

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
-

ハンズオンの準備として以下の作業を行います。

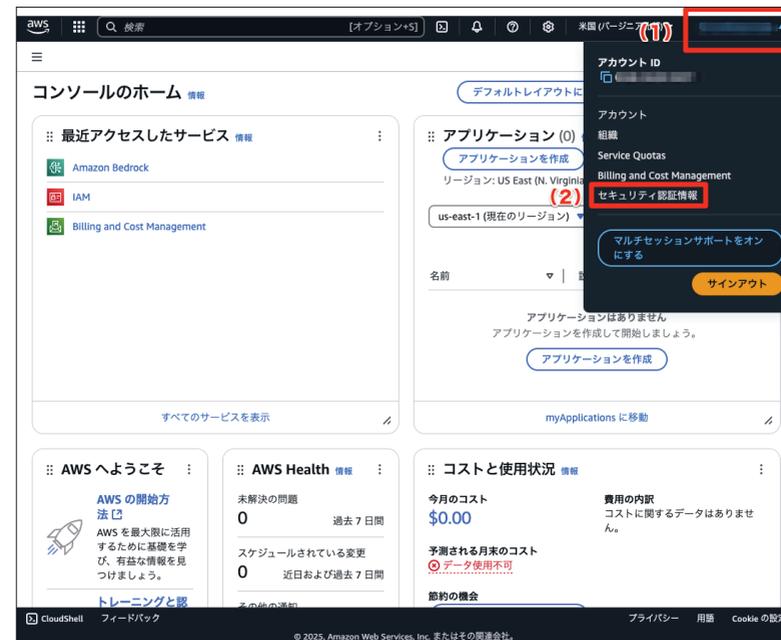
- ルートユーザーのMFA設定
- 作業用IAMユーザーの作成
- Amazon Bedrockで使用するモデルの有効化

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)。

ステップ1 MFA デバイスを選択

ステップ2 デバイスの設定

MFA デバイスを選択

MFA device name

デバイス名
この名前を、このデバイスの識別 AMN 内で使用されます。

(1) aif-certificate-book-mfa

最小 4 文字。英数字と「+」、「@」、「-」文字を使用できます。

MFA device

デバイスオプション
ユーザー名とパスワードに加えて、このデバイスを使用してアカウントへの認証を行います。

パスキーまたはセキュリティキー
指紋、顔、または画面ロックを使用して認証します。このデバイスでパスキーを作成するか、FIDO2 セキュリティキーなどの別のデバイスを使用してください。

(2) 認証アプリケーション
モバイルデバイスまたはコンピュータにインストールされたアプリケーションによって生成されたコードを使用して認証します。

ハードウェア TOTP トークン
ハードウェア TOTP トークンまたは他のハードウェアデバイスによって生成されたコードを使用して認証します。

キャンセル (3) 次へ

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)。

ステップ1 MFA デバイスを選択

ステップ2 デバイスの設定

デバイスの設定

認証アプリケーション
仮想 MFA デバイスはデバイス上で動作するアプリケーションで、QR コードをスキャンすることで設定できます。

(1) 1 Google Authenticator、Duo Mobile、Authy アプリなどの互換性のあるアプリケーションを、モバイルデバイスまたはコンピュータにインストールします。
互換性のあるアプリケーションのリストを表示

(2) 2 QR コードを表示
認証アプリを開いて、このページで [QR コードを表示] を選択し、アプリを使用してコードをスキャンします。または、シークレットキーを入力することもできます。
シークレットキーを表示

(3) 3 2 つの連続した MFA コードを以下で入力してください
仮想アプリケーションのコードを以下で入力してください
MFA コード 1
30 秒待ってから、2 つ目のコードエントリを入力してください。
MFA コード 2

キャンセル (4) MFA を追加

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。

IAM > セキュリティ認証情報

Identity and Access Management (IAM)

IAM の検索

ダッシュボード

▼ アクセス管理
ユーザーグループ
ユーザー
ロール
ポリシー
ID プロバイダ
アカウント設定
ルートアクセス管理

▼ アクセスレポート
Access Analyzer
外部アクセス
未使用のアクセス
アナライザーの設定
認証情報レポート
組織のアクティビティ
サービスコントロールポリシー
リソースコントロールポリシー
詳細

IAM Identity Center
AWS Organizations

アクティブな MFA デバイス
You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

アカウントの詳細
アカウント名: aif-certificate-book
E メールアドレス: [redacted]
AWS アカウント ID: [redacted]
ID プロバイダ: [redacted]
正権ユーザー ID: [redacted]

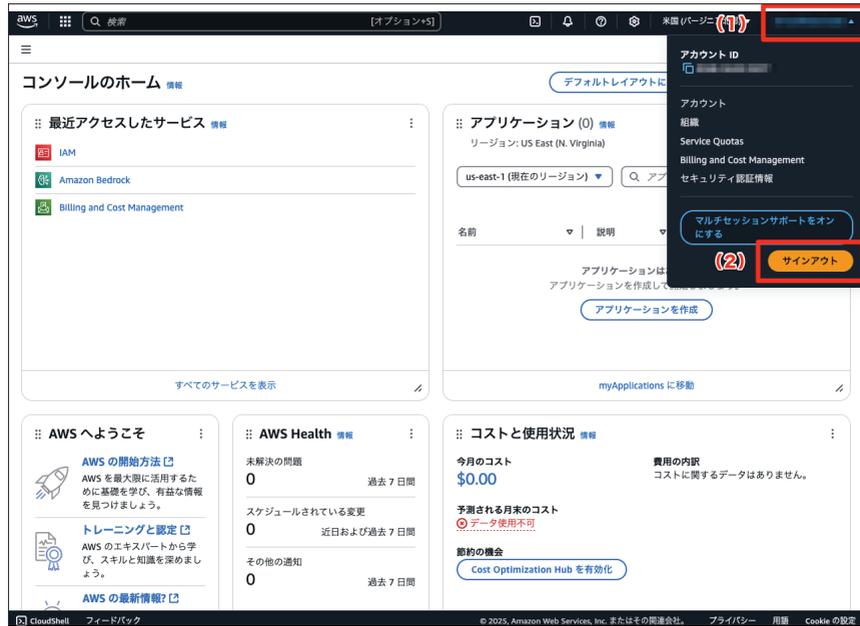
多要素認証 (MFA) (2)
MFA を使用して AWS 環境のセキュリティを強化します。MFA を使用してサインインするには、MFA デバイスからの認証コードが必要です。各ユーザーには、最大 8 つの MFA デバイスを割り当てることができます。詳細はこちら

タイプ	識別子	認証	作成日
仮想	[redacted]	[redacted]	[redacted]
仮想	[redacted]	[redacted]	[redacted]

アクセスキー (0)
アクセスキーを使用して、AWS CLI、AWS Tools for PowerShell、AWS SDK、またはダイレクト AWS API コールからプログラムによる呼び出しを AWS に送信します。一度に持つことができるアクセスキー (アクセスキーまたはサブアクセスキー) は最大 2 つです。詳細はこちら

アクセスキー ID	作成日	最後に使用したアクセスキー	最後に使用したリージョン	最後に使用したサービス	ステータス
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	アクセスキーなし

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が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いますが、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。

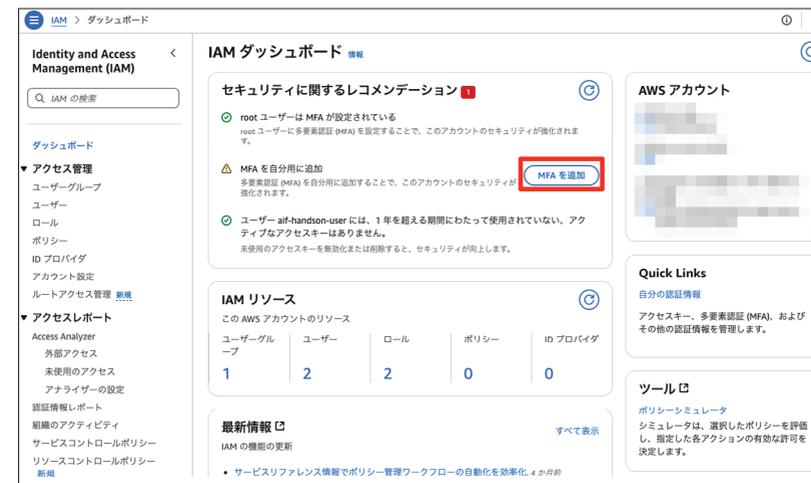
	A	B	C	D	E	F	G
1	ユーザー名	パスワード	コンソールサインイン URL				
2	aif-handson-						
3							
4							
5							

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。



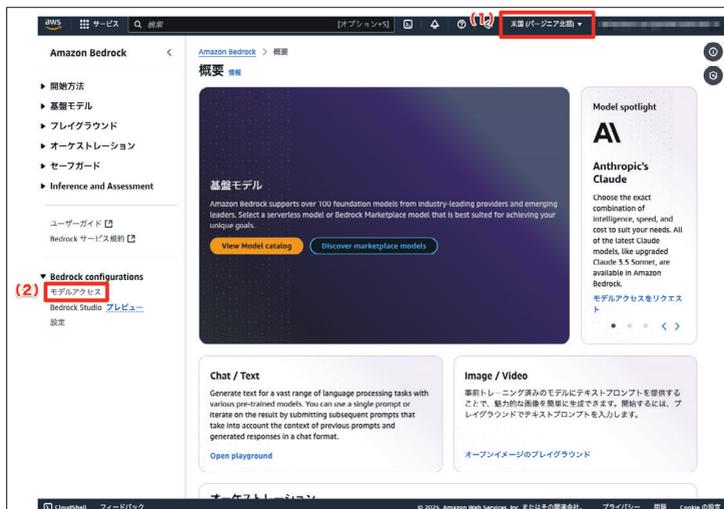
Amazon Bedrockで使用するモデルの有効化

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)。



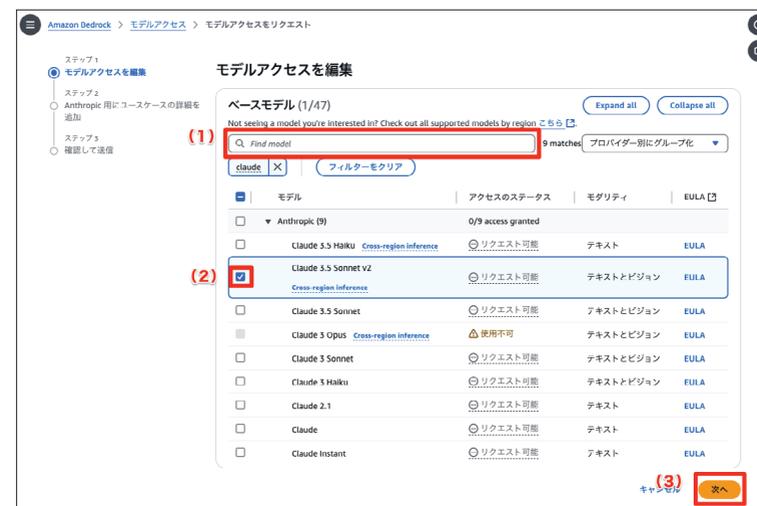
Amazon Bedrock のモデルアクセストップ画面にいくと、利用可能な基盤モデルが並んでいます。本ハンズオンでは個別にモデルを有効化しますので、**特定のモデルを有効にする** をクリックしてください。



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)。

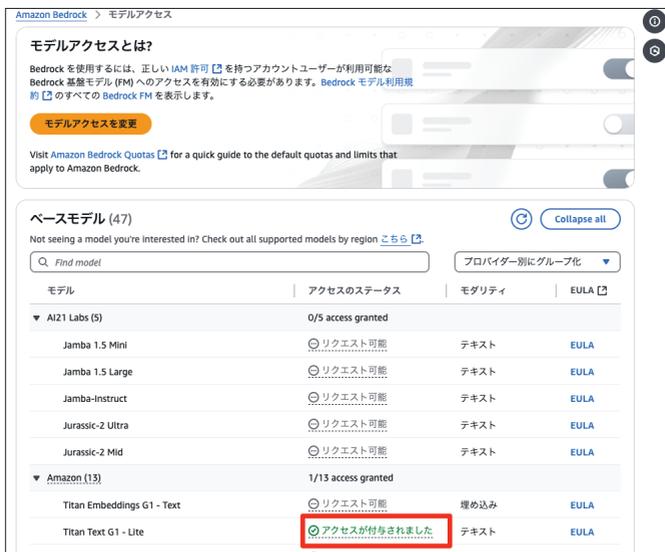


Anthropic 用にユースケースの詳細を追加の画面に遷移しますので、以下の情報を入力してください。ユースケースの説明は「検証のため」と入力します。

- 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

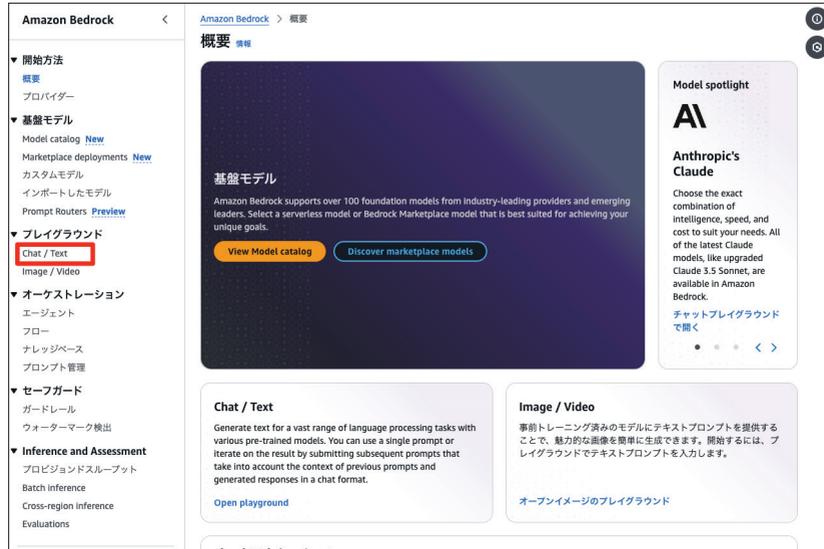
Amazon Bedrock を試してみよう

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。

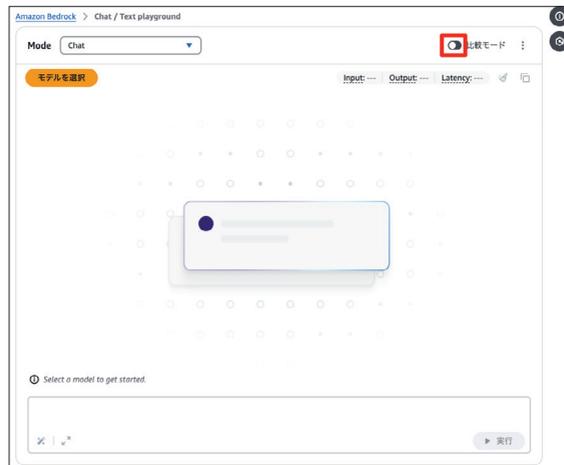
2つの基盤モデルを比較してみよう

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。



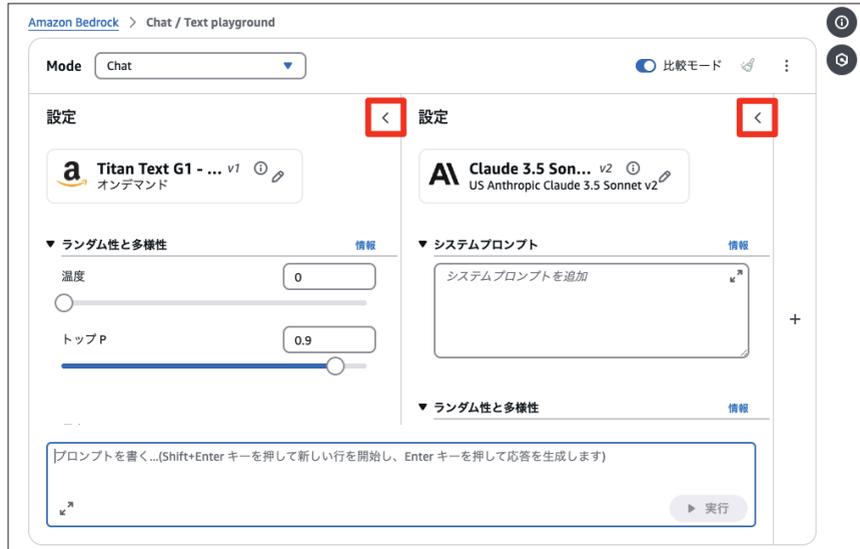
モデルを選択というボタンがそれぞれ出てきますので、モデルを2つ選択します。先ほどモデルアクセスを有効化したClaude 3.5 Sonnet v2とTitan Text G1 - Expressを比較してみましょう。モデルを選択をクリックすると以下のようなポップアップが表示されますので、モデルプロバイダー、モデルの順にクリックしていきます。



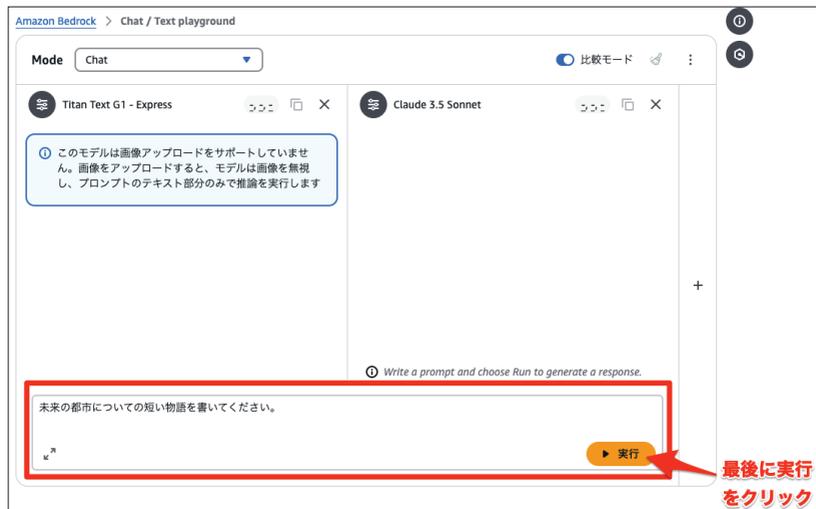
Claude 3.5 Sonnet v2とTitan Text G1 - Expressのモデルプロバイダーは以下の通りです。

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。

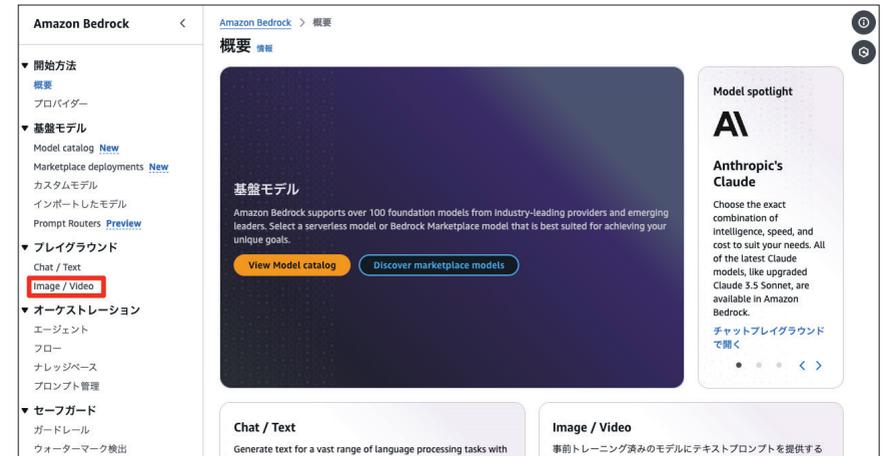


それでは画面下部にあるプロンプトに入力を行っていきましょう。ここでは是非読者の皆さんも楽しんで様々なプロンプトを入力していただければと思います。なお筆者は以下画像のように入力してみました。続きが気になる方は試してみてください。プロンプトを入力した後は**実行**ボタンを忘れずに入力するようにしましょう。

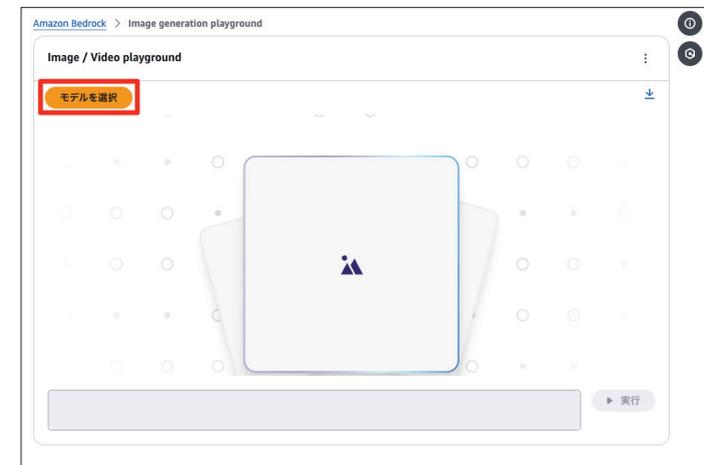


画像を生成してみよう

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。

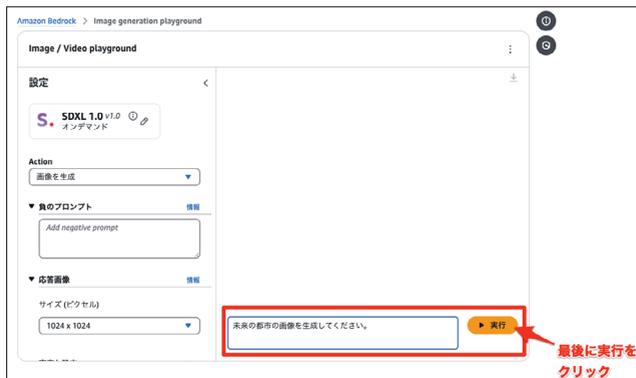


モデルを選択のポップアップが表示されたら先ほど有効化したSDXL 1.0を使ってみましょう。SDXL 1.0のモデルプロバイダーは以下の通りです。

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、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。

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。本ハンズオンで実際に動かしてみても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/>

<p>受験者 ビジネスアナリスト、IT サポート、マーケティングプロフェッショナル、製品またはプロジェクトマネージャー、事業部門または IT マネージャー、セールスプロフェッショナル</p> <p>受験オプション Pearson VUE テストセンターまたはオンライン監督付き試験</p> <p>対象言語 英語、日本語、韓国語、ポルトガル語 (ブラジル)、簡体字中国語</p>	<p>2025 年 2 月 15 日までにこの認定資格を取得すると、Early Adopter (アドプター) のデジタルバッジも授与されます。</p> 
---	---

試験に向けて準備する

初歩から始めて、認定を取得しましょう。オンライン学習センターの AWS Skill Builder で Exam Prep Plan に従って学習を進め、自信をもって試験当日に臨みましょう。

- #### 試験について知る

4ステップのプランに沿って準備を進めます。
試験ガイドを確認する
- #### AWS の知識とスキルをリフレッシュする

知識やスキルのギャップを埋める必要があるデジタルコースに登録し、AWS Builder Labs、AWS Cloud Quest、AWS Jam で練習します。

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。

Amazon S3

任意の量のデータをどこからでも保存および取得

Amazon S3 は、業界トップクラスのスケールビリティ、データの可用性、セキュリティ、パフォーマンスを提供するオブジェクトストレージサービスです。

バケットの作成

S3 内のすべてのオブジェクトはバケットに保存されます。ファイルとフォルダを S3 にアップロードするには、オブジェクトを保存されるバケットを作成する必要があります。

バケットを作成

料金

S3 には最低料金はありません。使用した分についての料金のみをお支払いいただきます。料金は S3 バケットの構成に基づいています。

AWS 料金見積りツール¹を使用して月額料金を見積もる

[料金の詳細を表示](#)

リソース

- ユーザーガイド
- API リファレンス
- よくある質問

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)

バケットを作成

バケットは S3 に保存されたデータのコンテナです。

一般的な設定

AWS リージョン
米国東部 (バージニア北部) us-east-1

バケットタイプ

(1) 汎用
ほとんどのユースケースとアクセスパターンに推奨されます。汎用バケットが S3 のバケットタイプです。これにより、最新の API やコンソール機能に最新のアップデートを簡単に適用して最新の S3 サービスを簡単に使用できます。

デフォルト
ほとんどのユースケースに推奨されます。これらのバケットは、単一のアプリケーション内でのみ最新のデータ保護を提供する S3 Express One Zone ストレージクラスのみを参照します。

(2) バケット名: aif-handson-bucket-

既存のバケットから設定をコピーオプション
次の設定がバケットに追加されます。

バケットを選択する

形式: us:/bucket/prefix

(3) オブジェクト所有者

他の AWS アカウントからこのバケットに書き込まれたオブジェクトの所有者と、アクセスコントロール (ACL) の使用を管理します。オブジェクトの所有者は、オブジェクトへのアクセスを指定できるユーザーを決定します。

ACL 無効 (推奨)
このバケット内のすべてのオブジェクトは、このアカウントによって所有されます。このバケットとそのオブジェクトへのアクセスは、ポリシーを介して管理されています。

ACL 有効
他の AWS アカウントがこのバケット内のオブジェクトの所有者になることができます。このバケットとそのオブジェクトへのアクセスは、ACL を使用して管理されます。

オブジェクト所有者
バケット所有者の権限

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ンングは**無効**に設定してください (2)。

このバケットのブロックパブリックアクセス設定

パブリックアクセスは、アクセスコントロールリスト (ACL)、Access Control List、バケットポリシー、アクセスポイントポリシー、またはオブジェクトポリシーを使用して許可されます。このバケットとそのオブジェクトへのパブリックアクセスが許可されている場合は、パブリックアクセスをすべてブロックする前に、パブリックアクセスをすべてブロックする必要がある場合があります。AWS ではパブリックアクセスをすべてブロックすることを推奨しません。これらの設定を使用する前に、アプリケーションが公開アクセスなしで正しく機能することを確認してください。このバケットやオブジェクトのある範囲の公開アクセスが必要な場合は、各ストレージクラスに適合して以下にある**元の設定を元に戻す**をクリックしてください。

(1) パブリックアクセスをすべてブロック
パブリックアクセスを許可しないように、このバケットの公開アクセスをすべてブロックします。次の設定は互いに独立しています。

- 新しいアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
ACL、新しく追加されたバケットポリシー、バケットポリシー、またはオブジェクトポリシーを使用してパブリックアクセスをすべてブロックし、既存のバケットまたはオブジェクトに対する新しいパブリックアクセス ACL、バケットポリシー、またはオブジェクトポリシーを適用しないようにします。この設定では、ACL を使用して S3 リージョンへのパブリックアクセスを許可する範囲のオブジェクトを指定できます。
- 既存のアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
S3 はバケットとオブジェクトへのパブリックアクセスを付与するまで ACL を参照します。
- 新しいパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする
バケットポリシー、アクセスポイントポリシー、またはオブジェクトポリシーを使用してパブリックアクセスを許可する範囲のオブジェクトを指定できます。
- 既存のパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスとバケットポリシーをブロックする
S3 は、バケットとオブジェクトへのパブリックアクセスを付与するポリシーを適用したバケットまたはオブジェクトへのパブリックアクセスとバケットポリシーを参照します。

バケットのバージョンング
バージョンングは、オブジェクトの複数のバージョンを同じバケット内に保持する手段です。バージョンングを使用すると、Amazon S3 バケットに格納されているすべてのオブジェクトすべてのバージョンを保持、取得、復元できます。バージョンングを使用すると、無効なバージョンと無効なアプリケーションバージョンの両方から簡単に復元できます。詳細

(2) バケットのバージョンング
 無効にする
 有効にする

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**サーバー側の暗号化 (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、最後にバケットを作成をクリックします (4)。

(1) タグオプション (0)
バケットタグを使用して、ストレージコストを最適化し、バケットを整理できます。詳細はこちら

このバケットに関連付けられたタグはありません。

タグの追加

デフォルトの暗号化

サーバー側の暗号化は、このバケットに保存された新しいオブジェクトに自動的に適用されます。

(2) 暗号化タイプ

- Amazon S3 マネージドキーを使用したサーバー側の暗号化 (SSE-S3)
- AWS Key Management Service キーを使用したサーバー側の暗号化 (SSE-KMS)
- AWS Key Management Service キーを使用したデュアルレジャーサーバー側の暗号化 (SSE-KMS)
- Amazon S3 の暗号化 (SSE-S3) を使用して、Amazon S3 の暗号化 (SSE-S3) の暗号化を許可する範囲のオブジェクトを指定できます。

(3) バケットキー
Amazon S3 バケットキーを使用すると、Amazon S3 の暗号化コストを最適化できます。SSE-KMS の S3 バケットキーはサポートされていない場合があります。詳細

- 無効にする
- 有効にする

詳細設定

バケットを作成したら、バケットにファイルとフォルダをアップロードし、追加のバケット設定を行うことができます。

(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。



アップロードが成功したことを確認します。



アップロードのボタンをクリックします。

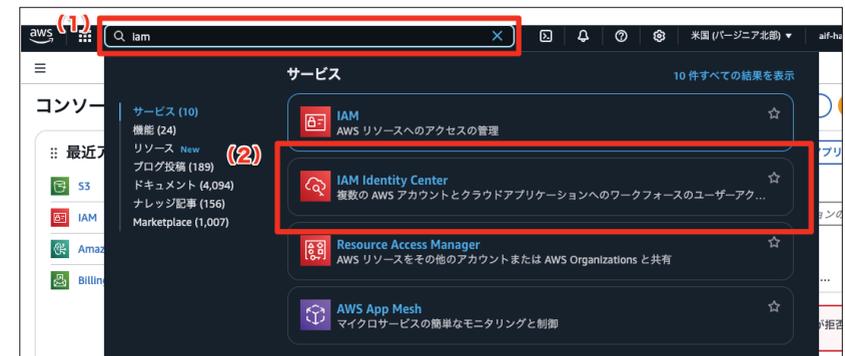


ファイルを追加をクリックすると、操作している端末のフォルダが表示されますので、対象のPDFを選択します (1)。選択が完了したら、アップロードをクリックします (2)。



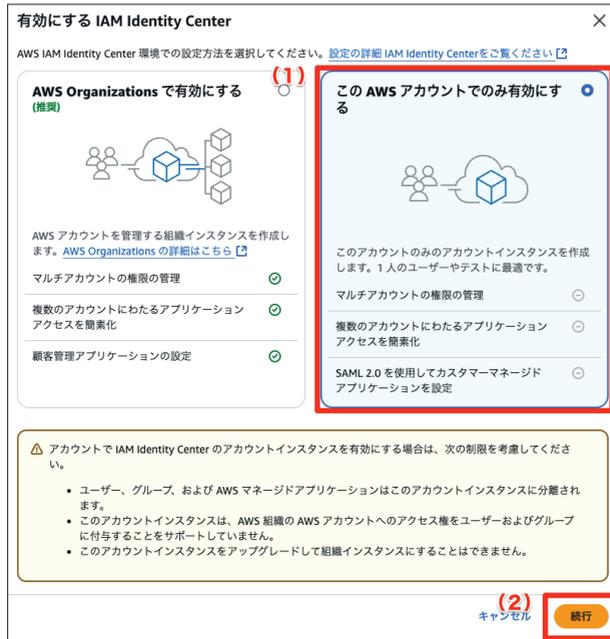
続いてAWS IAM Identity Centerを作成します。5章「AWSのAI関連サービス紹介」で先述した通り、Amazon Q BusinessではID管理にAWS IAM Identity Center を利用しますのでその準備を行います。AWS IAM Identity Centerは複数のAWSアカウントやアプリケーションのユーザーを一括管理できるサービスです。

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

ユーザーの詳細を指定

プライマリ情報

ユーザー名
このユーザー名は、このユーザーが AWS access portal にサインインするために必要です。ユーザー名は後で変更することはできません。
aif-handson-q-user
最大長は 128 文字です。英数字または +、@、_、! のいずれかを複数使用できます。

パスワード
このユーザーがパスワードを受け取る方法を選択します。詳細はこちら
このパスワードの設定手順が完了したとメールをこのユーザーに送信します。
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
Eメールアドレスを確認

名
aif-handson-q-user
姓
aif-handson-q-user
表示名
これは通常、ワークフォースユーザーのフルネーム (姓名) で、検索可能であり、ユーザーリストに表示されます。
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。

aif-handson-q-user

表示名
これは通常、ワークフォースユーザーのフルネーム (姓名) で、検索可能であり、ユーザーリストに表示されます。
aif-handson-q-user

お問い合わせ方法 - 任意

ジョブ関連情報 - 任意

アドレス - 任意

環境設定 - 任意

追加の属性 - 任意

キャンセル **次へ**

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。

IAM Identity Center > ユーザー > ユーザーを追加

ステップ 1 ユーザーの詳細を指定
ステップ 2 任意
ステップ 3 ユーザーをグループに追加
ステップ 4 ユーザーの確認と追加

ユーザーをグループに追加 - 任意
このユーザーを 1 つ以上のグループに割り当てることができます。

グループ (0) グループを作成

グループ名を検索する

グループ名 | 説明

グループが見つかりません

キャンセル 戻る **次へ**

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。

ワンタイムパスワード

ユーザー「aif-handson-q-user」のユーザーパスワードがリセットされました。

AWS access portal にサインインするための手順をコピーしてユーザーと共有するか、手順を E メールで送信できます。このパスワードを表示およびコピーできるのは、このときだけです。

AWS access portal URL コピー

ユーザー名
aif-handson-q-user

ワンタイムパスワード
パスワードを表示

閉じる

正常に追加されると以下のような画面になります。

IAM Identity Center > ユーザー

IAM Identity Center

ユーザー「aif-handson-q-user」が正常に追加されました。
このユーザーがワンタイムパスワードを使用してサインインし、パスワードを変更できるのは 7 日間です。
このユーザーがサインインした場合はアプリケーションに通知を送信する場合があります。その他のユーザーは、AWS access portal にサインインする前に割り当てられた AWS アカウントやクラウドアプリケーションにアクセスする必要があります。詳細はこちら

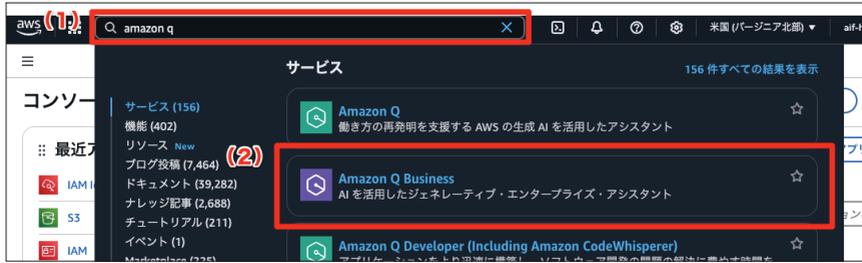
ユーザー (1) ユーザーを削除 ユーザーを追加

このユーザーがサインインしているユーザーは、AWS access portal にサインインして、AWS アカウントと割り当てられたクラウドアプリケーションにアクセスできます。詳細はこちら

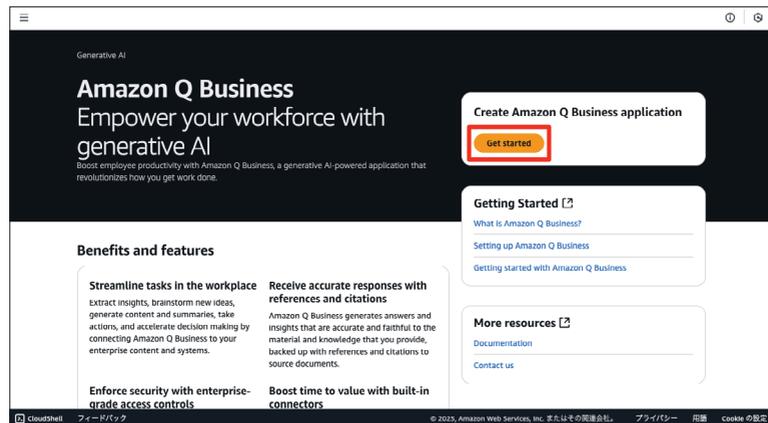
ユーザー名 ユーザー名を検索

ユーザー名	表示名	ステータス	MFA デバイス	作成者
aif-handson-q-user	aif-handson-q-user	有効	なし	手動

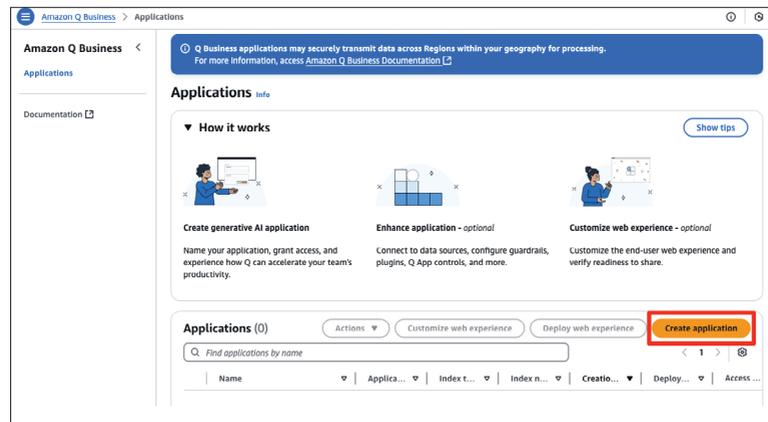
では Amazon Q Business のアプリを作っていきます。マネジメントコンソールのトップ画面上部にある検索窓に amazon q と入力し (1)、該当サービスのリンクをクリックします (2)。



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

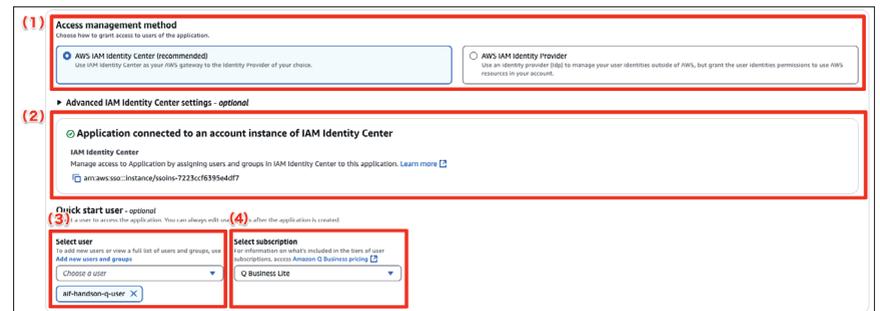


Create application をクリックします。



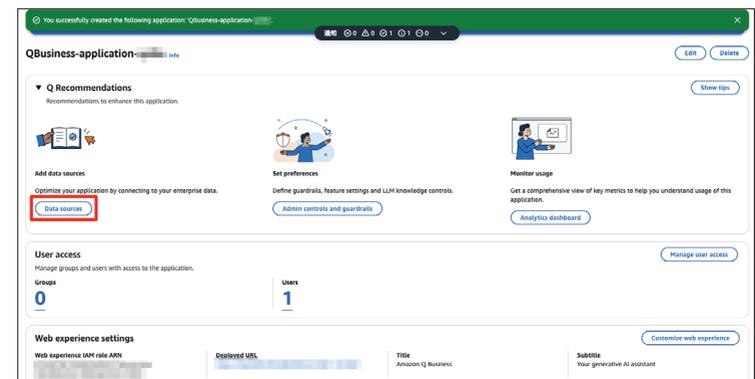
アプリの詳細設定では、以下のポイントを確認していきます。

- 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)。

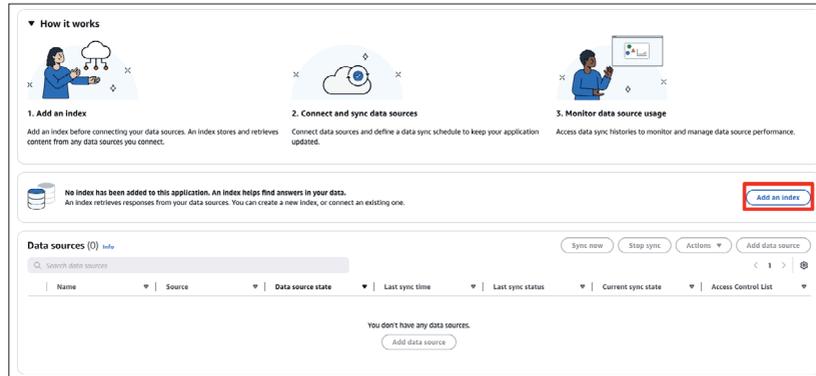


確認できれば画面最下部にある **Create** ボタンをクリックします。アプリが出来上がるのには数分ほどかかります。

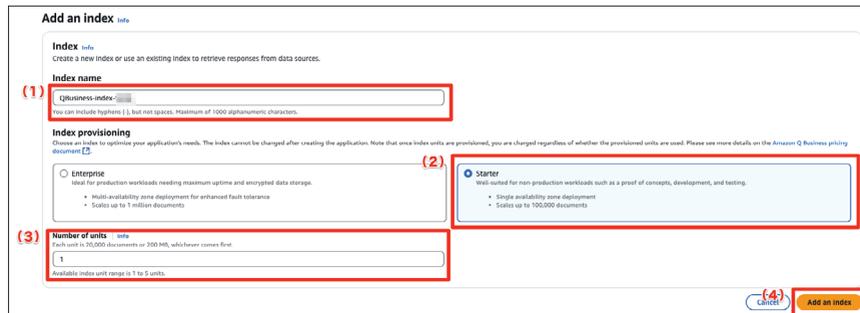
アプリが完成したら次の画面になります。データソースを読み込ませるので、**Data sources** をクリックします。



続いて **Add an index** を選択します。

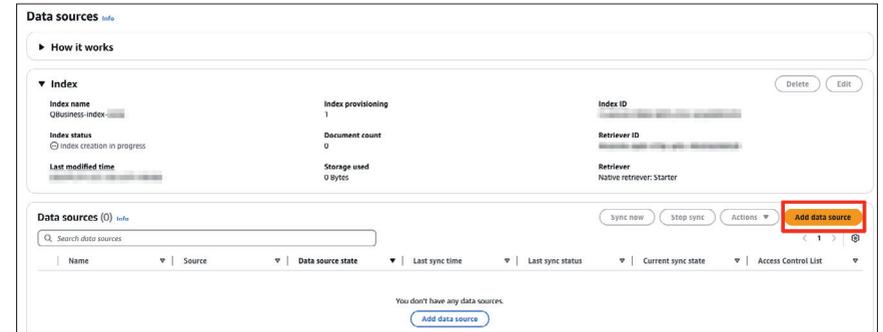


Index名は任意のものを入力します。最初に入力されているものをそのまま使って問題ありません (1)。続いてIndex provisioningは **Starter** を選択します (2)。Number of unitsはデフォルトのまま変更なしにします (3)。最後に **Add an index** をクリックします (4)。

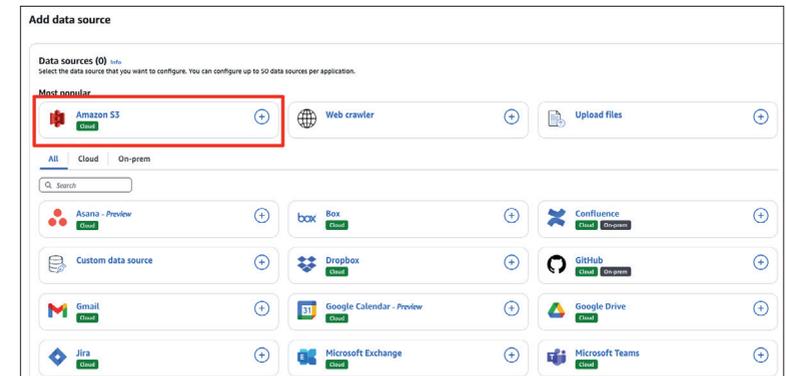


これでIndexの作成が始まりました。完成までは大凡20分ほどかかります。その間にデータソース (RAGに使用するデータの取り込み先設定) の追加を進めましょう。先ほど作成したS3バケット上にあるPDFを読み込みます。

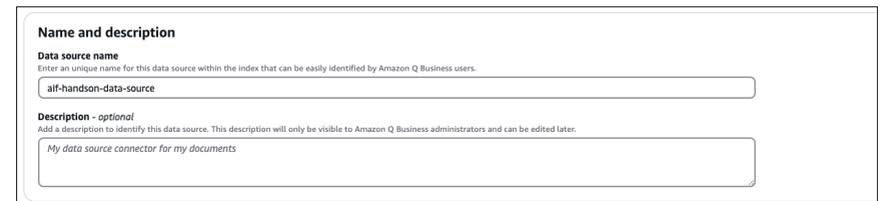
Add data source をクリックします。



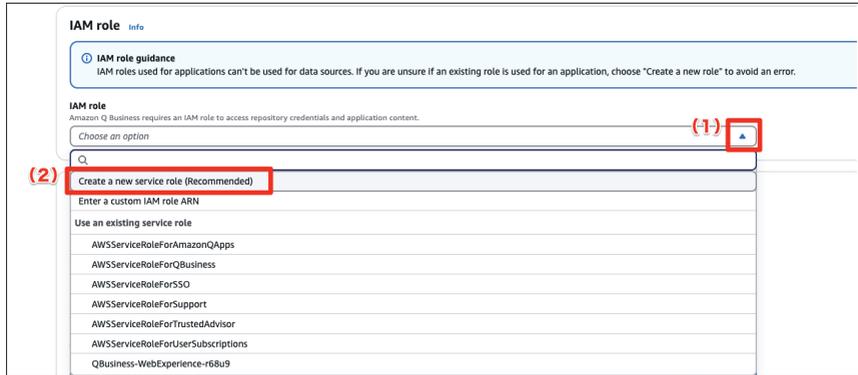
S3を選択します。



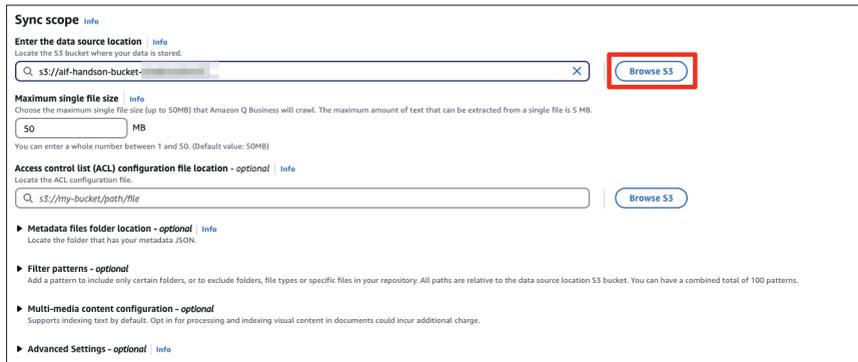
Name and descriptionでは名前のみ設定が必要です。ここでは aif-handson-data-source としました。



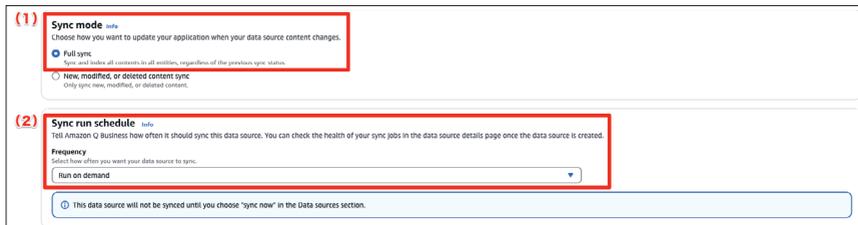
続いてIAM roleですが、今回は新規作成とします。IAM roleのセレクトボックスをクリックすると (1)、**Create a new service role (Recommended)** と出てきますのでこちらをクリックします (2)。Role nameは提案されたものをそのまま使用して問題ありません。



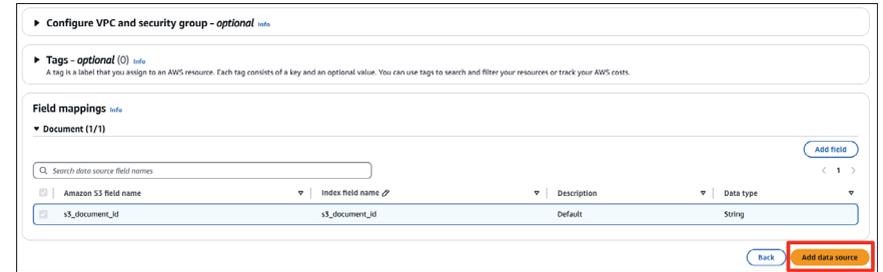
Sync scope では先ほど作成した S3 バケットを選択します。Browse S3 をクリックすると S3 バケットの一覧が見られますので、対象の S3 バケットを選択します。その他の設定はデフォルトのままです。



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)。



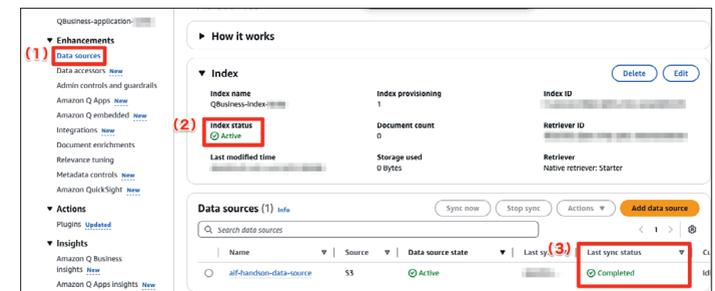
残りの設定はそのまま画面最下部にある Add data source をクリックします。



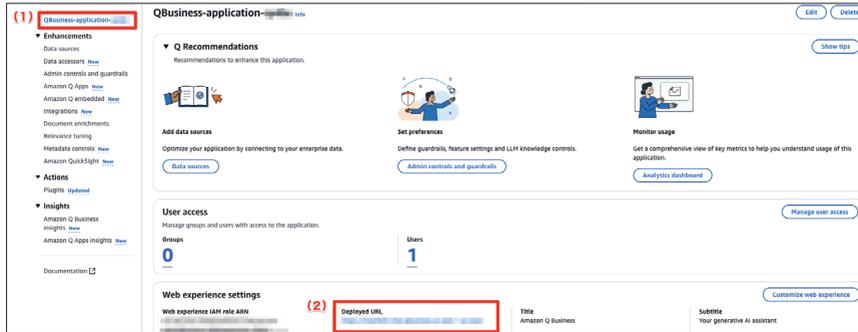
数分ほどで設定が完了します。続いてデータを同期します。設定が完了したら Status が Active になっていることを確認して (1)、Sync now をクリックしてください (2)。同期には数分ほどかかります。



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。



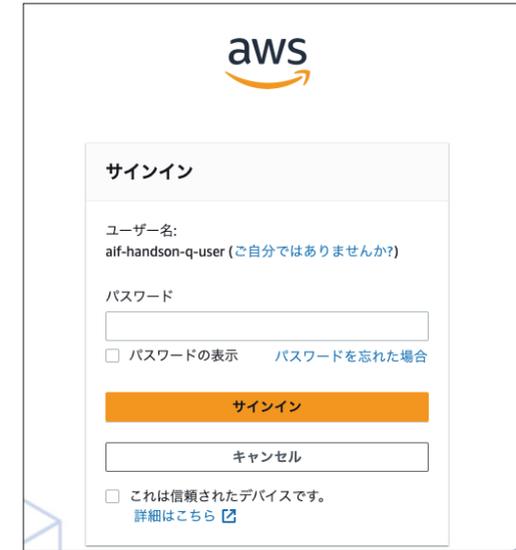
続いて作成した Amazon Q Business アプリ画面のトップに移動します。左側のナビゲーションメニューにアプリ名がありますのでそちらをクリックします (1)。トップ画面に Deployed URL がありますのでこちらのリンクをクリックします (2)。



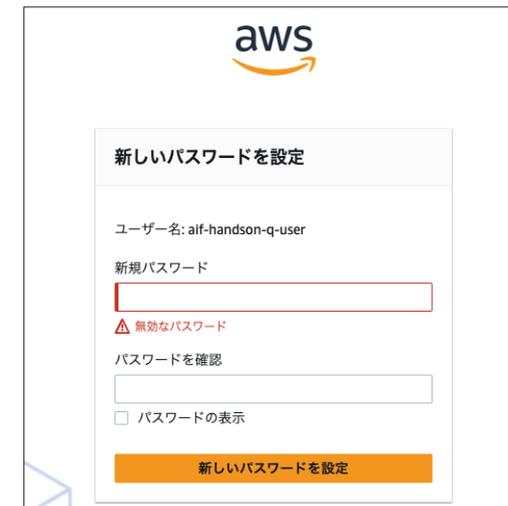
ログインを求められますので、先ほど AWS IAM Identity Center で作成したユーザーのユーザー名を入力します。



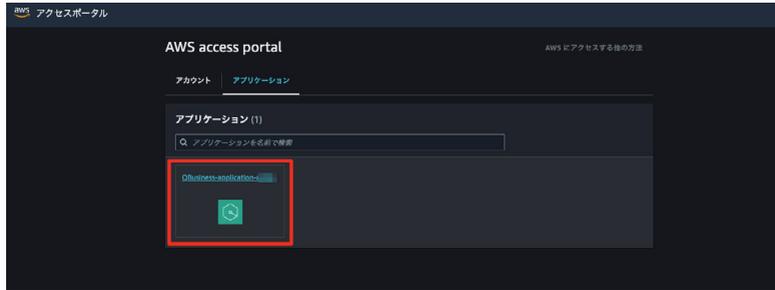
続いてパスワードを求められるので入力します。初回のログインなのでワンタイムパスワードを入力します。



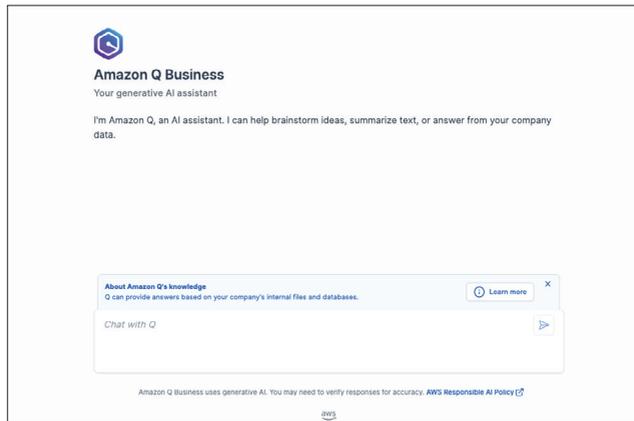
続いて MFA の設定を求められますが、本章の準備の中で行なったルートユーザー及び IAM ユーザーの MFA 設定と同様の手順で登録を進めてください。無事に MFA の認証が終わると次のようにパスワードの再設定が求められます。



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。



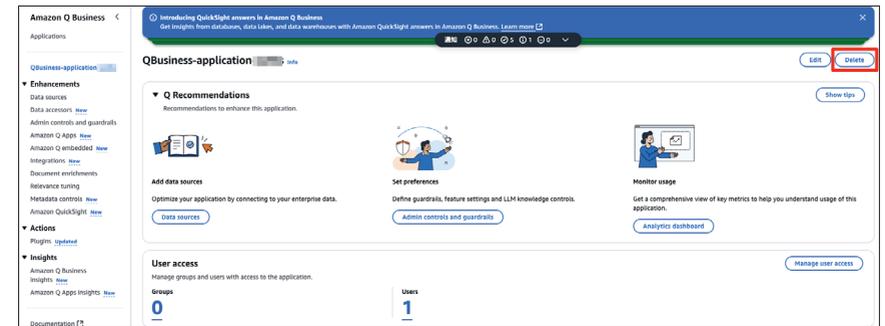
以下のような画面が表示されれば Amazon Q Business アプリへのアクセス成功です。



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も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。