CA Chorus™ Software Manager

管理ガイド

バージョン 06.0.00、第 1 版

ca technologies

このドキュメント（組み込みヘルプ システムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本 CA 株式会社（以下「CA」）により随時、変更または撤回されることがあります。 本ドキュメントは、CA が知的財産権を有する機密情報であり、CA の事前の書面による承諾を受けずに本書の全部または一部を複写、譲渡、変更、開示、修正、複製することはできません。

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

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

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

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

本書の制作者は CA および CA Inc. です。

「制限された権利」のもとでの提供: アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2014 CA. All rights reserved. 本書に記載されたすべての商標、商号、サービス・マークおよびロゴは、それぞれの各社に帰属します。

CA Technologies 製品リファレンス

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

- CA Chorus™ Software Manager（CA CSM）
- CA ACF2™ for z/OS
- CA Allocate™ DASD Space and Placement（CA Allocate）
- CA Auditor for z/OS
- CA Chorus™
- 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 Easytrieve® Simplified Design System（CA Easytrieve）
- CA Panvalet®（CA Panvalet）
- CA PDSMAN® PDS Library Management（PDSMAN）
- CA SMF Director
- CA SYSVIEW
- CA Top Secret® for z/OS
- 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。

- 「はじめに (P. 13)」：章を再構成し、古くなった情報を削除して、概要トピックを「*リリース ノート*」に移動
- 「インストールの準備」：章を削除し、情報を「*インストール ガイド*」および「*サイト準備ガイド*」に移動
- 「CA CSM のインストールとセットアップ」：章を削除し、情報を「*インストール ガイド*」および「*サイト準備ガイド*」に移動
- 「インストール後のタスク」：章を削除し、情報を「*インストール ガイド*」および「*サイト準備ガイド*」に移動
- 「CA CSM のセットアップ (P. 23)」：削除されたセクションから既存のトピックを引き継ぎ、新しい章を追加
- 「CA CSM のセットアップ (P. 29)」：削除されたセクションから既存のトピックを引き継ぎ、新しい章を追加
- 「CA CSM の設定」-「UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 29)」：別のセキュリティ システムに関連するトピックにメッセージ EDC5129I に関する情報を追加
- 「CA CSM の設定」-「別の LPAR での CA CSM の実行 (P. 36)」：新規トピックを追加
- 「CA CSM の設定」-「FTP および HTTP 接続の設定」-「新規インストール用の FTP 接続の設定」-「HTTP プロキシ設定の構成 (52P. , 51P.)」：セクションを複数のトピックに分割して再構成
- 「CA CSM の設定」-「HTTPS を使用するための CA CSM の設定 (P. 52)」：セクションを再構成し、外部セキュリティ マネージャに格納された証明書を使用した HTTPS の有効化、および HTTP をオーバーライドするための CA CSM の設定についての新規トピックを追加
- 「CA CSM の設定」-「MUF スタートアップの IEC988I メッセージの有効化」：情報が古いため、トピックを削除
- 「CA CSM の設定」-「展開用のセキュア FTP 接続のセットアップ (P. 62)」：新規トピックを追加

- 「CA CSM の保守 (P. 65)」 : 削除されたセクションから既存のトピックを引き継ぎ、新しい章を追加
- 「CA CSM の保守」 - 「CA CSM の停止 (P. 77)」 : z/OS、CA SYSVIEW および SDSF のコマンドに関する情報で手順 2 を更新
- 「データベース管理」 : 章を削除し、情報をシナリオ「*CA CSM データベースの管理*」に移動
- 「SCS アドレス空間管理 (P. 85)」 : 再構成し、章を簡略化
- 「CA CSM の実装およびステータス」 -「実装チェックリスト」 -「セキュリティ管理者 (P. 124)」 : IBM RACF プログラム制御用のデータセットを更新し、CA SAF HFS セキュリティを使用した場合のアクセス権に関する情報を追加
- 「CAMSM> の実装およびステータス」 -「実装チェックリスト」 -「オプション ファイル キーワード」 : セクションを削除し、「*インストール ガイド*」に内容を移動
- 「CA CSM の実装およびステータス」 -「CA CSM ソフトウェア展開生成手順エンティティ (P. 128)」 : SMPJHOME 用の例を更新
- 「CA CSM の実装およびステータス」 - 「CA CSM 機能のセキュリティ」 - 「リソース プロファイル (P. 141)」 : SYSREG.@PROFILE.UPDATE.*systemname* プロファイルを追加
- 「CA CSM の実装およびステータス」 - 「DBINIT および DBUPDATE の設定 (P. 149)」 : HTTP を含めないように PASAdvancedSettingsMember の説明を更新
- 「外部インターフェース (P. 173)」 - 新しい付録（以前「ユーザ ガイド」にあった）を追加
- 「トラブルシューティング」 - 「Microsoft Internet Explorer 8 の実行速度の低下 (P. 197)」 : 新規トピックを追加
- 「トラブルシューティング」 -「SMP/E 環境がツリーに表示されない (P. 200)」 : 新規トピックを追加

目次

第 1 章: はじめに 13

CA CSM の動作の仕組み 13
CA CSM 運用アーキテクチャ図 16
ネットワーク フロー 20

第 2 章: CA CSM のセットアップ 23

ユーザのセキュリティ セットアップ 23
ユーザの USS 許可のセットアップ 23
CA CSM 機能のユーザ セキュリティのセットアップ 25
CA CSM 関連セキュリティ ID - OMVS セグメントおよびホーム ディレクトリ 27

第 3 章: CA CSM の設定 29

UID(0) を使用しない CA CSM ユーザ ID の設定 29
前提条件 30
CA Top Secret for z/OS に対して UID(0) を使用しない CA CSM ユーザ ID の設定 30
CA ACF2 for z/OS に対して UID(0) を使用しない CA CSM ユーザ ID の設定 32
IBM RACF に対して UID(0) を使用しない CA CSM ユーザ ID の設定 34
別の LPAR での CA CSM の実行 36
CA CSM の［Notice and Consent］バナーの有効化 38
CA CSM アプリケーション サーバのマルチ TCP/IP スタック環境の TCP/IP スタックへのバインド 39
FTP および HTTP 接続の設定 40
既存インストール用の FTP 接続の設定 40
既存インストール用の HTTP 接続の設定 40
新規インストール用の FTP 接続の設定 41
HTTP プロキシ設定の構成 51
HTTPS を使用するための CA CSM の設定 52
USS ファイルに格納された証明書を使用した HTTPS の有効化 53
外部セキュリティ マネージャに格納された証明書を使用した HTTPS の有効化 55
HTTP をオーバーライドする HTTPS の設定 57
CA CSM ファイル システムのマウント パラメータの設定 58
MUF メッセージ出力の設定 61
出力記述子の設定 61
展開用のセキュア FTP 接続のセットアップ 62

gskkyman データベースからの証明書のエクスポート 63
SAMPLIB(MSMLIB) メンバのリモート システムの SYSUT3 および SYSUT4 用の UNIT パラメータの指定 64

第 4 章: CA CSM のメンテナンス 65

CA CSM の起動 65
メンテナンス 67
CA CSM へのメンテナンスの APPLY 68
メンテナンスが理由で CA CSM が失敗する場合のリカバリ 72
CA CSM のバックアップおよびディザスタ リカバリ 73
CA CSM のバックアップ方法 74
バックアップからの CA CSM のリカバリ方法 77
CA CSM の停止 77

第 5 章: 追加の管理タスク 79

現在のユーザへのメッセージ送信 79
ユーザにメッセージを送信するサンプル JCL 81
実行中タスクの確認 83
Java ホーム ディレクトリの再割り当て 83

第 6 章: SCS アドレス空間管理 85

SCS アドレス空間操作の考慮事項 85
許可プログラム機能 86
補助アドレス空間 87
暗号化通信 88
SSL 伝送サポートの実装 88
System SSL 使用のセットアップ 93
AT-TLS 伝送サポートの実装 94
オペレータ通信インターフェース 94
SCS アドレス空間オペレータ コマンド 95
SCS アドレス空間 ASID オペレータ入力の例 103
SCS アドレス空間のデータ空間識別子の入力 104
JCL EXEC ステートメント PARM キーワードおよび START コマンド パラメータ 105
パラメータ ライブラリ 107
MSMCPARM メンバ 108
SCS アドレス空間メッセージ ログ（SCSLOG） 115
syslog デーモンの設定 116
syslog デーモン設定変更の有効化 118

汎用トレース機能 119
GTF の開始 119
GTF の停止 121

付録 A: CA CSM の実装およびステータス 123

実装チェックリスト 123
ネットワーク管理者 123
Security Administrator 124
USS 管理者 127
システム プログラマ 127
CA CSM ソフトウェア展開生成手順エンティティ 128
USS ファイル システム 128
CA CSM のインストールとセットアップ 129
CA CSM のダウンロード 129
CA CSM の起動 129
一時ファイル システムの使用 130
ソフトウェア カタログ 131
CA CSM データ セットとファイル システム 132
CA CSM データ セット タイプ 132
CA CSM ファイル システム 133
CA Common Services コンポーネントの要件 137
FMID 137
CAICCI のセットアップ 139
CA CSM 機能のセキュリティ 139
リソース名 139
リソース プロファイル 141
SMP/E 処理中の SAF チェック 147
SMP/E 環境の移行 147
基本製品のインストール 147
メンテナンス管理 148
展開 149
DBINIT および DBUPDATE の設定 149
DBUPDATE DD を使用した値の修正 158
ASCII 設定ファイル 158
ASCII ファイルの編集 158
context.xml パラメータ 159
ジョブ割り当て詳細 161
CSMaxx01 162
CSMaxx04 165

CSMaxx07 165
CSMN6009 166
CSMU5102 167
CSMU5002 169
CSMU4102 170
CSMUxx09 172

付録 B: 外部インターフェース 173

CA CSM の外部でタスクを実行 173
MVS MODIFY コマンド 173
コマンド検証 180
ログ メッセージ 180

付録 C: トラブルシューティング 183

SMP/E 内のメンテナンスの ACCEPT または RESTORE が失敗する 183
CA CSM アドレス空間が正しく機能しない 185
MSMLOG ファイルの CA CSM アプリケーション サーバ エラー 186
MSMLOG ファイルの起動時の CA CSM アプリケーション サーバ エラー 187
CA CSM アプリケーション サーバのタイムアウト 188
SAF セキュリティが有効な状態での CA CSM の開始に失敗する 189
CA CSM が例外で失敗する 191
［Tasks］タブの［Delete Task］ボタンが無効 192
SMPOUT の展開で、GIMUNZIP メッセージが表示される 193
一時データ セットおよび RELFILE データ セットの動的割り当てエラー 193
ソフトウェア インストール中の MACLIB ライブラリの動的な割り当てが失敗する 194
不正な製品更新成功ステータス 195
GIM54701S ** ALLOCATION FAILED FOR SMPJHOME 195
SMP/E が生成したデータ セットで I/O エラーが発生する 196
Microsoft Internet Explorer 8 の実行速度の低下 197
MSMTC が RC=100 で失敗する 197
CA CSM にアクセスするとき、No Ticket エラー メッセージが表示される 198
製品リストの更新が失敗する 199
SMP/E の APPLY または ACCEPT 処理が失敗する 199
SMP/E 環境がツリーに表示されない 200
SMP/E 環境の移行が、SMP/E Environment Migration ウィザードの［SMP/E Environment Functions］手順で失敗する 201

用語集 203

第 1 章: はじめに

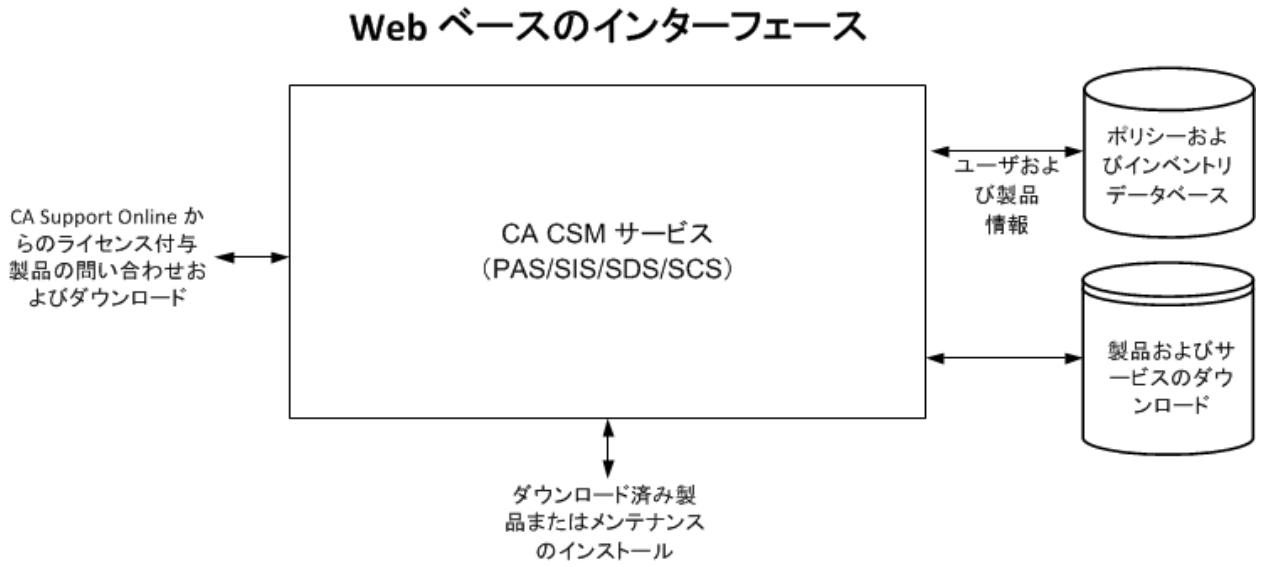
このセクションには、以下のトピックが含まれています。

CA CSM の動作の仕組み (P. 13)
ネットワーク フロー (P. 20)

CA CSM の動作の仕組み

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

以下の図は、主要なコンポーネントとデータ フローについて示しています。



CA CSM には以下の主要なコンポーネントがあります。

CA CSM サービス

以下のサービスを提供します。

製品取得サービス（PAS）

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

ソフトウェア インストール サービス（SIS）

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

Software Deployment Service（SDS）

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

ソフトウェア構成サービス（SCS）

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

データベース

CA CSM が使用する情報を格納します。

ポリシー

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

インベントリ

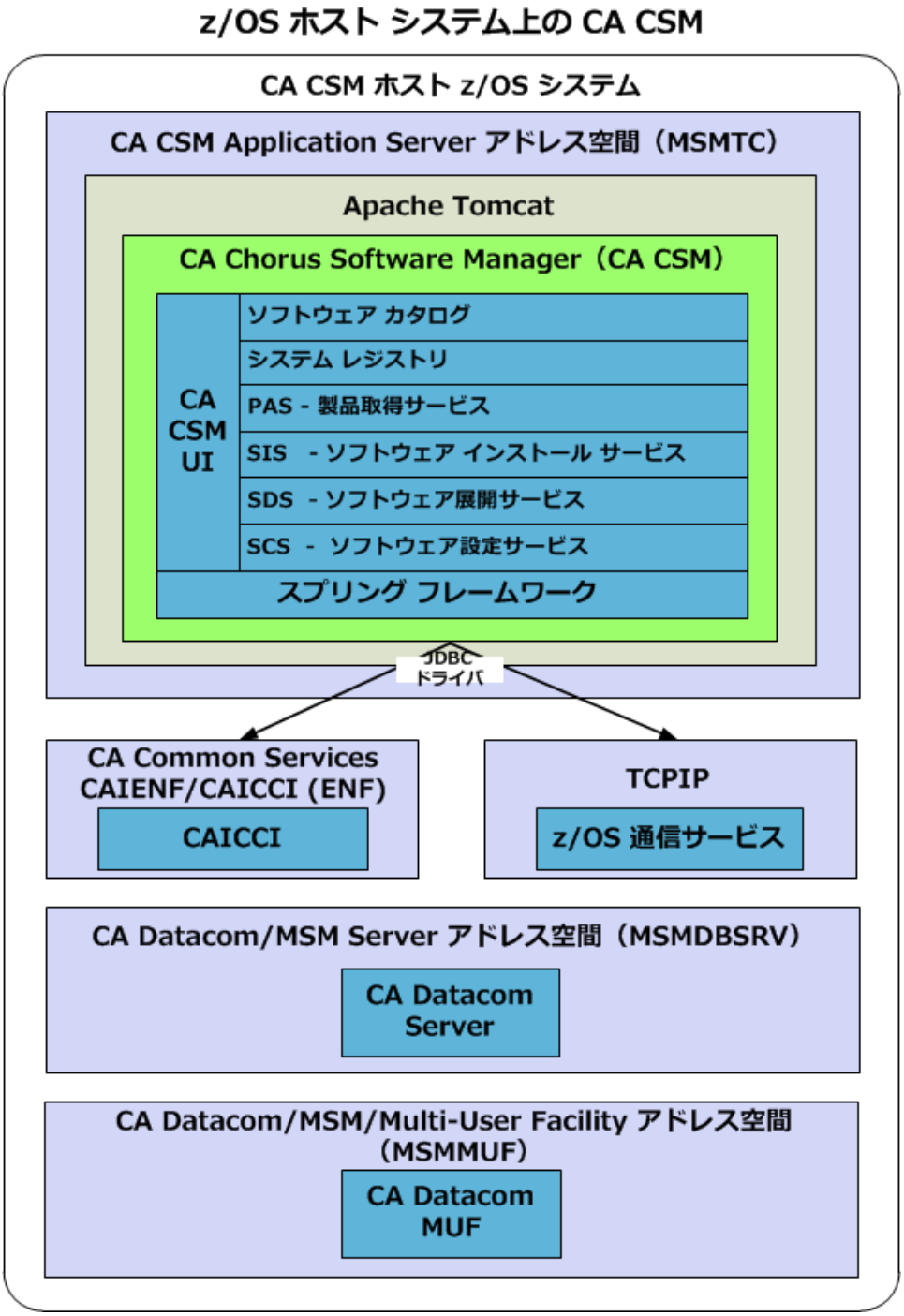
ユーザにライセンスが付与された CA Technologies メインフレーム製品に関する情報を格納します。

Web ベース インターフェース

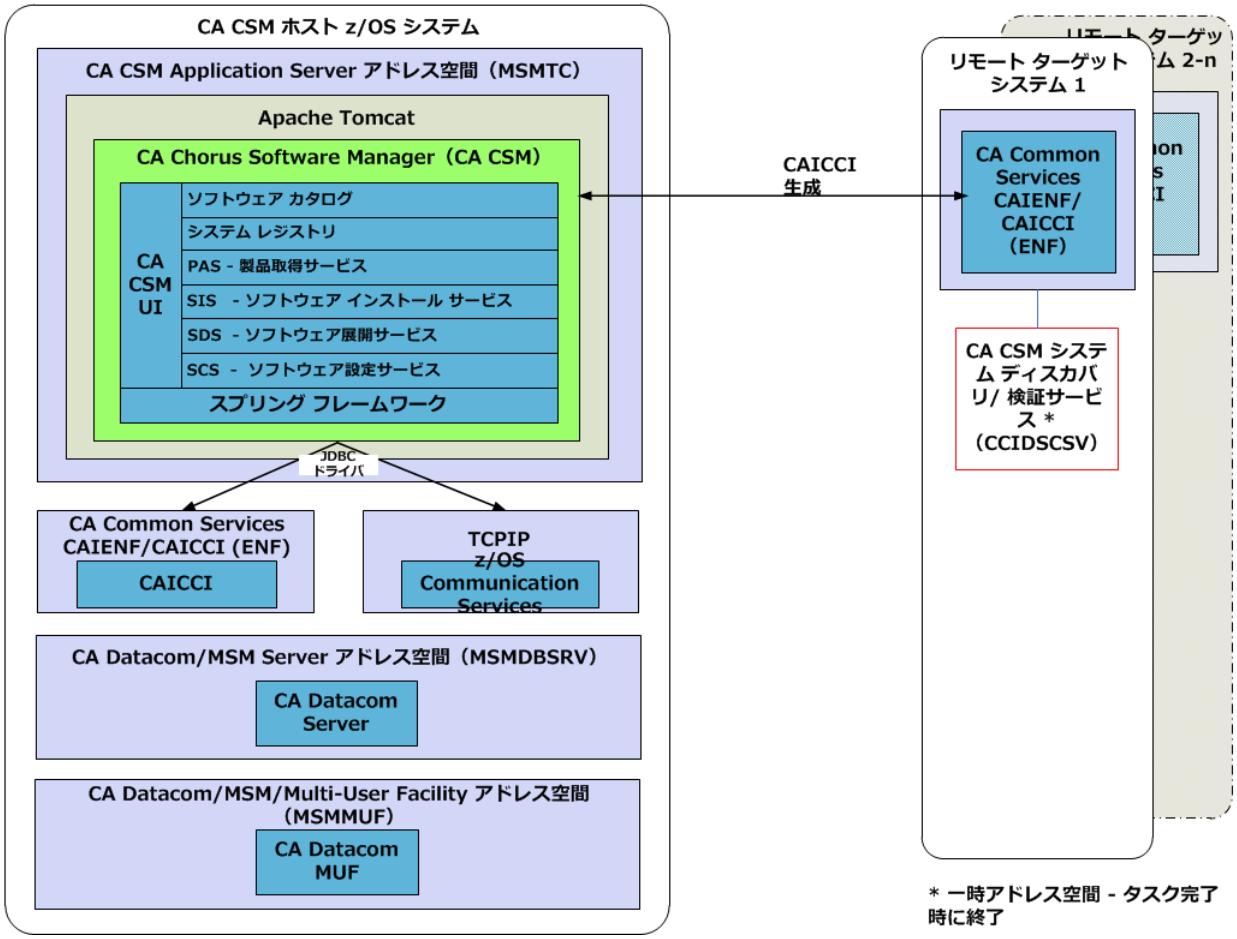
CA CSM カタログから取得した、CA Technologies メインフレーム製品の取得、インストール、メンテナンス、展開、設定、および SMP/E 環境の管理ができるようになります。 Web ベース インターフェースにはオンライン ヘルプが用意されており、CA CSM の使用方法に関する情報が提供されます。

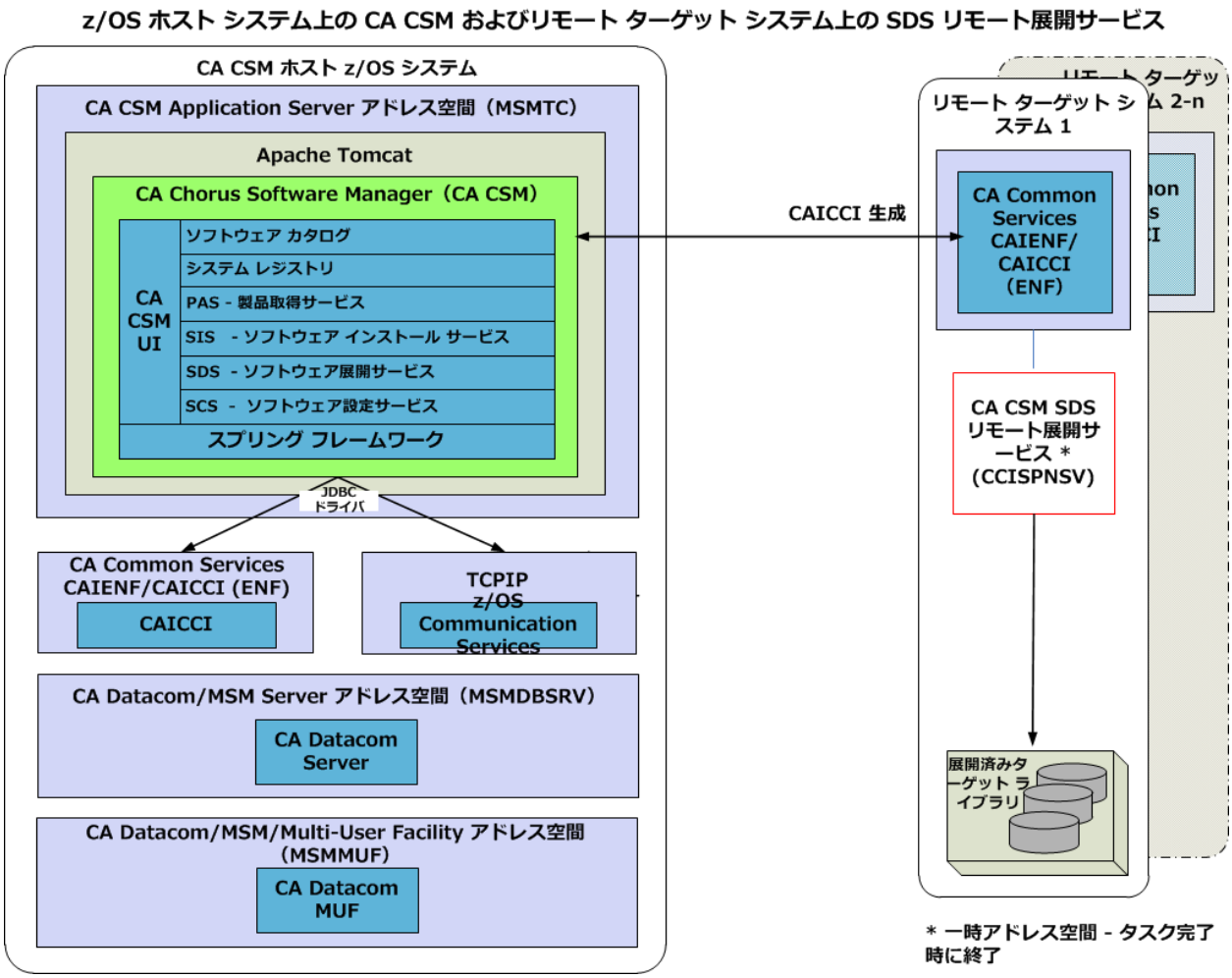
CA CSM 運用アーキテクチャ図

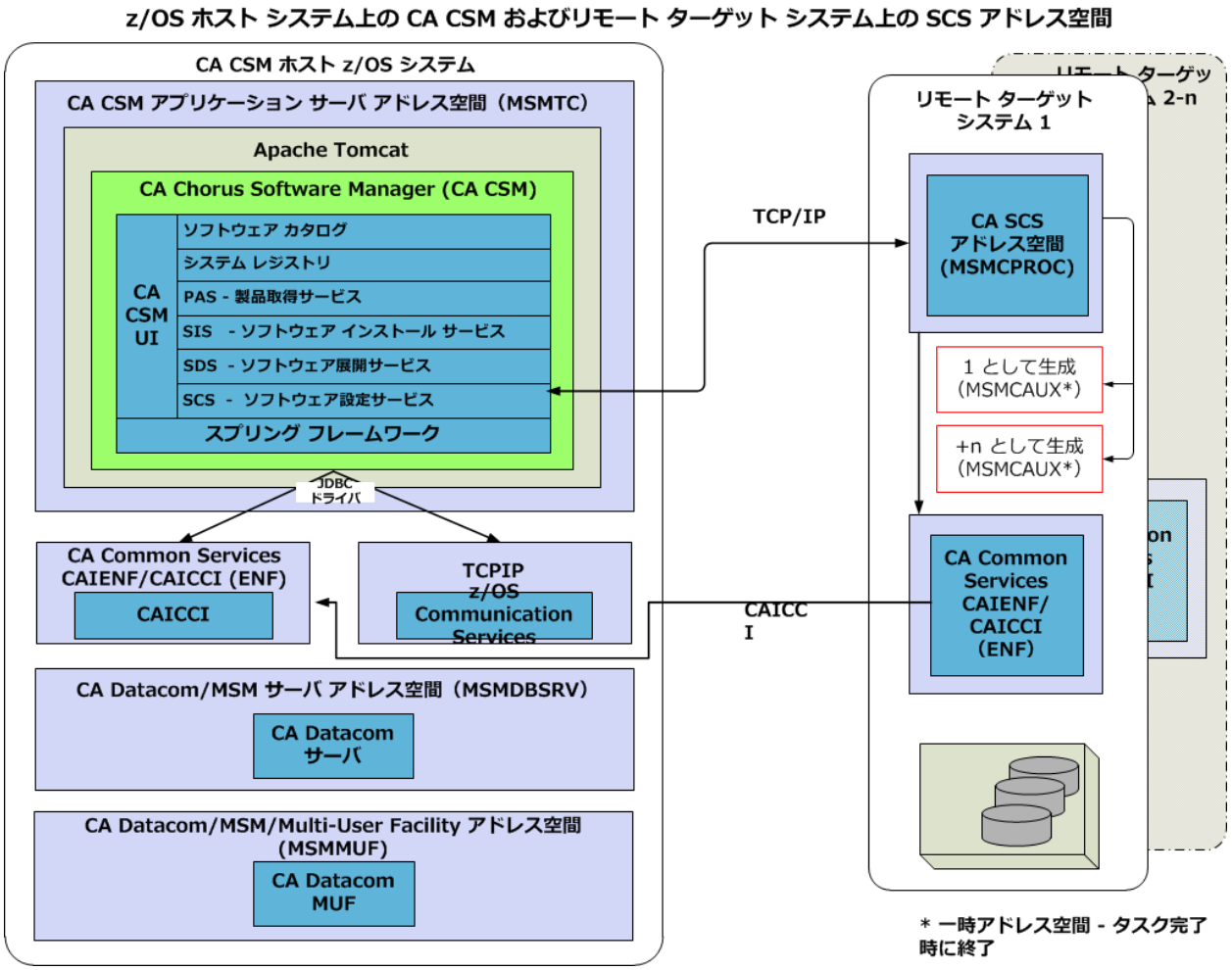
以下の図は、リモートおよびローカル システム上の CA Common Services for z/OS を使用した CA CSM の設定を示します。

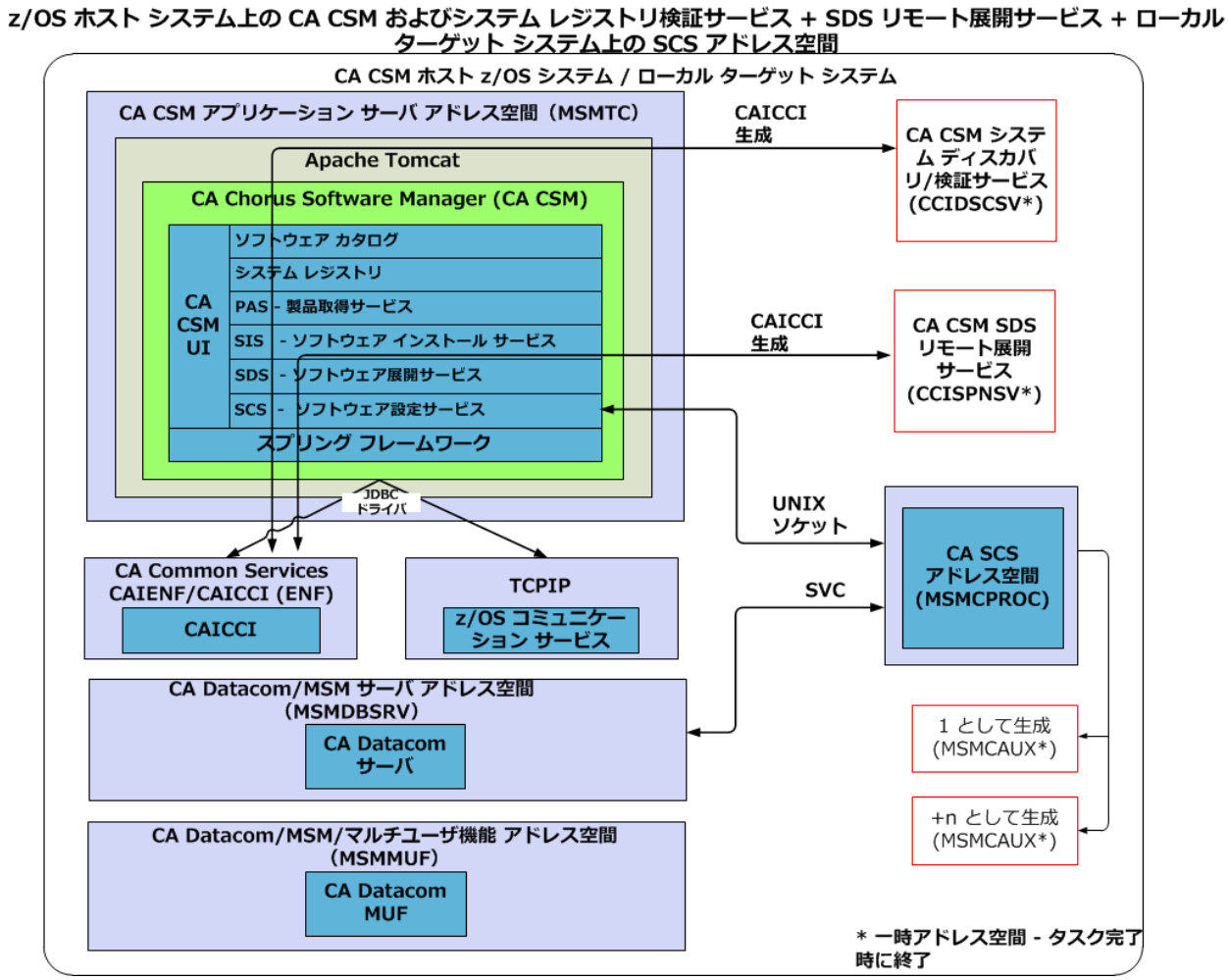


z/OS ホスト システム上の CA CSM およびリモート ターゲット システム上のシステム ディスカバリソース/検証サービス




z/OS ホスト システム上の CA CSM およびリモート ターゲット システム上の SDS リモート展開サービス
CA CSM ホスト z/OS システム
CA CSM Application Server アドレス空間（MSMTC）
Apache Tomcat
CA Chorus Software Manager（CA CSM）
CA CSM UI
ソフトウェア カタログ
システム レジストリ
PAS - 製品取得サービス
SIS - ソフトウェア インストール サービス
SDS - ソフトウェア展開サービス
SCS - ソフトウェア設定サービス
スプリング フレームワーク
JDBC ドライバ
CA Common Services CAIENF/CAICCI (ENF)
CAICCI
TCPIP z/OS Communication Services
CA Datacom/MSM Server アドレス空間（MSMDBSRV）
CA Datacom Server
CA Datacom/MSM/Multi-User Facility アドレス空間（MSMMUF）
CA Datacom MUF
CAICCI 生成
リモート ターゲット システム 1
CA Common Services CAIENF/ CAICCI (ENF)
CA CSM SDS リモート展開サービス * (CCISPNSV)
展開済みターゲット ライブラリ
* 一時アドレス空間 - タスク完了時に終了


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



ネットワーク フロー

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

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

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

   HTTPS

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

   FTP

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

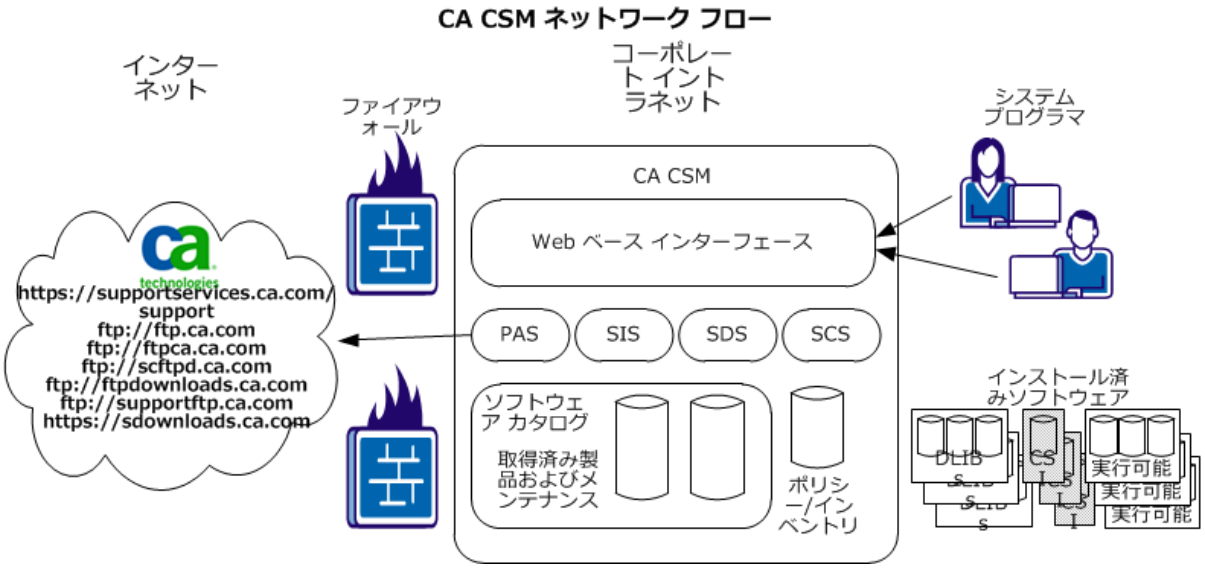
   - ftp://scftpd.ca.com
   - ftp://ftp.ca.com
   - ftp://supportftp.ca.com

注: 以下の情報は、CA Technologies との間で受け渡される唯一の暗号化されていないデータです。

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

これらのデータは、プライバシー標準または暗号化標準の一部ではありません。

以下の図で、このプロセスを説明します。



第 2 章: CA CSM のセットアップ

このセクションには、以下のトピックが含まれています。

ユーザのセキュリティ セットアップ (P. 23)
CA CSM 関連セキュリティ ID - OMVS セグメントおよびホーム ディレクトリ (P. 27)

ユーザのセキュリティ セットアップ

このセクションには、以下のトピックが含まれています。

ユーザの USS 許可のセットアップ (P. 23)

CA CSM 機能のユーザ セキュリティのセットアップ (P. 25)

ユーザの USS 許可のセットアップ

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

以下の手順に従います。

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

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

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

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

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

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

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

   - IBM RACF システムについては、以下のコマンドを入力します。

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

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

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

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

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

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

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

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

   - IBM RACF システムについては、以下のコマンドを入力します。

     ```
     LISTUSER uuuuuu OMVS NORACF
     ```

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

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

   たとえば、UID*nnn* 用の /u/name という名前のディレクトリを設定するには、OMVS UNIX シェルで以下のコマンドを発行します。

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

5. 以下のコマンドを使用して、所有者およびディレクトリへのアクセスを確認します。

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

   以下の結果が表示されます。

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

CA CSM 機能のユーザ セキュリティのセットアップ

CA CSM は CAMSM リソース クラスのリソース プロファイル (P. 141)を使用し、Web ベース インターフェース上のリソースへのアクセス権を付与します。 これらのプロファイルを使用して、ユーザ セキュリティを設定します。 CA CSM 機能のセキュリティ チェックの有効化が予定されている場合、セキュリティ管理者はユーザが Web ベース インターフェースにアクセスする前に、セキュリティを設定する必要があります。

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

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

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

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

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

重要: SAF セキュリティが有効化された CA CSM の開始に失敗 (P. 189)した場合、以下のエラーが CA CSM ジョブ ログに表示されます。

SafError - Error during DSI java open. RC=13

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

以下の手順に従います。

1. リソース プロファイルを使用してユーザ セキュリティを設定します。

   ユーザはさまざまなロールに対してセキュリティ保護されます。

2. CA CSM アプリケーション サーバを再利用します。

   設定されたセキュリティが有効になります。

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

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

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

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

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

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

第 3 章: CA CSM の設定

このセクションには、以下のトピックが含まれています。

UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 29)
別の LPAR での CA CSM の実行 (P. 36)
CA CSM の［Notice and Consent］バナーの有効化 (P. 38)
CA CSM アプリケーション サーバのマルチ TCP/IP スタック環境の TCP/IP スタックへのバインド (P. 39)
FTP および HTTP 接続の設定 (P. 40)
HTTPS を使用するための CA CSM の設定 (P. 52)
CA CSM ファイル システムのマウント パラメータの設定 (P. 58)
MUF メッセージ出力の設定 (P. 61)
出力記述子の設定 (P. 61)
展開用のセキュア FTP 接続のセットアップ (P. 62)
SAMPLIB(MSMLIB) メンバのリモート システムの SYSUT3 および SYSUT4 用の UNIT パラメータの指定 (P. 64)

UID(0) を使用しない CA CSM ユーザ ID の設定

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

このセクションには、以下のトピックが含まれています。

前提条件 (P. 30)

CA Top Secret for z/OS の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 30)

CA ACF2 for z/OS の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 32)

IBM RACF の UID(0) を使用しない CA CSM ユーザ ID の設定 (P. 34)

前提条件

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

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

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

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

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 30)。
2. CA CSM のインストール完了後、お使いのセキュリティ システムで、たとえば GID 定義がある CACSMGRP のようなグループを作成し、以下の手順を実行します。
   a. CACSMGRP を DFLTGRP として各 CA CSM ユーザに追加します。
   b. CACSMGRP を DFLTGRP として CA CSM ユーザ ID に追加します。

3. SUPERUSER 権限で以下のコマンドを発行して所有者およびグループを変更します。

```
chown –R CA_CSM_USER_ID MSMPATH
chgrp –R CACSMGRP MSMPATH
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
chown –R CA_CSM_USER_ID RunTimeUSSPath
chgrp –R CACSMGRP RunTimeUSSPath
```

上記の MSMPATH、MountPath、RunTimeUSSPath は MSMSetupOptionsFile.properties ファイルで参照される値です。

注: *RunTimeUSSPath* 用のコマンドを発行すると、以下のメッセージが表示される場合があります。

```
EDC5129I No such file or directory
```

このメッセージは ioeagfmt ファイルに対して発行され、コマンドの完了にはまったく影響しません。このメッセージは無視してもかまいません。

重要: MSMDEPLY ジョブの実行後にもこれらのコマンドを発行します。

4. CA CSM ユーザ ID のパラメータを設定します。
   a. Facility STC を割り当てます。
   b. Master FAC に MSM を割り当てます。

      注: 事前に、Master FAC が存在することを確認してください。

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

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

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

```
UNIXPRIV SUPERUSER.FILESYS.CHANGEPERMS ACCESS(READ)
UNIXPRIV SUPERUSER.FILESYS.MOUNT ACCESS(UPDATE)
UNIXPRIV SUPERUSER.FILESYS.PFSCTL ACCESS(READ)
```

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

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

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

   ```
   chown –R CA_CSM_USER_ID MountPath
   chgrp –R CACSMGRP MountPath
   ```

   上記の MountPath は、MSMSetupOptionsFile.properties ファイルで参照される値です。

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

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 30)。
2. CA CSM のインストールが完了した後、お使いのセキュリティ システムで、GID 定義があるグループ（たとえば CACSMGRP）を作成し、以下の手順を実行します。
   a. CA CSM ユーザ ID を CACSMGRP のメンバとして定義します。
   b. 各 CA CSM ユーザを CACSMGRP のメンバとして定義します。

3. SUPERUSER 権限で以下のコマンドを発行して所有者およびグループを変更します。

```
chown –R CA_CSM_USER_ID MSMPATH
chgrp –R CACSMGRP MSMPATH
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
chown –R CA_CSM_USER_ID RunTimeUSSPath
chgrp –R CACSMGRP RunTimeUSSPath
```

上記の MSMPATH、MountPath、RunTimeUSSPath は MSMSetupOptionsFile.properties ファイルで参照される値です。

注: *RunTimeUSSPath* 用のコマンドを発行すると、以下のメッセージが表示される場合があります。

```
EDC5129I No such file or directory
```

このメッセージは ioeagfmt ファイルに対して発行され、コマンドの完了にはまったく影響しません。このメッセージは無視してもかまいません。

重要: MSMDEPLY ジョブの実行後にもこれらのコマンドを発行します。

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

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

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

```
SUPERUSER.FILESYS.CHANGEPERMS   READ
SUPERUSER.FILESYS.MOUNT         UPDATE
SUPERUSER.FILESYS.PFSCTL        READ
```

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

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

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

```
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
```

上記の MountPath は、MSMSetupOptionsFile.properties ファイルで参照される値です。

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

お使いのセキュリティ システム設定に従って、この手順を変更します。

以下の手順に従います。

1. 前提条件を確認します (P. 30)。
2. CA CSM のインストールが完了した後、お使いのセキュリティ システムで、GID 定義があるグループ（たとえば CACSMGRP）を作成し、以下の手順を実行します。
   a. CA CSM ユーザ ID を CACSMGRP のメンバとして定義します。
   b. 各 CA CSM ユーザを CACSMGRP のメンバとして定義します。

3. SUPERUSER 権限で以下のコマンドを発行して所有者およびグループを変更します。

```
chown –R CA_CSM_USER_ID MSMPATH
chgrp –R CACSMGRP MSMPATH
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
chown –R CA_CSM_USER_ID RunTimeUSSPath
chgrp –R CACSMGRP RunTimeUSSPath
```

上記の MSMPATH、MountPath、RunTimeUSSPath は MSMSetupOptionsFile.properties ファイルで参照される値です。

注: *RunTimeUSSPath* 用のコマンドを発行すると、以下のメッセージが表示される場合があります。

```
EDC5129I No such file or directory
```

このメッセージは ioeagfmt ファイルに対して発行され、コマンドの完了にはまったく影響しません。このメッセージは無視してもかまいません。

重要: MSMDEPLY ジョブの実行後にもこれらのコマンドを発行します。

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

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

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

```
SUPERUSER.FILESYS.CHANGEPERMS   READ
SUPERUSER.FILESYS.MOUNT         UPDATE
SUPERUSER.FILESYS.PFSCTL        READ
```

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

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

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

```
chown –R CA_CSM_USER_ID MountPath
chgrp –R CACSMGRP MountPath
```

上記の MountPath は、MSMSetupOptionsFile.properties ファイルで参照される値です。

別の LPAR での CA CSM の実行

共有 DASD を持つシスプレックス内の別の LPAR で CA CSM を実行できます。 たとえば、CA CSM を LPAR1 にインストールし、その後再インストールせずに LPAR2 で実行します。

注: 同じ USS ファイル システムを使用している CA CSM は一度に 1 つの LPAR でのみ実行できます。適切なレベルの CA Common Services for z/OS 関数 CETN*xxx* を新しい LPAR にインストールしていることが必要です。 CA Common Services for z/OS 関数 CETN*xxx* のレベルは、お使いの CA CSM のバージョンによって異なり、最初の LPAR 上のバージョンと同じです。

重要: CA CSM は、CA Datacom データベースでファイル システムに使用される USS パスを格納しています。 両方の LPAR システムで同じ USS パス名を使用する必要があります。

たとえば、LPAR1 に以下の USS パスがあります。

```
/u/users/csmpt/PT51/mpm/scroot/DatabaseM/CA/CA_ACF2_-_MVS/
```

LPAR2 へのインストールでも同じ USS ファイル システムを使用してください。 LPAR2 上で CA CSM を再起動すると、共有ファイル システムによって USS パスの前に接頭辞が自動的に追加され、CA CSM が正しいシステムにマウントされます。

以下の手順に従います。

1. LPAR1 で実行中の CA CSM にログインし、［Settings］タブの［System Settings］ -［Mount Point Management］に移動します。 ［Unmount at Shutdown］を選択します。 ［Apply］ボタンをクリックして、変更を保存します。
2. LPAR1 上の CA CSM をシャットダウンします。
3. LPAR1 から CA CSM USS ファイル システムをマウント解除します。 このファイル システムは、CA CSM アプリケーション サーバ スターティッド タスクまたはバッチ JCL の実行前にマウントされました。 このファイル システムは、SAMPLIB（MSMLIB）メンバでも参照されます。以下に例を示します。

   C_HOME=*/parent_path*/msmserv/*version_number*/msmruntime/tomcat

   前のケースでのマウントポイントは、以下のファイル システム向けです。

   /parent_path/msmserv/*version_number*/

4. （オプション）マウントポイントに必要なファイル システムおよび z/OS データ セット情報は、OMVS で以下のコマンドを発行して確認します。

   df –vkP | grep */parent_path*/msmserv/*version_number*/

5. CA CSM USS ファイル システムを LPAR2 にマウントします。
6. ［Edit ASCII］オプションを使用して、*parent_path*/msmserv/*version_number*/msmruntime/Tomcat/conf にある 2 つの XML ファイル（context.xml および server.xml）を編集します。ISPF エディタを使用することをお勧めします。
   - context.xml ファイルで、以下のパラメータを指定します。
     - SystemID
     - HostName

- （オプション） CA CSM が常駐する新規の LPAR2 用の URL で CA CSM が使用するポート番号を変更する必要がある場合は、server.xml ファイルを編集します。
  - シャットダウン ポートを編集するには、以下の行で shutdown パラメータを変更します。

    ```
    <Server port="25955" shutdown="MSMTCEND">
    ```

  - 接続ポートを編集してポートをリダイレクトするには、以下の行で port および redirectPort パラメータを変更します。

    ```
    <Connector connectionTimeout="20000" port="25958" protocol="HTTP/1.1"
    redirectPort="25957"/>
    ```

注: CA CSM を実行する各 LPAR 用のこれらのファイルは事前定義できます。 たとえば、CA CSM を実行可能な 2 つの LPAR （LPAR1 および LPAR2） があるとします。 コンテキストおよびサーバ ファイルは以下のように作成します。

- LPAR1 の場合： context.xml.LPAR1 および server.xml.LPAR1
- LPAR2 の場合： context.xml.LPAR2 および server.xml LPAR2

7. 現在の LPAR1 上の MUF および CA Datacom Server を停止します。
8. LPAR2 用の該当ファイルを複製し、それらを元の名前に変更します： context.xml および server.xml
9. LPAR2 上で MUF および CA Datacom Server スターティッド タスクまたはバッチ JCL を開始します。
10. （オプション）LPAR1 で実行中の CA CSM にログインし、［Settings］タブの［System Settings］-［Mount Point Management］に移動します。チェック ボックス［Unmount at Shutdown］をオフにします。［Apply］ボタンをクリックして、変更を保存します。

CA CSM の［Notice and Consent］バナーの有効化

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

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

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

ファイルにはサンプルのバナーが含まれます。

以下の手順に従います。

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

   ```
   tomcat/webapps/
   ```

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

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

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

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

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

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

スタック親和性を確立するには、以下のいずれかのメソッドを選択します。

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

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

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

  ```
  export _BPXK_SETIBMOPT_TRANSPORT=stackname
  ```

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

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

FTP および HTTP 接続の設定

このセクションでは、新規および既存の CA CSM インストール用に FTP 接続を設定する方法、および HTTP 接続を設定する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。

既存インストール用の FTP 接続の設定

旧バージョンの CA CSM から CA CSM バージョン 6.0 にアップグレードする場合、FTP の設定変更は必要ありません。

既存インストール用の 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. 52)で確認します。 以下に例を示します。

```
mydomain¥user1
```

これ以外の場合は、旧バージョンの CA CSM から CA CSM バージョン 6.0 にアップグレードする際に、HTTP の設定変更は必要ありません。

新規インストール用の FTP 接続の設定

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 (P. 203)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. 44)

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. 44）
- ユーザ認証情報を使用する（P. 45）

ユーザ認証情報を使用しない設定

以下の手順に従います。

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

以下の手順に従います。

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. 47)

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 プロキシ設定の構成

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

以下の手順に従います。

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

以下の手順に従います。

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

以下の手順に従います。

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。

HTTPS を使用するための CA CSM の設定

このセクションでは、デジタル証明書を使用して HTTPS アクセスを有効にするための CA CSM の設定方法について説明します。

USS ファイルに格納された証明書を使用した HTTPS の有効化

証明書を格納する USS ファイルを使用して、ユーザ アクセスに対して HTTP の代わりに HTTPS を使用するように CA CSM を手動で設定できます。

以下の手順に従います。

1. 以下のように、キーストアを生成します。
   a. OMVS セッションを開始し、以下のコマンドを入力します。

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

      プロンプトが表示されます。

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

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

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

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

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

2. 以下のように、Apache Tomcat を設定します。
   a. tomcat/conf に移動し、server.xml ファイルを開きます。
   b. 以下のように、SSL コネクタの部分のコメントを解除するか、または置換します。

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

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

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

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

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

3. Apache Tomcat を起動（または再起動）します。

4. TLS 暗号化を使用するために、以下のようにしてブラウザを有効にします。

   - Microsoft Internet Explorer を使用する場合は、［ツール］-［インターネット オプション］ -［詳細設定］の順にクリックし、［セキュリティ］の下の［TLS 1.0 を使用する］チェック ボックスをオンにします。
   - Mozilla Firefox を使用する場合は、［ツール］-［オプション］-［詳細］の順にクリックし、［暗号化］タブの［TLS 1.0 を使用する］チェック ボックスをオンにします。

5. ブラウザを再起動します。

6. HTTPS URL にアクセスします。

   注: お使いのブラウザから HTTPS URL に初めてアクセスすると、証明書を信頼することを確認するメッセージが表示される場合があります。

7. ［Yes］をクリックし、信頼済みの証明書にこの証明書を追加します。

注: 詳細については、Apache Tomcat 7.0 Servlet/JSP Container のドキュメントを参照してください。

外部セキュリティ マネージャに格納された証明書を使用した HTTPS の有効化

デジタル証明書を格納する外部セキュリティ マネージャ（たとえば、CA Top Secret for z/OS、CA ACF2 for z/OS または IBM RACF）を使用して、ユーザ アクセスに対して HTTP の代わりに HTTPS を使用するように CA CSM を手動で設定できます。

以下の手順に従います。

1. Apache Tomcat 用のデジタル証明書を生成し、お使いの外部セキュリティ マネージャの適切な手順を使用して、SAF キー リングにそれを添付します。

   証明書は、RSA アルゴリズムを使用して生成することをお勧めします。推奨される証明書エイリアスは **Tomcat** です。

2. 以下のように、Apache Tomcat を設定します。

   a. Apache Tomcat サーバを停止します。

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

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

```
<!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
   <Connector port="30308" maxHttpHeaderSize="8192"
          maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
          enableLookups="false" disableUploadTimeout="true"
          SSLEnabled="true"
          algorithm="IbmX509"
          acceptCount="100" scheme="https" secure="true"
          clientAuth="false" sslProtocol="TLS"
          sslEnabledProtocols="TLSv1.2,TLSv1.1,TLSv1" />
          keystoreType="JCERACFKS"
          keystoreFile="safkeyring://KEY_RING_OWNER/KEY_RING_NAME"
          sslImplementationName="com.ca.sslsocket.CASSLImplementation" />
```

   d. ポート パラメータをニーズに合わせて変更します。

   e. 証明書を含む SAF キー リングを示すように、keystoreFile パラメータを変更します。

      a. *KEY_RING_OWNER* を Apache Tomcat サーバを実行するユーザの ID に置換します。ユーザにはそのキー リングの READ 権限が必要です。

      b. *KEY_RING_NAME* をキー リング名に置換します。

      例： keystoreFile="safkeyring://MSMSERV/CSMKEYRING"

f. 外部セキュリティ マネージャでデジタル証明書を管理するために IBM Integrated Cryptographic Services Facility （ICSF）がサイトで使用されている場合は、keystoreType パラメータを JCECCARACFKS の値に変更します。

g. Apache Tomcat で受信接続では常に HTTPS が強制的に使用されるようにする場合は、HTTP をオーバーライドするよう HTTPS を設定します (P. 57)。

3. Apache Tomcat サーバを起動します。

   注: Apache Tomcat サーバの起動時、以下のメッセージが出力に表示される可能性があります。

   ```
   WARNING: configured file: ./path/safkeyring://KEY_RING_OWNER/KEY_RING_NAME.
   does not exist.
   ```

   このメッセージは無視してもかまいません。

4. TLS 暗号化を使用するために、以下のようにしてブラウザを有効にします。

   - Microsoft Internet Explorer を使用する場合は、［ツール］-［インターネット オプション］ -［詳細設定］の順にクリックし、［セキュリティ］の下の［TLS 1.0 を使用する］チェック ボックスをオンにします。
   - Mozilla Firefox を使用する場合は、［ツール］-［オプション］-［詳細］の順にクリックし、［暗号化］タブの［TLS 1.0 を使用する］チェック ボックスをオンにします。

5. ブラウザを再起動します。

6. HTTPS URL にアクセスします。

   注: お使いのブラウザから HTTPS URL に初めてアクセスすると、証明書を信頼することを確認するメッセージが表示される場合があります。

7. ［Yes］をクリックし、信頼済みの証明書にこの証明書を追加します。

注: 詳細については、Apache Tomcat 7.0 Servlet/JSP Container のドキュメントを参照してください。

HTTP をオーバーライドする HTTPS の設定

ユーザ アクセスに対して HTTP の代わりに常に HTTPS を使用するように CA CSM を手動で設定できます。

以下の手順に従います。

1. HTTP（52P. , 51P. ）および HTTPS（P. 52）の両方を使用して CA CSM にアクセスできることを確認します。
2. Apache Tomcat をシャットダウンします。
3. web.xml ファイルで Apache Tomcat を設定します。
   a. tomcat/conf ディレクトリで、web.xml ファイルを開きます。
   b. 以下の XML を web-app タグの下に追加します。

```
<security-constraint>
     <web-resource-collection>
     <web-resource-name>Protected Context</web-resource-name>
        <url-pattern>/*</url-pattern>
     </web-resource-collection>
           <!-- auth-constraint goes here if you require authentication -->
      <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
      </user-data-constraint>
</security-constraint>
```

   c. web.xml ファイルを保存して閉じます。
4. server.xml ファイルで Apache Tomcat を設定します。
   a. Tomcat/conf ディレクトリで、server.xml ファイルを開きます。
   b. Apache Tomcat が実行される HTTP ポート番号を含む Connector XML 定義を検索します。
   c. redirectPort 属性を変更するか、必要な場合は Connector XML タグに追加します。その値を HTTPS Connector のポート番号として設定します。 以下に例を示します。

```
<!-- A "Connector" represents an endpoint by which requests
        and responses are returned. Documentation at :
        Java HTTP Connector: /docs/config/http.html (blocking &
        non-blocking)
     Java AJP  Connector: /docs/config/ajp.html
        APR (HTTP/AJP) Connector: /docs/apr.html
        Define a non-SSL HTTP/1.1 Connector on port 8080
    -->
    <Connector address="123.456.789.321" port="8080"
               protocol="HTTP/1.1"
               connectionTimeout="20000"
               redirectPort="30308" />
```

d. server.xml ファイルを保存して閉じます。

5. Apache Tomcat を起動します。
6. ブラウザを再起動します。
7. HTTP URL にアクセスし、それが HTTPS URL にリダイレクトすることを確認します。

注: 詳細については、Apache Tomcat 7.0 Servlet/JSP Container のドキュメントを参照してください。

CA CSM ファイル システムのマウント パラメータの設定

サイトおよび環境の要件に応じて、CA CSM 製品、ソフトウェア カタログ、一時および展開ファイル システムのマウント パラメータを設定できます。たとえば、セキュリティ チェックを実行するかどうか、またはファイル システムを所有するシステムがダウンした場合の処理方法を決定できます。

最初、CA CSM ではこれらのパラメータのデフォルト値を使用します。 デフォルト値はオーバーライドできます。

以下の手順に従います。

1. 次のいずれかの操作を実行します。
   - すべてのファイル システムを手動でマウント解除します。
   - CA CSM で、［Settings］タブ、［Mount Point Management］ページに移動し、［Unmount at Shutdown］チェック ボックスをオンにします。 変更内容を保存します。
2. CA CSM アプリケーション サーバを停止します。

3. *RunTimeMVSHLQPrefix*.SAMPLIB （MSMLIB）メンバ内の以下の行のコメントを外して更新します。

```
IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=SETUID|NOSETUID,SECURITY|NOSECURITY,
AUTOMOVE|NOAUTOMOVE|UNMOUNT"
```

SETUID|NOSETUID

setuid() および setgid() モード ビットがサポートされるかどうかを指定します。

SETUID

実行可能ファイル上の setuid() および setgid() モード ビットをサポートします。デフォルトでは、このオプションが選択されています。

NOSETUID

実行可能ファイル上の setuid() および setgid() モード ビットのサポートを無効化します。 プログラムが実行される場合、UID または GID は変更されません。また、APF およびプログラム制御の拡張属性は使用されません。 HFS 全体は制御されません。

SECURITY|NOSECURITY

UNIX アクセス権限チェックを実行するかどうかを指定します。

SECURITY

UNIX アクセス権限チェックを有効化します。デフォルトでは、このオプションが選択されています。

NOSECURITY

UNIX アクセス権限チェックを無効化します。 作成されるすべての新規ファイルやディレクトリには、リクエストを発行した UID とは無関係に UID（0）の所有者が割り当てられます。ユーザは、あらゆるファイルまたはディレクトリに対してアクセスまたは変更を行えます。

AUTOMOVE|NOAUTOMOVE|UNMOUNT

共有ファイル システムに参加しているシステムのシスプレックスに対して、ファイル システムを所有するシステムがダウンしたときの処理方法を指定します。

AUTOMOVE

ファイル システムの所有権を、共有ファイル システムに参加している別のシステムに自動的に変更します。デフォルトでは、このオプションが選択されています。

NOAUTOMOVE

ファイル システムの所有権を保持します。 その結果、ファイル システムはアクセス不可になります。

UNMOUNT

ノードがシスプレックスを離れる場合、ファイル システムをマウント解除します。

注: これらのオプションの詳細については、以下のドキュメントを参照してください。

- *IBM z/OS UNIX System Services Planning*
- *IBM z/OS UNIX System Services Command Reference*
- *IBM z/OS XL C/C++ Run-Time Library Reference*

4. CA CSM アプリケーション サーバを起動します。

   マウント パラメータは有効になります。

5. 手順 1 で［Unmount at Shutdown］機能を有効化している場合は、［Settings］タブ、［Mount Point Management］ページに移動して、［Unmount at Shutdown］チェック ボックスをオフにしてください。変更内容を保存します。

デフォルト値を復元するには、パラメータを空にしておくか、または *RunTimeMVSHLQPrefix*.SAMPLIB （MSMLIB）メンバ内の行をコメントアウトします。

例

この例では、実行可能ファイル上の setuid() および setgid() モード ビットを有効にし、セキュリティ チェックは無効にし、ファイル システムの所有権は変更されないようにします。

```
IJO="$IJO -DADD_MOUNT_DEFAULT_OPTIONS=NOSECURITY,NOAUTOMOVE"
```

MUF メッセージ出力の設定

複数の MUF リージョンを区別するには、(CUSMAC)MUFSTART メンバ内の MUFMSG パラメータを使用します。 このパラメータは、MUF ジョブ名、情報データおよび MUF 名の表示を指定するために設定されます。 これらのプロパティは、MUF が発行したメッセージ、および MUF 機能との通信に関係のある一部のメッセージのメッセージ番号の前に付けます。

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

プレフィクス付きメッセージは、以下の形式で表示されます。

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

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

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

出力記述子の設定

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

以下の例ではサイト固有の意味のある名前を使用して、出力記述子を示します。

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

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

展開用のセキュア FTP 接続のセットアップ

TLS （トランスポート層セキュリティ）上の FTP を使用してリモート システムに製品を展開する機能をサポートするために CA CSM をセットアップできます。 この機能を使用することで、安全で暗号化された方式でデータを交換できます。

この機能では X.509 デジタル証明書が使用されます。

証明書は SAF キー リングを使用して、セキュリティ マネージャ（CA Top Secret for z/OS、CA ACF2 for z/OS または IBM RACF）から読み取るか、または USS Java キー ストアから読み取ることができます。 さらに、CA CSM では、ハードウェア証明書管理に IBM Integrated Cryptographic Service Facility（ICSF）を使用するサイトのサポートを提供します。

以下の表では、CA CSM がサポートしている使用可能なキー ストア タイプの概要について説明します。

ストレージ	証明書管理	キー ストア
セキュリティ マネージャ	ソフトウェア	JCERACFKS
セキュリティ マネージャ	ハードウェア	JCECCARACFKS
USS	ソフトウェア	JKS、JCEKS、PKCS12
USS	ハードウェア	JCECCAKS

注: Java で使用できるキー ストア タイプの詳細については、「*Security Reference for IBM SDK、Java Technology Edition*」を参照してください。

以下の手順に従います。

1. ［Settings］タブをクリックし、左側にある［Settings］セクションの［System Settings］の下の［Software Deployment］リンクをクリックします。

   ［Deployed Software］ページが表示されます。

2. ［Key Store Settings］セクションで、使用するキー ストアのタイプを選択します。

   セクション内のフィールドが表示されます。 フィールドは選択したキー ストア タイプによって異なります。

3. フィールドの値をセットアップし、［Apply］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。

   FTP 接続設定が保存されます。

4. FTP ロケーションを追加します。 FTP ロケーションを追加する場合、チェック ボックス［Enable Secure FTP Transmission］をオンにします。

   セキュアな FTP 転送が有効化された FTP ロケーションが追加されます。

   TLS 上の FTP を使用して製品を展開できるようになりました。

注: FTP ロケーションの追加の詳細については、オンライン ヘルプを参照してください。

詳細情報:

gskkyman データベースからの証明書のエクスポート (P. 63)

gskkyman データベースからの証明書のエクスポート

FTP サーバが FTP キー リングとして gskkyman キー データベースを使用する場合、gskkyman データベースから証明書をエクスポートして、Java JKS キー ストアにインポートします。これにより CA CSM が FTP サーバと同じ証明書を使用できるようになります。

以下の手順に従います。

1. *JAVA_HOME*/lib/security/ で cacerts ファイルのコピーを作成して、CA CSM キーストアに使用します。

   注: cacerts ファイルは IBM Java 付属のデフォルト JKS 証明書ファイルです。cacerts ファイルには複数のルート認証局証明書が含まれ、通常、新しい JKS キー ストアを用意するために使用されます。

2. gskkyman ユーティリティを使用し、バイナリ ASN.1 DER 形式によって、FTP キー リング ファイルから適切な認証局をエクスポートします。

   注: gskkyman ユーティリティの詳細については、「*z/OS Cryptographic Services System Secure Sockets Layer Programming*」を参照してください。

3. Java の keytool ユーティリティを使用して、手順 1a で作成したキー ストア データベースに認証局をインポートします。以下のコマンドを使用します。

   ```
   keytool –import –trustcacerts –file /path_to_exported_ca_certificate
   –keystore /path_to_copy_jks_cacerts/file_name
   ```

   ユーティリティによって、インポートした CA を信頼済みにして、キー ストア パスワードを入力するように要求されます。Java 付属の cacerts ファイルの初期パスワードは **changeit** です。

4. 展開に対してセキュア FTP 接続をセットアップします (P. 62)。

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

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

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

第 4 章: CA CSM のメンテナンス

このセクションには、以下のトピックが含まれています。

CA CSM の起動 (P. 65)
メンテナンス (P. 67)
CA CSM のバックアップおよびディザスタ リカバリ (P. 73)
CA CSM の停止 (P. 77)

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 (P. 203) 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 (P. 203)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"
```

重要: アップグレードしている場合は、旧バージョンの CA CSM からのアドレス空間が停止していることを確認します。また、APLROOT、SCROOT、LJWK マウント ポイントを旧バージョンからマウント解除します。 必要に応じて、旧バージョンの 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。

以下の手順に従います。

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

   CA Datacom/MSM Multi-User 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 (P. 203) リージョンのスタートアップ JCL には、コメント アウトされた SYSMDUMP DD ステートメントがあります。サイトの基準やシステムが、このダンプのスプール システムへの収集をサポートしている場合、この DD ステートメントのコメントを解除することで、失敗した場合のダンプを取得することができます。

CA CSM アプリケーション サーバ アドレス空間 (P. 203)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。

4. （CA CSM アップグレードのみ）CA CSM を最初に正常に起動した後、MSMTCSRV JCL メンバまたは MSMTC PROCLIB で 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 (P. 203) 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 (P. 203) 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。

メンテナンス

CA CSM をセットアップしてインストールした後、それを使用してそれ自体のメンテナンスを行うことができます。

CA CSM へのメンテナンスの APPLY

重要: メンテナンスをダウンロードするには、［Product Acquisition Settings］ページで CA CSM ログイン ユーザ名を CA サポート Online Web サイトの登録ユーザと関連付ける必要があります。

以下の手順に従います。

1. 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 (P. 77)。

   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。

SQL プランの更新

CA Datacom/MSM SQL プランに影響する更新を適用する必要がある場合があります。 これらの SQL プランは、CA Common Services for z/OS メンテナンスとして提供されます。 CA Common Services for z/OS には、MUF 環境のこれらの SQL プランの更新に使用できるサンプルの JCL メンバ MSMCXPLN が用意されています。

最新の SQL プランの実装

CA Common Services for z/OS SMP/E 環境のサンプル JCL ライブラリにあるメンバ MSMCXPLN はモデル化された JCL で、CA Datacom/MSM SQL プランの更新に使用することができます。 少なくとも 1 つのモジュール要素と、関連する SQL プラン要素が含まれる PTF を APPLY する場合は常に、この JCL を実行します。 ユーザは、PTF を APPLY するプロセス中に発生する ++HOLD 条件アクションにより、サンプルの JCL メンバ MSMCXPLN に修正と実行が必要であると通知されます。 ++HOLD コメントに示される手順に従って、このメンバを適切に修正および実行します。

注: CETN600（MSMCCS 6.0）が CA Common Services for z/OS に存在する場合は、SQL プランが CA Datacom/MSM データベース バージョン 6.0 および実行中の CA Common Services for z/OS ライブラリで同期されることを確認してください。DDDEF CAW0EXP で表される CA Common Services for z/OS ライブラリの各 MSMC*SQL メンバに対し、CA Common Services for z/OS JCL ライブラリから MSMCXPLN ジョブをサブミットします。

サンプル JCL のデータ セット リファレンス

適切なサンプル JCL ライブラリのデータ セット名を特定するには、DDDEF 要素 CAW0JCL を参照してください。

SQL プランのデータ セット リファレンス

適切な SQL プラン ライブラリのデータ セット名を特定するには、DDDEF 要素の CAW0EXP を参照してください。

旧バージョンからのコードを含んだ SCS アドレス空間での CA CSM バージョン 6.0 の実行

CA CSM バージョン 6.0 には、旧バージョンの CETN400 および CETN500 の SQL プランと同じバージョンは含まれていません。 この状況では、旧バージョン（CETN400 または CETN500）の SCS アドレス空間に接続するとき、SQL -124 リターン コードを受け取る場合があります。

CA CSM バージョン 6.0 にアップグレードした後、このセクションで説明する手順に従って CETN400 または CETN500 ライブラリから SQL プランをインポートします。 この手順では、CETN600 を CETN400 に読み替えます。 1 つ以上の CA CSM アドレス空間に接続する際に、それらのアドレス空間に引き続き旧バージョン（CETN400 または CETN500）のコードが含まれており、CA Common Services for z/OS を CETN600 にアップグレードできない場合は、この手順を実行します。

詳細情報:

CA CSM アドレス空間が正しく機能しない (P. 185)

CA CSM からのメンテナンスのバックアウト

APPLY した（しかし ACCEPT されていない）メンテナンスを、CA CSM からバックアウトできます。 CA CSM メンテナンスをバックアウトするとき、まず CA CSM リストア アクションを使用し、SMP/E ターゲット ライブラリと USS パスを更新します。 その後、CA CSM を停止し、MSMDEPLY ジョブをサブミットしてランタイム ライブラリおよび USS パスを更新します。 CA CSM を再起動すると、それらの更新は有効になります。

以下の手順に従います。

1. RESTORE アクションを使用してメンテナンスをバックアウトします。

   CA CSM 用の SMP/E ターゲット ライブラリおよび USS パスのコンテンツが更新されます。 これらのライブラリとパスは、MSMSetupOptionsFile.properties オプション ファイルの TargetHLQ と MSMPATH キーワードを使用してセットアップされます。

   注: メンテナンスのバックアウトの詳細については、オンライン ヘルプを参照してください。

2. CA CSM を停止します (P. 77)。

   CA CSM は稼働を停止します。

3. 更新された SMP/E ターゲット ライブラリおよび USS パスのコンテンツを、CA CSM ランタイム ライブラリおよび USS パスに展開します。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、*backout* を第 1 引数に指定します。

   b. ジョブをサブミットします。

4. CA CSM を起動します (P. 65)。

   CA CSM はメンテナンスなしで稼働可能になります。

フェイルセーフ バックアウト

まれに、CA CSM に対する不正なテスト修正により、CA CSM が稼働不能になることがあります。その問題を解決するため、MSMDEPLY ジョブを使用して CA CSM ランタイム ライブラリと USS パスを稼働可能な状態にリストアすることができます。第一引数に *backout* を指定して MSMDEPLY ジョブをカスタマイズし、サブミットします。ジョブが完了した後、CA CSM を再起動し、通常の手順に従って不正なテスト修正をバックアウトします。

MSMDEPLY ジョブに *deploy* を指定して実行すると、現行の CA CSM ランタイム ライブラリおよび USS パスのコピーが、展開の前に保存されます。MSMDEPLY ジョブに *backout* を指定して実行すると、CA CSM ランタイム ライブラリおよび USS パスの最後に保存されたコピーが展開されます。

重要: ただ 1 つの CA CSM ランタイム ライブラリおよび USS パスのコピーがメンテナンスされます。 MSMDEPLY ジョブに *deploy* を指定して実行するたびに、最後に保存したランタイム ライブラリおよび USS パスは、新しいコピーで置き換えられます。 MSMDEPLY ジョブに *backout* を指定して何度実行しても、複数保存されたコピーのバックアウトはできません。

メンテナンスが理由で CA CSM が失敗する場合のリカバリ

CA CSM が依存するソフトウェアに適用されたメンテナンスが原因で CA CSM が失敗することがあります。 CA CSM を使用してその問題を修正できなくなる可能性があります。

- メンテナンスが CA CSM 自体に APPLY されている場合は、フェイルセーフ バックアウト メソッド (P. 72)を使用し、CA CSM を稼働可能な状況に戻します。
- CA CSM に影響する別の製品に属するソフトウェアにメンテナンスが適用されたことが原因で問題が発生した場合、SMP/E バッチ ジョブを使用して、新しい修正メンテナンスを適用するか、メンテナンスをバックアウトします。次に、CA CSM を再起動します。この処理には CA CSM 自体への新しい修正メンテナンスの APPLY が含まれます。 CA CSM 自体に新しい修正メンテナンスを APPLY する場合、CA CSM を再起動する前にメンテナンスを展開する必要があります。

CA CSM のバックアップおよびディザスタ リカバリ

障害発生に備えて、CA CSM 環境の定期的なバックアップの実施をお勧めします。

ディザスタ リカバリの処理を開始する前に、CA CSM によって管理されるすべての SMP/E 環境およびデータ セットをバックアップします。

ディザスタ リカバリを実行する場合は、以下の手順に従います。

1. CA CSM が管理するすべての SMP/E 環境をリカバリします。
2. CA CSM 自体をリカバリします。

CA CSM が最初にインストールされた同じ環境に、CA CSM がリカバリされる必要があります。 すなわち、リカバリ システムの以下の設定は、元のシステムのものと同じである必要があります。

- TCP/IP ポート、DASD、HLQ などのオペレーティング システム設定
- CA CSM に必要な APF 許可データ セットの設定

- Java

  注: CA CSM がサポートするバージョンの Java である必要があります。
- 展開で指定されるシステムの TCP/IP 設定、ホスト名、IP アドレス、CAICCI SYSID

注:

- リカバリ システム用の SAF 設定には、CA CSM のセットアップ時に使用したすべての変更済み SAF 設定が含まれている必要があります。
- CA Datacom/DB ユーティリティ関数 DBUTLTY を使用した CA Datacom/MSM データベース データ領域の定期的なバックアップにより、お使いの製品へのアクセシビリティに影響を与える、スケジュールされたイベントまたはスケジュール外のイベント中の CA Datacom/MSM データを保護することができます。 データベースを再編成する方法の詳細については、「*Best Practices Guide*」を参照してください。

CA CSM のバックアップ方法

CA CSM のバックアップは、複数の手順で処理されます。

注: バックアップについては、ユーザのサイトと環境にとって適切な方法を選択し、使用してください。 バックアップの管理は、ディザスタ バックアップ ルーチンの一部である必要があります。

以下の手順に従います。

1. CA CSM アプリケーション サーバ (P. 203)を停止します。
2. 以下のオペレーティング システム設定をバックアップします。
   - ポート、DASD、HLQ などのオペレーティング システムの設定
   - Java

     注: CA CSM がサポートするバージョンの Java である必要があります。
   - TCP/IP
   - SAF

   注: CA Datacom/MSM SVC は同じものになることが想定され、APF 許可されたデータ セットのリストは保存されます。

3. 展開ファイル システム、ソフトウェア カタログ ファイル システムなどを表すデータ セットの一覧を取得します。 データ セットはマウント ポイント テーブルの MP_DATASET 列に格納されます。

   注: データ セットの一覧を取得するため、SQL ステートメントを実行する JCL をサブミット (P. 75)できます。

4. CA Datacom/MSM サーバおよび MUF を停止します。

5. 以下の CA CSM データ セットをバックアップします。

   - マウント ポイントを表すデータ セット

     これらのマウント ポイントに個別のファイル システムを割り当てなかった場合は、以下の手順を実行します。

     a. 以下のファイル システムでマウントされたファイル システムがある場合は、すべてマウント解除します。

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

     b. /u/users/msmserv に相当するディレクトリ構造をバックアップします。

   - マウントポイント テーブルから取得したすべてのデータ セット。
   - オプション ファイル（MSMSetupOptionsFile.properties）で指定された HLQ（CSIHLQ、TargetHLQ、DlibHLQ、DatabaseHLQ、RunTimeMVSHLQPrefix）の下のすべてのデータ セット。

SQL ステートメントを実行する JCL

以下のサンプルは、マウントポイント テーブルのコンテンツを検出する SQL ステートメントを実行するためにサブミットできる JCL の例です。

```
//*******************************************************************************
//*******************************************************************************
//*                                                                             *
//*JOBLIB DD DSN=HLQ.CUSLIB replace HLQ with HLQ of your CA CSM installation  *
//*          DSN=HLQ.CAAXLOAD replace HLQ with HLQ of your CA CSM installation*
//*                                                                             *
//*******************************************************************************
//*******************************************************************************
```

```
//B2UP     OUTPUT DEST=LOCAL,JESDS=ALL,DEFAULT=Y,
//         PAGEDEF=32D3,CHARS=GT20,FORMDEF=P2B111
//JOBLIB   DD DSN=HLQ.CUSLIB,
//         DISP=SHR
//         DD DSN=HLQ.CAAXLOAD,
//         DISP=SHR
//         DD DSN=SYSDEV.CCS.LINKLIB,
//         DISP=SHR
//         DD DSN=CEE.SCEERUN,DISP=SHR
//         DD DSN=CEE.AIGZMOD1,DISP=SHR
//*
//SQLEXEC  EXEC PGM=DBSQLPR,
//       PARM='prtWidth=1500,inputWidth=80'
//SYSUDUMP DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//STDERR   DD  SYSOUT=*
//STDOUT   DD  SYSOUT=*
//OPTIONS  DD  *
AUTHID=CASWMGT
/*
//SYSIN    DD  *
   SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
/*
```

以下のサンプルは、マウントポイント テーブルのコンテンツを検出するために JCL をサブミットした後に受信する出力の一部です。

```
Command Line Options

____________________
INPUTWIDTH=80
PRTWIDTH=1500
Option File Options

____________________
AUTHID=CASWMGT
INPUT STATEMENT:
SELECT MP_DATASET
   FROM MOUNTPOINT WHERE NOT MP_TYPE='PRODUCT' OR MP_TYPE IS NULL;
MP_DATASET
VARCHAR(45)

_____________________________________________
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
...
```

入力ステートメントの後に戻されるデータ セットは、バックアップする必要があります。

```
OMVSUSR.CAMSM.APLROOT
OMVSUSR.CAMSM.LJWK
OMVSUSR.CAMSM.MSMT1
OMVSUSR.CAMSM.MSMT3
```

バックアップからの CA CSM のリカバリ方法

バックアップから CA CSM をリカバリするには、以下の手順を実行します。

1. オペレーティング システム設定をリカバリします。
2. CA CSM データ セットをリカバリします。
3. CA CSM を起動します (P. 65)。

CA CSM の停止

CA CSM を停止する場合（たとえばメンテナンス中など）、CA CSM の開始 (P. 65)とは逆の順序で CA CSM を停止します。

以下の手順に従います。

1. 以下の z/OS システム コマンドを入力します。

   ```
   P MSMTC
   ```

   CA CSM アプリケーション サーバ (P. 203)は正常に終了し、以下のメッセージがシステム コンソールに表示されます。

   ```
   MSM0011I CA CSM HAS TERMINATED SUCCESSFULLY
   ```

   注: このメッセージが表示されない場合、CA CSM は稼働停止に失敗しています。 以下のコマンドを使用して、強制的にシャットダウンします。

   ```
   F MSMTC,APPL=FORCESHUTDOWN
   ```

強制シャットダウンが完了した後、以下のメッセージがシステム コンソールに表示されます。

```
MSM0012W CA CSM TERMINATION WAS FORCED
```

重要: 強制的にシャットダウンする場合、データの一部が失われる可能性があります。そのため、標準的な停止方法が作動しない場合のみ、この方法を使用してください。

CA CSM アプリケーション サーバが停止した後、Tomcat ジョブが停止します。

2. MSMDBSVP JCL メンバをサブミットするか、または MSMDBSRP PROCLIB メンバを開始します。

   CA Datacom/MSM サーバが停止します。

   注: あるいは、セキュリティ アクセスに基づいて以下のコマンドを入力することもできます。 *started_task_name* を MUF データベース サーバ ジョブ名および MUF ジョブ名に置換します。

   - z/OS の場合：

     ```
     F started_task_name,EOJ
     ```

   - CA SYSVIEW の場合：

     ```
     MVS F started_task_name,EOJ
     ```

   - System Display and Search Facility （SDSF）の場合：

     ```
     /F started_task_name,EOJ
     ```

3. MSMMUFP ジョブまたはスターティッド タスクをサブミットします。

   MUF が停止し、CA CSM は稼働停止します。

第 5 章: 追加の管理タスク

このセクションには、以下のトピックが含まれています。

現在のユーザへのメッセージ送信 (P. 79)
Java ホーム ディレクトリの再割り当て (P. 83)

現在のユーザへのメッセージ送信

z/OS MODIFY コマンドを使用して、CA CSM Web ベース インターフェースにログインしている 1 人のユーザまたはすべてのユーザにメッセージを送信できます。 たとえば、メンテナンスのために CA CSM をシャットダウンする前に、CA CSM アプリケーション サーバにログインしているすべての CA CSM ユーザにメッセージを送信し、CA CSM がシャットダウンしようとしていることを知らせることができます。

現在ログインしているすべての CA CSM ユーザにメッセージを送信するには、以下のコマンドを入力します。

```
/F jobname,APPL=MSG,message text
```

注: 1 人のユーザにメッセージを送信するには、以下のように TSO ユーザ ID を追加します。

```
/F jobname,APPL=MSG,TSOuserID,message text
```

jobname

システムの CA CSM アプリケーション サーバの名前を指定します。

APPL=MSG

CA CSM アドレス空間に対して指定し、この修正リクエストをメッセージ送信リクエストとして処理します。

TSOuserID

（オプション） メッセージを送信する対象のユーザの TSO ユーザ ID を指定します。TSO ユーザ ID が指定されていない場合、メッセージはサーバに現在ログインしているすべてのユーザに送信されます。

message_text

メッセージの本体を指定します。自由形式のメッセージ テキストを入力し、CA CSM アプリケーション サーバにログインしているすべてのユーザに表示するか、または TSO ユーザ ID が指定されている場合は、1 人のユーザに表示します。

制限 : メッセージ テキスト自体に引用符を使用している場合でも、カンマを含めないでください。

ユーザにメッセージを送信するサンプル JCL

以下のサンプル JCL は、CA CSM にログインしているすべてのユーザにメッセージを送信する方法、および DOEJON01 の TSO ユーザ ID を持つ 1 人の CA CSM ユーザにメッセージを送信する方法を示します。

Proclib メンバ INFORMSM は以下のとおりです。

```
//*******************************************************************************
//*****                                                                      *****
//*****  Send Message to CA CSM users                                       *****
//*****                                                                      *****
//*****  SERVER= is the number of the server to receive message.           *****
//*****  MSMMSG= is the message you want sent to the server user(s)        *****
//*****                                                                      *****
//*****  EXAMPLE JCL shown below how to send message to ALL users          *****
//*****                                                                      *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                        *****
//*****  //          EXEC INFORMSM,SERVER=2,                               *****
//*****  // MSMMSG='CA CSM - IS SHUTTING DOWN - RESTART REQUESTED'         *****
//*****                                                                      *****
//*****  EXAMPLE JCL shown below how to send message to a CA CSM User      *****
//*****                                                                      *****
//*****  /*JOBPARM SYSAFF=MACHINE31                                        *****
//*****  //          EXEC INFORMSM,SERVER=2,                               *****
//*****  // MSMMSG='DOEJON01,TEST MESSAGE FROM JCL'                        *****
//*****                                                                      *****
//*******************************************************************************
//*
//INFORMSM  PROC  MSMMSG=,
//             SERVER=
//*
//OPSCMD   EXEC PGM=OPSCMD,PARM='F MF2T&SERVER.SRV,APPL=MSG,&MSMMSG.'
//*
//OPS$OPSP DD DUMMY         Direct request to production subsystem OPSP
//*
//INFORMSM  PEND
//*
```

メッセージを送信する JCL は以下のとおりです。

```
//INFORM5S  JOB (129300000),'Inform CA CSM user',
//        COND=(4,LT),
//        CLASS=A,
//        MSGCLASS=X,
//        NOTIFY=&SYSUID,
//        MSGLEVEL=(1,1)
//*
/*JOBPARM SYSAFF=MACHINE31
//*
// JCLLIB ORDER=(MF20.MSM.PROCLIB)
//*
//*********************************************************************
//*****                                                          *****
//*****  send message to CA CSM server user(s)                  *****
//*****                                                          *****
//*********************************************************************
//*
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server is closing down in fifteen minutes       '
//          EXEC INFORMSM,SERVER=5,
// MSMMSG='CA CSM - Server will be restarted soon after             '
//
//*
// MSMMSG='DOEJON01, send a message to a user on a CA CSM server    '
//*
```

実行中タスクの確認

CA CSM を停止する前に、実行中のタスク、およびそれらの急な終了による影響について把握してください。 それらのタスクを開始したユーザは、現在 CA CSM にログインしていない可能性があります。

以下の手順に従います。

1. CA CSM Web ベース インターフェースにログインし、［Tasks］タブをクリックし、［Current Tasks］サブタブが選択されていることを確認します。

   そのユーザのタスクのみを表示した［Tasks］ページが表示されます。

2. ［Show］ドロップダウン リストから［All tasks］を選択します。

   すべてのタスクが一覧表示されます。

3. タスクのステータスを確認し、Executing ステータスのタスクがある場合は、CA CSM を停止する前にそのタスクの所有者に連絡をとることを検討してください。

Java ホーム ディレクトリの再割り当て

Java の新しいマイナー バージョンを別のディレクトリにインストールして、古いバージョンを保存するときなど、Java ホーム ディレクトリを再割り当てすることがあります。Java ディレクトリを変更する場合は、以下の場所の Java のパスを修正します。

- SAMPLIB（MSMLIB）メンバの JAVA_HOME 変数の値を変更します。

  例： 以下のサンプル SAMPLIB（MSMLIB）メンバの、*original_path* を新しいパスに置換します。

  ```
  export JAVA_HOME=original_path
  ```

- Java ホーム ディレクトリを指す CA CSM CSI の SMPJHOME DDDEF 値を変更します。CA CSM CSI は CSIHLQ.SMPCSI.CSI にあります。グローバル（GLOBAL）ゾーン、ターゲット（CAIT0）ゾーン、および配布（CAID0）ゾーンの SMPJHOME DDDEF 値を変更します。 UCLIN ステートメントを使用して、SMPJHOME DDDEF 値を変更します。

  例： この UCLIN ステートメントを使用して、ゾーンの変数を各ゾーン名（CAID0、CAIT0、GLOBAL）に置換することにより、すべての CA CSM CSI ゾーンの SMPJHOME DDDEF 値を変更します。

```
SET
BOUNDARY(zone).
UCLIN.
REP  DDDEF(SMPJHOME)
     PATH('new_path').
ENDUC.
```

注: ユーザが MSMTC ジョブを開始した後は、ジョブ ログ メッセージ内の JAVA_HOME パスは、CA CSM CSI 内の SMPJHOME DDDEF のパスと以下のように一致させる必要があります。

```
JVMJZBL1006I JAVA_HOME = new_path
```

- *MSMPATH*/CEGPHFS ディレクトリにある MSMSetupOptionsFile.properties オプション ファイル内の JAVAPATH オプションを変更します。

  例： 以下の MSMSetupOptionsFile.properties オプション ファイル のサンプルで、*original_path* を新しいパスに置換します。

  ```
  JAVAPATH=original_path
  ```

第 6 章: SCS アドレス空間管理

*SCS アドレス空間*は、特別に定義された場所で、出力およびコンソールのトラフィックを照会するためのシステム レジストリやコマンドが存在する、オペレーティングシステム内の場所です。 SCS アドレス空間は、ターゲットの z/OS システム間で設定を実装するのに必要なサービスおよび処理を提供します。SCS の処理をサポートするための各ターゲット システムは、SCS アドレス空間を実行する必要があります。

このセクションには、以下のトピックが含まれています。

SCS アドレス空間操作の考慮事項 (P. 85)
暗号化通信 (P. 88)
オペレータ通信インターフェース (P. 94)
JCL EXEC ステートメント PARM キーワードおよび START コマンド パラメータ (P. 105)
パラメータ ライブラリ (P. 107)
SCS アドレス空間メッセージ ログ（SCSLOG） (P. 115)
汎用トレース機能 (P. 119)

SCS アドレス空間操作の考慮事項

このセクションには、以下のトピックが含まれています。

許可プログラム機能 (P. 86)

補助アドレス空間 (P. 87)

許可プログラム機能

重要: SCS アドレス空間のドキュメントでは、すべての SYS1.PARMLIB データ セットへの参照は、論理的な PARMLIB 連結で定義されている任意のデータ セットを示します。

許可プログラム機能（APF）を使用して、重要なシステム機能を使用するプログラムを特定します。 SCS アドレス空間は、APF 許可されたジョブ ステップとして開始される必要があります。SCS アドレス空間ロード ライブラリは、SCS アドレス空間が開始される各 z/OS システム上で APF 許可される必要があります。

確実に SCS アドレス空間を APF 許可されたジョブ ステップとして開始するには、SCS アドレス空間 STEPLIB 連結に含まれるすべてのライブラリを APF 許可します。 APF 許可されていない連結にライブラリを格納すると、ライブラリ連結全体がその APF 許可を失います。

APF リストは SYS1.PARMLIB メンバ PROG*xx* にあります。 このリストには、APF 許可されたライブラリの名前が含まれています。リスト内のエントリの順序は重要ではありません。

動的な形式で PROG*xx* メンバを使用する場合は、z/OS コマンド SET PROG=*xx* を発行できます。変更は次の IPL の前に有効になります。

注: APF リストの詳細については、「*IBM Initialization and Tuning Reference*」を参照してください。

補助アドレス空間

最初の補助アドレス空間は、SCS アドレス空間によって実行されるサービス リクエストから作成されます。 必要に応じて追加の補助アドレス空間が作成されます。

補助アドレス空間は、同時設定リクエストのレベルに応じて、動的に作成、管理されます。 補助アドレス空間は、SCS アドレス空間の代わりにサービス リクエストを処理します。

SCS アドレス空間は、設定を実行しているユーザの代わりにサービス リクエストを実行します。 SCS アドレス空間は補助アドレス空間を作成し、それらがアクティブになったとき、補助アドレス空間に対してサービス リクエストをスケジュールします。 補助アドレス空間はリクエストを実行し、その結果は SCS アドレス空間に返されます。

補助アドレス空間の操作

SCS アドレス空間は必要に応じて自動的に補助アドレス空間を作成し、リクエストをスケジュールします。 補助アドレス空間は、SCS アドレス空間が作成するワークロード マネージャ（WLM）依存エンクレーブで実行されます。 スケジュールされたサービスがある場合、すべての SCS 補助アドレス空間はアクティブ状態のままになります。 実行するリクエストがそれ以上ないとき、アクティブではない補助アドレス空間は停止します。

注: SCS アドレス空間は、処理される同時サービス リクエストの数に応じて、最大 20 までの数の補助アドレス空間を作成および管理します。

SCS アドレス空間パラメータを指定して、同時にアクティブな補助アドレス空間の最大数を 20 未満の数に制限できます。

補助アドレス空間に対して、自動化操作を実行する必要はありません。これは、SCS アドレス空間が動的にその操作を開始するからです。 非常に稀ですが、SCS アドレス空間が失敗すると、すべての補助アドレス空間は停止します。

暗号化通信

SCS アドレス空間との暗号化通信を有効にするには、以下のいずれかの暗号化方式を設定します。

- IBM System Secure Socket Layer（SSL）
- IBM Application Transparent Transport Layer Security（AT-TLS）

Web ベース インターフェース リモート ホストから SCS アドレス空間に接続する場合、アドレス空間は System SSL または IBM AT-TLS の使用を検出します。 どちらの方式も検出されない場合、Web ベース インターフェースとの通信はクリア テキストで実行されます。

SSL 伝送サポートの実装

SCS アドレス空間をセットアップして、以下の*いずれか*を使用します。

- 階層型ファイル システム（HFS）にあるキー ストア ファイルを使用した、IBM System Secure Socket Layer （SSL）ツールキット。

  注: シェル プロンプトで OMVS の下のプログラム *gskkyman* を実行します。このプログラムの実行により、HFS 上でキー ストア ファイルが作成され、自己署名の認証局証明書が生成され、サーバ証明書が生成されます。

- 外部セキュリティ マネージャ（ESM）

  注: ESM のコマンドを実行することによりサーバ証明書を生成します。

キー ストア ファイルの作成

SSL を使用するために SCS アドレス空間をセットアップする際に、zFS または HFS 上でキー ストア ファイルを作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Create new database］を選択し、新しいキー ストア ファイルまたはデータベースへのパスおよびファイル名を入力します。

   注: パスとファイル名は、書き込み可能なパスおよびファイル名である必要があります。

3. データベース パスワードを入力し、パスワードの有効期限を日数で入力します。

   注: パスワードに有効期限を設けない場合は、ENTER キーを押します。

4. データベース レコード長に「**5000** 」を入力し、データベース モードに「**0**」を入力します。
5. キー データベースが作成されたことを伝える確認通知を待ちます。
6. ［Exit program］を選択します。

   キー ストア ファイルが作成されます。

自己署名の認証局証明書の作成

SSL を使用するために SCS アドレス空間をセットアップする際に、自己署名の認証局証明書を作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力し、データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。

3. ［Create self-signed certificate］を選択します。
4. 1024 ビット RSA キーの認証局証明書を選択し、［SHA-512］を選択します。

   注: 1024 ビット RSA キーの認証局証明書を選択すると、認証局が作成されます。

5. 自己署名の認証局証明書のラベルを入力し、共有名を入力します。

   注: 共有名はラベルと同じでかまいません。

6. プロンプトに表示された、証明書の所有権に関するデータを入力します。 所有権には以下のデータが含まれます。
   - 組織単位
   - 編成
   - 組織の国、都道府県、市町村
7. 証明書が有効な日数を入力し、「**0**」を入力して続行します。

8. 証明書が作成されるまで待機します。
9. ［Exit program］を選択します。

   自己署名の認証局証明書が作成されます。

サーバ証明書の作成

SSL を使用するために SCS アドレス空間をセットアップする際に、サーバ証明書を作成できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力し、データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
3. ［Manage keys and certificates］を選択し、使用する認証局証明書の番号を入力します。

   注: 事前に作成した番号を使用できます。
4. ［Create a Signed Certificate and Key］を選択し、1024 ビット RSA キーのユーザ証明書またはサーバ証明書を選択します。
5. サーバ証明書のラベルを入力し、共有名を入力します。

   注: 共有名はラベルと同じでかまいません。
6. プロンプトに表示された、証明書の所有権に関するデータを入力します。 所有権には以下のデータが含まれます。
   - 組織単位
   - 編成
   - 組織の国、都道府県、市町村
7. 証明書が有効な日数を入力し、「**0**」を入力して続行します。
8. 証明書が作成されるまで待機します。
9. ［Exit program］を選択します。

   サーバ証明書が作成されます。

デフォルト証明書としてのサーバ証明書の設定

SSL を使用するために SCS アドレス空間をセットアップする際に、サーバ証明書をデフォルト証明書として設定できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースのパスを入力します。
3. データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
4. ［Manage keys and certificates］を選択し、サーバ証明書のラベルの数を入力します。
5. オプションを選択し、キーをデフォルトとして設定します。
6. ［Exit program］を選択します。

   サーバ証明書がデフォルト証明書として設定されます。

認証局証明書のエクスポート

SSL を使用するために SCS アドレス空間をセットアップする際に、認証局証明書をエクスポートできます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースへのパスを入力します。
3. データベース パスワードを入力します。

   ［Key Management］メニューが表示されます。
4. ［Manage keys and certificates］を選択し、エクスポートする認証局証明書のラベルの数を入力します。
5. ［Export certificate to a file］を選択し、［Binary ASN.1 DER］を選択します。

6. 証明書をエクスポートするパス名およびファイルを入力し、Enter キーを押します。
7. ［Exit program］を選択します。

   認証局証明書がエクスポートされます。

データベース パスワードまたはキー ストア パスワードの stash ファイルへの格納

SSL を使用するために SCS アドレス空間をセットアップする際に、stash ファイルにデータベース パスワードまたはキー ストア パスワードを保存できます。

以下の手順に従います。

1. メインフレーム コンソールから、*gskkyman* を実行します。
2. ［Open database］を選択し、作成したデータベースのパスを入力します。
3. データベース パスワードを入力し、［Store Database Password］を選択します。

   database_*name*.sth ファイルは、データベース ファイルが格納されている場所に格納されます。
4. ［Exit program］を選択します。

   データベース パスワードまたはキー ストア パスワードが、stash ファイルへ保存されます。

Java キー データベースへの認証局証明書のインポート

SSL を使用するために SCS アドレス空間をセットアップする際に、認証局証明書を Java キー データベースへインポートできます。

以下の手順に従います。

1. Java SDK に付属の keytool プログラムをスーパーユーザ モードで実行します。
2. キー ストアのパスワードを入力します。

   デフォルト： changeit
3. 「yes」を入力し、証明書を信頼します。

   注: 証明書が正常に追加された場合、この設定は完了です。

   認証局証明書は Java キー データベースへインポートされます。

例: keytool プログラムの実行

以下のサンプルは、keytool プログラムの実行方法の例です。

```
keytool –import –trustcacerts –file /path/to/exported/ca/certificate –keystore
$JAVA_HOME/lib/security/cacerts
```

System SSL 使用のセットアップ

SCS アドレス空間が System SSL を使用するには、PDSE メンバの GSKSSL が以下の 2 つの方法のうち 1 つを使用して、プログラムにアクセスできる必要があります。

- 動的 LPA（PROG*xx* メンバ）への *pdsename*.SIEALNKE という名前の PDSE の追加。

  注: System SSL のセットアップの詳細については、IBM の「*z/OS Cryptographic Service System Secure Sockets Layer Programming*」を参照してください。
- SCS アドレス空間の開始に使用される JCL プロシージャを含む PROCLIB メンバの修正。 名前は一般的には MSMCPROC（P. 204）です。 STEPLIB の DD ステートメントを追加することによって、*pdsename*.SIEALNKE への参照を含めます。

SCS アドレス空間設定 XML に移動して、アドレス空間で SSL を有効にします。

認証局証明書およびサーバ証明書を作成したら、SCS アドレス空間の *MSMCPARM* という名前のパラメータ ファイルを修正します (P. 107)。

デフォルト： MSMCPARM

XML ドキュメントに SSL タグを配置し、キー ストア/データベース ファイルに keyring 属性を設定します。対応する stash ファイルに stashfile 属性を設定します。

XML ドキュメントの SSL 要素で keyring と stashfile を設定して SCS アドレス空間設定 XML を更新し、キーストア データベースおよびパスワードの stash ファイルを指すようにします。

AT-TLS 伝送サポートの実装

Application Transparent Transport Layer Security（AT-TLS）は z/OS のコンポーネントで、機密データを交換するが暗号化の手段が備わっていないアプリケーションに対し、暗号化サービスを提供します。 このサービスは、暗号化を行うための余計な API の呼び出しを追加することなく、アプリケーションに送信されるデータの暗号化を可能にします。

SCS アドレス空間で AT-TLS を使用するには、以下の作業を完了しておく必要があります。

- Communications Policy Agent の設定
- AT-TLS ポリシーの設定
- サーバ証明書および認証局証明書のインストール

注: IBM Policy Agent の詳細については、「*IBM z/OS V1R11 Communications Server TCP/IP Implementation Volume 4: Security and Policy-Based Networking*」を参照してください。

オペレータ通信インターフェース

z/OS オペレータ コマンドは、SCS アドレス空間の操作を制御するために使用されます。

オペレータ コマンドを発行できるユーザのグループを制御できます。 CA ACF2 for z/OS、CA Top Secret for z/OS または IBM RACF を使用し、一部またはすべてのコマンドの発行をユーザに許可または制限します。

オペレータ コマンドの使用を制御するには、SAF OPERCMDS クラスでプロファイルを作成します。

コマンドの説明文は、そのコマンドに対する権限の要件を説明します。ほとんどの場合、1 つ以上のレベルの権限が必要です。また、コマンドを発行するユーザには、指定されたすべてのアクセス権限が必要です。

SCS アドレス空間オペレータ コマンド

このセクションでは、SCS アドレス空間がサポートするコマンドを説明します。

START コマンド -- SCS アドレス空間を開始する

START コマンドは、SCS アドレス空間を開始します。 START または省略形の「S」を入力できます。 このコマンドを使用するには、*MVS.START.STC.procname* という名前の、SAF OPERCMDS クラス リソースに対する UPDATE 権限が必要です。

注: MSMCAUX プロシージャを手動で開始しないでください。 MSMCAUX プロシージャは SCS アドレス空間（MSMCPROC）によって開始されます。

START コマンドのガイドラインを以下に示します。

- START コマンドのパラメータ値は、JCL EXEC ステートメント PARM キーワードのパラメータ値をオーバーライドします。
- 2 つ以上のパラメータを持つキーワードをカンマまたはスペースで区切ります。
- 2 つ以上のサブパラメータを持つキーワードをカンマまたはスペースで区切ります。
- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（/*）でコメントを開始します。 （オプション）コメント終了区切り文字（*/）でコメントを終了します。
- 不正に指定されたパラメータは無視されます。

このコマンドの構文は以下の通りです。

```
Start procname[,,,(start_parameters)][,REUSASID=YES][,PARMS='exec_parameters']
```

procname

SCS アドレス空間を開始するために使用される JCL プロシージャが含まれているシステム PROCLIB メンバの名前を指定します。 名前は一般的には MSMCPROC (P. 204) です。

,,,(*start_parameters*)

（オプション） SCS アドレス空間用の START コマンド パラメータ (P. 105)を指定します。START コマンドのパラメータ値は、JCL EXEC ステートメントの PARM パラメータ値をオーバーライドします。

,REUSASID=YES

（オプション） z/OS が、再利用可能なアドレス空間識別子（ASID）を SCS アドレス空間に割り当てることを指定します。

,PARMS='*exec_parameters*'

（オプション） SCS アドレス空間の JCL EXEC ステートメントの PARM パラメータ (P. 105)を、指定したパラメータでオーバーライドすることを指定します。 指定する exec_parameter 値で、JCL EXEC ステートメントの PARM パラメータ値がオーバーライドされます。

例：SCS アドレス空間の開始

これらの例は、START コマンドを使用して、SCS アドレス空間を開始する方法を示しています。

```
S MSMCPROC,REUSASID=YES,PARMS='CONFIG(SCSPARMS)'
```

```
S MSMCPROC,,,(CONFIG(SCSPARMS)),REUSASID=YES
```

SCS アドレス空間の初期化

以下のメッセージを受信すると、SCS アドレス空間が初期化されます。

```
MSMC0002I SCS initialization complete. SYSNAME=system_name, CCINAME=CAICCI_name
```

以下のメッセージを受信すると、SCS アドレス空間は完全に稼働中になります。

```
MSMC0423I Task MSMCIENG database connection opened
MSMC0424I Task MSMCFCOM database connection opened
```

SCS アドレス空間が接続の待機中であることを確認するには、接続をリッスンし、以下のメッセージを探します。

```
MSMC0617I The SCS address space is now listening for connections on the UNIX socket
MSMC0618I The SCS address space is now listening for connections on the INET/INET6
socket, port nnnn
```

STOP コマンド - SCS アドレス空間の停止

STOP コマンドは、SCS アドレス空間の正常終了を開始します。 STOP または省略形の P を入力できます。 このコマンドを使用するには、CAMSMSCS.STOP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を指定します。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.STOP.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.STOP.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

このコマンドの構文は以下の通りです。

```
stoP jobname
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 204) です。

例: SCS アドレス空間の停止

この例は、STOP コマンドを使用して SCS アドレス空間を停止する方法を示します。

```
P MSMCPROC
```

MODIFY コマンド - SCS アドレス空間を変更します

MODIFY コマンドを使用して、SCS アドレス空間の操作を制御します。MODIFY または省略形の F を入力できます。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.*procname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.*jobname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

MODIFY コマンドは以下のとおりです。

- ABEND
- DUMP
- STOP

MODIFY コマンドの仕様を以下に示します。

- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（/*）でコメントを開始します。 （オプション）終了区切り文字（*/）でコメントを終了します。

- 2 つ以上のパラメータが指定されたキーワード（オプション値があるキーワード）をカンマまたはスペースで区切ります。
- 2 つ以上のサブパラメータを持つキーワードをカンマまたはスペースで区切ります。

  注: コメントがパラメータ文字列の最後にある場合、コメント終了区切り文字は省略可能です。

MODIFY ABEND コマンド - SCS アドレス空間の異常終了を開始する

MODIFY ABEND コマンドを使用して、SCS アドレス空間の異常終了を開始します。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.ABEND という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を指定します。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します

このコマンドの構文は以下の通りです。

```
modiFy jobname,ABEND
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 名前は一般的には MSMCPROC (P. 204) です。

例: MODIFY ABEND コマンドを使用して、SCS アドレス空間を修正する

この例は、MODIFY ABEND コマンドを使用して、SCS アドレス空間を修正する方法を示します。

```
F MSMCPROC,ABEND
```

MODIFY DUMP コマンド - SCS アドレス空間の SVC ダンプを収集する

MODIFY DUMP コマンドは、SCS アドレス空間の SVC ダンプを収集するために使用されます。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.DUMP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を指定します。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.*procname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.*jobname* という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

このコマンドの構文は以下の通りです。

```
modiFy jobname,DUMP[ASID(asid_list)]JOBNAME(job_list)[DSPNAME(dsp_list)]
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 204) です。

デフォルト： JOBNAME が指定されない場合は、SCS アドレス空間。

ASID（*asid_list*）

（オプション） ダンプに含める 1 つ以上のアドレス空間のアドレス空間識別子オペレータ入力 (P. 103)を指定します。

制限： 1 ～ 32767 の 10 進数の範囲または 1 ～ 7FFF の 16 進数の範囲

デフォルト： ASID パラメータが指定されない場合は、SCS アドレス空間。

JOBNAME(*job_list*)

ダンプに含める 1 つ以上のアドレス空間の名前を指定します。

注: *ジョブ名*には、疑問符（?）またはアスタリスク（*）のワイルドカード文字を含めることができます。疑問符は単一のマスク文字を意味します。 アスタリスクは 0 以上のマスク文字を意味します。

制限： 引用符で囲んだ文字列 *'abc'*、または囲んでいない文字列 *abc* で表される 1 ～ 8 文字。 区切り記号または区切り文字で終了を示します。

DSPNAME(*dsp_list*)

（オプション） ダンプに含める 1 つ以上のデータ空間のデータ空間識別子 (P. 104)を指定します。

デフォルト： DSPNAME が指定されていない場合、SCS アドレス空間が所有するデータ空間。

注: JOBNAME と DSPNAME のパラメータでワイルドカード文字を使用すると、ダンプに含めるアドレス空間を複数選択できるようになります。

例: MODIFY DUMP コマンドを使用して、SCS アドレス空間および補助アドレス空間をダンプする

この例は、MODIFY DUMP コマンドを使用して、SCS アドレス空間と補助アドレス空間をダンプする方法を示します。

```
F MSMCPROC,DUMP JOBNAME(MSMCPROC,MSMCAUX)
```

MODIFY STOP コマンド - SCS アドレス空間の正常終了の開始

MODIFY STOP コマンドを使用して、SCS アドレス空間の正常終了を開始します。 MODIFY または省略形の F を入力できます。 このコマンドを使用するには、CAMSMSCS.STOP という名前の SAF OPERCMDS クラス リソースに CONTROL 権限を指定します。

注: STOP コマンドと MODIFY STOP コマンドの実行結果はまったく同じになります。

権限を設定するには、SCS アドレス空間の開始方法に応じて、以下のいずれかの方法を使用します。

- SCS アドレス空間がスターティッド タスクとして開始された場合は、MVS.MODIFY.STC.procname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。
- SCS アドレス空間が開始されたジョブとして開始された場合は、MVS.MODIFY.JOB.jobname という名前の SAF OPERCMDS クラス リソースに UPDATE 権限を指定します。

このコマンドの構文は以下の通りです。

```
modiFy jobname,STOP
```

jobname

SCS アドレス空間スターティッド タスクまたは開始されたジョブ名を指定します。 一般的な名前は MSMCPROC (P. 204) です。

例: MODIFY STOP コマンドを使用して、SCS アドレス空間を修正する

この例は、MODIFY STOP コマンドを使用して、SCS アドレス空間を修正する方法を示します。

```
F MSMCPROC,STOP
```

SCS アドレス空間 ASID オペレータ入力の例

例

以下の例では、16 進数（A ～ F、0 ～ 9）で表された SCS アドレス空間 ASID オペレータ入力値を示します。

X'nnnn'

以下の例では、10 進数（0 ～ 9）で表された SCS アドレス空間 ASID オペレータ入力値を示します。

ddddd

結合時に、以下のアドレス空間が 15 を超える場合、最初の 15 のアドレス空間のみがダンプに含まれます。

- SCS アドレス空間
- ASID パラメータが指定するアドレス空間
- JOBNAME パラメータが指定するアドレス空間
- DSPNAME パラメータが指定するデータ空間を所有するアドレス空間

SCS アドレス空間のデータ空間識別子の入力

受理されるデータ空間識別子の入力指示子を以下に示します。

asid.name

ダンプに含める、所有するアドレス空間の 16 進数のアドレス空間識別子（ASID）、およびデータ空間の *data_space_name* を指定します。

制限： 1 ～ 7FFF の 16 進数の範囲（ASID）

デフォルト： SCS アドレス空間の ASID およびデータ空間

注: 指定する ASID 値の最初の文字は、10 進数にする必要があります。所有するアドレス空間の ASID の最初の有効桁が、10 進数でない場合は、ゼロから始まる ASID を指定します。

jobname.name

ダンプに含める、所有するアドレス空間の *ジョブ名*および *data_space_name* を指定します。 *ジョブ名*には、疑問符（?）またはアスタリスク（*）のワイルドカード文字を含めることができます。 疑問符は単一のマスク文字を意味します。 アスタリスクは 0 以上のマスク文字を意味します。

制限： 引用符で囲まれていない 1 ～ 8 文字

注: 256 を超えるデータ空間をダンプに含むことはできません。 パラメータでワイルド カード文字を使用すると、ダンプに含めるデータ空間を複数選択できるようになります。

ダンプに含まれていないアドレス空間がデータ空間を所有している場合、ASID のアドレス空間をダンプに含まれているアドレス空間のリストに追加します。 最大 15 のアドレス空間が許可されています。 アドレス空間の制限により、256 以上のデータ空間の指定はできません。

JCL EXEC ステートメント PARM キーワードおよび START コマンド パラメータ

SCS アドレス空間のパラメータは、パラメータ ライブラリ メンバで指定されます。SCS アドレス空間パラメータは以下の要素で指定されることもあります。

- アドレス空間スタートアップ JCL 内の JCL EXEC ステートメントの PARM キーワード パラメータ
- SCS アドレス空間の開始に使用される START コマンド。

JCL EXEC ステートメントの PARM キーワード パラメータ、および START コマンドで指定できるパラメータはまったく同じです。

これらの代替方法のいずれかを使用して SCS アドレス空間パラメータを指定する場合、以下のガイドラインに従ってください。

- START コマンドのパラメータ値は、JCL EXEC ステートメント PARM キーワードのパラメータ値をオーバーライドします。
- 2 つ以上のパラメータを持つキーワードをカンマまたはスペースで区切ります。
- 2 つ以上のサブパラメータを持つキーワードをカンマまたはスペースで区切ります。
- パラメータは、キーワードのパラメータとして指定されます。 キーワードのサブパラメータは位置パラメータにすることができます。
- パラメータは、任意の順序で指定できます。
- パラメータ文字列には、スペースがある場所であればどこにでもコメントを含めることができます。 コメント開始区切り文字（/*）でコメントを開始します。 必要に応じてコメント終了区切り文字（*/）でコメントを終了します。
- 不正に指定されたパラメータは無視されます。

JCL EXEC ステートメントの PARM キーワード パラメータおよび START コマンドと共に使用されるパラメータを以下に示します。

CONFIG(*name)*

SCS アドレス空間設定パラメータが含まれるパラメータ ライブラリ メンバの名前を指定します。

制限： 引用符で囲んだ文字列 *'abc'*、または囲んでいない文字列 *abc* で表される 1 ～ 8 文字。 区切り記号または区切り文字で終了を示します。

デフォルト： CONFIG が指定されていない場合、MSMCPARM。

ROUTCDE(*routing code list*)

経路指定コード、または WTO メッセージに割り当てられる経路指定コードの範囲を指定します。

ダッシュ（-）で区切られた 2 つの値によって、経路指定コードの包括的な範囲を指定します。

指定された経路指定コードは、各メッセージに定義された特定の経路指定コードに追加されます。

制限： 1 ～ 128

例： *ddd*（*d* は有効な 10 進数（0 ～ 9））

CASE(MIXED|UPPER)

WTO のメッセージを大小混合文字、または大文字のみを使用して書き込むことを指定します。

MIXED

WTO のメッセージを大文字と小文字の混合で書き込むことができます。

UPPER

WTO のメッセージを大文字を使用して書き込むことができます。

デフォルト： MIXED

DAE(YES|NO)

DAE ダンプ抑制を許可するか禁止するかを指定します。

YES

DAE ダンプ抑制は許可されます。

NO

DAE ダンプ抑制は禁止されます。

デフォルト： YES

パラメータ ライブラリ

SCS アドレス空間パラメータは、パラメータ ライブラリのメンバで設定パラメータとして指定されます。

パラメータ ライブラリは、SCS アドレス空間の JCL プロシージャ内の MSMPARM DD ステートメントに割り当てられたデータ セット、または複数のデータ セットです。

パラメータ ライブラリは、区分データ セットまたは区分データ セットの連結である必要があります。また各区分データ セットには可変長レコードが必要です。 各パラメータ ライブラリ メンバには、アドレス空間パラメータを指定し、さまざまな要素を含んだ XML ドキュメントがあります。

SCS アドレス空間の複数インスタンス用の共通設定パラメータを使用して簡素化するために、パラメータ ライブラリのメンバの設定パラメータに z/OS のシステム記号を含めることができます。

注: CA CSM には MSMCPARM パラメータ ライブラリ メンバが用意されており、そのメンバにはデフォルトの SCS アドレス空間パラメータが含まれています。

MSMCPARM メンバ

アドレス空間パラメータを指定する MSMCPARM メンバ ドキュメントに、以下の要素を含めることができます。

データ リカバリ パラメータ

データ リカバリ用にディスク記憶域の SCS アドレス空間の使用と関連するパラメータを設定します。 このパラメータは、リカバリ用に既存データを保存するために作成されたデータ セットを割り当てるときに使用されます。

データ リカバリ パラメータは、以下の属性を使用して指定されます。

dsnhlq

データ リカバリ用に作成されたデータ セットの割り当て時に使用される、データ セット名の高レベル修飾子を指定します。

制限： 1 ～ 17 バイト。 値には静的および動的システム記号、およびインストールで定義された静的システム記号を含めることができます。

注: システム記号の一覧については、IBM の「*z/OS MVS Initialization and Tuning リファレンス*」を参照してください。

（オプション） *&SYSUID*

どのデータ セットがリカバリ用に作成されたかという設定リクエストを開始した CA CSM ユーザのユーザ ID を指定します。

制限： アンパサンド文字（&）は XML ドキュメントの属性値のため、リテラルとして指定できません。 この文字は、後続の文字を制御シーケンスに変換するために、文字列「*&*」を使用して変換する必要があります。

例： '&SYSNAME..MSM', dsnhlq='&SYSNAME..MSM'

デフォルト： &SYSUID..MSMDATA

単位

データ リカバリ用に作成された z/OS データ セットの割り当て時に使用される、ユニット名を指定します。

制限： 1 ～ 8 バイト

デフォルト： なし

volser

データ リカバリ用に作成されたデータ セットの割り当て時に使用される、ボリューム シリアル番号を指定します。

制限： 1 ～ 6 バイト。 シリアル番号の文字は英文字、各国文字、またはハイフンである必要があります。

デフォルト： なし

mgmtclas

データ リカバリ用に作成されたデータ セットの割り当て時に使用される、SMS 管理クラスを指定します。

制限： 1 ～ 8 バイト。 クラス名の先頭文字は、英文字または各国文字である必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： なし

storclas

データ リカバリ用に作成されたデータ セットの割り当て時に使用される、SMS ストレージ クラスを指定します。

制限： 1 ～ 8 バイト。 クラス名の先頭文字は、英文字または各国文字である必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： なし

TCP/IP

CA CSM の他のコンポーネントと通信するために、SCS アドレス空間と TCP/IP 間のインターフェース用のアドレス空間パラメータを指定します。

TCP/IP パラメータは以下の属性を使用して指定されます。

ipaddr

SCS アドレス空間が他の CA CSM コンポーネントからの TCP 接続要求を受け付けるインターフェースの IP アドレスを指定します。

制限： 標準のドット区切り 10 進表記法を使用した IPv4 アドレス。

（オプション）RFC 4291 の IPv6 アドレス体系で定義されている標準のテキスト フォームの 1 つを使用した IPv6 アドレス

例 1： 0.0.0.0

例 2： ::

注: IPv4 の未指定のアドレス 0.0.0.0 は、SCS アドレス空間がすべての IPv4 インターフェースからの TCP 接続要求を受け入れることを指示するために使用されます。 IPv6 の未指定のアドレス :: は、SCS アドレス空間がすべての IPv4 および IPv6 インターフェースからの TCP 接続要求を受け付けることを指示するために使用されます。

デフォルト： ::

port

SCS アドレス空間が、他の CA CSM コンポーネントからの TCP 接続要求をリッスンするために使用するポート番号を指定します。

制限： 65535

デフォルト： 49152

コンソール

z/OS コマンドの発行、コマンド応答の受信、および非送信請求メッセージ トラフィックの受信を行う拡張 MCS コンソールの SCS アドレス空間の使用と関連するパラメータを設定します。

コンソール パラメータは、以下の属性を使用して指定されます。

prefix

拡張 MCS コンソール名の作成に使用されます。

制限： 1 ～ 5 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： CAMSM

auth

拡張 MCS コンソールが z/OS コマンドを発行するための権限を指定します。

割り当てられた権限により、コンソールから入力できるコマンドが指定されます。 空白スペースまたはカンマで複数の値を区切ります。

コンソールから以下の値のうち 1 つ以上を入力します。

MASTER

コンソールがマスタ コンソールとして動作することを可能にし、そのコンソールがすべての MVS コマンドを発行します。

ALL

コンソールによる、システム制御コマンド、入力および出力コマンド、コンソール制御コマンドおよび情報提供コマンドの発行が可能になります。

SYS

コンソールによる、システム制御コマンドおよび情報提供コマンドの発行が可能になります。

IO

コンソールによる、入力および出力コマンド、および情報提供コマンドの発行が可能になります。

CONS

コンソールによる、コンソール制御コマンドおよび情報提供コマンドの発行が可能になります。

INFO

コンソールによる、情報提供コマンドの発行が可能になります。

デフォルト： INFO

注: SYS、IO および CONS は、任意の組み合わせで指定できます。 他はすべて、排他関係にあります。

特定の権限レベルでコンソールから入力できるコマンドについての詳細については、IBM の「*z/OS MVS System Commands Reference*」を参照してください。

注: セキュリティ製品の設定は、セキュリティ製品が保護する z/OS コマンド用のコンソール コマンド権限設定をオーバーライドします。たとえば CA ACF2 for z/OS は、OPERCMDS クラスがアクティブの場合、コマンドを保護するためのプロファイルが定義されます。

SAF

System Authorization Facility （SAF）への SCS アドレス空間インターフェースに関連するパラメータを設定します。

SAF パラメータは以下の属性を使用して指定されます。

application

SCS アドレス空間に割り当てられるアプリケーション名を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： MSMCAPPL

requestor

サブシステムに存在する一連の制御ポイント内で一意の制御ポイントを割り当てる、SCS アドレス空間に割り当てられる名前を指定します。

注: リクエスタ名を指定し、かつ IBM RACF がインストールされている場合、IBM RACF ルータ テーブルを一致するエントリで更新してください。 テーブルを更新しない場合、IBM RACF 処理が省略されます。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： なし

subsystem

SCS アドレス空間に割り当てられるサブシステム名、バージョンおよびリリース レベルを指定します。

注: サブシステム名を指定し、かつ IBM RACF がインストールされている場合、IBM RACF ルータ テーブルを一致するエントリで更新してください。 テーブルを更新しない場合、IBM RACF 処理が省略されます。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： なし

クラス

リソース プロファイルで CA CSM がセキュリティ ルールに使用するリソース クラス名を指定します。

制限： 1 ～ 8 バイト。 名前の文字はすべて英数字または各国文字にする必要があります。

デフォルト： CAMSM

SSL

System SSL Cryptographic Services への SCS アドレス空間インターフェースと関連するパラメータを設定します。

SSL パラメータは以下の属性を使用して指定されます。

keyring

リモート システムからデータを暗号化するために使用されるキー リング データベース ファイルのパスおよびファイル名、または CA ACF2 for z/OS、CA Top Secret for z/OS、IBM RACF などの外部セキュリティ マネージャで SCS アドレス空間に割り当てられたユーザ ID に対して定義された SAF キー リングのラベルを指定します。

デフォルトの証明書を取得してクライアント側に送り、通信用の接続を保護する処理を開始するために使用されます。

デフォルト： なし

stashfile

keyring 属性がキー リング データベース ファイルのパスおよびファイル名に設定される場合、stashfile のパスおよびファイル名を指定します。

stashfile には、キー リング データベース ファイルにアクセスするためのパスワードが含まれています。

制限： keyring 属性がキー リング データベース ファイル名に設定されている場合は必須です。

デフォルト： なし

AUX

SCS AUX アドレス空間に関連付けるパラメータを設定します。

SCS AUX アドレス空間パラメータは、以下の属性を使用して指定されます。

procname

SCS AUX アドレス空間用のソース JCL を含んだ、JCL プロシージャ ライブラリ メンバの名前を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： MSMCAUX (P. 204)

jobname

SCS AUX アドレス空間に割り当てられるジョブ名を指定します。

制限： 1 ～ 8 バイト。 最初の文字は、英文字または各国文字にする必要があります。 残りの文字は、英数字または各国文字にする必要があります。

デフォルト： ソース JCL がプロシージャの場合は、JCL プロシージャ ライブラリ メンバ名、またはソース JCL がジョブの場合は、JOB ステートメントで割り当てられるジョブ名。

reusasid

SCS AUX アドレス空間に対して、再利用可能な ASID を要求するかどうかを決定します。

SCS AUX アドレス空間は、以下のいずれかの値を受け取ります。

YES

DIAG*xx* PARMLIB メンバに REUSASID（YES）も指定されている場合、SCS AUX アドレス空間に再利用可能な ASID が割り当てられます。

NO

SCS AUX アドレス空間には、再利用可能な ASID は割り当てられません。

デフォルト： YES

注: CA Technologies 製品の設定で使用される製品またはプログラムに、再利用可能な ASID を使用するためのアップグレードが実行されていない場合、再利用可能な ASID を使用するとシステム 0D3 の異常終了（ABEND）が発生します。

ASID の再利用の詳細については、IBM の「*z/OS MVS Programming: Extended Addressability Guide*」を参照してください。

maxactive

同時にアクティブな SCS AUX アドレス空間の最大数を指定します。

制限： 1 ～ 20 の数字

デフォルト： 20

SCS アドレス空間メッセージ ログ（SCSLOG）

SCS アドレス空間メッセージ ログ（SCSLOG）は、SCS アドレス空間によって書き込まれる、すべてのメッセージの詳細ログです。

z/OS ハードコピー メッセージ ログに書き込まれる SCS アドレス空間メッセージは、SCSLOG にも書き込まれます。さらに、SCSLOG はより詳細なメッセージに使用され、これは問題の診断に役立ちます。 従って、SCSLOG は SCS アドレス空間のアクティビティに関する、より完全な記録になります。

SCSLOG は、z/OS UNIX System Services（USS） の syslog デーモンを使用して実行されます。 syslog デーモンは z/OS システム製品の一部です。 syslog デーモンは、USS の syslogd コマンドを使用して明示的に開始する必要があります。

注: syslog デーモンの詳細については、IBM の「*z/OS Communications Server: IP Configuration Guide*」および「*z/OS Communications Server: IP Configuration Reference*」を参照してください。

syslog デーモンの設定

設定ファイルにより、syslog デーモン（syslogd）の処理が制御されます。

デフォルト： `/etc/syslog.conf`

設定ファイル内のステートメントにより、ログ記録ルール、およびログ メッセージの出力先が定義されます。syslog デーモン設定ファイルでログ記録ルールを定義し、特定の送信先に SCS アドレス空間メッセージを送信します。

ログ記録ルールは、ファシリティ名と優先度コードを使用して定義されます。 メッセージを生成するプログラムのユーザ ID およびジョブ名も、ログ記録ルールで指定することができます。

注: AUX アドレス空間のメッセージは、SCS アドレス空間で実行中のプロセスによって syslog デーモンに書き込まれています。 SCS アドレス空間のジョブ名用のログ記録ルールのみを定義してください。AUX アドレス空間のジョブ名用のログ記録ルールは必要ありません。

syslog デーモンに書き込まれたすべての SCS アドレス空間メッセージは、ファシリティ名として「user」を指定します。

syslog デーモンに書き込まれた各 SCS アドレス空間メッセージは、以下のいずれかの優先度コードを指定します。

info

この優先度コードのメッセージは、情報を提供するメッセージです。

warning

この優先度コードのメッセージは警告メッセージです。

error

この優先度コードのメッセージはエラー メッセージです。

crit

この優先度コードのメッセージは深刻なエラー メッセージです。

debug

この優先度コードのメッセージはデバッグ メッセージです。

例: syslog デーモンへのステートメントの追加

MSMCPROC ジョブによって書き込まれたすべてのメッセージを、ファイル /tmp/syslogd/msmcproc.syslog に書き込めるようにするには、以下のステートメントを syslog デーモン設定ファイルに追加し、変更を有効化します。

```
#
#  CA CSM SCS message log(SCSLOG)
#
*.MSMCPROC.*.* /tmp/syslogd/msmcproc.scslog
```

syslog デーモン設定変更の有効化

syslog デーモン設定ファイルを更新した後、syslog デーモンに SIGHUP シグナルを送信します。 これによりデーモンは設定ファイルを再読し、修正したパラメータが有効化されます。

USS の kill コマンドを使用して、SIGHUP 信号を送信します。

このコマンドの構文は以下の通りです。

```
kill –s SIGHUP pid
```

pid

syslog デーモンのプロセス ID を指定します。

開始方法に応じて、syslog デーモンはそのプロセス ID をファイルに格納します。 ファイルはデーモンの再設定に使用できます。

- syslog デーモンが標準モード、またはローカル専用モードで開始される場合、ファイル名は以下のとおりです。

  /etc/syslog.pid

- syslog デーモンがネットワーク専用モードで開始される場合、ファイル名は以下のとおりです。

  /etc/syslog_net.pid

syslog デーモンは、設定ファイルを再度読み込んだ後、設定で指定されたファイルにログ メッセージを追加し続けます。

注: syslog -c オプションが指定されない限り、syslog デーモンが使用するすべてのログ ファイルは、syslog デーモンが開始もしくは再設定される前に、z/OS UNIX ファイル システムで作成される必要があります。 -c オプションが指定される場合、syslog デーモンは存在していないログ ファイルを動的に作成します。

汎用トレース機能

SCS アドレス空間は汎用トレース機能（GTF）を使用し、診断用のデータを収集します。 GTF は z/OS システム製品の一部です。 GTF は、START GTF コマンドの発行によって明示的に有効化する必要があります。

注: GTF の詳細については、「*IBM MVS Diagnosis Tools and Service Aids*」を参照してください。

GTF の開始

GTF を開始するには、START GTF コマンドを入力します。 IBM のプロシージャまたは GTF 開始用の内部プロシージャを使用して、GTF を開始できます。

注: GTF の複数のインスタンスを同時にアクティブにできます。 各インスタンスは、スターティッド タスクとして、それ自身のアドレス空間で実行されます。

各 GTF のインスタンスには一意の識別子を割り当てることができ、その識別子は START GTF コマンドで指定されます。 この識別子により、GTF の特定のインスタンスの認識と制御が可能になります。 一意の識別子が指定されない場合、オペレーティング システムはトレース データ セットがあるデバイスのデバイス番号を割り当てます。

GTF がトレースするイベントは、オプションとして指定します。 SCS アドレス空間に対し、USRP と JOBNAMEP オプションを指定します。

USRP GTF オプションを指定した後、GTF はイベント識別子（EID）の一覧を求めるプロンプトが表示されます。

SCS アドレス空間は以下の EID を使用します。

301

SCS アドレス空間のインフラストラクチャ コンポーネント用の診断データを収集します。

302

SCS アドレス空間の通信サーバ コンポーネント用の診断データを収集します。

303

SCS アドレス空間の通信サーバ イベント API コンポーネント用の診断データを収集します。

304

SCS アドレス空間のコンテナ セクション コンポーネント用の診断データを収集します。

305

SCS アドレス空間の実装エンジン コンポーネント用の診断データを収集します。

306

SCS アドレス空間のサービス セクション コンポーネント用の診断データを収集します。

307

SCS アドレス空間のシステム情報エージェント コンポーネント用の診断データを収集します。

注: 不要な情報の出力を回避するには、USRP オプションを使用して GTF のトレース出力を制限します。

JOBNAMEP GTF オプションが指定されている場合、トレース出力がキャプチャされるジョブ名のリストを求めるプロンプトが表示されます。 メインまたは補助の SCS アドレス空間の名前を指定します。 一般的な名前は、順番に MSMCPROC (P. 204) および MSMCAUX です。

例

CA CSM には以下の GTF トレース オプションを含む MSMCGTFP サンプル メンバが用意されています。

```
TRACE=USRP,JOBNAMEP
USR=(301,302,303,304,305,306,307)
JOBNAME=(MSMCPROC,MSMCAUX)
END
```

GTF の停止

GTF を停止するには、STOP GTF コマンドを発行します。 START GTF コマンドの識別子を指定します。識別子が START GTF コマンドで指定されていない場合は、トレース データ セットがあるデバイスのデバイス番号で識別子を指定します。

付録 A: CA CSM の実装およびステータス

このセクションには、以下のトピックが含まれています。

実装チェックリスト (P. 123)
CA CSM ソフトウェア展開生成手順エンティティ (P. 128)
USS ファイル システム (P. 128)
CA CSM データ セットとファイル システム (P. 132)
CA Common Services コンポーネントの要件 (P. 137)
CA CSM 機能のセキュリティ (P. 139)
SMP/E 処理中の SAF チェック (P. 147)
DBINIT および DBUPDATE の設定 (P. 149)
ASCII 設定ファイル (P. 158)
ジョブ割り当て詳細 (P. 161)

実装チェックリスト

このセクションのチェックリストを使用して、各ロールがそれぞれに関連付けられたタスクを完了していることを確認します。

ネットワーク管理者

以下の Web サイトへのアクセス権を設定します。

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

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

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

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

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

Security Administrator

1. 以下のデータ セットまたはライブラリへの UPDATE 権限を、CA CSM を実装するユーザに付与します。
   - SYS*x*.PARMLIB
   - CA CSM アドレス空間を開始するために使用される、JCL ジョブを格納するプロシージャ ライブラリ（たとえば、SYS3.PROCLIB）
   - （オプション） CA CSM データ セット プレフィクスに対してエイリアス エントリを定義する場合のマスタ カタログ
2. CA CSM セットアップ ユーティリティ MSMSetup.sh に関連付けられたユーザ ID に、以下のアクセス権を付与します。
   - USS へのアクセス権
   - UNIX に関連する、以下の FACILITY クラスのプロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）
     - BPX.SERVER（UPDATE 権限）
     - BPX.CONSOLE（READ 権限）
   - SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）

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

  注: ユーザ ID は BPX.SUPERUSER アクセス権を持つことができ、それを SUPERUSER に切り替えることができます。 このとき、切り替えられた SU ID には、オプション ファイルで指定された MVS データ セット修飾子に対する CREATE および MODIFY アクセス権が必要です。
- IBM RACF を使用している場合、プログラム制御用の以下のデータ セットにアクセスします。
  - SYSx.MIGLIB
  - CEE.SCEERUN2
  - メンバ IEANTCR、IEANTDL および SYS1.CSSLIB の IEANTRT
  - Java ロード モジュールがインストールされているデータ セットのメンバ JVMLDM76 （64 ビット Java 7.0 用）
  - （オプション） SYS1.IDI.SIDIAUTH のメンバ IDIXCEE （オプションの EXIT として IDIXCEE を使用する場合のみ）

  注: リソースを表示するには、RLIST コマンドを発行します。

  プログラムを制御するために、IBM RACF を設定できます。 リソースが存在しない場合は、以下のコマンドを発行します。

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

  以下に例を示します。

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

  リソースが存在する場合は、以下のコマンドを発行します。

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

  以下に例を示します。

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

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

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

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

3. CA CSM アプリケーション サーバ（MSMTC ジョブまたはスターティッド タスク）に関連付けられたユーザ ID に、以下のアクセス権を付与します。
   - USS へのアクセス権
   - ファイル システムの作成およびマウント権限
   - UNIX に関連する、以下の FACILITY クラスのプロファイルへのアクセス許可
     - BPX.FILEATTR.APF（READ 権限）
     - BPX.FILEATTR.PROGCTL（READ 権限）
     - BPX.FILEATTR.SHARELIB（READ 権限）
     - BPX.SERVER（UPDATE 権限）
     - BPX.CONSOLE（READ 権限）
   - SERVAUTH クラス プロファイルへのアクセス許可である、EZB.STACKACCESS（READ 権限）
   - CA ACF2 for z/OS のみ： CA CSM を開始するユーザに対する MUSASS 許可
   - サイトで CA SAF HFS セキュリティを使用する場合は、以下のアクセス権を設定します。
     - BPX.CAHFS.SET.RLIMIT （READ 権限）
     - BPX.CAHFS.PTRACE（READ 権限）
     - BPX.CAHFS.MOUNT（READ 権限）
     - BPX.CAHFS.UNMOUNT（READ 権限）
     - BPX.CAHFS.CHANGE.FILE.MODE （READ 権限）

     注: CA SAF HFS セキュリティは CA ACF2 for z/OS および CA Top Secret for z/OS の機能です。
4. CA CSM ユーザ用の OMVS セグメントをセットアップします。

USS 管理者

以下の構造を使用し、USS パスをセットアップします。

```
/u/users/msmserv（プライマリ マウント ポイント）
     msminstall（1000 シリンダ）
     msm（750 シリンダ）
     msmruntime（750 シリンダ）
     mpm（CA CSM が使用するマウント ポイント）
```

システム プログラマ

1. 必須要件が満たされていることを確認します。
2. オプション ファイル キーワードを確認し、必要な値を収集します。
3. CA CSM をダウンロードします。
4. 以下のように CA CSM を解凍します。

   ```
   pax -rvf 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。
5. UNZIPJCL をカスタマイズしてサブミットし、CA CSM 製品ファイルを展開します。
6. MSMSetupOptionsFile.properties ファイルをカスタマイズします。
7. MSMSetup.sh を実行します。
8. 以下のメンバを順番に使用して、CA CSM を開始します。
   - MSMMUFS JCL メンバまたは MSMMUF PROCLIB メンバ
   - MSMDBSVS JCL メンバまたは MSMDBSRV PROCLIB メンバ
   - MSMTCSRV JCL メンバまたは MSMTC PROCLIB メンバ
9. Web ブラウザを使用して CA CSM にアクセスし、初期設定を実行します。

10. USS ディレクトリをクリーン アップします。
11. 製品の展開をサポートするため、各 CA Technologies 製品の展開アクティブ化要素が取得され、インストールされていることを確認してください。

    注: 製品の展開の詳細については、オンライン ヘルプを参照してください。

CA CSM ソフトウェア展開生成手順エンティティ

以下のエンティティは、CA CSM ソフトウェア展開手順の中でインストールされます。これは CA Common Services for z/OS、CAIENF および CAICCI のコンポーネントに依存する機能です。

SMPCPATH

SMP/E Java アプリケーション クラスのパスを指定します。

プリセット： /usr/lpp/smp/classes/

SMPJHOME

Java ホーム ディレクトリを指定します。

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

注: 異なる Java ホーム ディレクトリがインストールされている場合は、そのディレクトリ名を使用します。

SMPDRIWK

このエンティティは 775 の許可で定義される必要があります。

プリセット： /cai/msm/ccispnsv/smpe

注: 手順では /cai/msm/ccispnsv/smpe に設定されます。 これを社内標準に合わせます。

USS ファイル システム

このセクションでは、z/OS UNIX System Services （USS）およびファイル システムのセットアップの詳細を説明します。

CA CSM のインストールとセットアップ

MSMSetup.sh ユーティリティを実行する前に、CA CSM インストールのマウント ポイントを定義します。 マウント ポイントには以下のディレクトリが含まれます。

- MSMSetupOptionsFile.properties の MSMPATH キーワードが参照するインストール ディレクトリ（たとえば、/u/users/msmserv/msminstall）
- MSMSetupOptionsFile.properties の RunTimeUSSPath キーワードが参照するランタイム ディレクトリ（たとえば、/u/users/msmserv/msmruntime）

CA CSM のダウンロード

CA CSM は pax ファイルとして提供されます。pax ファイルは、マウントされたファイル システムまたはディレクトリ（たとえば、/u/users/msmserv/msminstall）にダウンロードされ、インストールされます。 ファイルの名前は、DVD10155349E.pax.Z です。 ファイルを展開すると、新規ディレクトリが作成されます。

CA CSM の起動

このセクションでは、新規および既存の CA CSM インストールの CA CSM 起動プロセスについて説明します。

起動時に、CA CSM はファイル システムおよび USS ディレクトリを割り当ててマウントします。MSMSetup.sh を実行する前に、APLROOT ファイル システム用のマウント ポイント（たとえば、/u/users/msmserv/mpm）を定義します。CA CSM はファイル システムを割り当て、そのファイル システムをこのマウント ポイントにマウントします。

注: MSMSetupOptionsFile.properties の MountPath キーワードは、APLROOT ディレクトリを指定します。 MSMSetup.sh は、SAMPLIB（DBINIT）メンバの mpmPath パラメータに、この値を読み込みます。 CA CSM を初めて開始するときは、DBINIT メンバが使用されます。 起動時に、この値はデータベースに格納されます。 Web ベース インターフェースで［Settings］タブの［Mount Point Management］ページの［Application Root］フィールドを使用して、値を変更できます。

APLROOT ファイル システムの下では、CA CSM は sdsroot、scroot、ljroot、tmproot の 4 つの USS ディレクトリを作成します。 USS ディレクトリ ljwk は、ljroot ディレクトリの下に作成されます。

以下のリストは、永続ファイル システムおよびそれらのマウント ポイントを示します。

- *mountpath* にマウントされた *hfs_prefix*.APLROOT（105,105 トラック）
- *mountpath*/ljroot/ljwk にマウントされた *hfs_prefix*.LJWK（2370,105 トラック）
- *mountpath*/sdsroot にマウントされた *hfs_prefix*.SDSROOT（105,105 トラック）

hfs_prefix

このプレフィクスは、MSMSetupOptionsFile.properties の MVSHFSDsnPrefix キーワードによって指定されます。 MSMSetup.sh は、SAMPLIB（DBINIT）メンバの mpmHlq パラメータに、この値を読み込みます。 起動時に、この値はデータベースに格納されます。 Web ベース インターフェースで、［Settings］タブの［Mount Point Management］ページにある［Data Set Prefix］フィールドを使用して、この値を変更できます。

tmproot USS ディレクトリは、CA CSM 稼働中に必要な一時ファイル システムを割り当ててマウントする (P. 130)ために使用されます。

CA CSM が起動時にファイル システムをマウントするかどうかを定義できます。 Web ベース インターフェースの［Settings］タブの［Mount Point Management］ページには、［Automount］オプションがあります。 オプションが有効な場合、CA CSM は管理するすべてのファイル システムを検索してマウントします。オプションが有効ではない場合、SYS*x*.PARMLIB の BPXPRM*xx* メンバを更新してマウント ポイントを管理します。

一時ファイル システムの使用

さらに、CA CSM は製品の取得、製品のインストール、および他のタスクの実行中に、必要に応じて一時ファイル システムを割り当てます。デフォルトでは、CA CSM は一時ファイル システムを 60 分間保持します。 ファイル システムが 60 分間のアイドル状態を続けた後、CA CSM は一時ファイル システムの割り当てを解除し、解放します。

ファイル システムの名前は、*hfs_prefix*.T*x* のような形式です。

x

7 文字以内の内部生成された数字です。

CA CSM は以下のパスに一時ファイルをマウントします。

mountpath/tmproot/MSM.*unique_number*.scratchpad

割り当てられマウントされたファイル システムを CA CSM が保持するタイム スロットを変更できます。 SAMPLIB（MSMLIB）メンバで、以下のパラメータに必要な分単位の数を設定し、CA CSM アプリケーション サーバを再起動します。

IJO="$IJO –DCSM_MPM.TEMPSPACE.MINIMUM.IDLE.MINUTES=60"

最小有効値は 60 です。ユーザが 60 未満にパラメータの値を設定した場合、CA CSM はそれを再度 60 に設定します。

このパラメータが 0 に設定される場合、CA CSM は実行中に一時スペースを割り当て、終了時にそれを解放します。

ソフトウェア カタログ

CA CSM は、ソフトウェア カタログが使用するためのファイル システムを必要に応じて割り当ててマウントします。 CA CSM は、これらのファイル システムを *mountpath*/scroot の下にマウントします。

ファイル システムの名前は、*hfs_prefix.suffixn* の形式です。

suffix

ファイル システム名の最後の部分を定義するもので、SAMPLIB（DBINIT）メンバの scDatasetPrefix パラメータによって指定されます。

n

4 文字以内の内部生成カウンタを定義します。

CA CSM データ セットとファイル システム

このセクションでは、CA CSM データ セットおよびファイル システムの詳細について説明します。

このセクションには、以下のトピックが含まれています。

CA CSM データ セット タイプ (P. 132)

CA CSM ファイル システム (P. 133)

CA CSM データ セット タイプ

CA CSM には 5 つのグループのデータ セットがあります。 グループは以下のタイプで構成されます。

アプリケーション ルート: *hlq*.APLROOT

このデータ セットはルートの USS ファイル システムとして使用され、CA CSM のディレクトリ構造を格納します。

一時領域: *hlq*.T*x*

これらのデータ セットは一時ファイル システムで、CA CSM 処理用の一時領域として使用されます。 これらのデータ セットは CA CSM 稼働中に必要に応じて割り当てられ、必要とされなくなったときに削除されます。

ログ ジャーナル: *hlq*.LJWK*x*

これらのデータ セットはタスクの出力結果を保存するために使用され、その内容は完了したタスク用の［Tasks］タブに表示されます。 CA CSM を使用してこの内容を削除するには、［Task］タブの［Delete Task］ボタンを使用します。

ソフトウェア カタログ: *hlq*.CASC*x*

これらのデータ セットはすべてのダウンロードされた製品およびメンテナンス パッケージを格納し、それらはソフトウェア カタログに表示されます。 サフィックスが CASC のデータ セットは通常、CASC のデフォルト値があります。 展開が完了または削除された後に、データ セットは削除されます。

注: 旧バージョンの CA CSM では、デフォルトのソフトウェア カタログ データ セットは、サフィックスが MSMT でした。

展開一時領域: *hlq*.SDSROOT

このデータ セットは一時ファイル システムで、CA CSM 展開処理用の一時領域として使用されます。データが必要なくなった後、CA CSM はこのファイル システムのコンテンツを削除します。 CA CSM をシャットダウンした後にコンテンツがそこに残っている場合、適切な USS ディレクトリからコンテンツを手動で削除でき、CA CSM に影響を与えることはありません。

展開: *hlq*.D*x*

これらのデータ セットは展開処理に使用され、展開データが含まれています。 CA CSM を使用してこのコンテンツを削除するには、［Deployment］タブの［Action］ドロップダウン リストから［Remove］を選択します。

重要: これらのデータ セットやコンテンツを、CA CSM の外部で、手動でデータ セットから削除しないでください。 手動でデータ セットを削除すると、タスク出力が失敗、または CA CSM が失敗します。

CA CSM ファイル システム

以下の表では、CA CSM が割り当てて使用するファイル システムを示します。 以下の用語が表で使用されています。

mpm

アプリケーション ルートへの UNIX パスを指定します。 mpm は、ファイル システムのマウント ポイント ディレクトリを指定します。 初期マウント ポイントは、CA CSM のインストール中に設定されます。

hlq

CA CSM が割り当てる新規ファイル システムに対して作成されるデータ セット名の HLQ を指定します。

データ セット名（DSN）

このディレクトリにマウントされるファイル システムの DSN、または このディレクトリにマウントされているファイル システムがない場合には、このディレクトリを含むファイル システムの DSN を指定します。

標準サイズ

ファイル システムの標準サイズを指定します。この値は、そのパスにマウントされたファイル システムがあるパスに対してのみ指定します。

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm	*hlq*.APLROOT	Yes	アプリケーション ルート	CA CSM のメインのマウント ポイント ディレクトリ。 このディレクトリは *hlq*.APLROOT データ セットにあります。	14400 KB
mpm/ljroot	*hlq*.APLROOT	No	ログ ジャーナル ルート	ログ ジャーナル（タスク出力）用のルート ディレクトリ。	N/A
mpm/scroot	*hlq*.APLROOT	No	ソフトウェア カタログのルート	ソフトウェア カタログ（製品およびメンテナンス パッケージを格納） 用のルート ディレクトリ。	N/A
mpm/sdsroot	*hlq*.SDSROOT	Yes	展開のルート	展開パッケージ用のルート ディレクトリ。	158400 KB
mpm/ljroot/ljwk	*hlq*.LJWK	Yes	ログ ジャーナル	このディレクトリは *hlq*.LJWK データ セットにあります。	137760 KB
mpm/scroot/tmp	*hlq*.APLROOT	No	ソフトウェア カタログ	ソフトウェア カタログの一時ディレクトリが含まれるディレクトリ。	N/A

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm/scroot/tmp/tmp*x*	*hlq*.CASCn	Yes	ソフトウェア カタログ	ソフトウェア カタログの一時ディレクトリ。	400000 KB
mpm/scroot/DatabaseM	*hlq*.APLROOT	No	ソフトウェア カタログ	ソフトウェア カタログ データベースが含まれるディレクトリ。	N/A
mpm/scroot/DatabaseM/CA	*hlq*.APLROOT	No	ソフトウェア カタログ	すべてのベンダーのダウンロードが格納された、CA Technologies ベンダー ディレクトリ。	N/A
mpm/scroot/DatabaseM/CA/error_hold_data	*hlq*.APLROOT	No	ソフトウェア カタログ	ALL-HOLDDATA.txt ファイルが格納されるディレクトリ。 このファイルには、すべての CA Technologies 製品用の HOLDDATA が含まれます。	N/A
mpm/scroot/DatabaseM/CA/COMMONS	*hlq*.APLROOT	No	ソフトウェア カタログ	CA Common Services 用のインストールが格納されるディレクトリ。	N/A
mpm/scroot/DatabaseM/cars	*hlq*.CASCn	Yes	ソフトウェア カタログ	CA RS ファイルが格納されるディレクトリ。	4800 KB
mpm/scroot/DatabaseM/CA/MAINTENANCE	*hlq*.CASCn	Yes	ソフトウェア カタログ	すべてのメンテナンス パッケージが格納されるディレクトリ	4800 KB
mpm/scroot/DatabaseM/CA/*product_name*	*hlq*.CASCn	Yes	ソフトウェア カタログ	特定の製品用の製品ディレクトリ。	4800 KB

パス	データ セット名	パスにマウントされたデータ セット	タイプ	目的	標準サイズ
mpm/scroot/DatabaseM/CA/*product_name*/*release*/*servicepack*/*packagename*/*date*	*hlq*.CASCn	Yes	ソフトウェア カタログ	製品ディレクトリに組み込まない、特定の製品パッケージ用のディレクトリ。	4800 KB
mpm/sdsroot/*deployment_ID*	*hlq*.Dn	Yes	Software Deployment Service（SDS）	ID *deployment_ID* で行う展開用に保存されたデータを格納するディレクトリ。このディレクトリは *hlq.deployment_ID* データ セットにあります。	21024 KB
mpm/tmproot	*hlq*.APLROOT	Yes	一時領域	このディレクトリには、一時ファイル システム用の一時マウント ポイントが含まれます。	N/A
mpm/tmproot/MSM.*n*.scraptchpad	*hlq*.T*n*	Yes	一時領域	このディレクトリは一時ファイル システムのマウント ポイントとして機能し、CA CSM が製品の取得、製品のインストール、その他のタスクの実行中に、必要に応じて割り当てます。	57408 KB

CA Common Services コンポーネントの要件

CA Common Services for z/OS には、CA Technologies の実装に共通の分散サービスと、z/OS に固有のソリューションが用意されています。 CA Common Services for z/OS は、複数の統一されたリソース ビューを作成するための共通のインターフェースとイベント サービスを提供します。

CA Common Services for z/OS ソフトウェア サービスは、以下のコンポーネントを含む、さまざまな機能を実行する複数のソフトウェア コンポーネントを CA CSM に提供します。

- CAICCI
- CAIENF (Base)
- CAIRIM
- CA-C Runtime

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

FMID

CA CSM では、さまざまな機能を実行するために CA Common Services for z/OS リリース 14.1 またはバージョン 14.0 のコンポーネントが必要です。機能変更 ID（FMID）が、これらのコンポーネントに対して用意されています。

以下の表の FMID は、CA Common Services for z/OS バージョン 14.0 に基づきます。

FMID	コンポーネント
CAF3E00	CA-C Runtime
CAS9E00	CAIRIM
CAW1E00	CAIENF
CAW4E00	CAICCI （SSL を使用）

以下の表の FMID は、CA Common Services for z/OS リリース 14.1 に基づきます。

FMID	コンポーネント
CAF3E00	CA-C Runtime
CAS9E10	CAIRIM
CAW1E10	CAIENF
CAW4E10	CAICCI （SSL を使用）

以下の表の FMID は CA Common Services for z/OS バージョン 14.0 およびそれ以降のバージョンを基にしています。 この FMID は CA Common Services for z/OS に依存する機能であり、SDS と SCS に対してのみ使用されます。

FMID	コンポーネント
CETN600	CAICCI を使用する CA CSM Common Services

注: 完了する必要があるセットアップおよび設定の手順の詳細については、「*CA Common Services for z/OS インストール ガイド*」を参照してください。

CAICCI のセットアップ

CAICCI をまったくセットアップしていない場合は、この手順を使用します。詳細については、「*CA Common Services for z/OS インストール ガイド*」を参照してください。

以下の手順に従います。

1. 以下の形式を使用し、CAIENF パラメータ ファイル内、または ENFPARMS に連結された個別の CCIPARM PDS メンバのどちらかで、CAICCI SYSID を定義します。

   SYSID(*sysid*)

   sysid

   CAICCI 識別子を指定します。

   制限： 8 文字

2. CAICCI データ収集モジュール（DCM） CAS9DCM3 を CAIENF パラメータ ファイルに定義します。 以下に例を示します。

   ```
   DCM(CAS9DCM3)         * ENF V1.0 CCI Event
   ```

CA CSM 機能のセキュリティ

CA CSM 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 (P. 141)は、CA CSM リソース クラスで定義されています。 リソース プロファイルにより、サイトはさまざまなリソースやアクションへの権限を特定のユーザに付与し、少しの設定で汎用アクセス権を設定できるようになります。

リソース名

CA CSM は、リソースへのアクセス用の READ、UPDATE、CONTROL、ALTER を区別しません。 その代わりに、アクセス権はリソース名にエンコードされます。 リソースに対するアクセス権がある場合、リソース上の指定されたアクションを実行できます。

付与される権限レベルは重要ではありません。 リソースにアクセスできる（READ、UPDATE、CONTROL、ALTER の任意の組み合わせ）かできないかは、バイナリ方式で管理されます。たとえば、以下のリソース プロファイルは、［Settings］タブのシステム設定へのアクセスを制御します。

ADMIN.SETTINGS.SYSTEM

ユーザにシステム設定の表示と更新を許可します。

ADMIN.SETTINGS.SYSTEM.@DISPLAY

ユーザにシステム設定の表示を許可します。

ADMIN.SETTINGS.SYSTEM.@UPDATE

ユーザにシステム設定の更新を許可します。

@DISPLAY および @UPDATE プロファイルの両方があるリソースについては、@UPDATE プロファイルに対してのみのアクセス権の付与はエラーになります。 値を表示する権限がないため、たとえそのレベルのアクセス権が付与されているとしても、値を変更することはできません。

すべてのシステム設定は ADMIN.SETTINGS.SYSTEM の下に構成されるため、1 人以上のユーザに ADMIN.SETTINGS.SYSTEM プロファイルに対する権限を付与することで、すべてのシステム設定へのアクセス権を与えることができます。 これらのユーザは、CA CSM の管理の役割を担います。

ユーザ設定は ADMIN.SETTINGS.USER の下に構成されます。設定は、CA CSM で各ユーザに対して個別に保守されます。 リソースの表示または更新のアクセス権は、リソース プロファイル内の @SELF 修飾子を使って管理されます。 たとえば、USER01 および USER02 ユーザ ID に ADMIN.SETTINGS.USER.@SELF.@DISPLAY および ADMIN.SETTINGS.USER.@SELF.@UPDATE プロファイルへの権限を付与することにより、ユーザは自分の Web ベース インターフェースの設定を更新できるようになります。 ただし、USER01 は、USER02 用の設定の表示や更新はできません。 ADMIN.SETTINGS.USER.@SELF へのアクセス権を、すべての CA CSM ユーザに付与することをお勧めします。

リソース プロファイル

セキュリティ ルールを使用してアクセスを許可または拒否することによって、CA CSM の特定の一部を保護することができます。これを*リソース プロファイル*と呼びます。 リソース クラス CAMSM を使用し、これらのリソース プロファイルを関連するセキュリティ パッケージに作成します。

重要: ユーザに *.@UPDATE リソース プロファイルへのユーザ権限を付与する場合、それに対応する *@DISPLAY リソース プロファイルにもそのユーザ権限を付与する必要があります。

LOGON

CA CSM へのアクセス権を付与します。

ADMIN.SETTINGS

［Settings］タブ上のすべての設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.SYSTEM

すべてのシステム設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.SYSTEM.@DISPLAY

すべてのシステム設定への DISPLAY 権限を付与します。

ADMIN.SETTINGS.SYSTEM.@UPDATE

すべてのシステム設定への UPDATE 権限を付与します。

ADMIN.SETTINGS.USER.@SELF

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定へのフル アクセス権を付与します。

ADMIN.SETTINGS.USER.@SELF.@DISPLAY

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定への DISPLAY 権限を付与します。

ADMIN.SETTINGS.USER.@SELF.@UPDATE

CA サポート オンライン Web サイトのユーザ アカウントをはじめとする、ユーザ自身の設定への UPDATE 権限を付与します。

ADMIN.LMPKEY

［LMP Keys Browser］ページ上のリソースへのフル アクセス権を付与します。

ADMIN.LMPKEY.UPDTKEYS

［LMP Keys Browser］ページ上の［Update Keys］へのアクセス権を付与します。

ADMIN.LMPKEY.REFRSITE

［LMP Keys Browser］ページ上の［Refresh Site IDs］へのアクセス権を付与します。

CONFIG

［Configurations］タブ上のリソースへのフル アクセス権を付与します。

CONFIG.@DISPLAY

SCS に関係するリソースへの表示専用アクセス権を付与します。

CONFIG.@ACTION.CREATE

SCS に関係するリソースの作成、または更新のためのフル アクセス権を付与します。

CONFIG.@ACTION.REMOVE

［Deployments］タブ上のリソースへのフル アクセス権を付与します。

CONFIG.@ACTION.IMPL

リモート システムの設定を実装するためのアクセス権を付与します。

DEPLOY

［Deployment］タブ上のリソースへのフル アクセス権を付与します。

DEPLOY.@DISPLAY

［Deployments］タブ上で提供される情報への読み取り専用権限を付与します。

DEPLOY.@SELF

展開の作成、システムとカスタム データ セットの割り当て、さらに CA CSM ユーザ ID が展開の所有者としてマークされている場合は展開のすべてのアクションの割り当てを行う権限を付与します。

DEPLOY.@BUILD

展開の作成および更新、システムおよびカスタム データ セットの割り当て、および展開のプレビューを行う権限を付与します。

DEPLOY.@EXECUTE

スナップショットの実行、転送、展開、展開の確認を行う権限を付与します。

METHOD

すべての方法へのフル アクセス権を付与します。

METHOD.@DISPLAY

すべての方法への読み取りアクセス権を付与します。

METHOD.@SELF

ユーザが所有者として登録された方法のみに、フル アクセス権を付与します。

METHOD.@UPDATE

［Maintain Methodologies］ページ内から、方法を作成、編集、削除するためのアクセス権を付与します。 このプロファイルは、展開ビュー内の方法の隣にある［Edit］ボタンを有効にするかどうかも制御します。

SC

［Products］タブ上のリソースへのフル アクセス権を付与します。

SC.@ACTION

［Products］タブ上のアクションへのフル アクセス権を付与します。

SC.@ACTION.UPDTCAT

［Products］タブ上のすべての［Update Catalog］アクションへのアクセス権を付与します。

SC.@ACTION.SHOWLMP

［Products］タブ上の［Actions］セクション内の［Show License Keys］アクションへのアクセス権を付与します。

SC.@ACTION.INSRTPRD

［Products］タブ上の［Actions］セクション内の［Add Product］アクションへのアクセス権を付与します。

SC.@ACTION.INSTPKG

［Products］タブ上の［Actions］セクション内の［Install External Package］アクションへのアクセス権を付与します。

SC.@HIDE

［Products］ツリーの［Hide Product］アクション、および［Products］タブ上の［Show Hidden Products］ダイアログ ボックスの［Show Products］ボタンへのアクセス権を付与します。

SIS.BASE.@SELF.WORKDD.@UPDATE

製品インストール中の作業 DDDEF の設定を更新するためのアクションにアクセス権を付与します。

SMPE.@ACTION

［SMP/E Environments］タブ上のアクションへのフル アクセス権を付与します。

SMPE.@ACTION.MIGRATE

SMP/E 環境を移行するためのアクションへのフル アクセス権を付与します。

SMPE.@ACTION.REMOVECSI.*csidatasetname*

［SMP/E Environments］ - ［SMP/E Environment Information］タブ上の［Remove SMP/E Environment from CA CSM］へのアクセス権を付与します。 このアクセス権は指定された SMP/E 環境用です。

.csidatasetname

ユーザが削除できる SMP/E 環境のデータ セット名を指定します。

この値には、1 つの SMP/E 環境に一致するフル ネーム、または複数の SMP/E 環境データ セット名に一致するプレフィクスを指定できます。

SYSREG

［System Registry］タブ上のリソースへのフル アクセス権を付与します。

SYSREG.@DISPLAY

すべての System Registry 値の表示権限を付与します。

注: このアクセス権で定義されたユーザは、すべてのパネル上のいかなる情報も作成、削除、更新できません。

SYSREG.@ACTION

［System Registry］タブ上のアクションへのフル アクセス権を付与します。

SYSREG.@ACTION.CREATE

［Create Non-Sysplex System］リンク、［Create Sysplex］リンク、［Create Shared DASD Cluster］リンク、［Create Staging System］リンクへのアクセス権を付与します。 このプロファイルによって、［System Registry］ツリーの各プライマリ ノードの画面内の［Create］ボタン、および［Data Destinations］内の［Create］ボタンも有効になります。 Create 権限には、Update 権限も含まれます。

SYSREG.@ACTION.REMOVE

［System Registry］ツリーの各プライマリ ノードの内の［Actions］ボタンからの［Select check box］および［Remove item］へのアクセス権を付与します。

注: ユーザにこの権限がない場合、これらのアイテムは無効になっています。

SYSREG.@PROFILE

システム レジストリの各プライマリ ノード内の情報へのフル アクセス権を付与します。 この情報は、設定の作成または実装を行う組織内の CA CSM ユーザに適用することができます。 このアクセス権が付与されていない場合、システム情報は Web ベース ユーザ インターフェース内に表示されません。

注: 実装の結果としてのリモート システムでの変更が正しく行われなかった場合、リモート システムの安定稼働に悪影響を与えるおそれがあります。このリソース プロファイルに対する権限を制限することをお勧めします。

SYSREG.@PROFILE.DISPLAY

システム レジストリの各システム ノード内から、このアクセス権を持ったユーザはプロファイル内のいかなる値も修正する権限がありません。 これらのアイテムは表示されますが、すべての［Action］ボタンは無効になります。

SYSREG.@PROFILE.UPDATE

システム レジストリの各システム ノード内から、システム レジストリ プロファイル内の任意の既存値を更新するか、反復可能なシステム レジストリ プロファイルのオカレンスの作成を行うためのアクセス権を付与します。 システム レジストリがリソース ルール SYSREG@PROFILE.DISPLAY でセキュリティ保護されている場合、このアクセス ルールは任意のシステム情報の更新を可能にするために必要です。

SYSREG.@PROFILE.UPDATE.*systemname*

システム レジストリ プロファイル内の既存値を更新するか、またはシステム *systemname* の反復可能なシステム レジストリ プロファイルのオカレンスを作成するためのアクセス権を付与します。

SYSREG.@SYSTEM

［System Registry］タブ内に定義されたすべてのシステムへのフル アクセス権を付与します。

SYSREG.@SYSTEM.*systemname*

［System Registry］タブ内のシステム *systemname* へのアクセス権を付与します。 システムが CA CSM セッション内で作成され、特定のシステム レベル セキュリティが必要な場合、セキュリティ管理者は、そのシステムが CA CSM ユーザに対して表示される前に、新しく定義されたシステムへのアクセス権を付与する必要があります。 このレベルのセキュリティは、どの定義済みシステムをユーザが利用可能かのみを制御します。 定義済みシステムの情報を更新または削除する機能は、SYSREG.@ACTION.CREATE、SYSREG.@ACTION.REMOVE、SYSREG.@PROFILE.UPDATE リソースを使用して許可されます。

TM.TASK.ARCHIVE

［Task］タブ内の［Manage History］機能へのアクセス権を付与し、権限のあるユーザによるタスク アーカイブ ポリシーの作成、実行、削除を可能にします。

TM.TASK.@SELF.DELETE

ユーザ自身のタスクを削除するためのアクセス権を付与します。

TM.TASK.SYSTEM.DELETE

任意のタスクを削除するためのアクセス権を付与します。

SMP/E 処理中の SAF チェック

SMP/E コマンドを実行するすべての CA CSM 機能は、CA CSM にログインし、これらの機能を操作するユーザのセキュリティ コンテキスト内でこのチェックを行います。 CA CSM の機能により異なりますが、さまざまな SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

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

SMP/E 環境の移行

カスタマ提供の JCL を使用して新しい DDDEF を移行済みの SMP/E 環境に追加する場合、ユーザには以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.CMD.SET
- GIM.CMD.UCLIN

基本製品のインストール

製品をインストールするには、以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.PGM.GIMUNZIP
- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RECEIVE
- GIM.CMD.APPLY
- GIM.CMD.ACCEPT

既存の SMP/E 環境に製品をインストールするときにエラーが発生する場合、CA CSM はインストールを開始する前に UNDO 操作を実行し、SMP/E 環境をその状態にリストアします。

CA CSM が実行する UNDO 操作のレベルに応じて、以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。

- GIM.CMD.SET
- GIM.CMD.UCLIN
- GIM.CMD.RESTORE
- GIM.CMD.REJECT

メンテナンス管理

メンテナンスを管理するため、GIM.CMD.SET SAF 機能クラス リソースへの READ アクセス権が必要です。

その他の要件は、以下の特定のメンテナンス操作により異なります。

- メンテナンスをインストールするには、少なくとも以下の SMP/E SAF 機能クラス リソースへの READ アクセス権が必要です。
  - GIM.CMD.RECEIVE
  - GIM.CMD.APPLY
- また、メンテナンスを ACCEPT するには、ユーザには GIM.CMD.ACCEPT SAF 機能クラス リソースへの READ アクセスが必要です。
- 1 つ以上のメンテナンス パッケージで基本の SMP/E コマンドを実行するには、ユーザには以下の対応する SAF 機能クラス リソースへの READ アクセス権が必要です。
  - GIM.CMD.RECEIVE（RECEIVE 操作用）
  - GIM.CMD.APPLY（APPLY 操作用）
  - GIM.CMD.ACCEPT（ACCEPT 操作用）
  - GIM.CMD.RESTORE（RESTORE 操作用）
  - GIM.CMD.REJECT（REJECT 操作用）

展開

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

DBINIT および DBUPDATE の設定

CA CSM を初めて起動する際に、DBINIT メンバ *RunTimeMVSHLQPrefix*.SAMPLIB（DBINIT）が使用されます。 CA CSM インストーラは、このメンバのコンテンツを設定します。

重要: CA サポート から要求された場合のみ、メンバのコンテンツを変更してください。 キーワードに設定された値の中には、CA CSM セットアップ オプション ファイルと *RunTimeMVSHLQPrefix*.SAMPLIB（DBINIT）メンバの間で異なるものもあります。 そのため、CA サポート からの指示に忠実に従うことが重要です。

DBINIT メンバは、CA CSM スタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））の DBINIT DD に割り当てられます。 DBINIT メンバは、CA CSM が初めて実行されるときにのみ使用されます。

起動中、DBINIT メンバから取得した値はデータベースに格納されます。 1 回だけ設定できる値があります。 それらを変更することはできず、値を変更してもまったく効果がありません。 後で CA CSM Web ベース インターフェースを使用して、その他の値を修正できます。

Web ベース インターフェースを使用して修正できない値を変更するには、DBUPDATE DD (P. 158) を使用します。 DBUPDATE DD は、CA CSM の起動中に処理されます。

重要: CA サポート から要求された場合のみ、これらの値を更新してください。 それ以外の場合に更新すると、データの不整合が起こる可能性があります。

DBINIT と DBUPDATE のコンテンツはレコードで、# で始まるコメント、または以下の形式での値が設定されます。

```
setting=value
```

値は DBINIT または DBUPDATE 処理中には検証されません。

以下の設定がマウント ポイント マネージャで利用可能です。

mpmPath

CA CSM が作業ファイルに使用する、USS ディレクトリへのパスを定義します。セットアップ ユーティリティの実行時に、このディレクトリが利用可能である必要があります。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Application Root］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この値を変更しても、既存のデータは新しいパスにコピーされません。 新しいパスが有効であることを確認します。

mpmHlq

ファイル システムの割り当てに使用されるプレフィクスを定義します。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Data Set Prefix］フィールドを使用して、Web ベース インターフェースで変更できます。

制限： 40 文字

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmStorclas

［Settings］タブの［Mount Point Management］ページの SMS ストレージ クラスを定義します。

値は空白でもかまいません。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Storage Class］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmVolser

［Settings］タブの［Mount Point Management］ページで、対応する DASD のボリューム シリアル番号を定義します。

値は空白でもかまいません。 値を定義する場合、mpmVolser はオンライン ボリュームのボリューム シリアル番号である必要があります。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［VOLSER］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmFilesystemType

ファイル システムの割り当てに使用されるファイル システム タイプを指定します。

以下のオプションがあります。

- HFS
- zFS

注: zFS ファイル システムの使用をお勧めします。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。 既存のデータ セットはそのまま残します。

mpmAutomount

CA CSM が起動時にすべてのファイル システムをマウントするかどうかを指定します。

以下のオプションがあります。

- true
- false

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Automount check］チェック ボックスを使用して変更できます。

mpmunit

［Settings］タブの［Mount Point Management］ページで、データ セットを配置する DASD のタイプを指定します。

この値は Web ベース インターフェースで、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Unit］フィールドを使用して変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmDataClas

［Settings］タブの［Mount Point Management］ページで、ファイル システム データ セットの SMS データ クラスを指定します。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Data Class］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmMgmtClas

［Settings］タブの［Mount Point Management］ページでファイル システム データ セットに対する SMS 管理クラスを指定します。

この値は、［Settings］タブの［System Settings］ - ［Mount Point Management］ページの［Storage Class］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

mpmAllocation

［Settings］タブの［Mount Point Management］ページで、ファイル システムに新しいデータ セットを割り当てるときに SMS を使用するかどうかを指定します。

以下のオプションがあります。

- SMS
- NONSMS

mpmStorclas が定義されている場合、mpmAllocation は SMS として扱われます。 それ以外の場合、mpmAllocation は NONSMS として扱われます。

この値は、［Settings］タブの［System Settings］-［Mount Point Management］ページの［Use SMS］または［Use Non-SMS］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

以下の設定がソフトウェア カタログで利用可能です。

scDatasetPrefix

データ セット名のサフィックスを指定します。データ セットには内部生成カウンタもあります。

名前の形式は、以下のとおりです。

`mpmHlq.scDatasetPrefix`*n*

この値は、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Data Set Suffix］フィールドを使用して、Web ベース インターフェースで変更できます。

注: この設定を変更する場合、その設定は新しく割り当てられたデータ セットに対してのみ使用されます。

scRoot

CA サポート Online Web サイトから取得したパッケージを格納する、カスタマ サイトの Software Catalog データベースのルート ディレクトリを定義します。 ディレクトリは CA CSM のアプリケーション ルート、mpmPath と関連付けられています。

この値は、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Root Directory］フィールドを使用して、Web ベース インターフェースで変更できます。

注: 新しいパスが有効なソフトウェア カタログのルートを指していることを確認してください。

scPrimBig

USS データベースの、製品またはリリース レベルで暗黙的にマウントされているデータ セットの初期量のデフォルト値を指定します。

この値は、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Primary Quantity］フィールドを使用して、Web ベース インターフェースで変更できます。

scSecBig

USS データベースの、製品またはリリース レベルで暗黙的にマウントされているデータ セットの増分量のデフォルト値を指定します。

この値は、［Settings］タブの［System Settings］ - ［Software Catalog］ページの［Secondary Quantity］フィールドを使用して、Web ベース インターフェースで変更できます。

以下の設定が CA DSI Server で利用可能です。

dsiHost

CA CSM がセキュリティ機能を提供するために内部で使用する、CA DSI Server のホスト名を指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

dsiPort

CA CSM がセキュリティ機能を提供するために内部で使用する、CA DSI Server のポート番号を指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

dsiConf

CA DSI Server 設定ファイルのパスを指定します。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

以下の設定がソフトウェア インストール サービスで利用可能です。

sisGimunzipTempPrefix

製品のインストールとメンテナンス中に GIMUNZIP 出力一時データ セットを割り当てるために CA CSM が使用するプレフィクスを定義します。データ セットの名前は、*prefix.jobname.unpacked_file_name* のようになります。 作成された一時作業ファイルは、SMP/E で制御されたデータ セットではありません。 CA CSM は製品インストール プロセスで、それらのファイルを削除します。 これらのファイルは、製品を SMP/E 環境のグローバル ゾーンに RECEIVE する際に、SMP/E 処理の入力関連ファイルとして使用されます。

この値は、［Settings］タブの［Software Installation］ページの［GIMUNZIP Temporary Prefix］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

制限： 12 ～ 19 文字（*ジョブ名*に使用される文字数により異なる）

注: デフォルトの 6 文字の *ジョブ名*を使用する場合、GIMUNZIP 一時プレフィクスには 14 文字まで入力できます。

sisExecutorServerDsnPrefix

実行されたプログラムによって使用される一時データ セット用のプレフィクスを定義します。

一時データ セットの名前は、以下の形式になります : *prefix*.R*n*.*ddname*（*n* は実行リクエスト番号です）。

この値は、［Settings］タブの［Software Installation］ページの［Temporary Data Set Prefix］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

デフォルト： *userid*.CAMSM.*jobname*

制限： 24 文字

sisGimunzipTempVolser

インストール中に GIMUNZIP によって作成された一時データ セットに使用する DASD のボリューム シリアル番号を指定します。

この値は、［Settings］タブの［Software Installation］ページの［GIMUNZIP Temporary VOLSER］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

制限： 1 ～ 6 文字の英数文字またはアスタリスク（*）。 アスタリスクを指定すると、自動クラス選択（ACS）ルーチンが許可する場合、SMS は新しい VSAM データ セット用のボリュームを割り当てます。

sisExecutorOutputStorclas

実行したプログラムが一時データ用に使用するデータ セットの SMS ストレージ クラスを指定します。

この値は、［Settings］タブの［Software Installation］ページの［Storage Class］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

sisExecutorOutputVolser

実行されたプログラムが一時データ用に使用するデータ セットに使用する DASD のボリューム シリアル番号を指定します。

この値は、［Settings］タブの［Software Installation］ページの［VOLSER］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

制限： 1 ～ 6 文字の英数文字

sisExecutorOutputUnit

実行されたプログラムが一時データ用に使用するデータ セットを配置する DASD のタイプを指定します。

この値は、［Settings］タブの［Software Installation］ページの［Unit］フィールド（［System Settings］と［User Settings］の両方）を使用して、Web ベース インターフェースで変更できます。

以下の設定が PAS コンポーネント キーに対して利用可能です。

PASAdvancedSettingsPDS

FTP プロキシの拡張設定のサンプルが格納されるメンバのデータ セットを定義します。

デフォルト： *RunTimeMVSHLQPrefix*.SAMPLIB

RunTimeMVSHLQPrefix

CA CSM ランタイム データ セットのプレフィクスを指定します。これはターゲット データ セットのランタイム コピーです。

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

PASAdvancedSettingsMember

FTP 拡張プロキシ設定を設定できる FTP プロキシ拡張設定のサンプルが格納されるメンバを定義します。

デフォルト： PASADVOP

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

以下の設定がタスク管理に対して利用可能です。

sysTaskDeleteOverrideEnabled

CA CSM 内のセキュリティ機能が無効なとき、すべての CA CSM ユーザが完了したタスクを削除できるようにします。

true

任意のユーザが任意の完了タスクを削除できます。

false

ユーザは完了したタスクを削除できません。

注: セキュリティ機能が CA CSM で有効な場合、タスクの削除はセキュリティ リソース (P. 141)によって管理されるため、このパラメータは無視されます。

デフォルト： なし

この値は Web ベース インターフェースで変更できませんが、DBUPDATE を使用して修正できます。

DBUPDATE DD を使用した値の修正

DBUPDATE DD を使用して CA CSM データベース内の入力値を修正するには、CA CSM のスタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に DBUPDATE DD を追加します。

以下の手順に従います。

1. *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバを作成します。
2. 修正する *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバ内の設定（P. 149）およびその値のみを追加します。
3. CA CSM のスタートアップ JCL（*RunTimeMVSHLQPrefix*.JCL（MSMTCSRV））に *RunTimeMVSHLQPrefix*.SAMPLIB（DBUPDATE）メンバを指す DBUPDATE DD を追加します。
4. CA CSM アプリケーション サーバを再起動します。
5. *RunTimeMVSHLQPrefix*.JCL（MSMTCSRV）内の DBUPDATE DD をコメントアウトします。

ASCII 設定ファイル

tomcat/conf フォルダ内のすべてのファイルおよび tomcat/webapps/MSM フォルダ内のすべての設定ファイルは、ASCII に格納されます。 したがって、標準的な方法でこれらのファイルを編集することはできません。 このセクションでは、いくつかの ASCII ファイルを紹介し、それらを編集する方法について説明します。

ASCII ファイルの編集

いくつかのテキスト ファイルは、USS に ASCII で保存されます。 EBCDIC のようなファイルを開こうとすると、バイナリで表示されることがあります。

ASCII の要件は Java に起因するものです。Java は ASCII でのみ実行されます。USS （OMVS）は ASCII と EBCDIC のコードを実行できます。

注: OEDIT と ISHELL は EBCDIC 用であり、ASCII ファイルの編集には使用できません。

以下のいずれかの方法を使用して、ASCII モードのファイルを編集できます。

- USS からの ASCII ファイルを直接編集できる、サードパーティ製のユーティリティを使用します。
- 以下の手順で、ASCII ファイルをテキスト エディタでローカルで編集します。

  1. FTP を使用して、バイナリ モードでコンピュータにファイルをダウンロードします。これにより、エンコードは転送中に変更されません。
  2. コンピュータ上のファイルをテキスト エディタで編集します。
  3. FTP を使用して、ファイルをバイナリで再度アップロードします。
- 以下の手順で、USS 内の ISPF UI Tool を使用して ASCII ファイルを編集します。

  1. ISPF プライマリ オプション メニューから［UTILITIES］を選択します。

     ［Utility Selection Panel］が開きます。
  2. ［Udlist］を選択します。

     ［z/OS UNIX Directory List Utility］が開きます。
  3. パス名を入力し、次に通常の USS コマンドを使用し、必要なディレクトリまでパスをたどります。
  4. ユーザをスーパーユーザにし、適切なファイル上で EA コマンドを入力します。

ファイルは読み取り可能な形式のため、更新することができます。

context.xml パラメータ

context.xml ファイル内の値を編集できます。 context.xml ファイルは ASCII ファイルです。 このファイルを編集する (P. 158)場合、特殊な処理を使用します。

context.xml 内のいくつかのパラメータは、CUSMAC(SRVLIB) メンバ内の対応するパラメータに依存します。

- context.xml で ServerName の値を変更する場合は、それに応じて、CUSMAC(SRVLIB) メンバ内の SERVERNAME パラメータを変更します。

- context.xml で ApplicationID の値を変更する場合は、それに応じて、CUSMAC(SRVLIB) メンバ内の APPLID パラメータを変更します。
- CUSMAC(SRVLIB) メンバで PROTOCOL=BOTH を定義している場合は、context.xml 内の以下のパラメータを設定します。

  HostPort

  このパラメータが CUSMAC(SRVLIB) メンバ内の TCPIP_PORT オプションに一致していることを確認します。

  ConnectType

  このパラメータを TCP に設定します。
- PROTOCOL=CCI を定義しているか、PROTOCOL を定義しておらず、それがデフォルト値の PROTOCOL=CCI に設定されている場合は、context.xml 内の以下のパラメータを設定します。

  HostPort

  このパラメータがユーザのシステム上の CA Common Services for z/OS で設定される CA CCITCP または CCISSL ポート番号に一致していることを確認します。

  ConnectType

  このパラメータを CCI に設定します。

以下の例は context.xml のサンプルです。

```
url="jdbc:datacom:/ServerName=SRVMUF,SystemID=A31SENF, ApplicationID=SRVMUF,
HostPort=1202,ConnectType=CCI, HostName=AA01,UserID=SWMGRQA"
```

URL 文字列は以下のパラメータから構成されます。

ServerName

CA CSM アプリケーション サーバが使用する CA Datacom/MSM サーバを定義します。

SystemID

CA CSM アプリケーション サーバが使用するシステムの CA-ENF CAICCI SYSID を定義します。

ApplicationID

CA Datacom/MSM サーバ名を定義します。

HostPort

CUSMAC(SRVLIB) メンバ内の PROTOCOL パラメータの設定方法に応じて、システムの CA Common Services for z/OS で設定される CA CCITCP または CCISSL ポート番号（たとえば、1202）、または CUSMAC(SRVLIB) メンバ内の TCPIP_PORT パラメータの値を定義します。

ConnectType

CA CSM アプリケーション サーバ (P. 203) と CA Datacom/MSM サーバ間の接続のタイプを定義します。 CUSMAC(SRVLIB) メンバ内の PROTOCOL パラメータの定義内容に従って、このパラメータを CCI または TCP に設定します。

HostName

お使いのシステムのホスト システムの名前または IP アドレスを定義します。

UserID

データベースにアクセスするために CA CSM によって使用される、ユーザ ID を定義します。

ジョブ割り当て詳細

このセクションでは、z/OS および USS の詳細、また CA CSM がインストールされた後に作成されるファイルおよびフォルダの詳細について説明します。

以下のジョブは、CA CSM のインストールまたはアップグレードのどちらが実行されているかに基づいてサブミットされます。 ジョブ名は、CSM*axxyy* の形式です。

a

新規インストール（N）か、アップグレード（U）かを表します。

xx

どのバージョンからアップグレードするかを示します または、新規インストールに対しては 60 を指定します。

yy

ジョブのシーケンス番号を表します。

このセクションには、以下のトピックが含まれています。

- CSMaxx01（P. 162）（新規インストールとアップグレード）
- CSMaxx04（P. 165）（新規インストールとアップグレード）
- CSMaxx07（P. 165）（新規インストールとアップグレード）
- CSMN6009（P. 166）（新規インストールのみ）
- CSMU5102（P. 167）（CA CSM R5.1 からのアップグレードのみ）
- CSMU5002（P. 169）（CA MSM V5.0 からのアップグレードのみ）
- CSMU4102（P. 170）（CA MSM R4.1 からのアップグレードのみ）
- CSMUxx09（P. 172）（アップグレードのみ）

CSMaxx01

以下の表は、このジョブが実行されるときに作成されるデータ セットおよび USS ファイルの一覧を示します。

注: シリンダの基本数量の合計は、922/3390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<CSIHLQ>.SMPCSI.CSI	該当なし	該当なし	該当なし
<CSIHLQ>.SMPCSI.CSI.DATA	CYLS	15	
<CSIHLQ>.SMPCSI.CSI.INDEX	CYLS	2	
<CSIHLQ>.SMPHOLD	CYLS	5	1
<CSIHLQ>.SMPLOG	CYLS	5	5
<CSIHLQ>.SMPLOGA	CYLS	5	5
<CSIHLQ>.SMPLTS	CYLS	5	5
<CSIHLQ>.SMPMTS	CYLS	5	5
<CSIHLQ>.SMPPTS	CYLS	187	10
<CSIHLQ>.SMPSCDS	CYLS	4	1
<CSIHLQ>.SMPSTS	CYLS	5	5
<DatabaseHLQ>.MSM.ADCXX.BKP	CYLS	1	17

名前	スペース単位	基本数量	2 次数量
<DatabaseHLQ>.MSM.DB002.BKP	CYLS	7	17
<DatabaseHLQ>.MSM.DB015.BKP	CYLS	3	17
<DatabaseHLQ>.MSM.JNL4000.BKP	CYLS	1	15
<DatabaseHLQ>.MSM.PCY4000.BKP	CYLS	1	15
<DatabaseHLQ>.MSM.SRG4000.BKP	CYLS	1	15
<DlibHLQ>.AAAXDATV	CYLS	40	6
<DlibHLQ>.AAAXHFS	CYLS	10	10
<DlibHLQ>.AAAXMAC	CYLS	6	2
<DlibHLQ>.AAAXMOD0	CYLS	140	1
<DlibHLQ>.AAAXSAMP	CYLS	10	1
<DlibHLQ>.AAAXML	CYLS	5	1
<DlibHLQ>.AEG1JAR	CYLS	30	2
<DlibHLQ>.AEG1SHSC	CYLS	1	1
<DlibHLQ>.AEGPHFS	CYLS	30	10
<DlibHLQ>.AEGPJAR	CYLS	80	10
<DlibHLQ>.AEGPJCL	CYLS	1	1
<DlibHLQ>.AEGPPROC	CYLS	1	1
<DlibHLQ>.AEGPSAMP	CYLS	1	1
<MSMPATH>/CEG1JAR	該当なし		
<MSMPATH>/CEG1SHSC	該当なし		
<MSMPATH>/CEGPHFS	該当なし		
<MSMPATH>/CEGPJAR	該当なし		
<MSMPATH>/datacom/dbsrv	該当なし		
<MSMPATH>/dsi	該当なし		
<RunTimeMVSHLQPrefix>.CAAXLOAD	CYLS	140	5
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO1	CYLS	50	5
<RunTimeMVSHLQPrefix>.CAAXLOAD.BO2	CYLS	50	5

名前	スペース単位	基本数量	2 次数量
<RunTimeMVSHLQPrefix>.CAAXMAC	CYLS	6	1
<RunTimeMVSHLQPrefix>.CAAXSAMP	CYLS	10	2
<RunTimeMVSHLQPrefix>.CUSLIB	TRKS	100	15
<RunTimeMVSHLQPrefix>.CUSMAC	TRKS	30	15
<RunTimeMVSHLQPrefix>.DEPLOYIN	CYLS	1	1
<RunTimeMVSHLQPrefix>.JCL	CYLS	1	2
<RunTimeMVSHLQPrefix>.PROCLIB	CYLS	1	1
<RunTimeMVSHLQPrefix>.SAMPLIB	CYLS	2	1
<RunTimeMVSHLQPrefix>.SYSPRINT	CYLS	1	1
<RunTimeUSSPath>/dsi	該当なし		
<RunTimeUSSPath>/tomcat	該当なし		
<TargetHLQ>.CAAXDATV	CYLS	40	6
<TargetHLQ>.CAAXLOAD	CYLS	140	5
<TargetHLQ>.CAAXLPA	TRKS	12	6
<TargetHLQ>.CAAXMAC	CYLS	6	1
<TargetHLQ>.CAAXSAMP	CYLS	10	1
<TargetHLQ>.CABDXML	CYLS	10	2
<TargetHLQ>.CEGPJCL	CYLS	2	1
<TargetHLQ>.CEGPPROC	CYLS	1	1
<TargetHLQ>.CEGPSAMP	CYLS	1	1

CSMaxx04

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの基本数量の合計は、10/3390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.CUSMAC	TRKS	30	15
<dbHLQ>.CUSLIB	TRKS	100	15

CSMaxx07

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの基本数量の合計は、540/3390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.CBS1006	CYLS	15	15
<dbHLQ>.CXX	CYLS	35	10
<dbHLQ>.DDD015	CYLS	15	15
<dbHLQ>.DD1002	CYLS	60	15
<dbHLQ>.FXX	CYLS	90	15
<dbHLQ>.IXX002	CYLS	45	15
<dbHLQ>.IXX006	CYLS	15	15
<dbHLQ>.IXX015	CYLS	15	15
<dbHLQ>.IXX016	CYLS	5	5
<dbHLQ>.IXX016	CYLS	5	5
<dbHLQ>.IXX1006	CYLS	15	15
<dbHLQ>.IXX1007	CYLS	10	5

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.LXX	CYLS	90	15
<dbHLQ>.MSG015	CYLS	15	15
<dbHLQ>.PXX	CYLS	90	15
<dbHLQ>.SIT015	CYLS	5	5
<dbHLQ>.SQ1016	CYLS	5	5
<dbHLQ>.TTM017	CYLS	10	5

CSMN6009

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの基本数量の合計は、2,180/3390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.A011007	CYLS	15	5
<dbHLQ>.A021007	CYLS	15	5
<dbHLQ>.AUD4000	CYLS	500	350
<dbHLQ>.DEL1020	CYLS	15	5
<dbHLQ>.INV4000	CYLS	600	100
<dbHLQ>.IXX1007	CYLS	15	15
<dbHLQ>.IXX1018	CYLS	15	5
<dbHLQ>.IXX1019	CYLS	15	15
<dbHLQ>.IXX1020	CYLS	15	5
<dbHLQ>.IXX4000	CYLS	120	30
<dbHLQ>.JNL4000	CYLS	120	30
<dbHLQ>.PCY4000	CYLS	35	15
<dbHLQ>.SCS4000	CYLS	130	60

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.SDS4000	CYLS	180	60
<dbHLQ>.SNP1019	CYLS	15	5
<dbHLQ>.SRG4000	CYLS	60	15
<dbHLQ>.STA1018	CYLS	15	15
<dbHLQ>.XML4000	CYLS	300	300

CSMU5102

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

基本数量スペース割り振りは、関連する z/OS のジョブストリームで定義されている内容を反映した、十分な割り当て量である必要があります。ただし、総量は現在の環境の使用状況に基づいて、実際に必要な量に調整されます。

以下の値は、CA CSM R5.1 から CA CSM バージョン 6.0 にアップグレードする場合に必要です。

注: シリンダの基本数量の合計は、2,060/3390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMU5002

以下の値は、CA MSM V5.0 から CA CSM バージョン 6.0 にアップグレードする場合に必要です。

注: シリンダの基本数量の合計は、2,645/3,390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMU4102

以下の値は、CA MSM R4.1 から CA CSM バージョン 6.0 にアップグレードする場合に必要です。

注: シリンダの基本数量の合計は、3,495/3,390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.CXX.BACKUP	CYLS	35	10
<PREVDBHLQ>.DB4000.BACKUP	CYLS	350	300
<PREVDBHLQ>.DDDBBU.BACKUP	CYLS	60	10
<PREVDBHLQ>.DDDDBU.BACKUP	CYLS	15	15
<PREVDBHLQ>.BEXCLAUD>	CYLS	200	200
<PREVDBHLQ>.BEXCLINV	CYLS	200	200

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.BEXCLJNL	CYLS	200	200
<PREVDBHLQ>.BEXCLPCY	CYLS	200	200
<PREVDBHLQ>.BEXCLSCS	CYLS	200	200
<PREVDBHLQ>.BEXCLSDS	CYLS	200	200
<PREVDBHLQ>.ESDSM94	CYLS	150	150
<PREVDBHLQ>.NSDSM94	CYLS	150	150
<PREVDBHLQ>.ESDSC12	CYLS	150	150
<PREVDBHLQ>.NSDSC12	CYLS	150	150
<PREVDBHLQ>.EAUDAOP	CYLS	15	15
<PREVDBHLQ>.EAUDAVR	CYLS	15	15
<PREVDBHLQ>.ESCSCNP	CYLS	15	15
<PREVDBHLQ>.ESCSCRS	CYLS	15	15
<PREVDBHLQ>.ESCSDUF	CYLS	50	25
<PREVDBHLQ>.ESCSICP	CYLS	15	15
<PREVDBHLQ>.ESCSOPE	CYLS	15	15
<PREVDBHLQ>.ESDSC13	CYLS	50	25
<PREVDBHLQ>.ESDSC23	CYLS	50	25
<PREVDBHLQ>.NSDSC23	CYLS	50	25
<PREVDBHLQ>.ESDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.ESDSSYS	CYLS	15	15
<PREVDBHLQ>.ESRGSR1	CYLS	15	15
<PREVDBHLQ>.NAUDAOP	CYLS	15	15
<PREVDBHLQ>.NAUDAVR	CYLS	15	15
<PREVDBHLQ>.NSCSCNP	CYLS	15	15
<PREVDBHLQ>.NSCSCRS	CYLS	15	15
<PREVDBHLQ>.NSCSICP	CYLS	15	15

名前	スペース単位	基本数量	2 次数量
<PREVDBHLQ>.NSCSOPE	CYLS	15	15
<PREVDBHLQ>.NSDSC13	CYLS	50	25
<PREVDBHLQ>.NSDSC24	CYLS	50	25
<PREVDBHLQ>.NSDSSYS	CYLS	15	15
<dbHLQ>.CXX?NAME.BK60CXX	CYLS	35	10
<dbHLQ>.CXX?NAME.BK600002	CYLS	60	15
<dbHLQ>.CXX?NAME.BK6000015	CYLS	15	15
<dbHLQ>.CXX?NAME.BK604000	CYLS	350	300

CSMUxx09

以下の表は、このジョブが実行されるときに作成されるデータ セットの一覧を示します。

注: シリンダの基本数量の合計は 460/3,390 DASD スペースです。

名前	スペース単位	基本数量	2 次数量
<dbHLQ>.BK60CXX	CYLS	35	10
<dbHLQ>.BK600002	CYLS	60	15
<dbHLQ>.BK600015	CYLS	15	15
<dbHLQ>.BK604000	CYLS	350	300

付録 B: 外部インターフェース

Web ベース インターフェースを使用して実行するタスクの一部は、外部インターフェースを使用して、CA CSM の外部で実行することもできます。CA CSM は外部アプリケーションからコマンドを受け取り、それらを適切な形式に変換し、それらに基づいてタスクを生成できます。

CA CSM の外部でタスクを実行

外部スケジューラを使用して、カタログ ツリーの更新や、製品および製品リリースに対する更新の取得などの PAS タスクを定期的に実行できます。 タスク管理ポリシーの実行および log4j 設定の変更なども行うことができます。

スケジューラをセットアップして MVS コマンド MODIFY （F）に変換されるコマンドを発行します。 このコマンドは、ユーザ ID、実行するコマンド タイプおよびそのプロパティなどのパラメータ セットを取得します。

注: スケジューラの設定方法の詳細については、該当ドキュメントを参照してください。

スケジュールされたタスクが実行されるごとに、CA CSM では受信されるコマンドを検証します。 検証が成功した場合、CA CSM で適切なタスクが作成され、実行されます。 ［Tasks］タブからタスク ステータスを表示できます。

注: 自動更新をセットアップするには、有効な TSO ユーザ ID、および CA サポート Online Web サイトでセットアップされたアカウントが必要です。

MVS MODIFY コマンド

MODIFY （F）コマンドによって以下のアクションを実行できます。

- 製品ツリーの更新
- 製品および製品リリースの更新
- タスク管理ポリシーの実行
- log4j 設定の変更

各アクションのコマンドには特定のパラメータ セットが含まれます。

MODIFY コマンドの形式は以下のとおりです。

F *jobname*,APPL=*command*,*parameter*=*value*[,*parameter*=*value*,…]

jobname

開始されるジョブの名前を定義します。

APPL=*command*

発行されるコマンドを定義します。

command

コマンド タイプを指定します。 下記のオプションが利用可能です。

UPDTTREE

製品ツリーを更新します。

UPDTCAT

製品および製品リリースを更新します。

CHNGLOG

実行時に一時的に log4j 設定を変更します。

EXECPLCY

タスク管理ポリシーを実行します。

parameter=value

発行するコマンドのタイプによって異なるパラメータを定義します：製品ツリーの更新 (P. 174)、製品または製品リリースの更新 (P. 175)、log4j 設定の変更 (P. 178)、またはタスク管理ポリシーの実行 (P. 179)。

製品ツリーの更新

製品ツリーの更新用のコマンドは以下の形式です。

F *jobname*,APPL=UPDTTREE,USERID=*user_id*[,FILTER=*filter_name*][,VENDOR=*vendor_name*]

USERID=*user_id*

コマンドを発行するユーザを定義します。

FILTER=*filter_name*

（オプション）カタログ ツリーの更新に使用するサイト ID フィルタの名前を定義します。

注: フィルタ名が定義されない場合、コマンドは拒否されます。 フィルタが定義されない場合、すべてのサイト ID が使用されます。VENDOR パラメータが指定される場合、FILTER パラメータは VENDOR パラメータよりも前にくることが必要があります。

VENDOR=*vendor_name*

（オプション）カタログ ツリーを更新するベンダーの名前を定義します。

注: ベンダー名が定義されない場合、コマンドはデフォルト ベンダー（CA）に対して実行されます。

注: コマンド パラメータの順序を変更しないでください。変更すると、解析エラーが発生する場合があります。

例

この例では、CA Technologies メインフレーム製品の製品リストが更新されます。

```
F MSMTC,APPL=UPDTTREE,USERID=MYUSERID,VENDOR=CA
```

製品および製品リリースの更新

製品および製品リリースの更新を取得するコマンドは以下の形式です。

```
F jobname,APPL=UPDTCAT,USERID=user_id,PRODUCT=product_name
[,RELEASE=release_number][,TYPE=FULL|PTFS][,MODE=EXECUTE|CHECK|ATOMIC]
```

USERID=*user_id*

コマンドを発行するユーザを定義します。

PRODUCT=*product_name*

更新を取得する製品名を定義します。

注: 名前が一意ではない（名前の一部を共有する）製品を区別するには、*product_name* に一重引用符を付けます。 たとえば、PRODUCT='CA IDMS SQL OPTION - MVS' では *CA IDMS SQL OPTION - MVS* という名前の製品が検索され、*CA Easytrieve Report Generator CA IDMS SQL OPTION - MVS* は無視されます。.

RELEASE=*release_number*

（オプション）更新を取得する製品リリースを定義します。

TYPE=FULL|PTFS

（オプション）取得する製品またはリリースの更新のタイプを指定します。

注: このタイプがコマンド構文で明示的に定義されていない場合、コマンドは FULL タイプで実行されます。

FULL

製品パッケージおよびメンテナンス パッケージをすべて取得します。 これはデフォルトです。

PTFS

その製品リリースが前回更新された後にリリースされたメンテナンス パッケージのみを取得します。

MODE=EXECUTE|CHECK|ATOMIC

（オプション）製品および製品リリースの更新を取得するコマンドの実行モードを指定します。

注: このモードがコマンド構文で明示的に定義されていない場合、コマンドは EXECUTE タイプで実行されます。

EXECUTE

コマンドを検証し、それに基づいて生成されるタスクを実行します。 これはデフォルトです。

CHECK

コマンドを検証し、エラーを返しますが、タスクは実行しません。

ATOMIC

CHECK モードでコマンドを実行することで、コマンドが検証され、それに基づいてタスクが生成されますが、タスクはすぐには実行されません。すべての検証済みタスクが格納されて、全タスクの検証が完了した場合にのみ実行されます。

注: WARNING として定義された検出済みの検証エラーは、すべて SEVERE として処理されます。 重大度レベルが WARNING または SEVERE のエラーによりコマンド全体が失敗します。

注: コマンド パラメータの順序を変更しないでください。変更すると、解析エラーが発生する場合があります。

例

1 つまたは複数の製品で利用可能な更新の取得

これらの例では、CA Panvalet の使用可能なすべてのリリースの更新を取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET – MVS,TYPE=FULL
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS
```

この例では、CA Panvalet、CA Auditor for z/OS、および CA SMF Director のすべての使用可能なリリースの更新を取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS, CA AUDITOR - MVS,
CA SMF DIRECTOR - MVS
```

この例では、CA IDMS SQL OPTION MVS の使用可能なすべてのリリースの更新を取得し、*CA IDMS SQL OPTION MVS* が名前の一部に含まれる製品の更新は無視します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION MVS'
```

1 つの製品の特定の更新の取得

この例では、CA SMF Director のリリース 6.0、11.0 および 12.0 の更新を CHECK モードで取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=6.0,11.0,12.0,MODE=CHECK
```

この例では、CA IDMS SQL OPTION MVS のリリース 16.0 の更新を取得し、*CA IDMS SQL OPTION MVS* が名前の一部に含まれる製品の更新は無視します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION
MVS',RELEASE=16.0
```

複数製品の特定の/利用可能な更新の取得

この例では、CA SMF Director のリリース 6.0 および 11.0 の更新、および CA Panvalet のすべての使用可能なリリースの更新を ATOMIC モードで取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=6.0,11.0,PRODUCT=CA PANVALET - MVS,MODE=ATOMIC
```

この例では、CA SMF Director のリリース 12.0 および CA Panvalet のリリース 14.5 の更新を取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA SMF DIRECTOR -
MVS,RELEASE=12.0,PRODUCT=CA PANVALET - MVS,RELEASE=14.5
```

この例では、CA Auditor for z/OS のリリース 12.1 の前回の更新後にリリースされたその製品リリース用のメンテナンス パッケージのみを取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA AUDITOR -
MVS,RELEASE=12.1,TYPE=PTFS
```

この例では、CA Panvalet のその製品リリースの前回の更新後にリリースされた CA Panvalet の全リリース用のメンテナンス パッケージのみを取得します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT=CA PANVALET - MVS,TYPE=PTFS
```

この例では、CA IDMS SQL OPTION MVS のリリース 16.0 および CA IDMS/DB - MVS のリリース 16.0 の更新を取得し、*CA IDMS SQL OPTION MVS* または *CA IDMS/DB* を名前の一部に含む製品の更新は無視します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION
MVS',RELEASE=16.0,PRODUCT='CA IDMS/DB - MVS',RELEASE=16.0
```

この例では、CA IDMS SQL OPTION MVS のすべての使用可能なリリース、およびリリース 16.0 および CA IDMS/DB - MVS のすべての使用可能なリリースの更新を取得し、*CA IDMS SQL OPTION MVS* または *CA IDMS/DB - MVS* を名前の一部に含む製品の更新は無視します。

```
F MSMTC,APPL=UPDTCAT,USERID=MYUSERID,PRODUCT='CA IDMS SQL OPTION MVS,CA IDMS/DB
- MVS'
```

log4j 設定の変更

実行時に一時的に log4j 設定を変更するコマンドは以下の形式です。

```
F jobname,APPL=CHNGLOG,logger[*]:loglevel
```

logger

log4j ロガー（通常はクラスまたはパッケージ名）を定義します。

loglevel

DEBUG、INFO、WARN、ERROR または FATAL など、表示するメッセージの最低 log4j レベルを指定します。

注:

- コマンド パラメータの順序を変更しないでください。変更すると、解析エラーが発生する場合があります。
- CA サポートからの指示がない限り、log4j 設定は実行時に変更しないでください。

例

この例では、SCS ロガーの log4j 設定を一時的に警告またはそれ以上（WARN、ERROR または FATAL）に変更します。

```
F MSMTC,APPL=CHNGLOG,com.ca.scs:WARN
```

この例では、すべての SAM 通信ロガーの log4j 設定を一時的にデバッグまたはそれ以上（DEBUG、INFO、WARN、ERROR または FATAL）に変更します。

```
F MSMTC,APPL=CHNGLOG,com.ca.SAM.Communications.*:DEBUG
```

この例では、すべてのロガーの log4j 設定を一時的に情報またはそれ以上（INFO、WARN、ERROR または FATAL）に変更します。

```
F MSMTC,APPL=CHNGLOG,*:INFO
```

タスク管理ポリシーの実行

タスク管理ポリシーを実行するコマンドは以下の形式です。

F *jobname*,APPL=EXECPLCY,USERID=*user_id*,POLICY=*policy_name*

USERID=*user_id*

コマンドを発行するユーザを定義します。

POLICY=*policy_name*

実行するポリシーの名前を指定します。

ポリシー名は CA CSM 内の有効なポリシー名である必要があります。

注: コマンド パラメータの順序を変更しないでください。変更すると、解析エラーが発生する場合があります。

例

この例では、MYARCHIVEPOLICY という名前のタスク管理ポリシーを実行します。

```
F MSMTC,APPL=EXECPLCY,USERID=MYUSERID,POLICY=MYARCHIVEPOLICY
```

コマンド検証

スケジュール済みの更新が実行されるたびに、CA CSM では以下の条件が満たされていることを確認します。

- コマンド形式および構文が正しい。
- コマンドで定義されたデータ（製品名、リリース番号）が有効であり、CA CSM データベース内のデータと一致する。
- コマンドを発行するユーザに適切な認証情報がある。

これらの指示のいずれかが満たされていない場合、以下のイベントが発生します。

- コマンドが実行されない。
- タスクが生成されない。
- CA CSM 領域の JOBLOG 内の STDOUT DDNAME にエラーがログ記録される。

ログ メッセージ

スケジュール済みの更新用のコマンドを発行すると、CA CSM 領域の JOBLOG の STDOUT DDNAME に一連のメッセージが記録されます。 これらのメッセージは、リクエストの処理中に CA CSM が実行する手順を反映しています。

各メッセージは MSMM で始まり、4 桁の数字およびメッセージ ステータス コードが後に続きます。 メッセージ ステータス コードは以下のとおりです。

- I – 情報
- E - エラー
- S - 重大

例

この例では、USER1 が CA Panvalet リリース 14.5 の更新を取得するコマンドを発行した後に、CA CSM 領域の JOBLOG の STDOUT DDNAME に記録されたメッセージを表示します。

```
MSMM0101I - MODIFY command received: UPDTCAT
MSMM0100I - Handling command: UPDTCAT - USERID=USER1,PRODUCT=CA PANVALET -
MVS,RELEASE=14.5
MSMM0191I - Authenticating user: USER1.
MSMM0153E - Release 14.5 for product CA PANVALET - MVS not found in software catalog.
MSMM0162I - PAS task executed for specific product releases.
```

注: CA CSM メッセージの詳細については、「*Message Reference Guide*」を参照してください。

付録 C: トラブルシューティング

この付録が提供する、よくある質問およびトラブルシューティングの情報を使用し、CA CSM を使用するときに起こりうる問題の識別および解決ができるようになります。付録に CA CSM エラー メッセージは含まれていません。

注: CA CSM メッセージの完全なリストについては、「*メッセージ リファレンス ガイド*」を参照してください。

SMP/E 内のメンテナンスの ACCEPT または RESTORE が失敗する

問題の状況:

SMP/E 環境でメンテナンスを ACCEPT または RESTORE しようとすると、タスクが失敗し、また SPMOUT がエラー メッセージのレポートを出力します。

- メンテナンスの ACCEPT に対し、以下のエラー メッセージが出力される場合があります。

  GIM51702S ** THE ACCEPT COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

- メンテナンスの RESTORE に対し、以下のエラー メッセージが出力される場合があります。

  GIM51702S ** THE RESTORE COMMAND WAS NOT PROCESSED BECAUSE NO RELATED ZONE WAS SPECIFIED IN THE ZONE DEFINITION ENTRY.

  GIM50801S ** ZONE *zone_name* WAS NOT USED BECAUSE IT IS NOT DEFINED BY A ZONEINDEX SUBENTRY IN THE GLOBAL ZONE.

理由:

実行しているアクションにより異なりますが、理由は以下のいずれかによるものです。

- メンテナンスを受け入れた場合、影響を受ける配布ゾーンに関連するターゲット ゾーンが SMP/E 環境にないか、関連するターゲット ゾーンが存在しません。
- メンテナンスをリストアした場合、影響を受けるターゲット ゾーンに関連する配布ゾーンが SMP/E 環境にないか、関連する配布ゾーンが存在しません。

解決方法:

- 以下の例のような手順でバッチ ジョブをサブミットし、影響を受ける配布ゾーンに関連する欠落したターゲット ゾーンを追加するか、既存のターゲット ゾーンを定義します。

```
SET
   BOUNDARY(distribution_zone_name) .
UCLIN .
ADD DLIBZONE(distribution_zone_name)
  RELATED(target_zone_name) .
ENDUCL .
```

- 以下の例のような手順でバッチ ジョブをサブミットし、影響を受けるターゲット ゾーンに関連する欠落した配布ゾーンを追加するか、既存の配布ゾーンを定義します。

```
SET
   BOUNDARY(target_zone_name) .
UCLIN .
ADD TARGETZONE(target_zone_name)
  RELATED(distribution_zone_name) .
ENDUCL .
```

CA CSM アドレス空間が正しく機能しない

症状:

SCS アドレス空間が正しく機能しません。また、以下のサンプルのようなメッセージがログに表示されます。

```
MSMC0501E SQL PREPARE VERSIONSTMT for task MSMCJTSK failed, SQLCODE=-124,
SQLSTATE=51002, RETCODE=,
                              IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST
MSMC0501E SQL ROLLBACK for task MSMCJTSK failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0503E SQL error message: PLAN CASWMGT.MSMCFSQL_050_001 DOES NOT EXIST


MSMC0501E SQL PREPARE_DEPUNIT for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
MSMC0501E SQL ROLLBACK for task MSMCIENG failed, SQLCODE=-124, SQLSTATE=51002,
RETCODE=, IRETCODE=X'0000'
```

さらに、以下のようなメッセージが表示されます。

```
MSMC0401E EVTINIT for task MSMCIES0 failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCIENG failed, RETCODE=X'00000020'
MSMC0401E EVTINIT for task MSMCCEVH failed, RETCODE=X'00000020'
```

原因:

CA Datacom/MSM データベース内の SQL プランが最新ではありません。

解決方法:

CA Datacom/MSM データベース内の SQL プランを更新し、同期します。

MSMLOG ファイルの CA CSM アプリケーション サーバ エラー

症状:

CA CSM アプリケーション サーバ MSMLOG ファイルで、以下のエラー メッセージが表示されます。

```
WARNING: Error reading /dev/urandom
Throwable occurred: java.io.FileNotFoundException: /dev/urandom (EDC5157I An
internal error has occurred.)
 at java.io.FileInputStream.<init>(FileInputStream.java:112)
```

理由:

以下の条件が両方とも満たされる場合にのみ、このメッセージが表示されます。

- PTF RO21996 が CA CSM r2.0 （FMID CEG1200）にインストールされています。
- IBM Integrated Cryptographic Service Facility （ICSF）は、CA CSM アプリケーション サーバ セッションを実行している z/OS システム上で開始されていません。

解決方法:

このメッセージが表示されても、CA CSM のパフォーマンスには全く影響しません。また CA CSM は引き続き機能します。 dev/urandom が実行されており、CA CSM と互換性があることを確認する場合は、以下のコマンドを使用します。

```
$ cat </dev/urandom | head -c12 | od -X
```

コマンドを実行すると、エラーのないランダム データが返ってきます。以下に例を示します。

```
0000000000          60621BCF        8AAD1F12        8944D619
0000000014
```

デバイスが動作していない場合、警告メッセージが表示されます。 以下に例を示します。

```
FSUM7343 cannot open "/dev/urandom" for input: EDC5157I An internal error
has occurred.
0000000000
```

このエラー メッセージが表示される場合は、/dev/random デバイスを再設定し、コマンドがこのデバイスから正常に読み取れるようにします。

注: /dev/random デバイスの詳細については、IBM の「*z/OS V1R10.0 UNIX System Services Planning*」（GA22-7800-14）を参照してください。

MSMLOG ファイルの起動時の CA CSM アプリケーション サーバ エラー

症状:

CA CSM アプリケーション サーバが起動中に失敗し、MSMLOG ファイルに以下のエラー メッセージが表示されます。

```
SEVERE: StandardServer.await: create[22150]:
Throwable occurred: java.net.BindException: EDC8116I Address not available.
              at java.net.PlainSocketImpl.socketBind(Native Method)
              at java.net.PlainSocketImpl.bind(PlainSocketImpl.java:384)
              at java.net.ServerSocket.bind(ServerSocket.java:331)
```

原因:

localhost Domain Name System（DNS）エントリが、ローカルの DNS に定義されていません。

解決方法:

ネットワーク管理者は、localhost の DNS エントリを定義する必要があります。

CA CSM アプリケーション サーバのタイムアウト

症状:

メンテナンス パッケージの一覧を選択して表示すると、以下のメッセージが表示されます。

```
Reading maintenance packages from Software Catalog
```

その後、以下のエラー メッセージが表示されます。

```
The call failed on the server; see server log for details
```

MSMTC ジョブのログに、以下のメッセージが表示されます。

```
SEVERE: Exception while dispatching incoming RPC call
Throwable occurred: java.net.SocketTimeoutException: Read timed out
at java.net.SocketInputStream.read(SocketInputStream.java:140)
```

この問題は、Microsoft Internet Explorer で CA CSM の作業を行っているときのみ発生します。

原因:

CA CSM は大量のデータ表示に失敗します。

解決方法:

必要に応じ、以下の手順を実行します。

1. 表示する表の行数を確認します。 この数は、［Settings］タブの［User Settings］ -［User Preferences］ページの［Table Rows］フィールドで定義されます。 行の数が 250 の場合は、それをより低い値（たとえば 50 または 100）に設定します。

2. 表の行数を 250 のまま維持する必要がある理由がある場合は、CA CSM アプリケーション サーバのタイムアウト パラメータを更新します。

   tomcat/conf ディレクトリにある server.xml ファイルで、以下の行を見つけます。

   ```
   connectionTimeout="20000"
   ```

   このパラメータは、TCP/IP スタックが着信パケットを待機する時間（ミリ秒）を定義します。 このパラメータを、より大きな値（たとえば、180000）に設定します。 次に、変更を有効にするために、CA CSM アプリケーション サーバを再起動します。

   注: server.xml ファイルは、ASCII で保存されます。

詳細情報:

ASCII ファイルの編集 (P. 158)

SAF セキュリティが有効な状態での CA CSM の開始に失敗する

症状:

SAF セキュリティが有効な状態で、CA CSM が失敗します。 RC=13 または RC=15 の SafError がジョブのログに表示されます。 ログは以下の例のようなエラー メッセージを表示します。

```
FATAL (main) 2012-06-13 14:12:37,056
(SafManagerImpl.java:434):SafManager–initialize
DSI():Return code from DDSI_java_open is higher than zero.RC=13
FATAL (main) 2012-06-13 14:12:37,067 (SystemManager.java:491):
com.ca.mf20.zos.services.saf.errors.SafError: null

Additional Diagnostic Data:
Error during DSI java open. RC=13
Path to 'dsi.conf': /u/users/msmr51/msmruntime/dsi/dsi.conf
BEGINNING OF 'dsi.conf’:
This is the DSI Server component configuration file
host localhost
port 22130
TLSKeyringFile /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.kdb
TLSKeyringStash /u/users/msmdev/dsi/cert/CA_SelfSigned_Server.sth
TLSKeyLabel "Cert for SelfSigned Server"
TLSVerifyClient ON
END OF 'dsi.conf'
```

```
DSI parameters from table USERCONFIG in database:
Required parameters are marked with (*):
KEY:            DEFAULT_VALUE:  VALUE
*dsiPort:       22130:          22130
*dsiHost:       localhost:      localhost
*dsiConf:       N/A:            /u/users/msmr51/msmruntime/dsi/dsi.conf
>dsiKdb:        N/A:            Uninitialized
>dsiSth:        N/A:            Uninitialized
>dsiLabel:      N/A:            Uninitialized
>dsiVerPeer:    N/A:            false
```

解決方法:

必要に応じて、以下の手順を実行します。

- localhost エントリがユーザの DNS で定義されているかどうかを確認します。 以下の USS コマンドを発行します。

  ```
  oping localhost
  ```

  コマンドによりエラー メッセージ（EZZ3111I Unknown host 'localhost'）が返される場合、localhost エントリが定義されていません。この場合、以下のいずれかのアクションを実行します。

  - ネットワーク管理者に依頼し、ユーザの DNS に localhost エントリを定義します。
  - USERCONFIG データベース テーブルおよび dsi.conf で、dsiHost エントリを 127.0.0.1 に設定します (P. 158)。

- dsi.conf ファイル内の host および port パラメータが、USERCONFIG データベース テーブルの dsiHost および dsiPort のパラメータと同じであることを確認します。 host と dsiHost、および port と dsiPort のパラメータが異なる場合は、dsi.conf ファイルまたはデータベース エントリ (P. 158)のいずれかを更新します。 dsi.conf ファイルのコンテンツ、USERCONFIG データベース テーブルの CA DSI Server パラメータ、および dsi.conf ファイルへのパスが、エラー メッセージに表示されます。

- CA DSI Server のポート（port および dsiPort）が開放されていることを確認します。 以下の USS コマンドを発行します。

  ```
  onetstat -P port_number
  ```

  以下に例を示します。

  ```
  onetstat –P 22130
  ```

  このコマンドによって空の表が返される場合、ポートは開放されています。

- CA DSI Server のポートが CA CSM 用に予約済みかどうかを確認します。以下の USS コマンドを発行します。

  ```
  onetstat -o
  ```

  このコマンドは、予約済みポートの一覧を表示します。 CA DSI Server ポートが表示されない場合、CA DSI Server ポートを予約することをお勧めします。

CA CSM が例外で失敗する

症状:

CA CSM が、たとえば以下のような例外で失敗します。

```
MSM0008E - System startup failed - please see error output for further information.
Fatal error that has stopped the startup was:
or g.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online in
Session(connect)).

MSM0010E - CA CSM startup failed.

FATAL (main) 2011-01-12 15:05:15,098 (SystemManager.java:333): java.lang.Error:
org.apache.tomcat.dbcp.dbcp.SQLNestedException: Cannot create
PoolableConnectionFactory (IO error sending or receiving native data:
ca.datacom.db.DBIOException: CCICONV FAILURE:  No receiver online
in Session(connect))
```

原因:

CUSMAC(SRVLIB) メンバと context.xml ファイルの両方で、CA Datacom/MSM サーバの ServerName、または ApplicationID が一致しません。

解決方法:

context.xml または CUSMAC(SRVLIB) のいずれかで ServerName または ApplicationID を変更し (P. 159)、それらが一致するようにします。

[Tasks]タブの[Delete Task]ボタンが無効

問題の状況:

［Tasks］タブからタスクを削除できません。また［Delete Task］ボタンが無効です。

理由:

タスクを削除するためのアクセス権がありません。

解決方法:

CA CSM のセキュリティ機能が有効かどうかを確認し、以下のいずれかのアクションを実行します。

- セキュリティ機能が有効な場合は、以下のリソース プロファイルが作成されていることを確認します。

  TM.TASK.@SELF.DELETE

  ユーザ自身のタスクを削除するためのアクセス権を付与します。

  TM.TASK.SYSTEM.DELETE

  任意のタスクを削除するためのアクセス権を付与します。

- セキュリティ機能が無効な場合は、CA CSM オプション ファイルで以下のオプションが指定されていることを確認します。

  `sysTaskDeleteOverrideEnabled=Y`

  sysTaskDeleteOverrideEnabled

  CA CSM ユーザにタスクの削除を許可するかどうかを指定します。

  Y

  任意のユーザが任意の完了タスクを削除できます。

  N

  ユーザは完了したタスクを削除できません。

  デフォルト： N

SMPOUT の展開で、GIMUNZIP メッセージが表示される

症状:

展開タスクの SMPOUT レポートで、メッセージ GIM69158I が表示されます。

原因:

展開を実行するユーザに UNIX SUPERUSER 属性がないか、それらに権限が割り当てられていないときにメッセージが表示されます。 ターゲット システムの GIMUNZIP の動作は、SUPERUSER 属性の存在に影響を受けます。

解決方法:

このメッセージは情報提供用です。

注: メッセージに関連する特定のリターン コードまたは理由コードの詳細については、「*IBM SMP/E Messages and Codes*」を参照してください。

一時データ セットおよび RELFILE データ セットの動的割り当てエラー

問題の状況:

一時データ セットと RELFILE データ セットの動的な割り当てエラーが発生します。

理由:

HLQ オプションが、使用が許可されていない値に設定されています。

解決方法:

HLQ オプションを、使用が許可されている値に変更します。

ソフトウェア インストール中の MACLIB ライブラリの動的な割り当てが失敗する

問題の状況:

製品インストール中に SMP/E 環境を作成すると、メッセージ ログに以下のエラーが表示されます。

```
Dynamic allocation of input data set member SYS1.MACLIB(GIMZPOOL) failed. DD: ZP3 RC: 4 Error code: 0x1708 Info code: 0x2.
```

理由:

CA CSM がデフォルトの MACLIB ライブラリ、SYS1.MACLIB を見つけることができません。 たとえば、ライブラリの名前が変更されたことなどが理由です。

解決方法:

SAMPLIB (MSMLIB) メンバで、新しい Java ランタイム オプション maclib.dsn 変数を定義します。新しいデータ セット名が 38 文字を超えていないことを確認してください。

例:

```
IJO="$IJO -Dmaclib.dsn=CUSTOM.MACLIB"
```

不正な製品更新成功ステータス

問題の状況:

CA CSM は、Succeeded ステータスで製品更新を完了しますが、ソフトウェア カタログが更新されていません。

注: HTTPS ダウンロードがアクティブなとき、この問題は発生しません。

理由:

Pax と ESD の製品ファイルは、即時ダウンロードが利用できないことがあります。 この状況が発生すると、CA CSM は Request Product PrePackage 処理を開始します。 この処理によってこれらのファイルは Web ページで使用可能になり、処理が完了するとユーザに電子メールが送信されます。CA サポート Online Web サイトの内部的な変更が理由で、CA CSM は CA CSM Build 442 PTF 5EGP442、またはそれ以降のバージョンがインストールされないかぎり、Request Product PrePackage 処理を開始しません。

解決方法:

CA CSM Build 442 PTF 5EGP442 またはそれ以降のバージョンがインストールされていることを確認してください。

GIM54701S ** ALLOCATION FAILED FOR SMPJHOME

問題の状況:

メンテナンス パッケージを APPLY すると、以下の SMP/E エラー メッセージが表示されます。

```
GIM54701S ** ALLOCATION FAILED FOR SMPJHOME - IKJ56228I PATH
/sys/java31bt/v6r0m0/usr/lpp/java/J6.0 NOT IN CATALOG OR CATALOG CAN NOT BE ACCESSED.
```

注: CA CSM が必須パスを指定しないため、Java ホーム パスが、旧メッセージの Java ホーム パスとは異なっている可能性があります。

理由:

メンテナンス パッケージを APPLY した SMP/E 環境で、SMPJHOME DDDEF が正しく設定されていません。

解決方法:

SMP/E 環境の SMPJHOME DDDEF を変更します。

- SMPJHOME DDDEF が CA CSM SMP/E 環境で正しく設定されていない場合、UCLIN ステートメントを使用し、CA CSM SMP/E 環境の SMPJHOME DDDEF を修正します。 (P. 83)
- SMPJHOME DDDEF が別の SMP/E 環境で正しく設定されていない場合は、UCLIN ステートメントを使用し、SMP/E 環境内のすべてのゾーンでの SMPJHOME DDDEF を修正します (P. 83)。

SMP/E が生成したデータ セットで I/O エラーが発生する

症状:

製品のインストール、またはメンテナンス パッケージの管理を行おうとすると、タスク出力がある 1 つ以上の手順がタスクに不足しています。これらの手順は、SMPLIST、SMPPRINT、SYSPRINT、SYSTERM のタイプである可能性があります。 MSMTC ジョブのログで以下のエラー メッセージが表示されます。

```
Errno2: -1070137335, ErrorCode: 0, FeedbackFdbk: 0, FeedbackFtncd: 0,
FeedbackRc: 0, LastOp: 3, ErrnoMsg: EDC5066I A read system error was detected.
```

原因:

CA CSM は、作成したタスク出力の一時データ セットの 1 つの読み込みに失敗すると、それ以上の読み込みができません。

解決方法:

以下の手順に従います。

1. SAMPLIB (MSMLIB) データ セット メンバに以下のパラメータを含めます。

   ```
   IJO="$IJO -DWriteEmptyRecordMVS=true"
   ```

2. CA CSM アプリケーション サーバを再起動します。

Microsoft Internet Explorer 8 の実行速度の低下

症状:

一度に多数のメンテナンス パッケージを適用するなど、リソースを消費するタスクを実行すると、以下のエラー メッセージが表示されます。

```
Stop running this script?
A script on this page is causing Internet Explorer to run slowly. If it continues to run, your computer may become unresponsive.
Do you want to abort the script?
```

この問題は、Microsoft Internet Explorer 8 で CA CSM の作業を行っているときにのみ発生します。

原因:

スクリプトは、大量のデータを転送および処理しようとしています。

解決方法:

Mozilla Firefox の使用をお勧めします。

Mozilla Firefox を使用しない場合は、以下のいずれかのアクションを実行します。

- メッセージが表示されなくなるまで、［No］をクリックします。 処理中のデータ量に応じて、このメッセージは複数回表示される可能性があります。
- Microsoft のナレッジ ベース記事 175500 の手順に従います。
- Microsoft Internet Explorer をアップグレードします。

  注: サポートされている Microsoft Internet Explorer のバージョンの詳細については、「*サイト準備ガイド*」を参照してください。

MSMTC が RC=100 で失敗する

問題の状況:

ジョブが開始された後、MSMTC ジョブが RC=100（MAXCC=100）で失敗します。

以下に例を示します。

```
04.30.18 JOB00480 $HASP165 MSMTC    ENDED AT SYSSERV1  MAXCC=100 CN(INTERNAL)
```

STDMSG 出力には以下のメッセージが表示されます。

```
JVMJZBL2007E Stack trace follows:
java.lang.NoClassDefFoundError: org.apache.catalina.startup.Bootstrap
Caused by: java.lang.ClassNotFoundException: org.apache.catalina.startup.Bootstrap
```

注: STDMSG 出力は、MSMTC のジョブ ログの一部ではない場合があります。これは、RunTimeMVSHLQPrefix.JCL （MSMTCSRV）の以下のステートメントによって管理されます。

```
//   ARGS='start 1>stdout 2>stdERR',   <-- Args to Java class
```

ARGS が ''（空）の場合、STDMSG は作成されています。

理由:

MSMTC ジョブの最初の手順は、RunTimeUSSPath/tomcat にある CA CSM アプリケーション サーバ (P. 203)を開始することです。

RunTimeUSSPath が空のとき、この手順は RC=100 で失敗します。
RunTimeUSSPath が空になる理由の 1 つに、このフォルダに属するファイル システムがマウントされていないことが考えられます。

解決方法:

- RunTimeUSSPath にファイル システムをマウントし、他のファイル システムも正しくマウントされていることを確認します。
- CA サポートにお問い合わせください。

CA CSM にアクセスするとき、No Ticket エラー メッセージが表示される

症状:

Web ブラウザを使用して CA CSM にアクセスしようとすると、No Ticket エラー メッセージをはじめとする複数のエラー メッセージが表示されます。そしてアクセスは失敗します。

原因:

Cookie がお使いの Web ブラウザで許可されていません。

解決方法:

お使いの Web ブラウザで Cookie を許可します。

サイトの標準が Cookie の使用を制限している場合、CA CSM アクセス URL を信頼済みサイトに追加します。

注: Cookie を許可する方法、および信頼済みサイトへの URL の追加方法の詳細については、お使いの Web ブラウザのユーザ ドキュメントを参照してください。

製品リストの更新が失敗する

症状:

製品リストを更新すると、以下のサンプルのようなメッセージが表示されます。

```
IO Error was detected during PAS processing.
Additional Diagnostic Data:
IO Exception Error.(UnknownHostException) Error encountered while
accessing the following URL:
https://supportservices.ca.com/support
supportservices.ca.com
Please review your http proxy settings and validate that your system has network
connectivity to the above URL.
```

解決方法:

CA CSM アプリケーション サーバが正しい TCP/IP スタックを使用していることを確認します。 必要に応じ、CA CSM アプリケーション サーバのスタートアップ ジョブ（MSMTCSRV）、またはアプリケーション サーバのスターティッド タスクの SYSTCPD DD カードのコメントを解除します。

```
//SYSTCPD DD DSN=VTAM.TCPIP.TCPIP.DATA,
//           DISP=SHR
```

SMP/E の APPLY または ACCEPT 処理が失敗する

問題の状況:

SMP/E の APPLY または ACCEPT 処理が、ターゲットまたは配布ライブラリの空きディレクトリ ブロックの不足により、失敗します。

理由:

PDSMAN のような製品がインストールされ、PDS ディレクトリ ブロックがデフォルトよりも多くのスペースを占有する方法で設定されています。この特定の PDS データ セットが、空きのディレクトリ ブロックを使い果たしています。

解決方法:

PDS ディレクトリ ブロックの増加パーセンテージを変更します。

以下の手順に従います。

1. 以下のコマンドを使用して、MSMTC アドレス空間をシャットダウンします。

   ```
   P MSMTC
   ```

2. STDENV スタートアップ スクリプトで、MSMTC STC プロシージャの STDENV DDNAME が指しているデータ セットの、msm.pds.dirblk.percentage の変数を指定します。または、変数の値を増やすことができます。

   ```
   IJO="$IJO –Dmsm.pds.dirblk.percentage=25”
   ```

3. 以下のコマンドを使用して、MSMTC アドレス空間を開始します。

   ```
   S MSMTC
   ```

4. 失敗したタスクを再試行します。

SMP/E 環境がツリーに表示されない

症状:

［SMP/E Environments］タブで、SMP/E 環境の左側のツリーに SMP/E 環境が表示されません。 他のユーザは、ツリーにこの SMP/E 環境を表示できます。

原因:

お使いのユーザ ID は、SMP/E 環境にアクセスする権限がありません。

解決方法:

- SMP/E 環境 CSI データ セットの HLQ へのアクセス権があるかどうか確認してください。
- CA CSM の外部で SMP/E 環境にアクセスします。 サイトが使用するセキュリティ システムから受信するメッセージを分析します。

  たとえば、CA Top Secret for z/OS を使用している場合、以下のメッセージが表示されます。

  ```
  TSS7221E Dataset Not Accessible
  ```

  セキュリティ管理者に連絡し、SMP/E 環境へのアクセス権を取得してください。

SMP/E 環境の移行が、SMP/E Environment Migration ウィザードの［SMP/E Environment Functions］手順で失敗する

症状:

SMP/E 環境の移行が、ウィザードの［SMP/E Environment Functions］手順で失敗します。または以下のいずれかのメッセージが表示されます。

- SMP/E Environment Migration ウィザードで、以下のメッセージが表示されます。

  ```
  MMR0005S - An error occurred during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so was not found. MMI0084S - Initialization of CAGIMAPI address space failed.
  ```

- MSMTC ジョブのログで、以下のいずれかのメッセージが表示されます。

  ```
  .1299171650. CGIMAPIExtractor_ForkStub: Exception occurred during Initialize() processing: mcCagimapiHandshake

  .1299171650. CGIMAPIExtractor_ForkStub: Exception text: Initialization of CAGIMAPI address space failed.

  An exception has occurred during native_initialize(): MMI0101S - A serious error has occurred while initializing GIMAPI Extractor.

  ERROR (http-17310-5) 2011-03-03 14:49:43,895 (DataExtractionDriver_Jni.java:305): Initialization of DataExtractionDriver_Jni has failed.

  INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206): A new message was read and enqueued in the message log: MMR0005S - An error occurred during dlopen(libGIMAPI03040026.so): CEE3501S The module libGIMAPI03040026.so was not found.  at ./CGIMAPIExtractionLibrary.C:51
  ```

```
INFO  (http-17310-5) 2011-03-03 14:49:43,896 (BufferedMessageReader.java:206):
A new message was read and enqueued in the message log: MMI0084S - Initialization
of CAGIMAPI address space failed. At ./CGIMAPIExtractor_ForkStub.C:430
```

原因:

CA CSM は共有オブジェクト ファイル（DLL）をロードできません。ファイルに必要な属性がないのが理由です。 すべてのファイルには、以下の属性が必要です。

+p、+s、+r、+x

libcci.so ファイルには、以下の属性も必要です。

+a

解決方法:

SO ファイルおよび DLL ファイルの属性および権限が正しいことを確認します。 必要な属性および権限を、それらが不足しているファイルに追加します。

1. 以下のコマンドを使用して、.../tomcat/lib ディレクトリ内のすべての SO ファイルおよび DLL ファイルの属性および権限を確認します。

   ```
   ls –E  *.so *.dll
   ```

   以下の例のような結果が表示されます。

   ```
   -rwxr-xr-x  aps-  1 USERID  GROUPID   233472 Aug 17  2010 libcci.so
   ```

2. 以下のコマンドを使用し、共有オブジェクト ファイルの属性を修正します。

   ```
   extattr attribute filename
   ```

   たとえば、+a 属性を libcci.so ファイルに追加するには、以下のように入力します。

   ```
   extattr +a libcci.so
   ```

3. 以下のコマンドを使用し、アクセス権限を修正します。

   ```
   chmod attribute filename
   ```

   たとえば、+r 属性を libcci.so ファイルに追加するには、以下のように入力します。

   ```
   chmod +r libcci.so
   ```

用語集

CA CSM Common Services

CA CSM Common Services（CETN600）は、Software Deployment Service（SDS）および Software Configuration Service （SCS）で構成される、CA Common Services for z/OS の有用なコンポーネントです。

CA CSM アプリケーション サーバ

*CA CSM アプリケーション サーバ*は、CA CSM アプリケーション コードをサポートする CA CSM Tomcat のリージョンです。

CA Datacom/MSM サーバ

*CA Datacom/MSM サーバ*は、ワークステーション ベースのアプリケーションが CA Datacom/MSM データベースを使用できるようにするサーバです。

CA Recommended Service（CA RS）

*CA Recommended Service（CA RS）*は、メインフレーム統合システム テスト環境でテスト済みのメンテナンス パッケージ セットです。 CA RS メンテナンスをインストールして、ご使用の製品を常に最新の状態に保持しておくことをお勧めします。新しい CA RS メンテナンスが利用可能であるかどうかを知るには、その CA RS レベル用に公開されたメンテナンスの一覧を示す CA RS ファイルをすべて自動または手動でダウンロードします。

FTP ポート

*FTP ポート*は、ファイルが転送される接続のポイントです。 デフォルトは 21 です。

GIMZIP

GIMZIP は IBM のユーティリティで、*z* のサフィックスを持つソフトウェアのポータブル パッケージを作成します。

MSMCAUX

MSMCAUX は JCL プロシージャで、補助アドレス空間を開始するために使用されます。 CA CSM が使用する CA Common Services for z/OS には、CA Common Services for z/OS CAW0PROC （CCS*hlq*.CAW0PROC）ライブラリのメンバ MSMCAUX にサンプル プロシージャが用意されています。 このプロシージャを、z/OS START コマンドが使用するシステム PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。 MSMCAUX サンプル メンバは、必要な変更を説明します。 MSMCAUX プロシージャを手動で開始しないでください。 MSMCAUX プロシージャは SCS アドレス空間（MSMCPROC）によって開始されます。

MSMCPROC

MSMCPROC は JCL プロシージャで、SCS アドレス空間を開始するために使用されます。 CA CSM が使用する CA Common Services for z/OS には、CA Common Services for z/OS CAW0PROC （CCS*hlq*.CAW0PROC）ライブラリのメンバ MSMCPROC にサンプル プロシージャが用意されています。 このプロシージャを z/OS START コマンドが使用するシステムの PROCLIB にコピーし、ユーザのインストール環境に合うように修正する必要があります。 MSMCPROC サンプル メンバは、必要な変更を説明します。

MSMTC/MSMTCSRV

MSMTC/MSMTCSRV は、CA CSM アプリケーション サーバ (P. 203)に関連付けられたジョブ ストリームまたはスターティッド タスクです。

MUF

MUF は CA Datacom/MSM Multi-User-Facility です。

SCS アドレス空間

*SCS アドレス空間*は、特別に定義された場所で、出力およびコンソールのトラフィックを照会するためのシステム レジストリやコマンドが存在する、オペレーティングシステム内の場所です。 SCS アドレス空間は、ターゲットの z/OS システム間で設定を実装するのに必要なサービスおよび処理を提供します。SCS の処理をサポートするための各ターゲット システムは、SCS アドレス空間を実行する必要があります。

Software Configuration Service （SCS）

Software Configuration Service（SCS）によって、製品の設定が容易になります。設定は、ターゲット ライブラリをランタイム ライブラリにコピーし、製品をユーザのサイトに合わせてカスタマイズして実行可能な状態にするプロセスです。

Software Deployment Service （SDS）

Software Deployment Service （SDS）によって、製品の展開が容易になります。 展開は、ドライビング システム（CA CSM アプリケーション サーバが実行されているシステム）からターゲット（リモートの配布先）システムに SMP/E ターゲット ライブラリをコピーするプロセスです。 ターゲット システムは、ローカルの z/OS システム、リモート z/OS システム、ステージング システムまたはシスプレックスのいずれかです。

UNIX System Services（USS）ファイル

z/OS システム用の *UNIX System Services*（*USS*） *ファイル*については、3 つのタイプのファイル システム、すなわち HFS（階層型ファイル システム）、zFS（zSeries ファイル システム）、および NFS（ネットワーク ファイル システム）があります。 USS ファイルは、これらのファイル システムの任意の 1 つ、または組み合わせであり、単一のスラッシュ（/）によって表されるルート ディレクトリから始まります。

VOLSER

VOLSER はボリューム シリアル番号で、明示的なボリュームにデータを配置します。

確認

展開が完了したことを*確認します*。 これはユーザの最終アクションです。 確認されるまで、展開は完了しません。 確認した後、展開は確認済み展開リストに移動します。

カスタム データ セット

*カスタム データ セット*は、z/OS データ セットまたは USS パスのいずれかを含むデータ セットです。

共有 DASD クラスタ

*共有 DASD クラスタ*システムは、DASD を共有するシステムのセットで、シスプレックスおよび非シスプレックス システムから構成することができます。ステージング システムを共有 DASD クラスタの一部にすることはできません。

検証

ユーザがシステムの［System Registry Page］上のシスプレックス システム、非シスプレックス システム、共有 DASD クラスタに対する［Actions］ドロップ ダウンで［Validate］ボタンを選択すると、*検証*プロセスが開始されます。 これによって、CAICCI 検証サービスを使用したバックグラウンド セキュリティ手順が開始され、このシステムが検証されます。

システム レジストリ

*システム レジストリ*は、すべての CA CSM 管理製品が共有する変数データのリポジトリです。システム レジストリ リポジトリには、CA CSM に定義され、展開と設定のターゲットとして選択されるシステムに関する情報が格納されます。非シスプレックス、シスプレックス、共有 DASD クラスタおよびステージング システムを作成できます。登録したシステムを保持、検証、表示、削除することができ、また失敗した検証を調査できます。

シスプレックス

シスプレックス（SYStem comPLEX）は IBM のメインフレーム システム複合体で、1 つ以上の物理システム上で動作する単一の論理システムです。シスプレックスを構成する各物理システムは、しばしば「メンバ」システムと呼ばれます。

ステージング システム

*ステージング システム*は、ターゲット システムで製品をアクティブ化する前に展開および設定に使用できる仮想システムです。 ターゲット システムが CA CSM ドライビング システムと同一である場合、ソフトウェアはローカルでアクティブ化されます。 ステージング システムを使用するには、CA CSM ドライビング システムが CA CSM システム レジストリに登録されている必要があります。

ストレージ クラス

*ストレージ クラス*は SMS 管理のデータ セットおよびオブジェクトにのみ適用されます。 ストレージ クラスにより、異なるレベルのパフォーマンスと可用性サービスを、データ セットに定義できるようになります。 ストレージ クラスを使用し、データ セットやオブジェクトに必要なサービス レベルと、その物理的特性を分離できます。ストレージ クラスにより、動的キャッシュ管理、順次データ セット ストライピング、および同時コピーの属性のような情報が提供されます。

ストレージ クラスは、SMS 管理のデータ セットまたはオブジェクトにする、データ セットまたはオブジェクトを持つストレージ クラスの集合です。 このため、動的キャッシュ管理や順次データ セット ストライピングのような機能は、SMS 管理のデータ セットのみに適用されます。 SMS 管理または非 SMS 管理のデータ セットがある可能性があります。 オブジェクトは SMS 管理される必要があります。

スナップショット

*スナップショット*は、CA CSM が IBM のユーティリティ GIMZIP を使用して作成する、ターゲット ライブラリのセットのコピーです。 CA CSM は GIMZIP を使用して、APPLY されたメンテナンスのリストをはじめとする、これらのライブラリの圧縮アーカイブを作成します。 このアーカイブ作成処理中、アーカイブ済みデータの整合性を保証するために、SMP/E 環境はロックされます。

製品取得サービス（PAS）

*製品取得サービス（PAS）*を使用すると、メインフレーム製品とそのサービス（プログラム一時修正（PTF）など）を簡単に取得できます。 PAS は、ユーザのサイトにライセンスされている製品に関する情報を取得します。 次に、PAS はそれらのライセンス情報を、ユーザのドライビング システムでメンテナンスされているソフトウェア インベントリに記録します。

接続システム

*接続システム*は、展開をどのシステム上で解凍するかを定義します。 つまり、解凍処理を実行するために、どのシステム CAICCI を生成するかが定義されます。

設定

*設定*は、インストール済みソフトウェアまたは CA CSM の展開済みソフトウェアをカスタマイズするために作成する CA CSM オブジェクトです。 設定によって、ソフトウェアがユーザの環境で使用できるようになります。 設定にはユーザの環境に固有のプロファイル、変数およびリソースが含まれます。

ソフトウェア インストール サービス（SIS）

*ソフトウェア インストール サービス（SIS）*によって、実行システムのソフトウェア インベントリでのメインフレーム製品のインストールおよびメンテナンスが容易になります。 簡略化される操作には、ダウンロード済みソフトウェア パッケージの参照、実行システムでの SMP/E 統合ソフトウェア インベントリの管理、およびインストール タスクの自動化などがあります。

ディレクトリ パス

*ルートのディレクトリ パス*は、FTP サーバがアクセスを許可された基本のディレクトリです。 FTP サーバはこのディレクトリ、およびそのサブディレクトリにファイルを作成し、そこからのファイルの読み取りを許可されます。 ディレクトリ パスは USS パス名です。これは、スラッシュ（/）で区切られた 1 つ以上のディレクトリ リーフで構成されます。また、最大入力長は、スラッシュを含めて 255 文字です。 ディレクトリ パスが変換されるとき、最大長は 255 文字になります。

データ宛先

システムごとに*データ宛先*を定義する必要があります。 データ宛先は、転送データをリモート システムに転送するためにどのテクニックを使用するかを CA CSM に指示する方法です。 データ宛先は、非シスプレックス システム、シスプレックス システム、および共有 DASD クラスタに割り当てられます。 データ宛先は名前付きオブジェクトで、システム レジストリ内の複数のエンティティに割り当てられる場合があります。また、データ宛先自身の独立したメンテナンス ダイアログ ボックスがあります。

データ セット名マスク

*データ セット名マスク*は、各データ セットを識別する一意の名前です。これは、ピリオドで区切られた 1 つ以上の修飾子で構成され、ピリオドを含めた最大入力長は 64 文字です。 データ セット名マスクを変換するとき、ピリオドを含めた最大長は 44 文字です。

展開

*展開*機能により、スナップショット、転送、展開のアクションが 1 つのアクションに集約され、社内中のシステムに CA CSM 製品をコピーすることが可能になります。 たとえば、共有 DASD にコピーし、または FTP を経由して、1 つまたは多数の製品を 1 つまたは多数のシステムに送信できます。

展開

*展開*では、ライブラリおよびデータ セットを展開できます。 このプロセスでは、SMP/E に定義されたターゲット ライブラリおよびユーザ データ セットを、共有 DASD およびネットワーク環境の両方にコピーします。

転送

*転送*機能により、FTP 経由で組織全体のシステムに製品をコピーすることができ、今後の展開に備えることができます。

統一資源識別子（URI）

*統一資源識別子（URI）*は、インターネット上の名前またはリソースを識別するために使用される文字列です。 この識別子により、特定のプロトコルを使用したリソースの表現との対話が、ネットワーク間で（通常は、World Wide Web）可能になります。 具体的な構文法および関連するプロトコルを指定するスキームにより、各 URI が定義されます。
共有 DASD クラスタまたはシスプレックスについては、URI は接続システムの URI である必要があります。

トポロジ

企業システム *トポロジ*には、共有 DASD 環境、ネットワーク環境、および z/OS システムを含めることができます。

ドライビング システム

*ドライビング システム*は CA CSM アプリケーション サーバが実行されているシステムです。

非シスプレックス

*非シスプレックス*は、シスプレックスまたはモノプレックス システムの一部ではない、スタンドアロンの z/OS システムです。

プレビュー

*プレビュー*では、展開は名前で識別され、製品、システム、転送方法、ターゲット ライブラリ（ソース、ターゲット、解決を含む）、および SMP/E の環境とスナップショットが簡潔に表示されます。

モノプレックス

*モノプレックス*は、ただ 1 つのメンバ システムと、最小の単一のカップリング ファシリティを持つシスプレックスです。 現在、モノプレックスはシスプレックスと同じ方法でトラックされます。違いは、Web ベース インターフェースで表示されるシスプレックス名が、実際のモノプレックスのシステム名であることです。