



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[AWS Black Belt Online Seminar]

Amazon QuickSight のBI機能を 独自アプリケーションやSaaSに埋め込む サービスカットシリーズ

Amazon Web Services Japan
Solutions Architect
下佐粉 昭 (Akira Shimosako)
2020/11/17

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



自己紹介

下佐粉 昭 (しもさこ あきら)

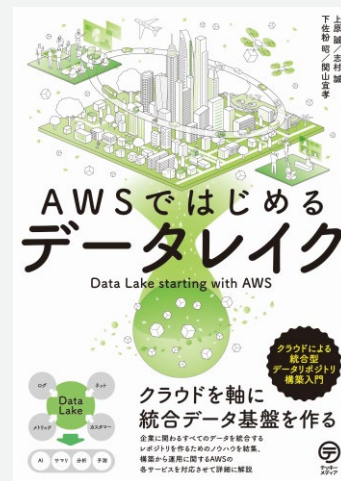
Twitter - [@simosako](https://twitter.com/@simosako)

所属：

アマゾン ウェブ サービス ジャパン
ソリューションアーキテクト

好きなAWSサービス:QuickSight, Redshift, S3 ...

人間が運用等から解放されて楽になるサービスが好きです



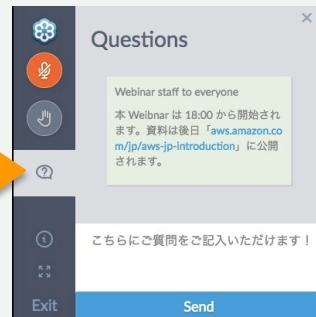
AWS Black Belt Online Seminar とは

「サービス別」「ソリューション別」「業種別」のそれぞれのテーマに分かれて、アマゾンウェブ サービス ジャパン株式会社が主催するオンラインセミナーシリーズです。

質問を投げることができます！

- 書き込んだ質問は、主催者にしか見えません
- 今後のロードマップに関するご質問は
お答えできませんのでご了承下さい

- ① 吹き出しをクリック
- ② 質問を入力
- ③ Sendをクリック



Twitter ハッシュタグは以下をご利用ください
#awsblackbelt

内容についての注意点

- 本資料では2020年11月17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.

内容

- SaaSへのBI機能追加にAmazon QuickSightを選択するメリット
- 認証とID管理
- アプリケーションへの埋め込み
- アクセス制御（認可）の方法
- 関連機能 & Tips

- まとめ

注) 本資料で説明する多くの機能が
QuickSight Enterprise Edition
を前提にしています

補足資料

- 料金体型とエディションの違い

SaaSへのBI機能追加に Amazon QuickSightを 選択するメリット



Amazon QuickSightの特徴



サーバ運用管理不要・オートスケール

サーバやソフトウェアを導入、管理、運用する必要はありません。スモールスタートし、10,000ユーザまでスケール可能



AWSとフル・インテグレーション

AWS内でエンド・ツー・エンドの分析を実現。プライベートVPCにセキュアにアクセス、アクセスコントロール、MLインテグレーション



セキュアかつグローバル利用

エンド・ツー・エンドの暗号化、高可用性設計、グローバル10リージョン展開、HIPAA/PCI/ISO/SOC/FedRamp等適合



容易な開発とメンテナンス

QuickSightでデザインし、APIで連携。行レベル・列レベルセキュリティ制御、SSOによるシームレスな認証



高速で、一貫したパフォーマンス

高速で、常に一貫したパフォーマンスを提供。同時実行ユーザ数が増加しても、サービスがスローダウンしづらい設計



全員が活用できる料金体系

全ユーザに利用権限を与え、使った分だけの支払。事前コスト不要。利用しないユーザのコスト不要



MLインサイト（機械学習インサイト）

コンテキストに関連したインサイトを提供。MLによる異常検出、予測、アラート、カスタマイズ可能なナラティブ



カスタマイズと埋め込み

わずかな時間でアプリケーションに埋め込み、分析を実現。組み込みに膨大な作業は不要。テーマ機能でアプリケーション、企業イメージに適應

管理者

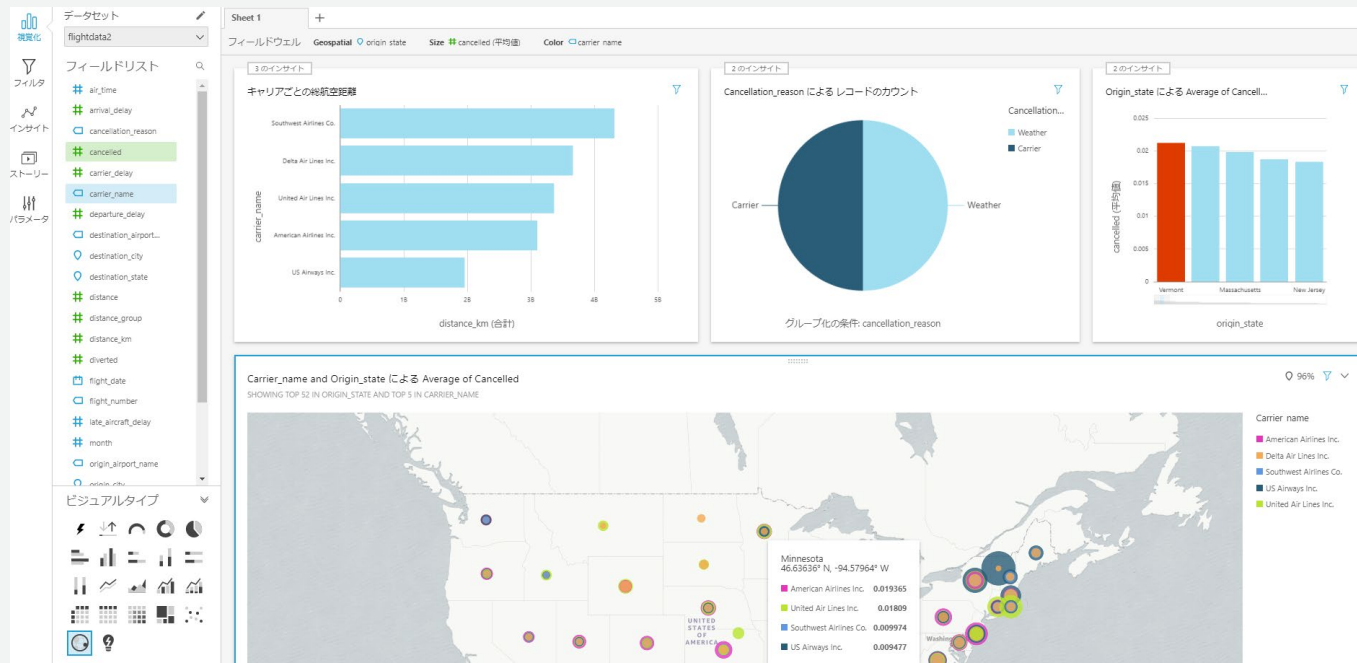


メリット

エンドユーザ

ブラウザのみで全機能が利用可能

利用者も管理者もソフトウェアの導入は不要
ドラッグ&ドロップでの直感的な操作




























※サポートされるブラウザ https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/supported-browsers.html

多様なデータソースに対応

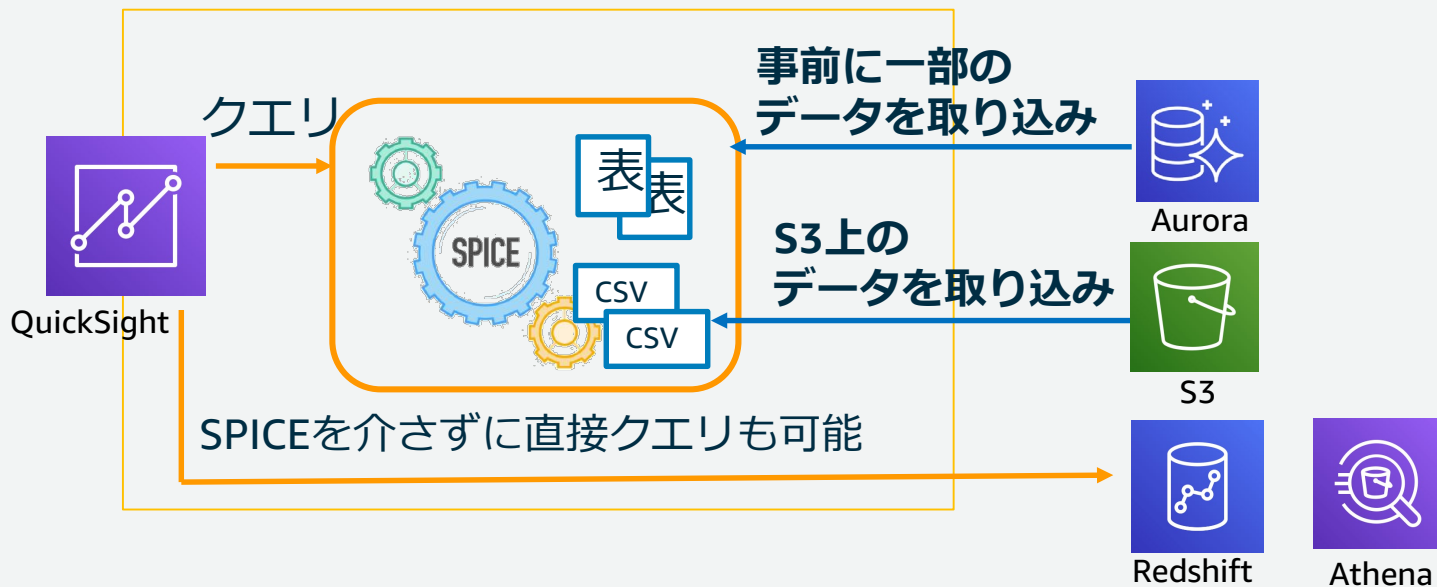
多様なデータソースに標準で対応

以下に無いものは、Amazon AppFlowでS3にデータを取得し、AWS Glueでデータ整形する等の対応をご検討ください

 ファイルのアップロード (.csv, .tsv, .clf, .elf, .xlsx, .json)	 Salesforce Salesforce に接続	 S3 分析	 S3	 Athena
 RDS	 Redshift 自動検出	 Redshift 手動接続	 MySQL	 PostgreSQL
 ORACLE	 SQL Server	 Aurora	 MariaDB	 Presto
 Spark	 Teradata 提供元: Teradata	 Snowflake	 AWS IoT Analytics	 Timestream
 GitHub	 Twitter	 Jira	 ServiceNow	 Adobe Analytics

SPICE : インメモリカラムナデータベース

- サーバレスのインメモリ型データベースを内蔵
- 1データセットあたり最大2.5億行 *まで格納可能
- 既存RDBにBIクエリの負荷がかからない構成が実現可能



*SPICE 1データセットあたりの最大サイズ

- Enterprise Edition : 最大2.5億行 (もしくは500GB)
- Standard Edition : 最大2,500万行 (もしくは25GB)

QuickSight+Athena+S3でフルサーバレスのBIサービス

大規模データであってもサーバレスでBI環境を実現



SaaSの成長に合わせた利用が可能な料金体系

- Enterprise EditionのReaderライセンスは、使った分だけの利用
- 使わなければゼロ円**。最大で\$5/ユーザ/月の上限

Author 

データソース、データセットの作成と共有
ビジュアル、ダッシュボードの作成と共有

\$18

/ ユーザー / 月
年単位契約

\$24 / ユーザー / 月 (月単位契約)

Reader 

共有されたダッシュボードを閲覧

\$0.30 最大で **\$5**

/ セッション* / ユーザー / 月

*1 セッション = ログインから 30 分間

API/CLIによる連携、自動化

JavaScript, Java, .NET(C#), Python 3, CLI をサポート

- ユーザ・グループ操作
- データソース、データセット操作
- SPICE操作
- 埋め込み
- テンプレート

- バージョン管理機能
 - テンプレートとダッシュボードに対応

APIとテーマ

<https://aws.amazon.com/jp/blogs/news/evolve-your-analytics-with-amazon-quickights-new-apis-and-theming-capabilities/>
QuickSight CLI

https://docs.aws.amazon.com/ja_jp/cli/latest/reference/quicksight/index.html

[aws]

quicksight

Description

Amazon QuickSight is a fully managed, serverless business intelligence service for the AWS Cloud that makes it easy to extend data and insights to every user in your organization. This API reference contains documentation for a programming interface that you can use to manage Amazon QuickSight.

Available Commands

- cancel-ingestion
- create-dashboard
- create-data-set
- create-data-source
- create-group
- create-group-membership
- create-iam-policy-assignment
- create-ingestion
- create-template
- create-template-alias
- delete-dashboard
- delete-data-set
- delete-data-source
- delete-group
- delete-group-membership
- delete-iam-policy-assignment
- delete-template
- delete-template-alias
- delete-user
- delete-user-by-principal-id
- describe-dashboard
- describe-dashboard-permissions
- describe-data-set
- describe-data-set-permissions
- describe-data-source
- describe-data-source-permissions
- describe-group
- describe-iam-policy-assignment
- describe-ingestion
- describe-template
- describe-template-alias
- describe-template-permissions
- describe-user

認証とID管理



QuickSightのユーザー分類



Admin

BI環境全体の管理者

- (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、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)
- ※Enterprise Editionでのみ利用可能

QuickSightにおける認証とID管理

QuickSight内におけるID管理は、以下の3つの方法で実現可能

- emailアドレス管理（QuickSight独自）
- IAM
 - フェデレーション (SAML, OpenID Connect)も併用可能
- Active Directory 連携（*本資料では触れません）

emailアドレス管理

概要：

- QuickSight独自のID管理機能
- 外部にID管理機能(IdP)を用意する必要が無いので手軽に始められる
- emailアドレスをIDとする（自社のemailアドレス以外でも可能）
 - 登録したemailアドレスに確認用URLを含むメールが届く

用途：

- SaaS側ですでにemailベースでユーザ管理している場合
- 社内用の小規模な運用
 - 規模が大きくなると手動での管理が負担になる点に注意



IAM (+フェデレーション)

概要 :

- ID管理にAWS IAMの機能を利用する
- IAMユーザがQuickSightに初めてアクセスした際、自動的にプロビジョンする設定（自己プロビジョニング）が可能
- IAMの機能を使った権限調整（fine-grained access control）が可能
- SAML/OpenID Connectを使用したフェデレーションによるSSOが可能
 - 例 : ADFS, Okta, PingFederate, Auth0 ...

用途 :

- SaaS側でIAMユーザベースで管理をしている場合
- SAML 2.0のフェデレーションを利用している、利用する計画である場合
- IAMによるリソースアクセス管理を実施する場合

IAMユーザーの自己プロビジョニング

自己プロビジョニングを許可する場合、以下のIAMポリシーが必要です

Amazon QuickSight の IAM アイデンティティベースのポリシー: ユーザーの作成 (閲覧者ロールの例)

```
{
  "Version": "2012-10-1
  "Statement": [
    {
      "Action": [
        "quicksight:CreateReader"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:quicksight::[自分のアカウントID]:user/${aws:userid}"
      ]
    }
  ],
}
```

Action句の許可によって、自己プロビジョニングによって作成するAmazon QuickSightユーザーの権限が変わります。

Action	Amazon QuickSightロール
quicksight:CreateReader	Readerとして登録
quicksight:CreateUser	Authorとして登録
quicksight:CreateAdmin	Adminとして登録

Resource句を絞ることで、自アカウントのAmazon QuickSightのみに限定します。

参考: Amazon QuickSight の IAM アイデンティティベースのポリシー: ユーザーの作成
https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/iam-policy-examples.html

注: IAMユーザーからの自己プロビジョニングを用いる場合の設定。管理者がユーザー登録(招待)を行う場合は、このAction句は不要です。詳しくはドキュメントを参照下さい。
https://docs.aws.amazon.com/IAM/latest/UserGuide/list_amazonquicksight.html#amazonquicksight-actions-as-permissions

SAML IdPによるSSO設定の流れ①

0. 前準備：IdP環境の構築（サインアップ）、ID、グループの作成...等

1. 相互認証の確立

① SAMLメタデータをAWSサイトからダウンロード

<https://signin.aws.amazon.com/static/saml-metadata.xml>

② 上記SAMLメタデータをIdPにアップロード

リレーステートには <https://qicksight.aws.amazon.com> を指定

ログアウトURLは空白

③ 上記ステップでIdP側のフェデレーションメタデータ(XML)が作成されるのでダウンロード

SAML IdPによるSSO設定の流れ②

2. AWSのIAM IDプロバイダとして登録

- ①IAMコンソールから、IDプロバイダを選択し、SAMLタイプとして登録（前ステップでダウンロードしたフェデレーションメタデータを登録）
- ②IDプロバイダが作成されると、ARNが発行される

3. フェデレーション用のIAM Roleを作成

(*policyに必要なActionについては後述
もしくは下記資料を参照)

※参考：Azure ADとSAML 2.0でSSOする例

<https://aws.amazon.com/jp/blogs/big-data/enabling-amazon-quicksight-federation-with-azure-ad/>

4. IAM Roleの信頼関係IDプロバイダARNを指定 =>

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Federated": "arn:aws:iam::...."
    }
  },
  "Action": "sts:AssumeRoleWithSAML",
  "Condition": {
    "StringEquals": {
      "SAML:aud": "https://signin.aws.amazon.com/saml"
    }
  }
}
```

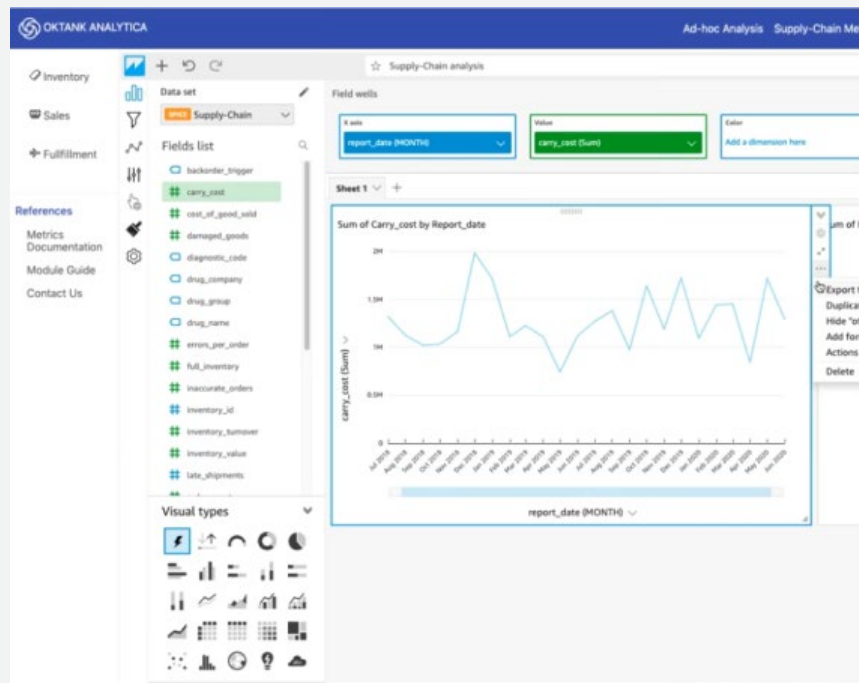
アプリケーションへの 埋め込み



SaaS等アプリへの埋め込み

SaaSやイントラネットのアプリケーションにQuickSightの機能を**埋め込むこと(Embed)**が可能

- ダッシュボード埋め込み
- コンソール埋め込み
- iFrameのURLを取得して埋め込む
- 認証されている状態をSaaS内で実現する必要がある
=>STSでクレデンシャルを取得する**



<https://aws.amazon.com/jp/blogs/news/embed-interactive-dashboards-in-your-application-with-amazon-quicksight/>
<https://docs.aws.amazon.com/quicksight/latest/user/embedding-the-quicksight-console.html>



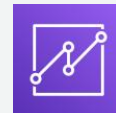
USER



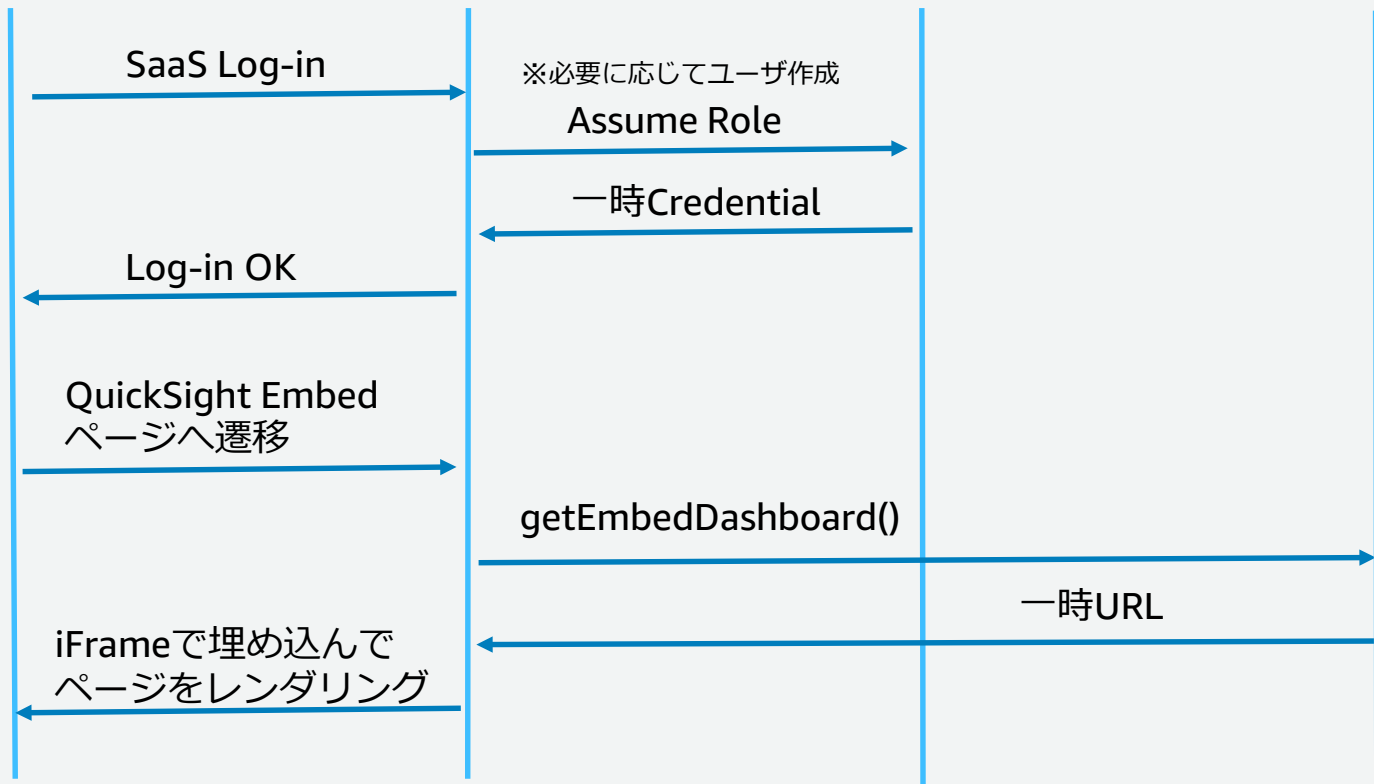
SaaS App



IAM



QuickSight



ステップ①：ドメインの登録(QuickSight)

- 埋め込むドメイン名をQuickSight管理GUIからホワイトリスト登録
- (オプション)必要に応じてグループ等にダッシュボードを共有しておく

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

埋め込みダッシュボードのドメイン管理

埋め込みダッシュボードは、送信元ドメインを明示的に許可している場合にのみ機能します。

ドメイン

https://myapp.example.com/

サブドメインを含める ①

追加

ドメイン

サブドメインを含める

参考：<https://docs.aws.amazon.com/quicksight/latest/user/embedded-dashboards-setup.html>

ステップ②：権限範囲の設定(IAM)

STSのAssumeRoleで呼び出されるIAM Roleを作成する

IAM Roleは1つ以上のIAM Policy（権限セット）で構成される

IAM Policyに最低限必要になるIAM アクション（権限）は以下の通り

- ダッシュボード埋め込みの場合
 - quicksight:RegisterUser - ユーザの動的な登録をする場合に必要
 - quickSight:GetAuthCode - ユーザ管理がQuickSight独自(email)の場合に必要
 - quickSightGetDashboardEmbedURL - ダッシュボードの一時URL取得
- QuickSightコンソールを埋め込む場合 (※Readerユーザは利用不可)
 - quicksight:RegisterUser - ユーザの動的な登録をする場合に必要
 - quickSight:GetAuthCode - ユーザ管理がQuickSight独自(email)の場合に必要
 - quickSight:GetSessionEmbedUrl - コンソールの一時URL取得

補足 : IAM Policyの例

以下のようにIAM Policyを作成し、それを含むIAM Roleを作成しておく
例) 新規ユーザの登録と特定ダッシュボード閲覧のURL取得を許可

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "quicksight:RegisterUser",
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "quicksight:GetDashboardEmbedUrl",
      "Resource": "arn:aws:quicksight:ap-northeast-1:123456789012:dashboard/26a7dcad-1234-5678-90ab-ffeeddccbbaa",
      "Effect": "Allow"
    }
  ]
}
```

補足：SaaSアプリケーション側に必要になる権限

アプリケーション（もしくはバックエンドAPI）が持つIAM Role/Userには、以下のTrust Policyが許可されている必要がある

アプリ側でユーザ管理を行う場合

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::123456789012:role/QuickSightEmbed"
  }
}
```

AssumeRoleを呼び出すためのIAMアクション

前ステップで作成したロール

(補足) SAML 2.0連携環境の場合

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRoleWithSAML",
    "Principal": {"Federated": "arn:aws:iam::ACCOUNT-ID-WITHOUT-HYPHENS:saml-provider/PROVIDER-NAME"},
    "Condition": {"StringEquals": {"SAML:aud": "https://signin.aws.amazon.com/saml"}}
  }
}
```

SAMLでAssumeRoleを呼び出すためのIAMアクション

プロバイダー側に合わせた設定(※)

(※)詳細：https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_create_for-idp_saml.html

ステップ③：認証し、一時URLを取得 (App Server)

例では、role session IDが
QuickSightEmbed/john@example.comになる
これがQuickSight内のIDとしても利用される
(各ユーザでユニークになるようにする)

1. STSでAssumeRole

```
aws sts assume-role --role-arn ¥  
  "arn:aws:iam::123456789012:role/QuickSightEmbed" ¥  
  --role-session-name john@example.com
```

2. (ユーザがまだQuickSight上に存在しないなら) ユーザを動的に作成

※グループへの追加も必要であればcreate-group-membershipで実施 (後述)

```
aws quicksight register-user --aws-account-id 111122223333 ¥  
  --namespace default --identity-type IAM ¥  
  --iam-arn "arn:aws:iam::123456789012:role/QuickSightEmbed" ¥  
  --user-role READER --session-name "john@example.com" ¥  
  --email john@example.com --region ap-northeast-1
```

3. 一時URLを取得

```
aws quicksight get-dashboard-embed-url --aws-account-id 123456789012 ¥  
  --dashboard-id 26a7dcad-1234-5678-90ab-ffeeddccbba9 --identity-type IAM
```

参考：<https://aws.amazon.com/jp/blogs/news/embed-interactive-dashboards-in-your-application-with-amazon-quicksight/>

補足：Userが事前に作成されている場合

QuickSight上にUserが事前に作成されている場合
(User ARNが存在する場合) は、

`aws quicksight describe-user` でuser arnを取得し、

`aws quicksight get-dashboard-embed-url`の引数`--user-arn <...>`
でそのユーザを指定して、一時URLを取得します

ステップ④：埋め込みを実施 (App Server)

```
{
  "Status": "200",
  "EmbedUrl": "https://quicksight.aws.amazon.com/embed/620bef10822743fab329.....",
  "RequestId": "7bee030e-f191-0000-0000-d9faf0e00000"
}
```

取得したURL を埋め込むには、QuickSight Embedding SDKの利用を推奨
<https://www.npmjs.com/package/amazon-quicksight-embedding-sdk>

Embedding SDK (JavaScript)では以下の機能を提供

- ダッシュボードを埋め込むembedDashboard() 関数
- ロケール（言語）設定
- パラメータ（引数）をダッシュボードに引き渡す
- エラーハンドリング

※SDKのサンプルコードは以下を参照

<https://github.com/aws-labs/amazon-quicksight-embedding-sdk>



[参考] 事例 : NFL Next Gen Stats

Player	N...	Team	Season	TTT	Cmp	Att	Cmp %	Pass Yds	Pass TD	INT	Rating	Y/A	A/A	AD/A	TW %	Sep	AYTS	LCAD	QBP	QBP...	ScrYds/Att	Exp Cmp %	Cmp % Above Exp	
Jared Goff																								
Carson Wentz																								
Deshaun Watson																								
Jacoby Brissett																								
C.J. Beathard																								
Joe Flacco																								
Blaine Gabbert																								
Tom Brady																								
Brian Hoyer																								
Matthew Stafford																								
Russell Wilson																								
Derek Carr																								
Matt Ryan																								
Philip Rivers																								
Sean Mannion																								
Ben Roethlisberger																								
Landry Jones																								
Kirk Cousins																								
Drew Brees																								

- NFLの試合におけるリアルタイム情報
- NFL Next Gen Statsポータルに埋め込み
- 32のNFLクラブチームと、配信パートナーにリアルタイムに分析を届けている

"Amazon QuickSightとそのReader料金により、利用しやすく、セキュアでカスタマイズされたダッシュボードを全クラブチームに、サーバの運用管理無しで届けることができます。利用量に応じて支払うだけで良いのです"

*Matt Swensson, Vice President,
Emerging Products and Technology*

アクセス制御（認可） の方法



QuickSight全体のアクセス権限の設定

- ①ではこのアカウントで利用するサービス一覧を定義
- ②デフォルトでは「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」だが、これを「拒否する」にして③で詳細設定することが可能
- ③この定義でIAMベースのアクセス制御(Fine-Grained Access Control) を定義する

QuickSight

アカウント名: hisnakad
エディション: エンタープライズ版

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

セキュリティとアクセス権限

QuickSight は、以下の設定により、アカウント全体からユーザーやグループまでの AWS リソースへのアクセスをコントロールすることができます。

● 接続された製品とサービス

Amazon Redshift Amazon RDS IAM Amazon S3 Amazon Athena Amazon S3 ストレージ分析 AWS IoT Analytics

AWS アカウント内にある S3、Athena およびその他の AWS リソースへの QuickSight アクセスを管理します。

追加または削除する

● ユーザーとグループの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、接続されたリソースへのアクセス権限がありません。以下のアクセスポリシーを設定します。

特定のユーザーまたはグループに対してアクセスポリシー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の許可または拒否を承認できます。

変更する

● ユーザーおよびグループのリソースアクセスポリシー

リソースに対するアクセスをユーザーおよびグループごとに IAM ポリシーを使用して詳細に制御することができます。

IAM の割り当てを管理する

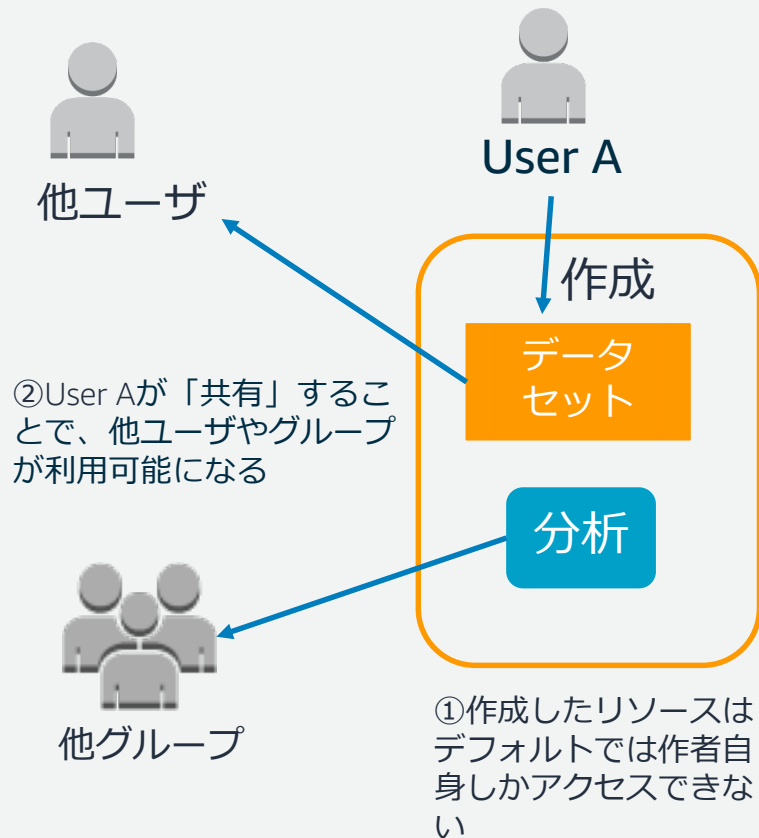
①QuickSightがアクセスできるリソースを定義。ここに定義されないサービスはデータソースとして利用できない

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ポリシーを用いて設定

QuickSightにおける認可の考え方

- QuickSightのアカウント（サインアップ）は1つのAWSアカウント内に1つのみ存在します
- 原則として、リソースを作成直後は作成者しかアクセスできません
- 作成者が「共有」することで、他ユーザがアクセス可能になります
 - ユーザに共有
 - グループに共有
 - 共有フォルダに共有
- 加えて、IAM側での認可の実施も可能（Fine-Grained Access Control）



Authorの権限管理

各Authorの権限を限定する機能

Authorの権限範囲

- データソースの作成・更新
- データセットの作成・更新
- emailレポートの作成
- 各種リソースの共有
- emailレポートのサブスクライブ

例) ISVのAuthorのみデータソース、データセットを作成できるようにし、他のAuthorはそれを使って分析（アナリシス）を作成できるようにする

Create custom permissions

Name

① Use alphanumeric and +,=, @, _ characters. Maximum 64 characters.

Restrictions

- Restrict creating or updating data sources
- Restrict creating or updating datasets
- Restrict creating or updating email reports
- Restrict sharing analyses
- Restrict sharing dashboards
- Restrict sharing datasets
- Restrict subscribing to email reports

Create

グループ機能①

- QuickSight内にグループを作成し、そこにユーザを所属させることが可能
- 認可をグループに与えることで、そのグループに所属するユーザ全員がリソースにアクセス可能になる
- グループは認証の仕組み(email、IAM、AD)とは独立して登録可能
 - ただしAD連携している場合、ADのグループとQuickSightのグループを同期させることが可能
 - ADFSでも要求ルールベースでグループの制御が可能（後述）
- 利用方法：AWS CLIもしくはAPIから



グループ機能② 作成方法 (例)

register.json
(email管理の例)

#ユーザ登録

```
$ aws quicksight register-user --cli-input-json  
file://register.json
```

#グループ作成

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

#グループにユーザを入れる

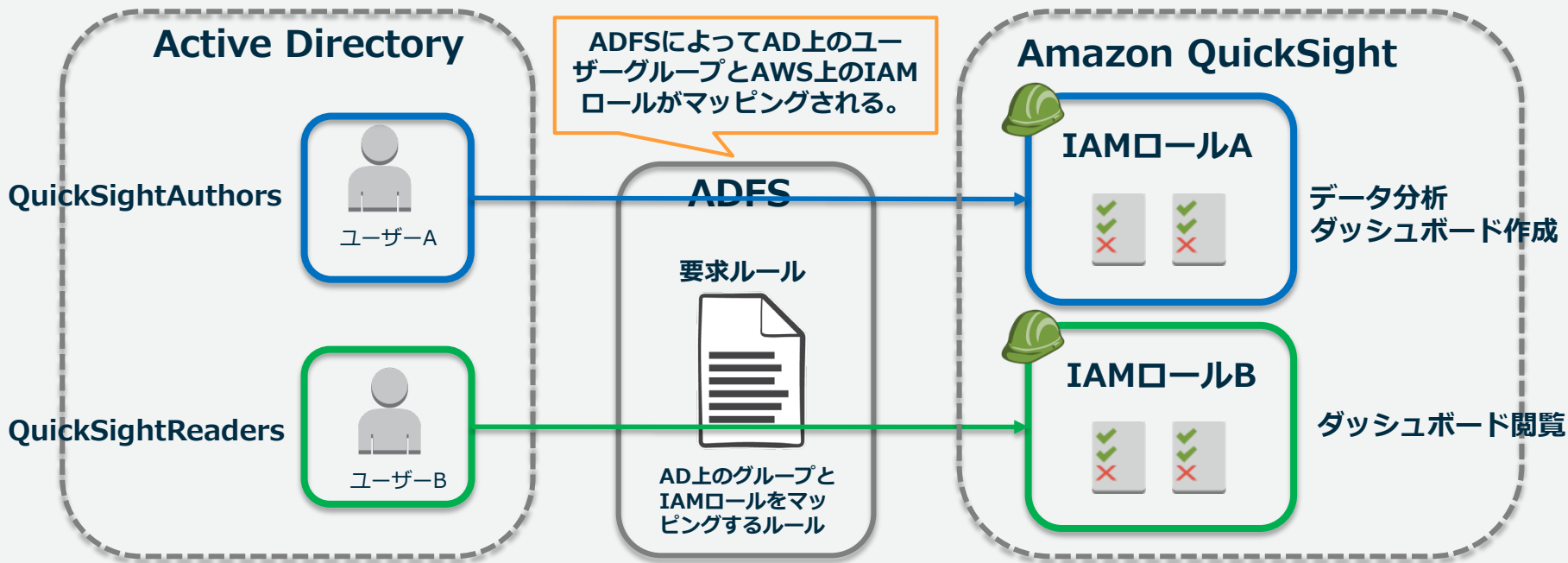
```
$ aws quicksight create-group-membership --aws-  
account-id <your aws account> --namespace 'default'  
--group-name 'group-a' --member-name 'reader-a'
```

```
{  
  "Email": "reader-a@example.com",  
  "UserRole": "READER",  
  "AwsAccountId": "<aws account>",  
  "Namespace": "default",  
  "UserName": "reader-a",  
}
```

参考 - <https://docs.aws.amazon.com/cli/latest/reference/quicksight/index.html>

補足: ADFSでのSSO

AD上のグループとAWS上の権限をマッピング



データセット上のアクセス範囲の制御 行レベルセキュリティ・列レベルセキュリティ

行レベルセキュリティ

- ユーザやグループ単位で閲覧可能な「行」を限定する
- 制御用データセット（表）を作成し、元データセットに適用

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

列レベルセキュリティ

- ユーザやグループ単位で閲覧可能な「列」を限定する
- データセットの設定画面で列を指定する

<input type="checkbox"/> 列名	データ型	アクセス権を持つユーザーとグループ
<input type="checkbox"/> Patient ID	Int	全ユーザー
<input type="checkbox"/> Admit Date	Date	全ユーザー
<input type="checkbox"/> Discharge Date	Date	全ユーザー
<input type="checkbox"/> Priority	String	全ユーザー
<input type="checkbox"/> Hospital	String	全ユーザー
<input type="checkbox"/> Profit	Decimal	simosako
<input type="checkbox"/> Price	Decimal	simosako
<input type="checkbox"/> Cost	Decimal	全ユーザー

共有フォルダーによる認可の実現

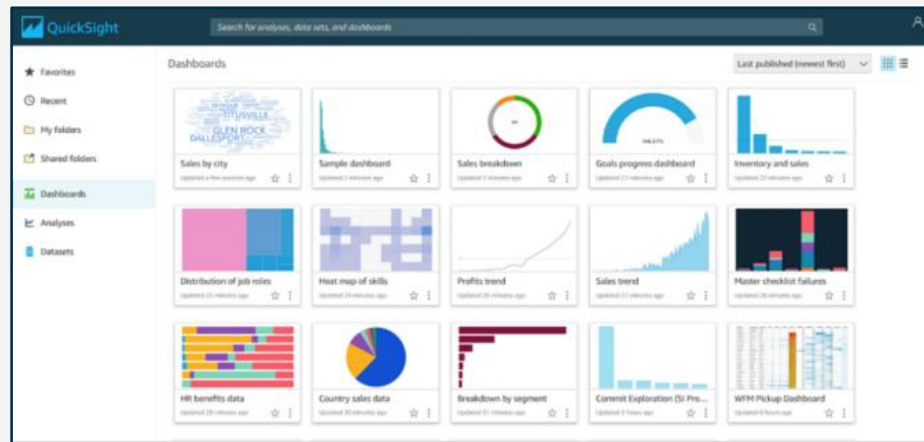
共有フォルダ：フォルダー単位でアセット（ダッシュボードやデータセット等）の共有/権限管理をする

共有フォルダではOwnerあるいはViewerのアクセス権限を付与して管理

親フォルダの権限は子フォルダに引き継がれる

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/>

ネームスペース（名前空間）を使ったマルチテナント構成

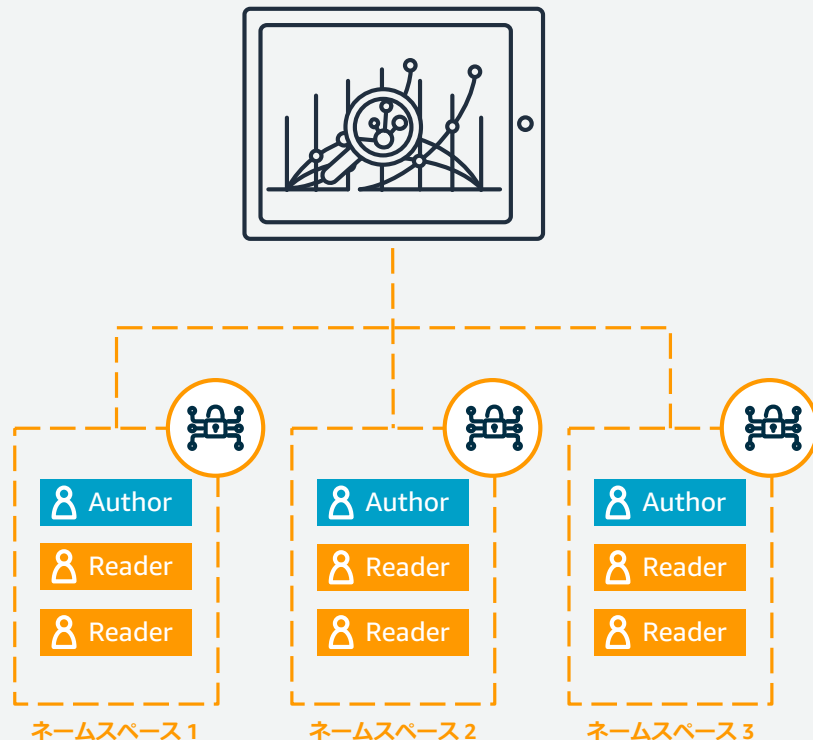
ユーザーおよびアセットを隔離された空間に分離することで、よりセキュアな環境を構築

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

リージョンをまたがって有効

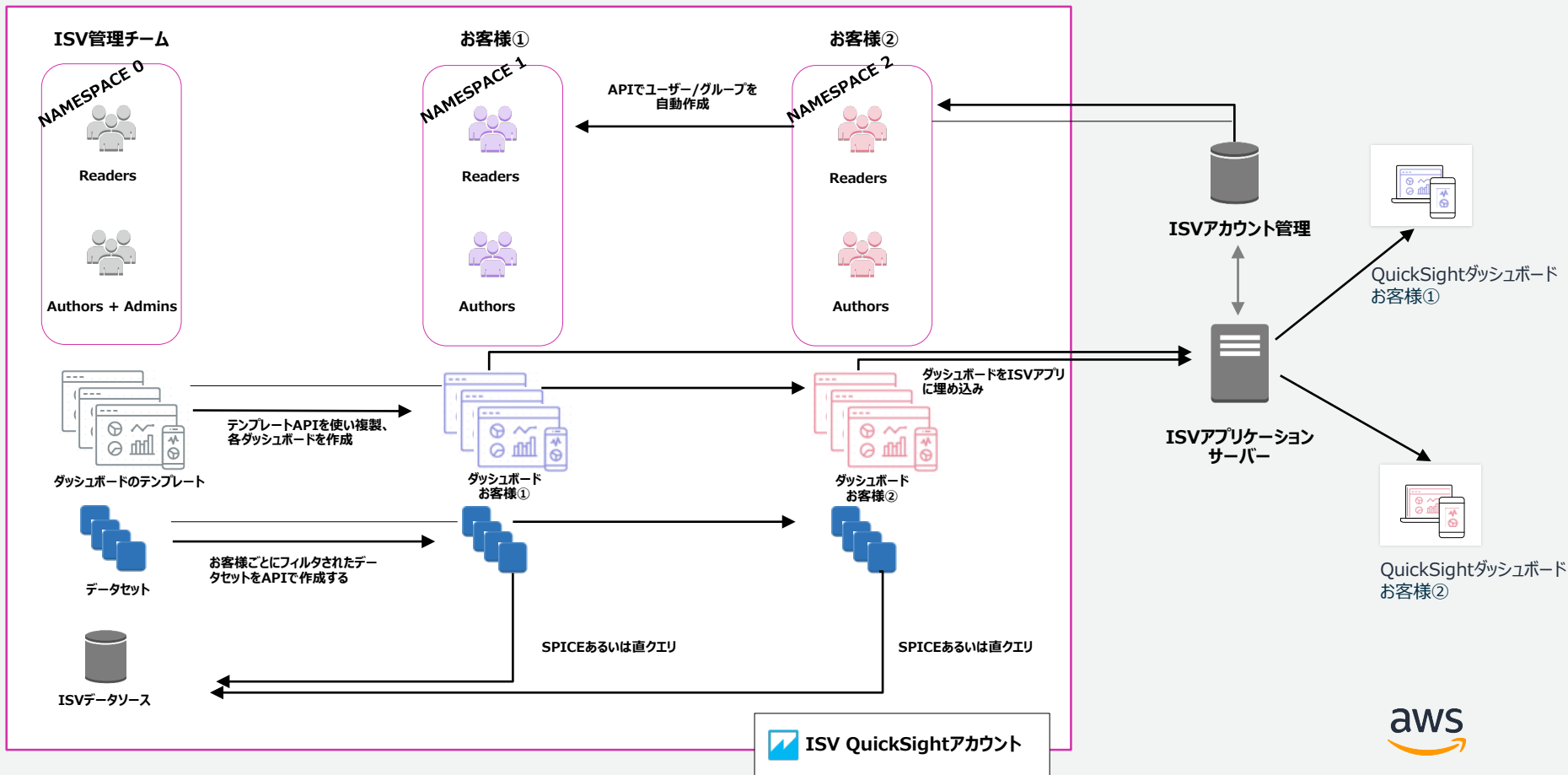
ISVのスーパーユーザがTemplate等を使って各Namespaceに、データセットが異なるダッシュボードを配布することも可能

利用方法：AWS CLIもしくはAPIから



参考：<https://docs.aws.amazon.com/quicksight/latest/user/namespaces.html>

名前空間で分離された環境間では一切の情報共有やユーザー一覧の共有ができない SaaS(ISV)のアカウントは、各名前空間にリソースの共有が可能



補足：ネームスペース（名前空間）利用時の注意点

名前空間には、本資料執筆時点で次の制限・制約があります

- カスタム名前空間(default以外)では以下が未サポート
 - パスワードベースのログイン
 - GUIでログインしたい場合、Federated Single-Sign Onが必須です
 - 資格情報ベースの Active Directory ログイン
 - 行レベルセキュリティ (RLS) を使用するデータセット
- ユーザーをあるネームスペースから別のネームスペースに直接転送することはできません

参照：

https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/namespaces.html

補足：ISV用のSuper Userを登録するスクリプト

全アセットにアクセス権限を持つSuper Userを作成するためのスクリプト

<https://answers.quicksight.aws.amazon.com/sn/articles/6273/script-to-enable-full-object-access-for-admins.html>

※全てのデータにアクセス可能なため、利用には注意が必要です

関連機能 & Tips



アクションを使ってQuickSightからSaaSに連携する

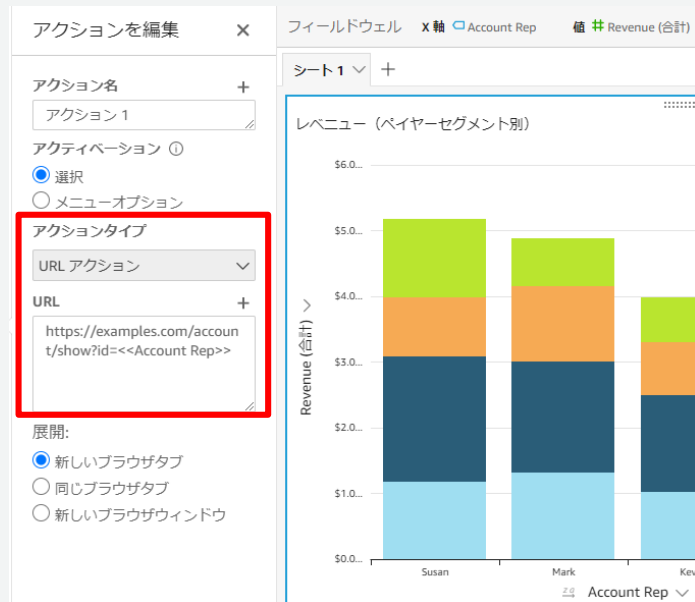
アクション

- ビジュアルをクリックした際に、フィルタ、パラメータ、URLのアクションを作成可能
- URLアクションでは、引数を付けてSaaS等のURLを呼び出す事が可能

例：

<https://examples.com/account/show?id=<<Account Rep>>>

※ここにユーザがクリックしたAccount Rep名が入る



補足：QuickSightダッシュボード間の連携

- QuickSightのダッシュボードは、中のシートごとに個別のURLが提供される
 - URLアクションでダッシュボード間やシート間を移動することが可能
- 各ダッシュボードのパラメータ（変数）には、URLで値を渡すことが可能
 - これによりダッシュボード上でクリックした値を、#p.パラメータ名で指定することで、パラメータに値を渡すことが可能
 - URLの例：

`https://ap-northeast-`

`1.quicksight.aws.amazon.com/sn/dashboards/xxxx/sheets/yyyy#p.rep=<<Account Rep>>`

テーマでシステム間のイメージを統一する

メインカラー、テキストの色、ボーダーの幅等を環境に合わせてカスタマイズ

The image shows a screenshot of an Amazon QuickSight dashboard with several annotations pointing to specific UI elements:

- Selection & hover accents:** Points to the top navigation bar.
- Sheet Background:** Points to the background of the dashboard tiles.
- Visual tile background:** Points to the background of a gauge chart tile.
- Data Colors:** Points to the colors used in a pie chart.
- Text Color:** Points to the text color in a line chart.
- Controls on Dashboard:** Points to the interactive controls on a chart tile.
- COLOR OPTIONS:** A bracket on the right side groups the first five annotations.
- LAYOUT OPTIONS:** A bracket on the right side groups the gutter and page margin annotations.
- Gutter:** Points to the space between dashboard tiles.
- Page margin:** Points to the margin around the dashboard content.
- Visual tile border:** Points to the border of a dashboard tile.

The dashboard itself contains several visualizations:

- Sales Dashboard w/QuickSight 2019:** A header tile with the Amazon logo.
- Sales:** A KPI card showing 687.14M.
- Orders:** A KPI card showing 154.45K.
- Progress to date:** A gauge chart showing 687.14M.
- Sales by State:** A pie chart showing sales distribution by state.
- Sales trend:** A line chart showing sales over time.
- Sales by Age Range:** A bar chart showing sales by age group.
- Sales by Category:** A bar chart showing sales by product category.
- Details by Category:** A table listing product details.

category	sub_category	order_id	sales_am...
Exercise	Hand & Arm Exercisers	5387464	\$37.89
Access...	Women's Cross-body	5387936	\$34.09
Hardware	Mailboxes	5387752	\$100.00
Home	Collectibles	5387780	\$31.00
Fragranc...	Women's	5387792	\$62.00
Outdoors	Climbing Equipment	5387794	\$10.95
Fragranc...	Men's	5387844	\$70.00
Arts & Kits	Kits	5387802	\$20.00
Arts & Kits	Kits	5387800	\$2.99
Outdoors	Water Bottles	5387872	\$22.95
Arts & Kits	Kits	5387802	\$16.99
Home	Candles	5387802	\$38.00
Electrical	Heating & Accessories	5387894	\$70.55
Washes	Combs/Packs	5387890	\$17.99
Washes	Washes	5387890	\$17.99

<https://aws.amazon.com/jp/blogs/news/evolve-your-analytics-with-amazon-quicksights-new-api-and-theming-capabilities/>

ダークテーマ適用例



ダッシュボードのAWSアカウント間転送

- 現時点ではQuickSightには異なるAWSアカウント間でリソースを転送する機能はありません
- しかし一旦ダッシュボードからテンプレートを作成し、テンプレートのArnのパーミッションに別アカウントのプリンシパルからのアクセスを許可することで、そのテンプレートをもとに、別アカウントへダッシュボードが作成可能になります
- 詳細なステップは以下のURLを参照ください
 - <https://answers.quicksight.aws.amazon.com/sn/articles/5721/cross-account-dashboard-copy-with-apis.html>

QuickSight

QuickSightはクラウドネイティブに作られた分析サービス
メンテナンス不要、高速でスケーラブル、埋め込み可能
お客様のリクエストで今後も新機能を追加予定です



Native AWS
service



No server licensing
or maintenance costs



Pay-as-you-go



Scalable,
fast, easy



No deployment
time

Try it free Today @
[Quicksight.AWS](https://quicksight.aws)

Q&A

お答えできなかったご質問については

AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて

後日掲載します

AWS の日本語資料の場所「AWS 資料」で検索



The screenshot shows the AWS Japanese website header with the AWS logo, navigation links for '日本語' (Japanese), 'アカウント' (Account), and 'サポート' (Support), and a 'サインイン' (Sign In) button. Below the header is a navigation menu with links for '製品' (Products), 'ソリューション' (Solutions), '料金' (Pricing), 'ドキュメント' (Documentation), '学習' (Learning), 'パートナー' (Partners), 'AWS Marketplace', and 'その他' (Other). The main content area features the title 'AWS クラウドサービス活用資料集トップ' (AWS Cloud Service Usage Resource Collection Top) and a paragraph of introductory text. At the bottom, there are four buttons: 'AWS Webinar お申込' (AWS Webinar Registration), 'AWS 初心者向け' (AWS for Beginners), '業種・ソリューション別資料' (Resources by Industry/Solution), and 'サービス別資料' (Resources by Service).

aws

日本語 サポート アカウント

サインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

AWS Webinar お申込 »

AWS 初心者向け »

業種・ソリューション別資料 »

サービス別資料 »

<https://amzn.to/JPArchive>

ご視聴ありがとうございました

AWS 公式 Webinar

<https://amzn.to/JPWebinar>



過去資料

<https://amzn.to/JPArchive>



補足資料 エディションと料金



※料金は資料作成時のものです
最新の情報は以下のURLでご確認ください
<https://aws.amazon.com/quicksight/pricing/>

エンタープライズエディション

組織全体にスケールする形でインサイトを共有

Author



Reader



ダッシュボードを作成して公開

\$18

/ ユーザー / 月

年単位契約

\$24 / ユーザー / 月 (月単位契約)

作成済みダッシュボードを閲覧

\$0.30 最大で **\$5**

/ セッション*

/ ユーザー / 月

*1 セッション = ログインから 30 分間

* Authorユーザーあたり 10 GB の SPICE容量が付属

* SPICE 追加容量 1 GB あたり 0.38 USD

© 2020, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



エンタープライズエディションで利用可能な セッションキャパシティ料金

Readerが多い利用ケースのため、
セッション単価をさらに下げるオ
プションを提供可能

(Enterprise Editionで、Reader
にのみ適用可能)

セッション数が多くなるに従って、
ディスカウントが適用 (次ペー
ジ)

※管理コンソールからは切り替えできませんので、
AWSまでお問い合わせください

Reader



作成済みダッシュボードを閲覧

200,000セッション/年を利用可能な
セッションキャパシティ料金

\$4,800/月

*1 セッション = ログインから 30 分間

*1年間単位の支払い

セッションキャパシティ料金の詳細

年間セッションキャパシティー	月額 (年払い)	年間契約合計	セッション毎の超過料金
200,000	4,800 USD	57,600 USD	0.30 USD
400,000	8,000 USD	96,000 USD	0.24 USD
800,000	13,500 USD	162,000 USD	0.20 USD
1,600,000	21,500 USD	258,000 USD	0.16 USD
3,000,000+	<u>お問い合わせください</u>		

※管理コンソールからは切り替えできませんので、AWSまでお問い合わせください

スタンダードエディション

小規模なチームでデータを探索・分析するのに最適なプラン

Author

ダッシュボードを作成して公開

\$9

/ ユーザー / 月

年単位契約

\$12 / ユーザー / 月 (月単位契約)

- * ユーザーあたり 10 GB の SPICE 容量
- * SPICE 追加容量 1 GB あたり 0.25 USD
- * Reader料金は利用不可

エディション比較 (抜粋)

	スタンダードエディション	エンタープライズエディション
料金 (Author)	1ユーザあたり9USD (年間契約) もしくは12USD (月契約)	1ユーザあたり18USD (年間契約) もしくは24USD (月契約)
料金 (Reader)	(※StandardではReader利用不可)	1セッションあたり0.30USD(最大5USD/ユーザ/月) ※セッション単位料金も適用可能
SPICE	1データセット最大2500万行(最大25GB)	1データセット最大2.5億行(最大500GB)
認証	Local (QS独自) Federated SSO (SAML経由) IAM	スタンダード・エディションの全ての方法 + Active Directory連携

以下の機能はエンタープライズエディションのみ利用可能

- 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
- 暗号化
- グループ管理
- Readerプライス
- SPICEの1時間単位リフレッシュ
- Eメールレポート
- VPC内部へのセキュアなアクセス
- ダッシュボード埋め込み
- API
- 機械学習 (ML) インサイト
- テーマ
- テンプレート
- 共有フォルダ

※2020年11月時点の一部抜粋。詳細は以下URLを参照
<https://aws.amazon.com/quicksight/pricing/>

QuickSightを無料で利用する

Free Trial（試用期間）

- Standard EditionやEnterprise Editionを60日間無料で試用可能
 - 正確には2回の支払い締め日を迎えるまで利用可能
- SPICEを10GB利用可能
- 試用期間中のユーザ数は合計4名まで

Free Tier（無料枠）

- 無料で期限無しに利用し続けることが可能
- SPICEを1GB利用可能
- 無料枠で利用可能なユーザ数は1アカウントあたり1名のみ
- SPICEが不足した場合は利用料金を払うことで容量を追加可能

参考情報

Amazon QuickSightホームページ

<https://aws.amazon.com/jp/quicksight/>

Amazon QuickSightドキュメント

https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/welcome.html

Amazon QuickSight ギャラリー（ダッシュボードのサンプルが確認できます）

<https://aws.amazon.com/jp/quicksight/gallery/>

Amazon QuickSight 更新履歴

https://docs.aws.amazon.com/ja_jp/quicksight/latest/user/WhatsNew.html

Amazon QuickSight 使い方動画

<https://www.youtube.com/channel/UCqtl0cKSreCwUUuK0IA1tow> （最新情報はこちら）
<https://aws.amazon.com/jp/quicksight/resource-library/product-videos/> （日本語字幕付き）

Amazon QuickSightハンズオン資料（3種類）

<https://aws.amazon.com/jp/blogs/news/amazon-quicksight-handson-202006/>

Amazon QuickSight 埋め込みAuthor機能のハンズオン（英語）

<https://author-embed-workshop.learnquicksight.online/index.html>