FUJITSU

Fujitsu Software Systemwalker Centric Manager V17.0.5

解説書

UNIX/Windows(R)共通

J2X1-8230-08Z0(00)
2025年9月

まえがき

本書の目的

本書は、Systemwalker Centric Managerの機能概要について説明しています。

本書の読者

本書は、Systemwalker Centric Managerの運用方法、および利用方法の概要を理解しSystemwalker Centric Managerの導入を検討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、SMTP、SNMP、ディレクトリサービス(Active DirectoryまたはLDAP)などの一般的な知識をご理解の上でお読みください。

本書の表記について

固有記事の表記、使用している記号、および略称表記については、“本書の表記について”を参照してください。

Systemwalker Centric Manager 技術情報ホームページについて

ツールやテンプレート、マニュアルなどの技術情報については、Systemwalker Centric Manager 技術情報で公開しています。必要に応じて、以下を参照してください。

https://www.fujitsu.com/jp/software/technical/systemwalker/centricmgr/

登録商標について

登録商標については、“登録商標について”を参照してください。

輸出管理規制について

本ドキュメントを輸出または第三者へ提供する場合は、お客様が居住する国および米国輸出管理関連法規等の規制をご確認のうえ、必要な手続きをおとりください。

改版履歴
2021年 12月 初版
2022年 5月 第2版
2022年 8月 第3版
2023年 9月 第4版
2024年 4月 第5版
2024年 10月 第6版
2025年 5月 第7版
2025年 9月 第8版

Copyright 1995-2025 Fujitsu Limited

Copyright PFU Limited 1995-2025

目　次

第1章 概要 1
1.1 Systemwalker Centric Managerの概要 1
1.1.1 Systemwalkerとは 1
1.1.2 Systemwalker Centric Managerの役割 2
1.1.3 Systemwalker Centric Managerの機能 3
1.2 製品体系 5
1.3 管理対象 6
1.4 インストール種別 6
1.4.1 運用管理サーバ 6
1.4.2 部門管理サーバ 6
1.4.3 業務サーバ 7
1.4.4 運用管理クライアント 7
1.4.5 クライアント 7
1.4.6 ライセンスとインストール種別の関係 8
1.5 エージェントのインストール形態 8
1.6 運用形態 9
1.6.1 基本的な構成の運用形態 9
1.6.2 エージェントを導入しないでシステムを監視する 13
1.6.3 プラットフォームやバージョンが混在した形態 15
1.6.4 Virtual Machine(VM)環境のシステムを監視する 16
1.6.5 Server Core環境に導入する【Windows版】 18
1.6.6 グローバルサーバを監視する 19
1.6.7 マルチテナントにおける監視 20
1.6.8 Nano Serverを監視する 21
1.6.9 IPバージョンが混在した形態 21
1.6.10 その他の運用形態 22

第2章 機能の説明 24
2.1 コンソール 24
2.1.1 Systemwalkerコンソール 24
2.1.2 Systemwalker Webコンソール 26
2.1.3 Systemwalker Webコンソール(モバイル版) 28
2.2 セキュリティ 31
2.2.1 Systemwalkerセキュリティ指針 32
2.2.1.1 セキュリティとは 32
2.2.1.2 セキュリティの要件 32
2.2.1.3 セキュリティ対策 32
2.2.2 Systemwalkerコンソールの操作を制御する 35
2.2.3 サーバの利用を制御する 36
2.2.4 監査ログを管理/分析する 37
2.3 構成情報の管理（フレームワーク） 41
2.3.1 ネットワークの構成情報を管理する 42
2.3.2 システムの構成情報を管理する 44
2.4 監視 46
2.4.1 ネットワーク/システムの監視 50
2.4.1.1 ネットワーク/システムの障害を監視する 53
2.4.1.2 ネットワーク/システムの稼働状況を監視する 58
2.4.1.3 ネットワーク/システムの性能を監視する 60
2.4.1.4 グローバルサーバのシステムを監視する 63
2.4.1.5 グローバルサーバのサブシステムを監視する 66
2.4.2 アプリケーションの監視 66
2.4.2.1 アプリケーションの障害を監視する 67
2.4.2.2 アプリケーションの稼働状況を監視する 67
2.4.2.3 アプリケーションの性能を監視する 69
2.4.3 業務の監視 70

2.4.4 管理者への通知 72
2.4.5 Systemwalker自身の監視 72
2.4.6 ノードの変更監視 73
2.4.7 メッセージ返答要求・返答操作【Solaris版/Linux版】 73
2.4.8 イベントから連携製品の状況確認 74
2.4.9 Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントの監視 74
2.4.9.1 監視対象 75
2.4.9.2 サポート機能 75
2.5 障害復旧 81
2.5.1 リモートから復旧操作する 81
2.5.1.1 リモート操作 82
2.5.1.2 リモートコマンド 84
2.5.1.3 リモートからの電源制御 86
2.5.2 障害への対処を自動化する 86
2.5.2.1 自動アクション 86
2.5.2.2 ServiceNow連携 87
2.6 ソフトウェア修正管理 89
2.7 資源の配付 90
2.7.1 いろいろな資源を配付する 92
2.7.2 配付先システムを選択する 93
2.7.3 世代を管理する 93
2.7.4 適用日をスケジュールする 94
2.7.5 大規模システムで配付する 94
2.7.6 大量データを配付する 95
2.7.7 グローバルサーバシステムで配付する 95
2.8 評価 96
2.8.1 ネットワークのサービスレベルを評価する 96
2.8.2 システムのサービスレベルを評価する 97
2.9 SDK 99
2.9.1 Systemwalkerスクリプトの概要 99
2.9.2 インテリジェントサービスを使用する 100
2.10 ユーザ管理 102

第3章 動作環境 103
3.1 ハードウェア資源 103
3.1.1 ディスク容量 103
3.1.1.1 静的ディスク容量 103
3.1.1.2 動的ディスク容量 107
3.1.1.3 パーティションについて【Linux版の場合】 109
3.1.2 メモリ容量 109
3.1.2.1 メモリ使用量 110
3.1.3 スワップ容量【Solaris版/Linux版】 112
3.1.4 推奨スペック 112
3.1.5 必要なハードウェア資源 113
3.2 ソフトウェア資源 115
3.2.1 動作OS 115
3.2.1.1 Windows版 115
3.2.1.2 Solaris版 116
3.2.1.3 Linux版 117
3.2.2 関連ソフトウェア資源 118
3.2.3 共存時に注意が必要なソフトウェア資源 125
3.2.3.1 共存できないソフトウェア 125
3.2.3.2 共存時に注意が必要なソフトウェア 126
3.2.4 リモートデスクトップ（ターミナルサービス）を使用する場合の注意事項 128
3.2.5 LDAP参照環境で使用する場合の注意事項【UNIX版】 128
3.3 Global Enterprise Editionの動作環境 129
3.3.1 監視・操作できるシステム 129

3.3.2 ハードウェア環境 129
3.3.2.1 監視システム 129
3.3.2.2 被監視システム 129
3.3.2.3 ネットワーク環境 130
3.3.3 動作OS 130
3.3.4 監視に必要なソフトウェア環境 130
3.3.4.1 監視システムに必要なソフトウェア 131
3.3.4.2 被監視システムに必要なソフトウェア 131
3.3.5 資源配付に必要なソフトウェア環境 134
3.3.5.1 運用管理サーバに必要なソフトウェア 134
3.3.5.2 管理対象システムに必要なソフトウェア 134
3.3.6 監査ログ管理に必要なソフトウェア 135
3.3.6.1 被監視システムに必要なソフトウェア 135

付録A Systemwalker Centric Managerと他製品の連携 137
A.1 連携製品一覧 137
A.1.1 Systemwalkerファミリ 137
A.1.2 アプリケーションサーバ 138
A.1.3 データベースソフト 138
A.1.4 ハードウェア監視ソフト 138
A.1.5 クラウドサービスソフト 138
A.1.6 その他 139

付録B OS別機能差一覧 140
B.1 構成の管理 140
B.1.1 ネットワークの構成情報の管理 140
B.1.2 システムの構成情報の管理 140
B.1.3 コンソール 140
B.2 資源の配付 141
B.2.1 資源配付 141
B.3 ネットワーク/システムの監視 141
B.3.1 稼働監視 141
B.3.2 障害監視 141
B.3.3 ネットワーク性能監視 142
B.3.4 サーバ性能監視 142
B.3.5 DHCP監視 143
B.3.6 イベントコリレーション 143
B.3.7 メッセージ変換 143
B.3.8 イベント抑止 143
B.3.9 監視抑止 144
B.4 アプリケーションの監視 144
B.4.1 稼働監視 144
B.4.2 障害監視 144
B.4.3 性能監視 145
B.5 ソフトウェア修正管理 145
B.6 ポリシー 145
B.7 Systemwalker自身の監視 146
B.7.1 イベントトレース 146
B.7.2 Systemwalkerのプロセス監視 146
B.7.3 Systemwalkerセルフチェック 146
B.7.4 スローダウン監視 146
B.7.5 IPC資源の一元管理 147
B.8 障害の復旧 147
B.8.1 リモートからの操作 147
B.8.2 リモートからの電源投入・切断 147
B.8.3 障害対処の自動化 148
B.9 返答メッセージ 148

B.10 評価 148
B.10.1 監査ログ分析 148
B.11 セキュリティ 149
B.11.1 サーバアクセス制御 149
B.11.2 コンソール操作制御 149
B.11.3 操作ログ出力 149
B.11.4 監査ログ出力 150
B.11.5 監査ログ管理 150
B.11.6 監査ログ分析 150
B.12 共通(さまざまなシステムでの利用) 150
B.12.1 高信頼システムの管理 150
B.12.2 管理サーバの高信頼化 151
B.12.3 大規模システム 151
B.13 Systemwalkerスクリプト 151
B.14 トラブルシューティング 152
B.14.1 調査資料の採取 152
B.15 注釈 152

付録C 製品の組み合わせ 156
C.1 エディションの組み合わせ 156
C.2 バージョンの組み合わせ 161
C.2.1 プラットフォームとバージョン混在時の接続性 162
C.2.2 リモート操作エキスパートとリモート操作クライアントの接続 163
C.2.3 上位システムの製品バージョンレベルが、下位システムより古い場合のサーバOS表示について 163
C.2.4 Windows 11のOS表示について 164

付録D Systemwalker Centric Managerの制限値と推奨値 165
D.1 制限値のある主な機能 165
D.1.1 監視 165
D.1.2 管理者への通知 167
D.1.3 高信頼性システム 167
D.1.4 管理形態 167
D.1.5 返答メッセージ 167
D.2 円滑に運用管理するための推奨値 167
D.2.1 監視 168
D.2.2 資源配付 169
D.3 ポーリング間隔 170
D.3.1 稼働状態の監視間隔 170
D.3.2 MIBしきい値監視間隔 170
D.3.3 ネットワークの性能異常の監視間隔 170
D.4 監視間隔 170
D.4.1 サーバの性能異常の監視間隔 170
D.4.2 アプリケーションの稼働状況の監視間隔 171
D.4.3 アプリケーションの性能異常の監視間隔 171
D.4.4 アプリケーションの稼働監視間隔 171

付録E 構成情報一覧 172

付録F 監視できるインストールレス型エージェントのOS 175
F.1 Windows 175
F.2 Solaris 176
F.3 Linux 177
F.4 HP-UX 179
F.5 AIX 180

付録G 本書の表記、登録商標について 182
G.1 本書の表記について 182
G.2 登録商標について 189

第1章　概要

Systemwalker Centric Managerの機能の概要を説明します。

1.1　Systemwalker Centric Managerの概要

Systemwalker Centric Managerの概要について説明します。

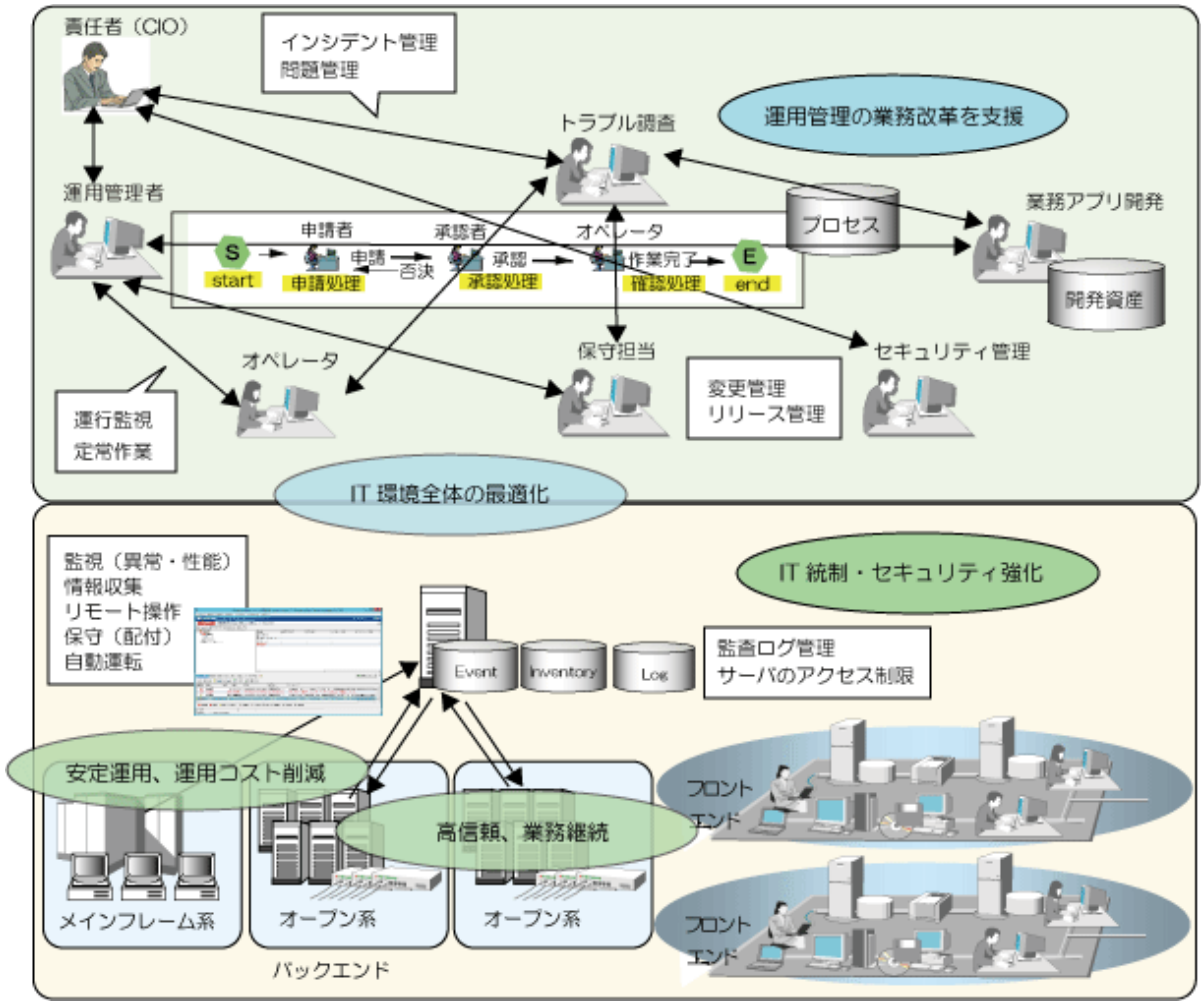
1.1.1　Systemwalkerとは

業務の再編、企業統合、企業間連携などにより、企業のIT環境は、ダイナミックに変化、柔軟に連携できることが求められ進化してきております。反面、情報システムの運用管理は、より複雑さ、困難さが増大しております。さらに、内部統制やITガバナンスの強化に対する要請が強くなっています。

運用管理には、情報システムの単なる作業支援ではなく、企業全体の情報システムの最適化やIT関連の業務改革を推進する役割が求められます。

これらの要件に対応するために、Systemwalkerでは、情報システムの運用管理だけでなく、情報システムの運用に関わる部門全体の運用業務を支援し、IT環境全体の最適化を実現する機能を提供します。

図1.1 IT環境のライフサイクル管理



安定運用・コスト削減

情報システムの安定運用のために、システムの構成情報の収集、運行状態、異常メッセージ、資源使用量などの監視、コマンド・操作などの制御機能を提供します。また、これらの機能は、1箇所での集中管理・時間や状態の変化などさまざまなトリガによる自動運転ができますので、管理に関わるコストが削減できます。

高信頼・業務継続性

ビジネスの継続性を実現するために、情報システムには、24時間365日無停止で稼働することが求められます。高信頼化のために、サーバの二重化、通信パスの二重化、無停止での拡張・メンテナンスなどを実現しています。

IT統制・セキュリティ強化

IT統制を実現するためには、情報システムに関連する情報部門の役割が重要になります。情報システムを守るためのアクセス制御、監査ログ収集などの情報システムのセキュリティを強化します。

IT環境全体の最適化

企業内にあるさまざまなシステムを統合して管理できます。メインフレームからフロントエンドのPCクライアントまで、また標準のインタフェースで、他社の運用管理ソフトウェアとも連携できます。これにより、企業内のIT環境全体の最適化を実現します。

運用管理の業務改革を支援

情報システムだけでなく、運用プロセスを含めたIT環境全体のライフサイクルを管理できます。これにより、IT戦略に基づいて計画どおりに稼働できていること、問題の継続的な改善など、IT環境を中心とする業務改革を支援します。

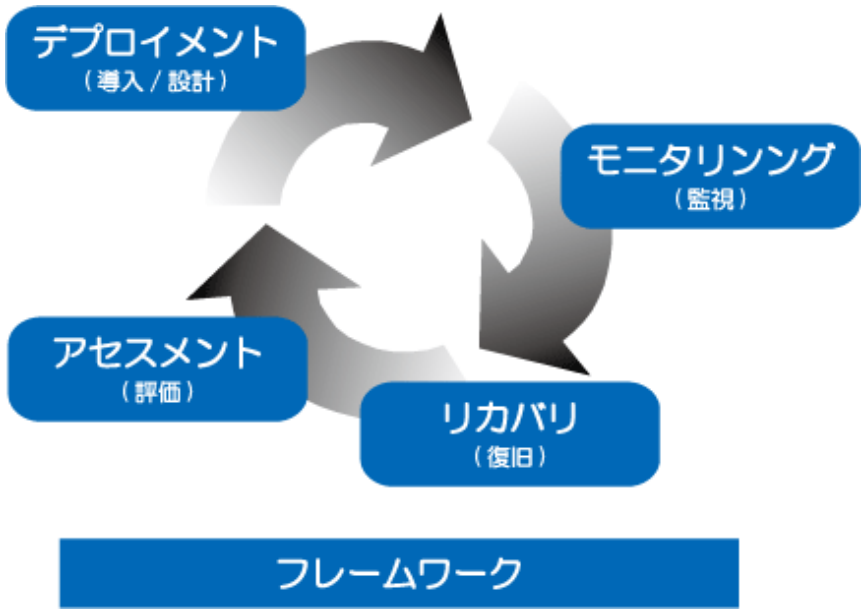
1.1.2 Systemwalker Centric Managerの役割

Systemwalker Centric Managerは、IT環境の運用管理を行うための統合基盤となる製品です。IT環境を構成する資源(ネットワーク、ハードウェア、OS、アプリケーション、利用者など)、業務および運用部門を含めた、企業のIT環境全体のライフサイクルを戦略(ポリシー)に基づいて管理します。

ライフサイクル・マネージメント

Systemwalker Centric Managerでは、IT資源のライフサイクルを管理します。

IT資源のライフサイクルを次の4つのフェーズにわけ、効率的に運用管理を行います。



・ デプロイメント(導入/設計)

IT資源および業務をシステムへ導入/設定するフェーズです。情報システムで利用する資源の配付・適用を行います。

・ モニタリング(監視)

運用フェーズに入ってからのIT資源や業務の稼働状況、性能などを監視するフェーズです。IT資源の稼働監視、異常監視、性能監視を行い業務が正しく稼働していることを監視します。

・ リカバリ(復旧)

トラブル時の対処、復旧のフェーズです。トラブル発生時に調査や対処を行い、障害を管理します。

・ アセスメント(評価)

業務の安定稼働を評価するフェーズです。業務の稼働情報や、業務を構成するIT資源の情報から業務のサービスレベルを評価/分析します。業務のボトルネックの検出やキャパシティプランニングを行います。

・ フレームワーク

運用管理作業においては、上記の4つのマネージメント機能が、相互に連携してIT環境のライフサイクルを管理します。マネージメント機能間での情報共有、シームレスな機能連携、統一した管理ビューを提供するのが、フレームワークです。フレームワークは、管理対象資源(ネットワーク、ハードウェア、OS、ソフトウェアなど)の構成情報、運用ポリシー、および、メッセージ、操作ログ、履歴などの各種ログ情報などを一元管理します。

1.1.3 Systemwalker Centric Managerの機能

Systemwalker Centric Managerで提供するライフサイクル・マネージメントの機能とその特徴について説明します。

デプロイメント(配付)

資源の配付

アプリケーションやデータなど情報システムで利用する資源(ファイル)を一元管理し、対象のサーバ・クライアントへ配付します。資源は、論理的なグルーピングにより、情報システムや業務構成と関係付けて管理できます。これにより、業務資源を効率よく管理でき、配付作業のミスを防止し、管理者の負荷を削減します。

グローバルサーバをホストとして運用している環境の上位に配置したサーバから、グローバルサーバおよびグローバルサーバ配下のシステムの管理を行うことができます。

ソフトウェア修正管理

ソフトウェア修正管理は、富士通が提供するソフトウェア製品の修正を提供するサイト(アップデートサイト)と連携して、修正の適用を管理します。

資源の配付と組み合わせることで、業務アプリケーションからソフトウェアまで一貫した管理が可能になります。

モニタリング（監視)

監視

IT環境を構成するネットワーク、ハードウェア、OS、ソフトウェアの稼働状況、障害状況、性能状況を監視できます。また、これらの資源を論理的なグルーピングにより、情報システムや業務構成と関係付けて監視できます。これにより、障害範囲の把握、障害の発生箇所や原因の特定が容易にでき、迅速な対処・復旧が可能になります。

また、Systemwalker Centric Manager GEEでは、グローバルサーバのハード監視機能による監視、サブシステムの稼働監視を行います。

以下に主な管理対象と監視の方法を示します。

表1.1 モニタリング(監視)

管理対象	ネットワーク	ハードウェア	ソフトウェア
稼働状況	IP(SNMP、ICMP、HTTPなどのプロトコル)による通信状態の監視	稼働状態(OS、管理ソフトウェアから取得)	プロセス、サービスの稼働状態(OS、管理ソフトウェアから取得)
障害状況	SNMPトラップ	SNMPトラップ システムログ(UNIX syslog、Windows Event Logなど)	SNMPトラップ システムログ(UNIX syslog、Windows Event Logなど)ログファイル
性能状況	SNMP(MIBのしきい値監視)による通信量、破棄パケット量など	CPU使用量、メモリ使用量、IO性能など	応答時間、処理量、処理待ち時間など

イベントの集約

OSやソフトウェアが出力する個々のイベント、メッセージでは、発生している事象を把握できないことがあります。また、保守作業時には、大量にメッセージが出力されるので、ほかのシステムの監視を阻害することがあります。このような問題を解決するために、複数のイベントを集約して通知したり、わかりやすいメッセージに変換したり、一時的に監視を抑止することが必要です。複数のイベントを集約する機能をイベントコリレーションと呼びます。イベントコリレーションや、メッセージ変換、一時的な監視を抑止する機能により、監視者に必要なメッセージに変換して通知したり、不要なメッセージの通知を抑止したりできます。

Systemwalker Centric Manager GEEでは、基幹系マルチサーバ(グローバルサーバ、UNIX、Windows)のメッセージを一元管理します。

リカバリ(障害復旧)

障害復旧

障害が発生したサーバに対する復旧や調査などの操作(コマンド操作、画面操作など)を運用者の管理コンソールから実施することができます。これにより、復旧や調査のために現地に行かなくても操作することが可能です。また、監視機能と連動して、発生した事象に対して、特定の対処操作を自動化することも可能です。

トラブルに対する情報や対処方法をノウハウとして蓄積して活用することも可能です。また、さまざまなハードウェアやソフトウェアに対するノウハウは、富士通のサイト(テクニカルデスク)から提供しています。なお、MSP・XSPシステムを監視する場合には、システムメッセージガイド(CD-ROM)によりメッセージの説明を自動的に表示することが可能です。

アセスメント(評価)

レポーティング

Systemwalkerが収集した構成情報、メッセージやログ情報、稼働情報はグラフや表などに表示することができます。これにより、運用報告書等の作成が容易にできます。また、障害の傾向や資源の活用状況などの分析が可能になり業務改革につなげることができます。

アクセス制御と監査ログ

運用管理者が管理コンソールから行う操作や、サーバの資産に対して、目的や役割にあったアクセス制御が可能になります。

また、操作履歴を収集・管理し、情報システムの運用に関する点検を行うことができます。

監査ログ分析

各システムで出力された監査ログを、分析目的に応じた問い合わせサンプルファイルを利用することにより、簡単に集計・分析ができます。集計・分析は、運用管理サーバのスケジューラに登録して夜間に実行し、表形式(CSV形式、またはHTML形式)でファイルに出力します。必要な作業はセキュリティ管理者による分析結果の確認だけです。ログの見落としなどのチェックミス発生を防ぐことができます。

フレームワーク

フレームワークは、以下の機能を提供します。

Systemwalkerが収集したさまざまな情報を格納する構成管理データベースを装備しています。ネットワーク、ハードウェア、ソフトウェアの構成情報、稼働状態やメッセージ、性能情報、操作履歴などのログ情報を管理します。

利用者が役割や目的にあった操作・作業ができるような管理コンソール(GUI)を提供します。Systemwalker Centric Managerが提供する機能だけでなく、ほかの富士通製品やツールの統合が可能なコンソールのフレームワークです。

富士通以外のベンダが提供する運用管理製品と連携して、構成情報やメッセージの統合管理が可能です。

1.2 製品体系

Systemwalker Centric Managerの製品体系について説明します。

Systemwalker Centric Managerは、以下の3種類のエディションがあります。

- Systemwalker Centric Manager Standard Edition
- Systemwalker Centric Manager Enterprise Edition
- Systemwalker Centric Manager Global Enterprise Edition

Systemwalker Centric Manager Standard Edition

TCP/IPネットワーク上の標準的なクライアント-サーバ環境、インターネット環境における業務のライフサイクルを管理する機能を提供します。

Systemwalker Centric Manager Enterprise Edition

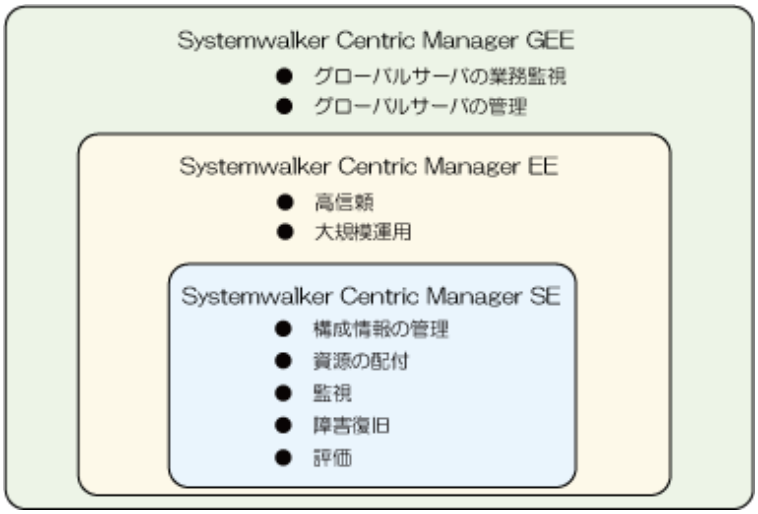
大規模、高信頼な環境向けの製品です。SE版の機能に加えて、マネージャの階層化など柔軟な運用形態、高信頼システムを管理するための機能などを提供します。

Systemwalker Centric Manager Global Enterprise Edition

SE版およびEE版の機能を包含し、さらに、グローバルサーバのライフサイクルを管理する機能を提供します。

以下に、3種類のエディションの関係を示します。

図1.2 Systemwalker Centric Managerの製品の関係



Systemwalker Centric Manager EE、Systemwalker Centric Manager SEで、提供する機能差については、“OS別機能差一覧”を参照してください。

また、Systemwalker Centric Manager GEEだけで提供されている機能については、“Systemwalker Centric Manager 使用手引書 グローバルサーバ運用管理ガイド”を参照してください。

1.3　管理対象

Systemwalker Centric Managerで管理するIT資源を以下に示します。

- ネットワーク

  TCP/IPプロトコルをベースとしたネットワーク

- ハードウェア

  ネットワーク機器（ルータ、バブ）、サーバ機（UNIX、AT互換機）、プリンタなどIPを持ったハードウェア

- システム

  Solaris、HP-UX、AIX、Linux、Windowsなどのオペレーティングシステム

- アプリケーション

  データベース、グループウェアなどのミドルウェア、市販のソフトウェア、および顧客で作成したアプリケーションなどの実行ファイル

1.4　インストール種別

Systemwalker Centric Managerは、通信負荷を軽減し、システムを効率的に管理するため階層構造を構築して管理します。

Systemwalker Centric Managerでは、インストール時に以下のインストール種別からコンピュータにインストールする種別を選択します。インストール種別により、階層構造での位置や役割が異なります。それぞれのサーバおよびクライアントの役割を説明します。

- 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
- クライアント

各インストール種別をインストールできるOS

動作OSの詳細については“動作OS”を参照してください。

1.4.1　運用管理サーバ

集中管理を行うためのサーバです。システムから収集した情報は、運用管理サーバ上で管理します。管理者は、運用管理サーバに接続したコンソール（運用管理クライアント）から監視、操作などを行います。

Windows版Systemwalker Centric Managerの場合、運用管理サーバに運用管理クライアント機能が包含されています。

1.4.2　部門管理サーバ

システム全体で管理対象のノードが多い場合や地域的に離れている場合などは、負荷分散のために部門管理サーバを設置します。

部門内の管理を行うためのサーバで、以下の役割を持ちます。

- 部門内のノードおよびサブネットに対して、ネットワークの情報収集やSNMP/ICMP/HTTPなどのプロトコルでのポーリングによる監視などを行います。
- 部門内で発生したイベントを収集し、運用管理サーバへ中継します。運用管理サーバへの中継は、必要なイベントだけを選択して行うことができます。
- 部門内のサーバおよびクライアントへ資源を配付する際の中継を行います。

部門管理サーバは管理するだけでなく、業務サーバと同様に被管理対象となります。

1.4.3　業務サーバ

被管理対象となるサーバです。運用管理サーバまたは部門管理サーバから管理されます。管理されるだけでなく、資源の配付、イベント通知、情報集中のための中継としての役割も果たします。

1.4.4　運用管理クライアント

運用管理サーバに接続して管理するためのコンソールです。管理者は、運用管理クライアントから監視、操作を行います。
運用管理クライアントは、Windows OSのPC端末に作成します。UNIX版Systemwalker Centric Managerの運用管理サーバを使用する場合、必ず1台以上のPC端末を運用管理クライアントとして用意してください。
Windows版Systemwalker Centric Managerの場合は、運用管理サーバで兼務することができます。

ポイント

運用管理クライアントの接続台数

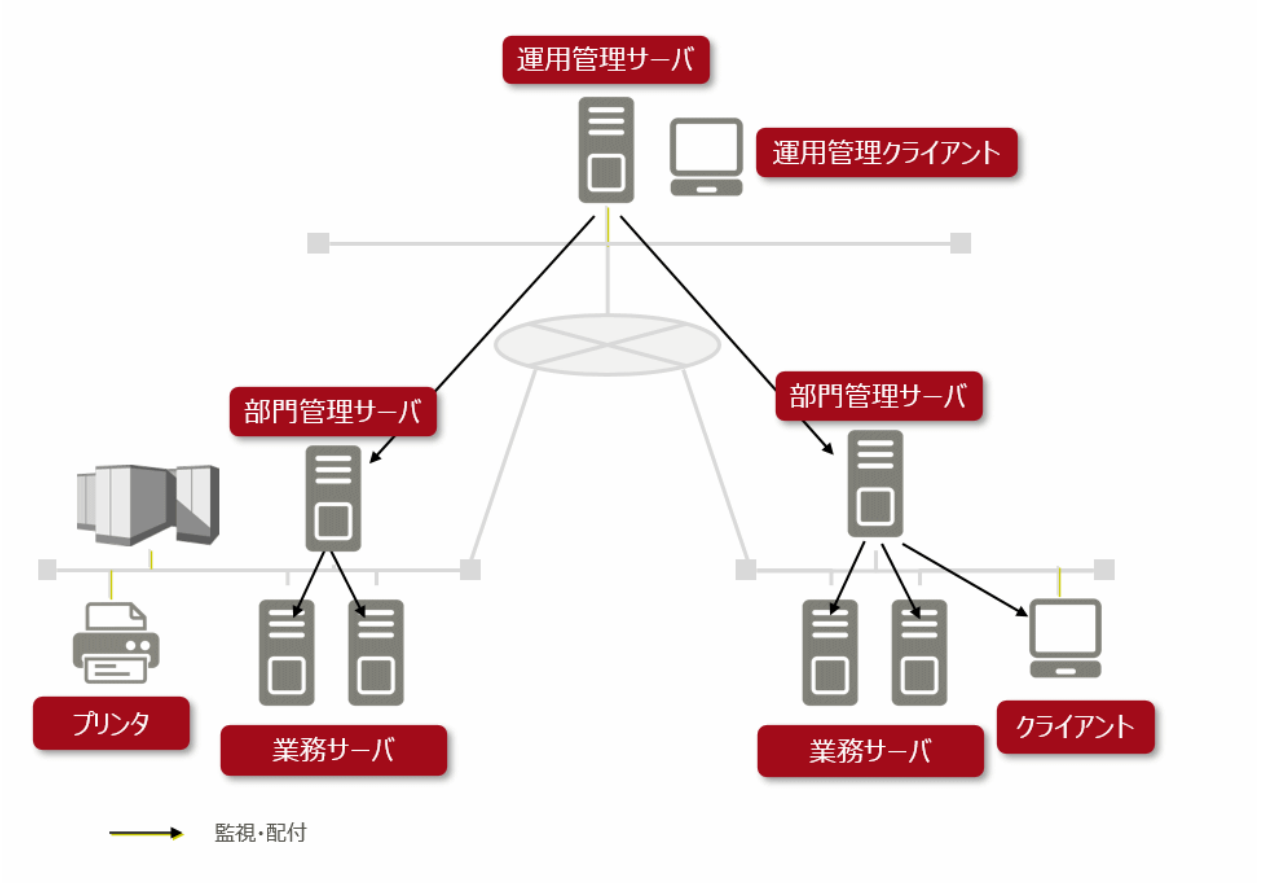
1台の運用管理サーバに同時に接続可能な運用管理クライアントは、以下の台数までです。

- Systemwalker Centric Manager SEの場合 : 8台まで
- Systemwalker Centric Manager EE/GEEの場合 : 50台まで

1.4.5　クライアント

被管理のクライアントPCです。

以下に、管理形態のモデルを示します。



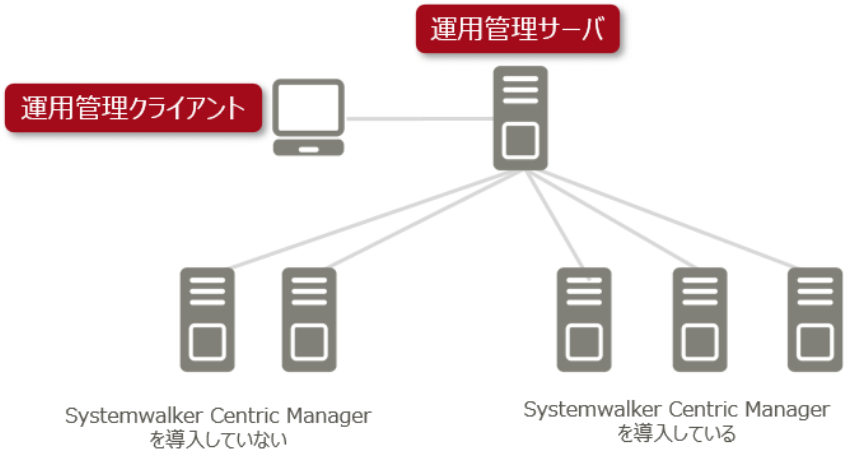
1.4.6　ライセンスとインストール種別の関係

購入したライセンスとインストールできる種別の関係は以下のとおりです。

ライセンス	インストール種別
マネージャ	運用管理サーバ
エージェント	部門管理サーバ
	業務サーバ
クライアント	運用管理クライアント
	クライアント
イベント監視エージェント	業務サーバ （イベント監視機能）
資源配付エージェント	業務サーバ （資源配付機能）
資源配付クライアント	運用管理クライアント （資源配付機能）
	クライアント （資源配付機能）

1.5　エージェントのインストール形態

運用管理サーバ、および部門管理サーバからは、Systemwalker Centric Managerのエージェントをインストールしているサーバとインストールしていないサーバの両方を監視することができます。



- インストール型エージェント監視

  運用管理者が被監視システムにSystemwalker Centric Managerをインストールして、運用管理サーバ/部門管理サーバからシステムを監視する形態です。

- インストールレス型エージェント監視

  運用管理者が被監視システムにSystemwalker Centric Managerをインストールすることなく、運用管理サーバ/部門管理サーバからシステムを監視する形態です。

  インストールレス型エージェント監視では、以下の2つの方式があります。

  ー 非デプロイ方式

  運用管理サーバ/部門管理サーバ上のインストールレス型エージェントが、被監視システムに対してSystemwalker Centric Managerのエージェント機能を配付することなく、被監視システムのOS機能を利用して監視を行います。

－ デプロイ方式

運用管理サーバ/部門管理サーバ上のインストールレス型エージェントが、被監視システムに対して自動でSystemwalker Centric Managerのエージェント機能を配付して監視を行います。非デプロイ方式よりも幅広い機能を利用できます。

1.6 運用形態

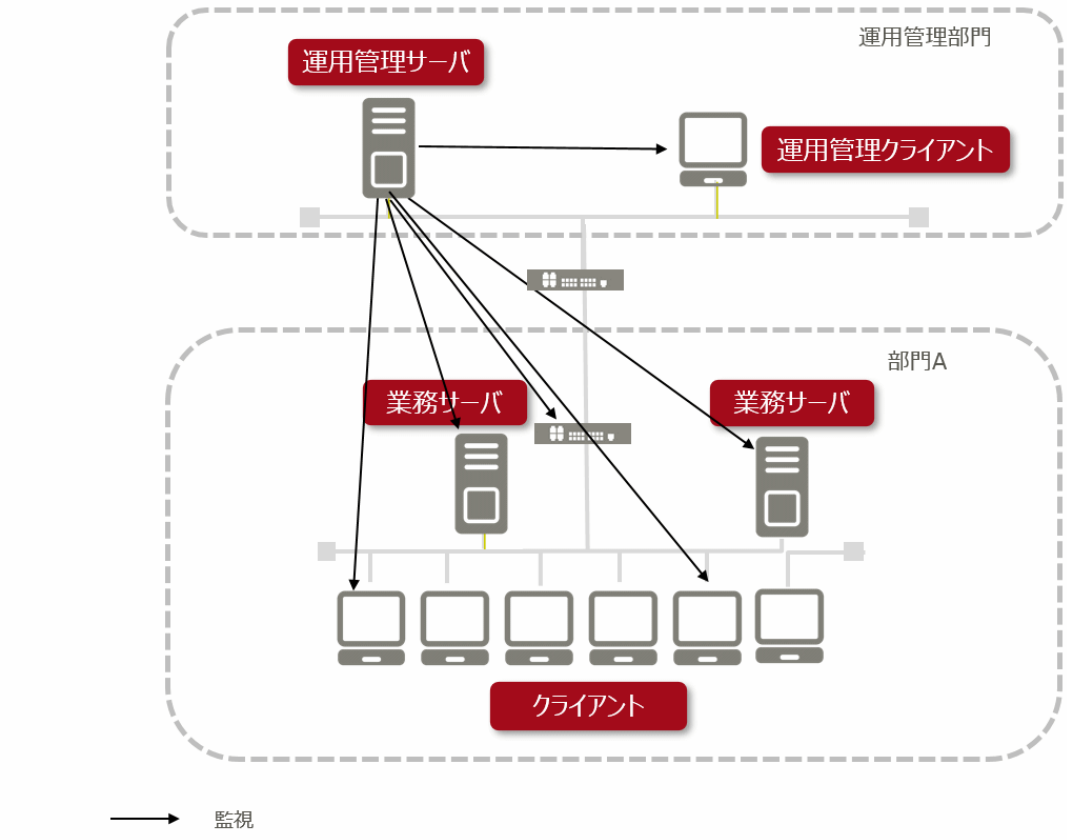
情報システムには、利用目的や規模などにより、さまざまな形態があります。Systemwalker Centric Managerは、多様な情報システムの運用形態に合わせて、さまざまな運用形態が可能です。ここでは、代表的な運用形態について説明します。

1.6.1 基本的な構成の運用形態

小規模なシステムの運用形態(2階層構成)

同一部門内のある管理対象の数が比較的小規模(数十台程度)なシステムの運用形態です。運用管理サーバから直接、監視対象のサーバを管理します。

図1.3 小規模なシステムの運用形態



大規模および分散しているシステムの運用形態(3階層構成)

以下のようなシステムの場合には、運用管理サーバの配下に、中継機能を持つ部門管理サーバを配置した運用形態をとることができます。

- 管理台数が多い(数千台規模)システムの場合

  スケーラビリティ向上のために、部門管理サーバを設置します。部門管理サーバが、配下の業務サーバの監視や収集した情報の集約・中継を行います。

- 分散している複数部門のサーバで構成されるシステムの場合

  ネットワークの負荷軽減のために、部門管理サーバを設置します。部門管理サーバが、配下の業務サーバの監視や収集した情報の集約・中継を行います。

- 企業内センタなどに複数のシステムを集約する場合(サーバ集約)

  運用管理業務の標準化や情報システム全体のコスト削減のために、企業内のセンタに、情報システムを集約して運用する形態です。

  同一の運用ポリシーを部門管理サーバおよび配下の業務サーバに適用できます。

  運用部門の作業分担や役割に合わせて、複数の運用管理サーバを束ねて、全体を管理するような運用管理サーバを設置する階層化形態をとることもできます。

以下のような場合にお勧めする構成です。

- LAN-WAN-LAN環境での監視(WANを経由して監視する)
- 監視対象部門内の監視対象ノード数が多く、トラフィック量を削減したい場合

部門管理サーバを設置することで、運用管理サーバと監視対象の部門間で発生する監視のためのトラフィックの削減、および運用管理サーバの負荷を分散することができます。

- 部門管理サーバを設置することで、以下を監視するために発生するトラフィックを削減できます。

  ー トラップの監視

  ー MIB監視

  ー 稼働状態の監視

  ー 性能監視

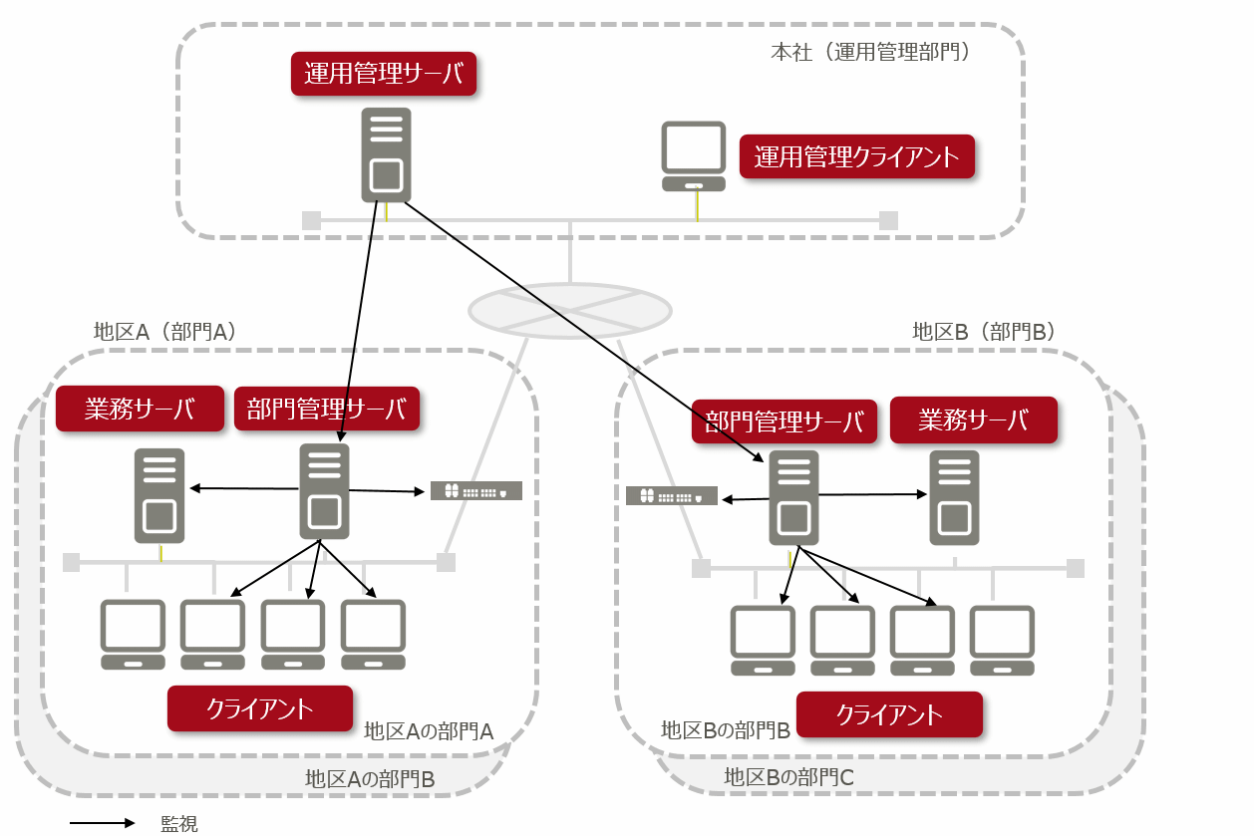
  各機能は、“ネットワーク/システムの監視”を参照してください。
  LAN-WAN-LAN環境で監視する場合でも、監視対象部門内に監視対象ノードが少なく、トラフィック量を削減する必要がない場合や、上記機能を使用しない場合は部門管理サーバを設置する必要はありません。

- 部門内の業務サーバで発生したイベントを、部門管理サーバを経由して運用管理サーバに通知することができます。

  このような運用では、運用管理サーバの移設などによりイベントの通知先を変更するときに、部門内の業務サーバの台数が多い場合でも、部門管理サーバの定義を変更するだけで運用が可能になります。しかし、部

門管理サーバがなんらかの原因でダウンした場合、部門内のイベントが運用管理サーバに通知されなくなりますので、注意が必要です。

図1.4 大規模および分散しているシステムの運用形態



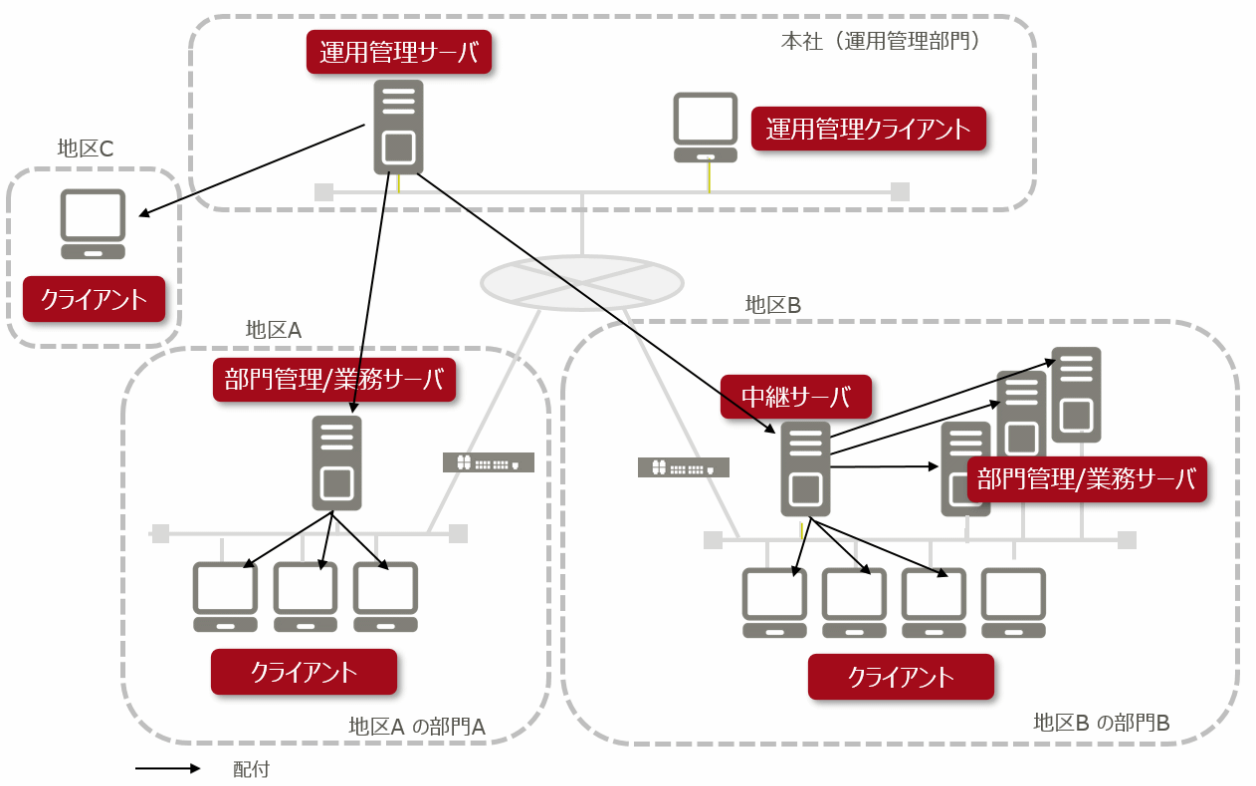
大規模なシステムの運用形態(ソフトウェア資源を階層的に配付する)

ソフトウェア資源を部門内のサーバやクライアントへ配付する構成は、監視する構成と別の構成にすることが可能です。管理対象の地区の数やサーバ、クライアントの数により、ネットワークやサーバへの負荷削減を考慮してさまざまな構成をとることができます。ソフトウェア資源を配付する機能については、“資源の配付”を参照してください。

“ソフトウェア資源を配付する場合の構成例”にソフトウェア資源を配付する場合の構成例を示します。

部門管理サーバまたは業務サーバ（エージェントライセンス、資源配付エージェントライセンス）を、ソフトウェア資源を中継して配付する中継サーバとして利用できます。
ソフトウェア資源を配付する場合、部門管理サーバと業務サーバの機能は同じです。

図1.5 ソフトウェア資源を配付する場合の構成例

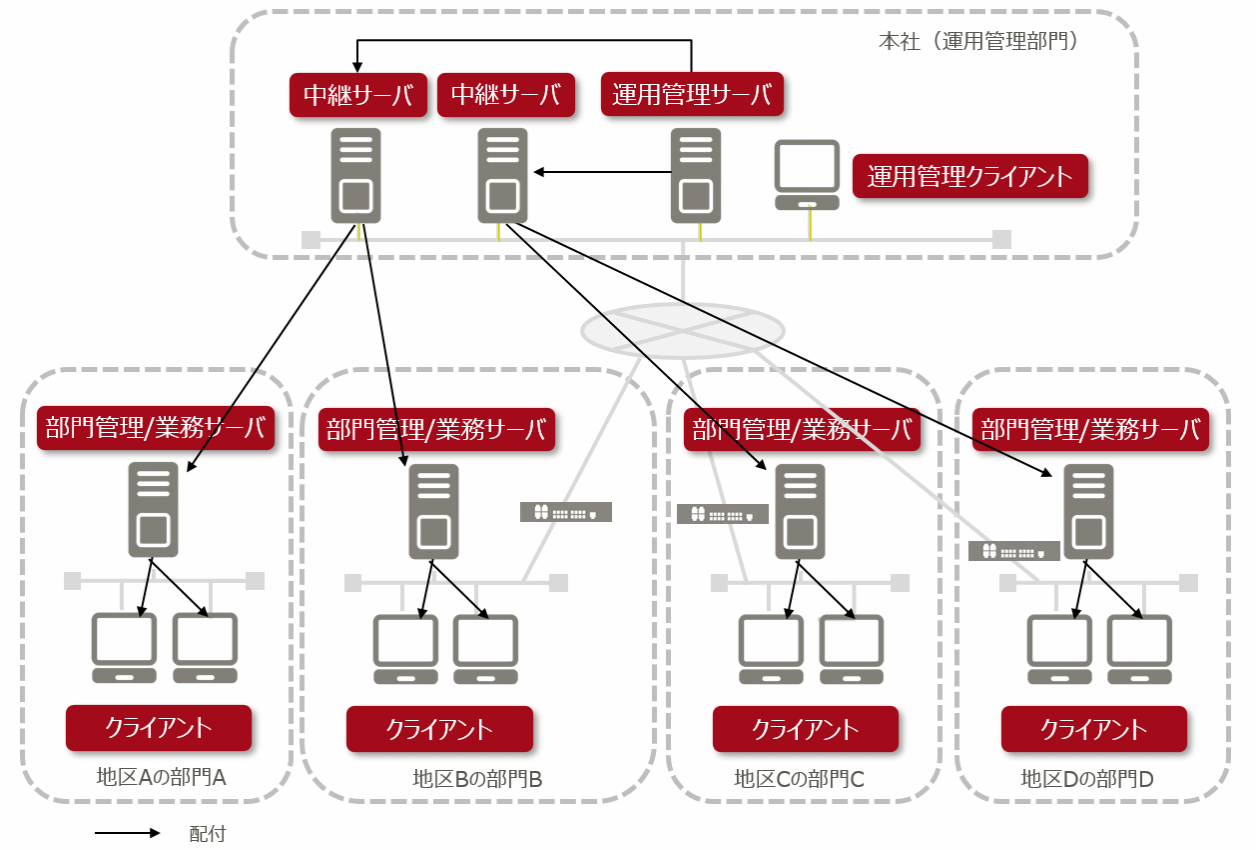


地区A：配付対象の部門管理/業務サーバ数が少ないので運用管理サーバから直接資源を配付します。
遠隔地のクライアントへは、RAS接続で資源を配付することも可能です。
地区B：配付対象の部門管理サーバが多いので部門内の中継サーバを中継し、部門内への資源を配付します。
地区C：配付対象がクライアントだけの部門は運用管理サーバから直接配付することができます。

また、配付先の部門数が多い場合に、運用管理サーバにかかる負荷を分散することも可能です。

“資源の配付先の部門数が多い場合の構成例”に、資源の配付先の部門数が多い場合の構成例を示します。

図1.6 資源の配付先の部門数が多い場合の構成例



地区A・地区B：配付先の部門数が多い場合、本社運用管理部門内の中継サーバを経由して資源を配付します。
運用管理サーバの負荷を削減できます。

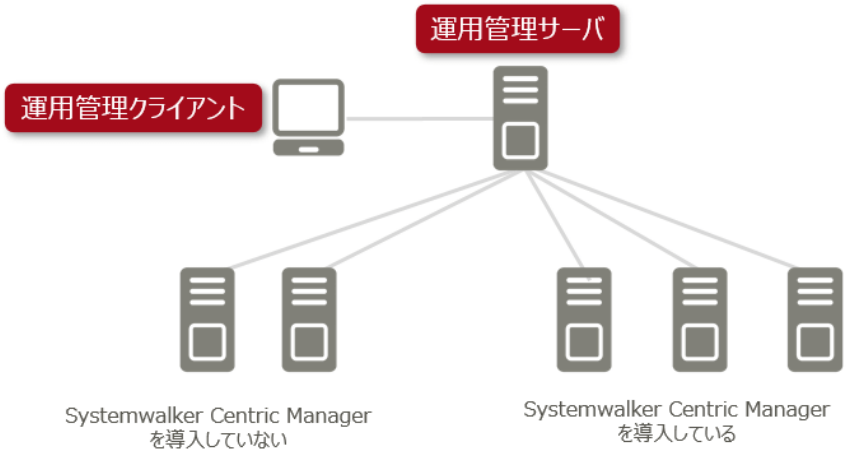
1.6.2　エージェントを導入しないでシステムを監視する

Systemwalker Centric Managerでは、インストールレス型エージェントにより、Systemwalker Centric Managerのエージェントを導入していないサーバも監視することができます。

これにより、Systemwalker Centric Managerのインストール、および設定にかかる運用管理コストを削減できます。

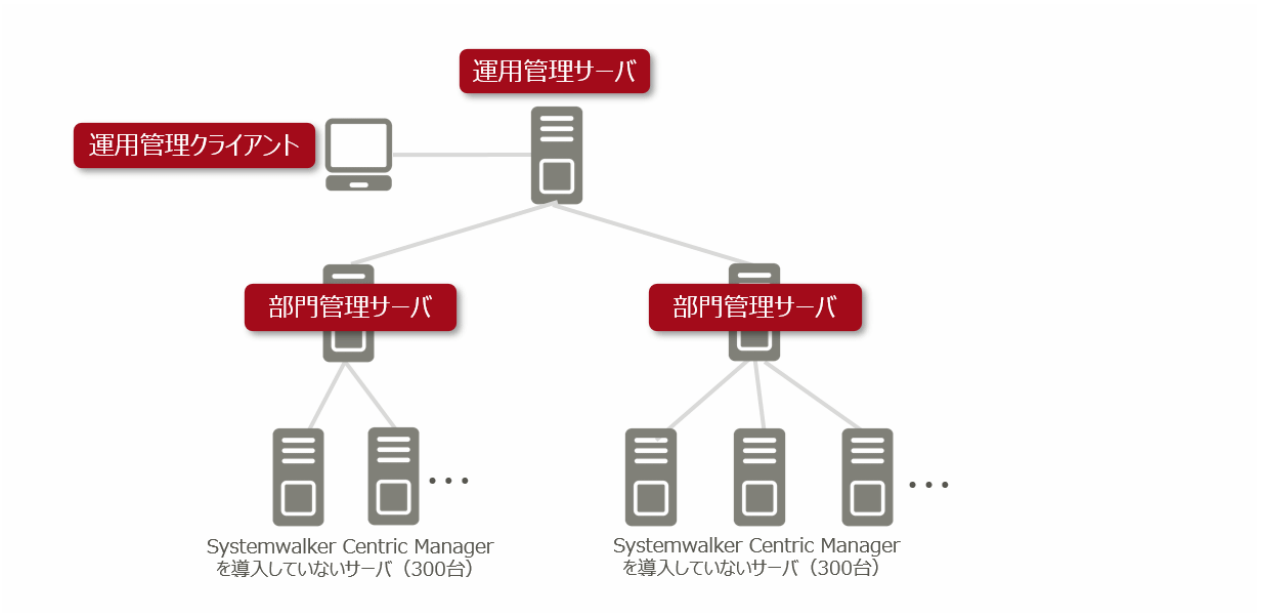
ここでは、運用管理サーバだけにSystemwalker Centric Managerをインストールし、運用管理サーバから直接、業務サーバを監視する運用例について説明します。

なお、Systemwalker Centric Managerのエージェントを導入していないサーバを監視する場合は、セキュリティの強化を考慮して、SSHで運用することを推奨します。



Systemwalker Centric Managerのエージェントを導入していない業務サーバが300台以上の構成の場合

1台の運用管理サーバで監視する、Systemwalker Centric Managerのエージェントを導入していない業務サーバが300台以上の構成の場合は、部門管理サーバを設置し3階層で監視します。

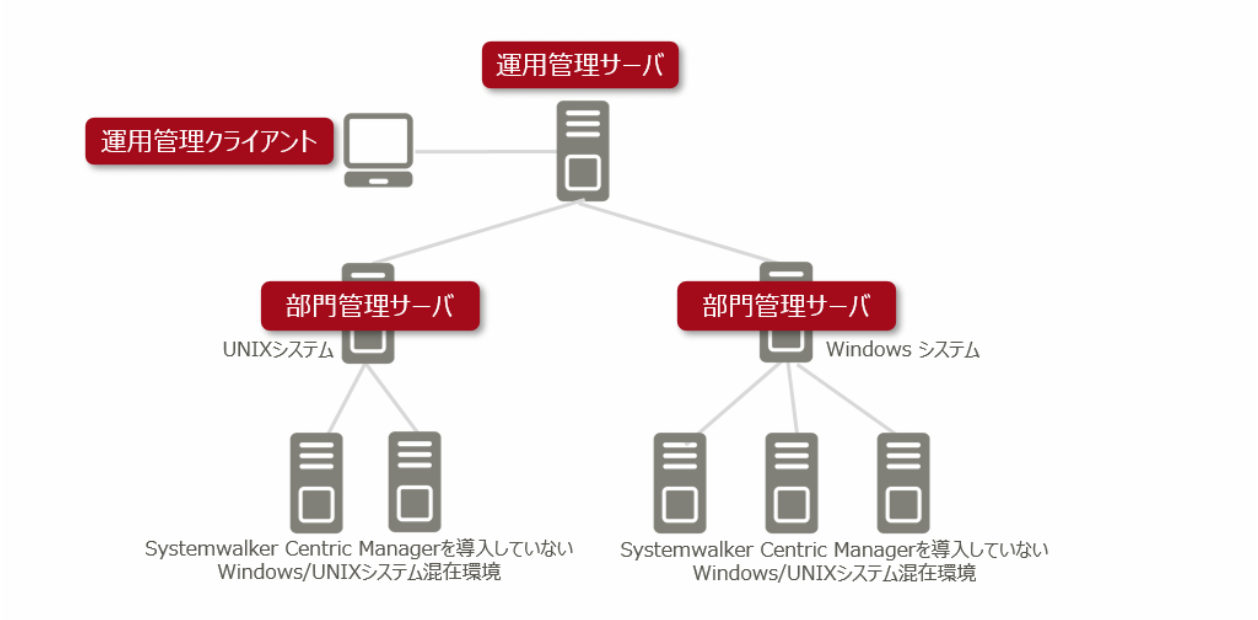


ノード一覧ツリー上で、Systemwalker Centric Managerが導入された業務サーバと同じように、エージェントを導入していない業務サーバを監視する部門管理サーバを配置します。

部門管理サーバとエージェントを導入していない業務サーバとの関係を明示する場合は、部門管理サーバごとに、エージェントを導入していない業務サーバをまとめて配置してください。

WindowsとUNIXの混在環境の場合

業務サーバがWindowsとUNIXが混在する環境においても1台の監視サーバで直接監視できます。



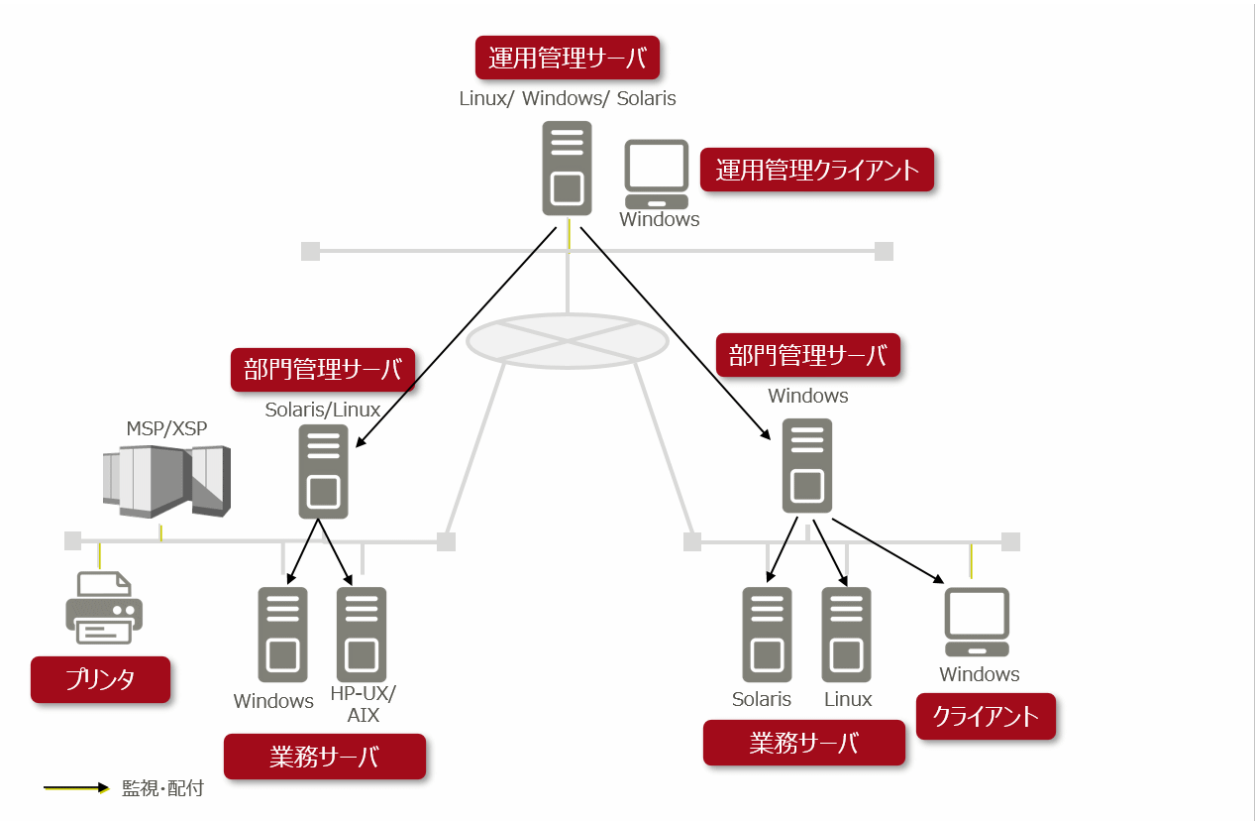
1.6.3　プラットフォームやバージョンが混在した形態

Systemwalker Centric Managerでは、さまざまなプラットフォームのシステムを混在させての構成が可能です。また、Systemwalker Centric Managerのバージョンが混在する環境も管理できます。このような混在した環境で、資源の配付や、異常の監視などの運用管理を行うことができます。

プラットフォームとバージョン混在時の接続性の詳細については、“バージョンの組み合わせ”を参照してください。

注意

Solaris版の運用管理サーバ・部門管理サーバは、Systemwalker Centric Manager V15.1.1までの提供です。



1.6.4 Virtual Machine(VM)環境のシステムを監視する

Systemwalker Centric Managerでは、Virtual Machine(VM)環境のシステムを監視することができます。

Virtual Machine(VM)環境のシステムを監視することで仮想化環境でのシステム監視を実現します。

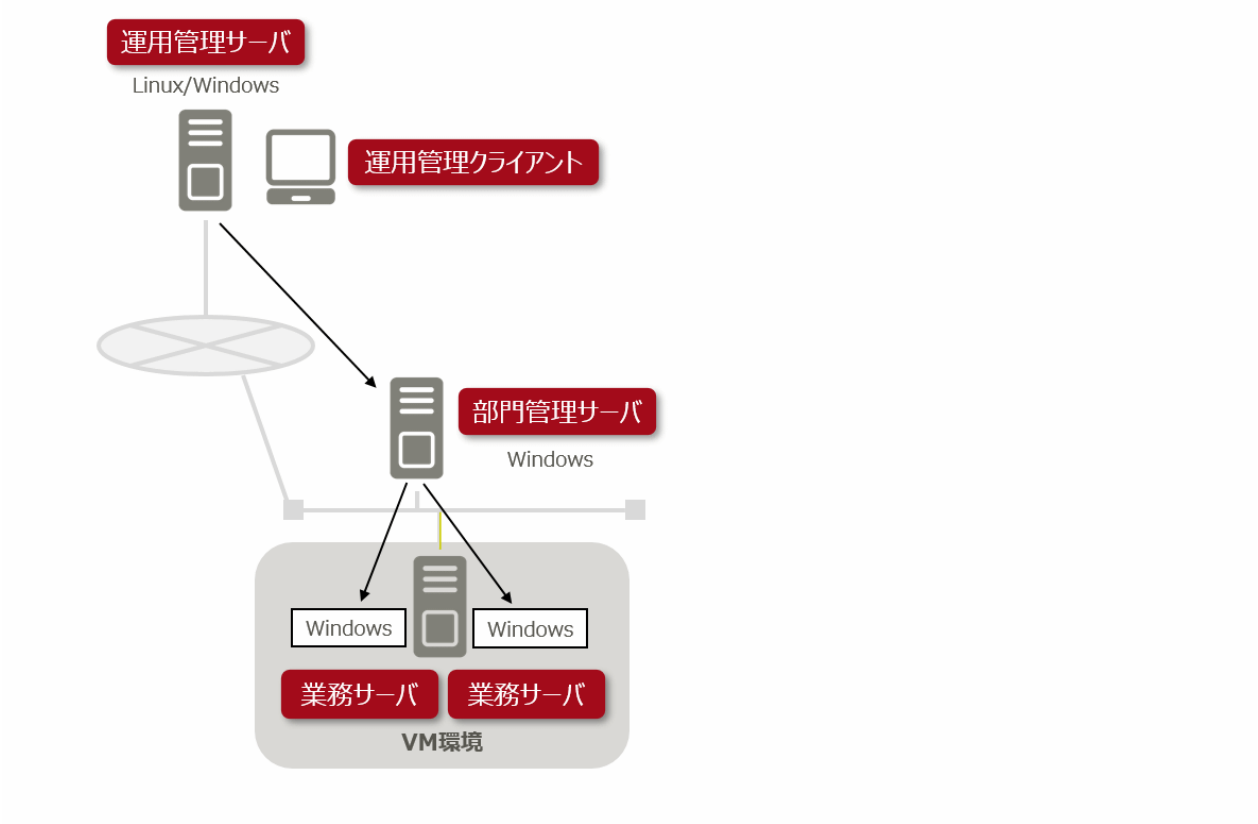
Systemwalker Centric ManagerでVM環境のシステムを監視する場合の運用例を以下に示します。

Virtual Machine環境

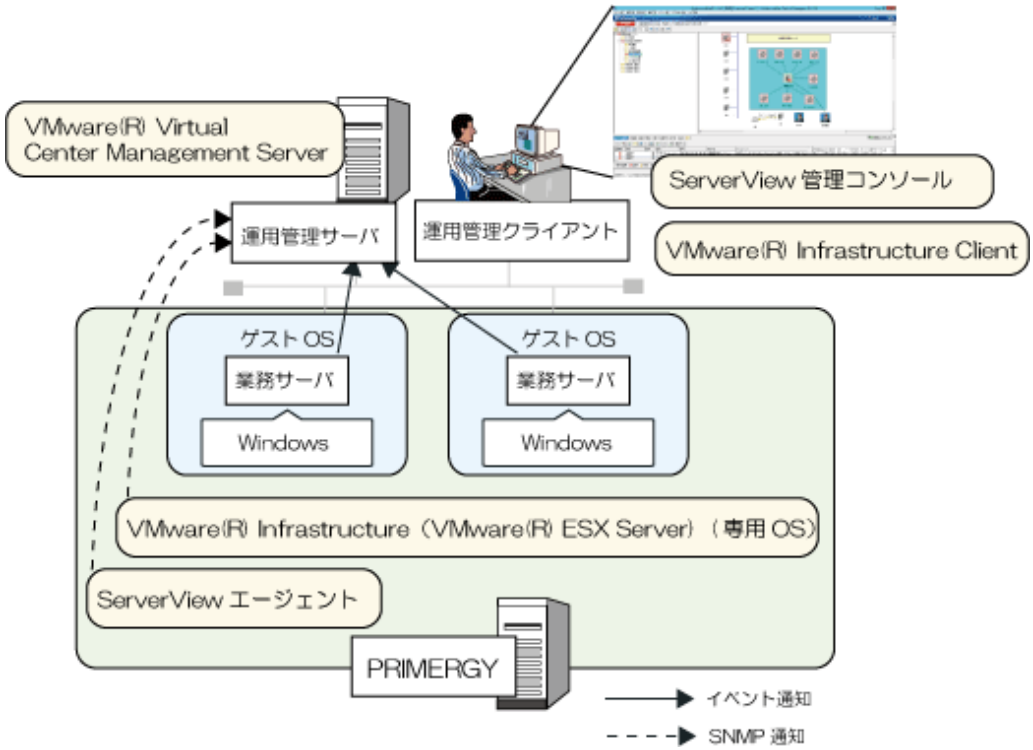
Systemwalker Centric Managerでは、Virtual Machine(VM)環境上で異なるプラットフォームのシステムを混在させた構成で、運用管理を行えます。

注意

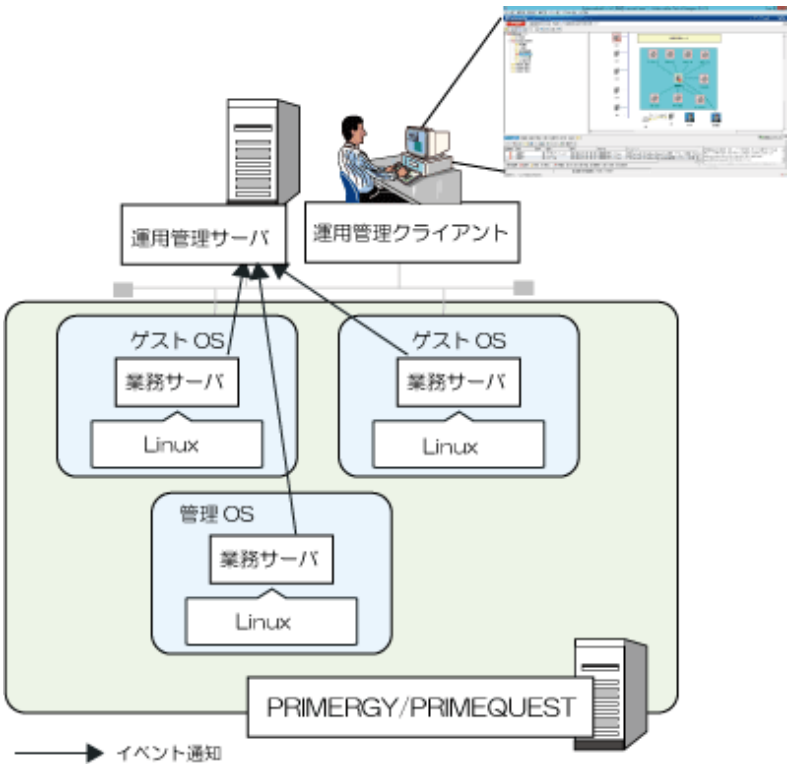
Solaris版の運用管理サーバ・部門管理サーバは、Systemwalker Centric Manager V15.1.1までの提供です。



VMware(R) Infrastructure 3の場合



PRIMEQUEST 仮想マシン機能/Linux 仮想マシン機能の場合



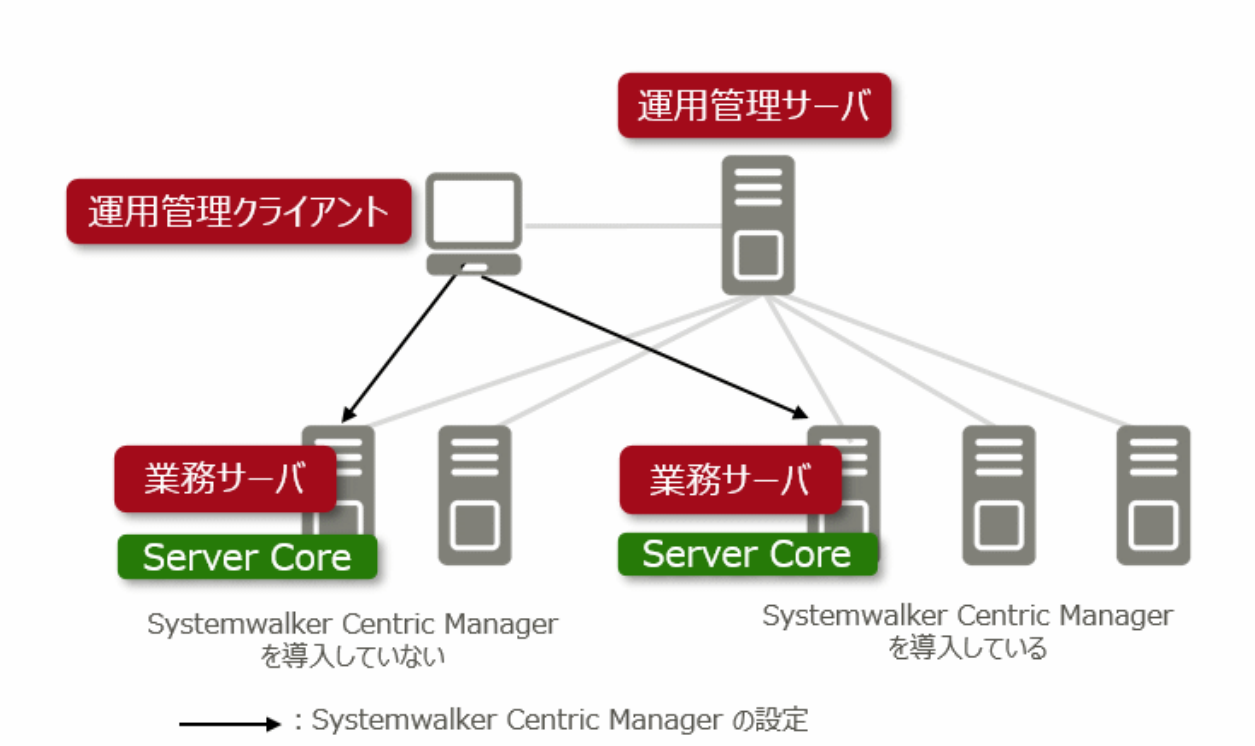
VM環境のシステムを監視する運用の詳細については、“Systemwalker Centric Manager PRIMERGY/PRIMEQUEST運用管理ガイド”を参照してください。

Hyper-Vを監視する場合は、“Systemwalker Centric Manager 使用手引書 監視機能編”を参照してください。

1.6.5 Server Core環境に導入する【Windows版】

Server Core環境にSystemwalker Centric Managerを導入して、Server Core環境での異常の監視やインベントリ情報の収集などを行うことができます。

Systemwalker Centric ManagerでServer Core環境を監視するシステム構成例を以下に示します。



Server Core環境にインストールできるインストール種別は、業務サーバだけです。

また、対応している購入ライセンスは、エージェント、イベント監視エージェント、および資源配付エージェントです。

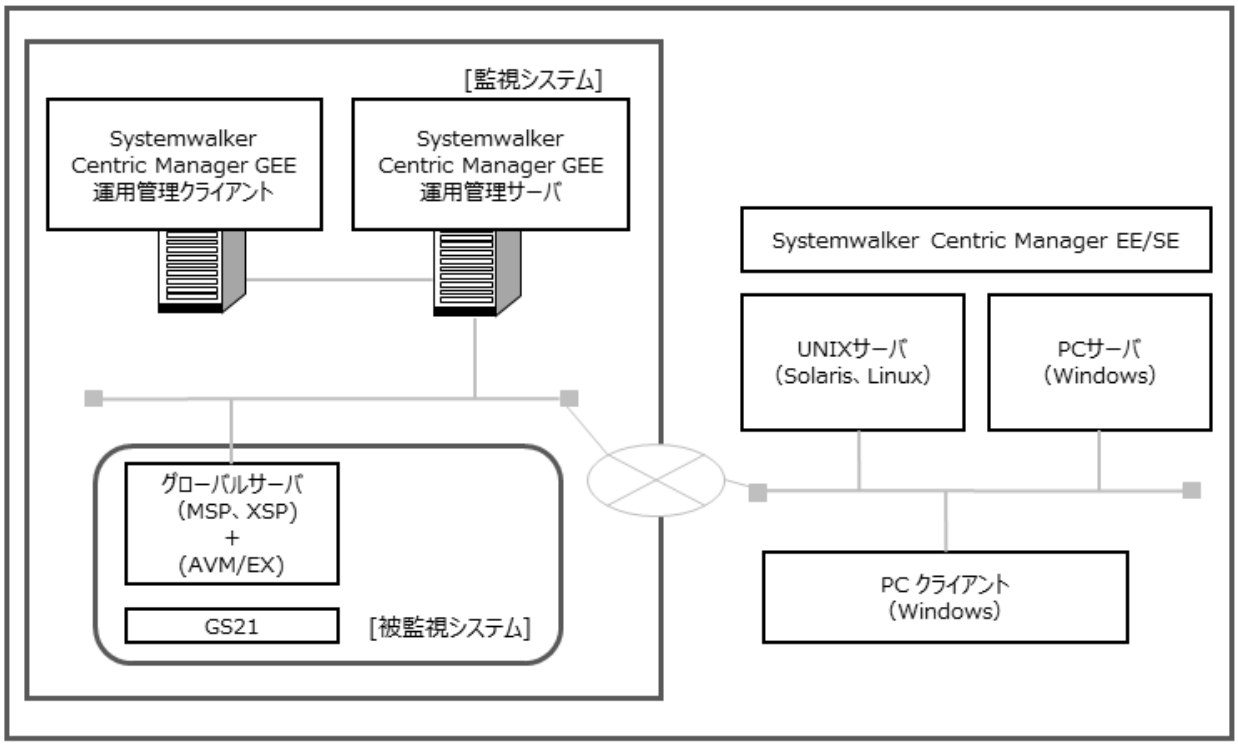
なお、オプション機能の[ドキュメント]は、Server Core 環境では利用できません。

Server Core環境の業務サーバの設定や、GUIからの操作を行う場合、運用管理クライアント、またはクライアントを配置してください。

GEE

1.6.6　グローバルサーバを監視する

Systemwalker Centric Manager GEEでは、グローバルサーバ、PRIMEFORCE を含むシステム構成を監視することができます。



グローバルサーバ、PRIMEFORCE を含むシステムを監視・操作する方法については、“Systemwalker Centric Manager 使用手引書 グローバルサーバ運用管理ガイド”を参照してください。

UNIXシステム、およびWindowsシステムを監視する

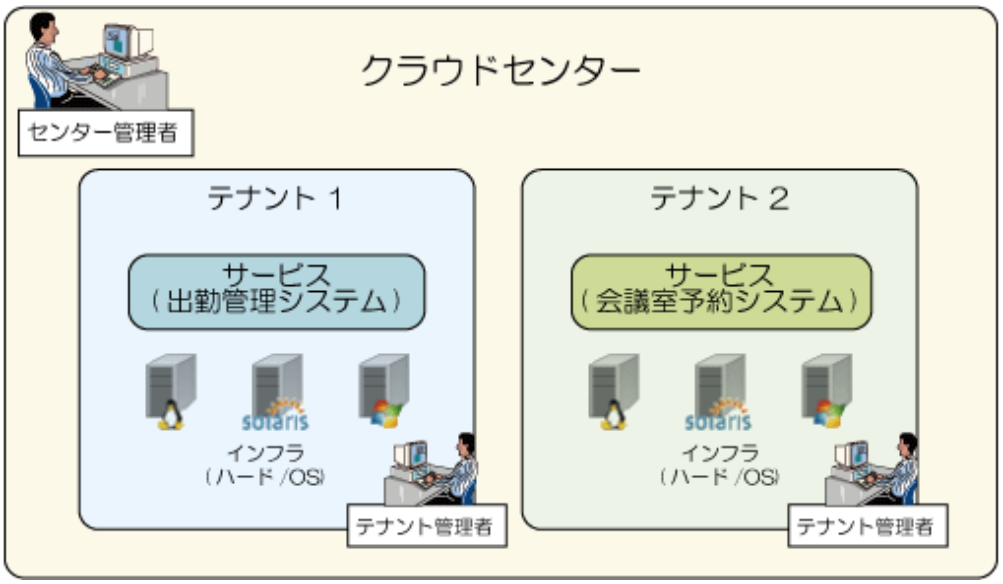
Systemwalker Centric Manager GEEは、TCP/IPネットワーク上のUNIXシステムやWindowsシステムを監視・操作することができます。UNIXシステムやWindowsシステムを監視・操作する方法については、Systemwalker Centric Managerの各マニュアル、および“Systemwalker Centric Manager オンラインヘルプ”を参照してください。

1.6.7 マルチテナントにおける監視

通常の運用では、センター全体の管理者（Systemwalker Centric Manager の更新権ユーザー）がすべての運用設定をします。

プライベートクラウドでは、テナント（特定の監視ノード、アプリケーションの集まり）ごとに個別の運用/監視を行う場合があります。マルチテナント運用時の設定を行うことで、テナントごとに管理者（Systemwalker Centric Manager の操作権ユーザー）がテナント個別の運用/監視を行えるようになります。

マルチテナント環境における監視設定については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“マルチテナント環境を監視する”を参照してください。



1.6.8 Nano Serverを監視する

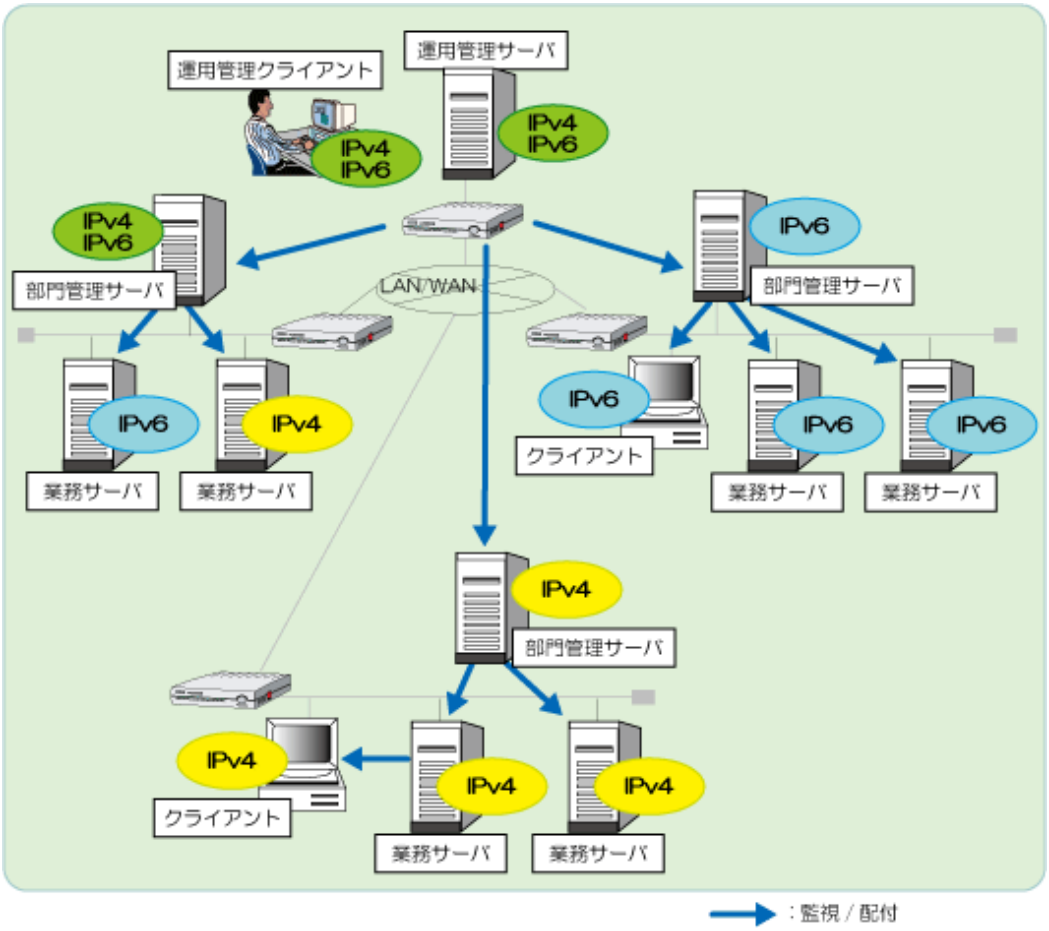
Systemwalker Centric Managerでは、インストールレス型エージェント（非デプロイ方式）でNano Serverを監視することができます。

1.6.9 IPバージョンが混在した形態

Systemwalker Centric Managerでは、さまざまなIPバージョンのシステムか混在するシステムを監視・管理することができます。

IPバージョンが混在した運用形態

以下の図のようなIPバージョンが混在した環境で、資源の配付や、異常の監視などの運用管理を行うことができます。



ポイント

- IPv4、IPv6、IPv4/IPv6デュアルスタック環境で動作できます。

  ただし、運用管理サーバと運用管理クライアントをIPv6環境で動作させる場合は、IPv4インタフェースを無効にしないでください。

  また、部門管理サーバ、業務サーバ、クライアントにおいても、IPv6シングルスタック環境で運用する場合、IPv4をアンインストールする以下の操作は、実施しないでください。【Windows版】

  ー IPv4をアンインストールするコマンド

  ```
  netsh interface ipv4 uninstall
  ```

  IPv4のアンインストールを実施してしまった場合は、再度IPv4のインストールを実施してください。

  ー IPv4をインストールするコマンド

  ```
  netsh interface ipv4 install
  ```

- IPv6のシステムで運用管理を行う場合の注意事項については、“Systemwalker Centric Manager 導入手引書”の“IPv6運用の注意事項”を参照してください。

1.6.10　その他の運用形態

Systemwalker Centric Managerでは、そのほかにも以下のような運用形態をサポートしています。

- 高信頼システムを管理する(クラスタシステムの監視)
- 公開ゾーン(DMZ)を管理する

- 管理サーバの信頼性を高くする(管理サーバのクラスタ化、二重化)
- 多階層で管理する(全体監視)
- アウトソーシング
- Systemwalker Centric Managerを導入しないコンピュータを監視する

第2章 機能の説明

Systemwalker Centric Managerの機能を説明します。

2.1 コンソール

Systemwalker Centric Managerの運用管理作業は、統合されたメインコンソールから行うことができます。管理者は、以下のコンソール画面を使い、利用形態に合わせた管理作業を行うことができます。

- Systemwalkerコンソール
- SystemwalkerWebコンソール
  - Systemwalker Webコンソール
  - Systemwalker Webコンソール(互換)
- Systemwalker Webコンソール(モバイル版)

2.1.1 Systemwalkerコンソール

Systemwalkerコンソールを使用して、監視から復旧操作まで、業務のライフサイクルに従った管理を行うことができます。また、他ソフトウェアとのシームレスな連携により、運用管理操作をスムーズに行うことができます。

使用できる機能

本コンソールでは、業務の視点で以下の作業が可能です。

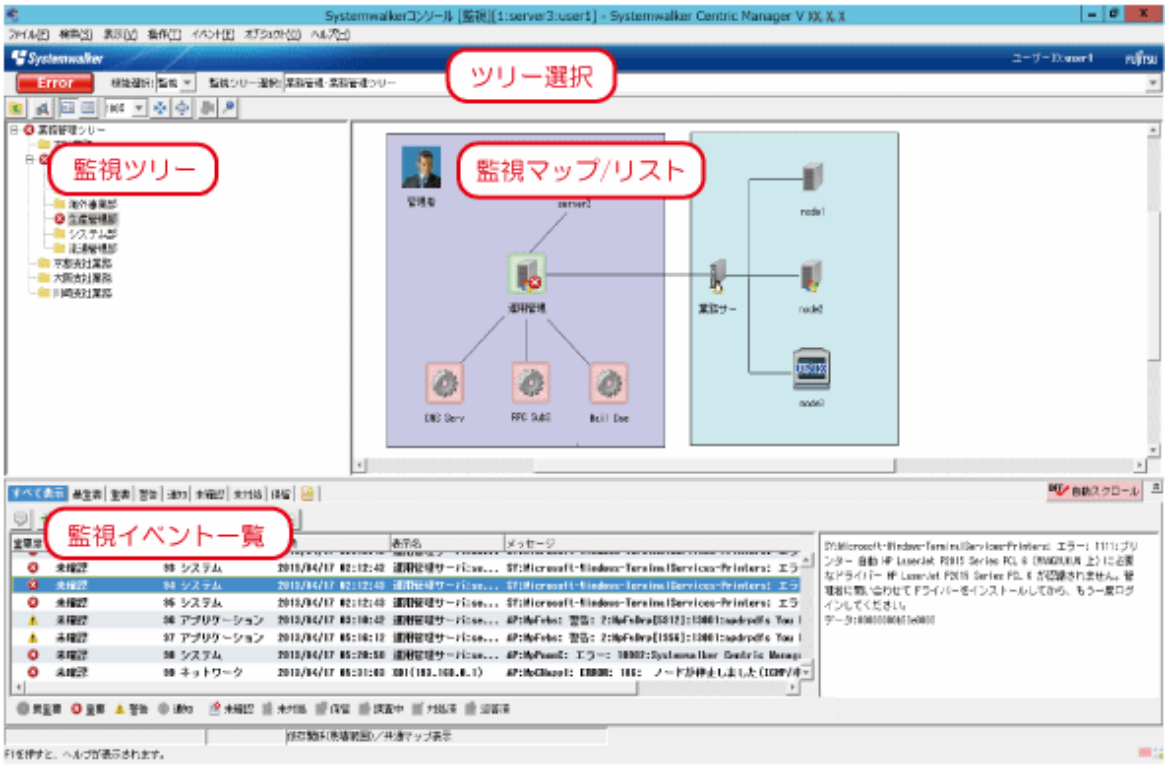
- 資源配付
  - 資源配付ポリシーの設定と配付
  - 資源の配付と配付状況の表示
  - インベントリ情報の収集と表示
- 監視
  - 監視用のポリシーの設定と配付
  - ネットワーク/システムの障害の監視(MIB監視/イベント監視)および対処
  - ネットワーク/システムの性能の監視(性能監視)
  - 業務の稼働状況の監視(アプリケーション管理)
  - Webサービスの稼働監視
  - IPv6インタフェースの稼働監視
- 障害復旧
  - 影響範囲の把握
  - 監視画面からアプリケーションを起動するなどの復旧操作

Systemwalkerコンソールは、次の環境で表示できます。

- UNIX版Systemwalker Centric Manager
  運用管理クライアント
- Windows版Systemwalker Centric Manager
  運用管理サーバ、および、運用管理クライアント

画面例

以下に、Systemwalkerコンソールの画面例と構成するサブウィンドウの名称を以下に示します。



「監視マップ」について

複数のサブネットワークを持つネットワーク全体の構成を把握し、ネットワークに接続されたルータやワークステーションなどのノードの監視を行います。インストールした直後の起動では、ローカルネットワークに対して自動的にノード検出を行います。ネットワークに接続されているクライアントやルータなどのノードを自動認識し、ネットワークの階層に応じた、正確なネットワーク構成図(監視マップ)を自動的に作成します。また、LAN、WAN経由のリモートLANを管理することができます。

監視マップの背景には、地図や写真、オフィスレイアウトなどを設定し、実務に近いノードアイコンを利用することで、実際の運用環境を画面上に展開することができます。新しくノードが追加された場合でも、新ノード検出によって速やかに監視マップに反映できます。また、ノードの設置場所を移動した場合でも、アイコンの削除や移動によって、監視マップを自由に変更することができます。

システム管理者は、この監視マップからネットワークの構成、ノードの状態を監視することができます。

「監視ツリー」について

ネットワークの構成が、多階層のツリー構造で画面上に表示されます。監視ツリーをクリックすると、下位階層が表示されます。監視マップには、そのサブネットワーク配下のノードが、ノードアイコンとして表示されます。

ネットワークおよびノードに対するアイコンは、自由に割り当てることができ、利用者が作成したアイコンを表示することができます。また、監視マップには、背景画を入れることができます。

業務とは

Systemwalker Centric Managerでは、監視対象のノードやアプリケーションなどを管理者が監視する単位でグループ化したものを業務といいます。
業務を構成するシステム、ネットワーク、アプリケーションなどをオブジェクトと呼び、業務は以下のオブジェクトと関連する項目で構成されます。

- システムやネットワークのノード
- アプリケーション
- データベース
- ほかの業務(別に定義した業務)

- 管理者
- ワークユニット(Interstage上で作成された業務)
- IJServerクラスタ(Interstage上で作成された業務)

障害の影響範囲の把握と復旧処理

Systemwalkerコンソールを使用すると、業務を構成するオブジェクトを業務単位で監視できます。業務単位で監視することにより、異常が発生したとき、どの業務に影響があるのかを、以下のように簡単に把握し、適切に対処できます。

- システムやネットワークなどで異常が発生すると、影響を受ける業務が、異常として監視画面に通知されます。異常が通知された業務を選択し、どのオブジェクトが異常の原因かを調査することができます。
- 異常発生時の影響度を把握し、適切な優先度で復旧処理を行います。

さらに、異常が発生したシステムやネットワーク、アプリケーションに関連して、影響を受けるシステムやネットワーク、アプリケーションなどを把握できます。あらかじめシステムやネットワーク、アプリケーションなどの関係を定義しておくことにより、異常が発生して影響を受ける範囲と、影響度が監視画面に表示されます。影響度が確認しやすくなり、障害復旧作業の優先度を判断することができます。
影響度は以下のように表示されます。

- イベントが発生したオブジェクト
- 重大な影響があるオブジェクト
- 軽度の影響があるオブジェクト

システムやネットワーク、アプリケーションなどで異常が発生したとき、Systemwalkerコンソールだけでなく、アクション定義などにより管理者にいろいろな方法で異常を通知することができます。

- 対象業務の管理者として定義された人へ、イベントの内容を通知することができます。
- 管理者への通知は、E-mailなどで行うことができます。

詳細については“業務の監視”を参照してください。

2.1.2 Systemwalker Webコンソール

Systemwalker Webコンソールは、WWW(World Wide Web)ブラウザからSystemwalker Centric Managerの機能を使用する場合に使用します。リバースプロキシを使用することにより、イントラネット外からもSystemwalker Webコンソールを使用することができます。

管理者は監視イベントの通知を電子メールなどで受け付け、遠隔地(出張先など)でイベントの一覧を参照できます。

Systemwalker Webコンソールには、以下の2つがあります。

- Systemwalker Webコンソール
- Systemwalker Webコンソール(互換)

Systemwalker Webコンソール

Systemwalker Webコンソールの[ポータル]画面には、監視イベント情報が表やグラフで視覚的に表示されるため、監視対象全体の状況をすばやく把握することができます。

使用できる機能

Systemwalker Webコンソールからは、Systemwalker Centric Managerの以下の機能を利用することができます。

なお、コンソール操作制御運用時にはSystemwalker Webコンソールから監視機能を利用できません。

- 監視
  - ネットワーク/システムの障害の監視(MIB情報取得/イベント監視)および対処

- 業務の監視

Web連携機能を使用する場合は、“Systemwalker Centric Manager 導入手引書”の“Web連携機能を使用する場合”を参照してください。

画面例

以下に、Systemwalker Webコンソールの画面例を示します。

- [ポータル]画面

  監視イベント情報を集計した情報が表やグラフにまとめたノードのサマリ情報が表示されます。



Systemwalker Webコンソール(互換)

Systemwalker Web連携で使用するコンソールです。

なお、Systemwalker Webコンソール(互換)では、監視状況の表示が利用できないため、Systemwalker Webコンソールを使用することを推奨します。

使用できる機能

Systemwalker Webコンソール(互換)からは以下の機能を利用することができます。なお、コンソール操作制御運用時にはSystemwalker Webコンソール(互換)は使用できません。

- 監視
  - ネットワーク/システムの障害の監視(MIB情報取得/イベント監視)および対処
  - 業務の監視

また、Systemwalker Web連携機能では、以下の機能を利用することができます。

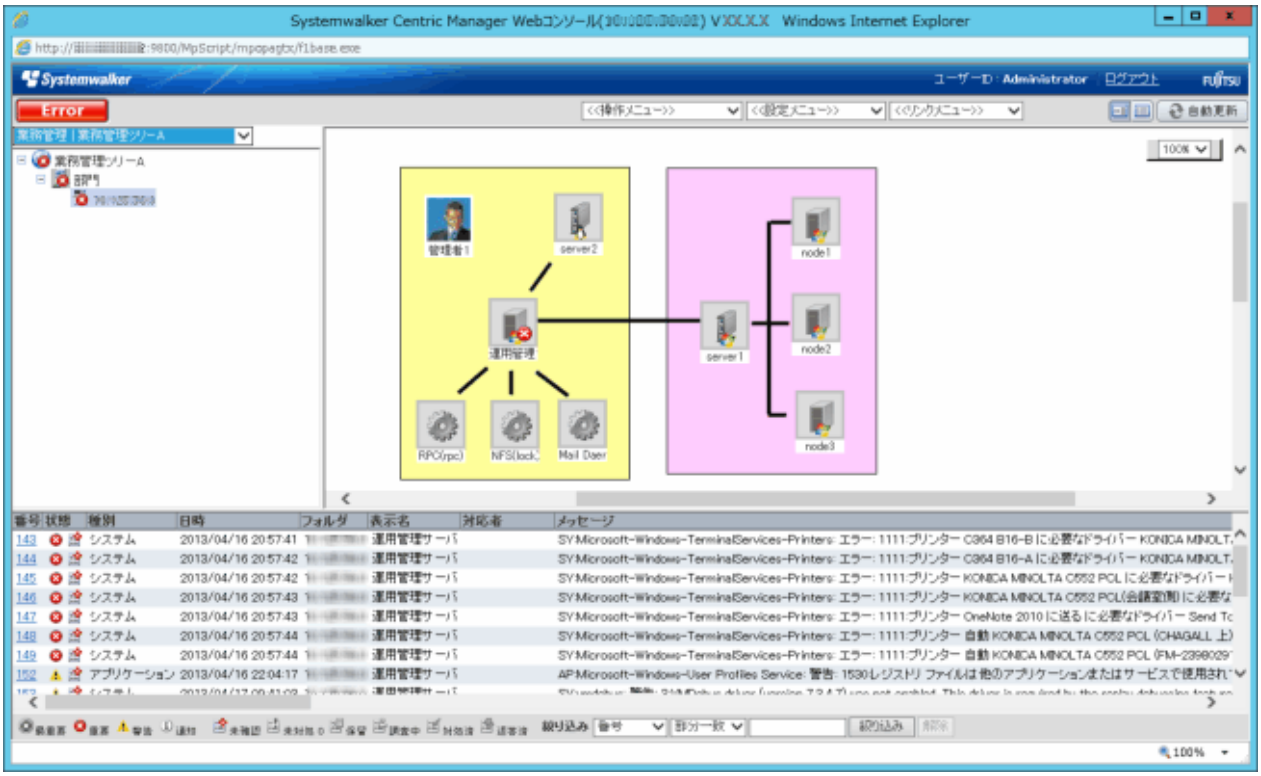
- 資源の配付
  - 資源の配付状況の表示

－ インベントリ情報の表示

Web連携機能を使用する場合は、“Systemwalker Centric Manager 導入手引書”の“Web連携機能を使用する場合”を参照してください。

画面例

以下に、Systemwalker Webコンソール(互換)の画面例を示します。



ポイント

イントラネット外からSystemwalker Centric Managerに接続する場合

運用管理サーバをイントラネット内に作成し、リバースプロキシを使用して安全を確保します。これにより、IPアドレスが漏れるなどの心配が不要になります。

2.1.3 Systemwalker Webコンソール(モバイル版)

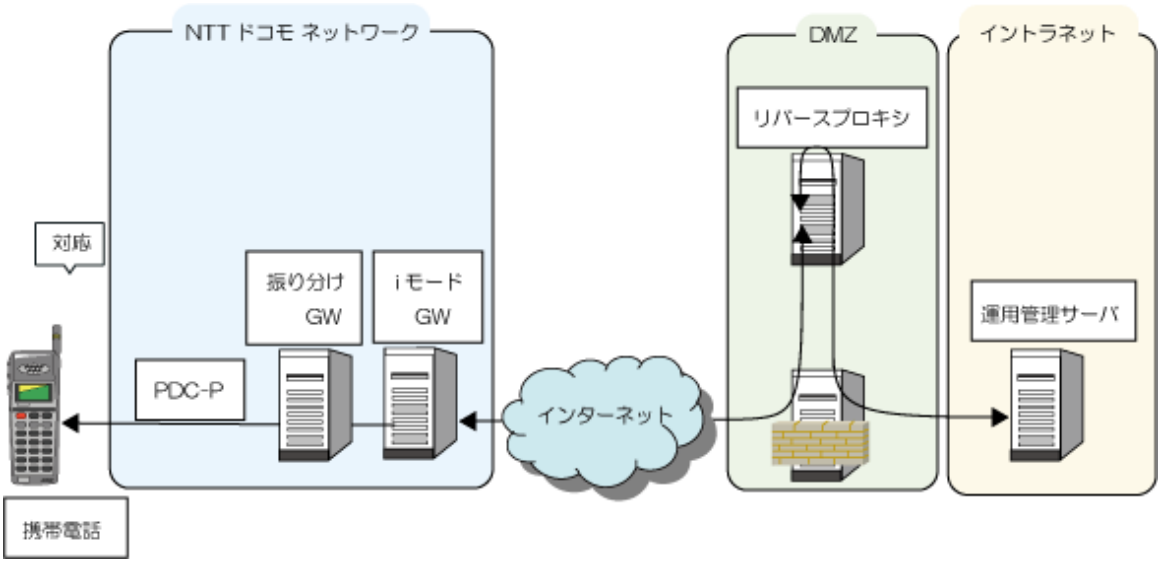
Systemwalker Webコンソール(モバイル版)は、イントラネット外からSystemwalker Centric Managerの機能を使用する場合に使用します。

次のような機器をモバイル端末として使用できます。

- iモード対応の携帯電話
- PalmOSを搭載したPDA

なお、コンソール操作制御運用時にはSystemwalker Webコンソール（モバイル版）は使用できません。

Systemwalker Webコンソール(モバイル版)を使用する場合の運用形態を以下に示します。



注意

インターネット環境で使用する場合の注意事項

Systemwalker Webコンソール(モバイル版)をインターネット環境で使用する場合は、運用管理サーバをインターネットから安全に参照できるセキュリティレベルを確保してください。

詳細については“Systemwalker Centric Manager 導入手引書”の“インターネット環境でのSystemwalker Webコンソール(モバイル版)の設定”を参照してください。

使用できる機能

管理者は、監視イベントの通知をiモード対応の携帯電話などで受け付け、遠隔地で以下の機能を利用することができます。

- イベント監視
  - イベント一覧の表示
  - 監視イベント絞り込み
  - 監視イベントへの対処
  - リモートコマンドの発行

モバイル対応時の安全性について

運用管理サーバは、イントラネット内に作成し、リバースプロキシを使用して安全を確保します。これにより、IPアドレスが漏れるなどの心配を不要にしています。

画面例

- iモード対応の携帯電話で表示したSystemwalker Webコンソール(モバイル版)の画面例



- PalmOSを搭載したPDAで表示したSystemwalker Webコンソール(モバイル版)の画面例



2.2　セキュリティ

Systemwalker Centric Managerのセキュリティ機能について説明します。

はじめに、“Systemwalkerセキュリティ指針”を説明し、Systemwalker Centric Managerの各機能について説明します。

- Systemwalkerセキュリティ指針
- Systemwalkerコンソールの操作を制御する
- サーバの利用を制御する
- 監査ログを管理/分析する

2.2.1 Systemwalkerセキュリティ指針

2.2.1.1 セキュリティとは

インターネットに代表されるコンピュータネットワークの発達により、企業内はもちろん、さまざまな場所から企業内ネットワークにアクセスが可能となっています。利便性が向上した反面、不正アクセスや情報漏洩といったセキュリティ上の問題も深刻になってきました。

セキュリティとは「安全」や「危険、危害といった安全を脅かすもの（脅威）に対する防衛」の意味です。セキュリティの脅威は、大きく以下のように分類されます。

分類		脅威の具体例
偶発的脅威	天災	地震、落雷、火事など
	故障	ハードウェア障害、ソフトウェア障害など
	誤操作	運用ミス、接続間違いなど
意図的脅威	第三者の悪意ある行為	不正アクセス、なりすましなど
	関係者の悪意ある行為	パスワードの漏洩、顧客情報の暴露など

2.2.1.2 セキュリティの要件

セキュリティを確保するための要件として以下の3つがあります。

- 機密性

  アクセス許可されている情報以外は絶対に見えないようにすること。

- 完全性

  情報が常に完全な形で保たれており、意図的、または偶発的な不正によって改ざんされないこと。

- 可用性

  システムの資源や保存されている情報がいつでも利用できること。

これらの要件が満たされなくなることにより、脅威が発生します。

要件の喪失	具体的脅威
機密性の喪失	管理者権限が必要な操作が管理者権限を持たない担当者によって利用される、など。
完全性の喪失	管理用の定義データが何者かによって不正に改ざんされる、など。
可用性の喪失	システム異常により大量の監視イベントが発生し、ディスク資源やネットワーク資源が枯渇する、など。

2.2.1.3 セキュリティ対策

セキュリティの要件が満たされなくなることによって脅威が発生します。したがって、セキュリティを確保するためには、セキュリティの要件を満たすような対策を講じる必要があります。

アクセス制御（機密性を満たすための対策）

アクセス制御では、利用者(ユーザ)の管理、利用者(ユーザ)の権限の管理が必要です。

Systemwalker管理者アカウントについて(UNIX)

Systemwalker管理者アカウントをインストール前にあらかじめ作成する必要があります。Systemwalker管理者アカウント作成の際には破られにくいパスワードの設定を行ってください。また、漏洩しないようにパスワードの管理を厳重に行ってください。

Systemwalker Centric Managerの利用者とロールについて

Systemwalker Centric Managerの利用者は運用管理者です。運用管理者は、システム管理者(UNIXではroot、WindowsではAdministratorsグループに所属するユーザ)とシステムの異常を監視する監視担当者、プログラムやデータなどのシステム資源の配付を行う配付担当者に分類されます。

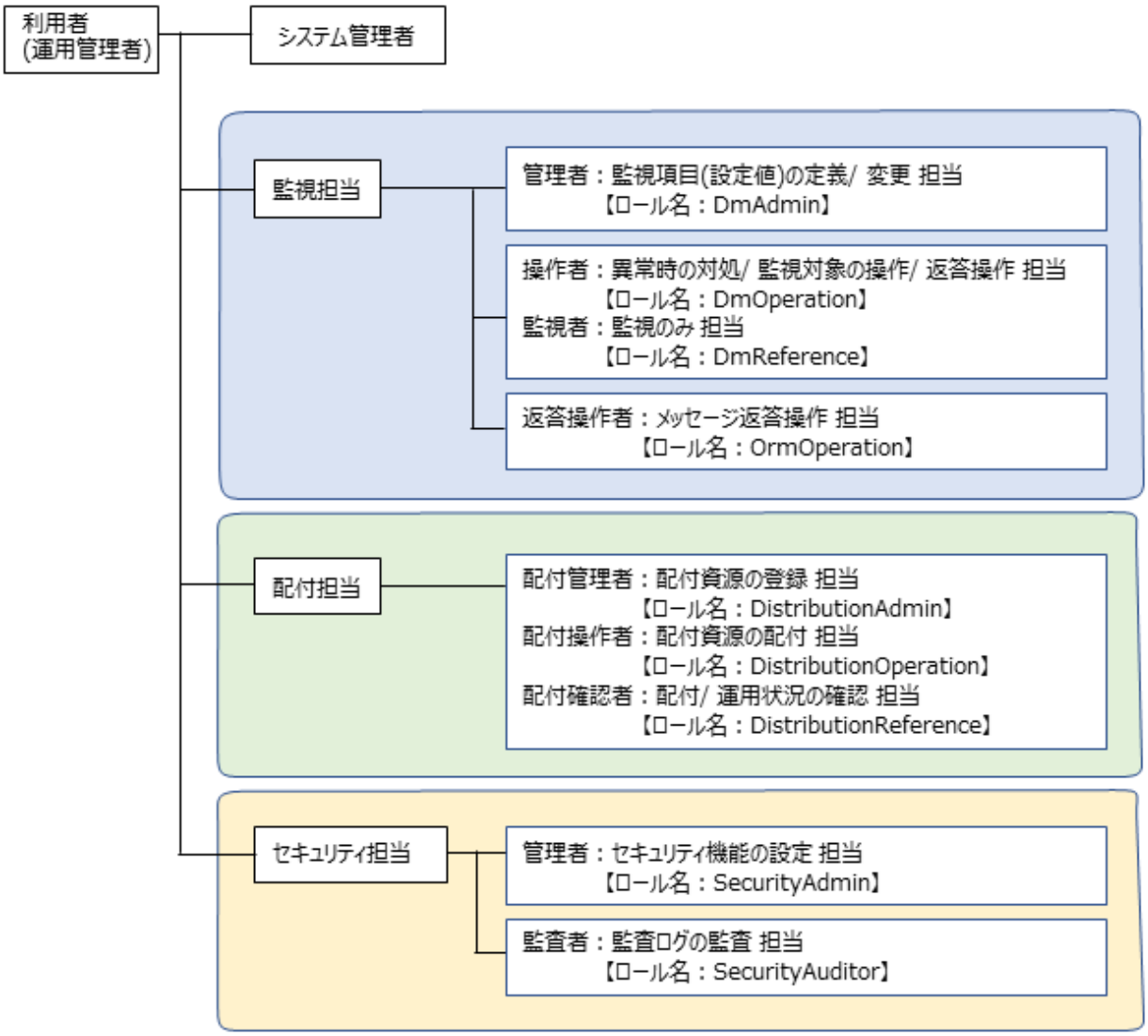
Systemwalker Centric Managerは、ロールという単位で各機能の利用権限を定義しています。ロールとは、共通の役割(権限)を持つ利用者から構成するグループのことです。Systemwalker Centric Managerをインストールすると、以下のロールが登録されます。

ロール名	説明	使用機能
DmAdmin	監視機能の管理系ロール	Systemwalkerコンソール リモート操作(注)
DmOperation	監視機能の操作系ロール	
DmReference	監視機能の参照系ロール	
DistributionAdmin	資源配付の管理系ロール	資源配付
DistributionOperation	資源配付の操作系ロール	
DistributionReference	資源配付の参照系ロール	
OrmOperation	返答機能の操作系ロール	返答操作のコマンド
SecurityAdmin	セキュリティの管理者	Systemwalkerコンソール 監査ログ管理 サーバアクセス制御
SecurityAuditor	セキュリティの監査者	Systemwalkerコンソール 監査ログ管理 サーバアクセス制御 監査ログ分析

注)

「クライアント」以外のインストール種別でインストールした場合にロール設定が必要です。

Systemwalker Centric Managerの利用者(運用管理者)とロールの関係を以下に示します。



所属させるロールの種類により、ユーザが使用できる機能と利用権限が決まります。

システム管理者は、運用管理者を上記のロールに適宜所属させてください。

また、監視担当の管理者(DmAdmin)は監視用のロールと返答機能の操作系ロールに利用者を登録することができます。

配付担当の管理者(DistributionAdmin)は配付用のロールに利用者を登録することができます。

セキュリティ担当の管理者(SecurityAdmin)はセキュリティ用のロールに利用者を登録することができます。

Systemwalker Centric Managerのディレクトリ、ファイルのアクセス権について

【Windows版】

Systemwalker Centric Managerに関係するディレクトリ、ファイルへのアクセス権を各ロールに対して与えています。システム管理者、監視担当の管理者、配付担当の管理者はSystemwalker Centric Managerを利用するユーザすべてを、適切なロールに登録してください。

【UNIX版】

Systemwalker Centric Managerに関係するディレクトリ、ファイルへのアクセス権をオーナーとswadminグループに所属しているユーザに限定しています。

インストール時にswadminグループが作成されますので、システム管理者はSystemwalker Centric Managerを利用するユーザすべてをswadminグループに登録してください。

アクセスできる資源の制限について

Systemwalkerコンソールでは、ノード管理ツリーや業務管理ツリーを利用することで、利用者が監視/操作できる資源を制限することができます。
ノード管理ツリーや業務管理ツリーについては、“Systemwalker Centric Manager 使用手引書 監視機能編”を参照してください。

物理的保護、ネットワーク環境の保護 （完全性を満たすための対策）

Systemwalker Centric Managerの利用者は運用管理者であり、一般の利用者とは異なります。Systemwalker Centric Managerに関連する機器、記録媒体などを物理的に保護することは、非常に有効な対策です。

具体的な例としては、以下などがあげられます。

- 運用管理者だけが入退室可能な鍵のかかる部屋に機器を設置する。
- 入退室の記録を取り不審者のチェックを行う。(建物単位での入出管理も同様)
- 耐震設備のある施設に機器を設置し、災害による影響から保護する。

また、ネットワーク上を流れるデータの保護も重要です。Systemwalker Centric Managerでは一部データの暗号化機能をサポートしていますが、運用管理用の専用LANを用意し、ネットワーク環境として安全性を保護する方法も非常に有効な対策です。

運用設計について （可用性を満たすための対策）

Systemwalker Centric Managerでは、大量メッセージ発生時に一定数以上のメッセージを棄却し、ディスク資源やネットワーク資源といった利用資源の枯渇を防ぐ機能を持っていますが、運用で適切なパラメタを設定する必要があります。運用設計時に資源の見積もりを十分に行い、円滑に運用が行えるように設計を行ってください。

また、運用時に利用者(運用管理者)が操作ミスや不正な操作を試みないように、利用者(運用管理者)に対する教育も適宜行うような組織のセキュリティポリシーを策定することも重要な対策となります。

EE GEE 2.2.2 Systemwalkerコンソールの操作を制御する

コンソール操作制御機能を使用することで、Systemwalkerコンソールの操作を制御できます。

認証方式

コンソール操作制御では、以下の認証方式を使用できます。

- ログインIDでの操作の保護
- 操作ごとの保護

ログインIDでの操作の保護

Systemwalkerコンソールにログインするごとに、Systemwalkerコンソールで操作できる機能に対して、ロールによる利用権限に比べて細かな権限を設定できます。

システム管理者やオペレータごとに運用管理クライアント用の端末が割り当てられており、各担当者にSystemwalkerにログインするIDを割り当てる場合や、操作する資源ごとに専用の運用管理クライアントが存在し、運用管理クライアントごとにログインするIDを割り当てる場合などに、Systemwalkerコンソールにログインするユーザごとに操作の制限を設定できます。

操作ごとの保護

操作ごとの保護機能では、Systemwalkerコンソールで操作を行うときに操作を行うユーザのID(ユーザーID)の入力が必要です。Systemwalkerコンソールを操作するときに入力したユーザーIDごとに、Systemwalkerコンソールで操作できる機能に対して、より細かな権限チェックを設定することができます。

運用管理クライアントをオペレータやシステム管理者が共同で使用するなど、Systemwalkerコンソールは常時起動した状態で運用し操作を行うユーザごとに操作を制限する場合に使用します。

また、複数の運用管理サーバを監視するために、1台の運用管理クライアントから一括で認証できるようになります。

SMARTACCESSとの連携

運用管理クライアントに富士通のソフトウェア製品であるSMARTACCESSを導入することにより、ICカード(Felica方式)や指紋認証等の認証デバイスを使用してセキュリティを強化できます。

SMARTACCESSを連携した場合、Systemwalkerコンソールの操作を行うユーザは管理者が登録した認証デバイスを使用するため、ユーザーID /パスワードを知る必要がなくなります。そのため、システムを操作するためのユーザーIDやパスワードが漏洩する可能性が低くなり、なりすましを防止できます。

Windows版の運用管理サーバ上ではSMARTACCESSを使用できません。Windows版の運用管理サーバでは操作を行うユーザがユーザーID、パスワードを知る運用になります。運用管理サーバは管理者だけが使用する運用をおすすめします。

また、SMARTACCESSのアプリケーションログオン機能により、操作ごとの保護機能を使用したときに必要となるユーザのID(ユーザーID)の入力が自動化できます。

2.2.3 サーバの利用を制御する

サーバのアクセス制御では、管理対象サーバの資産に対するアクセス許可・拒否を制御し、アクセス監査ログを出力することができます。

また、システム保守作業において、既存のセキュリティ設定を変更することなく保守作業を実施し、保守作業の履歴を管理・点検することができます。

サーバアクセス制御では、以下の3つの機能を提供しています。

- アクセス制御
- 監査ログ出力
- 安全なシステム保守支援機能

アクセス制御

管理対象サーバの資産へのアクセスを設定することで不正なアクセスを禁止できます。

また、管理者を含め利用者ごとに、最低限のアクセス許可を与えることでセキュリティレベルを高く保つことができます。

OS標準のアクセス制御機能との関係

OSが標準で提供しているアクセス制御機能とサーバアクセス制御で提供するアクセス制御機能について説明します。

OSが標準で提供しているアクセス制御機能

任意アクセス制御機能(Discretionary Access Control、DAC)と呼ばれており、Linuxシステムにおいては2種類のDACが存在します。この機能の特徴は、以下のとおりです。

- 資源の所有者(ファイルの場合は、ファイルの持ち主)が自由にアクセス制御を変更することができる
- システムの管理者(rootユーザ)は、所有者が設定したアクセス制御を無視してすべての資源にアクセス可能

サーバアクセス制御で提供するアクセス制御機能

DACアクセス制御により許可されている資源に対してアクセス監査ログの出力、およびアクセス制御を提供します。このため、OS標準のDACによってもともとアクセスできない資源に対しては、サーバアクセス制御機能でログ出力/アクセス制御はできません。

監査ログ出力

サーバアクセス制御は、アクセス監査ログ、操作の録画データ、Systemwalkerコンソール監査ログを監査ログとして出力します。

監査ログを分析することで、サーバ資産に対する不正な操作が行われていないことを点検できます。不正な操作が行われていた場合は、アクセス制御の設定を見直し、再度設定することで、サーバ資産の安全性を高めることができます。

アクセス監査ログ

- 管理対象サーバの資産へのアクセス情報
  - ファイルへのアクセス
  - レジストリへのアクセス
  - プロセスの起動/強制停止
  - ネットワークへのアクセス
  - ログイン
- 安全なシステム保守支援機能を使用した際の作業情報
- アクセス制御のポリシーが適用された際のポリシーの内容

  アクセス監査ログの詳細については、“Systemwalker Centric Managerリファレンスマニュアル”の“アクセス監査ログファイル”を参照してください。

操作の録画データ【Linux版】

- 安全なシステム保守支援機能を使用した際の操作内容

Systemwalkerコンソール監査ログ

- 運用管理クライアントのサーバアクセス制御の操作内容や操作結果
- サーバアクセス制御機能のコマンド実行時の情報

  システム管理者が、Systemwalker Centric Manager の使用状況を監査するログです。

詳細については、“Systemwalker Centric Managerリファレンスマニュアル”の“監査ログファイル”を参照してください。

安全なシステム保守支援

システム保守を行う場合、特権(root、Administrator権限など)を必要とする作業があります。安全なシステム保守支援機能では、セキュリティ管理者が承認した利用者にのみ、特権の利用を許可し、承認された範囲で保守作業することができます。



Windows版を使用する場合の注意事項

Windows Server 2012以降の場合、以下の機能は使用できません。

- プロセス停止のアクセス制御、ログ出力
- コンソールログイン/ネットワークログインのアクセス制御
- 安全なシステム保守支援機能

2.2.4 監査ログを管理/分析する

監査ログを出力し、監査ログを管理/分析する機能について説明します。

- 監査ログを管理する(監査ログ管理機能)
- 監査ログを分析する(監査ログ分析機能)

監査ログを管理する

監査ログ出力

監査ログ出力は、Systemwalkerの画面に対する操作について、いつ、誰が、どこ(どのサーバ/クライアント)から、どのような操作・変更を行ったかの履歴を監査ログとして出力します。

監査ログは、運用管理サーバに収集することができます。
なお、以下の機能については、監査ログ出力の対象外です。

- アプリケーション管理
- 返答メッセージ
- Systemwalker Webコンソール(モバイル版)

監査ログの管理

分散化された各サーバのログを収集し、指定した運用管理サーバで一元管理することができます。利用例を以下に示します。

- ログファイル監視による一部の異常監視をするのではなく、すべてのログを収集したい。
- ログを蓄積することで、異常が発生した場合、問題点の手がかりとしたい。また、問題操作の抑止力としたい。

収集するログファイル形式は、以下のとおりです。

- Windows イベントログ

  以下のイベントログの収集が可能です。

  - アプリケーション
  - セキュリティ
  - システム
  - DNS Server
  - Directory Service
  - ファイル複製サービス
  - DFS レプリケーション
  - ハードウェア イベント
  - 転送された イベント
  - Hyper-V Server イベントログ
- UNIX OSのログ
  - シスログ
  - /var/adm/loginlog・・・・・・Solarisのみ
  - suログ (/var/adm/sulog)・・・Solaris、HP-UXのみ
- GSシステムのログ
  - アクセス(RACF)ログ
  - 業務(AIM)ログ
- Windows Internet Information Service(IIS) ログ
  - NCSA 共通ログ ファイル形式
  - Microsoft IIS ログ ファイル形式
  - W3C拡張形式
- Apache
  - アクセスログ NCSA形式(初期形式)
  - エラーログ

- Systemwalker Centric Managerのリモートコマンド検索コマンド(opacmdrev)で出力したテキストログ
- Systemwalkerコンソールの監査ログ、またはSystemwalker Centric Managerのサーバアクセス制御の監査ログ
- Systemwalker Desktop Keeperのバックアップコマンドによるクライアント操作ログ
- ETERNUS NR1000F seriesイベントログ
- テキストログ
  - 監査ログ管理機能の収集規約に合致しているものについて収集可能です。
- バイナリファイルのログ
  - バイナリファイルのログ収集は、V13.2.0以降の運用管理サーバ、被管理サーバまたは中継サーバが必要です。
- Systemwalker Operation Manager操作ログ

ログの収集、収集規約については、“Systemwalker Centric Manager 使用手引書 セキュリティ編”の“監査ログ管理でログを収集するために”の“監査ログ管理の収集規約”を参照してください。

監査ログ管理機能では、以下のようにサーバ種別を定義しています。

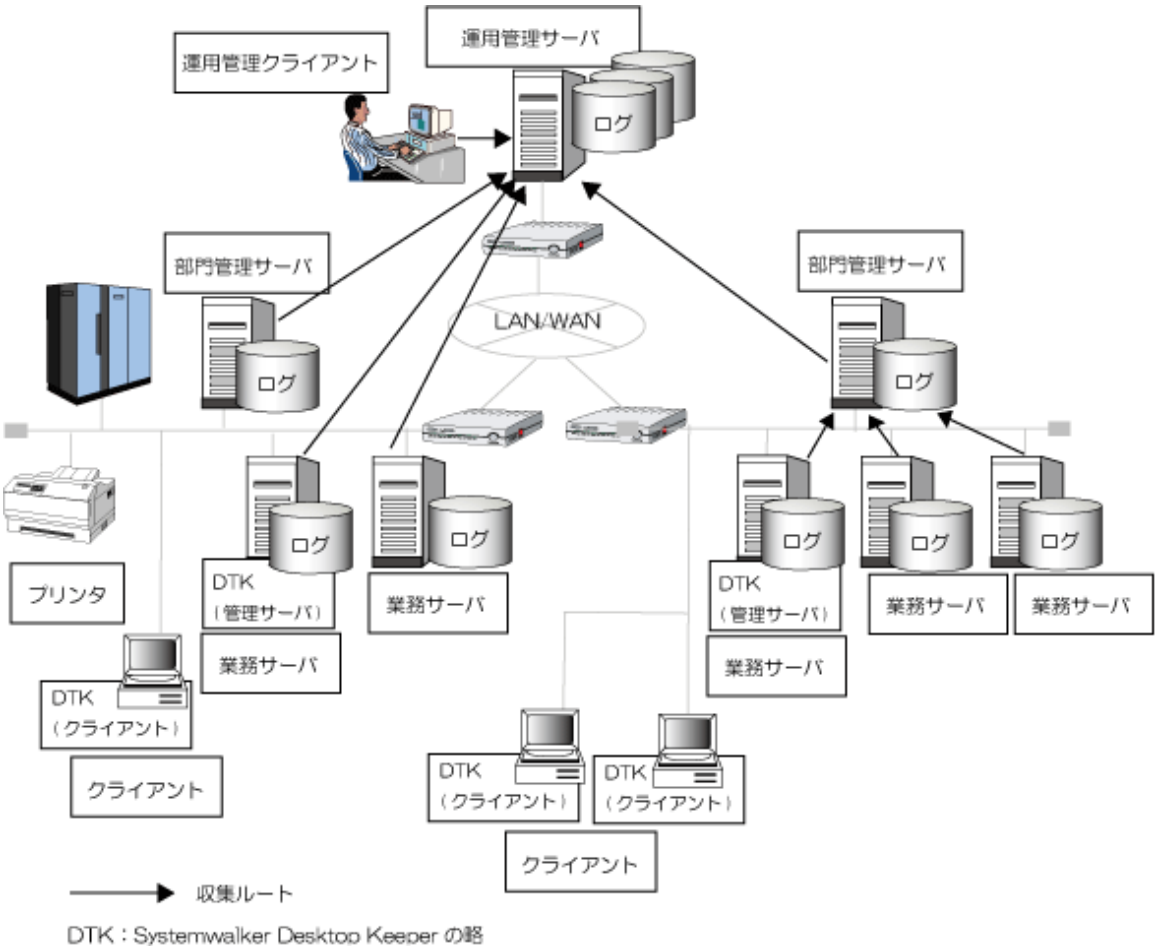
サーバ種別	説明
運用管理サーバ	ログ収集対象サーバから収集されたログを一括管理するサーバ(ログ収集対象サーバの機能も含んでおり、運用管理サーバ上にあるログ収集もできます)
被管理サーバ (部門管理サーバ/業務サーバ/運用管理クライアント)	ログ収集対象となるサーバ
中継サーバ (運用管理サーバ/部門管理サーバ/業務サーバ)(注)	ログ収集対象サーバから収集したログを一時的に管理するサーバ(運用管理サーバと被管理サーバの機能を含んでいます) 運用管理サーバから中継サーバ上のログを収集することで、運用管理サーバ上でログを一括管理します。

注)

運用管理サーバを中継サーバとする場合は、全体監視サーバ運用を行った場合のみ使用してください。
中継サーバにできるサーバは、V13.2.0以降の運用管理サーバ、部門管理サーバ、または業務サーバです。

Systemwalker Operation Managerなどのジョブ管理製品、OSのスケジュール機能を使用することにより、定期的なログの収集・保管が可能となります。

監査ログ管理機能を使用した構成例を以下に示します。



監査ログ管理機能を使用し、ログを保管するには、運用管理サーバのディスク容量に余裕のあるパーティション、ドライブが必要となります。

監査ログ管理機能を使用するために必要なディスク容量は、“Systemwalker Centric Manager 導入手引書”で、“運用管理サーバの環境構築”の“監査ログ管理に必要な資源”を参照してください。

監査ログを分析する

各システムで出力された監査ログは、分析目的に応じた、問い合わせサンプルファイルで簡単に分析することができます。

Systemwalker Centric Managerが分析できる監査ログ

- Windows イベントログ
- UNIX OSのログ
  - シスログ
  - /var/adm/loginlog・・・・・・Solarisのみ
  - suログ (/var/adm/sulog)・・・Solaris、HP-UXのみ
- GSシステムのログ
  - アクセス(RACF)ログ
  - 業務(AIM)ログ
- Windows Internet Information Service(IIS) ログ
  - NCSA 共通ログ ファイル形式
  - Microsoft IIS ログ ファイル形式

  - W3C拡張形式
- Apache
  - アクセスログ NCSA形式(初期形式)
  - エラーログ
- Systemwalker Centric Managerのリモートコマンド検索コマンド(opacmdrev)で出力したテキストログ
- Systemwalkerコンソールの監査ログ、またはSystemwalker Centric Managerのサーバアクセス制御の監査ログ
- Systemwalker Desktop Keeperのバックアップコマンドによるクライアント操作ログ
- ETERNUS NR1000F seriesイベントログ
- テキストログ
- バイナリファイルのログ(該当ログをテキスト変換する参照用コマンドを利用することにより実現)
- Systemwalker Operation Manager操作ログ

レポーティング

ログを分析した結果から監査資料を作成できるように、レポート出力機能を備えています。
集計結果や監査コメントを出力できます。

2.3 構成情報の管理（フレームワーク）

Systemwalker Centric Managerは、管理対象とするすべてのノードの構成情報を管理しています。
Systemwalker Centric Managerでは、ネットワークやシステム全体の構成情報を収集し、一元管理します。

収集/管理した情報は次のような目的に使用できます。

- ネットワーク構成の把握
- 容易な資産管理

構成情報の管理について説明します。

構成情報とは

Systemwalker Centric Managerでは、以下の構成情報を一元管理します。

- ネットワークの構成情報
- システムの構成情報

構成情報の詳細については、“構成情報一覧”を参照してください。

構成情報の管理対象

構成情報の管理対象を以下に示します。

構成情報の種類	部門管理/業務サーバ		クライアント	ネットワーク機器
	Windows	UNIX		
ネットワークの構成情報	○(注)	○(注)	○(注)	○(注)
システムの構成情報 (インベントリ情報)	○	○	○	－

○：管理可能
－：対象外

注)

Systemwalker Centric Managerが導入されていないノードも管理可能です。
ただし、イントラネット外または、DMZ内のノードについては、Systemwalker Centric Managerを導入し、監視対象として登録したノードだけが、ネットワーク構成情報として管理できます。

2.3.1　ネットワークの構成情報を管理する

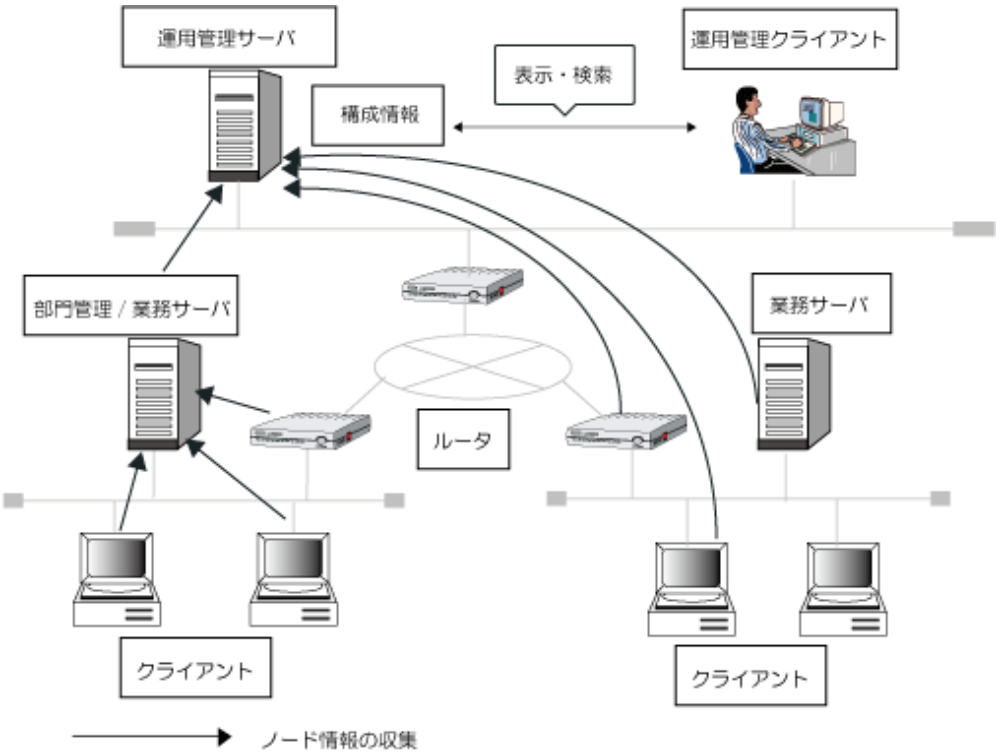
ネットワークに接続されたシステムやネットワーク機器(ノード)を検出し、ネットワーク構成を一元管理します。収集/一元管理された情報は、ネットワーク構成の把握、資産管理に利用できます。

ネットワークの構成情報は、Systemwalker Centric Managerが導入されていないノードも管理可能です。次のIT資源について、管理できます。

- UNIXサーバ、Windowsサーバ
- Windowsクライアント
- ネットワーク機器

ネットワークの構成情報の管理について概要を、“ネットワーク構成情報の管理”に示します。

図2.1 ネットワーク構成情報の管理



ノード自動検出

ネットワークに接続されたノードを検出し、監視マップ/リストを自動的に作成します。運用途中にノードがネットワークに接続された場合、自動的にノードを検出し、監視マップ/リストに反映します。

ノードは、ARPテーブルの参照、pingによるポーリング、プロトコルの接続確認により自動検出されます。

プロトコルの選択により、ファイアウォールによって遮断された環境においても、ノードを自動検出することができます。

収集する情報

複数のサブネットに接続されたノードを検出することができます。自動検出されたノードは、IPアドレスやノード名(ホスト名)などの情報を構成情報として一括管理します。

SNMPエージェントが起動しているノードに対しては、さらに詳細な情報(MACアドレス、OSやメーカ名)を収集できます。

ネットワーク構成情報の活用

自動検出されたノードは、IPアドレスやノード名などの構成情報を運用管理サーバ上で一括管理します。構成情報は、IPアドレスやノード名を指定して、ノードを検索することができるので、ノードがどこのネットワークに所属しているかひと目でわかります。また、収集した構成情報をCSV形式に出力し、Excelなどのソフトウェアで活用することができます。

MIB情報の表示/設定

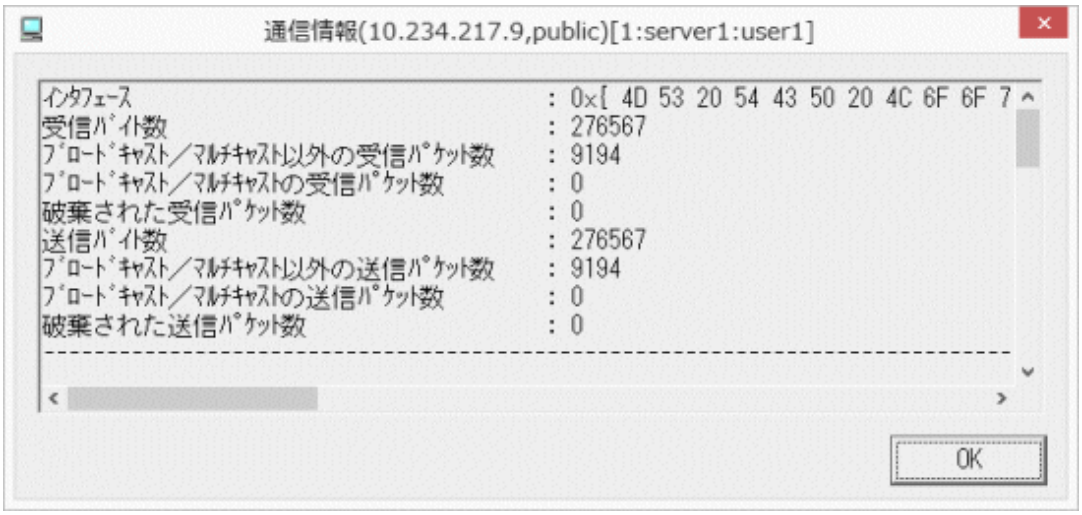
SNMPエージェントが起動しているノードのMIB情報を表示することで、ネットワークの構成情報、性能情報、および障害情報の管理に必要な情報を確認することができます。

また、MIB情報の設定を行うことでノードに対する制御を行うことができます。

なお、設定できるMIB情報は、SNMPエージェント側の設定に依存します。

操作方法およびMIB情報の詳細については、“Systemwalker Centric Manager 使用手引書 監視機能編”を確認してください。

以下に、表示の例を示します。



HUB接続状況の表示

SNMPエージェントが起動しているハブに接続されているノードを表示することができます。

操作方法については、“Systemwalker Centric Manager 使用手引書 監視機能編”を確認してください。

以下に、表示の例を示します。



2.3.2　システムの構成情報を管理する

クライアントやサーバのハードウェア/ソフトウェア構成情報などのシステム構成情報をインベントリ情報といいます。Systemwalker Centric Managerは、システムの構成情報をインベントリ情報として一元管理します。

ただし、Server Core環境では、インベントリ情報を表示することはできません。Server Core環境のインベントリ情報は、運用管理サーバ、または運用管理クライアントで表示してください。インベントリ情報を表示する方法については、"Systemwalker Centric Manager 使用手引書 資源配付機能編"を参照してください。

また、インベントリ情報の変更履歴は、以下のCSVファイルで参照することができます。

ファイル名	格納先
history.csv	Systemwalkerインストールディレクトリ¥mpwalker.dm¥mpcompcl¥history¥drms

なお、CSVファイルの形式は、"Systemwalker Centric Manager リファレンスマニュアル"の"インベントリ情報の変更履歴"を参照してください。

インベントリ情報とは

WMI(Windows Management Instrumentation)を使用し、コンピュータのモデル名、シリアル番号など、コンピュータの資産管理に有用な情報が収集できます。収集/一元管理された情報は、資産管理などに利用できます。インベントリ情報には、以下の情報が含まれます。

- ハードウェア情報
- ソフトウェア情報
- テキスト情報
- レジストリ情報

インベントリ情報の収集契機

インベントリ情報は、通常スケジュールを設定し、定期的に収集します。
インベントリ情報に関しては、特定のマシンにおける最新の構成情報を知りたいとき、またはトラブル発生時などに、すばやくオンデマンドで最新のインベントリ情報を収集できます。

インベントリ管理

ネットワーク上に接続されているサーバやクライアントのハードウェア構成やソフトウェア構成の情報を、インベントリ情報として一元管理し利用することができます。

以下の情報を収集/管理します。

・ ハードウェア情報

CPU種別、物理メモリ量、ディスク容量などサーバやクライアントのハードウェアに関する情報です。ユーザが資産管理上必要となる任意の情報(資産管理番号、管理者名、管理者連絡先など)をクライアント個々で設定することにより、それらの情報をインベントリ情報として扱うことも可能です。この情報をユーザ情報と呼び、ユーザ情報はクライアントごとに10個まで設定して、ハードウェア情報に含めることができます。

・ ソフトウェア情報

サーバやクライアントにインストールされているソフトウェア製品の製品名、バージョンなど、ソフトウェアに関する情報です。ファイル名、ファイルサイズ、Windows(R)システムのレジストリ情報などをもとに、市販されているソフトウェア製品およびユーザ作成の業務アプリケーションを特定し管理することができます。

・ テキスト情報

動作環境設定ファイルなど、サーバやクライアント上のテキストファイルの内容に関する情報です。クライアントのインベントリ情報として管理したい設定情報、業務アプリケーションの設定情報などを、テキスト情報として収集し参照することができます。

・ レジストリ情報

Windowsのレジストリキーに設定されている値を収集し、収集したレジストリキーの値はインベントリ管理の各画面で表示することができます。これにより、処理結果をレジストリに記録するようなSEツールや、シリアルキーをレジストリに記録するアプリケーションの管理が簡単にできるようになります。

収集するレジストリキーの定義は、レジストリ情報収集設定ファイルを作成して、管理対象のサーバおよびクライアント内のレジストリ情報を収集します。

ノードの自動検出

インベントリ情報が収集されたノードが監視マップ/リスト上に存在しない場合、自動的に監視マップ/リストへ反映することができます。このとき、サブネットフォルダが存在しない場合は、サブネットフォルダも合わせて作成されます。

インベントリ情報の履歴表示

クライアントのインベントリ情報の変更履歴を確認することができます。変更履歴を確認することにより、以下の効果を得ることができます。

・ トラブル発生時にインベントリ情報の変更履歴を確認することにより、トラブルの早期解決を図る。

・ ユーザによるクライアントの不正な使用方法の検出。

インベントリデータのCSV出力

インベントリ情報を条件にして検索したクライアントのインベントリデータをCSVファイルに出力することができます。出力したCSVファイルは、ユーザの用途に合わせてカスタマイズし、活用することができます。

インベントリ情報CSVファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

インベントリ情報の活用

収集されたインベントリ情報は、以下の用途で活用することができます。

資産の管理

ハードウェア情報・ソフトウェア情報をもとに、購入資産の状況を把握することができます。また、収集するインベントリ情報に資産管理に必要となるユーザ固有の情報(資産管理番号、管理者名、管理者連絡先などのユーザ情報)を付加することができます。

個々のシステム状況の把握

クライアントの利用者が個別にインストールしたソフトウェア資産を、システム単位に把握することができます。

収集すべきソフトウェア情報の特定

新しく購入したソフトウェア製品、およびユーザ固有の業務アプリケーションの導入状況を把握するために、インベントリ情報として収集対象となるソフトウェア情報を特定することができます。ソフトウェア情報の特定は、ソフトウェア辞書をカスタマイズし更新されたソフトウェア辞書情報をクライアントに配付します。

ソフトウェア辞書のカスタマイズ方法については、“Systemwalker Centric Manager 使用手引書 資源配付機能編”の“ソフトウェア辞書情報のカスタマイズ”を参照してください。

業務アプリケーションの状態確認

システム単位に保持する業務アプリケーションおよび環境設定などの任意の情報を、テキスト情報として収集することができます。収集した情報をもとに、各システムの環境およびアプリケーションの状態を確認することができます。

2.4 監視

Systemwalker Centric Managerでは、ネットワークやシステム、業務などの状況を集中的に監視することができます。以下のようなさまざまな目的で使用できます。

- ネットワーク負荷の集中箇所を監視しトラブルを未然に防止する
- 管理者のいないサーバで発生するトラブルをセンタで集中して監視する
- トラブル発生による業務への影響をすばやく把握する
- ウィルス検出製品と連携し、ウィルスを早期検出する

Systemwalker Centric Managerでは、ネットワーク、システム、アプリケーションについて、次の観点から集中的に監視することができます。

- 障害の監視
- 稼働状況の監視
- 性能の監視
- Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントの監視
- ホストの監視

さらに、ネットワーク、システム、アプリケーションについての監視を組み合わせ、業務の観点から監視することができます。

また、監視したい事象の発生をアクション定義の機能を使用し、管理者へ音声などで通知することができます。

障害の監視

Systemwalker Centric Managerでは、システム異常、ネットワーク異常などの発生をイベントとして集中的に監視できます。稼働状況や性能を監視している場合の異常もイベントとして監視することができます。

障害の監視は、個々のシステム、アプリケーションなどの単位のほか、業務単位で監視することが可能です。

イベントが発生すると、Systemwalkerコンソール画面に通知され、どこで、どのようなイベントが発生したかを確認することができます。

さらに、イベントの発生をメールなどで自動的に管理者へ通知するなどのアクションを自動的に実行することができます。アクションの自動実行については“自動アクション”を参照してください。

Systemwalkerコンソールから行う障害の対処

監視画面から直接、ほかのアプリケーションを起動することができます。ネットワーク機器の管理ツールや、[Systemwalker Operation Manager]ウィンドウを呼び出すことにより、監視イベントの詳細な調査や対処が可能になります。

監視対象

障害の監視対象を以下に示します。

監視する障害の種類	部門管理/業務サーバ		クライアント	ネットワーク機器
	Windows	UNIX		
ネットワーク (トラップ監視/MIB監視)	○(注1)	○(注1)	○(注1)	○(注1)
システム (イベント監視)	○	○	△(注2)	－
アプリケーション/業務 (イベント監視)	○	○	－	－

○：監視可能
△：一部監視可能
－：対象外

注1)

Systemwalker Centric Managerが導入されていないノードも管理可能です。ただし、トラップ監視/MIB監視では、SNMPエージェントからのトラップ受信/MIB収集により監視を行うため、SNMPエージェントが動作していることが必要です。

注2)

以下のOSの場合に、クライアントのイベント監視が可能です。

- Windows(R) 10 Pro
- Windows(R) 10 Enterprise
- Windows(R) 11 Pro
- Windows(R) 11 Enterprise

稼働状況の監視

Systemwalker Centric Managerでは、サーバやルータ、アプリケーションなどの稼働/停止状態を集中的に監視します。

Systemwalkerコンソールに、稼働/停止などの状態や、状態の変化を通知します。状態の変化とは、停止状態への遷移または起動状態への遷移を示します。

監視対象

稼働状況の監視対象を以下に示します。

監視する稼働状況の種類	部門管理/業務サーバ		クライアント	ネットワーク機器
	Windows	UNIX		
ネットワーク/システム (稼働状態の監視)	○(注)	○(注)	○(注)	○(注)
アプリケーション/業務	○	○	－	－

○：監視可能
－：対象外

注)

稼働状態の監視では、Systemwalker Centric ManagerやSNMPエージェントが導入されていないノードも管理可能です。稼働状態の監視の“状態表示”では、インタフェース情報のMIBを収集し、監視を行うため、SNMPエージェントが動作していることが必要です。
また、稼働状態の監視では、監視に使用する以下のプロトコルを一覧から選択できます。

- ICMP、SNMP、HTTP、FTP、TELNET、DNS、POP3、SMTP、HTTPS、Database、任意ポート

性能の監視

Systemwalker Centric Managerでは、システム、ネットワーク、アプリケーション、業務などの性能を集中的に監視します。各種性能情報を収集し、グラフ表示により性能の傾向を知ることができます。また、あらかじめ設定されたしきい値超えを監視し、性能の異常をイベントとして管理者へ通知します。しきい値超えを監視することで、性能トラブルの未然防止が可能です。

ネットワークやシステムの性能は、以下のように監視します。

- ネットワーク性能監視

  ネットワークシステム全体の性能状況(トラフィック情報)を把握するための機能です。ネットワークシステム全体に一律のしきい値を適用して監視します。

- サーバ性能監視

  監視システムごとに個別のしきい値を適用して、それぞれのシステムがその特性どおりに運用できているかを監視します。

監視の目的に合わせて、上記機能を使い分けることができます。ネットワークやシステムの性能監視の詳細については、“ネットワーク/システムの性能を監視する”を参照してください。

ネットワーク上に分散された複数のサーバ上に存在するアプリケーションの性能は、アプリケーション管理で集中して監視します。

アプリケーション管理による性能監視では、監視システムごとに個別の基準を適用して、それぞれのシステムがその特性どおりに運用できているかを監視することができます。アプリケーション管理については、“アプリケーションの性能を監視する”を参照してください。

ネットワークやシステムの性能監視に必要なエージェント

ネットワークやシステムの性能を監視するには、それぞれ以下のエージェントの機能が動作している必要があります。

監視対象	SNMPエージェント	Systemwalker Centric Managerのシステム性能収集エージェント
ネットワークの性能	○(注)	×
ネットワークの性能とシステムの性能(基本情報だけ)	○(注)	○
サーバ性能	○(注)	○

○：必要
×：不要

注)

代表インタフェースがIPv6アドレスのノードを監視対象とする場合、監視対象ノードにインストールされているSNMPエージェントが、IPv6の通信をサポートしている必要があります。

上記の条件を満たさないノードを監視する場合には、以下の機能が使用できません。

- mpsetnod(性能監視ノード構成情報登録コマンド)
- ネットワーク性能監視機能
- サーバ性能監視機能の以下の画面
  - ノード詳細表示(サーバ性能)画面
  - ヒストリ表示(サーバ性能)画面

監視対象

性能の監視対象を以下に示します。

性能監視の種類	部門管理/業務サーバ		クライアント	ネットワーク機器
	Windows	UNIX		
ネットワークの性能の監視	○(注2)	○(注1、注2)	○(注2)	○(注2)
システムの性能の監視	○	○	－	－
アプリケーションの性能の監視	○	○	×	－

○：監視可能×：監視不可
－：対象外

注1)

Linuxは制限があります。“OS別機能差一覧”を参照してください。

注2)

Systemwalker Centric Managerが導入されていないノードも管理可能です。

Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントの監視

Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントの監視をインストールレス型エージェント監視といいます。

インストールレス型エージェント監視は、管理者が被監視システムにSystemwalker Centric Managerのエージェント機能を手動でインストールすることなく、運用管理/部門管理サーバから監視可能にするための機能です。

インストールレス型エージェント監視では、以下の2つの方式があります。

非デプロイ方式

運用管理/部門管理サーバ上のインストールレス型エージェントが、被監視システムに対してSystemwalker Centric Managerのエージェント機能を配付することなく、被監視システムのOS機能を利用して監視を行います。

デプロイ方式

運用管理/部門管理サーバ上のインストールレス型エージェントが、被監視システムに対して自動でSystemwalker Centric Managerのエージェント機能を配付して監視を行います。非デプロイ方式よりも幅広い機能を利用できます。

インストールレス型エージェントとインストール型エージェントを監視する場合の差異

インストールレス型エージェントで監視する場合と、インストール型エージェントを導入したサーバ/クライアントを監視する場合の差異を以下に示します。

	インストールレス型エージェント (デプロイ方式/非デプロイ方式)	インストール型エージェント
監視方法	一定時間間隔で情報を取得し、監視します。	リアルタイムで監視します。
ネットワーク負荷	すべてのイベントを一旦監視サーバに集めるため、導入している場合に比べ、監視サーバと業務サーバの間の通信データ量が大きくなります。	業務サーバでイベントをフィルタリングできるため、監視サーバと業務サーバの間の通信データ量を抑えることができます。
構成	システムの構成に合わせて、2階層や3階層のシステム構成を柔軟に組むことができます。1台の監視サーバで監視できるサーバは300台までです。	システムの構成に合わせて、2階層や3階層のシステム構成を柔軟に組むことができます。

GEE

ホストの監視

Systemwalker Centric Manager GEEは、TCP/IPネットワーク上のUNIXシステムやWindowsシステムを監視する機能に加えて、グローバルサーバを監視することができます。

ホストの監視の詳細については、“Systemwalker Centric Manager 使用手引書 グローバルサーバ運用管理ガイド”の“グローバルサーバ監視について”を参照してください。

2.4.1 ネットワーク/システムの監視

ネットワークの監視

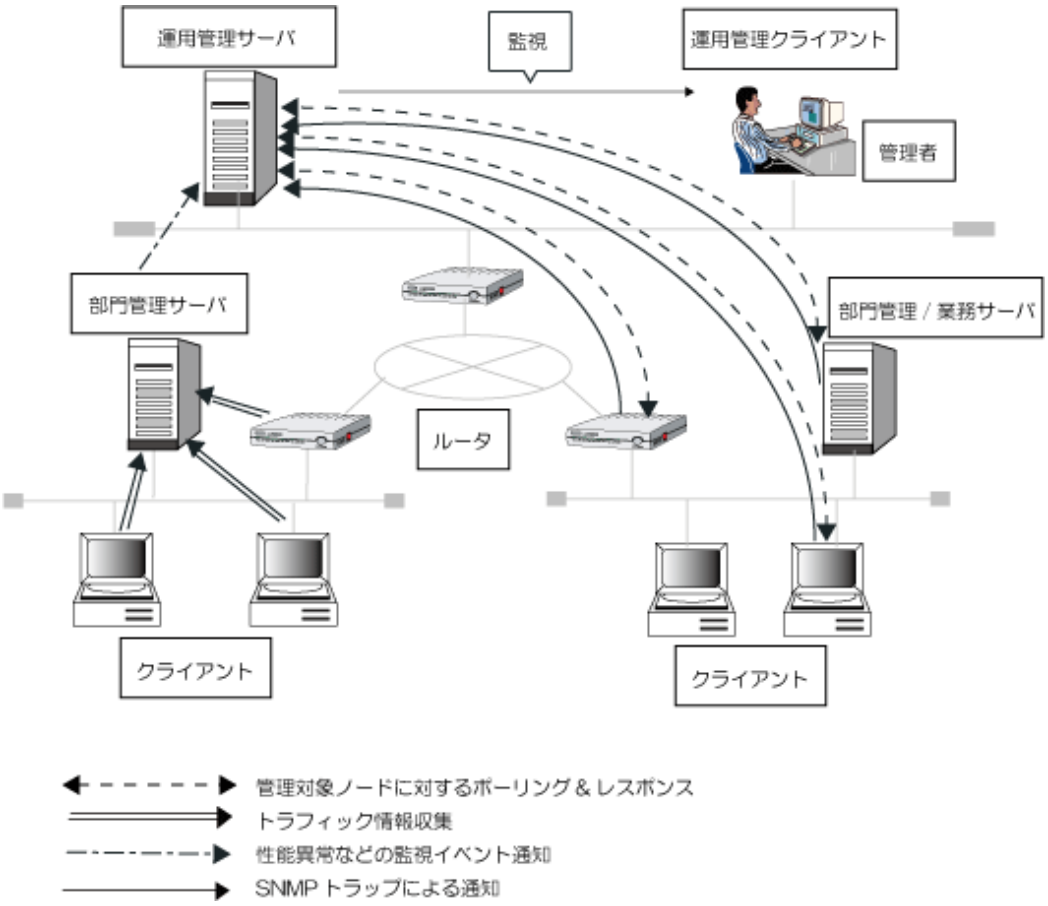
ネットワークの監視では、TCP/IPを使用したネットワークを監視対象としていることから、LANだけの小規模ネットワークからWANを含む大規模ネットワークまで監視することができます。

なお、ネットワークを監視するには、監視対象ノードにおいて、SNMPに対応したSNMPエージェントの機能が動作している必要があります。また、監視対象ノードがIPv4/IPv6のデュアルスタックノードの場合、IPv6インタフェースの稼働監視スクリプトにより、IPv6インタフェースの稼働状況が監視できます。

MIB取得、およびMIB監視により、ipv6MIBグループのMIBを取得/監視することが可能です。

ネットワークの監視の概要を、“ネットワークの監視の概要”に示します。

図2.2 ネットワークの監視の概要



SNMPトラップ

ネットワークの監視は、SNMP(Simple Network Management Protocol)を使用し、TCP/IPをベースとしたコンピュータネットワークを監視します。TCP/IPは、現在最も広く普及しているネットワークプロトコルであり、SNMPは、TCP/IPを使用したネットワークでの標準的なネットワーク管理プロトコルです。

通信負荷の軽減

クライアントやネットワーク機器で発生したトラップは、SNMPエージェントによって、運用管理サーバに通知されます。また、監視対象ノードの情報は、ポーリング・レスポンスによって運用管理サーバに通知されます。これらの通信負荷を軽減したい場合は、部門管理サーバを導入し、配下のノードに対して、トラップの受信やポーリングを行い、必要な情報だけを運用管理サーバに送信します。

システムの監視

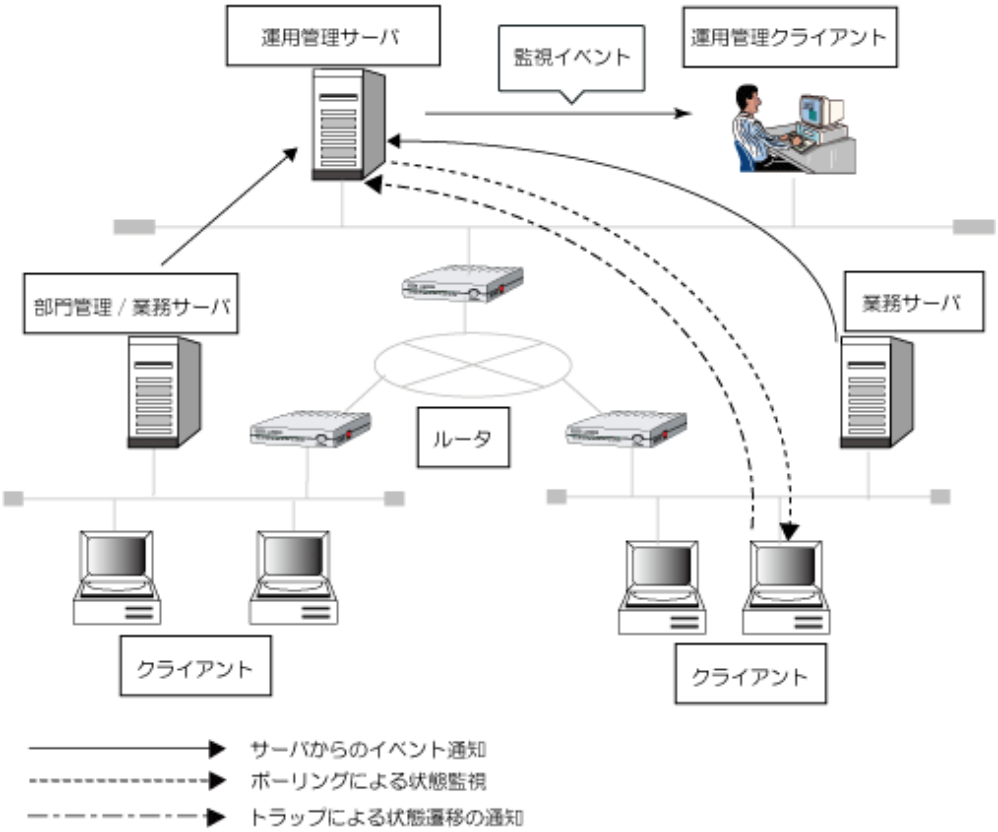
システムの監視では、サーバとクライアントの異常などを集中的に監視・操作します。

システムの集中監視を行うことで、以下の監視ができます。

- 遠隔地のサーバの電源が投入されているか確認する
- 管理者のいないサーバで発生するイベントをセンタで集中監視する
- 負荷が特定のサーバに集中していないか監視する

システムの監視の概要を以下に示します。

図2.3 システムの監視の概要



メール連携機能

イベント監視が監視するメッセージを上位システムに送信する場合、E-mailを使用してイベントを送信することができます。これによりファイアウォールを越えてシステムを監視できます。なお、本機能は送信側および受信側の両方に、Systemwalker Centric Managerの以下いずれかのサーバが必要です。

送信側システム:

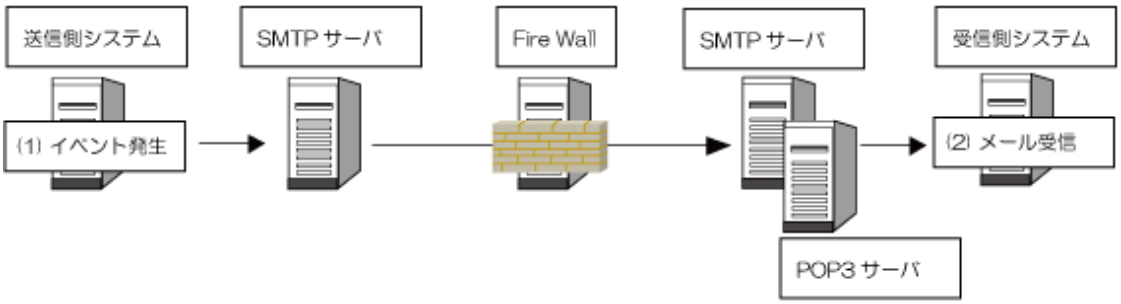
運用管理サーバ、部門管理サーバ、業務サーバまたはクライアント

受信側システム:

全体監視サーバ、運用管理サーバ、部門管理サーバまたは業務サーバ

メール連携の概要を以下に示します。

図2.4 メール連携の概要



(1) イベント発生システムでは、通知先システムに送信する情報を作成し、E-Mail を送信します。
(2) 受信側システムでは、イベント発生システムから送られたメールを POP3 サーバから受信します。

メッセージ説明を登録して監視する

データセンタ等の運用では、発生したイベントに対する対処手順書をあらかじめ作成しておくことがあります。対処手順書の内容をSystemwalkerコンソールに登録しておくと、発生したイベントごとの対処手順をその場で確認することができ、イベントに対する迅速な対処が可能となります。

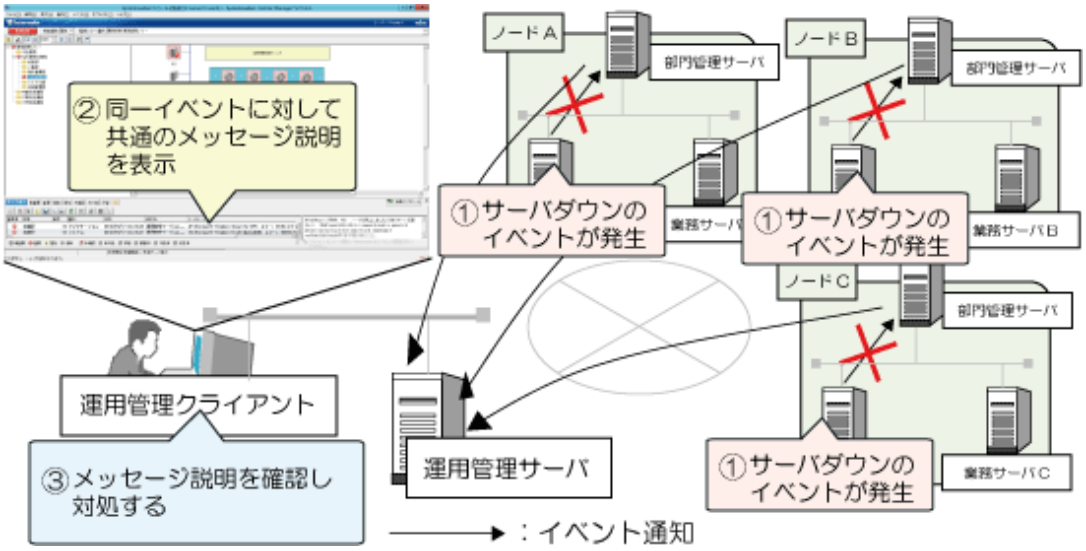
メッセージ説明を登録して監視するには、以下の2つの運用形態があります。

- 共通のメッセージ説明を登録して監視する
- フォルダごとにメッセージ説明を変更して監視する

共通のメッセージ説明を登録して監視する

1台の運用管理サーバで複数のノードを監視する場合、同一イベントに対して共通の対処方法や連絡先を表示することができます。

共通のメッセージ説明を登録して監視した場合の例を以下に示します。



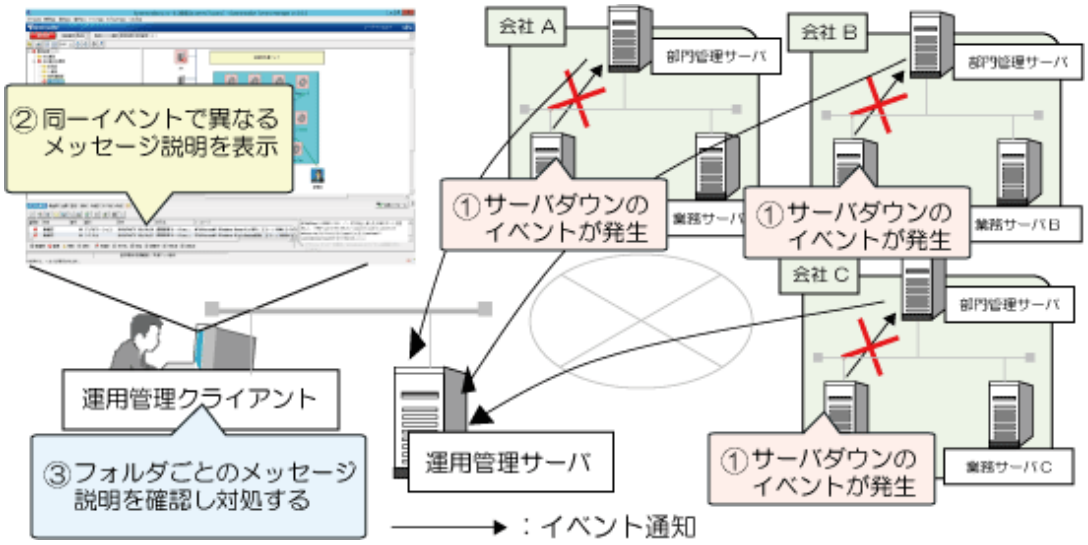
フォルダごとにメッセージ説明を変更して監視する

1台の運用管理サーバで複数のユーザのノードを監視する場合、ユーザごとにイベント発生時の対処方法や連絡先が異なります。

また、同一ユーザでもノードの設置場所によって、イベント発生に関する連絡先が異なる場合があります。

このような場合、同一イベントに対して、Systemwalkerコンソールの監視ツリーで監視しているフォルダごとに異なるメッセージ説明を表示することができます。

フォルダごとにメッセージ説明を変更して監視した場合の例を以下に示します。



SNMPバージョンとサポート機能について

以下にSNMPバージョンとサポートする機能について説明します。

- SNMPv1、SNMPv2C(注)、SNMPv3(注)をサポートする機能
  - ノード検出
  - 稼働状態の監視
  - MIB監視
  - SNMPトラップ監視
  - ネットワーク性能監視
  - サーバ性能監視
  - MIB取得
  - MIB設定
- SNMPv1をサポートする機能
  - MIB情報の表示(特定のMIBを表示する機能)
  - HUB接続状況の表示
  - サンプルスクリプト(MIBしきい値監視)
  - Systemwalker WebコンソールによるMIB情報表示
  - 自動運用支援(SNMPトラップ通知)
  - プロセス監視
  - mpsetnod(性能監視ノード構成情報登録コマンド)

注)
GetBulk、GetResponse、INFORM request、Reportは未サポートです。
ただし、INFORM requestは、ETERNUS TR seriesにおいて制限付きでサポートしています。詳細は、“Systemwalker Centric Manager 使用手引書 監視機能編”の“SNMPトラップの監視”または“Systemwalker Centric Manager 使用手引書 監視機能編 (互換用)”の“SNMPトラップの監視”を参照してください。

2.4.1.1 ネットワーク/システムの障害を監視する

ネットワーク機器とシステムの障害の監視について説明します。

トラップの監視

ノードからSNMPによるトラップで通知される事象を監視します。通知されたトラップをSystemwalker Centric Managerで扱うイベントの形式に変換し、ほかのイベントとあわせて監視イベント一覧で管理できます。また、受信したSNMPトラップを他製品にも転送できます。

MIB監視

ノードの通信異常などを集中的に監視するために、トラフィックやエラーに関するMIBの値を監視します。一定間隔であらかじめ設定されたしきい値と比較し、しきい値条件を超えた場合に、トラップとして通知し、メッセージが監視イベント一覧に出力されます。しきい値監視によりノードの異常を未然に防止することができます。また、MIBを操作し、MIB情報を収集し、グラフ表示することができます。MIB拡張機能により、標準で提供されているMIB-II以外のMIBを扱うこともできます。

イベント監視

ネットワークに接続されているシステムの異常を、イベント監視で集中的に監視します。イベント監視では、部門管理サーバ、業務サーバおよびクライアントで発生するシステム異常を監視します。システム異常が発生すると、監視画面にイベントが通知されます。監視画面では、どこで、どのようなシステム異常が発生したかを確認することができます。

イベント監視では、“イベント監視が監視するメッセージ”に示すイベント(メッセージ)を監視することができます。

表2.1 イベント監視が監視するメッセージ

対象システム	監視するメッセージ	出力先
Windows	システムおよびサービスがイベントログに出力するメッセージ (注4)	イベントログ
	Systemwalker Centric Managerの各機能が監視するイベント (注1)(注4)	イベントログ
	Systemwalker Centric Manager以外の連携製品が監視するイベント(注4)	イベントログ
	アプリケーションがイベントログに出力するメッセージ(注4)	イベントログ
	アプリケーションが一般ファイルに出力するメッセージ	テキストファイル
	SNMPトラップ	-
UNIX	システムおよびサービスが自システムのシスログに出力するメッセージ (注3)	シスログ
	Systemwalker Centric Managerの各機能が監視するイベント (注2)(注3)	シスログ
	Systemwalker Centric Manager以外の連携製品が監視するイベント(注3)	シスログ
	アプリケーションがシスログに出力するメッセージ(注3)	シスログ
	アプリケーションが一般ファイルに出力するメッセージ	テキストファイル
	任意のログファイルの監視(増分がメッセージとして監視される)	テキストファイル
	SNMPトラップ	-

注1)

以下のイベントについては、Systemwalker Centric Managerでは監視できません。
監視対象にするための設定方法もありません。

- ソース名がMpFwbs、イベントIDが3、説明(メッセージテキスト)が以下で始まるメッセージ
  50000009, 50200007, 50200008, 50200005

- ソース名がMpOpagtでイベントIDが以下のメッセージ
  4, 6, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 40, 44, 45, 46, 48, 49, 51, 52, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 75, 76, 77, 80, 81, 82, 83, 84, 85, 100, 101, 103, 105, 106, 111, 112, 113, 115, 116, 119, 120, 121, 122, 123, 126, 129, 130, 131, 140, 150, 151, 154, 155, 156, 157, 158, 159, 160, 165, 170, 171, 176, 177, 178, 179, 190, 206, 207, 208, 210, 211, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 300, 301, 302, 303, 304, 305, 310, 320, 322, 323, 324, 325, 326, 327, 398, 576, 594, 653, 654, 3001, 3003, 3004, 3010, 3100, 3101, 3102, 3103, 3104, 3105, 3106, 3107, 3202, 3203, 3204, 3205, 3206, 3390, 3391, 3392, 3393, 3394, 3395, 3396, 3397, 3398, 3400, 3401, 3500, 3501, 4041, 4042, 4043, 4044, 4045, 4046, 4052, 4060, 4061, 4062, 8002, 8003, 8004, 8005, 8103, 8104, 8105, 8301, 8302, 8303, 8304, 8305, 8306, 8307, 8308, 8309, 8310, 8311, 8312, 8313, 8314, 8400, 8401, 8402, 8403, 8404, 8405, 8406, 8407, 8408, 8409, 8528, 8529, 8530, 8531, 8532, 8751, 8752, 8753, 8754, 8755, 8756, 8757, 8758, 8759, 8760, 8761, 8762, 8763, 8764, 8801, 8802, 8803, 8804, 8807, 9000, 9052, 9053, 9054, 9074, 9081, 9082, 9091, 9092, 9104

注2)

以下のイベントについては、Systemwalker Centric Managerでは監視できません。
監視対象にするための設定方法もありません。

- MpFwemsで始まる以下のメッセージ
  50000009, 50200007, 50200008, 50200005

- UX:opagtdで始まるメッセージ番号が以下のメッセージ
  3, 4, 6, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 26, 27, 28, 29, 40, 44, 45, 46, 48, 49, 51, 52, 54, 55, 56, 57, 58, 60, 75, 76, 77, 80, 81, 82, 83, 84, 85, 90, 91, 94, 97, 119, 154, 158, 159, 165, 170, 171, 176, 177, 178, 179, 206, 207, 208, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 300, 301, 302, 303, 305, 310, 320, 322, 323, 324, 325, 326, 327, 398, 576, 594, 653, 654, 3001, 3003, 3004, 3010, 3100, 3101, 3102, 3103, 3104, 3105, 3106, 3107, 3202, 3203, 3204, 3205, 3206, 3390, 3391, 3392, 3393, 3394, 3395, 3396, 3397, 3398, 3400, 3401, 3500, 3501, 4000, 4001, 4002, 4003, 4004, 4005, 4006, 4007, 4008, 4009, 4010, 4011, 4012, 4014, 4015, 4016, 4018, 4019, 4023, 4024, 4025, 4026, 4027, 4028, 4029, 4030, 4031, 4032, 4033, 4034, 4035, 4038, 4041, 4042, 4043, 4044, 4045, 4046, 4052, 4060, 4061, 4062, 4600, 8002, 8003, 8004, 8005, 8101, 8102, 8103, 8104, 8105, 8301, 8302, 8303, 8304, 8305, 8306, 8307, 8308, 8309, 8310, 8311, 8312, 8313, 8314, 8400, 8401, 8402, 8403, 8404, 8405, 8406, 8407, 8408, 8409, 8528, 8529, 8530, 8531, 8532, 8751, 8752, 8753, 8754, 8755, 8756, 8757, 8758, 8759, 8760, 8761, 8762, 8763, 8764, 8801, 8802, 8803, 8804, 8807, 9000, 9052, 9053, 9054, 9074, 9081, 9082, 9091, 9092, 9093, 9094, 9104

注3)

初期設定ではレベルがwarning(警告)以上のメッセージが監視対象となります。監視対象を変更する場合は、“Systemwalker Centric Manager 導入手引書”の“監視するメッセージの設計”を参照して“/etc/syslog.conf”または“/etc/rsyslog.conf”の設定を変更してください。なお対象システムのOSがHP-UXの場合で、システムのホスト名が8バイトを超える場合は、シスログのメッセージ監視はできません。

注4)

初期設定では下記種類のイベントログのうち、システムに登録されているものが監視対象となります。下記以外のカスタムイベントログも監視することができます。詳細については、“Systemwalker Centric Manager 使用手引書 監視機能編”を参照してください。

なお、イベントサブスクリプションを使用して転送されたイベントは監視対象外です。そのため、転送されたイベントが格納されるイベントログ（ForwardedEvents ログまたはサブスクリプションで指定したログ）は監視できません。

- アプリケーション
- システム
- セキュリティ
- DNS Server

- ファイル複製サービス
- Directory Service
- DFSレプリケーション
- ハードウェア
- Media Center
- Internet Explorer
- Key Management Service
- Virtual Server
- Microsoft-Windows-Hyper-V-Config-Admin
- Microsoft-Windows-Hyper-V-Config-Operational
- Microsoft-Windows-Hyper-V-High-Availability-Admin
- Microsoft-Windows-Hyper-V-Hypervisor-Admin
- Microsoft-Windows-Hyper-V-Hypervisor-Operational
- Microsoft-Windows-Hyper-V-Image-Management-Service-Admin
- Microsoft-Windows-Hyper-V-Image-Management-Service-Operational
- Microsoft-Windows-Hyper-V-Integration-Admin
- Microsoft-Windows-Hyper-V-Network-Admin
- Microsoft-Windows-Hyper-V-Network-Operational
- Microsoft-Windows-Hyper-V-SynthNic-Admin
- Microsoft-Windows-Hyper-V-SynthStor-Admin
- Microsoft-Windows-Hyper-V-SynthStor-Operational
- Microsoft-Windows-Hyper-V-VMMS-Admin
- Microsoft-Windows-Hyper-V-Worker-Admin
- Microsoft-Windows-Hyper-V-SynthFc-Admin
- Microsoft-Windows-Hyper-V-VID-Admin
- Microsoft-Windows-Hyper-V-VMMS-Networking
- Microsoft-Windows-Hyper-V-VMMS-Operational
- Microsoft-Windows-Hyper-V-VMMS-Storage

“セキュリティ”だけ、または全種類のイベントログを監視対象外にする場合は、“イベントログ監視設定ファイル”の設定を変更してください。“イベントログ監視設定ファイル”については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

なお、新規インストール時のイベントログ監視設定ファイルは、セキュリティイベントログを監視対象からはずす設定となっています。バージョンアップ時には移行前の設定が引き継がれます。

これらのメッセージのうち、どのメッセージを監視するかを、定義することができます。監視対象としたメッセージは、メッセージ一覧として参照することができます。

- **監視イベント**

  サーバのシステム異常により発生するイベント、ネットワーク異常により発生するSNMPトラップなどの中から、監視したいイベントおよびトラップだけを選択して監視できます。監視対象とするイベントやトラップを、監視イベントと呼びます。
  イベント監視では、メッセージに重要度レベルを設定して管理します。重要度レベルが通知、警告、重要または最重要のものは、監視イベントとしてその発生が監視画面に通知され、集中監視できます。

- **ウィルス監視**

  Systemwalker Centric Managerは、クライアント/サーバ環境、イントラネットでのウィルス検出機能があるファイルサーバ用のウィルス検出製品と連携することができます。ネットワークやシステムなどの異常とともに、ウィルス検出製品が検出した異常/警告も集中的に監視できます。連携できるウィルス検出製品や環境設定については、Systemwalker Centric Manager 技術情報を参照してください。

イベントコリレーション機能

イベントコリレーション機能では、複数の異なるイベントを関連付けて監視することができます。

例えば、システムで発生した1個の障害に対して複数のイベントが発生する場合に、これらをまとめて1個のイベントとして通知することができます。また、正常時には特定の順序で発生するはずのイベントが発生しないなどの監視も可能です。

以下にイベントコリレーション機能を使用した運用例を示します。

- 同一事象から発生する複数の異なるイベントを1個のイベントとして通知する
- サーバの停止(LinkDownのイベント)が3回発生したら異常を通知する
- 異常発生によりクラスタの切り替えが発生した場合、10分以内に待機系が起動完了すれば正常とし、起動しない場合はアラームを通知する
- 障害が発生してから1時間以内に復旧しない(障害のイベントが発生してから1時間以内に復旧のイベントが発生しない)場合、アラームを発生させる
- 業務が順番に終了しなかった(業務終了のイベントが順番どおりに発生しなかった)場合、アラームを発生させる
- サーバが停止後、一定時間内に起動した（停止のイベントが発生後、一定時間内に起動のイベントが発生）場合、正常扱いとする

メッセージ変換機能

メッセージ変換機能は、発生したメッセージを、定義されたメッセージに変換します。

メッセージ変換機能は、指定された条件に一致するメッセージを変換ルールに従い、別のメッセージに置き換えます。

置き換えたメッセージは、以下の処理の対象となります。

- イベントコリレーションの監視条件
- イベント監視の条件定義のイベント監視との比較

また、以下のメッセージは変換後のメッセージとなります。

- Systemwalkerコンソールに表示されるメッセージ
- メッセージ監視アクションにおいてメッセージの編集で指定したプロシジャに渡されるメッセージ
- “%MSG”を指定したアクションで展開されるメッセージ
- メール通知で“イベントの内容を送信する”を指定した場合にメール本文に設定されるメッセージ
- メール連携機能で他マシンに通知されるメッセージ
- 音声通知アクションのメッセージの読み上げでイベント内容の通知を指定した場合に通知されるメッセージ

イベント抑止機能

イベント抑止機能は、以下の3つがあります。

- 同一イベントを抑止する

  一定時間内に、全く同じ内容のイベントが複数発生した場合に、2つ目以降のイベントを抑止します。

・ 類似イベント/大量イベントを抑止する

イベントが多発した場合に、ある一定時間以降のイベントを抑止します。イベントの一部だけが異なるような類似イベントだけを抑止することもできます。発生頻度が低くなった場合に、抑止を解除します。

・ 未確認イベント/未対処イベントを抑止する

あるイベントが発生した場合、そのイベントと同じイベントグループに属するイベントがすでに通知されており、かつ、未確認または未対処の状態である場合に抑止します。

なお、同一イベント抑止機能と類似イベント抑止/大量イベント抑止機能は、同時利用が可能です。

監視抑止機能

システムのメンテナンスや保守を行う場合などに、特定ノードに対する稼働監視を抑止したり、特定ノードからのイベント通知を抑止したりすることかできます。

抑止される監視内容は、一時的に監視を抑止する設定を行った場合、以下の監視が抑止されます。

・ 稼働状態の監視

・ MIBの監視

・ ネットワーク性能監視

また、監視抑止対象ノードから通知された以下のイベントについては監視イベント一覧、および[監視イベントログの検索]画面への表示を行いません。

・ イベントログ／シスログに出力されたイベント

・ 監視対象となっているアプリケーションのログファイルに出力されたメッセージ

・ メッセージ作成/出力コマンドを使用したイベント

・ アプリケーションの稼働違反、しきい値違反のイベント

イベント通知の抑止は、イベントの発生元ホストが、監視抑止の対象となっているノードであった場合に、監視イベント一覧に表示しないよう運用管理サーバで抑止します。

以下の機能については、抑止解除後の監視再開時には、抑止前の状態を引き継がずに、状態をリセットして監視を行います。

・ アプリケーションの稼働違反、しきい値違反のイベント

・ ネットワーク性能監視

以下の機能については、抑止解除後の監視再開時には、抑止前の状態を引き継いで監視を行います。

・ 稼働状態の監視

・ MIBの監視

抑止解除後の監視再開時のスクリプトにおいて、状態をリセットして監視を行う場合は、“Systemwalker Centric Manager 使用手引書 監視機能編”の“監視を抑止/再開する”の“スクリプトによる監視を行っている場合”を参照してください。

なお、以下のイベントは、監視抑止機能で「監視しない」から「監視する」に変更することで、業務サーバで未対処のイベントが運用管理サーバに再度通知されます。

・ アプリケーションの稼働違反、しきい値違反のイベント

2.4.1.2 ネットワーク/システムの稼働状況を監視する

ネットワーク機器とシステムの稼働状況の監視について説明します。

ルータなどのネットワーク機器、サーバ、クライアントなどをあわせてノードと呼びます。ネットワークに接続されているサーバやクライアント、ルータやゲートウェイなどのネットワーク機器(ノード)の稼働状況を、集中して監視します。

ノードの稼働状況は、対象ノードに対し、pingによるポーリング、SNMPによるインタフェース情報のMIB収集、プロトコル、またはDatabaseサーバの稼働確認により監視されます。

稼働状態の監視

サーバ、ルータなどのノードに対して、稼働/停止などの状態を監視画面に表示します。稼働/停止などの状態は、一定間隔ごとにポーリング、および任意のタイミングで監視し、稼働/停止等の状態をSystemwalkerコンソールの監視マップに表示されているアイコンの枠に色で表示します。Systemwalkerコンソールから一目で稼働、停止などのノードの状態が確認できます。また、ノード状態変化を検出した場合、Systemwalkerコンソールの監視マップ上のノード状態色を変更するとともに、メッセージとして状態変化を通知できます。

通知と表示方法

監視結果を通知する動作は以下の2つを指定できます。

- イベントを通知

  監視結果をイベントで通知します。

- 状態を表示

  監視結果をノードアイコンの枠で表示されるラベルカラーで通知します。

Systemwalkerコンソールに通知する単位は以下の2つから選択できます。

- プロトコル単位で通知/表示

  [イベントを通知]を指定した場合に、監視結果をプロトコル単位のイベントとして表示します。表示されるイベント、ラベルカラーは以下のとおりです。

イベントメッセージ	ラベルカラー
ERROR:106: %1ポート(%2)から応答がありました。	正常:緑色 すべてのポートから応答がある場合 異常: 赤色 いずれかのポートから応答がない場合
ERROR:106: %1ポート(%2)から応答がありません。	同上

  %1： 指定した監視方法(ICMPやSNMPやHTTPなどのプロトコル名)が格納されます。
  %2： 監視に使用したポート番号が格納されます。

- ノード単位で通知/表示

  [イベントを通知]を指定した場合に、監視結果をノード単位のイベントとして表示します。表示されるイベント、ラベルカラーは以下のとおりです。

  なお、複数プロトコルを選択している場合、ラベルカラーは[プロトコル単位で通知/表示]と異なる条件で設定されるため注意してください。

イベントメッセージ	ラベルカラー
ERROR: 106: ノードが起動しました。	正常:緑色 いずれかのポートから応答がある場合
ERROR: 106: ノードが停止しました。	異常:赤色 すべてのポートから応答がない場合

- インタフェースの監視を行う場合の動作について

  [監視方法]に[SNMP]を指定し、[インタフェースの監視を行う]を選択した場合の動作は、以下の2とおりです。

  - [動作]で[イベントを通知]を指定した場合

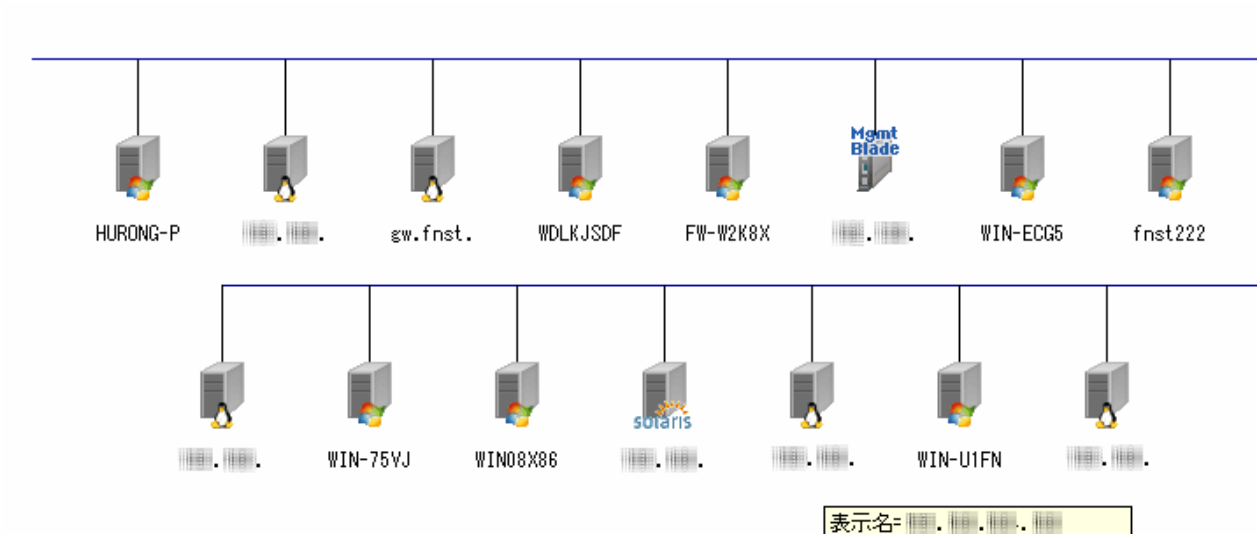
イベントメッセージ
ERROR: 106: SNMPエージェントが起動しました。
ERROR: 106: SNMPエージェントが停止しました。

イベントメッセージ
ERROR: 106: 一部インタフェースが起動しました。
ERROR: 106: 一部インタフェースが停止しました。

- [動作]で[状態を表示]を指定した場合、かつ[通知/表示単位]で[ノード単位で通知/表示]を指定した場合

監視マップでの表示の初期設定	監視リストの[稼働状態]カラムでの表示	状態
緑色	SNMPエージェント動作中	ノードが起動状態、かつ、SNMPエージェント動作中
緑色	一部インタフェースが停止中	ノードが起動状態、かつ、SNMPエージェント動作中、かつ、一部インタフェースが停止中
緑色	動作中	ノードが起動状態、かつ、SNMPエージェント未起動
赤色	未起動	ノードが未起動状態
なし	-	ノード状態が取得できていない（ノードの状態を監視していない）

監視マップの表示例を以下に示します。



2.4.1.3 ネットワーク/システムの性能を監視する

ネットワークに接続されているネットワーク機器やサーバなどのネットワーク性能情報、セグメントの性能情報を収集し、集中して監視します。また、システムの性能を集中監視し、システムの負荷増大などから発生するスローダウンなどを防止します。

以下の監視を性能監視で行います。

- 性能異常の監視
- 性能情報を表示

性能異常の監視

性能監視では、ネットワーク性能監視とサーバ性能監視を使い分けて、ネットワークやシステムの性能を監視できます。ネットワーク性能監視とサーバ性能監視の違いを以下に示します。

項目	ネットワーク性能監視機能	サーバ性能監視機能
監視方式	運用管理サーバまたは部門管理サーバからのポーリング監視	被監視ノード上での自律監視
監視情報	・ トラフィック情報 ・ サーバ性能情報(基本情報)	・ サーバ性能情報
監視方法	・ 固定のしきい値による監視(サービスレベル監視) ・ 過去の統計情報との比較による監視(ベースライン監視)	・ 固定のしきい値による監視
しきい値	管理システム全体に1つのしきい値を設定	被監視ノード単位にしきい値を設定
情報蓄積	ポーリング結果をロギングし、ロギング結果は統計レポートとして出力可能	なし

トラフィックの異常およびサーバ性能情報の異常を監視します。サーバ、ネットワーク機器(SNMPのMIBIIをサポートするノード)、RMON(Remote network MONitoring)などから採取したトラフィック情報をしきい値監視し、異常が発生した場合にイベントとして通知します。

しきい値監視は、以下の2種類の方法で監視できます。

・ サービスレベル監視

ネットワーク設計時に設定した目標値をあらかじめ定めておき、これを上回ることがないかどうかを監視する方法です。

・ ベースライン監視

過去の統計から求めた通常状態におけるネットワークの性能値(基準値)をもとに性能監視を行う方法です。

しきい値監視するトラフィック情報用CSVファイル、およびサーバ性能情報用CSVファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

ハブ/スイッチングハブ/スイッチングルータ/VLANのネットワーク性能監視

ネットワーク性能監視機能において、ハブ、スイッチングハブ、スイッチングルータ、およびVLANの監視はできません。ハブ、スイッチングハブ、スイッチングルータ、およびVLANのトラック情報を把握したい場合には、各ポートに接続されているノードを監視対象にしてください。
ただし、以下の条件を満たすL3スイッチについては監視を行うことが可能です。

・ 物理ポートごとにIPアドレスが割り当てられている。

・ IPアドレスに対してSNMP MIB IIの情報が収集できる。

なお、ネットワーク性能情報の収集で必要となるMIBは、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

サーバ性能監視機能の監視項目については、“Systemwalker Centric Manager リファレンスマニュアル”の“性能監視の監視項目一覧”を参照してください。

ネットワーク性能監視機能の監視項目については、“Systemwalker Centric Manager リファレンスマニュアル”の“性能監視の監視項目一覧”を参照してください。

Oracle SolarisのSPARC Servers環境のCPU使用率のサーバ性能監視

コアのCPU使用率を考慮した監視では、cpustatコマンドを使用します。

cpustatコマンドは同時に複数実行できないため、対象ノードでは以下を実施することはできません。

・ cpustatコマンド、およびcpustatコマンドを利用するコマンドの実行

・ Systemwalker Service Quality Coordinatorによる監視

性能情報の表示

性能監視で、サーバ、ネットワーク機器(SNMPのMIBIIをサポートするノード)、RMONなどの性能情報を表示します。トラフィック情報は、ネットワークの接続関係に従い監視できます。各ノード間の接続関係とともにトラフィック情報が表示されるので、トラフィック集中箇所等を迅速に発見できます。同時にサーバ性能情報も表示可能です。

性能監視では、サーバやルータなどから採取したトラフィック情報やサーバ性能情報をもとに、以下のような監視、操作が可能です。

- 性能監視マップの表示
- ノードの性能情報を表示
- 性能情報の推移を出力

性能監視マップの表示

性能監視マップには、監視対象の各ノードの接続関係およびトラフィック情報を表示します。性能監視が監視するトラフィックの異常が発生すると、イベントが監視画面に通知されます。監視画面から性能監視マップを表示し、トラフィック異常が発生した箇所周辺の状況を一目で把握できます。また、CPU情報やメモリ情報等のサーバ性能情報も表示されるので、性能異常の判断材料にすることができます。

さらに、性能監視マップから、各ノードのトラフィック情報の詳細や、各インタフェースのトラフィック情報の推移をグラフ表示することができます。また、性能監視マップから他アプリケーションを呼び出すことができるので、性能調査用のアプリケーションを呼び出すことにより、さらに詳細な異常の調査/解析を行うこともできます。

以下の2種類の性能監視マップを使用できます。

- ノード中心マップ

  選択したノードの属するサブネットを中心にして、そのサブネット内にある監視対象ノードを同心円上に配置し、接続関係を表示します。また、個々のノードを中心に関連するサブネットを同心円上に配置します。接続しているノード(ハブ、ルータを含む)間のトラフィック情報およびノードのサーバ性能情報を表示します。

- ペアノード経路マップ

  選択した2つのノード間のサブネットとノードの関係を描画し、トラフィック情報、サーバ性能情報を表示します。



監視対象がLinuxノードの場合の注意事項

パケット数の表示はできません。

ノード性能情報を表示

性能監視の監視対象としているノードの性能情報一覧を表示することができます。ノードのトラフィック情報およびサーバ性能情報を表示します。

- トラフィック情報

  選択したノードおよびインタフェースのトラフィック情報が表示されます。

- サーバ性能情報

  サーバ性能監視機能で設定した監視項目の状況を表示できます。設定した監視項目、インスタンス名、性能値が表示されます。



監視対象がLinuxノードの場合の注意事項

受信バイト数、送信バイト数、回線使用率だけ表示します。その他は「?」で表示されます。

注意

サーバ性能情報で表示されるディスク名には、先頭にプレフィックス“disk-”が付加されます。

プレフィックス“disk-”が付加された後のディスク名が255バイトを超える場合は、先頭から255バイト分を格納し、それを超える部分は切り捨てられます。

性能情報の推移を出力

収集した性能情報を、以下の2種類の形式で出力することができます。

- ヒストリ表示

  トラフィック情報またはサーバ性能情報を、現在からさかのぼってグラフ表示します。ネットワークやシステムの性能の推移を容易に確認できます。

- 性能情報出力

  収集した性能情報を、運用管理サーバ上でCSVファイルに出力することができます。また、ネットワークの性能情報は、Systemwalker Service Quality Coordinatorと連携して、グラフとしてレポート出力し、性能情報の管理に利用できます。詳細については、“ネットワークのサービスレベルを評価する”を参照してください。

GEE

2.4.1.4 グローバルサーバのシステムを監視する

グローバルサーバのシステムの監視は、以下の事項について説明します。

- 監視パス
- 監視メッセージ

監視パス

Systemwalker Centric Manager GEEは、被監視システムの監視・操作を行うために、以下の2つの監視パスを使います。

- 主監視パス
- 代替監視パス

それぞれの監視パスについて説明します。

主監視パス

Systemwalker Centric Managerと被監視システム間のTCP/IP接続により接続した通信経路を、主監視パスといいます。被監視システムのうち、MSPおよびXSPの監視・操作には、主監視パスが使われます。

被監視システム側では、MC/FSOCKETが動作し、被監視システムのシステム情報(システムコンソールに出力されるメッセージなど)を採取・送信します。Systemwalker Centric Manager GEEは、これを受け取り監視画面に表示します。また、Systemwalker Centric Manager GEEの監視画面からの操作は、MC/FSOCKETを経由して行われます。

主監視パスは、監視・操作の信頼性向上のために二重化することができます。

代替監視パス

グローバルサーバにSVPM-Sが接続されている場合は、SVPM-Sと連携することにより、AVM/EXを監視・操作できるようになります。また、SVPM-Sが監視するハードウェアの異常も監視できます。このSVPM-Sと連携する通信経路を代替監視パスと呼びます。

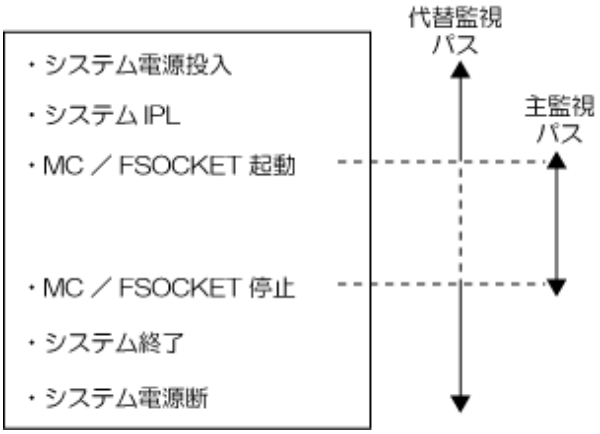
Systemwalker Centric Managerのマニュアルでは、特に注意する必要がない場合は、SVPM-SをSVPMと呼びます。

MSPおよびXSPにSVPMが接続されている場合は、代替監視パスによって、主監視パスで監視できなかった以下の監視・操作ができ、システムの起動から運用までのすべての段階について連続した監視・操作ができます。

- システムの電源状態の監視

・ システムのIPL時からの監視操作

・ MC/FSOCKETが停止中のシステムの監視操作



代替監視パスは、主監視パス接続後でもSVPMと連携することにより、AVM/EXを監視・操作できるようになります。また、SVPMが監視するハードウェアの異常も監視できます。代替監視パスは、SVPMのLANまたは装置を二重化することにより、監視・操作の信頼性を向上することができます。

なお、Systemwalker Centric Manager GEEは、MC/FSOCKETを介して被監視システムのシステム情報(監視メッセージ、動的状態情報など)を受け取り監視・操作を行いますので、代替監視パスによる監視を行う場合も、必ず被監視システムにはMC/FSOCKETを導入し、主監視パスによる監視を行ってください。

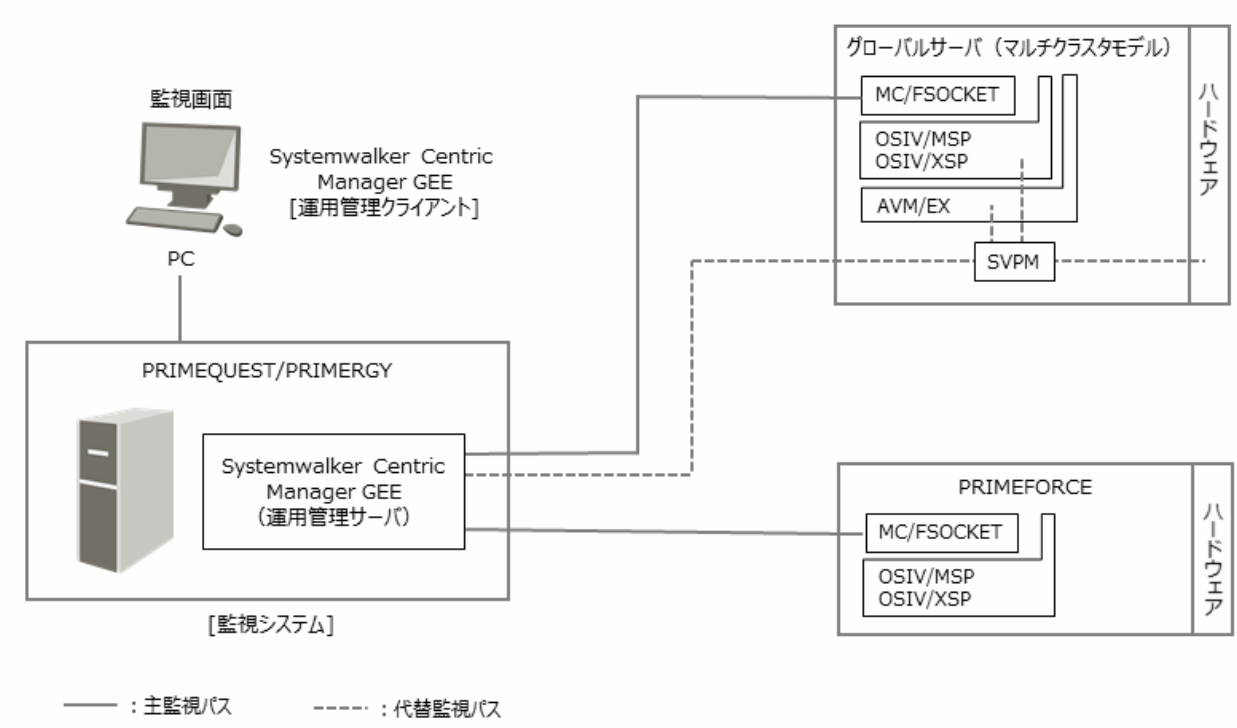
なお、以下の監視については代替監視パスでは監視できません。

・ グローバルサーバのサブシステムを監視する

・ グローバルサーバの業務を監視する

以下に主監視パスと代替監視パスの概要を示します。

図2.5 主監視パスと代替監視パスの概要



監視メッセージ

Systemwalker Centric Manager GEEでは、被監視システムのシステムコンソールに出力される、以下のメッセージを監視することができます。これらのメッセージのうち、被監視システムごとに、どのメッセージが監視できるかを“監視メッセージ”に示します。

- システムメッセージ
- 連携製品が出力する異常メッセージ
  - SystemWalker/OFESが監視するジョブネットの異常終了
  - FCMSYS/EMが監視する性能異常

SVPMが導入されている場合は、以下のメッセージも監視することができます。

- システムコンソールに出力される以下のメッセージ

  NIPメッセージ:

  システムのIPL後からシステムコンソールが動作するまでの間に出力されるメッセージです。

  システムダンプ:

  MSPのSADUMPのメッセージ、およびXSPのSYSDUMPのメッセージです。システムに異常が発生し、資料を採取するためにダンプ処理を起動した場合に出力されるメッセージです。

  システム重要メッセージ:

  XSPにおけるMC/FSOCKET起動前の重要メッセージです。詳細については、“OS IV/XSP MC/FSOCKET 説明書 V21用”を参照してください。
- AVM/EXのコンソールに出力されるメッセージ(AVMがSVPMに通知するメッセージに限られます。)
- SVPMが監視するハードウェアの異常(SVPMが監視する装置に発生した異常メッセージです。)

表2.2 監視メッセージ

監視メッセージ			被監視システム				
			グローバルサーバ			XSP	SVPM
			MSP	XSP	AVM/EX		
主監視パス	システムメッセージ		○	○	－	○	－
	連携製品	SystemWalker/OFES	○	○	－	○	－
		FCMSYS/EM	○	○	－	○	－
代替監視パス	NIPメッセージ		○	○	－	－	－
	システムダンプ		○	○	－	－	－
	システム重要メッセージ		－	○	－	－	－
	AVM/EXコンソールメッセージ		－	－	○	－	－
	ハードウェア異常メッセージ		－	－	－	－	○
サブシステム監視機能	グローバルサーバのサブシステムを監視		△	△	－	△	－
	グローバルサーバの業務を監視		△	△	－	△	－

○：使用可能

△：サブシステム監視機能は、Solaris上で動作するSystemwalker Centric Manager GEEで提供している機能です。

Linux上で動作するSystemwalker Centric Manager GEEでは使用できません。なお、サブシステムや業務が出力するメッセージを監視することで、サブシステムや業務を監視できます。

－：使用不可

メッセージは、[メッセージ一覧]ウィンドウに表示されます。このうち、トラブルとして定義したメッセージは、Systemwalkerコンソールの監視イベント一覧に表示され、監視画面から対処することができます。

GEE

2.4.1.5　グローバルサーバのサブシステムを監視する

Systemwalkerコンソールからグローバルサーバ上のサブシステムを監視するために、以下の機能を使用できます。サブシステムを監視できるのは、主監視パスで接続しているときのみです。

グローバルサーバのサブシステムの監視は、Solaris版 Systemwalker Centric Manager GEEでのみ利用できます。Linux版では利用できません。

- サブシステムの検出

  監視を行うサブシステムをMC/FSOCKETに定義することにより、サブシステムを検出し、Systemwalker Centric Managerに登録します。

- サブシステムのメッセージ監視

  監視対象サブシステムが発行したメッセージを、[イベント一覧]に表示することができます。また、メッセージを出力したサブシステムだけでなく、影響のある上位業務を点灯させることもできます。

- サブシステムの稼働監視

  サブシステムの稼働違反を[イベント一覧]に表示することができます。また、稼働違反が発生したサブシステムだけでなく、影響のある上位業務を点灯させることもできます。

- サブシステムの稼働状態表示

  サブシステムの稼働状態を画面に表示できます。

- サブシステムの表示

  サブシステムの情報を表示できます。

- サブシステムを業務に追加

  検出したサブシステムを業務に所属させ、業務として監視することができます。

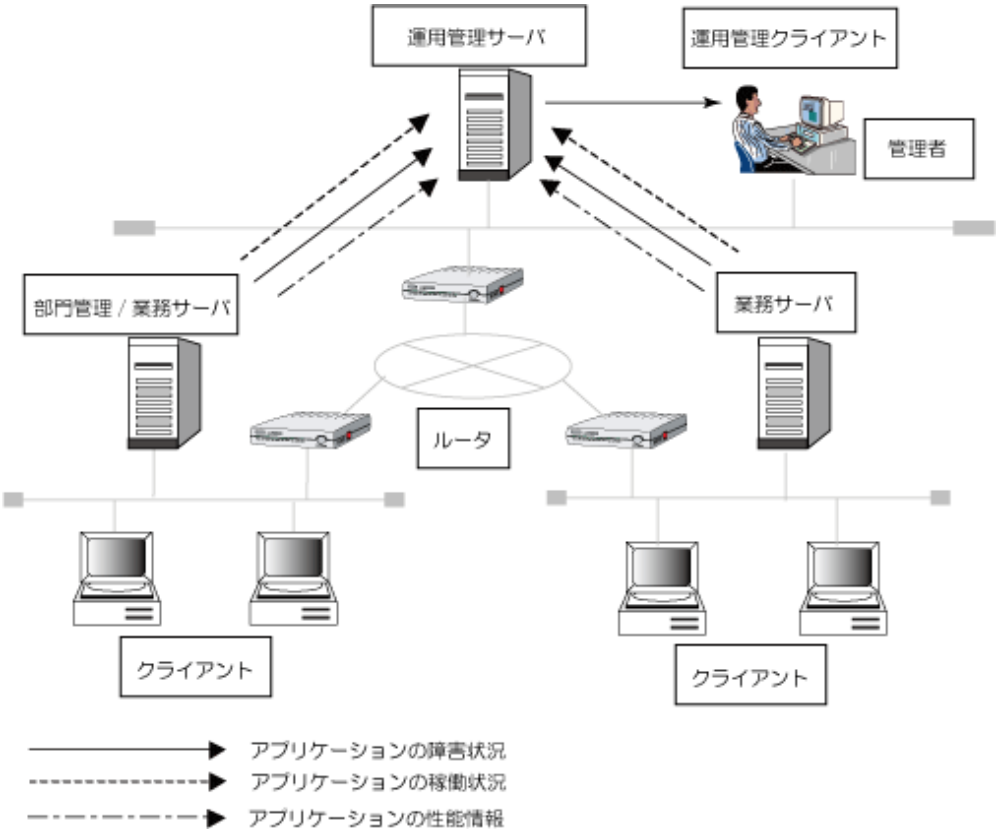
2.4.2　アプリケーションの監視

ネットワーク上に分散された複数のサーバ上に存在するアプリケーションを、集中的に監視します。アプリケーションの監視では、以下のことが可能です。

- 重要なアプリケーションの稼働/停止状態を監視する
- 予定どおりの時間にアプリケーションが稼働しているかを監視する

以下にアプリケーションの監視の概要を示します。

図2.6 アプリケーションの監視



アプリケーションの監視では、ネットワーク上に分散された複数のサーバ上に存在するアプリケーションに対し、以下の監視を行います。アプリケーションの監視は、監視間隔ごとに定期的に実施します。

- アプリケーションの障害状況の監視
- アプリケーションの稼働状況の監視
- アプリケーションの性能の監視

アプリケーションの稼働監視は、部門管理サーバ/業務サーバのアプリケーション管理機能が稼働ポリシー違反を検出し、運用管理サーバに通知することで行います。

2.4.2.1 アプリケーションの障害を監視する

サーバ上のアプリケーションで発生した異常(イベント)を集中監視できます。

アプリケーションのイベント監視

アプリケーションのポリシーとして定義した稼働要件に反した事象が発生した場合、ノードに発生したアプリケーションの異常をイベントとしてSystemwalkerコンソールに表示することができます。

異常が発生すると、監視画面に通知され、どこで、どのようなアプリケーション異常が発生したかを確認することができます。

2.4.2.2 アプリケーションの稼働状況を監視する

サーバのアプリケーションの稼働状況を、集中して監視します。以下の監視が可能です。

- アプリケーションの稼働状態の表示
- アプリケーションの稼働状態の監視

アプリケーションの稼働状態の表示

アプリケーションの稼働状況を監視し、状態を監視画面に表示します。一定間隔ごとに、監視対象としたアプリケーションの稼働状況を監視し、監視画面に状態を色で表示します。監視画面では、アプリケーションの動作中、未動作の状態が確認できます。

監視対象は以下のアプリケーションです。

【Windows】

Windows:拡張子が「.exe」のファイル

ワークユニット

IJServerクラスタ

クラスタサービス

【Linux】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh、python)

ワークユニット

IJServerクラスタ

クラスタサービス

【Solaris】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh)

ワークユニット

IJServerクラスタ

クラスタサービス

【HP-UX】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh)

クラスタサービス

例えば、ユーザ作成アプリケーションの場合、アプリケーションに含まれる実行形式ファイルから起動される常駐プロセスを、常駐プロセス単位で監視できます。

Oracleのような市販ソフトウェアの場合、Oracleで起動される常駐プロセスを、プロセス単位で監視できます。また、それぞれのプロセスは、どの市販ソフトウェアで起動されるプロセスなのかがわかるので、なんらかのトラブルでプロセスが停止した場合など、どの市販ソフトウェアに異常が発生しているのか、ひと目で把握することができます。

ワークユニット/IJServerクラスタ

Interstage Application Serverと連携することで、Interstageの監視をSystemwalker Centric Managerで行うことができます。構成表示および監視対象のワークユニット種別や機能は、Interstageのバージョンにより異なります。詳細については、“Systemwalker Centric Manager Interstage Application Server 運用管理ガイド”を参照してください。

アプリケーションの稼働状態の監視

特に重要なアプリケーションに対して、管理者が設定した稼働条件(ポリシー)どおりに稼働しているかどうかを監視します。ポリシーどおりに稼働していない場合には、イベントとして通知します。

例えば、以下のようなアプリケーション稼働の異常を監視できます。

- 朝9:00に起動されるアプリケーションが、なんらかの障害により予定どおりに起動されていない。
- アプリケーションが、ループ状態で指定した終了時刻に終了していない。

アプリケーションの稼働状態の監視により、「異常終了」のイベントが発生したアプリケーションだけではなく、ループ状態のアプリケーションなどが監視できます。管理者は、監視したいアプリケーションに対して、以下のポリシーを設定し監視します。

- 起動予定時刻
- 終了予定時刻

ポリシーに違反し、起動予定時刻と終了予定時刻の間にアプリケーションが稼働していない場合、または、終了予定時刻にアプリケーションが稼働している場合、イベントとして通知します。

さらに、ポリシーに違反し、起動予定時刻と終了予定時刻の間にアプリケーションが稼働していない場合、ポリシーに従って自動的にアプリケーションを起動させることが可能です。同様に、終了予定時刻にアプリケーションが停止していない場合、自動的にアプリケーションを停止することも可能です。

監視対象は以下のアプリケーションです。

【Windows】

Windows:拡張子が「.exe」のファイル

【Linux】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh、python)

【Solaris】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh)

【AIX】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh)

【HP-UX】

実行形式のファイルおよびシェルスクリプト(sh、ksh、csh、tcsh)



注意

起動/停止操作の注意事項

以下の種類のアプリケーションを、起動コマンドとして指定された場合は、起動/停止の操作は保証できません。

- ユーザ固有の情報にアクセスするアプリケーション
  - ユーザ環境変数
  - ネットワークドライブ
  - ネットワークプリンタ
  - ショートカット
- GUIアプリケーション (画面付きアプリケーション)
- 対話型の操作を必要とするコマンド
- Scheduleサービス (ATコマンド)から起動して動作しないアプリケーション
- 上記のようなアプリケーションを起動するバッチファイル
- pauseコマンドを含むバッチファイル

2.4.2.3 アプリケーションの性能を監視する

ネットワーク上に分散された複数のサーバ上に存在するアプリケーションの性能を、アプリケーション管理で集中して監視します。

アプリケーションの性能監視には、以下の2とおりの方法があります。

- 性能異常をイベントとして監視
- 性能情報を表示

性能異常をイベントとして監視

プロセスのCPU使用率などを、しきい値を設定して監視します。しきい値を超える異常が発生した場合には、イベントを通知することができます。しきい値監視するアプリケーションの性能値を以下に示します。

- CPU使用率:
  現在起動中プロセスのCPU使用率
- 仮想メモリ容量:
  確保している仮想メモリのサイズ

性能情報の表示

アプリケーションのCPU使用率やメモリ容量などの性能情報を表示します。表示する性能値を以下に示します。

- 起動経過時刻(プロセスが起動してからの経過時刻)
- CPU使用率(対象プロセスが使用しているCPUの使用率)
- 仮想メモリ容量(プロセスが確保している仮想メモリサイズ)

さらに、性能情報をグラフ表示することも可能です。グラフは、収集された性能値がしきい値とともに表示され、負荷状況の推移などがひと目で確認できます。グラフ表示する性能値を以下に示します。

- CPU使用率(対象プロセスが使用しているCPUの使用率)
- 仮想メモリ容量(プロセスが確保している仮想メモリサイズ)



UNIX版を使用する場合の注意事項

シェルスクリプトの性能異常をイベントとして監視、性能情報を表示はすることはできません。

2.4.3 業務の監視

基幹系業務やOA系業務などは、複数のノードやアプリケーションから構成されているため、業務が正常に稼働するためには、これらすべてが正常に稼働している必要があります。

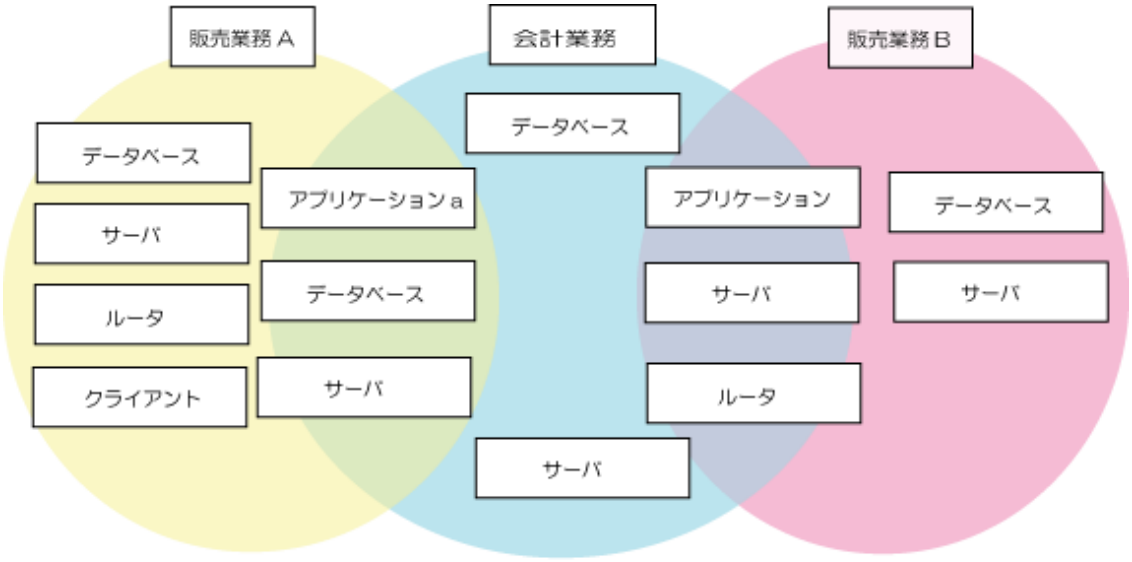
ここでは、監視対象のノードやアプリケーションなどを管理者が監視する単位でグループ化したものを業務、業務を構成するシステム、ネットワーク、アプリケーションなどをオブジェクトと呼び、業務を構成するこれらのオブジェクトを業務単位で監視できます。

業務単位での監視により、以下のようなことが可能となります。

- 複雑に構成された業務でも、業務を構成するオブジェクトのどれかで異常が発生した場合に、どの業務に影響があるのか容易に把握可能
- どれかのオブジェクトで異常が発生した場合、その影響度を容易に把握可能
- 異常発生時の影響度を把握し、適切な優先度で復旧処理を行うことが可能

トラブル発生時の、業務への影響範囲を把握する例を“業務の監視の例”に示します。

図2.7 業務の監視の例



1. “アプリケーション a” でトラブルが発生する。
2. “アプリケーション a” を使用する “販売業務 A” と “会計業務” に影響があることが通知される。
3. すぐに “販売業務 A” と “会計業務” の利用者へ通知し、復旧処理を開始。
4. “販売業務 B” には影響がないので、業務続行が可能。

業務は以下のオブジェクトと関連する項目で構成されます。

- システムやネットワークのノード
- アプリケーション
- データベース
- ほかの業務(別に定義した業務)
- 管理者
- ワークユニット(Interstage上で作成された業務)

業務の監視では、障害の発生による以下の影響範囲を把握できます。

- 障害の影響を受ける業務の把握
- 障害の影響を受けるオブジェクトの把握

ワークユニット

Interstage Application Serverと連携することで、Interstageの監視をSystemwalker Centric Managerで行うことができます。詳細については、“Systemwalker Centric Manager Interstage Application Server 運用管理ガイド” を参照してください。

グローバルサーバ上のワークユニット/オブジェクトの監視

Systemwalkerコンソールから、グローバルサーバ上のサブシステムやInterstageのワークユニットなどを、業務として監視することができます。

Systemwalker Centric ManagerではInterstageと連携することにより、ワークユニットおよびオブジェクトについて、以下の機能を使用できます。グローバルサーバの業務を監視できるのは、主監視パスで接続しているときのみです。

グローバルサーバの業務を監視する場合は、Systemwalker Centric Manager GEEで監視することができます。Linuxでは監視することはできません。

- グローバルサーバ上で動作するワークユニット、およびオブジェクトの表示

  グローバルサーバ上で動作するワークユニット、およびオブジェクトを検出し、構成を表示します。

- グローバルサーバ上で動作するワークユニット、およびオブジェクトの稼働監視

  グローバルサーバ上で動作するワークユニット、およびオブジェクトの稼働状態を表示します。グローバルサーバ上で動作するワークユニットの異常終了を画面にアラーム通知します。

- グローバルサーバ上で動作するワークユニット、およびオブジェクトの性能情報の表示

  待ちメッセージ数、累積処理件数が表示できます。

障害の影響を受ける業務の把握

システムやネットワーク、アプリケーションなどで異常が発生したとき、どの業務に影響があるのかを、以下のように簡単に把握できます。

- システムやネットワークなどで異常が発生すると、影響を受ける業務が、異常として監視画面に通知されます。
  - 監視画面では、異常が通知された業務を選択し、どのオブジェクトが異常の原因かを調査することができます。対象業務の管理者として定義された人へ、イベントの内容を通知することができます。
  - 管理者への通知は、E-mailなどで行うことができます。

障害の影響を受けるオブジェクトの把握

システムやネットワーク、アプリケーションなどで異常が発生したとき、さらに関連して影響を受けるシステムやネットワーク、アプリケーションなどを把握できます。あらかじめ定義された関係により、異常が発生して影響を受ける範囲と、その影響度が監視画面に表示されます。

影響度は以下のように表示されます。

- イベントが発生したオブジェクト
- 重大な影響があるオブジェクト
- 軽度の影響があるオブジェクト

影響度の確認により、障害復旧作業の優先度を判断することができます。

2.4.4 管理者への通知

イベント監視が監視するメッセージの通知を契機として、メールなどによる管理者への自動通知などのアクションを自動的に実行することができます。アクションとしてあらかじめ復旧コマンドを設定しておき、特定のトラブル発生時に、自動的に復旧コマンドを起動し、対処を自動化することもできます。

詳細については、“自動アクション”を参照してください。

2.4.5 Systemwalker自身の監視

Systemwalker Centric Managerでは、Systemwalker Centric Managerの運用中に発生するSystemwalker自身のトラブルを早期発見するために、Systemwalker自身を監視する以下の機能を提供しています。

イベントのスローダウン監視

運用管理サーバ上で、Systemwalker Centric Managerの監視メッセージ、または監視イベントの通知時に、イベントの大量発生などによる通知の遅延が発生した場合、遅延したことをSystemwalkerコンソールに通知する機能です。

Systemwalkerのプロセス監視

Systemwalker Centric Managerが動作しているサーバで、Systemwalker Centric Manager自身のプロセスが正常に稼働しているかを一定間隔で監視し、プロセスの稼働違反（起動されているべきプロセスが存在しない）を検出した場合、Systemwalkerコンソールに通知する機能です。

Systemwalkerのセルフチェック

プロセス監視では、検知できないOS異常やハード障害などのシステム異常時にSystemwalker Centric Managerが停止した場合、Systemwalker Centric Managerの異常として検知する機能です。

Systemwalkerセルフチェックスクリプトを使用して監視をします。

イベントトレース

表示されるべきイベント（メッセージ）が表示されない場合に、Systemwalker Centric Managerのイベント監視機能の動作を確認します。

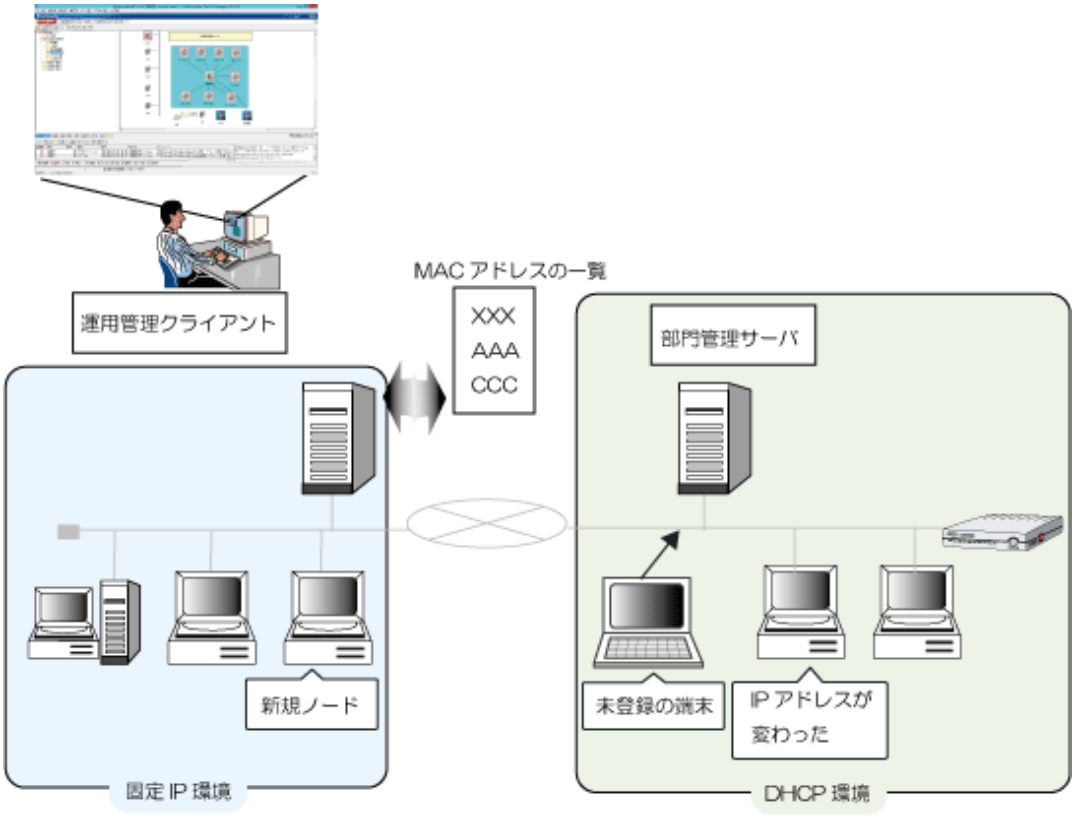
IPC資源の一元管理

Systemwalker Centric Managerが使用するIPC資源について、使用状況を確認します。

IPC資源を回収できなかった場合には、その旨のメッセージをシスログ に出力して通知します。さらに、IPC資源状態表示コマンドにより、回収できなかった IPC資源情報を確認します。

2.4.6　ノードの変更監視

ノードの変更監視は、ノードの変更を定期的に監視し、新たなノードの検出、IPアドレスの変更、ノードの削除、および許可されていないノードがネットワークに接続したことを監視します。
また、MACアドレスを監視し、許可されていないMACアドレスを持つノードがネットワークに接続したことを監視します。

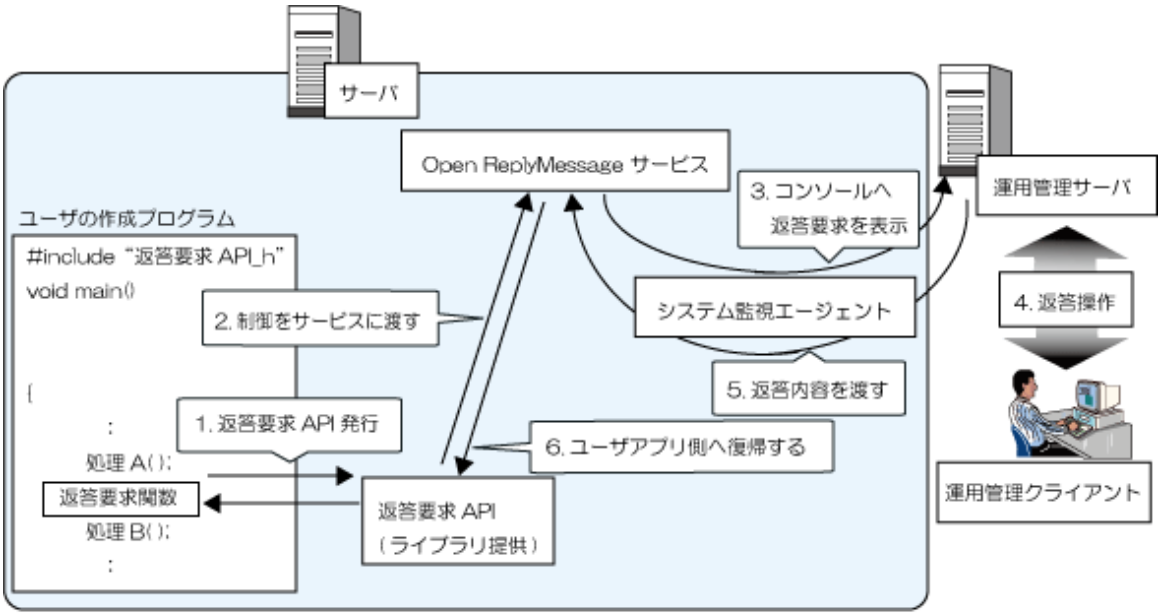


2.4.7　メッセージ返答要求・返答操作【Solaris版/Linux版】

メッセージ返答要求・返答操作は、ユーザが作成したプログラム中でオペレータの返答が必要な処理がある場合、ユーザが作成したプログラムから返答要求メッセージを発行し、返答要求メッセージに対して、オペレータから返答を行うことができます。
以下にメッセージ返答要求・返答操作の概要を示します。

注意

Solaris版の運用管理サーバ・部門管理サーバは、Systemwalker Centric Manager V15.1.1までの提供です。



返答メッセージ機能(Open ReplyMessageサービス)が、Systemwalkerの1機能として提供されます。

1. ユーザが作成したプログラム中でオペレータの返答が必要な処理がある場合、ユーザが作成したプログラムから返答要求APIを発行する。
2. 返答要求APIは必要な情報をOpen ReplyMessageサービスへ渡し、返答待ちとなる。
3. 返答要求APIが発行されると、運用管理サーバのコンソール画面へ必要な情報を表示する。
4. 運用管理クライアントより、Systemwalkerコンソールに表示されたメッセージを選択して、返答画面を表示し、返答画面よりオペレータがメッセージに対する返答操作を行う。
5. オペレータによる返答内容を運用管理サーバからシステム監視エージェントに渡し、システム監視エージェントからOpen ReplyMessageサービスに渡す。
6. Open ReplyMessageサービスは返答内容をもって返答要求APIを復帰させる。

返答メッセージ機能を利用する場合、上位システムは、Solaris版/Linux版のSystemwalkerがインストールされる必要があります。また、リモートコマンドが動作する必要があります。

自動返答機能

返答要求メッセージに対し、自動的に返答を行うことができます。詳細については、“Systemwalker Centric Manager使用手引書 監視機能編” の“メッセージに返答する”を参照してください。

2.4.8 イベントから連携製品の状況確認

Systemwalkerコンソールの監視イベント一覧に表示されたメッセージの内容に応じた障害の調査、状況の確認をするために、イベントから連携製品の詳細画面を直接呼び出します。連携製品の呼び出しは、メッセージのイベント種別に定義されたコマンドを呼び出すことで関連付けられた画面を起動することができます。
定義コマンドには、URLまたはアプリケーションの実行を指定することができ、メッセージ本文のテキストをパラメタとして渡し、連携製品側でメッセージを解析し異常が発生したリソースの詳細画面を呼び出します。

連携製品については、“連携製品一覧”を参照してください。

2.4.9 Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントの監視

Systemwalker Centric Managerのエージェントを導入していないサーバ/クライアントを監視することができます。

Systemwalker Centric Managerのエージェントを導入していない監視対象を、インストールレス型エージェントと呼びます。

2.4.9.1 監視対象

インストールレス型エージェントとして監視できるのは、以下に記載するOSが動作するサーバ、および、クライアントです。

- 監視できるインストールレス型エージェントのOS

なお、Systemwalker Centric Managerのエージェントが導入されているサーバ/クライアントでも、以下の条件を満たしている場合、監視することができます。

- Systemwalker Centric Managerのエージェントが導入されているサーバ/クライアントのメッセージ送信先システムの定義にインストールレス型エージェント監視を行う監視サーバ(運用管理サーバ/部門管理サーバ)を設定していない場合

2.4.9.2 サポート機能

インストールレス型エージェントの場合、以下の機能を使用できます。

システム監視

インストールレス型エージェントでサーバ/クライアントのシステム監視機能を利用する場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

	インストールレス型エージェント		インストール型エージェント
	非デプロイ方式	デプロイ方式	
シスログ/イベントログ監視	○(注1)(注2)	○(注2)	○
リモートコマンド	○	○	○
ログファイル監視	×	○(注3)	○(注3)
メッセージフィルタリング	×	×	○
運用形態名	×	×	○
共有ディスク上のログファイル監視	×	×	○

○：監視可能

×：監視不可

注1)

Hyper-Vのイベントログは監視できません。

注2)

カスタムイベントログは監視できません。

注3)

監視対象のファイルについて以下の違いがあります。

	インストールレス型エージェント	インストール型エージェント
監視可能なファイル数	20個	200個
監視可能なファイルの文字コード	システムの動作コードが監視可能	システムの動作コード、EUC、SJIS、UTF-8を監視対象ファイルごとに選択可能

シスログ/イベントログ監視

インストールレス型エージェントでサーバ/クライアントのシステムログ/イベントログを監視する場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

	インストールレス型エージェントの場合	インストール型エージェントの場合
監視間隔	一定時間間隔で情報を取得し、監視します。	リアルタイムで監視します。
メッセージの監視	インストールレス型エージェントのサーバの設定をしたあとに発生したメッセージが監視対象になります。	インストール後に発生したメッセージが監視対象になります。
転送されたシスログ/イベントログ	シスログ/イベントログの転送で通知された他システムのメッセージは監視対象外です。	
メッセージに付加されるホスト名	メッセージに付加されるホスト名は、監視ポリシーで設定したホスト名になります。(注)	メッセージに付加されるホスト名は、[通信環境定義]ダイアログの[自ホスト名]タブの内容に従って付加されます。
セキュリティイベントログ【Windows】	Windowsのセキュリティイベントログを監視対象からはずすことができます。	
コード系【UNIX】	監視できるコード系は、Systemwalker Centric Managerでサポートしている範囲です。 ・ EUC、SJIS、UTF-8、C	
大量イベント発生時の回避処理	監視間隔ごとに最新の1000件(2MBまで)です。	-

注)

監視ポリシーの設定については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“インストールレス型エージェント監視”を参照してください。

シスログ監視において、監視するデフォルトのシスログのファイルは以下のとおりです。

	通常時	シスログのローテートが発生したとき
Linux	/var/log/messages	/var/log/messages.1 /var/log/messages.01 /var/log/messages-YYYYMMDD(注1)
Solaris	/var/adm/messages	/var/adm/messages.0 /var/adm/messages-YYYYMMDD(注1)
HP-UX(注2)	/var/adm/syslog/syslog.log	/var/adm/syslog/OLDsyslog.log /var/adm/syslog/syslog.log-YYYYMMDD(注1) /var/adm/syslog/syslog.log.0
AIX	/var/adm/messages	/var/adm/messages.0 /var/adm/messages-YYYYMMDD(注1)

注1)

「YYYYMMDD」は8文字の年月日文字列です。

例)

20101120

注2)

HP-UXのsyslogdが「-v」オプションで起動している場合、ホスト名に付加されるファシリティ情報はメッセージに含まれません。

【システムログの出力内容】

```
Oct 18 20:29:44 3B:hostname root: test message
```

「-v」オプションにより、ファシリティ情報(上記の場合「3B:」)が追加されます。

【監視後のメッセージテキスト】

```
root: test message
```



注意

- ローテートしたときのファイル(messages.1など)はテキスト形式(アーカイブでない)のみ監視されます。
- シスログのローテートが発生した場合の監視対象のシスログは、以下の2つです。
  - ・ 現在更新されているファイル
  - ・ ローテートが発生し、ファイル名が変更になった1世代前のファイル

  2世代以上前のファイルは監視対象外となります。
  1世代前のログが切り替わる前に収集するように監視間隔を設定してください。

リモートコマンド

トラブルが発生した監視対象のサーバに対して、リモートからコマンドを投入し、復旧操作を行えます。
リモートコマンドを発行できるノードは、監視ポリシーの配付先に設定したサーバです。

インストールレス型エージェントの場合でも、インストール型エージェントを導入した場合と同様の機能が使用できます。

ログファイル監視

インストールレス型エージェント(デプロイ方式)でサーバ/クライアントのログファイル監視をする場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

	インストールレス型エージェント(デプロイ方式)	インストール型エージェント
監視ファイルのMAX数	20ファイル	200ファイル
監視間隔(秒)	30 (30～3600で設定可能)	30 (1～3600で設定可能)
ファイルタイプ	テキストファイル	
出力方法	追加型	
ログファイルのコード系	システムの動作コードと同じ	システムの動作コード、EUC、SJIS、UTF-8を監視対象ファイルごとに選択可能
ファイル監視の初回	導入後に発生したメッセージから監視します。	ファイルの先頭から監視します。【Windows版】 最新の500件までさかのぼって監視します。【UNIX版】
扱うメッセージの最大長	2047byte	
大量イベント発生時の回避処理	監視間隔ごとに最新の1000件です。	－

	インストールレス型エージェント(デプロイ方式)	インストール型エージェント
ログ切り替わり判定基準	以下の条件のとき、ログファイルの先頭から監視します。 ・ファイルサイズが減少 ・ファイルサイズが0byte ・ファイルが存在しない	
ファイル名が途中で変わるログファイルの監視（監視ファイル名格納ファイル）	×	○
opafmonext(ログファイル監視拡張コマンド)	×	○
mpopfmcsv(監視ログファイル定義のCSV入出力コマンド)	×	○

○：使用できます。
×：使用できません。

インベントリ情報の収集

インストールレス型エージェントでサーバ/クライアントのインベントリ情報を収集する場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

【Windows版】

	インストールレス型エージェント		インストール型エージェント
	非デプロイ方式	デプロイ方式	
ハードウェア情報(注1)	○	○	○
ユーザ情報	×	×	○
ソフトウェア情報(注1)	○	○	○
レジストリ収集情報	×	○(注2)	○
テキスト情報	×	×	○
ソフトウェア辞書情報収集(Windows系OS用)	×	○(注2)	○

【UNIX版】

	インストールレス型エージェント		インストール型エージェント
	非デプロイ方式	デプロイ方式	
ハードウェア情報(注1)	○	○	○
ユーザ情報	×	×	○
ソフトウェア情報(注1)	△	△	△
テキスト情報	×	×	○
ソフトウェア辞書情報収集(UNIX系OS用)	△	△	△

○：使用できます。
△：収集対象のOSがSolaris/Linuxの場合にだけ使用できます。
×：使用できません。

注1)

ハードウェア情報/ソフトウェア情報の一部の情報は、収集不可、または収集内容がエージェント導入の場合と異なる場合があります。

また、Nano Serverの場合は収集できません。

注2)

収集に時間がかかるため、インベントリ収集コマンドで収集することを推奨します。

アプリケーション監視

インストールレス型エージェント(デプロイ方式)でサーバ/クライアントのアプリケーション監視をする場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

	インストールレス型エージェント(デプロイ方式)	インストール型エージェント
アプリケーションの稼働違反監視	○	○
アプリケーションのプロセス数違反監視	○	○
アプリケーションの性能しきい値監視	×	○
アプリケーションの性能取得	×	○
アプリケーションの性能グラフ表示	×	○
スクリプトによるアプリケーションの稼働監視	×	○
スクリプトによるアプリケーションのプロセス数監視	×	○
アプリケーションの稼働違反時プロセス制御	×	○
アプリケーションのプロセス制御	×	○
アプリケーションの稼働状態表示	×	○
アプリケーションの最新稼働状態の取得	×	○
アプリケーションの稼働違反抑止/再開	×	○
アプリケーションの自動検出	×	○
Interstageワークユニットの稼働監視	×	○
クラスタサービスの監視	×	○

○：監視可能
×：監視不可

ただし、監視可能(○)とされている場合でも、監視対象システムのOSがHP-UXで、監視対象アプリケーションがシステムコールを発行してカーネルモードで動作中の場合は監視できません。アプリケーション監視は、psコマンドの出力結果により、稼働監視を行っています。アプリケーション監視のサービスが、psコマンドを発行したときに、監視対象アプリケーションがシステムコールを発行していた場合、その監視対象アプリケーションは、停止中として検知されます。システムコールを発行し、カーネルモードで動作中のプロセスは、システムコールが復帰するまで監視できません。

サーバ性能監視

インストールレス型エージェント(デプロイ方式)でサーバ性能監視をする場合、エージェント機能をインストールした場合と比べ、以下の差異があります。

	インストールレス型エージェント(デプロイ方式)	インストール型エージェント
ノード詳細表示	×	○

	インストールレス型エージェント(デプロイ方式)	インストール型エージェント
ヒストリ表示	×	○
ノード中心マップ/ペアノード経路マップ(サーバ性能情報)	×	○
しきい値監視 －CPU使用率 －実メモリ使用率 －ディスク使用率	○ イベント自動対処は不可 復旧イベントにて代替	○
しきい値監視 －ページフォルト数 －ディスクビジー率 －実メモリ空き容量 －ページファイル使用量 －ページファイル空き容量 －プロセス数 －プロセッサ待ちスレッド数 －ディスク空き容量 －HD待ち要求数	×	○
性能情報出力（サーバ性能情報）	×	○
論理ディスク単位、ストレージプール単位の監視(mptrfbypartコマンド)	×	○
サーバ性能MIB	×	○

○：監視可能
×：監視不可

クラスタ運用時

・ 被監視システムがクラスタ運用している場合

機能名	運用方法
システム監視	それぞれのノードを個別に監視します。(注) ノード一覧にクラスタ名、運用形態名は表示されません。 共有ディスク上のログファイル監視はできません。
インベントリ収集	それぞれのノードに対して個別にインベントリ収集を実施してください。
アプリケーション監視	それぞれのノードを個別に監視します。
性能監視	それぞれのノードを個別に監視します。

注)

AIXでクラスタ運用する場合

－ Systemwalkerコンソールの被監視システムのノードプロパティにおいて、[ネットワーク]タブの[ホスト名]には、永続ノードIPラベルに対応したホスト名を設定してください。

- 監視サーバで、AIXを監視する監視ポリシーを配付する前に、インストールレス型エージェント監視のクラスタノード定義ファイル(als_clshosts)を用意してください。

  定義するホスト名は上記で設定した永続ノードIPラベルに対応したホスト名を設定してください。インストールレス型エージェント監視のクラスタノード定義ファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

2.5 障害復旧

Systemwalker Centric Managerで行う、障害復旧までの対処について説明します。障害復旧までの対処には、以下の方法があります。

- リモートから復旧操作する
  - リモート操作
  - リモートコマンド
  - リモートからの電源制御
- 障害への対処を自動化する
  - 自動アクション

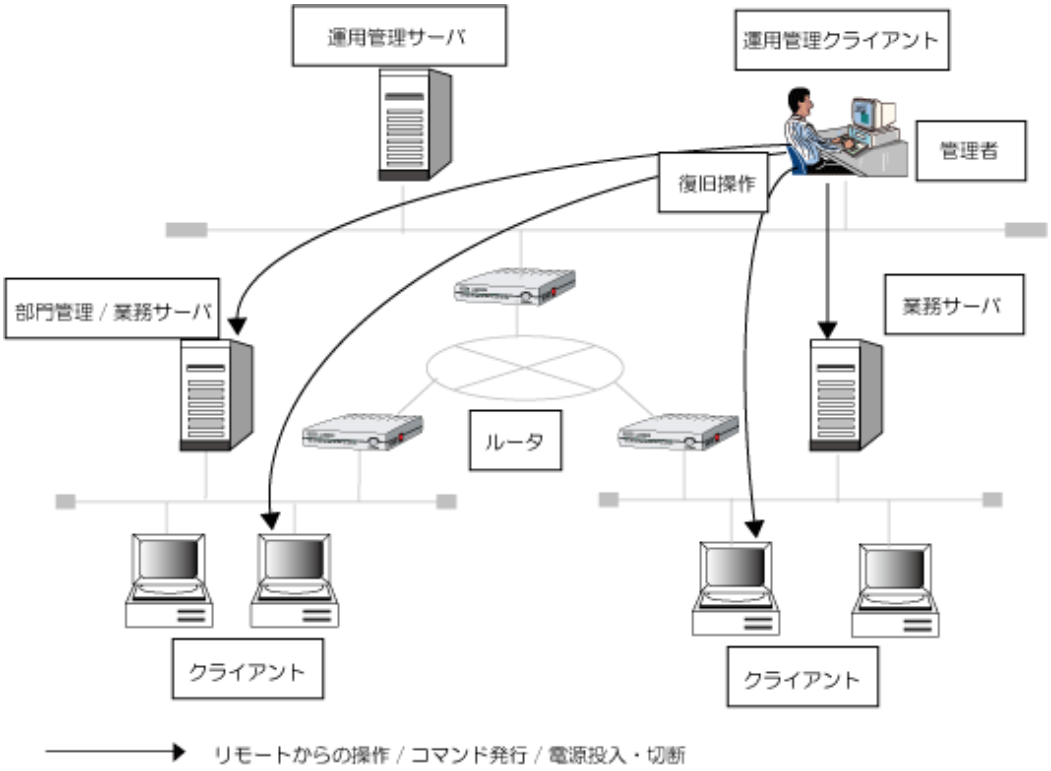
2.5.1 リモートから復旧操作する

障害が発生したシステムの復旧作業をリモートから効率良く行うことができます。リモートからの復旧操作には、以下の方法があります。

- リモートから操作する
- リモートからコマンドを発行する
- リモートから電源を投入・切断する

障害発生時の復旧操作を“障害の復旧操作”に示します。

図2.8 障害の復旧操作



また、障害復旧の操作対象を以下に示します。

復旧操作の種類	部門管理/業務サーバ			クライアント	備考
	Windows	UNIX	Linux		
リモートからの操作	○	×	×	○	リモート操作機能がインストールされている必要があります。 (注1)
リモートからのコマンド発行	○	○	○	×	イベント監視機能がインストールされている必要があります。
リモートからの電源制御	○	△(注2)	○	○	リモート電源制御機能がインストールされている必要があります。

○：操作可能
△：一部操作可能
×：操作不可

注1)

リモート操作機能は、パブリッククラウドでは使用できません。

注2)

Solarisの場合は実行可能です。ただし、Solaris版の運用管理サーバ・部門管理サーバは、Systemwalker Centric Manager V15.1.1までの提供です。
HP-UXおよびAIXの場合は実行できません。

2.5.1.1 リモート操作

遠隔地のシステムで障害が発生した場合、リモート操作により、管理者が自席から復旧操作が可能です。

リモート操作では、管理者が、トラブルの発生したサーバやクライアントの画面を自席で参照し、サーバやクライアントと画面を共有して復旧操作が可能です。リモート操作は、障害の復旧操作のほかに、遠隔地のクライアントに対するサポートや、操作説明などにも使用できます。

リモート操作による復旧操作は、Windowsのサーバとクライアントが対象です。

ただし、Server Core環境では、リモート操作機能は動作しません。Server Core環境にSystemwalker Centric Managerを導入する場合、リモート操作機能を選択せずにインストールしてください。
なお、リモート操作機能をインストールした場合、OS起動時に以下のリモート操作機能に関するイベントログが出力されますが、OSの動作に問題を引き起こすことはありません。

```
Log Name: Application
Source: LHCTLSVC
Event ID: 1002
Level: 情報
Description:
Information : Live Help Control Service was started.
```

このイベントログを表示しないようにするには、以下のコマンドを実行して、リモート操作機能をアンインストールしてください。

・ リモート操作エキスパートの場合

```
Systemwalkerインストールディレクトリ¥MPWALKER.DM¥dmunins¥mplhlpex¥setup.exe /exp
```

・ リモート操作クライアントの場合

```
Systemwalkerインストールディレクトリ¥MPWALKER.DM¥dmunins¥mplhlpcl¥setup.exe /cli
```

リモート操作では、復旧操作される側をリモート操作クライアントと呼びます。

復旧操作するには、リモート操作エキスパートとリモート操作モニタの2種類があります。これらは、以下の特徴があります。

機能	リモート操作 エキスパート	リモート操作 モニタ
復旧操作画面の複数同時起動(最大8個まで)	×	○
セッション開催	○	×
リモート操作クライアントへの画面送信	○	×
復旧操作画面の縮小表示	○	○
リモート操作クライアントとの同時動作	×	○

○: 実行できる
×: 実行できない

リモート操作クライアント

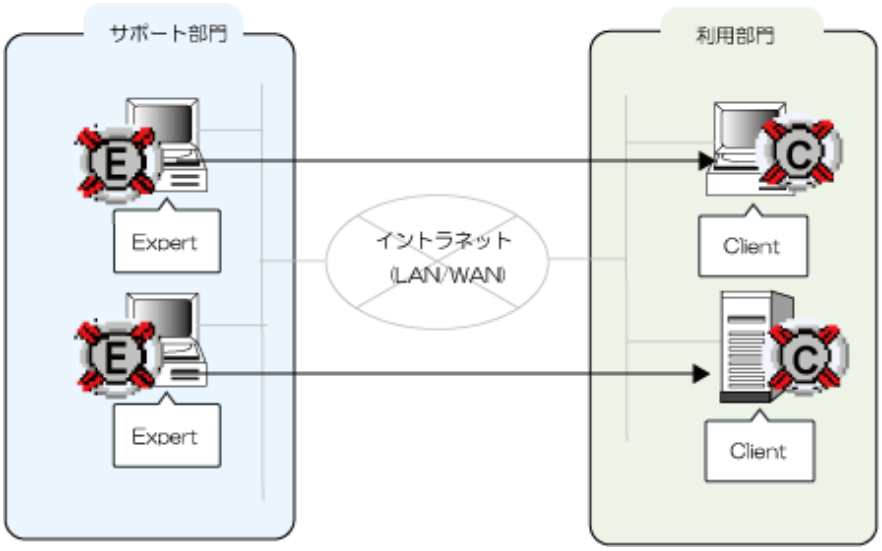
復旧操作されるクライアントには、導入時にリモート操作クライアントをインストールします。Windowsの部門管理/業務サーバに対しても、リモート操作クライアントをインストールすることで、復旧操作が可能になります。

リモート操作エキスパート

リモート操作エキスパートは、ほかのエキスパートの支援を必要とする場合や、相談したい場合には、ほかのリモート操作エキスパートのセッションに参加することができます。

リモート操作の運用方法

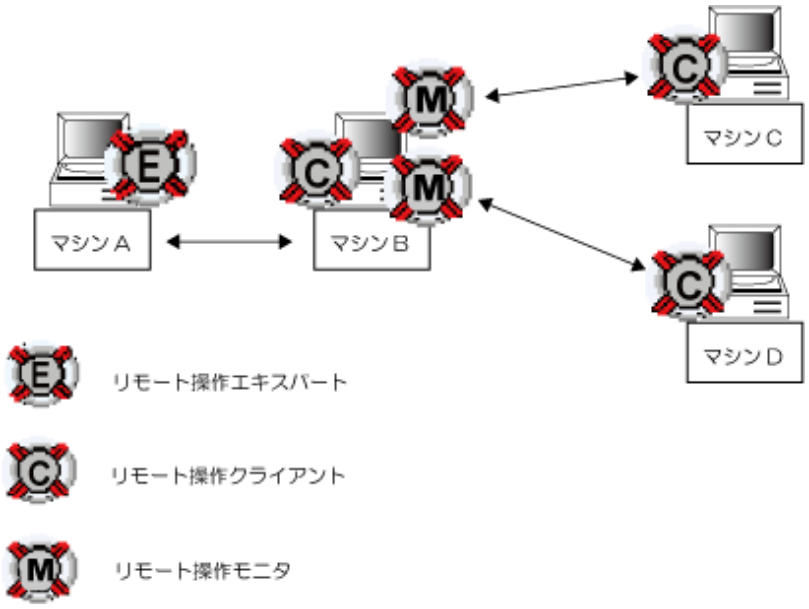
リモート操作による復旧操作は、問題の発生したクライアントが、サポート要請を起動します。エキスパートが問題の発生したシステムのIPアドレスを直接指定してセッションが始まります。クライアント側はリモート操作の操作方法を知る必要はなく、エキスパート側からクライアントを操作して問題を解決します。



リモート操作モニタとリモート操作クライアントの接続

リモート操作モニタは、1つの端末から複数起動し、同時に操作することができます。

リモート操作モニタとリモート操作クライアントを同時に起動し、中継コンピュータとします。中継コンピュータを使用して画面転送やリモート操作を実施できます。このように、中継コンピュータを使用して遠隔地のクライアントを接続する方法をチェイン接続といいます。



リモート操作での復旧操作

リモート操作では、エキスパートが、以下の操作によりクライアントで発生したトラブルの復旧操作を行います。

クライアントのリモート操作

セッションが始まると、自動的にクライアントの画面がエキスパートに送信され、クライアントをリモート操作できる状態になります。エキスパートとクライアントは電話で話をしながら、クライアントの画面を一緒に操作して、即座にその結果を双方で見ることができます。そこでは、クライアントのコンピュータの前にいるようなイメージで、自分のキーボードやマウスを使ってクライアントのアプリケーションやデスクトップを操作することができます。

セッションにほかのエキスパートが参加している場合、そのエキスパートはリモート操作されているセッションを見ることができます。ただし、同時には1人のエキスパートしかリモート操作権を持つことができませんので、必要に応じてリモート操作権を移して操作します。

リモート操作エキスパート画面の送信

リモート操作エキスパートは、クライアントの画面を受信するだけでなく、自身の画面をリモート操作クライアントに送信することもできます。クライアントにエキスパートの画面を見せて説明したい場合は、エキスパートの画面を送信して、エキスパートの画面に表示されるマウスの動きを含めたすべての内容をクライアントに見せることができます。

セッションにほかのエキスパートが参加している場合は、そのエキスパートも画面を見ることができるので、エキスパートどうしでの検討もできます。

情報の送信

リモート操作エキスパートからクライアントにトラブル解決のための情報として、ファイル、テキストメッセージ、またはクリップボードの内容を送受信することができます。

2.5.1.2 リモートコマンド

遠隔地のシステムでトラブルが発生した場合に、監視対象のサーバに対して、リモートからコマンドを投入し、復旧操作が可能です。

リモートコマンドは、リモートからGUI操作するリモート操作に比べ、ネットワーク上の転送データ量が少なくて済むため、低速回線を利用している場合や、簡単なトラブル復旧に有効です。

また、リモートコマンドグループとしてコマンドをグループにして登録し、利用することができます。これにより、一連の操作を繰り返し行う場合、操作ミスを防止し、操作の利便性を向上させることができます。

リモートコマンド実行時のユーザは以下のとおりです。

・ インストール型エージェント

発行先のシステムごとに以下のようになります。

	V13.2.0以前		V13.3.0以降	
	運用管理サーバ	運用管理サーバ以外	運用管理サーバ	運用管理サーバ以外
UNIX版	通信環境設定の[コマンドユーザ]に指定されたユーザ。デフォルトはrootです。	通信環境設定の[コマンドユーザ]に指定されたユーザ。デフォルトはrootです。	通信環境設定の[コマンドユーザ]に指定されたユーザ。デフォルトはrootです。	通信環境設定の[コマンドユーザ]に指定されたユーザ。デフォルトはrootです。
Windows版	インストール時に指定したスタートアップアカウント	インストール時に指定したスタートアップアカウント	インストール時に指定したスタートアップアカウント	ローカルシステムアカウント

・ インストールレス型エージェント

[インストールレス型エージェント監視]画面で指定したログオンアカウント。インストールレス型エージェントではデフォルトのアカウントはありません。

リモートコマンドは、下記いずれかのシステムに対して発行することができます。

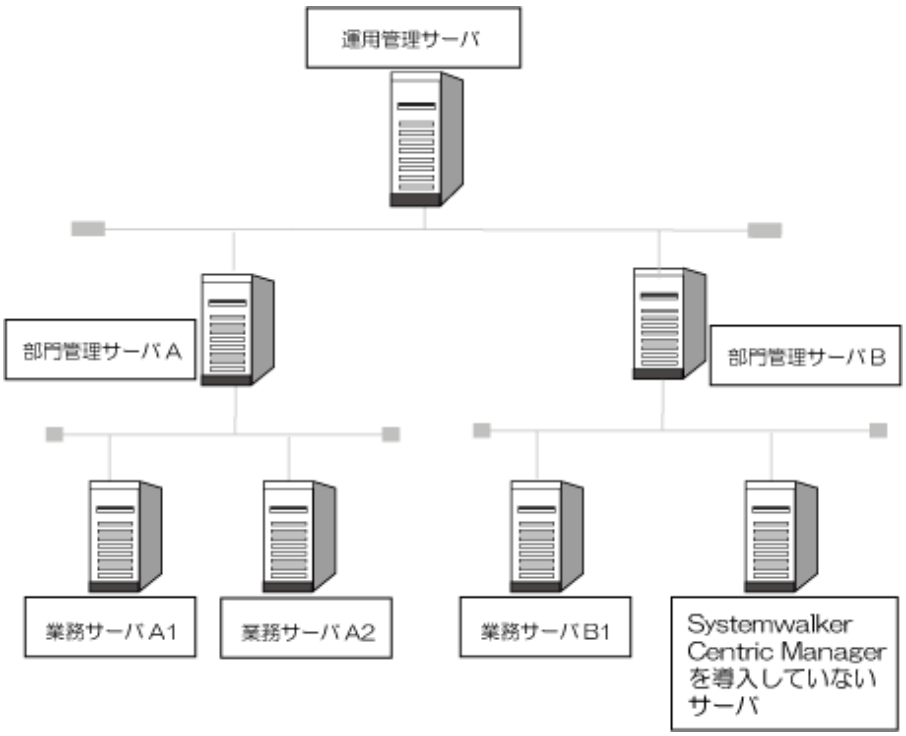
・ 自システム

・ 論理的通信構造によって接続している（イベント通知先に自システムまたは自システムへの中継システムを定義している）、自システムの下位システム

下位システムがクラスタ構成の場合は、物理ノードに対して発行可能です。論理ノードに対して発行することはできません。

・ インストールレス型エージェントでSystemwalker Centric Managerを導入していないシステム

下記の構成となっている場合、部門管理サーバAからリモートコマンドの発行対象にできるのは、部門管理サーバAと業務サーバA1、A2になります。



2.5.1.3　リモートからの電源制御

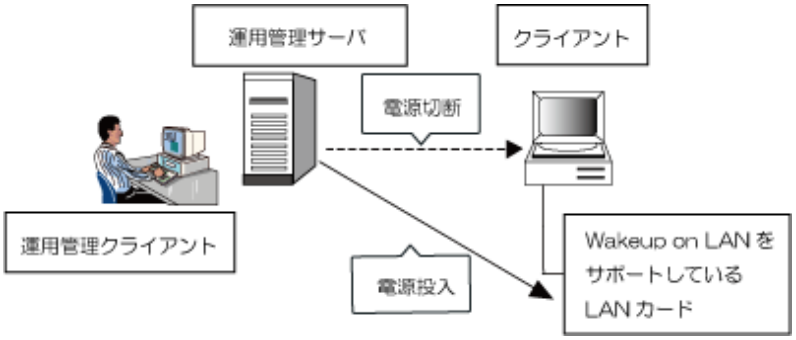
リモート電源制御により、遠隔地のクライアントの電源制御を行います。

クライアントの電源投入/切断

リモート電源制御により、遠隔地のクライアントの電源を投入/切断することができます。

障害復旧時の利用だけでなく、リモートからクライアントの電源を投入することができるため、会社が休みの日であっても資源配付機能などを利用して一斉にソフトウェアを配付することができます。

リモート電源制御による、電源投入は、Wakeup on LAN対応しているクライアントに対して可能です。また、クライアントの電源切断は、Windowsから電源切断のできるクライアントで、Systemwalker Centric Managerのクライアント機能がインストールされている場合に可能です。



2.5.2　障害への対処を自動化する

同様の障害が繰り返し発生する場合、復旧操作を自動化することが可能です。

2.5.2.1　自動アクション

発生した監視イベントに対してあらかじめ復旧コマンドを設定しておくことで、特定のトラブル発生時に、自動的に復旧コマンドを起動し、自動的に対処することができます。復旧コマンドだけでなく、メールなどによる管理者への自動通知もできます。

このように、監視イベントに対して復旧コマンドや管理者への通知方法を定義しておくことをアクション定義といいます。アクション定義は、イベント監視の条件の1つとして定義します。イベント監視の条件やアクション定義の詳細については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“イベントの対処を自動化する”を参照してください。

自動実行可能なアクションを以下に示します。

- 音声による通知:
  テキスト読み上げ、WAVファイルの再生、またはBEEP音で通知します。
- 電子メール(Microsoft(R)-Mail、E-mail)送信:
  Microsoft(R)-MailまたはE-mailで任意の文書を通知します。
- ポップアップメッセージ通知:
  ポップアップメッセージで任意のメッセージを通知します。
- ショートメール通知:
  ショートメールで任意のメッセージを通知します。
- SNMPトラップ送信:
  SNMPトラップを発行します。
- アプリケーション起動:
  アプリケーションを起動します。
- リモートコマンド発行:
  リモートコマンドを発行します。

・ イベントログ出力:
  イベントログ(アプリケーション)に出力します。

自動アクションは、それぞれのサーバで実行します。

ただし、音声による通知、ショートメール通知、Microsoft(R)-Mail送信、ポップアップメッセージ通知は、UNIXサーバの場合、サーバ自身では実行できません。これらのアクションについては、運用管理クライアント、または、クライアントで実行するように定義します。
また、Microsoft(R)-Mail送信は、Windows NT(R)だけ実行可能です。Microsoft(R)-Mail送信を実行する場合は、バージョンがV12.0L11以前のSystemwalker Centric Managerがインストールされ たWindows NT(R)のホストで実行するように定義します。

自動アクションは、1つのイベントに対して複数定義することができます。

ポイント

アクション管理機能

アクション管理機能では、アクションの実行状況を監視することができます。音声通知、メール送信、ポップアップ、ショートメールの各アクションを監視および操作することができます。

監視したいアクション種別だけを[アクション管理]ウィンドウに表示させることができるので、アクションの実行状況をひと目で監視できます。また、自動アクションの情報は一覧表示だけでなく、自動アクションごとに詳細な情報を表示することもできます。

さらに、実行待ちの自動アクションに対して、実行の一時停止や削除などの操作を行うことができます。実行されるアクションが多いなどの理由で、自動アクションが実行されないときに、自動アクションの実行順序を変更してほかのアクションよりも先に実行させて運用を効率化することができます。

注意

HP-UX版 Systemwalker Centric Manager使用時の注意事項

HP-UXでは、HTTPS、S/MIMEが未サポートのため、これらの機能は使用できません。HP-UX版 Systemwalker Centric Manager使用時には、アクションとして電子メール送信を行う場合、S/MIMEを使用しないでください。

2.5.2.2 ServiceNow連携

自動アクションを活用してServiceNowと連携することができます。

ServiceNow ITSMのIncident Management機能と連携を行い、Systemwalker Centric Managerの監視イベントから、ServiceNow上に新たなインシデントを登録できます。

インシデント登録は、Systemwalker Centric Managerがインストールされたサーバ(運用管理サーバまたは部門管理サーバ)上のServiceNowインシデント登録コマンド(swsn_increg)の実行により、ServiceNowのRESTインタフェースを利用して行われます。

ServiceNowインシデント登録コマンド(swsn_increg)、および、ServiceNow上に作成されるインシデントの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

ServiceNow上に作成されたインシデントは、ServiceNowの運用により処理を実施してください。

以下にシステム構成の例を示します。

図2.9 運用管理サーバからServiceNowにインシデント登録を行う場合

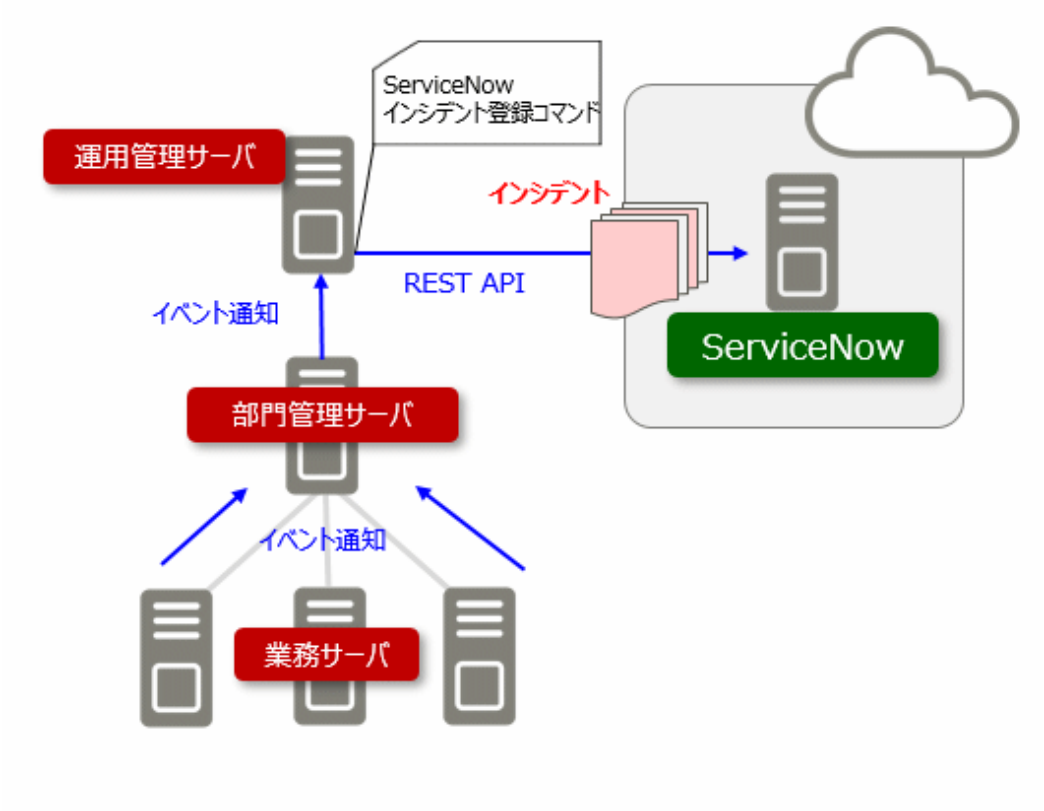
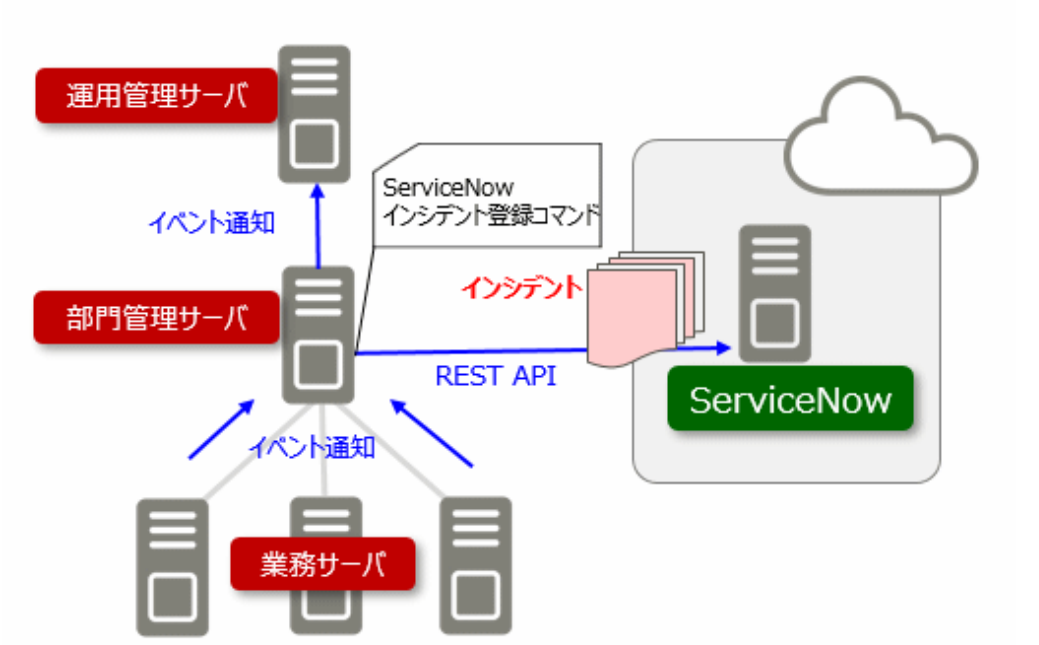


図2.10 部門管理サーバからServiceNowにインシデント登録を行う場合



注意

ServiceNow連携を行う場合の注意事項

インシデント登録の対象とするイベントは、Systemwalker Centric Managerのイベント監視の条件定義によってフィルタリングされたイベントにしてください。イベントを特定する条件を緩和した場合、大量のイベントが

発生した時に、ServiceNowへのインシデント登録の要求が多発し、Systemwalker Centric Managerが動作するシステムの負荷が上がる可能性があります。特定する条件としてホスト名、エラー種別、監視イベント種別など、複数の項目(条件)を組み合わせてフィルタリングするなど、インシデント登録の要求が多発しないように注意してください。

なお、環境によって異なりますが、ServiceNowへ登録するインシデント件数は、1時間あたり30件程度を上限とした運用が目安値となります。

2.6 ソフトウェア修正管理

ソフトウェア修正管理は、富士通が提供するソフトウェア製品の修正をアップデートサイトと連携して管理します。

各サーバのミドルウェア修正適用状況を収集し、アップデートサイトから最新の修正情報を収集することにより、全サーバの修正適用状況を一元管理することができます。

ソフトウェア修正管理の機能を以下に示します。

- 修正適用状況の収集機能

  適用されている修正の情報を、UpdateAdvisor（ミドルウェア）(注)の機能と連携し、収集します。収集した修正情報は、運用管理サーバのデータベース(インベントリデータベース)へ格納します。

- 修正適用状況の表示機能

  インベントリデータベースに格納されている修正適用状況を、[ソフトウェア修正管理]画面より表示します。

- 最新の修正適用状況の取得機能

  各サーバから収集した修正適用状況をもとに、アップデートサイトから最新の修正情報を収集し、各サーバに未適用の修正を検出します。

- 修正適用状況のCSV出力機能

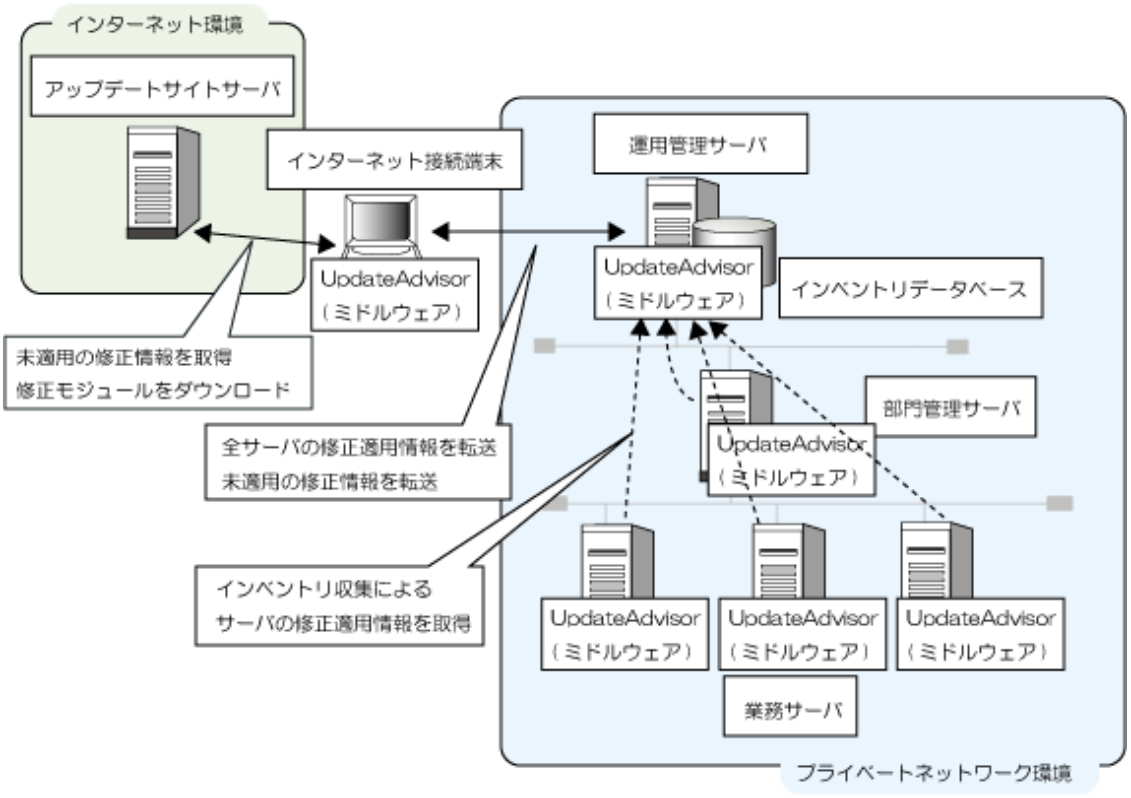
  収集した修正適用状況は、CSVファイルに出力が可能です。この機能により、修正の適用状況をExcel等のデータ管理ソフトを使用して管理することが可能です。

- 修正のダウンロード機能

  サーバに未適用の修正をダウンロードします。運用によって全サーバに未適用の修正を一括してダウンロード、または必要な修正のみ選択してダウンロードすることができます。

- 修正の配付機能

  各サーバに、ダウンロードした未適用の修正を配付します。



なお、詳細については、“Systemwalker Centric Manager 使用手引書 ソフトウェア修正管理機能編”を参照してください。

注)

UpdateAdvisor（ミドルウェア）:アップデートサイトから修正をダウンロードし、コンピュータに適用するためのソフトウェアです。
UpdateAdvisorは、修正情報管理の対象となるすべてのサーバに導入します。

2.7　資源の配付

サーバまたはクライアントで使用するアプリケーションやデータなどの資源を、運用管理サーバで集中管理し、サーバまたはクライアントにオンラインで配付することができます。従来手動で行っていた資源の管理、変更および保守作業からシステム管理者を解放します。

資源配付の設定方法や利用方法の詳細については、“Systemwalker Centric Manager 使用手引書 資源配付機能編”を参照してください。

資源配付機能により、資源を確実に矛盾なく配付することができます。配付前に配付先や配付物、配付方法についての事前定義が必要ですが、一度定義しておくと以降のバージョンアップは容易になります。

資源配付機能は、以下の特長を持っています。

- アプリケーションだけでなく、スクリプトや文書も配付できます。
- 2階層から多階層まで、いろいろな構成で配付が可能です。
- 配付する資源に応じて、配付先をきめ細かく設定できます。
- 配付する資源を、世代管理することができます。
- 適用日(配付した資源が有効になる日)をスケジュールできます。
- 配付する資源に応じて、配付方法を選択できます。

システム構成と資源の流れ

資源配付のシステム構成では、Systemwalker Centric Managerのインストール種別とは別に、次の役割を持つコンピュータが必要になることがあります。

- 中継サーバ

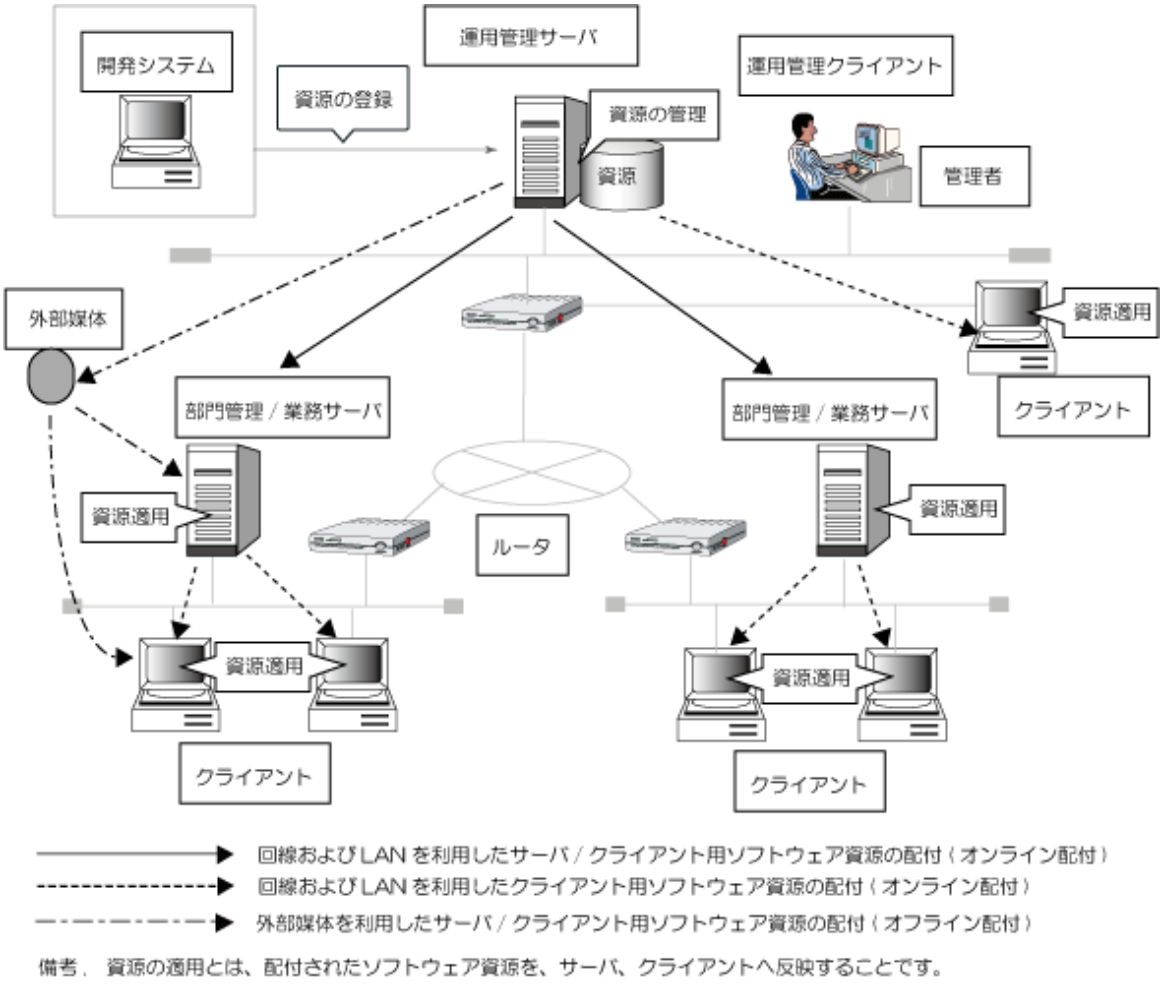
  配付先システムが多い場合、運用管理サーバと部門管理/業務サーバの間に、資源を中継する中継サーバを設置し、多階層で資源を配付することにより、トラフィックを軽減することが可能です。

- 開発システム

  開発した資源を、資源配付のアップロード機能を使用して、運用管理サーバに登録するためのシステムです。登録する資源に合わせてUNIXサーバまたは、Windowsサーバ/クライアントを用意し、Systemwalker Centric Managerを導入する必要があります。

概要を、“資源配付の概要”に示します。

図2.11 資源配付の概要



配付する資源の流れは、次のようになります。

1. 開発システムで配付する資源を作成します。
2. 開発した資源を、資源配付のアップロード機能を使用して、開発システムから運用管理サーバに登録します。
3. 運用管理サーバから部門管理サーバ/業務サーバ/クライアントへ資源を配付します。次の方法が選択できます。

   ー 直接オンラインで配付することができます。

   ー 部門管理サーバや業務サーバを中継して配付することができます。このとき、データを中継する部門管理サーバや業務サーバを中継サーバといいます。

4. 配付先で資源を適用します。

2.7.1 いろいろな資源を配付する

資源配付では、部門管理/業務サーバ、クライアントで使用するさまざまな資源を配付できます。配付する資源は、以下の3種類に分類することができます。

- データ
- アプリケーション
- スクリプト

配付対象の資源の詳細については、“Systemwalker Centric Manager 使用手引書 資源配付機能編”を参照してください。

アプリケーションとスクリプトは、配付するだけでなく、配付後に自動的にインストールや実行することができます。インストールや実行方法の詳細については、アプリケーションの種類やスクリプトの適用時との関係で異なります。

以下、配付する資源について説明します。

データの配付

資源配付機能で、配付/適用できるデータの例として以下のデータがあります。

- CSVファイルなど各種のデータファイル
- アプリケーションが使用する画面/帳票定義、オーバレイなどのプリンタ資源
- グローバルサーバ上の帳票システムと連携している場合のグローバルサーバの帳票

アプリケーションの配付

業務アプリケーションを、運用管理サーバから配付/インストールできます。

アプリケーションの種類により、以下に分類して説明します。

- インストーラがないアプリケーション

  顧客作成の業務アプリケーションなど、ディレクトリに複写するだけで使用可能なアプリケーションです。資源を配付/適用することで、使用可能になります。

- サイレントインストールのアプリケーション

  バッチ処理型のインストーラを起動して、導入するアプリケーションです。資源を配付/適用後に、インストーラを自動起動し、アプリケーションをインストールします。インストーラの自動起動については、“スクリプトの配付”を参照してください。

スクリプトの配付

スクリプトとは、UNIXのシェルスクリプト、および、Windowsのバッチプログラムのことを指します。資源配付では、スクリプトを配付し、配付先で実行することができます。スクリプトの配付には以下の方法があります。

- 資源適用時にスクリプトを実行

  データやアプリケーションなどの資源を適用する前、または適用したあとに、任意のスクリプトを組み込むことができます。前、後スクリプトは、資源の登録時に指定して、資源と同時に配付します。

  インストーラをスクリプトとして、資源適用後に起動させることで、アプリケーションのインストールが可能となります。アプリケーションのインストールについては、“アプリケーションの配付”を参照してください。

- スクリプト単体の配付

  スクリプトだけを資源として配付し、適用時に実行することができます。スクリプトの実行結果は適用結果として管理できます。

2.7.2　配付先システムを選択する

配付する資源の使用目的などに合わせて、資源の配付先と配付方法を選択できます。

- システム全体の一斉配付
- 部門単位の一斉配付
- 特定システムへの配付

メンテナンス版数とは

複数の配付資源を業務などの単位にまとめて、配付することができます。この単位をメンテナンス版数として、配付資源に対する配付結果と適用結果を管理できます。
メンテナンス版数には、システム全体で共通に管理する共通メンテナンス版数と、部門単位や業務単位で管理する個別メンテナンス版数があります。
メンテナンス版数を利用することで、これまでのメンテナンス作業の結果および履歴を把握、管理することができます。また、メンテナンス版数を利用することで、以下の運用が可能となります。

- 部門管理/業務サーバ、クライアントへ、一斉に資源を配付
- サーバとクライアント間で資源適用の同期を保証
- 版数順に適用することにより、資源の適用抜けの防止
- 部門管理サーバおよびクライアント単位で、適用結果の容易な確認

システム全体の一斉配付

全社共通で使用する資源を、一度の配付作業で、システム全体に対して一斉に配付できます。全社共通で使用する基幹業務の資源などを配付する場合に利用できます。

システム全体に一斉に配付する場合は、共通メンテナンス版数を利用して配付します。

部門単位の一斉配付

部門単位や事業所内単位で使用する業務の資源を、業務単位で対象のシステムに一斉に配付できます。特定の部門や、一部のシステムだけで使用する基幹業務の資源などを配付する場合に利用できます。

部門単位で一斉に配付する場合は、個別メンテナンス版数を利用して配付します。

特定システムへの配付

資源単位で、特定のシステムにだけ資源を配付します。特定のシステムにだけ資源を配付する場合は、個別資源として配付します。

部門管理サーバ/業務サーバからの呼び出し配付

部門管理サーバや業務サーバから、運用管理サーバに対して資源の取り出しを要求し、資源を配付することができます。
このとき、HP-UXでは、業務サーバからHTTPSを使用した資源の取り出しはできません。S/MIMEも使用できません。HTTPを使用してください。
また、クライアントからHP-UXの業務サーバに対して、ダウンロード機能を起動する場合も、HTTPSを使用した資源の取り出しはできません。S/MIMEも使用できません。

2.7.3　世代を管理する

資源配付では、配付する資源を運用管理サーバで世代管理しています。配付時に世代をチェックし、配付されていない世代だけを配付することができるので、無駄な資源のダウンロードを防ぐことができます。また、配付されていない世代が複数ある場合には、世代順に適用して世代抜けが発生しないように配付することができます。適用時の世代チェックは自動で行われるため、効率的で確実な資源の配付を実現できます。

資源を累積で適用

複数の世代に分けて累積して登録された資源を、未適用の世代から順に適用します。部分的に修正が発生する業務の資源などは、累積された資源を世代順に適用することで、資源の適用抜けを防ぐことができます。

最新の資源だけ適用(クライアントの場合)

最後に登録された世代の資源だけを適用します。それまでに未適用の世代がある場合でも、最新より前の世代は適用されません。同じ資源が複数の世代に登録されている場合、最新の世代の資源だけが適用されるので、無駄な資源の適用を避けることができますが、最新の世代より前に登録された資源は未適用であっても適用されないので注意が必要です。

2.7.4 適用日をスケジュールする

全社一斉に始まる新規業務の資源、配付してすぐ使用する資源など、業務の運用にあわせて資源の適用のタイミングを指定できます。

適用タイミングの指定

管理者が適用予定日時を指定し配付すると、適用予定日時を経過した資源だけを適用します。適用予定日時は、適用方法を後刻適用として配付する場合に指定できます。

全社一斉に始まる新業務の資源は、新業務開始日を適用予定日時として、新業務開始日以前に資源を配付します。配付された資源は、適用予定日時を経過するまでは適用されません。適用予定日時を経過すると資源が適用され、一斉に新業務を開始できます。

資源の適用方法

- 資源を受信して続けて適用を行う即時適用
- システムの起動を契機に適用するIPL適用
- システムの起動を契機に適用予定日時を超えている資源だけを適用する後刻適用
- 利用者の指示を契機に適用する手動適用

強制配付

強制配付機能により、管理者の指示で強制的に各クライアントへ資源を配付/適用することができます。夜間に業務のレベルアップなどを行う場合には、管理者の指示で強制的にダウンロード/適用ができます。クライアントの夜間の業務レベルアップ作業に必要な電源制御については、“リモートからの電源制御”を参照してください。

サーバ/クライアントの同期適用

部門管理/業務サーバとその配下に接続されているクライアントを1つの単位として扱い、サーバ用・クライアント用資源の適用を、同期をとって行うことができます。資源の適用の同期をとることで、クライアント・サーバ型の新業務を全社一斉に開始することが容易になります。サーバ用・クライアント用の資源は、メンテナンス版数として配付することで、同期をとった適用が可能です。また、メンテナンス版数の適用結果から、新業務が運用可能な状態になっているか、容易に確認が可能です。

また、データ量の大きい資源を配付する場合、事前配付により、適用予定日時よりも前に資源をクライアントまで配付しておき、適用予定日時に一斉に適用することが可能です。

注意

適用予定日時を設定し、通常に資源を配付した場合、設定した日時を経過するまで、クライアントへ資源をダウンロードすることはできません。適用予定日時を設定し、事前配付で資源を配付した場合、設定した日時を経過しなくてもクライアントへ資源をダウンロードできます。

2.7.5 大規模システムで配付する

配付先システム数が多い場合でも、サーバやネットワークの負荷を軽減して配付できます。

中継サーバ

配付先システムが多い場合、運用管理サーバと部門管理/業務サーバの間に、資源を中継する中継サーバを設置し、多階層で資源を配付することにより、トラフィックを軽減することが可能です。中継サーバには、部門管理サーバ、

業務サーバのどちらかを利用します。運用管理サーバから配付した資源は、中継サーバに転送されます。ネットワークの構成により、中継サーバを複数経由することも可能です。

遠隔地の多数のシステムに資源を配付する場合も、配付先システムは、同一LAN内の部門管理/業務サーバから資源をダウンロードさせることで、WANへの課金を削減できます。また、配付先システムが多い場合、中継サーバを複数設置することで、1台のサーバへ負荷が集中することを防ぎます。

2.7.6 大量データを配付する

大量データを配付する場合、システムやネットワークの負荷を軽減して次の方法で配付できます。

分割配付

配付資源を分割し、ネットワークのトラフィック負荷を抑えて配付できます。資源を分割して配付するには、以下の方法があります。

- サーバ間の分割配付
- サーバとクライアント間の分割事前デリバリ

サーバ間の分割配付

サーバ間で配付資源を分割して配付します。一定の転送量や送信間隔を指定し分割、転送できるので、運用に与える影響を最小限に抑えることができます。

サーバとクライアント間の分割事前デリバリ

サーバとクライアント間で、配付資源を分割して配付します。配付された資源は、指定された適用日時にクライアントに適用できます。サーバとクライアントで、同期をとって適用が必要な業務資源を、新業務開始時までに業務運用と並行してクライアントまで事前に資源を配付しておき、新業務開始時に一斉にクライアントで適用することで、スムーズに新規業務が開始できます。

サーバとクライアント間の分割事前デリバリは、クライアントに事前配付する資源だけが可能です。事前配付については、“適用日をスケジュールする”を参照してください。

オフライン配付

大量データを配付する場合や転送能力の低い回線で配付するなど、回線を経由しての配付が困難な場合には、オフラインで配付することが可能です。

運用管理サーバで外部媒体に移出した資源を、部門管理/業務サーバやクライアントへ移入することで、オンラインで配付した資源同様の管理を行うことも可能です。

GEE 2.7.7 グローバルサーバシステムで配付する

Systemwalker Centric Manager GEEの資源配付が管理対象とするシステムと資源について説明します。

管理対象システム

運用管理サーバが管理する範囲は、GS部門管理サーバ、GS部門管理サーバ直下のクライアント、およびGS部門管理サーバ配下の各種業務サーバの配付状況です。

管理対象システムの構成例は、“資源配付に必要なソフトウェア環境”を参照してください。

登録/配付対象資源

運用管理サーバでは、Systemwalker Centric Manager(EE)で扱っていた資源のほかに、GSが扱う資源の登録/配付を行います。以下に示すグローバルサーバで扱う資源を示します。

- グローバルサーバ用資源(ユーザ資源、システム修正データ)
- Gシリーズ用資源(ユーザ資源、システム修正データ)

サポートシステムと資源種別

Systemwalker Centric Manager GEEで管理対象となるシステムとサポートする資源を以下に示します。

種別	管理対象システム	サポートする資源種別
EE	HP Solaris Windowsサーバ Windowsクライアント	ユーザ資源 パッケージ(UNIX用) パッケージ(Windows用)
GEE	グローバルサーバ クライアント	ユーザ資源 システム修正データ

これらの資源は、開発システム(グローバルサーバ)からのアップロードにより登録し、グローバルサーバを経由(自動中継)して配付します。

2.8 評価

Systemwalker Centric Managerで蓄積されたトラブルの発生状況や性能情報は、目的にあわせて分析できます。トラブルの発生状況や、性能情報を評価/分析することで、現状のシステムやネットワーク、業務に対し、次のようなフィードバックが可能です。

- 無駄なリソースを減らし効率的な設備投資を行う
- 適切な増設/移設の計画
- 潜在的な問題点の早期発見

2.8.1 ネットワークのサービスレベルを評価する

サーバ、ネットワーク機器、RMONなどから収集/蓄積されたネットワークの性能情報およびMIB情報をもとに、ネットワークの分析/評価を行うことができます。

ネットワークの性能を分析する

サーバやネットワーク機器から収集された性能情報は、運用管理サーバ上で形式化され、目的にあわせて使用できます。形式化された性能情報の利用方法を以下に示します。

- ネットワーク負荷の増加傾向を分析し機器構成を見直す
- ネットワーク負荷集中など潜在的な問題点の早期発見

収集する項目は以下のとおりです。

	収集する項目
トラフィック情報	受信バイト数 送信バイト数 回線使用率 受信パケット数 送信パケット数 破棄パケット率 エラーパケット率
トラフィック情報 (RMONの場合)	セグメントバイト数 セグメントパケット数 セグメントブロードキャストパケット数 セグメントマルチキャストパケット数 セグメント使用率 セグメントコリジョン発生率

注意

サーバ性能情報(基本情報)も同様に収集されます。サーバの性能情報については“システムのサービスレベルを評価する”を参照してください。

Linux版を使用する場合

Linux版 Systemwalker Centric Managerでレポート出力ができるのは以下の項目です。

- 受信バイト数
- 送信バイト数
- 回線使用率
- CPU使用率
- ページフォルト数
- Diskビジー率

レポーティング

ネットワークの性能の分析は、性能監視で収集したネットワークのトラフィック情報をCSVファイルに出力することで行えます。出力結果をカスタマイズして、ネットワーク負荷の傾向分析や、週報や月報の作成にも利用できます。

性能監視のCSVファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

Systemwalker Service Quality Coordinatorとの連携

Systemwalker Service Quality Coordinator(SSQC)と連携することにより、蓄積されたネットワークのトラフィック情報を、分析の目的に応じた任意のグラフで表示することができます。SSQCの性能データベース(PDB)に格納されたトラフィック情報から、レポートを生成/表示できます。
SSQCとの連携方法のF3crTrfBcsv(性能情報のCSV出力コマンド)の詳細については、“Systemwalker Centric Manager リファレンスマニュアル”、およびSSQCのマニュアルを参照してください。

MIB情報を分析する

MIB取得機能で取得したMIBログをCSV出力することで、任意のMIB情報を分析することができます。

例えば、以下の分析を行うことができます。

- 顧客システム上のネットワーク機器の稼働状況に問題がないか
- 稼働状況の傾向(パケット損失が多発していないか)の分析
- システム構成を見直す必要がないか

レポーティング

監視対象のMIBを取得し、取得したMIBログをCSV出力することで、MIB情報を分析することができます。ユーザ要件にマッチする任意のMIB情報や、機器固有の拡張MIBの統計レポートを扱うことができます。したがって、Interstage業務アプリケーションの性能やOracle/SQLサーバの性能情報など、SNMPを使用して収集した情報は、レポーティングすることができます。

収集したMIB情報をCSVファイルに出力し、レポートを出力します。出力結果をカスタマイズすることで、週報や月報を作成できます。

2.8.2 システムのサービスレベルを評価する

システムで発生したイベントの情報から、トラブルの発生傾向を表示/分析し、システムの評価を支援します。また、性能情報からは、潜在的な性能トラブル要因の発見と効率的な設備投資立案を支援します。

Systemwalker Centric Managerでは、システムを評価するための以下の機能を提供します。

- イベントの発生傾向を分析する
- 性能情報を分析する

イベントの発生傾向を分析する

収集された監視イベントの情報から、イベントの発生傾向が分析できます。

レポーティング

蓄積された監視イベントの情報をCSVファイルに出力できます。出力結果をカスタマイズして、週報や月報の作成に利用できます。システム監視のCSVファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

また、Systemwalkerコンソールを使用して、発生したイベントの傾向をグラフに表すことができます。イベントグラフ画面では、イベント一覧に表示されているイベントの傾向を種別、状態、時間ごとにグラフで表示できます。

- 種別ごとのイベント発生割合
- 時間ごとのイベント発生件数
- 種別ごとのイベント発生件数
- 状態ごとのイベント発生件数

性能情報を分析する

システムの性能情報を表示分析し、潜在的な性能トラブル要因の発見と効率的な設備投資立案を支援します。システムから収集/蓄積された性能情報は、運用管理サーバ上で一元管理され、サーバ性能の分析/評価に使用できます。

一元管理された性能情報の利用方法を以下に示します。

- サーバの負荷傾向を分析およびシステム構成の見直し
- サーバの負荷集中など潜在的な問題点の早期発見

システムの性能の分析は、性能監視で収集した情報を、レポーティングすることで、傾向分析ができます。

収集する項目は以下のサーバ性能情報です。

- CPU使用率
- ページフォルト数
- ディスクビジー率



注意

トラフィックの性能情報も同様に収集されます。トラフィックの性能情報については“ネットワークのサービスレベルを評価する”を参照してください。

レポーティング

収集したシステムの性能情報をCSVファイルに出力できます。出力結果をカスタマイズして、性能負荷の傾向分析や、週報や月報の作成に利用できます。性能監視のCSVファイルの詳細については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

なお、CSV出力できる情報は、ネットワーク監視機能により収集/蓄積したサーバ性能情報(基本情報)です。サーバ性能監視機能により監視している情報とは異なります。

ネットワーク監視機能とサーバ性能監視機能の違いについては、“ネットワーク/システムの性能を監視する”を参照してください。

2.9 SDK

SystemwalkerではISV(Independent Software Vender)やユーザ固有要件の実現に向け、システム開発環境(SDK)として提供してきたAPIやコマンドのほかに、Systemwalkerの機能を拡張する下記の特徴を持った、インテリジェントサービスを提供します。

- ユーザが容易に拡張・カスタマイズを行うことができます。
- 簡単に各サーバに配付できます

利用者は、本機能により、スクリプト言語を利用したインテリジェント運転が可能になります。

APIについては、“Systemwalker Centric Manager API・スクリプトガイド”を参照してください。

2.9.1 Systemwalkerスクリプトの概要

Systemwalkerスクリプトは、次の3種類があります。

- メッセージ監視アクション型

  イベントに対し、編集を行うスクリプトです。

  イベントの発生を契機に自動アクションとして起動します。本タイプのスクリプトは、提供されているサンプルスクリプトの可変部分を書き換えて登録します。

  本タイプのスクリプトとして、以下のようなサンプルスクリプトが提供されています。

  ー 通知されるイベントのテキストを書き換える

  ー 関係する複数のイベントの通知を抑止する

- 単体起動型

  1つのコマンドとして動作するスクリプトです。

  本タイプのスクリプトは、提供されているサンプルスクリプトの可変部分を書き換えて登録するだけでなく、ユーザ独自に作成し登録することができます。次の方法で起動することができます。

  ー OSのコマンドラインやリモートコマンドから起動する。

  ー Systemwalkerの起動・停止時に自動で起動する。

  ー 自動アクション(アプリケーション起動)として起動する。

  自動アクション(アプリケーション起動)としてスクリプトを起動する場合、イベントの発生を契機にした発生イベントに対する一次対処、通報などに利用することができます。

  本タイプのスクリプトとして、以下のようなサンプルスクリプトが提供されています。

  ー システムに常駐して異常を監視する

  ー 大量システムへ一括してコマンドを投入する

- ライブラリ型

  補助的な機能を定義するスクリプトです。

  本タイプのスクリプトは、提供されているサンプルスクリプトの可変部分を書き換えて登録するだけでなく、ユーザ独自に作成し登録することができます。定義された機能は、Systemwalkerスクリプトのコマンドとして、ほかのスクリプトから呼び出します。

  本タイプのサンプルスクリプトは、以下のサンプルスクリプトに含まれて提供されています。

  ー イベントテキストの書き換えスクリプト(メッセージ監視アクション型)

Systemwalkerスクリプトの編集方法や登録方法の詳細については、“Systemwalker Centric Manager API・スクリプトガイド”を参照してください。

2.9.2　インテリジェントサービスを使用する

インテリジェントサービス機能により、ユーザの運用環境に最適な監視機能を実現できます。標準提供のスクリプトを使用すると、以下の監視・操作を行うことができます。

イベントコリレーション

イベントコリレーションにより、以下が可能になります。

- 同一原因により大量に通知されるイベントを抑止する。
- イベント間の整合を目視ではなく自動で判断させることが可能になる。

その結果、監視の効率・視認性を向上させ、トラブル対処を迅速に行うことができます。

通知イベントの編集

通知されたイベントのメッセージを、自動的にわかりやすい内容に編集することができます。編集によってイベント監視の視認性が向上し、オペレータの負荷を軽減させることができます。

イベント詳細フィルタリング

イベント詳細フィルタリングにより、以下のような高度な条件設定によるイベントのフィルタリングを行うことができます。

- イベントの発生時刻によって通知/非通知を決める。
- 先行するイベントの内容によって後続のイベントへ設定する内容を決める

未発生イベントの監視

発生するはずのイベントが発生しなかったことを異常として検知することで、通常のイベント監視よりも早い段階で異常が検知でき、早期対処が可能となります。

大規模同報リモートコマンド

定型的なあて先(対象システム)とコマンド内容を指定して、複数のシステムに対してリモートコマンドを同時に実行できます。また、一塊の処理として自動実行することができます。システムごとに実行結果のレポートを行うことができます。

稼働状態の監視

業務サーバから被監視ノード(ノードまたはネットワーク機器)に対し、一定間隔でpingを行い監視対象がダウンしていた場合、運用管理サーバまたは部門管理サーバへトラップ通知を行い、以下の監視を行います。

- 部門管理サーバ間での相互監視
- 部門管理サーバから運用管理サーバの監視
- Systemwalkerの構成情報に存在しないノードに対する監視

MIBしきい値監視

監視対象ノードまたはネットワーク機器に対し、特定のMIB値異常を検知した場合、運用管理サーバまたは部門管理サーバへトラップ通知を行います。

サービス稼働監視

サービス稼働監視は、DMZ内およびイントラネット内で動作するインターネットサーバ(DNS、SMTP、WWWサーバなど)の稼働状況を定期的に監視し、インターネットサーバが停止(インターネットサーバへの接続不可)していた場合、運用管理サーバへイベント通知を行います。

Systemwalkerセルフチェック

上位サーバから下位サーバのシステム監視機能に定期的に接続し稼働状態を監視します。接続不可の場合、運用管理サーバにイベント通知し、Systemwalkerの監視機能のダウンを監視することができます。

Webサービス稼働監視

Webサービスについて以下の状態を監視し、停止していた場合は運用管理サーバへイベントを通知します。

- Webサービスを構成するSOAPサーバが停止していないか
- WebサービスへSOAPメッセージを送信し、応答があるかどうか

IPv6インタフェースの稼働監視

被監視ノード、またはネットワーク機器のIPv6インタフェースを監視します。ダウンしていた場合は、運用管理サーバまたは部門管理サーバへトラップを通知します。

関係イベントの自動対処

イベントの自動対処をします。

障害発生時に通知されるイベント(異常メッセージ用)とその障害が復旧したときに通知されるイベント(復旧メッセージ用)を定義することにより、障害の復旧メッセージを受信したときに異常メッセージと復旧メッセージの両方を自動的に対処済にします。

発生イベントしきい値監視

イベントを発生頻度で監視します。

通知イベントの発生頻度が単位時間と発生イベント数で監視しているしきい値に達しない間は、イベント通知を行いません。

イベントファイル出力

処理対象イベントの情報をファイルに出力します。

自動返答

Open ReplyMessageサービス機能を利用しているアプリケーションからの返答要求メッセージに対して、自動的に返答をします。

アプリケーション稼働監視

監視対象ノードのアプリケーションに対し一定間隔で稼働情報の監視を行い、稼働状態が変更になった場合、運用管理サーバへイベントを通知します。

Windowsサービス稼働監視

監視対象ノードのWindowsサービスに対し一定間隔で稼働状態の監視を行い、稼働状態が変更になった場合、運用管理サーバへイベントを通知します。

パラメタを含むプロセス稼働監視

パラメタを含むプロセスに対し一定間隔でプロセス数の監視を行います。プロセス数が下限値を下回った場合、運用管理サーバへイベントを通知します。

サンプルスクリプトの機能概要、カスタマイズ、使用方法については、“Systemwalker Centric Manager API・スクリプトガイド”を参照してください。

2.10　ユーザ管理

Systemwalker Centric Managerを使用する利用者のユーザ情報を管理するには、OSのユーザ管理機能を利用してください。

第3章 動作環境

Systemwalker Centric Managerを導入するために必要な環境について説明します。

- ハードウェア資源
- ソフトウェア資源

3.1 ハードウェア資源

Systemwalker Centric Manager導入時および運用時に必要なハードウェア資源を説明します。

3.1.1 ディスク容量

Systemwalker Centric Managerに必要なディスク容量を示します。

各ディレクトリにはインストールに必要な静的ディスク容量に加えて以下の動的ディスク容量が必要です。さらに、運用に応じてディスクが必要になります。

必要なディスク容量については、“Systemwalker Centric Manager 導入手引書”で、“運用管理サーバの環境構築”の“利用する機能により必要なディスク容量の見積もり”、“部門管理サーバ・業務サーバの環境構築”の“利用する機能により必要なディスク容量の見積もり”、または“運用管理クライアント・クライアントの環境構築”の“利用する機能により必要なディスク容量の見積もり”を参照してください。インストールする前にこれらの見積もりを実施してください。

- 静的ディスク容量
- 動的ディスク容量
- パーティションについて【Linux版の場合】

注意

2テラバイト以上のパーティションについて、以下の注意事項があります。

- 以下のディレクトリには、2テラバイト未満のパーティション上のディレクトリを指定してください。
  - 資源配付機能使用時に必要なDRMS管理ファイルディレクトリ
  - [監査ログ管理ポリシーファイル]に定義する[格納ディレクトリ]、[転送用ディレクトリ]【UNIX】
  - [mpatmtrsdef(ファイル転送情報定義コマンド)]で定義する、[格納ディレクトリ]、[転送用ディレクトリ]【UNIX】
  - [mpatmmediacopy(収集ログ二次媒体複写コマンド)]で定義する[複写先ディレクトリ]【UNIX】
  - [mpatmmediadef(収集ログ二次媒体複写先設定コマンド)]で定義する[複写先ディレクトリ]【UNIX】

3.1.1.1 静的ディスク容量

Systemwalker Centric Managerに必要な静的ディスク容量を示します。

- Windows版
- Solaris版
- Linux版

Windows版

WindowsのC:ドライブに固定で必要となるディスク量を“システムドライブ”に、Systemwalker Centric Managerのインストール先ディレクトリ(注)に必要となるディスク量を“インストールディレクトリ”に記載しています。

注）製品インストール時に指定するディレクトリ（デフォルトはC:¥Systemwalker）

(追加機能をすべて選択時)

使用領域	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ				クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
システムドライブ	0.50GB以上	0.50GB以上	0.50GB以上	0.50GB以上	0.50GB以上	－	0.50GB以上	0.50GB以上	0.50GB以上	0.50GB以上
インストールディレクトリ	2.50GB以上	1.60GB以上	0.63GB以上	1.17GB以上	1.17GB以上	0.02GB以上	0.78GB以上	0.78GB以上	0.78GB以上	0.59GB以上
合計	3.00GB以上+DB分(注)以上	2.10GB以上	1.13GB以上	1.67GB以上	1.67GB以上	0.02GB以上	1.28GB以上	1.28GB以上	1.28GB以上	1.09GB以上

富士通ミドルウェア製品共通プログラム(下記)がインストールされる場合に必要なディスク量が含まれています。ただし、他ミドルウェア製品によって、下記が導入済の場合は、追加でのインストールはされません。

－アンインストールと管理(ミドルウェア)：システムドライブに300MB程度

－FJQSS (資料採取ツール)：システムドライブに20MB程度

注)

DB分:以下のデータベース容量の合計です。

－ フレームワークのデータベース

－ インベントリ管理のデータベース

各機能のデータベースの容量については、“Systemwalker Centric Manager 導入手引書”の“運用管理サーバの環境構築”を参照してください。

Solaris版

(追加機能をすべて選択時)

使用領域	運用管理クライアント		業務サーバ				クライアント	
	クライアント	資源配付クライアント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
(root)(注1)	－	－	1MB以上	－	1MB以上	1MB以上	－	－
/opt(注1)	－	－	1300MB以上	－	1200MB以上	830MB以上	－	－

使用領域	運用管理クライアント		業務サーバ				クライアント	
	クライアント	資源配付クライアント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
/etc (注1)	－	－	15MB 以上	－	11MB 以上	1MB 以上	－	－
/var (注1)	－	－	30MB 以上	－	30MB 以上	4MB 以上	－	－
[監視ポリシー]-[インストールレス型エージェント監視]のポリシーの[デプロイ先のパス]に指定したディレクトリ (注1)	－	－	－	20MB 以上	－	－	－	－
システムディレクトリ	0.50 GB 以上	0.50GB 以上	－	－	－	－	0.50GB 以上	0.50GB 以上
インストールディレクトリ	1.60GB 以上	0.63GB 以上	－	－	－	－	0.78GB 以上	0.59GB 以上
合計	2.10GB 以上	1.13GB 以上	1346MB 以上	20MB 以上	1242MB 以上	836MB 以上	1.28GB 以上	1.09GB 以上

注1)

/opt、/etc および /varフォルダがない場合は、各領域の容量が/(root)フォルダに必要です。

Linux版

(追加機能をすべて選択時)

使用領域	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ				クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
/root (注2)	1MB 以上	－	－	1MB 以上	1MB 以上	－	1MB 以上	1MB 以上	－	－
/opt (注2)	1.8GB 以上	－	－	1.16GB 以上	1.08 GB 以上	－	990MB 以上	670 MB 以上	－	－
/etc (注2)	30MB 以上	－	－	20MB 以上	20MB 以上	－	2MB 以上	1MB 以上	－	－
/var (注2)	250MB 以上	－	－	30MB 以上	30MB 以上	－	20MB 以上	5MB 以上	－	－
[監視ポリシー]-[インストールレス型エージェント監視]のポリシーの[デプロイ先のパス]に指定したディレクトリ	－	－	－	－	－	20MB 以上	－	－	－	－
システム ドライブ (注3)	－	0.50 GB 以上	0.50 GB 以上	－	－	－	－	－	0.50 GB 以上	0.50 GB 以上
インストール ディレクトリ (注3)	－	1.60 GB 以上	0.63 GB 以上	－	－	－	－	－	0.78 GB 以上	0.59 GB 以上
合計	2.08GB 以上 +DB分(注1) 以上	2.10 GB 以上	1.13GB 以上	1.21GB 以上	1.13GB 以上	20MB 以上	1.01GB 以上	677MB 以上	1.28 GB 以上	1.09 GB 以上

注1)

DB分:以下のデータベース容量の合計です。

－ フレームワークのデータベース

－ インベントリ管理のデータベース

各機能のデータベースの容量については、“Systemwalker Centric Manager 導入手引書”の“運用管理サーバの環境構築”を参照してください。

注2)

/opt、/etc および /varフォルダがない場合は、各領域の容量が/(root)フォルダに必要です。

注3)

WindowsのC:ドライブに固定で必要となるディスク量を“システムドライブ”に、Systemwalker Centric Managerのインストール先ディレクトリ(※)に必要となるディスク量を“インストールディレクトリ”に記載しています。

※製品インストール時に指定するディレクトリ（デフォルトはC:¥Systemwalker）

3.1.1.2 動的ディスク容量

Systemwalker Centric Managerに必要な動的ディスク容量を示します。

Windows版

使用領域	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ			クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
インストールディレクトリ(注1)	3.70GB 以上	640MB 以上 (注2)	640MB 以上	1.50GB 以上	955MB 以上	625MB 以上	955MB 以上	420MB 以上	420MB 以上

注1)

インストールディレクトリに格納される情報は以下のとおりです。

－ Systemwalker Centric Managerのトレース情報

－ 各サービスが作成する一時ファイル

－ データベースのソート作業域

注2) Systemwalkerコンソールのログファイルについて

運用管理クライアントに格納されるSystemwalkerコンソールのログファイルは、WindowsのセッションIDごとに管理され、WindowsのセッションIDごとの最大値は約60MBです。このため、使用されるWindowsのセッションIDの数とログファイルの大きさによっては、使用される動的ディスク容量が大きくなる場合があります。
現在使用中のWindowsのセッションIDは、query sessionコマンドで確認できます。

Solaris版

使用領域	運用管理クライアント		業務サーバ			クライアント	
	クライアント	資源配付クライアント	エージェント	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
/var/opt (注1)(注2)	－	－	835MB 以上	795MB 以上	835 MB 以上	－	－
インストールディレクトリ(注1)	640MB 以上 (注3)	640MB 以上	－	－	－	420B 以上	420MB 以上
合計	640MB 以上 (注3)	640MB 以上	835MB 以上	795MB 以上	835 MB 以上	420MB 以上	420MB 以上

注1)

Systemwalker Centric Managerのトレース情報を格納します。

注2)

フレームワークのデータベースのソート作業域が作られます。

注3) Systemwalkerコンソールのログファイルについて

運用管理クライアントに格納されるSystemwalkerコンソールのログファイルは、WindowsのセッションIDごとに管理され、WindowsのセッションIDごとの最大値は約60MBです。このため、使用されるWindowsのセッションIDの数とログファイルの大きさによっては、使用される動的ディスク容量が大きくなる場合があります。
現在使用中のWindowsのセッションIDは、query sessionコマンドで確認できます。

Linux版

使用領域	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ			クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
/var/opt (注1)(注2)	3.00GB 以上	－	－	1.50GB 以上	835MB 以上	795MB 以上	835MB 以上	－	－
インストールディレクトリ(注1)	－	640MB 以上 (注3)	640MB 以上	－	－	－	－	420MB 以上	420MB 以上
合計	3.00GB 以上	640MB 以上 (注3)	640MB 以上	1.50GB 以上	835MB 以上	795MB 以上	835MB 以上	420MB 以上	420MB 以上

注1)

Systemwalker Centric Managerのトレース情報を格納します。

注2)

フレームワークのデータベースのソート作業域が作られます。

注3) Systemwalkerコンソールのログファイルについて

運用管理クライアントに格納されるSystemwalkerコンソールのログファイルは、WindowsのセッションIDごとに管理され、WindowsのセッションIDごとの最大値は約60MBです。このため、使用されるWindowsのセッションIDの数とログファイルの大きさによっては、使用される動的ディスク容量が大きくなる場合があります。
現在使用中のWindowsのセッションIDは、query sessionコマンドで確認できます。

クラスタシステムで使用する場合には、ディスク容量に以下の値を追加してください。

- 運用管理サーバ : 90MB以上
- 部門管理サーバ : 2MB以上

さらに、運用に応じてディスクが必要になります。監査ログ管理機能を使用し、ログを保管するには、運用管理サーバのディスク容量に余裕のあるパーティション、ドライブが必要となります。必要なディスク容量については、“Systemwalker Centric Manager 導入手引書”で、“運用管理サーバの環境構築”の“利用する機能により必要なディスク容量の見積もり”、“部門管理サーバ・業務サーバの環境構築”の“利用する機能により必要なディスク容量の見積もり”、または“運用管理クライアント・クライアントの環境構築”の“利用する機能により必要なディスク容量の見積もり”を参照してください。インストールする前にこれらの見積もりを実施してください。

3.1.1.3 パーティションについて【Linux版の場合】

Linux版Systemwalker Centric Managerは以下の数のパーティションを使用します。

パーティションが不足している場合は、ハードディスクの追加購入が必要です。

運用管理サーバ

運用管理サーバ	0～4（性能を重視する場合は4）

以下の機能を使用する場合は運用管理サーバにさらに追加のパーティションが必要です。

インベントリ管理を使用する場合	1

運用管理サーバ

Systemwalker Centric Managerに加えて下記の製品を運用管理サーバに導入する場合は、以下の数のパーティションが別途必要です。

Softek AdvancedCopy Manager ETERNUS SF AdvancedCopy Manager	4
Interstage List Works Interstage List Manager	6

なお、その他の製品については、各製品のマニュアルを参照してください。

3.1.2 メモリ容量

Systemwalker Centric Managerに必要なメモリ使用量を示します。

3.1.2.1 メモリ使用量

Systemwalker Centric Managerを運用するために必要なメモリ使用量は、運用方法によって異なります。必要なメモリ使用量の概略値を、以下に示します。

ただし、表示されているメモリ使用量には、システム起動に必要なメモリ使用量は、含まれていません。

- Windows版
- Solaris版
- Linux版

Windows版

	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ				クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
メモリ使用量(監視時)	690MB以上	90MB以上	80MB以上	150MB以上	120MB以上	10MB以上	100MB以上	20MB以上	80MB以上	80MB以上
メモリ使用量(資源配付時)	(式1)	4MB以上	4MB以上	(注)	(式2)	－	－	(式2)	4MB以上	4MB以上
メモリ使用量(正規化時)	(式3)	－	－	－	－	－	－	－	－	－
メモリ使用量(集計時)	(式4)	－	－	－	－	－	－	－	－	－

式1: 9 + 1.5 × 同時配付多重度 (単位：MB)
式2: 6 + 2 × 同時受信資源グループ数 (単位：MB)
式3: 120 × mpatalogcnvt同時実行多重度 (単位：MB)
式4: 80 × mpatareportput同時実行多重度 (単位：MB)

注)

(式1)または(式2)の大きい方の値。
資源の受信と送信を同時に行う場合は (式1) + (式2)

Solaris版

	運用管理 クライアント		業務 サーバ				クライアント	
	クライアント	資源配付クライアント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
メモリ使用量 (監視時)	90MB 以上	80MB 以上	470MB 以上	10MB 以上	290MB 以上	40MB 以上	80MB 以上	80MB 以上
メモリ使用量 (資源配付時)	4MB以上	4MB以上	(式1)	－	－	(式1)	4MB以上	4MB以上
メモリ使用量 (正規化時)	－	－	－	－	－	－	－	－
メモリ使用量 (集計時)	－	－	－	－	－	－	－	－

式1: 6 + 2 × 同時受信資源グループ数 (単位：MB)

Linux版

	運用管理 サーバ	運用管理 クライアント		部門管理 サーバ	業務 サーバ				クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
メモリ使用量 (監視時)	830MB以上	90MB 以上	80MB 以上	160MB 以上	160MB 以上	10MB 以上	110MB 以上	80MB 以上	80MB 以上	80MB 以上
メモリ使用量 (資源配付時)	(式1)	4MB以上	4MB以上	(注)	(式2)	－	－	(式2)	4MB以上	4MB以上
メモリ使用量 (正規化時)	(式3)									

	運用管理サーバ	運用管理クライアント		部門管理サーバ	業務サーバ				クライアント	
	マネージャ	クライアント	資源配付クライアント	エージェント	エージェント	インストールレス型エージェント（デプロイ方式）	イベント監視エージェント	資源配付エージェント	クライアント	資源配付クライアント
メモリ使用量(集計時)	(式4)									

式1: 9 + 1.5 × 同時配付多重度 (単位：MB)
式2: 6 + 2 × 同時受信資源グループ数 (単位：MB)
式3: 240 × mpatalogcnvt同時実行多重度 (単位：MB)
式4: 30 × mpatareportput同時実行多重度 (単位：MB)

注)

(式1)または(式2)の大きい方の値。
資源の受信と送信を同時に行う場合は (式1) + (式2)

3.1.3 スワップ容量【Solaris版/Linux版】

Systemwalker Centric Managerに必要なスワップ容量を示します。

システム提供のスワップ領域を超える場合は、スワップ領域を拡張してください。

Solaris版

業務サーバ		
エージェント	イベント監視エージェント	資源配付エージェント
470MB以上	290MB以上	40MB以上

Linux版

運用管理サーバ	部門管理サーバ	業務サーバ		
マネージャ	マネージャ	エージェント	イベント監視エージェント	資源配付エージェント
510MB以上	150MB以上	150MB以上	150MB以上	150MB以上

3.1.4 推奨スペック

以下の仕様のハードウェアをお勧めします。

運用管理サーバ/部門管理サーバ/業務サーバ

注意

Solaris版の運用管理サーバ・部門管理サーバは、Systemwalker Centric Manager V15.1.1までの提供です。

	Windows	Solaris	Linux
CPU	1.90GHz 以上	1.20GHz 以上	1.90GHz 以上
CPU数	4コア	4コア	4コア
メモリ（OS込み）(注)	8GB 以上	8GB 以上	8GB 以上

注)

業務サーバの場合は4GB以上になります。

運用管理クライアント/クライアント

	Windows
CPU	2.0GHz 以上
メモリ（OS込み）	4GB以上

3.1.5 必要なハードウェア資源

各機能使用時に必要なハードウェアを説明します。

共通

LANカードが必須です。

コンソール

Solaris版/Linux版Systemwalker Centric Managerの運用管理サーバを使用する場合、最低1台のPC端末が運用管理クライアントとして必要です。

モバイル端末

Systemwalker Webコンソール(モバイル版)を使用するためには、以下のハードウェアが1つ以上必要です。

機器	条件
PDA	Palmscape3.1以降 Xiino 2.0以上が動作するPalmOS搭載PDA
携帯電話	iモード対応携帯電話
上記以外のモバイル端末	HTML2.0以上に準拠したブラウザが動作すること

監視

管理者への通知(アクション定義)

イベント監視でアクション定義として指定したアクションの種類により、以下のハードウェア、およびソフトウェアが必要です。

アクションの種類	必要ハードウェア	必要ソフトウェア
電子メール		受信側にE-mail受信用プログラム
ショートメール通知	モデム NTTドコモの携帯電話(ショートメール対応のもの) ショートメール対応の電話機については、NTTドコモのホームページ等を参照してください。	

アクションの種類	必要ハードウェア	必要ソフトウェア
音声通知	WAVEオーディオカード(注)	Microsoft Speech API (SAPI 5.1以下)対応の音声合成エンジンが実装されている製品

注)

機種によりオーディオカードを搭載できない場合があります。

UNIX版の場合、上記のアクションを実行するには、運用管理クライアントなどに上記のハードウェアを搭載し、そこで実行します。

MIB情報の表示

MIB情報の表示で省電力情報を表示する場合、監視対象機器としてサポートするハードウェアは以下のとおりです。

- SPARC Servers
- PRIMERGY
- PRIMEQUEST

障害復旧

リモートからの復旧操作

クライアントの電源制御

リモートからクライアントの電源制御を行う場合、コンピュータが以下のハードウェア条件をすべて満たす必要があります。

- クライアント電源投入
  - Wakeup on LANをサポートしている機種
  - Wakeup on LANをサポートしているLANカード
  - Wakeup on LANによる電源投入がBIOSレベルで有効になっている
- クライアント電源切断
  - APM(Advanced Power Management)またはACPI(Advanced Configuration & Power Interface)をサポートしている機種
  - Windowsからの電源切断が可能になっている

障害対処の自動化

管理者への通知(アクション定義)と同じです。

EE GEE

コンソール操作制御

コンソール操作制御は、SMARTACCESSと連携することでスマートカードや指紋などによる認証が行えます。SMARTACCESSと連携する場合は、以下のハードウェアが必要です。

- SMARTACCESSがサポートする認証装置
  - スマートカード
  - ICカード(Felica方式)
  - 指紋センサー
  - 静脈センサー
    運用管理サーバでは、SMARTACCESSと連携することはできません。

リモート操作

Live Help（リモート操作機能）は、以下の各条件を満たすPC-AT互換機上で動作します。

周辺機器

ディスプレイモニタ、キーボードが接続されている必要があります。

上記周辺機器が接続されていないコンピュータには対応していません。

注意

動作しない環境についての注意事項

- クラスタ環境

  Live Helpは、クラスタ環境で使用できますが、クラスタのフェールオーバーには対応していません。この場合のリモート操作機能は、Windows OS上における通常の動作範囲となります。

- PRIMERGY FTモデル

  Live Helpは、PRIMERGY FTモデルで使用することができますが、CoServer上では動作しません。詳細については、“Systemwalker Centric Manager 使用手引書 リモート操作機能編 ユーザーズガイド”の“PRIMERGY FTモデルを利用するには”を参照してください。

3.2 ソフトウェア資源

Systemwalker Centric Managerに必要なソフトウェア資源について説明します。

3.2.1 動作OS

Systemwalker Centric Managerを導入するサーバ、およびクライアントの動作OSを以下に示します。

なお、最新のOS対応状況については、Systemwalker Centric Managerのホームページを参照してください。

動作OSごとの機能差については、“OS別機能差一覧”を参照してください。

3.2.1.1 Windows版

サポート期間が終了した基本ソフトウェアは、本製品のサポート対象外です。

運用管理サーバ/部門管理サーバ/業務サーバ

- Microsoft(R) Windows Server(R) 2016 Datacenter (注)
- Microsoft(R) Windows Server(R) 2016 Standard (注)
- Microsoft(R) Windows Server(R) 2019 Datacenter (注)
- Microsoft(R) Windows Server(R) 2019 Standard (注)
- Microsoft(R) Windows Server(R) 2022 Datacenter (注)
- Microsoft(R) Windows Server(R) 2022 Standard (注)

注意

- Nano Serverにはインストールできません。
- FIPSモードには対応していません。

運用管理クライアント

- Windows(R) 10 Pro
- Windows(R) 10 Enterprise

- Windows(R) 10 Education
- Windows(R) 11 Pro (注)
- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)

クライアント

- Windows(R) 10 Home
- Windows(R) 10 Pro
- Windows(R) 10 Enterprise
- Windows(R) 10 Education
- Windows(R) 11 Home (注)
- Windows(R) 11 Pro (注)
- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)



注意

Windows 11 24H2 以降のバージョンの利用にあたっては、留意事項があります。

詳細は、弊社ホームページ「ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況）」内の「OSへの対応状況」、または、Systemwalker Centric Managerホームページの「型名/価格/適応機種/適応OSの一覧」から参照できる「OSへの対応状況」でご確認ください。

3.2.1.2 Solaris版

サポート期間が終了した基本ソフトウェアは、本製品のサポート対象外です。

業務サーバ

Solaris 11 (SPARC)



注意

- 本製品でサポートしているマイナーバージョンは、下記のとおりです。
  - Solaris 11.3～11.4まで
- Solaris 11.4の場合、以下のOSパッチを適用してください。
  - SRU33(SRU21051)以降
- Systemwalker Centric Managerのインストール/セットアップ後にnon-global zoneを作成しないでください。
- FIPSモードには対応していません。

運用管理クライアント

- Windows(R) 10 Pro
- Windows(R) 10 Enterprise
- Windows(R) 10 Education
- Windows(R) 11 Pro (注)

- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)

クライアント

- Windows(R) 10 Home
- Windows(R) 10 Pro
- Windows(R) 10 Enterprise
- Windows(R) 10 Education
- Windows(R) 11 Home (注)
- Windows(R) 11 Pro (注)
- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)

注意

Windows 11 24H2 以降のバージョンの利用にあたっては、留意事項があります。

詳細は、弊社ホームページ「ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況)」内の「OSへの対応状況」、または、Systemwalker Centric Managerホームページの「型名/価格/適応機種/適応OSの一覧」から参照できる「OSへの対応状況」でご確認ください。

3.2.1.3 Linux版

サポート期間が終了した基本ソフトウェアは、本製品のサポート対象外です。

運用管理サーバ/部門管理サーバ/業務サーバ

- Red Hat Enterprise Linux 7 (for Intel64)
- Red Hat Enterprise Linux 8 (for Intel64)
- Red Hat Enterprise Linux 9 (for Intel64)

注意

- 本製品でサポートしているマイナーバージョンは、それぞれ下記のとおりです。
  本製品がサポートしているマイナーバージョンの詳細は、弊社ホームページ「ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況)」内の「OSへの対応状況」、または、Systemwalker Centric Managerホームページの「型名/価格/適応機種/適応OSの一覧」から参照できる「OSへの対応状況」でご確認ください。
  - Red Hat Enterprise Linux 7.9
  - Red Hat Enterprise Linux 8.10まで
  - Red Hat Enterprise Linux 9.4まで
- FIPSモードには対応していません。

運用管理クライアント

- Windows(R) 10 Pro
- Windows(R) 10 Enterprise

- Windows(R) 10 Education
- Windows(R) 11 Pro (注)
- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)

クライアント

- Windows(R) 10 Home
- Windows(R) 10 Pro
- Windows(R) 10 Enterprise
- Windows(R) 10 Education
- Windows(R) 11 Home (注)
- Windows(R) 11 Pro (注)
- Windows(R) 11 Enterprise (注)
- Windows(R) 11 Education (注)



注意

Windows 11 24H2 以降のバージョンの利用にあたっては、留意事項があります。

詳細は、弊社ホームページ「ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況)」内の「OSへの対応状況」、または、Systemwalker Centric Managerホームページの「型名/価格/適応機種/適応OSの一覧」から参照できる「OSへの対応状況」でご確認ください。

3.2.2　関連ソフトウェア資源

動作OS、および各機能使用時に前提としているソフトウェアや関連するソフトウェアについて説明します。

Linuxの場合

“Systemwalker Centric Manager 必須パッケージ【Linux】”に記載されているパッケージがインストールされている必要があります。

Solarisの場合

- Solaris 11の場合
  - 日本語版では以下のパッケージがインストールされている必要があります。
    - system/locale/extra
    - system/library/iconv/extra (注1)
    - system/library/iconv/unicode (注1)
    - system/library/iconv (注2)

    注1) Solaris 11.3以前の場合に必要です。

    注2) Solaris 11.4以降の場合に必要です。
  - Solaris 11.4 以降のnon-global zoneの場合は、以下のパッケージがインストールされている必要があります。
    - package/svr4

必須ソフトウェア

Systemwalker Centric Manager動作時の必須ソフトウェアについて説明します。

再頒布可能パッケージ

以下の再頒布可能パッケージは、Systemwalker Centric Managerの動作に必要なソフトウェアとなります。

- Microsoft Visual C++ 2015-2019 Redistributable (x64)
- Microsoft Visual C++ 2015-2019 Redistributable (x86)

Systemwalker Centric Managerがインストールされている場合には、アンインストールしないよう注意してください。

コンソール

Systemwalker Webコンソール

Systemwalker Webコンソールを使用する場合、Systemwalker Webコンソールを使用する側に以下のどれかのソフトウェアが必要です。

DMZ内

インターネットでSystemwalker Webコンソールを使用して監視する場合、DMZ内にリバースプロキシが必要です。以下の製品のHTTPアプリケーションゲートウェイ機能(リバース機能)を使用してください。

ー Interstage Application Server

Systemwalker Webコンソールを使用する側

WWWブラウザが必要です。以下に示すWWWブラウザが使用できます。

ー Internet Explorer 11

ー Microsoft Edge(Internet Explorerモード)

ー firefox (Systemwalker Webコンソール(互換)の場合のみ)【Solaris版/Linux版】

Systemwalker Webコンソール(互換)の操作を行う場合は、画面の解像度を1280×1024ピクセル(SXGA)以上で表示してください。

WWWブラウザを起動する画面（Systemwalker Webコンソール(互換)を除く)の解像度は1024×768ピクセル(XGA)以上で表示してください。

資源の配付

資源を圧縮して配付する

- Windows用の資源の場合

  資源を登録するシステムにCOMPRESS.EXEが必要です。COMPRESS.EXEは、以下の書籍に同梱されています。

Microsoft(R) Windows(R) 2000 Serverリソースキット

- Linux用の資源の場合

  Red Hat Enterprise Linux 8以前の場合

  資源を登録するシステムと適用するシステムの両方に圧縮／解凍ユーティリティ(ncompressパッケージ)が必要です。

  Red Hat Enterprise Linux 9以降の場合

  資源を適用するシステムに圧縮／解凍ユーティリティ(gzipパッケージ)が必要です。

注意

資源を圧縮して配付する機能を利用する場合の注意事項

Red Hat Enterprise Linux 9以降では下記のパッケージが提供されないことにより、資源の圧縮機能が利用できません。

ー 圧縮／解凍ユーティリティ(ncompressパッケージ)

携帯端末へ配付する

モバイル端末に必要なOSについては、携帯端末クライアントのソフトウェア説明書およびマニュアルを参照してください。

監視

ネットワーク/システムの監視

トラップの監視、MIB監視の監視対象となるノードでは、以下が動作している必要があります。

使用する監視機能	必須機能
トラップの監視、MIB監視を使用したネットワーク/システムの障害の監視	SNMPエージェント
ネットワーク性能の監視	MIBIIをサポートするSNMPエージェント RMON-MIBをサポートするSNMPエージェント(RMONとして監視する場合)
システム性能の監視	SNMPエージェント

管理者への通知(アクション定義)

必要なハードウェア資源の“管理者への通知(アクション定義)”を参照してください。

インストールレス型エージェントの監視

関連ソフトウェア

以下のパッケージが必要になります。インストールされていない場合は、インストールしてください。

OS	パッケージ
Solaris 10 以前	SUNWaccu SUNWesu
Solaris 11 以降	system/accounting/legacy-accounting system/xopen/xcu4

監視サーバと被監視システム間の通信のために必要となるソフトウェアは以下のとおりです(OSのインストール媒体に含まれているソフトウェア、サービスを使用してください)。

監視サーバ	被監視システム	通信方式	監視サーバへの導入必要性				被監視システムへの導入必要性			
			TELNETクライアント	SSHサーバ	WMIクライアント	FTPサーバ(注3)	TELNETサーバ	SSHサーバ	WMIサービス	FTPクライアント
UNIX	UNIX	TELNET(非デプロイ方式)	必要	－	－	－	必要	－	－	－
		SSH(非デプロイ方式)	－	必要	－	－	－	必要(注2)	－	－
		TELNET(デプロイ方式)	必要	－	－	必要	必要	－	－	必要
		SSH(デプロイ方式)	－	必要	－	－	－	必要(注2)(注4)	－	－
Windows	Windows	TELNET(非デプロイ方式)	必要	－	－	－	必要	－	－	－
		SSH(非デプロイ方式)	－	必要(注1)	－	－	－	必要(注1)	－	－
		WMI(非デプロイ方式)	－	－	必要	－	－	－	必要	－
		TELNET(デプロイ方式)	必要	－	－	必要	必要	－	－	必要
		SSH(デプロイ方式)	－	必要(注1)	－	－	－	必要(注1)	－	－
UNIX	Windows	TELNET(非デプロイ方式)	必要	－	－	－	必要	－	－	－
		SSH(非デプロイ方式)	－	必要	－	－	－	必要(注1)	－	－
		TELNET(デプロイ方式)	必要	－	－	必要	必要	－	－	必要
		SSH(デプロイ方式)	－	必要	－	－	－	必要(注1)(注5)	－	－
Windows	UNIX	TELNET(非デプロイ方式)	必要	－	－	－	必要	－	－	－
		SSH(非デプロイ方式)	－	必要(注1)	－	－	－	必要(注2)	－	－

監視サーバ	被監視システム	通信方式	監視サーバへの導入必要性				被監視システムへの導入必要性			
			TELNETクライアント	SSHサーバ	WMIクライアント	FTPサーバ(注3)	TELNETサーバ	SSHサーバ	WMIサービス	FTPクライアント
		TELNET(デプロイ方式)	必要	－	－	必要	必要	－	－	必要
		SSH(デプロイ方式)	－	必要(注1)	－	－	－	必要(注2)	－	－

注1)

Windowsシステムにおいて、SSH通信する場合は、必ず以下のソフトウェアが必要です。

－ SSH V2.0以上

SSHがインストールされていない環境では、OpenSSH(cygwin OpenSSH V1.7以上)をインストールしてください。

Windows Server 2022、または、Windows Server 2019の業務サーバをSSH通信により監視する場合は、その業務サーバのWindows Defenderの設定で、Windows Defender Exploit Guardを無効にしてください。

なお、被監視システムがNano Serverの場合は、SSH通信は利用できません。

注2)

UNIXシステムにおいて、SSH通信する場合は、OSのバージョンによって以下のソフトウェアが必要となる場合があります。

－ SSH V2.0以上

Solaris 9、Solaris 10、Linux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。SSHがインストールされていない環境では、OpenSSH、OpenSSLをインストールしてください。HP-UX、AIXの場合、ベンダーより入手してください。

注3)

FTP通信する場合はOSにより以下のソフトウェアが必要です。

【Windows】

「FTPサービス」（Windows Server 2012以降）をインストールしてください。

【Linux】

vsftpdをインストールしてください。

【Solaris】

SUNWftpr(Solaris 10)、SUNWftpu (Solaris 10)、service/network/ftp（Solaris 11)をインストールしてください。

注4)

UNIXシステムにおいて、SSH通信でデプロイする場合は、OSのバージョンによって以下のソフトウェアが必要となる場合があります。

－ rsync 3.0以上

注5)

Windowsシステムにおいて、SSH通信でデプロイする場合は、必ず以下のソフトウェアが必要です。

－ rsync 3.0以上

cygwinのインストーラを使用して、rsyncパッケージをインストールしてください。

性能監視

関連ソフトウェア

性能監視機能によりSolarisサーバのサーバ性能を監視する場合には、Solarisサーバに以下のパッケージがインストールされている必要があります。インストールされていない場合は、インストールしてください。

OS	パッケージ
Solaris 11以降	system/accounting/legacy-accounting

障害復旧

障害対処の自動化

必要なハードウェア資源の“管理者への通知(アクション定義)”を参照してください。

評価

ネットワークの評価

レポーティング

性能情報の収集対象となるノードに必要な環境を示します。

- MIBIIをサポートするSNMPエージェント
- RMON-MIBをサポートするSNMPエージェント(RMONとして監視する場合)

また、部門管理サーバから収集ログを転送するために、運用管理サーバにはFTPサーバが必要です。

システムの評価

レポーティング

性能情報の収集対象となるノードでは、SNMPエージェントおよびSystemwalker Centric Managerの性能監視拡張エージェントの機能が動作している必要があります。性能情報の収集対象は、運用管理サーバ、部門管理サーバ、業務サーバです。

EE GEE

クラスタシステムの構成

対象となるクラスタシステムを以下に示します。

【Windows】

- 以下に含まれるMicrosoft(R) Fail Over Clustering
  - Microsoft(R) Windows Server(R) 2019 Datacenter(注)
  - Microsoft(R) Windows Server(R) 2019 Standard(注)
  - Microsoft(R) Windows Server(R) 2016 Datacenter(注)
  - Microsoft(R) Windows Server(R) 2016 Standard(注)

    注）以下のコンポーネントを追加インストールしてください。

    - FailoverCluster-AutomationServer
    - FailoverCluster-CmdInterface

【Linux】

- PRIMECLUSTER Enterprise Edition 4.7まで
- PRIMECLUSTER HA Server 4.7まで
- PRIMECLUSTER Clustering Base 4.7まで

【Solaris】

- PRIMECLUSTER Enterprise Edition 4.6まで
- PRIMECLUSTER HA Server 4.6まで
- PRIMECLUSTER Clustering Base 4.6まで
- Oracle Solaris Cluster 3.3/4.4

LAN二重化の構成

対象となるLAN二重化製品を以下に示します。

- PRIMECLUSTER GL 4.7まで（Solarisは4.6まで）

イベント監視の条件定義

「イベントコリレーション定義」をEvent Designerで変更/参照する場合、以下に示すMicrosoft Excelが必要です。

- Microsoft Excel 2016（32ビット版/64ビット版）
- Microsoft Excel 2019（32ビット版/64ビット版）
- Microsoft Excel 2021（32ビット版/64ビット版）
- Microsoft Excel for Office 365（32ビット版/64ビット版）

Event Designerは、イベント監視の条件定義をCSVファイル形式で簡単に変更することができるツールです。

アクションを実行する条件としてカレンダの運用日/休日を指定する場合には、Systemwalker Operation Managerが必要です。Windows(64bit)版の場合は、V13.4.0以降のSystemwalker Operation Managerが必要です。Linux for Intel64版の場合は、V13.4.0以降のSystemwalker Operation Managerが必要です。

ソフトウェア修正の適用状況の管理

ソフトウェア修正管理機能を使用して修正情報を管理する場合、最新のUpdateAdvisor(ミドルウェア)が必要です。

UpdateAdvisor(ミドルウェア)の導入方法については、アップデートサイトの公開ホームページの機種別メニューから参照できる「<ミドルウェア>」項目の「UpdateAdvisor(ミドルウェア)をご利用にあたって」を参照してください。

EE GEE

コンソール操作制御

コンソール操作制御でSMARTACCESSと連携して認証装置を使用する場合は、以下のどちらかのソフトウェアが必要です。

- SMARTACCESS/Basic（ハードの添付ソフトウェア）
- SMARTACCESS/Premium V5.5まで
  ICカード（Felica方式）、静脈認証を使用する場合に必要です。
  運用管理サーバでは、SMARTACCESSと連携することはできません。

監査ログ分析

監査ログ分析機能を使用する場合、以下のソフトウェアが必要です。

運用管理サーバの場合

- Windows版の場合

  Windows(64bit)版 Interstage Navigator Server Standard Edition/Enterprise Edition V9.5.0

- Linux版の場合

  Linux for Intel64版 Interstage Navigator Server Enterprise Edition V9.6.0

VM運用

Systemwalker Centric ManagerのVM運用で使用できるソフトウェアを以下に示します。

	VM製品
PRIMEQUEST	PRIMEQUEST 仮想マシン機能
PRIMERGY	VMware(R) vSphere 7 Enterprise Plus/Standard (注1) VMware(R) vSphere 8 Enterprise Plus/Standard (注1)
	Windows Server の Hyper-V (注2)
	Linux Virtual Machine 機能

注1)

- 以下のVMwareの機能を使用する場合は、定期的にSystemwalker Centric Managerをバックアップしてください。
  - HA (VMware vSphere High Availability)
  - DR (VMware vCenter Site Recovery Manager)
- クローニングする場合、“Systemwalker Centric Manager 導入手引書”の“クラウド環境でSystemwalker Centric Managerを導入した仮想マシンのクローニングを行う”の手順を実施する必要があります。
- VMware ESXi 6.5以降において、仮想ホストと仮想マシンの関係を検出して作成する監視マップ(仮想マシンの監視マップ)は作成できません。

注2)

運用管理サーバのライブマイグレーション、クイックマイグレーション、およびフェールオーバーは停止中のみ動作可能です。
Hyper-V レプリカは未サポートです。
インポート/エクスポートはIPアドレスやホスト名が変更される場合、“Systemwalker Centric Manager 導入手引書”の“IPアドレスの変更/ホスト名の変更”の手順を実施する必要があります。

仮想マシンの監視マップ作成

VMware ESXi 6.5以降において、仮想ホストと仮想マシンの関係を検出して作成する監視マップ(仮想マシンの監視マップ)を作成することができません。

ServiceNow連携

ServiceNowがサポートしているバージョンに対して、連携が可能です。

ServiceNow連携で、自動アクションにより実行されるスクリプトを動かすために、以下が必要となります。

- Python3（Python3.12）
- Python3外部ライブラリ
  - certifi
  - pycryptodome
  - pywin32 (Windowsのみ)

3.2.3 共存時に注意が必要なソフトウェア資源

Systemwalker Centric Managerと共存できないソフトウェア、または共存時に注意が必要なソフトウェアについて説明します。

3.2.3.1 共存できないソフトウェア

以下の製品は、Systemwalker Centric Managerと共存できません。

【Windows版】

- Systemwalker Live Help Client
- Systemwalker Live Help Expert
- Systemwalker Live Help Connect
- Systemwalker Desktop Patrolのリモート操作機能
- Systemwalker Runbook Automation 管理サーバ【Windows(32bit)版】

利用する機能により共存できない製品

- リモート操作機能を使用する場合
  - 他社のリモートコントロール製品
  - MetaFrame
- 資源配付エージェントを使用する場合
  - Systemwalker Operation Manager V13.2.0以前

インストール種別により共存できない製品

- 運用管理サーバおよび運用管理クライアントの場合

  【Solaris版】
  - Internet Navigware Enterprise LMS Server 9.x/V9.x
- 運用管理クライアントの場合(接続する運用管理サーバのシステムコード系がUTF-8の場合)【UNIX版】
  - Interstage Application Server

3.2.3.2　共存時に注意が必要なソフトウェア

Interstage

運用管理サーバおよび運用管理クライアントでは、Systemwalker Centric Managerと以下のバージョン、エディションのInterstageおよびObjectDirectorは共存できません。

【Windows版】

Interstage Application Server Standard-J Edition V10以降(注1)

Interstage Application Server Enterprise Edition V10以降(注1)

Interstage Application Server Enterprise Edition 【Windows(32bit)版】

Interstage Application Server Standard-J Edition 【Windows(32bit)版】

Interstage Web Server Express V11

Interstage Studio Standard-J Edition V10以降

Interstage Business Application Manager Enterprise Edition for .NET V1 以降 (注2)

Interstage Business Application Manager Standard Edition for .NET V1 以降 (注2)

Interstage Business Application Manager Developer Edition for .NET V1 以降 (注2)

Interstage Business Application Manager Component Connector for .NET V2 以降 (注2)

Interstage Business Application Server Standard Edition V10以降

Interstage Business Application Server Enterprise Edition V11以降

Interstage List Works Standard Edition V9以降 (注4)

Interstage List Works Enterprise Edition V9以降 (注4)

Interstage Shunsaku Data Manager Enterprise Edition V8以降

【Solaris版】

Interstage Application Server Enterprise Edition V10以降(注1)

Interstage Application Server Standard-J Edition V10以降(注1)

Interstage Business Application Server Standard Edition V10以降

Interstage Business Application Server Enterprise Edition 7.0以降

Interstage List Works Standard Edition V10以降

Interstage List Works Enterprise Edition V10以降 (注2)

Interstage Shunsaku Data Manager Enterprise Edition V9以降 (注2)

【Linux版】

Interstage Application Server Enterprise Edition V10以降 (注1) (注4)

Interstage Application Server Standard-J Edition V10以降 (注1) (注4)

Interstage Web Server Express V11

Interstage Business Application Server Standard Edition V10.0以降

Interstage Business Application Server Enterprise Edition V10.0以降

Interstage List Works Enterprise Edition V9.0以降 (注2)

Interstage Shunsaku Data Manager Enterprise Edition V9以降 (注2)

注1)

Web Package機能をインストールする場合、共存できません。

注2)

クライアント機能と運用管理クライアントは共存可能です。

注3)

Solaris版Interstage Application Server Web-J Edition 7.x は、Interstage HTTP Server(FJSVihs)のみをpkgadd コマンドでカスタムインストールした場合は共存可能です。

注4)

以下の組み合わせでの共存はできません。

- Windows(64bit)版Systemwalker Centric Manager と、Windows(32bit)版Interstage List Works
- Linux(64bit)版Systemwalker Centric Manager と、Linux(32bit)版Interstage List Works

ただし、Systemwalker Centric Managerの運用管理クライアントとInterstage List Worksのクライアントは共存可能です。

InterstageおよびObjectDirectorとSystemwalker Centric Managerを共存する場合は、“Systemwalker Centric Manager Interstage, Symfoware, ObjectDirectorとの共存ガイド”を参照してください。

Systemwalker Service Quality Coordinator

Systemwalker Centric ManagerでコアのCPU使用率を考慮した監視を行う場合は、V13.2.0以降のSystemwalker Service Quality Coordinatorと共存することができません。共存する場合は、Systemwalker Centric Managerでは、個々のCPU使用率の監視、または全体のCPU使用率の監視を実施してください。

ServerView

ServerView エージェントとSystemwalker Centric Managerの運用管理サーバまたは部門管理サーバが共存する場合、設定が必要になります。共存する場合の設定方法など詳細については、“Systemwalker Centric Manager 導入手引書”の“インストール前の確認”を参照してください。

リモートデスクトップ、およびターミナルサービス

Live Help（リモート操作機能）は、リモートデスクトップ(ターミナルサービス)と共存させることができます。ただし、ターミナルサービスが起動しているコンピュータ上でのLive Helpの使用は、特定の条件下でのみ可能です。詳細については、“Systemwalker Centric Manager 使用手引書 リモート操作機能編 ユーザーズガイド”の“ターミナルサービスとの同時動作”を参照してください。

リモートアシスタンス機能

Live Help（リモート操作機能）は、リモートアシスタンス(Windows Messenger)機能と共存させることができます。ただし、Live Helpを使用する場合には、事前にリモートアシスタンス機能を終了し、また、リモートアシスタンス機能を使用する場合には、事前にLive Helpを終了してください。リモートアシスタンス機能とLive Helpを同時に使用する運用は、サポートしていません。

3.2.4 リモートデスクトップ（ターミナルサービス）を使用する場合の注意事項

リモートデスクトップ(ターミナルサービス)で使用する場合の注意事項を以下に示します。

電源制御

他のユーザが電源切断対象の端末にリモートデスクトップ(ターミナルサービス)によりログインを行っている状態でクライアントの電源切断を行った場合、電源切断が中止されます。他のユーザがログインを行っている場合でも強制的に電源切断を行いたい場合は、電源切断オプションに/EFを指定する必要があります。

リモート操作

Live Help（リモート操作機能）は、リモートデスクトップ(ターミナルサービス)と共存させることができます。ただし、ターミナルサービスが起動しているコンピュータ上でのLive Helpの使用は、特定の条件下でのみ可能です。詳細については、“Systemwalker Centric Manager 使用手引書 リモート操作機能編 ユーザーズガイド”の“ターミナルサービスとの同時動作”の項を参照してください。

[ハード監視制御]ウィンドウ

リモートデスクトップ(ターミナルサービス)で使用できません。

3.2.5 LDAP参照環境で使用する場合の注意事項【UNIX版】

LDAPクライアントを使用してLDAP上のユーザーを参照できるOS環境において、Systemwalker Centric Managerを使用する場合の注意事項を、以下に示します。

LDAPユーザーでの認証について

Systemwalker Centric Managerへの認証に、LDAP上のユーザーは使用できません。

LDAPユーザーの指定について

Systemwalker Centric ManagerでOSユーザー一覧を表示する画面にLDAPユーザーも表示されますが、LDAPユーザーを選択しないようにしてください。

また、Systemwalker Centric Managerでユーザーを指定する画面／コマンド／定義ファイルに、LDAP上のユーザーは指定しないでください。

LDAPユーザーでOSにログインした場合の操作について

LDAPユーザーでOSにログインした場合は、Systemwalker Centric Managerのコマンドを実行しないでください。

GEE

3.3 Global Enterprise Editionの動作環境

3.3.1 監視・操作できるシステム

Systemwalker Centric Manager GEEでは、監視を行う運用管理サーバと運用管理クライアントを監視システムと呼びます。

Systemwalker Centric Manager GEEでは、グローバルサーバ上の以下のシステムを監視・操作することができます。

- OSIV/MSP
- OSIV/XSP

また、SVPM-Sと連携した場合は、さらに以下のシステムを監視・操作できるようになります。

- OSIV AVM/EX (V10L10以降)
- OSIV AVM/EXS (V10L10以降)

Systemwalker Centric Managerのマニュアルでは、OSIV/MSPをMSP、OSIV/XSPをXSP、AVM/EXとAVM/EXSを併せてAVM/EXと呼びます。また、Systemwalker Centric Manager GEEが監視するMSP、XSP、AVM/EXを併せて、被監視システムと呼びます。

3.3.2 ハードウェア環境

3.3.2.1 監視システム

運用管理サーバと運用管理クライアントは、以下のハードウェアで動作します。

運用管理サーバ

- PRIMEQUEST
- PRIMERGY

運用管理クライアント

- 運用管理クライアントが動作するハードウェア

3.3.2.2 被監視システム

Systemwalker Centric Manager GEEでは、以下を監視・操作することができます。

- FUJITSU Server GS21

なお、本製品のマニュアルでは、FUJITSU Server GS21を「グローバルサーバ」と記載する場合があります。

集中監視装置

以下のシステムを監視・操作する場合は、集中監視装置が必要です。

- AVM/EXおよびAVM/EXSに対する監視・操作

  メッセージ監視

- ハードウェア異常(CPU、周辺機器)の監視

  NIPメッセージ、システムダンプのメッセージ監視

Systemwalker Centric Manager GEEが連携する集中監視装置は以下のとおりです。

- SVPM-S(GS21 1600/1400モデルグループ以降)

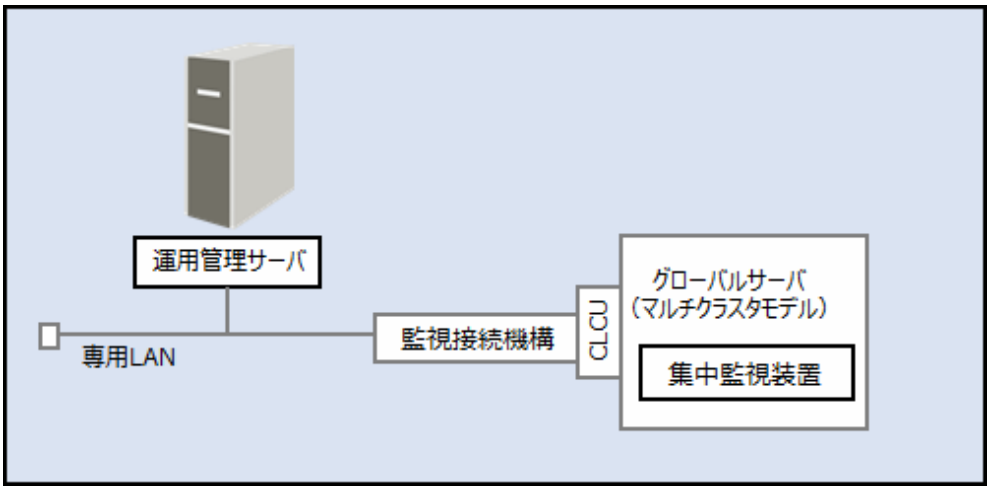
注意

- 1台の運用管理サーバ(Systemwalker Centric Manager GEE)が連携できるSVPM-Sは、最大8台です。
- 1台のSVPM-Sと接続できる運用管理サーバ(Systemwalker Centric Manager GEE)は最大4台です。各運用管理サーバは、SVPM-Sの1台のコンソールとして接続されます。
  SVPM-Sには、最大5台までコンソールが接続可能ですが、最低1台はSVPM-Sの専用コンソールを接続する必要があります。
  なお、SVPM-Sのエディションによって最大接続台数が変わります。SVPM-Sのマニュアルを確認してください。

3.3.2.3 ネットワーク環境

監視システムとグローバルサーバとのLAN環境は、DSLINKまたはFSLINKで構成されたネットワークが必要です。
また、遠隔地から監視・操作する場合は、監視システムとグローバルサーバとのLANを回線で接続します。

集中監視装置(SVPM-S)と連携する場合は、グローバルサーバ側に監視接続機構が必要です。

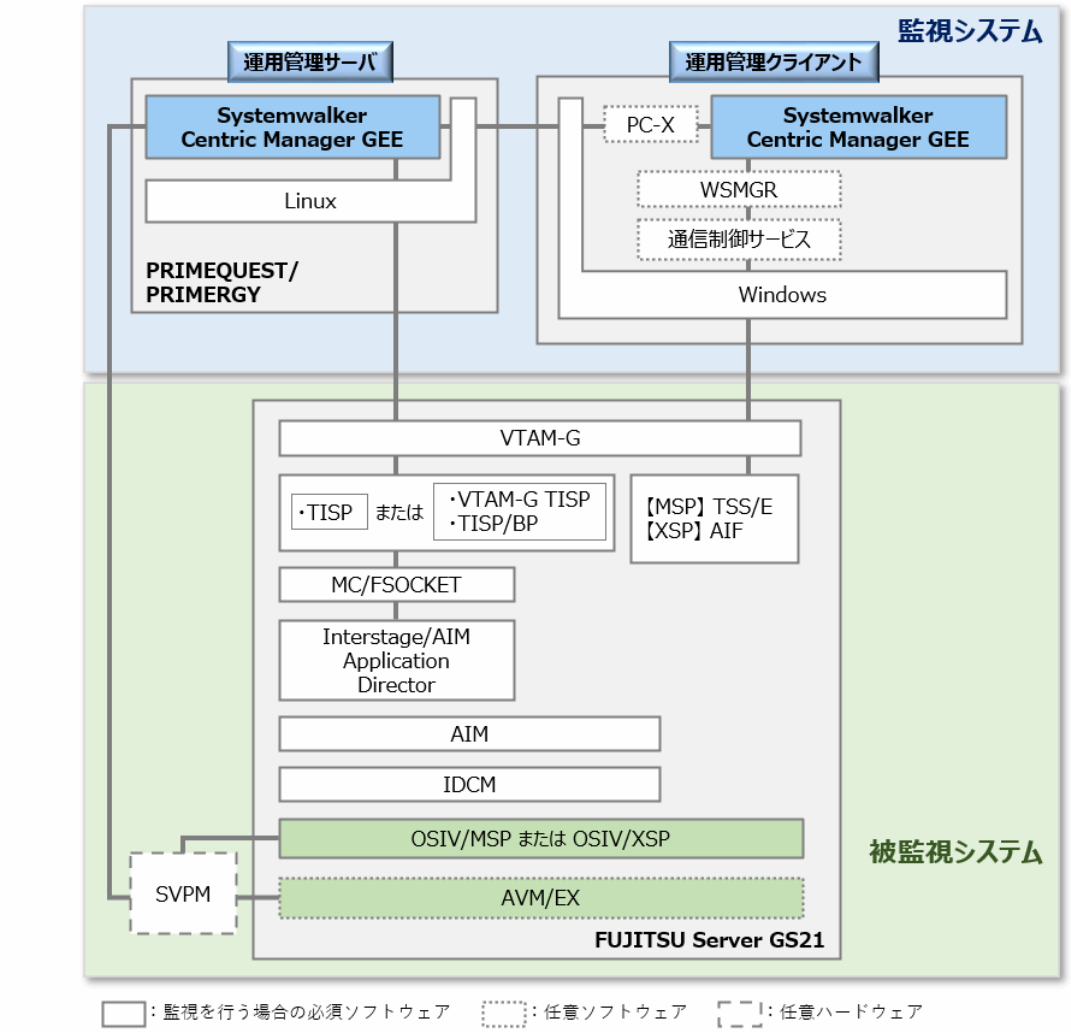


3.3.3 動作OS

運用管理サーバと運用管理クライアントの動作OSについては、“動作OS”を参照してください。

3.3.4 監視に必要なソフトウェア環境

監視を行う場合のソフトウェア構成例



3.3.4.1　監視システムに必要なソフトウェア

[ハード監視]ウィンドウを使用する場合

運用管理クライアントに以下のソフトウェアが必要です。

ソフトウェア名	説明	V/L
PC-X	[ハード監視]ウィンドウを使用する場合に必要です。 運用管理サーバがSolaris版の場合、PC-XはSolaris向け製品を、Linuxの場合はLinux向け製品を使用してください。	[Solaris製品] 1.5以降
		[Linux製品] V20L35以降
WSMGR	エミュレータを使用する場合に必要です。	V9.0以降
通信制御サービス(FNA通信サポート)	エミュレータでFNAプロトコルを使用する場合に必要です。	V9.0以降

3.3.4.2　被監視システムに必要なソフトウェア

必須ソフトウェア

以下のソフトウェアが必要です。

- 「V/L」欄にPTFの表示がないものは、「DLIB」です。
- 「備考」欄に※印がついているソフトウェアはGSS21sxに含まれています。

MSPの場合

以下のどちらかの組み合わせ

ソフトウェア名	V/L	備考
OSIV/MSP AFII	V10L10 C94091.PTF以降	※
OSIV/MSP VTAM-G	V30L20 C97031.PTF以降	※
OSIV/MSP VTAM-G TISP	V10L10以降	※
OSIV/MSP TISP/BP	V10L10以降	※
OSIV/MSP MC/ FSOCKET	V21L10以降	サブシステム/業務の監視を行う場合は、C01121以降 ※

または

ソフトウェア名	V/L	備考
OSIV/MSP AFII	V10L10 C94091.PTF以降	※
OSIV/MSP VTAM-G	V30L20 C97031.PTF以降	※
OSIV/MSP TISP	V20L10以降	
OSIV/MSP MC/ FSOCKET	V21L10以降	サブシステム/業務の監視を行う場合は、C01121以降

XSPの場合

以下のどちらかの組み合わせ

ソフトウェア名	V/L	備考
OSIV/XSP AFII	V10L10 V96031.PTF以降	※
OSIV/XSP VTAM-G	V30L10 V97061.PTF以降	※
OSIV/XSP VTAM-G TISP	V10L10以降	※
OSIV/XSP TISP/BP	V10L10以降	※
OSIV/XSP MC/ FSOCKET	V21L10以降	サブシステム/業務の監視を行う場合は、V02051以降 ※

または

ソフトウェア名	V/L	備考
OSIV/XSP AFII	V10L10 V96031.PTF以降	※
OSIV/XSP VTAM-G	V30L10 V97061.PTF以降	※
OSIV/XSP TISP	V20L10以降	
OSIV/XSP MC/ FSOCKET	V21L10以降	サブシステム/業務の監視を行う場合は、V02051以降 ※

業務の監視に必要なソフトウェア

業務の監視を行う場合は、以下のソフトウェアが必要です。

- 「V/L」欄にPTFの表示がないものは、「DLIB」です。
- 「備考」欄に※印がついているソフトウェアはGSS21sxに含まれています。

MSPの場合

ソフトウェア名	V/L	備考
OSIV/MSP TSS/E	V11L20以降	TSS操作をする場合に必要です。 ※
OSIV/MSP IDCM	V10L10 D01061.PTF以降	※
OSIV/MSP AIM	V20L10 D01061.PTF以降	※
OSIV/MSP INTERSTAGE/ AIMApplicationDirector	V20L10以降	※

XSPの場合

ソフトウェア名	V/L	備考
OSIV/XSP AIF	V11L20以降	AIF操作をする場合に必要です。 ※
OSIV/XSP IDCM	V10L10 D01071.PTF以降	※
OSIV/XSP AIM	V20L10 D01071.PTF以降	※
OSIV/XSP INTERSTAGE/ AIMApplicationDirector	V20L10以降	※

コンソール操作を行う場合に必要なソフトウェア

コンソール操作を行う場合は、以下のソフトウェアが必要です。

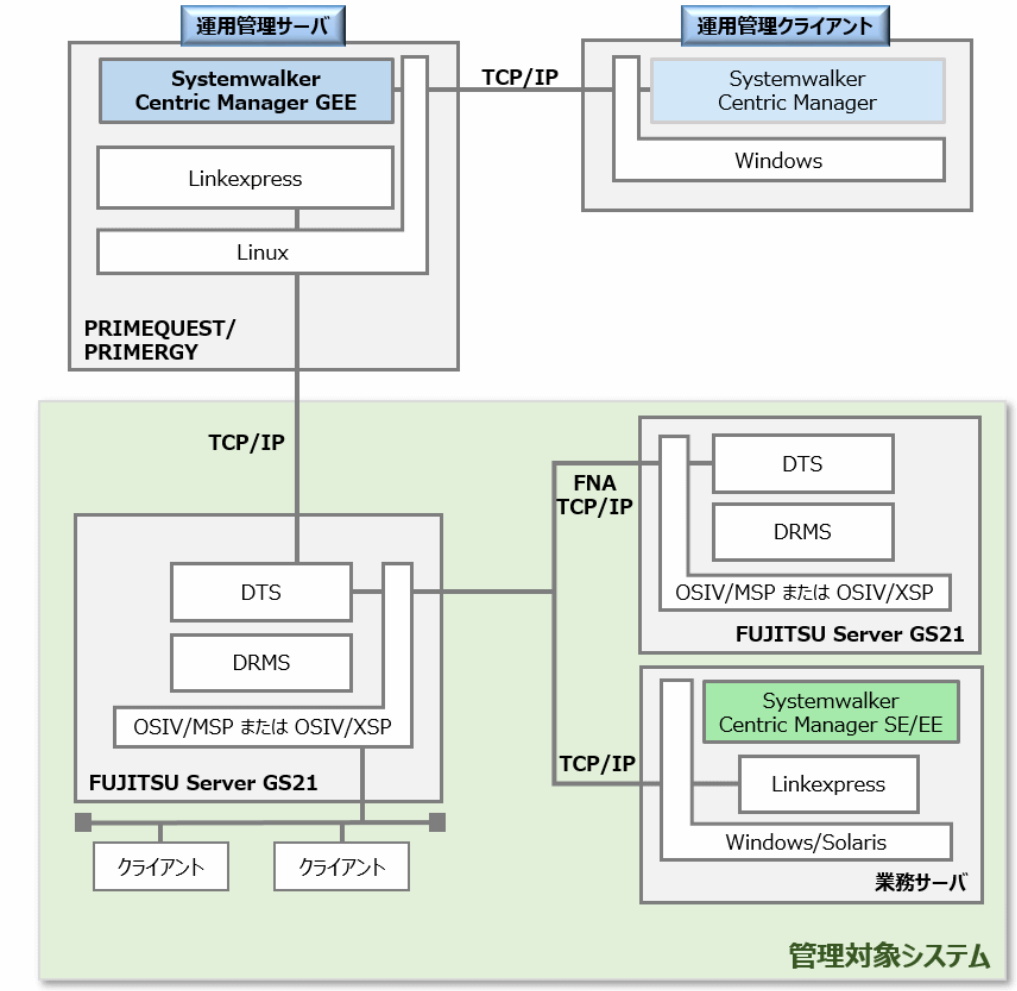
- 「V/L」欄にPTFの表示がないものは、「DLIB」です。
- 「備考」欄に※印がついているソフトウェアはGSS21sxに含まれています。

MSPの場合

ソフトウェア名	V/L	備考
OSIV/MSP ECS	V11L10以降	※

3.3.5　資源配付に必要なソフトウェア環境

資源配付を行う場合のソフトウェア構成例



3.3.5.1　運用管理サーバに必要なソフトウェア

Linuxの場合

以下のソフトウェアのどれかが必要です。

ソフトウェア名	V/L	備考
Linkexpress Standard Edition	V5.0aL23 以降	
Linkexpress Enterprise Edition	V5.0aL23 以降	

3.3.5.2　管理対象システムに必要なソフトウェア

必須ソフトウェア

資源配付機能を利用する場合は、管理対象システムに以下のソフトウェアが必要です。

- 「V/L」欄にPTFの表示がないものは、「DLIB」です。
- 「備考」欄に※印がついているソフトウェアはGSS21sxに含まれています。

MSPの場合

ソフトウェア名	V/L	備考
OSIV/MSP IDCM	V10L10 D91061.PTF以降	※
OSIV/MSP DTS	V20L10 L97031.PTF以降	※
OSIV/MSP ADJUST	V12L10 L94121.PTF以降	※
OSIV/MSP DRMS	V22L20	

XSPの場合

ソフトウェア名	V/L	備考
OSIV/XSP IDCM	V10L10 D91121.PTF以降	※
OSIV/XSP DTS	V20L10 L97031.PTF以降	※
OSIV/XSP ADJUST	V11L30 L93091.PTF以降	※
OSIV/XSP DRMS	V22L20	

グローバルサーバ上で作成した帳票資源を配付する場合

帳票システムと連携しグローバルサーバ上で扱っていた帳票資源を配付する場合は、連携する部門管理サーバ/業務サーバに以下のソフトウェアが必要です。

ソフトウェア名	V/L	備考
Interstage Charset Manager	V9以降	

また、管理対象システムのOSに応じて、以下のソフトウェアが必要です。

Solaris 11の場合

以下のソフトウェアのどれかが必要です。

ソフトウェア名	V/L	備考
Linkexpress Standard Edition	V5.0L20 以降	
Linkexpress Enterprise Edition	V5.0L20 以降	

Windowsの場合

以下のソフトウェアのどれかが必要です。

ソフトウェア名	V/L	備考
Linkexpress Standard Edition	V5.0L21 以降	
Linkexpress Enterprise Edition	V5.0L21 以降	

また、グローバルサーバおよびPRIMEFORCE側はDRMS V22L10以降に対応しています。その他のグローバルサーバおよびPRIMEFORCE側の環境は、DRMSの“ソフトウェア説明書”を参照してください。

3.3.6 監査ログ管理に必要なソフトウェア

3.3.6.1 被監視システムに必要なソフトウェア

監査ログ管理機能を使用する場合は、被監視システムに以下のソフトウェアが必要です。

MSPの場合

ソフトウェア名	V/L	備考
OSIV/MSP AFII	V10L10 C94091以降	
OSIV/MSP RACF	V12L10 C07061以降	
OSIV/MSP AIM	V20L10 D07061以降	

XSPの場合

ソフトウェア名	V/L	備考
OSIV/XSP AFII	V10L10 V07091以降	
OSIV/XSP RACF	V11L10 V07091以降	
OSIV/XSP AIM	V20L10 D07071以降	

ファイル転送製品

ファイル転送製品が必要です。

ファイル内の文字コードは変換が必要です。転送元システム(GSシステム)のファイル内の文字コードはEBCDIC(ASCII)です。ファイル転送後、転送先システム(運用管理サーバ)のファイル内の文字コードを(EBCDIC(ASCII)から)ASCIIに変換しておく必要があります。

以下に、推奨するファイル転送製品を示します。

・ グローバルサーバ側（推奨製品）

ソフトウェア名	V/L	備考
Linkexpress File Transfer	V10L10	

・ オープン側(サーバ)

ー Solaris 11の場合

以下のソフトウェアのどれかが必要です。

ソフトウェア名	V/L	備考
Linkexpress Standard Edition	V5.0L20 以降	
Linkexpress Enterprise Edition	V5.0L20 以降	

ー Windowsの場合

以下のソフトウェアのどれかが必要です。

ソフトウェア名	V/L	備考
Linkexpress Standard Edition	V5.0L21 以降	
Linkexpress Enterprise Edition	V5.0L21 以降	

付録A　Systemwalker Centric Managerと他製品の連携

Systemwalker Centric Managerは、他製品と連携し、より多くの機能を実現することができます。

A.1　連携製品一覧

他ソフトウェア製品との連携方法は、以下に示す方法があります。

- 他ソフトウェア製品をSystemwalker Centric Managerで監視する

  ほかのソフトウェア製品が通知するイベントをSystemwalker Centric Managerで監視することで、さまざまな異常を集中的に監視することができます。例えば、ハードウェアの異常を監視するソフトウェアをSystemwalker Centric Managerで監視することで、アプリケーションやシステムの異常と同様に、ハードウェアの異常も集中的に監視することができます。

- 他ソフトウェア製品をSystemwalker Centric Managerのコンソールから起動する

  ほかの管理ソフトウェア製品のコンソールをSystemwalker Centric Managerのコンソールから直接呼び出すことで、イベントの詳細な調査を行うことや、対処範囲を拡大することができます。

- Systemwalker Centric Managerの監視イベントを他ソフトウェア製品に通知する

  Systemwalker Centric Managerで監視したイベントを、ほかのソフトウェア製品(サービス)にインシデントとして登録することができます。

Systemwalker連携製品認定制度「Systemwalker Enabled」による認定を受けているパートナー製品については、Systemwalkerのホームページを参照してください。

A.1.1　Systemwalkerファミリ

製品名	機能概要
Systemwalker Operation Manager (富士通)	本製品は、定型バッチ業務のスケジューリングをすることで業務運用の省力化を実現します。本製品で運用しているジョブで発生した異常をSystemwalker Centric Managerで監視できます。 Systemwalkerコンソールの監視イベント一覧に表示されたメッセージから詳細画面を直接呼び出すこともできます。
Systemwalker Service Quality Coordinator (富士通)	レスポンス性能、カーネルリソース性能、アプリケーションサーバ性能、データベース性能など、ITシステムのさまざまな構成要素の性能情報を定常的に収集することにより、IT基盤上のサービスが想定どおりに稼働しているか、Systemwalker Centric Managerで監視できます。 また、Systemwalker Centric Managerが収集したネットワーク性能情報を本製品でレポーティングできます。 本製品を利用することで稼働管理と性能管理の統合管理を実現できます。 Systemwalkerコンソールの監視イベント一覧に表示されたメッセージから詳細画面を直接呼び出すこともできます。
Systemwalker Desktop Patrol(富士通)	本製品は、企業・企業グループ全体でパソコンのセキュリティ状況の監査・パッチ適用・ソフトウェアライセンス管理・IT資産の管理を行う製品です。 本製品が検知したライセンス違反など、および本製品のサーバ機能の動作状況・動作異常を Systemwalker Centric Managerの監視画面に表示できます。
ETERNUS SF Storage Cruiser (富士通)	本製品は、SAN (Storage Area Network)、DAS (Direct Attached Storage)、NAS (Network Attached Storage)などの大規模なストレージシステムに対して、構成・障害・性能・関係管理を行う製品です。Storage Cruiserで検知した、ストレージシステムでの障害をSystemwalker Centric Managerで集中監視することができます。

製品名	機能概要
	本製品の管理画面をSystemwalker Centric Managerの監視画面から呼び出すこともできます。

A.1.2 アプリケーションサーバ

製品名	機能概要
Interstage Application Server (富士通)	Interstageを利用した業務アプリケーション(ワークユニット/IJServerクラスタ)の構成の表示および稼働監視が可能です。また、Interstageの性能監視機能(拡張MIB)と連携して性能情報の表示やしきい値監視が可能です。
Oracle E-Business Suite (Oracle)	Oracle E-Business Suiteで構築したシステムを、Systemwalker Centric ManagerおよびSystemwalker for Oracleで監視することにより、システムの安定稼働を実現します。
Interstage Business Application Server (富士通)	Interstageを利用した業務アプリケーション(ワークユニット/IJServerクラスタ)の構成の表示および稼働監視が可能です。また、Interstageの性能監視機能(拡張MIB)と連携して性能情報の表示やしきい値監視が可能です。
SAP	SAP CCMSと連携し、SAP CCMS警告モニタで検知した異常を、Systemwalker Centric Managerで監視することができます。

A.1.3 データベースソフト

製品名	機能概要
Oracle (ORACLE)	Systemwalker for OracleによりOracleで発生したメッセージの意味や対処方法の表示、Oracleのパフォーマンス情報の収集などが可能です。
Symfoware Server (富士通)	Systemwalker for Symfoware Serverにより、Symfowareデータベースの状態監視ができます。検出された異常の対処ノウハウがSystemwalker Centric Managerの監視画面に自動的に表示されるため、対処がスムーズに行えます。 ただし、Systemwalker for Symfoware Serverが連携できるSystemwalker Centric Managerのバージョンは V10.0までであり、Systemwalker Centric Manager V11.0以降でのSymfowareデータベースの状態監視は「メッセージ監視ツール」が必要です。 「メッセージ監視ツール」は、Systemwalker Centric Manager 技術情報に公開されています。

A.1.4 ハードウェア監視ソフト

製品名	機能概要
ServerView Resource Orchestrator	Systemwalkerの管理コンソールにServerViewConsoleを登録しておくことにより、Systemwalkerでイベント確認後に詳細のオペレーションをServerViewにより実行可能です。また、ServerViewで提供される各種MIBデータを登録することにより、サーバハードウェア通知をより詳細かつ正確にシステム管理者へ通知することが可能です。
EPICenter (ExtremeNetworks)	ExtremeNetworks社製ネットワーク装置の設定・監視など詳細な管理が可能です。

A.1.5 クラウドサービスソフト

製品名	機能概要
ServiceNow	Systemwalker Centric Managerで監視したイベントを、ServiceNowにインシデントとして登録し、ServiceNowで管理することができます。ServiceNow連携の詳細については、“ServiceNow連携”を参照してください。

A.1.6 その他

製品名	機能概要
SystemcastWizard Professional	電源投入だけで、OSのセットアップからSystemwalkerのセットアップまでを自動化することができます。

付録B　OS別機能差一覧

Systemwalker Centric Managerの適用対象となるOSの種類により提供される機能が変わります。適用対象OSごとの機能の違いを示します。

なお、Systemwalker Centric Manager V17.0.0以降、Solaris版については業務サーバのみを提供しています。運用管理サーバと部門管理サーバは提供していません。

B.1　構成の管理

B.1.1　ネットワークの構成情報の管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
ノードの検出	○	○	○	△ (注3)	○	○ (注1)	○ (注1)
アプリケーションの検出	○	○	○	○	○	△ (注2)	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.1.2　システムの構成情報の管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
インベントリ管理	△ (注2)	○	○ (注9)	○	○ (注9)	△ (注2)	△ (注2) (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.1.3　コンソール

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
Systemwalkerコンソール	○	○	○	○	○	－	－

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
Systemwalker Web コンソール	○	○	○	○	○	－	－
Systemwalker Web コンソール(モバイル版)	△ (注13)	△ (注14)	△ (注7) (注14)	△ (注14)	△ (注7) (注14)	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.2　資源の配付

B.2.1　資源配付

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
資源配付	△ (注2)	△ (注2)	△ (注2、10)	△ (注2)	△ (注2、10)	△ (注2)	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3　ネットワーク/システムの監視

B.3.1　稼働監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
稼働状態の監視	○	○	○	△ (注3)	○	○ (注1)	○ (注1)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.2　障害監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
トラップの監視	○ (注11)	○	○ (注7)	○	○ (注7)	○ (注1)	○ (注1)
MIBしきい値監視	○	○	○ (注7)	△ (注3)	○ (注7)	○ (注1)	○ (注1)
システムのイベント監視 (注4)	○	○	○ (注16)	○	○ (注16)	△ (注2)	△ (注2) (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.3　ネットワーク性能監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
性能異常の監視	○	○	○	△ (注3)	○	○	○
性能情報の表示	○	○ (注20)	○ (注7) (注20)	△ (注3)	○ (注7)	○	○

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.4　サーバ性能監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
性能異常の監視	○	○ (注21)	○ (注21)	△ (注18)	○ (注18)	△ (注2)	△ (注2) (注19)
性能情報の表示	○	○	○ (注7)	△ (注18)	○ (注7) (注18)	△ (注2)	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.5　DHCP監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE
DHCPクライアント監視	○	○	○ (注7)	○	○ (注7)	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.6　イベントコリレーション

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
イベントコリレーション	○	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.7　メッセージ変換

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
メッセージ変換	○	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.8　イベント抑止

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
イベント抑止	○	○	○	○	○	△ (注6)	△ (注6)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.3.9　監視抑止

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
監視抑止	○	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.4　アプリケーションの監視

B.4.1　稼働監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
アプリケーションの稼働状態の表示	○	○	○	○	○ (注23)	○ (注1)	×
アプリケーションの稼働状態の監視	○	○	○	○	○ (注23)	○ (注1)	○ (注1) (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.4.2　障害監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
アプリケーションのイベント監視	○	○	○	○	○	○ (注1)	○ (注1) (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.4.3　性能監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
性能異常の監視	○	○	○ (注7)	○	○ (注7)	○	×
性能情報の表示	○	○	○ (注7)	○	○ (注7)	○	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.5　ソフトウェア修正管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
ソフトウェア修正管理	○	○	○	○	○	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.6　ポリシー

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
ポリシーの配付	○	○	○ (注7)	○	○ (注7)	○	○
ポリシーの参照	○	○	○ (注7)	○	○ (注7)	○	○
ポリシーの移出	○	○	○ (注7)	○	○ (注7)	○	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.7　Systemwalker自身の監視

B.7.1　イベントトレース

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
イベントトレース	○	○	○ (注7)	○	○ (注7)	○ (注1)	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.7.2　Systemwalkerのプロセス監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
Systemwalkerのプロセス監視	○	○	○ (注7)	○	○ (注7)	○	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.7.3　Systemwalkerセルフチェック

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
Systemwalkerセルフチェック	○	○	○ (注7)	○	○ (注7)	○ (注1)	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.7.4　スローダウン監視

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
イベントのスローダウン監視	○	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.7.5　IPC資源の一元管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
IPC資源の一元管理	－	○	○ (注7)	○	○ (注7)	○	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.8　障害の復旧

B.8.1　リモートからの操作

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
リモート操作	○ (注22)	× (注5)	× (注5)	× (注5)	× (注5)	× (注5)	× (注5)
リモートコマンド (サーバの操作はメニューからtelnetを呼び出し操作できます。)	○	○	○ (注8)	○	○ (注8)	○ (注1)	○ (注1) (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.8.2　リモートからの電源投入・切断

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux			HP-UX	AIX
	SE/EE	SE/EE	GEE	SE	EE	GEE (注15)	SE/EE	SE/EE
クライアントの電源投入・切断 (運用管理クライアントから運用管理サーバを経由して操作できます。)	○	○	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.8.3　障害対処の自動化

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
自動アクション	○	○	○	○	○	○	○ (注19)

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.9　返答メッセージ

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
返答メッセージ	－	○	○	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.10　評価

B.10.1　監査ログ分析

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
監査ログ分析	○	○	○	○	○	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.11　セキュリティ

B.11.1　サーバアクセス制御

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
サーバアクセス制御	○ (注24)	× (注17)	× (注17)	× (注17)	× (注17)	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.11.2　コンソール操作制御

注釈の詳細については、“注釈”を参照してください。

機能	Windows		Solaris			Linux			HP-UX	AIX
	SE	EE	SE	EE	GEE	SE	EE	GEE (注15)	SE/EE	SE/EE
コンソール操作制御 (注12)	×	○	×	○	○	×	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.11.3　操作ログ出力

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
操作ログ出力	○	○	○	○	○	○	－

○：該当機能使用可能
△：該当機能のうち一部使用可能

×：該当機能使用不可
－：該当なし

B.11.4　監査ログ出力

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
監査ログ出力	○	○	○	○	○	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.11.5　監査ログ管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
監査ログ管理	○	○	○	○	○	○	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.11.6　監査ログ分析

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
監査ログ分析	○	○	○	○	○	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.12　共通(さまざまなシステムでの利用)

B.12.1　高信頼システムの管理

注釈の詳細については、“注釈”を参照してください。

機能	Windows		Solaris			Linux			HP-UX		AIX	
	SE	EE	SE	EE	GEE	SE	EE	GEE (注15)	SE	EE	SE	EE
クラスタ構成の管理	×	○	×	○	○ (注7)	×	○	○ (注7)	－	－	－	－
クラスタサービスの稼働監視												
業務サーバのクラスタ化	×	○	×	○	－	×	○	－	×	○	×	×
LAN二重化環境の監視	×	×	×	○	○	×	○	○	×	×	×	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.12.2　管理サーバの高信頼化

注釈の詳細については、“注釈”を参照してください。

機能	Windows		Solaris			Linux			HP-UX	AIX
	SE	EE	SE	EE	GEE	SE	EE	GEE (注15)	SE/EE	SE/EE
管理サーバのクラスタ化 (EE版の運用管理サーバ、部門管理サーバで使用可能)	×	○	×	○	○	×	○	○	－	－
運用管理サーバ二重化	×	○	×	○	○	×	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.12.3　大規模システム

注釈の詳細については、“注釈”を参照してください。

機能	Windows		Solaris			Linux			HP-UX	AIX
	SE	EE	SE	EE	GEE	SE	EE	GEE (注15)	SE/EE	SE/EE
全体監視 (EE版の運用管理サーバで使用可能)	×	○	×	○	○	×	○	○	－	－

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.13　Systemwalkerスクリプト

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
Systemwalkerスクリプト	○	○	○ (注7)	○	○ (注7)	○	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.14　トラブルシューティング

B.14.1　調査資料の採取

注釈の詳細については、“注釈”を参照してください。

機能	Windows	Solaris		Linux		HP-UX	AIX
	SE/EE	SE/EE	GEE	SE/EE	GEE (注15)	SE/EE	SE/EE
保守情報収集ツール	○	○	○	○	○	○	×

○：該当機能使用可能
△：該当機能のうち一部使用可能
×：該当機能使用不可
－：該当なし

B.15　注釈

注1)

被監視機能と資源配付を受ける機能だけサポートしています。

注2)

被監視機能と資源配付を受ける機能をサポートしていますが、制限事項があります。

－ アプリケーションの検出
以下のパッケージ情報は取得できません。

- インストール日付
- 製品名
- 製品バージョン
- 会社名
- 著作権
- 説明
- パッケージ名

－ インベントリ管理
収集可能なインベントリ情報については、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

ー 資源配付

- クライアント/業務サーバからの呼び出し配付は、HTTPS、S/MINEが使用できません。詳細については、“配付先システムを選択する”を参照してください。

ー システムのイベント監視
メール連携機能を使用してイベントを通知する場合、暗号化(S/MIME)を使用して通知することはできません。

- HP-UXの場合

  システムのホスト名が8バイトを超える場合、シスログのメッセージ監視はできません。

ー サーバ性能監視

- HP-UXの場合
  実メモリ使用率、実メモリ空き容量の監視ができません。
  「性能監視(システム性能収集)機能」をインストールした場合、SNMPv3を使用した運用はできません。

- AIXの場合
  HD待ち要求数の監視ができません。
  マイクロ・パーティショニングによりLPAR環境上で動作している場合、割り当てられた仮想CPU単位にCPU使用率を監視します。

- 以下の項目は、監視を行うために必要なソフトウェアをインストールする必要があります。

  インストールが必要なソフトウェアについては、“関連ソフトウェア資源”を参照してください。

  -AIX版

  ・実メモリ使用率

  -HP-UX版

  ・HD待ち要求数

  -Linux版

  ・プロセッサ待ちスレッド数

  ・HD待ち要求数

注3)

監視/被監視の機能をサポートしていますが、被監視機能に制限があります。

ー ノードの検出
以下のインタフェース情報を正しく検出できません。

- インタフェース名
- MACアドレス
- ifType
- ifSpeed

ー 稼働状態の監視
複数インタフェースをもつノードの場合、ノードの状態が青色(一部インタフェース停止)で表示される場合があります。

ー MIBしきい値監視
SNMPエージェントが起動されていても、MIB情報が正しく取得できない場合があります。詳細については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“ノードのMIB情報を監視する”を参照してください。

ー ネットワーク性能監視
回線使用率だけ監視できます。
ノード中心マップ/ペアノード経路マップでは、パケット数は表示されません。
[インタフェース詳細表示]では、[受信バイト数]、[送信バイト数]、[回線使用率]だけが表示されます。そのほかは「?」、または「--」で表示されます。

注4)

被監視ノードがWindowsの場合は、ウィルス監視が可能です。

注5)

Windows版との併用によりクライアントへの操作ができます。

注6)

ネットワーク/システムの監視でイベント抑止を使用する場合、同一イベント抑止機能だけ使用可能です。

注7)

被監視システムがUNIX/Windowsの場合、EE版と同じ範囲の機能が使用できます。被監視システムがグローバルサーバの場合、機能は使用できません。

注8)

リモートコマンドAPIを使用して作成したアプリケーションでは、グローバルサーバの応答は取得できません。

同時に使用できる[リモートコマンド実行]ウィンドウの数は、「リモートコマンドウィンドウ識別子の登録」で定義したリモートコマンドウィンドウ識別子の数です。

注9)

被監視システムがグローバルサーバの場合、インベントリ管理機能は使用できません。

注10)

GSをホストとして運用している環境の場合、上位にUNIX運用管理サーバを置き、運用管理サーバからGSおよびGS配下のシステムに対して、以下の管理・操作を行うことができます。

- GS部門管理サーバ、GS部門管理サーバ直下のクライアント、およびGS部門管理サーバ配下の各種業務サーバに対して、配付状況の管理
- GSが扱う資源の登録/配付

注11)

Microsoft SNMP Trap Serviceとの連携を行う場合、SNMPv2C形式のEnterprise Specificトラップ、およびSNMPv3形式のSNMPトラップを監視することができません。

注12)

コンソール操作制御を使用する場合、Systemwalker Webコンソールは使用できません。

注13)

運用管理サーバがWindows(64bit)版の場合、Systemwalker Webコンソール(モバイル版)は使用できません。

注14)

運用管理サーバの文字コードがUTF-8の場合、Systemwalker Webコンソール(モバイル版)は使用できません。

注15)

Linux for Intel64版が対象です。

注16)

被監視システムがグローバルサーバの場合、これらをインストールレス型エージェントとして監視することはできません。

注17)

運用管理サーバでは、部門管理サーバ/業務サーバ(ともにWindows)に対するセキュリティポリシーの設定を行うことはできますが、運用管理サーバ自身のサーバアクセス制御はサポートしていません。

注18)

「実メモリ使用率」および「実メモリ空き容量」は、free -kコマンドの出力結果から算出します。Red Hat Enterprise Linux 7.0以前とRed Hat Enterprise Linux 7.1以降で算出方法が異なります。

【Red Hat Enterprise Linux 7.0以前】

実メモリ使用率 = (「-/+ buffers/cache」行の「used」項の値)/(「Mem」行の「total」項の値)×100

実メモリ空き容量 = (「-/+ buffers/cache」行の「free」項の値)

【Red Hat Enterprise Linux 7.1以降】

実メモリ使用率 = ((「Mem」行の「total」項の値)-(「Mem」行の「available」項の値))/(「Mem」行の「total」項の値)×100

実メモリ空き容量 = (「Mem」行の「available」項の値)

注19)

利用できるのは、インストールレス型エージェント監視機能の範囲だけです。

注20)

部門管理サーバおよび業務サーバの場合、non-global zoneで動作するノードは、ネットワーク性能監視機能のトラフィック情報となるMIBの値が0となります。

注21)

部門管理サーバおよび業務サーバの場合、non-global zoneで動作するノードに対し、サーバ性能の監視を行うことはできません。

注22)

以下のOSの場合、リモート操作機能のメッセージ転送で入力できる文字はASCII文字のみとなります。

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10

注23)

グローバルサーバで動作するワークユニット、アプリケーションは監視できません。

注24)

Windows Server 2022 上のSystemwalker Centric Managerに対して、サーバアクセス制御機能は使用できません。

付録C　製品の組み合わせ

ここでは、Systemwalker Centric Managerの製品組み合わせの詳細について説明します。

- エディションの組み合わせ
- バージョンの組み合わせ

C.1　エディションの組み合わせ

Systemwalker Centric Manager SEとSystemwalker Centric Manager EEを組み合わせて導入することができます。Systemwalker Centric Manager EEは、Systemwalker Centric Manager EEで提供している機能が必要なシステムにだけ導入します。

Systemwalker Centric Manager EEとSystemwalker Centric Manager SEを組み合わせる場合、以下の方法で組み合わせることができます。

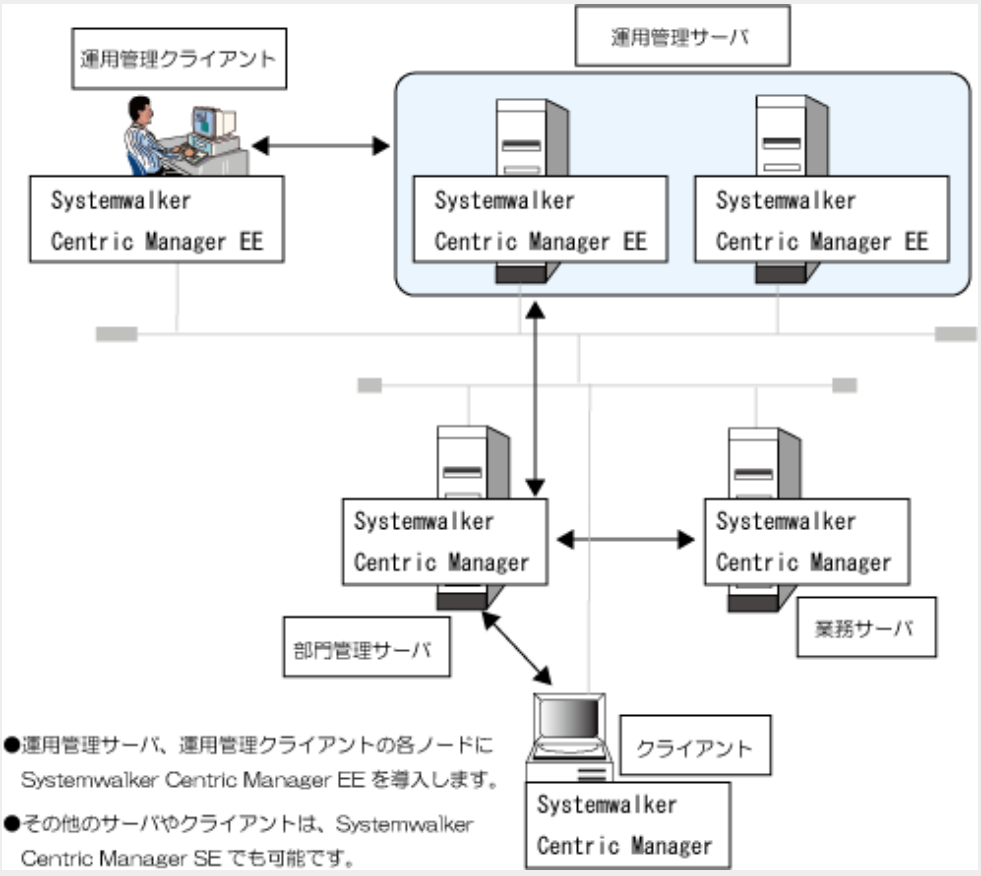
- 運用管理サーバと運用管理クライアントに導入するSystemwalker Centric Managerのバージョンとエディションは同一とします。ただし、異なるマイナーバージョン（レベル）でも、監視することは可能です。
- 部門管理サーバ、業務サーバ、クライアントには、Systemwalker Centric Manager EEで提供している機能が必要なシステムだけにSystemwalker Centric Manager EEを導入します。
- クラスタシステムに導入する場合は、ノードごとにSystemwalker Centric Manager EEを導入します。

以下に、組み合わせて導入する場合の構成例を示します。

EE GEE **運用管理サーバをクラスタ構成にする場合**

運用管理サーバをクラスタシステムに導入する場合の導入方法について“運用管理サーバをクラスタ構成にする場合”に示します。

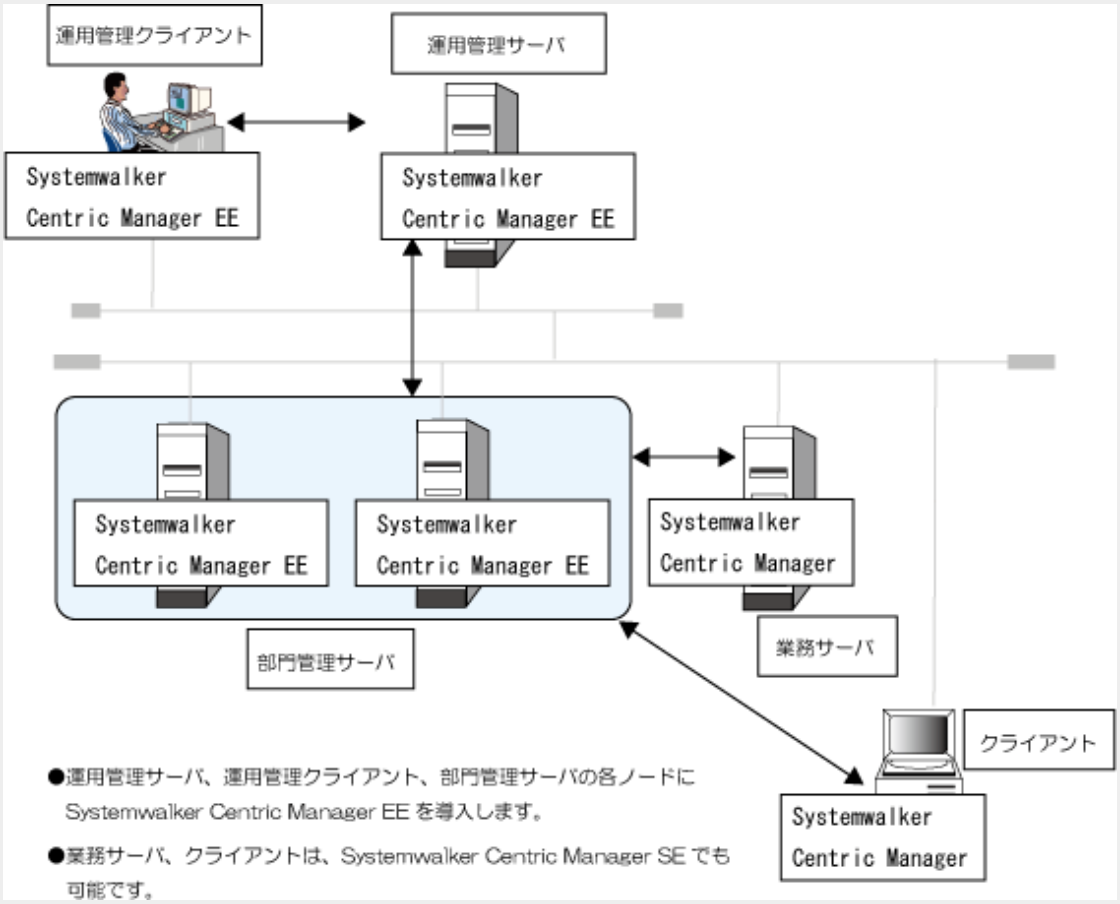
図C.1 運用管理サーバをクラスタ構成にする場合



EE GEE 部門管理サーバをクラスタ構成にする場合

部門管理サーバをクラスタシステムに導入する場合の導入方法について“部門管理サーバをクラスタ構成にする場合”に示します。

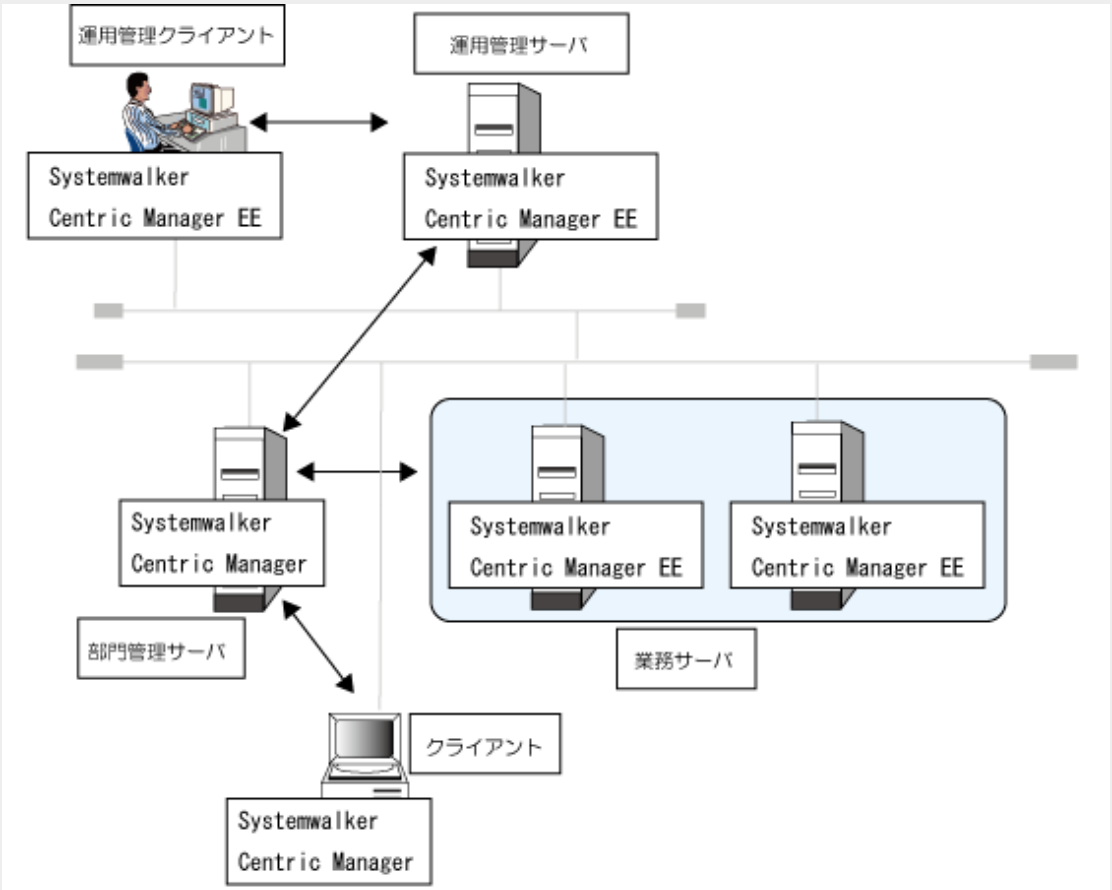
図C.2 部門管理サーバをクラスタ構成にする場合



EE GEE 業務サーバをクラスタ構成にする場合

業務サーバをクラスタシステムに導入する場合の導入方法について“業務サーバをクラスタ構成にする場合”に示します。

図C.3 業務サーバをクラスタ構成にする場合

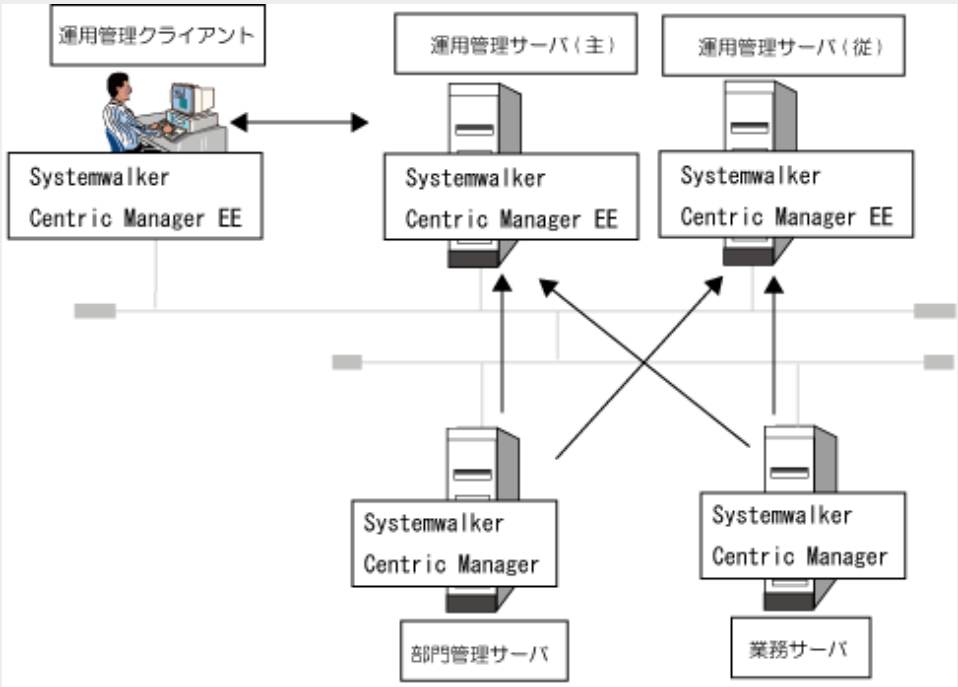


●運用管理サーバ、運用管理クライアント、業務サーバの各ノードに、Systemwalker Centric Manager EE を導入します。
●部門管理サーバ、クライアントは、Systemwalker Centric Manager SE でも可能です。

EE GEE **管理サーバを二重化する場合**

運用管理サーバを複数台設置するような運用を行う場合の導入方法について、“管理サーバを二重化する場合”に説明します。

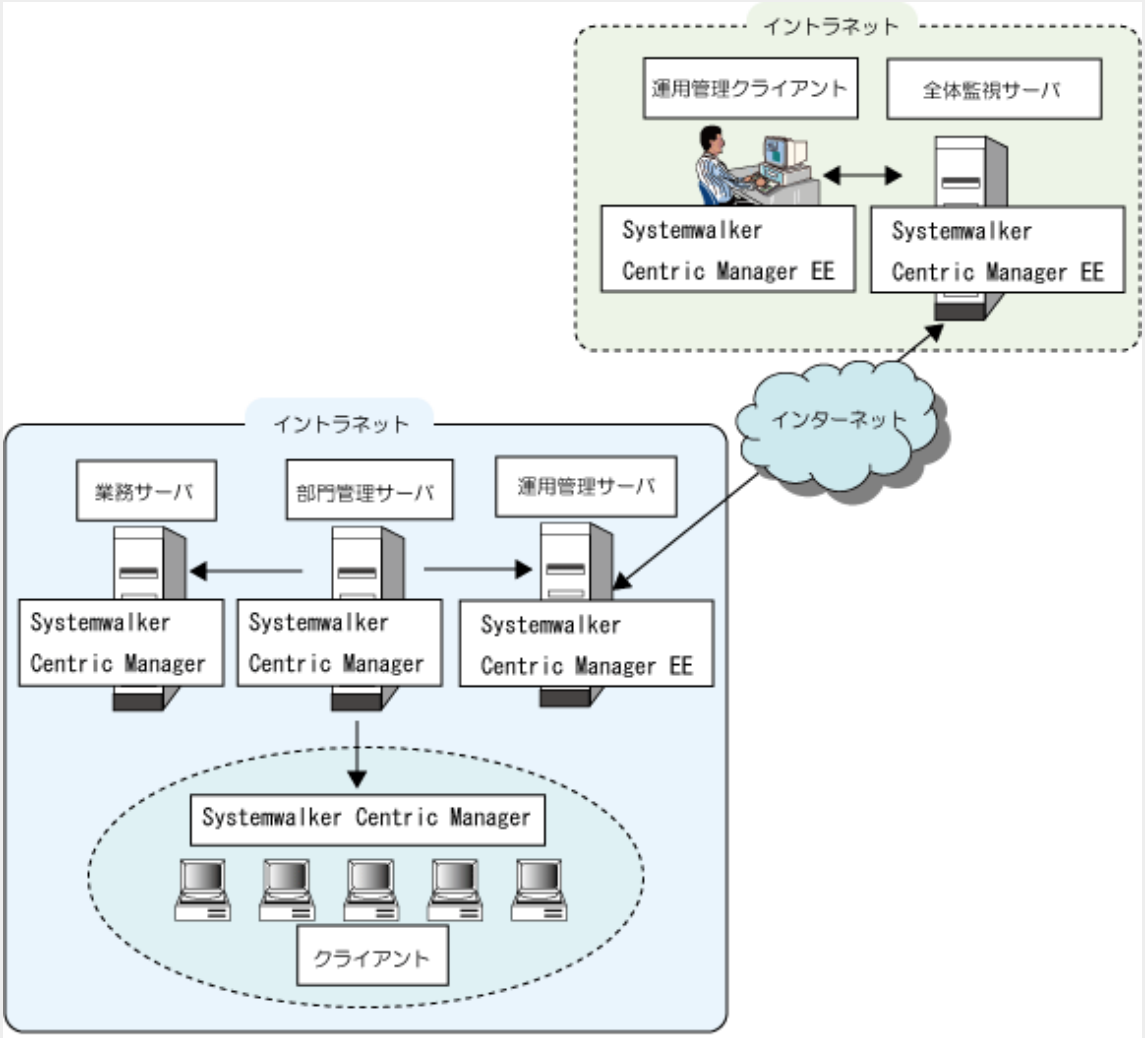
図C.4 管理サーバを二重化する場合



EE GEE **アウトソーシングを行う場合**

アウトソーシングを行う場合の導入方法について、“アウトソーシングを行う場合”に説明します。

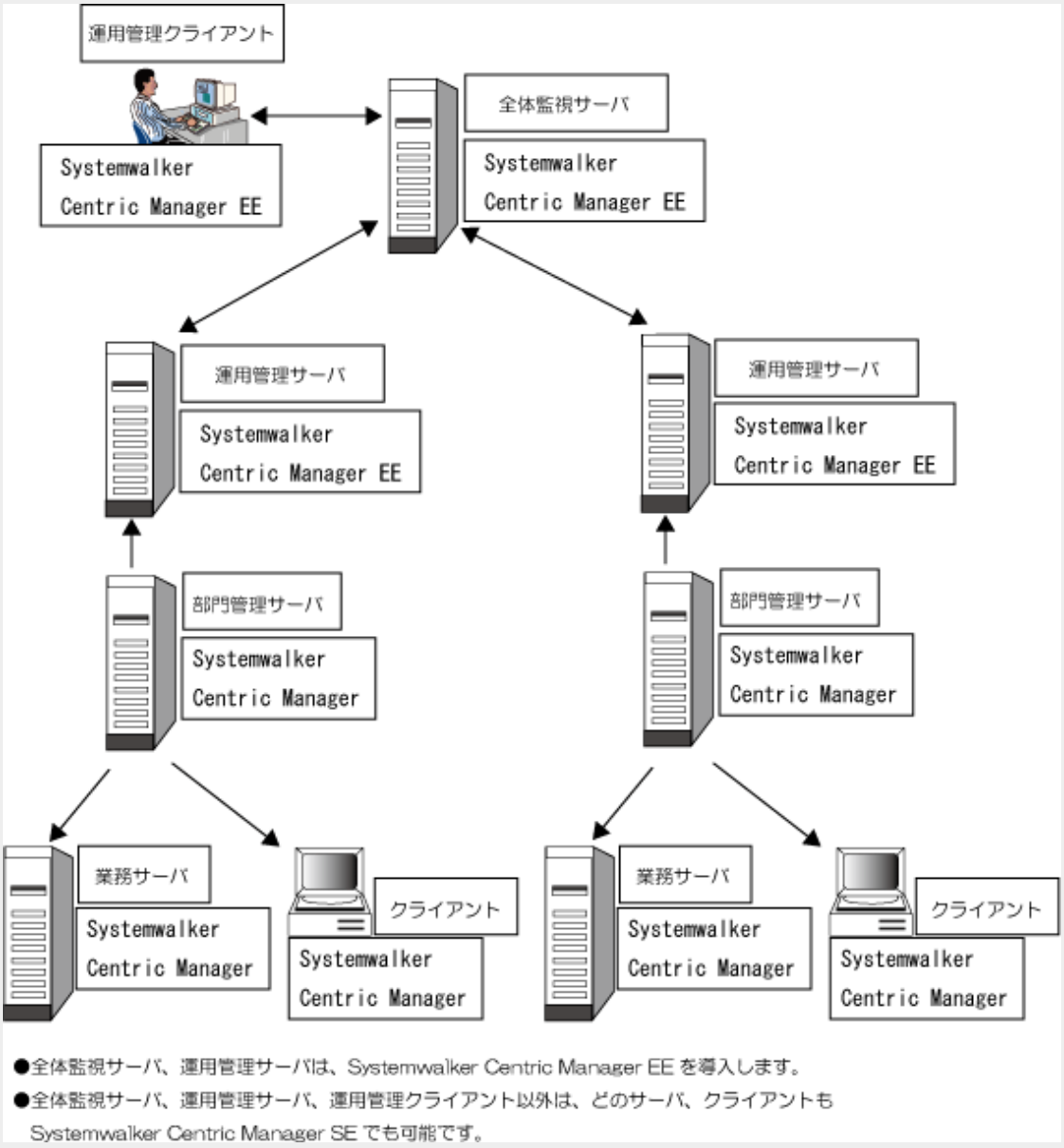
図C.5 アウトソーシングを行う場合



EE GEE **全体監視を行う場合**

個々のサイトを管理する運用管理サーバ(マネージャ)の上位に、それらを集約する運用管理サーバを置くM of M(Manager of Manager)運用を行う場合の導入方法について、“全体監視を行う場合”に説明します。

図C.6 全体監視を行う場合



C.2　バージョンの組み合わせ

Systemwalker Centric Manager間のプラットフォーム、およびバージョンの組み合わせについて説明します。

V15.3.0以降のバージョンと組み合わせる場合

運用管理サーバへ接続する運用管理クライアントの機能

運用管理クライアントのバージョンが、V15.3.0以降の場合、以下の機能については、運用管理クライアントのバージョンの機能範囲に限定されます。

- 仮想ノードの監視に関する機能
  - Systemwalkerコンソール
    - [仮想ノードの検出(全体)]メニュー
    - [仮想ノードの検出(指定ノード)]メニュー

- [仮想ノードの追加]メニュー
- [ポリシー]メニューの[仮想ノードの監視]メニュー
- [関係情報作成]画面
- [関係情報プロパティ]画面
- [ノードプロパティ]画面
- [ノード作成]画面

・ ローリングアップデートに関する機能

ー 資源配付コンソール

- [設定]-[連携]メニュー
- [資源の適用]メニュー

V13.3.0以降のバージョンと組み合わせる場合

インストールレス型エージェント監視機能

V13.3.0以降の運用管理サーバ、および部門管理サーバを監視サーバに指定してインストールレス型エージェント監視する場合、使用できる機能は監視サーバのバージョンにおける機能範囲となります。

V13.2.0以前のバージョンと組み合わせる場合

インターネットサーバ管理機能

運用管理サーバ、部門管理サーバ、および業務サーバ上では、インターネットサーバ管理機能は使用できません。

また、V13.2.0以前のバージョンからバージョンアップする場合の注意事項については、“Systemwalker Centric Manager バージョンアップガイド”の“インターネットサーバ管理機能を使用していた場合”を参照してください。

ヘルプデスク機能

ヘルプデスク機能は使用できません。

C.2.1 プラットフォームとバージョン混在時の接続性

プラットフォームやバージョンを混在して接続した場合、使用できる機能は、それぞれのSystemwalker Centric Managerが共通でサポートしている範囲です。

運用管理サーバと運用管理クライアントの接続性

運用管理サーバと運用管理クライアントはメジャーバージョンが同一、かつ運用管理クライアントのマイナーバージョンが同一以上の場合、相互接続が可能です。

接続できない運用管理サーバに接続した場合、運用管理クライアントに以下のメッセージが表示されます。

指定された運用管理サーバは、Systemwalkerコンソールが接続できないバージョンであるため、ログインできません。

運用管理サーバと部門管理サーバ/業務サーバ/クライアントの組み合わせ

運用管理サーバと部門管理サーバ/業務サーバ/クライアントは、共通でサポートしている機能範囲で使用可能です。

		運用管理サーバのOS	
		Solaris Linux	Windows
部門管理サーバ/ 業務サーバのOS	UNIX Linux	○	○
	Windows	○	○
クライアント		○	○

○：接続可（共通でサポートしている機能範囲で使用可能）

部門管理サーバ/業務サーバと業務サーバ/クライアントの組み合わせ

部門管理サーバ/業務サーバと業務サーバ/クライアントは、共通でサポートしている機能範囲で使用可能です。

		部門管理/業務サーバのOS	
		UNIX Linux	Windows
業務サーバのOS	UNIX Linux	○	○
	Windows	○	○
クライアント		○	○

○：接続可（共通でサポートしている機能範囲で使用可能）

EE GEE **全体監視サーバと運用管理サーバの組み合わせ**

全体監視サーバと運用管理サーバのバージョンレベルが異なる場合、接続できるのは同じバージョンレベルか、より新しいバージョンレベルの全体監視サーバになります。

C.2.2 リモート操作エキスパートとリモート操作クライアントの接続

複数のバージョンやレベルのリモート操作エキスパート(操作する側)とリモート操作クライアント(リモート操作される側)が共存していても、接続は可能です。

ただし、リモート操作クライアントは、リモート操作エキスパートと同じバージョンレベルか、より新しいバージョンレベルのリモート操作クライアントになります。

なお、リモート操作モニタは、リモート操作エキスパートと同じになります。

C.2.3 上位システムの製品バージョンレベルが、下位システムより古い場合のサーバOS表示について

上位システムの製品バージョンレベルが、下位システム(監視対象)より古い場合、監視対象となるWindowsのサーバOSが最新であっても、OS種別は異なって表示されます。

上位システムの製品バージョンレベル	監視対象のWindowsのOS	表示されるOS種別/OS名(注1)
Systemwalker Centric Manager V15.3.0	Windows Server 2022	Windows Server 2019
Systemwalker Centric Manager V15.2.1	Windows Server 2022 Windows Server 2019	Windows Server 2016
Systemwalker Centric Manager V13.6.1～V15.2.0	Windows Server 2022 Windows Server 2019	Windows Server 2012

上位システムの製品バージョンレベル	監視対象のWindowsのOS	表示されるOS種別/OS名(注1)
	Windows Server 2016	
Systemwalker Centric Manager V13.3.0～V13.6.0	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012	Windows Server 2008
Systemwalker Centric ManagerV13.2.0 以前	Windows Server 2022 Windows Server 2019 Windows Server 2016 Windows Server 2012 Windows Server 2008	Windows Server 2003

注1)

ノード検出またはインベントリ収集を行った場合、[OS種別]が“Unknown”となることがあります。この場合は、手動で下記の設定を行ってください。

[Systemwalkerコンソール[編集]]画面から[ノードプロパティ]画面を表示します。

- [OS種別]:“Other”を選択
- [OS名]: 上記の表内の当該バージョンレベルの「表示されるOS種別/OS名」を選択

C.2.4 Windows 11のOS表示について

Windows 11が下位システム(監視対象)のOSであった場合、導入する製品バージョンレベル、および、上位システム(監視サーバ)の製品バージョンレベルによって、OS種別が“Windows 10”と表示される場合があります。

製品バージョンレベルの組み合わせにより、表示されるOS種別を以下に示します。

上位システムの製品バージョンレベル	監視対象の製品バージョンレベル	表示されるOS種別/OS名
Systemwalker Centric Manager V17.0.0以降 Linux	Systemwalker Centric Manager V17.0.1以降	Windows 11
	Systemwalker Centric Manager V17.0.0	Windows 10(注)
Systemwalker Centric Manager V17.0.0以降 Windows	Systemwalker Centric Manager V17.0.0以降	Windows 10(注)

注)

ノード登録時、[OS種別]が“Unknown”となることがあります。この場合は、手動で下記の設定を行ってください。

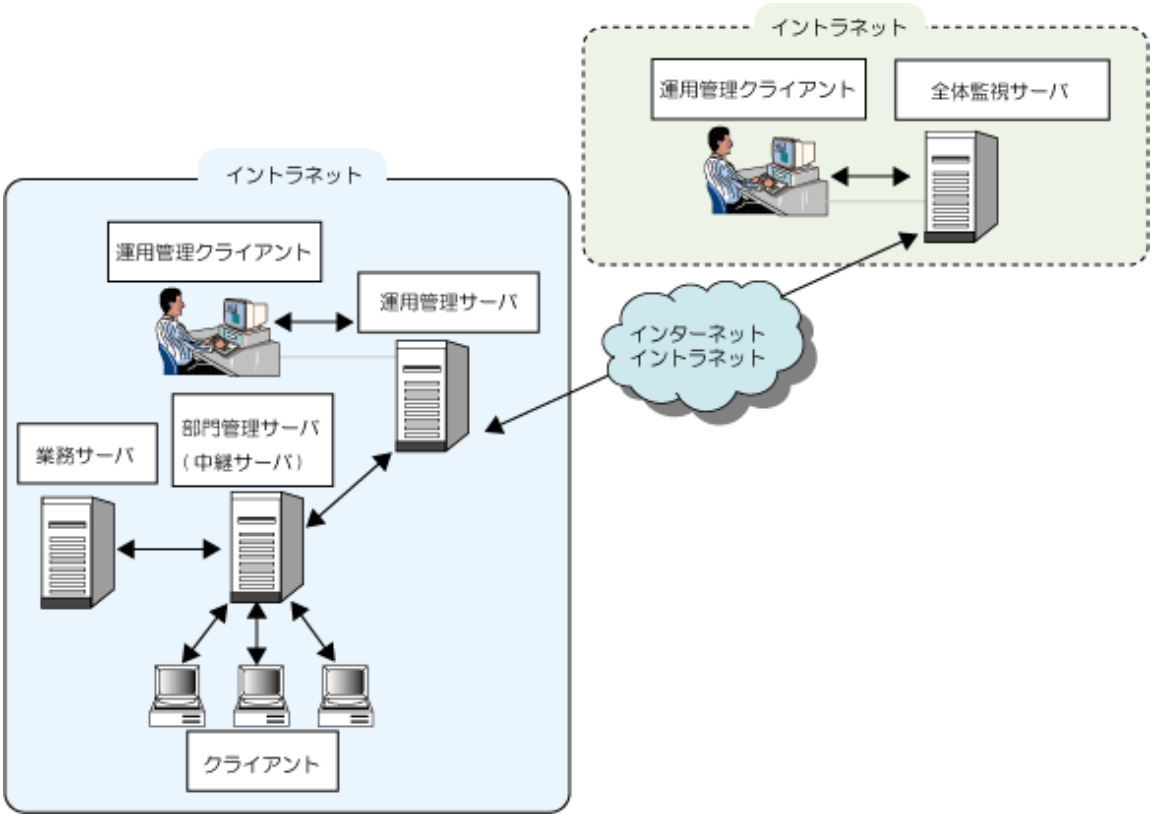
[Systemwalkerコンソール[編集]]画面から[ノードプロパティ]画面を表示します。

- [OS種別]:“Other”を選択
- [OS名]: 上記の表内の当該バージョンレベルの「表示されるOS種別/OS名」を選択

付録D　Systemwalker Centric Managerの制限値と推奨値

Systemwalker Centric Managerの主な制限値および推奨値について説明します。構成図を以下に示します。

図D.1 構成図



D.1　制限値のある主な機能

制限値のある機能について説明します。

D.1.1　監視

内容	インストール種別	制限値	備考
アプリケーションの異常監視を行う場合に監視可能なログファイル数 (イベントログやシスログにメッセージを出力しないアプリケーションのテキスト形式のログファイル監視)	運用管理サーバ 部門管理サーバ 業務サーバ	1サーバにつき200ファイル	
監視イベント一覧に表示できるメッセージの件数	全体監視サーバ 運用管理サーバ	1,000件 (カスタマイズが可能です。詳細は“Systemwalker Centric Managerリファ	

内容	インストール種別	制限値	備考
		レンスマニュアル”の“Systemwalkerコンソールサービスの定義ファイル”を参照してください。)	
メッセージをログとして蓄積できる数	全体監視サーバ 運用管理サーバ 部門管理サーバ 業務サーバ	フレームワークデータベースのサイズに依存します。 詳細は、“Systemwalker Centric Manager 導入手引書”の“データベース領域の詳細見積もり式”を参照してください。 部門管理サーバ、業務サーバは以下の制限値があります。 ・ Windows の場合：327,660 ・ Solaris 、 HP-UX、Linux の場合：2,000,000 フレームワークデータベースには依存しません。	
Systemwalker Centric Managerの起動前に、シスログまたは監視ログファイルにメッセージ出力された場合に、監視対象となるメッセージ数		シスログ: 最新の500件 監視ログファイル: 最新の500件(監視ログファイルごと)	UNIX版だけの制限値
ログファイル監視を行う対象ファイルの最大サイズ		2GB	UNIX版だけの制限値 ただし、Linux for Intel64版ではこの制限はありません。
監査ログのログ収集コマンドの同時実行数	運用管理サーバ	10多重 (注)	被管理サーバ(部門管理サーバ、業務サーバ)の台数が50台の場合は、10台ごとに時間をあけてスケジュールする必要があります。
監査ログを圧縮したログ(圧縮ログ)の上限サイズ	運用管理サーバ	2GB	
収集対象のイベントログのイベントの「説明」の上限	運用管理サーバ 部門管理サーバ 業務サーバ	1つのイベントのすべての項目(日付、時刻など)の長さの合計が4KB	

内容	インストール種別	制限値	備考
インストールレス型エージェントの監視	運用管理サーバ 部門管理サーバ	300台	1台の運用管理サーバ/部門管理サーバで監視できる被監視サーバは、300台です。
全体監視サーバで監視できる運用管理サーバの台数	全体監視サーバ→運用管理サーバ	61台	全体監視サーバの性能と回線速度に依存します。

注) 同時に実行開始できるのが10多重です。

D.1.2 管理者への通知

内容	インストール種別	制限値	備考
自動アクションでメール通知できるあて先の数		無制限	

D.1.3 高信頼性システム

内容	インストール種別	制限値	備考
運用管理サーバの多重化できる台数	運用管理サーバ	4台	EEだけのサポート

D.1.4 管理形態

内容	インストール種別	制限値	備考
1台の運用管理サーバに同時接続できる運用管理クライアントの台数	運用管理クライアント	SE: 8台 EE: 50台 GEE: 50台	

D.1.5 返答メッセージ

内容	インストール種別	制限値	備考
同時に発行できる返答要求の数	運用管理サーバ 部門管理サーバ 業務サーバ	100件	UNIX版だけのサポート

D.2 円滑に運用管理するための推奨値

本書の値は、円滑に運用できるための推奨値です。

回線や監視台数によっては、値が異なる場合があります。

D.2.1 監視

内容	インストール種別	推奨値	備考
全体監視サーバで監視できる運用管理サーバの台数	全体監視サーバ → 運用管理サーバ	32台	全体監視サーバの性能と回線速度に依存
1台の運用管理サーバで監視できる部門管理サーバの台数	運用管理サーバ → 部門管理サーバ	50台	運用管理サーバの性能と回線速度に依存
1台の運用管理サーバで監視できる業務サーバの台数	運用管理サーバ → 業務サーバ(注)	300台	運用管理サーバの性能と回線速度に依存
1台の運用管理サーバで監視できるノード数(運用管理サーバ+部門管理サーバで監視できるノード数も同様)	運用管理サーバ(+部門管理サーバ)→ 部門管理サーバ、業務サーバ(注)、クライアント	3,000ノード	運用管理サーバの性能と回線速度に依存 (部門管理サーバを含む場合、部門管理サーバの性能にも依存)
1台の運用管理サーバで監視できるネットワーク性能の監視対象数(部門管理サーバで監視できる数も同様)	運用管理サーバ(部門管理サーバ) → 業務サーバ(注)、クライアント	300インタフェース (監視対象ノードのインタフェースの合計)	運用管理サーバ(部門管理サーバ)の性能と回線速度に依存
1台の運用管理サーバのSystemwalker Webコンソールに Webブラウザから同時接続する台数	運用管理サーバ	SE: 8台以下 EE: 50台以下 GEE: 50台以下	同一の運用管理サーバに運用管理クライアントのSystemwalkerコンソールから同時接続する場合、運用管理クライアントの台数も合計した値が推奨値となるようにしてください。
パフォーマンスを保てるアプリケーションの監視数	運用管理サーバ → 部門管理サーバ、業務サーバ(注)	・ 被監視サーバ1ノード =約100 アプリケーション ・ 監視するすべてのサーバのアプリケーション監視数を合計した数(アプリケーション総数)が、約5,000個	監視サーバが、総数5,000個を超えるアプリケーションを監視したいときは、以下のように稼働状況(表示色)を0分にして、稼働状態通知を随時通知しないように設定します。 そして必要な場合だけ、Systemwalkerコンソールから、「最新稼働状態を表示」を操作するようにすれば、パフォーマンスを下げることなく運用することができます。 ・ [稼働ポリシー監視間隔]：任意 ・ [稼働状況取得間隔]：0分
1台の運用管理サーバまたは中継サーバでログ収集できる被管理サーバ（部門管理サー	運用管理サーバまたは中継サーバ	75台	次の環境に大きく依存します。 ・ 運用管理サーバの性能、ディスク容量

内容	インストール種別	推奨値	備考
バ、業務サーバ）の台数			・ 回線速度(ネットワーク) ・ 収集するログのサイズ 以下の運用の考慮により75台以上の収集が可能です。 ・ 収集を実施する時間(業務時間外の実施) ・ 収集の段階的実施(10台ずつ単位で収集操作をずらしての実施) ・ 複数回の収集の実施(1回あたりの収集ログ量を減らす)
監査ログのログ収集コマンドの同時実行数	運用管理サーバ	10多重	被管理サーバ(部門管理サーバ、業務サーバ)の台数が50台の場合は、10台ごとに時間をあけてスケジュールする必要があります。
ワイルドカード指定で収集されるファイルの最大数	運用管理サーバ 部門管理サーバ 業務サーバ	366以内	
収集対象ログファイルの1回あたりの容量	運用管理サーバ →部門管理サーバ業務サーバ	60MB以下	収集対象ログファイルの、1ファイル1回あたりの転送容量になります。
アクセス制御ポリシーの優先ルールに設定するユーザ/グループ数の合計	運用管理サーバ 部門管理サーバ 業務サーバ	10以下	運用管理サーバ、部門管理サーバ、および業務サーバの性能に依存します。

注) インストールレス型エージェント監視の業務サーバも含みます。

D.2.2 資源配付

内容	インストール種別	推奨値	備考
運用管理サーバから資源を配付できる中継サーバの台数	運用管理サーバ → 中継サーバ	50台 (同時接続数)	次の要因により変更 ・ 配付する資源のサイズ ・ 回線の太さ 配付のタイミング、資源の分割、同時接続数などのサーバのパラメタ設定やクライアントの受信タイミングなどにより50台以上も接続可能
中継サーバから資源を配付できるクライアントの台数	中継サーバ → クライアント	100台 (同時接続数)	

D.3　ポーリング間隔

運用管理サーバまたは部門管理サーバから、ネットワークやシステムを監視するため定期的にポーリングを行います。

ポーリング間隔の最小、最大、初期値について説明します。

D.3.1　稼働状態の監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
ノードの稼働状態を監視する。 稼働状態の監視結果としては、稼働状態の変化に伴い、監視イベント一覧にイベントを表示する。 また、監視マップ上に表示されるノードアイコンの枠の色が稼働状態によって変化する。	分	1分	10分	999分

D.3.2　MIBしきい値監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
ノードのネットワークやシステムの性能異常をMIBごとに監視する。	分	1分	10分	999分

D.3.3　ネットワークの性能異常の監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
トラフィック情報のしきい値超えを監視する。	分	1分	2分	20分 (注)

注)

設定単位は、1分、2分、5分、10分、20分

D.4　監視間隔

被管理サーバ(部門管理サーバ/業務サーバ)の性能監視およびアプリケーションの監視を行う場合、設定された間隔で監視が行われます。

監視間隔の最小、最大、初期値について説明します。。

D.4.1　サーバの性能異常の監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
サーバのCPU使用率、メモリ使用量、ディスク空き容量のしきい値超えを監視する。	秒	60秒	初期設定ON: 60秒 初期設定OFF: 180秒	9,999秒

D.4.2　アプリケーションの稼働状況の監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
プロセスの稼働状態を、監視マップ/監視リストに表示します。	分	1分(注)	5分	23時間59分

注)

0分の指定も可能です。その場合、アプリケーションの稼働状況の監視は行いません。

D.4.3　アプリケーションの性能異常の監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
常駐プロセスが利用するCPU、メモリなどの性能情報のしきい値超えを監視する。	秒	60秒	180秒	9,999秒

D.4.4　アプリケーションの稼働監視間隔

内容	設定単位	制限値		
		最小	初期値	最大
監視マップ上の常駐プロセスが稼働しているか停止しているかを監視する。	分	1分	5分	23時間59分

付録E　構成情報一覧

Systemwalker Centric Managerで管理する構成情報の一覧を以下に示します。構成情報を登録する機能は、イベント通知、ノード検出、インベントリ収集です。

イベント通知およびノード検出方法については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“通信環境を設定する”および“監視するノードを登録する”を参照してください。インベントリ収集方法については、“Systemwalker Centric Manager 使用手引書 資源配付機能編”を参照してください。

[ノードプロパティ]項目

[ノードプロパティ]項目名		イベント通知	ノード検出	インベントリ収集	備考
[基本情報]タブ					
	[表示名]	○ (注3)	○ (注3)	○ (注3)	
	[説明]	×	×	×	
	[クラスタ名]	○	×	×	
	[ベンダー名]	×	△	×	
	[マシン種別一覧]	○	△	○	
[ネットワーク]タブ					
	[ホスト名]	○ (注1)	○	○	
	[コンピュータ名]	×	×	○	
	[Rコミュニティ名]	×	○	×	
	[Wコミュニティ名]	×	○	×	
	[DHCP]	○	○	○	
	[RAS]	○	×	×	
	[INTERNET]	×	×	×	
	[MIB SysDesc]	×	△	×	
	[有効なSNMPエージェントのバージョン]	×	○	×	
[インタフェース]タブ					
	[代表]	○	○	○	
	[業務]	○	○	○	
	[ホスト名]	○ (注1)	○	○ (注4)	
	[IPアドレス]	○ (注2)	○	○ (注4)	IPv6アドレスのリンクローカルアドレスは登録されません。
	[サブネットマスク]	×	○	○ (注4)	
	[インタフェース名]	×	△	○	
	[MACアドレス]	×	△	○	
	[IfType]	×	△	×	
	[IfSpeed]	×	△	×	
	[IfIndex]	×	△	×	

[ノードプロパティ]項目名		イベント通知	ノード検出	インベントリ収集	備考
[OS]タブ					
	[OS種別]	○	△	○	
	[OS詳細情報]	×	△	○	
[監視ポリシー]タブ					
	[ポリシー種別]	×	×	×	
	[ポリシー名]	×	×	×	
	[配付状況]	×	×	×	
[Systemwalker Centric Manager]タブ					
	[Systemwalker Centric Manager がインストールされている]	○	×	○	
	[種別]	○	×	○	
	[サーバオプション]	○	×	○	
[Systemwalker Operation Manager]タブ					
	[Systemwalker Operation Manager がインストールされている]	○	×	○	
	[Systemwalker Operation Manager 運用種別]	○	×	○	
[電源制御]タブ					
	[電源制御装置あり]	×	×	×	
	[電源制御オプション]	×	×	×	
	[オプション]	×	×	×	
[詳細情報]タブ					
	[ノード詳細情報]	○	△	○	
[ビデオ]タブ					
	[ビデオ詳細情報]	×	×	○	
[アイコン]タブ					
	[イメージファイル]	×	×	×	
	[サイズ]	×	×	×	

○:登録する
×:登録なし
△:被監視ノードでSNMPエージェントが動作している場合だけ登録する

注1)

イベント発生元システムにおける、[通信環境定義詳細]-[自ホスト名]の設定内容に従って決まるホスト名

注2)

IPアドレスが複数ある場合、イベント通知により自動設定されるIPアドレスは1つだけです。

注3)

新規追加時のみ(ホスト名)

注4)

新規追加時のみ

付録F　監視できるインストールレス型エージェントのOS

インストールレス型エージェントとして監視可能なOSについて、説明します。

なお、サポート期間が終了した基本ソフトウェアは、本製品のサポート対象外です。

F.1　Windows

注意

インストールレス型エージェント監視を行う場合、被監視システムにおいて以下のコマンドが実行可能である必要があります。

- echo
- wmic
- Eventcreate
- cscript
- wscript
- PowerShell
- VBScript

- Windows(R) 10 Home (注1)
- Windows(R) 10 Pro (注1)
- Windows(R) 10 Enterprise (注1)
- Windows(R) 10 Education (注1)
- Windows(R) 11 Home (注1)
- Windows(R) 11 Pro (注1)
- Windows(R) 11 Enterprise (注1)
- Windows(R) 11 Education (注1)
- Microsoft(R) Windows Server(R) 2016 Datacenter (注1)
- Microsoft(R) Windows Server(R) 2016 Standard (注1)
- Microsoft(R) Windows Server(R) 2016 Essentials (注1)
- Microsoft(R) Windows Server(R) 2019 Datacenter (注1)
- Microsoft(R) Windows Server(R) 2019 Standard (注1)
- Microsoft(R) Windows Server(R) 2019 Essentials (注1)
- Microsoft(R) Windows Server(R) 2022 Datacenter (注1)
- Microsoft(R) Windows Server(R) 2022 Standard (注1)
- Microsoft(R) Windows Server(R) 2022 Essentials (注1)

注1)

WMI接続、SSH接続の場合のみ監視可能です。

F.2 Solaris

注意

インストールレス型エージェント監視を行う場合、被監視システムにおいて以下のコマンドが実行可能である必要があります。

- cd
- tail
- dirname
- date
- awk
- basename
- date
- df
- egrep
- expr
- grep
- kill
- ls
- mpstat
- pagesize
- rm
- sed
- prtconf
- cut
- echo
- head
- printf
- sar
- wc
- nawk
- ps
- touch
- chmod
- mkdir
- iconv
- uname
- mv
- dos2unix

- tr
- cat
- netstat
- mount
- swap
- hostname
- psrinfo
- pkginfo
- ifconfig

- Solaris 10 (SPARC)
- Solaris 11 (SPARC)(注)

  注)

  Solaris 11.4以降では、TELNET接続は利用できません。

F.3 Linux

本製品がサポートしているRed Hat Enterprise Linuxのマイナーバージョンの詳細は、弊社ホームページ「ソフトウェア：富士通（ソフトウェアの一覧表（システム構成図）と各種対応状況)」内の「OSへの対応状況」、または、Systemwalker Centric Managerホームページの「型名/価格/適応機種/適応OSの一覧」から参照できる「OSへの対応状況」でご確認ください。



注意

インストールレス型エージェント監視を行う場合、被監視システムにおいて以下のコマンドが実行可能である必要があります。

- cd
- tail
- dirname
- date
- awk
- basename
- date
- df
- egrep
- expr
- grep
- kill
- ls
- vmstat
- rm
- sed

- free
- cut
- echo
- head
- printf
- sar
- wc
- gawk
- ps axww
- touch
- chmod
- mkdir
- iconv
- uname
- mv
- dos2unix
- tr
- cat
- netstat
- ip
- hostname
- rpm
- ifconfig

- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.10 まで (注1)
- Red Hat Enterprise Linux 9.4 まで (注1)
- SUSE Linux Enterprise Server 15 まで (注1)(注2)
- Oracle Linux 7.9 まで
- Oracle Linux 8.6 まで
- Oracle Linux 9.0 まで

注1)

SSH接続の場合だけ監視可能です。

注2)

シスログのメッセージフォーマットを変更する必要があります。

シスログのメッセージフォーマットの変更方法については、“Systemwalker Centric Manager 導入手引書”の“Systemwalker Centric Managerをインストールしない被監視システム側の設定”を参照してください。

F.4 HP-UX

注意

インストールレス型エージェント監視を行う場合、被監視システムにおいて以下のコマンドが実行可能である必要があります。

- cd
- tail
- dirname
- date
- awk
- basename
- date
- df
- egrep
- expr
- grep
- kill
- ls
- vmstat
- pagesize
- rm
- sed
- dmesg
- cut
- echo
- head
- printf
- crashconf
- wc
- ps
- touch
- chmod
- mkdir
- iconv
- uname
- mv
- dos2ux
- tr

- kctune
- cat
- netstat
- lanscan
- bdf
- mount
- model
- swapinfo
- hostname
- ioscan
- machinfo

HP-UX 11i

F.5 AIX

注意

インストールレス型エージェント監視を行う場合、被監視システムにおいて以下のコマンドが実行可能である必要があります。

- cd
- tail
- dirname
- date
- awk
- basename
- df
- egrep
- expr
- grep
- kill
- ls
- vmstat
- pagesize
- rm
- sed
- svmon
- cut
- echo
- head

- printf
- sar
- wc
- nawk
- ps axww
- touch
- chmod
- mkdir
- iconv
- uname
- mv
- tr
- cat
- netstat
- mount
- oslevel
- lsps
- hostname
- lsdev
- prtconf
- ifconfig

AIX 7.2

付録G　本書の表記、登録商標について

G.1　本書の表記について

固有記事の表記について

エディションによる固有記事

Systemwalker Centric Managerのマニュアルでは、標準仕様である“Systemwalker Centric Manager 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、または本文に付けています。

EE:

“Systemwalker Centric Manager Enterprise Edition”の固有記事

GEE:

“Systemwalker Centric Manager Global Enterprise Edition”の固有記事

EE/GEE:

“Systemwalker Centric Manager Enterprise Edition”、および“Systemwalker Centric Manager Global Enterprise Edition”の固有記事

固有記事の範囲は、タイトル、または本文に付いた場合で以下のように異なります。

タイトルに付いている場合

章/節/項などのタイトルに付いている場合、タイトルの説明部分全体が、固有記事であることを示します。この場合、タイトルに対して、オンラインマニュアルの場合は色付けされます。

本文に付いている場合

固有記事全体に対して、オンラインマニュアルの場合は色付けされます。

Windows版とUNIX版の固有記事

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付けて共通の記事と区別しています。

本文中でWindows版とUNIX版の記載が分かれる場合は、“Windows版の場合は～”、“UNIX版の場合は～”のように場合分けして説明しています。

タイトル【Windows版】

タイトル、小見出しの説明部分全体が、Windows版固有の記事です。

タイトル【UNIX版】

タイトル、小見出しの説明部分全体が、UNIX版固有の記事です。

記号について

画面項目名、およびコマンドで使用する記号について説明します。

[ ]記号

Systemwalker Centric Managerで提供している画面名、メニュー名、および画面項目名をこの記号で囲んでいます。

コマンドで使用する記号

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。

略語表記について

本書では、以下の略称を使用しています。

オペレーティングシステム

正式名称	略称
Microsoft(R) Windows Server(R) 2022 Datacenter Microsoft(R) Windows Server(R) 2022 Standard	Windows Server 2022 Windows Server(R) 2022 Windows Server® 2022
Microsoft(R) Windows Server(R) 2019 Datacenter Microsoft(R) Windows Server(R) 2019 Standard	Windows Server 2019 Windows Server(R) 2019 Windows Server® 2019
Microsoft(R) Windows Server(R) 2016 Datacenter Microsoft(R) Windows Server(R) 2016 Standard	Windows Server 2016 Windows Server(R) 2016 Windows Server® 2016
Nano ServerインストールしたWindows Server 2016	Nano Server
Microsoft(R) Windows Server(R) 2012 R2 Foundation (x64) Microsoft(R) Windows Server(R) 2012 R2 Standard (x64) Microsoft(R) Windows Server(R) 2012 R2 Datacenter (x64) Microsoft(R) Windows Server(R) 2012 Foundation (x64) Microsoft(R) Windows Server(R) 2012 Standard (x64) Microsoft(R) Windows Server(R) 2012 Datacenter (x64)	Windows Server 2012 Windows Server(R) 2012 Windows Server® 2012
Microsoft(R) Windows Server(R) 2012 R2 Foundation (x64) Microsoft(R) Windows Server(R) 2012 R2 Standard (x64) Microsoft(R) Windows Server(R) 2012 R2 Datacenter (x64)	Windows Server 2012 R2 Windows Server(R) 2012 R2 Windows Server® 2012 R2
Microsoft(R) Windows Server(R) 2008 Datacenter Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM)	Windows Server 2008 DTC Windows Server(R) 2008 DTC Windows Server® 2008 DTC
Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2 DTC Windows Server(R) 2008 R2 DTC Windows Server® 2008 R2 DTC
Microsoft(R) Windows Server(R) 2008 Enterprise	Windows Server 2008 EE

正式名称	略称
Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM)	Windows Server(R) 2008 EE Windows Server® 2008 EE
Microsoft(R) Windows Server(R) 2008 R2 Enterprise	Windows Server 2008 R2 EE Windows Server(R) 2008 R2 EE Windows Server® 2008 R2 EE
Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM)	Windows Server 2008 STD Windows Server(R) 2008 STD Windows Server® 2008 STD
Microsoft(R) Windows Server(R) 2008 R2 Standard	Windows Server 2008 R2 STD Windows Server(R) 2008 R2 STD Windows Server® 2008 R2 STD
Microsoft(R) Windows Server(R) 2008 Foundation	Windows Server 2008 Foundation Windows Server(R) 2008 Foundation Windows Server® 2008 Foundation
Microsoft(R) Windows Server(R) 2008 R2 Foundation	Windows Server 2008 R2 Foundation Windows Server(R) 2008 R2 Foundation Windows Server® 2008 R2 Foundation
Server Coreインストールした以下のOS Microsoft(R) Windows Server(R) 2008 Standard Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Enterprise Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V(TM) Microsoft(R) Windows Server(R) 2008 Datacenter Microsoft(R) Windows Server(R) 2008 Datacenter without Hyper-V(TM)	Windows Server 2008 Server Core Windows Server(R) 2008 Server Core Windows Server® 2008 Server Core
Microsoft(R) Windows Server(R) 2008 R2 Foundation Microsoft(R) Windows Server(R) 2008 R2 Standard Microsoft(R) Windows Server(R) 2008 R2 Enterprise Microsoft(R) Windows Server(R) 2008 R2 Datacenter	Windows Server 2008 R2 Windows Server(R) 2008 R2 Windows Server® 2008 R2
Microsoft® Windows Server® 2008 for Itanium-Based Systems	Windows Server 2008 for Itanium-Based Systems
Microsoft® Windows Server® 2008 Foundation Microsoft® Windows Server® 2008 Standard Microsoft® Windows Server® 2008 Enterprise Microsoft® Windows Server® 2008 Datacenter Microsoft® Windows Server® 2008 Standard without Hyper-V(TM) Microsoft® Windows Server® 2008 Enterprise without Hyper-V(TM)	Windows Server 2008 Windows Server(R) 2008 Windows Server® 2008

正式名称	略称
Microsoft® Windows Server® 2008 Datacenter without Hyper-V(TM) Microsoft® Windows Server® 2008 R2 Foundation Microsoft® Windows Server® 2008 R2 Standard Microsoft® Windows Server® 2008 R2 Enterprise Microsoft® Windows Server® 2008 R2 Datacenter	
Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems Microsoft(R) Windows Server(R) 2003, Datacenter Edition	Windows Server 2003 DTC Windows Server(R) 2003 DTC Windows Server® 2003 DTC
Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition	Windows Server 2003 DTC (x64) Windows Server(R) 2003 DTC (x64) Windows Server® 2003 DTC (x64)
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems Microsoft(R) Windows Server(R) 2003, Enterprise Edition	Windows Server 2003 EE Windows Server(R) 2003 EE Windows Server® 2003 EE
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition	Windows Server 2003 EE (x64) Windows Server(R) 2003 EE (x64) Windows Server® 2003 EE (x64)
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Standard Edition	Windows Server 2003 STD Windows Server(R) 2003 STD Windows Server® 2003 STD
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition	Windows Server 2003 STD (x64) Windows Server(R) 2003 STD (x64) Windows Server® 2003 STD (x64)
Microsoft(R) Windows Server(R) 2003, Standard Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition	Windows Server 2003 Windows Server(R) 2003

正式名称	略称
Microsoft(R) Windows Server(R) 2003, Datacenter Edition Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition Microsoft(R) Windows Server(R) 2003 R2, Datacenter Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise Edition for Itanium-based Systems Microsoft(R) Windows Server(R) 2003, Datacenter Edition for Itanium-based Systems	Windows Server® 2003
Microsoft(R) Windows Server(R) 2003, Standard x64 Edition Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003, Datacenter x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition Microsoft(R) Windows Server(R) 2003 R2, Datacenter x64 Edition	Windows Server 2003 x64 Editions Windows Server(R) 2003 x64 Editions Windows Server® 2003 x64 Editions
Microsoft(R) Windows(R) 2000 Professional Microsoft(R) Windows(R) 2000 Server Microsoft(R) Windows(R) 2000 Advanced Server Microsoft(R) Windows(R) 2000 Datacenter Server	Windows 2000 Windows(R) 2000 Windows® 2000
Windows(R) 11 Home Windows(R) 11 Pro Windows(R) 11 Enterprise Windows(R) 11 Education	Windows 11 Windows(R) 11
Windows(R) 10 Home Windows(R) 10 Pro	Windows 10 Windows(R) 10

正式名称	略称
Windows(R) 10 Enterprise Windows(R) 10 Education	
Windows(R) 8.1 (x86) Windows(R) 8.1 Pro (x86) Windows(R) 8.1 Enterprise (x86) Windows(R) 8.1 (x64) Windows(R) 8.1 Pro (x64) Windows(R) 8.1 Enterprise (x64) Windows(R) 8 (x86) Windows(R) 8 Pro (x86) Windows(R) 8 Enterprise (x86) Windows(R) 8 (x64) Windows(R) 8 Pro (x64) Windows(R) 8 Enterprise (x64)	Windows 8 Windows(R) 8 Windows® 8
Windows(R) 8.1 (x86) Windows(R) 8.1 Pro (x86) Windows(R) 8.1 Enterprise (x86) Windows(R) 8.1 (x64) Windows(R) 8.1 Pro (x64) Windows(R) 8.1 Enterprise (x64)	Windows 8.1 Windows(R) 8.1 Windows® 8.1
Windows(R) 7 Home Premium Windows(R) 7 Professional Windows(R) 7 Enterprise Windows(R) 7 Ultimate	Windows 7 Windows(R) 7 Windows® 7
Windows Vista(R) Home Basic Windows Vista(R) Home Premium Windows Vista(R) Business Windows Vista(R) Enterprise Windows Vista(R) Ultimate	Windows Vista Windows Vista(R) Windows Vista®
Microsoft(R) Windows(R) XP Professional x64 Edition Microsoft(R) Windows(R) XP Professional Microsoft(R) Windows(R) XP Home Edition	Windows XP Windows(R) XP Windows® XP
Microsoft(R) Windows NT(R) Server network operating system Version 4.0 Microsoft(R) Windows NT(R) Workstation operating system Version 4.0 Microsoft(R) Windows NT(R) Server network operating system Version 3.51 Microsoft(R) Windows NT(R) Workstation operating system Version 3.51	Windows NT Windows NT(R) Windows NT®

正式名称	略称
Microsoft(R) Windows NT(R) Server network operating system Version 4.0 Microsoft(R) Windows NT(R) Server network operating system Version 3.51	Windows NT(R) Server
Microsoft(R) Windows NT(R) Workstation operating system Version 4.0 Microsoft(R) Windows NT(R) Workstation operating system Version 3.51	Windows NT(R) Workstation
Microsoft(R) Windows NT(R) Server network operating system Version 4.0 Microsoft(R) Windows NT(R) Workstation operating system Version 4.0	Windows NT 4.0 Windows NT(R) 4.0 Windows NT® 4.0
Microsoft(R) Windows(R) 95 operating system、 Microsoft(R) Windows(R) 95 Second Edition	Windows 95 Windows(R) 95 Windows® 95
Microsoft(R) Windows(R) 98 operating system、 Microsoft(R) Windows(R) 98 Second Edition	Windows 98 Windows(R) 98 Windows® 98
Microsoft(R) Windows(R) Millennium Edition	Windows Me Windows(R) Me Windows® Me
上記のオペレーティングシステムすべて	Windows Windows(R) Windows®
Microsoft(R) Azure(R)	Windows Azure Windows Azure(R) Windows Azure®
Solaris 11 Solaris 10 Solaris 9	Solaris(注)
Red Hat Enterprise Linux 9 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 5	Linux
Red Hat Enterprise Linux 9 (for Intel64) Red Hat Enterprise Linux 8 (for Intel64) Red Hat Enterprise Linux 7 (for Intel64) Red Hat Enterprise Linux 6 (for Intel64) Red Hat Enterprise Linux 5 (for Intel64)	Linux for Intel64
Red Hat Enterprise Linux 6 (for x86)	Linux for x86

正式名称	略称
Red Hat Enterprise Linux 5 (for x86)	
Itaniumに対応したWindows	Windows for Itanium
Itaniumに対応したLinux	Linux for Itanium

注)
Oracle SolarisはSolaris、Solaris Operating System、Solaris OSと記載することがあります。

その他の製品

製品名称	略称
Microsoft(R) SQL Server(TM)	SQL Server
Microsoft(R) Visual C++	Visual C++
Microsoft(R) Internet Explorer	Internet Explorer

Systemwalker Centric Managerの表記

Systemwalker Centric Manager	略称
Windows上で動作するSystemwalker Centric Manager	Windows版
32bit版のWindows上で動作するSystemwalker Centric Manager	Windows(32bit)版
64bit版のWindows上で動作するSystemwalker Centric Manager	Windows(64bit)版
Solaris上で動作するSystemwalker Centric Manager	Solaris版
Linux上で動作するSystemwalker Centric Manager	Linux版
Linux for Intel64上で動作するSystemwalker Centric Manager	Linux for Intel64版
Linux for x86上で動作するSystemwalker Centric Manager	Linux for x86版
HP-UXで動作するSystemwalker Centric Manager V13.2.0	HP-UX版
AIXで動作するSystemwalker Centric Manager V13.2.0	AIX版
Itaniumに対応したLinux上で動作するSystemwalker Centric Manager	Linux for Itanium版
Itaniumに対応したWindows上で動作するSystemwalker Centric Manager	Windows for Itanium版

G.2　登録商標について

Amazon Web Services、その他のAWS商標は、Amazon.com, Inc.またはその関連会社の商標です。

Apache、Tomcatは、Apache Software Foundationの商標または登録商標です。

APC、PowerChuteは、シュナイダー・エレクトリック・アイティー・コーポレーションの登録商標です。

Arcserveのすべての製品名、サービス名、会社名およびロゴは、Arcserve (USA), LLC.またはその子会社の登録商標または商標です。

Ethernetは、富士フイルムビジネスイノベーション株式会社の登録商標です。

HP-UXは、米国およびその他の国におけるHewlett-Packard Companyの登録商標です。

IBM、IBMロゴ、AIX、AIX 5L、HACMP、Power、PowerHAは、世界の多くの国で登録された International Business Machines Corporationの商標です。

Intel、Itaniumは、アメリカ合衆国および / またはその他の国における Intel Corporation またはその子会社の商標です。

InterScan、ウイルスバスターは、トレンドマイクロ株式会社の登録商標です。

JP1は、(株)日立製作所の日本における商品名称(商標または登録商標)です。

LANDeskは、米国およびその他の国におけるIvanti Software, Inc.およびその関係会社の商標または登録商標です。

Laplinkは、米国Laplink Software, Inc.の米国およびその他の国における登録商標または商標です。

Linux(R)は米国およびその他の国におけるLinus Torvaldsの登録商標です。

MC/ServiceGuardは、米国Hewlett Packard Enterprise Development LPの米国およびその他の国における登録商標です。

Microsoft、Windows、Windows NT、Windows Vista、Windows Server、Azureまたはその他のマイクロソフト製品の名称および製品名は、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。

Mozilla、Firefoxは、米国Mozilla Foundation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。

NEC、WinShareは、日本電気株式会社の商標または登録商標です。

Norton AntiVirusは、ノートンLifeLockまたは関連会社の米国およびその他の国における商標または登録商標およびサービスマークです。

Oracle(R)、Java、およびOracle Cloudは、オラクルおよびその関連会社の登録商標です。

SAPおよびSAPのロゴ、その他のSAPの製品およびサービスは、ドイツおよびその他の国におけるSAP SE(またはその関連会社)の商標または登録商標です。

Red HatおよびRPMは、米国およびその他の国におけるRed Hat, Inc.およびその子会社の商標または登録商標です。

ServiceNow、ServiceNow のロゴ、Now、その他の ServiceNow マークは、米国および/またはその他の国における ServiceNow, Inc. の商標または登録商標です。

UNIXはX/Open Company, Ltd.の登録商標です。

UXP、Systemwalker、Interstage、Symfowareは、富士通株式会社の登録商標です。

Veritasは、米国およびその他の国における Veritas Technologies LLC またはその関連会社の登録商標です。

VirusScanおよびNetShieldは、米国法人 McAfee, LLC または米国またはその他の国の関係会社における登録商標または商標です。

VMwareおよびVMwareの製品名は、Broadcom Inc.の米国および各国での商標または登録商標です

Zabbixはラトビア共和国にあるZabbix LLCの商標です。

ショートメール、iモードは、株式会社NTTドコモの登録商標です。

そのほか、本マニュアルに記載されている会社名および製品名は、それぞれ各社の商標または登録商標です。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。