T 1 - 4

Amazon QuickSight で実現する セキュアな BI 環境

野上 恭平
アマゾン ウェブ サービス ジャパン株式会社
ソリューションアーキテクト

自己紹介

野上 恭平

ソリューションアーキテクト

Web業界のお客さまを担当

好きなサービス

- Amazon Redshift

本セッションのAgenda

- QuickSight の概要
- QuickSight で実現可能なセキュリティ対策
  - ユーザーを一元管理したい
  - 役割ごとに権限管理を実施したい
  - ユーザーごとにアクセス可能なデータを制限したい
  - データソースへのアクセスをセキュアに行いたい
  - ユーザーの操作ログを保管したい

Amazon QuickSight とは

クラウドネイティブで作られたスケーラブル・従量課金のクラウドBI ツール

スケーラブルな料金体型

利用量ベース

規模によらず
コストを最適化

オートスケール＆サーバーレス

グローバルで
100万ユーザー以上が
利用可能な環境を
サーバレスで構築

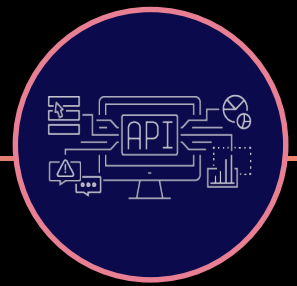
組み込みの高可用性

AWSサービスとのフル・インテグレーション

AWS データへの
セキュア・プライベートアクセス

S3 のデータレイク権限との統合

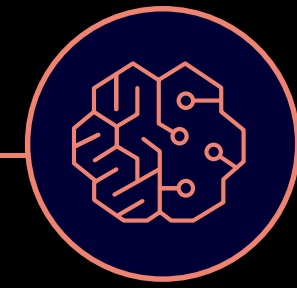
開発者支援



プログラムによる
ユーザー管理と
コンテンツ管理

アプリケーションへの
容易な組み込み

機械学習

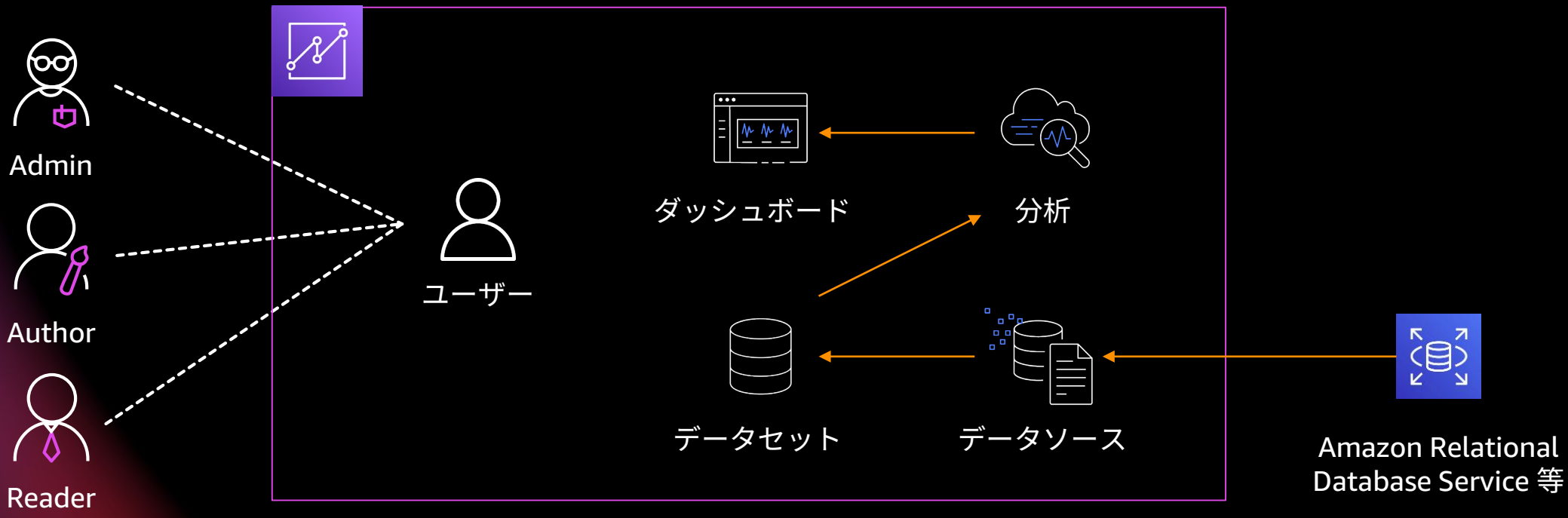


機械学習による組み込み
異常検知・予測機能

Amazon SageMakerで
作成した独自モデルの利用

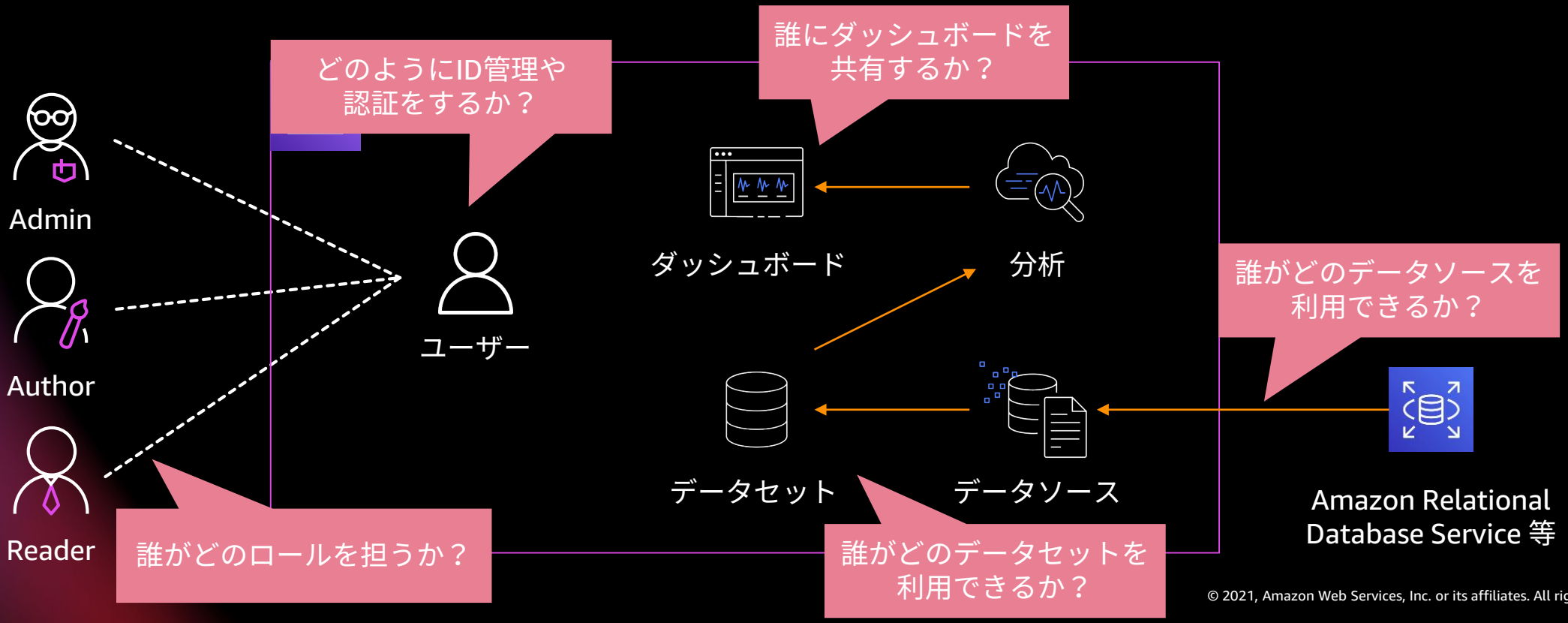
QuickSightで登場する概念の整理

1. Admin/Authorはデータソースを定義し、分析用のデータセットを準備する。
2. Authorはデータセットを基に分析を作成、Readerにダッシュボードとして共有する。
3. Readerはダッシュボードをブラウザや、スマートフォンから閲覧する。



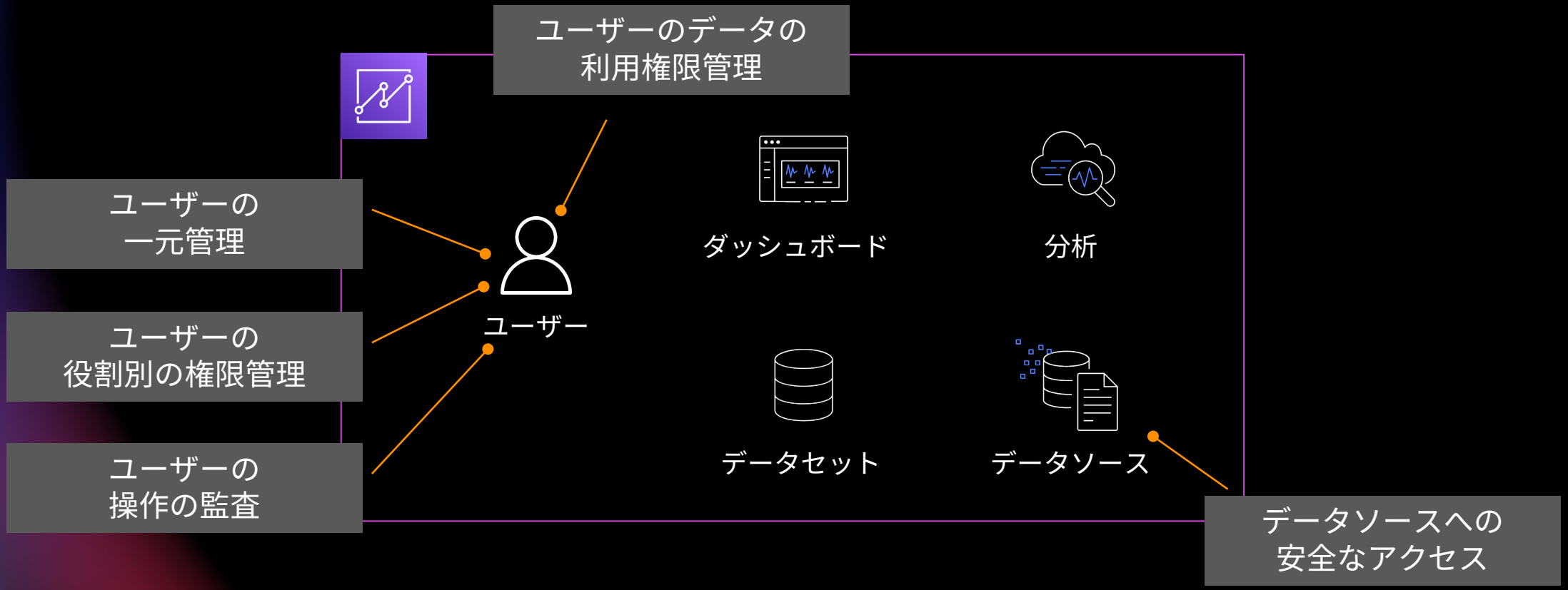
どんなセキュリティの考慮点があるか？

1. Admin/Authorはデータソースを定義し、分析用のデータセットを準備する。
2. Authorはデータセットを基に分析を作成、Readerにダッシュボードとして共有する。
3. Readerはダッシュボードをブラウザや、スマートフォンから閲覧する。



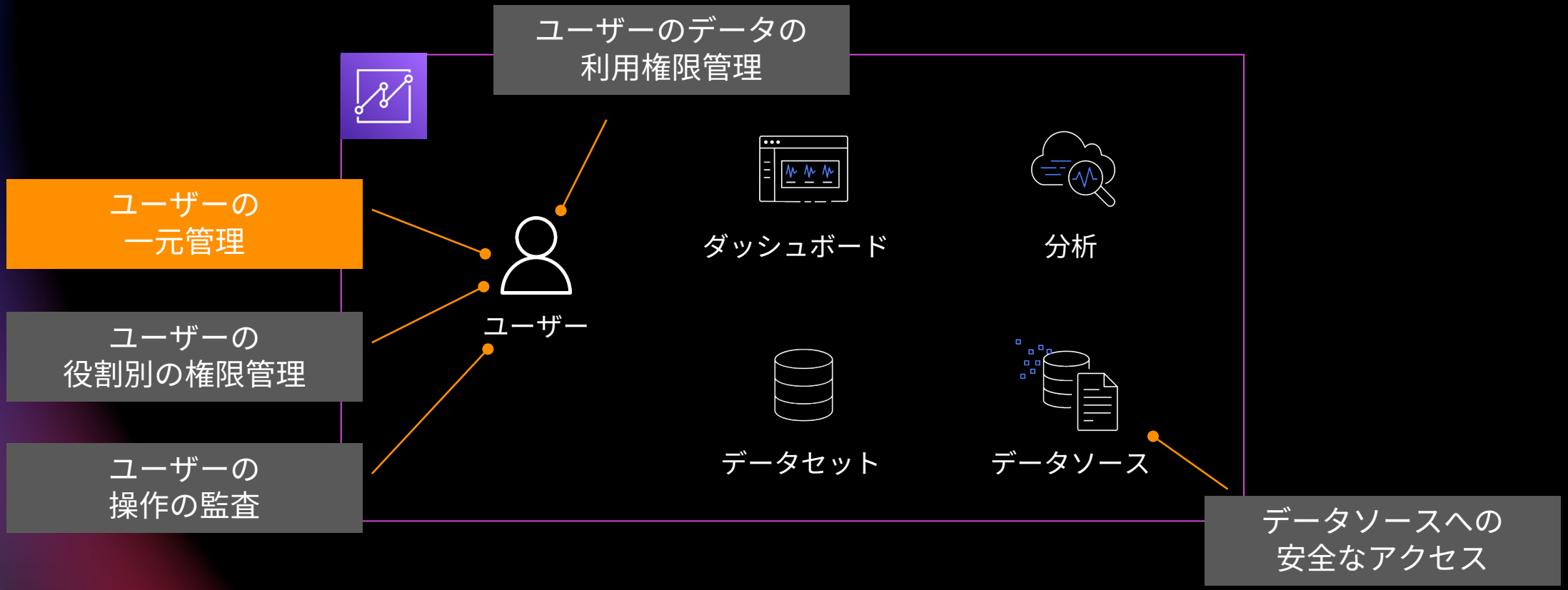
QuickSightで実現可能なセキュリティ対策

QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



QuickSightで実現可能なセキュリティ対策

QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



ユーザーを一元管理したい

QuickSightにおけるID管理の方式

QuickSightにおけるID管理は、3つの実現方法がある。

① Emailアドレス管理

- emailアドレス用いてQuickSight独自でIDを管理する。

② IAM+フェデレーションによるSSO

- AWS Identity and Access Management （IAM）の機能でIDを管理する。
- IAMユーザを直接利用するか、SAML 2.0のIdPとフェデレーションしSSOを実現する。

③ Active Directory 連携

- 既存の Microsoft Active Directory でIDを管理する。
- QuickSightのホームリージョンに AWS Managed Microsoft AD または Active Directory Connectorが必要。

ユーザーを一元管理したい

ID管理方式の選択指針

管理工数を減らすためにIAM+フェデレーションによるSSOを前提とするのがよい。

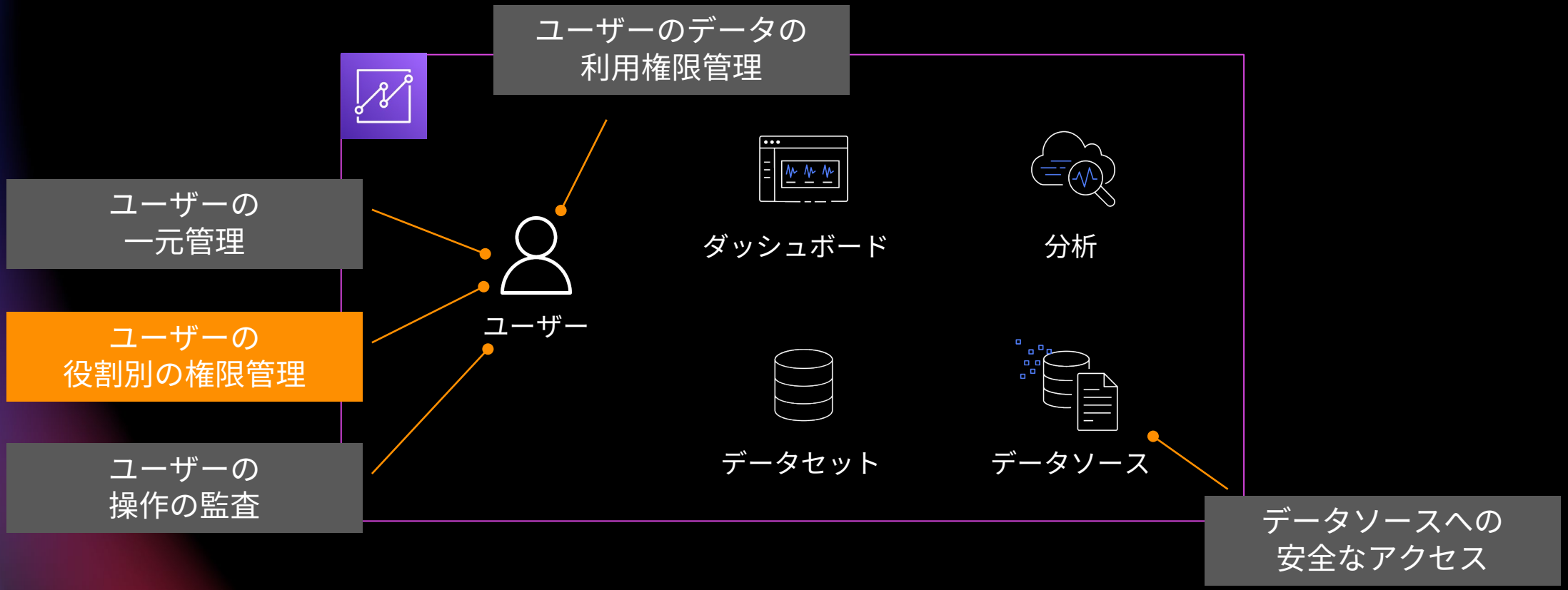
小規模での利用や一部のユーザーのみ個別にIDを発行する場合にはEmailアドレス管理も選択しうる。

ID管理にどの方式を利用するかは、QuickSightへのサインアップ時にのみ指定でき、
下記の3つのパターンから選択する。

ID管理方式	Emailアドレス管理	IAM+フェデレーションによるSSO	Active Directory連携
利用シーン	小規模での利用	中～大規模での利用	すでにADを利用中 かつ、ADの所属情報を利用する
パターン1	○	○	
パターン2		○	
パターン3			○

QuickSightで実現可能なセキュリティ対策

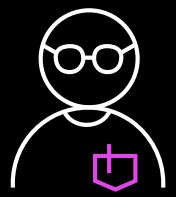
QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



役割ごとに権限管理を実施したい

ユーザーごとにロールを設定する

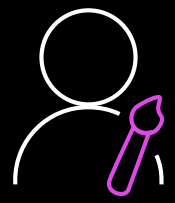
ユーザーが必要な操作ごとにロールを設定し、実施できる操作を制限できる。



Admin

BI 環境の管理者

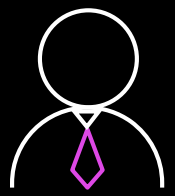
（Author の全ての機能に加えて）
- QuickSight ユーザーの管理
- SPICE 容量の管理や購入
- サブスクリプションの変更
- IAM を使って QuickSight から他 AWS サービスへのアクセス権限の制御



Author

分析やダッシュボードの編集者

（Reader の全ての機能に加えて）
- データソースの作成、管理
- データセットの作成、管理
- 分析の作成、管理
- ダッシュボードの作成、管理



Reader

ダッシュボードの閲覧者

- ダッシュボードの閲覧（ドリルダウン、フィルタ等）

役割ごとに権限管理を実施したい

カスタムパーミッションで、より柔軟な制限を実現

カスタムパーミッションを定義し、ユーザーごとにQuicksight上での操作を制限できる。
このとき、元々ロールが有している権限よりも強い権限は与えられない。

実装例と目的

AuthorA

分析を作成してダッシュボードを公開できるが、データセットの操作権限を禁止してデータセットの乱立を防ぐ。

AuthorB

分析を作成してダッシュボードを公開できるが、CSV/Excel のエクスポートを禁止して、QuickSight上のデータの持ち出しを防ぐ。

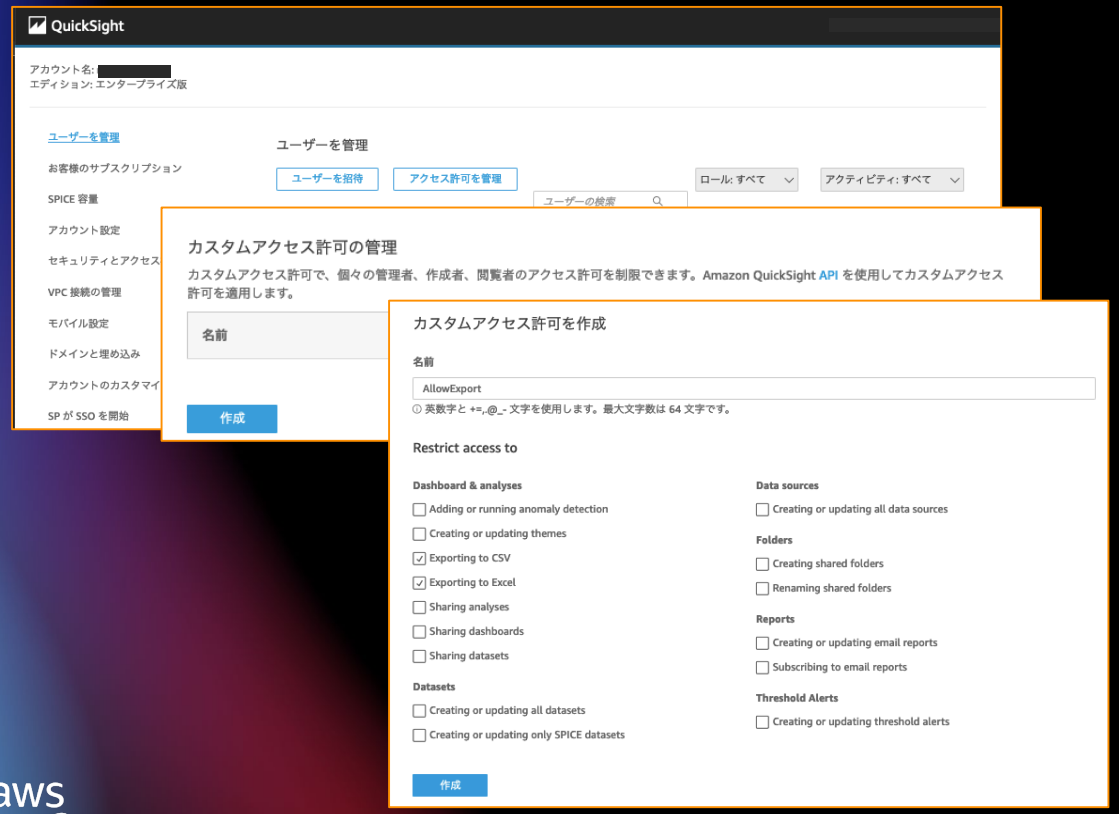
分類	制限可能な操作
データソースとデータセット	• すべてのデータセットの作成/更新 • SPICE データセットのみを作成/更新 • データソースの作成/更新
分析とダッシュボード	• 異常検出の追加または実行 • テーマの作成または更新 • CSV へのエクスポート • Excel へのエクスポート • 分析の共有 • ダッシュボードの共有 • データセットの共有
フォルダー	• 共有フォルダの作成 • 共有フォルダの名前を変更する
レポート	• 電子メールレポートの作成または更新 • 電子メールレポートの購読
しきい値アラート	• しきい値アラートの作成または更新

役割ごとに権限管理を実施したい

カスタムパーミッションの設定方法

カスタムパーミッションの作成/管理は、 QuickSight のマネジメントコンソールから実施可能。
各ユーザーへの割り当ては API 経由で実施する。

カスタムパーミッションの作成

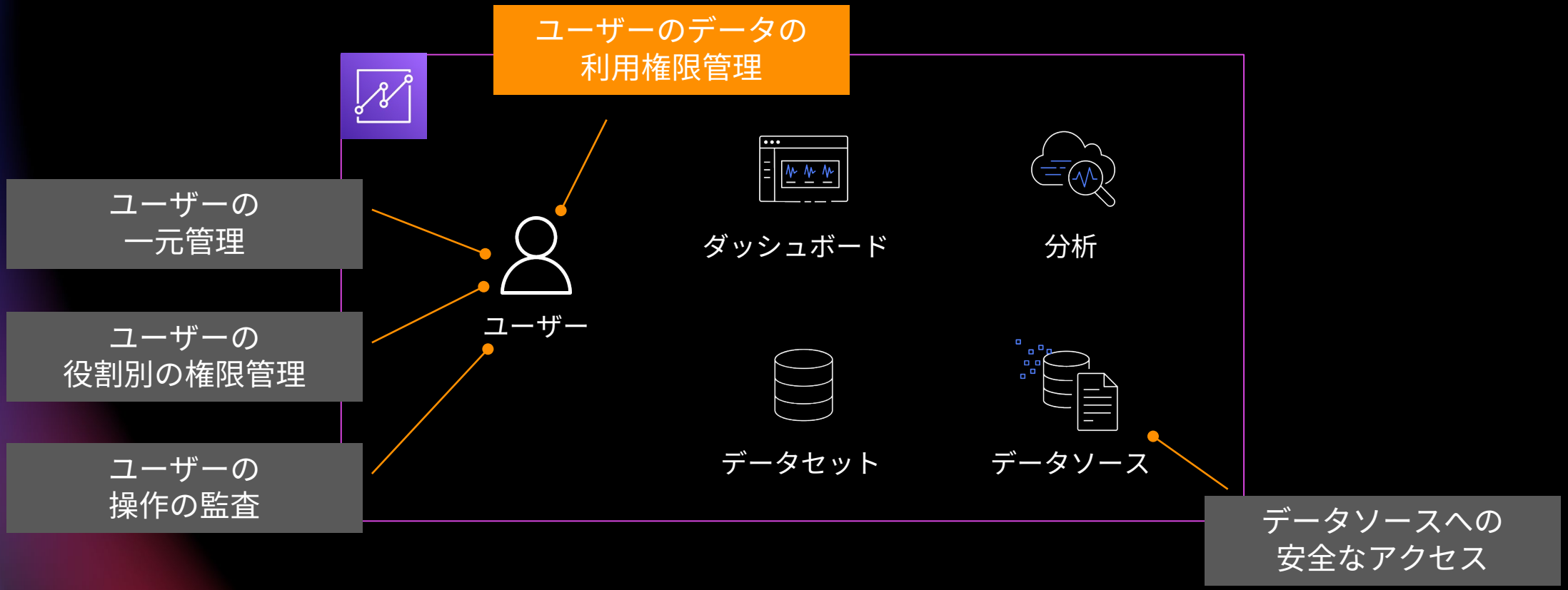


カスタムパーミッションの割り当て

```
$ aws quicksight update-user ¥
    --user-name user1 ¥
    --aws-account-id 012345678910 ¥
    --namespace default ¥
    --email user1@example.com ¥
    --role AUTHOR ¥
    --custom-permission-name AllowExport
```

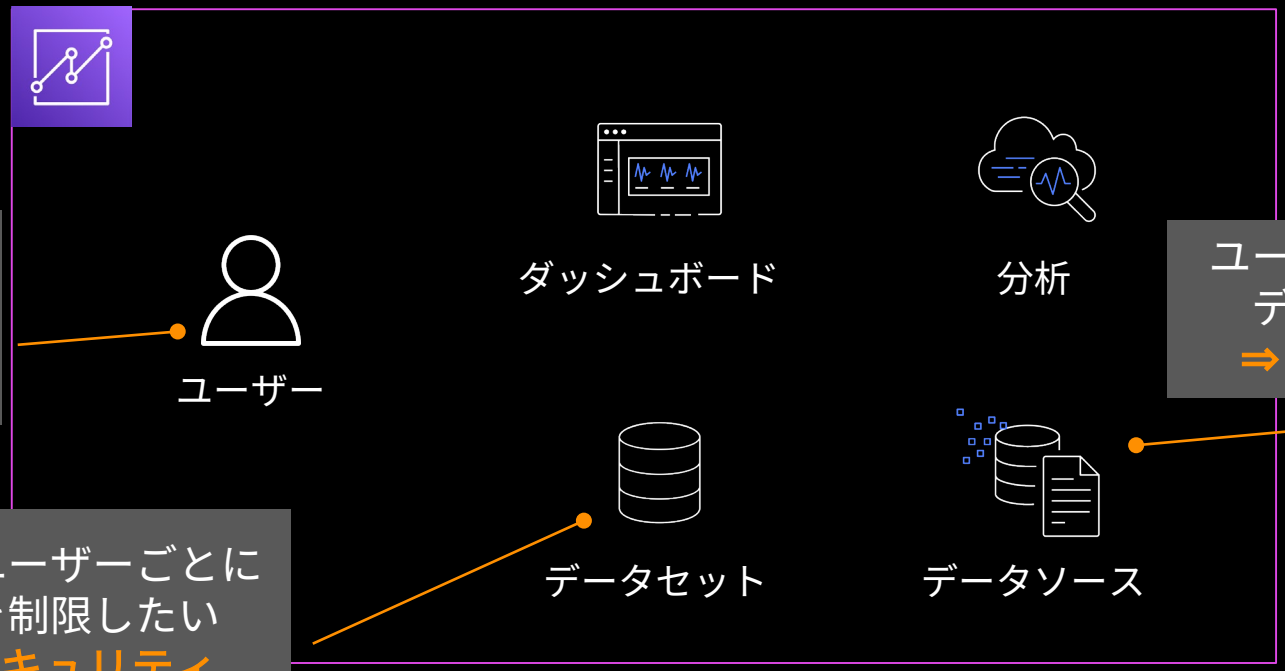
QuickSightで実現可能なセキュリティ対策

QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



ユーザーごとにアクセス可能なデータを制限したい

ユースケースの細分化



ユーザーごとにリソースへのアクセス権限を設定したい
⇒リソースの共有、マルチテナンシー

ユーザーごとにアクセス可能なデータソースを制限したい
⇒ スコープダウンポリシー

同じデータセットでも、ユーザーごとにアクセス可能なデータを制限したい
⇒行レベル/列レベルセキュリティ

ユーザーごとにアクセス可能なデータを制限したい

QuickSightリソースの共有

ダッシュボード、分析、データセット、データソースのいずれも
作成直後は作成したユーザーのみがアクセス可能。
明示的な共有操作をしてはじめて他のユーザーが利用できるようになる。

QuickSightのグループでユーザーを束ね、
グループに対してリソースを共有すると、
グループに所属するユーザーに一括で共有できる。

グループの作成やグループのユーザー管理は API で操作可能。

グループ作成

```
$ aws quicksight create-group ¥
    --group-name group1 ¥
    --aws-account-id 012345678910 ¥
    --namespace default
```

グループへのユーザー追加

```
$ aws quicksight create-group-membership ¥
    --group-name group1 ¥
    --member-name user1 ¥
    --aws-account-id 012345678910 ¥
    --namespace default
```

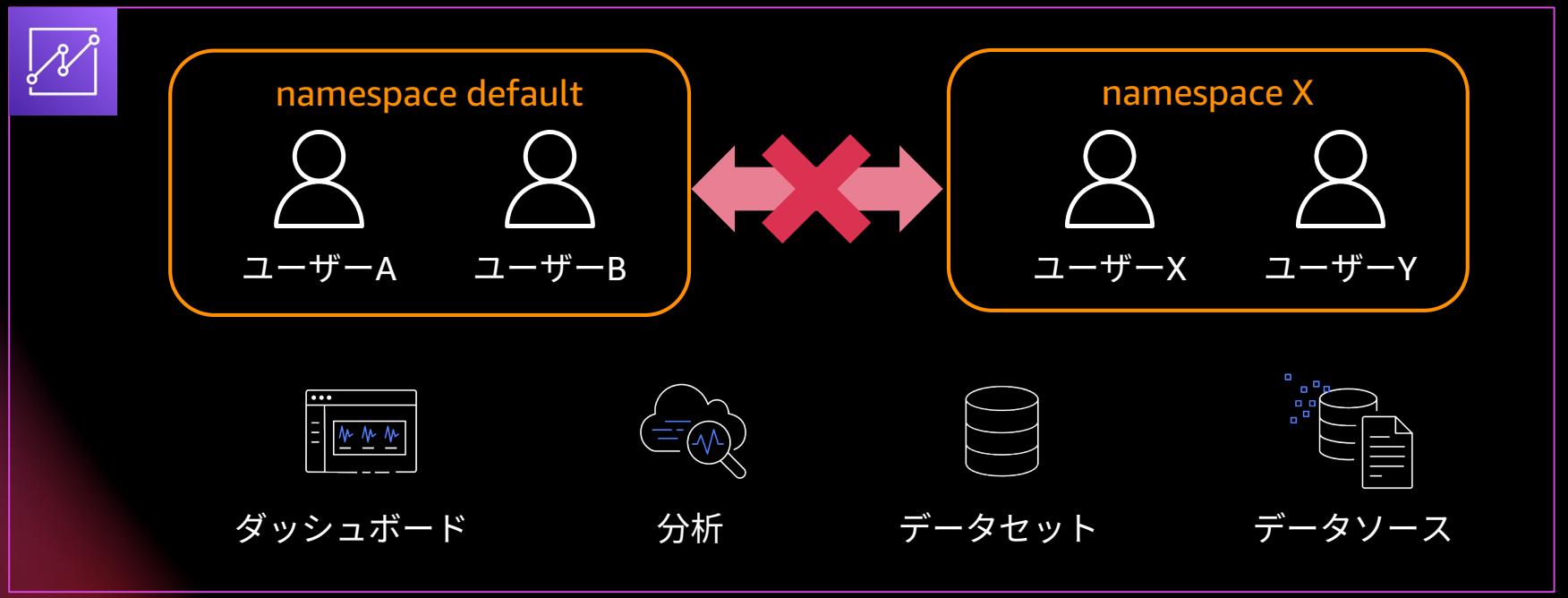
分析の共有例

ユーザーごとにアクセス可能なデータを制限したい

マルチテナンシー

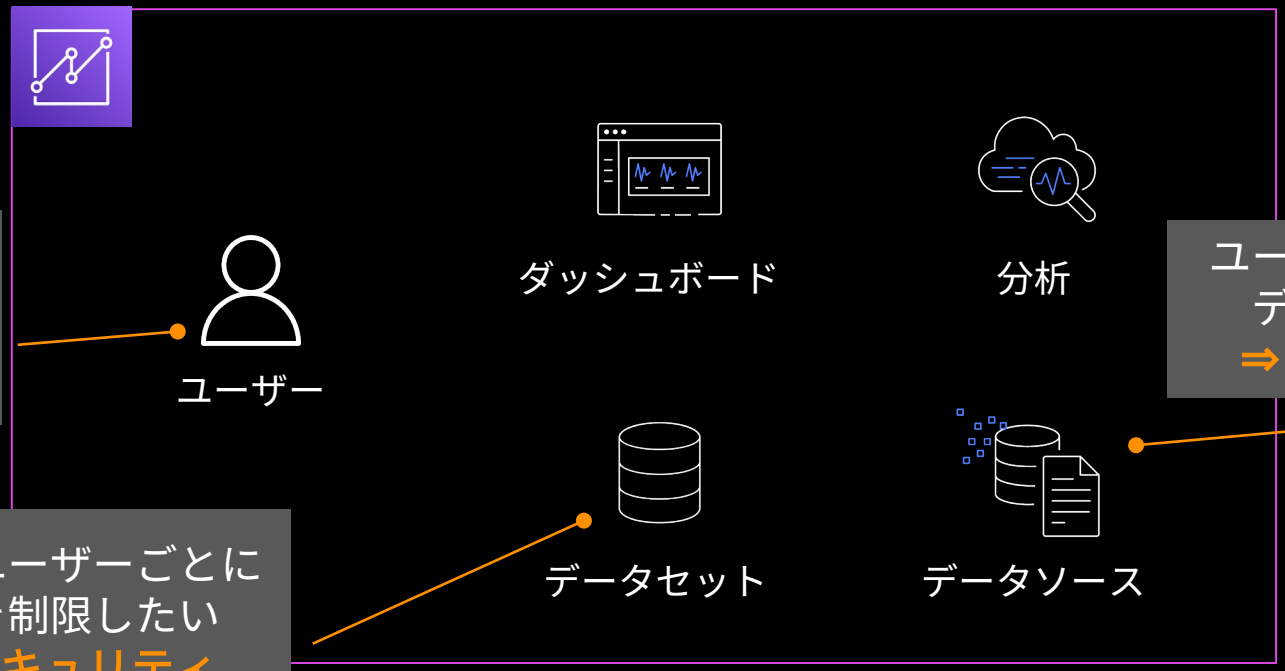
論理的なグループで名前空間（namespace）を分割し、ユーザーを名前空間で分離する。
分離された名前空間の間では互いに不可視となり、誤ったデータ共有を防ぐことができる。

とくに、個人情報を利用したり、複数社が共同で利用する場合などの厳密な管理が必要な場合に、
AWSアカウント自体を分けずともマルチテナンシーを実現できる。



ユーザーごとにアクセス可能なデータを制限したい

再掲）ユースケースの細分化



ユーザーごとにリソースへのアクセス権限を設定したい
⇒リソースの共有、マルチテナンシー

ユーザーごとにアクセス可能なデータソースを制限したい
⇒ スコープダウンポリシー

同じデータセットでも、ユーザーごとにアクセス可能なデータを制限したい
⇒行レベル/列レベルセキュリティ

ユーザーごとにアクセス可能なデータを制限したい

行レベル/列レベルセキュリティ

行レベルセキュリティ（RLS）と列レベルセキュリティ（CLS）を使用して、
データを共有する際に、特定の権限を持つユーザーのみにデータを参照させることができる。

いずれの場合も、既存のデータセットに加工を追加することなく、制限を加えることが可能。

	行レベルセキュリティ	列レベルセキュリティ
ユースケース	売上管理のダッシュボードで 担当エリアのデータのみを 参照できるようにする。	売上管理のダッシュボードで 営業部門のみが売上を 参照できるようにする。

イメージ

Customer	Prefecture	Sales
001	Tokyo	100
002	Tokyo	200
003	Saitama	300

PrefectureがTokyoのみ参照可能

Customer	Prefecture	Sales
001	Tokyo	100
002	Tokyo	200
003	Saitama	300

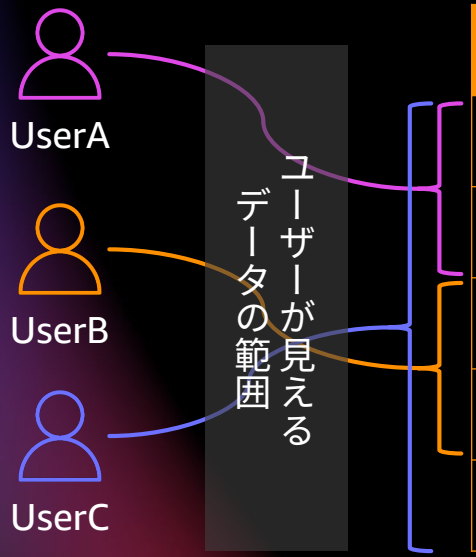
Sales列は参照不可

ユーザーごとにアクセス可能なデータを制限したい

行レベルセキュリティの実現方法

行レベルセキュリティは、制限対象のデータセットとは別に**権限データセット**を作成する。

権限データセットではユーザー名やグループ名に加えてアクセス許可を行う列を定義し、
アクセス許可を行う列に、カンマ区切りで許可する値を設定する。



制限対象のデータセット

Customer	Prefecture	Sales
001	Tokyo	100
002	Tokyo	200
003	Saitama	300
004	Chiba	100
005	Kanagawa	200

権限データセット

UserName	Prefecture
UserA	Tokyo
UserB	Saitama,Chiba
UserC	

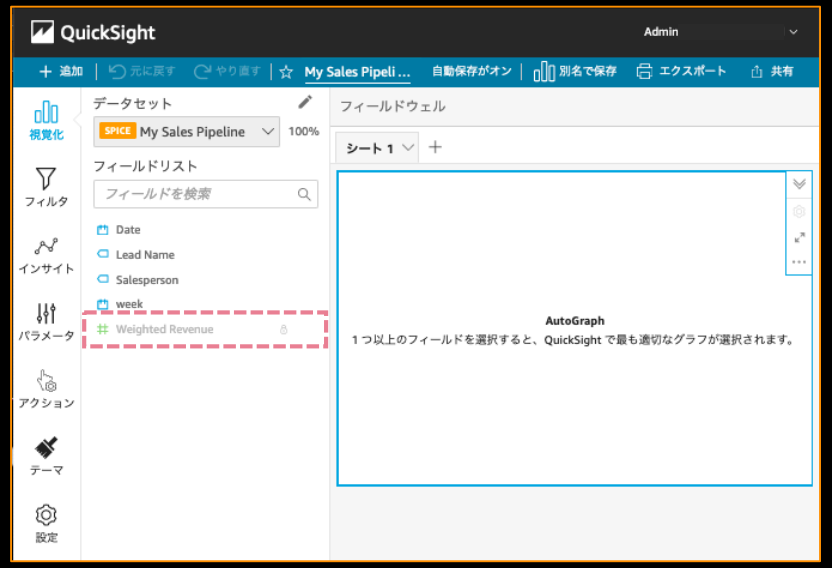
アクセス許可を行う列が空の場合
すべてのデータを許可する。

ユーザーごとにアクセス可能なデータを制限したい

列レベルセキュリティの実現方法

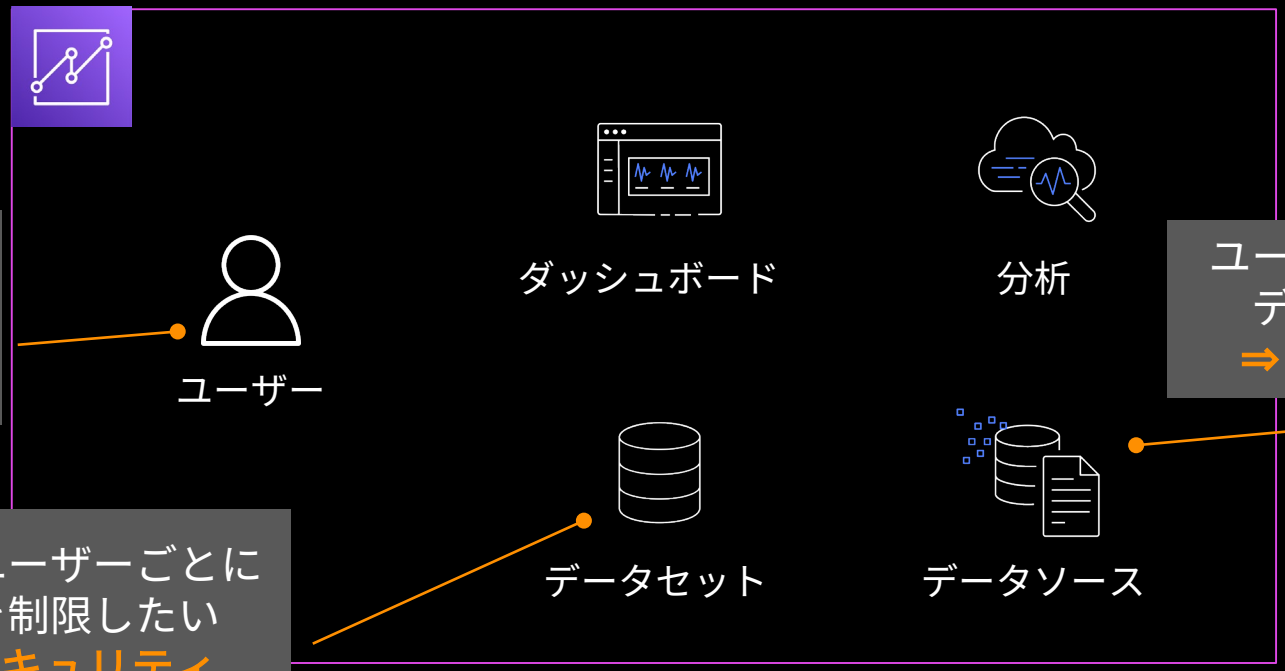
データセットの設定で、列ごとに権限を与えるユーザー、グループを選択する。

権限を持たないユーザーが、そのデータセットを分析で使おうとしても選択できない。
ダッシュボード上で参照した場合、"Not Authorized"と表示される。



ユーザーごとにアクセス可能なデータを制限したい

再掲）ユースケースの細分化



ユーザーごとにリソースへのアクセス権限を設定したい
⇒リソースの共有、マルチテナンシー

ユーザーごとにアクセス可能なデータソースを制限したい
⇒ スコープダウンポリシー

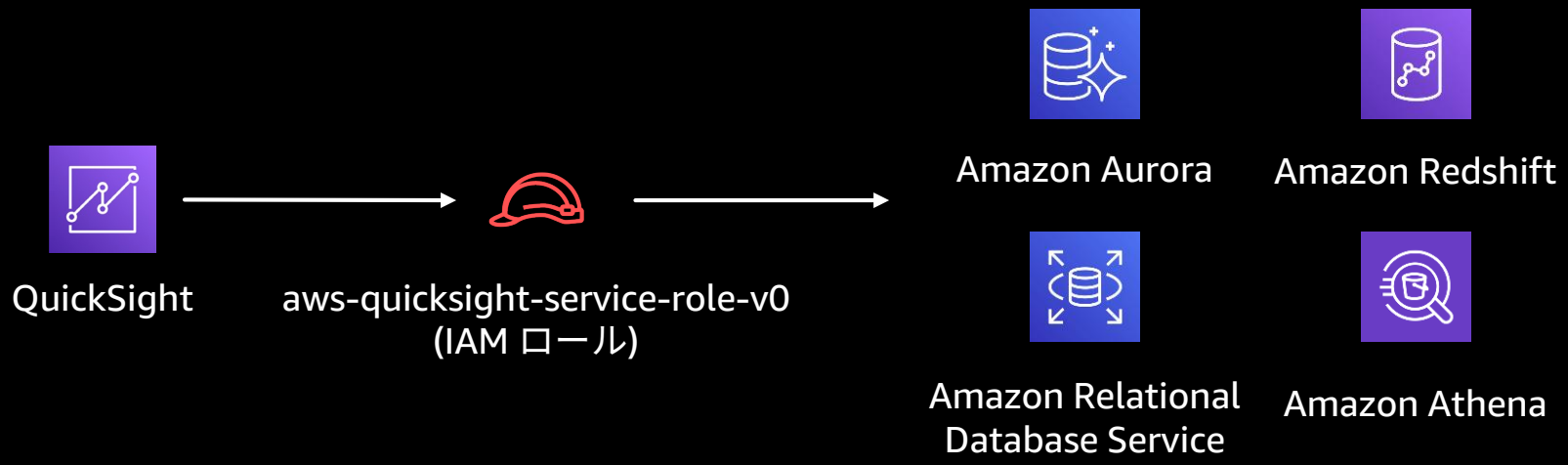
同じデータセットでも、ユーザーごとにアクセス可能なデータを制限したい
⇒行レベル/列レベルセキュリティ

ユーザーごとにアクセス可能なデータを制限したい

QuickSight が利用する IAM ロール

データへのアクセス時に QuickSight が利用する AWS リソースへのアクセス権限は、
サインアップ時に自動で作成される IAM ロール(aws-quicksight-service-role-v0) で管理される。

権限を変更する場合は、このIAMロールやIAMポリシーを直接変更するのではなく、
QuickSightの管理画面（セキュリティとアクセス権限）から調整する。



ユーザーごとにアクセス可能なデータを制限したい

QuickSightのセキュリティ設定機能(管理画面)

①ではこのアカウントで利用するサービス一覧を定義 する
②「すべてのAWSのデータおよびリソースのアクセスをすべてのユーザーに許可する」が
　デフォルト値である。これを「拒否する」にして、③で詳細設定することが可能
③IAMポリシーを割り当て、アクセス制御(Fine-Grained Access Control)を定義する

①QuickSightがアクセスできるリソースを定義。
ここに定義されないサービスは データソースとして利用できない。
（aws-quicksight-service-role-v0に変更が反映される）

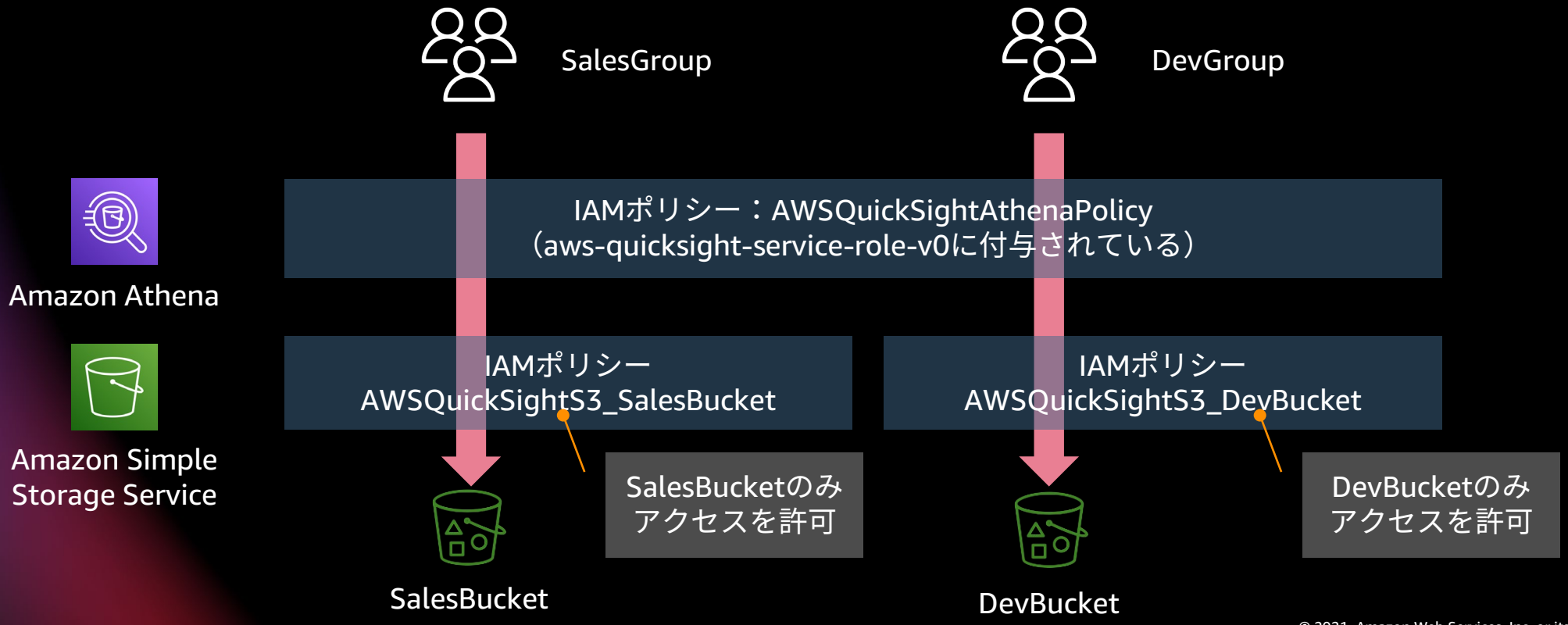
②ユーザー/グループのデフォルトのリソースアクセス方法を選択

③ユーザー/グループが接続するアクセスポリシーを
　IAMポリシー（スコープダウンポリシー）を用いて設定

ユーザーごとにアクセス可能なデータを制限したい

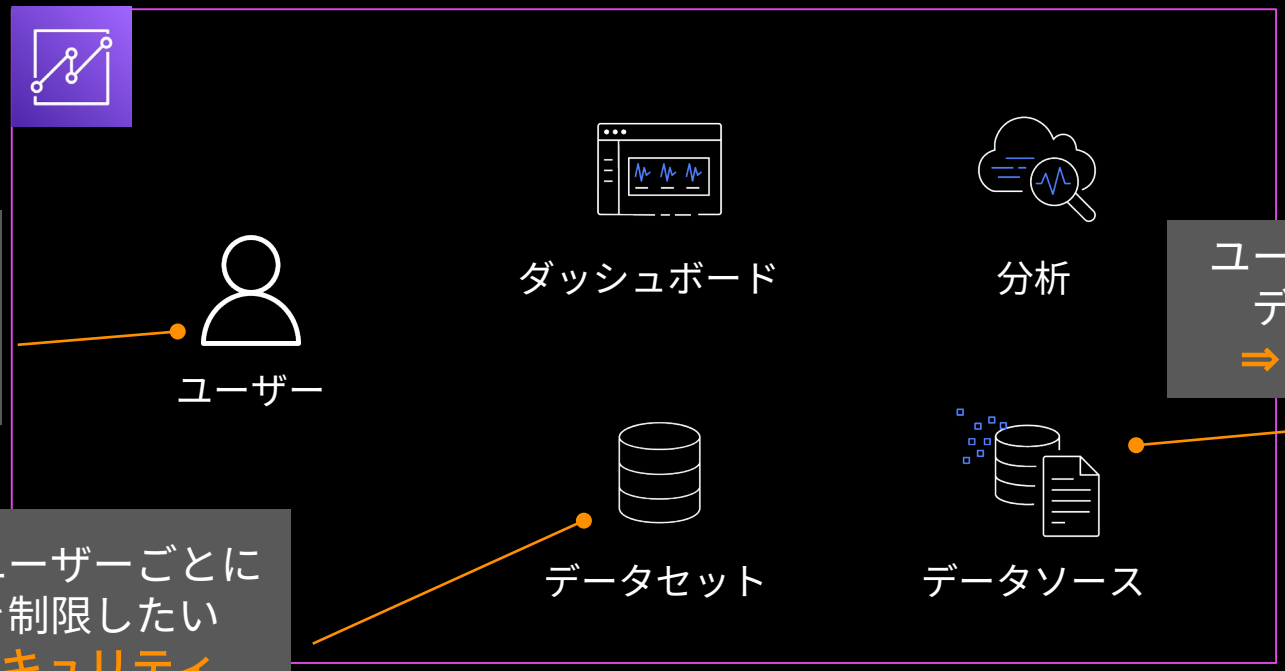
スコープダウンポリシーによるアクセス制御

IAMポリシー（スコープダウンポリシー）により、特定のS3バケットには特定のグループのみしかアクセスできないよう制限することが可能。
設定したポリシー以上の権限を有さないため、データセットを誤って共有した場合にもデータの参照ができない。



ユーザーごとにアクセス可能なデータを制限したい

再掲）ユースケースの細分化



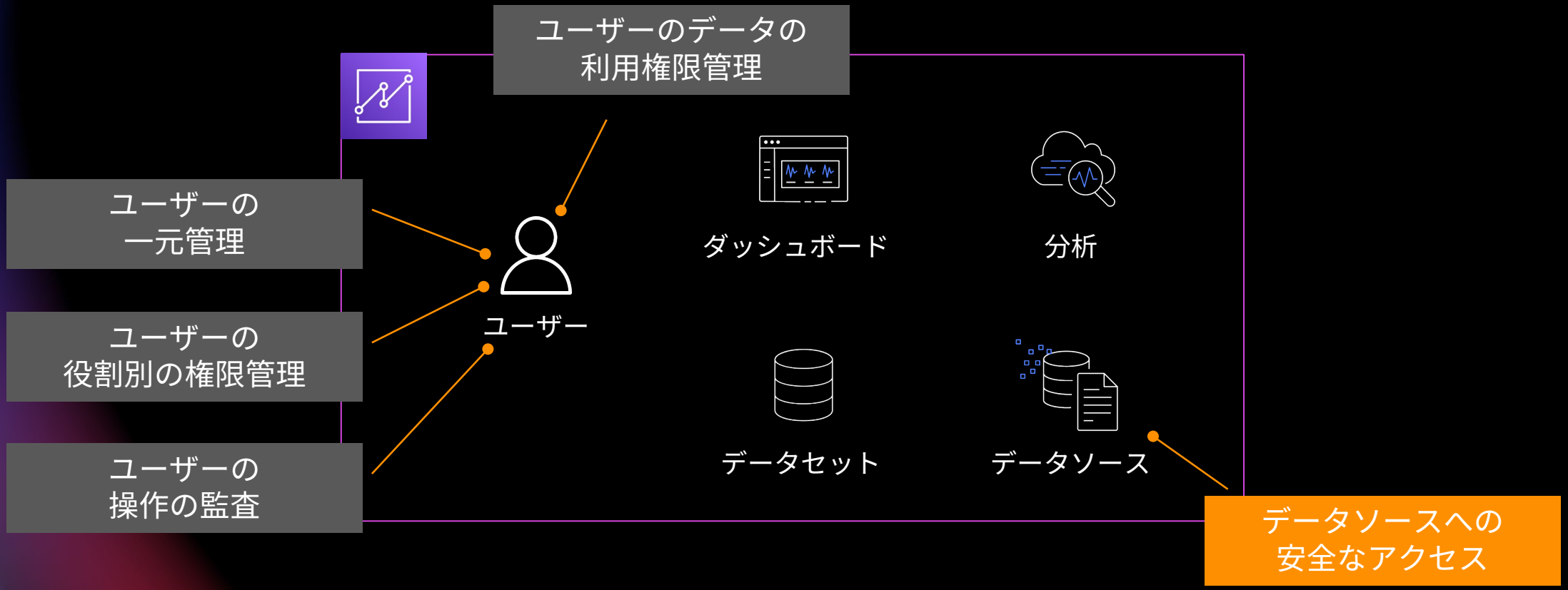
ユーザーごとにリソースへのアクセス権限を設定したい
⇒リソースの共有、マルチテナンシー

ユーザーごとにアクセス可能なデータソースを制限したい
⇒ スコープダウンポリシー

同じデータセットでも、ユーザーごとにアクセス可能なデータを制限したい
⇒行レベル/列レベルセキュリティ

QuickSightで実現可能なセキュリティ対策

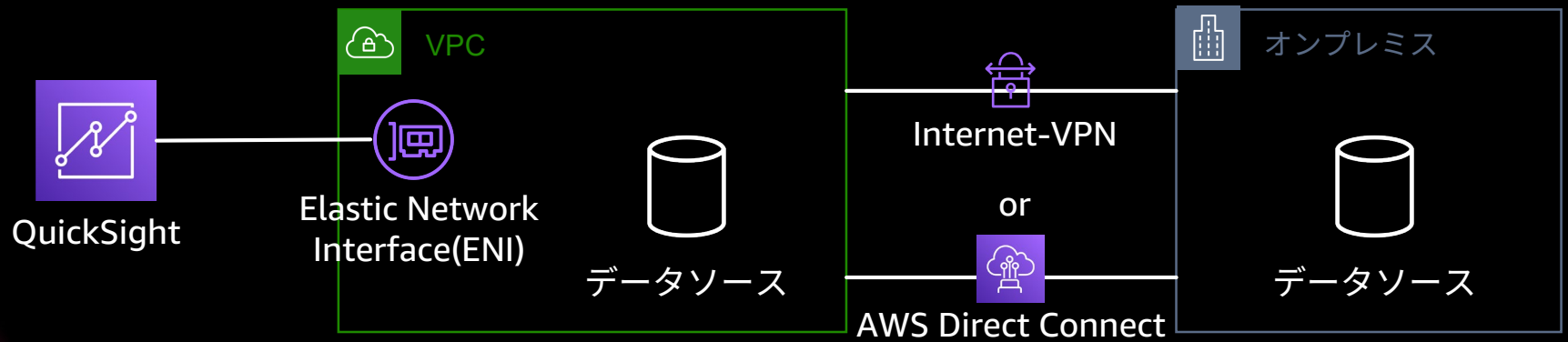
QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



安全にデータソースにアクセスさせたい

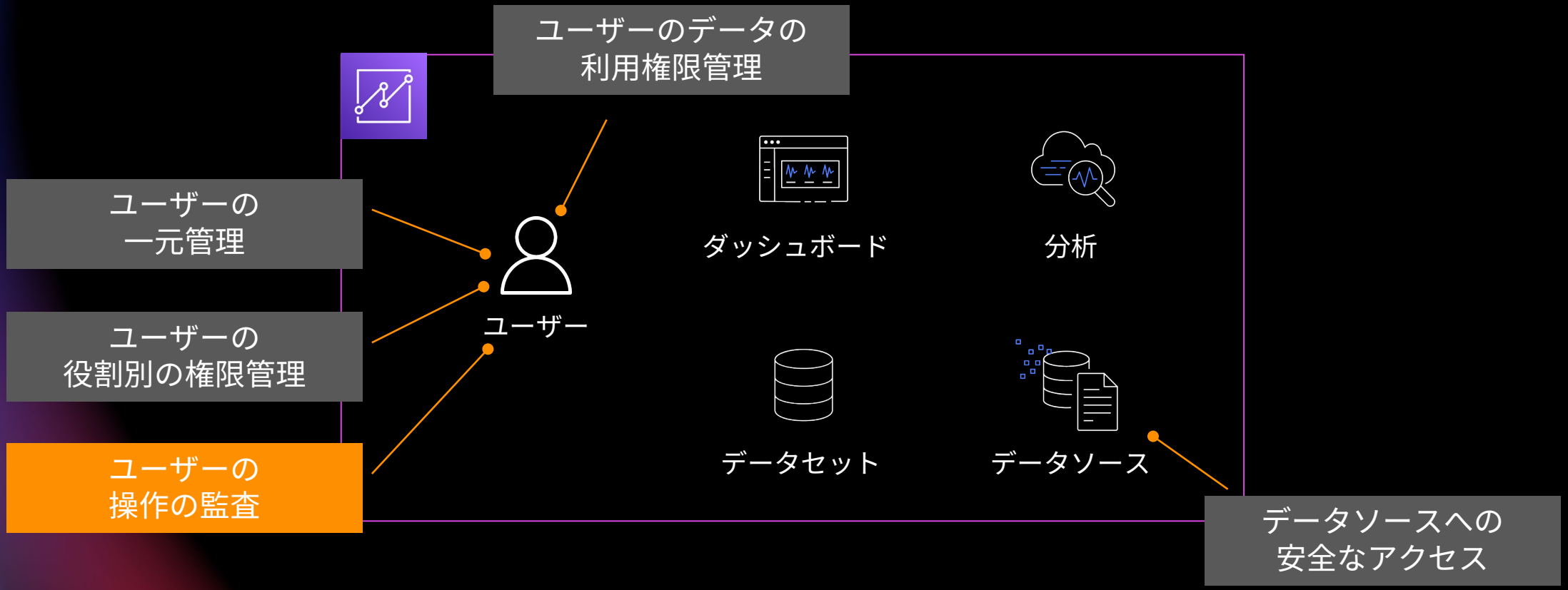
QuickSight からの、VPC（Virtual Private Cloud）内のデータソースや VPC と接続した
オンプレミスのデータソースへのアクセスは、セキュアなネットワーク内に閉じることができる。

QuickSight で指定した VPC 内に Elastic Network Interface (ENI)を作成し、
データソースへのアクセスは ENI を介するため、データソースをパブリックに公開する必要が無い。



QuickSightで実現可能なセキュリティ対策

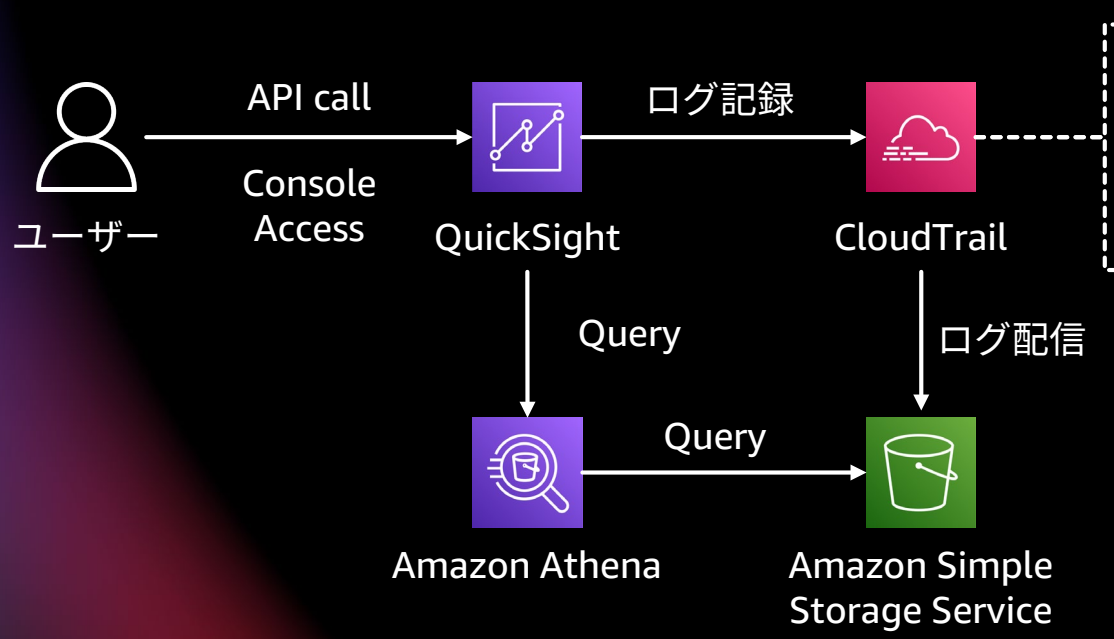
QuickSight自身が持つ機能や他のAWSサービスと連携することで、高度なセキュリティを実現可能。



ユーザーの操作ログを保管したい

QuickSight は AWS CloudTrail と統合されており、
QuickSight API の呼び出しとQuickSight コンソールでの操作が記録される。

Amazon Simple Storage Service（S3）へログを配信して監査ログとして保管することもでき、
Amazon Athenaでログデータをクエリし、利用状況の把握に利用可能。



EventType = AwsApiCall

QuickSight の **API 呼び出し**
例）AWS Command Line Interfaceを用いた
ユーザー追加

EventType = AwsServiceEvent

QuickSight の **API 呼び出し以外**の操作
例）QuickSight のコンソールでの分析の表示

まとめ

- ユーザーを一元管理したい場合は、IAM+IdPを用いてSSOを提供する。
- 役割ごとに権限管理を実施したい場合、ユーザーごとに適切なロールを割り当て、必要であればカスタムパーミッションで権限を制限する。
- ユーザーごとにアクセス可能なデータを制限したい場合は、グループ、マルチテナンシー、行レベル/列レベルセキュリティ、スコープダウンポリシーを利用する。
- データソースへのアクセスをセキュアに行いたい場合は、VPC接続の機能でデータソースとのプライベートな接続を確立する。
- ユーザーの操作ログを保管したい場合は、CloudTrailのログを保管する。

ご清聴ありがとうございました