Google Cloud

Google Workspace で実現する ChatOps について

片岡 亮介

株式会社ジェーシービー
デジタルソリューション開発部 部長（担当）

Speaker

Ryosuke Kataoka

（ ryosuke.kataoka@jcblab.jp ）

Product Owner

(JDEP)

- ビジネスアジリティを高める開発部隊mgr.
- Cloud Native な Platform の PO
- Google Cloud は 20 年 4 月から本格利用中
- 好きな Google Cloud サービス : Cloud Spanner

What’s JCB

「Brand Holder」

世界中で JCB カードが使えるインフラを整え、
国内外の大手金融機関と提携し JCB ブランドカード会員を
世界中に拡げています。ブランドホルダーの機能は
国際ブランドを保有する企業のみが持っており、日本では
唯一 JCB だけが持つ機能です。

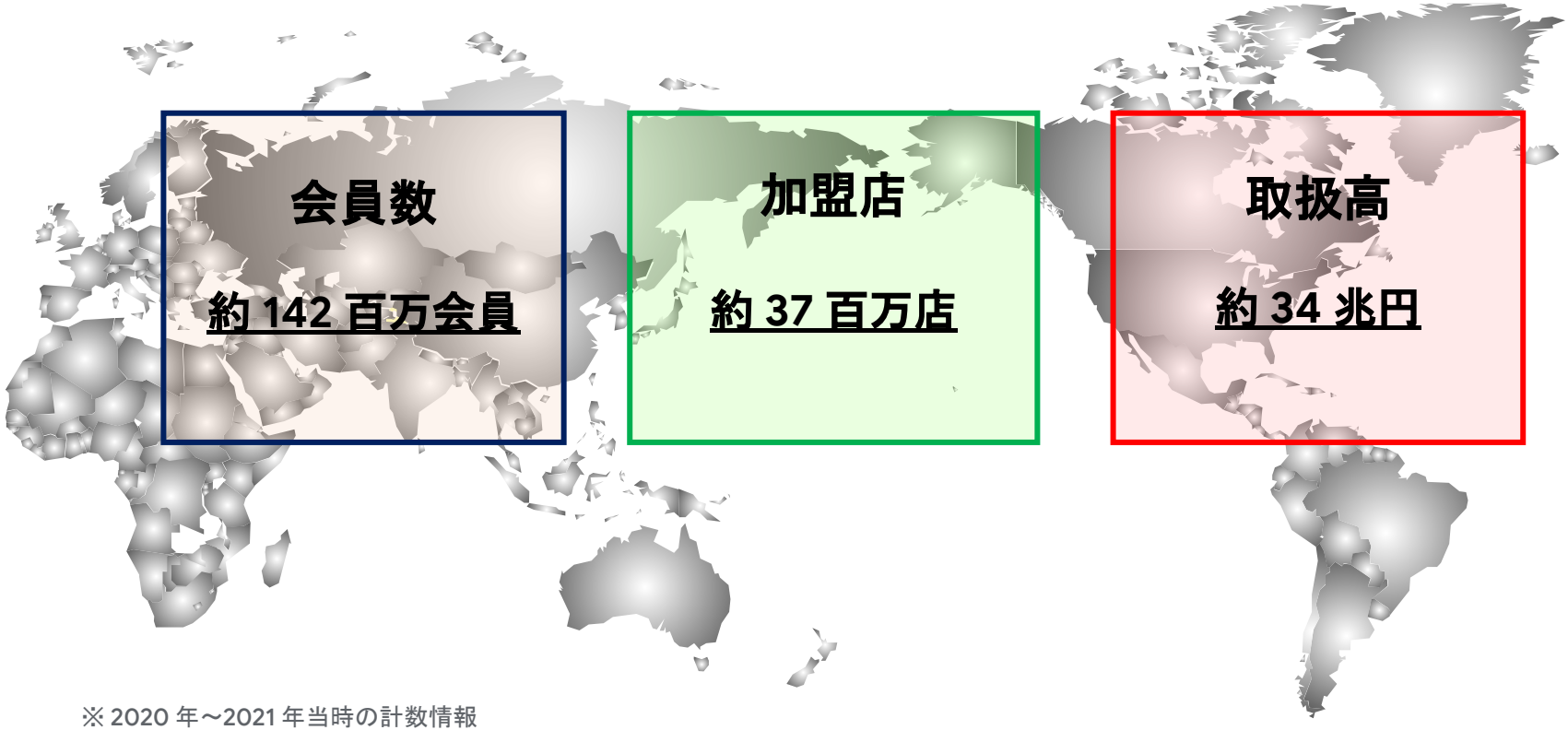
「Issuer」

カード会員の募集・発行、新規カードの立ち上げ、
カード付帯サービスをカード会員に提供しています。

「Acquirer」

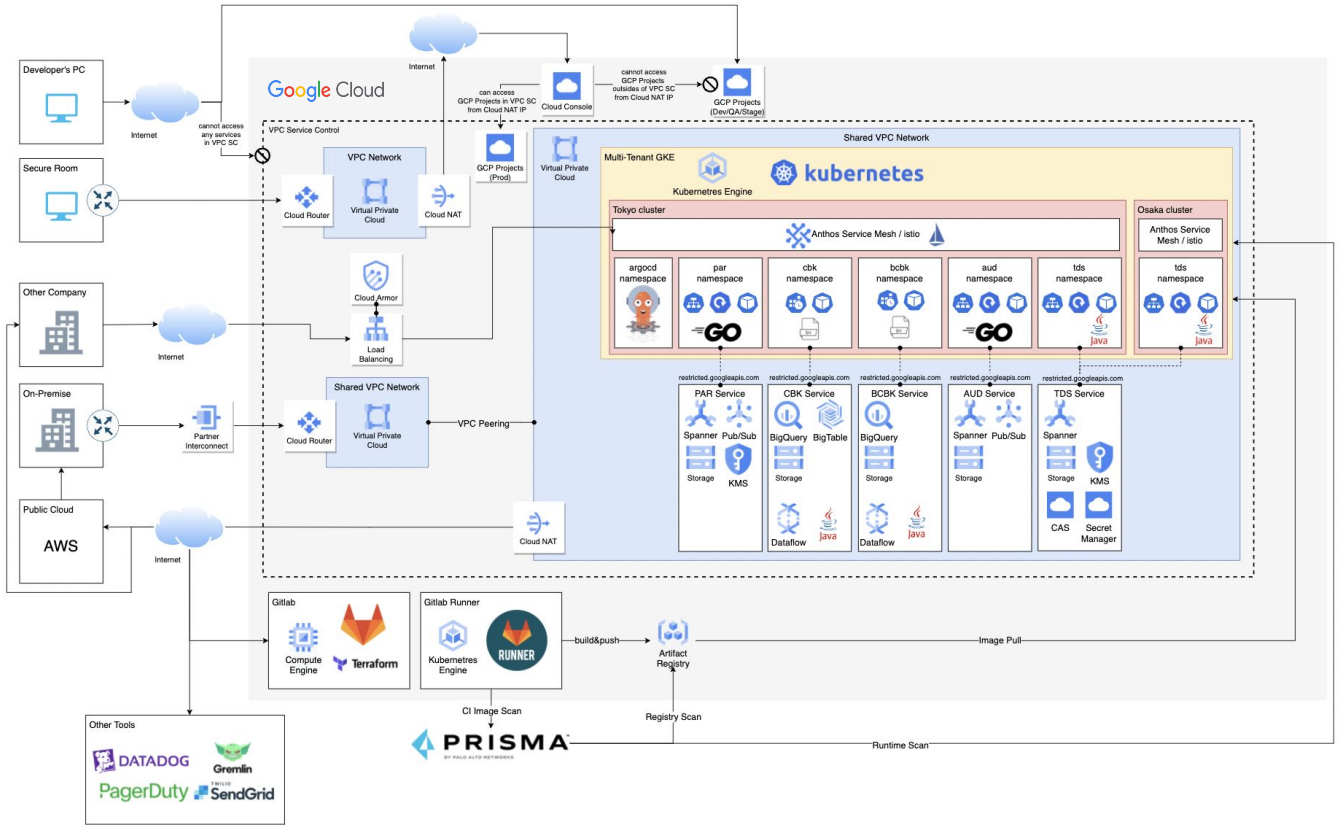
国内すべての加盟店との契約を担う
「シングルアクワイアリング」の強みを活かし、国内最大級
の加盟店ネットワーク網を構築・維持しています。

What's JCB



※ 2020 年～2021 年当時の計数情報

With Google



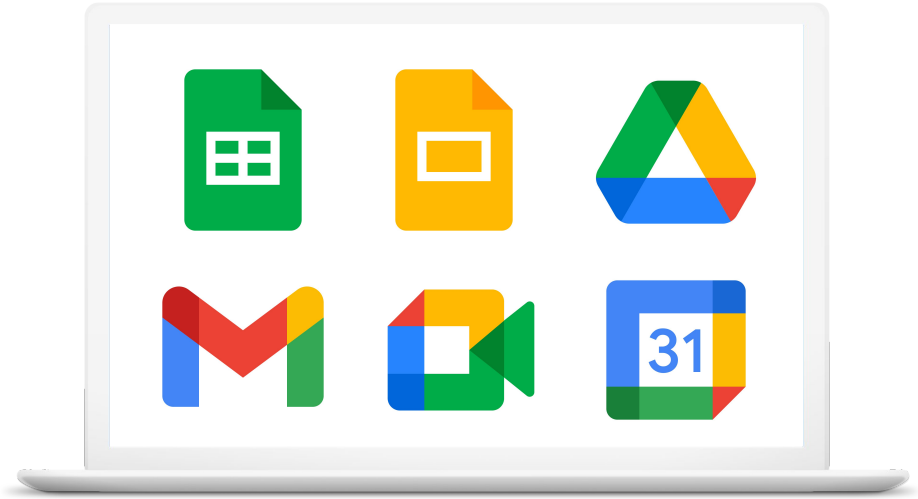
JCB Digital Enablement Platform

Google Cloud を用い GKE(Kubernetes) と Anthos Service Mesh(Istio)をコアプロダクトして構築。Cloud Spanner の特性を活かし東京/大阪両現運用を実現。

また、アジリティあるシステム開発を可能とするため、APL 開発は DDD 設計やマイクロサービスアーキテクチャを導入。

なお、Datadog や Gitlab など様々な外部サービスや OSS を積極活用。
低コストで柔軟な Platform とし、JCB のビジネスアジリティを高るコアプロダクトとして確立。

With Google



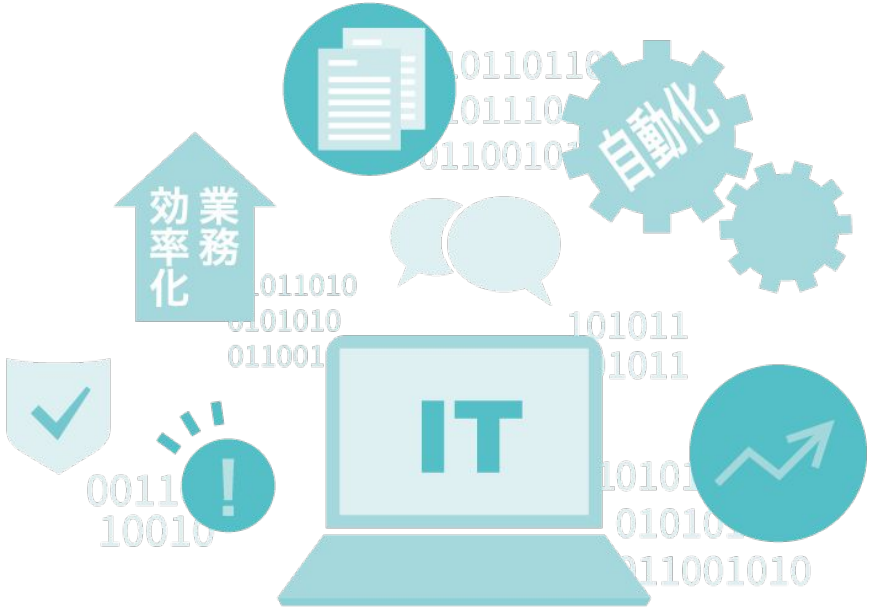
Google Workspace

ChatOps

Why ChatOps ?

ChatOps

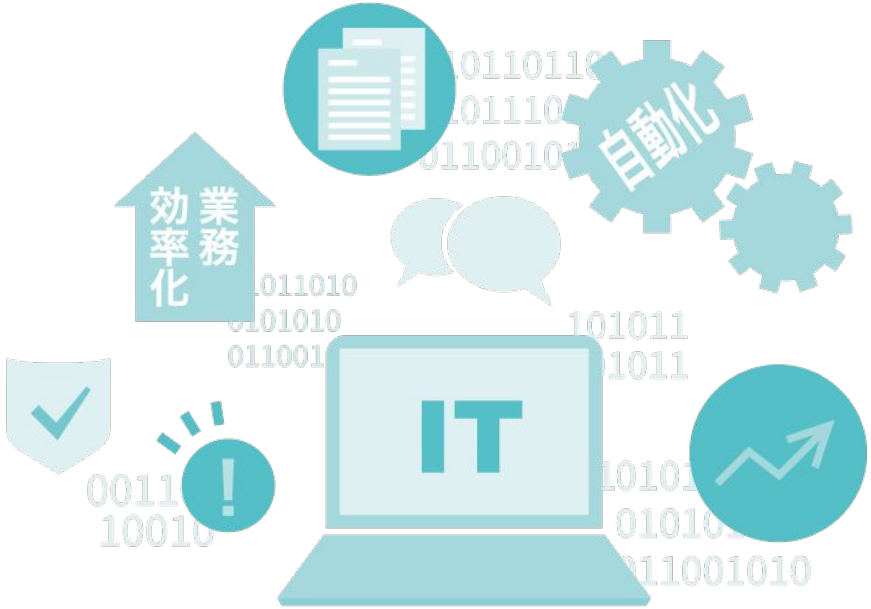
chat x operations を合わせた造語。利用者フレンドリーな Chat ベースの UI を活用し、様々な運用業務の自動化を図り、各種運用業務の高度化が実現できる。



Why ChatOps ?

メリット

- ❑ 運用業務の効率化
- ❑ アジリティ向上
- ❑ ミストラブル抑止
- ❑ コンプライアンス強化
- ❑ システム品質の向上



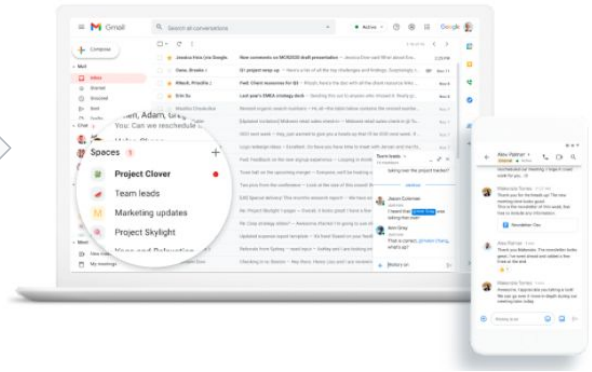
How ChatOps ?

How ChatOps ?

Operators

Developers

Chat



PagerDuty

Google Cloud

DATADOG

How ChatOps ?

PagerDuty

Google Cloud

DATADOG

How ChatOps ?

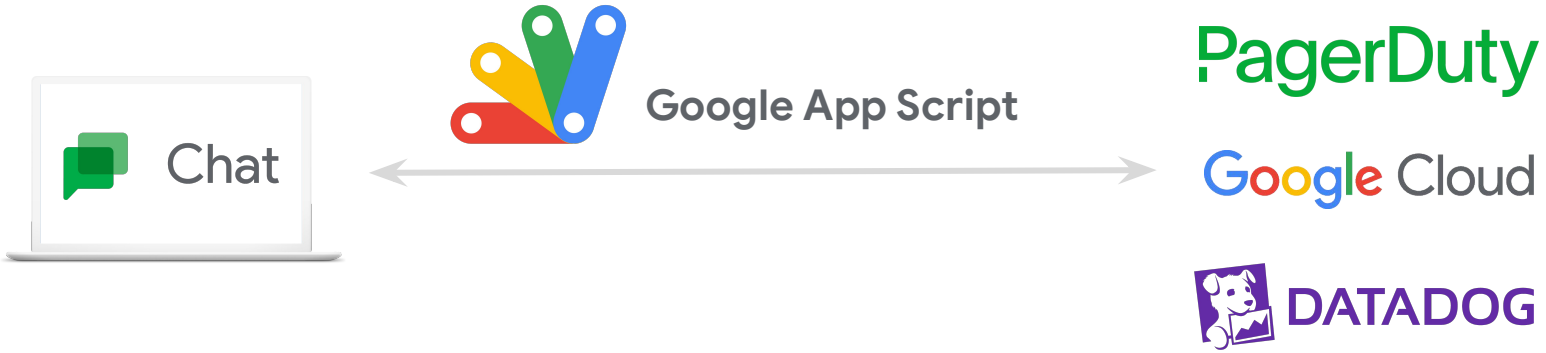
PagerDuty

Google Cloud

DATADOG

他 Chat に比べて各種ソリューション
との連携機能が劣る・・・

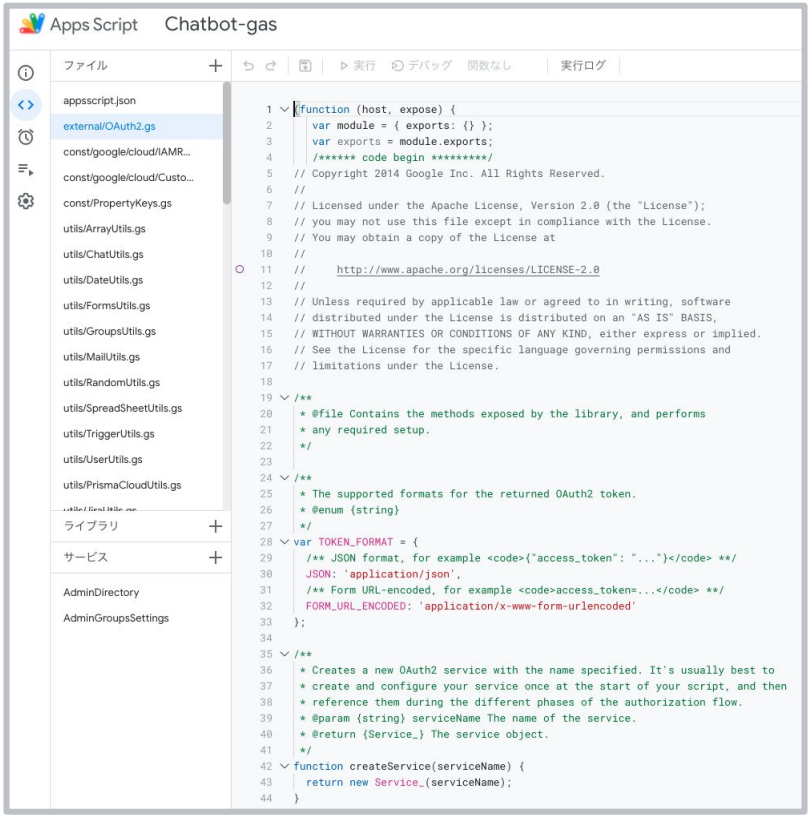
How ChatOps ?



How ChatOps ?

Google App Script

Google 社が提供するスクリプトプラットフォーム。JavaScript ベースでの開発言語であり、エンジニアが容易に開発することが可能。また、各種 Google プロダクトとの API ライブラリも提供されており、Google Workspace 全体を活用した ChatOps を実現できる。



Google Workspace の各種機能

Google フォーム

- 情報登録（INPUT）

スプレッドシート

- 加工用中間データ
- 操作履歴管理

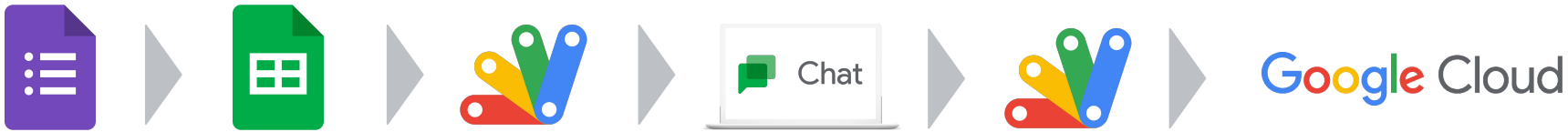
Google ドライブ

- 各種データ置き場
- データ保護（DLP）

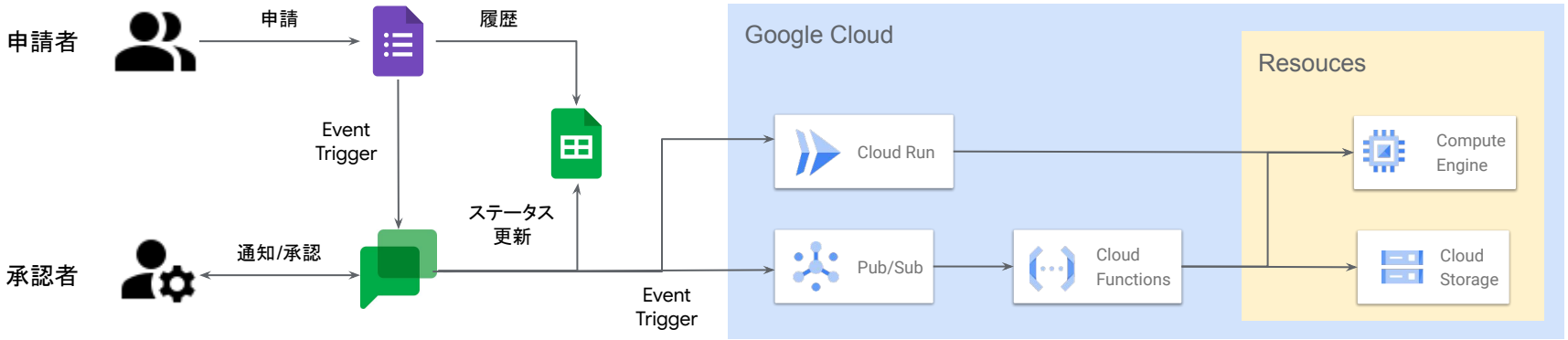
Gmail

- 情報共有
- 備忘メモ

ChatOps flows



ChatOps flows



Use Case

ChatOps Use Case

JCB では 2020 年から段階的に Google Chat を UI とした ChatOps の運用を導入。今では 50 を超える ChatOps が実装され、日々のシステム開発の活動で利用中。

なお、ChatOps はあくまでも手段の一つであり、根本目的は「運用業務の効率化」や「システム品質」などの向上や課題解決を行うことこと。

本日は JCB が実現している ChatOps を具体例を紹介させて頂く。

内容
システム ID の払出し
IAM 権限の付与
システムリリース（リソース配布）
システム構成違反の検知
インシデント発生時の連絡
Security アラート連絡
外部へのデータ持ち出し

etc...

ChatOps Use Case

JCB では 2020 年から段階的に Google Chat を UI とした ChatOps の運用を導入。今では 50 を超える ChatOps が実装され、日々のシステム開発の活動で利用中。

なお、ChatOps はあくまでも手段の一つであり、根本目的は「運用業務の効率化」や「システム品質」などの向上や課題解決を行うことこと。

本日は JCB が実現している ChatOps を具体例を紹介させて頂く。

内容
システム ID の払出し
IAM 権限の付与
システムリリース（リソース配布）
システム構成違反の検知
インシデント発生時の連絡
Security アラート連絡
外部へのデータ持ち出し

etc...

IAM 権限の付与

IAM 権限の付与

IAM は複雑なため、権限設定付与のミスに伴う
インシデント発生リスクが高い。また、ユーザに
高権限の IAM ロールを付与しておくことでの情報漏洩の
リスクも残存。

そのため、JCB ではユーザ ID に時間指定で IAM
ロールを付与する仕組みを ChatOps で行っている。

目的

- IAM 付与ミスに伴う作業ミスの抑止
- IAM 権限管理の適切化
  → 高権限付与の適正な管理
- ID・PW 管理の効率化（業務負荷軽減）

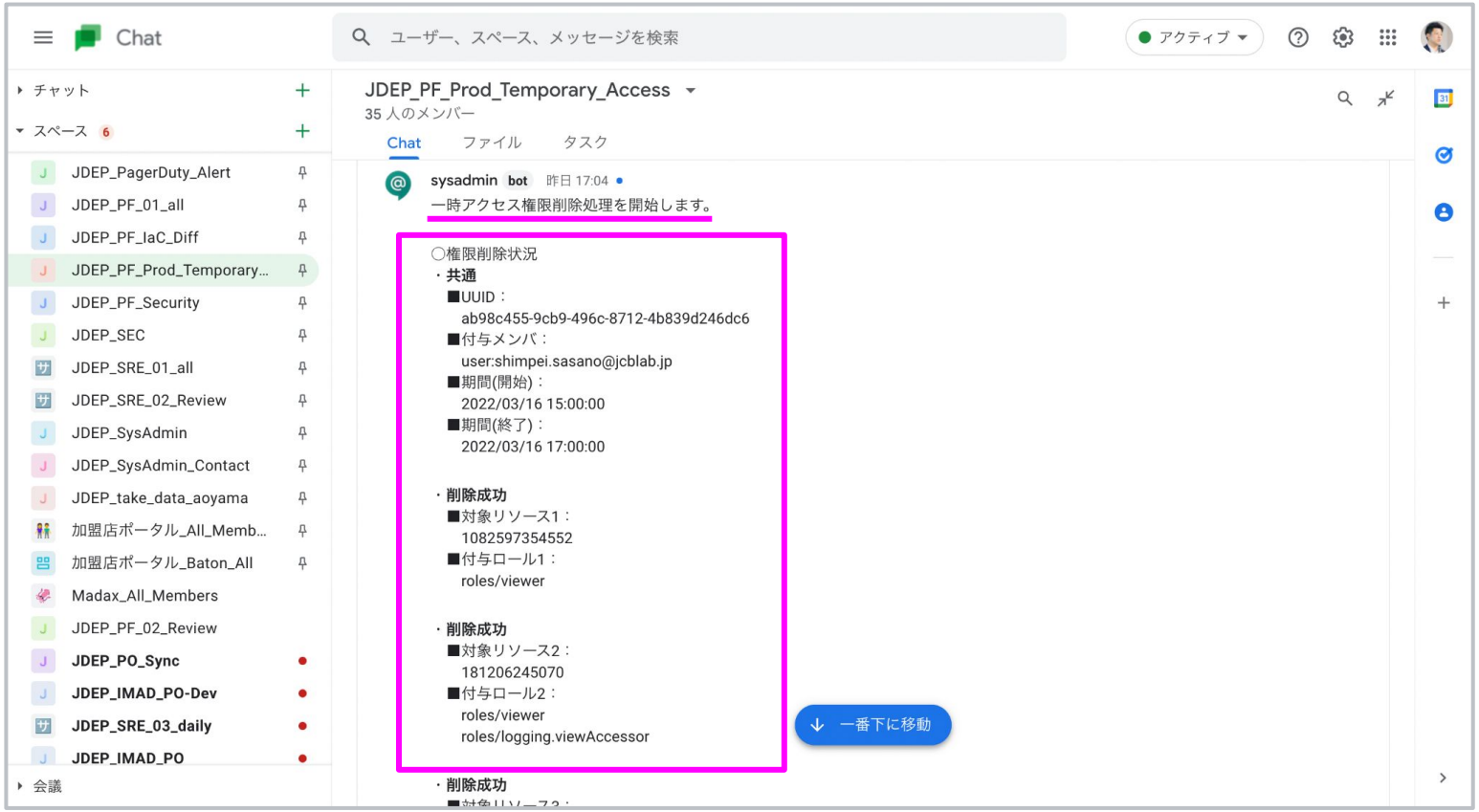
動画あり：視聴ページをご覧ください

Step1
権限申請

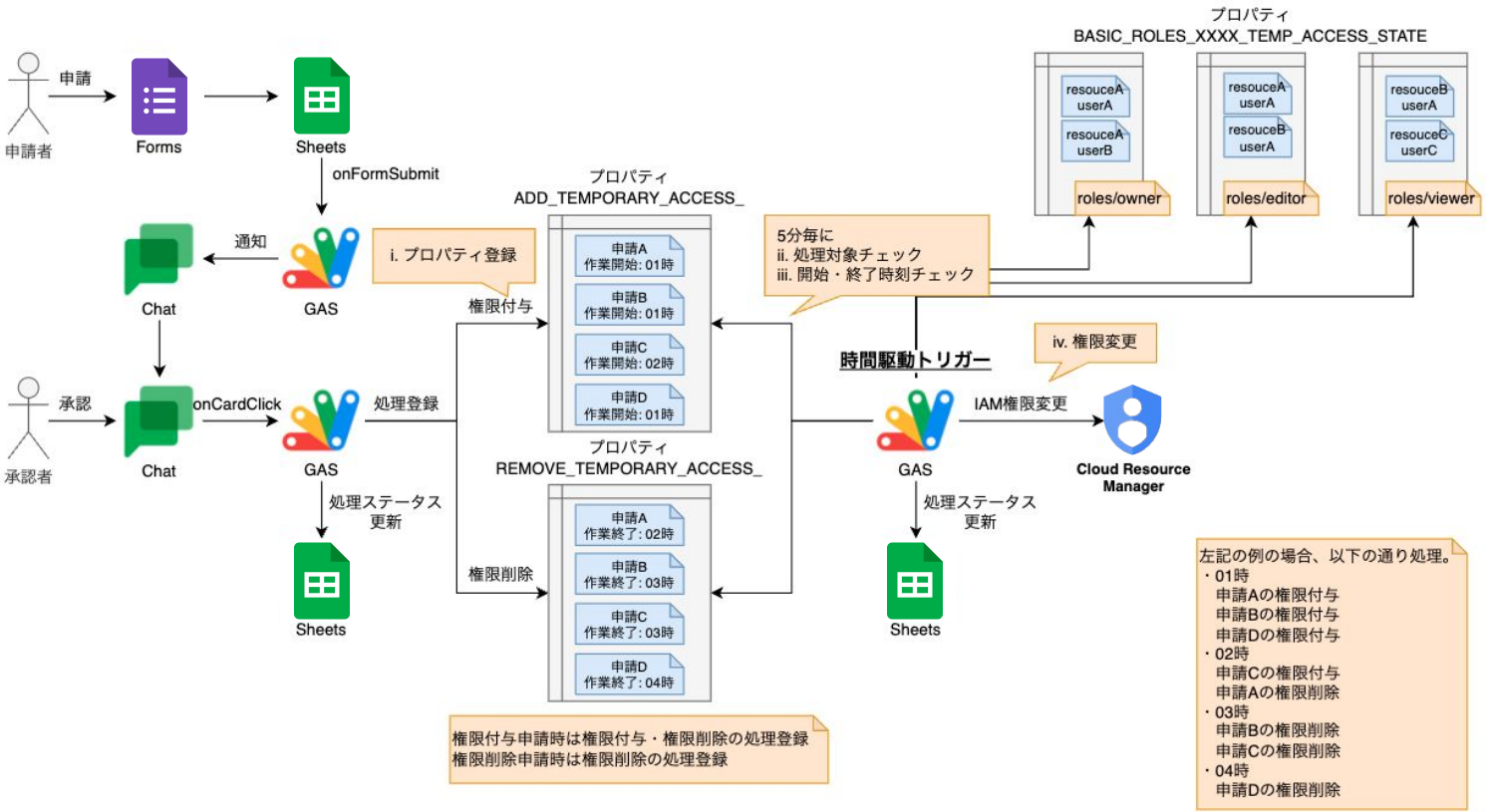
Step2
権限承認

動画あり：視聴ページをご覧ください

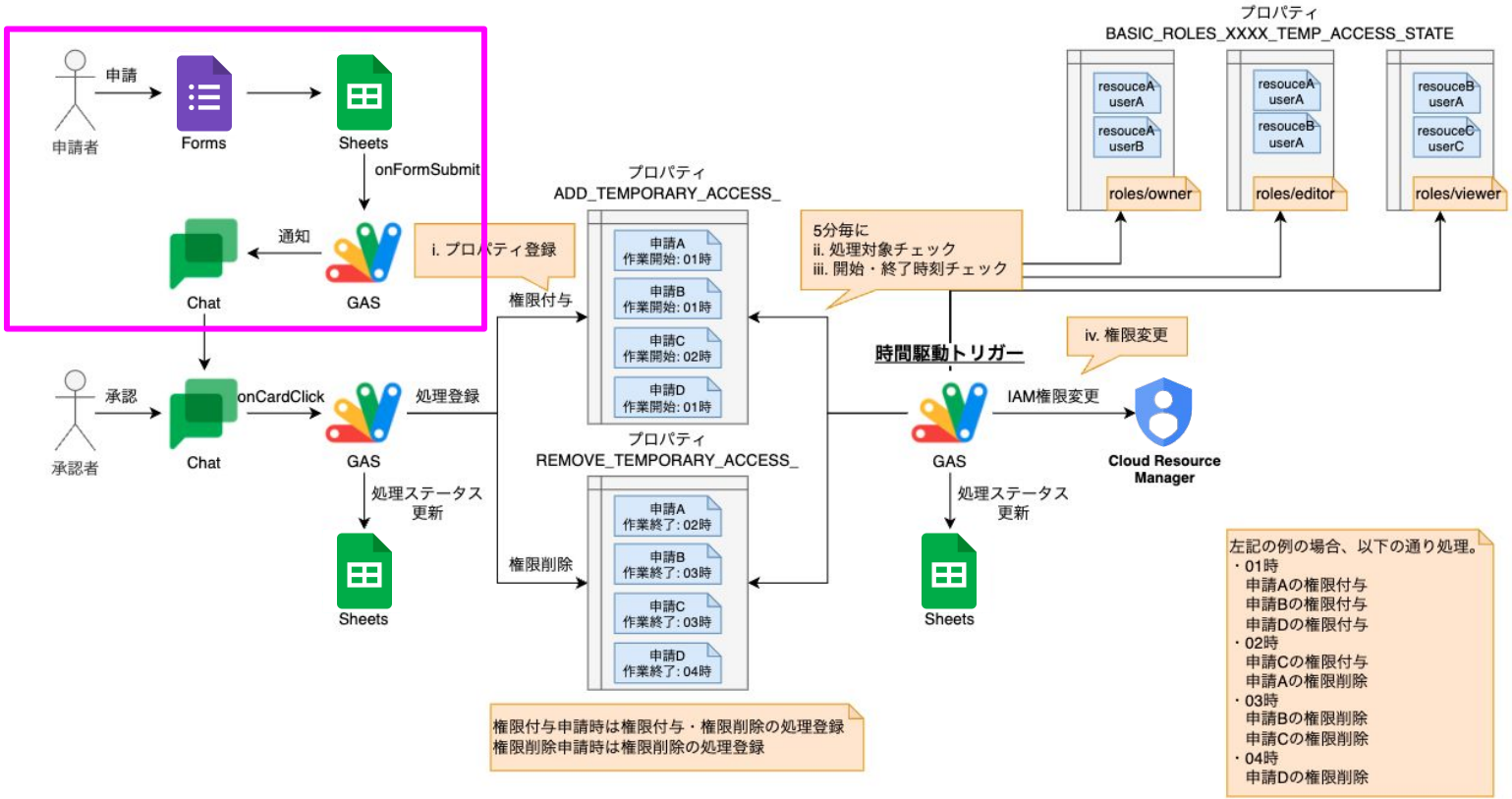
Step3
権限削除


Chat
ユーザー、スペース、メッセージを検索
アクティブ
チャット
スペース 6
JDEP_PagerDuty_Alert
JDEP_PF_01_all
JDEP_PF_IaC_Diff
JDEP_PF_Prod_Temporary...
JDEP_PF_Security
JDEP_SEC
JDEP_SRE_01_all
JDEP_SRE_02_Review
JDEP_SysAdmin
JDEP_SysAdmin_Contact
JDEP_take_data_aoyama
加盟店ポータル_All_Memb...
加盟店ポータル_Baton_All
Madax_All_Members
JDEP_PF_02_Review
JDEP_PO_Sync
JDEP_IMAD_PO-Dev
JDEP_SRE_03_daily
JDEP_IMAD_PO
会議
JDEP_PF_Prod_Temporary_Access
35 人のメンバー
Chat
ファイル
タスク
sysadmin bot 昨日 17:04
一時アクセス権限削除処理を開始します。
○権限削除状況
・共通
■UUID：
ab98c455-9cb9-496c-8712-4b839d246dc6
■付与メンバ：
user:shimpei.sasano@jcblab.jp
■期間(開始)：
2022/03/16 15:00:00
■期間(終了)：
2022/03/16 17:00:00
・削除成功
■対象リソース1：
1082597354552
■付与ロール1：
roles/viewer
・削除成功
■対象リソース2：
181206245070
■付与ロール2：
roles/viewer
roles/logging.viewAccessor
一番下に移動
・削除成功

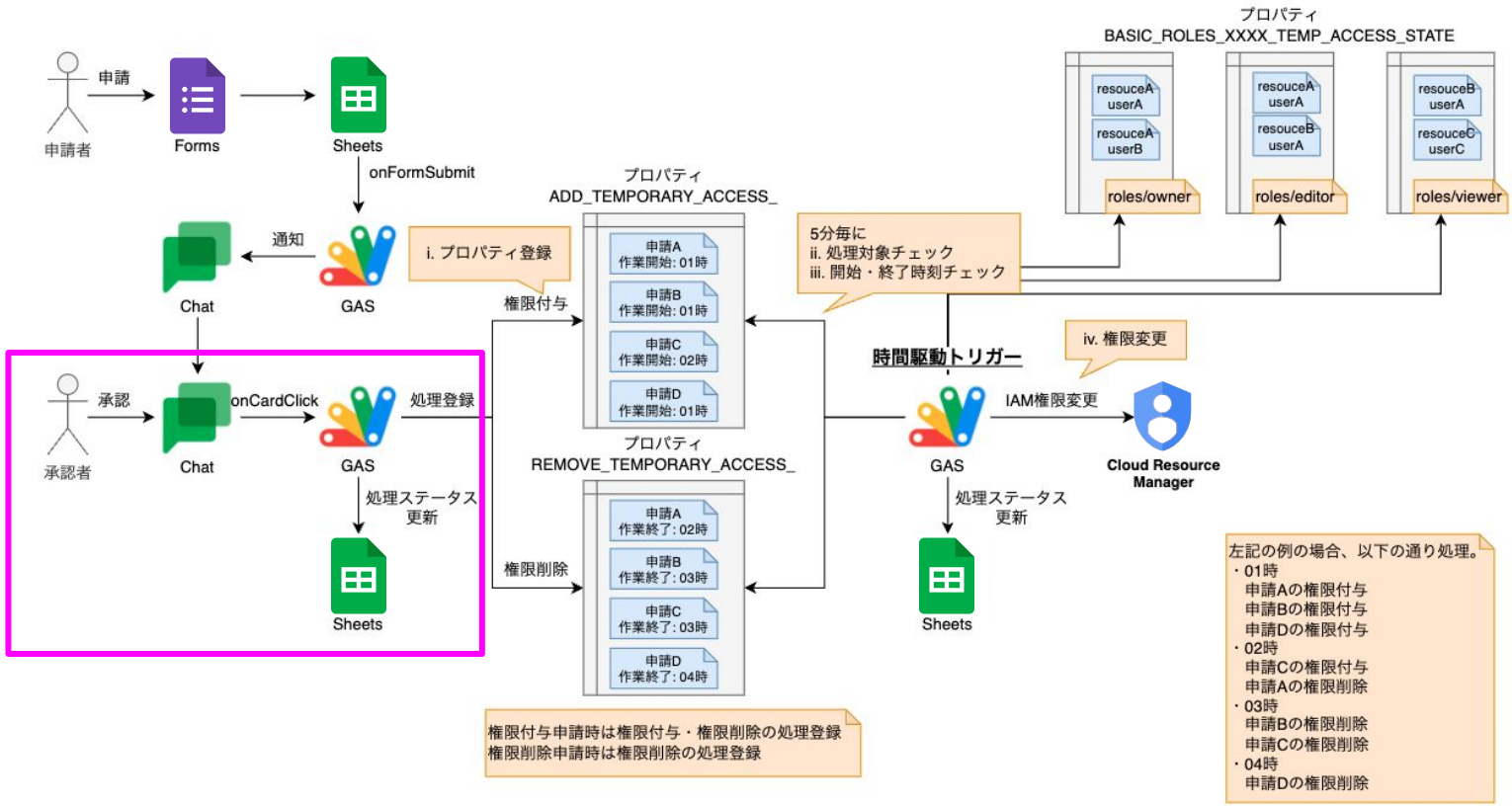
IAM 権限の付与


申請
申請者
Forms
Sheets
onFormSubmit
通知
Chat
GAS
i. プロパティ登録
プロパティ
ADD_TEMPORARY_ACCESS_
申請A
作業開始: 01時
申請B
作業開始: 01時
申請C
作業開始: 02時
申請D
作業開始: 01時
権限付与
プロパティ
BASIC_ROLES_XXXX_TEMP_ACCESS_STATE
resouceA
userA
resouceA
userB
roles/owner
resouceA
userA
resouceB
userA
roles/editor
resouceB
userA
resouceC
userC
roles/viewer
5分毎に
ii. 処理対象チェック
iii. 開始・終了時刻チェック
時間駆動トリガー
iv. 権限変更
承認
承認者
Chat
onCardClick
GAS
処理登録
IAM権限変更
Cloud Resource
Manager
処理ステータス
更新
Sheets
プロパティ
REMOVE_TEMPORARY_ACCESS_
申請A
作業終了: 02時
申請B
作業終了: 03時
申請C
作業終了: 03時
申請D
作業終了: 04時
権限削除
GAS
処理ステータス
更新
Sheets
権限付与申請時は権限付与・権限削除の処理登録
権限削除申請時は権限削除の処理登録
左記の例の場合、以下の通り処理。
・01時
申請Aの権限付与
申請Bの権限付与
申請Dの権限付与
・02時
申請Cの権限付与
申請Aの権限削除
・03時
申請Bの権限削除
申請Cの権限削除
・04時
申請Dの権限削除

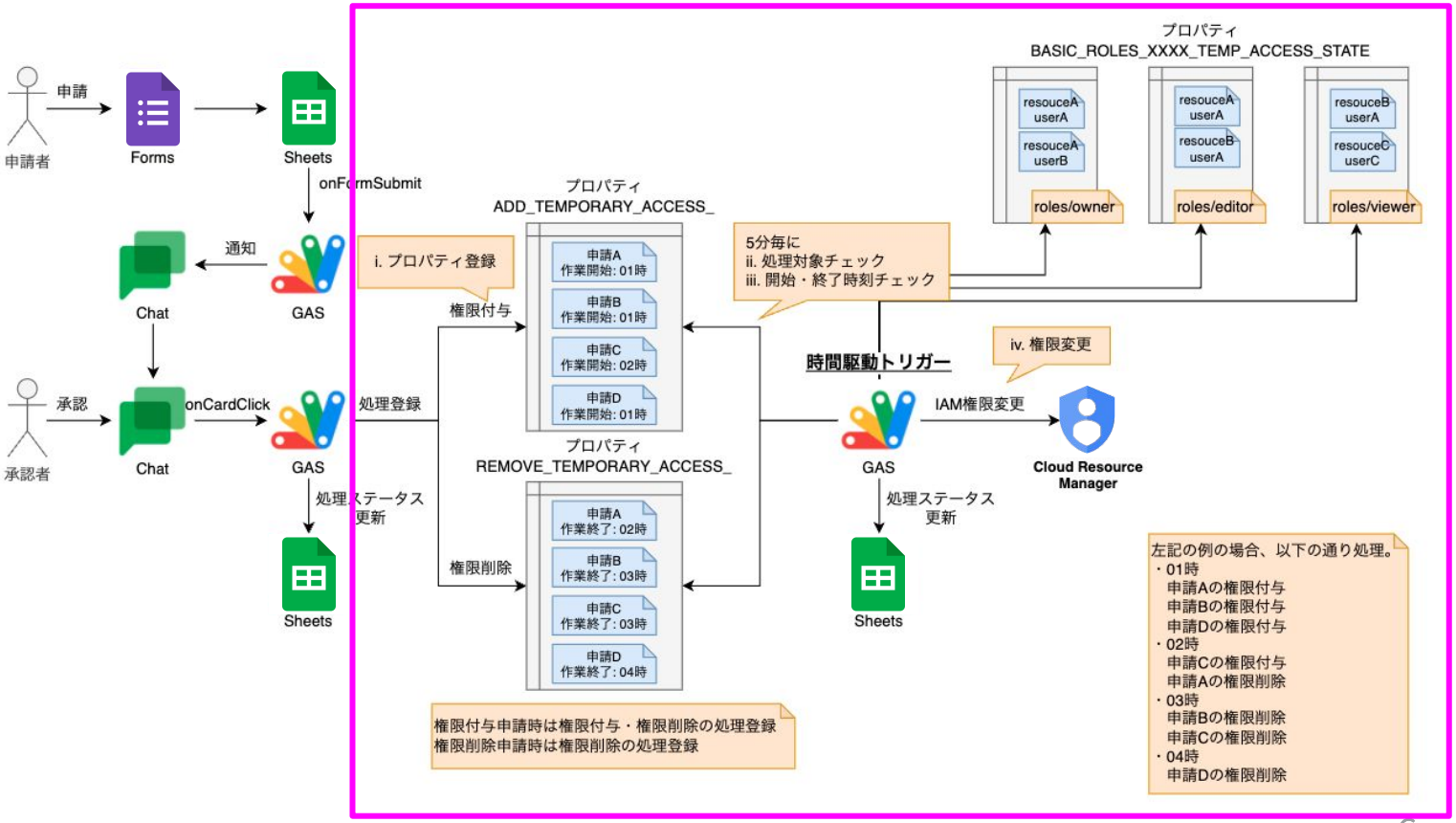
IAM 権限の付与


申請
申請者
Forms
Sheets
onFormSubmit
通知
Chat
GAS
i. プロパティ登録
承認
承認者
Chat
onCardClick
GAS
処理登録
処理ステータス
更新
Sheets
権限付与
権限削除
プロパティ
ADD_TEMPORARY_ACCESS_
申請A
作業開始: 01時
申請B
作業開始: 01時
申請C
作業開始: 02時
申請D
作業開始: 01時
プロパティ
REMOVE_TEMPORARY_ACCESS_
申請A
作業終了: 02時
申請B
作業終了: 03時
申請C
作業終了: 03時
申請D
作業終了: 04時
権限付与申請時は権限付与・権限削除の処理登録
権限削除申請時は権限削除の処理登録
プロパティ
BASIC_ROLES_XXXX_TEMP_ACCESS_STATE
resouceA
userA
resouceA
userB
roles/owner
resouceA
userA
resouceB
userA
roles/editor
resouceB
userA
resouceC
userC
roles/viewer
5分毎に
ii. 処理対象チェック
iii. 開始・終了時刻チェック
時間駆動トリガー
iv. 権限変更
GAS
IAM権限変更
Cloud Resource
Manager
処理ステータス
更新
Sheets
左記の例の場合、以下の通り処理。
・01時
申請Aの権限付与
申請Bの権限付与
申請Dの権限付与
・02時
申請Cの権限付与
申請Aの権限削除
・03時
申請Bの権限削除
申請Cの権限削除
・04時
申請Dの権限削除

IAM 権限の付与


申請
申請者
Forms
Sheets
onFormSubmit
通知
Chat
GAS
i. プロパティ登録
プロパティ
ADD_TEMPORARY_ACCESS_
申請A
作業開始: 01時
申請B
作業開始: 01時
申請C
作業開始: 02時
申請D
作業開始: 01時
権限付与
プロパティ
BASIC_ROLES_XXXX_TEMP_ACCESS_STATE
resouceA
userA
resouceA
userB
roles/owner
resouceA
userA
resouceB
userA
roles/editor
resouceB
userA
resouceC
userC
roles/viewer
5分毎に
ii. 処理対象チェック
iii. 開始・終了時刻チェック
時間駆動トリガー
iv. 権限変更
承認
承認者
Chat
onCardClick
GAS
処理登録
処理ステータス
更新
Sheets
IAM権限変更
Cloud Resource
Manager
GAS
処理ステータス
更新
Sheets
プロパティ
REMOVE_TEMPORARY_ACCESS_
申請A
作業終了: 02時
申請B
作業終了: 03時
申請C
作業終了: 03時
申請D
作業終了: 04時
権限削除
権限付与申請時は権限付与・権限削除の処理登録
権限削除申請時は権限削除の処理登録
左記の例の場合、以下の通り処理。
・01時
申請Aの権限付与
申請Bの権限付与
申請Dの権限付与
・02時
申請Cの権限付与
申請Aの権限削除
・03時
申請Bの権限削除
申請Cの権限削除
・04時
申請Dの権限削除

IAM 権限の付与


申請
申請者
Forms
Sheets
onFormSubmit
通知
Chat
GAS
承認
承認者
Chat
onCardClick
GAS
処理ステータス更新
Sheets
プロパティ
ADD_TEMPORARY_ACCESS_
i. プロパティ登録
権限付与
処理登録
申請A 作業開始: 01時
申請B 作業開始: 01時
申請C 作業開始: 02時
申請D 作業開始: 01時
プロパティ
REMOVE_TEMPORARY_ACCESS_
権限削除
申請A 作業終了: 02時
申請B 作業終了: 03時
申請C 作業終了: 03時
申請D 作業終了: 04時
権限付与申請時は権限付与・権限削除の処理登録
権限削除申請時は権限削除の処理登録
プロパティ
BASIC_ROLES_XXXX_TEMP_ACCESS_STATE
resouceA userA
resouceA userB
roles/owner
resouceA userA
resouceB userA
roles/editor
resouceB userA
resouceC userC
roles/viewer
5分毎に
ii. 処理対象チェック
iii. 開始・終了時刻チェック
時間駆動トリガー
iv. 権限変更
GAS
IAM権限変更
Cloud Resource Manager
処理ステータス更新
Sheets
左記の例の場合、以下の通り処理。
・01時
申請Aの権限付与
申請Bの権限付与
申請Dの権限付与
・02時
申請Cの権限付与
申請Aの権限削除
・03時
申請Bの権限削除
申請Cの権限削除
・04時
申請Dの権限削除

IAM権限の付与

ポイント

事前に必要となる作業内容と IAM ロールをマッピングしておくことが重要。

上記により IAM ロールの付与不正に伴うミストラブルが抑止できる。

role名	障害解析	DBリストア	閲覧
roles/viewer	●	●	●
roles/spanner.databaseUser	●		
roles/pubsub.editor	●		
roles/cloudkms.cryptoKeyEncrypterDecrypter			
roles/cloudkms.publicKeyViewer			
roles/cloudfunctions.developer			
roles/iam.serviceAccountUser			
roles/storage.objectAdmin			
roles/logging.configWriter			
roles/cloudkms.admin			
roles/spanner.backupAdmin		●	
roles/spanner.restoreAdmin		●	
roles/spanner.databaseAdmin		●	
roles/serviceusage.serviceUsageConsumer		●	
roles/storage.admin			
roles/cloudscheduler.admin			
roles/pubsub.admin			
roles/vpcaccess.user			
roles/logging.viewAccessor	●	●	●

IAM 登録のチェック

IAM 構成のチェック

サービスアカウントに付与している IAM 情報と、IAM 設計情報を Daily で差分比較チェックを実施。最新状態が正しい状態を担保。

GCPリソース差分監査ツール bot 3月9日, 8:40

IAM差分監査結果(2022/03/09)

■請求先アカウント
・差分なし

■組織
・差分なし

■Folder
・差分なし

■Organization
・差分なし

■common-dev
・差分なし

■common-prod
・差分なし

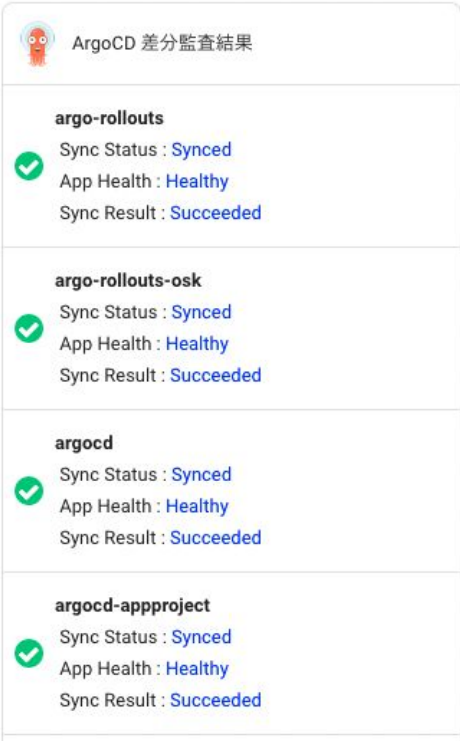
■dev
・差分なし

■prod
・Spreadsheet:記載あり / GCP：設定なし
jdep-prod-bcbk,func-verify-cbk-sq@jdep-prod-bcbk.iam.gserviceaccount.com,Pub/Sub 閲覧者

その他 ChatOps

インシデント情報通知

外部へのFile持ち出し申請



リリース結果の確認

まとめ

- ChatOps は**目的（実現したいこと）**を考えて導入することが需要
- ChatOps の効果は、単なる効率化には止まらない
- ChatOps の実現に Google Workspace を駆使することも選択肢
- Google Workspace で ChatOps を実現するための Keytool は GAS

Thank you.

Google Cloud