



このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[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~ Part1

Solutions Architect 保坂 匠
2019/1/29

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



過去資料
<https://amzn.to/JPArchive>



自己紹介

保坂 匠 (ほさか たくみ)

アマゾン ウェブ サービス ジャパン
ソリューション アーキテクト



普段の業務

金融機関のお客様のクラウドへのマイグレーション支援

好きなAWSサービス

AWS Identity and Access Management (IAM)

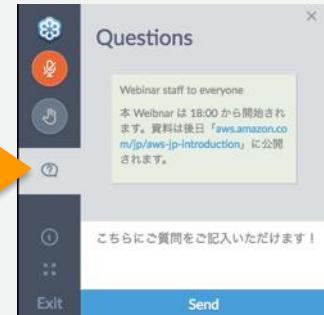
AWS Black Belt Online Seminar とは

「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、Amazon 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29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	<ul style="list-style-type: none">✓ AWSアカウントのルートユーザーの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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 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の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AWS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マネーフォワード管理ポリシーを使用する
- ✓ 追加セキュリティに対するAWS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、AWS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 (本日お話する範囲)

Part 2



本日 (Part1) のアジェンダ

- AWS IAMの概要
- IDと認証情報の管理
- アクセス権限の管理
- まとめ

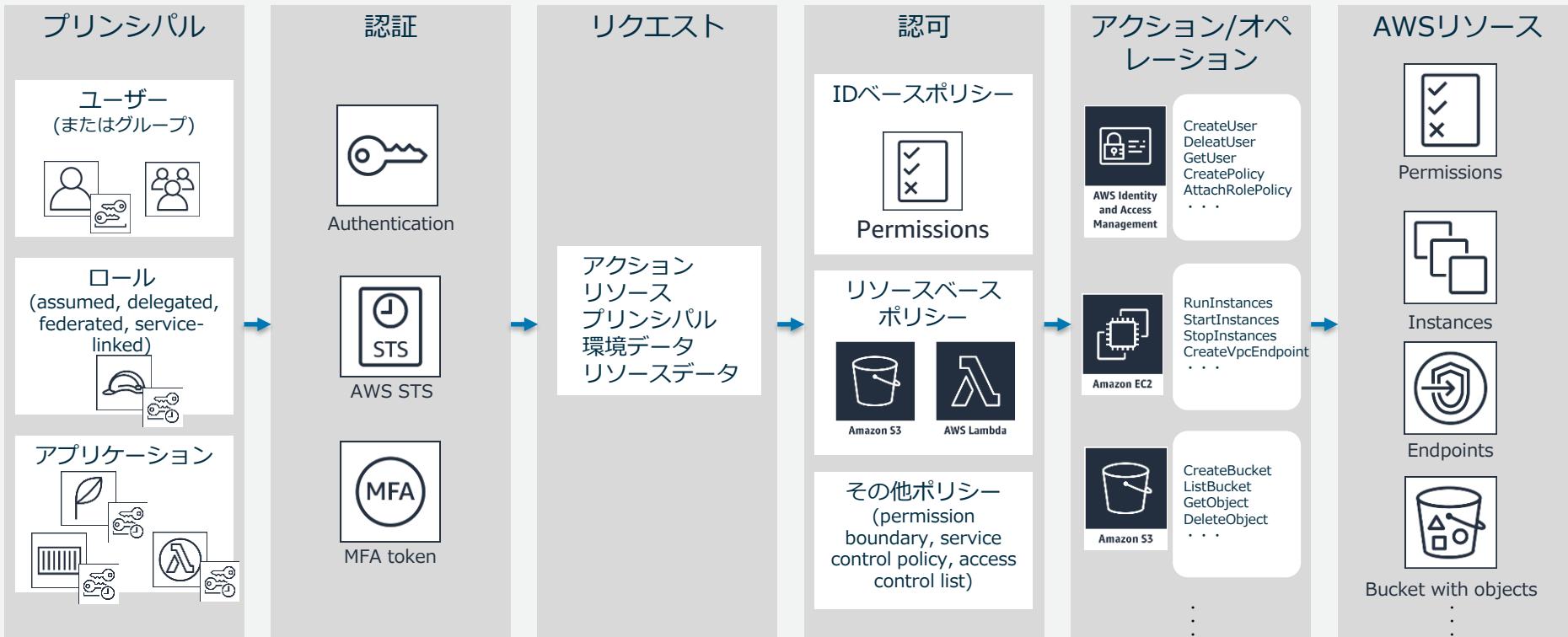
AWS IAMの概要

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



IDと認証情報の管理

- ✓ AWSアカウントのルートユーザーの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

AWSアカウントのルートユーザー

- ・ そのアカウントの全てのAWSサービスとAWSリソース全てに完全なアクセス権を持つユーザー
- ・ AWSマネジメントコンソールへはAWSアカウントを作成したときのメールアドレス/パスワードでサインイン
- ・ IAMで設定するアクセスポリシーではアクセス許可を制限できない
 - ・ AWS Organizationsのサービスコントロールポリシー(SCP)によってサービスを制限可能
- ・ **極力ルートユーザーを使用しないでください！**
 - ・ とはいえるルートユーザーでの認証が必要なタスクもある

ルートユーザーの認証が必要なAWSタスクの例

- ルートユーザーのメールアドレスやパスワードの変更
- IAMユーザーによる課金情報へのアクセスのActivate/Deactivate
- 支払オプションの変更
- AWSサポートプランの変更
- IAMユーザーへのアクセス許可のリストア
- 無効な制約を設定したAmazon S3 バケットポリシーの修正
- 脆弱性診断フォームの提出
- 逆引きDNS申請
- CloudFrontキーペアの作成
- AWSアカウントの解約

(2019年1月29日時点)

アクセスキー

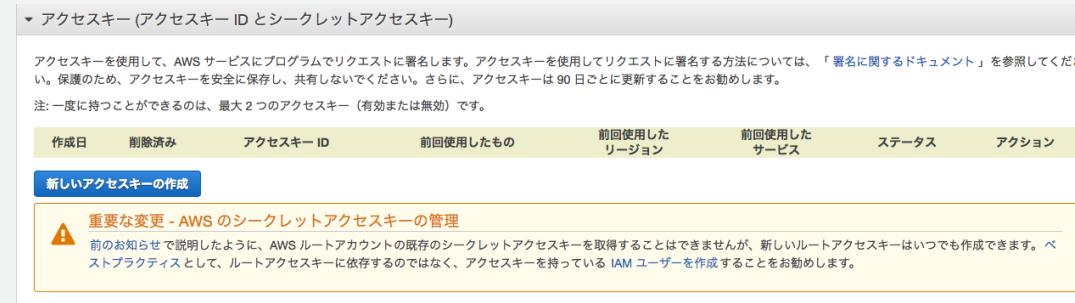


- AWSアカウントのルートユーザーまたはIAMユーザーの長期的な認証情報
 - 手動で取り消すまで有効
- アクセスキーを用いてAWS CLIやAWS SDK等からリクエストに署名
- アクセスキーID/シークレットアクセスキーで構成される
- 安全なローテーションのために、最大2つのアクセスキーを持つことができる

✓ 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

Lock Away Your AWS Account Root User Access Keys

- ルートユーザーのアクセスキーは削除してください！
- すでに持っている場合は削除してください！
 - ルートユーザーでサインインし、セキュリティ認証情報のページからアクセスキーを削除
- ルートユーザーの認証情報を他者に開示したり、プログラムに埋め込んだりしないでください！



IDと認証情報の管理

- ✓ AWSアカウントのルートユーザーの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

IAMユーザー



- AWSで作成するエンティティ (ユーザーまたはアプリケーション)
- 名前と認証情報で構成される
- IAMユーザーを識別する方法
 - ユーザーの「フレンドリ名」：ユーザー作成時に指定
“Alice”と“alice”は同一のユーザーと見なされ、作成しようとするとエラー
 - ユーザーのARN (Amazon Resource Name)：リソースポリシーのPrincipal要素で指定
例：arn:aws:iam::0123456789012:user/*Alice*
 - ユーザーの一意の識別子：フレンドリ名を再利用したいとき等に権限のエスカレーションを避けることができる
例：AIDAJQABLZS4A3QDU576Q
- 認証情報
 - コンソールパスワード
 - アクセスキー

✓ 個々のIAMユーザーの作成

Create Individual IAM Users

- ・ 個別のIAMユーザーを作成してください。
- ・ 必要な場合を除き、AWSアカウントのルートユーザー認証情報を使用してAWSにアクセスしないでください！
- ・ 個別のIAMユーザーを作成するメリット
 - ・ 認証情報を個別に変更(ローテーション)できる
 - ・ アクセス許可をいつでも変更、無効化できる
 - ・ Amazon CloudTrailログからアクションを追跡できる

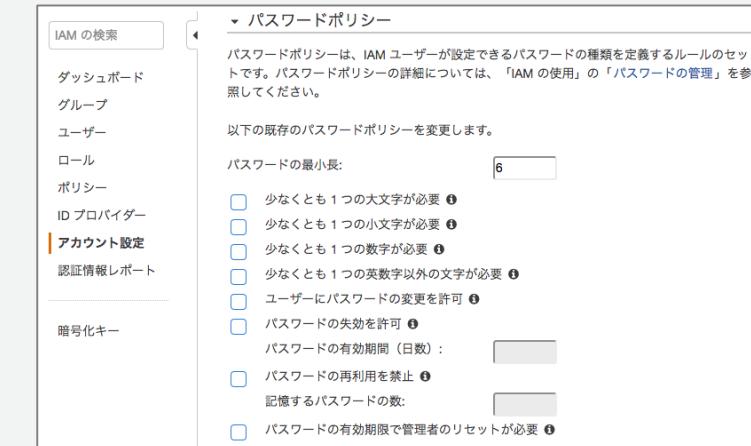
IDと認証情報の管理

- ✓ AWSアカウントのルートユーザーの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

✓ ユーザーの強力なパスワードポリシーを設定

Configure a Strong Password Policy for Your Users

- ・ 強力なパスワードポリシーを設定してください！
- ・ パスワードに要求される強度とパスワード管理のポリシーを設定可能
 - ✓ 最小文字数
 - ✓ 少なくとも1つの英大文字
 - ✓ 少なくとも1つの英小文字
 - ✓ 少なくとも1つの数字
 - ✓ 少なくとも1つの特殊文字
 - ✓ ユーザー自身によるパスワード変更の許可
 - ✓ パスワードの有効期限
 - ✓ パスワード再利用禁止の世代数
 - ✓ 管理者による期限切れパスワードのリセット
- ・ AWSアカウントのルートユーザーのパスワードポリシーには適用されない



IDと認証情報の管理

- ✓ AWSアカウントのルートユーザーの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

✓ アクセスキーを共有しない

Do Not Share Access Keys

- 複数の人がAWSリソースへのアクセス権を共有したい場合でも、アクセスキーを共有しないでください！
- AWSへのアクセスを必要とするアプリケーションの場合は、IAM ロールを使用して一時的セキュリティ認証情報を取得する (Part2で解説)
- 情報の置き場に注意
 - GitHubリポジトリ
 - AMIの中への埋め込み
 - 設計書等のドキュメント内に記載
 - プレーンテキストでの保管
 - ハードコーディング(AWS認証情報ファイル/環境変数)

IDと認証情報の管理

- ✓ AWSアカウントのルートユーザーの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

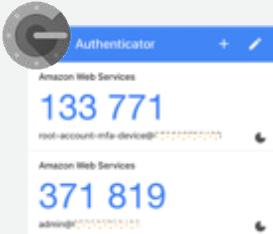
MFA (Multi-Factor Authentication:多要素認証)



- ・ パスワードやアクセスキーによる認証に追加して、セキュリティを強化する
しくみ
- ・ AWSがサポートするMFAメカニズム:
 - ・ 仮想MFAデバイス
 - ・ U2Fセキュリティキー
 - ・ ハードウェアMFAデバイス
- ・ ルートユーザー、IAMユーザーの各IDに個別のMFA設定が可能
- ・ MFA条件を指定したポリシーを関連付けできる対象:
 - ・ IAMユーザーまたはIAMグループ
 - ・ Amazon S3バケット、Amazon SQSキュー、Amazon SNSトピック等のリソース
 - ・ IAMロールの信頼ポリシー



AWSがサポートするMFAメカニズム



	ソフトウェア	New!	ハードウェア
製品	Google Authenticator, Authy 2-Factor Authentication	Yubikeyセキュリティキー	Gemalto
形式	スマホアプリ	USBスティック型	トークン型
コスト	無料	有料(4,500円程度)	有料(2,000円程度)
機能	単一のデバイスで複数のトークンをサポート	单一のセキュリティキーで複数のルートユーザー/IAMユーザーをサポート 手入力不要	不正開封防止用キーホルダー型デバイスで内蔵電池により単体でOTPを発行

✓ 特権ユーザーに対してMFAを有効化する

Enable MFA for Privileged Users

- AWSアカウントのルートユーザーや強い権限を持つIAMユーザーにはMFAを有効化し、通常利用しないようにしてください！
 - MFAデバイスも厳重に管理してください！
- 認証プロセスを完了するには、ユーザーの認証情報とデバイス生成のレスポンスが必要になるため、アイデンティティの保護に役立つ
- MFAデバイスの紛失/盗難/不具合が発生したら、代替の認証要素を使って認証し、新しいMFAデバイスを有効化し、パスワードも変更する

ここまでまとめ：IDと認証情報の管理に関するベストプラクティス

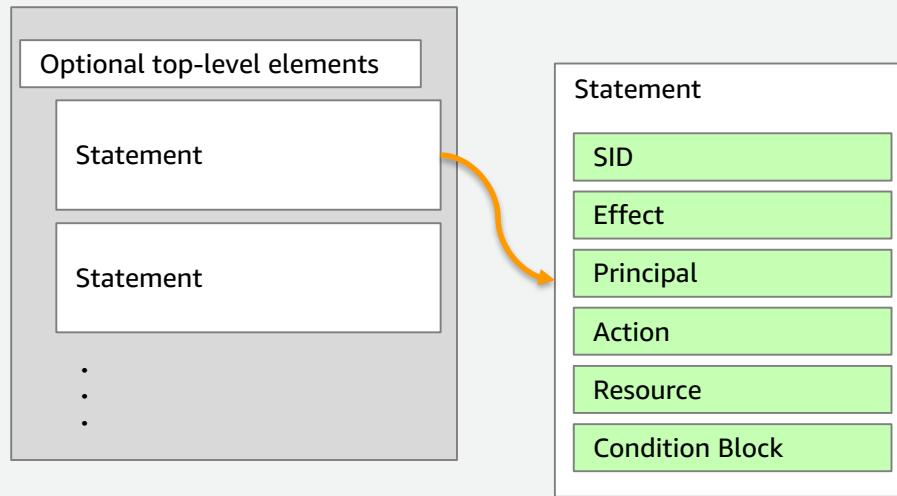
- ✓ AWSアカウントのルートユーザーのアクセスキーをロックする
- ✓ 個々のIAMユーザーを作成
- ✓ ユーザーの強力なパスワードポリシーを設定
- ✓ アクセスキーを共有しない
- ✓ 特権ユーザーに対してMFAを有効化する

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

ポリシー

- IAMアイデンティティやAWSリソースに関連づけることによってアクセス許可を定義することができるオブジェクト
- 通常、JSONポリシードキュメントでアクセス条件を記述
- ポリシードキュメントは1つ以上のStatementブロックで構成



AWSがサポートするポリシータイプ

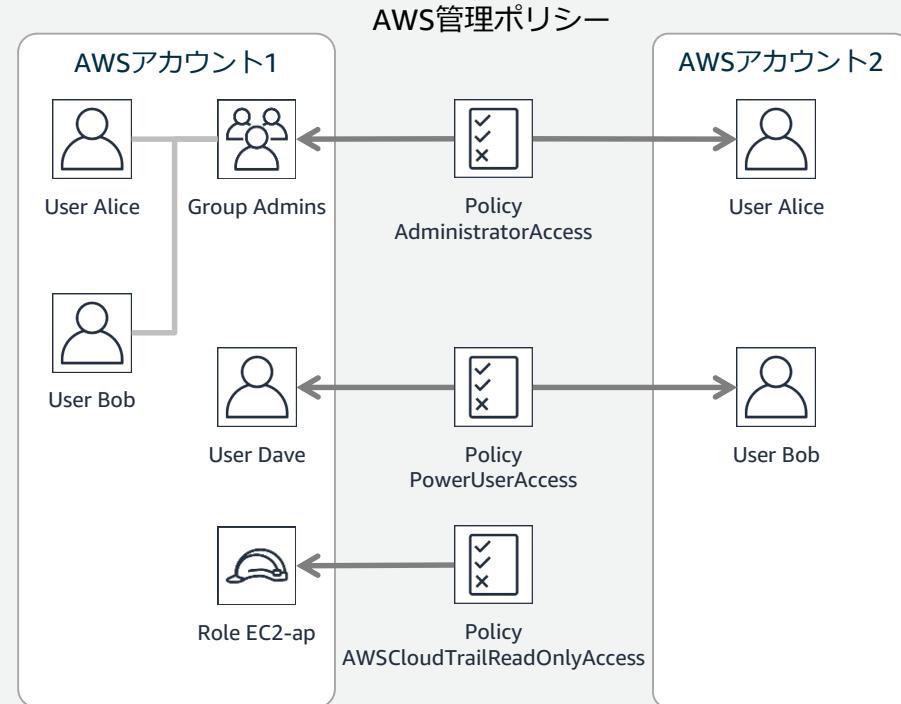
- アイデンティティベースのポリシー
 - 管理ポリシー
 - AWS管理ポリシー
 - カスタマー管理ポリシー
 - インラインポリシー
- リソースベースのポリシー
 - AWS IAMロールの信頼ポリシー、Amazon S3のバケットポリシー、Amazon SNSトピックのアクセス許可、Amazon SQSキューのアクセス許可
- パーミッションバウンダリー
 - AWS IAMアクセス許可の境界、AWS Organizationsサービスコントロールポリシー (SCP)
- アクセスコントロールポリシー (ACL)
 - Amazon S3のバケットのACL、Amazon VPCのサブネットのACL
- セッションポリシー

アイデンティティベースのポリシー

- 管理ポリシー
 - 複数のIAMユーザー、IAMグループ、IAMロールに関連付け可能 (最大10個)
 - 再利用可能
 - 一元化された変更管理
 - バージョニングとロールバック
 - 種類
 - AWS管理ポリシー
 - カスタム管理ポリシー
- インラインポリシー
 - 単一のIAMユーザー、IAMグループ、IAMロールに直接埋め込む

AWS管理ポリシー

- AWSにより事前定義された管理ポリシー
- AWSが作成および管理され、編集不可
- すべてのAWSアカウントで利用可能
 - AWSによる管理
例：AmazonEC2FullAccess
AmazonS3ReadOnlyAccess
 - ジョブ機能
例：AdministratorAccess
SecurityAudit
DataScientist
- AWSにより更新される



✓ AWS管理ポリシーを使用したアクセス許可の使用開始

Get Started Using Permissions With AWS Managed Policies

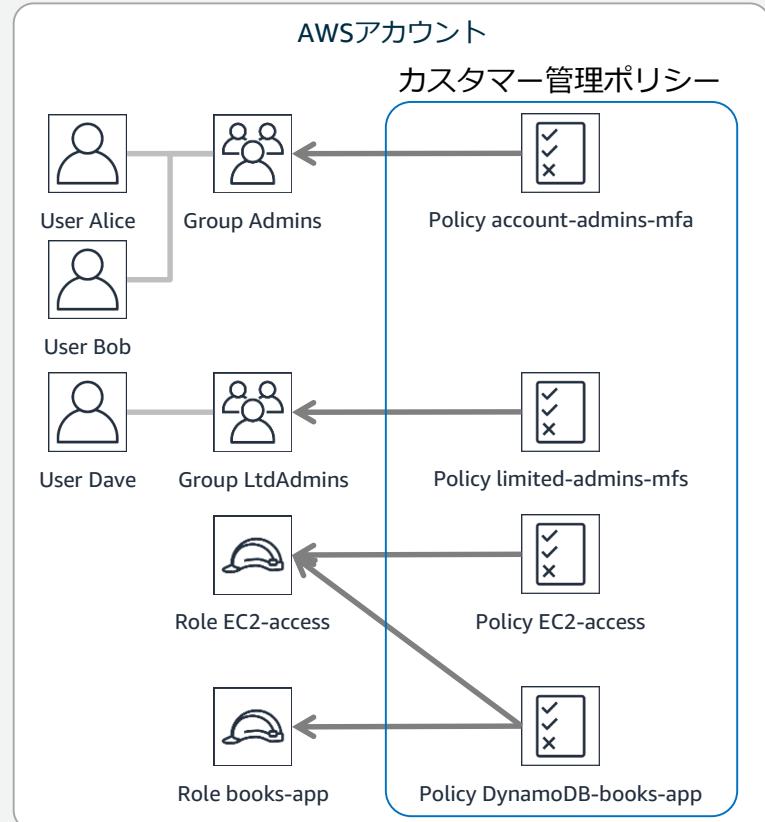
- AWS管理ポリシーを用いると多くのユースケースすぐにポリシーの適用を開始できる
- 適切なアクセス権限を付与するにはIAMポリシーの詳細な知識が必要
- まずはポリシードキュメントの扱いに慣れる

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

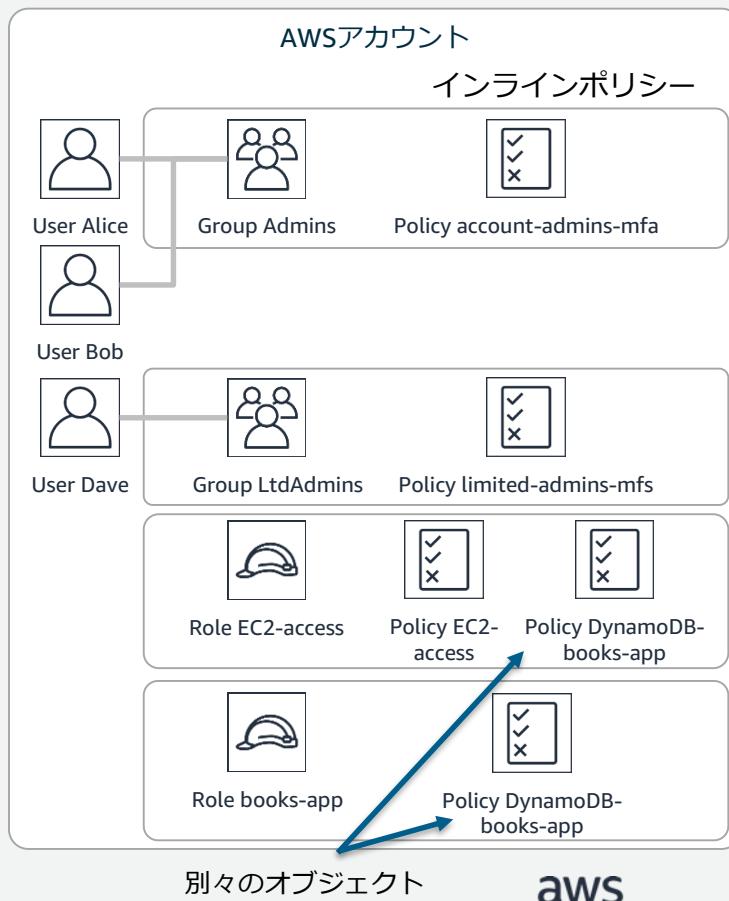
カスタマー管理ポリシー

- AWSアカウントで管理することができるカスタムポリシー
- AWS管理ポリシーでは要件を満たせない場合等にカスタマー管理ポリシーを適用



インラインポリシー

- 1つのIAMエンティティ (IAMユーザー、 IAMグループ、 IAMロール)に直接埋め込まれるポリシー
- IAMエンティティに紐づいた固有のオブジェクト
例えば、右図のEC2-accessロールとbooks-appロールのインラインポリシーDynamoDB-books-appは別物のポリシーオブジェクト
- IAMエンティティを削除するとインラインポリシーも削除される
- IAMエンティティとポリシーとの厳密な1対1の関係を維持する必要がある場合等にインラインポリシーを適用



✓ 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 Use Customer Managed Policies Instead of Inline Policies

- カスタマー管理ポリシーはカスタマイズ可能で、再利用性も高く管理面で有利
- カスタマー管理ポリシーの利点は全ての管理ポリシーを1ヶ所で確認できること
- インラインポリシーの利用はできるだけ避けてください。
- インラインポリシーはカスタマー管理ポリシーに変換することが可能

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

ポリシーの主要な要素

要素	概要
Version	ポリシー言語のバージョン。"2012-10-17"が現行バージョン。Version要素を含めないとポリシー変数(\${aws:username}等)は文字列として扱われる。
Statement	アクセス許可に関する複数要素 (Effect/Action/Resource等) を含むステートメントブロック。複数のステートメントブロックを並べることができる。
Effect	"Allow"または"Deny"。ステートメントの結果を許可または明示的な拒否にするか指定する。
Principal	リソースベースのポリシー (バケットポリシーや信頼ポリシー等) に記述する。リソースへのアクセスを許可または拒否するIAMエンティティ (IAMユーザー、フェデレーテッドユーザー、IAMロール、AWSサービス等) をARN形式で指定する。
Action	Effect要素で許可または拒否する対象となる特定のアクションを記述する。大文字小文字の区別はされない。各AWSサービスを識別する名前空間 (iam, ec2, s3等) でサポートされるアクションが定義されている。
Resource	Action要素の対象となる特定のリソースをARN形式で記述する。指定したAction (ec2:DescribeInstances等) によっては個々のリソースを指定することができず、"* (ワイルドカード)"を指定する必要がある。
Condition	ポリシーを実行する条件を指定することができる。Condition要素は条件演算子、ポリシー変数、条件値から構成される。

Principal要素

- AWSリソースへのアクセスが許可/拒否されるIAMエンティティを指定する
- リソースベースポリシーで使用
- AWSアカウント、IAMユーザー、IAMロール、フェデレーティッドユーザー、引き受けたロールユーザー(assumed-role user)をARN形式で記述
 - "Principal" : { "AWS" : "arn:aws:iam::123456789012:/root"}
 - "Principal" : { "AWS" : "arn:aws:iam::123456789012:/user/Alice"}
 - "Principal" : { "AWS" : "arn:aws:iam::112233445566:/role/s3ReadOnlyRole"}
 - "Principal": { "AWS" : "arn:aws:sts::222255558888:assumed-role/*role-name/role-session-name*" }
- 注：IAMグループの指定は不可、大文字小文字は区別される、ユーザーを指定する際に“すべてのユーザー”の意味でワイルドカード (*) を使用することはできない
- IAMロールの信頼ポリシーのPrinicpal要素に指定したIAMユーザーとIAMロールを削除すると信頼関係は壊れる。
 - 同じ名前でIAMエンティティを作成してもプリンシパルIDが異なるため、同じ名前で再作成した場合はロールの再編集が必要

Action要素

- 許可/拒否される特定のアクションを指定する
 - Statement要素にはAction/NotAction要素が必須
 - AWSサービスで行うことができるタスクを記述する独自のアクションセットを記述
 - 有効なアクション名はドキュメントを参照、またはポリシーエディターから選択
 - 形式：“Action”：“<各サービスの名前空間>:<アクション名>”
 - “Action”：“ec2:StartInstances”
 - “Action”：[“sns:SendEmail” , “sns:ReceiveMessage”]
 - “Action”：“iam:*AccessKey”
 - “Action”：“IAM:listaccesskeys”
- 注：複数のアクションを指定可能、ワイルドカード(*)を使用可能、値は大文字小文字の区別なし

Resource要素

- ステートメントで取り扱う一連のオブジェクトを指定する
 - Statement要素にはResource/NotResource要素が必須
 - AWSサービスが持つ一連のリソースセットをARN形式で記述
 - 有効なリソースはドキュメントを参照、またはポリシーエディターから選択
 - "Resource" : "arn:aws:sqs:us-east-2:**123456789012:queue1**"
 - "Resource" : "arn:aws:iam::**123456789012:user/accounting**/*"
 - "Resource" : ["arn:aws:dynamodb:us-east-2:**123456789012:table/books_table**", "arn:aws:dynamodb:us-east-2: **123456789012 :table/magazines_table**"]
 - "Resource" : "arn:aws:dynamodb:us-east-2:**123456789012:table/\${aws:username}**"
- 注：複数のリソースを指定可能、ワイルドカード(*)を使用可能、JSONポリシー変数を指定可能

Condition要素 (1/2)

- ポリシーが有効になるタイミングの条件を指定する
- Condition要素の記述はオプション
- 条件キー:条件値に対する評価方法として条件演算子を作用させる演算式を記述
 - 形式 : "Condition" : { <条件演算子> : { <条件キー> : <条件値> } }
 - 条件演算子
 - 条件比較のタイプ (文字列条件、数値条件、IPアドレス条件等)を指定する
 - 条件キーごとに使用できる条件演算子の種類が決まっている
 - 条件キー
 - AWSグローバル条件コンテキストキー ("aws:"で始まる)
 - 全てのサービスで使用可能なキー、一部のサービスでのみ使用可能なキーがある
 - AWSサービス固有のキー (そのサービス固有の名前 ("s3:"等) で始まる)
 - IAMの条件コンテキストキー

Condition要素 (1/2)

- "Condition" : { "StringEquals" : { "aws:username" : "johndoe" } }
 - "Condition" : { "StringEqualsIgnoreCase" : { "aws:username" : "johndoe" } }
 - "Condition" : { "IpAddress" : { "aws:SourceIP" : ["192.0.2.0/24" , "203.0.113.0/24"] } }
 - "Condition" : { "StringEquals" : { "ec2:ResourceTag/*tagkey*" : "*tagvalue*" } }
 - "Condition" : { "StringEquals" : { "s3:prefix": "projects" } }
 - "Condition" : { "StringEquals" : { "iam:PassedToService" : "cloudwatch.amazonaws.com" } }
 - "Condition" : { "ForAllValues:StringEquals": { "dynamodb:Attributes": ["*ID*", "*Message*", "*Tags*"] } }
- 注：条件キーは大文字小文字は区別しない、条件値の大文字小文字の区別は使用する条件演算子によって異なる
- 参考情報

条件演算子

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

グローバル条件キー

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_condition-keys.html

IAMの条件コンテキストキー

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies_iam-condition-keys.html

要素のAND条件とOR条件

```
"Condition" : {  
    "DateGreaterThan" : {  
        "aws:CurrentTime" : "2019-01-29T12:00:00Z"  
    },  
    "DateLessThan": {  
        "aws:CurrentTime" : "2019-01-29T15:00:00Z"  
    },  
    "IpAddress" : {  
        "aws:SourceIp" : ["192.168.176.0/24","192.168.143.0/24"]  
    }  
}
```

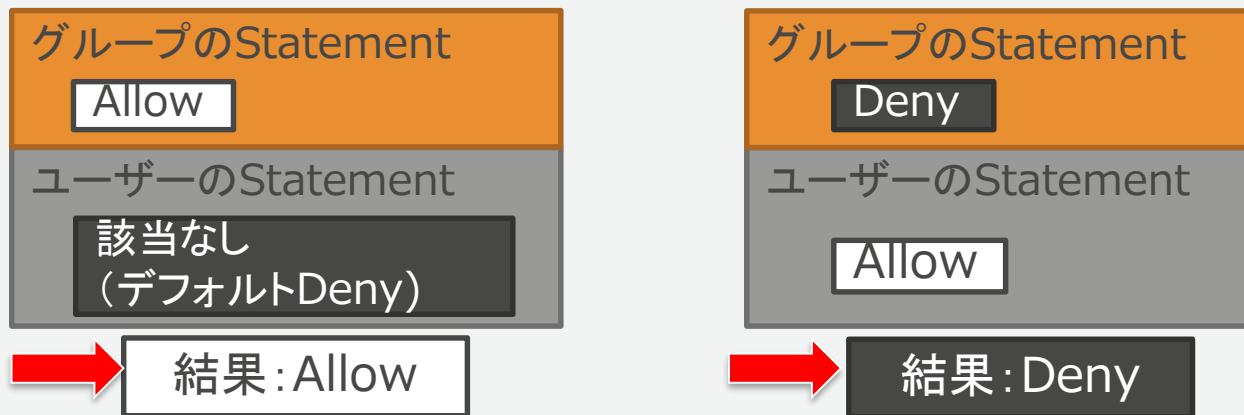
The diagram illustrates the logical structure of the AWS IAM policy condition block. It shows three main components: DateGreaterThan, DateLessThan, and IpAddress. Red double-headed arrows labeled 'AND' indicate that DateGreaterThan and DateLessThan are combined via an AND operation. A yellow double-headed arrow labeled 'OR' indicates that the entire Date range condition is combined via an OR operation with the IpAddress condition.

Condition下のブロックはAND条件、演算子に対する値はOR条件

この例の場合、"2019/1/29の12:00から15:00の間に、ソースIPアドレス192.168.176.0/24もしくは192.168.143.0/24のネットワークからアクセスしたリクエスト"を意味する

アクセス可否の決定ロジック

- 暗黙的なDeny (デフォルト) < 明示的なAllow < 明示的なDeny
- すべてのアクセスはデフォルトで拒否 (暗黙的なDeny)
- アクセス権限に“Allow”の条件があった場合、アクセス許可
- ただしアクセス権限に 1 つでも“Deny”の条件があった場合、アクセス拒否(明示的なDeny)



IAMポリシーの作成を支援するツール群

- ビジュアルエディター機能
 - 最初から新しいポリシー構築可能
- AWS Policy Generator : <http://awspolicygen.s3.amazonaws.com/policygen.html>
 - AWSのサービスについて、必要情報を入力するとポリシー文書を自動作成してくれるツール
- ポリシー言語の文法チェック機能
 - ポリシー保管時にポリシー言語の文法チェック、自動フォーマットを実施
 - 「Validate Policy」により明示的な確認が可能
- IAM Policy Validator
 - 自動的に既存の IAMポリシーを調べ、IAMポリシーの文法に準拠しているか確認
 - ポリシーに対する推奨の変更を提示
 - Policy Validator を使用できるのは、準拠していないポリシーがある場合のみ
- IAM Policy Simulator : <https://pollicysim.aws.amazon.com/home/index.jsp>
 - プロダクションへの実装前にポリシーをテスト可能
 - パーミッションのトラブルシューティング
 - Condition、ポリシー変数、リソースベースのポリシーを入れたテスト

✓ 追加セキュリティに対するポリシー条件を使用する

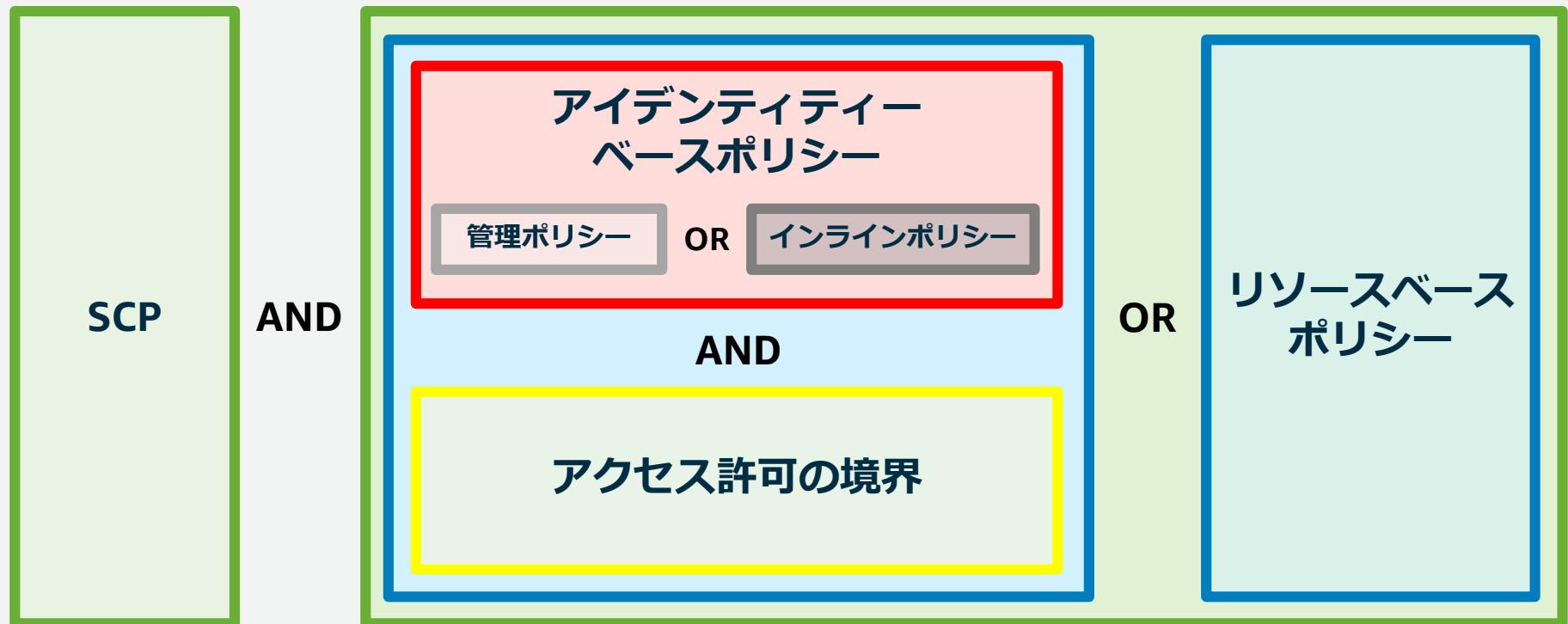
Use Policy Conditions for Extra Security

- より安全なポリシーの適用のために、Condition要素によってポリシーが有効になる条件をさらに絞り込む
 - リクエストを許容するソースIPアドレスの範囲
 - 日付または時間の範囲
 - MFAデバイスでの認証の要求
 - SSL使用の要求

アクセス権限の管理

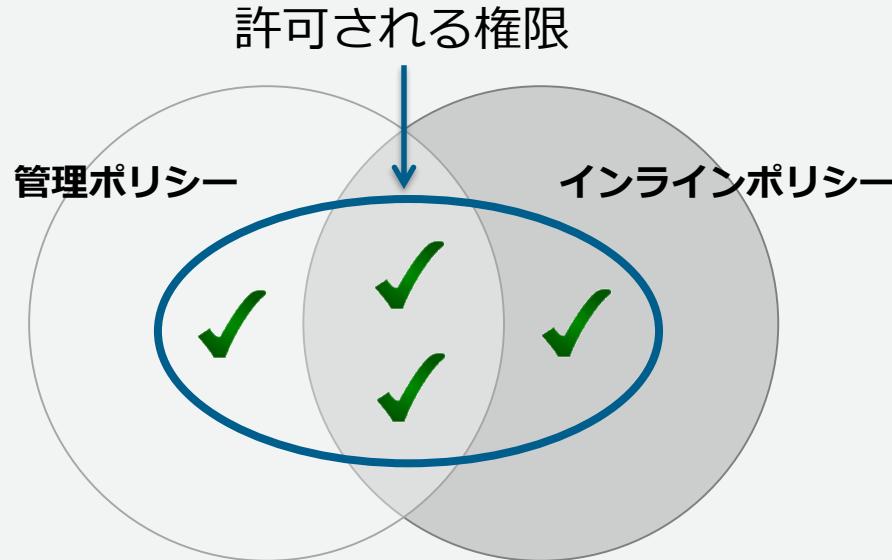
- ✓ AWS管理ポリシーを使用したアクセス許可の使用開始
- ✓ インラインポリシーではなくカスタマー管理ポリシーを使用する
- ✓ 追加セキュリティに対するポリシー条件を使用する
- ✓ **最小権限を付与する**
- ✓ IAMユーザーへのアクセス許可を割り当てるためにグループを使用する

アクセス権の決定ロジック (同一アカウントの場合)



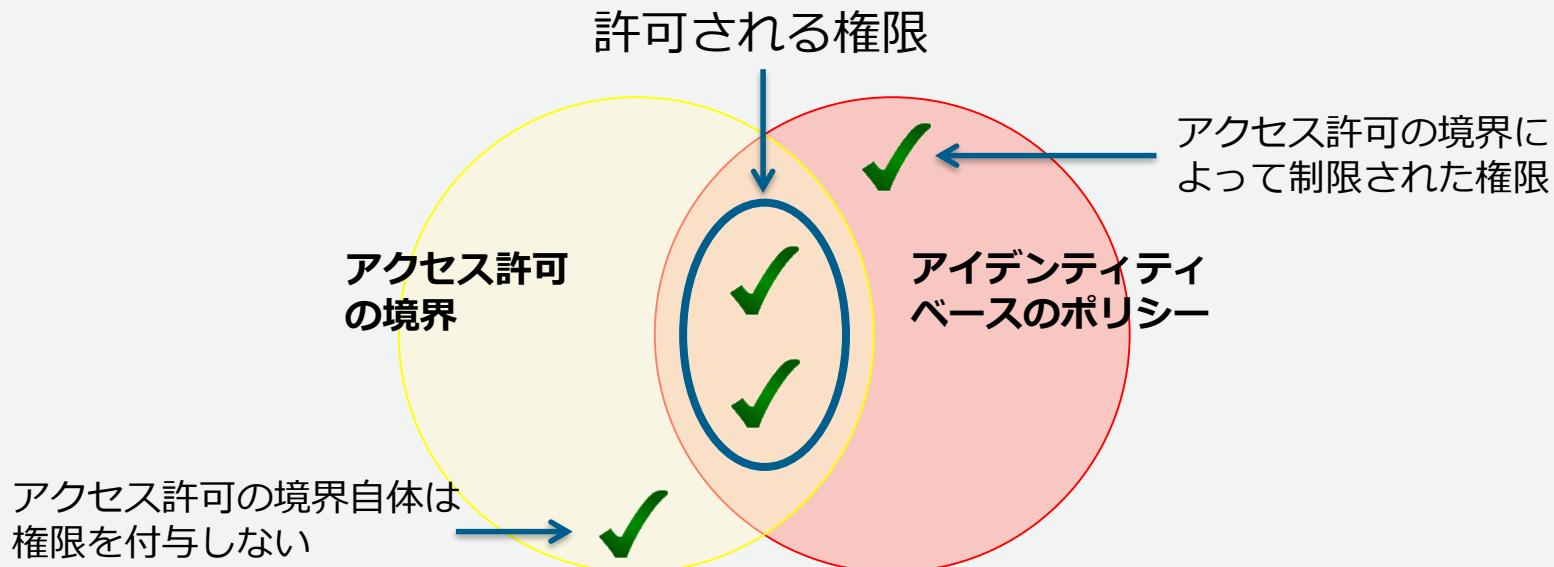
アイデンティティベースのポリシー

- 管理ポリシーとインラインポリシーのそれぞれで許可されているものが有効な権限となる (OR条件)



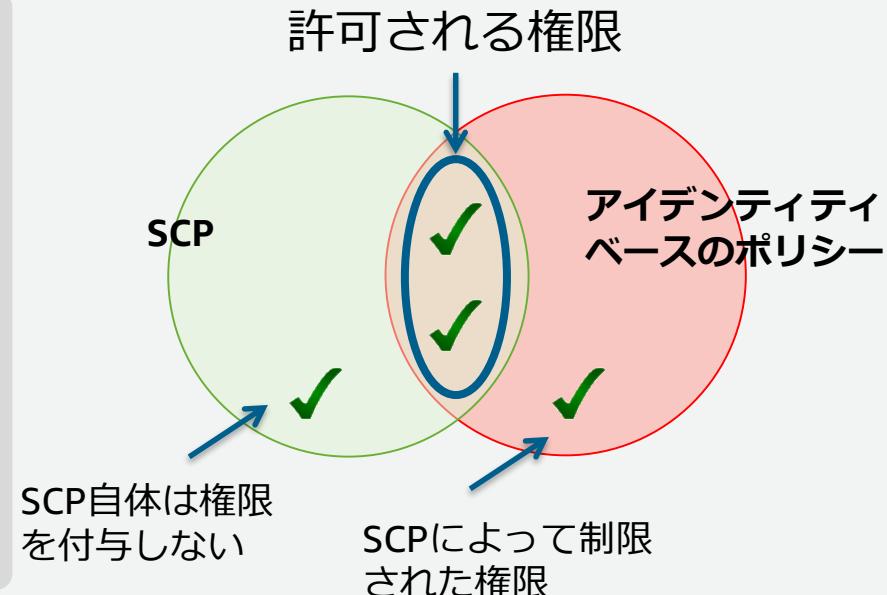
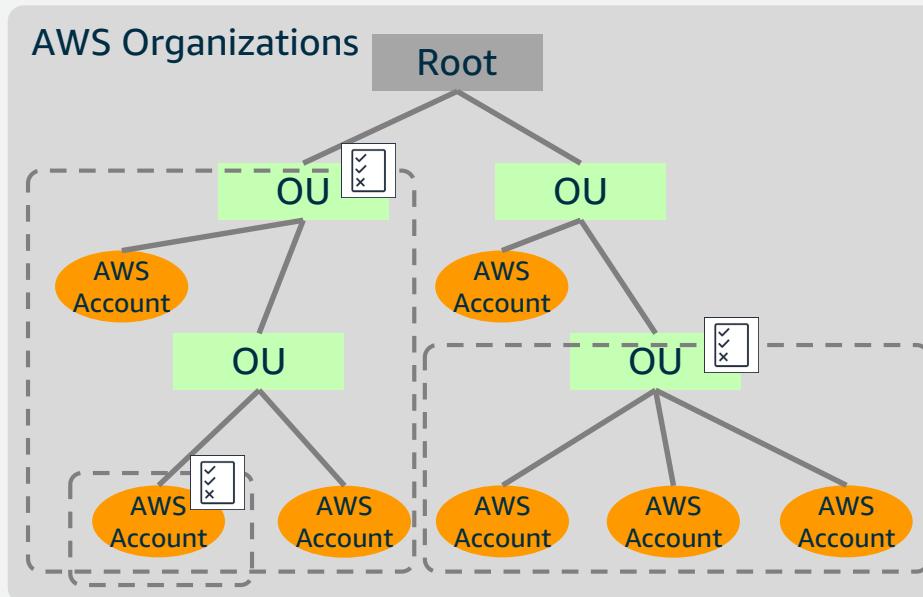
アクセス許可の境界 (Permission Boundary)

- アクセス許可の境界とアイデンティティベースのポリシーの両方で許可されているものが有効な権限となる (AND条件)



AWS Organizations サービスコントロールポリシー (SCP)

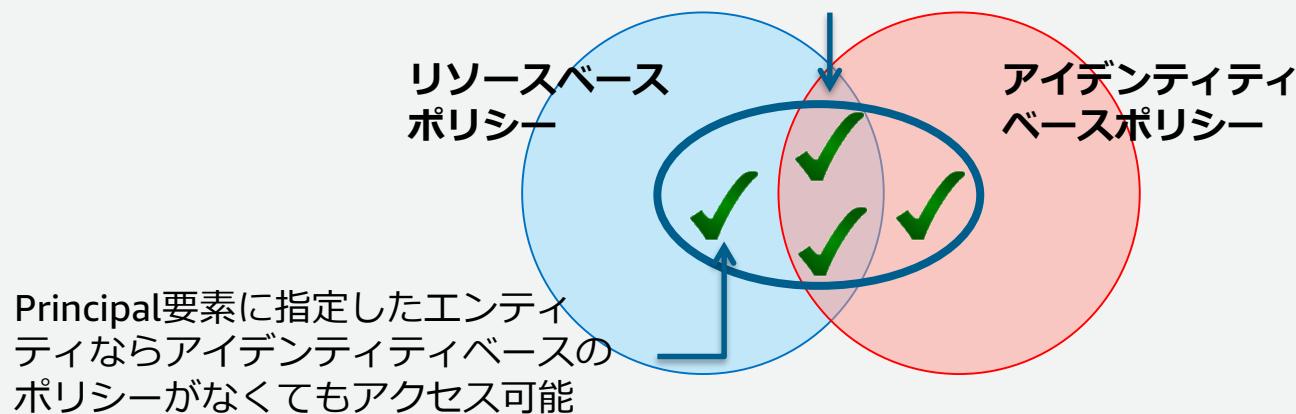
- SCPとアイデンティティベースのポリシーの両方で許可されているものが有効な権限となる (AND条件)



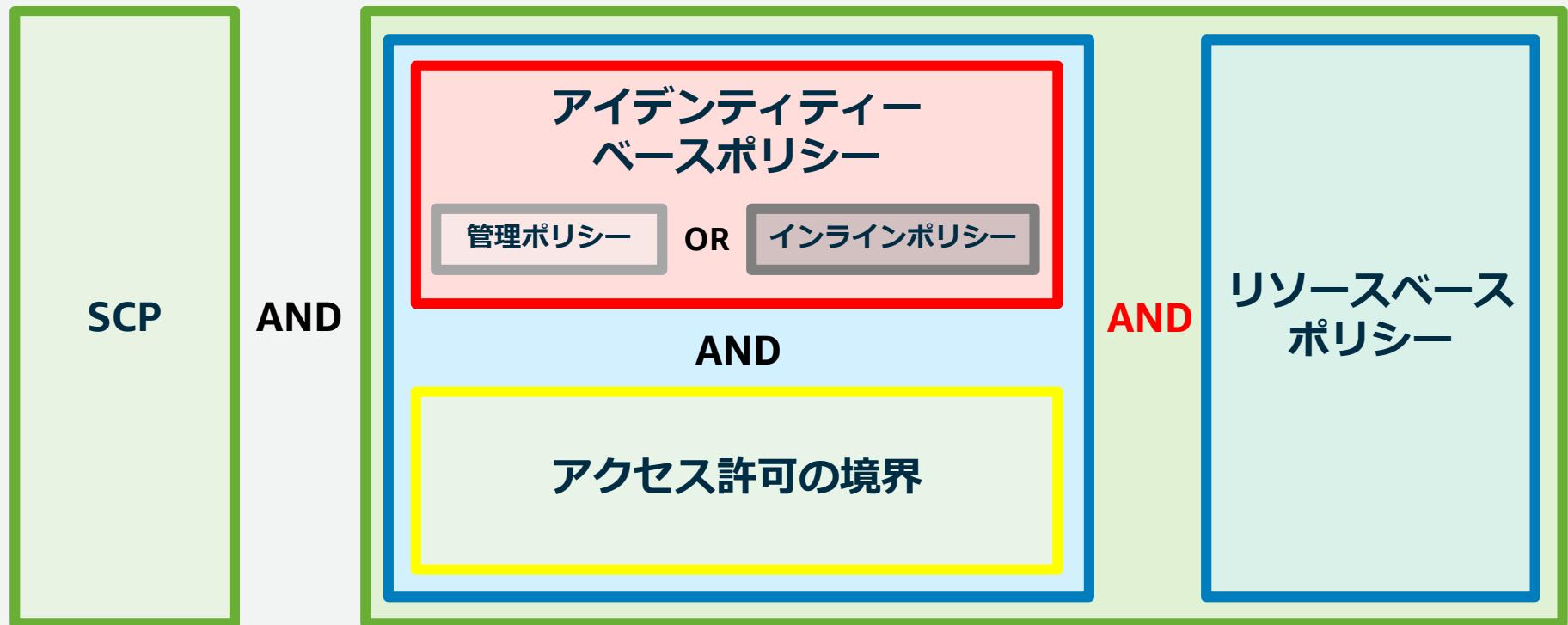
リソースベースポリシー (同一アカウントの場合)

- 同一アカウントの場合、リソースベースポリシーとアイデンティティベースポリシーのそれぞれで許可されているものが有効となる (OR条件)

そのリソースに対して許可される権限



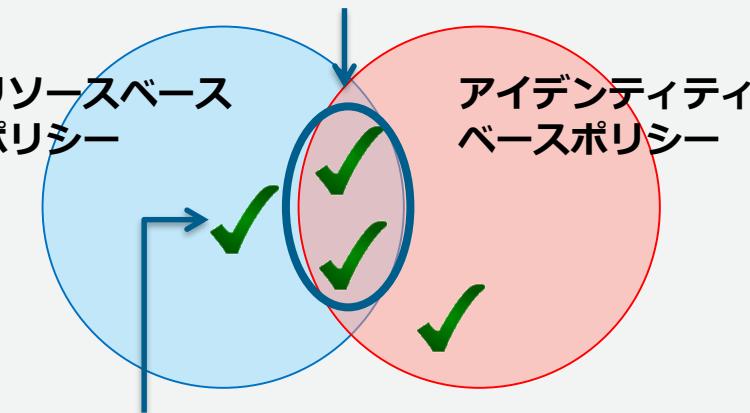
アクセス権の決定ロジック (クロスアカウントの場合)



リソースベースポリシー (クロスアカウントの場合)

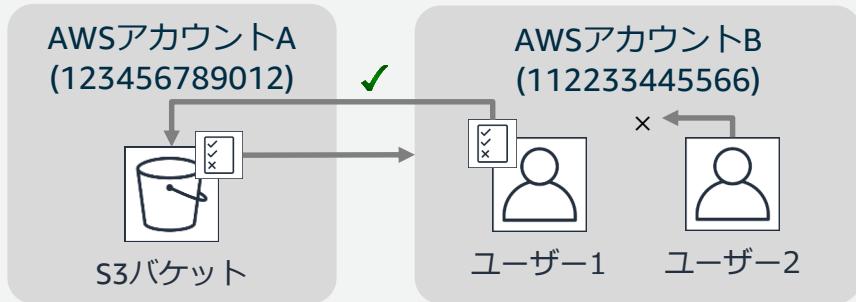
- クロスアカウントの場合、リソースベースポリシーとアイデンティティベースポリシーの両方で許可されているものが有効となる (AND条件)

そのリソースに対して許可される権限



Principal要素に信頼するエンティティの指定が必要

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.



1.AWSアカウントAのバケットポリシーに以下の権限を設定

```
{  
  "Statement": {  
    "Effect": "Allow",  
    "Principal": {"AWS": "arn:aws:iam::112233445566:root"},  
    "Action": "s3:*",  
    "Resource": "arn:aws:s3:::mybucket/*"  
  }  
}
```

Principalは、実行をしているユーザーに対する条件設定

2.AWSアカウントBのエンティティにアクセス権限を付与

```
{  
  "Statement": {  
    "Effect": "Allow",  
    "Action": "s3:GetObject",  
    "Resource": "arn:aws:s3:::mybucket/*"  
  }  
}
```



✓ 最小権限を付与する

Grant Least Privilege

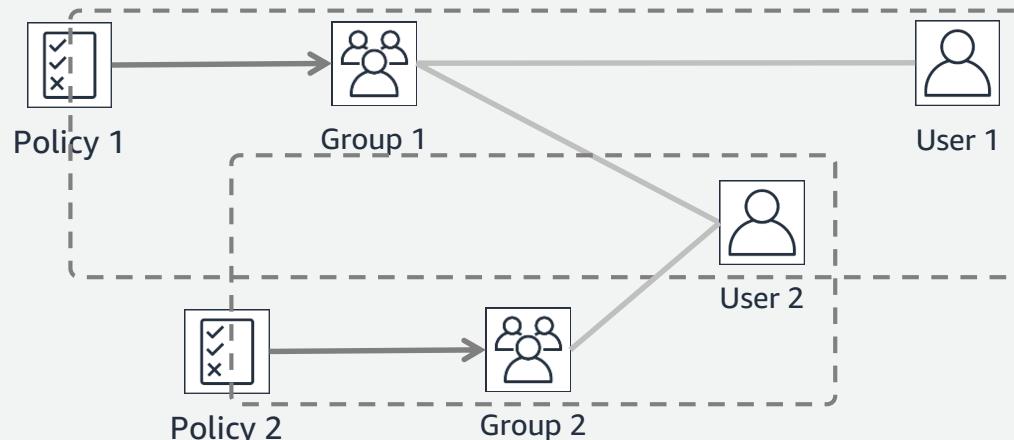
- IAMポリシーを作成する場合、タスクの実行に必要なアクセス許可のみ付与する
- 最小限のアクセス権限から開始し、必要に応じてアクセス権限を追加する
 - あとでアクセス権限を強化するより安全なアプローチ
- 役立つ情報
 - アクセスアドバイザーのサービスの最終アクセス時間データ
 - Amazon CloudTrailのイベントログ
 - IAMポリシーのリファレンス
 - https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_policies.html
 - Blackbeltオンラインセミナー AWSサービスの権限管理
 - https://d1.awsstatic.com/webinars/jp/pdf/solution-casestudy/20160621_AWS-BlackBelt-Authority-public.pdf

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

IAMグループ

- IAMユーザーの集合
- IAMグループやIAMロールをIAMグループに所属させることは不可
- IAMユーザーは複数のIAMグループに所属することができる (最大10)
- IAMグループに関連付けられたIAMポリシーは所属するIAMユーザーに継承される



✓ 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 Use Groups to Assign Permissions to IAM Users

- ポリシーの関連付けを簡単にするためにはIAMグループを利用した方が便利
- 組織またはジョブ機能に関連したIAMグループを作成し、IAMグループに対してアクセスIAMポリシーを関連付ける
- 会社内で組織異動がある場合は、そのIAMユーザーが所属するIAMグループを変更すればよい

ここまでまとめ：アクセス権限の管理のベストプラクティス

- ✓ 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

まとめ

AWS IAMのベストプラクティス

IDと認証情報の管理	<ul style="list-style-type: none">✓ AWSアカウントのルートユーザーアクセキーをロックする✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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✓ 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、最小権限を確認する✓ 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
IDと権限のライフサイクル管理	<p>Part 2</p>

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
- 最小限の認証情報の生成、強力なパスワードポリシー、特権ユーザーでのMFA有効化がアイデンティティの保護に有効
- ポリシードキュメントとポリシーの論理評価ロジックに対する理解を深めて、最小権限を追求

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_awst10.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>





このコンテンツは公開から3年以上経過しており内容が古い可能性があります
最新情報については[サービス別資料](#)もしくはサービスのドキュメントをご確認ください

[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

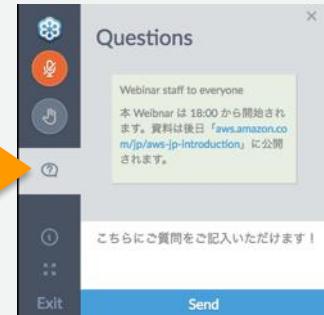
AWS Black Belt Online Seminar とは

「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、Amazon 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	<ul style="list-style-type: none">✓ AWSアカウントのルートユーザーの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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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 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の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TFA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回収する

Part 1

Part 2

(本日お話する範囲)

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

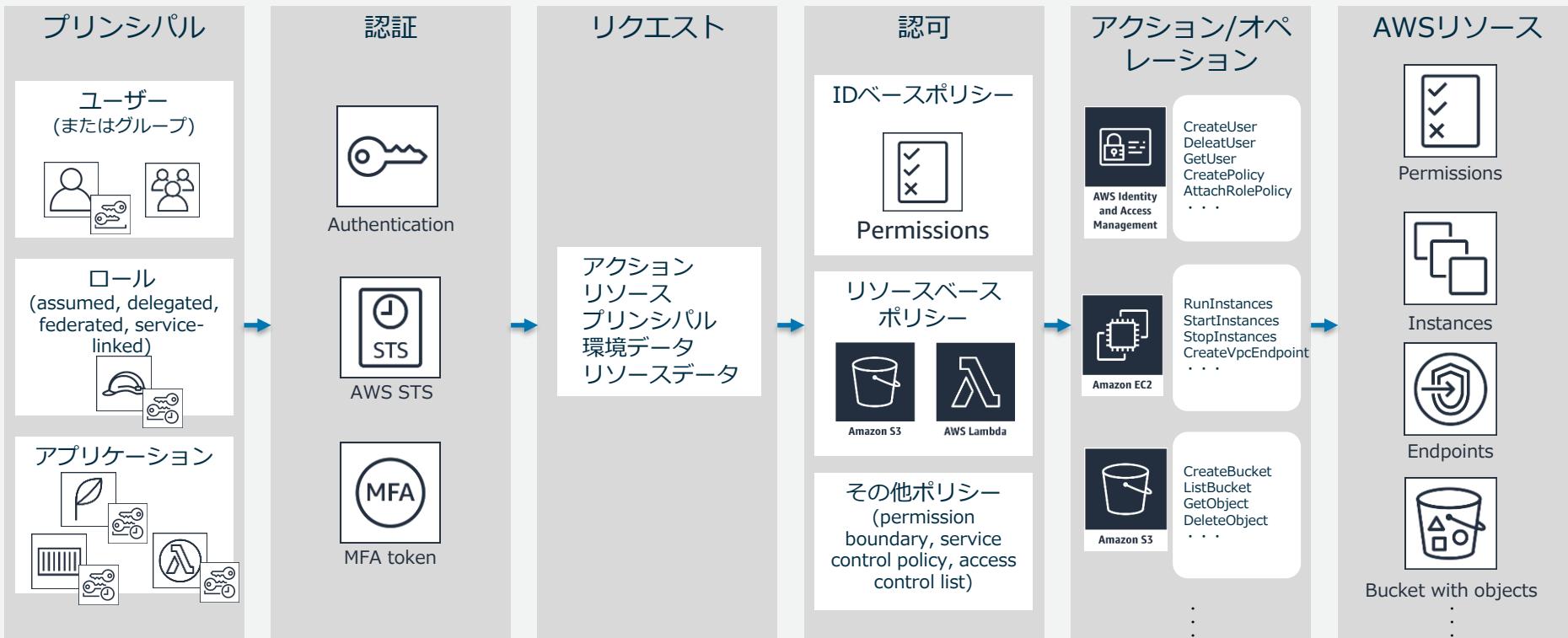
AWS IAMの概要

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

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



一時的なセキュリティ認証情報を取得するためのAPI

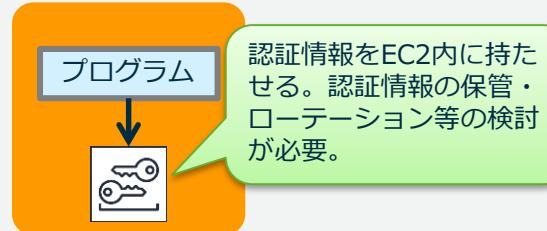
STSで利用できるAPI Action	概要
AssumeRole	既存のIAMユーザーの認証情報を用いて、IAM Roleの temporary security credentialsを取得するためのアクション
AssumeRoleWithWebIdentity	AmazonやFacebook、Googleによる承認情報を使用してロールを引き受け、temporary security credentialsを取得するためのアクション
AssumeRoleWithSAML	IdPによる認証とSAMLのアサーションをAWSにポストすることでロールを引き受けtemporary security credentials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

✓ 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



IAMロールによる権限はEC2上に恒久的に保管されるものではなくテンポラリ。ローテーション等は自動で行われる。

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

ロールを使用したアクセス許可の委任の例

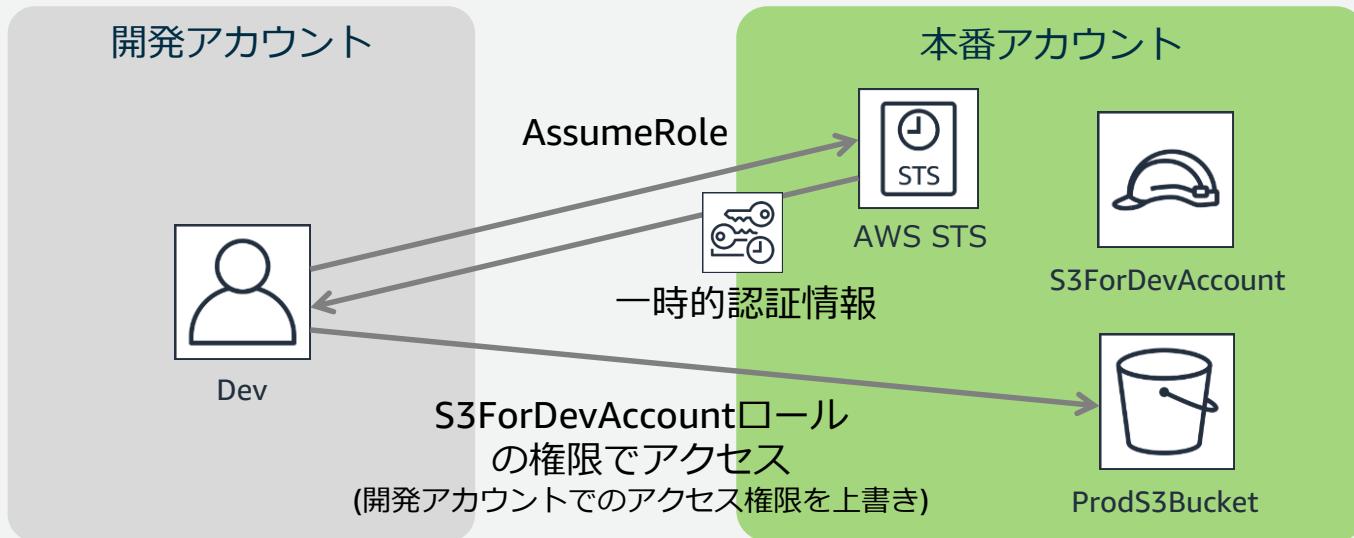
別の AWS アカウントのユーザーが、認証情報を共有せずに、自分の AWS アカウントのリソースにアクセスを制御可能にすることが可能。

ユースケース：

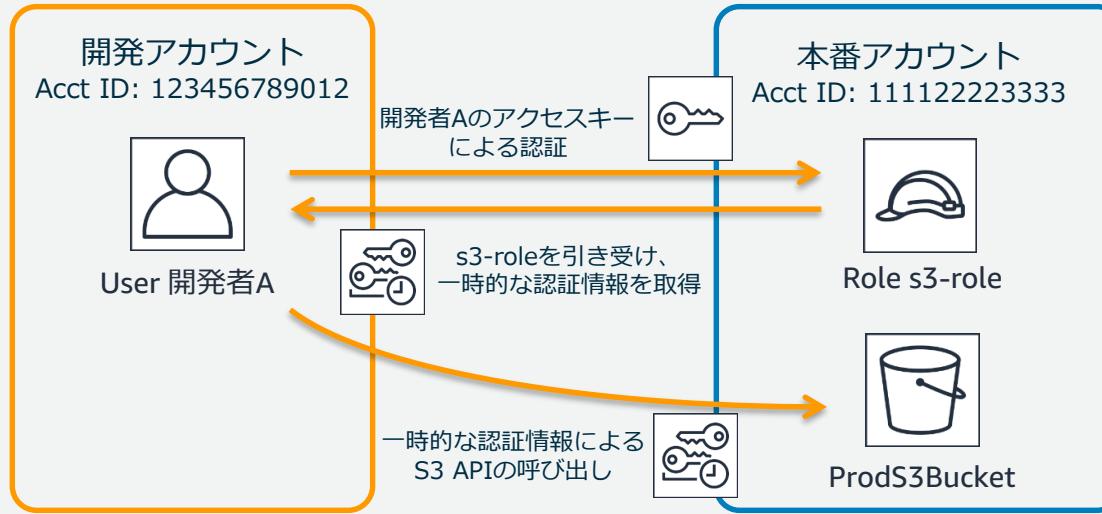
1. IAMロールによるクロスアカウントアクセス
2. クロスアカウントアクセスにより権限管理を効率化
3. SAML2.0ベースのIDフェデレーション
4. SAML2.0ベースのAWSマネジメントコンソールへのシングルサインオン (SSO)
5. Amazon Cognitoを用いたモバイルアプリのWeb IDフェデレーション

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



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" } ] }
```

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

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

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": {"NumericGreaterThanOrEqual": {"aws:MultiFactorAuthAge": "3600"}}

Create role

Select type of trusted entity

AWS service EC2, Lambda and others

Another AWS account Belonging to you or 3rd party

Web identity Cognito or any OpenID provider

SAML Your own SAML provider

Allows entities in other accounts to perform actions in this account. Learn more

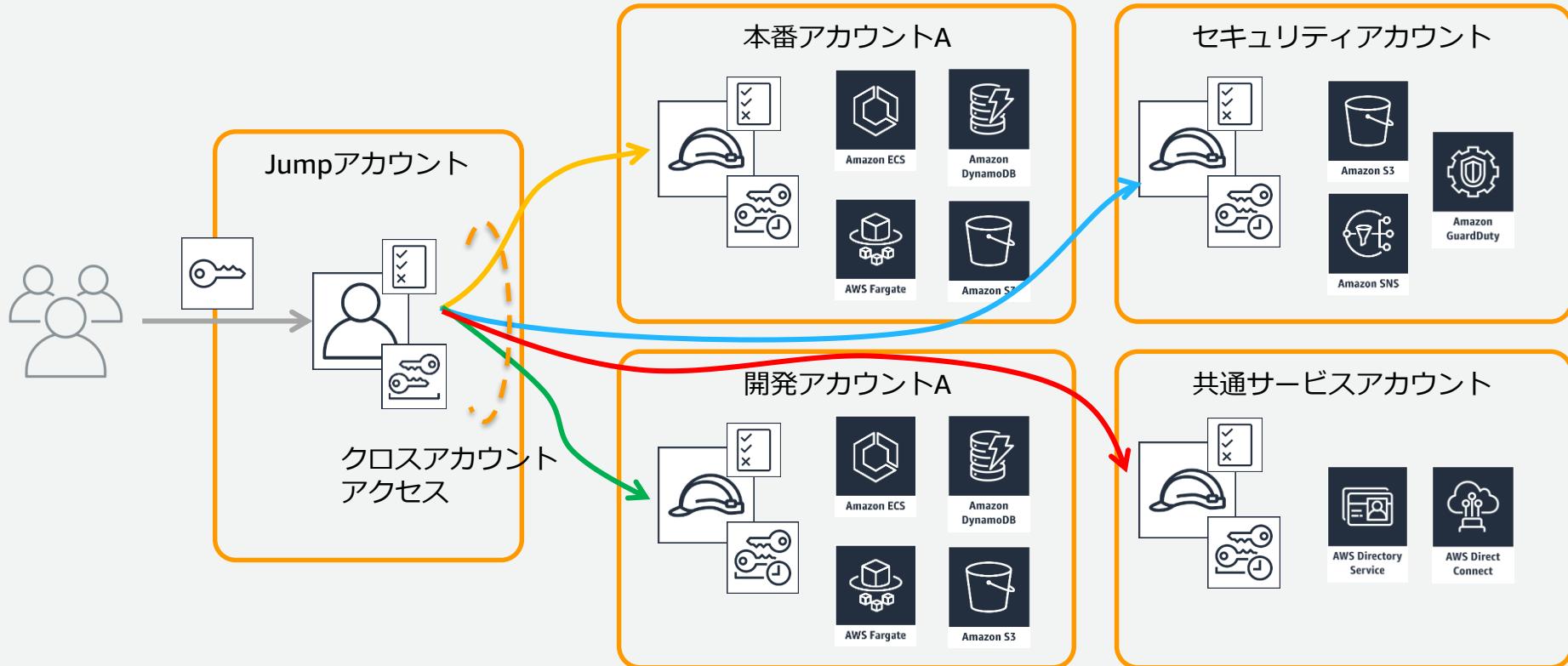
Specify accounts that can use this role

Account ID*

Options Require external ID (Best practice when a third party will assume this role) Require MFA

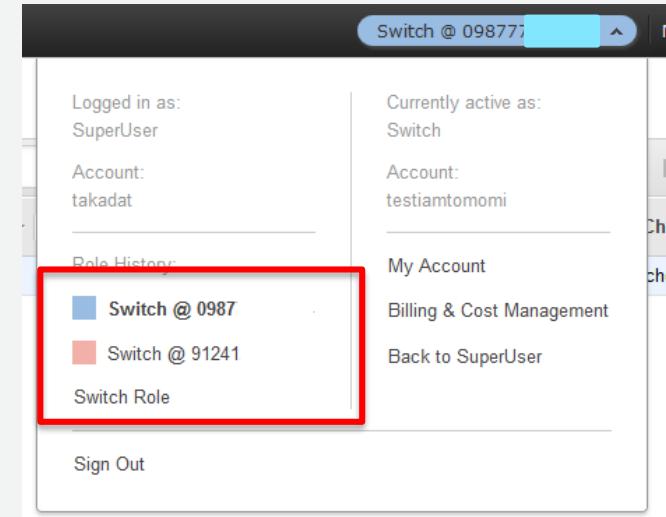
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "ec2:*",  
      "Resource": "*",  
      "Condition": {  
        "NumericLessThan": {"aws:MultiFactorAuthAge": "3600"}  
      }  
    }  
  ]  
}
```

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

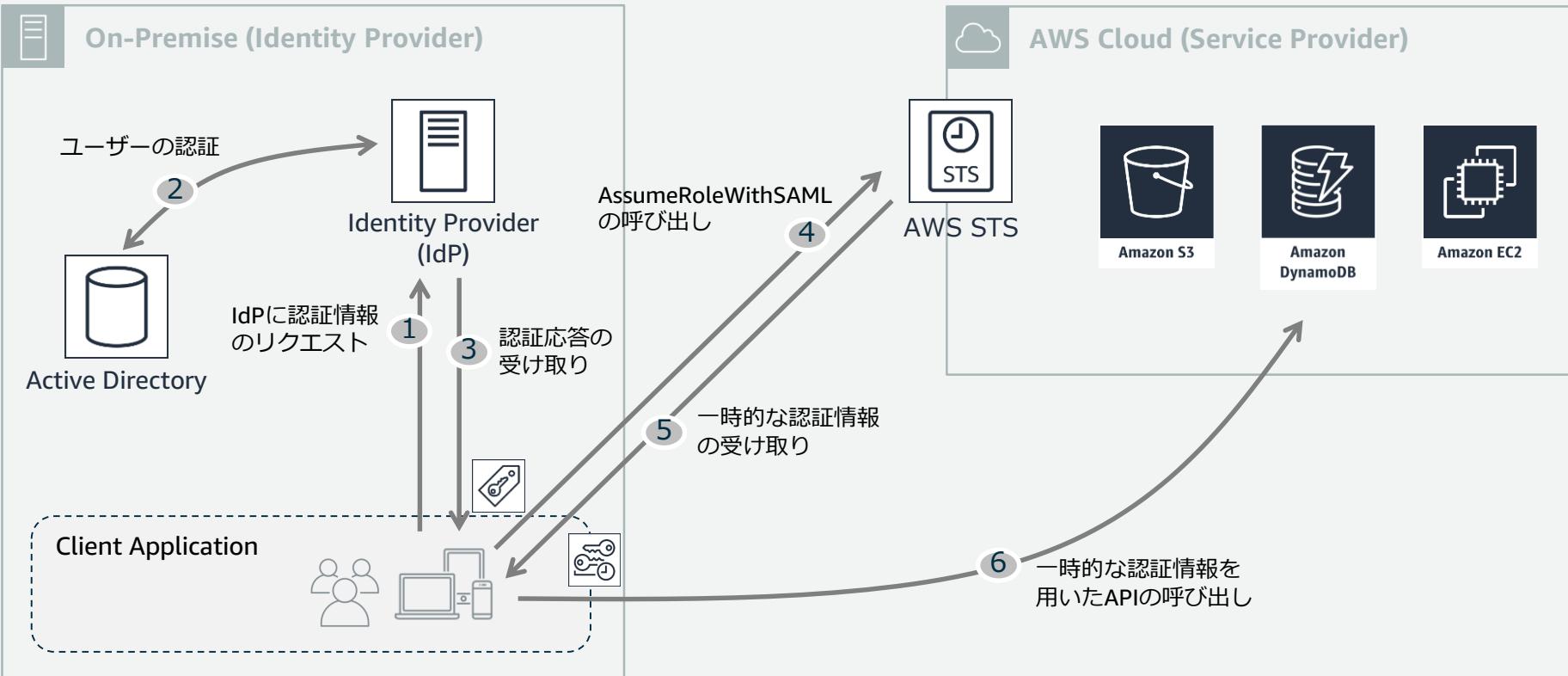
- IAMユーザーからクロスアカウントアクセス用IAMロールにコンソールから切替が可能
 - 必ずしも別アカウントである必要はなく、同じアカウントでもOK
- 必要な時のみIAMユーザーの権限を“昇格”させる
 - IAMユーザーには読み取り権限のみを付与
 - IAMロールには更新権限を付与



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

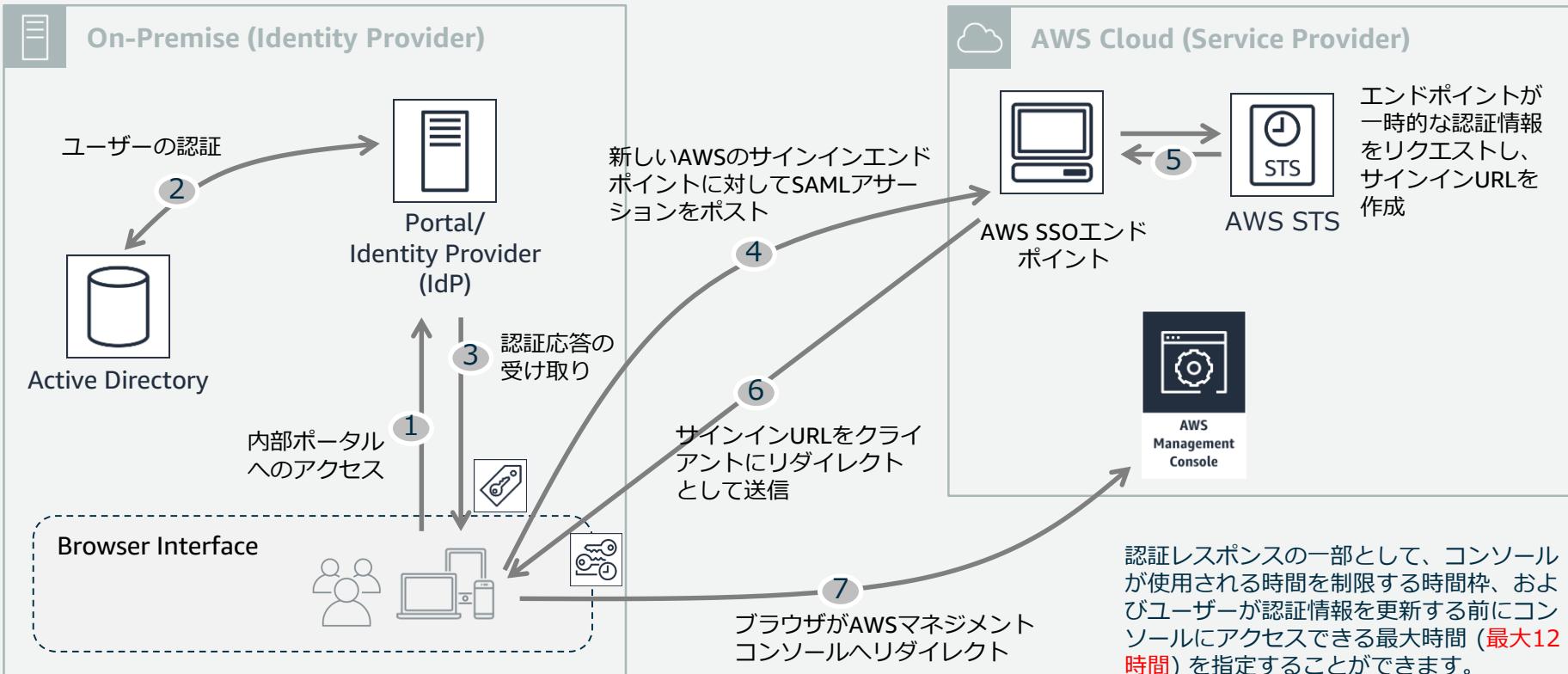
SAML2.0ベースのIDフェデレーションの動作



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



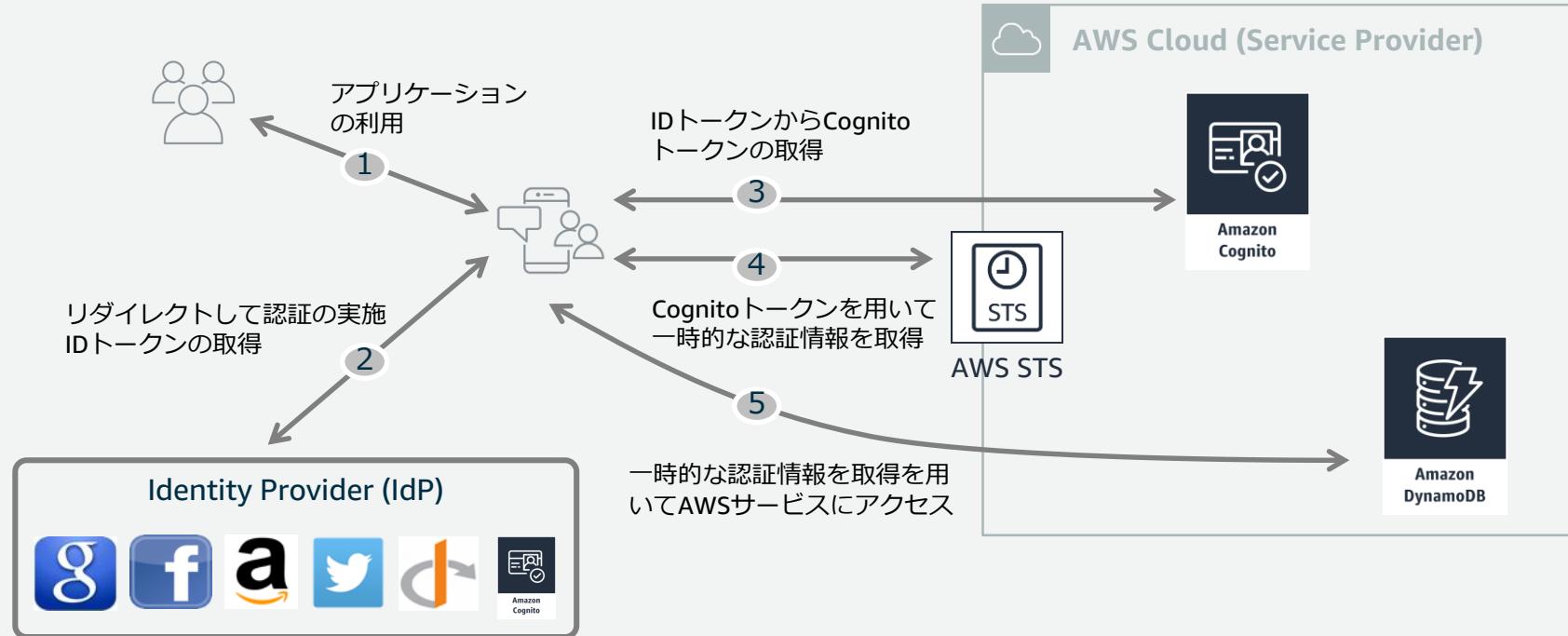
AWSマネジメントコンソールフェデレーションのメリット

- ・ 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



フェデレーション/SSOのパートナーソリューション



BITIUM



One Global Identity to Drive Business in a Distributed World



✓ 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

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

- CloudFront が受信したユーザーリクエストを記録。

Amazon CloudFront



Amazon
CloudFront

- 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
CloudTrail

- 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

Amazon CloudWatch



Amazon
CloudWatch

- 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

AWS Config



AWS
Config

- Amazon S3 バケットへのアクセスリクエストを記録

Amazon S3



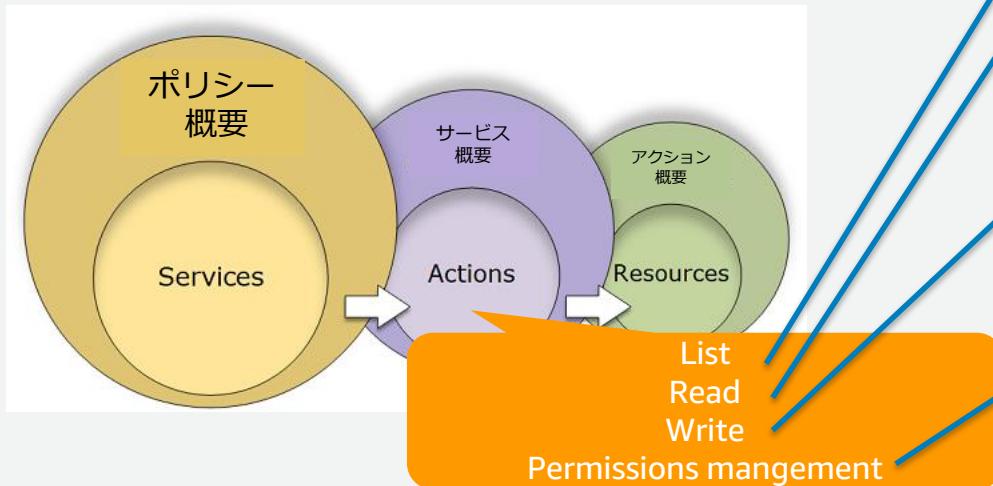
Amazon
S3

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
ポリシー概要 JSON					
戻る S3					
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）

The screenshot shows the AWS IAM User Details page for a user named 'amplify-user'. The left sidebar has a red box around the 'User' link under the 'Groups' section. The main content area has a red box around the 'Access Advisor' tab in the navigation bar. Below it, a note says: 'アクセスアドバイザーには、このユーザーに付与されたサービスのアクセス権限と、これらのサービスが最後にアクセスされた時間が表示されます。この情報をを使ってポリシーを変更できます。 詳細はこちら'.

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

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

Policy Document Attached Entities Policy Versions Access Advisor

Access advisor shows the service permissions granted to this user and when those services were last accessed. You can use this information to revise your policies. [Learn more](#)

Note: recent activity usually appears within 4 hours. Access Advisor tracking began on Oct 1, 2015. [Learn more](#)

Showing 76 results

Service Name	Access by Entities	Last Accessed
AWS Identity and Access Management	lambda_basic_execution and 1 more	Today
Amazon CloudWatch Logs	lambda_basic_execution and 1 more	Today
AWS Config	lambda_basic_execution and 1 more	Today
Amazon S3	lambda_basic_execution and 1 more	Today

Access by Entities

Service Name: AWS Identity and Access Management
Policy: AdministratorAccess

Name	Type	Last accessed
lambda_basic_execution	Role	2016-09-18 10:00-11:00 UTC+0900
Admin	User	2016-08-31 19:00-20:00 UTC+0900
Platform	User	Not accessed in the tracking period
CFnGenerator	Role	Not accessed in the tracking period

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簡単に識別可能

✓ 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。

The screenshot shows two side-by-side IAM policy review interfaces.

Left Panel (Policy Advisor):

- Header tabs: 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.
- Sub-tabs: ポリシー概要, [JSON].
- Content: A JSON code editor showing a policy document with one statement allowing S3 actions on all resources.

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3>List*"
9       ],
10      "Resource": "*"
11    }
12  ]
13 }
  
```

Right Panel (Usage Metrics):

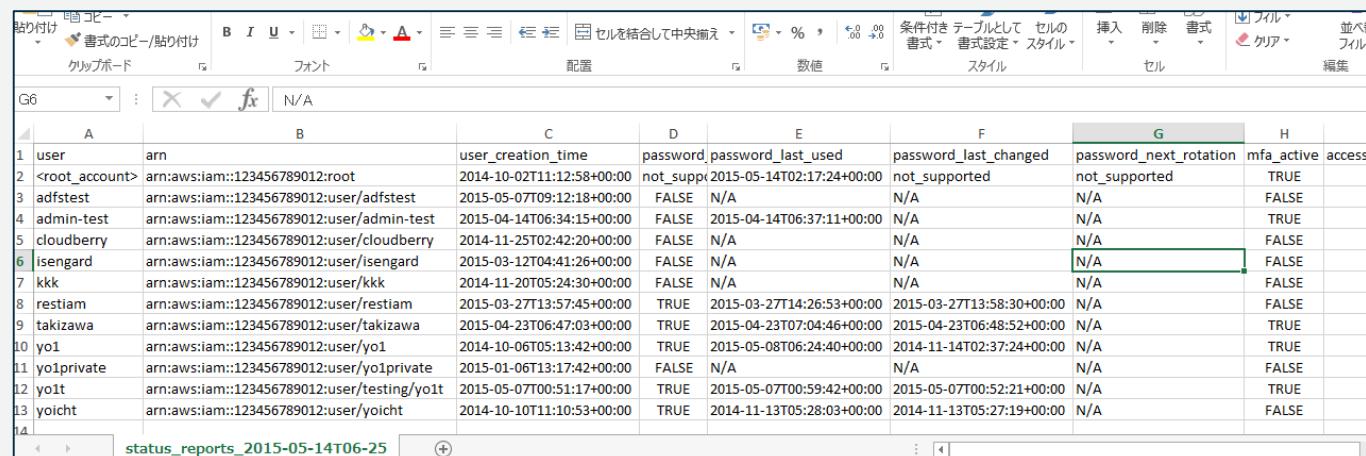
- Header tabs: アクセス権限, ポリシーの使用状況, ポリシーのバージョン, アクセスアドバイザー.
- Sub-tabs: ポリシー概要, [JSON].
- Search bar: Q フィルター.
- Filter dropdown: サービス ▾ (S3 selected), アクセスレベル (All selected), リソース (All selected).
- Summary: 許可 (169 サービス中 1) 残りの 168 を表示.
- Table rows: S3, 完全: 読み込み 制限: リスト, すべてのリソース.

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



The screenshot shows a Microsoft Excel spreadsheet titled "status_reports_2015-05-14T06-25". The table contains data for 14 IAM users, including their ARN, creation time, password history, and MFA status. The columns are labeled A through H.

A	B	C	D	E	F	G	H
1 user	arn	user_creation_time	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_supported	2015-05-14T02:17:24+00:00	not_supported	not_supported	TRUE
3 adftest	arn:aws:iam::123456789012:user/adftest	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							

認証情報レポートは、
4 時間ごとに 1 回生成
できます。

✓ 不要な認証情報を削除する

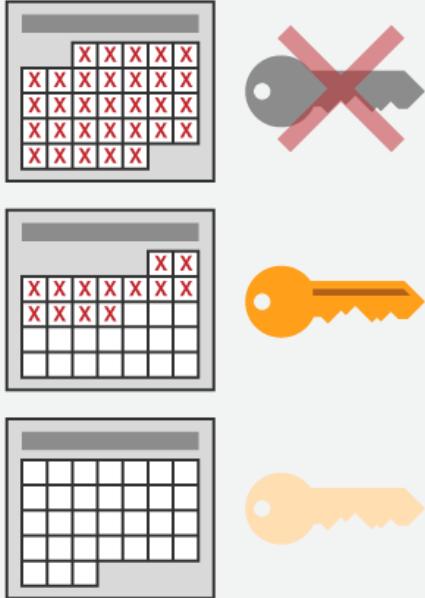
Remove Unnecessary Credentials

- 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。



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

IAM の検索

追加

1 つの結果

フィルター ▾

- ユーザー takizawa をグループに追加
- ユーザー yo1 をグループに追加
- ユーザー yo1-alexa をグループに追加
- ユーザー yo1-mac をグループに追加
- ユーザー yo1private をグループに追加
- ユーザー yo1t をグループに追加

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

The screenshot shows the AWS IAM Policy Editor interface. At the top, there are tabs for 'Visual Editor' (highlighted with a red box), 'JSON' (highlighted with a blue box), and 'Policy Editor' (highlighted with an orange box). The 'Policy Editor' tab has a red arrow pointing to it from the 'Visual Editor' tab. The main area displays the policy document for 'AWSQuickSightIAMPolicy'. It includes sections for 'Actions' (with 'iam>List*' selected), 'Access levels' (with 'List' selected), and 'Resources' (with 'All resources' selected). The top right corner shows the ARN of the policy: 'arn:aws:iam::843552679084:policy/service-role/AWSQuickSightIAMPolicy'. The status bar at the bottom right says 'さらにアクセス許可を追加する' (Add more access).

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            "ServiceNamespace": "cloudformation",  
            "LastAuthenticatedEntity            "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	<ul style="list-style-type: none">✓ AWSアカウントのルートユーザーアクセキーをロックする✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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	<ul style="list-style-type: none">✓ 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

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_awst10.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>



AWS Black Belt Online Seminar

AWS Identity and Access Management (IAM) Access Analyzer

田中 嶽

Cloud Support Engineer

2024/12



自己紹介

田中 峻

アマゾン ウェブ サービス ジャパン合同会社
技術支援本部 クラウドサポートエンジニア

好きな AWS サービス



AWS Identity and Access Management (IAM)



AWS IAM Identity Center



AWS Security Hub



AWS Black Belt Online Seminar とは

- ・ 「サービス別」「ソリューション別」「業種別」などのテーマに分け、
アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- ・ AWS の技術担当者が、 AWS の各サービスやソリューションについてテーマごとに動画を公開します
- ・ 以下の URL より、過去のセミナー含めた資料などをダウンロードすることができます
 - <https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/>
 - <https://www.youtube.com/playlist?list=PLzWGOASvSx6FIwIC2X1nObr1KcMCBBlqY>

𝕏 ご感想は X (Twitter) へ！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

- ・ 本資料では資料作成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。AWS のサービスは常にアップデートを続けているため、最新の情報は AWS 公式ウェブサイト (<https://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には別途消費税をご請求させていただきます
- ・ 技術的な内容に関しましては、有料の [AWS サポート窓口](#)へお問い合わせください
- ・ 料金面でのお問い合わせに関しては、[カスタマーサポート窓口](#)へお問い合わせください (マネジメントコンソールへのログインが必要です)

本セミナーの対象者と得られること

本セミナーの対象者

- AWS IAM のアクセス権限の管理・運用を担当されている方
- AWS IAM Access Analyzer の利用を検討されており、各種機能の理解を深めたい方

本セミナーで得られること

- AWS IAM Access Analyzer の各種機能に対する理解
- AWS IAM Access Analyzer を用いたアクセス権限管理の効率化について

アジェンダ

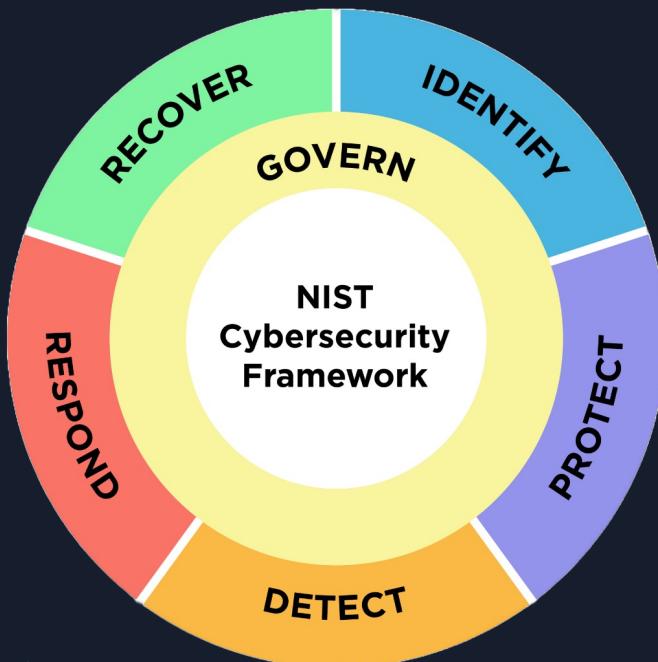
1. アクセス権限管理の重要性・課題
2. AWS IAM Access Analyzer の概要
3. AWS IAM Access Analyzer の各種機能
4. AWS IAM Access Analyzer の料金

アクセス権限管理の重要性・課題

アクセス権限管理の重要性

NIST サイバーセキュリティフレームワーク (CSF) とは、米国国立標準技術研究所 (NIST) が政府や民間から意見を求めて作成したもので、CSF を活用することにより、統治、識別、防御、検知、対応、復旧という 5 つの機能を中心としたセキュリティ対策のベースラインを構築できる。

その内の防御の対策の 1 つとして、アクセス制御が挙げられている。



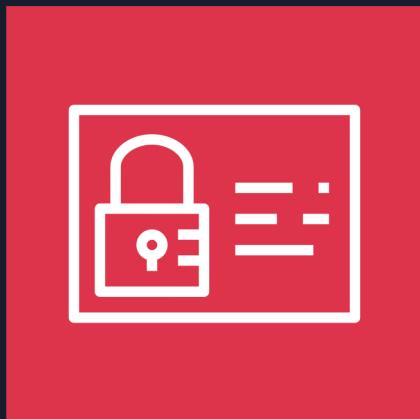
Protect 防御

- アイデンティティ管理、認証、アクセス制御
- 意識向上とトレーニング
- データセキュリティ
- プラットフォームセキュリティ
- 技術インフラのレジリエンス

<https://www.nist.gov/cyberframework>

AWS におけるアクセス権限管理

AWS におけるアクセス権限管理は、AWS Identity and Access Management (IAM) を用いて一元的に実施可能



AWS Identity and Access Management (IAM)

- AWS IAM は AWS サービスに対して認証と認可を提供
- 許可したい、もしくは拒否したい操作を IAM ポリシーに定義
- 作成した IAM ポリシーを IAM エンティティ (ユーザー・ロール) にアタッチし、アクセス権限を管理

AWS IAM のアクセス権限管理における課題



使われていない IAM エンティティやアクセス権限を頻繁にモニタリングする必要がある



組織拡大により管理対象のアカウント・リソースが増え、運用負荷が増大する

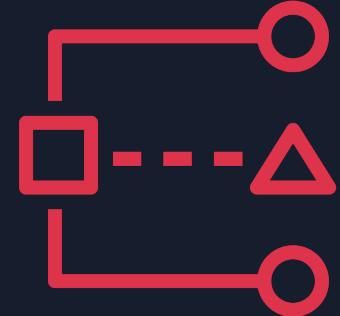


利用者毎に最低限必要なリソースやアクションの許可のみを与えること(= 最小権限)を実現しようとすると、運用コストが高くなる

AWA IAM Access Analyzer の概要

AWS IAM Access Analyzer

AWS IAM の機能の一部であり、アクセス権限管理・運用を効率化するのに役立つ機能を提供



主な機能

- 外部エンティティから利用可能なリソースの特定
- アカウント内の使用されていない認証情報やアクセス権限の特定
- AWS CloudTrail ログを用いたアクティビティに基づく IAM ポリシー生成
- IAM ポリシーについて、ポリシーの文法やベストプラクティスに照らして検証

AWS IAM Access Analyzer のメリット

	セキュリティ強化	<ul style="list-style-type: none">不適切なアクセス権限を特定最小権限の実現を効率化IAM ポリシー検証でポリシーを検証外部アクセスが許可されたリソースを検出
	可視化	<ul style="list-style-type: none">使われていない認証情報やアクセス権限を特定し、表示
	オートメーション	<ul style="list-style-type: none">IAM リソースや S3 バケットなどのリソースを自動的に分析Amazon EventBridge と連携することで、意図しないアクセス権限の修正を自動化し、運用を効率化
	管理容易性	<ul style="list-style-type: none">AWS Security Hub と統合し、検出結果を一元管理使われていない認証情報やアクセス権限に対して、レコメンデーションを提示

AWS IAM のセキュリティベストプラクティス抜粋

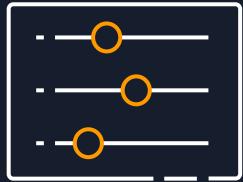


- ・ ワークロードが AWS にアクセスする場合に IAM ロールを使用する
- ・ 多要素認証 (MFA) を必須とする
- ・ アクセスキーを定期的にローテーションする
- ・ ルートユーザーの認証情報を保護する
- ・ 最小権限を付与する
- ・ AWS 管理ポリシーの使用から始めて、最小権限のポリシーに移行する
- ・ IAM ポリシーで条件を指定して、アクセス権限をさらに制限する
- ・ 未使用の AWS IAM リソースを定期的に確認して、不要なものを削除する
- ・ AWS IAM Access Analyzer を使用して、アクティビティに基づいてポリシーを生成する
- ・ AWS IAM Access Analyzer を使用して、外部からアクセス可能なリソースを確認する
- ・ AWS IAM Access Analyzer を使用して IAM ポリシーを検証する

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

AWA IAM Access Analyzer の各種機能

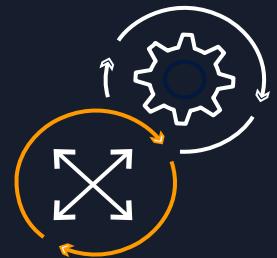
利用できる 5 つの機能



外部アクセスアナライザー



未使用アクセスアナライザー



ポリシー生成



ポリシーチェック



カスタムポリシーチェック

外部アクセスアナライザー

- AWS リソースが外部エンティティからアクセス可能となっているかを自動的に分析し、特定可能
 - 外部エンティティからアクセス可能である場合には、**検出結果**を生成
- アカウントまたは組織レベルで外部アクセスアナライザーを有効化
- アクセスログを調べて、実際に外部エンティティが AWS リソースにアクセスしたかどうかを判断しない
 - AWS リソースのリソースベースポリシーなどのメタデータを分析
- 分析したいリソースがあるリージョンで有効化する必要がある



外部アクセスアナライザーが分析するサービス

外部アクセスアナライザーでは主要なサービス・リソースをサポート



Amazon Simple Storage
Service (Amazon S3)



AWS Identity and Access
Management (IAM)



AWS Key Management
Service (AWS KMS)



AWS Lambda



Amazon Simple Notification
Service (Amazon SNS)



AWS Secrets Manager



Amazon Simple Queue
Service (Amazon SQS)



Amazon Elastic Block Store
(Amazon EBS)



Amazon Elastic Container
Registry (Amazon ECR)



Amazon Relational Database
Service (Amazon RDS)



Amazon DynamoDB



Amazon Elastic File System
(Amazon EFS)

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/access-analyzer-resources.html

外部アクセスアナライザーの仕組み

- サービスにリンクされたロール: **AWSServiceRoleForAccessAnalyzer** を用いて AWS リソースのリソースベースポリシーなどのメタデータを取得
➡ 分析したいリソースのリソースベースポリシーでは、IAM ロール **AWSServiceRoleForAccessAnalyzer** からのアクセスを拒否してはいけない ※ KMS キーでは例外的に明示的な許可も必要となります
- 自動推論エンジンを用いて分析

```
{  
  "Effect": "Deny",  
  "Principal": "*",  
  "Action": "s3:*",  
  "Resource": [  
    "arn:aws:s3:::EXAMPLE-BUCKET",  
    "arn:aws:s3:::EXAMPLE-BUCKET/*"  
  ],  
  "Condition": {  
    "StringNotEquals": {  
      "aws:PrincipalArn": "arn:aws:iam::123456789012:role/EXAMPLE-ROLE"  
    }  
  }  
}
```

エラーが発生するバケットポリシー例

```
{  
  "Effect": "Deny",  
  "Principal": "*",  
  "Action": "s3:*",  
  "Resource": [  
    "arn:aws:s3::: EXAMPLE-BUCKET",  
    "arn:aws:s3::: EXAMPLE-BUCKET/*"  
  ],  
  "Condition": {  
    "StringNotEquals": {  
      "aws:PrincipalArn": [  
        "arn:aws:iam::123456789012:role/EXAMPLE-ROLE",  
        "arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer"  
      ]  
    }  
  }  
}
```

バケットポリシーの変更例

外部アクセスアナライザーの検出結果への対応

検出結果を確認し、意図された設定ではない場合には対象リソースの見直しを実施

意図された設定である場合には手動でアーカイブすることが可能

また、アーカイブルールを作成することで、類似した検出結果を自動的にアーカイブできる

The screenshot shows the AWS IAM Access Analyzer results page. At the top, there's a breadcrumb navigation: IAM > Access Analyzer > 外部アクセス > 検出結果の詳細. On the right, there's a "再スキャン" (Rescan) button. The main area has two tabs: "詳細" (Details) and "次のステップ" (Next Steps). The "詳細" tab displays the following information:

検出結果 ID	外部プリンシパル (AWS アカウント)	Resource control policy (RCP) restriction	アクセスレベル
[REDACTED]	[REDACTED]	Not applicable	Write
リソース arn:aws:iam:[REDACTED]:role/[REDACTED] [REDACTED]	条件 -	更新済み 2 months ago	sts:AssumeRole
リソース所有者アカウント [REDACTED]	次を介して共有済み: -	ステータス アクティブ	

The "次のステップ" tab contains two sections: "意図されているアクセス" (Intended access) and "意図されていない" (Unintended access). The "意図されているアクセス" section includes a red box around the "アーカイブ" (Archive) button. The "意図されていない" section includes a "次に移動: IAM コンソール" (Move to: IAM console) button.

未使用アクセスアナライザー

- IAM ロールと IAM ユーザーを継続的にモニタリングし、追跡期間中に使用されていないアクセス許可・認証情報を特定
- IAM Access Analyzer が自動でモニタリングを行うため、セキュリティ担当者がこれまで実施していたタスクを肩代わりし、運用コスト削減が可能
- デフォルトの追跡期間は 90 日間
(1~180 日間で設定可能)
- アカウントまたは組織レベルで未使用アクセスアナライザーを有効化

生成される検出結果タイプ

- 未使用の IAM ロール
- 未使用の IAM ユーザーのコンソールパスワード
- 未使用の IAM ユーザーのアクセスキー
- 未使用のアクセス許可



未使用アクセスアナライザーの検出結果への具体的な修復手順を提供

未使用アクセスアナライザーでは、検出されたリソースに対する推奨事項を提供

The screenshot shows the AWS IAM Access Analyzer interface. On the left, a sidebar titled "推奨事項" (Recommendations) lists steps to resolve unused access permissions. Step 1 involves IAM roles, and Step 2 involves creating policies to attach to existing resources. The main area displays a table comparing existing and recommended policies for the "AdministratorAccess" role.

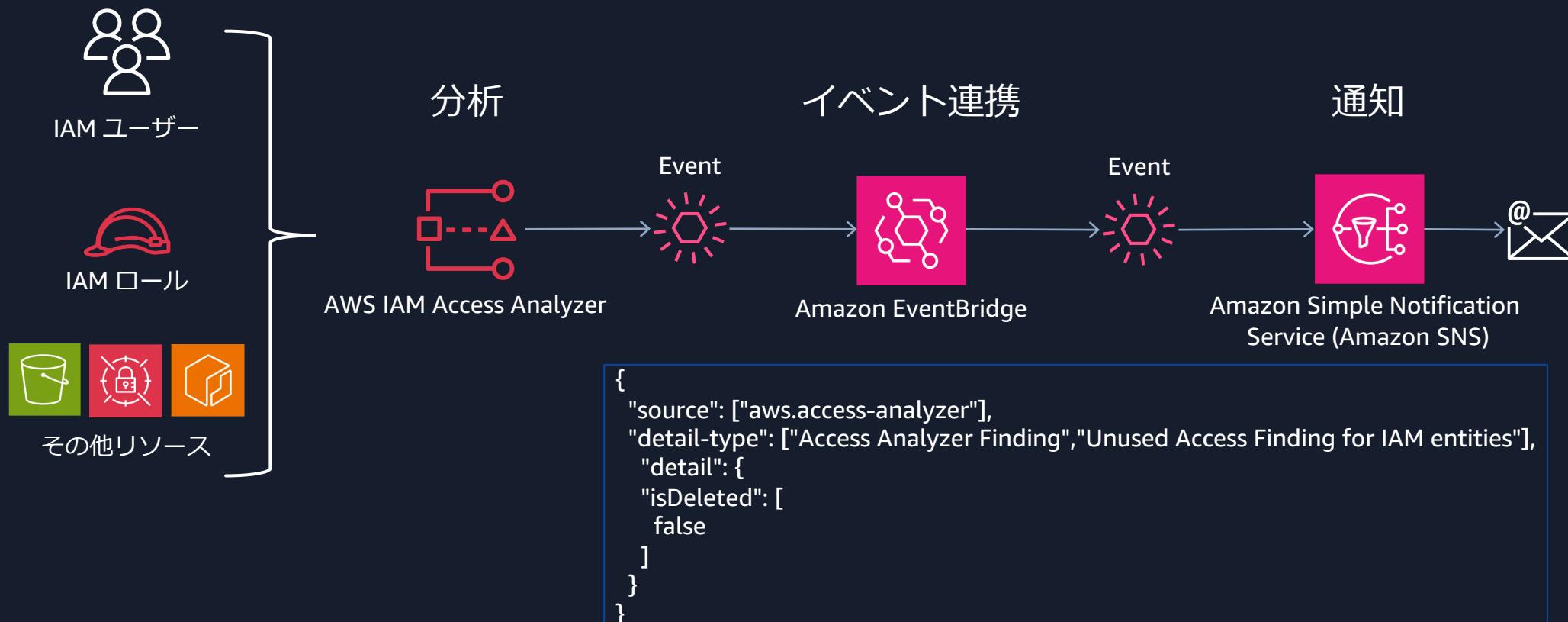
既存のアクセス許可ポリシー	推奨ポリシー	プレビュー
AdministratorAccess-recommended-1	ポリシーをプレビュー	
AdministratorAccess-recommended-2	ポリシーをプレビュー	
AdministratorAccess-recommended-3	ポリシーをプレビュー	

A red box highlights the "ポリシーをプレビュー" (Preview Policy) link for the first recommended policy. Below the table, a section titled "意図されている未使用の許可" (Intended unused permissions) is shown. To the right, a large preview window displays the detailed JSON content of the recommended policy, listing numerous EC2-related actions. Navigation buttons "前のポリシー" (Previous Policy) and "次のポリシー" (Next Policy) are at the bottom of the preview window.

```
146 "ec2:DescribeInstanceTypes",
147 "ec2:DescribeInstances",
148 "ec2:DescribeInternetGateways",
149 "ec2:DescribeKeyPairs",
150 "ec2:DescribeLaunch",
151 "ec2:DescribeLocalGatewayRouteTablePermissions",
152 "ec2:DescribePlacementGroups",
153 "ec2:DescribeRegions",
154 "ec2:DescribeSecurityGroups",
155 "ec2:DescribeSnapshots",
156 "ec2:DescribeSubnets",
157 "ec2:DescribeTags",
158 "ec2:DescribeVerifiedAccessInstanceWebAclAssociations",
159 "ec2:DescribeVolumeStatus",
160 "ec2:DescribeVolumes",
161 "ec2:DescribeVpcs",
162 "ec2:DisassociateVerifiedAccessInstanceWebAcl",
163 "ec2:GetEbs",
164 "ec2GetInstanceMetadataDefaults",
165 "ec2:GetResourcePolicy",
166 "ec2:ImportByIpCidrToIpam",
167 "ec2:InjectApiError",
168 "ec2:PauseVolumeIO",
169 "ec2:PurchaseCapacityBlock",
170 "ec2:PutResourcePolicy",
171 "ec2:SendSpotInstanceInterruptions",
172 "ec2:StopInstances",
173 "ec2:TerminateInstances",
174 "tag:GetResources",
175 "tag:GetTag",
176 "
```

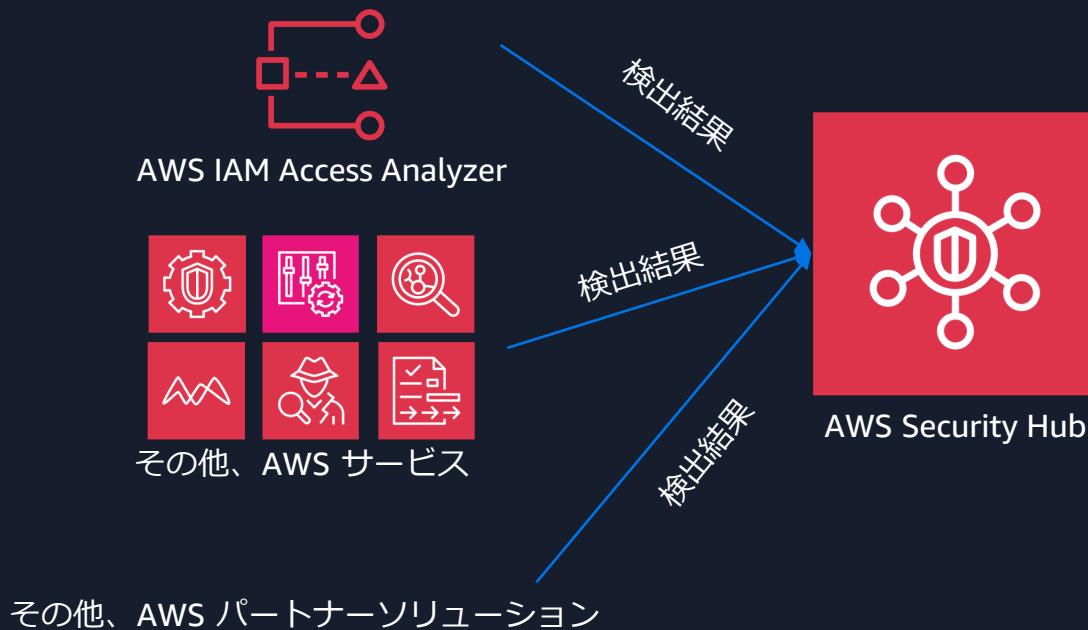
Amazon EventBridge との連携を通じた自動化

AWS IAM Access Analyzer の検出結果イベントを、Amazon EventBridge を介して様々な AWS サービスに対して受け渡して連携することが可能
例えば、検出時にメールで通知するようなアクションを実行



AWS Security Hub との統合を通じた検出結果の一元管理

外部アクセスアナライザー・未使用アクセスアナライザーの検出結果を AWS Security Hub に統合することで、他のセキュリティサービスの検出結果とあわせて一元的に管理が可能

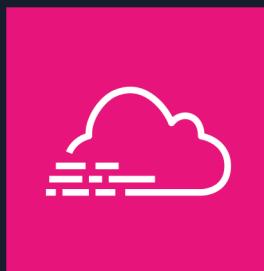


ポリシー生成機能

AWS CloudTrail 証跡を分析し、IAM エンティティ (ユーザーまたはロール) のアクティビティに基づく IAM ポリシーを自動的に生成

これにより、セキュリティ担当者の運用負荷を軽減することが可能

ただし、必ずしも完全な最小権限のポリシーを生成するわけではない



AWS CloudTrail 証跡



分析が完了すると
ポリシーが生成



生成されたポリシーを確認し、
適宜カスタマイズした後、
IAM ポリシーとして保存

ポリシーの生成

▼ CloudTrail イベントに基づいてポリシーを生成

このユーザーのアクセスアクティビティに基づいて新しいポリシーを生成すると、ポリシーのカスタマイズや生成、このロールへの添付が可能になります。AWSはCloudTrailイベントを使用して、使用されるサービスとアクションを識別し、ポリシーを生成します。詳細は[こちら](#)

ポリシーを生成

過去 7 日間におけるポリシー生成リクエストはありません。



CloudTrail イベントを分析する期間の指定
(最長で 90 日間の範囲を指定可能)

CloudTrail イベントを分析する期間とアクセス権限

期間を選択
 直近 1 日
 特定の日付
最長で 90 日間の範囲を選択します。

▼ CloudTrail アクセス

分析する CloudTrail 記録
このアカウントのイベントをログに記録する CloudTrail 記録を指定
米国東部(バージニア北部) []

リージョンを指定
ポリシーを生成するために、選択したリージョンからのサービスのアクティビティのみが確認されます。
リージョンを選択 []

この user のアクセスアクティビティを分析するために、IAMはユーザーに代わって以下のサービスロールを使用して、指定された記録にアクセスします。

新しいサービスロールを作成して使用
 既存のサービスロールを使用
AccessAnalyzerMonitorServiceRole [] ロールの詳細を表示

キャンセル ポリシーを生成

ポリシー生成機能について知っておくべきこと

- AWS CloudTrail 証跡の有効化が必要
- Amazon S3 データイベントなどのデータイベントについては分析しない
- iam:PassRole アクションについては AWS CloudTrail ログに記録されないため、生成されたポリシーには含まれない
- 分析期間を短くすることで、ポリシー生成時間の短縮が可能
- 生成されたポリシーは、IAM コンソールにて最大 7 日間確認可能

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/access-analyzer-policy-generation.html#access-analyzer-policy-generation-know

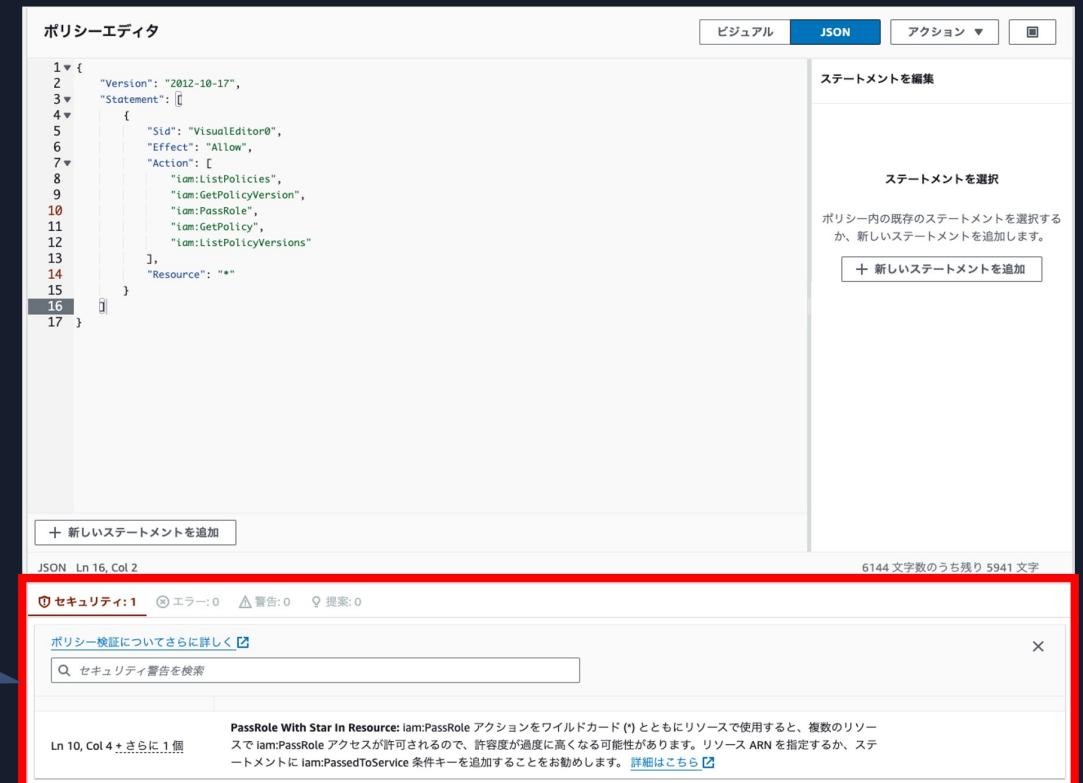
https://docs.aws.amazon.com/ja_jp/general/latest/gr/access-analyzer.html#limits_accessanalyzer



ポリシーチェック

- IAM ポリシーについて、文法および AWS のベストプラクティスに準拠しているかをチェック
- IAM ポリシーの作成や編集時に、設定ミスによる過度なアクセス許可を未然に防ぐことが可能
- IAM コンソールまたは AWS API を用いてチェック
- 事前に定義された 100 以上のチェック項目
 - セキュリティ警告
 - 文法エラー
 - 一般的な警告
 - 提案

IAM コンソールの
ポリシーエディタにて、
ポリシーを作成・変更する際に
自動チェック



https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/access-analyzer-reference-policy-checks.html

カスタムポリシーチェック

IAM ポリシー変更に対して、意図しない権限が付与されていないか、パブリックアクセスを許可するポリシーかどうかを検証

CheckNoNewAccess

ポリシーの変更によって、新しく権限が付与されないかをチェック

入力
変更前後のポリシー

出力
PASS – 新しい権限が付与されない
FAIL – 新しい権限が付与

CheckAccessNotGranted

ポリシーが、リソースへの意図しないアクセスを許可していないかをチェック

入力
ポリシーとアクションのリスト

出力
PASS – 指定アクションが許可されない
FAIL – 指定アクションが許可

CheckNoPublicAccess

リソースベースポリシーが、パブリックアクセスを許可していないかをチェック

入力
ポリシーとリソースタイプ

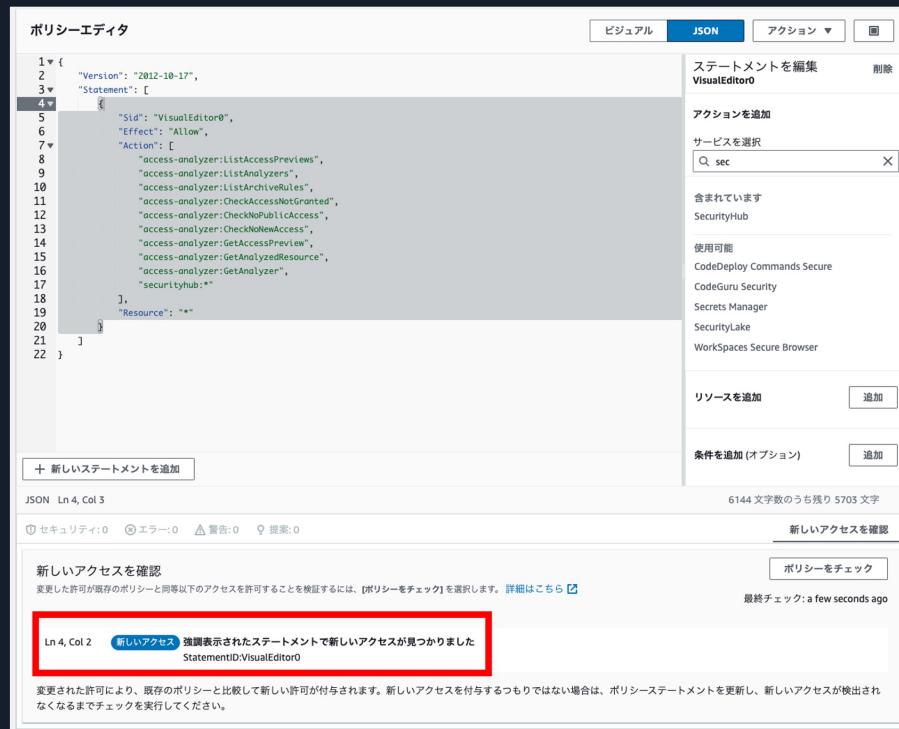
出力
PASS – パブリックアクセスが許可されない
FAIL – パブリックアクセスが許可

CheckNoNewAccess – 新しい権限

既存のポリシーと比較して、更新されたポリシーに対して新しい権限が許可されているかどうかをチェックできる機能

CheckNoNewAccess API を直接実行することで、特定のポリシーとも比較可能

特定のポリシーより強い権限を持つポリシーを作成させたくないユースケースに利用可能



IAM コンソールの
ポリシーエディタの他に、
CheckNoNewAccess API
を実行することでチェック可能

CheckAccessNotGranted – 特定リソースへの権限

ポリシーの作成・変更前に、アクセスさせたくないリソースへの権限を意図せず許可していないかを検証し、セキュリティを強化

特定の CloudTrail 証跡へのアクセス権がないかどうか調べたい場合は・・・

```
$ aws accessanalyzer check-access-not-granted --policy-document file://ct.json \
--access resources="arn:aws:cloudtrail:us-east-1:123456789012:trail/MySensitiveTrail" \
--policy-type IDENTITY_POLICY --output json
```

許可されている場合

```
{
  "result": "FAIL",
  "message": "The policy document grants access to perform one or more of the listed actions or resources.",
  "reasons": [
    {
      "description": "One or more of the listed actions or resources in the statement with index: 0.",
      "statementIndex": 0
    }
  ]
}
```

許可されていない場合

```
{
  "result": "PASS",
  "message": "The policy document does not grant access to perform the listed actions or resources."
}
```

CheckNoPublicAccess – パブリックアクセス

機密情報が保存されているなど、外部に公開したくないリソースが意図せず公開されるリスクを低減
Amazon SQS でパブリックアクセスが許可されていないか調べるには・・・

```
$ aws accessanalyzer check-no-public-access --policy-document file://resource.json \ --resource-type AWS::SQS::Queue --output json
```

許可されている場合

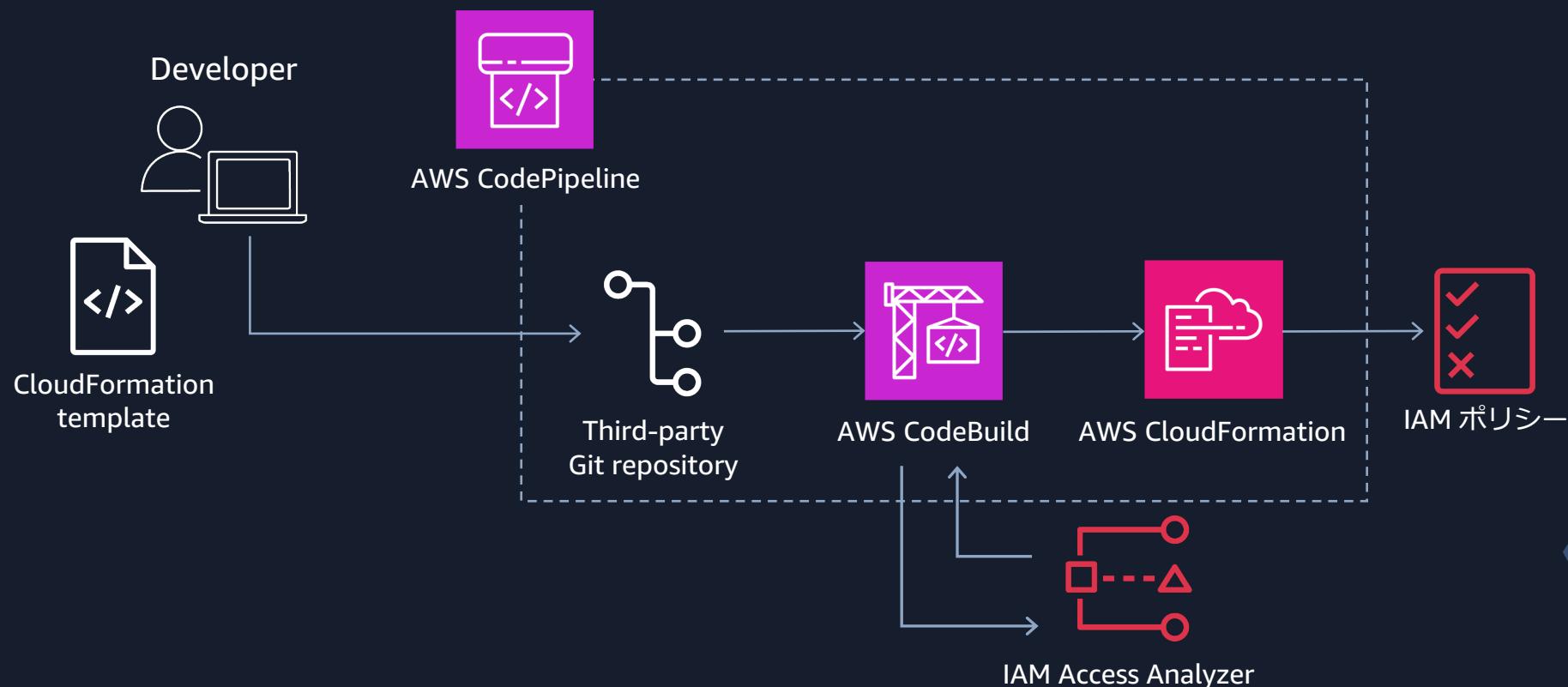
```
{  
  "result": "FAIL",  
  "message": "The resource policy grants public access for the given resource type.",  
  "reasons": [  
    {  
      "description": "Public access granted in the following statement with sid: SqsResourcePolicy.",  
      "statementIndex": 0,  
      "statementId": "SqsResourcePolicy"  
    }  
  ]  
}
```

許可されていない場合

```
{  
  "result": "PASS",  
  "message": "The resource policy does not grant public access for the given resource type."  
}
```

カスタムポリシーチェックの活用イメージ

CI/CD パイプラインにカスタムポリシーチェックを組み込むことで、意図しない IAM ポリシーが AWS 環境にデプロイされるのを防ぐことが可能



Third-party Git repository に IAM ポリシーを作成する AWS CloudFormation テンプレートがプッシュされるとパイプラインが開始され、AWS CodeBuild にてカスタムポリシーチェックを実行し、問題がなければリソースがデプロイされる

<https://github.com/awslabs/aws-cloudformation-iam-policy-validator>

<https://aws.amazon.com/blogs/security/introducing-iam-access-analyzer-custom-policy-checks/>

AWA IAM Access Analyzer の料金

AWS IAM Access Analyzer の料金

無料でご利用いただける機能

- 外部アクセスアナライザーによる分析
- AWS CloudTrail ログを用いたアクティビティに基づく IAM ポリシー生成
- ポリシー文法やベストプラクティスに関するポリシーチェック

有料でご利用いただける機能

- 未使用アクセスアナライザーによる分析
 - 0.20 USD – 1 ヶ月あたりに分析された IAM ロールとユーザー数 ※ 東京リージョン
 - カスタムポリシーチェック
 - 0.0020 USD – 1 ヶ月あたりの API 呼び出し数 ※ 東京リージョン

<https://aws.amazon.com/jp/iam/access-analyzer/pricing/>



まとめ

- AWS IAM Access Analyzer は、セキュリティベースラインを構築する上で重要なアクセス権限管理を効率化するツール
- AWS IAM のセキュリティベストプラクティスを実現するために、AWS IAM Access Analyzer は有用
- AWS IAM Access Analyzer では多くの機能を無料で利用可能なので、まずは始めてみましょう！

Thank you!

