



Hinemos

運用アナリティクスを実現！
最新Hinemos ver.6.1の全体像

2018年4月11日
NTTデータ先端技術株式会社
眞野 将徳

- 
1. Hinemosとは
 2. 最新Hinemos ver.6.1で実現する
運用アナリティクス
 3. Hinemosの3大基本機能
収集・蓄積
 4. Hinemosの3大基本機能
監視・性能
 5. Hinemosの3大基本機能
自動化
 6. 統合運用管理のための共通基本機能
 7. Hinemosの動作環境
 8. まとめ



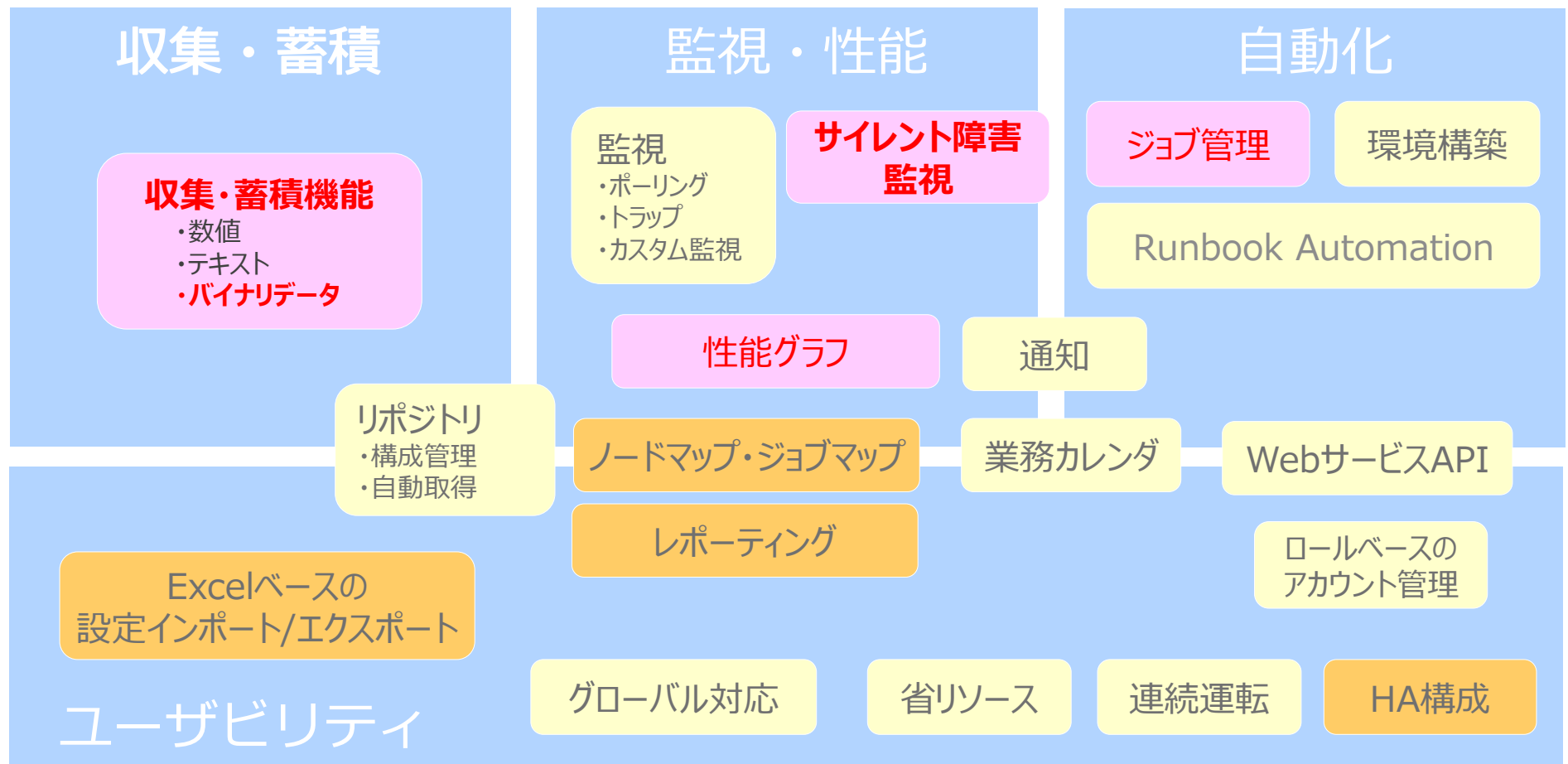
エンタープライズシステム運用管理に必要な幅広い機能を備えた
統合運用管理ソフトウェア

自動化

監視・性能

収集・蓄積

Hinemos ver.6.1の全体像



これらの機能が**ワンパッケージ**

- ・ デジタルデータ収集に専用の製品は不要
- ・ 収集データの統計値や相関による高度な監視を基本機能で提供

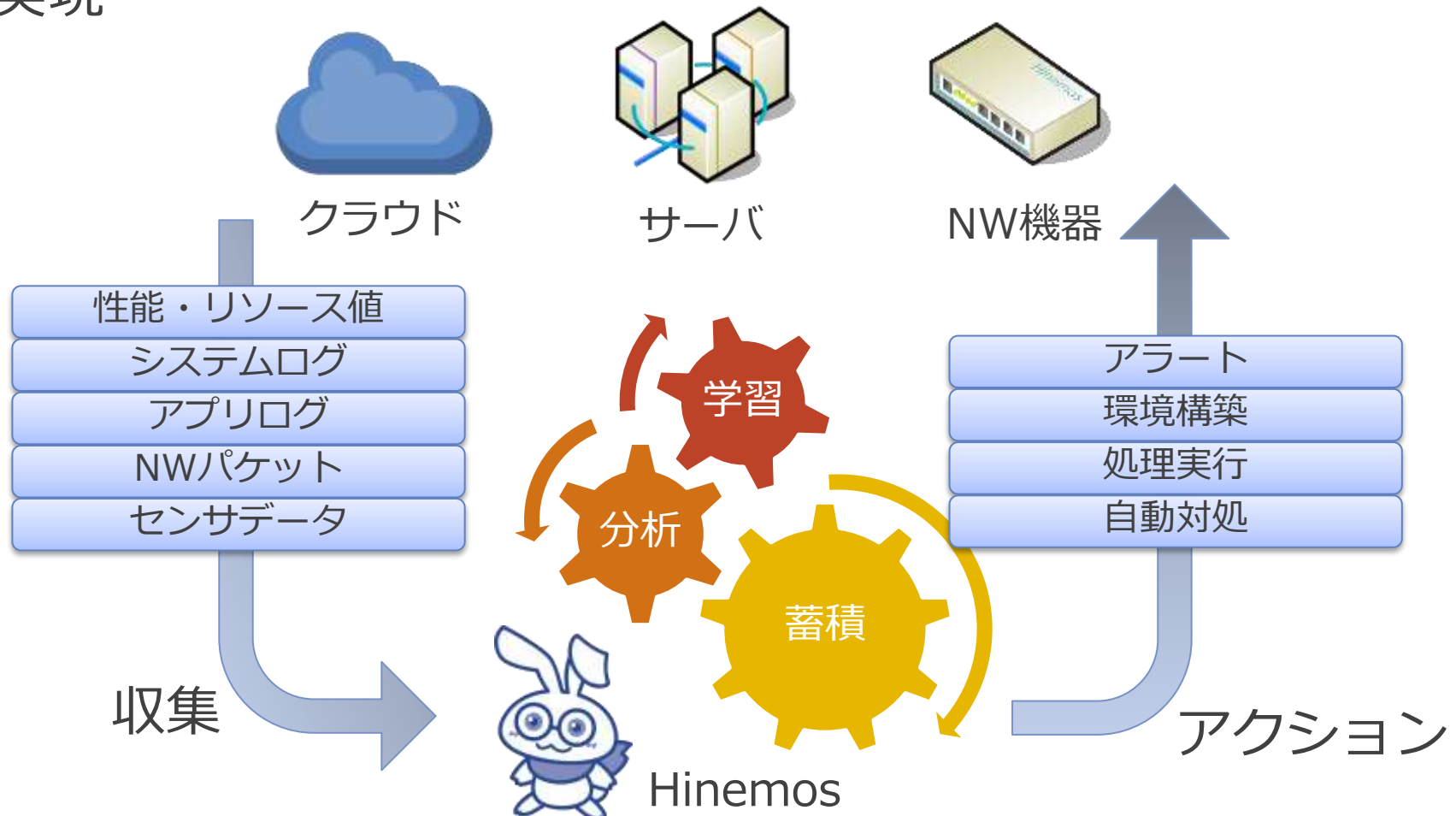
Ver.6.1強化機能

サブスクリプション提供機能

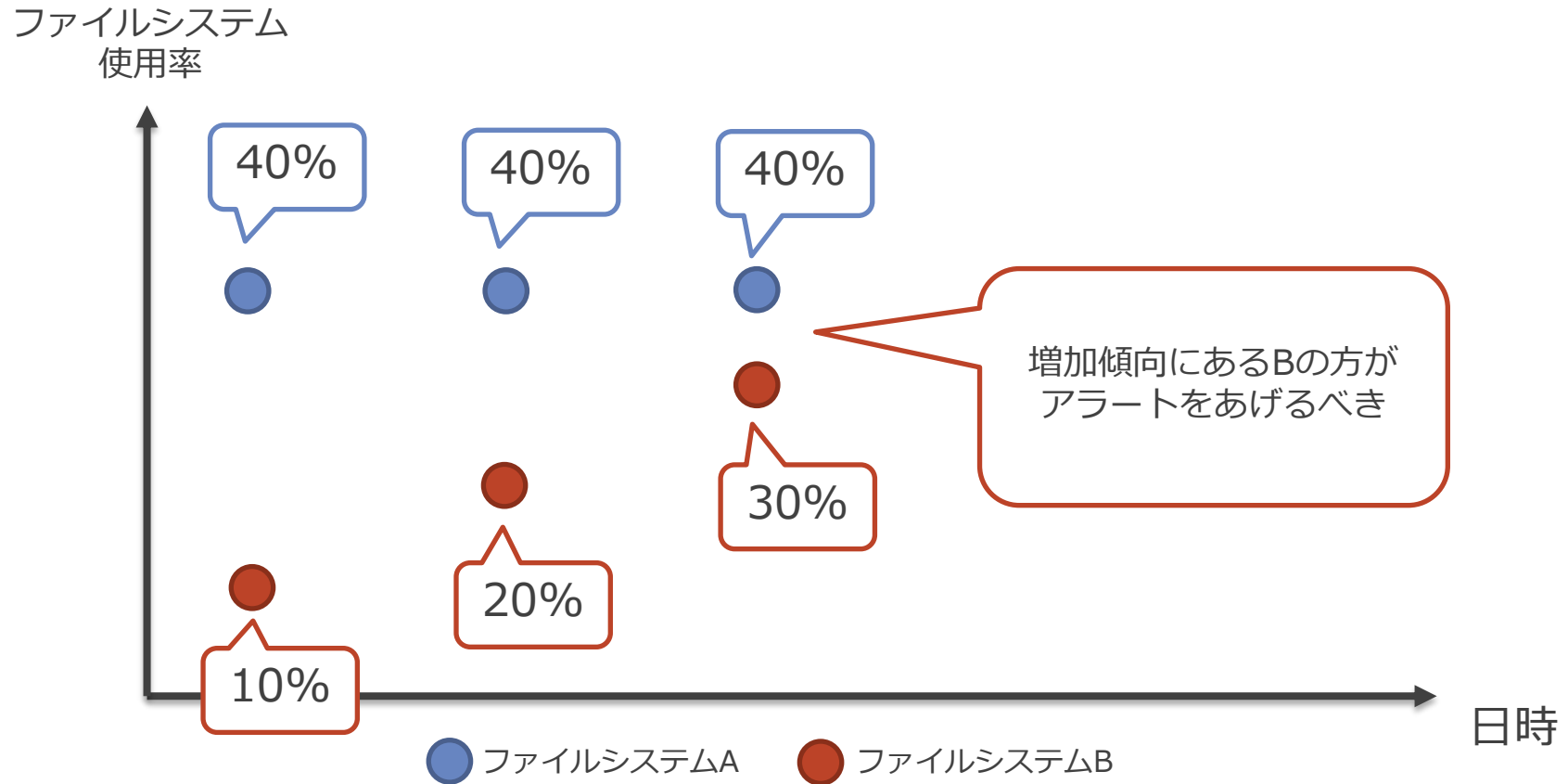
最新Hinemos ver.6.1で実現する 運用アナリティクス

運用アナリティクスとは

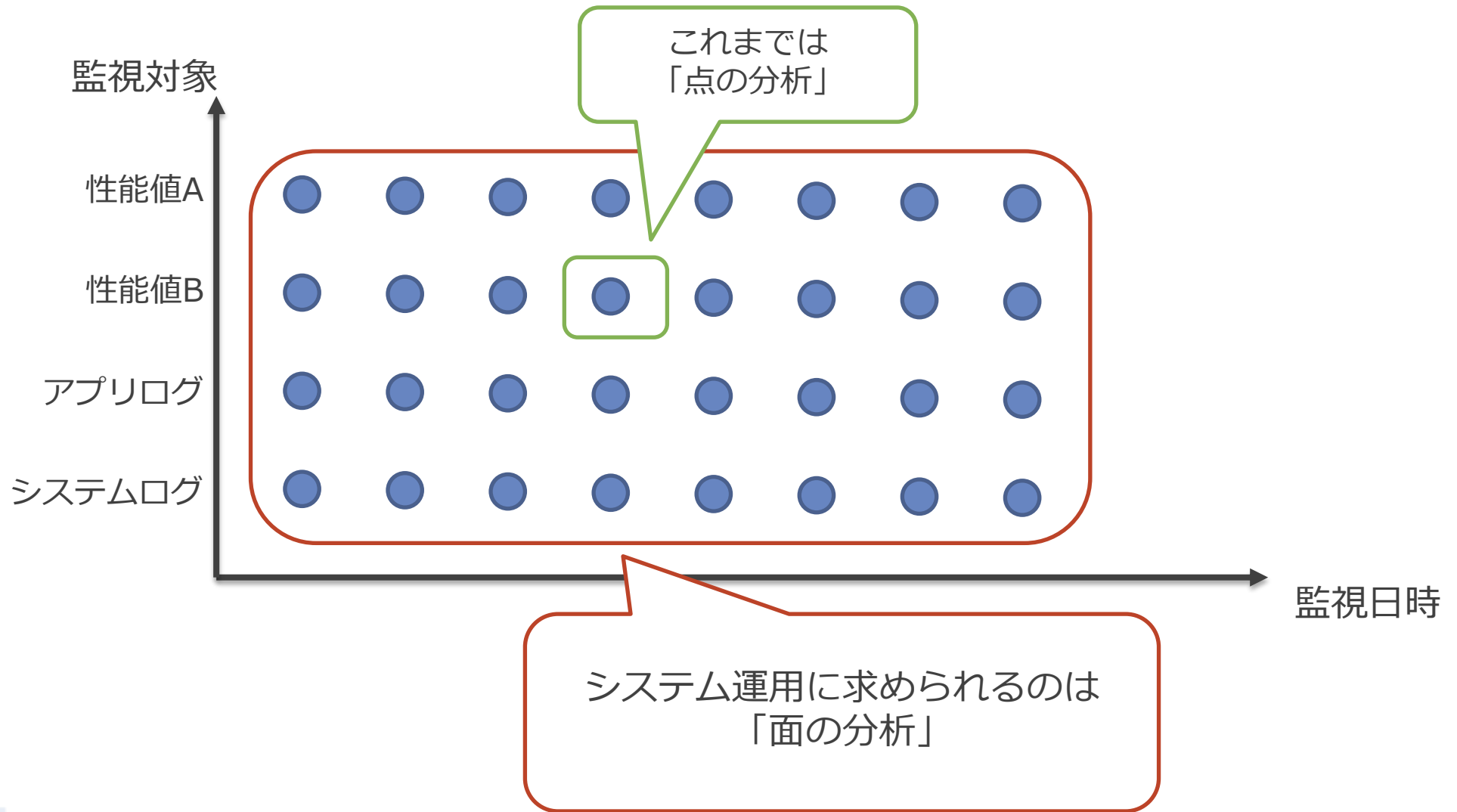
Hinemosが収集・蓄積したデータをもとに
リアルタイムなシステム状態把握と未来を予見した予防保全
を実現



運用アナリティクスとは



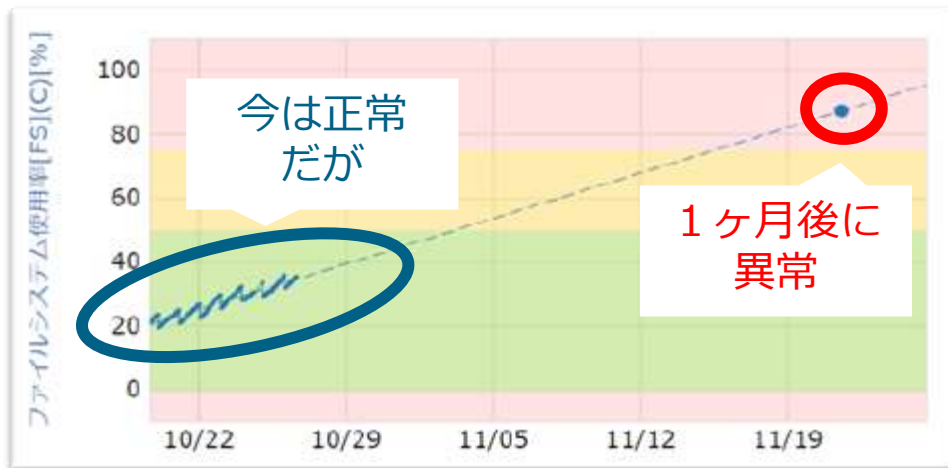
運用アナリティクスとは



Hinemos ver6.1新機能① 将来予想値や変化量を監視

これまで収集したデータを元に未来の異常をいち早く検知

将来予測監視



リソース枯渇はアラートが出てからだと手遅れです。
変化の多い環境でも、Hinemosが将来を予測し、いち早く対策を打てます。

変化監視



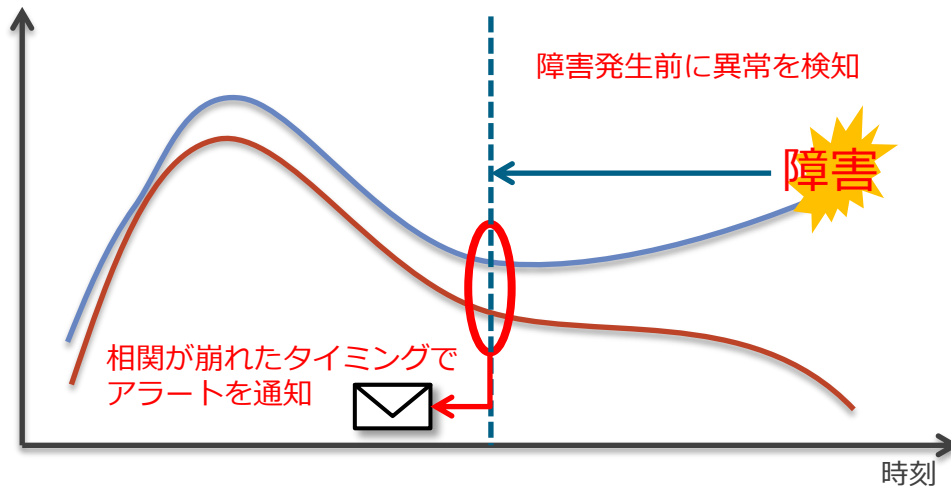
閾値内の変動でも普段と違う動きは異常の前触れかもしれません。
次の動きを予測し監視をすることで、いち早く異常の傾向を察知できます

※ボリンジャー・バンドアルゴリズムを採用

Hinemos ver6.1新機能② 相関や条件組み合わせで監視

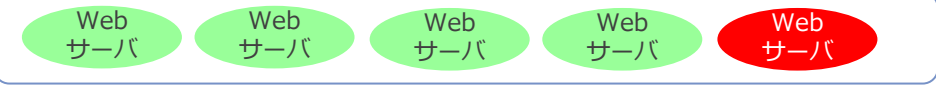
複数のデータの関係性から分かる異常をいち早く正確に検知

相関係数分析

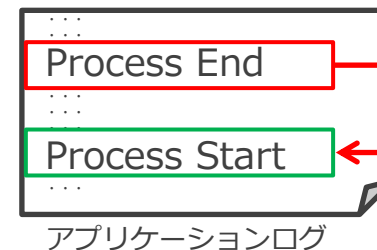


あるデータの異常は、他のデータとの関係性から気づけることがあります。相関係数を使って、関係性の崩れから将来的な異常をいち早く察知できます。

収集値統合監視



一台の障害は**警告**レベル
全台の障害は**危険**レベル



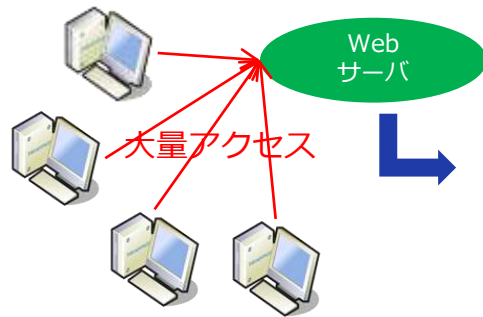
プロセスが停止しても
時間内に再起動すれば
正常レベル

1つのデータでは、重要度を正しく表現することが出来ない場合があります。複数のデータを組み合わせた監視により障害のレベルを正確に把握できます。

Hinemos ver6.1新機能③ ログ件数・メタ情報からの監視

ログメッセージのメタ情報を活用し異常を察知

ログ件数からの監視①



一定時間内に閾値を超えるログメッセージが出力されるとアラートを上げることが可能

```
...
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
192.168.0.101 [12/May/2014:20:41:48] "GET /index.html HTTP/1.1~
...
```

アクセスログ

メッセージは正しくても
短時間に大量出力等の
異常な状態の可能性も検出

ログ件数からの監視②

ログ件数をカウントする際に、メタ情報を活用することで、簡易にターゲットメッセージを指定することが可能

■ (例) /var/log/secureからsrc_ipaddress毎のログイン失敗件数をカウント

Sep 27 13:57:18 webserver sshd[13666]: Invalid user admin from 198.51.100.101 port 3100

src_ipaddress=198.51.100.101

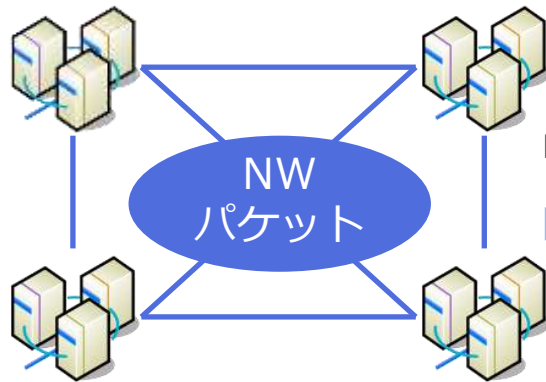
ログフォーマットにて
メタ情報を抽出し
検索・カウントで利用可



Hinemos ver6.1新機能④ NWパケット・バイナリ対応

NWパケットもバイナリファイルも収集・監視そして活用へ

ネットワークパケット監視



HinemosさえあればNWパケットも簡単収集・監視でき
使い慣れたツールで分析・解析が可能に

Hinemosエージェントが
収集・監視

Hinemosクライアントから
簡単取得

Hinemos

管理
DB



バイナリファイル監視

追記型のバイナリファイルも定期・不定期に出力される
バイナリファイルもテキストファイル同様に管理可能に

Java
アプリケーション

ミドルウェア

クラッシュ時に
ヒープダンプを出力

定期的にバイナリ形式
のログ出力

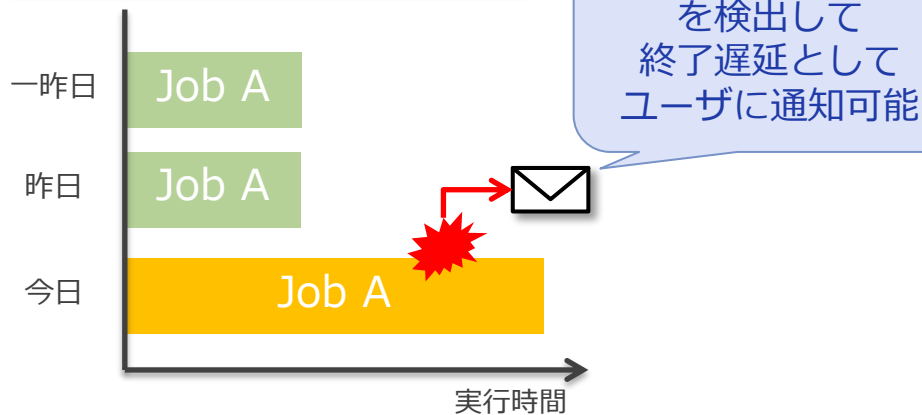
Hinemosエージェントがあれば
バイナリファイルも
簡単に収集・監視、活用が可能

Hinemos

管理
DB

Hinemos ver6.1新機能⑤ ジョブの機能強化・拡張

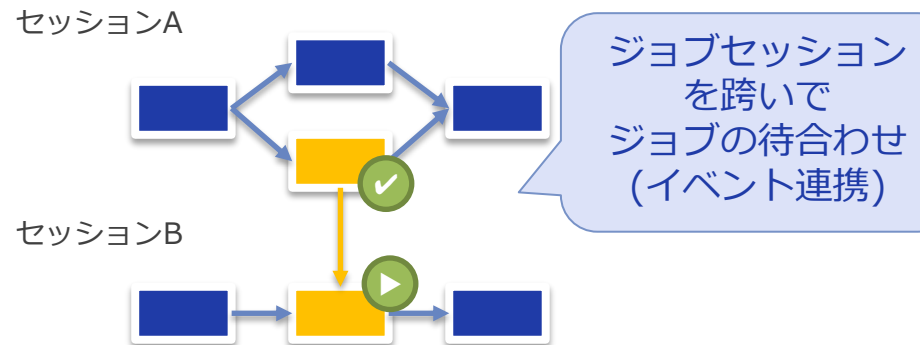
実行時間予測による 終了遅延検知



ジョブの実行の 優先度指定



セッションを跨いだ イベント連携



その他の強化・改善

- ・ 条件指定の繰り返し実行
- ・ 実行時間のグラフ表示
- ・ ジョブネット/ジョブ単位の定義インポート・エクスポート対応
- ・ 実行間隔の拡張(1分/2分/3分の追加)

監視機能

ポーリング型の監視の間隔の拡張（30秒間隔を追加）

環境構築機能

環境構築設定の参照呼び出しの追加

環境構築変数を導入

実行コマンド/チェックコマンド/モジュール実行時のログイン情報
モジュールの実行結果の格納に利用可能

モジュール実行結果により後続モジュールの制御の追加

チェックコマンド省略時の動作指定の追加

デモ

デモ内容

デモ 1 <https://www.youtube.com/watch?v=jtWjqmcNlw4>



攻撃者

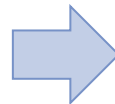


Webサーバ

セキュリティホールがないか攻撃
→404が多発



検知！



実際のパケットを調査

デモ 2 <https://www.youtube.com/watch?v=pj46QbXGfBw>

ファイルシステム使用率の傾向を監視
将来的なリソース枯渇を対処可能なうちに検知

Hinemosの3大基本機能

収集・蓄積

収集・蓄積機能

■ ありとあらゆるデータを収集・蓄積してビックデータ分析に活用

収集・蓄積

サーバ機器、端末、OS、MW、APなどのありとあらゆるデータを収集
収集するメッセージのタグ抽出や解釈の機能を拡張
外部のビックデータ基盤、機械学習・AI基盤に転送する機能を提供

数値・文字列・バイナリデータや、端末情報やHinemosの実行履歴までありとあらゆる情報を収集可能

数値データ

PING応答時間
プロセス数
Web応答時間
各種リソース情報
各種サービスの応答時間
各種ポートの応答時間
SNMPレスポンス
SQLレスポンス
JMXレスポンス
ログ件数
相関係数
コマンド実行結果
JSONメッセージ

文字列データ

ログファイル
syslog
Windowsイベント
Webレスポンス
SNMPレスポンス
SNMPTRAP
SQLレスポンス
コマンド実行結果
JSONメッセージ

バイナリデータ

バイナリファイル
NWキャプチャ

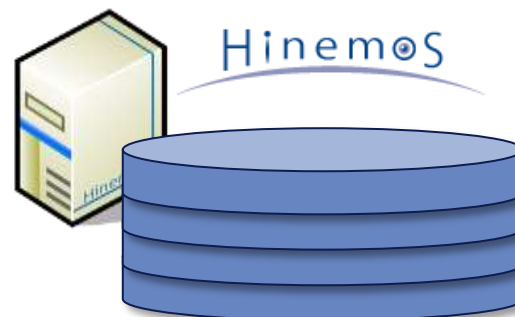
その他端末データ

Android端末情報
(GPS、バッテリー残量、ビーコン)

Hinemos実行履歴

イベント履歴

ジョブ実行履歴



ログの特性にあわせて分割、タグ付けで検索を用意に

ログ複数行対応

主にファイルログのようなログの区切りがアプリケーション・ミドルウェアによって異なる場合に、どこからどこまでが「1つのログ」かを識別します。

■ Javaスタックトレース

```
java.lang.NumberFormatException: For input string: "1.1"
    at java.lang.NumberFormatException.forInputString(Unknown Source)
    at java.lang.Integer.parseInt(Unknown Source)
    at java.lang.Integer.<init>(Unknown Source)
    at ExceptionPrintDemo.formatInt(ExceptionPrintDemo.java:7)
    at ExceptionPrintDemo.main(ExceptionPrintDemo.java:14)
```

■ Oracleアラートログ

```
Sat Feb 07 12:35:53 2015
create tablespace TEST_SPACE datafile size 5m autoextend on
Completed: create tablespace TEST_SPACE datafile size 5m autoextend on
Sat Feb 07 12:38:40 2015
alter database datafile
'/u01/app/oracle/oradata/CDB122/0/datafile/o1_mf_test_spa_bfc20s53_.dbf'
resize 8m
```

- ・先頭パターン
- ・終端パターン
- ・区切り文字

■ Linuxシステムログ

```
Jun 29 17:38:11 Tiger shutdown[30243]: shutting down for system halt
```

ログフォーマットによるタグ抽出

規則性のあるログメッセージの内容をタグとしてメタ情報（キー・バリュー）を定義し抽出することができます。

■ Apacheアクセスログ

198.51.100.101 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif HTTP/1.0" 200 2326

先頭は
送信元IP

[]内は
日付情報

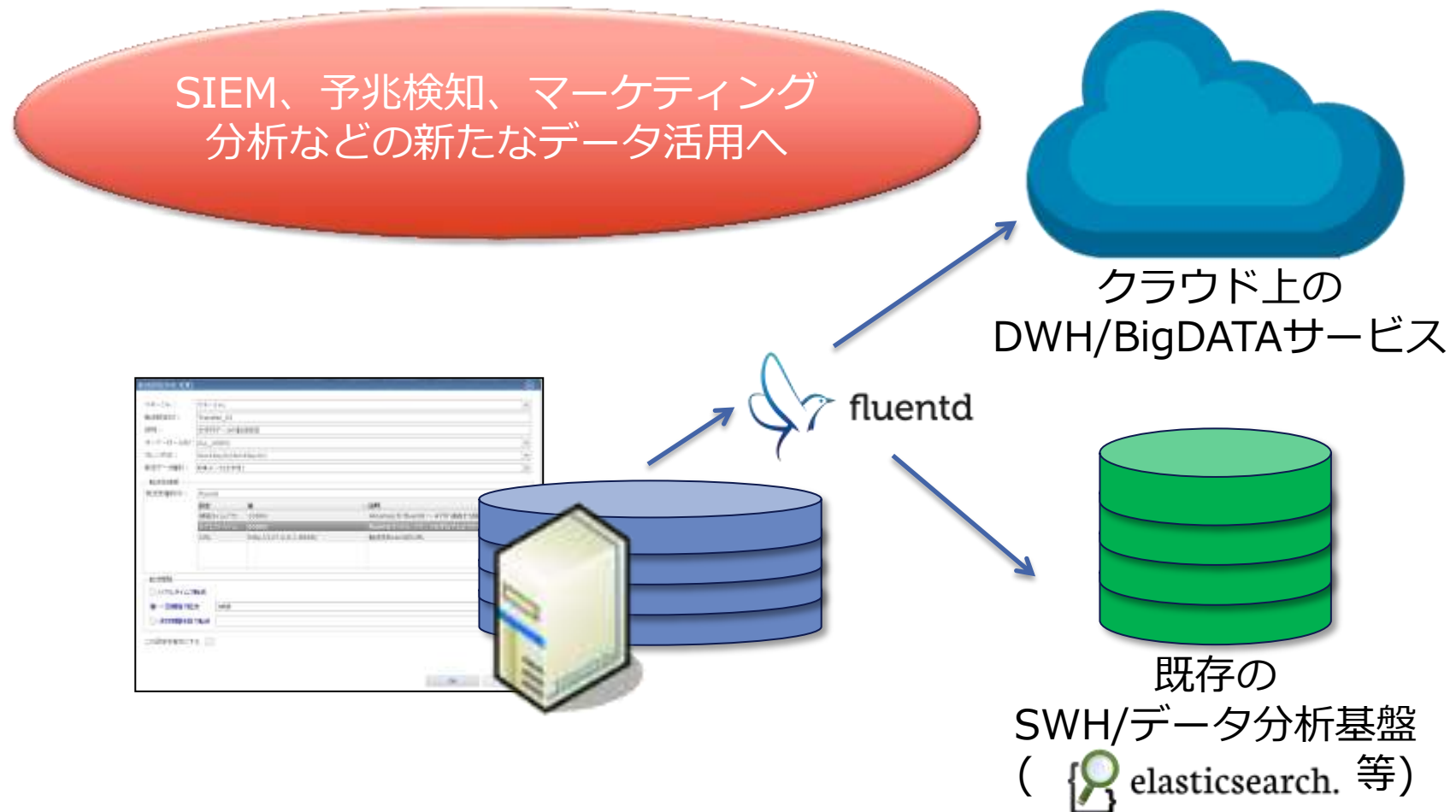


規則性からタグ抽出

キー	値
src_ipaddress	<u>198.51.100.101</u>
date	<u>10/Oct/2000:13:55:36 -0700</u>
method	<u>GET</u>
status_code	<u>200</u>
send_byte	<u>2326</u>

収集・蓄積 データ分析基盤への転送

収集データを転送しSWH/ビックデータ分析基盤へ連携可能



Hinemosの3大基本機能

監視・性能

■ システムの稼働状況を確認し、見える化と傾向分析を実現

監視

システムの稼働状況を確認するための**22種類の監視機能**を提供
複雑な作り込みは不要のため**GUI操作だけ**で監視を開始可能
ユーザによる**監視のカスタマイズ**（スクリプト・コマンド連携）も可能

性能

監視結果や収集したデータを**性能グラフ**として表示
グラフ上から**閾値（正常・警告・危険）**のフィードバックが可能
蓄積データによる未来予測・変化量を使い「**過去**」から「**未来**」まで見える化

多種多様な監視をGUIから簡単設定・簡単実行

監視項目	概要
PING監視	対象機器へのping応答の有無により死活状態を監視します。
プロセス監視	起動しているプロセス数から状態を監視します。
リソース監視	対象機器のリソース情報を取得してその状態を監視します。
サービス・ポート監視	特定のサービス・ポートについて、応答有無や応答時間から状態を監視します。
Windows サービス監視	Windows サービスの状態を監視します。
Windowsイベント監視	Windowsイベントログに出力されたメッセージを監視します。
Hinemosエージェント監視	Hinemos エージェントの死活状態を監視します。
HTTP監視	Webサーバの応答有無や応答時間、レスポンスの内容から状態を監視します。
HTTPシナリオ監視	複数のURLへ順にアクセスし、想定されるアクセスが可能であることを監視
SNMP監視	汎用的なプロトコルSNMPの応答の内容を監視します。
SNMPTRAP監視	対象機器からSNMPTRAPを受信することで、対象機器の状態を把握します。

監視項目	概要
SQL監視	DBサーバの応答有無や応答時間、SQLレスポンスの内容から状態を監視します。
JMX監視	Javaアプリケーションのヒープメモリサイズ等の状態を監視します。
ログファイル監視	特定のログファイルに出力されたメッセージを監視します。
システムログ監視	各種OSのシステムログに出力されたメッセージを監視します。
ログ件数監視	指定のメッセージを含むログの一定期間の出力量を閾値監視をします。
相関係数監視	2値の相関係数に対して閾値監視をします。
収集値統合監視	指定した複数の条件を満たすか否かを監視します。
バイナリファイル監視	バイナリファイルを監視します。
パケットキャプチャ監視	パケットキャプチャを監視します。
カスタム監視	ユーザ定義のコマンド/スクリプトの実行結果(数値・文字列)を監視します。
カスタムトラップ監視	json形式でHinemosマネージャに送信された情報(数値・文字列)を監視します。

監視機能 エージェントレスで利用可能な監視機能

多くの監視機能は、**エージェントレスで利用可能**

エージェントレスで利用できる監視機能

※ログ件数監視、相関係数監視、収集値統合監視は他の監視設定を入力とする監視のため、本分類には登場しません。

監視機能(Linux)		監視項目(Windows)	
Ping監視	プロセス監視	Ping監視	プロセス監視
リソース監視	サービス・ポート監視	リソース監視(※1)	サービス・ポート監視
SNMP監視	JMX監視	SNMP監視	JMX監視
HTTP監視	HTTPシナリオ監視	HTTP監視	HTTPシナリオ監視
SQL監視	SNMPTRAP監視	SQL監視	SNMPTRAP監視
システムログ監視	カスタムトラップ監視	Windowsサービス監視	カスタムトラップ監視

(※1) エージェントレスの場合、取得項目に一部制限あり

エージェントの導入が必要な監視機能

監視機能(Linux)		監視項目(Windows)	
Hinemosエージェント監視	ログファイル監視	Hinemosエージェント監視	ログファイル監視
バイナリファイル監視	パケットキャプチャ	バイナリファイル監視	パケットキャプチャ
カスタム監視(※2)		Windowsイベント監視	カスタム監視(※2)

(※2) 監視対象以外の代理サーバ上のエージェントを利用可能

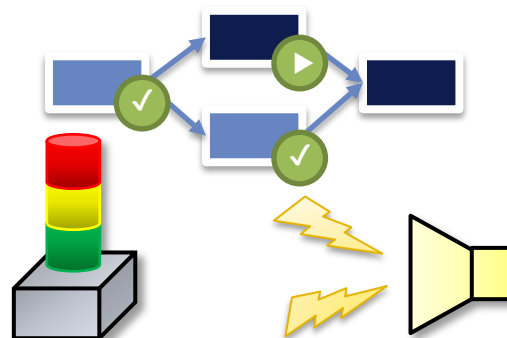
監視機能 監視結果の通知

Hinemosの各機能は、**実行結果を様々な形で通知可能**

監視コンソールで
視覚的に通知



監視結果に連動して
処理実行



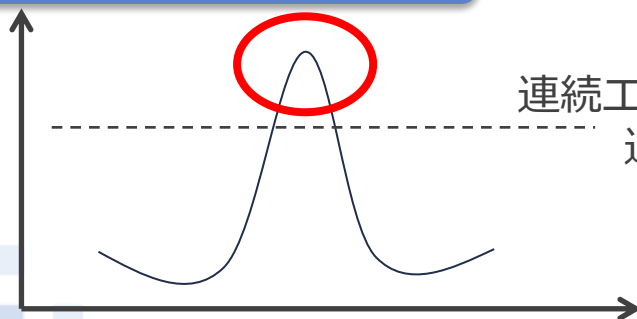
監視結果を
外部に通知



syslog

瞬間的な異常やメッセージラッシュを抑制し**本当の問題のみ通知**

瞬間的な異常



連続エラーで無ければ
通知しない

メッセージラッシュ

INFO service start
ERROR diskio /hoge
ERROR diskio /hoge
ERROR diskio /hoge
ERROR diskio /hoge
ERROR diskio /hoge

初回通知後は一定時間は
通知しない

性能グラフ機能 機能概要

システムの「過去」から「未来」までの見える化を実現可能

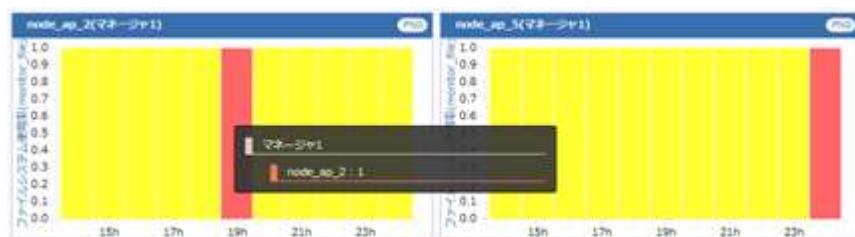


積み上げ面グラフ



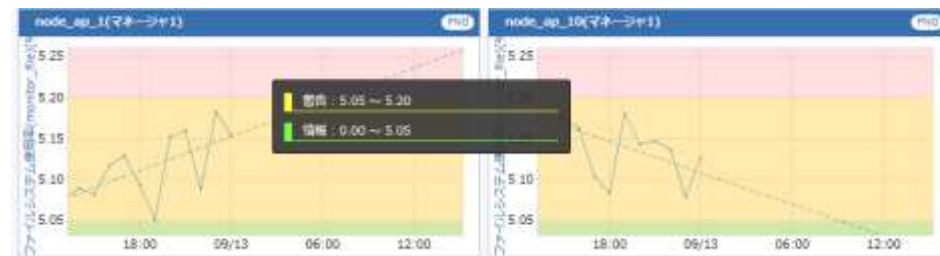
散布図・相関係数

例. CPU使用率とHTTPのレスポンスタイムの相関



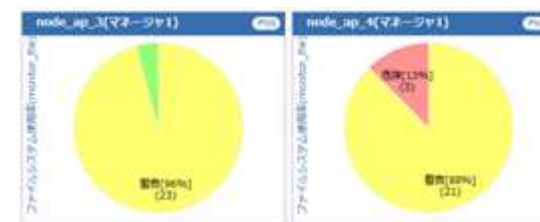
期間表示

例. 特定の期間の情報・警告・危険イベント



折れ線グラフ

Hinemosクライアント上で
システムの傾向分析を
効率的に行えます。

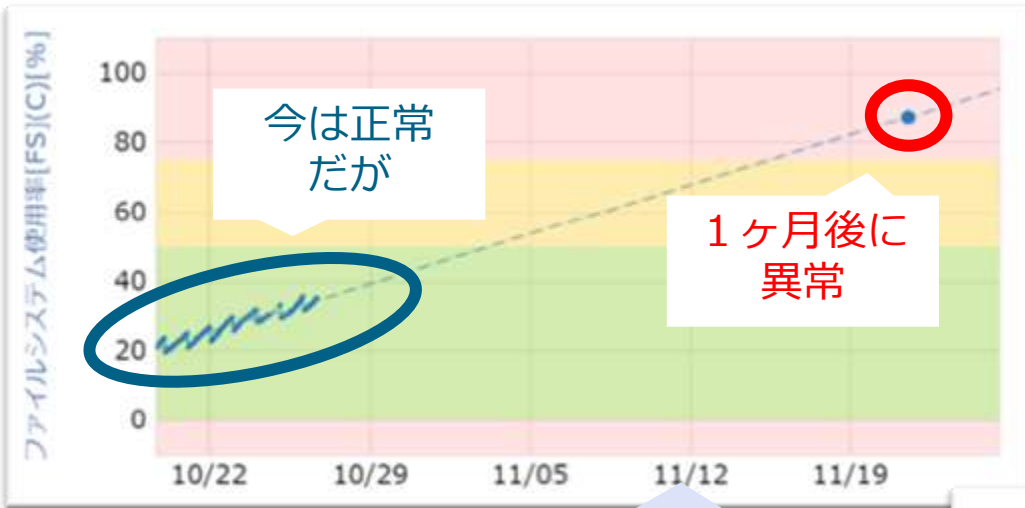


円グラフ

例. 特定の期間で情報・警告・危険イベント

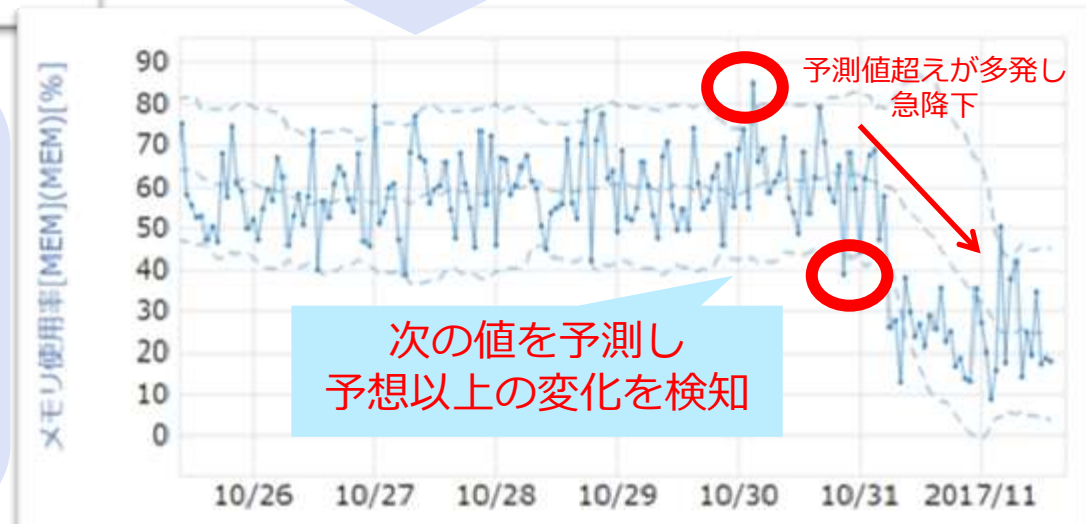
性能グラフ機能 将来予測と変化量によるグラフ表示

収集したデータを元に将来予測値や変化量からの分析が可能



普段の傾向との差を
視覚的に確認

将来的な異常を
視覚的に確認



Hinemosの3大基本機能

自動化

自動化機能

■ 環境構築から業務処理、オペレータによる運用までを自動化

構築自動化 (環境構築)

サーバ環境構築のセットアップといった一連の作業を定型化
複数環境に対しても一括で環境構築
設定ファイルの配布・置換といった定型操作も簡単に設定

業務自動化 (ジョブ管理)

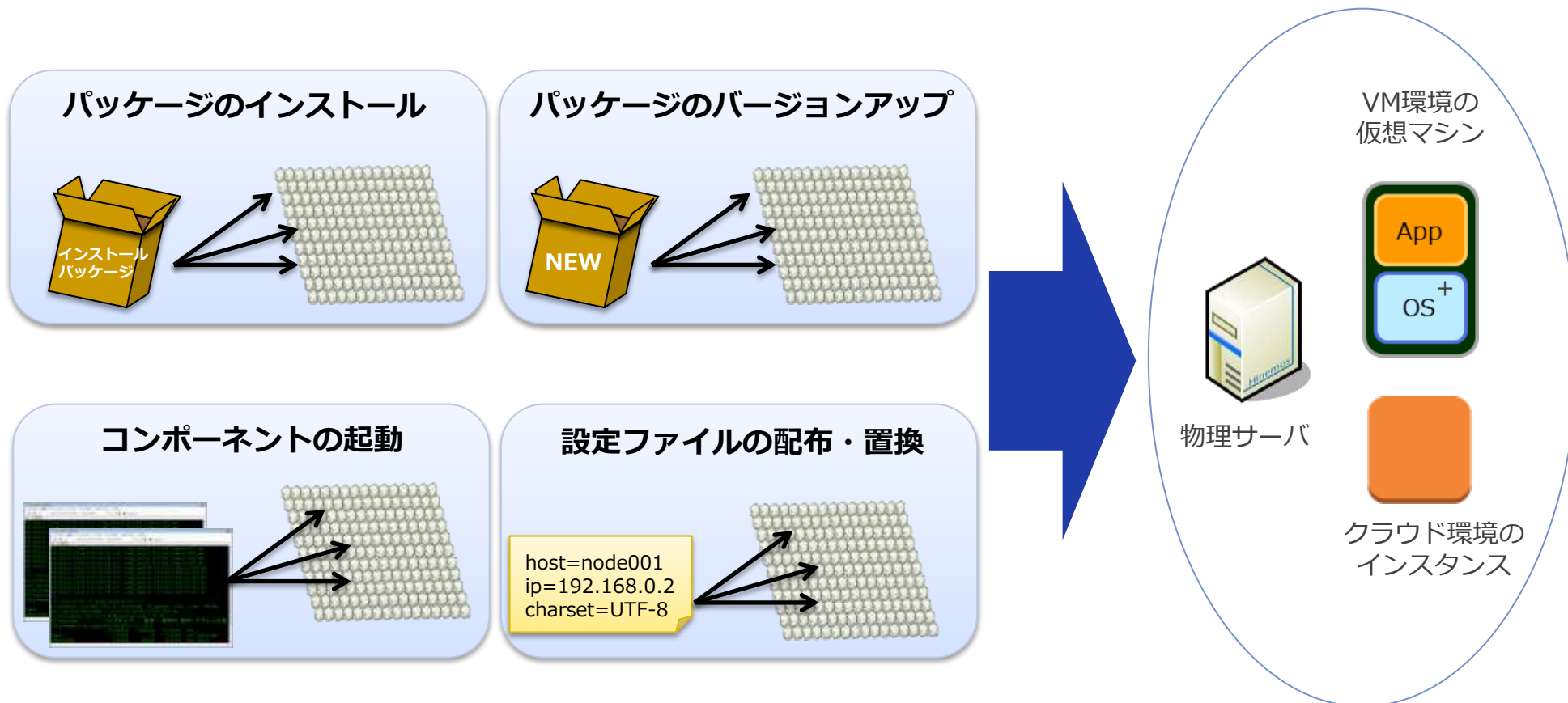
サーバ間を跨る処理フロー（ジョブネット）を一元管理
即時実行・スケジュール起動・他システム連動など様々な起動契機に対応
48時間カレンダー対応し運用時刻変更による特異日試験など運行管理に必要な機能を提供

運用自動化 (Runbook Automation)

運用手順書(Runbook)の自動化(Automation)を支援
人が行う確認・判断作業から障害確認まで簡単に設定可能
ジョブ管理と同一インタフェースで提供

構築自動化 環境構築機能概要

OS上の定型的な初期構築・環境変更の作業を定型化・一括実行



頻繁なOS初期セットアップや定期的なバージョンアップ作業等を効率的に実現します。

構築自動化 環境構築機能 特長

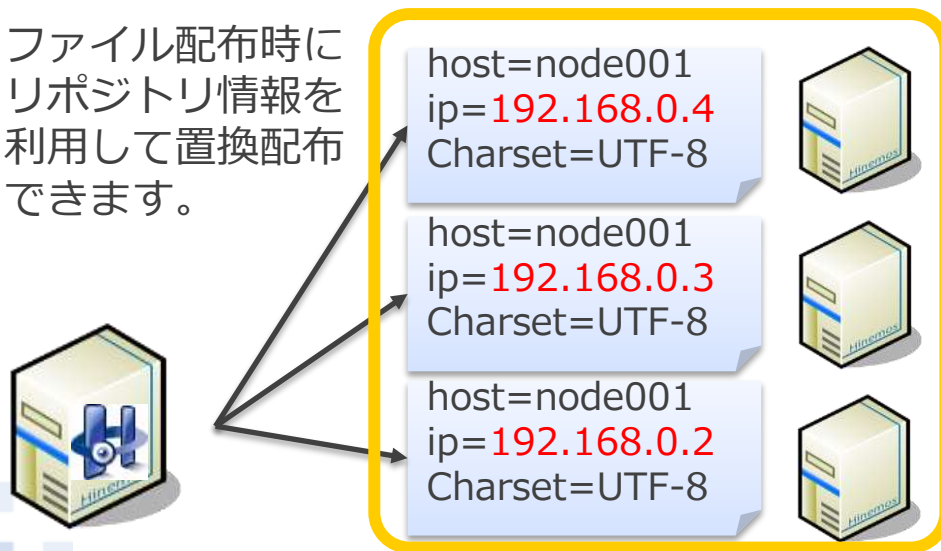
エージェントレス

Hinemosエージェントは導入不要です。Hinemosエージェントのインストールも本機能で実現できます。



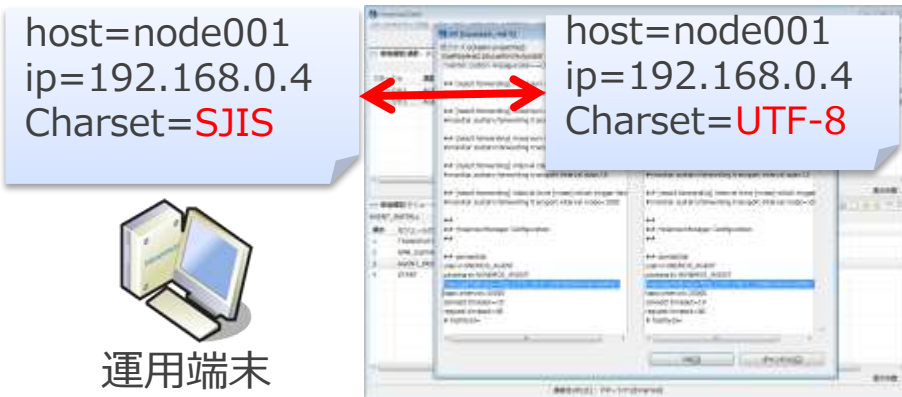
置換配布

ファイル配布時にリポジトリ情報を利用して置換配布できます。



差分確認

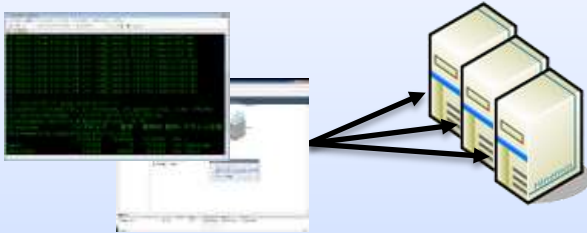
ファイル配布時に既存ファイルとの差分を確認できます。



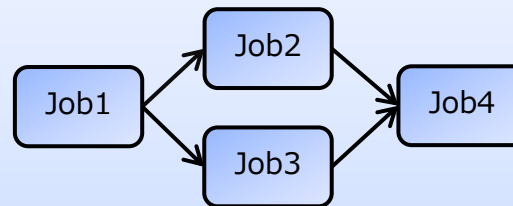
業務自動化 ジョブ管理機能

複数のサーバを跨る一連の処理フロー（ジョブネット）を一元管理

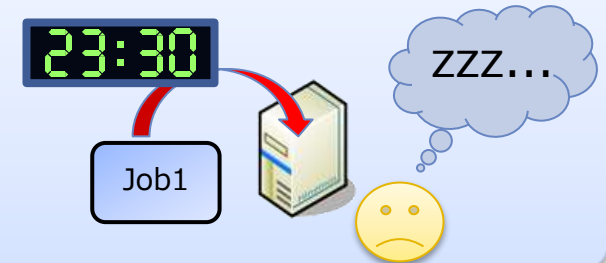
業務・ミドルウェア処理



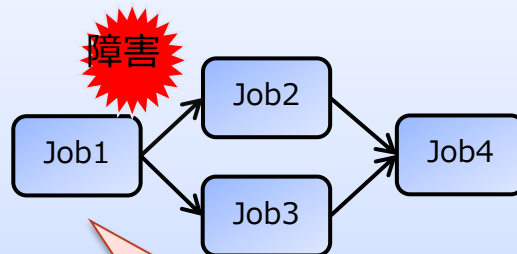
連続・複雑な操作



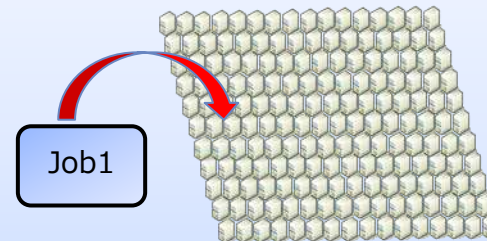
定時処理/深夜処理



処理結果の確認



大量ノードへの一括実行



HinemoS

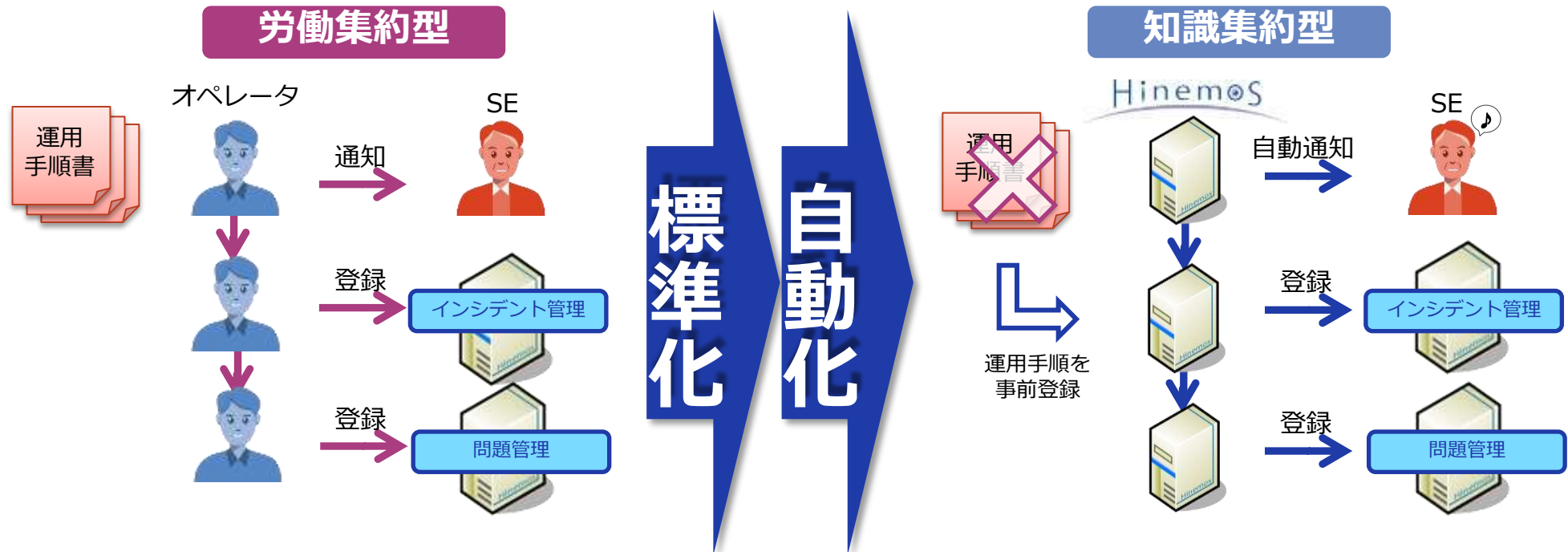


ジョブの
一元管理

- ・システム運行に必要な処理(ジョブ)の管理
- ・システム異常発生時に必要な処理(ジョブ)の管理

運用自動化 運用手順書(Runbook)の自動化(Automation)

Hinemosに手順書を登録することで運用自動化を実現



運用オペレータ作業の課題

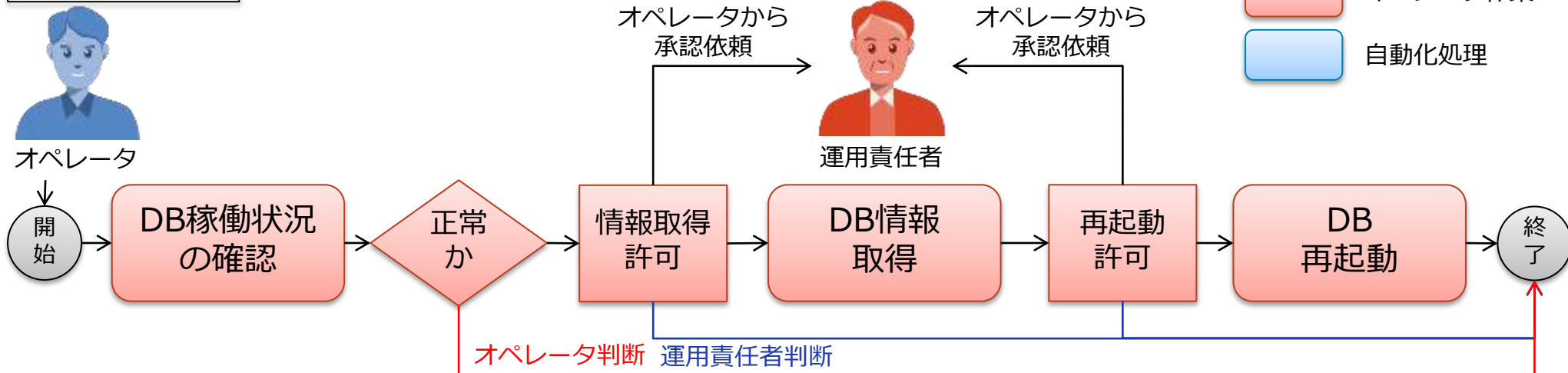
- ・ オペレーションが属人化
- ・ 要員による作業品質差
- ・ 複数の管理ツールを組み合わせ
- ・ 運用プロセス・運用ポリシーがバラバラ

Hinemos適用による自動化

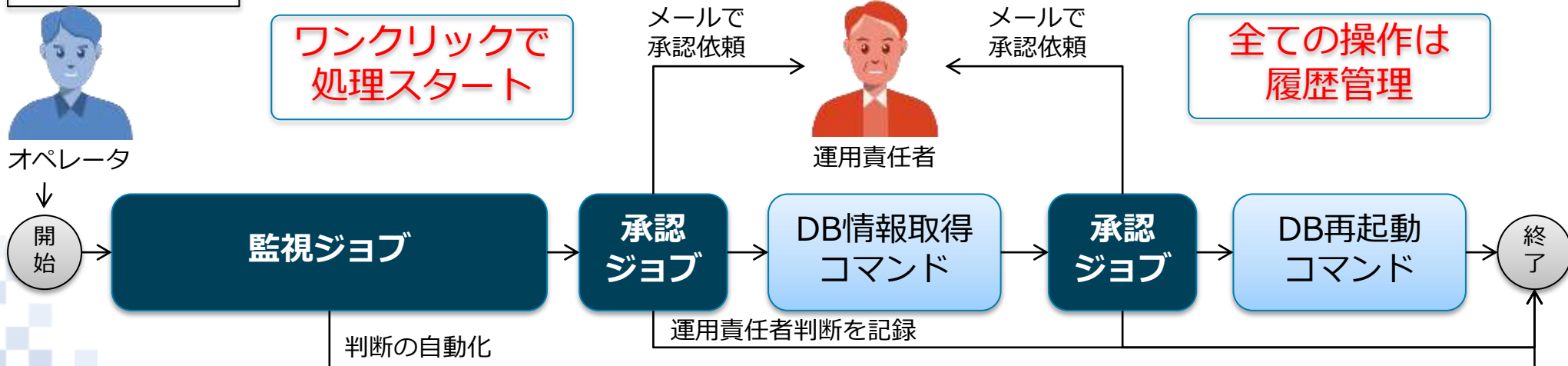
- ・ オペレーションを自動化
- ・ 自動化による品質均一
- ・ 管理ツール間のフローを連携
- ・ 運用プロセス・運用ポリシーを統一

運用自動化 ユースケース DB障害時の運用手順

手順書ベース



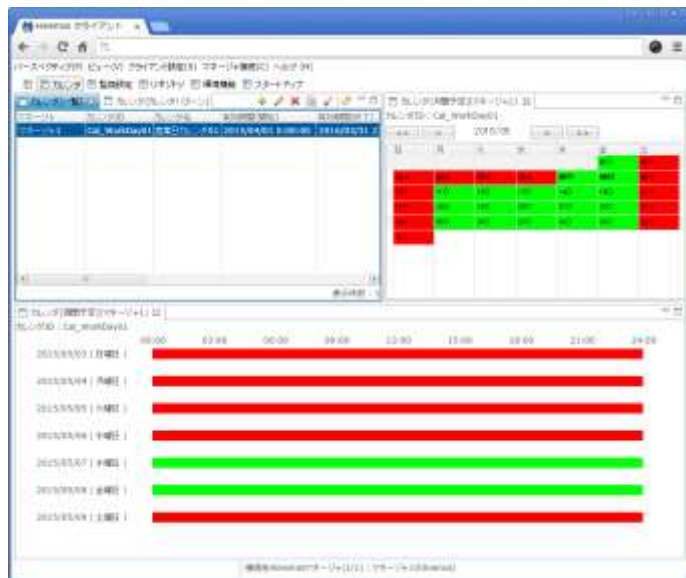
Hinemos



統合運用管理のための共通基本機能

カレンダー ジョブ管理分野で培った高度なカレンダー設定

業務の営業日・メンテナンス日に合わせたカレンダー定義が可能



定期的なカレンダー

- ・ 年月日、曜日の定期ルールで指定可能
- ・ 前後日指定で、日数ずらした定義可能
- ・ 非稼働日の場合の振替日・振替回数を指定可能

不定期なカレンダーパターン

- ・ 定期的ではない祝日パターンを指定可能
- ・ 会社の創立記念日、緊急メンテナンス日も指定可能

稼働スケジュールを
視覚的に確認可能

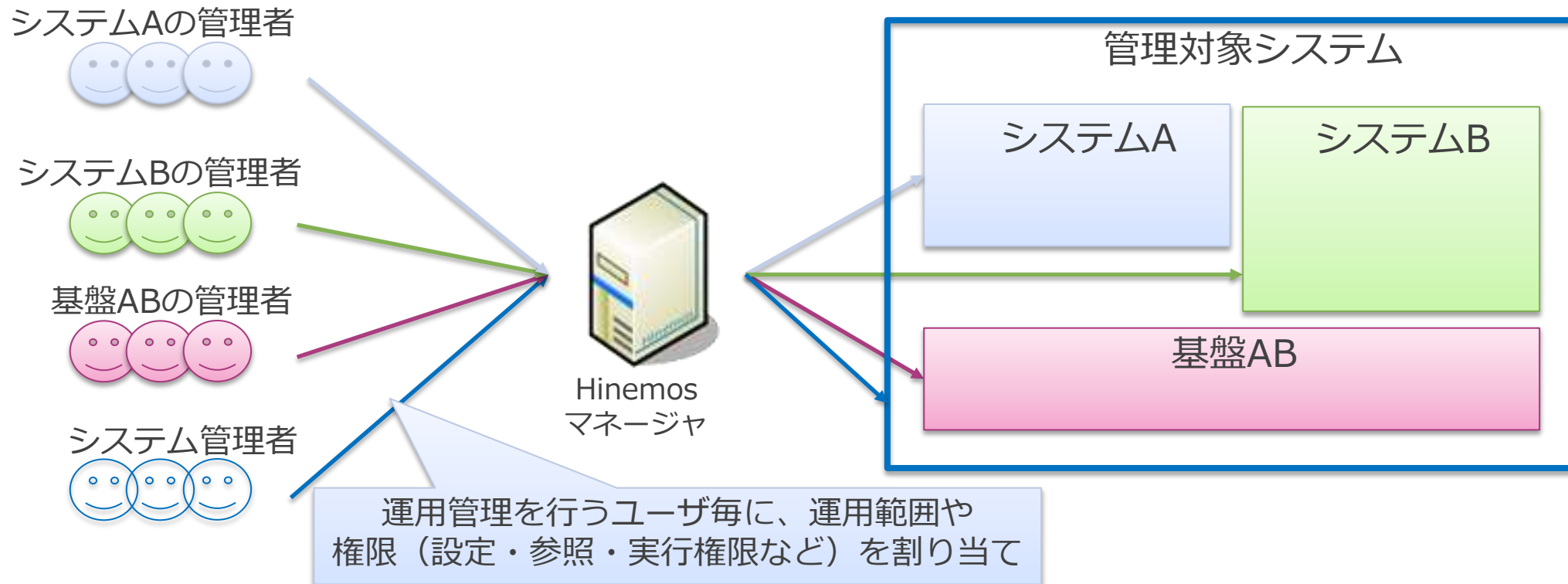
昼間・夜間の異なる運用を
実現可能

監視・ジョブ・通知などの
各機能で指定可能

複数テナント間での
カレンダー共有・非共有が可能

アカウント 1マネージャでマルチテナント利用が可能

管理対象システムの要件に応じた、柔軟なアクセス制御可能



オーナー、ロール、システム権限、オブジェクト権限を指定することで
運用管理者毎の役割に応じた運用範囲・権限設定が可能に

収集・蓄積したデータの保存管理と管理DBのメンテナンス機能を完備

データの保存管理

収集・蓄積したデータ、実行履歴の保存期間の指定やバックアップ、リストアなどのデータ管理の機能が用意されています。

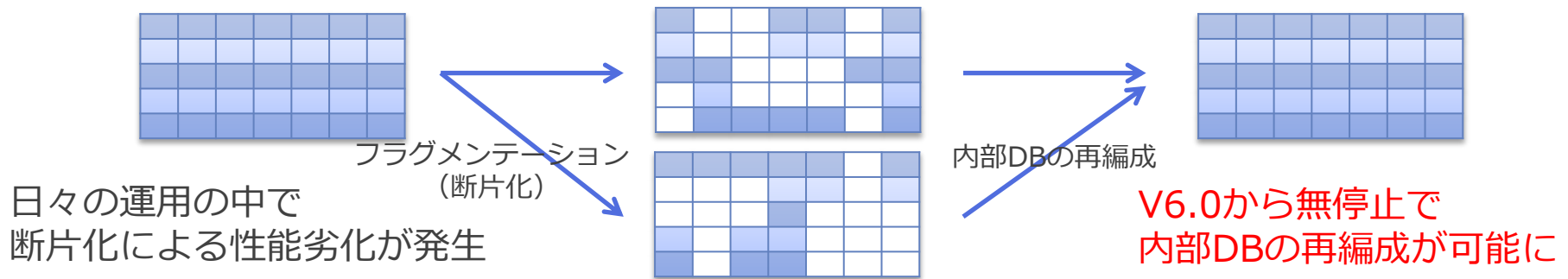


- ・直近1年間を管理DBに保存
- ・1年以上前のデータはエクスポート/アーカイブし、管理DBからは削除

ユーザ作り込み不要

管理DBのメンテナンス

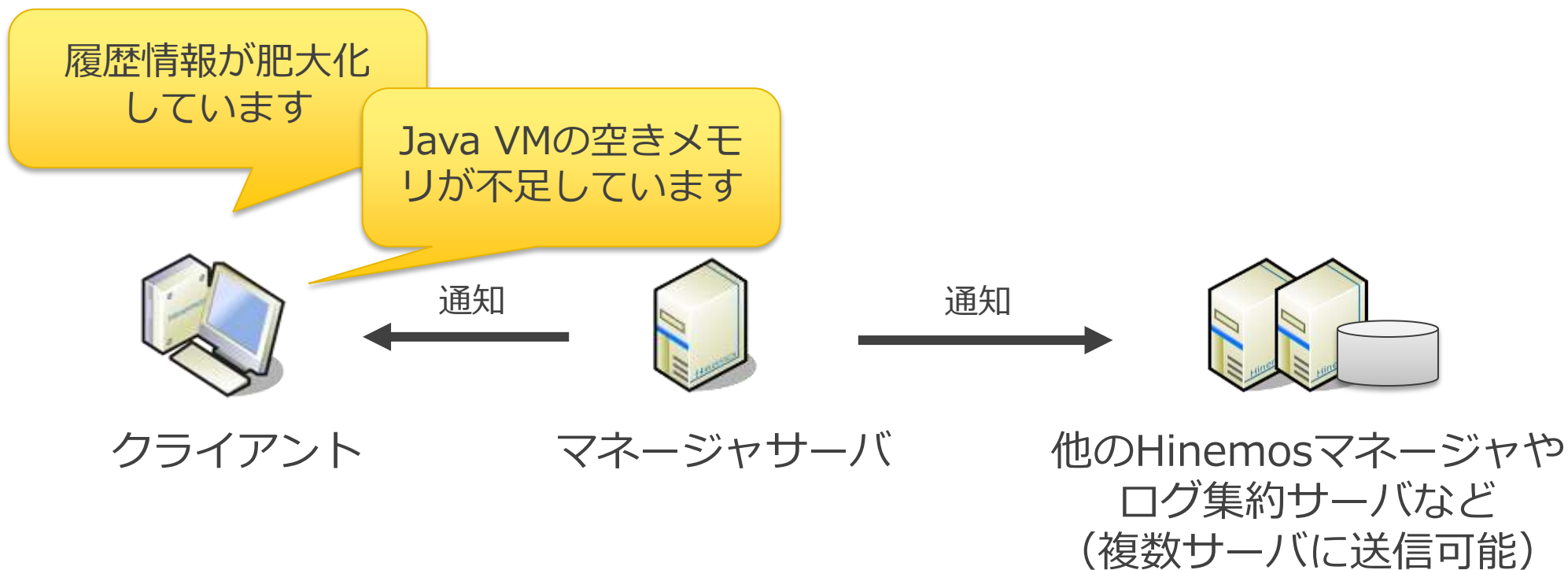
Hinemosに限らずDB管理にはフラグメンテーションに対し定期的な再編成が必要です。Hinemosではオンラインで可能です。



※ver.6.1では無停止での管理DB再編成はLinuxマネージャのみになります。

セルフチェック機構

自分自身の異常の予兆をいち早く検知しINTERNALイベントで通知



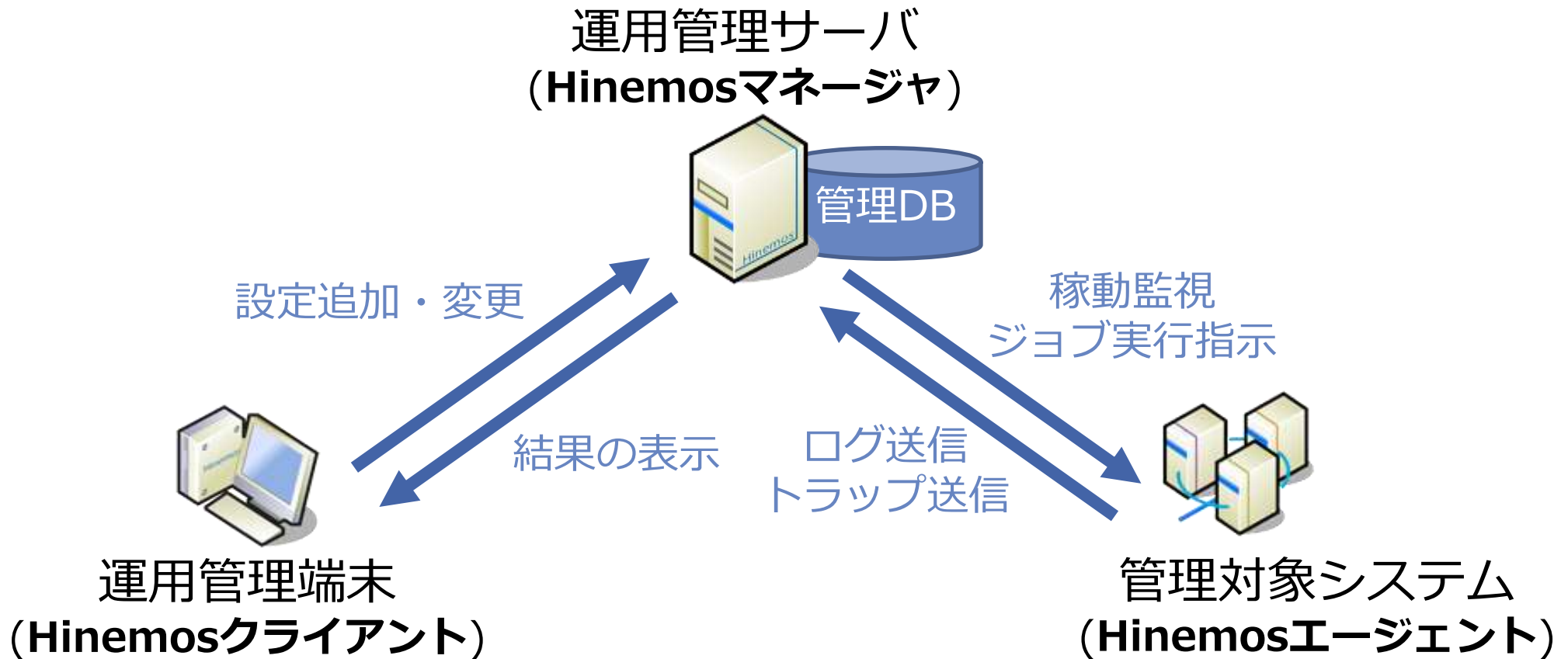
異常発生前に
障害予兆を確認できる

INTERNALイベントから
対処方法を確認できる

Hinemosの動作環境

Hinemosの基本構成

- Hinemosは3つのコンポーネントから構成



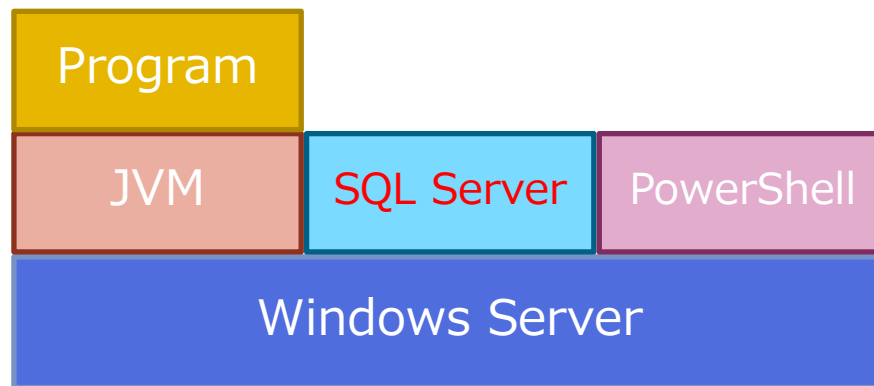
Hinemos ver.6.1の動作環境

コンポーネント	動作環境	提供方法
Hinemosマネージャ	RHEL/CentOS 7	GitHub
	RHEL/CentOS 6	ご契約者向けサイト
	Windows Server 2016, 2012R2	ご契約者向けサイト
Hinemosエージェント	RHEL/CentOS/OracleLinux 7, 6, 5	GitHub
	Windows Server 2016, 2012R2, 2012, 2008R2, 2008	GitHub
	Windows 10, 8.1, 8, 7	GitHub
	Amazon Linux	GitHub
	Solaris 11,10 HP-UX 11i v3, AIX 7.2, 7.1	ご契約者向けサイト
	SLES 12, 11	GitHub
	Ubuntu 16.04 LTS	GitHub
	Android 4.1, 5.0, 5.1, 6.0	Google Play
Hinemosクライアント (リッチクライアント)	Windows Server 2016, 2012R2, 2012, 2008R2	GitHub
	Windows 10, 8.1, 8, 7	GitHub
Hinemosクライアント (Webクライアント)	Internet Explorer, Firefox, Chrome ※サポート対象ブラウザ	GitHub

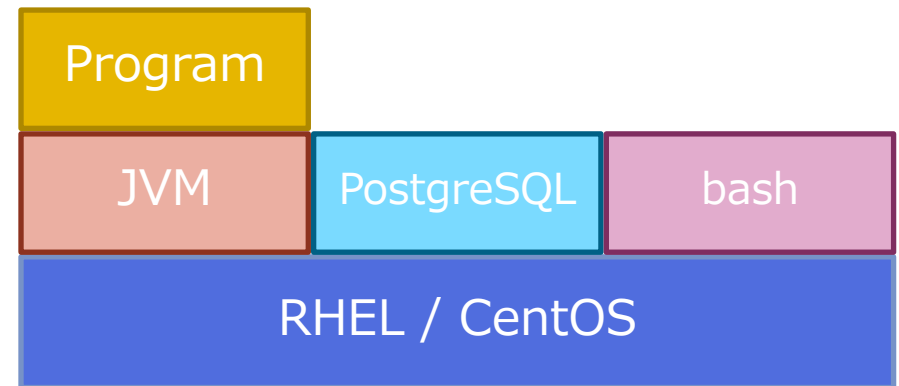
Hinemos Windows版マネージャ

■ ALL Windows環境で安定運用するためWindows対応をリリース

- データベースは、Windowsにおいて信頼性が高い**SQL Server**を採用
- スクリプトは、**PowerShell**を採用
- Hinemosマネージャの起動・停止・異常時は**Windowsイベントログ**にメッセージを出力

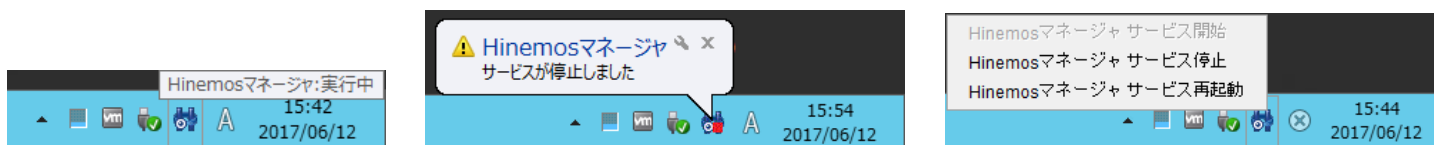


Windows版マネージャ



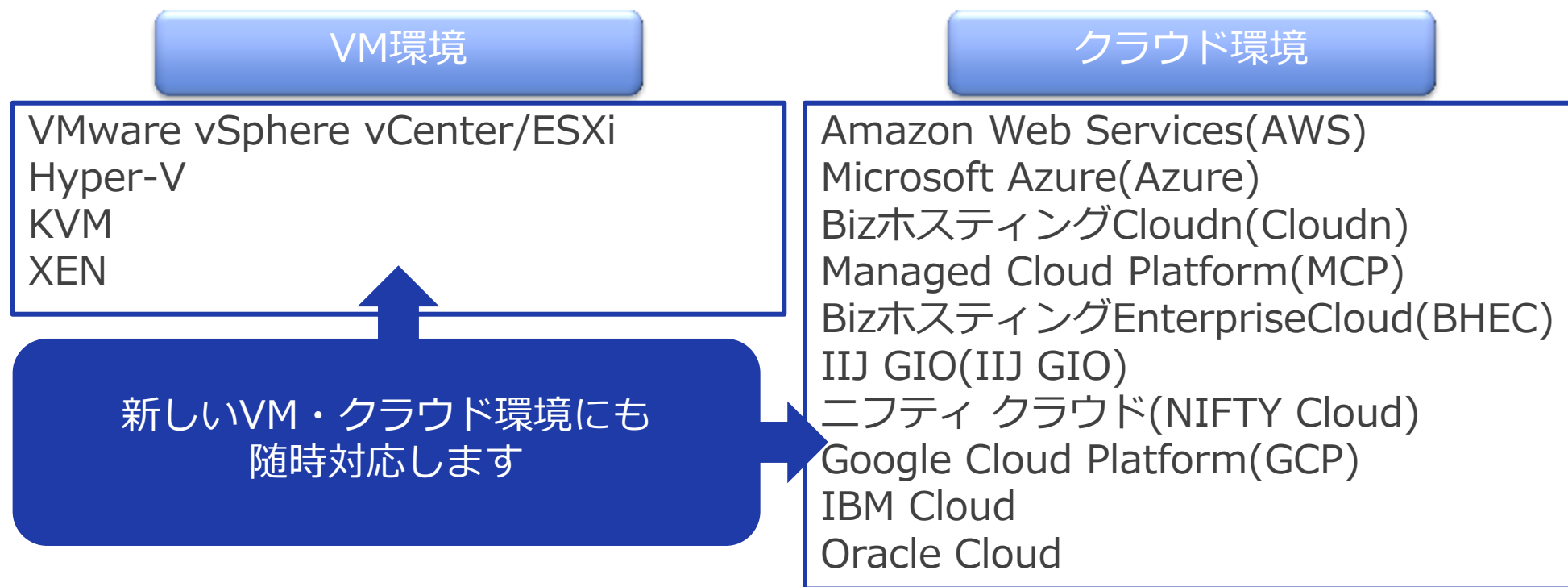
Linux版マネージャ

- **タスクトレイ**で状態確認や再起動などが可能



HinemosのVM・クラウド環境の動作サポート

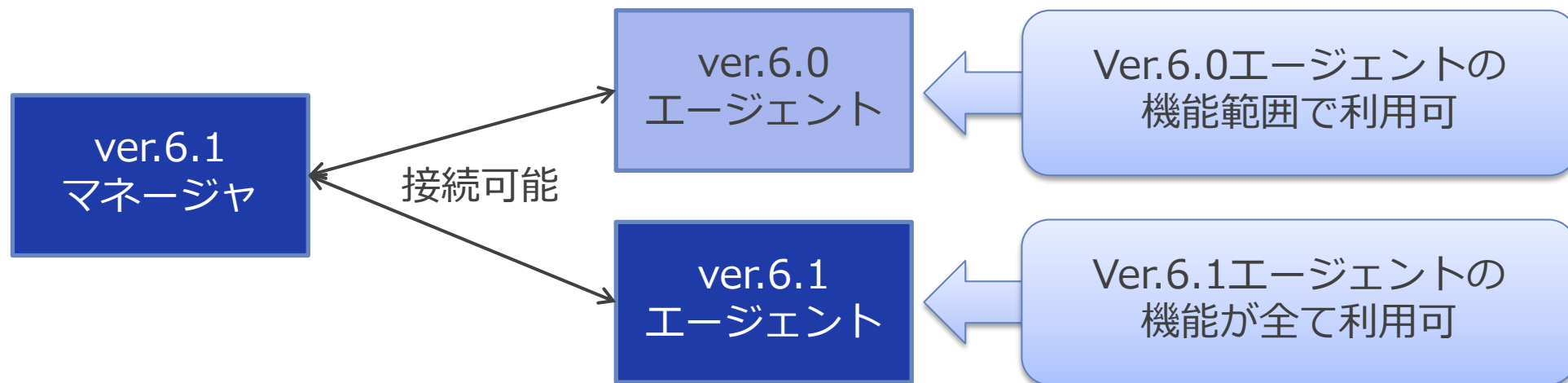
■ 様々なVM・クラウド環境上でHinemosの動作をサポート



オンプレミス環境からVM・クラウド環境に移行した場合でも安心してHinemosが使えるように動作サポートを推進します。

バージョン互換性

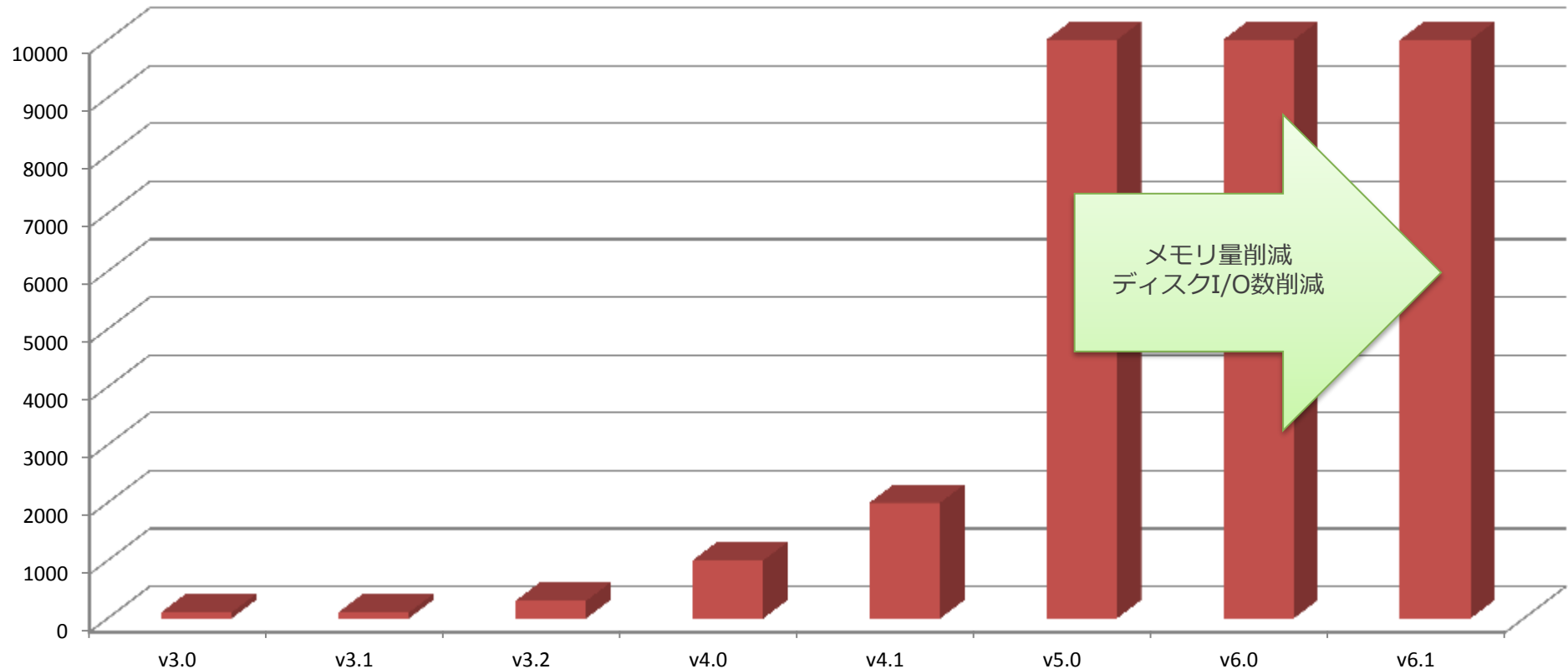
- Ver.6よりバージョン互換性の対応を進めます。



新バージョンの新機能を利用したい場合に
管理対象サーバに導入したHinemosエージェントをそのまま
Hinemosマネージャのみのバージョンアップで対応できます。

Hinemosのパフォーマンス システム規模 サーバ数

■ 1マネージャあたりで管理できるサーバ数は**10,000台**規模

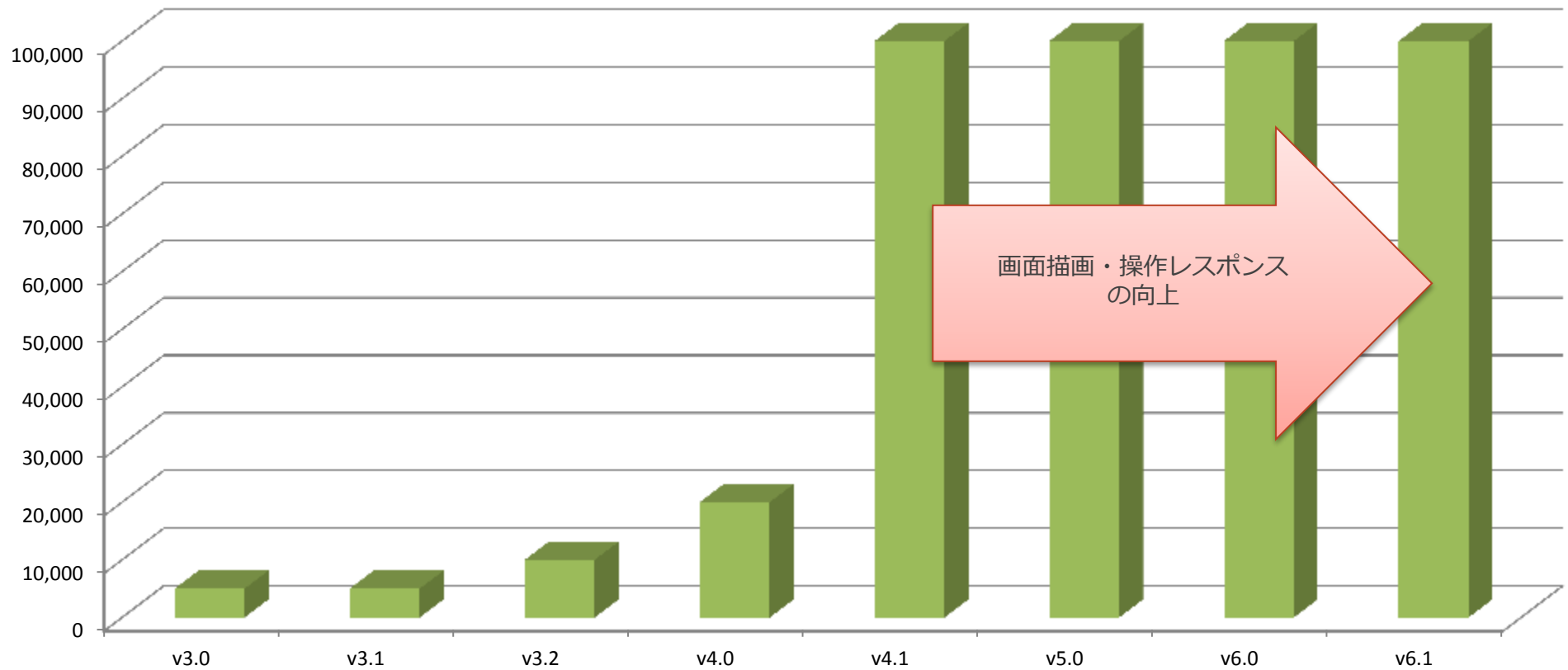


	v3.0	v3.1	v3.2	v4.0	v4.1	v5.0	v6.0	v6.1
監視対象サーバ数	100	100	300	1,000	2,000	10,000	10,000	10,000

※あくまで製品リリース時の特定条件における評価結果です。実際の運用の際に性能評価・サイジングを実施することを推奨します。

Hinemosのパフォーマンス システム規模 ジョブ数

■ 1マネージャあたりで管理できるジョブ数は**100,000ジョブ**規模



	v3.0	v3.1	v3.2	v4.0	v4.1	v5.0	v6.0	v6.1
ジョブ登録数	5,000	5,000	10,000	20,000	100,000	100,000	100,000	100,000

※あくまで製品リリース時の特定条件における評価結果です。実際の運用の際に性能評価・サイジングを実施することを推奨します。

まとめ

- Hinemosは、サーバ機器、端末、OS、MW、APなどのありとあらゆるデータを**収集/蓄積**が可能となります
- Hinemosは、収集したデータをもとに、システムの稼動状況の**監視や、グラフ**を用いた分析が可能となります
- Hinemosは、**環境構築の自動化、システム運行の自動化（ジョブ）、運用プロセス自動化（Runbook Automation）**が可能となります
- **運用アナリティクス**により蓄積したデータを活用してリアルタイムな状況把握、未来への予防保全が可能となります

