



AWS BLACK BELT ONLINE SEMINAR

AWS Lake Formation

基礎編

佐藤 祥多 (Shota Sato)

Analytics Specialist Solution Architect

AWS Black Belt Online Seminar とは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾンウェブサービスジャパン合同会社が提供するオンラインセミナーシリーズです
- AWS の技術担当者が、AWS の各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
- <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>

内容についての注意点

- 本資料では 2023 年 09 月時点のサービス内容および価格についてご説明しています。最新の情報は AWS 公式ウェブサイト (<https://aws.amazon.com/>) にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格と AWS 公式ウェブサイト記載の価格に相違があった場合、AWS 公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっております。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

名前：佐藤 祥多 (Shota Sato)

所属：アマゾンウェブサービスジャパン
アナリティクス事業本部
ソリューションアーキテクト本部
アナリティクスソリューションアーキテクト

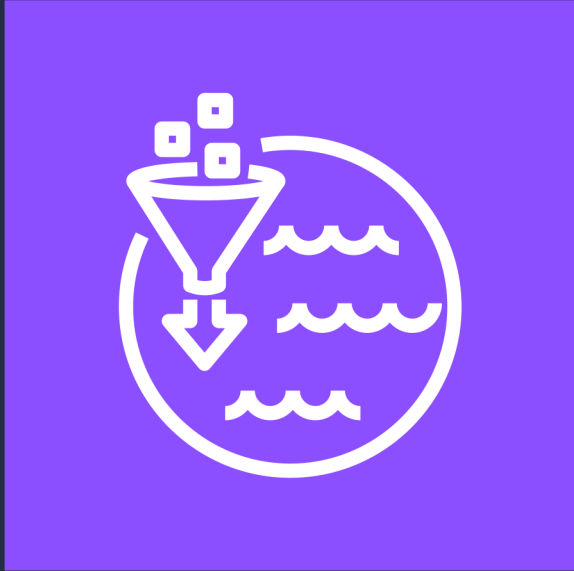
好きなAWSサービス：
AWS Lake Formation, Amazon DataZone, AWS Glue



アジェンダ

- AWS Lake Formation の概要
- AWS Lake Formation の機能
 - アクセス制御の概要と機能
 - ブループリントの概要と機能
 - データ共有の概要と機能
- AWS Lake Formation の料金
- まとめ

AWS Lake Formation の 概要



AWS Lake Formation

安全なデータレイクを簡単に作成し
幅広い分析にデータを利用可能にする



使い慣れたデータベースのような機能を使用して、データレイクをすばやく作成、管理、保護



大規模なセキュリティ管理とガバナンスを簡素化し、データレイク全体できめ細かなアクセス許可が可能



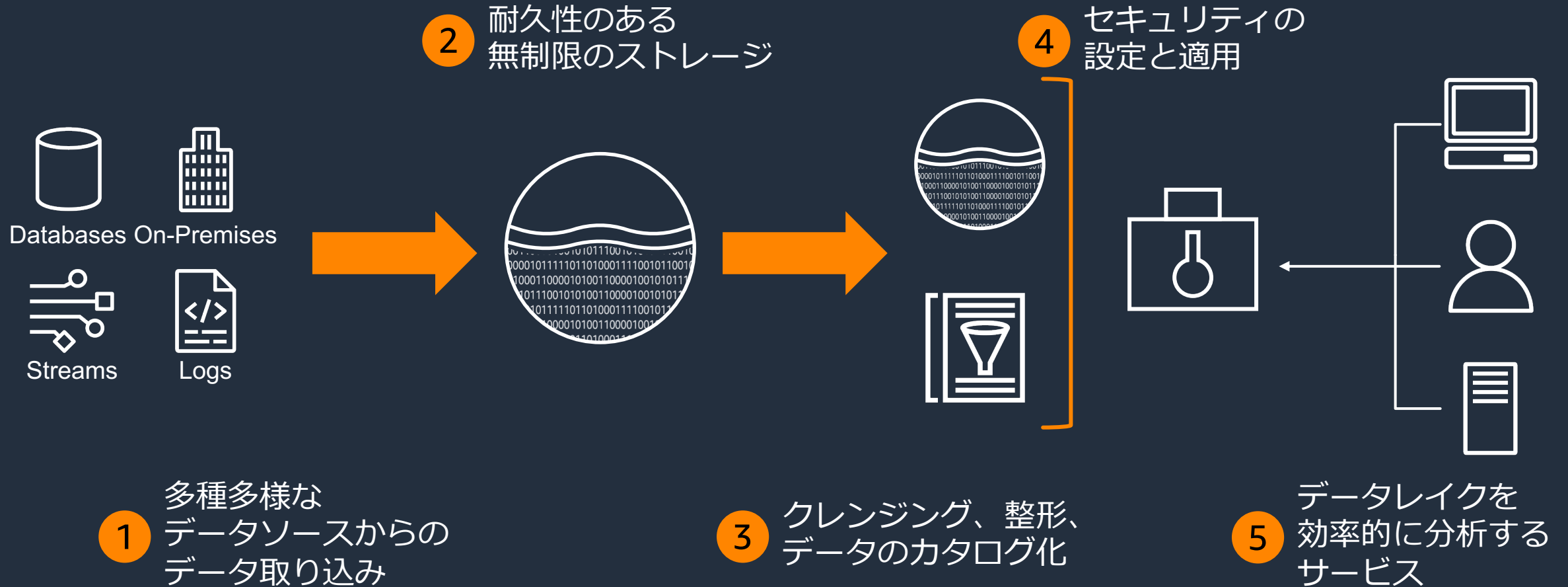
一元化されたデータカタログですべてのデータを検出、アクセス



クロスアカウントデータ共有により、組織全体のデータアクセスをサポート

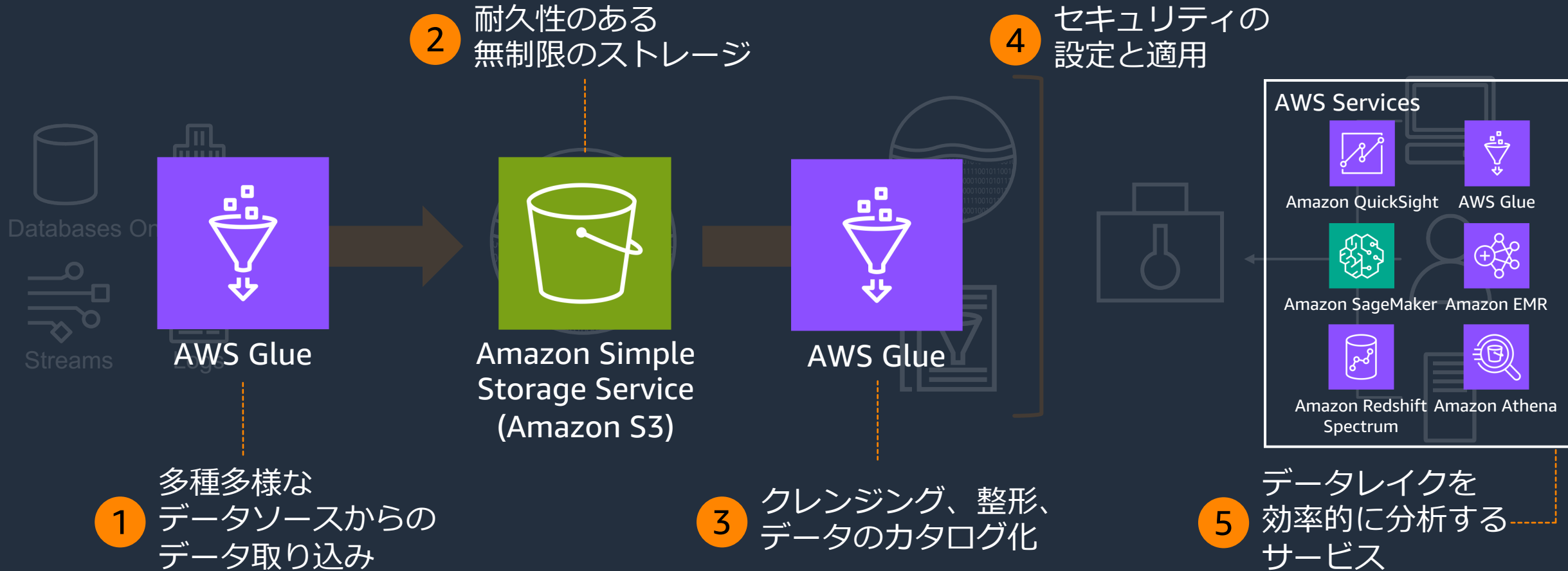
データレイクを作るためには

数多くの考慮事項があり、それぞれ適切な対応が必要



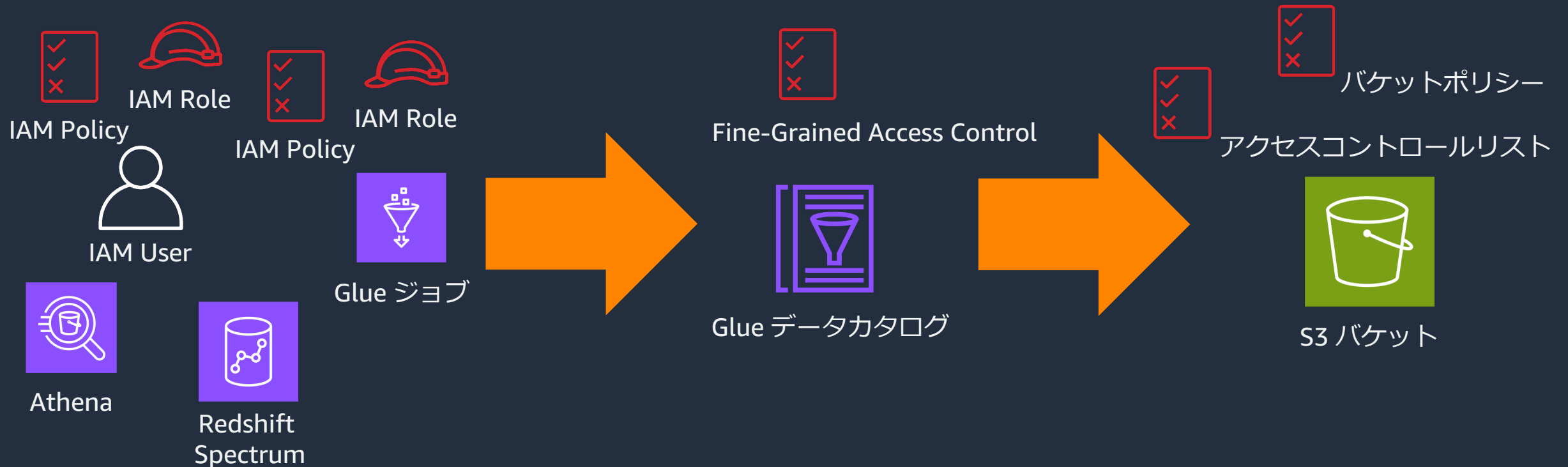
安全なデータレイクを作るための AWS のソリューション

それぞれの考慮事項に対して AWS では様々なソリューションを提供



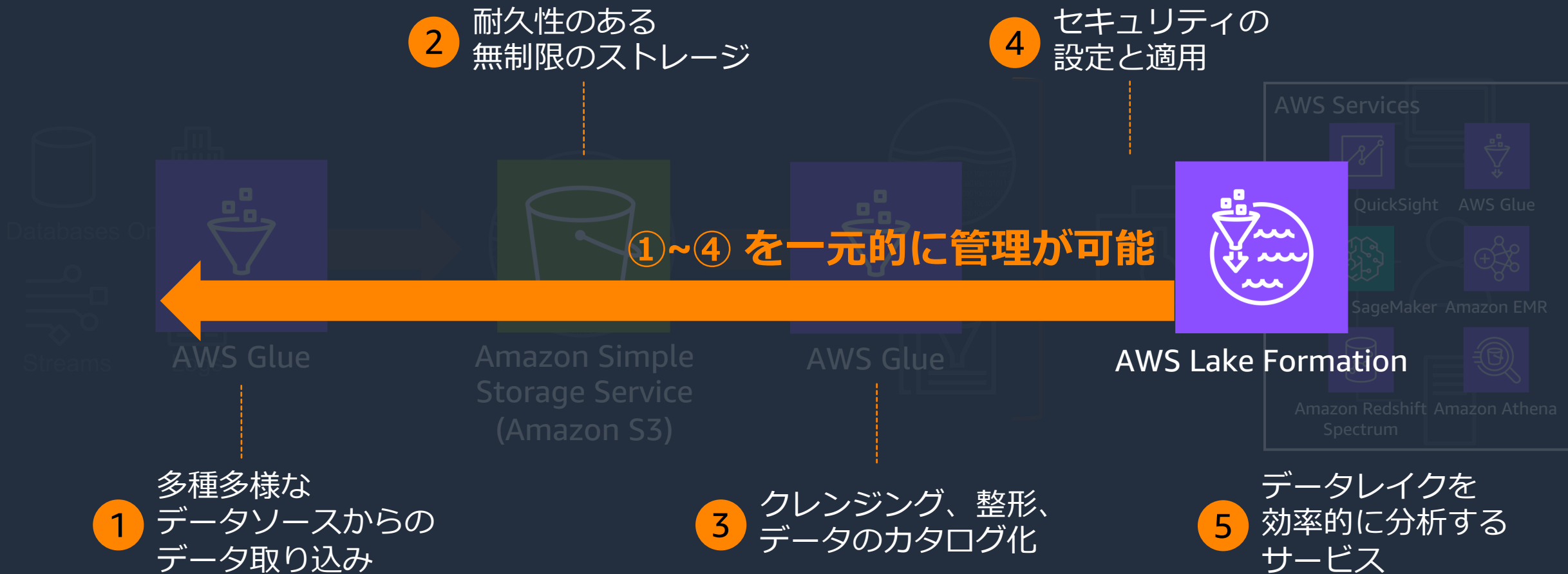
従来のデータレイク認可の課題

IAMポリシーとバケットポリシーなどを複数の異なる箇所にポリシーを登録する必要があり、管理が煩雑だった



AWS Lake Formation の導入効果

データレイクへのデータ取り込みからセキュリティの設定/適用を一元的に実施可能



AWS Lake Formation の主要な機能

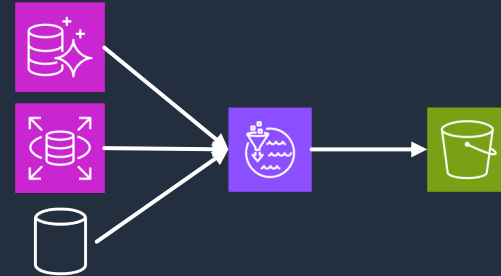
安全なデータレイクを簡単に作成するために Lake Formation には3つの主要機能がある



一元管理による 細かな粒度のアクセス制御

データレイク管理者が AWS サービスの S3 へのアクセスを一元的に制御

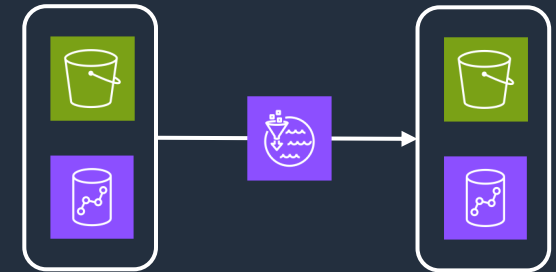
細かなアクセス制御に基づいて行レベル/列レベル/セルレベルのセキュリティを実現



ブループリント機能を利用 したデータの取り込み

Glue の Connection を利用して様々なデータソースからデータレイクにデータ取り込み

洗い替えだけでなく増分的なデータ取り込みにも対応

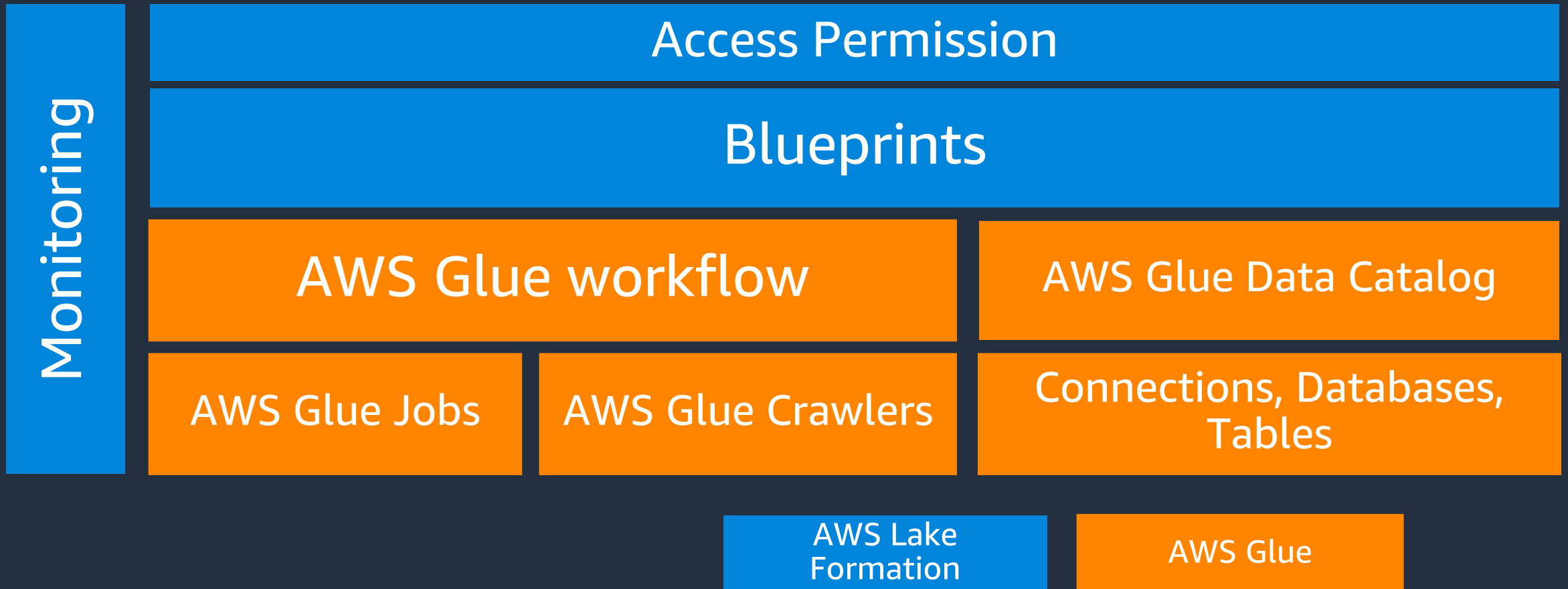


安全なデータ共有の制御

S3 のデータレイクや Redshift のデータを安全に別 AWS アカウントや別リージョンに共有し制御可能

補足 : AWS Lake Formation と AWS Glue の関係

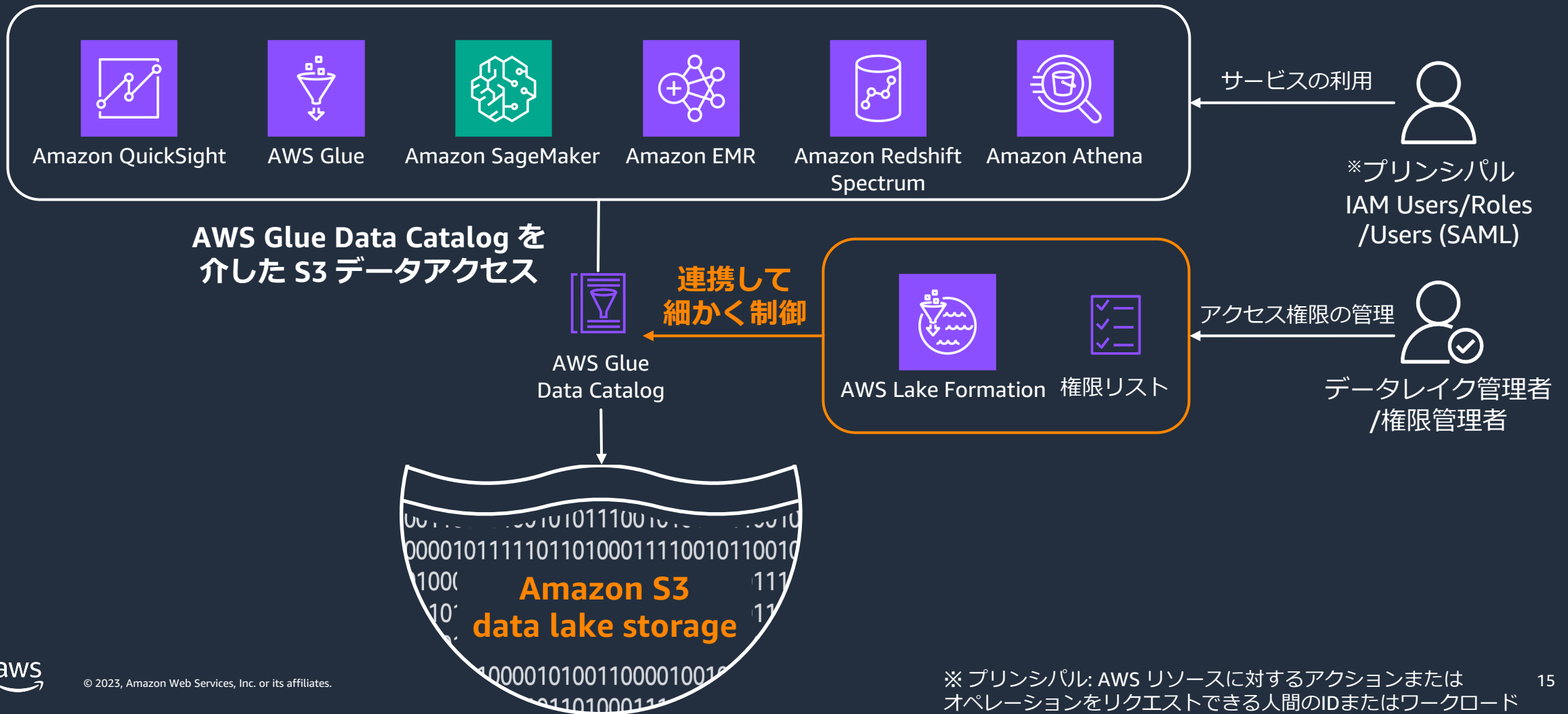
AWS Lake Formation は AWS Glue の拡張機能と言え、Glue Data Catalog へのセキュリティ強化やブループリントによるデータ取り込み等、データレイク構築に必要な機能を一元的に提供



AWS Lake Formation の機能 - アクセス制御の概要と機能

AWS Lake Formation のアクセス制御の全体像

AWS Lake Formation は AWS Glue Data Catalog を介した Amazon Simple Storage Service (S3) へのアクセスを細かな粒度で制御する



AWS Lake Formation を利用する際のユーザーロール

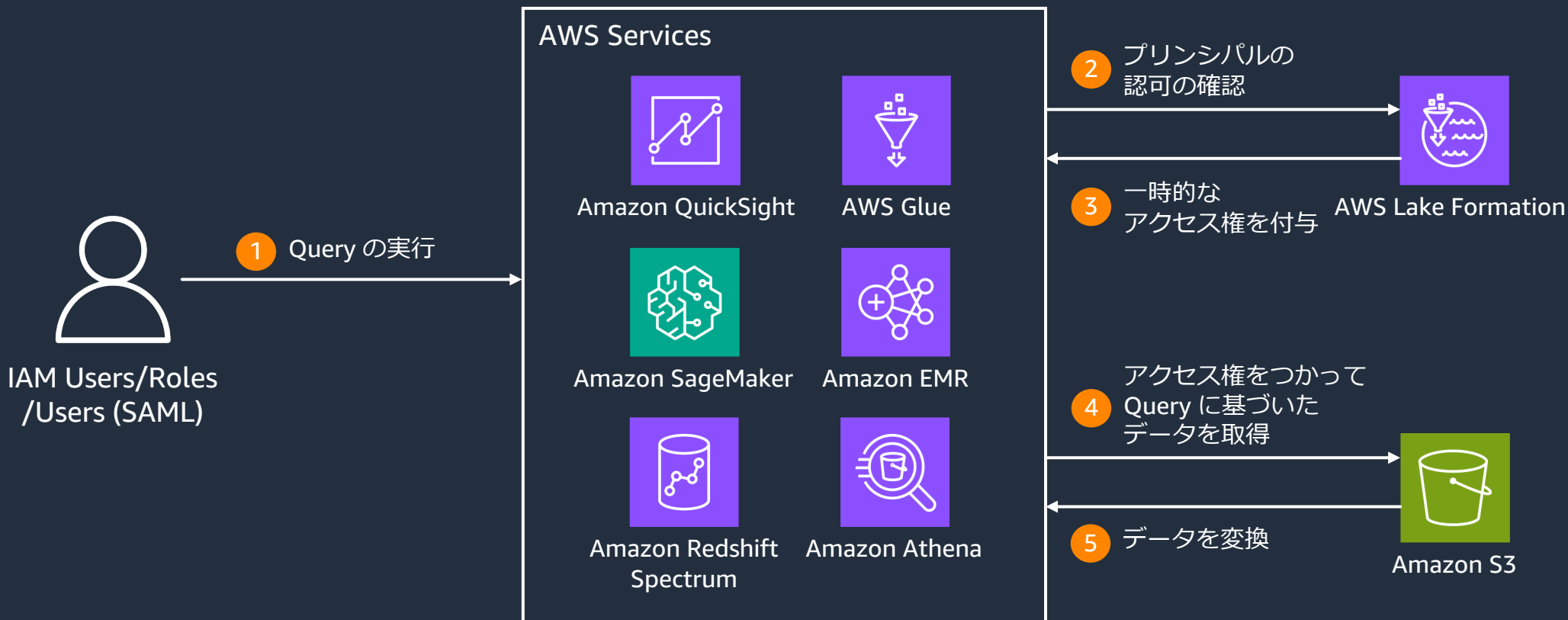
アクセス制御を管理するためにはユーザのロールを整理すると良い。Lake Formation の利用では3つのロールに分類できる



- データレイクの構築/管理を行う
- あらゆるリソースやデータロケーションへのアクセス許可を他のプリンシパルに付与可能
- アクセス許可の付与を行う許可を他のプリンシパルに付与可能で権限管理者に権限付与権限を付与する
- アクセス権限を管理する
- データレイク管理者から付与された権限付与権限を利用して利用者へアクセス権限を付与する
- データレイクを利用する

アクセス制御の裏側

AWS Glue Data Catalog を介した S3 へのアクセスが発生すると、AWS Lake Formation は AWS サービスに一時的な認証情報を返して、サービスはその一時的な認証情報をつかって S3 にアクセスする



アクセス制御の対象となる S3 パスの登録

AWS Lake Formation は事前に登録された S3 パスの配下にあるリソースのみアクセス制御を行うため、事前に Glue Data Catalog のリソースがポイントする S3 パスを登録する必要がある

Register location

Amazon S3 location
Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path
Choose an Amazon S3 path for your data lake.
e.g.: s3://bucket/prefix/ Browse

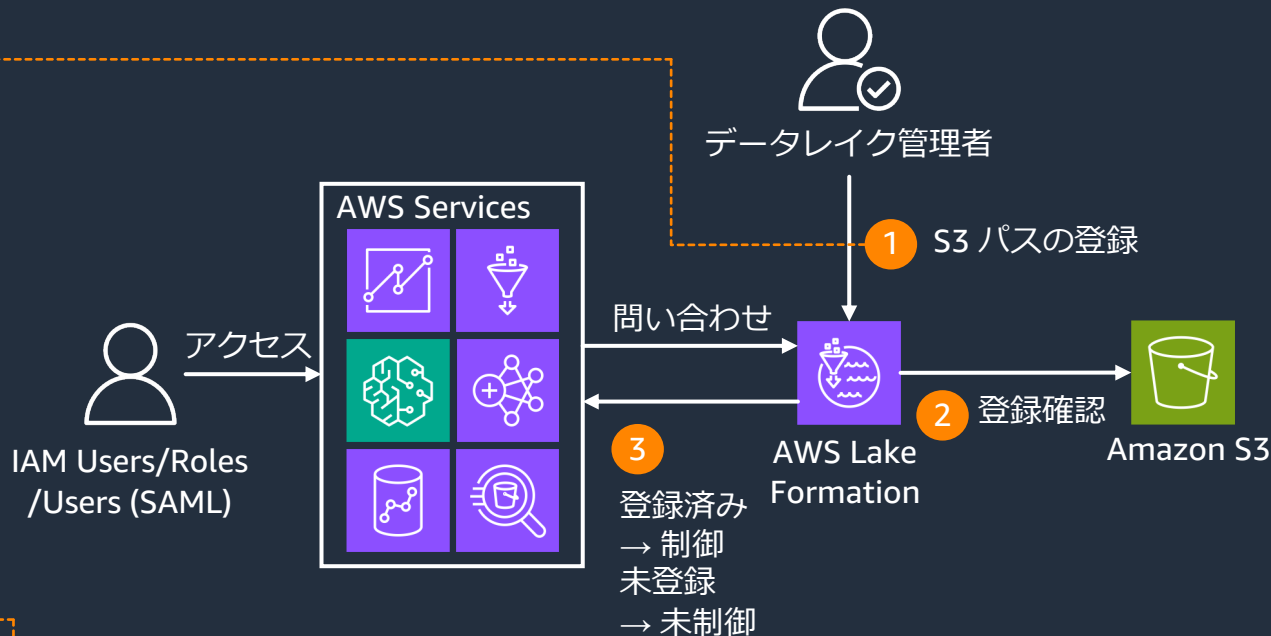
Review location permissions - strongly recommended
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.
Review location permissions

IAM role
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.
AWSServiceRoleForLakeFormationDataAccess

Do not select the service linked role if you plan to use EMR.

Enable Data Catalog Federation
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Cancel Register location



- Lake Formation が S3 に write/read を行うための IAM ロールを指定する
- `AWSServiceRoleForLakeFormationDataAccess` がデフォルトで指定されている

AWS Lake Formation のアクセス制御対象

AWS Lake Formation は AWS Glue Data Catalog に対するメタデータのアクセス制御と Amazon S3 ロケーション内のデータへのアクセス制御を行っている



- **プリンシパルが Glue Data Catalog のメタデータにアクセスする権限を制御**
- [Data lake permissions] から設定可能
- IAM Principals/SAML/External Accounts に Glue Data Catalog の DB/Table への **CRUD + 参照 (Describe)** 権限を付与
- **プリンシパルが S3 をポインタする Glue Data Catalog のメタデータを作成/変更する権限を制御**
- [Data locations] から設定可能
- IAM Principals/SAML/External Accounts に Glue Data Catalog がポイントする S3 リソースへの **CREATE_TABLE/ALTER** 権限を付与

各権限で必要なアクセス制御

各権限で必要なアクセス制御は以下の通り

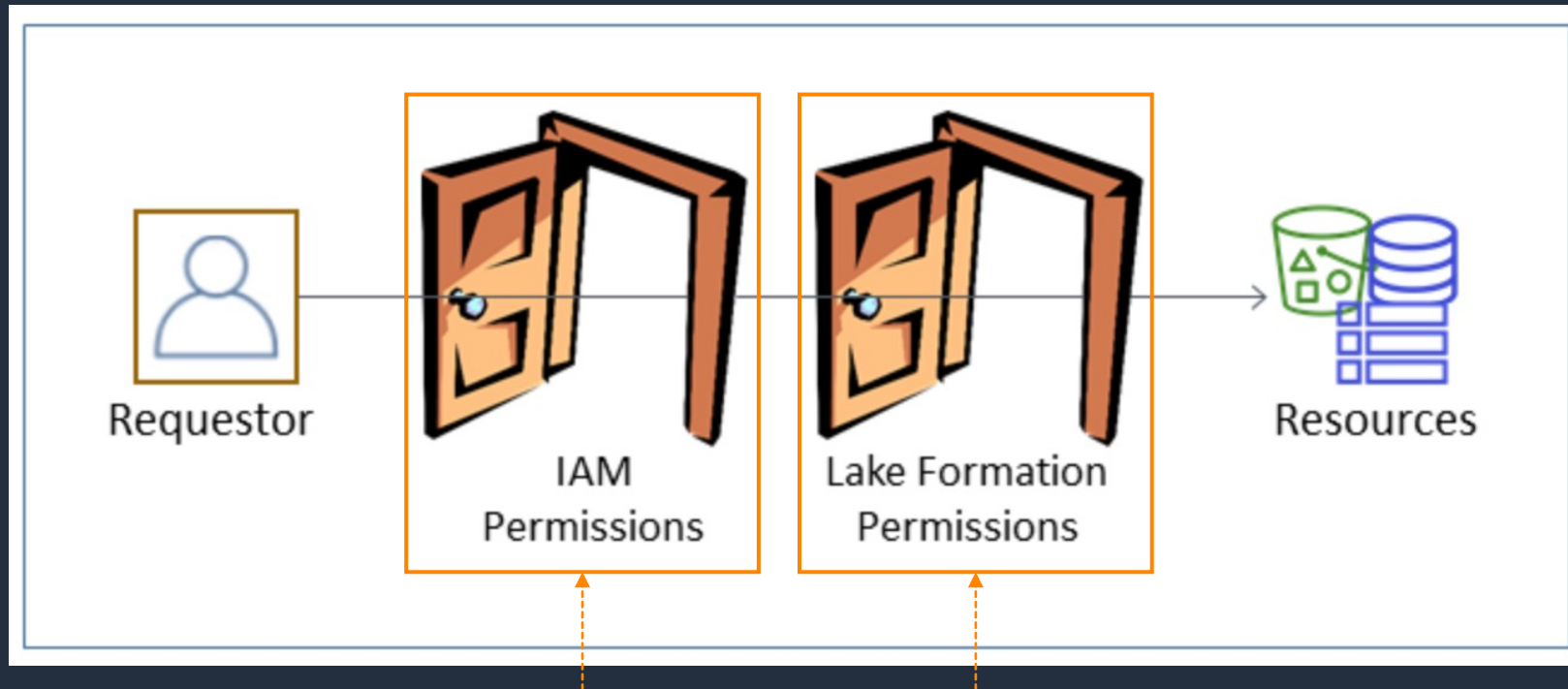
種別	権限	メタデータのアクセス権の要否	ロケーションのアクセス権の要否
DB	Create Table	○	○
	Alter	○	○
	Drop	○	×
	Describe	○	×
Table	Select	○	×
	Insert	○	×
	Delete	○	×
	Describe	○	×
	Alter	○	○
	Drop	○	×

Create Table/Alter はメタデータのアクセス権だけでなくロケーションのアクセス権が必要

※ データレイク管理者はアクセス制御対象となる
S3 パスに対するロケーションアクセス権をデフォルトで所持してる

補足 : IAM と AWS Lake Formation の制御の関係

AWS Lake Formation によるアクセスの制御は IAM による制御の後に行われる。そのため Lake Formation による細かな制御を行うには、まず IAM による制御を荒くする必要がある



以下のような荒い粒度の制御を IAM では行う

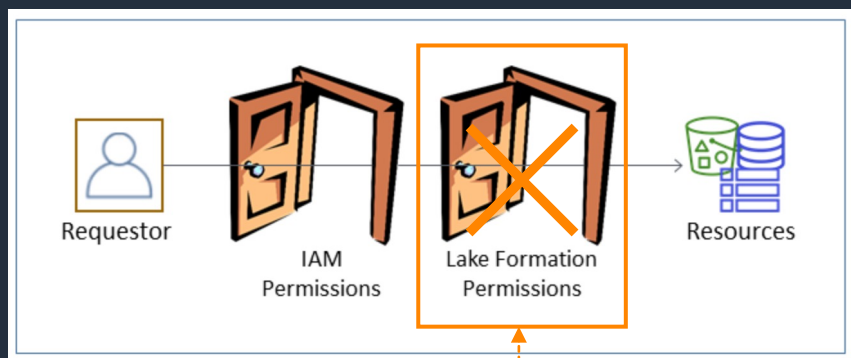
- "athena:*": 利用する AWS サービスの権限
- "glue:*": Glue Data Catalog の操作権限
- "lakeformation:*" Lake Formation の操作権限

Lake Formation 上で Glue Data Catalog へ細かなアクセス制御を行う

補足 : IAMAllowedPrincipals

AWS Lake Formation は IAM による制御を妨げないような設定がデフォルトで行われており、それが IAMAllowedPrincipals による設定である

IAMAllowedPrincipals



- ここを無効化する仕組みが IAM Group: IAMAllowedPrincipals による制御
- **IAMAllowedPrincipals には IAM Policy で Glue Data Catalog へのアクセスが許可されている IAM User/Role が全て含まれる**
- Lake Formation はデフォルトで IAMAllowedPrincipals に Glue Data Catalog の DB/Table 両方に Super 権限を付与する

Lake Formation の初期設定

[AWS Lake Formation](#) > Data catalog settings

Data catalog settings

Default permissions for newly created databases and tables
These settings maintain existing AWS Glue Data Catalog behavior. You can still set individual permissions on databases and tables, which will take effect when you revoke the Super permission from IAMAllowedPrincipals. See [Changing Default Settings for Your Data Lake](#).

- Use only IAM access control for new databases **IAMAllowedPrincipals に新しく作られた DB への Super 権限を付与する**
- Use only IAM access control for new tables in new databases **IAMAllowedPrincipals に新しく作られた Table への Super 権限を付与する**

Database creators (2)

Choose IAM principals permitted to create databases in your AWS Glue Data Catalog.

Find database creators

Principal	Principal type	Permissions
<input type="radio"/> IAMAllowedPrincipals	Group	Create database

IAMAllowedPrincipals Glue Data Catalog で DB を作る権限を付与する

アクセス制御を始めるためには

※ 設定ドキュメントのリンク

※ 設定ドキュメントのリンク

AWS Glue Data Catalog にリソースがない場合とある場合で開始方法が異なる。
ある場合は IAMAllowedPrincipals の設定をリソースから排除する必要があるが、ない場合
含めて基本的な流れは次の通り

1. データレイク管理者用の IAM User/Role の設定
 - Lake Formation を管理するのに必要な IAM Policy の設定をする
2. デフォルトの許可モデルを変更
 - IAMAllowedPrincipals の設定を排除する
3. データレイク用の Amazon S3 ロケーションを設定
 - S3 パスを Lake Formation に登録する
4. データロケーションのアクセス制御を設定
 - S3 へのロケーションアクセス制御の設定をする
5. メタデータのアクセス制御を設定
 - Glue Data Catalog のメタデータへのアクセス制御の設定をする

1. データレイク管理者用の IAM User/Role の設定

データレイク管理者は S3 ロケーションの登録と Lake Formation 上でアクセス制御を管理する。IAM に然るべき Policy を付与した後、Lake Formation 上のコンソールで設定をする

1. 必要な IAM (マネージド) ポリシー

- 必須
 - AWSLakeFormationDataAdmin
 - サービスリンク用インラインポリシー
- オプション
 - AWSGlueConsoleFullAccess
 - CloudWatchLogsReadOnlyAccess
 - Glue を使う場合
 - AWSLakeFormationCrossAccountManger
 - クロスアカウント共有を使う場合
 - AmazonAthenaFullAccess
 - Athena を使う場合

2. データレイク管理者の登録

The screenshot shows the 'Add administrators' dialog in the AWS IAM console. It is divided into three main sections: 'Access type', 'IAM users and roles', and 'Active Directory and Amazon QuickSight users and groups, and federated users'. In the 'Access type' section, the 'Data lake administrator' radio button is selected. The 'IAM users and roles' section includes a dropdown menu labeled 'Choose IAM principals to add' and a note that up to 30 administrators can be added. The 'Active Directory and Amazon QuickSight users and groups, and federated users' section contains a text input field with an example ARN: 'arn:aws:iam::<AccountId>:saml-provider/<SamlProviderName>:user/<UserName>'. At the bottom right, there are 'Cancel' and 'Confirm' buttons.

- [Administrative roles and tasks] → [Data lake administrators] → [Add]
- IAM User/Role, SAML ユーザを登録する

2. デフォルトの許可モデルを変更

IAMAllowedPrincipals の影響を排除する

1. Data Catalog の設定を変更

Default permissions for newly created databases and tables

These settings maintain existing AWS Glue Data Catalog behavior. You can still set individual permissions on databases and tables, which will take effect when you revoke the Super permission from IAMAllowedPrincipals. See [Changing Default Settings for Your Data Lake](#).

Use only IAM access control for new databases

Use only IAM access control for new tables in new databases

- [Data catalog settings]
- チェックボックスをすべて外す
 - 外すと新しく作られる Glue Data Catalog の DB/Table で IAMAllowedPrincipals の設定が追加されなくなる

2. IAMAllowdPrincipals の Revoke

Database creators (2)

Choose IAM principals permitted to create databases in your AWS Glue Data Catalog.

Find database creators

Principal	Principal type	Permissions
<input type="radio"/> IAMAllowedPrincipals	Group	Create database

- [Administrative roles and tasks] → [Database creators] → [Revoke]
- IAMAllowedPrincipals から DB の作成権限を削除する

3. データレイク用の Amazon S3 ロケーションを設定する

Lake Formation で管理する S3 ロケーションと登録する

AWS Lake Formation > Data Lake Locations > Register location

Register location

Amazon S3 location
Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path
Choose an Amazon S3 path for your data lake.
e.g.: s3://bucket/prefix/

Review location permissions - strongly recommended
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

IAM role
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.

Do not select the service linked role if you plan to use EMR.

Enable Data Catalog Federation
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Permission mode
Select the permission mode you want to use to manage access.

Hybrid access mode - new
Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access. [Learn more](#)

Lake Formation
Only Lake Formation permissions are enforced.

- [Data lake locations] → [Register location]
- デフォルトのサービスリンクロールを IAM Role として指定する場合は p16 で作ったインラインポリシーがデータレイク管理者に必要

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "lakeformation.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy"
      ],
      "Resource": "arn:aws:iam::<account-id>:role/aws-service-
role/lakeformation.amazonaws.com/AWSServiceRoleForLakeFormationDataAccess"
    }
  ]
}
```

4. データロケーションのアクセス制御を設定

[Data locations] → [Grant] でプリンシパルに権限を付与する

AWS Lake Formation > Data locations

Data locations (5) Refresh Revoke Grant

Choose a storage location for which to review, grant or revoke user permissions.

Browse X

< 1 > Settings

	Principal ▲	Principal type ▼	Resource
<input type="radio"/>	AWSGlueServiceRole-Crawler	IAM role	s3://lakeformation-808127639386
<input type="radio"/>	datazone-usr-c-proj-armilxjqggev	IAM role	s3://datazone-proj-armilxjqggev-1692

Grant permissions X

Add access permissions for specific storage locations.

My account
User or role from this AWS account.

External account
AWS account, AWS organization or IAM principal outside of this account

IAM users and roles
Add one or more IAM users or roles.

Admin X
Role

Active Directory and Amazon QuickSight users and groups, and federated users
Enter an Active Directory ARN (EMR beta only), Amazon QuickSight ARN, or federated user ARN. Press Enter to add additional ARNs.

Storage locations
Choose one or more data lake locations.

Browse

Registered account location
The account where this storage location is registered in AWS Lake Formation.

Grantable

Cancel Grant

指定するのは Prefix のため
配下のリソース含めて
権限が付与される

5. メタデータのアクセス制御を設定

[Data lake permissions] → [Grant] でプリンシパルに権限を付与する

AWS Lake Formation > Permissions

Too many permissions? Filter by database or table. In the navigation page, choose **Databases** or **Tables**. Then choose a database or table, and on the **Actions** menu, choose **View Permissions**.

Data permissions (124) Refresh Revoke Grant

Filter permissions by property or value

	Principal ▲	Princip... ▼	Princip... ▼	Resourc... ▼	Database ▼	Table
<input type="radio"/>	Admin	IAM role	arn:aws:ia...	Database	lakeforma...	-
<input type="radio"/>	Admin	IAM role	arn:aws:ia...	Database	aurora_ex...	-
<input type="radio"/>	Admin	IAM role	arn:aws:ia...	Database	cleanrooms	-
<input type="radio"/>	Admin	IAM role	arn:aws:ia...	Database	redshift_s...	-
<input type="radio"/>	Admin	IAM role	arn:aws:ia...	Data locat...	-	-

AWS Lake Formation > Grant permissions

Grant data permissions

Principals

- IAM users and roles**
Users or roles from this AWS account.
- SAML users and groups**
SAML users and group or QuickSight ARNs.
- External accounts**
AWS account, AWS organization or IAM principal outside of this account

IAM users and roles
Add one or more IAM users or roles.
Choose IAM principals to add

LF-Tags or catalog resources

- Resources matched by LF-Tags (recommended)**
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.
- Named Data Catalog resources**
Manage permissions for specific databases or tables, in addition to fine-grained data access.

No LF-Tags selected
Add LF-Tag key-value pair
You can add 50 more LF-Tags.

Database permissions

Database permissions
Choose specific access permissions to grant.

Create table Alter Drop Super
This permission is the union of all the individual permissions to the left, and supersedes them.

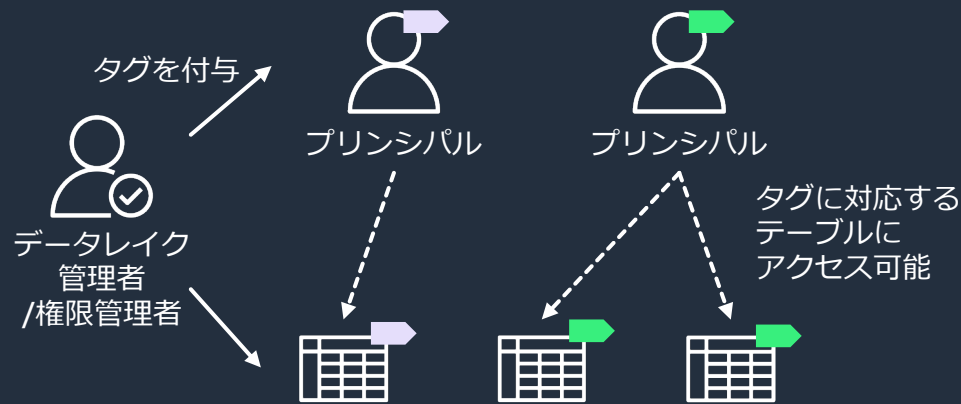
Grantable permissions
Choose the permission that may be granted to others.

Create table Alter Drop Super
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

メタデータアクセス制御方法の種類

メタデータのアクセス制御方法には LF Tag を使った方法とリソースを指定する方法の2種があり、それぞれ特徴がある

LF タグ 方式 (推奨)

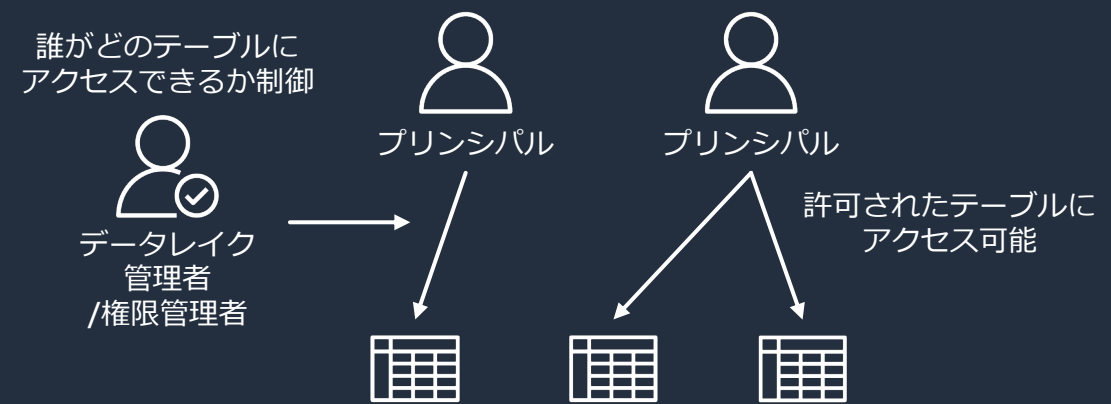


プリンシパルの数 + テーブルの数

- LF タグ : 列レベル

利用者とテーブルにそれぞれタグを付与するためスケールがしやすいがセキュリティは列レベルまで

リソース方式



プリンシパルの数 × テーブルの数

- シンプルな列フィルタリング : 列レベル
- データフィルタ : 行/列/セルレベル

利用者とテーブルの組み合わせに許可を付与するためスケールがしにくいがセキュリティは細かく制御可能

権限制御の数

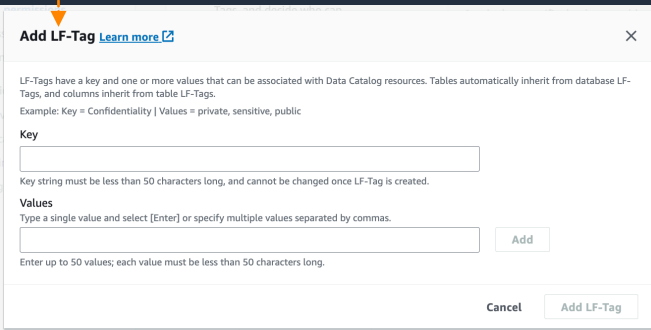
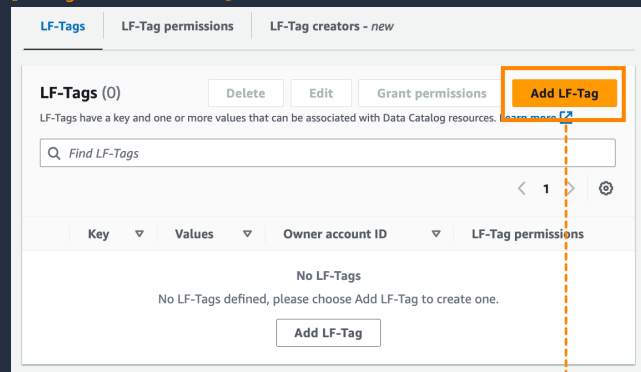
セキュリティの細かさ

LF タグ方式の設定方法

3つのステップで設定をおこなう

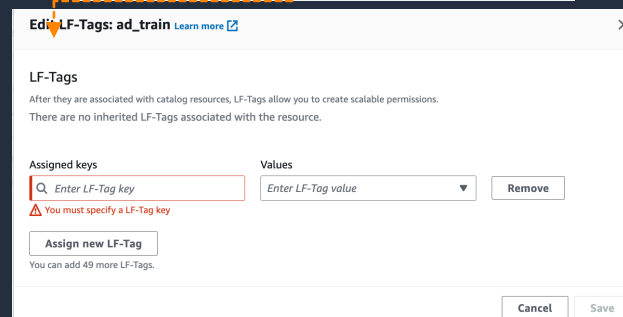
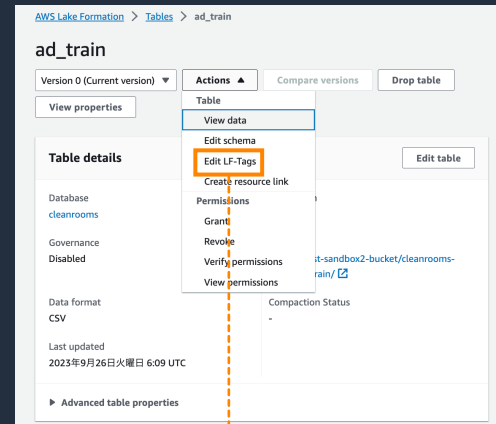
1. LF タグ を定義

[LF-Tags and Permissions]



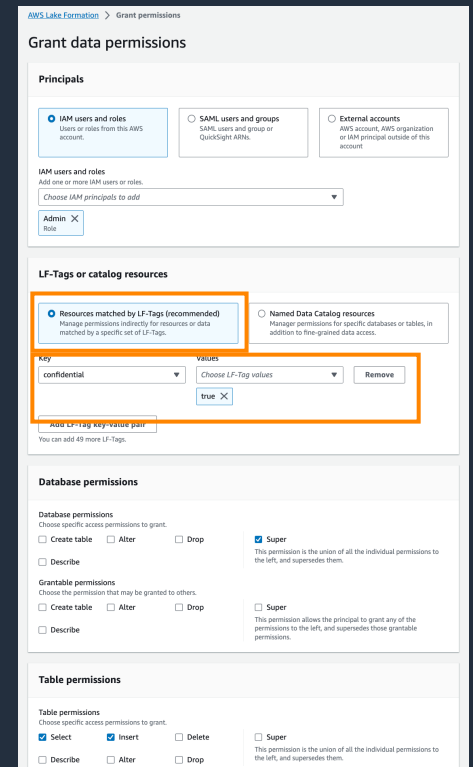
同時にそのタグを
誰が付与できるかも設定

2. LF タグをリソース (DB/Table) に付与



DB/Table/Column に付与可能
タグは下位リソースに自動で継承
(DB のタグが Table/Column に継承)
継承されたタグは上書き可能

3. LF タグを プリンシパルに付与



プリンシパルにタグと
権限を付与

LF タグによる列レベルセキュリティ

LF タグは Table の列にも付与ができるため、列に異なる LF タグを付与することで列レベルのセキュリティを実施できる

AWS Lake Formation > Tables > table1

table1

Version 0 (Current version) | Actions | Compare versions | Drop table

View properties

Table details

- Table
- View data
- Edit schema**
- Edit LF-Tags
- Create resource link

Permissions

- Grant
- Revoke
- Verify permissions
- View permissions

Governance

Disabled

Compaction Status

-

Database

lakeformation

Location

s3://shotast-sandbox1-lakeformation/table1/

Last updated

2023年8月18日 金曜日 13:01 UTC

▶ Advanced table properties

AWS Lake Formation > Tables > table1 > Edit schema

table1

Version 0 (Current version)

Schema | Upload schema | Delete | Edit | **Edit LF-Tags** | Add column

Find columns

#	Column name	Data type	Comment	LF-Tags
<input checked="" type="checkbox"/>	1	sepal_length	string	-
<input checked="" type="checkbox"/>	2	sepal_width	string	-
<input type="checkbox"/>	3	petal_length	string	-
<input type="checkbox"/>	4	petal_width	string	-
<input type="checkbox"/>	5	species	string	-

Edit LF-Tags: 2 columns

Showing only LF-Tags that are shared by all selected columns.

LF-Tags

After they are associated with catalog resources, LF-Tags allow you to create scalable permissions. There are no inherited LF-Tags associated with the resource.

Assigned keys

sensitive

Values

true

Remove

Assign new LF-Tag

You can add 49 more LF-Tags.

Cancel Save

LF タグが複数付与されている場合の挙動

LF タグはリソースに複数付与することができるが、対応するタグがプリンシパルに1つでも付与されてれば、その権限でリソースにアクセスができる

タグに以下の許可:
DESCRIBE, SELECT



プリンシパル1

Table に対して
DESCRIBE, SELECT
が可能

タグに以下の許可:
DESCRIBE, SELECT
DELETE



プリンシパル2

Table に対して
DESCRIBE, SELECT, DELETE
が可能



Table

タグによるリソースへのアクセス制御は
タグの and 条件ではなく or 条件になる

リソース方式の設定方法

誰が (プリンシパル) どのリソース (DB/Table) にアクセスできるか直接設定する

AWS Lake Formation > Grant permissions

Grant data permissions

Principals

IAM users and roles
Users or roles from this AWS account.

SAML users and groups
SAML users and group or QuickSight ARNs.

External accounts
AWS account, AWS organization or IAM principal outside of this account.

IAM users and roles
Add one or more IAM users or roles.

Choose IAM principals to add

Admin X
Role

LF-Tags or catalog resources

Resources matched by LF-Tags (recommended)
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.

Named Data Catalog resources
Manager permissions for specific databases or tables, in addition to fine-grained data access.

Databases
Select one or more databases.

Choose databases

lakeformation X

Tables - optional
Select one or more tables.

Choose tables

All tables X

Data filters - optional
Select one or more data filters.

Choose data filters

Load more Create new

Manage data filters

Table permissions **こちらのチェックボックスで権限を設定**

Table permissions
Choose specific access permissions to grant.

Select Insert Delete Super
This permission is the union of all the individual permissions to the left, and supersedes them.

Describe Alter Drop

Grantable permissions
Choose the permission that may be granted to others.

Select Insert Delete Super
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Describe Alter Drop

Cancel Grant

リソース方式のシンプルな列フィルタリング

[Grant data permissions] でプリンシパルとテーブルの組み合わせに権限を付与する際に、アクセスできる列を指定できる

Table permissions

Table permissions
Choose specific access permissions to grant.

Select Insert Delete Super
 Describe Alter Drop

Grantable permissions
Choose the permission that may be granted to others.

Select Insert Delete Super
 Describe Alter Drop

Super
This permission is the union of all the individual permissions to the left, and supersedes them.

Super
This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Data permissions

All data access
Grant access to all data without any restrictions.

Column-based access
Grant data access to specific columns only.

Choose permission filter
Choose whether to include or exclude columns.

Include columns
Grant permissions to access specific columns.

Exclude columns
Grant permissions to access all but specific columns.

Select columns
Choose one or more columns

Cancel Grant

データフィルタによる行/列/セルレベルセキュリティ

リソース方式の設定ではデータフィルタを設定することができ、このデータフィルタでは行/列/セルレベルのセキュリティを設定できる

Create data filter

Data filter name
Enter a name that describes this data access filter.
data_filter1
Name may contain letters (A-Z), numbers (0-9), hyphens (-), or underscores (_), and must be less than 256 characters long.

Target database
lakeformation Load more

Target table
catalog_sales

Column-level access
Choose whether this filter should have column-level restrictions.

Column-level access
Choose whether this filter should have column-level restrictions.

- Access to all columns
Filter won't have any column restrictions.
- Include columns
Filter will only allow access to specific columns.
- Exclude columns
Filter will allow access to all but specific columns.

Row filter expression
Enter the rest of the following query statement SELECT * FROM catalog_sales WHERE...
Please see the documentation for examples of filter expressions. [PartiQL による記述](#)

order_number=1

Cancel Create filter

Grant data permissions

Principals

- IAM users and roles
Users or roles from this AWS account.
- SAML users and groups
SAML users and group or QuickSight ARNs.
- External accounts
AWS account, AWS organization or IAM principal outside of this account.

IAM users and roles
Add one or more IAM users or roles.
Choose IAM principals to add

Admin X
Role

LF-Tags or catalog resources

- Resources matched by LF-Tags (recommended)
Manage permissions indirectly for resources or data matched by a specific set of LF-Tags.
- Named Data Catalog resources
Manage permissions for specific databases or tables, in addition to fine-grained data access.

Databases
Select one or more databases.
Choose databases lakeformation X Load more

Tables - optional
Select one or more tables.
Choose tables catalog_sales X

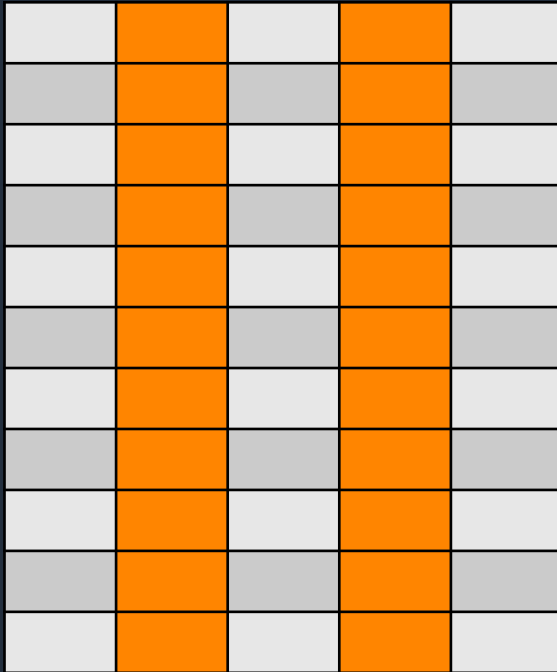
Data filters - optional
Select one or more data filters.
Choose data filters data_filter1 X Load more Create new

Manage data filters

対象となるテーブルとともに Data filter も指定する

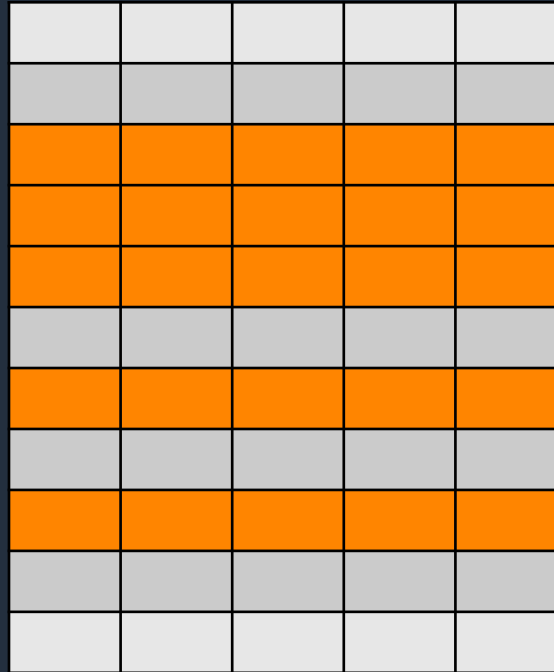
データフィルタによる行/列/セルレベルのセキュリティイメージ

Columns



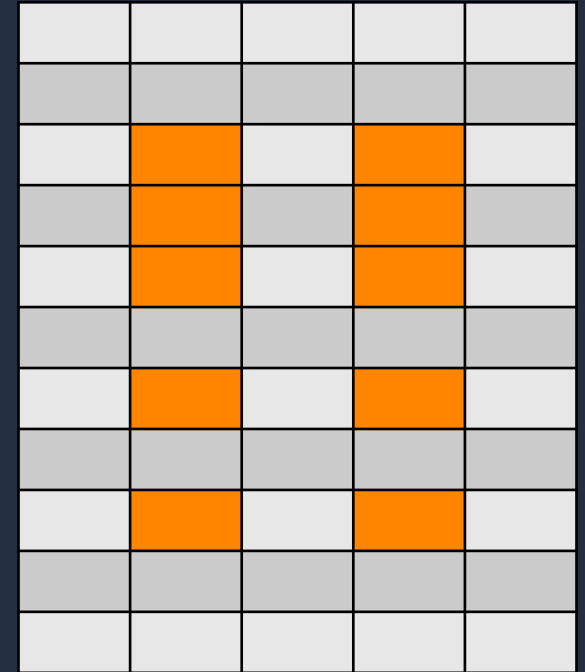
列を含む/除外する設定

Rows



PartiQL による行の設定

Cells



行と列の設定の組み合わせ

Amazon Athena, AWS Glue, Amazon Redshift Spectrum
に対応

セキュリティレベルと AWS の各サービスの対応状況

サービスによって使えるセキュリティが異なる

メタデータ アクセス制御方式	制御方法	Amazon Athena	Amazon Redshift Spectrum	AWS Glue	Amazon EMR	Amazon QuickSight
LF タグ方式	LFタグによる 列フィルタリング	○	○	×	○	※2 ○
リソース方式	シンプルな 列フィルタリング	○	○	×	○	※2 ○
	データフィルタ	○	○	○	※1 △	※2 ○

※1 PartiQL による行レベルのセキュリティは無視される

※2 QuickSight は Athena を経由した場合のみ Lake Formation の制御を受ける

黙示的な Lake Formation の許可

明示的に権限を付与しなくても各ロールには権限が付与される



データレイク
管理者

- データカタログ内のすべての Describe リソースへのアクセス
- データレイク全体に対する データロケーションへの アクセス許可
- データカタログ内の任意の リソースへのアクセス権を 任意のプリンシパルに付与可能
- データベース作成権限を 別プリンシパルに付与



データベース
作成者

- 作成するデータベースに 対するデータベース許可と そこに作成されるテーブルに 対する許可
- データベース内の テーブル作成権限を 別プリンシパルに付与



テーブル
作成者

- 作成するテーブルに対する すべての許可
- 作成するテーブルに対する アクセス権を別のプリンシパルに 付与
- 作成するテーブルが含まれる データベースの表示

権限付与権限の付与

LF タグ方式/リソース方式ともに他のプリンシパルに権限を付与するための権限付与権限を付与することができ、それによってデータレイク管理者に依存せずにアクセス権限の制御が可能

Table permissions

Table permissions
Choose specific access permissions to grant.

<input type="checkbox"/> Select	<input type="checkbox"/> Insert	<input type="checkbox"/> Delete	<input type="checkbox"/> Super
<input type="checkbox"/> Describe	<input type="checkbox"/> Alter	<input type="checkbox"/> Drop	This permission is the union of all the individual permissions to the left, and supersedes them.

Grantable permissions
Choose the permission that may be granted to others.

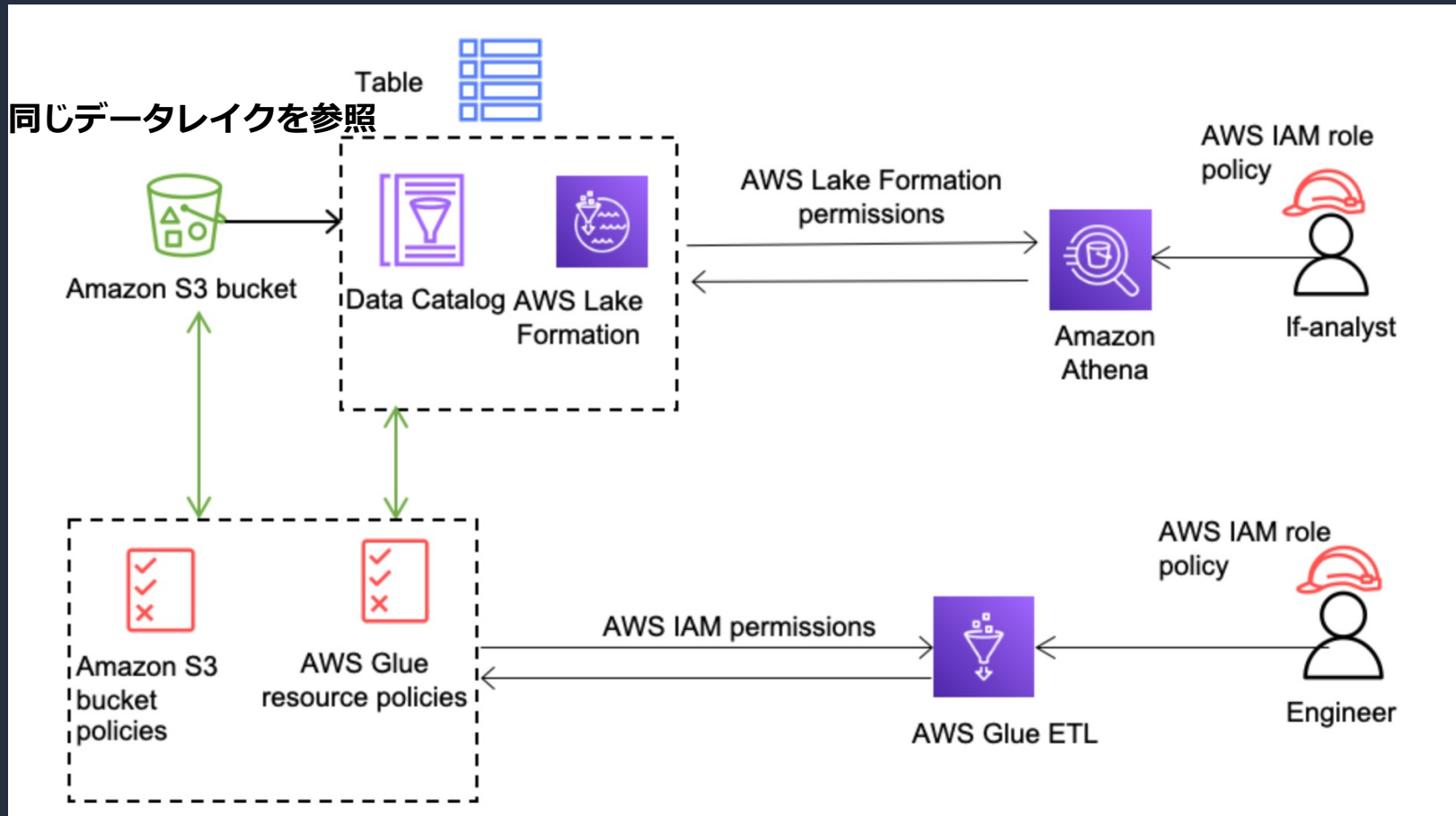
<input type="checkbox"/> Select	<input type="checkbox"/> Insert	<input type="checkbox"/> Delete	<input type="checkbox"/> Super
<input type="checkbox"/> Describe	<input type="checkbox"/> Alter	<input type="checkbox"/> Drop	This permission allows the principal to grant any of the permissions to the left, and supersedes those grantable permissions.

Cancel Grant

対象のリソースに対して SELECT/INSERT /DELETE/DESCRIBE/ALTER/DROP の権限をプリンシパルに付与できる権限を付与する

Hybrid access mode

標準の IAM による制御と Lake Formation による制御を両立させることができるモード



If-analyst は
LF の制御を受ける

Engineer は
LF の制御を受けない

Hybrid access mode の設定方法

2つのステップで設定をおこなう

1. データレイクを Hybrid access mode で登録

AWS Lake Formation > Data Lake locations > Register location

Register location

Amazon S3 location
Register an Amazon S3 path as the storage location for your data lake.

Amazon S3 path
Choose an Amazon S3 path for your data lake.
e.g.: s3://bucket/prefix/

Review location permissions - strongly recommended
Registering the selected location may result in your users gaining access to data already at that location. Before registering a location, we recommend that you review existing location permissions on resources in that location.

IAM role
To add or update data, Lake Formation needs read/write access to the chosen Amazon S3 path. Choose a role that you know has permission to do this, or choose the `AWSServiceRoleForLakeFormationDataAccess` service-linked role. When you register the first Amazon S3 path, the service-linked role and a new inline policy are created on your behalf. Lake Formation adds the first path to the inline policy and attaches it to the service-linked role. When you register subsequent paths, Lake Formation adds the path to the existing policy.
AWSServiceRoleForLakeFormationDataAccess

Do not select the service linked role if you plan to use EMR.

Enable Data Catalog Federation
Checking this box will allow Lake Formation to assume a role to access tables in a federated database.

Permission mode
Select the permission mode you want to use to manage access.

Hybrid access mode - new
Lake Formation permissions can co-exist with IAM permission policies for AWS Glue and S3 actions to manage access. [Learn more](#)

Lake Formation
Only Lake Formation permissions are enforced.

登録済みのものは
[Data lake locations] →
[Actions] → [Edit]
で編集する

2. プリンシパルの制御を Lake Formation で行うように強制

AWS Lake Formation > Hybrid access mode

Hybrid access mode

In hybrid access mode, Lake Formation permissions and IAM policies for AWS Glue/S3 work together. Note that granting permissions using LF-Tags is not fully supported yet in hybrid access mode. [Learn more](#)

How it works

Register data lake location
Register data locations and enable hybrid access mode.

Add policies
Add lakeformation:GetDataAccess permissions to the user's IAM policies and grant data location access. [Learn more](#)

Grant permissions
Grant permissions to the user and add resources and principals in hybrid access mode.

Finish setup
Lake Formation permissions are enforced after you add resources and principals in hybrid access mode.

Resources and principals in hybrid access mode (1)
To enforce Lake Formation permissions, you need to opt-in databases, tables, and resources to hybrid access mode.

AWS Lake Formation > Hybrid access mode > Add resources and principals

Add resources and principals

Choose databases, tables, and principals to add in hybrid access mode. Lake Formation permissions will be enforced. [Learn more](#)

Resources

Databases
Select one or more databases.
Choose databases

Tables - optional
Select one or more tables.
Choose tables

Principals

IAM users and roles
Users or roles from this AWS account.

IAM users and roles
Add one or more IAM users or roles.
Choose IAM principals to add

External accounts
AWS account, AWS organization or IAM principal outside of this account.

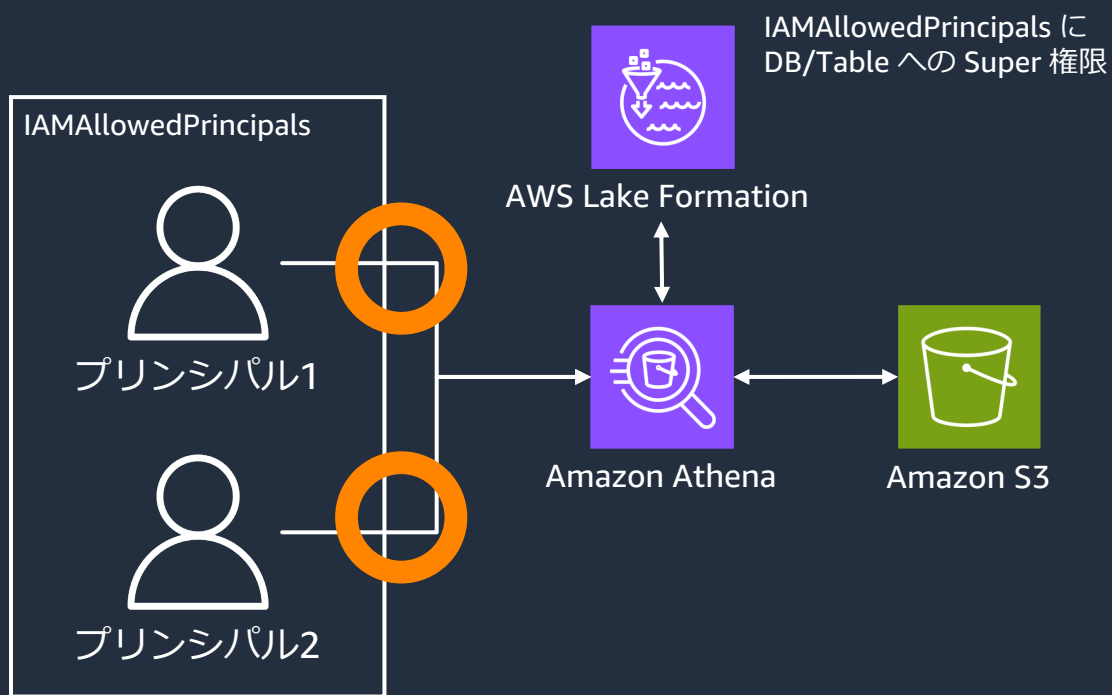
LF 制御を強制するリソースと
プリンシパルの対象を
選択する

LF タグによる制御を利用してる
場合も同様に強制するリソース
とプリンシパルを選択する

Hybrid access mode の仕組み

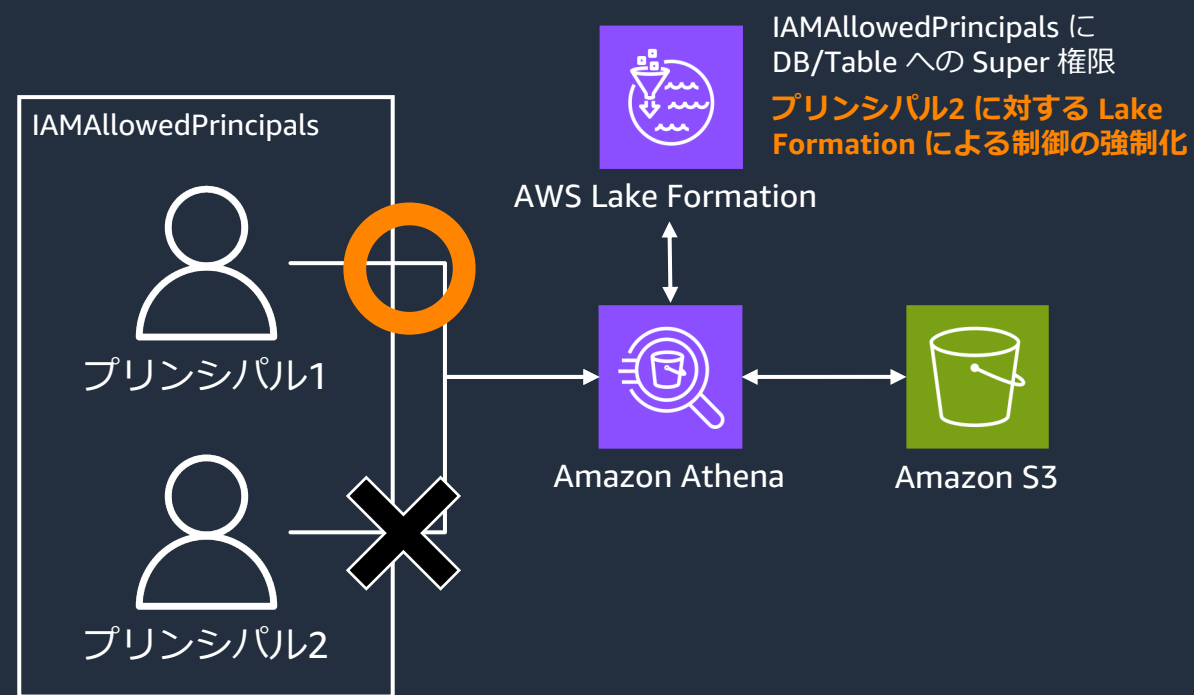
Hybrid access mode は IAMAllowedPrincipals が付与されていても Lake Formation による制御を強制的に行わせる機能

Lake Formation モード



IAMAllowedPrincipals に Super 権限が付与されているため IAMAllowedPrincipals に属するプリンシパルは任意の DB/Table にアクセス可能

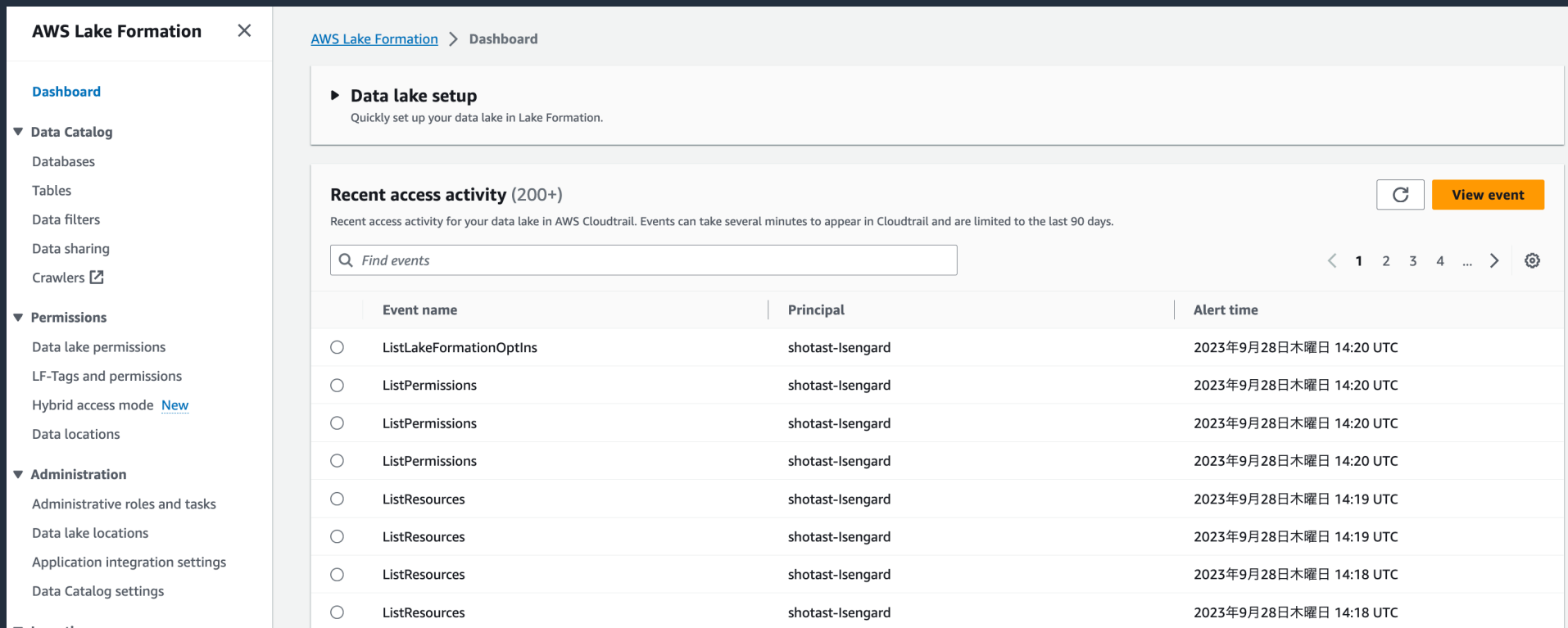
ハイブリッドアクセスモード



Lake Formation による制御が強制化されているため プリンシパル2 は IAMAllowedPrincipals に属しながらそれとは別に Lake Formation 上でメタデータのアクセス許可が必要

CloudTrail との統合

Lake Formation は CloudTrail と統合されており、Lake Formation API のコールをイベントとしてキャプチャする。Lake Formation のコンソール画面で確認が可能



The screenshot displays the AWS Lake Formation console interface. On the left is a navigation sidebar with sections for Dashboard, Data Catalog, Permissions, and Administration. The main content area shows the 'Recent access activity (200+)' section, which includes a search bar and a table of events. The table lists event names, principals, and alert times.

Event name	Principal	Alert time
ListLakeFormationOptIns	shotast-lsengard	2023年9月28日木曜日 14:20 UTC
ListPermissions	shotast-lsengard	2023年9月28日木曜日 14:20 UTC
ListPermissions	shotast-lsengard	2023年9月28日木曜日 14:20 UTC
ListPermissions	shotast-lsengard	2023年9月28日木曜日 14:20 UTC
ListResources	shotast-lsengard	2023年9月28日木曜日 14:19 UTC
ListResources	shotast-lsengard	2023年9月28日木曜日 14:19 UTC
ListResources	shotast-lsengard	2023年9月28日木曜日 14:18 UTC
ListResources	shotast-lsengard	2023年9月28日木曜日 14:18 UTC

AWS Lake Formation の機能 - ブループリントの概要と機能

ブループリント機能とは？

ブループリントはデータレイクにデータを取り込むためのワークフローを手軽に実装できる機能で、様々な種類がある

[AWS Lake Formation](#) > [Blueprints](#) > Use a blueprint

Use a blueprint

Blueprint type
Configure a blueprint to create a workflow.

Database snapshot
Bulk load data to your data lake from MySQL, PostgreSQL, Oracle, and Microsoft SQL Server databases.

Incremental database
Load new data to your data lake from MySQL, PostgreSQL, Oracle, and SQL Server databases.

AWS CloudTrail
Bulk load data from AWS CloudTrail sources.

Classic Load Balancer logs
Load data from Classic Load Balancer logs.

Application Load Balancer logs
Load data from Application Load Balancer logs.

Glue Connect で接続できるデータソースから洗い替え or 増分更新が可能

AWS の各種ログを一括ロード

Import frequency

Schedule the workflow.

ワークフローのトリガーは時間により発火

Frequency
Choose how often to run the workflow.

Run on demand

ブループリントの作成例

それぞれの種類によって必要な設定が異なる

Incremental Database (増分更新)

Import source

Configure the workflow source.

Database connection
Choose the connection to the data source. [Create a connection in AWS Glue](#)

None defined

Source data path
Enter the path from which to ingest data. For JDBC databases with schema support, enter database/schema/table (case sensitive). Substitute the percent (%) wildcard for schema or table.

database-name/table-name

Advanced options

Hash field
The name of a column in the JDBC table to be used to divide the data into partitions.

Hash partitions
The number of parallel reads of the JDBC table. If this property is not set, the default and maximum value is 7.

Server side encryption
Enables Amazon S3-managed encryption of the data at the target (SSE-S3).

Enable SSE-S3 encryption.

Incremental data

Enter tables in the data source to import along with bookmark columns to determine previously imported data.

Table name	Bookmark keys	Bookmark order	Partitioning scheme - optional	
Enter a table name	Enter a bookmark Comma-delimited list of bookmark columns.	Choose a s...	Type partitioning	Remove

Add

増分管理のための単調増加するキー (bookmark key) を指定

AWS CloudTrail

AWS CloudTrail
Bulk load data from AWS CloudTrail sources.

Classic Load Balancer logs
Load data from Classic Load Balancer logs.

Application Load Balancer logs
Load data from Application Load Balancer logs.

Import source

Configure the workflow source.

CloudTrail name **CloudTrail の名前を指定**
Choose a CloudTrail source.

Choose a trail

Start date **取り込み開始時期を指定**
Choose a CloudTrail source start date.

Choose a start date

補足：ブループリント vs AWS Glue

ブループリントは AWS Glue workflow でトリガ、ジョブ、クローラーを自動的に設定するため、実装の難易度が低いのがポイント。AWS Glue はブループリントよりも遥かに実装の自由度が高い。Glue で実装ができるのであれば、障害対応や実装の透明性の観点で Glue を推奨

ブループリント

AWS Glue

GUI での実装

可能 (CLI にはなし)

AWS Glue Studio を使えば可能

Spark コード
の実装有無

不要
(ブループリントが全て用意)

場合によっては必要
(Glue Studio を使うと自動で生成できる)

ワークフロー
の実装有無

不要
(ブループリントが全て用意)

必要で、AWS Glue workflow や
AWS Step Functions などを利用

トリガーの
自由度

時間や頻度のみ
(裏でAWS Glue workflowが作られるので
それを編集すれば他の Glue Job や
EventBridge と連携可能)

使うワークフローエンジンに依存する

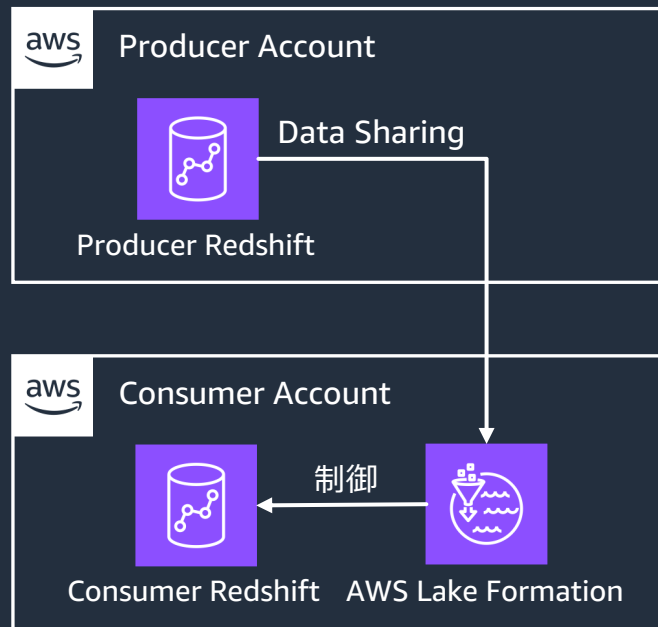
AWS Lake Formation の機能

- データ共有の概要と機能

AWS Lake Formation によるデータ共有の種類

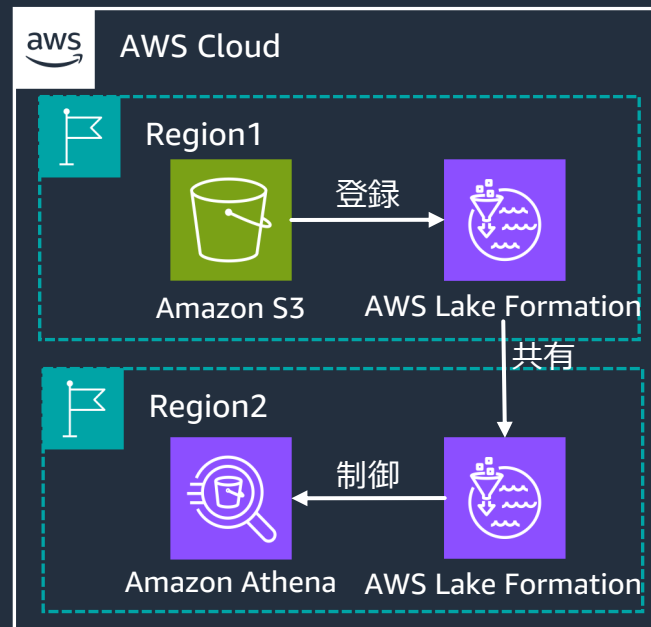
Lake Formation は3種類のデータ共有を制御することが可能

Redshift Data Sharing



共有された Redshift のデータを
Consumer 側で制御

クロスリージョン共有



同じアカウントだが
リージョンを跨いだ
データレイクの共有と制御が可能

クロスアカウント共有

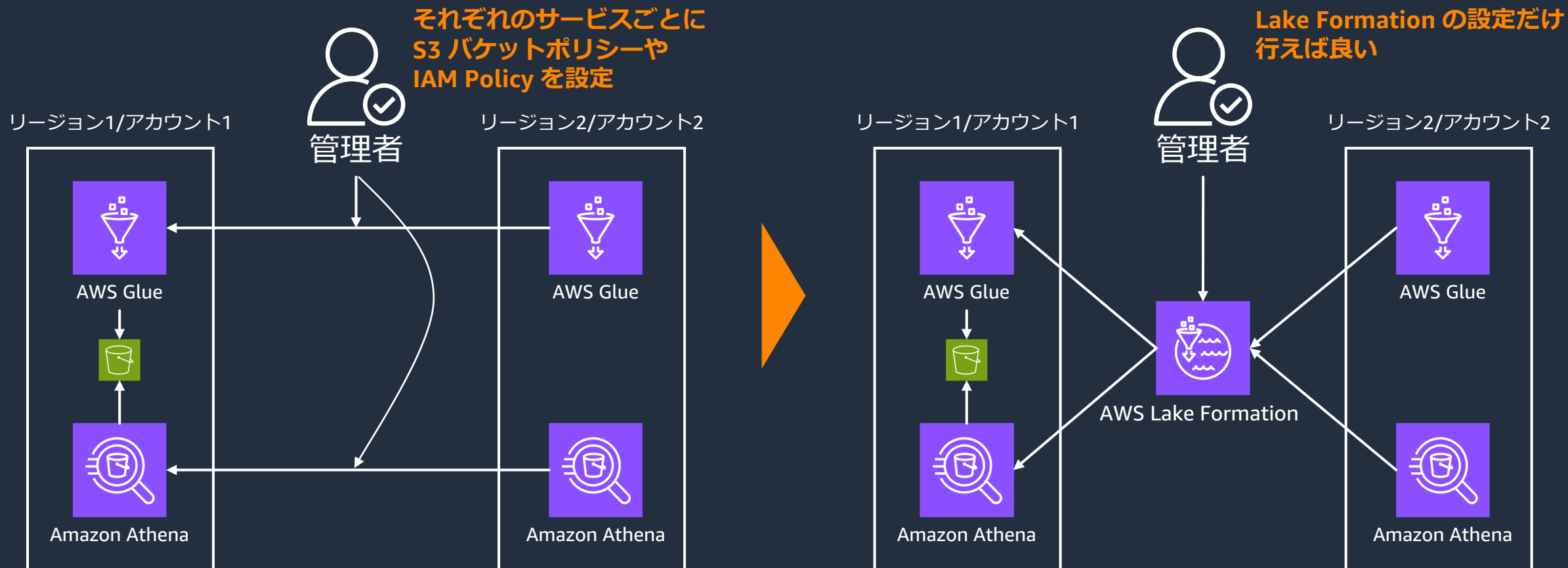


同じリージョンだが
アカウントを跨いだ
データレイクの共有と制御が可能

組み合わせることでリージョンと
アカウントを跨いでデータレイクの共有が可能

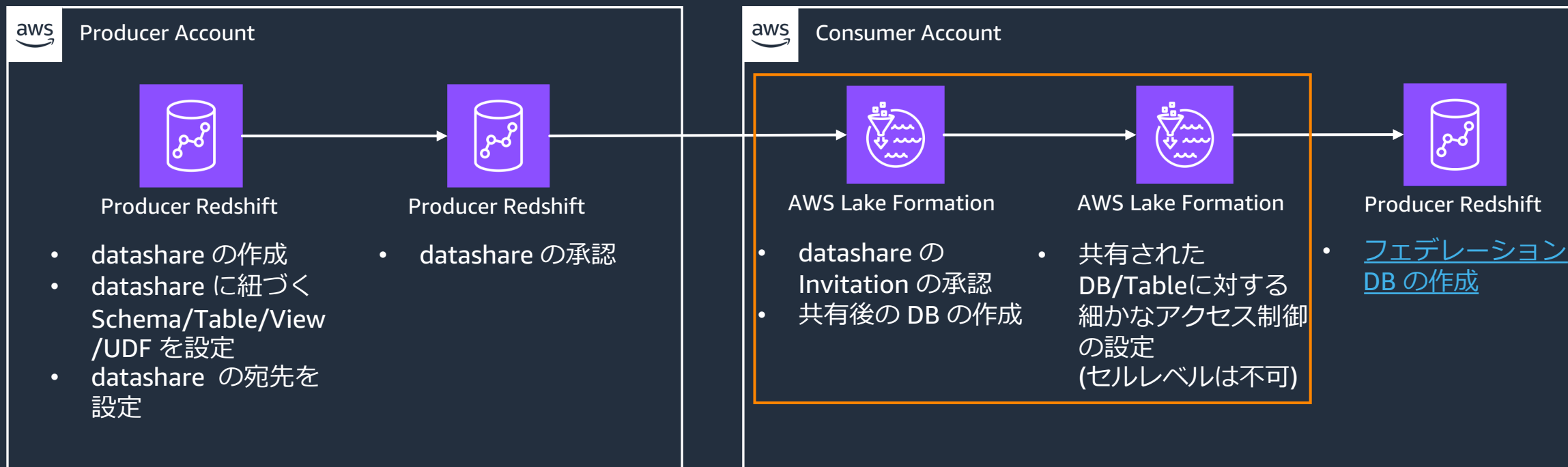
AWS Lake Formation を利用する理由

クロスリージョン/クロスアカウント共有は Lake Formation を使わなくても実現可能だが、Lake Formation を使うことで一元的に設定が可能のため、運用負荷が減る



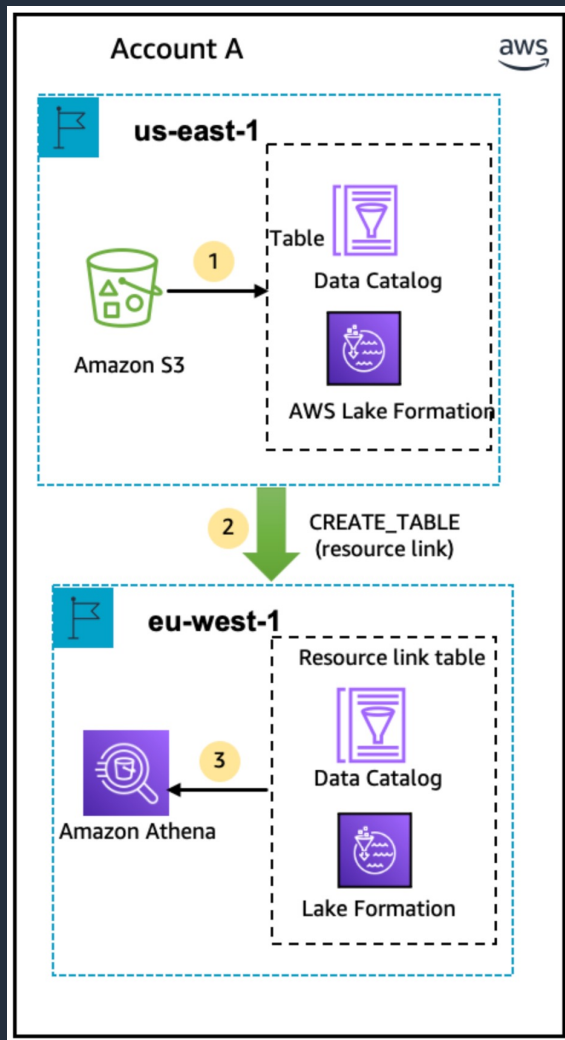
Redshift Data Sharing における Lake Formation の制御

Redshift Data Sharing を行う際に Consumer 側で Lake Formation による制御を行い、共有された側で細かな粒度のアクセス制御を実現できる



クロスリージョン共有

リソースリンクを作ることで、同一アカウント他リージョンへのリソースを共有することが可能



1 S3 のリソースを共有元リージョン (Producer) で Lake Formation に登録して細かな粒度のアクセス制御を実施

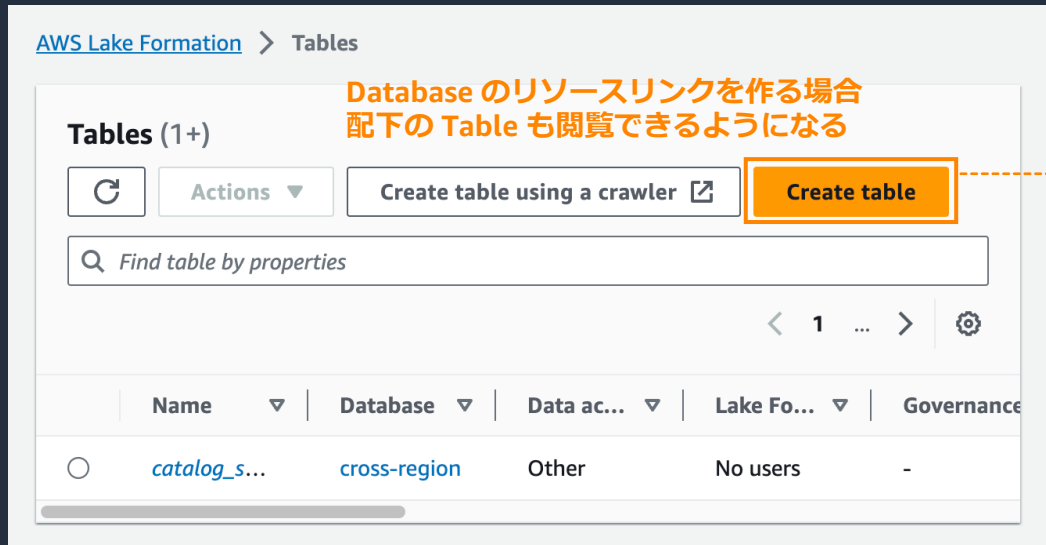
2 共有先リージョン (Consumer) で Producer の資源を指定して Lake Formation 上でリソースリンクを作成

3 Consumer 側で Lake Formation のアクセス制御を利用して Athena 等のサービスでアクセス制御を実施

※ Consumer 側では [Describe]/[Drop] の権限しか設定できないため、
見せる見せないの制御しかできない。細かな粒度の制御は Producer 側で実施する

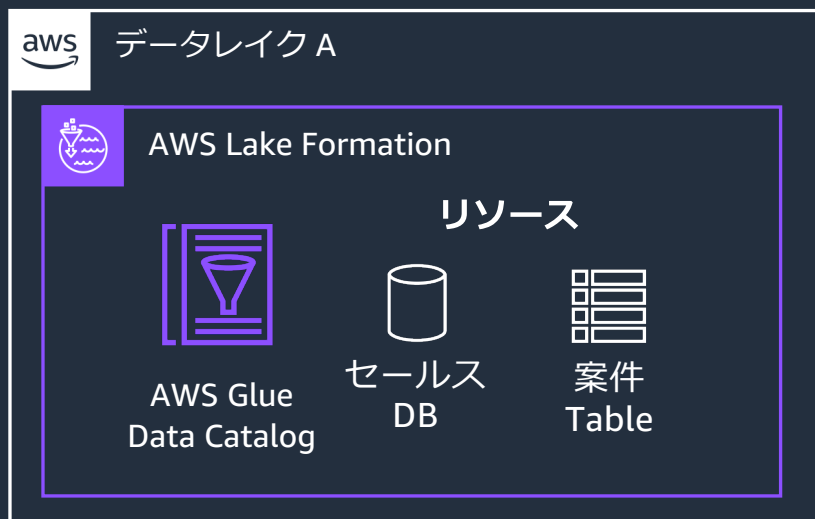
クロスリージョン共有 – リソースリンクの作成

共有先 (Consumer) のリージョンで [Databases]/[Tables] → [Create database]/[Create table] から作成が可能



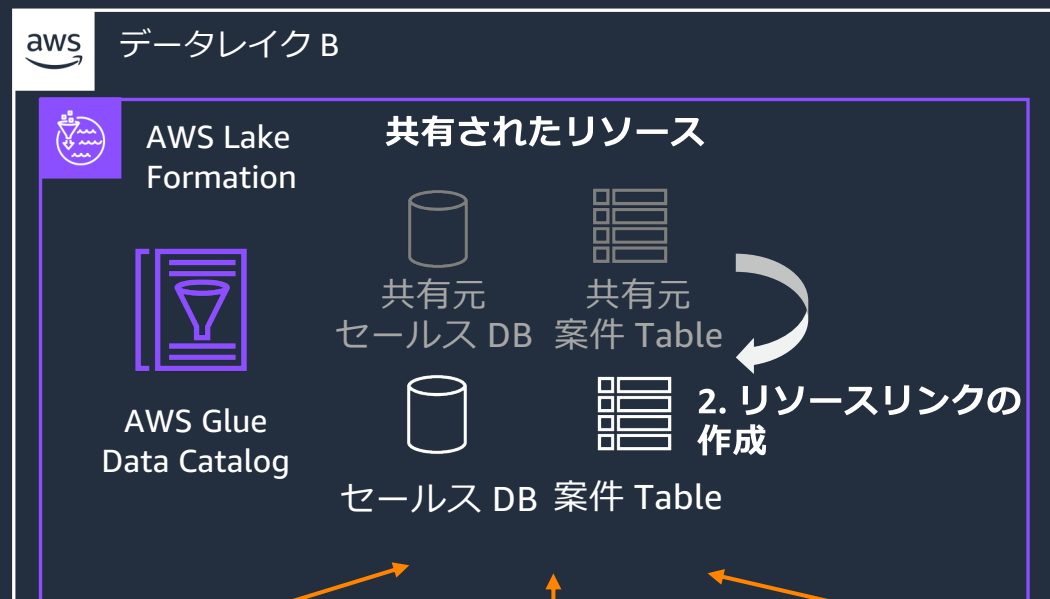
クロスアカウント共有

Lake Formation による細かな粒度のアクセス制御を実施した状態で、他 AWS アカウントにデータレイクを共有可能（LFタグ方式、リソース方式どちらも可能）



1. AWS Lake Formation による共有設定

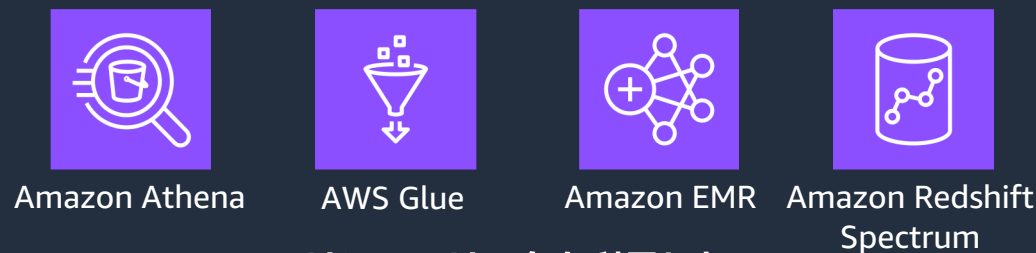
共有先 AWS アカウントを指定



1. AWS Lake Formation のクロスアカウント共有でデータ共有元のデータアクセス権限をデータ共有先に付与

2. データ共有先でリソースリンクを作成し、リソースリンクに対してアクセス権限を管理

※ リソースリンクは [Describe]/[Drop] の権限のみ設定可能



リソースリンクを利用したデータレイク A のリソースへのアクセス

クロスアカウント共有 – Producer 側の設定（前提条件）

クロスアカウント共有を始めるためには権限の整理や AWS Glue のリソースポリシーの変更が必要

- 共有するリソースに対して IAMAllowedPrincipals 許可をすべて排除する
 - IAMAllowedPrincipals があると AccessDeniedException が発生する
- AWS Glue リソースポリシーの更新
 - 以下の JSON を Glue API で実行

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ram.amazonaws.com"
      },
      "Action": "glue:ShareResource",
      "Resource": [
        "arn:aws:glue:<region>:<source-account-id>:table/*/*",
        "arn:aws:glue:<region>:<source-account-id>:database/*",
        "arn:aws:glue:<region>:<source-account-id>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "<target-account-id>"
      },
      "Action": "glue:*",
      "Resource": [
        "arn:aws:glue:<region>:<source-account-id>:table/*/*",
        "arn:aws:glue:<region>:<source-account-id>:database/*",
        "arn:aws:glue:<region>:<source-account-id>:catalog"
      ],
      "Condition": {
        "Bool": {
          "glue:EvaluatedByLakeFormationTags": "true"
        }
      }
    }
  ]
}
```

policy.json

リソース方式に必要な設定
<region> と <source-account-id> に
適切な値を入れる

LF タグ方式に必要な設定
<target-account-id>, <region> と
<source-account-id> に
適切な値を入れる

```
aws glue put-resource-policy --policy-in-json  
file://policy.json --enable-hybrid TRUE
```

※ ファイルを指定する場合 file:// が必要

クロスアカウント共有 – Producer の設定①

[Data Catalog settings] → [Cross account version settings] で、クロスアカウントの仕様バージョンを切り替えられるが、基本最新の Version4 を使えば良い

Cross account version settings

These settings control how Lake Formation manages RAM Resource Shares when granting or revoking cross account permissions. See [Granting permissions on cross-account resources](#).

Current cross account version **前のバージョンを利用していた
以外の理由で古いバージョンを
使うメリットはない**

- Version 4 ▲
- Version 1
- Version 2
- Version 3
- Version 4 ✓

Cancel Save

**Producer と Consumer は同じバージョンにしておくのが良い
Producer が v1, v2 で Consumer が v3, v4 だとエラーが発生する
(Invalid cross account grant request)**

クロスアカウント共有 – Producer の設定②

LF タグ方式のアクセス制御で共有を行う場合は、Consumer 側に LF タグの権限を付与する
(リソース方式では不要)

[LF-Tags and Permissions]

LF-Tag permissions (18)

View and manage the permissions granted on LF-Tags. [Learn more](#)

Find permissions by LF-Tag key and value

	Principal	Principal type	Keys	Values	LF-Tag permis
<input type="radio"/>	[REDACTED]	AWS account	lftag	true	-
<input type="radio"/>	[REDACTED]	AWS account	lftag	true	-
<input type="radio"/>	[REDACTED]	AWS account	key1	true	-

Grant LF-Tag permissions

Select the principals to grant permissions to, the LF-Tags to grant permissions on, and the specific set of permissions.

Permission type
Choose the type of permission to grant. [Learn more](#)

- LF-Tag permissions - new
Grant permissions on LF-Tags to create, update, and delete LF-Tags.
- LF-Tag key-value pair permissions
Grant permissions on LF-Tag key-value pairs to assign LF-Tags to Data Catalog resources and grant permissions on the resources to principals.

Principals

- IAM users and roles
Users or roles from this AWS account.
- SAML users and groups
SAML users and group or QuickSight ARNs.
- External accounts
AWS account, AWS organization or IAM principal outside of this account

AWS account, AWS organization, or IAM principal outside of this account
Enter one or more AWS account IDs, AWS organization IDs, or IAM principal ARNs. Press Enter after each ID or ARN.

Choose AWS account, AWS organization ID, or IAM principal ARN

LF-Tag key-value pair permissions

Key: lftag | Values: Choose LF-Tag values | true X | Remove

Add LF-Tag key-value pair

You can add 49 more LF-Tags.

Permissions
Choose the specific key-value pair permissions to grant.

- Describe
See keys and values.
- Associate
Assign LF-Tags to databases, tables, and columns.

Grantable permissions
Choose the permissions that the grant recipient(s) can grant to other principals.

- Describe
See keys and values.
- Associate
Assign LF-Tags to databases, tables, and columns.

Describe の権限だけで良い

クロスアカウント共有 – Producer の設定③

[Data lake permissions] で Consumer の AWS Account/IAM Role を指定して、方式に応じてアクセス制御を行い、共有

LF タグ方式

The screenshot shows the 'Grant data permissions' interface. Under 'Principals', the 'External accounts' radio button is selected and highlighted with an orange box. Below it, there is a text input field for 'Choose AWS account, AWS organization ID, or IAM principal ARN'. In the 'LF-Tags or catalog resources' section, the 'Resources matched by LF-Tags (recommended)' radio button is selected. Below this, there is a table with columns 'Key' and 'Values'. The 'Key' is 'lftag' and the 'Values' is 'true'. There is a 'Remove' button and an 'Add LF-Tag key-value pair' button.

LF タグ方式の共有では LF タグによる
列レベルセキュリティを実施可能

リソース方式

The screenshot shows the 'Grant data permissions' interface. Under 'Principals', the 'External accounts' radio button is selected and highlighted with an orange box. Below it, there is a text input field for 'Choose AWS account, AWS organization ID, or IAM principal ARN'. In the 'LF-Tags or catalog resources' section, the 'Named Data Catalog resources' radio button is selected. Below this, there are sections for 'Databases' and 'Tables - optional'. The 'Databases' section has a dropdown menu with 'lakeformation' selected. The 'Tables - optional' section has a dropdown menu with 'catalog_sales_data_filter' selected. There is also a 'Data filters - optional' section with a dropdown menu and a 'data_filter_test' filter selected. There are 'Load more' and 'Create new' buttons.

Data Filter による
行列セルレベルの制御が可能

どちらも External accounts を設定

クロスアカウント共有 – Consumer 側の設定①

同じ AWS Organization に属していない場合、AWS RAM での受け入れ承認が必要

The image shows two screenshots from the AWS Resource Access Manager console. The left screenshot shows the 'Resource Access Manager' sidebar with '自分と共有' (Self and Shared) selected, and a list of shared resources. The right screenshot shows the details for a specific resource, 'LakeFormation-V4-FD1GDVTQBG', with a confirmation dialog to accept or reject the resource sharing request.

Resource Access Manager

自分と共有

リソースの共有

共有リソース

プリンシパル

自分と共有

リソースの共有 **2 招待**

共有リソース

プリンシパル

Resource Access Manager > 自分と共有: リソース共有

自分と共有: リソース共有

自分のアカウントがアクセスできるリソース共有

リソース共有 (2)

テキストとプロパティ値によるフィルタリング

	名前
<input type="radio"/>	LakeFormation-V4-FD1GDVTQBG
<input type="radio"/>	LakeFormation-V4-GEPUNXIMTN

Resource Access Manager > 自分と共有: リソース共有 > リソース共有 7d1733ff-2411-42bc-bcb9-c2e6bf3bdcc8

LakeFormation-V4-FD1GDVTQBG (7d1733ff-2411-42bc-bcb9-c2e6bf3bdcc8)

このリソース共有に関する詳細や情報。

リソース共有を拒否 **リソース共有を承認**

概要

名前	LakeFormation-V4-FD1GDVTQBG	所有者	[REDACTED]
招待日	2023/10/02	ステータス	🕒 保留中

クロスアカウント共有 – Consumer 側の設定②

共有されたリソースは Lake Formation のコンソールからは確認できるが、Athena 等から利用できないため、リソースリンクを作成する

Databaseのリソースリンクを作る場合
配下の Table も閲覧できるようになる

Producerのリソースが確認可能で
選択してリソースリンクを作る

Name	Owner account ID
amazondatazone-database...	7551-██████████
cleanrooms	7551-██████████
lakeformation	8081-██████████
lakeformation-link	7551-██████████
myspectrum_db	7551-██████████
sandbox	7551-██████████

Resource link name
lakeformation_link
Name may contain letters (A-Z), numbers (0-9), hyphens (-), or underscores (_), and must be less than 256 characters long.

Shared database's region
US East (N. Virginia)

Shared database
lakeformation

Shared database's owner ID
██████████

Cancel Create

AWS Lake Formation の料金



AWS Lake Formation 費用

AWS Lake Formation 自体の利用は無償

配下で活用するサービスに
かかる費用のみのお支払い



まとめ

まとめ

- 細かな粒度のアクセス制御を様々な AWS サービスに実施可能
 - アクセス制御の裏側、制御の対象、IAMAllowedPrincipals など Lake Formation の権限管理の仕組みを紹介
 - LF タグによるアクセス制御とリソース方式によるアクセス制御を説明
- ブループリントによる簡単なデータ取り込み
 - DB, AWS ログの自動取り込み、Glue のトリガー、ジョブ、クローラーの自動設定
- Lake Formation を利用した安全なデータ共有
 - Redshift Data Sharing の Consumer 側での制御、クロスリージョン共有、クロスアカウント共有が可能
- Lake Formation 自体の費用は無償
 - 配下で仕様するサービス費用のみ

参考資料

- AWS Lake Formation 公式ドキュメント
 - <https://docs.aws.amazon.com/lake-formation/latest/dg/what-is-lake-formation.html>
- Amazon Redshift “What is datashare?”
 - https://docs.aws.amazon.com/redshift/latest/dg/what_is_datashare.html#lf_datashare_overview
- AWS 公式ブログ “Lake Formation を使用し AWS アカウント間でセキュアにデータ共有を実現”
 - <https://aws.amazon.com/jp/blogs/news/lake-formation-cross-account/>
- AWS CLI Command Reference “glue”
 - <https://docs.aws.amazon.com/cli/latest/reference/glue/#cli-aws-glue>



Thank you!