ハンズオン

- ハンズオンの準備
- Amazon Bedrockを試してみよう
- Amazon Q Businessのアプリを作ってRAGを体験してみよう

01 ハンズオンの準備

ハンズオンの準備として以下の作業を行います。

- **ルートユーザーのMFA設定**
- **作業用IAMユーザーの作成**
- **Amazon Bedrockで使用するモデルの有効化**

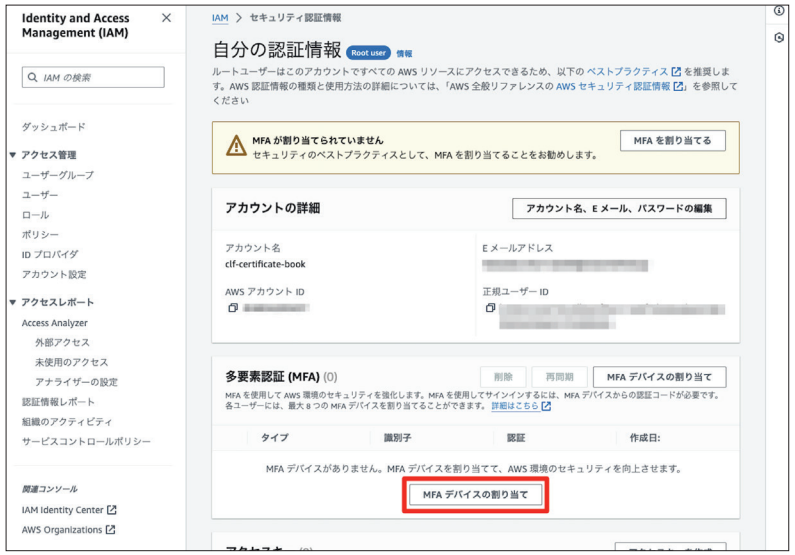
ルートユーザーのMFA設定

6章「AIシステムの管理とAWSのサービス紹介」にあるIAMのご説明で少し紹介をしましたが、AWSのアカウントを発行し最初に使用するユーザーをルートユーザーと呼びます。ルートユーザーはアカウント内の全権限や支払い情報なども扱えるアカウントとなりますので普段AWSを運用する上で使用することは非推奨となっています。そのため、まずAWSのアカウントを開設したらやるべきことはルートユーザーの保護となります。

ルートユーザーの保護対策として有効なのがMFAです。MFAとは、Multi-Factor Authenticationのことで、多要素認証とも呼ばれます。ログインで使用するEメールアドレスとパスワードとは別の認証要素を追加することで、万が一認証情報が流出してしまってもアカウントが乗っ取られることを防ぎます。それでは設定を進めていきましょう。

AWSマネジメントコンソールを開き、右上のアカウント名をクリックします（1）。ナビゲーションが開きますので、その中にある**セキュリティ認証情報**を選択してください（2）。

以下画像の画面に切り替わりますので、**MFAデバイスの割り当て**をクリックします。



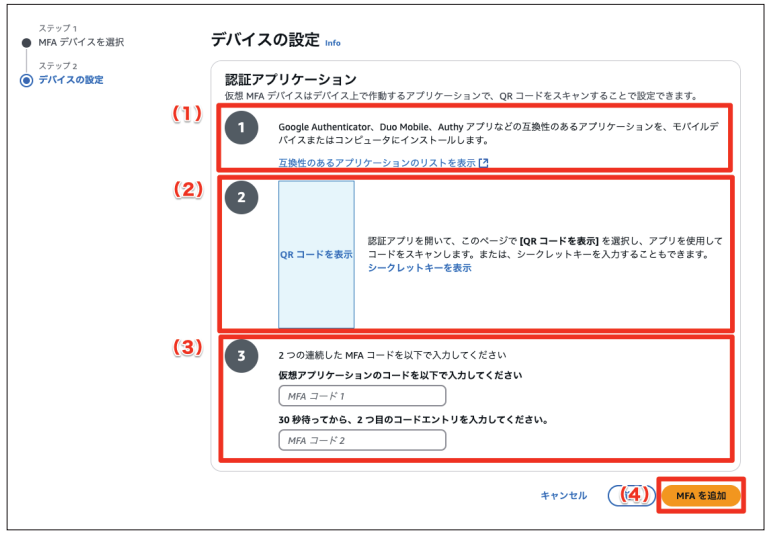
MFAデバイスを登録する画面に切り替わります。MFAデバイスはいくつか選択できるのですが、今回はスマートフォンでも使用可能な仮想認証アプリケーション（Authenticator app）を採用します。仮想認証アプリケーションはGoogle Authenticatorが扱いやすくお勧めです。アプリケーションの細かい操作説明は本書では割愛しますが詳しく知りたい方は以下のブログを併せてご参照ください。

Webサイト

『AWS IAM MFAをスマートフォンで設定する方法』| DevelopersIO
https://dev.classmethod.jp/articles/set-up-aws-mfa-on-my-smartphone/

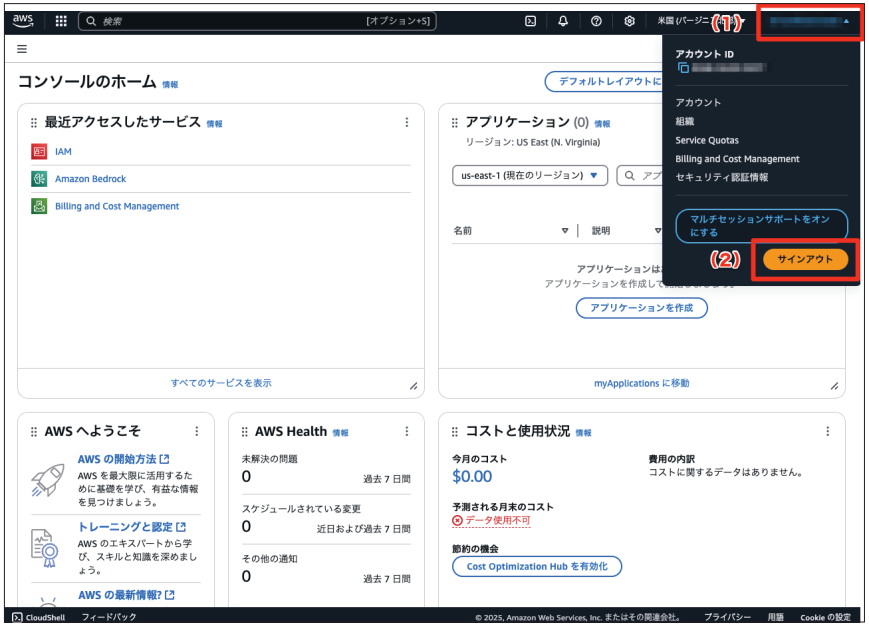
まずデバイス名を入力します（1）。ここではaif-certificate-book-mfaとします。続いてMFAデバイスを選択するので**認証アプリケーション**を選択します（2）。**次へ**をクリックして次の画面に進みます（3）。

仮想認証アプリケーションの準備をします。ここについてはAWSマネジメントコンソール上での操作は不要です（1）。**QRコードを表示**をクリックするとQRコードが表示されるので仮想認証アプリケーションからQRコードを読み取ります（2）。仮想認証アプリケーションでQRコードが正しく読み込めると数字（MFAコード）が表示されるので、それを連続して2回入力します（3）。完了したら**MFAを追加**をクリックします（4）。



正しくMFAが設定できると成功メッセージと、多要素認証（MFA）に登録したMFAが表示されます。

では実際にMFAが設定できているか確認するため、ログアウト後に再ログインしてみましょう。画面右上のアカウント名をクリックします（1）。**サインアウト**のボタンが表示されるのでこちらをクリックします（2）。



無事にログアウトできたらルートユーザーでログインしてみましょう。以下画像のようにMFAコードの入力を求められたらMFAの設定完了です。仮想認証アプリケーションで表示されるMFAコードを入力してログインしましょう[注1]。

注1　2024年12月執筆現在、ログイン画面（サインインUI）は新旧どちらかが表示されます。本ハンズオンにおいては新画面を使用しております。

作業用のIAMユーザーの作成

ルートユーザーの保護ができたら作業用のIAMユーザーを作成します。IAMユーザーとは6章「AIシステムの管理とAWSのサービス紹介」にあるIAMの中で先述した通りAWSアカウント内で作成されるユーザーアカウントです。ルートユーザーは普段AWSを運用する上で使用することは非推奨となっていますので、保護を行ったら普段は使わないようにします。

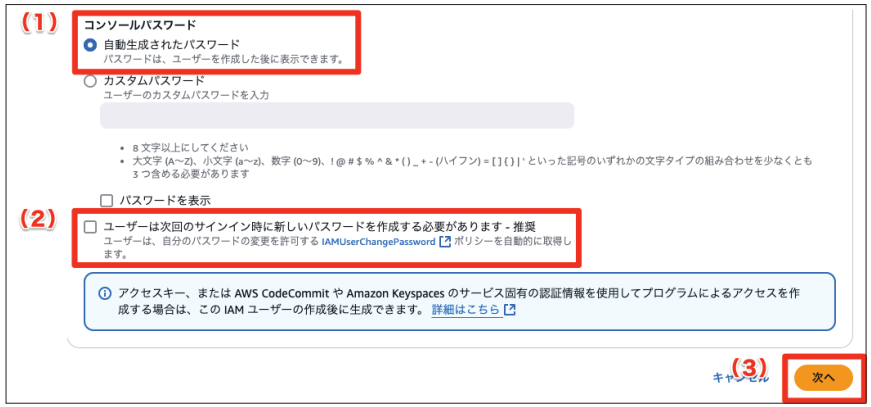
では、作業用のIAMユーザーを作成していきましょう。AWSマネジメントコンソールの上部に検索ボックスがあります。そこにIAMと入力し検索を行います（1）。IAMサービス画面へのリンクが出てきますのでこちらをクリックします（2）。

IAMサービスページのトップは以下画像のようになっています。左側のナビゲーションメニューより**ユーザー**を選択してください。

ユーザーの画面に**ユーザーの作成**というボタンがありますのでこちらをクリックします。

ユーザー名を入力するボックスがありますので、使用可能な文字の規則に従ってユーザー名を入力します。ここでは「aif-hendson-user」としました（1）。続いて、**人にコンソールアクセスを提供していますか？**の質問に対し、**IAMユーザーを作成します**のチェックボックスにチェックを入れます。

コンソールパスワードは、**自動生成されたパスワード**を選択します（1）。次回、作成したIAMユーザーでログインした際に、パスワードを変更させることを強制するオプションがありますが、今回はチェックを入れません。**ユーザーは次回のサインイン時に新しいパスワードを作成する必要があります - 推奨**のチェックを外してください（2）。**次へ**をクリックします（3）。



許可を設定の画面ではユーザーに付与する権限の設定を行います。具体的には６章「AIシステムの管理とAWSのサービス紹介」にあるIAMの中で先述したIAMポリシーをIAMユーザーにアタッチしていく作業になります。

許可のオプションにて、**ポリシーを直接アタッチする**を選択します（1）。許可ポリシーの中に検索ボックスがあるので対象のポリシーを検索して（2）、チェックボックスにチェックを入れます（3）。本ハンズオンでは以下のポリシーを選択します。

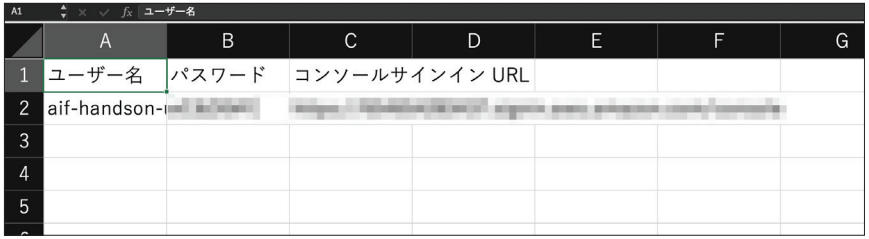
●AdministratorAccess

チェックを入れ終わったら画面下にある**次へ**をクリックします（4）。

作成するユーザーの情報に誤りがないことを確認し、**ユーザーの作成**をクリックします。

正しくユーザーが作成されると以下の画面が表示されます。本画面で作成したIAMユーザーを使用してログインするための情報が表示されてはいるのですが、筆者はcsvファイルをダウンロードしておくことを推奨します（1）。csvファイルをダウンロードしたら、**ユーザーリストに戻る**をクリックしましょう（2）。

csvファイルについて簡単にご紹介しますと、csvとはComma Separated Valuesの略で、カンマ（,）で各項目が区切られたテキストデータのことを指します。なのでエクセルのような表計算アプリケーションで開くことができます。今回ダウンロードしたIAMユーザーのcsvファイルの中には以下の画像のようにユーザー名とパスワード、そしてログインのためのURLが記載されていますのでこの情報を元にIAMユーザーとしてAWSマネジメントコンソールにログインしましょう。



ここまで作業できたらルートユーザーはもう使用しませんので、先ほどの手順でログアウトしましょう。次はIAMユーザーとしてサインインを行います。IAMユーザーのcsvファイルに書かれていたコンソールサインインURLにアクセスしましょう。

すると以下の画像のようにアカウントIDが既に入った状態でログイン画面が表示されますので、IAMユーザーのcsvファイルに書かれていたユーザー名とパスワードを使ってログインします。

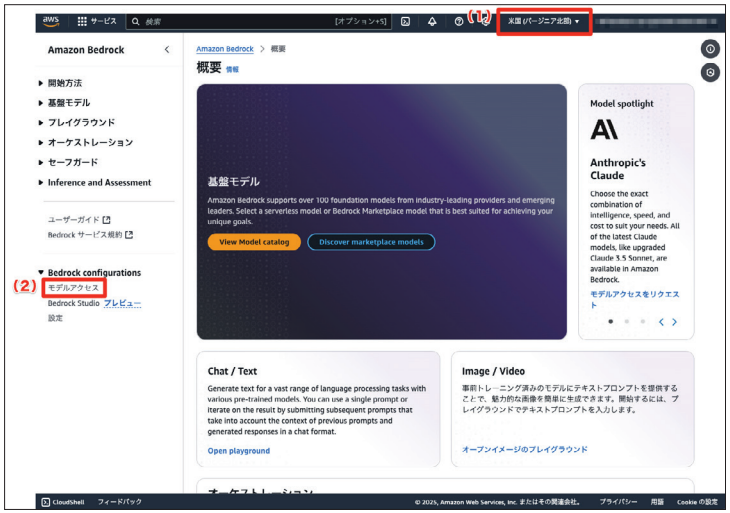
ログインが完了したらこのIAMユーザーにもMFAを設定しましょう。IAMのサービスページトップに遷移しますと、**MFAを自分用に追加**という項目がありますのでここから先ほどのルートユーザーと同様にMFAの設定を進めてください。

Amazon Bedrockで使用するモデルの有効化

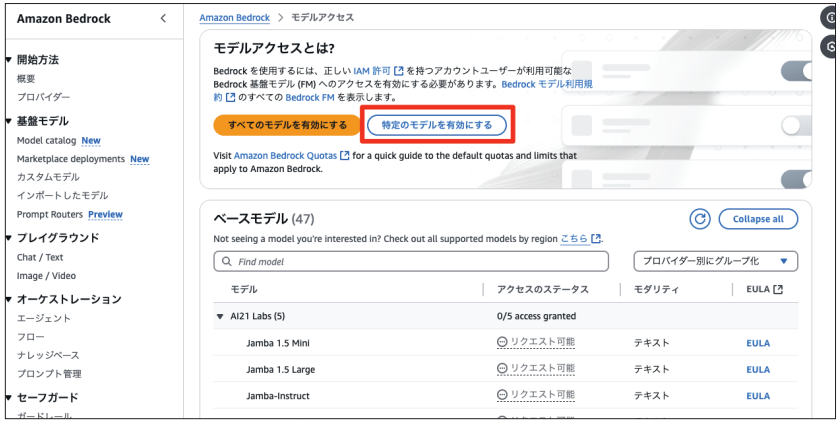
Amazon Bedrockは様々な基盤モデルを提供してくれるサービスですが、最初にモデルアクセスの有効化を行う必要があります。まずはIAMの時と同様にAWSマネジメントコンソールの上部に検索ボックスがありますので、そこにbedrockと入力し（1）、検索にヒットしたAmazon Bedrockのリンクをクリックしましょう（2）。

Amazon Bedrockのトップ画面に遷移したら、まずはリージョンを確認します（1）。

米国（バージニア北部）リージョンになっていることを確認したら左側のナビゲーションメニューの中にある**モデルアクセス**をクリックします（2）。



Amazon Bedrockのモデルアクセストップ画面にくると、利用可能な基盤モデルが並んでいます。本ハンズオンでは個別にモデルを有効化しますので、**特定のモデルを有効にする**をクリックしてください。



基盤モデルは検索ボックスより検索が行えるようになっています（1）。検索後、有効化したいモデルにチェックを入れます（2）。本ハンズオンでは以下のモデルを有効化します。

- **Claude 3.5 Sonnet v2**
- **Titan Text G1 - Express**
- **SDXL 1.0**

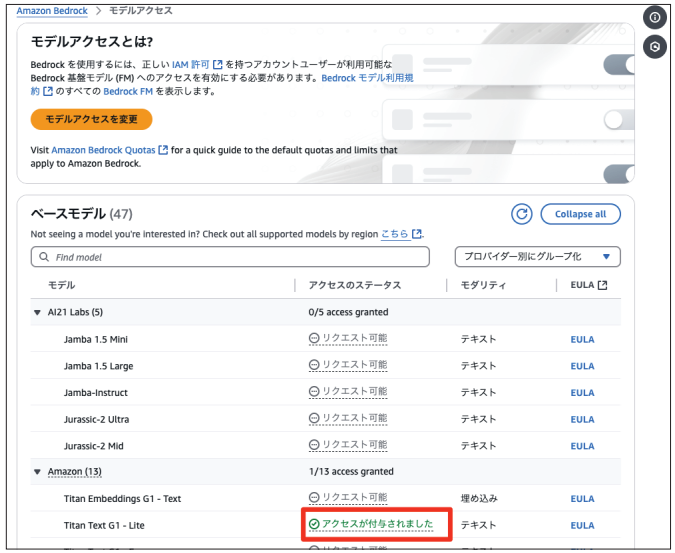
対象のモデル全てにチェックを入れたら**次へ**をクリックします（3）。

Anthropic 用にユースケースの詳細を追加の画面に遷移しますので、以下の情報を入力してください。ユースケースの説明は「検証のため」と入力します。

- **会社名**
- **会社のウェブサイトの URL**
- **どの業界で事業を行っていますか？**
- **対象ユーザーは誰ですか？**
- **ユースケースの説明を入力してください（PII や IP 情報は共有しないでください）。**

最後に確認画面が表示されますので、内容に誤りがないことと利用規約を確認し送信ボタンをクリックします。

しばらくすると対象モデルへのアクセス権が付与されます。アクセス権付与の確認はモデルアクセストップ画面より確認が可能です。



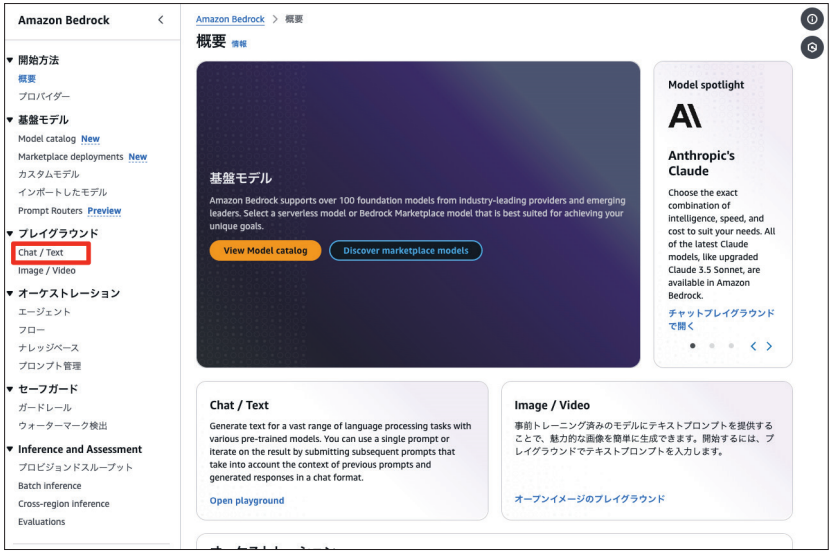
02 Amazon Bedrockを試してみよう

Amazon Bedrockは5章「AWSのAI関連サービス」の中でご紹介した生成AI系アプリケーションを作るための開発者向けAIサービスです。開発者向けとある通り、生成AIアプリケーションを開発するにあたって様々な便利な機能を提供したり他のAWSリソースとの連携が容易に行えたりするところが最大の魅力ではあるのですが、いくつかの機能は実際に開発を行わなくてもマネジメントコンソールから簡単に扱うことができます。その中でも、実用的なものをピックアップして読者の皆様にお届けします。

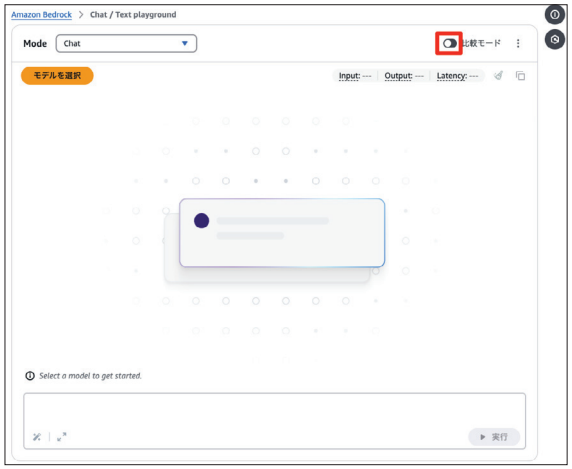
2つの基盤モデルを比較してみよう

基盤モデルの比較及び検討を行う際にはパフォーマンスのテストを行います。パフォーマンステストの中にはどうしても人間によるチェックが必要なものもあり、例えば実際に使用されるプロンプトを入力し応答を比べてみたいというケースがあります。Amazon Bedrockでは2つの基盤モデルに対し同一のプロンプトを送信し応答を容易に比較できる機能があるので実際に使ってみましょう。

Amazon Bedrockのトップ画面左側にあるナビゲーションメニューより、プレイグラウンドの**Chat/Text**をクリックしてください。



プレイグラウンド（Playground）とは、5章「AWSのAI関連サービス紹介」でも先述した通りマネジメントコンソール上でAmazon Bedrockが扱うことができる基盤モデルのコンテンツ生成を試すことができる機能です。この中のChat/Textにて、基盤モデルの比較を行ってみます。**比較モード**という項目があるのでクリックしてください。



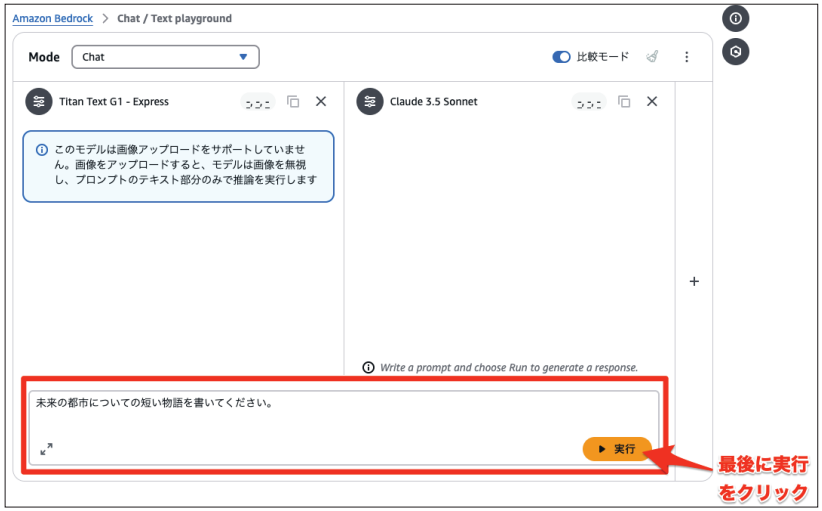
モデルを選択というボタンがそれぞれ出てきますので、モデルを2つ選択します。先ほどモデルアクセスを有効化したClaude 3.5 Sonnet v2とTitan Text G1 - Expressを比較してみましょう。モデルを選択をクリックすると以下のようなポップアップが表示されますので、モデルプロバイダー、モデルの順にクリックしていきます。

Claude 3.5 Sonnet v2とTitan Text G1 - Expressのモデルプロバイダーは以下の通りです。

モデルプロバイダー	モデル
Anthropic	Claude 3.5 Sonnet v2
Amazon	Titan Text G1 - Express

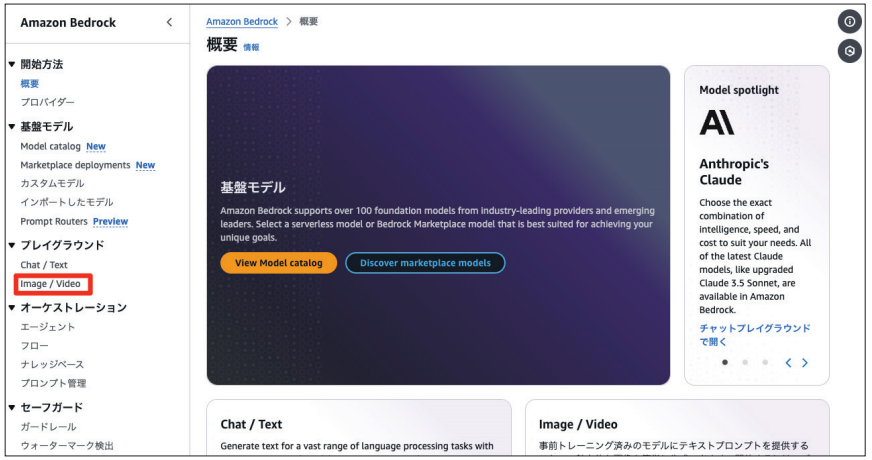
それぞれモデルを選択できると設定画面が表示されますが、今回はデフォルト設定で比較します。右上の閉じるボタン（<）をクリックし設定を閉じましょう。

それでは画面下部にあるプロンプトに入力を行ってみましょう。ここは是非読者の皆さんも楽しんで様々なプロンプトを入力してみていただければと思います。なお筆者は以下画像のように入力してみました。続きが気になる方は試してみてください。プロンプトを入力した後は**実行**ボタンを忘れずに入力するようにしましょう。

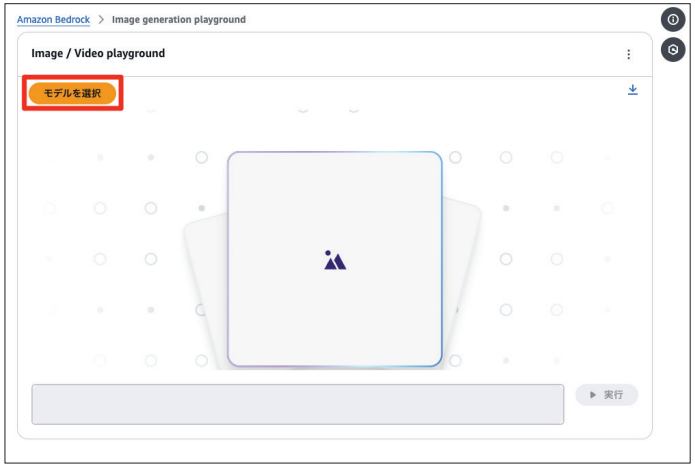


画像を生成してみよう

Amazon Bedrockのプレイグラウンドではテキスト生成だけでなく、画像の生成も試すことができます。Amazon Bedrockのトップ画面左側にあるナビゲーションメニューより、プレイグラウンドの**Image/Video**をクリックしてください。



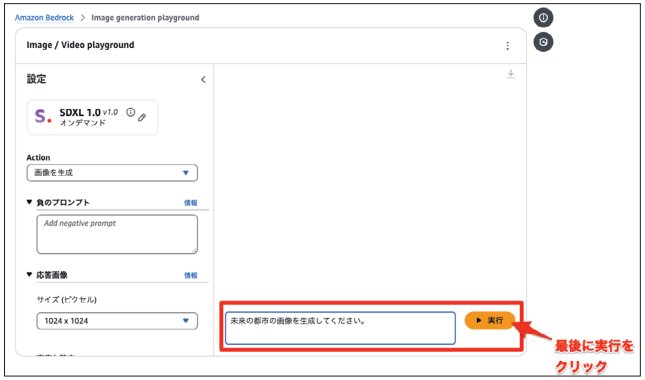
Image/Video playground画面に遷移したら、**モデルを選択**をクリックします。



モデルを選択のポップアップが表示されたら先ほど有効化したSDXL 1.0を使ってみましょう。SDXL 1.0のモデルプロバイダーは以下の通りです。

モデルプロバイダー	モデル
Stability AI	SDXL 1.0

設定はデフォルトのままで、何か生成してほしい画像のプロンプトを入力してみましょう。筆者が以下のように入力してみました。続きが気になる方は試してみてください。プロンプトを入力した後は実行ボタンを忘れずに入力するようにしましょう。



なお生成された画像は著作権で保護されている可能性があります。あくまで使用は検証目的とし、無断及び無確認での使用などは避けましょう。

03 Amazon Q Businessのアプリを作ってRAGを体験してみよう

5章「AWSのAI関連サービス紹介」で先述した通り、Amazon Q Businessは主に企業の知的資産を最大限に活用するために素早く生成AIを取り入れることに特化したサービスです。主にRAGの機能を提供するものですが、ビジネス向けということもあり専門的な知識がなくても業務用生成AIアプリケーションをマネジメントコンソールからの操作のみで作れることが魅力ですので本ハンズオンで実際に動かしてみてRAGを体験してみましょう。

まずは取り込むサンプルデータを用意する必要があります。今回はAIプラクティショナーの試験ガイドを取り込ませましょう。対象のPDFはAIプラクティショナーの公式ページにありますのでダウンロードします。

Webサイト

『AWS Certified AI Practitioner 認定』| AWS
https://aws.amazon.com/jp/certification/certified-ai-practitioner/

執筆現在の対象PDFリンクを掲載しておきます。

Webサイト

『AWS Certified AI Practitioner（AIF-C01）試験ガイド』| AWS
https://d1.awsstatic.com/ja_JP/training-and-certification/docs-ai-practitioner/AWS-Certified-AI-Practitioner_Exam-Guide.pdf

続いて、ダウンロードしたPDFをS3バケットにアップロードします。マネジメントコンソール上部の検索窓に「s3」と入力し（1）、該当サービスのリンクをクリックします（2）。

S3のページトップにアクセスできましたら、**バケットを作成**というボタンがあるのでこちらをクリックします。

続いてバケットの設定を入力していきます。本書執筆現在、バケット名以外は全てデフォルトの設定で問題ありませんでした。念のため各項目の設定も併せて記載しておきます。

まずバケットタイプは**汎用**に設定します（1）。続いて任意のバケット名を入力ください（2）。ここでは以下の命名規則で入力しました。バケット名は全世界で重複しないように設定する必要があります。

S3バケット名:aif-handson-bucket-<AWSのアカウントID>

オブジェクト所有者では**ACL無効**を選択してください（3）

なお、AWSのアカウントIDは画面右上から確認できます。

ではS3バケットの設定に戻ります。このバケットのブロックパブリックアクセス設定は**パブリックアクセスをすべてブロック**にチェックを入れます（1）。バケットのバージョニングは**無効**に設定してください（2）。

タグの追加は行わず、そのままスキップしてください（1）。デフォルトの暗号化は、**Amazon S3マネージドキーを使用したサーバ側の暗号化（SSE-S3）**を選択します（2）。バケットキーは**有効にする**を選択してください（3）。詳細設定はそのままで、最後にバケットを作成をクリックします（4）。

バケットの作成が完了すると以下の画面になりますので、**詳細の表示**をクリックします。

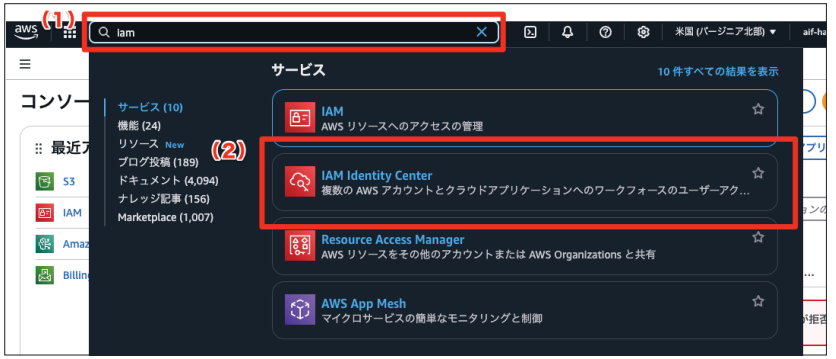
アップロードのボタンをクリックします。

ファイルを追加をクリックしますと、操作している端末のフォルダが表示されますので、対象のPDFを選択します（1）。選択が完了したら、**アップロード**をクリックします（2）。

アップロードが成功したことを確認します。

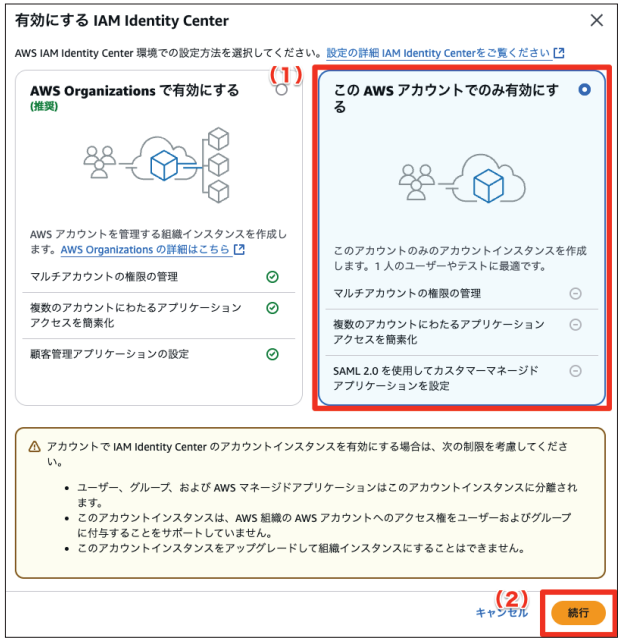
続いてAWS IAM Identity Centerを作成します。5章「AWSのAI関連サービス紹介」で先述した通り、Amazon Q BusinessではID管理にAWS IAM Identity Center を利用しますのでその準備を行います。AWS IAM Identity Centerは複数のAWSアカウントやアプリケーションのユーザーを一括管理できるサービスです。

マネジメントコンソールのトップ画面上部にある検索窓にiamと入力し（1）、該当サービスのリンクをクリックします（2）。



AWS IAM Identity Centerには「組織インスタンス」と「アカウントインスタンス」の2種類があります。組織インスタンスはAWS Organizationsとい

うAWSのアカウントを管理するサービスと連携する機能です。今回はAWS Organizationsを使わないので**このAWSアカウントでのみ有効にする**を選択します（1）。**続行**をクリックします（2）。



タグは追加せず、有効化を行います。画面下部にある**有効にする**ボタンをクリックしてください。

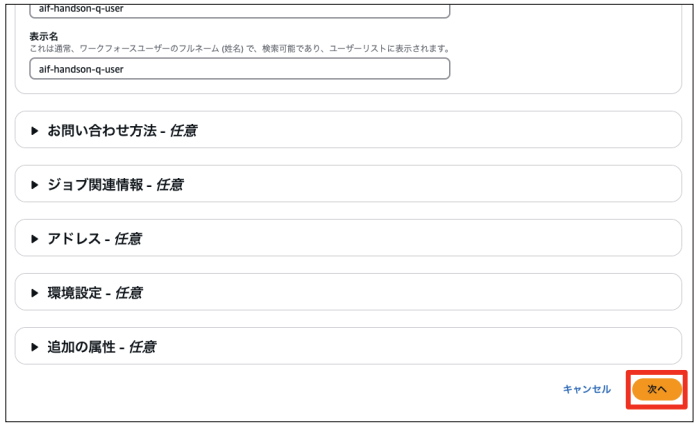
有効化されたことを確認します。

続いてAmazon Q Businessアプリにサインインするユーザーを作成します。左側のナビゲーションメニューより**ユーザー**をクリック（1）、**ユーザーを追加**をクリックします（2）。

ユーザーの詳細を指定という画面が出てきますので、プライマリ情報に以下の設定値を入力します。

項目名	設定値
ユーザー名	aif-handson-q-user
パスワード	このユーザーと共有できるワンタイムパスワードを生成します。
E メールアドレス	任意のメールアドレス
名	aif-handson-q-user
性	aif-handson-q-user
表示名	aif-handson-q-user

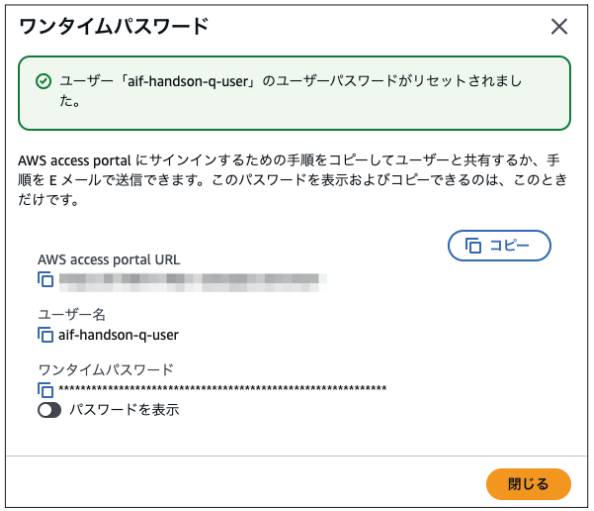
プライマリ情報以外は設定せず、入力が完了したら画面下部にある**次へ**ボタンをクリックしましょう。



ユーザーをグループに追加の画面では追加せずに**次へ**をクリックします。

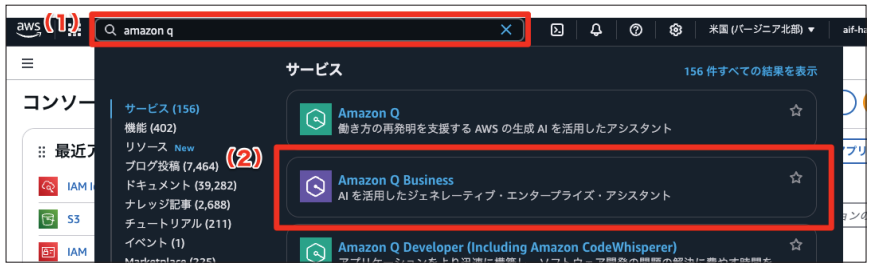
最後に情報を確認し、入力内容に間違いがなければ画面下部にあるユーザーを追加ボタンをクリックします。

ユーザーの追加完了しますと以下のようなサインイン情報が表示されますので、無くさないようにメモに控えておきましょう。

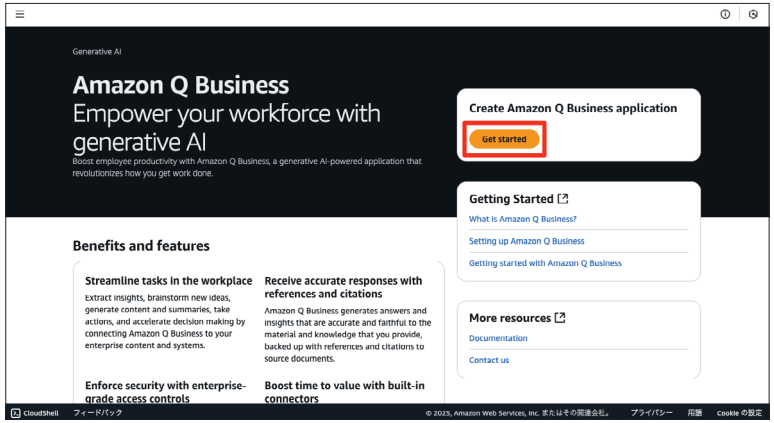


正常に追加されると以下のような画面になります。

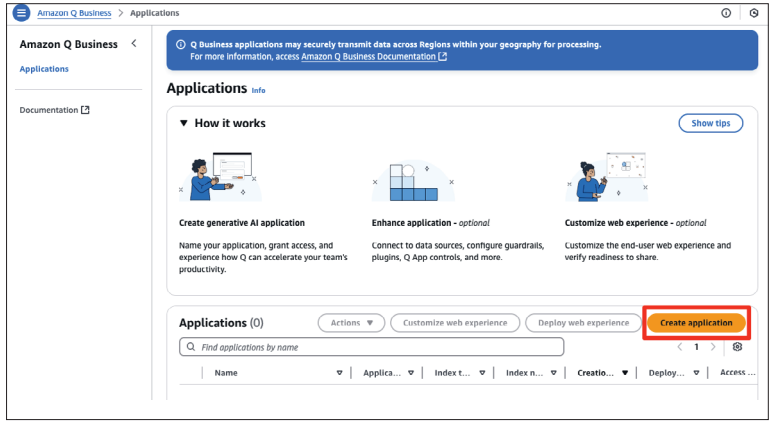
ではAmazon Q Businessのアプリを作っていきましょう。マネジメントコンソールのトップ画面上部にある検索窓にamazon qと入力し (1)、該当サービスのリンクをクリックします (2)。



Amazon Q Businessの画面に遷移したら**Get started**をクリックします。

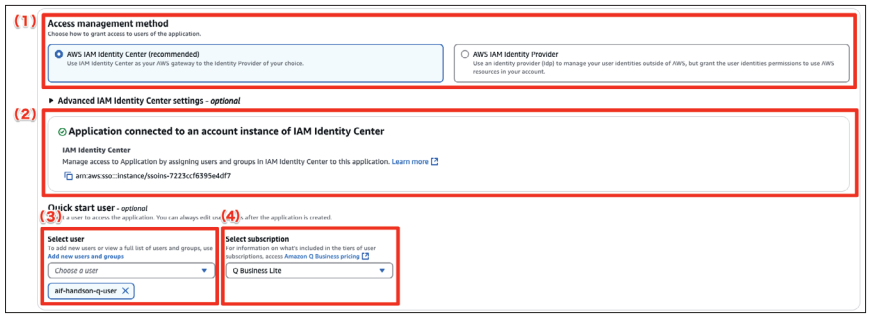


Create applicationをクリックします。



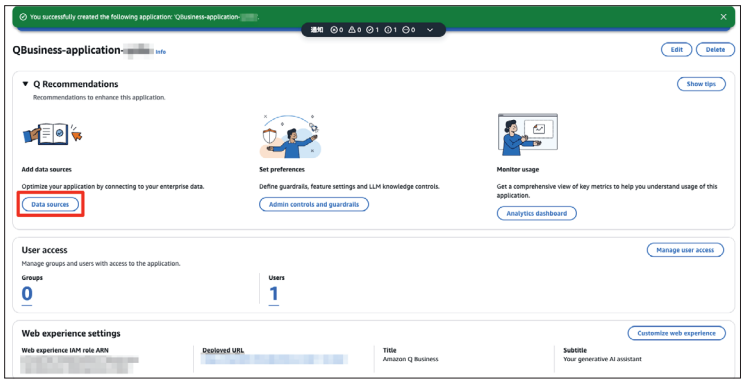
アプリの詳細設定では、以下のポイントを確認していきます。

- Access management methodがAWS IAM Identity Centerとなっていることを確認します (1)。
- 先ほど作成したAWS IAM Identity Centerに繋がっていることを確認します (2)。
- 作成したユーザーがQuick start userとして選択されていることを確認します (3)。
- SubscriptionのプランをQ Business Liteに設定します (4)。

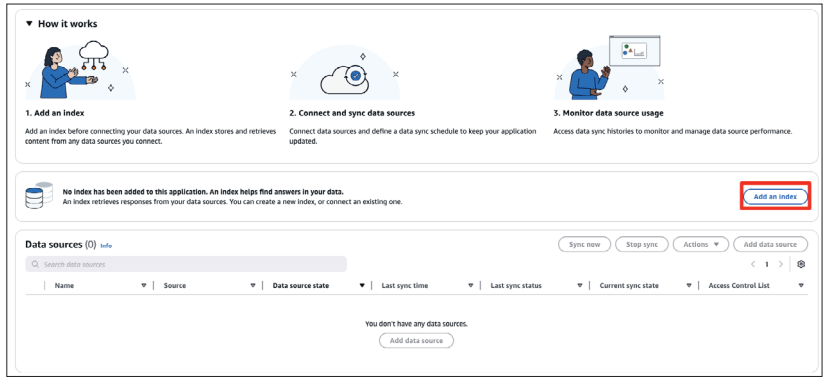


確認できたら画面最下部にある**Create**ボタンをクリックします。アプリが出来上がるのには数分ほどかかります。

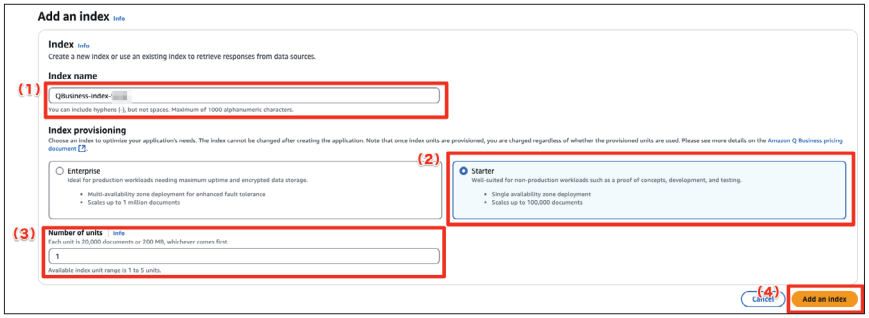
アプリが完成したら次の画面になります。データソースを読み込ませるので、**Data soures**をクリックします。



続いて**Add an index**を選択します。

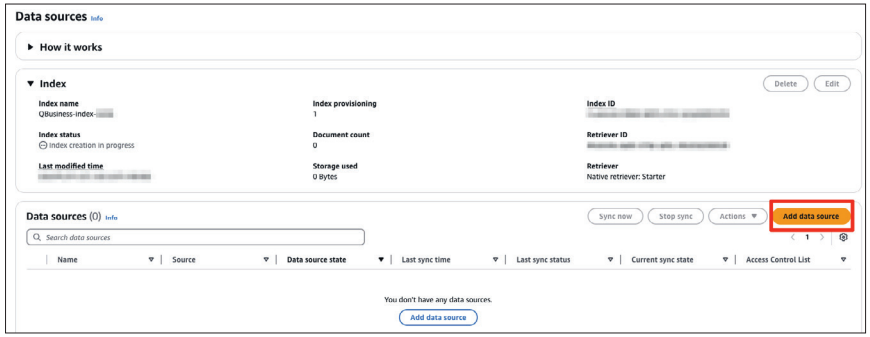


Index名は任意のものを入力します。最初に入力されているものをそのまま使って問題ありません（1）。続いてIndex provisioningは**Starter**を選択します（2）。Number of unitsはデフォルトのまま変更なしにします（3）。最後に**Add an index**をクリックします（4）。

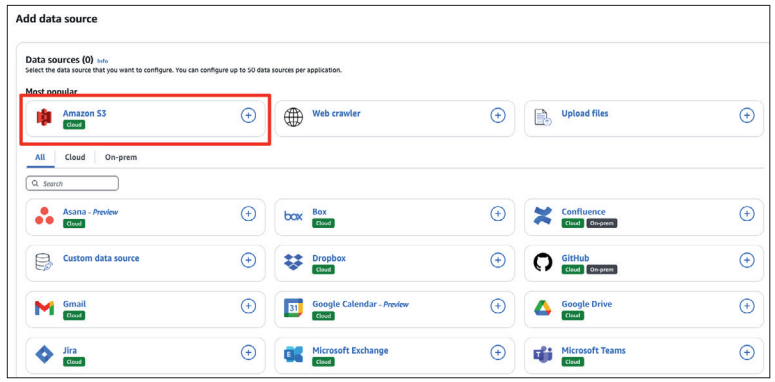


これでIndexの作成が始まりました。完成までは大凡20分ほどかかります。その間にデータソース（RAGに使用するデータの取り込み先設定）の追加を進めましょう。先ほど作成したS3バケット上にあるPDFを読み込みます。

Add data sourceをクリックします。

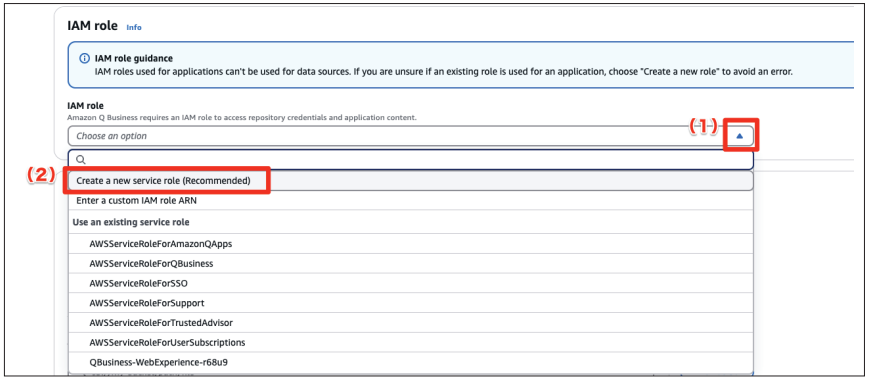


S3を選択します。

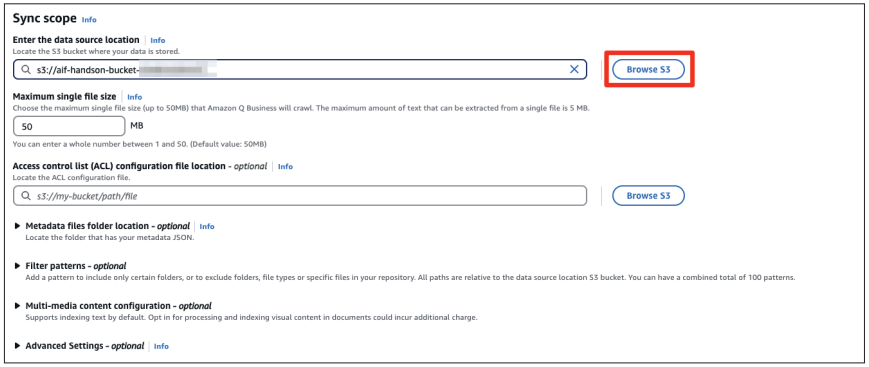


Name and descriptionでは名前のみ設定が必要です。ここではaif-handson-data-sourceとしました。

続いてIAM roleですが、今回は新規作成とします。IAM roleのセレクトボックスをクリックすると（1）、**Create a new service role (Recommended)**と出てきますのでこちらをクリックします（2）。Role nameは提案されたものをそのまま使用して問題ありません。

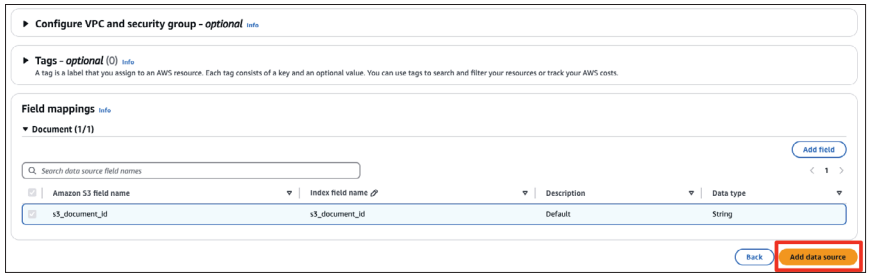


Sync scopeでは先ほど作成したS3バケットを選択します。**Browse S3**をクリックするとS3バケットの一覧が見られますので、対象のS3バケットを選択します。その他の設定はデフォルトのままで問題ありません。



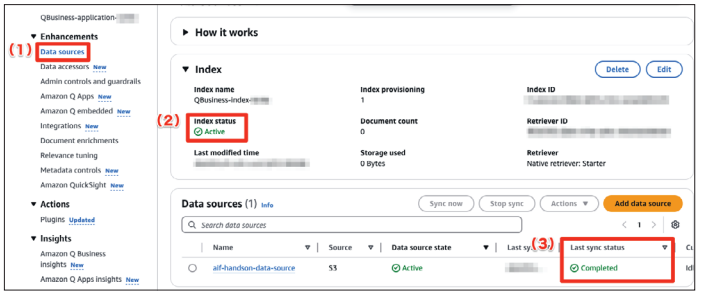
続いて同期の設定です。Sync modeは**Full sync**を選択してください（1）。Sync run scheduleは同期のスケジュールです。日次や月次などが選べますが、ここでは手動同期の**Run on demand**を選択します（2）。

残りの設定はそのままで画面最下部にある**Add data source**をクリックします。

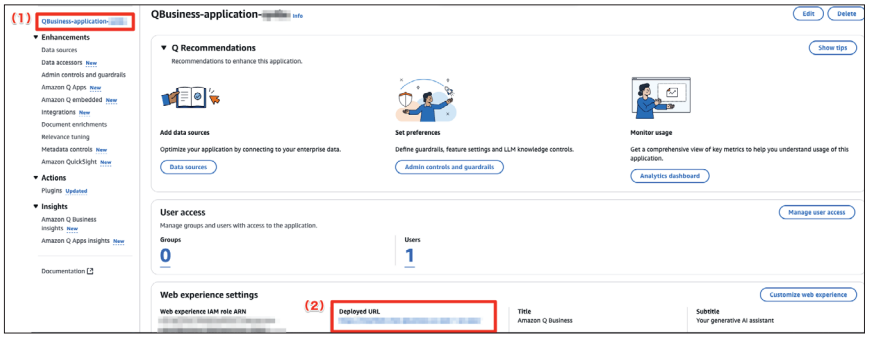


数分ほどで設定が完了します。続いてデータを同期します。設定が完了したらStatusがActiveになっていることを確認して（1）、**Sync now**をクリックしてください（2）。同期には数分ほどかかります。

同期が完了しましたら左側のナビゲーションメニューより**Data sources**を選択し（1）、Index statusが**Active**になっていて（2）、Last sync statusが**Completed**になっていること（3）を確認しましょう。



続いて作成したAmazon Q Businessアプリ画面のトップに移動します。左側のナビゲーションメニューにアプリ名がありますのでそちらをクリックします（1）。トップ画面にDeployed URLがありますのでこちらのリンクをクリックします (2)。

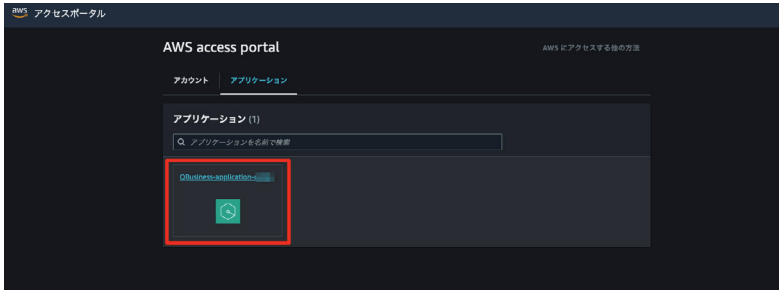


ログインを求められますので、先ほどAWS IAM Identity Centerで作成したユーザーのユーザー名を入力します。

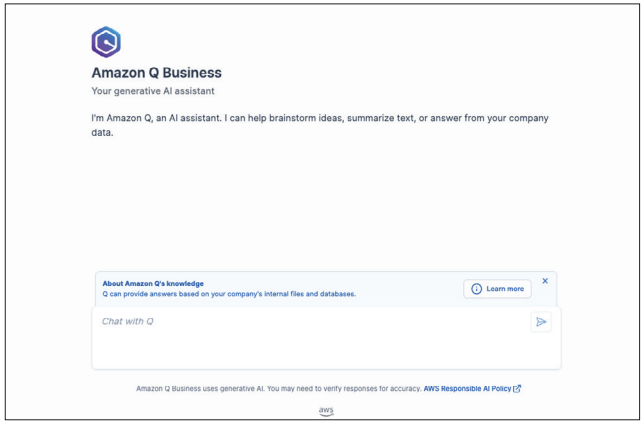
続いてパスワードを求められるので入力します。初回のログインなのでワンタイムパスワードを入力します。

続いてMFAの設定を求められますが、本章の準備の中で行なったルートユーザー及びIAMユーザーのMFA設定と同様の手順で登録を進めてください。無事にMFAの認証が終わると次のようにパスワードの再設定が求められます。

サインインが完了するとAWS access portal画面に遷移しますので、先ほど作成したAmazon Q Businessアプリがあることを確認し、クリックします。

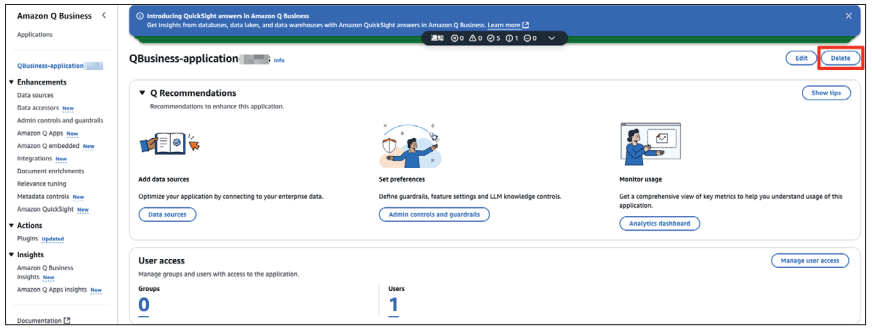


以下のような画面が表示されればAmazon Q Businessアプリへのアクセス成功です。

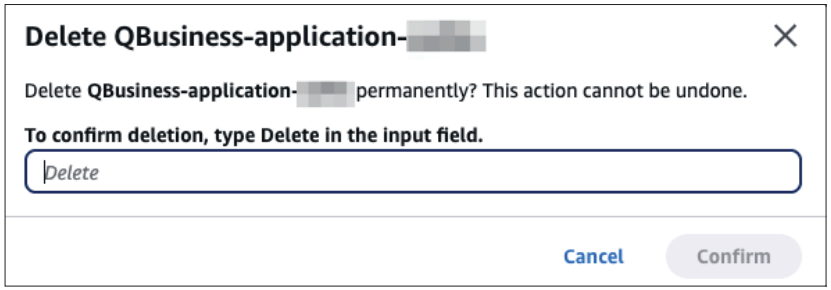


試しにAIプラクティショナーの試験について質問してみると、先ほどアップロードしたPDFの情報に基づいて回答されていることが分かります。

では一通り試し終わったらAmazon Q Businessアプリのリソースは削除するようにしましょう。従量課金なのでそのまま放置しておくと請求額が高額になる恐れがあります。対象のAmazon Q Businessアプリトップ画面に遷移し、**Delete**ボタンをクリックします。



以下のポップアップが表示されますので、説明文に従いDeleteと入力します。



しばらく待つと削除が完了します。

Amazon S3は対象のバケットを空にした（1）後に、バケットを削除可能です（2）。

AWS IAM Identity Centerで作成したユーザーは、料金が発生しないので

放置しても問題ありませんが、セキュリティ上気になる場合には削除しましょう。AWS IAM Identity Centerのトップページにアクセスし、左側のナビゲーションメニューでユーザーを選択（1）、対象のユーザーを選択し（2）、**ユーザーを削除**をクリックします（3）。

以上でハンズオンは終了となります。