストールを終了するかを選択するプロンプトを表示します。

ユーティリティは、SMP/E のインストール、ランタイム、およびデータベースのパラメータについて、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。

また、ユーティリティは、マウント ポイント マネージャのデータ セット HLQ およびパス名が、新しいオプション ファイルの値と同じであることを確認します。

キーワードが正しく設定されていない場合、MSMSetup.sh はエラーのあるオプションのリストを表示して処理を終了します。 オプションの値を修正して、MSMSetup.sh を再実行してください。

インストール プロセスが失敗した場合、失敗した時点から再開するか、またはインストール プロセスを最初から開始することができます。 以前に失敗した実行を解決する際に、オプション ファイル MSMSetupOptionsFile.properties 内のキーワードを更新した場合、インストールを最初から開始する必要があります。 そうしないと、新しいキーワードが処理されません。

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。

CA CSM のインストールおよびセットアップ

CA CSM ファイルを抽出するディレクトリ .../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 ユーティリティが含まれています。

MSMSetup.sh インストール ユーティリティを、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。

ご使用のサイトに、PDSE に対して POU を強制実行する SMS ACS ルールがある場合、これらの設定によりインストール ジョブ CSMU*xx*01 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。

次の手順に従ってください:

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. 16) 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 ファイルをコピー (P. 62) して、確実にサイトの要件に従います。

3. 必須 USS パス (P. 59) 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. 以前の CA CSM バージョンが実行されていないことを確認します。

6. OMVS から 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、以下の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、以下のステートメントが真であることを確認します。

   - MSMSetupOptionsFile.properties ファイルが現在のパス内にあること。
   - オプション ファイル内の JAVAPATH パラメータ フィールドが有効であること。
   - 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、最初にユーザの入力が要求されます。 出力は、Msminstaller*Logyyyy-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.

7. 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（特に OMVS obrowse コマンド）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。

8. 「**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 でインストール ユーティリティ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、インストール ユーティリティ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 でインストール ユーティリティを再開すると、インストールは正常に再開して完了します。

   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、インストール ユーティリティ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。

9. （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。インストール ユーティリティの表示に 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、次にインストール ユーティリティを再実行します。

   Y（Yes）を入力すると、インストールは続行します。

10. 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。

11. 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、各インストール ジョブの確認を求めるプロンプトが表示されます。 その後、インストール ジョブは自動的にサブミットされます。 このモードでは、JCL スペースの割り振りを調節 (P. 74)できます。

    M

    Manual モードでは、ジョブ CSMU*xx*01 の確認および編集を求めるプロンプトが表示されます。 ISPF 環境でのセットアップ処理の後に、JCL ライブラリから残りの各インストール ジョブを手動でサブミットします。このモードでは、JCL スペースの割り振りを調節 (P. 74)できます。

    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。
    - インストーラで必要なメモリは 17200 KB を超える場合があります。

    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）を必要な場合に表示します。

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 ステートメントが編集モードで開きます。 JOB ステートメントを修正し、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。

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. （FTP ジョブ サブミット 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 ユーティリティを再起動します。

15. ユーティリティが以前の CA CSM バージョンの CA Datacom/MSM データベースをバックアップして、CA CSM 用の SMP/E 環境を作成し、CA CSM コンポーネントをセットアップすることを確認します。

    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。

16. 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。

17. （Manual モードのみ）このサマリ レポートで指定されているように、インストール ジョブ CSMUxxyy (P. 72)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。

18. 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 (P. 45)。

    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。

19. 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。

20. 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。

    - 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。

21. CA CSM を起動します。

    CA CSM が操作可能になります。

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 (P. 75)することもできます。

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 の内容を解凍する CSMU*xx*01 ジョブは、インストール モードにかかわらず、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*02 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。 CA CSM の旧バージョンからアップグレードする場合、インストーラは Automatic および Review モードでインストール ジョブ CSMU*xx*02 をサブミットします。 Manual モードでは、インストーラが完了した後に、ジョブ CSMU*xx*02 をサブミットする必要があります。
- 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。

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、カスタマイズされた 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 CSM R5.1 からアップグレードしている場合、ジョブ番号は CSMU5101、CSMU5102、...、CSMU5110 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（CA CSM 製品の解凍）

z/OS と USS コンテンツを解凍します。

CSMU*xx*02（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*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 カスタム データ セットの作成）

CA Datacom/MSM IDCUSIB をアセンブルおよびリンク エディットします。また、CUSMAC parmlib メンバを初期化します。

CSMU*xx*05（クエリ CA Datacom PC の初期化）

CA Datacom 用にロードされた初期化済みプログラム コール（PC）のレポートに対して CA Common Services for z/OS CAIRIMU ユーティリティを実行します。

CSMN*xx*06（CA Datacom/MSM PS ルーチンのロード）

CAIRIM モジュールを実行し、CA Datacom/MSM PC ルーチンをロードします。

CSMU*xx*07（CA Datacom/MSM データベース システム データ セットの割り振りおよび初期化）

CA Datacom/MSM データベース システム環境データ セットの割り振りと初期化を実行します。

CSMU*xx*08（CA Datacom MUF の開始）

CA Datacom/MSM MUF を開始します。

CSMU*xx*09（CA Datacom/MSM に固有の製品データベースを定義および初期化し、変換済みデータを移行）

CA Datacom/MSM に固有の製品データベースを定義および初期化し、変換済みデータを移行します。

CSMU*xx*10（CA Datacom MUF の停止）

CA Datacom/MSM MUF を停止します。

データベース割り振りの調整

場合によって、計画された CA CSM の使用（SCS 機能を含む）、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 スペース割り振りを JCL ジョブ ストリームに調節する必要があります。

ジョブ CSMU*xx*09 は、CA CSM の通常使用に適した 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.

新しいディスク割り振りが、現在使用中の CA Datacom/MSM ディスク領域と少なくとも等しいことを確認します。

MSMSetup.sh インストール ユーティリティ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、以下のアクション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。

- 製品の設定に CA CSM 機能を使用していない場合は、最低 1 つのシリンダで十分です。
- 製品の設定に少量の CA CSM 機能を使用している場合は、最低 300 のシリンダが必要です。
- 製品の設定に平均量から大量の CA CSM 機能を使用している場合は、最低 3,000 のシリンダが必要です。

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。

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 レポートに示されます。 これらのメンバのいずれかをサブミットまたは開始して、バッチ ジョブまたはスターティッド タスクとして実行できます。

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 サーバを開始する MSMTCSRV JCL メンバ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 サーバは、768 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、SAMPLIB(MSMLIB) メンバの以下のステートメントで、Xmx 値を更新します。

```
IJO="-Xms128m -Xmx768m -Xss768m"
```

次の手順に従ってください:

1. CA CSM の以前のバージョンのアドレス空間が停止していることを確認します。
2. 旧バージョンの APLROOT、SCROOT および LJWK マウント ポイントをマウント解除します。
3. （オプション）以前のバージョンの CA CSM の開始プロシージャをバックアップし、最新バージョンのプロシージャを本番環境のライブラリにコピーします。

4. 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 Facility（MUF）アドレス空間が開始されます。

   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。

   ```
   DB00226I - MULTI-USER ACTIVATED XCF SUPPORT
   DB00222I - MULTI-USER ACTIVATED CCI SUPPORT
   DB00201I - MULTI-USER ENABLED, CXX=cxx_name  MUFNAME=muf_name   AD
   ```

5. 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。

   ```
   DSV00049I-CA Datacom Server Version 14.0 INITIALIZED –server_name
   ```

6. 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 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。

7. 初めて CA CSM を正常に起動した後で、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。

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 CSM アプリケーション サーバのスタートアップ JCL パラメータは、CA サポートによって要求された場合を除いて、一切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。
- 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。

アップグレード後のタスクの実行

このセクションでは、CA CSM の最新バージョンにアップグレードした後に実行するタスクについて説明します。

CA CSM のデータ整合性の確認

CA CSM を最新のバージョンにアップグレードした後、以前のバージョンにあったデータが正しく、破損していないことを確認します。

データの整合性を確認するには、Web ベース インターフェースを使用して CA CSM の最新のバージョンにログインし、以前の CA CSM のデータがすべて CA CSM の最新バージョンで利用可能であることを確認します。

永続的な APF 許可ライブラリ

MUF を APF 許可されたジョブ ステップとして確実に開始するには、MUF STEPLIB 連結に含まれるすべてのライブラリを APF 許可します。

メンバ PROG*xx* の APF リストに以下のライブラリを追加します。

- 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

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。

以前のバージョンのファイル システムの削除

CA CSM バージョン 6.0 では 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。

CA CSM 機能のユーザ セキュリティのセットアップ

CA CSM が提供するリソースおよび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。

注: CA CSM 機能のセキュリティの詳細については、「管理ガイド」を参照してください。

CA CSM スタートアップ パラメータの更新

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 スタートアップ パラメータを更新します。

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。

次の手順に従ってください:

1. PassTicket を外部操作に使用するようにセキュリティ マネージャ（CA ACF2 for z/OS、CA Top Secret for z/OS、または IBM RACF）を設定済みであることを確認してください。

   注: PassTicket の設定の詳細については、「*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「*サイト準備ガイド*」を参照してください。

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

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

   applid

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

   デフォルト： CHORWEBS

3. CA CSM アプリケーション サーバを再起動します。

   変更が有効になります。

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 に移行します。

次の手順に従ってください:

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 環境の指定を求める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 環境のゾーンがリスト表示されます。

   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、ユーザが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、下にある［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。

あるいは、最新バージョンの CA CSM から旧バージョンの CA CSM SMP/E 環境を削除することもできます。

注: 旧バージョンの CA CSM SMP/E 環境の削除、または SMP/E 環境の削除の詳細については、オンライン ヘルプを参照してください。

SVC の削除

CA CSM バージョン 6.0 では、CA Datacom/MSM スーパーバイザ コール（SVC）は必要ありません。 ご使用のサイトで任意の CA Datacom インスタンス用の SVC を必要としない場合、アンインストールすることができます。

HTTP 接続の設定

CA CSM の旧バージョンで NTLM 認証を使用する HTTP プロキシ サーバを使用した場合は、すべてのユーザのユーザ名に NTLM ドメインが含まれていることを確認します。 ［Settings］タブの［User Settings］ -［Software Acquisition］ページ (P. 45)で確認します。 以下に例を示します。

```
mydomain¥user1
```

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。 以下のエンティティを削除できます。

- 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。

次の手順に従ってください:

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_specfic_directory

   pax コマンドで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。

古い展開のクリーンアップ

CA CSM リリース 5.1 より古いバージョンからアップグレードする場合、古い展開スナップショットをクリーンアップして、ご使用のシステム上の DASD スペースを解放してください。

注: 展開スナップショットのクリーンアップに関する詳細については、オンライン ヘルプを参照してください。

旧バージョンからのデータ セットをクリーン アップします。

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、システムから削除することができます。

- 旧バージョンが単一のファイル システムにインストールされます。msminstall、msm、msmruntime、msmtmp および 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 システムにインストールされます。msminstall、msm、msmruntime、msmtmp および 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。 その後、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。

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。

次の手順に従ってください:

1. CA サポート Online Web サイトの CA CSM メンテナンス情報によってソフトウェア 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 セクションに掲載されている <productname >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］をクリックします。

      メッセージは非表示になります。

   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: テスト修正の適用および CA CSM の外部でダウンロードされたメンテナンスの管理の詳細については、オンライン ヘルプ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、オンライン ヘルプを参照してください。

4. CA CSM を停止します。

   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。 ライブラリおよび USS パスは、MSMSetupOptionsFile.properties オプション ファイルの RunTimeMVSHLQPrefix と RunTimeUSSPath 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。

   CA CSM とそのメンテナンス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。

SDS および SCS の設定

CA CSM を使用して製品を展開および設定する予定の場合は、ソフトウェア展開サービス（SDS）およびソフトウェア設定サービス（SCS）を設定します。

注: SDS および SCS の構成に関する詳細については、「*CA CSM での SDS および SCS の構成*」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。

付録 A: オプション ファイル ワークシート

オプション ファイル キーワードを確認し、組織で使用する必要な値を収集します。

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

使用する値：

_____

JAVAPATH

IBM 64 ビット Java SDK for z/OS コンポーネントのパスを指定します。

注: 31 ビット Java SDK はサポートされていません。

例： /sys/java64bt/v7r0m0/usr/lpp/java/J7.0_64

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。

デフォルト： CAI

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。 TargetHLQ の値は RunTimeMVSHLQPrefix および DatabaseHLQ とは異なる必要があります。

デフォルト： CSIHLQ の値

使用する値：

_____

TargetZoneName

SMP/E 環境のターゲット ゾーン名を指定します。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。

制限： 7 文字以下

デフォルト： CAIT0

使用する値：

_____

DlibHLQ

配布データ セットのプレフィクスを指定します。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。 DlibHLQ の値は RunTimeMVSHLQPrefix および DatabaseHLQ とは異なる必要があります。

デフォルト： CSIHLQ の値

使用する値：

_____

DlibZoneName

SMP/E 環境の配布ゾーン名を指定します。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。

制限： 7 文字以下

デフォルト： CAID0

使用する値：

MSMPATH

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。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。

例： /u/users/msmserv/v60/msm

使用する値：

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。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。RunTimeMVSHLQPrefix の値は TargetHLQ および DlibHLQ とは異なる必要があります。

例： CAI.CSM60.RT

使用する値：

RunTimeUSSPath

CA CSM ランタイムが使用する 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。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。

例： /u/users/msmserv/v60/msmruntime

使用する値：

_____

DatabaseHLQ

インストール プロセス中に作成される CA Datacom データ セットのプレフィクスを指定します。

最新の CA CSM バージョンにアップグレードしている場合は、前の CA CSM バージョンの値とは別のこのキーワードに対する一意の値を指定します。DatabaseHLQ の値は TargetHLQ および DlibHLQ とは異なる必要があります。CA Datacom/AD Version 14 以降では、CXX 名はデータ セット名の一部になっています。

制限： 27 文字以下

デフォルト： RunTimeMVSHLQPrefix の値

使用する値：

_____

CXXNAME

CA Datacom/MSM データベース CXX ディレクトリ 用の一意の識別子の名前を指定します。

CXXNAME に対して指定する値は、最後の修飾子ノードの次としてすべての CA Datacom/MSM データベース データ セット名の一部になります。

制限： 1 ～ 7 の英数文字

デフォルト： CSM60

注: CXXNAME の命名規則の詳細については、「*CA Datacom/DB DBUTILTY Reference Guide for z/OS*」を参照してください。

使用する値：

_____

ServerName

CA Datacom/MSM サーバの名前を指定します。 CA Datacom はこの名前を使用して、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 マルチユーザ機能（MUF）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。

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に失敗しないよう保証することができます。 最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

制限： 1 ～ 32 の英数文字

デフォルト： CSM60、または CXXNAME キーワードに指定した値

注: デフォルト値を維持することをお勧めします。

例： CSMV6SRV

注: ServerName の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

Applid

CA Datacom/MSM アプリケーションに対して CA Datacom Server を識別するために使用する名前を指定します。

制限： 1 ～ 20 の英数文字

デフォルト： CSM60、または CXXNAME キーワードに指定した値

注: Applid の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

PROTOCOL

CA CSM と CA Datacom Server 間のデータ転送に使用する通信プロトコルを指定します。 データ伝送は、システム上の CAICCI インターフェースを介して、またはポート番号上でリスンするより単純な TCP/IP インターフェースを使用して実行できます。 ある環境においては、TCP/IP サービスにより CA CSM 操作中に、よりよいパフォーマンスが提供される場合があります。

以下のオプションがあります。

CCI

CAICCI プロトコルが使用されます。

BOTH

TCP/IP プロトコルが使用されます。 このオプションを使用する場合は、値を指定するか、またはキーワード TCPIP_HOST、TCPIP_PORT および TCPIP_CONNECT_QUEUE に対するデフォルト値を使用します。

デフォルト： CCI

注: PROTOCOL の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

TCPIP_HOST

（PROTOCOL=BOTH の場合にのみ適用されます）CA Datacom Server が CA CSM からの受信 TCP/IP データ トラフィックをリスンするホスト名または IP アドレスを指定します。

PROTOCOL=CCI の場合、このキーワードは無視されます。

デフォルト： 現在のシステムの IP アドレス

注: TCPIP_HOST の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

TCPIP_PORT

（PROTOCOL=BOTH の場合にのみ適用されます）CA Datacom Server が CA CSM からの 受信 TCP/IP データ トラフィックをリスンするポート番号を指定します。このポート割り当ては、ユーザの環境でその他の TCP/IP サービスには使用されないようにしてください。

PROTOCOL=CCI の場合、このキーワードは無視されます。

制限： 1024 ～ 65535

デフォルト： 5465

注: TCPIP_PORT の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

TCPIP_CONNECT_QUEUE

（PROTOCOL=BOTH の場合にのみ適用されます）CA Datacom Server がすぐに処理できる CA CSM からの TCP/IP データベース リクエストの数を指定します。

PROTOCOL=CCI の場合、このキーワードは無視されます。

制限： 1 ～ 9999

デフォルト： 250

注: デフォルト値を維持することをお勧めします。

注: TCPIP_CONNECT_QUEUE の詳細については、「*CA Datacom Server User Guide*」を参照してください。

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 22120

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 22130

使用する値：

_____

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。 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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 22140

使用する値：

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 22150

使用する値：

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。

重要: 最新の CA CSM バージョンにアップグレードしている場合は、このキーワードの値がアップグレード前のバージョンと同じであることを確認します。

デフォルト： OMVSUSR.CAMSM

使用する値：

MountPath

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: 最新の CA CSM バージョンにアップグレードしている場合は、このキーワードの値がアップグレード前のバージョンと同じであることを確認します。

例： /u/users/msmserv/mpm

使用する値：

---

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

以下のオプションがあります。

Y

CA CSM はスタートアップ中にファイル システムを自動的にマウントします。

N

CA CSM を開始する前にファイル システムを手動でマウントする必要があります。

デフォルト： Y

使用する値：

USSFileSystemType

一時ファイル用に HFS ファイル システムまたは zFS ファイル システムのどちらを使用するかを指定します。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

以下のオプションがあります。

- HFS
- ZFS

zFS ファイル システムを使用することをお勧めします。 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* ガイド」を参照してください。

使用する値：

_____

mpmAllocation

（オプション）［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ためのストレージ基本設定を指定します。

以下のオプションがあります。

- SMS
- NONSMS

デフォルト： SMS

使用する値：

_____

mpmStorageClass

（オプション。mpmAllocation=SMS の場合にのみ適用）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。このキーワードは製品のインストールおよびメンテナンス時に使用されます。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 空白

例： SYSSC

使用する値：

_____

mpmMgmtClas

（オプション。mpmAllocation=SMS の場合にのみ適用）［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 管理クラスを指定します。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

使用する値：

_____

mpmDataClas

（オプション。mpmAllocation=SMS の場合にのみ適用）［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。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： SYSDC

使用する値：

_____

mpmUnit

（オプション。mpmAllocation=NONSMS の場合にのみ適用）［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。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： 3390

使用する値：

---

mpmVolumeSer

（オプション。mpmAllocation=NONSMS の場合にのみ適用）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。この値は製品のインストールおよびメンテナンス時に使用されます。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 空白

例： DASD01

使用する値：

TempSpaceCleanupInterval

CA CSM が一時ワークスペースをクリーンアップする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。

制限： 0、60 ～ 1440

デフォルト： 60

使用する値：

---

sisExecutorOutputStorclas

（オプション）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のインストール中に、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。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

デフォルト： 空白

例： SYSSC

使用する値：

_____

sisExecutorOutputUnit

（オプション）プログラムを実行したデータ セットが、一時データとして使用する DASD のタイプを指定します。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： 3390

使用する値：

_____

sisExecutorOutputVolser

（オプション）プログラムを実行したデータ セットが一時データとして使用する、DASD のボリューム シリアル番号を指定します。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： DASD01

使用する値：

_____

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 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（SMS または NONSMS 管理）を指定します。

デフォルトのサイト設定を使用するには、このキーワードを空白のままにするか、またはアスタリスク（*）を指定します。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

例： WRK001

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

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。

例： CAI.CSM.V60.TEMP

使用する値：

_____

DATASETSUFFIX

製品の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 セット名が以下の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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

制限： 4 文字

デフォルト： CASC

例

```
MVSHFSDsnPrefix = OMVSUSR.CACSM
DATASETSUFFIX = CASC
完全なデータ セット名： OMVSUSR.CACSM.CASC1234
```

使用する値：

_____

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。

制限： 24 文字以下

例： PUBLIC

使用する値：

_____

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。

最新の CA CSM バージョンにアップグレードしている場合は、このキーワードを前の CA CSM バージョンで使用していた同じ値に設定できます。

以下のオプションがあります。

Y

SAF セキュリティを有効にします。

N

SAF セキュリティを無効にします。

デフォルト： N

使用する値：

---

safResourceClass

（safSecurity=Y の場合にのみ適用）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

使用する値：

---

sysTaskDeleteOverrideEnabled

（safSecurity=N の場合にのみ適用）CA CSM ユーザにタスクの削除を許可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

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

使用する値：

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。デフォルト値を使用することをお勧めします。

以下のオプションがあります。

Y

HASH 検証を有効にします。

N

HASH 検証を無効にします。

デフォルト： Y

使用する値：

ICSF

（HASH=Y で、システムに Integrated Cryptographic Services Facility（ICSF）がインストールされている場合にのみ適用）HASH 検証に ICSF 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。

Y

HASH 検証に ICSF を使用します。

N

HASH 検証に ICSF を使用しません。

デフォルト： Y

使用する値：

SMPCPATH

（HASH=Y と ICSF=N 両方の場合にのみ適用）SMP/E Java アプリケーション クラスへのパスを指定します。

デフォルト： /usr/lpp/smp/classes

使用する値：

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。

SMS デフォルト ボリュームを使用する場合は、アスタリスク（*）を指定します。 CSIVOL 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（新規インストールの場合は CSMN6001、アップグレードの場合は CSMU*xx*01）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。 そのケースでは、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。

PTF RO60802 が適用されていて CA Allocate を使用する場合、このキーワードの値としてボリューム プール名を指定できます。

デフォルト： *

使用する値：

_____

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。

SMS デフォルト ボリュームを使用する場合は、アスタリスク（*）を指定します。

PTF RO60802 が適用されていて CA Allocate を使用する場合、このキーワードの値としてボリューム プール名を指定できます。

デフォルト： CSIVOL の値

使用する値：

_____

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。

SMS デフォルト ボリュームを使用する場合は、アスタリスク（*）を指定します。

PTF RO60802 が適用されていて CA Allocate を使用する場合、このキーワードの値としてボリューム プール名を指定できます。

デフォルト： CSIVOL の値

使用する値：

_____

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。

SMS デフォルト ボリュームを使用する場合は、アスタリスク（*）を指定します。

PTF RO60802 が適用されていて CA Allocate を使用する場合、このキーワードの値としてボリューム プール名を指定できます。

デフォルト： *

使用する値：

_____

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。

SMS デフォルト ボリュームを使用する場合は、アスタリスク（*）を指定します。

PTF RO60802 が適用されていて CA Allocate を使用する場合、このキーワードの値としてボリューム プール名を指定できます。

デフォルト： RuntimeVOL の値

使用する値：

_____

TEMPUNIT

一時作業データ セット用のデバイス名を指定します。

デフォルト： SYSDA

使用する値：

STORAGE

SMP/E 一時データセットに対するストレージ基本設定を指定します。

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。

以下のオプションがあります。

- SMS
- NONSMS

デフォルト： SMS

使用する値：

MGMTCLAS

（STORAGE=SMS の場合にのみ適用）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。

ACS 設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： SYSMC

使用する値：

STORCLAS

（STORAGE=SMS の場合にのみ適用）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。

ACS 設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： SYSSC

使用する値：

_____

DATACLAS

（STORAGE=SMS の場合にのみ適用）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。

ACS 設定を使用するには、このキーワードを空白のままにします。

デフォルト： 空白

例： SYSDC

使用する値：

_____

UNIT

（STORAGE=NONSMS の場合にのみ適用）一時 SMP/E データ セットを配置する DASD のタイプを指定します。

例： 3390

使用する値：

_____

VOLUME

（STORAGE=NONSMS の場合にのみ適用）一時 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。

例： DASD01

使用する値：

_____

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。

デフォルト： SYS1.SIEALNKE

使用する値：

CCSdsn

CAIRIM モジュールが存在する 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。

例： CAI.CAW0LOAD

使用する値：

CCScaipdsedsn

LIBCCI および LIBCCI6E ロード モジュールが存在する CA Common Services for z/OS CAW0PLD データ セットの完全修飾名を指定します。

例： CAI.CAW0PLD

使用する値：

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

使用する値：

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
```

例: A91SENF

使用する値：

_____

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。

以下のオプションがあります。

- JES2
- JES3

デフォルト： JES2

使用する値：

_____

JOBNAME

（オプション）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： S が追加された CA CSM セットアップ ユーティリティの実行ユーザ ID。

使用する値：

_____

ACCOUNT

（オプション）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。

デフォルト： 空白

例： ’1234,dept01,NY NY’

使用する値：

クラス

（オプション）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

使用する値：

MSGCLASS

（オプション）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

使用する値：

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。

デフォルト： *

使用する値：

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。

以下のオプションがあります。

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。 サイトが静的 APF 形式で設定されている場合は、動的形式に変更されます。また、データ セットは APF リストに追加されます。

N

CA Datacom/MSM データ セットを手動で追加する必要があります。インストール後にサマリ レポートを確認して、インストールを完了するためのこれらの手動手順を実行します。

デフォルト： Y

使用する値：

_____

HOSTNAME

（オプション）システムのホスト名または IP アドレスを指定します。

デフォルト： 現在の LPAR の IP アドレス

例： 110.64.255.255

使用する値：

_____

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

使用する値：

_____

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

使用する値：

_____

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

使用する値：

_____

TCPdsn

TCPIP.DATA データ セットの名前を指定します。このオプションは、サイト TCP/IP スタック設定に応じて必要になる場合があります。

このキーワードを空白のままにすることができます。 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。

デフォルト： VTAM.TCPIP.TCPIP.DATA

使用する値：

_____

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管理されており、z/OS リンクリスト（LNKLST）にあります。

デフォルト： TCPIP.SEZATCP

使用する値：

_____

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

使用する値：

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

使用する値：

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

使用する値：

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

使用する値：

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

使用する値：

---

job.submission.mode

CA CSM インストーラが、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 コードの検証を行うために使用するメソッドを指定します。

以下のオプションがあります。

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。 このモードは完全に自動化されます。

注: この方法を使用することをお勧めします。

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 モードのみで実行されます。1 つのジョブ（新規インストールの場合）または 2 つのジョブ（アップグレードの場合）のみがサブミットされます。ユーティリティが完了した後、手動でインストール ジョブの残りをサブミットする必要があります。

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。

デフォルト： FTP

使用する値：

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

使用する値：

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

使用する値：

---

msm.ssl.secure.connection.enable

（オプション）CA CSM が HTTP または HTTPS 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。

Y

HTTPS を使用します。

N

HTTP を使用します。

デフォルト： N

使用する値：

---

first.name.and.last.name

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）URL ドメイン名を指定します。

デフォルト： 空白

例： www.your.domain

使用する値：

---

organization.name

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）組織名を指定します。

デフォルト： 空白

使用する値：

---

organization.unit.name

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）組織ユニット名を指定します。

デフォルト： 空白

使用する値：

_____

city

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）市町村名を指定します。

デフォルト： 空白

使用する値：

_____

state

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）州名を指定します。

デフォルト： 空白

使用する値：

_____

country.code

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）州名を指定します。

デフォルト： 空白

使用する値：

_____

keystore.location

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）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。

注: 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。

デフォルト： RunTimeUSSPath に作成されます

使用する値：

_____

validity.period

（オプション。msm.ssl.secure.connection.enable=Y の場合にのみ適用）生成されたキーストア証明書の有効期間を日数単位で指定します。

デフォルト： 365

使用する値：

_____

PreviousRelease.MSMPATH

（最新の CA CSM バージョンにアップグレードしている場合にのみ適用）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 CA CSM バージョンの CEGPHFS ディレクトリで利用可能な MSMSummaryReport.txt またはオプション ファイルを参照してください。

例： /u/users/msmserv/msm

付録 B: 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 R4.1 以前のバージョンから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 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。

- 12 の旧バージョンの CA Datacom/MSM データベース テーブルがコピーおよび再構成され、データがあれば変換されます。
- 7 つの既存の CA Datacom/MSM テーブルが削除されます。
- 18 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。

- 8 の旧バージョンの CA Datacom/MSM データベース テーブルがコピーおよび再構成され、データがあれば変換されます。
- 8 つの既存の CA Datacom/MSM テーブルが削除されます。
- 18 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 CSM R5.1 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。

- 10 の旧バージョンの CA Datacom/MSM データベース テーブルがコピーおよび再構成され、データがあれば変換されます。
- 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。
- 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。