
aws
SUMMIT
TOKYO | APRIL 20-21, 2023

CUS-11

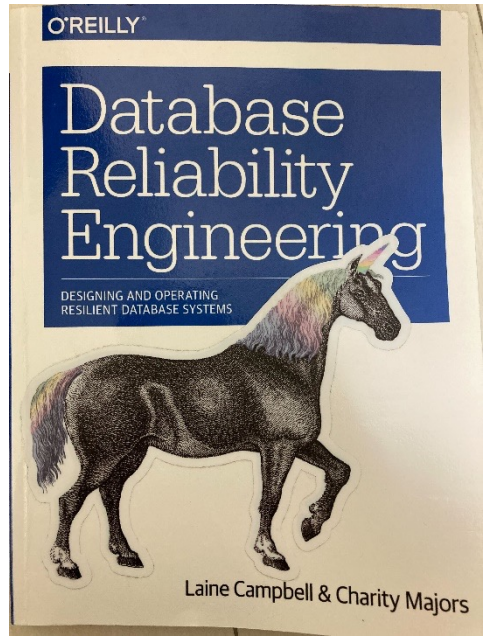
クルマのサブスク「KINTO」のアジリティとガバナンスを両立するDBREの取り組み

粟田 啓介
KINTO テクノロジーズ株式会社
シニア DBRE エンジニア

Database Reliability Engineering (DBRE) とは

Software Engineering と Database 管理の Best Practice を組み合わせたアプローチ

- 主な役割
  - SLO/SLI を測定しそれに合わせた開発組織へのアプローチ
  - 自動化、自律化推進による生産性の向上
  - Backup/Restore などサービスの稼働率の向上
  - Database セキュリティ & ガバナンスの担保
  - 他分野のスペシャリストとの分野を超えたコラボレーション



Database に対する専門知識と判断を用いてサービスの**信頼性を担保する**こと

DBRE (DBA) は企業にとって必要？

Public Cloud の台頭により Database Engineer の必要性が小さくなってきている

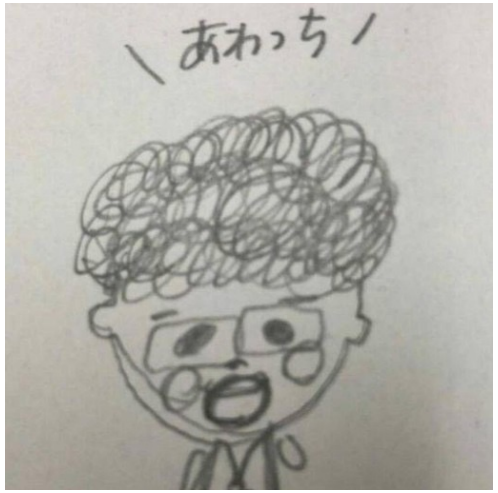
- Cloud によって誰でも一定のレベルで解決できる土壌が揃っている
  - Cloud 技術の爆発的な発展
  - DevOps /SRE 思想の醸成
  - AI 技術の進歩

- Database そのものに対する基本的なアプローチはこれまでと変わっていない
  - 環境分離
  - 構成管理
  - パフォーマンス測定
  - Backup/Restore
  - セキュリティ対応, etc.

変化しているのは Database を取り巻く周りの環境

KINTO Technologies

自己紹介




```
mysql > SELECT * FROM me ¥G
*************************** 1. row ***************************
    name: 粟田 啓介
nickname: あわっち
 company: KINTO テクノロジーズ株式会社
 twitter: @_awache
    role: DBRE, CCoE
favorite: Amazon RDS for MySQL / AWS Trusted Advisor
1 rows in set (0.00 sec)
```


KINTO Technologies

本セッションについて

KTC はなぜ DBRE を組成したのか、私たちの具体的な Activity の共有

セッション対象者

- DBRE の活動に興味がある方
- ビジネスと RDB 管理をどのように結びつけているかを知りたい方

セッションのゴール

- 自分たちの組織に DBRE が必要かどうか検討することができること
- KTC の DBRE が何をどのようにアウトプットしているのかをお持ち帰りいただくこと

お話ししないこと

- Amazon Aurora MySQL 以外の Database 領域の話

KINTO テクノロジーズ株式会社について

KINTO テクノロジーズ (通称: KTC) の手がけるプロダクト

クルマのサブスク「KINTO」をはじめとして様々なモビリティサービスを展開

KINTO ONE

KINTOで手軽にマイカーを。
車のサブスクリプションサービス

任意保険や自動車税など、クルマにかかる諸経費がコミコミ月々定額のクルマのサブスクリプションサービスです。WEBでも簡単にお申込みから契約までできて、気軽にカーライフを始めることができます。

https://kinto-jp.com/

KINTO FACTORY

クルマのオーナーに向けた
愛車のカスタム・機能向上サービス

トヨタ・レクサス既販車のソフトウェア・ハードウェアの機能やアイテムを最新の状態に「進化」させるサービスです。購入時設定が無かったオプションの後付けや、経年劣化した内外装の交換などを正規品質でご提供します。

https://factory.kinto-jp.com/

KINTO Technologies

KINTO テクノロジーズ (通称: KTC) の手がけるプロダクト

クルマのサブスク「KINTO」をはじめとして様々なモビリティサービスを展開

KINTO ONE 中古車

KINTO ONE クルマの持ち方がまた広がる。

KINTO ONEのリースアップ車を中心とした状態の良い修復なし車両を厳選したトヨタの中古車サブスクサービスです。マイカーにかかるさまざまな費用が、毎月コミコミの定額のサービスでご利用いただけます。

https://up.kinto-jp.com/

Prism Japan

「ここに行きたかったんだ」を、見つけよう。

Prism Japanは、あなた自身も気づいていないお出かけの好みやいまの気分を、独自のAIが分析。あなたにぴったりの場所を見つけ出す 、お出かけ先インスピレーションAIアプリです。

KINTO Technologies

KTC による開発・支援実績

クルマのサブスク「KINTO」をはじめとして様々なモビリティサービスを展開

モビリティマーケット

クルマライフの楽しさを広げるサービス「モビリティマーケット」。ドライブしたいと思い立ったときにぴったりなお出かけ先はもちろん、愛車のお手入れに役立つサービスなど、多彩なプログラムをWEBサイトでご紹介しています。

my route

移動手段の検索・予約・決済まで、移動に関する一連の機能をひとつのアプリ内で完結でき、街中における円滑な移動のサポートをするマルチモーダルモビリティサービスです。

グローバルIDプラットフォーム

2019年に誕生したKINTOブランドのサービスは全世界で展開されています。KINTOテクノロジーズ株式会社は、別々のID管理システムをつなげ、全世界のKINTOのお客様をグローバルで一意に管理するためのプラットフォーム、Global KINTO ID Platformを開発し、2021年にリリースしました。

TOYOTA wallet

トヨタのキャッシュレス決済アプリ「TOYOTA Wallet」のアプリケーション開発およびテスト自動化環境構築の支援を行っています。

WOVEN CITY

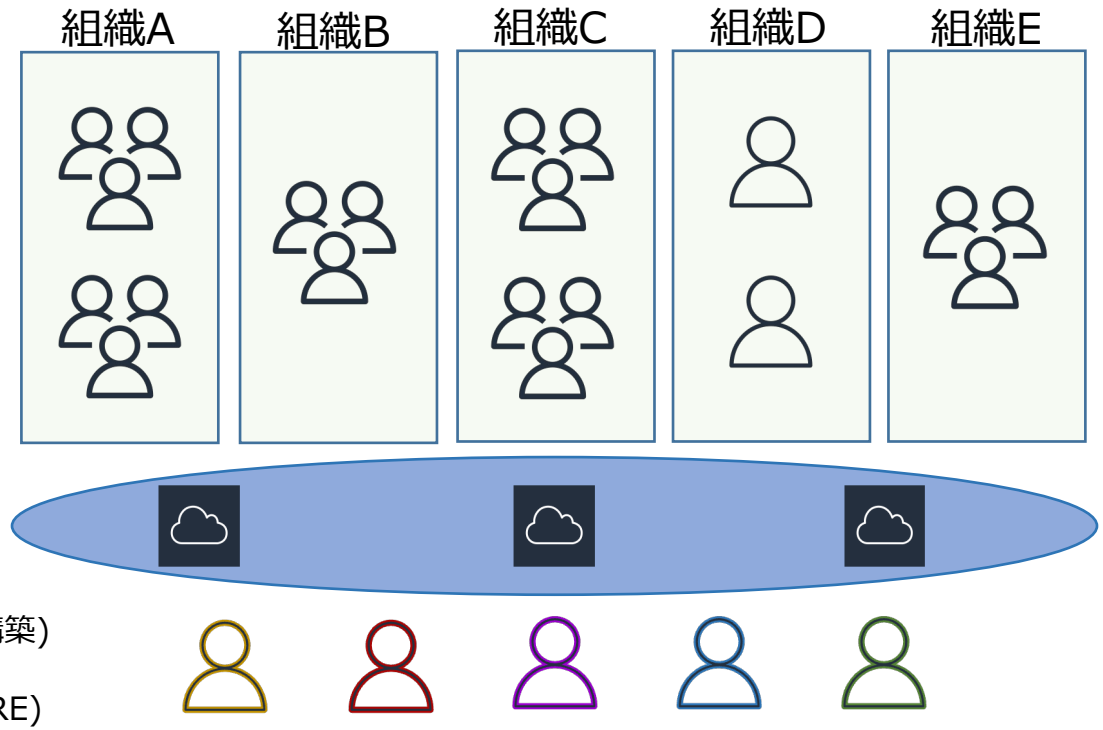
Woven Cityは、未来の当たり前を発明するモビリティのテストコースです。価値の交換、移動にかかわる決済プラットフォームを作り、発明家と住民の皆さんに提供し、この街で行われる新たな価値の発明をサポートします。※Woven Cityは2024年～2025年に一部実証を開始予定

KTC における DBRE の立ち位置

エンジニア組織: 16 グループ

社内のエンジニアの数: 約 300名

アプリケーション開発組織
- サービス開発
- モバイルアプリ開発
- 共通プラットフォーム開発, etc.



…

横断組織
- SysAd (クラウドインフラ構築)
- DevOps (DevOps 推進)
- SRE (Embedded SRE)
- ***DBRE*** (DBRE 推進)
- MSP (24*365 保守運用対応)
- CCoE (クラウド利活用推進)

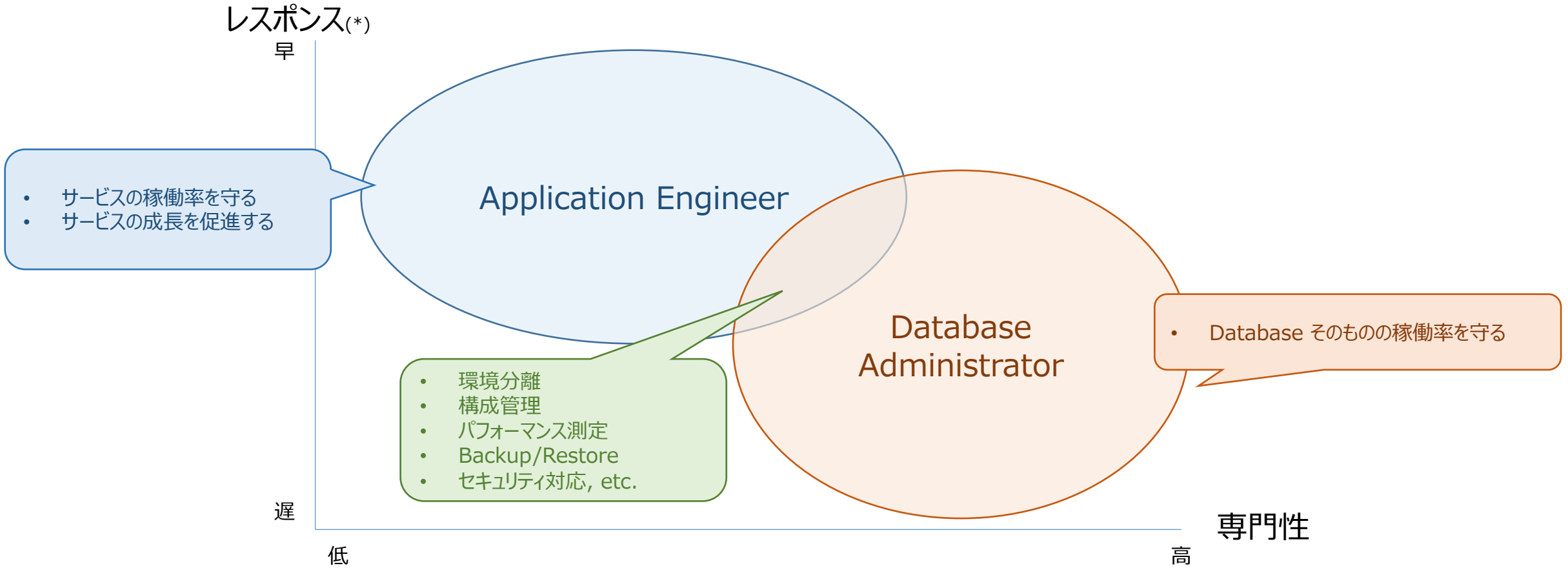
フルクラウドでサービス運営
- クラウドはデフォルトの選択肢
- アーキテクチャ、運用、プロセス、組織の形はクラウド活用を前提に改善され続けている

01

なぜ KTC に DBRE が必要だったのか

Application Engineer と Database Administrator の関係性

それぞれの役割が明確に分かれていて専門領域を DBA が監視

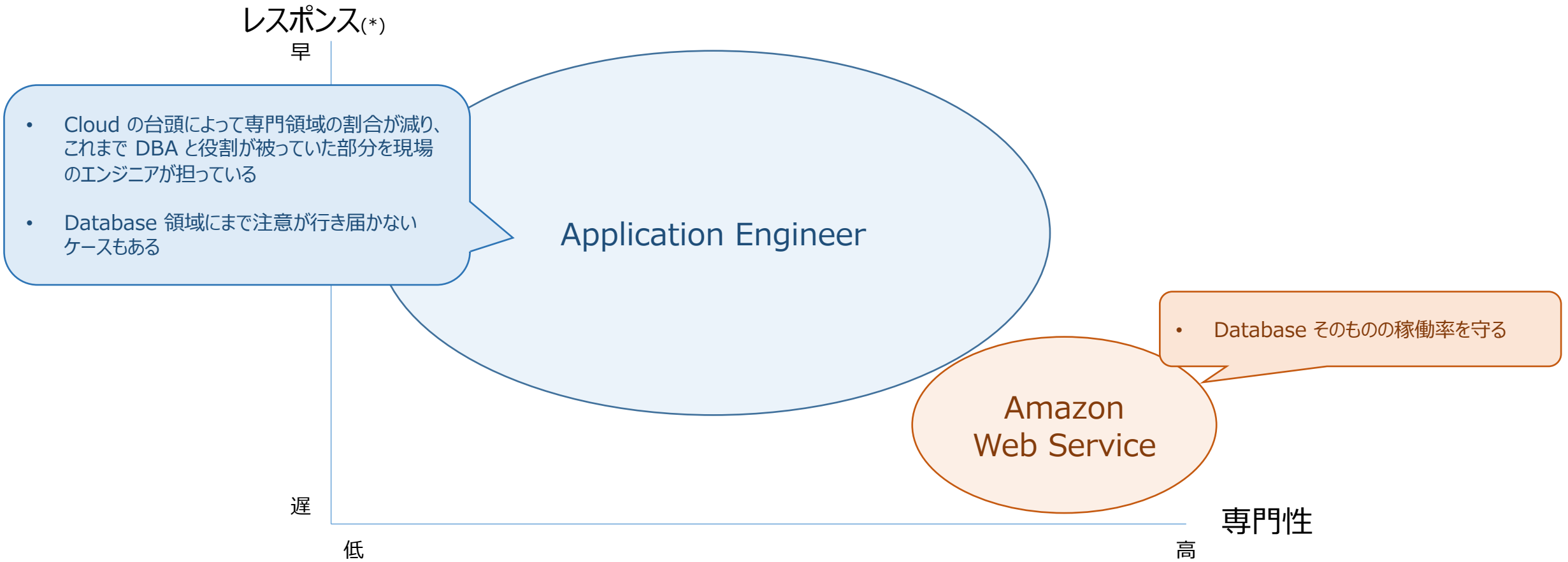


(*) ここでのレスポンスとはサービスに対する適用速度、トラブルが発生した時の応答速度、必要なデータを抽出するなど通常オペレーションで必要な作業時間などが含まれる

KINTO Technologies

Cloud によって変わった Database 運用の役割

DBA の役割が薄れ、DBA がいない組織も増加傾向

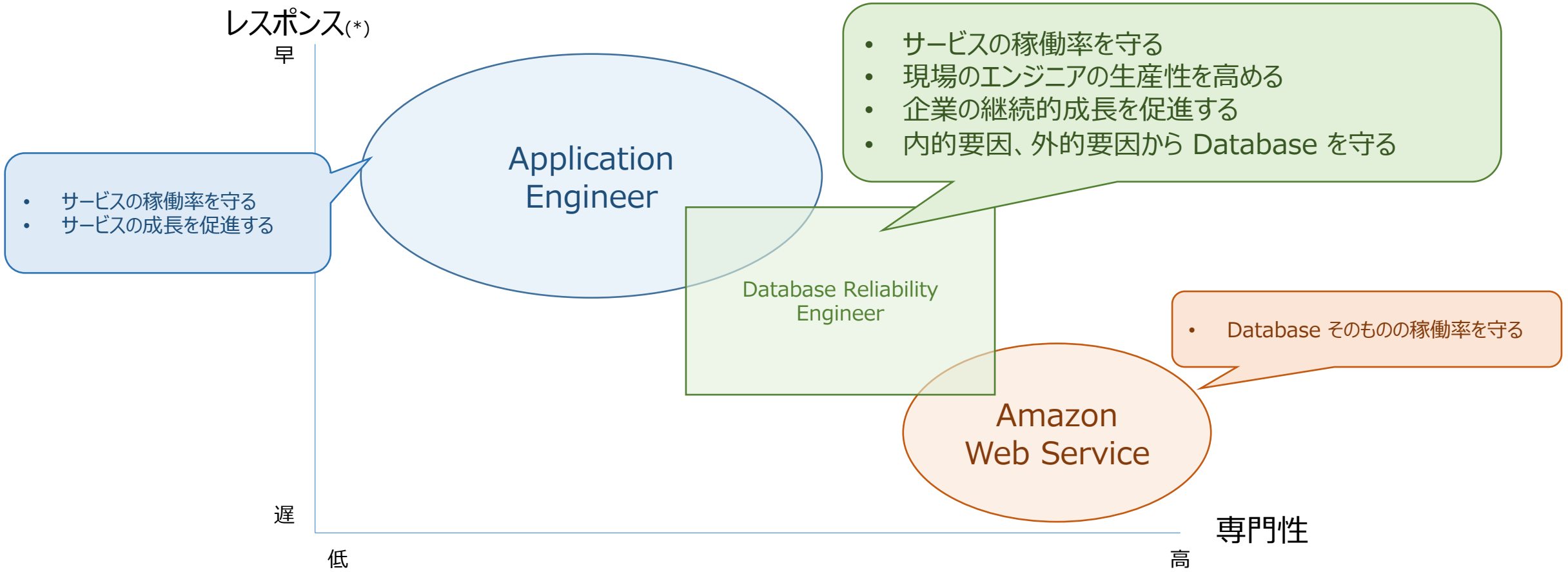


(*) ここでのレスポンスとはサービスに対する適用速度、トラブルが発生した時の応答速度、必要なデータを抽出するなど通常オペレーションで必要な作業時間などが含まれる

KINTO Technologies

Cloud 時代の DBRE の役割

現場のエンジニアが事業成長に注力できる環境を提供すること



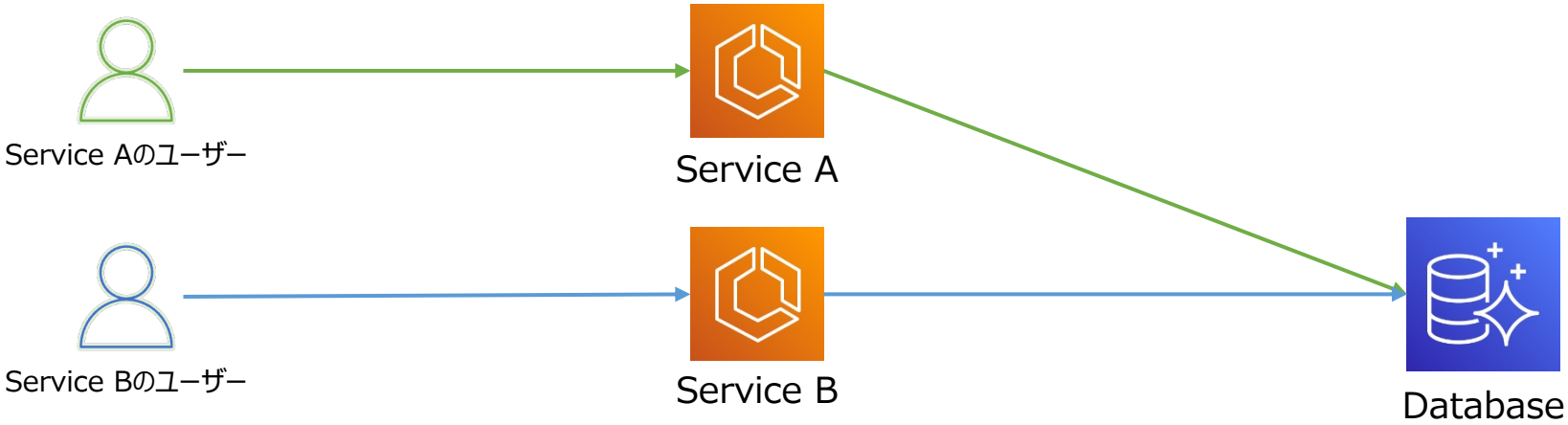
(*) ここでのレスポンスとはサービスに対する適用速度、トラブルが発生した時の応答速度、必要なデータを抽出するなど通常オペレーションで必要な作業時間などが含まれる

KINTO Technologies

サービスの稼働率を守る

サービスが正常な状態は Database が正常に機能していることが前提になる

- Database のダウンタイムはそのままサービスのダウンタイムにつながる
  - サービスの復旧時間 > Database の復旧にかかる時間
    - 正しく適切に素早く復旧させるためには Database スキルが必要不可欠
- Database が正常に機能しないとそのサービスがダウンする
  - 複数のサービスで一つの Database を参照している場合、ドミノ倒しのようにサービスが倒れていくリスクがある



現場のエンジニアの生産性を高める

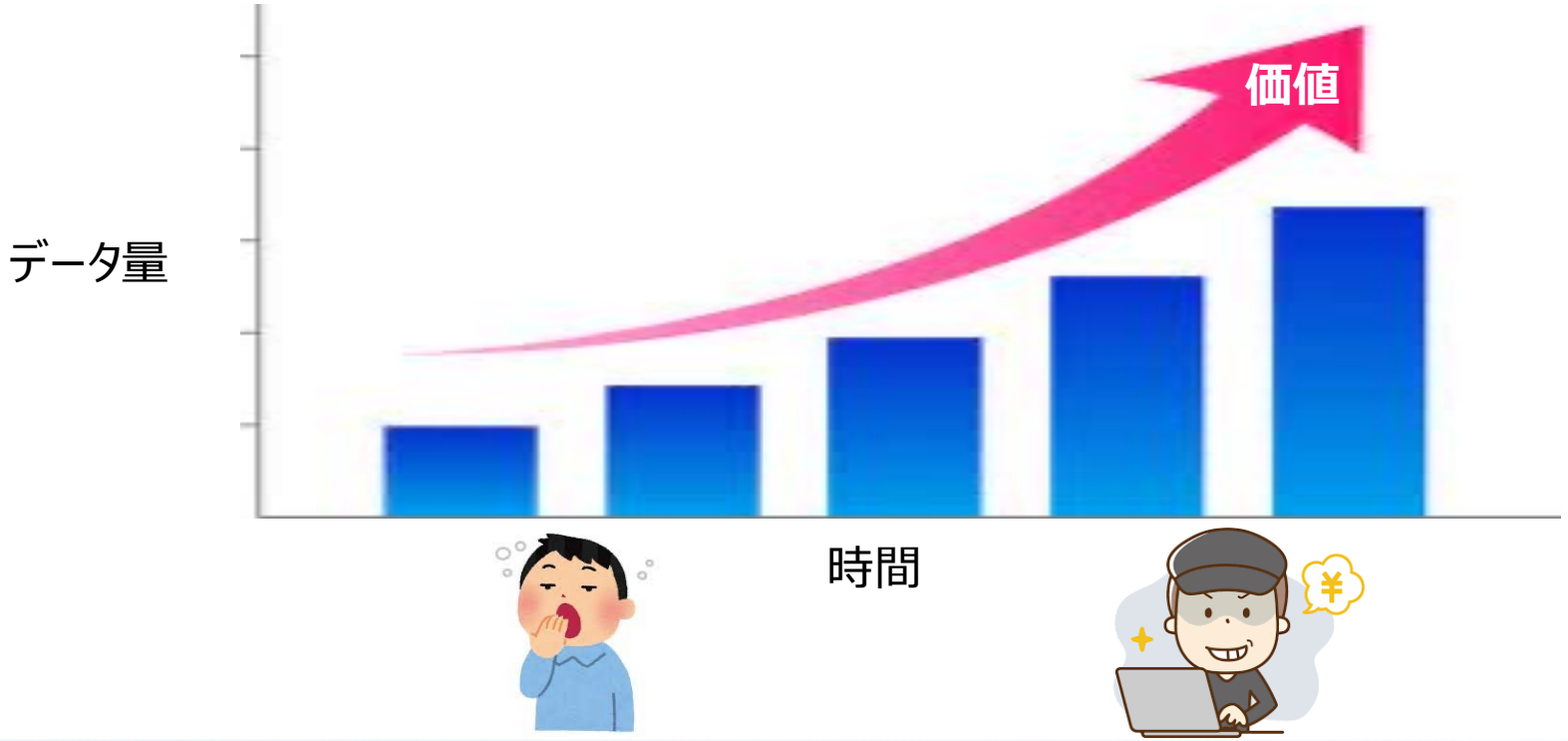
Database に関するオペレーションはちょっとした手間で補完できることが多い

- 「ちょっとした手間」もエンジニア全体の工数で見ると大きくなる
  - ちょっとした手間を簡略化、標準化することは全体の生産性に貢献できる
    - 企業のガイドラインに適用した Platform の提供
    - Database Document の自動生成, etc.
  - 必ず行うべき設定や各サービスのお困りごとを解決する
    - Cloud 技術の新機能検証と適用
    - SlowQuery の対応サポート
    - トラブル対応サポート, etc.

企業の継続的成長を促進する

Database の重要性は事業の成長と共に高まっていく

- Database そのものの価値は時間に比例して高まる
  - 価値が高まった Database は常に狙われる
  - データ流出が発生した場合、実害だけでなくそれに伴う甚大なレピュテーションリスクを抱えることになる



内的要因、外的要因から Database を守る

Database 運用に求められることは年々厳しくなっている

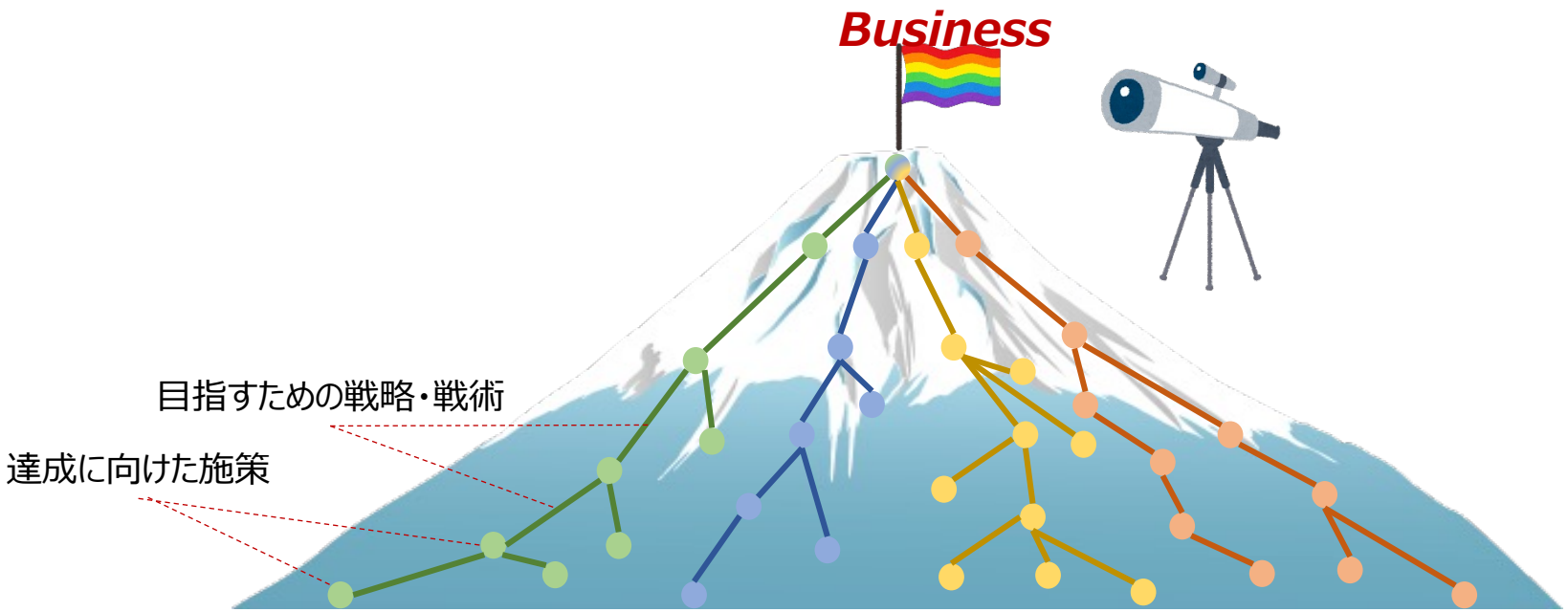
- データはその重要性から外部要因の変化による影響も受けやすい
  - 政治、法律、世論 などの変化
    - 個人情報保護法は定期的に改定されており改定の度に罰則が厳しくなる傾向にある
    - GDPR などグローバル標準への追従

KINTO Technologies

KTC DBRE の目指すべき姿

KTC における DBRE は横断組織

- 自分たちのアウトプットがビジネスに反映されることによって価値提供される
  - 横断組織はそこにあるだけでは何に使われるか分からない税金と同じ
  - ビジネスに対して良い影響を与えることが重要



KTC DBRE の目指すべき姿

ルールや Review だけで対応できないほど事業の変化のスピードは早くなっている

- Database の知識を現場のエンジニアに還元して KTC 全体の **Reliability** を守る
  - Database におけるモノゴトを Engineering で解決
    - ルールでがんじがらめにするのではなく、アプリケーションエンジニアと**協働**して解決する
    - 高いアジリティを保持しつつ、サービスのガバナンスコントロールを実現する

02

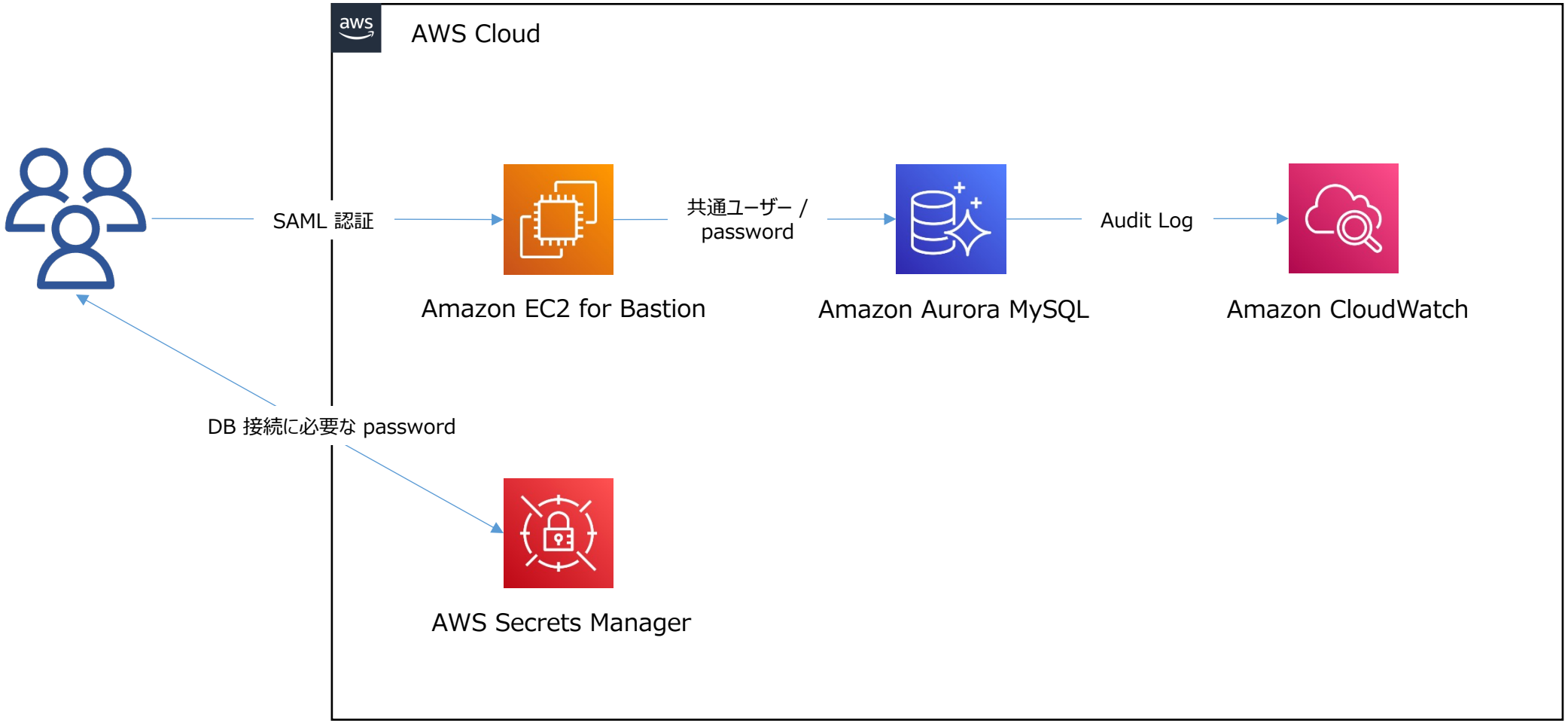
KTC の Database 運用上の課題

Q: Databaseに接続するための踏み台サーバを使用していますか？

KINTO Technologies

KTC では踏み台サーバを利用している

Database に関連するオペレーションのために専用の Amazon EC2 インスタンスを構築



KINTO Technologies

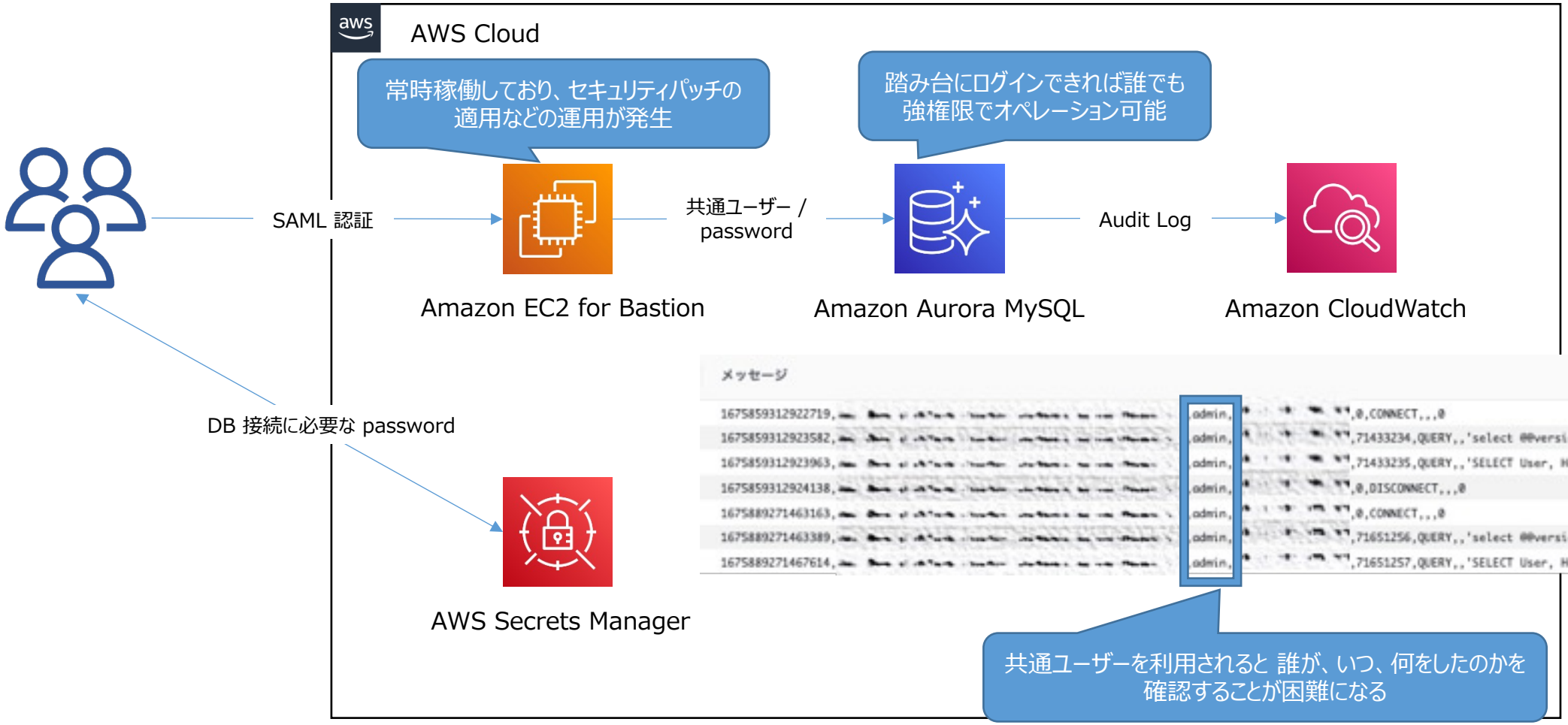
KTC の運用ガイドライン (一部抜粋)

Database 運用に必要とされる要件

カテゴリ	概要
ログ	• 行われたオペレーションが全て記載されていること • オペレーションを行なった個人を特定することが容易であること • ログの改竄ができないこと
ユーザー/パスワード管理	• オペレーションに応じた権限が都度付与されること • 共通ユーザーを使用しないこと • パスワードには十分な長さと複雑さがあること • 定期的にパスワードが更新されること
アクセス管理	• いつ、誰が該当作業を承認したのかがわかること • 作業完了後そのアクセスはできなくなること
脆弱性対応	• 脆弱性への対応が速やかに展開されること

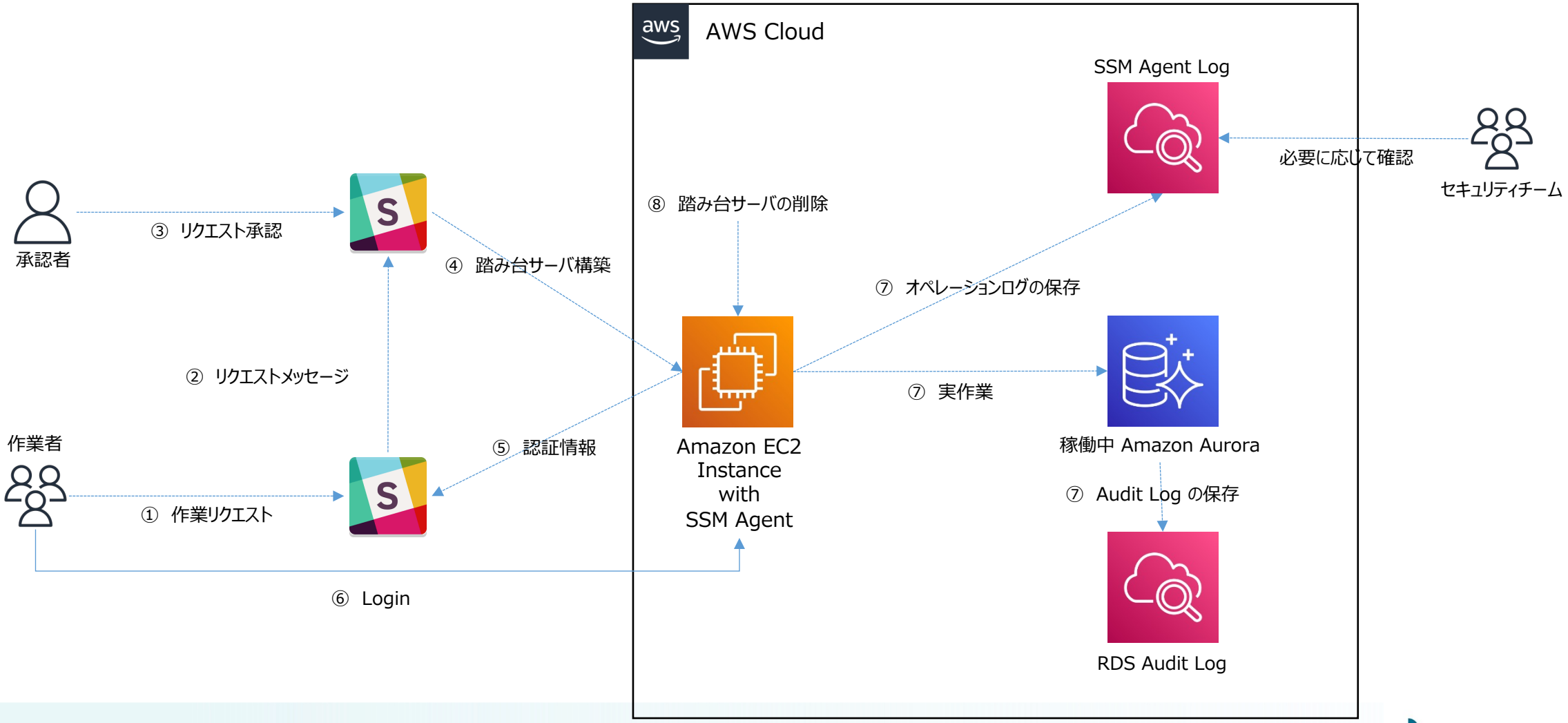
踏み台サーバを運用していく上での課題

KTC ガイドラインに則るためには課題が多い



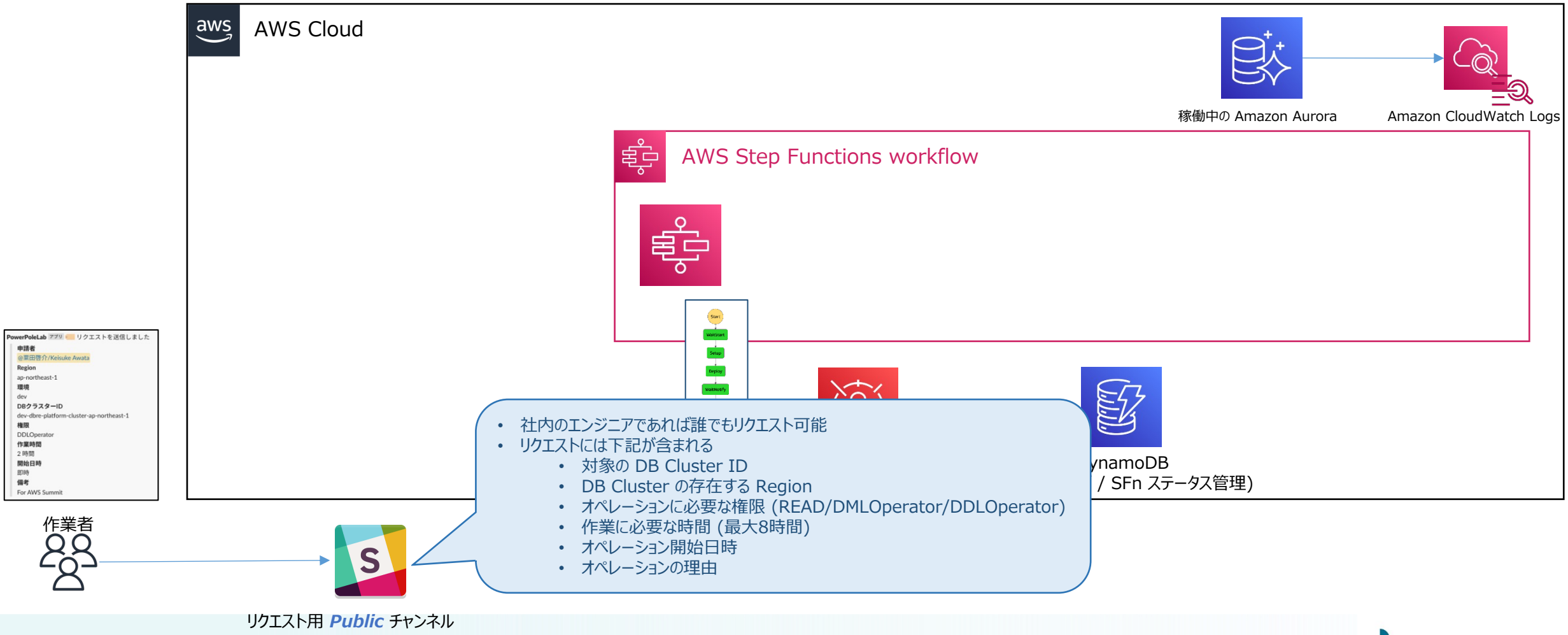
課題解決のための DBRE のアクション

ガイドラインに準拠したインスタントな踏み台サーバを構築する Platform を開発

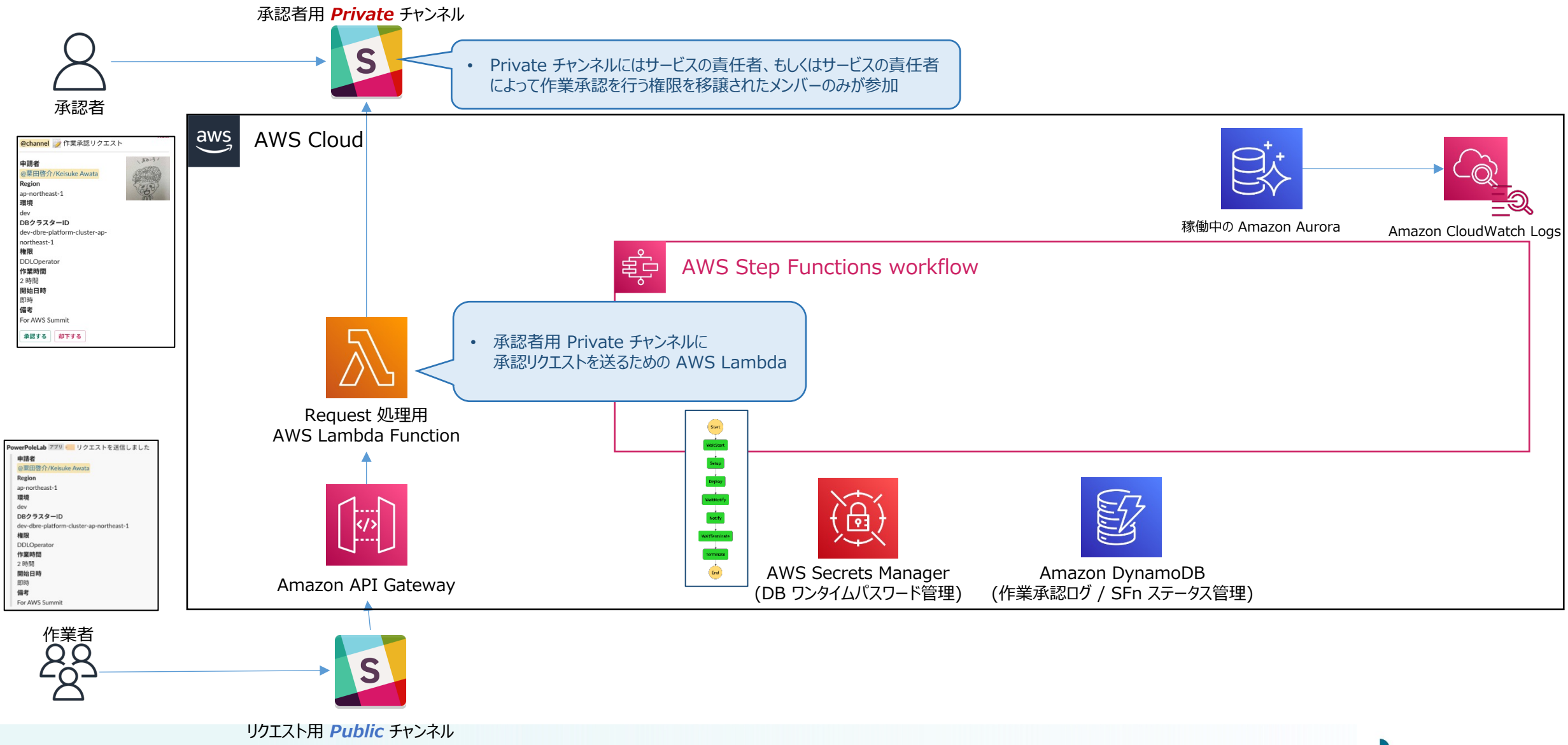


KINTO Technologies

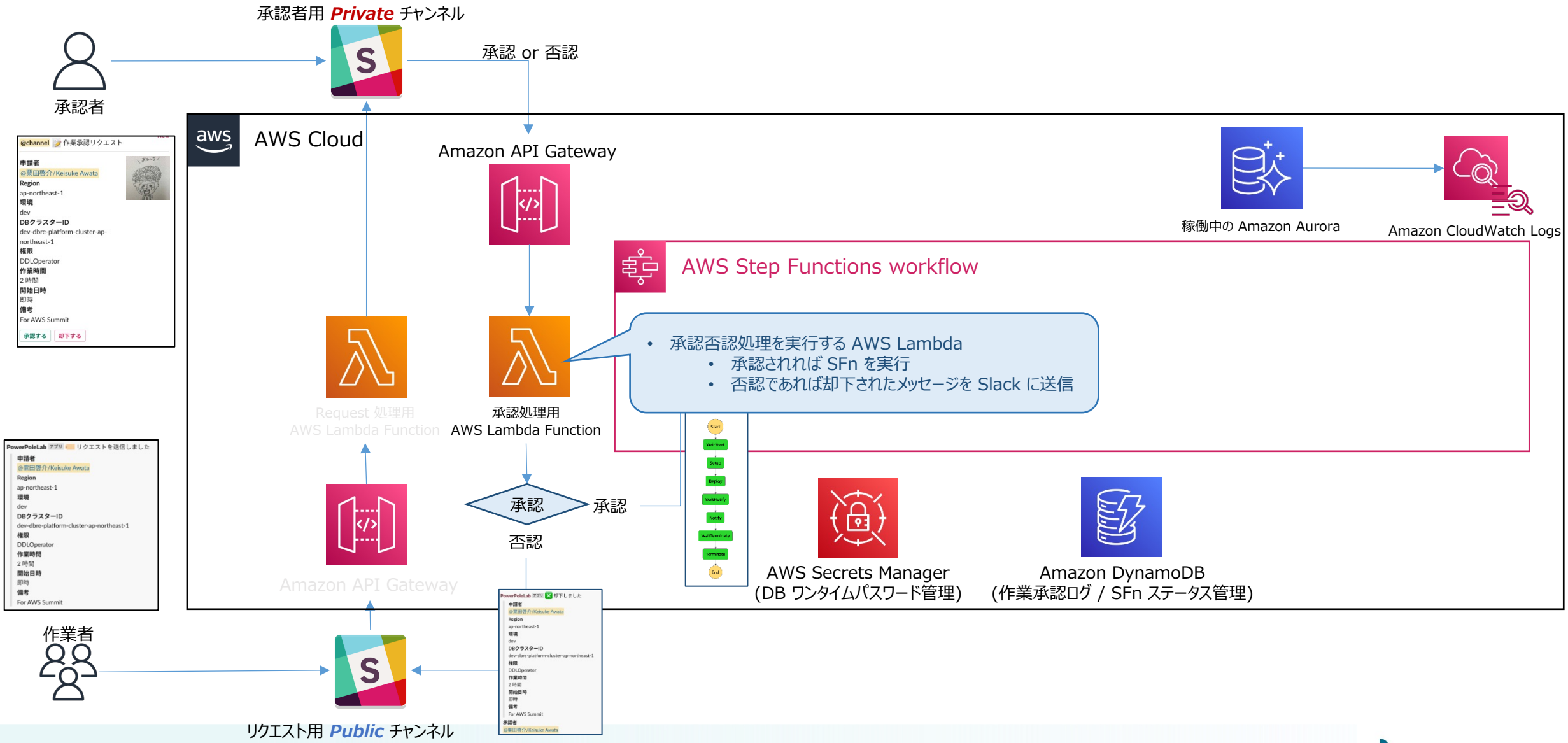
詳説: Architecture



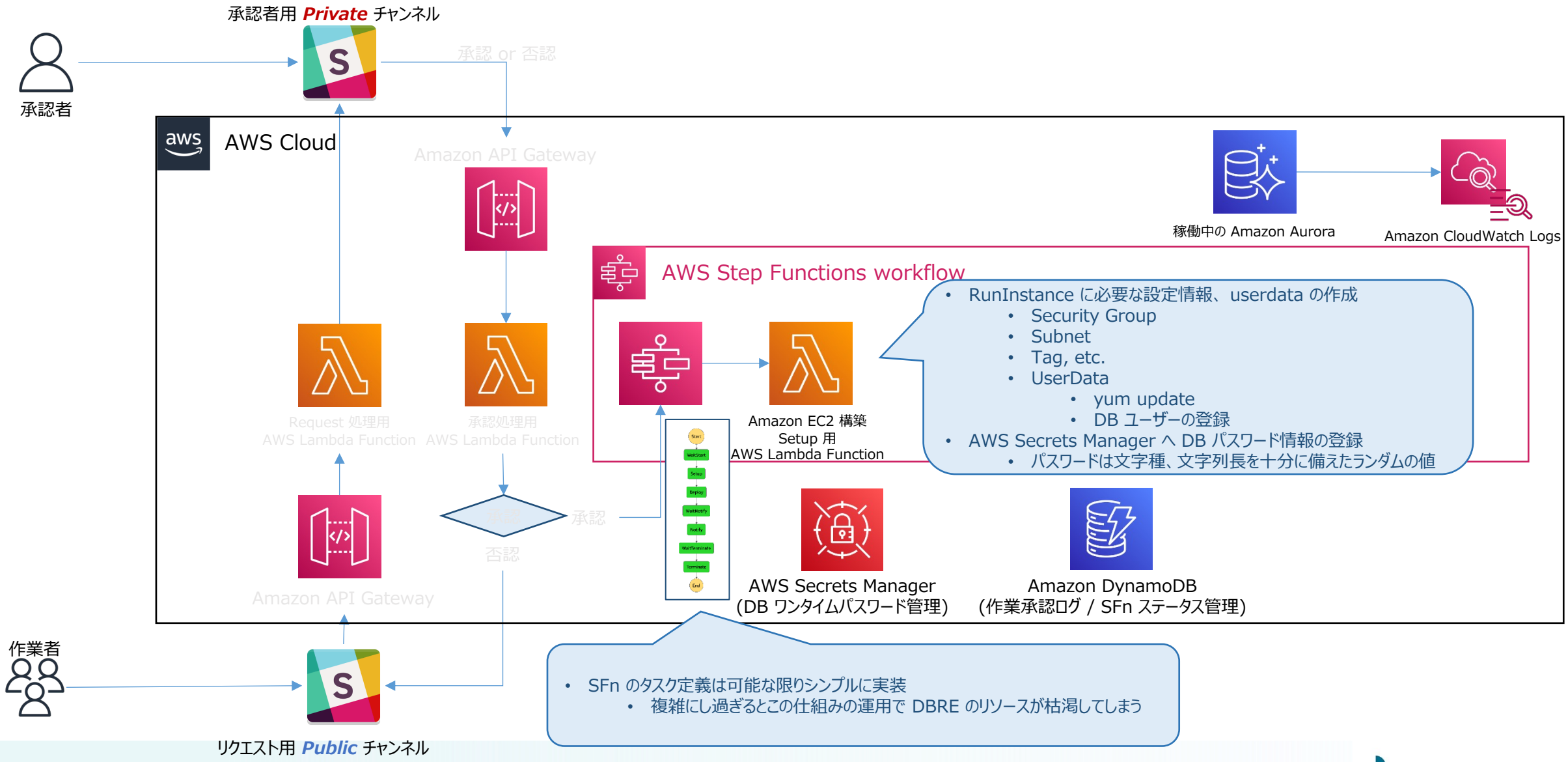
詳説: Architecture



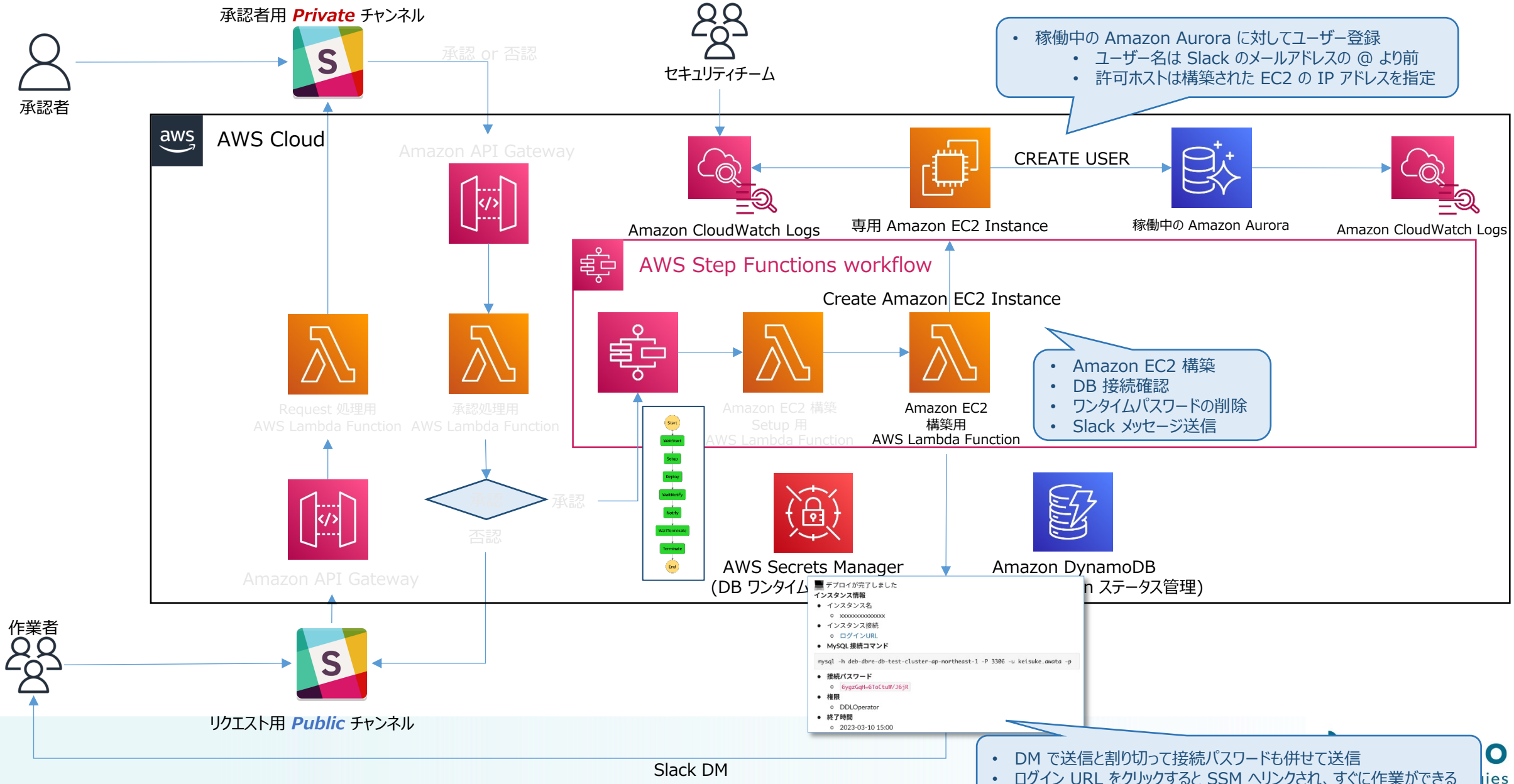
詳説: Architecture



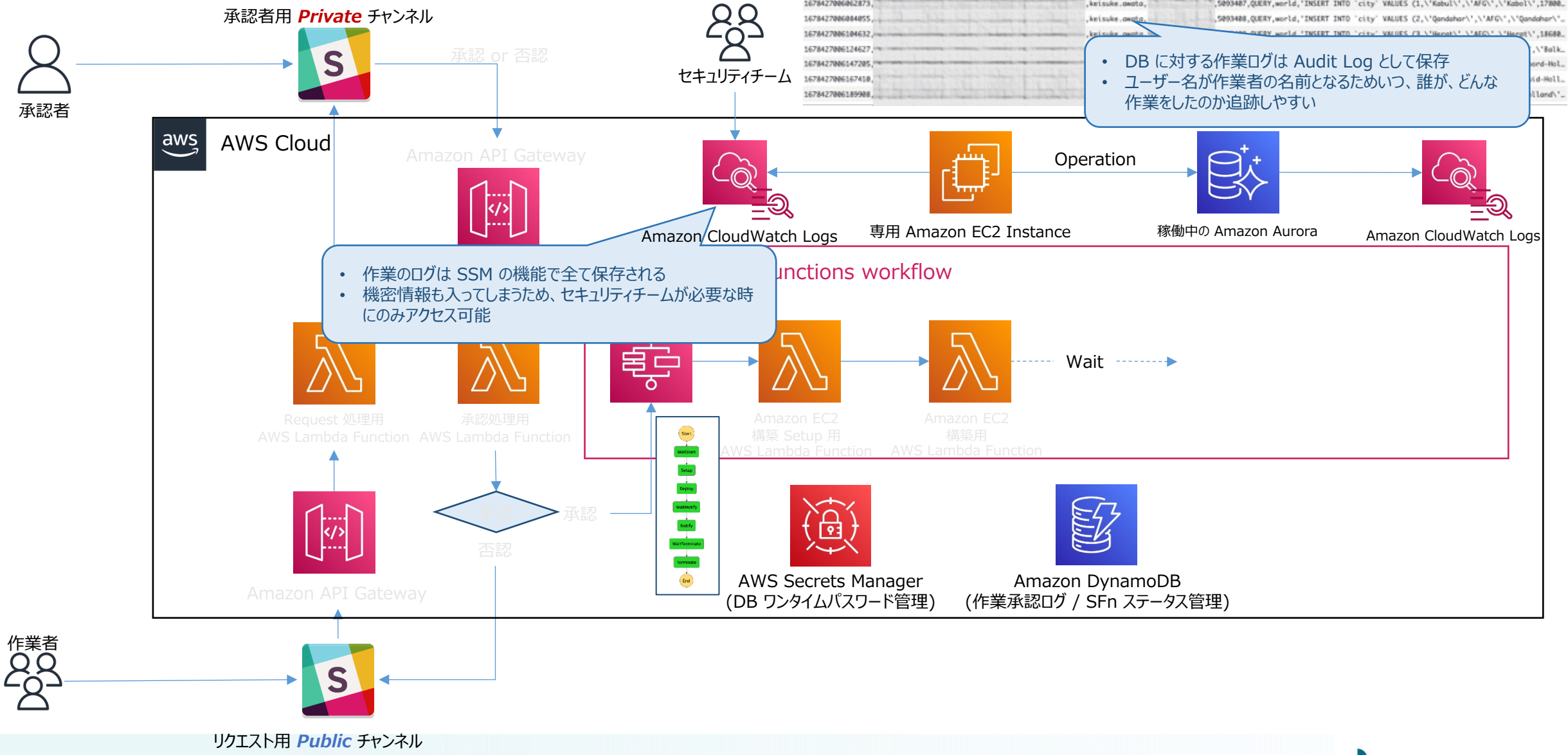
詳説: Architecture



詳説: Architecture



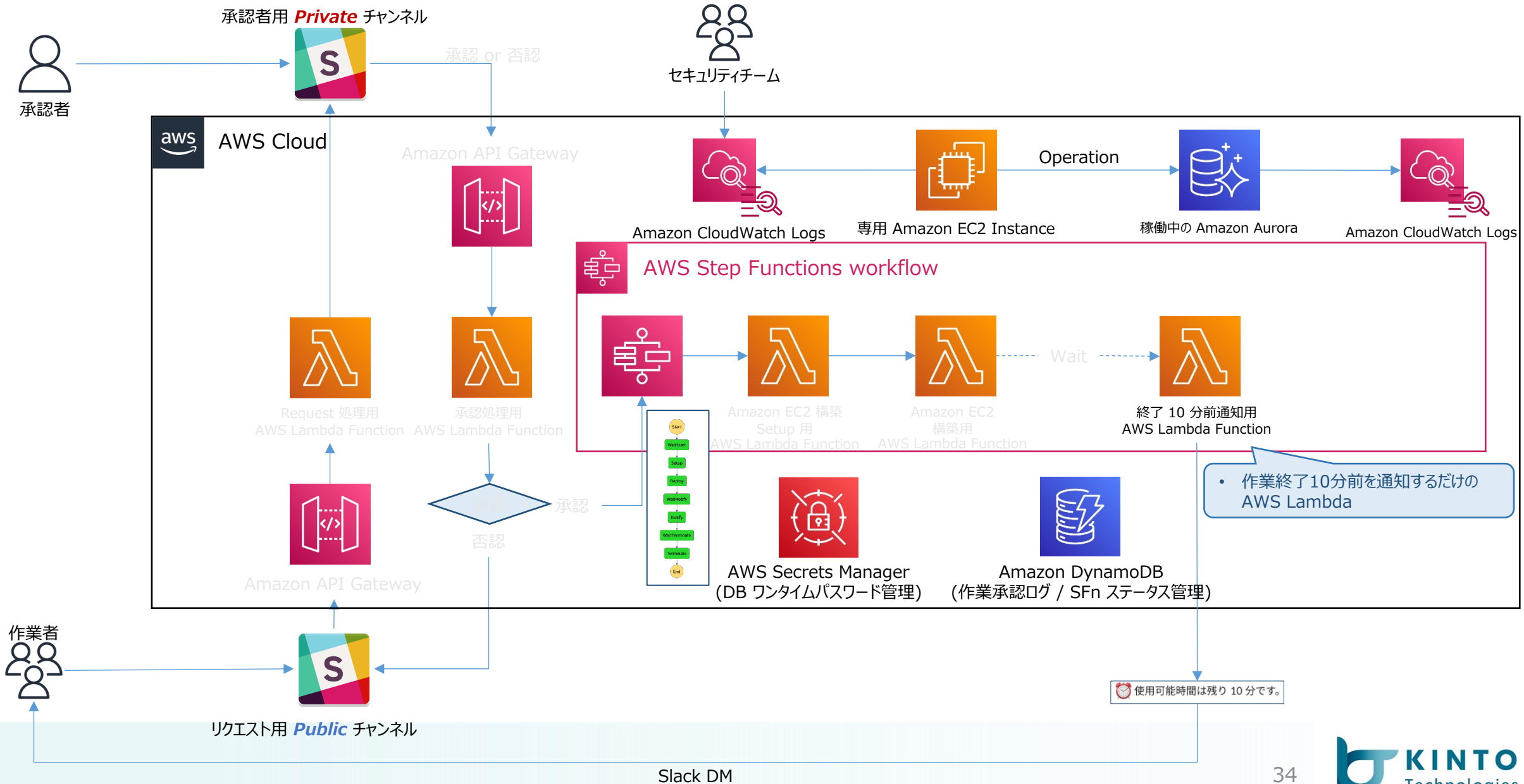
詳説: Architecture



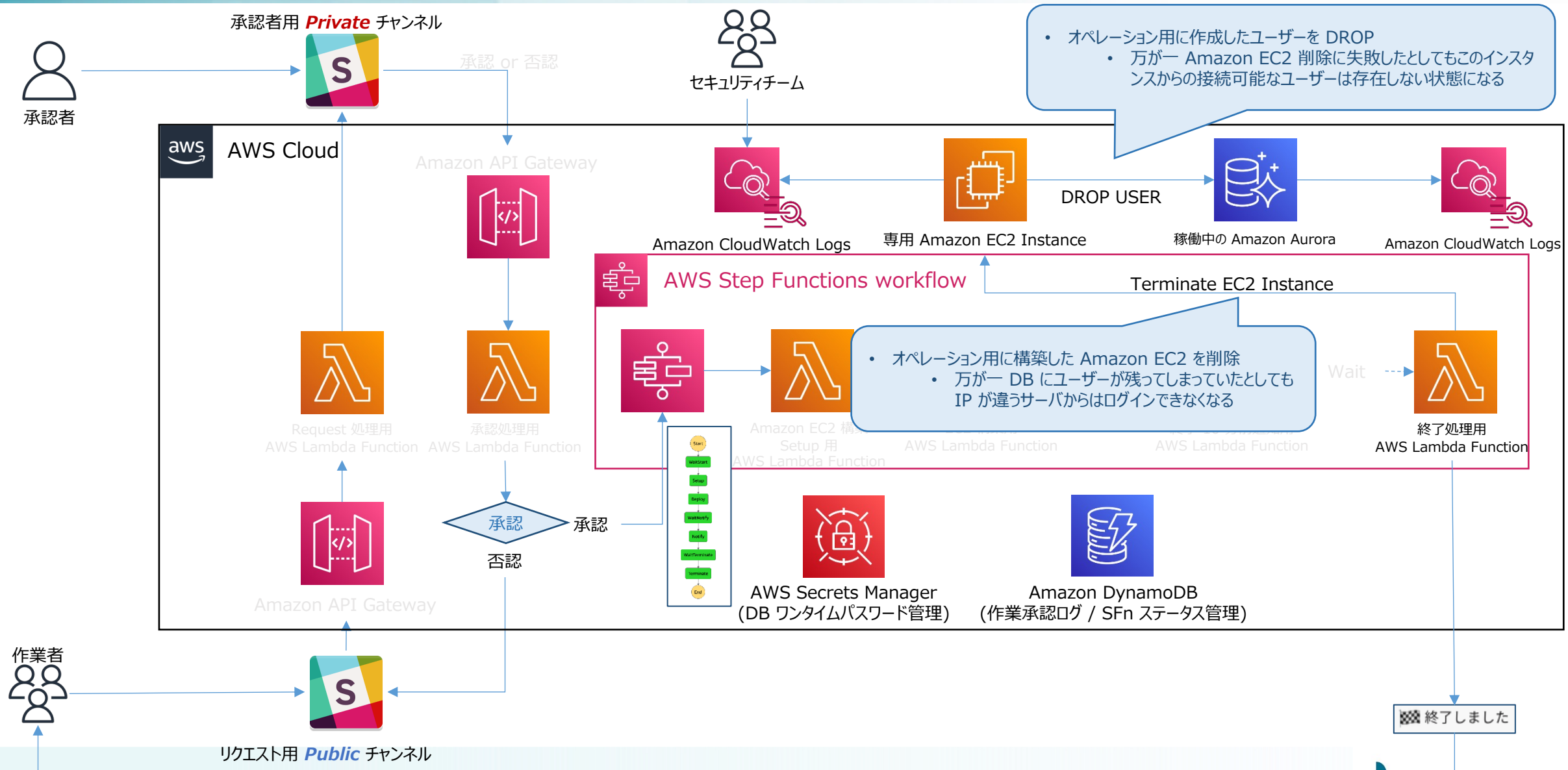
Slack DM

KINTO Technologies

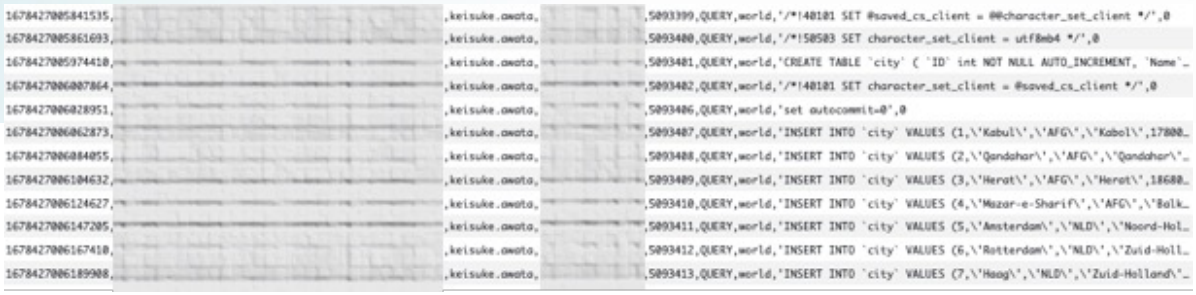
詳説: Architecture



詳説: Architecture



全体像: Architecture



承認者用 ***Private*** チャンネル

承認者

承認 or 否認

セキュリティチーム

AWS Cloud

Amazon API Gateway

Amazon CloudWatch Logs

専用 Amazon EC2 Instance

CREATE USER

DROP USER

稼働中の Amazon Aurora

Amazon CloudWatch Logs

AWS Step Functions workflow

Terminate EC2 Instance

Create EC2 Instance

Wait

Wait

Request 処理用
AWS Lambda Function

承認処理用
AWS Lambda Function

Amazon EC2 構築
Setup 用
AWS Lambda Function

Amazon EC2
構築用
AWS Lambda Function

終了 10 分前通知用
AWS Lambda Function

終了処理用
AWS Lambda Function

承認

承認

否認

Amazon API Gateway

AWS Secrets Manager
(DB ワンタイム

Amazon DynamoDB
ステータス管理)

作業者

リクエスト用 ***Public*** チャンネル

使用可能時間は残り 10 分です。

終了しました

Slack DM

KINTO Technologies

DBRE Platform によるガイドライン準拠

Database 運用に必要とされる要件を Engineering で解決

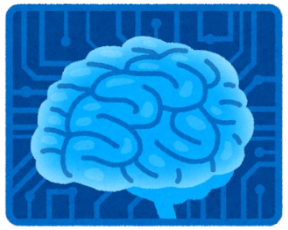
カテゴリ	Before	After
ログ	• 行われたオペレーションが全て記載されていること • オペレーションを行なった個人を特定することが容易であること • ログの改竄ができないこと	• Audit Log / SSM Log の適切な利用 • Database のユーザー名をSlack のメールアドレスの @ より前を使用することで個人の特定が容易
ユーザー/パスワード管理	• オペレーションに応じた権限が都度付与されること • 共通ユーザーを使用しないこと • パスワードには十分な長さと複雑さがあること • 定期的にパスワードが更新されること	• オペレーションリクエスト時に必要な権限を申請 • 都度 Database にユーザー登録を行う • パスワードは要件を満たすためのプログラムで毎回ランダムで作成
アクセス管理	• いつ、誰が該当作業を承認したのかがわかること • 作業完了後そのアクセスはできなくなること	• 全てのプロセスを DynamoDB に登録 • 作業完了後 Database からユーザーを削除
脆弱性対応	• 脆弱性への対応が速やかに展開されること	• 踏み台を起動するタイミングで yum update を実施

DBRE Platform Tools

組織横断的に利用できる Tool の開発

スローガン

- How の部分をモダンで楽しく開発
  - 実現していることは枯れたことかもしれない
    - 本日紹介させていただいたツールは一言で言うと踏み台サーバを使いたい時に構築しているだけ
    - そこに DBRE としてのナレッジとアマゾン ウェブ サービス（AWS）の技術を組み込んで実現



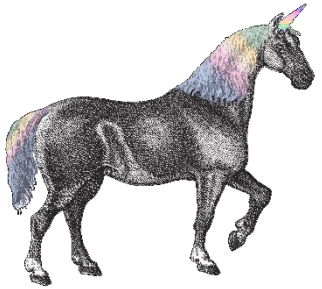
DB に関する経験・知見

x

AWS

AWS Cloud Engineering

=



KTC DBRE

KINTO Technologies

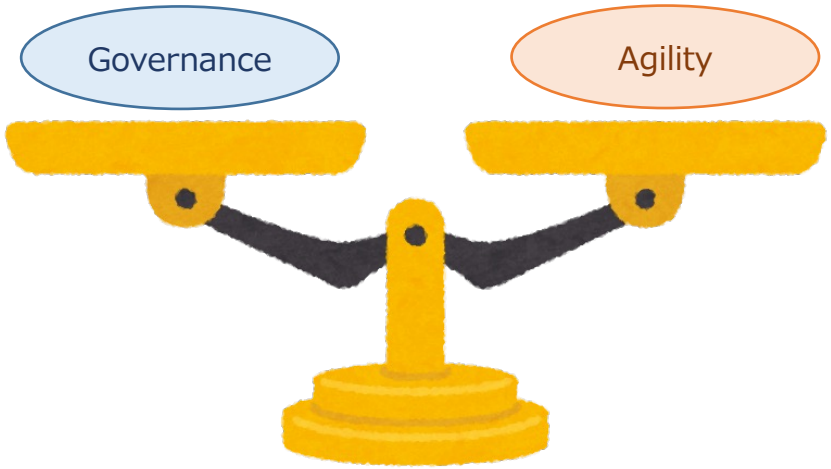
KTC DBRE を支える技術

- AWS
  -  Amazon API Gateway
  -  Amazon Aurora for MySQL
  -  Amazon CloudWatch
  -  Amazon DynamoDB
  -  Amazon EC2
  -  AWS Lambda
  -  AWS Secrets Manager
  -  AWS Step Functions
- 特にこだわったポイント
  - Slack App
    - 承認者には都度確認を強いるため負荷を減らす必要があった
- 平均構築時間
  - 40秒未満
- 開発手法
  - Scrum
- 開発言語
  - Golang
- Monorepo 管理
  - Nx
- CICD
  - GitHub Actions
- Infrastructure as Code
  - terraform

ガバナンス vs アジリティ ??

Cloud の強みを活かしてある程度ガバナンスとアジリティを両立させることができる

- ガバナンスを適用するためにはアジリティを犠牲にしてしまうこともある
  - Cloud を正しく活用することでそれぞれの効率を最大化する
  - どのレベルまで確保できるかが DBRE としての腕の見せ所



03

KTC DBRE 現在の取り組み

現在取り掛かり中のプロジェクト

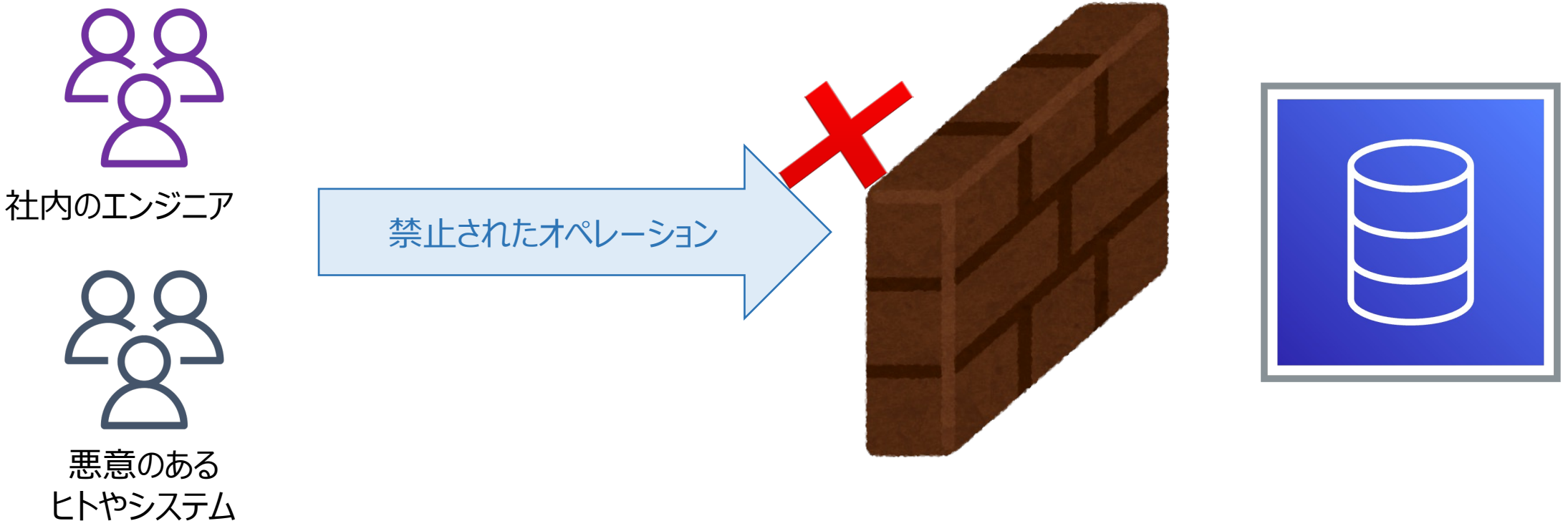
Database 版 発見的ガードレールの構築

- ガードレールとは
  - 可能な限り**自由を確保**しつつ、**望ましくない領域のみ制限、または発見**するソリューション
    - 「ゲート」によるブロッカーとなる制御から「ガードレール」として禁止操作を制限して危険な設定を検出することで**アジリティを維持してガバナンスコントロールを実現**する
  - クラウドガードレールの種類

ガードレール	役割	概要
予防的ガードレール	制限	• 対象の操作をできないようにする
発見的ガードレール	検知	• 望ましくない操作をおこなった、された場合、それを発見、検知する
訂正的ガードレール	修正	• 望ましくない設定がされた場合に自動で修正する

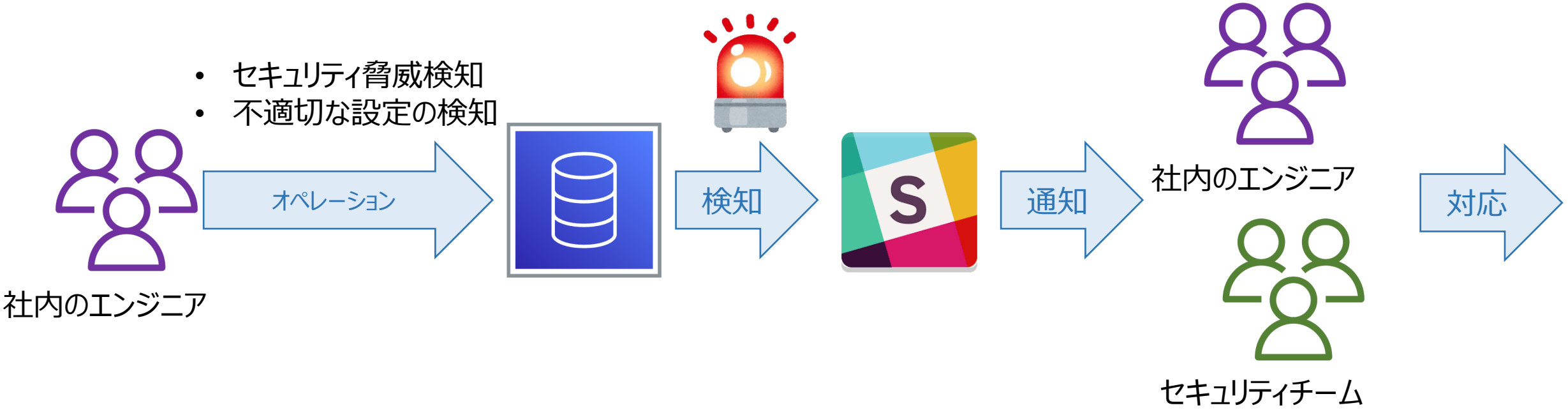
予防的ガードレール

制限をかけることでリスクの発生**前**に予防する



発見的ガードレール

制限をかけることでリスクの発生**後**に検知する

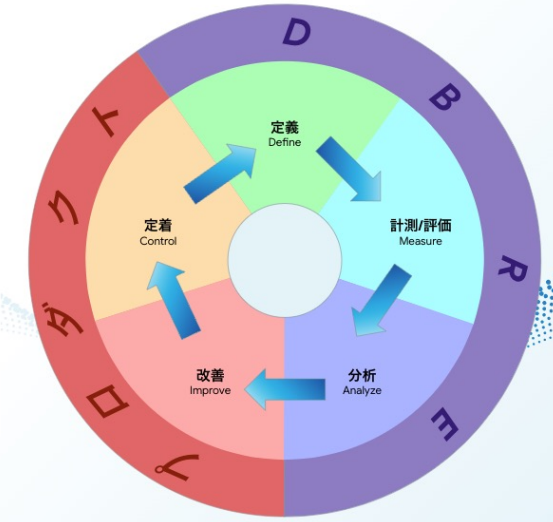


どのように実装するか

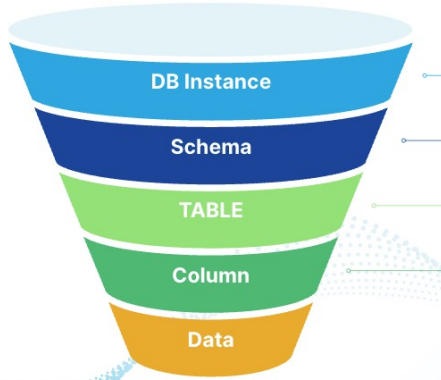
時間の都合により KTC Techblog をご確認ください

ガードレール構想と責任分界点イメージ

- Define: 計測/評価の範囲や内容を定義
  - 文書化
  - Script 化
- Measure: 計測/評価を実施して結果を収集
  - Script 実行
- Analyze: 原因の分析・レポーティング
  - 組織全体の可視性を高める
- Improve: 不具合の改善・改善計画の作成
  - 問題に対してスムーズな対応を実施
- Control: 成果を確認し、定着を目指す
  - サービスとして健全な状態が継続されている



自動化の軸



各クラウドの API や performance_schema 等を利用
(クラウドの設定、設定パラメータ、USER など)

Information_schema から情報を取得

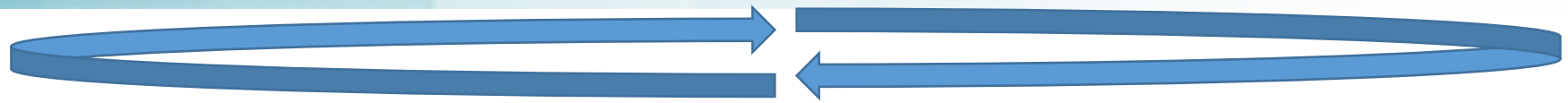
Information_schema から情報を取得

Information_schema から情報を取得

DBRE ガードレール

KINTO Technologies

その他: DBRE 4つの柱を軸に様々な活動を実施



Security & Governance	脅威についての定義がされている	脅威検知の仕組みがある	脅威に対する対応がスムーズに実施される	脅威に対する対応が横展開されている	脅威にさらされない設定が全社的になされている	**組織の DB レイヤのリスクを最小化し続けている**
Cost Optimization	コストの現状を把握できる	リソースの状態が把握できる	リソースの状態から適切な状態を定義できる	コストが最適化されている		**事業に対するコストを最適化し続けている**
Quality Improvement	企業として最低限守るべき SLO がある	SLO の継続的なモニタリングがされている	SLO/SLI によってアクションを決めることができる			**企業としての SLO を保証し続けている**
Delivery Efficiency	機能開発に向かっている時間が長い状態を作る	DB に関する技術情報が集約されている	DB に対する課題解決を伴走する			**組織の開発効率を最大化し続けている**

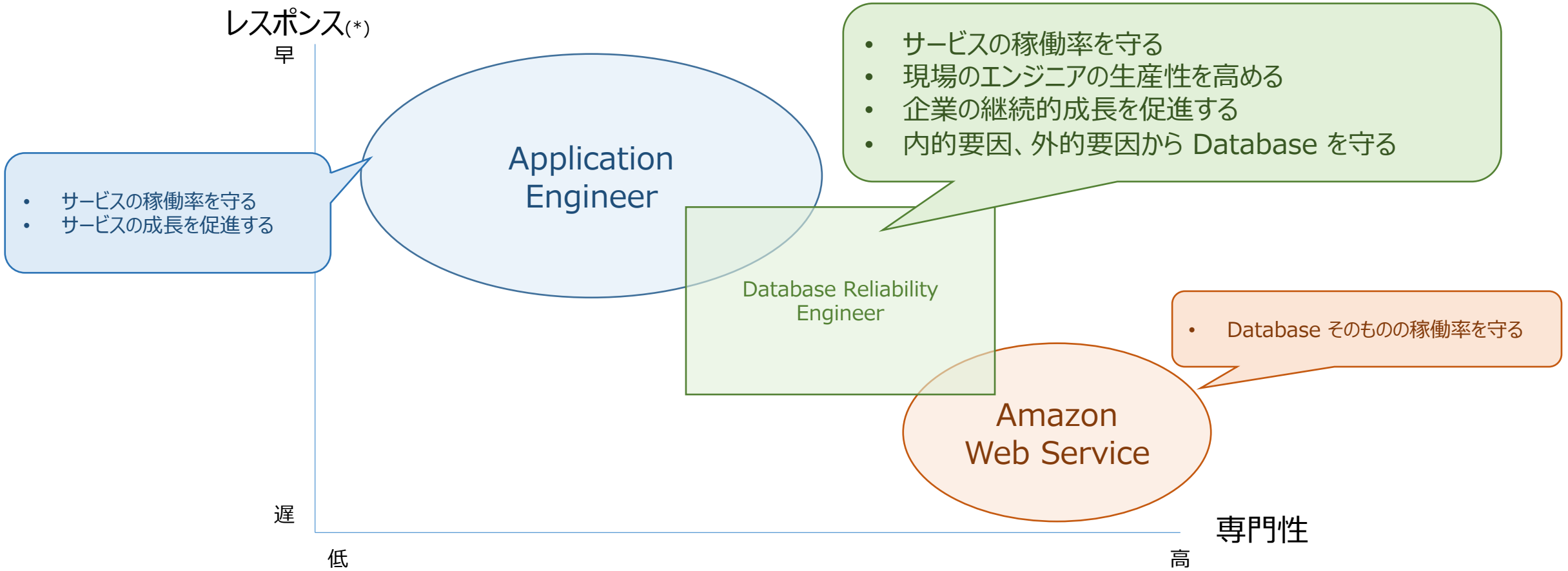
KINTO Technologies

04

まとめ

KTC における DBRE の役割

現場のエンジニアが事業成長に注力できる環境を提供すること



(*) ここでのレスポンスとはサービスに対する適用速度、トラブルが発生した時の応答速度、必要なデータを抽出するなど通常オペレーションで必要な作業時間などが含まれる

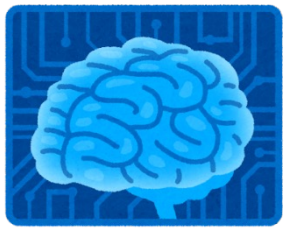
KINTO Technologies

KTC DBRE のアウトプット

Database の Reliability を向上させるためのプラットフォーム構築

- **Database** の知識を還元して KTC 全体の **Reliability** を守る
  - その手段として **Engineering** で解決する道を選択
    - Cloud を適切に活用して アジリティを確保しつつ Database のセキュリティとガバナンスを守る
    - Platform へと昇華させ企業全体に展開することでビジネスに良い影響を与え続ける

Database Reliability Engineering というアプローチ



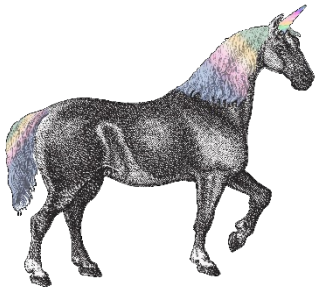
DB に関する経験・知見

x

AWS

AWS Cloud Engineering

=



KTC DBRE

KINTO Technologies

mysql > SELECT ‘**Thank you**’ FROM me;

KINTO Technologies


KINTO
Technologies

Thank you!