AWS Black Belt Online Seminar

AWS Identity and Access Management (IAM) Access Analyzer

田中　崚

Cloud Support Engineer

2024/12

自己紹介

田中　崚

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

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ましては、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

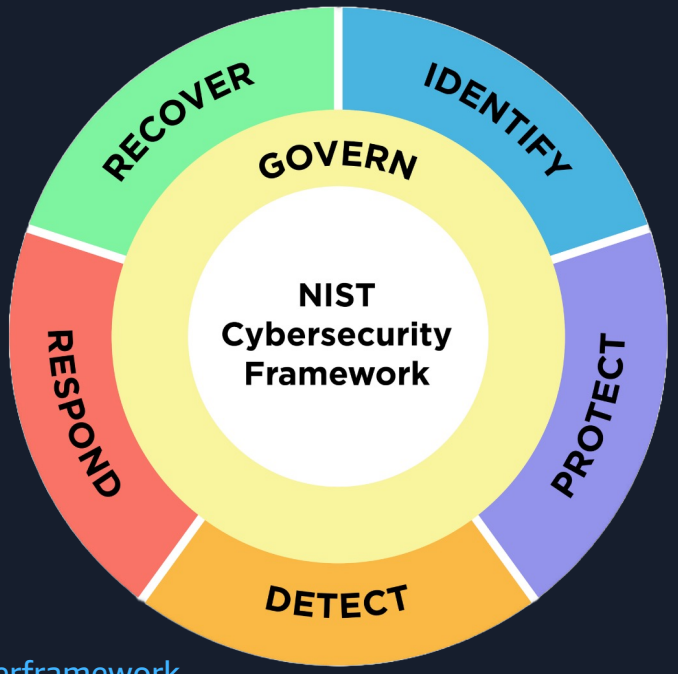
1. アクセス権限管理の重要性・課題
2. AWS IAM Access Analyzer の概要
3. AWS IAM Access Analyzer の各種機能
4. AWS IAM Access Analyzer の料金

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

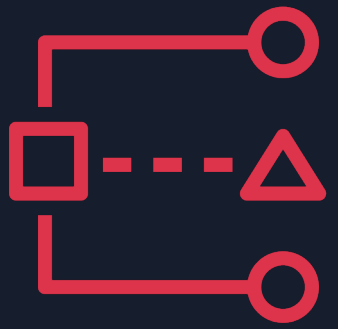
組織拡大により管理対象のアカウント・リソースが増え、運用負荷が増大する

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**	• 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 ポリシーチェックでポリシーを検証 • 外部アクセスが許可されたリソースを検出
 **可視化**	• 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**	• 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**	• AWS Security Hub と統合し、検出結果を一元管理 • 使われて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

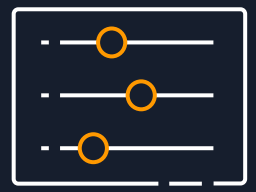
AWS IAM のセキュリティベストプラクティス抜粋

- 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

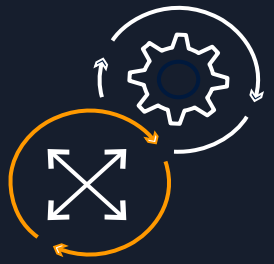
AWA IAM Access Analyzer の各種機能

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



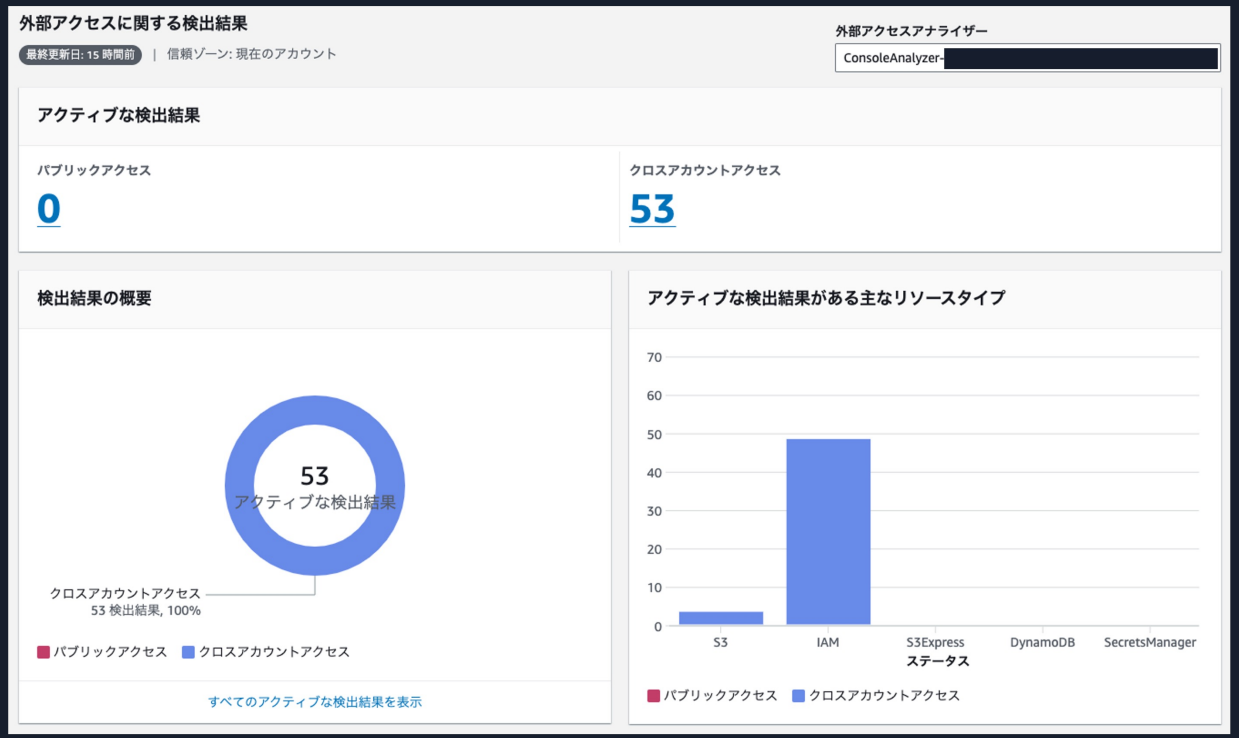
ポリシー生成

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

未使用アクセスアナライザー

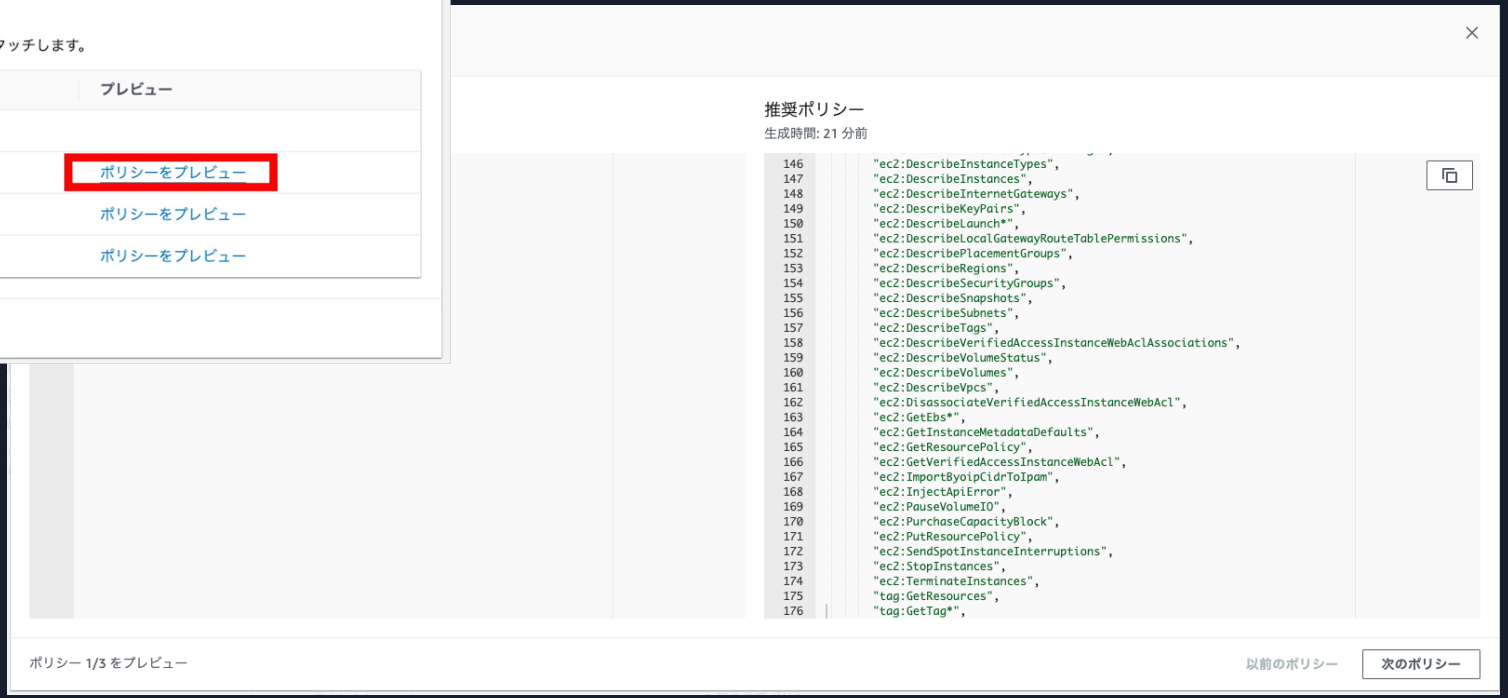
- IAM ロールと IAM ユーザーを継続的にモニタリングし、追跡期間中に使用されていないアクセス許可・認証情報を特定
- IAM Access Analyzer が自動でモニタリングを行うため、セキュリティ担当者がこれまで実施していたタスクを肩代わりし、運用コスト削減が可能
- デフォルトの追跡期間は 90 日間
(1～180 日間で設定可能)
- アカウントまたは組織レベルで
未使用アクセスアナライザーを有効化

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

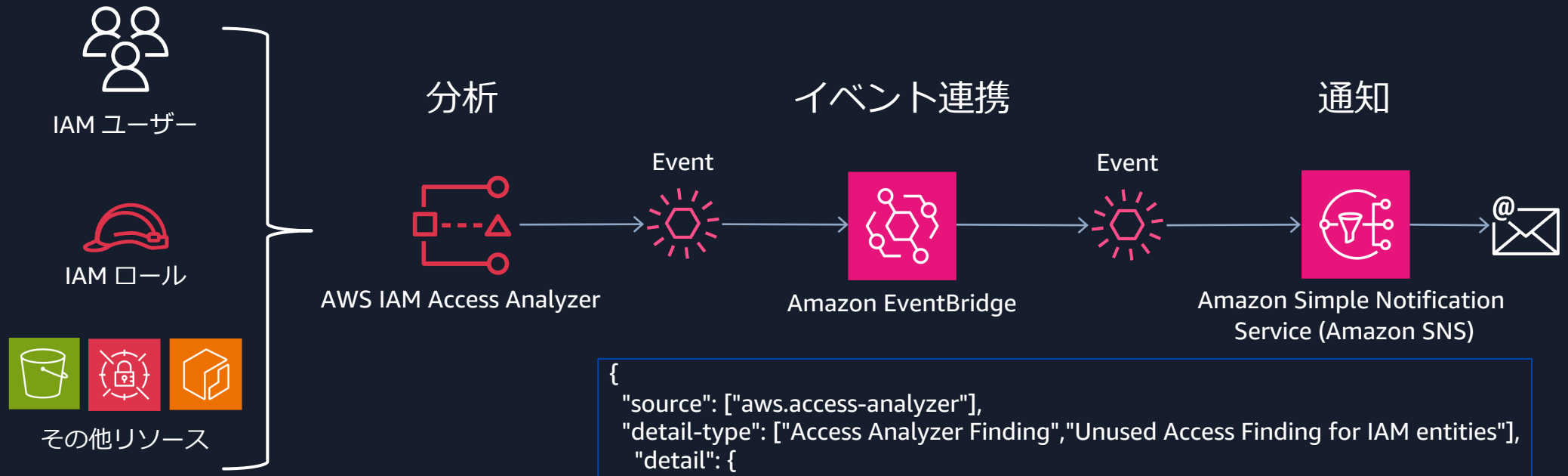
未使用アクセスアナライザーの検出結果への具体的な修復手順を提供

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



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

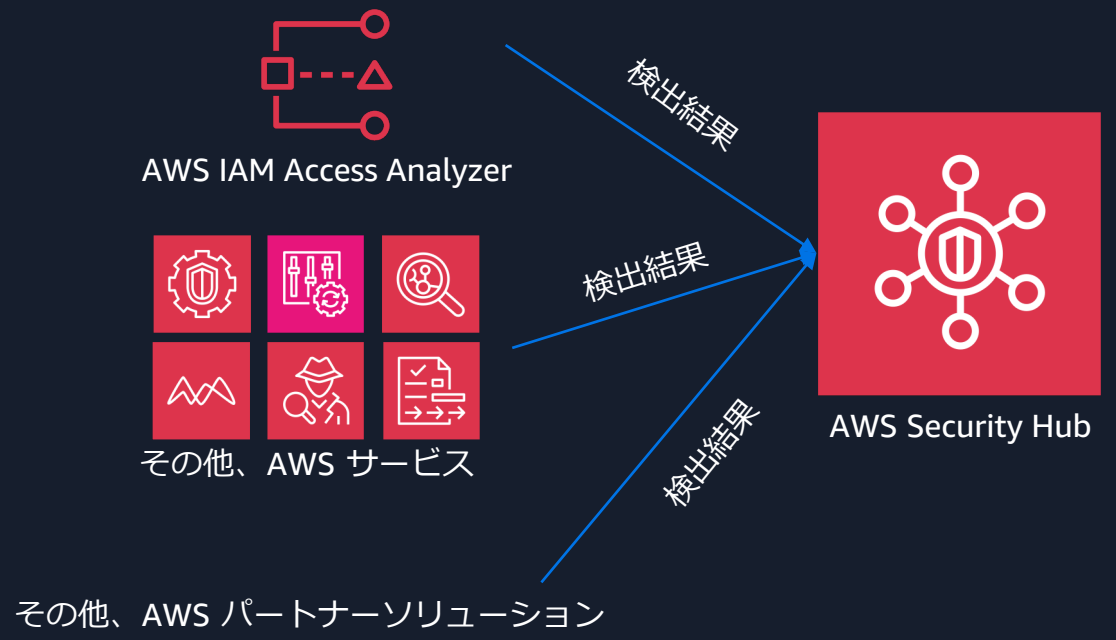



```
{
  "source": ["aws.access-analyzer"],
  "detail-type": ["Access Analyzer Finding","Unused Access Finding for IAM entities"],
    "detail": {
    "isDeleted": [
      false
    ]
  }
}
```

Amazon EventBridge ルールのイベントパターン

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

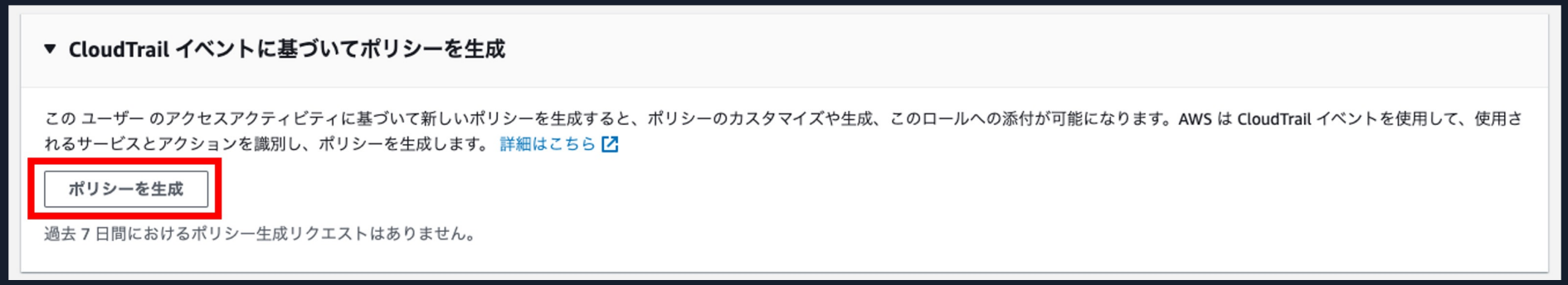
ただし、必ずしも完全な最小権限のポリシーを生成するわけではない

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 イベントを分析する期間の指定
（最長で 90 日間の範囲を指定可能）

分析に使用するサービスロールを指定

ポリシー生成機能について知っておくべきこと

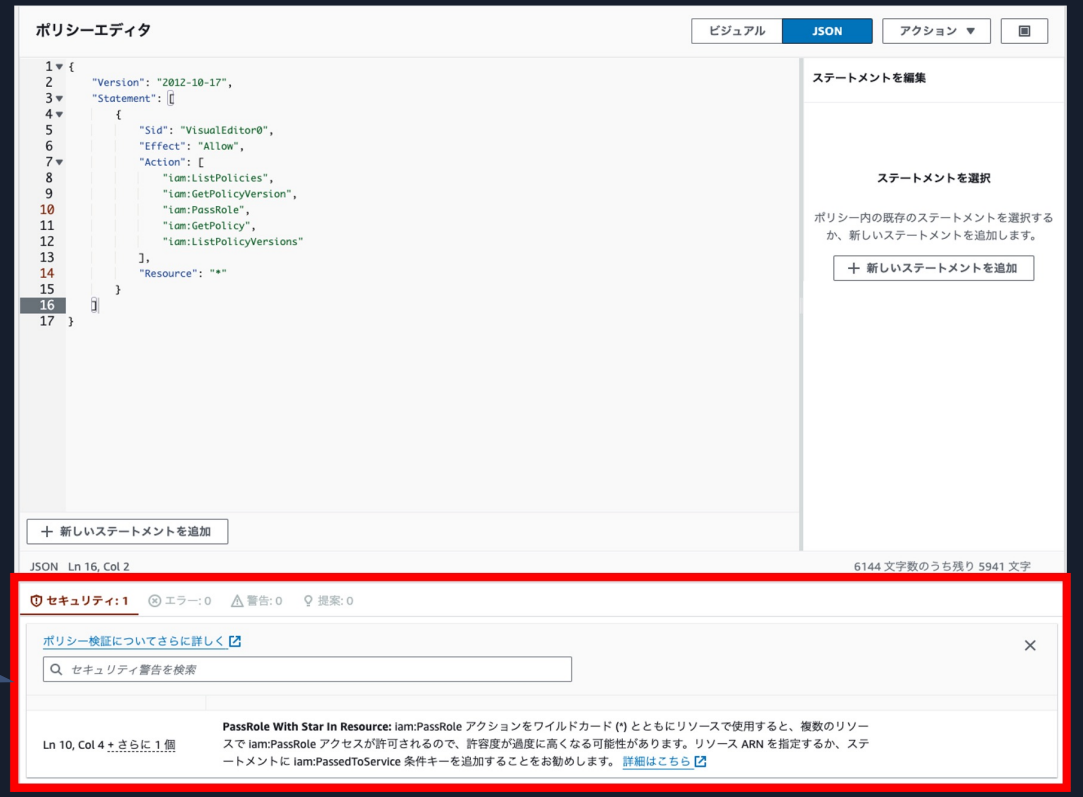
- AWS CloudTrail 証跡の有効化が必要
- Amazon S3 データイベントなどのデータイベントについては分析しない
- iam:PassRole アクションについては AWS CloudTrail ログに記録されないため、生成されたポリシーには含まれない
- 分析期間を短くすることで、ポリシー生成時間の短縮が可能
- 生成されたポリシーは、IAM コンソールにて最大 7 日間確認可能

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

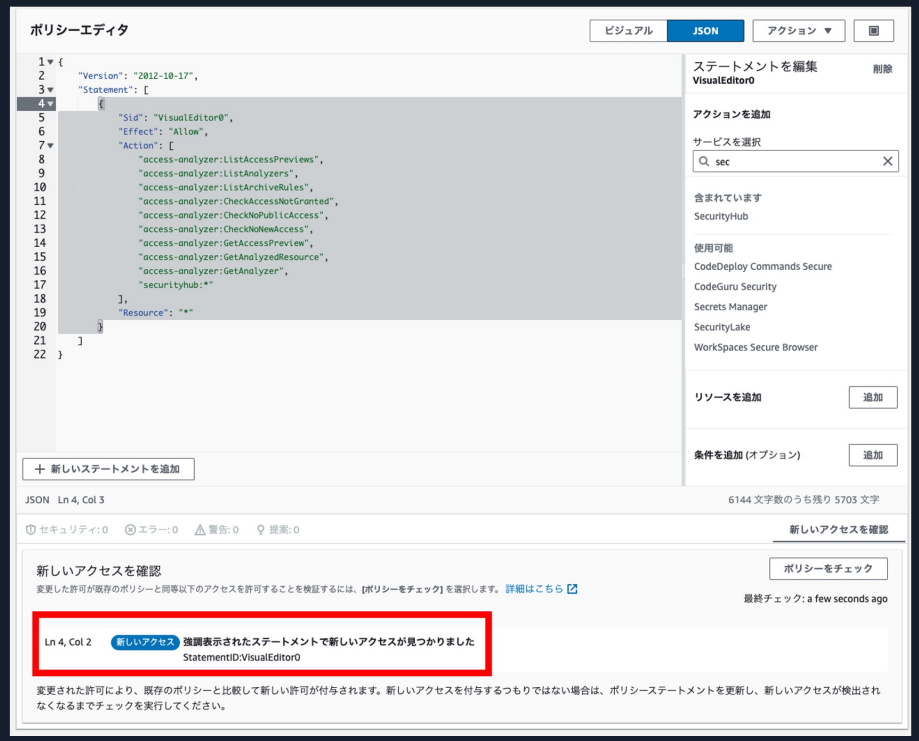
入力
ポリシーとリソースタイプ

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を調べたい場合は・・・

```
$ 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

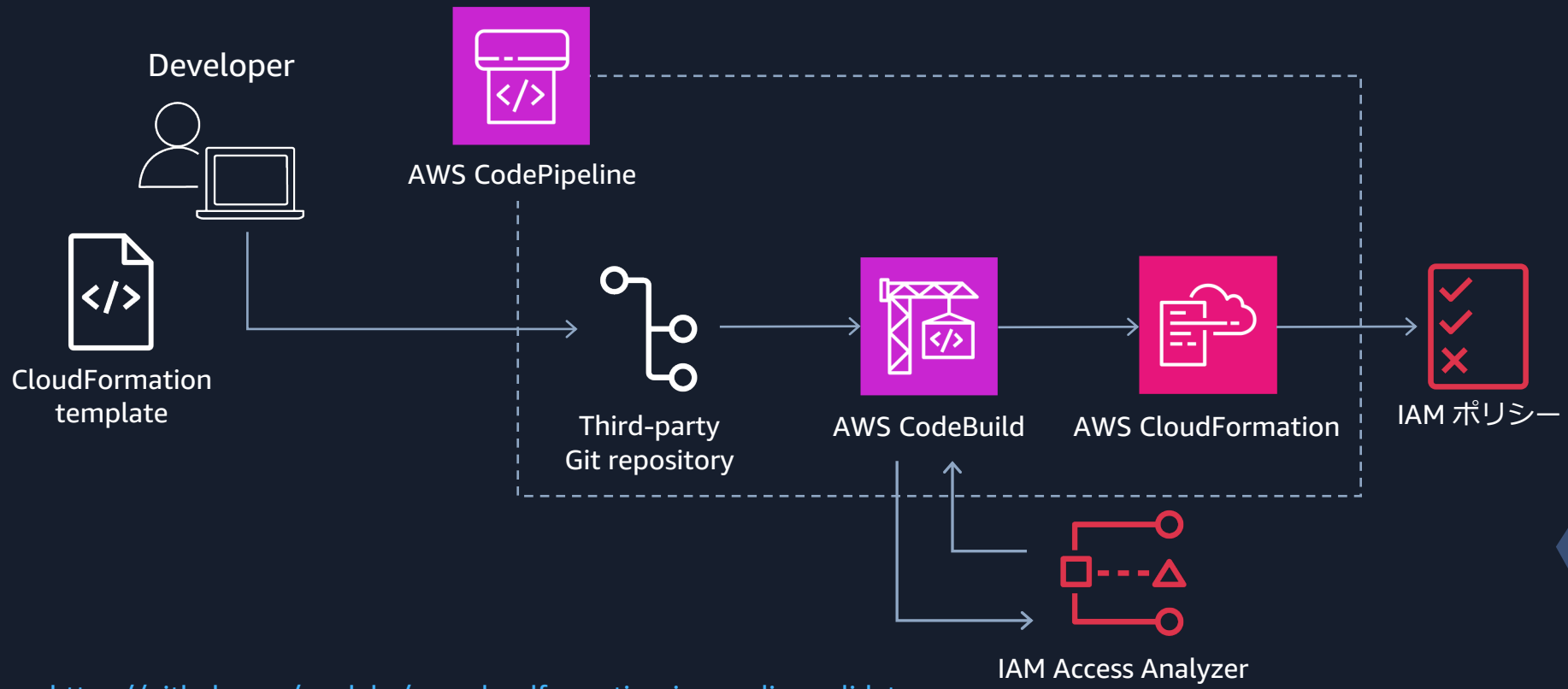

```
{
    "result": "FAIL",
    "message": "The resource policy grants public access for the given resource type.",
    "reasons": [
        {
            "description": "Public access granted in the following statement with sid: SqsResourcePolicy.",
            "statementIndex": 0,
            "statementId":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