改めて監視を考えよう

～モニタリング・オブザーバビリティ～

Internet Week 2023

運用設計ラボ合同会社

シニアアーキテクト 波田野 裕一

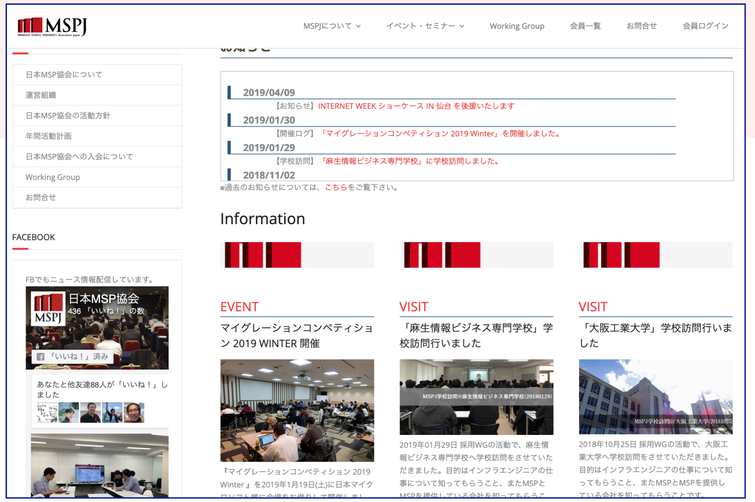
2023-11-20

日本MSP協会

IT情報基盤の運用サービスを提供するマネージド・サービス・プロバイダ及びIT情報基盤の運用に携わる技術者等と協力し、**運用の技術向上と品質向上、運用技術に携わる人材の発掘と育成、運用に関連する様々な評価軸を整理して明確化**するために日本MSP協会を設立します。そして、利用者にとって最適なIT情報基盤の選定と、適切なコストで安全かつ効率的に基盤を運用する指標を提供することで、さらなるIT産業界の活性化に貢献していきます。

MSPJ
MANAGED SERVICE PROVIDER'S Association Japan

https://mspj.jp/



運用設計ラボ合同会社

Operation 運用設計Lab

シニアアーキテクト

波田野 裕一

AWS Samurai 2017 (個人)
AWS Samurai 2020 (CLI専門支部)

AWS Community Hero

日本MSP協会 特別会員

インプットご支援

OpsLearn ®

科学的工学的な考え方に基づく講義とワークショップで
30年先も活きる運用設計スキルを身に付ける

OpsCLI ®

世界で最もAWS APIの仕様に忠実なeラーニングで
10年先も活きるAWSスキルを身に付ける

現場での実践ご支援

運用設計支援　　よろず相談

アウトプットご支援

ホワイトペーパー/ガイドライン策定支援
ホワイトペーパやガイドラインの制作や内製をご支援いたします。

概要

近年、「オブザーバビリティ」というキーワードが、クラウド界隈を中心として話題となっており、数多くのオブザーバビリティを謳ったサービスやツールが提供され、普及しつつあります。
この「オブザーバビリティ」は、従来、運用組織が担ってきた監視とは何が違うのでしょうか?

本セッションでは、監視とオブザーバビリティについて整理した上で、今改めて、監視には何が求められるのかについて、考え方を解説し、議論します。

アジェンダ

1. 監視とは

2. オブザーバビリティとは

3. 監視とオブザーバビリティ

4. 今後の「監視」

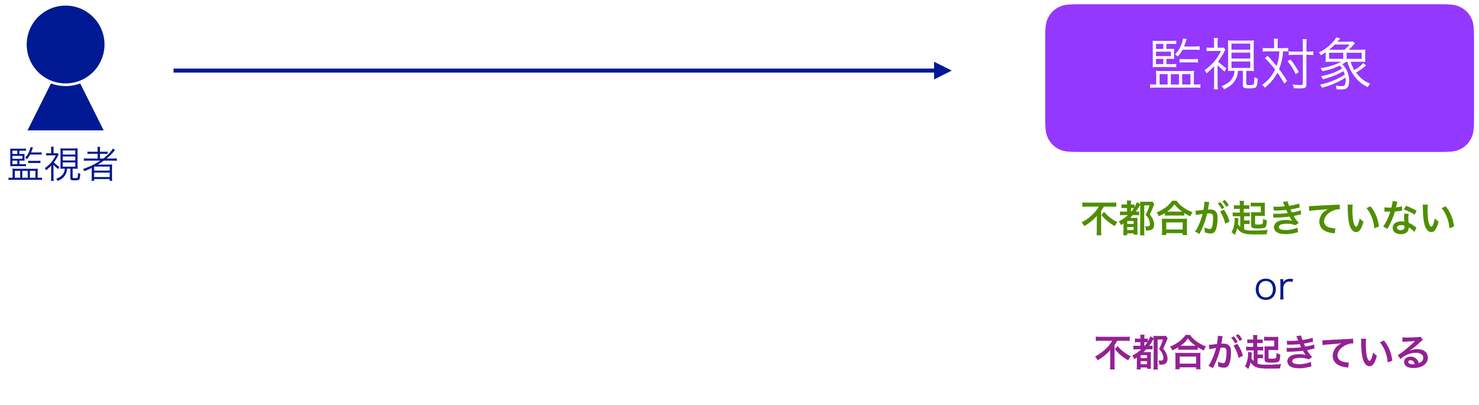
1. 監視とは

「監視」の定義

監視

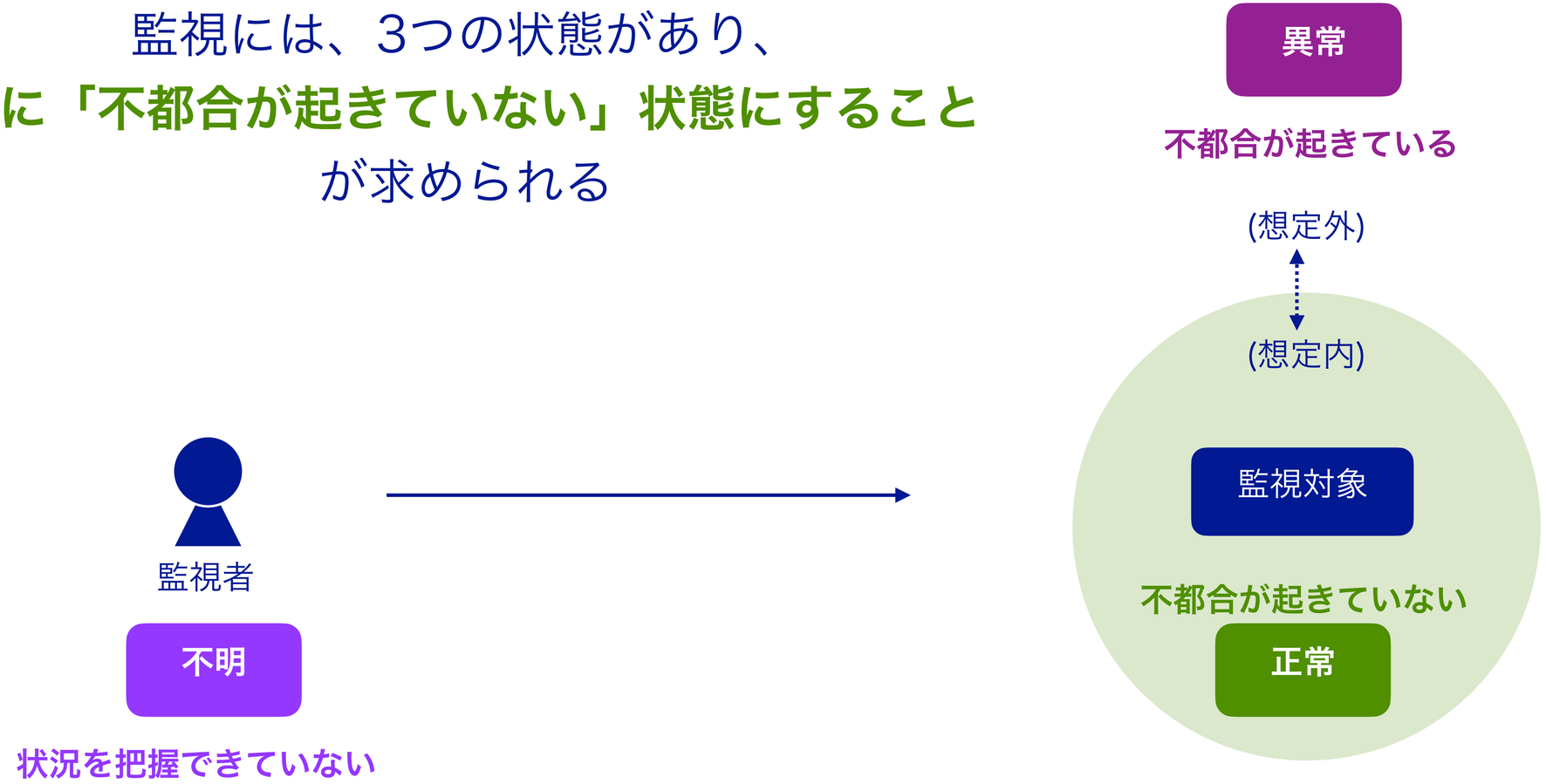
不都合な事の起こらぬように警戒して人の動きなどを見張ること。

(出典: スーパー大辞林)



「監視」における3つの状態

監視には、3つの状態があり、
常に「不都合が起きていない」状態にすること
が求められる

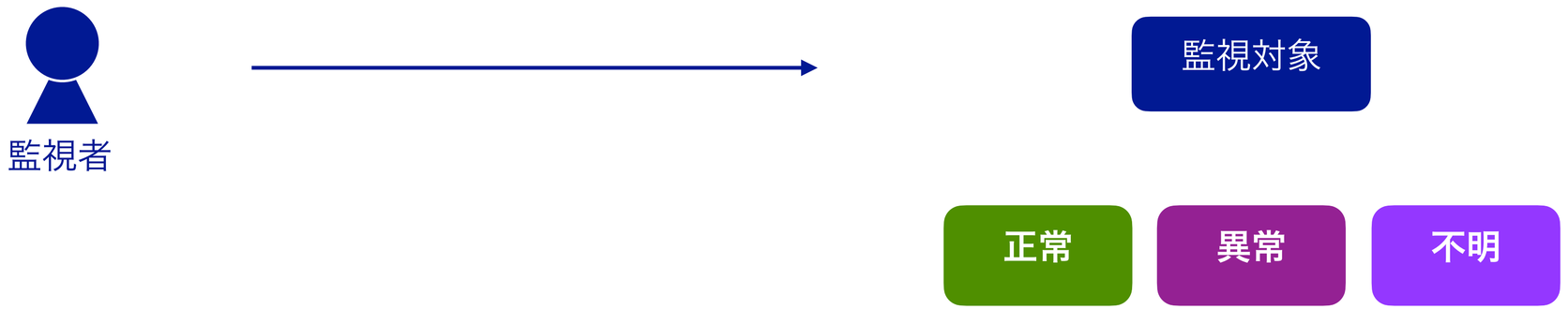


「監視」とは

監視とは

顧客に提供するサービスやその構成要素が**安定的に稼動していることを継続的に確認**し、その稼動が非安定的な状態にある場合には**復旧に必要な情報を収集し、対応**すること。

と定義する.

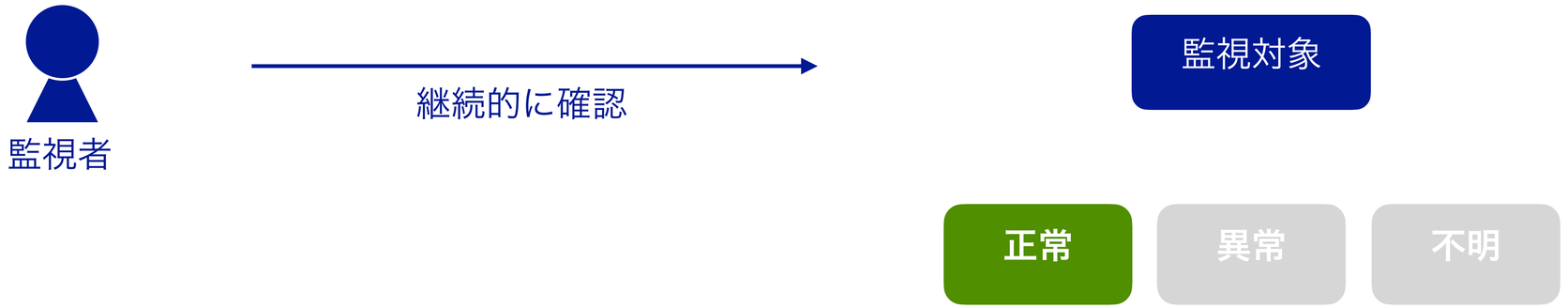


「監視」とは (正常確認)

監視とは

顧客に提供するサービスやその構成要素が**安定的に稼動していることを継続的に確認**し、その稼動が非安定的な状態にある場合には復旧に必要な情報を収集し、対応すること。

と定義する.

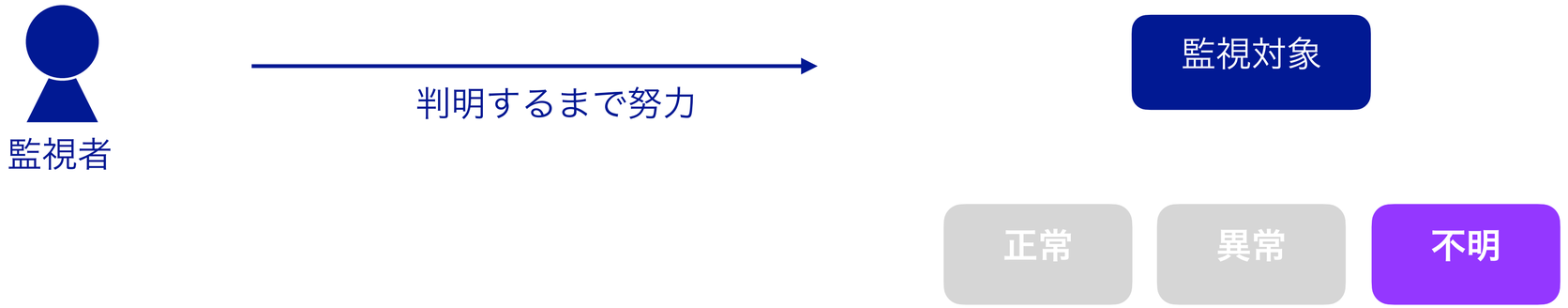


「監視」とは (不明の解消)

監視とは

顧客に提供するサービスやその構成要素が**安定的に稼動していることを継続的に確認**し、その稼動が非安定的な状態にある場合には復旧に必要な情報を収集し、対応すること。

と定義する.

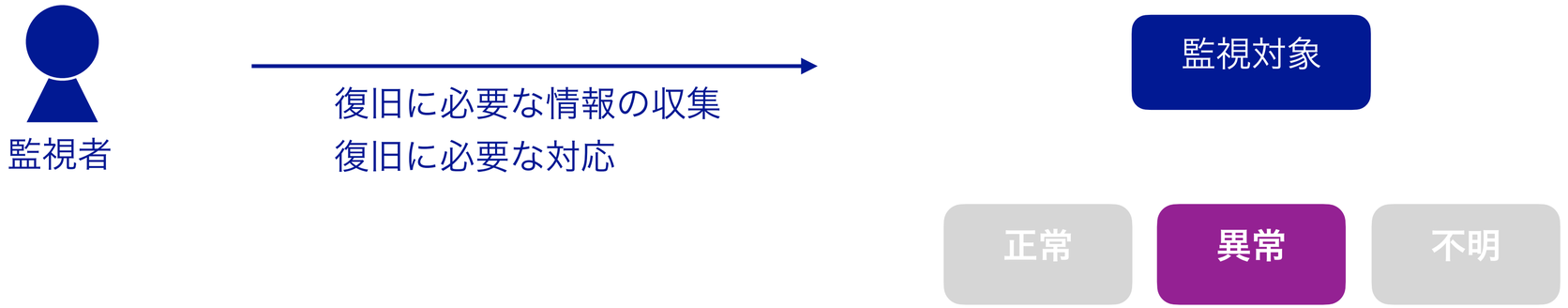


「監視」とは (異常の解消)

監視とは

顧客に提供するサービスやその構成要素が安定的に稼動していることを継続的に確認し、その稼動が非安定的な状態にある場合には**復旧に必要な情報を収集し、対応**すること。

と定義する.



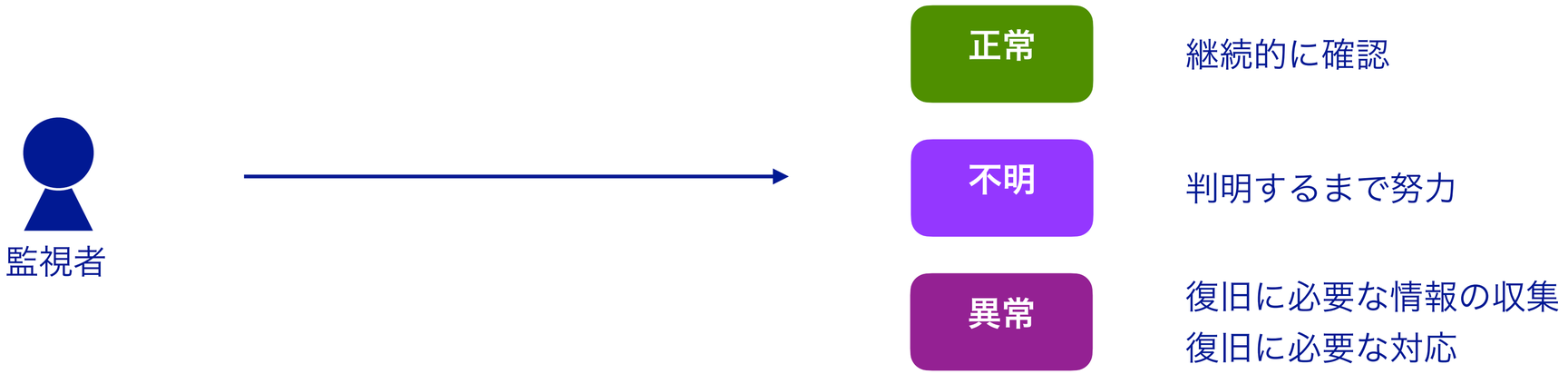
監視の目的

監視はサービスの安定的な稼動が最終的な目的

監視とは

顧客に提供するサービスやその構成要素が安定的に稼動していることを継続的に確認し、その稼動が非安定的な状態にある場合には復旧に必要な情報を収集し、対応すること。

と定義する.



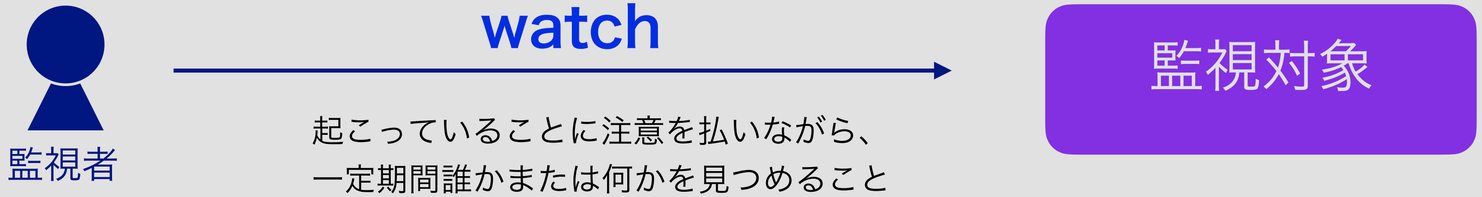
参考:「monitor」の定義

monitor

to carefully **watch** and check a situation in order to see how it changes over a period of time

ある期間の経過とともに状況がどのように変化するかを注意深く観察して確認すること

(出典: ロングマン現代英英辞典)



「**動きのあるものを注意して見る**」というニュアンス

監視の3つの分類

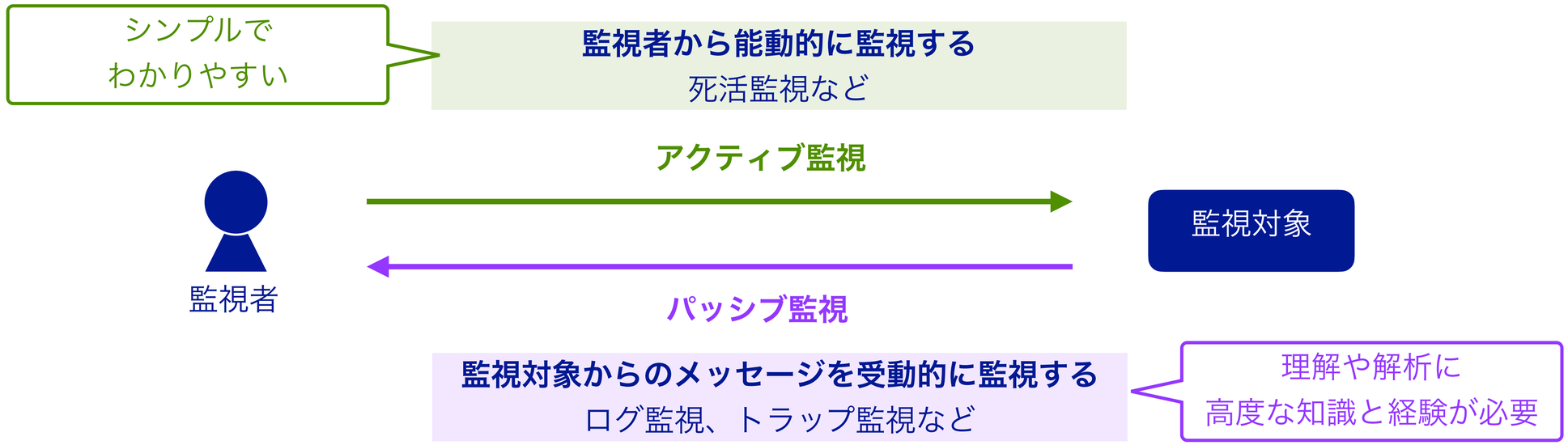
アクティブ監視とパッシブ監視

直視監視と死角監視

一次対応と二次対応

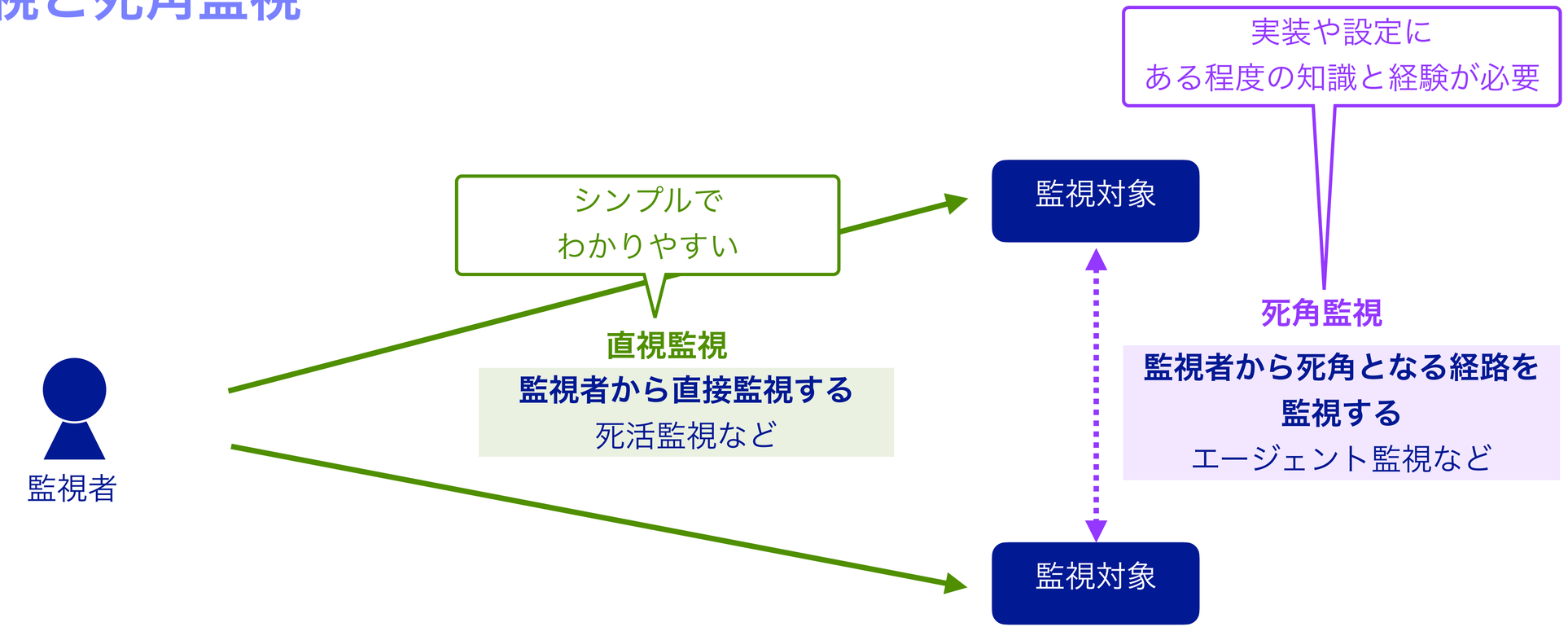
監視の分類1: アクティブ監視とパッシブ監視

アクティブ監視とパッシブ監視



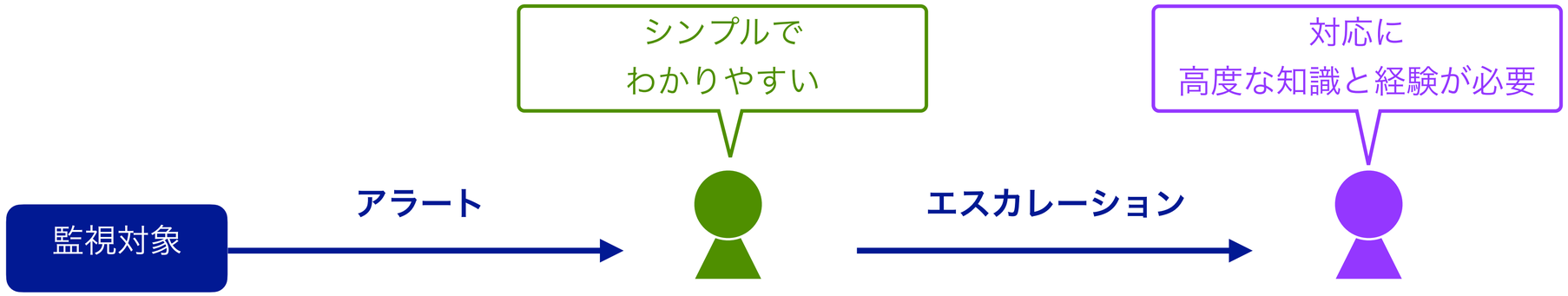
監視の分類2: 直視監視と死角監視

直視監視と死角監視



監視の分類3: 一次対応と二次対応

一次対応と二次対応



既知アラートは自分で対応
未知アラートは二次対応にエスカレーション

未知アラートへの対応
時には、予防的対応も実施

まとめ: 監視の分類

アクティブ監視とパッシブ監視

アクティブ監視

監視者から能動的に監視する

死活監視など

パッシブ監視

監視対象からのメッセージを受動的に監視する

ログ監視、トラップ監視など

直視監視と死角監視

直視監視

監視者から直接監視する

死活監視など

死角監視

監視者から死角となる経路を監視する

エージェント監視など

一次対応と二次対応

一次対応 (365日24時間 初動対応)

既知アラートは自分で対応

未知アラートは二次対応にエスカレーション

二次対応 (専門対応)

未知アラートへの対応

時には、予防的対応も実施

シンプルで
わかりやすい

理解・解析・対応に
高度な知識と経験が必要

2. オブザーバビリティとは

オブザーバビリティ (o11y)

可観測性

SREの文脈で出てきた。

特にアプリケーションと関連して重視されている。　　今後はアプリケーションだけではなくなるのでは...?

IT界隈での初出は2013年頃だが、話題に上がってきたのは2019年頃から。

オブザーバビリティ3つの柱

- **メトリクス** (タイムスタンプ + 測定値)
- **ログ** (タイムスタンプ + メッセージ)
- **トレース** (一つのリクエストに対する一連の挙動)

機械制御理論とオブザーバビリティ

可制御性と可観測性

1960年頃に機械制御理論の世界で登場

可制御性　Controllablity

システムに対してある入力を行うことで、有限時間以内に、任意の最終状態に到達することができる性質

インプットで制御

可観測性　Observability

システムからの出力により、システム内部の状態を推測することができる性質

アウトプットで推測

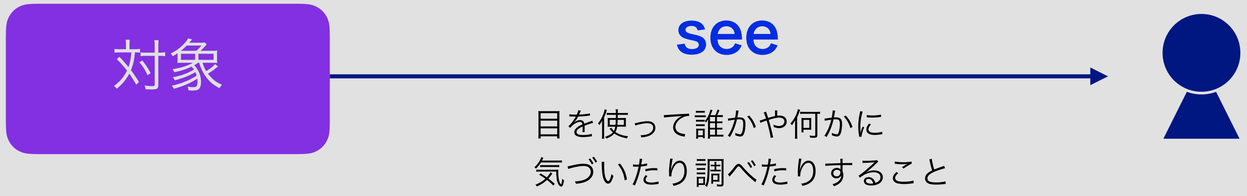
参考:「observe」の定義

observe

to **see** and notice something

何かを見て気づくこと

(出典: ロングマン現代英英辞典)



「**自然に目に入る**」というニュアンス

機械制御理論と健康維持

可制御性 Controllablity

システムに対してある入力を行うことで、有限時間以内に、任意の最終状態に到達することができる性質

インプットで制御　**食事で健康を制御する**

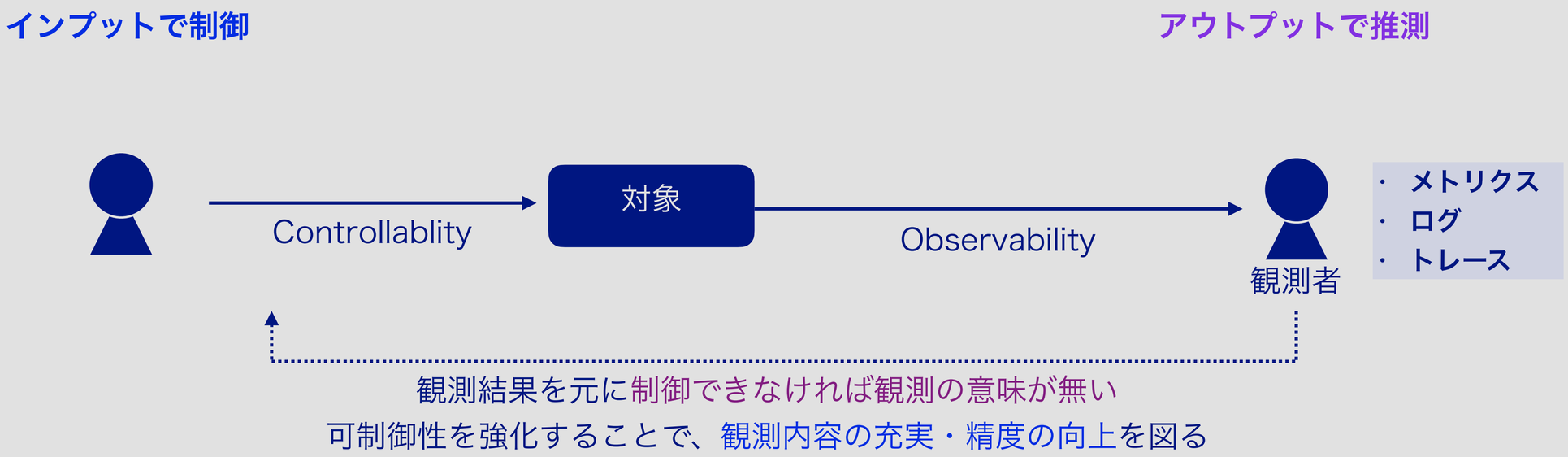
可観測性 Observability

システムからの出力により、システム内部の状態を推測することができる性質

アウトプットで推測　**検尿・検便・血液検査などで健康を推測する**

参考: 可観測性を向上するためには

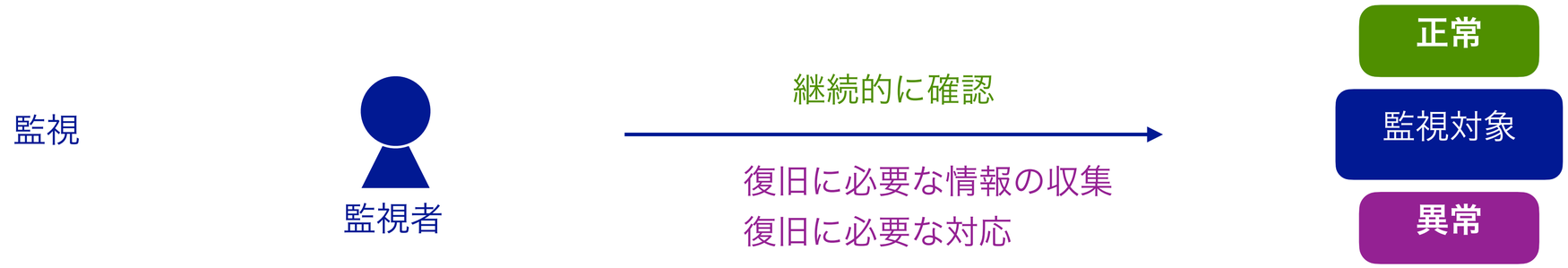
可観測性(アウトプットで推測)**を向上**させるためには、
可制御性(インプットで制御)**を向上**させる必要がある



健康診断の結果により、システムへのインプット(方法・内容)を改善する

3. 監視とオブザーバビリティ

監視とオブザーバビリティ



監視とオブザーバビリティの違い (1. 能動性)

監視

監視者

アクティブ

能動的 (watch)

特定の情報を**取りに行く**

オブザーバビリティ

対象

- メトリクス
- ログ
- トレース

パッシブ

受動的 (see)

アウトプットが出るのを待つ

観測者

監視とオブザーバビリティの違い (2. 事前性)

監視

監視者

リアクティブ

事後的 (reactive)

正常

監視対象

異常

発生後の対応が前提

オブザーバビリティ

対象

- メトリクス
- ログ
- トレース

プロアクティブ

事前的 (proactive)

観測者

発生前に対応できる可能性がある

監視とオブザーバビリティの違い (3. 対象)

監視

監視者

適切な**絞り込み**が重要

過剰なデータやアラートがノイズとなり
悪影響を及ぼす場合がある

オブザーバビリティ

対象

- **メトリクス**
- **ログ**
- **トレース**

観測データの**拡充**が重要

データが多いことによって
悪影響を及ぼすことはほとんど無い

観測者

監視とオブザーバビリティの違い (4. アクセス)

監視

監視者

一般的に
監視対象の**外部から監視**

サーバの外部から監視
プロセスの外部から監視

監視では「外部影響」の有無が重要

正常
監視対象
異常

オブザーバビリティ

対象

- **メトリクス**
- **ログ**
- **トレース**

一般的に
観測対象の**内部から取得**

リソース状態
ログの取得

観測者

監視とオブザーバビリティの違い (5. 動作の周期)

監視

監視者

動作は**周期的**

通常、1分周期や5分周期

オブザーバビリティ

対象

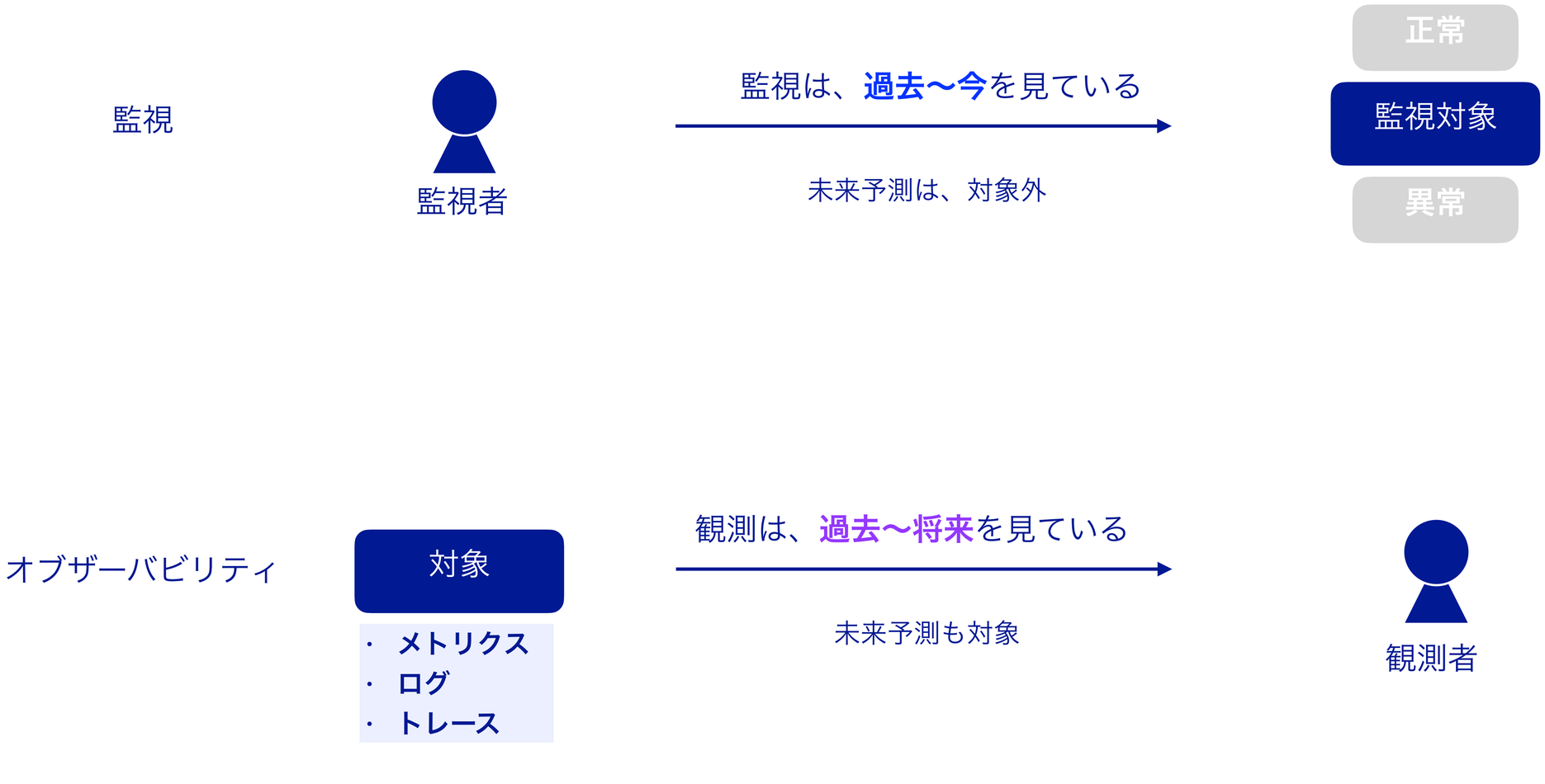
- **メトリクス**
- **ログ**
- **トレース**

動作は**随時的**

タイムスタンプとともに随時出力される

観測者

監視とオブザーバビリティの違い (6. フォーカスする時期)



監視とオブザーバビリティの違い (7. データの複雑さ)

監視

監視者

ある程度**モデル化**しやすい

24時間(一次対応)センターで
データの理解が可能

正常

監視対象

異常

オブザーバビリティ

対象

- **メトリクス**
- **ログ**
- **トレース**

複雑かつ変化しやすい

専門チーム(二次対応以降)でなければ
データの理解は困難

本来の「ログ監視」はこちら

観測者

監視とオブザーバビリティの違い (8. やりたい事)

監視

監視者

障害からの復旧

狭義の「事業継続」

今起きた障害を、すぐに復旧させたい

オブザーバビリティ

対象

- **メトリクス**
- **ログ**
- **トレース**

サービスやアプリの可視化

広義の「事業継続」

現状を推測したり、将来を予測したりする

観測者

まとめ: 監視とオブザーバビリティの違い

	監視	オブザーバビリティ
能動性	**アクティブ**	**パッシブ**
事前性	**リアクティブ**	**プロアクティブ**
対象	適切な**絞り込み**が重要	観測データの**拡充**が重要
アクセス	監視対象の**外部から監視**	観測対象の**内部から取得**
動作の周期	監視動作は**周期的**	監視動作は**随時的**
フォーカスする時期	監視は、**過去〜今**を見ている	観測は、**過去〜将来**を見ている
データの複雑さ	ある程度**モデル化**しやすい	**複雑かつ変化**しやすい
やりたい事	**障害からの復旧**	**サービスやアプリの可視化**

監視とオブザーバビリティは車の両輪

狭義の「事業継続」

今起きた障害を、
すぐに復旧させたい

目的が明確

	監視	オブザーバビリティ
	アクティブ	**パッシブ**
	リアクティブ	プロアクティブ
	適切な絞り込みが重要	観測データの拡充が重要
	監視対象の外部から監視	観測対象の内部から取得
	監視動作は周期的	監視動作は随時的
	監視は、過去〜今を見ている	観測は、過去〜将来を見ている
	ある程度モデル化しやすい	複雑かつ変化しやすい
	障害からの復旧	サービスやアプリの可視化

広義の「事業継続」

現状を推測したり、
将来を予測したりする

目的が多岐

従来の「監視」をオブザーバビリティの文脈で捉えなおす

(従来通りの) **監視**

アクティブ監視

監視者から能動的に監視する

死活監視など

直視監視

監視者から直接監視する

死活監視など

一次対応 (365日24時間 初動対応)

既知アラートはシフト勤務で対応

未知アラートは二次対応にエスカレーション

シンプルで
わかりやすい

オブザーバビリティ (として捉えなおすべき監視)

パッシブ監視

監視対象からのメッセージを受動的に監視する

ログ監視、トラップ監視など

死角監視

監視者から死角となる経路を監視する

エージェント監視など

(監視かオブザーバビリティかはケースバイケース)

二次対応 (専門対応)

未知アラートへの対応

時には、予防的対応も実施

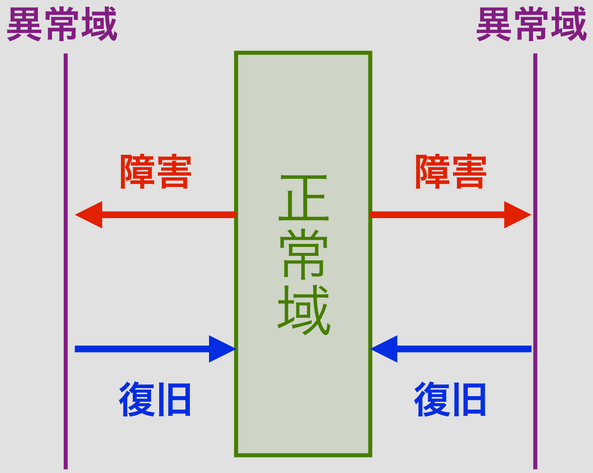
理解・解析・対応に
高度な知識と経験が必要

参考: 「変化」に対する立ち位置の違い

監視

変化に対してネガティブ

(変化が無い前提)



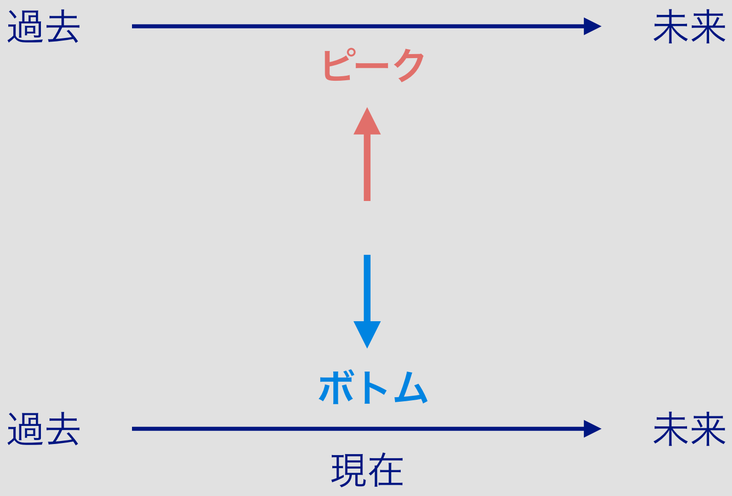
「正常」から逸脱したら戻さないといけない。

リリースによるネガティブな影響を捉える。

オブザーバビリティ

変化に対して中立的

(変化が有る前提)



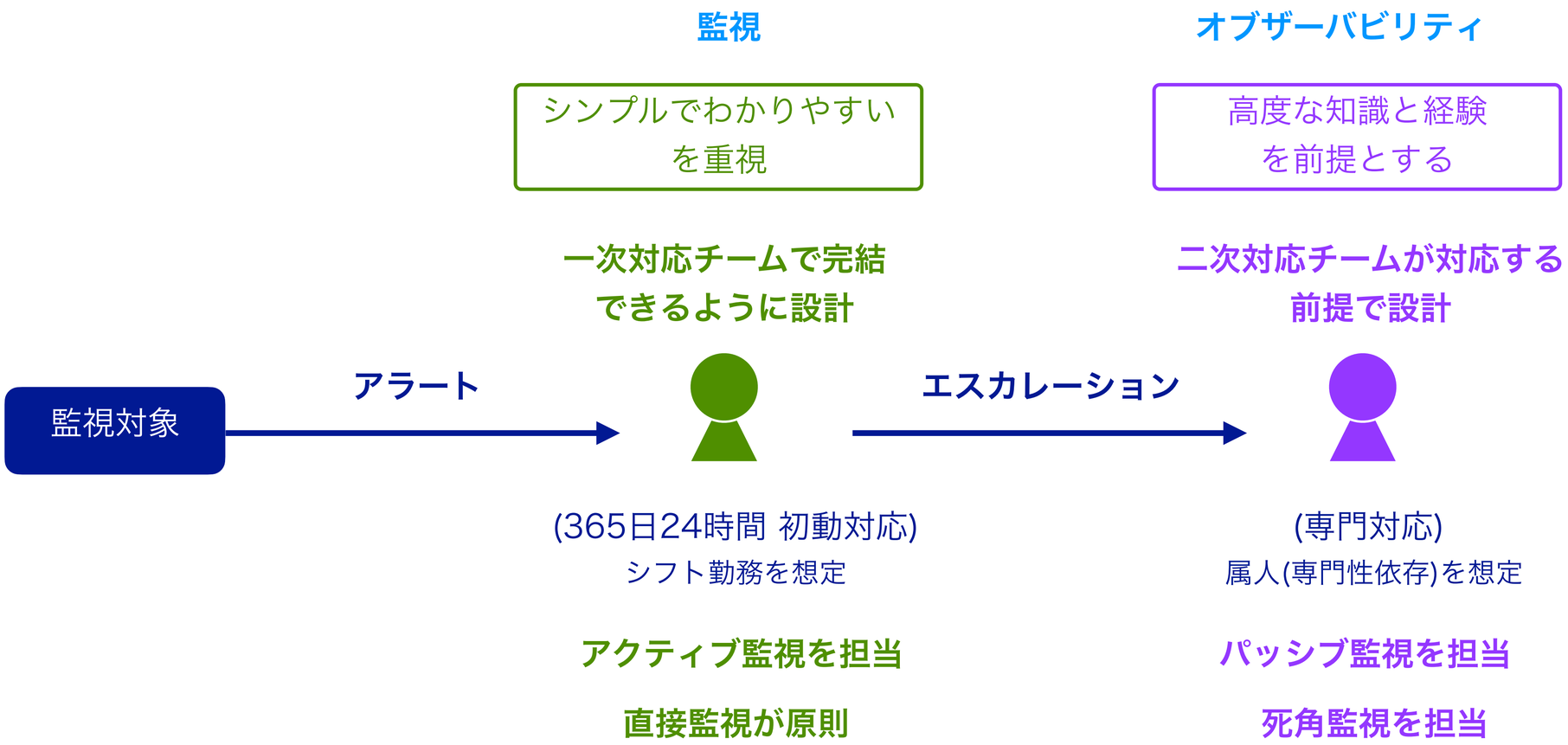
変化を捉えるために行う。

リリースによる変化を中立的に捉える。

4. 今後の「監視」

監視を改めて整理する

オブザーバビリティは目新しくはない。従来の監視を整理する良いきっかけ。



今後の監視 (ステップ0: 混在)

一つの監視チームで全てのアラートに対応

(従来からの)**監視**

既知のアラートと未知のアラートが混在
要求される知識と経験が多様で曖昧

アクティブ監視とパッシブ監視が混在

直接監視と死角監視が混在

今後の監視 (ステップ1: 監視の確立)

一次対応チームの対応内容を明確にし、エスカレーション先を整備する

監視

シンプルでわかりやすい
を重視

一次対応チームで完結
できるように設計

(365日24時間 初動対応)
シフト勤務を整備

アクティブ監視を担当

直接監視が原則

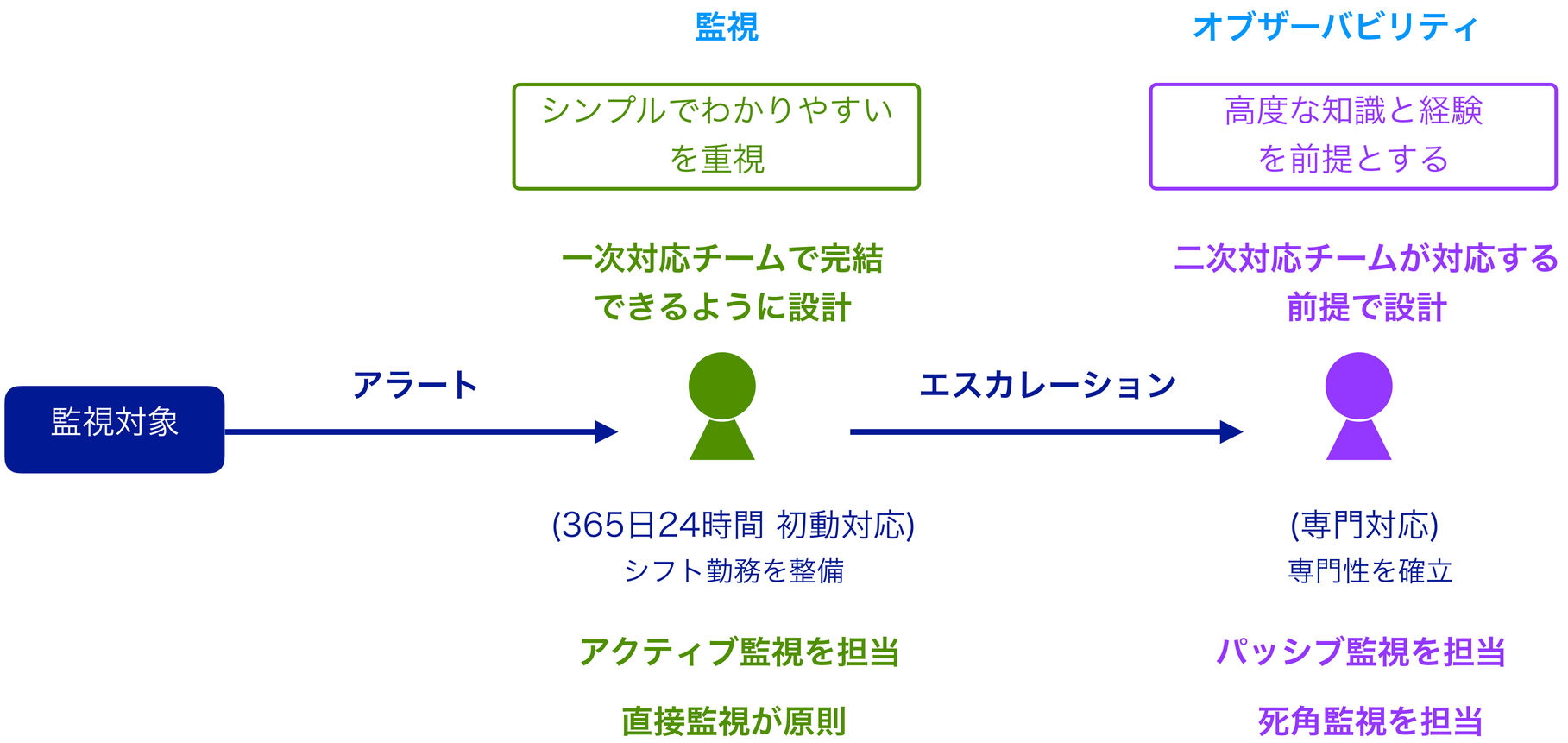
(専門対応)
属人(専門性依存)を想定

パッシブ監視を一次チームから分離

死角監視を一次チームから分離

今後の監視 (ステップ2: オブザーバビリティの確立)

エスカレーション先を二次チーム(オブザーバビリティ担当)として整備する



まとめ: 今後の監視

ステップ0: 混在

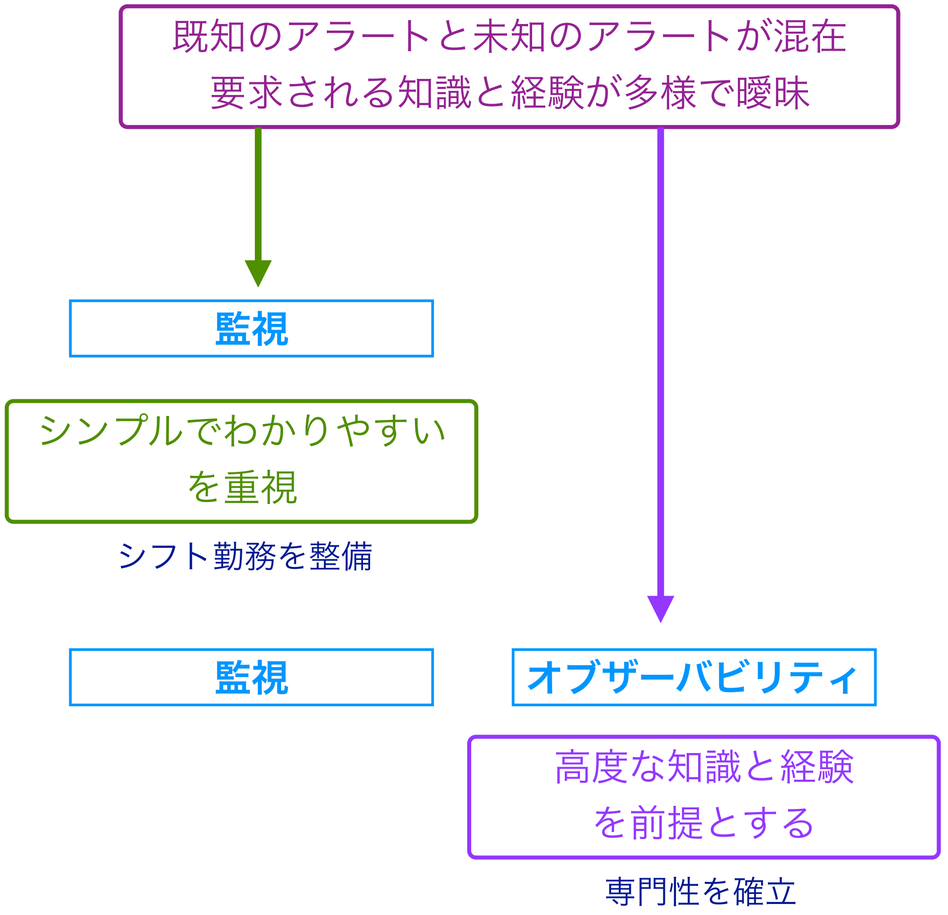
一つの監視チームで全てのアラートに対応

ステップ1: 監視の確立

一次対応チームの対応内容を明確にし、
エスカレーション先を整備する

ステップ2: オブザーバビリティの確立

エスカレーション先を二次チーム(オブザーバビリティ担当)
として整備する



参考: 監視やオブザーバビリティで大事なこと

監視システムと監視運用は一体で設計・運用する

監視システムと監視運用が別部署の所管になると、監視運用に最適化された監視システムとはなりにくい。

監視運用が主であり、そのために監視システムが存在する、と考える。

オブザーバビリティのシステムと運用も同様に考えるべきだが、ステークホルダーが多いため難易度は高い。

「ツールありき」はアンチパターン

ツールは、その目的に沿った用途には効果を発揮するが、万能ツールではない。

まず、どんな運用をするのかが先に必要で、その運用に合致したツールを選択することが大事。

運用が変われば、適したツールも変わっていく。

参考: 過去の発表資料

過去の発表資料は
OpsLab.jp というサイトに置いてあります。

https://www.opslab.jp/publish/

Operation運用設計Lab

http://www.operation-lab.co.jp/