

社内セキュリティチェックリストのAWS前提での書き直しと、 リストに準拠した自動チェックの実装

JAWS FESTA 2024 in 広島

ダイキン工業 TICデータ活用推進G 角田潤也

自己紹介

角田 潤也 (Junya Tsunoda)

- ダイキン工業株式会社 テクノロジー・イノベーションセンター(R&D)
- 実行支援チーム(ITインフラ整備/セキュリティ整備/開発チーム支援)

業務: R&DのAWSアカウント100超を管理



↑をAWS Control Tower/**Config**/CDK/(GitHub)等で効率化したい

経歴:

- 2019年: 新卒入社(工学部 非情報系)
- ~2020年度上期: ダイキン情報技術大学
- 2020年度下期: AWSベンダーに長期出張
- 2021年度~: 現所属に(現在6年目)

ダイキン工業をあらわすキーワード

創業**1924**年
100年の歴史

人を基軸に
おく経営

空調機器と冷媒を
両方手がけている
総合空調メーカー

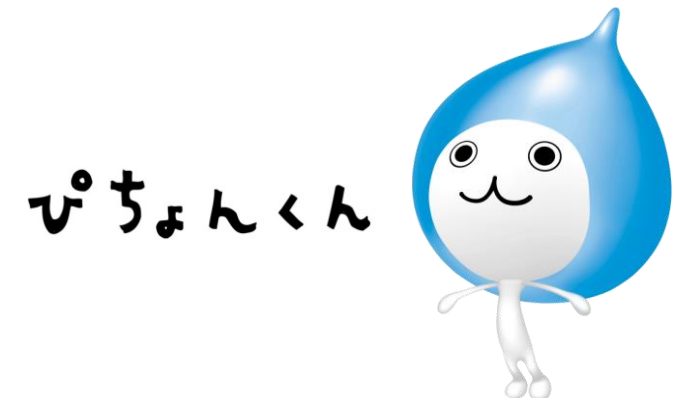
グローバル生産拠点
110カ所以上

全社売上高
4兆円以上

従業員**9.6**万人
海外従業員比率は8割以上

170カ国以上へ
事業展開

海外売上高比率
85%



社内外との協創を通じたイノベーションの加速

技術開発拠点 テクノロジー・イノベーションセンター(TIC)



- 総床面積: 約5.8万㎡、6階建て
- 所在地: 大阪府摂津市(当社淀川製作所内)
- 投資額: 約380億円
- 開所: 2015年11月25日
- 人員数: 700人規模

産学・研究機関と新たな空気価値創造の取り組み



東京大学

「**空気の価値化**」を実現する未来技術やビジネスモデルを東京大学の教員陣3,000人や東大発のベンチャー企業群とともに創出し社会実装する

大阪大学

「**ダイキン情報技術大学**」を設立、AI・IoT人材を大阪大学教員と共に育成。また、新キャンパス(箕面)を舞台に次世代スマートビルの実現もめざす

京都大学

「**ニューノーマル時代を見据えた研究開発テーマ**」を掲げ、ヘルスケアやエネルギーからアジア・アフリカ地域研究まで幅広い領域で成果創出に取り組む

他社との主な取り組み

日立製作所

ものづくりに必要な「**技能伝承**」にAIを活用。品質の安定や生産性向上、人材育成を推進



Point0

異業種20社以上で知的生産性向上を実現する「**未来のオフィス空間**」づくりをめざした『CRESNECT』プロジェクトの一環。パナソニック、オカムラ、ライオン、TOTOなどの社員が中心となり、IoTを駆使してサービスを開発



本セッションで話すこと

■社内セキュリティチェックリストのAWS前提での書き直し

- なぜ書き直しが必要だったか？
- リストを「誰でも一定の基準で対応できるよう改修」するために、何をしたか？

■リストに準拠した自動チェックの実装

- なぜ自動チェックが必要だったか？
- 自動チェックになぜカスタムルールが必要か？
- カスタムルールをAWSマネージドサービスで実装・運用する方法の概要

■話さないこと

- カスタムルールのロジック記述方法の詳細
 - 別のイベントで話しています
- [CLOSING EVENT – Cloud Operator Days Tokyo 2024 \(cloudopsdays.com\)](https://cloudopsdays.com)



Deep Dive CloudFormation Guard

～社内ルール準拠のAWS自動チェック～

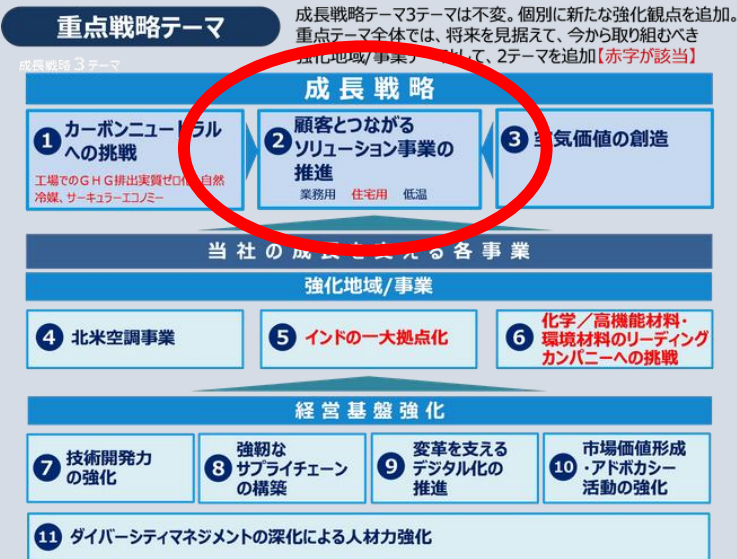
Cloud Operator Days Tokyo 2024

ダイキン工業 TICデータ活用推進G 角田潤也

なぜ、社内セキュリティチェックリストの書き直しが必要だったか？

背景①クラウド活用の高まり

- 5か年計画が「ソリューション」中心
- クラウド上で俊敏に開発したい



背景②「ダイキン情報技術大学」出身の若手が開発

- 新入社員が2年間「企業内大学」でITを学ぶ
- 400人↑が修了、今までITと縁がない部署にも配属される

「DX銘柄2023」が映すデジタル企業の勘所 + 特集をフォロー

通常業務を2年間免除、ダイキンは企業内大学で「IT型人材」を徹底育成

渥美 友里 日経クロステック/日経コンピュータ

通常業務を2年間免除、ダイキンは企業内大学で「IT型人材」を徹底育成 | 日経クロステック(xTECH) (nikkei.com)

はたして「タダ飯食らい」だったのか、ダイキンのAI社内大学がもたらしたもの

(第1回) 400人の修了生と現場のベテランが融合し、必然的にDXが進む

はたして「タダ飯食らい」だったのか、ダイキンのAI社内大学がもたらしたもの | Japan Innovation Review powered by JBpress (ismedia.jp)

全社IT部門の作成した、社内基準とのギャップ

オンプレミス前提で書かれた、有識者でないとわからないリスト

AWSの場合、読み替えが必要

若手が読むと誤読のリスクあり

リストをどう書き直すか？

オンプレミス前提で書かれた、有識者でないとわからないリスト

AWSの場合、読み替えが必要

若手が読むと誤読のリスクあり



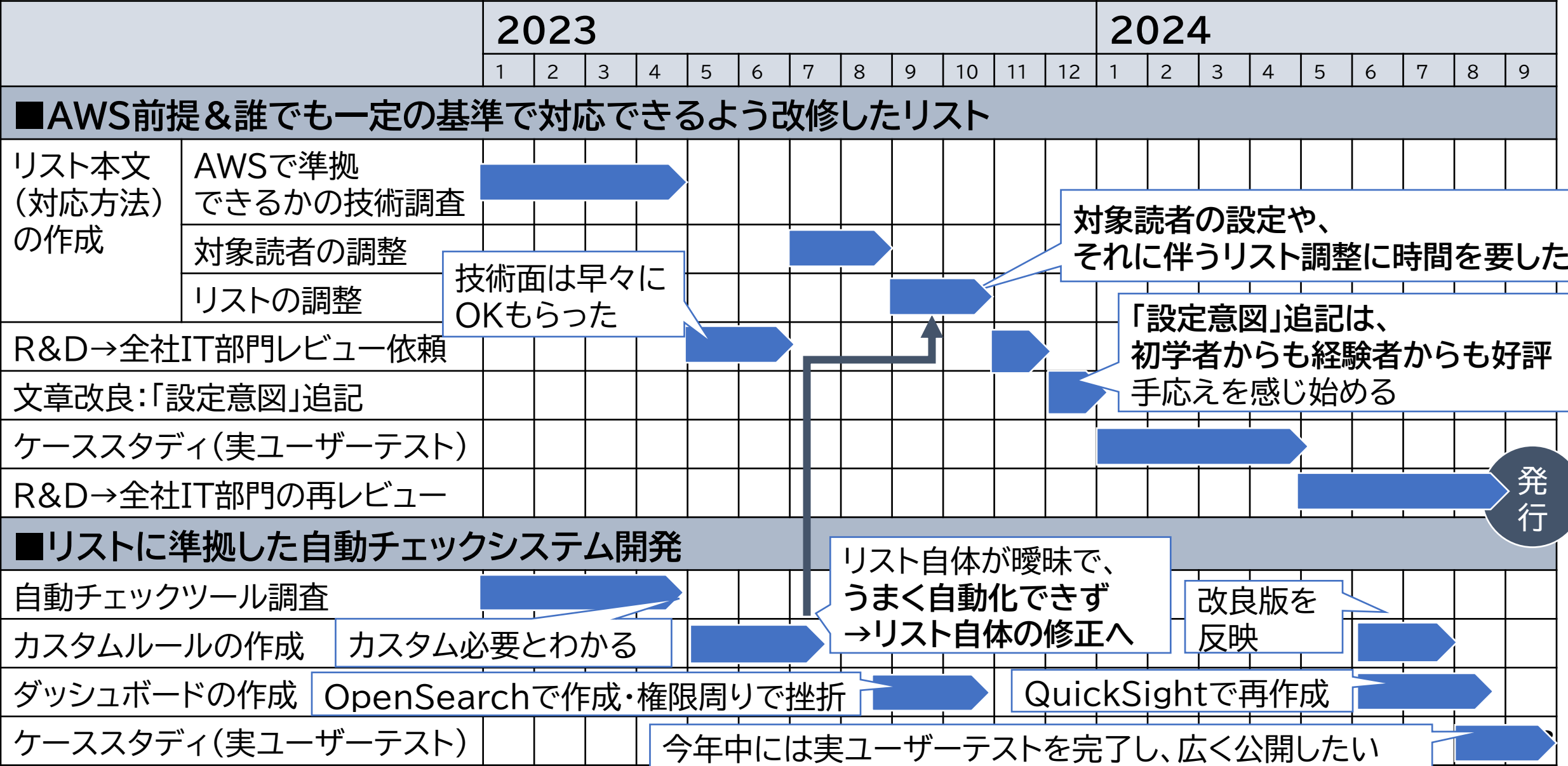
- AWS前提 & 誰でも一定の基準で対応できるリスト
- リストに準拠した自動チェックシステム

必要な理由は後述

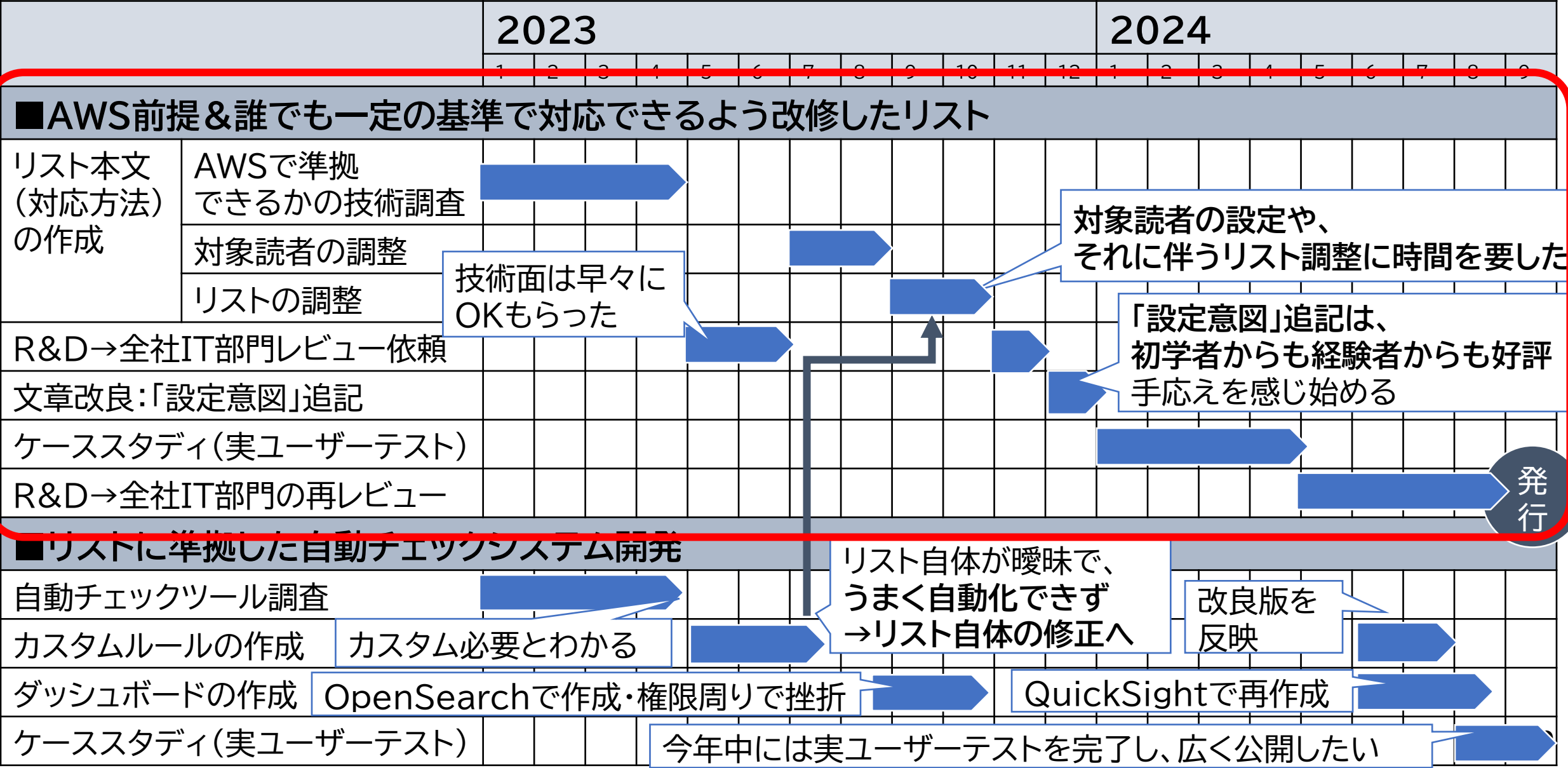
を
作成し、社内に普及させたい！

今回は、Webアプリケーションを対象にしたリストについて上記作業を実施
(「ダイキン情報技術大学」人材が一番よく使うリスト)

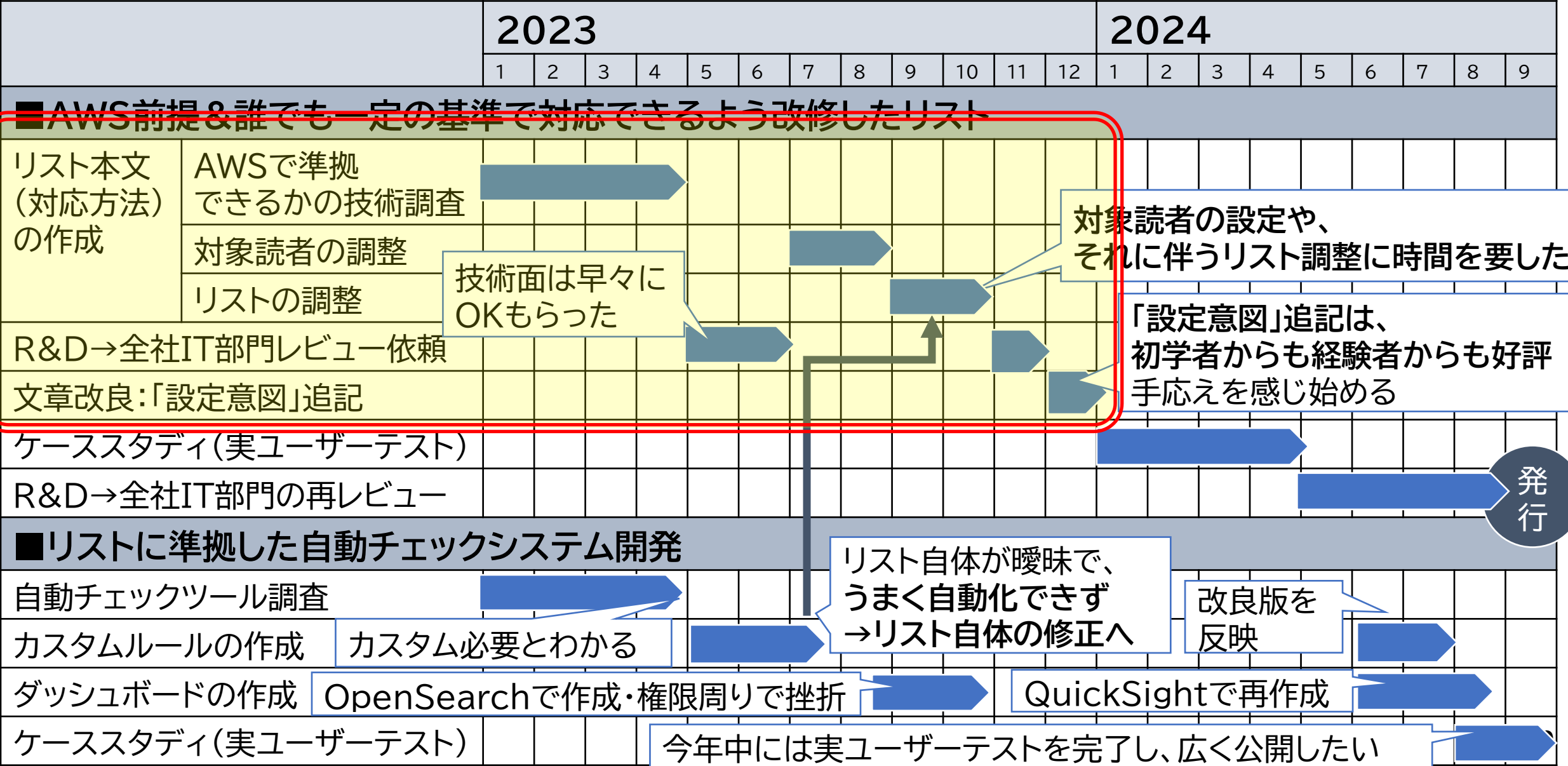
社内向けリリースまでの道のり



社内向けリリースまでの道のり



社内向けリリースまでの道のり



「誰でも一定の基準で対応できる」リストを実現する2つの柱

①

抽象度を下げて、
AWSでの具体的な内容(設定方法や設計意図)を記載

②執筆体制の強化

①抽象度を下げて、AWSでの具体的な内容(設定方法や設計意図)を記載

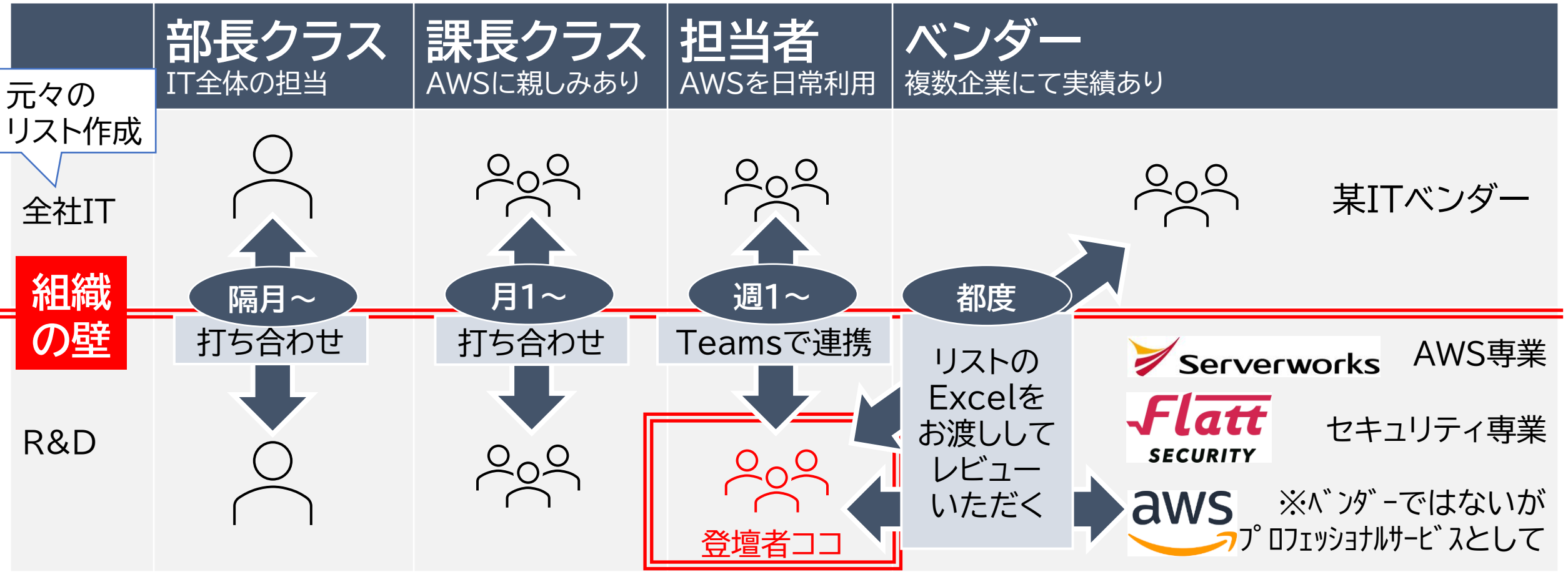
元リスト	
項目	補足
オンプレ/クラウドに共通する概要のみ記載	
通信路を暗号化しているか？	重要情報を送受信する場合は、サーバとクライアントの間の通信を暗号化する。 TLSに利用するサーバ証明書は信頼できる機関から発行されたものを利用することが望ましい。

社内の利用状況を基に、主要サービスを中心に対応			
CDN/ゲートウェイ	ALB	CloudFront	...
サーバー・フロント	EC2/ECS	Lambda	...
認証	Cognito	...	
データベース・ストレージ	S3	DynamoDB	...

AWS版リスト				
1.規則	2.規則を遵守するための選択肢	3-a.各選択肢毎の実施事項 概要	3-b.補足	4.規則を設定した意図
インターネット上の全てのHTTP通信において、HTTPSによる暗号化を有効にしているか？	①新規構築の場合、各サービスにて、〇〇〇〇以上での暗号化通信のみを許可する。 ②...	①HTTPS化手順は... ・ALB:<略> ・CloudFront:<略> ...	②で...	インターネット上の通信経路においては、通信データ盗聴リスクがあるため、暗号化が望ましいため、インターネット上の通信経路の全暗号化を推奨する。 ■全暗号化を推奨する理由 ・AWSではマネージドサービスの活用により、比較的容易にインターネット上の通信経路を暗号化することができる。
具体的なAWSサービス名を記載 文量こそ増えたが、対応しやすさは向上			設定意図を記載 内容が腹落ちした状態での対応が可能	

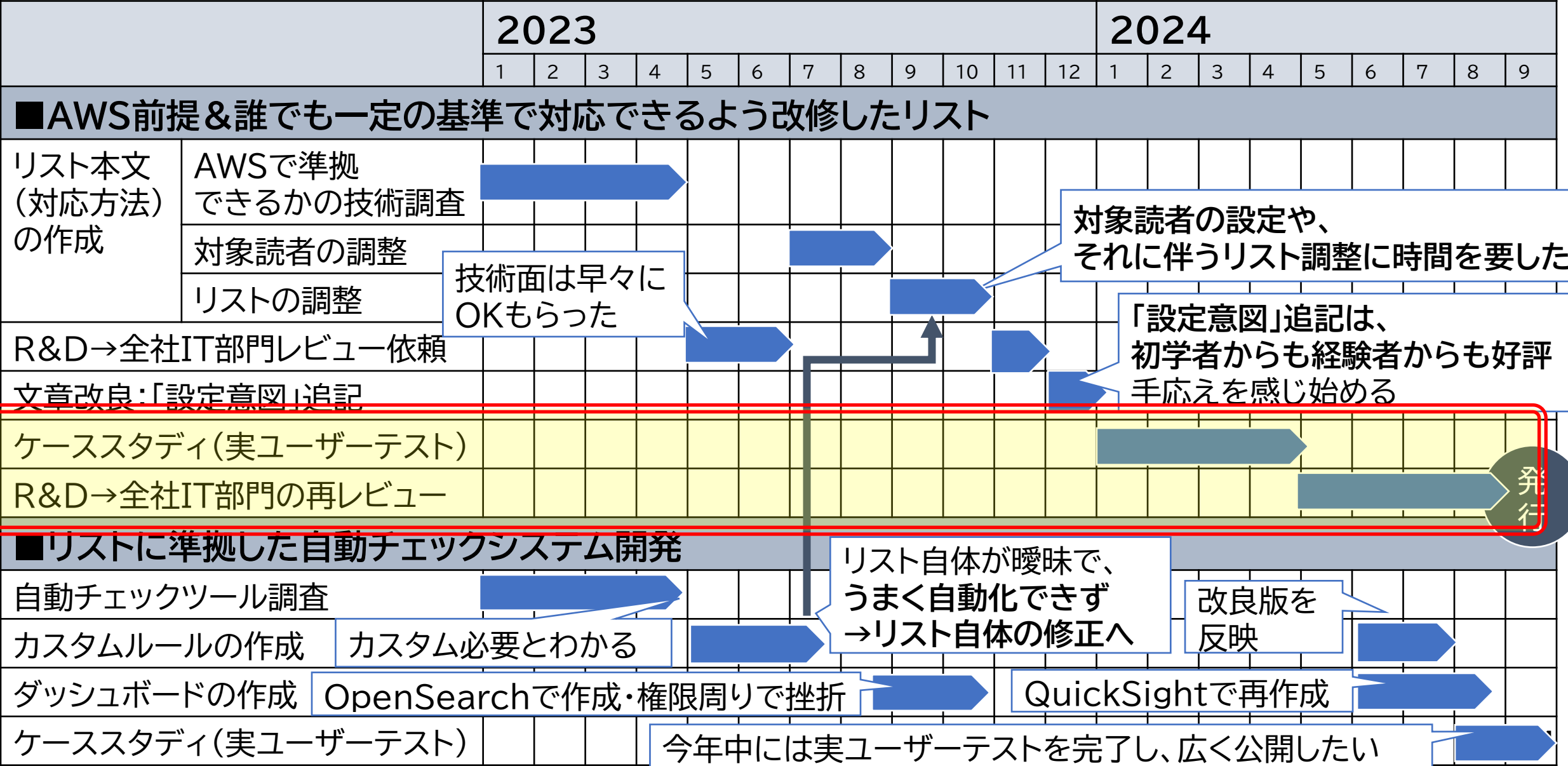
試行錯誤の末、このスキーマに

②執筆体制の強化



元々のリストを作成した全社IT部門と、
前提のすり合わせ / 進捗の共有 / 各組織でキャッチした利用者の声の反映 を行った 13

社内向けリリースまでの道のり



ケーススタディで何を行ったか

■対象: R&D部門で運用しているシステム2件 + 事業部で運用しているシステム2件

以下条件に基づき選定した

- 「ALB+EC2」か「CloudFront+S3」のどちらかを採用するWebシステムを対象とする
- 若手のみで開発するシステムと、中堅含めて開発するシステムの両方が対象になるようにする

■評価箇所

実テーマにリストを適用し、テーマ担当者が以下で困らないかを見てもらう

- 「AWS前提 & 誰でも一定の基準」を満たす上で、文章構成・表現の誤りや不足がないか
 - 具体例①: セキュリティ施策の誤読にともなう、誤った対応をしないか
 - 具体例②: リストの文章が正しいかだけでなく、読みづらさを感じないか

■実施結果

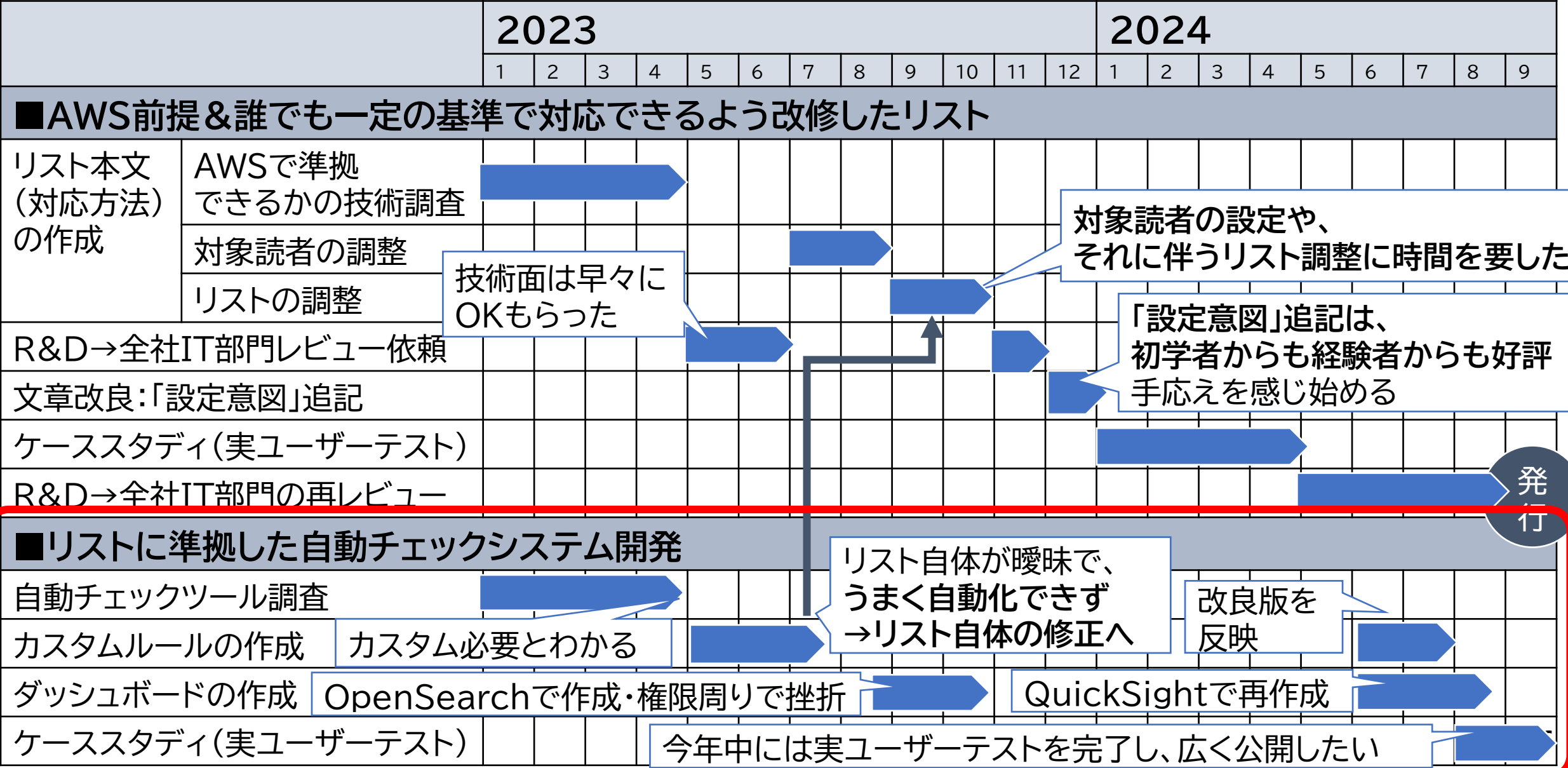
多数の指摘を頂いた。

実際のテーマに適用しないと見えない粗がある。

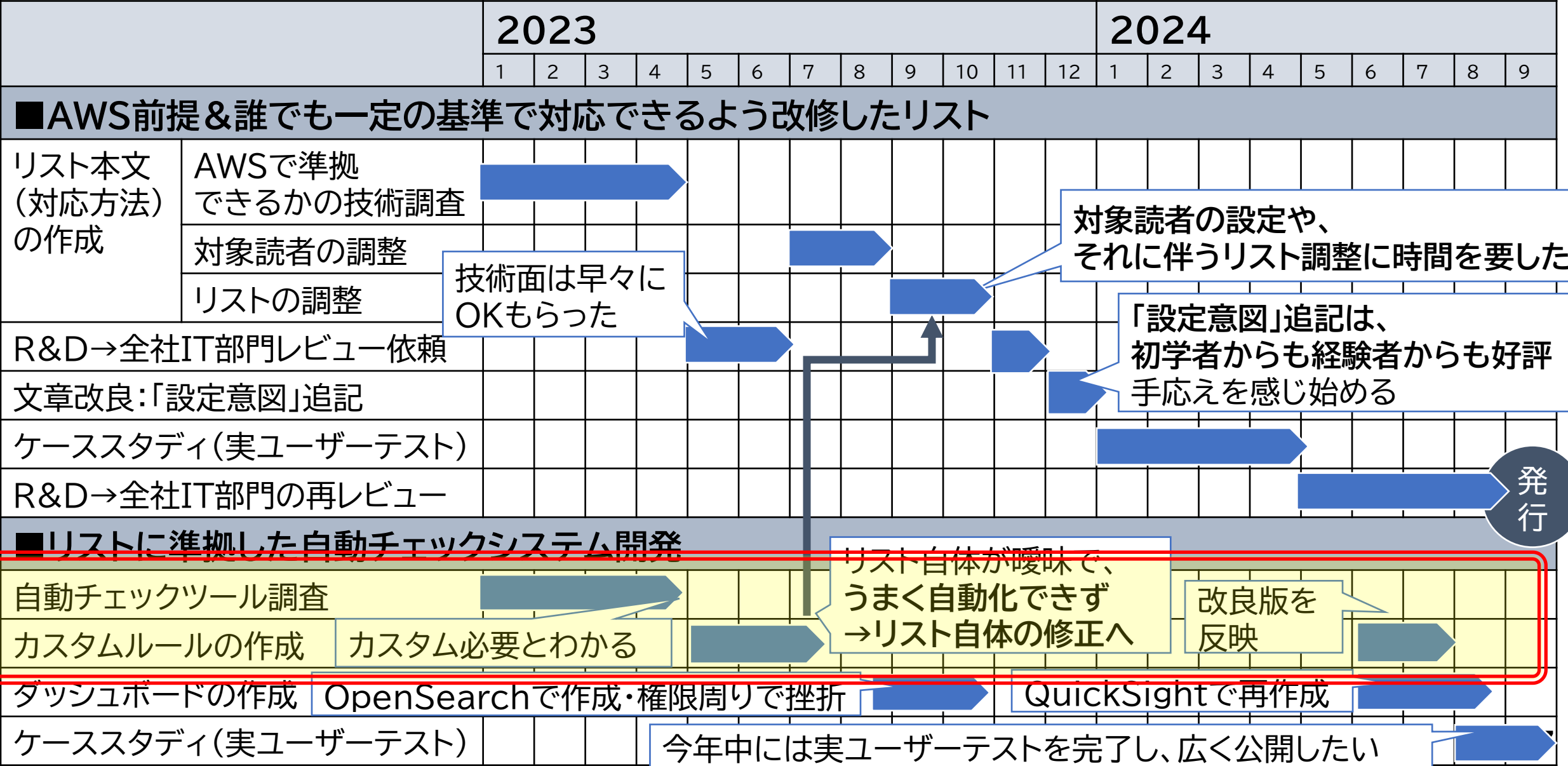
時間はかかった(4か月)が、非常に重要な取り組みだった

重要度	割合	誤る可能性	詳細
大	8%	高	• 誤った施策が記載されており、誤った施策を実施してしまう
中	41%	中	• 誤りはないが、意図が分かりづらく、誤った対策を実施してしまう。 • 誤りはないが、判断基準がないため、誤った対策を実施してしまう
小	51%	低・なし	• 誤字、脱字、情報不足で追加の情報を与える必要がある

社内向けリリースまでの道のり

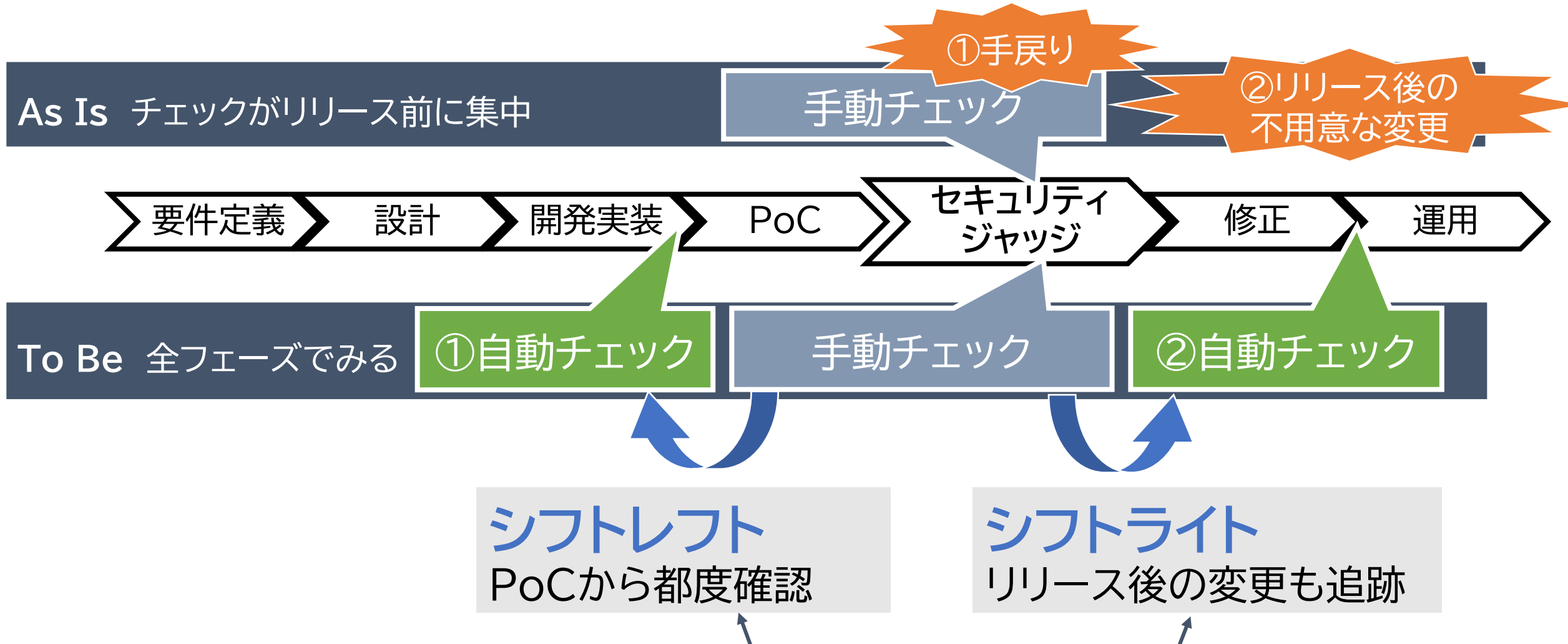


社内向けリリースまでの道のり



なぜ自動チェックが必要か

R&D部門の課題: 開発フロー内で、いつ社内ルールの準拠状況をチェックするか？



対応工数が増えるので、自動チェックの活用が不可欠

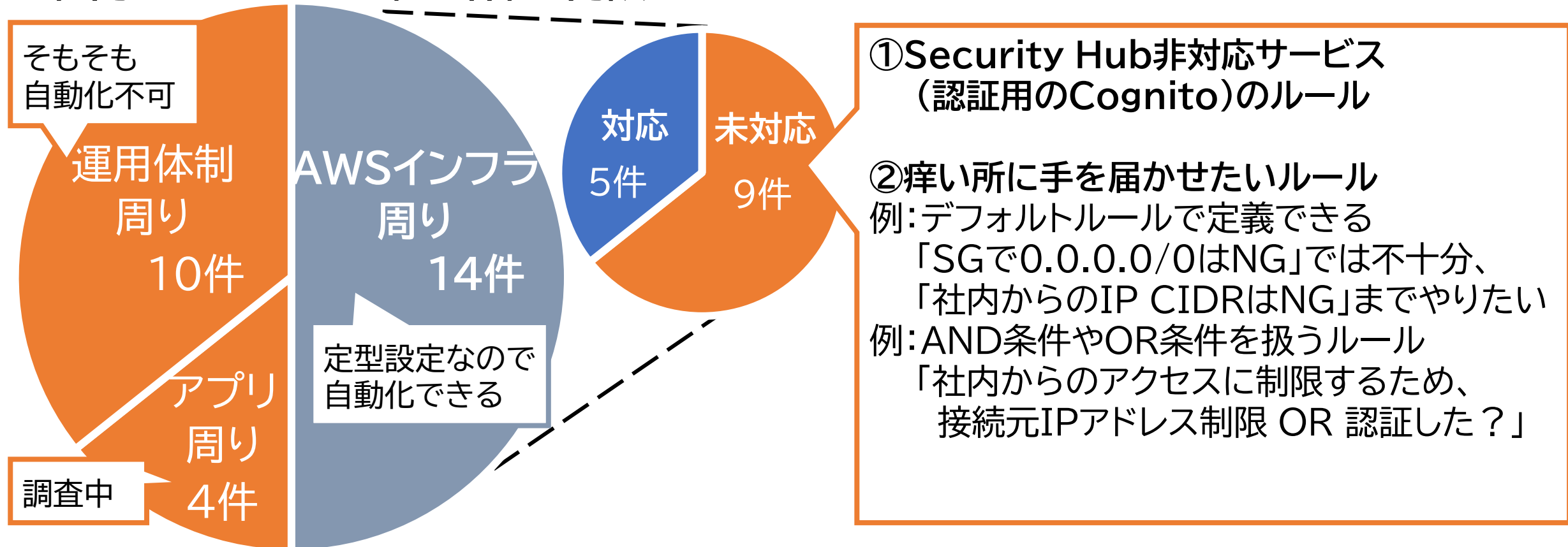
なぜ自動チェックにカスタムルールが必要か

まず、AWS Security Hub(AWS公式で用意された自動チェック)を利用

→社内チェックリストのうち、5/28件(18%)しか自動化できなかった

→カスタムルールで9件を追加対応し、14/28件(50%)を自動化した

■社内チェックリスト(28件)の内訳

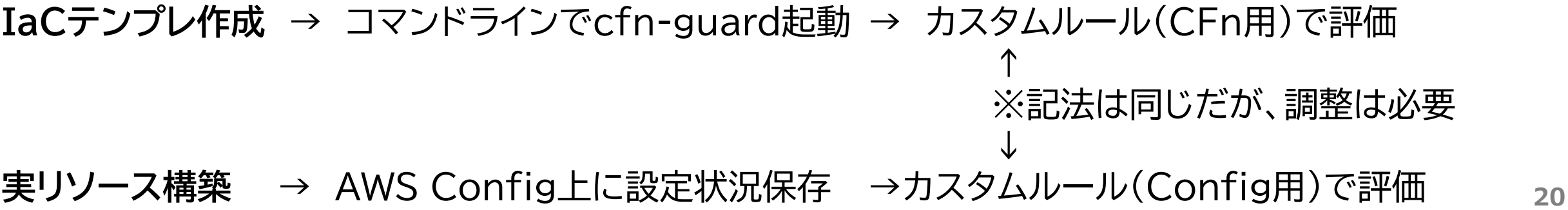


カスタムルールをどのツールで実装するか？ 星取表

※: <https://github.com/aws-samples/policy-as-code>

要件		AWSサービス	OSSツール: AWS公式ワークショップ(※)を基に選定			
		Security Hub	AWS製		それ以外	
			cfn-lint	cfn-guard	OPA	Checkov
ルール実装しやすさ ○: 専用言語で書く △: 汎用の言語で書く		- 実装不可	△ Python	○ 独自DSL	○ Rego	○ Yaml
チェック対象	IaCテンプレート	×	○	○	○ Regula	○
	実リソース	○	×	○	△	×
マルチクラウド対応		×	×	×	○	○

決め手: IaCテンプレートと実リソースのチェックに両対応



cfn-guardを実際に用いる場面

決め手:IaCテンプレと実リソースのチェックに両対応

IaCテンプレ作成 → コマンドラインでcfn-guard起動 → カスタムルール(CFn用)で評価

※記法は同じだが、調整は必要

実リソース構築 → AWS Config上に設定状況保存 → カスタムルール(Config用)で評価

■SARIF出力機能を使って自動化することで、開発フローに組み込める

■エディタ上

■CIツール

①ファイルを保存

②保存時にcfn-guardが走るよう設定

```
cdk-tsundaj → /workspaces/DUP_ChecklistAutomation_Web/src/CFnTemplate/ALB/cfn-template-ValidateResult.sarif
```

③その場で指摘

github-actions / WebList-Validate

[cfn-guard]

home/runner/work/DUP_ChecklistAutomation_Web/DUP_ChecklistAutomation_Web/docs/SystemTests/CFnTemplate/AlbCognito-template.yaml#L1 <ALBORCLOUDFRONT_パブリックからの無制限アクセスを許可しないようIPアドレス制限か二要素認証を有効にしているか_IP制限編_SECURITYGROUP>

'Resources/PUT::SecurityGroup/Properties/SecurityGroupIngress/2/CidrIp[L:201,C:18] Value="0.0.0.0/0"]

非準拠時にCI停止



cfn-guardを実際に用いる場面

決め手: IaCテンプレと実リソースのチェックに両対応

IaCテンプレ作成 → コマンドラインでcfn-guard起動 → カスタムルール(CFn用)で評価

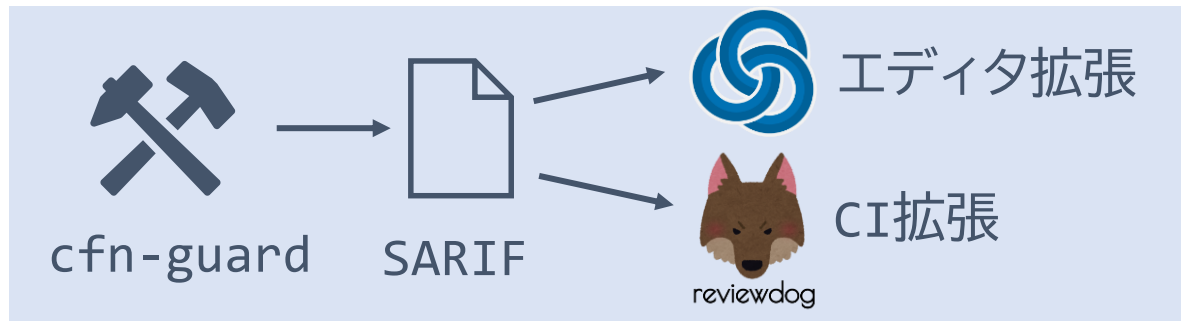
※記法は同じだが、調整は必要

実リソース構築 → AWS Config上に設定状況保存 → カスタムルール(Config用)で評価

■ SARIF出力機能を使って自動化することで、開発フローに組み込める

SARIFとは？

静的解析ツール向けの標準フォーマット
出力結果を後段のツールに渡しやすい



②保存時にcfn-guardが走るよう設定

非準拠時にCI停止



reviewdog

cfn-guardを実際に用いる場面

決め手:IaCテンプレと実リソースのチェックに両対応

IaCテンプレ作成 → コマンドラインでcfn-guard起動 → カスタムルール(CFn用)で評価

↑
※記法は同じだが、調整は必要
↓

実リソース構築 → AWS Config上に設定状況保存 → カスタムルール(Config用)で評価

■AWS Config上で、cfn-guard記法で書いたルールを動かすことが可能

AWSマネージドな自動チェック基盤としては優秀(チェック用のリソース管理が不要)

しかし、表示基盤(マネコン上)としては見づらい

フィルタリングが弱い(準拠/非準拠のみ)

順序がバラバラ(ルール名に数字を入れても無視される)

マルチアカウントが大変(アカウント毎にログインが必要)

SecurityHubのマネージドルールと混ざる

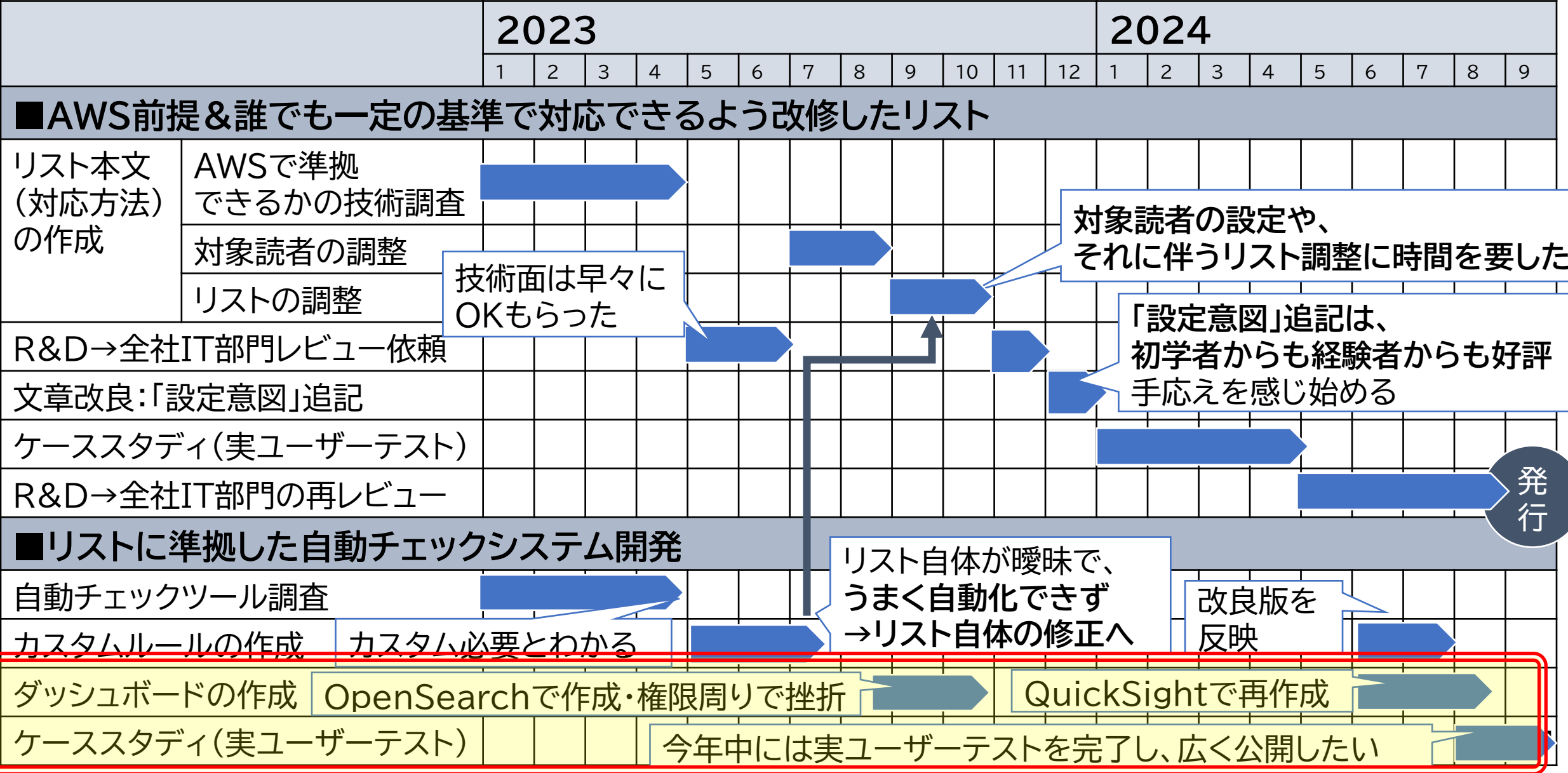
ルール

コンプライアンスステータスによるフィルタリング

すべて

名前	修復アクション	タイプ
CL_WS_A1_2_WAF_WebAcl	設定されていません	カスタムポリシー
CL_WS_A4_ALB	設定されていません	カスタムポリシー
CL_WS_A5_ACM	設定されていません	カスタムポリシー
CL_WS_A3_CloudFront	設定されていません	カスタムポリシー
CL_WS_C2_S3	設定されていません	カスタムポリシー
securityhub-alb-http-to-h...	設定されていません	AWS マネージド型

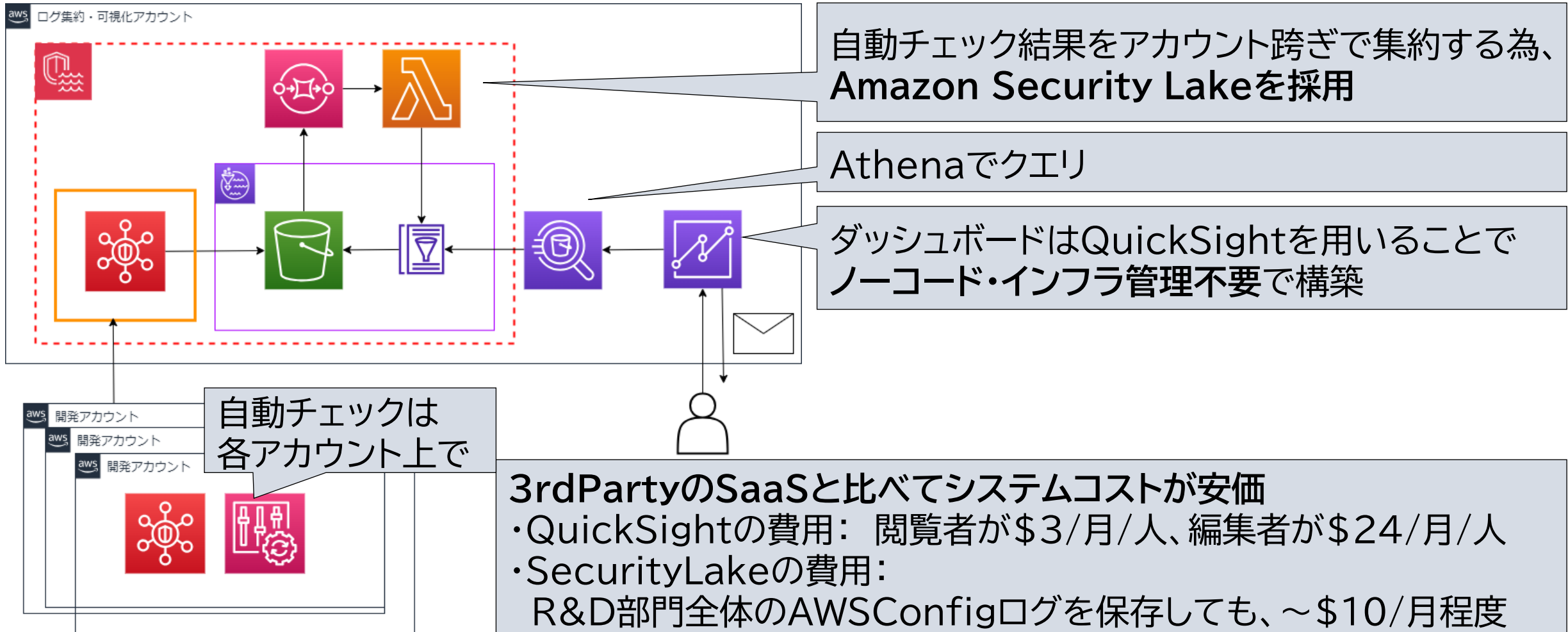
社内向けリリースまでの道のり



ダッシュボードを作ろう

■AWSマネージドでダッシュボードを自作し、必要な機能を実装している
ある程度の運用しやすさを担保しつつ、高い拡張性・安価なランニングコストを実現

■アーキテクチャ



ダッシュボードを作ろう

■AWSマネージドでダッシュボードを自作し、必要な機能を実装している
ある程度の運用しやすさを担保しつつ、高い拡張性・安価なランニングコストを実現

■QuickSight上の画面

非準拠の総数を表示

アカウント跨ぎで確認 アカウント毎フィルタリングも可能

The screenshot displays a dashboard with four summary cards (A, B, C, D) showing non-compliance counts. Below these is a table titled 'A:CDN/ゲートウェイレイヤ(ALB/APIGW/CloudFront)に関する確認事項'. The table has columns for item number, rule, AWS service name, selection options for rule compliance, rule name, region, resource ID, creation time, last update time, and compliance status (Compliant/Non-compliant). A callout points to the 'Non-compliant' count of 1 in the first row of the table.

項目	規則	awsサービス名	規則を遵守するための選択肢	ルール	region	resource_uid	作成日時	最終更新...	準拠	非準拠
A-1	Webサイトが社内向けの場合、本番環境におけるパブリックからの無制限アクセスを禁止しているか？								0	1
A-2	開発環境からの無制限アクセスを禁止しているか？								0	0

大本のExcelチェックリストと同じ順序で整列

非準拠項目を表示

まとめ

■発表内容

- **社内の急速なIT発展に対応する為、セキュリティチェックリストを作り直した**
AWS前提で、抽象度を下げた具体的な内容や設計意図を記載 実テーマでのケーススタディを実施
- **社内ルール準拠のAWS自動チェックの実現には、自社向けカスタムルールが必要**
 - SecurityHubでは社内ルールの18%のみ→カスタムルール作成し50%に対応
 - カスタムルール実装には、IaCを使うチームもそうでないチームも使える、cfn-guardを選定した
- **カスタムルールを実装するツールとして、cfn-guardを選定した**
最大の理由は、IaCテンプレと実リソースに両対応、IaC未普及なチームも使える

当社が目指す未来を一緒に実現しませんか？
興味を持った方、是非ご応募ください。

ダイキンにはゲンバが沢山あります！
“ダイキン情報技術大学”出身の若手たちと
デジタル改革を推進していく
ITエンジニア募集！！



応募ページはこちら



<https://daikin-career.net/jobfind-pc/>



連絡先



キャリア採用

DAIKIN
MID-CAREER
RECRUITMENT



研究開発拠点

TECHNOLOGY AND
INNOVATION CENTER



CSR・環境

サステナビリティ
レポート 2023



経営・財務

統合報告書2023



ダイキン公式 SNS



no+e



YouTube



TikTok



facebook

