

コンプライアンス対応を チームの力に

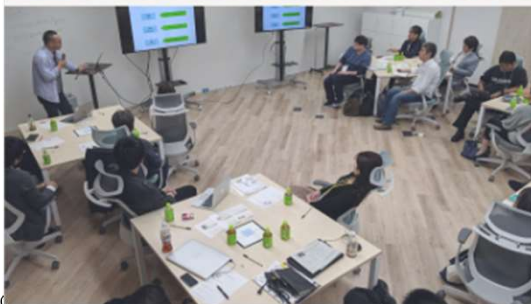
監査人が考える今後のDevOps
2022年4月



岡島 幸男(Yukio Okajima)



永和システムマネジメント
取締役CTO / Agile Studioディレクター



PwC



福井県 CDO補佐官



福井大学 非常勤講師(ソフトウェア工学)

佐藤 要太郎 (Yotaro Sato)

- 監査法人に所属
 - 外部監査/内部監査支援
 - 監査関連のアドバイザリーサービス
- 元Sler
 - アジャイル、DevOpsは当時の憧れ。実践できず。
- カッコイイ
 - “HELPING GEEKS FEEL SAFE IN THE WORLD”
(kentbeck.com)



slido



DevOpsやっていますか？

① Start presenting to display the poll results on this slide.

本セッションのお題

コンプライアンス 対応

DevOpsと衝突しやすいコンプラ対応(例)

タイトル	コンプラ概要	よくある伝統的な対応
職務の分離	アプリケーションやインフラを不適切に変更できないように、職務を分離すること	<ul style="list-style-type: none">アプリケーション開発者と、本番データ修正やリリース作業を行う運用担当者を分離する。兼務させない。
テストと承認	意図した通りの変更が行われるように、適切なテストと承認をおこなうこと	<ul style="list-style-type: none">上長承認を行う<ul style="list-style-type: none">開発計画や本番作業計画工程ごとの中間成果物変更内容のリリース前

slido



「コンプライアンス」のイメージは？

① Start presenting to display the poll results on this slide.

なぜコンプライアンスに対応するのか？

- マーケットから締め出されないようにするために
- 競合他社を一步リードするために

(想定ケース) マーケットからの締め出し



- 規制業界でサービスを提供するプロダクトA
 - 伝統的な、ガチガチのルールでサービスを運営
- サービス利用者の個人情報を、別プロダクトBにも流用
 - 流用することの同意をサービス利用者から取得している
 - プロダクトBの規制は異なるので、“それなり”ルールでサービスを運営
- プロダクトBから漏えいした、プロダクトA利用者の個人情報による犯罪が発生
- 規制当局から行政処分を受ける

(想定ケース) 競合他社を一步リードする

- **住宅ローンA社(レポートの例)**
 - 最近、大企業に買収された。急成長するプロダクトZ
- **親会社内部監査部門によるIT監査**
 - 「職務を分離すること」を含む、いくつかの改善指摘
 - プロダクトZは、サービス改善スピードを落としたいくない
- **伝統的解釈ではなく、DevOpsならではの新たな解釈で対応**
- **競合他社よりも優れたサービス改善スピードを維持**

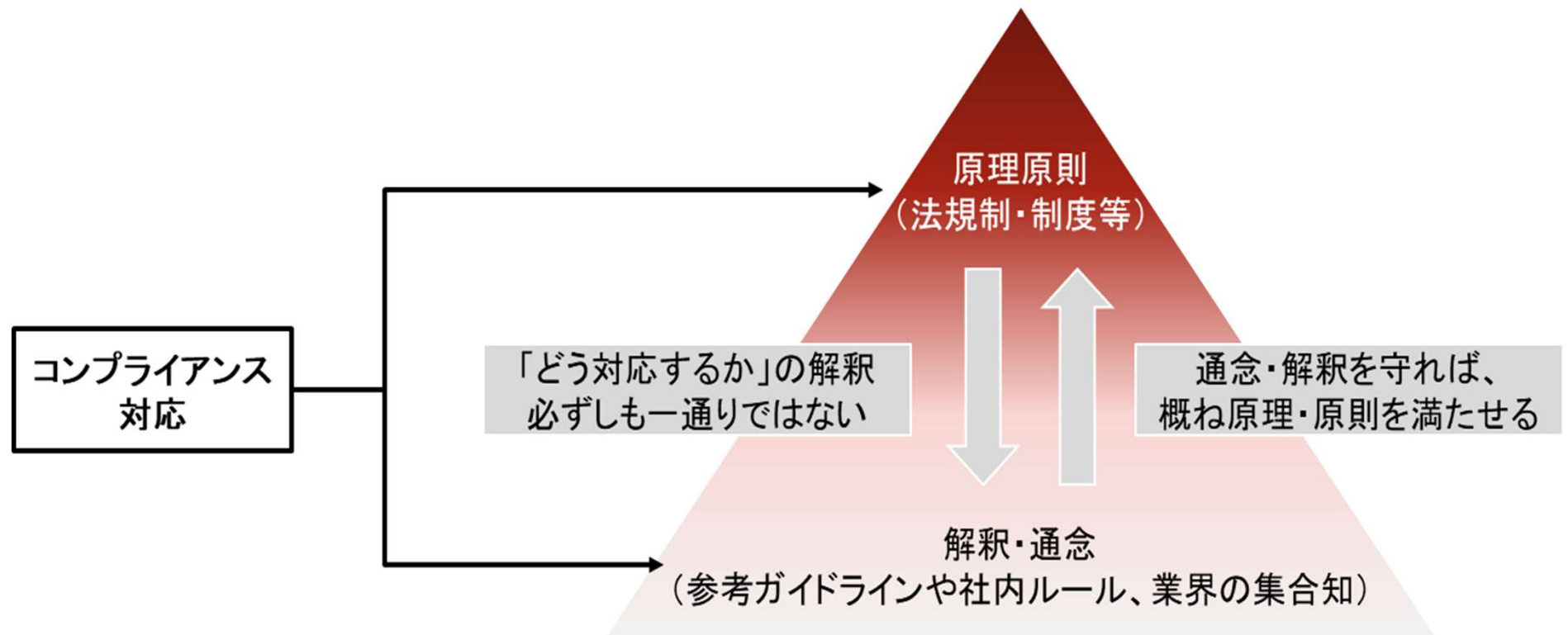


なぜコンプライアンスに対応するのか？

- マーケットから締め出されないようにするために
➡ 広義のビジネス要件。ただし、ユーザーからは出てこない。
- 競合他社を一步リードするために
➡ 伝統的な解釈で対応するとDevOpsと衝突しやすい。工夫する。

そもそもコンプライアンス対応とはなにか？

大元となる原理原則と、実践する上での解釈・通念がある



DevOpsと衝突しやすいコンプラ対応(例 再掲)

タイトル	原理・原則 コンプラ概要	解釈・通念 よくある伝統的な対応
職務の分離	アプリケーションやインフラを不適切に変更できないように、職務を分離すること	<ul style="list-style-type: none">アプリケーション開発者と、本番データ修正やリリース作業を行う運用担当者を分離する。兼務させない。
テストと承認	意図した通りの変更が行われるように、適切なテストと承認をおこなうこと	<ul style="list-style-type: none">上長承認を行う<ul style="list-style-type: none">開発計画や本番作業計画工程ごとの中間成果物変更内容のリリース前

新たな解釈

タイトル

原理・原則 コンプラ概要

職務の分離

アプリケーションやインフラを不適切に変更できないように、職務を分離すること

テストと承認

意図した通りの変更が行われるように、適切なテストと承認をおこなうこと

解釈・通念 新たな対応手法

- ブランチ、パイプラインの保護
- 重要な行為の通知と承認

- リグレッションテストの自動化、パイプラインへの組み込み
- テストスクリプトの構成管理・保護
- パイプライン設定の妥当性確認

実装例

ブランチ、パイプラインの保護

図表10：GitHubブランチ保護設定（両立させるための新たな統制 1）¹¹

Branch name pattern

master

Protect matching branches

☒ Require pull request reviews before merging

When enabled, all commits must be made after approving reviews and no changes requested until the pull request is approved.

Required approving reviews: 1

☒ Dismiss stale pull request approvals

New reviewable commits pushed to a branch will dismiss previous approvals.

☐ Require review from Code Owners

Require an approved review in pull request before merging.

☐ Require status checks to pass before merging

Choose which status checks must pass before merging. All required status checks must pass before a pull request can be merged.

☐ Require signed commits

Commits pushed to matching branches must be signed.

☐ Require linear history

Prevent merge commits from being pushed to matching branches.

☒ Include administrators

Enforce all configured restrictions above for administrators.

図表12：GitHubによるマージボタンのWarning（両立させるための新たな統制 1）

テスト実行中はマージ不可

Some checks haven't completed yet

1 expected, 1 pending, and 2 successful checks

sonarqube — Waiting for status to be reported

Required

continuous-integration/travis-ci/pr — The Travis CI build is in progress

Details

ci/circleci — Your tests passed on CircleCI

Details

continuous-integration/travis-ci/push — The Travis CI build passed

Details

Required statuses must pass before merging

All required status checks on this pull request must run successfully to enable automatic merging.

Update branch

Merge pull request

You can also open this in GitHub Desktop or view command line instructions.

テスト失敗時はマージ不可

Some checks haven't completed yet

1 expected and 3 failing checks

sonarqube — Waiting for status to be reported

Required

ci/circleci — Your tests failed on CircleCI

Details

continuous-integration/travis-ci/pr — The Travis CI build failed

Required Details

continuous-integration/travis-ci/push — The Travis CI build failed

Required Details

Required statuses must pass before merging

All required status checks on this pull request must run successfully to enable automatic merging.

Update branch

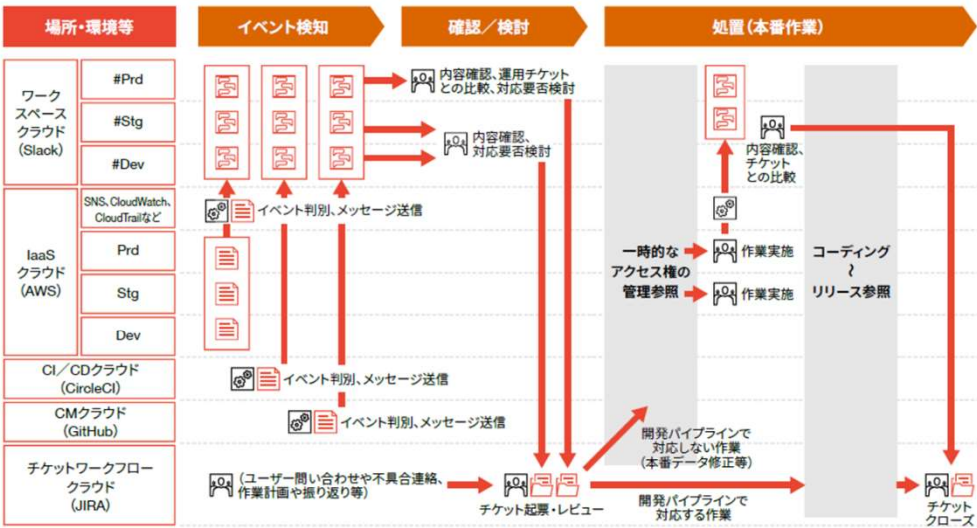
Merge pull request

You can also open this in GitHub Desktop or view command line instructions.

実装例

重要な行為の通知と承認

図表13：システム監視、本番作業（両立させるための新たな統制 3）



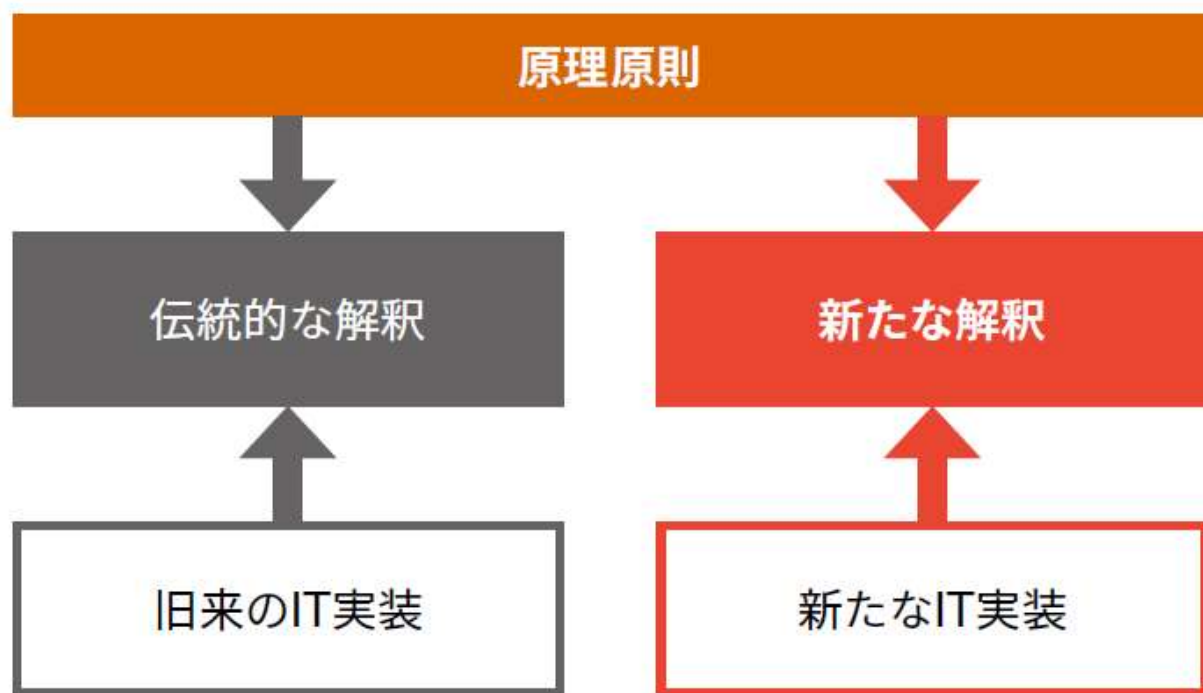
コンプライアンス対応をチームの力に
PwC

図表14：Slackへの通知・確認コメント（両立させるための新たな統制 3）¹²



解釈を再鑄造する


原理原則に対して、DevOpsに沿った新たな解釈を検討する。



✓ いわゆる「IT統制」「ITコンプライアンス」対応の伝統的な解釈は、旧来のIT実装が前提となっている。

✓ 原理原則に立ち返って、新たなIT実装であるDevOps環境のリスクを検討し、新たなコントロールを構築（解釈を再鑄造）する

プロダクトチームの皆様へ

- コンプライアンス対応は、ビジネス要件の一部。ただしユーザーからは出てこない。
 - チームの働き方に関する内容が含まれている。画一的な対応がボディブローのように影響する。
- 
- まるでPBIを起票するように（あるいは実際に起票して）、タイムリーに真正面から対応すべき。
 - そうすることで、「チームならではの」働き方を獲得できる。

slido



プロダクトバックログに書くとしたら？

① Start presenting to display the poll results on this slide.

関連レポート トラストをともに駆ける

<https://www.pwc.com/jp/ja/knowledge/thoughtleadership/dev-ops220228.html>

具体的なケースを交えて「DevOpsのコンプライアンス対応」を検討しています。

トラストをともに駆ける

——DevOpsにおけるコンプライアンス対応の要所

目次

はじめに	3
DevOpsとは	4
コンプライアンス対応とは	6
ケース設定	9
要件#1 職務の分離への対応	12
要件#2 テストと承認への対応	19
要件#3 アクセス権を必要最小限に保つ対応	22
推奨事項 可監査性の確保への対応	26
解釈を再構築する	28
おわりに	29

コンプライアンス対応をチームの力に
PwC

永和システムマネジメント

永和システムマネジメントは、日本において、2000年からアジャイルソフトウェア開発を実践しております。コーチング・教育・エンジニアリングを得意とする専門家チームが、金融・医療・組込みなど幅広い事業分野に対しサービスを提供しています。2018年には、アジャイル開発拠点である Agile Studio を創設し、技術的卓越性によってお客さまと共に成長できる、共創・共育型のビジネスとソフトウェアづくりを推進中です。Agile Studio は随時リモート無料見学会を実施しており、これまで1,000人以上の方がアジャイルなソフトウェア開発の現場を体験されています。詳しくは、agile-studio.jp をご覧ください。



平鍋 健児
代表取締役社長



岡島 幸男
取締役CTO/
Agile Studio
ディレクター



村上 雅彦
Agile Studio
エンジニア

PwCあらた有限責任監査法人

PwCあらた有限責任監査法人は、PwCグローバルネットワークのメンバーファームとしてデジタル社会に信頼を築くリーディングファームとなることをビジョンとしています。世界で長年にわたる監査実績を持つPwCネットワークの監査手法と最新技術により世界水準の高品質な監査業務を提供するとともに、その知見を活用した会計、内部統制、ガバナンス、サイバーセキュリティ、規制対応、デジタル化対応、株式公開など幅広い分野に関する助言（ブローダーアシュアランスサービス）を通じて社会の重要な課題解決を支援しています。



宮村 和谷
パートナー



佐藤 豊太郎
シニアマネージャー



伊藤 英毅
シニアマネージャー



横山 和典
マネージャー



小田切 洋介
シニアアソシエイト

2022/04/11

20

slido



Audience Q&A Session

① Start presenting to display the audience questions on this slide.

Github.comで、ご意見をお待ちしております。

<https://github.com/PwC-Aarata-SPA/DevOps-and-Compliance>

Thank you

www.pwc.com/jp

© 2022 PricewaterhouseCoopers Aarata LLC. All rights reserved.

PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.