aws DEV DAY
ONLINE JAPAN

Session B-2

Cognito/Amplify で加速する エンタープライズのアプリケーション開発

安藤 裕紀

プラットフォームアーキテクト

NRIデジタル株式会社

In Partnership with intel

自己紹介

安藤 裕紀（あんどう ゆうき）

- NRIデジタル プラットフォームアーキテクト
  （2011年 野村総合研究所入社、2017年 NRIデジタル出向）
- Webシステムのサーバ構築・運用を中心としたインフラエンジニアとして流通・金融・製造など複数業種の技術支援を経験
- ここ最近は、AWS上に構築されたECサイトや会員サービスの開発運用を効率化すべくSRE / DevOpsエンジニア寄りの業務に従事
- 2020 APN AWS Top Engineers選出

In Partnership with intel

本日お話しすること（セッション概要より）

エンタープライズの新サービスを開発する際、企業はグループ内の複数のサービスを横断した顧客体験の向上とデータ活用によってビジネスの価値を高めようとします。そこで必要になるのが、エンドユーザの認証の統合とサービスごとの認可の制御です。

Cognito/Amplifyは新サービスを開発する際に認証機能を素早く実装する手段として知られていますが、IDaaSと連携した認証とサービスに必要な認可の機能を実装するために利用することで、エンタープライズが求める認証・認可を素早く実現するノウハウをお伝えします。

アジェンダ

- NRIデジタルについて
- エンタープライズに認証・認可が求められる背景
- アプリケーション開発を加速するためのAWSマネージドサービス活用
- まとめ

aws DEV DAY
ONLINE JAPAN

NRIデジタルについて

In Partnership with intel

NRIdigital

野村総合研究所（NRI）グループの
デジタルビジネス専門の戦略子会社

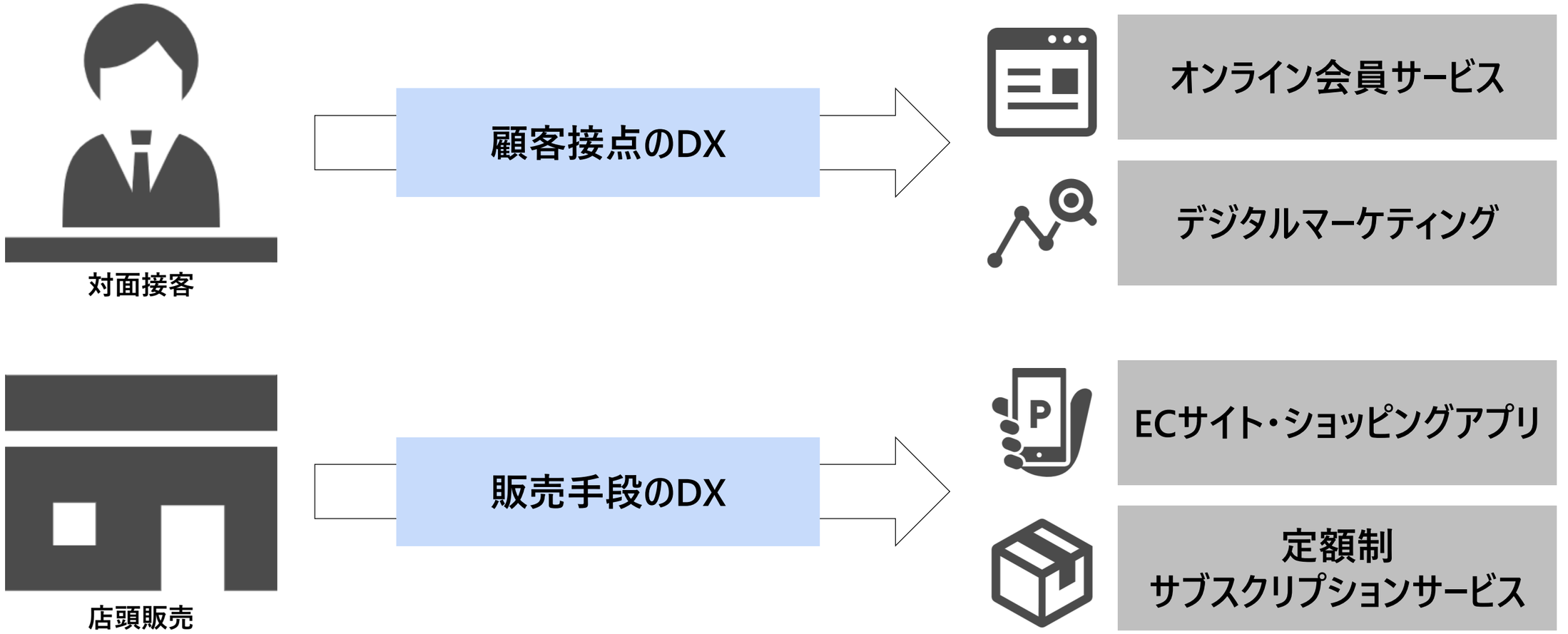
NRIグループ内外から組織の壁を超えて
集結した多様なプロフェッショナルが
"ワンチーム"で、お客様と共に
デジタルによるビジネス変革を推進

多様なプロフェッショナルが集結

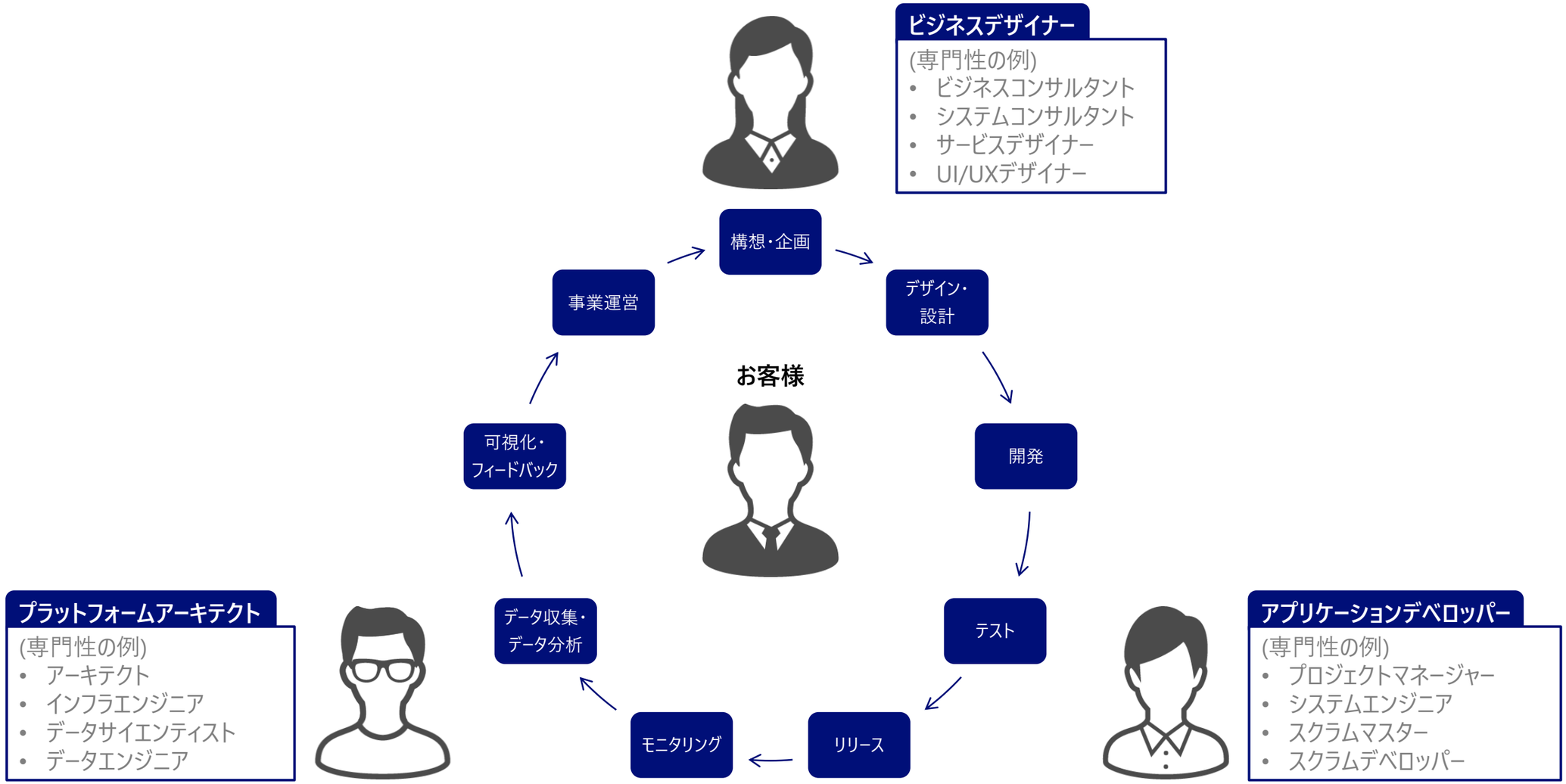
新たなテクノロジー領域への挑戦

価値共創型のビジネス創出

多くの企業が、ビジネス環境の激しい変化に対応するため、テクノロジーを活用したビジネスの変革（DX）に取り組んでいる



NRIデジタルはお客様のビジネス変革の全てのフェーズに関わり、多様な専門性を持つプロフェッショナルが協力してDXを推進している



aws DEV DAY
ONLINE JAPAN

エンタープライズに認証・認可が求められる背景

In Partnership with intel

エンタープライズ（大企業）

XYZ ホールディングス（持株会社）

X事業会社

Y事業会社

Z 事業会社

In Partnership with

ビジネスを変革するための経営トップの意思決定

DXやるぞ！

XYZ ホールディングス（持株会社）

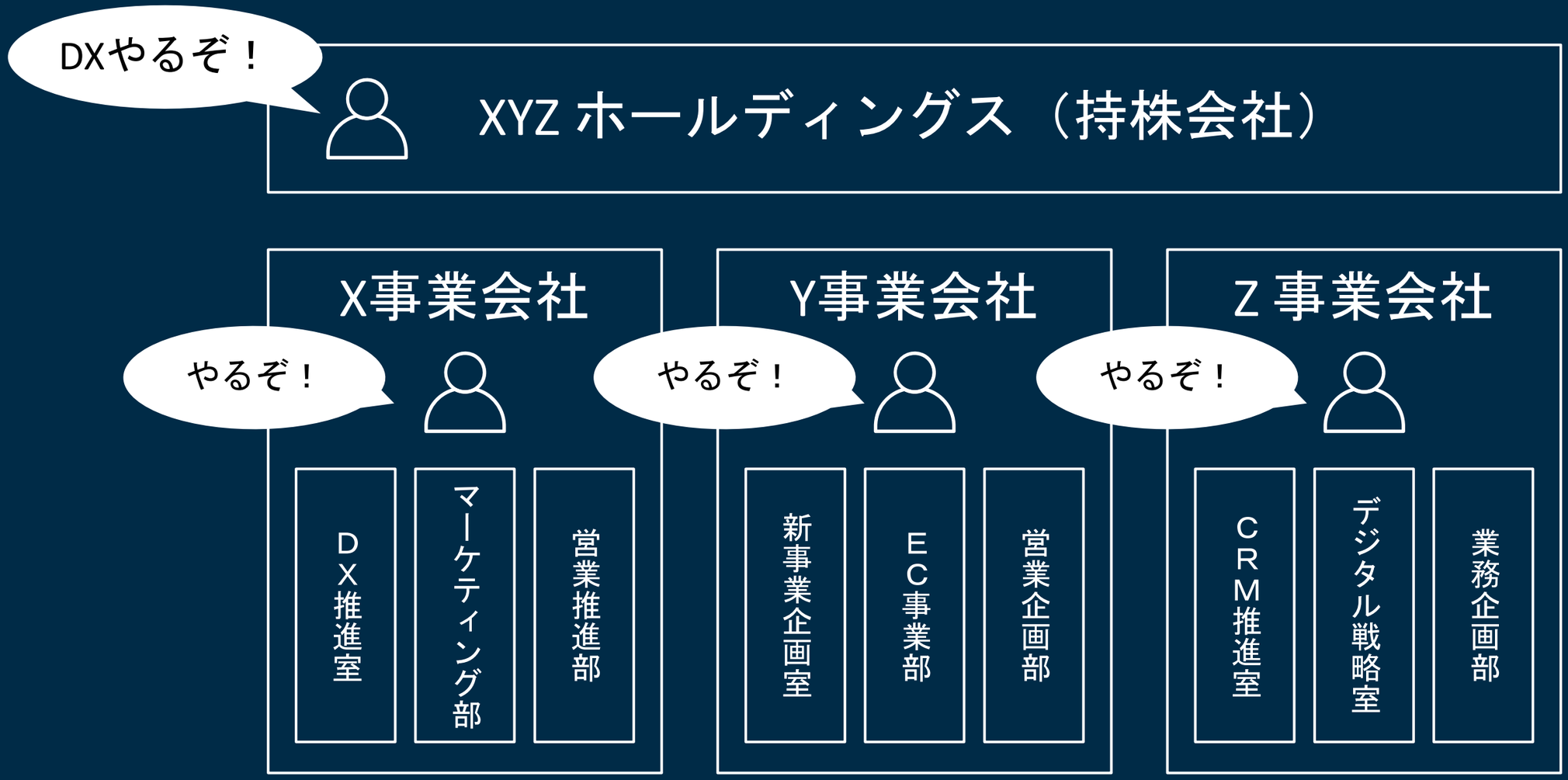
X事業会社

Y事業会社

Z 事業会社

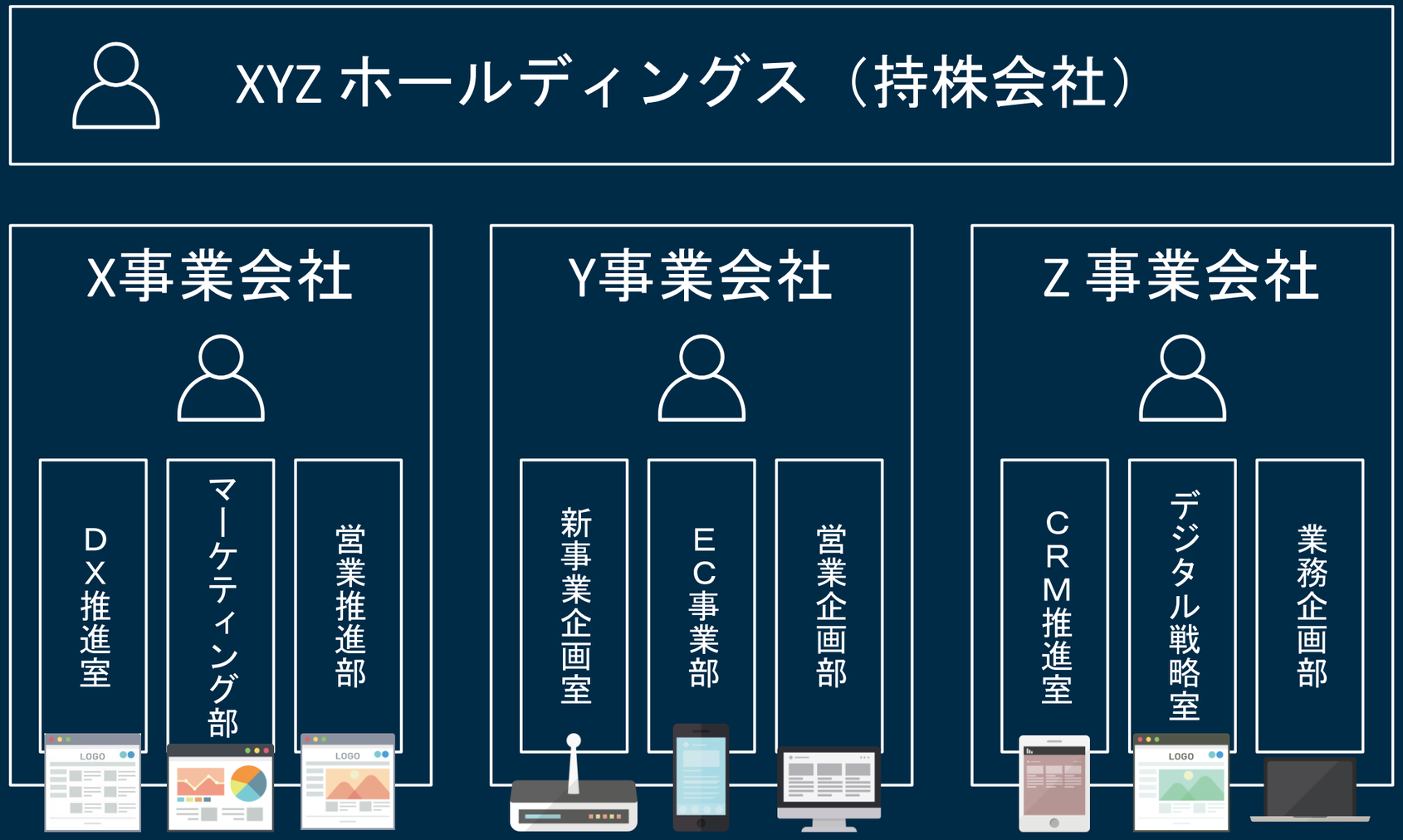
In Partnership with intel

各事業会社の各部門で新サービスを検討



In Partnership with intel

Web、モバイル、IoTなど新サービスが続々と開始



In Partnership with intel

グループ横断のデータ活用により顧客体験を向上したい

グループのシナジーを発揮するぞ！

XYZ ホールディングス（持株会社）

X事業会社

- DX推進室
- マーケティング部
- 営業推進部

Y事業会社

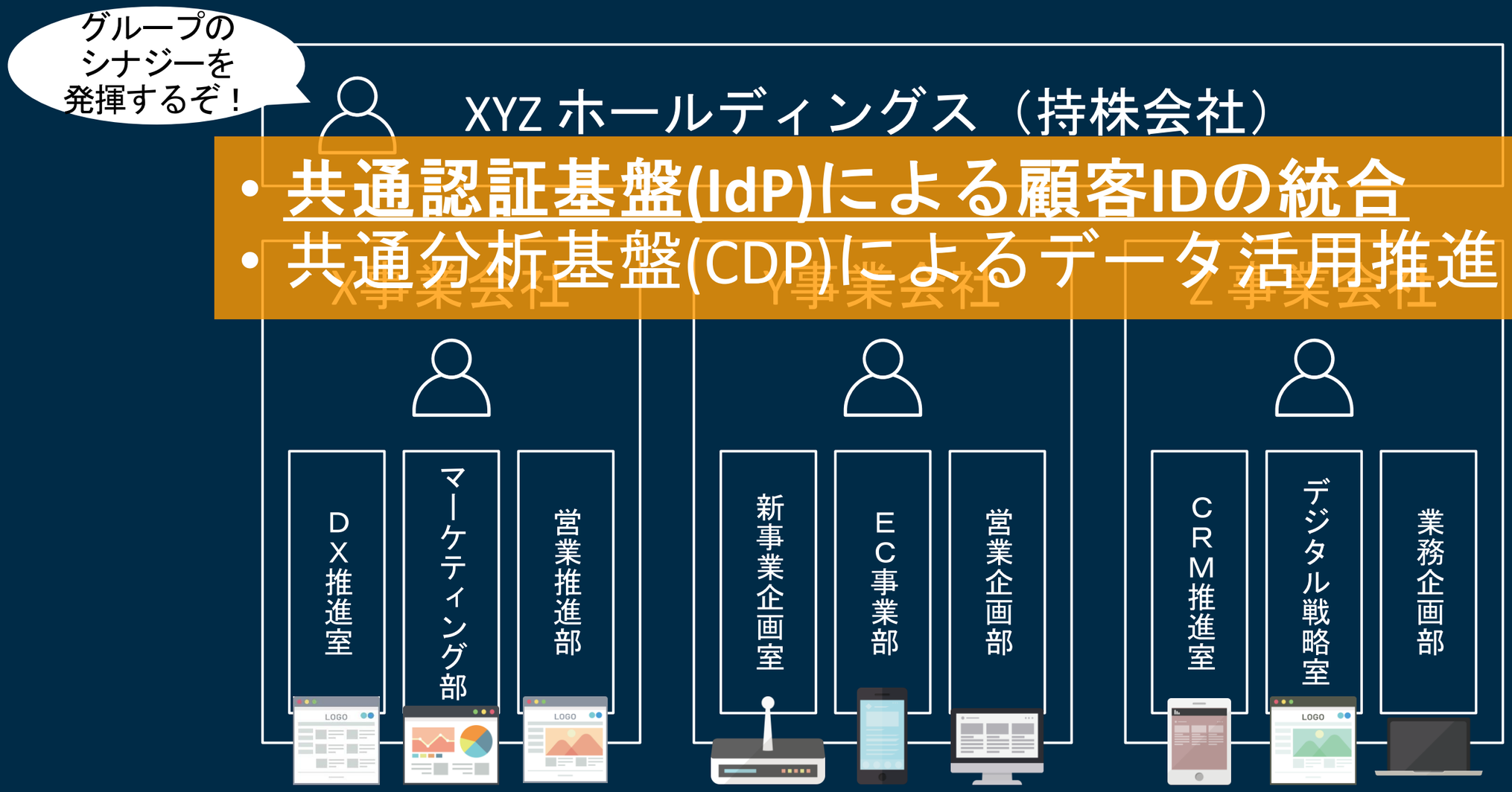
- 新事業企画室
- EC事業部
- 営業企画部

Z 事業会社

- CRM推進室
- デジタル戦略室
- 業務企画部

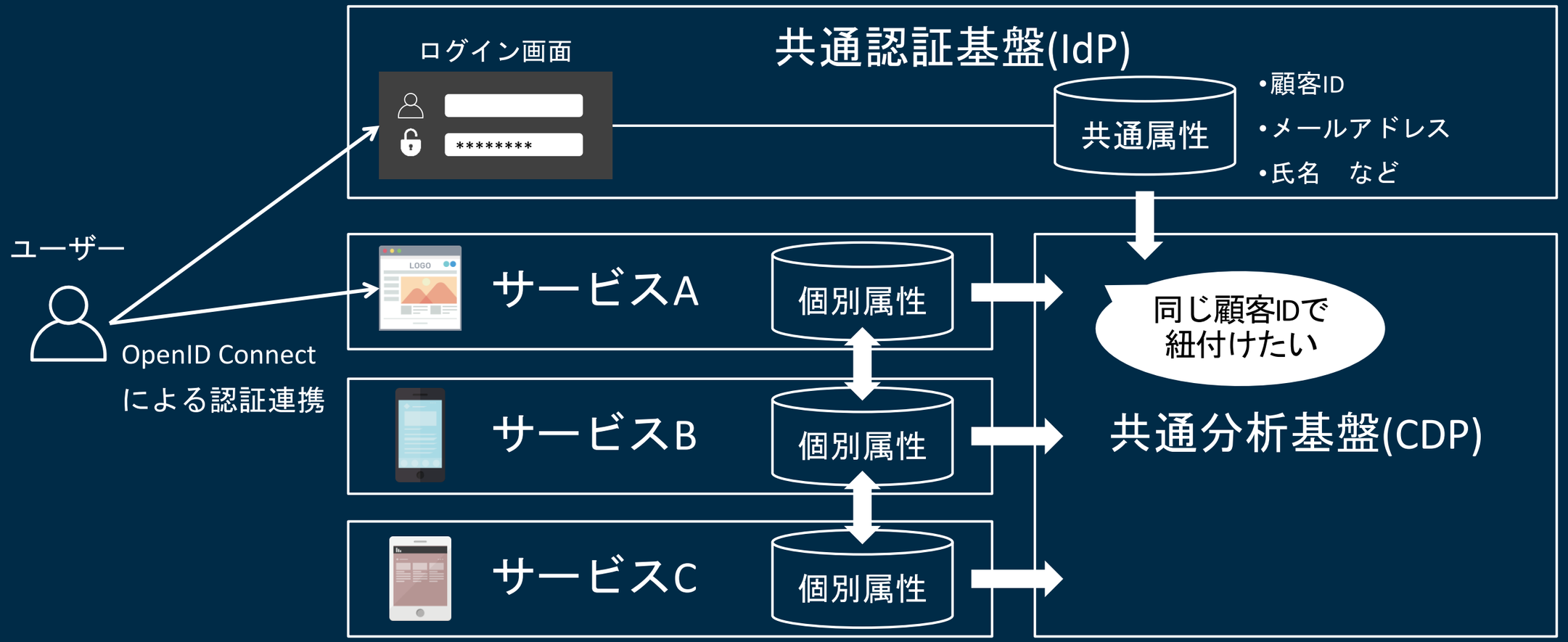
In Partnership with intel

グループ横断のデータ活用により顧客体験を向上したい



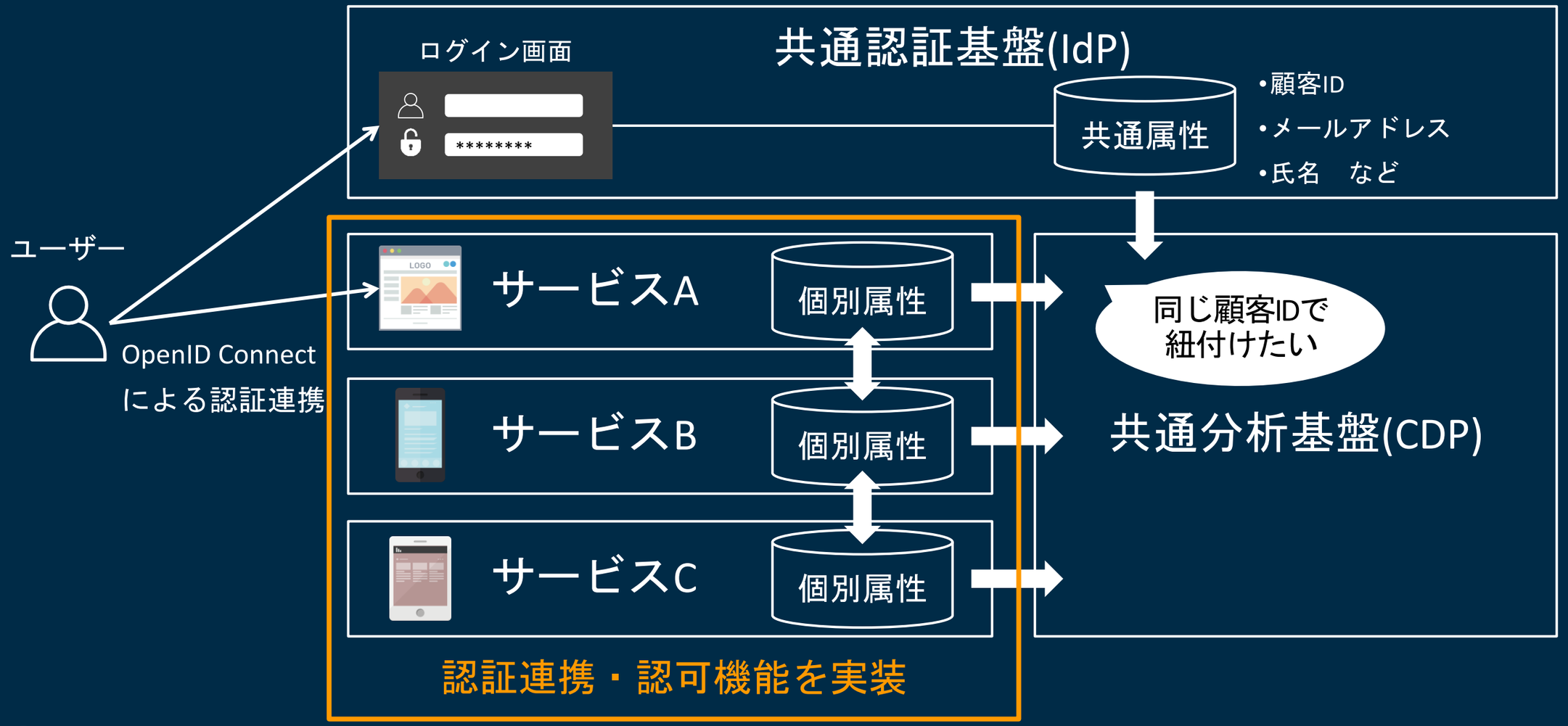
In Partnership with intel

顧客IDを統合するために



In Partnership with intel

サービス側で認証連携と認可機能を実装する必要がある



In Partnership with intel

認証・認可とは？

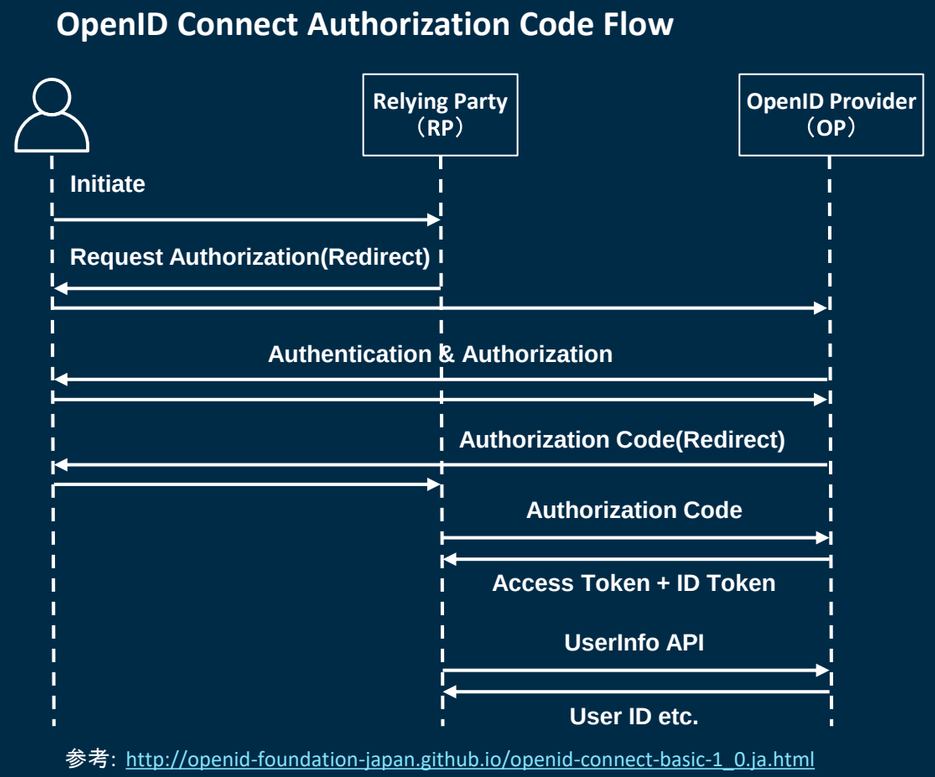
- 認証 (AuthN , Authentication)
  - 相手が誰であるかを確認すること
    例）ログインによる本人確認

- 認可 (AuthZ , Authorization)
  - 誰かに許可を与えること
    例）ログイン済みユーザにAPIへのアクセスを許可

認証・認可とは？

- 認証 (AuthN , Authentication)
  - 相手が誰であるかを確認すること
    例）ログインによる本人確認

- 認可 (AuthZ , Authorization)
  - 誰かに許可を与えること
    例）ログイン済みユーザにAPIへのアクセスを許可



参考: http://openid-foundation-japan.github.io/openid-connect-basic-1_0.ja.html

とても重要な機能だが、認証・認可の機能自体はビジネスの差別化につながらない

アプリケーション開発を加速するために、サービス側で実装する負担を減らしたい

In Partnership with intel

aws DEV DAY
ONLINE JAPAN

アプリケーション開発を加速するための AWSマネージドサービス活用

In Partnership with intel

エンタープライズとサービス開発の要件を両立する

- エンタープライズの要件
  - 共通の認証基盤・分析基盤を利用する
    - グループ横断のデータ活用
    - 共通のセキュリティ・ガバナンス
  - グループ内他サービスとユーザ情報連携
    - 他サービスの個別属性を連携する
      例）会員ランク・住所など
      - バッチによるファイルインターフェース

- サービス開発の要件
  - 開発アジリティ
    - サービス開発の実験と反復を繰り返し、顧客により良い体験を提供したい
  - ランニングコストの変動費化
    - ユーザー数を明確に想定できないため、ランニングコストが最初から固定費になるのは避けたい
  - 運用の手離れの良さ
    - 開発チームは他のサービスの開発にも着手するため、ビジネスの差別化に直結しない運用からは手離れしたい

In Partnership with intel

アプリケーション開発を加速するための基本方針

- AWSのマネージドサービスを活用する
  - アプリケーションで実装する機能の一部をマネージドサービスで実現
    - 車輪の再発明がなくなる→コード量が減る→ビジネスロジックの開発に注力
      例）認証・認可の機能をCognito/Amplifyで実装
  - バックエンドの機能をサーバーレスで開発
    - サーバーの運用管理がなくなる→インフラ運用がなくなり、コストは変動費に
    - キャパシティ不足による機会損失やセキュリティリスクを最小化

- フロントエンド開発にリソースを集中する
  - WebアプリはSingle Page Application(SPA)で開発する
    - リッチで操作性の高いUIを提供しやすい
    - フロントエンド(UI)とバックエンド(API)で開発者の関心事を分離できる
    - モバイルアプリ向けAPIにバックエンドの流用が可能

本セッションの主役はこちら

Amazon Cognito

Webアプリ、モバイルアプリのための
シンプルでセキュアな認証・認可を提供

AWS Amplify

Webアプリ、モバイルアプリの作成、設定、
実装を加速するツールとサービスのセット

In Partnership with

本セッションの主役はこちら

Amazon Cognito

Webアプリ、モバイルアプリのための
シンプルでセキュアな認証・認可を提供

- ユーザープール
  アプリへのアクセスに利用できるトークンを提供
- IDプール
  AWSにアクセスできるクレデンシャルを提供
- Cognito Sync
  モバイルアプリとクラウド間のデータ同期を実現

AWS Amplify

Webアプリ、モバイルアプリの作成、設定、
実装を加速するツールとサービスのセット

- Amplify Framework
  AWSのサービスで構築したバックエンドに直感的なインターフェースで接続できるライブラリ
- Amplify CLI
  AWSのサーバーレスなバックエンドを
  コマンドラインで構築・管理するCLIツール
- Amplify Console
  GitベースのSPAや静的サイトのCI/CDパイプラインを提供する静的Webホスティングサービス

In Partnership with intel

ソリューション構成

フロントエンド(UI)

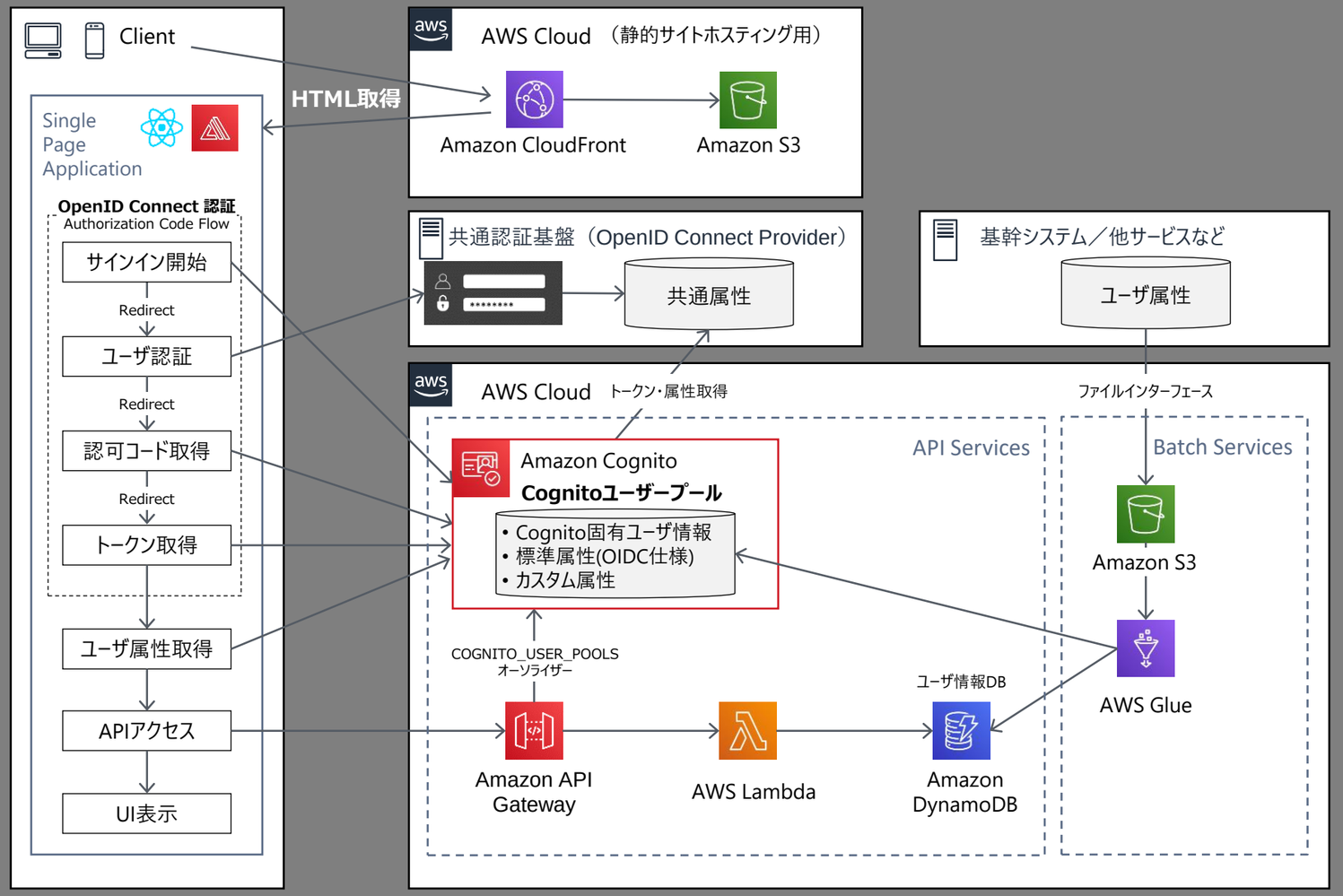
- React/Amplify を利用したSPA
- CloudFront/S3 にホスティング

バックエンド(API)

- Cognito
- API Gateway
- Lambda
- DynamoDB

バックエンド(Batch)

- S3
- Glue



In Partnership with intel

ソリューション構成

フロントエンド(UI)

- React/Amplify を利用したSPA
- CloudFront/S3 にホスティング

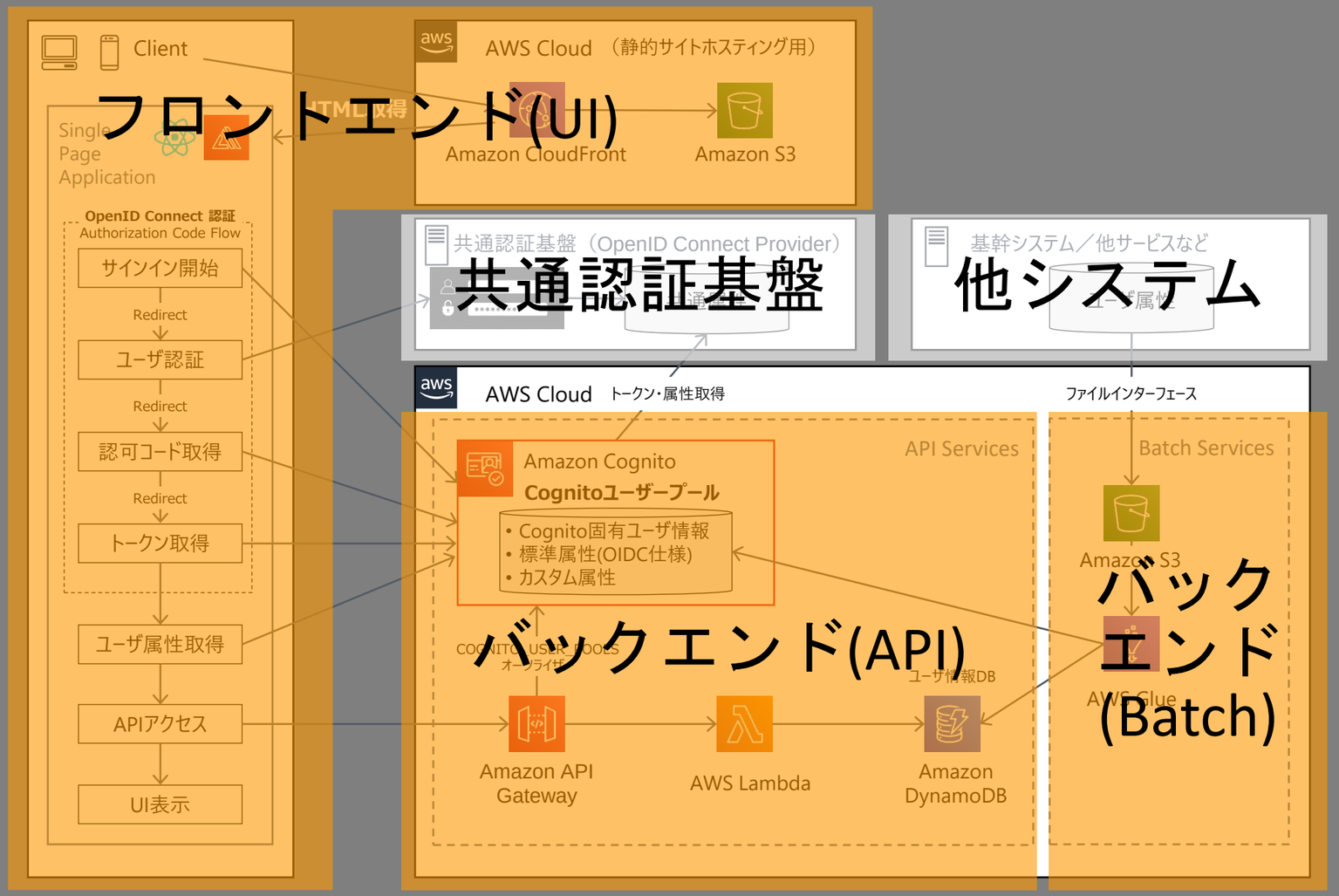
バックエンド(API)

- Cognito
- API Gateway
- Lambda
- DynamoDB

バックエンド(Batch)

- S3
- Glue

サービス開発側の実装範囲



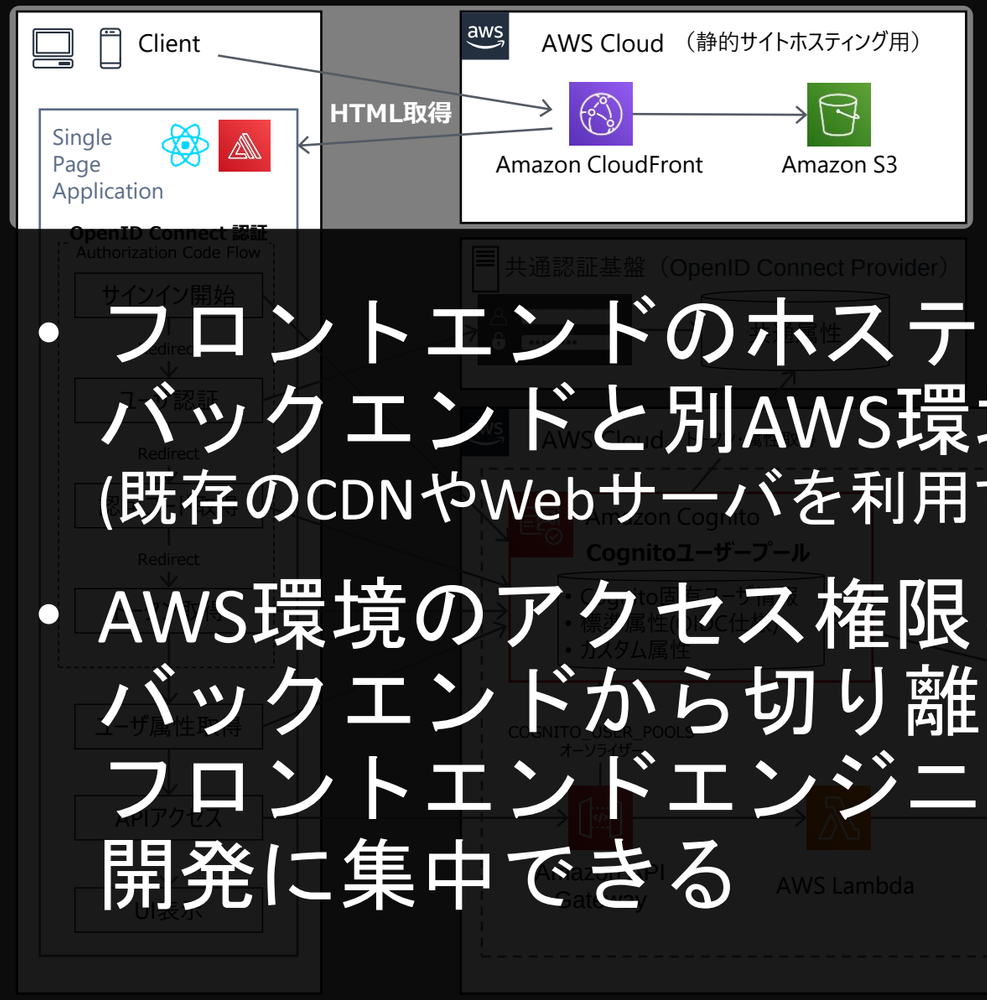
In Partnership with intel

ソリューション構成

フロントエンド(UI)
React/Amplify を利用したSPA
CloudFront/S3 にホスティング

バックエンド(API)
Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)
S3
Glue



- フロントエンドのホスティング先はバックエンドと別AWS環境
(既存のCDNやWebサーバを利用することも可能)
- AWS環境のアクセス権限と関心事がバックエンドから切り離されることでフロントエンドエンジニアはUIの開発に集中できる

In Partnership with intel

ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

バックエンド(API)

Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- OpenID Connectのバックエンド側(Relying Party)の実装は、Cognitoを利用することで環境設定のみで実現可能
- 認証連携サーバの運用管理も不要に

In Partnership with intel

ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

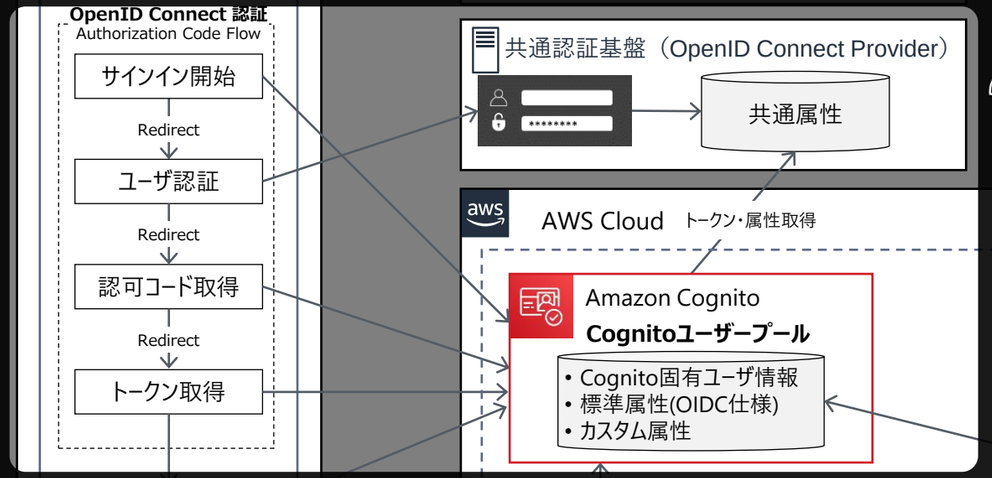
バックエンド(API)

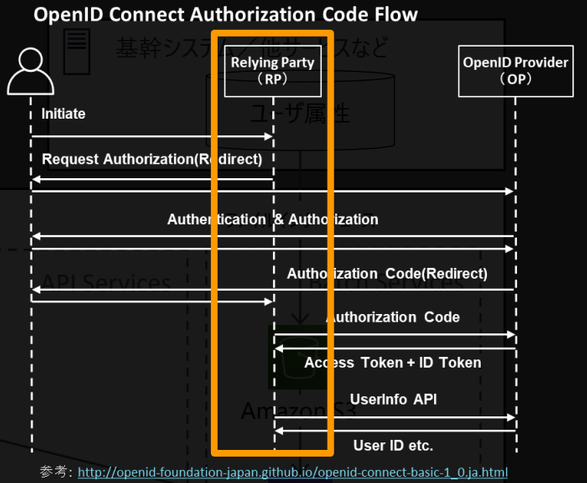
Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- OpenID Connectのバックエンド側(Relying Party)の実装は、Cognitoを利用することで環境設定のみで実現可能
- 認証連携サーバの運用管理も不要に





CognitoコンソールでのIDプロバイダー、属性マッピング設定

ソリューション構成

フロントエンド(UI)

- React/Amplify を利用したSPA
- CloudFront/S3 にホスティング

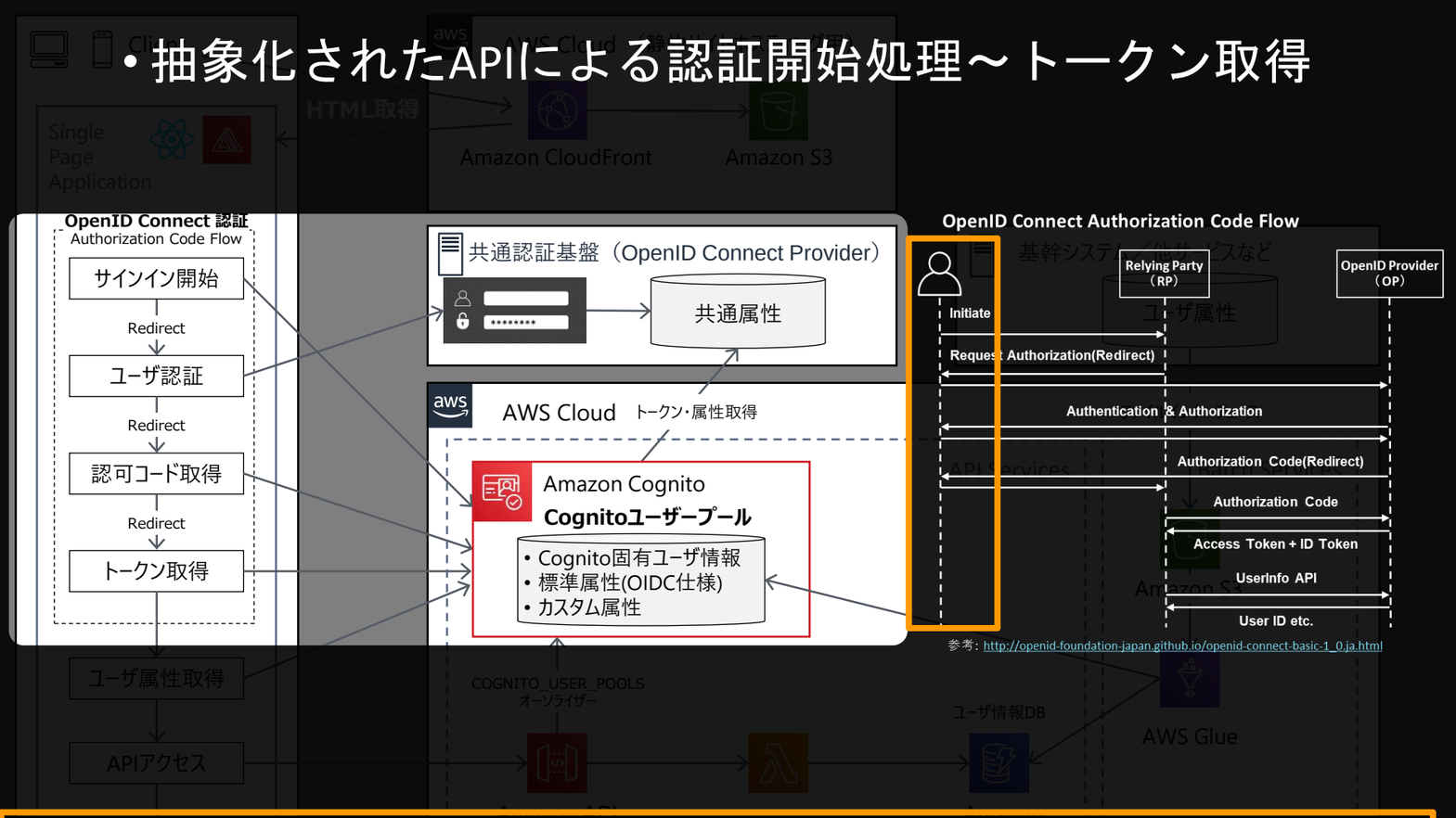
バックエンド(API)

- Cognito
- API Gateway
- Lambda
- DynamoDB

バックエンド(Batch)

- S3
- Glue

- OpenID Connectのフロント側の実装もAmplifyを利用することで、負担を軽減
  - 抽象化されたAPIによる認証開始処理～トークン取得



(Reactの場合) OpenID Connectによるサインインボタン

```
<button onClick={() => Auth.federatedSignIn({provider})}>Sign In</button>
```


In Partnership with intel

ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

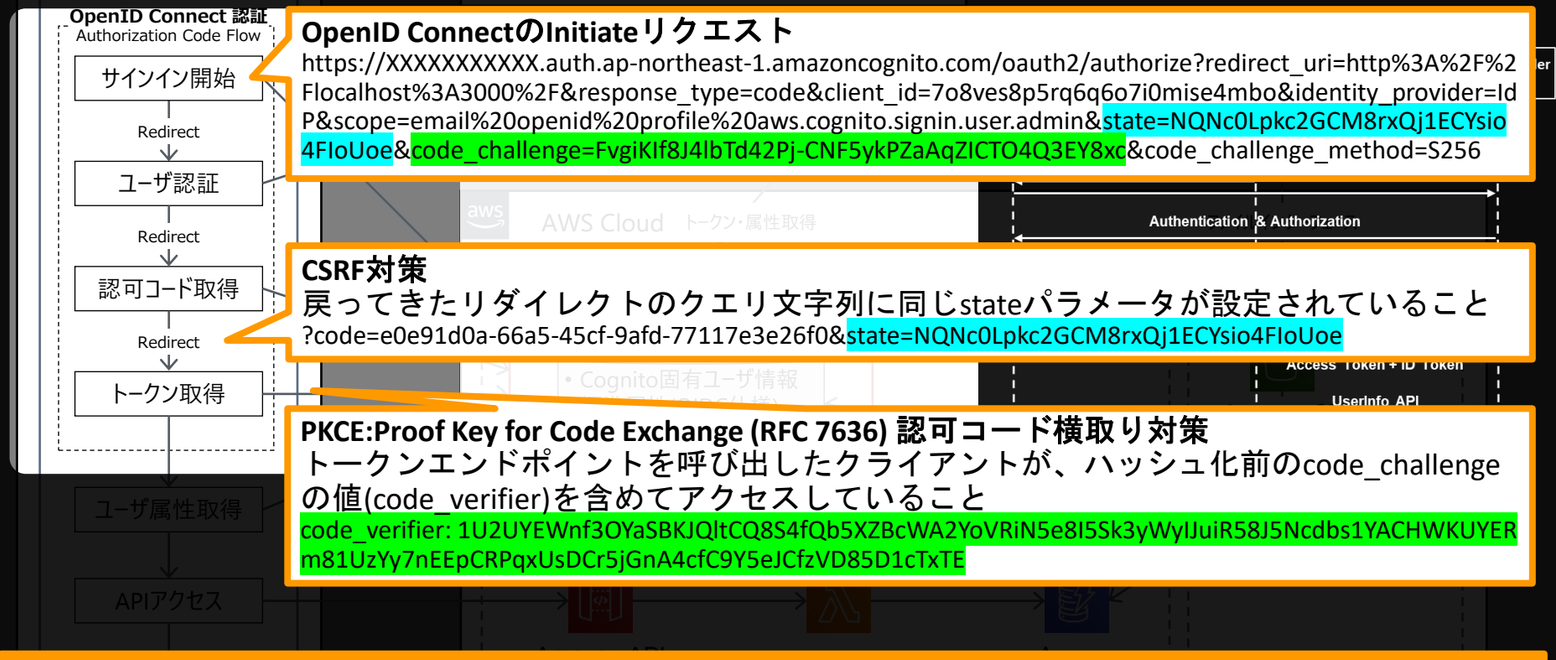
バックエンド(API)

Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- OpenID Connectのフロント側の実装もAmplifyを利用することで、負担を軽減
  - 抽象化されたAPIによる認証開始処理～トークン取得
  - state,PKCEの設定・検証による標準セキュリティ対策



これだけのセキュリティ対策の実装がコード１行！！！

```
<button onClick={() => Auth.federatedSignIn({provider})}>Sign In</button>
```


In Partnership with intel

ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

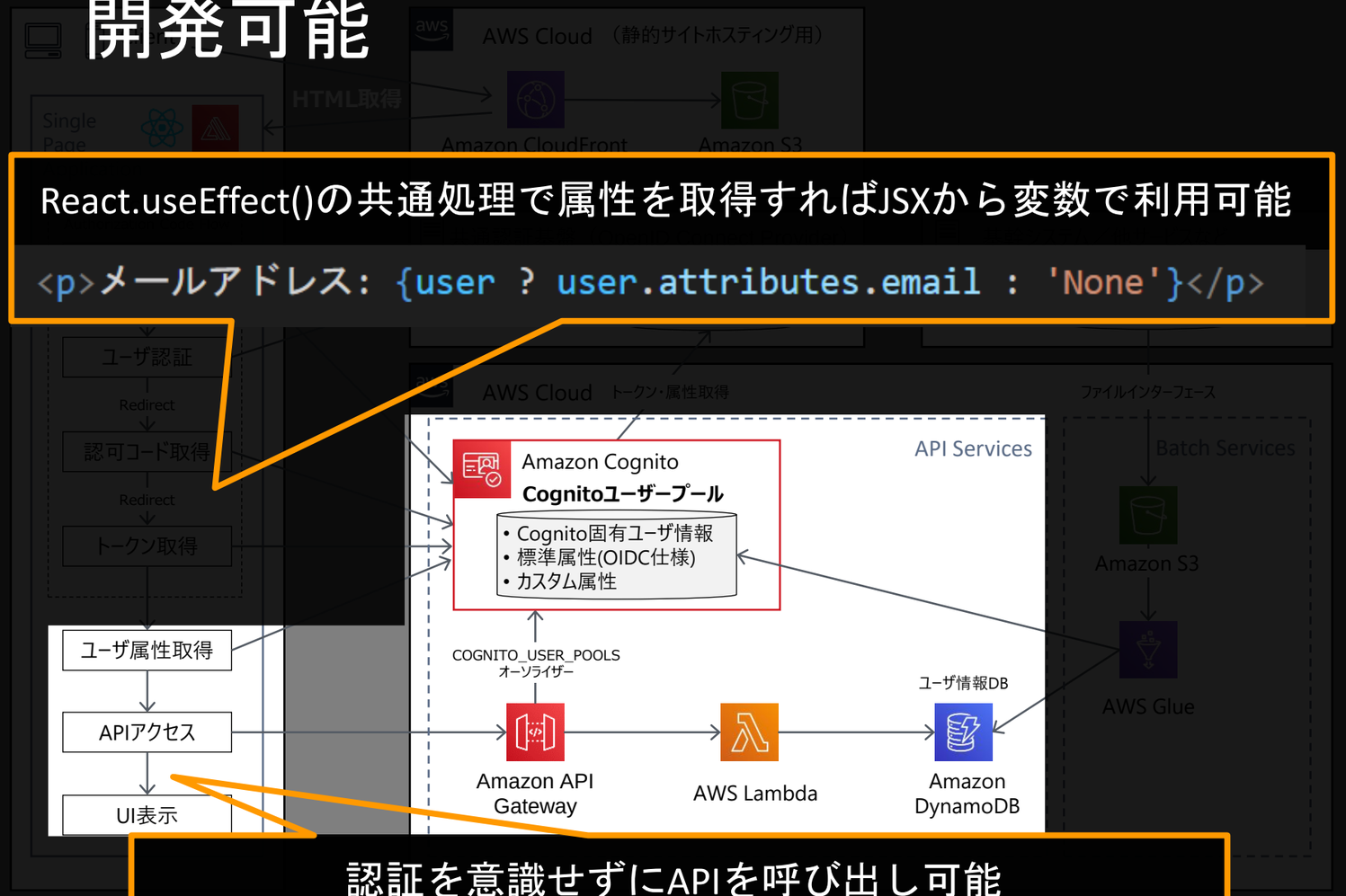
バックエンド(API)

Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- Cognito/Amplifyによって、フロント側はAPIの呼び出しに認証を意識せずに開発可能



ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

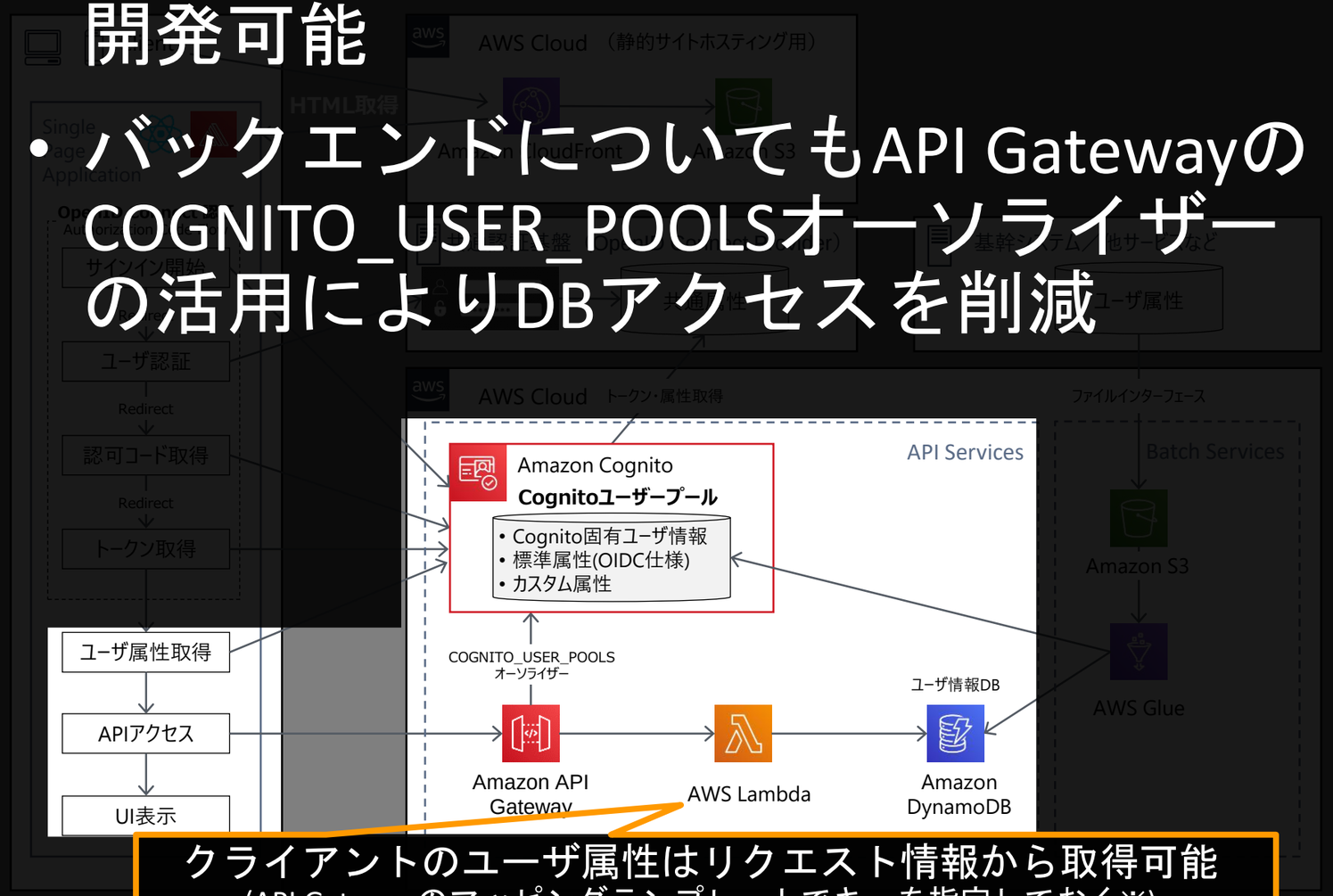
バックエンド(API)

Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- Cognito/Amplifyによって、フロント側はAPIの呼び出しに認証を意識せずに開発可能
- バックエンドについてもAPI GatewayのCOGNITO_USER_POOLSオーソライザーの活用によりDBアクセスを削減



※ https://docs.aws.amazon.com/ja_jp/apigateway/latest/developerguide/apigateway-enable-cognito-user-pool.html

ソリューション構成

フロントエンド(UI)

React/Amplify を利用したSPA
CloudFront/S3 にホスティング

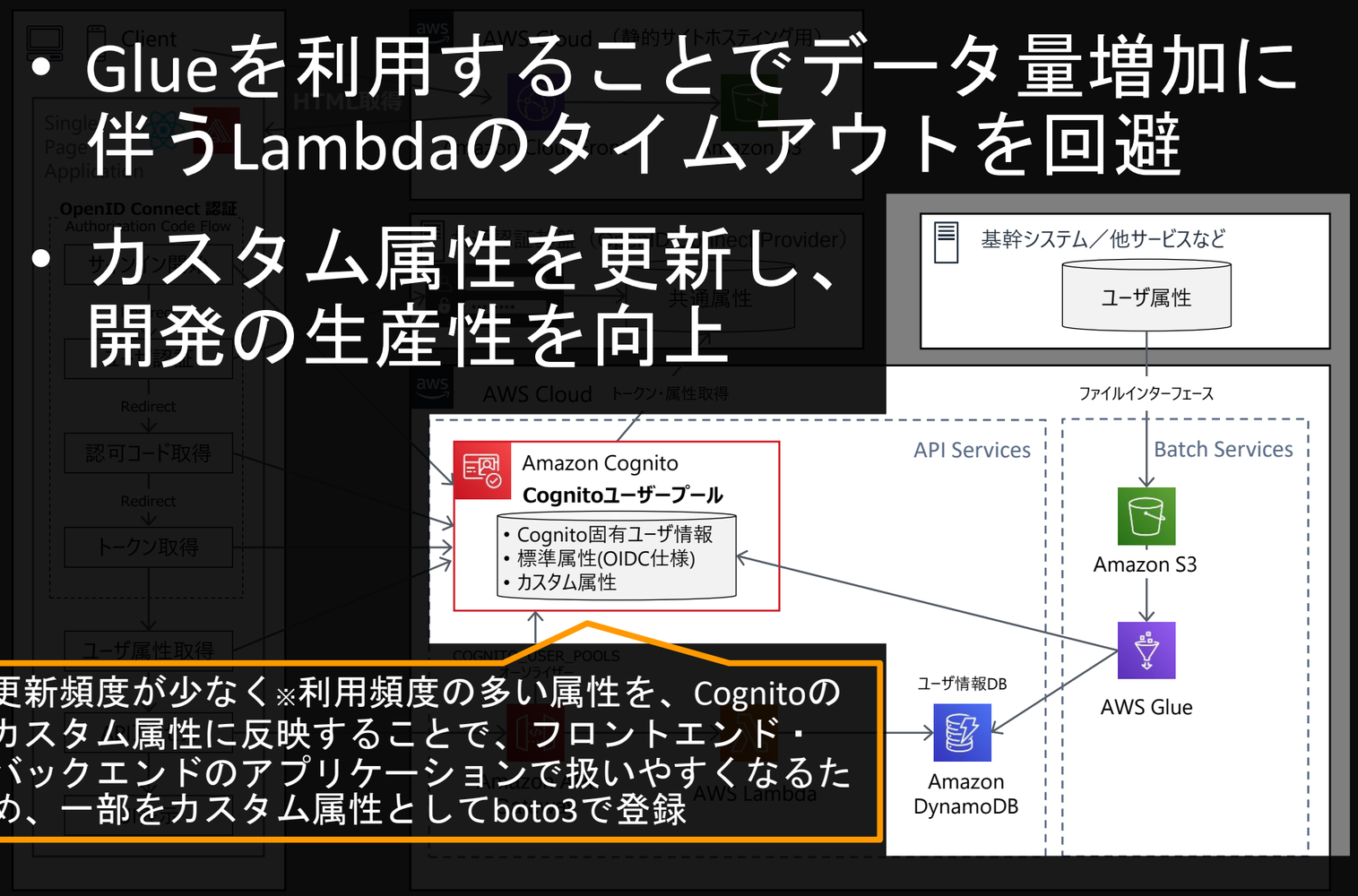
バックエンド(API)

Cognito
API Gateway
Lambda
DynamoDB

バックエンド(Batch)

S3
Glue

- バッチによる外部システムからのファイル転送をS3で受付
- Glueを利用することでデータ量増加に伴うLambdaのタイムアウトを回避
- カスタム属性を更新し、開発の生産性を向上



更新頻度が少なく※利用頻度の多い属性を、Cognitoのカスタム属性に反映することで、フロントエンド・バックエンドのアプリケーションで扱いやすくなるため、一部をカスタム属性としてboto3で登録

※更新頻度が多い属性をユーザープール属性とするのは推奨されていない
https://docs.aws.amazon.com/ja_jp/cognito/latest/developerguide/user-pool-settings-attributes.html

エンタープライズとサービス開発の要件を両立する

- エンタープライズの要件
  - 共通の認証基盤・分析基盤を利用する
    - グループ横断のデータ活用
    - 共通のセキュリティ・ガバナンス

Cognito/Amplifyで認証連携を実現

  - グループ内他サービスとユーザ情報連携
    - 他サービスの個別属性を連携する
      例）会員ランク・住所など
      - バッチによるファイルインターフェース

S3/Glueでバッチによるデータ連携を実現

- サービス開発の要件
  - 開発アジリティ
    - サービス開発の実験と反復を繰り返し、顧客により良い体験を提供したい

Cognito/Amplifyで開発スピードUP

  - ランニングコストの変動費化
    - ユーザー数を明確に想定できないため、ランニングコストが最初から固定費になるのは避けたい

フルマネージドサービス利用で固定費ほぼゼロ

  - 運用の手離れの良さ
    - 開発チームは他のサービスの開発にも着手するため、ビジネスの差別化に直結しない運用からは手離れしたい

サーバーレスのため運用は最小限に

aws DEV DAY
ONLINE JAPAN

まとめ

In Partnership with intel

本日お話ししたかったこと

- エンタープライズで新サービス開発をする際、認証やデータの連携は避けて通れない課題となり、開発アジリティとのトレードオフが発生

- Cognito/Amplifyは、独自のユーザ認証・ユーザ管理を実現するためだけでなく、OpenID Connect Providerと認証連携可能なアプリケーションを素早く実装するために活用できる

- マネージドサービスやサーバーレスは開発・運用コストの削減効果が大きいが、エンタープライズに求められる要件を充足するどうかは、“信頼しつつも検証すべき”

aws DEV DAY
ONLINE JAPAN

エンタープライズの認証・認可要件を素早く実現するために、CognitoやAmplifyを活用してアプリケーションの開発を加速させましょう

In Partnership with intel

aws DEV DAY
ONLINE JAPAN

ご清聴ありがとうございました！

安藤 裕紀
y-ando@nri-digital.jp

In Partnership with intel

aws DEV DAY
ONLINE JAPAN

20-22.10.2020

DEV DAY

In Partnership with intel