



IBM Systems - iSeries

システム管理

Common Information Model (CIM)

バージョン 5 リリース 4





IBM Systems - iSeries

システム管理

Common Information Model (CIM)

バージョン 5 リリース 4

ご注意

本書および本書で紹介する製品をご使用になる前に、49 ページの『特記事項』に記載されている情報をお読みください。

本書は、IBM i5/OS (プロダクト番号 5722-SS1) バージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りが無い限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

<http://www.ibm.com/jp/manuals/main/mail.html>

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

<http://www.ibm.com/jp/manuals/> の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原 典： IBM Systems - iSeries
Systems management
Common Information Model
Version 5 Release 4

発 行： 日本アイ・ビー・エム株式会社

担 当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財)日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、
平成角ゴシック体™W5、平成角ゴシック体™W7

© Copyright International Business Machines Corporation 2004, 2006. All rights reserved.

© Copyright IBM Japan 2006

目次

Common Information Model	1	CIM サーバーのトラブルシューティング	21
V5R4 の新機能	2	CIM サーバーが始動しない	21
トピックの印刷	3	CIM サーバーが予想と異なる振る舞いをする	22
Pegasus の構成	3	Pegasus のコマンド行ユーティリティ	23
i5/OS に、必須のオプションがインストールされて		cimmoftl の使用について	24
いることを確認する	3	cimconfig の使用について	26
必要な構成パラメーターを設定する	4	cimprovider の使用について	28
Pegasus を扱うために必要な権限をユーザーに付		ssltrustmgr の使用について	30
与する	13	Pegasus 開発者の手引き	33
CIMOM ジョブを開始する	13	サポートされる CIM 基本オペレーティング・シ	
Pegasus の保護	13	ステム・クラス	33
SSL 鍵および Pegasus 用証明書の作成	14	i5/OS メトリック	43
クライアントの証明書を検査する CIM サーバー		CIM 指示プロバイダーに対する i5/OS サポート	46
の構成	16	CIM の関連情報	47
認証	17		
Kerberos を使用可能にする	17	付録. 特記事項	49
Pegasus の許可	18	プログラミング・インターフェース情報	50
バックアップおよび回復の考慮事項	19	商標	51
破壊されたファイルの復元	20	資料に関するご使用条件	51

Common Information Model

Common Information Model (CIM) は、Distributed Management Task Force (DMTF) という、IBM®をはじめとする主要なハードウェアおよびソフトウェア・ベンダーのコンソーシアムが、Web Based Enterprise Management (WBEM) イニシアチブの一環として開発した標準です。

WBEM には、分散ネットワーク環境の管理ソリューションを提供するさまざまな標準やテクノロジーが含まれています。WBEM の主な焦点は相互運用性です。WBEM テクノロジーを使用すると、さまざまなリソースに使用できる単一系列の管理アプリケーション群を開発することができます。

CIM は WBEM イニシアチブの主要コンポーネントで、企業全体のデータを記述し、これにアクセスするためのモデルを提供します。CIM は仕様とスキーマの両方から構成されています。仕様では、他の管理モデルとの統合の詳細が定義され、スキーマでは実際のモデル記述が提供されます。

IBM i5/OS™ V5R4 版の CIM には以下のものが組み込まれています。

- システム呼び出し先プロバイダーの、サーバー・リソース用の媒介機能。標準化 CIM クラスのサブセットに基づくプロバイダーが、システム上のデータを収集します。CIM クライアントは、Common Information Model Object Manager (CIMOM) を介してプロバイダーにアクセスし、このデータを操作することができます。
- クライアントとプロバイダー間の通信を管理する Pegasus (バージョン 2.5) という CIMOM のオープン・ソース・インプリメンテーション。CIMOM は、セキュリティーを含む管理機能、および、管理者が構成と管理の機能を使用できるようにする一連のコマンドも提供します。
- システム管理機能を表すための情報モデルを定義するスキーマ (CIM スキーマ、バージョン 2.9)。
- クライアントと CIMOM 間の通信のための標準化フォーマットのインプリメンテーション (CIM in XML V2.1 および CIM Operations over HTTP V1.1)。これらの標準について詳しくは、WBEM Web サイトを参照してください。

CIM 標準について詳しくは、DMTF Web サイトの「Introduction to CIM」および「CIM Specification 2.2」を参照してください。

IBM のそれぞれのオペレーティング・システムは、Pegasus (バージョン 2.5) をサポートしています。Pegasus は、DMTF により CIM Operations over HTTP 仕様で定義されている CIM 操作の大半をサポートしています。i5/OS でのサポートについて詳しくは、後述の『開発者の手引き』を参照してください。

Pegasus は、IBM のそれぞれのオペレーティング・システムでサポートされるオープン・ソースの CIM インプリメンテーションです。他の IBM オペレーティング・システムにおける Pegasus サポートについては、IBM Systems Software Information Center の CIM の項を参照してください。オープン・ソースの Pegasus プロジェクトについて詳しくは、Pegasus の Web サイトを参照してください。

i5/OS V5R3 以降が実行されているシステムでの Pegasus のサポートにより、ユーザーは拡張可能な業界標準のモデルを通して iSeries™ サーバーのリソースにアクセスできるようになりました。

関連情報

WBEM Web サイト

Introduction to CIM

CIM 仕様 2.2 (CIM Specification 2.2)

V5R4 の新機能

このトピックでは、V5R4 でこのトピック・コレクションに加えられた変更を中心に説明します。

V5R4 では、i5/OS は Pegasus バージョン 2.5 をサポートしています。Pegasus バージョン 2.5 をサポートすることで、i5/OS はセキュリティーが強化され、構成が強化されて、CIM 基本オペレーティング・システム・クラスが追加されました。

構成の強化

cimconfig コマンドには、新規の基本開始オプションおよび拡張開始オプションがあります。また、cimmofl コマンドおよび cimprovider コマンドも、新しいオプションによって拡張されました。

- 5 ページの『cimconfig コマンドの基礎開始オプション』
- 6 ページの『cimconfig コマンドの拡張開始オプション』
- 26 ページの『cimconfig の使用について』
- 24 ページの『cimmofl の使用について』
- 28 ページの『cimprovider の使用について』

セキュリティーの強化

Pegasus バージョン 2.5 では、Secure Sockets Layer (SSL) のサポートを提供することで、CIM のセキュリティーを強化しました。

- 14 ページの『SSL 鍵および Pegasus 用証明書の作成』
- 16 ページの『クライアントの証明書を検査する CIM サーバーの構成』
- 30 ページの『ssltrustmgr の使用について』

CIM 基本オペレーティング・システムおよび i5/OS メトリックの強化

13 個の新しい CIM 基本オペレーティング・システム・クラスがサポートされるようになりました。その他の強化には、新しい i5/OS メトリックや、CIM 指示のサポートなどがあります。

- 33 ページの『サポートされる CIM 基本オペレーティング・システム・クラス』
- 43 ページの『i5/OS メトリック』
- 46 ページの『CIM 指示プロバイダーに対する i5/OS サポート』

情報の強化

V5R4 では、新しいトラブルシューティング情報、および、バックアップとリカバリーの情報が追加されました。

- 19 ページの『バックアップおよび回復の考慮事項』
- 20 ページの『破壊されたファイルの復元』
- 21 ページの『CIM サーバーのトラブルシューティング』

新着情報または変更情報の表示方法

テクニカルな変更が加えられた箇所がわかるようにするために、この情報では以下を使用します。

-  イメージは、新規または変更された情報の開始点を示すマークです。

-  イメージは、新規または変更された情報の終了点を示すマークです。

このリリースの新着情報または変更情報に関するその他の情報を検索するには、『プログラム資料説明書』を参照してください。

トピックの印刷

この情報の PDF を表示および印刷するために使用してください。

PDF 版をダウンロードし、表示するには、「Common Information Model (CIM)」を選択します。

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右クリックする (上記のリンクを右クリックする)。
2. PDF をローカルで保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「保存」をクリックする。

Adobe Reader のダウンロード

- PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。
- これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html)  から無料でダウンロードすることができます。

Pegasus の構成

Pegasus CIMOM には、数多くの構成オプションを設定する機能があります。

CIMOM を構成する場合、管理者は次のことを行う必要があります。

- IBM i5/OS システムに、必要なインストール・オプションがあることを確認する
- 必要な構成パラメーター (特にセキュリティー) を設定する
- Pegasus を扱うために必要な権限をユーザーに付与する
- CIMOM ジョブを開始する

関連概念

23 ページの『Pegasus のコマンド行ユーティリティー』

オープン・ソースの Pegasus インプリメンテーションには、Pegasus 環境の制御や変更に使用できるコマンド行ユーティリティーのセットが含まれています。

26 ページの『cimconfig の使用について』

cimconfig コマンドを使用して CIMOM の開始オプションを構成します。

i5/OS に、必須のオプションがインストールされていることを確認する

CIM には、i5/OS の特定のインストール・オプションが必要です。

必要なオプションは以下のとおりです。

- 拡張基本ディレクトリー・サポート (5722-SS1 オプション 3)
- ユニコードの国際対応コンポーネント (5722-SS1 オプション 39)

- Qshell インタープリター (5722-SS1 オプション 30)

重要: Secure Sockets Layer (SSL) を使用するようにサーバーが構成されている場合は、OpenSSL (5733-SC1 オプション 1) をインストールする必要があります。さらに、OpenSSL を使用するには、システムにポータブル・アプリケーション・ソリューション環境 (PASE) (5722-SS1 オプション 33) がインストールされている必要があります。

必要な構成パラメーターを設定する

CIM サーバーを始動する前に、**cimconfig** コマンドを使用していくつかの構成プロパティーを設定しておく必要があります。

特に、クライアント認証の指定方法を決定する必要があります。以下の方法のいずれかを使用することができます。

- Secure Sockets Layer (SSL) 証明書ベースの認証を使用する
- Basic 認証または Kerberos 認証を使用する
- クライアントとサーバー間の CIM データの暗号化には SSL を使用し、認証には Basic または Kerberos を使用する

Pegasus 2.5 は以下の接続で SSL をサポートしています。

- CIM クライアント接続用の SSL 保護ポートを介した外部接続
- CIM エクスポート・クライアントとの接続

SSL を使用するには、HTTPS 接続の使用可能化 (`enableHttpsConnection`) プロパティーを、`true` (デフォルトの設定値) に設定する必要があります。このプロパティーは、HTTPS TCP/IP 通信の使用を許可するものです。HTTPS 接続のセキュリティは HTTP 接続のセキュリティより優れています。SSL は単独で使用するか、Basic 認証または Kerberos 認証と併せて使用することができます。

HTTP 認証 (`httpAuthType`) プロパティーを設定して、使用する認証のタイプを指定します。このプロパティーの有効な値は Basic と Kerberos の 2 つです。Basic 認証はパスワードを保護しないため、常に SSL と併せて使用することをお勧めします。

要確認: ほとんどの CIM クライアントは、Kerberos 認証ではなく Basic 認証をサポートしています。CIM サーバーを構成する前に、ご使用の環境の CIM クライアントがどちらの認証タイプをサポートしているのかを確認してください。

cimconfig コマンドを使用して、CIM サーバーの現行の構成プロパティーまたは計画の構成プロパティーを設定することができます。現行の構成プロパティーの中で、以下のプロパティーは変更可能です。

- `shutdownTimeout`
- `logLevel`
- `traceComponents`
- `traceFilePath`
- `traceLevel`

これらのプロパティーは動的です。つまり、これらのプロパティーを変更すると、その変更内容が直ちに反映されます。変更を有効にするために CIM サーバーを再始動する必要はありません。現行の構成プロパティーを更新できるのは、CIM サーバーが実行されている場合のみです。

| 計画された構成プロパティーの場合は、CIM サーバーの実行、停止にかかわらず、すべてのプロパティー
| を変更することができます。計画された構成プロパティーが変更された場合、それらの変更は CIM サーバ
| ーを再始動するまで有効になりません。 CIM サーバーが始動すると、計画されたの構成プロパティーが現
| 行の構成プロパティーになります。

cimconfig コマンドの基礎開始オプション

cimconfig コマンドを使用して CIMOM の基礎開始オプションを変更することができます。

| 以下のリストで、**cimconfig** コマンドの開始オプションおよびデフォルト値について説明します。どの基礎
| 開始オプションも動的ではありません。

enableHttpConnection

| HTTP TCP/IP 通信を使用した、httpPort からのユーザー・アクセスを許可します。デフォルトは
| false です。これは、CIM サーバーが httpPort での listen を行わないことを意味します。ご使用の
| 環境が確実に保護されている場合は、このプロパティーを true に設定します。

| このプロパティーを false に設定する場合は、enableHttpsConnection を true に設定して HTTPS 接
| 続を許可する必要があります。

デフォルト値

false

enableHttpsConnection

| HTTPS TCP/IP 通信を使用した、httpsPort からのユーザー・アクセスを許可します。HTTPS 接続
| のセキュリティーは HTTP 接続のセキュリティーより優れているため、デフォルトは true です。

デフォルト値

true

httpPort

| HTTP 要求を listen するポート。これを設定する場合は、有効なポート番号に設定する必要があります
| ます。このポート番号は、TCP/IP サービス・テーブルの wbem-http サービスのポート番号をオー
| ーライドします。設定しない場合は、wbem-http サービスのポートが使用されます。このプロパ
| ティーも wbem-http サービス・ポートも設定されていない場合は、ハードコーディングされたデフ
| オルトの 5988 が使用されます。

| このプロパティーは、enableHttpConnection が true に設定されている場合にのみ反映されます。

デフォルト値

5988

httpsPort

| HTTPS 要求を listen するポート。これを設定する場合は、有効なポート番号に設定する必要があ
| ります。このポート番号は、TCP/IP サービス・テーブルの wbem-https サービスのポート番号をオ
| ーライドします。設定しない場合は、wbem-https サービスのポートが使用されます。このプロ
| パティーも wbem-https サービス・ポートも設定されていない場合は、ハードコーディングされた
| デフォルトの 5989 が使用されます。

| このプロパティーは、enableHttpsConnection が true に設定されている場合にのみ反映されます。

デフォルト値

5989

httpAuthType

| HTTP 認証のタイプ (Basic または Kerberos)。

注: 以下の条件のどちらかまたは両方を満たしていない限り、Basic 認証は使用しないでください。

- HTTPS を使用している。
- 平文パスワードの引き渡しがないような、高度に保護された環境を使用している。

このプロパティは、HTTP ポートおよび HTTPS ポートで認証を行うかどうかを決定します (sslClientVerificationMode プロパティも参照してください)。このプロパティは、wbem-exp-https ポートにおける認証は決定しません (enableSslExportClientVerification プロパティも参照してください)。

デフォルト値

Basic

注: httpAuthType の値を Basic に設定すると、ユーザーのパスワードは平文で送信されます。このオプションを認識されない値に設定すると、httpAuthType は自動的にデフォルトの Kerberos に設定されます。

kerberosServiceName

httpAuthType を Kerberos に設定すると、CIMOM サービス用の Kerberos のサービス名が、鍵配布センター (KDC) で構成された CIMOM サービス名と一致するように設定されます。

デフォルト値

cimom

cimconfig コマンドの拡張開始オプション

cimconfig コマンドを使用して、CIM サーバーの拡張開始オプションを変更することができます。

以下のリストに、cimconfig コマンドの拡張開始オプション、そのデフォルト値、および動的に変更可能かどうかを記述します。

注: shutdownTimeout、logLevel、traceLevel、traceComponents、および traceFilePath 設定は、動的に変更可能です。その他は不可です。他のプロパティの場合はすべて、変更を示すために **-p** パラメーターを使用する必要があります。その後、CIM サーバーを停止および再始動して、変更内容を有効にする必要があります。

重要: これらのオプションの使用は、上級者向けです。

messageDir

メッセージ・バンドルを検索するためのデフォルトのディレクトリです。デフォルト値は、配送済みのメッセージ・バンドルを示しています。

デフォルト値

/QIBM/ProdData/OS400/CIM/msg

動的 いいえ

logLevel

ログに記録されたデータのレベルを設定します。TRACE、INFORMATION、SEVERE、FATAL に設定します。ログ・データは、QYCMCIMOM ジョブ・ログに保管されます。

デフォルト値

INFORMATION

動的 はい

enableNormalization

true に設定する場合は、プロバイダーから配信されたオブジェクトが完全かつ正確であることを確認します。デフォルトは false です。信頼できるエンティティーからのオブジェクトを正規化しないでください。リポジトリ、制御プロバイダー、IBM が配送したプロバイダー、および信頼できる有効なオブジェクトを作成することが分かっている特定のベンダー・プロバイダーからのオブジェクトは、正規化しないでください。配布に追加されたサード・パーティーのプロバイダーからのオブジェクトのみ、正規化する必要があります。値は true または false です。

デフォルト値

false

動的 いいえ

excludeModulesFromNormalization

特定のプロバイダー・モジュールからのオブジェクトの正規化を使用不可にします。enableNormalization が true に設定されている場合、この除外リストに記載されているもの以外のすべてのプロバイダー・オブジェクトが正規化されます。

デフォルト値

“”

動的 いいえ

repositoryIsDefaultInstanceProvider

デフォルトで CIM オブジェクトを提供するために、CIM サーバーのリポジトリ・コンポーネントを使用可能にします。デフォルトとは、CIM インスタンスのクライアント要求のサービスを行うプロバイダーがない場合に、CIM サーバー・リポジトリが使用されることを意味します。これには、インスタンスの作成と検索の両方が含まれます。repositoryIsDefaultInstanceProvider オプションの値を false に変更すると、CIM メトリック・クラスをインプリメントする i5/OS プロバイダーが正しく機能しなくなります。値は true または false です。

デフォルト値

true

動的 いいえ

enableAuthentication

true に設定すると、CIM サーバーによる任意の要求の処理を許可する前に、認証が行われます。デフォルトは true です。このプロパティを false に設定すると、CIM サーバーへの非認証アクセスが許可されます。

ご使用の環境が確実に保護されており、極めて妥当な理由がある場合にのみ、enableAuthentication を false に設定してください。

値は true または false です。

デフォルト値

true

動的 いいえ

sslCertificateFilePath

CIM サーバーの証明書ファイルのパスです。

enableHttpsConnection または enableSslExportClientVerification が true に設定されている場合、このプロパティに有効な証明書を設定する必要があります。CIM サーバーによるロード時には、有効期限が切れた証明書も有効とみなされますので注意してください。

sslKeyFilePath が指定されていない場合、CIM サーバーは証明書ファイルから秘密鍵をロードしようとします。

デフォルト値

ssl/keystore/servercert.pem

動的 いいえ

sslKeyFilePath

CIM サーバーの秘密鍵ファイルのパスです。 sslCertificateKeyPath で指定した証明書に秘密鍵が含まれている場合は、このプロパティを設定する必要はありません。

このファイルはパスフレーズ (パスワード) によって保護されないため、保護されているディレクトリに保持する必要があります。デフォルト値で指定される値は、保護されているディレクトリです。

デフォルト値

ssl/keystore/serverkey.pem

動的 いいえ

sslTrustStore

CIM 操作要求用の信頼できる証明書が入っている、ディレクトリまたはファイルのパスです。トラストストアには、CA 証明書を組み込むことができます。

sslClientVerificationMode を required に設定する場合は、このプロパティを設定する必要があります。

sslClientVerificationMode を optional に設定する場合は、このプロパティを空に設定することができます。その場合は、どの証明書も信頼されません。

このプロパティを空のディレクトリまたは空のファイルに設定すると、どの証明書も信頼されません。

sslClientVerificationMode を disabled に設定すると、このプロパティは使用されません。

デフォルト値

ssl/truststore/

動的 いいえ

exportSSLTrustStore

CIM エクスポート要求用の信頼できる証明書が入っている、ディレクトリまたはファイルのパスです。トラストストアには、CA 証明書を組み込むことができます。

enableSSLExportClientVerificationMode を true に設定する場合は、このプロパティを設定する必要があります。

このプロパティを空のディレクトリまたは空のファイルに設定すると、どのエクスポート証明書も信頼されません。

このプロパティは、enableSSLExportClientVerification が true に設定されている場合のみ有効です。

デフォルト値

ssl/exporttruststore/

動的 いいえ

crlStore

証明書取り消しリスト (CRL) が入っている、ディレクトリーまたはファイルのパスです。

このプロパティを設定しないか、空のディレクトリーまたは空のファイルに設定すると、どの CRL もロードされません。

このプロパティは、`sslClientVerificationMode` が `required` または `optional` に設定されているか、`enableSslExportClientVerification` が `true` に設定されている場合のみ有効です。

デフォルト値

`ssl/crlstore/`

動的 いいえ

sslClientVerificationMode

SSL クライアント証明書検査のモードを設定します。

`required`、`optional`、または `disabled` に設定します。

`required` に設定すると、CIM サーバーは常に HTTPS ポート上のクライアント証明書の検査を要求し、クライアント証明書が信頼されていない場合は要求をリジェクトします。`httpAuthType` プロパティは使用されません。

`optional` は、CIM サーバーがクライアント証明書が使用可能であればそれを使用して検査し、それ以外の場合には、`httpAuthType` 設定を使用してクライアント検査を行うことを意味します。

`disabled` は、CIM サーバーが常に `httpAuthType` 設定を使用してクライアント検査を行うことを意味します。

このプロパティは、`enableHttpsConnection` が `true` に設定されている場合にのみ有効です。

デフォルト値

`optional`

動的 いいえ

sslTrustStoreUserName

証明書認証の使用時に CIM 操作要求用のユーザー・コンテキストとなるユーザー名を識別します。ユーザー名を特定の証明書ファイルと関連付けることはできません。ユーザー・コンテキストは i5/OS ユーザー・プロファイルです。これを使用してプロバイダーが呼び出され、CIM 要求が実行されます。このプロパティは、i5/OS 上の正当なユーザー・プロファイルに設定する必要があります。

`sslClientVerificationMode` を `disabled` に設定すると、このプロパティは無効になります。

`sslTrustStore` を `directory` に設定すると、このプロパティは無効になります。ディレクトリー内の証明書ファイルに関連付けられたユーザー名は、CIM 操作要求のユーザー・コンテキストです。`sslTrustStore` のデフォルトの設定値は、`directory` です。

`sslTrustStore` を単一のファイルに設定する場合は、このプロパティをユーザー名に設定する必要があります。そうしないと、CIM サーバーにエラーが生じ、サーバーは起動しません。この場合、そのファイル内のすべての証明書が、`sslTrustStoreUserName` で指定されたユーザー名に割り当てられます。このユーザー名が、CIM 操作要求のユーザー・コンテキストになります。

デフォルト値

`""`

動的 いいえ

| **enableSubscriptionsForNonprivilegedUsers**

| true または false に設定します。デフォルトは false です。false は、*IOSYSCFG 権限および *ALLOBJ 権限を持つユーザーのみが、指示サブスクリプションの作成を許可されることを意味します。

| **デフォルト値**

| false

| **動的** いいえ

| **enableSSEExportClientVerification**

| true または false に設定します。true の場合、サービス名 wbem-exp-https によって指定されたポート上の HTTPS を使用してエクスポート・クライアントが接続することを許可します。このポートでは、CIM エクスポート要求のみ許可されます。

| **注:** システムの TCP/IP サービス・テーブルで wbem-exp-https ポートが定義されていない場合、CIM サーバーにエラーが生じ、サーバーは起動しません。wbem-exp-https は IANA 標準サービスであるため、デフォルトでは i5/OS サービス・テーブルに入っています。

| false の場合、wbem-exp-https ポート上で要求は許可されません。

| **デフォルト値**

| true

| **動的** いいえ

| **shutdownTimeout**

| 秒数を設定します。ENDTCPSVR *CIMOM コマンドが発行される場合、タイムアウトは、CIM サーバーがシャットダウンするまでに未処理の CIM 操作要求の完了に費やすことができる最大の秒数です。指定されたタイムアウト期間が満了すると、CIM サーバーは、進行中の CIM 操作が残っている場合でもシャットダウンします。最小値は 2 秒です。デフォルト値は 10 秒です。

| **デフォルト値**

| 10

| **動的** はい

| **traceLevel**

| デバッグ・トレースのレベルです。範囲は 1 から 4 までです。traceLevel 1 は、最小のトレースである機能終了のトレースのみを行います。トレース・レベル 4 が最大のトレースです。

| **デフォルト値**

| 1

| **動的** はい

| **traceFilePath**

| トレース・ファイルのパスです。

| **デフォルト値**

| /qibm/userdata/os400/cim/cimserver.trc

| **動的** はい

| **traceComponents**

| トレースする Pegasus コンポーネント。有効な設定は、11 ページの『traceComponents オプションの設定』にリストします。

| デフォルト値
| 空
| 動的 はい

| **enableAssociationTraversal**

| true または false に設定します。デフォルトは true です。 true は、アソシエーション・トラバーサルが使用可能であることを意味します。 false は、アソシエーション・トラバーサルを使用不可にします。

| デフォルト値
| true
| 動的 いいえ

| **enableIndicationService**

| true または false に設定します。デフォルトは true です。 true は、指示サービスが使用可能であることを意味します。 false は、指示サービスを使用不可にします。

| デフォルト値
| true
| 動的 いいえ

| **tempLocalAuthDir**

| Pegasus サーバーがローカル認証中に使用する一時ファイルを書き込むディレクトリーです。

| デフォルト値
| /tmp
| 動的 いいえ

| **関連概念**

| 30 ページの『ssltrustmgr の使用について』
| このコマンドは、トラストストアまたは証明書取り消しリスト (CRL) で X.509 証明書を管理するためのコマンド行インターフェースを提供します。

| **関連タスク**

| 14 ページの『SSL 鍵および Pegasus 用証明書の作成』
| Pegasus を Secure Sockets Layer (SSL) モードで実行する場合には、秘密鍵および証明書が必要です。 Pegasus は、始動時にその秘密鍵および証明書を確認します。 それらのファイルが存在していない場合、Pegasus は秘密鍵および自己署名した 365 日間有効の証明書を作成します。また、以下の情報を使用して秘密鍵および証明書を作成することも可能です。

traceComponents オプションの設定

traceComponents オプションでは以下の設定が有効です。

- ALL
- AsyncOpNode
- Authentication
- Authorization
- BinaryMessageHandler
- Channel
- CimData
- CIMExportRequestDispatcher

- CIMOMHandle
- Config
- ConfigurationManager
- ControlProvider
- CQL
- DiscardedData
- Dispatcher
- ExportClient
- Http
- IndDelivery
- IndicationHandlerService
- IndicationService
- IndicationServiceInternal
- IndHandler
- IPC
- L10N
- Listener
- Memory
- MessageQueueService
- MetaDispatcher
- ObjectResolution
- OsAbstraction
- ProviderAgent
- ProviderManager
- ProvManager
- Registration
- Repository
- Server
- Shutdown
- SSL
- SubscriptionService
- Thread
- UserManager
- WQL
- XmlIO
- XmlParser
- XmlReader
- XmlWriter

Pegasus を扱うために必要な権限をユーザーに付与する

ユーザー許可を必要とする CIM 操作のタイプは 2 つあります。

ローカルの CIM スキーマを変更する操作がアプリケーション管理で制御されるのに対し、i5/OS システム・オブジェクトを変更する操作は i5/OS のオブジェクト権限を使用して制御されます。

関連タスク

『Pegasus の保護』

このトピックは、CIM サーバーの機密性を確保するために利用できるオプションを見つけるために使用してください。

CIMOM ジョブを開始する

iSeries サーバーの Pegasus は i5/OS V5R3 以降に組み込まれています。これには、i5/OS 用のサポートされるプロバイダー・セット、CIM スキーマ、および Pegasus CIMOM が含まれます。

すべての Pegasus 機能は、単一の TCP/IP サーバー・ジョブ QYCMCIMOM 下で実行されます。QYCMCIMOM は、QSYSWRK サブシステムで実行されますが、デフォルトでは開始されません。CIMOM ジョブを開始するには、以下のステップを実行します。

1. 「ネットワーク」 → 「サーバー」 → 「TCP/IP」と選択して、iSeries ナビゲーターで CIMOM ジョブを扱うようにする。
2. 「CIMOM」を選択する。このウィンドウでは、CIMOM の開始または停止、および CIMOM がデフォルトで TCP/IP から開始するかどうかを指定することができます。

注: また、CIMOM ジョブは、コマンド行インターフェースからコマンド STRTCPSVR *CIMOM を使用して開始することもできます。

CIMOM ジョブの停止には、コマンド ENDTCPSPVR *CIMOM を使用することができます。

Pegasus の保護

このトピックは、CIM サーバーの機密性を確保するために利用できるオプションを見つけるために使用してください。

Pegasus の管理者にとって最も重大な関心事の 1 つが、セキュリティーを構成する方法です。これは、i5/OS プラットフォームのセキュリティー要件上、i5/OS の場合には特に当てはまります。オープン・ソースのインプリメンテーションに重要な機能が追加されました。Pegasus には、認証と権限の 2 つのタイプのセキュリティー検査があります。

関連概念

『EIM (エンタープライズ識別マッピング)』のトピック

26 ページの『cimconfig の使用について』

cimconfig コマンドを使用して CIMOM の開始オプションを構成します。

『ネットワーク認証サービス』のトピック

『ホスト名解決の考慮事項』のトピック

SSL 鍵および Pegasus 用証明書の作成

Pegasus を Secure Sockets Layer (SSL) モードで実行する場合には、秘密鍵および証明書が必要です。Pegasus は、始動時にその秘密鍵および証明書を確認します。それらのファイルが存在していない場合、Pegasus は秘密鍵および自己署名した 365 日間有効の証明書を作成します。また、以下の情報を使用して秘密鍵および証明書を作成することも可能です。

この手順を実行するには、あらかじめシステムに OpenSSL がインストールされている必要があります (LPO 5733-SC1)。

秘密鍵および証明書は、cimconfig コマンドの sslKeyFilePath および sslCertificateFilePath 構成プロパティで定義されているパスに保管されます。これらのパスに、独自の証明書および秘密鍵を作成することができます。これらのパスに証明書または秘密鍵のいずれかがない場合は、CIM サーバーによって独自の証明書および秘密鍵が作成されます。CIM サーバーは、サブジェクト名に対して、以下の属性を持つ証明書を作成します。

```
State or Province Name: Minnesota
Locality: Rochester
Organization Name: IBM
Organizational Unit: iSeries
Common Name: hostname of system
Email Address:
```

注:

- Common Name フィールドは、システムのホスト名で置き換えられます。
- Email Address フィールドはブランクのままにします。
- この証明書は自己署名されます。証明書の有効期限は、作成日から 365 日後に設定されます。

これらのファイルの作成後は、証明書の更新およびリカバリーを管理する必要があります。証明書が有効ではない場合、有効期限が切れた場合、またはセキュリティが危なくなった場合には、SSL 鍵および証明書を作成する必要があります。証明書は、証明書ファイルを削除し、CIM サーバーを再始動することで再作成することができます。CIM サーバーは、有効期限が 365 日以内の新しい証明書を作成します。

注: Pegasus では、パスフレーズ (パスワード) のない秘密鍵ファイルしかサポートされません。そのため、秘密鍵は保護ディレクトリー内に保持することが重要です。デフォルトでは、Pegasus の秘密鍵は、PUBLIC *EXCLUDE があり専用認可のない QSYS 所有のディレクトリーに置かれます。sslKeyFilePath プロパティを変更する場合は、このディレクトリーを保護することをお勧めします。

Pegasus は、疑似乱数発生ルーチン (PRNG) の初期化 (シード) のための OpenSSL デフォルトを許可します。Pegasus は SSL_library_init アプリケーション・プログラミング・インターフェース (API) を呼び出し、この API は i5/OS Qc3GenPrns API (Generate Pseudorandom Numbers) を呼び出します。i5/OS 上の Pegasus は、ファイルからの PRNG のシードをサポートしません。

Pegasus の証明書および秘密鍵を作成する方法の 1 つは、i5/OS でデジタル証明書マネージャー (DCM) を使用する方法です。

DCM は、i5/OS システム上のローカル認証局 (CA) または外部の認証局が発行する、Pegasus サーバー証明書の作成を許可します。

Pegasus は DCM とは統合されていないので注意してください。DCM で作成されたすべての証明書を、Pegasus にエクスポートする必要があります。Pegasus では、PEM 形式の証明書しかサポートされません。

- 秘密鍵および証明書を作成するには、以下のステップを実行します。
- DCM で Pegasus タイプ・サーバーのアプリケーション定義を作成する。Pegasus は DCM と統合されていないため、アプリケーション定義の詳細は重要ではありません。しかし、推奨されるアプリケーション ID は QIBM_CIMOM です。
 - CA によって発行される Pegasus アプリケーション用証明書を作成する。Pegasus 用に証明書を入力する、サブジェクト名の注記を作成します。
 - 以下のステップを実行して、証明書を DCM から Pegasus にエクスポートする。
 - ナビゲーション・フレームで、「証明書の管理」および「証明書のエクスポート」を選択する。
 - 証明書のタイプとして、「サーバーまたはクライアント」を選択する。
 - Pegasus 用に作成した証明書を選択し、「エクスポート」をクリックする。
 - エクスポート先として、「ファイル」を選択する。
 - エクスポート・ファイル名では、Pegasus `sslCertificateFilePath` プロパティで定義されているディレクトリを使用し、ファイル名は `pegasuscert.p12` とする。このファイルは PKCS12 形式になります。

注：ここで入力するパスワードを忘れないようにしてください。これは後で、エクスポートされた証明書を暗号化解除するために使用します。
 - 以下のステップに従って、OpenSSL コマンドを実行して証明書を PKCS12 形式から Privacy Enhanced Mail (PEM) 形式に変換する。
 - i5/OS コマンド行で `CALL QP2TERM` と入力して PASE 環境を始動する。
 - エクスポートされた証明書が位置するディレクトリに移動する。
 - PKCS12 ファイルから証明書を抽出し、OpenSSL コマンド `openssl pkcs12 -in pegasuscert.p12 -out pegasuscert.pem -nokeys -clcerts` を使用して PEM 形式に変換する。このコマンドは、「**DCM エクスポート (DCM Export)**」ページで入力したパスワードを尋ねるプロンプトを出します。

作成される PEM ファイルには、複数の証明書が含まれる場合があります。Pegasus 証明書と、その Pegasus 証明書を発行した CA の証明書の両方が含まれる場合があります。Pegasus ではこのタイプの PEM ファイルをサポートしていないため、CA 証明書を除去する必要があります。

 - PEM ファイルを編集 (Pegasus 証明書の 1 行を除くすべての行を削除) して、CA 証明書を除去する。Pegasus 証明書には、DCM で証明書を作成したときに使用した Pegasus subject 名がありません。Bag Attributes から END CERTIFICATE までの Pegasus 証明書の行を保持します。
 - PKCS12 ファイルから秘密鍵を抽出し、OpenSSL コマンド `openssl pkcs12 -in pegasuscert.p12 -out pegasuskey.pem -nocerts -nodes` を使用して PEM 形式に変換する。このコマンドは、「**DCM エクスポート (DCM Export)**」ページで入力したパスワードを尋ねるプロンプトを出します。

これで証明書および秘密鍵は PEM 形式に変換されました。

 - 証明書を `sslCertificateFilePath` プロパティで定義したパスに配置して、Pegasus がこの証明書を使用できるようにする。
 - 秘密鍵を `sslKeyFilePath` プロパティで定義したパスに配置して、Pegasus がこの秘密鍵を使用できるようにする。

関連概念

6 ページの『`cimconfig` コマンドの拡張開始オプション』

`cimconfig` コマンドを使用して、CIM サーバーの拡張開始オプションを変更することができます。

『デジタル証明書マネージャー』のトピック・コレクション

19 ページの『バックアップおよび回復の考慮事項』

既存のバックアップ・プランの一部として、Pegasus リポジトリを定期的にバックアップします。ほとんどの場合、最新のバックアップ・コピーからの復元を行うことで損傷したリポジトリを回復することができます。

関連情報

OpenSSL Web サイト

クライアントの証明書を検査する CIM サーバーの構成

CIM サーバーを、メインの SSL ポートおよびエクスポート SSL ポートで Secure Sockets Layer (SSL) を使用してクライアントの証明書を検査し、証明書取り消しリスト (CRL) を確認するように構成することができます。

CIM サーバーは、**GetInstance** 要求や **EnumerateInstance** 要求などの CIM 操作要求に、メインの SSL ポートを使用します。エクスポート SSL ポートの目的は、CIM エクスポート要求が、ユーザー名およびパスワードを必要としないポート上で、証明書ベースの自動認証を使用できるようにすることです。CIM エクスポート要求は、CIM Indications の配信に使用されます。エクスポート要求には関連するユーザー名がないため、保護された指示を配信する唯一の方法は、エクスポート SSL ポート上の SSL を使用することです。

CIM サーバーは、CRL に対してクライアントの証明書を確認することもできます。

メイン SSL ポートにおけるクライアント証明書検査の構成

CIM サーバーを、メイン SSL ポートでクライアント証明書を検査するように構成するには、**cimconfig** コマンドの **sslClientVerificationMode** プロパティを使用します。このプロパティは、以下のタスクのいずれかを実行するように設定することができます。

- クライアント証明書検査の使用不可化
- クライアント証明書検査の要求
- クライアント証明書の検査 (使用可能な場合) および **httpAuthType** プロパティの使用 (証明書が使用不可の場合)

これらの選択肢を使用することで、証明書検査、Basic 認証、および Kerberos 認証によってクライアントを認証することができます。

メイン SSL ポートに対するサーバーのトラストストア内の証明書は、**ssltrustmgr** コマンドを使用して管理することができます。この場合、トラストストア名は **cim_trust** です。

エクスポート SSL ポートにおけるクライアント証明書検査の構成

CIM サーバーを、エクスポート SSL ポートでクライアント証明書を検査するように構成するには、**cimconfig** コマンドの **enableSSLExportClientVerification** プロパティを使用します。このプロパティを **true** に設定すると、CIM サーバーは証明書をエクスポート・クライアントで送信するように要求します。**exportSSLTrustStore** プロパティは、トラストストアのロケーションを示します。ほとんどの場合、**exportSSLTrustStore** プロパティのデフォルト値を使用することができます。

エクスポート SSL ポートに対するサーバーのトラストストア内の証明書は、**ssltrustmgr** コマンドを使用して管理することができます。この場合、トラストストア名は **export_trust** です。

1 CRL に対するクライアント証明書の構成

1 CIM サーバーを、CRL に対してクライアント証明書を検査するように構成するには、**crlStore** プロパティ
1 ーを使用します。ほとんどの場合、**crlStore** プロパティのデフォルト値を使用することができます。CIM
1 サーバーは、ローカル・システム上の CRL ファイルまたはディレクトリーを検査します。CRL について
1 リモートの CIM サーバーに問い合わせることはありません。**crlStore** プロパティは、CRL ストアのロ
1 ケーションを示します。**crlStore** は、メイン SSL ポートおよびエクスポート SSL ポートで作成された要
1 求に適用されます。

1 認証

1 Pegasus は、認証プロセスを使用して、CIMOM にログインできるユーザーを判別します。**cimconfig** コマ
1 ンドの **enableAuthentication** プロパティが **false** に設定されていない限り、認証は接続ごとに実行さ
1 れ、認証されないユーザーは CIM データにアクセスすることができません。

1 i5/OS 環境の Pegasus の場合、ユーザーは Basic 認証または Kerberos 認証のいずれかを使用して、HTTP
1 または HTTPS でログインします。HTTPS に加えて、証明書ベースの認証を使用したログインという選
1 択肢もあります。

ログインする場合、ユーザーの認証には i5/OS プロファイルまたは EIM (エンタープライズ識別マッピング)
が使用されます。

オープン・ソースのインプリメンテーションでは、Pegasus は、ユーザーが CIM ユーザー・プロファイル
を使用してサインインできるように別個のアクセス制御リスト (ACL) を保持しているため、必ずしもシス
テム上に対応するプロファイルは必要ありません。逆に、Pegasus の i5/OS インプリメンテーションで
は、各ユーザーが i5/OS にプロファイルを所有していることが必要になります。ユーザーが認証される
と、ユーザー (またはユーザーのジョブ) に、CIMOM の管理下にあるプロバイダーと CIM スキーマへ
のアクセス権が付与されます。

Kerberos を使用可能にする

iSeries の Pegasus は、Kerberos と EIM (エンタープライズ識別マッピング) の両方をサポートします。
Kerberos を使用可能に設定するには、**cimconfig** コマンドを使用して、**httpAuthType** 構成オプションを
Kerberos に設定します (これがデフォルト値です)。

すべての IBM サーバー・プラットフォームで、Kerberos のデフォルト・サーバー名は **cimom** です。
i5/OS では、サービス名 **krbsvr400** を使用することもできます。i5/OS 上の Kerberos について詳しく
は、『ネットワーク認証サービス』のトピックを参照してください。Kerberos のホスト名解決につい
ては、『ネットワーク認証サービス』トピック・コレクション内の『ホスト名解決の考慮事項』に記載され
ている指示に従ってください。

例えば、CIMOM サービス・プリンシパルを設定する 1 つの方法として、次のコマンドを入力するとしま
す。

1. KDC が実行されている i5/OS システムで、次のコマンドを使用してサービス・プリンシパル **cimom**
を追加する。

```
addprinc cimom/<host>@<realm>
```

KDC のパスワードの入力を求めるプロンプトが表示されます。

2. CIMOM サーバーを実行する必要がある i5/OS ごとに、次のコマンドを使用してサービス・プリンシ
パル **cimom** を追加する。

```
keytab add cimom/<host>@<realm>
```

keytab ファイルのパスワードの入力を求めるプロンプトが表示されます。

この例では、次のことを前提とします。

- KDC と keytab ファイルのパスワードが一致すること。
- ホストが、『ホスト名解決の考慮事項』に記載されている指示に従って判別されていること。

注:

- 『ネットワーク認証サービス』のトピックで Keytab コマンドの情報を参照してください。
- Kerberos 認証が使用可能に設定されている場合、CIM サーバーに接続できるのは、Kerberos 認証をサポートしている CIM クライアントのみです。

EIM が使用可能に設定されていない場合は、Kerberos プリンシパルが、CIMOM が実行されているシステム上のユーザー ID として直接使用されます。管理者は、すべてのシステムで一致するユーザー ID を設定しなければなりません。例えば、ユーザーが EIM を構成して使用可能に設定しないようにした場合、管理者は Kerberos プリンシパル john が常にローカル・ユーザー ID として john にマッピングされるように注意する必要があります。

Pegasus の許可

i5/OS の Pegasus に必要なタイプのセキュリティー検査は、ユーザーが変更しようとしているオブジェクトへのアクセス権を持っていることを確認することです。このプロセスのことを許可と言います。

Pegasus には、ユーザーに権限が必要な操作として、CIM クラスおよび修飾子の操作と CIM インスタンスの操作の 2 つのタイプがあります。

CIM クラスおよび修飾子の操作では、CIM スキーマのローカル・コピー (例えば、DeleteClass) が変更されます。CIM 提供のシステム管理データを扱う、次の情報にリストされている操作を使用するためには、ユーザーにこれらの操作に対する権限が必要です。これらの操作で i5/OS システム・オブジェクトが変更されることはありませんが、クライアントに送る CIM スキーマが変更されるため、これらの操作を使用する場合は権限が必要になります。iSeries サーバーでは、これらの操作の権限は、iSeries ナビゲーターのアプリケーション管理で制御されます。

アプリケーション管理で CIM 操作の権限を処理するには、次のようにします。

1. iSeries ナビゲーターを開始する。
2. 「ユーザー接続」から、変更するシステムを右クリックする。
3. 「アプリケーション管理」を選択する。
4. 「ローカル設定 (Local Settings)」を選択する (選択可能な場合)。
5. 「ホスト・アプリケーション」タブを選択する。
6. 「CIMOM サーバー (CIMOM server)」を展開する。
7. 次の操作に対するユーザー権限またはグループ権限を追加または削除する。

アプリケーション管理でユーザーに権限を付与することができる操作は次のとおりです。

- GetClass
- DeleteClass
- CreateClass
- ModifyClass
- EnumerateClasses

- EnumerateClassNames
- GetQualifier
- SetQualifier
- DeleteQualifier
- EnumerateQualifiers

CIM インスタンスの操作では、ユーザーは Pegasus プロバイダーによってモデル化されたサーバー・リソースを操作することができます。これらのプロバイダーは i5/OS ではサーバー出口プログラム (*SRVPGM) としてインプリメントされるため、ユーザーがこれらのサービス・プログラムを使用するには、その権限が必要になります。メトリック・プロバイダー QSYS/QYCPCSMV を除き、V5R3 に組み込まれているすべてのプロバイダーには出荷時に PUBLIC *USE 権限が付与されています。メトリック・プロバイダー QSYS/QYCPCSMV には、出荷時に PUBLIC *EXCLUDE 権限が付与されています。出荷時に PUBLIC *USE 権限が付与されていないプロバイダーを追加する場合、管理者は明示的にそれらのオブジェクトの権限をユーザーに付与する必要があります。

バックアップおよび回復の考慮事項

- | 既存のバックアップ・プランの一部として、Pegasus リポジトリを定期的にバックアップします。ほとんどの場合、最新のバックアップ・コピーからの復元を行うことで損傷したリポジトリを回復することができます。
- | Pegasus リポジトリは、統合ファイル・システムの qibm/userdata/os400/cim ディレクトリにあります。Pegasus は、管理対象オブジェクトおよびこのリポジトリ内にあるそのプロバイダーに関するデータの定義を保持します。さらに、クライアントおよびプロバイダーによって、その他の定義が追加される場合があります。
- | CIMOM サーバーとともにインストールされる定義は以下のとおりです。
 - root: DMTF 仕様に準拠するために存在するルート・ネーム・スペースです。
 - root/cimv2: 標準 CIM スキーマはこれになります。また、配送済みプロバイダーのスキーマでもあります。
 - root/PG_Interop: これはプロバイダー登録用です。このスペースは、プロバイダー専用予約されており、プロバイダーはすべてここに登録する必要があります。
 - root/PG_Internal: このスペースは Pegasus CIMOM サーバー専用予約済みです。
 - root/ibmsd: 基本オペレーティング・システムに同梱されている IBM Director によって所有および使用されるネーム・スペースです。
- | Pegasus はまた、以下の 2 つの重要な構成ファイルを qibm/userdata/os400/cim ディレクトリに保管します。
 - cimserver_current.conf。このファイルには、デフォルトではなく現行値が入ります。
 - cimserver_planned.conf。このファイルには、デフォルトではなく、まだ有効になっていない、予定の値が入ります。
- | **重要:** 構成ファイルを手動で編集しないでください。 **cimconfig** コマンドを使用する必要があります。
- | このディレクトリ内のファイルが削除、移動、または破壊された場合は、バックアップからリストアする必要があります。
- | **重要:**

最新のバックアップ・リポジトリが V5R3 リリースのものである場合は、Pegasus V2.5 が入っているシステムに復元しないでください。Pegasus V2.5 をインストールし、リポジトリをアップグレードしたら、CIM サーバーの再始動後すぐに、新しいリポジトリをバックアップしてください。

サーバーの SSL 証明書および秘密鍵ファイルは、qibm/userdata/os400/cim/ssl/keystore ディレクトリーにあります。CIM サーバーの SSL 証明書ファイルのバックアップ・ファイルがない場合は、証明書を再作成することができます。

CIM サーバーの SSL ファイルに関連するその他のディレクトリーは、以下のとおりです。

- サーバーの CIM クライアント・トラストストアは、/qibm/userdata/os400/cim/ssl/truststore にあります。
- サーバーの CIM Export クライアント・トラストストアは、/qibm/userdata/os400/cim/ssl/exporttruststore にあります。
- サーバーの証明書取り消しリストは、/qibm/userdata/os400/cim/ssl/crlstore にあります。

トラストストア証明書または証明書取り消しリストのバックアップ・ファイルがない場合は、qshell から **ssltrustmgr** コマンドを使用して再作成し、トラストストアまたは crlstore に追加する必要があります。

注: **ssltrustmgr** コマンドを使用して、破壊された証明書をトラストストアから除去します。**ssltrustmgr** コマンドが破壊された証明書の除去に失敗した場合は、サービス・プロバイダーに連絡してください。

関連概念

26 ページの『cimconfig の使用について』

cimconfig コマンドを使用して CIMOM の開始オプションを構成します。

関連タスク

14 ページの『SSL 鍵および Pegasus 用証明書の作成』

Pegasus を Secure Sockets Layer (SSL) モードで実行する場合には、秘密鍵および証明書が必要です。Pegasus は、始動時にその秘密鍵および証明書を確認します。それらのファイルが存在していない場合、Pegasus は秘密鍵および自己署名した 365 日間有効の証明書を作成します。また、以下の情報を使用して秘密鍵および証明書を作成することも可能です。

関連情報

『サーバーのバックアップ』のトピック

破壊されたファイルの復元

この情報は、CIM リポジトリおよび SSL ファイルのバックアップ・コピーが破壊された場合に使用してください。

カスタマー・ファイルをリカバリーするには、以下のリストにある情報を使用します。

リポジトリ・クラスおよびクォリファイア (静的データ)

クラスまたは修飾子を作成するために行った操作を取り消します。例えば、クライアント・アプリケーションをアンインストールするか、行った操作を取り消すための手順を手動で実行します。その後、クラスまたは修飾子を以前と同じ状態に戻します。例えば、クライアント・アプリケーションを再インストールします。問題が解決しない場合には、サービス・プロバイダーに連絡してください。

リポジトリ・インスタンス

インスタンスを作成するために行った操作を取り消します。例えば、クライアント・アプリケーションをアンインストールするか、行った操作を取り消すための手順を手動で実行します。その後、

クラスまたは修飾子を以前と同じ状態に戻します。例えば、クライアント・アプリケーションを再インストールします。まだ問題が解決しない場合には、サービス・プロバイダーに連絡してください。

プロバイダー登録データ (インスタンスも含む)

cimprovider コマンドを使用して、プロバイダー登録を削除します。その後、**cimmofl** コマンドを使用してデータを再コンパイルし、再登録します。まだ問題が解決しない場合には、サービス・プロバイダーに連絡してください。

SSL ファイル

CIMOM SSL 証明書および秘密鍵

古い証明書および秘密鍵を削除してから、14 ページの『SSL 鍵および Pegasus 用証明書の作成』の手順を実行して新しい証明書および秘密鍵を作成します。

トラストストアおよび **crlstore** のリカバリー

ssltrustmgr コマンドを使用して、トラストストアおよび **crlstore** を再作成します。

CIM サーバーのトラブルシューティング

ここに記載する情報は、CIM サーバーのトラブルシューティングを行うために使用してください。

この情報は、CIM サーバーが始動しない場合、または CIM サーバーが始動はするが予想と異なる動作をする場合に使用してください。

関連情報

OpenSSL 資料

CIM サーバーが始動しない

CIM サーバーが始動しない場合は、以下のステップを実行します。

注: Pegasus V2.5 のインストール後初めて CIMOM サーバーを始動する場合は、サーバーの始動に時間がかかります。その間に、リポジトリのアップグレード、および以前のリポジトリからのユーザー・データのマイグレーションが行われます。

CIM サーバーが正しく構成されていることを確認します。

CIM サーバーの構成については、4 ページの『必要な構成パラメーターを設定する』を参照してください。

基本認証を使用するために、Kerberos 構成の変更、または CIM サーバーの変更を行う必要があるかどうかを確認します。

以下のメッセージが表示される場合は、認証にエラーがあります。ご使用の認証を修正するか、基本認証などの別の形式の認証を使用する必要があります。

CPDDF82: (メッセージは CIM サーバーの QYCMCIMOM のジョブ・ログに表示されます)

PGS02000: CIM サーバーの Kerberos 認証ハンドラーを適切に初期化することに失敗しました。

CIM サーバーは始動していません。

注: HTTPS、または、平文パスワードの引き渡しが必要な高度に保護された環境を使用していない限り、基本認証は使用しないでください。 **cimconfig** コマンドを使用して CIM 構成設定を変更するには、**QSHELL** (オプション 30) がインストールされている必要があります。

権限を基本に変更するには、コマンド行に以下のコマンドを入力します。

```
| qsh  
| cd / QIBM/UserData/OS400/CIM  
| cimconfig -shttpAuthType=Basic -p
```

| システムに正しいオプションがインストールされていることを確認します。

| CPDDF80 理由コード 07 が表示される場合は、必須指定のオプション 39 がインストールされて
| いません。オプション 39 (ICU) をインストールしてください。

| SSL が使用不可に設定された状態でサーバーが始動し、サーバー・ジョブ・ログに OpenSSL が必
| 要であるというメッセージが書き込まれている場合は、LPO 5733-SC1 (OpenSSL) をインストール
| する必要があります。この場合は、サーバーは SSL を使用するよう構成されていますが、
| OpenSSL がインストールされていません。OpenSSL をインストールするか、SSL を使用しないよ
| うにサーバーを構成することができます。サーバーのデフォルトの構成では、wbem-https と
| wbem-exp-https の両方のポートで SSL が使用可能になっています。

| また、LPO 5733-SC1 にインストール・エラーがある場合にも、サーバー・ジョブ・ログにこのメ
| ッセージが書き込まれ、SSL が使用不可の状態です。サーバーが始動します。この場合には、
| CHKPRDOPT コマンドを使用して、LPO のエラー状況を確認することができます。

| OpenSSL を使用するには、PASE (基本 OS のオプション 33) がインストールされている必要があ
| ります。サーバーの始動後、PASE が未インストールで、サーバーでは SSL が使用可能になっ
| ている場合は、OpenSSL がサーバー・ジョブ・ログに CPFB9C1 エスケープ・メッセージを送信
| し、サーバーは終了します。

| CIM サーバーが予想と異なる振る舞いをする

| CIM サーバーに問題がある場合は、以下の指示を参照してください。

| コマンド行に **WRKJOB QYCMCIMOM** と入力して、CIM サーバーが実行されているかどうかを確認し
| ます。アクティブ・ジョブがない場合は、コマンド行に **STRTCPSVR *CIMOM** と入力して CIM サーバ
| ーを始動します。

| **CIMOM** リポジトリが破壊されていないかどうかを確認する。

| 統合ファイル・システムの QIBM/UserData/OS400/CIM ディレクトリーに、リポジトリ・ディレ
| クトリーおよび構成ファイルがあるかどうかを確認します。これらのファイルのいずれかが欠落し
| ている場合は、バックアップからすべてのリポジトリ・ディレクトリーおよびファイルをリスト
| アします。Pegasus V2.5 PTF がインストールされていない V5R3 システムではなく、Pegasus
| V2.5 バックアップのファイルのバックアップを使用する必要があります。

| 復元可能なバックアップがない場合は、20 ページの『破壊されたファイルの復元』の手順に従い
| ます。

| プロバイダーが登録されていないか使用不可のときに、要求の処理を試行していないかどうかを確認しま
| す。プロバイダーが登録されていないか使用不可のときに要求の処理を試行していないかどうかを確認
| するには、以下のステップを実行します。

- | 1. **cimprovider -l -s** と入力して、登録済みプロバイダー・モジュールの名前と状況をリストす
| る。
- | 2. **cimprovider -l-m module name** と入力して、そのモジュール内の個々のプロバイダーを表示す
| る。

| ジョブ・ログ・ファイルを検査します。

| ジョブ・ログ・ファイルを検査するには、以下のステップを実行します。

- | 1. コマンド行に **WRKACTJOB** と入力する。
- | 2. **QSYSWRK** サブシステムの中から **QYCMCIMOM** ジョブを探す。

3. 5 (これを扱う仕事をする) を選択してから 10 (アクティブであればジョブ・キューにジョブ・ログを表示するか、または保留する) を選択する。
4. QYCMCIMOM ジョブが実行されていない場合は、WRKJOB QYCMCIMOM と入力する。
5. 最新のジョブの隣に 1 (選択) を入力して選択する。
6. 状況が OUTQ の場合は、4 (スプール・ファイルで作業する) を入力してから、QPJOBLOG ファイルの隣に 5 (表示) を入力する。

SSL 証明書関連のメッセージの原因が、CIM クライアント要求の失敗かどうかを確認します。

リモート CIM サーバーの証明書が、クライアント・システム上のトラストストア・ファイルに追加されていることを確認します。クライアント・アプリケーションがクライアントの証明書および秘密鍵を使用しており、クライアント証明書がサーバーから信頼されていることを確認します。

Pegasus のコマンド行ユーティリティー

オープン・ソースの Pegasus インプリメンテーションには、Pegasus 環境の制御や変更に使用できるコマンド行ユーティリティーのセットが含まれています。

i5/OS バージョンの Pegasus では、これらのコマンドに、i5/OS 環境での Pegasus の実行をサポートするための変更が一部加えられています。通常の使用では、管理者がこれらのコマンドを使用する必要はほとんどありません。

コマンドには次のものがあります。

- **cimmofl**
- **cimconfig**
- **cimprovider**
- **ssltrustmgr**

i5/OS インプリメンテーションの場合、**cimmofl**、**cimconfig**、および **cimprovider** コマンドには、*IOSYSCFG および *ALLOBJ の特殊権限が必要です。**ssltrustmgr** コマンドには、*SECADM および *ALLOBJ の特殊権限が必要です。

コマンド行ユーティリティーはすべて QSHELL コマンド行から実行する必要があるため、QSHELL 製品 (SS1 opt. 30) がシステムにインストールされていなければなりません。これらのコマンドは /QIBM/UserData/OS400/CIM から実行することができます。

関連概念

3 ページの『Pegasus の構成』

Pegasus CIMOM には、数多くの構成オプションを設定する機能があります。

24 ページの『cimmofl の使用について』

このコマンドは、プロバイダー登録をコンパイルする場合と、CIM クラス記述 (Managed Object Format (MOF) 言語使用) をコンパイルして、リポジトリに保管するクラス・スキーマに挿入する場合に使用します。

26 ページの『cimconfig の使用について』

cimconfig コマンドを使用して CIMOM の開始オプションを構成します。

28 ページの『cimprovider の使用について』

主にテストの際に、登録済みのプロバイダーを使用可能/使用不可に設定します。このコマンドを使用する場合は CIMOM が実行されていなければなりません。

cimmofl の使用について

このコマンドは、プロバイダー登録をコンパイルする場合と、CIM クラス記述 (Managed Object Format (MOF) 言語使用) をコンパイルして、リポジトリに保管するクラス・スキーマに挿入する場合に使用します。

このコマンドを使用する前には CIMOM を停止する必要があります。

注: このコマンドは /QIBM/UserData/OS400/CIM から実行することができます。

名前 cimmofl - CIM クラス記述 (MOF 言語使用) をコンパイルして、リポジトリに保管するクラス・スキーマに挿入する場合に使用します。このコマンドを使用する前には CIMOM を停止する必要があります。

形式 使用法:

```
cimmofl -h | --help
cimmofl --version
cimmofl [ -w ] [ -E ] [ -uc ] [ -aE | -aV | -aEV ] [ -I path ] [ -n namespace |
--namespace namespace ] [ --xml ] [ --tracefile ] [ -q ]
[ -R repositorydir | --CIMRepository repositorydir ] [ -N repositoryname ] [ -M
repositorymode] mof_file...
```

説明

このコマンドは、プロバイダー登録をコンパイルする場合と、CIM クラス記述 (MOF 言語使用) をコンパイルして、リポジトリに保管するクラス・スキーマに挿入する場合に使用します。このコマンドを使用する前には CIMOM を停止する必要があります。

Pegasus MOF コンパイラーは (DMTF CIM 仕様で定義される MOF フォーマットを使用している) MOF ファイルを Pegasus リポジトリにコンパイルするコマンド行ユーティリティーです。インクルード・プラグマを使用した MOF ファイルの構造からのコンパイルを可能にし、Pegasus リポジトリへのコンパイルや、MOF ファイルの構文チェックの実行を可能にします。コンパイラーの使用では、入力 MOF ファイルが現行ディレクトリーに入っていることや、完全修飾パスを指定することが要求されます。 #pragma インクルードを使用して組み込まれる MOF ファイルは、現行ディレクトリーまたは -I コマンド行スイッチで指定されるディレクトリーに入っていなければなりません。

オプション

-h, --help

使用メッセージをコマンド定義と共に出力する。

--version

CIMOM サーバーのバージョンを表示する。

-E 入力の構文チェックを実行する場合に使用する。このオプションでは、リポジトリは更新されません。

-w 警告メッセージを抑制する。

-q コマンド行使用エラーを除くすべてのメッセージを抑制する場合に使用する。

-uc 既存のクラス定義の更新を許可する場合に使用する。このオプションでは、リーフ・クラスを更新することができます。サブクラスを持つスーパークラスまたはクラスの更新は認められません。

-aE 試験的修飾子によるクラスの追加または変更を許可する場合に使用する。

-aV 結果的にバージョン変更が発生するクラスの更新に使用する。このオプションは、クラスの主なバージョンを変更可能にするか、バージョンのレベルを下げられるようにするか、あるいはバージョンを削除できるようにします。バージョンは有効なフォーマットで指定してください。フォーマットは `m.n.u` です。ここで、`m` はメジャー・バージョン、`n` はマイナー・リリース、`u` は更新を示します。例えば、`2.7.0` は CIM スキーマ `2.7.0` の有効なフォーマットです。入力クラスのバージョンがリポジトリ内のクラスと同じ場合、そのクラスは更新されません。

-aEV 試験的スキーマ変更とバージョン・スキーマ変更の両方を許可する。

-R<path>

書き込み先のリポジトリのパスを指定する。絶対パスまたは相対パスを指定します。デフォルトは `/QIBM/UserData/OS400/CIM` です。

--CIMRepository<path>

これを指定した場合は、現行のリポジトリ・パスがオーバーライドされる。絶対パスまたは相対パスを指定します。デフォルトは `/QIBM/UserData/OS400/CIM` です。

-I<path>

インクルード MOF ファイルのパスを指定する場合に使用する。

-n<path>

デフォルトの CIM リポジトリ・ネーム・スペースをオーバーライドする場合に使用する。デフォルトは `root/cimv2` です。

--namespace<path>

デフォルトの CIM リポジトリ・ネーム・スペースをオーバーライドする場合に使用する。デフォルトは `root/cimv2` です。

--xml 標準出力に対して XML を生成する場合に使用する。このオプションでは、リポジトリは更新されません。

--trace トレース情報をファイルに書き込む場合に使用する。出力の宛先は標準出力です。

--trace=<tracefile>

トレース情報を指定のファイルに書き込む場合に使用する。

-N repositoryname

リポジトリ名を指定するために使用する。これは、**-R** オプション内のディレクトリーの相対パスです。デフォルトは `repository` です。

-M repositorymode

リポジトリ・モード (XML、BIN) を指定するために使用する。

注: デフォルトは **XML** です。これは、`i5/OS` に許可されている唯一の値です。

例 `cimmofl -w -Rtestrepository -I./myDir myDir/CIM_Schema.mof`

注: ディレクトリー `myDir` にある `CIM_Schema.mof` という名前の MOF (Managed Object Format) ファイルをコンパイルします。 `CIM_Schema.mof` には、同じ MOF ディレクトリーに入っているその他の MOF ファイルに対するプラグマが含まれています。このコマンドでは、デフォルトのネーム・スペース `root/cimv2` を使用してディレクトリー `testrepository` にリポジトリを作成します。 `testrepository` ディレクトリーが存在することが前提となります。 `-w` オプションを使用すると、警告メッセージが抑止されます。

```
| cimmofl -w -R/qibm/userdata/os400/cim -I/qibm/proddata/os400/cim/schemas/cim -nroot/cimv2  
| /qibm/proddata/os400/cim/schemas/cim/CIM_Schema.mof
```

注: ディレクトリー /qibm/proddata/os400/cim/schemas/cim にある CIM_Schema.mof という名前の MOF ファイルをコンパイルします。CIM_Schema.mof には、同じ /qibm/proddata/os400/cim/schemas/cim ディレクトリーに入っているその他の MOF ファイルに対するプラグマが含まれています。このコマンドでは、ネーム・スペース root/cimv2 を使用してディレクトリー /qibm/userdata/os400/cim にリポジトリーを作成します。/qibm/userdata/os400/cim ディレクトリーが存在することが前提となります。-w オプションを使用すると、警告メッセージが抑止されます。

iSeries 固有の使用上の注意: iSeries サーバーでこのコマンドを使用する場合は、*IOSYSCFG 権限と *ALLOBJ 権限が必要です。

関連概念

23 ページの『Pegasus のコマンド行ユーティリティー』
オープン・ソースの Pegasus インプリメンテーションには、Pegasus 環境の制御や変更で使用できるコマンド行ユーティリティーのセットが含まれています。

cimconfig の使用について

cimconfig コマンドを使用して CIMOM の開始オプションを構成します。

| 計画されている構成設定内の任意の構成プロパティーを変更した場合、CIM サーバーを再始動するまで変更内容は有効になりません。

| **注:** このコマンドは /QIBM/UserData/OS400/CIM から実行することができます。

名前 cimconfig - CIMOM 構成プロパティーを取得、設定、設定解除、またはリストする。

形式 使用方法:

- cimconfig -g name [-c] [-d] [-p] [-q]
- cimconfig -s name=value [-c] [-p] [-q]
- cimconfig -u name [-c] [-p] [-q]
- cimconfig -l [-c | -p]
- cimconfig -h
- cimconfig --help
- cimconfig --version

注釈 cimconfig コマンドは、CIMOM 構成プロパティーを管理するためのコマンド行インターフェースを提供します。

cimconfig の最初の形式では、指定の構成プロパティーの現行値、計画値、およびデフォルト値を指定します。

2 番目の形式では、指定の構成プロパティーの現行値と計画値を指定された値に設定することができます。

3 番目の形式では、指定の構成プロパティーの現行値と計画値を設定解除してデフォルト値に戻すことができます。

このコマンドの最後の形式では、すべての構成プロパティーのリストを作成することができます。-c オプションまたは -p オプションを指定すると、すべての現行 (current) または計画 (planned) 構成プロパティーの名前と値のリストが作成されます。

オプション

cimconfig コマンドで認識されるオプションは次のとおりです。

- | **-h, --help**
| コマンドのヘルプ情報を表示する。
- | **--version**
| CIMOM サーバーのバージョンを表示する。
- | **-g name**
| 指定の構成プロパティの現行値を取得する。 CIMOM が実行されていない場合はエラーを返します。
- | **-g name -c**
| 指定の構成プロパティの現行値を取得する。 CIMOM が実行されていない場合はエラーを返します。
- | **-g name -p**
| 指定の構成プロパティの計画値を取得する。
- | **-g name -d**
| 指定の構成プロパティのデフォルト値を取得する。 CIMOM が実行されていない場合はエラーを返します。
- | **-s name=value**
| 構成プロパティの現行値を指定の値に設定することで、その構成プロパティが追加または更新されることを示す。 CIMOM が実行されていない場合または指定のプロパティを動的に更新できない場合は、エラーを返します。
- | **-s name=value -c**
| 構成プロパティの現行値を指定の値に設定することで、その構成プロパティが追加または更新されることを示す。 CIMOM が実行されていない場合または指定のプロパティを動的に更新できない場合は、エラーを返します。
- | **-s name=value -p**
| 構成プロパティの計画値を指定の値に設定することで、その構成プロパティが追加または更新されることを示す。
- | **-u name**
| 指定の構成プロパティの現行値をデフォルト値にリセットすることを示す。 CIMOM が実行されていない場合または指定のプロパティを動的に更新できない場合は、エラーを返します。
- | **-u name -c**
| 指定の構成プロパティの現行値をデフォルト値にリセットすることを示す。 CIMOM が実行されていない場合または指定のプロパティを動的に更新できない場合は、エラーを返します。
- | **-u name -p**
| 指定の構成プロパティの計画値をデフォルト値にリセットすることを示す。
- | **-l** すべての構成プロパティの名前を表示する。 CIMOM が実行されていない場合はエラーを返します。
- | **-l -c** すべての現行の構成プロパティの名前と値のペアを表示する。 CIMOM が実行されていない場合はエラーを返します。
- | **-l -p** すべての計画の構成プロパティの名前と値のペアを表示する。
- | **-q** q (quiet) オプションでは、出力を標準出力または標準エラーに送信しないことを指定する。

iSeries 固有の使用上の注意: iSeries サーバーでこのコマンドを使用する場合は、 *IOSYSCFG 権限と *ALLOBJ 権限が必要です。

注: cimconfig コマンドでは、CIMOM の現行または計画の構成プロパティを設定することができます。現行の構成プロパティを更新できるのは、CIMOM が実行されている場合のみです。計画の構成プロパティの場合は、CIMOM の実行、停止にかかわらず、すべてのプロパティを変更することができます。計画の構成プロパティが変更された場合、それらの変更は CIMOM を再始動するまで有効になりません。CIMOM が始動すると、計画の構成プロパティが現行の構成プロパティになります。

関連概念

19 ページの『バックアップおよび回復の考慮事項』

既存のバックアップ・プランの一部として、Pegasus リポジトリを定期的にバックアップします。ほとんどの場合、最新のバックアップ・コピーからの復元を行うことで損傷したリポジトリを回復することができます。

23 ページの『Pegasus のコマンド行ユーティリティー』

オープン・ソースの Pegasus インプリメンテーションには、Pegasus 環境の制御や変更に使用できるコマンド行ユーティリティーのセットが含まれています。

3 ページの『Pegasus の構成』

Pegasus CIMOM には、数多くの構成オプションを設定する機能があります。

関連タスク

13 ページの『Pegasus の保護』

このトピックは、CIM サーバーの機密性を確保するために利用できるオプションを見つけるために使用してください。

cimprovider の使用について

主にテストの際に、登録済みのプロバイダーを使用可能/使用不可に設定します。このコマンドを使用する場合は CIMOM が実行されていなければなりません。

1 **注:** このコマンドは /QIBM/UserData/OS400/CIM から実行することができます。

名前 cimprovider - 登録済みの CIM プロバイダーまたは CIM プロバイダーのモジュールおよびモジュール状況を使用不可、使用可能、除去、またはリストします。

形式 使用法:

- cimprovider -d -m module [-q]
- cimprovider -e -m module [-q]
- cimprovider -r -m module [-p provider] [-q]
- cimprovider -l [-s | -m module]
- cimprovider -h
- cimprovider --help

制限 このコマンドによる CIM プロバイダー・モジュールまたは CIM プロバイダーの使用不可/使用可能の設定、または除去は、1 つずつ行われます。

説明

cimprovider コマンドは、登録済みの CIM プロバイダーを使用不可に設定、使用可能に設定、登録解除、およびリストするためのコマンド行インターフェースを提供します。CIM プロバイダーが使用不可になると、CIMOM はそのプロバイダーに対する要求を拒否します。CIM プロバイダー

が使用可能になると、CIMOM は要求をそのプロバイダーに転送します。また、CIM プロバイダーが登録解除されると、CIMOM はそのプロバイダーに関する情報を失います。 `cimprovider` コマンドを使用するためには、`cimserver` が実行されていること、および指定のプロバイダー・モジュール (同一の *SVRPGM にあるプロバイダーのグループ) またはプロバイダーが CIMOM に登録されていることが必要です。

`cimprovider` の最初の形式は、指定のプロバイダー・モジュールを使用不可にします。指定のプロバイダー・モジュールが使用不可の状態になると、そのプロバイダー・モジュールに含まれるプロバイダーに対する新規要求はすべて拒否されます。

`cimprovider` の 2 番目の形式は、指定のプロバイダー・モジュールに含まれるプロバイダーを使用可能にします。指定のプロバイダー・モジュールに含まれるプロバイダーが新規要求を受け取ることができるようになります。

`cimprovider` の 3 番目の形式は、指定のプロバイダー・モジュール、および指定のプロバイダー・モジュールに含まれるすべてのプロバイダーまたは指定のプロバイダーを除去 (登録解除) します。プロバイダーまたはプロバイダー・モジュールを除去した場合には、再登録が必要になります (一般的には、`cimmofl` コマンドを介して登録スキーマをロードします)。

`cimprovider` の最後の形式は、登録済みのすべてのプロバイダー・モジュールとモジュール状況、または指定のプロバイダー・モジュール内のすべてのプロバイダーをリストします。すべてのモジュール内のすべてのプロバイダーをリストするには、`cimprovider -l` コマンドの後に、リストされるモジュールごとに `cimprovider -l -m` を実行します。

オプション

`cimprovider` コマンドで認識されるオプションは次のとおりです。

- | **-h, --help**
 - | コマンドのヘルプ情報を表示する。
- | **--version**
 - | CIMOM サーバーのバージョンを表示する。
- | **-d** 指定の CIM プロバイダー・モジュールを使用不可にする。モジュールがすでに使用不可になっている場合は、エラー・メッセージが戻されます。
- | **-e** 指定の CIM プロバイダー・モジュールを使用可能にする。モジュールがすでに使用可能になっている場合、または現在使用不可に設定中の場合は、エラー・メッセージが戻されます。
- | **-r** 指定のプロバイダー・モジュールおよびそこに含まれるすべてのプロバイダーを除去する。プロバイダーが指定された場合は、指定のプロバイダー・モジュール内の指定のプロバイダーが除去され、そのモジュール内のその他のプロバイダーには影響しません。
- | **-l** 登録済みのすべてのプロバイダー・モジュールを表示する。
- | **-m Module**
 - | 操作対象のプロバイダー・モジュールを指定する。
- | **-p Provider**
 - | 操作対象のプロバイダーを指定する。
- | **-q** q (quiet) オプションでは、出力を標準出力または標準エラーに送信しないことを指定する。
- | **-s** プロバイダー・モジュールの状況を表示する。

例

cimprovider -d -m myProviderModule

プロバイダー・モジュール myProviderModule およびそこに含まれるすべてのプロバイダーを使用不可にします (停止状態にします)。

cimprovider -e -m myProviderModule

プロバイダー・モジュール myProviderModule およびそこに含まれるすべてのプロバイダーを使用可能にします (OK 状態にします)。

cimprovider -r -m myProviderModule

プロバイダー・モジュール myProviderModule およびそこに含まれるすべてのプロバイダーを除去 (登録解除) します。

cimprovider -r -m myProviderModule -p MyProvider

プロバイダー・モジュール myProviderModule に含まれる MyProvider プロバイダーを除去 (登録解除) します。

cimprovider -l

登録済みのプロバイダー・モジュールをリストします。

cimprovider -l -s

登録済みのプロバイダー・モジュールとその状態 (OK、停止中、停止など) をリストします。

cimprovider -l -m myProvider

プロバイダー・モジュール myProviderModule に含まれる登録済みプロバイダーをリストします。

iSeries サーバー固有の使用上の注意: iSeries サーバーでこのコマンドを使用する場合は、*IOSYSCFG 権限と *ALLOBJ 権限が必要です。

関連概念

23 ページの『Pegasus のコマンド行ユーティリティー』

オープン・ソースの Pegasus インプリメンテーションには、Pegasus 環境の制御や変更で使用できるコマンド行ユーティリティーのセットが含まれています。

| **ssltrustmgr の使用について**

| このコマンドは、トラストストアまたは証明書取り消しリスト (CRL) で X.509 証明書を管理するためのコマンド行インターフェースを提供します。

| QSHELL コマンド行から ssltrustmgr コマンドを実行する必要があります。そのためには、システムに QSHELL 製品がインストールされている必要があります。このコマンドは /QIBM/UserData/OS400/CIM から実行することができます。

| このコマンドを使用する場合は CIMOM が実行されていなければなりません。

| **名前** ssltrustmgr - PEM 形式のトラストストアにある X.509 証明書を、追加、除去、取り消し、またはリストします。

| **形式** 使用法:

| • ssltrustmgr -a [-t truststore] -c certuser -f certfile

| • ssltrustmgr -a -T trustpath -f certfile

| • ssltrustmgr -a -R -f crlfile

| • ssltrustmgr -r [-t truststore | -T trustpath] -i issuername -n serialnumber

| • ssltrustmgr -r -R -i issuername

- | • `ssltrustmgr -l [-t truststore | -T trustpath] [-i issuername [-n serialnumber]]`
- | • `ssltrustmgr -l -R [-i issuername]`
- | • `ssltrustmgr -h | --help`
- | • `ssltrustmgr -v | --version`

| **注釈** コマンドを実行しているユーザーが特権ユーザーではない場合、このコマンドはエラー状況とともに終了します。特権ユーザーには `*ALLOBJ` および `*SECADM` 特殊権限があります。 `ssltrustmgr` コマンドを使用するには、CIM サーバーが実行されている必要があります。

| 説明

| `ssltrustmgr` コマンドは、トラストストアまたは証明書取り消しリスト (CRL) で X.509 証明書を管理するためのコマンド行インターフェースを提供します。トラストストアまたは CRL ストアが存在しないか、またはディレクトリー形式になっていない場合は、コマンドはエラー状況とともに終了します。

| `ssltrustmgr` コマンドの `add` オプションは、以下のいずれかで X.509 証明書を追加します。

- | • `certfile` を指定された `truststore` または `trustpath` へ。
- | • `crfile` の CRL を CRL ストアへ。

| サポートされる `truststore` 名は、`cim_trust` および `export_trust` です。 `truststore` が指定されていない場合は、`cim_trust` がデフォルトの `truststore` として使用されます。 `truststore` が指定されている場合は、`certuser` を指定する必要があります。 `certuser` は、`certfile` 内の証明書と関連するユーザー名を指定します。 `crfile` で指定された CRL が既に CRL ストア内に存在している場合、既存の CRL は上書きされます。

| `ssltrustmgr` コマンドの `remove` オプションは、指定済みの `issuername` および `serialnumber` と一致する X.509 証明書を、指定済みの `truststore` または `trustpath` から除去します。 `remove` オプションはまた、指定済みの `issuername` の CRL ストアから CRL を除去します。

| `ssltrustmgr` コマンドの `list` オプションは、指定済みの `truststore` または `trustpath` 内の X.509 証明書をリストします。リストは、`issuername` および `serialnumber` を指定することによってフィルタリングすることができます。 `list` オプションはまた、指定済みの `issuername` の CRL もリストします。

| オプション

| `ssltrustmgr` コマンドは以下のオプションを使用します。

- | **-a** 指定済みの証明書をターゲットの `truststore`、`trustpath`、または CRL ストアに追加します。 `truststore` または `trustpath` が存在しない場合は、エラー・メッセージが戻されて、アクションは実行されません。指定された `certfile` に X.509 証明書が含まれていない場合や、無効の証明書が含まれている場合も、エラー・メッセージが戻されて、アクションは実行されません。また、指定された `crfile` に無効な CRL が含まれている場合も、エラー・メッセージが戻されて、アクションは実行されません。 `crfile` で指定された CRL が既に CRL ストア内に存在している場合、既存の CRL は上書きされます。
- | **-r** `issuername` によって発行された `serialnumber` と一致する証明書を、ターゲットの `truststore` または `trustpath` から除去します。指定済みの `issuername` および `serialnumber` の証明書が存在しない場合は、エラー・メッセージが戻されて、アクションは実行されません。 `-R` オプションを指定すると、指定済みの `issuername` によって発行された CRL が除去されます。
- | **-l** ターゲットの `truststore` または `trustpath` にある X.509 証明書を表示します。 `issuername` および `serialnumber` を指定すると、一致する証明書のみ表示されます。 `-R` オプションを指定すると、

| CRL ストア内のすべての CRL が表示されます。 **issuename** を **-R** オプション付きで指定すると、その発行者によって発行された CRL が表示されます。

| **-R** 要求された追加、除去、またはリスト操作を、CRL ストアに対して実行するように指示します。

| **-t truststore**
 | ゼロまたは 1 つ以上の X.509 証明書を含むトラストストア名を指定します。

| **-T trustpath**
 | ゼロまたは 1 つ以上の X.509 証明書を含むトラストストアのパスを指定します。

| **-f certfile / crlfile**
 | X.509 証明書または CRL を含む PEM 形式ファイルを指定します。

| **-c certuser**
 | 指定済みの証明書と関連付けられる **username** を指定します。指定される **username** は、ターゲット・システムで有効なシステム・ユーザーである必要があります。

| **-i issuename**
 | 証明書または CRL の発行者名を指定します。

| **-n serialnumber**
 | 証明書のシリアル番号を指定します。

| **-h | --help**
 | コマンドのヘルプ情報を表示する。

| **-v | --version**
 | CIMOM のバージョン番号を表示します。

終了状況

| エラーが発生すると、stderr にエラー・メッセージが書き込まれ、エラー値 1 が戻されます。以下の値が戻されます。

| **0** 成功
 | **1** エラー

例

| **ssltrustmgr -a -t cim_trust -c username -f cert.pem**
 | **cert.pem** ファイル内の X.509 証明書を CIMOM 上のトラストストア **cim_trust** に追加し、ユーザー **username** を証明書と関連付けます。

| **ssltrustmgr -a -T /QIBM/UserData/OS400/CIM/mytruststore -f cert.pem**
 | **cert.pem** ファイル内の X.509 証明書を、トラスト・パス **/QIBM/UserData/OS400/CIM/mytruststore** によって指定されるトラストストアに追加します。トラスト・パスが指定される場合、ユーザーの関連付けは必要ありません。

| **ssltrustmgr -a -R -f class1crl.pem**
 | **ssltrustmgr -aR -f class1crl.pem**
 | これらの例はどちらも **class1crl.pem** 内の CRL を CIMOM 上の証明書取り消しリストに追加します。

| **ssltrustmgr -r -i "/C=US/ST=California/L=Cupertino/O=Smart & Secure/OU=Secure Software Division/CN=dev.admin.ss.com" -n 01**
 | 指定済みの **issuename** および **serialnumber** と一致する証明書を、**cim_trust** トラストストアから除去します。

```
| ssltrustmgr -l -t export_trust
|           export_trust トラストストア内のすべての X.509 証明書をリストします。
|
| ssltrustmgr -l
| ssltrustmgr -l -t cim_trust
|           これらの例はどちらも、cim_trust トラストストア内のすべての X.509 証明書をリストします。
|
| ssltrustmgr -lR -i "/C=US/ST=California/L=Cupertino/O=Smart & Secure/OU=Secure Software
| Division/CN=dev.admin.ss.com"
|           その発行者名で発行された CRL をリストします。
|
| iSeries 固有の使用上の注意: iSeries サーバーでこのコマンドを使用する場合は、*SECADM 権限と
| *ALLOBJ 権限が必要です。
|
|   関連概念
|
|   6 ページの『cimconfig コマンドの拡張開始オプション』
|   cimconfig コマンドを使用して、CIM サーバーの拡張開始オプションを変更することができます。
```

Pegasus 開発者の手引き

CIM 標準には、i5/OS に組み込まれている CIM プロバイダーから提供されるシステム管理データを扱うための管理アプリケーションを開発する機能が用意されています。

CIM を扱うために、開発者は DMTF で定義されている CIM 標準を完全に理解しておくことが必要です。CIM 標準について詳しくは、Distributed Management Task Force (DMTF) Web サイトの「CIM Specification 2.2」を参照してください。

i5/OS 上の Pegasus は、Service Location Protocol (SLP) をサポートしていません。

また、Pegasus には、開発ツール、サンプル、および参照資料も含まれています。

IBM は、基本オペレーティング・システム情報と一部のパフォーマンス・メトリックをサポートするプロバイダーを i5/OS に組み込んでいます。

関連概念

43 ページの『i5/OS メトリック』

i5/OS は、Common Management Model (CMM) をサポートしています。

関連情報

CIM 仕様 2.2 (CIM Specification 2.2)

Pegasus Web サイト

サポートされる CIM 基本オペレーティング・システム・クラス

IBM は、基本オペレーティング・システム情報を提供するために、IBM 提供のプロバイダーとして CIM クラスをインプリメントしました。

IBM から提供されているプロバイダーは以下のとおりです。

- IBMOS400_ComputerSystem: CIM_Computer_System のサブクラス
- IBMOS400_OperatingSystem: CIM_OperatingSystem のサブクラス
- IBMOS400_RunningOS: CIM_RunningOS のサブクラス
- IBMOS400_Process: CIM_Process のサブクラス

- IBMOS400_OSProcess: CIM_OSProcess のサブクラス
- | • IBMOS400_VirtualProcessor: CIM_Processor のサブクラス
- | • IBM_IPProtocolEndpoint: CIM_IPProtocolEndpoint のサブクラス
- | • IBM_LocalFileSystem: CIM_LocalFileSystem のサブクラス
- | • IBM_RemoteFileSystem: CIM_RemoteFileSystem のサブクラス
- | • IBM_NFS: CIM_NFS のサブクラス
- | • IBMOS400_NetworkPort: CIM_NetworkPort のサブクラス
- | • IBM_EthernetPort: CIM_EthernetPort のサブクラス
- | • IBM_TokenRingPort: CIM_TokenRingPort のサブクラス
- | • IBMOS400_CSVirtualProcessor: CIM_SystemDevice のサブクラス
- | • IBM_CSNetworkPort: CIM_SystemDevice のサブクラス
- | • IBMOS400_HostedFileSystem: CIM_HostedFileSystem のサブクラス
- | • IBM_BootOSFromFS: CIM_BootOSFromFS のサブクラス
- | • IBM_NWPortImplementsIPEndpoint: CIM_PortImplementsEndpoint のサブクラス

DMTF 標準に示されているグローバルゼーション・インターフェースに従う CIM クライアントでは、一部のプロパティ値を複数の言語で利用することができます。

以下の図は、IBM 拡張クラスによって拡張された CIM 基本クラスを示しています。

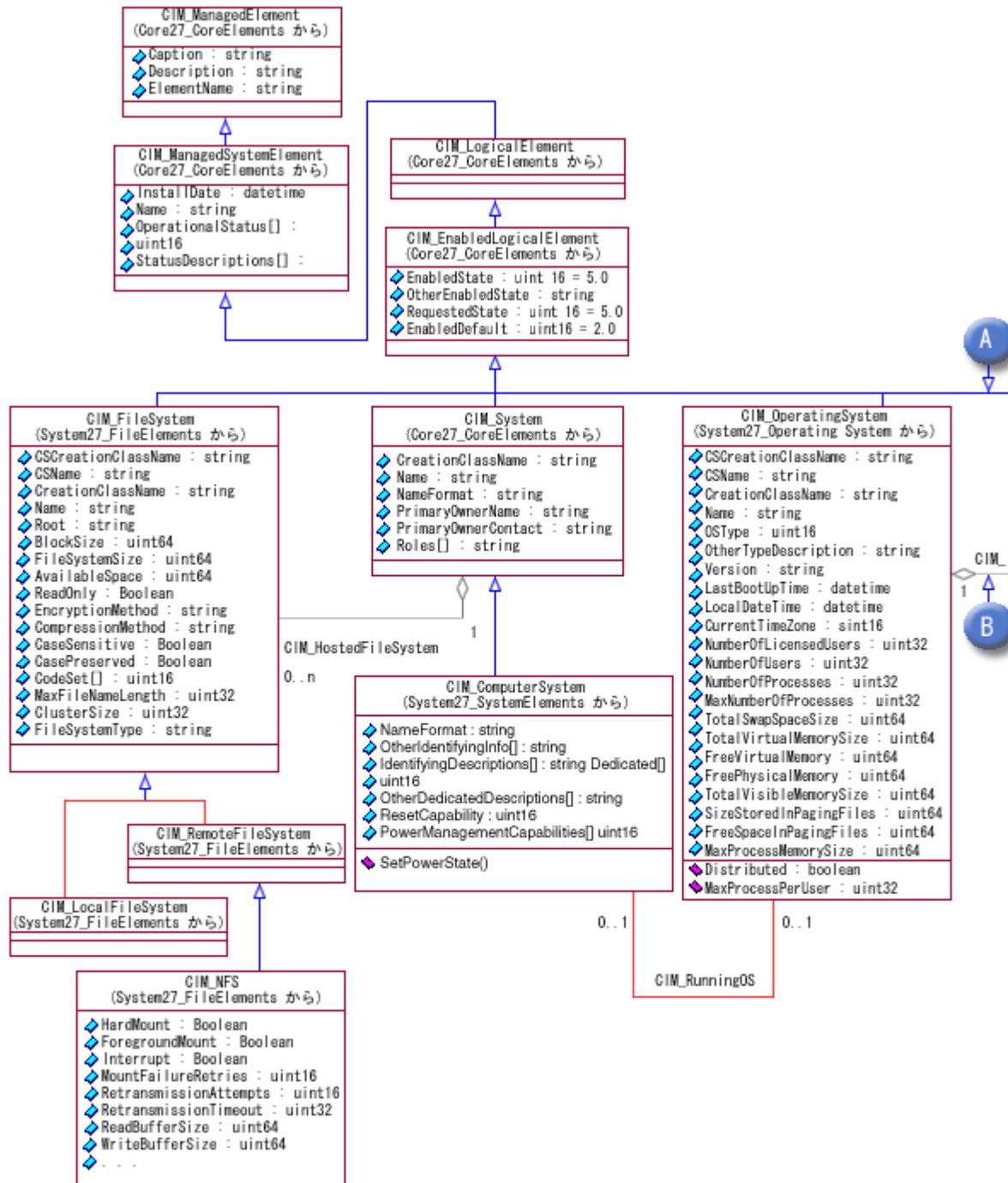


図 1. CIM クラス

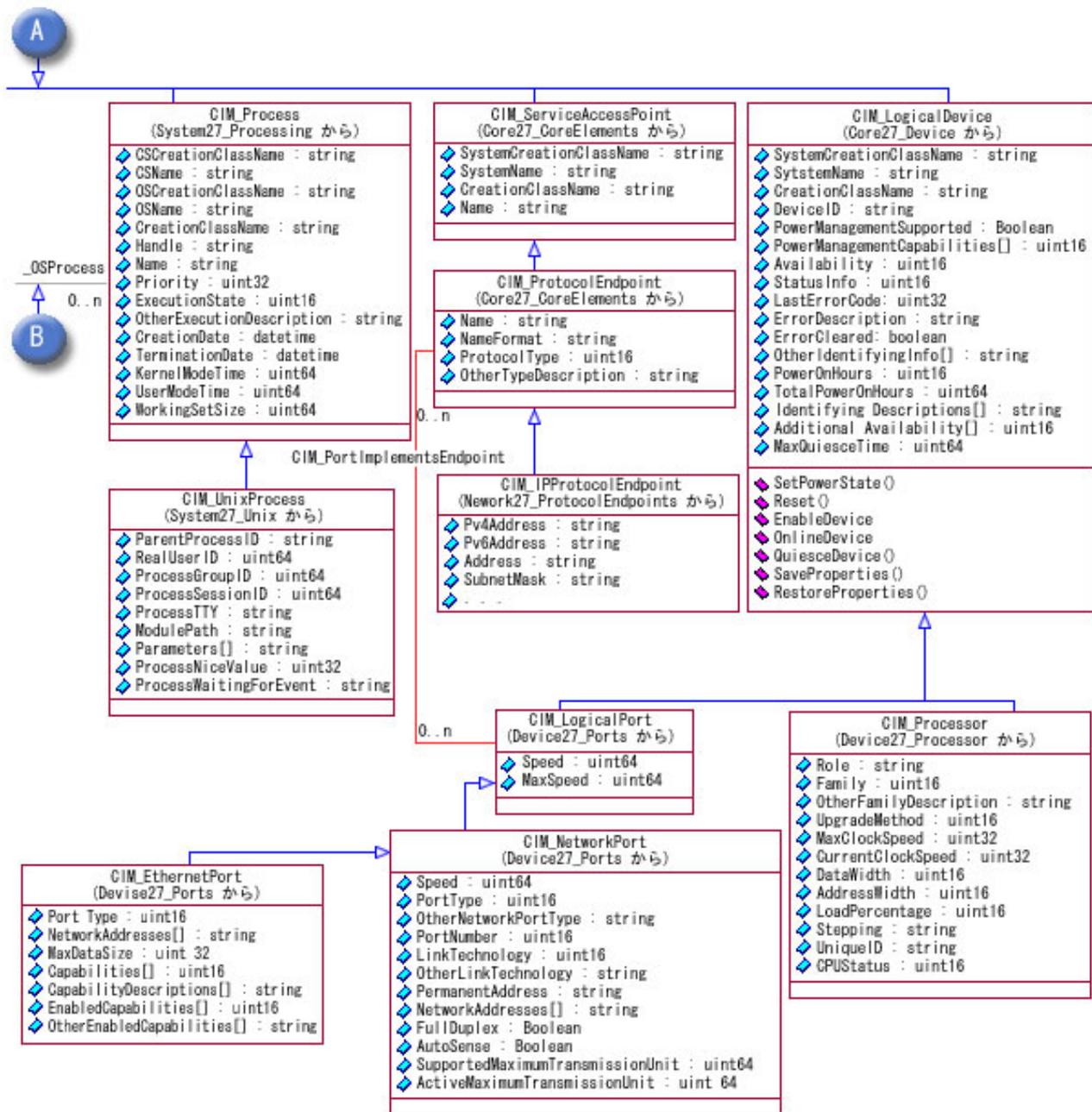


図2. CIM クラス--続き

これらのクラスを定義する管理対象オブジェクト形式 (MOF) ファイルは、/QIBM/ProdData/OS400/CIM/Schemas/OS400/ ディレクトリーにあります。ファイルの名前は以下のとおりです。

- IBMOS400_OSBase.mof
- IBMOS400_BootOSFromFS.mof
- IBMOS400_CSNetworkPort.mof
- IBMOS400_CSVirtualProcessor.mof
- IBMOS400_FileSystem.mof
- IBMOS400_HostedFileSystem.mof

- IBMOS400_NWPortImplementsIPEndpoint.mof
- IBMOS400_NetworkPort.mof
- IBMOS400_ProtocolEndpoints.mof
- IBMOS400_VirtualProcessor.mof

IBMOS400_ComputerSystem

このクラスは、コンピューター名、状況情報などの基本的なコンピューター・システム情報を利用可能にします。このクラスを装備するこのプロバイダーは、実行環境である管理下のシステム（一般にはサーバーまたは装置）の識別の基本知識の一部としてクライアントで用いられます。

次のプロパティのデータは、i5/OS に固有のものである場合と、i5/OS システム固有の属性にマップされる場合があります。

プロパティ	プロパティ値とデータ・ソース
string OtherIdentifyingInfo[]	システムの次のデータを戻す: <ul style="list-style-type: none"> • タイプ • シリアル番号 • モデル • 区画 ID
名前	TCP/IP ホスト・テーブル内の最初のエントリーに基づくシステム名。

注: IBMOS400_ComputerSystem のメソッドはインプリメントされていません。このプロバイダーはメソッド・プロバイダーとして登録されていません。

IBMOS400_OperatingSystem

このクラスは、対応するプロバイダーの実行環境である管理下のシステム（一般的にはサーバーまたは装置）の識別の基本知識の一部としてクライアントで用いられます。

次のプロパティのデータは、i5/OS に固有のものである場合と、i5/OS 固有の属性にマップされる場合があります。

プロパティ	プロパティ値とデータ・ソース
uint32 NumberOfUsers	システム上の対話式ジョブの数
uint32 NumberOfProcesses	システム内に現時点で存在するユーザー・ジョブとシステム・ジョブの総数。総数には、次のジョブが含まれます。 <ul style="list-style-type: none"> • 処理を待機しているジョブ待ち行列内のすべてのジョブ。 • 現在アクティブ (処理中) であるすべてのジョブ。 • 実行を完了したが、まだ生成されていない出力が出力待ち行列にあるすべてのジョブ。
uint32 MaxNumberOfProcesses	システム上の最大許容ジョブ数。
string LanguageEdition	QLANGID システム値を戻す。
string CodeSet (maximum length is 64)	QCHRID システム値からコード・ページ・フィールドを戻す。

プロパティ	プロパティ値とデータ・ソース
uint32 DefaultPageSize (in bytes)	常に 4096 を戻す。

注: IBMOS400_OperatingSystem クラスの Shutdown() メソッドおよび Reboot() メソッドは、V5R4 でインプリメントされました。

IBMOS400_RunningOS

このクラスのこのプロバイダーは、クライアントが、コンピューター・システムと、そのコンピューター・システムで現在実行されているオペレーティング・システムとの間の関連付けを探す場合に用いられます。

IBMOS400_Process

このクラスのプロバイダーは、プロセス名 (i5/OS 上の完全修飾ジョブ名)、優先順位、実行時の状態など、基本的なプロセス情報を利用可能にします。IBMOS400_Process は iSeries サーバー上の i5/OS ジョブにマップされます。クライアント・アプリケーションはこのプロバイダーを使用して、オペレーティング・システムのコンテキスト内で管理下のシステム上で実行されているプロセス (ジョブ) の知識をクライアントに提供します。

注: 所定の i5/OS システム上で実行中か、または待ち行列で待機中の i5/OS ジョブは多数あります (数千個になる場合もあります)。パフォーマンス上の理由から、i5/OS ジョブのリストを取得する必要がある CIM クライアント・アプリケーションは、まず EnumerateInstanceNames を実行してから、インスタンス・データが必要である i5/OS ジョブごとに GetInstance を実行する必要があります。

次のプロパティのデータは、i5/OS に固有のものである場合と、i5/OS 固有の属性にマップされる場合があります。

プロパティ	プロパティ値とデータ・ソース
string ElementName	次の Name フィールドからストリング (コマンド行インターフェースに表示される、i5/OS 上の完全修飾ジョブ名) を戻す。
string Name	コマンド行インターフェースに表示される i5/OS 上の完全修飾ジョブ名: <i>Job number</i> フィールド + / + <i>User name</i> フィールド + / + <i>Job name</i> フィールド。ここで、 <i>Job number</i> はシステム生成のジョブ番号です。 <i>User name</i> はジョブのユーザー名 (ジョブが開始されたときのユーザー・プロファイルの名前と同じ) です。 <i>Job name</i> はシステムで識別されるジョブの名前です。
string Handle [Key]	i5/OS 作業管理 API で使用される i5/OS 上の完全修飾ジョブ名: <i>Job name</i> フィールド + / + <i>User name</i> フィールド + / + <i>job number</i> フィールド。ここで、 <i>Job name</i> はシステムで識別されるジョブの名前です。 <i>User name</i> はジョブのユーザー名 (ジョブが開始されたときのユーザー・プロファイルの名前と同じ) です。 <i>Job number</i> はシステム生成のジョブ番号です。
uint16 ExecutionState	Retrieve Job Information (QUSRJOBI) API、フォーマット JOBI0100、Job status フィールドから取得されるジョブ状況に基づく。 これは i5/OS のアクティブ・ジョブ状況に基づく。i5/OS のアクティブ・ジョブ状況値は、次のように ExecutionState 値にマップされます。

プロパティ	プロパティ値とデータ・ソース
string OtherExecutionDescription	アクティブ・ジョブ状況をストリングとして戻す。アクティブ・ジョブ状況の大半は、説明に完全な文章を必要とするので、CHAR(4)のアクティブ・ジョブ状況そのものが戻されます。
datetime CreationDate	ジョブがシステム上で実行を開始し、ジョブがアクティブになった日時。この情報は、ジョブがアクティブにならなかった場合は利用できません。
datetime TerminationDate	ジョブが終了した日時。システム上で実行されていたジョブが完了したとき。ジョブが完了しなかった場合は、ゼロが戻されます。
uint64 KernelModeTime (in milliseconds)	実行に費やされたシステム時間。i5/OS はシステム時間とユーザー時間を区別しないため、この値を報告することはできません。0 (ゼロ) は、情報を利用できないことを示します。
uint64 UserModeTime (in milliseconds)	実行に費やされたユーザー時間。i5/OS はシステム時間とユーザー時間を区別しないため、この値は、ジョブに使用された処理装置時間 (ミリ秒単位) を反映します。この情報はアクティブなジョブの場合のみ利用できます。

IBMOS400_OSProcess

このクラスのプロバイダーは、オペレーティング・システムと、そのオペレーティング・システムのコンテキスト内で実行されているプロセスとの間のリンクを提供します。クライアント・アプリケーションはこのプロバイダーを使用して、オペレーティング・システムのコンテキスト内で管理下のシステム上で実行されているプロセス (ジョブ) の知識をクライアントに提供します。

IBMOS400_VirtualProcessor

このクラスのプロバイダーは、パーティションの内部仮想プロセッサを表す内部ハイパーバイザー配列エレメントをモデリングします。

注: アクティブなプロセッサのみが戻されます。

プロパティ	プロパティ値とデータ・ソース
string DeviceID [Key]	ハイパーバイザーの内部配列へのインデックスを表す数値。この数値は、ストリングに変換されます。
uint16 OperationalStatus[] (ValueMap)	エレメントの現行状況。常に 2 (OK) を戻します。

IBM_IPProtocolEndpoint properties

IBM_IPProtocol エンドポイントは、i5/OS iSeries システム上の TCP インターフェースにマップされます。

プロパティ	プロパティ値とデータ・ソース
string Description	IP アドレスおよび関連する回線記述。例えば、i5/OS IP プロトコル・エンドポイントの名前は 1.2.3.4 で、関連する回線記述は TRNLINE などです。
string ElementName	TCP インターフェースの IP アドレス。例えば、1.2.3.4。

IBM_LocalFileSystem、IBM_RemoteFileSystem、IBM_NFS プロパティ

IBM_LocalFileSystem クラスは、i5/OS 上の Root、QOpenSys、QDLS、QSYSLIB、UDFS、Optical、および IASP QSYSLIB ローカル・ファイル・システムをモデリングします。IBM_RemoteFileSystem クラスは、i5/OS の QFileServer400、Netware、および QNTC リモート・ファイル・システムをモデリングします。

IBM_NFS クラスは、i5/OS の NFS ファイル・システムをモデリングします。

プロパティ	プロパティ値とデータ・ソース
string ElementName	ファイル・システムのルートを定義するパス名またはその他の情報。
string Name	コンピューター・システム内のファイル・システム・インスタンスのキー。
string Root	ファイル・システムのルートを定義するパス名またはその他の情報。

IBMOS400_NetworkPort、IBM_EthernetPort、および IBM_TokenRingPort プロパティ

IBM_EthernetPort プロパティは、i5/OS のイーサネット回線記述をモデリングします。

IBM_TokenRingPort プロパティは、i5/OS のトークンリング回線記述をモデリングします。

IBMOS400_NetworkPort プロパティは、他のすべての回線記述タイプをモデリングします。

プロパティ	プロパティ値とデータ・ソース
string Description	回線記述の名前およびタイプ。
string ElementName	回線記述の名前。

IBMOS400_CSVirtualProcessor

IBMOS400_CSVirtualProcessor は、パーティション仮想プロセッサをコンピューター・システムと関連付けるアソシエーション・クラスです。

プロパティ	プロパティ値とデータ・ソース
IBMOS400_ComputerSystem REF GroupComponent	アソシエーション内の親コンピューター・システム。 IBMOS400_ComputerSystem クラスへの参照を戻します。
IBMOS400_VirtualProcessor REF PartComponent	コンピューター・システムのコンポーネントである仮想プロセッサ。この特定の仮想プロセッサを表す IBMOS400_VirtualProcessor クラスへの参照を戻します。

IBM_CSNetworkPort

IBM_CSNetworkPort は、ネットワーク・ポートをコンピューター・システムと関連付けるアソシエーション・クラスです。

プロパティ	プロパティ値とデータ・ソース
IBMOS400_ComputerSystem REF GroupComponent	IBMOS400_ComputerSystemIBM クラスへの参照を戻すアソシエーション内の親コンピューター・システム。 IBMOS400_ComputerSystem クラスへの参照を戻します。
CIM_NetworkPort REF PartComponent	コンピューター・システムのコンポーネントであるネットワーク・ポート。この特定のネットワーク・ポートを表す CIM_NetworkPort クラスへの参照を戻します。

IBMOS400_HostedFileSystem

IBMOS400_HostedFileSystem アソシエーション・クラスは、ファイル・システムをコンピューター・システムと関連付けます。

プロパティ	プロパティ値とデータ・ソース
IBMOS400_ComputerSystem REF GroupComponent	アソシエーション内の親コンピューター・システム。 IBMOS400_ComputerSystem クラスへの参照を戻します。
CIM_FileSystem REF PartComponent	コンピューター・システムのコンポーネントであるファイル・システム。 この特定のファイル・システムを表す CIM_FileSystem クラスへの参照を戻します。

IBM_BootOSFromFS

IBM_BootOSFromFS アソシエーション・クラスは、ファイル・システムをオペレーティング・システムと関連付けます。

プロパティ	プロパティ値とデータ・ソース
CIM_FileSystem REF Antecedent	オペレーティング・システムのロード元のファイル・システム。 CIM_FileSystem クラスへの参照を戻します。
IBMOS400_OperatingSystemREF Dependent	オペレーティング・システム。IBMOS400_OperatingSystem クラスへの参照を戻します。

IBMOS400_NWPortImplementsIPEndpoint

IBMOS400_NWPortImplementsIPEndpoint アソシエーション・クラスは、論理ポートをプロトコル・エンドポイントと関連付けます。

プロパティ	プロパティ値とデータ・ソース
CIM_NetworkPort REF Antecedent	IP プロトコル・エンドポイントの先にあるデバイスを表すネットワーク・ポート。CIM_NetworkPort クラスへの参照を戻します。
IBM_IPProtocolEndpoint REF Dependent	論理ポートにインプリメントされている IPProtocolEndpoint。 IBM_IPProtocolEndpoint クラスへの参照を戻します。

サポートされる CIM メトリック・クラス

パフォーマンス情報を提供する IBM 提供のプロバイダーとしてインプリメントされている CIM クラスは、次のとおりです。

- IBMOS400_ColSrvMetricDefinition: CIM_BaseMetricDefinition のサブクラス
- IBMOS400_ColSrvMetricValue: CIM_BaseMetricValue のサブクラス
- IBMOS400_ColSrvMetricInstance: CIM_MetricInstance のサブクラス - メトリック定義とメトリック値のクラスまたはインスタンスとの間の関連付け
- IBMOS400_ColSrvMetricDefForME: CIM_MetricDefForME のサブクラス - 管理下のエレメント (リソース) とメトリック定義のクラスまたはインスタンスとの間の関連付け
- IBMOS400_ColSrvMetricForME: CIM_MetricForME のサブクラス - 管理下のエレメント (リソース) とメトリック値のクラスまたはインスタンスとの間の関連付け

注: IBMOS400_ColSrvMetricValue のすべてのインスタンスは揮発性データを戻します。現行のデータのみサポートされます。履歴データはこのリリースではサポートされません。

i5/OS でサポートされるメトリックのリストについては、i5/OS のメトリックを参照してください。また、CIM クラスおよびインスタンスの MOF ファイルも参照してください。クラスの MOF ファイル

IBMOS400_ColSrvMetric.mof、およびインスタンスの MOF ファイル
 IBMOS400_ColSrvMetricDefInstance.mof は、/QIBM/ProdData/OS400/CIM/Schemas/OS400/ にあります。

次の図に、IBM 拡張クラスと、それらが拡張する CIM 基本クラスとの関係を示します。

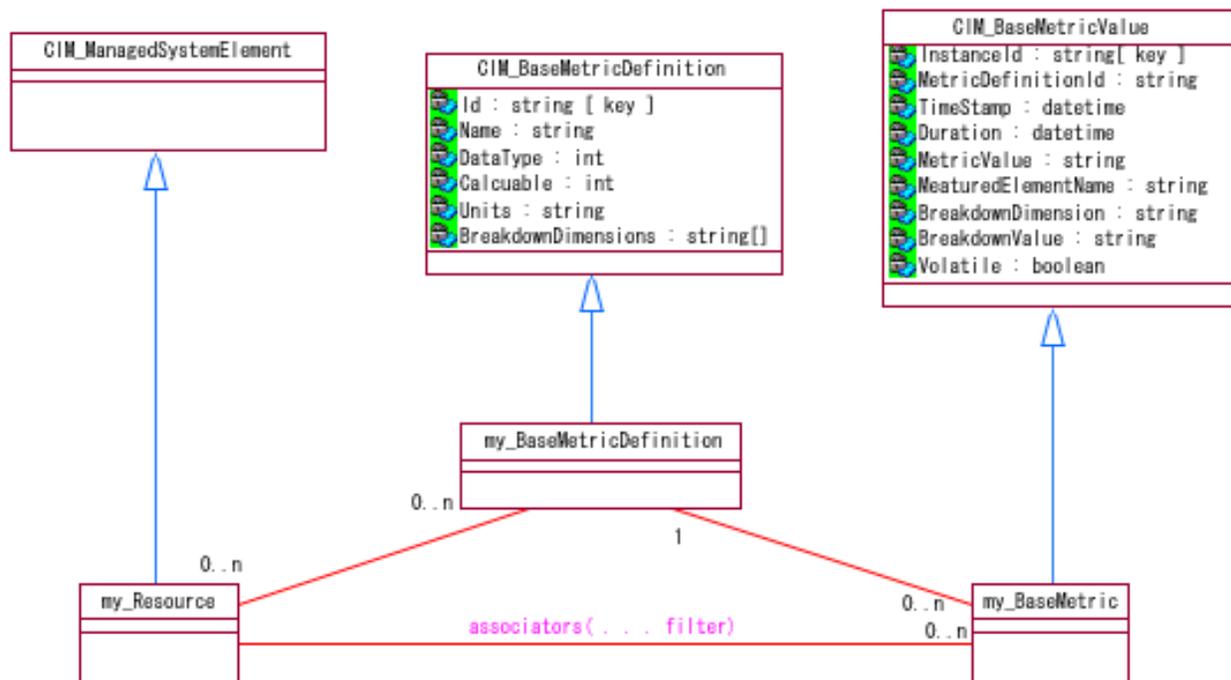


図3. i5/OS メトリック・クラスによって拡張されている CIM クラス

i5/OS メトリック

i5/OS は、Common Management Model (CMM) をサポートしています。

表 1 は、i5/OS がサポートする CMM メトリックについて説明しています。

表 1.

リソース/基本 CIM クラス	メトリック
IBMOS400_OperatingSystem	<p>NumberOfUsers サンプル・インターバルの間にアクティブとなる対話式ジョブの数</p> <p>NumberOfProcesses サンプル・インターバルの間にアクティブとなるジョブの数</p> <p>FreeVirtualMemory システム Auxiliary Storage Pool (ASP) におけるフリー・スペース</p> <p>FreePhysicalMemory i5/OS は常に 0 を返す</p> <p>FreeSpaceInPagingFiles システム ASP におけるフリー・スペース</p> <p>PageInRate すべてのプールで 1 秒間にページングされるページの数</p> <p>OperationalStatus i5/OS は常に OK を返す</p> <p>UserModeTime 使用された合計システム CPU 時間</p> <p>KernelModeTime i5/OS は常に 0 を返す</p> <p>TotalCPUTime UserModeTime と同じ</p> <p>内部から見たカーネル・モードの比率 i5/OS は常に 0 を返す</p> <p>InternalViewUserModePercentage i5/OS は常に 0 を返す</p> <p>InternalViewTotalCPUPercentage オペレーティング・システムから見たユーザー・モードの比率</p> <p>InternalViewIdlePercentage オペレーティング・システムから見たアイドルの比率</p> <p>CPUConsumptionIndex このオペレーティング・システムによって使用された可能性のある CPU 時間で除算した、使用された CPU 時間</p> <p>ExternalViewTotalCPUPercentage 外部から見た CPU 比率</p> <p>ExternalViewUserModePercentage 外部から見たユーザー・モードの比率</p> <p>ExternalViewKernelModePercentage i5/OS は常に 0 を返す</p>

表 1. (続き)

リソース/基本 CIM クラス	メトリック
IBMOS400_ComputerSystem	<p>PctPartitionDefinedCapacityUsed 使用されたシステム CPU 時間を構成済み容量の比率として表す (使用する CPU 論理区画の容量が構成される)</p> <p>ActiveVirtualProcessors アクティブな仮想プロセッサの平均数</p> <p>UnusedPartitionCPUCapacity この OS コンテナに対して予約済みだが未使用の容量</p> <p>UnusedGlobalCPUCapacity グローバル・サーバー・レベルで使用されていない CPU 時間 (ミリ秒)</p>
IBMOS400_Process	<p>KernelModeTime i5/OS は常に 0 を返す</p> <p>UserModeTime JOB で使用された CPU 時間 (すべての 2 次スレッドを含む)</p> <p>TotalCPUTime UserModeTime と同じ</p> <p>InternalViewKernelModePercentage i5/OS は常に 0 を返す</p> <p>InternalViewUserModePercentage UserModeTime に関連する比率値。測定のインターバルに、このプロセスのためにユーザー・モードで使用されたシステム CPU の比率。</p> <p>InternalViewTotalCPUPercentage TotalCPUTime に関連する比率値</p> <p>ExternalViewTotalCPUPercentage 外部から見た CPU 比率の合計</p> <p>ExternalViewUserModePercentage 外部から見たユーザー・モードの比率</p> <p>ExternalViewKernelModePercentage i5/OS は常に 0 を返す</p> <p>AccumulatedKernelModeTime i5/OS は常に 0 を返す</p> <p>AccumulatedUserModeTime プロセスの作成以降にこのプロセスのためにユーザー・モードで費やされた CPU 時間</p> <p>AccumulatedTotalCPUTime プロセスの作成以降にこのプロセスのために費やされた CPU 時間</p>
IBMOS400_Processor	<p>TotalCPUTimePercentage 仮想プロセッサが使用された時間を経過間隔時間の比率として表す</p>

表 1. (続き)

リソース/基本 CIM クラス	メトリック
IBMOS400_NetworkPort	BytesTransmitted 送信されたバイトの合計数 (フレーム文字を含む) BytesReceived 受信されたバイトの合計数 (フレーム文字を含む) ErrorRate ネットワーク・エラー数/秒

関連概念

33 ページの『Pegasus 開発者の手引き』

CIM 標準には、i5/OS に組み込まれている CIM プロバイダーから提供されるシステム管理データを扱うための管理アプリケーションを開発する機能が用意されています。

CIM 指示プロバイダーに対する i5/OS サポート

CIM メトリック指示プロバイダーを使用して、特定のメトリック・イベントの発生時に、アプリケーションに通知することができます。

CIM 指示プロバイダーは、そのプロバイダーが監視するサーバーで、指定されたメトリック・データが発生したときに、ユーザー・アプリケーションに通知します。各アプリケーションは、データが欲しいイベントに関する情報を照会形式で提供することで、プロバイダーをサブスクライブする必要があります。イベントとは、意味のある現象のオカレンスです。イベントの例には、認証障害、ディスク書き込みエラー、またはマウス・クリックなどのオカレンスがあります。プロバイダーは、イベントが発生するとアプリケーションに通知します。そのようなオカレンスを指示と言います。メトリックとクライアントがサブミットした照会が一致すると、指示プロバイダーは指示を作成し、クライアントに戻します。

重要: メトリック指示プロバイダーは、InstanceId プロパティまたは MetricDefinitionId プロパティのいずれかでフィルタリングする照会のみ受け入れます。プロバイダーは、空のフィルターや、上記の 2 つのプロパティ以外のプロパティのみを提供するフィルターはリジェクトします。

QYCP_ColSrvMetricIndicationProvider C++ クラスは、メトリック指示の処理に関連するメイン・クラスです。指示プロバイダーは、以下のメソッドを定義します。

CIM プロバイダーのタイプおよび操作	説明
enableIndications	プロバイダーによる指示の生成の開始が予想されるときに呼び出されます。
createSubscription	プロバイダーに、指定されたサブスクリプションと一致する指示をモニターするように告げます。
modifySubscription	プロバイダーに、指定されたサブスクリプションが変更されたことを知らせます。
deleteSubscription	プロバイダーに、指定されたサブスクリプションと一致する指示のモニターを停止するように告げます。
disableIndications	プロバイダーに、これ以上指示を生成しないように告げます。

関連情報

Open Group CIMIndicationProvider 資料

CIM の関連情報

ここでは、Common Information Model のトピックに関連する Web サイトおよび Information Center トピックをリストします。

Web サイト

- WBEM Web サイト (<http://www.dmtf.org/standards/wbem>)

Web-Based Enterprise Management (WBEM) イニシアチブの公式サイトです。

- Introduction to CIM (<http://www.wbemsolutions.com/tutorials/CIM/cim.html>)

このサイトには CIM のチュートリアルがあります。

- Pegasus Web サイト (<http://www.openpegasus.org>)

OpenPegasus のホーム・ページです。

- OpenSSL 資料 (<http://www.openpegasus.org>)

このサイトには OpenSSL の資料があります。

その他の情報

- 『ネットワーク認証サービス』のトピック
- 『ホスト名解決の考慮事項』のトピック
- 『keytab ファイルを管理する』のトピック
- 『サーバーのバックアップ』のトピック
- 『デジタル証明書マネージャー』のトピック
- IBM Systems Software Information Center の CIM トピック

PDF ファイルの保存

表示用または印刷用の PDF ファイルをワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を右クリックする (上記のリンクを右クリックする)。
2. PDF をローカルで保存するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「保存」をクリックする。

Adobe Reader のダウンロード

1. PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。
1. これは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から無料でダウンロードすることができます。
1. とができます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとしします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

- | 本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム
- | 契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項
- | に基づいて、IBM より提供されます。

本書の一部は Web サイト openpegasus.org から引用しました。

Copyright (c) 2000, 2001, 2002 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; The Open Group; Tivoli Systems. Copyright (c) 2003 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; EMC Corporation; The Open Group. Copyright (c) 2004 BMC Software; Hewlett-Packard Development Company, L. P.; IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group. Copyright (c) 2005 Hewlett-Packard Development Company, L.P.; IBM Corp. EMC Corporation; VERITAS Software Corporation; The Open Group.

このソフトウェアの複製物およびその関連文書ファイル

(以下「ソフトウェア」といいます) を取得する何人にも、以下の条件で、この「ソフトウェア」を、使用、複製、改変、結合、出版、配布、再使用許諾し、また「ソフトウェア」の複製物を販売する権利、ならびに「ソフトウェア」の提供を受けた者にこれらの行為を許諾する権利を含め (これらに限りません)、「ソフトウェア」を制約なく取引する権利を無償で付与します。

上記の著作権表示および本許諾通知が、すべてのこの「ソフトウェア」の複製物または主要な部分に含まれていなければなりません。ソフトウェアは、特定物として現存するままの状態を提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含む、すべての明示もしくは黙示の保証責任または保証条件を負わないものとします。

かかるソフトウェアの作成者または著作権者は、債務不履行、不法行為その他請求原因を問わず、そのソフトウェアの使用、その他取扱い起因または関連する、請求、損害賠償その他のいかなる責任についても、何等責任を負わないものとします。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確認できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

プログラミング・インターフェース情報

この「Common Information Model (CIM)」資料には、プログラムを作成するユーザーが CIM のサービスを使用するためのプログラミング・インターフェースが記述されています。

商標

以下は、IBM Corporation の商標です。

- | i5/OS
- | IBM
- | IBM ロゴ
- | iSeries

他の会社名、製品名およびサービス名などはそれぞれ各社の商標または登録商標です。

資料に関するご使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態を提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。



Printed in Japan