第38回 システム監査学会 研究大会

システム管理基準に基づく アジャイル開発・DevOps監査 のガイダンス

2024年6月14日

「先端領域におけるシステム監査のベストプラクティス」
研究プロジェクト

三井住友銀行/三井住友フィナンシャルグループ
佐藤　稔
CISA,CIA,システム監査技術者

この資料の内容は、発表者を含む研究プロジェクトメンバーの見解であり、メンバーの所属組織等とは関係ありません。

目次

1． 本研究プロジェクトの紹介

2023年4月の「システム監査基準」「システム管理基準」の改訂内容を踏まえ、対象外の先端領域を対象に監査着手時の「きっかけ」を得るべく、2024年1月から活動開始しました。

名称	先端領域におけるシステム監査のベストプラクティス
開始	2024年1月より
終了	主要な先端領域を対象とした検討が終わるまで。現時点で未定
運営	原則、月に１回、Zoomで開催（完全非対面。約90分）
主査	佐藤 稔（詳細は次葉）。ただし、本研究プロジェクトから初めて当学会に加入
特徴	システム監査人協会の方も参画していること …現時点で存在しない先端領域のガイドラインの検討と関係が深いため
メンバー	全16名（主査、NPO法人 日本システム監査人協会の方も含む）

2．発表者紹介

三井住友銀行監査部に13年間所属。システム監査の領域に専ら従事し、その間、グループ長⇒担当部長と管理職も経験、現在に至っています。

佐藤　稔

1990年	三井住友銀行　入社
2011年迄	主にホールセール部門で業務企画に従事
2011年4月	監査部システム監査グループ
2022年4月	監査部システム監査担当部長
2024年4月	監査部ＩＴ監査担当

保有資格	ＣＩＳＡ、ＣＩＡ、ＡＵ、ＣＡＭＳ、ＣＩＳＭ、等

3．研究目的

本プロジェクトの目的は、現時点で確立された国際標準やベストプラクティスが存在しない先端領域をどのように監査すべきかを明らかにして、システム監査に貢献することです。

2023年4月に経済産業省が「システム監査基準」「システム管理基準」を改訂。但し、リスクの変化が著しい先端領域は対象外

一方、先端領域に関する文献は種々。監査に使える内容を探す必要がある

先端領域に対してどのようにシステム監査をすべきかを明らかにすること。
成果物は、先端領域のリスクに応じた監査着手時の「きっかけ」になるもの

但し、本領域では標準やベストプラクティスは未確立 ⇒
唯一の正解ではなく、変化する状況に適応し随時更新することを、目指す

システム管理基準をベースにリスクとコントロールを明確化
（DevOpsの場合。他の先端領域では領域に適したアプローチを検討）

４．現状報告：DevOpsに関するシステム監査要領（案）
(1) システム管理基準におけるDevOpsの位置づけ

本プロジェクトの先行事例にすべDevOpsを対象として、システム監査要領（案）を検討中です。その第１歩は、DevOpsを、定義等からシステム管理基準で位置づけすることです。

定義

DevOpsは、従来、分業・分断されていた開発（Dev）と運用（Ops）の担当者がそのシステムやサービスのビジネスゴールを共有し、テスト・構成管理・デプロイ等をできる限り自動化することで、スピードと品質を担保したうえで、柔軟かつ迅速な開発を目指す。

IPA(2023), DX白書, p.254, https://www.ipa.go.jp/publish/wp-dx/dx-2023.html

留意点

- アジャイル開発とDevOps（DX白書2023より抜粋）
  「ビジネス変化と開発スピードのギャップ」⇒アジャイル開発
  「スピードを上げたい開発部門と安全性・安定性を重視する運用部門とのギャップ」⇒DevOps
- 開発と運用の職責分離

位置づけ

システム管理基準における、「システムライフサイクルの改善の取組」

４．現状報告：DevOpsに関するシステム監査要領（案）
(2) DevOpsに関するシステム監査要領

DevOpsの定義からリスクを特定。これにDevOpsに関する各種文献を参考に、コントロール（管理活動）を例示。システム監査要領はこのリスク＋コントロールの構成を目指しています。

リスク

- 開発と運用で、ビジネスゴールが共有されない。
- 柔軟かつ迅速な開発が実現できず、スピードと品質が担保されない。

コントロール（例）

① 作業をみえる化し、無駄を省く
② 専任のチームを組成する
③ 目標と期限を経営陣が承認し、すべての関係者に周知する
④ 開発、テスト、本番の各環境を必要な時に用意できるようにする
⑤ 一貫性のあるライブラリ管理システテを構築する
⑥ 高速で信頼性の高い自動テストを実現する
⑦ 目標の達成状況を可視化するデータを作り出し、継続的にモニタリングする
⑧ 組織内で情報を共有する

参考文献

- ジーン・キム（著）、ジェズ・ハンブル（著）、パトリック・ドボア（著）、ジョン・ウィリス（著）、榊原彰（監修）、長尾高弘（訳）、The DevOps ハンドブック 理論・原則・実践のすべて、日経BP、2017年
- レン・バス（著）、インゴ・ウェーバー（著）、リーミン・チュー（著）、長尾高弘（訳）、DevOps 教科書、日経BP、2016年
- Jennifer Davis, Ryn Daniels（著）、吉羽龍太郎（監訳）、長尾高弘（訳）、Effective DevOps 4本柱による持続可能な組織文化の育て方、オライリー・ジャパン、2018年

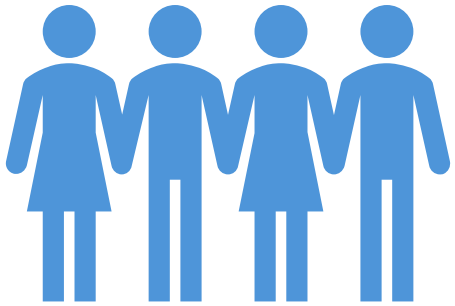
5．今後展開予定の先端領域

DevOpsの他にも、システム監査を検討する際の「きっかけ」になるシステム監査要領を増やす予定です。

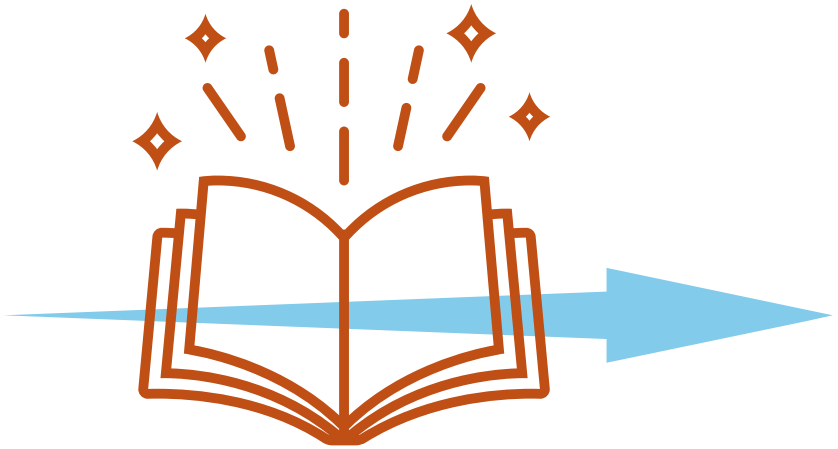
- DevOps（まずはこれから）
- アジャイル開発
- IoTシステム
- クラウドサービス利活用
- オープンソースソフトウェア利活用
- …
- …

5．おわりに

本プロジェクトは、国際基準やベストプラクティスがまだ取り扱っていない領域を対象にし、本研究プロジェクトの成果物は、それら領域の参考文献への導線を作る役割を目指しています。



先端領域のシステム監査を目指す皆さん



本研究プロジェクトの成果物＝
システム監査要領

国際基準（ISO、IEEE等）やベストプラクティス（COBIT、PMBOK等）になっていない、参考文献