AWS 資料
IMA ユーザの作成

改訂履歴

年月	版	作成者	詳細
2021年11月26日	1.0	青山	新規作成

内容

1. IAM ユーザの作成

1.1. 手順

① ログイン

② AWS Identity and Access Management (IAM)サービス画面に移動する

左上にある「サービス」をクリックするか、隣のカラムに「IAM」を入力します。

左ペインに「Identity and Access Management (IAM)」と出てきたら OK です。

1.2.　IAM ユーザーを作成する

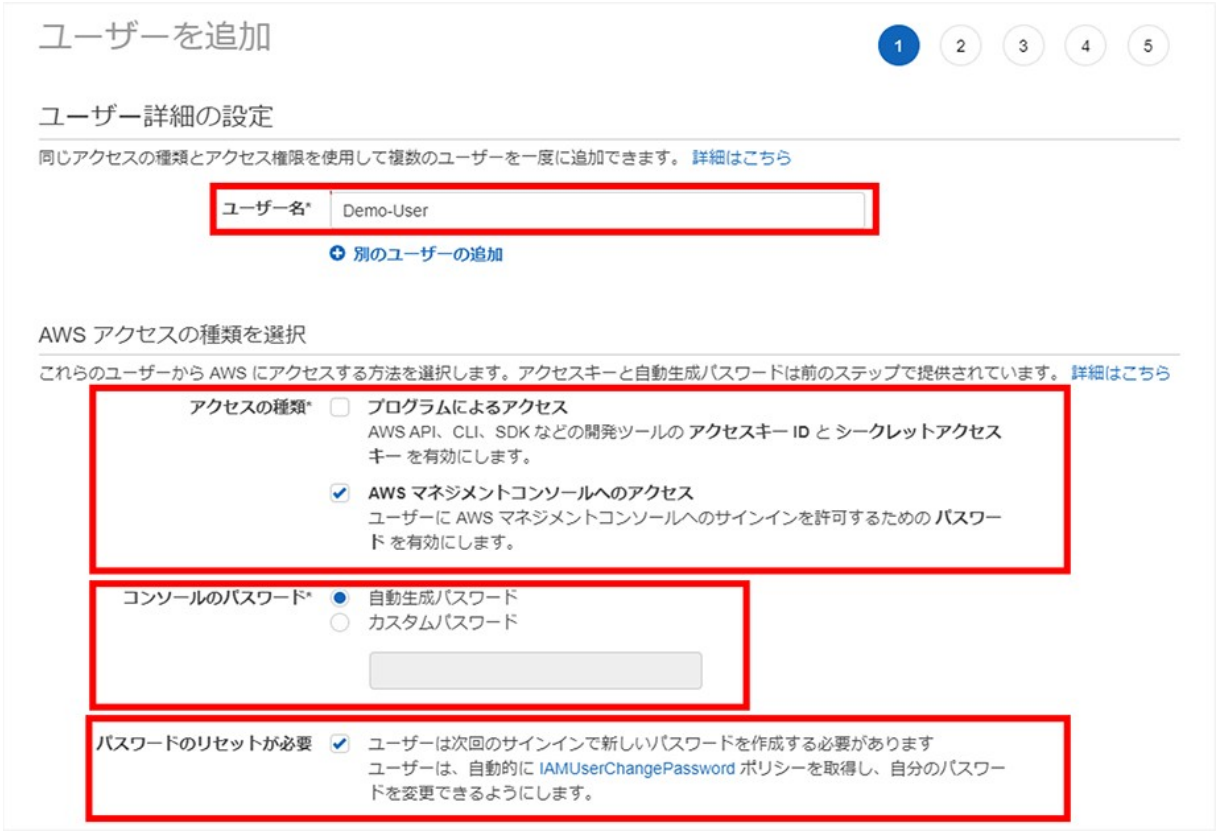
左ペインから、「ユーザ」をクリックしましょう。

ユーザーを追加」をクリックします。

ユーザーの設定をしていきます。

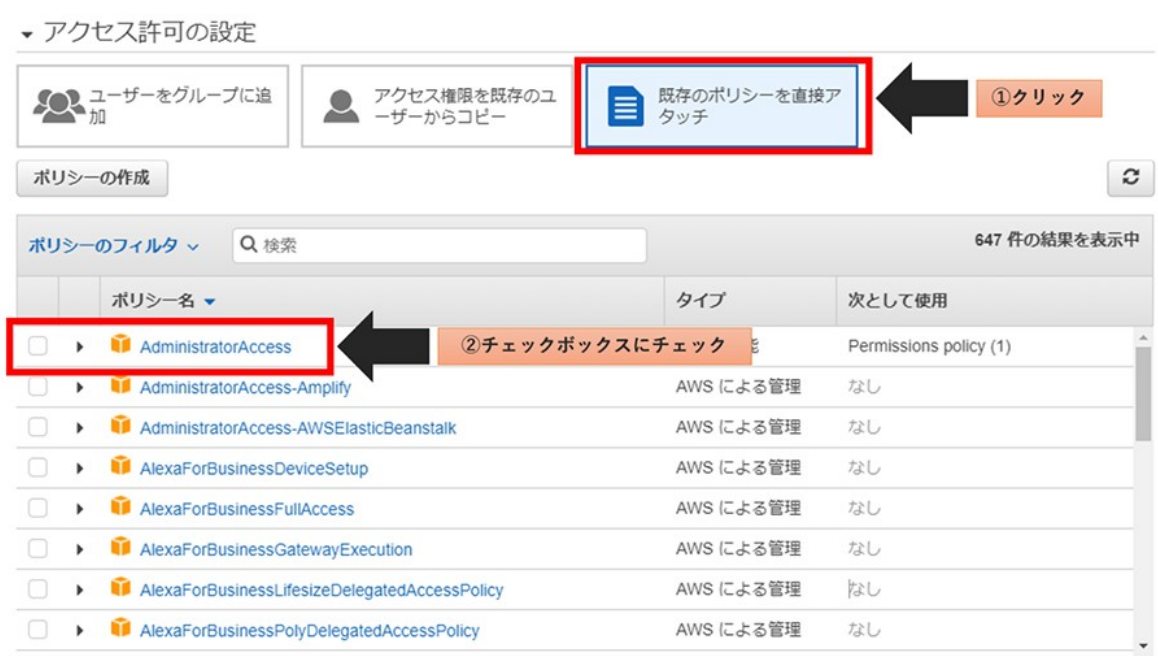
それぞれの設定を入力したら、右下から「次のステップ：アクセス権限」をクリックしてください。

設定値	設定内容
ユーザー名	IAM ユーザーの名前を設定してください。アカウントの中ではユニークである必要があります。
アクセスの種類	そのユーザーが許可されるアクセスの方法を設定してください。 プログラムによるアクセス：Amazon CLI などを利用したアクセス方法 AWS マネジメントコンソールへのアクセス：Web ブラウザを利用したコンソールへのアクセス方法
コンソールのパスワード	自動でパスワードを生成されるようにするか、自身でパスワードを指定するかを設定してください。
パスワードのリセットが必要	初回ログイン時にパスワード変更を求めるかを設定してください。



次の画面では、作成する IAM ユーザーに対して IAM ポリシー等を利用して権限を付与することが可能です。

詳細な設定はせず、下記項目を選択し、「次のステップ：タグ」をクリックしてください。



更に、「次のステップ：確認」をクリックします。

確認の画面が出てきますので、その画面上で「ユーザーの作成」をクリックしてください。

パスワードを自動で生成されるように設定した場合は、

「csv のダウンロード」か、「パスワード」で「表示」をクリックしてパスワードを確認してください。パスワード情報を確認できる画面はここだけですので注意してください。

確認が終わりましたら「閉じる」をクリックしてください。

2. 作成した IAM ユーザーに IAM ポリシーを適用する(1 で解決済み)

IAM ユーザーに対して、権限を新たに付与していきます。

ユーザ名をクリックします

つぎに、「アクセス権限の追加」をクリックしてください。

管理者権限用の IAM ポリシーをアタッチしていきます。

①「既存のポリシーを直接アタッチ」をクリックします

②「AdministratorAccess」（こちらが管理者権限の IAM ポリシーです）のチェックボックスをチェックします

操作が終わったら、「次のステップ：確認」をクリックしてください。

追加されるアクセス権限を確認し、「アクセス権限の追加」をクリックします。

追加した IAM ポリシーがアタッチされていることをご確認ください。

3. AWS アカウント（ルートアカウント）の保護

3.1. AWS アカウントへ二段階認証を導入

AWS アカウントでのログインは、AWS アカウント作成時のメールアドレス・パスワードだけでできてしまう。心許ないにもほどがあるので、まずは二段階認証を設定しよう。

3.1.1. IAM のページを開く

3.1.2. 「ルートアカウントの MFA を有効化」を選択して、「MFA の管理」ボタンをクリック

3.1.3. 「仮想 MFA デバイス」にチェックが入っていることを確認し、「次のステップ」ボタンをクリック

3.1.4. 注意書きを読んで、「今後はこのダイアログボックスを表示しない。」にチェックを入れて「次のステップ」ボタンをクリック

3.1.5. Google Authenticator などで、QR コードを読み取って、表示された認証コード二つを入力し、「仮想 MFA の有効化」ボタンをクリック

3.1.6. 「完了」ボタンをクリック

4. グループの作成

権限を設定したグループを作成し、ユーザを所属させます。

4.1. IAM のページを開く

https://console.aws.amazon.com/iam/home

4.2. 「グループを使用してアクセス許可を割り当て」を選択し、「グループの管理」ボタンをクリック

4.3. 「新しいグループの作成」ボタンをクリック

4.4. グループ名を入力し、「次のステップ」ボタンをクリック

4.5. 「AdministratorAccess」ポリシーにチェックをいれて、「次のステップ」ボタンをクリック

4.6. 内容を確認し、「グループの作成」ボタンをクリック

4.7. グループ一覧から作成したグループをクリック

4.8. 「グループにユーザーを追加」ボタンをクリック

4.9. 作成したユーザを選択し、「ユーザーの追加」ボタンをクリック

ここで設定している「AdministratorAccess」は、AWS アカウントに次ぐ強力な権限なので常用してはいけない。
AWS に慣れてきたら、適切な範囲の権限設定に変更します。

5. IAM パスワードポリシーの適用

デフォルトの設定では、パスワードポリシーがかなり緩いので、可能な範囲で縛りを入れよう。

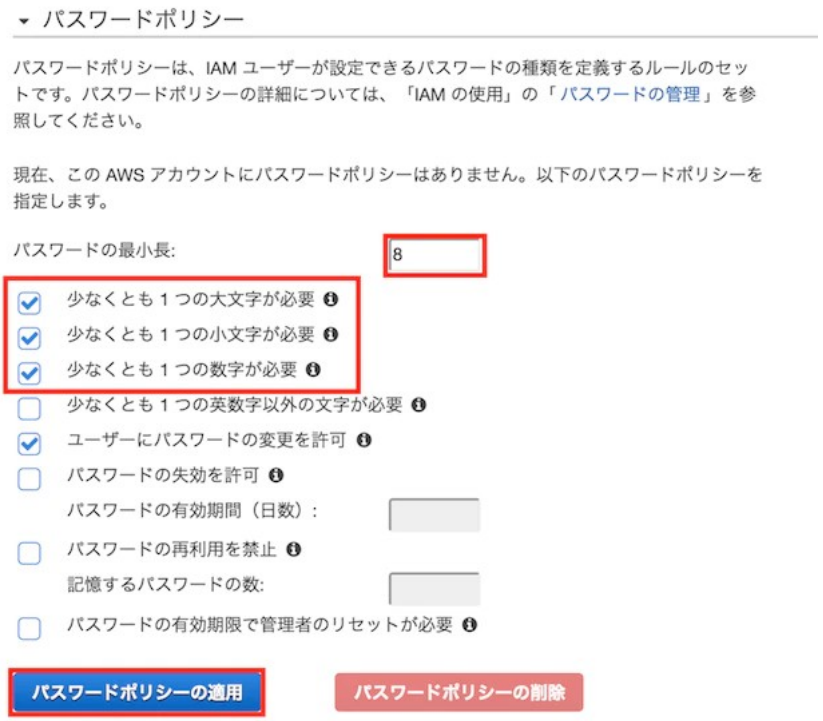
5.1. IAM のページを開く

https://console.aws.amazon.com/iam/home

5.2. 「IAM パスワードポリシーの適用」を選択し、「パスワードポリシーの管理」ボタンをクリック

5.3. 任意のパスワードポリシーを設定し、「パスワードポリシーの適用」ボタンをクリック

企業単位のセキュリティポリシーを適用します



オプションの設定はドキュメントを参照

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html