

AWSアカウントの作成と設定

ハンズオンを進めるためにAWSアカウントを取得し、セキュリティ上最低限必要となる設定をしましょう。なお、既に個人または検証用のAWSアカウントを所有しており、そちらを利用できる方は新規で作成する必要はありません。

AWSアカウントの取得自体は簡単です。クレジットカードとスマートフォンを準備して始めましょう。

■AWSアカウントの作成

AWSのトップページにアクセスしてサインアップします。

検索エンジンで「aws」と検索すると、次のページがヒットします。アクセスしてみましょう。

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

ページにアクセスし、[無料でお試ください]あるいは画面右上の[AWSアカウントを作成]をクリックしてサインアップページに遷移しましょう。また、ページによってはボタンの名称が異なっている場合があることに注意してください。アカウントを作成するボタンから次に進みます。

図1 AWSのページからサインアップページへ進む



アカウントの作成画面が表示されます。英語で表示される場合は、画面右上のドロップダウンリストから「日本語」を選択しましょう。

以下の手順でアカウントの作成を行ってください。

- ① ログイン情報となるメールアドレス、AWS マネジメントコンソールへログインするためのパスワード、AWSアカウント名を入力します。

図2 サインアップページ①

- ② 連絡先情報となる、住所や電話番号等、詳細な個人情報を入力します。なお、入力は半角英数字のみしか受け付けません。住所は英語表記で入力します。電話番号については、日本の国番号は「81」となります。「+818012345678」のように入力します。

図3 サインアップページ②

③ 支払情報を入力します。

図4 サインアップページ③

日英辞書

aws

セキュアな検証

① AWS 無料利用枠内のご利用に対し、料金は発生しません。ご本人様確認のため、1-4 日後、i.m@amazon.co.jp 宛のメールとして通知が送信されます。

AWS にサインアップ

請求情報

クレジットカードまたはデビットカード番号

VISA

MasterCard

Amex

Discover

AWS では、ほとんどの主要なクレジットカードとデビットカードがご利用いただけます。詳細は「Amazon の支払い方法」では、よくある疑問をご確認ください。

有効期限日

▼

▼

カード保有者の氏名

☒ 連絡先住所を使用する

2-4-5 Roppongi
Minato-ku Tokyo 106-0032
JP


☐ 新しい住所を使用する


確認して進むへ (ステップ 4/5)

確認済みの請求先住所を承認するときに、銀行のオンラインアカウントリンクの登録が必要となります。

④SMSまたは電話による本人認証をします。SMSが簡単なのでこちらをオススメします。しばらくすると入力した番号宛てに認証コードが送られてきます。認証コードを入力して次に進みましょう。

図5 サインアップページ④





AWS にサインアップ

本人確認

AWS アカウントを登録する前に、電話番号を
検証する必要があります。続行すると、AWS
が電話システムから、任意の電話ユーザを
識別いたします。

検証ユーザの例の形式

- ① 日本電話番号 (9桁)
- ② 国際電話

国または地域コード

アメリカから


携帯電話番号


お手持の携帯電話


h y s t 4

上に表示された数字を入力してください

AWS 登録完了 (サインアップ)







AWS にサインアップ

本人確認

ユーザを確認

続行 (サインアップ)

お手持の携帯電話番号を入力してください。番号は
国コードを含む必要があります。お手持の国
番号から付いている場合は、番号の+を省略し、
国コードのみを入力してください。

- ⑤ サポートプランを選択します。まずは、無料のベーシックで問題ありません。
サポートプランはあとから変更も可能です。

図6 サインアップページ⑤



以上で、アカウントの作成が完了しました。登録したメールアドレス宛にウェルカムメールも届いているはずです。

図7 AWSアカウントのサインアップ完了



さっそくAWS マネジメントコンソールへアクセスしてみましょう。AWSトップページの [コンソールにサインイン] をクリックします。

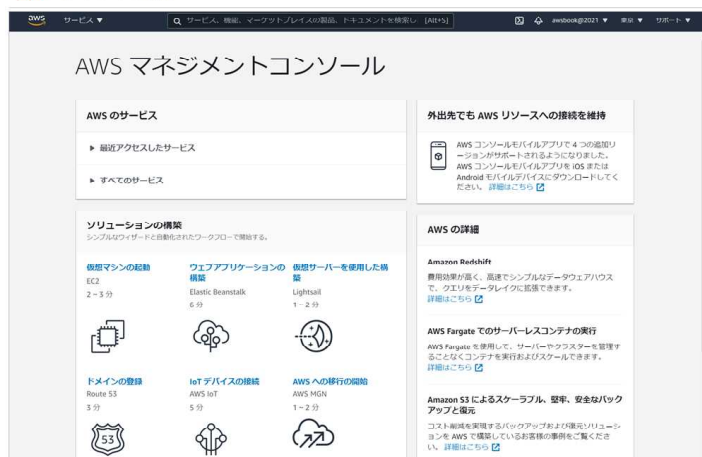
サインインページが開いたら、[ルートユーザー]を選択し、先ほど登録したメールアドレスとパスワードを入力しサインインしましょう。

図8 サインインページ



サインインをすると、次のようなページが表示されます。

図9 サインイン完了

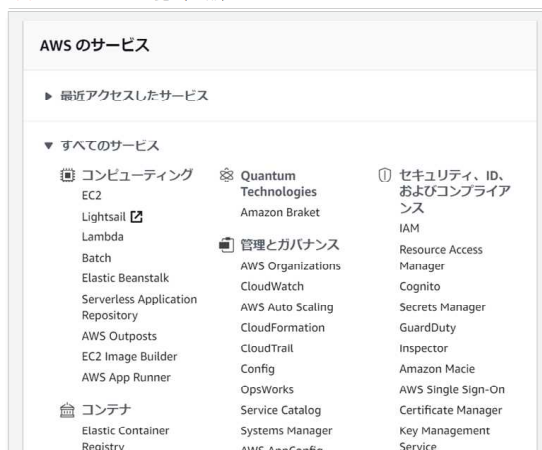


画面にある、[すべてのサービス]という文字をクリックすると、アコーディオンが展開されて、数多くのサービスが表示されます(画面は2021年9月時点のものです)。一昔前はマネジメントコンソールのトップにサービス名が並んでいました。AWSが急速な進化を遂げて、サービスを一画面で表示できなくなったあたりから、サービス名が折りたたまれています。

喜ばしいことですが、サービスが膨大であるため、一覧から目当てのサービスを探すことが非常に大変になりました。画面上部にある検索バーを利用して目当

てのサービスへ遷移するとよいでしょう。

図10 サービス一覧（一部）



■MFA(Multi-Factor Authentication)の設定

AWS マネジメントコンソールにサインインして最初に実施することは、「**MFA**」の設定です。

近年、リスト型アカウントハッキング(IDとパスワードのペアでログインを試みる攻撃)が増加しています。これに対抗する1つの対策として、多要素認証(MFA)が用いられます。特に、**現在ログインしているユーザーは「ルートユーザー」**と呼ばれ、AWSアカウントに対するあらゆる権限を所有しています。ルートユーザーを乗っ取られると、AWSのリソースを自由に使われてしまい、高額請求をされたり犯罪に利用されることがあります。

こういった事態を避けるためにAWS上のセキュリティプラクティスとしては次のことが強く推奨されています。

- ・ルートユーザーにはMFAを必ず設定する
- ・日常的なタスクには、それが管理者タスクであっても、ルートユーザーを使用しない^{※1}

まずは早急にMFAの設定をしておきましょう。

※1 https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_root-user.html

●MFAデバイスの用意

MFAを利用するためには、**認証コードを発行するデバイス**が必要になります。これを「MFAデバイス」と呼びます。MFAには仮想MFAデバイスやセキュリティキー、ハードウェアMFAデバイス等があります。それぞれの特徴については今回は割愛します。今回はお持ちのスマートフォンを仮想MFAデバイスとして利用します。

仮想MFAデバイスには、スマートフォン用アプリケーションを利用します。利用できるアプリケーションはAWSの公式サイトのMFAのページを参照してください。対象のアプリケーションをスマートフォンにインストールして利用します。筆者は「Authy」を日常的に利用しています。

[AWS公式サイトのMFAのページ\(英語\)](#)

<https://aws.amazon.com/jp/iam/features/mfa>

図11 仮想MFAデバイスとして動作するアプリケーション一覧

Android	Authy , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator
iPhone	Authy , Duo Mobile , LastPass Authenticator , Microsoft Authenticator , Google Authenticator

●MFAの設定

アプリケーションのインストールが完了したら、MFAの設定を行います。

AWS マネジメントコンソール上部の[サービス]タブより「IAM」を選択します。IAMのトップページ(ダッシュボード)に、「セキュリティアラート」と表示されています。[MFAを有効]のリンクをクリックしましょう。

セキュリティ認証情報のページに遷移したはずですが。画面に表示されている[MFAの有効化]をクリックしてMFA設定を行います。

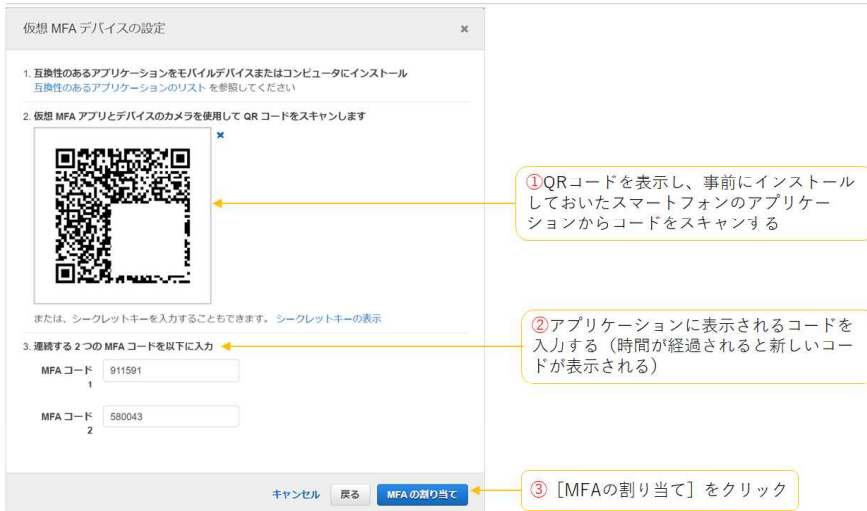
図12 セキュリティ認証情報ページ



図13 MFA設定①



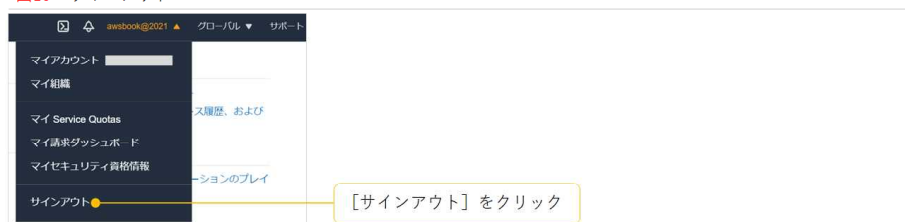
図14 MFA設定②



以上で、MFAの設定は完了です。設定完了のポップアップを閉じて、IAMのダッシュボードに戻ります。左側のナビゲーションから[ダッシュボード]を選択して遷移します。先ほどまで表示されていたセキュリティアラートが消えていることが確認できます。

それでは一度、サインアウトをしてMFAを利用したサインインができることを確認しましょう。

図15 サインアウト



AWSのトップページに戻りますので、再度同じ手順でサインインをしましょう。同様にメールアドレス、パスワードを入力して画面を進めるとMFAコードが求められます。仮想MFAデバイスに表示されるコードを入力しましょう。正しいMFAコードを入力すると、AWS マネジメントコンソールへログインできます。

このように、今後ログインする際にはMFAコードが求められます。仮想MFAデバイスの管理には十分に気を付けましょう。

■その他のやるべき設定

ルートユーザーのセキュリティの強化後にも実施すべき項目はいくつかあります。ここでは、それぞれの作業はCloudFormationを利用して自動設定をします。

まずは、設定すべき内容について1つずつ触れていきます。その後、CloudFormationのテンプレートを取得し、CloudFormationを実行します。

●IAMユーザーの作成

次にやるべきことは、IAMユーザー(AWS マネジメントコンソールで利用するユーザーアカウント)の作成となります。

前述の通り、AWSを操作する際はルートユーザーを利用せず、IAMユーザーを使用するためです。

用途別に細かく権限制御ができることや、必要な権限のみに制限しておくことで、IAMユーザーが乗っ取られた場合においても被害を軽減できるためです。プライベートで個人利用する場合であっても、**必ずIAMユーザーを作成し、ルートユーザーの利用はしないでください。**

今回は「sbcntr-user」というユーザーを作成します。また、IAMユーザーをグループ化することで同じ役割を持ったIAMユーザーに対しての権限付与が簡単になります。この機能はIAMグループを作成し、IAMグループにIAMユーザーを追加することで実現します。今回は、「Administrator」というIAMグループを作成します。次にAdministratorグループに対して、権限付与をするために、IAMポリシーを付与します。今回付与するIAMポリシーは、AWSが管理するIAMポリシーを利用します。基本的な操作が一通り可能な「AdministratorAccess」管理ポリシーを付与しましょう。最後に、Administratorグループに今回利用するIAMユーザーを追加することで、「AdministratorAccess」管理ポリシーで規定された権限のIAMユーザーによる操作が可能となります。

●パスワードポリシーの設定

IAMユーザーに設定するパスワードのルールを決めることができます。**文字数の長さの制限、文字種類の制限、有効期限等を設定**できます。

これらの設定は組織や用途に応じて設定してください。ただし、複雑なパスワードポリシーを設定した場合であっても必ずMFAを設定することをオススメします。

●AWS CloudTrailの有効化

作成したAWSアカウント上で、誰がいつ、どのような操作をしたか記録することが重要です。記録を残しておくことで、予期せぬトラブルの原因の特定、変更管理、不正な操作の監視等、さまざまな用途で利用できます。

AWSへの操作はAWS マネジメントコンソールやAWS CLI、AWS SDK等、多様な方法があります。しかし、**いずれの操作も全てAPIを通じた操作**となっています。つまり、APIの操作を監視しておけば、どの方法で操作された場合であっても操作を監視できます。

AWS CloudTrailをONにすると、APIの操作の監視を自動で実施できます。必ずオンにしておきましょう。

●各種設定の適用

それでは、テンプレートファイルを利用して、CloudFormationを実行しましょう。AWS マネジメントコンソール上部の[サービス]タブより「CloudFormation」を選択します。リージョンは「東京」を選択します。

図16 リージョンは東京リージョンを選択



テンプレートファイルは次のURLより取得します。テンプレートファイルは本書のサポートページ(<https://isbn2.sbcr.jp/07654/>)でも配布しています。

<https://github.com/uma-arai/sbcntr-resources/tree/main/cloudformations/appendix1.yml>

[スタックの作成]をクリックし、CloudFormationの実行をします。以下の図に従って作業を進めてください。

図17 各種設定の適用①

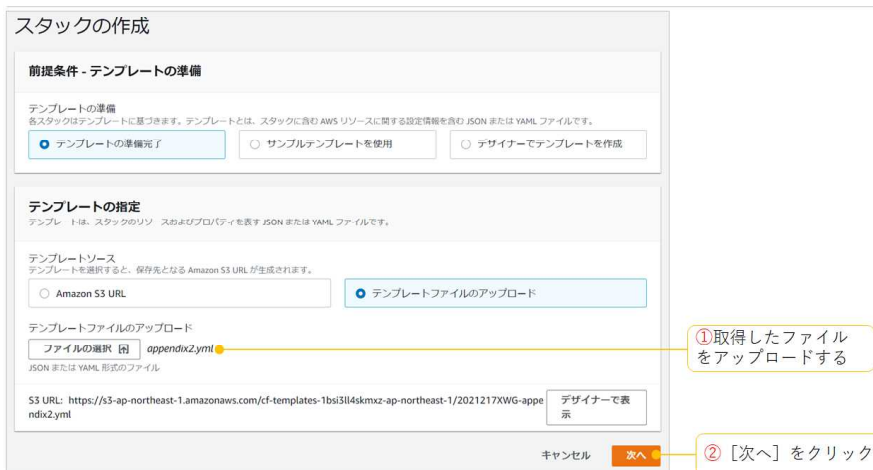


図18 各種設定の適用②

スタックの詳細を指定

スタックの名前

スタックの名前

base-settings

スタック名では、大文字および小文字 (A-Z~a-z)、数字 (0-9)、ダッシュ (-) を使用することができます。

パラメータ

パラメータは、テンプレートで定義されます。また、パラメータを使用すると、スタックを作成または更新する際にカスタム値を入力できます。

InitialIAMPassword

Initial login password

キャンセル

戻る

次へ

①スタックの名前を設定する

② [次へ] をクリック

図19 各種設定の適用③

スタックオプションの設定

タグ

スタックのリソースに適用するタグ (キーと値のペア) を指定できます。スタックごとに一意のタグを 50 個まで追加できます。 [詳細はこちら](#)

キー

値

削除

タグの追加

アクセス許可

CloudFormation を使用して、スタックのリソースを作成、変更、削除する方法を明示的に定義する IAM ロールを選択します。ロールを選択しない場合、CloudFormation はユーザーの認証情報に基づき、アクセス許可を使用します。 [詳細はこちら](#)

IAM ロール - オプション

スタックで実行されるすべてのオペレーションで使用する CloudFormation の IAM ロールを選択します。

IAM ロール名

Sample-role-name

削除

詳細オプション

通知オプションやスタックポリシーなど、スタックのオプションを追加設定することができます。 [詳細はこちら](#)

▶ スタックポリシー

スタックの更新中の意図しない更新から保護するリソースを定義します。

▶ ロールバック設定

スタックの作成時および更新時にモニタリングする CloudFormation のアラームを指定します。オペレーションでアラームのしきい値を超過した場合、CloudFormation では値がロールバックされます。 [詳細はこちら](#)

▶ 通知オプション

▼ スタックの作成オプション

失敗時のロールバック

スタックの作成に失敗した場合にスタックをロールバックするかどうかを指定します。

☒ 有効

☐ 無効

タイムアウト

スタック作成がタイムアウトするまでの時間 (分)。

分

削除保護

スタックが誤って削除されるのを防ぎます。作成後は、スタックアクションを使用して更新することができます。

☐ 無効

☒ 有効

①誤って削除しないように、削除保護をオンにする

- 12 -

図20 各種設定の適用④



レビュー画面で設定内容を確認し、CloudFormationの実行をします。

CloudFormationのダッシュボードへ戻り、スタックの状態が「CREATE_COMPLETE」になるまで待ちます。

「CREATE_COMPLETE」になったことを確認し、各種リソースが作成されていることを確認しましょう。

- ・ IAMグループ
- ・ IAMユーザー
- ・ パスワードポリシー
- ・ CloudTrail用のS3バケット
- ・ CloudTrailの証跡

●IAMユーザーのパスワード/MFAを設定

最後にCloudFormationで作成したIAMユーザーのパスワードとMFAを設定し、サインインできることを確認しましょう。IAMダッシュボードの[ユーザー]から設定が可能です。

まずはパスワードの設定を行います。

図21 作成したIAMユーザーのパスワード設定①



図22 作成したIAMユーザーのパスワード設定②



図23 作成したIAMユーザーのパスワード設定③



図24 作成したIAMユーザーのパスワード設定④



自動生成されたパスワードが表示されます。[表示]ボタンを押して、クリップボードにパスワードをコピーするか、csvファイルをダウンロードしてパスワード情報を控えておきます。

この画面から続けてMFA設定も実施します。

図25 作成したIAMユーザーのMFA設定



MFAの設定画面が表示されます。ルートユーザーで実施した手順と同様の流れでMFAを設定してください。

設定完了後、『MFAデバイスの割り当て』に「(仮想)」と表示されていればOKです。

サインアウト前に、同画面にある[コンソールのサインインリンク]のURLをメモしてください。次のIAMユーザーのサインインで利用します。

メモをしたら、ルートユーザーをサインアウトして、[コンソールのサインインリンク]のURLをブラウザにコピーして遷移しましょう。アカウントIDがセットされた状態の「IAMユーザーとしてサインイン」ページが表示されたはずです。サインインをしましょう。

図26 作成したIAMユーザーでサインイン①

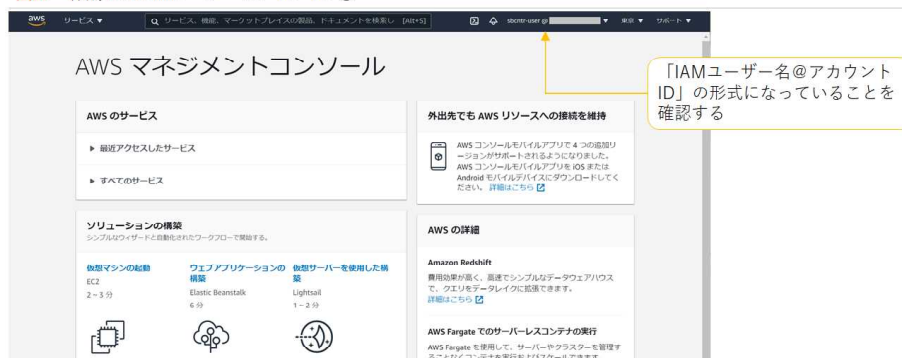


図27 作成したIAMユーザーでサインイン②



AWS マネジメントコンソールのトップ画面が表示されます。アカウント名の表示部分が「IAMユーザー名@アカウントID」となっていることを確認しましょう。

図28 作成したIAMユーザーでサインイン③



以上で、作成したIAMユーザーによるMFAを利用したサインインを確認できました。以後、こちらのIAMユーザーを利用してAWS マネジメントコンソールを操作してください。

今回、最低限のセキュリティ設定をCloudFormationから設定しました。高額請求を防ぐための課金アラーム、リソースの変更を検知するAWS Config、AWSアカウントやワークロードを保護するGuard Duty等、設定しておけば安心のサービスもいくつかあります。

作成したAWSアカウントの用途に合わせて、IAMグループ/ユーザーの追加やサービスの設定等を実施し、安全なAWSライフを楽しんでください。