SUMMIT

TOKYO | APRIL 20-21, 2023

CUS-10

トヨタ CCoE が進める Developer eXperience のカイゼン

馬渕 充啓
トヨタ自動車株式会社
デジタル変革推進室 クラウドCoEグループ 主幹 CCoEリード

馬渕 充啓

Mitsuhiro MABUCHI

TOYOTA

所属

デジタル変革推進室 クラウドCoE G 主幹/CCoEリード

(先進データサイエンス統括部 DS基盤開発室 クラウドCoE G GM)

経歴

2010/4　トヨタ自動車入社

～現在　セキュリティ/AI先行開発/研究に従事

2021/1　R&Dでクラウド支援立ち上げ (CCoE前進)

2022/4　CCoE 立ち上げ

～現在　CCoE リード

好きなAWSサービス

Amazon EC2

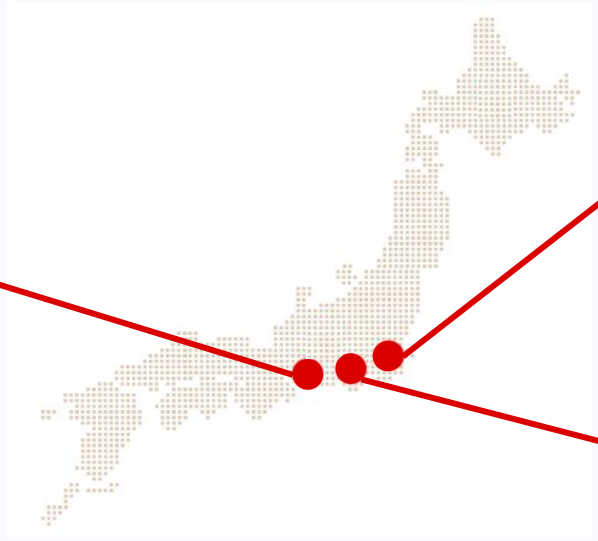
AWS Control Tower

会社概要

TOYOTA

会社名　：　トヨタ自動車株式会社
創　立　：　1937年（昭和12年）
本　社　：　愛知豊田市
拠　点　：　国内各事業所
　　海外事業所　28か国/53地域
従業員　：　約74,000人

＜主な国内研究開発拠点＞
※太字 CCoE 拠点



愛知県
・豊田 (本社)
・名古屋

東京都
・文京区 (東京本社)
・大手町

静岡県
・東富士研究所

本セッションの内容

TOYOTA

ゴール（以下が伝わって欲しい）

- トヨタCCoEの立ち上げた理由、目的、活動内容
- 本気で Developer eXperience (DevEx) の向上に取り組んでいること

話すこと

- トヨタCCoEの目的と目標
- Developer eXperience (DevEx) カイゼン施策
- TORO PFの概要と今後

話さないこと

- AWSの説明
- トヨタCCoEのサービス詳細
- 細かい実装の話

注意点

TOYOTA

- トヨタ内の全てのクラウド環境が、CCoEのプラットフォームで動いているわけではありません
- Developer eXperience を DevEx と略しています

TOYOTA

CONTENTS

TOYOTA

SECTION
1

トヨタのCCoE

- 背景
- ミッション

トヨタ内の最新の動向

TOYOTA

“モビリティカンパニーへのフルモデルチェンジ”、
”デジタル化”の取り組みが加速

ソフト開発がメインではない部門も
新たな取組 (DX) にチャレンジ

取り組みが活発になる一方で、
ソフト開発やクラウドに不慣れな
メンバーが増加…

現場の課題 (CCoE 以前)

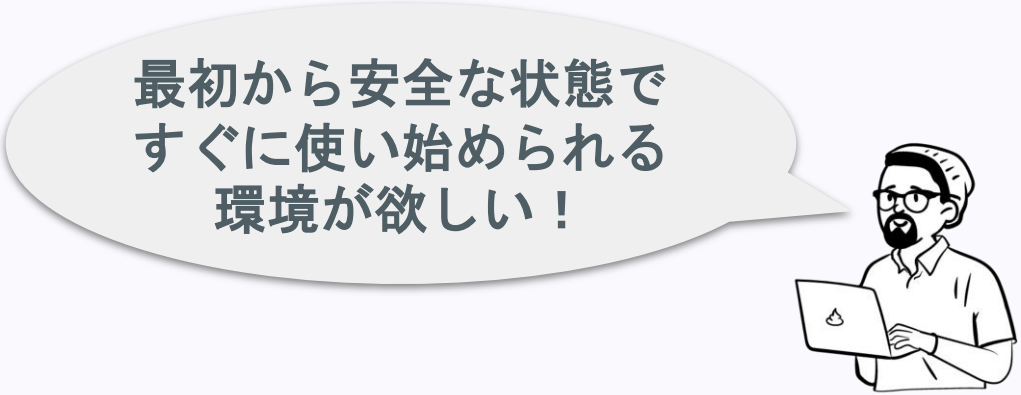
TOYOTA

- **使いたいタイミングですぐに使えない！**
  - ○ 使うまでの**ハードルが高い** (利用申請、セキュリティなど)
  - ○ 標準環境がないため、各部署・プロジェクトで**環境整備 (平均約2ヶ月)**
  - ○ クラウド開発者の交流が少なく、こういった**ノウハウが共有されない**

実はCCoEメンバーも…

TOYOTA

- みんな元々は**システム・アプリ開発者** (IT部門外)
  - ○ **時間をかけてベスプラ調べて**セキュリティ設定
  - ○ 不慣れながらも**日々コスト管理**
  - ○ システム・アプリのデプロイ、**最初はほぼ手動**



CCoE設立（2022年4月）

TOYOTA

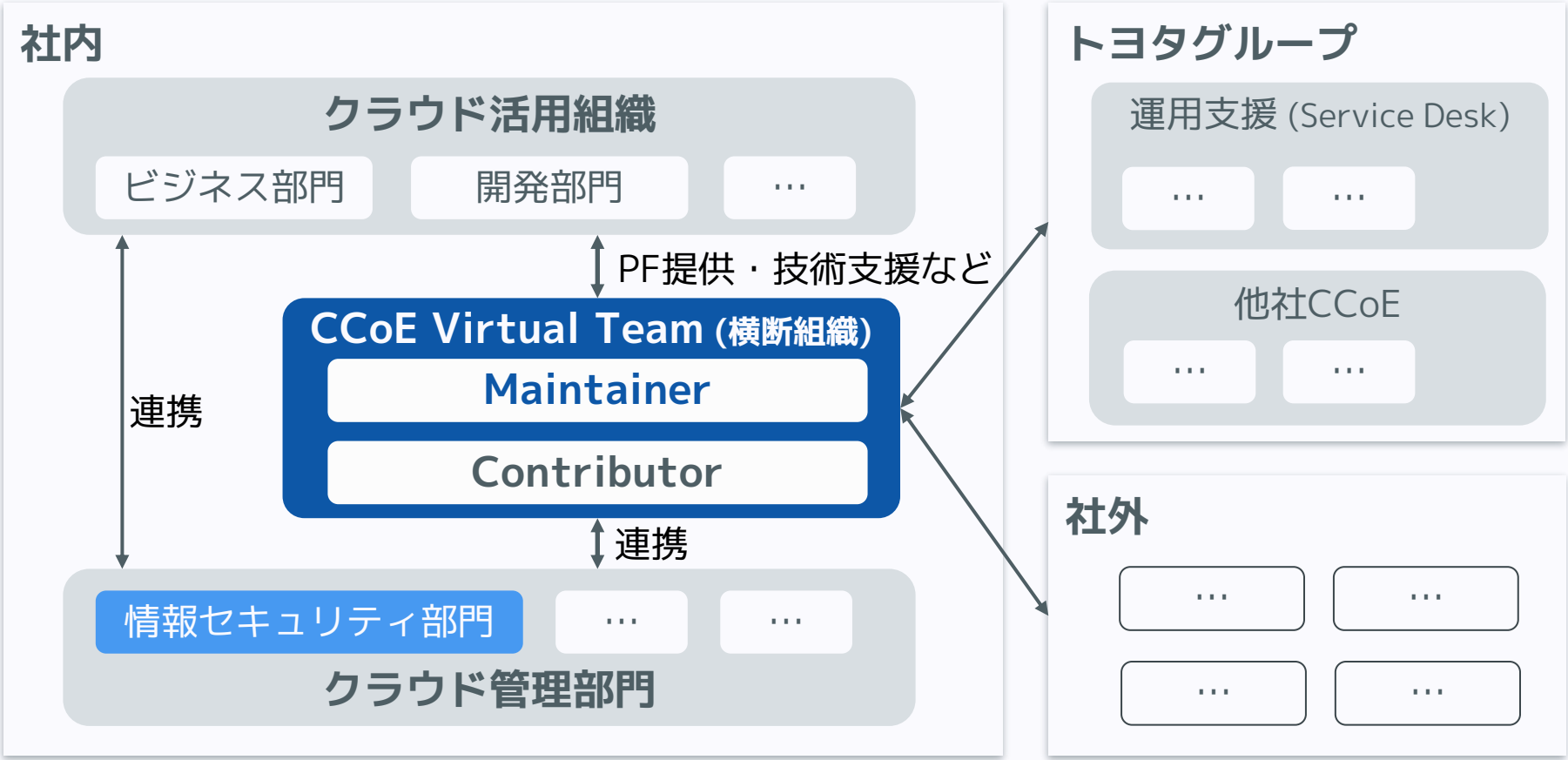
- 開発者の仕事を楽にすることで（**DevExカイゼン**）、
  モビリティカンパニーへのフルモデルチェンジを加速させる

「**安心して開発運用できるクラウド環境**」と「**クラウドに関する社内外の情報**」を整備し、トヨタの**全開発者がすぐに使える**ようにする

- **Just In Time** で安心・安全なクラウド環境を提供する
- クラウドを**使いこなす**ための技術支援・教育を提供する
- **仲間といつでも相談**できる場を提供する

CCoEの体制

TOYOTA



TOYOTA

＜トヨタCCoE＞

クラウドを活用して、

「開発者自身」が「開発者」のために
最高の **DevEx** 提供を目指す組織

TOYOTA

SECTION
2

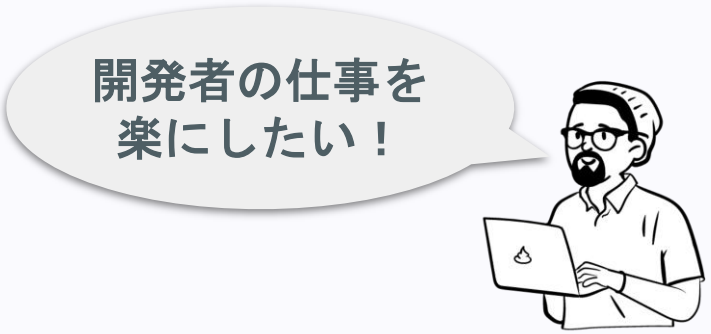
DevExカイゼン

- 考え方
- 取り組み

やりたいこと

TOYOTA

＜CCoEメンバーの想い＞

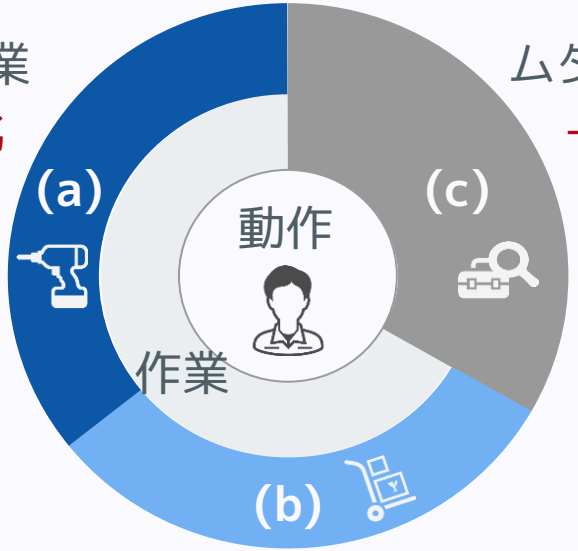


＋

＜トヨタ生産方式 (TPS)＞

正味作業
→最大化

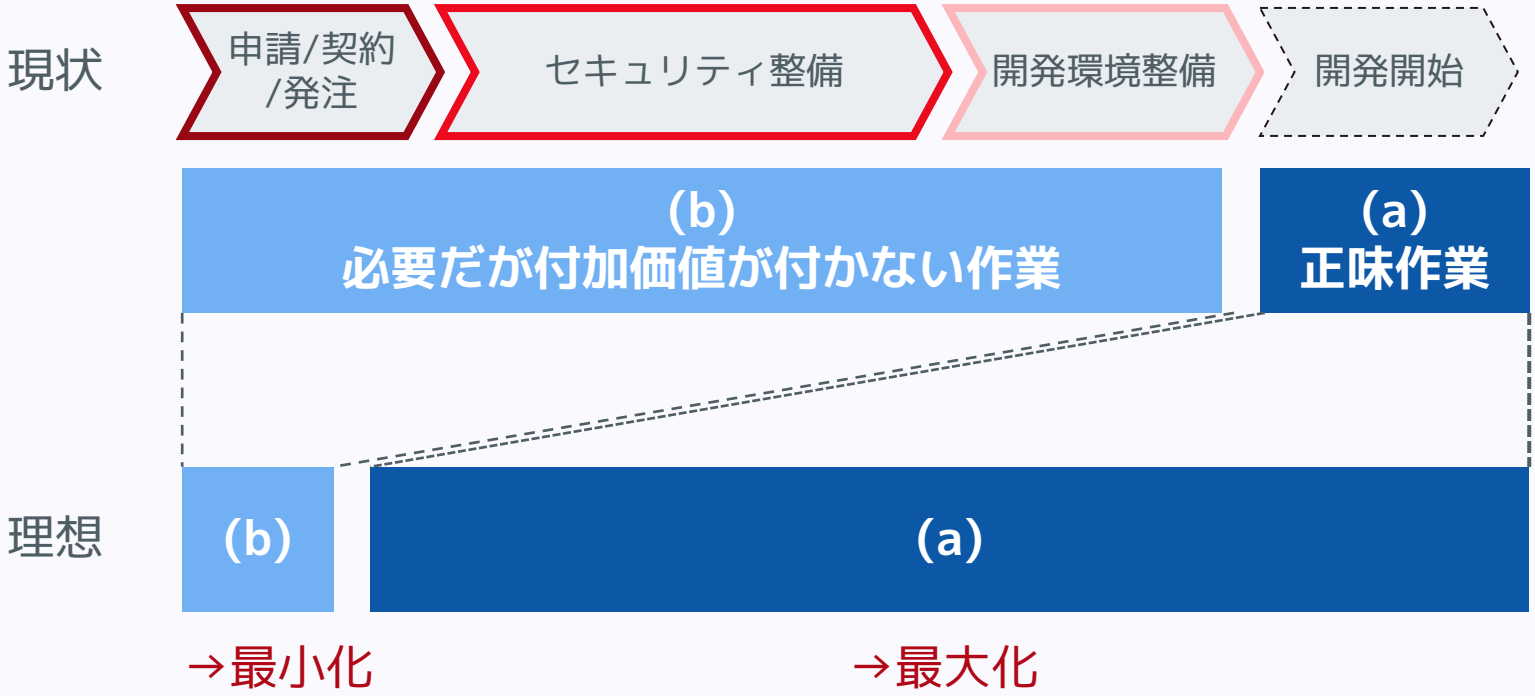
ムダな作業
→0



必要だが付加価値が
付かない作業
→最小化

つまり…

TOYOTA

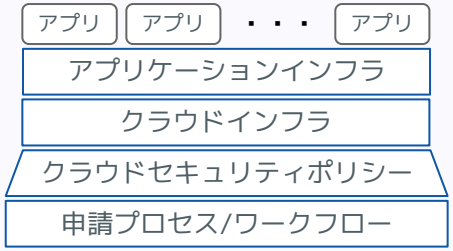


注意) かなりデフォルメしています。

CCoEの取り組み範囲

TOYOTA

1 プラットフォーム開発・運用

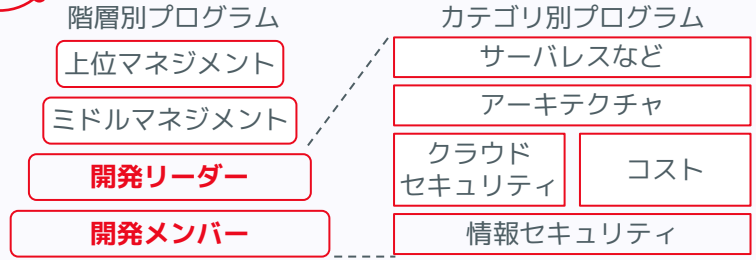


DevEx 向上

2 プロジェクト支援

技術力UP

3 クラウド人材育成



クラウドリテラシー向上

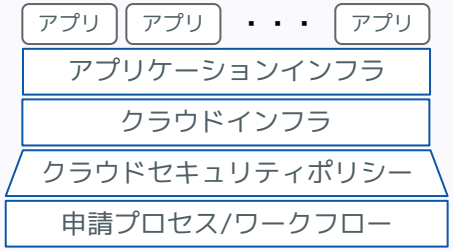
4 コミュニティ形成・運用

仲間とともに成長

CCoEの取り組み範囲

TOYOTA

1 プラットフォーム開発・運用



DevEx 向上

2 プロジェクト支援

技術力UP

3 クラウド人材育成

クラウドリテラシー向上

4 コミュニティ形成・運用

仲間とともに成長

プラットフォーム開発・運用

TOYOTA

- 「Just In Time で安心・安全なクラウド環境の提供」
  - ○ インフラだけではなく、プロセス含めて全体を見直し

TOYOTA

SECTION
3

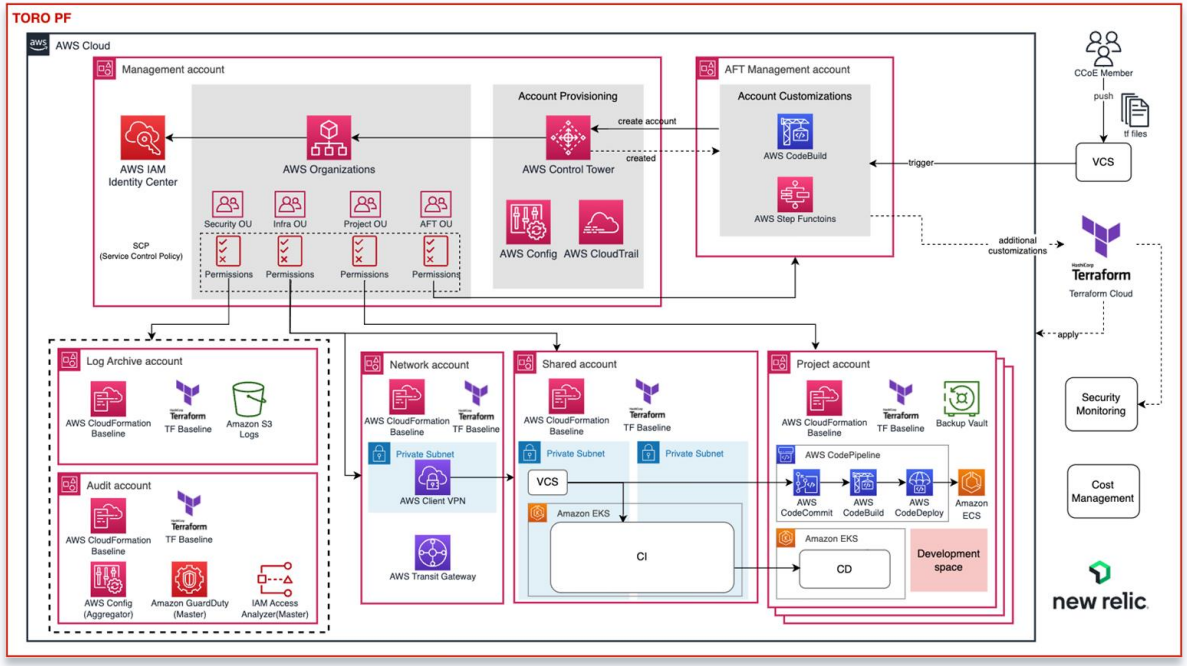
TORO PF

- 概要
- 特徴

TORO PFとは

TOYOTA

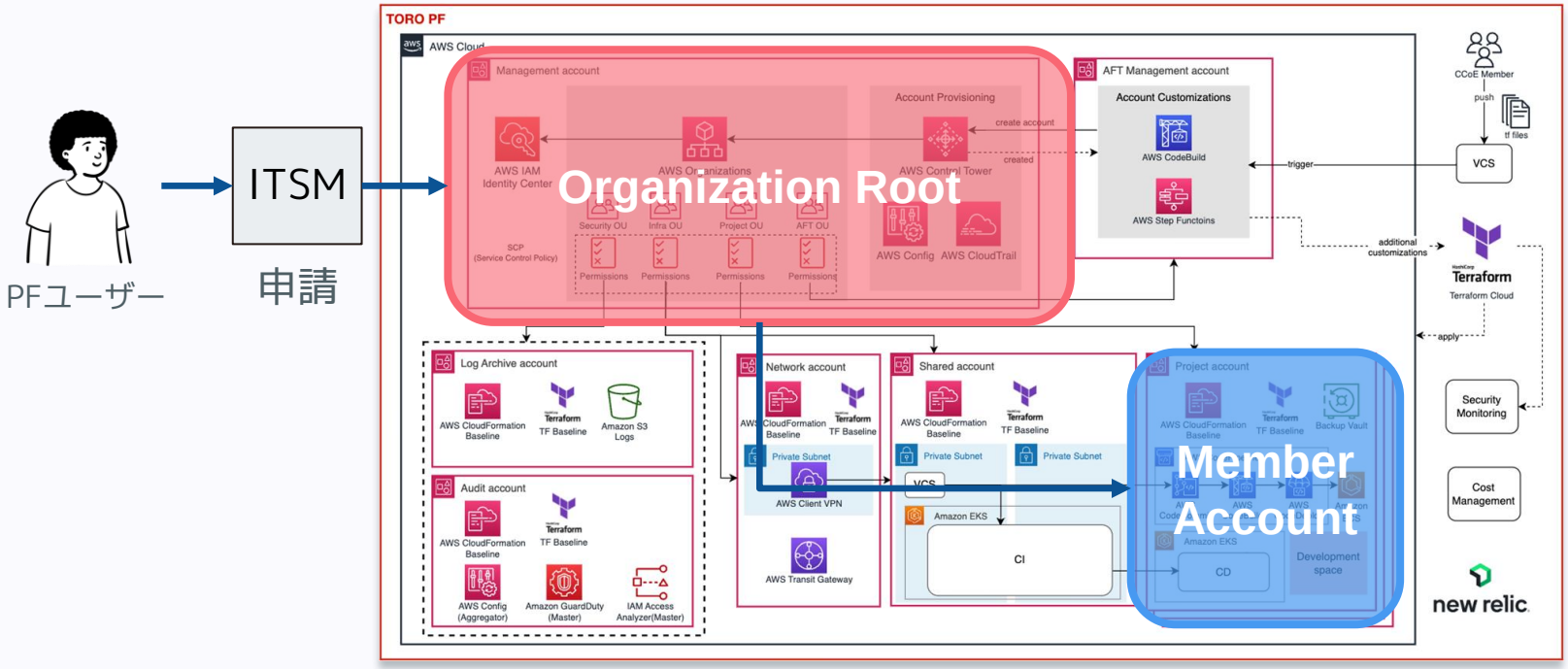
- **TO**yota **R**eliable **O**bservatory/**O**rchestration
  - **AFT (Account Factory for Terraform)** を採用して構築
  - 社内限定で CCoE と **TORO ロゴ作ってブランディング**



TORO PFとは

TOYOTA

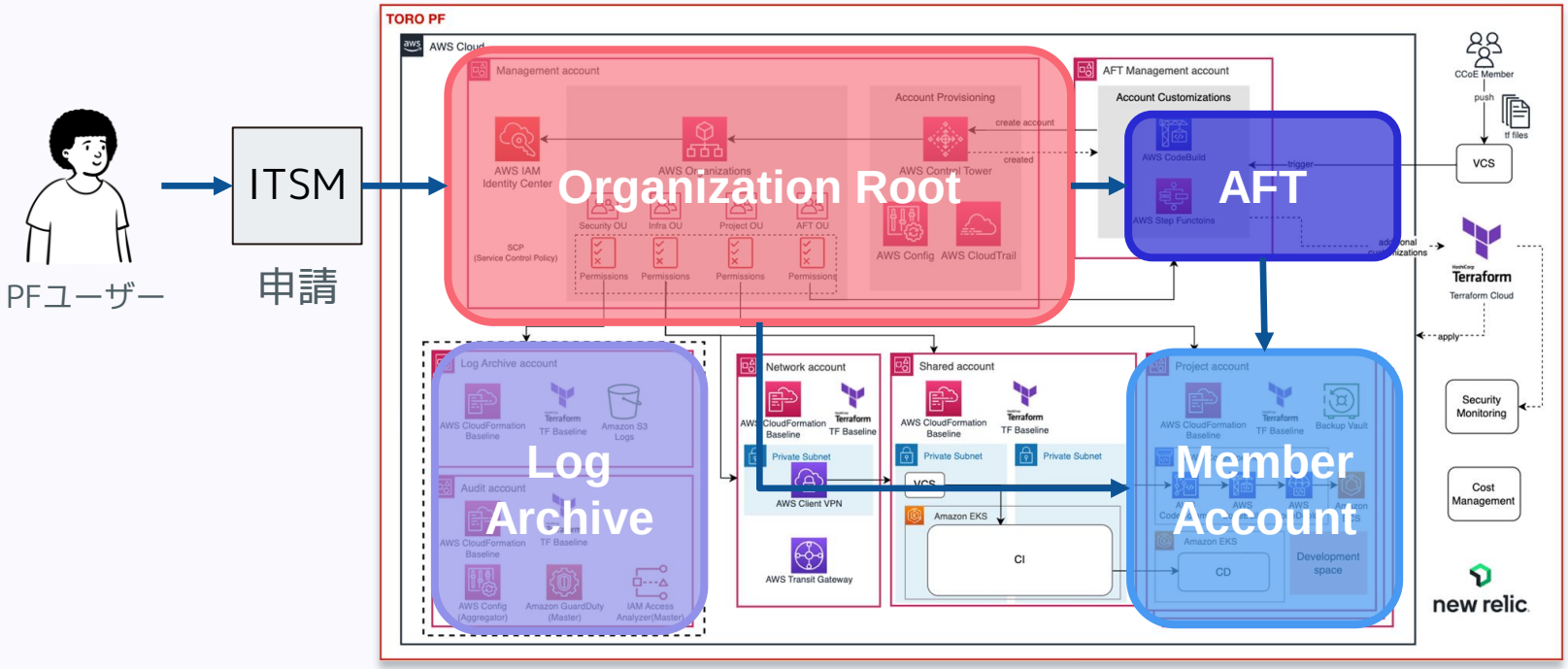
- 申請プロセスを簡略化
  - ○ 発注・利用**申請一体化**。エクセル→**ITSM**



TORO PFとは

TOYOTA

- 自動でセキュリティ設定（トヨタガイドラインの**約40%に対応**）
  - **ログも一括管理**！

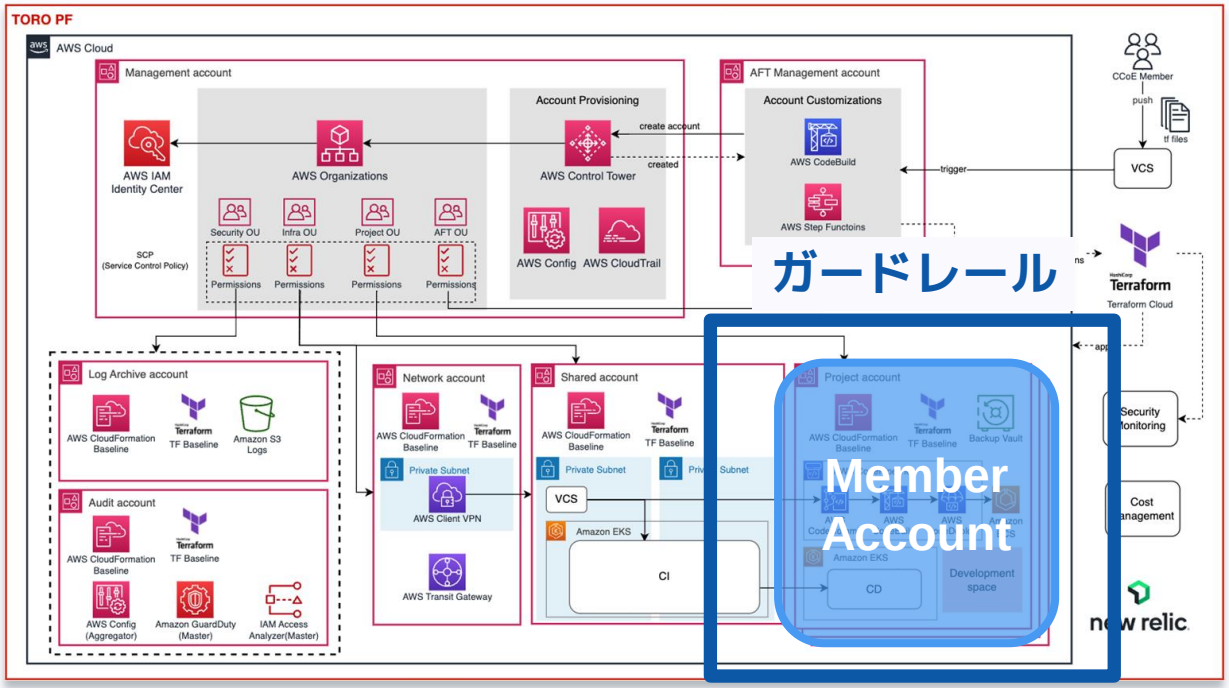


TORO PFとは

TOYOTA

- **ガードレール型セキュリティ**
  - ○ 各プロジェクトが**運用責任を持つ代わりに管理者権限**も付与

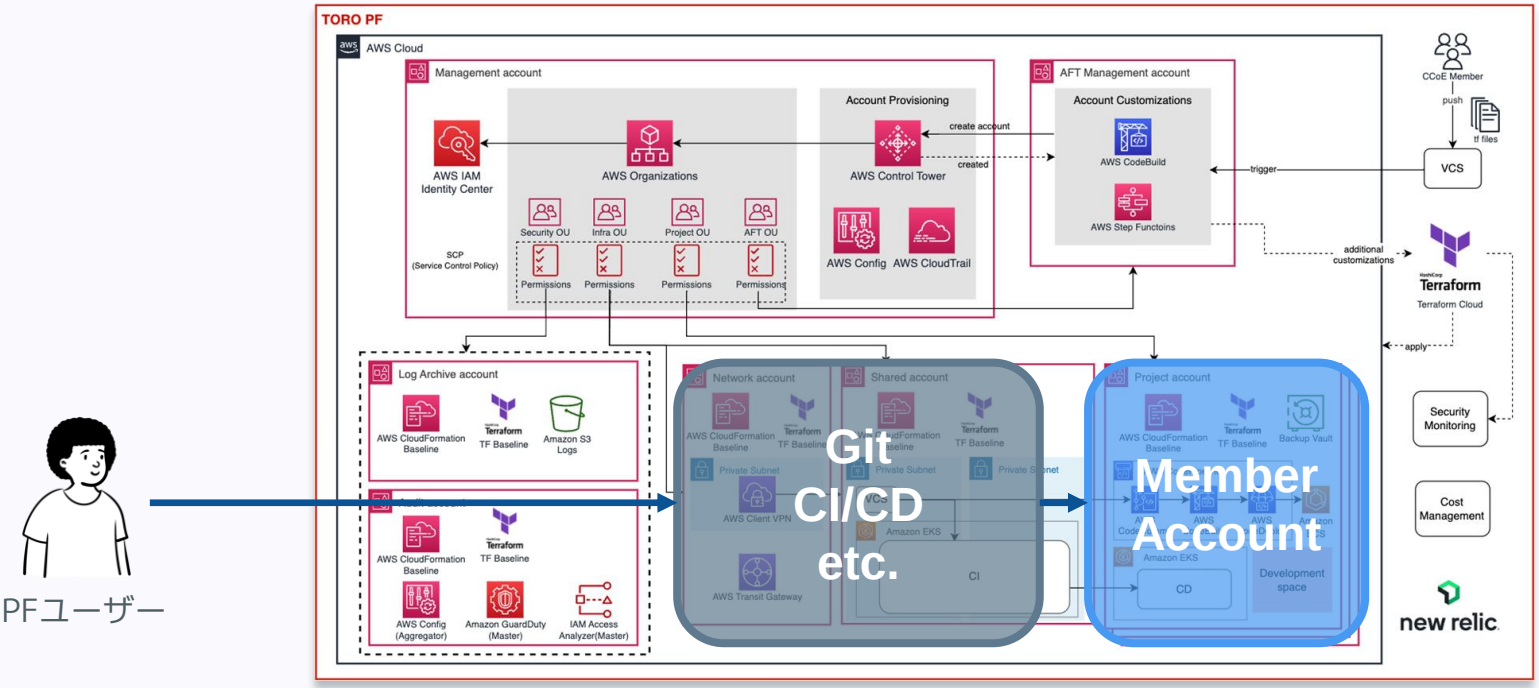
主なガードレール
・Rootユーザー禁止
・リージョン制限
・パブリック公開禁止
など



TORO PFとは

TOYOTA

- 最低限開発に必要な**GitやCI/CDなども提供**
  - 導入後**すぐ開発開始**できる！（コード・コンテナスキャンもあるよ）



TORO PFの効果

TOYOTA

開発開始までのリードタイムを**約96%削減 (2ヶ月→2日※最短2時間以内)**

TORO PFの土台

TOYOTA

- AWS Control Tower + Account Factory for Terraform (AFT)
  - **2021年11月29日**にAFTがリリース
  - AWSアカウントの発行と初期設定が楽になるソリューション

なぜAFTか？

TOYOTA

- AFT以前は**Customization for Control Tower (CfCT)**を利用
  - アカウント発行を**コードで実行できない**
  - **AWS外のSaaSとの連携**が自動でできない

なぜAFTか？

TOYOTA

- AFTだと...
  - ○ **AWSアカウント発行をコードで実行**できる

account_request

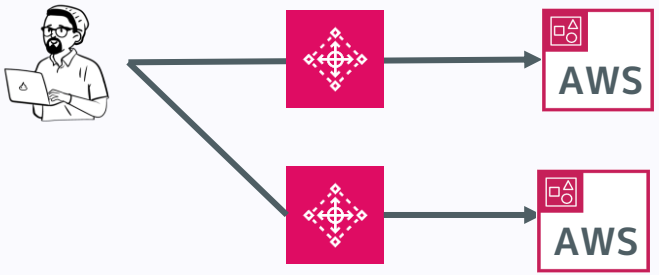
```
module "sandbox" {
  source = "./modules/aft-account-request"

  control_tower_parameters = {
    AccountEmail              = `<ACCOUNT_EMAIL>`
    AccountName               = "sandbox-aft"
    ManagedOrganizationalUnit = "Learn AFT"
    SSOUserEmail              = `<SSO_EMAIL>`
    SSOUserFirstName          = "Sandbox"
    SSOUserLastName           = "AFT"
  }

  account_tags = {
    "Learn Tutorial" = "AFT"
  }

  change_management_parameters = {
    change_requested_by = "HashiCorp Learn"
    change_reason       = "Learn AWS Control Tower Account Factory for Terraform"
  }

  custom_fields = {
    group = "non-prod"
  }

  account_customizations_name = "sandbox"
}
```

なぜAFTか？

TOYOTA

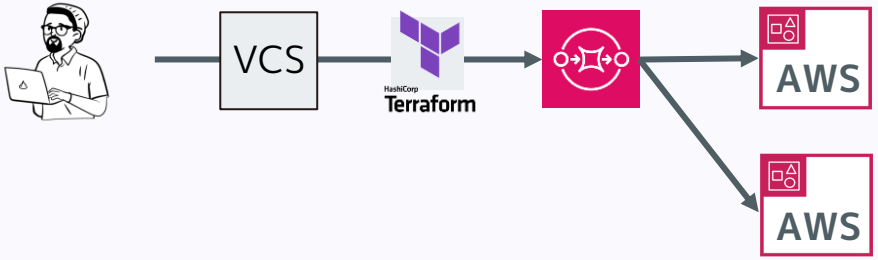
- AFTだと...
  - AWSアカウント発行をコードで実行できる
  - **複数アカウントの発行を一度に設定**できるようになる

従来



- 1アカウントずつ発行
- 1つ目が完了してから、次を実施

AFT

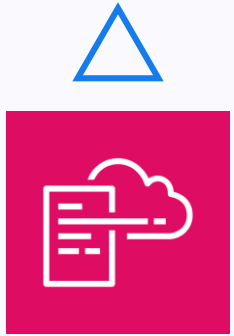


- 複数アカウントを一気に発行指示
- SQSでキューイングされて、連続処理

なぜAFTか？

TOYOTA

- AFTだと...
  - AWSアカウント発行をコードで実行できる
  - 複数アカウントの発行を一度に設定できるようになる
  - **他のクラウドリソースの自動払い出し** (CSPM, o11y, コスト管理など)



AWS CloudFormation

TORO PFでのカスタマイズ例

TOYOTA

Global Customizations

全アカウント共通

- Amazon S3のブロックパブリックアクセス
- CSPM設定
- メトリクスアラーム
- 汎用的な通知機能

など

Account Customizations

アカウント個別

- VPC関連リソース作成
- リソースお掃除ツール

など

個別要件に近く、セキュリティ目線から大きく外れるようなものは基本的にAFT外で実施

AFTのここが惜しい…

TOYOTA

- Planが**期待と違っていてもApply**しちゃう (Auto Apply)
- 自動生成される**Terraform Cloudワークスペースのカスタムが面倒**
- 発行済みのアカウントの**アカウント名変更できない**
- **GitLab対応**して欲しい（AWS CodeStar側の影響）
- バックアップ無制限で**保存期間/容量制限できない**

注意) 2023年3月27日時点の情報です。

TORO PFの主な特徴

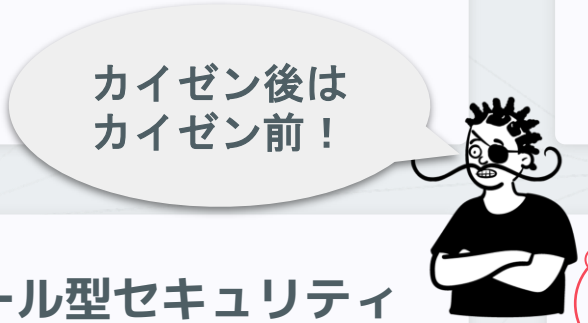
TOYOTA

POINT 1 2時間でアカウント発行

最短2時間、通常2営業日以内で
AWSアカウントをユーザー提供

POINT 2 セキュリティ設定工数96%減

アカウント発行時点で基礎的な
セキュリティ設定を実施済
ガイドラインの40%カバー
e.g. GuardDuty有効化、CSPM設定



POINT 3 ガードレール型セキュリティ

安全で**開発者の邪魔をしない**、
みんなが嬉しいセキュリティ

e.g. SSH/RDPやS3のパブリック公開禁止

POINT 4 アプリ開発も支援

セキュリティも考慮したCI/CD
Pipelineにより、**即デプロイ可**

e.g. コンテナ/コードスキャン、SBOM

TOYOTA

SECTION
4

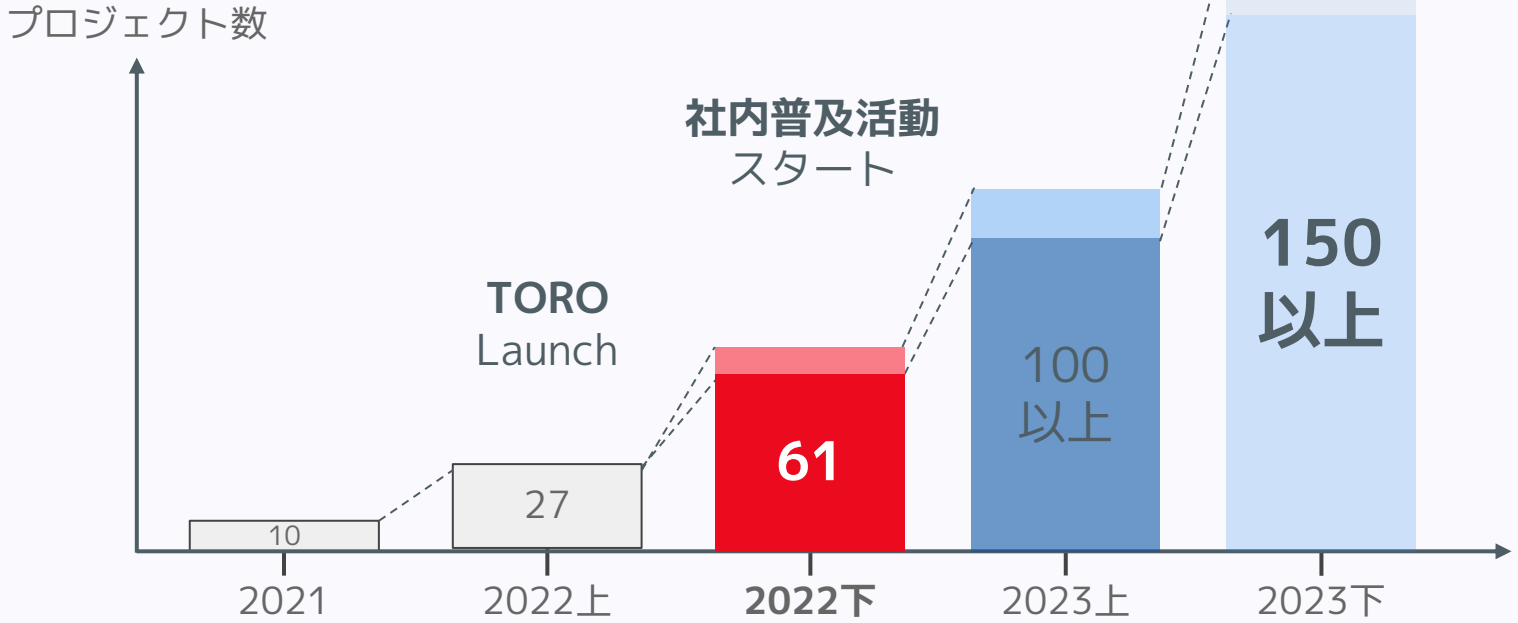
まとめ

- 現状
- 今後

TORO PF利用状況

TOYOTA

- 利用プロジェクトは**1年間で約6倍**。社内普及活動で順調に増加
- 今までは**新規プロジェクト中心**
- 今後は**既存AWS環境の移行をメイン**に狙う



今後の予定

TOYOTA

- 開発者が**さらに開発に集中できる (DevEx向上)** サービスの拡充
- ２～3年でTORO PFを**トヨタ内のDX用デファクトPF**にする
- ユーザーのさらなる増加に備え、**運用自動化**を加速

DevExのカイゼンはまだ始まったばかり

Thank you!