運用プロセスを1つにすっきりまとめたい

2019.7.26 JANOG44 武井

自己紹介

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - JNSA 日本ネットワークセキュリティ協会
  - ISOG-J 日本セキュリティオペレーション事業者協議会
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6) リーダー
- JANOG歴：39、42 BoF、43 ハッカソン運営委員
- NTTテクノクロス株式会社
  - セキュアシステム事業部　第三ビジネスユニット　勤務
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル、CISSP、RISS

テーマは「The One」。一つにまとまるためにも先人の知恵を集めたい

- 運用の定義とは
- 運用におけるプロセス
- 自動化と成熟度の関係
- プロセスとスキル

前回もなんかやってましたよね？

- はい。SPで10分1本勝負で課題提起のみでした
- 今回はより具体化し、みなさんとの議論をしたいです

で、「運用」ってなに？
（半年ぶり2度目）

近いのはあった（ありがとうIPAさん）

技術参照モデル(TRM)第5章「技術ドメイン解説」クイックリファレンス

https://www.ipa.go.jp/files/000025495.pdf

5.9.運用管理

運用管理とは、主にコンピュータ上で稼動し、様々なサービスを提供しているシステムが、想定外の要因によって停止することなく利用顧客に対してサービスを提供できるよう当該環境を維持管理することである。

InternetWeekで見た（ありがとうInternetWeek2018）

https://www.nic.ad.jp/iw2018/program/s11/
S11 価値ある運用とは何か～流行に惑わされない運用の本質を学ぼう！～
運用の価値とロールモデル / 波田野 裕一(運用設計ラボ合同会社)
運用の価値に影響を与える最近の流れ / 藤崎 正範(株式会社ハートビーツ)
価値ある運用とは何か ～具体的な事例に学ぼう～ (パネルディスカッション)
(上記2名に加えて)
松本 哲(弥生株式会社 技術フェロー)
坂部 広大(ウォンテッドリー株式会社 インフラチーム リーダー)
宇野 素史(株式会社クララオンライン)

敬称略

どうやらこんな感じ

- IPA的には：様々なサービスが、想定外の要因によって停止することなく利用顧客に対してサービスを提供できるよう維持管理することである

- 波多野さん：「サービスを継続的にデリバリすること」
  - 「運用組織のリソースを活用し、対価や評価を得ることを目的に、外部に対して、継続的に何らかのサービスを提供し続けること。」
  - 連載：現場視点からの運用方法論　第3回 明日の運用現場のために – 運用フレームワークという視点
  - https://thinkit.co.jp/story/2010/12/16/1934?page=0%2C2

オペレーションとは/オペレーションの定義

「組織、各種システム、アプリケーションなど対象となるものが、あらかじめ定められた あるいは、期待されている（想定されている）機能、性能を発揮／達成する状態を維持･管理する行為」

であり、

セキュリティオペレーションは、

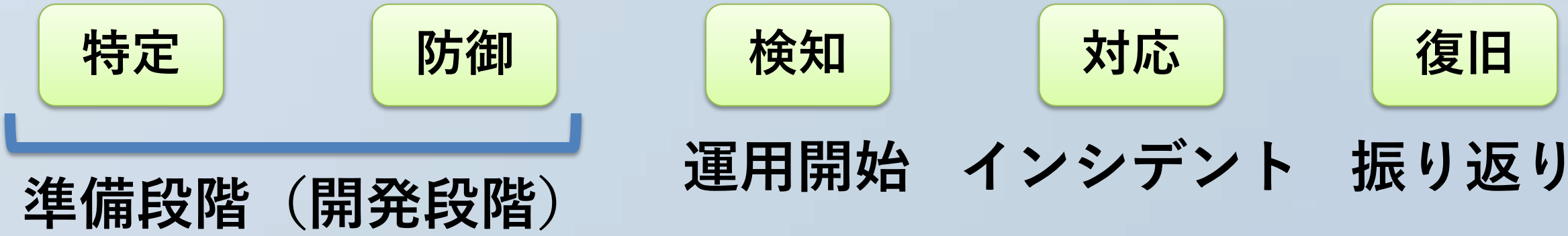
「あらかじめ定められた あるいは、期待されている（想定されている）機能、性能」の部分が、

「あらかじめ定められた あるいは、期待されている（想定されている）セキュリティに関わる機能、性能」

となる。

セキュリティで語られるフレームワークと運用

- よく語られるサイバーセキュリティフレームワーク
  - NIST https://www.nist.gov/cyberframework
  - v1.1日本語版 https://www.ipa.go.jp/files/000071204.pdf



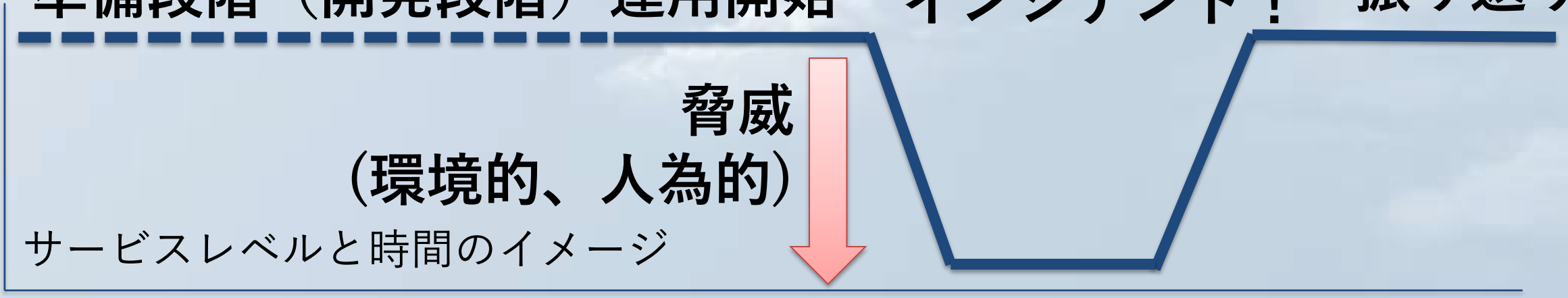
各機能の概要

機能	概要	詳細
特定 (Identity)	システム、人、資産、データ、機能に対するセキュリティリスクの管理に必要な理解を深める	「資産管理」「ビジネス環境」「ガバナンス」「リスクアセスメント」「リスクマネジメント戦略」
防御 (Protect)	重要サービスの提供を確実にするための適切な保護対策を検討し、実施する	「アイデンティティ管理とアクセス制御」「意識向上およびトレーニング」「データセキュリティ」「情報を保護するためのプロセス及び手順」「保守」「保護技術」
検知 (Detect)	サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施する	「異常とイベント」「セキュリティの継続的なモニタリング」「検知プロセス」
対応 (Respond)	検知されたサイバーセキュリティインシデントに対処するための適切な対策を検討し、実施する	「対応計画の作成」「コミュニケーション」「分析」「低減」「改善」
復旧 (Recover)	レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティインシデントによって阻害されたあらゆる機能やサービスを元に戻すための適切な対策を検討し、実施する。	「復旧計画の作成」「改善」「コミュニケーション」

サービスレベルと時間のイメージ、脅威の違い

特定　防御　検知　対応　復旧

準備段階（開発段階）　運用開始　インシデント！　振り返り



脅威

人為的：意図的な攻撃、偶発的な操作ミス

セキュリティの運用で多い

環境的：偶発的な障害、災害や故障

システムやネットワークの運用で多い

これ、うまく重ならないかな

（大目的）
サービス・業務の継続

特定　防御　検知　対応　復旧

システム

ネットワーク

セキュリティ

（後続の何か……）

前段階も大事

特にこの辺の連携

InternetWeek2018でのひとこま

- Q:各分野の人たちと**連携した運用**のために、「刺さる言葉」とか概念とかないですか？

- A:「刺さる言葉」ではなく、**論理的なプロセスや論理的に語れる**方が大事

運用の自動化について

- 運用の自動化、ホットトピックですね。
- 「運用」の指す言葉の意味が広すぎて議論が噛み合いにくい
- 運用に関わっている度合いによっても議論が噛み合いにくい

能力成熟度モデル統合(CMMI)を参考に

- CMMI(Capability Maturity Model Integration, 能力成熟度モデル統合)
- 運用自動化はレベル4～5くらいで、結果的に利用されるもの？

レベル

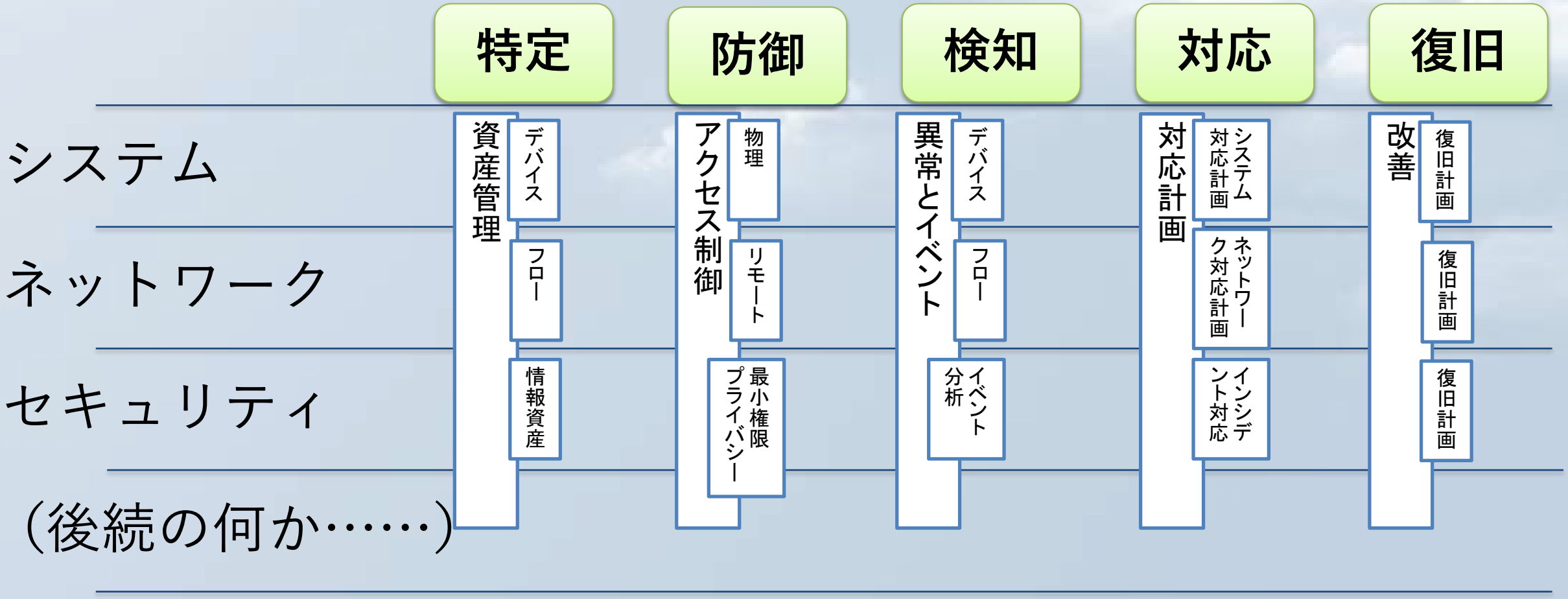
1：プロセスが確立されていない	初期段階
2：特定のプロジェクトリーダーや技術者に依存している状態	管理された
3：首尾一貫したプロセスを標準として持っている段階	定義された
4：標準化されたプロセスを定量的に測定し、洗練化していく状態	定量的に管理された
5：技術・要件環境の違いによって、標準プロセスを最適化して用いられる段階	最適化している

運用自動化の議論のために

- プロセスにおいて、どの範囲の業務なのか？
- 現在の運用の成熟度はどのレベルなのか？
- 運用の自動化が目的になっていないか？

プロセスとスキル

- 分野とプロセスを横断的にスキルマップができないか



(参考) JNSA セキュリティ知識分野(SecBok 2019) https://www.jnsa.org/result/2018/skillmap/

これが整理できれば……

- どんなスキルがあれば、何ができる がわかる
- 次にこのスキルを身につければ、「これ」ができる がわかる

- ある分野だけで足りる足りないの話ではなく、運用全体として人材を確保、ローテーションできるのでは

「統合運用センター」のようなもの

- システム運用、ネットワーク運用、セキュリティ運用を別々にやらない

- まとめて1つにして、リソース（人員、予算、時間）を取り合うのではなく効率的に

テーマは「The One」。一つにまとまるためにも先人の知恵を集めたい

- 運用の定義とは
  - サービスや機能を維持・管理して、継続的に提供する
- 運用におけるプロセス
  - サイバーセキュリティフレームワークを例に
  - 共通の認識で、論理的な連携ができるようにしたい
- 自動化と成熟度の関係
  - どのプロセスのどの部分の話になるかを明らかにしたい
- プロセスとスキル
  - 人材は統合的な運用センターでずっと育てたい

議論したいこと

- このような整理について、これまで他の方法論や手法があったかどうか？
- それが現在までに活用されている事例や成功例はあるか？
- 成功していないのであれば、既存の手法はどう改善すべきなのか？