# 障害監視 &システム運用を語ろう

## ～障害監視フレームワークと運用方法論研究～

波田野 裕一

(日本UNIXユーザ会)

JANOG24 2009-07-09

# 略歴

- ADSLキャリアでISP運用
- 小規模ISPの立ち上げ支援
- 官庁小規模システムの運用/Close
- ASPでの運用設計

# 障害監視とツール

- いろいろな監視・運用ツールがあった
  - Net-Saint, MRTG, OpenView, アプライアンスの管理ツール, etc
- それぞれの強みやフォーカスがばらばら
  - 死活監視、リソース監視、ハードウェア、GUI/レポート機能
- 特にツール連携が難しい、面倒。
  - 「統合監視」は、画面を並べただけ、みたいなことにも。

# 障害監視 自作ツール

- 補完するために自作ツールを作ってみる、のは定番
  - だんだん機能や役割があちこちで重複
  - じゃ、モジュール化して使いまわしをしてみよう。
  - なんか、モジュール間連携が上手く動きません(泣
  - 更に、仕様変更や新規案件に意外と上手く対応できません(泣

# はたっと気付く

- そもそも、障害監視に必要な機能ってなんだっけ?
- そもそも、障害監視ってどんなプロセスがあるんだっけ?

# 試行錯誤してみました。

- オブジェクト指向分析/設計(OOA/OOD)ってのがあるらしい
  - アクター、ユースケース、MVCフレームワーク。。
  - 重複の排除、部品の独立性向上、依存関係の非循環。。

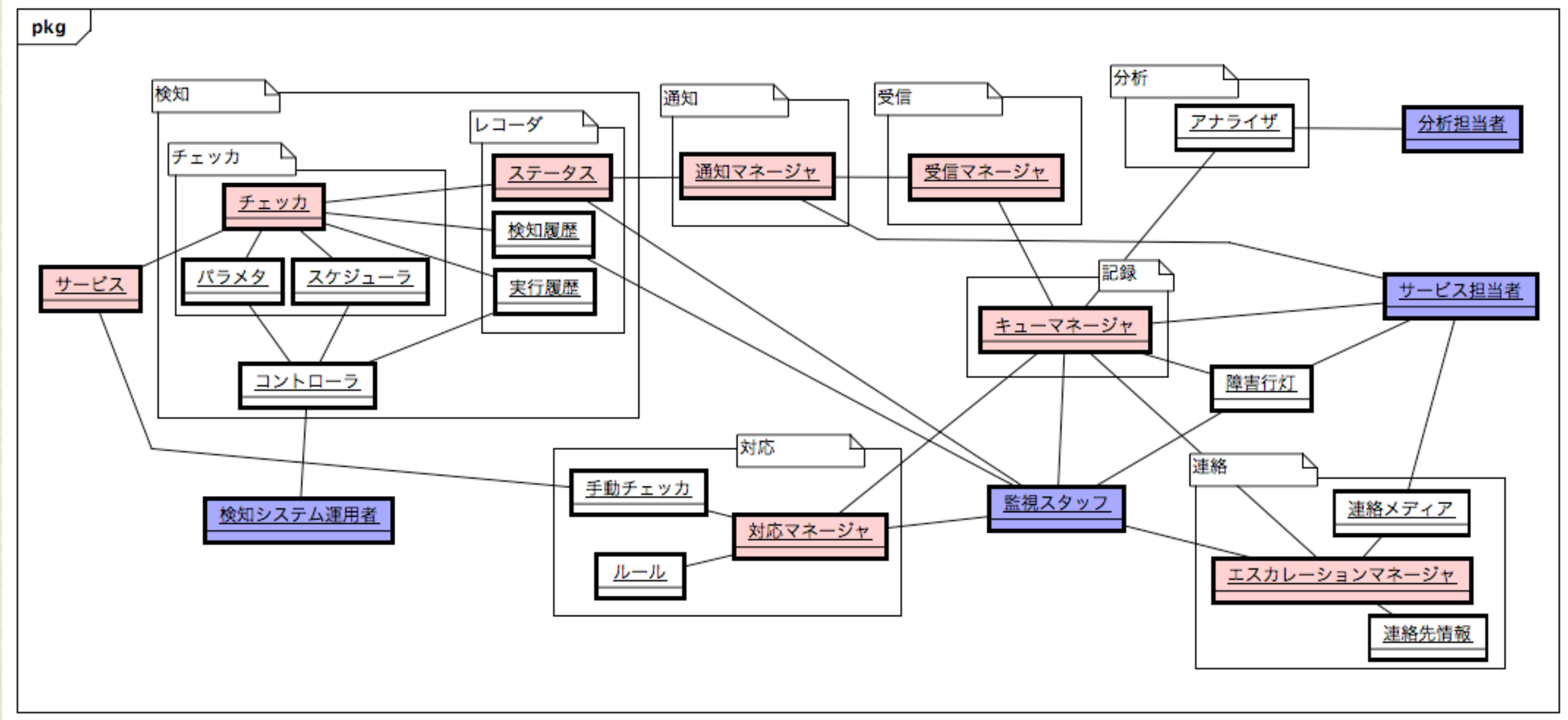
# ぶっちゃけオブジェクト指向

- ヒト/モノ(オブジェクト)が、
- 相互にメッセージで会話する、
- 一連の相互作用を把握/表現するもの。

※個人的な意訳です:-)

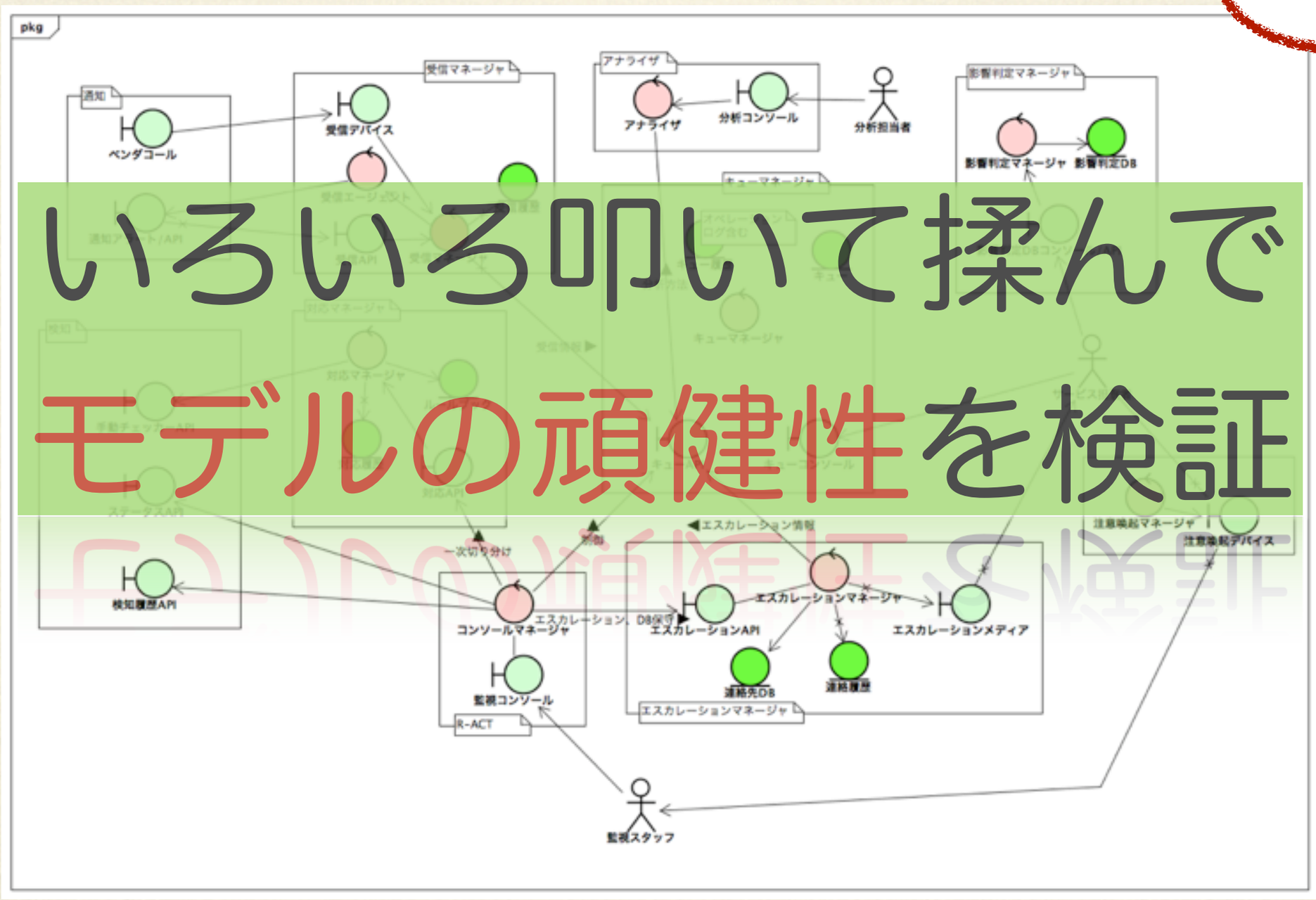
# 障害監視 (オブジェクト図)

Step1



# ロバストネス分析

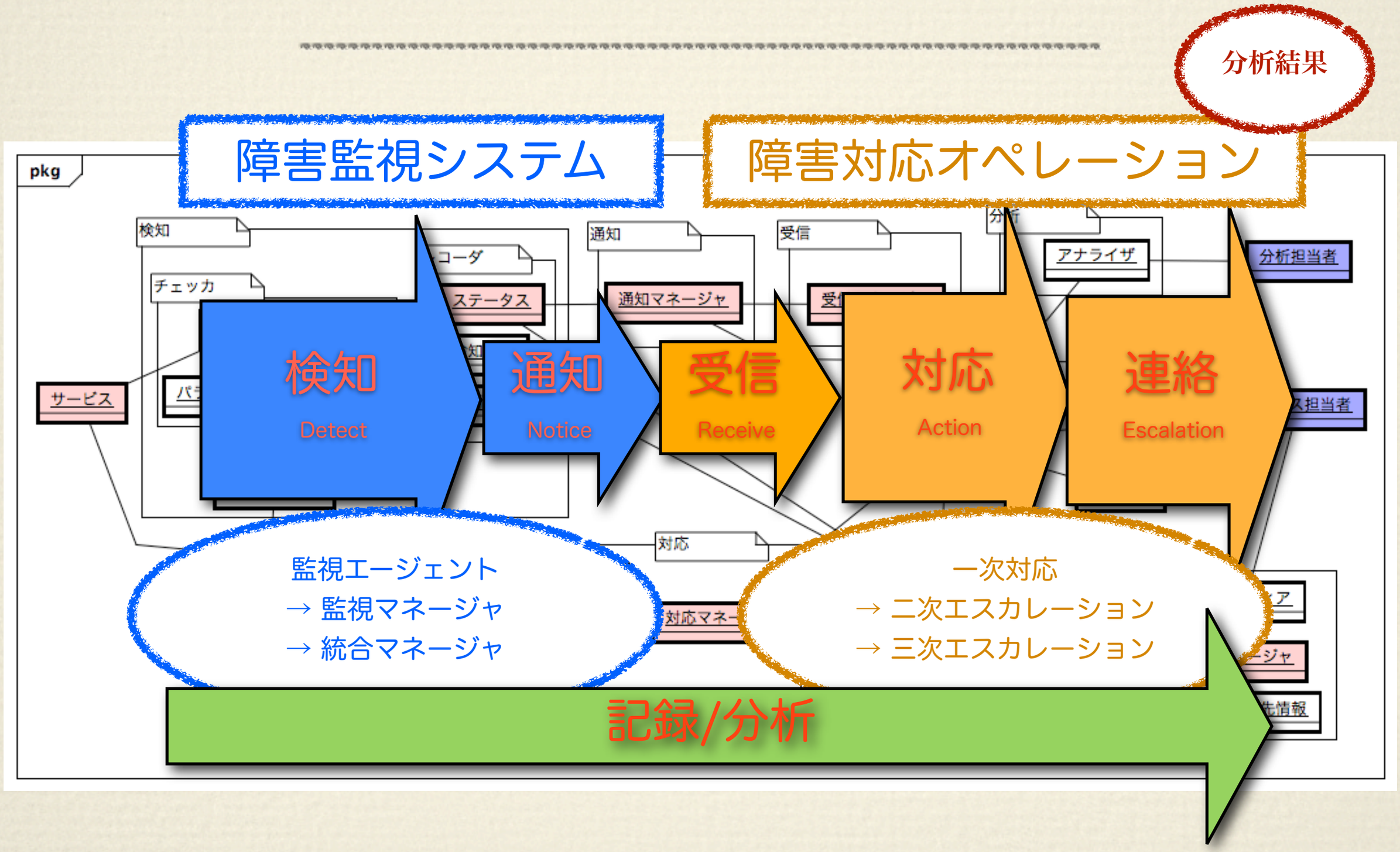
Step2




いろいろ叩いて揉んで

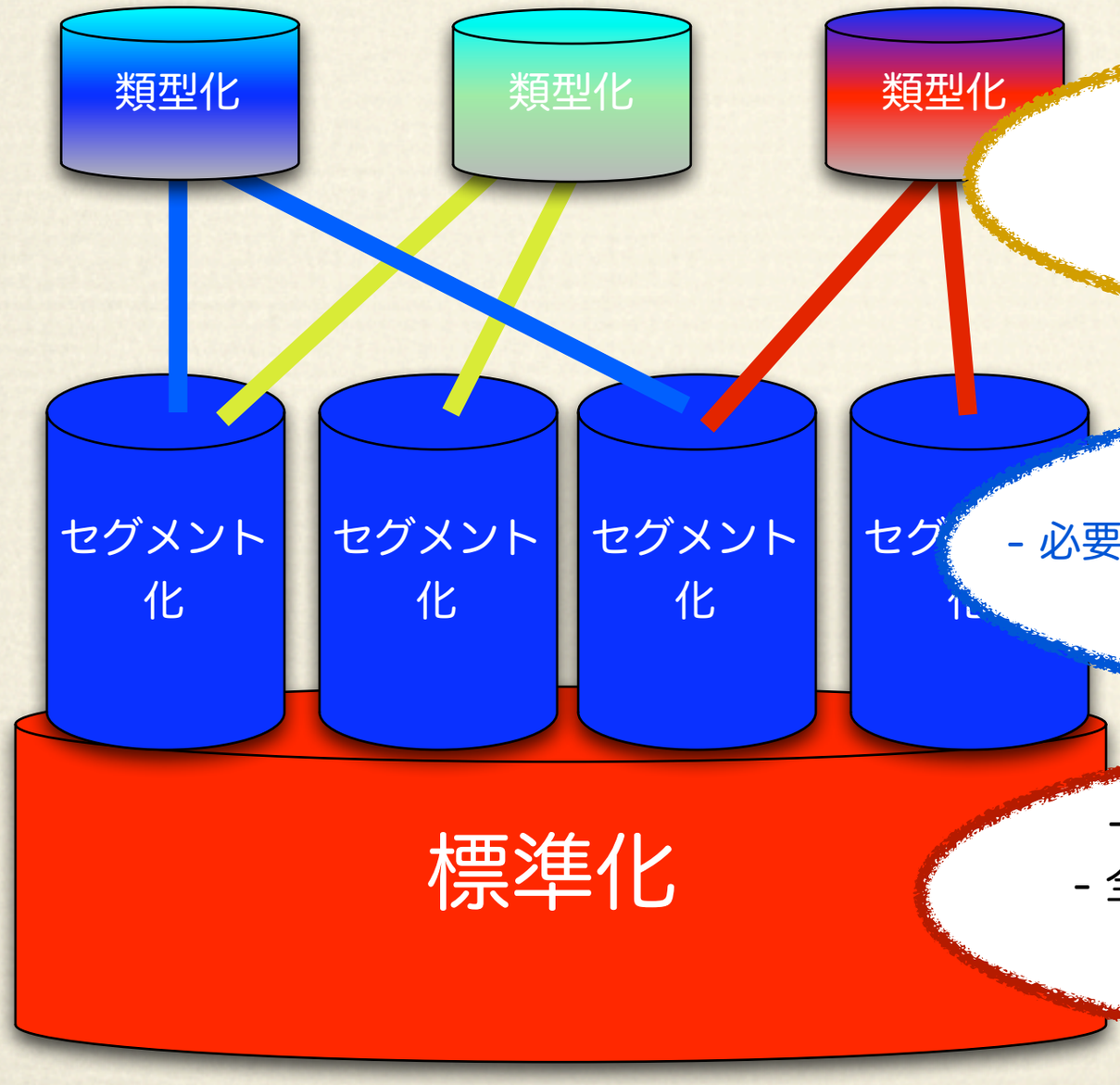
モデルの頑健性を検証

# 障害監視の6分野


分析結果
障害監視システム
障害対応オペレーション
pkg
検知
チェッカ
コーダ
ステータス
通知
通知マネージャ
受信
受
分析
アナライザ
分析担当者
サービス
対応
対応マネー
ア
ージャ
先情報
検知
Detect
通知
Notice
受信
Receive
対応
Action
連絡
Escalation
監視エージェント
→ 監視マネージャ
→ 統合マネージャ
一次対応
→ 二次エスカレーション
→ 三次エスカレーション
記録/分析

# 3つの方向性

# 標準化 / セグメント化 / 類型化




- 類似問題点の共通化、ナレッジ化
- 類型に基く個別モデル化
- セミオートメーション化

- S/N比の改善
- 必要な情報を必要あるとき必要あるところへ。
- 個別事情への柔軟な対応

- 不統一によるオーバヘッドの削減
- 全体問題点の明確化、改善サイクル化
- 導入/展開の迅速化

# 6分野 × 3つの方向性 = 障害監視「論点表」

| 分野 / 領域 | D.検知 | N.通知 | R.受信 | A.対応 | E.連絡 | P.記録/分析 |
|---|---|---|---|---|---|---|
| 標準化 | • D00 検知ログ | • N00 通知ログ | • R00 受信ログ | • A00 対応ログ | • E00 エスカレーションログ | |
| | • D01 検知手法<br>• D02 発動と復旧 (検知ID)<br>• D03 アクティブ監視 サイジング (監視対象の選別基準)<br>• D04 パッシブ監視 サイジング (バースト防止基準) | • N01 フォーマット<br>• N02 通知メディア<br>• N03 通知サイジング (流量) | | • A01 対応フロー<br>• A02 インシデント ID<br>• A03 復旧通知による発動の消し込み<br>• A04 対応状況の集中管理/進捗共有<br>• A05 短期特別対応フロー | • E01 エスカレーションフロー<br>• E02 連絡先管理 | • P01 インシデント管理<br>• P02 問題管理<br>• P03 分析/KPI |
| セグメント化 | • D05 現象重要度<br>• D06 ノード重要度<br>• D07 影響範囲 (単体)<br>• D08 影響サービス群 | • N04 通知先 | -- | -- | • E05 連絡先<br>• E06 伝達レベル | |
| 類型化 | • D09 潜在リスク要素のカタログ化<br>• D10 潜在リスク アセスメント (ツール)<br>• D11 現象パターン化<br>• D12 ベンダコール受信 | • N05 通知リスク アセスメント (ツール) | | • A06 一次対応パターン<br>• A07 イレギュラルール<br>• A08 リカバリパターン<br>  • 手順化<br>  • 自動化<br>• A09 影響範囲 (複合) | • E03 伝達項目<br>• E04 連絡シナリオ | |

# 考えてみませんか?

- 監視技法ってどこかに体系的にまとまってます?
- 現場でパッチワーク的に仕込んでいません?
- 監視システムちゃんと使いこなせています?
- 障害監視のベストプラクティスってなんだろう?

# そもそも障害はなぜ起きる?

- 実は、サービス障害のほとんどは人災。
- 障害発生(具現化)は、設計と運用の積み重ねから。
  - アラートストームは、ダメな設計、ダメな運用の結果。
- 美しい設計と運用をしていれば、サービス障害は最低限に(なるはず
- 障害とは結局、設計と運用の通信簿(いいすぎ?

# じゃ、運用ってなんだ?

- 運用の妙は一心に存す (宋史岳飛伝、14世紀中葉)
- うまく機能を働かせ用いること、活用。
  (広辞苑 第六版)
- そのもののもつ機能を生かして用いること。活用。 (大辞泉)

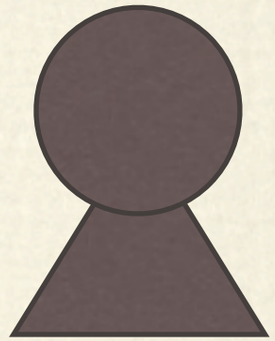
# 「運用」の正しい(?)イメージ

調査研究
って運用?

構成変更
って運用?

運用の
対象

あるものを
あるがままに
活用する



部署間調整
って運用?

障害原因の
追求って運用?

# 「運用」のたてつけがおかしい

- 人によって概念が異なる。
- 本当(?)の「運用」に対する予算がない
- ドキュメントがない
- 属人的だ
- 障害が起きても、実は初動手順はない
- 設計が悪くてもフィードバックできない

# 「障害」は「運用」の結果?

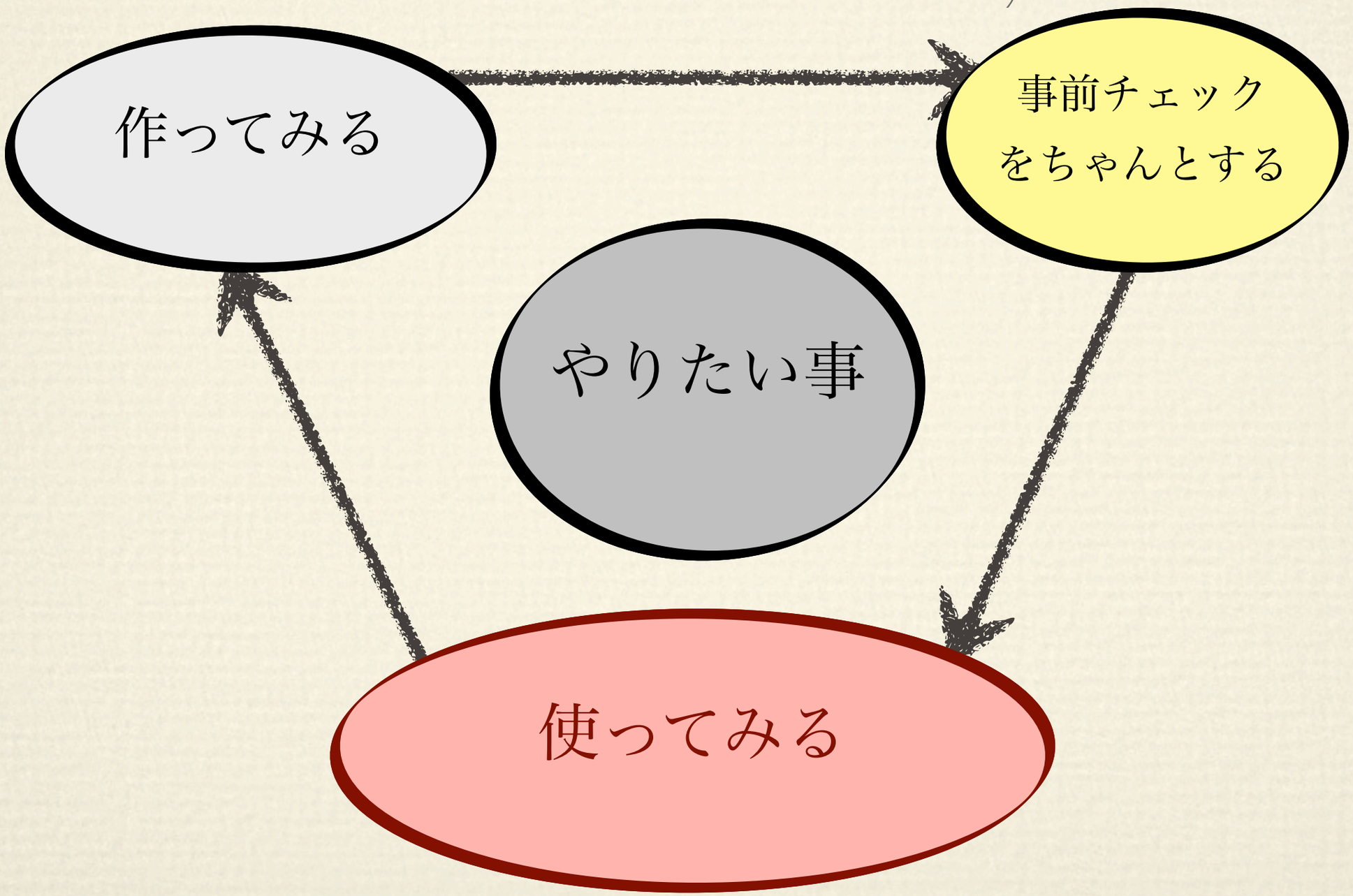
標準的な「運用」の枠組みがあれば、たてつけ良くなり、結果として障害が減るのでは?

# 運用のベストプラクティスは?

# ITIL Version3 ?

# ITライフサイクル (ITIL v3)

※個人的な超訳です:-)



# ITIL v3では物足りない

- ITIL v3の大きな特徴は、ServiceTransitionの概念の導入かなと。
- ITサービスのライフサイクルという概念は、意外と良いたてつけかも。
- しかし、ServiceOperationの内容は粗い印象。
- 無ければ作る、のがエンジニア(そうか?

※個人的な認識です:-)

# 運用の体系イメージ

1. 定義、カバーする範囲
2. 工数(予算)管理上の体系
3. ドキュメント管理上の体系
4. スキル管理上の体系
5. ツール整備上の体系

# 運用 5つの体系

## 1. 定義、カバーする範囲

- 守備範囲の明確化
- 理想と現実の差分見える化

# 運用5つの体系

## 2. 工数(予算)管理上の体系

- 工数コストの明確化、予算可能化
- リソースの適正配分へ

# 運用5つの体系

## 3. ドキュメント管理上の体系

- 業務とドキュメントは表裏一体
- オペミス防止
- ドキュメント査読の定常化

# 運用5つの体系

## 4. スキル管理上の体系

- 業務とスキルのマッチング
- スキルパスの明確化
- OJT対象の明確化

# 運用5つの体系

## 5. ツール整備上の体系

- 業務とツールのマッチング
- カバー部分の明確化
- 整備対象、優先順位の明確化
- オペミス防止

# 運用体系化のイメージ

定常運用

非定常運用

情報管理

要員管理

コスト管理

# 運用体系化のイメージ

定常運用

## 定時に実施する作業のフロー

# 定時作業

- 引継ぎ
- イベント確認 (計画作業など予定の確認)
- 正常性確認
- 手動バッチ実行
- 定時レポート作成/確認 (日報、実績データ抽出など)、など

# 運用体系化のイメージ

定常運用

定常フローに従った申請対応のフロー

# 申請対応

- 新規運用案件の申請受入
- 構成変更申請 (サービス追加やシステム構成の変更など)
- 障害対応手順変更申請、など

# 運用体系化のイメージ

非定常運用

## 非常時対応

(インシデント)

サービス障害(reactive)/予兆(proactive)対応

運用基盤自体に対するインシデント

# 運用体系化のイメージ

非定常運用

## 非定常対応

## (イレギュラー)

手順化されていない緊急依頼など

# 運用体系化のイメージ

## 情報管理

運用に関連する情報媒体の管理フロー
(定時作業/申請対応に関連するデータ、
構成情報など)

# 運用体系化のイメージ

## 要員管理

運用に関連する要員の管理フロー

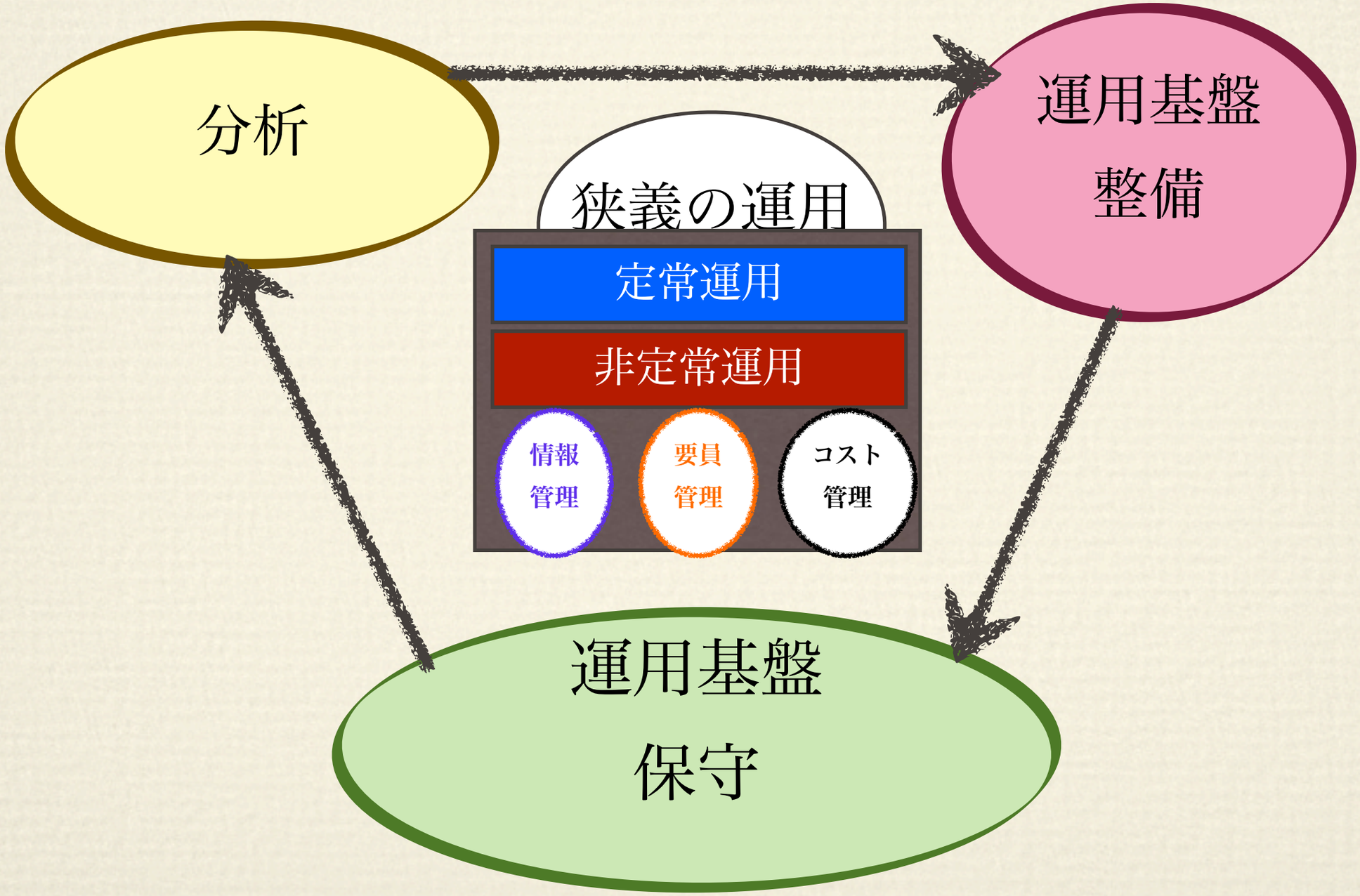
(シフト管理、運用委託を含む)

# 運用体系化のイメージ

## コスト管理

運用に関連するコストの管理フロー/基準

# 運用体系化のイメージ



# 運用体系化のイメージ

## 運用基盤

## 保守

- 基盤契約管理フロー
- 補修 (運用系バグ修正/故障対応)

# 運用体系化のイメージ

## 分析

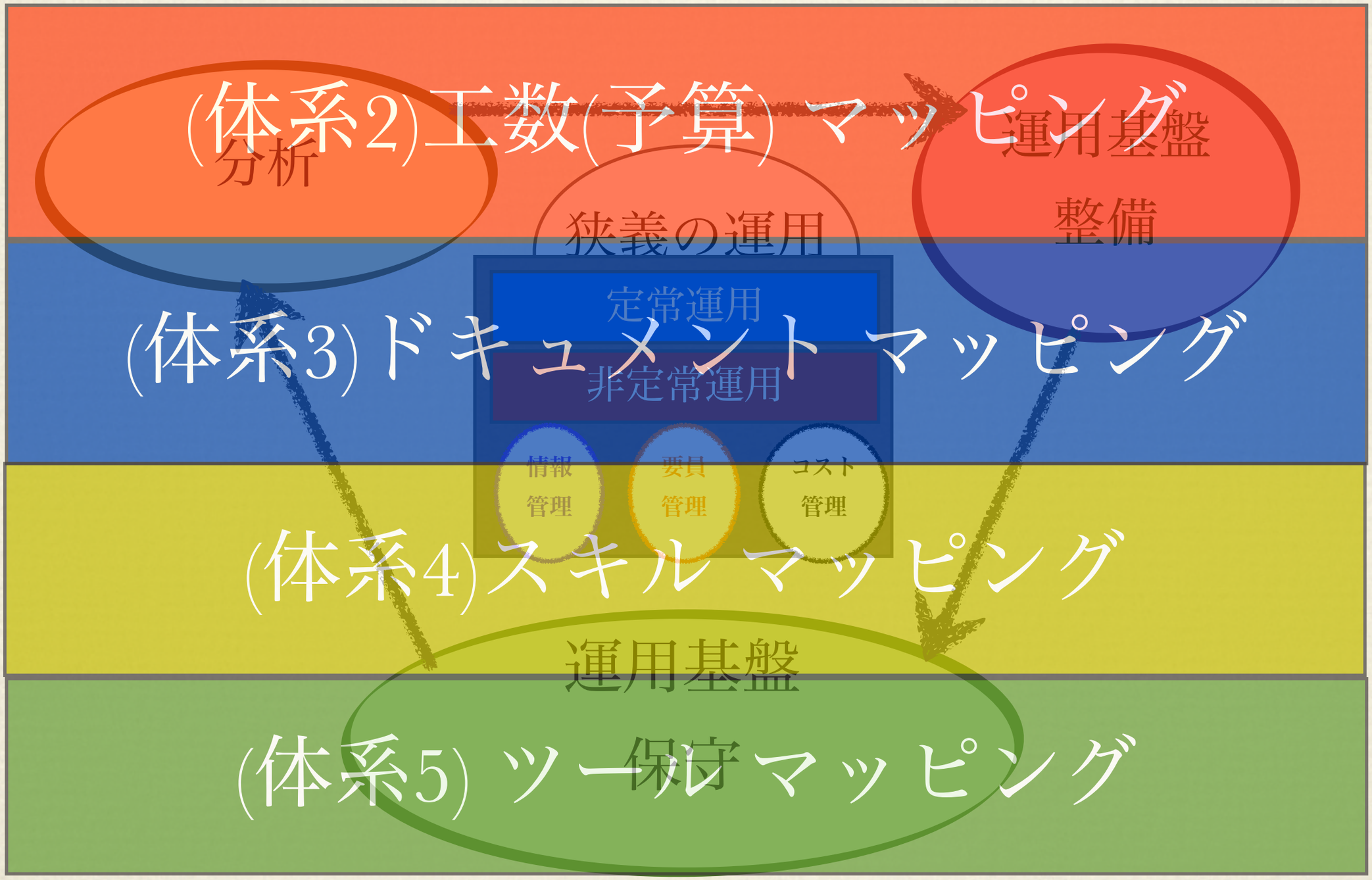
- 運用に関わるKPIの検討、改訂、その指針
- 運用/運用基盤の課題分析

# 運用体系化のイメージ

## 運用基盤整備

- 業務フロー/ツールの改善プロセス
- 運用基盤の強化/改善

# 「運用」のカバー範囲(体系1)



# 運用研究会

- 有志で「運用」や「障害監視」のフレームワークを探る活動を行ないます。
- 期間は2年。
- 協力 日本UNIXユーザ会(jus)
- 詳しくは、hatano@jus.or.jp まで
  - 日本語のメールでお願いします(笑