Systemwalker Service Quality Coordinator

使用手引書

Windows/Solaris/Linux

J2X1-6820-02Z0(01)
2010年8月

まえがき

■本書の目的

本書では、Systemwalker Service Quality Coordinatorの管理機能について説明しています。

ミドルウェア連携や、しきい値の設定、Browser Agentのパッケージの作成およびインストールの方法など、応用的な内容を説明しています。

■本書の読者

本書は、Systemwalker Service Quality Coordinatorを管理機能の設定および操作する方を対象としています。

また、本書を読む場合、OSやGUIの一般的な操作、およびTCP/IPやSMTPなどの一般的な知識をご理解の上でお読みください。

■本製品のマニュアル体系

Systemwalker Service Quality Coordinator のマニュアル構成は以下です。

- Systemwalker Service Quality Coordinator 解説書

  機能の概要について説明しています。

- Systemwalker Service Quality Coordinator 導入手引書

  インストール、セットアップについて説明しています。

- Systemwalker Service Quality Coordinator 使用手引書

  機能の使用方法について説明しています。

- Systemwalker Service Quality Coordinator 使用手引書(コンソール編)

  機能の使用方法のうち、画面の使用に関する説明をしています。

- Systemwalker Service Quality Coordinator 使用手引書(ダッシュボード編)

  ダッシュボード機能の使用方法を説明しています。

- Systemwalker Service Quality Coordinator リファレンスマニュアル

  コマンド、データフォーマット、メッセージ等について説明しています。

- Systemwalker Service Quality Coordinator トラブルシューティングガイド

  トラブルの対処方法について説明しています。

- Systemwalker Service Quality Coordinator Web利用状況管理編

  本製品の提供する機能のうち、Web 利用状況分析機能、Web コンテンツの改ざん監視機能について説明しています。

■本書の構成

- 第1章 他製品との連携

  Systemwalker Service Quality Coordinatorと他製品との連携についての、設定手順を説明しています。

- 第2章 収集テンプレート

  性能情報を取得するためにテンプレート上で行う定義設定について説明しています。

- 第3章 インストールレス型Agent管理

  Agentをインストールしていない被監視サーバをリモートで管理する方法について説明しています。

- 第4章 エンドユーザレスポンス管理

  エンドユーザレスポンス測定の概要、環境設定、Browser Agentのパッケージの作成およびインストールの方法、について説明しています。

- 第5章 サービス稼働管理

  サービス稼働管理の概要および環境設定について説明しています。

- 第6章 レスポンス・稼働管理対象構成情報(ServiceConf.xml)

  ServiceConf.xmlの編集方法やBodyファイルの作成方法について説明しています。

- 第7章 しきい値監視

  しきい値監視しきい値を定義する方法や、管理者に知らせるためのアクションの種類について説明しています。

- 第8章 Webトランザクション量管理

  Webトランザクション量を管理する手順を説明しています。

- 第9章 ユーザデータ管理

  業務データやシステム稼働データなどユーザーの固有データを管理する方法について説明します。

- 第10章 ポリシー配付

  ポリシー配付機能の運用方法について説明しています。

- 第11章 バックアップ/リストア

  Systemwalker Service Quality Coordinatorの運用環境のバックアップとリストアの方法を説明しています。

- 第12章 エコ情報管理

  監視対象となるITシステムの消費電力や温度を可視化し、現状を把握する方法を説明しています。

- 付録A セットアップコマンド、常駐プロセス一覧

  セットアップ時に使用するポリシーコマンドと、起動するプロセスの説明を記載しています。

■本書の位置づけ

本書は、Systemwalker Service Quality Coordinatorの共通マニュアルです。本書は、以下の製品に対応しています。

- Systemwalker Service Quality Coordinator Enterprise Edition V13.4.0 Windows版
- Systemwalker Service Quality Coordinator Standard Edition V13.4.0 Windows版
- Systemwalker Service Quality Coordinator Enterprise Edition V13.4.0 Windows for Itanium版
- Systemwalker Service Quality Coordinator Standard Edition V13.4.0 Windows for Itanium版
- Systemwalker Service Quality Coordinator Enterprise Edition V13.4.0 Linux版
- Systemwalker Service Quality Coordinator Standard Edition V13.4.0 Linux版
- Systemwalker Service Quality Coordinator Enterprise Edition V13.4.0 Linux for Itanium版
- Systemwalker Service Quality Coordinator Standard Edition V13.4.0 Linux for Itanium版
- Systemwalker Service Quality Coordinator Enterprise Edition V13.4.0 Solaris(TM) オペレーティングシステム版
- Systemwalker Service Quality Coordinator Standard Edition V13.4.0 Solaris(TM) オペレーティングシステム版

■略語表記について

- Microsoft(R) Windows NT(R) Server network operating system Version 4.0およびMicrosoft(R) Windows NT(R) Workstation operating system Version 4.0を"Windows NT(R)"と表記します。
- Microsoft(R) Windows(R) 2000 Professional operating system、Microsoft(R) Windows(R) 2000 Server operating systemおよびMicrosoft(R) Windows(R) 2000 Advanced Server operating systemを"Windows(R) 2000"と表記します。
- Microsoft(R) Windows(R) 98 operating systemを"Windows(R) 98"と表記します。
- Microsoft(R) Windows(R) XP Professionalを"Windows(R) XP"と表記します。
- Microsoft(R) Windows Server(R) 2003 Enterprise Edition、Microsoft(R) Windows Server(R) 2003 Standard Edition、Microsoft(R) Windows Server(R) 2003 Web Editionを、"Windows(R) 2003" と表記します。
- Microsoft(R) Windows Server(R) 2008 Enterprise、Microsoft(R) Windows Server(R) 2008 Standardを、"Windows(R) 2008" と表記します。
- Microsoft(R) Windows Vista(R) Ultimate、Microsoft(R) Windows Vista(R) Home Premium、Microsoft(R) Windows Vista(R) Home Basic、Microsoft(R) Windows Vista(R) Business、Microsoft(R) Windows Vista(R) Enterprise を"Windows Vista(R)"と表記します。
- Microsoft(R) Windows(R) 7 Ultimate、Microsoft(R) Windows(R) 7 Professional、Microsoft(R) Windows(R) 7 Home Premium、Microsoft(R) Windows(R) 7 Home Basicを"Windows(R) 7"と表記します。
- Microsoft(R) SQL Server(TM) を、"SQL Server"と表記します。
- Microsoft(R) Cluster Serverを"MSCS"と表記します。
- Solaris(TM) オペレーティングシステムを"Solaris"と表記します。
- Systemwalker Centric Managerを"Centric Manager"と表記します。
- Symfoware Serverを"Symfoware"と表記します。
- Interstage Application Serverを"Interstage"と表記します。
- Oracle Databaseを"Oracle"と表記します。
- Systemwalker Resource Coordinatorを"Resource Coordinator"と表記します。
- Windows上、およびItaniumに対応したWindows上で動作するSystemwalker Service Quality Coordinatorを"Windows版"と表記します。
- Itaniumに対応したWindows上で動作するSystemwalker Service Quality Coordinatorの固有記事を"Windows for Itanium版"と表記します。
- Solarisで動作するSystemwalker Service Quality Coordinatorを"Solaris版"と表記します。
- Linux上、Itaniumに対応したLinux上で動作するSystemwalker Service Quality Coordinatorを"Linux版"と表記します。
- Itaniumに対応したLinux上で動作するSystemwalker Service Quality Coordinatorの固有記事を"Linux for Itanium版"と表記します。
- Solaris版、Linux版およびLinux for Itanium版のSystemwalker Service Quality Coordinatorを包括して、“UNIX版”と表記します。
- Agent for Server/Agent for Businessの共通記事を"Agent"と表記します。

■本書の表記について

- エディションによる固有記事について

  本書では、標準仕様である「Systemwalker Service Quality Coordinator Standard Edition」の記事と区別するため、エディションによる固有記事に対して以下の記号をタイトル、または本文につけています。

  EE Systemwalker Service Quality Coordinator Enterprise Edition固有の記事です。

SE

Systemwalker Service Quality Coordinator Standard Edition固有の記事です。

- Windows版とUNIX版の固有記事について

  本書は、Windows版、UNIX版共通に記事を掲載しています。Windows版のみの記事、UNIX版のみの記事は、以下のように記号をつけて共通の記事と区別しています。

  【Windows版】

  Windows版固有の記事です。

  【UNIX版】

  UNIX版固有の記事です。

  本文中でSolaris/Linux/AIX/HP-UXの記載が分かれる場合は、「**【Solaris版】**」、「**【Linux版】**」、「**【AIX版】**」、「**【HP-UX版】**」のように場合分けして説明しています。

■記号について

コマンドで使用している記号について以下に説明します。

【記述例】

```
[PARA={a |b |c |… }]
```

【記号の意味】

記号	意味
[]	この記号で囲まれた項目を省略できることを示します。
{}	この記号で囲まれた項目の中から、どれか1つを選択することを示します。
__	省略可能記号“[ ]”内の項目をすべて省略したときの省略値が、下線で示された項目であることを示します。
|	この記号を区切りとして並べられた項目の中から、どれか1つを選択することを示します。
…	この記号の直前の項目を繰り返して指定できることを示します。

■商標について

- MS-DOS、Microsoft、Windows、Windowsロゴ、Windows NTは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。
- Sun、Sun Microsystems、Sunロゴ、Java(TM) およびすべてのJava(TM)に関連する商標およびロゴは、米国およびその他の国における米国Sun Microsystems,Inc.の商標または登録商標であり、同社のライセンスを受けて使用しています。
- UNIXは、米国およびその他の国におけるオープン・グループの登録商標です。
- Solaris(TM) オペレーティングシステムおよびすべてのSolaris(TM) オペレーティングシステムに関連する商標およびロゴは、米国およびその他の国における米国Sun Microsystems,Inc.の商標または登録商標であり、同社のライセンスを受けて使用しています。
- Oracleは、米国Oracle Corporationの登録商標です。
- Linuxは、Linus Torvalds氏の米国およびその他の国における商標または登録商標です。

- Red Hat、RPM、および Red Hat をベースとしたすべての商標とロゴは、米国およびその他の国における Red Hat, Inc. の商標または登録商標です。
- Intel、Pentium、およびItaniumは、Intel Corporationの登録商標です。
- Systemwalkerは、富士通株式会社の登録商標です。
- Interstageは、富士通株式会社の登録商標です。
- Symfowareは、富士通株式会社の登録商標です。
- その他、本書に記載の会社名および製品名などは、該当する各社の商標または登録商標です。

■謝辞

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2010年2月

■お願い

- 本書を無断で他に転載しないようお願いします。
- 本書は予告なしに変更されることがあります。

■変更履歴

追加・変更内容	変更箇所	マニュアルコード
機能概要の記事を修正しました。	1.2	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
参考の記事を修正しました。	1.4.5	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
必須ソフトウェアの記事を修正しました。	3.1.1	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
必須ソフトウェアの記事を修正しました。	3.2.1	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
ポイントの記事を追加しました。	5.1	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
サービスの稼働情報の記事を修正しました。	5.3	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
実行環境の注意事項を修正しました。	第7章	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
しきい値監視IDについての注意事項を修正しました。	7.1.1	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
注意事項を追加しました。	10.1.1	J2X1-6820-02Z0(01) J2X1-6820-02Z2(01)
"■本手順を行う前に"の記事を修正しました。	第11章	J2X1-6820-02Z0(01)

追加・変更内容	変更箇所	マニュアルコード
		J2X1-6820-02Z2(01)

目　次

第1章 他製品との連携

本章は、ミドルウェアの性能管理を行う場合に

- 連携対象の確認(導入確認)
- 定義方法(カスタマイズ、セットアップ)
- 表示(表示)

の各手順について説明します。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■本手順を行う前に

ポイント

Enterprise Manager上でミドルウェアの性能管理を行う場合は、サービス/デーモンが正しく停止しているか確認後、「2.4 Enterprise Managerでのミドルウェア連携設定」を参照して、template.datを修正、または修正されていることを確認してください。

以下、ミドルウェアの性能管理の設定について説明します。

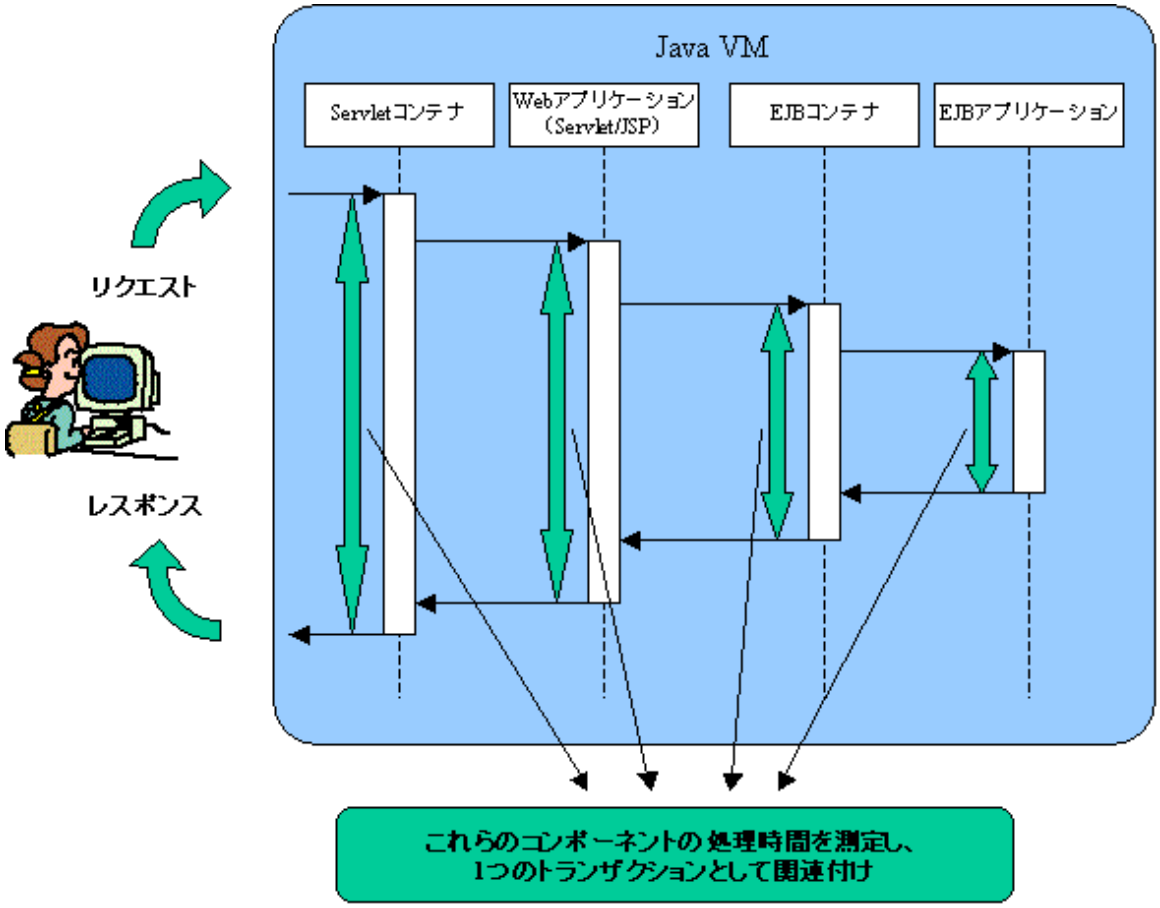
1.1 Interstage Application Serverとの連携

■機能概要

Interstage Application Server上で動作するJavaヒープ量/コネクション状況/処理時間などの業務アプリケーションの性能を、Systemwalker Service Quality Coordinatorで分析することにより、目的に応じたわかりやすいレポートとともにシステムの稼働状況や傾向を把握することができます。

また、IJServerワークユニットを監視する場合は、J2EEアプリケーションのコンポーネント毎の処理時間を測定することが可能になります。

これにより、J2EEアプリケーションのトランザクションの、内訳の性能分析が可能になり、ボトルネックの検出を支援することができます。



参照

詳細についてはInterstage Application Serverのマニュアルを参照してください。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.1.1 導入確認
- 1.1.2 トランザクション内訳分析
- 1.1.3 定義方法
- 1.1.4 セットアップ
- 1.1.5 表示

1.1.1 導入確認

■実行環境

Interstage Application Serverのアプリケーションサーバ機能がインストールされている環境へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Interstage Application Server側での作業

収集ポリシーの作成と適用を行う前に、Interstage Application Server側で以下の準備/確認が必要になります。

注意

本製品では、Interstage Application Serverのマルチシステム機能は未サポートです。

- EJB/TD/CORBAワークユニットの性能管理を行う場合は、性能分析監視環境が作成されていること。(ispstatusコマンド実行時にエラーメッセージが表示されない)

  ※性能分析監視環境の作成についてはInterstage Application Serverのマニュアルを参照してください。

  ※収集間隔は5分間に設定してください。

- 性能分析監視環境が作成されている(ispstatusコマンド実行時にエラーメッセージが表示されない)こと。(EJB/TD/CORBAワークユニットの性能管理を行う場合のみ必要です。IJServerワークユニットの性能管理を行う場合は必要ありません。)

- Interstageの各サービス/デーモンが起動していること。

- IJServerワークユニットの「トランザクション内訳分析」を行う場合は、「1.1.2 トランザクション内訳分析」に記載する設定を行っていること。

1.1.2 トランザクション内訳分析

IJServerワークユニットの「トランザクション内訳分析」を行う場合は、Interstage管理コンソールから以下の設定を行います。

- トランザクション内訳分析を有効にする。

- サンプリング頻度(測定間隔)

トランザクション内訳分析の測定を行う際に、動作する全てのトランザクションを対象に情報収集すると、システムへのオーバヘッドが大きくなるため、一部のデータのみをサンプリングするようになっています。
サンプリングする頻度は、デフォルトでは、1000トランザクションに1回の割合でデータ収集する頻度(0.1%)になっており、この頻度は、Interstage の動作パラメタ「測定間隔」として変更できるようになっています。

通常は、デフォルト値「1000」で運用することを推奨します。トランザクションの発生が少なく、トランザクション内訳分析用のデータが、ほとんど収集できない場合に限って割合を変更して下さい。デフォルト値の1000は、秒間10トランザクションの負荷を想定した値となっています。したがって、デフォルト値を変更する場合は、100秒間に1回程度の割合で情報収集される値を目安に変更してください。

この測定間隔が短すぎる場合は、システムへのオーバヘッドが大きくなります。ある一定以上に負荷がかかった場合(内部で保持するバッファがフルになった場合)は、これ以上負荷がかかることを抑止するために、データ収集を一時的に中断します。結果、トランザクション内訳分析データとしては、一部が欠落した情報になります。この時、通常昇順に採番されるトランザクションIDが、途中欠番がある状態になっていますので、詳細画面で収集データを表示することで確認できます。

トランザクションIDの詳細については、使用手引書（コンソール編）「3.2.3.3 Interstage(TxnAnalysis)ツリー」を参照してください。

トランザクションIDが途中欠番となった状態が確認できましたら、測定間隔が短すぎる状況になっておりますので、設定値を見直してください。

参照

上記の設定方法については、Interstage Application Serverのマニュアルを参照してください。

1.1.3 定義方法

デフォルトの設定状態の場合、IJServerワークユニットで収集可能なレコードは以下になります。

- IS_JMX_JVM
- IS_JMX_JTARESOURCE
- IS_JMX_JDBCRESOURCE

定義手順を実施することにより、以下のレコードの収集が可能になります。

- IS_JMX_SERVLET
- IS_JMX_ENTITYBEAN_METHOD
- IS_JMX_ENTBEAN_POOL_AND_PASSIVATE
- IS_JMX_STFBEAN_METHOD
- IS_JMX_STFBEAN_INS_AND_IDLE
- IS_JMX_STLSBEAN_METHOD
- IS_JMX_MESSBEAN_METHOD
- IS_JMX_MESSBEAN_INFO

ポイント

デフォルトで収集される項目で要件を満たす場合は、以降の手順を実施する必要はありません。

注意

IJServerワークユニット上で動作するアプリケーションによっては、収集ができないレコードがあります。

定義手順を実施することにより収集できるレコード数が増加するため、監視対象数が多い場合など、収集間隔内で収集処理が完了できず、エラーが発生する場合があります。

■IJServerの性能情報収集の拡張手順

template.datを修正します。

■定義場所

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

```
/etc/opt/FJSVssqc/template.dat
```

■修正内容

以下のように、INTSGセクションの「ARMTXN=...」の次の行に「LEVEL=2」を追記してください。

```
########################################
## Interstage ispreport DCA_CMD
[INTSG]
DCAID="INTSGREPO"
AUTOFLAG="ON"
INTERVAL=5
TDOBJ="ON"
EJBAPL="ON"
IMPLID="ON"
IJSERVER="ON"
ARMTXN="ON"
LEVEL=2                    ★この行を追記します。
########################################
```

1.1.4 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

この後にワークユニットの追加/削除など構成を変更した場合は、再度収集ポリシーの作成と適用を実施する必要があります。

また、収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.1.5 表示

トランザクション内訳分析情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「Interstage(EJB)Monitor」ノード、「Interstage(TD)Monitor」ノード、「Interstage(CORBA)Monitor」ノードまたは、「Interstage(IJServer)Monitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「Interstage(TxnAnalysis)」ノード配下に、ワークユニット毎にノードが生成されます。ワークユニットを選択することで、そのワークユニットで実行された全てのトランザクションが表示されます。また、トランザクションIDのノードを設定することにより、1トランザクション毎に参照することも可能です。詳細は、使用手引書(コンソール編)「3.2.3.3 Interstage(TxnAnalysis)ツリー」を参照してください。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.2 Interstage Application Framework Suite/Interstage Business Application Serverとの連携

注意

当機能は、本製品のSolaris版/Linux for Itanium版の環境でのみ利用可能です。

■機能概要

Interstage Application Framework Suite/Interstage Business Application Serverの標準ログから業務アプリケーションの性能を分析することにより、目的に応じたわかりやすいレポートでシステムの稼働状況や傾向を把握することができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.2.1 導入確認
- 1.2.2 トランザクション内訳分析
- 1.2.3 定義方法
- 1.2.4 セットアップ
- 1.2.5 表示

1.2.1 導入確認

■実行環境

本製品の AgentをInterstage Application Framework Suite/Interstage Business Application Server のサーバへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Interstage Application Framework Suite/Interstage Business Application Server側での作業

収集ポリシーの作成と適用を行う前に、Interstage Application Framework Suite/Interstage Business Application Server側で以下の準備/確認が必要になります。詳細は、「1.2.2 とトランザクション内訳分析」を参照してください。

1. Interstage Application Framework Suite/Interstage Business Application Server の標準ログが設定されていること。

ポイント

ログの出力レベルについては以下のように設定しておく必要があります。

ー 同期トランザクションの場合
ログレベル 3以上

ー 非同期トランザクションの場合
ログレベル10以上

当機能では、標準ログとして出力されるログのうち、性能ログを分析対象とします。

参照

Interstage のログ出力定義の詳細については、Mccoordinator ユーザーズガイド、Interstage Business Application Server アプリケーション開発ガイド、Interstage Business Application Server 運用ガイド（アプリケーション連携実行基盤編）を参照してください。

2. Interstage Application Framework Suite/Interstage Business Application Server の各サービス/デーモンが起動していること。

参考

詳細については、Interstage Application Server 運用ガイド、Interstage Application Server リファレンスマニュアル(コマンド編) または Interstage Business Application Server運用ガイド(アプリケーション連携実行基盤編) を参照してください。

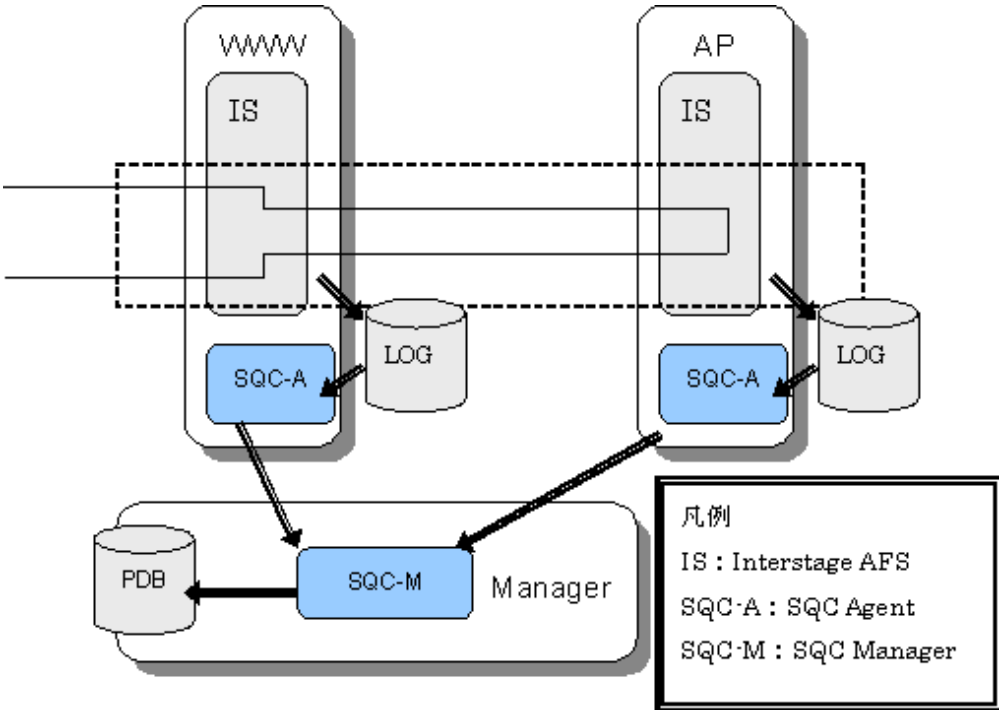
1.2.2 トランザクション内訳分析

トランザクション内訳分析機能は、複数および単一サーバを使用して動作する Interstage Application Framework Suite/ Interstage Business Application Server の業務アプリケーションの標準ログファイルから、動作性能を分析します。これにより、トランザクションの実行状況を可視化して性能問題発生時に問題箇所の特定を容易にします。

また、サマリ機能により、実行される業務アプリケーションの実行数や実行時間の状況を監視し、システム設計段階でのキャパシティプランニングを支えます。

参照

詳細については、Interstage Application Framework Suite/Interstage Business Application Server のマニュアルを参照してください。



1.2.3 定義方法

以下の定義ファイルを用意します。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Solaris版/Linux for Itanium版】

```
/opt/FJSVssqc/control/tda.ini
```

■形式

```
[ISLog]
TYPE = AFS | BAS
APLOGFILE = aplog-file
MULTIASYNCLOGFILE = multi-asynclog-file
JAVAASYNCLOGDIR = java-asynclog-dir
MCLOGDIR = mclog-dir
APLOGFORMAT = "aplog-format"
MULTIASYNCLOGFORMAT = "multi-asynclog-format"
JAVAASYNCLOGFORMAT = "java-asynclog-format"
MCLOGFORMAT = "mclog-format"
SAMPLING_RATIO = sample-ratio
```

TIMEZONE = timezone

MAXNAMELENGTH = max-name-length

LANGUAGE = ASCII | EUCJP | SJIS | UTF8

ポイント

- 空行は、コメントとして扱われます。
- '#'で始まる行は、コメントとして扱われます。
- セクション名（ISLog）およびエントリー名（TYPE、APLOGFILE、...等）は、大文字・小文字の区別はしません。

■説明

[ISLog]

Interstage ログ関連パラメタの設定を行うセクションを示します。

TYPE = AFS | BAS

Interstage の種別の定義です。選択肢の意味は以下のとおりです。

選択肢	意味
AFS	Interstage Application Framework Suite
BAS	Interstage Business Application Server

デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

TYPE=BAS

APLOGFILE = aplog-file

分析対象ログファイルのパスを定義します。
aplog-file には、Interstage の同期アプリケーション実行基盤によって、COBOLまたはC言語のアプリケーションを利用した場合（フレームワークApcoordinator）に出力される標準ログファイルのパスを指定します。

MULTIASYNCLOGFILE = multi-asynclog-file

分析対象ログファイルのパスを定義します。
multi-asynclog-file には、Interstage の非同期アプリケーション実行基盤によって、COBOLまたはC言語のアプリケーションを利用した場合に出力される標準ログファイルのパスを指定します。

JAVAASYNCLOGDIR = java-asynclog-dir

分析対象ログファイルの出力先ディレクトリを定義します。
java-asynclog-dir には、非同期アプリケーション実行基盤で、Javaのアプリケーションを利用した場合に出力されるログファイルについて、IJServer のログ出力ディレクトリ（IJServer 名まで）のパスを指定します。指定されたディレクトリ配下の全ての標準ログファイルが解析されます。複数の IJServer を解析する場合、JAVAASYNCLOGDIR文を複数指定します。

注意

複数のJAVAASYNCLOGDIR文を指定する場合、各分析対象ログファイルのログ記録形式が同じである必要があります。ログ記録形式は後述のJAVAASYNCLOGFORMAT文で指定します。

MCLOGDIR = mclog-dir

分析対象ログファイルの出力先ディレクトリを定義します。
mclog-dir には、Interstage のフレームワークの一つ Mccoordinator で出力されるログファイルについて、解析対象

IJServer のログ出力ディレクトリ（IJServer 名まで）のパスを指定します。指定されたディレクトリ配下の全ての標準ログファイルが解析されます。複数の IJServer を解析する場合、MCLOGDIR文を複数指定します。

注意

複数のMCLOGDIR文を指定する場合、各分析対象ログファイルのログ記録形式が同じである必要があります。ログ記録形式は後述のMCLOGFORMAT文で指定します。

APLOGFORMAT = "aplog-format"

APLOGFILE文で指定された分析対象ログファイルのログ記録形式を定義します。
aplog-format にデータに対応したトークンを実際のログと同じ順番、同じ区切りとなるように指定します。ダブルクォーテーションで括って指定します。トークンの種類と意味は、以下のとおりです。

トークン	意味	必須
context-id	コンテキストID	○
type	ログ種別	○
trigger	ログの採取契機	○
msgid	メッセージID	○
business	業務名	○
appl	アプリケーション名	○
start{time-format}	開始時刻	○
end{time-format}	出力時刻	○
elapse	経過時刻	○
*	上記以外の可変要素	

time-format には、時刻の形式に対応したトークンの指定をする必要があります。トークンは、以下のとおりです。

トークン	意味	必須
yyyy	西暦年（1980～2038）	○
mm	月（01～12）	○
dd	日（01～31）	○
HH	時（00～23）	○
MM	分（00～59）	○
SS	秒（00～59）	○
sss	ミリ秒（000～999）	○

トークン対して出力される文字数の幅が予め分かっている場合（固定幅）、その幅を指定できます。以下の形式で指定します。

token{fixedwidthDDD}

token はトークンを示します。DDD は0～999 までの10進数で、トークンの幅（単位 バイト）を示します。

■例

24バイトの任意文字

```
*{fixedwidth24}
```

MULTIASYNCLOGFORMAT = "multi-asynclog-format"

MULTIASYNCLOGFILE文で指定された分析対象ログファイルのログ記録形式を定義します。
APLOGFORMAT文 と同様にして、multi-async-logformat ログ形式を指定します。トークンの種類と意味は、以下のとおりです。

トークン	意味	必須
context-id	コンテキストID	○
type	ログ種別	○
trigger	ログの採取契機	○
msgid	メッセージID	○
destque	アクティビティのキューDestination名	○
flow	フロー定義名	○
appl	アプリケーション名	○
start{time-format}	開始時刻	○
end{time-format}	出力時刻	○
elapse	経過時刻	○
*	上記以外の可変要素	

time-format には、時刻の形式に対応したトークンの指定をする必要があります。前述のAPLOGFORMAT文のtime-formatと同じトークンを使って指定します。

ポイント

- 非同期トランザクションの場合は、コンテキストID にコリレーションID が出力されます。標準ログのログ記録形式については、Interstage Business Application Server 運用ガイド(アプリケーション連携実行基盤編)を参照してください。
- トークン対して出力される文字数の幅が予め分かっている場合(固定幅)、その幅を指定できます。指定方法は前述のAPLOGFORMAT文と同じです。

JAVAASYNCLOGFORMAT = "java-asynclog-format"

JAVAASYNCLOGDIR文で指定された分析対象ログファイルのログ記録形式を定義します。
前述のMULTIASYNCLOGFORMATと同じ方法で指定します。

MCLOGFORMAT = "mclog-format"

MCLOGDIR文で指定された分析対象ログファイルのログ記録形式を定義します。
mclog-format には、以下のトークンを使用します。フォーマットの指定方法はAPLOGFORMAT と同様です。トークンの種類と意味は、以下のとおりです。

トークン	意味	必須
context-id	コンテキストID	○
msgid	メッセージID	○
session-host	セッション情報のホスト名	○
session-subsys	セッション情報のサブシステム名	
start{time-format}	開始時刻	○
end{time-format}	出力時刻	○
elapse	経過時刻	○

トークン	意味	必須
*	上記以外の可変要素	

time-format には、時刻の形式に対応したトークンの指定をする必要があります。前述のAPLOGFORMAT文のtime-formatと同じトークンを使って指定します。

トークン対して出力される文字数の幅が予め分かっている場合（固定幅）、その幅を指定できます。指定方法は前述のAPLOGFORMAT文と同じです。

SAMPLING_RATIO = sample-ratio

サンプリング比率を指定します。
sample-ratio には、サンプリング比率を、0～10000までの整数で指定します。サンプリング処理で選択されたトランザクションのみが詳細画面の解析対象になります。
デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

SAMPLING_RATIO=1000

ポイント

sample-ratio に0を指定すると、詳細データは採取されません。すなわち、詳細表示による分析は行えません。

sample-ratio に1を指定した場合には、サンプリングは行われません。すなわち、すべてのトランザクションが解析対象となります。

注意

サンプリング処理は、デフォルト形式のコンテキストID/コリレーションID を元に行われます。このため、ユーザーの定義などによって、コンテキストID/コリレーションID がデフォルト形式と異なるトランザクションはサンプリングの対象にならない可能性があります。

TIMEZONE = timezone

分析対象ログファイルに記録されている時刻データのタイムゾーンを定義します。
timezone には、ログに出力された時刻のタイムゾーンを指定します。形式は、以下のとおりです。

形式	説明
[+|-]HHMM	+：進んでいることを表す。 -：遅れていることを表す。 HH：時(00～23) MM：分(00～59)

デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

TIMEZONE=+0000

MAXNAMELENGTH = max-name-length

トランザクション名を構成する各キーワードの文字数を示します。
max-name-length には、キーワード文字数を指定します。トランザクション名は、業務名、アプリケーション名、フロー定義名などの情報をキーワードとし、これらのキーワードから構成されます。キーワードは各情報の先頭max-name-length文字で作成されます。max-name-length には、1～1024までの値を指定できます。単位は文字です。（日本語、英数字のどちらの場合でも同じです）
デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

MAXNAMELENGTH=16

LANGUAGE = ASCII | EUCJP | SJIS | UTF8

分析対象ログの文字コードを定義します。選択肢の意味は以下のとおりです。

選択肢	意味
ASCII	アスキー
EUCJP	日本語EUC
SJIS	シフトJIS
UTF8	UNICODEの UTF-8

LANGUAGE文が定義されていない場合は、デフォルト値（動作している環境の言語情報）が採用されます。

■定義例

```
[islog]
sampling_ratio = 1000
timezone = +0900
multiasynclogfile = /var/log/islog*.log
multiasynclogformat = "[*] [context-id] type trigger msgid [destque] flow appl *{fixedwidth24} start{yyyy/mm/dd HH:MM:SS.sss} end{yyyy/mm/dd HH:MM:SS.sss} elapse "
```

1.2.4 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度セットアップを実施した後に、Interstage Application Framework Suite/Interstage Business Application Server のシステム構成を変更した場合は、再度セットアップを実施することで、当機能に Interstage Application Framework Suite/ Interstage Business Application Server のシステム構成の変更を反映してください。

また、再度収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書（コンソール編）「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.2.5 表示

トランザクション内訳分析情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「TxnAsyncMonitor」ノードまたは、「TxnSyncMonitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「TxnAnalysis(Sync)」ノード配下と「TxnAnalysis(ASync)」ノード配下に生成される「TxnTime」ノードを選択することで表示できます。
また、「TxnTime」ノード配下の「TxnIDs」を選択し、トランザクションIDのノードを設定することにより、1トランザクション毎に参照することも可能です。詳細は使用手引書（コンソール編）「3.2.3.4 TxnAnalysis(Sync)/TxnAnalysis(Async)ツリー」を参照してください

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

注意

表示されるトランザクション名、コンテキストID/コリレーションID などの情報は、標準ログが出力する性能ログのメッセージ本文から作成されます。ただし、メッセージ本文に以下に示す文字が含まれた場合、

```
¥ < > " , $ ' [ ] & =
```

次のように置き換えて表示されます。

```
|該当文字の16進コード|
```

1.3 Interstage Service Integratorとの連携

■機能概要

Interstage Service Integrator運用管理コンソールの機能に加え、Systemwalker Service Quality Coordinatorと連携することで数分前のメッセージ量と比較することができます。メッセージの急激な増加や滞留が、表やグラフでいち早く確認できます。

Interstage Service Integratorで構築されたシステムの業務処理量や滞留数などを監視(しきい値監視)し、各業務の稼働状態を把握することができます。

■収集間隔

収集間隔は、1分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.3.1 導入確認
- 1.3.2 セットアップ
- 1.3.3 表示

1.3.1 導入確認

■実行環境

本製品のAgentをInterstage Service Integratorのサーバへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Interstage Service Integrator側での作業

セットアップを行う前に、Interstage Service Integrator側で以下の準備/確認が必要になります。

- Interstage Service Integratorのサービスが起動されていること。

1.3.2 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度収集ポリシーの作成と適用を実施した後に、Interstage Service Integratorのグループ、キュー、シーケンスなどの構成を変更した場合は、再度収集ポリシーの作成と適用を実施する必要があります。

また、再度収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.3.3 表示

Interstage Service Integratorの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「ISI　SequenceMonitor(Summary)」ノード、「ISI　SequenceMonitor(Detail)」ノード、「ISI QueueMonitor(Summary)」ノードまたは、「ISI QueueMonitor(Detail)」ノードを選択することで表示できます。

詳細

詳細ツリーの、「ISI」ノード直下でシーケンス処理件数をあらわす「Sequence」ノードおよび、キュー滞留数を表す「Queue」ノードにツリーが分かれます。「Sequence」ノード配下は、ISIのグループ名のノード、エンドポイント名のノード、およびシーケンス名のノードの3段階の構成で表示され、「Queue」ノード配下は、ISIのグループ名のノード、およびキュー名のノードの2段階の構成で表示されます。詳細は、使用手引書(コンソール編)「3.2.3.5 ISIツリー」を参照してください。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.4 Symfoware Serverとの連携

■機能概要

データベースサーバの稼働状況をSystemwalker Service Quality Coordinatorで監視することにより、ボトルネックを可視化することができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.4.1 導入確認
- 1.4.2 定義方法
- 1.4.3 セットアップ
- 1.4.4 表示
- 1.4.5 本製品のAgentを導入したSymfoware Serverを停止する場合

- 1.4.6 Symfowareの性能情報を取得しない場合

1.4.1 導入確認

■実行環境

本製品のAgentをSymfoware Serverへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Symfoware Server側での作業

収集ポリシーの作成と適用を行う前に、Symfoware Server側で以下の準備/確認が必要になります。

- 性能表示のための各コマンド(rdbsar, rdbps, rdbspcinf, rdbinf)が利用可能な状態になっている(RDBシステムが動作中である)こと。

参照

詳細については、Symfoware Server RDB管理者ガイドを参照してください。

1.4.2 定義方法

本連携機能を使用した場合、デフォルトで収集される項目は以下のとおりです。

- RDBSAR_EB
- RDBSAR_ED
- RDBSAR_EM
- RDBSAR_AGE
- RDBSAR_EL
- RDBPS_S
- RDBPS_R

定義手順を実施することにより、以下の項目が収集可能になります。

- RDBSAR_ER
- RDBSAR_EC
- RDBPS_IA
- RDBINF_AI
- RDBINF_AP
- RDBSPCINF_PD

ポイント

デフォルトで収集される項目で要件を満たす場合は、以降の手順を実施する必要はありません。

■手順1

template.datを修正します。

■定義場所

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

/etc/opt/FJSVssqc/template.dat

■修正内容

RDBSAR_ER／RDBSAR_ECを収集する場合

SYMSARセクションの、

- DSIBUFオプションを"ON"にすると、RDBSAR_ERの収集が有効になります。
- RDBCOMオプションの"ON"にすると、RDBSAR_ECの収集が有効になります。

SYMSARセクションの抜粋

```
##########################################
## Symfoware RDBSAR DCA_CMD
[SYMSAR]
DCAID="SYMFOSAR"
INTERVAL=5
AUTOFLAG="ON"
BUFPOOL="ON"
DBSPIO="ON"
TMPLOG="ON"
ARCLOG="ON"
MEMORY="ON"
DSIBUF="OFF"      ★RDBSAR_ERを有効にするには"ON"にします。
RDBCOM="OFF"      ★RDBSAR_ECを有効にするには"ON"にします。
```

注意

- RDBSAR_ECは、Symfoware側でロードシェア機構が有効になっていないと収集ができません。
- RDBSAR_ERの収集を有効にすると、環境によってはSymfowareに負荷をかけたり、収集されるデータ量が多すぎて、収集間隔内に収集が完了せず、正常に動作しない可能性があります。ご注意ください。

RDBPS_IAを収集する場合

SYMPSセクションの、

- DSISTATUSオプションを"ON"にすると、RDBPS_IAの収集が有効になります。

SYMPSセクションの抜粋

```
##########################################
## Symfoware RDBPS DCA_CMD
[SYMPS]
DCAID="SYMFOPS"
INTERVAL=5
AUTOFLAG="ON"
SQLSTATUS="ON"
PRGSTATUS="ON"
DSISTATUS="OFF"      ★RDBPS_IAを有効にするには"ON"にします。
```

注意

- RDBPS_IAの収集を有効にすると、環境によってはSymfowareに負荷をかけたり、収集されるデータ量が多すぎて、収集間隔内に収集が完了せず、正常に動作しない可能性があります。ご注意ください。

RDBINF_AI/RDBINF_APを収集する場合

SYMINFセクションの、

- SPCINFOオプションを"ON"にすると、RDBINF_APの収集が有効になります。
- DSIINFOオプションを"ON"にすると、RDBINF_AIの収集が有効になります。

SYMINFセクションの抜粋

```
##########################################
## Symfoware RDBINF DCA_CMD
[SYMINF]
DCAID="SYMFOINF"
AUTOFLAG="ON"
INTERVAL=5
SPCINFO="ON"     ★RDBINF_APを収集する場合はONにします。
DSIINFO="ON"     ★RDBINF_AIを収集する場合はONにします。
```

ATTR::DBセクションを修正します。

GROUPパラメタに、キーワード"SYMINF"を追加します。

ATTR::DBセクションの抜粋

```
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
    ↓
GROUP="SYMSAR,SYMPS,ORA,SYMINF"
```

注意

- RDBINF_AI/RDBINF_APの収集を有効にするには、さらに監視対象として、DSI名、DBスペース名をMiddlewareconf.xmlへ設定する必要があります。

- 監視対象数が多い場合、環境によってはSymfowareに負荷をかけたり、収集されるデータ量が多すぎて、収集間隔内に収集が完了せず、正常に動作しない可能性があります。できる限り監視対象の絞り込みを行ってください。

RDBSPCINF_PDを収集する場合

SYMSPCINFセクションの、

- SPCALLをOFFにして、かつ、SPCSEPをONにすると、RDBSPCINF_PDの収集が有効になります。

SYMSPCINFセクションの抜粋

```
##########################################
## Symfoware RDBSPCINF DCA_CMD
[SYMSPCINF]
DCAID="SYMFOSPCINF"
INTERVAL=5
AUTOFLAG="ON"
SPCALL="ON"     ★OFFにしてください。
SPCSEP="OFF"    ★ONにしてください。
```

ATTR::DBセクションを修正します。

GROUPパラメタに、キーワード"SYMSPCINF"を追加します。

ATTR::DBセクションの抜粋

```
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
    ↓
GROUP="SYMSAR,SYMPS,ORA,SYMSPCINF"
```

注意

RDBSPCINF_PDの収集を有効にするには、さらに監視対象としてDBスペース名をMiddlewareconf.xmlへ設定する必要があります。

RDBSPCINF_PDの収集を有効にすると、環境によってはSymfowareに負荷をかけたり、収集されるデータ量が多すぎて、収集間隔内に収集が完了せず、正常に動作しない可能性があります。ご注意ください。

■手順2

MiddlewareConf.xmlを修正します。

■定義場所

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥MiddlewareConf.xml
```

【UNIX版】

```
/etc/opt/FJSVssqc/MiddlewareConf.xml
```

注意

本ファイルは、ポリシー作成コマンドの実行で作成されます。

ポリシー作成コマンド実行時に、監視対象のSymfowareを検出していることを確認後、修正を実施してください。

■修正内容

RDBINF_AP/RDBINF_APAI/RDBSPCINF_PDを収集する場合は、ポリシー作成コマンドの実行時に、Symfowareを検出したことを示すメッセージを確認した後、監視対象とするDB/DBスペース/DSIの名前を本ファイルへ設定します。

修正前の状態

ポリシー作成コマンドにてSymfowareを検出すると、本ファイル内に以下のようなRDB_Systemまでのタグが自動生成されています。

```
<Symfoware DisplayName="Symfoware" InstanceName="" NodeType="F">
 <SymfoEE DisplayName="" InstanceName="" NodeType=""/>
 <RDB_System DisplayName="GYOMU" InstanceName="GYOMU" NodeType="I">
★この間に記述
 </RDB_System>
</Symfoware>
```

★印に位置に、監視対象とするDB/DBスペース/DSIの名前を設定します。

■修正方法

<RDB_System>タグ内(★印の行)に収集対象とするDBの情報を記述します。

記述形式

```
<DBタグ>            #必須
 <DB_Spaceタグ>    #必須
  <DSI タグ />      #RDBINF_AIを収集する場合は必要
 </DB_Spaceタグ>
</DBタグ>
```

■修正例

```
<Symfoware DisplayName="Symfoware" InstanceName="" NodeType="F">
 <SymfoEE DisplayName="" InstanceName="" NodeType=""/>
 <RDB_System DisplayName="GYOMU" InstanceName="GYOMU" NodeType="I">
★  <DB DisplayName="DB_A" InstanceName="DB_A" NodeType="I">
★    <DB_Space DisplayName="DSPACE" InstanceName="DSPACE"
NodeType="I">
★      <DSI DisplayName="DSI1" InstanceName="DSI1" NodeType="I-D"/>
★       <DSI DisplayName="DSI2" InstanceName="DSI2" NodeType="I-D"/>
★            :
★            :
```

```
★   </DB_Space>
★  </DB>
 </RDB_System>
</Symfoware>
```

注)・DBタグのDisplayName属性、InstanceName属性には、DB名を記述します。NodeType属性には必ず"I"を記述します。

・DB_SpaceタグのDisplayName属性、InstanceName属性には、DBスペース名を記述します。NodeType属性には必ず"I"を記述します。

・DSIタグのDisplayName属性、InstanceName属性には、DSI名を記述します。NodeType属性には必ず"I-D"を記述します。

1.4.3 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度収集ポリシーのセットアップを実施した後に、Symfoware ServerのRDBシステム構成を変更した場合は、再度収集ポリシーの作成と適用を実施することで、Symfoware Serverのシステム構成に合わせた収集を実施してください。

また、再度収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

注意

Symfoware Serverにデフォルト RDBシステムが存在しない状態で収集ポリシーの作成を行った場合、エラーメッセージ(qdg13315uなど)が出力される場合があります。
これはRDBシステムの構成を確認する為に出力されるエラーメッセージです。収集ポリシー作成コマンドが正常終了した場合は問題ありません。

1.4.4 表示

Symfoware Serverの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「SymfowareMonitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「Symfoware」を選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

ポイント

Symfoware Server ロードシェア縮退機能が有効になっている場合、RDBSAR_ELレコードのリソースIDは、「RDBシステム名:ロググループ名」が表示されます。

1.4.5 本製品のAgentを導入したSymfoware Serverを停止する場合

本製品が、Symfoware Serverを管理しているシステムでは、Symfoware Serverの通常停止ができません。Symfowareを停止する場合は、以下の方法で停止してください。

- 強制切断モード(rdbsstop -mc)で停止する。(Symfoware Server 9.0以降で利用可能)
- 本製品のサービスを先に停止し、Symfoware Serverを停止する。

参考

本製品のサービスを先に停止し、Symfoware Serverを停止する場合は、以下の手順で実施してください。

1. 本製品のAgentの停止
   「A.4 常駐プロセス、起動と停止」を参照して、サービス/デーモンを起動してください。
2. ポリシーの一時変更

   「A.3 ポリシー一時変更コマンド」を参照して、ポリシーを変更してください。
3. Symfoware Serverの停止
   rdbstopコマンド(詳細はSymfoware Serverのマニュアルを参照してください。)

1.4.6 Symfowareの性能情報を取得しない場合

Symfowareの性能情報を取得しない設定については、以下の手順を実施してください。

注意

本手順を実施した場合、OracleやSQLServerの性能情報の収集も無効になります。

■定義場所

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥template.dat
```

■定義方法

SERVERTYPE セクションの以下のキーを次のように編集してください。他のキーは変更しないでください。

```
[SERVERTYPE]
   :
DB="ON"
   :
```

以下のように変更します。

```
[SERVERTYPE]
   :
DB="OFF"
```

:

1.5 Oracle Database Serverとの連携

■機能概要

Oracle Database Serverで構築された、データベースシステムのキャッシュ使用状況やテーブルの空き容量などを監視(しきい値監視)し、各業務の稼働状態を把握することができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.5.1 導入確認
- 1.5.2 定義方法
- 1.5.3 セットアップ
- 1.5.4 表示

1.5.1 導入確認

■実行環境

本製品のAgentをOracle Database Serverのサーバへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Oracle Database Server側での作業

収集ポリシーの作成と適用を行う前に、Oracle Database Server側で以下の準備/確認が必要になります。

- Oracleの各サービス/デーモンが起動していること。

参考

詳細については、Oracleのマニュアルを参照してください。

1.5.2 定義方法

■定義手順

1. Systemwalker Service Quality Coordinator側の設定を行います。
   収集テンプレートにOracle性能情報を取得するための定義が必要です。

   定義方法については、「第2章 収集テンプレート」を参照してください。

2. Oracleのパス情報を確認/設定します。

   【Windows版】

   環境変数「PATH」にOracleのパスが設定されていることを確認してください。これは通常、Oracleをインストールした際に、自動的に設定されています。なんらかの理由により設定されていない場合は、「PATH」変数に追加する必要があります。
   詳細については、Oracleのマニュアルを参照してください。

   【UNIX版】

   収集テンプレートに設定を行います。
   詳細は「2.1 Oracle Database Serverの管理設定」を参照してください。

本連携機能を使用した場合、デフォルトで収集される項目は以下のとおりです。

- ORA_IO
- ORA_QUEUE
- ORA_RETR
- ORA_TSS
- ORA_RC
- ORA_LC
- ORA_LT
- ORA_RBS

以降で解説する定義手順を実施することにより、以下の項目が収集可能になります。

- ORA_USR
- ORA_MEMORY
- ORA_TSF
- ORA_OSE
- ORA_DFS
- ORA_FS
- ORA_SEGS
- ORA_REDO
- ORA_WAIT
- ORA_FMEM

ポイント

デフォルトで収集される項目で要件を満たす場合は、以降の手順を実施する必要はありません。

■監視項目の拡張手順

1. 対象ノード上で、Systemwalker Service Quality Coordinatorが動作している場合は停止します。
2. template.dat を編集します。

   ■定義場所

   【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

/ect/opt/FJSVssqc/template.dat

■修正内容

```
    :
########################################
# Oracle Information
[ORA]
DCAID="ORA"
INTERVAL=5
SID=""
USERNAME=""
PASS=""
VER="*.*.*"
ORAHOME=""
★ここに追加します。
########################################
    :
```

追加可能なキーは以下になります。

項目名	キー
ORA_USR	USR="ON" or "OFF"
ORA_IO	IO="ON" or "OFF"
ORA_QUEUE	QUEUE="ON" or "OFF"
ORA_MEMORY	MEMORY="ON" or "OFF"
ORA_RETR	RETR="ON" or "OFF"
ORA_TSS	TSS="ON" or "OFF"
ORA_TSF	TSF="ON" or "OFF"
ORA_OSE	OSE="ON" or "OFF"
ORA_DFS	DFS="ON" or "OFF"
ORA_FS	FS="ON" or "OFF"
ORA_SEGS	SEGS="ON" or "OFF"
ORA_RC	RC="ON" or "OFF"
ORA_LC	LC="ON" or "OFF"
ORA_LT	LT="ON" or "OFF"
ORA_REDO	REDO="ON" or "OFF"

項目名	キー
ORA_WAIT	WAIT="ON" or "OFF"
ORA_RBS	RBS="ON" or "OFF"
ORA_FMEM	FMEM="ON" or "OFF"

コンソールの詳細ツリー上で 項目名を表示したい項目のキーを"ON"に、

表示したくない項目を"OFF"にして追加してください。

3. Oracle収集SQL定義元ファイルを編集します。

■定義場所

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥dsa_ora_all.sql
<可変ファイル格納ディレクトリ>¥control¥dsa_ora_<Oracleバージョン>.sql

【UNIX版】

/opt/FJSVssqc/control/dsa_ora_all.sql
/opt/FJSVssqc/control/dsa_ora_<Oracleバージョン>.sql

定義ファイルについて

dsa_ora_all.sqlには、各Oracleバージョン共通の収集用SQLが定義されています。

dsa_ora_<Oracleバージョン>.sqlには、各Oracleバージョン固有の収集用SQLが定義されています。

※ORA_IOの収集は、OracleバージョンによりSQL定義方式が異なるためです。

用意されている定義ファイルの一覧は以下のとおりです。

/etc/opt/FJSVssqc/dsa_ora_all.sql

【V9用】

/etc/opt/FJSVssqc/control/dsa_ora_v9.sql

【V10以降用】

/etc/opt/FJSVssqc/control/dsa_ora_v10.sql

上記の各ファイルから、監視したい項目に該当する処理のコメント識別子'--'を外します。

以下に、ORA_USRの収集を行いたい場合を例に説明します。

■定義例

【修正前】

※ここで監視項目名を判断します。但し、ORA_QUEUE →ORA QUE、ORA_MEMORY→ ORA MEMとしています。 ↓ ～　-- ORA USR records %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

```
～   -- TABLES NEED TO BE READ: V$SYSSTAT
～   -- The following data collection parameter set repo
～   -- the database.
～   --
～   -- [0300] COLUMN
～   --    (PKEY, INTERVAL, SAMPLE, INTERVAL, SAMPLE, IN
～   --    DELIM=",";
～★  -- PROMPT dsa_oracle_data_start 300 column 7 interva
 ★  -- SELECT  VALUE SYSSTAT
 ★  -- FROM    V$SYSSTAT
 ★  -- WHERE   NAME IN ('logons cumulative'
 ★  --              ,'logons current'
 ★  --              ,'opened cursors cumulative'
 ★  --              ,'opened cursors current'
 ★  --              ,'user calls'
 ★  --              ,'user commits'
 ★  --              ,'user rollbacks'
 ★  --              )
 ★  -- ORDER BY NAME;
```

PROMPTのある行から、SQL文の範囲にある'--'を削除してください。(★印の行)

ヘッダー情報の'--'を削除しないように注意してください。

【修正後】

```
※ここで監視項目名を判断します。但し、ORA_QUEUE →ORA QUE、ORA_MEMORY→
ORA MEMとしています。
        ↓
～   -- ORA USR records %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
～   -- TABLES NEED TO BE READ: V$SYSSTAT
～   -- The following data collection parameter set repo
～   -- the database.
～   --
～   -- [0300] COLUMN
～   --    (PKEY, INTERVAL, SAMPLE, INTERVAL, SAMPLE, IN
～   --    DELIM=",";
～★   PROMPT dsa_oracle_data_start 300 column 7 interva
 ★   SELECT  VALUE SYSSTAT
 ★   FROM    V$SYSSTAT
 ★   WHERE   NAME IN ('logons cumulative'
 ★               ,'logons current'
```

```
★              ,'opened cursors cumulative'
★              ,'opened cursors current'
★              ,'user calls'
★              ,'user commits'
★              ,'user rollbacks'
★              )
★  ORDER BY NAME;
```

その他の追加したい監視項目についても、同様の修正を行ってください。

1.5.3 セットアップ

1. sqcSetPolicyを実行します。

■定義場所

【Windows版】

```
<インストールディレクトリ>¥bin¥sqcSetPolicy.exe
```

【UNIX版】

```
/opt/FJSVssqc/bin/sqcSetPolicy.sh
```

注意

1度もポリシー作成コマンド(sqcRPolicy)を実行していない場合は、手順を実施する前に、ポリシー作成コマンド(sqcRPolicy)を実行してください。

■定義場所

【Windows版】

```
<インストールディレクトリ>¥bin¥sqcRPolicy.exe
```

【UNIX版】

```
/opt/FJSVssqc/bin/sqcRPolicy.sh
```

sqcSetPolicyを実行することにより、編集したOracle収集SQL定義元ファイルを元にして収集用の定義ファイルが作成されます。

■定義場所

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥<セクション名>_all_sel.sql
<可変ファイル格納ディレクトリ>¥control¥<セクション名>_<Oracleバージョン>_sel.sql
```

【UNIX版】

/etc/FJSVssqc/<セクション名>_all_sel.sql
/etc/opt/FJSVssqc/<セクション名>_<Oracleバージョン>_sel.sql

定義ファイルについて

<セクション名>・・・template.datで定義されたOracle収集セクション名がセットされます。

<Oracleバージョン>・・・template.datで定義されたOracleバージョン名がセットされます。

<セクション名>_all_sel.sqlには、各Oracleバージョン共通の収集用SQLが定義されています。
※上記は、dsa_ora_all.sqlがベースになっています。

<セクション名>_<Oracleバージョン>_sel.sqlには各Oracleバージョン固有の収集用SQLが定義されています。
※上記は、dsa_ora_<Oracleバージョン>.sqlがベースになっています。

【定義例】

/ect/opt/FJSVssqc/control/ORA_all_sel.sql
/ect/opt/FJSVssqc/control/ORA_v9_sel.sql

ポイント

複数のインスタンスを監視（template.datに複数のOracle収集定義セクションを追加）している場合は、監視している数だけ定義ファイルが生成されます。

2. Systemwalker Service Quality Coordinatorを起動します。

   5分程度(Pull運用の場合は10分)経過したら、管理コンソールから構成情報取得を実施してください。

注意

環境によって性能情報量が多くなると収集間隔内に収集を完了できない場合があります。その場合は、収集間隔内に収集が完了できるように、収集する項目を減らすなど調整が必要になります。

一度収集ポリシーの作成と適用を実施した後に、Oracleの監視対象としているインスタンスを変更した場合は、本節の作業をもう一度実施してください。

また、再度収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書（コンソール編）「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.5.4 表示

Oracle Database Serverの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「OracleMonitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「Oracle」を選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.6 Systemwalker Centric Managerとの連携

■機能概要

Systemwalker Centric Managerとの連携は以下の機能を提供いたします。

- しきい値監視
- サマリ画面の呼び出し
- 性能情報(トラフィック情報)のPDB格納

しきい値監視

しきい値監視で、しきい値超えが検知されると、Systemwalker Centric Managerの監視画面では、該当するノードにて異常が発生した旨の通知(ノードアイコンの点滅など)を行うことができます。

サマリ画面の呼び出し

Systemwalker Centric Managerの監視画面から、本製品のサマリ画面を呼び出すことができます。

性能情報(トラフィック情報)のPDB格納

Systemwalker Centric Managerの部門管理サーバ(または運用管理サーバ)から、性能情報のCSV出力コマンドF3crTrfBcsvの出力結果(トラフィック情報)を取得し、そのCSV出力ファイルをPDBに格納すると、本製品のレポート画面からトラフィック情報のレポートを出力することができます。

■手順

連携を行うための手順を以下の順に説明します。

- 1.6.1 導入確認
- 1.6.2 しきい値監視
- 1.6.3 サマリ画面の呼び出し連携
- 1.6.4 性能情報(トラフィック情報)のPDB格納

1.6.1 導入確認

■実行環境

Systemwalker Centric Managerが導入されている環境で連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Systemwalker Centric Manager側での作業

収集ポリシーの作成と適用を行う前に、Systemwalker Centric Manager側で以下の準備/確認が必要になります。

しきい値監視機能を使用する場合

1. 監視イベント種別「性能監視」を登録する

   「性能監視」は初期登録されている種別です。通常は登録する必要はありません。削除されている場合に限り、Systemwalker Centric Managerの以下のマニュアルを参照して登録してください。
   Systemwalker Centric Manager 使用手引書 監視機能編

2. 監視イベントを登録する

   Systemwalker Centric Managerの[イベント監視の条件定義]ウィンドウで監視イベントを追加し、Systemwalker Service Quality Coordinatorのメッセージに対して性能監視を行えるように定義します。

   - Systemwalker Service Quality Coordinatorのメッセージを特定する為の条件は以下です。
     [イベント監視の条件定義]の[イベント定義]において、[ラベル名]の定義でソース名に"SSQC"を指定します。
   - 性能監視を行う為の[アクション定義]の設定は以下です。
     [イベント監視の条件定義]の[アクション定義]において、[監視イベント種別]で"性能監視"を選択します。

   Systemwalker Centric Managerの[イベント監視の条件定義]の詳細については、以下のマニュアルを参照してください。
   Systemwalker Centric Manager 使用手引書 監視機能編

サマリ画面の呼び出し

特に作業は必要ありません。

性能情報(トラフィック情報)のPDB格納

性能監視機能(ネットワークトラフィック情報の監視)を有効にしておく必要があります。

参照

詳細については、Systemwalker Centric Managerのマニュアルを参照してください。

1.6.2 しきい値監視

しきい値監視で、しきい値超えが検知されると、Systemwalker Centric Managerの監視画面では、該当するノードにて異常が発生した旨の通知が行われます(ノードアイコンの点滅など)。

サーバ内リソース情報のしきい値監視については、Systemwalker Centric Managerの監視画面で認識されている管理対象ノードと、本製品の管理対象は合致します。しかし、レスポンス・稼働情報のしきい値監視については、しきい値超えの結果、どのノードアイコンを点滅させるか、事前に決めておく必要があります。

どのノードアイコンを点滅させるかは、レスポンス・稼働管理対象構成情報(ServiceConf.xml)の、各タグ内のAlertTarget属性で定義します。定義方法の詳細については、「第6章 レスポンス・稼働管理対象構成情報(ServiceConf.xml)」を参照してください。

ポイント

インストール時に、しきい値超えが発生した場合の通知方法として「イベントログ/syslog」を選択した場合は、実行するアラームアクションの種類として「Centric Manager」を定義する必要があります。定義方法の詳細については、「7.3 アラームアクション定義」を参照してください。

1.6.3　サマリ画面の呼び出し連携

Systemwalker Centric Managerの監視画面から、本製品のサマリ画面を呼び出す場合は、Systemwalker Centric Managerの監視画面で、本製品のサマリをメニュー登録する必要があります。サマリ画面の呼び出し方法については、使用手引書（コンソール編）「3.3.1 サマリ呼び出し方法」を参照してください。

1.6.4　性能情報(トラフィック情報)のPDB格納

Systemwalker Centric Managerの部門管理サーバ(または運用管理サーバ)から、性能情報のCSV出力コマンドF3crTrfBcsvの出力結果(トラフィック情報)を取得し、そのCSV出力ファイルをPDBに格納すると、本製品のレポート画面からトラフィック情報のレポートを出力することができます。

ポイント

当連携は、ファイル渡しによる連携のため、Systemwalker Centric Managerと本製品のAgentは、必ずしも同一ホスト上に配置する必要はありません。

以下に手順を示します。

1.6.4.1　定義方法

トラフィック情報をPDBに格納するには、まず、以下の定義ファイルを用意します。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥cntrcconf.ini
```

【UNIX版】

```
/etc/opt/FJSVssqc/cntrcconf.ini
```

■形式

```
[MIDDLEWARE_CONF]
XML=ON | OFF
```

■説明

[MIDDLEWARE_CONF]

トラフィック情報を管理するか否かを定義します。

XML=ON | OFF

選択肢の意味は以下のとおりです。初期値は、OFFになっています。

選択肢	意味
ON	トラフィック情報を管理します。
OFF	トラフィック情報を管理しません。

1.6.4.2　セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

また、収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.6.4.3　PDBへの格納

トラフィック情報をPDBに格納するには、sqcPDBcloadコマンドを使用します。

■格納パス

【Windows版】

```
<インストールディレクトリ>¥bin
```

【UNIX版】

```
/opt/FJSVssqc/bin
```

■記述形式

sqcPDBcload	-c trafficdata-file

■オプション

-c trafficdata-file

PDBに格納する、トラフィックデータファイル(CSVファイル)を指定します。トラフィックデータファイルは、性能情報のCSV出力コマンドF3crTrfBcsvの出力結果です。

■使用例

【Windows版/UNIX版】

```
> sqcPDBcload -c traffic.csv
```

1.6.4.4　表示

トラフィック情報は、以下の方法で表示することができます。

レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

注意

「データ間隔」は「1時間単位」のみ使用可能です。それ以外の単位を指定しても表示は行われません。

1.7 Systemwalker Operation Managerとの連携

■機能概要

Systemwalker Operation Manageと連携することで、バッチジョブの実行状況とバッチサーバやDBサーバの負荷状況の相関関係を可視化・分析することができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.7.1 導入確認
- 1.7.2 定義方法
- 1.7.3 セットアップ
- 1.7.4 表示

1.7.1 導入確認

■実行環境

本製品のAgentをSystemwalker Operation Managerのサーバへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Systemwalker Operation Manager側での作業

収集ポリシーの作成と適用を行う前に、Systemwalker Operation Manager側で以下の準備/確認が必要になります。

1. Systemwalker Operation Managerがインストールされていること。
2. Systemwalker Operation Managerの環境設定が行われていること。
3. 環境設定時に、稼働実績情報ファイルが保存されるように設定されていること。
4. 予測時間超えジョブ数を分析する場合、環境設定時に、ジョブスケジューラの起動パラメタのイベント出力設定において、ジョブの実行予測時間を過ぎても終了しない場合に通知を行うように設定されていること。
5. Systemwalker Operation Managerの各サービス/デーモンが起動されていること。

   以下で説明する、特定のサブシステム、キュー、及び、プロジェクトのみを分析対象としたい場合、Systemwalker Operation Managerの各サービス/デーモンは起動されている必要はありません。

参照

キューを追加、変更または削除した場合や、稼働実績情報ファイルの保存場所を変更した場合には、変更を有効にするためにSystemwalker Operation Managerの各サービス/デーモンを初期かモードで再起動してください。

詳細については、Systemwalker Operation Managerのマニュアル等を参照してください。

注意

本機能では、本製品のEnterprise Edition と Standerd Editionで以下の機能差があります。

EE Systemwalker Operation Manager の全てのサブシステムを管理対象にすることができます。

SE Systemwalker Operation Manager のサブシステム0 のみを管理対象にすることができます。

また、本製品のStandard Editionと、Systemwalker Operation ManagerのEnetrprise Editionを組み合わせた場合、起動時に警告メッセージが出力されます。

1.7.2 定義方法

Systemwalker Operation Managerの特定のサブシステム、キュー、及び、プロジェクトのみを分析対象としたい場合、以下の定義ファイルを用意します。

また、Systemwalker Operation Managerが動作中でないが、いずれ起動する場合にも、以下の定義ファイルを用意します。

ポイント

本定義ファイルを利用し、分析対象のサブシステム、プロジェクト、及び、キューを制限することにより、PDBへ格納されるデータ量を抑えられ、管理サーバの負荷を軽減することにも利用できます。

注意

- 本定義ファイルの設定を行った場合、設定を行ったサブシステム、キュー、及び、プロジェクト以外のデータはPDBには格納されません。
- 本定義ファイルを設定しない場合、Systemwalker Operation Managerで設定されているすべてのサブシステム、キュー、及び、プロジェクトを分析対象とします。

  そのため、特定のサブシステム、キュー、及び、プロジェクトを絞り込んだ分析を行わない場合は、定義ファイルの設定は必要ありません。

  インストール時は、本定義ファイルが存在しません。
- 監視対象サーバであるが、Systemwalker Operation Managerが停止状態、もしくは、待機状態などの理由により、動作中でないサーバに関しまして、サブシステム名、プロジェクト名、及び、キュー名の情報を取得することが出来ないため、本定義ファイルの設定を行ってください。

  本定義ファイルが設定されていない場合、Systemwalker Operation Managerが停止状態から動作中に変わった場合、正しくデータを採取することができません。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥jla.ini

【UNIX版】

/opt/FJSVssqc/control/jla.ini

なお、テキストファイルに日本語を記述する場合は、Operation Managerが動作している文字コードを使用する必要があります。

■形式

```
[subsystem]
subsystem = LL
[project]
subsystemMM = project_name
[queue]
subsystemNN = queue_name
```

■説明

[subsystem] (Standard Editionの場合は設定を行わないでください。)

収集対象のサブシステムの定義ブロックの開始を表します。また、他の定義ブロックの終了を表します。

分析対象となるサブシステムを以下の定義文にて設定します。

```
subsystem = LL
```

LL:00～09までの2桁の整数で、対象となるサブシステムの番号を1つ設定します。

注意

- 本製品は、リソースIDにサブシステム、キュー、及び、プロジェクトが設定され、レポート画面にて前方一致という形式で絞り込むことができます。そのため、サブシステムの番号に一意性を持たせるため、2桁の整数で扱うようになっておりますので、Systemwalker Operation Managerのサブシステムの番号が1桁の場合、ゼロ(0)を前に加えて、2桁の整数に読み替えてください。

  ■例
  2の場合→02

- 複数のサブシステムを指定する場合は、同様に複数行設定します。
- LLの部分が指定されていない行は無視されます。
- 本ブロック内に定義文が1行もなく、本セクションを省略した場合、全サブシステムが分析対象になります。

[project]

対象プロジェクトの定義ブロックの開始を表します。また、他の定義ブロックの終了を表します。

分析対象となるプロジェクトを以下の定義文にて設定します。

```
subsystemMM = project_name
```

MM：00～09までの2桁の整数、対象となるプロジェクトのサブシステムの番号を設定します。

project_name：対象となるプロジェクト名を1つ設定します。

注意

- 複数のプロジェクト、サブシステムを指定する場合は、同様に複数行設定します。
- project_nameの部分が指定されていない行は無視されます。
- [project]内に設定されていないサブシステムについては、その[subsystem]内の全プロジェクトが分析対象になります。
- 同じ指定が重複して指定された場合も問題ありません。
- 本ブロック内に定義文が1行もない場合は、本ブロックを省略することができます。
- プロジェクト名にSystemwalker Service Quality Coordinatorの禁止文字(¥ : < > " , $ ' [ ] & =)が使用された場合、禁止文字が以下のフォーマットに変換されて表示されます。

  ```
  “|16進の禁止文字のコード|”
  ```

  ■例

  ```
  “&” -> “|26|”
  ```

[queue]

対象キュー定義ブロックの開始を表します。また、他の定義ブロックの終了を表します。

分析対象となるキューを以下の定義文にて設定します。

```
subsystemNN = queue_name
```

NN：00～09までの2桁の整数、対象となるキューのサブシステムの番号を設定します。

queue_name：対象となるキュー名を1つ設定します。

注意

- 複数のキュー、サブシステムを指定する場合は、同様に複数行設定します。
- queue_nameの部分が指定されていない行は無視されます。
- [queue]内に設定されていないサブシステムについては、その[subsystem]内の全キューが分析対象になります。
- 同じ指定が重複して指定された場合でも問題ありません。
- 本ブロック内に定義文が1行もない場合は、本ブロックを省略することができます。

・ [subsystem]、[project]、[queue] ブロックの順序による影響はありません。

・ シャープ(#)から始まる行はコメントと見なして、無視されます。

■定義例

定義例は、以下のとおりです。

```
[subsystem]
subsystem = 00
subsystem = 01
[project]
subsystem00 = eigyo
subsystem00 = keiri
subsystem01 = soumu
[queue]
subsystem00 = queue0
subsystem00 = queue1
subsystem01 = queue0
subsystem01 = queue1
```

■クラスタシステム運用を行う場合

・ サーバ構成が運用待機形態の場合

定義ファイルを、現用側、待機側の両方のサーバに同一の設定を行ってください。

・ サーバ構成が相互待機形態

両方のサーバで分析対象としたいサブシステム、プロジェクト、及び、キューを合わせて定義ファイルに設定を行います。

また、定義ファイルは、両側に同一の設定を行ってください。

1.7.3 セットアップ

収集ポリシーセットアップを行う前に、Systemwalker Operation Managerの各サービス/デーモンが起動されていることを確認してください。

定義ファイル(jla.ini)が設定されている場合、Systemwalker Operation Managerの各サービス/デーモンは起動されている必要はありません。

収集ポリシーのセットアップを行う前に、定義ファイル(jla.ini)に分析対象を設定していない場合は、以下のような分析を行いますのでご注意ください。

・ 定義ファイル(jla.ini)にて分析対象サブシステムを設定していない場合は、収集ポリシー作成時に動作しているサブシステムのみ分析を行います。

・ 定義ファイル(jla.ini)にて分析対象プロジェクトを設定していない場合は収集ポリシー作成時に登録されているプロジェクトのみ分析を行います。

・ 定義ファイル(jla.ini)にて分析対象キューを設定していない場合は収集ポリシー作成時にSystemwalker Operation Managerの初期化ファイル(ジョブ実行制御)に定義されているキューのみ分析を行います。

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度収集ポリシーのセットアップを実施した後に、サブシステム、キュー、またはプロジェクトにおいて、追加また削除をした場合は、収集ポリシーの作成と適用を実施することで、Systemwalker Operation Managerのシステム構成に合わせた収集を実施してください。

また、収集ポリシーの作成と適用を実施した後に、コンソールへの反映が必要になります。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.7.4 表示

Systemwalker Operation Managerの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「OperationMgrMonitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「OperationMGR」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.8 Systemwalker Network Managerとの連携

■機能概要

Systemwalker Network Managerの運用管理サーバで、本製品とのレポート連携機能を使用することで、本製品のレポート画面からSystemwalker Network Managerのログデータのレポートを出力したり、サーバ間のTCP通信やネットワーク機器の状態を分析することができます。

Systemwalker Network Managerの運用管理サーバから、本製品とのレポート連携機能を使用することで、サーバ間のTCP通信やネットワーク機器の状態を分析することができます。

■手順

連携を行うための手順を以下の順に説明します。

1.8.1 導入確認

■実行環境

本製品のAgentは、Systemwalker Network Managerの運用管理サーバへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

参考

詳細については、Systemwalker Network Managerのマニュアルを参照してください。

■Systemwalker Network Manager側での作業

Systemwalker Network Managerの運用管理サーバで、本製品とのレポート連携機能による統計監視スケジュールを行うことで、自動的に、ログデータをPDBに格納します。

1.8.2 定義方法

ログデータを本製品で表示するには、以下の定義ファイルを用意します。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【UNIX版】

```
/etc/opt/FJSVssqc/snmconf.ini
```

■形式

```
[MIDDLEWARE_CONF]
XML=ON | OFF
```

■説明

[MIDDLEWARE_CONF]

ログデータを管理するか否かを定義します。

XML=ON | OFF

選択肢の意味は以下のとおりです。初期値は、OFFになっています。

選択肢	意味
ON	ログデータを管理します。
OFF	ログデータを管理しません。

1.8.3 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

また、収集ポリシーの作成と適用を実施した後に、コンソールへの反映が必要になります。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.8.4 表示

ログデータは、以下の方法で表示することができます。

レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

注意

「データ間隔」は「1時間単位」および「1日単位」のみ使用可能です。それ以外の単位を指定しても表示は行われません。(IP稼働監視は「1日単位」のみ使用可能です)

1.9 Systemwalker Resource Coordinator (サーバプロビジョニング)との連携

■機能概要

本製品は、Systemwalker Resource Coordinatorのサーバプロビジョニング機能で、サーバリソースの割り当て動作(管理対象サーバへのソフトウェアイメージ配信)に連動して自動セットアップされるソフトウェアの1つです。
アプリケーションが利用するサーバのリソース配分を必要に応じて最適化し、システム資源を有効に使用することができ、プロビジョニングを支援します。

■手順

連携を行うための手順を以下の順に説明します。

1.9.1 導入確認

1.9.2 手動での登録方法

1.9.1 導入確認

■実行環境

本製品のAgentをSystemwalker Resource Coordinatorのエージェント(管理対象サーバ)へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Systemwalker Resource Coordinator側での作業

サーバリソースの割り当て動作が行われると、環境設定画面の未登録Agent情報(UnregisteredAgents)に、割り当てられたサーバが未登録のAgentとして表示されます。

この連動は、以下の仕組みによって行われます。

- 本製品は、インストールされた時に、Systemwalker Resource Coordinator側に、本製品のセットアップ内容を登録します。

・ Systemwalker Resource Coordinatorは、その登録内容にしたがって、サーバリソースを割り当てる時に、本製品のセットアップを実施します。

なお、上記は、以下の順番で製品をインストールした時に行われます。

・ Systemwalker Resource Coordinatorのエージェントのインストール

・ Systemwalker Service Quality CoordinatorのAgentのインストール

注意

本製品のAgentが先にインストールされた場合は、セットアップ内容が登録されません。その場合は、「1.9.2 手動での登録方法」を参照して手動で登録してください。

1.9.2 手動での登録方法

■格納パス

【Windows版】

```
<インストールディレクトリ>¥bin
```

【UNIX版】

```
/opt/FJSVssqc/bin
```

■記述形式

【Windows版】

```
sqcRCset.exe -c|-d
```

【UNIX版】

```
sqcRCset.sh -c|-d
```

■オプション

-c

セットアップ内容を登録します。

-d

セットアップ内容を削除します。

S

1.10 Systemwalker Resource Coordinator (ネットワークリソースマネージャー)との連携

注意

当機能は、本製品のSolaris版の環境でのみ利用可能です。

■機能概要

Systemwalker Resource Coordinatorのネットワーク監視機能の連携することにより、ネットワークの状況をSystemwalker Service Quality Coordinatorからレポートすることができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

1.10.1 導入確認

1.10.2 セットアップ

1.10.3 表示

1.10.1 導入確認

■実行環境

本製品のAgentをSystemwalker Resource Coordinatorのエージェント(ネットワークリソースマネージャー)へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Systemwalker Resource Coordinator側での作業

収集ポリシーの作成と適用を行う前に、Systemwalker Resource Coordinator側で以下の準備/確認が必要になります。

1. パッケージFJSVnetsrがインストールされていること。
2. ネットワーク監視が利用できる状態になっていること。
3. Systemwalker Resource Coordinatorの各サービス/デーモンが起動していること。

参照

詳細については、Systemwalker Resource Coordinatorのマニュアルを参照してください。

1.10.2 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度収集ポリシーの作成と適用を実施した後に、Systemwalker Resource Coordinatorのシステム構成を変更した場合は、再度収集ポリシーの作成と適用を実施することで、Systemwalker Resource Coordinatorのシステム構成に合わせた収集を実施してください。

また、再度収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.10.3 表示

Systemwalker Resource Coordinator (ネットワークリソースマネージャー)の性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「TcpNetworkMonitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「TcpNetwork」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.11 Systemwalker Resource Coordinator (ストレージリソースマネージャー)/ ETERNUS SF Storage Cruiserとの連携

■機能概要

Systemwalker Resource Coordinatorのストレージ管理機能または、ETERNUS SF Storage Cruiserと連携することにより、ストレージデバイスの稼働状況をSystemwalker Service Quality Coordinatorからレポートすることができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.11.1 導入確認
- 1.11.2 セットアップ
- 1.11.3 表示

1.11.1 導入確認

■実行環境

本製品のAgentをSystemwalker Resource Coordinatorのマネージャー(ストレージリソースマネージャー)または、ETERNUS SF Storage Cruiserへ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Systemwalker Resource Coordinator側での作業

収集ポリシーの作成と適用を行う前に、Systemwalker Resource Coordinatorまたは、ETERNUS SF Storage Cruiser側で以下の準備/確認が必要になります。

1. ストレージリソースマネージャーまたは、ETERNUS SF Storage Cruiserがインストールされていること。

2. ストレージリソースマネージャーまたは、ETERNUS SF Storage Cruiserの各サービス/デーモンが起動していること。
3. 性能情報の収集設定が完了していること。

参照

詳細については、Systemwalker Resource Coordinatorまたは、ETERNUS SF Storage Cruiserのマニュアルを参照してください。

1.11.2 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

一度収集ポリシーの作成と適用実施した後に、Systemwalker Resource Coordinatorまたは、ETERNUS SF Storage Cruiserのシステム構成を変更した場合は、再度収集ポリシーの作成と適用を実施することで、Systemwalker Resource Coordinatorまたは、ETERNUS SF Storage Cruiserのシステム構成に合わせた収集を実施してください。

また、再度収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

注意

- 次の場合、RAIDGroupに関する情報が収集されません。
  - LogicalVolumeの割り当てられていないRAIDGroup。
  - E6000でMLUが割り当てられているRAIDGroup。
- ROE(RAID Offload Engine)を搭載していないETERNUSの場合は、ROEに関する性能情報が収集されません。

1.11.3 表示

Systemwalker Resource Coordinator (ストレージリソースマネージャー) または、ETERNUS SF Storage Cruiserの性能情報は以下の方法で表示することができます。

詳細

詳細ツリーの「StorageResource」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.12 Microsoft SQL Serverとの連携

■機能概要

データベースサーバの稼働状況をSystemwalker Service Quality Coordinatorで監視することにより、ボトルネックを可視化することができます。

■収集間隔

収集間隔は、1分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.12.1 導入確認
- 1.12.2 定義方法
- 1.12.3 セットアップ
- 1.12.4 表示

1.12.1 導入確認

■実行環境

Microsoft SQL Serverがインストールされている環境へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Micirsoft SQL Server側での作業

事前にMicirsoft SQL Server側で以下の準備/確認が必要になります。

1. Micirsoft SQL Serverがインストールされていること。
2. Microsoft SQL Serverの各サービス/デーモンが起動していること。

1.12.2 定義方法

収集テンプレートにMicrosoft SQL Serverの性能情報を取得するための定義が必要です。

■定義場所

template.datの格納場所は以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

/etc/opt/FJSVssqc/template.dat

定義方法については、「2.3 Microsoft SQL Serverの管理設定」を参照してください。

参照

詳細については、Microsoft SQL Serverのマニュアルを参照してください。

1.12.3 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

1.12.4 表示

Microsoft SQL Serverの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「MS-SQL_Monitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「MS-SQL」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.13 Microsoft .NETとの連携

■機能概要

.NETを構成する各種リソースの状態を監視し、レポートすることができます。

■収集間隔

収集間隔は、1分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.13.1 導入確認
- 1.13.2 定義方法
- 1.13.3 セットアップ
- 1.13.4 表示

1.13.1 導入確認

■実行環境

Microsoft .NET(IISのASP.NET、および、.NET Framework)がインストールされている環境へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■Micirsoft .NET側での作業

収集ポリシーの作成と適用を行う前に、Micirsoft .NET側で以下の準備/確認が必要になります。

・ Micirsoft .NETアプリケーションが起動していること。

1.13.2 定義方法

収集テンプレートにMicrosoft .NETの性能情報を取得するための定義が必要です。

■格納場所

template.datの格納場所は以下のとおりです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥template.dat
```

【UNIX版】

```
/etc/opt/FJSVssqc/template.dat
```

定義方法については、「2.2 Microsoft .NET Serverの管理設定」を参照してください。

1.13.3 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

1.13.4 表示

Microsoft .NETの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「MS-.NET_Monitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「MS-.NET」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

1.14 SAP NetWeaverとの連携

■機能概要

本製品は、SAP NetWeaverが提供するCCMS連携インターフェースを利用して性能情報を収集します。

SAP NetWeaver上で動作する業務アプリケーションの性能をSystemwalker Service Quality Coordinatorで分析することにより、アプリケーションサーバの性能、および業務アプリケーションのレスポンスや処理量などのサービス品質を管理することができます。

■収集間隔

収集間隔は、5分です。

■手順

連携を行うための手順を以下の順に説明します。

- 1.14.1 導入確認
- 1.14.2 定義方法
- 1.14.3 セットアップ
- 1.14.4 表示

1.14.1 導入確認

■実行環境

SAP NetWeaverがインストールされている環境へ導入することで連携が可能です。

対応インストール種別の関係については、解説書「1.2.3 管理対象と対応インストール種別」を参照してください。

■SAP NetWeaver側での作業

収集ポリシーの作成と適用を行う前に、SAP NetWeaver側で以下の準備/確認が必要になります。

- SAP NetWeaverの警告モニタ(Alert Monitor)が、利用できる状態になっていること。

1.14.2 定義方法

SAP NetWeaverから性能情報を収集するには、以下に示す二つの定義ファイルが必要です。

- 1.14.2.1 接続先システム定義ファイル
- 1.14.2.2 接続パラメタ定義ファイル

1.14.2.1 接続先システム定義ファイル

SAP NetWeaverシステムに接続するためには、saprfc.ini ファイルに設定する必要があります。

参照

saprfc.ini ファイルの記述形式詳細は、SAP NetWeaverのドキュメントを参照してください。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、テキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥saprfc.ini

【UNIX版】

```
/etc/opt/FJSVssqc/saprfc.ini
```

■形式

```
DEST=destination
TYPE=A
ASHOST=hostname
SYSNR=system-number
```

■説明

DEST=destination

接続先システム定義名を定義します。

ここで定義した名前は、「接続先システム定義名」と呼ばれます。この名前は、次項で説明する接続パラメタ定義ファイルのDEST定義文と合わせておく必要があります。

TYPE=A

接続タイプを指定します。必ず A を指定してください。

注意

タイプA は、特定のアプリケーションサーバを監視対象とする場合に指定するパラメタです。タイプA以外のタイプを指定すると、監視機能は正常に動作しません。

ASHOST=hostname

監視対象のSAP NetWeaverアプリケーションサーバのホスト名を定義します。ホスト名には hosts ファイルで定義された名前を指定します。

SYSNR=system-number

監視対象のSAP NetWeaverアプリケーションサーバのシステム番号を定義します。システム番号は2 桁の半角英数字(00～99)で指定します。

■定義例

定義例は以下のとおりです。

```
DEST=BIN_HS0011
TYPE=A
ASHOST=HS0011
SYSNR=01
```

1.14.2.2　接続パラメタ定義ファイル

本定義ファイルは、SAP NetWeaverシステムとのセッション開設に必要なパラメタなどを記述したファイルです。

■定義場所

定義ファイルは、テキストファイルです。ファイルの作成と編集は、テキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥sqcGetSAPalertmon.ini

【UNIX版】

/etc/opt/FJSVssqc/sqcGetSAPalertmon.ini

■形式

DEST=destination-name
CLIENT=signon-data-client
USER= signon-data-user
PASSWORD= signon-data-password
LANGUAGE= signon-data-language

■説明

DEST=destination-name

接続先システム定義名を定義します。

前項で説明した接続先システム定義ファイル(saprfc.ini)のDEST定義文で定義した接続先システム定義名を指定してください。

注意

DEST定義文に始まる一連の定義は、1セットのみ定義してください。複数のアプリケーションサーバに対する定義は設定できません。

CLIENT=signon-data-client

SAP NetWeaverシステムに接続する時に使用するクライアント番号を指定します。クライアント番号とは、ユーザー登録した際に定義した付加情報です。

USER=signon-data-user

SAP NetWeaverシステムに接続する時に使用するユーザー名を定義します。

使用するユーザーには、以下の権限が必要です。

権限オブジェクト名	権限	詳細
RFC アクセス権限チェック	S_RFC	汎用モジュールグループには SYST、SXMI、SALX が必要となります。
外部管理ツールの権限	S_XMI_PROD	以下のように権限情報を設定します。 ・ COMPANY（接続を認める製品企業情報） * または fujitsu を設定 ・ EXTPRODUCT（接続を認める製品情報） * または SW/SQC を設定

権限オブジェクト名	権限	詳細
		・ INTERFACE（接続を認めるインターフェースのカテゴリ） * または XAL を設定

PASSWORD=signon-data-password

SAP NetWeaverシステムに接続する時に使用するユーザーのパスワードを定義します。USER定義文に対応するパスワードを指定してください。

LANGUAGE= signon-data-language

SAP NetWeaverシステムに接続した時に出力されるログ言語を指定します。指定可能な言語は、SAP NetWeaver システムのログ出力で指定できる言語です。

代表的な言語に、日本語、英語、ドイツ語があります。日本語の場合はJ またはJA、英語の場合はE またはEN、ドイツ語の場合はD またはDE を指定します。

■定義例

定義例は以下のとおりです。

```
DEST=BIN_HS0011
CLIENT=100
USER=ssqc
PASSWORD=password
LANGUAGE=J
```

1.14.3 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

また、収集ポリシーの作成と適用を実施した場合は、コンソールに反映が必要です。使用手引書（コンソール編）「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

1.14.4 表示

SAP NetWeaverの性能情報は、以下の方法で表示することができます。

サマリ

サマリツリーの「SAP Monitor」ノードを選択することで表示できます。

詳細

詳細ツリーの「SAP」ノードを選択することで表示できます。

レポート

総点検分析・レポート

カテゴリ別診断分析・レポート

詳細分析・レポート

第2章 収集テンプレート

性能情報を収集するために、一部の管理対象は収集テンプレートへの定義設定が必要になります。

以下、定義方法を説明します。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

/etc/opt/FJSVssqc/template.dat

■定義方法

本ファイルには、常時収集する項目が定義されており、ポリシー作成/ポリシー適用の実行時に本定義にしたがって自動的に収集ポリシーが作成されます。

但し、以下のミドルウェアを管理対象とするには、本定義に設定を追加することで、収集ポリシーが作成されます。

管理対象	本定義ファイル内のセクション名	参照
Oracle Database Server	[ORA]	2.1 Oracle Database Serverの管理設定
Microsoft .NET Server	[ATTR::AP]	2.2 Microsoft .NET Serverの管理設定
Microsoft SQL Server	[ATTR::DB]	2.3 Microsoft SQL Serverの管理設定

2.1 Oracle Database Serverの管理設定

Oracleを管理対象にする場合は、[ORA]セクションの以下のキーを定義します。

項目	定義内容	定義例
[ORA]	セクション名です。変更しないでください。	ORA
DCAID	Oracleを監視するための固有のIDです。変更しないでください。	"ORA"
INTERVAL	収集間隔です。単位は分です。変更しないでください。	5
SID	「Oracleインスタンス名」を設定します。	ORCL

項目	定義内容	定義例
	ポイント ここで設定する名前はリソースIDの先頭に付加されます。	
USERNAME	Oracleにアクセスし、動的パフォーマンスビューから情報を取得するためのユーザー（DBAロールを付与した管理者ユーザー）のIDを入力します。 通常、Oracleのデフォルトでは“system”です。デフォルトから変更する場合は、「2.1.1 Oracleの動的パフォーマンスビューにアクセスできるユーザーを新規で作成する方法」を参照してください。	System
PASS	Oracleにアクセスし、動的パフォーマンスビューから情報を取得するためのユーザー（DBAロールを付与した管理者ユーザー）のパスワードを入力します。 通常、Oracleのデフォルトでは“manager”です。デフォルトから変更する場合は、「2.1.1 Oracleの動的パフォーマンスビューにアクセスできるユーザーを新規で作成する方法」を参照してください。	manager
VER	監視するOracleインスタンスのバージョンを記述します。「X.X.X」という3桁の形式で記述してください。	9.2.0
ORAHOME	監視するOracleのORACLE_HOMEの内容を設定します。	/opt/app/9iee/product/9.2.0

■定義例

```
    :
########################################
# Oracle Information
[ORA]
DCAID="ORA"
INTERVAL = 5
SID = ORCL
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
    :
```

ポイント

二つ以上のOracleインスタンスを監視する場合は、以下の定義を行います。

1. セクションを追加し、パラメタを設定します。

   ー セクションは、テンプレート内で自由に定義可能ですが、セクション名がテンプレート内で重複しないように定義します。ここでは、「ORA2」というセクションを追加した例を記述します。

   ー 複数のOracleインスタンスを監視する場合も、「DCAID」キーの値は変更せず、「"ORA"」と定義してください。

   ■定義例

```
    :
########################################
# Oracle Information
```

```
[ORA]
DCAID="ORA"
INTERVAL = 5
SID = ORCL
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
[ORA2]
DCAID="ORA"
INTERVAL = 5
SID = ORCL2
USERNAME = system
PASS = manager
VER = 9.2.0
ORAHOME="/opt/app/9iee/product/9.2.0"
    :
```

2. 「1.」で追加したセクションを、「ATTR::DB」セクションの「GROUP」キーに追加します。1.の例のように定義した場合には、以下のように修正します。

■定義前

```
    :
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
    :
```

■定義後

```
    :
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA,ORA2"
    :
```

2.1.1 Oracleの動的パフォーマンスビューにアクセスできるユーザーを新規で作成する方法

注意

当作業は、OracleのデフォルトのID/PASSWORDを使用する場合は必要ありません。

Oracleの動的パフォーマンスビューにアクセスできるユーザーを新規で作成する場合、以下のSQLコマンドをsvrmgrl等からOracleの管理者用ID（通常はsystem）で投入します。

以下の例では、id1というIDにパスワードpass1でその権限を与えています。

```
create user id1 identified by pass1;
grant dba to id1;
grant connect to id1;
```

2.2 Microsoft .NET Serverの管理設定

Microsoft .NET Serverを管理対象にする場合は、[ATTR::AP]セクションのGROUPキーに、DOTNETを追加します。

■定義前

```
    :
[ATTR::AP]
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT"
    :
```

■定義後

```
    :
[ATTR::AP]
GROUP="INTSG,SSC,DSA_JLA,UDATA,CNT,DOTNET"
    :
```

2.3 Microsoft SQL Serverの管理設定

Microsoft SQL Serverを管理対象にする場合は、[ATTR::DB]セクションのGROUPキーに、MSSQLを追加します。

■定義前

```
    :
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA"
    :
```

■定義後

```
    :
[ATTR::DB]
GROUP="SYMSAR,SYMPS,ORA,MSSQL"
    :
```

2.4 Enterprise Managerでのミドルウェア連携設定

Enterprise Manager上で、ミドルウェアの性能管理を行う場合は本設定を行ってください。

SERVERTYPEセクション内のパラメタをOFFの状態からONへ修正します。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥template.dat
```

【UNIX版】

```
/etc/opt/FJSVssqc/template.dat
```

■定義前

```
    :
[SERVERTYPE]
OS="ON"
DB="OFF"
AP="OFF"
PM="OFF"
WB="OFF"
TA="ON"
MG="ON"
    :
```

■定義例

- DBサーバの監視を行う場合

  DB="OFF"→DB="ON"

- APサーバの監視を行う場合

  AP="OFF"→AP="ON"

- WEBトランザクションの監視を行う場合

  WB="OFF"→WB="ON"

```
    :
[SERVERTYPE]
OS="ON"
DB="ON"
AP="ON"
PM="OFF"
```

```
WB="ON"
TA="ON"
MG="ON"
    :
```

■セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

2.5 ミドルウェアを管理対象から外す設定

ポリシー作成/ポリシー適用の実行時に自動的にミドルウェアが検出され、収集ポリシーに従ってミドルウェアが管理対象となります。

ミドルウェアを管理対象から外したい場合には、本設定を行ってください。

■格納場所

設定ファイルの格納場所は以下のとおりです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥template.dat
```

【UNIX版】

```
/etc/opt/FJSVssqc/template.dat
```

■設定方法

1. template.datの設定の変更

   本ファイルには、常時収集する項目が定義されており、ポリシー作成/ポリシー適用の実行時に本定義にしたがって自動的に収集ポリシーが作成されます。

   自動的に収集ポリシーが作成される以下のミドルウェアを管理対象から外したい場合には、本ファイル内の対応するパラメーターを削除してください。

管理対象	本ファイル内のセクション名	GROUPキーから削除するパラメーター
Interstage Application Server	[ATTR::AP]	INTSG
Interstage Service Integrator	[ATTR::AP]	ISI
Systemwalker Operation Manager	[ATTR::AP]	DSA_JLA
Systemwalker Resource Coordinator(Storage) ETERNUS SF Storage Cruiser	[ATTR::AP]	SSC
Symfoware Server	[ATTR::DB]	SYMSAR SYMPS

注意

template.datを修正する前には、必ずバックアップしてください。

管理対象のミドルウェアは、プラットフォーム、インストール種別によって異なります。そのため、template.datに管理対象でないミドルウェアのパラメーターは、存在しないことがあります。

「■設定方法」に記載のないパラメーターは変更しないでください。

2. セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

■設定例

「Interstage Application Server」を管理対象から外す場合は、以下のように[ATTR::AP]セクションのGROUPキーからINTSGパラメーターを削除します。

設定前

```
    :
[ATTR::AP]
GROUP="INTSG,SSC,DSA_JLA,DSA_TDA,UDATA,CNT,SNM,SAP,ISI"
    :
```

設定後

```
    :
[ATTR::AP]
GROUP="SSC,DSA_JLA,DSA_TDA,UDATA,CNT,SNM,SAP,ISI"
    :
```

第3章 インストールレス型Agent管理

本章では、Agentをインストールしていない被監視サーバをリモートで管理する方法について説明します。

インストールレス型Agentの機能については、解説書「2.4 インストールレス型Agentの運用モデル」「3.2.1.2 インストールレス型Agent」を参照してください。

インストール型Agentとインストールレス型Agentの違いについては、解説書「3.2.1 Agent」を参照してください。

■実行環境

Manager/Proxy Manager で実行可能です。

■実行に必要な権限

【Windows 版】

Administrators グループに所属するユーザー権限が必要です。

【UNIX 版】

システム管理者(スーパーユーザー)権限が必要です。

■通信方式

リモートで性能情報を収集するときの監視サーバと被監視サーバ（インストールレス型Agent）の通信方式は、telnetかsshを選択することができます。セキュリティを考慮した場合、sshでの運用を推奨します。

注意

- telnetを使用する場合、監視サーバから被監視サーバにtelnet(ポート番号23)で接続できるように環境を設定してください。
- sshを使用する場合、監視サーバから被監視サーバとssh(ポート番号22)で接続できるように環境を設定してください。

■システム時刻について

監視サーバと被監視サーバのシステム時刻は、同じ時刻になるように設定してください。

■管理対象

インストールレス型Agentで以下の性能管理を行うための設定について説明します。

- 3.1 サーバ性能管理
- 3.2 仮想資源管理

3.1 サーバ性能管理

■機能概要

サーバ性能管理では、Windows、Solaris、Linux、AIX、HP-UXのOSのCPU、メモリ、ディスクなどの性能情報を収集し、一元管理します。

インストール型Agentと比べて、インストールレス型Agentで収集する場合は、収集項目や収集間隔などの違いがあります。詳細は「3.1.5 インストール型Agentとインストールレス型Agentの違いについて」を参照してください。

■収集間隔

収集間隔は、5分です。

■手順

インストールレス型Agentでサーバ性能管理を行うための手順を以下の順に説明します。

3.1.1 前提条件

監視サーバ(Manager/Proxy Manger)と被監視サーバ(インストールレス型Agent)のハードウェアおよび動作OSについては、導入手引書「第2章 インストール条件と資源見積もり」を参照してください。

■必須ソフトウェア

監視サーバと被監視サーバ間の通信のために必要となるソフトウェアについて説明します。

通信方式	監視サーバ	被監視サーバ (インストールレス型Agent)
telnet	—	telnetサーバ
ssh	—	sshサーバ(※)

※) SSHで通信する場合、以下のソフトウェアが必要です。

- SSH V2.0以降
  - ー Windowsの場合

    SSHは標準機能としてインストールされていません。

    Microsoft(R) Windows 2000の場合は、OpenSSH for Windows(バージョン3.8.1p1以降)をインストールしてください。

    それ以外のOSの場合は、telnetで通信してください。
  - ー UNIXの場合

    Solaris9、Solaris10、Linux(Red Hat Enterprise Linux v.5)の場合は、OSの標準機能としてインストールされています。

■資源見積もり

接続セッション数

被監視サーバの性能情報を収集するために、被監視サーバ側で必要なtelnet/sshの接続セッション数を以下に説明します。

被監視サーバのプラットフォーム (インストールレス型Agent)	telnetまたはsshの 接続セッション数
Windows	2
Solaris	7
Linux	5
AIX	8

被監視サーバのプラットフォーム (インストールレス型Agent)	telnetまたはsshの接続セッション数
HP-UX	7

注意

- 接続セッションの合計数が多い場合、監視サーバのDCMサービス/デーモンの起動および停止に時間がかかる場合があります。
- ネットワークの状態が良くない環境（断続的に接続が切断されるなど）や被監視サーバがビジー状態にある場合は、telnetもしくはsshによる通信が正常に行われない可能性があります。常に正常な通信が行える環境で監視を行ってください。
- Windowsのtelnetの場合、デフォルトで同時に接続できるセッションの最大数は「2」です。そのため、「3.1.2 被監視サーバの設定」の手順に従って、同時に接続できるセッションの最大数を変更してください。
  UNIXのtelnetおよびsshの場合、デフォルトで同時に接続できるセッションの最大数の制限はありません。

空きディスク容量

被監視サーバの性能情報を収集するために、被監視サーバ側で必要な空きディスク容量を以下に説明します。

- 被監視サーバに必要な空きディスク容量：1MB

3.1.2 被監視サーバの設定

被監視サーバの性能情報を収集するために必要な設定について以下に説明します。

被監視サーバがWindowsの場合

■telnetで通信する場合

1. リモートで接続するためにユーザーを作成します。

   ユーザーは、「ユーザーは次回ログオン時にパスワードの変更が必要」を設定しないでください。

2. リモートで接続して情報を収集するために必要なグループ（「TelnetClients」グループと「Performance Monitor Users」グループ）をユーザーに追加します。

   以下の手順に従って、設定してください。

   a. 「TelnetClients」ローカルグループを作成します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

      3. グループ「TelnetClients」が詳細ウィンドウにすでに存在する場合は、次の手順をスキップして、「b. ユーザーを「TelnetClients」グループに追加します。」を実施してください。

      4. [グループ]を右クリックし、[新しいグループ]をクリックします。

      5. [新しいグループ]ダイアログボックスに、「TelnetClients」と入力します。必要に応じて、説明を追加できます。

      6. ユーザーを作成済みの場合、[追加]をクリックして、[ユーザー、コンピュータ、またはグループの選択]ダイアログボックスにユーザー名を入力します。

      7. [作成]をクリックします。

   b. ユーザーを「TelnetClients」グループに追加します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

3. 「TelnetClients」グループをダブルクリックします。

4. [追加]をクリックします。

5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「TelnetClients」グループにユーザーを追加し、[OK]をクリックします。

c. ユーザーを「Performance Monitor Users」グループに追加します。

1. [コンピュータの管理]を開きます。

2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

3. 「Performance Monitor Users」グループをダブルクリックします。

4. [追加]をクリックします。

5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「Performance Monitor Users」グループにユーザーを追加し、[OK]をクリックします。

注意

- セキュリティの観点から「Administrators」グループに所属するユーザーは使用しないことを推奨します。
- コンピュータの管理を開くには、[スタート]ボタン、[コントロール パネル]の順にクリックし、[管理ツール]、[コンピュータの管理]の順にダブルクリックします。
- グループ名「TelnetClients」のスペルは、表示どおりに作成してください。
- 「TelnetClients」グループを作成した後は、「Telnet サーバー」サービスを停止して開始するまでユーザーはログオンできません。

3. 「Telnet」サービスを自動起動に設定します。

Windows Server® 2003の場合
「Telnet」サービスを自動起動に設定します。

注意

「Telnet」サービスは、デフォルトでは自動起動に設定されていません。

a. [コンピュータの管理]を開きます。

b. コンソール ツリーで、[サービス] をクリックします。

c. 「Telnet」サービスをダブルクリックします。

d. スタートアップの種類を[自動]にし、サービス状態を[開始]にし、[OK]をクリックします。

Windows Server® 2008の場合
「Telnet サーバー」機能を有効化し、「Telnet」サービスを自動起動に設定します。

注意

「Telnet サーバー」機能は、デフォルトでは無効化されています。

また、「Telnet」サービスは、デフォルトでは自動起動に設定されていません。

「Telnet サーバー」機能を有効化し、「Telnet」サービスを自動起動する手順は以下のとおりです。

a. Windowsの[サーバー マネージャー]を起動します。

b. 左側のツリーで[機能]を選択し、右側の画面で[機能の追加]をクリックします。

c. [Telnet サーバー]を選択し、[次へ]をクリックします。

d. [インストール]をクリックします。

インストールが完了したら、Windowsの[サービス]を起動し、[Telnet]サービスを自動起動に設定する手順は以下のとおりです。

a. [コンピュータの管理]を開きます。

b. コンソール ツリーで、[サービス] をクリックします。

c. 「Telnet」サービスをダブルクリックします。

d. スタートアップの種類を[自動]にし、サービス状態を[開始]にし、[OK]をクリックします。

4. 「Telnet」サービスの同時に接続できるセッションの最大数を変更します。

「Telnet」サービスは、デフォルトの同時に接続できるセッションの最大数は「2」です。
「接続セッション数」に記載されている必要なセッション数を考慮して、最大数を設定します。

Windowsの「tlntadmn」コマンドで同時に接続できるセッションの最大数を設定します。

```
tlntadmn config maxconn=<接続セッションの最大数>
```

注意

Windows Server® 2008で実行する場合は、管理者権限で実行する必要があります。[スタート]メニューから、[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]メニューを右クリックし、[管理者として実行]を選択してコマンドプロンプトを起動してください。そこで以下に説明するコマンドを実行してください。

```
tlntadmn config maxconn=<接続セッションの最大数>
```

5. 新しく作成したユーザーでコンピュータにログオンします。

注意

リモートで接続して情報を収集するためには、接続するユーザーのユーザー・プロファイルが必要です。そのために、接続するユーザーでWindowsのコンピュータに必ずログオンしてください。

6. 設定したサーバに、telnetで接続し、作成したユーザーでログインできることを確認してください。

■sshで通信する場合

1. リモートで接続するためにユーザーを作成します。

ユーザーは、「ユーザーは次回ログオン時にパスワードの変更が必要」を設定しないでください。

2. リモートで接続して情報を収集するために必要なグループ(「Performance Monitor Users」グループ)をユーザーに追加します。

以下の手順に従って、設定してください。

a. ユーザーを「Performance Monitor Users」グループに追加します。

1. [コンピュータの管理]を開きます。

2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

3. 「Performance Monitor Users」グループをダブルクリックします。

4. [追加]をクリックします。

5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「Performance Monitor Users」グループにユーザーを追加し、[OK]をクリックします。

注意

- セキュリティの観点から「Administrators」グループに所属するユーザーは使用しないことを推奨します。
- コンピュータの管理を開くには、[スタート]ボタン、[コントロール パネル]の順にクリックし、[管理ツール]、[コンピュータの管理]の順にダブルクリックします。

3. 「OpenSSH for Windows」をインストールし、アクセス許可の設定、sshサービスを起動します。

   設定手順の例は以下のとおりです。

注意

インストールやサービスの起動、設定方法の詳細は、「OpenSSH for Windows」のマニュアルを参照してください。

   a. コマンドプロンプトを開き、カレントディレクトリを<OpenSSHのインストールディレクトリ>¥binに移動します。

```
cd <OpenSSHのインストールディレクトリ>¥bin
```

   b. グループ権限ファイルを作成します。下記の設定により、Windowsのローカルグループのみ許可します。

```
mkgroup -l >> ..¥etc¥group
```

   c. ユーザ権限ファイルを作成します。下記の設定により、Windowsのローカルグループの新しく作成したユーザにアクセスを許可します。

```
mkpasswd -l -u [ユーザー名] >> ..¥etc¥passwd
```

   d. サービスで[OpenSSH Server]サービスを起動します。

4. 新しく作成したユーザーでコンピュータにログオンします。

注意

リモートで接続して情報を収集するためには、接続するユーザーのユーザー・プロファイルが必要です。そのために、接続するユーザーでWindowsのコンピュータに必ずログオンしてください。

5. 設定したサーバに、sshで接続し、作成したユーザーでログインできることを確認してください。

被監視サーバがUNIXの場合

■telnetで通信する場合

1. リモートで接続するためにユーザーを作成します。そのときに、ユーザーのホームディレクトリを設定してください。

   例えば、useraddまたはusermodコマンドを使う場合は、-dオプションなどでユーザーのホームディレクトリを設定してください。また、ホームディレクトリが存在しない場合は、ホームディレクトリを作成してください。ホームディレクトリには、ユーザーの書き込みできる権限を設定してください。

注意

被監視サーバがAIXの場合、sarコマンドを実行するためには、admグループに登録されているユーザーが必要です。
リモートで接続するためのユーザーがrootでない場合、ユーザーをadmグループに登録してください。

2. telnetデーモンを自動起動に設定します。

   デーモンの起動、設定方法は、telnetのマニュアルを参照してください。

3. 設定したサーバに、telnetで接続し、作成したユーザーでログインできることを確認してください。また、ログインしたときのカレントディレクトリが、作成したホームディレクトリになっていることを確認してください。

■sshで通信する場合

1. リモートで接続するためにユーザーを作成します。そのときに、ユーザーのホームディレクトリを設定してください。

   例えば、useraddまたはusermodコマンドを使う場合は、-dオプションなどでユーザーのホームディレクトリを設定してください。また、ホームディレクトリが存在しない場合は、ホームディレクトリを作成してください。ホームディレクトリには、ユーザーの書き込みできる権限を設定してください。

注意

被監視サーバがAIXの場合、sarコマンドを実行するためには、admグループに登録されているユーザーが必要です。
リモートで接続するためのユーザーがrootでない場合、ユーザーをadmグループに登録してください。

2. sshデーモンを自動起動に設定します。

   sshがインストールされていない環境では、SSH(またはOpenSSH)をインストールしてください。
   インストール方法やデーモンの起動、設定方法は、sshのマニュアルを参照してください。

3. 設定したサーバに、sshで接続し、作成したユーザーでログインできることを確認してください。また、ログインしたときのカレントディレクトリが、作成したホームディレクトリになっていることを確認してください。

3.1.3 監視サーバの設定

監視サーバの設定の手順を以下の順に説明します。

1. 定義方法
2. セットアップ

3.1.3.1 定義方法

被監視サーバ から性能情報を収集するには、以下に示す2つの定義ファイルが必要です。

- 接続アカウント定義ファイル
- リモート監視定義ファイル

3.1.3.1.1 接続アカウント定義ファイル

監視サーバと被監視サーバのtelnet/ssh通信の接続に関する設定を定義します。

接続アカウント定義ファイル(remoteAccount.txt)を編集します。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows 版】

<可変ファイル格納ディレクトリ>¥control¥remoteAccount.txt

【UNIX 版】

/etc/opt/FJSVssqc/remoteAccount.txt

上記ファイルを以下の定義方法に従って編集してください。

■定義方法

本ファイルはiniファイル形式です。

監視サーバと被監視サーバの通信のための接続アカウントのグループ単位にセクションを設定します。

通信方式により定義方法が異なります。通信方式に合わせて編集してください。

1. 通信方式がtelnetの場合

No	項目	必須/任意	形式	説明
-	[ACCOUNT]	必須	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)のみで63文字以内	セクション名として任意のアカウントグループの名前を設定します。 セクション名は一意の文字列になるように設定してください。
1	CONNECT TYPE	必須	TELNET	インストールレス機能で接続する際の接続方式を設定します。 telnet接続のため、「TELNET」を設定します。
2	USER	必須	64文字以内 以下の文字は使用不可 ¥/[];:|<>+=,?*@.	telnet接続用のログインアカウントを設定します。
3	PASSWORD	必須	genpwdで作成した文字列 ※1	telnet接続用のパスワードを設定します。

※1 genpwd(パスワード暗号化コマンド)の使用方法は、「A.6 genpwd(パスワード暗号化コマンド)」を参照してください。

2. 通信方式がsshの場合

No	項目	必須/任意	形式	説明
-	[ACCOUNT]	必須	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)のみで63文字以内	セクション名として任意のアカウントグループの名前を設定します。 セクション名は一意の文字列になるように設定してください。
1	CONNECT TYPE	必須	SSH	インストールレス機能で接続する際の接続方式を設定します。 ssh接続のため、「SSH」を設定します。

No	項目	必須/任意	形式	説明
2	USER	必須	64文字以内 以下の文字は使用不可 ¥/[];:|<>+=,?*@.	ssh接続用のアカウントを設定します。
3	PASSWORD	任意	genpwdで作成した文字列 ※1	ssh接続用のパスワードを設定します。

※1 genpwd(パスワード暗号化コマンド)の使用方法は、「A.6 genpwd(パスワード暗号化コマンド)」を参照してください。

■定義例

通信方式がtelnet、sshの場合の定義例は以下の通りです。

```
#通信方式がtelnetの場合
[TELNET-ACCOUNT1]
CONNECTTYPE=TELNET
USER=telnetuser
PASSWORD=C5sJGBE3ONs=
#通信方式がsshの場合
[SSH-ACCOUNT2]
CONNECTTYPE=SSH
USER=sshuser
PASSWORD=6zAp+gTGDzHyzswPuANqsw==
```

3.1.3.1.2　リモート監視定義ファイル

被監視サーバに関する設定を定義します。

リモート監視定義ファイル(remoteAgent.txt)を編集します。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows 版】

```
<可変ファイル格納ディレクトリ>¥control¥remoteAgent.txt
```

【UNIX 版】

```
/etc/opt/FJSVssqc/remoteAgent.txt
```

上記ファイルを以下の定義方法に従って編集してください。

■定義方法

本ファイルはiniファイル形式です。

被監視サーバ単位にセクションを設定します。

No	項目	必須/任意	形式	説明
-	[HOSTNAME]	必須	半角英数字および半角の -(ハイフン)、. (ドット)、#(シャープ)のみで63文字以内	セクション名として任意のセクション名を設定します。 セクション名は一意の文字列になるように設定してください。 ホスト名を指定することをお勧めします。
1	HOSTNAME	必須	半角英数字および半角の -(ハイフン)、. (ドット)、#(シャープ)のみで63文字以内	被監視サーバに接続するためのIPアドレス、または、ホスト名を指定します。
2	DISPLAYNAME	任意	半角英数字および半角の -(ハイフン)、. (ドット)、#(シャープ)のみで63文字以内	SQCコンソール画面で表示されるシステム名を指定します。 ※指定がない場合は、HOSTNAMEがシステム名になります。
3	OSTYPE	任意	WINDOWS LINUX SOLARIS AIX HP-UX	監視対象ホストのOS種別 WINDOWS : Windowsの場合 LINUX : Linuxの場合 SOLARIS : Solarisの場合 AIX : AIXの場合 HP-UX : HP-UXの場合 ※指定がない場合は、監視サーバと同じOS種別になります。
4	ACCOUNT	必須	半角英数字および半角の -(ハイフン)、. (ドット)、#(シャープ)のみで63文字以内	被監視サーバとの通信のための接続アカウントを指定します。 「接続アカウント定義ファイル(remortAccount.txt)」で設定したアカウントグループのセクション名を指定します。
5	CONNECTION	任意	ON or OFF	監視のON/OFFを指定します。 監視を停止する場合は、「OFF」を指定します。 ※指定がない場合は「ON」になります。

■定義例

通信方式がtelnet、sshの場合の定義例は以下の通りです。

```
# 監視サーバがSolarisの場合
[host1]
HOSTNAME=host1
OSTYPE=SOLARIS
ACCOUNT=TELNET-ACCOUNT1
# 監視サーバがLinuxの場合
# 本監視サーバを監視しないようにする場合
[linux-host2]
HOSTNAME=192.168.1.2
```

```
DISPLAYNAME=host2
OSTYPE=LINUX
ACCOUNT=SSH-ACCOUNT2
CONNECTION=OFF
```

3.1.3.2　セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

ポイント

セットアップ時に、定義ファイルに記述された文字列のチェックを行います。被監視サーバに接続できるかどうかの確認は、サービスを実行して行ってください。接続できない被監視サーバについては、性能情報収集の実行時にイベントログに警告メッセージが出力されます。リファレンスマニュアル「5.1 共通メッセージ」を参照し対処を行ってください。

定義ファイル「接続アカウント定義ファイル」「リモート監視定義ファイル」に設定された内容に誤りがある場合、誤った定義がおこなわれている被監視サーバについては管理の対象となりません。

sqcSetPolicyを実行した際、定義の誤りにより管理の対象から外される被監視サーバについては、以下のメッセージを出力します。

```
(Warning) : <Install-less Agent> ignored section name[セクション名]
```

セクション名には「リモート監視定義ファイル」に定義されたセクション名を出力します。

また、定義ファイルに1つでもエラーがある場合は、以下のメッセージを出力します。

```
(Warning) : <Install-less Agent> There is an error in definition.
Please confirm the file (ファイル名).
```

ファイル名には以下を出力します。

【Windows 版】

```
<可変ファイル格納ディレクトリ>¥log¥setpolicy_error.log
```

【UNIX 版】

```
/var/opt/FJSVssqc/setpolicy_error.log
```

メッセージが表示された場合、ファイルの内容を確認し、ファイルに記述されているメッセージをもとに定義ファイル「接続アカウント定義ファイル」「リモート監視定義ファイル」を修正して、再度セットアップを実行してください。ファイルに出力されるメッセージについては、リファレンスマニュアルの「1.1.3 sqcSetPolicy(ポリシー適用コマンド)」を参照してください。

なお、収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書（コンソール編）の「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

注意

- Manager/Proxy Managerのサービスを起動してから、コンソールの「UnregisteredAgentsフォルダ」に表示されるまで、15～20分程度かかります。

表示されない場合、Manager/Proxy Managerのイベントログ/syslogにメッセージが出力されていないか確認してください。

- インストールレス型Agent管理では、監視を行うために必要なディレクトリおよびファイルを被監視サーバに作成します。
  ディレクトリおよびファイルが作成される場所は以下のとおりです。

  ー 被監視サーバがWindowsの場合
  %USERPROFILE%¥sqc_tempディレクトリ
  %USERPROFILE% : ユーザープロファイルフォルダのパス名

  ー 被監視サーバがUNIXの場合
  ユーザーのホームディレクトリ

  作成されるディレクトリの名前は以下のとおりです。
  dsa_temp_***
  監視中は、上記のディレクトリを削除しないでください。ディレクトリを削除すると、性能情報が収集されなくなります。
  もし、ディレクトリを削除してしまった場合は、Manager/Proxy Managerのサービスを再起動してください。
  監視対象から外した場合は、上記のディレクトリを削除してください。

3.1.4 表示

インストールレス型Agentで収集したOSの性能情報は、以下の方法で表示することができます。

サマリ画面

サマリツリーの「ServerMonitor」ノードを選択することで表示できます。

詳細画面

詳細ツリーの「Windows」「Solaris」「Linux」「AIX」「HP-UX」ノードを選択することで表示できます。

レポート画面

総点検分析・レポート

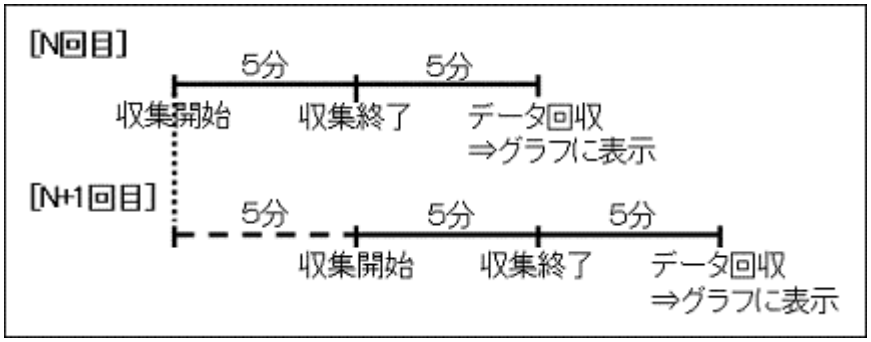
カテゴリ別診断分析・レポート

詳細分析・レポート

注意

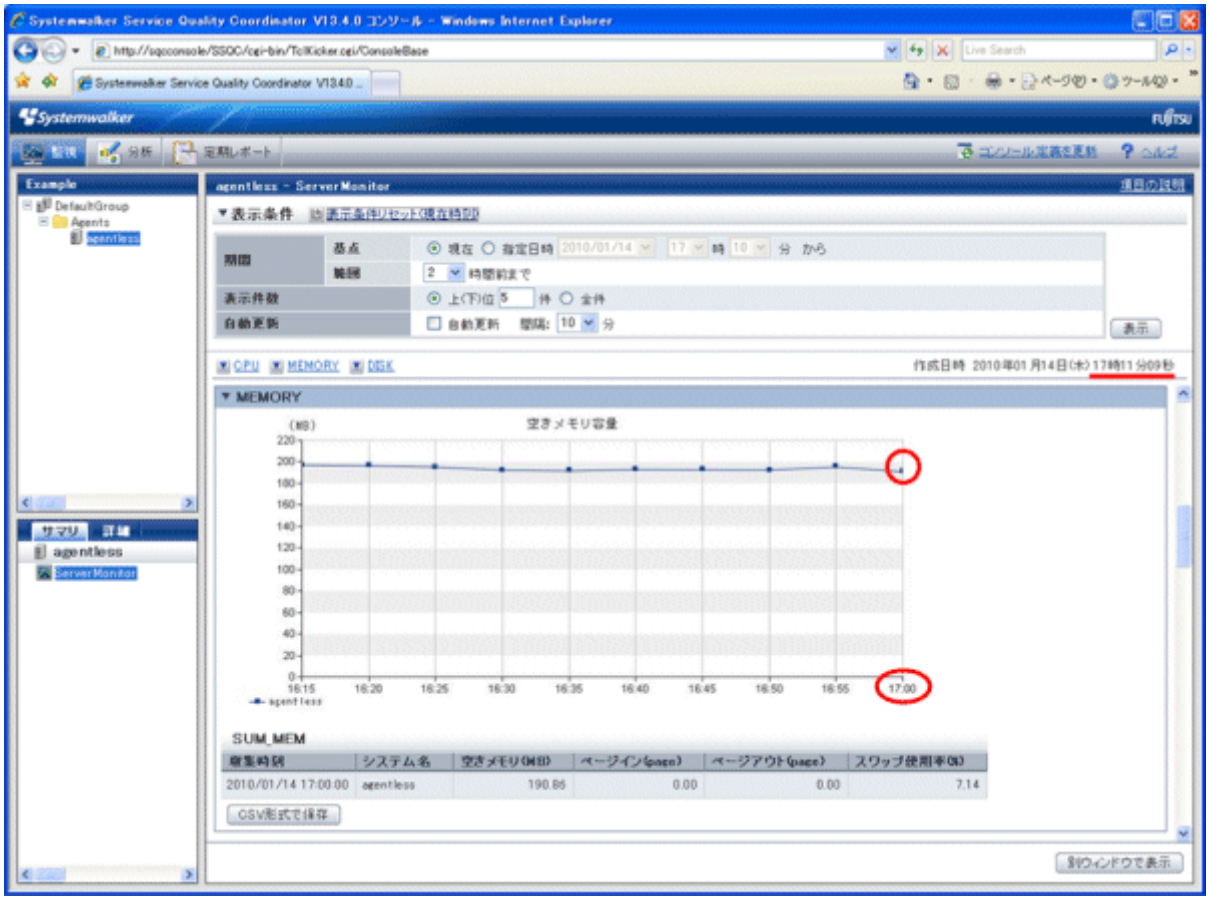
- 総点検レポート、カテゴリ別診断レポートは、レポートタイトルに「Windows」または「UNIX」を含むレポートを表示することができます。ただし、「Windows プロセス」「UNIXプロセス」のレポートは表示できません。

- サマリ画面でデータを表示した場合、データの表示が10～15分程度遅れているように見えます。
  これはインストールレス型Agentの場合、以下の流れでデータが収集されるためです。



【例 17:00データの場合】

17:00	収集を開始
17:05	収集を終了
17:10	Manager/Proxy Managreが性能データを回収 このとき、17:00のデータとしてコンソールに表示されます(収集開始の時刻を基準として表示しています。17:00データの値は17:00から17:05までの平均値となります)。 次の性能データの回収まで、5分間(17:15ごろまで)この状態が続きます。



・ Manager/Proxy Managerのサービスを起動したあと、最初の収集タイミングに被監視サーバ側にスクリプトを送るため、15分～20分程度後に最初のデータが表示されます。

3.1.5 インストール型Agentとインストールレス型Agentの違いについて

インストール型Agentとインストールレス型Agentの違いについて説明します。

■収集間隔

収集間隔の違いは以下のとおりです。

Agent種別	収集間隔
インストール型Agent	1分

Agent種別	収集間隔
インストールレス型Agent	5分

■収集項目

インストール型Agentとインストールレス型Agentでは、収集するOSの性能情報の値が異なります。

主な収集項目の違いは以下のとおりです。

Agent種別	主な収集項目
インストール型Agent	CPU、メモリ、ディスク、ネットワーク、プロセス、IPC資源
インストールレス型Agent	CPU、メモリ、ディスク

レコードIDごとの詳細な収集項目の違いは以下のとおりです。
レコードIDについては、リファレンスマニュアルの「第4章 データフォーマット」を参照してください。

インストール型Agent：Ag、インストールレス型Agent：Agl
○：収集する ×：収集しない －：該当する収集項目が存在しない

データの種類	レコードID	Windows		Solaris		Linux		AIX		HP-UX	
		Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl
サマリデータ	SUM_PROC	○	○	○	○	○	○	○	○	○	○
	SUM_MEM	○	○	○	○	○	○	○	○	○	○
	SUM_DISK	○	○	○	○	○	○	○	○	○	○
リソースデータ	WIN_DISKSPACE	○	○	－	－	－	－	－	－	－	－
	WIN_PROCESS	○	×	－	－	－	－	－	－	－	－
	WIN_LOGDISKBUSY	○	○	－	－	－	－	－	－	－	－
	WIN_PHYDISKBUSY	○	○	－	－	－	－	－	－	－	－
	WIN_MEMORY	○	○	－	－	－	－	－	－	－	－
	WIN_PAGEFILE	○	○	－	－	－	－	－	－	－	－
	WIN_CPUBUSY	○	○	－	－	－	－	－	－	－	－
	WIN_NET_INTERFACE	○	×	－	－	－	－	－	－	－	－
	WIN_NET_SYSTEM	○	×	－	－	－	－	－	－	－	－
	WIN_SYSTEM	○	○	－	－	－	－	－	－	－	－
	UX_DISKSPACE	－	－	○	○	○	○	○	○	○	○
	UX_SYSCALLS	－	－	○	○	○	○	○	○	○	○
	UX_FILEIO	－	－	○	○	－	－	○	○	○	○
	UX_MQSEMA	－	－	○	○	－	－	○	○	○	○
	UX_PAGING	－	－	○	○	○	○	○	○	○	○
	UX_CPUQUEUE	－	－	○	○	○	○	○	○	○	○
	UX_MEMFREE	－	－	○	○	○	○	○	○	○	○

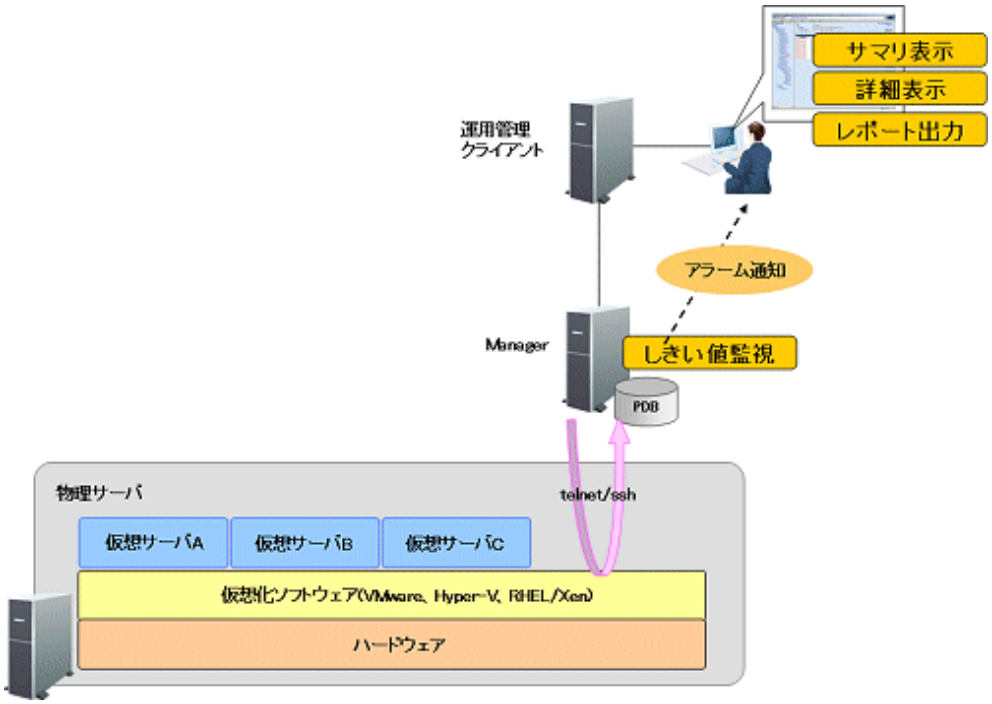
データの種類	レコードID	Windows		Solaris		Linux		AIX		HP-UX	
		Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl	Ag	Agl
	UX_SYSTBLS	－	－	○	○	○	○	○	○	○	○
	UX_SWAPIO	－	－	○	○	○	○	○	○	○	○
	UX_PROCESS	－	－	○	×	○	×	○	×	○	×
	UX_NET_INTERFACE	－	－	○	×	○	×	○	×	○	×
	UX_NET_SYSTEM	－	－	○	×	○	×	○	×	○	×
	UX_DISKBUSY	－	－	○	○	○	○	○	○	○	○
	UX_CPUBUSY	－	－	○	○	○	○	○	○	○	○
	UX_SWAPSTATUS	－	－	○	○	○	○	○	○	○	○
	UX_SWAPUSAGE	－	－	○	○	－	－	○	○	○	○
	UX_SYS_PAGINGDETAIL	－	－	○	○	－	－	－	－	－	－
	UX_KMA	－	－	○	○	－	－	－	－	－	－
	UX_IPCSMQ	－	－	○	×	○	×	○	×	○	×
	UX_IPCSMQSUM	－	－	○	×	○	×	○	×	○	×
	UX_IPCSSM	－	－	○	×	○	×	○	×	○	×
	UX_IPCSSMSUM	－	－	○	×	○	×	○	×	○	×
	UX_IPCSSEM	－	－	○	×	○	×	○	×	○	×
	UX_IPCSSEMSUM	－	－	○	×	○	×	○	×	○	×
	UX_ZONE	－	－	○	×	－	－	－	－	－	－
	UX_CPUSTAT_CORE	－	－	○	×	－	－	－	－	－	－
	LX_DISKBUSY	－	－	－	－	○	○	－	－	－	－
	LX_MEMFREE	－	－	－	－	○	○	－	－	－	－
	LX_SYSTBLS	－	－	－	－	○	○	－	－	－	－
	LX_PAGING	－	－	－	－	○	○	－	－	－	－
	LX_CPUQUEUE	－	－	－	－	○	○	－	－	－	－
	LX_MEMORY	－	－	－	－	○	○	－	－	－	－
	AX_DISKBUSY	－	－	－	－	－	－	○	○	－	－
	AX_KERNELPROC	－	－	－	－	－	－	○	○	－	－
	AX_PAGING	－	－	－	－	－	－	○	○	－	－
	HP_PAGING	－	－	－	－	－	－	－	－	○	○

3.2 仮想資源管理

■機能概要

仮想資源管理では、OSや仮想化ソフトウェアから物理サーバ、仮想サーバの性能情報を収集し、一元管理します。
本機能で収集した仮想サーバの性能情報を、物理サーバの性能情報と突き合わせて総合的に判断することによって、サーバ内でのリソースを最適化でき、利用効率の向上を図ることができます。

- 物理サーバの性能情報をレポートとして表示します。これにより、物理サーバのCPU、メモリ、ディスクの使用状況を把握できます。
- 仮想サーバの性能情報をゲスト単位で積み上げてレポートとして表示します。これにより、各ゲストのCPU、メモリ、ディスクの使用状況を把握できます。



■収集できる情報

- 仮想化ソフトウェアからインストールレス型Agentの機能を使って、telnetやsshでリモートから接続して、物理サーバや仮想サーバの性能情報を収集します。

  収集できる性能情報は、監視対象の仮想化ソフトウェアによって異なります。

  監視対象の仮想化ソフトウェアについて、物理サーバ、仮想サーバの性能情報を収集する方法と主な性能情報は以下のとおりです。

仮想化ソフトウェア	物理サーバ	仮想サーバ
VMware	VMwareから、CPU／メモリ／ディスクの性能情報を収集します。	VMwareから、CPU／メモリ／ディスクの性能情報を収集します。
Hyper-V	Hyper-Vから、CPUの性能情報を収集します。 ホストOS(Windows)から、メモリ／ディスクの性能情報を収集します。	Hyper-Vから、CPUの性能情報を収集します。
Red Hat仮想化機能	ホストOS(Linux)から、CPU／メモリ／ディスクの性能情報を収集します。	Xenから、CPU／メモリ／ディスクの性能情報を収集します。

注意

- Hyper-Vを監視対象とした場合、ホストOSのWindowsの性能情報も収集されます。
  ただし、Hyper-Vのホスト OS(Windows)から取得したCPUの性能情報は値が正しくありません。物理サーバのCPUの性能情報を確認したい場合は、Hyper-Vから取得したCPUの性能情報の値を確認してください。
- Red Hat仮想化機能を監視対象とした場合、ホストOSのLinuxの性能情報も収集されます。

- 仮想サーバのリソースを積み上げてレポートとして表示します。

・ 各情報に対して、しきい値監視を行い、監視項目の値が定義値を超えた場合は、アラームを通知できます。

■収集間隔

収集間隔は、5分です。

■手順

インストールレス型Agentで仮想資源管理を行うための手順を以下の順に説明します。

3.2.1 前提条件

■必須ソフトウェア

監視サーバと被監視サーバ間の通信のために必要となるソフトウェアについて説明します。

通信方式	監視サーバ	被監視サーバ (インストールレス型Agent)
telnet	—	telnetサーバ
ssh	—	sshサーバ(※)

※) SSHで通信する場合、以下のソフトウェアが必要です。

・ SSH V2.0以降

－ Hyper-V(Windows)の場合

telnetで通信してください。

－ VMware、Red Hat仮想化機能の場合

標準機能としてインストールされているsshを使用してください。

■収集できる条件

・ VMwareの場合:
性能情報を収集するためのコマンド(esxtop)が利用できる状態でなければなりません。

・ Hyper-Vの場合:
性能情報を収集するためのコマンド(typeperf)が利用できる状態でなければなりません。

・ Red Hat仮想化機能の場合:
性能情報を収集するためのコマンド(xentop)が利用できる状態でなければなりません。

■資源見積もり

接続セッション数

被監視サーバの性能情報を収集するために、被監視サーバ側で必要なtelnet/sshの接続セッション数を以下に説明します。

被監視サーバのプラットフォーム (インストールレス型Agent)	telnetまたはsshの接続セッション数
VMware	1
Hyper-V	3
Red Hat 仮想化機能	6

注意

- 接続セッションの合計数が多い場合、監視サーバのDCMサービス/デーモンの起動および停止に時間がかかる場合があります。
- ネットワークの状態が良くない環境（断続的に接続が切断されるなど）や被監視サーバがビジー状態にある場合は、telnetもしくはsshによる通信が正常に行われない可能性があります。常に正常な通信が行える環境で監視を行ってください。
- Hyper-V(Windows)のtelnetの場合、デフォルトで同時に接続できるセッションの最大数は「2」です。そのため、「3.2.2 被監視サーバの設定」の手順に従って、同時に接続できるセッションの最大数を変更してください。
  VMware/Red Hat 仮想化機能(UNIX)のsshの場合、デフォルトで同時に接続できるセッションの最大数の制限はありません。

空きディスク容量

被監視サーバの性能情報を収集するために、被監視サーバ側で必要な空きディスク容量を以下に説明します。

- 被監視サーバに必要な空きディスク容量：1MB

3.2.2 被監視サーバの設定

被監視サーバがVMwareの場合

■sshで通信する場合

1. リモートで接続するためにユーザーを作成します。

   a. VMware ClientでVMware ESXホストに直接ログインします。

   ・ESX 3.5の場合
   VMware Infrastructure ClientでVMware ESXホストに直接ログインします。

   ・ESX 4.0の場合
   VMware vSphere ClientでVMware ESXホストに直接ログインします。

   注意

   ・ESX 3.5の場合
   VirtualCenterにログインした場合は、ユーザーの作成はできません。VMware ESXホストに直接ログインしてください。

・ESX 4.0の場合
vCenter Serverにログインした場合は、ユーザーの作成はできません。VMware ESXホストに直接ログインしてください。

b. 左ペインからサーバを選択します。

c. [ユーザーおよびグループ(Users & Groups)]タブをクリックして、[ユーザー(Users)]をクリックします。

d. ユーザーテーブル上で右クリックして、[追加(Add)]をクリックします。

e. [新規ユーザーの追加(Add New User)]ダイアログが開きます。

f. ログイン、ユーザー名、数値のユーザーID(UID)、パスワードを設定します。

g. [このユーザーへのシェル アクセスの許可(Grant shell access to this user)]を選択します。

h. グループはユーザーを追加する既存の各グループに対して、グループ名を入力して、[追加(Add)]をクリックします。

i. [OK]をクリックします。

2. SSHサーバを自動起動に設定します。

ポイント

デフォルトでは、VMware ESXのSSHサーバは自動起動するように設定されています。

SSHサーバの起動、設定方法は、VMwareのマニュアルを参照してください。

3. 設定したサーバに、sshで接続し、作成したユーザーでログインできることを確認してください。

4. 作成したユーザーに性能情報を収集するために使用するコマンドを実行する権限を追加します。

ユーザーにコマンドを実行する権限を与えるために、以下の設定を実施してください。

a. VMwareにログインし、スーパーユーザーになります。

b. visudoコマンドを実行し、sudoersファイルを編集します。

```
# /usr/sbin/visudo
```

c. sudoersファイルの最後に以下の行を追加して、保存します。
以下は、接続アカウントが「user1」の場合の設定例です。接続アカウントにあわせて変更してください。

【設定例】

```
user1 ALL=(ALL) NOPASSWD: /usr/bin/esxtop
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
user1 ALL=(ALL) NOPASSWD: /usr/sbin/vdf
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
user1 ALL=(ALL) NOPASSWD: /bin/egrep
user1 ALL=(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

d. 接続アカウントでログインして、「sudo -l」コマンドを実行します。

```
$ sudo -l
```

【実行結果例】

```
$ sudo -l
User user1 may run the following commands on this host:
    (ALL) NOPASSWD: /usr/bin/esxtop
    (ALL) NOPASSWD: /usr/sbin/esxcfg-vmhbadevs
```

```
(ALL) NOPASSWD: /usr/sbin/vdf
(ALL) NOPASSWD: /usr/sbin/esxcfg-nics
(ALL) NOPASSWD: /usr/sbin/esxcfg-vswitch
(ALL) NOPASSWD: /bin/egrep
(ALL) NOPASSWD: /usr/sbin/esxcfg-scsidevs
```

被監視サーバがHyper-Vの場合

■telnetで通信する場合

1. リモートで接続するためにユーザーを作成します。

   ユーザーは、「ユーザーは次回ログオン時にパスワードの変更が必要」を設定しないでください。

2. リモートで接続して情報を収集するために必要なグループ(「TelnetClients」グループと「Performance Monitor Users」グループ)をユーザーに追加します。

   以下の手順に従って、設定してください。

   a. 「TelnetClients」ローカルグループを作成します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

      3. グループ「TelnetClients」が詳細ウィンドウにすでに存在する場合は、次の手順をスキップして、「b.ユーザーを「TelnetClients」グループに追加します。」を実施してください。

      4. [グループ]を右クリックし、[新しいグループ]をクリックします。

      5. [新しいグループ]ダイアログボックスに、「TelnetClients」と入力します。必要に応じて、説明を追加できます。

      6. ユーザーを作成済みの場合、[追加]をクリックして、[ユーザー、コンピュータ、またはグループの選択]ダイアログボックスにユーザー名を入力します。

      7. [作成]をクリックします。

   b. ユーザーを「TelnetClients」グループに追加します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

      3. 「TelnetClients」グループをダブルクリックします。

      4. [追加]をクリックします。

      5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「TelnetClients」グループにユーザーを追加し、[OK]をクリックします。

   c. ユーザーを「Performance Monitor Users」グループに追加します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

      3. 「Performance Monitor Users」グループをダブルクリックします。

      4. [追加]をクリックします。

      5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「Performance Monitor Users」グループにユーザーを追加し、[OK]をクリックします。

注意

- セキュリティの観点から「Administrators」グループに所属するユーザーは使用しないことを推奨します。

- コンピュータの管理を開くには、[スタート]ボタン、[コントロール パネル]の順にクリックし、[管理ツール]、[コンピュータの管理]の順にダブルクリックします。
- グループ名「TelnetClients」のスペルは、表示どおりに作成してください。
- 「TelnetClients」グループを作成した後は、「Telnet サーバー」サービスを停止して開始するまでユーザーはログオンできません。

3. 「Telnet」サービスを自動起動に設定します。

   「Telnet サーバー」機能を有効化し、「Telnet」サービスを自動起動に設定します。

   注意

   「Telnet サーバー」機能は、デフォルトでは無効化されています。

   また、「Telnet」サービスは、デフォルトでは自動起動に設定されていません。

   「Telnet サーバー」機能を有効化し、「Telnet」サービスを自動起動する手順は以下のとおりです。

   a. Windowsの[サーバー マネージャー]を起動します。
   b. 左側のツリーで[機能]を選択し、右側の画面で[機能の追加]をクリックします。
   c. [Telnet サーバー]を選択し、[次へ]をクリックします。
   d. [インストール]をクリックします。

   インストールが完了したら、Windowsの[サービス]を起動し、[Telnet]サービスを自動起動に設定する手順は以下のとおりです。

   a. [コンピュータの管理]を開きます。
   b. コンソール ツリーで、[サービス] をクリックします。
   c. 「Telnet」サービスをダブルクリックします。
   d. スタートアップの種類を[自動]にし、サービス状態を[開始]にし、[OK]をクリックします。

4. 「Telnet」サービスの同時に接続できるセッションの最大数を変更します。

   「Telnet」サービスは、デフォルトの同時に接続できるセッションの最大数は「2」です。
   「接続セッション数」に記載されている必要なセッション数を考慮して、最大数を設定します。

   Windowsの「tlntadmn」コマンドで同時に接続できるセッションの最大数を設定します。

   ```
   tlntadmn config maxconn=<接続セッションの最大数>
   ```

   注意

   管理者権限で実行する必要があります。[スタート]メニューから、[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]メニューを右クリックし、[管理者として実行]を選択してコマンドプロンプトを起動してください。そこで以下に説明するコマンドを実行してください。

   ```
   tlntadmn config maxconn=<接続セッションの最大数>
   ```

5. 新しく作成したユーザーでコンピュータにログオンします。

注意

リモートで接続して情報を収集するためには、接続するユーザーのユーザー・プロファイルが必要です。そのために、接続するユーザーでWindowsのコンピュータに必ずログオンしてください。

6. 設定したサーバに、telnetで接続し、作成したユーザーでログインできることを確認してください。

■sshで通信する場合

1. リモートで接続するためにユーザーを作成します。

   ユーザーは、「ユーザーは次回ログオン時にパスワードの変更が必要」を設定しないでください。

2. リモートで接続して情報を収集するために必要なグループ(「Performance Monitor Users」グループ)をユーザーに追加します。

   以下の手順に従って、設定してください。

   a. ユーザーを「Performance Monitor Users」グループに追加します。

      1. [コンピュータの管理]を開きます。

      2. コンソール ツリーで、[ローカル ユーザーとグループ] を展開し、[グループ] をクリックします。

      3. 「Performance Monitor Users」グループをダブルクリックします。

      4. [追加]をクリックします。

      5. [ユーザー、コンピュータまたはグループの選択]ボックスの指示に従って、「Performance Monitor Users」グループにユーザーを追加し、[OK]をクリックします。

注意

- セキュリティの観点から「Administrators」グループに所属するユーザーは使用しないことを推奨します。
- コンピュータの管理を開くには、[スタート]ボタン、[コントロール パネル]の順にクリックし、[管理ツール]、[コンピュータの管理]の順にダブルクリックします。

3. 「OpenSSH for Windows」をインストールし、アクセス許可の設定、sshサービスを起動します。

   設定手順の例は以下のとおりです。

注意

インストールやサービスの起動、設定方法の詳細は、「OpenSSH for Windows」のマニュアルを参照してください。

   a. コマンドプロンプトを開き、カレントディレクトリを<OpenSSHのインストールディレクトリ>¥binに移動します。

```
cd <OpenSSHのインストールディレクトリ>¥bin
```

   b. グループ権限ファイルを作成します。下記の設定により、Windowsのローカルグループのみ許可します。

```
mkgroup -l >> ..¥etc¥group
```

   c. ユーザ権限ファイルを作成します。下記の設定により、Windowsのローカルグループの新しく作成したユーザにアクセスを許可します。

```
mkpasswd -l -u [ユーザー名] >> ..¥etc¥passwd
```

   d. サービスで[OpenSSH Server]サービスを起動します。

4. 新しく作成したユーザーでコンピュータにログオンします。

注意

リモートで接続して情報を収集するためには、接続するユーザーのユーザー・プロファイルが必要です。そのために、接続するユーザーでWindowsのコンピュータに必ずログオンしてください。

5. 設定したサーバに、sshで接続し、作成したユーザーでログインできることを確認してください。

被監視サーバがRed Hat 仮想化機能の場合

■sshで通信する場合

1. リモートで接続するためにユーザーを作成します。
2. sshデーモンを自動起動に設定します。

   sshがインストールされていない環境では、sshをインストールしてください。
   インストール方法やデーモンの起動、設定方法は、sshのマニュアルを参照してください。
3. 設定したサーバに、sshで接続し、作成したユーザーでログインできることを確認してください。
4. 作成したユーザーに性能情報を収集するために使用するコマンドを実行する権限を追加します。

   ユーザーにコマンドを実行する権限を与えるために、以下の設定を実施してください。

   a. Red Hat 仮想化機能が動作しているLinuxサーバにログインし、スーパーユーザーになります。
   b. visudoコマンドを実行し、sudoersファイルを編集します。

   ```
   # /usr/sbin/visudo
   ```

   c. sudoersファイルの最後に以下の行を追加して、保存します。
   以下は、接続アカウントが「user1」の場合の設定例です。接続アカウントにあわせて変更してください。

   【設定例】

   ```
   user1 ALL=(ALL) NOPASSWD: /usr/sbin/xentop
   ```

   d. 接続アカウントでログインして、「sudo -l」コマンドを実行します。

   ```
   $ sudo -l
   ```

   【実行結果例】

   ```
   $ sudo -l
   User user1 may run the following commands on this host:
       (ALL) NOPASSWD: /usr/sbin/xentop
   ```

3.2.3 監視サーバの設定

監視サーバの設定の手順を以下の順に説明します。

1. 定義方法
2. セットアップ

3.2.3.1 定義方法

以下の順で定義します。

1. 接続アカウント定義ファイルの作成
2. リモート監視定義ファイルの作成

3.2.3.1.1　接続アカウント定義ファイルの作成

監視サーバと被監視サーバのtelnet/ssh通信の接続に関する設定を定義します。
接続アカウント定義ファイル(remoteAccount.txt)を編集します。

設定方法の詳細は、「3.1.3.1.1 接続アカウント定義ファイル」を参照してください。

3.2.3.1.2　リモート監視定義ファイルの作成

仮想サーバに関する設定を定義します。
リモート監視定義ファイル(remoteAgent.txt)を編集します。

ファイル格納場所

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥remoteAgent.txt

【UNIX版】

/etc/opt/FJSVssqc/remoteAgent.txt

ファイル形式

iniファイル形式

設定項目

被監視サーバ単位にセクションを設定します。

No	項目	必須/任意	形式	説明
-	[HOSTNAME]	必須	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)のみで63文字以内	セクション名として任意のセクション名を設定します。 セクション名は一意の文字列になるように設定してください。 ホスト名を指定することを推奨します。
1	HOSTNAME	必須	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)のみで63文字以内	被監視サーバに接続するためのIPアドレス、または、ホスト名を指定します。
2	DISPLAYNAME	任意	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)	SQCコンソール画面で表示されるホスト名を指定します。 ※指定がない場合は、HOSTNAMEがホスト名になります。

No	項目	必須/任意	形式	説明
			のみで63文字以内	
3	VMTYPE	任意	VMWARE HYPERV XEN	監視対象ホストの仮想サーバの種別 VMWARE : VMware ESXの場合 HYPERV : Hyper-Vの場合 XEN : Red Hat 仮想化機能の場合
4	ACCOUNT	必須	半角英数字および半角の - (ハイフン)、. (ドット)、# (シャープ)のみで63文字以内	被監視サーバとの通信のための接続アカウントを指定します。 「接続アカウント定義ファイル(remortAccount.txt)」で設定したユーザーグループのセクション名を指定します。
5	CONNECTION	任意	ON または OFF	監視のON/OFFを指定します。 監視を停止する場合は、「OFF」を指定します。 ※指定がない場合は、「ON」が設定されたものとみなします。

定義例

仮想サーバがVMware、Hyper-V、Red Hat 仮想化機能の場合の定義例を以下に示します。

```
# 監視サーバがVMwareの場合
[192.168.1.1]
HOSTNAME=192.168.1.1
DISPLAYNAME=vmware-host1
VMTYPE=VMWARE
ACOUNT=SSH-ACCOUNT1

# 監視サーバがHyper-Vの場合
[host2]
HOSTNAME=host2
VMTYPE=HYPERV
ACOUNT=TELNET-ACCOUNT2

# 監視サーバがRed Hat 仮想化機能で、監視しないようにする場合
[xen-host3]
HOSTNAME=192.168.1.2
DISPLAYNAME=host3
VMTYPE=XEN
ACOUNT=SSH-ACCOUNT3
CONNECTION=OFF
```

3.2.3.2　セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

ポイント

セットアップ時に、定義ファイルに記述された文字列のチェックを行います。被監視サーバに接続できるかどうかの確認はサービスを実行して行ってください。接続できない被監視サーバについては、性能情報収集の実行時にイベントログに警告メッセージが出力されます。リファレンスマニュアル「5.1 共通メッセージ」を参照し対処を行ってください。

定義ファイル「接続アカウント定義ファイル」「リモート監視定義ファイル」に設定された内容に誤りがある場合、誤った定義がおこなわれている被監視サーバについては管理の対象となりません。
sqcSetPolicyを実行した際、定義の誤りにより管理の対象から外される被監視サーバについては以下のメッセージを出力します。

```
(Warning) : <Install-less Agent> ignored section name[セクション名]
```

セクション名には「リモート監視定義ファイル」に定義されたセクション名を出力します。

また、定義ファイルに1つでもエラーがある場合は、以下のメッセージを出力します。

```
(Warning) : <Install-less Agent> There is an error in definition.
Please confirm the file (ファイル名).
```

ファイル名には以下を出力します。

【Windows 版】

```
<可変ファイル格納ディレクトリ>¥log¥setpolicy_error.log
```

【UNIX 版】

```
/var/opt/FJSVssqc/setpolicy_error.log
```

メッセージが表示された場合、ファイルの内容を確認し、ファイルに記述されているメッセージをもとに定義ファイル「接続アカウント定義ファイル」「リモート監視定義ファイル」を修正して、再度セットアップを実行してください。ファイルに出力されるメッセージについては、リファレンスマニュアルの「1.1.3 sqcSetPolicy(ポリシー適用コマンド)」を参照してください。

なお、収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書（コンソール編）の「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

注意

- Manager/Proxy Managerのサービスを起動してから、コンソールの「UnregisteredAgentsフォルダ」に表示されるまで、15～20分程度かかります。
  表示されない場合、Manager/Proxy Managerのイベントログ/syslogにメッセージが出力されていないか確認してください。
- インストールレス型Agent管理では、監視を行うために必要なディレクトリおよびファイルを被監視サーバに作成します。
  ディレクトリおよびファイルが作成される場所は以下のとおりです。

  ー 被監視サーバがHyper-Vの場合

  - telnetで通信する場合

    %USERPROFILE%¥SQC_TEMPディレクトリ

    %USERPROFILE% : ユーザープロファイルフォルダのパス名

  - sshで通信する場合

    %HOME%¥SQC_TEMPディレクトリ

%HOME% : ホームディレクトリのパス名

- 被監視サーバがVMware、Red Hat仮想化機能の場合

  ユーザーのホームディレクトリ

作成されるディレクトリの名前は以下のとおりです。

dsa_temp_***

監視中は、上記のディレクトリを削除しないでください。ディレクトリを削除すると、性能情報が収集されなくなります。もし、ディレクトリを削除してしまった場合は、Manager/Proxy Managerのサービスを再起動してください。

監視対象から外した場合は、上記のディレクトリを削除してください。

3.2.4 表示

インストールレス型Agentで収集した仮想サーバの性能情報は、以下の方法で表示できます。

VMwareの場合

- サマリ

  サマリツリーの、VMware(Physical)Monitorノード、VMware(Virtual)StackMonitorノードを選択すると表示できます。

- 詳細

  詳細ツリーの、VMwareノードを選択すると表示できます。

- レポート

  総点検分析・レポート
  カテゴリ別診断分析・レポート
  詳細分析・レポート

Hyper-Vの場合

- サマリ

  サマリツリーの、ServerMonitorノード、HyperV(Physical)Monitorノード、HyperV(Virtual)StackMonitorノードを選択すると表示できます。

- 詳細

  詳細ツリーの、Windowsノード、Hyper-Vノードを選択すると表示できます。

- レポート

  総点検分析・レポート
  カテゴリ別診断分析・レポート
  詳細分析・レポート

注意

Hyper-Vを監視対象とした場合、Windowsの性能情報も表示できます。

ただし、Hyper-VのホストOS(Windows)から取得した以下のCPUの性能情報は値が正しくありません。

- サマリのServerMonitorのCPU使用率
- 詳細のWindowsのCPUBUSY(WIN_CPUBUSY)の情報
- レポートのWindowsのCPUおよびWIN_CPUBUSYに関する情報

- 物理サーバのCPUの性能情報を確認したい場合は、Hyper-Vから取得したCPUの性能情報の値を確認してください。
- サマリのHyperV(Physical)MonitorのCPU使用率
- 詳細のHyper-VのHV_CPUの情報
- レポートのHyper-VのCPUおよびHV_CPUに関する情報

Red Hat仮想化機能の場合

- サマリ

  サマリツリーの、ServerMonitorノード、Xen(Virtual)StackMonitorノードを選択すると表示できます。

- 詳細

  詳細ツリーのLinuxノード、Xenノードを選択すると表示できます。

- レポート

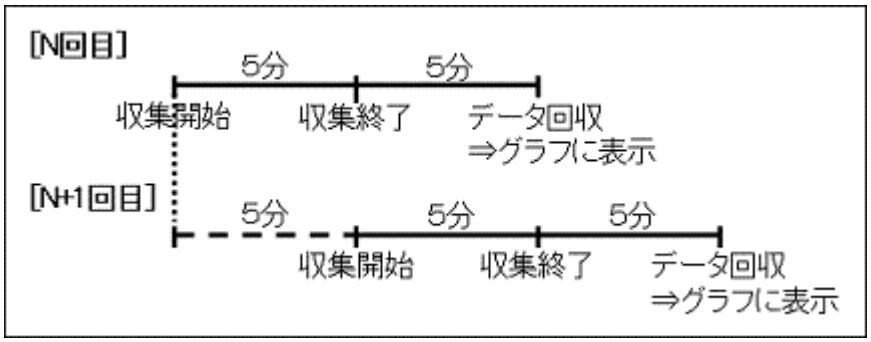
  カテゴリ別診断分析・レポート
  詳細分析・レポート

注意

Red Hat 仮想化機能を監視対象とした場合、Linuxの性能情報も表示できます。

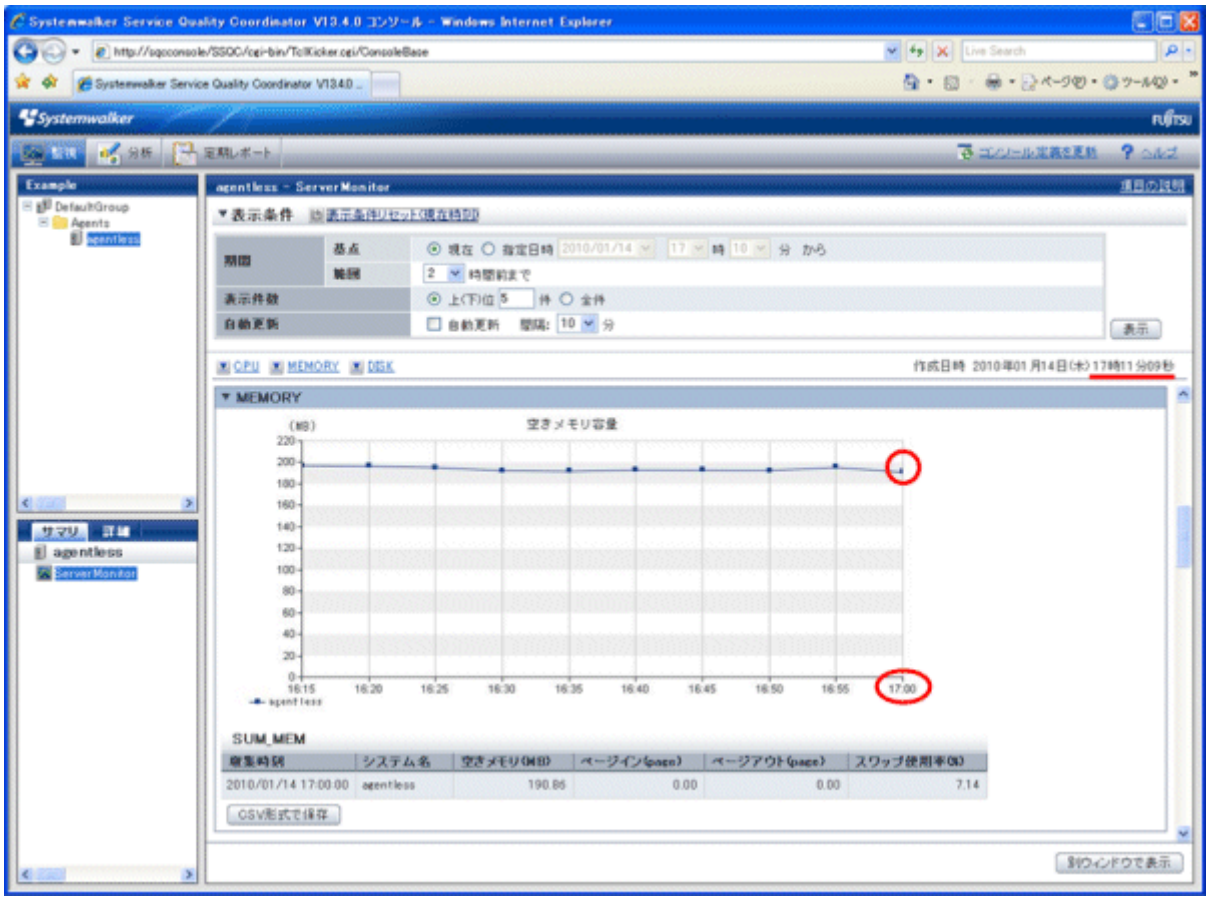
注意

- サマリ画面でデータを表示した場合、データの表示が10～15分程度遅れているように見えます。
  これはインストールレス型Agentの場合、以下の流れでデータが収集されるためです。



【例 17:00データの場合】

17:00	収集を開始
17:05	収集を終了
17:10	Manager/Proxy Managreが性能データを回収 このとき、17:00のデータとしてコンソールに表示されます（収集開始の時刻を基準として表示しています。17:00データの値は17:00から17:05までの平均値となります)。 次の性能データの回収まで、5分間(17:15ごろまで)この状態が続きます。



・ Manager/Proxy Managerのサービスを起動したあと、最初の収集タイミングに被監視サーバ側にスクリプトを送るため、15分～20分程度後に最初のデータが表示されます。

第4章 エンドユーザレスポンス管理

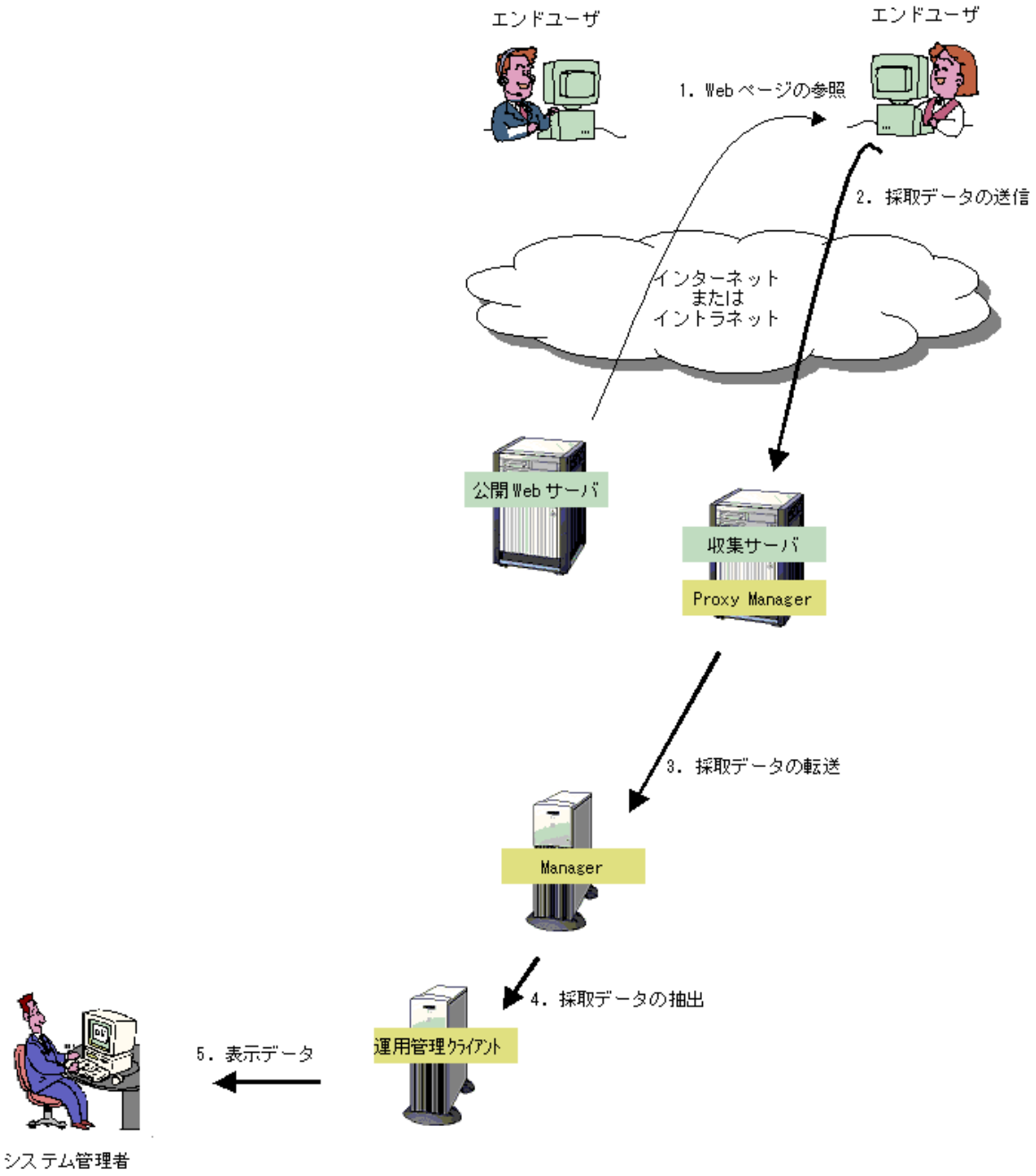
本章では、Browser Agentによるエンドユーザレスポンスの管理方法について説明します。

4.1 測定の概要

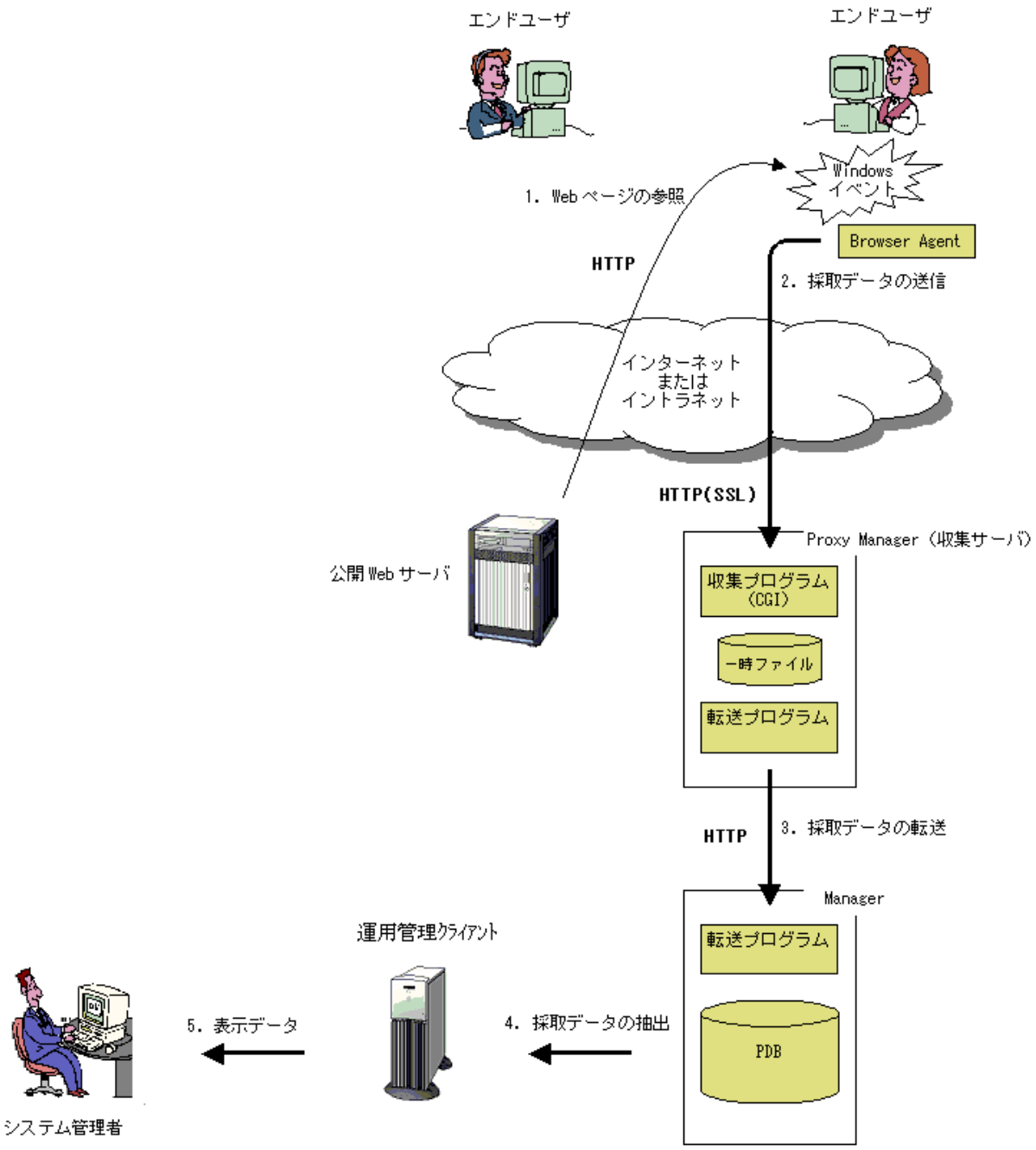
下図は、エンドユーザレスポンス測定の外観を示しています。エンドユーザーがブラウザを使用してWebページを参照すると(図中1)、エンドユーザレスポンス測定機能がデータを採取してProxy Manager(収集サーバ)へ送信します(図中2)。その後、Managerに転送されデータベース化されます(図中3)。

システム管理者がレスポンスデータの表示を要求すると、運用管理クライアントは、Managerからデータを抽出し(図中4)、表示の加工を行ってシステム管理者に表示します(図中5)。

なお、エンドユーザレスポンス情報は、Proxy Managerを介さず、Managerに直接送信することもできます。



このとき、Manager、Proxy Manager、およびエンドユーザーマシンの内部は、下図のとおり動作します。図中の黄色部分は、エンドユーザレスポンス測定機能の構成資材です。図中1の動作は、Windowsイベントを監視していたBrowser AgentがWebページ参照の完了を検出することで発生し、採取データをProxy Manager(収集サーバ)へ送信します。図中3の動作は、採取データをProxy ManagerからManagerへ転送し、データベース化します。



ポイント

- 企業内のWebシステムの場合、業務サービス利用者のマシンにBrowser Agentを導入してもらい、業務サービスが与える作業効率(レスポンス)について、実際に利用者が体感しているデータをもとに管理することができます。
- 企業間の電子商取引(BtoB)のWebシステムの場合、相手企業の業務端末にBrowser Agentを導入してもらい、自社のサービスが与える顧客満足度(レスポンス)について、実際に相手企業側が体感しているデータをもとに管理することができます。
- 消費者向け電子商取引(BtoC)のWebシステムの場合、会員顧客のマシンにBrowser Agentを導入してもらい、自社のサービスが与える顧客満足度(レスポンス)について、実際に個々の顧客が体感しているデータをもとに管理することができます。

4.2 環境設定

以下の順で設定を行います。

- 4.2.1 収集サーバの一時ファイル環境設定
- 4.2.2 収集サーバのCGI環境設定
- 4.2.3 収集ポリシーの作成と適用

4.2.1 収集サーバの一時ファイル環境設定

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

収集プログラム(CGI)および転送プログラム(CGI)は、CGI用のユーザー権限で実行されます。そのため、一時ファイルの格納先(ManagerもしくはProxy Managerのインストール資材に含まれる収集ディレクトリ)には、CGI用のユーザー権限に対し、適切なアクセス権限の設定が必要です。

インストール資材のアクセス権限がセキュリティ強化として一括変更されている場合、以下の方法で収集ディレクトリのアクセス権限を、Windowsの場合はインストール直後の状態に、Solaris/Linuxの場合は変更してください。(セキュリティ上のリスクは大きくなります)

【Windows版】

```
C:¥> <インストールディレクトリ>¥bin¥sqcSetFileSec.exe -u <可変ファイル格納ディレクトリ>¥wslm
```

【UNIX版】

```
# chmod 777 /var/opt/FJSVssqc/wslm
```

4.2.2 収集サーバのCGI環境設定

収集サーバ上のWebサーバにおいて、以下のディレクトリに対する仮想ディレクトリとして「SQC」を定義します。

【Windows版】

```
<インストールディレクトリ>¥www¥
```

【UNIX版】

```
/opt/FJSVssqc/www/
```

また、配下の以下のディレクトリに対してCGIプログラムの実行権を付加します。

【Windows版】

<インストールディレクトリ>¥www¥cgi-bin¥

【UNIX版】

/opt/FJSVssqc/www/cgi-bin/

参照

具体例については、導入手引書「第5章 通信環境のセットアップ」を参照してください。なお、上記設定は、既に仮想ディレクトリが定義済の場合は必要ありません。

注意

収集サーバがManagerであり、かつManagerがクラスタシステム運用の場合は、現用系サーバ・待機系サーバ両方で上記の設定を行ってください。(クラスタシステム運用はEnterprise Editionで提供される機能です。)

ポイント

Browser Agentと収集サーバのHTTP通信には、SSLを使用することができます。インターネット越しに情報を収集する場合、インターネット通過中の第三者への情報漏洩防止の点から、SSL使用をお奨めします。

SSL使用にあたっては、上記ディレクトリに対する仮想ディレクトリを、別途SSL用に定義してください。

また、Browser Agentと収集サーバのHTTP通信でSSLを使用する場合、クライアント認証を行うことができます。クライアント認証を行う場合には、SSL用に定義した仮想ディレクトリを、クライアント認証を行うように定義してください。

4.2.3 収集ポリシーの作成と適用

Browser Agentが管理対象とするサイト名をレスポンス・稼働管理対象構成情報(ServiceConf.xml)のレスポンス情報(WebSiteタグ)に定義します。

定義方法は、「第6章 レスポンス・稼働管理対象構成情報(ServiceConf.xml)」を参照してください。

4.3 Browser Agentの導入

導入は、測定条件をあらかじめ組み込んだBrowser Agentインストールパッケージ(以降、パッケージ)を使用し、以下の順で行います。

すべてWindowsシステム上での作業です。

■実行に必要な権限

【Windows版】

Windows 2000の場合　Administratorsグループに所属するユーザー権限が必要です。

Windows XPの場合　Administratorsグループに所属するユーザー権限が必要です。

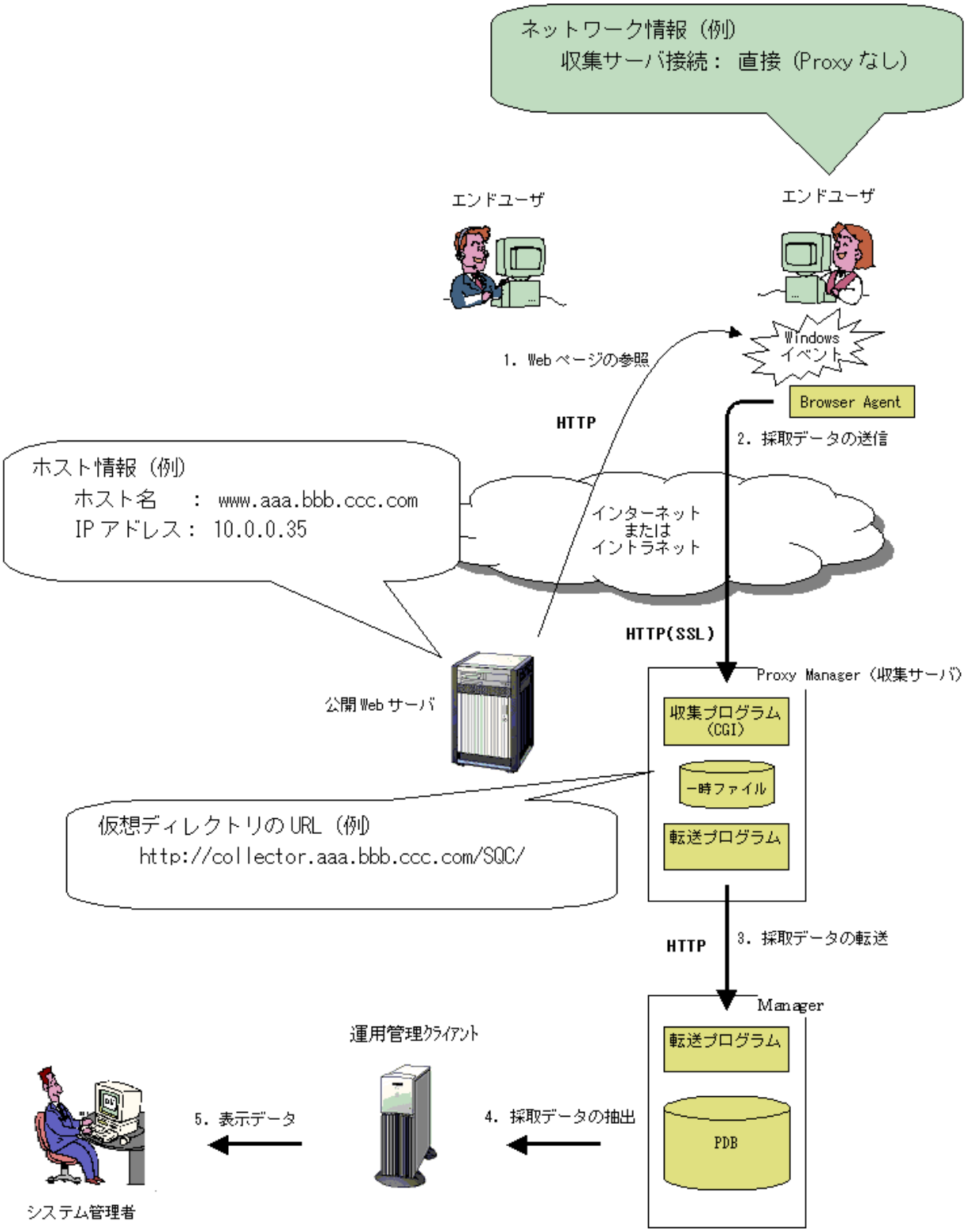
Windows Vistaの場合　Performance Monitor Users グループに所属するユーザー権限が必要です。

Windows 7の場合 Performance Monitor Users グループに所属するユーザー権限が必要です。

■手順

- 4.3.1 パッケージの作成
- 4.3.2 インストール条件と見積り
- 4.3.3 パッケージのインストール
- 4.3.4 Browser Agentの起動
- 4.3.5 Browser Agentのアップグレードおよび再インストール
- 4.3.6 Browser Agentのアンインストール

以降の説明では、例として、下図のとおり設定する方法について説明します。



4.3.1 パッケージの作成

まず、以下の手順でパッケージャを起動します。

【Windows版】

1. Windowsマシンにログインし、本製品のCD-ROMをドライブにセットします。

2. 次のパスのファイルを実行します。

<CD-ROMドライブ>:¥tools¥wslm¥wslmpack.exe

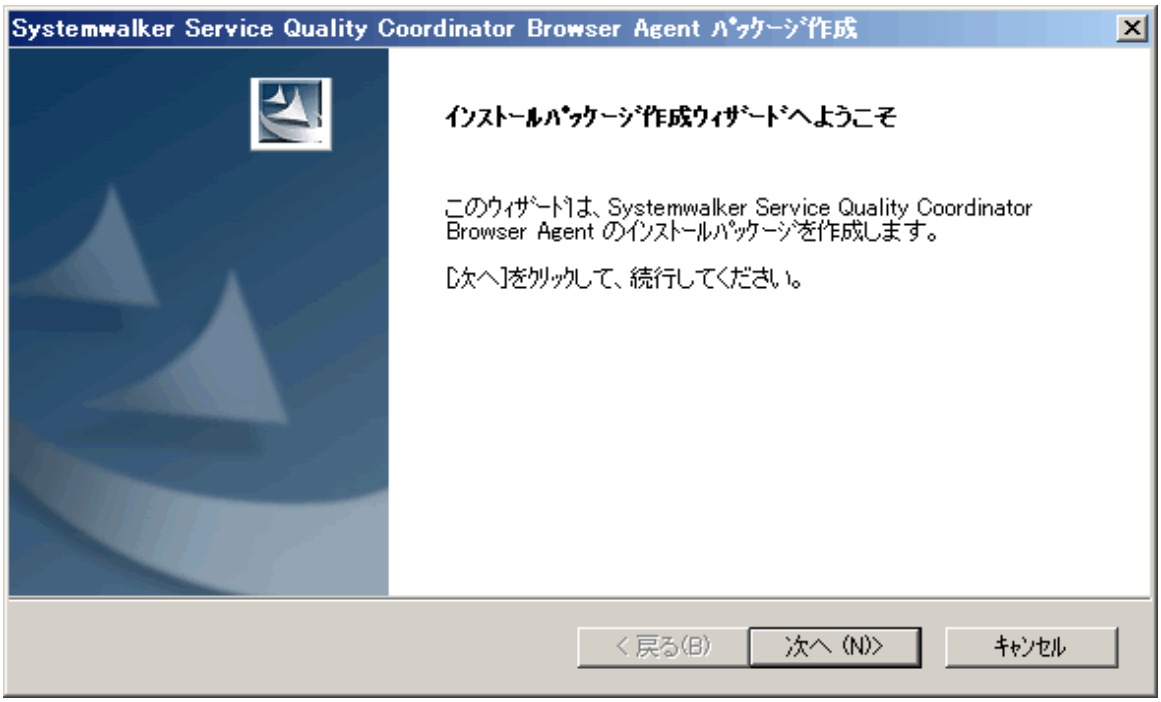
【UNIX版】

1. WindowsマシンのCD-ROM装置に本製品のUNIX版CD-ROMをセットします。
2. 次のパスのファイルを実行します。

＜CD-ROMドライブ＞:¥FJSVssqc¥tools¥wslm¥wslmpack.exe

前記例のとおりにするには、次に、下図のとおり作業を進めます。

作成画面



「次へ(N)>」を選択します。

パッケージ名の設定

ここでは、パッケージ名を「East01」とします。

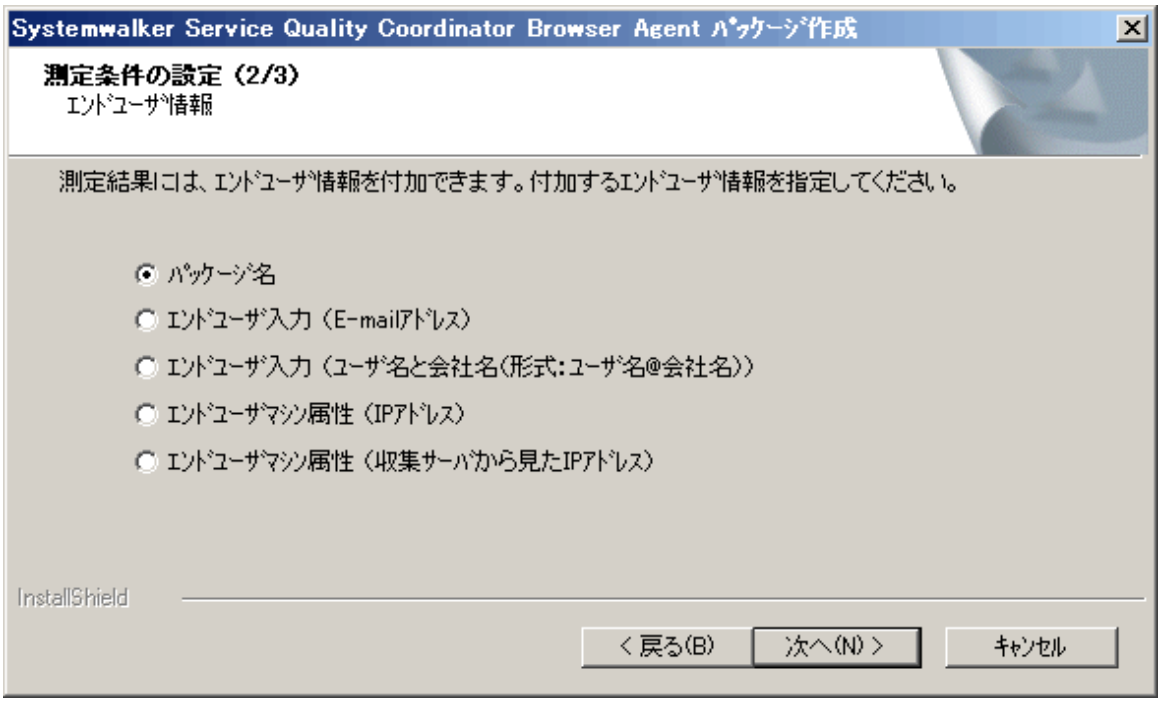
測定条件の設定(1/3)

測定対象のWebサイトは、最大5個まで指定できます。

上記のように設定した場合、以下のサイトが監視対象となります。

サイト	ホスト名	IPアドレス
サイト1	www.aaa.bbb.ccc.com	*.*.*.*

測定条件の設定(2/3)

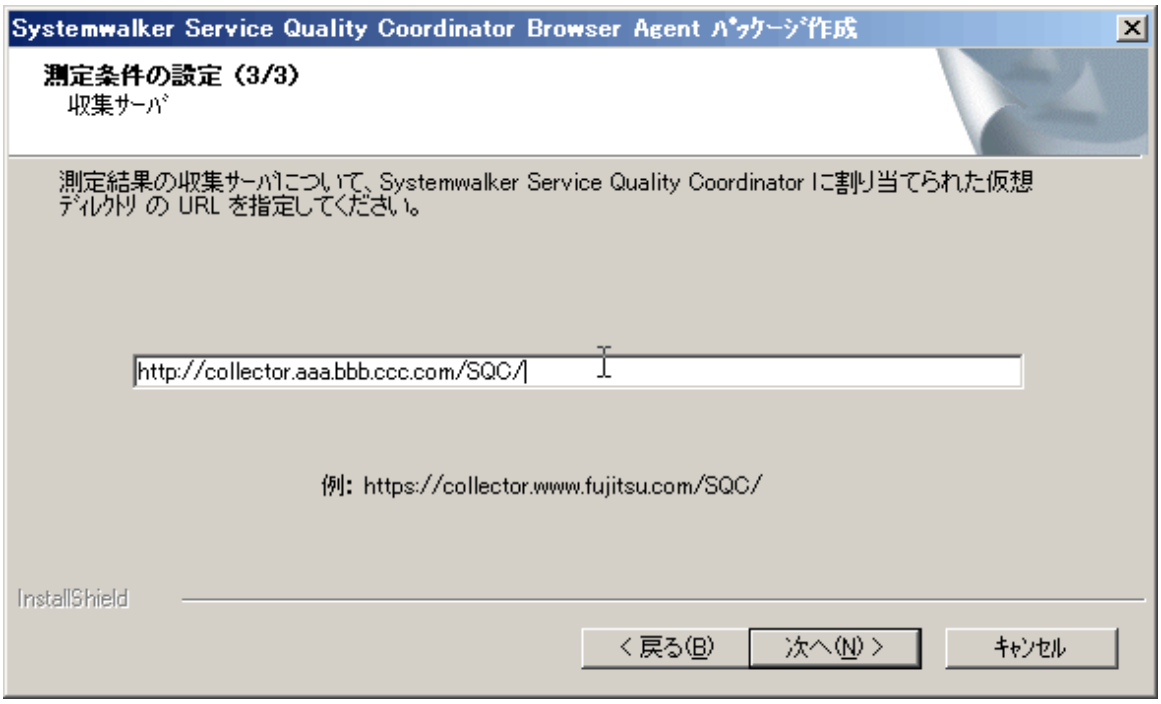


以下を選択した場合、「エンドユーザー入力の内容変更」を参照してください。

- エンドユーザー入力(E-mailアドレス)
- エンドユーザー入力(ユーザー名と会社名(形式:ユーザー名＠会社名))

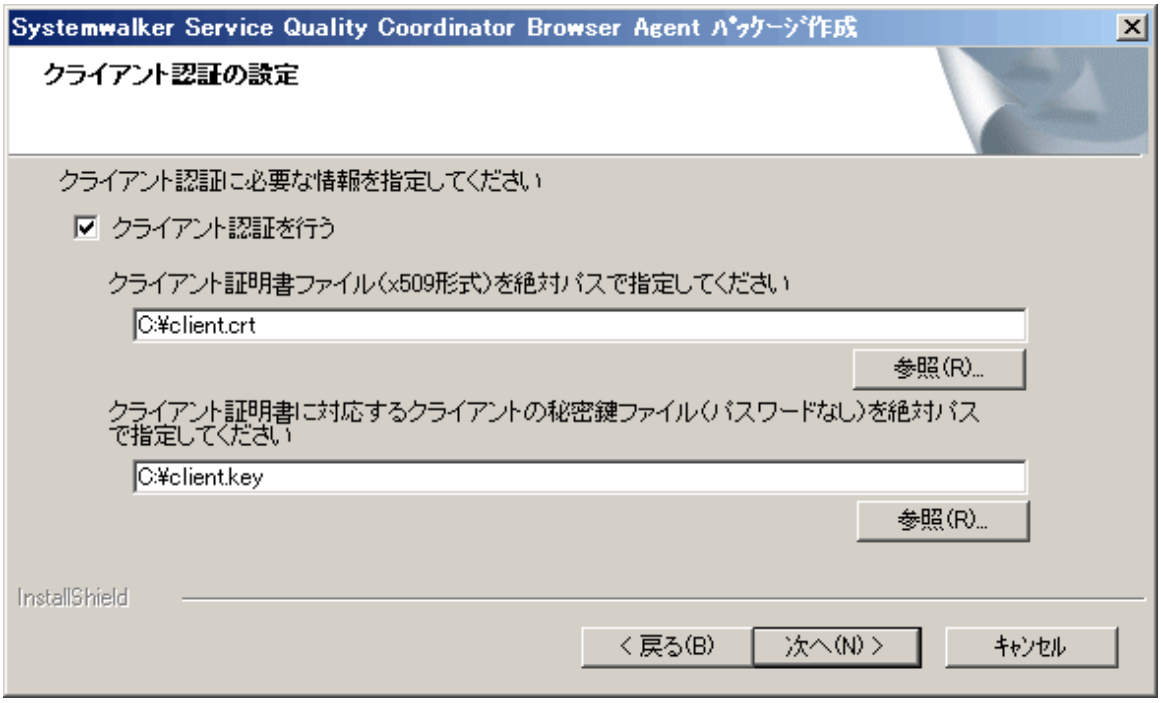
エンドユーザー情報は、レポート作成においてエンドユーザー単位の集計を可能とします。詳細については、「4.5 Browser Agentパッケージに関する補足事項」を参照してください。

測定条件の設定(3/3)



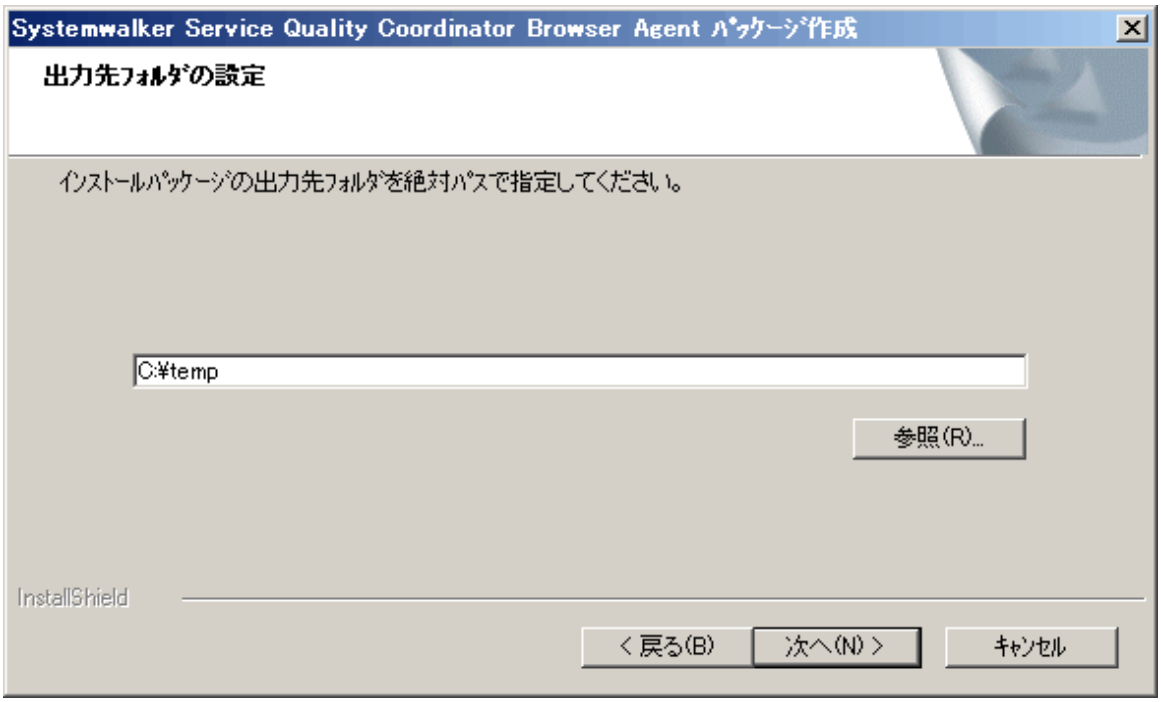
Systemwalker Service Quality Coordinatorに割り当てられた仮想ディレクトリのURLを指定します。

クライアント認証の設定



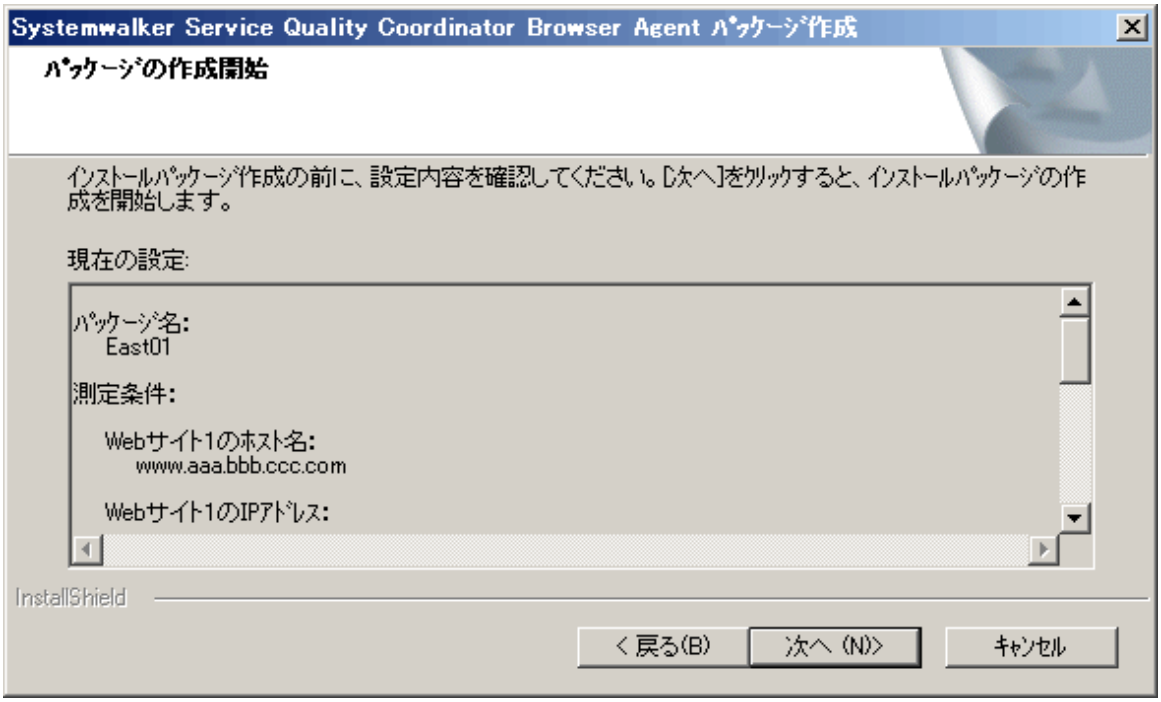
クライアント認証を行う場合は、クライアント証明ファイルを絶対パスで指定し、クライアント証明ファイルに対するクライアントの秘密鍵ファイルを絶対パスで指定します。

出力先フォルダの設定



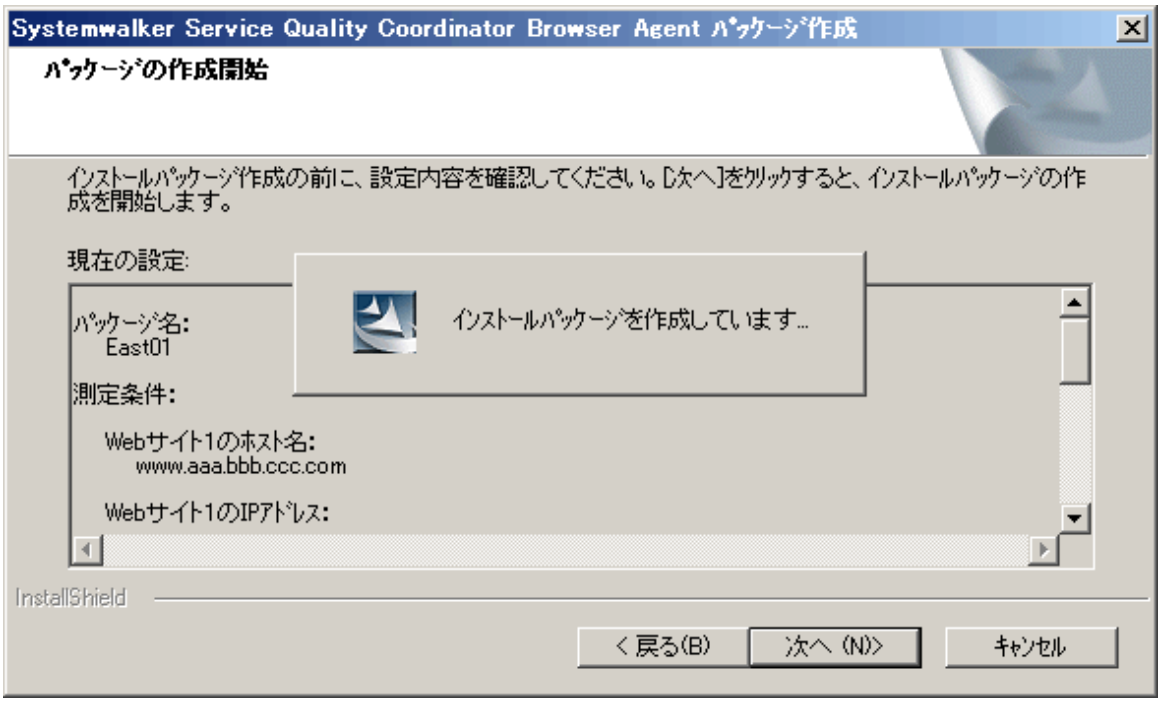
ここでは、パッケージの出力先ディレクトリを「C:¥temp」とします。

パッケージの作成開始(設定内容の確認)

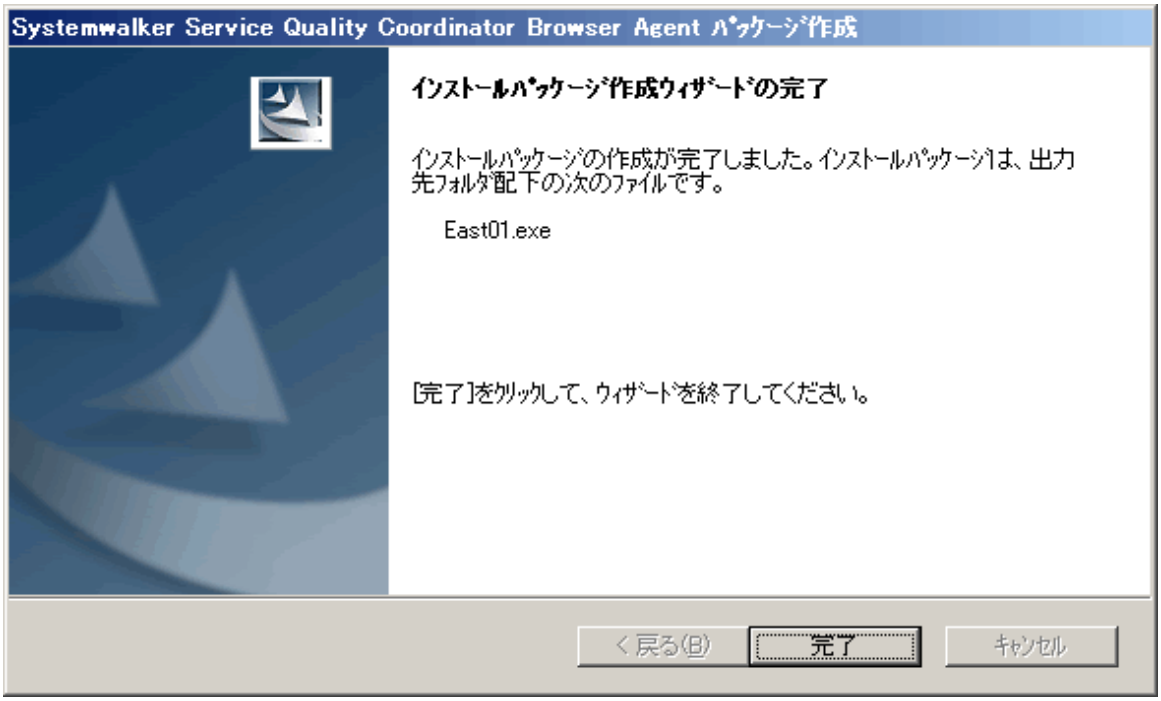


パッケージの設定内容を確認し、「次へ(N)>」を選択します。

パッケージの作成開始



パッケージ作成完了



注意

パッケージの作成が成功しても、設定した測定条件に誤りがあると、正しく測定できません。パッケージ作成後は、「4.3.3 パッケージのインストール」を参考に一度インストールを行い、測定条件に従って測定できることを確認してください。

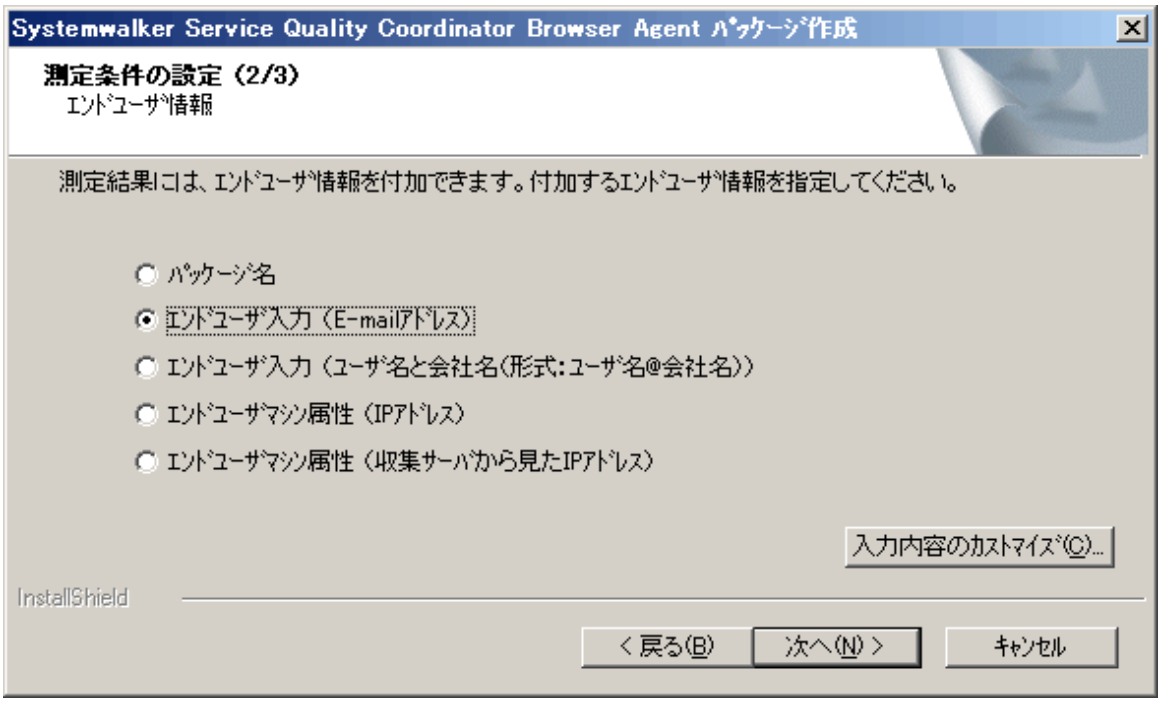
エンドユーザー入力の内容変更

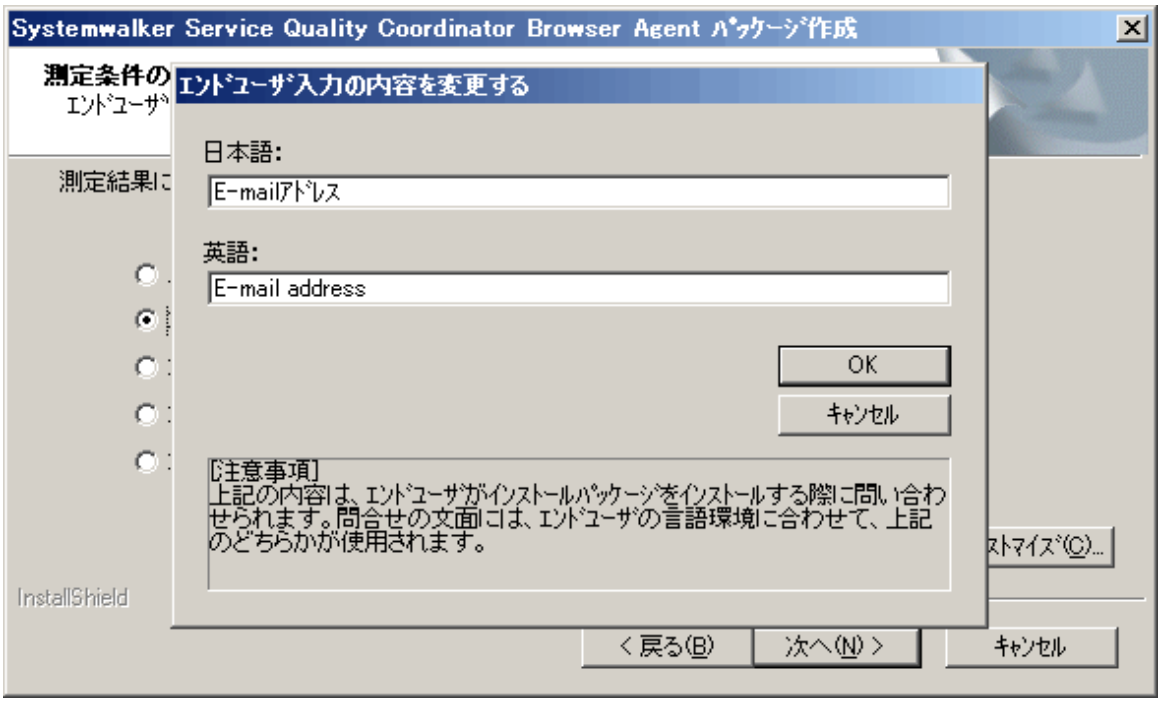
ポイント

[測定条件の設定(2/3)]画面で以下を選択した場合、以下の括弧内の内容は、エンドユーザーがインストールパッケージをインストールする際の問合せ内容となります。

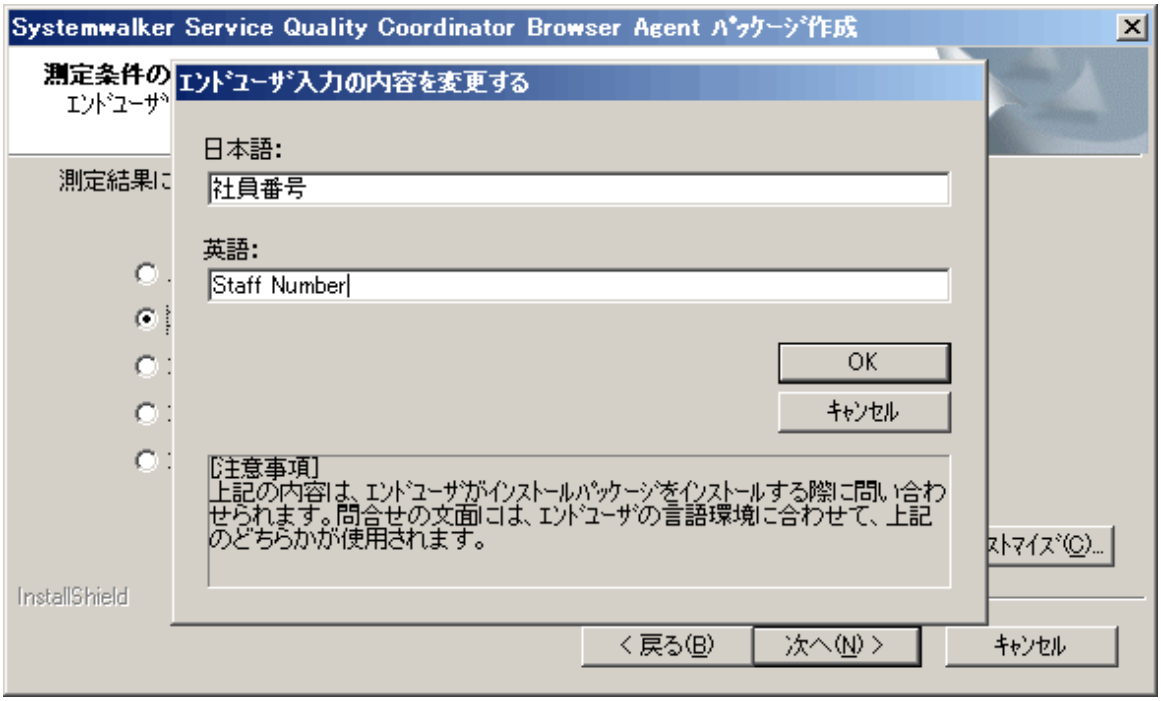
- エンドユーザー入力(E-mailアドレス)
- エンドユーザー入力(ユーザー名と会社名(形式:ユーザー名＠会社名))

なお、上記の選択時には、「入力内容のカスタマイズ」ボタンが表示され、括弧内の問合せ内容をカスタマイズすることができます。以下は、「入力内容のカスタマイズ」ボタンと選択後に表示される[エンドユーザー入力の内容を変更する]画面の例です。



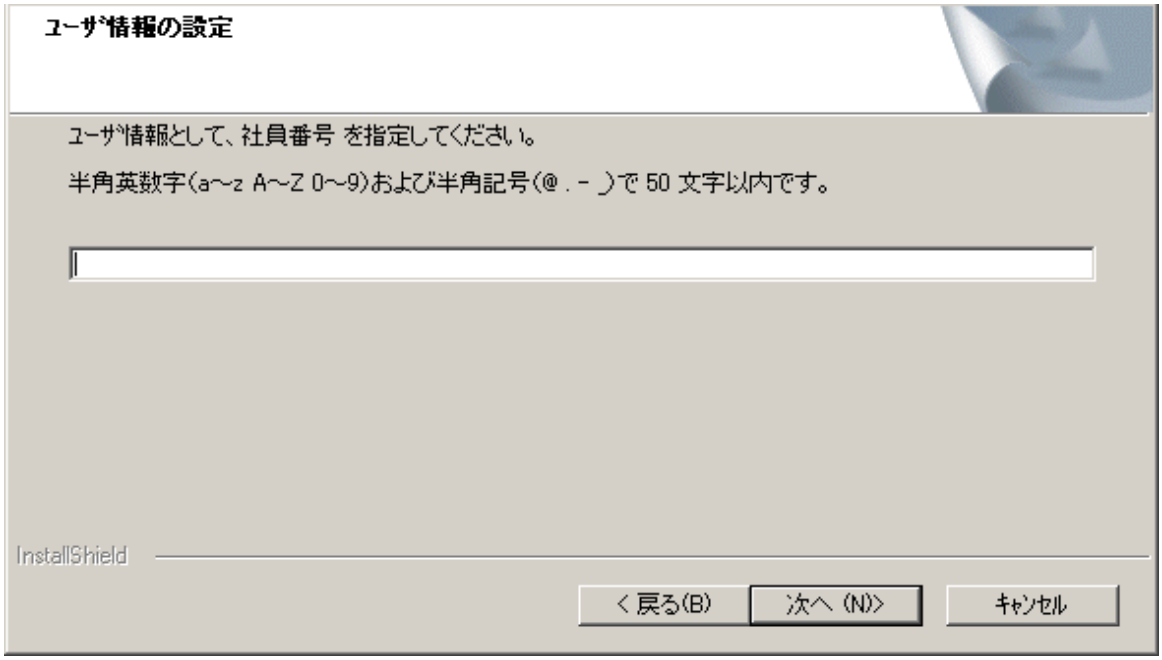


例えば、以下のようにカスタマイズします。

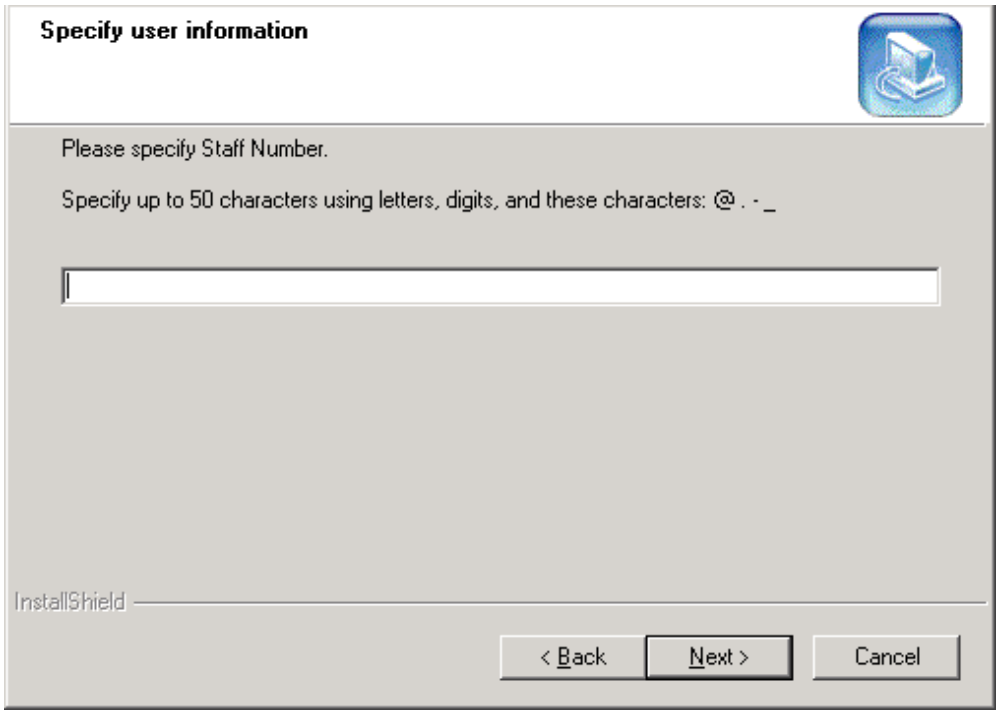


この場合、エンドユーザーがインストールパッケージをインストールする際の問合せは、エンドユーザーの言語環境に合わせて、以下のようになります。

・ 言語環境が日本語の場合



・ 言語環境が英語の場合



Browser Agentと収集サーバのHTTP通信でSSLを使用し、クライアント認証も行う場合、クライアント認証で使用するクライアント証明書ファイルおよび秘密鍵ファイルをパッケージに組み込む必要があります。

クライアント認証で使用するクライアント証明書ファイルと秘密鍵ファイルを事前に用意し、[クライアント認証の設定]画面で指定してください。

Browser Agentで使用できるクライアント証明書および秘密鍵は、以下の形式です。

ファイル種別	形式
クライアント証明書	X.509形式

ファイル種別	形式
秘密鍵	パスワードなし

パッケージの配布

システム管理者は、作成したパッケージをエンドユーザーへ配布します。

配布方法としては、フロッピィディスクなどの媒体による配布や、Web上のダウンロードサイトによる配布などがあります。

4.3.2 インストール条件と見積り

Browser Agentのインストール条件を以下に説明します。

4.3.2.1 動作ハードウェア

【Windows版】

項目		内容	備考
CPU		インテル(R) Pentium 3 相当以上	
ディスク空き容量	インストールディレクトリ	4MB以上	
メモリ空き容量		10MB以上	

4.3.2.2 動作OS

【Windows版】

項目	内容	備考
動作OS	Microsoft(R) Windows(R) 2000 Professional(x86)	
	Microsoft(R) Windows(R) XP Professional(x64)	
	Microsoft(R) Windows(R) XP Professional(x86)	
	Microsoft(R) Windows Vista(R) Ultimate(x64)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Home Premium(x64)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Home Basic(x64)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Business(x64)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Enterprise(x64)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Ultimate(x86)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Home Premium(x86)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Home Basic(x86)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Business(x86)	Service Pack 1/2
	Microsoft(R) Windows Vista(R) Enterprise(x86)	Service Pack 1/2
	Microsoft(R) Windows(R) 7 Ultimate(x86)	
	Microsoft(R) Windows(R) 7 Home Premium(x86)	

項目	内容	備考
	Microsoft(R) Windows(R) 7 Professional(x86)	
	Microsoft(R) Windows(R) 7 Enterprise(x86)	
WWWブラウザ	Microsoft(R) Internet Explorer 6.0以降(32-bit)	

4.3.2.3　排他製品

エンドユーザレスポンスの詳細データを収集する場合に、以下の排他製品があります。

製品名	備考
Systemwalker Centric Manager(運用管理サーバ、部門管理サーバ、業務サーバ、運用管理クライアント) Interstage Application Server	

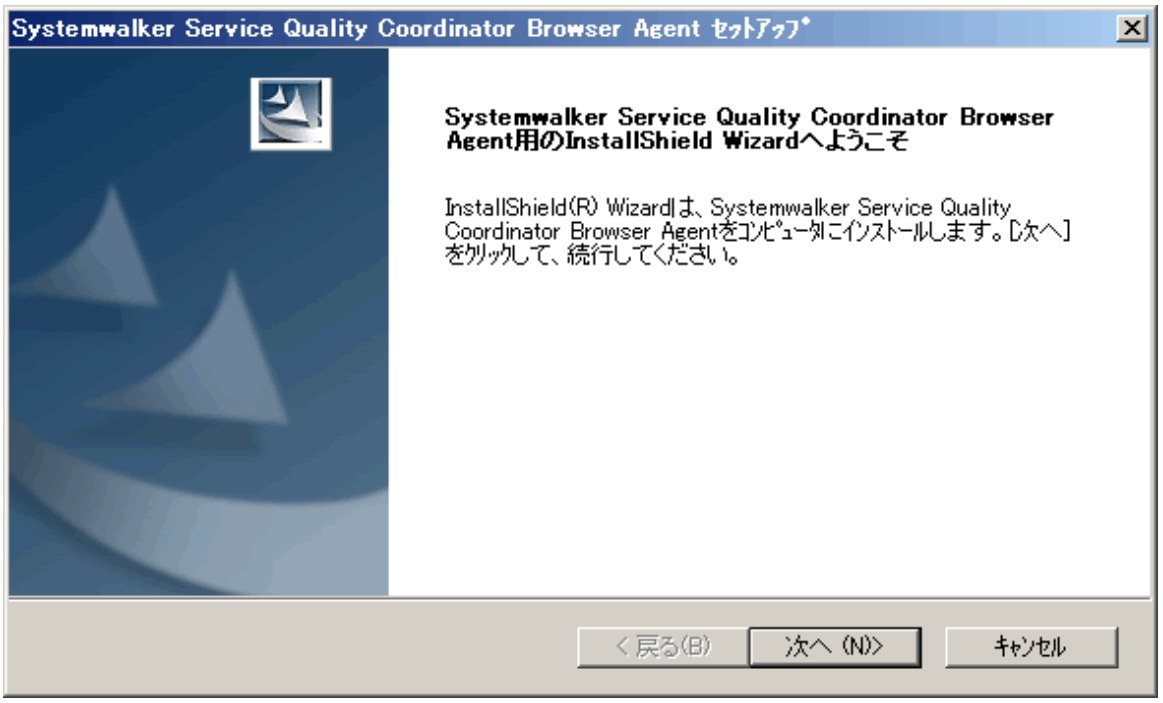
4.3.3　パッケージのインストール

作成したパッケージをインストールします。以下の手順に従って、インストールを行ってください。

1. Windowsシステムへログインします。
2. システム管理者から配布されたパッケージをコマンドとして実行します。

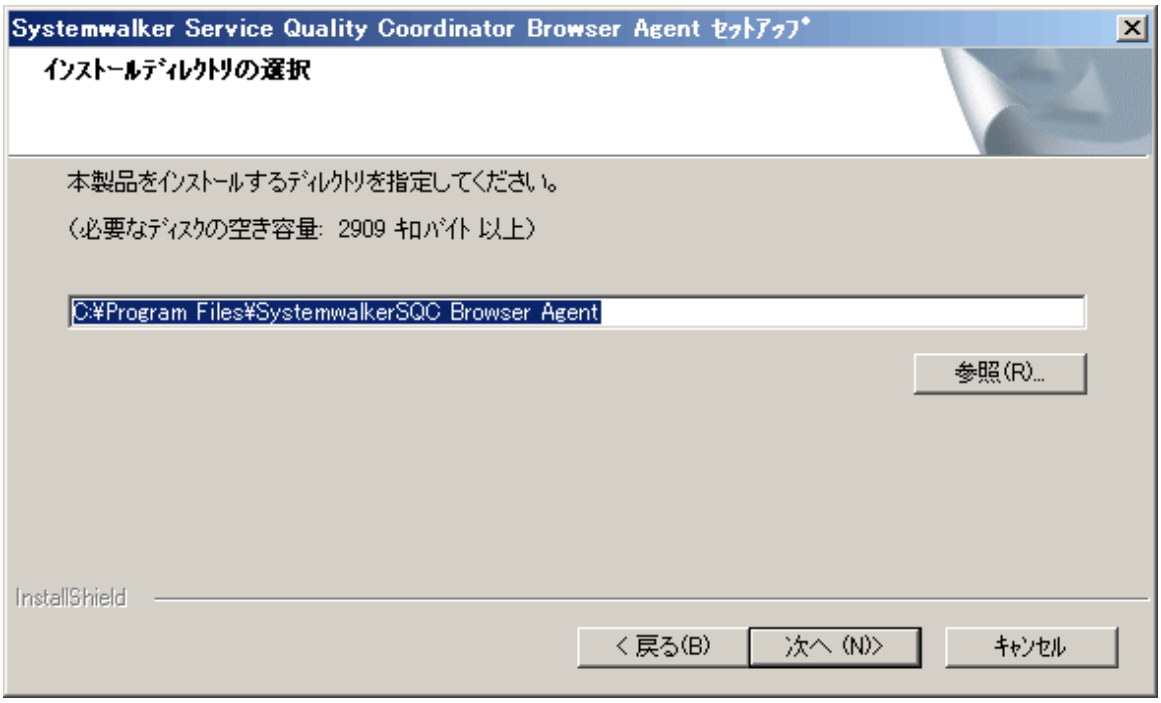
前記例のとおりとするには、次に、下図のとおり作業を進めます。なお、この例では、インストールディレクトリをデフォルトのままとしています。

インストール画面



ユーザー情報の設定(エンドユーザー情報がエンドユーザー入力の場合のみ)

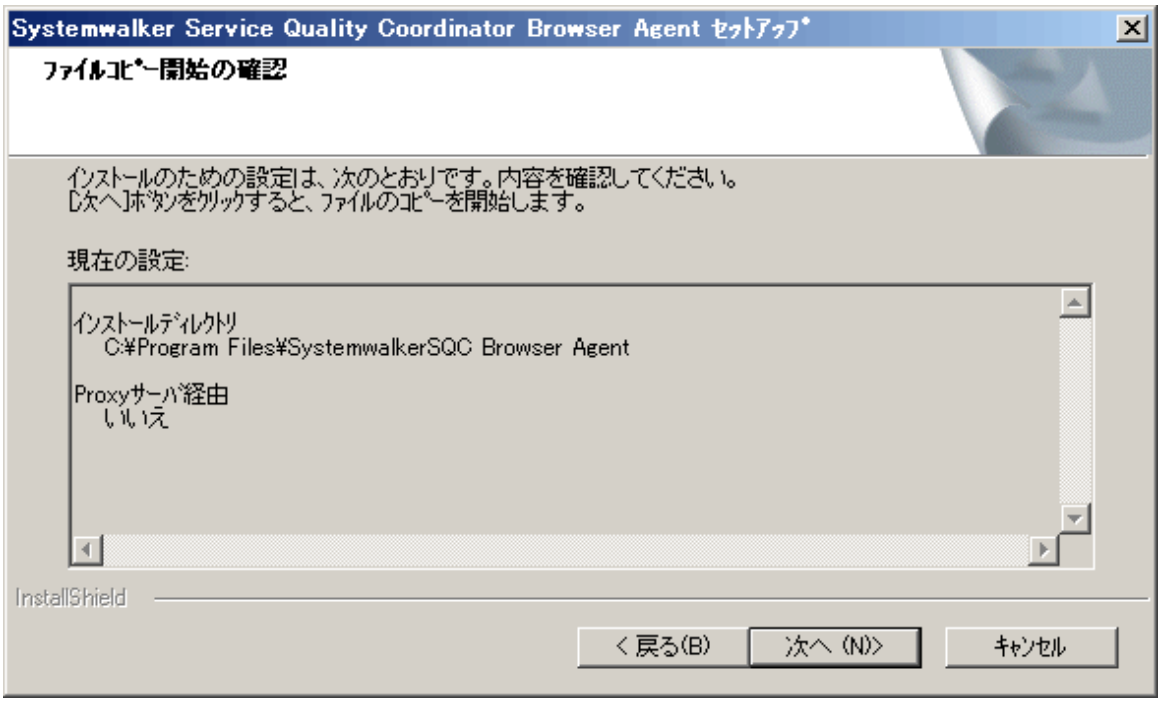
インストールディレクトリの設定



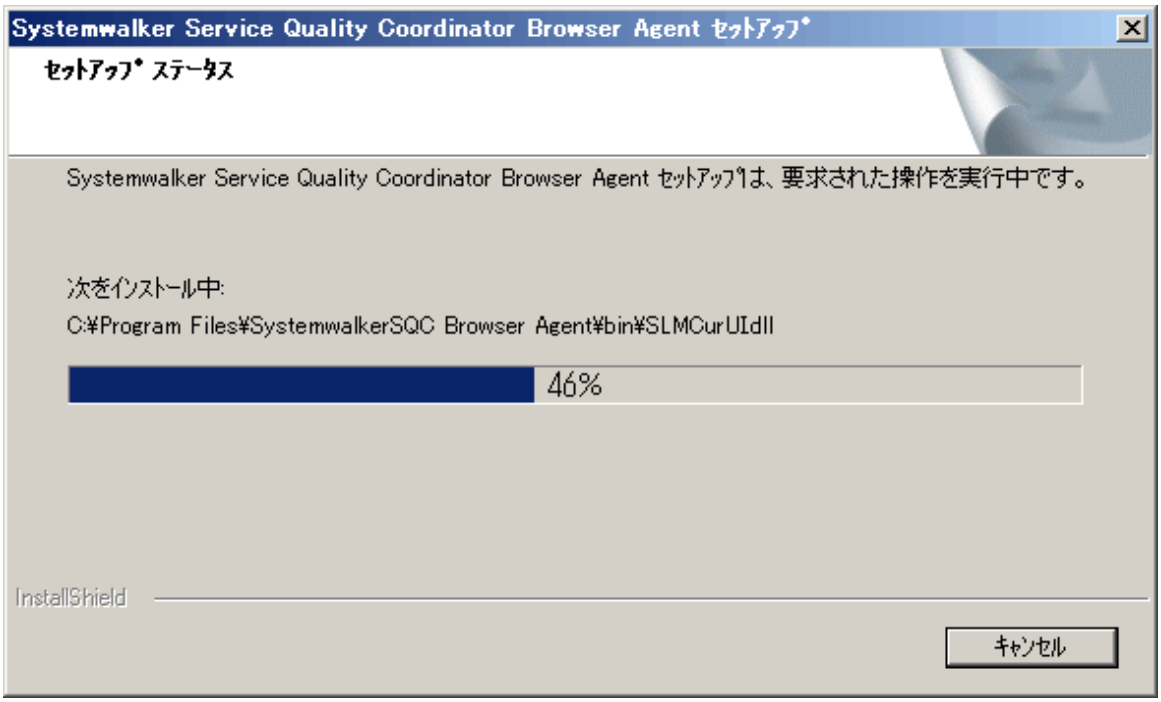
Proxyサーバ経由の選択

「はい」を選択した場合は、「Proxyサーバ情報の設定」を参照して下さい。

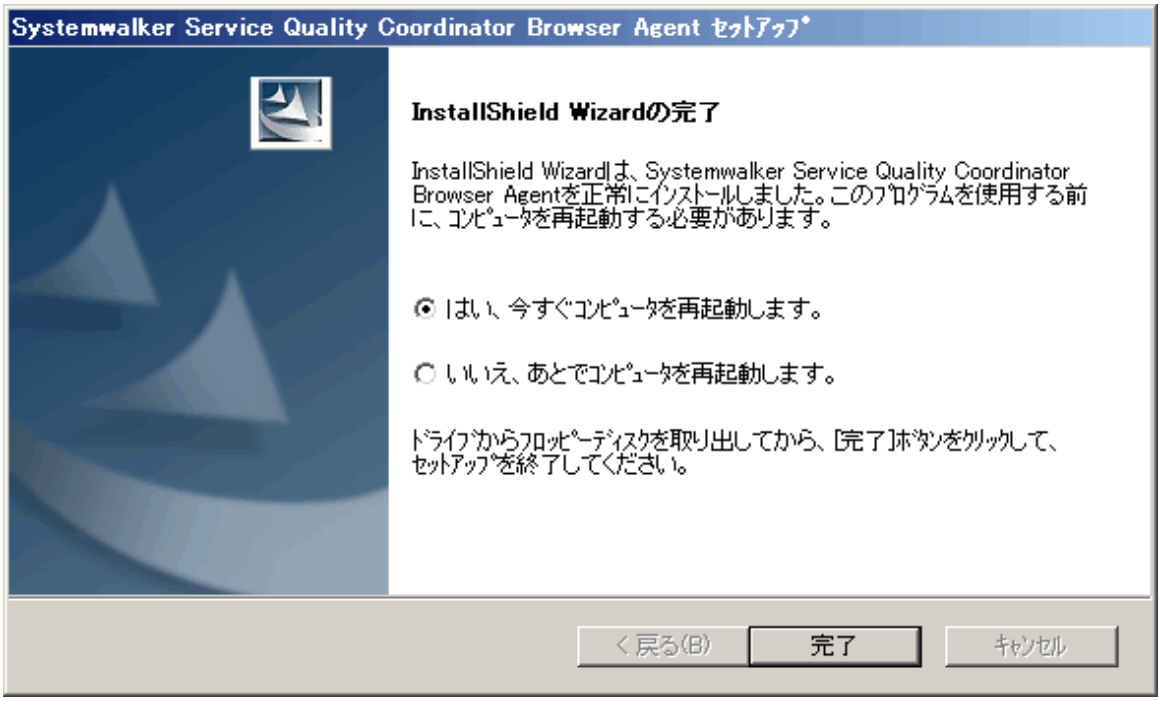
ファイルコピー開始の確認



セットアップステータス



インストール完了

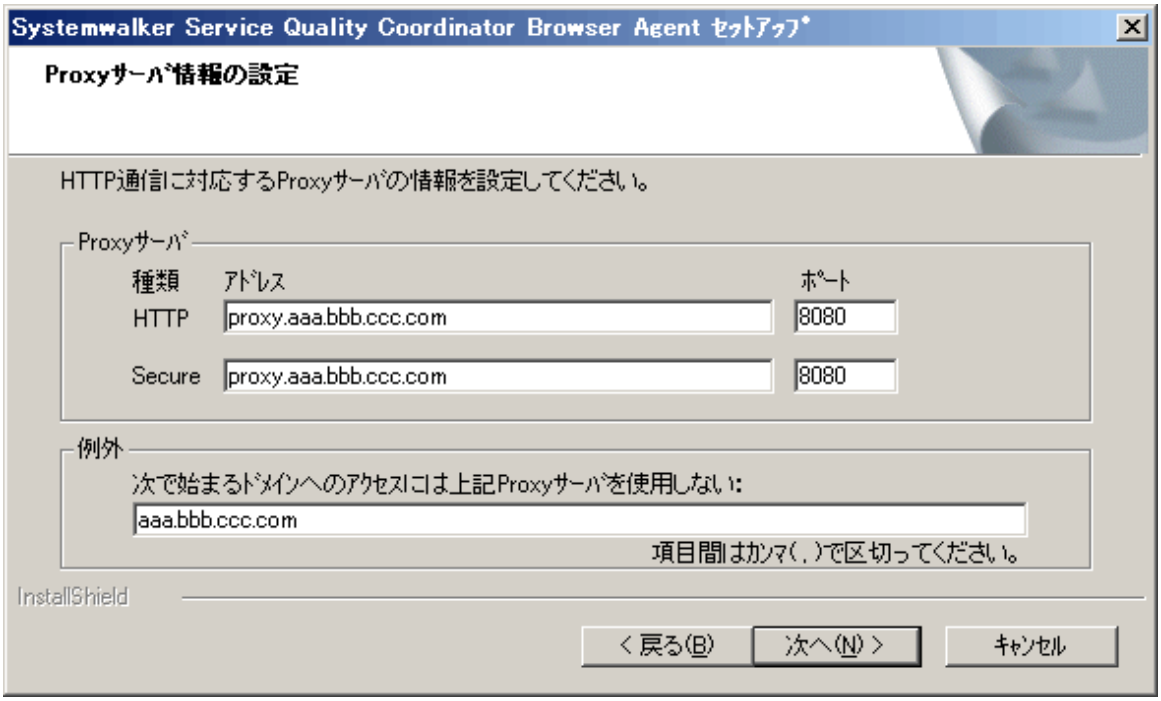


インストール完了後、再起動をしてください。

Proxyサーバ情報の設定

ポイント

「Proxyサーバ経由の選択」画面で、「はい」を選択した場合は、「Proxyサーバ情報の設定」画面で必要事項を設定してください。以下は、「Proxyサーバ情報の設定」画面の例です。



4.3.4 Browser Agentの起動

Browser Agentの起動方法について説明します。

- **スタートメニューからの起動方法**

  Browser Agentを利用するユーザーでログインし、スタートメニューから以下のように起動します。

  [スタート]→[プログラム]→[Webページ表示レスポンスの測定開始]

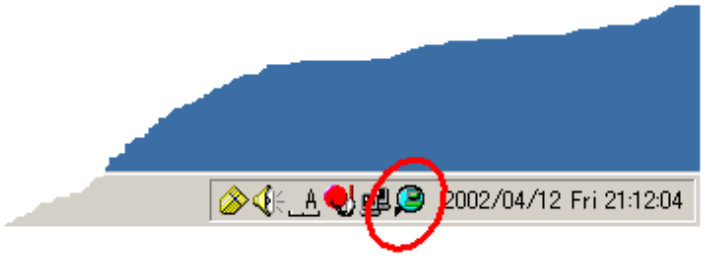
- **スタートアップへの登録による起動方法**

  Browser Agentを利用するユーザーのログインを契機に起動させる場合は、以下のファイルパスを、スタートアッププログラムに追加すると、ログオン時に自動起動します。

<インストールディレクトリ>¥bin¥SLMCurat.exe

起動後、Browser Agentが正常に動作すると、タスクトレイに次のアイコンが表示されます。

以下は、表示例です。赤で印した箇所です。



注意

エンドユーザーがMicrosoft(R) Internet Explorerをご利用する場合、まず、[ツール]→[インターネットオプション]でインターネットオプション画面を開き、[詳細設定]タグを選択し、[ブラウズ]の[サードパーティ製のブラウザ拡張を有効にする(再起動が必要)]がチェックされていることをご確認ください。

もし、チェックがされていない場合、Browser Agentのデータは収集サーバへ送信されません。

Browser Agentは、下位のバージョンのManager、Proxy Managerに対してのデータ送信はサポートしていません。送信した場合は、収集データが欠落する可能性があります。

4.3.5 Browser Agentのアップグレードおよび再インストール

Broser Agentのアップグレードおよび再インストールについて説明します。

すでにBrowser Agent がインストールされている環境に、Browser Agentをインストールする場合は、インストール前に、すでにインストールされている Browser Agentをアンインストールしてください。

Browser Agentのアンインストールについては、「4.3.6 Browser Agentのアンインストール」を参照してください。

Browser Agentのインストールについては、「4.3.3 パッケージのインストール」を参照してください。

4.3.6 Browser Agentのアンインストール

Systemwalker Service Quality Coordinator Browser Agentをアンインストールする手順を説明します。

■手順

以下の手順にそって実施してください。

【Windows版】

1. タスクトレイを調べ、Browser Agentが起動中かどうかを確認します。起動中の場合、次のどちらかのアイコンが存在します。

2. 起動中の場合は、アイコン上でマウスを右クリックしてポップアップメニューを表示し、Exitを選択してBrowser Agentを停止します。
3. コントロールパネルで [アプリケーションの追加と削除] または [プログラムの追加と削除] をダブルクリックします。
4. アプリケーションの一覧から「Systemwalker Browser Agent」を選択し、[追加と削除] または [変更と削除]ボタンをクリックします。

5. アンインストールが開始されます。

注意

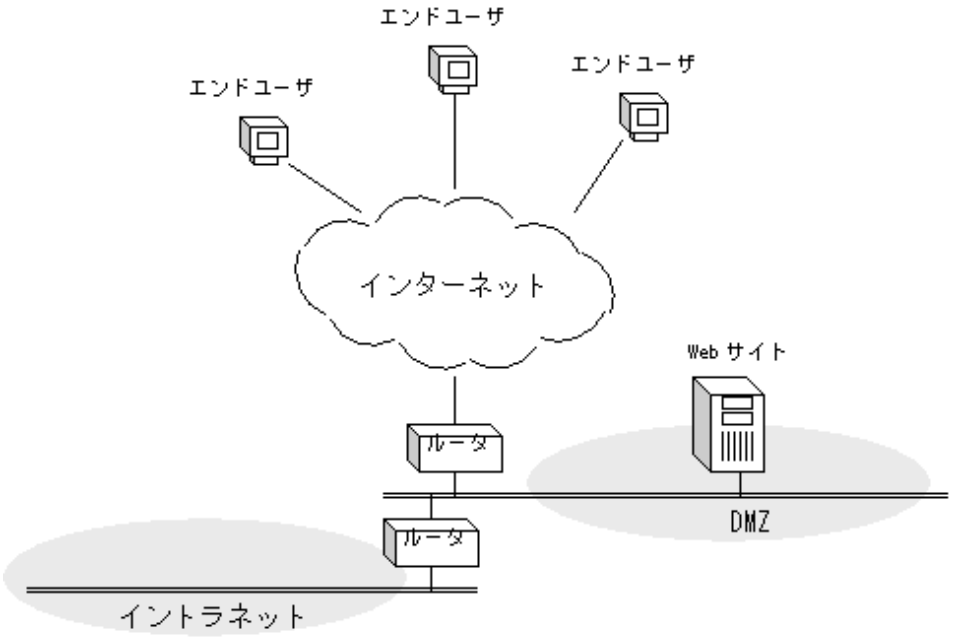
アンインストール時に、「InstallShield Wizardの完了」画面で「はい、今すぐコンピュータを再起動します。」を選択して完了ボタンを押した場合、再起動処理中に既にBrowser Agentがアンインストールされている可能性がある旨の警告メッセージが表示されることがありますが、アンインストールの処理には影響はありません。

4.4 製品配置に関する補足事項

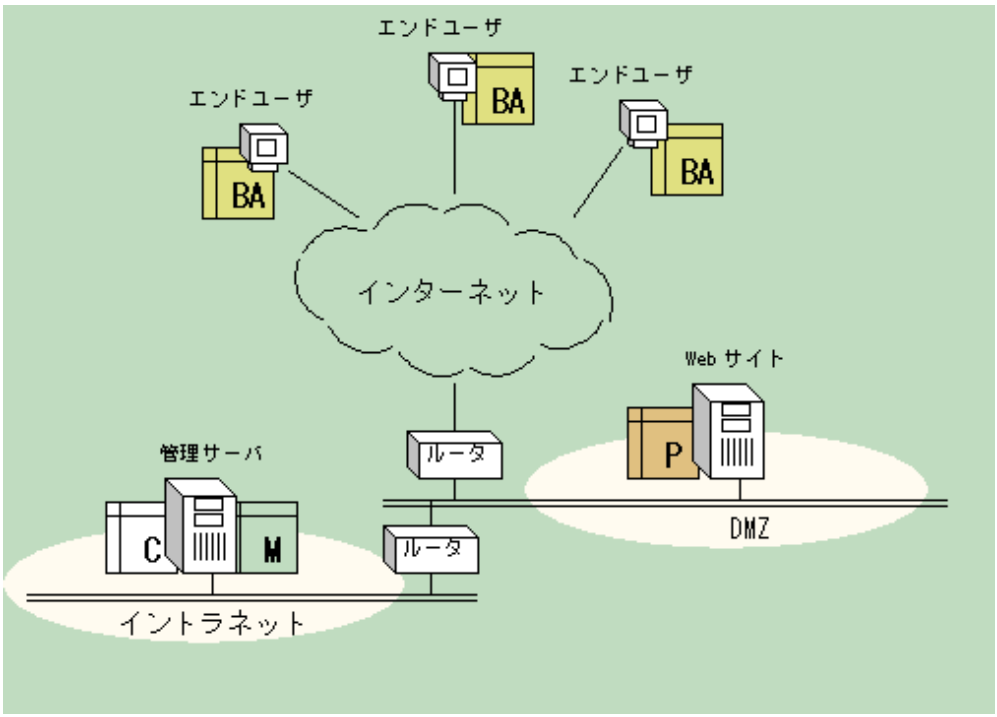
以降の説明では、各製品を示すアイコンとして、以下を使用します。

4.4.1 基本的な製品配置パターン

Webサイトの例として、以下のモデルを想定します。



この時、基本的な製品配置パターンは、以下のようになります。



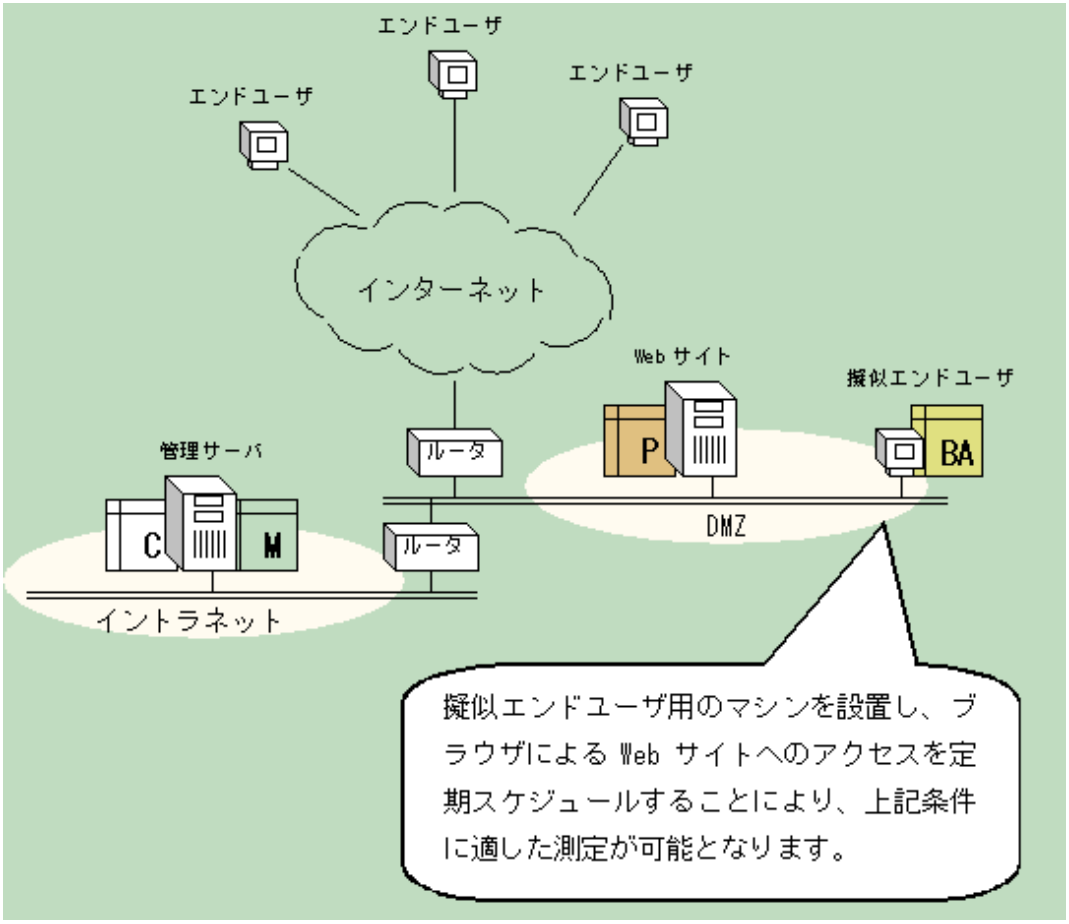
4.4.2 定期測定を実施したい場合の製品配置パターン

Webサイトの能力に着目して毎時の状況を把握したい場合、以下の条件が必要となります。

- エンドユーザー側の測定環境(マシン環境やネットワーク環境)が一定
- エンドユーザー側の測定が定期

前節(「4.4.1 基本的な製品配置パターン」)では、実際のエンドユーザーにBrowser Agentを配置しましたが、その場合、エンドユーザー側の測定環境は一定になりませんし、実際にエンドユーザーがWebサイトのサービスを利用した際に測定されるために測定は定期となりません。

そのため、上記の条件を満たすには、擬似的にエンドユーザーの操作を繰り返す環境(以降、擬似エンドユーザー)を用意した、以下の製品配置パターンがお奨めです。



以下、定期スケジュールの補助ツールについて補足します。

補足: ブラウザの定期起動ツール(コマンド)の提供について

格納場所:

Service Quality CoordinatorのCD-ROMで、以下。

<CD-ROM-Drive>:¥tools¥wslm¥repeatbrowser.exe

※別のフォルダにコピーして使用する場合は、下記3ファイルを同一フォルダに格納してrepeatbrowser.exeを実行してください。

－repeatbrowser.exe

－run_ie_default.vbs

－run_ie7_vis.vbs

動作条件:

OS : Microsoft(R) Windows 2000 Professional 以降

ブラウザ: Microsoft(R) Internet Explorer 6.0 以降

仕様:

[形式]

repeatbrowser interval period

[説明]

ブラウザの起動と停止を定期的に繰り返します。

[パラメタ]

interval : ブラウザの起動間隔を秒数で指定します。

period : ブラウザの動作時間を秒数で指定します。

※ intervalとperiodは、interval ＞ period ＞ 1 の範囲で指定します。

[事前準備]

事前に、ブラウザのホームページに定期アクセス先のWebページを設定します。(Internet Explorerの[ツール]→[インターネットオプション]→[全般]→ホームページにて設定)

アクセス時にブラウザキャッシュの使用を防止したい場合は、事前に、ブラウザ停止時のキャッシュ削除を有効に設定します。(Internet Explorerの[ツール]→[インターネットオプション]→[詳細設定] →セキュリティ→「ブラウザを閉じたとき、[Temporary Internet Files]を空にする」にて設定)

[起動方法]

DOSプロンプトでコマンドを実行します。

[停止方法]

CNTL-Cの入力により停止します。

[標準出力]

ブラウザの起動および停止の度にメッセージを出力します。

[標準エラー出力]

エラー発生時にメッセージを出力します。

[使用例]

例: 起動間隔3分(180秒)、動作時間1分(60秒)で起動します。

C:¥> repeatbrowser 180 60

2002/06/08 20:06:47 Start IE

2002/06/08 20:07:47 Stop IE

2002/06/08 20:09:47 Start IE

4.5 Browser Agentパッケージに関する補足事項

Browser Agentパッケージの配布にあたっては、レスポンスデータの分析をどのように行うかを検討し、それに適したパッケージを配布する必要があります。以降、Browser Agentパッケージの配布パターンについて、以下の順で説明します。

4.5.1 任意のグループで分析する場合

たとえば、関東地区と関西地区のように、測定結果を任意のグループで分析する場合には、Browser Agentパッケージをそれぞれのグループごとに作成し、「パッケージ名」にはそれぞれのグループを示す名前を付け、「エンドユーザー情報」には「パッケージ名」を指定します。パッケージ配布時には、グループごとに対応したパッケージを配布します。

参照

パッケージの作成については、「4.3.1 パッケージの作成」を参照してください。

4.5.2 エンドユーザー属性で分析する場合

測定結果をエンドユーザー属性(「E-mailアドレス」、「ユーザー名と会社名」または任意のユーザー情報のどれかひとつ)で分析する場合には、Browser Agentパッケージを1つ作成し、「エンドユーザー情報」には「エンドユーザー属性(E-mailアドレス)」または「エンドユーザー属性(ユーザー名と会社名)」のどちらかを指定します。(どちらもカスタマイズ可能)

参照

パッケージの作成については、「4.3.1 パッケージの作成」を参照してください。

4.5.3 エンドユーザーマシン属性で分析する場合

測定結果をエンドユーザーマシン属性(「IPアドレス」か「収集サーバから見たIPアドレス」のどちらか)で分析する場合には、Browser Agentパッケージを1つ作成し、「エンドユーザー情報」には「エンドユーザーマシン属性(IPアドレス)」か「エンドユーザー属性(収集サーバから見たIPアドレス)」のどちらかを指定します。

4.6 表示

エンドユーザレスポンス情報は、以下の方法で表示することができます。

- コンソールのサマリ表示

  サマリツリー内のUserResponseMonitorで表示します。

- コンソールの詳細表示

  詳細ツリー内のProxy Managersフォルダで表示します。

- レポート

  ― 総点検分析・レポート

  ― カテゴリ別診断分析・レポート

  ― 詳細分析・レポート

4.6.1 エンドユーザレスポンスの詳細データについて

WEBSLM_URL、WEBSLM_TCP、WEBSLM_DNSのデータ収集が必要な場合は、Browser Agentをインストールした環境で、以下のコマンドを実行してください。

注意

測定対象のWebサーバがHTTPSの場合は、WEBSLM_URL、WEBSLM_TCP、WEBSLM_DNSのデータを収集できません。

1. 管理者権限でログインします。
2. コマンドプロンプトを起動して、以下のフォルダに移動します。

   ポイント

   Windows Vista(R)、Windows(R)7の場合は、[スタート]メニューから、[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]メニューを右クリックし、[管理者として実行]を選択してコマンドプロンプトを起動してください。

   ```
   <Browser Agentインストールディレクトリ>¥tool
   ```

3. 以下のようにコマンドを実行します。

   ```
   instlsp -install
   ```

4. マシンを再起動します。

ただし、詳細データを収集する場合に、排他製品があります。排他製品については、「4.3.2.3 排他製品」を参照してください。

注意

WEBSLM_URL、WEBSLM_TCP、WEBSLM_DNSの詳細については、リファレンスマニュアル「4.2.1 ResponseConditionフォルダ配下/エンドユーザレスポンスレポート」を参照してください。

なお、WEBSLM_URL、WEBSLM_TCP、WEBSLM_DNS のデータ収集を停止するには、Browser Agentをインストールした環境で、以下のコマンドを実行してください。

1. 管理者権限でログインします。
2. コマンドプロンプトを起動して、以下のフォルダに移動します。

   ポイント

   Windows Vista(R)、Windows(R)7の場合は、[スタート]メニューから、[すべてのプログラム]-[アクセサリ]-[コマンドプロンプト]メニューを右クリックし、[管理者として実行]を選択してコマンドプロンプトを起動してください。

   ```
   <Browser Agent のインストールディレクトリ>¥tool
   ```

3. 以下のようにコマンドを実行します。

   ```
   instlsp -remove
   ```

4. マシンを再起動します。

■非互換情報

V13.3.0では、Browser Agent 機能において以下のRecord IDのデータをデフォルトで収集しなくなりました。

- WEBSLM_URL
- WEBSLM_TCP
- WEBSLM_DNS

WEBSLM_URL、WEBSLM_TCP、WEBSLM_DNSの詳細については、リファレンスマニュアル「4.2.1 ResponseCondition フォルダ配下/エンドユーザレスポンスレポート」を参照してください。

第5章 サービス稼働管理

本章では、サービス稼働状況の管理方法について説明します。

■実行環境

Manager/Proxy Managerで実行可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

5.1 測定の概要

サービスの稼働管理は、管理対象となったHTTPやDNSなどのサービスに対して、定期的に問い合わせ～応答確認することにより、稼働状況を監視します。

監視することができるサービスの種類には以下があります。

- HTTP(GET/POST) - Jsp/Servelet/Soapなどの通信を含みます
- DNS
- SMTP
- 任意TCPポート

ポイント

HTTPSの場合は、SSL 2.0のみ監視可能です。

5.2 環境設定

監視対象とするサービスに関する情報をレスポンス・稼働管理対象構成情報(ServiceConf.xml)に定義します。

- HTTPサービスを監視する場合は、HTTP稼働情報(HTTP_Serviceタグ)に
- DNSサービスを監視する場合には、DNS稼働情報(DNS_Serviceタグ)に
- SMTPサービスを監視する場合には、SMTP稼働情報(SMTP_Serviceタグ)に

任意のポートを監視する場合には、PORT稼働情報(PORT_Serviceタグ)をそれぞれ定義します。

定義方法は、「第6章 レスポンス・稼働管理対象構成情報(ServiceConf.xml)」を参照してください。

5.3 表示

サービスの稼働情報は、以下の方法で表示することができます。

- コンソールのサマリ表示

  サマリツリー内のServiceAvailMonitorで表示します。

- コンソールの詳細表示

  詳細ツリー内のServiceConditionフォルダーで表示します。

- レポート

  ― 総点検分析・レポート

  ― カテゴリ別診断分析・レポート

  ― 詳細分析・レポート

5.4 サービス稼働監視タイムアウト値設定

サービス稼働監視において、1監視対象あたり1タイムアウト値の設定手順を説明します。

ポイント

サービス稼働管理を行う場合に、サービス稼働監視タイムアウト値を変更する必要がある場合は、本手順を実施してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥template.dat

【UNIX版】

/etc/opt/FJSVssqc/template.dat

サービス稼働監視機能には2種類のタイムアウトが存在します。

・ **収集タイムアウト値**
収集タイムアウト値は、収集処理（収集間隔の度に動作する処理）時間の上限値です。デフォルト値は70秒です。
収集タイムアウトが発生した場合、収集間隔内で収集したデータはすべて無効となり、性能情報レコードは作成されません。

・ **監視タイムアウト値**
監視タイムアウト値は、監視対象へのリクエストの応答を受信するまでの時間の上限値です。デフォルト値は10秒です。
監視タイムアウトが発生した場合、タイムアウトした監視対象の性能値に"-1"が格納されます。

注意

"-1"が格納されるのはタイムアウト以外に通信エラーが発生した場合にも格納されます。

■監視対象を定義する上での考え方

収集タイムアウトが発生すると性能情報レコード自体の作成ができないことから、正常な監視を行うためには、収集タイムアウトが発生しないように定義する必要があります。

監視対象が複数存在する場合に、監視対象すべてに監視タイムアウトが発生した場合を考慮するため、監視可能な数は以下の計算式が成り立つ必要があります。

監視対象数 × 監視タイムアウト値(10秒) < 収集タイムアウト値(70秒)

※デフォルトでの監視対象数の最大値は6つです。

テンプレートファイル(template.dat)にて、サービス稼働監視の機能に対して以下の項目が変更可能です。

・ 収集間隔　　：1、2、5、10(分)の指定が可能
・ 監視タイムアウト値 ：収集間隔以下の任意の値
・ 収集タイムアウト値 ：5秒～収集間隔＋30秒

注意

監視タイムアウト値を長くすると、監視可能な数が少なくなるため、設定される際は監視対象数を考慮して設定してください。

「A.2 レスポンス・稼働情報収集ポリシーセットアップコマンド」により、監視対象数とタイムアウト値が上記の計算式に沿った正しい設定になっていない場合は、警告メッセージが出力されます。また、警告メッセージが出力されても、ポリシーは作成されます。

監視対象数が多い場合、かつ監視対象の設定に問題がある場合はコマンドの完了復帰が遅くなる場合があります。

■使用する情報

収集タイムアウト値

template.dat PINGセクション CMDTIMEOUTパラメータ 省略時70秒

監視タイムアウト値

template.dat PINGセクション TIMEOUTパラメタ 省略時10秒

監視対象数

ServiceConf.xml 監視種別ごとに数をまとめます。

5.4.1 定義方法

PINGセクションに以下のパラメタを追加します。

監視対象数とレスポンス時間の上限値を考慮して、以下の計算式が成り立つようにパラメタの設定を行います。

計算式:

監視対象数 × 監視タイムアウト値 < 収集タイムアウト値

パラメタ名	意味	デフォルト値
INTERVAL	収集間隔	(省略時)1(単位は分)
TIMEOUT	監視タイムアウト値	(省略時)10(単位は秒)
CMDTIMEOUT	収集タイムアウト値	(省略時)70(単位は秒)

■定義例

収集間隔1分、収集タイムアウト値70秒、監視タイムアウト値20秒の場合

```
##########################################
# ProtoPing Information
[PING]
DCAID="PING"
TIMEOUT=20
```

注意

「A.2 レスポンス・稼働情報収集ポリシーセットアップコマンド」を実行した場合、監視対象数と監視タイムアウト値の組み合わせによって以下の警告メッセージが出力されることがあります。

```
sqcAPolicy template.dat warning.
(The time taken for monitoring processing may exceed the collection interval
depending on the timeout value and the number of monitoring targets
specified with the <PORT> tag.)
```

その場合は、監視タイムアウト値を減らすか、収集タイムアウト値を増やして上記の計算式に沿った正しい設定になっているか確認してください。

ただし収集タイムアウト値は、5秒～収集間隔＋30秒の範囲内で設定してください。

第6章 レスポンス・稼働管理対象構成情報 (ServiceConf.xml)

下記の節にて、サービス稼働管理またはエンドユーザレスポンス管理を行う場合、本章を実施してください。

導入手引書

- 3.2 ManagerとAgentで構成する基本モデル
- 3.3 Proxy Managerによる中継モデル
- 3.4 Managerの二階層運用モデル
- 3.5 Managerの二重化運用モデル
- 3.6 MSCS/フェールオーバークラスタリングクラスタシステム運用モデル
- 3.7 PRIMECLUSTERクラスタシステム運用モデル

■実行環境

Manager/Proxy Managerで実行可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

本構成情報ファイルは、XMLの構造になっています。管理対象単位に、ツリー構造を持ったタグを追加していくという定義方法になります。

注意

動作環境として、Microsoft(R) Windows 2000 Professional以降、Microsoft Internet explorer5.5以降が必要です。

本XMLツールで編集した、もしくはWindowsサーバ上で編集したレスポンス・稼働管理対象構成情報 (ServiceConf.xml) をftp で該当サーバへ転送する場合は、ASCIIモードで転送してください。

ポイント

- レスポンス情報については、Browser Agentの管理対象とするサイト名を定義します。
- 稼働管理情報については、HTTP、DNS、SMTP、PORTの監視対象をそれぞれ定義します。
- クラスタシステム運用を行っている場合は、現用系でSystemwalker Service Quality Coordinatorの可変ファイル格納ディレクトが確認できる状態で実施してください。

XMLファイルの編集は、本製品のCD-ROMの、以下の場所に添付されているXMLエディタを使用すると、簡単に編集することができます。
以下のファイルを任意のフォルダにコピーしてから使用してください。

■格納場所

【Windows版】

```
<CD-ROM>
   |
   +-tools
       |
       +-xml
          |
          +-OpeneXeed.exe
```

【UNIX版】

UNIX版のCD-ROMをWindowsマシンから直接参照する場合は、以下の手順を行います。

1. WindowsマシンのCD-ROM装置に本製品のSolaris版/Linux版CD-ROMをセットします。
2. 以下のファイルを任意のディレクトリにコピーします。

```
<CD-ROM>
   |
   +-FJSVssqc
       |
       +-tools.exe
```

3. 2でコピーしたファイルは自己解凍形式です。ダブルクリックして解凍します。

   解凍すると、CD-ROMと同じディレクトリ構成が作成されます。

   XMLエディタを使用するには、以下のファイルを実行します。

```
<任意のディレクトリ>
   |
   +-tools
       |
       +-xml
          |
          +-OpeneXeed.exe
```

以下、ServiceConf.xmlの定義方法について説明します。

6.1 格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥ServiceConf.xml

【UNIX版】

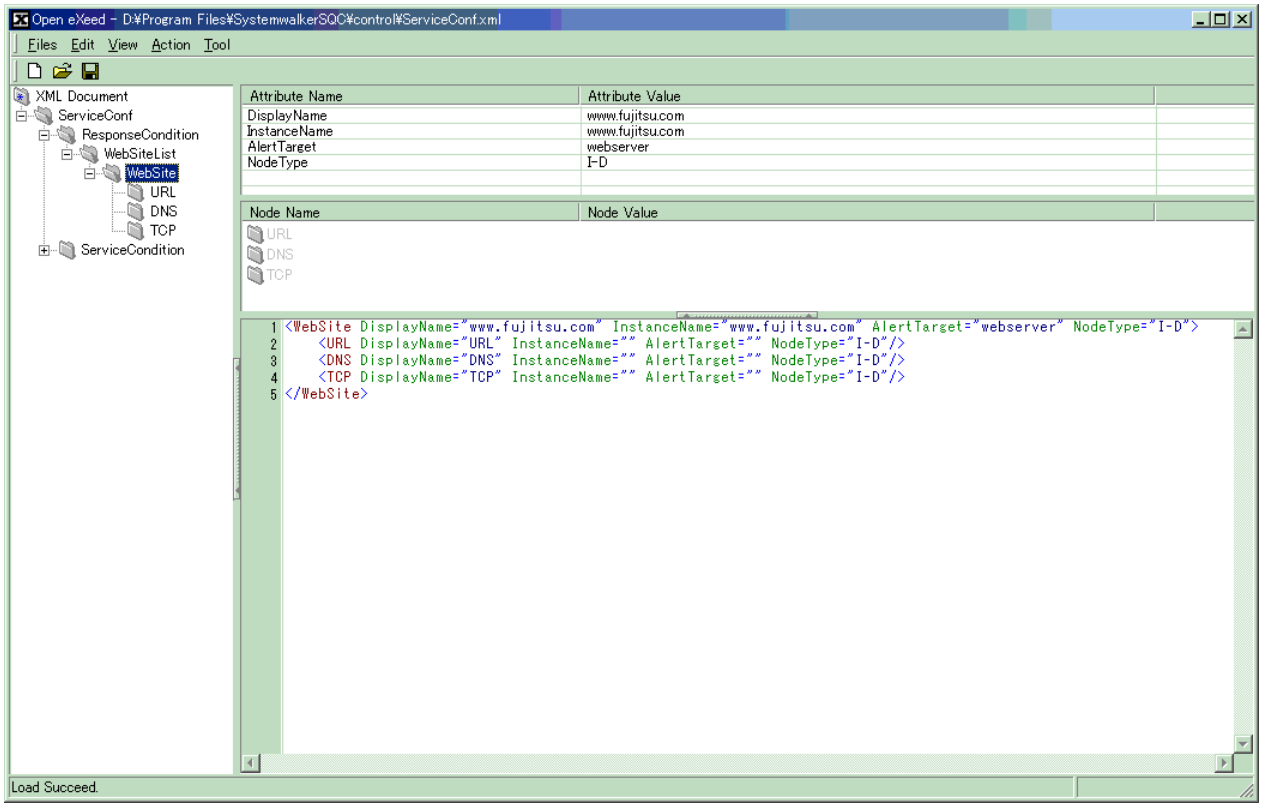
/etc/opt/FJSVssqc/ServiceConf.xml

上記と同じディレクトリ上にServiceConf.sampleというサンプルファイルがあります。このサンプルのバックアップを取り、ServiceConf.xmlとリネイムして編集してください。

6.2 定義方法

以降の項で各タグの定義方法を説明しています。本製品CD-ROM付属のXMLエディタを使用する場合は、以下がポイントになります。

- 各タグは、XMLエディタのツリー(View:XML Structure)で確認してください。
- 属性を定義する場合は、ツリー上で編集対象のタグを選択し、タグの属性が表示されている箇所(View:XML Data)において定義する属性名(Attribute Name)をダブルクリック、または右クリックメニューの[Edit」から表示される[属性の編集」ウインドウにて属性を定義してください。
- タグ単位に追加をする場合は、[Edit]メニューの[Copy][Paste]や右クリックメニューの[Duplicate]または[Copy][Paste]などを使用すると、簡単に編集できます。



注意

定義する際には、サンプルファイルをもとに編集してください。サンプルファイルの各タグの中には「Node Type」という属性名が含まれています。この属性についてはサンプルファイルに記述されている属性をそのまま使用し、変更しないでください。

定義する文字列に全角文字列、および以下の記号を使用することはできません。

¥ : , < > " $ '[ ] = & _ %

以下、各タグの定義方法を説明します。

- 6.2.1 レスポンス情報(WebSiteタグ)
- 6.2.2 HTTP稼働情報(HTTP_Serviceタグ)
- 6.2.3 DNS稼働情報(DNS_Serviceタグ)
- 6.2.4 SMTP稼働情報(SMTP_Serviceタグ)
- 6.2.5 PORT稼働情報(PORT_Serviceタグ)

6.2.1 レスポンス情報(WebSiteタグ)

WebSiteタグには、Browser Agentが管理対象とするサイト名を定義します。

属性名	定義内容	定義例
DisplayName	コンソール上に表示する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) ・全角文字(ただしShift-JISのみ使用可) 長さの制限は、半角全角に係わらず64文字以内です。	www.fujitsu.com
InstanceName	Browser Agentが管理対象とするサイトのホスト名を定義します。	www.fujitsu.com
AlertTarget	管理対象となったサイト名に対応する、Centric Managerが認識するノード名を定義します。Centric Managerメッセージ連携を行っている場合、アラーム発生元のノードになります。 省略した場合は、この定義が存在するManagerもしくは、Proxy Managerがアラーム発生元ノードになります。	webserver
NodeType	注意 制御情報です。この属性についてはサンプルファイルに記述されている属性をそのまま使用してください。	I-D

注意

WebSiteタグの子タグ(<WebSite>から</WebSite>までの間のタグ)には変更する属性はありません。サンプルファイルに記述されているまま修正しないでください。

ポイント

サイト名を複数定義する場合は、WebSiteタグ(<WebSite>から</WebSite>までのブロック)を、複数定義してください。

レスポンス収集対象を削除する場合は、<WebSite>から</WebSite>までのブロックを削除してください。

6.2.2 HTTP稼働情報(HTTP_Serviceタグ)

HTTP_Serviceタグには、稼働監視対象のHTTPサービスに関する情報を定義します。

属性名	定義内容	定義例
DisplayName	コンソール上に表示する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) ・全角文字(ただしShift-JISのみ使用可) 長さの制限は、半角全角に係わらず64文字以内です。	HTTPPage1
InstanceName	監視対象となるHTTPサービスを識別する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) 長さの制限は、64文字以内です。	HTTPPage1
AlertTarget	管理対象となったサイト名に対応する、Centric Managerが認識するノード名を定義します。Centric Managerメッセージ連携を行っている場合、アラーム発生元のノードになります。 省略した場合は、この定義が存在するManagerもしくは、Proxy Managerがアラーム発生元ノードになります。	webserver
IP_Address	IPベースのバーチャルホストを利用している場合、監視対象のサービスにアクセスするための論理IPアドレスを設定してください。それ以外は省略可能です。	100.100.100.100
URL	監視対象のサービスにアクセスするためのURLを設定してください。	http://host[:port]/path https://host[:port]/path
ProxyServer	Proxyサーバを経由する場合は“ON“。直接サービスにアクセスする場合は、“OFF“を定義してください。	ON
ProxyServer_Addr	Proxyサーバを経由する場合に、ProxyサーバのIPアドレスを定義してください。 直接サービスにアクセスする場合は、空文字列 "" を指定してください。	100.100.100.100
ProxyServer_Port	Proxyサーバを経由する場合に、Proxyサーバのポート番号を定義してください。 直接サービスにアクセスする場合は、空文字列 "" を指定してください。	8080
BodyFile	HTTPのPOSTメソッドでアクセスする形態の場合に、送信するBODYデータを記述したファイル(BODYファイル)の絶対パスを定義してください。 HTTPのPOSTメソッドでアクセスしない(空文字列 "" を定義)場合、GETメソッドが使用され、BODYファイルを指定した場合、POSTメソッドが使用されます。 **注意** BODYファイルを指定する場合は、必ず指定したパスにBODYファイルを用意してください。	C:¥temp¥body.txt /var/temp/body.txt

属性名	定義内容	定義例
BasicAuthentication	監視対象のURLが、Basic認証を行っている場合は“ON“。それ以外は“OFF“を定義してください。	ON
BasicAuthentication _User	Basic認証を行う場合に、アクセス可能なユーザーIDを設定してください。 それ以外は空文字列 "" を定義してください。	User1
BasicAuthentication _PassWord	Basic認証を行う場合に、アクセス可能なユーザーのパスワードを設定してください。 それ以外は空文字列 "" を定義してください。	User1
NodeType	**注意** 制御情報です。この属性についてはサンプルファイルに記述されている属性をそのまま使用してください。	I-D

ポイント

HTTPサービスを複数監視する場合は、HTTP_Service タグ(<HTTP_Service>から</HTTP_Service>までのブロック)を、複数定義してください。BODYファイルを複数作成する場合は、すべて同じディレクトリに格納してください。BODYファイルの作成方法については、「6.5 BODYファイルの作成方法」を参考にしてください。

HTTPサービス収集対象を削除する場合は、<HTTP_Service>から</HTTP_Service>までのブロックを削除してください。

6.2.3 DNS稼働情報(DNS_Serviceタグ)

DNS_Serviceタグには、稼働監視対象のDNSサービスに関する情報を定義します。

属性名	定義内容	定義例
DisplayName	コンソール上に表示する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) ・全角文字(ただしShift-JISのみ使用可) 長さの制限は、半角全角に係わらず64文字以内です。	DNS
InstanceName	監視対象となるDNSサービスを識別する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) 長さの制限は、64文字以内です。	DNS
AlertTarget	管理対象となったサイト名に対応する、Centric Managerが認識するノード名を定義します。Centric Managerメッセージ連携を行っている場合、アラーム発生元のノードになります。 省略した場合は、この定義が存在するManagerもしくは、Proxy Managerがアラーム発生元ノードになります。	dnsserver
IP_Address	監視対象のIPアドレスを定義します。	100.100.100.100
Port	監視対象のPort番号を定義します。	53
TargetHost	名前解決を行うホスト名を定義します。	abcserver
NodeType		I-D

属性名	定義内容	定義例
	注意 制御情報です。この属性についてはサンプルファイルに記述されている属性をそのまま使用してください。	

ポイント

DNSサービスを複数監視する場合は、DNS_Service タグ(<DNS_Service>から</DNS_Service>までのブロック)を、複数定義してください。

DNSサービス収集対象を削除する場合は、<DNS_Service>から</DNS_Service>までのブロックを削除してください。

6.2.4 SMTP稼働情報(SMTP_Serviceタグ)

SMTP_Serviceタグには、稼働監視対象のSMTPサービスに関する情報を定義します。

属性名	定義内容	定義例
DisplayName	コンソール上に表示する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) ・全角文字(ただしShift-JISのみ使用可) 長さの制限は、半角全角に係わらず64文字以内です。	SMTP
InstanceName	監視対象となるSMTPサービスを識別する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) 長さの制限は、64文字以内です。	SMTP
AlertTarget	管理対象となったサイト名に対応する、Centric Managerが認識するノード名を定義します。Centric Managerメッセージ連携を行っている場合、アラーム発生元のノードになります。 省略した場合は、この定義が存在するManagerもしくは、Proxy Managerがアラーム発生元ノードになります。	smtpserver
IP_Address	監視対象のIPアドレスを定義します。	100.100.100.100
Port	監視対象のPort番号を定義します。	25
NodeType	注意 制御情報です。この属性についてはサンプルファイルに記述されている属性をそのまま使用してください。	I-D

ポイント

SMTPサービスを複数監視する場合は、SMTP_Service タグ(<SMTP_Service>から</SMTP_Service>までのブロック)を、複数定義してください。

SMTPサービス収集対象を削除する場合は、<SMTP_Service>から</SMTP_Service>までのブロックを削除してください。

6.2.5 PORT稼働情報(PORT_Serviceタグ)

PORT_Serviceタグには、稼働監視対象の任意ポートに関する情報を定義します。

属性名	定義内容	定義例
DisplayName	コンソール上に表示する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) ・全角文字(ただしShift-JISのみ使用可) 長さの制限は、半角全角に係わらず64文字以内です。	PORT123
InstanceName	監視対象となる任意ポートを識別する名前を定義します。 以下の文字が使用できます。 ・半角英数字 ・半角記号(ただし¥:,<>"$'[]=&以外) 長さの制限は、64文字以内です。	PORT123
AlertTarget	管理対象となったサイト名に対応する、Centric Managerが認識するノード名を定義します。Centric Managerメッセージ連携を行っている場合、アラーム発生元のノードになります。 省略した場合は、この定義が存在するManagerもしくは、Proxy Managerがアラーム発生元ノードになります。	server123
IP_Address	監視対象のIPアドレスを定義します。	100.100.100.100
Port	監視対象のPort番号を定義します。	123
NodeType	注意 制御情報です。この属性についてはサンプルファイルに記述されている属性をそのまま使用してください。	I-D

ポイント

任意ポートを複数監視する場合は、PORT_Service タグ(<PORT_Service>から</PORT_Service>までのブロック)を、複数定義してください。

PORTサービス収集対象を削除する場合は、<PORT_Service>から</PORT_Service>までのブロックを削除してください。

6.3 定義例

以下、Webサイトタグに Browser Agentが管理対象とするサイト名「www.fujitsu.com」を定義し、HTTP_Serviceタグには、二つの監視対象「AAAPage」と「BBBPage」を定義し、さらにDNS_Serviceタグ、SMTP_Serviceタグ、PORT_Serviceタグを定義した例です。

定義例をコピーし、OpeneXeedのXML Sourceに貼り付け上書きをしてください。

定義が更新され、XML Structureの構成など確認することができます。

```
<?xml version="1.0" encoding="Shift_JIS"?>

<ServiceConf DisplayName="ManagedObject" NodeType="F">
```

```
<ResponseCondition DisplayName="ResponseCondition" NodeType="F">
<WebSiteList DisplayName="WebSites" NodeType="F">
<WebSite DisplayName="www.fujitsu.com" InstanceName="www.fujitsu.com" AlertTarget=""
NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
<URL DisplayName="URL" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</URL>
<DNS DisplayName="DNS" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</DNS>
<TCP DisplayName="TCP" InstanceName="" AlertTarget="" NodeType="I-D">
<ResourceList DisplayName="Resources(URL)" InstanceName="" NodeType="F"/>
</TCP>
</WebSite>
</WebSiteList>
</ResponseCondition>
<ServiceCondition DisplayName="ServiceCondition" NodeType="F">
<Default_ProxyServer Addr="" Port=""/>
<HTTP_ServiceList DisplayName="HTTP" NodeType="F">
<HTTP_Service DisplayName="AAA Home Page" InstanceName="AAAPage"
AlertTarget="manet" NodeType="I-D" IP_Address="" URL="http://manet.fujitsu.co.jp/"
ProxyServer="OFF" ProxyServer_Addr="" ProxyServer_Port="" BodyFile=""
BasicAuthentication="OFF" BasicAuthentication_User="" BasicAuthentication_PassWord=""/>
<HTTP_Service DisplayName="BBB Home Page" InstanceName="BBBPage"
AlertTarget="ent" NodeType="I-D" IP_Address="" URL="http://ent.fujitsu.co.jp/"
ProxyServer="OFF" ProxyServer_Addr="" ProxyServer_Port="" BodyFile=""
BasicAuthentication="OFF" BasicAuthentication_User="" BasicAuthentication_PassWord=""/>
</HTTP_ServiceList>
<DNS_ServiceList DisplayName="DNS" NodeType="F">
<DNS_Service DisplayName="DNS" InstanceName="DNS" AlertTarget="dnsserver"
IP_Address="100.100.100.100" Port="53" TargetHost="abcserver" NodeType="I-D"/>
</DNS_ServiceList>
<SMTP_ServiceList DisplayName="SMTP" NodeType="F">
<SMTP_Service DisplayName="SMTP" InstanceName="SMTP" AlertTarget="smtpserver"
IP_Address="100.100.100.100" Port="25" NodeType="I-D"/>
</SMTP_ServiceList>
<PORT_ServiceList DisplayName="PORT" NodeType="F">
<PORT_Service DisplayName="PORT123" InstanceName="PORT123"
AlertTarget="server123" IP_Address="100.100.100.100" Port="123" NodeType="I-D"/>
</PORT_ServiceList>
</ServiceCondition>
</ServiceConf>
```

6.4 セットアップ

本ファイルの編集内容を有効にするには、収集ポリシーの作成と適用を実施する必要があります。

「A.2 レスポンス・稼働情報収集ポリシーセットアップコマンド」を参照して、sqcAPolicy、およびsqcSetPolicyを実行してください。

6.5 BODYファイルの作成方法

HTTPサービスの稼働監視で、HTTP POST通信を行って監視する場合、本章で説明する注意事項を参考にBODYファイルを作成してください。

■BODYファイルに記載する必要のあるものと記載する必要がないもの

POSTメソッドのWebサービスを監視する場合には、クライアントがPOSTメソッドによりWebサービスに送信するメッセージのうち、監視対象のサービスが要求するHTTPヘッダー、パラメタ、およびパラメタの値をBODYファイルに定義します。

よって、BODYファイルに記載する内容は監視対象のサービスによって変わります。本節ではBODYファイルに記載する必要のあるもの、および記載する必要がないものについて説明します。

なお、BODYファイルを作成する前に、監視対象のサービスが要求するパラメタをあらかじめ調査しておく必要があります。

以下に送信データ例を挙げて、説明します。

POSTの場合の送信データ例

```
1 POST /examples/servlet/HttpTestServlet HTTP/1.1
2 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
3 Accept-Language: ja
4 Content-Type: application/x-www-form-urlencoded
5 Accept-Encoding: gzip, deflate
6 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Q312461; .NET CLR 1.0.3705)
7 Host: localhost:8001
8 Content-Length: 33
9 Connection: Keep-Alive
10 Cache-Control: no-cache
11 空行
12 msg=Hello+World&submit=%91%97%90M
```

上記の例の場合、BODYファイルを使用した監視を行う場合には、青字部分のメッセージとファイルの最後に改行を追加したBODYファイルを用意してください。

以下に上記の例の場合の、BODYファイルの定義を示します。

```
1 Content-Type: application/x-www-form-urlencoded
```

2 空行

3 msg=Hello+World&submit=%91%97%90M

1. HTTPヘッダー Content-Type を付加します。(必須)
2. 2. ヘッダーの終了を表わす改行(必須)
3. 3. パラメタおよび値(必須)

注意

BODYファイルに記載する内容は、監視するWebサービスに依存します。

HTTPヘッダーの意味については、Webサービスの開発者に問い合わせてください。

以下に注意点を示します。

項目	注意点
BODYファイルのファイルサイズ	ファイルサイズは全て含めて64kByteまでです。 ファイルサイズの制限をオーバーした場合、それ以降のデータは切り捨てられ、その場合の動作は保証されません。
格納ディレクトリ	複数のHTTPサービスを監視する際、BODYファイルは必ず同じディレクトリに格納してください。
ファイル名	ファイル名は、一意の半角英数字で定義してください。また、ファイルタイプはプレーンテキスト(拡張子:".txt")です。
サポートするHTTPプロトコルバージョン	HTTP/1.0
HTTPメッセージボディのメッセージ長(Content-Length HTTPヘッダー)	HTTPメッセージヘッダーにメッセージ長を記述する必要はありません。 HTTPメッセージのボディ部分のメッセージ長は、サービス処理性能監視機能が自動的に計算し、Content-Length HTTPヘッダーを追加して、Webサーバに送信します。 記述した場合(Content-Lengthヘッダーを多重定義した場合)の動作については送信先のWebサーバの仕様に依存します。
文字コード	BODYファイルの文字コードはWebサーバ、アプリケーションサーバで受け取れる文字コードにしてください。サービス処理性能監視機能では文字コードの変換は行いません。 特に日本語を使用する場合は注意が必要です。 **注意** また、サービス処理性能監視機能ではBase64エンコード・デコードを行いません。 通常、SOAP(XML)メッセージは UTF-8、UTF-16 を使用するため、BODYファイルの文字コードは、UTF8あるいはANSIとしてください。 UTF-8については、RFC-2279(RFC 2279 UTF-8, a transformation format of ISO 10646)を参照してください。 Microsoft(R) Windows 2000 に付属されているメモ帳でUTF-8を扱うことが可能です。

■BODYファイルの先頭から最初の文字までの空行は無視される

サービス稼働監視機能では、ファイルの先頭から最初の文字までの空行は無視します。

■BODYファイルの先頭のBOM(Byte Order Mark)を無視する

Microsoft(R) Windows 2000に付属しているメモ帳でUTF-8形式のファイルとして保存すると、ファイルの先頭にBOM(Byte Order Mark)を無条件に挿入します。

サービス稼働監視機能では、このMicrosoft(R) Windows2000で作成されたUTF-8形式のファイルを読み込むときにBOMを無視し、Webサーバには送信しません。

BOMが存在しない場合はファイルの先頭よりWebサーバに送信します。

■BODYファイルの動的変更はできない

サービス稼働監視機能ではBODYファイルを動的に変更できません。したがって、Webサーバからの応答メッセージとBODYファイルを組み合わせてWebサーバに返信は行いません。

サービス登録時[URL]に指定したURLでcookie 等、動的に変化するキーをPOSTしなければならない仕組みには対応していません。

第7章 しきい値監視

しきい値監視とは、システム全体が健全に稼働しているか、異常が発生していないかを監視するための機能です。

本製品では、しきい値監視のしきい値を定義することができます。監視項目の値が定義値を超えた場合に、アラームを通知します。

しきい値超えが発生した時に実行されるアラームアクション定義については「7.3 アラームアクション定義」を参照してください。

■実行環境

Enterprise Manager/Manager/Proxy Manager/Agentで実行可能です。

注意

しきい値監視の定義は、情報を収集しているサーバ上で定義してください。定義を設定したサーバ上でアラーム通知されます。

クラスタシステム運用を行っている場合は、現用系サーバ・待機系サーバ両方でしきい値監視を定義してください。

しきい値監視を定義する場所は以下のとおりです。

- インストール型Agent

  情報を収集しているAgent(Agent機能を使用しているEnterprise Manager/Manager/Proxy Managerも含む)上でしきい値監視を定義してください。
  インストール型Agentのしきい値をProxy Manager/Manager上で定義して、しきい値監視することはできません。

- インストールレス型Agent

  リモートで情報を収集しているManager/Proxy Manager上でしきい値監視を定義してください。

- エンドユーザレスポンス管理

  エンドユーザレスポンスのデータを収集している収集サーバ(Manager/Proxy Manager)上でしきい値監視を定義してください。

- サービス稼働管理

  情報を収集しているManager/Proxy Manager上でしきい値監視を定義してください。

- Webトランザクション量管理

  情報を収集しているManager/Proxy Manager/Agent for Business上でしきい値監視を定義してください。

- エコ情報管理

  情報を収集しているManager/Proxy Manager上でしきい値監視を定義してください。

- ユーザデータ管理

  情報を収集しているAgent(Agent機能を使用しているManager/Proxy Managerを含む)上でしきい値監視を定義してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

以下、しきい値の定義方法について説明します。

- 7.1 しきい値監視定義
- 7.2 しきい値監視定義サンプルファイル
- 7.3 アラームアクション定義

7.1 しきい値監視定義

しきい値監視の定義方法について説明します。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥alertconfig.txt

【UNIX版】

/etc/opt/FJSVssqc/alertconfig.txt

上記ファイルを以下の定義方法に従って編集してください。

注意

上記格納場所にファイルを配置した後、本製品の定期チェック(5分間隔)により、そのファイルの存在が確認されると、自動的に取り込まれ定義内容が反映されます。したがって、ファイルの編集は別の場所で実施して、定義作業が完了した後に上記格納場所に配置してください。

- 7.1.1 定義方法
- 7.1.2 定義例

7.1.1 定義方法

本ファイルは、CSV形式のファイルです。しきい値監視する項目ごとに一行ずつ定義します。

カラム位置	説明
1	しきい値監視ID。一行毎にユニークなIDをつけてください。 **注意** Manager/Proxy Manager上で、インストールレス型Agent機能によりサーバを監視している場合は、「しきい値監視ID」の後ろに「|<ホスト名>」を追加し、<ホスト名>にしきい値監視したいホスト名を設定してください。 <しきい値監視ID>|<ホスト名>

カラム位置	説明
	・ インストールレス型Agent機能により監視するサーバの場合 リモート監視定義ファイル(remoteAgent.txt)の「DISPLAYNAME」で指定したホスト名を<ホスト名>に設定してください。 ・ Manager/Proxy Manager自身のしきい値監視を行う場合 sqcSetPolicyで表示されるホスト名を<ホスト名>に設定してください。 例) しきい値監視IDを「AlertID1」、監視対象のホスト名が「hostnameA」の場合、 AlertID1|hostnameA また、ホスト名にはワイルドカードが使用できます。 例) ホスト名が"aaabbbccc"の場合、"aaabbbccc", "aaa*", "aa?bb?cc?", "???bbb???", "[abc]aa[abc]bb[abc]cc"などの指定が合致します。 「|<ホスト名>」を追加しない場合は、監視している全てのサーバがしきい値監視の対象となります。
2	監視する項目の「レコード番号」。レコード番号の値は、■監視項目のレコード番号とフィールド名対応を参照ください。
3	監視する項目の「フィールド名」＋「レコード番号」を指定します。 例)レコード番号 1052、フィールド名 usrprocを監視する場合は、"usrproc1052" を指定します。 フィールド名およびレコード番号の値は、■監視項目のレコード番号とフィールド名対応を参照ください。
4	監視するリソースのリソースIDを定義します。 リソースIDは、コンソールの詳細表示で、対象ノードのコンテンツを表示することで、"リソースID" カラムから調べることができます。 また、リソースIDにはワイルドカードが使用できます。 例)リソースIDが"aaabbbccc"の場合、"aaabbbccc", "aaa*", "aa?bb?cc?", "???bbb???", "[abc]aa[abc]bb[abc]cc"などの指定が合致します。
5	通知する監視項目の名前を定義します。
6	しきい値監視を行う時間帯の開始時刻を定義します。HH:MM:SSの形式で指定します。省略することはできません。なお、24時間監視する場合は、開始時刻には"00:00:00"を指定してください。
7	しきい値監視を行う時間帯の終了時刻を定義します。HH:MM:SSの形式で指定します。省略することはできません。なお、24時間監視する場合は、終了時刻には"00:00:00"を指定してください。
8	基準のサンプリング回数のうち、何回しきい値超えが発生した場合にアラーム通知するかという、しきい値超え発生回数(N)を定義します。
9	アラーム通知判定の基準のサンプリング回数(M)を定義します。なお、サンプリング回数の最大数は9、最小数は1です。1以上9以下の整数を定義してください。また、サンプリング回数が1の場合は、しきい値超え発生回数には1を定義してください。 なお、しきい値超え発生回数とサンプリング回数は、N >= M/2の関係になるよう定義してください。
10	警告(warning)しきい値
11	異常(error)しきい値
12	">" か "<" を定義します。 ">" - CPU使用率など、値が大きくなった場合にアラーム通知する場合。 "<" - 空きメモリ量など、値が小さくなった場合にアラーム通知する場合。

■監視項目のレコード番号とフィールド名対応

分類	レコード番号	フィールド名	項目の説明
Processor	1052	usrproc	ユーザーモードにおけるCPU使用率。
		sysproc	システムモードにおけるCPU使用率。
		intproc	Unix:IO完了待ち時間。 Windows:IO中断待ち時間。
		totproc	合計CPU使用率。
Memory	1053	freemem	空きメモリ。
		pagins	ページイン数。
		pagflts	ページフォルト数。
		swapused	使用中のスワップまたはページファイル数の割合。
		pagouts	ページアウトされたページ数。
Disk	1054	dskreads	ディスクからの読み込み回数。
		dskwrits	ディスクへの書き込み回数。
		kbread	キロバイト単位でのディスクからの読み込み回数。
		kbwritn	キロバイト単位でのディスクへの書き込み回数。
		dsksrvctim	Read/Writeのサービス時間。
		dskwaittim	Read/Writeの待ち時間。

上記の表に示した情報は、コンソールのサマリ画面に表示される、OSに関するリソース情報です。しきい値監視では、上記以外の項目を監視することもできます。その場合は、リファレンスマニュアル「第4章 データフォーマット」を参照して、該当するレコード番号とフィールド名を指定してください。

ポイント

しきい値監視定義の警告(warning)しきい値、異常(error)しきい値に指定可能な値は下記のとおりです。

- 整数
- 少数(少数の場合、少数点以下第15位まで指定可能です。)
- マイナス値も指定可能です。

指定する値は、半角数字で入力してください。

7.1.2 定義例

以下は、alertconfig.txtの定義例になります。

しきい値の大きさを設定するときは、詳細画面を参照してください。

```
################################################################################
##
# The following examples check the free space on all disks reported in 1018 records.
# The thresholds are a warning for less than 200MB and an error for less than 150MB.
#AlertId1,1018,free1018,*,FreeSpace,00:00:00,00:00:00,1,1,200000000.0,150000000.0,<
```

1,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>

2,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>

3,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<

4,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<

■説明

- ユーザーモードにおけるCPU使用率が、1回でも80%超えが発生したら警告(Warning)、95%超え発生したら異常(error) メッセージが発行されます。

```
1,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
```

- システムモードにおけるCPU使用率が、1回でも95%超え発生したら異常(error) メッセージが発行されます。

```
2,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,95,95,>
```

- 空きメモリが、6分で3回30%を切ったら警告(warning) メッセージが発行されます。

  ※メモリが1G(=1,000,000,000byte)の場合

```
3,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
```

- 空きメモリが、1回でも5%を切ったら異常(error) メッセージが発行されます。

  ※メモリが1G(=1,000,000,000byte)の場合

```
4,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
```

注意

Manager/Proxy Manager上で、インストールレス型Agent機能により、複数のサーバを監視している場合に、システム名「HostnameA」と「HostnameB」をしきい値監視したい場合は、以下のように設定してください。

```
HostnameA1|HostnameA,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameA2|HostnameA,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameA3|HostnameA,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
HostnameA4|HostnameA,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
HostnameB1|HostnameB,1052,usrproc1052,Total,UserCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameB2|HostnameB,1052,sysproc1052,*,SysCPU,00:00:00,00:00:00,1,1,80,95,>
HostnameB3|HostnameB,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,3,6,300000000,0,<
HostnameB4|HostnameB,1053,freemem1053,*,MEMORY,00:00:00,00:00:00,1,1,50000000, 50000000,<
```

1カラム目の「しきい値監視ID」は必ず任意のユニークなIDを設定してください。

7.2 しきい値監視定義サンプルファイル

しきい値監視定義ファイルのサンプルを使用することで、以下のサーバ性能情報の監視項目をしきい値監視できます。

■Windowsサーバ性能情報

監視対象がWindowsの場合に、サンプルを使用すると、以下のサーバ性能情報をしきい値監視することができます。

No.	監視項目	評価方法
1	CPU使用率[%]	使用率が80%(使用時間の場合、60秒間のうち使用時間が48秒)を継続的に超えるような場合、CPUがボトルネックとなって性能問題が発生している、または発生する可能性があります。
2	物理ディスクアイドル時間[sec]	物理ディスクのビジー率が継続的に60%以上(物理ディスクのアイドル時間の場合、60秒間のうち物理ディスクのアイドル時間が24秒以下)で推移する場合、ディスク負荷がボトルネックとなって性能問題が発生している、または発生する可能性があります。
3	ディスクスペース空き率[%]	ディスクのスペースの空き容量が少なくなった場合、業務が停止する可能性があります。
4	メモリ空き容量[bytes]	空きメモリ量が4MB付近を断続的に推移する場合、メモリ不足がボトルネックとなって性能問題が発生している、または発生する可能性があります。

■Solarisサーバ性能情報

監視対象がSolarisの場合に、サンプルを使用すると、以下のサーバ性能情報をしきい値監視することができます。

No.	監視項目	評価方法
1	CPU使用率[%]	使用率が90%(使用時間の場合、60秒間のうち使用時間が54秒)を継続的に超えるような場合、CPUがボトルネックとなって性能問題が発生している、または発生する可能性があります。
2	物理ディスクビジー時間[sec]	物理ディスクのビジー率が継続的に60%以上(物理ディスクのビジー時間の場合、60秒間のうち物理ディスクのビジー時間が32秒以上)で推移する場合、ディスク負荷がボトルネックとなって性能問題が発生している、または発生する可能性があります。
3	ディスクスペース空き率[%]	ディスクのスペースの空き容量が少なくなった場合、業務が停止する可能性があります。
4	メモリ空き容量[bytes]	空きメモリ量がlotsfree(注1)付近を断続的に推移する場合、メモリ不足がボトルネックとなって性能問題が発生している、または発生する可能性があります。

(注1) カーネルパラメタlotsfreeの設定値の確認は、kstatコマンドで行う必要があります。デフォルトは、物理メモリの1/64か512Kバイト(大きい方)になります。詳細は、Solarisのマニュアルを参照してください。

■Linuxサーバ性能情報

監視対象がLinuxの場合に、サンプルを使用すると、以下のサーバ性能情報をしきい値監視することができます。

No.	監視項目	評価方法
1	CPU使用率[%]	使用率が90%(使用時間の場合、60秒間のうち使用時間が54秒)を継続的に超えるような場合、CPUがボトルネックとなって性能問題が発生している、または発生する可能性があります。
2	物理ディスクビジー時間[sec]	物理ディスクのビジー率が継続的に80%以上(物理ディスクのビジー時間の場合、60秒間のうち物理ディスクのビジー時間が48秒以上)で推移する場合、ディスク負荷がボトルネックとなって性能問題が発生している、または発生する可能性があります。
3	ディスクスペース空き率[%]	ディスクのスペースの空き容量が少なくなった場合、業務が停止する可能性があります。

No.	監視項目	評価方法
4	メモリ空き容量[bytes]	空きメモリ量が低い値を断続的に推移する場合、メモリ不足がボトルネックとなって性能問題が発生している、または発生する可能性があります。 空きメモリ量のしきい値は、Linuxのバージョン/エディション/搭載メモリサイズなどにより異なります。運用に合わせて変更してください。サンプルファイルは、5,120KBに設定しています。

■格納先

サンプルファイルの格納ディレクトリは以下のとおりです。

【Windows版】

```
<インストールディレクトリ>¥sample¥alertconfig.txt
```

【UNIX版】

```
/opt/FJSVssqc/sample/alertconfig.txt
```

ポイント

しきい値監視するサーバ上でサンプルを使用する場合は、既に存在するしきい値定義ファイル(alertconfig.txt)のバックアップを取ってから、サンプルを上書きしてください。

7.3 アラームアクション定義

■実行環境

Enterprise Manager/Manager/Proxy Manager/Agentで実施可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

しきい値監視定義をすると、しきい値超えを管理者に知らせるためのアクションが実行されます。アクションの種類には、以下があります。

- イベントログ/syslog
- Systemwalker Centric Managerメッセージ連携
- メール
- トラップ
- ユーザー任意のコマンド実行

インストール終了時には、インストーラからの問い合わせに対して選択した結果に合わせて、イベントログ、もしくはSystemwalker Centric Managerメッセージが設定されています。

注意

- しきい値超えのアラームは、しきい値を超えたタイミングでのみ通知されます。しきい値超えの状態が継続した場合、アラームは始めの1回目のみで通知され、しきい値超えから一度復旧するまで通知されません。
- クラスタシステム運用の場合、現用系サーバと待機系サーバの両方で設定を行ってください。

■格納場所

本ファイルの格納場所は以下のとおりです。

【Windows版】

<インストールディレクトリ>¥bin¥threshold.bat

【UNIX版】

/opt/FJSVssqc/bin/threshold.sh

7.3.1 定義方法

7.3.1.1 アクションの種類の定義

実行したいアクションの種類をONまたはOFFで定義します。ONを選択するとそのアクションが実行されるという意味です。複数の項目をONにすることができます。

定義内容	意味
EVENTLOG="ON"または SYSLOG="ON"	イベントログまたはsyslog
OPAPOST2="OFF"	Systemwalker Centric Managerメッセージ連携
MAIL="OFF"	メール
TRAP="OFF"	トラップ
OTHER="OFF"	ユーザー任意のコマンド実行

注意

- MAIL、TRAP、OTHERを選択した場合は、以降に示す詳細パラメタの定義が必要です。
- 使用しないパラメタについては、定義を"OFF"にし削除しないようにしてください。

- 7.3.1.2 MAILを選択した場合
- 7.3.1.3 TRAPを選択した場合
- 7.3.1.4 OTHERを選択した場合

7.3.1.2　MAILを選択した場合

【Windows版】

Windowsのメール通知に関するパラメタを定義します。

定義内容	意味
MAILSMTPSRV="00.00.00.00"	SMTPサーバのアドレス
MAILSMTPPRT="25"	SMTPサーバのポート
MAILFROM="aa@xx.co.jp"	メールのfromアドレス
MAILTO="bb@xx.co.jp"	メールのtoアドレス
MAILPOP3PRT="110"	POP3サーバのポート(POP認証が必要な場合)
MAILPOP3SRV="00.00.00.00"	POP3サーバのアドレス(POP認証が必要な場合)
MAILAUTHTYPE="Pop"	POP認証が必要な場合に"Pop"を指定
MAILUSERID=""	ユーザーID(POP認証が必要な場合)
MAILPASSWD=""	パスワード(POP認証が必要な場合)
MAILCC="cc@xx.co.jp, dd@xx.co.jp"	メールのccアドレス
MAILBCC="ee@xx.co.jp, ff@xx.co.jp"	メールのbccアドレス
MAILSUB="SSQC threshold %MSGINFO: %2(%3)"	メールのSubject。下記の可変パラメタ(%文字)が指定可能。 %MSGINFO% エラー種別 %2 システム名 %PARA3% 監視項目名 %PARA4% リソースID %5 測定値 %6 しきい値 %7 検出回数 %8 検出基準回数

注意

POP認証が不要な場合は、以下のようにパラメタを修正してください。

- MAILPOP3PRT=""
- MAILPOP3SRV=""
- MAILAUTHTYPE=""
- MAILUSERID=""
- MAILPASSWD=""

【UNIX版】

UNIX版のメール通知に関するパラメタを定義します。

定義内容	意味
MAILSMTPSRV="00.00.00.00"	SMTPサーバのアドレス
MAILSMTPPRT="25"	SMTPサーバのポート
MAILFROM="aa@xx.co.jp"	メールのfromアドレス
MAILTO="bb@xx.co.jp"	メールのtoアドレス
MAILPOP3PRT="110"	POP3サーバのポート(POP認証が必要な場合)
MAILPOP3SRV="00.00.00.00"	POP3サーバのアドレス(POP認証が必要な場合)
MAILAUTHTYPE="Pop"	POP認証が必要な場合に"Pop"を指定
MAILUSERID=""	ユーザーID(POP認証が必要な場合)
MAILPASSWD=""	パスワード(POP認証が必要な場合)
MAILCC="cc@xx.co.jp, dd@xx.co.jp"	メールのccアドレス
MAILBCC="ee@xx.co.jp, ff@xx.co.jp"	メールのbccアドレス
MAILSUB="SSQC threshold $MSGINFO: $2($3)"	メールのSubject。下記の可変パラメタ($文字)が指定可能。 $MSGINFO エラー種別 $2 システム名 $3 監視項目名 $4 リソースID $5 測定値 $6 しきい値 $7 検出回数 $8 検出基準回数

POP認証が不要な場合は、以下のようにパラメタを修正してください。

- MAILPOP3PRT=""
- MAILPOP3SRV=""
- MAILAUTHTYPE=""
- MAILUSERID=""
- MAILPASSWD=""

7.3.1.3　TRAPを選択した場合

トラップ通知に関するパラメタを定義します。

定義内容	意味
TRAPAGT="$2"	Trapのエージェントアドレス
TRAPDEST="hostname"	Trapの送信先アドレス
TRAPCOMMUNITY="public"	Trapのコミュニティ名

定義内容	意味
TRAPENTERPRISE="1.3.6.1.4.1.211"	Trapのenterprise値
TRAPGENERIC="6"	Trapのgeneric値
TRAPSPECIFIC="1"	Trapのspecific値
TRAPOBJNAME="1.3.6.1.4.1.211"	オブジェクト名
TRAPOBJTYPE="2"	オブジェクトタイプ

7.3.1.4　OTHERを選択した場合

ユーザー任意のコマンドを実行することができます。

下記の行にコマンド名を定義します。

```
SQCOTHEREXE=""
```

下記の行からの処理を、コマンド仕様に合わせて編集します。

```
if "%OTHER%"==""ON"" (
```

第8章 Webトランザクション量管理

Webトランザクション量の管理機能は、Webサーバやプロキシサーバを通してシステムに入ってきたトランザクション(処理要求)を分析するための機能です。

Webサーバやプロキシサーバには、ユーザーからのアクセス情報がログファイルに蓄積されています。本機能では、そのログファイルから、リクエスト数、トラフィック量、リクエスト処理時間などを収集します。

本機能は、Webサーバやプロキシサーバのリクエスト状況を総合的に分析するための機能です。Webアクセスログから得られる以下のデータを収集します。

- トラフィック量
- リクエスト処理時間
- リクエスト回数
- エラー回数

■実行環境

Manager/Proxy Manager/Agent for Businessで実行可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

■収集間隔

収集間隔は、5分です。

■定義方法

Webトランザクション量管理の定義方法を説明します。

- 8.1 トランザクションログ定義
- 8.2 セットアップ
- 8.3 表示
- 8.4 トランザクションログ定義サンプルファイル

8.1 トランザクションログ定義

Webトランザクション量を管理するには、まず、トランザクションログ定義ファイルが必要です。本定義ファイルは、トランザクションログ分析機能のログ解析条件を記述したファイルです。

定義作業を行う場合は、サンプルファイルを元にして、定義作業を実施してください。

■格納先

【Windows版】

<インストールディレクトリ>¥sample¥tlawatch.ini

【UNIX版】

/opt/FJSVssqc/sample/tlawatch.ini

作業を行う前に、tlawatch.iniのバックアップを取ってください。

■定義場所

トランザクションログ定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥tlawatch.ini

【UNIX版】

/etc/opt/FJSVssqc/tlawatch.ini

なお、テキストの文字コードは、以下のとおりです。

【Windows版】

シフトJIS

【UNIX版】

日本語EUC

- 8.1.1 定義形式
- 8.1.2 定義内容の確認

8.1.1 定義形式

トランザクションログ定義ファイルは、以下の形式で記述します。

■形式

```
[RequestLog]
Service=service-name
Type=web | proxy
Path=log-path
Format=format-symbol | "format"
TimeZone=timezone
Inclusion=inclusive-record
```

ポイント

- '|' は、「または」の意味で、どちらかが指定できることを意味します。
- 空行は、コメントとして扱われます。
- '#'で始まる行は、コメントとして扱われます。

■説明

[RequestLog]

定義ブロックの開始を表します。また、前の定義ブロックの終了を意味します。定義可能な定義ブロック数は最大20です。

- **Service=service-name**

  分析対象ログの識別名を定義します。service-nameには、識別名を、半角文字を使って64文字以内で指定します。以下は使用できません。

  ```
  ¥ : < > " $ ' [ ] = & / * ? | ,
  ```

  ### 注意

  他の定義ブロックと同じservice-nameを指定することはできません。

- **Type=web | proxy**

  分析対象サーバの種別の定義です。選択肢の意味は以下のとおりです。

選択肢	意味
web	Webサーバ
proxy	プロキシサーバ

  デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

  Type=web

- **Path=log-path**

  分析対象ログファイルのパスを定義します。

  log-path に分析対象ログファイルの絶対パスを指定します。ログファイルが同一ディレクトリ配下に複数作成される場合には、ファイル名にワイルドカード('*') を使用して、複数のファイルすべてを包含したかたちで指定します。パスに空白が含まれる場合は、全体をダブルクォーテーション(")で囲んでください。

  ワイルドカードは、日時やファイルローテーションによって複数のログファイルが作成される場合のファイル名指定を行うために用意されています。任意の文字列に対して指定することは出来ません。

■定義例

	分析対象ログファイル	log-path
Windows版	"C:¥WINNT¥system32¥LogFiles ¥W3SVC3"配下で以下の形式で作成されるログファイル: ex041002.log、ex041003.log、...	C:¥WINNT¥system32¥LogFiles ¥W3SVC3¥ex*.log

	分析対象ログファイル	log-path
UNIX版	"/var/www/logs"配下で以下の形式でlogrotateで作成されるログファイル: accesslog、accesslog.1、accesslog.2、...	/var/www/logs/accesslog

注意

Path文を適切に指定しないと、最新のログファイルが検出できず分析できない場合があります。

- **Format=format-symbol | "format"**

  分析対象ログファイル内の記録形式を定義します。

  format-symbolは、定型の記録形式に対応したシンボルです。

  "format" は、記録形式をトークンと区切り文字で指定します。分析対象ログファイル内の記録形式が、定型の記録形式のどれにも該当しない場合は、"format" で指定してください。

  指定できるシンボル、トークンを一覧表に示します。

  1. format-symbolにログファイルを指定する場合
     - Webサーバのログファイルを分析する場合
     - プロキシサーバのログファイルを分析する場合
  2. "format"にトークンを指定する場合

1. format-symbolにログファイルを指定する場合

   - Webサーバのログファイルを分析する場合

シンボル	対応するログ 対応する"format"
Common	W3Cの Common Logfile Format。以下のログに対応。 W3C httpd (CERN httpd)のCommonログ形式 Apache httpdのCommonログ形式、Customログ形式 Microsoft Internet Information ServicesのCommonログ形式(NCSA共通ログファイル形式)、W3C Extendedログ形式(W3C 拡張ログ ファイル形式) Netscape Enterprise ServerのCommonログ形式、Flexibleログ形式、Customログ形式 Fujitsu InfoProvider ProのCommonログ形式、Extendedログ形式 ....など
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes"
Microsoft-MS50	Microsoft Internet Information Services独自の形式。以下のログに対応。 Microsoft Internet Information Services 5.0のMicrosoft Log Format形式 **注意** Microsoft Internet Information Services 5.0のインストール後、デフォルトの場合のみに有効。
	"s-time{yyyy-mm-dd HH:MM:SS} * * * * s-method s-path * s-status *"

シンボル	対応するログ 対応する"format"
Microsoft-MS60	Microsoft Internet Information Services独自の形式。以下のログに対応。 Microsoft Internet Information Services 6.0のMicrosoft Log Format形式 **注意** Microsoft Internet Information Services 6.0のインストール後、デフォルトの場合のみに有効。
	"s-time{yyyy-mm-dd HH:MM:SS} * * * s-method s-path * s-status * *"

- プロキシサーバのログファイルを分析する場合

シンボル	対応するログ 対応する"format"
Common	W3Cの Common Logfile Format。以下のログに対応。 Netscape Proxy ServerのCommonログ形式、Extendedログ形式、Extended2ログ形式、Flexibleログ形式、Customログ形式 SquidのCommonログ形式 DeleGateのCommonログ形式、Customログ形式 Apache httpdのCommonログ形式、Customログ形式 W3C httpd (CERN httpd)のCommonログ形式 Fujitsu InfoProxyのCommonログ形式 ....など
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes"
Common+Ts	Commonに処理時間(秒)を追加したもの。以下のログまたはそのカスタマイズした形式に適合可能。 Netscape Proxy ServerのFlexibleログ形式、Customログ形式 DeleGateのCustomログ形式 Apache httpdのCustomログ形式
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes s-elapse{s}"
Common+Tms	Commonに処理時間(ミリ秒)を追加したもの。以下のログまたはそのカスタマイズした形式に適合可能。 Netscape Proxy ServerのFlexibleログ形式、Customログ形式 DeleGateのCustomログ形式 Fujitsu InfoProxyのExtendログ形式
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes s-elapse{ms}"
Netscape-Extend	Netscape Proxy Server独自の形式。以下のログに対応。 Netscape Proxy ServerのExtendedログ形式、Extended2ログ形式
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes r-status * * * * * * * s-elapse{s}"

シンボル	対応するログ
	対応する"format"
Squid-Native11	Squid独自の形式。以下のログに対応。 SquidのNativeログ形式 (バージョン1.1形式)
	"s-time{seconds} s-elapse{ms} * */s-status s-bytes s-method s-url * */* *"
Microsoft-Native	Microsoft Proxy Server独自の形式。以下のログに対応。 Microsoft Proxy ServerのWebProxyログ形式
	"*, *, *, *, time{yy/mm/dd, HH:MM:SS}, *, *, *, *, *, *, *, s-elapse{ms}, s-bytes, *, *, *, s-method, s-url, *, *, s-status, *"
DeleGate-Default	DeleGate独自の形式。以下のログに対応。 DeleGateのHTTPのdefaultログ形式
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes s-elapse{ms}:*"
InfoProxy-Extend	Fujitsu InfoProxy独自の形式。以下のログに対応。 Fujitsu InfoProxyのExtendログ形式
	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes s-elapse{ms} r-status * * * * * * * * * * * * * *"

注意

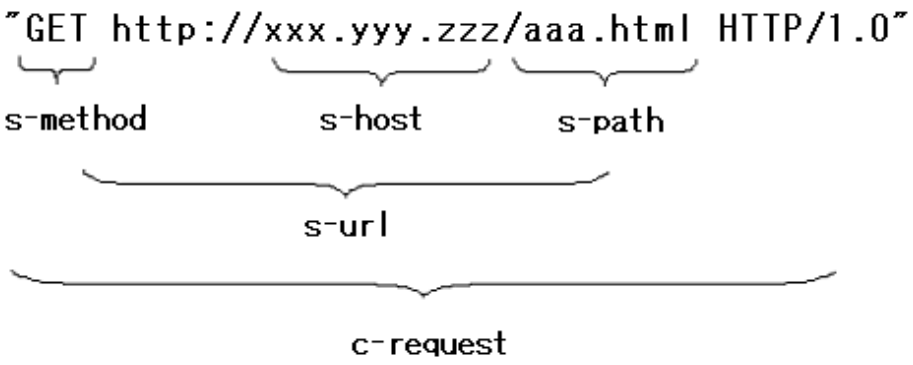
- シンボルで指定する場合は、対応するformatの内容と分析対象ログのレコードを比較し、記録形式が一致しているシンボルを指定してください。日付部分の形式はシステムにより異なる可能性があるので、十分注意してください。
- シンボルMicrosoft-MS50とMicrosoft-MS60は、それぞれMicrosoft Internet Information Services 5.0および6.0のインストール時、デフォルトの場合のみに有効となります。インストール後、ログ形式を変更した場合は、分析対象ログのレコードと記録形式が一致しているシンボルを指定してください。該当するシンボルがない場合は、formatで指定してください。
- シンボルで、ログの記録形式を指定する場合、以下の性能情報は収集されません。

シンボル	収集されない性能情報
Common	リクエスト処理時間
Microsoft-MS50 Microsoft-MS60	リクエスト処理時間 トラフィック量
Common+Ts Common+Tms	-
Netscape-Extend	-
Squid-Native11	-
Microsoft-Native	-
DeleGate-Default	リクエスト処理時間
InfoProxy-Extend	-

2. "format"にトークンを指定する場合

トークン	意味
s-time{time-format}	サーバがリクエストの処理を完了した時刻
c-request	クライアントがサーバへ送信した最初のリクエスト
s-method	クライアントがサーバへリクエストしたメソッド(c-requestの一部)
s-url	クライアントがサーバへリクエストしたURL(c-requestの一部)
s-host	クライアントがサーバへリクエストしたホスト名または、IPアドレス(s-urの一部)
s-path	クライアントがサーバへリクエストしたファイルパス(s-urlの一部)
s-status	サーバがクライアントへ送信したステータスコード
r-status	リモートサーバがサーバへ送信したステータスコード
s-bytes	サーバがクライアントへ転送したバイト数
s-elapse{elapse-format}	サーバがリクエストの処理に要した時間
*	上記以外の可変要素
¥	エスケープ文字(" ¥ を指定する場合は ¥" ¥¥ のようにエスケープ文字を付けます)

c-request、s-method、s-url、s-host、s-pathの関係を以下に記述します。



- time-format には、分析対象ログに記録された時刻のログ形式をトークンと区切り文字で指定します。トークンは、以下のとおりです。

トークン	意味
yyyy	西暦年(2005～2038)
yy	西暦年(00～99)
mm	月(01 ～ 12)
mon	月(Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec)
month	月(January、February、March、April、May、June、July、August、September、October、November、December)
dd	日(01～31)
HH	時(00～23)
MM	分(00～59)
SS	秒(00～59)
seconds	通算秒

- elapse-format には、経過時間の単位を示すトークンを記述します。トークンは、以下のどちらかです。

トークン	意味
s	単位は、秒
ms	単位は、ミリ秒

注意

- formatで、トークンの文字列に一致しないものは、全て区切り文字として扱います。トークンのスペルミスは、区切り文字として扱われますので、注意してください。
- 分析対象ログのレコードが、Formatで指定された記録形式に一致しない場合、レコードの情報は「分析不可レコード」として集計されます。また、記録形式に一致しないレコードが、ログファイルの分析開始位置から一定数だけ連続して存在した場合、処理を終了します。分析対象ログファイルのレコードとFormatの記録形式が正しく対応していることを確認してください。
- formatで、ログの記録形式を指定する場合は、以下に示す必須トークンが指定されていることを確認してください。必須トークンが指定されていない場合は、分析ができなくなりますので、十分注意してください。

必須トークン
s-time
s-status

- formatで、ログの記録形式を指定する場合は、操作画面の分析で必要となるトークンが指定されていることを確認してください。

分析(操作画面)	必要トークン
URL別の各種分析(詳細・レポート)	s-url(または、c-request、s-path)

- **TimeZone=timezone**

分析対象ログファイルに記録されている時刻データのタイムゾーンを定義します。timezoneには、UTC(協定世界時)からの時差を指定します。形式は、以下のとおりです。

形式	説明
[+|-]HHMM	+:進んでいることを表す。 -:遅れていることを表す。 HH:時(00～13) MM:分(00～59)

デフォルトは、以下のとおりです。デフォルトの場合、行自体を省略できます。

TimeZone=+0000

または

TimeZone=0000

注意

分析対象ログファイルで利用されている地域時刻は、各サーバのマニュアルで確認してください。

・ **Inclusion=inclusive-record**

分析対象となるURLを定義します。

詳細またはレポートにおける分析で、特定のURLに絞った監視・分析を行いたい場合に指定します。inclusive-recordには、分析対象とするURL(パラメタを除く)について、Webコンテンツのサーバ名部分を除いたパス名を二重引用符(")で括って指定します。使用可能文字数は、最大1023です。以下は使用できません。

```
^ | [ ] { } < > ( ) & $ # " ' * , ? = : ¥
```

定義可能なInclusion文数は最大20です。

なお、URL末尾がスラッシュ(/)の場合、指定されたURL配下の全コンテンツ(サブディレクトリを含む)をひとつのURLとして集計、監視します。ただし、以下の場合は、ファイル名として扱われます。配下のコンテンツは集計、監視の対象となりません。

```
Inclusion="/"
```

- Inclusion文で定義していない全てのURLは、URL名[CONTENTS]で分析が行われます。
- デフォルトの場合、全てのURLは、URL名[CONTENTS]で分析が行われます。デフォルトの場合、行自体を省略できます。

■定義例

Inclusion文の定義例は以下のとおりです。

```
Inclusion="/SSQC/eg.htm"
Inclusion="/cgi-bin/query.cgi"
Inclusion="/tool/program"
Inclusion="/segment01/"
```

注意

以下のURLは全てURL名"/SSQC/eg.htm"として監視されます。

- http://www.fujitsu.com/SSQC/eg.htm
- https://www.fujitsu.com/SSQC/eg.htm
- http://www.fujitsu.co.jp/SSQC/eg.htm

■定義例

定義例は、以下のとおりです。

【Windows版】

```
[RequestLog]
Service=www1
Path="C:¥WINNT¥system32¥LogFiles¥W3SVC1¥ex*.log"
Format="s-time{yyyy-mm-dd HH:MM:SS} * s-method s-url s-status s-bytes"
```

【UNIX版】

```
[RequestLog]
Service=www2
Type=web
Path=/usr/local/apache/logs/access_log
Format=Common
TimeZone=+0900
Inclusion="/cgi-bin/query.cgi"
```

8.1.2 定義内容の確認

トランザクションログ監視エンジンには、トランザクションログ定義ファイルに設定された内容の定義形式を確認するためのオプションが用意されています。確認方法は、以下のとおりです。

■手順

-cオプションを指定して、トランザクションログ監視エンジンを実行します。

【Windows版】

```
<インストールディレクトリ>¥bin¥tlawatch -c
```

【UNIX版】

```
/opt/FJSVssqc/bin/tlawatch -c
```

定義形式に問題がある場合、標準エラー出力にメッセージが出力されます。定義内容に問題が発見されない場合、メッセージは出力されません。

8.2 セットアップ

本ファイルの編集内容を有効にするには、収集ポリシーの作成と適用を実施する必要があります。

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

8.3 表示

Webトランザクション量の情報は、以下の方法で表示することができます。

コンソールのサマリ表示

サマリツリー内のWebTrnMonitorで表示します。

コンソールの詳細表示

詳細ツリー内のWebTrnフォルダーで表示します。

レポート

- 総点検分析・レポート
- カテゴリ別診断分析・レポート

8.4 トランザクションログ定義サンプルファイル

Webトランザクション量を管理する場合に、トランザクションログ定義ファイルのサンプルを使用することで、以下のWebサーバを監視することができます。

No.	監視対象Webサーバ	ログ形式	対象OS
1	Internet Information Services 5.0	Microsoft Log Format形式 ※IIS 5.0のインストール後、 デフォルトのログファイル形式	Windows
2	Internet Information Services 6.0	Microsoft Log Format形式 ※IIS 6.0のインストール後、 デフォルトのログファイル形式	Windows
3	Internet Information Services 7.0	Microsoft Log Format形式 ※IIS 7.0のインストール後、 デフォルトのログファイル形式	Windows
4	Apache HTTP Server	Commonログ形式	Windows Solaris Linux
5	Apache HTTP Server	Combinedログ形式	Windows Solaris Linux
6	Interstage HTTP Server	Commonログ形式	Windows Solaris Linux

■格納ディレクトリ

サンプルファイルの格納ディレクトリは以下のとおりです。

【Windows版】

<インストールディレクトリ>¥sample

【UNIX版】

/opt/FJSVssqc/sample

ポイント

- Webトランザクション量を管理するサーバ上でサンプルを使用する場合は、既に存在するトランザクションログ定義ファイル(tlawatch.iniのバックアップを取ってから、サンプルを上書きしてください。
- 「8.4.1 サンプルファイル」の該当するサンプルファイルの内容をご覧の上、変更する設定値がある場合は、変更してください。

8.4.1 サンプルファイル

サンプルファイルに格納されているトランザクションログ定義ファイルは以下のとおりです。

※Webサーバの環境によって、値を変更する必要があるパラメタがあります。[環境によって変更する値]欄に記載があるパラメタは、Webサーバの環境に合わせて変更してください。

- 8.4.2 トランザクションログ定義ファイル(Internet Information Services 5.0)
- 8.4.3 トランザクションログ定義ファイル(Internet Information Services 6.0)
- 8.4.4 トランザクションログ定義ファイル(Internet Information Services 7.0)
- 8.4.5 トランザクションログ定義ファイル(Apache HTTP Server [Commonログ形式])
- 8.4.6 トランザクションログ定義ファイル(Apache HTTP Server [Combinedログ形式])
- 8.4.7 トランザクションログ定義ファイル(Interstage HTTP Server [Commonログ形式])

8.4.2 トランザクションログ定義ファイル(Internet Information Services 5.0)

■使用用途

WebサーバがInternet Information Services 5.0のインストール後のデフォルトの場合(ログファイル形式を変更していない場合)にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_iis5

■サンプルファイルの設定値

【Windows版】

```
# Microsoft Internet Information Server 5.0 (Microsoft Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥WINNT¥system32¥LogFiles¥W3SVC1¥ex*.log"
Format=Microsoft-MS50
TimeZone=0000
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 "C:¥WINNT ¥system32¥LogFiles ¥W3SVC1¥ex*.log"	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析ログファイル内の記録形式	Format	Microsoft-MS50	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	0000	

8.4.3 トランザクションログ定義ファイル(Internet Information Services 6.0)

■使用用途

WebサーバがInternet Information Services 6.0のインストール後のデフォルトの場合(ログファイル形式を変更していない場合)にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_iis6

■サンプルファイルの設定値

【Windows版】

```
# Microsoft Internet Information Server 6.0 (Microsoft Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥WINDOWS¥system32¥LogFiles¥W3SVC1¥ex*.log"
Format=Microsoft-MS60
TimeZone=0000
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 "C:¥WINDOWS ¥system32¥LogFiles ¥W3SVC1¥ex*.log"	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。
分析ログファイル内の記録形式	Format	Microsoft-MS60	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	0000	

8.4.4 トランザクションログ定義ファイル(Internet Information Services 7.0)

■使用用途

WebサーバがInternet Information Services 7.0のインストール後のデフォルトの場合(ログファイル形式を変更していない場合)にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_iis7

■サンプルファイルの設定値

【Windows版】

```
# Microsoft Internet Information Server 7.0 (Microsoft Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥inetpub¥logs¥LogFiles¥W3SVC1¥u_ex*.log"
Format="s-time{yyyy-mm-dd HH:MM:SS} * s-method s-path * * * * * s-status * * s-elapse{ms}"
TimeZone=0000
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 C:¥inetpub¥logs¥LogFiles ¥W3SVC1¥u_ex*.log	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。
分析ログファイル内の記録形式	Format	s-time{yyyy-mm-dd HH:MM:SS} * s-method s-path * * * * * s-status * * s-elapse{ms}	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	0000	

8.4.5 トランザクションログ定義ファイル(Apache HTTP Server [Common ログ形式])

■使用用途

WebサーバがApache HTTP Serverのログファイル形式がCommon形式の場合にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_apache_common

■サンプルファイルの設定値

【Windows版】

```
# Apache HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥Program Files¥Apache Software Foundation¥Apache2.2¥logs¥access.log"
Format=Common
TimeZone=+0900
```

【UNIX版】

```
# Apache HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="/var/log/httpd/access_log"
Format=Common
TimeZone=+0900
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 "C:¥Program Files¥Apache Software Foundation¥Apache2.2¥logs¥access.log" 【UNIX版】 "/var/log/httpd/access_log"	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。
分析ログファイル内の記録形式	Format	Common	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	+0900	

8.4.6 トランザクションログ定義ファイル(Apache HTTP Server [Combined ログ形式])

■使用用途

WebサーバがApache HTTP Serverのログファイル形式がCombined形式の場合にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_apache_combined

■サンプルファイルの設定値

【Windows版】

```
# Apache HTTP Server (Combined Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥Program Files¥Apache Software Foundation¥Apache2.2¥logs¥access.log"
Format="* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes ¥"*¥" ¥"*¥""
TimeZone=+0900
```

【UNIX版】

```
# Apache HTTP Server (Combined Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="/var/log/httpd/access_log"
Format="* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes ¥"*¥" ¥"*¥""
TimeZone=+0900
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 "C:¥Program Files¥Apache Software Foundation¥Apache2.2¥logs¥access.log" 【UNIX版】 "/var/log/httpd/access_log"	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析ログファイル内の記録形式	Format	"* * * [s-time{dd/mon/yyyy:HH:MM:SS} *] ¥"c-request¥" s-status s-bytes ¥"*¥" ¥"*¥""	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	+0900	

8.4.7 トランザクションログ定義ファイル(Interstage HTTP Server [Common ログ形式])

■使用用途

WebサーバがInterstage HTTP Serverのログファイル形式がCommon形式の場合にWebトランザクション量を管理するために使用します。

■格納ディレクトリ

<インストールディレクトリ>¥sample¥tlawatch.ini.<OS名>_apache_common

■サンプルファイルの設定値

【Windows版】

```
# Interstage HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="C:¥Interstage¥F3FMihs¥logs¥accesslog"
Format=Common
TimeZone=+0900
```

【UNIX版】

```
# Interstage HTTP Server (Common Log Format) sample
[RequestLog]
Service=www1
Type=web
Path="/var/opt/FJSVihs/logs/accesslog"
Format=Common
TimeZone=+0900
```

■サンプルファイルの設定値の内容

定義項目	パラメタ	サンプルの値	環境によって変更する値
分析対象ログの識別名	Service	www1	
分析対象サーバの種別	Type	web	
分析ログファイルのパス	Path	【Windows版】 "C:¥Interstage¥F3FMihs¥logs¥accesslog" 【UNIX版】 "/var/opt/FJSVihs/logs/accesslog"	分析対象のログファイルのパスが左記のパスと異なる場合は、変更してください。
分析ログファイル内の記録形式	Format	Common	
分析対象ログファイルに記録されている時刻データのタイムゾーン	TimeZone	+0900	

第9章 ユーザデータ管理

業務データやシステム稼働データなどユーザーの固有データを管理する方法について説明します。

ある一定の条件を満たす形式のデータであれば、本製品のPDBに格納することができます。PDBに格納されたデータは、本製品のサマリ、詳細、レポートの各表示機能から参照することができます。

ここで、一定の条件を満たすデータ形式とは、以下のデータです。

- レコード中の各フィールドを、カンマをデリミタとして列挙した形式(CSV形式)であること
- 1レコード毎に改行されていること
- 各レコードが同一形式であること
- レコード中にそのレコードを識別する識別子(リソースID)があること

■実行環境

Manager/Proxy Manager/Agentで実行可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

以下、下記の順でユーザデータの管理方法を説明します。

9.1 ユーザデータ定義

ユーザデータを管理するには、まず、ユーザデータ定義ファイルが必要です。

■定義場所

ユーザデータ定義ファイルは、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。ファイルのパスは、以下のとおりです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥udataconf.ini
```

【UNIX版】

```
/etc/opt/FJSVssqc/udataconf.ini
```

9.1.1 定義形式

ユーザデータ定義ファイルは、以下の形式で記述します。

■形式

```
[MIDDLEWARE_CONF]
XML=ON | OFF
[SELECT_RECORDID]
UDATA_1=ON | OFF
UDATA_2=ON | OFF
UDATA_3=ON | OFF
UDATA_4=ON | OFF
UDATA_5=ON | OFF
・・・・・・・・
UDATA_20=ON | OFF
```

ポイント

- '|' は、「または」の意味で、どちらかが指定できることを意味します。
- 空行は、コメントとして扱われます。
- '#'で始まる行は、コメントとして扱われます。

■説明

[MIDDLEWARE_CONF]

ユーザデータを管理するか否かを定義します。

XML=ON | OFF

選択肢の意味は以下のとおりです。

選択肢	意味
ON	ユーザデータを管理します。
OFF	ユーザデータを管理しません。

初期値は、OFFになっています。

[SELECT_RECORDID]

ユーザデータを管理するために使用する、PDB上のレコードIDを選択します。レコードIDは、UDATA_1からUTATA_20まで(各、SUM_UDATA_1からSUM_UDATA_20を含む)の20種類が用意されており、この中から使用するレコードIDを選択します。

UDATA_1=ON | OFF
UDATA_2=ON | OFF
UDATA_3=ON | OFF
UDATA_4=ON | OFF
UDATA_5=ON | OFF

・・・・・・

UDATA_20=ON | OFF

選択肢の意味は以下のとおりです。

選択肢	意味
ON	レコードIDを選択します。 なお、選択すると、対応するSUM_UDATA_1～20も選択されます。
OFF	レコードIDを選択しません。

初期値は、ONになっています。

使用しないレコードIDはOFFにしてください。

■定義例

【Windows版/UNIX版】

2種類のユーザデータを管理する場合の定義例は、以下のとおりです。

```
[MIDDLEWARE_CONF]
XML=ON
[SELECT_RECORDID]
UDATA_1=ON
UDATA_2=ON
UDATA_3=OFF
UDATA_4=OFF
UDATA_5=OFF
UDATA_6=OFF
UDATA_7=OFF
UDATA_8=OFF
UDATA_9=OFF
UDATA_10=OFF
UDATA_11=OFF
UDATA_12=OFF
UDATA_13=OFF
UDATA_14=OFF
UDATA_15=OFF
UDATA_16=OFF
UDATA_17=OFF
UDATA_18=OFF
UDATA_19=OFF
UDATA_20=OFF
```

9.2 セットアップ

本ファイルの編集内容を有効にするには、収集ポリシーの作成と適用を実施する必要があります。

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

収集ポリシーのセットアップを実施した後に、運用管理クライアントのコンソールへの反映が必要になります。使用手引書(コンソール編)「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

9.3 ユーザデータのPDBへの格納

ユーザデータをPDBに格納します。

sqcPDBcloadの詳細については、リファレンスマニュアル「1.7.2 sqcPDBcload (ユーザデータ入力コマンド) 」を参照してください。

注意

ユーザデータのしきい値監視を行う場合は、sqcPDBcloadコマンドでPDBにユーザデータを取り込んだタイミングで、監視項目の値が定義値を超えていたときに、アラームを通知します。

■記述形式

【Windows版】

```
<インストールディレクトリ>¥bin¥sqcPDBcload.exe -u udata-file -i conv-file
```

【UNIX版】

```
/opt/FJSVssqc/bin/sqcPDBcload.sh -u udata-file -i conv-file
```

■オプション

-u udata-file

PDBに格納するユーザデータファイル(CSVファイル)を指定します。

-i conv-file

データ変換定義ファイル(iniファイル形式)を指定します。データ変換定義ファイルとは、ユーザデータをPDBへ格納するレコード形式に変換する際の変換ルールが記述された以下のようなファイルです。

```
[USERDATA]
consol_flag=2
record_id=1
col_resource_id=2,5
col_start_date_time=6
col_data_num1=10
col_data_num2=9
col_data_text1=4
```

【データ変換定義ファイル(conv-file)】

生成されるレコードの形式については、リファレンスマニュアル「第4章 データフォーマット」を参照してください。

consol_flag

データの種別を指定します。データの種別には、以下があります。それぞれ表示機能と保持期間が異なっています。解説書「3.2.2 Manager」を参照して、どのデータ種別で格納するかを設計してください。

・0 : サマリデータ
・1 : リソースデータ(10分)

・2 : リソースデータ(1時間)
・3 : リソースデータ(24時間)

0 を指定すると、「SUM_UDATA_*n*」レコードが生成されます。
1～3 を指定すると、「UDATA_*n*」レコードが生成されます。

record_id

生成するレコード「SUM_UDATA_1～20」または「UDATA_1～20」の内、1～20 どれを生成するかを指定します。

col_resource_id

リソースIDとするユーザデータファイルのフィールドの番号を指定します。リソースIDとは、そのレコードを一意に識別する識別子です。
例えば、プロセス情報なら、プロセス名がリソースIDになります。
なお、複数のフィールドをつなげてリソースIDにすることもできます。その場合は、col_resource_id=2,5とすることで、フィールド2と5を一つにつなげるという意味になります。

col_start_date_time

収集開始時刻となるフィールドの番号を指定します。
なお、格納するデータの形式は、以下のとおりです。

‘YYYY-MM-DD [hh[:mm[:ss]]]’
(YYYY:西暦、MM:月、DD:日、hh:時間、mm:分、ss:秒)

col_data_num1 ～ 7

フィールド「smud*n*data1～7」または「ud*n*data1～7」(Record ID が UDATA_1、2、3、6、7、8、11、12、13、16、17、18 の場合は ud*n*data5 まで)に格納する、ユーザデータファイルのデータ(数値)のフィールド番号を指定します。

col_data_text1 ～ 7

フィールド「smud*n*txt1」または「ud*n*txt1～7」(Record ID が UDATA_1、2、3、6、7、8、11、12、13、16、17、18 の場合は ud*n*txt5 まで)に格納する、ユーザデータファイルのデータ(テキスト)のフィールド番号を指定します。

【データ変換定義ファイル指定と生成されるレコードの例】

データ変換定義ファイル指定	生成されるレコード		補足
	Record ID	Field Name	
consol_flag=0 record_id=1 col_data_num3=9	SUM_UDATA_1	smud1data3	consol_flagに0を指定することで、SUM_UDATA_*n* のレコードが生成される。 record_idに**1**を指定することで、SUM_UDATA_**1**のレコードが生成される。 col_data_num**3**に**9**を指定することで、sumud1data**3**のフィールドには、CSVファイルの**9**番目のフィールドが格納される。
consol_flag=1 record_id=1 col_data_num3=9	UDATA_1	ud1data3	consol_flagに1～3を指定することで、UDATA_*n* のレコードが生成される。 record_idに**1**を指定することで、UDATA_**1**のレコードが生成される。 col_data_num**3**に**9**を指定することで、ud1data**3**のフィールドには、CSVファイルの**9**番目のフィールドが格納される。
consol_flag=3 record_id=2	UDATA_2	ud2data3	consol_flagに1～3を指定することで、UDATA_*n* のレコードが生成される。 record_idに**2**を指定することで、UDATA_**2**のレコードが生成される。

データ変換定義ファイル指定	生成されるレコード		補足
	Record ID	Field Name	
col_data_num3=9			col_data_num**3**に**9**を指定することで、ud2data**3**のフィールドには、CSVファイルの**9**番目のフィールドが格納される。

■使用例

【Windows版】

```
C:¥>cd C:¥Program Files¥SystemwalkerSQC¥bin
C:¥Program Files¥SystemwalkerSQC¥bin>sqcPDBcload -u C:¥temp¥udata.csv -i C:¥temp¥conv.ini
sqcPDBcload succeeded
```

【UNIX版】

```
# cd /opt/FJSVssqc/bin/
# ./sqcPDBcload.sh -u /tmp/udata.csv -i /tmp/conv.ini
sqcPDBcload succeeded.
```

この時、udata.csvの内容は以下のとおり。

```
2004-09-09 10:00:00,kaminaka,2,octets,data,767872,28856,22400
```

また、conv.iniの内容は以下のとおり。

```
[USERDATA]
consol_flag=2
record_id=1
col_resource_id=2,3
col_start_date_time=1
col_data_num1=6
col_data_num2=7
col_data_text1=4
```

9.4 表示

ユーザデータは、以下の方法で表示することができます。

- コンソールのサマリ表示

  サマリツリー内のUserDataMonitorで表示します。

- コンソールの詳細表示

  詳細ツリー内のAgentツリー配下のUserDataフォルダーで表示します。

・ レポート

詳細分析・レポートで表示します。

ポイント

サマリ表示は、sqcPDBcloadコマンドのオプションで指定するデータ変換定義ファイルで"consol_flag=0"を設定した時のみ表示されます。

第10章　ポリシー配付

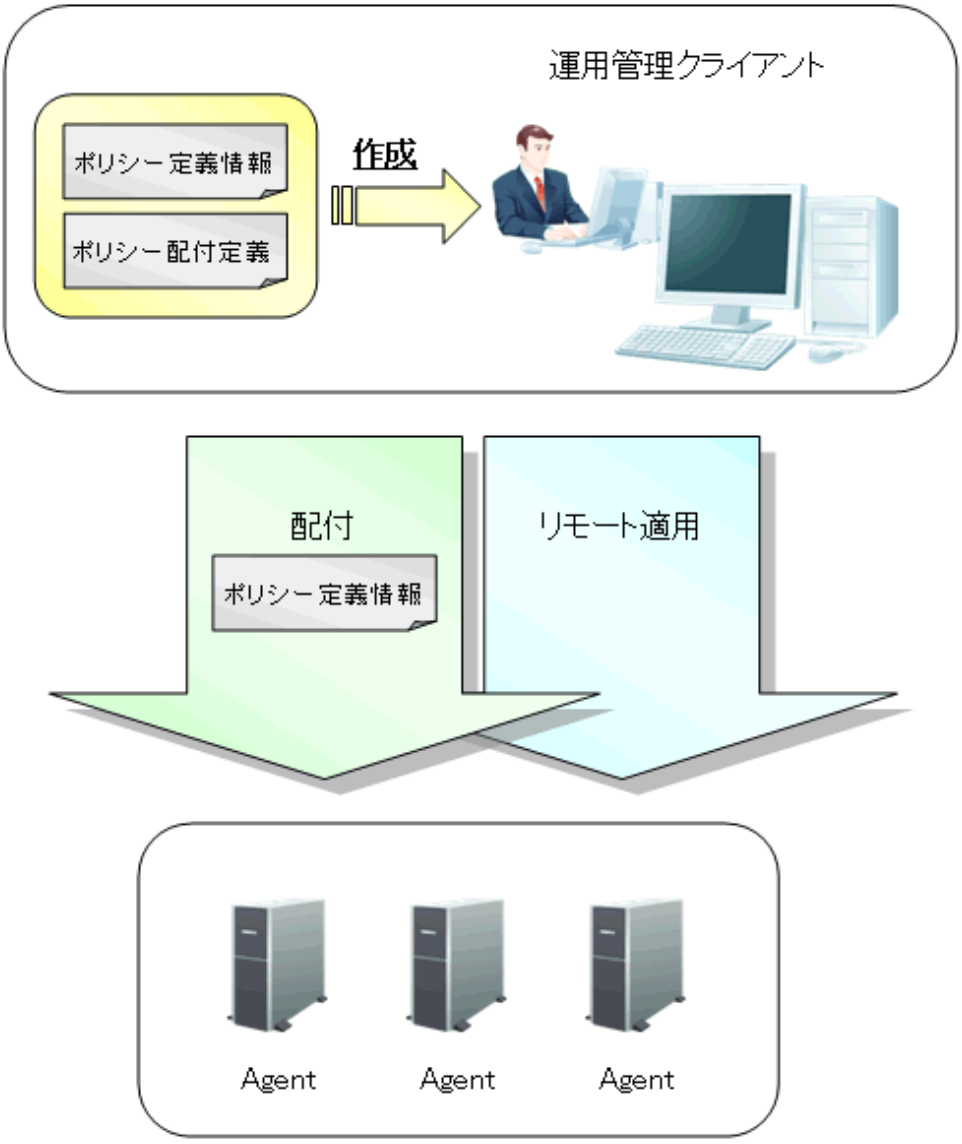
この章では、ポリシー配付機能の概要や運用方法について説明します。

10.1 ポリシー配付機能の概要

この節では、ポリシー配付機能の概要を説明します。

10.1.1 ポリシー配付機能

ポリシー配付とは、性能情報の収集および、しきい値監視に関する定義情報を、運用管理クライアントから各サーバへ配付する機能です。



※ポリシー定義情報とは、収集ポリシーおよび、しきい値監視定義を指します。

※Managerに配付する場合は、ManagerのAgent機能に対して配付します。

■特徴

ポリシー配付機能は以下のような特徴があります。

- 管理対象となるサーバへのログイン、定義設定が不要。
- 管理対象となるサーバ台数分行なっていた定義設定を、一括で行なうことができる。

注意

運用管理クライアントの通信環境のセットアップにおいて、基本認証を設定した場合、ポリシー配付機能は使用できません。

■手順

ポリシー配付機能を使用するには、運用管理クライアント上で以下の作業を行います。

1. 定義情報ファイルの作成

   性能情報の収集（サーバ内リソース情報/レスポンス・稼働情報）や、しきい値監視を行なうサーバに配付する定義情報ファイルを作成します。

2. 配付先サーバの定義

   配付先サーバ情報を、ポリシー配付定義ファイルに定義します。

3. 「1.」の定義情報を、「2.」で定義したサーバへ配付

   ポリシー定義情報を、配付先サーバへ配付する配付コマンドを実行します。

4. 配付先サーバに対し収集ポリシーの作成と適用

   配付先サーバに対して、ポリシーの作成と適用を行なうため、操作コマンドを実行し、リモートで収集ポリシーの作成と適用を行います。

ポイント

ポリシー配付機能は、同一の定義を複数のサーバに配付する場合に効果的です。管理対象となるサーバ台数や状況に応じて使用してください。、

なお、ポリシー配付機能を使用する際には、Systemwalker Service Quality Coordinatorのバージョンなど、条件を満たしている必要があります。

次項で、ポリシー配付機能の動作条件について説明します。

10.1.2 ポリシー配付機能の使用条件

10.1.2.1 ポリシー配付可能なバージョン

ポリシー配付機能を使用できる、Systemwalker Service Quality Coordinatorのバージョンは以下のとおりです。

運用管理クライアントV/L および Manager V/L	配布先サーバV/L		
	V11.0L10～V13.2.0	V13.3.0	V13.4.0
V11.0L10～V13.2.0	－	－	－
V13.3.0	×	○(注)	×
V13.4.0	×	○(注)	○(注)

注：クラスタで構成されたManagerおよびEnterprise Managerへのポリシー配付は除く

－：ポリシー配付機能無し
○：配付可能
×：配付不可

10.1.2.2 ポリシー配付機能の動作条件

ポリシー配付機能を使用する際には、以下の条件を満たしている必要があります。

1. 運用管理クライアントの接続先(Manager)サーバのDCMサービス/デーモン、thttpdサービス/デーモンが起動していること。

2. 配付先サーバ(Agent機能を保持しているサーバ）の接続先サーバが、「1.」のManagerであること。

3. 配付先サーバにおいて、DCMサービス/デーモン、thttpdサービス/デーモンが起動していること。

DCMサービス/デーモン、thttpdサービス/デーモンの起動方法は、「A.4 常駐プロセス、起動と停止」を参照してください。
プロセスについては、リファレンスマニュアル「第2章 常駐プロセス、起動と停止」を参照してください。

10.1.3 定義フォルダのディレクトリ構成

ポリシー配付機能は、運用管理クライアント上で定義します。

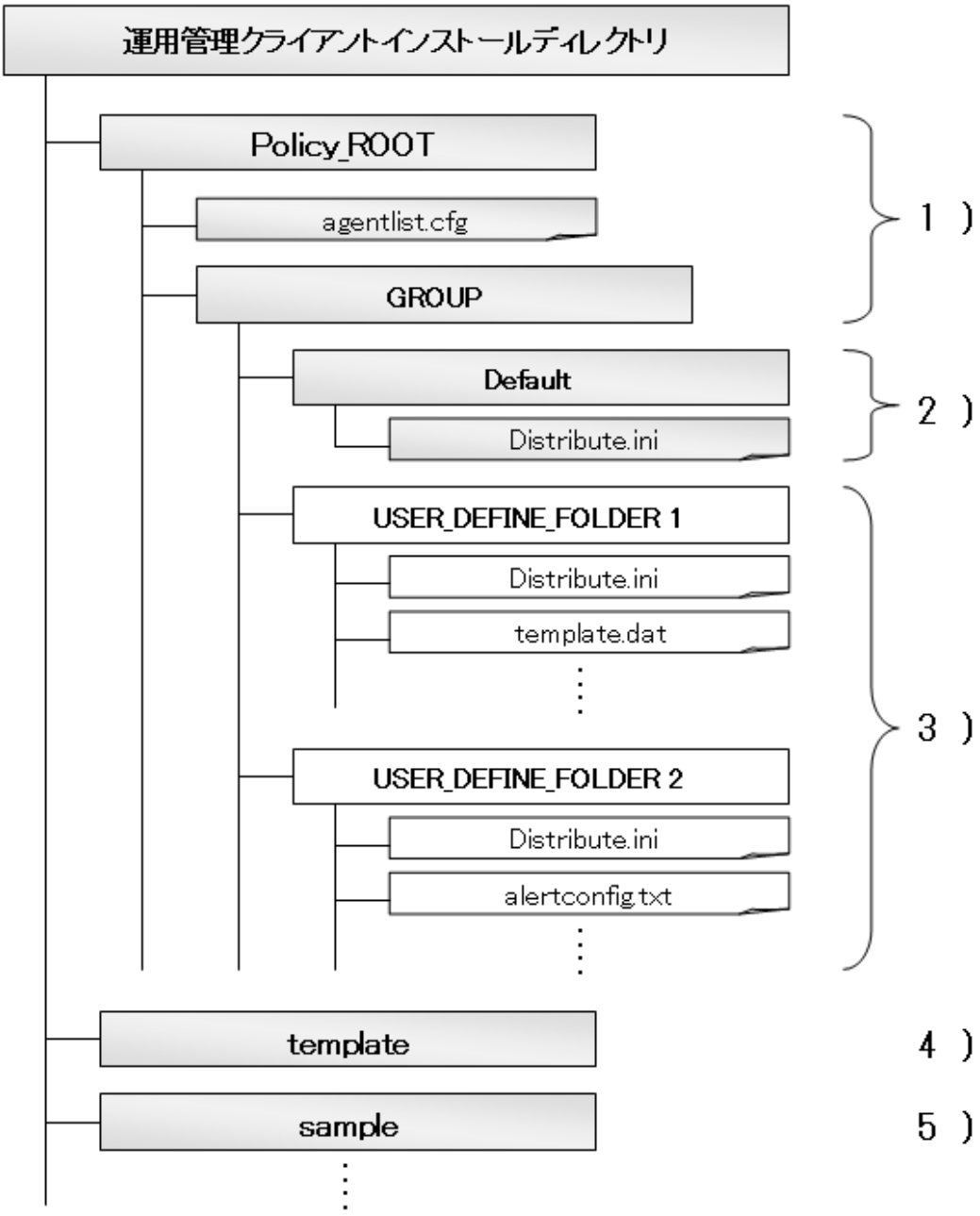
ここでは以下の定義を格納する、ポリシー管理フォルダのディレクトリ構成について説明します。

- 性能情報の収集（サーバ内リソース情報/レスポンス・稼働情報）やしきい値監視を行なうための、ポリシー定義情報ファイルの作成
- ポリシー定義情報ファイルの配付サーバを定義するポリシー配付定義ファイル(Distribute.ini)を作成します。

■格納先

ポリシー管理フォルダは、運用管理クライアントに格納されています。

<運用管理クライアントインストールディレクトリ>¥Policy_ROOT



1. **ポリシー管理フォルダ(Policy_ROOT、GROUP)**

   ポリシー配付グループフォルダの格納先です。

   ポリシー管理フォルダ(Policy_ROOT)には、ポリシー配付先サーバの接続情報を指定する接続先定義ファイル(agentlist.cfg)が格納されています。

2. **ポリシー配付グループフォルダ(Default)**

   Defaultフォルダは、各ポリシーグループのベースとなるフォルダで、インストール時から用意されています。

   Defaultフォルダをポリシー配付グループとして利用したり、コピーして複数のポリシー配付グループを作成します。ポリシー配付グループのフォルダ(Default)には、配付先を指定するポリシー配付定義ファイル(Distribute.ini)が格納されています。

3. **ポリシー配付グループフォルダ**

   インストール後は、Defaultフォルダしか存在しません。

   ポリシー配付グループを追加する場合は、GROUPフォルダの配下にDefaultフォルダをコピー、リネイムしてポリシー配付グループを作成します。作成するフォルダ名は、ポリシー配付時にポリシー配付グループを指定する際に使用します。

   また、ポリシー配付グループフォルダにはサーバに配付する、ポリシー定義情報ファイルも格納します。

4. **テンプレートフォルダ(template)**

   配付するポリシー定義情報ファイルのテンプレートが、各バージョンレベル、各OSごとにパッケージ単位で格納されています。配付先のバージョンレベル、OSに合わせて、ポリシー配付グループにコピーして使用します。

5. **サンプルフォルダ(sample)**

   しきい値監視および、Webトランザクション量管理に使用する定義ファイル例が格納されています。これらのファイルは、予め設定された定義ファイルでフォルダにコピーすることで使用できます。定義例は、Agentに格納されている定義例と同じものです。

   定義内容については、「7.2 しきい値監視定義サンプルファイル/8.4 トランザクションログ定義サンプルファイル」を参照してください。

注意

ポリシー配付機能を使用して、しきい値監視および、Webトランザクション量管理をする場合は、サンプルフォルダ(sample)に格納されている定義ファイル例を使用してください。

ポイント

配付される定義情報は暗号化されません。このため、パスワードの定義が必要となる、Oracle Database Server、SAP NetWeaverとの連携機能を使用する場合はポリシー配付を行なわないでください。

定義情報ファイルの詳細は、「10.2.2 ポリシー定義情報ファイルの作成」を参照してください。

10.2 ポリシー配付手順

ポリシー配付機能の実施手順を説明します。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

■実行環境

本機能は、運用管理クライアントで実施可能です。

- 10.2.1 ポリシー配付グループの作成
- 10.2.2 ポリシー定義情報ファイルの作成
- 10.2.3 ポリシー配付定義ファイルの作成
- 10.2.4 接続先定義ファイルの作成

- 10.2.5 ポリシー配付
- 10.2.6 リモートでのポリシー作成と適用

10.2.1 ポリシー配付グループの作成

■手順

ポリシー配付グループを作成するために、運用管理クライアントのインストールディレクトリにWindowsのエクスプローラ等でフォルダを作成します。

作成するフォルダ名は、ポリシー配付時にポリシー配付グループを指定する際に使用します。

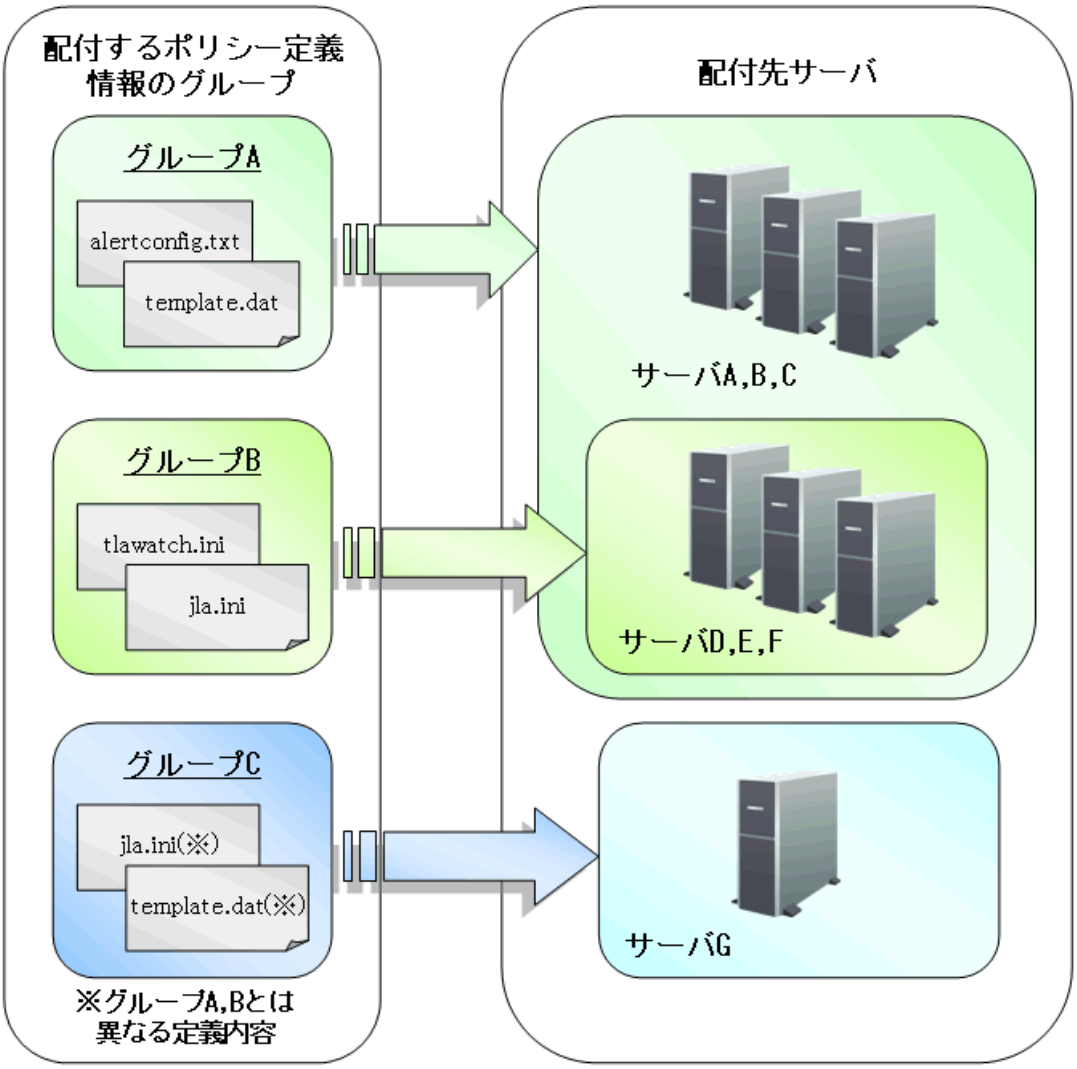
任意の名称でフォルダ名を作成し、配付するポリシー定義情報ファイルを格納します。

■格納先

<運用管理クライアントインストールディレクトリ>¥Policy_ROOT¥GROUP

以下の例を参考に、必要なポリシー配付グループを作成してください。

■例



図のグループA、グループB、グループCが、ポリシー配付グループにあたります。

グループA

グループAは、サーバGを除く全てのサーバに配付するための、ポリシー定義情報ファイルのグループです。

グループB

グループBは、サーバD、E、Fに対して配付するための、ポリシー定義情報ファイルのグループです。

グループC

グループCは、サーバGに対してのみ配付するための、ポリシー定義情報ファイルのグループです。

ポリシー配付を行なうグループを複数作成することで、異なるポリシー定義情報を必要なサーバにのみを配付することができます。

図のグループA、グループB、グループCの例で、グループAをPolicyGP01、グループBをPolicyGP02、グループCをPolicyGP03とした場合、以下のフォルダを作成して各フォルダにポリシー定義情報ファイルを格納します。

<インストールディレクトリ>¥Policy_ROOT¥GROUP¥PolicyGP01

<インストールディレクトリ>¥Policy_ROOT¥GROUP¥PolicyGP02

<インストールディレクトリ>¥Policy_ROOT¥GROUP¥PolicyGP03

10.2.2 ポリシー定義情報ファイルの作成

性能情報の収集(サーバ内リソース情報/レスポンス・稼働情報)や、しきい値監視を行なうサーバに配付するための定義情報ファイルの作成を行ないます。

■ポリシー定義情報ファイル

ポリシー配付機能では、収集ポリシーおよび、しきい値監視定義を配付することができます。これらの定義を総称して、ポリシー定義情報と呼びます。

収集ポリシー

- サーバ内リソース情報(サーバ情報/ミドルウェア情報)
  - 管理対象構成情報(リソース構成情報)
  - テンプレート(常時収集する情報)
- レスポンス・稼働情報
  - 管理対象構成情報 (レスポンス・稼働管理対象構成情報)
  - テンプレート(常時収集する情報)

しきい値監視定義

- しきい値監視定義

注意

収集ポリシーについては、複数の定義ファイルから構成されていますが、インストールレス型Agent、仮想資源管理、エコ情報、他社製品との連携(Oracle,SAP等)の設定ファイルの一部については、配付は行わず各サーバ上でローカルに設定する必要があります。これは、認証情報が必要な場合、定義情報を運用管理サーバで設定、保持および、ネットワーク上で送信することは、セキュリティ管理のリスク要因となるためです。

■手順

1. **配付するポリシー定義情報ファイルのコピー**

   ポリシー定義情報ファイルのテンプレートが以下に格納されています。

   ■格納先

   <運用管理クライアントインストールディレクトリ>¥template

   必要なポリシー定義情報のテンプレートをコピーし、「10.2.1 ポリシー配付グループの作成」で作成したポリシー配付グループに格納します。

   配付可能ファイルは以下です。下記以外のファイルは配付できません。

ファイル名	使用用途	マニュアル参照先
ServiceConf.xml	エンドユーザレスポンスの管理用	「第4章 エンドユーザレスポンス管理」
	サービス稼働状況の管理用	「第6章 レスポンス・稼働管理対象構成情報(ServiceConf.xml)」
alertconfig.txt	しきい値監視定義用	「第7章 しきい値監視」
threshold.bat (Windows版)	アラームアクション定義用	「7.3 アラームアクション定義」
threshold.sh (UNIX版)	アラームアクション定義用	「7.3 アラームアクション定義」
tlawatch.ini	Webトランザクション量の管理用	「第8章 Webトランザクション量管理」
cntrcconf.ini	Systemwalker Centric Managerとの連携用	「1.6 Systemwalker Centric Managerとの連携」
jla.ini	Systemwalker Operation Managerとの連携用	「1.7 Systemwalker Operation Managerとの連携」
snmconf.ini	Systemwalker Network Managerとの連携用	「1.8 Systemwalker Network Managerとの連携」
template.dat	Microsoft SQL Server	「1.12 Microsoft SQL Serverとの連携」
	Microsoft .NET Server	「1.13 Microsoft .NETとの連携」

2. **コピーしたポリシー定義情報ファイルの編集**

   各ファイルの定義方法については、上記マニュアル参照先で確認してください。

注意

ポリシー配付機能により配付された定義ファイルは、配付先サーバですでに存在している定義ファイルを上書きします。

10.2.3 ポリシー配付定義ファイルの作成

各ポリシー配付グループに対する、配付先サーバ情報をポリシー配付定義ファイル(Distribute.ini)に定義します。

ポリシー配付定義ファイル(Distribute.ini)は、ポリシー配付グループ用のフォルダごとに作成し、ポリシー配付グループに対する配付先の定義を行います。

予めポリシー配付定義を作成しておくことで、ポリシー配付時に定義した配付先へ自動的には配付されます。

ポリシー配付定義ファイル(Distribute.ini)の作成は必須ではありませんが、初回の導入時に定義ファイルを作成してポリシー配付した場合は、運用中の収集ポリシー変更が発生した際にも、影響を受けるポリシー配付先サーバに一括して再配付することが可能となるため運用負担も軽減します。

■格納場所

ポリシー配付定義ファイル(Distribute.ini)は、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。

【Windows版】

<運用管理クライアントインストールディレクトリ>¥Policy_ROOT¥GROUP¥<ポリシー配付グループ>¥Distribute.ini

■ファイル形式

```
[POLICY_DEF]
DISTHOST =
```

■説明

[POLICY_DEF]

セクションのDISTHOSTキーでポリシー定義情報の配付先サーバを定義します。

DISTHOST

ポリシー配付グループに対する、配付先サーバをホスト名で定義します。配付先サーバはカンマ' , '区切りで複数指定することが可能です。

ポイント

ポリシー定義情報配付コマンドの、パラメタで配付先サーバを直接指定することで、ポリシー配付が可能となりますが、本定義ファイルを作成しておくことで運用中の収集ポリシー変更時の運用負担が軽減できます。

■使用例

あるポリシー配付グループの配付先がHOSTA,HOSTB,HOSTC,HOSTDの場合、HOSTA,HOSTB,HOSTC,HOSTDを定義ファイルに定義しておくことで、収集ポリシー変更時も配付先サーバの再指定が不要となり、指定漏れも無くなります。

[POLICY_DEF]セクションのDISTHOSTキーでポリシー定義情報の配付先サーバを定義します。DISTHOSTにホスト名を定義してください。

複数のホスト名を指定する場合は、カンマ区切りで指定します。

```
#[POLICY_DEF]
#DISTHOST = AAAA,BBBBB,CCCC,DDDDD
[POLICY_DEF]
DISTHOST =
HOSTA,HOSTB,HOSTC,HOSTD,HOSTE,HOSTF,HOSTG,HOSTH,HOSTI,HOSTJ,HOSTL
```

10.2.4 接続先定義ファイルの作成

接続先定義ファイル(agentlist.cfg)は、ポリシー配付先サーバの接続情報を定義するファイルです。

ポリシー配付先サーバにIPアドレスが複数存在した場合など、自動取得した接続情報では運用管理クライアントから接続できないことがあります。このような場合に接続可能な情報をagentlist.cfgに定義してください。agentlist.cfgに定義した接続情報は、自動取得したものより優先的に使用されます。

■格納場所

接続先定義ファイル(agentlist.cfg)は、テキストファイルです。ファイルの作成と編集は、メモ帳などのテキストエディタを使用してください。

【Windows版】

```
<運用管理クライアントインストールディレクトリ>¥Policy_ROOT¥agentlist.cfg
```

■ファイル形式

ホスト名単位で、以下のエントリーを追加してください。

[AgentList]
ホスト名, http://接続先:ポート番号/SQC/

■定義方法

接続先　:運用管理クライアントから接続可能なIPアドレスまたはホスト名を定義してください。

ポート番号:ポリシー配付に使用するポート番号を定義してください。

■定義例

以下にagentlist.cfg の定義例を示します。

[AgentList]
system_name1, http://192.168.111.333:23440/SQC/
system_name2, http://192.168.111.444:23440/SQC/

10.2.5　ポリシー配付

作成したポリシー定義情報ファイルを配付先サーバに配付するには、運用管理クライアント上でsqcSendPolicy (ポリシー定義情報配付コマンド)を実行します。

sqcSendPolicy (ポリシー定義情報配付コマンド)の詳細については、リファレンスマニュアル「1.1.6 sqcSendPolicy (ポリシー定義情報配付コマンド)」を参照してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

■本手順を行う前に

「10.1.2.2 ポリシー配付機能の動作条件」を参照して、ポリシー配付機能の動作条件を満たしているか確認してください。

■記述形式

<インストールディレクトリ>¥bin ¥sqcSendPolicy.exe	-g <ポリシー配付グループ名>,…
	-g <ポリシー配付グループ名> [-s <サーバ名>,…]

■オプション

-g <ポリシー配付グループ名>

ポリシー配付グループ名を指定します。

グループを指定することにより、ポリシー配付グループフォルダで作成したポリシー定義情報ファイルを、ポリシー配付定義ファイル(Distribute.ini)で定義したサーバに配付します。

-s <サーバ名>

配付先となるサーバ名を指定します。

-sオプションが指定されている場合は、-gで指定したポリシー配付グループのポリシー配付定義ファイル(Distribute.ini)は無効になり、格納されているポリシー定義情報ファイル全てが指定したサーバに配付されます。

また、-sオプションを指定している場合は、-gで指定するポリシー配付グループは1つのみになります。

配付対象になるサーバを確認したい場合は、「10.3.1 ポリシー配付可能サーバの確認方法」を参照して、sqcViewPolicyを実行してください。

■使用例1

以下の定義で配付を実施する場合

【ポリシー配付グループ】

USER_DEFINE_FOLDER1

【ポリシー配付定義ファイル(Distribute.ini)で定義した配付先サーバ】

wasabi1,wasabi2

【ポリシー定義情報ファイル】

しきい値監視定義

```
C:¥Program Files¥SystemwalkerSQC-C¥bin¥sqcSendPolicy.exe -g USER_DEFINE_FOLDER1
```

■説明1

-g でUSER_DEFINE_FOLDER1を指定することで、ポリシー配付定義ファイル(Distribute.ini)で定義した配付先サーバ(wasabi1,wasabi2)に、ポリシー定義情報ファイル(しきい値監視定義)が配付されます。

■使用例2

以下の定義で配付を実施する場合

【ポリシー配付グループ】

USER_DEFINE_FOLDER

【ポリシー配付定義ファイル(Distribute.ini)で定義した配付先サーバ】

wasabi1,wasabi2

【ポリシー定義情報ファイル】

しきい値監視定義

```
C:¥Program Files¥SystemwalkerSQC-C¥bin¥sqcSendPolicy -g USER_DEFINE_FOLDER -s
wasabi3,wasabi4
```

■説明2

-s でwasabi3,wasabi4を指定することで、ポリシー配付定義ファイル(Distribute.ini)で定義した配付先サーバ(wasabi1,wasabi2)が無効になり、ポリシー定義情報ファイル(しきい値監視定義)がwasabi3,wasabi4に配付されます。

10.2.6 リモートでのポリシー作成と適用

配付先サーバに対して、運用管理クライアント上からリモートでポリシーの作成と適用を行ないます。ポリシーの作成と適用は、sqcCtrlPolicy(ポリシーリモート操作コマンド)を実行します。

sqcCtrlPolicy(ポリシーリモート操作コマンド) の詳細については、リファレンスマニュアル「1.1.7 sqcCtrlPolicy (ポリシーリモート操作コマンド)」を参照してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

■記述形式

<運用管理クライアントインストールディレクトリ>¥bin¥sqcCtrlPolicy.exe	-e <操作コマンド種別> {-g <ポリシー配付グループ>,・・・ | -s <サーバ名>,・・・}

■オプション

-e <操作コマンド種別>

リモート操作するコマンド種別を指定します。

- AP:収集ポリシー作成コマンド(sqcAPolicy:レスポンス/稼働情報収集ポリシー)
- RP:収集ポリシー作成コマンド(sqcRPolicy:サーバ内リソース情報収集ポリシー)
- SP:収集ポリシー適用コマンド(sqcSetPolicy)

-g <ポリシー配付グループ>

ポリシー配付グループ名を指定します。

-s <サーバ名>

リモート操作先のサーバを指定します。

配付対象になるサーバを確認したい場合は、「10.3.1 ポリシー配付可能サーバの確認方法」を参照して、sqcViewPolicyを実行してください。

ポイント

Systemwalker Service Quality Coordinator V13.3.0以降は、ポリシー適用コマンド実行時にサービス/デーモンの事前停止は不要です。

ただし、サービス/デーモンが動作中で各ミドルウェア等の性能データが収集中であった場合、それらはポリシー適用の実施中は一時的に停止され、終了後に再収集を開始します。

■使用例

以下の定義でポリシーリモート操作を実施する場合

【操作サーバ】

wasabi

【操作コマンド】

収集ポリシー作成(sqcRPolicy)

C:¥Program Files¥SystemwalkerSQC-C¥bin¥sqcCtrlPolicy.exe -e RP -s wasabi

10.3 補足事項

補足事項として、以下の説明をします。

- 10.3.1 ポリシー配付可能サーバの確認方法
- 10.3.2 ポリシー配付先サーバが使用するポート番号の変更

10.3.1 ポリシー配付可能サーバの確認方法

すでに導入が完了している場合は、運用管理クライアント上でsqcViewPolicy (ポリシー定義情報確認コマンド)を実行することにより配付可能なサーバの一覧を表示できます。

sqcViewPolicy (ポリシー定義情報確認コマンド)の詳細については、リファレンスマニュアル「1.1.5 sqcViewPolicy (ポリシー定義情報確認コマンド)」を参照してください。

■本手順を行う前に

「10.1.2.2 ポリシー配付機能の動作条件」を参照して、ポリシー配付機能の動作条件を満たしているか確認してください。

■記述形式

<運用管理クライアントインストールディレクトリ>¥bin¥sqcViewPolicy.exe [-l [as | ab | mg | pm | em]]
<運用管理クライアントインストールディレクトリ>¥bin¥sqcViewPolicy.exe -c

■オプション

-l パラメタ

ポリシー配付の対象となる、パラメタで指定されたインストール種別のホスト名を一覧で表示します。

※パラメタ指定が無い場合は、全てが対象になります。

-c

配付先サーバがポリシー配付可能な状態になっているか確認します。

■パラメタ

パラメタはインストール種別の略称を指定します。

各略称に対応するインストール種別は以下のとおりです。

as：Agent for Server

ab：Agent for Business

mg：Manager

pm：Proxy Manager

em：Enterprise Manager

10.3.2 ポリシー配付先サーバが使用するポート番号の変更

ポリシー配付先サーバが使用するポート番号を変更する場合は、ポリシー配付先サーバで以下の作業を行ないます。

Agent側のHTTP通信環境として、ポリシー配付機能を利用する場合、ポート番号はデフォルトで23440に設定されています。ポート番号を変更したい場合は、以下の定義ファイルを編集してください。(port=23440の箇所を変更)

■手順

1. ポリシー配付先サーバのthttpd.conf を変更します。

   ■格納先

   【Windows版】

<可変ファイル格納ディレクトリ>¥control¥thttpd.conf

   【UNIX版】

/etc/opt/FJSVssqc/thttpd.conf

   ■定義方法

cgipat=/cgi-bin/* chroot dir=C:¥Program Files¥SystemwalkerSQC¥www port=23440　　★ここを変更します。

2. 「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、収集ポリシーの適用を実施してください。
3. 「A.4 常駐プロセス、起動と停止」を参照して、ManagerとAgentのthttpdサービス/デーモンを再起動してください。

第11章　バックアップ/リストア

Systemwalker Service Quality Coordinator では、運用環境の移行時、または運用環境を誤って削除、破壊した場合に備えて、ユーザー登録情報や運用管理情報をバックアップ/リストアする手順を提供しています。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

■本手順を行う前に

バックアップ作業は以下の契機で行うことを推奨します。

- 定義や設定を変更した場合
- 運用データを保存した場合

以下、バックアップ/リストアの手順を説明します。

- 11.1 動作定義
- 11.2 性能データベース(PDB)のバックアップ/リストア

11.1 動作定義

■Enterprise Manager/Manager/Proxy Manager/Agent

動作定義の格納場所を以下に示します。ディレクトリ単位でバックアップを実施してください。リストアする場合も、バックアップしたファイルを同じ場所に配置してください。

【Windows版】

<可変ファイル格納ディレクトリ>¥control

【UNIX版】

/etc/opt/FJSVssqc

ポイント

Managerの二重化運用を行っている場合は、各Manager上でバックアップを実施してください。(Managerの二重化運用はEnterprise Editionで提供される機能です。)また、クラスタシステム運用を行っている場合は、現用系(管理業務を運用するノード)でバックアップを実施してください。(クラスタシステム運用はEnterprise Editionで提供される機能です。)

■運用管理クライアント

動作定義の格納場所を以下に示します。ディレクトリ単位でバックアップを実施してください。リストアする場合も、バックアップしたファイルを同じ場所に配置してください。

【Windows版】

<インストールディレクトリ>¥www¥

11.2 性能データベース(PDB)のバックアップ/リストア

Enterprise Manager/Manager上には、性能データベース(PDB)ファイルがあります。バックアップ/リストアの方法としては、以下に示す2つの方法がありますので、必要に合わせて組み合わせて運用してください。

- PDBファイル
- アーカイブファイル

注意

Managerの二重化運用を行っている場合は、各Manager上でバックアップを実施してください。また、クラスタシステム運用を行っている場合は、現用系(管理業務を運用するノード)でバックアップを実施してください。(クラスタシステム運用はEnterprise Editionで提供される機能です。)

以下、性能データベース(PDB)のバックアップ/リストアについて説明します。

- 11.2.1 PDBファイル
- 11.2.2 アーカイブファイル

11.2.1 PDBファイル

性能データベースファイルそのものをバックアップする方法です。リストアする場合も、バックアップしたファイルを同じ場所に配置して下さい。

■本手順を行う前に

バックアップを行う、Enterprise Manager/Managerのサービス/デーモンが起動している場合は、「A.4 常駐プロセス、起動と停止」を参照して、DCMサービス/デーモンを停止してください。また、常駐プロセスが正しく停止しているか確認してください。

PDBファイルは、以下のディレクトリ配下に格納されます。

【Windows版】

<可変ファイル格納ディレクトリ>¥data¥

【UNIX版】

/var/opt/FJSVssqc/PDB/

上記ディレクトリ配下に、以下のファイルが生成されます。

ファイル名	説明
pdb.dat	管理用のデータが格納される単一ファイルです。
pdb_SUMMARY.dat	サマリデータが格納される単一ファイルです。

ファイル名	説明
pdb_10MIN_yyyymmdd.dat	リソースデータ(10分間隔)が格納されるファイルです。1日ごとに生成され、ファイル名のyyyymmddは、ファイルが作成された日の日付になります。なお、PDBファイルはUTC標準時で切り替わります。
pdb_1HR_yyyymmdd.dat	リソースデータ(1時間間隔)が格納されるファイルです。一週間ごとに生成され、ファイル名のyyyymmddは、ファイルが作成された週の日曜日の日付になります。なお、PDBファイルはUTC標準時で切り替わります。
pdb_1DAY_yyyymmdd.dat	リソースデータ(1日間隔)が格納されるファイルです。一月ごとに生成され、ファイル名のyyyymmddは、ファイルが作成された月の月初めの日付になります。なお、PDBファイルはUTC標準時で切り替わります。

ポイント

- PDBファイルは、上記ディレクトリ内の、全ての *.dat ファイルを一緒に移動させてください。
- 移動させた*.datファイルのファイル名は変更しないでください。

11.2.2 アーカイブファイル

バックアップ用に出力されたアーカイブファイルをバックアップする方法です。このファイルは、毎日バックアップすることを想定したファイルです。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥spool¥BackupPDBinsert
```

【UNIX版】

```
/var/opt/FJSVssqc/BackupPDBinsert
```

上記ディレクトリ配下に、以下のファイルが出力されます。

```
pdbinsert_%SYSTEM%_%N%.txt
```

%SYSTEM% : システム名

%N% : ファイル番号

本アーカイブファイルは、24時間間隔、または、DCMのサービス/デーモンが起動する度に新たに生成されます。ただし、ファイル番号(%N%)が1～3の間で、サイクリックに使用されます。したがって、最大三日間の情報がアーカイブされることになります。

本アーカイブファイルをリストアする場合は、ファイルの拡張子を.txtから.tmpに変換した後、以下のディレクトリに配置してください。

【Windows版】

```
<可変ファイル格納ディレクトリ>¥transfer¥DsaPDBWriter
```

【UNIX版】

```
/var/opt/FJSVssqc/temp/DsaPDBWriter
```

注意

アーカイブファイルのリストア時、1回のトランザクションとしてPDBへ書込みます。その際、PDBがロック状態となり、アーカイブファイル以外の性能情報の書込み、及び読込みができなくなります。このため、アーカイブファイルをリストアするときは、複数のファイルに分割して格納してください。

第12章　エコ情報管理

サーバの消費電力や温度は、アプリケーションなどの稼働状況により変化するため、把握することが困難です。エコ情報管理機能により、監視対象となるITシステムの消費電力や温度を可視化でき、現状把握が可能になります。省エネルギーへの取り組み計画が立てやすくなると同時に、取り組みによる効果を評価することができます。

■実行環境

Manager/Proxy Managerで実行可能です。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

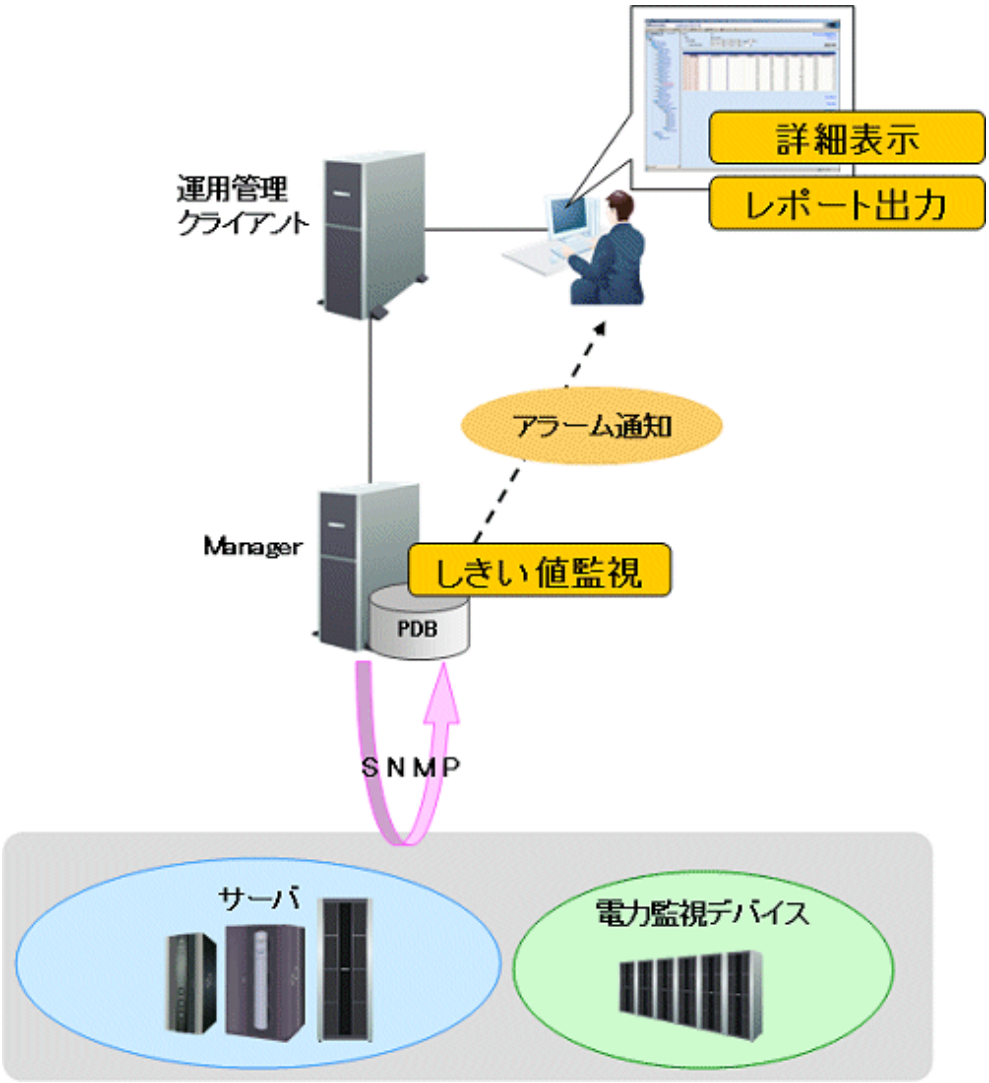
【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

12.1 測定の概要

■機能概要

エコ情報管理機能は、一般的に利用されているSNMPのMIBインターフェースを使って、電力や温度の情報を提供している機種に対して収集/表示します。



※監視対象は、下記の前提条件を満たす必要があります。

■前提条件

監視可能な機器は以下のとおりです。

- 監視対象機器が、管理情報ベース(MIB)ファイルを提供していること(製品やWeb公開で提供していること)
- 監視対象機器が、以下のエコ情報(電力、温度)のMIBのオブジェクトID(OID)のうち、いずれかを提供していること
  - ー 電力情報
    現在の消費電力、電力量
  - ー 温度情報
    現在の温度

注意

監視する前に、必ず、監視対象とする機器が、上記の2つの前提条件を満たしていることを確認してください。

■表示できる情報

エコ情報管理では、監視対象が提供している情報から、以下の情報を表示します。

・ 電力情報
電力、平均電力、最小電力、最大電力、電力量

・ 温度情報
温度、平均温度、最低温度、最高温度

■収集間隔

収集間隔は、10分です。

12.2 導入確認

・ 監視対象機器のSNMPエージェントが起動していること

・ 監視対象機器とネットワーク接続(ポート番号161)できること

注意

監視する前に、必ず、監視対象とする機器のSNMPに関する情報を確認してください。

12.3 定義方法

以下の順で設定します。

1. MIB定義ファイルの格納
2. エコ情報収集定義ファイルの設定
3. SNMPエージェントの構成情報ファイルの設定
4. 収集テンプレートの定義

12.3.1 MIB定義ファイルの格納

1. 監視対象機器が提供している以下の情報が定義されているMIB定義ファイルを準備します。

   ー 電力情報
   現在の消費電力、電力量

   ー 温度情報
   現在の温度

2. MIB定義ファイルの最初の行の「DEFINITIONS」の前のモジュール名をファイル名にし、拡張子をtxtにします。

   例）MIB定義ファイルの最初の行が以下の場合

   <MIB定義ファイルの最初の行>
   OPL-SP-MIB DEFINITIONS ::= BEGIN

   モジュール名が「OPL-SP-MIB」なので、拡張子「txt」を追加して、ファイル名を以下のようにします。

   <ファイル名>
   OPL-SP-MIB.txt

3. 作成したファイルを以下のフォルダに格納します。

   【Windows版】

<可変ファイル格納ディレクトリ>¥control¥mibs

【UNIX版】

/etc/opt/FJSVssqc/mibs

12.3.2 エコ情報収集定義ファイルの設定

エコ情報収集定義ファイル(collectOID.txt)を編集し、監視するエコ情報のオブジェクトID(OID)を機器ごとに定義します。

ファイル格納場所

【Windows版】

<可変ファイル格納ディレクトリ>¥control¥collectOID.txt

【UNIX版】

/etc/opt/FJSVssqc/collectOID.txt

ファイル形式

iniファイル形式

設定項目

項目	説明
[機種名] (必須)	セクション名です。 監視対象の機種名を定義します。
mibfilename (必須)	監視対象の機種のMIBファイル名を定義します。
powerresource	機種よりさらに細かい単位で監視したい場合は、その単位のOIDを定義します。 リソースIDには、以下のように表示されます。 「hostname:<シーケンス番号>:powerresource」 ※hostnameは、監視対象機器の構成情報ファイル(ecoAgentInfo.txt)に定義したIPアドレス(ホスト名)です。
power	電力のOIDを定義します。
poweravg	平均電力です。 電力のOID（powerと同じもの)を定義します。（電力から算出されます）
powermin	最小電力です。 電力のOID（powerと同じもの)を定義します。（電力から算出されます）
powermax	最大電力です。 電力のOID（powerと同じもの)を定義します。（電力から算出されます）
energy	電力量のOIDを定義します。
temperatureresource	機種よりさらに細かい単位で監視したい場合は、その単位のOIDを定義します。 リソースIDには、以下のように表示されます。 「hostname:<シーケンス番号>:temperatureresource」 ※hostnameは、監視対象機器の構成情報ファイル(ecoAgentInfo.txt)に定義したIPアドレス(ホスト名)です。

項目	説明
temperature	温度のOIDを定義します。
temperatureavg	平均温度です。 温度のOID（temperatureと同じもの)を定義します。（温度から算出されます）
temperaturemin	最低温度です。 温度のOID（temperatureと同じもの)を定義します。（温度から算出されます）
temperaturemax	最高温度です。 温度のOID（temperatureと同じもの)を定義します。（温度から算出されます）

すべての項目で指定可能な文字列は、半角英数字だけです。
監視対象の機種が複数ある場合は、セクションを追加してください。

定義例

SPARC Enterprise M3000を監視する場合の定義例

```
[OPL-SP-MIB]
mibfilename=OPL-SP-MIB.txt
power=multiple:scfSystemActualPowerConsumptionValue
poweravg=multiple:scfSystemActualPowerConsumptionValue
powermin=multiple:scfSystemActualPowerConsumptionValue
powermax=multiple:scfSystemActualPowerConsumptionValue
temperature=multiple:scfSystemAmbientTemperatureValue
temperatureavg=multiple:scfSystemAmbientTemperatureValue
temperaturemin=multiple:scfSystemAmbientTemperatureValue
temperaturemax=multiple:scfSystemAmbientTemperatureValue
```

12.3.3 SNMPエージェントの構成情報ファイルの設定

監視対象機器の構成情報ファイル(ecoAgentInfo.txt)を編集し、エコ情報を収集する監視対象機器を定義します。

ファイル格納場所

【Windows版】

```
<可変ファイル格納ディレクトリ>¥control¥ecoAgentInfo.txt
```

【UNIX版】

```
/etc/opt/FJSVssqc/ecoAgentInfo.txt
```

SNMPのバージョンが v2、v2cの場合

形式

```
IPアドレス（ホスト名）,バージョン,Community名,機種名
```

IPアドレス(ホスト名):

SNMPエージェントのIPアドレス、またはホスト名を指定します。

バージョン:

SNMPのバージョンを指定します。指定可能な値は、v2、v2c のどれかです。
SNMPのバージョンがv2cの場合、指定する値により、性能情報の収集方法を変更することができます。

・v2：GETNEXTで性能情報を収集します。
・v2c：GETBULKで性能情報を収集します。

Community名

SNMPエージェントのCommunity名を指定します。

機種名

監視対象機種のエコ情報収集定義ファイル(collectOID.txt)に定義した機種名を指定します。

SNMPのバージョンが v3の場合

形式

IPアドレス(ホスト名),バージョン,ユーザー名,パスワード,認証タイプ,機種名

IPアドレス(ホスト名):

SNMPエージェントのIPアドレス、またはホスト名を指定します。

バージョン:

v3 を指定します。

ユーザー名

認証に使用されるユーザー名を指定します。

パスワード

認証に使用されるユーザー名に対応するパスワードを指定します。
genpwdコマンドを使用して暗号化したパスワードを指定します。
genpwd(パスワード暗号化コマンド)の使用方法は、「A.6 genpwd(パスワード暗号化コマンド)」を参照してください。

認証タイプ

MD5またはSHAを設定します(デフォルト値はMD5です)。

機種名

監視対象機種のエコ情報収集定義ファイル(collectOID.txt)に定義した機種名を指定します。

定義例

```
#SNMPエージェントのパラメータ情報リスト
server1,v2c,public,OPL-SP-MIB
server2,v3,demo ID,demo PW,MD5,OPL-SP-MIB
192.168.1.100,v3,admin,"",SHA,OPL-SP-MIB
```

12.4 セットアップ

「A.1 サーバ内リソース情報収集ポリシーセットアップコマンド」を参照して、sqcRPolicy、およびsqcSetPolicyを実行してください。

各定義ファイルに設定された内容に誤りがある場合、誤った定義がおこなわれている被監視サーバについては管理の対象となりません。
sqcSetPolicyを実行した際、定義の誤りにより管理の対象から外される被監視サーバについては以下のメッセージを出力します。

```
(Warning) : <ECO> ecoAgentInfo.txt:ignored line(hostname[対象ホスト名またはIPアドレス])
```

対象ホスト名またはIPアドレスには「SNMPエージェントの構成情報ファイル」に定義された対象ホスト名またはIPアドレスを出力します。

また、定義ファイルに1つでもエラーがある場合は、以下のメッセージを出力します。

```
(Warning) : <ECO> There is an error in definition.
Please confirm the file (ファイル名).
```

ファイル名には以下を出力します。

【Windows 版】

```
<可変ファイル格納ディレクトリ>¥log¥setpolicy_error.log
```

【UNIX 版】

```
/var/opt/FJSVssqc/setpolicy_error.log
```

メッセージが表示された場合、ファイルの内容を確認し、ファイルに記述されているメッセージをもとに定義ファイルを修正して、再度セットアップを実行してください。ファイルに出力されるメッセージについては、リファレンスマニュアルの「1.1.3 sqcSetPolicy(ポリシー適用コマンド)」を参照してください。

なお、収集ポリシーのセットアップを実施した場合は、コンソールに反映が必要です。使用手引書(コンソール編)の「1.2.2.3 Agents」を参照して、Agent設定画面で構成情報の取得を行ってください。

12.5 表示

エコ情報は、以下の方法で表示できます。

- 詳細

  詳細ツリーのECOノードを選択すると表示できます。

- レポート

  詳細分析・レポート

注意

- 監視対象の機器によって、データの単位が異なる場合があるため、単位は表示されません。
  OIDを設定するときに、データの単位を確認してください。

付録A セットアップコマンド、常駐プロセス一覧

ここでは、各セットアップコマンドと、常駐プロセスの起動と停止方法について説明します。

詳細については、リファレンスマニュアル「1.1 ポリシーコマンド」、「第2章 常駐プロセス、起動と停止」を参照ください。

A.1　サーバ内リソース情報収集ポリシーセットアップコマンド

サーバ内リソース情報収集ポリシーセットアップコマンドについて説明します。

詳細については、リファレンスマニュアル「1.1.1 sqcRPolicy(サーバ内リソース情報収集ポリシー作成コマンド)」を参照してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

【Windows版】

ディスク系の性能情報を収集するには、Windowsのコマンドである diskperfコマンド を実行して、情報収集できる状態にしておく必要があります。使用例は以下のとおりです。

```
diskperf -y
```

diskperfコマンドの詳細については、Windowsのヘルプ等を参照して確認してください。なお、その際、物理ドライブ、論理ドライブ両方が有効になるように設定してください。

ポイント

- diskperfコマンドは、設定後、システムの再起動が必要です。
- diskperfコマンドは、Systemwalker Service Quality Coordinator DCMサービスを起動する(性能情報の収集開始)前に必要な作業です。

■記述形式

1. **サーバ内リソース情報収集ポリシー作成**

   【Windows版】

<インストールディレクトリ>¥bin¥sqcRPolicy.exe

【UNIX版】

/opt/FJSVssqc/bin/sqcRPolicy.sh

2. **ポリシーの適用**

【Windows版】

<インストールディレクトリ>¥bin¥sqcSetPolicy.exe [-h <host name>]

【UNIX版】

/opt/FJSVssqc/bin/sqcSetPolicy.sh [-h <host name>]

ポイント

Systemwalker Service Quality Coordinator V13.3.0以降は、ポリシー適用コマンド実行時にサービス/デーモンの事前停止は不要です。

ただし、サービス/デーモンが動作中で各ミドルウェア等の性能データが収集中であった場合、それらはポリシー適用の実施中は一時的に停止され、終了後に再収集を開始します。

なお、-hオプションを使用する場合は、「A.4 常駐プロセス、起動と停止」を参照して、サービス/デーモンを停止した上で実行してください。

■オプション

-h <host name>

以下のようなクラスタ運用を行っており、管理対象のシステム名を変更したい場合には、本オプションで設定したいシステム名を指定します。

- Managerで、かつManagerのサーバ内リソース情報を収集する場合(現用系と待機系のシステム名をひとつで管理したい場合)
- Agentで、かつノード名引継ぎを実施しているシステムを別々の名前で管理したい場合

ポイント

サーバ内リソース情報収集ポリシー作成コマンド(sqcRPolicy)、または「ポリシーリモート操作コマンド」の、sqcCtrlPolicy.exe -e RPコマンドを実行すると、MiddlewareConf.xmlが生成されます。管理対象を削除したい場合は、リファレンスマニュアル「第3章 リソース構成情報(MiddlewareConf.xml)を参照して、MiddlewareConf.xmlの内容を変更してください。

A.2　レスポンス・稼働情報収集ポリシーセットアップコマンド

レスポンス・稼働情報収集ポリシーセットアップコマンドについて説明します。

詳細については、リファレンスマニュアル「1.1.2sqcAPolicy(レスポンス・稼働情報収集ポリシー作成コマンド)」を参照してください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

1. **レスポンス・稼働情報収集ポリシー作成**

   【Windows版】

   ```
   <インストールディレクトリ>¥bin¥sqcAPolicy.bat
   ```

   【UNIX版】

   ```
   /opt/FJSVssqc/bin/sqcAPolicy.sh
   ```

2. **ポリシーの適用**

   【Windows版】

   ```
   <インストールディレクトリ>¥bin¥sqcSetPolicy.exe [-h <host name>]
   ```

   【UNIX版】

   ```
   /opt/FJSVssqc/bin/sqcSetPolicy.sh [-h <host name>]
   ```

ポイント

Systemwalker Service Quality Coordinator V13.3.0以降は、ポリシー適用コマンド実行時にサービス/デーモンの事前停止は不要です。

ただし、サービス/デーモンが動作中で各ミドルウェア等の性能データが収集中であった場合、それらはポリシー適用の実施中は一時的に停止され、終了後に再収集を開始します。

なお、-hオプションを使用する場合は、「A.4 常駐プロセス、起動と停止」を参照して、サービス/デーモンを停止した上で実行してください。

■オプション

-h <host name>

以下のようなクラスタ運用を行っており、管理対象のシステム名を変更したい場合には、本オプションで設定したいシステム名を指定します。

- Managerで、かつManagerのサーバ内リソース情報を収集する場合(現用系と待機系のシステム名をひとつで管理したい場合)
- Agentで、かつノード名引継ぎを実施しているシステムを別々の名前で管理したい場合

A.3　ポリシー一時変更コマンド

ポリシー適用後の運用中(収集動作中)に、ポリシーを変更します。具体的には、以下のミドルウェアに対する情報収集ポリシーが作成・適用されている状態で、その収集動作を停止したり(off指定時)、起動したり(on指定時)することができます。

- Symfoware Server
- Oracle Database Server

詳細については、リファレンスマニュアル「1.1.4 sqcMdPolicy(ポリシー一時変更コマンド)」を参照ください。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

ポイント

業務の運用形態に合わせて収集動作を制御したい場合や、クラスタの運用形態に合わせて収集動作を制御したい場合に使用します。

■記述形式

【Windows版】

```
<インストールディレクトリ>¥bin¥sqcMdPolicy.exe on|off -c Type [ -i instance-name ]
```

【UNIX版】

```
/opt/FJSVssqc/bin/sqcMdPolicy.sh on|off -c Type [ -i instance-name ]
```

■オプション

on|off

変更種別として、以下のいずれかを指定します。

- on: 対象ポリシーを有効化します。
- off: 対象ポリシーを無効化します。
- stat:ポリシーの状態を表示(有効／無効)

-c Type

以下のいずれかの管理対象を指定します。

- sym : Symfoware Server
- ora : Oracle Database Server
- reg:レジストリ(Windows版のみ)
- sar:サーバ性能(Unix版のみ)
- jla:OperationManger

-i instance-name(DBサーバのみ指定可)

-cで指定する管理対象に対するインスタンス名を指定します。本オプションを省略した場合は、管理対象の全インスタンスが対象になります。

- symの場合 : RDBシステム名
- oraの場合 : インスタンス名

ポイント

RDBシステム名に名前が無い場合は、-i @defaultを指定してください。

- oraの場合 : Oracleインスタンス名(SID)

A.4 常駐プロセス、起動と停止

ここでは、常駐プロセスの起動と停止方法について説明します。

プロセスなど詳細については、リファレンスマニュアル「第2章 常駐プロセス、起動と停止」を参照してください。

■Manager

【Windows版】

以下のサービスを起動(開始)/停止します。

- Systemwalker SQC DCM

ポイント

Pull方式での通信をする場合は、以下のサービスを起動(開始)/停止します。

- Systemwalker SQC sqcschdle

ポリシー配付機能を使用する場合は、以下のサービスも起動/停止します。

- Systemwalker SQC thttpd

thttpdサービスを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

注意

[Systemwalker SQC DCM]サービスの再起動を実施する場合、Windowsのサービス画面で「サービスの再起動」を実行しないでください。
「サービスの停止」を実行してから、しばらくして、「サービスの開始」を実行してください。

【UNIX版】

以下のスクリプトで起動/停止します。

起動 :

```
/etc/rc2.d/S99ssqcdcm start
```

停止 :

```
/etc/rc0.d/K00ssqcdcm stop
```

ポイント

Pull方式での通信をする場合は、以下のスクリプトを起動(開始)/停止します。

起動：

```
/etc/rc2.d/S99ssqcsch start
```

停止：

```
/etc/rc0.d/K00ssqcsch stop
```

ポリシー配付機能を使用する場合は、以下のスクリプトを起動/停止します。

起動：

```
/opt/FJSVssqc/bin/ssqchttp start
```

停止：

```
/opt/FJSVssqc/bin/ssqchttp stop
```

thttpdデーモンを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

■Agent/Proxy Manager

【Windows版】

以下のサービスを起動(開始)/停止します。

- Systemwalker SQC DCM

ポイント

Pull方式での通信およびポリシー配付機能を使用する場合は、以下のサービスを起動/停止します。

- Systemwalker SQC thttpd

thttpdサービスを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

注意

[Systemwalker SQC DCM]サービスの再起動を実施する場合、Windowsのサービス画面で「サービスの再起動」を実行しないでください。
「サービスの停止」を実行してから、しばらくして、「サービスの開始」を実行してください。

【UNIX版】

以下のスクリプトで起動/停止します。

起動：

```
/etc/rc2.d/S99ssqcdcm start
```

停止：

```
/etc/rc0.d/K00ssqcdcm stop
```

ポイント

Pull方式での通信およびポリシー配付機能を使用する場合は、以下のスクリプトを起動/停止します。

起動：

```
/opt/FJSVssqc/bin/ssqchttp start
```

停止：

```
/opt/FJSVssqc/bin/ssqchttp stop
```

thttpdデーモンを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

■Enterprise Manager

【Windows版】

以下のサービスを起動(開始)/停止します。

- Systemwalker SQC DCM

ポイント

ポリシー配付機能を使用する場合は、以下のサービスを起動/停止します。

- Systemwalker SQC thttpd

thttpdサービスを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

注意

[Systemwalker SQC DCM]サービスの再起動を実施する場合、Windowsのサービス画面で「サービスの再起動」を実行しないでください。
「サービスの停止」を実行してから、しばらくして、「サービスの開始」を実行してください。

【UNIX版】

以下のスクリプトで起動/停止します。

起動：

```
/etc/rc2.d/S99ssqcdcm start
```

停止：

```
/etc/rc0.d/K00ssqcdcm stop
```

ポイント

ポリシー配付機能を使用する場合は、以下のスクリプトを起動/停止します。

起動：

```
/opt/FJSVssqc/bin/ssqchttp start
```

停止：

```
/opt/FJSVssqc/bin/ssqchttp stop
```

thttpdデーモンを自動起動させる方法は、「A.5 thttpdサービス/デーモンの自動起動設定」を参照してください。

A.5　thttpdサービス/デーモンの自動起動設定

本手順は、Pull方式での通信およびポリシー配付機能を使用する場合に起動させるプロセスです。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

■手順

【Windows版】

1. コントロールパネルで[管理ツール]→[サービス]と選択します。
2. 「Systemwalker SQC thttpd」を選択し、[プロパティ]を起動します。
3. [全般]タブの、「スタートアップの種類」を「自動」に変更します。

【UNIX版】

以下のコマンドを実行して起動スクリプトを設定します。

```
# cd /etc/rc2.d
# ln -s /opt/FJSVssqc/bin/ssqchttp S99ssqchttp
```

以下のコマンドを実行して停止スクリプトを設定します。

```
# cd /etc/rc0.d
# ln -s /opt/FJSVssqc/bin/ssqchttp K00ssqchttp
```

A.6　genpwd(パスワード暗号化コマンド)

インストールレス型Agentの接続アカウント定義ファイル(remoteAccount.txt)やECO情報のSNMPエージェントの構成情報ファイル(ecoAgentInfo.txt)[SNMPエージェントのバージョンがv3の場合]において、本コマンドを実行して暗号化されたパスワードを生成し、接続するためのパスワードのパラメーターに定義する必要があります。

以下、暗号化されたパスワードを生成するコマンドについて説明します。

■実行に必要な権限

【Windows版】

Administratorsグループに所属するユーザー権限が必要です。

【UNIX版】

システム管理者(スーパーユーザー)権限が必要です。

■記述形式

【Windows版】

```
<インストールディレクトリ>¥bin¥genpwd.exe
```

【UNIX版】

```
/opt/FJSVssqc/bin/genpwd.sh
```

■機能説明

暗号化されたパスワードを生成します。

■オプション

なし。

■終了ステータス

正常終了 1

異常終了 1以外

■使用例

暗号化されたパスワードを生成する場合は、以下のように実行します。

コマンドを実行するとパスワードとパスワードの確認の入力の問い合わせがありますので、暗号化したいパスワードを入力してください。

生成された文字列をコピーして、定義ファイルのパスワードのパラメータに貼り付けてください。

【Windows版】

```
C:¥ cd C:¥Program Files¥SystemwalkerSQC¥bin
C:¥Program Files¥SystemwalkerSQC¥bin>genpwd.exe
Password:
Confirm password:
```

```
bpnM2i65/s+k5YhGb15JKw==
C:¥Program Files¥SystemwalkerSQC¥bin>
```

【UNIX版】

```
# cd /opt/FJSVssqc/bin
# ./genpwd.sh
Password:
Confirm password:
bpnM2i65/s+k5YhGb15JKw==
#
```

用語集

Systemwalker Service Quality Coordinator Standard Edition

標準的な環境における管理機能を提供します。

Systemwalker Service Quality Coordinator Enterprise Edition

Standard Editionに加え、二階層(二階層運用)などの大規模システム運用、二重化運用やクラスタシステム運用などの高信頼システム運用、仮想ドメイン数が20を越える大規模仮想Webサイトシステムに対応します。

二重化

二台のManagerで、同じ対象システムを監視/管理する運用形態です。Managerの信頼性を求める場合や、離れた地域から同じ資源を監視/管理する場合に有効な分散型の運用形態です。

クラスタシステム

クラスタソフトウェアにより構築した高信頼システム全体を指します。2台のサーバマシンを1台の仮想サーバマシンとして運用することで、高可用性(High Availability)を実現します。

Enterprise Manager

各部門単位に配置されたManagerを一元管理します。Managerを二階層で構築し、負荷分散することにより、大規模なシステムも管理することが可能になります。(Enterprise Editionのみ)

Manager

インストール型Agent、インストールレス型Agent、およびProxy Managerが収集した情報を一括管理します。また、サービス(HTTP/S, DNS, SMTP, 任意ポート)稼働の監視や、Browser Agentが採取した情報の収集サーバの役割も果たします。

Proxy Manager

ManagerとAgentの間で中継機能を提供します。ManagerとAgentが、ファイアウォールで区切られる形態で、Proxy ManagerをAgent側に配置して中継することにより、サイトのセキュリティを高めることができます。また、Managerが行う、サービス(HTTP/S, DNS, SMTP, 任意ポート)稼働の監視やBrowser Agentが採取した情報の収集サーバの役割を代替することができます。

インストール型Agent

被監視サーバにインストールし、OSまたはミドルウェアが提供しているコマンドやAPIを定期的に発行して、性能情報を収集します。

インストールレス型Agent

被監視サーバのOSが提供しているコマンドやAPIをManagerからリモートで定期的に発行して、性能情報を収集します。被監視サーバには、Agentはインストールされません。

Agent for Server

インストール型Agentのインストール種別です。サーバ内のリソース情報を管理することができます。

Agent for Business

インストール型Agentのインストール種別です。Agent for Serverの機能に加え、Webサーバ、アプリケーションサーバ、データベースサーバといった業務システムに関する資源を管理することができます。

Browser Agent

エンドユーザーがWebサーバにアクセスした情報から、エンドユーザーが実感するレスポンスを測定します。動作プラットフォームは、Windowsのみです。

運用管理クライアント

Manager/Enterprise Managerに接続して、管理・操作するためのコンソール機能を提供します。運用管理者は、運用管理クライアントをインストールしたマシンの他、別マシン上からも、Webブラウザを運用管理クライアントに接続することにより、管理操作を行うこともできます。

動作プラットフォームは、Windowsのみです。Manager/Enterprise ManagerのプラットフォームがWindowsの場合は、Manager/Enterprise Managerと運用管理クライアントを同一サーバに導入することができます。

エンドユーザレスポンス管理

エンドユーザーがWebにアクセスした時の体感応答時間を管理します。

サービス稼働管理

各種サービス(HTTP/S、DNS、SMTP、任意ポート)の稼働状態を管理します。

Webトランザクション量管理

Webシステムへのリクエスト数や、リクエストに対する応答時間を管理します。

サーバ性能管理

各プラットフォーム(Windows, Solaris, Linux)のOS/カーネルの性能を管理します。

ユーザデータ管理

業務データやシステム稼働データなど、ユーザーの固有データ(CSV形式)を管理します。

Web利用状況管理

本機能については、「Web利用状況管理編」を参照ください。

利用状況分析

Webサイトの利用状況をさまざまな観点から分析することにより、顧客ニーズに見合った商品やサービスを提供することを支援します。

改ざん監視

Webコンテンツを定期的に検査し、改ざんを検出する機能を提供します。

Pull方式

ManagerがAgentまたはProxy Managerに対して問い合わせを行い、性能データを引っ張りあげる形の通信です。また、Pull方式を使用する場合は、HTTPを使用します。

Push方式

AgentまたはProxy ManagerからManagerに対して性能データをPushする形の通信です。

通常はPush方式の運用になります。

サマリデータ

システムの状況を大まかに把握するためのサマライズされたデータです。

リソースデータ

リソース単位に収集された詳細データです。

リソース

業務を構成するシステムやネットワーク、アプリケーションなどのことをリソースと呼びます。クラスタシステムの場合は、クラスタ化する資源(サービス、IPアドレス、DISKなど)のことを指します。

リソースID

リソースID とは、レコードを一意に識別する識別子です。

例えば、プロセス情報なら、プロセス名がリソースID になります。

PDB

収集した性能情報を格納するためのデータベースです。Performance Databaseの略です。

サマリ表示

システム全体の現在状況をすばやく把握するための表示機能です。

詳細表示

問題発生時に詳細情報を表示する機能です。サマリ表示では、システム全体の概要のみを表示するのに対して、詳細表示では、リソースごとの詳細な情報を表示します。

総点検分析・レポート

システム管理者が、システムの稼働状況を定期的に点検するための分析・レポートです。

カテゴリ別診断分析・レポート

問題があったサーバ内の、ボトルネックの一次切り分けを行うための分析・レポートです。

詳細分析・レポート

特定のデータを観点とした、詳細情報を確認するための分析・レポートです。

分析機能

情報の粒度やレポート目的に応じて、総点検分析、カテゴリ別診断分析、詳細分析の、3つのレベルの分析を提供しています。

分析機能は、確認したいときにすぐにレポートを表示することができます。

定期レポート

情報の粒度やレポートの目的に応じて、総点検レポート、カテゴリ別診断レポート、詳細レポートの、3つのレベルのレポートを提供しています。予めレポートの条件を登録して、スケジューラに登録しておくことにより、日報、週報、月報などのレポート出力を、自動化する機能です。

ログデータ(Troubleshoot)

Managerのデータベースに格納されている情報より、さらに詳細な情報（OS情報のみ）が記録されています。

インストールディレクトリ

実行モジュールなど、固定の資源をインストールするディレクトリのパスです。

可変ファイル格納ディレクトリ

動作中に変更、または参照するファイルを格納するためのディレクトリのパスです。

PDBコマンド

PDBにアクセスするためのコマンドです。CSV出力コマンド、ユーザデータ入力コマンド、データ削除コマンド、構成情報移行コマンドの4つがあります。

現用系

クラスタシステムでクラスタサービスが動作している側のノードです。

待機系

クラスタサービスは通常稼働していないで、異常時に稼働するノードです。

グループ

クラスタシステムにおいて、切り替える対象となるリソースをまとめたもので、トラブルが発生した場合に待機側に切り替わる単位となります。

共用ディスク

クラスタシステムにおいて、現用系のノードと待機系のノードで共用して使用するディスク領域のことです。

収集テンプレート

本定義には、常時収集する項目が定義されており、ポリシー作成/ポリシー適用の実行時に本定義に従って自動的に収集ポリシーが作成されます。

しきい値

システムやアプリケーションの性能を監視する値です。

アラームアクション

しきい値監視定義をすると、しきい値超えを管理者に知らせるためのアクションが実行されます。アクションの種類には、以下があります。

イベントログ/syslog
Systemwalker Centric Managerメッセージ連携
メール
トラップ
ユーザー任意のコマンド実行

ポリシー配付機能

運用管理クライアント上で、情報収集、しきい値監視するサーバへ、収集ポリシー、しきい値監視定義を配付し、配付先サーバで収集ポリシーの作成と適用、しきい値監視を実施します。

ポリシー定義情報

ポリシー配付機能で配付することが可能な、収集ポリシーおよび、しきい値監視定義のことです。

ポリシー管理フォルダ

ポリシー配付を使用するために必要なファイルをフォルダごとに管理します。

ポリシー配付グループ

配付するポリシー定義情報の定義内容が異なる場合に作成します。

ポリシー配付定義

ポリシー定義情報の配付先サーバ情報を定義します。

フェールオーバ

クラスタシステムにおいて、グループ内のリソースにトラブルが発生し、運用側のノードが待機側に切り替わることです。

ホスト名

ネットワーク上の各ノードにおいて、一意的に割り当てられる名前です。HostsファイルやDNS等を利用してIPアドレスとホスト名を対応づけます。

アプリケーション・サーバ

処理時間、待ち時間、ヒープ量、レスポンス内訳分析など、業務システムの性能を管理します。

以下のアプリケーション・サーバ製品をサポートします。

Interstage Application Server
Interstage Business Application Server
Interstage Application Framework Suite
Interstage Service Integrator
Microsoft .NET Server
SAP NetWeaver

データベース・サーバ

IO、メモリ、キャッシュ、スペース、デッドロック、SQL回数など、データベース性能を管理します。下記のデータベース・サーバ製品をサポートします。

Symfoware Server
Oracle Database Server
Microsoft SQL Server

ジョブ

多重度や実行待ち数など、ジョブ実行性能を管理します。下記のジョブ管理製品をサポートします。

Systemwalker Operation Manager

ネットワーク

トラフィック量、パケット数、エラー数など、ネットワーク性能を管理します。下記のネットワーク管理製品をサポートします。

Systemwalker Network Manager
Systemwalker Centric Manager

ストレージ

IO、スループット、レスポンス、キャッシュなど、ストレージ性能を管理します。下記のストレージ管理製品をサポートします。

Systemwalker Resource Coordinator
ETERNUS SF Storage Cruiser

コンソール

本製品のメインの画面です。

サマリ表示、詳細表示、分析機能、定期レポート画面が表示されます。

強制終了

[Systemwalkerコンソール]で、選択しているアプリケーションに対し、プロセスを停止するように指示を出す機能です。停止時には、強制終了コマンドが使用されます。

DMZ

Demilitarized Zoneの略です。インターネットとイントラネットを分離するネットワークです。

EntryURL

Webサーバへの訪問で最初に参照したページです。

ExitURL

Webサーバへの訪問で最後に参照したページです。

HTTPサーバ

Hypertext Transfer Protocolサーバの略で、Webサーバともいいます。

SQC拡張ログ

SQC拡張ログ採取がSQC拡張ログファイルに蓄積するデータです。

SQC拡張ログ採取

Webサービスを構成する機能（Webサーバ等）で採取されていないデータを採取して蓄積する機能です。

SQC拡張ログファイル

SQC拡張ログ採取がSQC拡張ログを蓄積するファイルです。

Webサーバ

HTTPサーバのことです。

Webページ表示レスポンス

Webブラウザでコンテンツを表示するのに費やす時間です。

改ざん

ネットワークを通じてコンピュータに侵入し、Webページやアクセスログなどの情報を管理者の許可を得ずに書き換える行為です。

改ざん監視エージェント

改ざん監視プログラムから呼び出され、公開コンテンツの格納ファイルにアクセスし、メッセージダイジェストを生成するCGIです。

改ざん監視設定ファイル

コンテンツ改ざん監視機能の改ざん監視対象に関する設定情報が格納されているファイルです。

改ざん監視環境定義ファイル

コンテンツ改ざん監視機能の環境定義に関する設定情報が格納されているファイルです。

公開Webコンテンツ

Webサイトに公開されているコンテンツです。

コンテンツ公開

正当なコンテンツ管理者がネットワークを通じてWebサーバにコンテンツを転送する行為です。

コンテンツ改ざん監視

公開コンテンツの改ざんを監視する仕組みです。

コンテンツ改ざん監視プログラム

定期的に起動し、公開コンテンツの改ざんを検査するプログラムです。

コンテンツ改ざん監視通知

コンテンツの改ざん監視により改ざんが検出された場合の通知です。

コンテンツ管理者

公開コンテンツを管理している人、およびコンテンツ原本アップデート申告を行う人です。

コンテンツ原本

公開コンテンツの比較対象となるWebサイトコンテンツのオリジナルデータです。

コンテンツ公開申告

公開コンテンツのアップロードを行う際に、コンテンツ原本のアップデートを行う手続きです。

コンテンツ公開申告コマンド

コンテンツ原本のアップデートを申告する際に使用するコマンドです。

サイトアクセス量分析

サイトにアクセスされた量を観点とした分析です。

サイトナビゲーション分析

サイトにアクセスしたユーザーを観点とした分析です。

スナップショットDB

コンテンツ原本の情報（URL、ハッシュ値等）が格納されているファイルです。

セッション

同一クライアントが行った連続したアクセスのまとまりです。何人の人がアクセスしているかを知る指標となります。同一クライアントが複数回アクセスしているような場合、そのアクセスの間隔が15分未満の場合は、同一セッションとしてカウントします。

ドリルダウン

現在見ている情報を一歩踏み込んで、より詳細に見ることをドリルダウンといいます。本製品では、現在分析しているレベルからより詳細に分析することをドリルダウン分析といい、例えば、URLの分析を行い、ある特定のURLに対して、どのクライアントが見ているかというような分析をドリルダウン分析といいます。

分析画面

利用状況分析機能を構成する機能の一つです。Webブラウザ上で動作し、各種の分析結果ページを表示します。

分析ページ

分析画面がWebブラウザ上で表示するデータの分析結果のページです。

利用状況DB

利用状況分析のための基礎データを格納したデータベースです。

利用状況DB参照エンジン

利用状況分析機能を構成する機能の一つです。インストールマシン上で動作し、分析画面からの要求に応じて利用状況DBからデータを取り出します。

利用状況DB登録エンジン

利用状況分析機能を構成する機能の一つです。インストールマシン上で動作し、Webサービスを構成する各種機能（Webサーバ等）のログからデータを抽出し、利用状況DBに格納します。

利用状況分析機能

Webサービスの分析を支援する機能です。