ガバメントクラウドでの
予防的統制と発見的統制の考え方

2024年5月23日　デジタル庁 山本 教仁

デジタル庁
Chief Cloud Officer 山本教仁

外資系ITベンダーにてインフラ系デリバリーエンジニア、プリセールスアーキテクトを経て、2013年よりクラウドサービスプロバイダーにてコンサルティング組織を立ち上げ

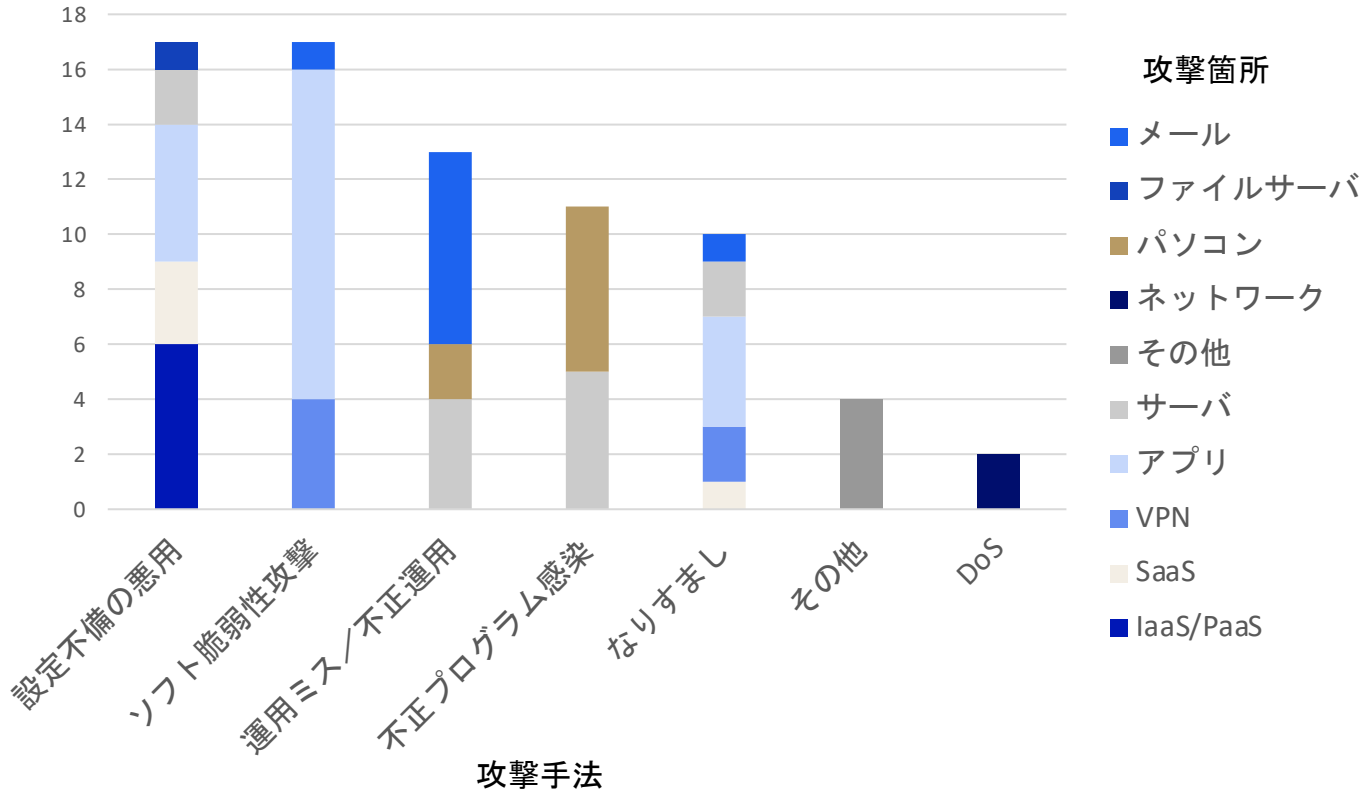
2020年4月に内閣官房政府CIO補佐官に着任
2021年9月のデジタル庁発足と同時にデジタル庁クラウドアーキテクトに就任
2023年1月よりガバメントクラウドのリード
2023年10月よりChief Cloud Officer

デジタル庁が整備するガバメントクラウドは、中央政府や地方公共団体、準公共分野向けのデジタル施策推進のための共通のクラウドサービス利用環境

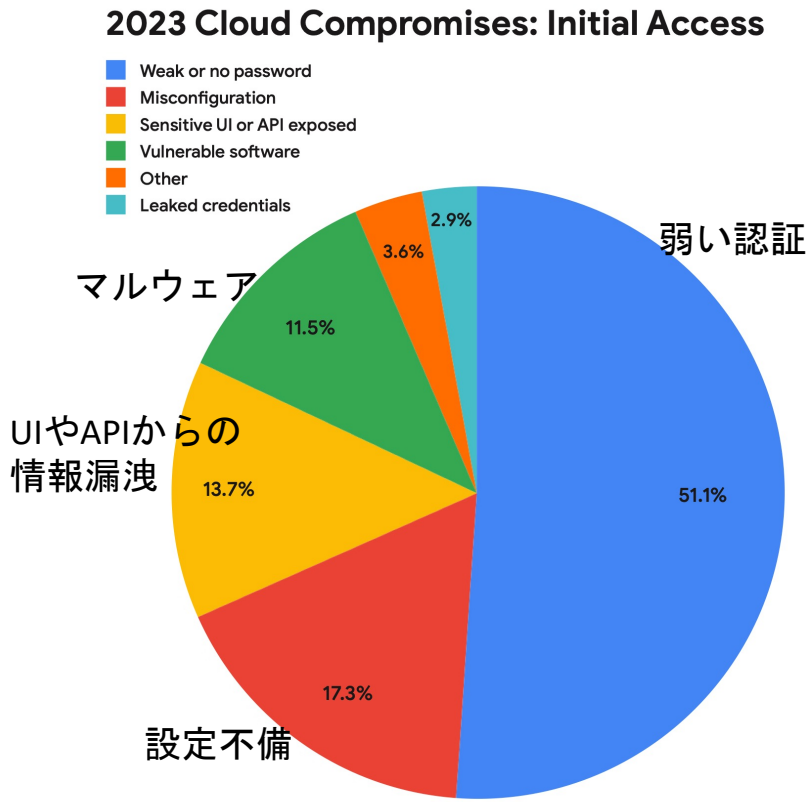
クラウドサービスの利点を最大限に活用して、迅速、柔軟、かつセキュアでコスト効率の高いシステムの実現を目指す

2023年のセキュリティインシデントのニュースの分類と、Google CloudのThreat Horizons Reportによるクラウド侵害要因の分類

2023年国内企業がニュースリリースを出し記事になったセキュリティインシデント138件のうち、攻撃手法がわかる74件の分類
（Google検索の期間指定で、nikkei.comの記事を抽出）



Google Cloud H1 2024 Threat Horizons Reportより
https://services.google.com/fh/files/misc/threat_horizons_report_h12024.pdf



ガバメントクラウドでの3つのセキュリティ対策

1 発見的統制

2 多要素認証

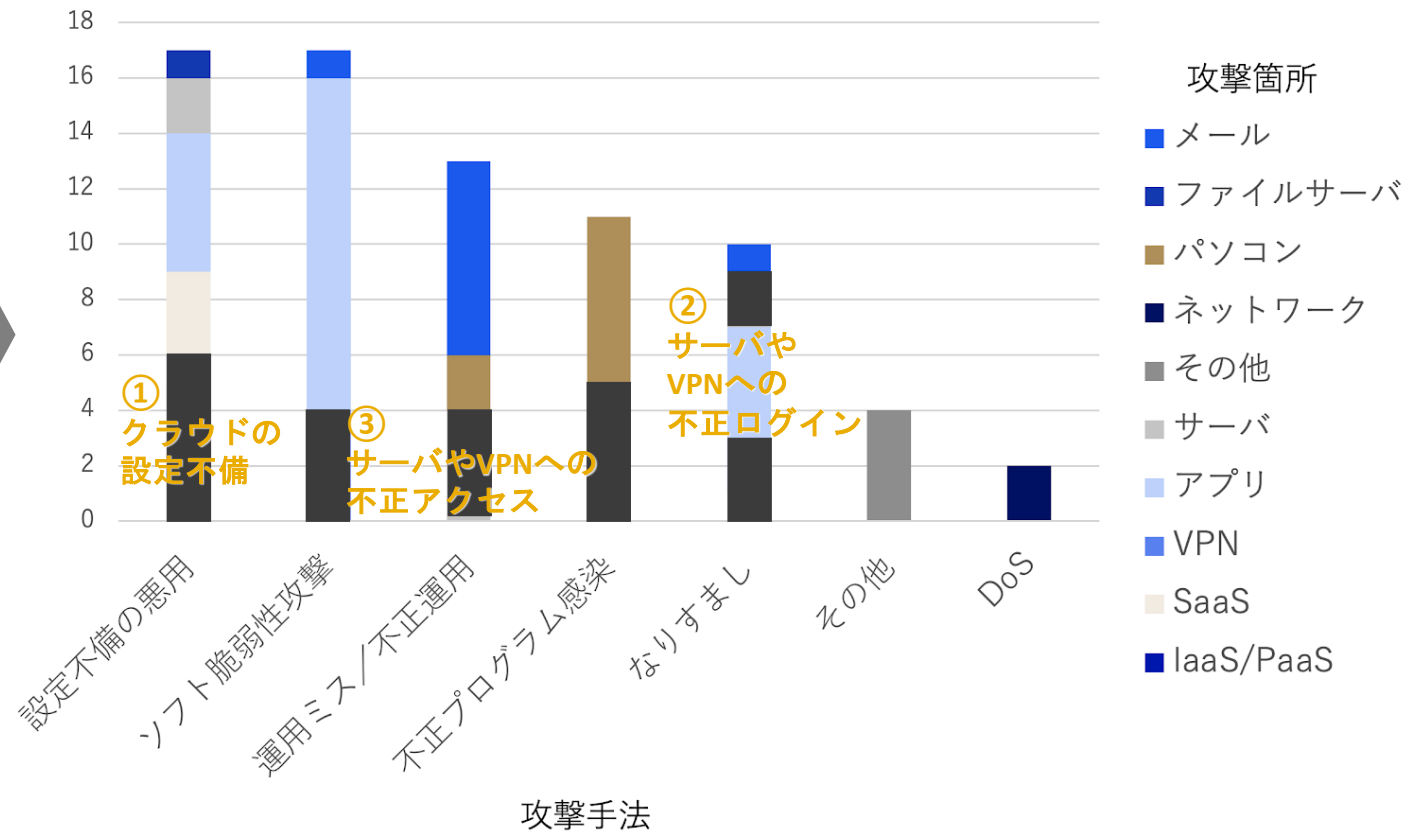
3 Zero Touch Production

シンプルなアーキテクチャと運用で実現する

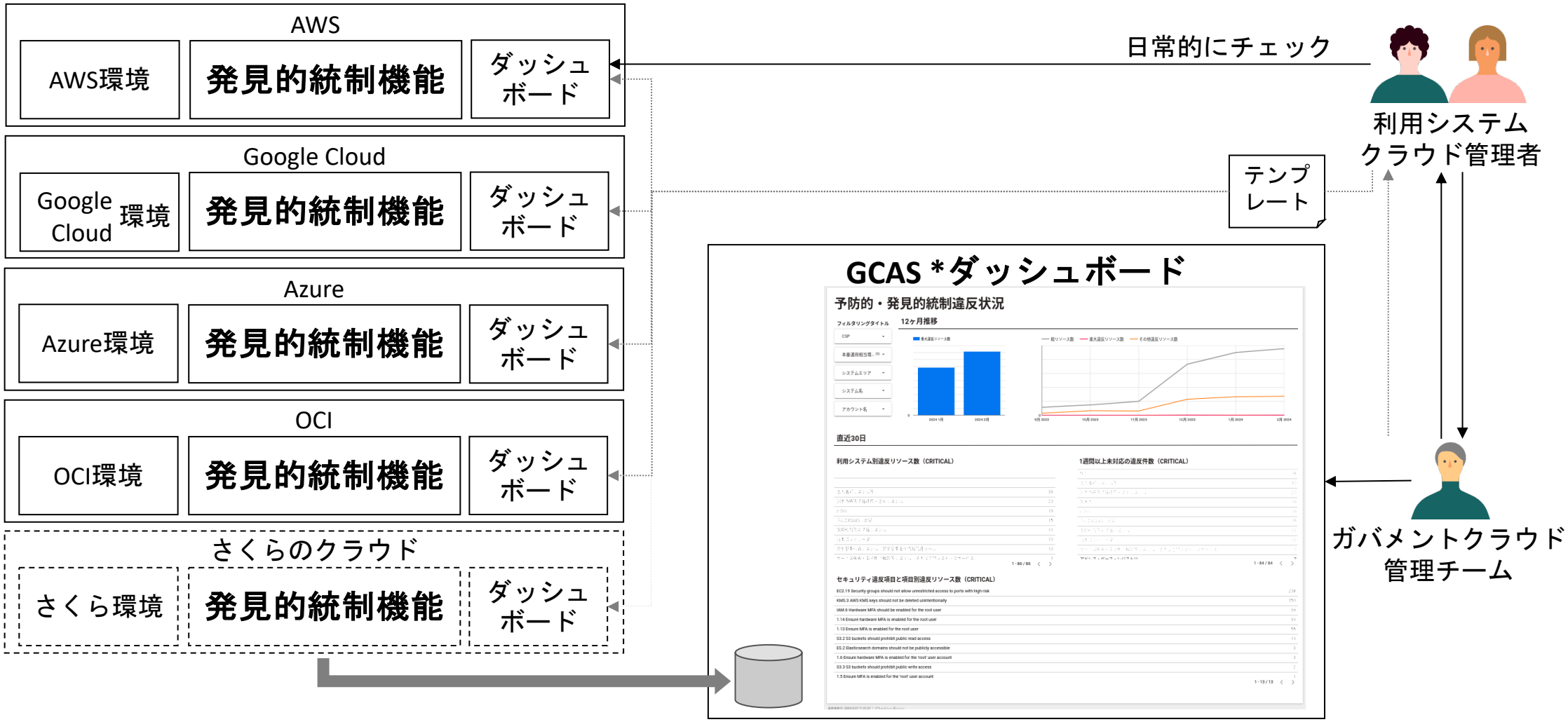
ガバメントクラウドでの3つのセキュリティ対策で防ぐこと

ガバメントクラウドでの3つのセキュリティ対策により、シンプルなアーキテクチャと運用を実現し、アプリケーションのセキュリティ対策にフォーカスする

1. 発見的統制
2. 多要素認証
3. Zero Touch Production

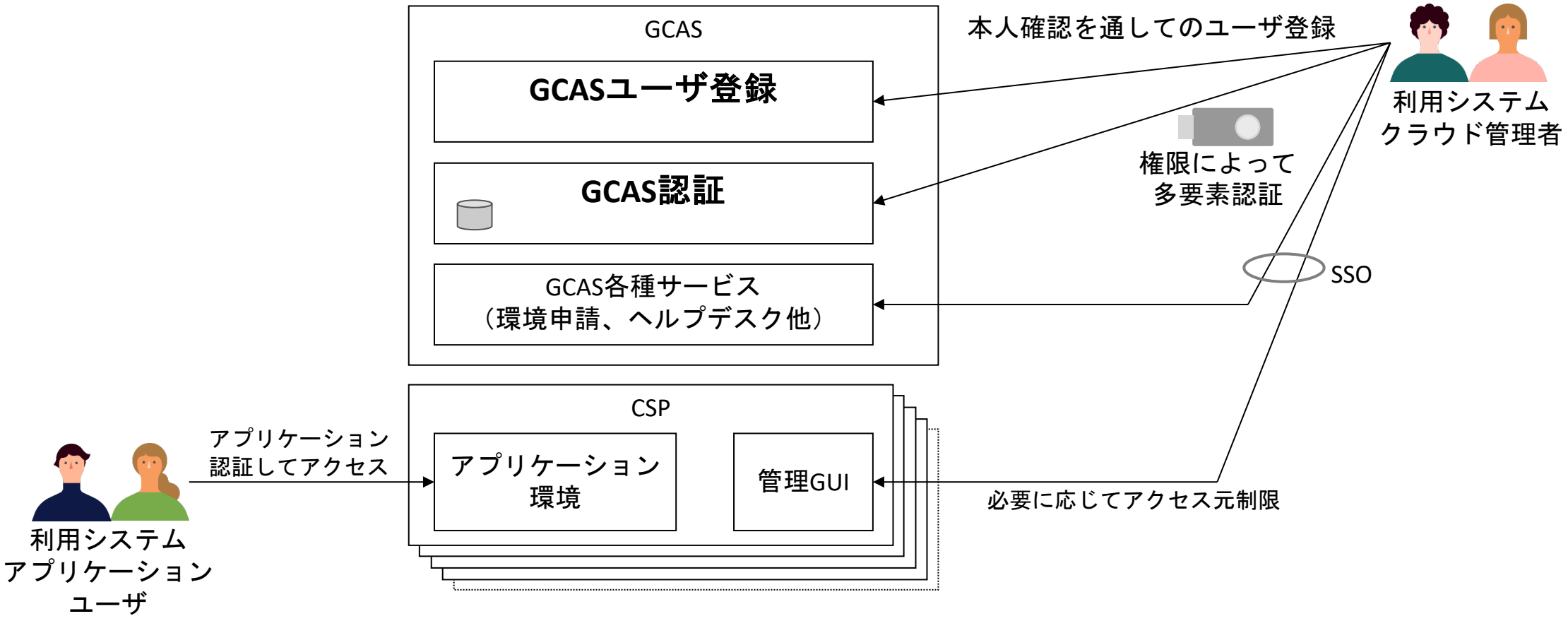


クラウドサービスの発見的統制機能で設定の不備や運用ミスを発見



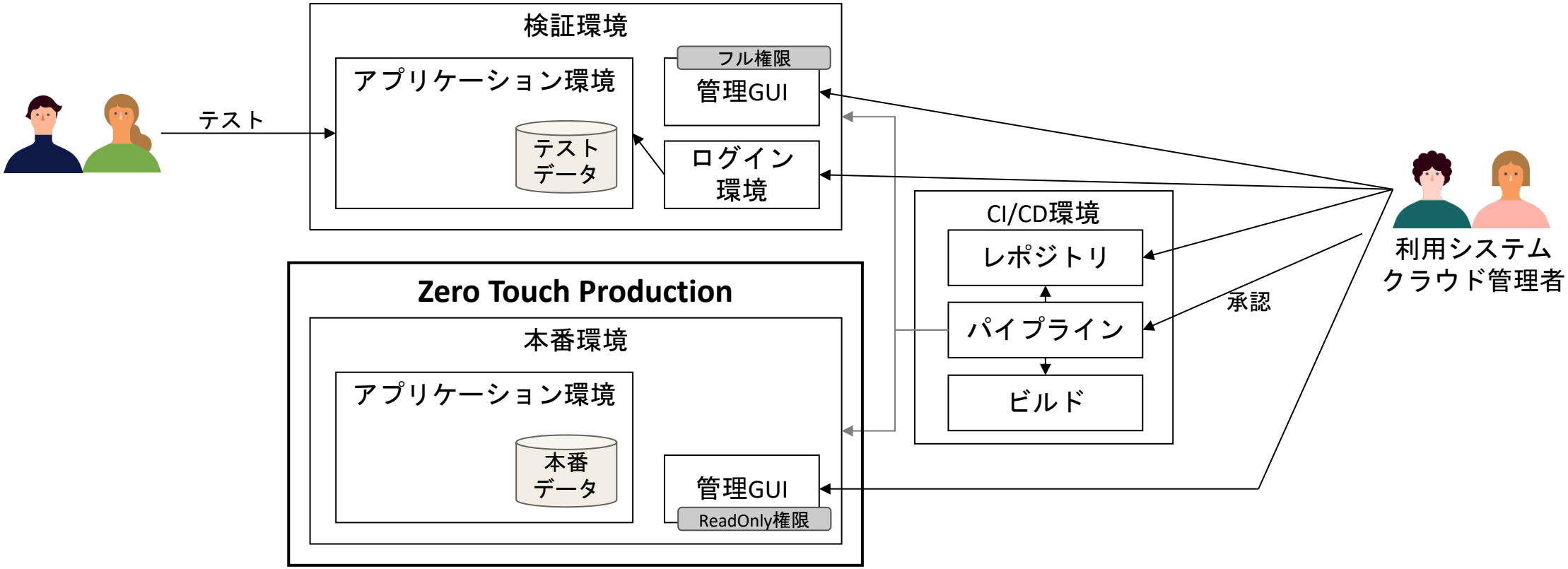
* GCAS：ガバメントクラウド支援サービス（Government Cloud Assistant Service）

クラウド管理GUIへのアクセスはGCASでユーザを一元管理しシングルサインオン（SSO）



ガバメントクラウドでの本番環境運用 - 3 Zero Touch Production

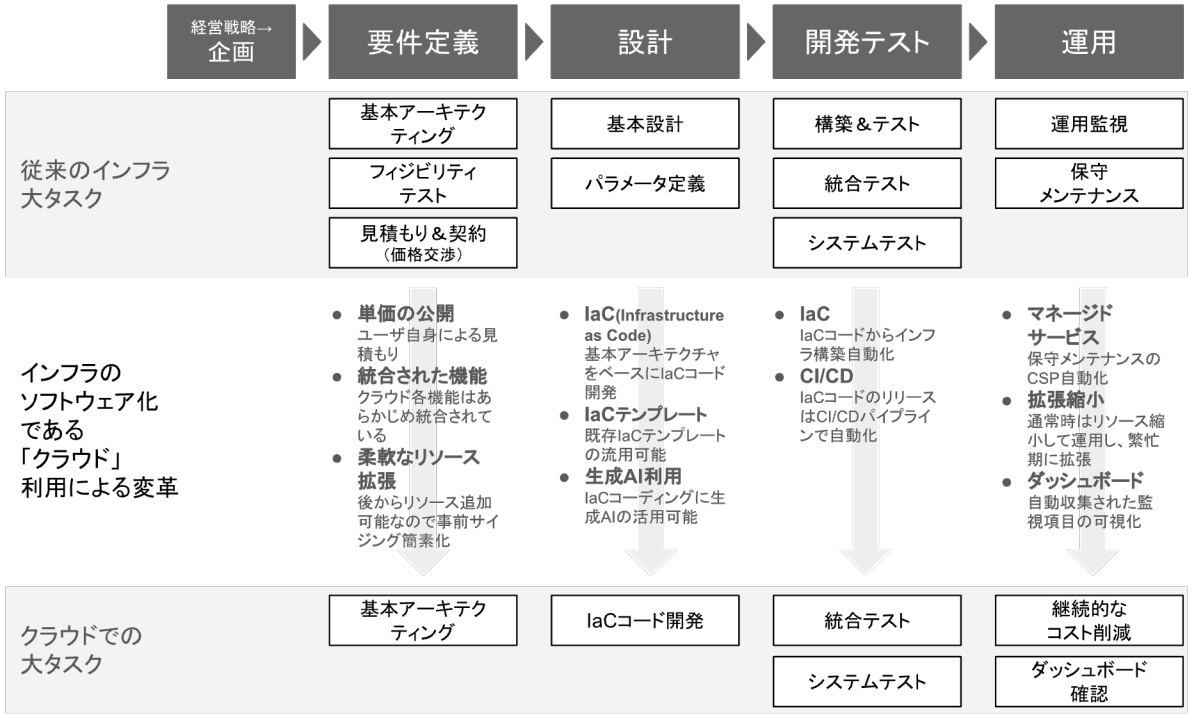
クラウドのマネージドサービスを使うことでサーバインスタンス＝ユーザが管理するOSが不要になる
IaC（Infrastructure as Code）でインフラを管理することで、本番環境の構築やメンテナンス作業をすべてコードで管理できるようになり、本番環境へのログインが不要になる
→本番環境に対する運用のためのアクセス経路がなくなる



ガバメントクラウドのnote記事

そもそもクラウドは、監査済みで、統合されテスト済みのサービスを活用できる
セキュリティにとっても、クラウドの活用はメリットが大きい、ただし、「賢く」使う必要がある
ガバメントクラウドでのクラウド利用については、今後もnote記事で配信

「クラウドサービスによるディスラプト（破壊的イノベーション）」



デジタル庁

Digital Agency