CA Common Services for z/OS

インストール ガイド

リリース 14.1.00

CA Technologies 製品リファレンス

このマニュアルでは、以下の CA 製品の一部を参照しています。

- CA 1® Tape Management
- CA 7® Workload Automation
- CA 11™ Workload Automation Restart and Tracking
- CA ACF2™
- CA Allocate™ DASD Space and Placement
- CA Audit
- CA Automation Point
- CA Balancing
- CA Bundl®
- CA Database Analyzer™ for DB2 for z/OS
- CA Datacom®/AD
- CA Data Compressor™ for DB2 for z/OS
- CA DB2
- CA Deliver™
- CA Disk™ Backup and Restore
- CA Dispatch™
- CA Earl™
- CA Endevor® Software Change Manager
- CA Fast Check® for DB2 for z/OS
- CA Fast Index® for DB2 for z/OS
- CA Fast Load for DB2 for z/OS
- CA Fast Recover® for DB2 for z/OS
- CA Fast Unload® for DB2 for z/OS
- CA IDMS™
- CA IDMB™/DB
- CA Insight™ Database Performance Monitor for DB2 for z/OS
- CA Index Expert™ for DB2 for z/OS

- CA JARS®
- CA JARS® Resource Accounting
- CA Jobtrac™ Job Management
- CA Log Analyzer™ for DB2 for z/OS
- CA Mainframe Software Manager™（CA MSM）
- CA Merge/Modify™ for DB2 for z/OS
- CA MIA Tape Sharing
- CA MIC Message Sharing
- CA MICS® Resource Management
- CA MII Data Sharing
- CA MIM™ Resource Sharing
- CA NetMaster® File Transfer Management
- CA NetMaster® Network Automation
- CA NetMaster® Network Management for SNA
- CA NetMaster® Network Management for TCP/IP
- CA NetMaster® Network Operations for TCP/IP
- CA NetSpy™ Network Performance
- CA Network and Systems Management
- CA NSM System Status Manager
- CA OPS/MVS® Event Management and Automation
- CA Partition Expert™ for DB2 for z/OS
- CA Plan Analyzer® for DB2 for z/OS
- CA Quick Copy for DB2 for z/OS
- CA Rapid Reorg® for DB2 for z/OS
- CA RC/Extract™ for DB2 for z/OS
- CA RC/Migrator™ for DB2 for z/OS
- CA RC/Query® for DB2 for z/OS
- CA RC/Secure™ for DB2 for z/OS
- CA RC/Update™ for DB2 for z/OS
- CA Recovery Analyzer™ for DB2 for z/OS
- CA Roscoe®

- CA Scheduler® Job Management
- CA SYSVIEW® Performance Management
- CA Service Desk（Service Desk）
- CA Spool™ Enterprise Print Management
- CA SQL Ease® for DB2 for z/OS
- CA SYSVIEW® Performance Management
- CA TCPAccess™ Communications Server for z/OS
- CA TLMS Tape Management
- CA Top Secret®
- CA TPX™ Session Management for z/OS
- CA Value Pack for DB2
- CA Vantage™ Storage Resource Manager
- CA View®
- CA XCOM™
- CA Workload Control Center

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。

目次

第 1 章: はじめに

このガイドでは、CA Common Services for z/OS のインストール方法および実行方法について説明します。

CA Common Services は、z/OS をはじめとする多くのオペレーティング システムで使用できる、オープンかつクロス プラットフォームのエンタープライズ マネジメント インフラストラクチャです。CA Common Services は、CA の IT 管理ソリューション向けの共通サービスおよびイネーブリング テクノロジを提供します。

このセクションには、以下のトピックが含まれています。

対象読者

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
- z/OS UNIX System Services
- 自社の IT 環境、エンタープライズ構造、領域構造

必要に応じて以下にご相談ください。

- システム プログラマ (z/OS および VTAM 定義に関して)
- ストレージ管理者 (DASD 割り当てに関して)

CA Common Services for z/OS

CA Common Services for z/OS には、z/OS に固有の CA の実装およびソリューションに共通する分散サービスが含まれています。CA Common Services for z/OS は、複数の統一されたリソース ビューを作成するための共通の GUI およびイベント サービスを提供します。

z/OS をホストとするこのエンタープライズ マネジメント アーキテクチャは、CA Common Services の Windows および UNIX プラットフォーム上での動作方法と同様に、何をどこで管理するかについての選択肢を広げます。また、Common Services for z/OS には、z/OS の統合管理を実現する基本コンポーネントおよび機能も用意されています。

CA Common Services for z/OS は、z/OS UNIX System Services ベースのアプリケーションに対応しています。また、CA Common Services for z/OS には、z/OS エージェントを実行するための Agent Technology インフラストラクチャも組み込まれています。

CA Common Services for z/OS では以下の操作を実行できます。

- メインフレームを他の分散プラットフォームと統合できます。
- Web サーバ、Java アプリケーション、UNIX アプリケーションなど、新たな z/OS ワークロードを管理できます。
- 既存の CA z/OS 管理ソリューションを使用してイベントを作成し、そのイベントを使って必要な結果が得られるエンタープライズ プラットフォームにイベントを送信することができます。
- 先進的なマネージャ/Agent Technology と CA 製品を併用して使用することにより、エンタープライズ全体にわたってクリティカル リソースの高度なモニタおよび管理を行います。

エンドツーエンド管理

CA Common Services for z/OS により、z/OS のソリューションと他のプラットフォーム上の管理ソリューションを統合して、リモートの場所や単一のコンソールから、エンタープライズ全体の「エンドツーエンド管理」を実現することができます。

CA Common Services for z/OS のソフトウェア テクノロジにより、さまざまなビジネス ニーズに合わせて適切なハードウェア プラットフォームとソフトウェア アプリケーションを実行し、多くのマシン上に展開できると同時に、それらを統合的に管理することができます。

ビジネス プロセス ビュー

ビジネス プロセス ビューとは、以下を表す管理対象オブジェクトのユーザ定義グループです。

- 特定のビジネス プロセス
- リソース機能
- 地域
- 組織構造
- アプリケーション

CA ネットワークおよびシステム マネジメントのアーキテクチャを利用して、会計プロセスや給与に関連するオブジェクトのみを表示するビジネス プロセス ビューを作成することができます。製造部門では、さまざまな工場、倉庫内のサーバ、ネットワーキング デバイス、およびセグメントを示すビューを作成することができます。表示オプションは数多くあります。CA Common Services for z/OS では、z/OS エージェントをインストールすることにより、CA ネットワークおよびシステム マネジメント ビジネス プロセス ビューに z/OS システムを含めることができます。

包括的な CA NSM 管理

CA Common Services for z/OS を使用して、他のプラットフォームにインストールした CA NSM コンポーネントがメインフレーム上のイベントに応答するように設定したり、逆にメインフレームが他のプラットフォーム上のコンポーネントに応答するように設定したりできます。

Event Management を利用して、以下の操作を実行できます。

- SNMP トラップ、アプリケーション イベント、システム イベントなど、各種の非同期イベントをモニタし、管理します。
- 他の CA NSM プラットフォームから z/OS Event Management コンソールを参照します。
- 他のプラットフォームの CA NSM Event Management コンソールを z/OS イベント管理 Java GUI から参照します。

多階層アーキテクチャ

CA Common Services for z/OS は、ソフトウェア サービス層と管理サービス層とで構成されます。ソフトウェア サービス層には、ソフトウェア アプリケーションを一元管理するための業界標準の統合および分散処理サービス スイートが含まれます。管理サービス層には、Web ベースのリアル ワールド グラフィカル インターフェースと、アプリケーション イベントおよびシステム イベントのモニタ機能が備えられています。

サービス コンポーネントはそれぞれ以下のいずれかのパッケージ バンドルに割り当てられています。

- Base
- Optional
- Legacy
- MFNSM（Mainframe CA NSM）

Base Common Services バンドル内にあるコンポーネントはすべてインストールする必要があります。他の 3 つのバンドル内にあるコンポーネントは、ユーザのサイトのニーズに応じて必要な場合があるので、CA Common Services のインストールでは任意であるとみなされます。

パッケージング バンドルの各々のコンポーネントを以下に示します。

Base Common Services（r14.1 で新規レベル）

CAECIS

CAICCI

CAIENF

CAIRIM

CA Health Checker

CA Master

CA MSM

Optional Common Services（r14.1 で新規レベル）

- CA-GSS
- CA-GREXX
- CA-XPS
- CAIENF/CICS
- CAIENF/CICS Spawn
- CAIENF/DB2
- CAIENF/USS
- CAISDI
- Apache Tomcat

Legacy Common Services（v14.0 から変更なし）

- CA-C Runtime
- CA-L-Serv
- CA Earl
- SRAM Service
- Viewpoint

Mainframe CA NSM Common Services（MFNSM）（v14.0 から変更なし）

- Agent Technology
- Event Management
- Event Management Utilities

ソフトウェア サービス

CA Common Services for z/OS のソフトウェア サービスは、各種機能を実行する多数のコンポーネントで構成されています。

Base Common Services

このセクションでは、Base Common Services パッケージング バンドルに含まれたコンポーネントを説明します。このバンドルにあるコンポーネントがすべてインストールされる必要があります。

CAIRIM

CAIRIM は、すべての CA アプリケーションに対するオペレーティング システム環境を作成し、それらのアプリケーションを開始するソフトウェア コンポーネントです。CAIRIM は、一連の動的初期化ルーチン用の共通ドライバです。ユーザ SVC、SMF EXIT、サブシステムなど、システム アプリケーションのインストール時に要求される一般的なインストール要件を不要にします。

CAIRIM の 4 つの構成要素は CAISSF、CA LMP、サービス性および zIIP Enablement Services です。

CAISSF

すべてのシステム リソース プロセスとアプリケーション リソース プロセスへの制御と監視アクセスのための外部セキュリティ機構が実現されます。CAISSF は多くの CA エンタープライズ アプリケーションに統合されており、他の CA Common Services for z/OS サービスでも使用されます。ユーザ サインイン、リソース アクセス制御、プロセス使用制御、違反行為の記録およびモニタのためのセキュリティ サービスを提供します。

CA LMP

CA LMP は、ライセンス ソフトウェアを監視する標準化された自動化アプローチを提供します。

サービス性

CA 製品によって利用できる以下の機能を含んでいます。

- エラーまたは障害に関連付けられたメッセージにより、問題の特定に役立つ情報を提供することを確認する。
- 必要なドキュメントをキャプチャする（DUMPS、SYSLOG、LOGREC、TRACE DATA）。
- リソースの所有権を識別する（アイキャッチャ）。
- 予防および修正メンテナンスの識別を簡素化する。

zIIP Enablement Services

zIIP Enablement Services は、CA 製品によっては、ある状況下で、zIIP プロセッサで CA 製品のコードのいくつかを実行するのに適格にするために利用される場合があります。

CAIENF（Base）

CAIENF（Base）はソフトウェア コンポーネントで、製品ライン全体を対象とし、テクノロジを利用して、CA のあらゆる z/OS アプリケーションに包括的なオペレーティング システム インターフェース サービスを提供します。オペレーティング システムおよび CA ソフトウェアが生成したイベント情報が標準インターフェースでドライブされることを可能にすることにより統合の水準は向上し、複数の製品間インターフェースや、さもなければ必要となるであろう関連するメンテナンスを単純化します。

CAICCI

CAICCI は、一般的な通信ソフトウェア層を、CA エンタープライズ アプリケーションに提供するソフトウェア コンポーネントです。このソフトウェア層によって、プロトコルの指定、エラー リカバリ、およびシステム接続の確立がアプリケーションで行われないようにします。

CAECIS

CA Examine Common Inventory Service（CAECIS）はサポート サービス コンポーネントで、特定の顧客サイトでインストールされた CA 製品のインスタンスを収集してレポートする CA サポート用のツールを提供しています。このサービスは、問題が発生した場合のトラブルシューティングに役立ちます。

CA Health Checker Common Service

CA Health Checker Common Service は、CA 製品でヘルス チェックを作成し、IBM Health Checker for z/OS で実行するための簡単で一貫した方法を提供します。IBM Health Checker for z/OS を使用すれば、システム パラメータや製品パラメータ、およびシステム ステータスを推奨設定と照合してチェックし、z/OS 環境内の潜在的な問題を識別できます。CA z/OS 製品のヘルス チェックは、以下のコンポーネントがインストールおよび構成されているシステムで製品が起動したときに、ターゲット システム上で自動的にアクティブ化されます。

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

CA Master

CAMASTER アドレス空間は初期の IPL で、機能制限がある、常駐システム アドレス空間で、任意の CA 製品によって利用される一連のシステム レベルのサービスを提供します。CAMASTER は、以下に対して権限のある CA コンポーネント用の機能を提供します。

1. SVC ルーチンの代わりに使用される可能性のある非スペース スイッチ PC 機能ルーチンを登録するか、ハードウェア支援プログラム コール メカニズムを使用してコンポーネント固有の機能ルーチンへの永続的なアクセスを提供します。
2. ESQA または ECSA など z/OS の共通のストレージ リソースを使用する必要をなくすために CAMASTER アドレス空間（CAMASTER によるスペース スイッチ PC ストレージ管理サービス、または AR ASC モードの CAMASTER ALET を使用した明示的な STORAGE OBTAIN による）によって提供される永続的なプライベート ストレージを使用します。
3. パブリック アクセス データ スペースなど CA 製品のオブジェクトを固定する CA 所有の常駐システム アドレス空間などを供給します。

要するに、CAMASTER により、CA 製品での ECSA 使用が減少し、ユーザ SVC の使用を避け、CA 製品が IBM *MASTER* アドレス空間を使用するのを避ける役に立ちます。

CA MSM Common Services

CA MSM Common Services は CA Mainframe 2.0 の CA Mainframe Software Manager（CA MSM）コンポーネントに用意されている一連のサービスで、これを使用してインストールされているソフトウェアを社内に展開できます。

Optional Common Services

このセクションでは、Optional Common Services パッケージング バンドルに含まれたコンポーネントを説明します。

CAIENF/CICS

CAIENF/CICS は、CICS をイベント モニタリングに組み込むことができるサポート サービス コンポーネントです。

CAIENF/CICS SPAWN

CAIENF/CICS SPAWN は、通信機能を提供するサポート サービス コンポーネントです。CA のアプリケーションで、CICS 領域外から CICS の作業単位を開始することができます。この機能により、CICS のリリースを問わず、アプリケーション ソフトウェアの実行を実現する層が提供されます。

CAIENF/DB2

CAIENF/DB2 は、DB2 システムをイベント モニタリングに組み込むことができるソフトウェア コンポーネントです。

CAIENF/USS

CAIENF/USS は、管理アプリケーションで、z/OS UNIX System Services サブシステムで発生するシステム イベントを処理することができるサポート サービス コンポーネントです。z/OS UNIX System Service の管理（CAIENF/USS）では、z/OS 上の UNIX Systems Services アプリケーションの管理をカプセル化および統合する、CA Common Services for z/OS の拡張機能を提供します。

CAISDI

CAISDI は、z/OS 環境からの CA Service Desk 要求を開くサービスのセットを提供するサポート サービス コンポーネントです。この要求は、CA 製品によって直接オープンすることも、インターフェースを使用している特定の製品の要求に応じてオープンすることもできます。

CA-GREXX

CA-GREXX は、REXX プログラミング言語を実行できるサポート サービス コンポーネントです。

CA-GSS

CA-GSS は、各種ソースの情報へのクイック アクセスを提供することで、さまざまな CA Technologies 製品が簡単に、シームレスに、そして確実に情報をやり取りできるようにする単純化された通信インターフェースを提供するサポート サービス コンポーネントです。CA-GSS は、単一のプログラムとして編集、コンパイル、実行される 1 つ以上の REXX サブルーチンを使用して接続を提供します。

CA-XPS

CA-XPS は、CA 7、CA Scheduler、CA Jobtrac Job Management を含む CA Technologies 製品のクロスプラットフォーム スケジューリングを実現するサポート サービス コンポーネントです。

Tomcat

Tomcat は、Apache プロジェクトで開発されている有名なオープン ソース Web アプリケーション管理ソフトウェアです。ソフトウェアをインストールする際の便宜上、CA Common Services と共に配布されます。これにより、ユーザが Apache Web サイトからダウンロードする必要性をなくし、インストールされたソフトウェアを CA 製品間で共有できるようにします。また、CA Common Services のインストールを通じて SMP/E 管理下に配置されます。関連付けられたオープン ソースのライセンス契約については、付録を参照してください。

Legacy Common Services

このセクションでは、Legacy Common Services パッケージング バンドルに含まれているコンポーネントを説明します。Legacy Common Services パッケージング バンドル（pax ファイル）は、CA Common Services for z/OS r14.1 に対しては変更ありません。Legacy Common Services バンドルの一部であるすべてのサービスに対して、CA Common Services for z/OS r14.0 SMP 環境を継続して使用できます。同じ SMP 環境を継続して使用することによって、すでに適用した Legacy Common Service PTF を適用する必要はなくなります。

CA-C Runtime

CA-C Runtime は、システムおよびリリースを問わず、プログラムの実行を可能にする C のランタイム機能を提供するサポート サービス コンポーネントです。

CA-L-Serv

CA-L-Serv は、CA Endevor Software Change Manager、CA Bundl、CA Balancing、CA-TPX、CA MIC Message Sharing などの CA Technologies 製品が使用する CA-L-Serv サービスを提供するサポート サービス コンポーネントです。これらのサービスには、一元化されたロギングとメッセージング機能、VSAM ファイルの管理、システム-間通信、および SQL テーブルの管理が含まれます。

Earl Service

Earl Service は、包括的なプログラミング システムの能力を備えた、ユーザ フレンドリなレポート定義機能を提供するサポート サービス コンポーネントです。Earl Service では、英語と類似したステートメントを使用して、定義済みの CA アプリケーション レポートのコンテンツおよびレイアウトを変更および出力できます。

SRAM Service

SRAM Service は、同時に複数のソートを起動させることで、データとロジックの流れを簡易化できるサポート サービス コンポーネントです。ソート処理に対する入力データは、ユーザ プログラムから高レベル言語を使って自由に操作できます。特殊な EXIT ルーチンは不要です。

Viewpoint

Viewpoint は、PC ベースのワークステーション製品の SQL エンジンを提供するサポート サービス コンポーネントです。ワークステーション製品は、ViewPoint を使用して z/OS 製品データベースへの照会を実行できます。基になるデータベース構造の知識は必要ありません。

Mainframe CA NSM Common Services

Mainframe CA NSM（MFNSM）Common Services パッケージング バンドルに含まれている管理サービス コンポーネントによって、社内のすべての IT リソースの統合管理が可能になります。これらのリソースには、ネットワーク デバイス、データベース、デスクトップ システムおよびメインフレーム用ビジネス アプリケーションなどがあります。これらの管理サービスは、Agent Technology および Event Management コンポーネントで構成されています。Mainframe CA NSM Common Services パッケージング バンドル（pax ファイル）は、CA Common Services r14.1 に対しては変更ありません。Agent Technology および Event Management サービスに関して、CA Common Services r14.0 SMP 環境を継続して使用できます。同じ SMP 環境を継続して使用することによって、すでに適用した Agent Technology または Event Management PTF を適用する必要がなくなります。

Agent Technology

Agent Technology インフラストラクチャは、z/OS 環境でエージェントの使用を可能にします。エージェントはエージェント マネージャに報告し、エージェント マネージャはリソースおよびアプリケーションの状況をモニタしてレポートを作成します。z/OS システム エージェント、CA IDMS、DB2 エージェント、CICS エージェントのほか、CA Common Services の仕様に合わせて作成されたその他のエージェントなど、既存の組み込み済みの z/OS エージェントをサポートしています。

Agent Technology は、幅広いプラットフォームをサポートしており、従来のクライアント/サーバ環境、インターネット環境、イントラネット環境に展開可能です。この汎用性により、z/OS のエレメントをエンタープライズ全体でモニタおよび管理することができ、z/OS 環境の機能をさらに拡張して真の異機種混合ネットワークに組み込むことができます。

Event Management

Event Management は単一の使いやすいグラフィカル ユーザ インターフェース（GUI）を備えた管理コンポーネントの集合体で、SNMP トラップ、アプリケーション イベント、システム イベントなどのさまざまな非同期イベントをモニタし、管理します。Event Management を使用すると、必要に応じて、関連するメッセージをネットワーク全体で収集して 1 箇所に表示したり、それらのメッセージを複数の場所に送信したりする操作を簡単に実行できます。z/OS の Event Management の GUI から、Event Management コンソール、メッセージ アクション レコードの管理、カレンダの管理にアクセスできます。

注: メッセージ アクションおよびカレンダは、CA Datacom/AD のインストールが必要な Event Management のオプションです。

CA Common Services for z/OS の Event Management は、幅広い範囲の分散イベントへの組み込みアクセスを用意し、CA Common Services が利用できるプラットフォーム上でトリガーされるアクションを許可することにより、CA OPS/MVS Event Management and Automation などの z/OS の自動化ソリューションを拡張できます。CA Common Services for z/OS はイベントの相関とイベント処理を行い、他のプラットフォーム上の CA Common Services Event Management 機能と完全に統合されています。また、CA Common Services for z/OS には、コマンド ラインやバッチ インターフェースなど、いくつかの SDK 機能もあります。

特定の Event Management ポリシーを定義することで、以下の処理を実行できます。

- メッセージへの応答
- メッセージの非表示
- CA Common Services for z/OS コマンドの発行
- その他のプログラムやスクリプトの起動
- CA OPS/MVS Event Management and Automation などのネットワークの管理アプリケーションや自動化アプリケーションへの情報の送信
- 他の管理対象プラットフォームへのメッセージの転送
- 他のプラットフォームで実行するコマンドの発行
- 追加アクションを確実に実行できるかどうかを決定するためのアクション結果の解釈

Event Management は、個々のサーバでメッセージを処理して、それを中央サーバや他のサーバに転送するように構成できます。Event Management を使用すると、必要に応じて、関連するメッセージをネットワーク全体で収集して 1 箇所に表示したり、複数の場所に送信したりする操作を簡単に実行できます。

イベント コンソール ログでは、ネットワーク上で発生しているシステム イベントおよびプロセスをモニタできます。実行中のプログラムおよびユーザ プロセスはすべて、照会メッセージおよび情報メッセージをこのログに送信することができます。

カレンダ

カレンダは、イベントがいつ発生したかに基づいて、アクションの流れを決定できる Event Management オプションです。イベントが、一般基準およびカレンダ プロファイルを用いて設定された日付、曜日、および時間の基準を満たすとアクションがトリガされます。カレンダの基本機能は、命名体系で識別できます。CA Common Services for z/OS には、ニーズに応じて必要な数のカレンダを定義し、格納する機能があります。

インストール処理の実行

重要: インストールを開始する前に、「*CA Common Services for z/OS リリース ノート*」を参照することを強くお勧めします。CA Common Services for z/OS リリースのいずれかをスキップしていて、次のリリースをインストールする場合は、必ずスキップしたリリースの「リリース ノート」を参照してください。

インストール プロセス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、サイトで必要な CA Common Services が含まれる pax ファイルを取得します。

   注: CA Common Services for z/OS は、4 つの別々の pax ファイル、Base、Optional、Legacy、MFNSM にバンドルされています。各 pax ファイルの内容については、「概要」の章を参照してください。Base CA Common Service バンドルに含まれている CA Common Services コンポーネントをすべてインストールする必要があります。

   - 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。

   - Electronic Software Delivery (ESD) で配布される Pax ファイル

     CA Mainframe Software Manager 製品ページにある CA Mainframe Software Manager ドキュメント マニュアル選択メニューのインストール手順に従います。

     CA Support Online Web サイトのダウンロード センターから CA Common Services の pax ファイルをダウンロードできます。

   - DVD で配布される Pax ファイル

3. 製品をインストールします。インストールについては CA MSM と pax 拡張 SAMPJCL の 2 つの方法がサポートされています。

   必要なデータ セットを割り当て、SMP/E CSI をセットアップし、SMP/E プロセッシングを実行し、CA Common Services 製品を適用して許可するという点では、どちらのインストール方法も同じ手順を踏みます。

   2 つの方法の違いは、CA MSM がほとんどの作業をユーザに代わって実行するのに対し、SAMPJCL を使用したインストール方法では、ユーザが SAMPJCL データ セット中で発見されたさまざまなメンバを編集してサブミットする必要があるという点です。

4. 該当する場合、メンテナンスを APPLY します。

5. 展開します。

   注: Event Management および Agent Technology を展開する前に考慮すべき特殊事項があります。

6. 設定パラメータがある各 CA Common Service の最小の設定を構成します。

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。

コンポーネント FMID

Common Services コンポーネント FMID (機能上の SYSMODS) は、インストールする他のコンポーネントに必要です。どの Common Services コンポーネントが必要かついては、個々の製品のドキュメントを参照してください。

Common Services のコンポーネントは、BASE、OPTIONAL、LEGACY および MFNSM として知られる 4 つのバンドル (pax ファイル) で提供されます。BASE pax ファイル内のコンポーネントはすべてインストールする必要があります。

各 Common Services コンポーネントに関連付けられている FMID を以下の表に示します。

コンポーネント	FMID	必要なその他の FMID
CA-C Runtime - CA C 言語ランタイム機能 LEGACY pax ファイル	CAF3E00	なし
CAIRIM - CA リソース初期化マネージャ BASE pax ファイル	CAS9E10	CEI0E10
SRAM Service - CA リエントラント-ソート ツール LEGACY pax ファイル	CASR710	なし

コンポーネント	FMID	必要なその他の FMID
CAIENF - CA イベント通知機能 BASE pax ファイル	CAW1E10	CAS9E10 CA Datacom/AD - CAF3E00、および CAW4E10
CAIENF/CICS - CA CAIENF CICS インターフェース OPTIONAL pax ファイル	CAW3E10	CAS9E10 と CAW1E10
CAIENF/CICS SPAWN - CA CAIENF CICS-SPAWN インターフェース OPTIONAL pax ファイル	CAW3E11	CAS9E10、CAW1E10、CAW3E10 および CAW4E10
CAICCI - CA Common Communications インターフェース(Secure Sockets Layer をサポート) BASE pax ファイル	CAW4E10	CAS9E10、CAW1E10、および CEI0E10
CAIENF/DB2 - CA DB2 インターフェース OPTIONAL pax ファイル	CAW5E10	CAS9E10 と CAW1E10
Agent Technology - メインフレーム エージェント サポート機能 MFNSM pax ファイル	CB6DB30	なし
CA-L-Serv - システム間メッセージングおよびファイル サービス LEGACY pax ファイル	CBUJE00	CAS9E10
CA-GSS - 通信インターフェース OPTIONAL pax ファイル	CBYSE00	CCF3E00
CA-GREXX - REXX EXEC 環境 OPTIONAL pax ファイル	CCF3E00	なし
CA-XPS - クロスプラットフォーム スケジューリング共通コンポーネント OPTIONAL pax ファイル	CCF9E00	CAS9E10、CAW1E10、および CAW4E10
CAIENF/USS - CA CAIENF UNIX System Services インターフェース OPTIONAL pax ファイル	CCQ9E10	CAS9E10、CAW1E10、および CEI0E10

コンポーネント	FMID	必要なその他の FMID
CAECIS – CA-Examine 共通インベントリ サービス* BASE pax ファイル	CD0E350	なし
Event Management - イベント管理機能 MFNSM pax ファイル	CD5IB30	CAS9E10、CAW1E10、および CAW4E10 CA Datacom/AD の場合 - CAF3E00
Event Management ユーティリティ - イベント管理ユーティリティ MFNSM pax ファイル	CD5IB31	CD5IB30
Viewpoint - CA システム ソリューションのユーザ インターフェース LEGACY pax ファイル	CDU4E00	CAS9E10 および CAF3E00
CAISDI - CA Service Desk Simple Object Access Protocol OPTIONAL pax ファイル	CDYFE10	CAS9E10、CAW1E10、および CAW4E10
CA Health Checker Common Service - CA システム ヘルス チェック サービス BASE pax ファイル	CEF5E10	CEI0E10
CA Master BASE pax ファイル	CEI0E10	なし
CA MSM Common Services BASE pax ファイル	CETN500	CAW4E10
EARL Service - CA Easy Access Report Language レポート サービス LEGACY pax ファイル	CXE6100	なし
Apache Tomcat OPTIONAL pax ファイル	CEG1E00	なし

* CA Datacom/AD が必要かどうかに決定するために、「*Best Practices Guide*」の「CA CAIENF」または「Event Management」の章を参照してください。

ソフトウェア要件

CA Common Services for z/OS 用に以下のソフトウェアが必要です。

- IBM がサポートする z/OS のバージョン。
- セキュリティ サブシステム（CA Top Secret、CA ACF2 または IBM RACF のいずれか）のうちの 1 つのサポートされたリリース。

セキュリティ要件

セキュリティ要件は CA Common Services ごとに異なり、特定の CA Common Service について説明するこのガイドのセクション内で扱われています。

ストレージ要件

次のストレージ要件が満たされていることを確認してください。

ターゲット ライブラリ

CA Common Services for z/OS の SMP/E プロセスの一部として、以下のターゲット ライブラリが製品固有のルーチンにより更新されます。各ターゲット ライブラリのスペースの割り当てについては、インストールする各サービスのシステム要件を参照してください。

ターゲット データ セットは 3 セットあります。BASE と OPTIONAL のコンポーネント用に 1 セット、LEGACY コンポーネント用に 1 セット、そして MFNSM コンポーネント用に 1 セットです。

CA Common Services を使用する CA 製品の過去のリリースでは、依然として CAILIB または CAILOAD および CAIPDSE の低レベル修飾子を備えた CA Common Services ロード ライブラリを参照する場合があります。企業での CA 製品ライブラリを標準化するために、CAILIB/CAILOAD および CAIPDSE は CAW0LOAD と CAW0PLD に置換されています。

注: CA Common Services for z/OS r14.1 には BASE および OPTIONAL コンポーネントのみが含まれます。LEGACY および MFNSM コンポーネントは CCS v14.0 レベルのままになります。データ セットの観点から、この構成は、CCS v14.0 を使用している場合は、継続して CCS v14.0 の低レベル修飾子 CCCS* および CNSM* データ セットを使用することを意味します。実行中の低レベル修飾子 CAW0* データ セットのみを CCS r14.1 レベルの CAW0* データ セットに置換します。

BASE および OPTIONAL のターゲット ライブラリ

注: これらの説明では、CA ライブラリのデフォルト高レベル修飾子が使用されます。

CAI.CAW0CLS0

Common Service CLIST ライブラリです。

CAI.CAW0DCM

CAIENF 許可 DCM ロード ライブラリです。

CAI.CAW0EXP

Common Service Export Datacom Plan ライブラリです。

CAI.CAW0JCL

Common Service JCL ライブラリです。

CAI.CAW0LINK

この CA 製品に認可されたロード ライブラリには、システムのリンクリスト内にある必要がある BASE Common Services 用のサービス関連の実行可能モジュールが含まれます。

CAI.CAW0LOAD

この CA 製品に認可されたロード ライブラリには、BASE および OPTIONAL Common Services 用のサービス関連の実行可能モジュールが含まれます。このライブラリの展開されたバージョンは、オプションでシステム リンクリスト内にある場合があります。

CAI.CAW0LPA

CA リンク パック領域ライブラリには、システム LPA リストに載っている必要があるサービス関連の実行可能モジュールが含まれます。

CAI.CAW0MAC

CA Macro ライブラリには、サービス関連のプログラムをコンパイルする場合に使用するマクロが含まれています。

CAI.CAW0MSG0

Common Service メッセージ ライブラリです。

CAI.CAW0OPTN

CA 製品オプション ライブラリには、CA Common Services for z/OS のサンプルのパラメータ メンバが含まれています。

CAI.CAW0OPTV

Common Services の可変長オプション ライブラリです。

CAI.CAW0PLD

CA 製品に許可された PDSE ロード ライブラリには、プログラム フォーマット 3 で連係編集されたサービス関連の実行可能モジュールが含まれています。このデータ セットはシステム linklist に存在する必要があります。

CAI.CAW0PNL0

Common Service パネル ライブラリです。

CAI.CAW0PROC

CA プロシージャ ライブラリには、CA Common Services for z/OS とその関連ユーティリティの起動に関するサンプル プロシージャが含まれています。

CAI.CAW0SAMP

Common Service サンプル ライブラリです。

CAI.CAW0SCRN

CAIENF ユーティリティのパネル ライブラリです。

CAI.CAW0SCST

CA Common Services MSM SCS Template ライブラリ。

CAI.CAW0SDF

Common Services のサイド デッキです。

CAI.CAW0SMPI

CA-GSS サンプル IMOD ライブラリには、サンプル REXX ソースが含まれています。

CAI.CAW0SYSI

CA-GSS システムの IMOD ライブラリには、CA-GSS が使用する内部 IMOD のソースが含まれています。

CAI.CAW0XML

CA MSM XML ライブラリ。

CAI.CAW0XML0

Remote Deployment 用の XML ライブラリ。

TPV.CEG1ZFS1

バイナリ実行可能ファイルおよびベース設定ファイルを備えた Apache Tomcat USS ディレクトリを保持する Tomcat zFS ファイル システム。

LEGACY ターゲット ライブラリ

注: これらの記述では、CA ライブラリのデフォルト高レベル修飾子が使用されます。

CAI.CCCSCICS

CA CICS ロード ライブラリには、サービス関連の CICS 実行可能モジュールが含まれています。

CAI.CCCSCLS0

Common Service CLIST です。

CAI.CCCSJCL

Common Service JCL ライブラリです。

CAI.CCCSLINK

この CA 製品ロード ライブラリには、システムのリンクリスト内にある必要がある Legacy Common Services 用のサービス関連実行可能モジュールが含まれています。

CAI.CCCSLOAD

この CA 製品に認可されたロード ライブラリには、Legacy Common Services 用のサービス関連の実行可能モジュールが含まれます。このライブラリの展開されたバージョンは、オプションでシステム リンクリスト内にある場合があります。

CAI.CCCSMAC

CA Macro ライブラリには、サービス関連のプログラムをコンパイルする場合に使用するマクロが含まれています。

CAI.CCCSOPTN

CA 製品オプション ライブラリには、CA Common Services for z/OS のサンプルのパラメータ メンバが含まれています。

CAI.CCCSPNL0

Common Service パネル ライブラリです。

CAI.CCCSPROC

CA プロシージャ ライブラリには、CA Common Services for z/OS とその関連ユーティリティの起動に関するサンプル プロシージャが含まれています。

CAI.CCCSSRC

CA ソース ライブラリには、サービス関連のソース コードが含まれています。

CAI.VPOINT.CHOICES

ViewPoint チョイス ライブラリには、サービス関連の ViewPoint リストが含まれています。

CAI.VPOINT.DIALOG

ViewPoint ダイアログ ライブラリには、サービス関連の ViewPoint ダイアログが含まれています。

CAI.VPOINT.HELP

ViewPoint ヘルプ ライブラリには、サービス関連の ViewPoint ヘルプが含まれています。

CAI.VPOINT.MESSAGE

ViewPoint メッセージ ライブラリには、サービス関連の ViewPoint メッセージが含まれています。

CAI.VPOINT.PANEL

ViewPoint パネル ライブラリには、サービス関連の ViewPoint パネルが含まれています。

CAI.VPOINT.SQL

ViewPoint SQL ライブラリには、サービス関連の ViewPoint SQL ステートメントが含まれています。

CAI.VPOINT.TEMPLATE

ViewPoint テンプレート ライブラリには、サービス関連の ViewPoint テンプレートが含まれています。

MFNSM ターゲット ライブラリ

注: これらの記述では、CA ライブラリのデフォルト高レベル修飾子が使用されます。

CAI.CNSMJCL

Common Service JCL ライブラリです。

CAI.CNSMLOAD

この CA 製品に認可されたロード ライブラリには、Mainframe NSM Common Services 用のサービス関連の実行可能モジュールが含まれます。このライブラリの展開されたバージョンは、オプションでシステム リンクリスト内にある場合があります。

CAI.CNSMOPTV

Common Services の可変長オプション ライブラリです。

CAI.CNSMPLD

CA 製品に認可された PDSE ロード ライブラリには、プログラム フォーマット 3 で連係編集されたサービス関連の実行可能モジュールが含まれています。

CAI.CNSMPROC

CA プロシージャ ライブラリには、CA Common Services for z/OS とその関連ユーティリティの起動に関するサンプル プロシージャが含まれています。

CAI.CNSMSDF

Common Services のサイド デッキです。

CAI.CNSMSRCV

Common Services の可変長ソース ライブラリです。

CAI.MIBLIB

Agent Technology の MIB ソース ライブラリです。

CAI.RO.CB6DZFS

Agent Technology の読み取り専用 zFS です。

CAI.RW.CB6DZFS

Agent Technology の読み取り専用 zFS です。

CAI.RO.CD5IZFS

Event Management の読み取り専用 zFS です。

CAI. RW.CD5IZFS

Event Management の読み書き用 zFS です。

非 SMP/E 製品固有のデータ セット

以下は SMP/E データ セットではありませんが、特定の製品に固有のものです。

CAI.CAIEVENT

CAISDI イベント ライブラリ。

CAI.CETN500.RW.CAIZFS

CA MSM Common Services で使用される zFS ファイル システム。

CAI.SAMPIMOD

SAMPLE ISET ライブラリ用の CA-GSS VSAM IMOD ファイル。

CAI.SYSIMOD

INTERNAL ISET ライブラリ用の CA-GSS VSAM IMOD ファイル。

CAI.VPOINT.PROFILE

Viewpoint プロファイル ライブラリ。

ストレージ要件の概要

以下は、ターゲット ライブラリ内の各コンポーネントの最小ストレージ要件のリストです。このリストは、必ずしもインストール中に提供される実際のターゲット ライブラリ割り当てを表すものではありません。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は、IBM SMP/E パッケージング標準および CA パッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、システムでこれらのデータ セットに対して最適なブロック サイズを割り当てることができます。

ライブラリ名	ブロック サイズ	コンポーネント	トラック数	ディレクトリ ブロック数
CAI.CAW0CLS0	0	CA-GSS	2	2
		CAECIS	1	1
		CAIENF	1	1
		CAIRIM	1	1
CAI.CAW0DCM	6144	CA-XPS	2	1
		CAICCI	1	1
		CAIENF	2	1
		CAIENF/CICS	2	1
		CAIENF/USS	2	1
CAI.CAW0EXP	0	CAIENF	4	1
		CA MSM Common Services	47	1
CAI.CAW0JCL	0	CA-GSS	1	1
		CA-XPS	1	1
		CAECIS	1	1
		CAICCI	1	1
		CAIENF	6	6
		CAIRIM	2	2
		CAISDI	1	1
		CA MSM Common Services	1	2
CAI.CAW0LINK	6144	CA-HEALTH-CHECKER	11	3
		CA-MASTER	27	21
		CAICCI	1	1
		CAIENF	2	1
		CAIRIM	7	4

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CAW0LOAD	6144	CA-GREXX	6	1
		CA-GSS	108	5
		CA-XPS	6	3
		CAECIS	26	1
		CAICCI	65	5
		CAIENF	31	20
		CAIENF/CICS	11	2
		CAIENF/CICS-SPAWN	6	2
		CAIENF/DB2	5	1
		CAIENF/USS	12	9
		CAIRIM	16	5
		CAISDI	24	6
CAI.CAW0LPA	6144	CAIRIM	2	1
CAI.CAW0MAC	0	CA-GSS	3	1
		CAIRIM	1	1
		CAISDI	1	1
CAI.CAW0MSG0	0	CA-GSS	1	1
		CAECIS	1	1
CAI.CAW0OPTN	0	CA-GSS	4	7
		CA-XPS	1	1
		CAICCI	219	2
		CAIENF	1	1
		CAIRIM	1	3
		CAISDI	2	3
		CA MSM Common Services	1	1
CAI.CAW0OPTV	25600	CAIENF	1	1
		CAISDI	1	1

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CAW0PLD	6144	CA Health Check	3	0
		CAICCI	41	0
		CAIENF	7	0
		CAIRIM	4	0
		CAISDI	19	0
		CA MSM Common Services	173	0
CAI.CAW0PNL0	0	CA-GSS	20	82
		CAECIS	5	2
CAI.CAW0PROC	0	CAI-GSS	1	1
		CA-XPS	1	1
		CAECIS	1	1
		CAICCI	2	2
		CAIENF	1	2
		CAIRIM	1	2
		CAISDI	1	2
		CA MSM Common Services	1	1
CAI.CAW0SAMP	0	CA-GSS	1	1
		CAIENF	1	1
		CAIRIM	7	2
CAI.CAW0SCRN	4104	CAIENF	8	23

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CAW0SCST	0	CA GREXX	1	1
		CA GSS	4	2
		CA Health Check	1	1
		CA Master	1	1
		CA XPS	1	1
		CAECIS	1	1
		CAICCI	2	4
		CAIENF	4	8
		CAIENF/CICS	1	1
		CAIENF/CICS-SPAWN	1	1
		CAIENF/DB2	1	1
		CAIENF/USS	1	1
		CAIRIM	2	6
		CAIDSI	1	3
		MSM CCS	2	1
CAI.CAW0SDF	0	CA Health Check	1	1
		CAICCI	1	1
		CAIRIM	1	1
		CA MSM Common Services	4	1
CAI.CAW0SMPI	3600	CA-GSS	3	6
CAI.CAW0SYSI	3600	CA-GSS	65	57

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CAW0XML	32760	CA GREXX	29	1
		CA GSS	40	1
		CA Health Check	29	1
		CA Master	29	1
		CA XPS	29	1
		CAECIS	29	1
		CAICCI	30	1
		CAIENF	32	1
		CAIENF/CICS	58	1
		CAIENF/DB2	29	1
		CAIENF/USS	29	1
		CAIRIM	59	2
		CAISDI/SOAP	30	1
		MSM-SCS	1	1
CAI.CAW0XML0	27998	CA MSM Common Services	162	4
TPV.CEG1ZFS1	25600	TPV-TOMCAT	50 サイクル	
CAI.CCCSCICS	6144	CA-C Runtime	8	4
		Viewpoint	14	1
CAI.CCCSCLS0	0	Viewpoint	1	1
CAI.CCCSJCL	0	CA-C Runtime	1	1
		CA-L-SERV	1	2
		EARL	1	1
		SRAM-Service	1	1
		Viewpoint	2	1
CAI.CCCSLINK	6144	CA-C Runtime	26	9
		SRAM-Service	2	2
CAI.CCCSLOAD	6144	CA-L-SERV	20	3
		EARL	19	1
		Viewpoint	91	9

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CCCSMAC	0	CA-CRuntime	1	1
		EARL	2	1
		SRAM-Service	1	1
		Viewpoint	5	1
CAI.CCCSOPTN	0	CA-CRuntime	1	1
		CA-L-SERV	4	4
		EARL	1	1
CAI.CCCSPNL0	0	Viewpoint	2	1
CAI.CCCSPROC	0	CA-L-SERV	1	1
CAI.CCCSSRC	0	EARL	1	1
TPV.CEG1ZFS1	-	Tomcat	50 サイクル	-
CAI.CNSMJCL	0	Agent Technology	3	2
		Event Management	6	2
		Event Management/Utilities	1	1
CAI.CNSMLOAD	6144	Agent Technology	103	5
		Event Management	3	1
		Event Management/Utilities	1	1
CAI.CNSMOPTV	25600	Agent Technology	1	1
CAI.CNSMPLD	6144	Event Management/Utilities	11	
CAI.CNSMPROC	0	Agent Technology	1	1
		Event Management	1	1
CAI.CNSMSDF	0	Agent Technology	8	1
		Event Management	1	1
		Event Management/Utilities	1	1
CAI.CNSMSRCV	25600	Agent Technology	2	1
CAI.MIBLIB	25600	Agent Technology	15	1
CAI.RO.CB6DZFS	-	Agent Technology	30 サイクル	-
CAI.RO.CD51ZFS	-	Event Management	700 サイクル	-
CAI.RW.CB6DZFS	-	Agent Technology	30 サイクル	-

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.RW.CD5IZFS	-	Event Management	200 サイクル	-
CAI.VPOINT.CHOICES	4104	ViewPoint	1	1
CAI.VPOINT.DIALOG	8204	ViewPoint	15	5
CAI.VPOINT.HELP	4104	ViewPoint	38	28
CAI.VPOINT.MESSAGE	4104	ViewPoint	6	8
CAI.VPOINT.PANEL	4104	ViewPoint	6	6
CAI.VPOINT.SQL	0	ViewPoint	2	1
CAI.VPOINT.TEMPLATE	0	ViewPoint	1	1

非 SMP/E 製品固有のデータセットを以下に示します。

ライブラリ名	ブロックサイズ	コンポーネント	トラック数	ディレクトリブロック数
CAI.CAIEVENT	8000	CAISDI	68	50
CAI.CAITXLIB	32760	Agent Technology Event Management	10 サイクル 10 サイクル	10 10
CAI.RW.CETNZFS	-	CA MSM Common Services	500 サイクル	
CAI.SAMPIMOD	-	CA-GSS	1 サイクル	-
CAI.SYSIMOD	-	CA-GSS	4 サイクル	-
CAI.VPOINT.PROFILE	0	ViewPoint	5	10

コンポーネントのインストール要件

このセクションでは、各 CA Common Services コンポーネントに必要なインストール要件および配布ライブラリの一覧を示します。

Agent Technology 要件

Agent Technology のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- zFS 物理ファイル システムが実装されているフル機能モードの UNIX System Service（OpenEdition または OMVS とも呼ぶ）。
- TCP/IP のサポート バージョン
- IBM C/C++ for z/OS をサポートするバージョン（サンプル エージェントを使用する場合、または独自のカスタム エージェントを作成する場合）。
- ディスク スペース（RO および RW zFSs）は約 60 シリンダ
- 新規 Agent Technology ユーザの作成を許可するセキュリティ定義。

以下の表に Agent Technology 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。 BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AB6DJCL	0	2	2	JCL ライブラリ
CAI.AB6DMIB	25600	15	1	MIB ライブラリ
CAI.AB6DMOD	6144	160	5	モジュール ライブラリ
CAI.AB6DOPTV	25600	1	1	ソース ライブラリ
CAI.AB6DPROC	0	1	1	プロシージャ ライブラリ
CAI.AB6DSDF	0	8	1	サイド デッキ
CAI.AB6DSRCV	25600	2	1	ソース ライブラリ
CAI.AB6DZFS	32760	144	1	ZFS エレメント ライブラリ

Agent Technology のインストールの準備

Agent Technology をインストールする前に、以下の作業を実行し、システムの準備が整っていることを確認してください。

1. z/OS システム エージェントを管理し、メインフレーム トラップを受信する各リモート システムの IP アドレスを書き留めます。
2. ユーザ サイトの TCP/IP プロシージャを検査します。

   TCP/IP 構成データセットのデータセット プレフィクスが TCPIP（IBM のデフォルト値）ではない場合は、//SYSTCPD DD ステートメントで、代わりのプレフィクスを識別する DATASETPREFIX ステートメントが入っているデータセットが指定されていることを確認します。

   //SYSTCPD DD ステートメントの TCP/IP データセット名を書き留めます。
3. 以下のデータセットが存在し、他の TCP/IP データセットと同様にカタログされていることを確認します。
   - ETC.SERVICES
   - HOSTS.ADDRINFO
   - HOSTS.SITEINFO
4. インストール時に使用するすべての端末で大文字/小文字のサポートを使用可能にします。

CA-C Runtime 要件

CA-C Runtime は、IBM がサポートする z/OS バージョンで動作します。

CA-C Runtime は、以下の製品をサポートしています。

- CA Roscoe Interactive Environment（ETSO）のすべてのリリース
- CICS（z/OS）のすべてのリリース
- TSO のすべてのリリース
- IMS/DC のすべてのリリース
- z/VM のすべてのリリース

以下の表に CA-C Runtime 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および(MSM) XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。 BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAF3CICS	6144	8	4	CICS ロード ライブラリ
CAI.AAF3JCL	0	1	1	JCL ライブラリ
CAI.AAF3MAC	0	1	1	MACRO ライブラリ
CAI.AAF3MOD	6144	35	9	モジュール ライブラリ
CAI.AAF3OPTN	0	1	1	オプション ライブラリ

CA-GREXX 要件

CA-GREXX のインストールには、IBM がサポートしている z/OS バージョンが必要です。

以下の表に CA-GREXX 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ACF3MOD0	6144	5	-	モジュール ライブラリ
CAI.ACF3SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.ACF3XML	32760	29	1	XML ライブラリ

CA-GSS（システム インターフェース）要件

CA-GSS のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- CA-GSS は、APF 許可ライブラリにインストールする必要があります。CA-GSS ルーチンは、STEPLIB 連結または LNKLST 連結から実行できます。
- クロスメモリ通信の要件により、CA-GSS はスワップ不可になります。
- CA-GSS は複数のアプリケーションおよびタスクを提供するため、CA-GSS のディスパッチング優先順位は、CA-GSS サービスを要求するタスクの最も高いディスパッチング優先順位と同じまたはそれ以上である必要があります。

以下の表に CA-GSS 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ABYSCLS0	0	2	2	CLIST ライブラリ
CAI.ABYSJCL	0	1	1	JCL ライブラリ
CAI.ABYSMAC	0	3	1	MACRO ライブラリ
CAI.ABYSMOD0	6144	96	-	モジュール ライブラリ
CAI.ABYSMSG0	0	1	1	メッセージ ライブラリ
CAI.ABYSOPTN	0	4	7	オプション ライブラリ
CAI.ABYSPNL0	0	20	82	パネル ライブラリ
CAI.ABYSPROC	0	1	1	プロシージャ ライブラリ
CAI.ABYSSAMP	0	1	1	サンプル ライブラリ
CAI.ABYSSCST	0	4	2	MSM SCS テンプレート ライブラリ
CAI.ABYSSMPI	3600	3	6	SAMP IMOD ライブラリ

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ABYSSYSI	3600	65	57	システム IMOD ライブラリ
CAI.ABYSXML	32760	40	1	XML ライブラリ
CAI.ACF3MOD0	6144	5	-	

以下の表に、CA-GSS に必要なパーマネント VSAM IMOD ライブラリを示します。

ISET ライブラリ名	シリンダ数	説明
CAI.SAMPIMOD	1	SAMPIMOD ライブラリ
CAI.SYSIMOD	4	SYSIMOD ライブラリ

CA-GSS メモリ要件

CA-GSS メモリは、機能に基づいて分類できます。割り当てられるメモリのタイプは、以下のとおりです。

- システム レベル メモリ - 一度割り当てられると、CPU が IPL が実行されるまで保持されます。
- 1 次 CA-GSS メモリ - 1 次(または唯一の)CA-GSS サブシステムによってのみ割り当てられます。
- ISERVE メモリ - 1 次 CA-GSS サブシステムを含め、システムで実行される各 CA-GSS サブシステムによって割り当てられます。

システム レベル メモリ

CA-GSS には、プログラム コール(PC)ルーチン用のシステム リンケージ インデックス(LX)が 1 つ必要です。これは、初期化時に自動的にシステムから提供されます。CA-GSS を再起動すると、以前に取得した LX が再利用されます。

IPL の実行後、初めて CA-GSS を起動したときに、CSA 領域と ECSA 領域が予約されます。これらの領域が取得されるのは、IPL 時の 1 回のみです(CA-GSS を再起動しない限り、2 つ目の領域セットは取得されません)。これらの領域は、次に IPL を実行するまで保持されます。必要なストレージ量は以下のとおりです。

- CSA: 40 バイト(サブシステム アンカ用)
- ECSA: 23.6 KB(共通ルーチンおよびデータ テーブル用)

これらの領域は、CA-GSS のバックグラウンド タスクで使用され、CA-GSS サービスを使用するすべてのアドレス空間で共有されます。

CA-GSS を再ロード(PGM=GSSLOAD、PARM=RELOAD)すると、新しい ECSA 領域が割り当てられて、古い領域は保持されます。これにより、別のアドレス空間によって使用中の領域が解放されることはなくなります。CA-GSS の 3 度目のロードでは、最初のストレージが解放されて、2 度目のロードが保持されます。保持の対象となるのは、CA-GSS の最新の 2 つのバージョンだけです。

1 次 CA-GSS メモリ

CA-GSS 1 次サブシステムに必要なストレージは以下のとおりです。ストレージの推定量はすべて、基本構成に基づいて算定した値で、ここに含まれるのは、CA-GSS が明示的に使用するストレージのみです。他の CA Technologies 製品、オペレーティング システム、VTAM、およびその他のエンティティが使用するストレージは含まれません。

- 私用ストレージ: 3 MB(最小)。入出力バッファおよび一部の外部ルーチンへのインターフェースを除き、このストレージはすべて 16 MB 境界より上に存在します。
- CSA: 160 バイト(サブシステム アンカおよび関連ストレージ用)。
- ECSA: 120 KB このストレージは、バッファ、通信、および PC ルーチンに使用します。 このストレージは、CA-GSS の終了時または再起動時に解放、回復、または再使用されます。

ISERVE メモリ

ISERVE のコピーを実行する(1 次を含む)たびに、以下のメモリが必要です。

- CSA: 120 バイト
- ECSA: 95.4 KB
- プライベート エリア ストレージ(16 MB 境界より上): 3 MB

CA-GSS プログラムはすべて再入可能で、AMODE 31 および RMODE ANY です。

ISERVE が取得する ECSA は、終了時に保持され、同じサブシステム ID を用いて ISERVE を次に初期化したときに解放されます。これにより、クロスメモリの ISERVE ユーザが影響を受けることがなくなります。

ISERVE の CSA の使用には、サブシステム アンカ ブロックで使用する 40 バイトが含まれます。インストールによる事前定義または動的な取得を問わず、このブロックは次の IPL まで保持され、ISERVE を再起動するたびに再利用されます。

REXX ADDRESS コマンドを使用して ISERVE と一緒に使用される CA Technologies 製品には、それぞれ追加の CSA または ECSA が必要になります。追加ストレージの要件については、インストールされている各製品の適切なマニュアルを参照してください。

ISERVE に必要な専用ストレージの容量は、選択するオプションおよびシステムのトラフィック量に応じて異なります。4 MB から始めることをお勧めします。

リソースの使用

インストール制御のトレース オプションによっては、スプールにかなりの領域が使用される場合があります。スプールされたログ ファイルは、オペレータ コマンドによりいつでもクローズし、スパンすることができます。

動作時に、CA-GSS が実行する入出力は最小限に抑えられます。したがって、データセットの場所は通常は問題になりません。

CPU を著しく使用する状況は避ける必要があります。CA-GSS への不正な要求または不適切な要求により、CPU が過剰に使用される可能性がありますが、内部のリソース制限手法によりこの状況は最小限に抑えられます。

システム セキュリティ

CA-GSS アドレス空間で実行している IMOD は、さまざまなデータセットおよびデータ領域にアクセスし、それらを更新することができます。無許可のアクティビティを防ぐため、CA-GSS は、IBM のシステム許可機能（SAF）と互換性のあるシステム セキュリティ ソフトウェアをサポートしています。

z/OS では、各タスクは、すべてのリソースへのアクセスを制御する、ACEE（Accessor Environment Element）の制御下で動作します。SAF と互換性のあるセキュリティ ソフトウェアは、ユーザ ID に基づいて ACEE を管理し、必要な検査を確実に実行します。

CA-GSS では、実行中の各 IMOD に対し適切な ACEE が確保されると同時に、IMOD のために呼び出されるサービスすべてが、その ACEE の制御下で実行されます。

ユーザ ID

CA-GSS は、適切なセキュリティを確保するために 2 つの有効なユーザ ID を必要とします。

- システムが CA-GSS スターティッド タスクまたはジョブに割り当てる 1 次ユーザ ID。
- 関連するユーザ ID が割り当てられていないか、または CA-GSS が関連するユーザ ID を判別できないサービス要求のデフォルト ID として使用するユーザ ID。

このユーザ ID は、セキュリティ ソフトウェアに対して定義してから、SECURITY 初期化パラメータで CA-GSS に定義する必要があります。これはデフォルトのユーザ ID なので、適用範囲を制限する必要があります。

注: CA-GSS の初期化パラメータについては、「*Reference Guide*」を参照してください。

CAGSS ユーザ ID

通常、インストールによってスターティッド タスクに特定の ID が割り当てられることはあまりありません。少なくとも CA-GSS 用の 1 つのユーザ ID を割り当てる必要があります。

CA-GSS は、初期化時および一部のハウスキーピング機能の実行時に、独自のユーザ ID 下で実行されます。

IMOD は、初期化時とハウスキーピング機能の実行時、および他に有効なユーザ ID が指定されていないときに、CA-GSS のユーザ ID の権限下で実行されます。

IMOD ユーザ ID

IMOD タスクが作成されると、CA-GSS はそのタスクに有効なユーザ ID を割り当てて、それに対応する ACEE を取得します。

一般に、ユーザ ID は、IMOD タスクを起動したタスクから引き継がれます。たとえば、TSO ユーザ（IMOD エディタまたは SRVCALL() 関数）からの要求には、TSO ユーザ ID が割り当てられます。

CA-GSS は、使用するユーザ ID を判別できない場合があります。たとえば、ユーザ ID を持たないスターティッド タスクが WTO を実行し、その WTO が IMOD を起動するようなケースです。このような場合、CA-GSS は IMOD タスクに CA-GSS のデフォルト ユーザ ID を割り当てます。

注: CA-GSS の初期化時にデフォルト ユーザ ID が定義されなかった場合、IMOD タスクは CA-GSS アドレス空間の 1 次ユーザ ID の権限下で実行されます。

CA-GSS における IMOD のユーザ ID の選択方法

以下の表に、CA-GSS で IMOD を実行するユーザ ID を判別する方法に関する追加情報を示します。

IMOD のタイプ	CA-GSS がユーザ ID を判別する方法
オペレータ コマンドをサポートする IMOD	PARMLIB データセットの COMMAND パラメータを介してユーザ ID が定義されている場合は、CA-GSS はそのユーザ ID を使用します。それ以外の場合は、CA-GSS はデフォルト ユーザ ID を使用します。

IMOD のタイプ	CA-GSS がユーザ ID を判別する方法
WTO で起動される IMOD	PARMLIB データセットの WTO パラメータを介してユーザ ID が定義されている場合、CA-GSS はそのユーザ ID を使用します。定義されていない場合、CA-GSS は、WTO を実行したユーザ ID の判別とその使用を試みます。それでも判別できない場合、CA-GSS はデフォルトユーザ ID を使用します。 **注**: 実行中、IMOD タスクは、新しいユーザ ID とそのパスワードを SECURITY() 関数に提供することでユーザ ID を切り替える場合があります。
ASID 値が MONITOR コマンドで指定されている値に一致する、WTO で起動される IMOD	CA-GSS は、WTO を実行したユーザ ID の判別とその使用を試みます。それ以外の場合は、CA-GSS はデフォルト ユーザ ID を使用します。
ログオン機能をサポートしている IMOD	ユーザ ID とパスワードが指定されている場合は、それらを使用します。それ以外の場合は、CA-GSS はデフォルト ユーザ ID を使用します。
サーバ IMOD	CA-GSS は、それらを開始した IMOD のユーザ ID を使用します。
ADDRESS 環境とサブタスク	CA-GSS は、それらを起動した IMOD のユーザ ID を使用します。 **注**: サブタスクが別の IMOD に再割り当てされると、ユーザ ID は変更されます。

CA-L-Serv 要件

CA-L-Serv サービスは、IBM がサポートする z/OS バージョンで正常に動作します。

以下の表に CA-L-Serv 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および (MSM) XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。 BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ABUJJCL	0	1	2	JCL ライブラリ
CAI.ABUJMOD	6144	64	23	モジュール ライブラリ
CAI.ABUJOPTN	0	4	4	オプション ライブラリ
CAI.ABUJPROC	0	1	1	プロシージャ ライブラリ

XCF 通信に関する考慮事項

システム間で XCF 通信を使用する予定がある場合は、CAIRIM（CAS9E10）がインストールされていること、および CALServ-- からロード ライブラリにアクセスできることを確認してください。

CA-L-Serv の実行に、CAS9 プロシージャの実行は必要ありません。

CA-L-Serv には、LMP キーは必要ありません。

z/OS 要件

CA-L-Serv は、許可されたロード ライブラリに常駐している必要があります。

CA-L-Serv が他の Common Services とは異なるロード ライブラリにインストールされているので、以下の事項に注意してください。

- CA-L-Serv と Common Services が実行されているロード ライブラリは両方とも、APF 許可がなければなりません。
- Communications Server の XCF コンポーネントのユーザは、CA-L-Serv が Common Services CAW0LOAD データセットへのアクセス権を持っていることを確認する必要があります。
- Common Services CAW0LOAD データセットには、CA--LServ 起動プロシージャ内の STEPLIB 連結、または LINKLIST からの CA-L-Serv からアクセス可能である必要があります。

仮想ストレージの要件

CA-L-Serv に必要な仮想ストレージの容量は以下のとおりです。

ストレージのタイプ	最小仮想ストレージ容量
CSA	CSA が 3 KB、および拡張 CSA が 2 KB。
ESQA	必要な容量は 4 KB ～ 500 KB 以上で、VSAM バッファ プールのサイズと数によって異なります。

CSA ストレージは、CA-L-Serv がシャットダウンしても解放されず、CA-L-Serv を再起動したときに再使用されます（起動プロシージャで REUSE=YES が指定されている場合）。

ESQA ストレージは VSAM で使用され、ファイル サーバのユーザにのみ必要となります。

CA-L-Serv の SQL ディクショナリ

SQL Server に必要な VSAM データベースは以下のとおりです。

データベース	説明
SQL ディクショナリ	SQL サーバで管理される SQL テーブルの定義が含まれています。

SQL ディクショナリのストレージ要件は、ユーザ サイトの要件によって異なります。

注: このファイルは、SQL サーバのユーザのみ必要となります。

CA-XPS 要件

CA-XPS（Cross-Platform Scheduling Common Component）により、CA-7、CA-Scheduler、および CA Jobtrac Job Management は、他のプラットフォームからスケジューリング要求を受け入れることができるようになります。「CA-XPS」の代わりに「XPS ROUTER」という名称を使っているマニュアルもあります。

CA 7 または CA Scheduler では、CA-XPS コードは CA 7 または CA Scheduler のアドレス空間で実行されます。CA Jobtrac Job Management では、CA-XPS コードは CA-GSS アドレス空間で実行されます。

CA-XPS を使用したクロスプラットフォーム スケジューリングの実行については、以下のいずれかのマニュアルを参照してください。--

- *CA NSM CA 7 Interfaces Guide*
- *CA NSM CA Scheduler Interfaces Guide*
- *CA Jobtrac Job Management Installation and Maintenance Guide*

以下の表に CA-XPS 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ACF9JCL	0	1	1	JCL ライブラリ
CAI.ACF9MOD0	6144	5	-	モジュール ライブラリ
CAI.ACF9OPTN	0	1	1	オプション ライブラリ
CAI.ACF9PROC	0	1	1	プロシージャ ライブラリ
CAI.ACF9SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.ACF9XML	32760	29	1	XML ライブラリ

CAECIS 要件

CA Examine Common Inventory Service は、IBM がサポートする z/OS バージョンで動作します。

以下の表に CAECIS 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AD0ECLS0	0	1	1	CLIST ライブラリ
CAI.AD0EJCL	0	1	1	JCL ライブラリ
CAI.AD0EMOD	6144	28	-	モジュール ライブラリ
CAI.AD0EMSG0	0	1	1	メッセージ ライブラリ
CAI.AD0EPNL0	0	5	2	パネル ライブラリ
CAI.AD0EPROC	0	1	1	プロシージャ ライブラリ
CAI.AD0ESCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.AD0EXML	32760	29	1	XML ライブラリ

CAICCI 要件

CAICCI のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- CAICCI は、APF 許可ライブラリにインストールする必要があります。このライブラリは、CAIENF サービスのインストールに使用したライブラリと同じである必要があります。
- CAICCI は、個々のデータ センターの要件に合わせてカスタマイズできる各種制御オプションをサポートします。

- CAICCI には、モジュールおよびグローバル制御ブロック用として ECSA が 172 KB 必要です。さらに、並行ホスト プログラムごとに ECSA が 304 バイト必要です。必要な ECSA の量は、個々のデータ センターの構成と一般的なアクティビティによって異なります。以下の公式を使用して推定量を算出することができます。

  172 K バイト +(CAICCI を使用する並行ホスト関連プログラムの数)*
  (308 バイト)+ 328 *(マルチ CPU 環境でのセッションの数)

  ENF STATUS の CCIR オペレータ コマンドを使用して、CAICCI を使用する並行ホスト関連の(アプリケーション)プログラムの数を求めます。このコマンドを実行すると、CAICCI リソースの一般的な状況が表示されます。

  メッセージ CAS9701I に、保留中の受信側プログラム(CAICCI を使用しているプログラム)の数が表示されます。

- マルチ CPU 環境では、定義されている CPU ごとに 256 KB を追加します。
- CCITCP、CCITCPGW、CCISSL、CCISSLGW の各スターティッド タスクに関連付けられた ID に対し、有効な OMVS セグメントを定義する必要があります。

以下の表に CAICCI 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および(MSM) XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAW4JCL	0	1	1	JCL ライブラリ
CAI.AAW4MOD	6144	82	-	モジュール ライブラリ
CAI.AAW4OPTN	0	219	2	オプション ライブラリ
CAI.AAW4PROC	0	2	2	JCL プロシージャ ライブラリ
CAI.AAW4SCST	0	2	4	MSM SCS テンプレート ライブラリ
CAI.AAW4SDF	0	1	1	サイド デッキ ファイル
CAI.AAW4XML	32760	30	1	XML ライブラリ

CAIENF の要件

CAIENF のインストール要件および考慮事項は以下のとおりです。

- IBM サポートの z/OS バージョン。
- CAIENF スターティッド タスクに関連付けられる ID には、有効なセキュリティ OMVS セグメントが定義されている必要があります。
- CAIENF は、APF 許可ライブラリにインストールする必要があります。LINKLIST は必須ではありませんが、STEPLIB 問題の発生を防ぐため、登録することをお勧めします。
- CAIENF は、スターティッド タスクとして実行されます。CAIENF スターティッド タスクの JCL が含まれているプロシージャは、PROCLIB データセットで定義する必要があります。CA Common Services for z/OS 配布メディアに格納されているサンプルは、データ センターの要件に合わせてカスタマイズできます。

  CAIENF は、個々のデータ センターの要件に合わせてカスタマイズできる各種制御オプションをサポートしています。

  注: CAIENF 制御オプションのカスタマイズの詳細については、「*Administration Guide*」を参照してください。
- CAIENF には、モジュールおよびグローバル制御ブロック用の共通ストレージが必要です。必要な CSA の量は個々のデータ センターの構成によって異なりますが、概算では、90 KB になります。

  CAIENF に必要な CSA の約 50 %は、ESCA に割り当てられます。CAIENF アドレス空間に必要なストレージの量は、システム全体の負荷、記録オプション、およびデータベース サービスの回数によって異なります。CAIENF アドレス空間には、プライベート エリア モジュールと作業域として約 3 ～ 4 メガバイト、および各待機イベント要求ごとに 平均 256 バイトが必要です。待機イベント要求の数は、ENF STATUS オペレータ コマンドから判別できます。また、CAIENF は、各アプリケーションのアドレス空間に約 4 KB を必要とします。ただし、この値は、アプリケーション構造によって異なります。

- CAIENF は CAIENF/CICS 通信用の SVC 159 を動的にインストールします。SVC 番号を選択する必要はありません。
- ACF2 ユーザは、CAIENF スターティッド タスクに対してログオン ID（LID）を作成する必要があります。
- CAIENF DCM モジュールをイベントの処理に使用できるようにするには、CAIENF 構成メンバ ENFPARM 内の DCM ステートメントで DCM モジュールを指定しておく必要があります。 DCM ステートメントの仕様の詳細については、「*Reference Guide*」の「CAIENF Control Options」のセクションを参照してください。

注: CA Datacom/AD に切り替えることで、CAIENF スターティッド タスクの JCL 内での ENFDB DD ステートメントは必要ありません。

以下の表に CAIENF 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAS9MOD	6144	24	-	
CAI.AAW1CLS0	0	1	1	CLIST ライブラリ
CAI.AAW1EXP	0	4	1	EXPORT ライブラリ
CAI.AAW1JCL	0	6	6	JCL ライブラリ
CAI.AAW1LOAD	6144	1	1	ロード ライブラリ
CAI.AAW1MOD	6144	42	-	モジュール ライブラリ
CAI.AAW1OPTN	0	1	1	オプション ライブラリ
CAI.AAW1OPTV	25600	1	1	可変長オプション ライブラリ
CAI.AAW1PROC	0	1	2	プロシージャ ライブラリ
CAI.AAW1SAMP	0	1	1	サンプル ライブラリ
CAI.AAW1SCRN	4104	8	23	画面

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAW1SCST	0	4	8	MSM SCS テンプレート ライブラリ
CAI.AAW1XML	32760	32	1	XML ライブラリ

CAIENF/CICS の要件

CAIENF/CICS のインストール要件は以下のとおりです。

- CAIENF/CICS は、IBM によって一般的にサポートされている CICS TS のすべてのリリースで動作します。
- CAIENF/CICS には、CAIENF アドレス空間内で実行されるサブタスクがあります。このサブタスクの基本機能は、すべての CICS 領域の追跡とオペレータ コマンドの処理です。CAIENF スターティッド タスクの JCL が含まれているプロシージャは、PROCLIB データセットで定義する必要があります。CA Common Services for z/OS 配布メディアで提供されるサンプルは、ユーザのデータ センターの要件に合わせてカスタマイズできます。
- CAIENF/CICS は、個々のデータ センターの要件に合わせてカスタマイズできる各種制御オプションをサポートします。
- CAS9DCM2 DCM モジュールは、CAIENF により 処理される必要があります。ENFPARMs ファイル内の DCM(CAS9DCM2) CAIENF パラメータを指定します。データベースは必要ではありませんが、DCM をインストールする必要があります。
- CAIENF/CICS インターフェースの主な機能は、CICS リリースの依存関係を処理するための 1 つの共通サービスを提供することです。これにより、新しい CICS リリースが CA CICS ソリューションに及ぼす影響が少なくなります。
- CAIENF/CICS インターフェースは、CICS リリースごとに異なるロード モジュールのセットで構成されています。これらのモジュールは、CAIENF を開始したときに CSA にロードされます。必要に応じて、適切なロード モジュールを CICS プライベート エリアにロードすることもできます。モジュール毎に、CSA または CICS プライベート エリアを約 40 KB 使用します(どちらを使用するかは、ロードされている場所によって異なります)。

- CICS 領域が開始されると、CAIENF/CICS は、CENFLIB の DDNAME が存在するかどうかをチェックします。この DDNAME が定義されていると、CAIENF/CICS は適切なモジュールを CICS プライベート エリアにロードします。CENFLIB の DDNAME が定義されていないと、CAIENF/CICS は、STEPLIB からモジュールのロードを試みます。 モジュールが STEPLIB で見つかった場合、それらが CICS プライベート エリアにロードされます。見つからない場合、最後に、CAIENF/CICS は CSA でモジュールを探します。
- この機能を使用してグローバルな CAIENF/CICS モジュールの保守を行う場合は、ENF REFRESH（CAS9Cxx）制御オプションを入力します（xx は CICS のリリース）。

以下の表に CAIENF/CICS 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロックサイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAW3MOD	6144	36	-	モジュール ライブラリ
CAI.AAW3SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.AAW3XML	32760	29	1	XML ライブラリ

CAIENF/CICS SPAWN の要件

CAIENF/CICS SPAWN のインストール要件は以下のとおりです。

- CAIENF/CICS SPAWN は、IBM によって一般的にサポートされている CICS TS のすべてのリリースで動作します。
- CAIENF/CICS SPAWN は、個々のデータ センターの要件に合わせてカスタマイズできる各種制御オプションをサポートします。
- CAICCI は必須ソフトウェアであるため、CAIENF/CICS SPAWN をインストールする前にインストールしておく必要があります。

注: CAIENF/CICS SPAWN の詳細については、「*Administration Guide*」を参照してください。

CAIENF/CICS SPAWN の基本機能は、CA ソリューションが CICS 領域外から CICS 作業単位を開始できるようにすることです。この機能により、CICS のリリースを問わず、アプリケーション ソフトウェアの実行を実現する層が提供されます。CAICCI は、この機能を使用可能にする独自の通信手段です。

CICS 領域が開始されると、CAIENF/CICS SPAWN は、CENFLIB の DDNAME が存在するかどうかをチェックします。この DDNAME が定義されていると、CAIENF/CICS SPAWN は適切なモジュールを CICS プライベート エリアにロードします。CENFLIB の DDNAME が定義されていないと、CAIENF/CICS SPAWN は、STEPLIB からモジュールのロードを試みます。モジュールが STEPLIB で見つかった場合、それらが CICS プライベート エリアにロードされます。見つからなかった場合、最後に、CAIENF/CICS SPAWN は CSA でモジュールを探します。

以下の表に CAIENF/CICS SPAWN 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAW3MOD	6144	36	-	モジュール ライブラリ
CAI.AAW3SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.AAW3XML	32760	29	1	XML ライブラリ

CAIENF/DB2 の要件

CAIENF/DB2 のインストール要件は以下のとおりです。

- CAIENF/DB2 は、DB2 R2.3 以降のすべての DB2 リリースをサポートします。
- ロード モジュール DSNXAUTH を LPA にロードすることはできません。これをロードすると、CAIENF/DB2 の初期化時に異常終了します。CAIENF/DB2 では、サブシステムでインターセプトを管理できるように、DSNXAUTH をプライベート エリアにロードする必要があります（必ずしもすべてのサブシステムでインターセプトが必要なわけではありません）。
- CAIENF/DB2 インターフェースの基本機能は、異なるレベルの DB2 のリリース依存関係を処理することです。これにより、今までは DB2 のリリースが新しくなるたびに CA DB2 ソリューションを変更する必要がありましたが、それが不要になりました。

- CAIENF/DB2 は、それ自身のロード モジュール用に CSA を約 20 KB 使用します。作業単位データ用の追加ストレージは、可能な限り拡張 CSA から取得されますが、作業単位によっては、個々のユーザ プライベート エリアからストレージが取得される場合もあります。使用する拡張 CSA の量は、個々の DB2 システムのサイズとワークロードから算出されます。
- DB2 サブシステムが開始されると、CAIENF/DB2 は制御を取得して、CAIENF ベースのアプリケーションに、必要な EXIT ポイントを照会します。実際に必要な EXIT ポイントのみがインストールされます。EXIT ポイントが必要ない場合は、1 次 CAIENF/DB2 アンカーのみがシステムにインストールされます。このアンカーは、DB2 サブシステムが終了するまで使用されません。

注: CAIENF/DB2 の詳細については、「*Administration Guide*」を参照してください。

以下の表に CAIENF/DB2 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAW5MOD	6144	5	-	CAIENF/DB2 モジュール ライブラリ
CAI.AAW5SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.AAW5XML	32760	29	1	

CAIENF/USS の要件

CAIENF/USS のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- CAIENF アドレス空間は、UNIX System Service の下で root 権限で実行する必要があります。CAIENF スターティッド タスクに関連するセキュリティ ID には、以下のものが必要です。
  - スーパーユーザ ID（UID 0）、または IBM Facility リソース BPX.SUPERUSER. のアクセス権。
  - 有効なグループ ID（GID）、ホーム ディレクトリ、およびシェル プログラム。
  - IBM Facility リソース BPX.DAEMON のアクセス権（インストールでこのリソースを定義した場合）。

  注: 詳細については、ご使用のセキュリティ製品のマニュアルを参照してください。
- CAIENF/USS コンポーネントを使用する製品も DCM（データ収集モジュール）を使用します。CAIENF/USS DCM およびすべての製品固有の DCM は、ENFPARMS パラメータ構成メンバ の DCM ステートメントで指定される必要があります。DCM ステートメントの仕様の詳細については、*「Reference Guide」*の「CAIENF 制御オプション」のセクションを参照してください。
- CAIENF/USS イベント インターセプトを有効化するには、CAIENF/USS DCM、CARRDCM0 を CAIENF 構成メンバ ENFPARM の DCM ステートメントで指定する必要があります。
- 最高のパフォーマンスを確保するため、CAIENF/USS では、新規オブジェクトを VLF（Virtual Lookaside Facility）に定義する必要があります。

VLF への新規オブジェクトの定義

新しいオブジェクトを VLF（Virtual Lookaside Facility）に定義すると、特定の CA Common Services for z/OS コンポーネントのパフォーマンスが向上する可能性があります。

VLF に新しいオブジェクトを定義するには、SYS1.PARMLIB の COFVLFxx メンバにエントリを追加します。xx は、システム プログラマが割り当てる VLF 識別子です。

例：VLF への新規オブジェクトの定義

```
CLASS NAME(CAENFU) /* ENF/USS パス名ルックアップ キャッシュ*/
EMAJ(PATHCACHE)    /* 必要な大分類名*/
MAXVIRT(512)       /* 512 = 2MB*/
```

クラス名（CAENFU）と大分類名（PATHCACHE）は、例に示すように正確に入力する必要があります。

多くの場合、MAXVIRT は 512 ～ 1024（仮想ストレージの 2 MB ～ 4 MB に相当）の範囲であれば十分ですが、以下の公式に従って変更することもできます。

```
MAXVIRT = MAXFILEPROC * MAXPROCSYS * 16
```

MAXFILEPROC と MAXPROC は、SYS1.PARMLIB（BPXPRMxx）にある UNIX System Service の構成パラメータです。

以下の表に CAIENF/USS 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ACQ9MOD	6144	9	-	モジュール ライブラリ
CAI.ACQ9SCST	0	1	1	MSM SCS テンプレート ライブラリ
CAI.ACQ9XML	32760	29	1	XML ライブラリ

CAIRIM 要件

CAIRIM サービスには CA LMP、サービス性および CAISSF サービスが含まれています。

注: CAISSF の CA セキュリティ製品以外のサポートの詳細については、「Administration Guide」を参照してください。

CAIRIM のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- CAIRIM は、あらゆる z/OS プロセッサ上で実行でき、特別な設定や変更の必要はありません。
- CAIRIM は、APF 許可ライブラリにインストールする必要があります。
- すべての SMF イベントまたはデータ処理ソリューション ルーチンで、CAIRIM SMF 記録がアクティブになっている必要があります。CAIRIM SMF Interceptor コンポーネントには、特定の SMF レコードは必要ありません。SMF パラメータで SMF がアクティブであることが指定されている場合に、必要に応じて、すべての SMF レコード タイプを抑制することができます。

  CA ソリューションによっては、特定の SMF レコードを記録する必要がある場合があります。この記録は、履歴分析とレポート作成にのみ使用され、ソリューションの操作や初期化には使用されません。
- CAIRIM には、ECSA が約 12 KB、および CSA が約 4 KB 必要です。常駐モジュールのその他の CSA 要件は、それぞれのサービスまたは製品によって異なります。その他のソリューション固有の情報については、そのソリューションのインストール マニュアルを参照してください。
- CA LMP には、ECSA が約 22 KB 必要です。

- CAISSF には、ルーチンへのセキュリティ組み込み用として CSA が約 1KB、およびそれぞれのセキュリティトランスレータ用として約 2KB ～ 4KB 必要です。
- CAIRIM は、CDE エントリの作成に、モジュールあたり SQA を約 30 バイト使用します。
- CA LMP は、CAIRIM の初期化時に動的にインストールされる SVC を使用します。CA LMP は最初に見つけた空き SVC スロットを使用するので、CA LMP の SVC 用として SVC エントリを選択する必要はありません。
- CAIRIM には CAILPA データ セットがあります。それはサービス性に必要です。CAILPA データ セットをシステム 'SYS1.PARMLIB'LPALSTxx メンバに追加する必要があります。ELPA 使用状況はおよそ 3.5K です。

以下の表に CAIRIM ユーティリティ配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AAS9CLS0	0	1	1	CLIST ライブラリ
CAI.AAS9JCL	0	2	2	JCL ライブラリ
CAI.AAS9MAC	0	1	1	
CAI.AAS9MOD	6144	24	-	モジュール ライブラリ
CAI.AAS9OPTN	0	1	3	オプション ライブラリ
CAI.AAS9PROC	0	1	2	JCL プロシージャ ライブラリ
CAI.AAS9SAMP	0	5	1	SAMP ライブラリ
CAI.AAS9SCST	0	2	6	MSM SCS テンプレート ライブラリ
CAI.AAS9SDF	0	1	1	サイド デッキ ライブラリ
CAI.AAS9XML	32760	59	2	ソース ライブラリ

CAISDI 要件

CAISDI は、soap、med、els の各コンポーネントで構成されています。以前はこれらのコンポーネントは個別にインストールする必要がありました。現在はこれらは 1 つの製品としてインストールされます。

CA Common Services for z/OS Release 14.1 以降、CAISDI/elmds は新規コンポーネントとして追加されています。CAISDI/elmds は med と els の機能を組み合わせて、常駐アドレス空間で実行されます。CAISDI/elmds は個々の med および els コンポーネントの一方または両方の代わりに使用できます。

CAISDI には、soap、els、med の個々のコンポーネントに関して以下のようなインストール要件があります。

注: CAISDI/elmds 固有の要件は明示的に示されます。

- IBM サポートの z/OS バージョン。(elmds に対しても。)
- 4 MB 以上の領域サイズを使用します。
- CAISDI/med は、共通ストレージ常駐サービスおよびインターセプトをロードするために、約 24 KB の拡張された共通サービス エリア(ECSA)を使用します。

  サービス コールが未処理である間、特定のタイプのサービス コールは約 100 KB の ECSA を使用します。ただし、CAISDI はクロス メモリ サービスを拡張的に使用して、共通ストレージエリアの必要性を回避します。
- CAISDI/els が使用する CSA の量は、どの製品がこのコンポーネントを使用するかによって変化します。(elmds に対しても。)

  CAISDI/els Interface Controller は、ECSA の使用状況を製品ごとに個別に報告します。
- CAI.CAW0OPTN には、すべての CAISDI コンポーネントの CAISDI 初期化ステートメントが含まれています。複数の z/OS システムがパラメータ データ セットを共有する場合、そのデータ セットは共有される DASD ボリューム上に存在する必要があります。
- CAI.CAIEVENT には、CAISDI/els コンポーネントのイベント定義が含まれています。このインターフェースを使用する CA Technologies 製品はイベント メンバを提供します。
- CAISDI は、TCP/IP を使用したネットワーク接続を介して、CA Service Desk のインターフェースを提供します。少なくとも 1 つの z/OS システムで、TCP/IP がオンになっていて、実行中であることを確認してください。CAISDI/soap クライアント インストールがそこで実行されます。(elmds に対しても。)

- CAISDI/soap クライアント アドレス空間のユーザ ID については、UNIX System Services プロファイルが UID 0 に定義されているか、SUPERUSER（BPX.SUPERUSER）である必要があります。（elmds に対しても。）
- CA Service Desk がインストールされ、正しく構成されていることを確認します。（elmds に対しても。）
- 一部の製品では、Service Desk 要求の記述内容が HTML 形式で生成されます。

デフォルトで、CA Service Desk は、要求を記述するフィールドの埋め込み HTML 命令をレンダリングします。この機能は無効にする事ができます。要求テキストを適切にレンダリングするには、CA Service Desk サーバで HTML レンダリングをサポートする必要があります。CA Service Desk 管理者にこのタスクの実行を依頼してください。

このタスクには、keeptag および keeplink のサポートを追加する、detail_cr.htmpl フォームのカスタマイズが含まれます。

注: CA Service Desk のインストールおよび構成の詳細については、「*CA Service Desk Installation Guide*」を参照してください。

以下のリストは、各 CAISDI 配布ライブラリの最小ストレージ要件を示しています。このリストは、必ずしもインストール中に提供される実際の配布ライブラリ割り当てを表すものではありません。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが含まれています。この変更は、IBM SMP/E パッケージング標準および CA パッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、システムでこれらのデータ セットに対して最適なブロック サイズを割り当てることができます。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ADYFJCL	0	1	1	マクロ ライブラリ
CAI.ADYFMAC	0	2	1	マクロ ライブラリ
CAI.ADYFMOD	6144	42	-	モジュール ライブラリ
CAI.ADYFOPTN	0	2	3	オプション ライブラリ
CAI.ADYFOPTV	25600	1	1	オプション V ライブラリ
CAI.ADYFPROC	0	1	2	プロシージャ ライブラリ

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ADYFSCST	0	1	3	MSM SCS テンプレート ライブラリ
CAI.ADYFXML	32600	30	1	XML ライブラリ

Earl Service の要件

Earl Service のインストール要件は以下のとおりです。

- IBM サポートの z/OS バージョン。
- Earl サービスには、CA Sort for z/OS、IBM DF/Sort、またはモジュール名が SORT の互換性のある製品が必要です。

以下の表に Earl サービス配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および(MSM) XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。 BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI. AAXEJCL	0	1	1	JCL ライブラリ
CAI. AAXEMAC	0	2	1	マクロ ライブラリ
CAI. AAXEMOD	6144	17	3	モジュール ライブラリ
CAI. AAXESRC	0	1	1	ソース ライブラリ

Event Management の要件

Event Management のインストール要件は以下のとおりです。

- 物理ファイル システムが実装されたフル機能の OMVS および zFS を含む IBM サポートの z/OS バージョン。
- データセットが外部セキュリティにより保護されている場合、OMVS ユーザ アドレス空間のユーザ ID は zFS データセットに対する更新権限が必要です。
- Event Management をインストールするときに使用するユーザ ID には、スーパーユーザ権限と以下のリソースに対する読み取りアクセス権が必要です。

  BPX.FILEATTR.APF

  BPX.FILEATTR.PROGCTL

  BPX.SERVER
- IBM HTTP サーバ
- JDK 1.4、1.5、または 1.6 レベルの Java runtime 環境

  重要: z/OS には、Java 環境が Web サーバと共に含まれており、両方が一緒にインストールされるようになっています。z/OS 上で Java を以前に使用していなかった場合は、IBM にテープのコピーを注文できます。必要な前提条件を確実にインストールすると共に、インストール マニュアルに厳密に従ってください。Event Management を起動する前に、IBM 提供の Java サンプル プログラムが実行できることを検証する必要があります。
- BPXPRMxx 設定値の MAXASSIZE が 128 MB を超える
- BPXPRMxx 設定値の MAXPROCUSER が 100 を超える
- BPXPRMxx 設定値の MAXCPUTIME が 86400
- ディスク領域（RO および RW zFS）は合計で約 900 シリンダ

  注: 一時 HFS 領域も必要です。一時 HFS ファイルに 50 MB 以上の利用可能領域があることを確認してください。
- 以下の表にオプションの Java GUI を使用するための上記のクラス CAIUNI のリソースのセキュリティ定義を示します。

定義対象のリソース	アクセス権の許可先
EMSRVC.APPMAP	Enterprise Management
EMSRVC.MSG RECORD	メッセージ
EMSRVC.MSG ACTION	メッセージ アクション

定義対象のリソース	アクセス権の許可先
EMSRVC.CALENDAR	カレンダ
EMSRVC.CONLOG	コンソール
EMSRVC.CONLOG ANNOTATION	コンソール メッセージの注釈

以下の表に Event Management 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AD5IJCL	0	5	1	JCL ライブラリ
CAI.AD5MOD	6144	5	1	モジュール ライブラリ
CAI.AD5IPROC	0	6	1	プロシージャ ライブラリ
CAI.AD5ISDF	0	4	1	サイド デッキ ファイル
CAI.AD5IZFS	32760	7000	3	ZFS 要素タイプ

Event Management ユーティリティの要件

以下の一覧には、各 Event Management ユーティリティ ライブラリの最小ストレージ要件が示されます。インストール中に提供される実際の配布ライブラリの割り振りを示しているとは限りません。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。 BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AD5IJCL	0	1	1	JCL ライブラリ
CAI.AD5IMOD	6144	1	1	モジュール ライブラリ
CAI.AD5ISDF	0	1	1	サイド デッキ ファイル

CA Health Checker Common Service の要件

CA Health Checker Common Service は、IBM がサポートするどのバージョンの z/OS でも動作します。

以下のリストは、各ライブラリの最小ストレージ要件を示しています。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AEF5MOD	6144	19	-	モジュール ライブラリ
CAI.AEF5SCST	0	1	1	MSM SCS ライブラリ
CAI.AEF5SDF	80	1	1	サイド デッキ ファイル
CAI.AEF5XML	32760	29	1	XML ライブラリ

CA Health Checker Common Service は、カスタマイズする必要はありません。唯一必要な条件は、そのロード モジュールがシステム リンクリストに登録されているということです。

CA MSM Common Services の要件

CA MSM Common Services は、IBM がサポートするどのバージョンの z/OS でも動作します。

以下の表に、配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。 データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AETNEXP	0	47	1	CA Datacom エクスポート
CAI.AETNJCL	0	1	2	JCL ライブラリ
CAI.AETNMOD	6144	178	-	PDSE モジュール ライブラリ
CAI.AETNOPTN	0	1	1	オプション ライブラリ
CAI.AETNPROC	0	1	1	プロシージャ ライブラリ
CAI.AETNSCST	0	2	1	MSM SCS テンプレート ライブラリ
CAI.AETNSDF	0	4	1	サイド デッキ ライブラリ
CAI.AETNXML	32760	1	1	XML ライブラリ
CAI.AETNXML0	27998	162	4	XML ライブラリ

SRAM Service の要件

SRAM Service は、IBM がサポートするバージョンの z/OS で機能します。

以下の表に SRAM 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM） XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.AASRJCL	0	1	1	JCL ライブラリ
CAI.AASRMAC	0	1	1	マクロ ライブラリ
CAI.AASRMOD	6144	3	2	モジュール ライブラリ
CAI.AASROPTN	0	2	1	オプション ライブラリ*

*USERMOD(ASR0001) のインストールに使用

ViewPoint 要件

ViewPoint サービスは、IBM がサポートする z/OS バージョンで正常に動作します。

以下の表に ViewPoint ユーティリティ配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。データ セット割り当て JCL および（MSM）XML には、LRECL が 80 の FB データ セットでブロック サイズが 0 のものが用意されています。この変更は IBM SMP/E パッケージング標準および CA のパッケージング標準の両方に準拠するために行なわれました。BLKSIZE=0 を指定すると、これらのデータ セット用に最も効率的なブロック サイズをシステムが選択できるようになります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
CAI.ADU4CICS	6144	14	1	CICS ロード ライブラリ
CAI.ADU4DLD	8204	14	5	ダイアログ ライブラリ
CAI.ADU4JCL	0	1	1	JCL ライブラリ
CAI.ADU4MLD	0	4	1	マクロ ライブラリ
CAI.ADU4MOD	6144	92	9	モジュール ライブラリ
CAI.ADU4PANL	4104	42	41	パネル ライブラリ
CAI.ADU4TLD	0	3	2	テンプレート ライブラリ

Apache Tomcat 要件

Tomcat は、IBM がサポートするどの z/OS バージョンでも正常に動作します。

v1.6 以上の IBM Java JDK が必要です。Java SDK の 64 ビット バージョンも v1.6 以降でサポートされています。

以下の表に Tomcat 配布ライブラリごとの最小ストレージ要件を示します。これらの最小ストレージ要件は、インストール時に配布ライブラリに実際に割り当てられるものと異なる場合があります。

ライブラリ名	ブロック サイズ	トラック数	ディレクトリ ブロック数	説明
TPV.AEG1JAR	6144	112	1	JAR ファイル ライブラリ
TPV.AEG1SHSC	27998	1	1	SMP 適用シェル スクリプト ライブラリ

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 Support 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 Mainframe Software Manager 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。

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。少なくとも、以下の Web ブラウザの*いずれか*が必要です。Microsoft Internet Explorer 6.0、7.0、8.0、または Mozilla Firefox 3.5。

CA MSM 管理者から CA MSM の URL を取得する必要があります。

Web ベース インターフェースを使用した CA MSM へのアクセス方法

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 Support 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 Support 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 Support 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。

CA MSM の使用方法: 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、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、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、製品をターゲット システムに展開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。

これを行うには、以下のタスクを完了します。

1. CA Support Online のアカウントを設定します。

   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 Support Online Web サイトで作成できます。

2. サイトの CA MSM の URL を決定します。

   CA MSM 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 Support Online Web サイトに対する認証情報を使用して、CA MSM アカウントを作成するように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]タブに移動して、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 Support Online Web サイト全体で、CA Support Online Web サイトに対する認証情報に関連付けられているサイト 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。

これで、製品をインストールまたは管理する準備が整いました。

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。

これを行うには、以下のタスクを完了します。

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。

Agent Technology と Event Management のインストール後の作業

Agent Technology と Event Management のインストール後に、以下のインストール後のタスクを実行します。これらのタスクは展開の前に完了する必要があります。

これらのインストール後の手順では、zFS データ セットがインストール時のマウント ポイントにマウントされると想定しています。

Agent Technology のインストール後の作業

Agent Technology のインストールを完了する方法

1. Agent Technology 用のユーザ ID を作成します。

   Agent Technology ジョブは 1 つのユーザ ID を使用して実行する必要があります。通常、このユーザ ID は AWADMIN で、グループ名は AWGROUP です。このユーザ ID には、以下の条件を満たすように UNIX System Services セグメントを定義する必要があります。

   注: ユーザ ID は、UID(0)以外にしてください。

   - ホーム ディレクトリは、Agent Technology のインストール パスと同じです。
   - デフォルトのシェルとして z/OS シェルが指定されています。通常、これは /bin/sh です。

   Agent Technology 用のユーザ ID が作成されます。

   インストール終了後、サイトのセキュリティ ポリシーによっては、別のユーザ ID を複製して本番のシステムで使用できます。

   CNSMJCL メンバ B6DI0015 で、このユーザ ID を作成できます。このジョブでは、RACF、CA ACF2、および CA Top Secret に対応する制御ステートメントが用意されています。

   セキュリティ パッケージに対応するステートメントを更新し、他のステートメントを削除します。

   重要: このジョブの実行に使用するユーザ ID には、コマンドを実行する権限が付与されている必要があります。

2. Agent Technology ディレクトリ グループ所有権および Agent Technology 用のユーザ ID 設定モード ビットを設定します。

   Agent Technology の一部のプログラムは、UID(0) で実行する必要があります。

   CNSMJCL メンバ B6DI0065 を編集して、これらのプログラムのユーザ ID ビットを設定します。

   このジョブは、Agent Technology zFS ファイルを所有する UID で実行されている必要があります。

3. Agent Technology のコマンド ライン EXEC を有効にします。

   必要に応じて、すべての OMVS ユーザが Agent Technology プログラムをコマンド ラインから実行できるように、環境変数を設定できます。このジョブでは、/etc/profile が更新されます。

   CNSMJCL メンバ B6DI0068 を使用します。

Event Management のインストール後の作業

Event Management のインストールを完了する方法

1. 追加の Event Management ディレクトリを作成します。
   a. CNSMJCL メンバ D5II0040 を変更してサブミットします。
   b. EXPAND の STEP で参照される STDOUT ファイルと STDERR zFS ファイルを確認して、このジョブの結果を確認します。リターン コードのみで正常に完了したと判断しないでください。
2. Event Management プロファイルを作成します。
   a. Event Management がすでにユーザのシステムにインストールされている場合は、/etc/profile ファイルにある Event Management 更新を削除(単なるコメント アウトではなく)します。次に、この手順に関連付けられているジョブをサブミットします。更新が存在する場合、それはファイルの最後に明確にマーキングされています。
   b. CNSMJCL メンバ D5II0050 を変更してサブミットします。Event Management の実行は、さまざまな環境変数の設定に依存します。

システムの標準に合わせて以下の変数を変更します。

- STEPLIB と CA_DBHLQ

  Calendars オプションまたは Message Actions オプションのいずれかを使用する予定がある場合、CA Common Services コンポーネントのインストールと設定を完了してから、CA Datacom/AD をインストールする必要があります。CA Datacom/AD データセットの名前または高レベル修飾子が不明な場合は、CA Datacom/AD のインストールの完了後に、この情報を使用してプロファイル ファイルを直接編集できます。

  STEPLIB は、CA Datacom/AD および CA Common Services ロード ライブラリを以下の順序で参照する必要があります。

  ```
  STEPLIB=$STEPLIB:CAI.DATACOM.CUSLIB
  STEPLIB=$STEPLIB:CAI.DATACOM.SMPE.CAAXLOAD
  STEPLIB=$STEPLIB:CAI.CAW0LOAD
  STEPLIB=$STEPLIB:CAI.CNSMLOAD
  ```

  CA_DBHLQ はユーザの CA Datacom/AD 高レベル修飾子を参照する必要があります。その値は、カスタム データ セット プレフィクスです。CA_DBHLQ の値の末尾がドットにならないようにする必要があります。この高レベル修飾子は、CUSLIB 用の STEPLIB で使用される修飾子と同じです。

  Calendars または Message Actions オプションを使用しない場合、CA Datacom/AD 参照を削除します。

  Calendars または Message Actions オプションを使用しない場合、STEPLIB はユーザの CA Common Services ロード ライブラリのみを参照します。CA Datacom/AD データセットを参照している STEPLIB ステートメントを削除します。CA Common Services ロード ライブラリは以下のとおりです。

  ```
  STEPLIB=$STEPLIB:CAI.CAW0LOAD
  STEPLIB=$STEPLIB:CAI.CNSMLOAD
  ```

  また、CA_DBHLQ ステートメントを削除します。

- CA_OPR_ZOSDB は、CA Datacom/AD データベースを使用するかどうかを示します。デフォルト値は N (いいえ) です。Calendars または Message Actions を使用する場合、この環境変数の値を Y (はい) に変更します。
- INSTALLSAF は、Store and Forward をアクティブにするかどうかを示します。デフォルト値は Y (はい) です。
- UPDATE_ETC は、/etc/profile を更新して、Event Management コマンドの実行に必要な環境変数を設定するかどうかを示します。デフォルト値は N (いいえ) です。

  ユーザが Y (はい) を選択し、Event Management がこのシステムにすでにインストールされている場合、/etc/profile は更新されません。/etc/profile の内容を確認して、定義されている現行の CAIGLBL0000 値が正しいかどうか、およびすべてのユーザにとってより望ましいものであるかどうかを判断します。

  N (いいえ) を選択した場合、CAIGLBL0000 ディレクトリにある tngprofile ファイルが、後にログインに使用される適切なプロファイル設定で更新されます。

3. Event Management のリンクを作成します。

   CNSMJCL メンバ D5II0065 は Event Management で必要なリンクを作成し、Event Management コンポーネントのインストール スクリプトを実行します。このジョブは長期間にわたります。

   EXPAND の STEP で参照される STDOUT ファイルと STDERR zFS ファイルを確認して、このジョブの結果を確認します。リターン コードのみで正常に完了したと判断しないでください。

   重要: JAVA_HOME を最初に初期化する必要があります。そうしない場合、この手順は正しく完了しません。

既存製品を保守する方法

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。

これを行うには、以下のタスクを完了します。

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 APPLY 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 プロセスが完了した製品は、いつでも展開できます。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。

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、すでに取得およびインストールしている 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 レジストリを設定します。
   a. 使用するシステムを決定します。
   b. それらのシステムに対して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、それらを検証します。
   d. データ宛先情報などの FTP 情報を各システム 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. New Deployment ウィザードの各手順を実行するなどして、展開を作成します。

   展開作成後、それを保存し、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、後でそれを変更するか、ウィザードから直接展開できます。

   注: 同じ手順を使用して以前定義されていたシステムに他の製品を展開する必要がある場合、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。これには、スナップショットの作成、ターゲットへの転送、およびユーザのメインフレーム環境への展開(アンパック)などが含まれます。

展開プロセスが完了した製品は、いつでも設定できます。設定プロセスを開始する前に、CA MSM の外部で他の手順を手動で実行する必要がある場合があります。

CA Common Services の展開

CA Common Services の展開プロセスは、展開製品リスト内の複数のオプションを提供します。コンポーネントをグループまたは単独で選択できます。BASE コンポーネント用に個別に製品を選択することはできません。それは、BASE コンポーネントはすべてインストールして展開する必要があるからです。

重要: Agent Technology および Event Management のインストールを実行後、「Agent Technology と Event Management のインストール後の作業 (P. 85)」セクションに述べられているタスクを実行します。Agent Technology と Event Management のインストール後の作業は展開する前に実行される必要があります。

コンポーネントのグループを選択するためには、選択した CSI にインストールしたすべてのコンポーネントが揃っている必要があります。そうでない場合、選択はブロックされます。

展開プロセスで展開されるのは、製品 ID に定義された FMID に関連する SMP/E ターゲット データ セットのみです。

Custom Data Sets セクション下のターゲット システム上に割り当てられコピーされる非 SMP/E ターゲット データ セットを追加できます。

カスタム データ セットを追加するには、[ADD DATASET]ボタンをクリックしてからデータ セット情報を入力します。

第 4 章: SAMPJCL メソッドを使用した Pax ファイルからのインストール

このセクションには、以下のトピックが含まれています。

Pax Enhanced ESD ファイル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 のプロセスについて説明します。初めて Pax-Enhanced インストールを実行する場合は、この概要を読み、全体の手順に従うことをお勧めします。経験のある UNIX ユーザなら、この後のインストールを実行するのに「*Pax-Enhanced ESD Quick Reference Guide*」またはこの概要で十分です。

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。

ユーザのサイトが z/OS UNIX System Services へのアクセスを制限し、書き込み権限がない場合は、権限を持つ個人に MVS データ セットのリストを渡し、手順 1 ～ 4 の実行を依頼します。USS は製品の実際の SMP/E RECEIVE に必要ではありません。ただし、残りのインストール手順は、インストールしている製品に応じて USS が必要な場合があります。Agent Technology、Event Management、または CA Common Services に付属して出荷される Tomcat のバージョンなど、USS が必要な製品をインストールする場合、インストールを実行するには USS 権限が必要です。

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

1. ファイル システムの割り当ておよびマウントを実行します。pax ファイルの受信や解凍手順を実行するために、このプロセスでは USS ディレクトリが必要です。Pax-Enhanced ESD 専用のファイル システムを割り当ててマウントし、このファイルシステム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に、このディレクトリへの書き込み権限があることを確認します。

2. ユーザの USS ディレクトリに製品の pax ファイルをコピーし、以下のいずれかのオプションを選択します。

   - CA Support Online からお使いの PC に zip ファイルをダウンロードした後、ファイルを解凍し、製品の pax ファイルを USS ディレクトリにアップロードします。
   - CA Support Online からユーザの USS ディレクトリに pax ファイルを直接 FTP 転送します。
   - DVD をユーザの PC にロードし、pax ファイルをユーザの USS ディレクトリにアップロードします。

   注: CA Common Services ソフトウェア コンポーネントは 4 つの pax ファイルを使用してパッケージングされています。どの pax ファイルをアップロードするかを決定するには、「概要」の章を参照してください。アップロードする各 pax ファイルを、それ自体の USS ディレクトリに格納します。たとえば、ESD 処理に対して作成された、"base" という名前のディレクトリを USS ファイル システム内に作成し、次に、CA Common Services base pax ファイルをこの "base" ディレクトリにアップロードします。

   アップロードした各 pax ファイルに対して、以下の手順を実行します。

3. pax ファイルから製品ディレクトリを作成します。pax ファイルが含まれるディレクトリを現在の作業ディレクトリに設定し、新規 USS ディレクトリを作成する以下のコマンドを入力します。

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

4. z/OS データ セットへのインストール ファイルのコピー z/OS インストールデータ セットを作成するには、SMP/E GIMUNZIP ユーティリティを使用します。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します。
5. 製品のインストールを実行します。製品のインストールを完了するには、README ファイルやインストールの注意事項などの製品固有のドキュメントを参照してください。
6. (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 コマンドによって作成されたディレクトリ、そのディレクトリ内のすべてのファイル、SMP/E RELFILE、SMPMCS、HOLDDATA データ セットを削除します。
7. メンテナンスを APPLY します。
8. 製品を展開します。
9. 設定を行います。

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. 96)」でダウンロード インターフェー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。

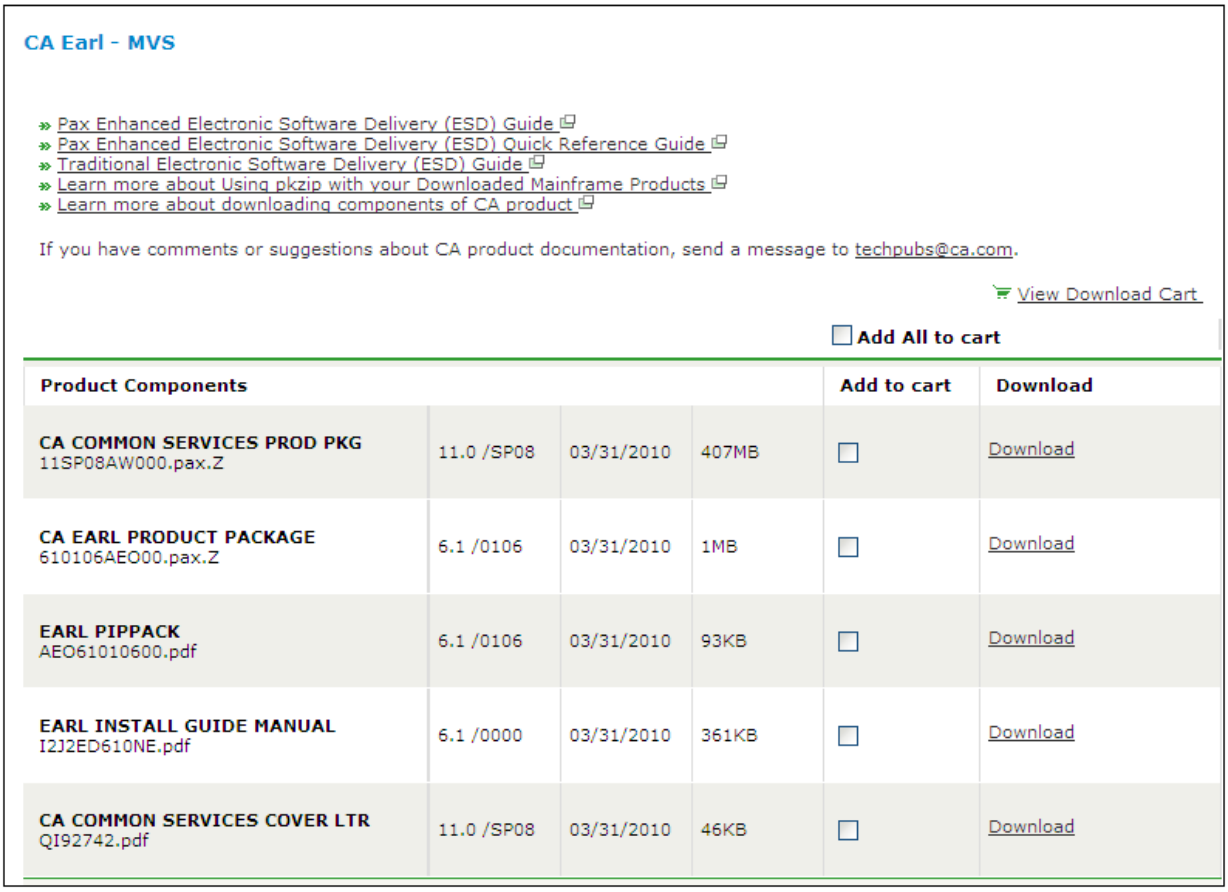
4. 製品固有の手順に従って、製品のインストール手順を実行します。

   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

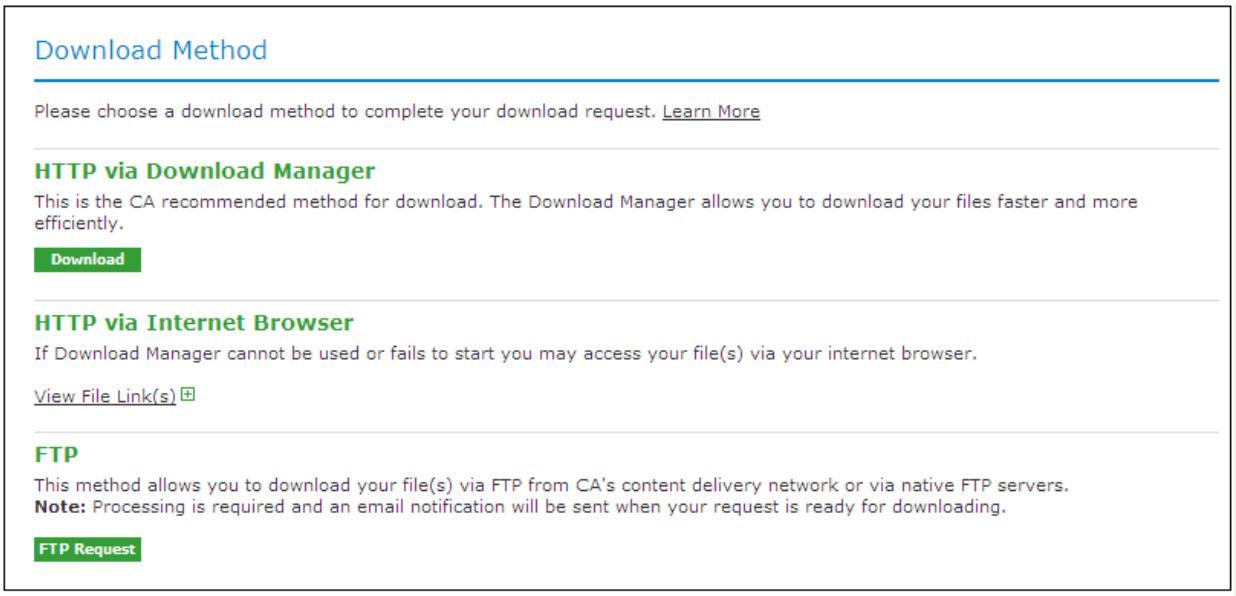
If you have comments or suggestions about CA product documentation, send a message to techpubs@ca.com.

View Download Cart

Add All to cart

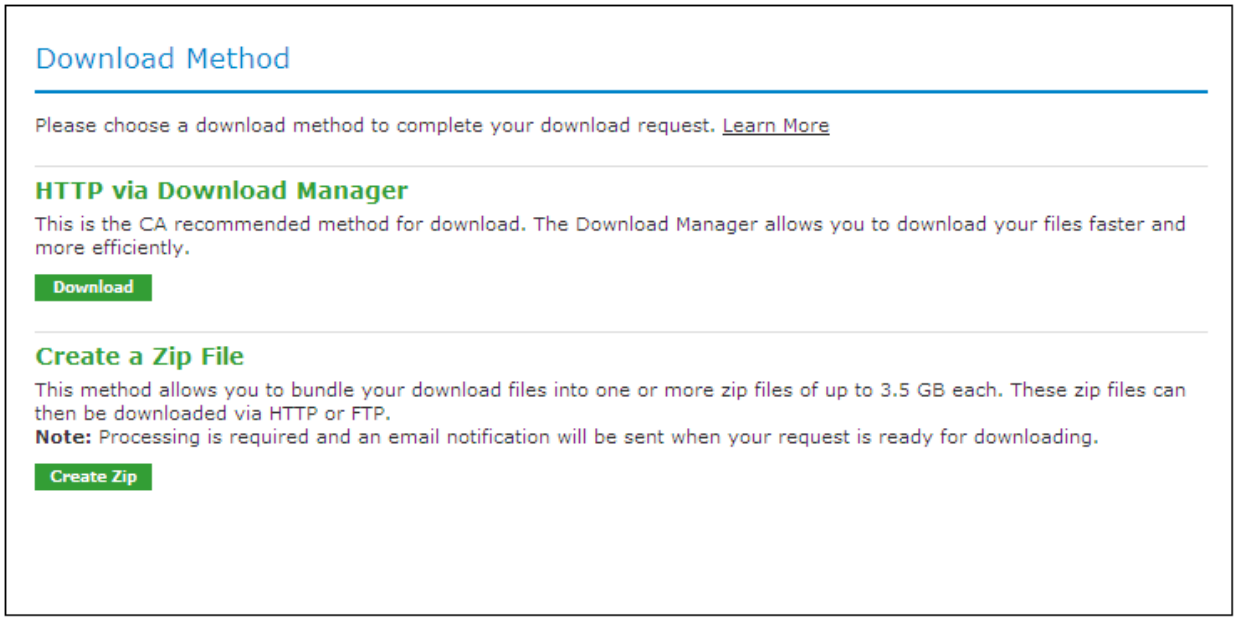
Product Components				Add to cart	Download
CA COMMON SERVICES PROD PKG 11SP08AW000.pax.Z	11.0 /SP08	03/31/2010	407MB	☐	Download
CA EARL PRODUCT PACKAGE 610106AEO00.pax.Z	6.1 /0106	03/31/2010	1MB	☐	Download
EARL PIPPACK AEO61010600.pdf	6.1 /0106	03/31/2010	93KB	☐	Download
EARL INSTALL GUIDE MANUAL I2J2ED610NE.pdf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



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。

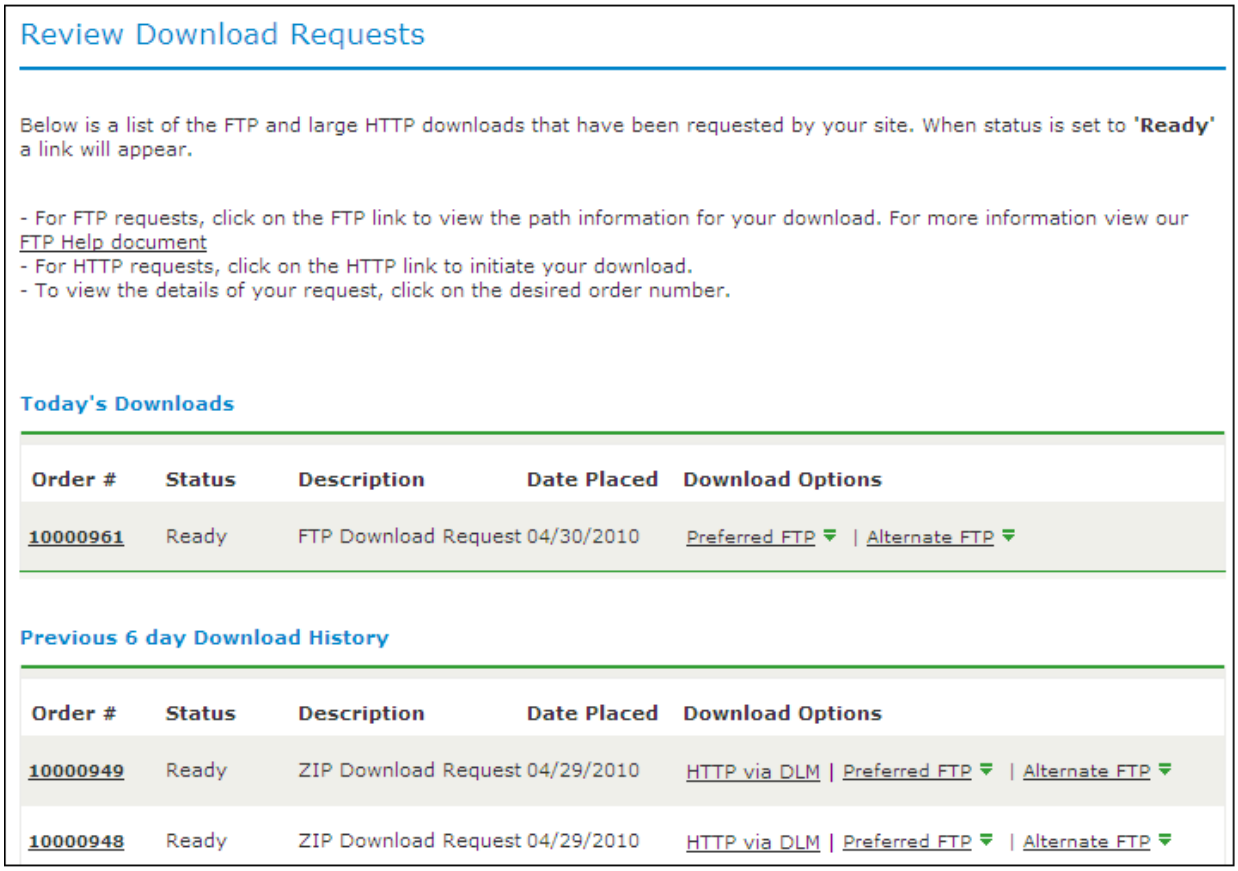
注：[HTTP] メソッドを使用したメインフレームのダウンロードについては、[Learn More]リンクをクリックしてください。



[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=IEFBR14
   //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、IBM の「*z/OS UNIX System Services User Guide（SA22-7802）*」を参照してください。

USS ディレクトリへの 製品の Pax ファイルのコピー

CA 製品の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の pax ファイルをコピーします。CA Common Services ソフトウェアのコンポーネントは 4 つの pax ファイルを使用してパッケージ化されているので、必要な pax ファイルを今すぐ USS ディレクトリにコピーする方が、後でこの手順に戻るよりも楽な場合があります。

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 システムに製品の pax ファイルを直接ダウンロードする。
- CA Support Online の FTP サーバから PC に pax ファイルをダウンロードし、z/OS システムにそれらのファイルをアップロードする。
- CA Support Online から PC に製品ファイルをダウンロードする。ダウンロードに ZIP ファイルが含まれていた場合は、ファイルを解凍し、解凍した pax ファイルを z/OS システムにアップロードする。
- DVD 上の pax ファイルをユーザの z/OS システムにアップロードする。

このセクションには、製品の pax ファイルを CA Support Online FTP サーバからユーザの z/OS システム上の USS ディレクトリに直接ダウンロードするサンプル バッチ ジョブ、pax ファイルをユーザの PC から z/OS システム上の USS ディレクトリにアップロードするサンプル 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。サイトで使用する適切な FTP 手順を決定するには、ローカルのネットワーク管理者に連絡してください。

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 Technologies Products Download]ウィンドウ上の対応する pax ファイルの[Size]カラムの値と一致する必要があります。

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、ファイルを入手でき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://ftpdownloads.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

添付されている CAtoMainframe.txt JCL ファイルに、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
バイナリ
get FTP location
quit
```

PC からのメインフレームへのファイルのアップロード

CA Support Online から PC に pax ファイルまたは zip ファイルをダウンロードする場合、または DVD を使用している場合、この手順で PC からユーザの 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. 製品の pax ファイルまたは zip ファイルを PC にダウンロードするには、「Pax-Enhanced ESD ダウンロードの仕組み」の手順に従います。ZIP ファイルをダウンロードする場合、製品の pax ファイルを使用するために、最初にファイルを解凍します。

   pax ファイルまたは ZIP ファイルがユーザの PC に展開されます。

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 コマンドをカスタマイズし、以下の変更を含むコマンドを入力します。

   a. *mainframe* を 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* をユーザの z/OS ユーザ ID に置き換えます。

   c. *password* をユーザの z/OS パスワードに置き換えます。

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

   e. *yourUSSESDdirectory* を ESD の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送られます。

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

製品の pax ファイルを製品のインストール ディレクトリに抽出するには、Unpackage.txt として PDF ファイルに添付されているサンプル ジョブを使用します。CA Common Services ソフトウェアのコンポーネントは 4 つの pax ファイルを使用してパッケージ化されているので、必要な pax ファイルすべてに今すぐこの手順を実行する方が、後でこの手順に戻るよりも楽な場合があります。pax ファイルごとに個別のディレクトリを作成する必要があります。

重要: Pax-Enhanced ESD プロセスを簡略化するために、このガイドの PDF 版には、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 リーダ下部の左端にあるクリップ アイコンをクリックします。クリックすると、添付ファイルを表示するウィンドウが開きます。ファイルをダブルクリックすると、サンプル JCL が表示されます。

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 ステートメントを用意します。
2. *yourUSSESDdirectory* を ESD のダウンロードに使用した USS ディレクトリの名前に置き換えます。

   ジョブは、ユーザが指定した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、ユーザが指定した pax ファイルを参照します。
4. ジョブをサブミットします。

   そのジョブが実行され、製品ディレクトリが作成されます。

注: このジョブで説明した変更を実行した後、PARM= ステートメントが 71 文字を超える場合は、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。CA Common Services ソフトウェアのコンポーネントは 4 つの pax ファイルを使用してパッケージ化されているので、必要な pax ファイルすべてに今すぐこの手順を実行する方が、後でこの手順に戻るよりも楽な場合があります。pax ファイルにはそれぞれそれ自身の UNZIPJCL ファイルが含まれます。

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 を使用しています。

5. インストール処理で使用される z/OS データ セットに対して、*YourHLQ* の出現箇所をすべて高レベル修飾子（HLQ）に変更します。展開されたそれぞれの CA Common Services の pax ファイルに対し、同じ HLQ を使用することをお勧めします。同じ HLQ を使用すれば、すべての CA Common Services コンポーネント用のインストールを一度で実行することができます。CA Common Services の pax ファイルにはそれぞれそれ自身の UNZIPJCL ファイルがあります。各 UNZIPJCL ファイル内の *YourHLQ* 値に対して別の HLQ を使用する場合、少なくとも、複数の SMP/E RECEIVE を実行して、解凍されたファイルを SMP/E インストール環境に持ち込む必要があります。SMP/E RELFILE に使用するのと同じ値を *yourHLQ* に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 の参照マニュアル「*SMP/E for z/OS Reference (SA22-7772)*」をご覧ください。

ネイティブ SMP/E JCL を使用した製品のインストール方法

以下の手順では、ネイティブ SMP/E JCL を使用して、製品をインストールする手順を説明します。

1. 製品データ セットおよび SMP/E データ セットを割り振ります。
2. SMP/E CSI を作成するか、既存の CA Common Services v14.0 CSI を使用します。システムを r14.1 にアップグレード注に CA Common Services v14.0 メンテナンスを適用している場合は、新規 Base および Optional Common Services r14.1 インストールに対して SMP/E CSI を作成します。

3. 基本機能を RECEIVE します。

   UNZIPJCL ジョブが作成した DASD 上のファイルを使用して、SMP/E RECEIVE を完了します。DASD から製品を RECEIVE するためにカスタマイズされたサンプル ジョブを含む、製品のサンプル JCL ライブラリを参照します。以下の値を指定します。

   - SMPPTFIN および SMPHOLD（該当する場合）の DASD データ セット名
   - UNZIPJCL ジョブで使用した、RECEIVE コマンドの RFPREFIX パラメータの HLQ

4. 基本機能を APPLY します。
5. 基本機能を ACCEPT します。
6. メンテナンスを APPLY します。

SAMPJCL インストール用 SMP/E 環境の準備

この手順でのメンバは、SMP/E データ セットを準備し、ゾーンを初期化し、z/OS 用の CA Common Services 用の DDDEF を作成します。外部 DDDEF データ セットが必要です。

Agent Technology、Event Management、または CA Common Services に同梱される Tomcat のバージョンをインストールする場合は、製品インストールの一環として USS 階層ファイル システムを確立します。ユーザが CA MSMCommon Services をインストールしている場合、USS は製品の必要な機能です。

CA Common Services ソフトウェアのコンポーネントは 4 つの pax ファイルを使用してパッケージングされているので、すべてのコンポーネントを一度にインストールする方が、Common Services コンポーネントまたは pax ファイルごとにこの手順を繰り返すより楽な場合があります。

注: CA Common Services v14.0 Legacy Common Services の既存のインストール、または Mainframe CA NSM Common Services を再インストールする必要はありません。これらの 2 つの pax ファイルは変更されていないため、Legacy Common Services または Mainframe CA NSM Common Services に対して確立した CA Common Services v14.0 SMP 環境を継続して使用できます。

BASE pax ファイルには、CA Common Services コンポーネントをすべてインストールするために SAMPJCL データ セットが含まれます。複数インストールの実行を選択した場合は、各インストールについて BASE SAMPJCL データ セットのコピーを作成してから、メンバを編集します。

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。

Base および Optional CA Common Services コンポーネントをすべて同じ SMP/E CSI にインストールします。

BASE pax ファイル内にある CA Common Services コンポーネントをすべてインストールします。

製品用に SMP/E 環境を準備する方法

1. BASE pax ファイルから解凍された SAMPJCL データ セット内にある、ISPF Edit マクロの AW0SEDIT をユーザのサイト固有の情報でカスタマイズし、SYSPROC の場所にコピーします。

   メンバ AW0SEDIT をカスタマイズするには、各 ISREDIT CHANGE マクロ コマンドの右端にあるパラメータをユーザ サイト固有の情報に置換します。

   インストール メンバを編集するたびに、TSO コマンド ラインに「AW0SEDIT」と入力し、Enter キーを押して、デフォルトを指定した値で置き換えます。

   マクロが SAMPJCL メンバをカスタマイズする準備ができました。

   重要: Base および Optional CA Common Services コンポーネントをすべて同じ CSI およびゾーンにインストールします。各 CA Common Services コンポーネントまたは pax ファイルを複数インストールすることにした場合、GLOBALHLQ および CAIT0HLQ の値に対する "変更" は各インストールで同じである必要があります。

   注: pax ファイル用の UNZIPJCL ファイル内の *yourHLQ* として指定したのと同じ値に CAI を置換することにより、DASDHLQ 用の SREDIT Change コマンドを更新します。この値は SMP/E RECEIVE 処理内に使用されます。

   CA Common Services コンポーネントを、各 UNZIPJCL pax ファイル内の *yourHLQ* に対する値が異なる複数の pax ファイルからインストールする場合、各 *yourHLQ* について SMP/E RECEIVE を実行します。

   ```
   ISREDIT CHANGE ALL DASDHLQ     CAI
   ```

   を以下に変更します。

   ```
   ISREDIT CHANGE ALL DASDHLQ     yourHLQ
   ```

   以下の手順には、新しい SAMPJCL メンバを開くたびに AW0SEDIT 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、AW0EDALL 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 AW01ALL を開き、コマンド ラインから AW0SEDIT マクロを実行します。

3. AW01ALL をサブミットします。

   そのジョブにより、以下のような結果になります。

   - BASE および OPTIONAL の CA Common Services コンポーネント用のターゲットおよび配布のデータ 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. インストールするコンポーネントが含まれる各 pax ファイルに対して、以下の副手順を完了します。

   xxx は以下の 3 文字のコードを表します。

   CCS - LEGACY コンポーネント

   NSM - MFNSM コンポーネント

   a. 編集セッションで SAMPJCL メンバ *xxx*1ALL を開き、コマンド ラインから AW0SEDIT マクロを実行します。

      xxx1ALL がカスタマイズされます。

   b. *xxx*1ALL をサブミットします。

   これらのジョブにより、以下の結果が生じます。

   - LEGACY および MFNSM の CA Common Services コンポーネント用のターゲットおよび配布のデータ セットが作成されます。

5. Agent Technology、Event Management、または CA Common Services に同梱された Tomcat のバージョンをインストールする場合は、インストールする各製品について以下の副手順を完了します。

   注: この手順の *ccc* はすべて、FMID を基にした、以下の 3 文字のコンポーネント コードを表します。

   B6D - MFNSM - Agent Technology

   D5I - MFNSM - Event Management

   EG1 - OPTIONAL - Tomcat

   a. SAMPJCL メンバ *ccc*1ALLU を Edit セッションで開き、コマンド行から AW0SEDIT マクロを実行します。

      *ccc*1ALLU がカスタマイズされます。

   b. *ccc*1ALLU をサブミットします。

      このジョブにより、zFS データ セットが割り当てられます。

c. SAMPJCL メンバ *ccc*2MKD を Edit セッションで開き、コマンド行から AW0SEDIT マクロを実行します。

*ccc*2MKD がカスタマイズされます。

d. *ccc*2MKD 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。

6. CA Common Services コンポーネントをすべて同じ SMP/E CSI にインストールします。この JCL は、すべての CA Common Services コンポーネントのための CSI を作成します。編集セッションで SAMPJCL メンバ AW02CSI を開き、コマンド ラインから AW0SEDIT マクロを実行します。

AW02CSI がカスタマイズされます。

7. AW02CSI 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。
- 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。
- 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。
- 必須 SMP/E データ セットの DDDEF が作成されます。

8. インストールするコンポーネントが含まれる各 pax ファイルに対して、以下の副手順を完了します。*xxx* は以下の 3 文字コードを表します。
   - AW0 - BASE および OPTIONAL コンポーネント DDDEF
   - CCS - LEGACY コンポーネント DDDEF
   - NSM - MFNSM コンポーネント DDDEF

   a. 編集セッションで SAMPJCL メンバ *xxx*2CSID を開き、コマンド ラインから AW0SEDIT マクロを実行します。

      *xxx*2CSID がカスタマイズされます。

   b. *xxx*2CSID をサブミットします。

      これらのジョブにより、以下の結果が生じます。

      - Common Services コンポーネントのデータ セット用 DDDEF エントリが作成されます。

9. Agent Technology、Event Management、または CA Common Services に同梱された Tomcat のバージョンをインストールする場合は、インストールする各製品について以下の副手順を完了します。

   a. SAMPJCL メンバ *ccc*3CSIU を edit セッションで開き、コマンド行から AW0SEDIT マクロを実行します。

      *ccc*3CSIU がカスタマイズされます。

      注: このセクションの ccc はすべて、FMID に基づく 3 文字のコンポーネント コードを示します。

   b. *ccc*3CSIU をサブミットします。

      このジョブは、USS ターゲット パスに関連付けられた DDDEF を追加して、CSI をカスタマイズします。

Common Services モードで実行される CA Easytrieve r11.6

CCS r14.1 を CCS v14.0 と同じ SMP/E 環境にインストールできます。

CCS r14.1 と同じ SMP/E ターゲット ゾーンに CA Easytrieve r11.6 をインストールするには、CCS r14.1 をインストールし、CA Easytrieve r11.6 をインストールする前に、CAW0JCL データ セット ジョブ CAW0EZTD をカスタマイズし実行します。ジョブ CAW0EZTD は CCS r14.1/v14.0 の SMP 環境から CA Easytrieve Common Reporting Service r6.4 を削除します。その後、新しい CA Easytrieve バージョンをインストールできます。

注: CA Common Services for z/OS r14.1 でパッケージングされた CA Easytrieve の変更の詳細については、「*リリース ノート*」を参照してください。

SAMPJCL 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。

以下のメンバの各々には、CA Common Services と関連付けられたすべての FMID が含まれます。メンバのそれぞれにインストールしない FMID と関連付けられた任意の FMID または手順を削除します。

インストール ジョブを実行する方法

1. 編集セッションで SAMPJCL メンバ AW03RECD を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW03RECD がカスタマイズされます。

   各 pax ファイルの UNZIPJCL 内の *your*HLQ に別の値を指定した場合、使用した各 *your*HLQ のこの JCL をカスタマイズしてサブミットする必要があります。

2. SAMPJCL メンバ AW03RECD をサブミットして、SMP/E 基本機能を RECEIVE します。

   CA Common Services for z/OS は受信され、グローバル ゾーン内に存在するようになりました。

3. 編集セッションで SAMPJCL メンバ AW04APP を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW04APP がカスタマイズされます。

4. SAMPJCL メンバ AW04APP をサブミットして、SMP/E 基本機能を APPLY します。

   製品が 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 AW05ACC を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW05ACC がカスタマイズされます。

6. SAMPJCL メンバ AW05ACC をサブミットして、SMP/E 基本機能を ACCEPT します。

   製品が ACCEPT され、配布ライブラリに配置されます。

7. メンテナンスを APPLY します。

8. 製品を展開します。

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。インストール処理をすべて完了するまで、この手順を使用しないでください。

CA 製品の pax ファイルのダウンロードと処理を実行した後、今後のダウンロード用にファイル システムのディスク容量を空けるには、USS ディレクトリからファイルを消去し、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、および HOLDDATA MVS データ セット

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

注: 今後の参照用に、*yourhlq*.INSTALL.NOTES などの 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。

pax ファイルおよび製品固有ディレクトリを削除する方法

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 製品の 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: また、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、それらを削除できます。

メンテナンスの APPLY

メンテナンスを実行する前に、メンテナンスで考慮する必要のある事項がないか、コンポーネント設定に関する章を確認します。

CA Support Online には、インストール データの作成後に発行されたメンテナンスおよび HOLDDATA が存在する場合があります。CA Support Online 上にあるメンテナンスに加えて、SAMPJCL メンバ、AW03RECD と関連付けられたインストール手順中にユーザの SMP/E 環境へすでに RECEIVE されていたメンテナンスがある場合があります。

メンテナンスを APPLY する方法

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。また、インストール処理中に RECEIVED されたが APPLIED または ACCEPTED されなかったメンテナンス用インストール処理中に作成された SMP/E データ セット SMPPTS を参照します。
2. CA Support Online で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 SAMPJCL メンテナンス メンバからアクセス可能になります。
3. AW0SEDIT 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 AW06RECP を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW06RECP 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、AW06RECP SMPPTFIN および SMPHOLD DD ステートメントをカスタマイズします。
6. AW06RECP 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 AW07APYP を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW07APYP がカスタマイズされます。
8. AW07APYP 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 AW08ACCP を開き、コマンド ラインから AW0SEDIT マクロを実行します。

   AW08ACCP がカスタマイズされます。
10. （オプション）AW08ACCP 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。

注: メンテナンスが入手可能かどうかを確認することをお勧めしますが、利用可能なメンテナンスが見つからない場合もあります。メンテナンスが入手可能ではない場合は、「製品のデプロイ」に移動してください。

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、特別な状態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 HOLDDATA の例を以下に示します。

ACTION

この SYSMOD を APPLY する前後に、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 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 Support Online から DASD ファイルに外部 HOLDDATA データをダウンロードし、SMPHOLD DD ステートメントにファイルを割り当てます。外部 HOLDDATA データを処理するには、ユーザの 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 を適用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決定しました。これらの SYSMOD を APPLY することをお勧めします。

外部 HOLDDATA データを確実に管理するには、SMP/E で自動的に管理することを許可してください。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。RECEIVE ステータスにある SYSMOD を解決する場合、SMP/E は状況を修正するために APPLY する SYSMOD を特定します。

CA Common Services 固有のインストール後の要件

Agent Technology および Event Management のインストールを実行後、「Agent Technology と Event Management のインストール後の作業 (P. 85)」セクションに述べられているタスクを実行します。Agent Technology と Event Management のインストール後の作業は展開する前に実行される必要があります。

製品の展開

SMP/E インストール プロセスの間に作成された SMP/E ターゲット データ セットを、CA Common Services のコンポーネントを実行するターゲット システム上で (少なくとも 一度) 利用可能なコピーを作成してすべて展開する必要があります。

コンポーネントを複数システム上で実行する場合、最小限、ターゲットのシステム上の共有された DASD によってそのコピーを利用可能にする必要があります。ただし、設定目的で SMP/E ターゲット データ セットのすべて、または部分的なコピーを複数作成したほうがいい場合もあります。

ほとんどの CA Common Services の SMP/E ターゲット データ セットは、文字 C で始まり、3 文字の pax ファイル識別子 AW0、CCS、または NSM が続く最も低レベルの修飾子で識別できます。SMP/E ターゲット データ セットの完全なリストについては、ストレージ要件に関する章を確認してください。

重要: SMP/E ターゲット データ セットを展開する前に、展開しようとしている製品の要件をターゲット システムが満たしていることを確認します。

Agent Technology、Event Management 、または CA Common Services に同梱された Tomcat のバージョンをインストールした場合、USS zfs データ セットの展開に関するこの章のセクションを参照してください。

SMP/E ターゲット データ セットを展開した後に、「製品の設定」の章に移動します。

USS ファイル システムの展開

USS を使用する製品を展開させる方法

- SMP/E CSI およびその SMP/E ターゲット USS 環境を使用して、ソフトウェアの変更のみを追跡します。
- Agent Technology および Event Management については、インストール後の手順を実行してからでないと SMP/E ターゲット データ セットを展開できません。

  Event Management については、Event Management インストール ディレクトリ（デフォルトでは/cai/nsmem）にある設定スクリプト fwsetup を実行する必要もあります。詳細については、「Event Management 設定スクリプトの実行」を参照してください。
- インストールされている場所または他のマシンで USS zfs データ セットのコピーを作成します。このコピーは、実行する CA Common Services コンポーネントで使用されます。

  ユーザの USS zFS データ セットをコピーするには、以下の手順に従います。この手順では、USS を使用する CA Common Services コンポーネントが正常にインストールされ、インストール z/OS イメージ上でポスト インストール処理が完了したと想定しています。

  1. CA Common Services BASE ロード ライブラリ（CAW0LINK、CAW0LOAD、CAW0LPA および CAW0PLD）のコピーをターゲット システム上で利用可能にします。

     Agent Technology または Event Management を展開している場合、MFNSM ロード ライブラリ（CNSMLOAD および CNSMPLD）、および CNSMJCL、CNSMOPTV および CNSMPROC も同様に利用可能である必要があります。

2. SMP/E USS z/FS データ セットのバックアップ コピーを作成します。USS z/FS データ セットはリニアな VSAM です。IDCAMS REPRO を使用してデータセットをバックアップします。

   バックアップを作成する前に、以下の手順に従います。

   - バックアップされている USS ファイル システムを使用している CA Common Services コンポーネントがないことを確認します。
   - Agent Technology については、インストール後のタスクがすべて完了したことを確認します。
   - Event Management については、インストール後のタスクがすべて完了し、設定スクリプト fwsetup が実行されていることを確認します。

3. ターゲット システム上の SAMPJCL メンバをカスタマイズしてサブミットし、zFS データ セットを割り当ててフォーマットします。

   - Agent Technology には、B6D1ALLU を使用します。

     グループ AWGROUP がこれまでユーザのシステム上で定義されていない場合は、以下の手順を実行します。

     (a) SAMPJCL メンバ B6D1ALLU を更新し、zFS ファイルの形式に -group AWGROUP が含まれないようにします。この更新は RO および RW zFS ファイルの両方に必要です。

     ```
     //FMTRW  EXEC PGM=IOEAGFMT,REGION=0M,
     // PARM=('-aggregate &CAI..RW.CB6DZFS -group AWGROUP -compat')
     ```

     を以下に変更します。

     ```
     //FMTRW  EXEC PGM=IOEAGFMT,REGION=0M,
     // PARM=('-aggregate &CAI..RW.CB6DZFS -compat')
     ```

     (b) ジョブ B6D1ALLU が正常に完了した後に、CNSMJCL ジョブ B6DI0065 を実行して、Agent Technology のグループ所有者権限および userID モードを設定します。

   - Event Management には D5I1ALLU を使用します。
   - Tomcat には EG11ALLU を使用します。

4. ターゲット システム上で SAMPJCL メンバをカスタマイズ、サブミットしてマウント ポイントを作成し、READ/WRITE モードの前の手順で作成された zFS データ セットをマウントします。

   READ/WRITE モードでマウントするのは設定を実行するためです。

   ターゲット システム上でマウント ポイント ディレクトリのみを作成します。

追加のディレクトリを作成するあらゆる手順を削除します。

- Agent Technology には B6D2MKD を使用します。
- Event Management には D5I2MKD を使用します。
- Tomcat には EG12MKD を使用します。

5. 手順 2 で作成したバックアップを、ターゲット システム上の新しく割り当てられた zFS データ セットの中にリストアします。
6. 新しい zFS データ セット用の MOUNT ディレクトリを備えたターゲット システム上で BPXPRMxx メンバを更新します。
   - DSName で読み取り専用として RO を指定して、zFS データ セットをマウントします。
   - DSName で読み取り/書き込みとして RW を指定して、zFS データ セットをマウントします。

複数システムへの Agent Technology の展開

Agent Technology を複数のシステムにインストールする場合、以下の 2 通りの方法があります。

- それぞれのシステムにインストールします。こうすると、各システムを独立して管理できるよう別々の CSI が提供されます。
- 既存の CSI を使用してソフトウェアを追跡するものとし、他のマシンには単にコピーをインストールします。

2 つ目のオプションを採用する場合は、SAMPJCL ジョブ B6D1ALLU および B6D2MKD により作成、フォーマット、マウントされた Agent Technology の読み取り専用 zFS を使用します。この読み取り専用 zFS は、すべての実行可能プログラムを格納していて、複数のシステムで共有することができます。このように、Agent Technology サービスを実行するには、読み取り/書き込み zFS2（比較的サイズの小さい）を 2 番目以降のシステムにコピーするだけです。この zFS 構造には製品のメンテナンス手順を単純化する効果もあります。ほぼすべての更新は共有された読み取り専用 zFS に適用するだけで済みます。

Agent Technology インストールのコピー

Agent Technology サービスのインストールを 2 つ目の z/OS イメージにコピーするには、以下の手順に従います。この手順は、すでに少なくとも 1 つの z/OS イメージ上で Agent Technology サービスのインストールとテストが正常に完了していることを前提としています。

Agent Technology のインストールをコピーする方法

1. ターゲット システムが z/OS Agent Technology の最小システム要件を満たしていることを確認します。
2. 既存の Agent Technology zFS のバックアップをソース LPAR に作成します。このバックアップは、aws_sadmin 保管ファイルが適切に初期化されてエージェント MIB がロードされた後、Agent Technology サービスが停止しているときに作成する必要があります。zFS ファイルは VSAM 線形データセットです。IDCAMS REPRO を使用してデータセットをバックアップします。
3. 共用 DASD を使用するか、ファイルをコピーすることにより、ターゲット システム上で Agent Technology の CNSMLOAD、CNSMJCL、CNSMOPTV、および MIBLIB の各区分データセットにアクセスできるようにします。
4. 必要に応じてターゲット システム上で CNSMJCL（B6DI0015）をカスタマイズおよびサブミットし、セキュリティ システムに対するユーザ ID AWADMIN およびグループ AWGROUP を定義します。
5. SAMPJCL（B6D1ALLU）をカスタマイズしてサブミットし、ターゲット システム上で読み取り/書き込み zFS のみを割り当ててフォーマットします。読み取り専用 zFS を割り当ててフォーマットした手順を必ず削除してください（ジョブの手順 DEFINRO および FMTRO）。
6. ターゲット LPAR 上で新しく割り当てた読み取り/書き込み zFS に対し、手順 2 で作成した読み取り/書き込み zFS のバックアップ ファイルをリストアします。
7. SAMPJCL（B6D2MKD）をカスタマイズしてサブミットし、zFS ファイルのマウントポイントを作成して、作成してフォーマットしたばかりの RW zFS をマウントします。RO zFS をマウントする手順を削除します。
8. 初期インストールで作成された読み取り専用 zFS を、ターゲット システムから読み取り専用モードでアクセスできるようにします。

9. ターゲット システム上の BPXPRMxx メンバを更新して、新規 zFS 用の MOUNT ディレクトリを追加します。
10. ターゲット LPAR 上で以下の設定タスクを実行します。
    a. ルート Agent Technology ディレクトリにある agentworks.profile スクリプトを、新しい環境を反映するように変更します。

       注意を要する重要な環境変数を以下に示します。

       - AWORKS_MVS_PREFIX は、Agent Technology z/OS ファイルのプレフィクスを指定します。
       - AGENTWORKS_DIR は、Agent Technology のホーム ディレクトリを指定します。
       - RESOLVER_CONFIG は、TCPIP.DATA ファイル用の DSN を指定します。つまり、新規システム上で稼働する TCP スタックの SYSTCPD DD ステートメントで指定される DSN であることが必要です。データセットが PDS である場合は、メンバ名が含まれている必要があります。

    b. yourCNSMOPTV 内のメンバ ENVFILE を変更します。複数の z/OS イメージ間で CNSMOPTV を共用する場合は、新しいシステム用に新規の固有メンバを作成する必要がある場合があります。これは、新規 LPAR 用の ENVFILE メンバの内容を変更する必要がある場合のみです。このファイルを変更または作成する際には、Agent Technology のルート ディレクトリを指定する AGENTWORKS_DIR に特に注意してください。
    c. すべてのスクリプト、構成ファイル、および JCL メンバに、ターゲット LPAR に必要となる修正を行います。

       - スクリプト: agentworks.profile スクリプト(上述)への変更のほかに、install_mibs スクリプト($AGENTWORKS_DIR/services/tools ディレクトリに存在)についても、エージェントを組み込みまたは除外するように変更する必要がある場合があります。これにより、エージェントがターゲット システム上で稼働するかどうかが決まります。
       - 構成ファイル: 最も変更が必要となる可能性が高いのは aws_sadmin.cfg ファイルです。このファイルは、SNMP コミュニティ ストリングのほか、トラップが送信されるトラップ宛先を含んでおり、/cai/agent/services/config/aws_admin ディレクトリにあります。
       - JCL: JCL の変更が必要な場合(異なる ENVFILE を参照するためなど)、新規システム用に固有の JCL コピーを作成する必要があります。

d. 読み取り/書き込み zFS を新しいシステム イメージにコピーし、リストアするプロセスによって、aws_sadmin 保管ファイルもコピーされます。ただし、すべてのターゲット システムでこれが該当するとは限りません。この保管ファイルがコピーされるのは、エージェントのリリースがすべてのシステムで共通している場合だけです。異なるリリースを実行している場合は、「*aws_sadmin 保管ファイルの作成*」という題名の前のセクションにあるプロシージャを実行する必要があります。

e. agentworks.profile スクリプトの起動後、UNIX System Services 内で awftest tcpip ユーティリティを実行します。このユーティリティは、TCPIP スタックが適切に構成されたかどうかを検査するものです。このユーティリティがエラーなく実行されるまで、Agent Technology サービスは開始しないでください。

11. ターゲット LPAR 上で Agent Technology サービスを開始します。

複数システムへの Event Management の展開

追加のシステム上への Event Management 展開については、「追加システムへの Event Management の展開 (P. 221)」を参照してください。

第 5 章: 製品の設定

このセクションには、以下のトピックが含まれています。

CA MSM で CA Common Services を設定する方法

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、インストールおよび展開した CA Common Services のこのリリースを設定できます。

次の手順に従ってください:

1. [Deployments]タブで設定する展開済み製品を選択して、Create Configuration ウィザードを開きます。
2. 以下のような Create Configuration ウィザードの各手順を実行するなどして、設定を作成します。
   a. 設定名を定義し、ターゲット システムを選択します。
   b. 設定機能および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. リソースを選択し編集します。

3. 設定を作成します。Create Configuration ウィザードの最後の手順で、設定を構築できます。
4. 設定を行います。CA MSM の実行プロセスでは、手順を 1 つずつ、実行する内容について丁寧に説明しながら作業を進めて、実行ロセスを開始、停止、管理する詳細な手順を指示します。

設定プロセスの完了後、CA Common Services は利用可能になります。

重要: MSM の部分では、CA Common Services がインストールされる必要があります。ターゲット システム上で MSM がアクティブである間は、新規に設定された CAIRIM、CAIENF および CCI アドレス空間を開始しないでください。

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。

第 6 章: CA MSM なしで CA Common Services を設定する方法

この章では、ご使用の環境で CA Common Services for z/OS を起動し、カスタマイズし、使用する前に必要な最小限の設定タスクを説明します。

展開されたデータ セットを使用して、CA Common Services コンポーネントを設定する必要があります。

設定手順

データ セットの APF 許可および LINK リストおよび LPA へのデータ セットの追加に関する詳細については、IBM の「*z/OS MVS 初期設定およびチューニング解説書*」を参照してください。

CA Common Services for z/OS 起動前にシステムを設定する方法

1. APF 許可データ セット
   a. サイトで APFlist を指定するために SYS1.PARMLIB メンバ IEAAPFxx または PROGxx のどちらを使用しているか確認します。
   b. サイトで使用している SYS1.PARMLIB APF リスト メンバに適用される以下のデータ セットを追加します。
      - *YourdeployHLQ*.CAW0LOAD - BASE コンポーネント インストール
      - *YourdeployHLQ*.CCCSLOAD - LEGACY コンポーネント インストール
      - *YourdeployHLQ*.CNSMLOAD - MFNSM コンポーネント インストール
      - *YourdeployHLQ*.CNSMPLD - MFNSM コンポーネント インストール

- *YourdeployHLQ*.CAW0DCM - BASE コンポーネント インストール - CAIENF
- *YourdeployHLQ*.CAW0LINK - BASE コンポーネント インストール
- *YourdeployHLQ*.CCCSLINK - LEGACY コンポーネント インストール
- *YourdeployHLQ*.CAW0PLD - BASE コンポーネント インストール

重要: これらのデータ セットの APF 許可に失敗すると、設定プロセスで後のジョブが正常に完了しなかったり、アドレス空間の起動に失敗したりします。

2. LINK LIST データセット

   a. サイトで LNKLST 連結を指定するために SYS1.PARMLIB メンバ LNKLSTxx または PROGxx のどちらを使用しているか確認します。

   b. サイトで使用している SYS1.PARMLIB LINK リスト メンバに適用される以下のデータ セットを追加します。

   - *YourdeployHLQ*.CAW0LINK - BASE コンポーネント インストール
   - *YourdeployHLQ*.CAW0PLD - BASE コンポーネント インストール
   - *YourdeployHLQ*.CCCSLINK - LEGACY コンポーネント インストール
   - *YourdeployHLQ*.CNSMLOAD – MFNSM コンポーネント インストール

   c. オプションで、ユーザのサイトで使用している SYS1.PARMLIB LINK リスト メンバに適用される以下のデータ セットを追加して、CA 製品および Common Services 関連 JCL に対して STEPLIB を使用する代わりに、システム リンクリストを使用します。

   - *YourdeployHLQ*.CAW0LOAD - BASE コンポーネント インストール
   - *YourdeployHLQ*.CCCSLOAD - LEGACY コンポーネント インストール

3. LPA ライブラリリストへの CAW0LPA の追加
   - ユーザの SYS1.PARMLIB LPALSTxx メンバへのデータ セット YourdeployHLQ.CAW0LPA の追加
4. コンポーネント設定手順の実行。CA Common Services コンポーネント用の特定のタスクを実行するには、以下の設定関連の章を参照してください。
   - CAIRIM 設定タスク
   - CAIENF 設定タスク
   - CAICCI 設定タスク
   - Event Management 設定タスク
   - Agent Technology 設定タスク
   - CA グローバル サブシステム設定タスク
   - CA-L-Serv 設定タスク
   - 他の設定タスク
5. すべてのマテリアルと出力を保存する

   この手順は、メンテナンスおよびアップグレードを行うために、情報を利用可能にする上で重要です。
6. CA Datacom/AD のインストールの実行
   - CA Common Services のこのリリースで出荷される CA Datacom/AD のバージョンを以前にインストールしている場合は、CA Datacom/AD を再度インストールする必要はありません。ただし、その場合でも CAIENF および(または)Event Management 用に CA Datacom/AD をカスタマイズする必要があることがあります。「CA Datacom/AD のインストール」の章を参照してください。

     CAIENF および Event Management では CA Datacom/AD をインストールするかどうかは任意ですが、特定の CAIENF および Event Management のオプションでは CA Datacom/AD データベースを使用する必要があります。

     CAIENF では、イベントの記録に CA Datacom/AD が必要です。

ユーザのサイトでイベントを記録するかどうか分からない場合、RECORD(YES) が CAIENF パラメータ ファイルで指定されているかどうかで確認できます。r12 より前の CAIENF リリースを実行している場合、CAIENF データベースを確認して、いずれかのイベント タイプに 1 以上のレコード カウントがあるかどうかで確認できます。CAIENF r12 より前のデータベースを確認するには、CAS9DB LIST DETAIL レポートを使用します。r12 より前の CAIENF リリースが稼働している場合、以下の CAS9DB JCL を使用できます。

```
//CAS9DB   EXEC PGM=CAS9DB,REGION=4M
//STEPLIB  DD DISP=SHR,DSN=yourHLQ.CAW0LOAD <=Update
//DBOUT DD SYSOUT=*
//DBIN     DD *
  LIST DB(*) DETAIL
/*
```

- Event Management では、Calendars オプションまたは Message Actions オプションに CA Datacom/AD が必要です。Calendars または Message Actions を使用する場合、Event Management zFS インストール ディレクトリにある PROFILE ファイルで、環境変数 CA_OPR_ZOSDB を Y に設定します。この変数は、CNSMJCL メンバ D5II0050 に関連付けられている Event Management 設定手順で既に設定されているはずです。そうでない場合、Event Management を起動する前に、いつでも環境変数を設定できます。
- CA Datacom/AD には CA Common Services が必要であるため、CA Datacom/AD をインストールする前に、CA Common Services コンポーネントに対する CA Common Services の設定手順を完了する必要があります。

  CA Datacom/AD には以下の CA Common Services コンポーネントが必要です。

  - CA C-RUNTIME
  - CAICCI
  - CA LMP と CAISSF を含む CAIRIM
- CA Common Services インストールで配布された CA Datacom/AD のバージョンを使用し、CA Datacom/AD のインストール」の章の手順に従います。

  注: CA Datacom/AD のインストールについては、「*CA Datacom/AD for z/OS r12 Installation and Maintenance Guide*」を参照してください。

第 7 章: CAIRIM の設定

CA Common Services for z/OS のインストール後、CAIRIM 用の設定タスクには、初期化パラメータの変更、RACF 製品向けの CAISSF のカスタマイズ、および CAIRIM の起動などがあります。これらのタスクを実行するとき、展開されたデータ セットを使用します。

このセクションには、以下のトピックが含まれています。

CAIRIM 初期化パラメータ

場合によっては、CAIRIM の初期化パラメータを変更する必要があります。このタスクは、CAIRIM をインストールして、CAS9 プロシージャの実行を予定している場合に必要です。他のサービスのために CAIRIM をインストールしていて、CAIRIM の実行を予定していない場合は、このタスクを実行する必要はありません。

CAIRIM によって初期化される各ソリューションは、CAIRIM parmlib メンバ (*Yourdeploy*HLQ.CAW0OPTN にあります) 内のエントリを通じて定義されます (サンプル プロシージャでは、メンバ CARIMPRM と説明されています)。ご使用のソリューションのインストール マニュアルには、インストールするソリューションやサービス用の CAIRIM パラメータ定義 (CA のソリューションで必要な場合) が記載されています。ステートメントの順序に関する要件があれば、CA ソリューションと共に提供される手順に含まれています。

CAIRIM を使用して実行され得るすべての弊社ソフトウェア ソリューションは、次の 2 つの汎用ルールに従います。

- **ルール 1:** サービスは製品より先に初期化される必要があります。 たとえば、CA Scheduler が ADAPTER と OMS を使用する場合、ADAPTER と OMS の初期化ステートメントを CA Scheduler の初期化ステートメントの前に配置する必要があります。
- **ルール 2:** 以前にインストール済みの弊社ソリューションに、以降のソリューションでも使用する 1 つ以上のサービスがすでに組み込まれている場合、既存のステートメントが使用され、そのサービスについては新たなステートメントは追加されません。

次の初期化ステートメントのパラメータ構造は、すべてのソフトウェア ソリューションおよびサービス定義において共通に使用されます。

```
PRODUCT(desc) VERSION(vers) LOADLIB(dsn) INIT(name) PARM(parm)
```

重要: CAIRIM 制御文は 72 カラム目を越えて指定できません。**注**: 制御ステートメントは、行の末尾にダッシュ「-」を付けて次の行に続けることができますが、かっこ内のキーワードとそのオペランドは同じ行にある必要があります。

例

```
PRODUCT(desc) VERSION(vers) LOADLIB(dsn)  -
INIT(name) PARM(parm)
```

以下の表は、パラメータとその説明のリストです。

パラメータ	必須	説明
desc	必須	ソリューションまたはサービス記述（最大 20 文字）。このパラメータは、インストールされる各製品に対して 1 回ずつ指定されます。
vers	必須	4 文字の識別子（2 文字のソリューションまたはサービス コードと 2 文字のバージョン コードから構成される）。
dsn	オプション	ソリューションまたはサービス ロード モジュールに対するデータセット名。モジュールが LINKLIST または CAIRIM プロシージャ STEPLIB にある場合、LOADLIB パラメータを指定する必要はありません。

パラメータ	必須	説明
name	オプション	初期化ルーチンの名前。デフォルトでは初期化モジュールの名前は、バージョン情報と「INIT」を合わせたものです。したがって、ソリューション KO42 の場合は、初期化モジュールは KO42INIT となります。INIT パラメータは、デフォルトのモジュール名が不適切な場合にのみ指定します。
parm	オプション	初期化ルーチンに渡される特殊なパラメータ。このパラメータは、再初期化または無効化のような任意のカスタム ソリューション機能に使用されます。PARM フィールドでは最大 32 文字を渡すことができます。

注: LOADLIB パラメータは、指定されたインストール プログラムのタスク ライブラリをそのデータセットに切り替えるものであり、APF 許可を必要とします。したがって、LOADLIB が使用される場合、INIT プログラムおよび関連する CAIRIM プログラム モジュールは、LINKLIST または LOADLIB ステートメントで記述されたライブラリのいずれかにある必要があります。INIT プログラムおよび関連する CAIRIM プログラム モジュールが CAIRIM STEPLIB にしかない場合、異常終了 S806 が発生することになります。

RACF または RACF 互換製品用の CAISSF のカスタマイズ

このタスクが必要になるのは、CAISSF と RACF の併用を計画している場合です。CA Top Secret または CA ACF2 を使用する場合は、このタスクをスキップすることができます。

RACF 用の CAISSF のカスタマイズには、以下のようなアクティビティがあります。

- CICS TS 用に CAS9SAFC を変更する
- CAS9RACL のインストール
- RACF の変更
- 共通サービス エリア（CSA）への CAISSF ルーチンの配置
- CAISSF インストール プロセス

重要: CAS9SAFC は変更できますが、Common Services で配布されたコードを変更なしに実行することを強くお勧めします。CAS9SAFC を変更するのは、そのプログラムの実際のロジックへ過去に変更が行なわれているというような稀な場合です。その場合は、サンプル モジュール内の RACF クラス名テーブルを更新して、CAIRIM での制御文の使用に加えて、インストール要件に一致するようにします。

CAISSF は、セキュリティ コールがどのように処理されるか識別するために RACF Class テーブルを必要とします。デフォルトのテーブルは作成されますが、一部の CA 製品では追加のエントリが必要です。これらのエントリの詳細は、関連製品のドキュメントに記載されています。これが CAS9 プロシージャにある場合、CAIRACF DD ステートメントにはこのテーブル用の制御文が含まれます。追加の RACF Class テーブル エントリを指定するには、メンバ RACFLIST をポイントする、CAS9 プロシージャ内の CAIRACF DD ステートメントのコメントを外します。最初、RACFLIST メンバは存在しません。RACFLIST メンバを作成し、それを更新して、RACFCLASS 制御ステートメントを含めます。

Standard Security Facility (CAISSF) は、CAIRIM サービスのサブサービスの 1 つです。このタスクの完了後、RACF 用の CAISSF がインストールされ、各 CA ソリューションで利用できるようになります。

RACF および CAS9SAFC のセキュリティ インターフェースは、オブジェクト形式とソース形式の両方で提供されます。CAS9SAFC 用のソースは、CA Common Source ライブラリの *Yourdeploy*HLQ.CAW0SAMP にあります。

注: CA ACF2 および CA Top Secret のセキュリティ変換プログラムである CAS9ACF2 と CAS9TS42 はそれぞれ、それらの CA ソリューションのインストール メディアで提供されます。そのため、これらのセキュリティ変換プログラムのサポートが必要な場合は、該当する CA ソリューションのサポート部門にご連絡いただく必要があります。オンライン テクニカル サポート、サポート部門の所在地、営業時間および電話番号については、CA サポートにお問い合わせください。

CICS TS 用に CAS9SAFC を変更する

CAISSF のインストール対象となる製品で RESOURCE ACCESS プロセスが必要ない場合は、このタスクを省略することができます。

CICS には以下の変更が必要です。

CAS9RACL PLT アプリケーションは、RESOURCE ACCESS 機能を使用する製品に必要です。PLT プログラム、CAS9RACL は RACFCLASS 初期化パラメータによって作成されるテーブル内にあるすべてのクラス名について RACLIST を実行します。CAS9SAFC 変換プログラムは RESOURCE ACCESS チェックを(RACF マクロ FRACHECK を使用して)行うために実行されますが、CICS は無許可で実行されるため、ストレージ内に関連するクラス名プロファイルを作成する RACLIST を実行することはできません。RESOURCE ACCESS 処理に必要なクラス名について RACLIST を実行するには、RACF 許可呼び出し元テーブルを使用して、CAS9LRAC、CAS9RACL、および DFHSIP プログラムを RACF に定義する必要があります。

注: CAS9RACL によって RACLIST が実行されたクラス名プロファイルに変更が加えられた場合、CICS リージョンをリサイクルする必要があります。

CAS9RACL のインストール

CAS9RACL をインストールする方法

1. RACF 許可呼び出し元テーブル ICHAUTAB に、プログラム DFHSIP、CAS9LRAC、および CAS9RACL を RACLIST 特権のみについて追加します。
2. CAS9LRAC プログラムを、次のエントリを使用して現行のスタートアップ用 CICS PLT に定義します。

   ```
   DFHPLT  TYPE=ENTRY,PROGRAM=CAS9LRAC
   ```

   PLT メンバに同一のエントリを追加して、CICS の起動時に RACLIST が実行されたすべてのクラスが、停止時に削除されるようにします。

   サンプルの PLT メンバの S910PLT および S910PLTS が、参照用として *Yourdeploy*HLQ.CAW0OPTN に用意されています。
3. 次のエントリを使用して、現行の CICS 用 PPT に CAS9LRAC プログラムを定義します。

   ```
   DFHPPT  TYPE=ENTRY,PGMLANG=ASSEMBLER,PROGRAM=CAS9LRAC
   ```

   サンプルの PPT メンバ S910PPT が、参照用として *Yourdeploy*HLQ.CAW0OPTN に用意されています。
4. DFHRPL を通じて CAS9LRAC プログラムをアクセス可能にし、CICS ジョブの STEPLIB または LNKLSTxx を通じて CAS9RACL プログラムをアクセス可能にします。

   CAS9RACL がインストールされました。

RACF の変更

CAISSF のインストール対象となる製品は、RACF および RACF 互換製品にインストールする必要のある製品固有のクラス名を持ちます。必要なクラス名の詳細については、ご使用の製品のマニュアルを参照してください。製品のクラス名は、RACF クラス記述子テーブル ICHRRCDE と、RACF SAF ルータ テーブル ICHRFRTB に追加する必要があります。

以下の例は、コーディングする必要があるものを示しています。これらの例ではクラス名 CACMD を使用しています。これらは単なる例です。CAISSF を使用する製品にはクラス名が必要でない場合もあります。

注: 制御ステートメントは、継続する行の最後にダッシュ(-)を付けると次の行に続けることができます。

例 1: CACMD に対するクラス記述子テーブル エントリ

```
CACMD    ICHERCDE   CLASS=CA@MD,          -
                   {GROUP=DFTGRP,}        -
                    MAXLNTH=8,            -
                    FIRST=ALPHANUM,     -
                    OTHER=ANY,          -
                    OPER=NO,          -
                    DFTUACC=NONE,       -
                    ID=CLASS_NUMBER,        -
                    POSIT=19-255
```

例 2: CACMD に対する SAF ルータ テーブル エントリ

```
CACMD    ICHRFRTB   CLASS=CA@MD,  -
                    ACTION=RACF
```

共通サービス エリア(CSA)への CAISSF ルーチンの配置

必要な場合は、CAISSF ルーチン(CAS9SEC)およびセキュリティ変換プログラム(RACF の場合は CAS9SAFC、CA Top Secret の場合は CAS9TS42)をオプションで CSA に配置することができます。

注: CA ACF2 では、インストール時のデフォルトで、変換プログラム CAS9ACF2 を PLPA に常駐させる必要があります。したがって、外部セキュリティはこのルーチンをロードしません。

CAISSF ルーチンを CSA に配置すると、次のような利点があります。

- 最新バージョンの CAISSF ルーチンがロードされ、実行される。
- 1 セットの CAISSF ルーチンを、CAISSF を必要とする CA ソリューションのすべてのアドレス空間にわたって使用できる。
- 保守が適用された場合に、CAIRIM の実行を通じて CAISSF ルーチンを再初期化できる。
- CAIRIM の実行を通じて CAISSF ルーチンを削除できる(必要な場合)。

CAISSF インストール プロセス

CAISSF ルーチンをインストールしているとき、システムによって以下のアクションが実行されます。

- CAISSF ルーチンの CSA へのインストールは、CAIRIM(CAS9 プロシージャ)の実行を通じて行います。CAIRIM 初期化ルーチン CAS9INIT は、CAISSF ルーチンを CSA にロードします。
- CAS9 プロシージャを実行する前に、次の CAIRIM 入力初期化制御ステートメントを *Yourdeploy*HLQ.CAW0OPTN データセットのメンバ CARIMPRM に追加します。

```
PRODUCT(CAIRIM) VERSION(CAS9) INIT(CAS9INIT)
```

- その後、CAS9 プロシージャの開始時に、CAIRIM は CAISSF 初期化ルーチンをアタッチします。CAISSF ルーチンが CAS9 STEPLIB またはリンクリスト データセットに存在する場合は、次にこの初期化ルーチンがそれらを CSA にロードします。

  注: CAISSF ルーチンの CSA へのオプション インストールを使用しない場合は、CAISSF の最初の APF 許可呼び出し元が、無条件に CAISSF ルーチンを CSA にロードすることになります。CAS9 プロシージャ(CAIRIM)を使用して CAISSF ルーチンをインストールしない場合は、CAISSF ルーチンの削除またはリフレッシュの機能は使用できません。CAISSF ルーチンの CSA へのオプショナル配置を使用しない場合は、CAS9 プロシージャ(CAIRIM)を実行する必要はありません。

LMP シート ライセンス登録セットアップ

CA 製品は LMP シート ライセンス登録共通サービスを使用して、以下を実行できます。

- 登録済み CA 製品同時ユーザを追跡し、レポートします
- CA 製品の同時ユーザの数を制限します
- LMP ライセンス キーを使用して CA 製品を有効にします

LMP シート ライセンス登録は、ライセンスされた各 CA 製品に対して LMP キーを使用する既存のライセンス管理共通サービスと共に使用されます。

IBM z/OS Product Registration コンポーネントは、指定された期間内の同時最大製品使用状況を記録しレポートするために使用されます。そのため、LMP シート ライセンス登録共通サービスは、ユーザのシステム上ですでにシート ライセンスの使用状況の検証に使用されている機能やプロシージャを使用できます。検証を必要とする CA 製品の同時最大シート ライセンス使用についてレポートすることは、比較的実行が容易なタスクです。

重要: SMF がタイプ 89 のレコードを記録していることを確認します

IBM 標準ユーティリティ プログラム IFAURP を使用して、CA 製品の同時最大ユーザ数を検証するレポートを作成します。IFAURP は、z/OS Product Registration コンポーネントによって作成された SMF タイプ 89 レコードを使用します。SMF タイプ 89 レコードが、Software Product Registration Report で IFAURP によってリストされている各 z/OS システムについて記録されていることを確認します。IFAURP の使用の詳細については、IBM から刊行されている「*z/OS MVS Product Management*」を参照してください。

レコードへのどの SMF レコードが論理 PARMLIB SMFPRMxx メンバで作成されるかの指定。IFAURP レポート ユーティリティは SMF タイプ 89、サブタイプ 2 レコードを入力として必要とします。SMFPRMxx メンバ内の SMF タイプ 89 を選択するか、または最低限、SMF タイプ 89、サブタイプ 2 レコードを選択します。SMF タイプ 89 レコードの記録の詳細については、IBM から刊行されている「*z/OS MVS System Management Facilities (SMF)*」を参照してください。

通常、インストールには後に取得およびレポートを行うために、SMF レコードの収集およびアーカイブに関する既存のプロシージャおよび方法があります。SMF タイプ 89、サブタイプ 2 レコードがインストールの管理対象 SMF 履歴データ セットにウィンドウ組まれていることを確認してください。これらのレコードは、少なくともソフトウェア製品登録レポートのレポート期間と同じ期間保存してください。

CAIRIM の起動

CAS9 プロシージャをスターティッド タスクとして起動する場合は、このプロシージャを *Yourdeploy*HLQ.CAW0PROC から有効なシステム プロシージャ ライブラリにコピーしておく必要があります。

重要: 現在実行している CAIRIM のバージョンが古い場合、新しいライブラリを使用して CAIRIM を開始する前に IPL が必要です。

重要: CAIRIM の起動時に CAIRIM と DATACOM がすでに実行されている場合、以下のようなエラー メッセージが表示される場合があります。

```
SVC NUMBER SELECTED IS ALREADY IN USE. SVC 254 IS AVAILABLE FOR USE.
```

結果は、「Datacom error: Init error: CA-DATACOM」となります。この問題は次のシステム IPL で解決されるため、次の IPL までこのエラーを無視しても構いません。

注: CAIRIM の起動については、「*Administration Guide*」を参照してください。

第 8 章: CAIENF の構成

CA Common Services for z/OS コンポーネントのインストール後、CAIENF 用の設定タスクには以下のものが含まれます。

注: これらのタスクを実行するとき、展開されたデータ セットを使用します。

- CAIENF プロシージャのカスタマイズ
- CAIENF の起動
- ENFSNMPM プロシージャのカスタマイズ
- CAIENF/USS の設定手順
- CAIENF 用の CA Datacom/AD のカスタマイズ

さらに、CAIENF を使用する他の CA Technologies 製品をお持ちの場合、DCM やコントロール オプションなど関連するセットアップ要件については、個々の製品のマニュアル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。

CAIENF プロシージャのカスタマイズ

このタスクは、CAIENF、CAIENF/CICS、CAIENF/DB2、CAIENF ユーティリティ、または CAICCI をインストールしている場合に必要です。

CAIENF プロシージャをカスタマイズする方法

1. CAIENF、CAIENF/CICS、および CAIENF/DB2 サービスの CAIENF プロシージャをカスタマイズします。

   CAIENF プロシージャは、*Yourdeploy*HLQ.CAW0PROC ライブラリにあります。各プロシージャは、スターティッド タスクとして、独自のアドレス空間で実行されます。

   CAW0PROC には、ENF、ENFXMUF、および ENFIMUF という 3 つの CAIENF プロシージャが組み込まれています。サイトの要件に合うプロシージャを選択します。

   ENF - イベントの記録や CA Datacom/AD のインストールを希望しない場合にこのプロシージャの JCL を使用します。

   ENFXMUF - イベントの記録が必要な場合にこのプロシージャの JCL を使用します。CA Datacom/AD はインストールされており、MUF は CAIENF 外部で（それ独自のアドレス空間で）実行されます。

   ENFIMUF - イベントの記録が必要な場合にこのプロシージャの JCL を使用します。CA Datacom/AD はインストールされており、MUF は CAIENF 内部で（CAIENF のアドレス空間で）実行されます。

2. 各プロシージャにアクセスし、ユーザ ソリューション標準に従って編集します。

シンボリック

以下は、CAIENF プロシージャに使用されているシンボリックを示しています。各シンボリックを必要に応じて変更してください。

シンボリック	説明	デフォルト
CAW0LOAD	CAIENF ロード ライブラリ	'CAI.CAW0LOAD'
CAW0DCM	CAIENF DCM ライブラリ	'CAI.CAW0DCM'
CAW0OPTN	CAIENF オプション ライブラリ	'CAI.CAW0OPTN'

シンボリック	説明	デフォルト
ENFPARM	CAIENF コントロール オプションを含んでいる OPTLIB データセットで定義されるメンバ	'ENFPARM'
ENFCMDS	自動コマンドを含んでいる OPTLIB データセットで定義されるメンバ	'ENFCMDS'
OUTC	SYSOUT クラス指定	'*'
optional	インストールされている CA ソリューションに依存。詳細については、ご使用の CA ソリューションのマニュアルを参照してください。	N/A
CCIPARM	CAICCI 初期化パラメータ メンバ	CCIPARM
SPNPARM	CAICCI Spawn 初期化パラメータ メンバ	SPNPARM
SYSTCPD	TCP/IP データ データ セット	'TCPIP.TCPIP.DATA'

CAW0LOAD、CAW0DCM、CAW0OPTN

展開されたデータ セットの高レベル修飾子によって、デフォルト値を更新します。

ENFPARM DD

イベント処理で必要な DCM と、CAIENF の起動中に処理される CAIENF コントロール オプションは、ENFPARM を使用して指定できます。 ENFPARM に加えて、オペレータの起動コマンドおよび EXEC JCL ステートメントから取得したパラメータが使用されます。ENFPARM DD ステートメントで、80 バイトの CAIENF コマンドを少なくとも 1 つ含んだファイルを指定する必要があります。

DCM ステートメントの構成の詳細については、「*Administration Guide*」を参照してください。

注: EXEC JCL ステートメントで入力されたコマンドまたは z/OS の起動コマンドは、パラメータ ファイルのエントリよりも優先されます。

ENFCMDS

CAIENF の初期化後に実行される z/OS オペレータ コマンドを指定する際に使用します。ENFCMDS でのコマンドの入力形式は、オペレータ コンソールの場合とまったく同じです。

ENFCMDS DD ステートメント

CAIENF が正常に初期化された後に実行される一連の z/OS オペレータ コマンドを含んだデータ セットを記述します。デフォルトのプロシージャでは、*Yourdeploy*HLQ.CAW0OPTN の ENFCMDS メンバを記述しています。

ENFCMDS ファイル

オペレータ コンソールから実行するときと同じ形式で、1 行につき 1 つの z/OS コマンドを記述します。このファイルでは、カラム 1 にアスタリスク (*) が指定されたすべての行がコメントと見なされます。

以下は、CA Scheduler を起動するための有効なコマンドの例です。

```
Col 1
    v
    *  Executes the CA Scheduler procedure
    START CASCHD
```

ENFCMDS ファイル内のコマンドは、CAIENF の初回起動時にのみ実行されます。CAIENF スターティッド タスクがなんらかの理由で再実行された場合、ENFCMDS ファイル内の自動コマンドは実行されません。

オプションの ENFDUMP DD ステートメントを記述することによって、ダンプ処理に対する CAIENF の動的割り当てを上書きできます。

通常、CAIENF コマンド DUMP を入力すると、その都度、SYSOUT データセットが SYSOUT コントロール オプションに従って動的に割り当てられます。必要に応じて ENFDUMP DD ステートメントを指定することにより、ダンプおよび他の診断データを強制的に DASD またはテープ データセットに記録させることが可能です。記述する場合、このデータセットは、133 の倍数となるブロック サイズと、FBA のレコード フォーマットで割り当てられている必要があります。

CAIENF パラメータ ファイルの設定

CAIENF パラメータにより、CAIENF がその機能を実行する方法のさまざまな点をカスタマイズし制御することを可能にします。これらのパラメータ設定には、システム上で実行する CA 製品の要件に基づいて実行する必要があるものもあります。CA 製品の CAIENF パラメータ要件については、特定の CA 製品ドキュメント内のソフトウェア要件セクションに説明があります。

CAIENF パラメータはそれぞれ「*CA Common Services for z/OS Reference Guide*」の「CAIENF」の章、「Control Options」のセクションに記述されています。

システム上で実行されている CA 製品のうちのいずれかが CAIENF イベント リカバリを実行した場合、これらの製品には CAIENF イベントのレコーディングが有効になる（RECORD（YES）パラメータ）手順があります。イベント レコーディングが有効である必要がある場合、CAIENF は CA Datacom/AD データベースで実行される必要があります。CAIENF で使用する CA Datacom/AD MUF およびデータベースの準備については、「CA Datacom/AD のインストール」の章を参照してください。イベント レコーディングが必要でない場合、CAIENF パラメータ NODB は設定できます。NODB は、CA Datacom/AD MUF との接続を確立しようとせずに開始するよう CAIENF に命じます。

リリース 12.0 の前に CA Common Services for z/OS リリースからアップグレードしている場合、ENFUTIL と呼ばれるツールを使用して、古い CAS9DB 機能（リリース 12.0 に先立つリリースで CAIENF 用に存在）を置換する CAIENF コントロール オプションを作成できます。ENFUTIL ユーティリティは、DCM および EVENT コントロール オプション ステートメントを作成するために、CAIENF リリース 12.0 から備わっています。このユーティリティでは、CA Common Services リリース 11 DB の詳細リスティングを入力として使用します。特別な DCM および EVENT のユーティリティの詳細については、「*Reference Guide*」を参照してください。

ENFUTIL 出力ファイルは CAIENF DCM および EVENT 制御オプション ステートメントのリストになります。このオプション ステートメントは、リリース 12.0 に先立つ CAIENF リリースで CAIENF データベースに格納されていた設定に一致します。これらのステートメントは、単に CAIENF パラメータ ファイルの後ろに置くだけです。

CA 製品 DCM 検索用 CAIENF JCL の設定

CAIENF 手順には DD 名//CAIDCM が含まれます。必要な CAIENF DCM ロード モジュールを含む CA Common Services および CA 製品ロード ライブラリの連結であるように、CAIDCM DD を設定する必要があります。連結内の最初のロード ライブラリは、常に CA Common Services for z/OS CAW0DCM ロード ライブラリである必要があります。

例

```
//CAIDCM   DD DISP=SHR,DSN=&CAW0DCM
//         DD DISP=SHR,DSN=ISLPROD.SCHEDULR.R11000.CAILOAD
//         DD DISP=SHR,DSN=SYSISL.CPM30.SP04A.CAIPDSE
//         DD DISP=SHR,DSN=BSTPROD.CA13.R1106.DISPATCH.LINKLIB
```

CA 製品 DCM 互換性

CAIENF DCM ロード モジュールを配布する CA 製品は、DCM が有効になるためには CAIENF コントロール オプション内で定義された DCM ステートメントが存在する必要があります。DCMs を使って次のようなことが可能になります。

- CAIENF へのイベントの定義
- CAIENF の初期化が完了した後、CAIENF が開始する必要のあるアプリケーションの定義
- イベントとアプリケーションの両方の定義

イベントを定義する DCM は CAIENF Release 12.0 以降と互換性がある必要があります。CAIENF リリース 12.0 以降の互換性に必要な CA 製品 PTF のリストについては、「*CA Common Services for z/OS Readme*」のセクション「Apply Necessary Fixes」を参照してください。CA 製品を提供するユーザの DCM が Readme リストに載っており、ユーザが Readme テーブルで示されたものより新しい製品リリースを実行している場合、ベース製品レベルでは互換性が組み込み済みです。

CAIENF の起動

CAIENF プロシージャがスターティッド タスクとして起動される場合は、有効なシステム プロシージャ ライブラリにこのプロシージャをコピーしておく必要があります。CAIENF スターティッド タスクに関連付けられる ID には、有効なセキュリティ OMVS セグメントが定義されている必要があります。

CAIENF には 3 つのサンプル プロシージャが 提供されています。その 3 つとは、ENF、ENFXMUF および ENFIMUF です。

ENF プロシージャに関連する JCL には、CA Datacom/AD データベース データセットへの参照が含まれておらず、CAIENF コントロール オプションである NODB と一緒に使用する必要があります。CAIENF の設定のこの時点では、CAIENF を開始するには ENF プロシージャのみ有効です。

残り 2 つのプロシージャである ENFXMUF と ENFIMUF は、CA Datacom/AD をインストールし、CAIENF 用に CA Datacom/AD を設定した後でのみ有効です。

このバージョンの CA Common Services と共に出荷された CA Datacom/AD のリリースを、以前のバージョンの CAIENF からインストール済みの場合、CAIENF プランのこのリリース バージョンを既存の CA Datacom/AD 環境にインポートする必要があります。「既存 CA Datacom/AD の CAIENF 向けカスタマイズ」の説明にしたがっていることを確認します。

重要: 実行している CAIENF のサービス レベルが低い場合、CAIENF を起動する前に、新しいライブラリを使って IPL を実行する必要があります。

コンポーネントのトレース機能の準備

デフォルトでは、CAIENF アドレス空間で、コンポーネント名 CAIENF を使用してコンポーネントトレース機能が初期化されます。環境は初期化されますが、MVS TRACE CT コマンドによってトレース機能は起動されている必要があります。

CAIENF Parm ENFCT は、コンポーネントトレース環境(コンポーネント名を含む)のアクティブ化とカスタマイズに使用されます。コンポーネントトレース機能 parmlib のメンバ名は、トレース機能をアクティブ化するために ENFCT コマンドで指定されます。parmlib メンバの構成方法については「*Reference Guide*」を参照してください。通常、CAIENF 用のコンポーネントトレースを有効にするのは、CA テクニカル サポートから要請があった場合のみになります。

注: external writer の プロシージャ名が parmlib メンバで指定されている場合、CAIENF を起動する前に external writer を指定する必要があります。
「 *Reference Guide*」のサンプル ENFXWTR プロシージャを参照してください。

CAIENF/USS 設定タスク

2 つの設定タスクが CAIENF/USS に関連しており、1 番目は必須で、2 番目はオプションです。

CAIENF/USS のタスクを実行する方法

1. CAIENF プロシージャが正常に動作するためには、そのプロシージャに割り当てられているユーザ ID のセキュリティ OMVS セグメントを定義する必要があります。

   新規ユーザ ID を定義するか、または TCP/IP や UNIX System Services などに使用されている既存のユーザ ID を使用できます。

2. (オプション)システムで使用する COFVLFxx メンバを更新して、CAIENF/USS が使用するクラスを追加します。以下に例を示します。

```
CLASS   NAME(CAENFU)
        EMAJ(PATHCACHE)
        MAXVIRT(512)
```

ENFSNMPM プロシージャのカスタマイズ

このタスクは、CAIENF SNMP モニタを使用する予定がある場合に必要です。

CAIENF SNMP モニタは、スターティッド タスクとして、独自のアドレス空間で実行されます。実行されるタイミングは、プライマリ CAIENF アドレス空間が立ち上がった後です。CAIENF SNMP モニタを起動するためのプロシージャは、*Yourdeploy*HLQ.CAW0PROC ライブラリで ENFSNMPM メンバとして配布されます。ユーザ ソリューション標準に従ってこのプロシージャをカスタマイズする必要があります。

ENFSNMPM プロシージャをカスタマイズする方法

1. CAW0OPTV データセットの SNMPVARS メンバを、スターティッド タスクによって使用される ENVVAR dsn にコピーし、必要に応じてカスタマイズします。

   CA Audit で ENFSNMPM モニタを使用する予定がある場合は、CAW1SNMP の実行可能プログラムが格納される *Yourdeploy*HLQ.CAW0PLD と共に、eTrust DLL が格納されているライブラリが APF 許可されている必要があります。

2. カスタマイズするサンプルとして、提供されている CAW0PROC ENFSNMPM プロシージャを使用します。

3. CAIENF SNMP モニタを使用する場合は、DCM ENF Parm ステートメントを CAS9DCM4 データ コレクタに追加します。CAS9DCM4 は *Yourdeploy*HLQ.CAW0DCM 内に提供されています。

4. CAIENF SNMP モニタ スターティッド タスクに関連付けられたユーザ ID 用のセキュリティ OMVS セグメントを定義します（TCP/IP が使用されるため）。セキュリティ パッケージに対する新しいユーザ ID を定義するか、すでに OMVS セグメントが定義されている既存のユーザ ID を使用することもできます。

5. ENFSNMPM プロシージャに対して、有効な OMVS セグメントを持つ TSS ACID を定義します。たとえば TSS ユーザ の場合は以下のように指定します。

   ```
   TSS ADD(stc) PROCNAME(ENFSNMPM) ACID(omvs)
   ```

   ここでは、プロシージャ ENFSNMPM をデフォルトの名前のままスターテッド タスクとして実行しており、OMVS がご利用の環境で使用する適切な ACID と仮定しています。

   これを適切に行わないと、理由コード x'90' の U4093 異常終了が発生します。

注: IPv6 サポートによって、ノード名や IP アドレスをさまざまな方法で指定できます。

IPv4 IP アドレスの例

```
141.202.65.31

141.202.66.11
```

ノード名の例

USILCA11

TCPIP11V

USI286ME.CA.COM

IPv6 IP アドレスの例

```
::1

fd00:7a06:0a20:0100:0000:0000:0000:0011..1086

0000:0000:0000:0000:0000:ffff:c0a8:060b..1088
```

第 9 章: CAICCI の設定

CA Common Services for z/OS のインストール後、CAICCI の実施と保守を最適化するためには CAICCI の設定タスクが必要です。

注: これらのタスクを実行するとき、展開されたデータ セットを使用します。

このセクションには、以下のトピックが含まれています。

CAICCI タスク

CAICCI の設定タスクには以下のものが含まれます。

- CAICCI の構成と起動
- 現行の CAICCI バージョンの追加設定タスク
- クライアント プラットフォームへの CAICCI のロード

CAICCI の構成と起動

CAICCI の構成と起動を行う方法

1. CCITCP、CCITCPGW、CCISSL、CCISSLGW の各スターティッド タスクに関連付けられた ID に対し、有効な OMVS セグメントを定義します。
2. 以下の DCM ステートメントが「CAIENF パラメータ ファイルの設定」セクションで定義されていない場合は、CAIENF パラメータ ファイル内で定義します。

   DCM（CAS9DCM3）
3. *Yourdeploy*HLQ.CAW0OPTN データセットのメンバ CCIPARM 内に保管されているデフォルトの CAICCI オプションを確認し、更新します。

   - CAICCI 用にカスタマイズしたオプションに加えて、インストールする CA ソリューション用に別途オプションを追加する必要があるかどうかを判断します。特に、CAICCI SPAWN 機能を使用する CA ソリューションでは、ENF PROC 内の SPNPARM DD ステートメントに追加する必要のある関連の SPAWN パラメータが提供されます。詳細については、ご使用のソリューションのマニュアルを参照してください。
   - CA ソリューションが Assured Delivery 機能を必要とする場合は、CCIPARM に LOGGER コマンドを追加します。

     注: Assured Delivery の詳細については、「*Administration Guide* 」を参照してください。
   - バージョン 14.0 において、CAICCI は、64 ビット（バーより上）ストレージの使用をサポートします。CA ソリューションは、キューとアプリケーション バッファ用に 64 ビット ストレージを割り当てて使用するために CAICCI を実行する場合があります。そのため、単一アドレス空間用に使用可能な仮想ページ数を境界を超えて設定するシステム MEMLIMIT は、2 ギガバイトといった、ゼロでない値に設定する必要があります。64 ビット ストレージを利用する特定の CA ソリューションは、それに特有の MEMLIMIT 要件を識別します。

     MEMLIMIT は、以下のいずれの方法でも設定できます。

     - JOB または EXEC ステートメント上で（「*z/OS MVS JCL 解説書*」参照）
     - SMFPRMxx parmlib メンバ内の MEMLIMIT パラメータによって（「*z/OS MVS 初期設定およびチューニング解説書*」を参照）
     - SET SMF または SETSMF コマンドによって（「*z/OS システム・コマンド*」を参照）
     - IEFUSI インストール EXIT によって（「*z/OS MVS インストール EXIT*」を参照）

CAICCI 用の追加設定タスク

このセクションでは、CAICCI のインストールを完了するために実行可能なオプションの設定手順について説明します。これらの手順のほとんどは、システム間で SSL CAICCI 接続を利用する場合にのみ必要となります。SSL は Secured Sockets Layer プロトコルの略称です。SSL により CAICCI で標準的な暗号化アルゴリズムを使ってデータを送信することができます。デジタル証明書を SSL と併せて使用することにより、送信データに高度な暗号化を適用すると共に、通信相手の本人性を確保することができます。SSL TCPIP プロトコルは、すべてのリンクに対して SSL を有効にしなくても実行できます。SSL リンクが存在しない場合、TCPSSL プロトコルおよび TCPSSLGW プロトコルは、それぞれ TCPIP プロトコルおよび TCPIPGW プロトコルとまったく同じように機能します。

注: CAICCI リンク プロトコルの詳細については、「*Administration Guide*」を参照してください。

このセクションの説明には、サンプル証明書である CCIP12 と CCIRTARM が用いられています。CCIP12 はエンド ユーザ証明書、CCIRTARM はそれに署名（認証）したルート証明書です。PC にも、これらと同じサンプル エンド ユーザ証明書とルート証明書がインストールされます（cci.pem および cciroot.pem）。これらのサンプル証明書をメインフレーム プラットフォームと PC プラットフォームに置くことにより、メインフレーム サーバの CCISSL が PC クライアントを認証できるようになります。同様に、これらと同じ証明書を使用することで、メインフレームのゲートウェイ サーバの CCISSLGW が、そのリモート ピア サーバを認証できるようになります。サイト独自の SSL 証明書を生成し、付属のサンプル証明書と置き換えて使用することを強くお勧めします。

SSL 通信リンクの利用

環境内で SSL リンクを利用できます。メインフレームから PC へのダウンロードには、FTP または IND$FILE（バイナリ転送）を使用してください。

SSL リンクを使用する方法

1. CCIPCS32 および（または） CCIPCS64 をダウンロードします（「クライアント プラットフォームへの CAICCI のロード (P. 179)」セクション参照）。
2. CCISSL をコピーします。キー データベース（キーリング）の場所と、秘匿保管されているパスワード ファイルの場所を確認しておく必要があります。
3. CCISSLGW をコピーします。キー データベース（キーリング）の場所と、秘匿保管されているパスワード ファイルの場所を確認しておく必要があります。
4. CCIRTARM をコピーします。
5. CCIP12 をコピーします。

注: 証明書キーの作成方法および外部キーリングへの追加方法（IBM のキー データベースを使用しない場合）については、ご使用の（外部の）セキュリティ マニュアルを参照してください。

CCISSL のコピー

CCISSL ファイルには、CAS9PDGM モジュールを実行するための JCL カタログ式プロシージャが含まれています。

CCISSL をコピーする方法

1. メンバ CCISSL を CAW0PROC データセットから、CCISSL が実行されるサイト固有のユーザ proclib にコピーします。
2. CCISSL を編集し、以下の内容を指定します。
   - IBM ディレクトリおよび CA ディレクトリに対するデータセットの命名規則
   - キー データベース（キーリング）の場所と、秘匿保管されているパスワード ファイルの場所

- 各種のパラメータ オプション (PARM=)

```
PARM
PORT=&PORT,US=&UNSECON,CLAUTH=&CLAUTH,CERT=&CERT,KEYRING=&KEYRING,
SV=&SSLVERS,CI=&CIPHERS,SSLT=&SSLTRCFN,SSLD=&SSLDUMP,CBDLL=&CBDLL,
TO=&TIMEOUT'
```

説明

「PORT=」は待機ポート(デフォルト: 1202)を示します。

「TCP=」は、CCISSL が使用する単一の TCP/IP プロトコル スタック名を示します。デフォルトでは、すべてのアクティブな TCP/IP スタック名になっています。

「UNSECON=」では、以下のいずれかを指定します。

- NEVER(デフォルト): 接続しようとする CCIPC が SSL に対応せず、有効になっていなければ、接続は拒否されます。
- ALLOW: 接続しようとする CCIPC が SSL 接続に対応し、かつ必要としている場合以外は、接続はセキュリティ保護されません。
- NONSSL: 接続しようとする CCIPC が(バージョン 1.1.7 より前の)SSL をサポートしていない場合は、セキュリティ保護されない状態で接続が可能です。接続しようとする CCIPC で SSL がサポートされ、かつ有効化されている場合、接続はセキュリティ保護されます。
- ONLY: セキュリティ保護されていない接続だけが許可されます。接続しようとする CCIPC が SSL をサポートし、かつ必要としている場合は、接続が拒否されます。このオプションは、この CCIPC サーバの SSL サポートを無効にします (CCITCP は恒久的にこの値に設定された CCISSL です)。

「CLAUTH=」では、以下のいずれかを指定します。

- N(デフォルト): クライアント証明書を認証しません。
- Y: クライアント証明書を認証します。
- Pass: クライアント証明書は認証されませんが、ユーザ EXIT の検証は要求されます。

「CERT=」はサーバ証明書のラベル名を示します。

- '*': ラベルが「CCIPC」である証明書が使用されます。見つからない場合は、ラベルが CAICCI Sysid に対してローカルな証明書が使用されます。見つからない場合は、ラベルが「CAICCI」である証明書が使用されます。
- 'label': 名前が label である証明書が使用されます。
- 何も指定しなかった場合: SystemSSL デフォルト証明書が使用されます。

注: 証明書のラベル名内の埋め込みブランクはサポートされません。

「KEYRING= 」は、(HFS キー データベースの代わりに使用される)外部のセキュリティ キーリングの名前を示します。

「SSLVERS= 」は、CCISSL が SSL サービスを要求するときに使用する System SSL のバージョンを指定します。

- 1: バージョン 1(OS/390 バージョン)
- 2:バージョン 2(z/OS 1.2 バージョン)
- 何も指定しない: 利用可能な最上位バージョン(デフォルト)

「PROT=」は、セキュリティ プロトコルの有効化される必要のあるものを示します。

- SSL: SSL バージョン 3 のみ(デフォルト)
- TLS: TLS バージョン 1 のみ
- SSL/TLS、TLS/SSL、S/T、T/S、BOTH: SSL バージョン 3 および TLS バージョン 1 の両方が有効化されます。

「CIPHERS= 」は、XXYYZZ... の形式で CAICCI パケットの暗号化に使用する 1 つまたは複数の SSL（バージョン 3）の暗号を優先度順に指定します。

- '01'：NULL MD5
- '02'：NULL SHA
- '03'：RC4 MD5
- '04'：RC4 MD5
- '05'：RC4 SHA
- '06'：RC2 MD5
- '09'：DES SHA
- '0A'：3DES SHA US
- '2F'：128-bit AES SHA US
- '35'：256-bit AES SHA US
- IBM：System SSL のデフォルトリスト（0504352F0A090306020100 など）
- 3DES：3DES を最上位とする System SSL デフォルトリスト：0A0504352F090306020100 など（デフォルト）
- AES128 または AES-128：128-bit AES を最上位とする System SSL デフォルトリスト（2F0504350A090306020100 など）
- AES、AES256、AES-256：256-bit AES を最上位とする System SSL デフォルトリスト（3505042F0A090306020100 など）

「SSLTRCFN= 」は、System SSL がトレース エントリを書き込むことのできる HFS ファイルの名前を示します。（ファイル名を指定するとトレースが有効になります）。

「SSLDUMP=」は、SSL パケットをトレース ファイル（TRCPRINT）にダンプするかどうかを指定します。

- No（デフォルト）
- Yes

「CBDLL=」は、クライアント（およびサーバ）証明書を検証するためのユーザ EXIT ルーチンが格納されている DLL のモジュール名を示します。

TIMEOUT= CCISSL（または CCITCP）によって切断されるまでの間、接続がアイドル状態を継続する秒数を指定します。

3. システム SSL ライブラリである連結にあるライブラリ、および C と C++ のランタイム ライブラリを APF 許可します。

このプロシージャには、STEPLIB を持つユーザ ID が割り当てられている必要があります。

- UNIX System Services セグメントが定義されていること
- キー データベースに対する読み取り/書き込み権限を持つこと

CCISSLGW のコピー

CCISSLGW には、CAS9PDPM モジュールを実行するための JCL カタログ式プロシージャが含まれています。

CCISSLGW をコピーする方法

1. メンバ CCISSLGW を CAW0PROC データセットから、CCISSLGW が実行されるサイト固有のユーザ proclib にコピーします。
2. CCISSLGW を編集し、以下の内容を指定します。
   - IBM ディレクトリおよび CA ディレクトリに対するデータセットの命名規則。
   - キー データベース(キーリング)の場所と、秘匿保管されているパスワード ファイルの場所。
   - 各種のパラメータ オプション(PARM=)。

     ```
     PORT=&PORT,TCP=&TCP,US=&UNSECON,RMAUTH=&RMAUTH,CERT=&CERT,
     KEYRING=&KEYRING,SV=&SSLVERS,CI=&CIPHERS,SSLT=&SSLTRCFN,SSL
     D=&SSLDUMP,CBDLL=&CBDLL'
     ```

     説明

     「PORT=」は待機ポート(デフォルト: 1202)を示します。

     「TCP=」は、CCISSLGW が使用する単一の TCP/IP プロトコル スタック名を示します。デフォルトでは、すべてのアクティブな TCP/IP スタック名になっています。

「UNSECON=」では、以下のいずれかを指定します。

- NEVER（デフォルト）：リモート CAICCI が SSL に対応せず、有効になっていなければ、接続は拒否されます。
- ALLOW：リモート CAICCI が SSL 接続に対応し、かつ必要としている場合以外は、接続はセキュリティ保護されません。
- NONSSL：リモート CAICCI が SSL をサポートしない場合は、セキュリティ保護されない接続が可能です。リモート CAICCI で SSL がサポートされ、かつ有効化されている場合、接続はセキュリティ保護されます。
- ONLY：セキュリティ保護されていない接続だけが許可されます。リモート CAICCI が SSL をサポートし、かつ必要としている場合、接続は拒否されます。このオプションは、このゲートウェイ サーバの SSL サポートを無効にします（CCITCPGW は恒久的にこの値に設定された CCISSLGW です）。

「RMAUTH=」では、以下のいずれかを指定します。

- N：リモート証明書を認証しません。
- （デフォルト）：リモート証明書を認証します。
- Pass：リモート証明書は認証されませんが、ユーザ EXIT の検証用にはやはり必要です。

「CERT=」はサーバ証明書のラベル名を示します。

- '*'：ラベルが「CCIGW」である証明書が使用されます。見つからない場合は、ラベルが CAICCI Sysid に対してローカルな証明書が使用されます。見つからない場合は、ラベルが「CCI」である証明書が使用されます。
- 'label'：名前が label である証明書が使用されます。
- 何も指定しなかった場合：SystemSSL デフォルト証明書が使用されます。

注：証明書のラベル名に空白を含めることはできません。

「KEYRING= 」は、（HFS キー データベースの代わりに使用される）外部のセキュリティ キーリングの名前を示します。

「SSLVERS= 」は、CCISSLGW が SSL サービスを要求するときに使用する System SSL のバージョンを指定します。

- 1: バージョン 1(OS/390 バージョン)
- 2:バージョン 2(z/OS 1.2 バージョン)
- 何も指定しない: 利用可能な最上位バージョン(デフォルト)

「PROT=」は、セキュリティプロトコルの有効化される必要のあるものを示します。

- SSL: SSL バージョン 3 のみ(デフォルト)
- TLS: TLS バージョン 1 のみ
- SSL/TLS、TLS/SSL、S/T、T/S、BOTH: SSL バージョン 3 および TLS バージョン 1 の両方が有効化されます。

「CIPHERS= 」は、XXYYZZ... の形式で CAICCI パケットの暗号化に使用する 1 つまたは複数の SSL(バージョン 3)の暗号を優先度順に指定します。

- '01': NULL MD5
- '02': NULL SHA
- '03': RC4 MD5
- '04': RC4 MD5
- '05': RC4 SHA
- '06': RC2 MD5
- '09': DES SHA
- '0A': 3DES SHA US
- '2F': 128-bit AES SHA US
- '35': 256-bit AES SHA US
- IBM: System SSL のデフォルトリスト(0504352F0A090306020100 など)の使用
- 3DES: 3DES を最上位とする System SSL のデフォルトリスト(0A0504352F090306020100 など)の使用(デフォルト)

- AES128 または AES-128: 128 ビット AES を最上位とする System SSL デフォルト リスト（2F0504350A090306020100 など）の使用
- AES、AES256、AES-256: 256 ビット AES を最上位とする System SSL デフォルト リスト（3505042F0A090306020100 など）の使用

「SSLTRCFN= 」は、System SSL がトレース エントリを書き込むことのできる HFS ファイルの名前を示します。（ファイル名を指定するとトレースが有効になります）。

「SSLDUMP=」は、SSL パケットをトレース ファイル（TRCPRINT）にダンプするかどうかを指定します。

- No（デフォルト）
- Yes

「CBDLL=」は、クライアント（およびサーバ）証明書を検証するためのユーザ EXIT ルーチンが格納されている DLL のモジュール名を示します。

3. システム SSL ライブラリである連結にあるライブラリ、および C と C++ のランタイム ライブラリを APF 許可します。

このプロシージャには、以下の条件を満たしたユーザ ID が割り当てられている必要があります。

- UNIX System Services セグメントが定義されていること
- キー データベースに対する読み取り/書き込み権限があること

CCIRTARM のコピー

CCIP12 をコピーする前に、以下の点に留意してください。

- CCISSL を使用しているとき、CCIRTARM が作用するためには、クライアント証明書を要求し、認証するように CCISSL の構成が済んでいることが必要です。
- デフォルトでは、このオプションがオフになります。
- CCIRTARM は、サンプルの CA（Certificate Authority）証明書です。メインフレーム サーバの CCISSL が、サンプルのキー/証明書（cci.pem）をエンド ユーザ証明書として使用する PC クライアントを認証する際に使用されます。

- cci.pem ファイルは、CCIPC/SSL のインストール中に C:¥CA_APPSW ディレクトリにコピーされます。
- このオプションを有効にした場合（CCISSL プロシージャの PARM ステートメント内または TCPSSL の PROTOCOL ステートメント内で CLAUTH=Y とするなど）、CCIRTARM は、PC クライアントからの cci.pem 証明書を認証する必要があります。

  HFS キー データベースを使用している場合は、CCIRTARM は、メインフレーム上の SSL キー データベース内に CA 証明書としてインポートされている必要があります。インポートには、gskkyman ユーティリティを使用します。

  z/OS キー データベースを使用している場合は、CCIRTARM は z/OS キー データベースに CA 証明書としてインポートされている必要があります。インポートには、Top Secret、ACF2、RACF などのセキュリティ ソフトウェアを使用します。

  注: 証明書キーのインポートおよび gskkyman ユーティリティの詳細については、IBM の「*System SSL Programming Guide and Reference (SC24-5877)*」を参照してください。

- CCISSLGW を使用しているとき、リモート ホスト（つまり、SSL セッションのクライアント側として機能するホスト）が接続を開始すると、リモート ホストからの証明書が CCIRTARM を使って認証されます。CCISSLGW とそのリモート ホストは、最終的にはピアツーピアで接続されますが、SSL セッションの確立に使用されるクライアント/サーバの初期 ID は、接続要求の開始元によって決定されます。接続はローカル ホストから開始される場合もあれば、リモート ホストから開始される場合もあるため、ローカル ホストとリモート ホストのどちらもが、SSL セッションのクライアント エンドになる可能性があります。そのため、CCIRTARM は、SSL 経由で接続するすべてのホストに存在している必要があります。
- 制御プロシージャの PARM オプション（RMAUTH=Y）はデフォルトで有効になります。

クライアント証明書を要求および認証するように CCISSL を構成した場合、または、CCISSLGW を実行する場合は、以下の手順に従います。

CCIRTARM をコピーする方法

1. ASCII（テキスト）転送を使用し、CAW0OPTN データセットの CCIRTARM を、CCISSL または CCISSLGW が実行されるメインフレーム上の HFS ファイルにコピーします。
2. ファイルを HFS 上に ccirt.arm として保存します。たとえば、TSO コマンド「OPUT *Yourdeploy*HLQ.CAW0OPTN(CCIRTARM) '/etc/ccirt.arm' TEXT」を発行します。
3. HFS キー データベースを使用している場合、System SSL ユーティリティ（gskkyman）を使用して、PC の ccirt.arm（CCIRTARM） を認証局証明書として、クライアント認証用に SSL キー データベースにインポートします。

   z/OS キー データベースを使用している場合、インポート処理については、セキュリティに関するソフトウェアのマニュアルを参照するか、セキュリティ管理者にご相談ください。

CCIP12 のコピー

CCIP12 をコピーする前に、以下の点に留意してください。

- CCIP12 は、IBM の System SSL キー データベースにインポートできるようにエクスポートされたサンプルのキー/証明書（PKCS#12 ファイル）です。CCISSL および CCISSLGW では、このファイルがエンド ユーザ証明書として使用されます。
- このキー/証明書を使用すると、難しい設定を行うことなく CCISSL サーバおよび CCISSLGW サーバを実行できますが、あくまでサンプルであり、一時的な用途を目的としています。
- 前述のように、SSL 接続のリモート クライアント側（PC、メインフレーム、UNIX など）が、サーバ証明書を有効として受け入れるためには、そのクライアントにも認証用の CA（Certificate Authority）証明書を置く必要があります。
- PC 環境の Certificate Authority ファイル（C:¥CA_APPSW ディレクトリの cciroot.pem）内に、認証用の CA 証明書がすでに存在する場合、CCIP12 を使用することによって、その PC による SSL 接続が許可されます。
- キー データベースまたはキーリングに CCIRTARM を Certificate Authority 証明書としてインポートすると、サンプル cci.pem（CCIP12 証明書）をそのエンド ユーザ証明書として使用するあらゆる PC またはリモート CAICCI ホストからの SSL 接続が可能になります。
- SSL 証明書は独自に生成することをお勧めします。生成した証明書に署名した Certificate Authority のコピーは、C:¥CA_APPSW ディレクトリの cciroot.pem ファイル内と、メインフレームのキー データベース内に置く必要があります。

CCIP12 をコピーする方法

1. バイナリ転送を使用し、CAW0OPTN データセットの CCIP12 を、CCISSL または CCISSLGW が実行されるメインフレーム上の HFS ファイルにコピーします。
2. ファイルを HFS 上に cci.p12 として保存します。たとえば、TSO コマンド「OPUT *Yourdeploy*HLQ.CAW0OPTN(CCIP12) '/etc/cci.p12' BINARY」を発行します。
3. HFS キー データベースを使用している場合、System SSL ユーティリティ（gskkyman）を使用して、キー/証明書ファイル CCIP12 を SSL キー データベースにインポートします。

   z/OS キー データベースを使用している場合、インポート処理については、セキュリティに関するソフトウェアのマニュアルを参照するか、セキュリティ管理者にご相談ください。

CCISSL の起動

CCISSL を起動する方法

CCISSL を CCITCP の代わりに使用する場合は、まず、以下の MVS コンソール コマンドを実行して CCITCP アドレスをキャンセルします。

```
C CCITCP
```

CCISSL を別のポート番号で実行するように構成することで、CCITCP と CCISSL の両方を実行することもできます。

CCISSL の自動化

CAIENF/CAICCI アドレス空間の開始と終了に伴う形で CCISSL の起動と停止を自動化することができます。

CCISSL を自動化する方法

1. メンバ PRTCPSSL を CAW0OPTN データセットから、CCISSL が実行されるメインフレームにコピーします。このメンバには、CAIENF/CAICCI に、指定したランタイム オプションで CCISSL プロシージャを開始させるための CAICCI PROTOCOL ステートメントが含まれます。
2. このファイルを編集し、PROTOCOL ステートメントの第 4 引数（メインフレームの sysid を指定する）を変更します。デフォルト値は MyMainFrameCCISysid です。
3. SSL のオプションと値は、プロシージャの PARM フィールドで定義します。ただし、PROTOCOL ステートメントを使用して、1 つ以上の SSL パラメータをセミコロン（;）で区切って指定することもできます。

   ```
   PROTOCOL(TCPSSL,Port;SSLKeyword1=SSLValue1;
   SSLKeyword2=SSLvalue2;…,1,MyMainFrameCCISysid,16384)
   ```

   ここで「*Port*」は CCISSL が接続を待機するポート番号です。ポート番号を指定する場合は、最初のネットワーク パラメータとして指定する必要があります。
4. このファイルの内容を、CAIENF プロシージャ内の ENFPARMS DD ステートメントで指定された既存のデータセットに追加または連結します。

コンソールからの CCISSL の起動と停止

CCISSL の起動と停止は、コンソール コマンドを使って行うこともできます。（自動的に起動させるのではなく）この方法を用いた場合、CCISSL プロシージャに直接記述された PARM= オプションが有効になります。

CCISSL をコンソールから起動および停止する方法

1. 以下のコマンドを入力します。

   ```
   S CCISSL
   ```

   CCISSL が正常に初期化されると、以下のメッセージが表示されます。

   ```
   CAS9850I - CCI/SSL Version 12 Active
   CAS9850I - CCI TCP/IP Host Name = myTCP/Iphostname
   CAS9850I - CCI TCP/IP SSL Server Ready. Port = myPort
   CAS9850I - Addr = myIpAddr
   ```

   これで CCISSL が指定ポート番号（myPort）で接続要求を受け付ける準備が整いました。接続の成功と失敗が、診断メッセージと共に表示されます。

2. 以下のコマンドを入力します。

   ```
   P CCISSL
   ```

   このコマンドを入力することにより、コンソールから CCISSL を停止できます。

CCISSLGW の起動と停止

CAICCI ホスト間接続に SSL を使用する場合は、CCISSLGW プロシージャを使用する必要があります。

CCISSLGW スターテッド タスクに関連付けられる ID には、有効なセキュリティ OMVS セグメントが定義されている必要があります。

CCISSLGW の自動化

CAIENF/CAICCI アドレス空間の開始と終了に伴う形で CCISSLGW の起動と停止を自動化することができます。

CCISSLGW を自動化する方法

1. メンバ PRTCPSSL を CAW0OPTN データセットから、CCISSLGW が実行されるメインフレームにコピーします。

   このメンバには、CAIENF/CAICCI に、指定したランタイム オプションで CCISSLGW プロシージャを開始させるための CAICCI PROTOCOL ステートメントが含まれます。

2. このファイルを編集し、PROTOCOL ステートメントの第 4 引数（メインフレームの sysid を指定する）を変更します。デフォルト値は MyMainFrameCCISysid です。

3. PROTOCOL ステートメントを使用して、1 つ以上の SSL パラメータをセミコロン（;）で区切って指定します。第 2 引数（オプションの「network」パラメータを指定する部分）を使用して、SSL 関連の情報を渡すこともできます。SSL のオプションと値は、プロシージャの PARM フィールドで定義できます。

   ```
   PROTOCOL(TCPSSLGW,Port;SSLKeyword1=SSLValue1;
   SSLKeyword2=SSLvalue2;…,1,MyMainFrameCCISysid,16384)
   ```

4. このファイルの内容を、CAIENF プロシージャ内の ENFPARMS DD ステートメントで指定された既存のデータセットに追加または連結します。

HFS キー データベースの作成とデータ入力

CAICCI では、TCP/IP で使用できるオプションの SSL がサポートされます。メインフレーム、PC、UNIX、および Linux ボックス間の接続は、SSL を実装した CAICCI でセキュリティ保護されます。セキュリティ証明書が含まれるキー データベースは、これらの SSL 接続のセキュリティ保護に使用されます。

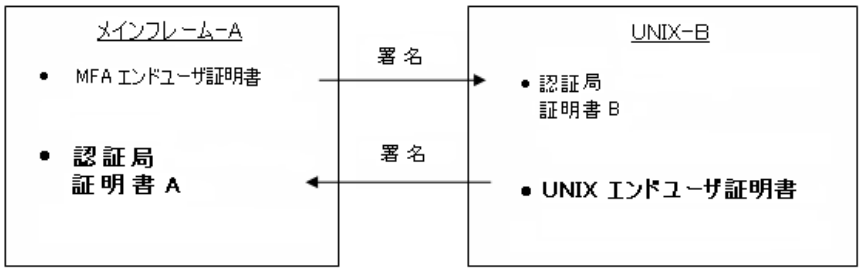
クライアント/サーバ接続では、メインフレーム スターティッド タスク CCISSL が使用されます。CAICCI-PC Configurator は、SSL を使用するかどうか、およびセキュリティ証明書の PC への適用方法を制御します。

ピアツーピア接続では、メインフレーム スターティッド タスク CCISSLGW が使用されます。証明書は、HFS またはセキュリティ パッケージのキーリングに保管されます。サポートされているセキュリティ パッケージは、CA Top Secret、CA ACF2、および RACF です。

セキュリティ証明書

SSL を使用する各ノードでは、2 つの証明書が必要です。エンドユーザ証明書と、別のノードでエンドユーザ証明書を署名または検証する CA（認証局）証明書です。CAICCI は、各ノードにインストールできる 2 つのデフォルトの証明書とともに提供されます。本番環境のセキュリティ保護のため、クライアント ノードは、基本インストールの後に、テスト済みのデフォルト証明書を使用してクライアント ノード専用の証明書を生成する必要があります。

たとえば、2 つのノードを持つ環境では、以下の図に示すように、合計 4 つの証明書があります。



キー データベースは、HFS 内のどこにでも保存できる通常のファイルです。たとえば、以下のようになります。

```
/etc/cci/keyring/cci.kdb
```

複数のキー データベースを定義できるほか、代わりに別のキー データベース ファイルを参照するように CCISSL と CCISSLGW のプロシージャを修正することもできます。これらのプロシージャには、キー データベースのパス名、証明書の名前、および秘匿保管されているパスワード ファイルのパス名を指定する必要があります。

HFS キー データベースを作成しデータを格納する方法

1. HFS キー データベースの格納場所となるディレクトリを作成します（/etc/cci/keyring など）。
2. このディレクトリに移動し、gskkyman を実行して残りの手順を実行します。

   通常、このプログラムを実行するには、まず GSK.SGSKLOAD（1.6 以前の z/OS）または SYS1.SIEALNKE（z/OS 1.6）を指すように STEPLIB 環境変数を設定する必要があります。これは、プロファイル メンバを更新（export STEPLIB=$STEPLIB:GSK.SGSKLOAD または export STEPLIB=$STEPLIB:SYS1.SIEALNKE）するか、エクスポート コマンド（特定のセッションのみを対象とする場合）を実行することによって行うことができます。
3. gskkyman の [Database] メニューから [Create new database] を選択します。
4. データベースに cci.kdb という名前を付けます。

5. パスワードとして cci を使用します。パスワードの有効期限は設定しないでください。
6. データベースのレコード長（デフォルトを使用）を入力します。
7. ［Store database password］を選択し、暗号化されたデータベース パスワードを cci.sth に保存します。
8. 以下の gskkyman メニューに従って、ccirt.arm（CCIRTARM）ファイルのルート証明書を、クライアント認証に必要なキー データベースに格納します。
   - gskkyman の [Key Management] メニューから［Import a Certificate］を選択します。
   - 証明書ファイル名に ccirt.arm を入力します。現行ディレクトリに存在しない場合は、フル パス名を含めて指定する必要があります。
   - ラベルとして CCIROOT を入力します。大文字を使用してください。ラベルでは大文字と小文字が区別されます。

   これでサンプル ルート証明書がキー データベースに保存されました。クライアント認証が要求されると、PC クライアントから送られてきた証明書が CCISSL によって検証されます。また、CCISSLGW も、接続の開始元のピア ホストを認証できます。
9. cci.p12（CCIP12）から証明書と秘密キーをインポートします。
   - gskkyman の [Key Management] メニューから［Import a Certificate and a private key］を選択します。
   - インポート ファイル名には cci.p12 を入力します。
   - インポート ファイルのパスワードには cacci を入力します。
   - ラベルとして CAICCI を入力します。大文字を使用してください。ラベルでは大文字と小文字が区別されます。

   これで、CAICCI エンド ユーザ証明書がキー データベースにインポートされ、CCISSL および CCISSLGW で利用できる状態になりました。PC が CCISSL に接続した場合、またはリモート ホストが CCISSLGW への接続を開始した場合、これらのローカル サーバが、このエンド ユーザ証明書で応答することによって PC またはリモート ホストの ID を確認します。PC またはリモート ホストがローカル サーバの ID を正しく認証するためには、その PC またはリモート ホストに、対応するルート証明書（ciroot.pem または CCIRTARM）がインストールされている必要があります。

   これらのサーバがすでに稼働している場合は再起動する必要があります。再起動しないと、証明書のエラー メッセージが表示されます。

クライアント プラットフォームへの CAICCI のロード

CAICCI をインストールしていて、メインフレームを使用して CA Datacom Server や CA IDMS Server などのクライアント/サーバ製品との PC 通信を計画する場合、CAW0OPTN メンバ CCIPCS32 および（または） CCIPCS64 をダウンロードして、CAICCI/PC をインストールする必要があります。

CAICCI/PC は CA Common Services for z/OS のインストール メディアで配布されます。CAICCI/PC では、SSL 、TCP/IPv4、TCP/IPv6 のプロトコルをサポートしています。

PC が IND$FILE ファイル転送プロトコルをサポートする 3270 エミュレータを使用してメインフレームに接続されている場合、メインフレームから TCPIP（FTP）または LU2 を使用して CAICCI/PC を導入できます。他のソフトウェアは必要ありません。必要な CAICCI/PC ファイルの一括配布を行うために、CA XCOM や Unicenter Software Delivery など、他のファイル転送アプリケーションを使用することもできます。各製品の詳細については、該当の製品マニュアルを参照してください。

注: CAICCI/PC は、LAN サーバ上にインストールして複数ユーザ間で共用することはできません。各 PC ごとに CAICCI/PC のコピーをインストールする必要があります。

CAICCI/PC を PC にインストールする方法

C:¥CA_APPSW ディレクトリにある CAINDREG プログラムを使用して、バージョン 14.0 より前の CAICCI-PC の任意のバージョンを削除します。バージョン 14.0 以降は、コントロール パネルにある*プログラムの追加と削除*ツールを使用して、アンインストールできます。

1. TCP/IP (FTP) または LU2 を使用して CAW0OPTN メンバ CCIPCS32 および(または) CCIPCS64 をユーザの PC にダウンロードします。

   32 ビット PC の場合は、32 ビットバージョンの CCIPCS32 のみをダウンロードする必要があります。64 ビット PC の場合は、使用されるアプリケーションに応じて両方のバージョンを必要とする場合があります。PC 上で実行されるクライアント/サーバ製品によって、どちらのパッケージを使用するかの選択を行う必要があります。クライアント/サーバ製品が混在していて両方のバージョンを必要とする場合、64 ビット PC に両方のパッケージをインストールできます。

   #### TCP/IP (FTP) でダウンロードする方法

   FTP を使用して z/OS ホストから CAICCI/PC ファイルをダウンロードするには、PC が TCP/IP 経由で接続されている必要があります。

   PC のコマンド プロンプトを使用する場合、以下の手順に従います。

   - 転送ファイルを受け取るディレクトリに移動します。
   - IP アドレスまたはリモート ホスト名を指定して ftp コマンドを入力します。
   - プロンプトが表示されたら、ユーザ ID とパスワードを入力してリモート ホストにログオンします。
   - バイナリ転送を指定します。

- ディレクトリ移動コマンドを入力します。その際、リモート ディレクトリの場所として *Yourdeploy*HLQ.CAW0OPTN データ セットを一重引用符で囲んで指定します。*Yourdeploy*HLQ は CA Common Services のインストールに使用した HLQ です。
- get コマンドを入力します。その際、リモート ディレクトリから現在のローカル ディレクトリに CCIPCS32.EXE または CCIPCS64.EXE のいずれかとして転送されるメンバの名前(CCIPCS32 または CCIPCS64 のいずれか)を指定します。32 ビット バージョンおよび 64 ビット バージョンの両方をダウンロードしようとする場合、次の例で示すように別個の get コマンドを使用する必要があります。

以下に示すのは、FTP セッションのサンプルです。

```
C:>ftp myIPname
User:
Password:
. . .
binary
. . .
cd 'YourdeployHLQ.CAW0OPTN'
get ccipcs32 ccipcs32.exe
get ccipcs64 ccipcs64.exe

quit
```

LU2 でダウンロードする方法

注: 以下の手順は CCIPCS32 (32 ビット バージョン) 用です。CCIPCS64 (64 ビット バージョン) が必要な場合は、同じ手順を使用し、CCIPCS32 とある箇所をすべて CCIPCS64 の名前に入れ替えます。

- PC 上に新規ディレクトリを作成します。
- ターミナル エミュレータのファイル転送機能を実行するためにボタンをクリックします。
- [Receive from Host]を選択します。
- ホスト ファイル名としては '*Yourdeploy*HLQ.CAW0OPTN (CCIPCS32)' または 'CAI.CAIOPTN (CCIPCS64)' を入力し、ホスト タイプとしては TSO を入力します。
- [PC file name]には、PC ドライブと新しく作成したディレクトリを入力し、その後に「CCIPCS32.exe」または「CCIPCS64.exe」と入力します。

  ```
  c:¥ccinst¥CCIPCS32.exe
  ```

  または

  ```
  c:¥ccinst¥CCIPCS64.exe
  ```

- 転送タイプは必ず BINARY にしてください。
- 転送を開始します。

2. ファイルのダウンロード完了後、新しく作成したディレクトリに移動し、CCIPCS32.exe のアイコンまたは CCIPCS64.exe のアイコンをダブルクリックして、自己解凍プロセスを開始させます。

   CAICCI/PC のインストールが開始されます。

3. インストールの完了後に、処理中に作成された Readme ファイルをお読みください。新しい証明書ファイルの説明、インストールに関する考慮事項、OpenSSL/SSLeay ライセンスのコピーなどが含まれています。

PC に対する CAICCI のロードの詳細については、「*Administration Guide*」を参照してください。

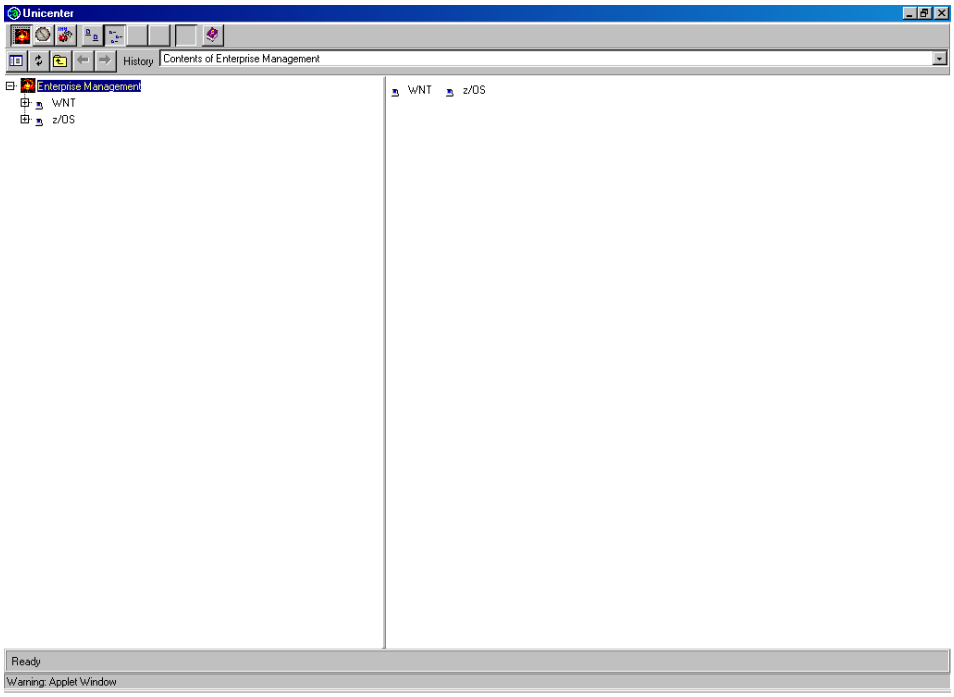
リモート マシンを使用したピアツーピア接続

ピアツーピア通信は、CCISSLGW を実行しているメインフレーム、または配布された CA NSM コンピュータおよびメインフレームで発生します。どちらの場合でも、メインフレーム タスク CCISSLGW により簡単に通信を行えます。

CA NSM Java GUI の単一インスタンスで、複数の CA Common Services または CA NSM コンピュータを利用できます。例えば、CA NSM の Workload コンポーネントは、z/OS の CA Common Services の一部として提供されなくても GUI から利用できます。コンピュータが CAICCI によって接続されていることが主な要件です。すべてのリモート コンピュータの CA NSM アプリケーションは、GUI で表示されます。セキュリティのために、リモート コンピュータのユーザ ID とパスワードの入力を求められます。

コンピュータの表示数を制限するには、表示させたいコンピュータの CAICCI SYSID をリストするファイル /cai/nsmem/emsrvc/data/nodelist を作成します。このディレクトリに nodelist.sample と呼ばれるサンプル ファイルが用意されます。コンピュータの表示数を制限すると、応答時間が削減されます。

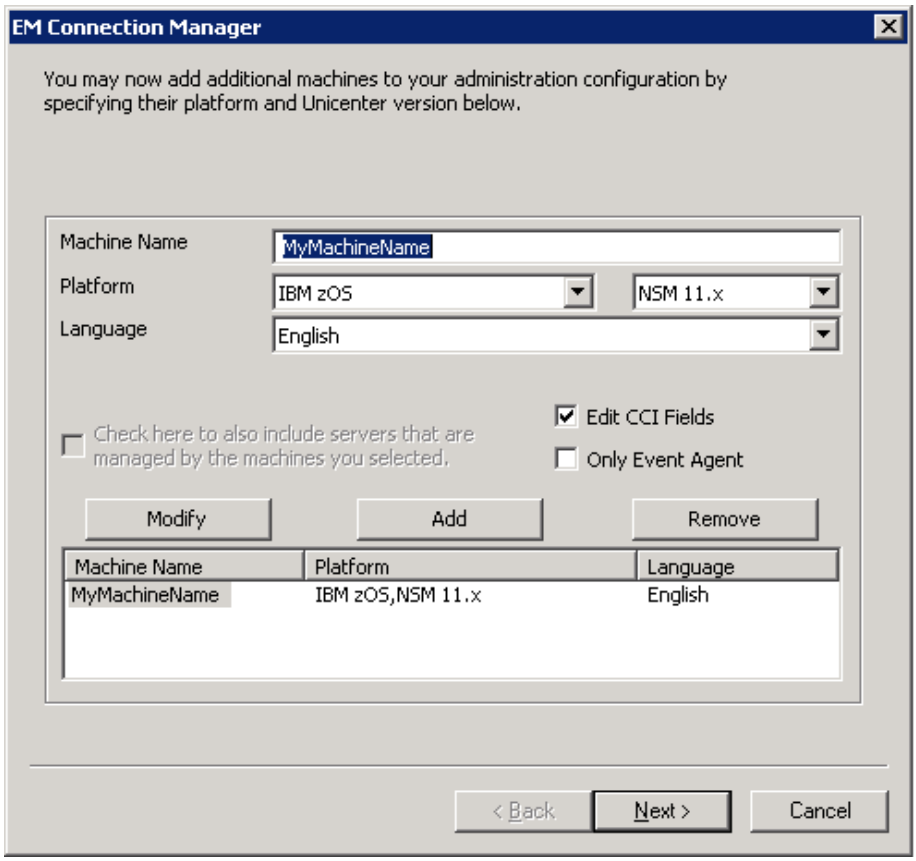
以下は、複数のコンピュータが表示されている GUI の例です。



CA NSM の使用

CA NSM を使用する方法

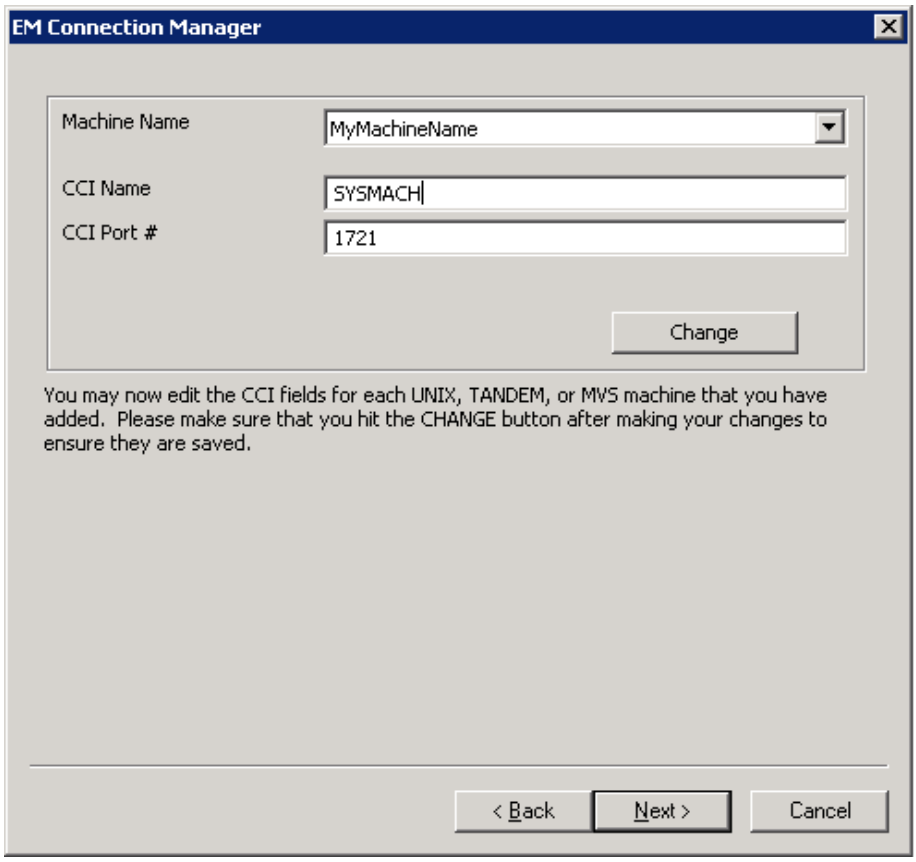
1. リモート CA NSM 分散コンピュータ上で EM Connection Manager を開き、以下の通り選択します。
   a. ［Machine Name］では、CAICCI SYSID をサーバの名前として選択します。
   b. ［Platform］では、IBM zOS を選択します。
   c. ［Edit CAICCI Fields］チェックボックスにチェックを入れます。
   d. ［Add］をクリックして、サーバをリストに追加します。



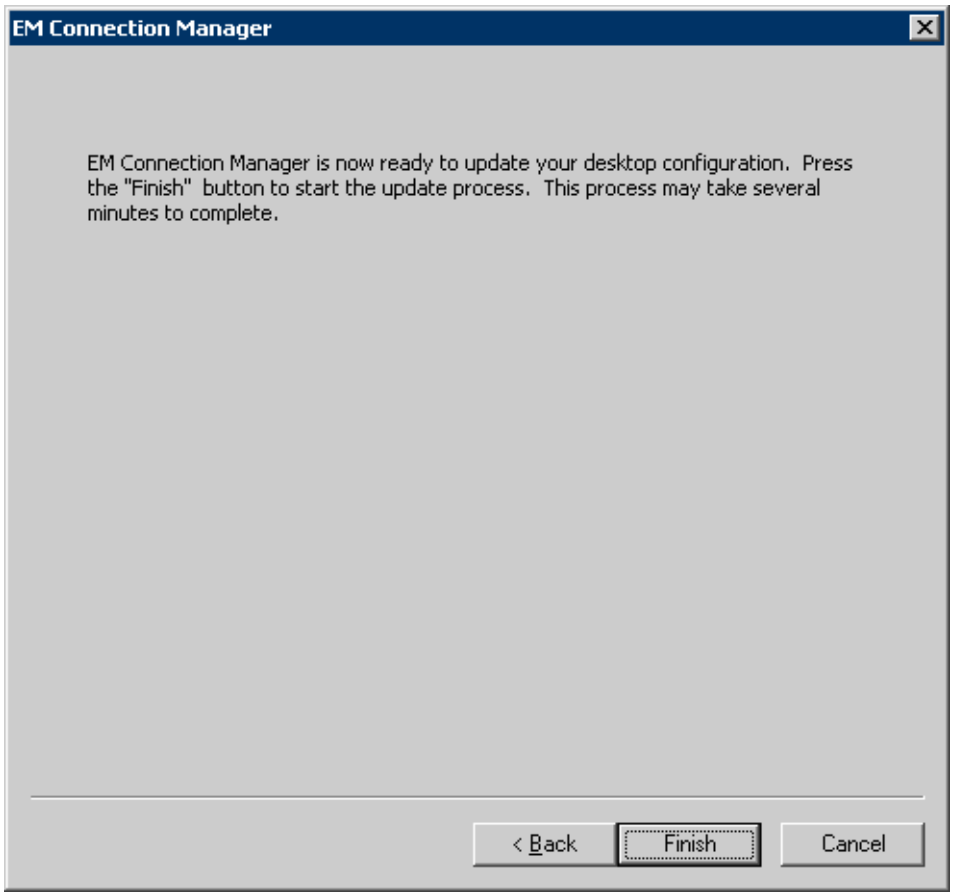
2. [Next] をクリックして、CAICCI フィールドを変更し、メインフレーム設定に合わせます。

3. CAICCI ポート番号に指定された値を、メインフレーム上で CCISSLGW スターテッド タスクにより使用されている値に一致させます。

   正しいポート番号を確認するために、CCISSLGW スターテッド タスク JOBLOG を z/OS システム上で調べることができます。エイリアスは CAICCI sysid が 8 文字より長い場合にのみ必要となるため、[Alias] フィールドは空白のままにしておきます。z/OS 上の CAICCI sysid は 8 文字を超えることはできません。



4. [Next]をクリックして、最後の画面を表示します。
5. [Finish] をクリックして、更新が正常に終了したというメッセージ ボックスが表示されるまで待ちます。



変更のアクティブ化

CA NSM の変更をアクティブにするには、以下のコマンドをリモート CA NSM 分散コンピュータから発行して CAICCI リモート コンポーネントを再起動する必要があります。

```
ccicntrl stop rmt
ccicntrl start rmt
```

変更の検証

CA NSM に加えられた変更を検証するには、リモート CA NSM 分散コンピュータ上で以下のコマンドを発行します。

```
ccii
```

このリストに z/OS sysid が表示されます。接続されるまで数分かかる場合がありますが、コマンドを発行できる状態になるまで待ちます。表示されないときは、以下を確認します。

- CCISSLGW タスクが z/OS 上でアクティブになっているか。

  Yes — SYSPRINT を参照して NT マシンからの接続メッセージを確認します。例えば、以下は Windows マシン上の ccirmtd.rc ファイルのサンプルです。

  ```
  LOCAL = BARNA03W2K BARNA03W2K 32768 startup ALIAS=BARNA03W
  REMOTE = 141.202.204.93 a93s 32768 startup PORT=7000
  REMOTE = 141.202.36.71 a71senf 32768 startup PORT=7000
  REMOTE = usilca11 a11senf 32768 startup PORT=7000
  REMOTE = 141.202.204.97 a97s 4096 startup PORT=7000
  ```

  この例では、メインフレームのホスト名 usilca11 に以下のメッセージが表示されることが想定できます。

  ```
  CAS9603I - CAICCI A11SENF  CONNECTED TO CAICCI BARNA03W
  ```

  No — CAICCI PARM にプロトコル ステートメントが含まれているかどうかを確認します。

  ```
  PROTOCOL(TCPIPGW)
  ```

  ```
  PROTOCOL(TCPSSLGW)
  ```

- NT NSM/caiusr ディレクトリの ccirmtd.rc ファイルを確認します。z/OS マシン用にエントリがあります。エントリは以下のように表示されます。

  ```
  REMOTE = hostname ccisysid 32768 startup PORT=portnumber
  ```

  hostname は z/OS マシンの TCP/IP 名または ipaddress を指定し、*ccisysid* は z/OS マシンの SYSID を指定し、*portnumber* は CAS9850I メッセージのポート番号を指定します。

  誤りがあれば訂正し、CAICCI リモートを再起動します。

  CCISSLGW スターテッド タスクの JOBLOG を調べ、次の z/OS コンソール コマンドを発行することで、これらの z/OS マシン値が得られます。

  ```
  ENF DISPLAY,SYSID
  ```

- z/OS 上でアクティブになっているレシーバーはあるか。以下のコンソール コマンドを発行し、どのローカル レシーバーが利用可能になっているを確認します。

  ```
  F ENF,DISPLAY,RECEIVER
  ```

  表示例:

  ```
  CAS9626I - CAICCI SUBSYSTEM IS OPERATIONAL
  CAS9701I - CCI # RCVRS(00000009) LOCAL(00000009) REMOTE(00000000)
  CAS9700I - ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  CAS9702I - CCI RESOURCE RECEIVER(#A93S     CA-TOP-SECRET       )
  CAS9703I - CCI RESOURCE SENDER(                                )
  CAS9704I - CCI RESOURCE OWN(A93S    ) RCVI(00000001) SND(00000000) T(L)
  CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(09:16:51.62) D(N)
  CAS9708I - CCI RESOURCE QUE(Y)  DOLSI(2003.300) TOLSI(09:16:51.62)
  CAS9700I - ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  CAS9702I - CCI RESOURCE RECEIVER(@A93S     W410_SPAWN_SERVER   )
  CAS9703I - CCI RESOURCE SENDER(@A93S     SPAWN_INQY_SERVICES )
  CAS9704I - CCI RESOURCE OWN(A93S    ) RCVI(00000003) SND(00000002) T(L)
  CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(12:54:18.47) D(N)
  CAS9708I - CCI RESOURCE QUE(N)  DOLSI(2003.300) TOLSI(12:52:11.72)
  CAS9700I - ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  CAS9702I - CCI Resource Receiver(#USI273ME CA_STARUNIX_SERVER  )
  CAS9703I - CCI Resource Sender(                                )
  CAS9704I - CCI Resource Own(USI273ME) RcvI(00000001) Snd(00000000) T(L)
  CAS9707I - CCI Resource Rout(Y) DOLRI(2003.300) TOLRI(16:11:40.36) D(N)
  CAS9708I - CCI Resource Que(Y)  DOLSI(2003.300) TOLSI(16:11:40.36)
  CAS9700I - ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
  CAS9702I - CCI RESOURCE RECEIVER(#A93S     CAI_OPR_DAEMON      )
  CAS9703I - CCI RESOURCE SENDER(                                )
  CAS9704I - CCI RESOURCE OWN(A93S    ) RCVI(00000002) SND(00000001) T(L)
  CAS9707I - CCI RESOURCE ROUT(Y) DOLRI(2003.300) TOLRI(15:33:10.06) D(N)
  CAS9708I - CCI RESOURCE QUE(Y)  DOLSI(2003.300) TOLSI(15:33:10.03)
  ```

  重要: レシーバーのリストにある CAI_OPR_DAEMON および CA_STARUNIX_SERVER を確認します。z/OS 上で実行されているイベント管理が、分散プラットフォームで実行されている CA NSM と完全に通信可能になるには、これらの 2 つのレシーバーが存在しなければなりません。

インストールの確認

クライアント/サーバ接続では、メインフレーム スターティッド タスク CCISSL が使用されます。

ピアツーピア接続では、メインフレーム スターティッド タスク CCISSLGW が使用されます。

CAICCI が正常に開始されたことを検証する方法

1. 次のステートメントが ENFPARMS 連結の CCIPARM で指定されている場合に CAICCI のサブタスクを開始する、CAIENF プロシージャを実行します。

   ```
   SYSID(xxxxxxxx)
   ```

2. CAIENF が初期化されたら、次のコンソール コマンドを実行してください。

   ```
   ENF STATUS
   ```

3. 出力において次のメッセージを探します。

   ```
   CAS9626I – CAICCI Subsystem is operational
   ```

   メッセージが存在しない場合は、CAICCI、CAS9DCM3 用の DCM ステートメントが CAIENF パラメータ ファイルに定義され、CCIPARM が更新されて有効な SYSID を含んでいることを確認してください。

4. CCISSL および CCISSLGW のスターティッド タスクが、システムのプロシージャ ライブラリにおいて利用可能であることを確認してください。これらのスターティッド タスクが、セキュリティ環境において適切にセットアップされていることを確認してください。CCISSL および CCISSLGW、さらに CAIENF には、セキュリティ OMVS セグメントが必要です。

   - CCISSL では、プロシージャ JCL の PGM が CAS9PDGM に設定されていることを確認します。
   - CCISSLGW では、プロシージャ内の PGM= が PGM=CAS9PDPM に設定されていることを確認します。

トラブルシューティング

このセクションでは、接続の現在のステータスの検証およびトレースのアクティブ化の方法を説明します。

現在のステータス

複数のマシンの接続およびマシン間で表示されるアプリケーションの現在のステータスを検証するために、発行できるコマンドがいくつかあります。

```
ENF CCI(DISPLAY,RESOURCE)
ENF CCI(DISPLAY,LINK)
```

トレースのアクティブ化

アプリケーションによって、トレースをオンにする複数の方法があります。

CCITCPGW

以下のコマンドを発行して、動的にトレースをオンにします。

```
F CCISSLGW,T,SYSPRINT(SSL の場合)
```

```
F CCITCPGW,T,SYSPRINT(SSL 以外の場合)
```

以下のコマンドでトレースが無効になります。

```
F CCISSLGW,T,NOTRACE(SSL の場合)
```

```
F CCITCPGW,T,NOTRACE(SSL 以外の場合)
```

注: CCISSLGW 起動でトレースをすぐに開始するには、スターテッド タスク JCL に TRCPRINT DD ステートメントを追加します。非アクティブ化については、前述の通りです。

ローカル CAICCI

ローカル CAICCI のトレースには、以下のコマンドを発行します。

```
ENF CCI(LINT)
ENF CCI(PRINTT)
```

CAICCI Spawn

アプリケーションによっては、CAICCI 生成も必要となります。この機能を使用するすべての製品には、*Yourdeploy*HLQ.CAW0OPTN メンバ内の CCISPNPM メンバを更新するためのインストール手順が含まれます。

CAICCI 生成用のトレースをオンにするには、SPNDEBUG DD ステートメントを CAIENF プロシージャに追加します。

コンポーネントのトレース機能の準備

デフォルトでは、CAICCI は、CACCI という名のコンポーネントを使用してコンポーネントトレース機能を初期化します。環境は初期化されますが、MVS TRACE CT コマンドによってトレース機能は起動されている必要があります。

CAIENF Parm CCICT は、コンポーネントトレース環境(コンポーネント名を含む)のアクティブ化とカスタマイズに使用されます。コンポーネントトレース機能 parmlib のメンバ名は、トレース機能をアクティブ化するために CCICT コマンドで指定されます。parmlib メンバの設定についての指示については、「*Reference Guide*」を参照してください。

注: external writer プロシージャ名が parmlib メンバで指定されている場合、CAIENF/CAICCI を起動する前に external writer を設定する必要があります。「*Reference Guide*」のサンプル CCIXWTR プロシージャを参照してください。

CAICCI/PC - ワークステーション製品の使用

CAICCI Configurator の [Trace] タブにあるチェック ボックスを使用して、クライアント側でトレースを有効にできます。トレース出力は指定されたファイルに出力されます。トレースを無効にするには、ボックスのチェックを外します。

z/OS 側でトレースを有効にするには、以下のコマンドを発行します。

```
F CCISSL,T,SYSPRINT(SSL の場合)
```

```
F CCITCP,T,SYSPRINT(SSL 以外の場合)
```

以下のコマンドでトレースが無効になります。

```
F CCISSL,T,NOTRACE(SSL の場合)
```

```
F CCITCP,T,NOTRACE(SSL 以外の場合)
```

CA TCPaccess Communications Server for z/OS に関する考慮事項

スターテッド タスク CCISSL および CCISSLGW は、OE ソケットと IBM TCP/IP を使用して CA TCPaccess Communications Server for z/OS をサポートします。

接続開始に関する考慮事項

CAICCI は、潜在的接続の片側からのみ開始されると機能が向上する傾向があります。すべてのノードが他のすべての定義されたノードとの接続を試みるように CAICCI が設定されることもあります。これは通常、ネットワーク内で過度の接続試行が発生する原因となります。一般的に、Windows および UNIX マシンのような分散プラットフォームでメインフレームへの接続を開始し、メインフレームでは分散プラットフォームへの接続を開始しないようにすることをお勧めします。そのためには、分散ノードの CCIPARM で CONNECT ステートメントをコード化しないでください。デフォルトの Windows および UNIX REMOTE ステートメントでは、表示されたノードへの接続を確立しようと試みます。

メインフレーム同士の接続には、接続と関係するシステム 1 つだけで CONNECT ステートメントをコーディングすることをお勧めします。CONNECT ステートメントがコーディングされるシステムは、テスト指向のより強い（ダウンする可能性が高い）システムでなければなりません。システムが完全に対等である場合は、CONNECT ステートメントを使用するシステムをどれか 1 つ選びます。多数のノードが関わり、すべて相互に接続を要求しているときは、単にそれぞれのノードに番号をつけてから、各ノードにより大きな番号のノードへの接続ステートメントを持たせます。

CA Workload Control Center

このセクションでは、CA Workload Control Center の使用例を説明します。

メインフレームのスケジューリング エンジンとの接続に問題がある場合は、CAICCI 接続を確認します。

メインフレーム上のアプリケーションを検索する方法

1. 2 つの CAICCI が接続されていることを確認します。これには次の DOS コマンドを入力します。

   ```
   rmtcntrl status
   ```

   接続の現在のステータスが出力されます。

2. リストにコンピュータが表示されない場合は、ccirmtd.rc ファイルを確認する必要があります。
3. リスト内にコンピュータが INACT RETRY と表示される場合は、CCITCPGW または CCISSLGW タスクがアクティブであるかどうか、メインフレームを確認します。

   a. アクティブでなければ、次のコンソール コマンドを発行して起動します。

      ```
      ENF PROTOCOL(TCPIPGW)（SSL 以外の場合）
      ENF PROTOCOL(TCPSSLGW)（SSL の場合）
      ```

   b. アクティブであれば、ローカル PC の IP アドレスが表示され接続を試みているかどうか確認します。表示も接続の試行もされていない場合は、次のコマンドを発行してローカル コンピュータの CAICCI を再起動します。

      ```
      CCICNTRL STOP RMT
      CCICNTRL START RMT
      ```

4. CAICCI の再起動後、rmtcntrl ステータス コマンドを再発行します。このコマンドの出力でメインフレーム マシンが ACTIVE と表示された場合、アプリケーションが利用可能であることを検証しなければなりません。

   UEJM の場合は、アプリケーションのレシーバー名は SUBMITC サーバです。CAICCI のアプリケーションが利用可能かどうかを調べるには、次の DOS コマンドを発行します。

   ```
   CCII sysid
   ```

   sysid はメインフレーム SYSID です。
5. リストにレシーバー名が表示されていない場合は、アプリケーションは利用できません。アプリケーション タスクが実行されていることを確認してください。UEJM の場合は、CPS のスターテッド タスクです。

第 10 章: Event Management 設定

CA Common Services for z/OS コンポーネントをインストールして展開した後、展開したイベント管理を実行し、保守するために、いくつかの設定タスクが必要です。これらの設定タスクは「USS ファイル システムの展開 (126P.)」に記述されているように、作成された最初の展開(ソース zFS)ファイルに対して実行することを意図しています。

このセクションには、以下のトピックが含まれています。

Event Management PROFILE の確認と調整

展開されたシステムで、/cai/nsmem/PROFILE ファイルの内容を確認し、特に CAIGLBL0000、STEPLIB、および(RESOLVER_CONFIG と _BPXK_SETIBMOPT_TRANSPORT のように)追加された可能性がある TCP/IP 環境変数用の設定が正確であるかに注意します。この展開されたシステムに必要な調整を行います。

展開されたシステム上の GUI タスク用の D5II0065 再実行

展開されたシステム上で Java GUI を使用する場合、このシステム上で CNSMJCL メンバ D5II0065 を実行し、環境の変化を検出する必要があります。ジョブ内に使用されてる変数がこのシステムに対する正しい値を反映していることを確認します。

Event Management 設定スクリプトの実行

BPXPRMxx 内に Event Management zFS を含めるには、Event Management 用の新しいマウント ポイントを含めるためにユーザのシステム BPXPRMxx メンバを更新します。

BPXPRMxx メンバに新しいマウント ポイントを追加すると、システムが IPL されるときに、自動的にマウントが実行されます。

Event Management をインストールするように選択した場合、ご使用の特定のシステムに対して所定のファイルをカスタマイズするために設定スクリプトを実行します。

SMP/E ターゲット USS ファイルに対して fwsetup スクリプトを実行しなかった場合は、展開先のシステム上でそれをすぐに実行します。SMP/E ターゲットに対して fwsetup を実行した場合、より短いカスタマイズ スクリプト fwmigrat を実行する必要があります。これは応答を必要としません。

fwsetup スクリプトと fwmigrat スクリプトは両方とも、指定された Event Management ディレクトリ（デフォルトでは /cai/nsmem）にあります。

注: メッセージとプロンプトは、スクリプトを初めて実行する場合、スクリプトを再実行する場合、または再インストールする場合によって異なります。いずれの場合にもあてはまらない場合は、近いものを選択します。

Event Management 設定スクリプトの実行方法

1. 以前インストールされた Event Management の /etc/profile にある任意の Event Management 更新を削除（単にコメントを外すのではなく）します。
2. システム上の OMVS に移動し、Event Management ディレクトリに移動します。

   ```
   cd /cai/nsmem
   ```

3. 以下のコマンドでスクリプトを起動します。

   。 fwsetup

   注: fwsetup は、数多くのタスクを実行するため、完了までに時間がかかる場合があります。 テキスト プロンプトは、自動的には画面に表示されません。テキスト プロンプトを表示するには、セッションのステータスが RUNNING から INPUT に変わったときに、F10 キーを押して画面を更新します。更新キーは何度押してもかまいません。テキスト プロンプトが表示された場合は、応答を入力してから Enter キーを押します。デフォルトを受け入れる場合は、何も入力せずに Enter キーを押します。これらの手順を「CA Common Services installation has completed」と表示されるまで繰り返します。

   重要: プロンプトに応答するか、プロンプトのデフォルトを受け入れるとき以外、Enter キーは押さないでください。Enter キーを押した場合、テキスト プロンプトがバイパスされ、応答する値を選択できなくなります。この場合は、デフォルト値が使用されます。

   以下のメッセージが表示されます。

   ```
   Installing CA Common Services...

   Installing Event Management component...
   ```

4. Store and Forward をアクティブにするかどうかを選択します。

   他の Event Management ノードにアクセスできない場合、Event Management の Store and Forward 機能で失敗したイベントを保存して、後で転送できます。

   Store and Forward（デフォルト: y）

5. ルール ファイルを作成して特定のメッセージ アクションの使用を制限するか、すべてのユーザがメッセージ アクションを実行できるようにするかを選択できます。

   デフォルトでは UNIXCMD と UNIXSH メッセージ アクションがすべてのユーザによってこのノード（CAICCI 接続されていると想定した）にサブミットされるのを許可します。Event Management はこれらのメッセージ アクションが制限されるのを許可します。これらのメッセージ アクションのルールは、「caevtsec」と呼ばれるユーティリティによって管理されます。caevtsec の詳細については、「*Administration Guide*」を参照してください。

- 初めてインストールする場合:

  スクリプトに既存のルール ファイルがない場合、ルール ファイルを作成するかどうか決定する必要があります。

  ```
  Would you like to restrict the UNIXCMD and UNIXSH message actions for this host?

  These actions were not restricted in Unicenter release 1.5.(y/n) (default: n)
  ```

  選択したら、以下のメッセージが表示されます。

  ```
  Installing Star Server component...
  ```

- スクリプトを再インストールまたは再実行する場合:

  新しいルール ファイルを作成するか、既存のルール ファイルを使用するかを確認するメッセージが表示されます。

  ```
  A version of the Event Security rules file has been detected on your system.

  Answering y will preserve the original rules file (from the previous installation or upgrade) and will remove the restrictions of UNIXCMD and UNIXSH message actions for this host.

  Answering n (default) will assume the restrictions previously enacted.

  Would you like to recreate Event Security rules file? (y/n) (default: n)
  ```

  ルール ファイルを新規作成するように選択した場合、ルールが更新され、元のルール ファイルが保存されたことを示すメッセージが表示されます。

  ```
  The original rules file has been preserved as
  /cai/nsmem/opr/config/<nodename>/actnode.prf.sav
  ```

6. 環境変数を設定します。

   Event Management を使用するには、PATH や LIBPATH など、いくつかの環境変数を設定する必要があります。

   ユーザのログオン時に、システム ファイル etc/profile が、/cai/nsmem/PROFILE ファイルの Event Management 環境変数を自動的に設定するようにできます。

   - PROFILE ファイルの環境変数 UPDATE_ETC が Y(yes)に設定されている場合、/etc/profile が更新されて、PROFILE ファイルが自動的に実行されます。その後、EM 環境変数はユーザのログオン時に自動的に設定されます。
   - PROFILE ファイルの環境変数 UPDATE_ETC が N(No) に設定されている場合、/etc/profile は更新されず、すべてのユーザは EM 環境変数を手動で設定する必要があります。

- インストール中もインストール後も、PROFILE ファイル内の環境変数 UPDATE_ETC が設定されなかった場合、/etc/profile を更新するかどうかを確認するメッセージが表示されます。

  初めてのインストール時に、/etc/profile を更新して、ユーザのログオン時に変数を自動的に設定するかどうかを設定できます。

  ```
  Do you want to update /etc/profile? (y/n)
  ```

  - y (yes) を選択した場合、/etc/profile が更新され、すべてのユーザがログオン時に環境変数を設定できます。
  - n を選択した場合、いずれかのコマンドを発行する前に、tngprofile スクリプトを実行する必要があります。

  fwsetup スクリプトを再インストールまたは再実行する場合、/etc/profile が以前に更新されて PROFILE ファイルを実行したことが検出されると、以下のメッセージが表示され、/etc/profile を更新するオプションはバイパスされます。

  ```
  警告: /etc/profile has been previously updated. Please check the contents of
  /etc/profile to be sure the entry is valid for the current installation. If
  not, remove the update and re-run this fwsetup script.
  ```

  ```
  警告: /etc/csh.login has been previously updated. Please check the contents
  of the file to be sure the entry is valid for the current installation. If
  not, remove the update and re-run this fwsetup script.
  ```

7. 次のメッセージが表示されます。

   ```
   CA Common Services installation has completed.
   ```

8. fwsetup が正常に完了したことを確認します。
   - /etc/profile を更新するために y を選択した場合、Event Management の更新情報がこのファイルに挿入されています。
   - システムのノード名と同じ名前のサブディレクトリが /cai/nsmem/RW/config/ ディレクトリに存在することを確認してください。

イベント管理 GUI タスクの構成方法

イベント管理 GUI 要素を実行する予定がある場合は、以下のタスクが必須です。

1. UNIX System Services 環境を構成する。
2. Web サーバを構成して起動する。
3. 互換 Java 環境をインストールする。
4. イベント管理用のセキュリティ定義を検討する。
5. イベント管理 Java サーバを初期化する。

これらのタスクについては、この後の各セクションで説明します。

イベント管理用 UNIX System Services の構成

イベント管理では、USS が構成済みで、フル機能モードで稼働している必要があります。

BPXPARM メンバを確認する方法

1. 以下の USS 構成可能オプションが、少なくとも最小値に設定されていることを確認してください。

オプション	最小値
MAXPROCSYS	200
MAXASSIZE	128MB
MAXTHREADTASKS	200
MAXPROCUSER	100
MAXCPUTIME	86400

2. イベント管理の起動時には 3 つの POSIX 共有メモリ セグメントが作成されるので、IPCSHMNIDS パラメータがその要件を反映している必要があります。
3. 最大限のパフォーマンスを得るためには、必ず一時ファイルが TFS ファイル システムに割り当てられている必要があります。通常、イベント管理のインストールには、約 32MB の一時スペースが必要です。
4. BPXPRM メンバが zFS を起動していることを確認してください。FILESYSTYPE TYPE(ZFS) のエントリが含まれていることが必要です。

Web サーバの設定

Event Management GUI を使用するには、z/OS HTTP サーバが必要です。互換性のある HTTP、Java、および CGI スクリプト機能を備えていれば、任意の z/OS Web サーバを使用できます。Web サーバは、Event Management Java サーバがあるホストと同一のホスト上で稼働させる必要があります。

すでに z/OS 上で Web サーバを稼働させている場合、既存のサーバに CA Common Services for z/OS の定義を追加することができます。ただし、多くの場合、CA Common Services for z/OS の要求に対するサービス提供に特化した専用のセカンダリ Web サーバを稼働させることをお勧めします。

Web サーバを構成する際には、HTTPD 構成ファイルの更新または作成が必要になります。Event Management のインストール時に、$CAIGLBL0000/browser/httpd.conf（$CAIGLBL0000 はインストール先として選択したパス）内にサンプルが作成されます。このファイル内にある設定を確認してください。

以下の設定が必要です。

```
Exec            /scripts/*
Exec            /tngfw/scripts/*
Exec            /tng/scripts/*
Exec            /ubi/scripts/*
Exec            /ubifw/scripts/*
Pass            /tngfw/*
Pass            /tng/*
Pass            /browser/*
Pass            /UBIImages/*
Pass            /UBIImages/*
Pass            /ubi/*
Pass            /ubifw/*
Pass            /*
Pass            /*
```

ファイル $CAIGLBL0000/browser/httpd.conf.sample にあるすべての必要な Exec および Pass パラメータのリストを参照してください。

CA Common Services for z/OS 専用の Web サーバを稼働させている場合は、これらの構成オプションも指定する必要があります。

ステートメント	目的
Welcome tngfw.html	最初の CA Common Services for z/OS ページを定義します。
Port *nnnn*	指定された TCP/IP ポートにサーバを割り当てます。

Event Management HTML ファイルは、EBCDIC フォーマットで出荷されます。通常、z/OS Web サーバは、EBCDIC フォーマットの HTML ファイルを処理するように構成する必要があります。HTTPD 構成ステートメントを以下の例と同様にする必要があります。

```
AddType   .html   text/html   ebcdic   1.0
```

Event Management GUI は、機密リソースへのアクセスの際にユーザ認証とセキュリティ検証を実行します。しかし、Web サーバのセキュリティ オプションを見直したい場合も考えられます。CA Common Services for z/OS が必要とする特定の CGI スクリプトにはスーパーユーザ特権が必要であり、Web サーバが $CAIGLBL0000/browser/scripts で UID 0 を使用してスクリプトを実行するように構成されている必要があります。 この要件以外は、SSL、SAF、および証明書ベースの認証を含め、ご使用の Web サーバのマニュアルに概説されているセキュリティ機能を自由に使用できます。

$CAIGLBL0000/browser/scripts 内のスクリプトには、いくつかの環境変数を設定する必要があります。最大限のパフォーマンスを得るために、これらの変数を LE の envvar ファイル内に定義して、Web サーバの起動に使用することができます。Event Management をインストールすると、サンプルの環境変数ファイルが $CAIGLBL0000/browser/httpd.envvars に格納されます。このファイルを確認して、Web サーバの起動に使用される JCL の PARM= フィールドにこれを指定する必要があります。

Web サーバは、スターティッド タスクまたはバッチ ジョブとして実行することができます。CNSMPROC メンバである NSMWEBSV はモデルとして使用できます。CEE_ENVFILE 環境変数と関連付けられた DD カードの path ステートメントを /cai/nsmem/browser/httpd.envvars ファイルに設定し、/cai/nsmem/browser/httpd.conf 設定ファイルを使用していることを確認してください。

イベント管理に対するセキュリティ定義

イベント管理サーバは、ユーザがシステムに接続する際に認証を行い、個々のユーザに機密機能へのアクセスが許可されているか検査し、さらに代行をサポートすることによって、セキュアな環境を維持しています。メインフレーム上で起動されるすべてのトランザクションは、サーバではなく個々のサインオン済みユーザのセキュリティコンテキストを継承します。イベント管理サーバは、これらのセキュリティ インターフェースを外部セキュリティ製品との統合によって実施します。CA ACF2、CA Top Secret、および IBM の RACF が完全にサポートされています。

セキュリティ機能を実行するには、イベント管理サーバに特定のセキュリティ許可が必要です。これはご使用のセキュリティ製品、稼働させている z/OS のリリース、および実施しているセキュリティ ポリシーの詳細によって異なります。

以下の属性を持つ Java サーバおよび Web サーバ用のセキュリティ アカウントを作成してください。

- UID 0。Java サーバおよび Web サーバを稼働させるユーザ ID は、UID 0 を実際に定義する必要があります。0 以外の UID を割り当てて、そのユーザ アクセスに BPX.SUPERUSER リソースに対する許可を与えることはできません。
- 有効なグループ ID(GID)。
- 有効なホーム ディレクトリ(CA Common Services for z/OS のインストール先ディレクトリなど)。
- 有効なシェル プログラム(通常は「/bin/sh」)。
- IBM FACILITY リソースの BPX.SUPERUSER、BPX.DAEMON、および BPX.SERVER のいずれかに関する機能を実施する場合は、これらのリソースに対する READ 許可。
- オプションで、サーバによるパスワード チェックなしにサインオンさせるユーザに対する代理許可。

さらに、イベント管理のすべての実行可能プログラムと DLL ライブラリは制御されているプログラムとしてマークされている必要があり、また、特定の実行可能プログラムは APF 許可済みとマークされていなければなりません。イベント管理を zFS ディレクトリにインストールする場合は、インストール プロセスによって UNIX の extattr コマンドを使用して該当のファイルがマークされます。PDSE ライブラリにインストールする RACF ユーザは、すべてのイベント管理モジュールおよびライブラリを PADS 保護としてマークする必要があります。

これらの機能の実施方法の詳細については、ご使用のセキュリティ製品のマニュアルを参照してください。

Java サーバの初期化

CA Common Services for z/OS Event Management Java サーバは、$CAIGLBL0000/browser/scripts にある w2startup スクリプトを使用して稼働します。このスクリプトは、Event Management Java サーバを起動するもので、Java のインストール時に選択したディレクトリ名によっては次のような設定が必要になる場合があります。

- $CAIGLBL0000/browser/classes を Java CLASSPATH に追加する。

- Event Management と Java の実行可能プログラムを PATH に含める。
- Event Management と Java のライブラリ（DLL）のディレクトリを LIBPATH に含める。

これらの変数は、$CAIGLBL0000/browser/httpd.envvars ファイル内に設定されます。

w2startup スクリプトは、UNIX コマンドとして、または BPXBATCH 構文を使用したバッチ ジョブとして実行できます。CNSMPROC のサンプル メンバ NSMJSERV は、バッチ ジョブかスターティッド タスクとして実行できます。これは、本番稼動環境ではスターティッド タスクとして実行する必要があります。プロセス CaemRts およびプロセス CAEMRTA も w2startup によって開始されます。ジョブの STDOUT ファイルと STDERR zFS ファイルを参照して、このジョブのステータスを確認します。ジョブのリターン コードだけで正常に完了したと判断しないでください。

サーバの起動後は、以下の形式の URL で Web ブラウザ セッションを開始することによって、Event Management GUI にアクセスすることができます。

```
http://hostname:port
```

このとき、*hostname* はその Web サーバを稼働させるホストの名前または IP アドレスで、port は httpd.conf ファイルで割り当てたポート番号です。IP アドレスをハードコーディングせず、ホスト名を使用することを強くお勧めします。デフォルト ポートである 80 を受け入れる場合は、ポート番号を省略することができます。

GUI によってレポートされるノードを制限するには、ファイル $CAIGLBL0000/emsrvc/data/nodelist.sample を $CAIGLBL0000/emsrvc/data/nodelist にコピーし、レポート対象のノード名だけが含まれるようにそのファイルを編集します。これにより、GUI を表示するときのパフォーマンスが向上します。

Java サーバを終了するには、CNSMPROC ジョブ NSMJSTOP を実行するか、あるいは $CAIGLBL0000/browser/scripts にある w2kill スクリプトを USS から実行することができます。スクリプトはプロセス CaemRtS および CAEMRTA（5 つのインスタンス）を実行中のままにして、任意のリモート CA NSM マシンが z/OS 上の Event Management GUI にアクセスすることを可能にします。

ジョブの STDOUT ファイルと STDERR zFS ファイルを参照して、このジョブのステータスを確認します。ジョブのリターン コードだけで正常に完了したと判断しないでください。CaemRts および CAEMRTA プロセスをシャットダウンする場合は、CNSMPROC メンバ NSMSHRTS を実行します。

オプションの Event Management タスクの設定方法

ご使用の環境によっては、Event Management に関する以下のタスクが必要になります。

- Store and Forward のアクティブ化
- Berkeley syslog デーモンのセットアップ（必須）
- catrapd の有効化
- Event Management サーバの初期化
- OPSMVS EXIT のインストール
- emstart スクリプトおよび emstop スクリプトのカスタマイズ
- Event Management の複数システムへのインストール

複数のシステムでインストールする場合は、インストール方法を選択できます。

CAICCI をインストール済みの場合は、「CAICCI 設定タスク」の章の説明にあるように、CAICCI も設定して起動する必要があります。

注: Event Management の起動の詳細については、「*Administration Guide*」を参照してください。

ストア アンド フォワード

Store and Forward（SAF）機能は、ネットワークの問題やイベント マネージャが稼働していないなどの理由でターゲット ノードに即時配信できないメッセージを保管し、最終的に転送することによってメッセージの配信を保証します。Store and Forward は、$CAIGLBL0000/PROFILE ファイルの環境変数 INSTALLSAF=Y を設定およびエクスポートすることによりインストール時に有効化されます。

Store and Forward がアクティブであれば、イベント管理によってメッセージ配信機能もアクティブになることが保証されます。この機能がアクティブになっている場合、リアルタイムでの配信が不可能なメッセージは保管され、後ほど宛先アプリケーションが再び到達可能になった時点で自動配信されます。（配信不能メッセージは、デフォルトでは $CAIGLBL0000/opr/saf ディレクトリ内にあるファイルに保管されます。ファイル内のメッセージがすべて送信されると、このファイルは自動的に消去されます）。

SAF の適用対象ノードの限定

デフォルトでは、ストア アンド フォワードをアクティブにすると、すべてのノードでこの機能を使用することができます。SAF 機能を一部のノードに限定する場合は、それらのノード名をリストした設定ファイル（および必要に応じて、SAF ファイルのディレクトリ パス）を作成する必要があります。それ以降、リストされたこれらのノードのみが SAF の対象となります。SAF 構成ファイルが存在しているのに内容が空である場合は、どのノードにも SAF は適用されません。

テキスト エディタで、以下のサンプル SAF.CFG テンプレートを元に、特定のニーズを満たす SAF.CFG ファイルを作成します。

```
# Node                  Directory

#
  UGGP12                Dynamo
  UGIPP4                Pluto
  UXTTP1                Mercury
  UURET5                Neptune
```

SAF 構成ファイルの作成

メッセージの保存対象となるターゲット ノードをシステムに伝えるためには、SAF 構成ファイルを作成する必要があります。SAF 構成ファイルが存在しない場合、すべてのターゲット ノードがメッセージの保存対象になります。

SAF 構成ファイルを作成する方法

1. 作成したサンプル SAF.CFG ファイルを $CAIGLBL0000/opr/saf ディレクトリにコピーします。
2. SAF.CFG ファイルを以下のように編集します。
   - 各データ行の最初の位置には、SAF 機能を適用するマシン名（ノード）を指定します。この名前は最大で英数字 15 文字まで可能です。
   - 各データ行の 2 番目の位置で、SAF のルート下にあるディレクトリを指定します。このマシン（ノード）では、識別されたログ ファイルは、このディレクトリ経由でアクセスされます。
3. *編集済みファイルは*、SAF.CFG という名前で保管するか、固有のファイル名を選択します。

SAF インターバルの変更

保存されたメッセージが格納されたファイルがある場合、SAF デーモンは、指定された間隔に基づいて定期的にメッセージの再送信を試みます。この SAF 再試行の間隔(秒数)は変更できます。

SAF 間隔を変更する方法

1. $CAIGLBL0000/opr/scripts/envsetlocal ファイルを編集します。

   このファイルが存在しない場合は作成します。

2. このファイルに以下の行を追加します。

   ```
   CA_OPR_SAF_SCAN_INT=xx
   export CA_OPR_SAF_SCAN_INT
   ```

   このとき、xx は新しいスキャン インターバル(秒単位)です。

他のプラットフォームと z/OS との間で SAF を使用している場合は、該当のマニュアルで構成情報を参照してください。

他のタスクに対する Store and Forward の有効化

このタスクでは、OPSMVS など、他のタスクからの cawto、wto、またはその両方のメッセージに SAF を適用できるようにします。

OPSMVS または他のタスクの環境変数ファイルに、以下の環境変数を追加します。

```
export CA_OPR_SAF=Y
export CA_OPR_SAF_ROOT=$CAIGLBL0000/opr/saf
```

SNMP トラップを受信するための catrapd 有効化

Unicenter NSM には、SNMP トラップを送受信する機能があります。受信したトラップはイベント管理コンソールに表示されます。

トラップを受信するためには、デーモン catrapd が実行中でなければなりません。デフォルトでは、このプロセスはポート 161 で受信待機します。TCP/IP プロシージャには、予約されているポート番号を含む PROFILE DD があります。

SNMP メッセージを他のコンソールからルーティングするには、ポート 161 を使用可能にして catrapd を有効にする必要があります。

デフォルトのポートを使用して catrapd を有効化する方法

TCPIP プロファイル（TCPIP プロシージャ内の PROFILE という DD ステートメントで使用されるデータセット）を変更して以下のようにします。

- ポート 161 が OSNMPD（SNMP エージェント）用に予約されていない。
- AUTOLOG が OSNMPD を起動しない。

デフォルト以外のポートを使用して catrapd を有効化する方法

ポート 161 が使用できない場合は、$CAIGLBL0000/snmp/scripts ディレクトリの envset スクリプトに以下の 2 行を追加します。

```
CAICATD0001=nnn
export CAICATD0001
```

注: CAICATD0001=*nnn* は 待ち受け（listen）するポート番号です。*nnn* は実際のポート番号に置き換えてください。

catrap プログラムを使用してトラップを送信することができます。このコマンドの構文については、*Reference Guide*」で説明します。

Event Management プロセスの起動と停止

CA Common Services for z/OS Event Management サーバは、CNSMPROC メンバの NSMEMSTR を使用して起動します。このサーバは、バッチ ジョブかスターティッド タスクとして実行できます。これは、本番稼動環境ではスターティッド タスクとして実行する必要があります。 このジョブは、emstart スクリプトを起動して、Event Management に関する 4 つのデーモン（caiopr、logrdr、ca_calendar、stardaemon）を開始します。デフォルトでは、catrapd デーモンは開始されません。catrapd デーモンを開始する場合は、スクリプト /cai/nsmem/opr/scripts/emstart の「unicntrl start snmp」コマンドのコメントを解除してください。使用するコンポーネントだけが起動されるように、これらのスクリプトをカスタマイズします。不使用のコンポーネントをコメント化してください。

Event Management デーモンは、emstop スクリプトを起動して、CNSMPROC メンバの NSMEMSTP を使用して停止します。NSMEMSTP は、バッチ ジョブかスターティッド タスクとして実行できます。これは、本番稼動環境ではスターティッド タスクとして実行する必要があります。スクリプト /cai/nsmem/opr/scripts/emstop を編集して、emstart スクリプトによって開始されたプロセスと同じプロセスを停止します。

ジョブの STDOUT ファイルと STDERR HFS ファイルを参照して、このジョブのステータスを確認します。ジョブのリターン コードだけで正常に完了したと判断**しないでください**。

このジョブに割り当てられるユーザ ID は、UID 0 が割り当てられていると共に、BPX.DAEMON、BPX.SUPERUSER、BPX.SERVER の各機能（FACILITY）へのアクセス権を有している必要があります。

OPSMVS EXIT のインストール

イベント管理を使用して OPSUSS メッセージを処理する場合は、OPS ジョブ INSTUSEX を実行して、イベント管理の OPS EXIT をインストールする必要があります。

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

Berkeley syslog デーモンのセットアップ

イベント管理では、Berkeley syslog デーモンによる強力なメッセージング機能を利用することができます。このデーモンは、以下のような処理に使用することができます。

- メッセージのいくつもの優先度、レベル、および機能から選択する
- レベルまたは優先度により、異なるデバイスにメッセージをルーティングします。
- レベルまたは優先度により、異なるホストにメッセージをルーティングします。
- ほかのホストからメッセージを受け取ってローカル表示します。

Berkeley syslog デーモンの構成オプションは、通常、/etc/syslogd.conf ファイルに以下の形式で指定します。

```
selectoraction
```

- **selector** - メッセージのタイプを指定します。
- **action** - セレクタが送られる場所を示します。

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

サンプル syslogd 構成ファイル

エンタープライズ管理が単一のホストにインストールされている場合の syslogd 設定ファイルの例を以下に示します。

```
# @(#) $Revision:  66.1  $
#
# syslogd configuration file
#
# See syslogd(1M) for information about the format of this file
#
mail.debug       /usr/spool/mqueue/syslog
*.info,mail.none /usr/adm/syslog
*.alert          /dev/Event
*.alert          root
*.emerg          *
*.info           /cai/nsmem/opr/config/abcfred/pipe/oprpipexxxx
```

注: CAIGLBL0000 が /cai/nsmem、かつ現在のノード名が abcfred である場合、上記のエントリは *.info をイベント管理にルーティングします。**.info* に対するエントリは、caiopr プロセスの起動時に自動的に追加されます。

リモート ホストへのメッセージの転送

z/OS 上のイベント管理は、互換性のある BSD syslog サービスが稼働している任意のリモート システムから syslog メッセージを受け入れる事ができます。

すべてのメッセージをリモート マシンにルートするように syslog デーモンを設定するには、syslogd 設定ファイルを編集して、アクション部分の行にリモート ホスト名を挿入します。この際、ホスト名の頭にはアットマーク(@)を付けます。

注: syslog デーモンは DNS(ドメイン ネーム サービス)を使用しているため、受信側ホストのホスト名と IP アドレスの正しい定義に依存します。

例: 以下の syslogd 構成エントリは、ローカル ノードから情報メッセージ以上の優先度を持つすべてのメッセージを titan というリモート ホストにルーティングする例です。

```
# @(#) $Revision:  66.1  $
#
# syslogd configuration file

# See syslogd(1M) for information about the format of this file

mail.debug       /usr/spool/mqueue/syslog
*.info,mail.none /usr/adm/syslog
*.alert          /dev/Event
*.alert          root
*.emerg          *
*.info           /cai/nsmem/oprconfig/abcfred/pipe/oprpipexxxx
*.info           @titan
```

注: syslogd 構成ファイルには、フィールド区切り文字として、スペースのほかにタブが含まれています。通常、最初の列と 2 番目の列の区切りには、タブとスペースの両方が使用されます。syslog デーモンがその行を無視するか、不適切な結果を引き起こすことになるため、ブランクのみを使用してフィールドを区切らないようにしてください。

別のホストにもメッセージを送るには、必要に応じて行を追加します。一定の優先度または一定の機能のメッセージに制限する場合は、コマンド ラインの最初の部分でこれを指定してください。メッセージの選択とルーティングの詳細については、syslogd の man ページを参照してください。

変更の有効化

syslogd 構成の更新を有効にするには、syslog デーモンを停止して、root ID から再起動する必要があります。

変更をアクティブ化する方法

1. 以下のコマンドを入力して syslog デーモンを停止します。

   ```
   kill -15 `cat /etc/syslog.pid`
   ```

2. 以下のコマンドを入力して syslog デーモンを再開します。

   ```
   /usr/sbin/syslogd -f /etc/syslogd.conf
   ```

   この /etc/syslogd.conf は、syslogd 構成ファイルの名前です。

emstart スクリプトおよび emstop スクリプトのカスタマイズ

emstart スクリプトおよび emstop スクリプトは、以下のディレクトリに格納されています。

```
/cai/nsmem/opr/scripts
```

emstart および emstop は、イベント管理の起動スクリプトおよび停止スクリプトです。使用するコンポーネントだけが起動されるように、これらのスクリプトをカスタマイズします。不使用のコンポーネントをコメント化してください。

起動手順

CNSMPROC メンバ NSMEMSTR を使用して Event Management を起動します。デフォルトでは、これにより caiopr、logrdr、stardaemon、ca_calendar、newdaylog、および caidoc プロセスが起動されます。Event Management を正しく停止させるには、CNSMPROC メンバ NSMEMSTP を使用する必要があります。これらのジョブは両方とも、/cai/nsmem/opr/scripts ディレクトリにあるスクリプトを実行します。スクリプトを編集し、起動する必要のあるコンポーネントのみを含めることができます。

以下の起動に関する考慮事項にご注意ください。

- すべてのプロセスは UID(0) で開始され、プロセスが起動される前に CAICCI がアクティブでなければなりません。Event Management を CAIENF autocmd の一部として起動し、CAICCI が完全に初期化されたことを確認できます。
- stardaemon は追加サービスを必要としません。

- caiopr daemon にはリポジトリを使用するオプションがあります。Message Action および Calendars のどちらか、または両方の定義が必要な場合、リポジトリが必要です。リポジトリは Event Management の前に開始される必要があります。caiopr を 起動する前に、PROFILE ファイル内の STEPLIB 環境変数および CA_OPR_ZOSDB 環境変数が正しく設定されていることを確認してください。

  CA OPS/MVS Event Management and Automation を排他的に使用してメッセージのプロセスを行う場合は、リポジトリは必要ありません。caiopr を起動すると、メッセージを再ロードできないというリポジトリへの接続に関する警告メッセージが表示される場合がありますが、caiopr のプロセスは通常に継続されるため警告は無視してもかまいません。

- Event Management に割り当てられるユーザ ID は UID(0) でなければなりません。これは、Event Management ユーザ ID から、サインオンしたクライアントのユーザ ID にユーザを切り替えるために必要です。これにより、通常クライアントには入力が許可されない CA NSM コンソールへのコマンドを、クライアントが発行するのを防ぐことができます。

- SNMP トラップ リスナーの catrapd を起動する必要がある場合は、/cai/nsmem/opr/scripts/emstart ファイル内で以下の行を見つけて、行頭からシャープ記号(#)を削除します。

  ```
  #unicntrl start snmp
  ```

  削除した後は、該当する行は以下のようになります。

  ```
  unicntrl start snmp
  ```

Java GUI

このセクションでは、GUI 通信に関する考慮事項について説明します。

Timeout の設定

以下の設定は、GUI による応答待機時間の長さを制御します。

TIMEOUT=300

CAICCI に 300 秒の待機を指示します。この値は /cai/nsmem/browser/scripts/w2startup ファイルの終わり近くのところに設定されています。

PersistentServerTimeout

Java の TIMEOUT コマンドを使用して設定される、レジストリ設定です。このコマンド自体が、GUI が応答待機する秒数を表示します。パラメータの受け渡しにより、渡されたものに対して設定が変更されます。

タイムアウトのメッセージが表示され続ける場合は、TIMEOUT パラメータをさらに高く変更することにより、これらの設定値を上げてください。

セキュリティの要件

組み込みセキュリティ チェックにより、定義されたリソースが不明なソースによって変更されることを防ぎます。それらのリソースが保護されるように、セキュリティ システムに対してリソースを定義する必要があります。すべてのリソースは、単一のクラス CAIUNI に対して定義されます。ここでは、各リソースについて説明します。

EMSRVC.MSGRECORD

メッセージ レコードを定義/変更するアクセスを制御します。

EMSRVC.MSGACTION

メッセージ アクション レコードを定義/変更するアクセスを制御します。

EMSRVC.CALENDAR

カレンダを定義/変更するアクセスを制御します。

EMSRVC.CONLOG

CA NSM コンソール ログへのアクセスを制御します。

EMSRVC.ANNOTATION

CA NSM コンソール ログのコメント機能へのアクセスを制御します。

これらのリソースへのアクセスを許可するには、読み取りアクセス権が必要です。

エンタープライズ管理

エンタープライズ マネジメント アイコンは、CA NSM または CA Common Services で実行されていることが一覧できるすべてのマシンを表示します。

EMSRVC_ROUTER_U レシーバーを見つけるには、CAICCI を照会します。

見つかったそれぞれのマシンで、APPMAP の取得が試行されます。マップがロードされない場合は、マシンがリストから削除されています。

リストの表示数を制限するには、/cai/nsmem/emsrvc/data ディレクトリにノードリストを作成します。nodelist.sample ファイルをサンプルとして使用できます。リストに記載するノードを選択するには、該当するマシンの CAICCI SYSID を入力します。ローカル マシンもリストに含める必要があります。

Web サーバ設定

インストール手順では、Java GUI の実行に必要なすべての情報を含む構成定義ファイルを作成します。Web サーバの動作に影響を与えるオプションは数多くありますが、ここでは一部のオプションについてのみ説明します。

Web サーバの詳細については、ご使用のオペレーティング システム リリース用の IBM のマニュアル「*IBM HTTP Server*」を参照してください。

Web サーバがすでに実行されている場合は、そのサーバから複数のアプリケーションをサポートするか、そのうち 1 つアプリケーションのポート番号を変更できます。

ポート番号を変更するには、構成ファイルを編集して Port オペランドを変更します。

CA Common Services を既存の Web サーバにマージするには、以下を構成ファイルに追加する必要があります。

```
ServerRoot    /cai/nsmem/browser    イベント管理のインストール パスを含みます。
HostName      yourhostname          コンピュータのホスト名です。
Port          80                    接続先のポート: デフォルト値は 80 です。

#
# ユーザがシステムに接続すると Java サーバで認証が行われるため、
# デフォルトのフレームワーク構成では Web サーバ内のセキュリティが
# 指定されません。 (以下の)NOSEC の定義は、(特定の個々のコンテ
# クストとは反対に)Web サーバのセキュリティ コンテクストにおいて
# アクセスの発生を許可します。
#
Protection NOSEC {
                  ServerId        TNGFW_Server
                  AuthType        Basic
                  PasswdFile      %%SAF%%
                  UserID          %%SERVER%%
                  Mask            Anonymous
                 }
Protect             /scripts/*        NOSEC %%SERVER%%
Protect             /tngfw/scripts/*  NOSEC %%SERVER%%
Protect             /tngfw/*          NOSEC %%SERVER%%
Protect             /tng/*            NOSEC %%SERVER%%
Protect             /browser/*        NOSEC %%SERVER%%
#
# 以下の指示は、フレームワーク ディレクトリのロケーションを特定
# します。 フレームワークを既存のウェブ サーバに統合する場合は、これらの
# ステートメントに既存の HTTPD 構成ファイルが含まれている必要
# があります。
#
Exec          /scripts/*          /cai/nsmem/browser/scripts/*
Exec          /tngfw/scripts/*    /cai/nsmem/browser/scripts/*
Exec          /tng/scripts/*      /cai/nsmem/browser/scripts/*
Exec          /ubi/scripts/*      /cai/nsmem/browser/scripts/*
Exec          /ubifw/scripts/*    /cai/nsmem/browser/scripts/*
Pass          /tngfw/*            /cai/nsmem/browser/*
Pass          /tng/*              /cai/nsmem/browser/*
Pass          /browser/*          /cai/nsmem/browser/*
Pass          /UBIImages/*        /cai/nsmem/browser/images/*
Pass          /UBIImages/*        /cai/nsmem/browser/images/*
Pass          /ubi/*              /cai/nsmem/browser/*
Pass          /ubifw/*            /cai/nsmem/browser/*
Pass          /*                  /cai/nsmem/browser/*
Pass          /*                  /cai/nsmem/browser/*
#
```

```
Logging:
#           -- ロギングを有効にするには、以下の行のコメント設定を解除します  --
#  AgentLog          logs/Agent
#  AccessLog         logs/httpd-log
#  CgiErrorLog       logs/cgi-errors
#  ErrorLog          logs/httpd-errors
#  TraceLog          logs/jttrace
```

ステートメントの完全なリストは、/cai/nsmem/browser/httpd.conf ファイルに記載されています。ステートメントを既存の Web サーバ構成ファイルにコピーし、貼り付けることができます。

インストールの確認

イベント管理は、以下で構成されています。

- メッセージの処理、カレンダ、リモート サーバなどの、機能コンポーネントを構成するプロセス。
- 表示するメッセージと実行するアクションの追加、カレンダの作成、イベントコンソールの表示などの機能を持つ GUI インターフェース。

すべてのサイトで両方の検証プロセスが必要とされるわけではありません。

プロセスの実行の検証

CNSMPROC メンバ NSMEMSTR を使用して機能コンポーネントを起動できます。このジョブを開始した後、以下のコマンドを発行します。

```
D OMVS,A=ALL
```

少なくとも caiopr、newdaylog、caidoc および logrdr プロセスがすぐに実行されます。必要に応じて ca_calendar、stardaemon、oprsafd および catrapd も実行することができます。

GUI インターフェース サーバがアクティブであることの検証

GUI インターフェースでは、httpd サーバがアクティブで、かつ Java バックエンド サーバが起動および実行されている必要があります。まだ起動されていない場合は、CNSMPROC メンバ NSMWEBSV を使用して httpd サーバを起動することもできます。新しいサーバのセットアップや既存サーバへのマージの詳細については、「Java GUI (P. 215)」を参照してください。

Java サーバの起動

CNSMPROC メンバ NSMJSERV を使用して Java サーバを起動できます。システム コンソールに表示される以下のメッセージは、起動が完了したことを示します。

```
CAxx506I – TNG Root Processes Initialized
```

この時点では、OMVS は CaemRtS、CAEMRTA（5 インスタンス）、logonserver.exe、EMserver.exe を処理し、w2Tree が実行されている必要があります。

GUI への接続

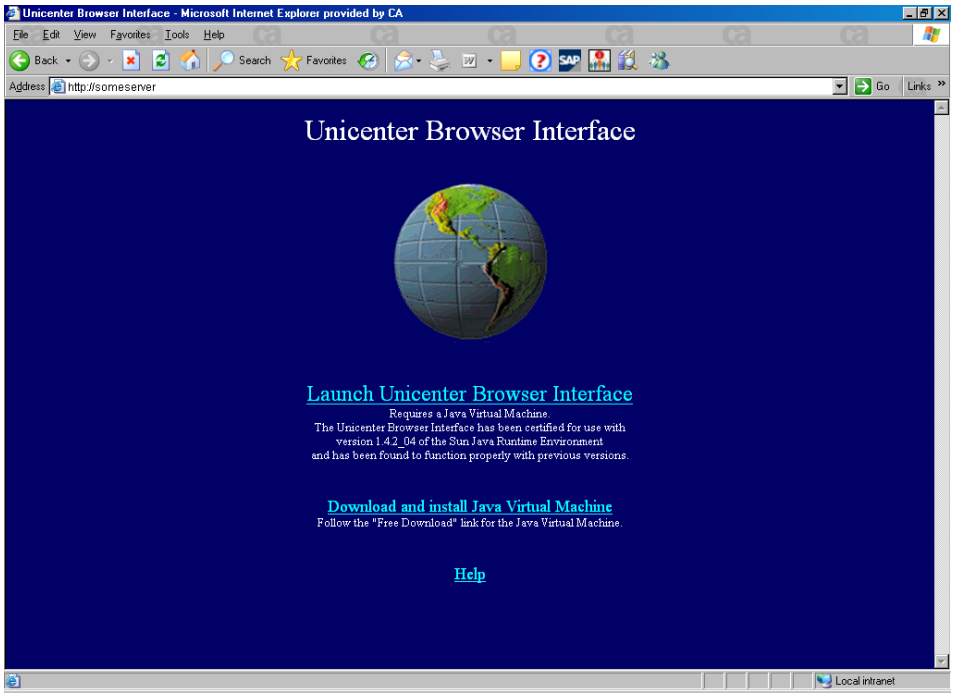
GUI に接続する方法

1. ブラウザを起動して以下の URL を入力すると、ウェルカム ページが表示されます。

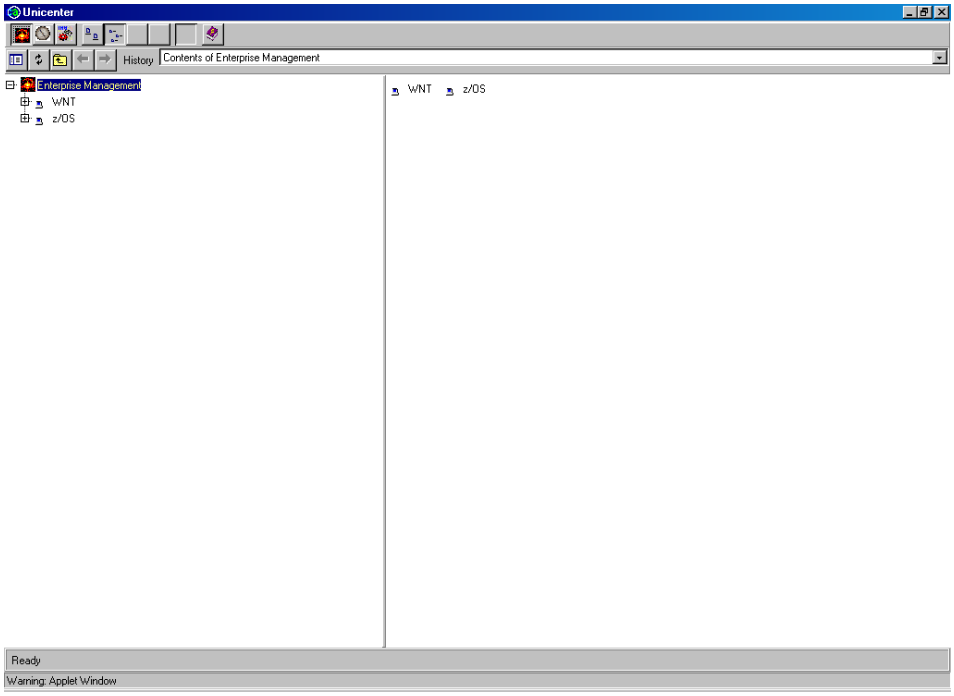
   ```
   http://hostname:port
   ```

   ウェルカム ページが示されます。

2. [Click Here] を選択して CA NSM ブラウザ インターフェースを起動します。



3. メインフレーム ユーザ ID とパスワードを入力します。
4. [OK] をクリックすると、メイン CA NSM GUI が表示されます。



追加システムへの Event Management の展開

最初の展開システムに加えて他のシステム上でも Event Management を実行する場合は、最初の展開システムから追加のシステムに zFS ファイルをコピーします。最初の展開（ソース zFS）ファイルはすでに設定されています。新規展開には、システム固有の設定が若干必要になります。

重要: 最初の展開ファイルを設定し、この章の以前の手順をすべて完了するまで、以下の手順を実行しないでください。

Event Management を追加システムに展開する方法

1. READ ONLY および READ/WRITE zFS のマウント ポイントがソース システムとターゲット システムで同じであることを確認します
2. （Calendars または Message Actions を使用していない場合、この手順をスキップします）。Calendars または Message Actions を使用している場合は、「*CA Datacom/AD Installation Guide*」を参照してください。ターゲット システムで Event Management を使用するには、あらかじめリポジトリのアドレス空間および JAVA GUI を起動します。

起動時にエラー メッセージが表示されるのを回避するために、Event Management コンポーネントを起動する前に、リポジトリを初期化します。

リポジトリのアドレス空間は、長時間実行のバッチ ジョブまたはスターティッド タスクとして起動する必要があります。リポジトリ アドレス空間が実行されていない場合、caiopr デーモンは起動しますが、Calendars デーモンは起動しません。

3. ターゲット システム上でシステム要件が満たされていることを確認します。
4. まだ行っていない場合は、ソース システム上で両方の Event Management zFS ファイルをバックアップします。
5. 共有 DASD を使用するか、データ セットをコピーして、BASE CAW0LOAD および CAW0PLD、および MFNSM CNSMLOAD、CNSMPLD, CNSMPROC、および CNSMJCL の区分化データ セットをアクセス可能にします。
6. CA Common Services が新システム上の /etc/ プロファイルで行った変更を確認して、適切な CAIGLBL0000 および STEPLIB を使用していることを確認します。正しい CAIGLBL0000 および STEPLIB が使用されていないセクションは必要に応じて削除してください。こうした変更は、以前のインストールで残ったものである可能性があります。

7. 新規システム上に新規 zFS データ セットを割り当て、以前保存された Event Management zFS バックアップを新規作成された zFS データ ストアにリストアします。読み取り専用 zFS および読み取り/書き込み zFS をマウントします。

   以下の箇条書きをよく読み、適切なマウント基準を見極めます。必ずターゲット システム上の BPXPRMxx メンバを更新して、読み取り/書き込み zFS（MODE RDWR）および 読み取り専用 zFS（MODE READ）の MOUNT ディレクトリを追加してください。

   - ターゲット システムで Java GUI を使用する場合、読み取り専用 zFS は読み取り/書き込みとしてマウントし、読み取り/書き込み zFS は 読み取り/書き込みとしてマウントします。次に、システム上でバッチ *yourdeployHLQ*.CNSMJCL ジョブ D5II0065 を実行して、Java GUI のいくつかのシステム固有の情報を確立します。
   - READ ONLY zFS を読み取り専用または 読み取り/書き込みとして、読み取り/書き込み zFS を 読み取り/書き込みとしてマウントします。ターゲット システム上でバッチ *yourdeployHLQ*.CNSMJCL ジョブ D5IFWMIG を実行します。その後、新システム用の必要なシステム固有ディレクトリが作成されます。STDOUT および STDERR で結果を確認します。読み取り専用 zFS がマウントされた読み取り専用である場合は、STDERR ファイル内の情報メッセージを無視します。新システム上で任意のジョブを実行する前に、Event Management タスクがすべてシャット ダウンされている（前リリースと同様）ことを確認します。

8. リポジトリのアドレス空間を開始する場合は、スターティッド タスクまたはバッチ ジョブを新しいシステムにコピーします。JCL/PROC に適切なデータセットとライブラリが指定されていることを確認します。

9. JAVA GUI を使用する場合は、以下の属性で、Java および Web サーバのセキュリティ アカウントを作成します。

   - UID 0 - 実 UID 0 で、Java サーバおよび Web サーバを実行するユーザ ID を定義します。UID がゼロ以外のユーザには、BPX.SUPERUSER リソースへのアクセスが拒否されます。
   - 有効なグループ ID（GID）。
   - 任意の有効なホーム ディレクトリ。適切な選択は、z/OS に対してインストールするディレクトリです。
   - 有効なシェル プログラム（通常は /bin/sh）。
   - IBM FACILITY リソースの BPX.SUPERUSER、BPX.DAEMON、および BPX.SERVER のいずれかの機能を実行する場合は、それらのリソースに対する READ 許可。オプションで、サーバのパスワード確認なしにユーザのサイン オンを許可する、代理許可を割り当てます。

10. JAVA GUI を使用する場合は、Web サーバおよび Java サーバのスターティッド タスクまたはバッチ ジョブを新しいシステムにコピーします。
11. http://*<host_name>:<port_number>* 形式の URL で Web ブラウザ セッションを開始して、Event Management GUI にアクセスします。ここで、「*host_name* 」は Web サーバを実行するホストの名前たは IP アドレスで、「*port_number*」は httpd.conf ファイルで割り当てられた番号です。ハードコードされた IP アドレスではなく、ホスト名を使用します。デフォルト ポートである 80 をそのまま使用する場合は、ポート番号を省略できます。

Event Management メンテナンスに関する考慮事項

Event Management および Event Management ユーティリティは、複数の異なる SMP/E ターゲット ライブラリにインストールされます。

- CNSMLOAD や CNSMPLD ロード ライブラリなどの従来からの PDS および PDSE データ セットは変更されます。JCL の CNSMJCL および CNSMPROC ライブラリも変更される可能性があります。
- 2 つの USS zFS データ セット。
  - 実行可能ファイル、スクリプト、HTML、および Java クラス ファイルを含む、読み取り専用の zfs 集合体。
  - システムの Event Management ログ ファイル、一時ファイル、および設定ファイルなどのシステム固有情報を含む、読み書き可能な zfs 集合体。

新しいサービス パックが利用可能になったとき、実行中のシステムを中断させずにメンテナンスを実行するためには、以下の手順に従います。

重要: 絶対に SMP/E ターゲット ライブラリを実行可能コードとして使用しないでください。常に SMP/E ターゲット ライブラリを少なくとも一度展開し、展開されたデータ セットを使用可能にします。

1. SMP/E 環境から実行されている CA Common Services コンポーネントがないことを確認します。
2. SMP/E DDDEF が正常で、最初にインストールした状態から変更されていないことを確認します。
3. SMP/E インストール時に使用されるのと同じポイントに SMP/E ターゲット USS zfs データ セットが RW 用としてマウントされていることを確認します。
4. SMP/E ターゲットに通常どおりメンテナンスを RECEIVE および APPLY します。
5. 本稼働 HLQ およびマウント ポイントからの別の HLQ およびマウント ポイントを使用して、SMP/E Read-Only zFS を本稼働システムへ再展開します。RW zFS は再展開しません。
6. 実行中のライブラリに対し事前メンテナンス ジョブ CNSMJCL (EMPREMT) を実行して、本稼動設定を保存します。 本稼働マウント ポイントを指すように、スクリプトを編集します。
7. まだ実行されていなければ、新規展開 Read-Only zFS をその一意のマウント ポイントにマウントします。
8. 実行中のライブラリからポスト メンテナンス ジョブ CNSMJCL (EMPOSTMT) を実行して、設定をリストアします。本稼働マウント ポイントおよび新規展開 USS zFS データ セット マウント ポイントの両方を参照するように、スクリプトを編集します。
9. EMPOSTMT スクリプトが完了すると、以下の操作を実行できます。
   a. 新規展開 zfs データ セットをマウント解除します。
   b. 実行中の製品をシャットダウンします。

c. 実行中の本稼働 zfs データ セットを両方ともマウント解除します。

d. 以前本稼働に使用されたのと同じマウントを使用して、すべての新規展開 RO データ セットを本稼働としてスワップ インします。既存の RW 本番環境データ セットを、その本環境マウント ポイントにマウントします。

10. SYS1.PARMLIB(BPXPRMxx) メンバは変更を必要としません。これは、zFS データ セットが以前使用されたのと同じマウント ポイントにマウントされるためです。

第 11 章: Agent Technology 設定

CA Common Services for z/OS をインストールして展開した後、展開された Agent Technology の開始準備が整うまで、タスクがいくつか残ります。

展開された Agent Technology 用のマウント ポイントを含めるためシステムの BPXPRMxx メンバを更新することにより、BPXPRMxx 内に Agent Technology zFS ファイルを含めます。

BPXPRMxx メンバに新しいマウント ポイントを追加すると、システムが IPL されるときに、自動的にマウントが実行されます。

このセクションには、以下のトピックが含まれています。

zFS システムでのプロファイル、スクリプト、および構成ファイルのカスタマイズ

Agent Technology を起動するには、zFS システム内の以下のファイルをカスタマイズしておく必要があります。

ファイル	タイプ	目的
agentworks.profile	プロファイル ファイル	CA Common Services for z/OS Agent Technology の実行に必要な環境変数を含む。
install_mibs	スクリプト ファイル	システムで使用予定の MIB をロードする。

ファイル	タイプ	目的
quick.cfg	設定ファイル	分散サービス バスとそのパートナ（aws_sadmin、エージェントなど）との間の通信に使用できるプロトコルを記述する。
aws_sadmin.cfg	設定ファイル	メインフレームトラップを受信する各リモート システムを識別する。
aws_snmp.cfg	設定ファイル	aws_sadmin サービスや SNMP ツールから使用できる UDP パラメータを記述する。

プロファイル ファイルの編集： /cai/agent/agentworks.profile

以下の環境変数は、ご使用のシステムを反映した値に設定する必要があります。

環境変数	説明
AWORKS_MVS_PREFIX	Agent Technology のデータセットに使用されるデータ セットの上位プレフィクス。これは、インストール スクリプトの実行時に CAI 変数に割り当てられた値と同一であることが必要です。
AGENTWORKS_DIR	zFS システム内で Agent Technology のファイルがインストールされるディレクトリを定義するフル パス名。これは、インストール スクリプトの実行時に AWORKDIR 変数に割り当てられた値と同一であることが必要です。
RESOLVER_CONFIG	TCP/IP 構成情報データセットの名前。これは、TCPIP プロシージャで SYSTCPD DD データ セットに割り当てられている値と同じである必要があります。データセットが PDS である場合は、メンバ名が含まれている必要があります。
_BPXK_SETIBMOPT_TRANSPORT	特定の TCP/IP スタック トランスポートのジョブ名に対して、明示的な親和性を持つ Agent Technology が確立されます。
AWS_STARTER_REQUEST	awservices プロセスに要求を出すために内部で使用される TCP/IP ポート番号。デフォルトは 9990 です。
AWS_STARTER_CONTROL	エージェントがアクティブなままで、awservices プロセスにサービスの制御を可能にする TCP/IP ポート番号。デフォルトは 9991 です。

環境変数	説明
TZ	ご使用のタイムゾーン。デフォルトは EST5EDT です。
AW_MAX_LOGSIZE_K	さまざまなログ ファイルの最大サイズ。デフォルトは MAX（ご使用のファイル システムで許容される最大サイズ）。指定可能な値は、ファイル サイズをキロバイト単位で示す整数値（たとえば最大サイズが 10 MB の場合は 10000）です。
AW_AUTO_START	awservices プロセスが実行されていない場合に、start コマンド オプションを使ったシェルから開始された他のサービスまたはエージェントが、awservices を暗黙的に開始できるかどうかを制御する変数。デフォルト値は ON です。

aws_sadmin プロセスによる統計情報の収集は、以下の 4 つの環境変数によって制御されます。この情報は、awsAdmin MIB で保持され、MIB ブラウザ ツールを使用して閲覧できます。aws_sadmin がこれらの統計情報を更新する際に消費される CPU 時間は、ベンチマーク テストの結果、40% 程度になることがわかっています。

環境変数	説明
AW_ADMIN_STAT_AGENT	awsAdminAgentTable テーブルに格納された統計情報を制御する。OFF に設定した場合、awsAdminAgentResponseAvg 変数は値 0 を返します。デフォルト値は ON です。
AW_ADMIN_STAT_SNMP	awsAdminSnmpGroup グループ内のすべての変数を制御する。OFF に設定した場合、グループのすべての変数は常に値 0 を返します。NOTOTAL に設定した場合、awsAdminSnmpInRequestsTotal 変数のみ累積されなくなります。この変数は、GET、GETNEXT、SET のすべての要求の合計を表します。デフォルト値は ON です。
AW_ADMIN_STAT_PERF	awsAdminPerfGroup グループ内のすべての変数を制御する。OFF に設定した場合、グループのすべての変数は値 0 を返します。デフォルト値は ON です。
AW_ADMIN_STAT_SOURCE	awsAdminSourceTable テーブル内のすべてのエントリを制御します。OFF に設定した場合、このテーブルには empty と表示されます。デフォルト値は ON です。

agentworks.profile の実行

Agent Technology ユーティリティを実行する前に、まず agentworks.profile ファイルを明示的に実行して、現在の環境を記述した変数に正しい値を割り当てる必要があります。

注: agentworks.profile ファイルは、Agent Technology コンポーネントで提供されるすべてのスクリプトによって自動的に実行されます。

agentworks.profile を実行する方法

1. USS でシェル セッションを開始します。
2. 現行ディレクトリを AGENTWORKS_DIR 環境変数によって定義されるディレクトリに設定します。

   ```
   cd /cai/agent
   ```

3. agentworks.profile スクリプトを起動します。

   ```
   . agentworks.profile
   ```

   注: 最初のピリオドに続くスペースは省略しないでください。

これで、Agent Technology ユーティリティを実行できます。

スクリプト ファイルの編集: /cai/agent/services/tools/install_mibs

選択した MIB を ldmib エントリに反映し、MIB の代替手段を選択します。

スクリプト ファイルを編集する方法

1. ldmib エントリを確認し、システムで使用する予定の MIB に合わせてカスタマイズします。awsAdmin MIB は必須です。
2. MIBLIB に提供されなくなった MIB について、以下のいずれかの代替手段を選択します。
   - エージェントの特定のライブラリから、対応する MIB を標準 MIBLIB にコピーし、install_mibs スクリプトで既存の ldmib エントリをアクティブ化します。Agent Technology の標準 MIBLIB は SMP/E ターゲット ライブラリであるため、SMP/E を使用して内容を追跡することをお勧めします。CNSMJCL ライブラリにはサンプル ジョブ「AWADDMIB」が含まれています。それによって、エージェントの MIB のコピーし、それを USERMOD として SMP/E 環境に追加する機能が強化されます。
   - エージェントの特定のライブラリ内の対応する MIB を維持し、install_mibs スクリプトの ldmib エントリを、正しいデータセットを指すように編集します。

構成ファイルの編集: /cai/agent/services/config/aws_orb/quick.cfg

quick.cfg 構成ファイルは、分散サービス バスとそのさまざまなパートナ間での通信に使用できるさまざまなプロトコルを記述します。各種パラメータの詳細な定義が記述されているほか、あらゆる環境に広く対応するデフォルト値が提供されています。

構成ファイルの編集: /cai/agent/services/config/aws_sadmin/aws_sadmin.cfg

この構成ファイルは、メインフレームトラップを受信する各リモートシステムを識別します。

aws_sadmin.cfg ファイルを編集する方法

1. 対応するマシン名、または IP アドレスとポート番号 162 または 6162 (リモートシステムのトラップ リスナーが使用するポート番号によります) を持つ SNMP_TRAP エントリを指定します。
2. デフォルトのファイルにサンプルとして記述されている値を、該当するマシン名または IP アドレスに置き換えます。マシン名を使用することをお勧めします。

   ```
   SNMP_TRAP xyzwin2k3.ca.com|162 # NSM マネージャ マシンへのトラップ
   ```

   または

   ```
   SNMP_TRAP 172.24.138.21|6162 # 別の NSM マネージャ マシンへのトラップ
   ```

   注: このファイルには、SNMP コミュニティ名とそれらの属性もリストされていますが、これらは通常変更しません。このファイル内のシャープ記号 (#) で始まる行はコメントで、ランタイム システムからは無視されます。

   以下のトラップの宛先は同一では*ありません*。

   正

   ```
   SNMP_TRAP 172.24.138.21|6162 # non-padded IP Address
   ```

   誤

   ```
   SNMP_TRAP 172.24.138.021|6162 # Padded IP Address
   ```

   注: IP アドレスに対するゼロ埋め込みは許可されていません。IP アドレスは、(たとえば、Windows の DOS プロンプトで IPCONFIG コマンドを使用して照会した際に) TCP/IP スタックから戻されるとおりに指定する必要があります。

   SNMP_TRAP キーワードと SNMP_COMMUNITY キーワード、およびその対応する値と続くコメントとの区切りには、タブ文字 (X'05') を使用します。通常、ISH や UNIX System Services のエディタでは、タブ文字がピリオドとして表示されます。

構成ファイルの編集: /cai/agent/services/config/aws_snmp/aws_snmp.cfg

aws_snmp.cfg 構成ファイルには、aws_sadmin サービスまたは SNMP ツールをカスタマイズする際に使用できるパラメータが記述されます。各種パラメータの詳細な説明が含まれます。

以下のパラメータがサポートされます。

- IP_TO_BIND: aws_sadmin サービスを特定の IP アドレスにバインドできます。デフォルトでは、SNMP リスナー ソケット(デフォルト ポート 6665)は、すべての TCP/IP スタックを待機します。

  注: マルチホーム環境で実行している場合、メインフレーム エージェントが複数の TCP/IP ノードで検出されるのを避けたい場合があります。メインフレーム エージェントの検出をデフォルトの TCP/IP スタックに限定するには、IP_TO_BIND パラメータを 127.0.0.1(ループバック指定)に変更します。

- SNMP_PORTS: SNMP 要求の生成時に aws_sadmin または他の SNMP ツール(awget、awnext など)によって使用されるポートを制御します。

構成ファイルの調整: /cai/agent/services/config/awservices/awservices.cfg

awservices.cfg 構成ファイルには、Agent technology 内でアクティブ化される可能性のあるさまざまなサービスやエージェントが記述されます。

CA NSM r3.0 以降の場合、Agent Technology で提供されるデフォルトの awservices.cfg ファイルには、aws_orb サービスと aws_sadmin サービスのエントリのみが含まれます。

通常、awservices.cfg ファイルには、エージェント(MQSeries エージェントなど)の標準インストール時に、新しいエントリが自動的に作成されます。

エージェントを再インストールせずに、以前のリリースの Agent Technology からアップグレードする場合は、現在 /agent/services/tools ディレクトリに格納されている install_agents スクリプト ファイルを使用します。このスクリプト ファイルを使用すると、現在 z/OS でサポートされている任意のエージェントまたはサービスのエントリを awservices.cfg ファイルに追加したり、awservices.cfg ファイルから削除したりできます。

awservices.cfg ファイルのエントリを追加または削除する方法

1. 「agentworks.profile の実行 (P. 230)」の手順を行います。
2. サポートされている各種パラメータの詳細な説明を取得するには、パラメータを指定せずに install_agents コマンドを入力します。

   例: サンプル エージェント(exagent)を実行する予定がある場合は、以下のコマンドを入力します。

   ```
   install_agents install exagent
   ```

CNSMOPTV 内の ENVFILE のカスタマイズ

ユーザの標準に適合するように CNSMOPTV(ENVFILE)をカスタマイズします。カスタマイズ可能な変数は、AGENTWORKS_DIR、TZ、AW_MAX_LOGSIZE、AWS_STARTER_REQUEST、および AWS_STARTER_CONTROL です。詳細については、「プロファイル ファイルの編集: /cai/agent/agentworks.profile (P. 228)」を参照してください。

TCP/IP ネットワーク構成の確認

TCP/IP ネットワーク構成に Agent Technology コンポーネントとの互換性があるかどうかを確認します。

TCP/IP ネットワーク構成を確認する方法

1. CNSMJCL から AWFTEST ジョブをサブミットします。
2. 出力を見て、gethostname()、gethostid() などの関数に正しい値が戻されていることを確認します。
3. AWFTEST ジョブが正常に実行されない場合は、TCPIP プロシージャを見直して TCPDATA 変数が適切にカスタマイズされているか確認します。 これは、SYSTCPD DD に割り当てられたデータセットと同一であることが必要です。

   このデータセットに PDS を使用している場合は、そのメンバ名が含まれていることを確認します。それでも問題が解決しない場合は、先へ進む前にネットワーク管理者にご相談ください。

aws_sadmin 保管ファイルの作成

最後に aws_sadmin 保管ファイルを作成すると、Agent Technology のインストールは完了です。

aws_sadmin 保管ファイルを作成する方法

1. CNSMJCL から CLEANADM ジョブを実行して、aws_sadmin 保管ファイルを割り当てます。

   このジョブのエラー メッセージは、/cai/agent/services/tools ディレクトリの clean_sadmin.out ファイルに出力されます。

2. clean_sadmin.out ファイルの内容を見て、ユーティリティが正しく実行されたことを確認します。

3. /cai/agent/services/tools/install_mibs スクリプト ファイルが、使用する予定の各エージェント用の ldmib エントリを含んでいるようにカスタマイズされていることを確認します。

4. CNSMJCL データセットの INSTMIBS ジョブをサブミットして、ご使用のシステムに適した MIB と一緒に aws_sadmin 保管ファイルをロードします。このジョブは、上記の install_mibs スクリプト ファイルを起動します。

   このジョブの結果は、/cai/agent/services/tools ディレクトリの install_mibs.out ファイルに出力されます。

5. install_mibs.out ファイルの内容を見て、ユーティリティが正しく実行されたことを確認します。

   重要: CLEANADM ジョブまたは INSTMIBS ジョブの BPXBATCH 手順からのリターン コード (ゼロ) は、呼び出されたスクリプトの正常終了を表わすわけではありません。正常終了を判断するには、.out ファイルの出力結果を確認する必要があります。.out ファイルにエラー メッセージが記録されている場合は、CA Common Services サポート Web サイトを参照してください。このサイトでは、Agent Technology の一般的な構成エラーを特定し、解決するためのヒントを提供しています。

これで、ご使用のマシンへの Agent Technology のインストールが完了しました。

注: ここで、新しい zFS のバックアップ コピーを作成することをお勧めします。

エージェント セキュリティ

セキュリティ管理者に、エージェントを実行するユーザ ID の作成または更新を依頼します。エージェントを実行するユーザは全員、UNIX System Services へのアクセス権を持ち、Agent Technology ファイルを所有するグループのメンバである必要があります。

エージェントの構成セットの検証

Agent Technology を複数のシステムにインストールするときや旧リリースの AgentTechnology からアップグレードするときにエージェントに付属の構成セットを使用する場合は、その時点でその構成セットをロードする必要があります。構成セットには、エージェントと共に配布されるものと、独自に作成されるものとがあります。特に、CA NSM System Status Manager CA-OPS/MVS Option のエージェントは、CA OPS/MVS Event Management and Automation に付属の構成セットがないと動作しません。構成セットのロードが必要かどうか、および、構成セットを再ロードする手順については、実行するエージェントのマニュアルを参照してください。

注: 構成セットをロードするための *ldconfig* ユーティリティの詳細については、「*Reference Guide*」を参照してください。

ロード ライブラリに関する考慮事項

現在、バッチ ジョブとエージェントによって使用されるすべての Agent Technology モジュールは、CNSMLOAD 内に存在するようになりました。

重要: エージェントを実行するすべてのジョブの JCL を確認し、STEPLIB DD ステートメントを修正して CAILOAD または CAILIB への参照を削除し、CAW0LOAD および CNSMLOAD の両方への参照を追加します。

注: システム LNKLST に対して CAW0LOAD および CNSMLOAD を定義した場合、エージェントを実行するジョブに STEPLIB 参照は不要です。

Agent Technology の起動

Agent Technology サービスを開始する方法

1. CNSMPROC 内の AWSTART を変更して開始します。
2. オンライン コマンド（シェル スクリプト）を発行して同じタスクを実行します。

注: バッチ ジョブおよび対応するシェル スクリプトの詳細については、「*Reference Guide*」を参照してください。

サンプル エージェント（EXAGENT）のビルドと実行

このタスクはオプションです。サンプル エージェントは、Agent Technology サービスが適切に動作することを確認する目的で設計されています。このエージェントは、独自のエージェントをコーディングする際のモデルとしても利用できます。サンプル エージェントのソース コードは、Agent Technology サービスと共に配布され、以下の場所に格納されます。

- CNSMSRCV にインストールされた EXAGENT メンバ
- /$AGENTWORKS_DIR/agents/samples/exagent ディレクトリ内の exagent.c ファイル

このエージェントは、UNIX System Services zFS 内のディレクトリ構造をトラバースする機能を備えています。

サンプル エージェントは、実行前にあらかじめサイトでコンパイルおよびリンクしておく必要があります。コンパイルとリンクは、USS 内でオンラインで実行できるほか、z/OS でバッチ ジョブをサブミットすることによって行うこともできます。どちらか適切な環境（オンラインまたはバッチ）を選択してください。

オンラインでのコンパイルとリンク（USS）

コンパイルとリンクは、USS 内でオンラインで実行できます。

サンプル エージェントをオンラインで実行する方法

1. 「agentworks.profile の実行 (P. 230)」の手順を実行します。
2. サンプル エージェントのディレクトリに移動します。

   ```
   cd /$AGENTWORKS_DIR/agents/samples/exagent
   ```

3. 以下のコマンドを実行します。

   ```
   make install
   ```

   このコマンドによって、サンプル エージェントのコンパイルとリンクが実行され、実行可能プログラムが「agents/bin」ディレクトリにコピーされます。

4. 以下のコマンドを実行してサンプル エージェントを起動します。

   ```
   exagent start
   ```

バッチ モードでのコンパイルとリンク(z/OS)

コンパイルとリンクは、バッチ ジョブをサブミットすることによって実行できます。

サンプル エージェントをバッチ モードで実行する方法

1. Common Services ランタイム JCL ライブラリ(CNSMJCL)内のメンバ EDCCPL をカスタマイズしてサブミットします。

   このジョブによって、サンプル エージェントのコンパイル、プリリンク、およびリンクが実行され、デフォルト ユーザのランタイム オプション モジュールのアセンブリを行い、Common Services のロード ライブラリに EXAGENT というモジュールが生成されます。

2. Common Services ランタイム JCL ライブラリ(CNSMJCL)内のメンバ EXAGNT をカスタマイズしてサブミットします。

   このジョブによってサンプル エージェントが起動されます。

上記で実行されるリンク処理では、サンプル エージェント用のデフォルト ユーザのオプションを含み、IBM Language Environment(LE)のランタイム オプションを提供します。サイト固有の要件を満たすために LE パラメータをカスタマイズする必要がある場合もあります。この場合は、ユーザ オプション テーブル CEEUOPT のアセンブリを行う EDCCPL ジョブ ステップを編集します。

上記のジョブ ストリームは、独自にビルドしたエージェントのコンパイル、リンク、およびサブミットを実行するためのサンプル JCL デックとしても使用できます。

注: これらのエージェントの開発と展開の詳細については、「*CA NSM Inside Systems Management Guide*」、および「*Inside Systems Monitoring Guide*」を参照してください。

Agent Technology のインストールの確認

Agent Technology z/OS サービスが正常に起動されたら、下記の手順を行ってください。

Agent Technology サービスが適切に動作していることを確認する方法

1. AT サービスの状態を確認します。OMVS で以下の手順を実行します。
   a. 以下のコマンドを発行します。

      ```
      . agentworks.profile
      ```

      注: このコマンドは引用符で囲まないでください。また、必ずピリオドとスペースを入力してから、agentworks.profile スクリプトを実際に呼び出してください。

   b. 以下のコマンドを発行します。

      ```
      awservices list
      ```

      生成されるレポートの最初の 2 行は、以下のようになります。

      ```
      RUNNING    aws_orb:aws_orb
      RUNNING    aws_sadmin:aws_sadmin
      ```

      注: レポートに、いくつかのサービスやエージェントが、「Stopped」というステータスとともに表示される場合があります。これは正常です。

2. AT サービスのポートの状態を確認します。OMVS で以下の手順を実行します。
   a. 以下のコマンドを発行します。

      ```
      onetstat
      ```

   b. 生成されるレポートには、すべての AT ポート(この章の「概要」を参照)とそのステータスが以下のように表示されます。

      ```
      Listen - For all TCP/IP socket ports
      UDP - For the SNMP listener port (normally 6665)
      ```

3. すべてのエージェント MIB とサービス MIB がオブジェクト ストアにロードされていることを確認します。OMVS で以下の手順を実行します。
   a. 以下のコマンドを発行します。

      ```
      . agentworks.profile
      ```

   b. 以下のコマンドを発行します。

      ```
      agentctrl -m
      ```

生成されたレポートには、awsAdmin MIB と、少なくとも 1 つの他のエージェント MIB が表示されている必要があります。以下に例を示します。

```
<awsAdmin>      is registered
<caiDatacom>    is registered
<caiDb2mvs>     is registered
<caiIDMS>       is registered
<caiSysAgtzOS>  is registered
<caiSysAgtCics> is registered
<caiSysAgtMqs>  is registered
<caiSysAgtMvs>  is registered
```

4. 問題が発生したら、($AGENTWORKS_DIR/services/var/log ディレクトリの下の) AT zFS 内のサービス ログ ファイルを確認して、問題の解決を試みます。これらのファイルは、AT サービスが起動されるたびに上書きされます。

第 12 章: CA グローバル サブシステムの設定

CA Common Services for z/OS をインストール後、CA グローバル サブシステム（CA-GSS）の設定タスクを実行する必要があります。

注: これらのタスクを実行するとき、展開されたデータ セットを使用します。

このセクションには、以下のトピックが含まれています。

GSS のインストールの完了

GSS のインストールを完了する方法

1. GSS VSAM のデータセットを割り当てます。

   CAW0JCL メンバ BYSI0010 を編集してサブミットし、INTERNAL および SAMPLE ISET 用に VSAM IMOD ファイルを割り当てます。

2. GSS IMOD ファイルをロードします。

   CAW0JCL メンバ BYSI0020 を編集して GSS IMOD ファイルをロードします。

   注: この手順を実行するには、STEPLIB データ セットに APF 権限が付与されている必要があります。

CA-GSS でのポスト設定プロセスの動作

CA-GSS のインストールを完了して使用可能にするには、以下の設定タスクを実行する必要があります。

- サブシステム ID を定義する。
- システム PROCLIB への CA-GSS プロシージャのコピー
- IMOD エディタをインストールする。
- ISERVE オペレータ制御パネルをインストールする。
- インストール後動作確認。
- 設定。

サブシステム ID の定義

CA-GSS CAW0OPTN RUNPARM メンバで SSNAME パラメータを使用して、ISERVE サブシステム ID を指定します。ドキュメント作成のために、SYS1.PARMLIB データセットで CA-GSS サブシステム ID（GOAL）および ISERVE サブシステム ID（ISRV）を指定することをお勧めします。

注: SYS1.PARMLIB データセットにサブシステム ID を追加しない場合は、CA-GSS の起動時にサブシステム名テーブルに動的に追加されます。

システム PROCLIB への CA-GSS プロシージャのコピー

CA-GSS プロシージャは CAW0PROC ライブラリに用意されています。このプロシージャはスターティッド タスクとして実行できるように、システム PROCLIB に移動する必要があります。

次の表に、コピーする CAW0PROC メンバの名前と、それぞれの推奨プロシージャの名前を示します。

CAW0PROC 名	PROCLIB 名	説明
BYSGSSA	GSSA	プライマリ CA-GSS スターティッド タスク
BYSGSSP	GSSP	CA-GSS 受動エリア ユーティリティ

システム PROCLIB にプロシージャをコピーする方法

1. CAW0PROC メンバを調べて、これらが適切にカスタマイズされていることを確認します。

   データセット名および JCL ステートメントは、使用するシステムに適した形に変更します。

   小文字のパラメータには値を適宜選択します。

2. メンバをシステム PROCLIB にコピーします。

複数の CA-GSS サブシステムを実行する予定がある場合は、セカンダリ GSS サブシステムを実行するために、サンプル プロシージャ BYSISRV を CAW0PROC ライブラリに組み込みます。

注: 複数の CA-GSS サブシステムの実行の詳細については、「*Administration Guide*」を参照してください。

IMOD エディタのインストール

IMOD エディタは、IMOD の作成、編集、コンパイル、およびテストを行うことができる ISPF ベースの機能です。IMOD エディタのインストールには、以下の要件があります。

- TSO ユーザが CA-GSS CAW0LOAD ロード ライブラリにアクセスできること。そのためには、LINK LIST を使用するか、適切な STEPLIB ステートメントを用意します。
- TSO ユーザが CA-GSS ISPF 関連ライブラリ（パネル、メッセージおよび CLIST）にアクセスできること。そのためには、CA-GSS エディタ プログラム（SRVEDIT）を呼び出す際に動的に割り振ります。
- CAW0OPTN データセットの ISET メンバ内にある CA-GSS アドレス空間に渡された情報に基づいてパラメータ リストを作成すること。
- 必要に応じて、ISPF パネルからの IMOD エディタの呼び出しを許可するために、適切な ISPF メニュー項目を追加すること。

IMOD エディタをインストールする方法

1. enqueue 要求を検討します。
   - CA-GSS は、ISET を破壊することなく複数のシステムで共有できるように、enqueue の整合性を監視します。enqueue が正しく処理されるためには、enqueue 管理ソフトウェアに CA-GSS enqueue について通知する必要があります。
   - 更新操作時には、IPGMGREX という qname と *F.dsn* という rname に対する排他的 enqueue が得られます（*dsn* はブランクで右パディングされた 44 バイトのクラスタ名です）。-
   - 編集操作時には、IPGMGREX という qname と *P.imod.dsn* という rname に対する排他的 enqueue が得られます（*imod* はブランクで右パディングされた 16 バイトの IMOD 名、*dsn* はブランクで右パディングされた 44 バイトのクラスタ名です）。--
   - すべての enqueue には、SYSTEMS の有効範囲があります。

2. パラメータリストを構成して CA-GSS RUNPARMS を更新します。

   IMOD エディタの入力パネルには、使用可能なすべての ISET（IMOD データセット）がリスト表示されます。このリストの各エントリには ISET 名と説明が含まれているだけでなく、ISET にリンクされている ISERVE アドレス空間のサブシステム ID がある場合はその ID も含まれます。

   以下を考慮してください。

   - 特定の ISET 名によって参照されるデータセットは 1 つだけですが、複数の ISET 名によって 1 つのデータセットが参照されることもあります。
   - IMOD の動的な再ロードまたは実行を許可する場合、ISET および DSNAME 参照は、CA-GSS アドレス空間に定義された ISET ステートメントに含まれるものと同一である必要があります。CAW0OPTN RUNPARM メンバ、ISETS メンバ、および EDITPARM メンバを使用することで、参照の同一性を保証できます。
   - UNIT=VIO がデータ センター内のデータセットの割り振りについて無効である場合は、IMOD コンパイラを実行する前に、VIOUNIT パラメータを組み込む必要があります。
   - パラメータリストは、EDITOR MEMBER ステートメントで指定するメンバ名の値によって参照されます。この値には、CAW0OPTN データセットの EDITPARM メンバを指定する必要があります。
   - CAW0OPTN データセットの ISETS メンバ内に、サンプルのパラメータリストが用意されています。使用中の環境に適した ISET 定義をこのメンバに加え、カスタマイズすることができます。小文字のパラメータには値を選択する必要があります。EDITOR MEMBER ステートメントで参照される EDITPARM メンバには、ISETS メンバに対する INCLUDE ステートメントが含まれています。これにより、CA-GSS タスクと SRVEDIT プログラムが同一の ISET リストを参照することが保証されます。

     注: ISET の初期化パラメータ ステートメントのフォーマットについては、「*Reference Guide*」を参照してください。

3. ISPF メニュー パネルを変更します。

   IMOD エディタは、GSSEDIT コマンドを実行することで起動するか、ISPF メニュー パネルから起動します。GSSEDIT コマンドは、配布 CLIST データセットに含まれる REXX EXEC です。

   ISPF から IMOD エディタを起動するには、適切な ISPF メニュー パネルを見つけ、次のメニュー項目をパネルおよび PROC セクション内に追加します。

   ```
   ISRV,'PGM(SRVEDIT) NEWAPPL(nnnn) NOCHECK'
   ```

   nnnn を任意の 4 文字の ISPF アプリケーション ID（ISRV など）に置き換えてください。

重要: ISPF プライマリ メニュー パネルを変更するときには注意が必要です。エラーが発生すると、ISPF を使用できなくなります。 ISPF から独立したバックアップ メンバとテスト済みプロシージャを常に保持しておいてください。

IMOD エディタに関する問題

IMOD エディタを選択したときに ISPPROF を示す ISPF エラー メッセージが発生した場合は、ISPPROF データセットに十分な領域があることを確認してください。

IMOD エディタから IMOD の再ロードまたは実行ができない場合は、以下の手順に従います。

- 障害の原因を示す長いエラー メッセージを表示するには、F1 キーを押すか、「HELP」と入力します。
- CA-GSS が実行されていることを確認します。このためには、GSSMAIN プログラムが実行されている必要があります。

  また、SRVSYS プログラムを使用してセカンダリ ISERVE が実行中である可能性もあります。

  ISERVE 参照および DSNAME 参照が、CA-GSS アドレス空間に定義された ISET ステートメントに含まれるものと同一であることを確認します。CAW0OPTN RUNPARM、ISETS、および EDITPARM メンバを使用することで、参照の同一性を保証できます。

CA-GSS/ISERVE オペレータ制御パネルのインストール

CA-GSS は、CA-GSS/ISERVE オペレータ制御パネルと呼ばれる ISPF ベースの制御機能を備えており、これを使用して端末から CA-GSS コマンドを実行できます（z/OS オペレータ コンソールへのアクセスは要求しません）。このコマンドは CA-GSS アドレス空間の操作と監視に使用でき、ユーザの z/OS システムで動作する任意の CA-GSS アドレス空間に適用できます。GoalNet では、任意の GoalNet 参加ノード宛のコマンド送信が許可されます。

これらのコマンドの結果はフルスクリーン モードでパネルに表示され、上下にスクロールして全体を見ることができます。他のコマンドに置き換えない限り、結果は画面からロールオフされません。

CA-GSS/ISERVE オペレータ制御パネルをインストールするには、GSSOPER コマンドを発行して、CA-GSS/ISERVE オペレータ制御パネルを起動します。これは ISPF メニュー パネルから起動することもできます。

このパネルを ISPF から起動するには、その ISPF パネルと、適切なパネルに該当する PROC セクションに、以下のメニュー項目を追加します。

```
ISRV0,'PGM(SRVOPER) NEWAPPL(mmmm) NOCHECK'
```

mmmm を任意の 4 文字の ISPF アプリケーション ID（OSRV など）に置き換えてください。

重要: ISPF プライマリ メニュー パネルを変更するときには注意が必要です。エラーが発生すると、ISPF を使用できなくなります。 ISPF から独立したバックアップ メンバとテスト済みプロシージャを常に保持しておいてください。

インストール後の動作確認

ここまでで、基本的なインストールの処理が完了しました。最終的な設定に進む前に、CA-GSS が適切にインストールされていることを確認します。

CA-GSS のインストールを検証する方法

1. CA-GSS を起動します。

   オペレータ コンソールから以下のコマンドを入力します。

   ```
   START GSSA
   ```

   初期化が速やかに実行され、完了すると以下のメッセージが表示されます。

   ```
   SRV220 Version 02.08.mm: Initialization Complete (ssid)
   ```

   mm は CA-GSS の現在のメンテナンス レベルを表し、*ssid* は ISERVE に指定されているサブシステム ID を表します。

2. CA-GSS をテストします。

   - ISPF パネルから以下のコマンドを実行して、CA-GSS/ISERVE 制御パネルを起動します。

     ```
     TSO EX 'CAI.CAW0CLS0(GSSOPER)'
     ```

   - CA-GSS/ISERVE 制御パネルから以下のコマンドを実行し、インストール検査プログラム（IVP）を実行します。

     ```
     IVP [PRINT [TO userid [AT node]]]
     ```

     かっこ内の文字を省略した場合は、コンソール上に出力が行われ、CA-GSS の動作が検証されます。必要に応じて、より詳細なレポートを出力するように指定できます。PRINT オプションを指定する場合は、出力されるリストの送信先となるユーザ ID およびノードを指定してください。

   - F3 キーを使用して ISPF パネルに戻ります。

3. IMOD エディタをテストします。

   - ISPF パネルから次のコマンドを実行して、IMOD エディタを起動します。

     ```
     TSO EX 'CAI.CAW0CLS0(GSSEDIT)'
     ```

   - 名前の横に S を指定して SAMPLIB ISET を選択します。次に、名前の横に S を指定して $$$VERSION メンバを選択します。

   - $$$VERSION メンバに CA-GSS の正しいバージョンが指定されていることを確認します（0208*mm* となるはずです）。

     バージョンが正しければ、F3 キーを使用して、SAMPLIB ISET の表示に戻ってください。

   - 名前の横に G を指定して、$$$VERSION メンバをコンパイルします。

     コンパイルが行われたことを確認するには、パネル上右隅に IMOD LOADED メッセージが表示されているか確認してください。

   - F3 キーを使用して ISPF セッションに戻ります。

4. CA-GSS を停止します。

   オペレータ コンソールから以下のいずれかのコマンドを入力して、CA-GSS を適切に停止します。

   ```
   STOP GSSA
   P GSSA
   F GSSA, STOP
   ```

   CA-GSS が数秒以内で停止しない場合は、以下のコマンドを入力してください。

   ```
   F GSSA, STOP FORCE
   ```

   それでも CA-GSS が停止しない場合は、アドレス空間をキャンセルし、JESLOG および ISRVLOG リストに診断メッセージがあるかどうか調べてください。

TSO での再コンパイル

TSO のもとで IMOD を再コンパイルすることをお勧めします。

TSO のもとで IMOD を再コンパイルには、以下の手順に従います。

1. ISET を選択し、IMOD 選択パネルを表示します。
2. TOGGLE コマンドを入力し、各 IMOD の現在のコンパイラのバージョンを表示します。
3. 再コンパイルが必要な IMOD を示す各行に、C(コンパイル)コマンドを入力します。
4. Enter キーを押して、C で指定されたすべての IMOD を再コンパイルします。

   IMOD が再コンパイルされます。

CA-GSS のカスタマイズ

CA-GSS を最初にインストールする際には、製品固有のパラメータなどを含む初期化パラメータを変更する必要があります。- しかし、通常はすべての CA-GSS 初期化パラメータをカスタマイズする必要はありません。CA-GSS の初期化パラメータの詳細と、カスタマイズの必要があるパラメータの判別方法については、「Administration Guide」を参照してください。

次のセクションでは、製品固有の設定手順について説明します。

CA Insight Database Performance Monitor for DB2 for z/OS 向けの CA-GSS のカスタマイズ

CA Insight Database Performance Monitor for DB2 for z/OS は CA-GSS のロギング、アクセス、オーディットなどのさまざまな機能を使用します。CA-GSS にアクセスするすべての CA Insight Database Performance Monitor for DB2 for z/OS 機能に対して REXX ベースの IMOD が使用されます。

CA Insight Database Performance Monitor for DB2 for z/OS のマニュアルを参照し、この製品に IMOD ライブラリ(ISET)が用意されているかどうか確認してください。ISET が用意されている場合、それを DASD にロードする必要があります。

CA Insight Database Performance Monitor for DB2 for z/OS の CA-GSSIMOD メンバを使用して、ISET をロードできます。このメンバ内で JCL をサブミットする前に、UNIT および VOLSER の番号が、CA Insight Database Performance Monitor for DB2 for z/OS 配布メディア上の番号と一致していることを確認します。

CA Insight Database Performance Monitor for DB2 for z/OS をカスタマイズする方法

1. ILOG を割り振ります。

   ILOG は、CA-GSS がサブシステムの情報を記録するために使用する VSAM 線形データセットです。それぞれの ILOG は 2 つの *サブファイル*(データセット)で構成されます。一方はプライマリ、もう一方はプライマリがフルになった際に使用されるバックアップです。

   CA-GSS がモニターする各 DB2 サブシステムにデータセットを 2 つずつ割り振る必要があります。それには、1 つ以上の ALLOC_ILOG コマンドが含まれる SRVMAINT ジョブを変更してサブミットします。1 つの ALLOC_ILOG ステートメントで、2 つの VSAM 線形データセットが割り振られます。これらのデータセットを割り振る方法として、CAW0JCL データセットの BYSIALI メンバを変更してサブミットするという方法もあります。

   割り振りジョブのために以下の変更を加えます。

   - ILOG ファイルが置かれる DASD のボリュームの VOLSER を指定します。
   - 各 DB2 サブシステムに DEFINE 手順が 1 つずつあることを確認します。

- データセット名を指定します。プライマリ サブファイルについては LOG*nn*#0、バックアップ サブファイルについては LOG*nn*#1 という命名規則を使用することをお勧めします（*nn* は DB2 サブシステムを表します）。以下に、3 つの DB2 サブシステムに対応するファイルの命名例を示します。

サブシステム	プライマリ	セカンダリ
01	LOG01#0	LOG01#1
02	LOG02#0	LOG02#1
03	LOG03#0	LOG03#1

- BYSIALI メソッドを使用する場合は、LINEAR パラメータと SHAREOPTIONS パラメータのどちらの値も変更しないでください。

2. CA Insight Database Performance Monitor for DB2 for z/OS に ILOG を指定します。

   CAW0OPTN データセットの INSIGHT メンバを使用して、CA-GSS に ILOG データセットを指定します。

   各 ILOG ステートメントで、1 つの ILOG ファイルおよび 1 つのサブファイルを指定します。ILOG ステートメントでは、以下の情報を指定します。

   - 他のアプリケーションで使用されていない固有の ILOG 番号
   - ILOG で使用するために割り振ったデータセットの DS 名
   - ILOG 用のサブファイル

3. 次の DD ステートメントを追加して、GSSA システムの PROCLIB メンバを変更します。

   ```
   //DB2SSID DD DSN=CAI.CAW0OPTN(DB2SSID),DISP=SHR
   ```

   この DD ステートメントは、CAW0OPTN データセットの DB2SSID メンバを指定しています。

   CA-GSS は、初期化時にその DB2SSID メンバを読み取り、モニターする DB2 アドレス空間の内容、およびそれらのアドレス空間の情報を記録するための ILOG を判別します。

4. CA-GSS に DB2 サブシステムを指定します。

   GSSA システム CA-GSS PROCLIB メンバで参照される DB2SSID メンバで、CA-GSS がモニタする DB2 サブシステムそれぞれについて ILOG ステートメントを定義する必要があります。

   このメンバの ILOG 番号が、CAW0OPTN データセットの INSIGHT メンバの ILOG 番号に一致する必要があります（手順 2 で説明しました）。

5. CA-GSS パラメータを変更します。

   必要に応じて、CA-GSS のサポートに影響を与える CA-GSS 初期化パラメータを変更します。このパラメータの例は、CAW0OPTN データセットの DBDEL メンバに含まれています。

   変更する必要があるのは以下のパラメータです。

   - COMMAND - INSIGHT コンソールのコマンドを CA-GSS に定義します。

     CA Insight Database Performance Monitor for DB2 for z/OS は、名前のプレフィクスが $DBGL_ である IMOD のセットを配布します。この IMOD により、オペレータに追加の機能を提供するオペレータ コンソール コマンドが処理されます。

     ILOG - ILOG ファイルを定義します。このパラメータを、定義した ILOG に対してそれぞれ一回指定します。

   - ISET - CA Insight Database Performance Monitor for DB2 for z/OS の配布メディアに含まれる ISET（IMOD ライブラリ）を識別します。
   - PRODUCT - CA Insight Database Performance Monitor for DB2 for z/OS 向けの CAG-SS サポートをアクティブにします。
   - このパラメータは、他の PRODUCT パラメータの指定内容とは競合しません。
   - WTO - 指定した WTO が発行されるたびに、特定の IMOD を実行します。
   - WTO パラメータを使用すると、FLASHBACK ファイルのバックアップが必要であることを示す IDB2309 メッセージに応答して IDB2_IDB2309E IMOD が実行されます。

   ご使用のシステムの要件を満たすように、IMOD を変更する必要があります。

6. ロギング用の IMOD を指定します。

   大容量のデータをロギングする場合は、$USER_ILOG_FULL IMOD を指定する必要があります。これにより、CA-GSS はいっぱいになった ILOG を自動的に切り替えるか、またはリセットできるようになります。

   注: この IMOD の特殊用途については、「Reference Guide」を参照してください。

7. GoalNet をアクティブ化します。

   マルチ CPU 環境で CA Insight Database Performance Monitor for DB2 for z/OS を使用する場合は、共用 DASD の有無に関係なく GoalNet をアクティブにすることをお勧めします。これにより、CA Insight Database Performance Monitor for DB2 for z/OS では複数のシステムから情報を収集して表示を統合できます。

   CA Insight Database Performance Monitor for DB2 for z/OS System Condition Monitor を外部のシステムで使用するには、すべての CPU に CA-GSS をインストールする必要があります。情報が表示されるシステムには、CA Insight Database Performance Monitor for DB2 for z/OS が必要です。

CA Jobtrac Job Management のカスタマイズ

CA Jobtrac Job Management は、CA-GSS の機能を使用してその機能を拡張し、全面的にカスタマイズ可能なジョブ スケジューリングのサポートを実現します。さらに、CA Jobtrac Job Management のカスタマイズ情報は、他の CA-GSS クライアント ソフトウェア（ユーザが用意したものを含む）でも利用できます。

CAW0OPTN メンバ JOBTRAC には、サンプルの設定パラメータがあります。

注: 設定の詳細については、*CA Jobtrac Job Management* のドキュメントを参照してください。

CA MIM 向けの CA-GSS のカスタマイズ

CA MIM には、複数の CPU で共有されるデバイスについて、テープ デバイスの割り振りに関する情報を提供する Tape Preferencing Control Facility（TPCF）が用意されています。この情報は、ADDRESS TPCF と $SRV_TPCF サービス ルーチンを使用して REXX IMOD に渡すことができます。

GSS は、その REXX IMOD 機能を使用して以下の CA 製品の間の統合をセットアップできる場合があります。

- CA Sysview
- CA OPS/MVS
- CA Jobtrac
- CA View

他の統合パスは、これら製品と他の製品の間で利用可能にすることができます。製品統合を行うことを決定した場合は、他の方法がないか製品ドキュメントを核にするか、CA テクニカル サポートにお問い合わせください。いくつかの高度なテクニックは、GSS の統合方法より優れている場合があります。

MIMAPI1 API モジュールが利用可能であることを確認します。このモジュールは、CA MIM ロード ライブラリに置かれます。このライブラリは APF リストに含めておく必要があります。

注: CA MIM- 向けの API モジュールの詳細については、「CA NSM *CAMIA Systems Programmer Guide*」を参照してください。

CA MIM 向けに CA-GSS をカスタマイズする方法

1. JCL を変更します。

   LINKLIST ライブラリに CA MIM MIMAPI1 ロード モジュールがない場合は、CA-GSS PROC にそのライブラリを STEPLIB として組み込みます。

2. CA-GSS パラメータを変更します。

   必要に応じて CA-GSS の CA MIM サポートに影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの MIM メンバに、これらのパラメータの例が含まれています。

   MIM メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク(*)をブランクに置き換えます。

   MIM メンバの内容を RUNPARM メンバにコピーするか、単に MIM ステートメントを記述します。

   ADDRESS パラメータについては、以下の事項に注意してください。

   ADDRESS 環境は、REXX IMOD から利用可能なロード モジュールとして、CA MIM 配布メディアで用意されています。

   - CA が配布する IMOD では、アドレス名が TPCF であることを前提としています。他の名前を使用する場合は、ALTNAME パラメータを指定して TPCF を定義してください。
   - ロード モジュール名は、CA MIM 配布メディアで出荷された時と同じ名前です。このロード モジュールが CA-GSS からアクセス可能な APF-許可ライブラリにあることを確認します。

     詳細については、「オプション機能」を参照してください。

CA OPS/MVS Event Management and Automation 向けの CA-GSS のカスタマイズ

CA OPS/MVS Event Management and Automation は、CA-GSS 機能を使用して他の CA Technologies 製品にアクセスできます。さらに、CA-GSS 機能を通してその機能を他の製品で使用することもできます。

GSS は、その REXX IMOD 機能を使用して以下の CA 製品の間の統合をセットアップできる場合があります。

- CA Sysview
- CA OPS/MVS
- CA Jobtrac
- CA View

他の統合パスは、これら製品と他の製品の間で利用可能にすることができます。製品統合を行うことを決定した場合は、他の方法がないか製品ドキュメントを核にするか、CA テクニカル サポートにお問い合わせください。高度なテクニックが、GSS の統合方法より優れている場合があります。

CA OPS/MVS Event Management and Automation 向けに CA-GSS をカスタマイズする方法

1. CA OPS/MVS Event Management and Automation OPGLEVMG 通信モジュールが利用可能であることを確認します。このモジュールは CA OPS/MVS Event Management and Automation ロード ライブラリに置かれます。このライブラリは APF リストに含めておく必要があります。
2. CA-GSS で CA OPS/MVS Event Management and Automation 機能を使用できるような、適切な CA OPS/MVS Event Management and Automation セキュリティ規則を指定します。 たとえば、OPSCMD セキュリティ規則を指定すると、GSS OPER ADDRESS 環境を経由して z/OS コマンドを実行できるようになります。

3. GSSA システム PROCLIB メンバを変更します。

   - LINKLIST ライブラリ内に CA OPS/MVS Event Management and Automation OPGLEVMG ロード モジュールがない場合は、GSSA システム PROCLIB にそのライブラリを STEPLIB として組み込みます。
   - 必要に応じて CA-GSS の CA OPS/MVS Event Management and Automation サポートに影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの OPSMVS メンバに、これらのパラメータの例が含まれています。

     OPSMVS メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク(*)をブランクに置き換えます。

     OPSMVS メンバの内容を RUNPARM メンバにコピーするか、単に OPSMVS ステートメントを記述します。

     SSID パラメータは、関連する ADDRESS および関数要求を処理する CA OPS/MVS Event Management and Automation システムを識別します。

     ADDRESS パラメータは、REXX IMOD が、最大 4 つの ADDRESS 環境と関数呼び出しを利用できるようにします。

     ADDRESS パラメータについては、以下の事項に注意してください。

     - これらの ADDRESS 環境および関数呼び出しは、CA OPS/MVS Event Management and Automation OPGLEVMG ロード モジュールに用意されています。
     - OPSVALUE() 関数を利用可能にする場合は、適切な ADDRESS パラメーを指定します。
     - CA が配布する IMOD では、アドレス名が OPER、OPSREQ、AOF、OSF、および OPSVALUE であることを前提としています。他の名前を使用する場合は、ALTNAME パラメータを指定して OPER、OPSREQ、AOF、OSF、および OPSVALUE を定義してください。
     - ロード モジュール名は、CA OPS/MVS Event Management and Automation 配布メディアで出荷された時と同じ名前です。このロード モジュールが CA-GSS からアクセス可能な APF-許可ライブラリにあることを確認します。

CA SYSVIEW Performance Management のカスタマイズ

CA-SYSVIEW のカスタマイズの機能は IMOD によって使用され、また IMOD を使用することで他の CA Technologies 製品によって使用されます。

注: 設定の詳細については、*CA SYSVIEW Performance Management* のドキュメントを参照してください。

CA View 向けの CA-GSS のカスタマイズ

CA View のカスタマイズの機能は、IMOD により使用されたり、IMOD を使用することで他の CA Technologies 製品によって使用されたりします。

CA View SARINTF 通信モジュールが利用可能であるか確認します。このモジュールは CA View 配布メディアに格納されていて、APF-許可された LINKLIB データ セットに移動する必要があります。

CA View 向けに CA-GSS を設定する方法

1. GSSA システム PROCLIB メンバを変更します。

   LINKLIST ライブラリ内に CA View SARINTF ロード モジュールがない場合は、そのライブラリを STEPLIB として GSSA システム PROCLIB メンバに組み込みます。

2. CA-GSS パラメータを変更します。必要に応じて CA-GSS の CA View サポートに影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの VIEW メンバに、これらのパラメータの例が含まれています。

   - VIEW メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク(*)をブランクに置き換えます。
   - VIEW メンバの内容を RUNPARM メンバにコピーするか、単に VIEW ステートメントを記述します。

- CA-GSS の初期化パラメータについては、「Reference Guide」を参照してください。
- ADDRESS パラメータによって、CA-View 配布メディアにロード モジュールとして用意されている ADDRESS 環境が REXX IMOD で利用できるようになります。
- ADDRESS パラメータについては、以下の事項に注意してください。
  - CA が配布する IMOD は、アドレス名が XPVIEW であることを前提にしています。他の名前を選択した場合は、ALTNAME パラメータを使用して XPVIEW を定義してください。
  - ロード モジュールの名前は、出荷時の CA View 配布メディアの名前と同じです。このロード モジュールが CA-GSS からアクセス可能な APF 許可ライブラリに置かれていることを確認してください。
- VIEW パラメータは、CA View が提供する初期化 IMOD にパラメータを指定します。VIEW パラメータは、複数回指定することができます。

DB2 向けに CA-GSS をカスタマイズ

IBM DB2 データベース ソフトウェアが稼働している場合、動的 SQL ステートメントを実行して、IMOD でデータを取得することができます。

DB2 の DSNALI および DSNHLI2 通信モジュールが利用可能であるか確認してください。これらのモジュールは、APF 許可された LINKLIB データセット内にあることが必要です。

DB2 向けに CA-GSS を設定する方法

1. GSSA システム PROCLIB メンバを変更します。

   LINKLIST ライブラリ内に DB2 DSNALI および DSNHLI2 ロード モジュールがない場合は、GSSA システム PROCLIB メンバ内にこれらのライブラリを STEPLIB として組み込んでください。

2. CA-GSS パラメータを変更します。必要に応じて CA-GSS の DB2 サポートに影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの DB2 メンバに、これらのパラメータの例が含まれています。

   - DB2 メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク(*)をブランクに置き換えます。
   - DB2 メンバの内容を RUNPARM メンバにコピーするか、単に DB2 ステートメントを記述します。
     - ADDRESS パラメータは、CA-GSS/ISERVE の初期化中に DB2 DSNALI モジュールと DSNHLI2 モジュールをロードし、DB2() REXX 関数の処理に利用できるようにします。

- DB2PLAN パラメータは、SQL ステートメントが処理される DB2 にバインドされるプランを指定します。デフォルト名は、GSSPLAN です。別のプランを使用する場合は、DB2PLAN パラメータを使用して名前を指定してください。
- SSID パラメータは、CA-GSS が通信する必要のある DB2 アドレス空間を指定します。各 CA-GSS は、1 つの DB2 アドレス空間のみと通信できます。

  デフォルト値は DSN です。

  DB2 アドレス空間で別のサブシステム ID を使用する場合、または CA-GSS を他のアドレス空間と通信させる場合は、SSID パラメータを使用してアドレス空間を正しく指定してください。

  動的 SQL のプロセスを複数の DB2 アドレス空間で実行したい場合は、セカンダリ ISERVE アドレス空間をそれぞれの DB2 に 1 つずつ提供します。これで、GoalNet を使用してプロセス要求を適切な ISERVE アドレス空間に送ることができます。

3. SRVDB2P ロード モジュールを作成します。

   動的 SQL プログラムは、DB2 リリース レベル、プログラム名、およびプログラムのアセンブリ日時に大きく依存するため、CA-GSS では SRVDB2P プログラムをソース形式で配布しています。このプログラムとサンプル JCL は、CAW0JCL メンバ BYSDB2P 内にあります。

4. プランをバインドします。

   DB2() 関数を使用して動的 SQL を実行する前に、プラン（手順 2 で作成し、DB2PLAN 初期化パラメータで指定）をターゲットの DB2 アドレス空間にバインドする必要があります。

IDCAMS 向けに CA-GSS をカスタマイズ

CA-GSS/ISERVE により、IBM Access Method Services（IDCAMS、CA-GSS のカスタマイズ）の機能を IMOD で利用することができます。

IDCAMS ロード モジュールが利用可能であるか確認してください。このモジュールは、APF 許可 LINKLIB データセット内にあり、CA-GSS/ISERVE からアクセスできる必要があります。-

IDCAMS 向けに CA-GSS をカスタマイズする方法

1. GSSA システム PROCLIB メンバを変更します。

   LINKLIST ライブラリ内に IDCAMS ロード モジュールがない場合は、CA-GSS プロシージャ（BYSGSSA）にそのライブラリを STEPLIB として組み込みます。

2. CA-GSS パラメータを変更します。

   必要に応じて CA-GSS の IDCAMS サポートに影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの IDCAMS メンバに、これらのパラメータの例が含まれています。

   IDCAMS メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク（*）をブランクに置き換えます。

   IDCAMS メンバの内容を RUNPARM メンバにコピーするか、単に IDCAMS ステートメントを記述します。

   - ADDRESS パラメータは、IDCAMS ロード モジュールによって提供される ADDRESS 環境を REXX IMOD が利用できるようにします。
   - CA の提供する IMOD では、アドレス名が IDCAMS であることを前提にしています。- 他の名前を使用する場合は、ALTNAME パラメータを使用して IDCAMS を定義してください。

オプション機能

以下の CA-GSS オプション機能を使用する必要があるかどうかを考慮します。

GoalNet

GoalNet は LU 6.2 ベースの通信プロトコルで、CA-GSS が CA Technologies 製品およびユーザ記述の IMOD によるシステム間通信を許可するために使用します。

GoalNet は、VTAM を使用してローカル システム上の複数の z/OS 間または複数の CA-GSS 間の通信を有効化する場合に使用します。

ILOG

ILOG ファイルは、WTO テキストおよび他の対象イベントの記録に使用される VSAM 線形データセット(LDS)です。

CA Insight Database Performance Monitor for DB2 for z/OS を使用する場合、またはデータ取り込みやデータ処理用に IMOD アプリケーションを独自に作成した場合は、ILOG を使用する必要があります。

ログオン機能

ログオン機能を使用すると、VTAM アプリケーションから CA-GSS/ISERVE 制御パネルにアクセスできます。

CA-GSS の表示と制御を VTAM アプリケーションから行う場合、ログオン機能の使用をお勧めします。

GoalNet

GoalNet に参加する各 ISERVE は、ノードと呼ばれます。各 GoalNet ノードには単一の VTAM ACB が必要です。各ノードが GoalNet 内の他の全ノードと双方向リンクを作成します。

GoalNet は、ピアツーピア実装です。各ノードがネットワーク内で専用のメンバシップを持ちます。

GoalNet の定義

GoalNet は、CA-GSS アドレス空間に組み込まれた PARMLIB DD ステートメントを使って指定されるパラメータで定義されます。ネットワーク内のすべてのアドレス空間で共通のパラメータを使用することができます。

GOALNET パラメータ

ネットワークに参加する各 CA-GSS アドレス空間に対して、GOALNET パラメータを 1 回ずつ指定します。CA-GSS では、GOALNETLOCAL パラメータによって自分のノードを認識します。GOALNET パラメータによって定義されたノードとのみ通信することができます。

CAW0OPTN メンバ: GOALNET

サンプルの GoalNet 定義が、CAW0OPTN データセットの GOALNET メンバ内に用意されています。独自に GoalNet 定義を作成する前に、このメンバを検討してください。

注: GOALNET の詳細については、「*Reference Guide*」および「*Administration Guide*」を参照してください。

LOGMODE テーブルのサンプル

IBM による LU 6.2 (APPC) の 実装では、各会話は LOGMODE に基づきます。LOGMODE とは、会話を実行する方法を定義する一連のパラメータです。LOGMODE パラメータの互換性のあるサブセットを達成するために、2 つのノード間で一定量のネゴシエーションが実行されますが、GoalNet すべての参加ノードで同一の LOGMODE パラメータを使用する必要があります。

特殊な LOGMODE である SNASVCMG は基礎的な IBM コードで使用され、他の会話を確立するための会話の確立に使用されます。SNASVCMG は、IBM が提供する値から変更しないでください。-

LOGMODE 定義は *LOGMODE* テーブルに結合されます。その結果、各アプリケーション ID によって 1 つの LOGMODE テーブルが 1 つずつ指定され、その LOGMODE テーブルからすべての LOGMODE エントリが選択されます。LOGMODE テーブルとデフォルトの LOGMODE は両方とも、アプリケーション ID 定義で指定されます。これらの値は VTAM オペレータ コマンドで変更できます。

LOGMODE テーブルは、VTAM で指定される MACRO ライブラリを使用してアセンブルされ、SYS1.VTAMLIB データセット (またはそれに相当するデータセット) にリンク エディットする必要があります。-- 提供された値は、内容を十分理解している場合以外は変更しないでください。SNASVCMG LOGMODE は IBM によって提供され、セッションの確立時に内部プロトコルによって使用されます。SNASVCMG LOGMODE を変更すると、GoalNet は多くの場合動作しなくなります。

CAW0OPTN メンバ: BYSMTAB

サンプルの LOGMODE テーブルが、CAW0OPTN データセットの BYSMTAB メンバに用意されています。このテーブルはそのまま使用してください。

提供された LOGMODE テーブルをアセンブルおよびリンク エディットしたものが、GOALNETT の名前で CAW0LOAD データセット内に渡されます。- LOGMODE テーブルは VTAM MACRO バージョン 3 リリース 4 を使用してアセンブルされています。このモジュールが使用中の VTAM リリースと互換性があることがわかっている場合は、これをコピーできます。それ以外の場合、自分のマクロ ライブラリを使用して、提供されたテーブルのソース コードのアセンブルとリンク エディットを実行してください。-

VTAM への GoalNet の定義

GoalNet にノードとして参加する各 ISERVE には、VTAM アプリケーション ID（ACB）が必要です。この ACB は LU 6.2 通信用（APPC=YES）に構成されている必要があります。ノードでは ACB を使用して他の GoalNet ノードとの会話を確立します。1 つの会話に 1 つの VTAM セッションが必要です。z/OS 間でのオペレーション時には、その会話は通信継続中割り振られたままの状態です。ターゲット ノードで z/OS が稼働していない場合、リモート ノードに対する要求が行われるとすぐに会話が終了します。結果を戻す必要がある場合は、別の会話が割り振られます。

CAW0OPTN メンバ: BYSVTAM

CAW0OPTN データセットの BYSVTAM メンバには、GoalNet アプリケーションとログオン機能アプリケーションの両方に対応するサンプル定義があります。最小パラメータのみが示されます。

重要: VTAM 要件を十分に理解している場合以外は、これらのパラメータを変更または追加しないでください。

ILOG ファイル

ILOG ファイルは、WTO テキストおよび他の対象イベントの記録に使用される VSAM 線形データセット（LDS）です。

ISERVE アドレス空間 1 つにつき最大 100 個の ILOG を割り振ることができ、ILOG 1 つにつき最大 10 個のサブファイルを持たせることができます。各サブファイルは 1 つの VSAM LDS です。処理中にサブファイルがいっぱいになると、次のサブファイルに切り替えて記録されます。

1 つ以上の ALLOC_ILOG コマンドが含まれる SRVMAINT ジョブを変更してサブミットします。1 つの ALLOC_ILOG ステートメントで、2 つの VSAM 線形データセットが割り振られます。このジョブを変更する場合、LINEAR パラメータと SHAREOPTIONS パラメータは変更しないでください。

ステートメントの例

```
ALLOC_ILOG NAME CLUSTER VOLSER xxxxxx CYL 1 1
```

これらのデータセットを割り振る方法として、CAW0JCL データセットの BYSIALI メンバを変更してサブミットするという方法もあります。

ログオン機能

CA-GSS は、VTAM への LU2 ゲートウェイを提供します。これにより端末ユーザは CA-GSS に接続でき、IMOD タスクの制御下でセッションを確立できます。一部の CA Technologies 製品では、パーソナル コンピュータで実行されているソフトウェアと通信するためのセッション コントロール IMOD が用意されています。さらに、端末ユーザが CA-GSS と、またアドレス環境を通じて他の CA 製品と対話できるように、使用中のシステムでアプリケーションを開発することもできます。

セキュリティ

ログオン プロシージャの際、各ユーザはユーザ ID およびパスワードの入力を求められます。ご使用のシステムが RACF（または、他の SAF 互換）セキュリティ ソフトウェアを使用している場合、ユーザ セッションは、そのユーザ ID の権限で実行されます。

ISET のアップグレード

CA Common Services for z/OS で配布されていない ISET が存在する場合、それに含まれる IMOD は別のバージョンの CA-GSS でコンパイルされた可能性があります。

一般的には、コンパイラおよびインタープリタのバージョンが少々異なっても問題になりません。しかし、CA-GSS では潜在的なエラーを取り除くために、初期化時に自動的に下位レベル（または上位レベル）の IMOD を再コンパイルします。この再コンパイルはメモリ内で行われますが、DASD の ISET へは再保存されません。

CA-GSS SRVMAINT プログラムは、ISET 内のすべての IMOD や、現在のリリースレベルにないすべての IMOD を再コンパイルする UPGRADE コマンドを備えています。

CAW0JCL データセットの BYSUPGR メンバには、ISET をアップグレードするためのサンプル JCL および制御ステートメントがあります。

注: SRVMAINT プログラムの詳細については、「*Administration Guide*」を参照してください。

ログオン機能の定義

各アプリケーションがログオン時に確実に使用できるようにするためにログオン機能を定義できます。

ログオン機能を定義する方法

1. ネットワークを定義します。

   ログオン機能をアクティブにする前に、VTAM アプリケーション ID を定義する必要があります。VTAM システムのプログラマに問い合わせて、端末からのログオンを受け入れられる LU の名前を確認してください。通常は、デフォルトをすべてそのまま適用してかまいません。

   サンプルの VTAM 定義については、CAW0OPTN データセットの BYSVTAM メンバを参照してください (このメンバは GoalNet の定義にも使用されます)。

2. アプリケーションを指定します。

   各アプリケーションがログオンに適しているかを名前で判断する必要があります。また、端末からの入力の受け付け、処理、および表示用 3270 データストリームの提供の機能を持つ IMOD を各アプリケーションに付与します。たとえば、CA では CA-GSS オペレータ インターフェースを実現するアプリケーション IMOD(\$SRVV)を提供しています。

   注: アプリケーション IMOD の作成の詳細については、「*Administration Guide*」を参照してください。

3. CA-GSS パラメータを変更します。

   必要に応じて、ログオン機能に影響を与える CA-GSS 初期化パラメータを変更します。CAW0OPTN データセットの LOGON メンバに、これらのパラメータの例が含まれています。以下の事項に注意してください。

   - LOGON メンバのパラメータの多くはコメント化されています。これをアクティブにするには、先頭のアスタリスク(*)をブランクに置き換えます。
   - LOGON メンバの内容を RUNPARM メンバにコピーするか、INCLUDE LOGON ステートメントを記述します。
   - 以下の表で、変更が必要となる場合があるパラメータについて簡単に説明します。

パラメータ	説明
LOGON LUNAME `LOGON LUNAME luname password`	*luname* を VTAM に定義されたアプリケーション ID に置き換えます。これは、端末ユーザが CA-GSS とのセッションを要求するときに使用する名前です。また、使用中のシステムが VTAM パスワードを必要とする場合は、正しい値を指定する必要があります。*パスワードが必要でなければ*、password を削除し、このフィールドはブランクのままにします。 このパラメータは必須です。
LOGON APPLICATION `LOGON APPLICATION OPERator $SRVV`	ログオン機能で使用される各アプリケーションは、初期化の際に(または後で LOGON DEFINE コマンドを使用して)定義する必要があります。アプリケーション、アプリケーションの処理をサポートする IMOD、および IMOD に渡されるオプションの引数文字列に、名前を割り当てる必要があります。

注: アプリケーション名は、例に示すように大文字と小文字が区別されます。アプリケーションを選択する際、先頭の大文字はすべて指定する必要があります。一方で、後に続く小文字部分は省略できます。アプリケーション名の特別な使用法を除き、その他のフィールドでは大文字小文字が区別されません。たとえば、アプリケーション名「USERs」は、文字列「user」および「users」と一致します。しかし、文字列「use」または「userid」とは一致しません。

OPERATOR アプリケーションには CA-GSS(IMOD $SRVV)が用意されており、これをアクティブにすることで VTAM ベースの CA-GSS/ISERVE 制御パネルを利用することができます。

第 13 章: CA-L-Serv 設定タスク

CA Common Services for z/OS をインストールしたら、CA-L-Serv を起動する前に、設定タスクとプロシージャを実行する必要があります。

注: これらのタスクを実行するとき、展開されたデータ セットを使用します。

このセクションには、以下のトピックが含まれています。

CA-L-Serv の外部セキュリティの更新

CA-L-Serv を使用してデータセットを管理する予定がない場合は、このセクションを省略できます。

CA-L-Serv 3.5 では、主に以下に示す 2 つの点についてセキュリティが拡張されています。

- 外部セキュリティを呼び出して、CA-L-Serv によってユーザの代わりにデータセットをオープンさせるために必要な権限がユーザにあることを検証した後で、CA-L-Serv を使用したデータセットのオープンが許可されます。この検証は、新規の $LSRVDSN リソース クラスを使用して、ユーザ アクセスとデータセットを突き合わせてチェックすることにより実行されます。
- ADDFILE コマンドによって制御下に置かれたデータセットをオープンすることを CA-L-Serv に許可する前に、外部セキュリティを呼び出して、データセットをオープンする権限がその CA-L-Serv ユーザ ID にあるかを検証します。

更新の必要があるシステム

CA-L-Serv を初めてインストールする場合のセキュリティ システム、または CA-L-Serv レベル 9501 またはそれより古いレベルからアップグレードする場合は、セキュリティ システムを更新して以下の操作を実行する必要があります。

- CA-L-Serv スターティッド タスク固有のユーザ ID を作成し、管理対象データセットにアクセスできる権限をこのユーザ ID に付与します。
- ファイル サーバの管理下に置かれているデータセットのリソース クラスを作成し、この新しいリソース クラスにアクセスできる権限をユーザに付与します。

更新作業の実行

セキュリティを拡張する場合、一般にセキュリティ管理者は以下の作業を実行する必要があります。

- 新規のリソース クラス $LSRVDSN を作成します。
- 新規のリソース クラスに対し CA-L-Serv データセットを定義します。
- 新規のリソース クラスを使用してユーザにアクセスを許可します。
- CA-L-Serv スターティッド タスクのユーザ ID を作成します。
- CA-L-Serv のユーザ ID にデータセットへのアクセスを許可します。

使用上の注意

以下に注意事項を示します。

- CA Endevor Software Change Manager などの製品に事前に実装されているセキュリティ定義は、変更する必要はありません。これらの製品で行われるセキュリティ検査は、以前と同様に機能します。
- 各 CA-L-Serv データセットを区別しない場合は、クラス $LSRVDSN で「ALL」という名前のリソースを定義し、このリソースの CONTROL アクセス権をユーザまたはグループに付与することで、広範なセキュリティ定義を新たに作ることなく CA-L-Serv データセットへのアクセスを簡単に制御することができます。
- $LSRVDSN クラスを使用することをユーザを許可する場合、そのユーザに付与されるのは、CA-L-Serv を経由したデータセットへのアクセス権のみです。他のプログラム（IDCAMS REPRO など）を経由したデータセットへのアクセス権は付与されません。

- CALServ の管理下に置かれているデータセットへの CONTROL アクセス権をすでに持っている特権ユーザは、CA-L-Serv 以外の場合と同じ方法で、CA-L-Serv を使用してデータセットにアクセスすることができます。これらの特権ユーザには、追加定義は必要ありません。
- CA-L-Serv ユーティリティ プログラム LDMAMS は、データセットへの CONTROL アクセス権を持つユーザ ID のでのみ実行できます。

重要: CA Endevor Software Change Manager ユーザは、「代替」ユーザ ID ではなく「真」のユーザ ID に新規リソースクラスへのアクセス権を付与する必要があります。CA Endevor Software Change Manager が CA-L-Serv を呼び出すと、「代替」ユーザ ID ではなく「真」のユーザ ID に許可が付与されます。

以降のセクションでは、3 つの異なる環境における CA-L-Serv の外部セキュリティの実装について説明します。

CA Top Secret を使用したセキュリティの実装

以下に、CA Top Secret 環境で実行しているユーザ用のサンプル定義を示します。使用中の環境における実際の実装では、以下のテンプレートと異なる場合があります。

CA Top Secret を使用してセキュリティを実装する方法

1. CA Top Secret のリソース記述子テーブル(RDT)に対し、新規のリソース クラスを定義します。以下に例を示します。

   ```
   TSS ADD(RDT) RESCLASS($LSRVDSN) RESCODE(02) ATTR(LONG,DEFPROT)
                ACLST(CONTROL) DEFACC(CONTROL)
   ```

   注: コマンド構文と機能の詳細については、「*CA Top Secret Reference Guide*」を参照してください。

2. $LSRVDSN リソース クラスを使用してデータセットを保護します。

   1 つの方法は、CA-L-Serv の制御下にあるデータセットを定義するコマンドを実行することです。

   ```
   TSS ADDTO(owner_acid) $LSRVDSN(prefix1)
   TSS ADDTO(owner_acid) $LSRVDSN(prefix2)
   ```

   もう 1 つの方法は、CA-L-Serv 制御下のすべてのデータセットを表す「ALL」という名前の擬似データセットを定義することです。

   ```
   TSS ADDTO(owner_acid) $LSRVDSN(all)
   ```

3. CA-L-Serv データセットへのアクセスをユーザに許可します。

   リソースを保護した後、PERMIT コマンドを実行して、$LSRVDSN リソース クラスを使用したこれらのデータセットへのアクセスをユーザに許可します。

   ```
   TSS PERMIT(user_acid1) $LSRVDSN(dsname1) ACCESS(CONTROL)
   TSS PERMIT(user_acid1) $LSRVDSN(dsname2) ACCESS(CONTROL)
   TSS PERMIT(user_acid2) $LSRVDSN(dsname1) ACCESS(CONTROL)
   ```

   これは、総称プレフィクスを使用しても実行できます。

   ```
   TSS PERMIT(user_acid)  $LSRVDSN(prefix.) ACCESS(CONTROL)
   ```

   必要に応じて、「ALL」リソースへのアクセスをユーザに許可することもできます。

   ```
   TSS PERMIT(user_acid1) $LSRVDSN(all) ACCESS(CONTROL)
   TSS PERMIT(user_acid2) $LSRVDSN(all) ACCESS(CONTROL)
   ```

4. CA-L-Serv を CA Top Secret に定義します。

   ユーザ ID は、データセットにアクセスできるよう CA-L-Serv 向けに作成する必要があります。そのためには、以下を指定します。

   ```
   TSS CREATE(lserv_acid) TY(USER) DEPT(deptname) FAC(STC) -
       NAME('name') PASS(NOPW,0) NOSUBCHK
   ```

5. データセットへのアクセスを CA-L-Serv に許可します。

   データセットへのアクセス権を CA-L-Serv に付与するには、PERMIT コマンドを使用します。

   ```
   TSS PERMIT(lserv_acid) DSN(dsname1) ACCESS(CONTROL)
   TSS PERMIT(lserv_acid) DSN(dsname2) ACCESS(CONTROL)
   ```

   これは、総称プレフィクスを使用しても実行できます。

   ```
   TSS PERMIT(lserv_acid) DSN(prefix.) ACCESS(CONTROL)
   ```

CA ACF2 を使用したセキュリティの実装

以下に、CA ACF2 環境で実行しているユーザ用のサンプル定義を示します。使用中の環境における実際の実装では、以下のテンプレートと異なる場合があります。

- 新規の $LSRVDSN リソース クラスに、リソース タイプ LSV への CLASMAP を実行します。

  以下に例を示します。

  ```
  SET CONTROL(GSO)
  INSERT CLASMAP.LSRV2 ENTITYLN(44)-
         RESOURCE($LSRVDSN) RSRCTYPE(LSV)
  ```

  コンソールから MODIFY コマンドを実行します。

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

- $LSRVDSN リソース クラスを使用してデータセットを保護します。

  CA-L-Serv の制御下にあるデータセット用のリソース ルールを作成します。

  ```
  SET RESOURCE(LSV)
  COMPILE
  .$KEY(prefix1) TYPE(LSV)
  .UID(************userid1) SERVICE(DELETE) ALLOW
  .UID(************userid2) SERVICE(DELETE) ALLOW
  .<空白文字>
  STORE
  ```

  必要に応じて、CA-L-Serv の制御下にあるすべてのデータセットを表す「ALL」という擬似データセットを定義することもできます。

  ```
  SET RESOURCE(LSV)
  COMPILE
  .$KEY(ALL) TYPE(LSV)
  .UID(************userid1) SERVICE(DELETE) ALLOW
  .UID(************userid2) SERVICE(DELETE) ALLOW
  .<空白文字>
  STORE
  ```

- 関連するデータセットのアクセス ルールを作成または変更し、必要なアクセス権を CA-L-Serv に付与します。

```
SET RULE
COMPILE
.$KEY(prefix1)
.$MODE(ABORT)
.qualifier.qualifier UID(*************LSERV) WRITE(A)
.<空白文字>
STORE

COMPILE
.$KEY(prefix2)
.$MODE(ABORT)
.qualifier.qualifier UID(*************LSERV) WRITE(A)
.<空白文字>
STORE
```

RACF を使用したセキュリティの実装

以下に RACF 環境で実行しているユーザ用のサンプル定義を示します。使用中の環境における実際の実装では、以下のテンプレートと異なる場合があります。

- クラス記述子テーブル（CDT）に新規リソース クラスのエントリを追加します。次に、クラス記述子テーブル ICHRRCDE をアセンブルして、SYS1.LPALIB にリンクする必要があります。以下に例を示します。

```
LSERVDSN ICHERCDE CLASS=$LSRVDSN,                    X
               ID=(valid installation value),        X
               MAXLNTH=44,                           X
               FIRST=ALPHA,                          X
               OTHER=ANY,                            X
               POSIT=(valid installation value),     X
               OPER=NO,                              X
               RACLIST=ALLOWED,                      X
               DFTUACC=NONE
```

ID および POSIT の適切な値については、
RACF のマニュアルを参照してください。ID および POSIT IBM による制限とサイトによる制限をどちらも考慮する必要があります。

重要: クラス記述子テーブルに対する変更を有効にするには IPL が必要です。

- RACF ルータ テーブルへのリンクを更新します。

  CA-L-Serv インターフェースでは RACROUTE マクロを使用します。そのため、RACF ルータ テーブル（ICHRFR01）も
  更新され、リンクがリストされているライブラリにリンクされている必要があります。以下に例を示します。

```
ICHRFRTB CLASS=$LSRVDSN,                    X
         ACTION=RACF
```

- $LSRVDSN クラスをアクティブにします。

  新規のクラス記述子テーブルで IPL を実行した後、以下のコマンドを入力します。

```
SETROPTS CLASSACT($LSRVDSN)
```

- $LSRVDSN クラスを使用して、RACF に対しデータセットを定義します。

  CA-L-Serv の制御下にあるデータセットを定義するコマンドを実行できます。

```
RDEF $LSRVDSN dsname1 UACC(NONE) OWNER(ownerid)
RDEF $LSRVDSN dsname2 UACC(NONE) OWNER(ownerid)
RDEF $LSRVDSN dsname3 UACC(NONE) OWNER(ownerid)   (その他.. )
```

  必要に応じて、CA-L-Serv の制御下にあるすべてのデータセットを表す「ALL」というリソースを定義することもできます。

```
RDEF $LSRVDSN all     UACC(NONE) OWNER(ownerid)
```

- CA-L-Serv データセットへのアクセスをユーザに許可します。

  データセットをリソースとして定義した後、$LSRVDSN リソース クラスを使用したこれらのデータセットへのアクセスをユーザに許可するコマンドを実行します。

  ```
  PERMIT dsname1 ID(userid1) AC(CONTROL) CLASS($LSRVDSN)
  PERMIT dsname2 ID(userid1) AC(CONTROL) CLASS($LSRVDSN) ...
  ```

  必要に応じて、「ALL」リソースへのアクセスを CA-L-Serv ユーザに許可することもできます。

  ```
  PERMIT all     ID(userid1) AC(CONTROL) CLASS($LSRVDSN)
  PERMIT all     ID(userid2) AC(CONTROL) CLASS($LSRVDSN)
  PERMIT all     ID(userid3) AC(CONTROL) CLASS($LSRVDSN)
  ```

- RACF への CA-L-Serv の定義

  CA-L-Serv のデータセットへのアクセスを許可する CA-L-Serv 用のユーザ ID を作成します。それには、以下のコマンドを使用します。

  ```
  AU lsrv-id DFLTGRP(systask) PASSWORD(xxxxxxxx)
  ```

  この例では、ユーザ ID として *lsrv-id* を、グループとして *systask* を選択しています。これらの名前は任意に指定でき、名前の最大文字数は 7 文字です。

- RACF スターティッド プロシージャ テーブルに CA-L-Serv を追加します。

  RACF スターティッド プロシージャ テーブル（ICHRIN03）には、CA-L-Serv のエントリが含まれていることが必要です。これを実行するには、以下のどちらかの方法を使用します。

  - CA-L-Serv スターティッド タスク用に独立したエントリを設定します。
  - 以下に例を示します。

    ```
    LSERV DC CL8'LSERV'     CA-L-Serv proc name
            DC CL8'LSERVID'   CA-L-Serv userid
            DC CL8'SYSTASK'   CA-L-Serv group
            DC XL1'00'        unused
            DC XL7'00'        unused
    ```

    さらに、テーブル内のエントリの数に 1 を追加する必要があります。このテーブルをアセンブルして SYS1.LPALIB にリンクし、IPL を実行する必要があります。
  - このテーブル内に汎用エントリが存在する場合は、そのエントリに合わせて CA-L-Serv のプロシージャ名とユーザ ID を設定します。

- PERMIT コマンドを使用して、データセットへのアクセス権を CA-L-Serv に付与します。

  ```
  PERMIT 'data set name' ID(LSERVID) ACCESS(CONTROL)
  ```

VTAM への CA-L-Serv の定義

この手順は、VTAM を使用して、異なるシステムで実行されている CA-L-Serv のコピー間の通信をサポートする予定がある場合のみ必要です。

VTAM に対して CA-L-Serv を定義するには、以下の手順に従います。

1. CCCSOPTN メンバ SAMPACB をテンプレートとして使用して、SYS1.VTAMLST データセットにメジャー ノード メンバを作成します。
2. 別の z/OS イメージ上で実行されている別の CA-L-Serv インスタンスと VTAM を使用して通信するローカルの各 CA-L-Servv インスタンスについて、APPL ステートメントを指定します。
3. SYS1.VTAMLST の ATCCONxx メンバにメンバ名を追加して、VTAM に新しいメジャー ノードを指定します。これにより、VTAM を起動したときに対応する APPL がアクティブになります。
4. SYS1.VTAMLST データセットに対応する CDRSC 定義を追加して、VTAM に対しクロスドメイン リソースを定義します。

   注: *Yourdeploy*HLQ.CCCSOPTN データセットに用意されている SAMPACB の定義は、LU 0 あるいは LU 6.2 通信のどちらかで使用される可能性があります。
5. VTAM を再起動せずに新規定義をアクティブにするには、新たに定義されたリソースに対して「V NET,ACT,ID=...」コマンドを実行します。

起動パラメータのカスタマイズ

CA-L-Serv は、サンプル起動コマンド メンバ LSVPARM をターゲットの CCCSOPTN データセットに配置します。以下に、CA-L-Serv 起動パラメータ メンバの例を示します。以降で各行について詳しく説明します。

```
OPTION SVCDUMP(YES)                                (1)
ADDLOG  MSGLOG  SYSOUT(X)                          (2)
ADDLOG  SQLLOG  SYSOUT(X)
*
IFSYS SYSA                                         (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSA,            (4)
                      CONTYPE=LU0,
                      LOG=MSGLOG
    ACTIVATE COMMSYSB                              (5)
    ACTIVATE COMMSYSC
```

```
    ATTACH   FILESERVER SERVERTYPE=HOST          (6)
    ADDPOOL  01 (4096,32) (8192,16)              (7)
    ADDFILE  FILE1 XXXXXXX.FILE1.VSAM,POOL(1)    (8)
    ADDFILE  FILE2 XXXXXXX.FILE2.VSAM,POOL(1)
    ADDFILE  LDMSQL XXXXXXX.LSERV.SQLDICT,       (9)
                    BUFND=5 BUFNI=5
    ATTACH  SQLSERVER LOGID=SQLLOG AUDIT=ALL     (9)
ENDIF                                            (3)
*IFSYS SYSB                                       (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSB,
                    CONTYPE=LU0,
                    LOG=MSGLOG
    ACTIVATE COMMSYSA CONTYPE=LU0
    ATTACH FILESERVER SERVERTYPE=REMOTE          (*)
ENDIF                                            (3)
*IFSYS SYSC                                       (3)
    ATTACH COMMSERVER ACBNAME=COMMSYSC etc.
(...)
    ATTACH FILESERVER SERVERTYPE=REMOTE          (*)
ENDIF                                            (3)
```

補足:

(1) このコマンドにより、例外条件が発生したときのダンプを CA-L-Serv リカバリ コードでスケジュールできるようになります。

CA-L-Serv では、同じ異常終了が繰り返し発生した場合は重複してダンプを取らないため、このオプションは変更しないでください。

(2) ADDLOG コマンドにより、CA-L-Serv の各種コンポーネントのメッセージ ログが定義されます。

(3) IFSYS/ENDIF ステートメントにより、CA-L-Serv はシステムの sysid で一致が見つかるまで埋め込みコマンドをすべてスキップします。 これにより、単一の LDMPARM メンバ内の異なる z/OS イメージ上で関連する CA-L-Serv 領域が実行されている場合の起動パラメータの管理が容易になります。

(4) ATTACH コマンドを使用して、さまざまなサービスを z/OS サブタスクとしてアタッチします。 クライアント アプリケーションを正しく実行するために必要なサービスについては、クライアント アプリケーションのマニュアルを参照してください。

環境に関連のないステートメントを削除します。 たとえば、単一システム上で実行する場合は、通信サーバのコマンドはすべて不要です。

(5) ACTIVATE コマンドにより、同じサブシステム名を持ち、別々のシステムで実行されている CA-L-Serv 領域間の通信が確立されます。

注: このコマンドは VTAM 通信にのみ有効です。 XCF 通信を使用している場合は、コメント化するか削除します。

(6) このファイル サーバを HOST として指定します。これは、データセットに物理的にアクセスでき、SYSA 上で実行されているローカル領域からの要求と SYSB および SYSC 上で実行されているリモート呼び出し元からの要求を処理するサーバです。

注: 複合体内にある他のすべてのファイル サーバの SERVERTYPE は、REMOTE (*) です。単一 CPU 環境では、SERVERTYPE=LOCAL を指定します。

(7) ADDPOOL コマンドにより、VSAM を呼び出され、共有バッファのプールが作成されます。

(8) ADDFILE コマンドにより、データセットが動的に割り当てられ、CA-L-Serv で入出力要求を処理できるようになります。

(9) SQL Server を使用する予定がある場合は、このコンポーネントをアクティブにする前に SQL ディクショナリ(DDname=SQLDICT)を割り振る必要があります。

注: 独立した 3 つのメンバ(LSVPARM1、LSVPARM2、および LSVPARM3)における機能的に同等のセットアップは、*Yourdeploy*HLQ.CCCSOPTN データセットにも用意されています。

メッセージ テーブルの更新

CA-L-Serv をインストールすると、ターゲットの CAI.CCCSOPTN ライブラリにメッセージ メンバが挿入されます。CA-L-Serv を起動したときにこの新しいメッセージ メンバにアクセスできるように、このメンバをアクティブな CA-L-Servv PARMLIB にコピーする必要があります。

使用中のデータ センターの要件に合わせて、以下の JCL をカスタマイズします。

```
//LOAD     EXEC PGM=IEBCOPY,REGION=256K
 //SYSPRINT DD  SYSOUT=A
//I1       DD   DISP=SHR,
//         DSN=CAI.CCCSOPTN          <=== ご使用の展開された DSN
//O1       DD   DISP=SHR,
//         DSN=CAI.LDMCMND           <=== ご使用の展開された DSN
//SYSUT3   DD   UNIT=SYSDA,
//         SPACE=(CYL,(5,5))
//SYSUT4   DD   UNIT=SYSDA,
//         SPACE=(CYL,(5,5))
//SYSIN    DD *
  COPY O=O1,I=((I1,R))
  SELECT M=LSERVMSG
```

CA-L-Serv パラメータ データセットに古いバージョンの LSERVMSG メンバが含まれている場合は、この JCL をサブミットする前にそのメンバの名前を変更します。

起動プロシージャのコピーとカスタマイズ

CA-L-Serv のインストールにより、ターゲットのプロシージャ ライブラリ *Yourdeploy*HLQ.CCCSPROC に起動プロシージャ LSVPROC が追加されます。CA-L-Serv を起動したときにアクセスできるように、このプロシージャを SYS1.PROCLIB またはシステム プロシージャ ライブラリにコピーします。

以下のテンプレートが用意されています。

```
//LSVPROC PROC PLIB='CAI.CCCSOPTN', (1)/* CA-L-Serv PARMLIB    */
//  AUTHLIB='CAI.CCCSLOAD',           (2)/* CA-L-Serv LOADLIB    */
//  MEMB=LDMPARM,                    (3)/* CA-L-Serv parm member*/
//  JCL='CAI.CCCSJCL,                 (4)/* CA-L-Serv jcl lib    */
//  REUSE=YES,                       (5)/* Reuse CSA            */
//  SSN=LSRV                         (6)/* Subsystem name       */
//*
//********* CA-L-Serv ****************************************
//*
//* Use this procedure to start up L-Serv using a console command
//*
//*************************************************************
//*
//LSERV    EXEC PGM=LDMMAIN,REGION=8M,DPRTY=(15,15),TIME=1440,
//         PARM=('ME=&MEMB','REU=&REUSE','SSNM=&SSN')
//*
//STEPLIB  DD DSN=&AUTHLIB,DISP=SHR
//LDMCMND  DD DSN=&PLIB,DISP=SHR
//SYSPRINT DD SYSOUT=A
//SYSTERM DD  SYSOUT=A
//SYSUDUMP DD SYSOUT=A
//INTRDR   DD SYSOUT=(A,INTRDR)
//ERRORLOG DD SYSOUT=A
//JCLLIB   DD DSN=&JCL,DISP=SHR
```

起動プロシージャをカスタマイズする方法

1. LDMCMND DD を更新して、CA-L-Serv パラメータ データセット用に指定した名前を反映します。
2. STEPLIB DD を更新して、CA-L-Serv ロード ライブラリ用に指定した名前を反映します。
3. 初期化時に CA-L-Serv が読み取る LDMCMND PARMLIB の LDMPARM メンバを指定します。
4. JCLLIB DD を更新して、CA-L-Serv JCL ライブラリ用に指定した名前を反映します。
5. CA サポートによって特に指示されていない限り、必ず REUSE=YES を指定します。
6. 固有のサブシステム名を指定します。

重要: SYS1.PARMLIB のアクティブな IEFSSNxx メンバを使用して CA-L-Serv z/OS サブシステムを定義しないでください。CA-L-Serve および関連付けられている製品が正常に初期化されなくなります。

CA-L-Serv の起動

START コマンドを使用して、z/OS コンソールから CA-L-Serv を起動します。

- まったく同じ z/OS サブシステム名とプロシージャ名を使用する場合は、「START *lsvproc*,SUB=JES*x*」と指定することで、ジョブ入力サブシステムに対し実行内容を明示的に指示します。これにより、CA-L-Serv が z/OS マスタ スケジューラの制御下で実行されなくなります。
- パラメータに構文エラーがあると、CA-L-Serv が終了する場合があります。自動的に再起動すると、そのたびに余分なシステム リソースが割り振られるため、自動的に再起動するのではなく、エラーの原因を調べて訂正してから再起動するようにしてください。

通信サーバのインストールの検証

複数のシステム上で CA-L-Serv を使用する予定がない場合、または CA-L-Serv 通信サーバを使用しない場合は、このセクションを省略できます。

通信サーバ用のインストール検証プロシージャによって、異なるシステムで実行されている CA-L-Serv タスクが通信を確立してメッセージを交換できることを確認します。

以下の手順は、CA-L-Serv を使用して通信を確立する各システム間で繰り返し実行できます。

通信サーバのインストールを検証する方法

1. JCL メンバ HJ35IVC1 および HJ35IVC2 をカスタマイズします。

   インストール時に CCCSJCL データセットに挿入される、メンバ HJ35IVC1 および HJ35IVC2 で利用可能な以下のテンプレートをカスタマイズします。

   ジョブの受信:

```
//HJ35IVC1 JOB (JOBACCNT)                    (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB  DD   DISP=SHR,DSN=CAI.CCCSLOAD     (2)
//SSN$xxxx DD   DUMMY                        (3)
//SYSPRINT DD   SYSOUT=X
//SYSIN    DD *
  COMMTEST                                  (4)
  RECEIVE
  END
/*
```

ジョブの送信:

```
//HJ35IVC2 JOB (JOBACCNT)                    (1)
//MAMS0001 EXEC PGM=LDMAMS
//STEPLIB  DD   DISP=SHR,DSN=CAI.CCCSLOAD     (2)
//SSN$xxxx DD   DUMMY                        (3)
//SYSPRINT DD   SYSOUT=X
//SYSIN    DD *
  COMMTEST                                   (4)
  WAIT APPL(HJ35IVC1)
  SEND
  END
/*
```

補足:

(1) 有効なジョブ カードを指定します。

(2) CA-L-Serv ターゲット ライブラリに変更します。

(3) *xxxx* に、CA-L-Serv 起動プロシージャで指定した z/OS サブシステム名を指定します。

(4) どちらのジョブの SYSIN ステートメントも簡潔で、見たとおりの内容です。

重要: 2 つのジョブの名前は異なっている必要があります。

2. 両方のシステムで CA-L-Serv を起動します。

   テストを実行する 2 つの z/OS システムで CA-L-Serv を起動します。

   重要: このテストを正常に実行するには、通信サーバとファイル サーバの両方を ATTACH する必要があります。

3. HJ35IVC1 をサブミットします。

   2 つのシステムの一方で、このジョブをサブミットします。このジョブは、もう一方の z/OS システム上の相手側からメッセージを受け取るクライアント アプリケーションをエミュレートします。HJ35IVC1 は、送信側システムからデータを受け取るまで待機します。

4. HJ35IVC2 をサブミットします。

   2 つの z/OS システムのもう一方で、このジョブをサブミットします。このジョブは、もう一方のシステムで実行されているジョブ HJ35IVC1 に 512 バイトのデータを送信します。このジョブをサブミットすると、即時に両方のジョブが終了します。

5. 結果を検証します。

   - ジョブ HJ35IVC1 のスプール出力を参照します。以下のメッセージが含まれています。

```
      COMMTEST
LDM0829I CommServer initialization returned  RC=0000  Reason=0000
      RECEIVE
LDM0832I Receive complete: APPL=HJ35IVC2 QUAL=COMMTEST Length=512
      END
LDM0829I CommServer LCOMSHUT returned  RC=0000  Reason=0000
```

   - ジョブ HJ35IVC2 のスプール出力を参照します。これには以下のメッセージが含まれています。

```
      COMMTEST
LDM0829I CommServer initialization returned  RC=0000  Reason=0000
      WAIT APPL(HJ35IVC1)
      SEND
LDM0829I CommServer send returned  RC=0000  Reason=0000
      END
LDM0829I CommServer LCOMSHUT returned  RC=0000  Reason=0000
```

   どちらのジョブも、0 より大きいリターン コードがある場合は、問題があります。

   これで、通信サーバのインストールが検証されました。

トラブルシューティング : 通信サーバ IVP が正常に動作しない

症状

通信サーバの IVP が正常に実行されなかった場合、いくつかの原因が考えられます。このような問題を早期に特定することが、まさに IVP の目的とするものです。

解決方法

以下を実行してください。

- ジョブ HJ35IVC1 および HJ35IVC2 の出力を確認します。
- 両方のシステムの CA-L-Serv のメッセージ ログを調べ、対応するタイムスタンプを持つメッセージを探します。
- ファイル サーバと通信サーバが両方のシステムでアクティブであることを確認します。DISPLAY ACTIVE コマンドにより、現時点でアクティブなサーバをリスト表示します。

- 両方の IVP ジョブの SSN$xxxx DD DUMMY ステートメントで指定されているサブシステム名が CA-L-Serv プロシージャ（LSVPROC）で指定されているサブシステム名と一致することを確認します。
- VTAM 通信を使用している場合は、「DISPLAY NET,ID=」コマンドを実行して、APPL 定義と CDRSC 定義の状態を確認します。
- XCF を使用している場合は、「D XCF,G」コマンドを実行して、通信サーバで作成された XCF グループの状況を確認します。起動時に CA-L-Serv により初期化されるグループは LSRV*xxxx* です。ここで、「*xxxx*」は CA-L-Serv プロシージャ（LSVPROC）で指定されたサブシステム名です。

以上の項目を確認した後も問題が解決されない場合は、関連する診断情報を用意して、CA サポートまでお問い合わせください。

ファイル サーバのインストールの検証

CA-L-Serv を使用してデータセットを管理する予定がない場合は、このセクションを省略できます。

ファイル サーバのインストール検査手順では、CA-L-Serv と同じシステムで実行されているアプリケーションが、ファイル サーバの管理下にあるデータセットにアクセスできることを確認します。

CA-L-Serv をインストールすると、ターゲット ソース ライブラリ CCCSJCL にインストール検証用 JCL メンバ HJ35IVF1 および HJ35IVF2 が挿入されます。

ファイル サーバ IVP は、LDMAMS ユーティリティを使用して、管理対象データセットに対し簡単なメンテナンス タスクを実行します。

注: この手順では VSAMTEST ファイルを使用しますが、クライアント製品のデータセットの 1 つをバックアップする方法もあります。

ファイル サーバのインストールを検証する方法

1. VSAM テスト ファイルを初期化して、作業ファイルを割り振ります。

   インストール時に CCCSJCL データセットにコピーされたジョブ HJ35IVF1 をカスタマイズして実行します。このジョブにより、CAI.VSAMTEST VSAM データセットと順次作業ファイルが割り振られ、初期化されます。

```
//HJ35IVF1 JOB (JOBACCNT)                                      (1)
//IEFBR14  EXEC PGM=IEFBR14                                    (2)
//BACKUP   DD DISP=(,CATLG,DELETE),DSN=CAI.VSAMTEST.BACKUP,(3)
//         VOL=SER=XXXXXX,UNIT=SYSDA,                          (4)
//         DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB),
//         SPACE=(3120,(1,1))
//*
//DEFCL    EXEC PGM=IDCAMS                                     (5)
//SYSPRINT DD  SYSOUT=*
//SYSIN    DD *
 DEFINE CLUSTER (                                    -
                 NAME                  (CAI.VSAMTEST) -   (6)
                 VOLUMES                     (XXXXXX) -
                 TRACKS                       (1   0) -   (7)
                 RECORDSIZE                   (80 80) -   (8)
                 KEYS                         (10 00) -   (9)
                 FREESPACE                    (10 10) -
                 SHR                          (2   3) -
                 REUSE                                -  (10)
                 INDEXED                              -
                                                    ) -
```

```
         DATA   (                                        -
                 NAME             (CAI.VSAMTEST.DATA) -    (6)
                 CISZ                          (8192) -
                                                    ) -
         INDEX  (                                        -
                 NAME            (CAI.VSAMTEST.INDEX) -    (6)
                 CISZ                          (2048) -
                                                    )
//*
//REPRO   EXEC  PGM=IDCAMS
 //SYSPRINT DD  SYSOUT=A
//SYSIN    DD *
 REPRO INFILE(INFILE) ODS(CAI.VSAMTEST)                    (11)
//INFILE   DD   *
0000000000                                                 (12)
0000000001
0000000002
(etc..)
```

補足:

(1) 有効なジョブ ステートメントを指定します。

(2) 作業ファイルを割り振ります。

(3) 作業ファイルに有効な DS 名を指定します。

(4) 有効な VOLSER と装置名を指定します。

(5) VSAM テスト ファイルを割り振り、初期化します。

(6) 有効な DS 名と VOLSER を指定します。

(7) 領域を割り振ります。

(8) 8 バイトのレコード。

(9) キー フィールドの長さは 10 バイトで、先頭のオフセットは +0 です。

(10) リストアや圧縮など、他の LDMAMS 機能を実行する場合は、REUSE を指定します。

(11) VSAMTEST ファイルを初期化します。

(12) 複数の初期化レコードを指定し、重複するキーがないことと、順序に従っていることを確認します。

既存のデータセットをバックアップする場合は、この手順のほとんどを省略することができます。

2. CA-L-Serv を起動します。

   起動デックに ATTACH FILESERVER ステートメントが含まれていることを確認して、CA-L-Serv を起動します。ファイル サーバが正しく初期化されたことを検証するには、以下のコマンドを実行します。

   ```
   DISPLAY TASK(FILESERVER) ALL
   ```

3. VSAM テスト ファイルをファイル サーバの管理下に置きます。

   テスト用の VSAM データセットを CA-L-Serv の管理下に置くには、z/OS コンソールから以下のコマンドを実行します。

   ```
   ADDFILE ddname test.file.dsname
   ```

4. サイトの要件に合わせて HJ35IVF2 JCL をカスタマイズします。

   使用中のデータ センターの要件に合わせて、以下の JCL をカスタマイズします。

   ```
   //HJ35IVF2 JOB (JOBACCNT)                      (1)
   //MAMS0000 EXEC PGM=LDMAMS
   //STEPLIB  DD   DISP=SHR,DSN=CAI.CCCSLOAD       (2)
   //BACKUP   DD   DISP=SHR,DSN=VSAMTEST.BACKUP  (3)
   //SSN$xxxx DD   DUMMY                          (4)
   //SYSPRINT DD   SYSOUT=XA
   //SYSIN    DD *
      REPRO INFILE(VSAMTEST)  OUTFILE(BACKUP)    (5)
   ```

   補足:

   (1) 有効なジョブ ステートメントを指定します。

   (2) CA-L-Serv ターゲット ライブラリに変更します。

   (3) テスト順次データセットの DS 名を指定します。

   (3) *xxxx* に、CA-L-Serv 起動プロシージャで指定した z/OS サブシステム名を指定します。

   (5) 構文は IBM IDCAMS ステートメントに似ています。

   注: LDMAMS ジョブの手順では、VSAM ファイルを割り振らないでください。このファイルを割り振る必要はなく、割り振った場合はジョブが正しく実行されません。

5. ジョブ HJ35IVF2 をサブミットし、SYSPRINT データセットを調べます。

   以下のメッセージが含まれています。

```
REPRO INFILE(VSAMTEST) OUTFILE(BACKUP)

LDM0810I nn records copied from VSAMTEST to BACKUP - REPRO
         operation complete
```

第 14 章: 他の設定

CA Common Services for z/OS をインストールして展開したら、その後に必要なタスクをさらにいくつか実行する必要がある場合があります。CA Common Services for z/OS を使用するのはその後になります。

注: これらのタスクを実行するとき、展開されたデータ セットを使用します。

このセクションには、以下のトピックが含まれています。

CAECIS CA EXAMINE 設定タスク

CAISERVX は、環境に関する基本的な診断情報や製品情報を収集するための CA 共通インベントリ サービス(CAECIS)プログラムです。製品に関する疑問点や問題に対処する CA サポート担当者によって使用されます。このユーティリティを実行すると、実行環境についての有用な情報が生成されます。CA のサポート担当者は、この情報を元に特定の問題を迅速に解決することができます。

CAISERVX プログラムから報告される情報によって、実行環境の概要を把握することができます。たとえば、以下の情報を確認できます。

- オペレーティング システムのリリース
- JES(Job Entry Subsystem)情報
- SYSRES(System Residence)情報
- IPL 関連の情報(以下の内容を含む)
  - システム IPL の時刻/日付
  - CPU モデル/シリアル番号
  - IPL LOADPARM 値
  - アーキテクチャ モード

- CAIRIM 関連の情報（以下の内容を含む）
  - CAIRIM 経由で初期化された製品
  - CAIRIM によってインストールされた SMF インターセプト
  - CAIRIM によってインストールされたサブシステム名
- CAIENF スターティッド タスクのステータス
- 使用中のシステム リンク ライブラリ（LINKLIST）データセット
- 使用中のリンク パック エリア ライブラリ（LPA）データセット
- 使用中の APF 許可されたライブラリ
- インストール済みの CA メインフレーム管理ソリューションのインベントリ情報

CAECIS の利用

CA Common Services をインストールすると、CAECIS もインストールされます。

CAECIS を使用する方法

1. CA Technologies 製品の問題が、具体的にどの z/OS システムで発生しているかを特定します。CAISERVX を実行するためのバッチ ジョブは、このシステムで実行する必要があります。
2. *Yourdeploy*HLQ.CAW0JCL 内にある CAISERVX 実行 JCL を使用します。
3. 前の手順で作成したメンバの先頭に、SAMPJCL にある JOBCARD メンバをコピーします。
4. インストールの要件に応じて JOB ステートメントを修正します。TIME 値と CLASS 値を適宜調整します。CAISERVX では、システム リンク リストのすべてのデータセットが処理されるため、JOB ステートメント パラメータにはこの点を考慮する必要があります。
5. CA Common Services の展開時に作成された CAW0PROC データ セットを参照するように、適宜、JCLLIB ステートメントを修正します。

6. z/OS のユーザ ID に、以下の作業を実行できるだけの適切なセキュリティ権限があることを確認します。
   - z/OS の TSO（タイム シェアリング オプション）サービスを使用する。
   - すべてのシステム リンクリスト（LNKLSTxx）およびリンク パック域（LPA）ライブラリを読み取る。
   - ジョブをサブミットする（リターン コード 0 が返る）。
7. 出力を保存し、必要に応じて CA サポートに送信します。

   デフォルトでは、CAISERVX プロシージャは、ユーティリティ出力を CAICIS DD ステートメントに書き込み、それを SYSOUT データセットに割り当てます。必要であれば、CAISERVX プロシージャを修正し、ユーティリティ出力を物理データセットにリダイレクトすることもできます。詳細については、CAW0PROC の CAISERVX プロシージャ内の指示を参照してください。

CAISDI 設定タスク

CAISDI を実装することにより、soap、elmds、med、els のすべてのコンポーネントにアクセスできるようになります。

CAISDI タスクを実装する方法

1. z/OS システム上で TCP/IP を構成します。
2. z/OS システムからネットワーク経由でアクセス可能なサーバに CA Service Desk をインストールします。
3. z/OS システム上で CAICCI を構成します（まだ済んでいない場合）。
4. ご利用の環境の CAISDI コンポーネントを設定します。

   注: CAISDI/soap、CAISDI/elmds、CAISDI/med、CAISDI/els の設定の詳細については、「*CA Service Desk Integration Guide*」を参照してください。
5. CAISDI インターフェースを使用する CA Technologies 製品を設定します。

Earl Service 設定タスク

CA Earl Service には、オプションの設定タスクがあります。

CCCSJCL のメンバ AXEI0040 の指示に従い、デフォルトの EARLOPT オプション設定を変更します。このメンバによって、Earl オプション モジュール EARLOPT を SMP/E の制御下で更新する USERMOD UXE6101 が提供されます。

注: Earl Service のデフォルト オプションの詳細については、「*CA Earl Systems Programmer Guide*」を参照してください。

重要: カスタマイズしたオプション設定を保存する前に、必ずこの USERMOD のコピーをバックアップしてください。

重要: デフォルト値を変更する場合は、注意が必要です。デフォルト値は、Earl サービスを最大限に活用できるようにするために用意されています。これらのデフォルト値を変更すると、実行時に予期しない結果が発生する場合があります。

Earl Service のインストールの確認

Earl Service が正しくインストールされていることを確認するには、JCL とサブミットのコメントに従って、CCCSJCL メンバ AXEI0050 を変更します。

CA MSM Common Services の設定

CA MSM Common Services を設定するには、以下の手順に従います。

1. CA MSM Common Services zFS の集まりを定義し、フォーマットします。CAW0JCL のメンバ ETNI0100 を編集し、サブミットします。
2. マウント ポイントを作成し、zFS ファイルをマウントします。CAW0JCL メンバ ETNI0200 を編集し、サブミットします。
3. 新しい MOUNT ポイントを含めるために SYS1.PARMLIB 内の BPXPARM メンバを更新します。
4. 追加の設定手順およびコンポーネント情報については、「*CA Mainframe Software Manager Release Notes*」および「*CA Mainframe Software Manager Administration Guide*」を参照してください。

SRAM Usermod

SRAM では、日付を表示するときに年を 4 桁で表示します。ソートするデータに 2 桁の年がある場合、2000 年以降の年の日付が 1900 年代の日付としてソートされる可能性があります。この問題を解決するには、CCCSJCL メンバ ASRIOPTN を使用します。

2 桁の年をソートするキー タイプを操作するように SRAM をカスタマイズするには、USERMOD（ASR0001）を使用できます。次の表にキー タイプを示します。

キー	タイプ	サイズ
Y2C	Character Year	2 バイト
Y2Z	Zoned Year	2 バイト
Y2P	Packed Year	2 バイト
Y2S	Character Year	2 バイト
Y2D	Decimal Year	1 バイト
Y2B	Binary Year	1 バイト

usermod では、生成された Y2K ウィンドウのルールに基づき、2 桁の年に対応する西暦の値を定義します。

固定された Y2K ウィンドウまたは移動する Y2K ウィンドウを定義できます。CCCSOPTN データ セットの SRAMCNFG メンバでは、CAISRAM マクロはキーワード パラメータ Y2PAST= で起動されます。4 桁の年を指定して固定ウィンドウを定義します。2 桁の年を指定して移動ウィンドウを定義します。

```
CAISRAM Y2PAST=1967 fixed

CAISRAM Y2PAST=88 sliding
```

固定ウィンドウモードでは、2 桁の年の値以上の数値の日付は、指定した西暦と日付に変換されます。また、2 桁の年の値より小さい数値は、以下のように西暦に変換されます。

移動ウィンドウ モードでは、日付は、TIME マクロによってシステムから返された現在の日付を基準にして変換されます。

アセンブルされた SRAMCNFG は、デフォルトの固定フォーマット値「Y2PAST=1967」で配布されます。つまり、2 桁の日付の場合、xx が 67 より小さい場合は 20xx に変換され、xx が 67 以上の場合は 19xx に変換されます。

用意されているデフォルト設定が用途に適していない場合、Y2PAST 値を変更し、このジョブをサブミットして、この usermod を RECEIVE、APPLY、ACCEPT します。

Viewpoint 設定

Viewpoint のインストールを完了するには、メンバに対する必要な追加や変更を加えた後、Viewpoint プロファイル ライブラリを更新するために CCCSJCL メンバ DU4I0010 をサブミットします。DU4I0010 メンバは他の CA 製品と共有でき、追加パラメータを加えることができます。

この手順を実行する前に、他の製品によって ViewPoint プロファイル データ セットが使用されていないことを確認してください。この手順を実行することで、望ましくない結果が生じる可能性があるためです。

注: すべて大文字にする必要があるカタカナ端末の場合は、メンバ CACCENV を編集して KATAKANA=UPPER を追加します。デフォルトでは大文字と小文字が混在します。

第 15 章: CA Datacom/AD のインストール

CA Common Services for z/OS コンポーネント用の設定タスクをインストールし実行した後に、オプションで CA Datacom/AD をインストールできます。

CA Datacom/AD をインストールするには、特定の CA Common Services for z/OS 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。CA Common Services は 4 つのバンドルまたは PAX ファイルで出荷されます。LEGACY PAX ファイル内にある CA-C Runtime を除くすべての DATACOM/AD 要件が含まれる BASE PAX ファイルにバンドルされたコンポーネントをすべてインストールする必要があります。Datacom/AD をインストールするが、すべての必要な CA Common Services コンポーネントをインストール済みとは限らなかった場合は、インストールしてから CA Datacom/AD のインストールを続行します。

- コンポーネントの CAIRIM、CAICCI、CAIENF、および CAISSF が必要です。それらは CAW0LINK および CAW0LOAD データ セットにインストールされます。
- CA Dataquery にはコンポーネント CA-C Runtime が必要です。それは CCCSLINK データ セットへインストールされます。

このバージョンの CA Common Services が付属する CA Datacom/AD リリースのインストール手順については、「*CA Datacom/AD Installation and Maintenance Guide*」を参照してください。

インストールを実行したら、この章に戻って CAIENF および Event Management をカスタマイズする必要があります。

注: CAIENF で正しく機能するために、CA Datacom/AD r12.0 には PTF RO18150 を適用する必要があります。

CA Datacom/AD の新規ユーザと既存ユーザのどちらも、CAIENF が実行されている各システムで、CAIENF と Event Management のデータ処理のみに使用される固有の MUF を実行する必要があります。

CAIENF イベント データは、システムごとに固有です。他の CA 製品と CA Datacom/AD MUF を共用することは、以下の理由により実用的であるとは言えません。

- 他の CA 製品の場合は、通常、システム共通 MUF を使用して、複数のシステムでデータを共用します。
- 保守とバックアップに問題が発生する可能性があります。

この章で後述する CAIENF アドレス空間で CA Datacom/AD MUF を実行する場合は、ENFIMUF セットアップを使用することをお勧めします。

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 LMP

CA Datacom/AD がインストールされているとき、CAAXSAMP の低レベル修飾子を備えたライブラリが作られます。そのデータ セットにはメンバ DBDATIN2 があります。これは CA Datacom MUF スタートアップで使用されます。

メンバ DBDATIN2 内の以下のステートメントを変更します。

```
DATACOM      AD
```

以下のように変更します。

```
DATACOM     MSM
```

この変更により、スタートアップ中に CA Datacom/AD MUF LMP 確認は回避されます。CA Datacom/AD 機能の一部は失われますが、CAIENF および Event Management には影響しません。CAIENF または Event Management によって使用されている CAAXSAMP データ セットが CA Datacom/AD を使用する他の製品と共有されている場合は、必ず先にこのデータ セットをコピーしてからステートメントを更新するようにしてください。そのような場合には、CAIENF または Event Management は、それ自身の更新された CAAXSAMP データ セットを使用するようにします。

CA Datacom/AD Multi-User の展開

CA Datacom/AD r14 が 1 つの LPAR 上に正常にインストールされ、その LPAR 上で ENF r14.1 が起動した後に、任意の数の LPAR イメージ上に本稼働可能な CA Datacom/AD 環境を確立できます。

CA MSM を使用して Datacom/AD r14 をインストールした場合、CA MSM を使用して Datacom/AD を展開できる可能性があります。その代わりに、このプロシージャに概要が示されている手順を実行し、IBM ADRDSSU ユーティリティを使用して、最初にインストールされた LPAR から必要なデータ セットをすべてバックアップし、それを別の LPAR にリストアできます。このプロシージャを使用して、ソース システム上に、ターゲット システムで機能するようにカスタマイズされた新規データ セットを作成します。これらの新規データ セットはバックアップされ、後でターゲット システムにリストアされると、ターゲット システム上で完全に機能するカスタマイズされた Datacom/AD r14 が利用可能になり、ENF をそのシステム上で開始できます。

このプロシージャには 9 つの手順があります。JCL メンバはほとんどの手順に関連付けられています。各 JCL メンバには、その機能の記述と、実行するためにサブミットする前に行う必要がある変更に関する特別な指示が含まれています。

定義:

- ソース LPAR とは、最初の CA Datacom/AD の新しいインストールが実行された LPAR です。
- ターゲット システムは、追加の CA Datacom/AD マルチユーザ環境が確立される LPAR です。

Datacom/AD r14 で、各 LPAR 上の各 MUF にはそれぞれ一意の MUF 名が必要です。LPAR システム名は、SYSPLEX 内で生成された CA Datacom/AD のメッセージとレポートの発生元をより簡単に特定できるようにするために、MUF 名で使用することができます。

この展開プロシージャの実行に必要な JCL は、CAW0JCL ライブラリのメンバ DEPLOY 内に置かれます。このジョブを実行すると、必要なメンバがすべて入っている新しい展開 JCL ライブラリが作成されます。

注: ソース システムに対して手順 1 から 6 を実行し、ターゲット システムに対して手順 8 から 9 を実行する必要があります。

重要: 展開 JCL ライブラリが作成されたら、メンバ AXDEPIPJ の中に IPOUPDTE プロセスが含まれます。このプロセスは、以下に説明する CA Datacom/AD 展開メンバに対して必要なすべての編集を実行するために使用できるプロセスで、必要なカスタマイズを行う際に実行されなければなりません。このメンバを別のライブラリにコピーし、次にそのメンバをカスタマイズし、そのライブラリからサブミットして、展開 JCL ライブラリの更新時に変更内容が失われないようにします。

ターゲット LPAR 上で完全に機能する CA Datacom/AD r14 Multi-User Facility (MUF)を設定する方法

1. CAW0JCL 内のメンバ DEPLOY を編集します。インストール条件を満たすように JOB カードを変更します。DSN を SRC.DATACOM.DEPLJCL から SRC.DATACOM 高レベル修飾子に一致する名前に変更して、IEBUPDTE 手順の SYSUT2 ステートメントを変更します。このプロセスのその他のジョブに重大な変更が行われないようにするために、低レベル修飾子は DEPLJCL にする必要があります。UNIT と VOL=SER を変更してインストール条件を満たしてから、ジョブをサブミットします。
2. 変更内容を保存するために、作成したばかりの展開 JCL ライブラリからメンバ AXDEPIPJ を別のライブラリにコピーします。SYSIN ステートメントの後の各パラメータを変更します(最後の $/</ を除く)。ジョブ コメントに記述されている値に一致するように、山形かっこ(<<)で囲まれた値を変更します。このジョブをサブミットします。

   この例では、SRC.SMPE.DATACOM の 2 番目のインスタンスを変更します。

   ```
   SRC.SMPE.DATACOM<SRC.SMPE.DATACOM<
   ```

   重要: 最後のエントリ $/</ は削除または更新しないでください。
3. ソース システム上でジョブ AXDEP01D をサブミットして、カスタム モジュールをアセンブルし、展開カスタム ライブラリにリンクエディットします。
4. ソース システム上でジョブ AXDEP01T をサブミットして、カスタム モジュールをアセンブルし、ターゲット カスタム ライブラリにリンクエディットします。
5. ソース システム上でジョブ AXDEP02 をサブミットして、MUF 展開可能データセットおよびデータベースをすべて割り当てます。

6. ソース システム上でジョブ AXDEP03 をサブミットして、CA Datacom/AD 製品データ セットをバックアップします。

   重要: このジョブの実行中は、ソース システムのマルチユーザ機能（MUF）は非アクティブである必要があります。

7. ジョブ AXDEP03 で作成されたバックアップ ファイル、および DEPLJCL ライブラリをターゲット システムで利用可能にします。

8. ターゲット システム上でジョブ AXDEP04 をサブミットして、必要な CA Datacom/AD データ セットをすべてターゲット LPAR へリストアします。

9. ターゲット システム上の以下のターゲット システム データ セットを APF 許可します。

   - CA Common Services CAW0LOAD
   - CA Datacom/AD CAAXLOAD
   - CA Datacom/AD CUSLIB

CA Datacom/AD の CAIENF 向けカスタマイズ

CA Datacom/AD をインストールしたり、別の LPAR イメージ上で CA Datacom/AD を展開したりした後で、必要であれば、CA Datacom/AD を CAIENF 向けにカスタマイズすることができます。

CAIENF によってイベントを記録する場合は、CA Common Services の本バージョンと同梱されていた CA Datacom/AD のバージョンをインストールしておいたうえで、このプロシージャの各ステップを実行する必要があります。

CA Datacom/AD のインストールが完了した時点で、2 つの CA Datacom/AD ロード ライブラリ、つまり CAAXLOAD と CUSLIB が作成されます。これらのロード ライブラリは、CAIENF 向けに CA Datacom/AD をカスタマイズする際に使用され、両方ともに APF の許可を与えておく必要があります。

CA Datacom/AD の MUF に関する考慮事項

重要: CAIENF 向けの CA Datacom/AD のカスタマイズ プロシージャを実行する場合は必ず、事前に以下の考慮事項を検討する必要があります。

- このプロシージャに関連付けられている JCL が実行されるシステムで、CA Datacom/AD マルチユーザ機能（MUF）を実行しておく必要があります。
- CA Datacom/AD MUF は、それ独自のアドレス空間か CAIENF のアドレス空間で実行することができます。

- CAIENF 向けに CA Datacom/AD をカスタマイズしたり、CA Datacom/AD の CAIENF 向けカスタマイズの問題を解決したりするためには、CA Datacom/AD MUF がそれ独自のアドレス空間で実行されている必要があります。また、CAIENF は、コントロール オプションの NODB によって、CA Datacom/AD とは別のアドレス空間でダウンしたり起動したりするようにしておく必要があります。
- CAIENF 内部 MUF（下記の「ENFIMUF」を参照）の使用を決めた場合でも、Datacom/AD MUF スタートアップ JCL を保存してください。CAIENF がダウンしている間に MUF の起動が必要となるデータベース メンテナンスが発生する場合があります。

既存 CA Datacom/AD の CAIENF 向けカスタマイズ

重要：この手順を開始する前に、「*CA Datacom/AD for CAIENF のカスタマイズ*」で「CA Datacom/AD MUF に関する考慮事項」を参照してください。

既存 CA Datacom/AD の CAIENF 向けカスタマイズ

このバージョンの CA Common Services for z/OS と共に出荷された CA Datacom/AD のリリースを、以前のバージョンの CAIENF からインストール済みの場合、CAIENF プランのこのリリース バージョンを既存の CA Datacom/AD 環境にインポートする必要があります。

重要：以下の手順を実行するのは、このリリースの CAIENF のバージョンを実装する準備ができてからにしてください。

1. CAIENF の古いバージョンをシャットダウンします。
2. まだ開始されなければ、CAIENF の外の DATACOM/AD を開始します。
3. CAW0JCL メンバ AW1IMPRT を編集およびサブミットして、New CAIENF プランを DATACOM/AD に IMPORT します。
4. システムを IPL します。
5. CAIENF の新リリースを開始します。

新規 CA Datacom/AD の CAIENF 向けカスタマイズ

新規 CA Datacom/AD の CAIENF 向けカスタマイズ方法

1. CAIENF データベース定義が CA Datacom/AD にインストールされ、CAIENF データベースのデータセットが割り当てられるように、メンバ AW1ID001 を変更してサブミットします。

   - CA Datacom/AD データセット プレフィックスを指定する
   - CAIENF データベース データセットのボリュームを指定する
   - 指定したボリュームの装置タイプを指定する
   - CAIENF データベース索引 IXX700 のスペースを指定する

     概算量 3390 CYL 索引スペース

     ```
     A = (30 x # 総記録済みイベント数) /3036
     B = A + (A x .05) / 12
     Cyls = (B  / 15) + 1
     ```

   - CAIENF データベースのデータ エリア ENF700 のスペースを指定する

     概算量 3390 CYL エリア スペース

     ```
     Cyls = # 総イベント数 / 3600
     概算量 3380 CYL エリア スペース
     Cyls = # 総イベント数 / 3000
     ```

   注: AW1ID001 が正常に完了しなかった場合は、「CA Datacom/AD の CAIENF 向けカスタマイズの問題を解決する」を参照してください。

   CA Common Services r11 からアップグレード中の場合、イベント カウントの総数を知るために、現在実行中の CA Common Services for z/OS CAIENF r11 を使用すれば便利です。CAS9DB LIST DETAIL レポートは、ARCHIVE (BACKUP) 時の直前、可能ならば週の最も忙しい 3 曜日が過ぎてから実行してください。LIST DETAIL レポートには、現在、CAIENF r11 データベースのイベント タイプごとに記録さるレコードの総数が記載されます。したがって、それらを単に合計するだけですみます。以下に CAS9DB LIST DETAIL JCL を示します。

   ```
   //CAS9DB   EXEC PGM=CAS9DB,REGION=4M
   //DBOUT DD SYSOUT=*
   //DBIN     DD *
     LIST DB(*) DETAIL
    /*
   ```

   CAIENF r11 が起動し稼動状態にあり、上記の JCL をそのまま使用することを確認します。

2. CAIENF プロシージャを更新します。

   CAW0PROC には、ENF、ENFXMUF、および ENFIMUF という 3 つの CAIENF プロシージャが組み込まれています。サイトの要件に合うプロシージャを選択します。

   ENF - イベントの記録や CA Datacom/AD のインストールを希望しない場合にこのプロシージャの JCL を使用します。

   ENFXMUF - イベントの記録が必要な場合にこのプロシージャの JCL を使用します。CA Datacom/AD はインストールされており、MUF は CAIENF 外部で（それ独自のアドレス空間で）実行されます。

   ENFIMUF - イベントの記録が必要な場合にこのプロシージャの JCL を使用します。CA Datacom/AD はインストールされており、MUF は CAIENF 内部で（CAIENF のアドレス空間で）実行されます。

   ENFXMUF と ENFIMUF の場合は、以下のように処理します。

   - ADSHLQ と ADHLQ のパラメータ値を CA Datacom/AD の CAAXLOAD と CUSLIB のデータセット名プレフィックスに設定します。
   - DD ENFPARMS によって参照される CAIENF 入力パラメータを更新して、コントロール オプション ステートメントの RECORD(YES) と EVENT(イベント名,RECORD) を指定します。記録される EVENT ごとに 1 つの EVENT コントロール オプション ステートメントを指定する必要があります。

     下記は、イベントの記録専用のコントロール オプションです。

     ```
     RECORD(NO|YES)
     EVENT(イベント名,RECORD)|
     EVENT(イベント名,NOREC)
     ```

   - CA Datacom/AD MUF が CAIENF のアドレス空間で実行される場合は、DD ENFPARMS によって参照される CAIENF 入力パラメータを更新して、コントロール オプション IMUF を指定します。

     注: これらのコントロール オプションの詳細については、「*Reference Guide*」と「*Administration Guide*」を参照してください。

3. CAIENF を起動または再起動します。

   CAIENF によって、イベントを記録するための EVENT テーブルと、その他補助的なデータを記録するための CAIENF システム テーブルが動的に作成されます。

   RECORD(YES) を指定して CAIENF を初期化した場合に EVENT テーブルが作成されます。

   RECORD(YES) が指定されていて DATACOM/AD MUF が利用できない場合、CAIENF はシャットダウンします。

CA Datacom/AD の CAIENF 向けカスタマイズの問題の解決

CA Datacom/AD を CAIENF 向けにカスタマイズしているときに問題が発生する場合があります。たとえば、データセット名やスペースの割り当てが誤って指定されたり、CAIENF データベースのインストール CAW0JCL メンバ AW1ID001 がエラーを受け取ったりすることがあります。

多くの場合、エラーが発生したジョブ ステップで開始するように JCL を編集してそのエラーの原因となった問題を解決した後に、CAIENF データベースのインストール CAW0JCL メンバ AW1ID001 を再度サブミットすることができます。

しかし、中には、一部または完全にインストールされた CAIENF データベースを削除する方が望ましい場合もあります。

一部または完全にインストールされた CAIENF データベースを削除する方法

1. このプロシージャを開始する前に、「CA Datacom/AD の CAIENF 向けカスタマイズ」の「CA Datacom/AD の MUF に関する考慮事項」を参照してください。
2. CAW0JCL メンバ AW1AD001 をサブミットして、既存の CAIENF データセット テーブルのリストを表示します。

   行が表示されていない場合は、手順 4 に進んで、CAIENF データベースを削除してください。

3. すべての CAIENF テーブルがドロップされるように CAW0JCL メンバ CASQL004 を編集して実行します。

   このステップは、ジョブ AW1AD001 のリスト表示で指示された行が表示された場合にのみ必要です。

   RECORD(YES) ENFPARM コントロール オプションが指定されている場合、EVENT テーブルは CAIENF のスタートアップ時に動的にインストールされます。

   重要: CAIENF がアクティブにイベントを記録している間は、絶対に EVENT テーブルをドロップしないでください。詳細については、「CA Datacom/AD の CAIENF 向けカスタマイズ」の「CA Datacom/AD の MUF に関する考慮事項」を参照してください。

   注: DROP TABLE ステートメントによって、テーブルは不要とされ、その結果、テーブルのすべてのバージョンとステータスがデータ ディクショナリ データベースから除去され、ディレクトリ定義が削除され、データが削除されます。

   CASQL004 によってエラーが返された場合は、CAW0JCL メンバ CADB001 を実行して、すべての CAIENF テーブルを閉じてから、再度 CASQL004 をサブミットしてください。

   注: データベースのテーブル情報が CA Datacom/AD アドレス空間にキャッシュされたままになっている場合はエラーが返されます。

4. CAIENF データベース定義が CA Datacom/AD から削除されるように CAW0JCL メンバ CADB003 を編集してサブミットします。

   - CUSLIB 向けに CA Datacom/AD をインストールしている間に使用したデータセットの高レベル修飾子を使って、ADHLQ の JCL SET ステートメントを更新します。
   - CAAXLOAD 向けに CA Datacom/AD をインストールしている間に使用したデータセットの高レベル修飾子を使って、ADSHLQ の JCL SET ステートメントを更新します。

   重要: すべての CAIENF テーブルをドロップしてから、CAIENF データベースを削除します。

   注: インストールされたのが CAIENF データベースの一部である場合は、1 つ以上のコンポーネントが存在しない可能性があり、CADB003 によって、コンポーネントが存在しないことを示すエラーが返されることがあります。このようなエラーは無視しても差し支えありません。

5. CAIENF の CA Datacom/AD ディレクトリ定義が削除されるように CAW0JCL メンバ CADB004 を編集してサブミットします。

   このジョブを実行する必要があるのは、CAW0JCL メンバ AW1ID001 内の CA Datacom/AD CAIENF データベースのデータセットを定義および初期化するためのステップによって、Datacom/AD CXX ファイルが CAIENF の ENF0700 および IX0700 データセットの情報と一緒に正常に初期化された場合のみです。

   - CUSLIB 向けに CA Datacom/AD をインストールしている間に使用したデータセットの高レベル修飾子を使って、ADHLQ の JCL SET ステートメントを更新します。
   - CAAXLOAD 向けに CA Datacom/AD をインストールしている間に使用したデータセットの高レベル修飾子を使って、ADSHLQ の JCL SET ステートメントを更新します。

6. CAIENF データベースのデータ セットを削除するために CAW0JCL メンバ CADB005 を編集してサブミットします。

   このジョブを実行する必要があるのは、CAW0JCL メンバ AW1ID001 内の CA Datacom/AD CAIENF データベースのデータセットを定義および初期化するためのステップによって、CAIENF ENF0700 および IXX0700 データセットが正常に割り当てられた場合のみです。

   - CUSLIB 向けに CA Datacom/AD をインストールしている間に使用したデータセットの高レベル修飾子を使って、ADHLQ の JCL SET ステートメントを更新します。

7. CAW0JCL メンバ AW1ID001 を使用して CAIENF データベースを再インストールします。

CA Datacom/AD の Event Management 向けカスタマイズ

Event Management の場合、必要に応じて以下のステップを実行してください。

Event Management でカレンダやメッセージ アクションを使用する場合は、CA Datacom/AD をインストールして以下のステップを実行する必要があります。

カレンダとメッセージ アクションは、通常、Event Management と統合されている CA OPS/MVS Event Management and Automation を使用しているサイトでは必要ありませんが、CA OPS/MVS Event Management and Automation を使用していないサイトにとっては、イベントを処理する際に便利になる場合があります。

CA Datacom/AD のインストールを完了したら、CAAXLOAD と CUSLIB という 2 つの CA Datacom/AD ロード ライブラリと、CUSMAC という 1 つのパラメータ ライブラリが使用できるようになります。これらのライブラリは、Event Management 向けの CA Datacom/AD セットアップを完了するために必要です。

Event Management のリリース 3.0 に DATACOM/TR リポジトリを使用していた場合は、テーブル情報をその古いリポジトリから抽出して、新しい DATACOM/AD リポジトリにロードすることができます。既存のテーブル情報を抽出してロードするためのオプションのステップについては、このプロシージャの後の方を参照してください。

Event Management 向けに CA Datacom/AD をカスタマイズする方法

1. MUF DATAPOOL パラメータを更新します。

   DATAPOOL バッファを変更することによって、MUF 用の CA Datacom/AD スタートアップおよびチューニング パラメータ メンバを変更します。

   MUF の実行方法に応じて CAIENF か CA Datacom/AD MUF のいずれかのスタートアップ プロシージャ JCL SYSIN DD ステートメントを参照して、スタートアップ パラメータとチューニング パラメータが指定されているデータセットとメンバー名を確認します。

   以下を変更

   ```
   DATAPOOL    8K,2000,16K,2        DATA BUFFER SIZE,# OF BUFFERS
   ```

   変更後は以下のようになります。

   ```
   DATAPOOL    12K,2000,16K,2       DATA BUFFER SIZE,# OF BUFFERS
   ```

2. CA Datacom/AD を起動または再起動します。

   注: 以下のステップを実行する前に、このすぐ前に行った変更内容を有効にして、CA Datacom/AD MUF をアクティブにする必要があります。

3. DB 定義を作成します。

   CNSMJCL メンバ D5IRTV01 を変更してサブミットします。

4. 定義を確認してデータベースを初期化します。

   CNSMJCL メンバ D5IRTV02 を変更してサブミットします。

5. SQL テーブルを定義します。

   CNSMJCL メンバ D5IRTV03 を変更してサブミットします。

   注: ステップ 3、4、および 5 の D5IRTV ジョブが正常に完了しなかった場合は、「CA Datacom/AD の Event Management 向けカスタマイズの問題を解決する (P. 318)」を参照してください。

6. (オプション) CA Common Services r11 以降の CA Datacom/TR を使用していて、その CA Datacom/TR データを CA Datacom/AD にマイグレートする必要がある場合は、このステップを実行してください。過去のリリースでは、Event Management によって、CA Datacom/TR データベースに収められているメッセージ アクションのレコードとカレンダが保守されていました。

   - EM 3.0 Datacom R9 をアクティブにし、CNSMJCL メンバ D5IDBUTL を使用して Event Management データベースの CA Datacom/AD ユーティリティレポートを作成します。
   - Datacom R9 ユーティリティレポートを使用して、JCL メンバ D5IDBEXT に示されている Event Management テーブル名の OCCURRENCE ごとに、3 文字からなる TABLE NAME を指定して CNSMJCL メンバ D5IDBEXT を更新します。

     例 - Datacom ユーティリティレポート

     ```
     TABLE NAME - C27
     OCCURRENCE - CADB-OPRA_CTL
     ```

     JCL メンバ D5IDBEXT を以下のように変更します。

```
EXTRACT AREA=EM0,DBID=1011,DDNAME=DDOCTL,TABLE=C27, CADB-OPRA-CTL BLKSIZE=10236
```

   - CA Datacom/AD へマイグレートするために Datacom/TR データを抽出します。

     CNSMJCL メンバ D5IDBEXT を変更してサブミットします。

   - 抽出した Datacom/TR データを CA Datacom/AD にロードします。

     抽出したデータが CA Datacom/AD にロードされるように CNSMJCL メンバ D5IDBLD を変更してサブミットします。

     CA Datacom/AD を、現在起動しているならば、再起動します。

7. Event Management プロファイルを確認します。

   Common Services のインストール手順で、CA Datacom/AD に関する（Event Management プロファイルの作成）エントリが作成されています。

   /cai/nsmem/PROFILE ファイルが CA_OPR_ZOSDB=Y を指定するように編集されていることを確認します。

   これによって、Event Management で Calendars および Message アクションが使用できるようになります。インストール時に CA Datacom/AD のデータセット名またはデータセットの高レベル修飾子がわからない場合は、この時点でこの情報を使用して、/cai/nsmem/PROFILE ファイルを直接編集することができます。このファイルの編集方法については、「インストール手順」を参照してください。

   /cai/nsmem/PROFILE 内の STEPLIB 環境変数は、適切な CA Datacom/AD ライブラリを指す必要があります。

   CA Datacom/TR からマイグレートしているか、新しい CA Datacom/AD データベースを作成している場合は、STEPLIB 変数が正しい CAAXLOAD データセットと CUSLIB データセットを指していることを確認します。

   /cai/nsmem/PROFILE ファイルの更新が完了したら、CNSMJCL メンバ D5II0065 を再実行します。これによって、CA Datacom/AD データベースを使用するために必要なすべての情報が、適切な Event Management コンポーネントのスクリプトにおいて更新されます。

   ユーザがログオンした時点で EM 環境変数が設定されるようにシステムの /etc/profile ファイルを任意で更新した場合は、CA Datacom/AD ライブラリが STEPLIB 変数の中に反映されるように、スクリプト fwsetup を再実行する必要があります。詳細については、本書の「Event Management のインストール後のスクリプトの実行 (P. 196)」を参照してください。

8. MUF を起動します。

   CA Datacom/AD MUF は、それ独自のアドレス空間か CAIENF のアドレス空間で実行することができます。

   カレンダやメッセージ アクションを使用している場合は、Event Management コンポーネントを起動する前に、MUF を初期化する必要があります。MUF を初期化しなかった場合は、スタートアップのエラー メッセージが表示されると考えてください。MUF が実行されていない場合、caiopr デーモンは起動しますが、カレンダ デーモンは起動しません。

9. Event Management デーモンを起動します。

   新しいデータベースにアクセスするには、CNSMPROC メンバ NSMEMSTR を使用して Event Management デーモンを起動します。

CA Datacom/AD データベースの複製

CA Datacom/AD データベースを別のシステム上に複製する方法

1. 複製する Event Management CA Datacom/AD データベースを CNSMJCL メンバ D5IDBBAK を使用してバックアップします。

   注: CA Datacom/AD の Event Management 向けカスタマイズが完了した後ならばいつでもこのジョブを実行して、初期化の後に追加されたデータベース レコードをバックアップすることができます。

2. Event Management 向けに CA Datacom/AD をカスタマイズするためのプロシージャを実行して、ターゲット システム上に CA Datacom/AD 環境をセットアップします。

3. CNSMJCL メンバ D5IDBRST を使用して、ステップ 1 で作成したバックアップ ファイルを新しい Event Management CA Datacom/AD データベース内に復元します。

複数のシステム上の中央データベース

複数のシステムで中央データベースを使用するには、リモート システムごとに、環境変数 CAI_OPR_REMOTEDB=ccisysid をエクスポートする必要があります。リモート システムごとに、このエクスポート ステートメントを /cai/nsmem/PROFILE ファイルに追加します。

これによって、イベント管理コードでは、メッセージ レコード クエリを ccisysid ノード上のデータベース エンジンに送信し、そのノードからの応答を受信できるようになります。関係している複数のシステムの中には、CA NSM 3.0 を実行している分散システムもあります。たとえば、z/OS を実行中のイベント管理では、分散型の Microsoft SQL サーバ データベースをそのメッセージ レコード リポジトリとして使用することができます。

CA Datacom/AD の Event Management 向けカスタマイズの問題の解決

CA Datacom/AD を Event Management 向けにカスタマイズしているときに問題が発生することがあります。たとえば、データセット名やスペースの割り当てが誤って指定されたり、データベースのインストール CNSMJCL メンバ D5IRTV0* がエラーを受け取ったりすることがあります。

多くの場合、エラーを解決した後、エラーが発生したジョブ ステップで開始するように JCL を編集してから、そのエラーの原因となったデータベースのインストール CNSMJCL メンバ D5IRTV0* を再度サブミットすることができます。

中には、一部または完全にインストールされた Event Management データベースの削除が必要な場合があります。

重要: このプロシージャを開始する前に、「CA Datacom/AD の CAIENF 向けカスタマイズ (P. 307)」の「CA Datacom/AD の MUF に関する考慮事項」を参照してください。

一部または完全にインストールされた Event Management データベースを削除するには、以下の CNSMJCL メンバをその順番で変更してサブミットします。

- D5IDBU02
- D5IDBU04
- D5IDBU05
- D5IDBU06
- D5IDBU07

付録 A: サード パーティ ソフトウェアの使用条件

このセクションには、以下のトピックが含まれています。

Apache Software Foundation

This product includes software developed by the Apache Software Foundation, including Tomcat 6.0.29, CGLIB-NODEP 2.1.3, Commons Codec 1.3, Commons Collections 3.2.1, Commons Configuration 1.6, Commons DBCP 1.2.2, Commons HTTPClient 3.1, Commons IO 1.4, Commons Language 2.4, Commons Logging 1.1.1, Commons Net 2.0, Commons Pool 1.3, Log4j 1.2.15, Xalan-J 2.1.7, XML Resolver, Google (including Google Web Toolkit 1.7.1 and GWT-Log 2.6.2), and the Spring Framework Project (http://www.springframework.org). The Apache software is distributed in accordance with the following license agreement:

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of

this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify,

```
   defend, and hold each Contributor harmless for any liability
   incurred by, or claims asserted against, such Contributor by reason
   of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

   To apply the Apache License to your work, attach the following
   boilerplate notice, with the fields enclosed by brackets "[]"
   replaced with your own identifying information. (Don't include
   the brackets!)  The text should be enclosed in the appropriate
   comment syntax for the file format. We also recommend that a
   file or class name and description of purpose be included on the
   same "printed page" as the copyright notice for easier
   identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
```

索引

1

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

か

さ

た

な

は

ま

や

ら