

Fujitsu Software

システムウォーカー セントリックマネージャー

Systemwalker

Centric Manager

V17.0 データシート (機能紹介資料)



システムの導入／監視／トラブル復旧／評価
を支援する統合管理

FUJITSU

安定稼働 わかりやすい監視と復旧支援

監視（モニタリング）

● 稼働状態の表示

サーバ、ルータなどのノードに対して、稼働/停止の状態を監視画面に表示します。稼働/停止の状態は、一定間隔ごと、または任意のタイミングでpingによるポーリングで監視します。また、SNMPによるインターフェース情報のMIB収集による監視も行い、Systemwalkerコンソールの監視マップに配置されているノードアイコンの枠に色で表示します。これにより、一目でノードの状態が確認できます。

なお、ノード状態に変化があった場合は、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。

MIB : Management information base (管理情報ベース)

・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定期的なポーリング間隔

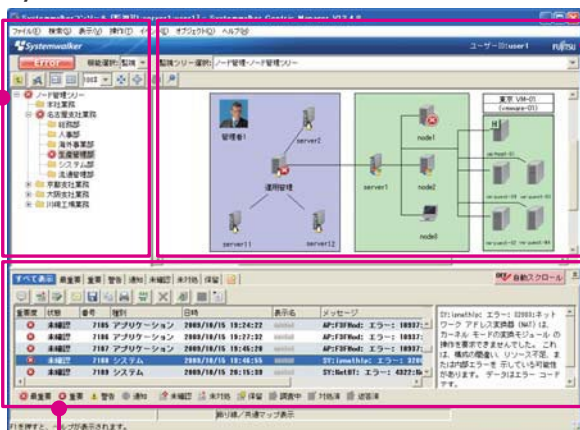
ポーリング間隔	最小	初期値	最大
稼働状態の監視間隔	1分	10分	999分
MIBしきい値監視間隔	1分	10分	999分
ネットワーク性能異常の監視間隔	1分	2分	20分(注)

(注)設定単位は、1分、2分、5分、10分、20分

● Systemwalker Webコンソールによる監視

イントラネット外からもWebコンソールを利用して、監視イベントの通知を電子メールで受信したり、出張先でイベントの一覧を参照できます。

Systemwalkerコンソール[監視]画面



ツリー情報

■ ノード一覧ツリー

運用形態にあわせた階層で、ノードを管理します。ノード一覧ツリーはインストール時に自動的に作成され、ノード一覧ツリーを含めて3階層まで管理可能です。

■ ノード管理ツリー

目的にあった配置/監視を行いたい場合に使用します。

サブドメイン、サブネットにとらわれない監視が可能です。例えば、...

- ある特定のノードを監視
- ネットワーク機器を監視
- 監視対象ノードのみを監視
- サーバのみを監視 等

■ 業務管理ツリー

アプリケーション、データベース、管理者、ワークユニット、パッケージを同時に監視が可能です。例えば、...

ある特定のノードおよびノード上で動作するアプリケーションを一括して監視

監視イベント一覧

発生した監視イベントが一覧で表示されます。最重要/重要/警告などの重要度によって監視コンソールに色分け表示が可能です。監視イベント一覧への表示は、表示する監視イベント数を定義することで、1000から最大 5000件まで拡張できます。

注意!

■ 重要度レベルについて

メッセージに対して設定される属性です。メッセージの重要度に応じて、利用者が設定します。重要度レベルには、以下の5種類があります。

- 最重要 (HALTレベルのメッセージ)
- 重要 (ERRORレベル/エラー種別なしのメッセージ)
- 警告 (WARNINGレベルのメッセージ)
- 通知 (NOTICEレベルのメッセージ)
- 一般 (INFOレベルのメッセージ)

※重要度が[一般]であるメッセージは、監視イベント一覧に表示されません。

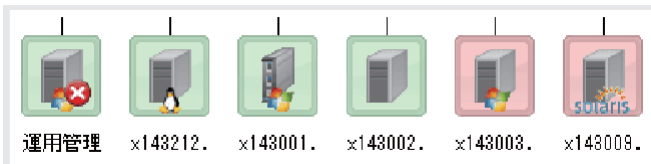
● 稼働状態の監視

ファイルサーバやルータなど、特に重要な監視対象として設定したノードの場合は、ポーリング、および任意のタイミングで監視し、停止状態への移行または起動状態への移行をトラップとして通知します。ノード状態に変化があった場合は、それぞれ以下のようなメッセージが監視イベント一覧に出力されます。

ノードが停止状態に遷移した場合「ノードとの通信が不可となりました。」
ノードが起動状態に遷移した場合「ノードとの通信が可能となりました。」

*ノード状態の監視は、SNMPエージェントが搭載されていないノードに対しても可能です。

ノードアイコン



表示色 : ノードの状態

緑色:ノードが起動状態、かつ、SNMPエージェント動作中

緑色:ノードが起動状態、かつ、SNMPエージェント動作中、かつ、一部インターフェースが停止中

緑色:ノードが起動状態、かつ、SNMPエージェント未起動

赤色: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)

● Systemwalkerコンソールで統合的な監視

Windowsや各種UNIX、Linux、メインフレームなど、マルチプラットフォーム環境の統合運用管理が可能です。各サーバやルータ、アプリケーションなどの稼働状態や異常メッセージが全て統合監視画面で確認でき、詳細状況の確認やトラブル対応など、一連の運用管理作業も統合監視画面から操作できます。また、Microsoft Azure、FUJITSU Hybrid IT Service for Microsoft Azure^{*1}などの環境も、統合的な監視が可能です。これにより、オンプレミス(Windows/Linux/UNIX)もパブリック・クラウドも一つのSystemwalkerコンソールで監視でき、安定稼働とコスト削減を実現します(ハイブリッド・クラウドの統合監視)。

*1:富士通が提供するクラウドサービス

監視マップ/リスト

監視ツリーで選択している配下の情報(ツリー配下のフォルダ、ノード)を表示します。監視マップ/リストは、フォルダ(ルートフォルダを除く)やノードをマップ形式、またはリスト形式で表示します。

仮想マシンも併せて監視

Hyper-V、VMwareを導入したVM環境を監視する場合、監視コンソール上に仮想マシンの監視マップを作成することで、ゲストOS/ホストOSの関係を確認できます。また、ハード障害(ホストOS障害)発生時の影響範囲も把握できます。

これは便利!

監視画面から、直接ほかのアプリケーションを起動したり、ネットワーク機器の管理ツールなどの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応が可能です。

【連携可能な主な他社製品】

- Oracle E-Business Suite (Oracle)
- SAP (SAP)
- EPICenter (ExtremeNetworks)

さらに、こんなこともできます…

メッセージ説明を登録して監視

データセンター等の運用では、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] に登録しておくことで、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応が可能となります。メッセージ説明を登録して監視するには、「共通のメッセージ説明を登録して監視」と「監視ツリーのフォルダごとにメッセージ説明を変更して監視」の2つの形態があります。

ハイブリッドクラウド環境の監視

● オンプレミスとパブリッククラウドが混在するハイブリッドクラウド環境を統合監視

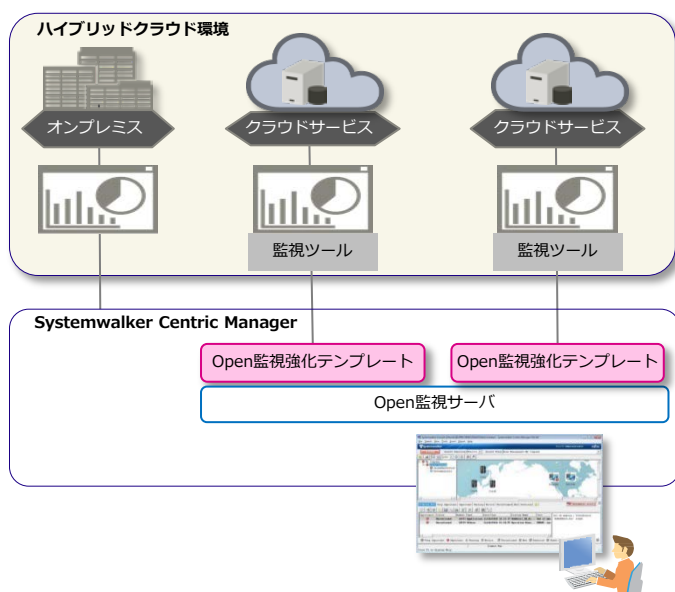
オンプレミスからクラウドサービスまですべてのシステムのイベント発生状況、監視設定を1つの画面で監視できます。

● クラウドサービスの監視

Open監視強化テンプレートを利用することにより、クラウドサービスを監視できます。

トラブル発生状況、対処状況、監視設定などを一目で把握できるため、迅速な状況把握と対処指示を行うことができます。

また、複数のクラウドサービスを1つの画面で監視できるようになるため、クラウドサービスの監視ツール固有の運用手順書の作成・メンテナンス負荷を削減できます。



■ メトリクス/メトリック監視

クラウド上のリソースのメトリクス/メトリックを監視します。

■ ログ監視

クラウド上のリソースのログを監視します。

■ オートスケール監視

新しいインスタンスが生成されると自動的に監視を開始し、インスタンスが削除されると監視を終了します。

Open監視強化テンプレート

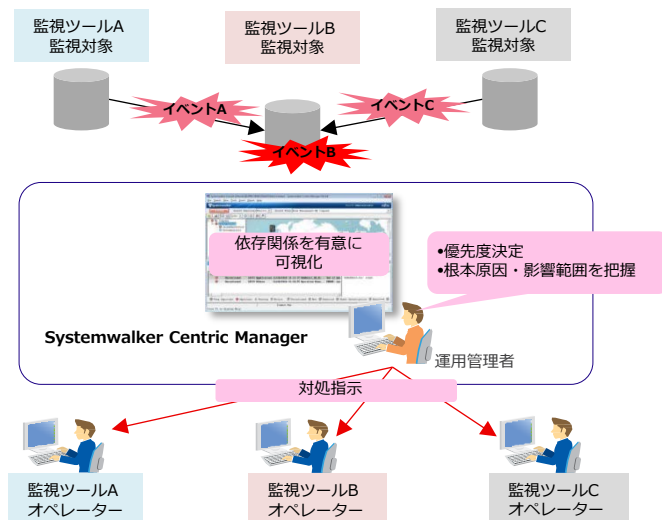
Open監視強化テンプレートの最新版はソフトウェア技術情報（P.14）で随時公開されます。

監視対象	Open監視強化テンプレート
Amazon Web Services	AWSメトリクス監視テンプレート
	AWSログ監視テンプレート
	AWSオートスケール監視テンプレート
Microsoft Azure	Azureメトリック監視テンプレート
	Azureログ監視テンプレート
	Azureオートスケール監視テンプレート
Oracle Cloud Infrastructure	OCIメトリック監視テンプレート
	OCIログ監視テンプレート

● トラブル発生時の認知迅速化・判断支援 **これは便利！**

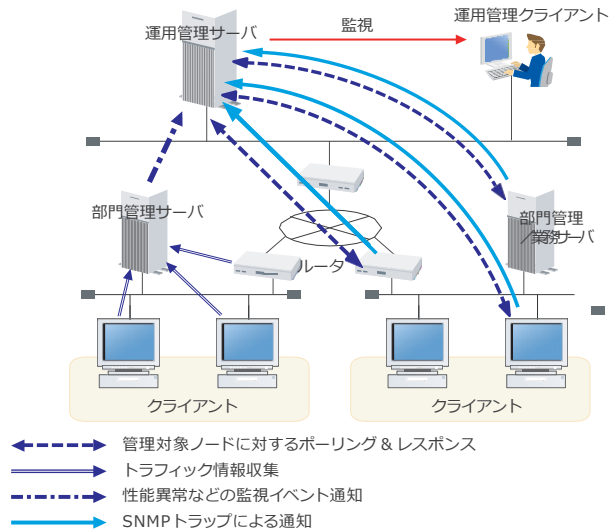
監視対象間の依存関係が監視画面上で有意に可視化されるため、根本原因や影響範囲を把握できます。

また、同時発生したイベントと関連情報を監視画面上で確認できるため、運用管理者がトラブル対処の優先度を決定することができます。



● ネットワーク/システム監視の運用イメージ

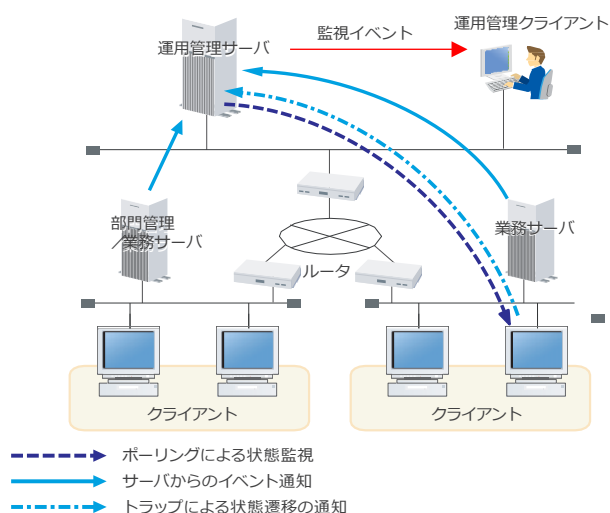
ネットワーク監視の概要



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できます。SNMP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。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^{*1}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も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することもできます。

*1: SNMPv1、SNMPv2C、SNMPv3に対応

システム監視の概要



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。遠隔地のサーバの電源が投入されているかを確認したり、管理者のいないサーバで発生するイベントをセンターで集中監視し、特定のサーバで問題が発生していないか監視します。

・メール連携機能でファイアーウォール越えのシステム監視

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(メール連携機能)することができます。これによりファイアー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どちらのシステムにも、Systemwalker Centric Managerが必要です。

● ネットワーク機器とシステムの障害の監視 解説

・トラップの監視

ノードからSNMP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]で管理します。

・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。この、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。

拡張MIB：

メーカーが自社のハードウェアに対し独自に作成したMIBで、標準MIBではカバーしきれない、細かな管理情報を扱うことができます。この拡張MIBを追加登録することでSystemwalkerで扱うことができます。なお、拡張MIB情報の入手については、各メーカーに問い合わせください。

・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、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	イベントログ
	Systemwalker Centric Managerの各機能が監視するイベント	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	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	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
UNIX/Linux	SNMPトラップ	—
	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	シスログ
	Systemwalker Centric Managerの各機能が監視するイベント	シスログ
	Systemwalker Centric Manager以外の連携製品が監視するイベント	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	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：

ネットワーク機器で障害や状態変化などのイベントがあった場合、SNMPエージェントがそのイベントをマネージャーに伝えるために利用されます。ネットワーク機器でイベントが生じた場合、エージェントはあらかじめ指定されたマネージャーに対し、それを通知するイベント通知メッセージを送信します。マネージャーは、イベント通知メッセージを受け取ることによって、いつ、どんな障害が発生したかを知ることができます。

● ノードの変更監視

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、ノードの削除を監視します。また、許可されていないノードや、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されていないか監視します。

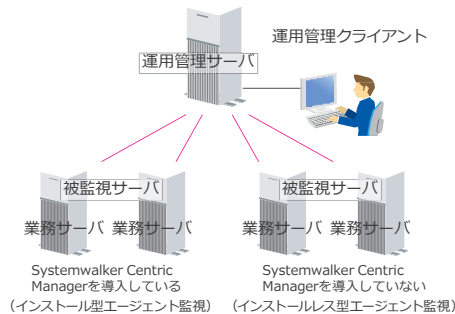
● マルチテナント監視

プライベートクラウド環境では、テナントごとに個別の運用/監視が必要となる場合があります。Systemwalker Centric Managerでは、テナント(業務システム)にあわせて自由に監視設定・監視業務ができる新たな監視機能を提供しています。(Open監視機能)

このOpen監視機能は、「簡単に導入」できるだけでなく、被監視(エージェント)側からの要求だけで監視が開始でき、例えば、仮想プロビジョニングしたシステムを管理サーバ側で設定することなく、監視業務が開始できます。

● 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

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には、以下の2つの方式があります。

非デプロイ方式	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
デプロイ方式	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 非デプロイ方式よりも幅広い機能を利用可能

※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の機能差 P.7

● アプリケーションの稼働監視

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アイコンの枠の色で通知します。

背景画像の色	アプリケーションの状態
緑色	アプリケーションが稼働中
	アプリケーションが起動遷移中
黄色	アプリケーションが稼働中(プロセス数不足)
	アプリケーションが稼働中(プロセス数超過)
赤色	アプリケーションが停止状態
	アプリケーションが停止遷移中
なし	アプリケーションが非監視状態

【監視対象のアプリケーション】

- ・UNIX : 実行形式のファイルおよびシェルスクリプト
- ・Windows : 拡張子が“.exe”のファイル
- ・ワークユニット

Interstageで構築した業務アプリケーションをワークユニットと呼びます。

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。

詳細は、Systemwalker 技術情報ホームページ内マニュアル「Systemwalker Centric Manager Interstage Application Server運用管理ガイド」を参照してください。 P.14

一言メモ

ユーザー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。

● 重要なアプリケーションの稼働監視

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、イベントとして異常を知らせます。

例えば...

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場合や、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場合などにイベントとして通知します。

なお、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や、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、自動的に停止することも可能です。

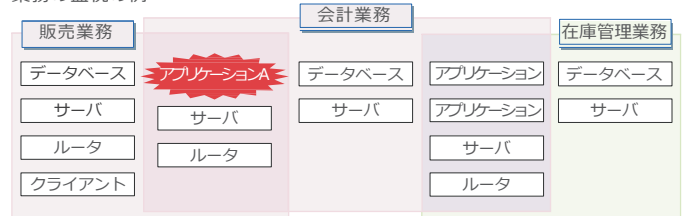
● 業務の監視 これは便利！

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する必要があります。

Systemwalker Centric Managerでは、業務を構成するオブジェクト^{*1}を業務単位で監視します。この監視形態により、業務を構成するオブジェクトのどれか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ので、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です。

- ^{*1} オブジェクト：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
業務：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。
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
 - ・管理者
 - ・ワークユニット(Interstage上で作成された業務) など

業務の監視の例



障害の影響を受ける業務の把握

"アプリケーションA" にトラブルが発生

- 「販売業務」と「会計業務」に影響があることが瞬時に分かる
- 業務担当者へ連絡
- 必要に応じて業務を閉塞

● 管理者の行動パターンに併せた通知

検知された異常メッセージは、さまざまな方法で管理者に通知できます。重要なトラブルは音声(男性、または女性)^{*2}やパトライト^{*3}で通知したり、夜間発生したトラブルはメールで担当者に通知するなど、メッセージの内容や管理者の行動パターンにあわせて、通知方法を複数組み合わせることが可能です。

^{*2} 音声通知(運用管理クライアント、またはクライアントへの通知)：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。

WAVEオーディオカード必須

(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。)

^{*3} パトライト：

イベントが発生した場合、Systemwalker Centric Manager が、RSH (リモートシェル) コマンドを用いて表示灯(株式会社パトライト社製)を点灯させることにより、異常発生を光と音で管理者に知らせます。

● 性能の監視で性能トラブルの未然防止

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。

・ネットワーク性能監視／サーバ性能監視

ネットワーク性能監視は、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。また、サーバ性能監視は、監視する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、異常が発生した場合にイベントとして通知します。

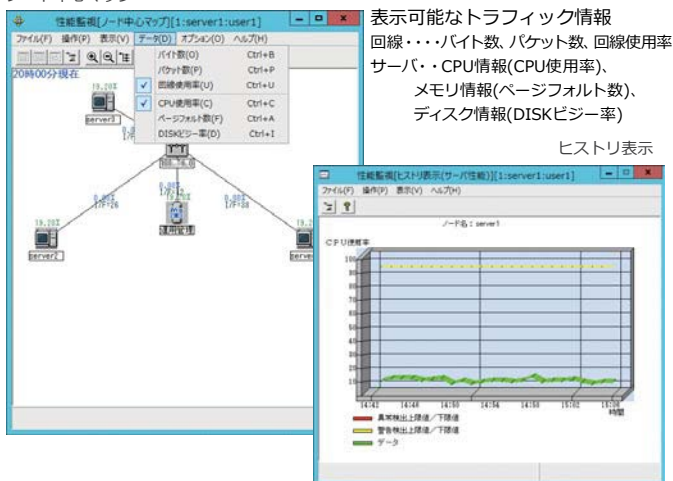
項目	ネットワーク性能監視機能	サーバ性能監視機能
監視方式	運用管理サーバまたは部門管理サーバからのポーリング監視	被監視ノード上での自律監視
監視情報	・ネットワーク機器(SNMPのMIB II サポートノード)、RMONなどから採取したトラフィック情報 ・サーバ性能情報(基本情報)	サーバ性能情報
監視方法	・固定のしきい値による監視(サービレベル監視) ・過去の統計情報との比較による監視(ベースライン監視)	固定のしきい値による監視
しきい値	管理システム全体に一つのしきい値を設定	被監視ノード単位にしきい値を設定
情報蓄積	ポーリング結果をロギングし、ロギング結果は統計レポートとして出力可能	なし

RMON(Remote network MONitoring)

・ノード中心マップ

選択したノードを中心にして、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、接続関係を示すと同時にノード間のトラフィック情報や、ノードのサーバ性能情報を表示します。本マップにより、特定のノードが、他のノードのサービスにどのような影響を与えているかを把握できます。

ノード中心マップ



・アプリケーションの性能監視

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。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。

なお、プロセスのCPU使用率や確保している仮想メモリ容量に、しきい値を設定して監視し、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。

表示する性能値

起動経過時刻・・・プロセスが起動してから経過時刻
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

性能情報のグラフ表示

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

※アプリケーション性能の傾向把握・分析には、収集した情報をSystemwalker Service Quality Coordinatorに取り込むことで行えます。

障害復旧(リカバリ)

● 自動アクションによる自動対処

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。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。

- ・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
- ・e-mail送信で任意の文章を通知
- ・ポップアップメッセージで任意のメッセージを通知
- ・SNMPトラップを発行・送信
- ・アプリケーションの起動
- ・リモートコマンドの発行
- ・イベントログ(アプリケーション)に出力

※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。

注) 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、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。

● 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。

より高度な監視を実現するために...

■ インテリジェントサービス機能 P.14

インテリジェントサービスは、さまざまなサンプルスクリプトを提供します。

・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など、他のシステムの監視を阻害することもあります。このような問題を解決するために、わかりやすいメッセージに変換したり、複数のイベントを集約して通知したり、一時的に監視を抑止することが可能です。

Systemwalker Centric Managerに添付されているEvent Designerツールを使用してイベント監視の条件定義を変更することで実現できます。

こんな時に利用...

ケース 1:

5分以内にwarningメッセージが3回以上発生したら異常と判断し、新規メッセージで異常を通知する。

ケース 2:

受付プロセス、処理プロセス、結果通知プロセス、印刷処理プロセスを監視し、どれかのプロセスが異常停止したら、自動的に全プロセスを停止し再起動させる。上記、全プロセスの起動メッセージを確認し、異常発生から再起動まで5分以内であれば対処済、5分以上であれば対処済にしない表示とする。

・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ができます。これにより、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。

資源の配付

● リモート操作*1

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、管理者が自席からの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。

なお、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。

*1: 本機能は、Systemwalker Live Helpとしても提供しています。

● ファイルの送受信と操作

Windows のエクスプローラと同様の操作で、遠隔地のパソコンのファイル送受信や、ファイルシステム構成の確認、フォルダの作成、ファイル／フォルダの削除、ファイル／フォルダの名前変更ができます。管理者のパソコンにあるマスターファイルやフォルダとの比較も可能です。

● クライアントのセキュリティと操作の記録

クライアント側では、様々なセキュリティ機能を提供します。

● パスワードによる認証

クライアントがパスワードを設定した場合、エキスパートは接続にあたってパスワードを入力する必要があります。

● 接続の承認処理

エキスパートが接続しようとしたとき、クライアントにエキスパートの名前が表示されます。クライアントはこれをみて、承認することも拒否することもできます。

● 接続制限リスト

エキスパートやクライアントがセッションに参加しようとするコンピュータをIPアドレスまたはホスト名によって制限することができます。

● 接続の強制切断

クライアントが何らかの理由でセッションを中止したい場合は、エキスパートの支援を受けているときでも、セッションを終了することができます。

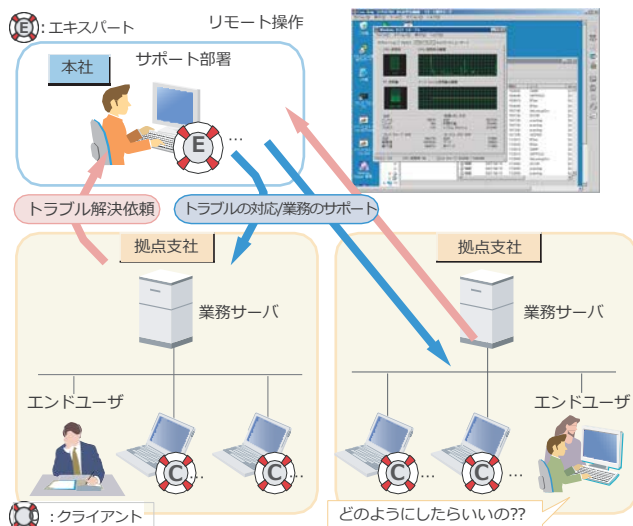
● ファイル操作の承認

エキスパートがクライアントのファイルシステムを操作しているとき、クライアントが操作内容を確認し、承認または拒否することができます。

● セッションの録画・再生

クライアントとのセッション内容を保存することができます。保存したセッションデータで、操作を再生することができ、セッション終了後に操作内容を確認したり、オフラインで操作内容を分析したりすることができます。

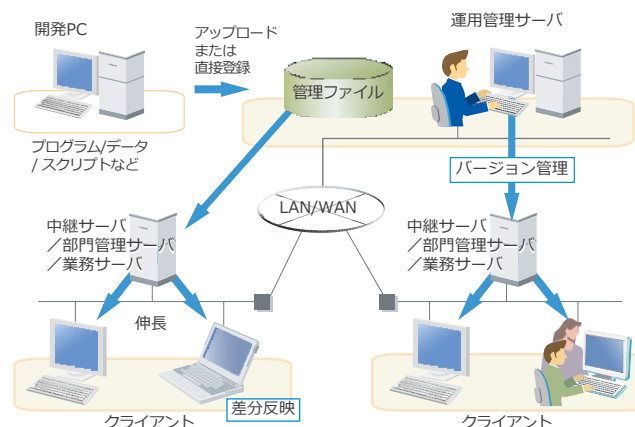
※リモート操作による復旧操作は、Windowsのサーバとクライアントが対象です。
Solaris / Linux については、Telnetを呼び出してリモート操作することが可能です。



● アプリケーションの修正変更を資源配付で自動化

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、運用管理サーバで一元管理し、対象のサーバやクライアントに配付できます。配付する資源は、使用目的にあわせて、資源の配付先と配付方法を選択できます。また、複数の配付資源を業務などの単位にまとめて、配付することもできます。

この単位を世代管理された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、配付ミスの防止と配付負荷の削減が可能です。



● 配付方法の選択

一斉配付	全社共通で使用する基幹業務の資源などを、一度の配付作業で、システム全体に一斉に配付したり、部門単位や事業所内単位で使用する業務の資源を、業務単位で対象システムに一斉に配付できます。
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。
強制配付	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。

● 資源適用日のスケジュール

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。全社一斉にはじ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。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。

● 中継サーバを経由した配付

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。また、同一 LAN 内の中継サーバから資源をダウンロードさせることで、WAN への課金も削減できます。

注) 中継サーバは、部門管理サーバ、業務サーバのどちらかを利用

● 資源を分割して配付

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

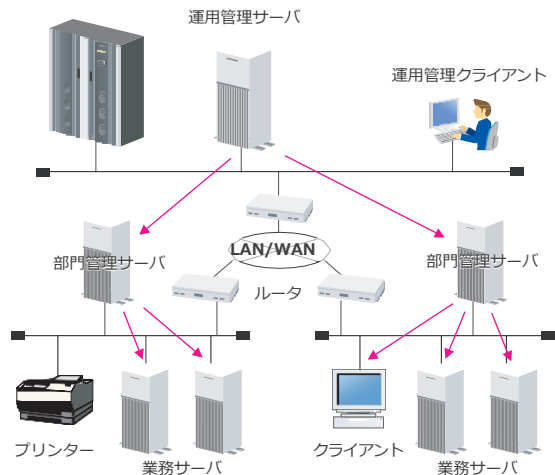
サーバ間で配付資源を分割して配付します。一定の転送量や送信間隔を指定し、分割、転送できるので、運用に与える影響を最小限に抑えることができます。

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。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は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を開始できます。

管理形態

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 で管理する ICT 資源

項目	内容
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、パフ）、サーバ機（UNIX、AT 互換機）、プリンターなど IP を持ったハードウェア
システム	UNIX（Solaris、HP-UX、AIX）、Linux、Windows などの OS
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、お客様が作成したアプリケーションなどの実行ファイル

■ 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。

■ 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として、以下の役割を持ちます。
・部門内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 でのポーリングによる監視を行います。
・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。

■ 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。

■ 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 端末で動作します。Linux 版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する必要があります。Windows 版の場合、運用管理サーバで兼務することができます。

■ クライアント

被管理のクライアント PC です。

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の機能差

	インストールレス型エージェントの場合 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の場合
監視方法	一定時間間隔で情報を取得し、監視	リアルタイムで監視
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い	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る
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る。1 台の監視サーバで監視できるサーバは 300 台まで	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る

システム監視

	インストールレス型エージェント 非デプロイ方式	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
シスログ/イベントログ監視	○ ※1、※2	○ ※2	○
リモートコマンド	○	○	○
ログファイル監視	×	○ ※3	○ ※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 ※1：Hyper-V のイベントログは監視できません。 ※2：カスタムイベントログは監視できません。
※3：監視対象ファイルについて、監視可能なファイル数/ファイルの文字コードに違いがあります。

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 非デプロイ方式	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
ハードウェア情報 注1	○	○	○
ユーザー情報	×	×	○
ソフトウェア情報 注1	○	○	○
レジストリ収集情報 (Windows のみ)	×	○	○
テキスト情報	×	×	○
ソフトウェア辞書情報収集 (Windows OS 用)	×	○	○
ソフトウェア辞書情報収集 (UNIX/OS 用)	○	○	○

○：使用可能、×：使用不可

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。

サーバ性能監視 注2

	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	×	○
ヒストリ表示	×	○
ノード中心マップ/ペアーノード経路マップ (サーバ性能情報)	×	○
しきい値監視 ー CPU 使用率 ー 実メモリ使用率 ー ディスク使用率	○ イベント自動対応は不可 復旧イベントにて代替	○
しきい値監視 ー ページフォルト数、ディスクビジー率、実メモリ空き容量 他	×	○
性能情報出力 (サーバ性能情報)	×	○
論理ディスク単位の監視 (mptfbypart コマンド)	×	○
サーバ性能 MIB	×	○

○：監視可能、×：監視不可

注2：サーバ性能監視は、インストールレス型エージェント (非デプロイ方式) では使用できません。

アプリケーション監視 注3

	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/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制/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	×	○
クラスターサービスの監視	×	○

○：監視可能、×：監視不可

注3：アプリケーション監視は、インストールレス型エージェント (非デプロイ方式) では使用できません。

あんしん セキュリティ対策と高信頼な監視

うっかり操作や不正な操作を抑止

● コンソールの操作制御^{*1}

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たり、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、セキュリティ上の問題も深刻になってきました。

Systemwalkerは、セキュリティの脅威である「偶発的脅威」、「意図的脅威」に対応しています。

^{*1}: 本機能は、Enterprise Edition / Global Enterprise Editionで提供

● 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ID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。

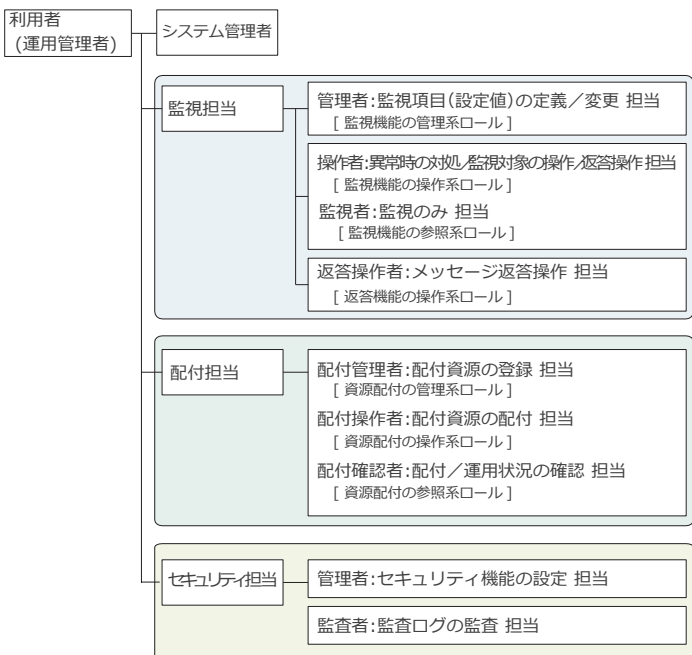
システム管理者やオペレーターごとに運用管理クライアント用の端末が配備され、各担当者にSystemwalkerにログインするIDを割り当てる場合や、操作する資源ごとに専用の運用管理クライアントが存在し、運用管理クライアントごとにログインするIDを割り当てる場合などに、Systemwalkerコンソールにログインするユーザーごとに操作の制限を設定できます。

● 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時に操作を行うユーザーのID(ユーザーID)の入力が必要です。Systemwalkerコンソールで操作する時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できます。運用管理クライアント^{*2}をオペレーター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ー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。

^{*2}: 運用管理サーバを操作するためのコンソール機能を持つクライアント端末。システム管理者やオペレーターは、運用管理クライアントより、分散システムの監視、操作、配付業務などを行います。

Systemwalker Centric Manager の利用者(運用管理者)とロールの関係



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。

● SMARTACCESSとの連携



運用管理クライアントにSMARTACCESS^{*3}を導入することにより、非接触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が強化できます。SMARTACCESSと連携した場合、システムを操作するためのユーザー名やパスワードが漏洩する可能性が低くなり、なりすましが防止できます。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ーのID(ユーザー名)の入力が自動化できます。

^{*3}: PCの不正使用対策ソフトウェア(富士通製)

Windows版の運用管理サーバ上ではSMARTACCESSを使用できません。

● サーバへのアクセスを制御 【対応OS : Windows】

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

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。

● 監査ログ出力

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。

項 目	内 容
アクセス監査ログ	管理対象サーバの資産へのアクセス(ファイルへのアクセスやプロセスの起動/強制停止など)を記録
操作の録画データ	「安全なシステム保守支援」機能を使用した際の作業情報を記録
Systemwalker コンソール監査ログ	システム管理者が、Systemwalker Centric Manager の使用状況を監査するログ。 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/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を記録

● 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。

監査証跡に必要なログを収集して分析

● 監査ログ出力

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。

● 監査ログ管理

企業コンプライアンスの要請に応じて、監査証跡に必要な様々なログを一元管理します。問題操作の抑止力として活用したり、各ITシステムでの問題発生時の追跡や監査時の証明のためにアクセスログの保管が可能です。また、テンプレートを利用して監査レポートを作成したり、Interstage Navigator Serverと連携して、容易な分析、レポートが可能で

・収集可能なイベントログ/ログ

OSのイベントログ/ログ関連

Windows OS	UNIX OS	Windows IISログ
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	シスログ /var/adm/loginlog (Solarisのみ対応) suログ (/var/adm/sulog) (Solaris、HP-UX、AIXのみ)	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

アプリケーション/他、関連

- ・Apache : アクセスログ NCSA形式(初期形式)/エラーログ
- ・Systemwalker Centric Manager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、コンソール操作/サーバアクセス制御の監査ログ
- ・Systemwalker Desktop Keeperバックアップコマンドによるクライアント操作ログ
- ・Systemwalker Operation Managerの操作ログ
- ・ETERNUS NR1000F seriesのイベントログ
- ・テキストログで 監査ログ管理機能の収集規約に合致しているもの
- ・バイナリファイルのログ*

*9: Systemwalker Centric Manager V13.2.0以降の運用管理サーバ、被管理サーバ、または、中継サーバで対応

セキュリティ対策の強化

● ネットワークセキュリティの強化

Systemwalker Centric Managerでは、不正パケット送信による妨害の防御や、通信傍受による情報漏洩を防ぐ取り組みを行っています。

・ネットワーク監視パケット傍受による情報漏洩を防止

「SNMPv3」を使用した監視機能を提供しています。管理サーバと監視対象ノードやネットワーク機器の間で、通信データを暗号化することにより、より安全に情報の送受信を行うことができます。

注)SNMPv3は、ユーザー認証や、通信データの暗号化をサポートしています。

SNMPv3を使用して監視を行うためには、監視を行うサーバおよびネットワーク機器のSNMP エージェントがSNMPv3に対応している必要があります。

・監視イベント傍受による情報漏洩を防止

「S/MIME」を使用したデータの暗号化機能を提供しています。S/MIMEを使用し、E-Mailを使用した通信を暗号化することにより、外部の第三者が通信データを傍受しても、データを解析することが困難となり、情報漏洩の脅威が大幅に軽減されます。

注) S/MIME (Secure/Multipurpose Internet Mail Extensions) : 電子メールの標準的な暗号化方式。RSA公開鍵暗号方式を使用しています。

・配信コンテンツの傍受による情報漏洩を防止

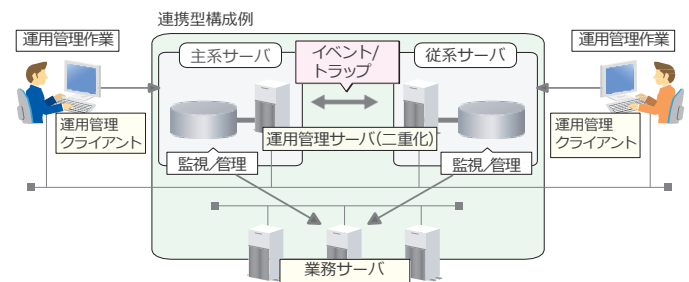
「HTTPS通信」を使用した資源配付機能を提供しています。HTTPS通信を使用して配付データを暗号化することにより、インターネットで構築されたネットワーク上でも安全に資源を配付できます。

高信頼な運用管理 Systemwalker のここがすごい！

確実で安定した監視運用を実現するため、さまざまなセルフチェック機構・トラブル追跡機構を装備しています。

① 運用管理サーバの二重化サポート*1

運用管理サーバでは、二重化構成をサポートしています。二重化構成では、H/Aクラスタ構成と比較し、主系管理サーバのトラブル時においても、従系管理サーバにおいて、切り替え時間0秒*2で継続監視が可能です。また、製品への修正適用においても、従系への修正適用後、管理サーバを切り替えることにより、監視運用を停止せずに修正適用が可能です。*1:本機能は、Enterprise Edition / Global Enterprise Editionで提供。*2:Systemwalkerは主系/従系で同時監視のため切り替えは不要です。



複数の運用管理サーバをそれぞれ主系サーバ、従系サーバと設定し、二重化するシステム構成です。クラスタシステムを用いて高信頼化する場合と異なり、両方のサーバから監視業務を行っているため、ノードダウン時でも監視は継続できます。また、同じ機能を持つ複数の運用管理サーバを設置し、それぞれで運用管理作業を行うシステムも構築できます。災害対策のため地域的分散を目的とした構成です。

② 運用管理システムのクラスタ対応による高信頼化*3

Systemwalker Centric Managerは、クラスタソフトウェアと連携して、高信頼環境での運用管理を実現します。運用管理サーバをクラスタシステムで動作させることで、片方のノードに障害が発生しても、正常な側のノードで監視業務を引き継ぎます。

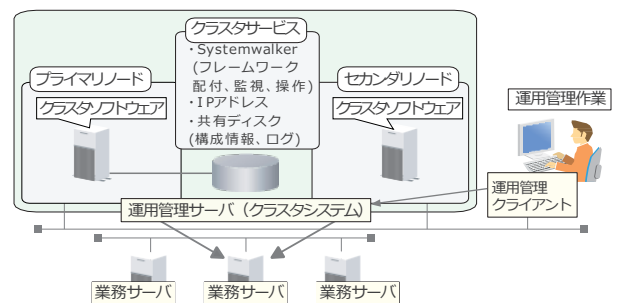
*3 : 本機能は、Enterprise Edition / Global Enterprise Editionで提供

クラスタシステムのサポート範囲

クラスタソフトウェア	対応OS	クラスタシステム				スケラブルクラス
		運用待機(1:1)	運用待機(1:N)	運用待機(N:1)	相互待機	
PRIMECLUSTER	Linux	○	○注	△	△	△
MFOC	Windows	○	○注	—	△	—

○ : Systemwalker自身が対象の運用形態をサポートしている 注:業務サーバのみサポート
△ : Systemwalker自身は、1:1運用待機で動作する
— : クラスタソフトウェアがサポートしない運用形態 MFOC : Microsoft Fail Over Clustering

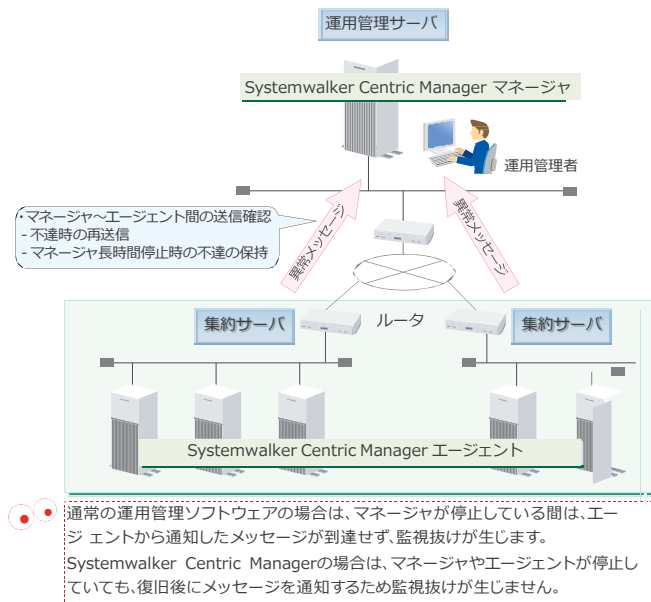
クラスタソフトウェアを利用した運用管理サーバのクラスタシステム構成



1:1の運用待機の構成で運用する例です。管理情報を共有ディスク上に配置し、運用系で異常が発生した場合は、クラスタシステムが異常を検出し、待機系に運用を引き継ぎます。クラスタシステムが制御する共有ディスクで管理情報を共有するため、引継ぎは自動で行われます。

③ メッセージ通知の高信頼性

Systemwalkerでは、マネージャ〜エージェント間での送達確認機能により、メッセージの不達時における再送信や、長時間マネージャが停止していた時に、エージェント側で未達メッセージの保持を行うことが可能です。これにより、メッセージ管理の高い信頼性を実現しています。



④ セルフチェック機構

これは便利！

・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コンソールに異常を通知します。

・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 コンソールに異常を通知します。

・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。👍 P.14

・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*1情報の一元管理

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。

*1: IPC（Inter Process Communication）資源とは、複数のプロセスや、スレッド間で情報を共有するために使われる、メッセージ、共有メモリ、およびセマフォなどのリソースを指します。

さまざまなシステム環境で高信頼な監視を実現

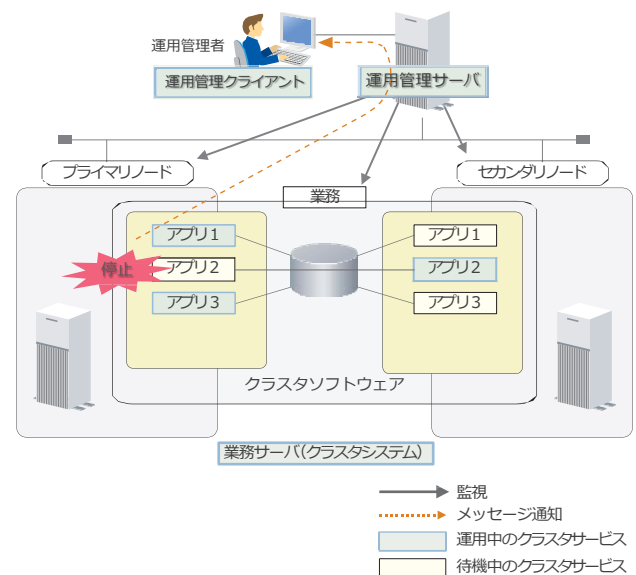
● クラスタシステムの監視

クラスタソフトウェアに登録されているクラスタサービスを自動検出し、個々のクラスタサービスを監視対象とすることができます。クラスタサービスがフェイルオーバーした場合は、メッセージを送信し、システム管理者にクラスタシステムの運用状態を通知します。なお、クラスタシステムを構成しているプライマリノード、セカンダリノードは、シングル環境と同様の操作で運用管理することができます。

*本機能は、Enterprise Edition / Global Enterprise Editionで提供

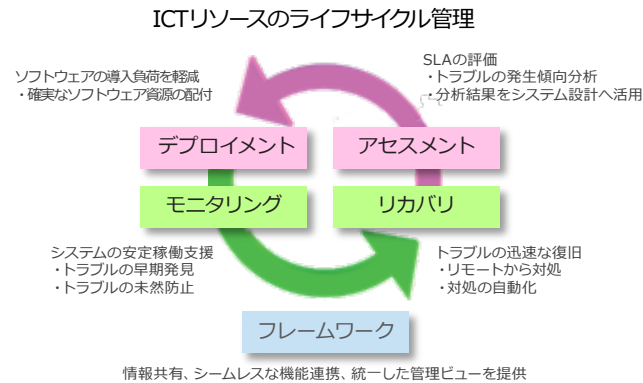
・サポートするクラスタシステムの形態

Systemwalker Centric Managerでは、Microsoft(R) Fail Over ClusteringならびにPRIMECLUSTER を使用する場合は、1:1運用待機および1:N構成の運用形態を、Oracle Solaris Clusterを使用する場合は、1:1運用待機をサポートしています。



かんたん 必要な機能をオールインワンで提供

運用のライフサイクルを網羅



ICTシステム運用のライフサイクルに必要な様々な支援機能を提供します。ICTシステムの円滑な運用に必要な不可欠な機能を統合することで、システムの安定稼働を実現します。また、運用管理に必要なシステム全体の情報の一元管理と、一連の運用管理操作のシームレスな連携により、運用コスト（TCO）を大幅に削減します。

ライフサイクル管理:
ICTシステムを運用管理するうえで、システムの導入・設定から稼働監視、トラブル対応（復旧）、運用評価・分析までの一連の運用業務をいいます。

機能		概要
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。
	ソフトウェア修正管理	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 ^{*1}	ICT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。
	イベントの集約	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可能です。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。
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。
	レポート	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。
アセスメント（評価）	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行き、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		・ 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他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ー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 監視対象と監視の手法

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) 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の閾値監視)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

これは便利！

● Systemwalker自身のインストール負荷を軽減

・サイレントインストール (サーバ/クライアント)

製品のインストール方法には、DVD-ROMから対話形式でインストールに必要な情報を入力しながら行う方法と、インストール時に作業者の入力を求めずに必要な情報をあらかじめ作成したインストール情報ファイルから読み込んで自動的にインストールする方法(サイレントインストール)があります。サイレントインストールは、作業の分散やインストール作業の負担を大幅に軽減させることができます。

【対応 OS : Windows, Solaris】

・資源配付機能を使用したアップグレードインストール

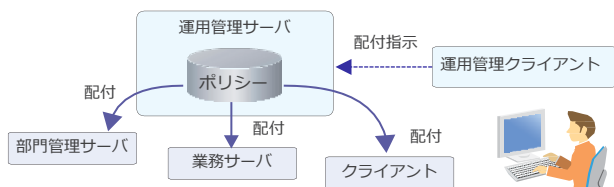
既にSystemwalker Centric Managerの資源配付機能を使用している場合は、資源配付機能を使用してサーバとクライアントのアップグレードインストールができます。資源配付機能でSystemwalkerのインストール媒体(DVD-ROM)の資源とサイレントインストール用のファイルを配付し適用します。配付適用後、資源配付機能で導入支援コマンドが起動され、サイレントインストールが実行されます。

注)本機能は、OSがWindowsの場合は、全サーバ、全クライアントに対して利用できます。また、OSがSolarisの場合は、業務サーバ、全クライアントに対して利用できます。

● 動作環境の設定 (ポリシー*設定)

管理者が策定したポリシーに従って、サーバやクライアントの各種設定を運用管理サーバ上で一元管理できます。また、これらのポリシーを運用管理サーバからすべての部門管理サーバ、業務サーバ、およびクライアントに対して一括して動作環境を設定できるため、管理者の導入作業負担を軽減するとともに、管理者が想定する統一された設定での運用を実現できます。一方、データセンターなどの大規模な環境では、お客様あるいは提供サービスごとに監視対象をツリーで分けて監視する必要があるため、お客様/提供サービス(テナント)ごとの管理者に監視ポリシーの設定権限を与え、監視ポリシーを設定することもできます。これにより、データセンター全体の管理者の作業工数を軽減できます(マルチテナント監視)。

*ポリシー：情報システム全体を、効率よく維持・管理するための運用方針のこと



【各種ポリシー設定項目】

- ・資源配付(インベントリ管理、資源配付)
- ・セキュリティ(監査ログ管理)
- ・監視(イベント、ノード、性能、アプリケーション、インストール型エージェント、他)

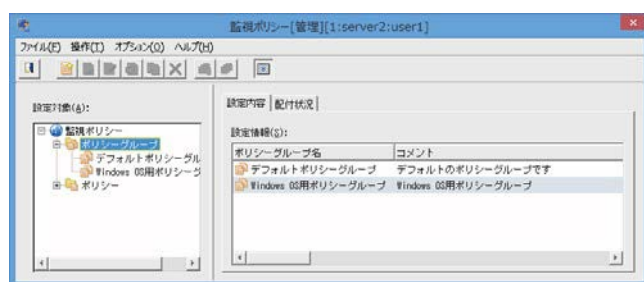
これは便利！

● 監視ポリシーの設定/グルーピング

標準的なデフォルトポリシーが予め設定されています。このため、監視対象サーバの割り当てだけで、運用を即座に開始できます。

なお、お客様固有の環境や要件に対応する場合は、デフォルトポリシーの変更、サーバ性能監視、MIB監視、特定ノード個別のネットワーク・インターフェース監視の設定、アプリケーション監視などを個別に設定してください。

監視ポリシーは、監視対象や監視の目的に合わせてポリシーグループ単位で管理できます。これにより、運用時に監視ポリシーの変更が必要となった場合は、該当する監視ポリシーだけを変更して配付することで、運用変更に簡単に対応できます。



● 稼働監視定義は、テンプレートを使用して作業の効率化

Systemwalker Centric Managerでは、監視対象の異常メッセージや常駐プロセスの監視定義をSystemwalkerテンプレートとして提供しています。Systemwalkerテンプレートを適用することで、監視の設定作業が簡単にできます。監視ポリシーにおいて使用するSystemwalkerテンプレートは、2種類があります。

・イベント監視テンプレート

サーバ、OS、およびミドルウェア製品が出力するメッセージを監視するための標準定義で、イベント監視の条件定義を監視ポリシーとして、メッセージのフィルタリングを行います。

- ー 不要なメッセージをフィルタリングし、異常メッセージだけを監視できます。
- ー メッセージのエラー種別に応じて、メッセージの重要度を補正できます。
- ー 異常メッセージの説明や対処方法を確認できます。

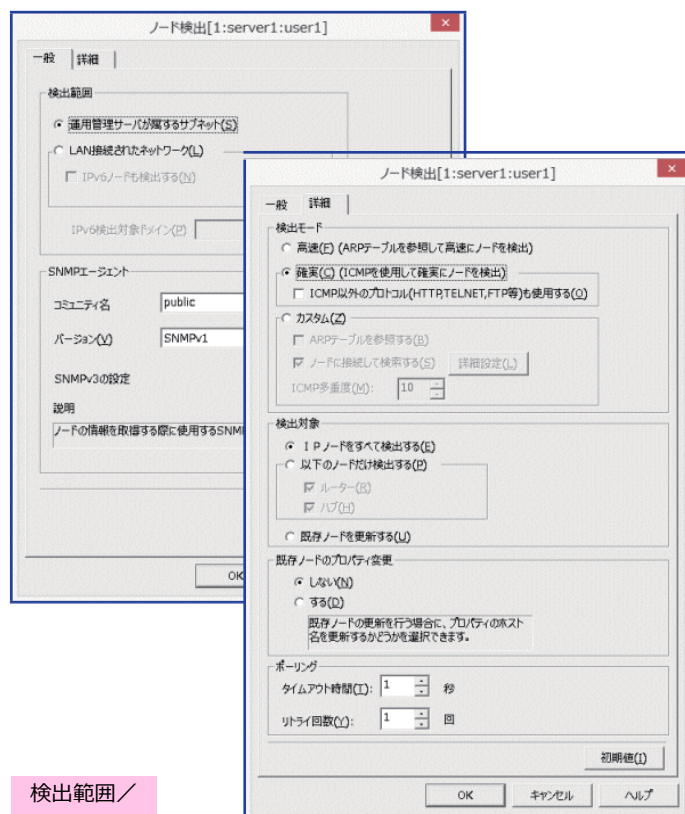
・プロセス監視テンプレート

ミドルウェアの監視対象アプリケーション(常駐するプロセス)の稼働状況を監視できます。

注)Systemwalkerテンプレートは、Systemwalker技術情報ホームページで最新版を公開しています。P.14

● 監視するネットワーク構成の自動検出

運用管理サーバの属するサブネットに接続しているノードを検出した後、運用管理サーバの属するサブネットだけでなく、LANで接続されているノードをすべて検出することが可能です。また、指定したサブネット(フォルダ)に所属するノードを検出することもできます。



検出範囲/
検出モード

運用管理サーバが属するサブネット

運用管理サーバの属するサブネットに接続しているノードを検出。

LAN接続されたネットワーク

運用管理サーバの属するサブネットだけでなく、LANで接続されているノードをすべて検出。

高速

ARPテーブル(IPアドレスとMACアドレスの対応表)を参照して高速にノードを検出。存在しないノードや停止しているノードでも、ノード検出処理中にARPテーブルに存在する場合は、新ノードとして検出される場合がある。

確実

ICMP(ping)を使用して確実にノードを検出。ICMP検査を行うとSNMPエージェントが動作していないノードでも、IP通信可能であれば検出。

● 動作環境のチェック これは便利！

Systemwalker Centric Managerが動作するために必要な動作環境として正しいかどうかを検証する「動作環境定義チェックツール」^{*1}を提供しています。

運用中のトラブルを回避するために事前に本ツールを使用し、環境設定に問題がないかを確認したり、運用中に環境異常によるトラブルが発生した場合は、Systemwalker Centric Managerに関係する環境設定に問題がないかどうかを確認することもできます。

*1: 本ツールは、製品に同梱されています。チェック項目の追加のために更新される場合があります。ご使用にあたっては、Systemwalker 技術情報サイトをご確認ください。👉 P.14

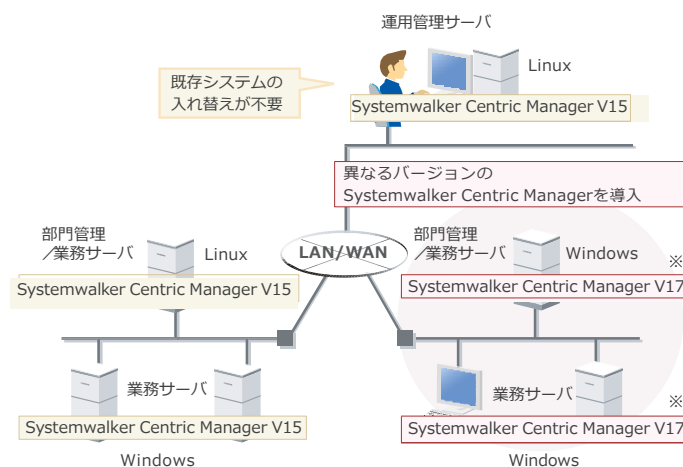
環境定義チェック機能		動作OS		
		Windows	Solaris	Linux
システムの環境チェック	ファイアーウォール機能の状態	○	—	—
	TCPポート	○	○	○
	SNMPエージェントの定義、起動可否	○	○	○
	デスクトップヒープ領域サイズ	○	—	—
	syslogのメッセージ監視におけるホスト名の整合性	—	○	○
	監視対象ノードのICMP応答	○	○	○
	監視対象ノードのSNMP応答	○	○	○
システムのファイルチェック	syslog.confのメッセージ監視定義	—	○	○
	servicesファイルの定義	○	○	○
	systemファイルの定義	—	○	○
Systemwalker Centric Managerの設定チェック	hostsファイルの存在・定義	○	○	○
	ネットワーク・インターフェースの搭載数	○	○	○
	性能監視の監視ポリシー	○	○	○

○: 動作可能項目
—: チェック対象外

Systemwalker のここがすごい

● プラットフォームやバージョンが混在した形態にも対応

さまざまなプラットフォームのシステムを混在させた構成や、Systemwalker Centric Managerの異なるバージョンが混在する環境も資源の配付や、異常監視などの運用管理を行うことができます。

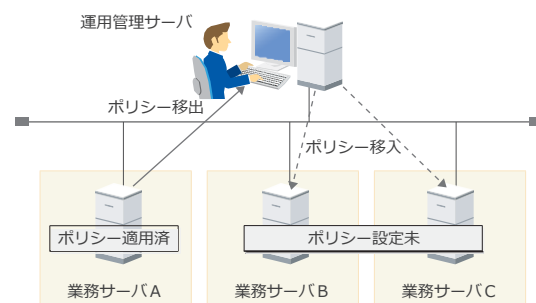


※古いバージョンレベルの範囲での機能を利用可能

● 被監視サーバの追加 これは便利！

新規にサーバを追加する場合、既に同じポリシーを適用したサーバがあれば、そのサーバのポリシーを移出し、新規に追加するサーバに移入することで、新規サーバのポリシーを設定することができます。

Systemwalkerのサイレント・インストール(無手順導入)と組み合わせることでインストール完了後は、即時、運用開始が可能です。



この機能を使用する場合、既にポリシーが設定されているサーバと新規にポリシーを設定するサーバには、以下の条件があります。

- ・同じOS
- ・同じバージョンレベル(本機能に対応しているのは、V11.0L10/11.0以降)
- ・同じインストール種別
- ・同じインストールオプションをインストールしている
- ・業務利用目的など、同じポリシー設定で監視できる

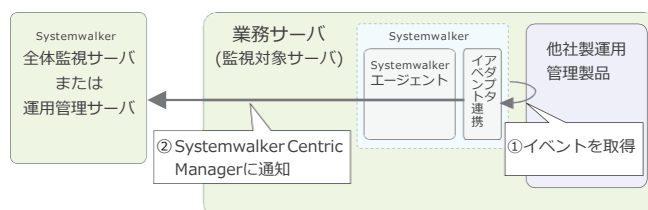
● 他社運用管理製品との連携

多くの企業システムは、最適なICT資源でシステムを構築するためにいろいろな機種が存在する環境となっています。

Systemwalker Centric Managerは、本製品が提供するエージェント機能と、他社の運用管理製品とが連携し、各製品が動作するプラットフォーム(Windows、Solaris)での管理機能を、包括的に管理・統合することができます。

なお、他社の運用管理製品と連携する場合は、Systemwalker技術情報サイトで提供される「他社運用管理製品連携アダプタ」を、併せてご利用頂くことで実現できます。

イベント通知の概要図



- ① イベント連携アダプタで他社製運用管理製品からイベントを取得します。
- ② イベントをSystemwalker Centric Managerに通知します。

● サンプルスクリプト これは便利！

ISV(Independent Software Vender)やお客様固有要件の対応のために、Systemwalkerの機能を容易に拡張・カスタマイズできる機能です。インテリジェントサービスは、さまざまなサンプルスクリプトを提供しています。標準提供のサンプルスクリプトを利用することにより、お客様の運用環境に最適な監視機能を実現できます。

サンプルスクリプト	説明
イベント固定テキスト変換	イベントテキストの変換を行います。変換は、1つのスクリプトで1パターンしか行えず、変換の組み合わせが複数ある場合は、その組み合わせの数だけスクリプトを作成する必要があります。
イベント切り分けテキスト変換	複数パターンのイベントテキストの変換を行います。ライブラリ型のスクリプトで変換の組み合わせを複数定義することで、1つのスクリプトで複数パターンの変換が行えます。
先頭通知コリレーション	発生した複数のイベントに対し、不要なイベントを破棄します。
末尾通知コリレーション	定義した一連のイベントの通知を抑止するとともに、一定時間内にそれらのイベントすべてが発生したかをチェックし、その結果に応じた異常通知を行います。
必要イベント未発生調査	現時刻から一定時間さかのぼってログ内を検索し、正常の場合に出力されるイベントが存在しない場合、イベントを新規発行します。また、その動作を一定間隔で繰り返すことができます。
大規模同報リモートコマンド	引数で指定されたコマンドを、システム監視を行っている複数システムに対して実行し、その応答結果をレポートします。
メッセージ監視アクション型スクリプト動作テスト	メッセージ監視アクション型サンプルをもとに作成したユーザスクリプトの動作確認テストをします。
稼働状態の監視	被監視ノード、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SNMPトラップを通知します。
MIBしきい値監視	被監視ノード、またはネットワーク機器に対し、一定間隔でMIB取得を行い、しきい値を超えた場合、運用管理サーバ、または部門管理サーバへSNMPトラップを通知します。
サービス稼働監視	監視対象ノードで動作するサービス(HTTP/SMTPなど)に対し、一定間隔で稼働状況の監視を行い、指定時間内に応答がない、またはエラーが発生した場合、運用管理サーバへイベントを通知します。
イベント詳細フィルタリング	単一の通知イベントに対して諸情報を解析し、その結果に応じてイベント情報の書き換えを行えるようにします。
切り替え型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相当の処理を「アクティブパターン」でデフォルトパターン「2種類持ち、トリガとなるイベントの発生によってどちらを使用するかを動的に切り替えてイベント情報の書き換えをします。
Systemwalkerセルフチェック	下位サーバで動作するシステム監視エージェントに対して、上位サーバから指定された監視間隔でTCP接続を行い、接続可能かどうか監視します。
Webサービス稼働監視	Webサービスを構成するSOAPサーバが停止していないか、また、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。
IPv6インターフェース稼働監視	被監視ノード、またはネットワーク機器のIPv6インターフェースに対し、一定間隔でpingを行い、監視対象のIPv6インターフェースが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SNMPトラップを通知します。
ライブラリ型スクリプト動作テスト	ライブラリ型サンプルをもとに作成したユーザスクリプトの動作確認テストをします。
関係イベント自動対処	イベント（異常メッセージと復旧メッセージ）の自動対処をします。
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。
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	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。
パラメータを含むプロセス稼働監視	パラメー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、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。

● Systemwalker Centric Manager 技術情報

多様化し、日々変化するシステム環境に素早く柔軟に対応できるよう、当社の長年の運用管理実績に基づいた50種類以上の運用管理ノウハウ^{*1}をデータ化し、インターネットからダウンロードしてご利用いただけます。これにより、運用管理システム環境を簡単に構築できるため、運用管理システムの構築や変更に必要な時間と費用を削減できます。

*1:効率的に運用管理システムを構築するための監視設定やレポートのテンプレート、ドキュメントなどが、ご利用できます。

● 運用管理の短期構築を支援

各種の監視ノウハウを監視フィルタ定義体の形で公開

● 監視ツール・連携ツールの提供

Systemwalkerファミリーや富士通のInterstageといった製品と連携するためのマニュアル、各種ミドルウェアを監視するための定義テンプレート、Cisco機器やMicrosoft Operations Managerと連携するためのツールなど

動作環境

製品名	サーバ動作OS	クライアント動作 OS
Systemwalker Centric Manager	Microsoft(R) Windows Server(R) 2022 Microsoft(R) Windows Server(R) 2019 Microsoft(R) Windows Server(R) 2016 Oracle Solaris 11 *1 Red Hat Enterprise Linux 9 Red Hat Enterprise Linux 8 Red Hat Enterprise Linux 7 AIX *2 HP-UX *2	Windows(R) 11 Windows(R) 10

*1：業務サーバのみ提供しています。
*2：インストールレスエージェント監視で対応します。

対応クラウド環境

製品名	クラウド環境
Systemwalker Centric Manager	FUJITSU Hybrid IT Service FJcloud-O FUJITSU Hybrid IT Service FJcloud-V FUJITSU Hybrid IT Service for Microsoft Azure FUJITSU Hybrid IT Service for AWS FUJITSU Cloud Service AZCLOUD IaaS Microsoft Azure Amazon Elastic Compute Cloud (Amazon EC2) Oracle Cloud Infrastructure FUJITSU Cloud Service for SPARC

商品体系

商品名称	Windows	Linux	Solaris
Systemwalker Centric Manager Standard Edition V17	●	●	● *1
Systemwalker Centric Manager Enterprise Edition V17	●	●	● *1
Systemwalker Centric Manager Global Enterprise Edition V17	—	●	—
Systemwalker Centric Manager クライアントライセンス V17		●	
Systemwalker Centric Manager クラウドサービス監視用 V17		●	—

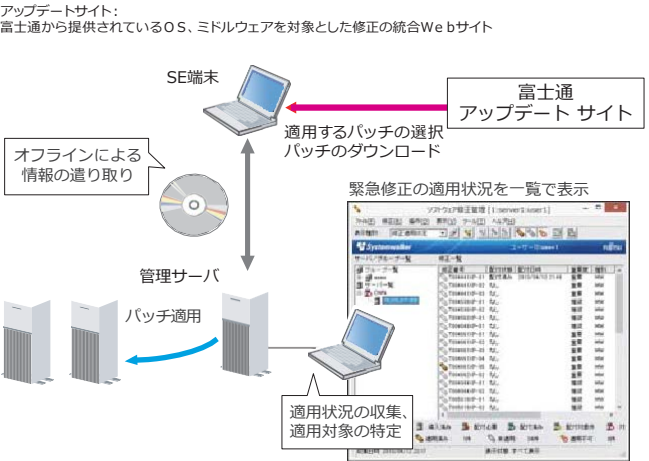
Systemwalker Centric Managerは、システム規模と信頼性への要件に応じて3つのエディションを提供します。
・Standard Edition：TCP/IPネットワーク上の標準的なクライアント・サーバ環境、インターネット環境における業務のライフサイクルを管理する機能を提供します。
・Enterprise Edition：Standard Editionの全ての機能に加えて、より高信頼（クラスタ対応等）、高度なセキュア環境、大規模な環境によるマネージャの階層化などの運用形態に最適な商品です。
・Global Enterprise Edition：Enterprise Editionの全ての機能に加えて、グローバルサーバを含む大規模な環境に対応した商品です。
クライアントライセンスは、Standard Edition、Enterprise Editionをご利用の際に、運用管理クライアント、またはクライアントを管理対象とした場合に必要です。
クラウドサービス監視用は、ハイブリッド監視機能でクラウドサービスを監視する場合に必要です。
*1：業務サーバのみ提供しています。

各エディションごとの機能表 ※動作させるOSにより、利用できる機能が若干異なります。

代表的な機能	Standard Edition	Enterprise Edition	Global Enterprise Edition
デプロイメント（配付）	○	○	○
モニタリング（監視）	○	○	○
リカバリ（障害復旧）	○	○	○
アセスメント（評価）	○	○	○
フレームワーク	○	○	○
SDK	○	○	○
高信頼システム構築機能 ・ クラスタシステムの監視 ・ 管理サーバのクラスタ対応 ・ 管理サーバの二重化 ・ ハイセキュア化機能 （ICカード(Felica方式)、指紋認証など）	—	○	○
大規模システム構築機能 ・ 全体監視(管理サーバの階層化)	—	○	○
グローバルサーバの監視	—	—	○

富士通アップデートサイトと連携してシステムの最新化を維持できます。

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。サーバで未適用となっているすべての修正をダウンロードして、サーバに適用する運用です。すべての修正をダウンロードするまでの処理を自動で行うことができます。



* Microsoft、Windows、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。
* Oracle Solaris は Solaris、Solaris Operating System、Solaris OS と記載することがあります。
* 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。
* 文中の社名、商品名等は各社の商標または登録商標である場合があります。
* 本資料に記載されているシステム名、製品名などには、必ずしも商標表示(TM、®)を付記していません。
■ このカタログに掲載されている内容については、改善などのため予告なしに変更することがありますのでご了承ください。