

CA-OPS/MVS® Event Management and Automation

インストール ガイド

リリース 12.0



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。

CA の事前の書面による承諾を受けずに本ドキュメントの全部または一部を複製、譲渡、開示、変更、複本することはできません。本ドキュメントは、CA が知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、(i) 本ドキュメントが関係する CA ソフトウェアの使用について CA とユーザとの間で別途締結される契約または (ii) CA とユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、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、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。

本ドキュメントの制作者は CA 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 Section 252.227-7014(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 © 2012 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このマニュアルでは、以下の CA 製品を参照します。

- CA 1[®] Tape Management (CA 1)
- CA 7[™] Workload Automation (CA 7 WA)
- CA ACF2[™] for z/OS (CA ACF2)
- CA Automation Point
- CA Common Services for z/OS (CCS for z/OS)
- CA Dynam[®]/TLMS Tape Management (CA Dynam/TLMS)
- CA Examine[®] Auditing (CA Examine)
- CA Hyper-Buf[®]VSAM Buffer Optimizer (CA Hyper-Buf)
- CA Jobtrac[®] Job Management (CA Jobtrac)
- CA MIC Message Sharing (CA MIC)
- CA NSM
- CA NSM System Status Manager CA OPS/MVS[®] Option (CA NSM SSM CA OPS/MVS Option)
- CA OPS/MVS[®] Event Management and Automation (CA OPS/MVS)
- CA Scheduler[®] Job Management (CA Scheduler)
- CA SYSVIEW[®] Performance Management (CA SYSVIEW)
- CA Top Secret[®] for z/OS (CA Top Secret)

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

マニュアルの変更点

以下のマニュアルの更新は、本書の前回のリリース以降に行われたものです。

注: PDF 形式の場合、参照ページ番号は変更されたトピックの先頭ページを指しています。実際にはそれより後ろのページが変更されている可能性があります。

- データセットライブラリ名を更新しました。詳細については、「[CA OPS/MVS リリース ノート](#)」を参照してください。
- 「[ユーザの環境に応じた CA OPS/MVS インストールのカスタマイズ \(P. 31\)](#)」セクションを追加しました。
- 「[ユーザの環境に応じた外部ライブラリ名のカスタマイズ \(P. 32\)](#)」セクションを追加しました。
- 「[Pax-Enhanced ESD からの製品のインストール \(P. 43\)](#)」の章を更新しました。
- 「[テープからの製品のインストール \(P. 73\)](#)」の章を更新しました。
- 「[SMP/E でインストールされたターゲット データセットの識別 \(P. 89\)](#)」セクションを追加しました。
- 「[CA MSM を使用しない展開方法 \(P. 91\)](#)」セクションを更新しました。
- 「[起動 JCL のカスタマイズ \(P. 98\)](#)」セクションを更新しました。
- 「[起動プロシージャのカスタマイズ \(P. 100\)](#)」セクションを更新しました。
- 「[OPSLOG およびチェックポイント VSAM 線形データセットの定義 \(P. 106\)](#)」セクションを更新しました。
- 「[INSTUSEX のカスタマイズおよび実行 \(P. 136\)](#)」セクションを更新しました。
- 「[別途ライセンスされている CA-OPS/MVS のコンポーネントのインストール方法 \(P. 147\)](#)」セクションを更新しました。
- 「[オプション バース コンポーネントのインストール方法 \(P. 148\)](#)」セクションを更新しました。
- 「[Linux Connector インタフェース\(LXC\) の設定 \(P. 224\)](#)」セクションを追加しました。
- 「[Linux Connector コンポーネントのセットアップ \(P. 224\)](#)」セクションを追加しました。
- 「[LXC パラメータ \(P. 225\)](#)」セクションを追加しました。

- 「[キーメンバシップ pp 値 \(P. 115\)](#)」セクションを更新しました。
- 「[CA Service Desk \(FMID\) へのインターフェース \(P. 245\)](#)」セクションを更新しました。
- 「[CAICCI を使用した CA OPS/MVS マルチシステム機能 \(P. 246\)](#)」セクションを更新しました。
- 「[OPSCAWTO OPS/REXX 関数 \(P. 246\)](#)」セクションを更新しました。
- 「[CA LMP \(P. 242\)](#)」セクションを更新しました。
- 「[IBM Health Checker へのインターフェース \(P. 242\)](#)」セクションを更新しました。
- 「[ADDRESS CA7 \(P. 242\)](#)」セクションを更新しました。
- 「[ADDRESS CASCHD \(P. 243\)](#)」セクションを更新しました。
- 「[ADDRESS JOBTRAC \(P. 243\)](#)」セクションを更新しました。
- 「[Automation Measurement Environment \(P. 243\)](#)」セクションを更新しました。
- 「[CA Automation Point とのインターフェース \(P. 244\)](#)」セクションを更新しました。
- 「[CA 7 Browse Log インターフェース \(P. 244\)](#)」セクションを更新しました。
- 「[CA Network および Systems Management System Status Manager CA-OPS/MVS オプションとのインターフェース \(P. 245\)](#)」セクションを更新しました。
- 「[CA Event Manager コンポーネントとのインターフェース \(P. 247\)](#)」セクションを更新しました。
- 「[CA OPS/MVS Switch Operations Facility \(SOF\) \(P. 248\)](#)」セクションを更新しました。

目次

第 1 章: 概要	13
CA OPS/MVS の概要	13
ベース製品のコンポーネント	14
オプション機能	17
CA OPS/MVS の概要	19
対象読者	20
インストール処理の実行	20
第 2 章: インストールの準備	23
ハードウェア要件	23
ソフトウェア要件	23
CA Common Services の要件	25
セキュリティの要件	26
TSO OPER 権限	28
輸出申告	28
ストレージ要件	28
ECSA の使用およびストレージの要件	29
配布ライブラリ、ターゲットライブラリ、およびデータ エリアの DASD スペース	29
同時リリース	30
ユーザの環境に応じた CA OPS/MVS のインストールのカスタマイズ	31
ユーザの環境に応じた外部ライブラリ名のカスタマイズ	32
ユーザの環境に応じた CA OPS/MVS OPSLOG WebView zFS Mount のカスタマイズ	34
第 3 章: CA MSM を使用した製品のインストール	35
CA MSM を使用する方法: シナリオ	35
製品の取得方法	36
製品のインストール方法	37
既存製品の保守方法	38
製品の展開方法	39
製品の構成方法	40
Web ベース インターフェースを使用した CA MSM へのアクセス	41

第 4 章: Pax-Enhanced ESD からの製品のインストール 43

Pax-Enhanced ESD を使用して製品をインストールする方法.....	43
Pax-Enhanced ESD ダウンロードの仕組み.....	45
ESD 製品のダウンロード ウィンドウ.....	45
USS 環境のセットアップ.....	48
ファイル システムの割り当ておよびマウント.....	49
製品 pax ファイルの USS ディレクトリへのコピー.....	51
バッチ JCL を使用したダウンロード.....	52
PC を経由したファイルのメインフレームへのダウンロード.....	55
pax ファイルからの製品ディレクトリの作成.....	57
Pax コマンド (Unpackage.txt) を実行するジョブの例.....	58
z/OS データ セットへのインストール ファイルのコピー.....	58
ネイティブ SMP/E JCL を使用したインストール方法.....	60
Pax インストールのための SMP/E 環境の準備.....	61
Pax インストール用のインストール ジョブの実行.....	63
USS ディレクトリのクリーンアップ.....	64
メンテナンスの適用.....	65
HOLDDATA.....	67
システム HOLDDATA.....	68
外部 HOLDDATA.....	70

第 5 章: テープからの製品のインストール 73

テープからのサンプル JCL のアンロード.....	74
ネイティブ SMP/E JCL を使用したインストール方法.....	75
テープ インストール用の SMP/E 環境の準備.....	76
テープ インストール用のインストール ジョブの実行.....	78
メンテナンスの適用.....	79
HOLDDATA.....	81
システム HOLDDATA.....	82
外部 HOLDDATA.....	84

第 6 章: 製品の開始準備 87

概要.....	88
展開を準備する方法.....	88
IBM APAR の適用 (オプション).....	88

SMP/E でインストールされたターゲット データ セットの識別.....	89
製品の展開.....	90
CA MSM による展開の完了方法.....	90
CA MSM を使用せずに展開する方法.....	90
製品の設定.....	91
CA MSM を使用して設定を完了する方法.....	91
CA MSM を使用して設定を開始する方法.....	91
CA MSM を使用した設定.....	92
CA OPS/MVS の単純な設定の例.....	92
CA MSM を使用する CA OPS/MVS 設定オプション.....	93
CA MSM によりカスタマイズされる起動 JCL プロシージャ.....	94
インストールの確認.....	96
設定の完了.....	97
CA MSM なしで設定する方法.....	97
起動 JCL PROC のカスタマイズ.....	97
起動 JCL のカスタマイズ.....	98
起動プロシージャのカスタマイズ.....	100
OPSLOG およびチェックポイント VSAM 線形データセットの定義.....	106
既存のお客様でのインストール.....	107
DIV データセットの配置方法.....	108
インストールの確認.....	109
必要な手動設定.....	110
ロードライブラリへの APF 権限の付与.....	111
ライセンスキーの CA Common Services PPOPTION データセットへの配置.....	112
製品ライセンスの設定.....	112
CA LMP キー証明書.....	112
CA LMP ステートメントの記述方法.....	114
KEYS メンバ - 実行キーの追加.....	114
データセットへのアクセスの付与.....	116
ベースコンポーネントの設定タスク.....	117
z/OS コンソールの定義.....	117
システムリンケージ インデックスの可用性の保証.....	118
ASVT エントリの置換.....	118
ISPF を使用して LPA にコマンド プロセッサを追加する.....	119
ISPF インターフェイス モジュールへのアクセスの提供.....	121
データセットの命名基準の確立.....	121

セキュリティ製品のログオン ID の作成.....	125
サブシステム ID の論理 Parmlib 連結への追加	132
ベースコンポーネント用のオプション インストール タスク	132
ロード モジュールのリンク パック領域への配置	133
TSO コマンド権限の付与.....	133
ロード モジュールへのアクセスの提供	134
OPSMODE コマンド プロセッサのインストール.....	135
CCS for z/OS のイベント管理コンポーネントとの UNIX System Services インターフェースのインストール.....	135
システム準備タスクの概要	137
インストール後の考慮事項.....	139
パラメータ ライブラリ メンバのカスタマイズ	140
OPSVIEW 機能を TSO で使用できるようにする	141
OPSVIEW データ セットの使用上の注意	143
製品の起動.....	143
製品の開始後の確認項目	143
サンプル ルール セットのルールの無効化.....	145
サンプル OPSAOF コマンド ルールの有効化(オプション)	145
第 7 章: オプション コンポーネントの設定およびインストール	147
別途ライセンスされている CA-OPS/MVS のコンポーネントのインストール方法.....	147
オプション ベース コンポーネントのインストール方法	148
別途ライセンスされたコンポーネントのタスク	148
Multi-System Facility (MSF) の設定	149
IMS Operations Facility のインストール.....	157
CICS/TS に対する XTDOU COF インターフェースのインストール	166
CA NSM SSM CA-OPS/MVS オプションのカスタマイズ.....	167
Expert Systems Interface (ESI) の設定	176
OPSLOG WebView の環境設定	176
オプションのベースコンポーネントのタスク.....	197
JES2 環境関数の設定 (JES2 で必要)	197
JES2OFFSETSUFFIX を使用して CPU 間でライブラリの共有を可能にする (JES2 のみ)	198
JES3 インターフェースの設定.....	199
共有ファイル VSAM KSDS の定義.....	200
UNIX System Services のインストール	201
EPI コンポーネント用の VTAM 端末の作成.....	207

NetView インターフェースのインストール.....	208
NetView Operator Facility のインストール.....	211
Tivoli OMEGAMON XE のインターフェースの設定.....	214
MVS/QuickRef インターフェースのインストール.....	220
CA 7 WA インターフェースの設定.....	221
ハードウェア サービス (HWS) の設定.....	222
Linux Connector インターフェース (LXC) の設定.....	224
ジェネリック データセットの直接出力.....	226
CA MIC とのインターフェースの設定.....	229
CA 7 Browse Log のオプションのメッセージ機能のインストール.....	233
z/OS Automatic Restart Management Facility の設定.....	234
付録 A: システム準備チェックリスト	237
タスクの記録.....	238
付録 B: CCS for z/OS コンポーネントの要件	241
CA LMP (ライセンス管理プログラム).....	242
IBM Health Checker へのインターフェース.....	242
ADDRESS CA7.....	242
ADDRESS CASCHD.....	243
プログラムライブラリの DASD 要件.....	243
ADDRESS JOBTRAC.....	243
Automation Measurement Environment.....	243
CA Automation Point とのインターフェース.....	244
CA 7 Browse Log インターフェース.....	244
CA Service Desk インターフェース.....	245
CA Network および Systems Management System Status Manager CA-OPS/MVS オプションとの インターフェース.....	245
CAICCI を使用する CA OPS/MVS Multi-System Facility の設定.....	246
OPSCAWTO OPS/REXX 関数.....	246
CA Event Manager コンポーネントとのインターフェース.....	247
Switch Operations Facility (SOF).....	248
付録 C: DASD 計算チャート	249
OPSLOG メッセージの DASD 要件.....	249

グローバル変数チェックポイント DIV データセットの DASD 要件	250
共有 VSAM データベースの DASD 要件 (オプション)	253
RDF および System State Manager の DASD 要件	253
グローバル変数データベースコントロールの提供 (オプション)	254
使用状況警告メッセージ	255
付録 D: CA MSM によって作成されるデータセット	257
ポスト SMP/E、展開、および設定データセット	257
索引	261

第 1 章：概要

このガイドでは、CA OPS/MVS をインストールおよび実装する方法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 OPS/MVS の概要 \(P. 13\)](#)

[対象読者 \(P. 20\)](#)

[インストール処理の実行 \(P. 20\)](#)

CA OPS/MVS の概要

CA OPS/MVS は、複数のシステムのクリティカルなリソースをステータスで管理します。また、環境を管理するための強力で複雑な自動化の展開を簡素化する自動アプリケーションを備えています。CA OPS/MVS は、災害時回復プロセスの自動化およびエンドツーエンド自動化に不可欠なコンポーネントです。

CA OPS/MVS は効率的な同期自動化を実現し、複雑なシステムおよびプロセスの自動化を効率的に作成および展開するためのツールを提供します。CA OPS/MVS は、CA の自動化、パフォーマンス管理、および作業負荷自動化製品と統合しています。

ベース製品のコンポーネント

CA OPS/MVS には、データセンターの運用を円滑化するためのツールが用意されています。これらのツールを使用すると、IT 環境の管理を統合および簡素化してより大きいビジネス成果を生み出すことができます。

CA OPS/MVS ベース製品 (正式の z/OS サブシステム) は、複数の z/OS アドレス空間で実行されます。以下に、ベース製品コンポーネントをアルファベット順に示します。

- Automated Operations Facility (AOF)
- Enhanced Console Facility (ECF)
- External Product Interface (EPI)
- Operator Server Facility (OSF)
- OPS/REXX Language
- OPSVIEW Interface
- Programmable Operations Interface (POI)
- Relational Data Framework (RDF)
- System State Manager (SSM)
- VM Guest Support (VMGS)

Automated Operations Facility

Automated Operations Facility (AOF) を使用すると、システム イベント (メッセージや時間の経過など) に対する応答をプログラミングできます。AOF ルールは、OPS/REXX 言語の拡張機能を使用することによって自動化操作をサポートする特殊な構造化 OPS/REXX プログラムです。

Enhanced Console Facility

Enhanced Console Facility (ECF) は、TSO (および OPSVIEW) のダウン時に使用します。ECF では、Z/OS または JES コンソールにログオンし、行モードの対話型 TSO セッションを実行できます。このセッションでは、TSO コマンドを発行するか、または TSO CLIST または OPS/REXX プログラム (追加入力のプロンプトを発行するものを含む) を呼び出すことができます。ECF にログオンすることによって、オペレータは TSO 操作に必要な SYS1.PROCLIB のメンバの修復などのタスクを実行できます。

External Product Interface

External Product Interface (EPI)を使用すると、VTAM で実行されている CA OPS/MVS は、IBM 3270 (SLU2)タイプの仮想端末をサポートする VTAM アプリケーションと通信できます。EPI は、任意の数の VTAM アプリケーションに接続されている任意の数の 3270 タイプ仮想端末をエミュレートできる真の 3270 端末として VTAM 側で認識されます。

EPIを使用すると、VTAM アプリケーションへのコマンドの発行および VATAM アプリケーションからのデータのフェッチを自動化し、OPS/REXX プログラム間で VTAM セッションを共有できます。

Operator Server Facility (OSF)

CA OPS/MVS のコンポーネントである Operator Server Facility (OSF)を使用すると、OPS/REXX プログラム、TSO コマンド、および TSO/E REXX プログラムまたは CLIST を CA OPS/MVS が実行できるようにスケジュールできます。さまざまな CA OPS/MVS コンポーネントが、AOF、ECF、IOF、MSF を含む OSF サービスを使用します。

OPS/REXX Language

REXX (*R*estructured *E*Xtended *e*Xecutor)は、IBM の Systems Application Architecture (SAA)に基づくすべての IBM 環境用の標準コマンド言語です。

CA OPS/MVS のような製品は何らかの言語でプログラム可能である必要があるため、CA OPS/MVS には OPS/REXX と呼ばれる独自の REXX 実装が用意されています。これにより、CA OPS/MVS への投資の長期的な安定性が実現されます。OPS/REXX は追加機能との SAA 互換性を提供するので、システム自動化タスク用のプログラムを記述できます。

OPSVIEW Interface

OPSVIEW は、データ処理専門家とエンド ユーザの両方が使用できるフル画面、メニュー駆動型の操作インターフェースです。OPSVIEW は、さまざまな z/OS システム機能を実行するためのパネルを備え、CA OPS/MVS 自体を制御する主要なコンポーネントです。

Programmable Operations Interface

Programmable Operations Interface (POI) は、TSO コマンド プロセッサおよび REXX 機能から構成されます。POI は、z/OS コンソールと CA OPS/MVS 機能の両方に対するプログラム可能なインターフェースです。コマンド プロセッサおよび機能を使用すると、カスタム操作自動化と生産性拡張アプリケーションを構築できます。POI を使用して構築されたアプリケーションの一例が CA OPS/MVS 操作インターフェースの OPSVIEW です。

Relational Data Framework

Relational Data Framework (RDF) 機能を使用すると、Structured Query Language (SQL) ステートメントによって、自動化ルールおよび OPS/REXX プログラムで必要な大量のシステム情報を管理できます。大量の変数セットを使用する代わりに、RDF を使用してシステム情報を収集し、関連するデータの行および列を含むリレーショナルテーブルとして編成し、関連するシステム情報を特定の行または列から選択することによって取得します。

自動化データの管理用として SQL を採用したのは、メインフレームおよび PC ユーザの間で広く普及しているためです。RDF は、リレーショナル SQL テーブル、および米国規格協会 (ANSI) 標準に準拠する SQL 言語のサブセットから構成されます。SQL の使用経験があれば、CA OPS/MVS サブセットをすぐに使用できます。

System State Manager

System State Manager (SSM) は、システム上のハードウェアおよびソフトウェア リソースのステータスを監視および制御します。

RDF リレーショナル テーブルの情報を使用して、SSM はシステムリソースの適切な状態のモデルを保持します。リソースの実際の状態がそのモデルから外れている場合 (オンラインであるはずのテープドライブがオフラインになっているなど)、SSM は OPS/REXX プログラムをディスパッチしてそのリソースを適切な状態にリストアします。

VM Guest Support

VM Guest Support (VMGS) を使用すると、z/OS コマンドを発行できる任意の環境で、CA OPS/MVS から CP コマンドを発行できます。このため、サイトが VM の下で z/OS を実行している場合、z/OS アクティビティと VM アクティビティを調整できます。

オプション機能

CA OPS/MVS には、すべての環境に必ずしも適用できない機能がいくつかあります。このため、これらの機能はオプション機能としてパッケージ化されています。以下に、これらのオプション機能のリストを示します。

- CICS Operations Facility (COF)
- Critical Path Monitoring (CPM)
- Expert Systems Interface (ESI)
- IMS Operations Facility (IOF)
- Multi-System Facility (MSF)
- Switch Operations Facility (SOF)

CICS Operations Facility

CICS Operations Facility (COF) は、CA OPS/MVS と CICS の間のインターフェースであり、AOF ルール処理の機能を CICS メッセージに適用します。CICS メッセージは、CICS 一時データキューにのみ書き込まれます。この追加のメッセージトラフィックは、CICS サブシステムを制御するために使用できる自動化可能なイベントの数を拡張します。COF を使用して AOF ルールで認識可能なイベントには、端末エラー、ユーザのログオンおよびログオフ アクティビティ、ジャーナルスイッチが含まれます。

COF インターフェースがインストールされている場合、CA OPS/MVS は無制限の CICS アドレス空間を処理できます。

Critical Path Monitoring

CA Critical Path Monitoring (CA CPM) バージョン 3 は、ユーザ定義のデッドラインと照らし合わせてバッチ ジョブ (フロー) のグループのパフォーマンスを監視できます。CA CPM バージョン 3 は、CA スケジューリング製品のいずれか (CA 7 WA、CA Scheduler、および CA Jobtrac) と連携してこの機能を提供します。CA CPM Version 3 と CA OPS/MVS を接続することによって、監視対象フローについての情報を CA NSM SSM CA OPS/MVS Option ワークステーション上で Web 対応または Windows ユーザ インターフェースを使用して表示できます。

Expert Systems Interface

Expert Systems Interface (ESI) アプリケーションプログラミング インターフェースの OPSLINK は、高級言語またはアセンブラ言語で記述されたアプリケーションから選択された CA OPS/MVS 機能にアクセスします。

ESI の用途には、オペレータ コマンドの実行、TSO コマンドの実行 (TSO TMP の下で対話的またはバッチ実行されている場合)、および CA OPS/MVS グローバル変数のアクセスおよび更新が含まれます。

IMS Operations Facility

IMS Operations Facility (IOF) は、CA OPS/MVS と IMS の間のインターフェースであり、CA OPS/MVS 機能を IMS に適用します。たとえば、IMS メッセージを処理する AOF ルールを記述したり、OPSVIEW を使用して IMS を操作したりできます。

1 コピーの CA OPS/MVS で、最大 32 コピーの IMS を処理できます。1 コピーの CA OPS/MVS の制御下で複数のコピーの IMS を実行する場合、IMS のコピーは、CA OPS/MVS がサポートする IMS レベルの組み合わせです。

Multi-System Facility

Multi-System Facility (MSF) は、CA OPS/MVS の機能を複数 CPU および複数サイト環境に適用します。MSF は、CA OPS/MVS のコピー間の VTAM、XCF、または TCP/IP セッションを確立し、任意のコピーが他のコピーにコマンドを発行し、その応答を受信できるようにします。

また、MSF は CCS for z/OS の CCI サービスを使用して TCP/IP 接続による CA Automation Point への接続を容易にします。

Switch Operations Facility

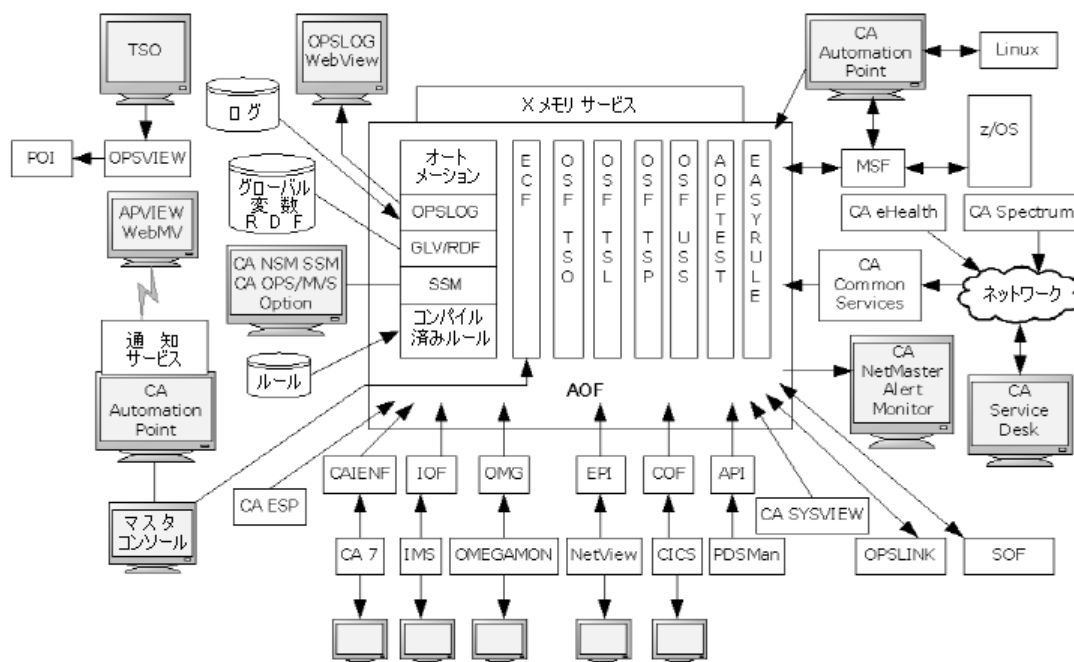
Switch Operations Facility (SOF) は、以下の機能によって I/O 設定管理を自動化します。

- 自動検出
- 自動連続監視
- 自動クロスシステム解決
- シングル ポイントの表示と制御
- ISPF インターフェース

- OPS/REXX ホスト環境
- 保存されたスイッチ設定

CA OPS/MVS の概要

以下の図に、CA OPS/MVS の概要と、z/OS オペレーティングシステムへの適合を示します。



CA OPS/MVS と統合される CA 製品の詳細については、「*Integration Guide*」を参照してください。

対象読者

本書の読者は、以下の領域に関する知識を持っている必要があります。

- JCL
- TSO/ISPF
- z/OS 環境、この環境へのソフトウェアのインストール
- 自社の IT 環境、エンタープライズ構造、領域構造

以下の担当者と仕事をする必要がある場合があります。

- システム プログラマ (z/OS および VTAM 定義のため)
- ストレージ管理者 (DASD 割り当てのため)

インストール処理の実行

インストール処理の手順は以下のとおりです。

1. インストールの準備を行い、お使いのサイトがインストール要件をすべて満たしていることを確認します。
2. 以下のいずれかの方法で製品を取得します。
 - CA MSM
注: CA MSM が存在しない場合、CA Support Online の Download Center からダウンロードできます。インストール手順については、「*CA Mainframe Software Manager Product Guide*」を参照してください。これは、<https://support.ca.com/> の Documentation ページで提供されています。
 - Pax-Enhanced ESD (Electronic Software Delivery)
 - テープ
3. 取得方法に基づいて製品をインストールします。
4. サイトで必要な CA Common Services が含まれている pax ファイルを使用して、CA Common Services をインストールします。すべてのサイトで、Required CA Common Service バンドル内に含まれている CA Common Services をすべてインストールする必要があります。

5. 該当する場合、保守を適用します。
6. 製品を設定します。

第 2 章: インストールの準備

このセクションでは、製品をインストールする前に必要な知識および作業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。

[ハードウェア要件](#) (P. 23)

[ソフトウェア要件](#) (P. 23)

[CA Common Services の要件](#) (P. 25)

[セキュリティの要件](#) (P. 26)

[ストレージ要件](#) (P. 28)

[同時リリース](#) (P. 30)

[ユーザ サイト用の CA OPS/MVS のインストールのカスタマイズ](#) (P. 31)

[ユーザ サイトの外部ライブラリ名のカスタマイズ](#) (P. 32)

[ユーザのサイトに合わせた CA OPS/MVS OPSLOG WebView zFS Mount のカスタマイズ](#) (P. 34)

ハードウェア要件

CA OPS/MVS r12 は、「ソフトウェア要件」で示すソフトウェアをサポートするハードウェアにインストールできます。

ソフトウェア要件

ご使用のソフトウェアやオペレーティング システムに応じて、CA OPS/MVS を実行するための要件を確認してください。サイトのソフトウェア レベルが正しくない場合、テクニカル サポート (<http://ca.com/support>) にお問い合わせください。

- オペレーティング システムのサポート:

z/OS

リリース 1.10 以降。

JES2

IBM がサポートするリリース。

JES3

IBM がサポートするリリース。形式が HJSnnnn の FMID は、CA OPS/MVS をインストールする予定のシステムの SMP/E ターゲットゾーン内にある必要があります。

TSO

TSO/E の IBM がサポートするリリース。

IMS

IMS Operations Facility (IOF) をインストールしている場合、バージョン 9.1 以降。

サポート対象の IMS リリースはどれでも混在させることができます。CA OPS/MVS は IMS バージョンとリリースレベルの差異を自動的に調整します。

CICS

CICS Transaction Server for z/OS バージョン 2.3 以降。

IBM がサポートする CICS のバージョンはどれでも組み合わせることができます。

- ソフトウェアレベル サポート:

z/OS Security Server (RACF)

IBM がサポートするリリース。

IBM Communications Server (VTAM)

IBM がサポートするリリース。

CA ACF2

CA がサポートするリリース。

CA Top Secret

CA がサポートするリリース。

CCS for z/OS

CA がサポートするリリース。

重要: これらのサポート対象ソフトウェアレベルは、CA OPS/MVS r12 の GA 日付けで有効です。サポート対象のレベルを確認するには、<http://ca.com/support> の URL の CA OPS/MVS Product Home ページで「Upgrade Information」リンクを参照してください。

CA Common Services の要件

CA OPS/MVS では、以下の CA Common Services が使用されています。

- CAICCI
- CAIRIM
- CAISSF
- CA LMP
- CA GSS
- CA Health Checker Common Service

注: 他の CA 製品がサイトにインストールされている場合は、これらのサービスの一部がすでにインストールされている可能性があります。

注: CA Common Services FMID の詳細については、付録「[CCS for z/OS コンポーネントの要件 \(P. 241\)](#)」を参照してください。

CAIRIM

オペレーティング システム環境ですべての CA アプリケーションのための準備が行われ、CA アプリケーションが起動されます。CAIRIM は、一連の動的初期化ルーチン用の共通ドライバです。ユーザ SVC、SMF EXIT、サブシステムなど、システム アプリケーションのインストール時に要求される一般的なインストール要件を不要にします。

CAIRIM の重要な 2 つの要素は、CAISSF と CA LMP です。

CAISSF

すべてのシステムリソースプロセスとアプリケーションリソースプロセスへの制御と監視アクセスのための外部セキュリティ機構が実現されます。CAISSF は、多くの CA エンタープライズ アプリケーションに組み込まれており、ほかの CCS for z/OS サービスによっても使用されます。CAISSF により、ユーザ ログオン用のセキュリティ サービス、リソース アクセス制御、プロセス使用制御、違反アクティビティの記録と監視が行われます。

CA LMP

CAIRIM の重要な要素として提供されています。CA LMP により、ライセンスされているソフトウェアの、標準化された自動トラッキング機能が実現されます。CAIRIM のインストール後に、すべての CA LMP サポート対象製品についてテクニカル サポートにアクセスできます。

CAICCI

CA エンタープライズ アプリケーションに共通通信ソフトウェア層が提供されます。これにより、アプリケーションがプロトコルの詳細、エラー回復、システム接続の確立を処理しなくても済みます。

CA GSS

CA GSS は、CA Common Services for z/OS の一部で、CA Common Services for z/OS と同時にインストールされます。

本製品の機能の一部を最大限に活用するには、ご自分のサイトに CA GSS がインストールされている必要があります。

CA Health Checker

CA 製品に対して、簡単で一貫性のある方法を提供して、IBM Health Checker for z/OS で実行するためのヘルスチェックを作成します。IBM Health Checker for z/OS は、ユーザが推奨される設定を使用してシステムまたは製品のパラメータ、およびシステム ステータスを調べることによって、z/OS 環境内で考えられる問題を特定するうえで有用です。CA では、CA z/OS 製品に対するチェックの作成において、他のベンダーを追加しました。以下のコンポーネントがインストールおよび設定されているシステム上で製品が開始されると、CA OPS/MVS ヘルス チェックがターゲットシステム上で自動的にアクティブになります。

- CA Health Checker Common Service
- IBM Health Checker for z/OS

CA Health Checker Common Service のインストールの詳細については、「*CA Common Service インストール ガイド*」を参照してください。

IBM Health Checker for z/OS の詳細については、「*IBM Health Checker for z/OS User Guide*」を参照してください。

セキュリティの要件

このガイドのタスクを完了するには、以下のセクションで説明するセキュリティ権限が必要です。

注: セキュリティ製品ログオン ID の要件の詳細については、「[製品セキュリティログオン ID の作成 \(P. 125\)](#)」を参照してください。

以下の表は、CA OPS/MVS に対するアクセス要件の概要を示しています。ユーザ独自のデータベースをアップデートするアプリケーションを開発する場合、これらのアプリケーションにもアクセスが必要です。製品の使用を開始し独自のアプリケーションを書いたら、独自の REXX、CLIST、OPSEXEC、および、おそらくユーザ ISPF データセットへのアクセスも提供する必要があります。

データセット名	アクセス	ユーザ ID
OPS.xxx.RULES	Read、Write	OPSMAIN および権限付与された TSO ユーザ
OPS.CCLXLOAD	Execute	OPSMAIN、OPSOSF、OPSECF およびすべての TSO ユーザ
OPS.CCLXEXEC	Read	OPSMAIN、OPSOSF、OPSECF およびすべての TSO ユーザ
OPS.CCLXCLS00	Read	OPSMAIN、OPSOSF、OPSECF およびすべての TSO ユーザ
OPS.OPSLOG	Read、Write	OPSMAIN
OPS.SYSCHK1	Read、Write	OPSMAIN
Logical Parmlib Concatenation	Read	OPSMAIN
OPS.CCLXHENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXPENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXMENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXSENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXTENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXOPEX	Read	権限付与されたすべての TSO ユーザおよび場合により OPSOSF

注: SSMGA を使用している場合、OPS.CCLXOPEX データセットも OPSMAIN プロシージャに割り当てする必要があります。

重要: データセットにアクセスするための十分な権限を各アドレス空間に与えないまま CA OPS/MVS を実行してしまうことは、インストールに関する最も一般的な問題です。

TSO OPER 権限

セキュリティパッケージを通してすべてのユーザ ID に TSO OPER 権限を付与します。これらのユーザ ID には、OPSMAIN や OPSOSF など、ADDRESS OPER コマンドを発行し、OPSVIEW 6 からコマンドを入力し、opslog OPSVIEW 1 パネルからコマンドを入力するすべてのユーザ ID が含まれます。

適切な TSO OPER 権限が付与されているかどうかを調べるには、OPS/REXX プログラム OPSIVP を実行します。

同様に、TSO のサブミット、ステータス、およびキャンセルのコマンドを使用する必要があるユーザ ID にも上述の作業が必要です。

輸出申告

米国政府は、CA OPS/MVS の暗号化機能についての技術審査を完了し、CCATS #G050502 および 5D002 ENC の商業分類を規定しました。本製品による暗号化の使用は、OPSLOG WebView 機能で説明されています。

ストレージ要件

このセクションでは、CA OPS/MVS をインストールして実行するために必要なストレージについて説明します。

ECSA の使用およびストレージの要件

CA OPS/MVS は標準次の CSA ストレージの必要最低限の量を使用します。CA OPS/MVS のアドレス空間はせいぜい、標準の 16 MB 次の約 2 KB のストレージを使用するだけです。CA OPS/MVS は z/OS のクロスメモリ サービスを広範に使用して、このように CSA の使用量を少なくしています。このため、メインの CA OPS/MVS アドレス空間の拡張プライベート領域では、グローバルに使用されたデータ領域を格納できます。ただし、CA OPS/MVS の大半のコード、およびいくつかのデータエリアは、拡張 CSA (ECSA) ストレージ内に存在しています。

このため、CA OPS/MVS で使用するために、500 KB の ECSA を確保しておくことを強くお勧めします。ほとんどのサイトでは、多量の ECSA が割り当てられているため、CA OPS/MVS に対して 500 KB を確保しておけば、ECSA の量を増やす必要はありません。ただし、制限された ECSA の量でサイトを実行している場合は、CA OPS/MVS をインストールする前に 500 KB 増やしてください。

注:

- ECSA の最下部は 1 MB 単位に切り上げられるので、思っているよりも多くの ECSA があります。
- CA OPS/MVS が異常終了した場合は、必要なすべてのモジュールをロードして、CA OPS/MVS を再開するのに十分な ECSA がない可能性があります。このような状況が発生した場合は、システムの IPL を行って共通ストレージの一部を解放してください。ご使用のデータセンタでこのような状況が発生する可能性があると思った場合は、IEASYSxx CSA パラメータの 2 番目の値が十分に大きいことを確認してください(CSA=(x,40000) など)。ECSA の常駐モジュールを再ロードするのに CA OPS/MVS のモジュール再ロード機能を使用すると、CA OPS/MVS の ECSA 使用率が増えることがわかります。置換されたモジュールは、製品をシャットダウンするまで削除されません。

配布ライブラリ、ターゲット ライブラリ、およびデータ エリアの DASD スペース

CA OPS/MVS はさまざまな目的のために DASD スペースを必要とします。たとえば、OPSLOG、グローバル変数、RDF および System State Manager 変数などの各種データエリア、配布ライブラリ、およびターゲットライブラリに使用されます。

これらの目的のために割り当てられる DASD スペースの大きさに関する概要を以下に示します。

- SMP/E が制御する配布ライブラリとターゲット ライブラリ
3390 シリンダの数: 340
- ESD インストールの場合のみ、追加の Relfile がインストールのために一時的に割り当てられます。この割り当ては、インストール後に OPS.SAMPJCL のクリーンアップ JCL を使用してクリーンアップできます。
3390 シリンダの数: 110
- 初期製品ユーザには十分な、データ エリアのデフォルト サイズ
3390 シリンダの数: 270

注: 必要な DASD の計算方法の詳細については、このガイドの付録「[DASD 計算チャート](#) (P. 249)」を参照してください。

同時リリース

CA OPS/MVS のこのリリースをインストールした場合でも、本番環境用に旧リリースを引き続き使用できます。旧リリースを引き続き実行する場合は、以下のことを考慮します。

- 既存の SMP/E 環境にインストールする場合は、このインストールによって旧リリースが削除されます。
- テープから、または Pax-Enhanced ESD で取得した場合は、現在のリリースがインストールされているゾーンとは別のターゲットおよび配布ゾーンを新リリース用として選択します。新しいゾーンは、現在のリリースとは異なるライブラリを使用します。

注: CA MSM は、デフォルトによって新しい CSI にインストールされます。

- 新しいゾーンに DDDEF エントリを定義して、SMP/E がインストール用の適切なライブラリを指すようにします。それらが新リリースのライブラリを指していることを確認します。

ユーザの環境に応じた CA OPS/MVS のインストールのカスタマイズ

CA OPS/MVS r12 のインストールは 5 つの個別の SMP/E 機能、または FMID に分割されます。CA OPS/MVS 基本機能 (FMID CCLXC00) のインストールは必須です。以下の他の機能 (FMID) のインストールはオプションです。

1. CA OPS/MVS OPSLOG WebView (CCLXC01)
2. CA Network および Systems Management (NSM) System State Manager (SSM) CA OPS/MVS オプション (CCLXC02)
3. CA OPS/MVS CICS Operations Facility (CCLXC03)
4. CA OPS/MVS OPSHMC REXX (CCLXC04)

Note: 機能 1、2 および 3 には個別のユーザ使用許諾契約が必要です。

インストール中に、基本機能に加えて、インストールする機能を選択する必要があります。

CA MSM インストールの手順 2 の実行中に、[Custom installation]を選択して、インストールする機能を選択します。すべての機能を簡単にインストールできるように、[Full Installation]オプションが用意されています。

Native SMP/E JCL インストール中に、SAMPJCL メンバを手動で編集して、インストールを選択した機能のみを SMP/E RECEIVE、APPLY、ACCEPT します。

ユーザの環境に応じた外部ライブラリ名のカスタマイズ

CA OPS/MVS r12 のインストールには、他の製品によってユーザ サイトにインストールされているライブラリの使用が必要になる場合があります。ユーザ固有の環境に合わせて、これらの "外部" 製品ライブラリの名前をカスタマイズします。これらのライブラリ名は SMP/E に DDDEF として定義されます。

CA MSM インストールの手順 4 の実行中に、選択した機能のインストールに必要な "外部" 製品ライブラリの名前を提供します。

Native SMP/E JCL インストール中に、SAMPJCL メンバ CLXSEdit を、選択した機能のインストールに必要な "外部" 製品ライブラリの名前で手動更新します。

必要になる可能性のあるデフォルトの "外部" 製品ライブラリ名のリスト、およびインストールにそのライブラリが必要な関連付けられた CA OPS/MVS 機能がそれに続きます。インストールする CA OPS/MVS 機能のリストの選択時に、ユーザ サイトのライブラリの実際の名前を指定します。

SYS1.SCSQLOAD

IBM Websphere MQ-Series ロードライブラリ。

CA OPS/MVS 基本機能 (FMID CCLXC00) にはこのライブラリが必要です。

重要: IBM WebSphere MQ-Series がユーザ サイトにインストールされていない場合、CA OPS/MVS によってインストールされる CA OPS/MVS サイドデッキ SMP/E ターゲットライブラリの名前を指定する必要があります。たとえば、hlq.CCLXSIDE です。

SYS1.SIEASID

IBM Cryptographic Services Secure Sockets Layer サイドデッキライブラリ。

CA OPS/MVS OPSLOG Webview 機能 (FMID CCLXC01) には、このライブラリが必要です。

CAI.CNSMSDF

CA Common Services (CCS) Agent Technologies サイドデッキライブラリ。

CA OPS/MVS NSM SSM Option 機能 (FMID CCLXC02) には、このライブラリが必要です。

このライブラリは、CCS r14 で CAI.CNSMSDF としてインストールされます。

このライブラリは、CCS r12 で CAI.CAISDF としてインストールされます。

このライブラリは、CCS r11 で CAI.EXP としてインストールされます。

SYS1.SDFHLOAD

IBM CICS ロード ライブラリ。

CA OPS/MVS CICS Operations Facility 機能 (FMID CCLXC03) には、このライブラリが必要です。

/user/dll/

IBM Hardware Console Management API DLL USS ディレクトリ。

CA OPS/MVS OPShMC REXX 機能 (FMID CCLXC04) には、この USS ディレクトリが必要です。

HWMCAAPI という名前の DLL ファイルを、IBM の Web サイトからこの USS ディレクトリのファイル HWMCAAPI にダウンロードします。このファイルは、<http://www.ibm.com/servers/resourcelink> からダウンロードできます。
[Services]-[API]-[z/OS] を順番にクリックします。詳細については、IBM のマニュアル「*System z Application Programming Interfaces (SB10-7030-14)*」を参照してください。

USER.HWMCAEXP

IBM Hardware Console Management API サイドデッキ ライブラリ。

CA OPS/MVS CA OPS/MVS OPShMC REXX 機能 (FMID CCLXC04) には、このライブラリが必要です。

このライブラリは RECFM=FB/LRECL=80 である必要があります。

HWMCAAPI.x という名前のサイドデッキ ファイルを、IBM の Web サイトからこのライブラリのメンバ HWMCAAPI へダウンロードします。このファイルは、<http://www.ibm.com/servers/resourcelink> からダウンロードできます。
[Services]-[API]-[z/OS] を順番にクリックします。詳細については、IBM のマニュアル「*System z Application Programming Interfaces (SB10-7030-14)*」を参照してください。

ユーザの環境に応じた CA OPS/MVS OPSLOG WebView zFS Mount のカスタマイズ

CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) のインストールでは、ユーザのサイトで zFS を割り当て、マウントします。割り当てられた zFS の高レベル修飾子、および作成された USS マウントポイントをカスタマイズします。zFS 名およびマウントポイントは、DDDEF として SMP/E に定義されます。

CA MSM インストールの手順 4 の実行中に、割り当てられる zFS の高レベル修飾子、および作成される USS マウントポイントを提供します。

Native SMP/E JCL インストール中に、SAMPJCL メンバ CL11ALLU、CL12MKD および CL13CSIU を、割り当てられる zFS の高レベル修飾子および作成される USS マウントポイントで手動更新します。

第 3 章: CA MSM を使用した製品のインストール

これらのトピックによって、CA MSM を使用して製品の管理を開始するのに必要な情報が提供されます。CA MSM のオンライン ヘルプを使用して、追加情報を取得できます。

これらのトピックを使用する前に、CA MSM がすでにサイトにインストールされている必要があります。CA MSM がインストールされていない場合、[CA サポート Online Web サイト](#)の Download Center からダウンロードできます。また、ここから CA MSM のすべてのドキュメントのリンクも利用できます。

注: このセクションに記載されている情報は、CA MSM の最新版に適用されます。以前のバージョンを使用している場合は、CA メインフレームソフトウェア マネージャの製品ページで適切なマニュアル選択メニューを参照してください。

CA MSM を使用する方法: シナリオ

以下に示すシナリオでは、最近あなたの組織が、CA Technologies 製品のインストールを簡略化し、それらの管理を統一化するために CA MSM を導入したものとします。また、新しい CA Technologies 製品のライセンスも取得したものとします。さらに、すでにインストール済みの製品の多数の既存 CSI があります。

- 最初のシナリオでは、CA MSM を使用して、新しい製品を取得する方法を示します。
- 2 番目のシナリオでは、CA MSM を使用して、新しい製品をインストールする方法を示します。
- 3 番目のシナリオでは、CA MSM を使用して、環境内にすでにインストールされている製品を管理する方法を示します。
- 4 番目のシナリオでは、CA MSM を使用して、その製品をターゲットシステムに展開する方法を示します。
- 5 番目のシナリオでは、CA MSM を使用して、展開した製品をターゲットシステムに適合するように構成する方法を示します。

製品の取得方法

製品取得サービス (PAS) を使用すると、メインフレーム製品とそのサービス (プログラム一時修正 (PTF) など) を簡単に取得できます。PAS は、ユーザのサイトにライセンスされている製品に関する情報を取得します。次に、PAS はそれらのライセンス情報を、ユーザの実行システムでメンテナンスされているソフトウェアインベントリに記録します。

CA MSM の PAS コンポーネントを使用して、CA Technologies 製品を取得できます。

以下の手順に従います。

1. CA Support Online アカウントをセットアップします。

CA MSM を使用して製品を取得またはダウンロードするには、CA Support Online のアカウントが必要です。アカウントがない場合は、[CA サポート Online Web サイト](#) でアカウントを作成できます。

2. サイトの CA MSM の URL を決定します。

[CA MSM \(P. 41\)](#) にアクセスするには、その URL が必要です。URL をサイトの CA MSM 管理者から取得し、z/OS 認証情報を使用してログインできます。初回ログイン時に、[CA サポート Online Web サイト](#) の認証情報で CA MSM アカウントの作成を促すメッセージが表示されます。このアカウントによって、製品パッケージをダウンロードできます。

3. CA MSM にログインし、Software Catalog ページに移動して、管理する製品を見つけます。

CA MSM にログインした後、[Software Catalog] タブにユーザの組織に対してライセンスが付与されている製品が表示されます。

取得する製品が見つからない場合は、カタログを更新してください。CA MSM は、[CA サポート Online Web サイト](#) 全体で [CA サポート Online Web サイト](#) に対するユーザの認証情報に関連付けられたサイト ID を使用して、カタログをリフレッシュします。

4. 製品インストール パッケージをダウンロードします。

カタログで製品が見つかったら、その製品のインストール パッケージをダウンロードできます。

CA MSM は CA FTP サイトからパッケージ (任意のメンテナンス パッケージを含む) をダウンロード (取得) します。

取得プロセスの完了後、製品はインストールまたは保守可能な状態になります。

製品のインストール方法

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 (CSI) 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。

CA MSM の SIS コンポーネントを使用して、CA Technologies 製品をインストールできます。

以下の手順に従います。

1. 製品のインストールを開始し、製品情報を確認します。
2. インストール タイプを選択します。
3. インストールの前提条件を確認します (何らかの条件が示されている場合)。
4. 以下の手順のいずれかを選択して、CSI を選択します。
 - CSI の作成:
 - a. グローバルゾーンをセットアップします。
 - b. ターゲットゾーンを作成します。
 - c. 配布ゾーンを作成します。
 - 作業セットの既存の CSI の使用:
 - a. グローバルゾーンを更新します。
 - b. ターゲットゾーンのセットアップ: ターゲットゾーンを作成するか既存のターゲットゾーンを使用します。
 - c. 配布ゾーンのセットアップ: 配布ゾーンを作成するか既存の配布ゾーンを使用します。

注: 製品またはそのコンポーネントのいずれかを既存のターゲットゾーンまたは配布ゾーンにインストールする場合、インストール プロセスによって古いバージョンがそれらのゾーンおよび関連付けられたターゲットおよび配布データセットから削除されます。必要に応じて現在のリリースにメンテナンスを適用できるように、今回のインストールには新しいターゲットゾーンと配布ゾーンを使用することをお勧めします。

5. インストール サマリを確認して、インストールを開始します。

これで、製品を展開できる状態になりました。

詳細:

[展開を準備する方法 \(P. 88\)](#)

既存製品の保守方法

既存の CSI がある場合、それらの CSI を CA MSM に移動して、インストール済みのすべての CA 製品を単一の Web ベースのインターフェースから一元的に保守できます。

PAS および SIS を使用して、CA Technologies 製品を保守できます。

以下の手順に従います。

1. CSI を CA MSM へ移行して、CA MSM で既存の CSI を保守します。
移行中に、CA MSM は CSI に関する情報をデータベースに格納します。
2. [Software Catalog] タブから、インストール済み製品リリース用の最新のメンテナンスをダウンロードします。
リリースが見つからない場合 (たとえば、リリースが古いため) は、リリースを手動でカタログに追加してから、リリースを更新し、メンテナンスをダウンロードします。
3. メンテナンスを適用します。

注: また、[SMP/E Environments] タブから、メンテナンスを特定の CSI にインストールできます。

メンテナンスプロセス完了後、製品は展開可能な状態になります。展開プロセスを開始する前に、CA MSM 外で手動で他の手順の実行が必要になる場合があります。

詳細:

[展開を準備する方法 \(P. 88\)](#)

製品の展開方法

ソフトウェア展開サービス (SDS) によって、実行システムのソフトウェア インベントリからターゲットシステムへのメインフレーム製品の展開が容易になります。簡略化される操作には、既知のトポロジ全体での適切な転送メカニズムによる、ポリシー準拠のインストール済み製品の展開などがあります。

CA MSM の SDS コンポーネントを使用して、すでに取得してインストールした CA Technologies 製品を展開できます。

これを行うには、以下のタスクを完了します。

1. システムレジストリをセットアップします。
 - a. 企業が保有するシステムを決定します。
 - b. それらのシステムのリモート認証情報をセットアップします。
 - c. ターゲットシステム (非シスプレックス、シスプレックスまたはモノプレックス、共有 DASD クラスタ、およびステージング) をセットアップし、検証します。
 - d. ネットワーク情報を、データ宛先情報を含めて、各システムレジストリエントリに追加します。
2. 方法をセットアップします。
3. 展開を作成します。その際、新しい展開ウィザードの各手順を実行します。

作成した展開を保存して、後でシステム、製品、カスタム データセット、および方法を追加および編集して変更したり、ウィザードから直接展開したりできます。

注: 同じ方法を使用して他の製品を以前定義したシステムに展開する必要がある場合は、別の展開を作成する必要があります。
4. 製品を展開します。その際、スナップショットの作成、ターゲットへの転送、およびメインフレーム環境への展開 (解凍) を実行します。

これで、製品を構成する準備ができました。

詳細:

[CA MSM による展開の完了方法 \(P. 90\)](#)

製品の構成方法

ソフトウェア構成サービス (SCS) によって、実行システムのソフトウェア インベントリからターゲットの z/OS オペレーティング システムへのメインフレーム製品の設定が容易になります。

CA MSM の SCS コンポーネントを使用して、すでに取得、インストール、および展開を行った CA Technologies 製品を構成できます。

以下の手順に従います。

1. [Deployments] タブで構成する展開済み製品を選択し、**Create Configuration** ウィザードを表示します。
2. 構成を作成します。その際、以下を含む **Create Configuration** ウィザードの各手順を実行します。
 - a. 構成名を定義し、ターゲットシステムを選択します。
 - b. 構成の機能とオプションを選択します。
 - c. システム基本設定を定義します。
 - d. ターゲット設定を作成します。
 - e. リソースを選択して編集します。
3. 構成を構築します。**Create Configuration** ウィザードの最後の手順で、構成を構築できます。
4. 構成を実装します。**CA MSM** の実装プロセスでは、順番に 1 つずつ手順を実行します。ユーザには丁寧な説明と、実装プロセスを開始、停止、および管理する詳細な手順が示されます。

構成プロセスを完了すると、製品はいつでも使用できる状態になります。場合によっては、**CA MSM** の外部で他の手順を手動で実行する必要があります。

注: **CA MSM** を使用して、製品をステージング システムに構成することはできません。

Web ベース インターフェースを使用した CA MSM へのアクセス

Web ベース インターフェースを使用して CA MSM へアクセスします。CA MSM 管理者から CA MSM の URL を取得します。

以下の手順に従います。

1. Web ブラウザを開き、アクセス先の URL を入力します。

ログイン ページが表示されます。

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

2. z/OS のログイン ユーザ名およびパスワードを入力し、[Log In] ボタンをクリックします。

開始ページが表示されます。初めてログインする場合、[CA サポート Online Web サイト](#) でアカウントを定義するように促すメッセージが表示されます。

注: インターフェースの詳細については、このページの右上隅にある [Help] リンクをクリックしてください。

3. [New] をクリックします。

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

重要: 認証情報が適用されるアカウントには、[Product Display Options] に「BRANDED PRODUCTS」が設定されている必要があります。[CA サポート Online Web サイト](#) にログインし、[My Account] をクリックして、アカウントの基本設定を表示および更新できます。正しい設定が指定されていない場合、CA MSM を使用して製品情報およびパッケージをダウンロードすることができません。

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

ユーザ設定の確認を促すメッセージが表示されます。

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

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

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

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

第 4 章: Pax-Enhanced ESD からの製品のインストール

このセクションの手順を使用し、Pax-Enhanced Electronic Software Delivery (ESD)を使用したユーザの製品の取得およびインストールを実行します。

このセクションの手順を完了したら、「製品の設定」に移動してください。

このセクションには、以下のトピックが含まれています。

[Pax-Enhanced ESD を使用して製品をインストールする方法 \(P. 43\)](#)

[ファイル システムの割り当ておよびマウント \(P. 49\)](#)

[製品 pax ファイルの USS ディレクトリへのコピー \(P. 51\)](#)

[pax ファイルからの製品ディレクトリの作成 \(P. 57\)](#)

[z/OS データセットへのインストール ファイルのコピー \(P. 58\)](#)

[ネイティブ SMP/E JCL を使用したインストール方法 \(P. 60\)](#)

[USS ディレクトリのクリーンアップ \(P. 64\)](#)

[メンテナンスの適用 \(P. 65\)](#)

[HOLDDATA \(P. 67\)](#)

Pax-Enhanced ESD を使用して製品をインストールする方法

このセクションでは、Pax-Enhanced ESD プロセスについて説明します。初めて Pax-Enhanced ESD のインストールを実行する場合は、この概要を読み、すべての手順を実行することをお勧めします。経験のある UNIX ユーザの場合、このあとのインストールを実行するには、「Pax-Enhanced ESD Quick Reference Guide」またはこの概要が役に立ちます。

重要: Pax-Enhanced ESD プロセスの一環として SMP/E インストール用 pax ファイルをダウンロードするには、ESD プロセスに使用されている USS (UNIX System Services) ディレクトリへの書き込み権限が必要になります。

重要: z/OS UNIX システム サービスにすべての CA 製品インストーラを含める必要がない場合、USS に関連するグループを割り当てた後、手順 1 から 4 を実行し、解凍された MVS データセットのリストを製品インストーラに指定します。製品の実際の SMP/E RECEIVE、または残りのインストール手順では USS は必要ありません。

Pax-Enhanced ESD を使用してファイルをインストールするには、以下の手順に従います。

1. ファイル システムを割り当ててマウントします。このプロセスでは、**pax** ファイルを受信して解凍手順を実行するための **USS** ディレクトリが必要です。**Pax-Enhanced ESD** 専用のファイル システムのマウントおよび割り当てを行い、そのファイル システム内にディレクトリを作成することをお勧めします。**pax** ファイルを使用するすべてのユーザがそのディレクトリに対する書き込み権限を持っていることを確認します。
2. 製品 **pax** ファイルを **USS** ディレクトリにコピーします。ファイルをダウンロードするには、以下のいずれかのオプションを選択します。
 - **CA Support Online** から自分のマシンに **ZIP** ファイルをダウンロードして解凍し、次に製品 **pax** ファイルを **USS** ファイル システムにアップロードします。
 - **CA Support Online** ディレクトリから **USS** ディレクトリに **pax** ファイルを **FTP** で直接ダウンロードします。

注: **USS** ディレクトリにアップロードする **pax** ファイルごとに、手順 3 ~ 6 を実行します。

3. **pax** ファイルから製品ディレクトリを作成します。現在の作業ディレクトリを **pax** ファイルが存在するディレクトリに設定し、以下コマンドを入力して **USS** ディレクトリに新規ディレクトリを作成します。

```
pax -rvf pax-file-name
```

4. **SMP/E GIMUNZIP** ユーティリティを使用して、**z/OS** インストール データ セットを作成します。手順 3 で **pax** コマンドによって作成されたディレクトリにある **UNZIPJCL** ファイルには、インストール パッケージを **GIMUNZIP** するためのサンプル ジョブが含まれています。**UNZIPJCL** ジョブを編集およびサブミットする方法
5. **SMP/E** パッケージを **RECEIVE** します。この手順では、手順 4 で **GIMUNZIP** によって作成されたデータセットを使用します。**SMPPTFIN** および **SMPHOLD** (該当する場合) **DASD** データセットを使用して、標準的な **SMP/E RECEIVE** を実行します。また、**RECEIVE** コマンドの **RFPREFIX** パラメータ上で **RELFILE** の高レベル修飾子を指定します。
6. 製品のインストールに進みます。製品マニュアル (**README** ファイルおよびインストールに関する注意を含む) に従ってインストールを完了します。
7. (オプション) **USS** ディレクトリをクリーンアップします。**pax** ファイル、**pax** コマンドで作成されたディレクトリ、そのすべてのファイル、および **SMP/E RELFILE**、**SMPMCS**、**HOLDDATA** データセットを削除します。

Pax-Enhanced ESD ダウンロードの仕組み

重要: Pax-Enhanced ESD プロセスの一部として SMP/E インストール用の pax ファイルをダウンロードするには、このガイドの手順を開始する前に、ESD プロセスおよび利用可能な USS ファイルスペースに使用する UNIX システム サービス (USS) ディレクトリに対して書き込み権限が必要です。その他の ESD の情報については、<http://www.ca.com/mainframe> を参照してください。Events の下に、Pax-Enhanced ESD プロセスについて詳しく説明するウェブキャストがあります。

Pax-Enhanced ESD を使用してファイルをダウンロードするには、以下の手順を使用します。

1. <https://support.ca.com/> にログインし、[Download Center]をクリックします。

CA Support Online Web ページが表示されます。

2. [Download Center]の下で、最初のドロップダウンリストから[Products]を選択した後、製品、リリースおよび genlevel (該当する場合)を指定し、[Go]をクリックします。

CA Product Download ウィンドウが表示されます。

3. CA 製品ソフトウェア パッケージ全体または個別の pax ファイルを PC またはメインフレームにダウンロードします。ZIP ファイルをダウンロードする場合、続行する前にそのファイルを解凍する必要があります。

両方のオプションについては、「[ESD 製品のダウンロード ウィンドウ \(P. 45\)](#)」でダウンロード インターフェイスが動作する仕組みについて説明します。

注: 従来のインストールのダウンロードについては、「*Traditional ESD User Guide*」を参照してください。<https://support.ca.com/> に移動し、ログインした後、[Download Center]をクリックします。ガイドへのリンクが[Download Help]見出しの下に表示されます。

4. 製品固有の手順に従って、製品のインストール手順を実行します。

製品がメインフレームにインストールされます。

ESD 製品のダウンロード ウィンドウ

CA 製品の ESD パッケージは複数の方法でダウンロードできます。選択肢は、ダウンロードする必要があるファイルごとのサイズやファイル数によって異なります。ユーザは、すべてのコンポーネントを含む完全な製品をダウンロードできます。また、製品またはコンポーネント用の個別の pax とドキュメントファイルを選択できます。

以下の図は、サンプルの製品ファイルを示しています。ここでは、製品のすべてのコンポーネントがリストされています。必要な 1 つまたは複数のコンポーネントを選択するか、[Add All to cart] チェックボックスを選択することによって、Download Cart を使用できます。すぐにコンポーネントをダウンロードする場合は、[Download] リンクをクリックします。

CA Earl - MVS

- ※ [Pax Enhanced Electronic Software Delivery \(ESD\) Guide](#)
- ※ [Pax Enhanced Electronic Software Delivery \(ESD\) Quick Reference Guide](#)
- ※ [Traditional Electronic Software Delivery \(ESD\) Guide](#)
- ※ [Learn more about Using pkzip with your Downloaded Mainframe Products](#)
- ※ [Learn more about downloading components of CA product](#)

If you have comments or suggestions about CA product documentation, send a message to techpubs@ca.com.

[View Download Cart](#)

Add All to cart

Product Components				Add to cart	Download
CA COMMON SERVICES PROD PKG 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	<input type="checkbox"/>	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	<input type="checkbox"/>	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	<input type="checkbox"/>	Download
EARL INSTALL GUIDE MANUAL I2J2ED610NE.pdf	6.1 /0000	03/31/2010	361KB	<input type="checkbox"/>	Download
CA COMMON SERVICES COVER LTR QI92742.pdf	11.0 /SP08	03/31/2010	46KB	<input type="checkbox"/>	Download

個別のコンポーネント用のリンクをクリックすると、[Download Method] ページに移動します。

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

HTTP via Internet Browser

If Download Manager cannot be used or fails to start you may access your file(s) via your internet browser.

[View File Link\(s\)](#)

FTP

This method allows you to download your file(s) via FTP from CA's content delivery network or via native FTP servers.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[FTP Request](#)

指定した製品ファイルのサイズや数によっては、[Download Method]画面に以下のオプションも表示されます。

注: [HTTP] メソッドを使用したメインフレームのダウンロードについては、[Learn More]リンクをクリックしてください。

Download Method

Please choose a download method to complete your download request. [Learn More](#)

HTTP via Download Manager

This is the CA recommended method for download. The Download Manager allows you to download your files faster and more efficiently.

[Download](#)

Create a Zip File

This method allows you to bundle your download files into one or more zip files of up to 3.5 GB each. These zip files can then be downloaded via HTTP or FTP.
Note: Processing is required and an email notification will be sent when your request is ready for downloading.

[Create Zip](#)

[HTTP]メソッドでは、すぐにダウンロードを開始できます。[FTP]メソッドでは、ユーザの選択を表示する[Review Orders]ページに移動します。ユーザの命令が処理されると、最初の[Pending]ステータスが[Ready]に変化します。

[Preferred FTP]では、新しいコンテンツ配信ネットワーク(CDN)を使用します。
[Alternate FTP]では、CA のニューヨークにある FTP サーバを使用します。

[Create a Zip File]オプションでは、最初に zip ファイルを作成し、準備ができると次の画面の[Zip Download Request]の例に示すオプションが表示されます。

Review Download Requests

Below is a list of the FTP and large HTTP downloads that have been requested by your site. When status is set to 'Ready' a link will appear.

- For FTP requests, click on the FTP link to view the path information for your download. For more information view our [FTP Help document](#)
- For HTTP requests, click on the HTTP link to initiate your download.
- To view the details of your request, click on the desired order number.

Today's Downloads

Order #	Status	Description	Date Placed	Download Options
10000961	Ready	FTP Download Request	04/30/2010	Preferred FTP ▼ Alternate FTP ▼

Previous 6 day Download History

Order #	Status	Description	Date Placed	Download Options
10000949	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼
10000948	Ready	ZIP Download Request	04/29/2010	HTTP via DLM Preferred FTP ▼ Alternate FTP ▼

USS 環境のセットアップ

以下のタスクを実行するには、UNIX システム サービス(USS)ディレクトリおよび十分な容量のあるファイルシステムが必要です。

- CA Support Online から pax ファイルを受信します。
- ユーティリティ機能を実行して、pax ファイルを解凍し、製品のインストールの完了に使用可能な MVS データセットにします。

Pax-Enhanced ESD 専用のファイル システムを割り当てて、マウントすることをお勧めします。ファイル システムに必要な容量は、以下によって異なります。

- ダウンロードする pax ファイルのサイズ。
- 解凍後に pax ファイルを保持するかどうか。この方法はお勧めしません。

pax ファイルのダウンロードおよび解凍には、1 つのディレクトリを使用することをお勧めします。同じディレクトリを再利用すると、USS のセットアップは最小限に抑えられます。USS のセットアップを 1 度だけ実行する必要があります。その後のダウンロードでは、同じディレクトリを再利用します。あるいは、pax ファイルのダウンロードごとに、新規ディレクトリを作成できます。

重要: Pax-Enhanced ESD プロセスの一環として SMP/E インストール用 pax ファイルをダウンロードするには、ESD プロセスに使用されている USS (UNIX System Services) ディレクトリへの書き込み権限が必要になります。また、ESD ディレクトリを含むファイル システムでは、pax ファイルのダウンロードおよびそのコンテンツの解凍を実行するために、pax ファイルの 3.5 倍の空き容量が必要です。たとえば、14MB の pax ファイルのダウンロードと解凍を行うには、ESD ディレクトリをホストしているファイル システムに約 49MB の空き容量が必要です。

ファイル システムの割り当ておよびマウント

Pax-Enhanced ESD のダウンロードには、zSeries File System (zFS) または階層ファイル システム (HFS) を使用できます。

この手順では、以下のタスクを実行する方法について説明します。

- HFS ファイル システムの割り当て
- 既存のメンテナンス ディレクトリでの新しいマウント ポイントの作成
- 新しく作成されたマウント ポイント上でのファイル システムのマウント
- オプションとして、ディレクトリ作成者と同じグループのユーザへの書き込み権限の許可

重要: USS コマンドでは大文字と小文字が区別されます。

ファイルシステムの割り当ておよびマウントを実行する方法

1. HFS を割り当てます。以下に例を示します。

```
//ALCHFS EXEC PGM=IEFB14
//CAESD DD DSN=yourHFS dataset name,
// DISP=(NEW,CATLG,DELETE),UNIT=3390,
// DSNTYPE=HFS,SPACE=(CYL,(primary,secondary,1))
```

HFS が割り当てられます。

2. ファイルシステムのマウントポイントを作成します。この例では、既存のディレクトリ /u/maint に /CA/CAESD ディレクトリを作成する方法について説明します。TSO OMVS シェルから、以下のコマンドを入力します。

```
cd /u/maint/
mkdir CA
cd CA
mkdir CAESD
```

注: このドキュメントでは、この構造を *USSESDdirectory* と呼びます。

マウントポイントが作成されます。

3. ファイルシステムをマウントします。たとえば、TSO から以下のコマンドを入力します。

```
MOUNT FILESYSTEM('yourHFS dataset name')
MOUNTPOINT('yourUSSESDdirectory')
TYPE(HFS) MODE(RDWR)
```

ファイルシステムがマウントされます。

4. (オプション)このディレクトリのセキュリティ権限を設定します。chmod コマンドを使用すると、他のユーザに ESD ディレクトリおよびディレクトリ内のファイルへのアクセスを許可することができます。たとえば、USS グループの他のユーザに ESD ディレクトリへの書き込み権限を許可するには、TSO OMVS シェルから以下のコマンドを入力します。

```
chmod-R 775 /yourUSSESDdirectory/
```

書き込み権限が許可されます。

注: chmod コマンドの詳細については、「z/OS UNIX System Services User Guide (SA22-7802)」を参照してください。

製品 pax ファイルの USS ディレクトリへのコピー

CA 製品インストール手順を開始するには、セットアップした USS ディレクトリに製品 pax ファイルをコピーします。以下のいずれかの方法を使用します。

- CA Support Online FTP サーバから z/OS システムに製品 pax ファイルを直接ダウンロードします。
- CA Support Online FTP サーバからローカル PC に製品 pax ファイルをダウンロードしてから、z/OS システムにアップロードします。
- CA Support Online からローカル PC に製品ファイルをダウンロードします。zip ファイルが含まれている場合は解凍し、解凍した pax ファイルを z/OS システムにアップロードします。

このセクションには、CA Support Online FTP サーバから z/OS システム上の USS ディレクトリに製品 pax ファイルを直接ダウンロードするためのバッチ ジョブ、およびローカル PC から z/OS システム上の USS ディレクトリに pax ファイルをアップロードするためのサンプルコマンドが含まれています。

重要: FTP 手順は、ローカルのファイアウォールの設定およびその他のセキュリティ設定によって異なる場合があります。ローカル ネットワーク管理者に問い合わせ、サイトで使用する適切な FTP 手順を調べてください。

重要: 製品の pax ファイルを保持するには、Pax-Enhanced ESD に使用する USS ファイル システムに十分な空き容量があることを確認してください。十分な空き容量が存在しない場合は、以下のようなエラー メッセージが表示されます。

```
EZA1490I Error writing to data set  
EZA2606W File I/O error 133
```

ダウンロードが完了すると、ユーザの USS ディレクトリにある pax ファイルのサイズは、CA 製品ダウンロードウィンドウ上の対応する pax ファイルのカラムの値と一致します。

バッチ JCL を使用したダウンロード

メインフレーム上でバッチ JCL を実行し、CA Support の製品ダウンロードウィンドウから pax ファイルをダウンロードするには、このプロセスを使用します。ダウンロードを実行するには、この PDF ファイルに CAtoMainframe.txt として添付されているサンプル JCL を使用します。

重要: Pax-Enhanced ESD プロセスを簡素化するために、このガイドの PDF バージョンには、メインフレームに直接コピーできるサンプル JCL ジョブが含まれています。このジョブにアクセスするには、PDF リーダの左下にあるクリップアイコンをクリックします。ウィンドウが開き、添付ファイルが表示されます。ファイルをダブルクリックしてサンプル JCL を表示します。

注: CA Support Online で説明されている推奨方法に従うことをお勧めします。この手順は推奨のダウンロード方法ですが、次のセクションでは PC を経由してメインフレームにダウンロードする手順も示します。

バッチ JCL を使用したダウンロード方法

1. 有効な JOB ステートメントを指定します。
2. *yourTCPIP.PROFILE.dataset* をシステム用の TCPIP プロファイル データセットの名前に置き換えます。必要な場合、ローカル ネットワーク管理者に問い合わせます。

ジョブは指定したプロファイルを参照します。

3. *YourEmailAddress* を自分の電子メール アドレスに置き換えます。

ジョブは指定した電子メール アドレスを参照します。

4. *yourUSSESDdirectory* を ESD ダウンロードに使用する USS ディレクトリの名前に置き換えます。

ジョブは指定した USS ディレクトリを参照します。

5. CA Support Online の製品ダウンロードウィンドウで、ダウンロードする製品コンポーネントを検索します。

ダウンロードする製品コンポーネントが見つかります。

6. 該当するファイルに対応する [Download] をクリックします。

注: ファイルをカートに追加してダウンロードを複数行うことができます。

[Download Method] ウィンドウが開きます。

7. [FTP Request]をクリックします。

[Review Download Requests]ウィンドウが開き、ダウンロードをリクエストしたすべてのファイルが表示されます。

注: ファイルをダウンロードする準備ができると電子メールが送信されます。または、ファイルを手に入れるようになるとウィンドウにリンクが表示されます。

8. 以下のいずれかの方法を選択します。

Preferred FTP

CA の世界規模のコンテンツ配信ネットワーク(CDN)を使用します。
Preferred FTP を使用してダウンロードできない場合は、会社でセキュリティ制限が設定されている可能性があります。この場合、社内ネットワークの外部に存在するダウンロード元のすべてのサーバの知識および設定が必要になります。

ホスト名: ftp://ftpdnloads.ca.com

Alternate FTP

ニューヨーク州ロングアイランドに置かれている元のダウンロードサーバを使用します。

ホスト名: ftp://scftpd.ca.com (製品ファイルおよびダウンロードカートファイル)、ftp://ftp.ca.com (個々のソリューションファイル)

いずれの方法でも、ホスト、ユーザ名、パスワード、および FTP の場所が表示されるので、それらをサンプル JCL にコピーできます。

注: FTP の詳細については、[Review Download Requests]ウィンドウに表示される[FTP Help document]リンクおよび[Download Methods]ウィンドウに表示される[Learn More]リンクを参照してください。

9. ジョブをサブミットします。

重要: FTP コマンドが正しくない場合、このジョブは失敗し、ゼロ状態コードを返す場合があります。ジョブ DDNAME SYSPRINT 内のメッセージを参照して FTP が成功したことを確認してください。

JCL を実行すると、指定したメインフレーム USS ディレクトリに pax ファイルが格納されます。

例: CAtoMainframe.txt JCL

添付の CAtoMainframe.txt JCL ファイルには以下のテキストが表示されます。

```
//GETPAX JOB (ACCOUNTNO),'FTP GET ESD PACKAGE',
//      MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to download a pax file directly from *
/* CA Support Online to a USS directory on your z/OS system.      *
/*                                                                *
/* This job must be customized as follows:                        *
/* 1. Supply a valid JOB statement.                               *
/* 2. Replace "yourTCPIP.PROFILE.dataset" with the name if the TCPIP *
/*    profile data set for your system.                           *
/* 3. Replace "Host" based on the type of download method.        *
/* 4. Replace "YourEmailAddress" with your email address.         *
/* 5. Replace "yourUSSESDdirectory" with the name of the USS      *
/*    directory used on your system for ESD downloads.            *
/* 6. Replace "FTP Location" with the complete path                *
/*    and name of the pax file obtained from the FTP location    *
/*    of the product download page.                               *
//*****
//GETPAX EXEC PGM=FTP,REGION=0K
//SYSTCPD DD DSN=yourTCPIP.PROFILE.dataset,DISP=SHR
//SYSPRINT DD SYSOUT=*
//OUTPUT DD SYSOUT=*
//INPUT DD *
Host
anonymous YourEmailAddress
lcd yourUSSESDdirectory
binary
get FTP location
quit
```

PC を経由したファイルのメインフレームへのダウンロード

CA Support Online から PC に pax または zip ファイルをダウンロードする場合は、この手順を使用して PC から z/OS USS ディレクトリに pax ファイルをアップロードします。

PC からメインフレームにファイルをアップロードする方法

1. 「[Pax-Enhanced ESD ダウンロードの仕組み \(P. 20\)](#)」で説明されている手順に従って、製品 pax または zip を PC にダウンロードします。zip ファイルをダウンロードした場合は、そのファイルを解凍して製品 pax ファイルを使用します。

pax または zip ファイルが PC に格納されます。

2. Windows コマンド プロンプトを開きます。

コマンド プロンプトが表示されます。

3. FTP コマンドを以下のようにカスタマイズして入力します。

- a. *mainframe* を対象 z/OS システムの IP アドレスまたは DNS 名に置き換えます。

- b. *userid* を z/OS ユーザ ID に置き換えます。

- c. *password* を z/OS パスワードに置き換えます。

- d. *C:¥PC¥folder¥for¥thePAXfile* を PC 上の pax ファイルの場所に置き換えます。

- e. *yourUSSESDdirectory* を ESD ダウンロードに使用する USS ディレクトリの名前に置き換えます。

- f. *paxfile.pax.Z* をアップロードする pax ファイルの名前に置き換えます。

pax ファイルがメインフレームに転送されます。

例: FTP コマンド

このリストは、ユーザの PC からユーザの USS Pax-Enhanced ESD ディレクトリに pax ファイルをアップロードする FTP コマンドのサンプルです。

```
FTP mainframe
userid
password
bin
lcd C:%PC%folder%for%thePAXfile
cd /yourUSSESDdirectory/
put paxfile.pax.Z
quit
exit
```

pax ファイルからの製品ディレクトリの作成

この PDF ファイルに `Unpackage.txt` として添付されているサンプル ジョブを使用して、製品 pax ファイルを製品インストール ディレクトリに抽出します。

重要: Pax-Enhanced ESD プロセスを簡素化するために、このガイドの PDF バージョンには、メインフレームに直接コピーできるサンプル JCL ジョブが含まれています。このジョブにアクセスするには、PDF リーダの左下にあるクリップアイコンをクリックします。ウィンドウが開き、添付ファイルが表示されます。ファイルをダブルクリックしてサンプル JCL を表示します。

Unpackage.txt サンプル ジョブを使用して製品インストール ディレクトリを作成する方法

1. 有効な JOB ステートメントを指定します。
2. `yourUSSESDdirectory` を ESD ダウンロードに使用する USS ディレクトリの名前に置き換えます。

ジョブは指定した USS ディレクトリを参照します。

3. `paxfile.pax.Z` を pax ファイルの名前に置き換えます。

ジョブは指定した pax ファイルを参照します。

4. ジョブをサブミットします。

ジョブが実行され、製品ディレクトリが作成されます。

注: ジョブに指定されている変更を行った後で、`PARM=` ステートメントが 71 文字を超えている場合は、代わりに 2 番目の `UNPAXDIR` の形式をコメント解除して使用します。このサンプル ジョブでは、カラム 72 で X を使用し、2 行目に `PARM=` パラメータを続けます。

Pax コマンド (Unpackage.txt) を実行するジョブの例

添付されている Unpackage.txt JCL ファイルに以下のテキストが表示されます。

```
//ESDUNPAX JOB (ACCOUNTNO),'UNPAX ESD PACKAGE ',
// MSGCLASS=X,CLASS=A,NOTIFY=&SYSUID
//*****
/* This sample job can be used to invoke the pax command to create *
/* the product-specific installation directory. *
/* *
/* This job must be customized as follows: *
/* 1. Supply a valid JOB statement. *
/* 2. Replace "yourUSSESDdirectory" with the name of the USS *
/* directory used on your system for ESD downloads. *
/* 3. Replace "paxfile.pax.Z" with the name of the pax file. *
/* NOTE: If you continue the PARM= statement on a second line, make *
/* sure the 'X' continuation character is in column 72. *
//*****
//UNPAXDIR EXEC PGM=BPXBATCH,
// PARM='sh cd /yourUSSESDdirectory/; pax -rvf paxfile.pax.Z'
/*UNPAXDIR EXEC PGM=BPXBATCH,
/* PARM='sh cd /yourUSSESDdirectory/; pax X
/* -rvf paxfile.pax.Z'
//STDOUT DD SYSOUT=*
//STDERR DD SYSOUT=*
```

z/OS データ セットへのインストール ファイルのコピー

SMP/E GIMUNZIP ユーティリティを呼び出して、製品固有のディレクトリから MVS データ セットを作成するには、この手順を使用します。

Pax-Enhanced ESD インストール ファイルを z/OS データ セットにコピーする方法

1. 必要に応じて、製品の `readme` ファイルまたはインストールの注意事項を探して参照します。これらのファイルは、`pax` コマンドで作成した製品固有のディレクトリにあります。このファイルには、インストール手順を完了するために必要な、製品固有の詳細情報が含まれています。

ここで製品固有のインストールの詳細が特定されました。

2. `UNZIPJCL` サンプル ジョブを編集するには、`ISPF EDIT` または `TSO ISHELL` を使用します。以下のいずれかの方法で、この手順を実行できます。
 - `ISPF EDIT` を使用します。`UNZIPJCL` ファイルの完全パス名を指定します。
 - `TSO ISHELL` を使用します。`UNZIPJCL` ファイルに移動し、`E` 行コマンドを使用してファイルを編集します。

ジョブが編集されます。

3. `SMPDIR DD PATH` を `pax` コマンドによって作成された製品固有ディレクトリに変更します。

製品固有ディレクトリが表示されます。

4. `ICSF` がアクティブでない場合は、以下の手順を実行します。
 - a. `SMPJHOME DD PATH` をユーザの `Java` ランタイム ディレクトリに変更します。このディレクトリはシステムによって異なります。
 - b. 以下の手順のいずれかを実行します。
 - `SMPCPATH DD PATH` をユーザの `SMP/E Java` アプリケーションクラス ディレクトリに変更します。通常は、`/usr/lpp/smp/classes/` です。
 - `GIMUNZIP` パラメータの `HASH=YES` を `HASH=NO` に変更します。

次のいずれかが発生します：`ICSF` はアクティブです。`Java` を使用していません。

5. すべての *YourHLQ* の表示をインストール処理によって使用される z/OS データセットの高レベル修飾子に変更します。パッケージを一意に識別するために、展開された各 *pax* ファイルに固有の HLQ を使用することをお勧めします。SMP/E RELFILE に使用するので、*yourHLQ* に同じ値を使用しないでください。

YourHLQ の表示はすべて z/OS データセットのユーザの高レベル修飾子に設定されます。

6. UNZIPJCL ジョブをサブミットします。

UNZIPJCL ジョブは、リターンコード 0 で完了する必要があります。出力メッセージの GIM69158I および GIM48101I、JES ログにある IKJ56228I は無視して構いません。

GIMUNZIP は、UNZIPJCL ジョブで指定した高レベル修飾子を使用して z/OS データセットを作成します。製品のインストールを実行するには、これらのデータセットを使用します。ここでは、*pax* ファイルおよび製品固有ディレクトリは必要なくなりました。

注: 詳細については、IBM の「*SMP/E for z/OS Reference (SA22-7772)*」マニュアルを参照してください。

ネイティブ SMP/E JCL を使用したインストール方法

以下の手順では、ネイティブ SMP/E JCL を使用した製品のインストールプロセスについて説明します。

1. 製品データセットおよび SMP/E データセットを割り当てます。
2. SMP/E CSI を作成します。
3. 基本機能を RECEIVE します。
4. 基本機能を APPLY します。
5. 基本機能を ACCEPT します。
6. サイトの要件に応じて製品を設定します。

Pax インストールのための SMP/E 環境の準備

このプロシージャで使用されるメンバは、CA OPS/MVS のデータ セットの準備、ゾーンの初期化、DDDEF の作成を行います。

このプロシージャを開始する前に、CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) をインストールするかどうかを決定します。

注: CA OPS/MVS OPSLOG WebView には、個別のユーザ ライセンス契約が必要です。

メンバの詳細については、JCL 内のコメントを参照してください。

以下の手順に従います。

1. サイト固有の情報を使用してマクロ CLXSEEDIT をカスタマイズし、そのマクロを SYSPROC がある場所にコピーします。各 ISREDIT CHANGE コマンドの一番右側のパラメータを置き換えます。インストール メンバを編集するたびに、コマンド行で「CLXSEEDIT」と入力し、Enter キーを押して、デフォルトのメンバをユーザ指定のメンバに置換します。

yourHLQ.SAMPJCL メンバをカスタマイズするためのマクロの準備ができました。

注: DASD ESD JCL を解凍するには、DASD HLQ を *yourHLQ* に対して指定した値と同じに設定します。

注: 以下の手順には、新しい SAMPJCL メンバを開くたびに CLXSEEDIT マクロを実行する手順が含まれます。すべての SAMPJCL メンバを同時に編集するには、CLXEDALL メンバの手順を読み、それに従ってください。

2. 編集セッションで SAMPJCL メンバ CLX1ALL を開き、コマンドラインから CLXSEEDIT マクロを実行します。

CLX1ALL がカスタマイズされます。

3. CLX1ALL をサブミットします。

このジョブにより以下のような結果となります。

- CA OPS/MVS 用のターゲット データ セットと配布データ セットが作成されます。
 - このターゲットゾーンに固有の SMPLTS、SMPMTS、SMPSCDS および SMPSTS データ セットが作成されます。
4. CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) のインストールを選択した場合は、以下のサブ手順を完了します。

- a. 編集セッションで SAMPJCL メンバ CL11ALLU を開き、コマンドラインから CLXSEEDIT マクロを実行します。
メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。
CL11ALLU がカスタマイズされます。
 - b. CL11ALLU をサブミットします。
このジョブは HFS データ セットを割り当てます。
 - c. 編集セッションで SAMPJCL メンバ CL12MKD を開き、コマンドラインから CLXSEEDIT マクロを実行します。
メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。
CL12MKD がカスタマイズされます。
 - d. CL12MKD をサブミットします。
このジョブはすべてのディレクトリを作成し、ファイルシステムをマウントします。
5. 編集セッションで SAMPJCL メンバ CL13CSIU を開き、コマンドラインから CLXSEEDIT マクロを実行します。
CL13CSIU がカスタマイズされます。
 6. CL13CSIU をサブミットします。
このジョブにより以下のような結果となります。
 - CSI のデータセットが定義されます。
 - SMPPTS データセットと SMPLOG データセットが割り当てられます。
 - グローバルゾーン、ターゲットゾーン、および配布ゾーンが初期化されます。
 - ユーザの製品用の DDDEF エントリが作成されます。
 - 必須 SMP/E データセットの DDDEF が作成されます。
 7. CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) のインストールを選択した場合は、以下のサブ手順を完了します。
 - a. 編集セッションで SAMPJCL メンバ CL13CSIU を開き、コマンドラインから CLXSEEDIT マクロを実行します。
メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。

CL13CSIU がカスタマイズされます。

- b. CL13CSIU をサブミットします。

このジョブは、ディレクトリに関連付けられた DDDEF を追加して、CSI をカスタマイズします。

Pax インストール用のインストール ジョブの実行

これらの SAMPJCL メンバを順番にサブミットして実行します。前のジョブが正常に完了するまで、次のジョブに進まないでください。

以下の手順に従います。

1. 編集セッションで SAMPJCL メンバ CLX3RECD を開き、コマンド行から CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX3RECD がカスタマイズされます。

2. *yourHLQ.SAMPJCL* メンバ CLX3RECD をサブミットして、SMP/E 基本機能を RECEIVE します。

CA OPS/MVS が RECEIVE され、グローバルゾーンに配置されます。

3. 編集セッションで SAMPJCL メンバ CLX4APP を開き、コマンド行から CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX4APP がカスタマイズされます。

4. *yourHLQ.SAMPJCL* メンバ CLX4APP をサブミットして、SMP/E 基本機能を APPLY します。

CA OPS/MVS が APPLY され、ターゲットライブラリに配置されます。

5. 編集セッションで SAMPJCL メンバ CLX5ACC を開き、コマンド行から CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX5ACC がカスタマイズされます。

6. *yourHLQ.SAMPJCL* メンバ CLX5ACC をサブミットして、SMP/E 基本機能を ACCEPT します。

CA OPS/MVS が ACCEPT され、配布ライブラリに配置されます。

USS ディレクトリのクリーン アップ

重要: この手順はオプションです。インストール処理がすべて完了するまで、この手順は使用しないでください。

CA Technologies 製品の **pax** ファイルのダウンロードおよび処理の実行後、今後のダウンロードのためにファイル システムのディスク領域を解放するには、USS ディレクトリからファイルを削除し、不要な **MVS** データ セットを削除することをお勧めします。以下の項目を削除できます。

- Pax ファイル
- **pax** コマンドによって作成された製品固有のディレクトリおよびそのディレクトリに含まれるすべてのファイル
- SMP/E RELFILE、SMPMCS、HOLDDATA MVS データセット

これらのデータ セットには **UNZIPJCL** ジョブに割り当てた **HLQ** があります。

注: 今後の参照用に、*yourHLQ.INSTALL.NOTES* など、SMP/E 以外のインストール データ セットは保持してください。

以下の手順に従います。

1. Pax-Enhanced ESD USS ディレクトリに移動します。
適用可能な USS ディレクトリが表示されます。
2. 以下のコマンドを入力して、**pax** ファイルを削除します。

```
rm paxfile
```

```
paxfile
```

ダウンロードした CA Technologies **pax** ファイルの名前を指定します。

pax ファイルが削除されます。

3. 以下のコマンドを入力して、製品固有のディレクトリを削除します。

```
rm -r product-specific-directory
```

```
product-specific-directory
```

pax コマンドによって作成された製品固有のディレクトリを指定します。

製品固有のディレクトリが削除されます。

注: TSO ISHELL を使用して **pax** ファイルおよび製品固有のディレクトリに移動し、D 行コマンドを使用して、それらを削除することもできます。

メンテナンスの適用

CA Support Online には、インストール データの作成後に公開されたメンテナンスおよび HOLDDATA があります。メンテナンスプロセスが完了した製品は、いつでも展開できます。

以下の手順に従います。

1. CA Support Online を確認し、このリリースが作成された後に発行された PTF と HOLDDATA をダウンロードします。ベースリリースが作成されたのが最近の場合、PTF または HOLDDATA はまだ発行されていません。
2. ダウンロードしたファイルを 2 つの個別の FB 80 順次データセットに転送します。1 つのデータセットを PTF を保持するために使用し、もう 1 つのデータセットを HOLDDATA を保持するために使用します。

PTF および HOLDDATA が *yourHLQ.SAMPJCL* メンテナンスメンバからアクセス可能になります。

3. CLXSEDI マクロは、インストール手順でカスタマイズされています。ベースインストールからの値がまだ存在することを確認します。
4. 編集セッションで SAMPJCL メンバ CLX6RECP を開き、コマンドラインから CLXSEDI マクロを実行します。

CLX6RECP は、JOB ステートメント、CSI の場所、およびゾーン名を使用してカスタマイズされます。

5. PTF および HOLDDATA の FB 80 データセットを参照するように、CLX6RECP SMPPTFIN および SMPHOLD DD ステートメントをカスタマイズします。
6. CLX6RECP をサブミットします。

PTF と HOLDDATA が RECEIVE されます。

7. 編集セッションで SAMPJCL メンバ CLX7APYP を開き、コマンドラインから CLXSEDI マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX7APYP がカスタマイズされます。

8. CLX7APYP をサブミットします。

PTF が APPLY されます。

9. (オプション) 編集セッションで SAMPJCL メンバ CLX8ACCP を開き、コマンドラインから CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX8ACCP がカスタマイズされます。

10. (オプション) *yourHLQ.SAMPJCL* メンバ CLX8ACCP をサブミットします。

PTF が ACCEPT されます。

注: この時点でジョブをサブミットする必要はありません。サイトのポリシーに従って、PTF を ACCEPT できます。

HOLDDATA

メンテナンスを適用するとき、通常 SMP/E HOLDDATA を使用します。エラーまたは特殊な条件の SYSMOD の SMP/E システムを通知するために HOLDDATA を使用します。以下の 2 種類の HOLDDATA をサポートされています。

システム HOLDDATA

特別な条件をユーザに知らせる SYSMOD のインストリーム部分にあるデータであることを示します。システムの HOLDDATA の例を以下に示します。

ACTION

この SYSMOD を適用する前または後に、特別な処理を実行する必要があることを示します。

DEP

外部的に確認する必要があるこの SYSMOD の依存関係を示します。

DELETE

SYSMOD のロード モジュールを削除します。SMP/E RESTORE コマンドを使用して、この種類の SYSMOD を元に戻すことはできません。

DOC

この SYSMOD を使用したドキュメントの変更を示します。

EC

この SYSMOD には、ハードウェア エンジニアリングの変更が必要であることを示します。EC がハードウェア デバイスに存在しない場合、通常、EC 保留 SYSMOD は製品に影響しません。

内部に保留のある SYSMOD をインストールするには、APPLY コマンド上でバイパス オペランドを設定します。必要なアクションを実行した後、または APPLY 後にアクションを実行している場合で、それが適切な場合のみ、バイパス オペランドを設定できます。

外部 HOLDDATA

外部 HOLDDATA は PTF に含まれていません。これは、別のファイルに存在します。一般的には、すでに配布済みで、問題を引き起こすことが後で判明した SYSMOD に使用されます。

CA Support Online から DASD ファイルに外部 HOLDDATA をダウンロードし、SMPHOLD DD ステートメントにファイルを割り当てます。外部 HOLDDATA を利用するには、SMP/E 環境で受信します。CA によって提供されたジョブを使用する場合、SMP/E は HOLDDATA を受信します。

SYSMOD に未解決の保留エラーがあると、ユーザがバイパスを APPLY コマンドに追加しない場合、SMP/E はそれをインストールしません。ユーザに該当しない状況でのエラー保留はバイパスできます。ユーザに該当しないエラー保留には、保有していないハードウェア デバイス、または使用していない製品機能のみで発生した問題が含まれている可能性があります。

保留を解決する SYSMOD を発行すると、SYSMOD の解決は保留エラーに優先されます。このアクションでは、修正する SYSMOD と共に元の SYSMOD を適用することができます。

ERREL と呼ばれる特別な HOLDDATA クラスが存在します。SYSMOD によって修正される問題は、それが引き起こす問題よりも重要であると決定しました。これらの SYSMOD を適用することをお勧めします。

確実に外部 HOLDDATA データを管理するには、SMP/E によって自動的に管理することを許可します。唯一の手動タスクは REPORT ERRSYSMODS を実行しています。このレポートでは、ユーザのシステムに適用されている保留 SYSMODS を特定します。受信ステータスにある SYSMOD を解決する場合、状況を修正するために適用する SYSMOD を特定します。

システム HOLDDATA

システム HOLDDATA は、SYSMOD のインストリーム部分のデータを示し、ユーザに特別な状態を通知します。CA OPS/MVS では、システム HOLDDATA で以下の理由が使用されます。

ACTION

この SYSMOD を適用する前または後に、特別な処理を実行する必要があることを示します。

AO

自動操作に影響します。メッセージ識別子またはメッセージの内部のフィールドの変位のいずれかを変更します。

DDDEF

データセットと DDDEF が追加されているか変更されることを示します。

DELETE

SYSMOD のロード モジュールを削除します。SMP/E RESTORE コマンドを使用して、この種類の SYSMOD を元に戻すことはできません。

DEP

外部的に確認する必要があるこの SYSMOD の依存関係を示します。

DOC

この SYSMOD を使用したドキュメントの変更を示します。

DYNACT

IPL を実行せずに、この修正を動的にアクティブ化する手順を説明します。

EC

この SYSMOD には、ハードウェア エンジニアリングの変更が必要であることを示します。EC がハードウェア デバイスに存在しない限り、通常、EC 保留 SYSMOD は製品に影響しません。

ENH

小規模のプログラミング拡張機能が提供されます。その HOLD ステートメントには、拡張機能を実装するための手順が含まれます。拡張機能の実装に必要なアクションがない場合は、拡張機能の要約を提供します。

EXIT

この SYSMOD によって提供された変更が、ユーザ EXIT の再アセンブルを必要としていることを示します。

EXRF

アクティブかつ代替状態にある拡張リカバリ機能に SYSMOD をインストールする必要があることを示します。

IPL

この SYSMOD を有効化するには IPL が必要であることを示します。動的なアクティブ化の選択肢がないときに限り、使用されます。

MSGSKEL

SYSMOD には国際化メッセージバージョンが含まれており、各言語でメッセージコンパイラで実行する必要があることを示します。

MULTSYS

前提条件、共存、または活用のいずれかの場合に、複数のシステムにこの **SYSMOD** を適用します。

RESTART

この **SYSMOD** を適用した後、ルーチン再起動ではなく特別な再起動をサイトで実行する必要があることを示します。

SQLBIND

DB2 以外のデータベースシステムにはバインドが必要であることを示します。

SYSMOD

この **SYSMOD** によって提供される要素の一部またはすべてが、ワークステーションにダウンロードされることを示します。

内部に保留のある **SYSMOD** をインストールするには、**APPLY** コマンド上でバイパスオペランドを設定します。バイパスオペランドを設定するのは、必要なアクションを実行した後、または **APPLY** の後にアクションを実行している場合で、それが適切な場合のみです。

外部 HOLDDATA

外部 **HOLDDATA** データは **PTF** に含まれていません。これは、別のファイルに存在します。一般的には、すでに配布済みで、問題を引き起こすことが後で判明した **SYSMOD** に使用されます。

CA サポートから **DASD** ファイルに外部 **HOLDDATA** データをダウンロードし、**SMPHOLD DD** ステートメントにそのファイルを割り当てます。外部 **HOLDDATA** データを利用するには、**SMP/E** 環境に **RECEIVE** します。**SMP/E** は **CA** に提供されたジョブから **HOLDDATA** を **RECEIVE** します。

SYSMOD に未解決の保留エラーがあると、ユーザがバイパスを **APPLY** コマンドに追加しない場合、**SMP/E** はそれをインストールしません。ユーザに該当しない状況でのエラー保留はバイパスできます。ユーザに該当しないエラー保留には、保有していないハードウェア デバイス、または使用していない製品機能のみで発生した問題が含まれている可能性があります。

保留を解決する **SYSMOD** を **CA** が発行すると、**SYSMOD** の解決が保留エラーより優先されます。このアクションでは、修正する **SYSMOD** と共に元の **SYSMOD** を **APPLY** することができます。

ERRELと呼ばれる特別な HOLDDATA データクラスが存在します。SYSMOD によって修正される問題は、それが引き起こす問題よりも重要であると判断しました。これらの SYSMOD を APPLY することをお勧めします。

唯一の手動タスクは REPORT ERRSYSMODS を実行しています。このレポートは、以下の項目を識別します。

- ユーザのシステムに APPLY されている保留中の SYSMOD。
- RECEIVE ステータスにある解決する SYSMOD。

SMP/E は SYSMOD を識別し、状況を修正するために APPLY します。

第 5 章: テープからの製品のインストール

このセクションには、以下のトピックが含まれています。

[テープからのサンプル JCL のアンロード](#) (P. 74)

[ネイティブ SMP/E JCL を使用したインストール方法](#) (P. 75)

[メンテナンスの APPLY](#) (P. 79)

テープからのサンプル JCL のアンロード

製品をインストールするためのサンプル JCL は、配布テープの CAI.SAMPJCL ライブラリにあります。

サンプル JCL をテープからアンロードする方法

1. 以下のサンプル JCL を実行します。

```
//COPY      EXEC PGM=IEBCOPY,REGION=4096K
//SYSPRINT DD  SYSOUT=*
//SYSUT1    DD  DSN=CAI.SAMPJCL,DISP=OLD,UNIT=unitname,VOL=SER=nnnnnn,
//          LABEL=(1,SL)
//SYSUT2    DD  DSN=yourhlq.SAMPJCL,
//          DISP=(,CATLG,DELETE),
//          UNIT=sysda,SPACE=(TRK,(15,3,6),RLSE)
//SYSUT3    DD  UNIT=SYSDA,SPACE=(CYL,1)
//SYSIN     DD  DUMMY
```

unitname

テープをマウントするためのテープユニットを指定します。

nnnnnn

テープ ボリューム シリアル番号を指定します。

yourhlq

インストール用のデータセットプレフィックスを指定します。

sysda

インストール ソフトウェアを配置する DASD を指定します。

SAMPJCL データセットが作成され、その内容がテープからダウンロードされます。

2. 継続するには、以下のいずれかのオプションを選択します。
 - すでに SMP/E 環境が設定されている場合は、「テープ インストール用のインストールジョブの実行」に進みます。
 - SMP/E 環境が設定されていない場合は、「テープ インストール用の SMP/E 環境の準備」に進みます。

ネイティブ SMP/E JCL を使用したインストール方法

以下の手順では、ネイティブ SMP/E JCL を使用した製品のインストールプロセスについて説明します。

1. 製品データセットおよび SMP/E データセットを割り当てます。
2. SMP/E CSI を作成します。
3. 基本機能を RECEIVE します。
4. 基本機能を APPLY します。
5. 基本機能を ACCEPT します。
6. サイトの要件に応じて製品を設定します。

テープ インストール用の SMP/E 環境の準備

このプロシージャで使用されるメンバは、CA OPS/MVS のデータ セットの準備、ゾーンの初期化、DDDEF の作成を行います。

このプロシージャを開始する前に、CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) をインストールするかどうかを決定します。

注: CA OPS/MVS OPSLOG WebView には、個別のユーザ ライセンス契約が必要です。

メンバの詳細については、JCL 内のコメントを参照してください。

以下の手順に従います。

1. マクロ CLXSEEDIT をユーザ サイト固有の情報でカスタマイズし、そのマクロを SYSPROC がある場所にコピーします。各 ISREDIT CHANGE コマンドの一番右側のパラメータを置き換えます。インストール メンバを編集するたびに、TSO コマンド行で「CLXSEEDIT」と入力し、Enter キーを押して、デフォルト値をユーザ指定の値に置き換えます。

これで、ユーザの *yourHLQ.SAMPJCL* メンバをカスタマイズするマクロの準備ができました。

注: 以下の手順には、新しい SAMPJCL メンバを開くたびに CLXSEEDIT マクロを実行する手順が含まれています。すべての SAMPJCL メンバを同時に編集するには、CLXEDALL メンバ内の指示を参照し、これに従ってください。

2. 編集セッションで SAMPJCL メンバ CLX1ALL を開き、コマンドラインから CLXSEEDIT マクロを実行します。

CLX1ALL がカスタマイズされます。

3. CLX1ALL をサブミットします。

このジョブにより以下のような結果となります。

- CA OPS/MVS 用のターゲット データ セットと配布データ セットが作成されます。
- このターゲットゾーンに固有の SMPLTS、SMPMTS、SMPSCDS および SMPSTS データ セットが作成されます。

4. CA OPS/MVS OPSLOG WebView 機能 (FMID CCLXC01) のインストールを選択した場合は、以下のサブ手順を完了します。

- a. 編集セッションで SAMPJCL メンバ CL11ALLU を開き、コマンド行から CLXSEEDIT マクロを実行します。

メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。

CL11ALLU がカスタマイズされます。

- b. CL11ALLU をサブミットします。

このジョブは HFS データ セットを割り当てます。

- c. 編集セッションで SAMPJCL メンバ CL12MKD を開き、コマンドラインから CLXSEEDIT マクロを実行します。

メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。

CL12MKD がカスタマイズされます。

- d. CL12MKD をサブミットします。

このジョブはすべてのディレクトリを作成し、ファイル システムをマウントします。

5. 編集セッションで SAMPJCL メンバ CLX2CSI を開き、コマンド行から CLXSEEDIT マクロを実行します。

CLX2CSI がカスタマイズされます。

CLX2CSI をサブミットします。

このジョブにより以下のような結果となります。

- CSI のデータ セットが定義されます。
- SMPPTS データ セットと SMPLOG データ セットが割り当てられます。
- グローバルゾーン、ターゲットゾーン、および配布ゾーンが初期化されます。
- ユーザの製品用の DDDEF エントリが作成されます。
- 必須 SMP/E データ セットの DDDEF が作成されます。

6. CA OPS/MVS OPSLOG WebView 機能 (FMID CLXC01) のインストールを選択した場合は、以下のサブ手順を完了します。

- a. 編集セッションで SAMPJCL メンバ CL13CSIU を開き、コマンド行から CLXSEEDIT マクロを実行します。

メンバのコメントに記載されているように、JCL に対して追加の変更を加えます。

CL13CSIU がカスタマイズされます。

- b. CL13CSIU をサブミットします。

このジョブは、ディレクトリに関連付けられた DDDEF を追加して、CSI をカスタマイズします。

テープ インストール用のインストール ジョブの実行

これらの SAMPJCL メンバを順番にサブミットして実行します。前のジョブが正常に完了するまで、次のジョブに進まないでください。

以下の手順に従います。

1. 編集セッションで SAMPJCL メンバ CLX3RECT を開き、コマンド行から CLXSEEDIT マクロを実行します。
注: 不要な FMID があれば、削除します。
CLX3RECT がカスタマイズされます。
2. *yourHL.SAMPJCL* メンバ CLX3RECT をサブミットして、SMP/E 基本機能を RECEIVE します。
CA OPS/MVS が RECEIVE され、グローバルゾーンに配置されます。
3. 編集セッションで SAMPJCL メンバ CLX4APP を開き、コマンド行から CLXSEEDIT マクロを実行します。
注: 不要な FMID があれば、削除します。
CLX4APP がカスタマイズされます。
4. *yourHLQ.SAMPJCL* メンバ CLX4APP をサブミットして、SMP/E 基本機能を APPLY します。
CA OPS/MVS が APPLY され、ターゲットライブラリに配置されます。
5. 編集セッションで SAMPJCL メンバ CLX5ACC を開き、コマンド行から CLXSEEDIT マクロを実行します。
注: 不要な FMID があれば、削除します。
CLX5ACC がカスタマイズされます。
6. *yourHLQ.SAMPJCL* メンバ CLX5ACC をサブミットして、SMP/E 基本機能を ACCEPT します。
CA OPS/MVS が ACCEPT され、配布ライブラリに配置されます。

メンテナンスの適用

CA Support Online には、インストール データの作成後に公開されたメンテナンスおよび HOLDDATA があります。メンテナンスプロセスが完了した製品は、いつでも展開できます。

以下の手順に従います。

1. CA Support Online を確認し、このリリースが作成された後に発行された PTF と HOLDDATA をダウンロードします。ベースリリースが作成されたのが最近の場合、PTF または HOLDDATA はまだ発行されていません。

2. ダウンロードしたファイルを 2 つの個別の FB 80 順次データセットに転送します。1 つのデータセットを PTF を保持するために使用し、もう 1 つのデータセットを HOLDDATA を保持するために使用します。

PTF および HOLDDATA が *yourHLQ.SAMPJCL* メンテナンス メンバからアクセス可能になります。

3. CLXSEEDIT マクロは、インストール手順でカスタマイズされています。ベースインストールからの値がまだ存在することを確認します。

4. 編集セッションで SAMPJCL メンバ CLX6RECP を開き、コマンド行から CLXSEEDIT マクロを実行します。

CLX6RECP は、JOB ステートメント、CSI の場所、およびゾーン名を使用してカスタマイズされます。

5. FB 80 データセットで PTF および HOLDDATA を参照するように、CLX6RECP SMPPTFIN および SMPHOLD DD ステートメントをカスタマイズします。

6. CLX6RECP をサブミットします。

PTF と HOLDDATA が RECEIVE されます。

7. 編集セッションで SAMPJCL メンバ CLX7APYP を開き、コマンド行から CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX7APYP がカスタマイズされます。

8. CLX7APYP をサブミットします。

PTF が APPLY されます。

9. (オプション) 編集セッションで SAMPJCL メンバ CLX8ACCP を開き、コマンド行から CLXSEEDIT マクロを実行します。

注: 不要な FMID があれば、削除します。

CLX8ACCP がカスタマイズされます。

10. (オプション) *yourHLQ.SAMPJCL* メンバ CLX8ACCP をサブミットします。

PTF が ACCEPT されます。

注: この時点でジョブをサブミットする必要はありません。サイトのポリシーに従って、PTF を ACCEPT できます。

HOLDDATA

メンテナンスを **APPLY** するとき、通常 **SMP/E HOLDDATA** を使用します。エラーまたは特殊な条件の **SYSMOD** の **SMP/E** システムを通知するために **HOLDDATA** を使用します。以下の 2 種類の **HOLDDATA** をサポートされています。

システム HOLDDATA

特別な条件をユーザに知らせる **SYSMOD** のインストリーム部分にあるデータであることを示します。システムの **HOLDDATA** の例を以下に示します。

ACTION

この **SYSMOD** を **APPLY** する前または後に、特別な処理を実行する必要があることを示します。

DEP

外部的に確認する必要があるこの **SYSMOD** の依存関係を示します。

DELETE

SYSMOD のロード モジュールを削除します。 **SMP/E RESTORE** コマンドを使用して、この種類の **SYSMOD** を元に戻すことはできません。

DOC

この **SYSMOD** を使用したドキュメントの変更を示します。

EC

この **SYSMOD** には、ハードウェア エンジニアリングの変更が必要であることを示します。 **EC** がハードウェア デバイスに存在しない場合、通常、 **EC** 保留 **SYSMOD** は製品に影響しません。

内部に保留のある **SYSMOD** をインストールするには、 **APPLY** コマンド上でバイパスオペランドを設定します。必要なアクションを実行した後、または **APPLY** 後にアクションを実行している場合で、それが適切な場合のみ、バイパスオペランドを設定できます。

外部 HOLDDATA

外部 HOLDDATA は PTF に含まれていません。これは、別のファイルに存在します。一般的には、すでに配布済みで、問題を引き起こすことが後で判明した SYSMOD に使用されます。

CA Support Online から DASD ファイルに外部 HOLDDATA をダウンロードし、SMPHOLD DD ステートメントにファイルを割り当てます。外部 HOLDDATA を利用するには、SMP/E 環境で RECEIVE します。CA によって提供されたジョブを使用する場合、SMP/E は HOLDDATA を RECEIVE します。

SYSMOD に未解決の保留エラーがあると、ユーザがバイパスを APPLY コマンドに追加しない場合、SMP/E はそれをインストールしません。ユーザに該当しない状況でのエラー保留はバイパスできます。ユーザに該当しないエラー保留には、保有していないハードウェア デバイス、または使用していない製品機能のみで発生した問題が含まれている可能性があります。

保留を解決する SYSMOD を発行すると、SYSMOD の解決は保留エラーに優先されます。このアクションでは、修正する SYSMOD と共に元の SYSMOD を APPLY することができます。

ERREL と呼ばれる特別な HOLDDATA クラスが存在します。SYSMOD によって修正される問題は、それが引き起こす問題よりも重要であると判断しました。これらの SYSMOD を APPLY することをお勧めします。

確実に外部 HOLDDATA データを管理するには、SMP/E によって自動的に管理することを許可します。唯一の手動タスクは REPORT ERRSYSMODS を実行しています。このレポートでは、ユーザのシステムに APPLY されている保留 SYSMODS を特定します。RECEIVE ステータスにある SYSMOD を解決する場合、状況を修正するために APPLY する SYSMOD を特定します。

システム HOLDDATA

システム HOLDDATA は、SYSMOD のインストリーム部分のデータを示し、ユーザに特別な状態を通知します。CA OPS/MVS では、システム HOLDDATA で以下の理由が使用されます。

ACTION

この SYSMOD を APPLY する前または後に、特別な処理を実行する必要があることを示します。

AO

自動操作に影響します。メッセージ識別子またはメッセージの内部のフィールドの変位のいずれかを変更します。

DDDEF

データセットと DDDEF が追加されているか変更されることを示します。

DELETE

SYSMOD のロード モジュールを削除します。SMP/E RESTORE コマンドを使用して、この種類の SYSMOD を元に戻すことはできません。

DEP

外部的に確認する必要があるこの SYSMOD の依存関係を示します。

DOC

この SYSMOD を使用したドキュメントの変更を示します。

DYNACT

IPL を実行せずに、この修正を動的にアクティブ化する手順を説明します。

EC

この SYSMOD には、ハードウェア エンジニアリングの変更が必要であることを示します。EC がハードウェア デバイスに存在しない限り、通常、EC 保留 SYSMOD は製品に影響しません。

ENH

小規模のプログラミング拡張機能が提供されます。その HOLD ステートメントには、拡張機能を実装するための手順が含まれます。拡張機能の実装に必要なアクションがない場合は、拡張機能の要約を提供します。

EXIT

この SYSMOD によって提供された変更が、ユーザ EXIT の再アセンブルを必要としていることを示します。

EXRF

アクティブかつ代替状態にある拡張リカバリ機能に SYSMOD をインストールする必要があることを示します。

IPL

この SYSMOD を有効化するには IPL が必要であることを示します。動的なアクティブ化の選択肢がないときに限り、使用されます。

MSGSKEL

SYSMOD には国際化メッセージバージョンが含まれており、各言語でメッセージコンパイラで実行する必要があることを示します。

MULTSYS

前提条件、共存、または活用のいずれかの場合に、複数のシステムにこの SYSMOD を APPLY します。

RESTART

この SYSMOD を APPLY した後、ルーチン再起動ではなく特別な再起動をサイトで実行する必要があることを示します。

SQLBIND

DB2 以外のデータベースシステムにはバインドが必要であることを示します。

SYSMOD

この SYSMOD によって提供される要素の一部またはすべてが、ワークステーションにダウンロードされることを示します。

内部に保留のある SYSMOD をインストールするには、APPLY コマンド上でバイパスオペランドを設定します。バイパスオペランドを設定するのは、必要なアクションを実行した後、または APPLY の後にアクションを実行している場合で、それが適切な場合のみです。

外部 HOLDDATA

外部 HOLDDATA データは PTF に含まれていません。これは、別のファイルに存在します。一般的には、すでに配布済みで、問題を引き起こすことが後で判明した SYSMOD に使用されます。

CA サポートから DASD ファイルに外部 HOLDDATA データをダウンロードし、SMPHOLD DD ステートメントにそのファイルを割り当てます。外部 HOLDDATA データを利用するには、SMP/E 環境に RECEIVE します。SMP/E は CA に提供されたジョブから HOLDDATA を RECEIVE します。

SYSMOD に未解決の保留エラーがあると、ユーザがバイパスを APPLY コマンドに追加しない場合、SMP/E はそれをインストールしません。ユーザに該当しない状況でのエラー保留はバイパスできます。ユーザに該当しないエラー保留には、保有していないハードウェア デバイス、または使用していない製品機能のみで発生した問題が含まれている可能性があります。

保留を解決する SYSMOD を CA が発行すると、SYSMOD の解決が保留エラーより優先されます。このアクションでは、修正する SYSMOD と共に元の SYSMOD を APPLY することができます。

ERRELと呼ばれる特別な HOLDDATA データクラスが存在します。SYSMOD によって修正される問題は、それが引き起こす問題よりも重要であると判断しました。これらの SYSMOD を APPLY することをお勧めします。

唯一の手動タスクは REPORT ERRSYSMODS を実行しています。このレポートは、以下の項目を識別します。

- ユーザのシステムに APPLY されている保留中の SYSMOD。
- RECEIVE ステータスにある解決する SYSMOD。

SMP/E は SYSMOD を識別し、状況を修正するために APPLY します。

第 6 章：製品の開始準備

この章では、CA OPS/MVS の開始および使用前に必要なタスク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。

[概要 \(P. 88\)](#)

[展開を準備する方法 \(P. 88\)](#)

[SMP/E でインストールされたターゲット データ セットの識別 \(P. 89\)](#)

[製品の展開 \(P. 90\)](#)

[製品の設定 \(P. 91\)](#)

[CA MSM を使用して設定を完了する方法 \(P. 91\)](#)

[CA MSM なしで設定する方法 \(P. 97\)](#)

[起動 JCL PROC のカスタマイズ \(P. 97\)](#)

[起動 JCL のカスタマイズ \(P. 98\)](#)

[起動プロシージャのカスタマイズ \(P. 100\)](#)

[OPSLOG およびチェックポイント VSAM 線形データ セットの定義 \(P. 106\)](#)

[インストールの確認 \(P. 109\)](#)

[必要な手動設定 \(P. 110\)](#)

[ロードライブラリへの APF 権限の付与 \(P. 111\)](#)

[ライセンスキーの CA Common Services PPOPTION データ セットへの配置 \(P. 112\)](#)

[製品ライセンスの設定 \(P. 112\)](#)

[データ セットへのアクセスの付与 \(P. 116\)](#)

[ベースコンポーネントの設定タスク \(P. 117\)](#)

[ベースコンポーネント用のオプション インストール タスク \(P. 132\)](#)

[システム準備タスクの概要 \(P. 137\)](#)

[インストール後の考慮事項 \(P. 139\)](#)

[パラメータライブラリ メンバのカスタマイズ \(P. 140\)](#)

[OPSVIEW 機能を TSO で使用できるようにする \(P. 141\)](#)

[製品の起動 \(P. 143\)](#)

この章では、ベースコンポーネントを開始できるように CA OPS/MVS を準備する手順について説明します。

注: オプションの CA OPS/MVS コンポーネントの設定については、「[オプション コンポーネントの設定およびインストール \(P. 147\)](#)」を参照してください。

概要

CA MSM を使用して、CA OPS/MVS をインストール、展開、および設定できます。

インストール

詳細については、「[CA MSM を使用した CA-OPS/MVS のインストール \(P. 35\)](#)」を参照してください。

展開

詳細については、「[製品の展開方法 \(P. 39\)](#)」を参照してください。

設定

CA MSM には、製品ソフトウェアの設定機能があります。この機能を利用して、CA OPS/MVS の必要な設定とカスタマイズの手順の一部は、CA MSM 内で実行します。現時点では、すべての設定とカスタマイズを実行する機能が CA MSM に実装されているわけではありません。手動で実行する必要がある手順については、「[必要な手動設定 \(P. 110\)](#)」を参照してください。オプションの設定とカスタマイズについては、「[オプションコンポーネントの設定およびインストール \(P. 147\)](#)」を参照してください。

展開を準備する方法

このセクションでは、展開プロセスを開始する前に実行する必要がある手動タスクについて説明します。

IBM APAR の適用(オプション)

CA テクニカル サポートは、適用されていない場合に CA OPS/MVS の動作またはパフォーマンスに影響を及ぼす可能性のある複数の IBM APAR を特定しています。私たちは、IBM APAR の最新のリストを確認し、ご利用の環境にとって適切なものだけを適用することをお勧めしています。

IBM APAR の最新のリストについては、付録「CA OPS/MVS に影響を及ぼす IBM APARS」または「」を参照してください。[CA サポート](#)にお問い合わせください。

注: この手順はオプションですが、実施することを推奨しています。

SMP/E でインストールされたターゲット データ セットの識別

以下の表は、インストール中に作成される SMP/E のターゲット データ セットのリストを示しています。SMP/E は CA OPS/MVS のベース製品およびメンテナンスをこれらのデータセットへインストールします。データセット名に 'CAI' 以外の高レベル修飾子を使用するように、インストールをカスタマイズしても構いません。低レベル修飾子を変更する必要はありません。

CA OPS/MVS の設定および実行に、これらのデータセットのランタイム コピーを展開します。

DS 名	SMPE のエレメントタイプ	内容
CAI.CCLXASM	++MAC	アセンブラ ソースおよびマクロ
CAI.CCLXCLS0	++CLIST	TSO CLISTS
CAI.CCLXCNTL	++SAMPENU	たとえば、サンプル JCL PROC、REXX、データおよびスクリプト。
CAI.CCLXEXEC	++EXEC	OPS/REXX (未コンパイル)
CAI.CCLXHFS.ZFS		マウントされた zFS
/usr/lpp/CAI/CCLXHFS	++HFS ++SHELLSCR	zFS のマウントポイントには、以下が含まれています。 OPSLOG WebView USS のコンポーネント
CAI.CCLXLOAD	++MOD	実行可能ロード ライブラリ (PDS である場合があります。)
CAI.CCLXMENU	++MSGENU	ISPF メッセージ
CAI.CCLXMIB	++DATA	SNMP MIB
CAI.CCLXOPEX	++USER5	OPS/REXX (コンパイル済み)
CAI.CCLXPENU	++PNLENU	ISPF パネル
CAI.CCLXPLD	++MOD	実行可能ロード ライブラリ (PDS/E である必要があります)
CAI.CCLXRULB	++USER3	BASE AOF ルール
CAI.CCLXRULM	++USER3	STATEMAN AOF ルール
CAI.CCLXRULS	++USER3	SAMPLE AOF ルール

DS 名	SMPE のエレメントタイプ	内容
CAI.CCLXSAMP	++SAMP	サンプル REXX
CAI.CCLXSENU	++SKLENU	ISPF のスケルトン
CAI.CCLXSIDE	++UTIN	LE サイドデッキ ファイル
CAI.CCLXTENU	++TBLENU	ISPF テーブル
CAI.CCLXXML	++PRODXML	MSM/SDS および MSM/SCS XML メタデータ

製品の展開

CA MSM による展開の完了方法

このセクションのトピックでは、[CA MSM を使用して製品を設定するとき \(P. 39\)](#)、実行する手動タスクについて説明します。

CA MSM を使用すると、CA OPS/MVS の SMP/E インストールしたすべてのターゲットライブラリのランタイムコピーを、サイトの個々のシステムまたはすべてのシステムに展開できます。

CAMSM を使用して、CA OPS/MVS チェックポイントファイルをカスタム データセットとして展開することもできます。

詳細については、「[製品の展開方法 \(P. 39\)](#)」を参照してください。

CA MSM を使用せずに展開する方法

このセクションのトピックでは、CA MSM を使用して製品を設定しないとき、実行する手動タスクについて説明します。

ISPF または バッチ JCL のいずれかを使用して、CA OPS/MVS の SMP/E でインストールされたターゲットライブラリのすべてのランタイムコピーを、ユーザサイトの 1 つまたはすべてのシステムに展開します。ただし、製品を起動する前に、「[CA MSM を使用せずに設定する方法 \(P. 90\)](#)」で説明されている手順を実行する必要があります。

重要: CA OPS/MVS の SMP/E でインストールされたターゲットライブラリを直接編集しないでください。CA OPS/MVS を CA OPS/MVS の SMP/E でインストールされたターゲットライブラリから直接実行しないでください。編集および実行するには、CA OPS/MVS の SMP/E でインストールされたターゲットライブラリのランタイムコピーを展開する必要があります。

製品の設定

このセクションのトピックでは、CA MSM を使用して、または手動で、設定している場合に実行する手動タスクについて説明します。

CA MSM を使用して設定を完了する方法

このセクションのトピックでは、[CA MSM を使用して製品を設定する \(P. 40\)](#)際に、実行する手動タスクについて説明します。

CA MSM を使用して設定を開始する方法

CA OPS/MVS の使用可能なコピーを設定するために CA MSM を使用できます。ただし、現時点では、CA OPS/MVS をカスタマイズできるすべてのパラメータが CA MSM に統合されているわけではありません。したがって、ここでは CA MSM を使用する設定を開始する方法についてのみ説明します。提供される OPSSXP00 パラメータファイルを使用したカスタマイズがさらに必要になる場合があります。OPSSPA00 で動作すると説明されているパラメータはどれも、ファイル OPSSXP00 でもまったく同じ動作を行います。

重要: 現時点で CA MSM を使用して設定することを選択する場合、CA MSM でサポートされていないパラメータをカスタマイズする必要があります。それらのパラメータは、メンバ OPSSXP00 ではなく、OPSSPA00 に追加する必要があります。

CA MSM を使用した設定

SMP/E によるインストール、展開、および設定の各手順を完了すると、CA MSM によってデータセットが作成されます。CA MSM によって作成されるデータセットの詳細については、「[CA MSM によって作成されるデータセット \(P. 257\)](#)」を参照してください。

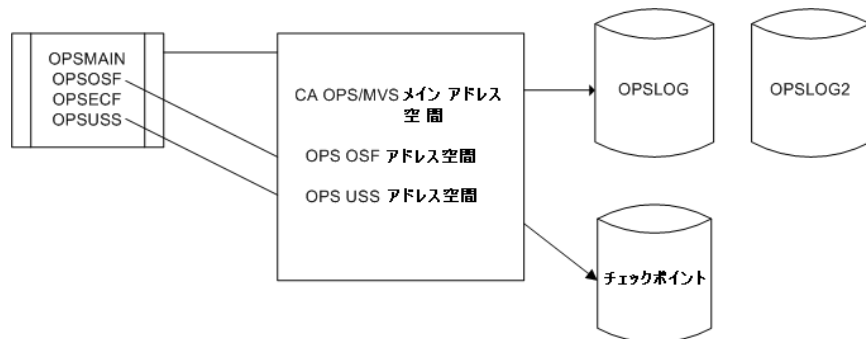
注: 念のため、テスト環境で CA OPS/MVS およびそのコンポーネントの初期インストールおよび設定を行うことを強くお勧めします。このテストによって、他のベンダー製品との競合が検出される可能性があります。

CA OPS/MVS の単純な設定の例

ここでは、CA MSM で設定できる単純な CA OPS/MVS 環境の例について説明します。この環境では、1 つの LPAR 上で CA OPS/MVS が 1 つ実行され、2 つの OPSLOG が定義されています。CA MSM では現在、複数のシステム機能を含む CA OPS/MVS パラメータファイルの設定はサポートされていません。

注: この環境は、CA OPS/MVS を実行および設定した経験が少ないか、またはまったく経験がないユーザが、CA OPS/MVS の最初の実装をテストする場合に便利です。

注: CA MSM を使用して設定すると、本マニュアルの他の部分で手順として説明されているいくつかの手順が自動的に実行されます。



CA MSM を使用する CA OPS/MVS 設定オプション

CA MSM を使用して、CA OPS/MVS の基本操作および以下のオプション コンポーネントを設定できます。

COF

CICS Operations Facility: 別途ライセンスコードが必要です。

HWS

ハードウェア サービス

MSF

Multi-System Facility: 別途ライセンスコードが必要です。

USS

Unix System Services: 別途ライセンスコードが必要です。

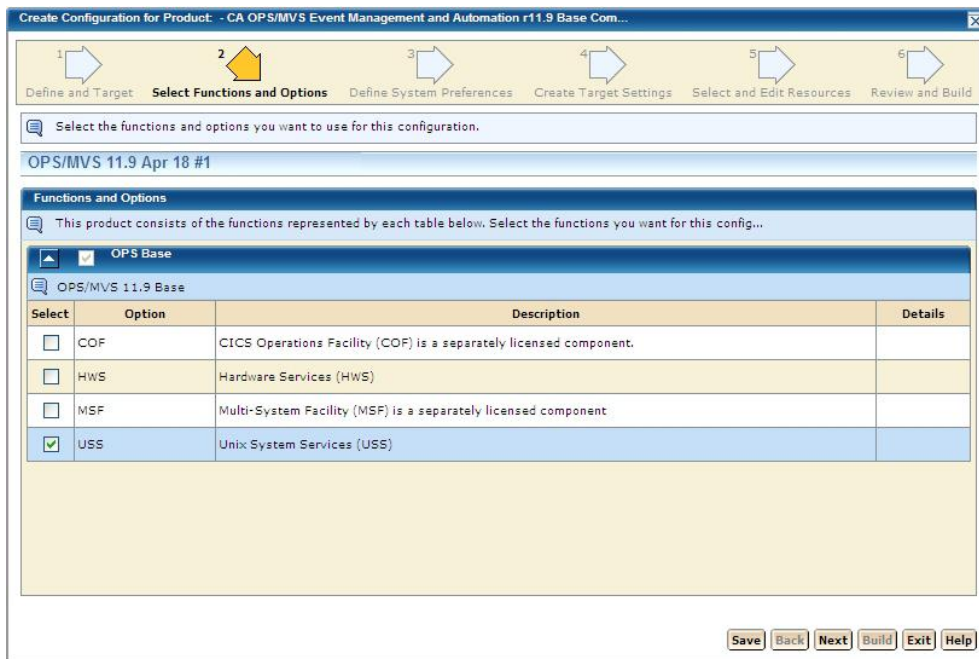
基本操作のみ設定する方法

オプションは一切選択しないでください。

基本操作とオプションを設定する方法

設定するオプションを選択します。

注: 表示されないコンポーネントおよび機能は、CA MSM では設定できません。ただし、それらは、*hlq.CCLXCNTL* データセット内の *OPSSXP00* メンバにカスタムパラメータを追加することで、手動で設定することもできます。



CA MSM を使用して設定する方法の詳細については、「[製品の構成方法 \(P. 40\)](#)」を参照してください。

CA MSM, を使用して CA OPS/MVS を設定した後、以下の手順を完了する必要があります。ただし、これには例外があります。CA MSM で行った選択内容によっては、一部の手順は CA MSM でその一部または全部が完了しています。これについては、適宜各サブセクションで説明されます。

注: CA MSM を使用して設定すると、本マニュアルの他の部分で手順として説明されているいくつかの手順が自動的に実行されます。

CA MSM によりカスタマイズされる起動 JCL プロシージャ

PROCLIB に対して CA MSM でユーザ *proclib* を指定し、CA MSM で PROCLIB 変数の値を指定した場合、CA MSM の実装手順で PROC が生成され、指定されたユーザ *proclib* で使用できるようになっています。

CA MSM の設定中に PROCLIB にユーザ *proclib* が指定された場合、PROC の値が生成され、指定されたユーザ *proclib* に存在します。

NONE が選択されたためにユーザ *proclib* が指定されていなかった場合、CA MSM で生成された PROC を、任意のユーザ *proclib* にコピーします。

CA MSM によって設定された JCL PROC を展開する方法

注: @OPSPFX@ の値は、先に CA MSM の設定プロセスで指定した CA MSM 設定の変数です。

1. SCSMAIN の OPSMAIN へのコピー

SYS2.PROCLIB(OPSMAIN) など、z/OS START コマンド処理中に自動検索される任意の JCL PROCLIB に、@OPSPFX@.CCLXCNTL(SCSMAN) をコピーします。この PROC は名前を変更できます。

2. SCSECF の OPSECF へのコピー

SYS2.PROCLIB(OPSECF) など、z/OS START コマンド処理中に自動検索される任意の JCL PROCLIB に、@OPSPFX@.CCLXCNTL(SCSECF) をコピーします。この PROC は名前を変更できます。

3. SCSOSF の OPSOSF へのコピー

SYS2.PROCLIB(OPSOSF) など、z/OS START コマンド処理中に自動検索される任意の JCL PROCLIB に、@OPSPFX@.CCLXCNTL(SCSOSF) をコピーします。この PROC は名前を変更できます。

4. SCSUSS のコピー (オプション - 存在する場合)

SYS2.PROCLIB(OPSUSS) など、z/OS START コマンド処理中に自動検索される任意の JCL PROCLIB に、@OPSPFX@.CCLXCNTL(SCSUSS) をコピーします。この PROC は名前を変更できます。

注: USS オプションが選択されていない場合、SCSUSS PROC は作成されません。

インストールの確認

CA OPS/MVS のインストールが不完全なために発生した問題を診断することは困難です。このような問題を回避するために、製品を開始する前に以下のチェックリストを使用します。

インストールを確認する方法

1. CA MSM によって生成されたユーザ PROCLIB に、OPSMAIN、OPSECF、および OPSOSF (およびオプションで OPSUSS) の各メンバが含まれることを確認します。変数 PROCLIB に NONE を指定した場合、製品を起動する前に、CA MSM によって生成されるプロシージャを proclib に手動でコピーする必要があります。このタスクを手動で実行する方法については、「CA MSM によりカスタマイズされる起動 JCL プロシージャ」の「CA MSM によって設定された JCL PROC を展開する方法」の手順に従ってください。
2. OPSMAIN、OPSOSF、および OPSECF のスターティッド タスクのいずれかに、CA OPS/MVS に配布されているすべてのロード モジュールが含まれている権限付与済みの STEPLIB があること、または、LNKLSTxx ロード ライブラリあるいは LPALSTxx ロード ライブラリでこれらのすべてのモジュールを使用できることを確認します。
3. 論理 Parmlib 連結にメンバ OPSSSC00 と OPSSXP00 が含まれていることを確認します。
4. SYSPROC に割り当てられたライブラリに、OPSTART1 CLIST および OPSLOGON CLIST が含まれていることを確認します。OPSTART2 は SYSPROC または SYSEXEC に配置することができます。
5. CA ACF2 のコマンド制限機能を使用している場合は、「ベースコンポーネントの設定タスク」の章の「CA ACF2 のコマンド制限リストを提供する」の表に記載されているエントリがあることを確認してください。

設定の完了

hlq.CCLXCNTL のパラメータファイル OPSSXP00 を使用して、手動で追加するパラメータを指定したり、既存のパラメータを上書きしたりできます。ファイル OPSSSC00 は、CA MSM によって自動的に保守されるので、変更しないでください。

設定プロセスを完了するには、「[必要な手動設定 \(P. 110\)](#)」の手順に従う必要があります。

また、初めて製品を起動する場合、事前に「[オプションコンポーネントの設定およびインストール \(P. 147\)](#)」を読んで、確認してください。

CA MSM なしで設定する方法

このセクションのトピックでは、CA MSM を使用して製品を設定しないとき、実行する手動タスクについて説明します。

このセクションでは、CA MSM を使用せずに CA OPS/MVS の設定プロセスを始める場合に実行する必要がある手順についてのみ説明します。

起動 JCL PROC のカスタマイズ

各システムで CA OPS/MVS コンポーネントを起動するために使用する JCL PROC をカスタマイズするには、以下の手順に従います。

起動 JCL のカスタマイズ

SYS1.OPS.CNTL データセットには、CA OPS/MVS のスターティッドタスクを実行するのに必要な JCL メンバとして、次の 4 つのものが含まれています。

- OPSMAIN (メインの CA OPS/MVS アドレス空間)
- OPSOSF (TSO サーバのアドレス空間)
詳細については、「*Administration Guide*」の「*Technical Notes*」の章の「*Regulating OSF Servers*」を参照してください。
- OPSECF (Enhanced Console Facility のアドレス空間)
- OPSUSS (UNIX System Services サーバのアドレス空間)

起動 JCL をカスタマイズする方法

1. OPSMAIN、OPSOSF、OPSECF、および OPSUSS のメンバを、スターティッドタスクのプロシージャライブラリにコピーします (マスタサブシステムで OPSMAIN を開始する場合、このライブラリは SYS1.PROCLIB にします)。これらのメンバは、以下の手順で説明しているようにカスタマイズできます。

2. OPSMAIN メンバ JCL を次のように変更します。

- PROC ステートメントの LOADLIB パラメータを、INSTSMP1 ジョブの TLOAD データセットの新しく作成された OPS.LOAD ライブラリの名前に変更します。CA OPS/MVS のロードライブラリ(SYS1.OPS.LOAD)を linklist または LPALST に配置している場合は、まず STEPLIB ステートメントを削除し、続いて、PROC ステートメントから LOADLIB パラメータを削除します。
- SYSPROC データセットの名前を、INSTSMP1 ジョブの FBCLIST の TARGET バージョンで OPS.FBCLIST データセットに指定した名前に変更します。
- ユーザの hlq.USER.REXX ライブラリに加えて、SYSEXEC データセット名を展開済みのランタイム OPS.CCLXEXEC ライブラリの名前に変更します。
- ご自分のインストール済みシステムで VIO データセットをサポートしていない場合は、SYSTSPRT DD ステートメントの UNIT=VIO を有効なユニット名に変更します。VIO OPSPARM に対して、定義済みの SYSDA などの名前が定義されていることを確認します。定義されていない場合は、OPSTSO DD を正しく割り当てます。
- SMF EXIT IEFUSI SMFPRM の xx parmlib メンバを使用して、64 ビットストレージの使用がインストールによって自動的に制限される場合は、パラメータ 'MEMLIMIT=4G' を OPSMAIN EXEC JCL ステートメントに追加するか、CA OPS/MVS が MEMLIMIT 制限に従わないようにする必要があります。

注: CAHBEXCL DD ステートメントは、CA Hyper-Buf 製品が、CA OPS/MVS アドレス空間内で VSAM の処理要求に影響を与えないようにします。

3. OPSOSF および OPSECF JCL を次のように変更します。

- STEPLIB ステートメントの DSN パラメータを、新しく作成した OPS.LOAD ライブラリの名前、または INSTSMP1 ジョブの TLOAD データセットの名前に変更します。CA OPS/MVS のロードライブラリ(SYS1.OPS.LOAD)を linklist または LPALST に配置している場合は、STEPLIB ステートメントを完全に削除します。
- SYSPROC データセットの名前を、OPS.FBCLIST データセットに指定した名前、または INSTSMP1 ジョブの FBCLIST の TARGET バージョンの名前に変更します。
- ユーザの hlq.USER.REXX ライブラリに加えて、SYSEXEC データセット名を展開済みのランタイム OPS.CCLXEXEC ライブラリの名前に変更します。

これで、起動 JCL メンバのカスタマイズが行われ、CA OPS/MVS のスターテッドタスクを実行する準備ができました。

起動プロセスのカスタマイズ

起動時に CA OPS/MVS は、カスタマイズ可能なプロセスを呼び出します。このプロセスは、起動の制御、および CA OPS/MVS パラメータの設定を行います。

起動プロセスをカスタマイズする方法

1. OPSTART1 初期化 CLIST をカスタマイズします。

OPSTART1 初期化 CLIST は、OPSMAIN プロセスの //SYSPROC 連結内に割り当てられている、展開済みのランタイム *hlq.CCLXCLS0* データセット内にあります。この CLIST は、製品の起動中に内部で作成された TMP で実行され、その主要な目的はさまざまな CA OPS/MVS パラメータを設定する OPS/REXX プログラムを呼び出すことにあります。OPSTART1 CLIST は、以下のステートメントを使用してこの OPS/REXX プログラムを呼び出します。

```
0X 'SYS1.PARMLIB(&SUBSYSNAME.PA&MEMBER)'
```

SYS1.PARMLIB の場所が望ましくない場合は、このステートメントを適宜変更します。また、SUBSYSNAME および MEMBER の置換変数は、OPSMAIN プロセス内で設定されるか、またはオプションで、OPSMAIN の START コマンドによって上書きされます (S OPSMAIN, MEMBER=99)。

デフォルトの SUBSYSNAME の設定: OPSS

デフォルトの MEMBER の設定: 00

したがって、OPSTART1 CLIST で呼び出されるデフォルトの起動 OPS/REXX プログラムの名前は OPSSPA00 です。CA OPS/MVS の新規インストールについては、デフォルトの SUBSYSNAME および MEMBER 設定を使用することをお勧めします。

2. 提供された起動 OPSSPA00 OPS/REXX プログラムをコピーし、カスタマイズします。

hlq.CCLXCNTL データセットのメンバ OPSSPA00 を、OPSTART1 CLIST (手順 1) で指定されたデータセットにコピーします。

このサンプルには、CA OPS/MVS 内のさまざまな制御パラメータを設定し、SYSCHK1 DIV データセット、およびインストールの手順 1 の実行中に DEFDIV ユーティリティを使用して作成された OPSLOG DIV データセットを割り当てるためのロジックが用意されています。これらの DIV データセットを適切に割り当て、特定の CA OPS/MVS パラメータのデフォルト値をオーバーライドするには、このメンバの初めのコメントに記載されている詳細な実行手順に従ってください。

RULEPREFIX

AOF ルールセットのプレフィックス名

RULESUFFIX

AOF ルールセットのサフィックス名

OSFCHAR

OPS/MVS サーバでデフォルトのコマンド文字「!」を上書きする

OSFSTC

デフォルトの OPSOSF を使用していない場合の、OPS/MVS サーバの JCL プロシージャ名

初めてのユーザは、CA OPS/MVS の残りの制御パラメータをデフォルトの設定のままにして、製品をすぐに起動および開始できます。将来的には、特定の自動化要件および環境の要件によっては、CA OPS/MVS の他の制御パラメータのデフォルト値の更新が必要になる場合があります。通常、更新されるパラメータは以下のとおりです。

GLOBAL* parms

グローバル変数のパラメータ制御が設定されます。

OSF*

OPSOSF のすべての側面が制御されます。

OCCONSOLENAME, EXTENDED*, EXTRA*

システムに対してコマンドを発行するために自動化で使用するコンソールのカウントおよび名前が制御されます。

SSICMD, SSIMSG

コマンドおよび WTO フックをどのように設定するかが決定されます。

STATEMAN, SSM*

System State Manager のコンポーネントが制御されます。

これらの一般的なパラメータ、およびその他のすべての CA OPS/MVS 制御パラメータの詳細については、「Parameter and Reference」を参照してください。また、このマニュアルではこれらのパラメータをインストール以外で設定する方法として、OPSPRM() OPS/REXX 関数を使用してプログラムによって設定する、または OPSVIEW 機能を使用して手動で設定する方法について説明しています。

3. (オプション) OPSTART2 OPS/REXX プログラムをカスタマイズします。

メイン CA-OPS/MVS のアドレス空間の内部初期化が完了しており(これは、AOF が完全にアクティブになっていることを意味しているわけではありません)、OSF のアドレス空間が開始される前の状態で、CA-OPS/MVS は、以下のコマンドを OSF TSO 実行キューに送信することによって、最初に準備が完了した OSF TSO サーバで OPSTART2 OPS/REXX プログラムを実行するようスケジュールします。

OI OPSTART2

OI OPSTART2 コマンドは、実行される最初の OSF TSO サーバコマンドです。配布された OPSTART2 プログラムは、OPS/REXX プログラムとして実行することのみを目的として設計されています。このプログラムが TSO/E REXX プログラムとして呼び出されると、ハイライト表示された警告メッセージが発行され、処理が終了します。OPSTART2 OPS/REXX プログラムは、OPSOSF プロシージャの SYSEXEC (ソース) または OPSEXEC (コンパイル済み) の連結のいずれかに配置されなければなりません。

OPSTART2 プログラムには、CA-OPS/MVS の起動後に実行する OPS/REXX 関数、ホスト コマンド、または TSO コマンドを含めることが可能です。

OPSTART2 は外部プロシージャ MSFINIT を呼び出し、MSFINIT は内部プロシージャ InitMSF を呼び出します。InitMSF プロシージャには、CA-OPS/MVS の現在のコピーと CA-OPS/MVS の 2 つのリモートコピーの間でセッションを開始するための、サンプル ADDRESS OPSCTL MSF 制御ステートメントが含まれています。

4. OPSTART2 を *hlq.SAMPLE.REXX* から *hlq.USER.REXX* にコピーします。

注: MSF は OPSTART2 プログラムで定義することができますが、このように定義するには、処理を開始する前に VTAM が実行されていることを確認してください。

OI OPSTART2 は、OSF サーバのデフォルトの初期コマンドです。このコマンドは、製品の初期化で BEGINCMD パラメータを使用して変更できます(詳細については、この章の「OPSSPA00 REXX プログラムのカスタマイズ」を参照してください)。別の OPS/REXX プログラム、または CLIST や TSO/E REXX プログラムを実行するよう BEGINCMD パラメータを設定することもできます。

以下に例を示します。

```
T = OPSPRM("SET", "BEGINCMD", "OI FIRSTPGM")
```

5. (オプション) AOF 初期化 OPS/REXX プログラムを実行します。

AOFINITREXX 製品パラメータを使用して、AOF の初期化中に実行されるように OPS/REXX プログラムの名前を指定することができます。この特別な OPS/REXX プログラムは、製品が自動対応のルールを有効にする前に実行して、AOF ルール環境を論理的に制御できるようにします。OPS/REXX 言語の機能を使用すると、SMF ID、1 日のうちの時刻、または各システムに対して意味のある何らかの基準に基づいて、AOF 環境を制御できます。

ADDRESS AOF のように、ほとんどすべてのホストコマンド環境はこのプログラムで使用できます。ただし ADDRESS TSO だけは例外で、ここでは、メインの製品アドレス空間内で TSO コマンドを使用できません。ADDRESS TSO ホストコマンドは、ADDRESS OSF ホストコマンドのように扱われ、サーバ内の実行キューに入ります。CA OPS/MVS の起動のこの時点では、サーバはまだ開始されていません。後でサーバが開始されたときに、キューに入っていたコマンドが実行されます。既存のグローバル変数、およびリレーショナルテーブルへのアクセスも可能です。これは、以前の IPL の情報を保持しておいたり、後で実行される自動ルーチンへ情報を渡したりする場合に有用です。

注:

- 関数呼び出しまたはホストコマンドで WAIT が発生すると、製品の AOF 初期化が遅れる原因となります。たとえば、OPSWAIT REXX 関数などが、この例です。
- REXX プログラム名を、値 8 の AOFINITREXX RETURN または EXIT して指定すると、AOF 初期化中のすべてのルールの自動有効化はバイパスされます。他のすべてのリターンコードでは、自動有効化が行われます。

6. (オプション) OSFSTART OPS/REXX プログラムをカスタマイズします。

CA OPS/MVS サーバのアドレス空間を作成する OPSOSF プロシージャは、最初のコマンドとして必ず OSFSTART TSO/E REXX EXEC を呼び出します。この REXX EXEC は SYS1.OPS.FBCLIST データセット内にあり、調整できます。

CA OPS/MVS は、OPS/REXX の ADDRESS TSO ホスト環境を介して、サーバの TSO に対応しているコマンドの出力を取得するためのデータセットを事前に割り当てできます。これを行うには、OSFSTART REXX EXEC で割り当てられている OPSTSO DD を使用します。この DD を指定すると、すべての REXX プログラムに対してデータセットを割り当てる代わりに、すべてのコマンドに対して事前の割り当てが使用されます。OSFSTART REXX の ALOPSTSO サブルーチンは、一意に名前が付けられた OPSTSO データセットを各サーバに対して動的に割り当てます。

OSFSTART REXX EXEC の一般的な目的は、サーバが使用するために ISPF データセットを割り当てることです。ISPF では、各サーバに対して一意のプロファイル データセット名が必要です。このデータセット名は、REXX EXEC を変更して提供することができます。

注: OPS.SAMPLES ライブラリに格納されている ALLOCSPF を使用して、サーバが使用するための ISPF データセットを割り当てることをお勧めします。このサンプルは、各サーバに対して一意の ISPF プロファイル データセットを割り当てるための 2 つの異なる方法を示しています。サンプルをカスタマイズして使用する場合は、最初にこのサンプルのコメントをよく読んでください。

これで起動プロセスが定義され、インストールを検証する準備ができました。

OPSLOG およびチェックポイント VSAM 線形データ セットの定義

CA OPS/MVS OPSLOG コンポーネントおよびグローバル変数のチェックポイント機能では、一意の VSAM 線形データ セットの割り当てが必要です。VSAM 線形データ セットは、DIV (仮想域内データ) または DIV データ セットともいいます。CA OPS/MVS を初めて使用する場合は、以下の手順に従ってください。

OPSLOG およびチェックポイント VSAM 線形データ セットを定義する方法

1. 詳細なコメントを確認してから、展開済みのランタイム `hlq.CCLXCNTL` データ セットのメンバ `DEFDIV` をカスタマイズします。このメンバには `IDCAMS DEFINE` コマンドが含まれています。このコマンドは、プライマリ OPSLOG DIV データ セット、オプションとしてセカンダリまたはバックアップの OPSLOG DIV データ セット、およびグローバル変数のチェックポイント機能で使用する `SYSCHK1 DIV` データ セットを作成するのに必要です。

注: DIV データ セットの配置は、「DIV データ セットの配置方法」に記述されている情報を基に決定する必要があります。

CA OPS/MVS を複数のシステムにインストールしている場合は、サンプル JCL に示されているように、システムの SMFID またはシステム名のいずれかをデータ セット名に組み込みます。これにより、共通の CA-OPS/MVS 起動メンバを共有することができます。詳細については、この章の「起動プロセスの更新」を参照してください。

DEFDIV メンバが更新されます。

2. 更新済みの `DEFDIV` メンバを、バッチ ジョブ内の `SYSIN` ステートメントとして使用するか、または TSO で REXX プログラムとして実行します。TSO で `DEFDIV` を実行するには、ISPF のオプション 6 または TSO コマンド プロンプトから以下のように入力します。

```
EXEC 'hlq.CCLXCNTL (DEFDIV)'
```

3. DFSMS を使用していない場合は、マスタ カタログでこれらのデータ セットを定義して、マスタ サブシステムで CA OPS/MVS を起動できるようにします。
4. この章の「OPSSPA00 REXX プログラムのカスタマイズ」の手順を実行するときに参照する必要があるため、OPSLOG および `SYSCHK1` のデータ セットに対して作成した名前をメモしておきます。

OPSLOG およびチェックポイント VSAM 線形データ セットが定義されます。

既存のお客様でのインストール

既存の CA OPS/MVS のお客様が製品の新しいリリースをインストールする場合は、以下のいずれかを行います。

- 「移行とアップグレードの考慮事項」の章に記述されている移行の問題を確認します。ご自分のサイトに関連する問題がある場合、それらに対処する必要があります。その後、以前のリリースの CA OPS/MVS で作成した現在の OPSLOG データセットと SYSCHK1 データセットをこのリリースで使用できるようになります。
- 上述の CA OPS/MVS の新規ユーザ用の手順に従って、新しい OPSLOG データセットと SYSCHK1 データセットを作成します。新しいデータセットには、現在のデータセットに指定したのと同じ割り当て指定を使用します。また、SYSCHK1 データセットの割り当てサイズを増やす必要があるかどうかを決定します。割り当てサイズを増やす方法については、付録の「[DASD 計算チャート](#) (P. 249)」を参照してください。

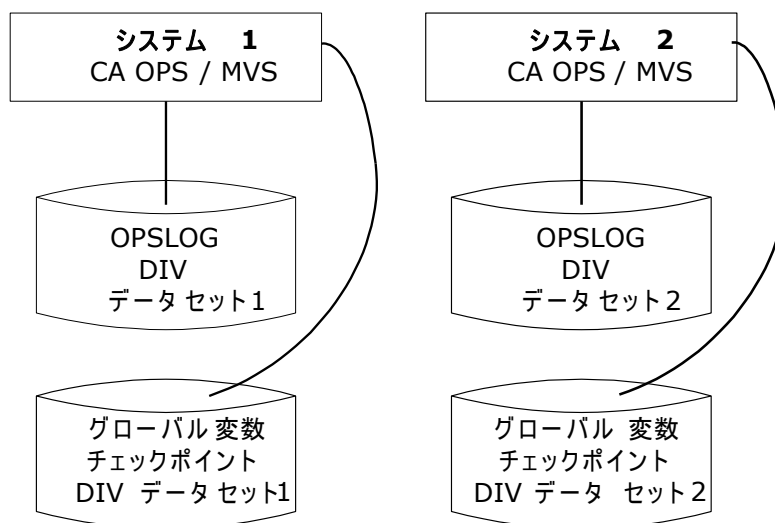
CA OPS/MVS グローバル変数バックアップユーティリティを実装している場合、このリリースの CA OPS/MVS を起動後に OPSSGVR5 を呼び出して新しい SYSCHK1 データセットにデータをコピーできます。CA OPS/MVS グローバル変数バックアップユーティリティが実装されていない場合、このリリースの CA OPS/MVS を起動する前に IDCAMS IMPORT や EXPORT などのシステムユーティリティを使用すれば、新しく割り当てた SYSCHK1 データセットに既存の SYSCHK1 データセットをコピーできます。

注: 同一の VSAM 線形データセットを割り当て中に、2 つのリリースの CA OPS/MVS は同時に実行できません。また、新しいリリースの CA OPS/MVS から古いリリースには変換できない場合があります。

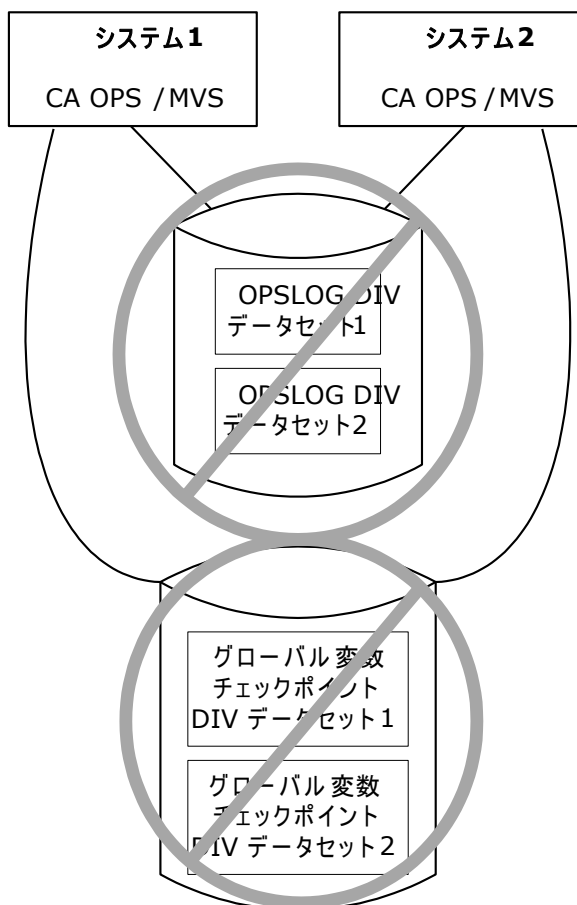
DIV データ セットの配置方法

CA OPS/MVS OPSLOG の Browse 機能、および REXX グローバル変数のチェックポイント機能に対する DIV データ セットは、ページデータセットと同じように配置します。システム間のロックアウトを避けるため、これらのデータセットは共有 DASD に配置してはいけません。また、ページデータセットなど、I/O や RESERVE アクティビティが頻繁に生じるデータセットが存在するボリューム上にも配置してはいけません。

以下の図は、DIV データセットの正しい配置を示しています。



以下の図は、DIV データセットの誤った配置を示しています。



重要: 上記の事項を無視すると、システム全体のパフォーマンスが下がったり、システムの IPL をやり直す必要が生じたり、またはその両方が発生する場合があります。

インストールの確認

CA OPS/MVS のインストールが不完全なために発生した問題を診断することは困難です。このような問題を回避するために、製品を開始する前に以下のチェックリストを使用します。

インストールを確認する方法

1. SYS1.PROCLIB (または、スターティッド タスク JCL プロシージャのコピー先であるプロシージャライブラリ) には、OPSMAN、OPSECF、および OPSOSF のメンバが含まれています。

2. OPSMAIN、OPSOSF、および OPSECF のスターティッド タスクのいずれかに、CA-OPS/MVS に配布されているすべてのロード モジュールが含まれている権限付与済みの STEPLIB があること、または、LNKLSTxx ロードライブラリあるいは LPALSTxx ロードライブラリでこれらのすべてのモジュールを使用できることを確認します。
3. 論理 Parmlib 連結にメンバ OPSSPA00 が含まれていることを確認します。また、OPSSPA00 メンバで設定されたパラメータ値が要件にあっていることを確認します。
4. SYSPROC に割り当てられたライブラリに、OPSTART1 CLIST および OPSLOGON CLIST が含まれていることを確認します。OPSTART2 は SYSPROC または SYSEXEC に配置することができます。
5. CA ACF2 のコマンド制限機能を使用している場合は、「ベースコンポーネントの設定タスク」の章の「CA ACF2 のコマンド制限リストを提供する」の表に記載されているエントリがあることを確認してください。

上記の項目が確認できたら、製品を開始することができます。

必要な手動設定

このセクションでは、CA OPS/MVS の設定に CA MSM を使用しているかどうかに関係なく、手動で実行する必要がある手順について説明します。

注: 以下のサブセクションの一部は、CA MSM を使用して設定プロセスを開始した場合はすでにその一部または全部が完了しています（「CA MSM を使用して設定を開始する方法」を参照してください）。そのようなサブセクションでは、CA MSM で実行済みの手順について注記しています。

ロードライブラリへの APF 権限の付与

CA OPS/MVS のロードライブラリには 2 種類あります。

.CCLXLOAD

製品モジュールのほとんどが含まれます。デフォルトでは標準 PDS であり、必ず APF 権限が付与されている必要があります。

.CCLXPLD

PDSE 内に置かれる必要のあるロードモジュールが含まれます。CA NSM SSM CA-OPS/MVS オプションまたは Switch Operations Facility (SOF) を使用している場合、このロードライブラリも APF 権限が付与される必要があります。現在インストールされている機能に関係なく、このライブラリには永続的な APF 権限を付与することをお勧めします。

上記のとおり、CA OPS/MVS .CCLXLOAD ロードライブラリは、APF 権限を付与されている必要があります。これを LNKST または LPALIB に配置すると、論理 Parmlib 連結の適切な IEASYSxx メンバで LNKAUTH=LNKST が指定されている（またはデフォルト設定できる）場合、CA OPS/MVS ロードライブラリは自動的にこの権限を取得します。それ以外の場合、ロードライブラリの名前、およびロードライブラリが存在するディスクのボリュームシリアル番号を論理 Parmlib 連結の適切な IEAAPFxx メンバに含めて、ロードライブラリに APF 権限を割り当てます。次に、変更を有効にするためにシステムに対して IPL を実行します。

IPL の実行による CA OPS/MVS への権限の付与を行いたくない場合、以下の z/OS コマンドのどちらかを使用して、APF 権限付与済みライブラリを動的に割り当てることができます。

```
SET PROG=xx  
SETPROG APF,ADD...
```

既存の権限付与済みライブラリ、または CA SYSVIEW、Tivoli OMEGAMON XE on z/OS、または RESOLVE/MVS といった主要なオンライン z/OS パフォーマンスおよび操作強化ツールを使用して、新しい権限付与済みライブラリのエントリを追加できます。

ライセンス キーの CA Common Services PPOPTION データ セットへの配置

起動中に、CCS の CAIRIM コンポーネントの CA LMP サービスが呼び出されて、CA OPS/MVS ライセンスの検証が実行されます。CAIRIM のインストール、CA LMP の有効化、および CA LMP キーのコーディングの詳細については、「CA Common Services for z/OS」のドキュメントを参照してください。

PPOPTION データ セットの KEYS メンバの中でアクティブにしたい CA-OPS/MVS コンポーネント(MSF、USS など)に、それぞれ CA LMP キーを配置します。PPOPTION データ セットは、CAS9 JCL プロシージャにあります。

製品ライセンスの設定

このセクションでは、CA LMP を使用してライセンス キーを設定する方法、およびご使用の製品の機能のロックを解除する方法について説明します。

CA LMP キー証明書

CA License Managed Program (CA LMP) キー証明書を検査します。この証明書には、以下の情報が含まれています。

Product Name (製品名)

指定されたサイトおよび CPU に対してライセンスが発行された製品の商標名または登録商標名を定義します。

Product Code (製品コード)

製品に対応する 2 文字のコードを定義します。

Supplement (補足)

特定の機能のライセンスの参照番号を定義します。形式は以下のとおりです。

*nnnnnn-**nnn***

この形式は北米地域とそれ以外で若干異なります。また、参照番号が一切提供されていないこともあります。

CPU ID

この製品のインストールが有効な特定の CPU を識別するコードを定義します。

Execution Key(実行キー)

CA LMP で製品のインストールに必要な暗号化コードを定義します。インストール時には、LMP コードとして参照されます。

Expiration Date(満了日)

ライセンスの有効期限日を定義します。形式は以下のとおりです。

ddmmyy

例: 21Mar12

Technical Contact(テクニカル コンタクト)

製品のインストールとメンテナンスを担当する、サイトに指定された技術担当者 の名前を定義します。弊社では、CA LMP に関するすべての連絡をこの担当者で行います。

MIS Director(MIS ディレクタ)

MIS ディレクタ(サイトでこの機能を実行する担当者)の名前を定義します。証明書に役職のみが指定されていて、個人名が指定されていない場合、証明書を修正または確認する際に実際の名前を追加してください。

CPU Location(CPU 所在地)

CPU がインストールされている建物の所在地を定義します。

CA LMP ステートメントの記述方法

この製品を起動する前に、製品ライセンス認証のために CA LMP ステートメントを記述する必要があります。

CA LMP ステートメントを記述するには、以下の手順に従います。

1. CAIRIM をインストールします。
2. LMP をアクティブ化します。
3. 製品ライセンスコードを LMP ステートメントに追加します。
4. PPOPTION データセットの KEYS メンバ内に LMP ステートメントを配置します。

注: PPOPTION データセットの KEYS メンバは、CAS9 JCL プロシージャに指定されます。詳細については、「*CA Common Services Administration Guide*」を参照してください。

KEYS メンバ - 実行キーの追加

適切に初期化が実行されるようにするために、製品のキー証明書で提供される CA LMP 実行キーを CAIRIM パラメータに追加する必要があります。

CA LMP 実行キーを CAIRIM パラメータに定義するには、KEYS メンバを変更します。

KEYS メンバ用のこのサンプル パラメータ構造は以下のような形式になっています。

```
PROD(pp) DATE(ddmmyy) CPU(tttt-mmmm/sssss)
LMPCODE(kkkkkkkkkkkkkkkk)
```

パラメータ定義は以下のとおりです。

PROD(pp)

2 文字の製品コードを指定します。このコードは、製品の以前のバージョン (存在する場合) の CAIRIM 初期化パラメータによってすでに使用されている製品コードと一致します。

pp の有効な値を次に示します。

A0 - CA OPS/MVS JES 2

CG - CA OPS/MVS JES 3

CI - CA OPS/MVS CICS Operations Facility (COF)

CJ - CA OPS/MVS Switch Operations Facility (SOF)

CN - CA OPS/MVS IMS Operations Facility (IOF)

CU - CA OPS/MVS Multi-system Facility (MSF)

CV - CA OPS/MVS Expert System Interface (ESI)

DATE(*ddmmyy*)

CA LMP ライセンス契約の有効期限 (例: 13MAR12) を指定します。

CPU(*tttt-mmmm/ssssss*)

tttt

CA LMP を実行する CPU のタイプ (例: 3090) が指定されます。

-mmmm

CA LMP を実行する CPU のモデル (例: 600) が指定されます。

注: CPU のタイプまたはモデルが 4 文字未満である場合は、未使用部分に空白が挿入されます。

/ssssss

CA LMP が実行される CPU のシリアル番号を指定します。

LMPCODE(*kkkkkkkkkkkkkkkk*)

CA LMP を実行するのに必要な実行キー (*kkkkkkkkkkkkkkkk*) が指定されます。この CA LMP 実行キーは、各 CA LMP ソフトウェアソリューションに同梱されたキー証明書に記載されています。

例: CA LMP 実行キーの追加

以下に、CA LMP 実行ソフトウェア パラメータに対する制御ステートメントの例を示します。

```
PROD(Y7) DATE(27JUN12) CPU(2096-E26 /370623)
LMPCODE(52H2K06130Z7RZD6)
```

この例では、指定された CPU 上で実行している製品について、CA LMP ライセンス契約が 2012 年 6 月 27 日で期限切れになります。ユーザのサイトで製品をインストールする場合、製品コードと実行キーの値は異なります。

注: CAIRIM パラメータへの CA LMP 実行キーの定義に関する包括的な手順説明、および CAIRIM の機能と関連ユーティリティの詳細については、「*CA Common Services for z/OS Administration Guide*」を参照してください。

データセットへのアクセスの付与

CA OPS/MVS 起動 JCL PROC を開始する前に、それまでのインストール手順で作成された CA OPS/MVS 製品ライブラリへの必要なセキュリティアクセスが付与されていることを確認します。

CA OPS/MVS 起動 JCL PROC には、以下のデータセットへの UPDATE アクセスが必要です。

- この章の「OPSLOG ファイルの割り当て」で作成された OPSLOG ファイル
- この章の「Checkpoint ファイルの割り当て」で作成されたチェックポイントファイル

CA OPS/MVS 起動 JCL PROC には、以下のデータセットの展開されたランタイムコピーへの READ アクセスが必要です。

- opspfx.CCLXCNTL
- opspfx.CCLXLOAD
- opspfx.CCLXPLD

注: CA OPS/MVS 起動 JCL PROC は、CA OPS/MVS 製品ライブラリへの適切なメインフレームセキュリティアクセスが付与されていない場合、失敗します。

ベースコンポーネントの設定タスク

以下のセクションでは、CA OPS/MVS をインストールする前に実行するタスクについて説明します。

z/OS コンソールの定義

CA OPS/MVS で z/OS (およびサブシステム) コマンドを発行し、レスポンスを受信できるようにするには、サブシステムと拡張コンソールのいくつかの組み合わせを指定します。

拡張コンソール

CA OPS/MVS は以下の初期化パラメータを使用して、拡張コンソールを制御します。

- EXTENDEDCONSOLES
- EXTCONSPREFIX

注: 詳細については、「*CA OPS/MVS Parameter Reference*」を参照してください。

システムコンソールの定義

拡張コンソールをサポートしない製品を実行している場合、サブシステムコンソールを使用して製品にコマンドを発行しなければならないことがあります。論理 Parmlib 連結の `CONSOLnn` メンバにサブシステムコンソールが定義されていない場合、追加する必要があります。

割り当てるサブシステムコンソールの数によって、CA-OPS/MVS がユーザに代りして同時に発行できる z/OS コマンドの最大数が決定されます。

サブシステムコンソールを定義する方法

1. SYS1.OPS.CCLXCNTL データセットの CONSOL00 メンバ内で以下のサンプルコンソールの定義を調整します。

```
CONSOLE DEVNUM(SUBSYSTEM),AUTH(ALL),NAME(OPSSSC01)
```

2. IPL を実行します。

サブシステムコンソールが定義されました。

重要: 特定のサブシステムコンソール ID に依存する自動化は、シスプレックス環境では失敗することがあります。ID は、z/OS により動的に割り当てられるので、IPL ごとに変換することがあるからです。

システムリンケージインデックスの可用性の保証

CA OPS/MVS では、システム関数テーブルにシステムリンケージインデックス (LX) が必要です。CA OPS/MVS が正常終了または異常終了した後に再起動した場合、このシステムリンクインデックスが再利用されます。CA OPS/MVS の複数のコピーを実行する場合は、コピーごとにシステムリンクインデックスが必要となります。

通常は、システムリンケージインデックスには、CA OPS/MVS に対応するだけの十分なエントリが含まれていなければなりません。このようになっていない場合は、論理 Parmlib 連結の該当する IEASYSxx メンバの NSYSLX の値を修正して、数を増やします。

注: CA SYSVIEW 製品を実行している場合は、システムリンケージインデックスに CA OPS/MVS に対応するだけの十分なエントリが含まれているかどうかを判断できません。判断方法の詳細については、CA SYSVIEW コマンドヘルプの LXATABLE コマンドを参照してください。逆に、CA SYSVIEW がない場合は、CA OPS/MVS の起動前にこのような状況になっているかどうかを判断できません。これは、z/OS オペレーティングシステムにはこのデータをチェックする機能がないからです。

システムリンケージインデックスの詳細については、IBM のドキュメントを参照してください。

ASVT エントリの置換

CA OPS/MVS は空間スイッチエントリテーブルを所有しているため、z/OS は、製品の終了後、メインの製品アドレス空間で使用された ASVT エントリを再利用不可としてマークします。CA OPS/MVS が停止と開始を繰り返している場合は、利用可能なアドレス空間が不足する可能性があります。

これらの再利用不能な ASVT エントリを置き換えられるようにするには、論理 Parmlib 連結の該当する IEASYSxx メンバの RSVNONR パラメータを、(5 などの) 小さい数だけ増やします。

ISPF を使用して LPA にコマンドプロセッサを追加する

LPA の外部で CA OPS/MVS を実行し、ISPF を使用している場合は、CA OPS/MVS コマンドプロセッサの名前を ISPF TSO コマンド テーブル モジュールに追加する必要があります。

コマンドプロセッサの名前を追加する方法

1. ISPTCM に対して行わなければならない修正において、SYS1.OPS.CCLXCNTL データセットのメンバ OPISPTCM のサンプルを確認します。

ISPTCM へ名前を追加する詳細については、ISPF の「インストール ガイド」を参照してください。

2. TSO コマンド名のリストが含まれている、ISPTCM モジュールに名前を入力します。

このテーブル モジュールに対する修正が完了しました。

3. テーブル モジュールを再アセンブルして、適切なロード ライブラリへリンクします。

コマンドプロセッサが追加されました。

詳細:

[CA ACF2 のコマンド制限リストを提供する \(P. 127\)](#)

その他コマンドプロセッサの考慮事項

CA OPS/MVS コマンドプロセッサが含まれている ISPTCM モジュールは、STEPLIB、linklist、または LPALIB からロードできます。ただし、CA OPS/MVS のコマンドプロセッサが STEPLIB または linklist からロードされている場合は、これらのプロセッサは、システムで使用している ISPTCM ロードモジュールには含まれてはいけません。

ただし、具体的には CA OPS/MVS の新しいリリースをテストするために、別のシナリオが存在することがあります。たとえば、以下のシナリオを作成することができます。

- STEPLIB 内に、CA OPS/MVS コマンドプロセッサを備えていない ISPTCM ロードモジュールがあり、テスト用の STEPLIB 内に新しい CA OPS/MVS コマンドプロセッサがある。
- linklist 内に、システムで実際に使用している ISPTCM モジュールがあり、LPALIB 内に CA OPS/MVS のコマンドプロセッサがある。

注: ISPTCM テーブルは STEPLIB、linklist、または LPALIB 内に存在することが可能なため、このテーブルの別のバージョンが、これらの場所のそれぞれに同時に存在することがあります。そのような場合に TSO コマンドプロセッサを ISPF の下でロードしようとすると、検索で最初に見つかった ISPTCM バージョンが制御 ISPTCM となります。

LPA の使用効率

LPA を最大限に活用するには、CA OPS/MVS モジュール OPSAEX を LPALST ライブラリにコピーします。これによって OPSVIEW とすべての CA OPS/MVS コマンドプロセッサがより迅速に実行され、共通コードを共有できるようになります。これにより、実ストレージおよびページングの全体的な要求が低減されます。

OPSAEX ロードモジュールを LPA に置く場合、メインアドレス空間は OPSAEX に含まれる多くのモジュールを共有できます。これを行うには、以下の DD カードを OPSMAIN JCL に追加します。

```
//OPSAEX DD DUMMY
```

これによって、OPSAEX が LPA 内に存在する場合、製品のメインアドレス空間により使用される ECSA の使用量が約 400 KB 低減されます。この DDNAME を省略すると、OPSAEX が LPA に存在する場合でもメインアドレス空間は OPSAEX の共有を試みません。

ISPF インターフェース モジュールへのアクセスの提供

CA OPS/MVS の要求ルールは ISPF サービスを使用できるため、ISPF インターフェース モジュール、ISPLINK および ISPEXEC を CA OPS/MVS のメインアドレス空間で使用するようになっています。これらがすでに LPALST 連結内にあるか、または LNKLST 連結内の APF 権限付与済みライブラリ内にある場合、何もする必要はありません。それ以外の場合は、それらの 2 つのモジュールを、CA OPS/MVS ロードライブラリまたはそれに連結されている APF 権限付与済みライブラリの CA OPS/MVS プロシージャに、STEPLIB としてコピーまたはリンクエディットします。SYS1.OPS.CCLXCNTL データセットのメンバ ISPFLINK には、ISPF インターフェース モジュールをリンクエディットし、CA OPS/MVS ロードライブラリに格納するためのサンプル JCL が含まれています。

データセットの命名基準の確立

CA OPS/MVS は、データセットの名前が SYS1.OPS で始まることを想定します。名前を変更して、データセットの命名規則と一致させることができます。

ユーザ REXX ライブラリの作成

ユーザが修正可能なプログラムは、hlq.CCLXSAMP ライブラリにあります。ユーザが修正可能なプログラムは、さまざまなサンプル自動アプリケーションのほか、エンドユーザ (System State Manager、OPSVIEW コマンド オプションなど) によってカスタマイズされる特定の CA OPS/MVS コンポーネントもサポートします。

重要: hlq.CCLXEXEC ライブラリに含まれる CA OPS/MVS プログラムは、CA OPS/MVS のベースコンポーネントの機能に必要ですので、決して CA サポートの指示がない場合は絶対に変更しないでください。

ユーザ REXX ライブラリを作成する方法

1. hlq.CCLXEXEC または hlq.CCLXSAMP ライブラリと同じ割り当て属性を使用して、hlq.USER.REXX データセットを作成します。
2. 必要に応じて、サンプルアプリケーションプログラムおよびユーザ指定コンポーネントプログラムを、hlq.CCLXSAMP ライブラリからユーザの hlq.USER.REXX ライブラリにコピーします。

この hlq.USER.REXX ライブラリには、ユーザが作成した自動アプリケーションのサポートに必要なすべての REXX プログラムと OPS/REXX プログラムも含まれます。

ルール セットの名前

データセットの命名規則も、ルール セットにおいて重要です。ルール セットは分割されたデータセットであり、CA OPS/MVS Automated Operations Facility (AOF) がシステム操作を自動化するために使用する、OPS/REXX プログラム(呼び出されたルール)が格納されています。名前の形式を以下に示します。

```
ruleprefix.rulesetname.rulesuffix.
```

CA OPS/MVS の起動時に、AOF はカタログ内のルール セットを検索します。

ルール セットのプレフィックスおよびサフィックスの設定

CA OPS/MVS の RULEPREFIX パラメータは、ルール セットに対するデータセット名のプレフィックスを指定します。このデフォルト値は **SYS1.OPS** になります。RULESUFFIX パラメータは、ルール セットに対するデータセット名のプレフィックスを指定します。デフォルト値は **RULES** になります。

たとえば、デフォルトのプレフィックスおよびサフィックスを使用しているルール セット名は、**SYS1.OPS.SYS1IEA.RULES** となります。

RULEPREFIX の値には 10 個のレベルを定義することが可能で、26 文字を指定することができます。特に、先行修飾子が **SYS1** の場合は、AOF がカタログをスキャンしてルール セットを探すときの処理を高速化するために、マルチレベルの RULEPREFIX を使用します。ただし、RULESUFFIX の値とルール セットの名前は、1 つのレベルのみを持つようにします。ルール セットの名前は、OPSVIEW の表示におけるルール セットを指定します。

重要: CA OPS/MVS ルール データセットに対しては、一意の高レベル修飾子を使用することを強くお勧めします。この警告どおりにしないと、CA OPS/MVS の初期化で失敗したり、パフォーマンスが低下したり、その両方が起こったりなどの問題が生じることがあります。

有効なルールセット名

前セクションで記載されている `ruleprefix` および `rulesuffix` にデフォルト設定を使用する場合、有効なルールセット名は以下のとおりです。

- `SYS1.OPS.SEC.RULES`
- `SYS1.OPS.TOD.RULES`
- `SYS1.OPS.JES.RULES`
- `SYS1.OPS.SUPP.RULES`

ルールセット名 `SYS1.RULES.HASP.RULES` は、異なる第 2 レベル修飾子を持つので無効です。

代替命名規則

上記のルールセット命名規則がニーズに合わない場合、以下の 2 つの命名規則のどちらかを代わりに使用します。これらの命名規則は、さまざまなルールセットのグループに対して異なる高レベル修飾子を使う必要があるサイトのためのもので、両方の代替命名規則を使用することはできません。

注: CA OPS/MVS は最大 70 までのルールセットをサポートします。

RULEALTFIX パラメータを使用します。

RULEALTFIX パラメータは、別のグループのルールセットに別の高レベル修飾子を使用できるようにします。

この代替命名方式を使用するには、RULEALTFIX パラメータを次のように使用して代替の高レベル修飾子のリストを指定します。

```
var = OPSPRM("SET", "RULEPREFIX", "SYS1.OPS")
var = OPSPRM("SET", "RULEALTFIX", "SYS2,SYS3,SYSX")
var = OPSPRM("SET", "RULESUFFIX", "RULES")
```

以下のルールセットが使用されます。

```
SYS1.OPS.*.RULES
SYS2.OPS.*.RULES
SYS3.OPS.*.RULES
SYSX.OPS.*.RULES
```

以下の事項を考慮する必要があります。

- 高レベル修飾子が違っていても、下位修飾子は一致する必要があります。
- すべての高レベル修飾子は同じ長さである必要があります。
- このサポートを使用する場合、ルールセット名は高レベル修飾子で始める必要があります。これにより、2つのルールセットに同一の名前を定義する間違いを避けられます。

適切なルールセット名の例を以下に示します。

```
SYS3.OPS.SYS3MSG.RULES  
SYS1.OPS.SYS1MSG.RULES
```

不適切なルールセット名の例を以下に示します。

```
SYS1.OPS.MESSAGE.RULES
```

- 例内の引用符は必須です。

RULEPREFIX2 パラメータを使用します。

この代替命名方式を使用するには、OPS/REXX の OPSPRM 関数を次のように使用して代替のプレフィックスを 1 つ指定します。

```
var = OPSPRM("SET", "RULEPREFIX", "SYS1.OPS")  
var = OPSPRM("SET", "RULEPREFIX2", "SYS2.OPS2")  
var = OPSPRM("SET", "RULESUFFIX", "RULES")
```

以下のルールセットが使用されます。

```
SYS1.OPS.*.RULES  
SYS2.OPS2.*.RULES
```

以下を考慮してください。

- パラメータ `RULEALTFIX` が指定されている場合、パラメータ `RULEPREFIX2` は無視されます。
- `RULEPREFIX2` では、`RULEPREFIX` 単独、または `RULEPREFIX` と `RULEALTFIX` を使用する場合よりオーバーヘッドが増加します。
- `RULEPREFIX2` で指定された高レベル修飾子は、`RULEPREFIX` で指定された高レベル修飾子から完全に独立しています。最大 10 レベルを指定でき、最大長は 26 文字です。
- `RULEPREFIX` で同じ名前のルール セットが見つかった場合、`RULEPREFIX2` で見つかった重複するルール セットは無視されます。

たとえば、以下のデータセットが存在したとします。

```
SYS1.OPS.MESSAGE.RULES  
SYS2.OPS2.MESSAGE.RULES
```

`SYS2.OPS2.MESSAGE.RULES` データセットは無視されます。

- 例内の引用符は必須です。

セキュリティ製品のログオン ID の作成

CA OPS/MVS は、多くのアドレス空間を使用します。CA ACF2、CA Top Secret、または別のセキュリティ製品を実行している場合は、以下の処理が必要になる場合があります。

- `OPSMMAIN`、`OPSECF`、`OPSOSF`、および `OPSUSS` のアドレス空間に対するユーザ ID を定義する。
- これらのアドレス空間で必要なデータセットを使用できるよう、アクセスルールを設定する。
- `OPSUSS` サーバに対するユーザ ID が、要求された種類の USS コマンドを実行するのに十分な USS セグメント権限を持っていることを確認します。

データ セットのアクセス要求

以下の表は、CA OPS/MVS に対するアクセス要件の概要を示しています。ユーザ自身のデータベースを更新するアプリケーションを開発する際に、これらのデータベースへのアクセスも必要です。製品の使用を開始し独自のアプリケーションを書いたら、独自の REXX、CLIST、OPSEXEC、および、おそらくユーザ ISPF データセットへのアクセスも提供する必要があります。

データ セット名	アクセス	ユーザ ID
OPS.xxx.RULES	Read、 Write	OPSMAIN および権限付与された TSO ユーザ
OPS.CCLXLOAD	Execute	OPSMAIN、 OPSOSF、 OPSECF およびすべての TSO ユーザ
OPS.CCLXEXEC	Read	OPSMAIN、 OPSOSF、 OPSECF およびすべての TSO ユーザ
OPS.CCLXCLS0	Read	OPSMAIN、 OPSOSF、 OPSECF およびすべての TSO ユーザ
OPS.OPSLOG	Read、 Write	OPSMAIN
OPS.SYSCHK1	Read、 Write	OPSMAIN
Logical Parmlib Concatenation	Read	OPSMAIN
OPS.CCLXHENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXPENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXMENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXSENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXTENU	Read	権限付与されたすべての TSO ユーザ
OPS.CCLXOPEX	Read	権限付与されたすべての TSO ユーザおよび場合により OPSOSF

注: SSMGA を使用している場合、OPS.CCLXOPEX データセットも OPSMAIN プロシージャに割り当てる必要があります。

重要: データ セットにアクセスするための十分な権限を各アドレス空間に与えないまま CA OPS/MVS を実行してしまうことは、インストールに関する最も一般的な問題です。

TSO OPER 権限の付与

セキュリティパッケージを通じてユーザ ID に TSO OPER 権限を付与する必要があります。権限を付与するユーザ ID には、OPSMAN ユーザ ID と OPSOSF ユーザ ID など、ADDRESS OPER コマンドを発行したり、OPSVIEW 6 からコマンドを入力したり、opslog OPSVIEW 1 パネルからコマンドを入力したりするユーザ ID すべてが含まれます。

TSO OPER 権限を付与するには、OPS/REXX プログラム OPSIVP を実行します。

同様に、TSO のサブミット、ステータス、およびキャンセルのコマンドを使用する必要があるユーザ ID にも上述の作業が必要です。

CA ACF2 のコマンド制限リストを提供する

サイトで CA ACF2 を使用しており、ユーザがコマンド制限リストを使用している場合は、OPSVIEW および他の製品のコンポーネントを機能させるために、いくつかのエントリを追加する必要があります。

CA ACF2 を実行していない、またはコマンド制限リストを使用していない場合は、このセクションを省略してください。

CA ACF2 の考慮事項

CA OPS/MVS は、ほとんどのセキュリティインターフェースの呼び出しに SAF (RACROUTE) を使用します。具体的には、一般的なリソースチェックの実行に OPSECURE('R',...) 関数を使用する CA ACF2 サイトに影響します。1 つか複数の CA ACF2 CLASMAP レコードを作成することによって、SAF リソースクラスを変換する必要があります。CLASMAP レコードは、8 文字からなる SAF リソースを 3 バイトの CA ACF2 リソースタイプのコードに変換します。

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

CA-OPS/MVS のコマンドプロセッサ

OPS.CCLXASM のメンバ OPA2CMLS には、サンプルのコマンド制限リストが用意されています。この中には、以下のリストに示されているコマンドが含まれており、これはユーザ自身のリストに統合されます。詳細については、「*CA ACF2 Systems Programmer Guide*」を参照してください。以下の表に、CA-OPS/MVS のアクセス要件の概要を示しています。ユーザ独自のデータベースを更新するアプリケーションを開発する場合、これらのアプリケーションへのアクセスも必要です。

OPAAMAIN

CA OPS/MVS Automation Analyzer。

エイリアス: なし

OPADDRUL

動的な自動フォーマット-ルール (ADDRULE)。

エイリアス: なし

OPBIND

EPI セッション エンキュー (BIND)。

エイリアス: なし

OPBOMD

OPSLOG Browse を呼び出すために OPSBRW/OB で使用する内部インターフェース。このコマンドは、エンドユーザは直接使用できません。

エイリアス: なし

OPDELRUL

動的な自動フォーマット ルールを削除します (DELRULE)。

エイリアス: なし

OPGETSCR

EPI 画面イメージの取り込み (GETSCRN)。

エイリアス: なし

OPPARSE

CLIST/REXX の解析コマンド (PARSE)。

エイリアス: なし

OPRXCMAP

コンパイル済みの REXX マネージャ。

エイリアス: なし

OPSBRW

CA OPS/MVS のメッセージログを参照します。

エイリアス: OB

OPSCMD

z/OS/IMS/VM/JES オペレータコマンド (OSCMD、CPCMD) を発行します。

エイリアス: OC、OPSOSCMD

OPSELV

グローバル変数 (DELVAR) を削除します。

エイリアス: なし

OPSDOM

保持されているコンソールメッセージを削除します (DOM)。

エイリアス: なし

OPSESS

EPI スクリーン エントリ (SESSCMD)。

エイリアス: なし

OPSEXC

明示的な OPS/REXX インタプリタ。

エイリアス: OX、OXDB、OXSCAN

OPSGETV

グローバル変数の値を取得します (GETVAR)。

エイリアス: なし

OPSGETVL

グローバル変数名のリストを取得します (GETVARL)。

エイリアス: なし

OPSHFI

共有ファイル I/O コマンド (READVAR、WRITEVAR)。

エイリアス: なし

OPSIMEX

暗黙的な OPS/REXX インタプリタ。

エイリアス: OI、OIDB

OPSMODE

現在も以前の Automate コマンドプロセッサをご利用されている Automate ユーザに対して、エイリアスのエントリポイントを提供します。

エイリアス: ADDRULE、BIND、CLIST、CPCMD、DELRULE、DELVAR、DOM、GETSCRN、GETVAR、GETVARL、MLWTO、OSCMD、PARSE、READVAR、REPLY、REXX、SESSCMD、SETVAR、SQL、STATETBL、TSOCMD、UNBIND、WAIT、WRITEVAR、WTL、WTO、WTOH、WTOR

OPSPARM

CA OPS/MVS のパラメータを表示/変更します。

エイリアス: OP

OPSQL

TSO から SQL コマンドを発行します (SQL)。

エイリアス: なし

OPSREPLY

WTOR に対する応答を発行します (REPLY)。

エイリアス: なし

OPSREQ

エンドユーザの処理要求を発行します。

エイリアス: なし

OPSRMT

リモート TSO コマンドを発行します (REXX TSOCMD、CLIST)。

エイリアス: OR

OPSETV

グローバル変数の値を更新します (SETVAR)。

エイリアス: なし

OPSSMTBL

System State Manager のリソース ディレクトリ テーブルを保持します (STATETBL)。

エイリアス: なし

OPSWAIT

指定された時間だけ待機します (WAIT)。

エイリアス: OW

OPSWTO

WTO メッセージまたは WTOR メッセージを発行します (WTL、WTO など)。

エイリアス: なし

OPUNBIND

EPI セッション デキュー (UNBIND)。

エイリアス: なし

OP310000

OPSVIEW アドレス空間のリソース機能。

エイリアス: なし

O332TBLD

OPSVIEW プリンタリソース機能。

エイリアス: なし

OPSVIEW

CA OPS/MVS のインタラクティブ サービスを起動します。

エイリアス: OPSV

サブシステム ID の論理 Parmlib 連結への追加

CA OPS/MVS は z/OS サブシステムとして実行されます。このようなサブシステムは、論理 Parmlib 連結の適切な IEFSSNxx メンバのステートメントを介して IPL 時間で定義されます。ただし実際には、ほとんどのサブシステムは動的に追加されます。

CA OPS/MVS がサイトの IEFSSNxx メンバ内で定義されていない場合、CA OPS/MVS は標準 z/OS インターフェースを使用して SSCT を動的に追加します。そのため、IEFSSNxx メンバを更新するかどうかの判断は、サイトのポリシーによります。

SYS1.OPS.CCLXCNTL データセットのメンバ IEFSSNOP には以下のサンプルステートメントが含まれています。これらのサンプルステートメントは、論理 Parmlib 連結の本番稼働 IEFSSNxx メンバに挿入して、CA OPS/MVS の標準本番稼働およびテストのサブシステム名の定義に使用できます。

OPSB	OPSLG BROWSE ONLY OPS/MVS
OPST	TEST OPS/MVS
OPSS	PRODUCTION OPS/MVS

上記の例のとおり、本番稼働 CA OPS/MVS は最後に表示されます。ただし最後に表示される必要がある別のサブシステムが存在する場合、本番稼働 CA-OPS/MVS はその最後のシステムの直前に表示されます。

パラメータ SSICMD および SSIMSG は、CA OPS/MVS がほかのサブシステムに関連するメッセージとコマンドを処理する際に影響します。

ベースコンポーネント用のオプション インストール タスク

以下のセクションでは、CA OPS/MVS のベースコンポーネントをインストールするときに必要に応じて実行できるタスクについて説明します。

ロードモジュールのリンクパック領域への配置

リンクパック領域 (LPA) 外で CA OPS/MVS を実行すると、ECSA 要件を大幅に削減することができます。ECSA 要件を削減するには、論理 Parmlib 連結の LPALSTxx メンバにロードライブラリの名前を追加します。

重要: 以下の CA OPS/MVS ロードライブラリモジュールは、LPALST 連結ライブラリにコピーしてはいけません。これらの連結ライブラリによって、z/OS IPL でエラーが生じる可能性があるからです。

ASOEDIT、ASOEDPAR、および ASOEDSYS

これらのモジュールは、Automate ルールエディタで使用されます。これらのモジュールは再入可能ではありません。

OPARSX35

このモジュールは、アーカイブされた OPSLOG がマージされる時に使用される SORT exit です。このモジュールは再入可能ではありません。

CAIXNYI@

これはデータのみで、CA Examine 用の情報を提供するために動的に更新されます。

LPALIB の外部で CA OPS/MVS を実行する場合は、ほとんどの CA OPS/MVS モジュールが LPA から使用されないことに注意してください (つまり、以下のパラグラフの推奨事項に従う場合です)。実際には、LPA にロードされる CA OPS/MVS は 10 KB 未満です。ほとんどのロードモジュールは ELPA にロードされます。

以下のモジュールは、RMODE 24 であるので、LPA ではなく、linklist または STEPLIB にコピーすることを強くお勧めします。

- OPAME010 モジュール (AME レポータで使用される)
- OPSQTETB モジュール (RDF テーブルエディタで使用される)

TSO コマンド権限の付与

TSO コマンドプロセッサの権限付与は不要です。CA OPS/MVS が実行中に権限付与サービスを提供します。このルールの唯一の例外は、CA OPS/MVS がダウンしている間に TSO ユーザのアドレス空間で CA OPS/MVS コマンドが実行される場合です。

以下の表は、権限付与できる TSO コマンドプロセッサの一覧です。これらのプライマリ名およびエイリアスは両方とも、IKJTSOxx に入る必要があります。

コマンド	エイリアス	説明
OPSCMD	OC	z/OS、JES2 または JES3、VM、および IMS オペレータコマンドを発行
OPSDOM	なし	ハイライト表示されたメッセージを削除
OPSREPLY	なし	WTOR に応答
OPSWTO	なし	WTO または WTOR メッセージを発行

これらの TSO コマンド権限付与に使用される方法は、サイトでインストールされている TSO/E のリリースによって異なります。

TSO コマンド権限の設定は、論理 Parmlib 連結の適切な IKJTSOxx メンバから行えます。この例は、SYS1.OPS.CCLXCNTL のメンバ IKJTSO00 を参照してください。CA SYSVIEW を使用している場合を除き、システムを再起動して、これらの変更を有効にする必要があります。CA SYSVIEW が使用できる場合は、システムを再起動することなく、これらの名前を TSO コマンドテーブルに動的に追加することができます。

権限付与済みプログラムまたは REXX プログラムから直接実行されたコマンドは、変数名が SYSAUTH で始まる場合にのみ REXX が作成した変数にアクセスできます。この TSO/E 制限は、OPSWTO コマンドプロセッサの TEXTVAR パラメータを使用している場合にのみ適用されます。詳細については、IBM のドキュメントを参照してください。

ロードモジュールへのアクセスの提供

CA OPS/MVS の機能にアクセスするすべてのアドレス空間は、すべての CA OPS/MVS ロードモジュールにアクセスする必要があります。ロードモジュールが存在するライブラリを LNKLST または LPALIB 内に配置するか、OPSMAN、OPSECF、OPSOSF、および OPSVIEW などの CA OPS/MVS の機能を使用する TSO ユーザのスターティッドタスク JCL に STEPLIB を追加できます。

重要: SYS1.OPS.CCLXLOAD を ISPF ユーザ用の ISPLLIB 連結に含めないでください。これは、権限が付与されて実行される CA OPS/MVS コマンドプロセッサが ISPLLIB からロードできないためです。

詳細:

[ロードモジュールのリンクパック領域への配置 \(P. 133\)](#)

OPSMODE コマンドプロセッサのインストール

以前に Automate を使用しており、現在も Automate コマンドプロセッサを使用している場合は、OPSMODE コマンドプロセッサをインストールできます。

OPSMODE をインストールするには、提供されている SMP/E USERMOD を使用できます (OPS.CCLXCNTL 内の USERMODS メンバを参照してください)。このメンバは、SMP/E への OPSMODE のサンプルです。CA OPS/MVS のテクニカルサポートでは、USERMOD の RECEIVE と APPLY のみを行い、ACCEPT は行わないことをお勧めします。この推奨事項に従うと、OPSMODE のメンテナンスのたびにこの USERMOD を再適用する必要があります。

CCS for z/OS のイベント管理コンポーネントとの UNIX System Services インターフェースのインストール

CA OPS/MVS の UNIX System Services (USS) コンポーネントは、UNIX シェルコマンドを実行する OSF のクラスを提供し、API 呼び出しを CCS for z/OS のイベント管理コンポーネントに送ります。

CA OPS/MVS USS による z/OS Event Management へのインターフェース接続には、z/OS システムに CCS のイベント管理コンポーネントがインストールされている必要があります。さらにその他いくつかの z/OS CCS コンポーネントも必要です。

詳細情報:

[UNIX System Services のインストール \(P. 201\)](#)

注: CCS for z/OS コンポーネントの FMID 別の一覧については、付録の「CCS for z/OS Component の要件」を参照してください。

USS からイベント管理へのインターフェース接続

CA OPS/MVS USS による z/OS Event Management への接続は、以下を行います。

- イベント管理コンソール メッセージを OPSLOG で利用可能にする
- USS ルールがイベント管理コンソール メッセージに対応できるようにする
- CA OPS/MVS から z/OS Event Management やその他の CCS イベント管理に接続されたプラットフォームに、コマンドおよびメッセージを送信できるようにする

INSTUSEX のカスタマイズおよび実行

OPS/MVS USS による z/OS Event Management へのインターフェース接続には、互換モードでメッセージ exit が z/OS Event Management HFS ディレクトリまたは zFS ディレクトリにコピーされる必要があります。この作業のために、INSTUSEX ジョブが OPS.CCLXCNTL ファイル内に提供されています。

INSTUSEX ジョブをカスタマイズして実行する方法

1. インストール基準に合わせて、ジョブ ステートメントを変更します。
2. DISKPFX パラメータを、展開済みのランタイム ライブラリのデータ セット名プレフィクスに設定します。
3. データ セットはジョブの実行後に割り当てられます。
4. USRPATH パラメータを設定します。CCS for z/OS モジュール TNEM EVT2 が格納されているディレクトリを知る必要があります。デフォルトのディレクトリは /cai/tngfw/lib です。TSO から OMVS コマンドまたは ISHELL コマンドを発行して確認できます。CA NSM のイベント管理コンポーネントがインストールされていない場合、コンポーネントが利用可能になった時点でこのジョブを実行してください。
5. INSTUSEX ジョブの調整および実行準備ができました。
6. INSTUSEX ジョブを実行します。
7. メッセージ exit は、互換モード ディレクトリ内の z/OS Event Management HFS または zFS にコピーされます。リターンコードが 0 であることを確認してください。

CCS for z/OS の caiopr 処理を停止および再開します。

コピーされたメッセージ exit がアクティブになります。

システム準備タスクの概要

以下のリストは、CA-OPS/MVS のシステム準備タスクをまとめたものです。各アイテムが CA-OPS/MVS の操作に与える影響を確認してください。

- CA LMP キー証明書
CA-OPS/MVS の初期化に必要な情報が含まれます。
- 互換性のあるソフトウェアのレベル
互換性のないレベルは問題となる可能性があります。 [CA サポート](#)にお問い合わせください。
- z/OS サブシステム コンソール
同時に発行される z/OS コマンドを制限します。サブシステム拡張コンソールがない場合、OPSCMD、OPSRMT、および OPSVIEW は機能しません。
デフォルト: 2
- 拡張コンソール
MIGID のない拡張コンソールの数
デフォルト: 8
推奨: 8
- 十分な ECSA が利用可能
ECSA が十分に利用できない場合、問題となる可能性があります。
SYS1.OPS.CCLXLOAD を LPA/ELPA に入れることによって、問題を解消または減少させます。
推奨: 500 KB
- プログラム ライブラリ用 DASD スペース、OPSLOG ブラウズ メッセージ、およびグローバル変数
CA OPS/MVS のインストールおよび実行に必要な DASD スペースの計算方法の詳細については、「*Administration Guide*」を参照してください。
- データセット命名基準
z/OS マスター カタログ内にデータセットを登録する必要はありません。
- CA-OPS/MVS ロード モジュールへのアクセス
STEPLIB、LINKLST、または LPALIB である必要があります。STEPLIB の方法を使うと、通常はインストールが速くなります。

- ロードライブラリの APF 権限付与
LINKLST ライブラリをコピーするか、SYS1.OPS.CCLXLOAD に動的に権限を付与することによって、IPL を実行しなくても済みます。
- TSO コマンド権限
製品がダウンしているときに、CA OPS/MVS の TSO コマンド(たとえば OPSCMD など)を実行する場合にのみ必要です。
- OPSMAIN、OPSECF、OPSOSF および OPSUSS 用のセキュリティユーザ ID およびデータセットアクセス。セキュリティシステムがある場合、それらが必要です。
- ユーザ ID に TSO OPER 権限を付与します。
- この権限は ADDRESS OPER パネル、OVEVIEW 6 パネル、または OPSVIEW 1 パネルからの z/OS コマンドの発行や、OPSIVP OPS/REXX プログラムの実行などを行うすべてのユーザ ID に付与される必要があります。
- CA ACF2 のコマンド制限リスト
- CA ACF2 を実行していてコマンド制限リストを使用する場合、補助コマンドが含まれない限り OPSVIEW は機能しません。
- サブシステム ID
サブシステム ID (OPSS のこと) は、parmlib ライブラリに存在しない場合は動的に挿入されます。
- MSF オプションコンポーネントの VTAM の定義
MSF で必要ですが、CA OPS/MVS のその他では必要ありません。個別メンバを使用する場合、定義は VTAM を再起動せずに追加できます。
- EPI オプションコンポーネントの VTAM の定義
上記と同じです。
- UEHURSVD フィールドの IMS AOI exit としての使用
問題となる可能性があります。 [CA サポート](#)にお問い合わせください。
- CCS for z/OS インストール済み
必須です。

インストール後の考慮事項

CA OPS/MVS スターテッド タスクが正常にインストールされ、開始されたら、以下の点について考慮する必要があります。

- CA OPS/MVS を調整して、特有のワークロードおよび処理要件が処理できるように最適化することは重要です。

注: 詳細については、「*CA OPS/MVS Event Management and Automation Administrator Guide*」および「*CA OPS/MVS Event Management and Automation Parameter Reference*」を参照してください。

- Web アプリケーションとサーバ アプリケーションのインストールおよび設定後、OPSLOG WebView セッションをこの形式の URL で開始することによって、Web ブラウザから OPSLOG WebView GUI にアクセスできます (リソース 5 を参照)。

`http://hostname.domain:port/applname`

`hostname` および `domain`

`hostname` および `domain` は IP アドレスです。数値の IP アドレスがわかる場合、その数値を使用してもかまいません。

`port`

HTTP (ブラウザ) アクセス用に定義する IP ポート番号です。デフォルトのポート 80 を定義する場合、URL から省略できます。

`applname`

`applname` は、この章の「Web アプリケーションの設定」で説明されているように、PASS ステートメント内で定義されます。

(新規関連グループ 1)

[Web アプリケーションの設定 \(P. 186\)](#)

パラメータライブラリメンバのカスタマイズ

CA MSM を使用して CA OPS/MVS を設定した場合、REXX ファイル OPSSXP00 (CCLXCNTL データセット内にあります) を使用して、手動で追加のパラメータを指定するか、既存パラメータをオーバーライドできます。ファイル REXX OPSSSC00 (CCLXCNTL データセット内にもあります) は、CA MSM によって自動的に保守されるので、変更しないでください。

OPSSSC00

CA MSM で指定されたパラメータが含まれます。決して手動で変更しないでください。

OPSSXP00

CA MSM を使用して製品を設定した場合に追加パラメータの指定に使用できるスケルトンコードが含まれます。

CA MSM を使用せずに CA OPS/MVS を設定した場合、CNTL データセットのメンバ OPSSPA00 にすべてのカスタマイズパラメータが含まれます。

OPSSPA00

CA MSM を使用せずに設定した CA OPS/MVS の設定のすべてのパラメータが含まれます。

CA OPS/MVS parmlib メンバのカスタマイズの詳細は、「*CA OPS/MVS Parameter Guide*」を参照してください。

OPSVIEW 機能を TSO で使用できるようにする

少なくとも CA-OPS/MVS の保守および管理の担当者に OPSVIEW が利用可能にしておく必要があります。また、ほとんどの場合には、コンソールにアクセスできるすべてのユーザが OPSVIEW を使用できるようにすることをお勧めします。

OPSVIEW データセットを TSO ユーザが使用できるようにする方法

1. ISPF ベースのすべてのアプリケーションと同様に、ライブラリと、ISPF/PDF の標準配布ライブラリを連結(またはコピー)します。
2. 以下の方法のいずれかで、OPSVIEW データセットに対して動的アクセスを提供します。
 - OPSVIEW ユーザが TSO にログオンするときに、OPSVIEW ISPF 関連のデータセットを割り当てます。
 - ユーザが OPSVIEW を起動したときに動的にアクセスを提供します。

SYS1.OPS.SAMPLES データセットの OPSVLBDF メンバには、OPSVIEW が起動されたときに OPSVIEW ISPF 関連のデータセットを動的に割り当てるための、カスタマイズ可能なサンプルが含まれています。この REXX EXEC は、TSO/E READY プロンプトから起動することも、ISPF で OPS/REXX または TSO/E REXX EXEC として起動することもできます。この REXX EXEC は ISPF LIBDEF サービスを使用して、以下の ISPF 関連の DD を割り当てます。

DD 名	データセット名	説明
SYSHELPENU	SYS1.OPS.CCLXHENU	TSO ヘルプ メンバ
ISPMLIB	SYS1.OPS.CCLXMENU	メッセージライブラリ
ISPPLIB	SYS1.OPS.CCLXPENU	パネルライブラリ
ISPTLIB	SYS1.OPS.CCLXTENU	ISPF コマンド テーブル
ISPTABL	一意のテーブル出力データセット、 またはユーザの ISPF プロファイル データセット名のどちらか	ISPF テーブル出力データセット
ISPSLIB	SYS1.OPS.CCLXSENU	ISPF ファイルのカスタマイズ スケルトン
STEPLIB	SYS1.OPS.CCLXLOAD (注を参照)	プログラムロードライブラリ
SYSEXEC	SYS1.OPS.CCLXEXEC HLQ.USER.REXX	ベース REXX プログラム ユーザが修正可能な OPS/MVS REXX プログラム

DD 名	データセット名	説明
SYSPROC	SYS1.OPS.CCLXCLS0	CLIST ライブラリ
OPSEXEC	SYS1.OPS.CCLXOPEX	コンパイル済み OPS/REXX プログラム(オプション。OPSVIEW のパフォーマンスが大幅に改善されます)

重要: OPSVIEW が正しく機能するよう、OPS/MVS ロード ライブラリを STEPLIB または LINKLIST に配置する必要があります。

3. OPSVLBDF に対して TSO/E の呼び出しシーケンスを使用すると、EXEC で以下の機能も実行できます。
 - CA OPS/MVS のコンパイル済み REXX データセットを OPSEXEC ddname に対して割り当て、および解放する。
 - CA OPS/MVS の REXXDDNAME パラメータを使用して、SYSEXEC ではなく OPS/REXX に ddname を提供すると、OPS/REXX ソースプログラムのデータセットを割り当ておよび解放することもできる。
4. メンバ OP6UEXIT を hlq.CCLXSAMP からユーザの hlq.USER.REXX へコピーします。
5. (オプション)既存の ISPF メニューの選択肢の 1 つとして OPSVIEW を追加します。ISPF パネルの &ZSEL 変換セクションで、OPSVIEW を起動するための以下の行を追加します。

```
&ZSEL = TRANS( TRUNC ( &ZCMD, '.' )
               S, 'CMD(OPSV)'
```

これで、OPSVIEW 機能を TSO で使用できるようになりました。

OPSVIEW データセットの使用上の注意

以下のリストは、OPSVIEW データセットの使用情報を示します。

- 複数のライブラリを連結する場合、指定された **ddname** のすべてのライブラリの **RECFM** が一致する必要があります。
- REXX プログラムを暗黙的に呼び出すために、**SYSEXEC ddname** が検索されます。この **ddname** にインストールライブラリまたはユーザ REXX ライブラリを連結できます。REXXDDNAME 製品パラメータに SYSEXEC 以外の値を設定している場合、SYSEXEC の代わりにその値を使用してください。
- システムリンクリストに **SYS1.OPS.CCLXLOAD** を指定する場合、**STEPLIB ddname** は必須ではありません。
- **CA OPS/MVS CCLXLOAD** ライブラリを **LPA** に移動し、それを **STEPLIB** または **LINKLIST** から削除する場合、**ISPTCM** テーブルを更新して、**CA OPS/MVS TSO** コマンドプロセッサ名を追加し、変数プールフラグをオンにします。
- **OPSVIEW CLIST OPPRIMOP** には、デフォルトの割り当てデバイス **SYSDA** の名前が記述されています。このデバイスの変更が必要な場合があります。
- **ISPTABL ddname** に割り当てたテーブル出力データセットも、**ISPTLIB** 連結内に記述する必要があります。

製品の起動

上記の項目を確認後、以下のコマンドで **CA OPS/MVS** を起動します。

```
START OPSMAIN, SUB=MSTR
```

製品の開始後の確認項目

CA OPS/MVS がアクティブになったら、以下のチェックを実行します。

- **DISPLAY ACTIVE** コマンドを発行して、**CA OPS/MVS** が少なくとも 1 つの **OPSOSF** アドレス空間を開始していることを確認します。

```
D A, OPSOSF
```
- コンソールから以下のコマンドを入力して、**OSF** をテストします。このコマンドでは、**OSFCHAR** パラメータのデフォルト値 (感嘆符 (!)) を使用しているものと仮定しています。

```
!OI OPSIVP
```

- OPSIVP を実行しているユーザ ID には、TSO OPER 権限が必要です。
 - OPSIVP OPS/REXX プログラムは REXX ライブラリにあります。CA OPS/MVS が「Program Not Found」というメッセージを返した場合、REXX ライブラリは、OPSOSF STC の SYSEXEC ddname では連結されません。
 - OPSIVP プログラムは CA OPS/MVS の WTO 機能および WTOR 機能をテストするため、コンソールで必ずメッセージまたはプロンプトを確認してください。WTOR に対しては応答する必要はありません。OPSIVP プログラムは、OPSCMD TSO コマンドを使用してコンソールコマンドを発行するための CA OPS/MVS 機能もテストします。OPSCMD コマンドで何らかのエラーがあると、OPSOSF のセキュリティ権限を示すデバッグメッセージが始動されます。
 - !OI OPSIVP コマンドでコンソールに出力が返されない場合は、Operator Server Facility (OSF) が機能していません。このような状況は通常、セキュリティ権限が十分でない、つまり自身のデータセットにアクセスするための権限を持っていないために OPSOSF のアドレス空間を開始できないことが原因で発生します。コンソールのメッセージをスキャンして、他に問題がないかチェックすることを忘れないでください。
- 自身の TSO ユーザ ID で OPSIVP プログラムを実行して、セキュリティ権限を確認してください。これを行うには、TSO READY 画面から以下のコマンドを発行します。

OI OPSIVP

- 以下のいずれかのオプションを使用して、CA OPS/MVS OPSVIEW のいくつかの機能をテストします。
 - TSO READY プロンプトで TSO セッションから以下のコマンドを入力します。
- OPSV
- ISPF の TSO セッションから以下のコマンドを入力します。

TSO OPSV

重要: 上記のコマンドで TSO のプレフィックスが付いたものは、ISPF でのみ発行できます。TSO のプレフィックスが付いたコマンドを TSO READY プロンプトから入力すると、エラーメッセージ「COMMAND TSO NOT FOUND」が発行されます。

- OPSVIEW Primary Options Menu で、[option 1]を選択して OPSLOG を表示します。SDSF LOG または SYSLOG に類似した表示ログが表示されます。表示が空白の場合は、CA OPS/MVS のメイン STC が非アクティブになっているか、またはエラーメッセージがコンソールに表示されている可能性があります。また、OPSVIEW オプション 4.1.1 にもアクセスする必要があります。ここでは CA OPS/MVS のすべてのパラメータが表示されます。
- この章の「OPSVIEW 機能を TSO で使用できるようにする」で実装したプロシージャを使用して OPSVIEW にアクセスします。

サンプル ルール セットのルールの無効化

サンプル ルールの自動有効化フラグは出荷時には OFF に設定されています。これは、CA OPS/MVS 起動時に AOF によって自動的に有効化されないようにするためです。

重要: サンプル ルール セットのルールは例であるため、すべてのシステムで機能するとは限りません。多くのルールは、有効化の前にカスタマイズされる必要があります。CA OPS/MVS を起動する前に、システム設定と競合する可能性のあるサンプル ルールを有効化していないことを確認してください。

サンプル OPSAOF コマンド ルールの有効化(オプション)

SYS1.OPS.SAMPLE.RULES のメンバ OPSAOF には、有用なサンプル コマンド ルールが含まれています。

OPSAOF コマンドでは、TSO が稼動していないときに、オペレータが AOF をコンソールで制御することができます。OPSVIEW オプション 4.5 は通常、AOF の操作を制御します。たとえば、アクティブなルール セットをすべて一覧で表示するには、MCS コンソールで以下のコマンドを入力します。

```
OPSAOF LIST
```

CA のデフォルトのルール セット命名規則を使用している場合は、ルール セットの 1 つが `SYS1.OPS.SAMPLE.RULES` になります。それ以外の場合は、`OPSAOF` を自身の製品ルール セットの 1 つにコピーします。`OPSAOF` のルールは、自動有効化フラグがオフの状態です。最初提供されるため、`CA OPS/MVS` の起動時に `OPSAOF` のルールは有効になりません。このため、このルールのインストールを完了するには、`OPSVIEW` オプション 4.5 を使用してこのフラグをオンにします。

注: ルールの有効化の詳細については、「*User Guide*」を参照してください。

第 7 章: オプション コンポーネントの設定およびインストール

このセクションには、以下のトピックが含まれています。

[別途ライセンスされている CA-OPS/MVS のコンポーネントのインストール方法 \(P. 147\)](#)

[オプション ベースコンポーネントのインストール方法 \(P. 148\)](#)

[別途ライセンスされたコンポーネントのタスク \(P. 148\)](#)

[オプションのベースコンポーネントのタスク \(P. 197\)](#)

別途ライセンスされている CA-OPS/MVS のコンポーネントのインストール方法

これらの手順は、CA OPS/MVS のベースコンポーネントではない別々にライセンスされた CA OPS/MVS のコンポーネントのインストール方法について説明します。このセクションの各手順は、これらの手順に記述されている特定のコンポーネントを使用するためのライセンスを取得済みの場合にのみ必要です。

- Multi-System Facility (MSF) の設定
- IMS Operations Facility のインストール
- CICS/TS 用 XTDOOUT CICS Operations Facility (COF) インターフェースのインストール
- CA NSM SSM CA OPS/MVS オプションのカスタマイズ
- Expert Systems Interface (ESI) のインストール
- OPSLOG WebView の環境設定

オプション ベース コンポーネントのインストール方法

これらの手順は CA OPS/MVS のオプション ベース コンポーネントのインストールについて説明しますが、これに従わなくてもかまいません。このセクションの各手順は、特定の手順の影響を受ける CA OPS/MVS のオプション機能を利用したい場合にのみ必要です。

- JES2 環境関数のインストール (JES2 のみ)
- JES2OFFSETSUFFIX で CPU 間のライブラリ共有の有効化 (JES2 のみ)
- JES3 インターフェースの設定
- 共有ファイル VSAM KSDS の定義
- UNIX System Services (USS) 機能のインストール
- EPI コンポーネント用の VTAM 端末の作成
- NetView インターフェースのインストール
- NetView Operator Facility (NOF) のインストール
- Tivoli OMEGAMON XE のインターフェースの設定
- MVS/QuickRef インターフェースのインストール
- CA 7 WA インターフェースの設定
- ハードウェア サービス (HWS) の設定
- Linux Connector インタフェース (LXC) の設定
- 一般データ セット出力の管理
- CA MIC にインターフェースを確立
- CA 7 Browse Log のオプションのメッセージ機能のインストール
- z/OS Automatic Restart Management Facility の設定

別途ライセンスされたコンポーネントのタスク

このセクションでは、別々にライセンスされた CA OPS/MVS のコンポーネントをインストールするために完了する必要があるタスクについて説明します。

Multi-System Facility (MSF) の設定

CA OPS/MVS のオプションの Multi-System Facility (MSF) 機能は、複数の z/OS マシンで稼動している複数の CA-OPS/MVS 間における通信を実現します。この機能は、複数の CA OPS/MVS と CA Automation Point 間における通信も提供します。

MSF のライセンスを取得している場合は、OPS/REXX の startup EXEC で INITMSF パラメータを YES に設定する必要があります。

CA MSM を使用して MSF を設定した場合、そのパラメータの一部はすでに、CNTL データセットのパラメータファイル OPSSSC00 に自動生成されています。MSF パラメータをさらに調整する必要がある場合は、CNTL データセットのファイル OPSSXP00 で設定します。

CA MSM 設定では、システム定義 (MSF DEFINE) は自動生成されません。

CA MSM を使用 *せず* に CA OPS/MVS を設定した場合、パラメータは CNTL データセットのファイル OPSSPA00 に保持されます。

サンプル MSF パラメータ

INITMSF

MSF インターフェースが初期化されます。

INITCCI

リモート MSF が CCI タイプとして定義されている場合に CAICCI インターフェースがアクティブ化されるかどうかが決まります。

MSFLOGMODE

すべての MSF APPC セッションに対するデフォルトの VTAM LOGMODE 名が指定されます。

MSFRESTARTREXX

MSF の再起動後に MSF 環境を設定するために記述した OPS/REXX プログラムの名前を指定します。

MSFSYSWAIT

MSF を使用する CA OPS/MVS コンポーネントのデフォルトの待ち時間が指定されます。

SYSID

MSF または MSF ネットワーク内のローカル システムの名前が定義されます。

セッション プロトコルの設定

CA OPS/MVS のコピー間の通信で使用するセッション プロトコルには、次の 2 種類があります。

- 論理ユニット (LU) 6.2 のセッション プロトコル セット (APPC)

CA OPS/MVS のネイティブ MSF は、LU 6.2 のセッション プロトコル セットのみ使用します。

- CAICCI が提供する通信サービス。CAICCI は LU2、XES、XCF、および TCP/IP に対するセッション プロトコルを提供します。

以下のセクションでは、MSF を設定して LU 6.2 および CAICCI を使用方法について説明します。

重要: CAICCI の LU2 プロトコルを使用することはお勧めしません。

LU 6.2 (APPC) セッション プロトコルを使用するための MSF の設定

MSF をインストールするには、以下の手順に従います。

- SYS1.VTAMLST にアプリケーション定義 (APPL) ステートメントを追加して、VTAM に各 z/OS システム上の CA OPS/MVS を定義します。
- 各システム上で VTAM クロスドメインのリソース環境を定義して、アプリケーションが相互に通信セッションを行えるようにします。

VTAM APPL ステートメント – VTAM に CA-OPS/MVS を定義する

各システムで CA OPS/MVS が必要とするのは、以下の形式を使用する 1 つの APPL ステートメントのみです。

```
netname APPL  APPC=YES,  
              AUTH=ACQ,  
              AUTOSES=1,  
              DSESLIM=3,  
              DMINWNL=1,  
              DMINWNR=1,  
              MAXPVT=512K,  
              MODETAB=modetab,  
              PARSESS=YES,  
              PRTCT=vtampswd
```

上記の APPL ステートメントのパラメータにおける有効な値の詳細については、VTAM ドキュメントを参照してください。

以下の例では、SYS1.OPS.CCLXCNTL データセットの OPSAPPL メンバに APPL の定義が指定されています。ここでは、3 つの z/OS システム (A、B、および C) を接続した 1 つのネットワークがあり、すべてのシステムが相互にクロスドメインセッションをサポートできると仮定しています。

例 1: この APPL ステートメントは、システム A の SYS1.VTAMLST にのみ示されます。

```
OPSMAINA APPL  APPC=YES,  
              AUTH=ACQ,  
              AUTOSES=1  
              DSESLIM=3  
              DMINWNL=1,  
              DMINWNR=1,  
              MODETAB=MTLU62,  
              PRTCT=OPSMVS,  
              MAXPVT=512K,  
              PARSESS=YES
```

例 2: この APPL ステートメントは、システム B の SYS1.VTAMLST にのみ示されます。

```
OPSMAINB APPL  APPC=YES,  
                AUTH=ACQ,  
                AUTOSES=1  
                DSESLIM=3  
                DMINWNL=1,  
                DMINWNR=1,  
                MODETAB=MTLU62,  
                PRTCT=OPSMVS,  
                MAXPVT=512K,  
                PARSESS=YES
```

例 3: この APPL ステートメントは、システム C の SYS1.VTAMLST にのみ示されます。

```
OPSMAINC APPL  APPC=YES,  
                AUTH=ACQ,  
                AUTOSES=1  
                DSESLIM=3  
                DMINWNL=1,  
                DMINWNR=1,  
                MODETAB=MTLU62,  
                PRTCT=OPSMVS,  
                MAXPVT=512K,  
                PARSESS=YES
```

VTAM クロスドメイン環境の定義

クロスシステムサービスを使用するには、接続先システムのクロスドメインリソースを定義する必要があります。

クロスドメインリソースを定義する方法

1. 接続先システムのクロスドメインメンバ名を見つけます。
2. クロスドメインリソースメンバを作成するか、接続先システムに既存クロスドメインリソースメンバがあればそれを変更します。このメンバにおいて、クロスドメインリソースマクロを使用して **CA OPS/MVS** が存在するシステムを指定します。

たとえば、コピー **OPS1** が **SYSTEMA** に存在し、**OPS2** と名づけられた別のコピーが **SYSTEMB** に存在する場合、**SYSTEMA** には以下のクロスドメインリソースが必要です。

```
OPS2 CDRSC CDRM=SYSTEMB, ISTATUS=ACTIVE
```

3. システムごとに上記の手順を繰り返します。
VTAM クロスドメイン環境が定義されました。

LU 6.2 VTAM モード テーブル エントリの定義

MSF に対して **APPC** セッションを使用している場合は、**LU 6.2** モード テーブル エントリを作成する必要があります。

LU6.2 モード テーブル エントリを定義する方法

1. **LU 6.2** セッション パラメータを持つモード テーブル エントリがすでに含まれている、既存の **VTAM** モード テーブルを検索します。
2. このようなエントリが見つからない場合は、新しい **LU 6.2** モード テーブル エントリを含めるための既存のモード テーブルを選択します。
3. **LU** 定義に関連付けられるモードに対して、新しいモード テーブル エントリを追加します。
4. モード テーブルをアセンブルおよびリンクエディットし、**SYS1.VTAMLIB** に対してロード モジュールを追加します。

これで **LU 6.2** **VTAM** モード テーブル エントリが定義されました。

ADDRESS OPSCTL MSF DEFINE - CAICCI を使用した MSF 接続の設定

CAICCI を使用する際、リモートシステムを定義するための ADDRESS OPSCTL MSF DEFINE コマンド指定に特別なルールがあります。APPLID キーワード値には、リモートシステムの CAICCI システム識別子 (*sysid*) を指定する必要があります。

たとえば、リモートシステムの *sysid* が、OPSS0B の MSF ID を持つシステム上で CCI0B の場合、ADDRESS OPSCTL MSF DEFINE コマンドは以下のとおりです。

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0B) APPLID(CCI0B) CCI"  
CCI0B
```

システム B 上にある CAICCI の *sysid* が識別されます。

MSF は、指定した値が有効であることを確認します。

注: ADDRESS OPSCTL MSF DEFINE コマンドでは、キーワード CCI はリモートシステムにのみ使用できます。

以下の例では、MSF 接続を定義する複数のシナリオを説明します。

例 1: CCI をローカルシステムとして定義する

この例では、CCI キーワードは使用されません。APPLID キーワードを使ってローカルシステム ID を CAICCI に指定します。

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0A) APPLID(CCI0A)"
```

例 2: VTAM および CCI を同時に使用する

- ローカル定義:

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0A) APPLID(OPSAPLID)"
```

- APPC 接続へのリモート定義:

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0BVT) APPLID(OP2APLID) APPC"
```

- CCI 接続へのリモート定義:

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0B) APPLID(CCI0B) CCI"
```

例 3: CCI のみを使用する

- ローカル定義:

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0A) APPLID(CCI0A)"
```
- リモート定義:

```
ADDRESS OPSCTL "MSF DEFINE MSFID(OPSS0B) APPLID(CCI0B) CCI"
```

CAICCI による通信の有効化

CAICCI はシステム間通信を採用しており、これにより CA ソリューションは、CAICCI プロトコル対応可能なシステムを経由してほかの CA ソリューションと通信できます。これにより、CA ソリューションは大規模なアプリケーションの変更を行うことなく、迅速かつ効率的に新しいネットワーク プラットフォームに適応できます。

CAICCI を通して、CA OPS/MVS は CAICCI サービスのサブスクリバとなり、CAICCI を介してすべての通信を扱えるようになります。CA OPS/MVS がローカルシステムのサブスクリバになると、そのシステムおよびリモートシステム上に存在するその他すべての CA OPS/MVS システムが、システム間機能を使用できます。

CAICCI ルーチンは CA z/OS サービスコード W411 に統合されています。CAICCI のインストールについての情報およびその特色と機能の詳細については、CCS for z/OS のドキュメントを参照してください。

CAICCI 関連パラメータの指定

CAICCI クロスプラットフォーム通信サービスを利用するには、パラメータ設定の以下のガイドラインに従います。

- INITCCI パラメータ値を YES に設定します。デフォルトは NO です。
- MSFDELAY パラメータ値を最低でも 10 に設定します。

システム上で VTAM がアクティブになる前に MSF CCI リンク経由でシステム間通信を行いたい場合、製品初期化中に MSFNONVTAMONLY パラメータ値を YES に設定します。

CA OPS/MVS の初期化後、VTAM が起動してから NO に設定できるように MSFNONVTAMONLY パラメータを変更することが可能です。これで、(すでに確立済みの CCI 接続に加えて) APPC を使用して他のシステムに接続できます。

VTAM がアクティブになる前に (VTAM を後ほど利用する目的で) CCI プロトコルを使用する場合、ローカル システムの MSF DEFINE ステートメント内で有効な VTAM APPLID を指定する必要があります。CA OPS/MVS の起動時に APPLID は非アクティブであり、通信は CCI を介して確立されます。ただし、VTAM がアクティブ化になると指定されたシステムに他のシステムが APPC 接続を介して接続できるので、その場合は VTAM APPLID が必要となります。

注: CAICCI パラメータの詳細については、「*Parameter Reference*」を参照してください。

IMS Operations Facility のインストール

CA optional IMS Operations Facility (IOF) は IMS コマンドおよび非送信要求メッセージを IMS AOI の exit ポイントから取得します。CA OPS/MVS は AOI の exit を、開始する各 IMS に動的に挿入します。IMS にはサンプルの AOI exit がありますが、これはインストールが必要な場合もあります。CA OPS/MVS AOI exit は、ユーザ独自の AOI exit の使用を妨げるものではありません。

各 IMS システムに対して CA OPS/MVS パラメータ `IMSnINSTALLEXITS` を YES (デフォルト値) に設定して、IMS の初期化時に IOF exit をインストールできます。IMS の開始前にこのパラメータを NO に設定すると、IOF exit のインストールがバイパスされます。

注: IMS の前回の初期化時に IOF exit がインストールされている場合、このパラメータを NO に設定しても、これらの exit はアンインストールされません。この exit を削除するには、IMS の再起動が必要です。IOF exit がインストールされていなくて、IMS がすでに初期化されている場合は、IMS がアクティブな状態でこのパラメータを YES に設定すると、次のメッセージ イベントで、IMS システムから IOF exit が自動的にインストールされます。

注: IMS WTOR を使用しない IMS コマンド発行に対して IOF バッチ メッセージ処理 (BMP) を使用することは、IOF AOI exit がインストールされているかどうかに影響されません。ここでは、2 種類の AOI exit があります。ひとつは IMS AOI のオリジナルの exit である DFSAOUE0 です。これは DB/DC または DCCTL-only システムでのみ呼び出されたもので、TYPE 1 の exit として示されます。もう 1 種類の AOI exit は DFSAOE00 です。これはすべての IMS システムタイプ (DB/TM、TM-only、および DBCTL-only) で呼び出されるもので、TYPE 2 の exit として示されます。現在、DBCTL-only の IMS システムは、IOF では完全にはサポートされていません。この IMS に対しては、OPS/MVS パラメータの `IMSnCHAR` を、DBCTL リージョンの CRC (コマンド認識文字) 以外の文字に設定することをお勧めします。

独自の AOI exit (TYPE 1 または TYPE 2 のいずれかの exit) がインストールされていない場合は、OPS.CCLXASM ライブラリで提供されているサンプルの exit をインストールする必要があります。IMS RESLIB を参照して、AOI exit がインストールされているかどうか確認します。RESLIB に exit がない場合は、該当するサンプルの exit をインストールする必要があります。OPS.CCLXASM ライブラリでは、サンプルの TYPE 1 exit のメンバ名が OPSAOUE0、サンプルの TYPE 2 の名前が OPSAOE00 になっています。これらのサンプル メンバは、RESLIB にアセンブルしてリンクエディットする必要があります。正しいリンクエディットステートメントは、各メンバの最後に提示されています。OPS.CCLXCNTL ライブラリの OPSAOUE0 メンバと OPSAOE00 メンバには、JCL および関連する使用方法が含まれています。

IMS Transaction Manager (TM) 環境では、複数の exit タイプを実現すると、CA OPS/MVS ユーザが考慮しなければならない共存の複雑さが増大します。

複雑化の要因への対応のルール

IOF は、複雑化の要因に対応するために以下のルールを使用します。

■ exit の組み合わせ

IMS は TYPE 1 exit と TYPE 2 exit の組み合わせを持つ場合があるため、以下のガイドラインに従います。TYPE 2 exit は、TYPE 1 exit の呼び出しを完全に制御していることに注意してください。

- ユーザまたは OEM TYPE 1 exit を有しているが、TYPE 2 exit はない場合。CA OPS/MVS に指定された TYPE 2 exit がインストールされる必要があります。

ユーザまたは OEM TYPE 1 exit が呼び出されると、OPSMMAIN が実行されていない場合でも、提供される OPSAOE00 アセンブラソースコードにマイナーな変更が必要となります。この変更を行うための手順がソースコードに含まれています。IMS RESLIB にプログラムをアセンブルおよびリンクエディットする前に、この変更を加えてください。

- ユーザまたは OEM TYPE 2 exit を有しているが、TYPE 1 exit はない場合。この場合 IOF TYPE 2 exit は、IOF を自動化させたい IMS システムに動的に挿入されます。独自の AOI exit の使用は妨げられず、既存の exit を呼び出す事が可能です。
- ユーザまたは OEM TYPE 2 exit を有しており、さらにユーザまたは OEM TYPE 1 exit もある場合。この場合、IOF TYPE 2 exit は TYPE 2 exit の応答コードを監視します。応答コードは TYPE 1 exit が制御を得るかどうかを決定します。これにより、ユーザは独自の exit の TYPE 1 呼び出しを制御できます。マルチセグメントメッセージでは、TYPE 2 exit がユーザの TYPE 1 セグメントの制御を放棄する場合、IOF はセカンダリセグメントを確認しません。

要約すると、TM 環境に TYPE 1 exit と TYPE 2 exit のどちらもインストールされていない場合、IOF には独自の TYPE 2 exit をインストールする必要があります。CA OPS/MVS で指定された TYPE 2 exit、OPSAOE00 内の OPSAOE00 がアセンブル、リンク、およびインストールされる必要があります。これらの exit のうちどちらかがあれば、IOF によって独自の AOI exit または OEM AOI exit の使用が妨げられることはありません(以下の制限事項を参照)。

■ Exit の制限事項

IOF TYPE 1 exit には制限事項が 1 つあります。IOF は IMS UEHB (ユーザ Exit ヘッダ ブロック) 制御ブロック内にある UEHURSVD フィールドの末尾 4 バイトを使用します。そのため、ご使用のサイトの AOI exit がこの領域を使わないようにする必要があります。IMS で送付されるサンプル AOI exit はこの領域を使用しません。

IOF TYPE 2 exit には、IMS によって指定された AOE0WRKA AOI exit 作業領域に関する制限があります。IOF は 256 バイトの作業領域のうち、先頭の 72 バイトと末尾 20 バイトを使用します。独自に作成した TYPE 2 EXIT 内でこれらの領域を変更した場合、IOF がその領域と重なって独自の exit にエラーが発生する原因となる可能性があります。IOF TYPE 2 exit は、ユーザ独自の TYPE 2 exit または OEM TYPE 2 exit よりも必ず先に制御を行います。AOE0WRKA の作業領域については、「*IMS Customization Guide*」を参照してください。

IOF 用の CA OPS/MVS フックは、ユーザ/OEM TYPE 1 exit またはユーザ/OEM TYPE 2 exit による IMS メッセージの抑制や削除を許可しません。IMS メッセージの抑制、削除、またはその両方は、CA OPS/MVS メッセージルール内で実行される必要があります。

独自の TYPE 1 exit があり、<CA OPS/MVS によって指定された TYPE 2 exit、OPSAOE00 をインストールする必要がある場合、CA OPS/MVS が操作可能で INITIMS パラメータもオンになっているとき以外、IMS RESLIB より先にインストールしないでください。そうしないと、ユーザ TYPE 1 exit が呼び出されない原因となります。

制限事項に抵触する場合は、テクニカル サポート (<http://ca.com/support>) にお問い合わせください。

詳細については、「*IMS Customization Guide*」および「*IMS Application Programming: Transaction Manager*」を参照してください。

INITIMS パラメータの設定

INITIMS パラメータは、IOF のアクティブ化を制御します。INITIMS のデフォルトは NO です。データセンタが IMS/DB のみのショップの場合は、INITIMS を NO の設定のままにして、起動時の IMS SVC の認識問題を回避するようにします。

INITIMS パラメータを YES に設定できるのは、IOF のライセンスを取得しているお客様だけです。また、このパラメータを YES に設定できるのは、製品の初期化のときだけです。IOF のライセンスを取得しているけれども、IMS を使用していない z/OS イメージを所有しているお客様の場合は、これらのシステムでパラメータを NO に設定することによって、CPU およびストレージのパフォーマンスにおけるメリットが得られます。

INITIMS の値が NO の場合は、OPSPARM/OPSPRM SHOW(ALL) コマンドプロセッサで、出力に IMS パラメータが含まれません。INITIMS を NO に設定すると、OPSVIEW オプション 4.1.1 では IMS パラメータの表示が抑制されます。この特性は設計上のもので、ストレージを少なくして、パフォーマンスを改善することを目的として実施されています。INITIMS が YES に設定されている場合、IMS パラメータは OPSPRM OPS/REXX 関数の出力、OPSPARM コマンドプロセッサの出力、および OPSVIEW オプション 4.1.1 の表示に示されます。

CA OPS/MVS の *Identify IMS* 関数 (OPSVIEW オプション 7.4) にアクセスすると、IMS Operation Facility に必要なパラメータカードを作成できます。この関数のバッチバージョンは、SAMPLES ライブラリの BATCHPRM メンバにあります。

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

IOF インストール パラメータ

IMS の制御リージョンに関連する CA OPS/MVS パラメータ (IMS1ID や IMS1DUPLICATE など) は、CA OPS/MVS のインストール時に設定しなければならないことがあります。これらのパラメータの詳細については、「*Parameter Reference*」を参照してください。

IOF の操作

IOF は、インストール後に、CA OPS/MVS のその他の機能の拡張セットとしてのみ明確になります。

BMP リージョンから発行される IMS コマンド

IOF は BMP リージョンを使用して、IMS コマンドを発行し、コマンドレスポンスを取得することができます。この機能により、IMS コマンドの発行が必要な場合にはいつでも、CA OPS/MVS が IMS WTOR メソッドを使う代わりに方法が提供される事になります。

IMS コマンドに対して IOF が BMP リージョンを使用すると、次のメリットがあります。

- IOF は、IMS WTOR を待機せずに、ほとんどの IMS コマンドを発行できます。
- コマンドのレスポンスについて、信頼性、効率ともに向上します。これは、コマンドの出力が (IMS WTOR から発行されたコマンドのように) コンソールに自動的にルーティングされず、サブシステム インターフェース (SSI) を介してもルーティングされないためです。

注:

- OPSCMD および ADDRESS OPER のキーワード BMPCMDOUT を使用して、現行のコマンド 出力をオプションでエコーすることができます。使用できる値は OPSLOG、WTO、または NONE です。
- OPSCMD および ADDRESS OPER のキーワード IMSREPLY は、現行のコマンドを BMP に強制的にバイパスさせて、IMS WTOR を介してコマンドを発行します。

これらのキーワードの詳細については、「*Command and Function Reference*」を参照してください。

BMP リージョンの設定

CA OPS/MVS が BMP リージョンを使用する機能を利用して IMS コマンドを発行するには、BMP リージョンを設定する必要があります。

BMP リージョンを設定する方法

1. IMS パラメータの AOIS を、デフォルト値の N 以外の値に設定します。有効な値の一覧については、IMS のインストール ガイドを参照してください。
2. BMP TRAN を IMS に定義します。

CA OPS/MVS BMP トランザクションおよびアプリケーションを IMS に定義するには、PSBGEN を実行する必要があります。OPS.CCLXCNTL データセットの OPSINBMP メンバには、サンプルの制御ステートメントが用意されています。

3. すべてのコマンドを発行するように BMP TRAN に権限を付与します。

IMS での必要に応じて、セキュリティパッケージを介してこのトランザクションに権限を付与します。IMS Security Maintenance Utility (SMU) を使用している場合は、SMU を実行して、すべてのコマンドを発行する権限を持つよう BMP トランザクションに権限を付与する必要があります。サンプルの制御ステートメントは、OPS.CCLXCNTL のメンバ OPSINBMP にあります。

4. BMP スタートアップ タスク JCL のバッチを作成します。

IMS PROCLIB のメンバ IMSBATCH を使用して、使用している RESLIB が、対象とする制御リージョンの RESLIB と一致することを確認します。CA OPS/MVS のロード モジュール ライブラリを、STEPLIB の連結に追加します。

CA OPS/MVS の IMSnBMPSTC パラメータを、BMP スタートアップ タスク JCL のメンバ名に設定します。

5. CA OPS/MVS のパラメータを指定します。

IOF がコマンドの発行で使用する BMP リージョンのアクティブ化または非アクティブ化を制御するには、これらの CA OPS/MVS パスワードを設定する必要があります。

- IMSnBMPSTC
- IMSnINITBMP
- IMSnPSBNAME
- IMSnTRANNAME

これらのパラメータの詳細については、「*Parameter Reference*」を参照してください。

BMP に対する WTOR 出力表示

WTOR の代わりに BMP を使用している場合、IMS が IMS コマンドの出力を表示する方法には 2 つの小さな違いがあります。

- コマンドが WTOR から発行されると、その出力では各行の最後に IMS ID が追加されます。IMS は BMP を使用して同じ方法で出力を表示しますが、異なる点は各行末に IMS ID は追加されず、プレースホルダとしてピリオドが追加されることです。
- IMS BMP は以下のコマンド出力を異なる方法で扱います。

```
"DFS058I hh:mm:ss cmd COMMAND {COMPLETED|IN PROGRESS EXCEPT....}"
```

コマンドの結果として、例外が発生しないが DFS058I メッセージ(たとえば、COMMAND COMPLETED や IN PROGRESS)となる場合、IMS は空白行を BMP に示します。この空白行により、BMP は DFS058I COMMAND IN PROGRESS というメッセージを返します。

例外(たとえば、START COMMAND COMPLETED EXCEPT PROGRAM XYZ)が発生した場合、出力メッセージは同じですが、各行末に IMS ID を追加しません。

IMS Type-2 メッセージに関する考慮事項

IMS Type-2 メッセージプロトコルは、OPS/MVS システムから IMSPLEX のメンバである任意の IMS システムに通信するために使用されます。この通信は、ローカル (OPS/MVS からアクティブな IMSPLEX に通信する機能を持つ同じ LPAR の上の IMS システムへ) か、またはクロスシステム (OPS/MVS が別の OPS/MVS システムへの MSF 接続を使用して IMS コマンドを送信し、そこから IMSPLEX に送信する) です。発行側の OPS/MVS は、直接 IMS と通信しません。ターゲット OPS/MVS は IMSPLEX マネージャに接続できる必要があります。

この機能が使用される場合、2 つの IBM モジュール (CSLSDR00 と CSLSRG00) が IMSPLEX に接続可能な OPS/MVS システムで利用可能である必要があります。これらのモジュールは、IMS RESLIB で IBM によって提供されます。以下に示す選択が可能です。

- それらを LNKLST に追加する
- OPS Loadlib にコピーする
- 元の IMS RESLIB に置いたままで、STEPLIB チェーンに連結する
- 別個の Loadlib に分離した後に連結する。

モジュールは、IMS 9 と下方互換です。最も高い IMS リリースのモジュールを使用することで、異なるリリースレベルの IMS システムが混在するサイトにサービスを提供できます。

特定または固有の IMSPLEX 設定または起動オプションに対する CA OPS/MVS の要件は存在しません。IMSPLEX 自体はサイト標準に従って調整され、名前は実行時に CA OPS/MVS コマンドに提供されます。

Type-2 メッセージおよびコマンドの IMSPLEX セキュリティに関する考慮事項については、IBM のマニュアル「*IMS Vnn IMSplex Admin Guide*」を参照してください。関連分野は、Common Service Layer (CSL) のコンポーネント SCI および OM との CA OPS/MVS インターフェースです。

CICS/TS に対する XTDOUT COF インターフェースのインストール

CICS/TS インターフェースに関連する事項を以下に示します。

- CICS グローバル exit (XTDOUT) を使用して、一時データの書き込み要求がすべてインターセプトされます。CA OPS/MVS は、一時データのキュー名と、AOF 処理に指定されているキュー名のリストを照合します。
- 一致したキュー名に送信されたメッセージは、ルール処理のために AOF に転送されます。これにより、メッセージの抑制および書き換えも可能になります。一致しないキュー名に送信されたメッセージは、exit によって無視されます。
- ADDRESS OPSCTL COF コマンドを使用して、指定されたキュー名の一覧を作成および保守します。
- 一時的なデータ メッセージをインターセプトするには、標準の CICS DCT を変更する必要はなく、特定の宛先の選択を動的に変更することができます。
- 各 CICS リージョンに対して、個別のキュー名リストを 1 つ作成し、未定義の CICS リージョンに対しては一般的なデフォルトのリストを使用することができます。

XTDOUT COF インターフェースをインストールする方法

1. SYS1.OPS.CCLXLOAD から、ロード モジュール OPCITDCN を CICS DFHRPL 連結内のライブラリへコピーします。

モジュールは、AMODE=31 および RMODE=ANY にリンクされます。

2. CICS RDO 機能を使用して、CICS にトランザクションおよびプログラムを定義します。

```
DEFINE GROUP(OPXTDOUT) PROGRAM(OPCITDCN)
    DATALOCATION(ANY) EXECKEY(CICS)
    LANGUAGE(ASSEMBLER) RESIDENT(YES)
    DESCRIPTION(OPS/MVS XTDOUT GLOBAL EXIT)
DEFINE GROUP(OPXTDOUT) TRANSID(OPTD) PROGRAM(OPCITDCN)
    TASKDATAKEY(CICS) TASKDATALOC(ANY)
    DESCRIPTION(OPS/MVS XTDOUT EXIT CONTROL)
INSTALL GROUP(OPXTDOUT)
ADD GROUP(OPXTDOUT) LIST(DFHLIST)
```

XTDOUT EXIT コードは OPCITDCN プログラムに含まれ、OPCITDEX という名前
でこのモジュールでエントリ ポイント アドレスとして有効になります。EXIT プ
ログラムは CICS に定義される必要はありません。

3. CICS 端末から OPTD を呼び出すか、または z/OS コンソールから MODIFY コマンドを使用して、XTDOUT exit を使用できるようにします。必要なときに、CICS の初期化で自動的に exit を有効にするために、CICS PLTPI のステージ 3 に OPCITDCN を追加することができます。
4. INITCOF パラメータおよび CICS AOF パラメータを YES に設定して、CICS メッセージの AOF 処理をアクティブ化し、デフォルトの一時データキュー名のリストを少なくとも 1 つ定義します。

```
X = OPSPRM('SET', 'INITCOF', 'YES')
X = OPSPRM('SET', 'CICSAOF', 'YES')
ADDRESS OPSCTL "COF DEFINE JOBNAME(DEFAULT)",
               "DESTIDS(CSMT, CSSL, CADL, ...)"
```

これで、CICS/TS に対して XTDOUT COF インターフェースがインストールされました。

AOF ルールによって一時データのキューメッセージの抑制を可能にする詳細については、「*Parameter Reference*」の CICSDELETE パラメータの説明を参照してください。

OPTD トランザクションを使用し、次のように 1 文字のコマンドで OPTD を呼び出して、任意のタイミングで exit を無効、および再有効化することができます。

- OPTD E-XTDOUT exit を有効にします (デフォルト コマンド)
- OPTD D-XTDOUT exit を無効にします
- OPTD S-XTDOUT exit のステータスを表示します
- OPTD T-一時的なデータキューに対してテストメッセージを発行します
- OPTD H-定期的な CICS ステータス メッセージ OPS34200 を発行します

CA NSM SSM CA-OPS/MVS オプションのカスタマイズ

このセクションでは、CA NSM SSM CA OPS/MVS Option 製品に対する CA OPS/MVS のカスタマイズについて説明します。CA NSM SSM CA OPS/MVS Option 製品をインストールする前に、CA OPS/MVS をインストールしてカスタマイズしておくことをお勧めします。CA OPS/MVS でサポートされているすべてのリリースで、CA OPS/MVS と CA NSM SSM CA OPS/MVS Option 間の通信方法として Agent Technology エージェントを使用することができます。

Agent Technology エージェントを使用する方法

1. CA OPS/MVS をインストールした後、以下のパラメータをカスタマイズします。

- CAUNICONFIGSET - Agent Technology エージェント インターフェースのインストール時に CA OPS/MVS および CA NSM SSM CA OPS/MVS Option に対して指定した Agent Technology の設定名をこのパラメータに設定します。設定データはほとんどの場合、CA OPS/MVS 製品の *prefix.CCLXCNTL* データセットのメンバ CFGSSMO にあります。ステートメント #CONFIGSET stateman: のコロンの後にある名前 OPSCNFG は、このパラメータで必要な名前です。デフォルト値はありません。

設定のステートメントには、使用する SNMP コミュニティ名、CA OPS/MVS の IP アドレスまたはホスト名、およびエージェントから SNMP トラップを受信する CA NSM SSM CA OPS/MVS Option のワークステーションも含まれています。

```
#CONFIGSET stateman:OPSCNFG
```

ここで、CAUNICONFIGSET パラメータは、CA OPS/MVS の初期化 REXX EXEC (通常は OPSSPA00) で、次のように設定されます。

```
OPSPRM('SET', 'CAUNICONFIGSET', "OPSCNFG")
```

- CAUNICONNECTWAIT - CA OPS/MVS のアドレス空間内で実行中の CA OPS/MVS サブタスクが、同じ z/OS イメージ上で実行中の Agent Technology に接続するために再試行する間隔が分単位で指定されます。この製品パラメータは、CA OPS/MVS の起動 OPS/REXX EXEC (通常は OPSSPA00) にあります。このパラメータには、0 ~ 120 までの任意の数値を設定できます。このパラメータは随時に変更できます。

デフォルト値: 0 (接続を試行しない)

推奨値: 2

- INITAWS - CA OPS/MVS および CA NSM SSM CA OPS/MVS Option を初期化するには、このパラメータを YES に設定します。

デフォルト値: NO

推奨値: YES

- CAUNIAGENT - CA OPS/MVS および CA NSM SSM CA OPS/MVS Option 製品を実行している CA NSM ワークステーションでの通信で、どの SNMP エージェントを使用するかが決定されます。

デフォルト値: AWS

推奨値: AWS

重要: CA-OPS/MVS のテクニカル サポートに指示されない限り、このパラメータはデフォルト値以外の値に設定しないでください。

- CAUNIALLOWSET - ワークステーションからの SNMP 設定要求が許可されるかどうか決定されます。CAUNIALLOWSET の値が NO に設定されている場合は、設定要求は許可されません。値が YES に設定されている場合は、System State Manager のテーブル、およびワークステーション上で修正可能なリソース値を変更する要求が、要求元に関係なく実行されます。

注: CA NSM のセキュリティまたは Windows のセキュリティを使用して、ユーザによる設定要求の使用を、さらにフィルタリングすることができます。

- CAUNIUSERCURRENT および CAUNIUSERDESIRED - current、desired、または current-desired ステートの組み合わせを定義します。これにはユーザステータスの値が割り当てられ、CA NSM 2D map 上に黒いアイコンとして表示されます。

デフォルト: ユーザステータスの定義なし。

2. CA OPS/MVS を開始します。

注: CA OPS/MVS のメインアドレス空間は、通信の相手先となる正しい TCP/IP スタートアップ タスクを判断するために、TCP/IP データセット (hlq.TCPIP.DATA) への読み込みアクセス権を持っていないければなりません。CA OPS/MVS の初期化時に実行される OPSSPA00 REXX プログラムの中で、または OPSMAIN で開始したプロシージャ内の JCL ステートメントを介して、システムにより明示的に データセットが ddname SYSTCPD に自動で割り当てられる必要があります。Agent Technology のインストールを担当しているシステム プログラマに連絡して、Agent Technology が通信に使う TCP/IP が使用する正しいデータセット名を調べてください。以下に例を示します。

```
ADDRESS TSO "ALLOCATE FI(SYSTCPD) DSN('hlq.TCPIP.DATA') SHR"
```

TCP/IP クライアント データセットの要件の詳細については、IBM のドキュメントを参照してください。

詳細については、「CA Network and Systems Management Systems Status Manager CA OPS/MVS Option User Guide」を参照してください。

3. (オプション) System State Manager のテーブルに TNGNOTIFY、TNGELIGIBLE、および RESOURCE_TEXT の列が含まれていない場合のみ、この手順を行います。

これらの新しい列を System State Manager のディレクトリテーブル、およびすべてのリソーステーブルへ挿入します。CA OPS/MVS の SAMPLES ライブラリ内の OPTNGCOL メンバには、この処理に役立つ OPS/REXX プログラムが収められています。

OPTNGCOL REXX EXEC の引数は次のとおりです。

SUBSYS

CA OPS/MVS サブシステムの名前(通常は OPSS)。

ACTIVATE

現在管理対象になっている System State Manager テーブルのリスト。これらのテーブルでは、TNGNOTIFY 列の値は ALWAYS に設定されています。現在管理されている System State Manager テーブルが ACTIVATE 引数に示されていない場合は、TNGNOTIFY 列を追加すると、値が NEVER になります。

注: TNGNOTIFY 列が追加されると、RESOURCE_TEXT 列が追加されます。

RESTABLE

TNGNOTIFY 列および RESOURCE_TEXT 列を追加し、TNGNOTIFY の値を NEVER に設定するためのテーブル名のリスト。ACTIVATE 引数が NULL の場合は、この引数は、デフォルト値の ALL になります。RESTABLE(ALL) は、現在監視されているすべての System State Manager テーブルに、TNGNOTIFY 列および RESOURCE_TEXT 列が追加されることを意味します。

プログラムの例を以下に示します。

```
OX 'OPSDIST.SAMPLES(OPTNGCOL)' SUBSYS(OPSS) ACTIVATE(SSMQA1)
```

4. CA OPS/MVS および CA NSM SSM CA OPS/MVS Option ヘステータスがレポートされる System State Manager のリソースすべてについて、リソーステーブルの TNGNOTIFY 列を ALWAYS に設定します。

5. TNGNOTIFY 列を ALWAYS に設定する System State Manager リソースが含まれているすべてのテーブルについて、ディレクトリテーブルの TNGELIGIBLE 列を YES に設定します (デフォルトのディレクトリテーブルは SSM_Managed_TBLS です)。
6. 日次のウォーム スタートトラップを作成するかどうか決定します。OPSMTRAP OPS/REXX 関数を使用します。この関数により、CA OPS/MVS エージェントは必要なときにウォームまたはコールドのスタート SNMP トラップを生成できます。また、日次の午前零時 AOF TOD ルールなど、さまざまな AOF ルールを使用することもできます。複数のシステムが CA NSM SSM CA OPS/MVS Option と通信している場合は、ネットワークの過負荷を避けるために、各システムが日次のウォーム スタートトラップを異なる時刻に送信することをお勧めします。

Agent Services への CA-OPS/MVS Option の定義

以下の手順を実行して、CA NSM SSM CA OPS/MVS Option が Agent Services に適切に定義されるようにします。CCS for z/OS のインストールおよびカスタマイズの担当者は、このセクションに記載されているユーティリティに精通していることが必須です。

Agent Services へ CA OPS/MVS Option を定義する方法

1. CA NSM Agent Services がインストールされており、実行中であることを確認します。
2. OPS CCLXCNTL(LDMIB) メンバに提供されている LDMIB ユーティリティを使用して、STATEMAN MIB を Object Store にロードします。適切な Agent and Agent Services データセットおよび STATEMAN MIB を参照するよう、環境変数をカスタマイズしてください。STATEMAN MIB は CCS for z/OS に配布されており、CCLXMIB ディレクトリにあります。コピーは、OPS.CCLXMIB(STATEMAN) メンバにもあります。

3. Agent Configuration ファイルを作成します。サンプルは、CA OPS/MVS CCLXCNTL(CFGSSMO) メンバで提供されています。この設定ファイルは次の目的で使用されます。

- 特定のエージェントに対して、デフォルトのコミュニティ定義、またはトラップの宛先を上書きする。

たとえば、CCLXCNTL(CFGSSMO) のエージェント サンプル設定ファイルから取得した以下の指定では、宛先のアドレス、コミュニティ名、エージェントで発行されるトラップのポートを設定します。#SNMPTRAP ホストおよびポートの情報は、CA OPS/MVS および CA NSM SSM CA OPS/MVS Option ワークステーションの IP アドレスおよびポートと一致している必要があります。指定されたポート番号は、すでに同じポート番号を使用している他の SNMP エージェントと競合しないように、TCP/IP の設定担当者が検証する必要があります。

また、CA OPS/MVS および CA NSM SSM CA OPS/MVS Option は、STATEMAN MIB から情報を取得するために public というコミュニティ名を使用し、MIB で定義されているフィールドを修正するために admin というコミュニティ名を使用する必要があります。

```
#SNMPTRAP
host      141.202.42.253
community public
port      162
#SNMPCOMMUNITY
access    read
community public
host      0.0.0.0
#SNMPCOMMUNITY
access    write
community admin
host      0.0.0.0
```

- エージェントに対して、最初の起動値を設定します。

サイトの要件に合わせてカスタマイズする必要があるのは、CA OPS/MVS および CA NSM SSM CA OPS/MVS Option ワークステーションのコミュニティ名およびトラップ宛先の指定だけです。その他のすべての設定は、このサンプルに記載されているままにします。

- ご使用のシステムで、`#SNMPTRAP` および `#SNMPCOMMUNITY` の指定も必要とする複数の CA エージェントを実行している場合は、指定されているこれらの値も調整する必要があります。OPSCNFG 設定セットでこれらの値を割り当てると、CA NSM Agent Technologies の `aws_sadmin.cfg` のデフォルト設定セットで割り当てられている値が上書きされます。これらの 2 つのパラメータの値はいずれかの設定セットで指定できますが、正常にロードされた後は、OPSCNFG の設定セットの値が優先されます。少なくとも OPSCNFG の設定セットには、提供されているすべての `#SNMPGROUP` の指定を含める必要があります。
4. Community の名前および Trap の宛先に対する Configuration の設定がカスタマイズされたら、OPS CCLXCNTL(LDCFG) で提供されている LDCONFIG ユーティリティを使用して、Configuration ファイルをオブジェクトストアにロードします。Agent Services、CA OPS/MVS、および CA NSM SSM CA OPS/MVS Option を実行している場合は、このユーティリティを実行する前に必ず CA OPS/MVS および CA NSM SSM CA OPS/MVS Option を停止します。Agent Services を実行している場合は、新しい設定ファイルを有効にする前に、`aws_sadmin` を再循環させる必要があります。詳細については、CA NSM CD に収められている「*CA NSM Working with Agents*」ガイドを参照してください。LDCONFIG JCL の環境変数をカスタマイズして、正しい Agent データセットおよび Agent Services データセット、また修正された Configuration ファイルを参照するようにします。また、コミュニティ名の指定が、UCA OPS/MVS および CA NSM SSM CA OPS/MVS Option で使用しているものと対応し、トラップが CA OPS/MVS および CA NSM SSM CA OPS/MVS Option ワークステーションにルーティングされるようにします。

詳細については、CA NSM CD に収められている「*CA NSM Working with Agents*」ガイドを参照してください。CA OPS/MVS および CA NSM SSM CA OPS/MVS Option のインストールに必要な CCS for z/OS コンポーネントの詳細については、付録「[CCS for z/OS コンポーネントの要件 \(P. 241\)](#)」を参照してください。

要求されるデータセット

各エージェントには、実行中に情報や診断メッセージを書き込むための、個別のログファイルが必要です。書き込まれるメッセージの数と種類は **CAUNIDEBUG** パラメータおよび **CAUNITRACE** パラメータで指定されている値によって変わります。これについてはこのセクションで後述します。連携エージェントが 2 つ存在するため、ログファイル用に 2 つの **DD** ステートメントが **CA OPS/MVS** スターティッドタスク プロシージャに追加される必要があります。**ddname** は次のとおりです。

DD 名	説明
ENVFILE	通常は CCS for z/OS SCRLIB データセット内にある CCS for z/OS ENVFILE を参照します。
OPSALOG	メイン エージェントのログ ファイル
OPSBLOG	セカンダリ エージェントのログ ファイル
SYSTCPD	TCP/IP プロファイル データセットを参照します。

以下は、2 つのエージェント用の **STDERR** ファイルおよび **STDOUT** ファイルと関連付けられた **ddname** です。これらのファイルは、エージェント初期化時にリダイレクトされます。2 つのエージェントは、リダイレクトされないと互いの **STDERR** ファイルおよび **STDOUT** ファイルを上書きするためです。

DD 名	説明
OPSAERR	プライマリ エージェントのリダイレクトされた STDERR DD
OPSBERR	セカンダリ エージェントのリダイレクトされた STDERR DD
OPSAOUT	プライマリ エージェントのリダイレクトされた STDOUT DD
OPSBOUT	セカンダリ エージェントのリダイレクトされた STDOUT DD
CEEDUMP	C 言語環境のためのダンプ データセット

注: **CA OPS/MVS** が **SUB=MSTR** 指定で起動した場合、上記のデータセットは **CA OPS/MVS CCLXCNTL(ALLOCAWS) JCL** を使用して永続的なデータセットとして事前に割り当てられる必要があります。さらに、**CA OPS/MVS** 初期化 **REXX EXEC** (通常は **OPSSPA00**) を使用してデータセットを動的に割り当てます。**SUB=MSTR** が指定されていない場合、**DD** は **DSN** 仕様の代わりに **SYSOUT** を指定できます。

前掲の表に記載されているファイルに加えて、STEPLIB DD と連結している以下の APF 権限付与済みデータセットが (LINKLST データセットとして定義されていない限り) CA OPS/MVS スターティッド タスク プロシージャに含まれる必要があります。

- OPSAGENT モジュールおよび OPSSTRAP モジュールが格納された CA OPS/MVS PDSE ロード ライブラリ。
- CCS for z/OS の一部としてインストールされたエージェント サービス ロード ライブラリ。
- 通常は CEE.SCEERUN と名付けられている、C ランタイム ライブラリ。

デバッグ用のパラメータ

エージェントのメッセージ ロギング サービスをアクティブにするには、パラメータ CAUNIDEBUG=YES を指定する必要があります。トラブル シューティングのシナリオ以外では、このパラメータは通常 NO に設定しておきます。

パラメータ CAUNITRACE=Fn は、CA OPS/MVS のアドレス空間内のワークステーション タスクで発行される SNMP のトラップ要求に対する SNMP DPI AWS サブエージェントからのトレースメッセージの生成を制御します。

ここで、8 つの重大度を次に示します。重大度が高い順 (レベルの番号が小さい順) に記載しています。

セキュリティレベル	説明
F0 - FATAL (致命的)	F0 では、重大度が FATAL のメッセージがログされます。
F1 - CRITICAL (重大)	F1 では、重大度が F0 から F1 のメッセージがログされます。
F2 - WARNING (警告)	F2 では、重大度が F0 から F2 のメッセージがログされます。
F3 - INFO (情報)	F3 では、重大度が F0 から F3 のメッセージがログされます。
F4 - DEBUG (デバッグ)	F4 では、重大度が F0 から F4 のメッセージがログされます。
F5 - DEBUG1 (デバッグ 1)	F5 では、重大度が F0 から F5 のメッセージがログされます。
F6 - DEBUG2 (デバッグ 2)	F6 では、重大度が F0 から F6 のメッセージがログされます。
F7 - DEBUG3 (デバッグ 3)	F7 では、重大度が F0 から F7 のメッセージがログされます。

詳細については、CA NSM CD に収められている *CA NSM* のドキュメントを参照してください。

Expert Systems Interface (ESI) の設定

Expert Systems Interface (ESI) を使用すると、高級言語またはアセンブラ言語で記述されたアプリケーションから選択された *CA OPS/MVS* 機能にアクセスできます。

ESI のライセンスを取得して使用する場合は、*INITESI* パラメータを **YES** に設定する必要があります。

ESI の使用方法の詳細については、「*User Guide*」の「*Expert Systems Interface*」を参照してください。

OPSLOG WebView の環境設定

OPSLOG WebView は、PC ワークステーションから *OPSLOG* メッセージを参照するためのクライアント/サーバアプリケーションです。クライアント側は、**Microsoft Internet Explorer** から起動された **Java** アプリケーションとして作動します。このアプリケーションは、自動的にダウンロードおよびインストールされます。

OPSLOG WebView のサーバ側を実行するには、**z/OS** システムに次の 2 つのコンポーネントをインストールする必要があります。

- **z/OS HTTP** サーバ上の **Web** アプリケーション (**IBM WebSphere** 製品など)
- **CA OPS/MVS** を実行している同じ **z/OS** システム上のサーバアプリケーション

注: サーバアプリケーションは **CA OPS/MVS** を実行している実稼動システムにインストールする必要がありますが、**Web** アプリケーションは、**CA OPS/MVS** を実行していないシステム上にもインストールできます。

システム全体の少なくとも 1 つのシステムに 1 つのサーバをインストールすると、MSF を使用して他のシステムにアクセスできます。CA は、1 つのシステムが停止しても、すべての **WebView** のアクセスがクローズしないよう、ご使用の環境で複数のシステム上にサーバをインストールすることをお勧めしています。サーバを実行しても、MSF アクセスは妨害されません。すべてのシステム上でサーバを実行しても、MSF を使用してシステムにアクセスできます。サーバを介して直接アクセスするよりも、MSF を介してアクセスする方がわずかに遅くなりますが、短期間では、1 つのサーバからログオフして別のサーバに接続するよりも、MSF を介してアクセスする方が簡単です。

リソース チェックリスト

OPSLOG **WebView** アプリケーションをインストールする前に、以下のリソースが必要です。

- **リソース 1:** ユーザは、CA OPS/MVS の配布メディアからインストールされた以下のデータセットに割り当てられている高レベル修飾子 (HLQ) を知っており、それに対する更新アクセス権を持っていないければなりません。

[HLQ].OPS.CCLXCNTL

- **リソース 2:** CA OPS/MVS の配布メディアからインストールされた、以下の 2 つのデータセットに割り当てられている HLQ を知っており、それらに対する更新アクセス権を持っていないければなりません。

- hlq.OPS.CCLXLOAD

- hlq.OPS.CCLXPLD

- **リソース 3:** USS の宛先パス (互換モード ディレクトリの HFS または zFS) を定義します。このパスに、OPSLOG **WebView** のサーバ ファイルをインストールします。これは一般的なパスの例ですが、任意のパスを指定できます。

/sys/opsmvs

注: OPSLOG **WebView** をインストールしても、この HFS または zFS は互換モード ディレクトリに作成されません。このディレクトリは、永続的に割り当てられているストレージまたは OPSLOG **WebView** のインストール前にマウントされたファイル システム上に存在する必要があります。サイズは約 5 MB あれば十分です。

- **リソース 4:** Web サーバ上の `httpd.conf` 構成ファイルに対して書き込みアクセス権を持っていないければなりません。ファイルは、たとえば次のような場所に存在していますが、この場所は、実際の Web サーバの設定によって異なります。

`/sys/http/etc/httpd.conf`

これは互換モードファイルの HFS または zFS ファイルなので、スーパーユーザの権限を使用して、このファイルへの書き込みアクセス権を付与できます。

- **リソース 5:** OPSLOG WebView セッションをオープンするためにアクセスする必要がある URL を定義します。

URL は、以下のような一般的な形式で指定します。

`http://hostname.domain/applname`

hostname

ホスト名を表し、論理 Parmlib 連結で定義されます。通常は、JES2 または JES3 ノードと同じ名前を使用します。

domain

会社の IP ドメインを表します。たとえば、CA のドメインは `ca.com` です。

applname

ユーザが OPSLOG WebView にアクセスするために入力した名前を表します。これは、インストールのときに指定されます。

注: *hostname* および *domain* では大文字/小文字は区別されませんが、*applname* では大文字/小文字が区別されます。

設定オプションの定義

次の 2 つの方法を使用して、サーバを初期化するとき、設定情報を OPSLOG WebView サーバに渡すことができます。

- JCL EXEC PARM=*value* フィールド

この方法は、z/OS により 100 文字の制限があります。必要なすべてのパラメータをサポートするのに、100 文字では不十分なことがあります。

- SYSIN ddname ステートメント。これは OPSLOGSV スターティッド タスク内にあります。

この方法はオプションで、以下の処理を行うことができます。

- 無制限の文字数に対応する
- PARM=*value* フィールドに加えて、またはこれに代わって使用する
- PDS メンバ、または固定長あるいは可変長のレコードが含まれているフラットファイルの名前を指定する

PARM で割り当てできるすべてのパラメータは、SYSIN DD ファイルを使用して割り当てすることもできます。これらの場所で定義されるすべてのパラメータは、SYSIN ファイルから設定されます。これらの 2 つのメソッドで異なる点は、PARM フィールドではすべてのオプションを連結された 1 つの文字列の中に定義するのに対して、SYSIN ファイルでは、各パラメータを個別のレコードに格納しなければならない、ということだけです。SYSIN は DASD 上に存在するファイルでなければなりません。

SYSIN レコードには、3 つのタイプのレコードがあり、列 1 の文字で区別されます。

- -(マイナス記号)または/(スラッシュ)

パラメータの行を表します。「/」と「-」は両方とも、まったく同じように機能します。これらの記号は、パラメータの設定で解析される行をマークします。

- *(アスタリスク)

コメント行を表します。アスタリスクのコメント行を使用して、設定、またはその他の一般的な情報についての詳細を保持します。アスタリスクのコメントは、SYSPRINT ファイルに送信されません。

- ;(セミコロン)

SYSPRINT データ ストリームに印刷されるコメント行を表します。

サンプルのプロシージャを以下に示します。

```
//OPSWEBVW EXEC PGM=OPSLGSGV,TIME=NOLIMIT,REGION=0M
//SYSPRINT DD SYSOUT=*           <=== For server console messages
//STDOUT   DD SYSOUT=*           <=== For error/debug messages
//STDERR   DD SYSOUT=*           <=== For error/debug messages
//CEEDUMP  DD SYSOUT=*           <=== For z/OS LE reports
//SYSUDUMP DD SYSOUT=*           <=== Dump dataset
//SYSIN    DD DISP=SHR,DSN=MY.PDS(SYSIN)
```

注: スターティッド タスクで JES Spool システムは使用できないため、以下のステートメントは指定できません。

```
//SYSIN    DD *
```

SSL 通信の定義

起動オプション **S** を使用して、**WebView** 通信でセキュアソケットレイヤ (SSL) 通信を使用するよう指定します。**S** オプションは、次の **SYSIN** 設定ファイルの抜粋に示すように、3 回指定する必要があります。

1. SSL モードをオンにして、SSL キーリングへのパスを設定します。

```
-S PATH /sys/usr/lpp/opsmvsc/cpp/skeys.kdb
```

2. このパスワードを使用してキーリングをオープンします。

```
-S PASS password
```

3. SSL はキーリングで、以下のラベルを持っているキーを検索します。

```
-S LABEL label
```

SSL はこれらの設定を使用してデジタル証明書へのアクセスを設定し、**WebView** サーバが SSL を使用するよう指示します。

サーバは、**MVS** スターティッド タスクとして **USS** 環境で動作します。このサーバは **IBM SSL** を使用するため、キーリング、キーリング パスワード、およびキーラベルの **IBM** 実装を使用します。**IBM** のキー管理プログラムは **gskkyman** で、これは互換モードの **HFS** または **zFS** 内の **/usr/lpp/gskssl/bin** にあります。

最小要件

WebView クライアントで **SSL** を実行するには、**Java Run time Environment 5.0** かそれ以上が必須です。

デジタル証明書プロトコル

SSL 暗号化は、公開鍵技術を使用して、クライアント/サーバのペア間に暗号化されたリンクを確立します。非常にシンプルなプロトコルを使用して、最初に通信パートナー間でアグリーメントを結ばずにクライアントとサーバ間に暗号化されたリンクを確立させることも可能です。ただし、このような状態で作成されたリンクは第三者からの攻撃に対して脆弱です。こういった攻撃では悪意を持つ攻撃者がホストへの通信を妨害し、パスワードやセッション中のすべての通信にアクセスします。

中間者攻撃を阻止するために、CA ではデジタル証明書プロトコルを採用しました。対象サーバの公開鍵を含むデジタル証明書が、SSL 暗号化を使用するクライアントシステムに郵便やその他のある程度安全な方法で届けられます。関連するデジタル証明書がホストでも利用可能です。この手法によって、クライアントは確実に目的のホストとのみリンクします。

WebView クライアントは Java で書かれているため、Java SSL が使用されます。デジタル証明書は：

- 認証機関からクライアント マシンに送信されます。
- Windows XP システムの Documents and Settings¥userid フォルダにある .keystore (ピリオド keystore) という名前のファイルにインストールされる必要があります。
- PC に複数のユーザがいる場合、各ユーザ用にインストールされた別々の .keystore ファイルを持つことができます。

Java のキーツール プログラムを使用して、各マシンに証明書をインストールします。

同じ証明書をすべてのユーザ用、複数ユーザのグループ用、または単独ユーザ用にインストールすることが可能です。セキュリティのために、CA では各ユーザ用に異なる証明書を使用することをお勧めします。たとえば、従業員が退職した場合、ほかのすべてのユーザとは別々にその従業員の証明書を無効にすれば、混乱は最低限で済みます。

デジタル証明書の管理には、最低でも証明書の作成および配布が含まれます。また、証明書の作成を専門とする営利企業である認証機関とのやりとりも伴うことがあります。独自の認証機関を構築するか、商用認証機関を利用します。どちらの場合も、それぞれ利点があります。

証明書の管理の詳細については、本マニュアルでは取り扱いません。詳細については、御社の認証機関 (CA) サポート チームにご連絡ください。

セキュリティが OPSLOG WebView に与える影響

以下のセキュリティ情報を確認します。

- Web Server

OPSLOG WebView サーバは、各クライアントについて、System Authorization Facility (RACF や CA Top Secret など) からセキュリティ環境を取得します。セキュリティ環境は、各ユーザに対して、特定のアクション (ホストコマンドの発行など) を実行できるかどうかを制御します。クライアントのセキュリティプロファイルを取得するためには、サーバに BPX.SERVER に対する UPDATE アクセス権が必要です。z/OS 1.7 以降を実行している場合は、サーバに、BPX.CONSOLE に対するアクセス権も必要です。このようなアクセス権がない場合、サーバは UID=0 として実行する必要があります。

また、Web Server (HTTPD または WebSphere) が、セキュリティパッケージのプログラムで制御された属性によってセキュリティを保証されているかどうかチェックします。このようになっている場合は、OPS.CCLXPLD 内にある OPSLOGV プログラム、および OPS.CCLXLOAD 内にある OPMFSB プログラムが、プログラムで制御されるようにする必要があります。この属性の設定の詳細については、セキュリティパッケージのドキュメントを参照してください。

- データの認証および暗号化

認証および暗号化に対して SSL プロトコルを使用して、送信中の OPSLOG WebView データのセキュリティを保証します。

OPSLOGSV スターティッド タスクについて **S** オプションを指定して、OPSLOG WebView サーバに対して SSL を有効にします。

暗号化されていないすべてのデータ (ただしパスワードは除く) は、OPSLOGSV スターティッド タスクに対して SSL を指定せずに **U** オプションを指定して伝送します。

OPSLOGSV スターティッド タスクについて、**S** オプションも **U** オプションも指定されていない場合は、OPSLOG WebView サーバは、デフォルトでクライアントとサーバの認証をバイパスし、XOR 暗号化スキームを使用して、送信中のデータを暗号化します。

■ システム

OSFSECURITY に CHECKUSERID が設定されているときに、OPSLOG WebView ユーザがターゲットシステム上でコマンドを発行できるようにするには、ターゲットシステムでセキュリティルールを有効にしておかなければなりません。

セキュリティルールがローカルシステムで有効になっていない場合は、ローカルシステムとリモートシステムの両方でデフォルトの権限が適用されます。

OSFSECURITY が CHECKUSERID に設定されており、ローカルシステムとリモートシステムの両方にセキュリティルールが書かれている場合は、OPSLOG WebView ユーザは、リモートシステムでセキュリティをチェックする前に、ローカルシステムでコマンドを発行する権限を持っている必要があります。言い換えると、OPSLOG WebView ユーザがリモートシステムでコマンドを発行するには、ローカルシステムとリモートシステムの両方で権限を持っていないければなりません。

注: ターゲットシステムでセキュリティルールを提供できない場合は、送信されたコマンドは実行されません。DEBUGOSF パラメータの値が ON に設定されない限り、エラーについて何も表示されません。

■ セキュリティルール

どのユーザが次の処理を実行できるか指定することにより、セキュリティルールを介して OPSLOG WebView から CA OPS/MVS へのアクセスを制御することができます。

- OPSLOG メッセージの参照
- ホストコマンドの発行

OPSLOG へのアクセスを制御するためのセキュリティルールが事前に存在しない場合は、デフォルトのセキュリティ権限が適用されます。つまり、OPSLOG WebView からすべてのユーザが OPSLOG を参照できますが、ホストコマンドを発行することはできません。

OPSLOG メッセージを表示するデフォルトの権限を上書きするには、セキュリティルールを作成して、あるユーザ、または複数のユーザが OPSLOG を参照することを許可します。この権限によりホストコマンド エリアも使用可能になるため、権限が付与されたユーザは、OPSLOG WebView からホストコマンドを入力できるようになります。

以下のサンプル ルールでは、`allow_users` リストのユーザのみが `OPSLOG` メッセージを参照できるようにします。

```
)SEC OPSBRW
)PROC
allow_users = "TSOUSER1 TSOUSER2 TSOUSER3"
user = sec.opausid
if WORDPOS(user,allow_users) = 0 then return "reject"
else return "accept"
```

ホスト コマンドを発行するためのデフォルトのセキュリティ制限を上書きするには、あるユーザ、または複数のユーザがホスト コマンドを発行することを許可するセキュリティルールを作成します。

以下のサンプル ルールでは、`allow_users` リストのユーザがホスト コマンドを発行できるようにします。

```
)SEC OPSCMD
)PROC
allow_users = "TSOUSER1 TSOUSER2 TSOUSER3"
user = sec.opausid
if WORDPOS(user,allow_users) = 0 then return "reject"
else return "accept"
```

配布されたサンプル ルール ライブラリのメンバ `SECWEBV1`、`SECWEBV2`、および `SECWEBV3` には、このセキュリティを規定する例が用意されています。詳細、およびセキュリティアクセスを付与するために必要な手順の一覧については、サンプルを参照してください。

`CA OPS/MVS` のセキュリティルールを使用してこれらの運用上の機能を保護している場合は、これらのサンプルを参照し、既存のルールに取り入れる必要があるロジックの変更を確認します。

■ ログイン ID

`OPSLOG WebView` セッションを確立する前に、`OPSLOG WebView` は各ユーザに、ターゲットの `z/OS` システムに対する正当なユーザ ID とパスワードを使用してログインするよう指示します。ユーザは、既存の `TSO` ユーザ ID を使用するか、この目的で新しいユーザ ID を定義するか、選択できます。必要なのは、そのユーザ ID にターゲット システムにログオンする権限が付与されていることのみです。

注： `OPSLOG WebView` アクセスが必要なユーザ ID に `OMVS` セグメントを定義する必要があります。これらのユーザ ID は、`OPSLOGSV STC` が実行されているシステムにログオンする必要があります。

SYSIN ステートメントのパラメータ

以下の SYSIN ステートメントが、OPSLOGSV スターティッド タスク プロシージャの SYSIN ファイル内にあります。

```
//SYSIN DD DISP=SHR,DSN=MY.PDS(SYSIN)
```

SYSIN ファイル内の以下のパラメータを設定します。

-C path

ユーザ設定が格納される互換モード ノードに HFS または zFS が設置されます。例: /sys/usr/caops/cfg。デフォルトの設定はありません。

-G 0|DISABLE または 1|ENABLE

ユーザが WebView で GO モードを有効化することをシステム管理者が拒否できます。

注: 0 と DISABLE、1 と ENABLE はそれぞれ同義です。

0|DISABLE

すべてのユーザの GO モードを無効化します。WebView の [OPTION] メニューにある [GO] オプションはグレー表示になり、ユーザが利用することはできません。

1|ENABLE

すべてのユーザの GO モードを有効化します。GO モードが有効化されていると、[GO] オプションは有効でありグレー表示になっていません。GO モードがアクティブとなるのは、ユーザによってアクティブ化された場合のみです。有効の指定は、デフォルト状態であるためオプションです。

デフォルト: 1|ENABLE

-I minutes

クライアントのアイドル状態が何分続いたらサーバがクライアントを強制切断するかが指定されます。デフォルトは 120 です。0 は強制ログアウトを回避するための特殊なケースです。

-M Maxcon

同時にサーバにログオンできるクライアントの数が指定されます。デフォルトおよび最大値は 50 です。

-P port

サーバとクライアントが相互通信を行うために使用する TCP/IP ポートが指定されます。

-S PATH name

暗号化マネージャとして **SSL** が選択され、キーリングの場所が指定されます。**PATH** は示される文字通りに指定する必要があります。名前がスラッシュで始まる場合、キーリングは互換モードの **HFS** または **zFS** に格納されていると見なされます。名前がスラッシュ以外の文字で始まる場合は、キーリングは **SAF** 保護されたスタッシュに、**MVS** によって格納されていると見なされます。

-S PASS password

HFS または **zFS** に互換モードで格納されるキーリングに使用されるパスワードが指定されます。各キーリングは、それぞれのパスワードを持ちます。パスワードを **SAF** 管理のスタッシュに格納する場合は、この行を省略します。

-S LABEL label

キーリング内の特定のキーに関連するプロパティである、ラベルを指定します。

-T level

トレースレベル(以前はデバッグレベル)は、**SYSPRINT** に送信される詳細のレベルを指定します。

注: **-T level** は、以前の **-d**(デバッグ)レベルに代わるものです。**-d** を指定すると **JCL** は失敗します。

-U Unencrypted

常に暗号化されるものであるパスワードを除いて、ホストサーバおよびクライアント間のいかなる通信も暗号化しないことが指定されます。**SSL** と非暗号化の両方が指定された場合、**SSL** がこの形式を無効にします。

Web アプリケーションの設定

OPSLOG WebView の Web アプリケーションを設定する前に、**IBM WebSphere** 製品などの **z/OS HTTP Web** サーバ環境をシステムにインストールしておく必要があります。次の詳細な設定の説明では、既存のサーバへ定義を追加する方法を示します。

Web アプリケーションを設定する方法

1. テキスト エディタを使用して、Web サーバの `httpd.conf` 設定ファイルを修正します (リソース 4 を参照)。

以下のように、PASS ステートメントをインクルードします。

```
PASS /applname/* /uss target path/*
```

applname

OPSLOG WebView サーバのアプリケーション名を指定します。これは、OPSLOG WebView クライアントセッションをオープンするのに使用する URL 上でユーザが指定します (リソース 5 を参照)。

uss_target_path

OPSLOG WebView のサーバファイルをインストールしたパス名を指定します (リソース 3 を参照)。

以下の `AddType` ステートメントがインクルードされ、OPSLOG WebView で使用される特定のファイル タイプを認識するための Web サーバを示しているようにします。

```
AddType .jnlp application/x-java-jnlp-file ebcdic 1.0 #JNLP - Java Web Start
AddType .css text/css ebcdic 1.0 #Cascade Style
AddType .js text/javascript ebcdic 1.0 #Javascript
```

2. テキストエディタを使用して、USS/HFS もしくは Zfs の互換コード宛先パスに配置されている `opslog.jnlp` ファイルをカスタマイズします。

```
codebase="http://hostname.domain/applname">
```

```
hostname.domain/applname
```

Web アプリケーションがインストールされているホスト名およびドメインを指定します。

注: 「リソース チェックリスト」のリソース 3 を参照してください。

例: カスタマイズされた `opslog.jnlp` ファイル

- Web サーバがホスト `USILXXX` およびドメイン `ca.com` で実行されている場合は、ファイルは以下ようになります。

```
codebase="http://USILXXX.ca.com/opslog">
```

- Web サーバが代替のポートを使用する場合は、次のように指定する必要があります。

```
codebase="http://USILXXX.ca.com:4080/opslog">
```

- Web サーバが代替のアプリケーション名 (`webview` など)を使用する場合は、以下のように指定する必要があります。

```
codebase="http://USILXXX.ca.com/webview">
```

詳細情報:

[インストール後 \(P. 194\)](#)

サーバアプリケーションの設定

セキュリティの考慮事項も含めて OPSLOG WebView のサーバアプリケーションを設定するには、以下の手順を実行します。

1. サンプル スタートアップ タスク プロシージャ OPSLOGSV は、*hlq.OPS.CCLXCNTL* で提供されます。このプロシージャをシステム PROCLIB にコピーし、ユーザ設定のデータストレージおよび CA OPS/MVS のデータセット名 (リソース 1 およびリソース 2 を参照) の互換モード パス名で適切な HFS または zFS (リソース 3 を参照) に修正します。

これらのデータセットがリンクまたは LPA リスト内にすでにある場合は、STEPLIB DD を削除できます。

2. (オプション) デフォルトでは、OPSLOG WebView サーバは、ポート 6001 を使用して TCP/IP ソケットを介してクライアントプログラムと通信します。

このポートが、メインフレーム システムまたはターゲット クライアント マシン上の他のポートと競合している場合は、次のようにデフォルトのポートを変更することができます。

- a. テキスト エディタ (以下のセクションを参照) を使用して、Web サーバの互換モード宛先パス (リソース 3 を参照) の USS/HFS または zFS にある、*opslog.jnlp* ファイルを開きます。<property name="connPort" value="6001"/> の行の 6001 を新しいポート番号に置き換えます。
- b. この変更を適用するには、Web サーバをいったん停止してから再起動します。
- c. PRT=6001 ステートメントの 6001 を新しいポート番号で置き換えるよう startup PROC OPSLOGSV を修正します。
- d. この変更を適用するには、OPSLOGSV をいったん停止してから再起動します。

注: CA OPS/MVS で自動的に管理される OSF TSO サーバおよび USS サーバとは異なり、OPSLOG サーバを管理するには外部の自動化、スケジューリング、またはシステム機能を使用する必要があります。CA OPS/MVS System State Manager のコンポーネントを使用して、サーバの起動および停止を制御できます。

OPSBRW および OPSCMD コマンド プロセッサに対するセキュリティアクセス権限または制限を指定します。

3. OPSLOG WebView サーバで SSL が有効にされている場合は、テキストエディタを使用して、OPSLOG WebView クライアントがプライベートキー ストアを検索できそうな場所を指定するよう `opslog.jnlp` ファイルを修正します。OPSLOG WebView のクライアントワークステーション上で、証明書、インポートされたキー、またはその両方を `opslog.jnlp` ファイルに指定した場所に格納します。

Java では、キーおよび証明書を格納するためのデフォルトのキー ストアが少なくとも 2 つ定義されます。市販の信頼されている証明書を保持しているストアはデフォルトで `cacerts` という名前のファイルで、ファイル ノード `$java_home¥lib¥security¥` に格納されています。`$java_home` は、環境変数 `java_home` の値を表します。ファイルの完全修飾名は、以下のようになります。

```
¥Program Files¥Java¥JRE1.6.0_03¥lib¥security¥cacerts
```

Java Runtime Environment で提供される `keytool` ユーティリティを使用して、自分の証明書をこのファイルにインポートし、PC にログオンするすべてのユーザに使用可能にすることができます。

これは、各 PC ユーザに対するプライベートキー ストアにもなります。このストアのデフォルトの場所は `$user.home¥keystore` で、通常は `.keystore` と呼ばれます。完全修飾名は、以下のようになります。

```
¥Documents and Settings¥username¥keystore
```

ここでは、PC システムのユーザと同じ数だけファイルが存在することが可能です。

ご使用の `opslog.jnlp` ファイルは `/sys/opsmvs` ディレクトリにあります。

`opslog.jnlp` ファイルのプロパティ設定により、クライアントが信頼済みの証明書を探す場所が SSL に知らされます。サンプルの `.jnlp` ファイル、プロパティ名、`javax.net.ssl.trustStore` は、プライベートキー ストアを探す場所をクライアントに知らせます。

プロパティ `javax.net.ssl.trustStore` の有効ないくつかの設定を以下に示します。

*USER は PC ファイルのノード、`$user_home¥username¥` を表し、他の名前が指定されない場合は、`.keystore` というファイル名を自動的に意味します。以下に例を示します。

```
value="*USER"          ==> ¥Documents and Settings¥username¥.keystore
value="*USER¥mykeys.kdb" ==> ¥Documents and Settings¥username¥mykeys.kdb
```

*SYSTEM は PC のパス `$java_home"¥lib¥security¥"` を表し、他の名前が指定されない場合は、`cacerts` という名前を自動的に意味します。以下に例を示します。

```
value="*SYSTEM"       ==> ¥Program Files¥Java¥JRE1.6.0_03¥lib¥security¥cacerts
value="*SYSTEM¥OPScert" ==> ¥Program
Files¥Java¥JRE1.6.0_03¥lib¥security¥OPScert
```

完全パスは次のように入力することができます。

```
value="C:¥Program Files¥Java¥JRE1.6.0_03¥lib¥security¥cacerts"
```

デフォルト: *SYSTEM

4. (オプション) 最小、およびデフォルトのリフレッシュ間隔を変更します。これらの設定はすべてのクライアントに適用されます。

デフォルトのリフレッシュ間隔: 30 秒

デフォルトの最小リフレッシュ間隔: 10 秒 [Options/Settings] ダイアログ ボックスでは、最小の間隔より短い設定はすべて受け入れられません。

新しい最小値およびデフォルト値を設定するには、システム管理者が、互換モードの HFS または zFS にある `opslog.jnlp` ファイルに以下の行を追加する必要があります。これらの行は、すでにサンプルの `.jnlp` ファイル内に存在する類似の「`property`」行の前か後に追加します。

これらのサンプル行では、最小とデフォルトの両方を 15 秒に設定しています。

```
<property name="GoModeRefresh" value="15"/>
```

```
<property name="GoModeDflt" value="15"/>
```

注: 最小の間隔は 10 秒未満には設定できません。またデフォルトの間隔は最小間隔よりも小さい値に設定できません。

5. サーバを起動するには、z/OS の `start` コマンド `S OPSLOGSV` を発行します。
6. サーバを停止するには、z/OS の `stop` コマンド `P OPSLOGSV` を発行します。

詳細:

[セキュリティが OPSLOG WebView に与える影響 \(P. 182\)](#)

テキストエディタの使用

テキストエディタを使用する方法

1. TSO Ready プロンプトで、「ISH」と入力します。
これにより、USS ファイルに対する I Shell ユーザ インターフェースが開始されます。
2. 画面の中央付近で、ISH は入力領域を表示します。ここで、編集するファイルが含まれている互換モード ディレクトリの HFS または zFS への USS パス名を入力します。以下に例を示します。

```
/sys/usr/lpp/opsmvs
```
3. コマンド行は空白のままにして、Enter キーを押します。
対象のファイルが含まれているディレクトリが表示されます。
4. PF7 キーおよび PF8 キーを使用して必要なだけスクロールして、編集するファイルを見つけます。
5. ファイル名の横に「?」(疑問符)を入力し、Enter キーを押します。
ポップアップ ボックスが表示されます。
6. ポップアップ ボックスに「5」と入力します。
エディタが起動されます。これは ISPF edit のように動作し、ファイルを編集することができます。

ASCII/EBCDIC の競合

OPSLOG WebView は、複数の種類のファイルを HFS または zFS に互換モードで格納します。これらのファイルは、バイナリ形式で配布されるものと、EBCDIC として配布されるものがあります。以下はその例です。

ファイルの種類	コード
.html	EBCDIC
.jpg	binary
.png	binary

.gif	binary
.js	EBCDIC
.css	EBCDIC

デフォルトでは、HTTPD はファイルを ASCII として扱います。ただし、HTTPD 設定ファイル内で **Addtype** 構成ステートメントを使用して、ASCII のデフォルトを無効にすることができます。多くのサイトは .html ファイルを EBCDIC コード化するように設定されています。ファイルの種類を明示的に ASCII に関連付けることもできます。これは必須ではありませんが、明示的に関連付けると、そのファイル形式がすでに使用されているということが HTTPD 設定ファイルのほかの保守管理者にもわかりやすくなります。

WebView 関連のファイルを定義するために使用した文字セットは、ご使用のサイトにインストールされているほかのソフトウェアが使用するファイル形式と異なる可能性もあります。 .js (Java スクリプト) および .css (スタイルシート) は、最も脆弱な形式です。 **OPSLOG WebView** のヘルプ ファイルのいずれかがほかのソフトウェアによって使用されている形式と違う場合、最も手軽な修正方法は、新規 **OPSLOG WebView** ヘルプ ファイルを EBCDIC から ASCII に変換することです。これを行うには、ファイルを PC に FTP 転送して EBCDIC から ASCII に変換し、次にファイルをバイナリ形式のファイルとしてホストに再送します。これにより、メインフレームシステムにあるファイルの ASCII インスタンスが確立されます。 EBCDIC 形式のファイルの名前を変更して保存し、その内容を簡単に参照できるようにしておくことをお勧めします。ファイルを ASCII に変換するには、その他の方法もあります。

.png ファイルなどのバイナリ特性を持つファイルは、ASCII でも EBCDIC でもありません。これらのファイルはバイナリであり、そのまま送信される必要があります。

インストール後

Web アプリケーションとサーバ アプリケーションのインストールおよび設定後、OPSLOG WebView セッションをこの形式の URL で開始することによって、Web ブラウザから OPSLOG WebView GUI にアクセスできます(リソース 5 を参照)。

`http://hostname.domain:port/applname`

hostname および *domain* は IP アドレスです。数値の IP アドレスがわかる場合、その数値を使用してもかまいません。

port は HTTP (ブラウザ) アクセス用に定義する IP ポート番号です。デフォルトのポート 80 を定義する場合、URL から省略できます。

applname は PASS ステートメント内で定義されます。この章にある「Web アプリケーションの設定」で説明されているとおりです。

詳細情報:

[Web アプリケーションの設定 \(P. 186\)](#)

OPSLOG WebView の初回の起動

Web ブラウザの制御オプションを使用してワークステーションの一時インターネット ファイルおよびオフライン コンテンツを削除し、確実に最新リリースの OPSLOG WebView から更新ファイルがダウンロードされるようにすることをお勧めします。

ワークステーションで OPSLOG WebView を起動するには、Java ランタイム環境がインストールされている必要があります。すでにインストールされている場合、Java コントロール パネルを使用して既存の OPSLOG WebView アプリケーションをすべて Java キャッシュから削除し、確実に現在のリリースの OPSLOG WebView クライアントがインストールされるようにすることをお勧めします。

ワークステーションに Java ランタイム環境がインストールされていない、または古いバージョンがインストールされている場合、OPSLOG WebView を初めて起動するときにセキュリティ警告画面が自動的に表示され、Java ランタイム環境の最新のリリースをインストールするよう表示されます。一般的なインストールの手順に従ってください。

Java ランタイム環境をワークステーションにインストールしたら、Java Web Start がワークステーションに OPSLOG WebView クライアント プログラムをダウンロードします。

クライアントプログラムがマシンにダウンロードされていることを示す画面が表示されます。

セキュリティ警告画面が表示されたら、[Start]をクリックします。

OPSLOG WebView サーバの動作

このセクションで説明しているコマンドを使用して、OPSLOG WebView Server セッションのさまざまな局面を制御できます。これらのコマンドは、MODIFY コマンドを使用して発行できます。OPSLOG WebView サーバのコマンド構文の例を以下に示します。

```
F OPSLOGSV,APPL=TRACE 5
```

注: サーバへコマンドを発行する場合には、APPL= が必ず必要です。

これらのコマンドからのレスポンスは、OPSLOG スターティッド タスクの JESMSG LG および SYSPRINT です。これらのレスポンスは、システム ログまたは OPSLOG にも示されています。

以下のコマンドリストで、大文字は、コマンドを入力するときに必要な最少文字数を表します。

CANcel SOCKET *nnn*

ソケット *nnn* を使用しているクライアントに対する接続が即座に終了されます。どのセッションを終了するかを確定するには、USERS コマンドを使用します。

GOMODE=0, GOMODE 0, GOMODE=DISABLE, GOMODE DISABLE |

GOMODE=1, GOMODE 1, GOMODE=ENABLE, GOMODE ENABLE

GO モード オプションのステータスが「on the fly」に変わります。最初の行の 4 つの書き方はすべて互いに同等で、GO モード オプションを無効にします。2 番目の行の 4 つの書き方も効果は同じで、Go モード オプションを有効にします。これらのコマンドは、新しいクライアントの接続に対してすぐに有効になりますが、既存のクライアントでは、サーバをログオフして再接続するまで、無効または有効のステータスがそのまま保持されます。

構文例: F OPSLOGSV,APPL=GOMODE=ENABLE

STATistics | STATs

このコマンドは、サーバ アクティビティの統計プロファイルを報告します。さまざまな設定によって、報告された情報には次の内容が含まれています。

- 現在ログオンしているクライアントの数
- クライアントのピーク数
- ログオンの失敗数(通常はパスワードの不正による)

TIMEout *nnnn*

最大のアイドル時間を分単位で設定します。ここで設定したアイドル時間が経過すると、サーバはセッションを終了します。有効な設定値は、1 ~ 1440 分(24 時間)です。タイムアウトのデフォルトは 99 分です。startup プロシージャの -i パラメータを使用して、この値を設定することもできます。

TRACE YES|NO|ON|OFF|*n*

サーバがトレースの出力メッセージを生成するかどうかを制御されます。また、トレース情報の詳細レベルも制御されます。**YES** を指定すると、トレース出力が有効になりますが、詳細の数値レベルは変わりません。**NO** を指定すると、トレースメッセージが表示されません。**ON** と **OFF** はそれぞれ、**YES** と **NO** に相当します。

数値の引数 *n* はトレース出力で報告される詳細レベルを設定します。**1** は最も大まかなレベルで、**9** が最も詳細なレベルを表します。**1** から **9** までの数値の引数により、トレース出力だけでなく、レベルの設定もできます。**0** の引数は、レベルが変わらずにトレースメッセージが抑止されます。これは **TRACE NO** と同等です。

USERS

現在アクティブになっているユーザのテーブルが、ユーザ名、割り当てられているソケット、ログオンしてからの経過時間、およびアイドル時間の合計も含めて一覧で表示されます。

オプションのベース コンポーネントのタスク

このセクションでは、オプションのベース コンポーネントのインストール タスクについて説明します。

JES2 環境関数の設定 (JES2 で必要)

JES2 環境の OPSINFO/OPSJES2 関数を使用するには、CA OPS/MVS の配布メディアに含まれている、JES2 のオフセット モジュール OPJ2CB をアセンブルおよびリンクします。JES2 オフセット モジュールをアセンブルおよびリンクするための JCL は、SYS1.OPS.CCLXCNTL(JES2ASM) にあります。ソースは、SYS1.OPS.CCLXASM(OPJ2CB) にあります。

JES2 システムで CA OPS/MVS を起動し、CA OPS/MVS がデフォルト (null) の OPJ2CB モジュールがロードされていることを検出した場合は、システム上で実行中の JES2 のバージョンに対してデフォルトのオフセット テーブルを見つけようとし、CA で提供されるデフォルトのオフセット テーブルは、JES2 の保守レベルと一致していない可能性があるため、正しく機能しないことがあります。デフォルトのオフセット テーブルが見つからない場合は、JES2 関連の OPSINFO() 関数および OPSJES2() 関数は機能しません。デフォルトのオフセット テーブルを利用するのではなく、必ず OPJ2CB/OPJ2CBxx をアセンブルすることを強くお勧めします。

モジュール OPJ2CB のアセンブリはリターンコード 4 で終わることがありますが、ゼロ以外のすべてのリターンコードは詳しく調べる必要があります。

重要: JES2 オフセットモジュール OPJ2CB のすべてのコピーは、CA OPS/MVS の開始を試行する前に再アセンブルする必要があります。古いリリースを使用しようとすると、結果がエラーになったり、異常終了したり、その両方が起こったりする可能性があります。

JES2OFFSETSUFFIX を使用して CPU 間でライブラリの共有を可能にする (JES2 のみ)

CA OPS/MVS のパラメータ JES2OFFSETSUFFIX を使用すると、JES2 のさまざまなバージョンを備えている複数の CPU 間で、共通の CA OPS/MVS ライブラリを共有することができます。これは、OPJ2CB モジュールの名前に 2 文字の英数字のサフィックスを追加できるようにして、共有を実現します。このパラメータは、新しい JES2 オフセットモジュールをロードするために随時に変更できます。

OPJ2CB モジュールにサフィックスを指定するには、以下の OPSPRM REXX 関数を使用します。このパラメータを次のように設定します。

```
var = OPSPRM("SET", "JES2OFFSETSUFFIX", "xx")
```

ここで「xx」は指定するサフィックスです。

JES2OFFSETSUFFIX を使用するには、OPJ2CB モジュールをアセンブルしてサフィックスにリンクします。OPS.CCLXCNTL の JES2ASM メンバには、アセンブルおよびリンクジョブの JCL が含まれています。新しいサフィックスを実行するには、JES2ASM メンバ内の NAME リンケージエディタステートメントを新しいサフィックスで修正します。

```
MODE RMODE(ANY),AMODE(31) SET ADDRESSING/RESIDENCE  
ENTRY OPJ2CB  
NAME OPJ2CBxx(R)      (<-- 必要なサフィックス)
```

JES2OFFSETSUFFIX を使用する場合は、OPJ2CB ロードモジュールを、テープに配布されているデフォルトのロードモジュールにする必要があります。

注: 再アセンブルした OPJ2CB は、アセンブルした OPJ2CBxx よりも優先されません。

JES3 インターフェースの設定

JES3 コマンドのサポートは、z/OS コンソール サポートとは分離されています。IATUX18 exit は、JES3 RJP コンソールで発行された JES3 コマンドを制御します。サブシステム インターフェース (SSI) は、z/OS コンソールで発行された JES3 コマンドを処理します。JES3 RJP コンソールがなくても、IATUX18 には、それ以上のサポートは提供していません。

CA OPS/MVS は、JES3 とインターフェース接続し、標準 JES3 IATUX18 exit メカニズムでコマンドのインターセプトを行います。CA OPS/MVS の exit コードは 1 つのモジュール (OPJS18PR) で、既存の IATUX18 ロード モジュールにリンクエディットできます。IATUX18 という名前の作成済みロード モジュールは、ユーザ exit および CA OPS/MVS exit の両方を含み、CA OPS/MVS exit は JES3 実行中の最初に入力されます。

IATUX18 Exit のインストール (JES3 で必須)

CA OPS/MVS は、JES3 とインターフェース接続し、標準 JES3 IATUX18 exit メカニズムでコマンドのインターセプトを行います。

IATUX18 Exit をインストールするには、既存の IATUX18 ロード モジュールを使用して CA OPS/MVS exit コード モジュール (OPJS18PR) をリンクエディットします。IATUX18 という名前の作成済みロード モジュールは、ユーザ exit および CA OPS/MVS exit の両方を含み、CA OPS/MVS exit は JES3 実行中の最初に入力されます。

OPJS18PR のインストール

CA OPS/MVS の exit コード モジュール OPJS18PR は、既存の IATUX18 ロード モジュールにリンクエディットします。

OPJS18PR をインストールするには、SYS1.OPS.CCLXCNTL データセットの LINKUX18 メンバを使用して、ご使用のサイトで IATUX18 モジュールにリンクエディットします。SYS1.OPS.CNTL データセットには、処理を行うための以下のサンプル ジョブが含まれています。

```
MODE      RMODE(24),AMODE(31)
INCLUDE   OPSLOAD(OPJS18PR)
INCLUDE   SYSLMOD(IATUX18)
ENTRY    OPJS18PR
NAME     IATUX18(R)
```

インストール ポリシーで使用する必要がある場合は、SMP/E にリンクエディットすることも可能です。

共有ファイル VSAM KSDS の定義

共有ファイル機能により、異なるシステム間において(共有 DASD または VSAM RLS を介して)共有できる外部 VSAM KSDS 上で、グローバル変数とその値を永続的に保存できるようになります。このデータセットは、グローバル変数チェックポイントデータセットから完全に独立しています。レコードは、OPSHFI コマンドプロセッサからのみ共有 VSAM データセットでの読み書きが可能です。このファイルの考えられる活用法のひとつは、大量の変数の一括の初期化です。このファイルを使用しない場合は、非常に多数の OPSVALUE() 呼び出しが必要となります。

たとえば、以下のコマンドは VSAM データセットを読み込み、指定された変数名のプレフィクスに一致するすべてのレコード用の一時的なグローバル変数を作成します。

```
OPSHFI READ GLVTEMPO.DEVICE.*
```

OPSHFI コマンドプロセッサで共有ファイルを使用するには、GLVSHAREDFILE、GLVSHAREDDED、GLVSHAREDRESERVE、および GLVSHAREDRLS 製品のパラメータを適宜確認し、設定します。

UNIX System Services のインストール

CA OPS/MVS のベース インストールには、UNIX System Services 機能が含まれません。このセクションでは、パラメータ設定、JCL 変更、およびその他のカスタマイズのタスクについて説明します。

ベース インストールでは以下のことを実行できます。

- Address USS USSCMD を利用する。
- USS 処理の作成および終了用のパラメータをオンにします。これにより、それぞれのインスタンスに OPSLOG 内の USS イベントが提供されます。次に、AOF USS ルールを使用して自動化を行います。

UNIX System Services の機能の仕組み

UNIX System Services (USS) 機能は、OPS/REXX プログラムおよび AOF ルールを利用して、さまざまな機能を実行します。

USS 機能では、以下のタスクを実行できます。

- UNIX シェル コマンドの発行
- REXX 変数でのコマンド応答の受信
- USS プロセス作成および終了の監視

CCS for z/OS Event Management (EM) コンポーネントがインストールされている場合、以下も可能です。

- OPSLOG 内の z/OS EM コンソールに表示されるすべてのメッセージへのアクセス (z/OS USS syslogd メッセージも含む)
- AOF USS ルール タイプを使用して、z/OS EM メッセージに対応する
- コマンドおよびメッセージを OPS/MVS から z/OS EM または接続されているその他の CA EM プラットフォームへ送信

これらの機能を組み合わせることで、CA OPS/MVS の自動化の範囲が z/OS UNIX ドメインおよび CA NSM エンタープライズ マネジメント ネットワークまで広がります。

注: NOOUTPUT モードは、MSG、CMD、その他のように待機できない AOF ルール タイプから暗黙的に示されます。コマンド応答を `nowait` ルールから取得することはできません。

プロセス監視コンポーネントのアクティブ化

USS プロセス作成およびイベントの終了を監視するには、動的システム exit モジュールを exit ポイントでインストールするだけです。これは IBM 発行の「z/OS V1R4.0 Unix System Services Planning (GA22-7800-03)」に文書化されています。

プロセス監視コンポーネントをアクティブ化するには、INITUSSPROC パラメータおよび USSPROC RULES パラメータの両方の値を YES に設定します。AOF USS メッセージルールが書き込まれ、USS プロセス作成イベントと終了イベントを自動化します。

CCS for z/OS のイベント管理コンポーネントのインストール

CCS の z/OS EM コンポーネントとインターフェース接続したい場合、CCS for z/OS および EM コンポーネントもインストールする必要があります。

CCS for z/OS の EM コンポーネントをインストールする方法

1. USS ベースの z/OS Event Management コンポーネントをアクティブ化し、これらの USS メッセージ イベントを AOF に渡します。CCS の z/OS Event Management コンポーネントを起動するためのサンプルのスターティッドタスクが、そのコンポーネントにより提供されています。

イベント管理コンポーネントの実行に必要な CCS for z/OS コンポーネントの一覧については、付録「[CCS for z/OS コンポーネントの要件 \(P. 241\)](#)」を参照してください。

2. SYS1.OPS.CCLXCNTL の INSTUSEX メンバを実行します。

CA OPS/MVS USS メッセージ exit は、互換モード ディレクトリの z/OS EM HFS または zFS にコピーされ、z/OS EM によってインストールされたメッセージ exit のダミーバージョンと置き換えられます。

重要: CCS for z/OS または CA OPS/MVS メンテナンスのどちらかによりメッセージ exit モジュールが変更された場合、必ずこのジョブを実行してください。

z/OS EM とインターフェース接続を行う以下のアドレス USS コマンドを使用できます。CMD、WTO、WTOR、PING、REPLY、および DOM。

USS 機能のパラメータ

以下のパラメータは、CA OPS/MVS における USS 機能の初期化および関数を制御します。

- **INITUSS-OPSSPA00** 初期化 REXX プログラムで **YES** に設定する必要があります。
- **USSSTC-OPSUSS** ではない場合は、USS サーバに対してスターティッド タスク プロシージャの名前を含める必要があります。
- **USSSWAPPABLE-NO** に設定して、USS サーバをスワップ不可能にできます。
- **USSALLOWRESTART-YES** に設定して、失敗した USS サーバを再起動できるようにすることが可能です。
- **USSRULES-USS** メッセージ イベントを発生させるには、**YES** に設定します。
- **BROWSEUSS-YES** に設定して、OPSLOG で USS メッセージを表示できます。
- **USSACTIVE-ADDRESS USS REXX** ホストコマンドを使用して、USS コマンドを実行目的で USS サーバに送信するには、**ON** に設定します。
- **BROWSEUSSPROC-YES** に設定して、USS プロセスの作成メッセージおよび終了メッセージを OPSLOG に表示できます。
- **INITUSSPROC-USS** プロセスの監視コンポーネントをアクティブにするには、**OPSSPA00** 初期化 REXX プログラムで **YES** に設定します。
- **USSPROC-RULES-USS** プロセスの作成および終了イベントを発生させるには、**YES** に設定します。

セキュリティの問題

USS サーバは、自動化アプリケーションに対して適切なタイプの USS コマンドを実行するために、セキュリティプロファイルの USS セグメントにおいて十分な権限が付与されていなければなりません。必要な権限は、基本ユーザからスーパー ユーザまで範囲があります。USS の機能をアクティブにする前に、セキュリティ管理者に相談してください。

対象のコマンドを実行するうえで障害が発生した場合、そのコマンドに対する実行権限が不足しているか、またはそのコマンドが含まれているディレクトリにアクセスできないことが原因となっていることがあります。コマンドの発行者の権限に対してセキュリティ環境を動的に修正できる OSF TSO サーバとは異なり、USS サーバは、そのサーバの現行の権限ですべてのコマンドを実行します。したがって、あるユーザが発行できる USS コマンドのタイプを制限する方法としては、AOF セキュリティルールを使用するしかありません。

USS サーバの環境変数

CCS for z/OS コマンドの Event Management コンポーネントを、shell コマンドとして、または USS サーバからのダイレクト API コマンドとして実行するには、shell とサーバアドレス空間の両方でいくつかの環境変数を設定する必要があります。これを行うために、USS サーバは、ENVFILE DD ステートメントに指定されているファイルを USS サーバの初期化時に読み込みます。このファイルに、環境変数とその値が定義されています。CCS for z/OS コマンドが含まれている適切な CCS for z/OS ディレクトリをインクルードするよう、PATH 変数を設定する必要があります。CCS for z/OS のダイレクト API コマンドに対する CCS for z/OS ダイナミックリンクライブラリを参照するよう、LIBPATH 変数を設定する必要があります。他に、頻繁に使用されるその他の USS ベースのアプリケーションに対するコマンドディレクトリをインクルードするよう、PATH 変数を拡張することもできます。ENVFILE ができるだけシンプルになっているように、shell コマンドまたはスクリプトを使用して、PATH 変数へディレクトリを追加することをお勧めします。

また、ENVFILE において CA で始まる、CCS for z/OS の変数を指定することも必要です。ベースの CCS for z/OS ディレクトリ内の PROFILE ファイルから、名前と値を取得できます。ENVFILE の変数定義において、記号置換の値として \$CAIGLBL0000 を CA 変数で使用しないでください。\$CAIGLBL0000 が出てきた場合は、すべて実際の値で置き換えます。SYS1.OPS.CCLXCNTL のメンバ USSENV00 には、デフォルトの CCS for z/OS ディレクトリ名 (/cai/tngfw) 用に調整された変数定義およびコメントを持つ、サンプルの ENVFILE が含まれています。

OPSUSS JCL の変更

OPSUSS メンバの場合

- STEPLIB データセット名を、インストール時に指定された名前に変更します。SYS1.OPSCCLXLOAD がリンクリストまたは LPA 内にある場合、それを削除できます。CCLXPLD ロードライブラリを使用するのは USS サーバのみであり、またこのライブラリは権限が付与されていない PDSE であるため、リンクリストや LPA から除外する必要があります。このライブラリ名を、インストール時に付けられた名前に変更します。
- 以下の条件に当てはまる場合、TCP/IP クライアントのデータセットは SYSTCPD DD に割り当てられる必要があります。
 - TCP/IP がシステム上にインストールされている。
 - TCP/IP クライアントデータセットの各タスクへの自動割り当てが行われていない。
 - TCP/IP クライアントデータセット名が TCP/IP の動的割り当て検索シーケンスに従っていない。

- それ以外の場合、この DD ステートメントは削除してもかまいません。

注: 正しい判断であるかどうか確信を持ってない場合は、TCP/IP ネットワーク管理者に連絡してください。

- ENVFILE データセットは連続データセットまたは PDS メンバ (USS サーバアドレス空間およびサーバがアタッチしている UNIX シェルに設定される環境変数の名前と値を含む PDS メンバ) を参照する必要があります。CCS for z/OS API 呼び出しおよびコマンドの Event Management コンポーネントが正しく機能するために、特定の環境変数を設定する必要があります。SYS1.OPS.CCLXCNTL のメンバ USSENV00 には、これらの変数のサンプルが含まれます。

注: 各 z/OS システム上の変数値は異なる場合があります。正しい変数値を決定するための指示がサンプル メンバ内に含まれています。

- EXEC ステートメントの PARM フィールドには、USS サーバ起動時に実行する初期コマンドが格納されている場合があります。このコマンドは、以下のいずれかの値をとります。
 - キーワード USSCMD によって示され、次にコマンド テキストが続く USS シェル コマンド
 - ADDRESS USS ホスト コマンドと同じ構文を持つ CCS for z/OS API コマンドの Event Management コンポーネント

SERVER キーワードおよび SUBSYS キーワードを PARM フィールド内で変更しないでください。デフォルトのコマンド (USSCMD printenv) は、ENVFILE 処理後のサーバシェル内の現在の環境変数値を表示する UNIX シェル コマンドです。

トラブルシューティング

USS サーバ コマンドで、コマンドが見つからないことを示すリターンコードを受け取った場合は、コマンドのパス指定および PATH 変数の値をチェックします。USS コマンド echo \$VNAME を使用して、特定の環境変数の値を表示することができます。また、TSO ISHELL コマンドを使用して、互換モード構造の HFS または zFS を簡単に参照して、予想されるディレクトリにコマンドが存在することを確認することができます。

すべての USS サーバダイレクト API CCS for z/OS コマンドが異常終了した場合は、ENVFILE に定義されている LIBPATH 環境変数の値をチェックし、LIBPATH で指定されているディレクトリパスのどこかにファイル TNEM EVT2 が存在することを確認します。ディレクトリ名の値が含まれている、CA の他の変数値をチェックして、同様に確認します。USS ファイル名は、大文字と小文字が区別されます。

SUB=MSTR を使用して USS サーバが開始されており、システムの起動後、完全には初期化できなかった場合は、システムパラメータライブラリの COMMNDxx メンバの EZAZSSI に対する開始コマンドを変更して、EZAZSSI SUB=MSTR も開始するようにします。初期化されなかったすべての USS サーバを、キャンセル、または(キャンセルできなかった場合は)強制終了します。

USS のプロセス監視コンポーネントは、BPX_POSPROC_INIT、BPX_IMAGE_INIT、および BPX_PREPROC_TERM という名前の exit において、OPUSPREX モジュールを動的なシステム exit としてインストールします。

これらの exit で exit モジュールを表示および管理するには、z/OS コマンド `D PROG,EXIT,...` および `SETPROG EXIT,...` を使用します。動的な exit は、初期化時に OMVS カーネルによって作成されるので、CA OPS/MVS の開始時には存在していない可能性があります。製品の動的な exit インストール モジュールは、OMVS が exit を定義するまでサブタスク内で待機しています。該当する exit 名が見つかったときに、exit モジュールがインストールされます。

EPI コンポーネント用の VTAM 端末の作成

EPI コンポーネントを使用すると、LU2 のアクセス機能を持つすべての VTAM アプリケーションに対して、スクリーン スクレイプの自動化スクリプトを作成できます。このコンポーネントの設定は、作成する自動化アプリケーションによって決定されます。CA OPS/MVS の EPI コンポーネントが必要な場合には、VTAM 設定に対して以下のカスタマイズを実行してください。

EPI コンポーネント用の VTAM 端末を作成する方法

1. SYS1.VTAMLST にアプリケーションの定義を追加して、VTAM に対する EPI 仮想端末を定義します。EPI では、実際の 3270 端末をエミュレートするために 1 つ以上の VTAM アプリケーション定義が利用可能である必要があります。
2. SYS1.VTAMLST に新しいメンバを作成するには、以下のステートメントを使用します。各端末に対して 1 つの APPL ステートメントを指定します。

```

majname  VBUILD  TYPE=APPL
xxxxnnnn APPL    EAS=1,
                PARSESS=NO,
                MODETAB=modetab,
                DLOGMOD=logmode,
                PRTCT=vtampswd
xxxxnnnn APPL    ...
.
.
.

```

このステートメントで DLOGMOD オプションには、この端末が外部製品にログオンするときに使用される logmode テーブル エントリの名前が指定されます。構造化フィールドをサポートしていない、実際の 3278 モデル 2、3、または 4 タイプの端末に対して使用する名前を使用します。logmode はクエリビットをオンにしません。EPI DEFINE コマンドまたは CHANGE コマンドを発行するときに LOGMODE キーワードを指定すると、EPI はこの名前を上書きできます。EPI DEFINE コマンドまたは CHANGE コマンドを発行するときに LOGMODE キーワードを指定すると、EPI はこの名前を上書きできます。

上記の APPL ステートメントにおける他のオプションの有効値の詳細については、VTAM のドキュメントを参照してください。

3. EPI が仮想端末を有効化しようとするときに、VTAM で EPI VTAM APPLID をアクティブにします。通常は、VTAM の起動時に APPLID をアクティブにします。VTAM が完全にアクティブになってから APPLID をアクティブにする場合は、EPI 仮想端末定義をアクティブにするときに以下の VTAM オペレータコマンドを使用することができます。

```
VARY NET,ACT,ID=majnode
```

```
majnode
```

EPI APPL ステートメントが格納されている SYS1.VTAMLST のメンバ名を指定します。

CA OPS/MVS AOF コンポーネントを使用して、VTAM の初期化の最後にこのコマンドを発行することも、OPSVIEW を使用して発行することもできます。

NetView インターフェースのインストール

CA OPS/MVS NetView インターフェースをインストールするには、以下の手順に従います。

1. NetView の非送信要求メッセージストリームにアクセスするには、モジュール OPNVEX11 を、NetView exit のエイリアス名である DSIEX11 に再リンクする必要があります。SMP/E を使用して DSIEX11 というエイリアスを追加するには、ライブラリ SYS1.OPS.CCLXCNTL(USEREX11) に含まれている usermod OPUM003 を適用します。必要な場合は、exit モジュール OPNVEX11 およびエイリアス DSIEX11 を、SYS1.OPSCCLXLOAD から NetView STEPLIB 連結内のライブラリへコピーします。DSIEX11 exit がすでに NetView 内にある場合は、<productname> で提供されている exit にロジックが含まれるように修正します。exit DSIEX11 を、SYS1.OPSCCLXLOAD から NetView STEPLIB 連結内のライブラリへコピーします。

DSIEX11 は、ソース形式で SYS1.OPS.CCLXASM 内にあります。この exit は非送信要求メッセージをマスタ コンソールへ送信し、次にサブシステム インターフェースを通じてそれらのメッセージをルーティングします。CA OPS/MVS はここでこれらのメッセージにアクセスし、自動化できます。

重要: ある時点で、もう DSIEX11 exit を使用しないと決めた場合は、ロードライブラリからエイリアス名を安全に削除できます。DSIEX11 exit は OPNVEX11 モジュールの単なるエイリアス名です。

2. SYS1.OPS.CCLXEXEC(OPSALEERT) を、NetView DSICLD 連結内のデータセットにコピーします。このプログラムは NetView REXX EXEC です。

3. NetView と MCS マスタ コンソール間の接続を確立します。CA OPS/MVS ルールまたは REXX プログラムから NetView コマンドを発行するためのインターフェイスは同じです。これは z/OS コンソールから NetView コマンドを発行できるように、IBM が提供しています。

NetView AUTOTASK コマンドを使用して、MCS マスタ コンソールと NetView ユーザ ID 間の関係を作成します。このコマンドは、NetView 端末で発行することも、NetView の initial CLIST メンバで発行することもできます。

このコマンドの構文は以下のとおりです。

```
AUTOTASK CONSOLE=consolenumber,OPID=operatorid
```

consolenumber

MCS のコンソール番号。

operatorid

MCS コンソールに関連付ける NetView のオペレータ ID。NetView のオペレータ ID は、NetView パラメータ データ セットの DSIOPF メンバに定義されています。

CA OPS/MVS NetView インターフェイスでは、NetView のオペレータ ID と MCS マスタ コンソール間で関係が確立されているとみなしています。NetView を開始したときにユーザに対して AUTOTASK コマンドを発行するには、NetView の start up CLIST を修正することを検討してください。

4. NetView の startup CLIST を修正して、以下のコマンドを発行します。

```
OPSALERT NOTIFY
```

このコマンドは、NPDA の一連のレコーディング フィルタ設定 (SRF) コマンドを発行して、NetView のアラート情報に CA OPS/MVS がアクセスできるようにします。NetView のインストール プロセスの手順 2 が完了した後で、NetView を再開せずに、このコマンドを発行することができます。

5. SYS1.OPS.CCLXCNTL(OPSAUTO) のメッセージ テーブル エントリを、NetView の自動メッセージ テーブルにコピーします。NetView の自動メッセージ テーブルがない場合は、NetView DSIPARM 連結内のデータ セットに OPSAUTO メンバをコピーして、以下のコマンドを発行します。

```
AUTOMSG MEMBER=OPSAUTO
```

NetView の起動時にこのコマンドが自動的に呼び出されるようにするには、コマンドを NetView の start up CLIST に配置します。

NetView のメッセージ テーブルがすでにある場合は、メッセージ テーブルのエントリを既存のメッセージ テーブルの最後にコピーし、AUTOMSG コマンドを使用して再度アクティブ化します。

6. SYS1.OPS.CCLXEXEC(ALERT) を、CA OPS/MVS ルールがアクセス可能なライブラリ (SYSEXEC 連結内のライブラリ) へコピーします。これにより、CA OPS/MVS ルールおよびプログラムが ALERT 関数を使用できるようになります。
7. CA OPS/MVS メッセージルールは、MSG.AFLAGS 変数のビットを設定することも、リセットすることも可能です。
詳細については、「*AOF Rules User Guide*」を参照してください。
8. NetView のコマンドプロセッサとして実行できる、POI コマンドプロセッサのサブセットを使用するには、NetView parmlib の DSICMD メンバに各コマンドプロセッサを定義します。

以下に例を示します。

```
*-----*
*   CA OPS/MVS NETVIEW CAPABLE POI COMMANDS   *
*-----*
OPSGETV  CMDMDL  MOD=OPSGETV,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
OPSGETVL CMDMDL  MOD=OPSGETVL,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
OPSSETV  CMDMDL  MOD=OPSSETV,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
OPSDELV  CMDMDL  MOD=OPSDELV,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
OPSQL    CMDMDL  MOD=OPSQL,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
*-----*
*   AUTOMATE/MVS COMMAND ALIASES OF OPSMODE  *
*-----*
GETVAR   CMDMDL  MOD=GETVAR,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
GETVARL  CMDMDL  MOD=GETVARL,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
SETVAR   CMDMDL  MOD=SETVAR,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
DELVAR   CMDMDL  MOD=DELVAR,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
SQL      CMDMDL  MOD=SQL,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
OPSMODE  CMDMDL  MOD=OPSMODE,TYPE=R,RES=Y,PARSE=N
          CMDCLASS=1,2,3
```

この例で定義されているロード モジュールが、システム linklist または LPA で使用できない場合は、CA OPS/MVS ロード ライブラリに対する STEPLIB を NetView のプロシージャ JCL に追加してから、ライブラリを APF 権限付与済みにする必要があります。Automate と CA OPS/MVS のバージョンの同じコマンドが、OPSMODE コマンドを介して選択的に使用されている場合は、Automate ロード ライブラリの前に、CA OPS/MVS のロード ライブラリを検索する必要があります。

1 つのシステムで複数の CA OPS/MVS サブシステムをアクティブにすることができるので、対象サブシステム名に対してすべてのコマンド要求をデフォルトでルーティングするには、OPSS\$xxxx という ddname を持つダミーのデータ セットを割り当てます。ここで xxxx はサブシステム名です。割り当てを行うには、JCL または NetView ALLOCATE コマンドを使用できます。OPSS はデフォルトのサブシステム名です。以下に例を示します。

```
ALLOC FILE(OPST) DUMMY  
//OPST DD DUMMY
```

CA OPS/MVS のセキュリティルールでは現在、グローバル変数のアクセスをセキュリティチェックするための NetView ユーザ ID にアクセスできません。NetView のコマンド プロセッサにグローバル変数へのアクセスを許可するには、NetView のアドレス空間に対して汎用的なセキュリティルールを有効にする必要があります。以下に例を示します。

```
)SEC OPSGLOBAL*  
)PROC  
  If Opsinfo('JOBNAME') = 'netview job name' Then  
    Return 'ACCEPT'  
  Else  
    Return 'NOACTION'  
)END
```

NetView Operator Facility のインストール

NetView Operator Facility (NOF) のインストールでは、CA OPS/MVS と NetView の両方の環境を変更する必要があります。NOF のインストールについて支援を受ける為、ご使用のサイトの NetView のシステムプログラマに 問い合わせを望む場合もあるかもしれません。

NOF は CA OPS/MVS の配布メディアにあります。以下のライブラリを使用します。

- CA OPS/MVS のサンプル ルール ライブラリ OPS.CCLXRULBS
- CA OPS/MVS の NetView CLIST ライブラリ OPS.CCLXCLSO

注: このライブラリは可変ブロックフォーマットでも提供されています。

- CA OPS/MVS ロード ライブラリ、OPSCCLXLOAD
- CA OPS/MVS の制御ライブラリ OPS.CCLXCNTL

NOF をインストールする方法

1. 以下の手順のいずれかを実行して、NOF で提供されているサンプルのルールを格納するためのルール セットを作成します。
 - 新しいルール セットを作成します。
 - OPS.CCLXRULB のすべてのメンバを既存のルール セットにコピーします。

サイトで CA OPS/MVS の SECURITYRULESET パラメータを使用している場合は、OPNFSEC をセキュリティルール セットにコピーします。OPNFSEC は、CA OPS/MVS のグローバル変数に対する NetView のアクセスを提供するセキュリティルールです。OPS.CCLXCNTL データセット内の OPNFCPYR ジョブを使用して、OPNFSEC およびその他の NOF ルールをコピーできます。

2. OPS.CCLXCLSO から NetView の DSICLD 連結のライブラリへ、NetView の REXX プログラムをコピーします。この処理を行うには、OPS.CCLXCNTL データセット内の OPNFCPYE ジョブを使用します。

注: NetView の STEPLIB 連結に対して、CA OPS/MVS のロード ライブラリを単純に連結すると、CA OPS/MVS DSIEX11 モジュール(以前の CA OPS/MVS NetView インターフェースの一部)が制御を行います。この章の「NetView インターフェースのインストール」を参照してください。

3. OPSCCLXLOAD ライブラリを NetView で使用できるようにします。CA OPS/MVS のロード ライブラリが z/OS LNKLST にある場合は、NetView にはすでにそのロード ライブラリに対するアクセス権限があります。ない場合は、以下のロード モジュールを、OPSCCLXLOAD からユーザの NetView の STEPLIB ライブラリへコピーする必要があります。OPS.CCLXCNTL データセット内の OPNFCPYL ジョブを使用して、この処理を行うことができます。

OPNFSGLV を使用すると、NetView が CA OPS/MVS グローバル変数を設定できます。

4. OPS.CCLXCNTL データライブラリの OPNFATBL メンバのエントリを、NetView のメッセージ自動テーブルにインクルードします。これらのエントリは、CA OPS/MVS が対象とするイベントをトラップします。OPNFATBL エントリをインクルードするには、NetView %INCLUDE 機能を使用することをお勧めします。この方法を使用すると、CA OPS/MVS のテーブル エントリを別に保持できるからです。
5. OPSMAIN は NetView を開始したときに自動的に始まるタスクなので、OPSMAN というユーザ ID を NetView に設定します。OPNFATBL メンバを変更してメッセージをルーティングする場合は、既存の autotask を使用できます。

注: NetView の TASKUTIL コマンドを使用して NOF のリソース消費を追跡できるので、新しい autotask を使用する方が適切です。autotask を作成する最も簡単な方法は、NetView の標準 autotask である AUTO1 の autotask 定義をコピーすることです。

6. (オプション) NetView の STATMON インターフェースを使用する場合は、SENDMSG というテキストで始まるステートメントからコメントを削除して、NetView のパラメータライブラリ(通常は DSIPARM)の DSICMN メンバを修正します。これらのステートメントをアクティブにすると、管理対象のリソースの状態が変わるたびに、NetView のステータス モニタで CNM094I のメッセージが発行されます。どのタイプのリソースでこれらのメッセージを生成するかを決めておくと、CNM094I メッセージの量を調節できます。
7. NetView のサブシステム アドレス空間がアクティブになっていることを確認します。これは、NetView のアラートを生成するのに必要です。このアドレス空間を管理するには、CA OPS/MVS System State Manager の機能を使用できます。

注: OPS/REXX の OPSNETV 関数を使用して、NetView サブシステムのアドレス空間のステータスを確定できます。OPSNETV の詳細については、「*User Guide*」を参照してください。

8. NetView LOADCL コマンドを使用して、NOF REXX プログラムをストレージにロードします。このようにすると NetView は、すべてのメッセージおよびアラートについて、ディスクから取得する代わりに、プログラムのストレージ内コピーを使用することができます。

9. 適切なアラートフィルタリングコマンドを発行するよう、NetView の起動プロセスを修正します。具体的なコマンドは次のとおりです。

NPDA SRF (レコーディングフィルタ設定)

保存しておくアラートを指定し、不要なアラートを除外します。すべてのアラートを NPDA へ転送し、NPDA 画面で表示し、CA OPS/MVS で自動化するには、NetView の startup CLIST 内で、または NetView がアクティブになった後で、以下のコマンドを発行する必要があります。

```
NPDA SRF AREC PASS DEFAULT
```

NPDA SVF (表示フィルタ設定)

どのアラートを表示するかを指定します。CA OPS/MVS によって生成されたすべてのアラートが NPDA ディスプレイに表示されるようにするには、NetView の start up CLIST 内で、または NetView がアクティブになった後で、以下のコマンドを発行します。

```
NPDA SVF PASS DEFAULT
```

上記に記載されている手順を完了すると、NOF を使用する準備ができます。NetView の新しいメッセージ自動テーブルをアクティブにすると、NOF は、既存の DSIEX11 モジュールのように動作します (つまり、DSIEX11 モジュールが非送信要求 VTAM メッセージをコンソールにエコーすると、NOF も同様にします)。この時点で、OPNOF コマンドを使用して NOF パラメータを設定すると良いでしょう。

Tivoli OMEGAMON XE のインターフェースの設定

CA OPS/MVS AOF コンポーネントは、Tivoli OMEGAMON XE on z/OS 製品のすべて、または一部で検出された例外に対して応答できます。これは、CA OPS/MVS が現在、以下の製品と連携できることを意味します。

- Tivoli OMEGAMON XE on z/OS
- Tivoli OMEGAMON for IMS on z/OS
- Tivoli OMEGAMON XE for CICS on z/OS
- Tivoli OMEGAMON XE for DB2 Performance Monitor/Expert on z/OS

例外分析のプロセス

すべての Tivoli OMEGAMON XE on z/OS 製品に共通の機能は、*例外分析*です。Tivoli OMEGAMON XE on z/OS 製品は、例外的な状況を検出するために監視対象システムを n 秒ごとに分析し、これらの例外をメッセージとして OMEGAMON 端末上に報告します。一般的に例外分析では、問題なく稼動しているシステムで多数の例外を検出しますが、実際には、これらの例外すべてが実際の画面に表示されるわけではありません。

例外分析プロセスへのインターフェース

AOF は OMEGAMON の例外メッセージを直接自動化することはできません。これらのメッセージは z/OS コンソール サポートを介してルーティングされないためです。幸い、すべての Tivoli OMEGAMON XE on z/OS 製品は、各分析の間隔の最後に、論理的な例外画面のコピーを書き込むログ ファイルをサポートしています。OMEGAMON の論理画面のサイズは起動パラメータの 1 つになっており (LROWS)、ユーザは通常、実際の画面の行数よりもかなり大きく論理画面のサイズを設定します。したがって、場所が足りず、OMEGAMON の実際の画面に重要な例外メッセージが表示されないことがあったとしても、これらのメッセージは OMEGAMON の論理画面上には収まり、ログ ファイルに書き込まれています。

OMEGAMON へのインターフェース

CA OPS/MVS と OMEGAMON 間のインターフェースを確立するには、OMEGAMON JCL プロシージャに OxREPORT DD ステートメントを挿入します。このステートメントは、SUBSYS キーワードを使用して、CA OPS/MVS をそのファイルのターゲットとして特定します。

```
SEND OMEGAMON MVS EXCEPTIONS TO CA OPS/MVS
//OMREPORT DD SUBSYS=(OPSS,OMEGAMON,MVS),
// DCB=(RECFM=FBA,LRECL=81,BLKSIZE=81)
SEND OMEGAMON CICS EXCEPTIONS TO CA OPS/MVS
//OCREPORT DD SUBSYS=(OPSS,OMEGAMON,CICS),
// DCB=(RECFM=FBA,LRECL=81,BLKSIZE=81)
SEND OMEGAMON CICS EXCEPTIONS TO CA OPS/MVS;
IDENTIFY SOURCE CICS SYSTEM
//OCREPORT DD SUBSYS=(OPSS,OMEGAMON,CICS,CICSTEST),
// DCB=(RECFM=FBA,LRECL=81,BLKSIZE=81)
SEND OMEGAMON IMS EXCEPTIONS TO CA OPS/MVS
//OIREPORT DD SUBSYS=(OPSS,OMEGAMON,IMS),
// DCB=(RECFM=FBA,LRECL=81,BLKSIZE=81)
SEND OMEGAMON DB2 EXCEPTIONS TO CA OPS/MVS
//ODREPORT DD SUBSYS=(OPSS,OMEGAMON,DB2),
// DCB=(RECFM=FBA,LRECL=81,BLKSIZE=81)
```

この JCL 例の形式は次のとおりです。

```
//ddname DD SUBSYS =(ssid,OMEGAMON,type{,reportid})
```

ddname

ファイルに関連付けられる *ddname* を指定します。

ssid

これらのメッセージが送信される、CA OPS/MVS の 4 文字のサブシステム ID を指定します (通常は OPSS)。

type

特定の Tivoli OMEGAMON XE on z/OS 製品を指定します。 *type* として、MVS、CICS、IMS、または DB2 を使用できます。

reportid

(オプション)メッセージの出力元を特定するためにルールにおいて使用できる一意のレポート ID を指定します。

起こりえる懸念事項

SUBSYS=*name* を指定する DD カードを持つ JCL プロシージャを起動する際にサブシステム名がアクティブでない場合、START コマンドは失敗し JCL エラーとなります。一般的に CA OPS/MVS は IPL の初期に起動し、IPL が終了するまで稼働し続けるため、これは問題にはなりません。

CA OPS/MVS に例外を渡している OMEGAMON タスクを止めずに、CA OPS/MVS の停止および再起動が可能です。CA OPS/MVS は、再起動の際に例外処理を継続します。

OMEGAMON 例外の供給

正しい出力が **OxREPORT** ファイルに必ず書き込まれるようにするには、**OMEGAMON** のカスタマイズが必要となります。カスタマイズ作業には、プロファイルを作成および定義するためのしきい値とオプションの選択が含まれます。**OMEGAMON** ユーザ プロファイル機能を使用して、これらのパラメータをカスタマイズします。

AOF を使用して **OMEGAMON** の例外を自動化する際には、以下に注意します。

1. **CA OPS/MVS** を **OMEGAMON** の前に起動する必要があります。
2. **OMEGAMON** セッションは、例外イベント処理を供給するためにはアクティブである必要があります。専用モード ターミナルがコンソール (常に例外分析画面の左側に位置します) の隣にある場合、そのターミナルを使用して例外データを提供します。ターミナルが頻繁にほかの画面を表示する場合は、オペレータが例外をその他の機能に使用する際に、重要な例外が欠損する恐れがあります。**CA OPS/MVS** が例外を監視できるのは、例外分析画面がアクティブになっているときのみです。

最も簡単なインターフェース設定方法は、例外分析が常にアクティブである専用セッションを持つことです。ただし、この解決法には 2 つの欠点があり、1 つめは前段落に記述されたとおりです。2 つめの欠点は、ローカルにアタッチされた **3270** デバイスを必要とすることです。

別の解決方法は、**EPI** 論理ターミナルを備えた **OMEGAMON VTAM** インターフェースを使用することです。この解決方法は設定がより複雑ですが、専用 **3270** ターミナルに関連する両方の問題が除去されます。**EPI** セッションは非表示であるため、ほかのユーザに画面を変更されることはありません。**EPI** がバーチャル **3270** として利用されるため、**3270** 実ターミナルは必要ありません。

3. **OMEGAMON** スターティッド タスク **JCL** の **LROWS** パラメータを確認し、すべての例外が **OxREPORT** ファイルに書き込まれる論理画面に合うようにします。**LROWS** パラメータのデフォルト値は物理画面を 2 倍したのから 1 を差し引いた値で、最大値は 999 です。

- すべての例外 **BOX** パラメータを **NO** に設定するか、インストールまたはユーザプロファイルでボックスをオフにして、すべての例外をアンボックス化する必要があります。デフォルトプロファイルを変更することはできません。制御オプションを **.SET** コマンドで設定したり、**XACB** コマンドか **XSET** コマンドのどちらか、または両方を使って例外しきい値を設定したりできます。テストではこれらのコマンドを実際に発生する例外分析画面で使用しますが、実稼動では、インストールまたはユーザプロファイル内に配置して **OMEGAMON** 起動時に実行させます。

注: **OMEGAMON** インストール手順のコマンドと実際のコマンドは、プラットフォームによって異なる場合があります。上記で参照されたコマンドは、**MVS** 用の **OMEGAMON** 固有のものである場合があります。**IMS**、**CICS**、および **DB2** リリース用の該当するインストールガイドを参照してください。

- OMEGAMON OxREPORT** ファイルのページ制限をより高い数値に設定してください。これを行うには、画面領域で **.PLM 999999999** を指定するか、可能な場合はユーザプロファイルで **PAGELIMIT** オプションを使用します。
- OMEGAMON** ログ機能はオンである必要があります。**LOGON** コマンドを **OMEGAMON** に発行して、**OxREPORT** ファイルに画面を書く必要があります。

専用ターミナルの **OMEGAMON 7.1.0** および **OMEGAMON II** 設定は以下のとおりです。

初期画面領域を作成し、**OMEGAMON** 画面領域作成のためのルールに従って、以下のコマンドを別々の行に入力します(コマンドは **2** カラム目から開始します)。

```
OUTP REPORT
DDNM OPREPORT      (または、proc で使用された DDNAME ならどれでも)
.LOGOUT
.LOGON
.FGO exscrn

exscrn
```

例外分析コマンドを含む画面領域の名前を指定します。

OMVTAM のための OMEGAMON II 設定:

- a. 初期画面領域を作成し、OMEGAMON 画面領域作成のためのルールに従って、以下のコマンドを別々の行に入力します(コマンドは 2 カラム目から開始します)。

```

OUTP REPORT
DDNM OPREPORT      (OMREPORT は使用できません)
.LOGOUT
.LOGON
.FGO exscrn
    
```

- b. OMVTAM にログオンします。

```

LOGON APPLID(OMVTAM) DATA('FSCR=yyyy')
YYYY
    
```

上記のコマンドを含む画面領域の名前を指定します。初期画面領域(専用または VTAM モード)の目的は、OMEGAMON の起動時にロギング機能を設定することです。続いて .FGO コマンドによって制御が例外分析画面領域に移されます。その後、制御は例外分析画面に残り、例外分析処理を定期的に行います(OMEGAMON セッションが自動更新モードである必要があります)。

7. 例外分析はコマンド LEXSY(OM の場合)、LXIMS(OI の場合)、または LCXSY(OC の場合)で呼び出します。コマンドを 1 カラム目から指定し、プレフィックス「L」を必ず付けます。プレフィックス L は、メッセージと併せて 4 文字の名前を画面に置くことによって例外をラベル付けするよう OMEGAMON に指示します。これらの例外名は、CA OPS/MVS が OMEGAMON ルールを呼び出すために使用するメッセージ ID です。

この時点で、OMEGAMON メッセージが OPSLOG に表示されており、メッセージを受けて実行されるようルールを有効化できます。各例外は画面が更新されるたびにメッセージを生成するため、OPSLOG が重要ではないメッセージでいっぱいにならないよう例外しきい値と更新時間を確認することをお勧めします。

OMEGAMON メッセージが OPSLOG に表示されないようにするには、CA OPS/MVS BROWSEOMG パラメータを使用してください。BROWSEOMG の値を OFF に設定した場合、SAY ステートメントまたはルール内で処理される例外メッセージのテキストを報告する ADDRESS WTO ホストコマンドを含めることによって、OMEGAMON ルールを実行する OMEGAMON メッセージの発生を監査することができます。

OMEGAMON Exception Logging Facility (XLF)を使用するライセンスがある場合、XLFLOG DD を OMEGAMON レポートファイルの代わりに使用してください。XLFLOG には、CA OPS/MVS への例外イベントを OMEGAMON のサイクルごとに繰り返し生成しないという利点があります。XLFを使用する場合、持続および制限のための OMEGAMON 例外分析値をカスタマイズする必要があります。

MVS/QuickRef インターフェースのインストール

ISPF において ChicagoSoft MVS/QuickRef 製品のインターフェースを使用したい OPSVIEW ユーザに対しては、MVS/QuickRef ロード モジュールへのアクセス権を与える必要があります。これを行うには、LNKLIST、LPALIB、STEPLIB、または ISPLLIB の連結内にモジュールを配置します。

MVS/QuickRef のデータベース名は、MVS/QuickRef オプション モジュール (QWIKOPTS)内に指定することを強くお勧めします。このようにしない場合は、CA OPS/MVS QUICKREFDBASE パラメータを介して MVS/QuickRef のデータベース名を指定します。MVS/QuickRef のオプション テーブルを変更する指示については、MVS/QuickRef のドキュメントを参照してください。

任意のユーザについて、LOGON プロシージャで適切なデータベースを割り当てることによって、各ユーザにおいて別々の MVS/QuickRef データベースを使用できます。または、TSO ALLOCATE コマンドによって、この処理を動的に行うこともできます。詳細については、MVS/QuickRef のドキュメントを参照してください。

注: OPSVIEW ユーザは、MVS/QuickRef ロードモジュールにアクセスできる必要があります。そのためには、ロード モジュールを LINKLIST、LPALIB、STEPLIB、または ISPLLIB の連結に配置します。

QUICKREFTYPE 製品パラメータは、デフォルトのままにするか、または TSOHELP に設定する必要があります。これにより、最新の CA OPS/MVS メッセージ情報が、MVS/QuickRef データベースではなく CA OPS/MVS ヘルプ ファイルから取得されるようになります (MVS/QuickRef データベースは多くの場合、実行中の製品のバージョンと一致しません)。

OPSQW コマンドの可用性の確認

必要な場合は、OPSQW コマンドが、CA OPS/MVS の配布メディアの OPBOCMDS コマンド テーブル内にあることを確認します。OPSQW コマンドを追加するには、同時に OPSLOG Browse を使用している場合を除いて ISPF/PDF オプション 3.9 を使用します。

注: OPSLOG Browse を使用している場合は、ISPF KEYS コマンドを使用して、OPSQW コマンドを適切な PF キーに割り当てることができます。

CA 7 WA インターフェースの設定

CA OPS/MVS および CA 7 WA 間のインターフェース接続によって、CA OPS/MVS は CA 7 WA へのコマンド送信および CA 7 WA Browse ログ宛のメッセージ処理が可能になります。

CA 7 WA へのコマンド送信

CA OPS/MVS による CA 7 WA へのコマンド送信には 2 つの方法があります。これら 2 つの方法についての説明を以下に示します。

■ 方法 1- ADDRESS CA7 ホスト REXX 環境からコマンド発行

この方法では、CA OPS/MVS OPS/REXX プログラムが CA 7 WA にコマンドを送信してコマンド応答を受信できる、双方向インターフェースが可能です。以下の手順を実行し、このタイプのコマンド インターフェースを実施します。

- CA 7 WA リリース 3.3 以降であることを確認します。
- CA GSS がアクティブであることを確認します。これは CCS for z/OS テープからインストールすることができます。
- ADDRESS CA7 IMOD を CA GSS プロシージャに追加します。CA 7 WA のテクニカル サポートに連絡し、以下の IMOD ステートメントを確認します。

```
ADDRESS CA7 CAL2X2WR 15 DETACH TYPE 0
```

上記すべての条件を満たすと、CA OPS/MVS OPS/REXX プログラム内にコード化された ADDRESS CA7 ホスト REXX ステートメントからコマンド応答を発行および受信できます。この例については、CA OPS/MVS のインストール中に作成された *hlq.SAMPLES* データセットのメンバ ADDRCA7 を参照してください。

■ 方法 2 - OPS/REXX OPSCA7 関数からコマンド発行

この方法では、U7SVC ルーチンを使用して、CA OPS/MVS から CA 7 WA にコマンドを発行します。この方法を利用する場合、コマンド応答は発行元の CA OPS/MVS OPS/REXX ルールまたは OPS/REXX プログラムに返されません。追加インストールは必要ありません。

OPSCA7 関数の詳細については、「*Command and Function Reference*」を参照してください。

CA 7 ブラウズ ログへのアクセス

CA 7 WA ブラウズ ログにアクセスするには、ENF データベースにデータコントロール モジュール (DCM) を追加する必要があります。

CA 7 WA ブラウズ ログにアクセスする方法

1. CA 7 WA リリース 3.3 以降をインストールします。
2. CA OPS/MVS INITCA7 パラメータを、OPSSPA00 メンバ内で YES に設定します。CA OPS/MVS に ENF 関連のトレースメッセージを生成させたい場合は、CA OPS/MVS DEBUGENF パラメータも YES に設定する必要があります。さらに、CA 7 WA が作成するブラウズ メッセージの量によっては、CAIENFMAX パラメータおよび CAIENFRATE パラメータのデフォルト値を調整する必要もあります。これらのパラメータの詳細については、「*Parameter Reference*」を参照してください。
3. DCM を ENF に追加します。SAMPJCL に L232DCM1 ジョブが含まれているかどうか、CA 7 WA テクニカル サポートに確認してください。

このジョブは CA 7 WA ブラウズ イベントをインストールします。すべてのインストール済み DCM をリストする ENF EVENT コマンドにより、以下のように表示されるはずです。

```
DCM module name: CAL2DCM1 Description: CA 7 BROWSE EVENT Installed  
date: 01.010 time: 11:25:20
```

ハードウェア サービス (HWS) の設定

CA OPS/MVS ハードウェア サービス (HWS) をアクティブにするには、必要に応じて初期化パラメータを設定する必要があります。また、HWS はハードウェア インターフェース サービスに接続するので、CA OPS/MVS を実行しているシステムでハードウェア インターフェース サービスが使用可能である必要があります。

HWS パラメータ

HWS をアクティブにするには、INITHWS パラメータを YES に設定する必要があります。

```
OPSPRM('SET', 'INITHWS', 'YES')
```

INITHWS を YES に設定すると、一般的な CA OPS/MVS ハードウェア サービス コンポーネントがアクティブになります。ハードウェア イベント通知をアクティブにするには、パラメータ HWSRULES も YES に設定する必要があります。

```
OPSPRM('SET', 'HWSRULES', 'YES')
```

HWSRULES が YES に設定されている場合、HWS は、API ルールで自動化可能な API イベントの形式で、ハードウェア イベント通知を提供します。

HWS は、初期化パラメータを使用して、いつでもアクティブまたは非アクティブにできます。

ハードウェア イベントタイプおよび関連する変数 (HWS イベント通知で使用できません) の詳細については、「*CA OPS/MVS AOF Rules User Guide*」の「Hardware Event API Rules」を参照してください。

注: CA OPS/MVS を初期化した後に INITHWS の値を NO から YES に変更した場合、変更後の値を有効にするには、z/OS コマンド `MODIFY OPSS,RESTART(HWS)` を発行する必要があります (OPSS は CA OPS/MVS のサブシステムの名前)。

INITHWS パラメータと HWSRULES パラメータの詳細については、「*CA OPS/MVS Parameter Reference Guide*」の「Hardware Services (HWS)」を参照してください。

ハードウェア イベントは OPS API イベントとして提供されるので、ハードウェア イベントを受信するには、OPS API インターフェースもアクティブにする必要があります。OPS API インターフェースをアクティブにするには、OPS APIACTIVE パラメータを YES に設定します。

```
OPSPRM('SET', 'APIACTIVE', 'YES')
```

APIACTIVE パラメータの詳細については、「*CA OPS/MVS Parameter Reference Guide*」の「Application Programming Interface Parameters」を参照してください。

API ルールのコーディングに関する一般的な情報およびハードウェア イベント API ルールのコーディングに固有の情報については、「*CA OPS/MVS AOF Rules User Guide*」の「Generic Event Application Program Interface」を参照してください。

CA OPS/MVS で HWS 関連のトレースメッセージを生成させるには、DEBUGHWS パラメータを ON に設定します。

```
OPSPRM('SET','DEBUGHWS','ON')
```

ハードウェア インターフェース サービスの設定

HWS は、ハードウェア インターフェース サービスを利用します。ハードウェア インターフェース サービスは、CA Technologies 製品がハードウェア機能にアクセスする際の共通インターフェース API を提供します。CA OPS/MVS は、ハードウェア インターフェース サービスに接続して、HWS 機能を実行します。したがって、HWS でハードウェア イベント通知などのサービスを提供するには、CA OPS/MVS を実行しているシステムで、ハードウェア インターフェース サービスを設定し、開始する必要があります。

ハードウェア インターフェース サービスのインストールおよび設定

ハードウェア インターフェース サービスのインストール、設定、および操作については、「*Hardware Interface Service Component Guide*」を参照してください。

Linux Connector インターフェース (LXC) の設定

CA OPS/MVS Linux Connector インターフェース (LXC) は、非送信請求 VM および Linux メッセージを自動化する機能を提供します。これらのメッセージは、同じシステム上で実行される Linux Connector Component 製品によって CA OPS/MVS に転送されます。Linux Connector コンポーネントは、接続されている VM および Linux システムに対するコマンドおよび応答処理も提供します。LXC は、VM および Linux ゲストシステムと直接通信することはありません。

Linux Connector コンポーネントのセットアップ

Linux Connector コンポーネントのインストール、設定、操作の詳細については、「*CA Mainframe Connector for Linux on System z Installation Guide*」を参照してください。

注: CA OPS/MVS のメインアドレス空間は、通信の相手先となる適切な TCP/IP スターティッド タスクを判断するために、TCP/IP データセット (hlq.TCPIP.DATA) に対する読み取りアクセス権限が必要です。データセットは DD 名 SYSTCPD に自動的に割り当てられる必要があります。これは、OS によって CA OPS/MVS のインストール時に実行される REXX プログラムを使用して明示的に、または OPSMAIN スターティッド プロシージャ内の JCL ステートメントを使用して行われます。

LXC パラメータ

LXC をアクティブにするには、INITLXC パラメータを YES に設定する必要があります。

```
OPSPRM('SET', 'INITLXC', 'YES')
```

INITLXC を YES に設定すると、LXC サブタスクは Linux Connector コンポーネントに接続し、接続されている VM および Linux システムからの非請求メッセージの受信を開始します。

パラメータ LXCONMSG および LXCONCMD は、それぞれ Linux Connector コンポーネントパラメータ MSGTOKEN および CMDTOKEN の値に一致する必要があります。これらのパラメータ値は、z/OS 名前/トークン ペアの名前部分です。このペアには、非請求メッセージおよびコマンド処理 IP サーバの IP ポート番号が含まれます。デフォルトの CA OPS/MVS パラメータ値が Linux Connector コンポーネント値と一致しない場合は、以下のようなステートメントを使用してパラメータを設定します。

```
OPSPRM('SET', 'LXCONMSG', 'CAMSGTOKENVAL:')  
OPSPRM('SET', 'LXCONCMD', 'CACMDTOKENVAL:')
```

非送信請求メッセージ AOF API ルール イベントをアクティブにするには、パラメータ LXCRULES を YES に設定します。

```
OPSPRM('SET', 'LXCRULES', 'YES')
```

VM および Linux メッセージに添付されている特殊なメッセージ ID 値で 1 つ以上の AOF API ルールをコーディングして、VM および Linux システムの自動化およびトラッキングを実装します。Linux Connector API イベントタイプおよび関連する変数の詳細については、「*CA OPS/MVS AOF Rules User Guide*」でトピック「Linux Connector API Rules」を参照してください。

BROWSELXC パラメータを YES に設定して、OPSLOG で CA OPS/MVS に渡される Linux Connector コンポーネント非送信請求メッセージ イベントを含めます。このパラメータを次のように設定します。

```
OPSPRM('SET', 'BROWSELXC', 'YES')
```

CA OPS/MVS で LXC 関連のトレースメッセージを生成するには、DEBUGLXC パラメータを ON に設定します。

```
OPSPRM('SET', 'DEBUGLXC', 'ON')
```

LXC は、初期化パラメータを使用して、いつでもアクティブまたは非アクティブにできます。

注: CA OPS/MVS の初期化後に INITLXC の値を変更する際に、z/OS コマンド「MODIFY OPSx,RESTART(LXC)」を発行して、新しい値を有効にします。OPSx は CA OPS/MVS のサブシステム名です。

INITLXC、LXCRULES およびその他の LXC パラメータの詳細については、「CA OPS/MVS Parameter Reference Guide」で「Linux Connector Interface Related Parameters」を参照してください。

ジェネリック データ セットの直接出力

AOF コンポーネントで処理するために、ログファイルなどのデータセットから CA OPS/MVS へ直接出力することができます。これを行うには、ジェネリック データセット インターフェース (GDI) を使用します。このインターフェースが有効になっていると、CA OPS/MVS は、ジェネリック データセットに書き込まれている各レコードを、メッセージ イベントとして参照します。これにより、AOF メッセージルールが実行されます。

ジェネリック データ セットの定義

CA OPS/MVS とのジェネリック データ セット インターフェースを確立するには、出力のターゲットとして CA OPS/MVS を認識する JCL を指定しますこの JCL は、以下のように指定します。

```
//ddname DD SUBSYS =(ssid,OPSDSN{,color}{,reportid}{,posmsgid})
```

ddname

ddname はファイルと関連付けられています。

ssid

一般インターフェース メッセージ (通常は OPSS) を受信する、4 文字の CA OPS/MVS サブシステム ID です。

color

(オプション) OPSLOG に表示される一般データセットメッセージの色を指定します。

有効値: GREEN、BLUE、RED、WHITE、PINK、YELLOW、または TURQ

reportid

(オプション) メッセージのソースを識別するために AOF ルールが使用できる、一意のレポート ID を指定します。

posmsgid

(オプション) 以下のいずれかが指定されます。

- CA OPS/MVS がメッセージ ID のスキャンを開始する、各レコードのテキスト内の数値の開始点。
- このデータセット内のすべてのレコードのメッセージ ID として使用される文字列。

数値の開始点がファイル内の特定レコードのいずれかより長い場合、そのレコードの最初からメッセージ ID のスキャンが開始されます。

例 1: サブシステム OPSS にメッセージを送信する

- メッセージは OPSLOG 内で青色
- MSG.COLOR は青色
- レポート ID は PERFRPT
- AOF は MSGID のスキャンを各レコードの最初の列から開始

```
//DD1 DD SUBSYS=(OPSS,OPSDSN,BLUE,PERFRPT)
```

例 2: サブシステム OPST にメッセージを送信する

- メッセージは OPSLOG 内でピンク色
- MSG.COLOR はピンク色
- レポート ID は ESPLOG
- このデータセットからのすべてのメッセージは ESPMSG の MSGID を持ちます。

注: このメッセージ ID は、メッセージに挿入されません。

```
//DD2 DD SUBSYS=(OPST,OPSDSN,PINK,ESPLOG,ESPMSG)
```

例 3: サブシステム OPSS にメッセージを送信する

- メッセージは OPSLOG 内で赤色
- MSG.COLOR は赤色
- レポート ID は MYLOG
- AOF は MSGID のスキャンを各レコードの 22 列目から開始

注: この手法は、各レコードの最初で長さまたはタイムスタンプ、あるいはその両方が固定されているか、メッセージ ID の前にあるその他の長さが固定されたプレフィックスを持つログファイルに便利です。

```
//DD3 DD SUBSYS=(OPSS,OPSDSN,RED,MYLOG,22)
```

ジェネリックデータセットインターフェースのガイドライン

ジェネリックデータセットインターフェースを使用する前に、以下のガイドラインを考慮してください。

- CA OPS/MVS セキュリティイベントは、CA OPS/MVS 向けのサブシステムデータセットがオープンするたびに発生します。データセットのオープンを許可または非許可として、セキュリティールールを書くことができます。
- スターティッドタスク、バッチプログラム、または TSO プログラムは、ジェネリックデータセットインターフェースを使用できます。
- *ssid* として指定された CA OPS/MVS サブシステムは、ジョブまたはスターティッドタスクが開始する際にアクティブになっている必要があります。
- データセットに書き込みを行うアプリケーションは、標準 QSAM または BSAM のどちらかを使用する必要があります。

- 各ファイルからメッセージ ID を選択する際、3 つの手法が考えられます。
 - posmsgid パラメータを指定しない場合、アプリケーションはメッセージ ID を各レコードの最初のトークンとして格納する必要があります。このトークンには、1 ～ 10 文字を含めることができます。
 - posmsgid パラメータを指定し、そのパラメータ値が負数でない場合、CA OPS/MVS は各レコード内の該当する位置から、またはその直後から、メッセージ ID のスキャンを開始します。
 - 上記の手法がいずれも実用的ではない場合、posmsgid パラメータ内のファイルのすべてのレコードに 1 ～ 8 文字から成る一意の非数値 MSGID を割り当てることができます。これら 3 つの手法それぞれの例は、前セクションを参照してください。
- 128 文字を超えるメッセージは、一部が表示されません。
- CA OPS/MVS が終了した場合、ジェネリック データ セット インターフェース メッセージの自動化は解除されます。CA OPS/MVS を再起動すると、メッセージは再び AOF に送信されます。CA OPS/MVS の起動時に同じ CA OPS/MVS サブシステム ID を使用する場合は、アプリケーションの停止および再起動を行う必要はありません。

CA MIC とのインターフェースの設定

CA OPS/MVS と CA MIC 間のインターフェースには、以下の機能があります。

- CA OPS/MVS サブシステムは、OPSCMD コマンド プロセッサまたは ADDRESS OPER OPS/REXX ホスト コマンド環境を使用して、MICplex 内の任意のシステムに対して CA MIC サブシステムを通してクロスシステム コマンドを発行できます。非送信要求コマンド応答メッセージが発行側に返され、オプションで OPSLOG に記録できます。
- CA OPS/MVS サブシステムは、MICplex にある任意のシステムから非送信要求メッセージを受け取って、OPSLOG に記録することができます。
- AOF ルールは、CA MIC でインポートした送信要求および非送信要求のメッセージを認識および問い合わせをして、提示されているメッセージ データに基づいてアクションを実行します。

MICplex は、単一のシスプレックス、非シスプレックス システム、複数シスプレックスのシステム、または CA MIC for VM がサービス マシンとして稼動している VM システムにおける、最大 128 個のシステムで構成できます。現在は、最大 128 システムからのメッセージを、CA MIC を介してすべての CA OPS/MVS サブシステムへ転送できます。

すべてのシステムが単一のシスプレックス内にある場合は、シスプレックス サービスを使用してこれらのほとんどの機能を実行することが可能です。ただし、CA MIC メッセージフィルタ条件は、シスプレックスのフィルタ条件よりすぐれています。Multi-System Facility (MSF) のライセンスを取得している場合は、OPSCMD および ADDRESS OPER の SYSTEM キーワードを使用し、AOF ルールを記述してメッセージを別のシステムに転送することによってこれらの機能を実行できます。

インターフェースの設定

以下を行うための CA MIC の設定方法については、「*CA MIC Message Sharing Systems Programmer Guide*」を参照してください。

- LINK コマンドを使用して、システム間コマンド応答機能を有効にする
- COLLECT コマンドを使用して、CA MIC に非送信要求メッセージをローカル CA OPS/MVS サブシステムへインポートさせる

CA MIC システム間コマンド インターフェースのみを使用し、コマンド応答の自動化や OPSLOG への表示はさせたくない場合は、CA OPS/MVS の設定は必要ありません。

CA MIC インポートメッセージを OPSLOG に表示させる場合は、BROWSEMESSAGES パラメータに MMSGLOBAL を設定する必要があります。AOF ルールによって CA MIC インポートメッセージを自動化する場合は、AOFMESSAGES パラメータを MMSGLOBAL に設定する必要があります。

注: このパラメータを変更すると、自動化に重大な影響を与える可能性があります。

両方の製品が稼働しているサイトの多くでは、通常 CA OPS/MVS は CA MIC より先に開始されます。ただし、CA MIC が CA OPS/MVS の前に開始され CA OPS/MVS SSIMSG パラメータ値が YES に設定されている場合、CA MIC 内部で暗号化されたメッセージ(メッセージ ID が GCM/ で始まるものすべて)が OPSLOG に表示されます。CA OPS/MVS は常に CA MIC の前に起動することをお勧めします。ただし、この順番が目的の自動化方式と一致しない場合、すべての GCM メッセージを OPSLOG から除外する方法を解説している (OPS/MVS サンプル ルール ライブラリのメンバ GCM にも含まれる) 以下のサンプル ルールを使用してください。

注: これらの GCM/ メッセージを抑制しないでください。CA MIC の機能に影響を及ぼします。

```
)MSG GCM/* NOOPSLOG
)PROC
return
```

CA MIC からの受信メッセージの識別

AOF ルールを記述する際、CA MIC インポート メッセージには以下の特性があることに注意する必要があります。

- MSG.MIC 環境変数は 1 に設定されています。
- MSG.REISSUE 環境変数は 1 に設定されています。
- MSG.SYNA 環境変数には、メッセージ送信元であるシステム名が含まれます。
- MSG.JOBNM 環境変数には、最初のメッセージ発行元であるタスクのジョブ番号が含まれます。元のタスクが z/OS サブシステムまたは VM アプリケーション(ジョブ番号がない)であった場合、フィールドには NONE の値が含まれます。
- MSG.JOBID 環境変数には、最初のメッセージ発行元であるタスクのジョブ番号が含まれます。元のタスクが z/OS サブシステムまたは VM アプリケーション(ジョブ番号がない)であった場合、フィールドには MVS のサブシステム名が含まれます。
- MSG.JOBNAME 環境変数には、最初のメッセージ発行元であるタスクの名前が含まれます。

システム上でどの CA MIC メッセージ編集パラメータ値が有効になっているかに関係なく、CA MIC は上記の基準を使用してインポートされたメッセージを CA OPS/MVS に渡します。つまり、CA MIC MIMINIT EDITMESSAGE、SYSNAME、SYSTYPE、および JOBID パラメータに基づいて指定されたシステム上で実行された CA MIC メッセージ編集とは関係なく、CA MIC は継続的に元のメッセージデータを CA OPS/MVS に渡します。

インポートされたメッセージをローカル CA MIC サブシステムがローカル CA OPS/MVS サブシステムに送信する際、AOF ルールが MSG.SYNA または MSG.REISSUE 環境変数、あるいはその両方を照会し、メッセージの発信元であるシステムを識別することが重要です。そうでない場合、これらのルールは CA MIC のインポート済みメッセージがローカルシステムからのものであると誤認し、予期できない、または誤ったアクションの原因となります。

以下のサンプル AOF MSG ルールを使用すると、インポートされた CA MIC メッセージを OPSLOG 内で容易に識別できます。USER カラムで MIC の値によりフィルタリングを行うと、表示を CA MIC インポート済みメッセージに限定します。また、COLOR カラムでフィルタリングを行うことにより、特定のシステムからインポートされたメッセージに表示を限定することもできます。

注: このロジックは、システム XE13、XE12、および XE07 からインポートされたすべてのメッセージを色付けします。CA MIC インポート済みメッセージに色付けのみを行いたい場合は、MSG.MIC = 1 を条件とするステートメントを選択する必要があります。このルールを適用する場合、ルールのロジックを既存の MSG * ルールに組み入れることをお勧めします。

```
)MSG *
)PROC
if MSG.MIC = 1 then
  MSG.USER = "MIC"
select
  when MSG.SYNA = "XE13" then
    MSG.COLOR = OPSCOLOR("TURQ")
  when MSG.SYNA = "XE12" then
    MSG.COLOR = OPSCOLOR("YELLOW")
  when MSG.SYNA = "XE07" then
    MSG.COLOR = OPSCOLOR("PINK")
  otherwise
    nop
end
```

CA 7 Browse Log のオプションのメッセージ機能のインストール

オプションで CA 7 Browse Log のメッセージ機能を使用すると、通常は CA 7 のログのみに示される CA 7 のメッセージについて自動化することができます。

CA OPS/MVS OPSLOG では、CA 7 のメッセージは MSG タイプのイベントとして表示され、これにより、MSG ルールを実行することができます。これらの MSG タイプのイベントには、CA 7 の exit タイプ があります。

ENF サービスのインストール方法

CA OPS/MVS は、CA 7 WA のメッセージを監視し、自動化します。これらのメッセージは、CCS for z/OS のイベント通知機能 (ENF) サービス、または CAI ENF の Common Services 部分を通じて、CA 7 Browse Log データセットへ送られます。

この機能をアクティブにするには、ENF サービスをインストールする必要があります。詳細については、*CCS for z/OS* のドキュメントを参照してください。

注: CA 7 Browse Log の実行に必要な CCS for z/OS コンポーネントの詳細については、付録の「[CCS for z/OS コンポーネントの要件 \(P. 241\)](#)」を参照してください。

CAI ENF と併用するパラメータ

CAI ENF 用に以下のパラメータを設定する必要があります。

INITCA7

CA OPS/MVS が CA 7 ブラウズ ENF イベントを検出できるようになります。

このパラメータの詳細については、「*Parameter Reference*」を参照してください。

複数行の CA 7 WA メッセージ

CA 7 WA メッセージには複数行のものもあり、メッセージルール指定処理において問題となる場合があります。CA 7 WA メッセージのプライマリ行のみが有効なメッセージ ID を含む行であるため、CA 7 WA は複数行メッセージのセカンダリ行が常にプライマリ行の後に続くかどうかを確定できません。そのため、CA OPS/MVS はメッセージ ID CA7BRWSE をすべてのセカンダリ行に指定し、メッセージ行が混在している場合にユーザが無効な情報を受信しないようにします。自動化ルールまたはプログラムは、一時的および永続的なグローバル変数を使用してセカンダリ行の判断と検証を行います。

ブラウザ イベント DCM の追加

CA OPS/MVS が CA 7 ブラウズ ログ イベントを使う為に、DCM が CAI ENF に追加される事が必要になります。

CA OPS/MVS でブラウザ イベント DCM を CAI ENF に追加する方法の詳細については、「*CA 7 Workload Automation Interfaces Guide*」を参照してください。

z/OS Automatic Restart Management Facility の設定

z/OS システムには、Automatic Restart Management (ARM) と呼ばれる機能があります。ARM は、システム障害の発生時にジョブおよびスターティッド タスクを同じシステム、または SYSPLEX 内の任意のシステムで自動的に再開します。ARM 機能を使用するには、SYSPLEX 固有の元素名でジョブまたは STC が ARM に登録されている必要があります。また、完全に初期化され、処理を実行できる状態になったときに ARM に通知する必要があります。タスクが登録抹消呼び出しを発行せずに終了した場合、ARM カップル データセットのインストールで定義されたポリシー ガイドラインに従って、ARM によってタスクが再開されます。ポリシーは、その他のタスクに依存するタスクを再起動する順位、頻度、時間、および再開のシステムリソースの制約を指定します。ARM の詳細については、IBM のドキュメントを参照してください。

CA OPS/MVS による ARM の使用は、過剰なメッセージレートなどのサーバエラー状態によって予期せず製品が終了した場合の、同システムにおいての製品の再起動に限られます。STOP コマンドにより、通常のシャットダウンの一部として CA OPS/MVS が ARM から登録抹消されます。CA OPS/MVS がキャンセルまたはシステムから強制終了された場合、z/OS CANCEL や FORCE コマンドで ARMRESTART オペランドが指定されていない限り、再起動はされません。

AOF の ARM ルールを利用して、その他のジョブやスターティッド タスクの再開を制御できます。z/OS の動的 exit 機能を利用して、CA OPS/MVS は IXC_ELEM_RESTART exit ポイントにおいて ARM 再開イベント exit をインストールします。この exit (IBM マクロ IXCYERE) に渡されたパラメータリストからのデータを使って、ARM イベントが作成され AOF に渡されます。AOF ARM ルールを施行するには、INITARM パラメータおよび ARMRULES パラメータが YES に設定されている必要があります。

AOF ARM ルールの調整

AOF ARM ルールを調整することによって、エラー発生後に ARM が CA OPS/MVS を再起動させるよう設定できます。

AOF ARM ルールを調整する方法

1. サイトのシステム プログラミング グループに連絡し、ARM がどのように利用されているか調査します。デフォルトのポリシーを持つ ARM 用カップル データセットが存在し、ARM が利用されるすべてのシスプレックスシステムにアクセスできることが最低条件です。ARM を起動する以下のコマンドをシステム初期化中に発行する必要があります。

```
SETXCF START,POLICY,TYPE=ARM
```

ARM のステータスを表示するには、以下のコマンドを使用します。

```
D XCF,ARMSTATUS,DETAIL
```

エラー発生後に CA OPS/MVS を ARM に再起動させる場合、シスプレックス固有のエレメント名と、オプションでエレメントの種類を決定します。ユーザが希望する再起動条件に基づいて ARM ポリシーを調整します。

CA OPS/MVS は稼動システム上でのみ再起動します。これはこの製品のほかのコピーがその他のシスプレックスシステム上ではすでにアクティブになっているからです。

2. 必須の ARMELEMNAME パラメータおよびオプションの ARMELEMTYPE パラメータと ARMELEMASSOC パラメータを、OPSSPA00 REXX プログラム内で目的の値に設定します。これらのパラメータを設定できるのは、この時のみです。

例

```
var = OPSPRM('SET','ARMELEMNAME','OPSMVSSYSA')
```

3. INITARM パラメータおよび ARMRULES パラメータを OPSSPA00 REXX プログラム内で設定します。

例:

```
var = OPSPRM('SET','INITARM','YES')
```

```
var = OPSPRM('SET','ARMRULES','YES')
```

注: ARMRULES はいつでも変更できます。

CA OPS/MVS が起動すると、メッセージ OPS0311I/OPS0312E が発行され、製品の各 ARM 呼び出しのステータスが表示されます。リターンコードとエラー コンディションの説明については、IBM のドキュメントを参照してください。

4. AOF ARM ルールの INITARM パラメータが YES に設定された場合、IXC_ELEM_RESTART MVS exit ポイントにおける OPMVAREX 動的 exit モジュールの導入のために、メッセージ OPS0310I が表示されます。製品が終了した後でも、この exit はアクティブなままとなり、製品が再起動されたときにこれをロードした元の製品サブシステムによって再使用されます。exit モジュールのステータスを表示するには、以下の z/OS コマンドを発行します。

```
D PROG,EXIT,EXITNAME=IXC_ELEM_RESTART,DIAG
```

また、この z/OS コマンドを使えば、exit を手動で操作することもできます。

```
SETPROG EXI,ADD/MODIFY/DELETE,EXITNAME=IXC_ELEM_RESTART,MODNAME=OPMVAREX,...
```

OPMVAREX exit モジュールが正しくインストールされていない場合、AOF ARM ルール イベントは発生しません。exit モジュールがメンテナンスのために変更された場合、新しいコピーを再ロードする必要があります。以下の CA OPS/MVS コマンドが、exit モジュールを無効にし、モジュールの新しいバージョンを再ロードし、exit を再度アクティブにします。

```
F OPSS,RELOAD(OPMVAREX)
```

exit がインストールに失敗した場合、OPSSPA00 REXX プログラム内で DEBUGDYN パラメータを YES に設定し、OPSLOG のメッセージを調査して失敗の原因とリターンコードを判断します。これらのコードの説明は、IBM 発行の「*Authorized Assembler Services Reference ALE-DYN*」の CSVDYNEX マクロに関するセクションにあります。

付録 A: システム準備チェックリスト

このセクションには、以下のトピックが含まれています。

[タスクの記録](#) (P. 238)

タスクの記録

このチェックリストは、CA OPS/MVS のインストール前に行ったタスクを簡単に記録しチェックを外す方法を提供します。

- 有効な CA LMP キー証明書
はい _____ いいえ _____
- TSO/E の IBM サポート対象のリリース
はい _____ いいえ _____
- IMS 8.1、9.1、または 10.1 (インストールされ、IOF オプションコンポーネントのライセンス取得済みの場合)
はい _____ いいえ _____
- CICS/TS バージョン 2.3、3.1、または 3.2 (インストールされ、COF オプションコンポーネントのライセンス取得済みの場合)
はい _____ いいえ _____
- CA ACF2 または CA Top Secret (インストールされている場合) の CA サポート対象リリース
はい _____ いいえ _____
- z/OS サブシステムコンソール生成済み

- 十分な ECSA が利用可能であるか (500 KB)
はい _____ いいえ _____
- プログラムライブラリ用 DASD スペース (270 シリンダ)
Volser (ボリューム シリアル番号): _____
- OPSLOG Browse データ (435*BROWSEMAX)
注: CA OPS/MVS のインストール後にこの数値を計算してください。
BROWSEMAX パラメータの詳細については、「*Administration Guide*」および「*Parameter Reference*」を参照してください。
Volser (ボリューム シリアル番号): _____

- グローバル変数チェックポイント(10 シリンダ)
高レベル修飾子: _____
- データセット命名基準
高レベル修飾子: _____
- ルール データセットプレフィックス
高レベル修飾子: _____
- プログラム アクセス
STEPLIB/リンクリスト: _____
- APF 権限
はい _____ いいえ _____
- TSO コマンド権限
はい _____ いいえ _____
- スターテッド タスクのセキュリティ ID

- TSO OPER 権限
はい _____ いいえ _____

付録 B: CCS for z/OS コンポーネントの要件

このセクションでは、CA OPS/MVS がさまざまな機能を実行するために必要な CA Common Services for z/OS コンポーネントおよび対応する FMID について説明します。詳細および最新情報については、「*CCS for z/OS Getting Started Guide*」の「System Requirements」の章にある「Installation Dependencies」を参照してください。

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 LMP \(ライセンス管理プログラム\) \(P. 242\)](#)

[IBM Health Checker へのインターフェース \(P. 242\)](#)

[ADDRESS CA7 \(P. 242\)](#)

[ADDRESS CASCHD \(P. 243\)](#)

[プログラムライブラリの DASD 要件 \(P. 243\)](#)

[ADDRESS JOBTRAC \(P. 243\)](#)

[Automation Measurement Environment \(P. 243\)](#)

[CA Automation Point とのインターフェース \(P. 244\)](#)

[CA 7 Browse Log インターフェース \(P. 244\)](#)

[CA Service Desk インターフェース \(P. 245\)](#)

[CA Network および Systems Management System Status Manager CA-OPS/MVS オプションとのインターフェース \(P. 245\)](#)

[CAICCI を使用する CA OPS/MVS Multi-System Facility の設定 \(P. 246\)](#)

[OPSCAWTO OPS/REXX 関数 \(P. 246\)](#)

[CA Event Manager コンポーネントとのインターフェース \(P. 247\)](#)

[Switch Operations Facility \(SOF\) \(P. 248\)](#)

CA LMP(ライセンス管理プログラム)

CA OPS/MVS のベース製品ライセンスを検証するには、以下の CCS for z/OS コンポーネントが必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI with SSL コンポーネントを指定します。

IBM Health Checker へのインターフェース

IBM Health Checker に対する CA OPS/MVS のインターフェースでは、以下の CCS for z/OS コンポーネントが必要です。

CEF5C00 または CEF5C10 または CEF5E00 または CEF5E10

CA Health Checker Common Service コンポーネントを指定します。

注: 完了しておく必要があるセットアップおよび設定の追加手順の詳細については、CCS for z/OS のドキュメントを参照してください。

ADDRESS CA7

ADDRESS CA7 を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CCS for z/OS r12 をベースとする FMID

CCF3410 または CCF3E00

CA-GREXX コンポーネントを指定します。

CBYS280 または CBYSE00

CA-GSS コンポーネントを指定します。

ADDRESS CASCHD

ADDRESS CASCHD を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CCF3410 または CCF3E00

CA-GREXX コンポーネントを指定します。

CBYS280 または CBYSE00

CA-GSS コンポーネントを指定します。

プログラム ライブラリの DASD 要件

CA OPS/MVS では、ユーザ ライブラリまたはプライベート ライブラリとして 60 3390 シリンダが必須です。

ADDRESS JOBTRAC

ADDRESS JOBTRAC を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CCS for z/OS r11 SP8 をベースとする FMID

CCF3410 または CCF3E00

CA-GREXX コンポーネントを指定します。

CBYS280 または CBYSE00

CA-GSS コンポーネントを指定します。

Automation Measurement Environment

AME (Automation Measurement Environment) を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CAF3C00 または CAF3E00

CA-C ランタイム コンポーネントを指定します

CA Automation Point とのインターフェース

CA OPS/MVS と CA Automation Point とのインターフェースでは、以下の CCS for z/OS コンポーネントが必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW5C00 または CAW5E00 または CAW5E10

CAIENF/DB2 コンポーネントを指定します。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI with SSL コンポーネントを指定します。

注: 完了しておく必要があるセットアップおよび設定の追加手順の詳細については、CCS for z/OS のドキュメントを参照してください。

CA 7 Browse Log インターフェース

CA 7 Browse Log インターフェースを CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW5C00 または CAW5E00 または CAW5E10

CAIENF/DB2 コンポーネントを指定します。

CA Service Desk (FMID) へのインターフェース

CA OPS/MVS と CA Service Desk とのインターフェースでは、以下の FMID が必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CDYFC00 または CDYFE00 または CDYFE10

CAISDI/med コンポーネントと CAI/soap コンポーネントを指定します。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI with SSL コンポーネントを指定します。

完了しておかなければならないその他のセットアップおよび設定の手順の詳細については、CCS for z/OS のドキュメントを参照してください。

CA Network および Systems Management System Status Manager CA-OPS/MVS オプションとのインターフェース

CCS for z/OS の CA Network および Systems Management System Status Manager CA OPS/MVS オプションを CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CB6DB30

Agent Technology コンポーネントを指定します。

完了しておかなければならないその他のセットアップおよび設定の手順の詳細については、CCS for z/OS のドキュメントを参照してください。

CAICCI を使用する CA OPS/MVS Multi-System Facility の設定

CAICCI を使用する CA OPS/MVS Multi-System Facility (MSF) を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW5C00 または CAW5E00 または CAW5E10

CAIENF/DB2 コンポーネントを指定します。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI with SSL コンポーネントを指定します。

注: 完了しておく必要があるセットアップおよび設定の追加手順の詳細については、CCS for z/OS のドキュメントを参照してください。

OPSCAWTO OPS/REXX 関数

OPSCAWTO OPS/REXX 関数を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW5C00 または CAW5E00 または CAW5E10

CAIENF/DB2 コンポーネントを指定します。

完了しておく必要があるセットアップおよび設定の追加手順の詳細については、CCS for z/OS のドキュメントを参照してください。

CA Event Manager コンポーネントとのインターフェース

特定の ADDRESS USS コマンドを CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

以下のコマンドは、z/OS Event Console と通信します。

- ADDRESS USS WTO
- ADDRESS USS WTOR
- ADDRESS USS REPLY
- ADDRESS USS DOM
- ADDRESS USS PING
- ADDRESS USS CMD

CD5IB30

Event Management コンポーネントを指定します。

CAS9C00 または CAS9E00 または CAS9E10

CAIRIM コンポーネントを指定します。

CAW1C00 または CAW1E00 または CAW1E10

CAIENF コンポーネントを指定します。

CAW5C00 または CAW5E00 または CAW5E10

CAIENF/DB2 コンポーネントを指定します。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI with SSL コンポーネントを指定します。

CAF3C00 または CAF3E00

CA-C RUNTIME コンポーネントを指定します。

Switch Operations Facility (SOF)

SOF を CA OPS/MVS で実行するには、以下の CCS for z/OS コンポーネントが必要です。

CAW4C00 または CAW4E00 または CAW4E10

CAICCI および CCS for z/OS の SSL コンポーネントを指定します。

注: 完了しておく必要があるセットアップおよび設定の追加手順の詳細については、CCS for z/OS のドキュメントを参照してください。

付録 C: DASD 計算チャート

このセクションには、以下のトピックが含まれています。

[OPSLOG メッセージの DASD 要件 \(P. 249\)](#)

[グローバル変数チェックポイント DIV データセットの DASD 要件 \(P. 250\)](#)

[共有 VSAM データベースの DASD 要件 \(オプション\) \(P. 253\)](#)

[RDF および System State Manager の DASD 要件 \(P. 253\)](#)

[グローバル変数データベースコントロールの提供 \(オプション\) \(P. 254\)](#)

OPSLOG メッセージの DASD 要件

デフォルト: 568 3390 シリンダ

推奨: 1 週間からのメッセージ (コンソールトラフィックによって変わります)

# OPSLOG メッセージ	デバイス タイプ	1 シリンダ当たりのイベント数	必須シリンダ数
400000	3380	1409	284
400000	3390	1690	237
600000	3380	1409	426
600000	3390	1690	356
800000	3380	1409	568
800000	3390	1690	474
1000000	3380	1409	710
1000000	3390	1690	592
1500000	3380	1409	1065
1500000	3390	1690	888
2000000	3380	1409	1420
2000000	3390	1690	1184
3000000	3380	1409	2130
3000000	3390	1690	1776

# OPSLOG メッセージ	デバイス タイプ	1 シリンダあたりのイベント数	必須シリンダ数
4000000	3380	1409	2839
4000000	3390	1690	2367

グローバル変数チェックポイント DIV データ セットの DASD 要件

グローバル変数チェックポイント DIV データ セットの DASD 要件の詳細については、「OPSLOG およびチェックポイント VSAM 線形データ セットの定義」で共有 DASD に対する制限を参照してください。

グローバル変数の数	各グローバル変数の長さ(バイト)	デバイス タイプ	シリンダあたりのブロック数 (256 バイト)	変数あたりのブロック数	算出シリンダ数	必須シリンダ数 (余分な 20% を含む)
5000	44	3380	2400	1	3	4
5000	44	3390	2880	1	2	3
5000	100	3380	2400	2	5	6
5000	100	3390	2880	2	4	5
5000	200	3380	2400	2	5	6
5000	200	3390	2880	2	4	5
5000	500	3380	2400	3	7	9
5000	500	3390	2880	3	6	8
5000	1,000	3380	2400	5	11	14
5000	1,000	3390	2880	5	9	11
5000	2500	3380	2400	11	23	28
5000	2500	3390	2880	11	20	24
10000	44	3380	2400	1	5	6
10000	44	3390	2880	1	4	5
10000	100	3380	2400	2	9	11
10000	100	3390	2880	2	7	9

グローバル変数の数	各グローバル変数の長さ(バイト)	デバイスタイプ	シリンダあたりのブロック数 (256 バイト)	変数あたりのブロック数	算出シリンダ数	必須シリンダ数 (余分な 20% を含む)
10000	200	3380	2400	2	9	11
10000	200	3390	2880	2	7	9
10000	500	3380	2400	3	13	16
10000	500	3390	2880	3	11	14
10000	1,000	3380	2400	5	21	26
10000	1,000	3390	2880	5	18	22
10000	2500	3380	2400	11	46	56
10000	2500	3390	2880	11	39	47
25000	44	3380	2400	1	11	14
25000	44	3390	2880	1	9	11
25000	100	3380	2400	2	21	26
25000	100	3390	2880	2	18	22
25000	200	3380	2400	2	21	26
25000	200	3390	2880	2	18	22
25000	500	3380	2400	3	32	39
25000	500	3390	2880	3	27	33
25000	1,000	3380	2400	5	53	64
25000	1,000	3390	2880	5	44	53
25000	2500	3380	2400	11	115	138
25000	2500	3390	2880	11	96	116
50000	44	3380	2400	1	21	26
50000	44	3390	2880	1	18	22
50000	100	3380	2400	2	42	51
50000	100	3390	2880	2	35	42
50000	200	3380	2400	2	42	51

グローバル変数の数	各グローバル変数の長さ(バイト)	デバイスタイプ	シリンダあたりのブロック数 (256 バイト)	変数あたりのブロック数	算出シリンダ数	必須シリンダ数 (余分な 20% を含む)
50000	200	3390	2880	2	35	42
50000	500	3380	2400	3	63	76
50000	500	3390	2880	3	53	64
50000	1,000	3380	2400	5	105	126
50000	1,000	3390	2880	5	87	105
50000	2500	3380	2400	11	230	276
50000	2500	3390	2880	11	191	230
100000	44	3380	2400	1	42	51
100000	44	3390	2880	1	35	42
100000	100	3380	2400	2	84	101
100000	100	3390	2880	2	70	84
100000	200	3380	2400	2	84	101
100000	200	3390	2880	2	70	84
100000	500	3380	2400	3	125	150
100000	500	3390	2880	3	105	126
100000	1,000	3380	2400	5	209	251
100000	1,000	3390	2880	5	174	209
100000	2500	3380	2400	11	459	551
100000	2500	3390	2880	11	382	459

共有 VSAM データベースの DASD 要件(オプション)

SYS1.OPS.CCLXCNTL データセット内の OPAMSVDB メンバには、共有 VSAM KSDS を作成および初期化するための IDCAMS DEFINE コマンドおよび JCL が含まれています。この JCL を調整および実行してファイルを作成します。共有 VSAM データベースの DASD 要件を決定するために必要な情報(キー サイズ、ファイルの平均および最小レコード サイズ、1 次および 2 次レコード割り当ての設定など)は、JCL のコメントに含まれています。各レコードはグローバル変数を保持することに注意してください。ボリューム パラメータを設定する必要があります。

RDF および System State Manager の DASD 要件

RDF および System State Manager の DASD 要件を決定するために、存在するテーブルの数およびサイズに基づいて必要な DASD スペースを計算します。

グローバル変数データベースコントロールの提供(オプション)

グローバル変数データベースを緊密に監視できるように、CA OPS/MVS はデータベースがいっぱいになると警告メッセージを発行します。CA OPS/MVS には、これらのデータベースインジケータを細かく制御および監視するためのパラメータが用意されています。これらは、CA OPS/MVS をインストールするときに設定する必要があります。

以下の CA OPS/MVS パラメータは、警告メッセージのレベルおよび頻度を制御します。

GLOBALWARNTHRESH

警告メッセージの発行が開始されるグローバル変数のしきい値パーセンテージです。

デフォルト: 80

GLOBALWARNINTVAL

グローバル変数に関する警告メッセージの発行頻度を分単位で指定します。このパラメータは、メッセージが再発行される頻度が高くなりすぎるのを防ぎます。

デフォルト: 5

GLOBALTEMPWARNTH

警告メッセージの発行が開始される一時 (CA OPS/MVS の寿命中の) グローバル変数のしきい値パーセンテージです。

デフォルト: 80

GLOBALTEMPWARNIV

一時 (CA OPS/MVS の寿命中の) グローバル変数に関する警告メッセージの発行頻度を分単位で指定します。このパラメータは、メッセージが再発行される頻度が高くなりすぎるのを防ぎます。

デフォルト: 5

使用状況警告メッセージ

また、CA OPS/MVS は、GLOBALWARNINTVAL の間隔中であっても、データベースの使用率がしきい値より 5 パーセント増加するたびに (容量の 85 パーセント、90 パーセント、および 95 パーセントなど) 警告メッセージを発行します。これらの警告メッセージをトリガする使用レベルは、GLOBALWARNTHRESH パラメータを別の値に変更しない限り、CA OPS/MVS ライフサイクル中にリセットされません。変更した場合、高使用レベルはしきい値にリセットされます。

警告メッセージ OPS42900 (永続グローバル変数データベースまたは一時グローバル変数データベースのいずれかに適用可能) には、以下の情報が含まれます。

- 警告の対象が一時グローバル変数データベースか永続グローバル変数データベースか。
- フル状態のデータベースの現在のパーセンテージ。
- 使用中のブロック数。
- データベース内のブロックの総数 (GLOBALMAX または GLOBALTEMPMAX パラメータの値によって決定されます)。
- しきい値に到達したか、しきい値を超えたときに実行されたプログラムまたはルールの名前。このプログラムまたはルールがデータベースがフル状態になった原因である場合もありますが、そうではない場合もあります。

注: CA OPS/MVS は、新しいグローバル変数が割り当てられるか、既存のグローバル変数が拡張されたときにのみ、しきい値の超過をチェックします。そのため、メッセージの間隔は定義された間隔より長い場合があります。

グローバル変数の DASD 割り当て要件については、「*Getting Started*」の「*Preparing Your System*」を参照してください。

永続または一時グローバル変数データベースのいずれかが完全にフル状態になった場合、CA OPS/MVS は OPS1093I メッセージを発行します。これが発行された場合、自動操作が正常に機能しなくなる可能性があります。そのため、障害の発生前にこのような状況の発生を警告する CA OPS/MVS しきい値警告メッセージを活用する必要があります。

付録 D: CA MSM によって作成されるデータセット

ポスト SMP/E、展開、および設定データセット

SMP/E、展開、および設定の各インストール手順を完了すると、CA MSM によってデータセットが正常に作成されます。

インストールの各手順で、以下のデータセットが作成されます。

- SMP/E では、以下のテーブルの POST SIS 列でデータセットを参照します。これらのデータセットをまとめて、CA OPS/MVS SMP/E 環境と呼びます。
- 展開では、以下のテーブルの POST SDS 列でデータセットを参照します。これらのデータセットをまとめて、CA OPS/MVS SMP/E 展開と呼びます。
- 設定では、以下のテーブルの POST SCS 列を参照します。これらのデータセットをまとめて、CA OPS/MVS ランタイム環境データセットと呼びます。

POST SIS	POST SDS	POST SCS
SMPEHLQ.ACLXASM		
SMPEHLQ.ACLXCLS0		
SMPEHLQ.ACLXCNTL		
SMPEHLQ.ACLXEXEC		
SMPEHLQ.ACLXHENU		
SMPEHLQ.ACLXHFS		
SMPEHLQ.ACLXMENU		
SMPEHLQ.ACLXMIB		
SMPEHLQ.ACLXMOD0		
SMPEHLQ.ACLXOPEX		

POST SIS	POST SDS	POST SCS
SMPEHLQ.ACLXPENU		
SMPEHLQ.ACLXRULE		
SMPEHLQ.ACLXSAMP		
SMPEHLQ.ACLXSENU		
SMPEHLQ.ACLXSHSC		
SMPEHLQ.ACLXSIDE		
SMPEHLQ.ACLXTENU		
SMPEHLQ.ACLXXML		
SMPEHLQ.CCLXASM	SDSHLQ.CCLXASM	OPSPFX.CCLXASM
SMPEHLQ.CCLXCLS0	SDSHLQ.CCLXCLS0	OPSPFX.CCLXCLS0
SMPEHLQ.CCLXCNTL	SDSHLQ.CCLXCNTL	OPSPFX.CCLXCNTL
SMPEHLQ.CCLXEXEC	SDSHLQ.CCLXEXEC	OPSPFX.CCLXEXEC
SMPEHLQ.CCLXHENU	SDSHLQ.CCLXHENU	OPSPFX.CCLXHENU
SMPEHLQ.CCLXHFS.ZFS	SDSHLQ.CCLXHFS.ZFS	OPSPFX.CCLXHFS.ZFS
SMPEHLQ.CCLXHFS.DATA	SDSHLQ.CCLXHFS.DATA	OPSPFX.CCLXHFS.DATA
SMPEHLQ.CCLXLOAD	SDSHLQ.CCLXLOAD	OPSPFX.CCLXLOAD
SMPEHLQ.CCLXMENU	SDSHLQ.CCLXMENU	OPSPFX.CCLXMENU
SMPEHLQ.CCLXMIB	SDSHLQ.CCLXMIB	OPSPFX.CCLXMIB
SMPEHLQ.CCLXOPEX	SDSHLQ.CCLXOPEX	OPSPFX.CCLXOPEX
SMPEHLQ.CCLXPENU	SDSHLQ.CCLXPENU	OPSPFX.CCLXPENU
SMPEHLQ.CCLXPLD	SDSHLQ.CCLXPLD	OPSPFX.CCLXPLD
SMPEHLQ.CCLXRULB	SDSHLQ.CCLXRULB	OPSPFX.CCLXRULB
SMPEHLQ.CCLXRULM	SDSHLQ.CCLXRULM	OPSPFX.CCLXRULM
SMPEHLQ.CCLXRULS	SDSHLQ.CCLXRULS	OPSPFX.CCLXRULS
SMPEHLQ.CCLXSAMP	SDSHLQ.CCLXSAMP	OPSPFX.CCLXSAMP
SMPEHLQ.CCLXSENU	SDSHLQ.CCLXSENU	OPSPFX.CCLXSENU
SMPEHLQ.CCLXSIDE	SDSHLQ.CCLXSIDE	OPSPFX.CCLXSIDE
SMPEHLQ.CCLXTENU	SDSHLQ.CCLXTENU	OPSPFX.CCLXTENU

POST SIS	POST SDS	POST SCS
SMPEHLQ.CCLXXML	SDSHLQ.CCLXXML	OPSPFX.CCLXXML
SMPEHLQ.CSI		
SMPEHLQ.CSI.DATA		
SMPEHLQ.CSI.INDEX		
SMPEHLQ.SMPHOLD		
SMPEHLQ.SMPLOG		
SMPEHLQ.SMPLOGA		
SMPEHLQ.SMPLTS		
SMPEHLQ.SMPMTS		
SMPEHLQ.SMPPTS		
SMPEHLQ.SMPSCDS		
		RULEPREFIX.BASE.RULESUFFIX
		RULEPREFIX.SAMPLE.RULESUFFIX
		RULEPREFIX.STATEMAN.RULESUFFIX
		OPSPFX.USER.REXX
		OPSPFX.SMFID.SYSCHK1
		OPSPFX.SMFID.SYSCHK1.DATA
		OPSPFX.SMFID.OPSLOG
		OPSPFX.SMFID.OPSLOG.DATA
		OPSPFX.SMFID.OPSLOG2
		OPSPFX.SMFID.OPSLOG2.DATA

索引

A

ADDRESS CA7、CCS 要件 - 242
ADDRESS CASCHD CCS 要件 - 243
ADDRESS JOBTRAC、CCS 要件 - 243
ADDRESS OPSCTL COF コマンド - 166
AOF
 CICS メッセージの処理 - 166
 説明 - 14
APPC セッション プロトコル - 153
APPL ステートメント - 151
ASVT エントリ、置換 - 118
Automation Measurement Environment、CCS
 要件 - 243

B

BMP、コマンドの発行とレスポンスの取得 - 162
BROWSEOMG - 217

C

CA 7 - 233
CA 7 ブラウズ ログ インターフェース、CCS 要件 -
 244
CA ACF2
 CA Top Secret。ログイン ID の作成 - 125
 コマンド制限リストの提供 - 127
CA ACF2 のコマンド制限リスト - 127
CA Automation Point - 18
CA Common Services (CCS) - 171
CA MIC インターフェース - 229
CA OPS/MVS
 OMEGAMON 製品との相互運用の有効化 -
 214
 インストール時のパラメータのリセット - 100
 起動プロシージャのカスタマイズ - 100
 制御の目的での OPSVIEW の使用 - 15
 セキュリティ製品ログイン ID の作成 - 125
CA Top Secret。ログイン ID の作成 - 125
CAI.SAMPJCL

サンプル ジョブ - 74
ライブラリ - 74

CAIXNYI@ モジュール - 133
CA イベント管理インターフェース、CCS 要件 -
 247
CCS (CA Common Services) - 171
CICS
 サブシステムの制御 - 17
CICS グローバル exit (XTDOUT) - 166
 CICS/TS インターフェースのインストール -
 166
 キュー名リスト - 166
COF のキュー名リスト - 166
Critical Path Monitoring (CPM)、説明 - 17

D

DEFDIV メンバのカスタマイズ - 106
DISPLAY ACTIVE - 143
DIV データ セット
 システム間のロックアウトの回避 - 108
 割り当て - 106
DSIEX11 - 208

E

ECF アドレス空間 - 98
ECSA
 要件の削減 - 133
ENF - 233
Enhanced Console Facility (ECF) - 14
EPI
 説明 - 15
ESD (電子ソフトウェア配布) - 20
EXIT
 IATUX18 - 199
 XTDOUT - 166
Expert Systems Interface (ESI) - 18
EXTENDEDCONSOLES - 117

G

GIMUNZIP ユーティリティ - 58

H

HFS ディレクトリ - 136

HOLDDATA - 67

I

IATUX18 - 199

ICSF (Integrated Cryptographic Services Facility) - 58

IEBCOPY - 74

IEFSSNxx、サブシステムの定義に使用 - 132

IKJTSO00 - 133

IKJTSOxx - 133

IMS - 18

 BMP - 162

 IMS Operations Facility のインストール - 157

 IMS/DB のみのショップ - 161

 WTOR - 162

 コマンドの発行 - 133

IMS Operations Facility (IOF) - 18

IMS1DUPLICATE - 161

IMS1ID - 161

INITCCI - 149

INITMSF - 149

IOF

 BMP の使用 - 162

 インストールに関する考慮事項 - 157

ISPEXEC - 121

ISPF、モジュールへのアクセスを提供 - 121

ISPLINK - 121

ISPTCM - 119, 120

J

Java バージョン サポート - 58

JES

 JES2 環境の関数のインストール - 197

 JES3 に対する IATUX18 exit のインストール - 199

 コマンドの発行 - 133

 サブシステム インターフェース - 199

JES2OFFSETSUFFIX - 198

L

Linux Connector インターフェース(LXC)の設定 - 224

LNKLST - 134

LPA

 利点 - 120

LPALIB - 133, 134

LPALST 連結 - 121

LU 6.2

 セッション パラメータ - 153

 セッション プロトコル - 150

LX (リンケージ インデックス) - 118

LXC パラメータ - 225

M

MCS マスタ コンソール、NetView の接続 - 208

MSFLOGMODE - 149

MSFRESTARTREXX - 149

MSFSYSWAIT - 149

Multi-system Facility (MSF) - 18

MVS/QuickRef - 220

N

Netview、インターフェースのインストール - 208

NOF、インストール - 211

O

O332TBLD - 128

OCCONSOLENAME - 100

OMEGAMON、CA-OPS/MVS をインタラクティブにする - 214

OP310000 - 128

OPA2CMLS - 128

OPAAMAIN - 128

OPADDRUL - 128

OPAME010 モジュール - 133

OPARSX35 モジュール - 133

OPBIND - 128

OPBOCMDS コマンド テーブル - 221

OPDELRUL - 128

Operator Server Facility (OSF)、説明 - 15

OPGETSCR - 128

OPJ2CB - 197

OPJS18PR - 200

OPNVEX11 - 208

OPPARSE - 128

OPRXCMAP - 128

OPS/REXX 言語、説明 - 15

OPSAOF コマンド - 145

OPSAOF メンバ - 145

OPSBRW - 128

OPSCAWTO 関数、CCS 要件 - 246

OPSCMD - 128, 133

OPSELV - 128

OPSDOM - 128, 133

OPSECF - 98, 125

OPSESS - 128

OPSEEXEC - 128

OPSGETV - 128

OPSGETVL - 128

OPSHFI - 128

OPSIMEX - 128

OPSINFO/OPSJES2 の関数 - 197

OPSLOG WebView

インストールと設定 - 176

サーバおよび Web アプリケーションのインストール - 189

サーバコマンド - 195

サーバ設定オプション - 179

セキュリティ - 182

リソース チェックリスト - 177

OPSMMAIN

JCL のカスタマイズ - 98

マスタ サブシステムでの起動 - 98

ユーザ ID の定義 - 125

OPSMODE - 128

OPSOSF - 98, 100, 125, 143

OPSPARM - 128

OPSPRM 関数 - 100

OPSQL - 128

OPSQW コマンド - 221

OPSREPLY - 128, 133

OPSREQ - 128

OPSRMT - 128

OPSSETV - 128

OPSSMTBL - 128

OPSSPA00 CLIST - 100

OPSSPA00 REXX プログラム - 100

OPSTART2 REXX プログラム - 100

OPSUSS - 98

OPSVIEW - 127, 128, 141

OPSWAIT - 128

OPSWTO - 128, 133

OPUNBIND - 128

OSF、CA-OPS/MVS インストール後のテスト - 143

OSFCHAR - 100

OxREPORT DD - 215

P

pax ESD プロシージャ

USS ディレクトリの設定 - 48

製品ディレクトリの作成 - 57

製品ファイルのコピー - 51

ファイルのダウンロード - 45

pax ファイル

USS ディレクトリへのファイルのコピー - 51, 52, 55

Q

QUICKREFDBASE - 220

R

read me - 43, 58

RULEPREFIX - 122

RULESUFFIX - 122

S

SMP/E

GIMUNZIP ユーティリティ - 58

SMP/E でインストールされたターゲット データセット - 89

SMU - 162

SNMP トラップ - 171

SQL ステートメントの使用 - 16

SSCT - 132

SSICMD - 100
SSIMSG - 100
SSL 通信 - 180
SSM ディレクトリおよびリソース テーブル - 167
STATEMAN - 100
Switch Operations Facility (SOF) - 18
SYS1.OPS - 121
SYS1.OPS.FBCLIST - 126
SYS1.OPS.HELP - 126
SYS1.OPS.LOAD - 126
SYS1.OPS.OPSEXEC - 126
SYS1.OPS.OPSLOG - 126
SYS1.OPS.OPSLIB - 126
SYS1.OPS.OPSPLIB - 126
SYS1.OPS.OPSSLIB - 126
SYS1.OPS.OPSTLIB - 126
SYS1.OPS.REXX - 126
SYS1.OPS.SAMPLE.RULES - 145
SYS1.OPS.xxx.RULES - 126
SYS1.PARMLIB - 126
SYS1.PROCLIB - 98
SYSID - 149

T

TNGELIGIBLE 列 - 167
TNGNOTIFY 列 - 167
TSO
 ESI を使用した TSO コマンドの実行 - 18
 コマンド プロセッサ - 133
 サーバを実行するための CLIST およびコマンドのスケジュール - 15
 シミュレートされたセッション - 14
TSO アドレス空間 - 98

U

UNZIPJCL - 58
USS
 インストールに関する一般的な問題 - 126
 サーバ環境変数 - 204
 パラメータ - 203
USS (UNIX System Services)
 アクセス要件 - 43, 48
 ディレクトリ構造 - 48

USS ディレクトリへのファイルのコピー - 51, 52, 55

V

VM
 ゲスト サポート - 16
 コマンドの発行 - 133
VTAM - 150
 EPI コンポーネント用の端末の作成 - 207
 モード テーブル エントリの定義 - 153

W

WTO、発行 - 133
WTOR メッセージへの応答 - 133
WTO および WTOR メッセージの発行 - 133

X

XTDOUT - 166

Z

z/OS
 コマンドの発行 - 133
 コンソール、定義 - 117
z/OS、JES、VM、および IMS コマンドの発行 - 133
zFS - 136

あ

空きスペース - 48
アクセス
 ログイン - 41
イベント通知機能 - 233
インストール
 LPA ノート - 167
 NOF - 211
 Pax-Enhanced ESD から - 43
 SSM ディレクトリおよびリソース テーブル - 167
TNGELIGIBLE 列 - 167
TNGNOTIFY 列 - 167
USS - 203

テープから - 73
最も一般的な問題 - 126
インストール時の問題 - 126

か

外部 HOLDDATA - 67
外部製品のインターフェース、「EPI」参照 - 15
外部ライブラリ名、カスタマイズ - 32
カスタマイズ インストール - 31
カスタマ サポート、問い合わせ - 3
仮想端末、VTAM への定義 - 207
環境変数、USS サーバ - 204
起動プロシージャ、カスタマイズ - 100
空間スイッチ エントリ テーブル - 118
グローバル変数、ESI を使用したアクセスおよび
更新 - 18
高レベル修飾子 - 58
コマンド
 DISPLAY ACTIVE - 143
 NetView AUTOTASK - 208
 z/OS、JES、VM、および IMS コマンドの発行 -
 133

さ

サーバ環境変数 - 204
サポート、問い合わせ - 3
サンプル
 APPL 定義 - 151
 コマンド ルール - 145
 モード テーブル エントリ - 153
サンプル JCL - 74
サンプル ジョブ - 52, 57
 CAtoMainframe.txt - 52
 Unpackage.txt - 57
ジェネリック データ セット インターフェース
(GDI) - 226
システム関数テーブル - 118
システム準備タスク - 137
システムリソース、保守 - 16
システムリンケージ インデックス - 118
処理の概要 - 43
スターティッド タスク プロシージャ ライブラリ - 98

製品
 取得 - 20
製品ダウンロード ウィンドウ - 45
製品の取得 - 20
製品レベル ディレクトリ - 57
セキュリティ
 TSO OPER 権限 - 28
 コマンド制限リスト - 128
 製品ログイン ID - 125
 要件 - 26
セッション プロトコル
 APPC - 153
 CAICCI による提供 - 150
説明 - 16
ソフトウェア
 配布 - 20

た

ダウンロード
 ESD を使用したファイル - 45
 PC 経由でメインフレームへ - 55
 オプション - 51
 概要 - 43
 バッチ JCL の使用 - 52
通信、SSL - 180
データセット、命名基準 - 121
テープ、インストールに使用 - 73
テキスト エディタ、OPSLOG WebView で使用 -
 192
テクニカル サポート、問い合わせ - 3
テクニカル サポートへの問い合わせ - 3
トラップ、SNMP - 171
トラブルシューティング - 205

な

内部 HOLDDATA - 67

は

配布
 テープ - 20
配布、製品の取得 - 20

ハッシュ設定 - 58
パラメータ値のリセット - 100
標準、ルールセットおよびデータセット名 - 121

ま

マスタサブシステム
 OPSMAIN の起動 - 98
 データセットのマスタカタログへの定義 -
 106
メイン CA-OPS/MVS のアドレス空間 - 98, 100
メッセージ、WTO および WTOR の発行 - 133

や

要求ルール、ISPF の使用 - 121
要件 - 23

ら

リソースの状態の保守 - 16
リンクバックエリア、「LPA」参照 - 120
リンケージインデックス(LX) - 118
ルール、要求 - 121
例外の分析 - 215

わ

割り当ておよびマウント - 49