[AWS Black Belt Online Seminar]

AWS Identity and Access Management (AWS IAM) ~ベストプラクティスで学ぶAWSの認証・認可~ Part2

Sr. Manager, Solutions Architect
瀧澤 与一

2019/1/30

AWS 公式 Webinar
https://amzn.to/JPWebinar

過去資料
https://amzn.to/JPArchive

自己紹介

瀧澤 与一

技術統括本部 レディネス＆テックソリューション本部
本部長 / プリンシパルソリューション アーキテクト

普段の業務

お客様のクラウドジャーニーを技術的にサポート

好きなAWSサービス

AWS Identity and Access Management (IAM)
Amazon EC2, AWS Well-Architected, Amazon GuardDuty など

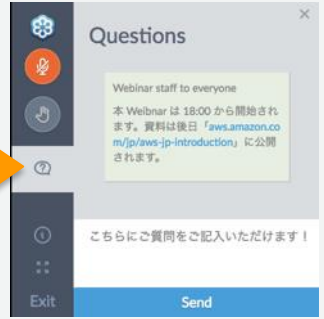
AWS Black Belt Online Seminar とは

「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2019年1月30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います。日本居住者のお客様が東京リージョンを使用する場合、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.

AWS IAMのベストプラクティス

IDと認証情報の管理	✓ AWSアカウントのルートユーザーアクセスキーをロックする ✓ 個々のIAMユーザーを作成 ✓ ユーザーの強力なパスワードポリシーを設定 ✓ アクセスキーを共有しない ✓ 特権ユーザーに対してMFAを有効化する
アクセス権限の管理	✓ AWS管理ポリシーを使用したアクセス許可の使用開始 ✓ インラインポリシーではなくカスタマー管理ポリシーを使用する ✓ 追加セキュリティに対するポリシー条件を使用する ✓ 最小権限を付与する ✓ IAMユーザーへのアクセス許可を割り当てるためにグループを使用する
権限の委任	✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する ✓ ロールを使用したアクセス許可の委任
IDと権限のライフサイクル管理	✓ AWSアカウントのアクティビティの監視 ✓ アクセスレベルを使用して、IAM権限を確認する ✓ 不要な認証情報を削除する ✓ 認証情報を定期的にローテーションする

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

AWS IAMのベストプラクティス

IDと認証情報の管理	✓ AWSアカウントのルートユーザーアクセスキーをロックする ✓ 個々のIAMユーザーを作成 ✓ ユーザーの強力なパスワードポリシーを設定 ✓ アクセスキーを共有しない ✓ 特権ユーザーに対してMFAを有効化する
アクセス権限の管理	✓ AWS管理ポリシーを使用したアクセス許可の使用開始 ✓ インラインポリシーではなくカスタマー管理ポリシーを使用する ✓ 追加セキュリティに対するポリシー条件を使用する ✓ 最小権限を付与する ✓ IAMユーザーへのアクセス許可を割り当てるためにグループを使用する
権限の委任	✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する ✓ ロールを使用したアクセス許可の委任
IDと権限のライフサイクル管理	✓ AWSアカウントのアクティビティの監視 ✓ アクセスレベルを使用して、IAM権限を確認する ✓ 不要な認証情報を削除する ✓ 認証情報を定期的にローテーションする

Part 1

Part 2

(本日お話する範囲)

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

本日のアジェンダ

- AWS IAMの概要
- 権限の委任
- IDと権限のライフサイクル管理
- IAM Tips
- まとめ

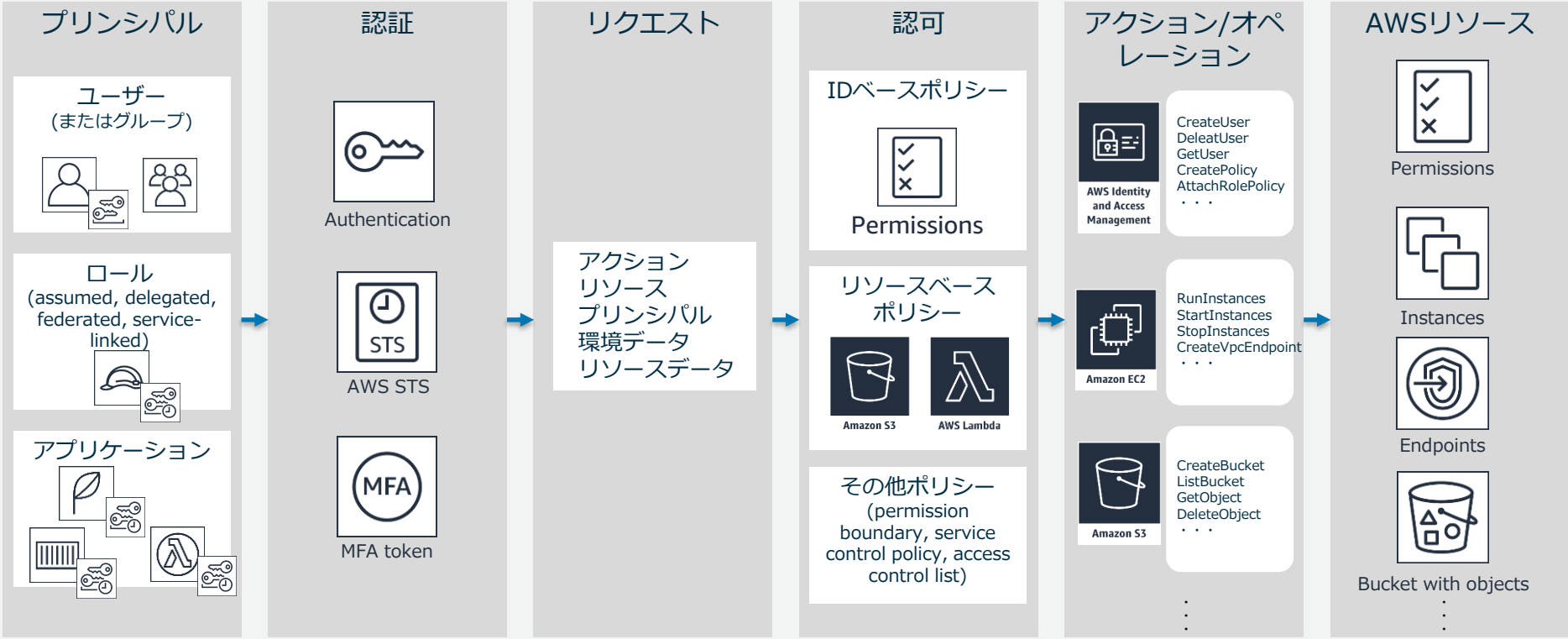
AWS IAMの概要

AWS Identity and Access Management (IAM)とは

- AWSリソースをセキュアに操作するために、認証・認可の仕組みを提供するマネージドサービス

- 各AWSリソースに対して別々のアクセス権限をユーザー毎に付与できる
- 多要素認証(Multi-Factor Authentication : MFA)によるセキュリティの強化
- 一時的な認証トークンを用いた権限の委任
- 他のIDプロバイダーで認証されたユーザーにAWSリソースへの一時的なアクセス
- 世界中のAWSリージョンで同じアイデンティティと権限を利用可能
  - データ変更は結果整合性を保ちながら全リージョンに伝搬
- AWS IAM自体の利用は無料

AWSリソースにアクセスするしくみ



権限の委任

- ✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する
- ✓ ロールを使用したアクセス許可の委任

IAMロール

- AWSサービスやアプリケーション等のエンティティに対してAWSリソースの操作権限を付与するための仕組み
  - ユーザーまたはアプリケーションがロールを一時的に“引き受ける”ことで関連付けられたアクセス許可を受けることができる
  - IAMユーザーやグループには紐付かない

- 認証方法
  - 一時的なセキュリティ認証情報を利用
- 複数のユーザーがロールを引き受け可能
  - 別のAWSアカウントのIAMユーザー, ロール等
  - Amazon EC2、AWS Lambda等のAWSサービス
  - SAML2.0またはOpenID Connect (OIDC) と互換性があるIDプロバイダーによって認証された外部ユーザー

aws

一時的なセキュリティ認証情報

- 有効期限付きのアクセスキーID/シークレットアクセスキー/セキュリティトークンで構成
    - 短期的な有効期限 (認証情報を取得する際に期限を設定)
    - 認証情報が不要になった時にローテーションしたり明示的に取り消す必要がない (ユーザー側に認証情報が保存されない)のでより安全
- ユーザーのリクエストによってAWS Security Token Service (STS) が動的に作成

AWS Security Token Service (STS)

- 一時的なセキュリティ認証情報を生成するサービス
  - 期限付きのアクセスキー/シークレットアクセスキー/セッショントークン
  - トークンのタイプにより有効期限は様々
- 発行した認証情報の期限の変更は不可
  - 必要がある場合は、特定の時点より前に発行したロールの認証情報の、すべてのアクセス許可をすぐに取り消し可能。
- STSエンドポイントは全リージョンで使用可能
  - デフォルトではグローバルサービスとして利用
  - 各リージョンのSTSエンドポイントでアクティベート可能
    - レイテンシーの低減
    - 冗長化の構築
  - PrivateLinkに対応 (オレゴンリージョンのみ*)
  - アクティベートしたリージョンでCloudTrailを有効化

*2019年1月29日時点

一時的なセキュリティ認証情報を取得するためのAPI

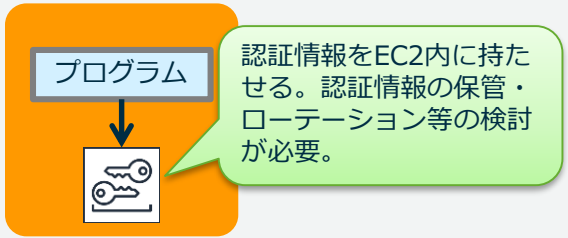
STSで利用できるAPI Action	概要
AssumeRole	既存のIAMユーザーの認証情報を用いて、IAM Roleの temporary security credentialsを取得するためのアクション
AssumeRoleWithWebIdentity	AmazonやFacebook、Googleによる承認情報を使用してロールを引き受け、temporary security credentialsを取得するためのアクション
AssumeRoleWithSAML	IdPによる認証とSAMLのアサーションをAWSにポストすることでロールを引き受けtemporary security credentialsを取得するためのアクション
GetSessionToken	自身で利用するIAMユーザーのtemporary security credentialsを取得するためのアクション
GetFederationToken	認証を受けたFederatedユーザーのtemporary security credentialsを取得するためのアクション

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp_request.html

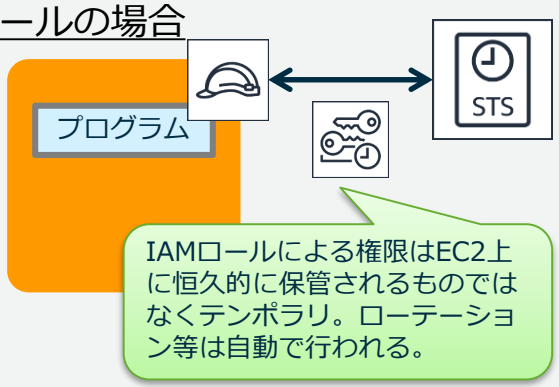
✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する Use Roles for Applications That Run on Amazon EC2 Instances

- アプリケーションがAWSサービスにアクセスするためには認証情報が必要
- 認証情報をEC2 (OS/アプリケーション) 側に持たせる必要がない、認証情報の漏洩リスクを低減可能
- IAMロールによる認証情報はAWSが自動的にローテーション
- AWS SDKによって認証情報取得と有効期限切れ前の再取得を自動的に実施可能
- AWS CLIもIAMロールに対応済み

IAMユーザーの場合



IAMロールの場合



権限の委任

- ✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する
- ✓ ロールを使用したアクセス許可の委任

ロールを使用したアクセス許可の委任の例

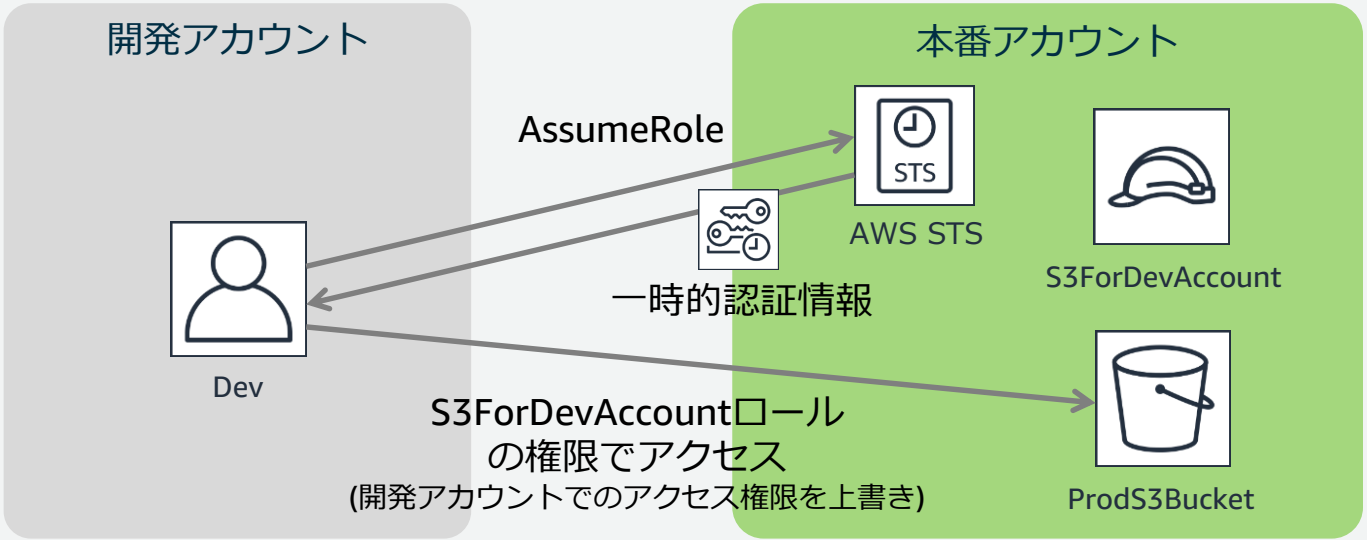
別の AWS アカウントのユーザーが、認証情報を共有せずに、自分の AWS アカウントのリソースにアクセスを制御可能にすることが可能。

ユースケース：

1. IAMロールによるクロスアカウントアクセス
2. クロスアカウントアクセスにより権限管理を効率化
3. SAML2.0ベースのIDフェデレーション
4. SAML2.0ベースのAWSマネジメントコンソールへのシングルサインオン (SSO)
5. Amazon Cognitoを用いたモバイルアプリのWeb IDフェデレーション

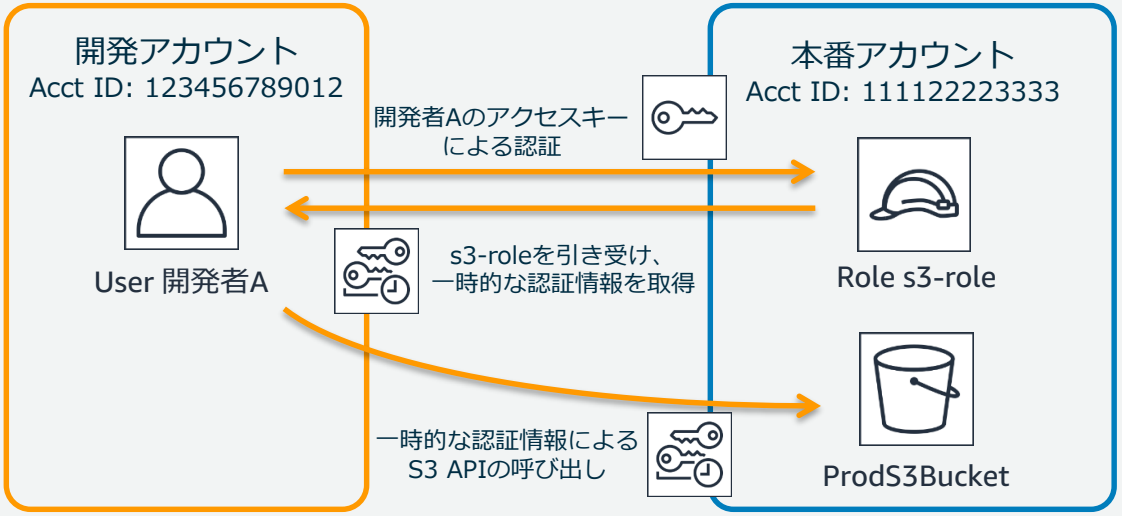
ユースケース：IAMロールによるクロスアカウントアクセス

- あるアカウントのユーザーに別のアカウントのIAMロールに紐づける機能
- 例えば開発アカウントを使って、本番環境のS3データを更新するようなケースで利用



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html

IAMロールによるクロスアカウントアクセスの動作



s3-roleに付与されているポリシー

```
{ "Statement": [
{
  "Effect": "Allow",
  "Action": “s3:*",
  "Resource": "*"
 }
]
}
```

```
{ "Statement": [{
  "Effect": "Allow",
  "Action": “sts:AssumeRole",
  "Resource": "arn:aws:iam::111122223333:role/s3-role"
 }
]
}
```

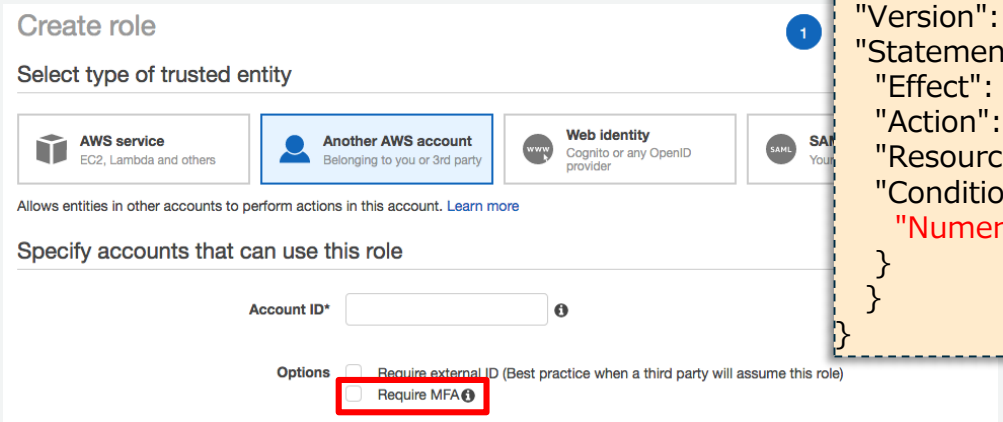
本番アカウントのs3-roleの引き受けを許可するポリシーを開発者Aに設定

```
{ "Statement": [{
  "Effect":"Allow",
  "Principal":{"AWS":"arn:aws:iam::123456789012:root"},
  "Action":"sts:AssumeRole"
 }
]
}
```

s3-roleを誰が引き受けられるか定義した信頼ポリシーをs3-roleに設定

クロスアカウントアクセスのためのMFA保護

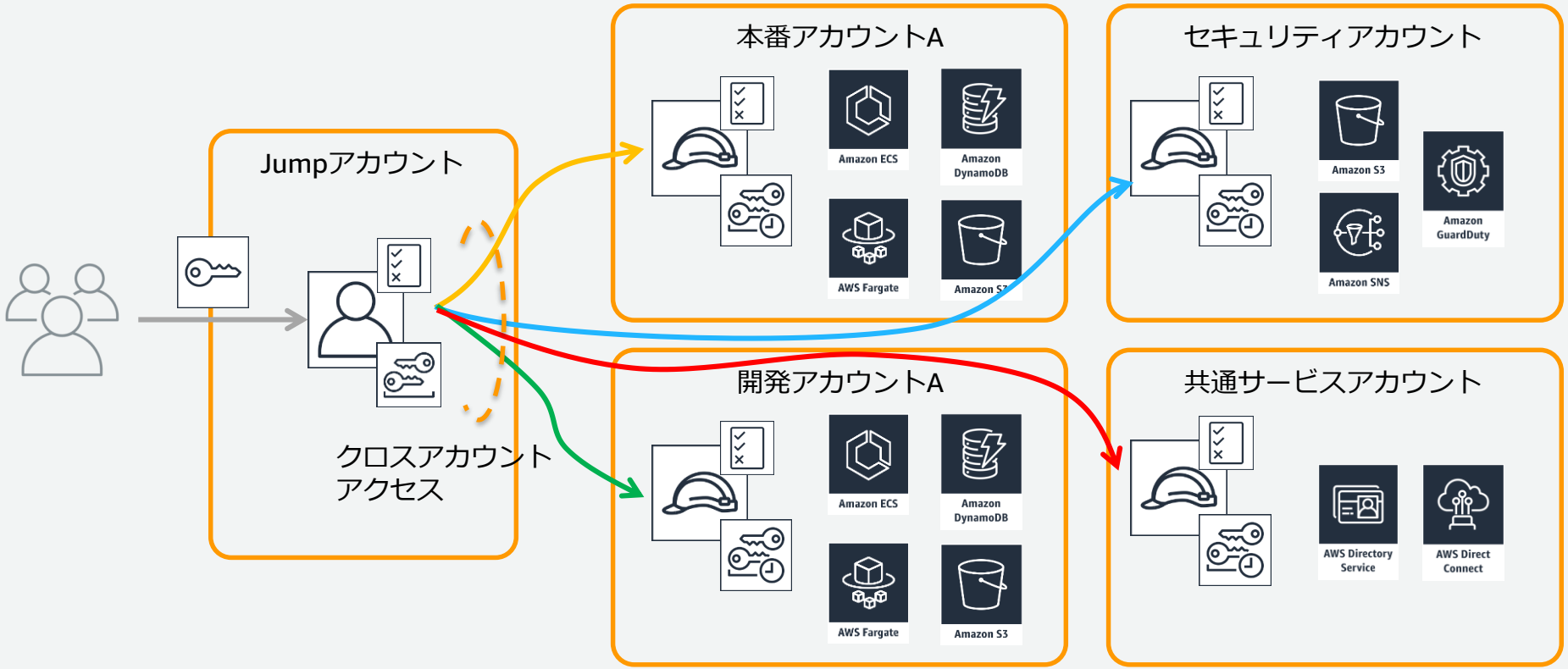
- AWSアカウント間でのアクセスのためのMFA保護を追加する機能
- AWSマネージメントコンソールでroleを作成する際に、Require MFAのチェックボックスを選択することで設定可能
- MFA認証されたユーザーのリクエストのみが有効に
  - MFAしたかどうか："Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
  - 一定時間内のMFA："Condition": {"NumericGreaterThanIfExists": {"aws:MultiFactorAuthAge": "3600"}}




```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "ec2:*",
   "Resource": "*",
   "Condition": {
     "NumericLessThan": {"aws:MultiFactorAuthAge": "3600"}
   }
  }
}
```


https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa_sample-policies.html

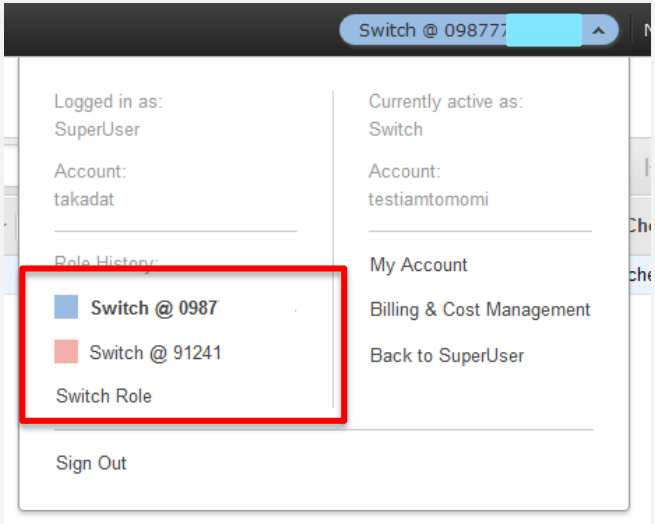
ユースケース：クロスアカウントアクセスにより権限管理を効率化



Switch Role

- IAMユーザーからクロスアカウントアクセス用IAMロールにコンソールから切替が可能
  - 必ずしも別アカウントである必要はなく、同じアカウントでもOK

- 必要な時のみIAMユーザーの権限を “昇格”させる
  - IAMユーザーには読み取り権限のみを付与
  - IAMロールには更新権限を付与

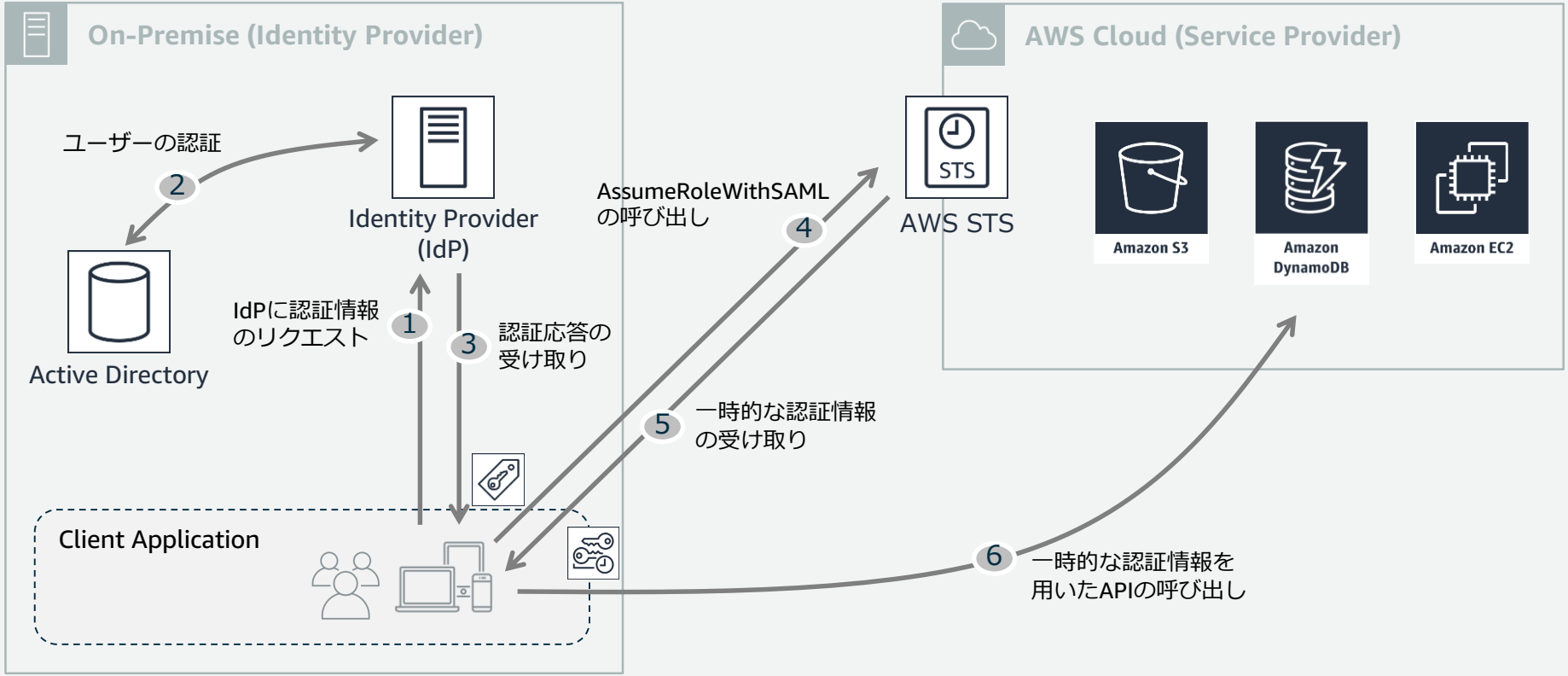


https://aws.amazon.com/blogs/aws/new-cross-account-access-in-the-aws-management-console/

ユースケース：SAML2.0ベースのIDフェデレーション

- SAML2.0を使用した IDフェデレーション
- 組織内の全員についてIAMユーザーを作成しなくても、ユーザーはAWSを利用可能
- 組織で生成した SAMLアサーションを認証レスポンスの一部として使用し、一時的セキュリティ認証情報を取得
- ユーザーは一時的セキュリティ認証情報でAWSのリソースにアクセス

SAML2.0ベースのIDフェデレーションの動作



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_saml.html

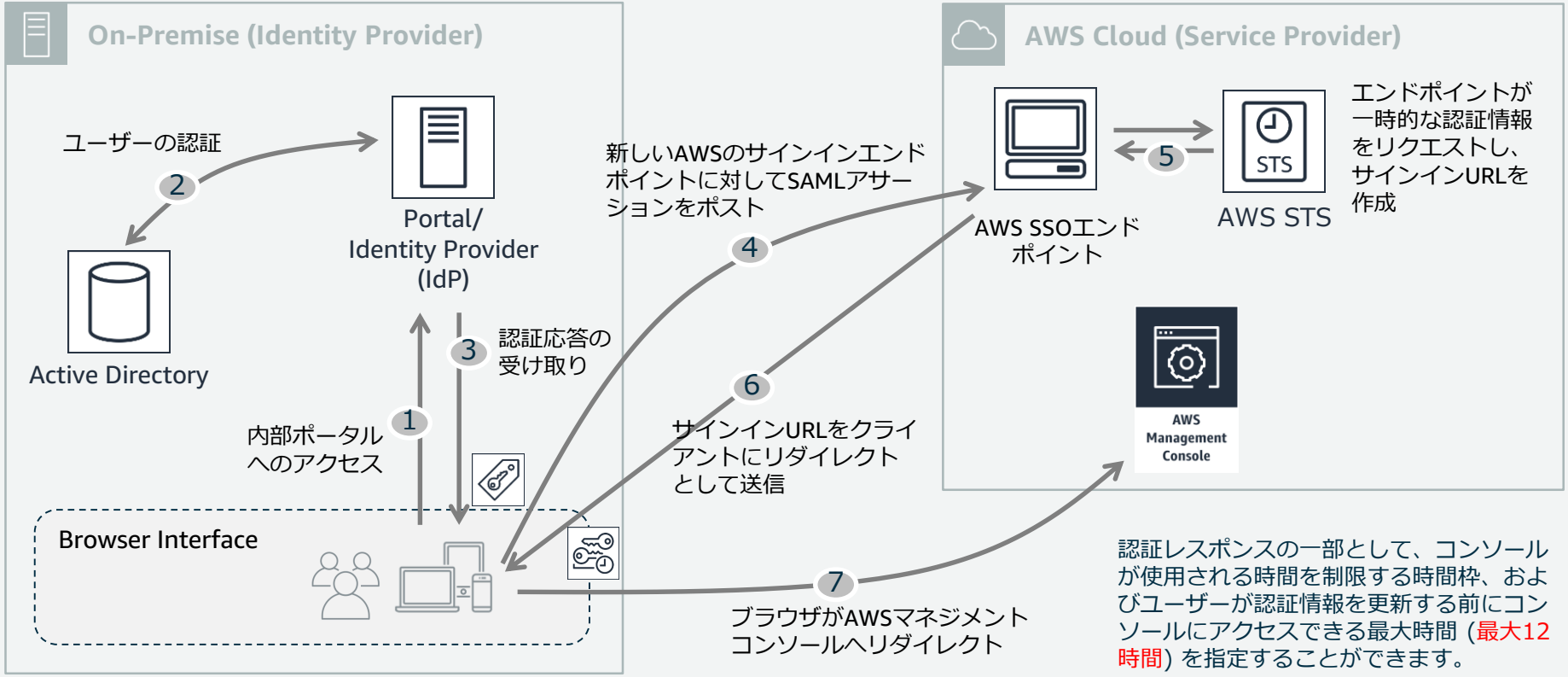
ユースケース：SAML2.0ベースのAWSマネジメントコンソールへのシングルサインオン (SSO)

- SAML 2.0互換IdPおよびIAMロールを使用した管理コンソールへのフェデレーションアクセス

- AssumeRoleWithSAML API を直接呼び出す代わりに、AWS SSO エンドポイントを使用する必要があります。エンドポイントはユーザーの代わりに API を呼び出し、URL を返すと、それによってユーザーのブラウザーが AWS マネジメントコンソールへ自動的にリダイレクトされます。

- エンドポイントはユーザーの代わりにAPIを呼び出し、URL を返すと、それによってユーザーのブラウザーがAWSマネジメントコンソールへ自動的にリダイレクト

SAML2.0ベースのAWSマネジメントコンソールへのSSOの動作



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

AWSマネジメントコンソールフェデレーションのメリット

- アカウント管理が統合され、リスクが低減する
- 既存のユーザ情報をそのまま利用
- 既存の権限ベースでの管理が可能
- 既存と同様のポリシーの利用が可能
  - アカウントロックポリシーや、パスワード管理ポリシー
- 入退社など一元的な管理が可能
- イントラネットからのみアクセス可能なログイン画面

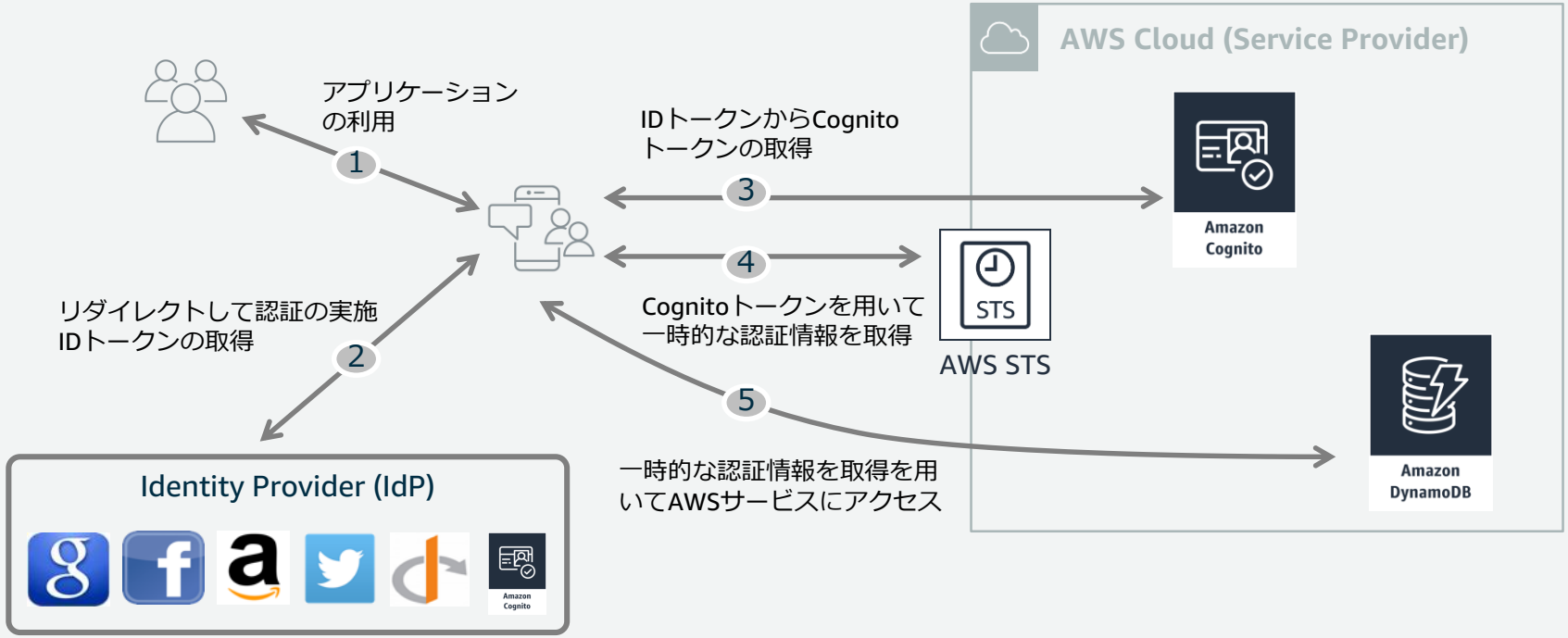
ユースケース：Amazon Cognitoを用いたモバイルアプリのWeb IDフェデレーション

- モバイルアプリから一時的なAWSセキュリティ認証情報を必要に応じて動的にリクエスト

- 認証を確認するサーバが不要
  - 例えばスマートフォンアプリとS3だけでシステムが作成可能

- 現在Google,Facebook,Amazon(Login with Amazon), twitter, Amazon Cognito及びOIDC準拠のIdPに対応

Amazon Cognitoを用いたモバイルアプリのWeb IDフェデレーションの動作



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_oidc_cognito.html

フェデレーション/SSOのパートナーソリューション

https://aws.amazon.com/jp/iam/partners/

✓ ロールを使用したアクセス許可の委任

Use Roles to Delegate Permissions

- アカウント間でセキュリティ認証情報を共有しないでください。
- これは、別の AWS アカウントのユーザーがお客様の AWS アカウントのリソースにアクセスできないようにするため。その代わりに、IAM ロールを使用します。他のアカウントの IAM ユーザーに許可されている権限を指定するロールを定義できます。

IAMロール利用の利点

- EC2上のアクセスキーの管理が容易
- 認証情報はSTS(Security Token Service)で生成
- 自動的に認証情報のローテーションが行われる
- EC2上のアプリケーションに最低権限を与えることに適している
- IAMユーザーの認証情報を外部に漏えいしてしまうリスクを低減させる

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/roles-resourcebasedpolicies-compare.html

権限の委任に関するベストプラクティス

- ✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する
- ✓ ロールを使用したアクセス許可の委任

IDと権限のライフサイクル管理

- ✓ AWSアカウントのアクティビティの監視
- ✓ アクセスレベルを使用して、IAM権限を確認する
- ✓ 不要な認証情報を削除する
- ✓ 認証情報を定期的にローテーションする

AWSアカウントのアクティビティの監視とは？
例えば、AWS CloudTrail

- AWS アカウントで行われた AWS API コールおよび関連イベントを記録。

AWS CloudTrail

AWSのリソースにどのような操作が加えられたか記録に残す機能であり
全リージョンでの有効化を推奨。
適切なユーザーが与えられた権限で環境を操作しているかの確認と記録に使用。

記録される情報には以下のようなものが含まれる

- APIを呼び出した身元（Who）
- APIを呼び出した時間（When）
- API呼び出し元のSource IP（Where）
- 呼び出されたAPI（What）
- APIの対象となるAWSリソース（What）
- 管理コンソールへのログインの成功・失敗

✓ AWSアカウントのアクティビティの監視

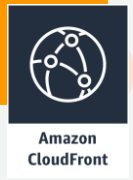
Monitor Activity in Your AWS Account

AWS のロギング機能を有効にして、ユーザーがアカウントで実行したアクションや使用されたリソースを確認してください。

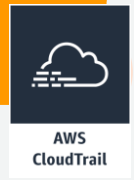
ログファイルには、アクションの日時、アクションのソース IP、不適切なアクセス許可のために失敗したアクションなどが示されます。

アクティビティを監視可能なAWSサービスの例

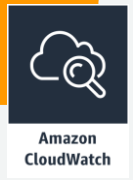
Amazon CloudFront
- CloudFront が受信したユーザーリクエストを記録。



AWS CloudTrail
- AWS アカウントで行われた AWS API コールおよび関連イベントを記録。

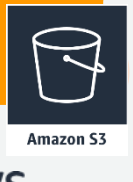


Amazon CloudWatch
- AWS クラウドリソースと AWS で実行されるアプリケーションをモニタリング記録



AWS Config
- IAM ユーザー、グループ、ロール、およびポリシーを含む、AWS リソースの設定に関する詳細な履歴情報

Amazon S3
- Amazon S3 バケットへのアクセスリクエストを記録

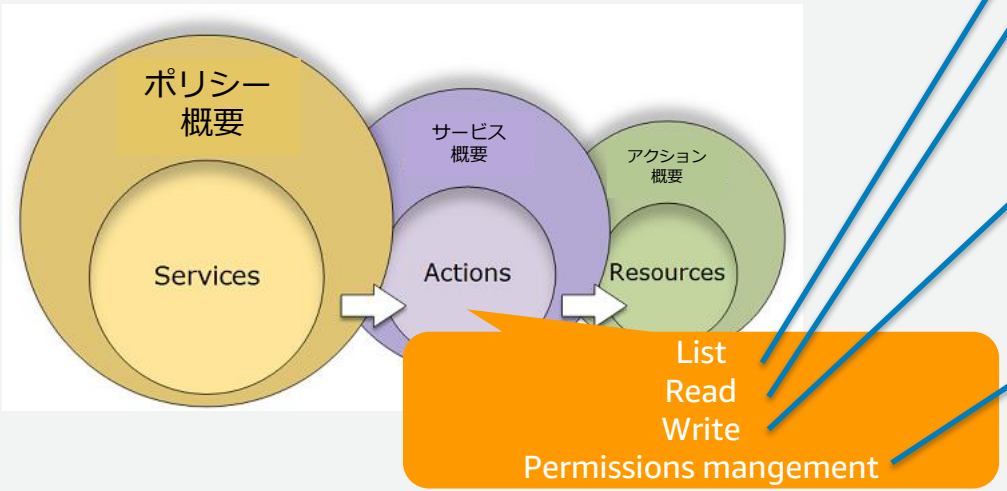


IDと権限のライフサイクル管理

- ✓ AWSアカウントのアクティビティの監視
- ✓アクセスレベルを使用して、IAM権限を確認する
- ✓ 不要な認証情報を削除する
- ✓ 認証情報を定期的にローテーションする

アクセスレベルとは？

アクセスレベルは、1)リスト（**List**）、2)読み込み（**Read**）、3)書き込み（**Write**）、4)アクセス権限の管理（**Permissions management**）で分類され、ポリシー概要にサービスが含まれる場合、そのアクセスレベルを定義。



アクセス権限 | ポリシーの使用状況 | ポリシーのバージョン | アクセスアドバイザー

‹ 戻る S3

ポリシー概要 | { } JSON

フィルター

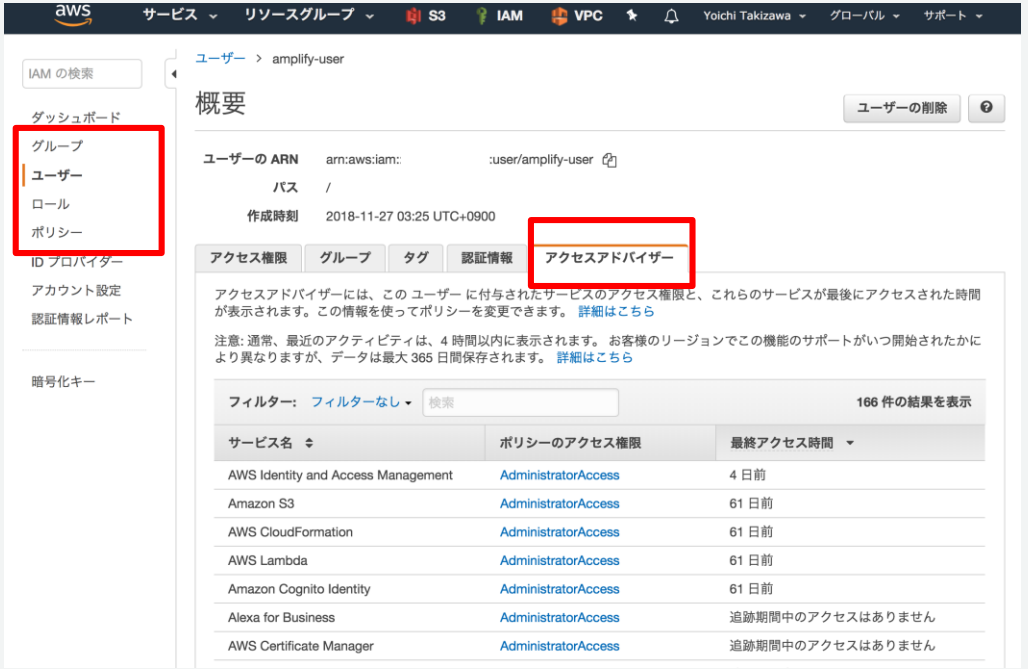
アクション (73) の {{actionsTable.knownActions.data.length}}) 残りの 62 を表示	リソース	リクエスト条件
リスト (3 アクション中1)		
ListBucket	BucketName | string like | dms-*	なし
読み込み (33 アクション中4)		
GetBucketLocation	BucketName | string like | dms-*	なし
GetBucketPolicy	BucketName | string like | dms-*	なし
GetObject	BucketName | string like | dms-*	なし
GetObjectVersion	BucketName | string like | dms-*	なし
書き込み (29 アクション中4)		
CreateBucket	BucketName | string like | dms-*	なし
DeleteBucket	BucketName | string like | dms-*	なし
DeleteObject	BucketName | string like | dms-*	なし
PutObject	BucketName | string like | dms-*	なし
アクセス権限の管理 (8 アクション中2)		
DeleteBucketPolicy	BucketName | string like | dms-*	なし
PutBucketPolicy	BucketName | string like | dms-*	なし

アクセスアドバイザー

IAM エンティティ (ユーザー、グループ、ロール) が、最後に AWS サービスにアクセスした日付と時刻を表示する機能

IAMの**最小限の権限**に関する設定に利用

- IAM ポリシー内で未使用または最近使用されていないアクセス許可を識別
- 未使用のサービスに関するアクセス許可を削除したり、類似の使用パターンを持つユーザーをグループに再編成
- アカウントのセキュリティを改善



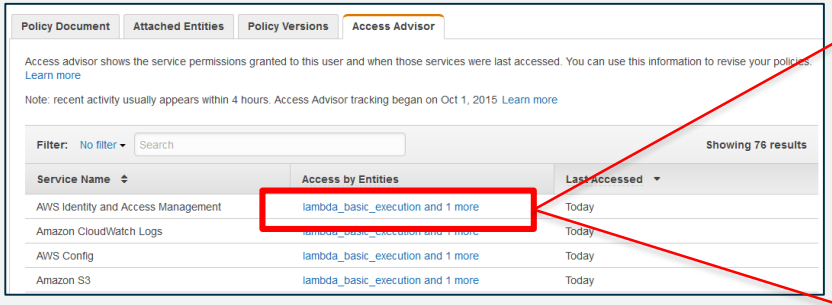
データ追跡されるリージョン（2019/1/30現在）
米国東部 (オハイオ)、米国東部（バージニア北部、米国西部 (北カリフォルニア)、米国西部 (オレゴン、アジアパシフィック (東京)、アジアパシフィック (ソウル)、アジアパシフィック (シンガポール)　、アジアパシフィック (シドニー)、アジアパシフィック (ムンバイ)　、カナダ (中部)、欧州 (フランクフルト、欧州 (アイルランド)、欧州 (ロンドン)　、EU (パリ、南米 (サンパウロ)

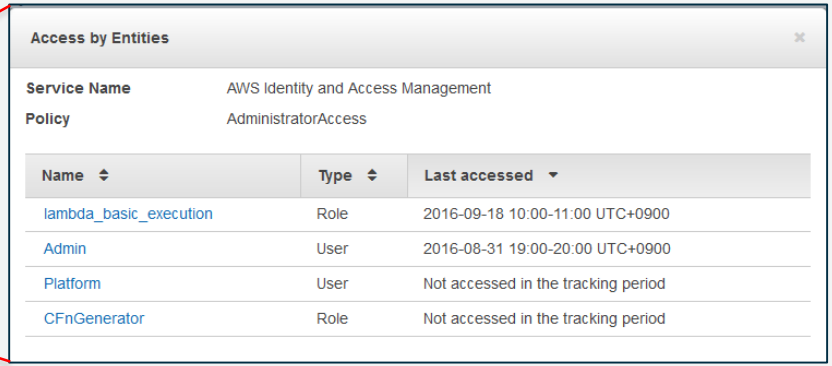
Service Last Accessed Dataの利用例

- ユーザーや、グループ、ロールに与えられた権限で利用されていないものを発見

サービス名	ポリシーのアクセス権限	最終アクセス時間
AWS Identity and Access Management	AdministratorAccess	4 日前
Amazon S3	AdministratorAccess	61 日前
AWS CloudFormation	AdministratorAccess	61 日前
AWS Lambda	AdministratorAccess	61 日前
Amazon Cognito Identity	AdministratorAccess	61 日前
Alexa for Business	AdministratorAccess	追跡期間中のアクセスはありません
AWS Certificate Manager	AdministratorAccess	追跡期間中のアクセスはありません

- IAMポリシーの利用状況と利用しているエンティティの識別





IAMポリシーを利用しているのが誰で最後にアクセスしたのがいつか容易に識別可能

✓ アクセスレベルを使用して、IAM権限を確認する

Use Access Levels to Review IAM Permissions

AWS アカウントのセキュリティを向上させるに、**IAM ポリシーを定期的に確認**し、モニタリングしてください。

- 「アクセスアドバイザー」を活用し、ポリシーにおいて、必要なアクションにのみ、必要な最小限の権限が付与されていることを確認します。
- 「ポリシー」の「ポリシーの使用状況」を確認し、適用されているユーザやグループ、ロールを確認してください。
- 「アクセス権限」で、最小権限かを確認。

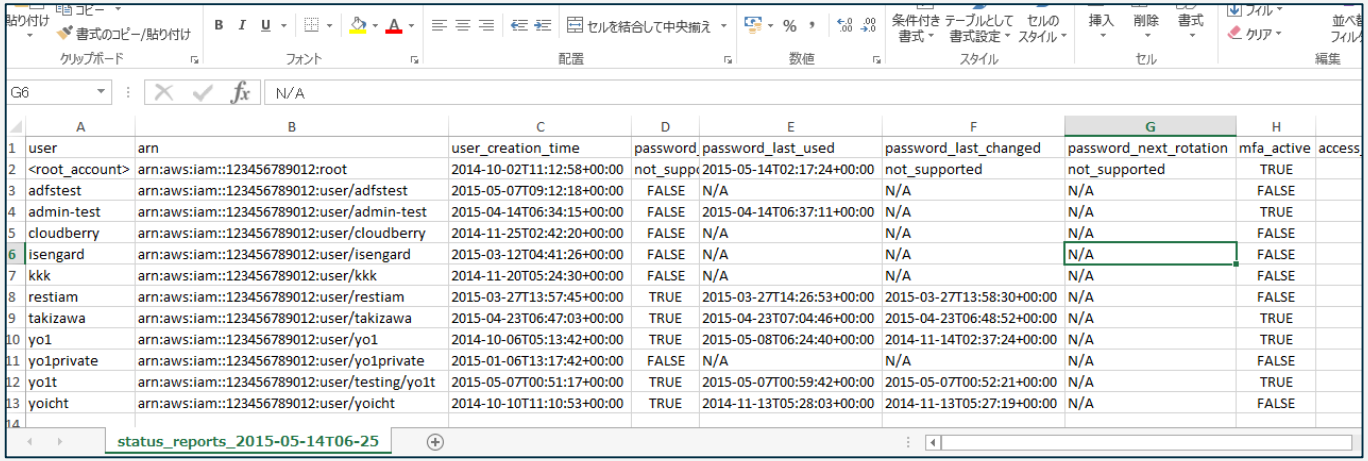
IDと権限のライフサイクル管理

- ✓ AWSアカウントのアクティビティの監視
- ✓ アクセスレベルを使用して、IAM権限を確認する
- ✓不要な認証情報を削除する
- ✓ 認証情報を定期的にローテーションする

IAM認証情報レポート (Credential Report)

- ユーザーの作成日時
- 最後にパスワードが使われた日時
- 最後にパスワードが変更された日時
- MFAを利用しているか
- Access KeyがActiveか
- Access Keyのローテートした日時
- Access Keyを最後に使用した日時
- Access Keyを最後に利用したAWSサービス
- 証明書はActiveか
- 証明書のローテートした日時

認証情報レポートは、4 時間ごとに 1 回生成できます。



	A	B	C	D	E	F	G	H	
1	user	arn	user_creation_time	password	password_last_used	password_last_changed	password_next_rotation	mfa_active	access
2	<root_account>	arn:aws:iam::123456789012:root	2014-10-02T11:12:58+00:00	not_supp	2015-05-14T02:17:24+00:00	not_supported	not_supported	TRUE	
3	adfstest	arn:aws:iam::123456789012:user/adfstest	2015-05-07T09:12:18+00:00	FALSE	N/A	N/A	N/A	FALSE	
4	admin-test	arn:aws:iam::123456789012:user/admin-test	2015-04-14T06:34:15+00:00	FALSE	2015-04-14T06:37:11+00:00	N/A	N/A	TRUE	
5	cloudberry	arn:aws:iam::123456789012:user/cloudberry	2014-11-25T02:42:20+00:00	FALSE	N/A	N/A	N/A	FALSE	
6	isengard	arn:aws:iam::123456789012:user/isengard	2015-03-12T04:41:26+00:00	FALSE	N/A	N/A	N/A	FALSE	
7	kkk	arn:aws:iam::123456789012:user/kkk	2014-11-20T05:24:30+00:00	FALSE	N/A	N/A	N/A	FALSE	
8	restiam	arn:aws:iam::123456789012:user/restiam	2015-03-27T13:57:45+00:00	TRUE	2015-03-27T14:26:53+00:00	2015-03-27T13:58:30+00:00	N/A	FALSE	
9	takizawa	arn:aws:iam::123456789012:user/takizawa	2015-04-23T06:47:03+00:00	TRUE	2015-04-23T07:04:46+00:00	2015-04-23T06:48:52+00:00	N/A	TRUE	
10	yo1	arn:aws:iam::123456789012:user/yo1	2014-10-06T05:13:42+00:00	TRUE	2015-05-08T06:24:40+00:00	2014-11-14T02:37:24+00:00	N/A	TRUE	
11	yo1private	arn:aws:iam::123456789012:user/yo1private	2015-01-06T13:17:42+00:00	FALSE	N/A	N/A	N/A	FALSE	
12	yo1t	arn:aws:iam::123456789012:user/testing/yo1t	2015-05-07T00:51:17+00:00	TRUE	2015-05-07T00:59:42+00:00	2015-05-07T00:52:21+00:00	N/A	TRUE	
13	yoicht	arn:aws:iam::123456789012:user/yoicht	2014-10-10T11:10:53+00:00	TRUE	2014-11-13T05:28:03+00:00	2014-11-13T05:27:19+00:00	N/A	FALSE	
14									

✓ 不要な認証情報を削除する

Remove Unnecessary Credentials

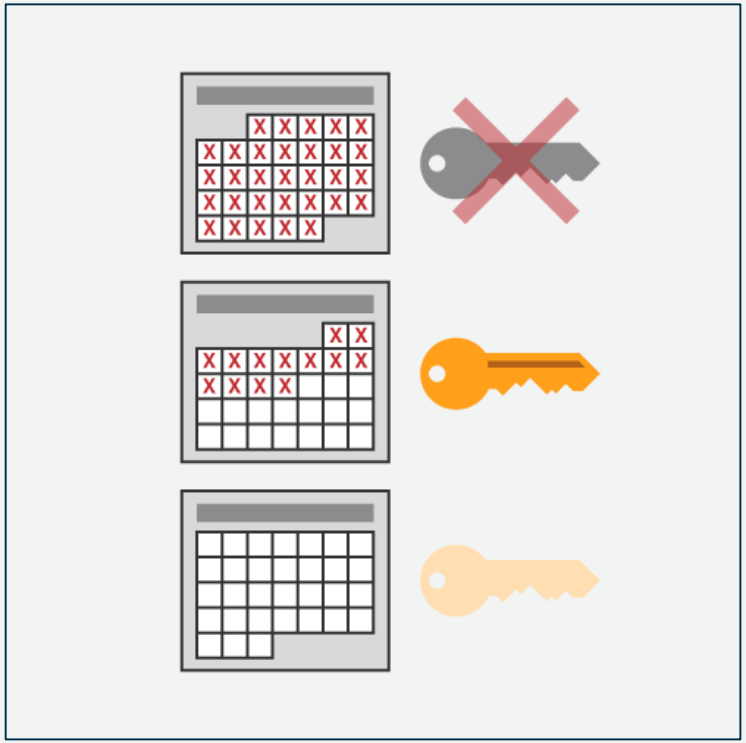
- パスワードやアクセスキーのローテーションなど、認証情報ライフサイクルの要件の結果を監査する。
    - コンソールを使用しないIAM ユーザにはパスワードを設定しない
    - 最近使用していないパスワード、アクセスキーは削除の対象。
- 社員の入社、退職、部署の異動や役割の変更など、人員のライフサイクルと連動させる。

- 認証情報レポートは、カンマ区切り値（CSV）ファイルとしてダウンロード可能。AWSマネジメントコンソールや AWS CLI, AWS APIで取得可能。
    - 生成するAWS CLI: aws iam generate-credential-report
    - 取得するAWS CLI: aws iam get-credential-report

IDと権限のライフサイクル管理

- ✓ AWSアカウントのアクティビティの監視
- ✓ アクセスレベルを使用して、IAM権限を確認する
- ✓ 不要な認証情報を削除する
- ✓認証情報を定期的にローテーションする

認証情報の定期的なローテーション



- IAMユーザーのパスワードやAccess Key/Secret Access Keyは定期的にローテーションすることを推奨

- 認証情報の利用状況はIAMのCredential Report機能で確認可能
  - ユーザーの作成日時
  - 最後にパスワードが使われた日時
  - 最後にパスワードが変更された日時
  - MFAを利用しているか
  - Access KeyがActiveか
  - Access Keyのローテートした日時
  - Access Keyを最後に使用した日時
  - Access Keyを最後に利用したAWSサービス
  - 証明書はActiveか
  - 証明書のローテートした日時

✓ 認証情報を定期的にローテーションする

Rotate Credentials Regularly

- IAMユーザーのパスワードローテーション
  - IAMのパスワードポリシーでユーザーがパスワードを変更できるように設定
  - パスワードに有効期限を設けることで利用者が自分で定期的にパスワードをローテーションできるようにする

- アクセスキーのローテーション
  - IAMユーザーの「認証情報」の「アクセスキー」から「アクセスキーの管理」を選択
  - 「アクセスキーの作成」で新しい認証情報の作成（２つまで）
  - 新しい認証情報でテストを行い、古いAccess KeyはInactiveにする
  - 万が一問題が起きた時は再びActivateすることが可能

IDと権限のライフサイクル管理に関するベストプラクティス

- ✓ AWSアカウントのアクティビティの監視
- ✓ アクセスレベルを使用して、IAM権限を確認する
- ✓ 不要な認証情報を削除する
- ✓ 認証情報を定期的にローテーションする

IAM Tips

Tips1: IAM基本の設定

組織と社員の権限に合わせて、IAMの設定を行う。

初期設定

- AllUsersというグループを作って、全ユーザを含める
- Adminグループを作り、管理者ユーザのみを含める。
- Developers, Managers, SysAdminsなどのグループを作り、適切なユーザを含める。

Amazon EC2

- AllUsersに、送信元のIPを許可したものだけにする。
- SysAdminsに、全てのAmazon EC2アクションを使用できるように権限を設定する。
- Developersには、DescribeInstances, RunInstances, StopInstances, TerminateInstances権限のみ。
- Managersには、Amazon EC2 の「Describe」 のみ許可

Amazon S3

- Example_bucketを作成
- キープレフィックスで、home/以下に、そのユーザのみの権限を付与。
- Share配下には、各々、開発者、管理者のみに許可

```
/example_bucket
     /home
          /zhang
          /mary
     /share
          /developers
          /managers
```

定期的に見直す

Tips2: IAMコンソールでIAMエンティティを探したり、アクションを素早く行う

さまざまな IAM リソースを管理する際に、必要な項目を探すため、アクセスキーが見つけたり、深くネストされた IAM リソースをを効率的に発見。

- アカウントに関連するアクセスキー、IAM エンティティ (ユーザー、グループ、ロール、ID プロバイダー)、ポリシーなどを名前で見つけることが可能。

主な使用方法：

- ユーザ名やグループ名、ロール名、ポリシー名を検索
- 「追加」と入力すると、関連するアクションが表示
- 「作成」、「削除」、「管理」、「編集」、「アタッチ」、「デタッチ」、「何ですか」などが利用可能

Tips3: パスワードを紛失した場合について

パスワードやアクセスキーを紛失または忘れた場合、IAM からそれらを取得することはできません。代わりに、次の方法を使用してリセットできます。

忘れたもの	方法
AWS アカウントのルートユーザー パスワード	ルートユーザーパスワードを忘れた場合は、AWS マネジメントコンソール からパスワードをリセットできます。
AWS アカウントのアクセスキー (使わないことを推奨)	既存のアクセスキーを無効にすることなく、新しいアクセスキーを作成できます。既存のキーを使用していない場合は、それらを削除できます。
IAM ユーザーパスワード	パスワードのリセットをその組織内の管理者に依頼する必要があります。
IAM ユーザーアクセスキー	新しいアクセスキーが必要です。独自のアクセスキーを作成するアクセス許可がある場合は、新しいアクセスキーを作成。必要なアクセス許可を持っていない場合は、新しいアクセスキーの作成を管理者に依頼する必要があります。まだ古いキーを使用している場合は、古いキーを削除しないように管理者に依頼します。

Tips4: MFAの管理

- IAM ユーザーの仮想およびハードウェア MFA デバイスがシステムと同期されていない場合、それらのデバイスを再同期できます。
    - IAM ユーザーは、デバイスを無効にするために管理者に連絡する必要があります。

•AWS アカウントのルートユーザーのMFAを紛失、損傷、動作しない場合、認証の代替方法を使用してサインインすることができます。

- 登録されている E メールと電話を使用してアイデンティティを確認してサインインすることができます。
- https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_mfa_lost-or-broken.html

- U2F セキュリティキーは同期しなくなることはありません。
    - U2F セキュリティキーを紛失または破損した場合は、U2F セキュリティキーを非アクティブにすることができます。

Tips5: IAMポリシーのトラブルシューティング

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/troubleshoot_policies.html

トラブルシューティングに関するトピック：

- ビジュアルエディタを使用したトラブルシューティング
- ポリシーの概要が使用したトラブルシューティング
- ポリシー管理のトラブルシューティング
- JSONポリシードキュメントのトラブルシューティング

Tips6: IAMロールのトラブルシューティング

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/troubleshoot_roles.html

- ロール名は大文字、小文字が区別される
- 引き受けるロールでは、sts:AssumeRole を 呼び出すアクセス許可が付与されていることを確認
- IAM アイデンティティが、IAM ポリシーで義務付けられている任意のタグでタグ付けされていることを確認
- Iam:PassRoleの権限がない場合は、管理者に依頼。
- AWS STS AssumeRole* API または assume-role* CLI オペレーションを使用してロールを引き受ける場合は、DurationSeconds パラメータの値を指定できます。900 秒 (15 分) からロールの [**最大 CLI/API セッション期間**] 設定までの値を指定できます。

  この設定の最大値は 12 時間です。管理者が最大のセッション期間を 6 時間に設定した場合、オペレーションは失敗する。

Tips7: IAMアクセスアドバイザーAPIを利用した AWS IAMアクセス権限分析の自動化の検討

2018/12/7に、IAMアクセスアドバイザーは、マネジメントコンソールだけでなく、AWS CLIやAPIを利用可能になりました。最小権限付与の有効な方法の一つ。

AWS CLI v1.16.89以降

1) generate-service-last-accessed-detailsを使用しJob-IDを取得

```
aws iam generate-service-last-accessed-details --arn arn:aws:iam::123456789012:user/amplify-user
```

```
{
  "JobId": "aeb4479d-ec11-077a-xx-xxx"
}
```

IAMアクセスアドバイザーに必要な権限

iam:GenerateServiceLastAccessedDetails
iam:GetServiceLastAccessedDetails
iam:GetServiceLastAccessedDetailsWithEntities
iam:ListPoliciesGrantingServiceAccess

2) get-service-last-accessed-detailsで確認

```
aws iam get-service-last-accessed-details --job-id "aeb4479d-ec11-077a-xx-xxx"
```

```
{
  "JobStatus": "COMPLETED",
  "JobCreationDate": "2019-01-27T12:14:50.402Z",
  "ServicesLastAccessed": [
    {
      "ServiceName": "Alexa for Business",
      "ServiceNamespace": "a4b",
      "TotalAuthenticatedEntities": 0
    },
    {
      "ServiceName": "AWS CloudFormation",
      "LastAuthenticated": "2018-11-26T18:38:00Z",
      "ServiceNamespace": "cloudformation",
      "LastAuthenticatedEntity": "arn:aws:iam::123456789012:user/amplify-user",
      "TotalAuthenticatedEntities": 1
```

利用したサービス
利用した日時などがわかる

まとめ

AWS IAMのベストプラクティス

IDと認証情報の管理	✓ AWSアカウントのルートユーザーアクセスキーをロックする ✓ 個々のIAMユーザーを作成 ✓ ユーザーの強力なパスワードポリシーを設定 ✓ アクセスキーを共有しない ✓ 特権ユーザーに対してMFAを有効化する
アクセス権限の管理	✓ AWS管理ポリシーを使用したアクセス許可の使用開始 ✓ インラインポリシーではなくカスタマー管理ポリシーを使用する ✓ 追加セキュリティに対するポリシー条件を使用する ✓ 最小権限を付与する ✓ IAMユーザーへのアクセス許可を割り当てるためにグループを使用する
権限の委任	✓ Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する ✓ ロールを使用したアクセス許可の委任
IDと権限のライフサイクル管理	✓ AWSアカウントのアクティビティの監視 ✓ アクセスレベルを使用して、IAM権限を確認する ✓ 不要な認証情報を削除する ✓ 認証情報を定期的にローテーションする

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

まとめ

- AWS IAMはAWSサービスを利用するための認証と認可を提供する。
- 権限の委任においては、Amazon EC2インスタンスで実行するアプリケーションに対し、ロールを使用する。ロールを使用したアクセス許可の委任が可能。
- IDと権限のライフサイクル管理においては、AWSアカウントのアクティビティの監視し、IAM権限を確認し、不要な認証情報を削除、認証情報の定期的なローテーションを行う。

参考情報へのリンク

- AWS IAM 公式サイト
https://aws.amazon.com/jp/iam/

- AWS IAMドキュメント
https://docs.aws.amazon.com/iam/index.html

- AWS Security Blog
http://blogs.aws.amazon.com/security/

- IAMの制限 (IAMドキュメント)
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_iam-limits.html

- AWSアカウントの認証管理 (AWS Summit Tokyo 2018)
https://d1.awsstatic.com/events/jp/2018/summit/tokyo/aws/40.pdf

- AWSご利用開始時に最低限おさえておきたい10のこと (Blackbelt Online Semminer)
https://d1.awsstatic.com/webinars/jp/pdf/services/20180403_AWS-BlackBelt_aws10.pdf

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
資料公開と併せて、後日掲載します。

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