

Amazon QuickSightの運用設計

きめ細かなユーザー権限とアクセス管理におけるポイント

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 事業開発
伊東 大騎
2020年10月14日

自己紹介

伊東 大騎

Amazon QuickSightの事業開発
お客様のデータ活用をご支援

前職：

小売企業にてEC/3DCG/画像認識/RFID領域のプロジェクト推進に従事

好きなAWSサービス：

Amazon QuickSight ・ Amazon Athena



本格的なBIの運用を始めよう！が。。。

考慮すべきポイントは？

どこまで細かく権限を設定できる？

権限はどう振り分ける？

どういう順番で考えるべき？

どのQuickSight機能を使えば良い？

QuickSightの構成要素

大きくは「**ユーザー**」と「**アセット**」（データ・分析・ダッシュボード）の2つ！

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

インフラ担当者

全権限を持つ管理者

全てのアセット権限を持つ分析者

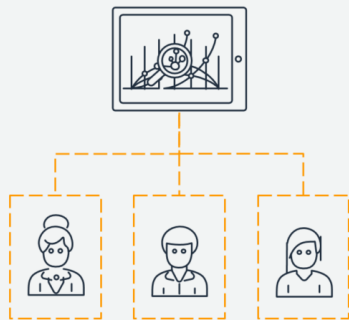
一部のアセット権限に限定された
分析者

閲覧者

QuickSightの運用設計 3ステップ

STEP-1

組織内の役割分担を定義



どの部署の誰がBI管理者となるか？
利用する部署は？
分析者にどこまでの権限を提供する？

STEP-2

各ユーザーの権限を決定



Admin / Author / Reader

QuickSightロールのAdmin、Author、
Readerを付与
Authorの場合は柔軟に権限設定

STEP-3

アセットへのアクセスを設定



アクセス管理に利用するQuickSightの機能
ネームスペース、フォルダー、行レベル
セキュリティ、IAM、など

まずは組織内の役割分担を明確に

STEP-1

*あくまでも一例であるため組織ごとに定義が異なります

BI管理者

アカウントの作成、
ユーザの追加・削除、
コストなどの**総管理者**

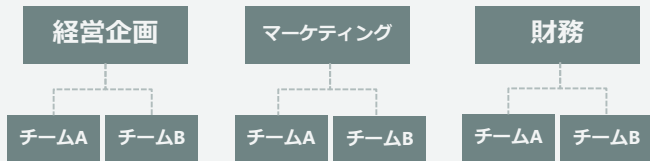
社内全体のデータ・分
析・ダッシュボードを
準備する**BIエンジニア**

全ダッシュボードの閲覧者

組織全体の責任を担う
社長や経営陣

部署を横断して案件を
推進する**プロジェクト
マネージャー**

部署単位のユーザー



部署毎のダッシュボー
ド作成を担う**分析者**で
SQLを使う

用途に応じてアドホッ
ク分析する**分析者**

日々の最新データを確
認するデータ**閲覧者**

次にQuickSightの各種ユーザー権限を付与する

STEP-2

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

インフラ担当者

全権限を持つ管理者(Admin)

全てのアセット権限を持つ分析者(Author)

一部のアセット権限に限定された
分析者(Author)

閲覧者(Reader)

権限 = そのアセットを追加・削除・共有できる

各役割の権限（ロール）を決定

STEP-2

	権限範囲					QuickSight ロール
	アカウント・ ユーザー	データソース	データセット	分析	ダッシュボード	
BI管理者	●	●	●	●	●	Admin
		●	●	●	●	Author 全権限
全ダッシュボードの 閲覧者					● 閲覧のみ	Reader
			●	●	●	Author 一部権限
部署単位の利用者				●	●	Author 一部権限
					●	Reader
					● 閲覧のみ	Reader

Authorのカスタム権限

STEP-2



戻る

カスタムアクセス許可を作成

名前

① 英数字と +, -, @, _ 文字を使用します。最大文字数は 64 文字です。

制限

- データソースの作成または更新を制限する
- データセットの作成または更新を制限する
- E メールレポートの作成または更新を制限する
- E メールレポートへのサブスクライブを制限する
- 分析の共有を制限する
- ダッシュボードの共有を制限する
- データセットの共有を制限する

作成

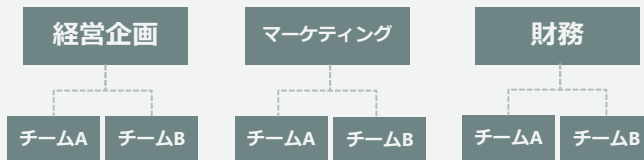
ユーザーを追加し権限の付与

STEP-2

BI管理者

全ダッシュボードの閲覧者

部署単位のユーザー



 Admin

アカウントの作成、
ユーザの追加・削除、
コストなどの総管理者

 Reader

組織全体の責任を担う
社長や経営陣

 Author

部署毎のダッシュボー
ド作成を担う分析者

 Author

社内全体のデータ・分
析・ダッシュボードを
準備するBIエンジニア

 Reader

部署を横断して案件を
推進するプロジェクト
マネージャー

 Author

用途に応じてアドホッ
ク分析する分析者

 Reader

日々の最新データを確
認するデータ閲覧者

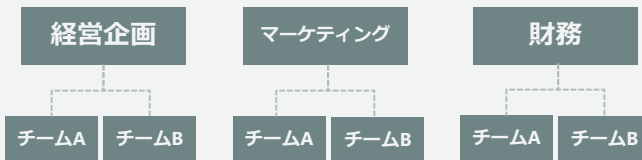
グループを作成

STEP-2

BI管理者

全ダッシュボードの閲覧者

部署単位のユーザー



 Admin

orgAdmin

アカウントの作成、
ユーザの追加・削除、
コストなどの総管理者

 Author

orgAuthor

社内全体のデータ・分
析・ダッシュボードを
準備するBIエンジニア

 Reader

orgReader

組織全体の責任を担う
社長や経営陣

 Reader

orgReader

部署を横断して案件を
推進するプロジェクト
マネージャー

 Author

markRep/
accounRep

部署毎のダッシュボー
ド作成を担う分析者

 Author

markAuthor/
accounAuthor

用途に応じてアドホッ
ク分析する分析者

 Reader

markReader/
accounReader

日々の最新データを確
認するデータ閲覧者

なぜグループが重要か？

STEP-2

グループ単位で権限を付与することで運用を効率化
(データ・Authorのカスタム権限・分析・ダッシュボード・フォルダー)

QuickSightのロール単位でまとめておくと便利

グループはコマンドラインで作成

STEP-2

```
$ aws quicksight create-group --aws-account-id <your aws account> --namespace  
'default' --group-name 'dashboard-readers'
```



最終アクティブ日時を使ったユーザー管理

STEP-2

非アクティブなAuthorや退職者を把握するのに便利

ユーザーを管理

[ユーザーを招待](#) [Manage permissions](#) Role: All

ユーザーの検索

ユーザー名 <small>📄</small>	Eメール <small>↑↓</small>	ロール	Permissions	Last active <small>↑↓</small>	アクション
Admin/itohdaik-lsengard	itohdaik@amazon.co.jp	管理者		2020-09-03 22:01	
QuickSight-Author/itohdai...	itohdaik@amazon.co.jp	作成者 <input type="text"/>		2020-02-24 21:42	<input type="text"/>

Showing 1 - 2 of 2 users.

各種アセットのアクセス管理

STEP-3

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

IAM

ネームスペース

個別にGUIあるいはAPI操作で共有

フォルダー

行レベルセキュリティ

各種アセットのアクセス管理

STEP-3



より厳密に分離したい場合は？

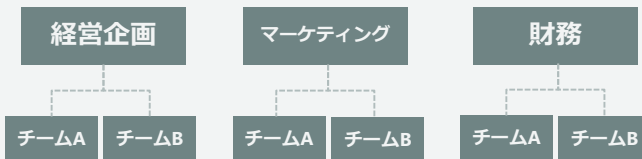
STEP-3

このままと同じ空間上に全ユーザー・アセットが存在するため

BI管理者

全ダッシュボードの閲覧者

部署単位のユーザー



 Admin

orgAdmin

アカウントの作成、
ユーザの追加・削除、
コストなどの総管理者

 Author

orgAuthor

社内全体のデータ・分
析・ダッシュボードを
準備するBIエンジニア

 Reader

orgReader

組織全体の責任を担う
社長や経営陣

 Reader

orgReader

部署を横断して案件を
推進するプロジェクト
マネージャー

 Author

markRep/
accounRep

部署毎のダッシュボー
ド作成を担う分析者

 Author

markAuthor/
accounAuthor

用途に応じてアドホッ
ク分析する分析者

 Reader

markReader/
accounReader

日々の最新データを確
認するデータ閲覧者

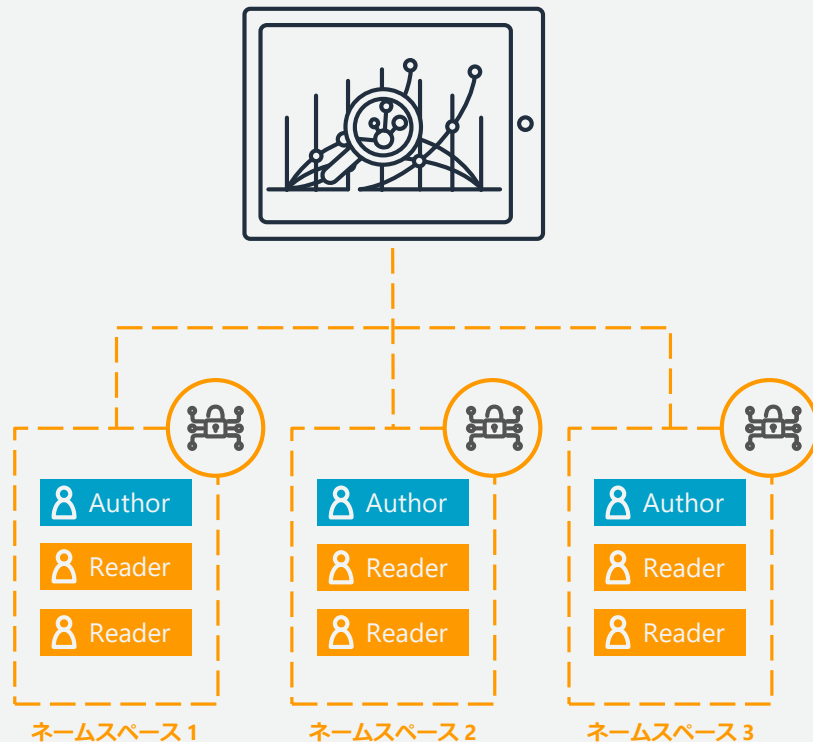
ネームスペースを使ったマルチテナント構成

STEP-3

ユーザーおよびアセットを隔離された空間に分離することで、よりセキュアな環境を構築

Authorは自分が入っているネームスペース以外のユーザーとアセットを共有することは一切できない

※ほとんどのユーザーがReaderという場合は、そもそも権限が限定されていてリスクがないため、ネームスペースを使う必要なし



ネームスペースを使ったマルチテナント構成 例①

STEP-3

個人情報を扱うカスタムソリューション部のみ他とは分離したい

“default” ネームスペース



“all” ネームスペース



“customerSolution” ネームスペース



defaultは全体を管理するネームスペースでアカウントに最初から準備されている

ネームスペースを使ったマルチテナント構成 例②

STEP-3

SaaSに組み込んで提供する場合、クライアント単位で分離したい

“default” ネームスペース



“companyA” ネームスペース



“companyB” ネームスペース



defaultは全体を管理するネームスペースでアカウントに最初から準備されている

各種アセットのアクセス管理

STEP-3

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

IAM

ネームスペース

個別にGUIあるいはAPI操作で共有

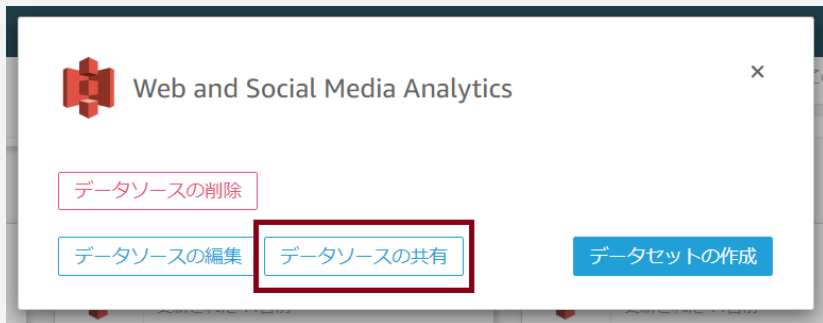
フォルダー

行レベルセキュリティ

各アセットをユーザーに共有しアクセス権限を与える

STEP-3

セキュリティ上、デフォルトではアセットへのアクセス権がなく、
共有操作によって明示的に許可を与える（GUIあるいはAPI操作に対応）
データセット・分析・ダッシュボードはフォルダーで管理すること推奨（次セクション）



```
{
  "AwsAccountId": "<your aws account>",
  "DataSourceId": "Development-Data-Source",
  "Name": "Development Data Source",
  "Type": "S3",
  "DataSourceParameters": {
    "S3Parameters": {
      "ManifestFileLocation": {
        "Bucket": "quicksight-development-lab-<your aws account>",
        "Key": "S3-development-manifest.json"
      }
    }
  },
  "Permissions": [
    {
      "Principal": "arn:aws:quicksight:us-east-1:<your aws account>:user/default/<your iam user name>",
      "Actions": [
        "quicksight:UpdateDataSourcePermissions",
        "quicksight:DescribeDataSource",
        "quicksight:DescribeDataSourcePermissions",
        "quicksight:PassDataSource",
        "quicksight:UpdateDataSource",
        "quicksight>DeleteDataSource"
      ]
    }
  ]
}
```

各種アセットのアクセス管理

STEP-3

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

IAM

ネームスペース

個別にGUIあるいはAPI操作で権限付与

フォルダー

行レベルセキュリティ

フォルダー管理

STEP-3

組織内でのアセット（データセット/分析/ダッシュボード）をフォルダー機能で効率的に管理。

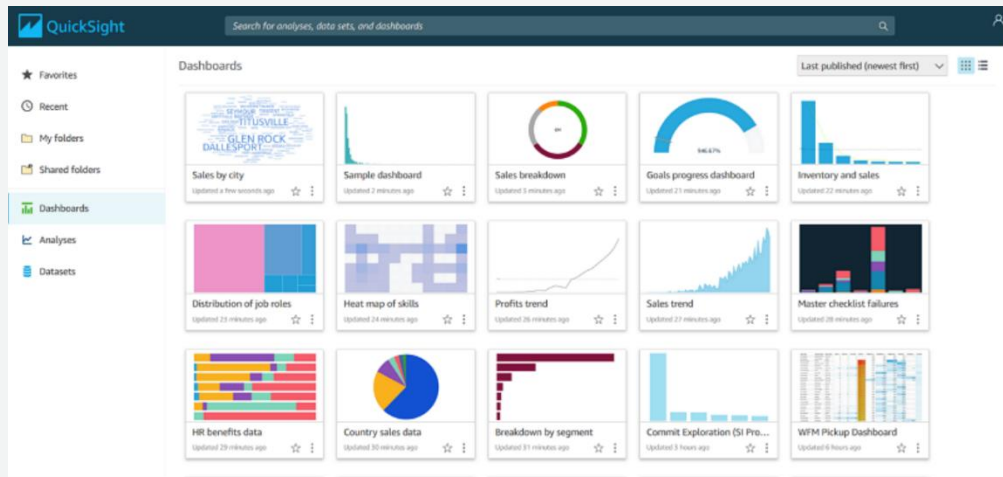
個人フォルダ：Admin/Authorが個人的に管理しやすいよう自由にフォルダーを作成しアセットを格納でき、個人フォルダは別ユーザーからは見えない。

共有フォルダ：フォルダー単位でアセットの共有/権限管理をするのに使う。

共有フォルダではAdmin/Author/ReaderにOwnerあるいはViewerのアクセス権限を付与して管理。

Owner：Admin/Authorに対してフォルダーへのアクセス権限を付与し、アセット（サブフォルダ含む）の追加/削除とユーザー/グループへの共有権限がある。

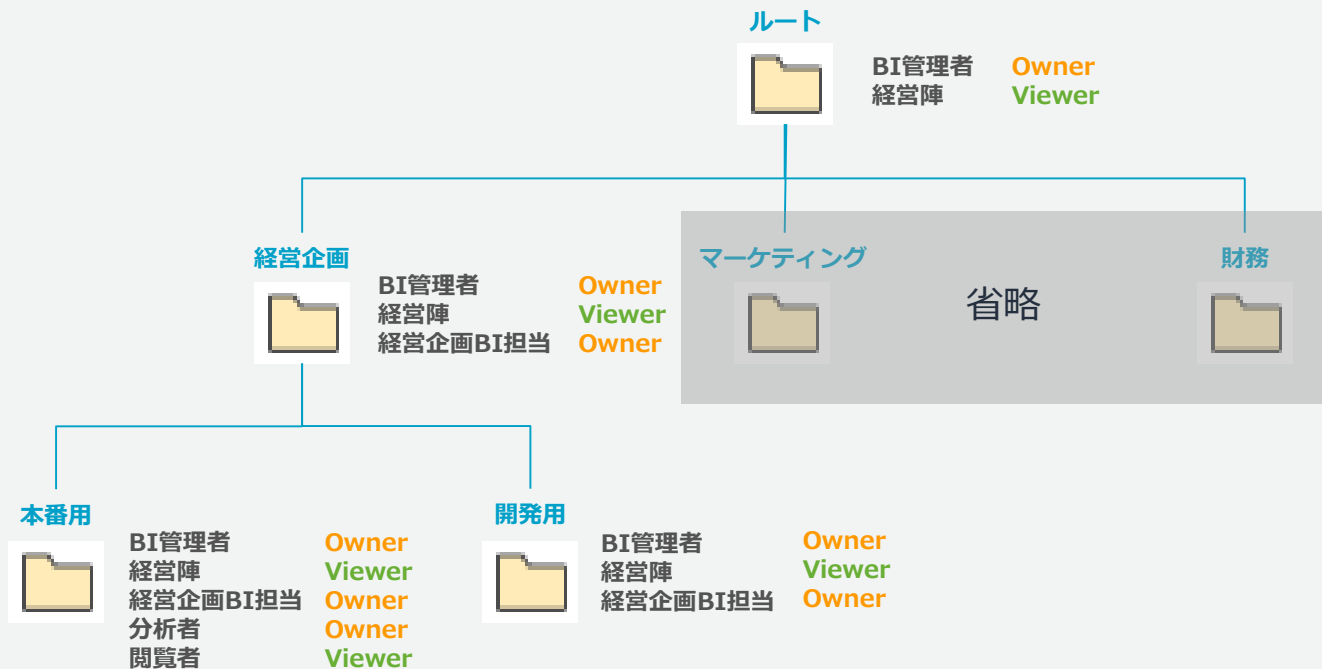
Viewer：Admin/Author/Readerに対して付与でき、フォルダー内のアセットを閲覧するのに限定されている。



Organize and share your content with folders in Amazon QuickSight
<https://aws.amazon.com/jp/blogs/big-data/organize-and-share-your-content-with-folders-in-amazon-quicksight/>

共有フォルダー 構成例

STEP-3



共有フォルダー 管理方法のコツ

STEP-3

共有フォルダーを活用することで煩雑なアセット単位での共有作業をなくし、権限管理の人的ミスも軽減できます。

管理上、初めのQuickSight運用設計時に右図のような階層構造とグループを定義することをお勧めします。

まず最上層の共有フォルダーはAdminのみが作成可能です。

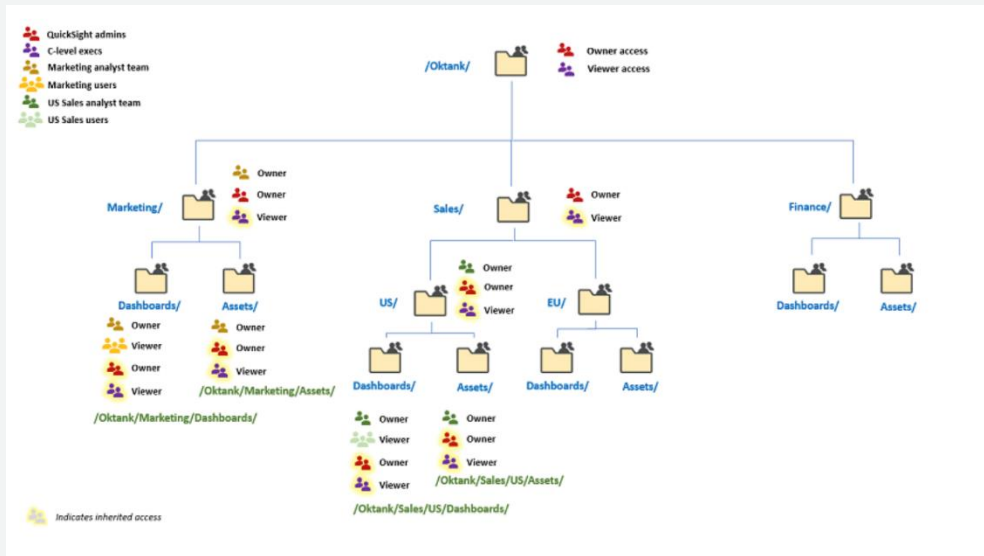
むやみに階層・アセット・アクセス権限が変更されないよう最上層のOwnerは限定することをお勧めします。

都度、新しいフォルダー階層を追加できるよう、運用プロセスおよび基準となる階層を定義することも重要です。

フォルダーの権限はサブフォルダーにも適用されます。

右図の場合、C-level execs（経営陣）は最上層のフォルダーにViewer権限が与えられているため、全フォルダーを見ることは可能ですが、変更を加えることはできません。

全アセットと公開用ダッシュボードのフォルダーを分け、前者へのアクセスを一部Authorに限定することで、重要なアセットや公開用ダッシュボードの間違った操作リスクを軽減できます。極力アクセスを限定したいユーザーは最下層のフォルダにアクセス付与することをお勧めします。



Organize and share your content with folders in Amazon QuickSight
<https://aws.amazon.com/jp/blogs/big-data/organize-and-share-your-content-with-folders-in-amazon-quicksight/>

各種アセットのアクセス管理

STEP-3

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

IAM

ネームスペース

個別にGUIあるいはAPI操作で権限付与

フォルダー

行レベルセキュリティ

マーケティング部と財務部に同じデータセットを適用するが、扱えるデータ範囲を制御したい場合は？

STEP-3

BI管理者

全ダッシュボードの閲覧者

部署単位のユーザー



Admin

orgAdmin

アカウントの作成、
ユーザの追加・削除、
コストなどの総管理者

Reader

orgReader

組織全体の責任を担う
社長や経営陣

Author

markRep/
accounRep

部署毎のダッシュボー
ド作成を担う分析者

Author

orgAuthor

社内全体のデータ・分
析・ダッシュボードを
準備するBIエンジニア

Reader

orgReader

部署を横断して案件を
推進するプロジェクト
マネージャー

Author

markAuthor/
accounAuthor

用途に応じてアドホッ
ク分析する分析者

Reader

markReader/
accounReader

日々の最新データを確
認するデータ閲覧者

データセット上のアクセス範囲をユーザー単位で制御

STEP-3

どのユーザー/グループがどのデータにアクセスできるかをCSVなどのテーブルで定義

Username	Category	State
Jane	Aquatics, Exercise & Fitness, Outdoors	WA, OR
Susan		CA

行レベルセキュリティで対象のデータセットに適用

行レベルのセキュリティを設定

Sales Pipeline

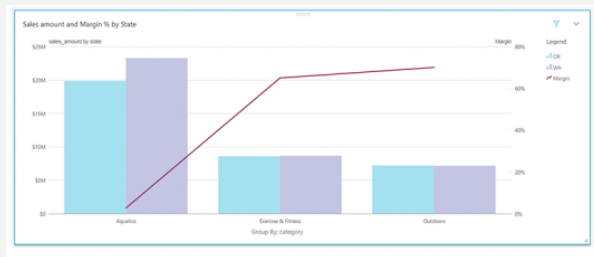
選択されたデータセットルール
なし

- Business Review S3
- People Overview S3
- Web and Social Media Analytics S3
- NS2 Data Set S3
- NS1 Data Set S3
- Default Data Set S3
- DynamicUserDefault-UTF8 ファイル

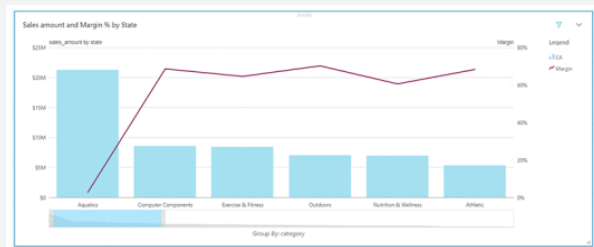
アクセス許可ポリシー:

- データセットへのアクセス権を付与する
- データセットへのアクセス権を拒否する

分析/ダッシュボードに反映



JaneはState=WA or ORが閲覧可能



SusanはState=CAのみ閲覧可能

各種アセットのアクセス管理

STEP-3

各種DB

データ

IAM

 Amazon QuickSight

データソース

データセット

分析

ダッシュボード

ネームスペース

個別にGUIあるいはAPI操作で権限付与

フォルダー

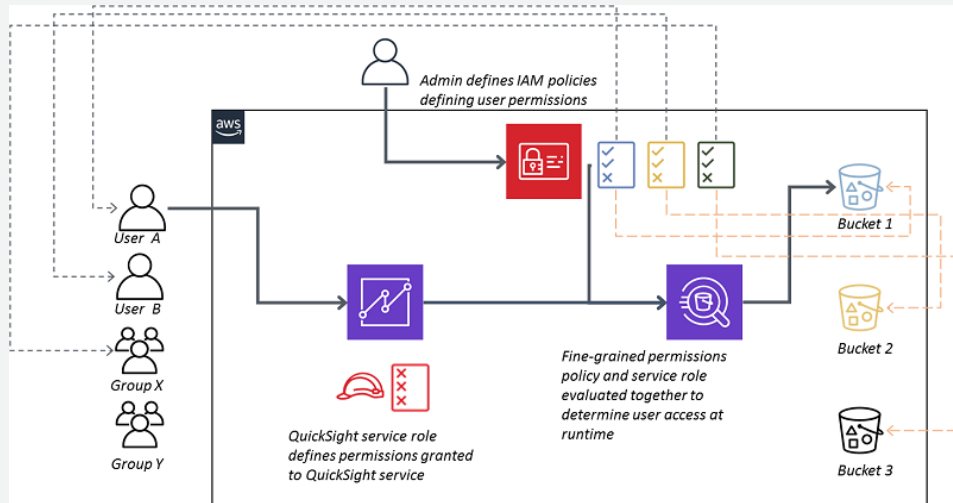
行レベルセキュリティ

各種DBへのアクセスコントロールをIAMで

STEP-3

ユーザがアクセスできるAWSリソース
(S3, Athena, RDS, Redshiftに対応) を
IAMで制限する

IAMポリシーをQuickSightユーザやグ
ループに紐付けておくと、AWSリソース
へのアクセス時に反映される



Introducing Amazon QuickSight fine-grained access control over
Amazon S3 and Amazon Athena
<https://aws.amazon.com/jp/blogs/big-data/introducing-amazon-quicksight-fine-grained-access-control-over-amazon-s3-and-amazon-athena/>

- ユーザーを管理
- お客様のサブスクリプション
- SPICE 容量
- アカウント設定
- セキュリティとアクセス権限**
- VPC 接続の管理
- モバイル設定
- ドメインと埋め込み
- アカウントのカスタマイズ

セキュリティとアクセス権限

QuickSight は、個々のユーザーおよびグループに加えて、アカウント全体の AWS リソースへのアクセスをコントロールできます

QuickSight の AWS のサービスへのアクセス

 Amazon Redshift  Amazon RDS  IAM  Amazon S3  Amazon Athena

AWS のサービスへのアクセスを設定することで、QuickSight はそれらのサービスのデータにアクセスできます。ユーザーとグループによるアクセスは、以下のオプションでコントロールできます。

[追加または削除する](#)

デフォルトのリソースアクセス

① ユーザーおよびグループは接続されているすべてのリソースへのアクセス権限があります。

特定のユーザーまたはグループに対して個々のアクセスコントロールが有効ではない場合に、QuickSight はデフォルトですべてのユーザーおよびグループへのアクセスを許可または拒否することができます。

[変更する](#)

個々のユーザーとグループのリソースへのアクセス

リソースへのアクセスは、IAM ポリシーを割り当てることによってコントロールされます。

[IAM ポリシーの割り当て](#)

実際の運用例 社内用途

STEP-3

各種DB

 Amazon QuickSight

データ

データソース

データセット

分析

ダッシュボード

インフラ担当

BIで可視化するテーブルを各種DB上に準備

 Admin

対象のデータソースをQuickSight上に作成

行レベルセキュリティで各部署が使えるデータ範囲を制御する

各部署の共有フォルダーをDev/Prodに分けて作成し、グループに共有

 Author

BIエンジニアは各部署が自由に使えるデータソースを作成し、各部署の担当Authorに共有

各部署の担当Authorが共有されたデータソースよりカスタムSQLを使って用途に応じたデータセットを作成し、他Authorにフォルダーで共有

共有されたデータセットをデータ準備画面で加工し自由にアドホック分析

全員が使うダッシュボード向けの分析を作成

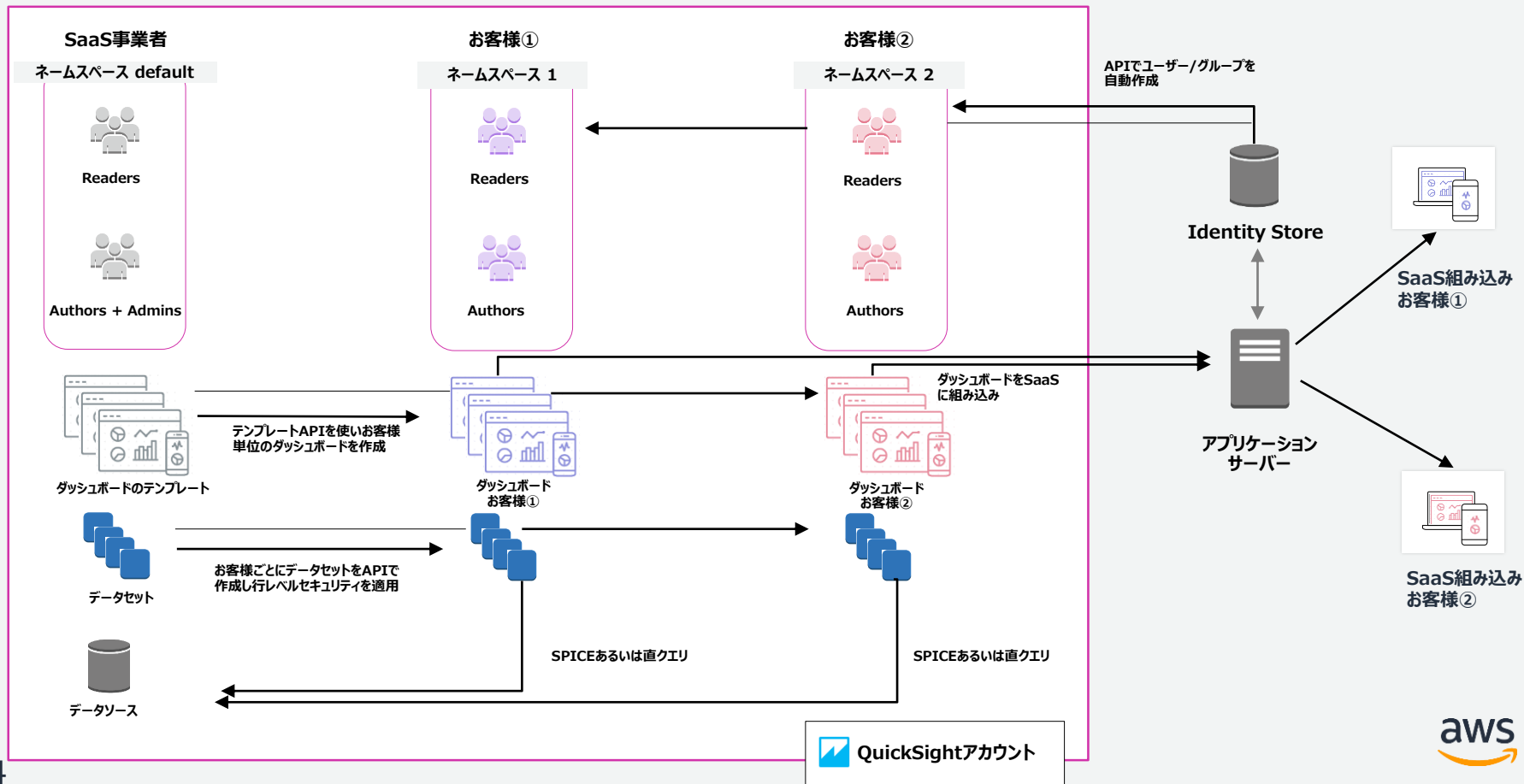
分析をダッシュボード化して部署全体に共有

 Reader

共有されたダッシュボードを使いデータ分析

実際の運用例 SaaSに組み込んで外部提供

STEP-3



まとめ

1 本格運用を始める前に権限管理の枠組みと運用フローを設計！

2 組織のニーズにあった方法を選択！

3 QuickSightで安心・安全なBI運用を！

内容についての注意点

- 本資料では2020年10月14日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(<http://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。
- AWS does not offer binding price quotes. AWS pricing is publicly available and is subject to change in accordance with the AWS Customer Agreement available at <http://aws.amazon.com/agreement/>. Any pricing information included in this document is provided only as an estimate of usage charges for AWS services based on certain information that you have provided. Monthly charges will be based on your actual use of AWS services, and may vary from the estimates provided.