

Chakra-WebSAM SystemNavigator 連携のご紹介

日本電気株式会社
第一システムソフトウェア事業部
2008年5月

Chakra導入時に運用管理も見直してみませんか？

■こんな要件はございませんか？

- ☑ ChakraによるDBセキュリティ監視とシステムの障害監視を一元化したい
- ☑ 既存システムが複数の管理ツールで管理されており、運用の見直しをしたい
- ☑ 現状、障害監視が出来ておらず、この機会に統合監視ツールを検討したい

■システムが別々に管理されていると？

- ▲ 日々の運用で、システム(機能)ごとに別々の画面を見なければならない
- ▲ 通報の設定が複数に分散され、登録や変更が煩雑になる
- ▲ メッセージの見え方やツールの操作方法が異なるので習得が大変



などの症例が出てくる可能性があります。

そこで！！

◎WebSAM System Navigatorが、Chakraを含めた統合管理で

システムの効率的な運用をサポートします。



Chakra-WebSAMの連携メリット

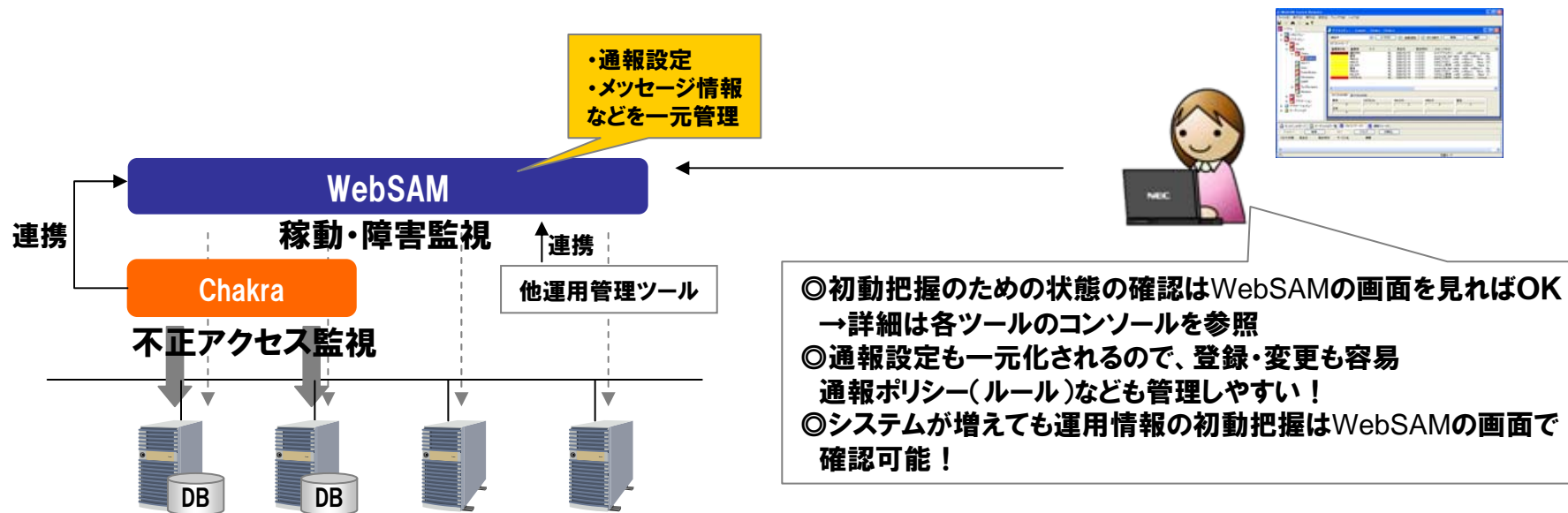
課題

- 日々の運用で、システム(機能)ごとに別々の画面を見なければならない
- 通報の設定が複数に分散され、登録や変更が煩雑になる
- メッセージの見え方やツールの操作方法が異なるので習得が大変



解決

WebSAMでシステムの状態や稼動状況を統合管理することで、通報設定やメッセージ確認を一元化することができ、システム異常の初動を効率良く把握することが出来ます



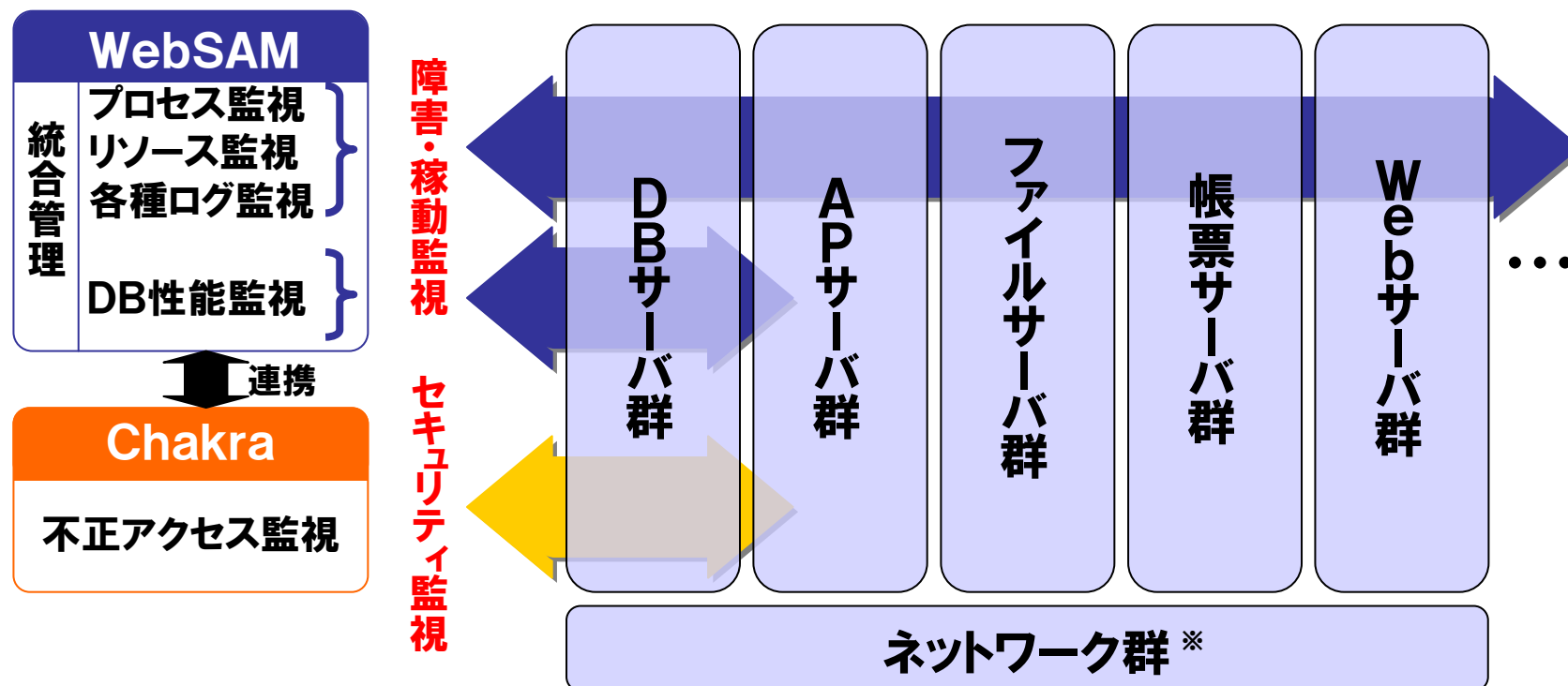
**Chakra – WebSAM System Navigator
連携詳細説明**



U can change.

Chakra-WebSAMの監視領域

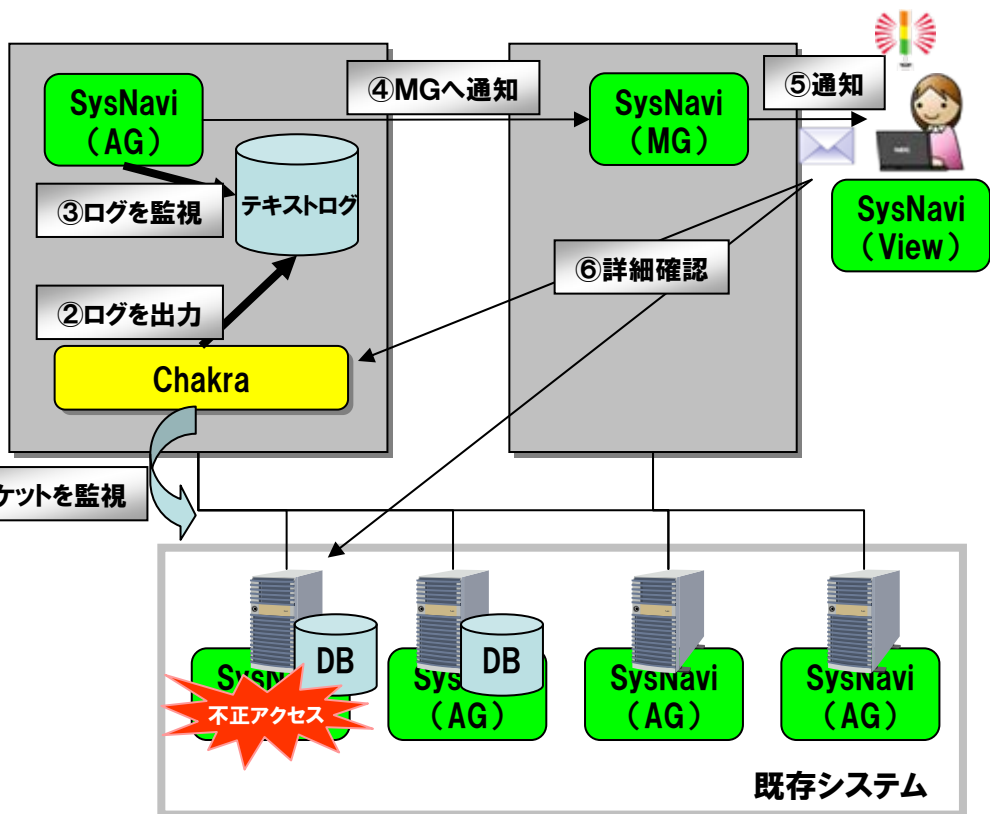
WebSAMでシステムの障害や稼動状況を監視し、Chakraで不正アクセスを監視！
通報や初動確認はWebSAMの統合コンソールで一元管理し運用を効率化



※WebSAM NetvisorPro Vで監視可能

Chakra – WebSAM連携による通報の流れ

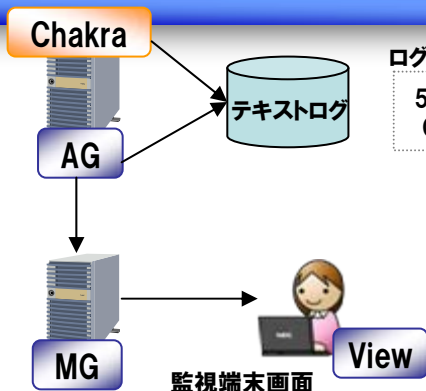
Chakra-WebSAM SystemNavigator連携は、アプリケーションログ連携を実施。
上記の連携により、テンプレート利用で簡単導入 & 運用を実現。



■処理の流れ

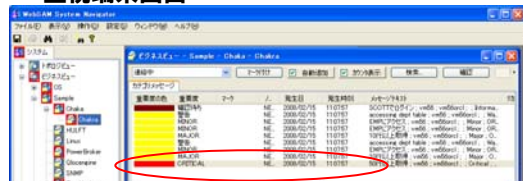
- ① Chakraがパケットを監視し不正パケットを検出
- ② Chakraが不正パケット検出をテキストログに吐出す。
- ③ SysNavi AGがテキストログを監視し、キーワードマッチングしたものを検出する。
- ④ SysNavi AGが異常を検知するとSysNavi MGへ通知
- ⑤ SysNavi MGから管理者へ通知を行う。
(メール、パトライト、コンソール表示など)
- ⑥ 管理者はWebSAMで初動を確認し、詳細はChakraやDBへアクセスして確認する。

WebSAM SystemNavigatorメッセージ表示画面

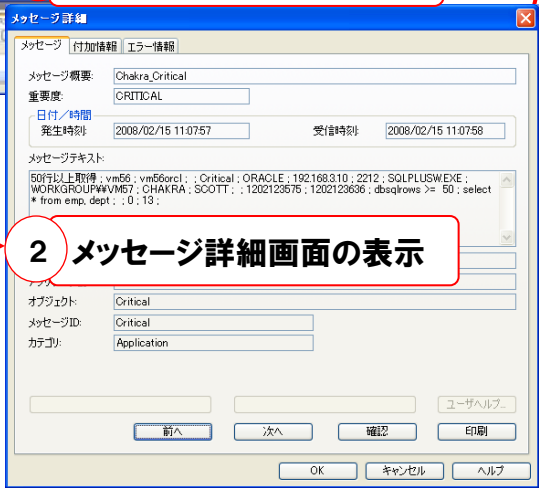


ログ出力例

```
50行以上取得: vm56: vm56orcl : Critical : ORACLE : 192.168.3.10 : 2212 : SQLPLUSW.EXE : WORKGROUP\VM57 : CHAKRA : SCOTT : : 1202123575 : 1202123636 : dbsqlrows >= 50 : select * from emp, dept : : 0 : 13 :
```



1 メッセージをダブルクリック



2 メッセージ詳細画面の表示

メッセージ詳細

メッセージ | 付加情報 | エラー情報

戻る | 進む

3 対応項目毎に、分類されたログ情報の表示

アラートポリシー名	50行以上取得
監視対象サーバ名	vm56
監視対象データベース名	vm56orcl
アラート重大度	Critical
DBMS種類	ORACLE
クライアントIPアドレス	192.168.3.10
クライアントポート番号	2212
アプリケーション名	SQLPLUSW.EXE
端末名	WORKGROUP\VM57
OSユーザ名	CHAKRA
データベースユーザ名	SCOTT
アラート時刻 (unix time)	1202123575
セッション開始時刻 (unix time)	1202123575

前へ | 次へ

エラー情報の補足

セミコロンの数だけ改行されて表示されます。アラート時刻 (unix time) とセッション開始時刻 (unix time) は、UNIX時刻で表示されます。(UNIX時刻とは、1970年1月1日0時0分からの時刻を加算した時刻を指します。)

前へ

【参考】
「エラー情報の補足」説明の表示

Chakra連携の設定イメージ

WebSAM System Navigatorとの連携もテンプレートを活用することにより、直ぐに設定でき、監視をスムーズに開始できます。

設定は提供されている
テンプレートを
インポートすればOK

インポートの指定

フィルタファイルのパス: C:\Documents and Settings\sengoku\Desktop

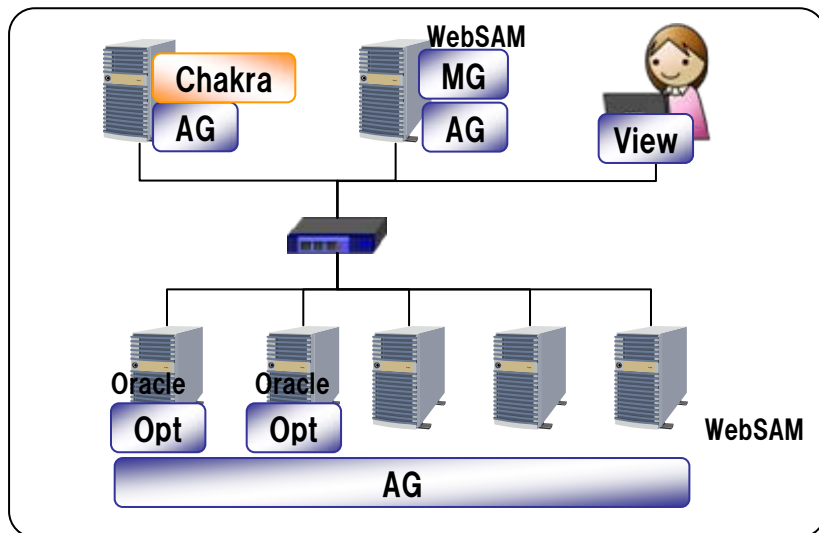
ファイル名	内容	バージョン
sample.txt	*	2.0

インポートボタンをクリックして
インポートするテンプレートを
選択してOKボタンをクリック！

※通報設定はお客様環境に合わせて別途設定いただく必要がございます。

システム構成例

■システム構成例



■要件詳細

- 監視対象サーバ台数7台(Windowsサーバ)
(内訳)Oracle DB 2台、その他 5台
- Oracle DBは表領域の監視も行う
- ChakraでOracle DB2台への不正アクセス監視を行う
- WebSAM の監視端末は1台

■WebSAM モジュール説明(WebSAM System Navigator)

- MG** 各エージェントからのメッセージを統合する機能
- AG** 監視対象サーバ上で動くモジュール
- View** 監視コンソール
- Opt** Oracleの表領域を監視するモジュール

■WebSAM System Navigator 参考価格

製品名	備考	希望小売価格	数量	小計
WebSAM System Navigator - Media	CD-Rom媒体	¥ 39,600	1	¥ 39,600
WebSAM System Navigator	MG×1、View×1、AG×1が同梱	¥ 1,092,800	1	¥ 1,092,800
WebSAM System Navigator - Base Agent-L (1AG)	AG追加ライセンス	¥ 59,600	2	¥ 119,200
WebSAM System Navigator Application Management for Oracle (1AG)	Oracle監視オプション	¥ 138,000	2	¥ 276,000
合計				¥ 1,527,600

※税別、1年間標準保守料込み(2年目以降の保守料は別途必要)

WebSAM System Navigatorのご紹介



U can change.

WebSAM System Navigatorの位置づけ

WebSAM Ver.7が持つ機能のうちサーバ統合運用管理に必要とされる機能を抽出しオールインワンにて提供

コーポレート・マネジメント

統合管理 業務の視点による障害監視、ナレッジデータベースによる復旧支援などにより、効率的な運用管理の実現を支援します	サービスレベル管理 ITサービス管理	資産管理 資産管理	IT全般統制支援 ID管理 ログ管理 システム変更管理
--	------------------------------	---------------------	---

オペレーション・マネジメント

ジョブ管理 ジョブ管理 帳票管理	ソフトウェア配布 ソフトウェア配布 高速リカバリ	プラットフォーム管理 リソース最適化 グリッド	バックアップ バックアップ アーカイブ
-------------------------------	---------------------------------------	--------------------------------------	----------------------------------

システム・マネジメント

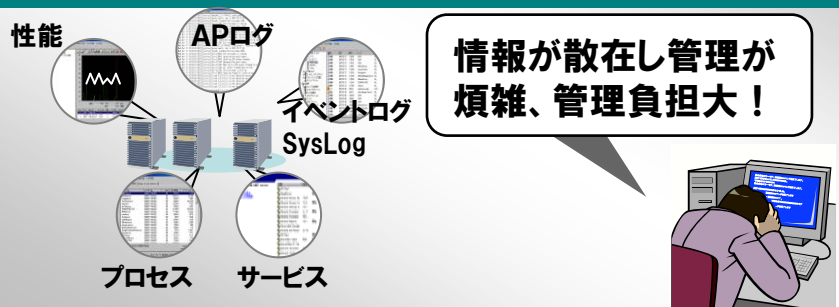
サーバ管理 複数のサーバを効率的かつ統合的な集中監視を実現します。	ネットワーク管理 SNMPトラップ受信オプションによりネットワーク機器のSNMPトラップを受信し、ネットワーク状態の変化を監視することができます。 (オプション)	ストレージ管理 ストレージ運用・構成管理 ストレージ性能管理・監視 無停止バックアップ構築簡易化	アプリケーション管理 Oracle, PostgreSQL, MySQL監視オプションによりOracle, OSSDBの稼動状況を監視します。 (オプション)
---	--	--	--

WebSAM System Navigator

システム運用でよくある課題

このままでは、運用コストも膨大！システムの安定稼動も望めません

人手によるサーバ/システム管理の限界



ユーザからの連絡で初めて障害に気づく



日々の運用ノウハウが共有できない



原因の一次切り分けができず復旧に時間がかかってしまう

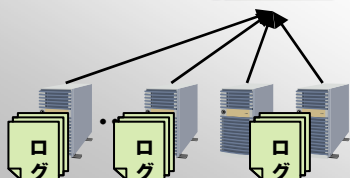


WebSAM System Navigatorで解決！

WebSAM System Navigatorでシステムを統合的に管理し運用の効率化
障害の未然防止／早期発見・分析・復旧を支援！

複数のサーバ／システム状況を
一元管理し運用を効率化

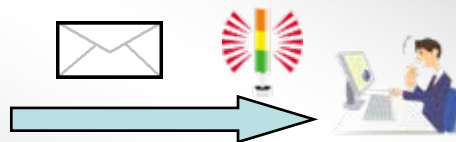
一画面で
把握可能！



監視

通報

異常時には通報機能
により素早く通知



メールで連絡が
あるので安心

業務視点による監視により原因の
特定・影響範囲の特定を支援

ナレッジ機能により
対処方法を共有

対処

分析

原因

ナレッジ機能

対処方法

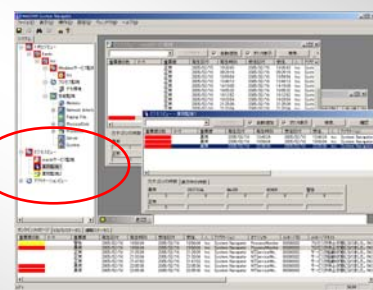


業務視点
(ビジネスビュー)

業務システム1

DB

APサーバ



こんな要件でご活用いただけます

お客様要件

異常時の初動を迅速に把握したい

プラットフォームを問わず、1つのツール(画面)で監視したい。

サーバ稼動監視に必要な機能が一通りそろっていて導入が容易であること

作りこみの業務アプリケーションのログを監視でき、障害情報ごとに通知先を変更したい

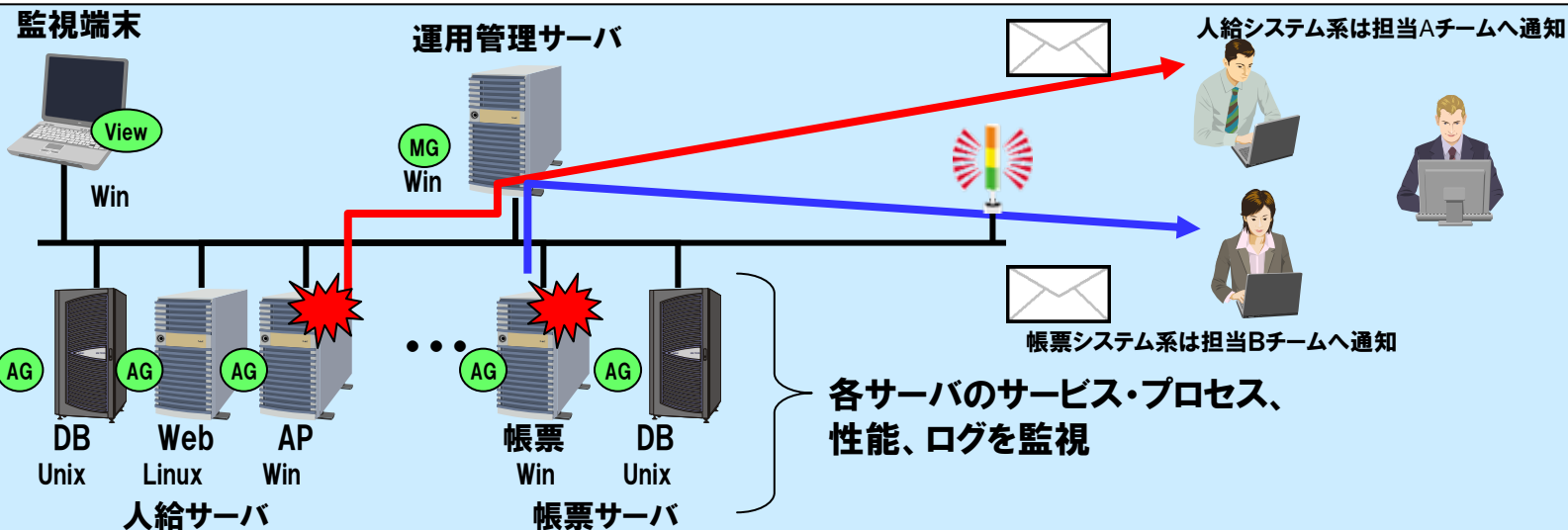
WebSAM System Navigatorでの解決例

監視+通報機能で解決

マルチベンダ対応可能(Windows、Linux (RedHat、Miracle)、UNIX(HP-UX、Solaris))

監視機能をAll in Oneで提供。設定もGUI操作で簡単に実施可能。

メッセージごとに通報先や手段を変更可能。



WebSAM System Navigatorの特長

簡単購入！

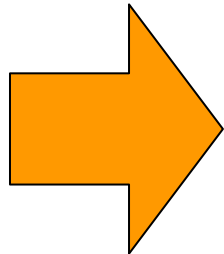
必要機能を一式提供
他のSWが不要な
オールインワン製品

簡単設定！

インストールが容易
GUIで監視設定でき
素早い運用が可能

簡単運用！

障害への一般的な対処
ノウハウを予め提供
運用しながらノウハウ蓄積
すぐに共有化できる



WebSAM System Navigatorは、
運用管理に必要な機能一式揃ったオールインワン製品
システムの効率的な運用管理を、シンプルに実現できます。

①簡単購入 統合監視に必要な機能をオールインワンで提供

統合管理に必要な機能を ALL in ONE で提供分かりやすい構成。複数製品の組み合わせが不要だからリソース消費も小さく、専用DBも不要！

ログ監視

OS、アプリケーションが出すログで危険、異常等を検知

プロセス・サービス監視

アプリケーションが異常終了した等の状態を検知

性能監視

CPUやメモリなどの性能異常を監視

メッセージ管理

システムのエラーメッセージや状態を一元管理

自動リカバリ

異常時にコマンド実行可

ナレッジ機能

異常時に対処方法をナビゲート

通報機能

異常時にメールやパトライトで管理者に通知可能

All in One

	マネージャー	エージェント	監視端末
推奨メモリ	100MB以上	50MB以上	100MB以上
推奨CPU	Intel PentiumIII 1GHz以上		

② 簡単設定 1つの画面でシンプルな操作性

1つ画面から監視の設定や、日々の運用監視ができるので操作がシンプル。
設定も専用のスクリプトは不要！

物理視点
サーバ単位の監視

ビジュアル監視

同じコンソールでモードを
変えれば監視設定も可能

The screenshot displays a complex monitoring interface with several key components:

- Left Panel (Tree View):** A hierarchical tree structure showing monitoring points for 'トポロジビュー' (Topology View) and 'ビジネスビュー' (Business View). The 'トポロジビュー' section includes MINE, PENTAGON, Windowsサービス監視, プロセス監視, 性能監視, LogicalDisk, Memory, and Processor. The 'ビジネスビュー' section includes OS (Windows2000), SQLServer, iStorage, 業務(在庫), 在庫管理, 生産管理, 業務(販売), and アプリケーションビュー.
- Center Panel (Map View):** A 3D map view titled 'トポロジビュー' showing server racks labeled 'MINE' and 'PENTAGON'.
- Right Panel (Performance Graph):** A line graph titled '性能監視 - Proc...' showing performance metrics over a 5-minute period. The Y-axis ranges from 0 to 100. A legend below the graph shows '重要度の色' (Priority Color), 'カラー' (Color), 'カウンタ' (Counter), and 'スケール' (Scale).

重要度の色	カラー	カウンタ	スケール	最
<input checked="" type="checkbox"/>	■	% Privileged Time	1.00000000	4.0
<input checked="" type="checkbox"/>	■	% Processor Time	1.00000000	6.0
- Bottom Panel (Event Console):** An event log table with columns for '重要度の色', '重要度', 'マーク', and 'メッセージ'. It shows several entries for 'PENTAGON' with various statuses like '正常' (Normal) and '異常' (Abnormal).

重要度の色	重要度	マーク	メッセージ
■	正常		PENTAGON 2005/07/04 11:06:21 SSDP Discovery Service サービ...
■	正常		PENTAGON 2005/07/04 11:06:21 SSDP Discovery Service サービ...
■	正常		PENTAGON 2005/07/04 11:06:21 SSDP Discovery Service サービ...
■	異常		PENTAGON 2005/07/04 11:06:21 SSDP Discovery Service サービ...
- Bottom Table (Summary):** A table showing event counts by category and severity.

カテゴリの件数	表示中の件数	異常	CRITICAL	MAJOR	MINOR	警告
異常		3	0	0	0	3
正常		69				
- Bottom Panel (Alerts):** A table showing alert details with columns for 'リカ/リ状態', '発生日', '発生時刻', 'サービス名', and '概要'.

リカ/リ状態	発生日	発生時刻	サービス名	概要
実行中	2005/07/04	17:16:58	BusinessView	ディスク空き容量不足

業務視点、業務単位で
グループ化して監視

イベントコンソール

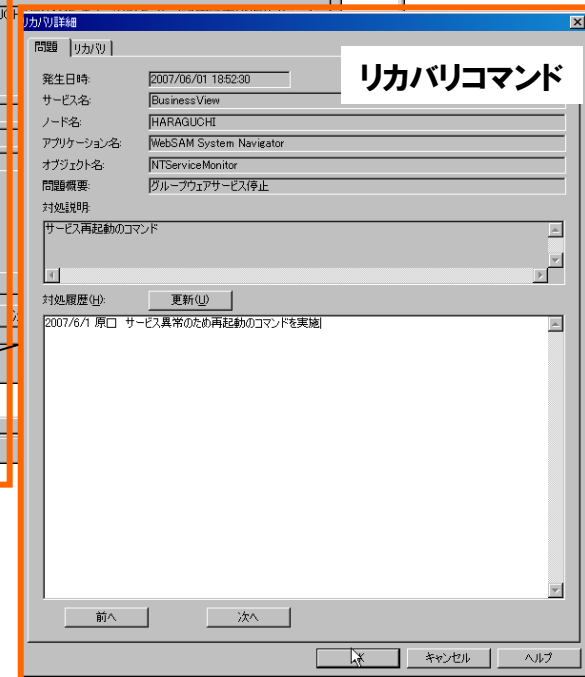
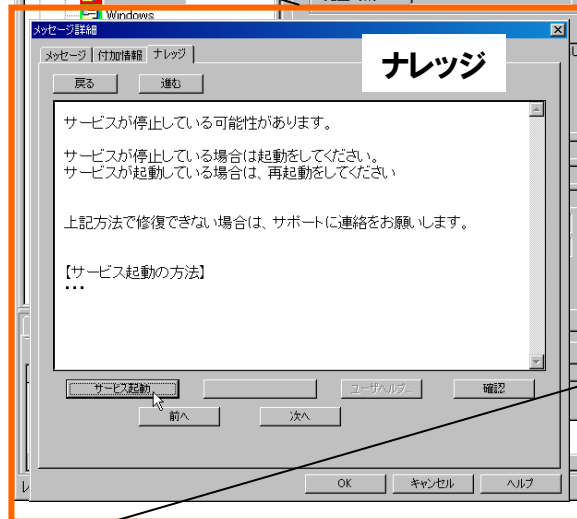
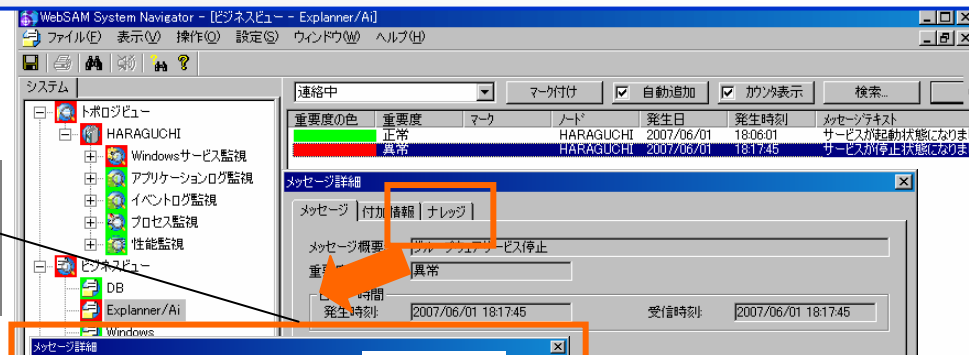
リソース監視

対処状況・通報状況

特長③ 簡単運用 対処方法をナビゲートする「ナレッジ」機能

- ・ナレッジを登録することによって、経験やスキルに依存しない高いレベルの運用を支援
- ・リカバリコマンドで簡易対策を自動化

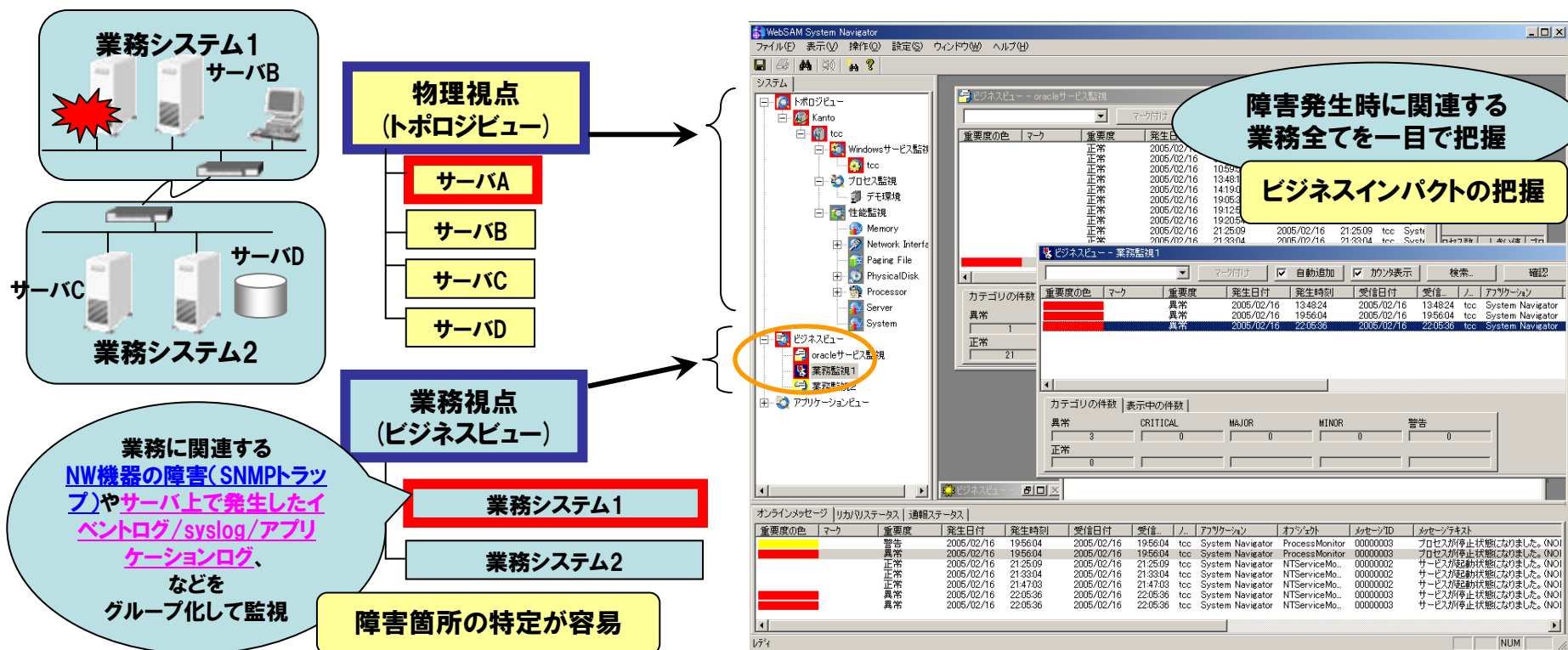
・ナレッジ機能で何が問題かだけでなく、どのように対処したら良いかをナビゲート
・設定もGUIから操作でき、即時に反映



リカバリコマンドの登録も可能で、自動/手動でコマンド発行ができます
(例: サービスの再起動、プロセスの起動ログの取得等)

特長③ 簡単運用 業務視点での監視で障害1次切り分けを効率化

システム別／重要度別／レイヤ別など運用にあわせて表示方法をカスタマイズでき、**物理視点**と**業務視点**の2つのビューで視覚的に効率よく障害を把握することができます。



WebSAM System Navigator導入効果

■ 統合運用管理 WebSAM System Navigator

- システム全体の稼動状況・障害情報を一元的に管理することで、システム状況を可視化や障害検知などシステム運用を効率化し、安定稼動を実現します。

■ WebSAM System Navigatorの導入効果

- 複数サーバ／アプリケーションの稼動状況を一元管理し運用を効率化
- 障害の未然防止
- 障害時の早期発見
- 業務視点による迅速な分析の支援
- ナレッジ機能による対処ノウハウの共有
- 性能情報の蓄積によるリソース傾向分析

■ WebSAM System Navigatorが監視できるアプリケーション例

- サービス・プロセスで動くアプリケーションの稼動状況
- イベントログ／syslogに吐かれるメッセージ
- テキスト形式のログ



WebSAM System Navigatorの機能一覧 (監視機能)

機能	機能概要	
標準機能	サービス監視	<ul style="list-style-type: none"> サービスの死活監視
	プロセス監視	<ul style="list-style-type: none"> プロセスの存在監視
	性能監視	<ul style="list-style-type: none"> 各サーバの稼働状況をグラフィカルに表示(CPU/メモリ使用率等) しきい値の超過を監視し、逐次/N回連続/N回平均の3つの判定によりオペレータに通知 稼働状況データを統計情報として蓄積、システムの問題点の分析および改善を支援
	OSメッセージ監視	<ul style="list-style-type: none"> OSメッセージを監視(Windows:イベントログ、UNIX/Linux:syslog) メッセージラッシュ対策として、エージェント側で同一メッセージ抑止が可能
	アプリケーションログ監視	<ul style="list-style-type: none"> アプリケーションが出力する任意のテキストログファイルから必要なログを抽出して、メッセージ監視 ログファイル内容の表示
	R3.0強化 ファイル・ディレクトリ監視	<ul style="list-style-type: none"> ファイル・ディレクトリの容量・更新を監視
クラスタ監視	<ul style="list-style-type: none"> CLUSTERPROと連携しフェールオーバーの発生、フェールオーバーグループの状態を監視 	
オプション	SNMPトラップ監視	<ul style="list-style-type: none"> ネットワーク機器が送信するSNMPトラップを監視
R3.0強化 アプリケーション監視	<ul style="list-style-type: none"> ソフトウェア固有のアラーム情報や性能情報を監視 <監視対象ソフトウェア> Oracle、PostgreSQL、MySQL 	

WebSAM System Navigatorの機能一覧 (管理機能)

機能	機能概要	
メッセージ管理	<ul style="list-style-type: none">・複数サーバのメッセージを一元管理・メッセージを業務などのカテゴリ毎に分類して表示することで、障害発生時に業務への影響範囲を即座に特定可能	
通報制御	<ul style="list-style-type: none">・メッセージ発生、監視プロセス/サービスの状態変化、リソースのしきい値超過契機で回転灯、電子メールでの通報が可能	
リカバリコマンド	<ul style="list-style-type: none">・メッセージ発生、監視プロセス/サービスの状態変化、リソースのしきい値超過契機でリカバリコマンドの自動/手動投入が可能	
ナレッジ制御	<ul style="list-style-type: none">・過去の対処履歴や製品ナレッジを参照して、適切な対処方法をナビゲート ※製品ナレッジ:OSやミドルウェアに関する対処方法や監視設定のナレッジ情報	
R3.0強化	オーディットログ管理	<ul style="list-style-type: none">・WebSAM System Navigator 上でのコマンド実行・設定変更履歴を記録
R3.1強化	メッセージ監視ON/OFF	<ul style="list-style-type: none">・マネージャ側の監視のON/OFFをすることが出来る。

標準機能

製品に関するお問合せ先

WebSAM System NavigatorおよびWebSAM製品全般に関する問合せは
下記連絡先へご連絡ください。

■お問合せ先

NEC ITプラットフォーム販売推進本部
プラットフォームコンタクトセンター ソフトウェアサポートグループ
TEL:03(3798)7177 FAX:03(3798)8414
E-mail: contact@soft.jp.nec.com

■製品紹介サイト

WebSAM System Navigator

<http://www.nec.co.jp/middle/WebSAM/products/sysnavi/index.html>

Empowered by Innovation

NEC