Oracle Developer Day 2026

ガバメントクラウド：
OCI環境払い出し自動化への取り組み

2026/05/21　　デジタル庁

デジタル庁
Digital Agency

目次

ガバメントクラウドとは

ガバメントクラウド
＝「技術要件を満たした民間クラウド」＋「モダンなITガバナンス機能」

公共情報システムのための共通のクラウドサービス利用環境

迅速、柔軟、セキュア、コスト効率の高いシステムの実現を目指す

利用者は、調達することなく、既成のクラウドサービスを選んでそのまま使うことができる

デジタル庁は、テンプレート等のガバナンスに必要な機能のみを利用者に提供し、クラウド最適でモダンなシステム構成の推進を方針とする

デジタル庁が契約したクラウドサービス

- Amazon Web Services
- Google Cloud
- Microsoft Azure
- Oracle Cloud Infrastructure
- さくらのクラウド

ガバメントクラウド利用状況（2026年3月31日時点）

- 国（情報システム）

	AWS	Google Cloud	Azure	OCI	計
国※1	140	5	18	1	164

※1 情報システムIDで集計

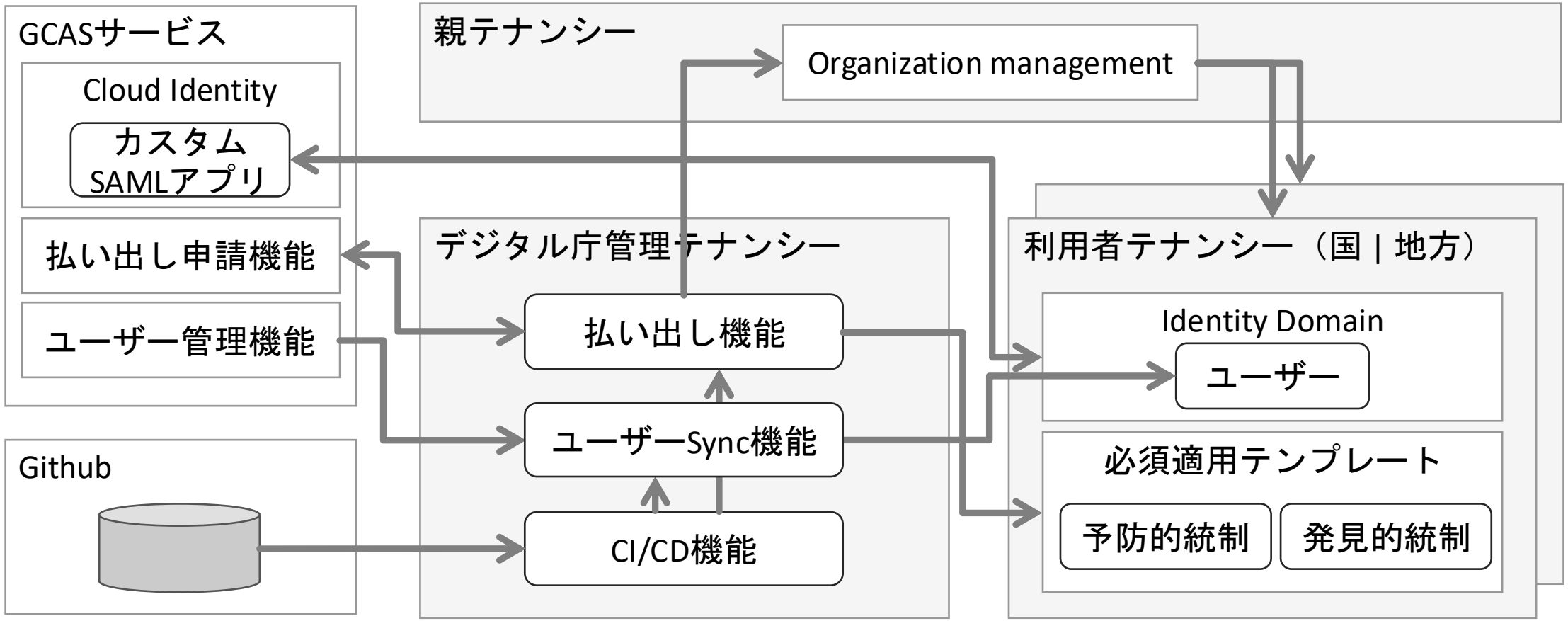
- 地方公共団体

	AWS	Google Cloud	Azure	OCI	計
地方公共団体数※2	1,564	8	0	461	1,676※3

※2 請求書を送付した地方公共団体数（都道府県・市区町村）を集計
※3 複数CSPを利用している団体については１件として集計

ガバメントクラウド（OCI）のアーキテクチャ

OCIの親テナンシーから利用者に子テナンシーを払い出す

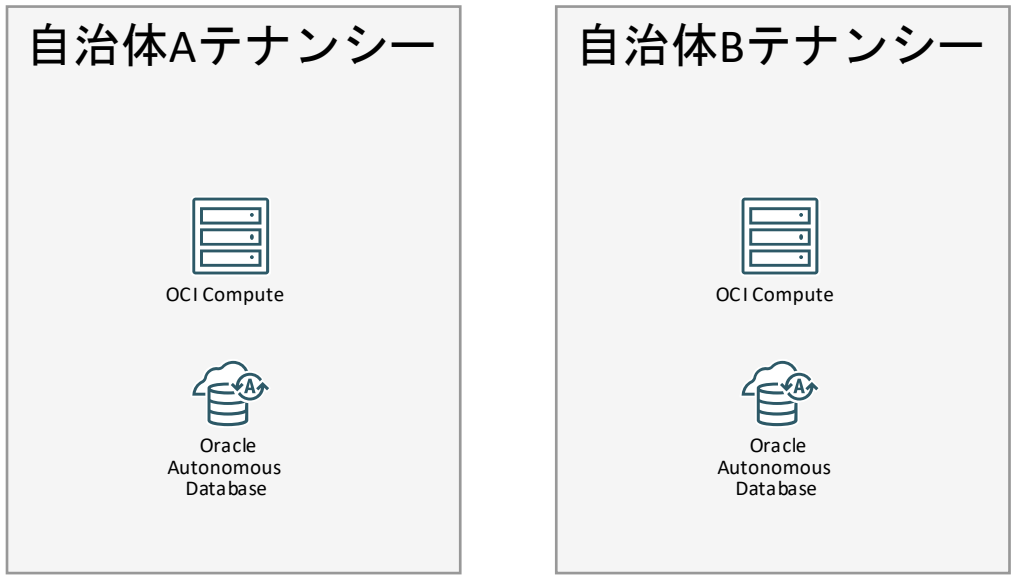


ガバメントクラウドとして守るべきガバナンスやセキュリティ機能をOCIの機能を活用し提供する

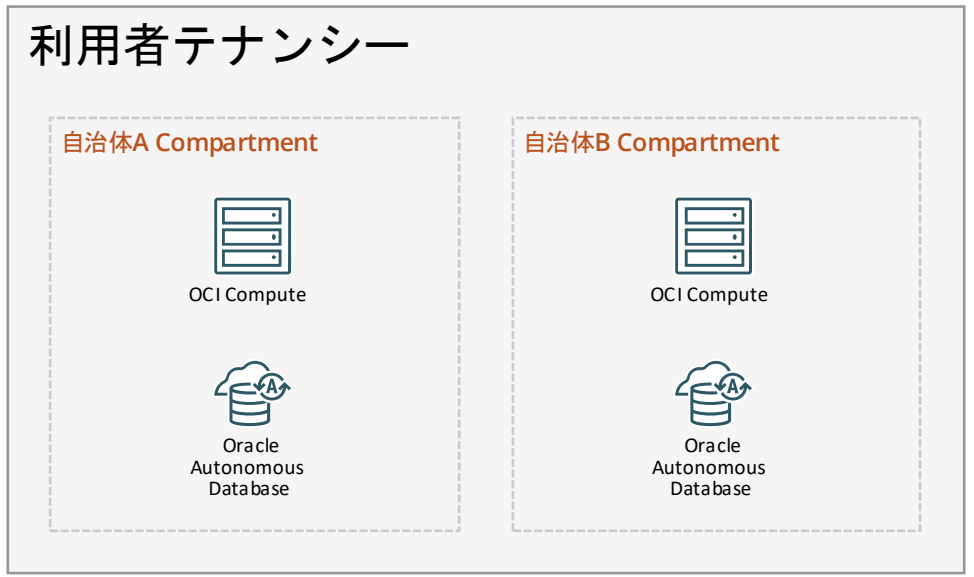
必須適用テンプレート		
予防的統制	• インターネット接続拒否（地方） • OCVS利用禁止 など	Security Zones Quota Policy
発見的統制	• ネットワークセキュリティグループの削除、変更 • Database終了 など	Cloud Guard
その他の機能	• 監査ログ収集 • SSO設定 など	Connector Hub Notifications Identity Domain など

OCIはコンパートメント機能を活かした共同利用方式が多い

単独利用



共同利用



払い出し作業の課題

400以上の団体への払い出しに手作業は限界であり、自動化が必須

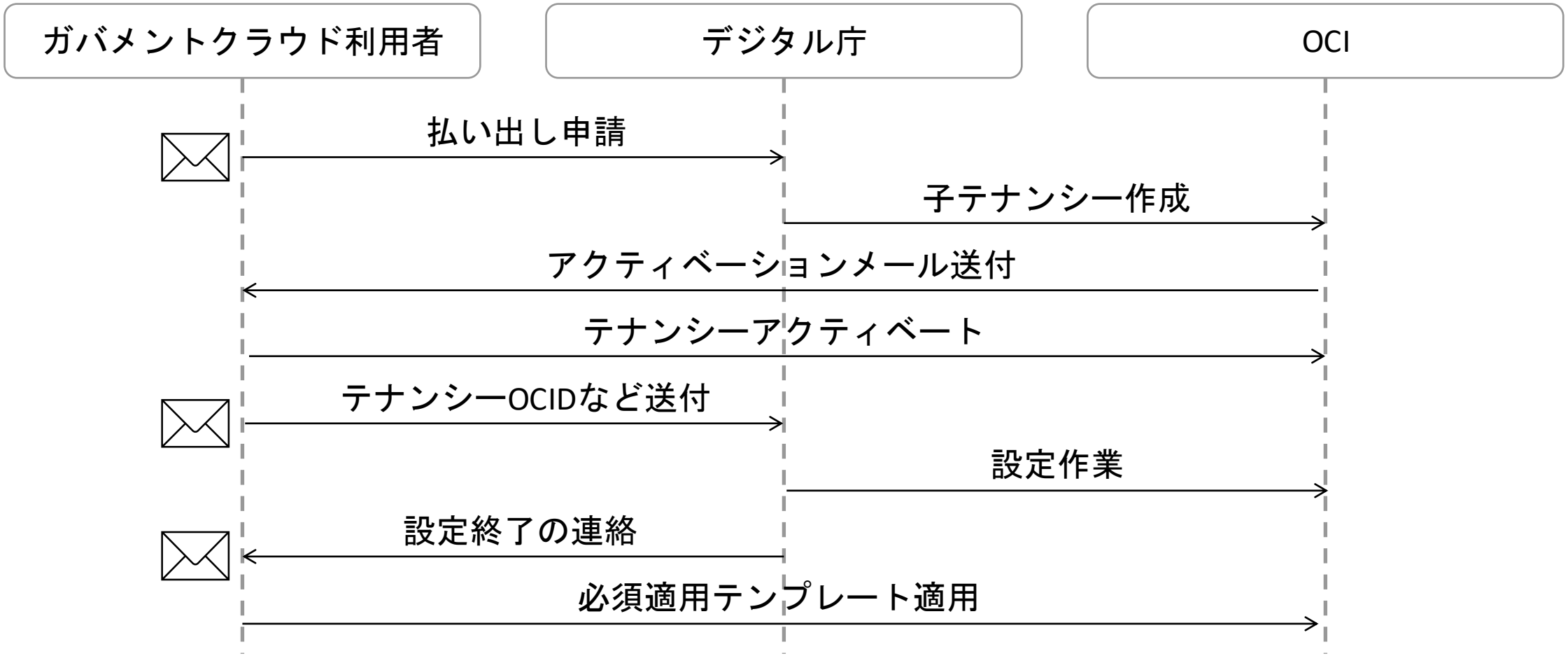
ガバメントクラウドが目指すこと

- 迅速
- 柔軟
- セキュア
- コスト効率

手作業の弊害

- リードタイムの長期化
- ヒューマンエラーのリスク
- 標準化の欠如
- 運用負荷が高い

利用者とメールのやり取りが必要で煩雑な作業が必要



目指したこと

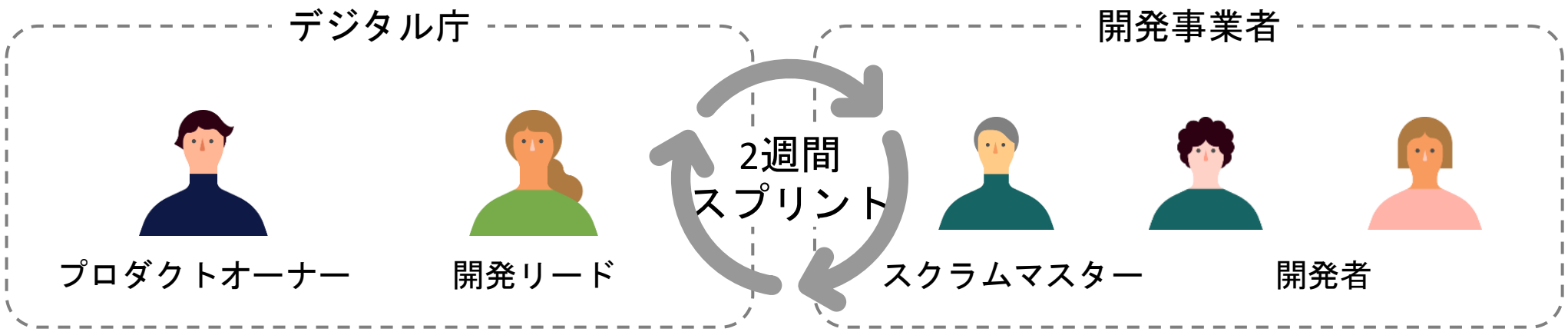
手作業をなくすために、４つの自動化を目指した

認証の自動化	クラウドで最もリスクが高いと言われるAPIキーなどの永続的な資格証明を利用しないこと
ジョブの自動化	GCASへ払い出し申請をトリガーとして、払い出しのジョブを自動で動かすこと
インフラ管理の自動化	障害や高負荷時に人手を介さず対応できること
監視の自動化	払い出しやエラーの状況を本番環境にログインせずに把握できること

払い出し自動化の取り組みと効果

OKRを設定し、各プロダクトチームがスクラム開発を導入している

Objectives	KeyResults	Epic	ストーリー
利用者が申請した日にガバメントクラウドを利用できる	払い出しのリードタイムがxx時間以内になっている	払い出し自動化	GCASから申請情報を取得できる
	払い出しのミスによる手戻り件数０件	GCAS連携のAPI化	申請された情報で子テナンシーを作成できる



上記のObjectivesなどは一例です。実際とは異なります。

チームの規模や開発のしやすさに合わせてスクラムのフレームワークを適用

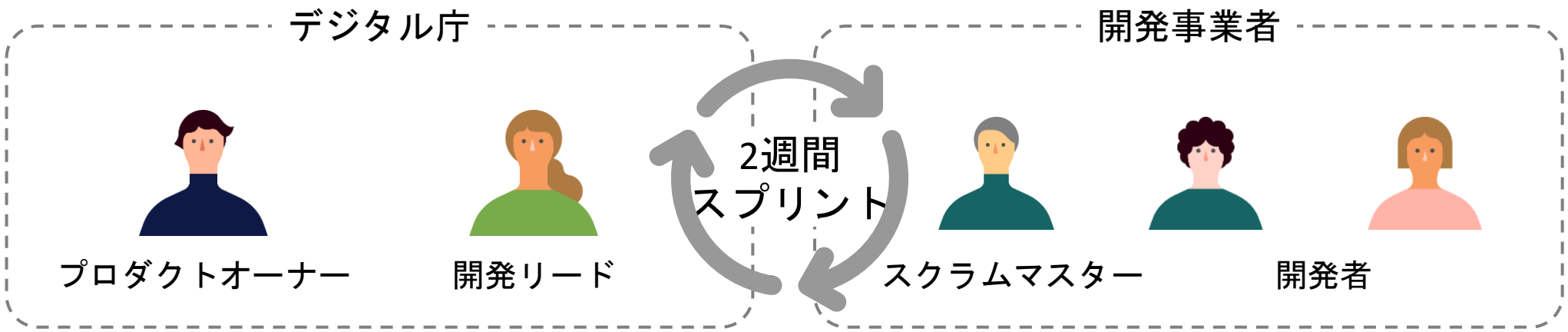
チケット管理

- 開発規模がそれほど大きくないので、OKRとバックログ（Epic, ストーリー）を直接紐づけて運用した
- チケット作成やストーリーポイント見積もりはAIを活用して効率化

上記のObjectivesなどは一例です。実際とは異なります。

チームの規模や開発のしやすさに合わせてスクラムのフレームワークを適用

体制	• プロダクトオーナーは手段（How）には口を出さず、ユーザーストーリー（プロダクトバックログ）の管理とプロダクト価値の最大化に専念 • ガバメントクラウド固有の技術的な制約事項は開発リードが担保



OKEで払い出しなどの全ての機能を制御している

GCASサービス

Cloud Identity

カスタム
SAMLアプリ

払い出し申請機能 API

メール通知機能 API

ユーザー管理機能 API

利用者

デジタル庁

親テナンシー

Organization management

デジタル庁管理テナンシー

ジョブ管理

払い出し機能

OKE

OCIR

Vault

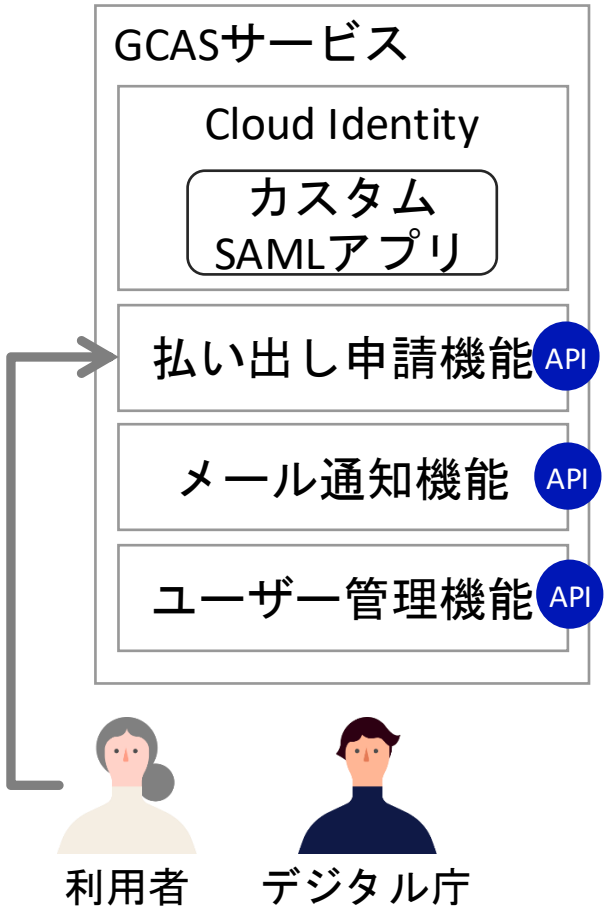
Logging

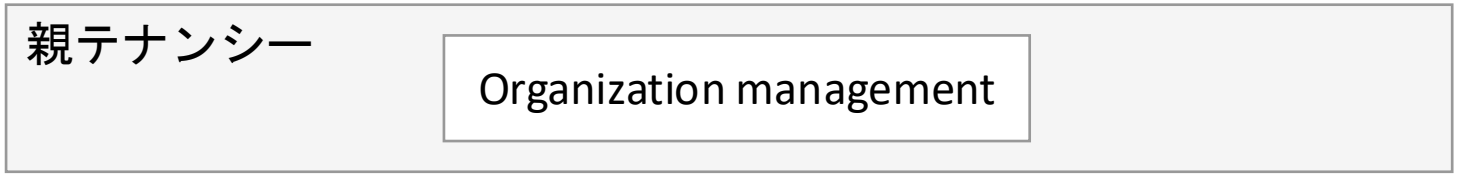
利用者テナンシー

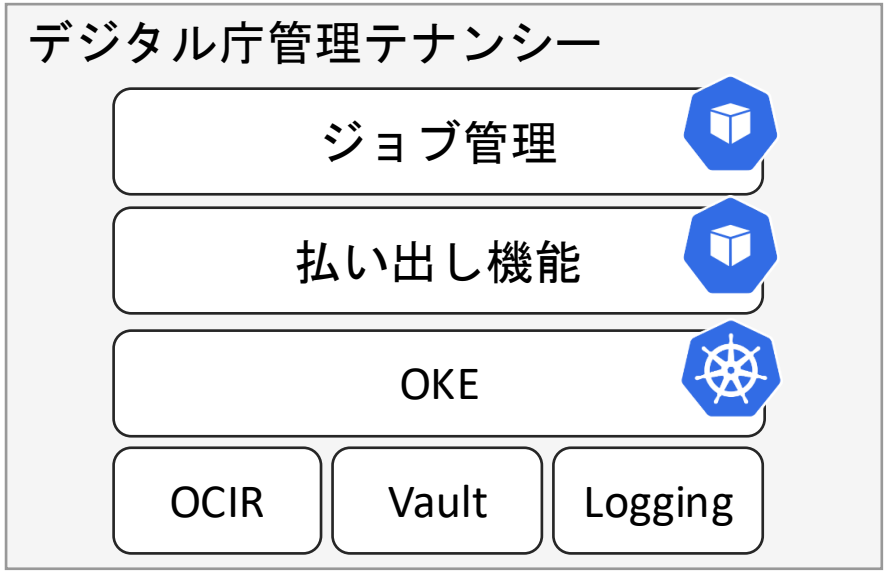
Identity Domain

必須適用
テンプレート

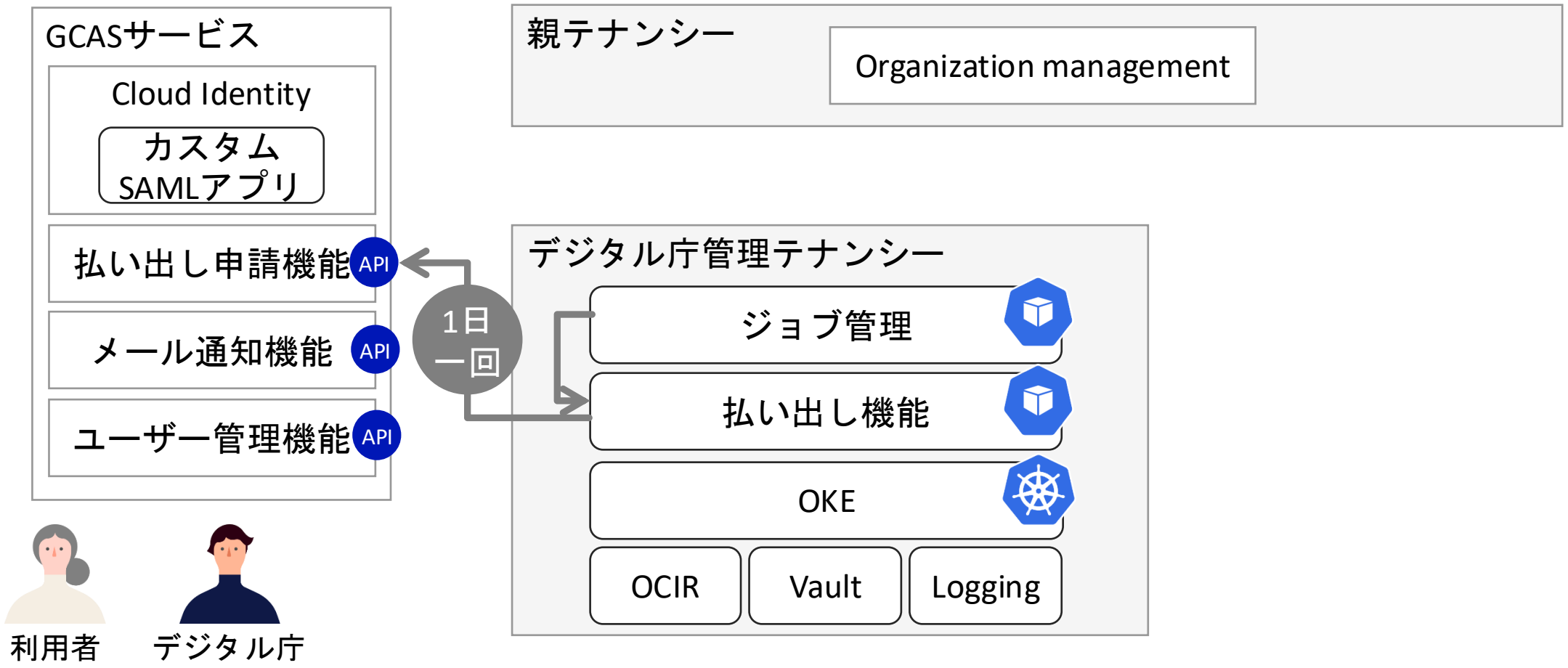
ガバメントクラウド利用者がGCASにテナンシーの情報を登録



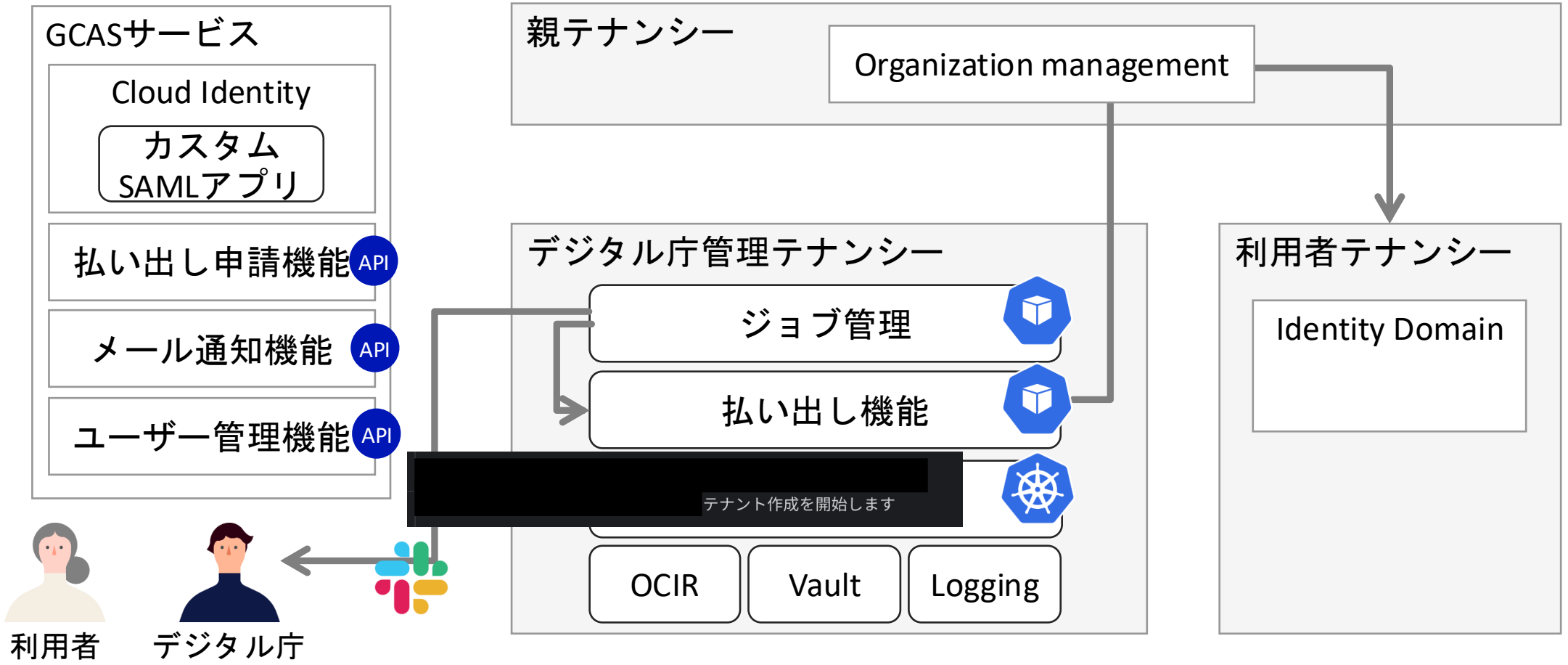




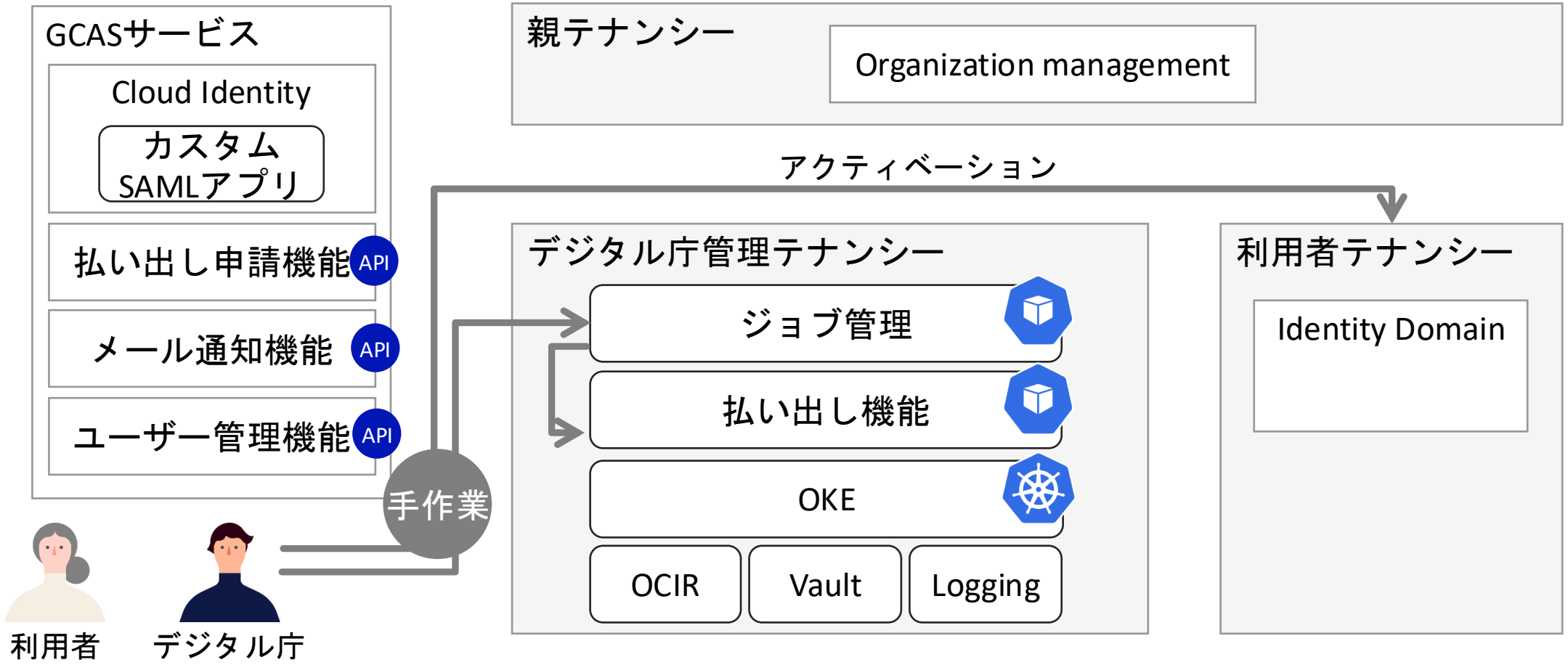
ジョブ管理が払い出し機能に指示を出し、GCASから申請情報を取得



払い出し機能が、登録された情報を元に子テナンシーを作成

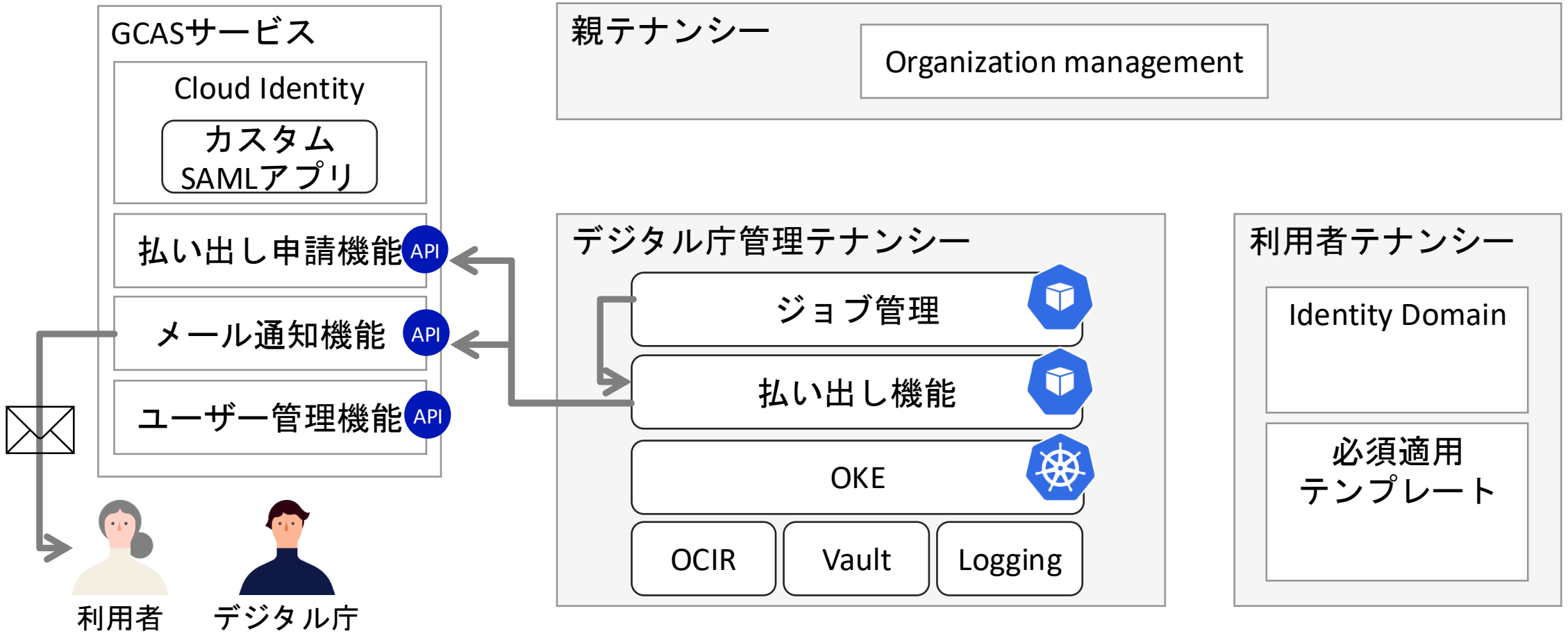


運用作業者が必須適用テンプレート適用のための認証情報を設定



払い出し機能が子テナンシーに必須適用テンプレートを適用

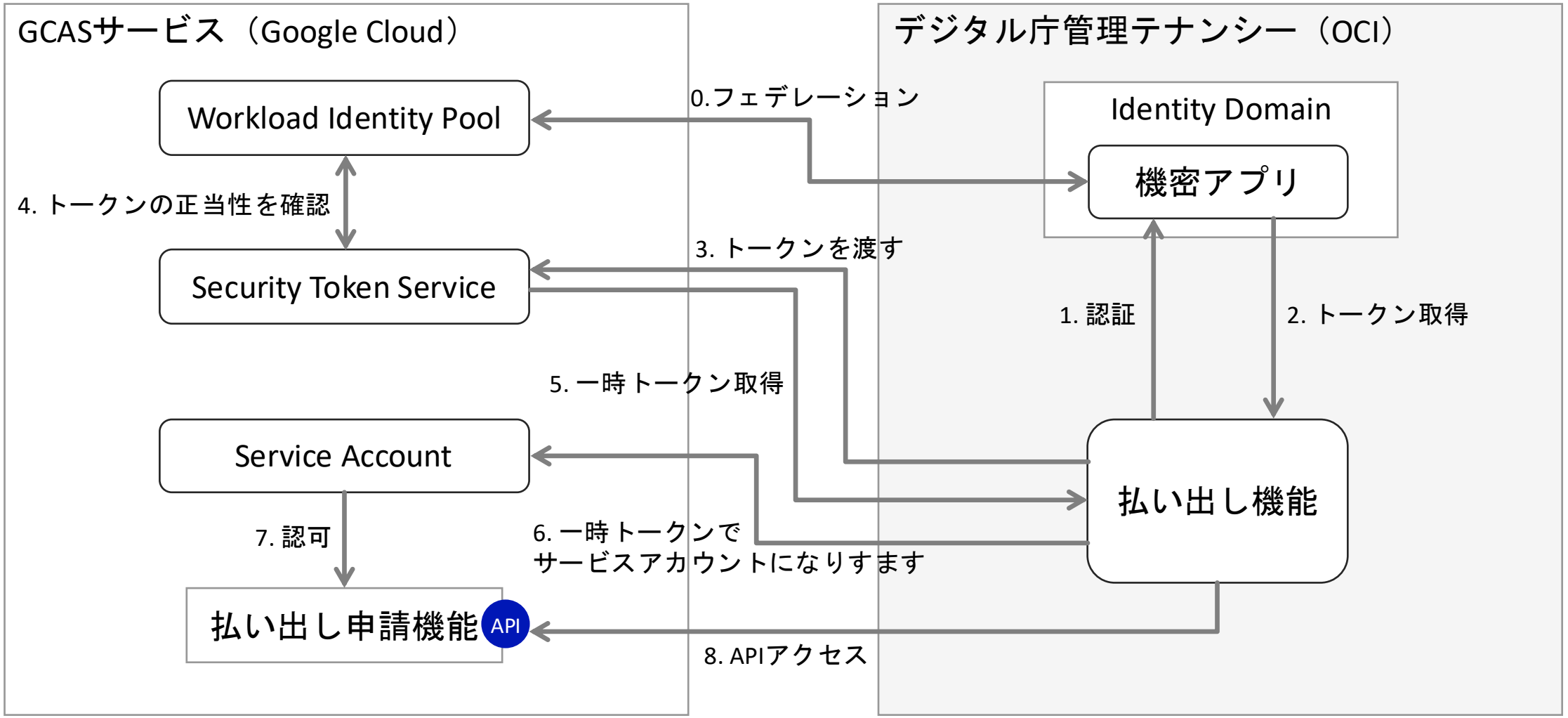
払い出しが完了したことをGCASに登録し、利用者にメール通知



セキュアかつ自律化により払い出しの運用負荷を最小化

認証の自動化	クラウドで最もリスクが高いと言われるAPIキーなどの永続的な資格証明を利用しないこと	OCIに機密アプリを作成しWorkload Identity FederationによってGCASと認証した
ジョブの自動化	GCASへ払い出し申請をトリガーとして、払い出しのジョブを自動で動かすこと	複数のジョブをジョブ管理ツールで自動化し、テナンシー作成から必須適用テンプレート適用までを自動化
インフラ管理の自動化	障害や高負荷時に人手を介さず対応できること	Kubernetesの機能でPod障害時に自律的に復旧
監視の自動化	払い出しやエラーの状況を本番環境にログインせずに把握できること	Slackと連携することで、払い出しやエラーの状況をSlackで把握できる

（参考）Workload Identity Federationによる認証フロー

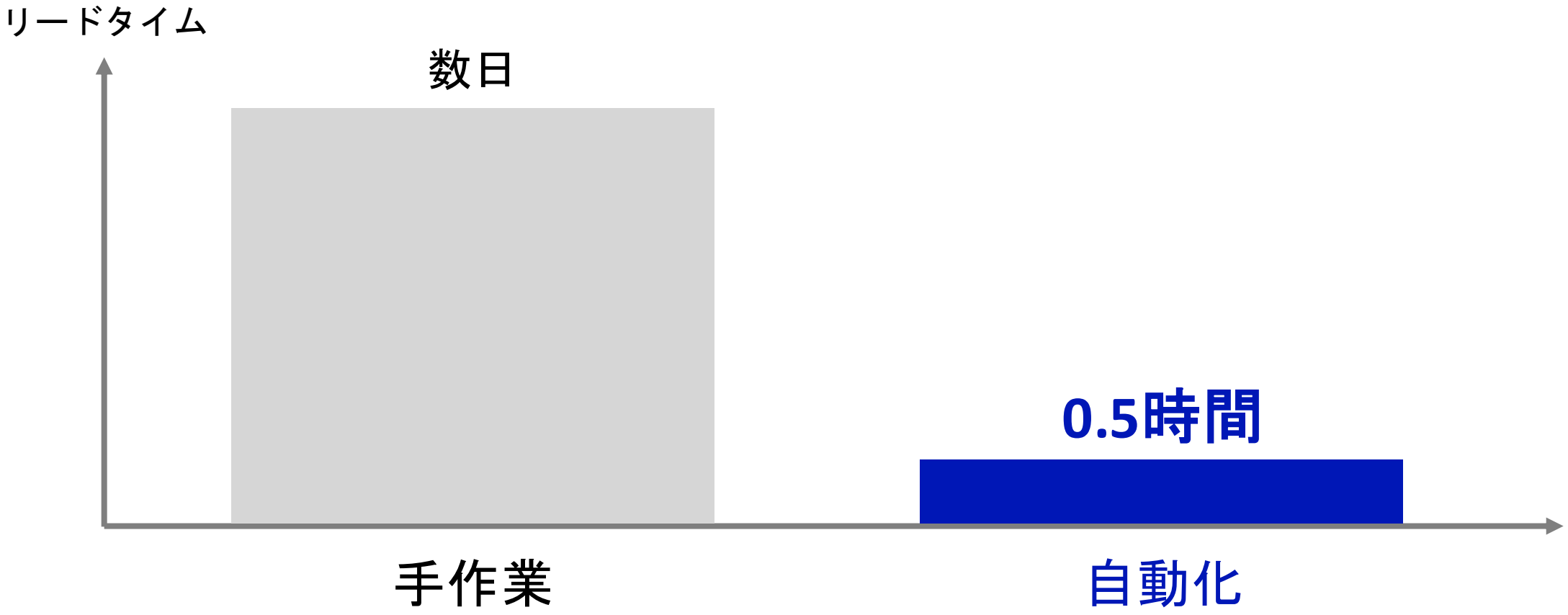


苦労したこと

自動化の阻害要因は他環境及び他チームとの連携

子テナンシーとの連携	• 必須適用テンプレート適用でエラーになることがあり、リトライの回数やリトライまでの時間を試行錯誤した • 大阪リージョンアクティベートなど時間がかかる処理の待ち時間も試行錯誤で最適な時間を設定した
他システムとの連携	• OCIとGoogle Cloud間でのWorkload Identity Federationによる認証の事例が少なく、手探り状態だった
他チームとの連携	• GCASおよび他CSPも並行して開発しており、APIの仕様決定までには密な情報連携が必要だった • GCASチームがAPIの仕様の叩き台を元に各CSPチームの要望を取り入れ仕様を確定し、API仕様を公開

自動化により、リードタイム削減と払い出し品質を向上



トラブル時の対応

自動化していても、エラーやトラブルはあるわけで

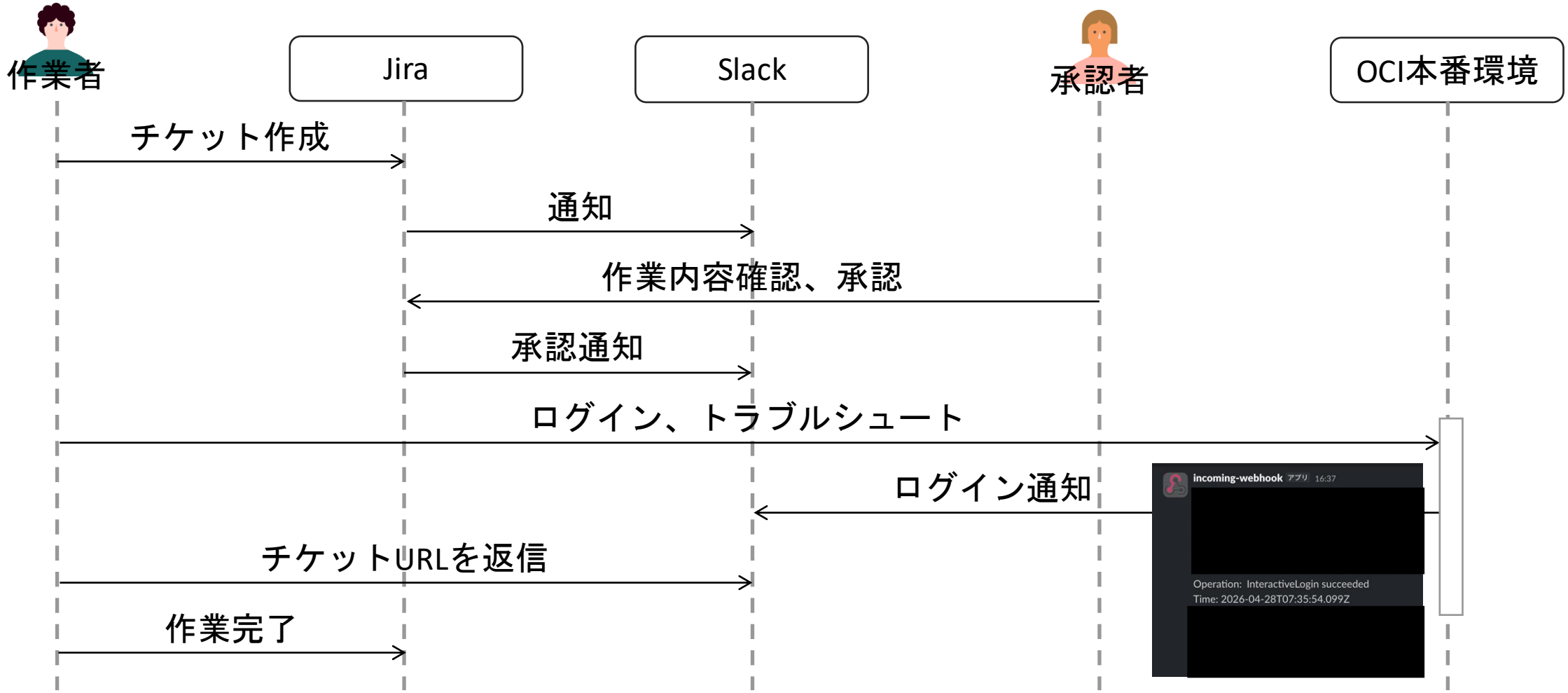
払い出しエラー時にはSlackで通知

ガバメントクラウドでは、セキュリティ、監査の観点で本番環境にログインしないようにしている

- 証跡管理
  - 誰が、いつ、何をしたのか記録が必要
- 最小権限の原則
  - 必要以上のアクセスはリスクになる
- 不正操作の防止
  - 人の手が入ることで意図しない変更が起こりうる

自動化、Slack連携により
通常運用時は、本番環境
にログインしない

トラブル時には証跡を残した上で本番環境にログインする



今後の展望、まとめ

完全自動化までの道のりはあと少し

認証の自動化	クラウドで最もリスクが高いと言われるAPIキーなどの永続的な資格証明を利用しないこと	
ジョブの自動化	GCASへ払い出し申請をトリガーとして、払い出しのジョブを自動で動かすこと	残る1回の手作業を自動化したい（具体的な方式は要検討）
インフラ管理の自動化	障害や高負荷時に人手を介さず対応できること	オートスケールなどを活用し、高負荷時の自律化、自動化を実現したい
監視の自動化	払い出しやエラーの状況を本番環境にログインせずに把握できること	Podの状態監視、通知機能の実装

自動化により、ガバメントクラウドの価値を高め続ける

- 自動化により手作業時に数日あったリードタイムを0.5時間に大幅削減
- 属人化を排除したことにより、作業の標準化と品質向上を実現
- デジタル庁自身が「迅速、柔軟、セキュア、コスト効率」を体現し、利用者への高い価値を提供する
- 完全自動化に向けて、引き続き改善を続けていく

デジタル庁

Digital Agency