[AWS Black Belt Online Seminar]

AWS CloudTrail

サービスカットシリーズ

Security Solutions Architect
中島 智広
2021/01/19

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

過去資料
https://amzn.to/JPArchive

自己紹介

中島　智広（Tomohiro Nakashima）

AWS Security Solutions Architect

お客様のセキュリティの取り組みを
AWSアーキテクチャの視点からご支援

好きなAWSサービス

セキュリティ関連サービス全般

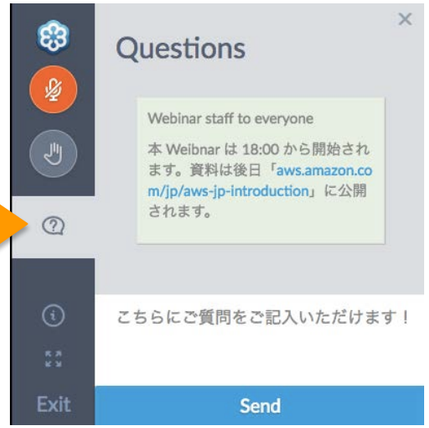
AWS Black Belt Online Seminar とは

「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2021年1月19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には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.

本セミナーの概要

AWS CloudTrail は、AWS アカウントのガバナンス、コンプライアンス、運用監査、リスク監査を行うためのサービスです。

AWS CloudTrail を使用すると、AWS インフラストラクチャ全体でアカウントアクティビティをログに記録し、継続的にモニタリングし、保持できます。

本セミナーでは、AWS CloudTrailの基礎と、その活用方法について解説します。

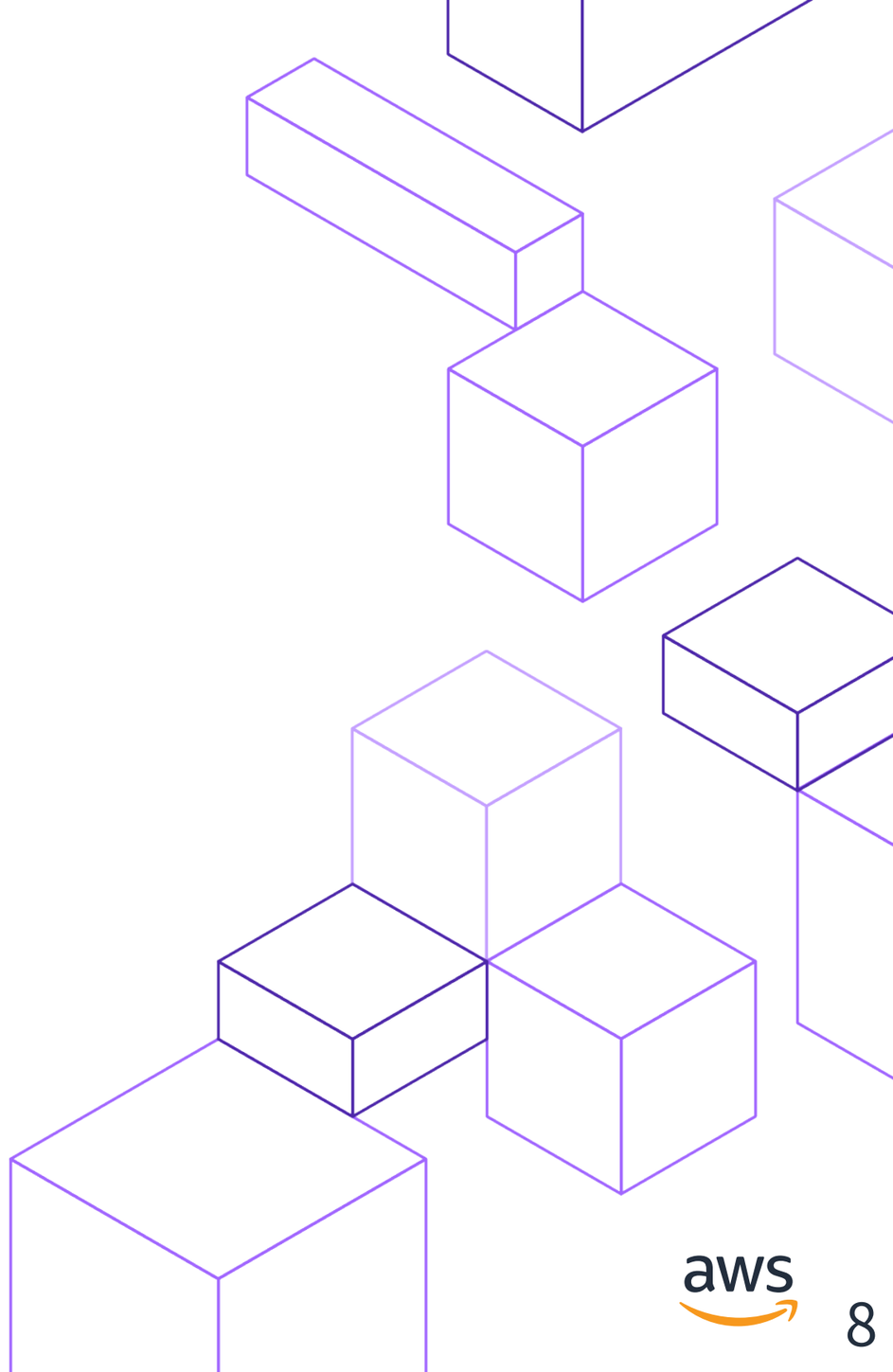
はじめに/Key Takeaways

- まずベースラインとして「ログの保全と脅威検知の有効化」から始める
    - すべてのAWSリージョンでAWS CloudTrailの証跡の有効化
    - Amazon GuradDutyの有効化
- 次に「AWS CloudTrail でのセキュリティのベストプラクティス」を取り込む
- さらに「調査、モニタリング、脅威検出」の体制を整備する

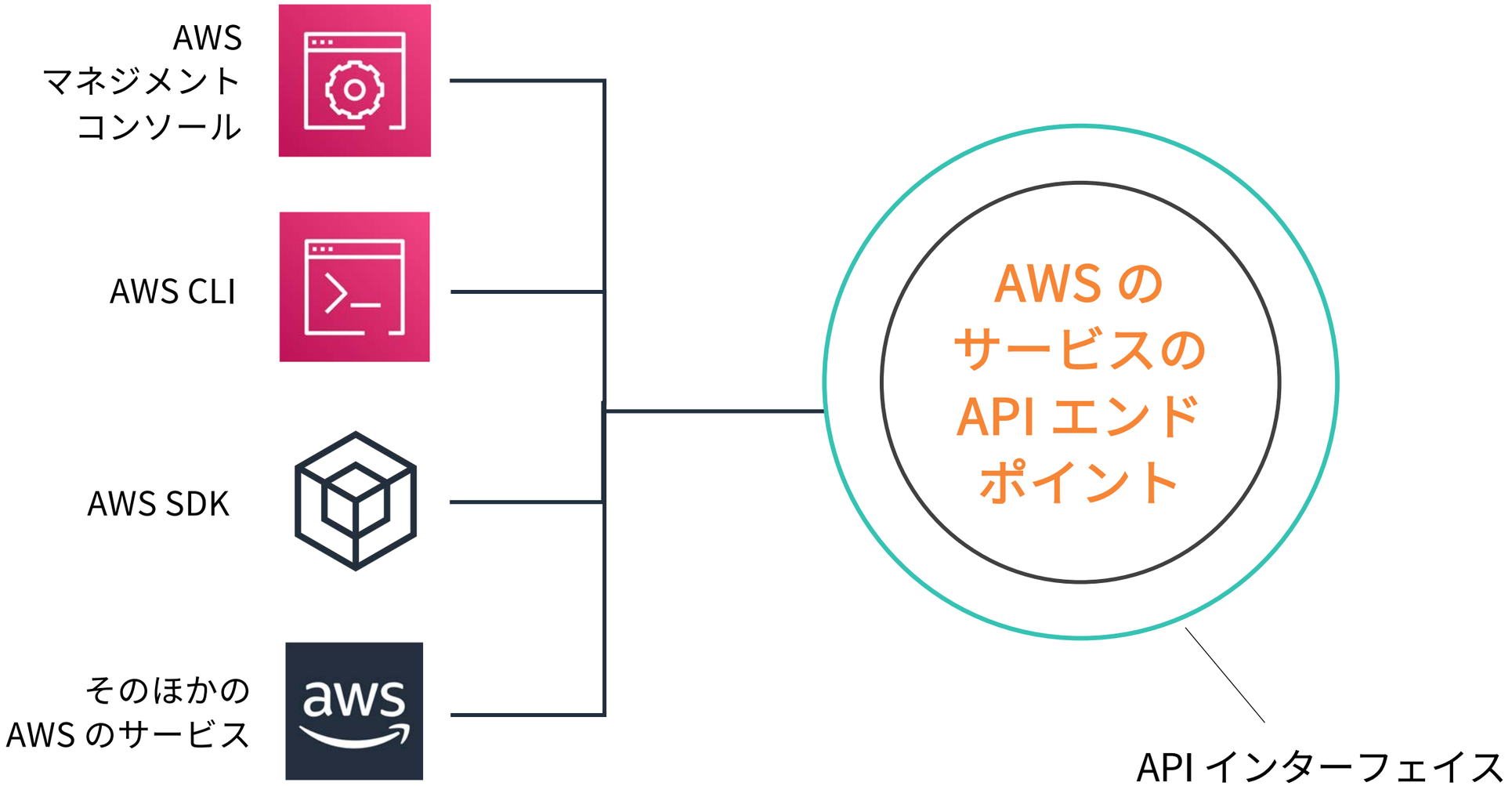
Agenda

1. AWS CloudTrailの基本
2. 証跡ログの保存、保護
3. コスト最適化
4. 証跡ログの調査
5. 証跡ログのモニタリング、脅威検出
6. ふりかえり

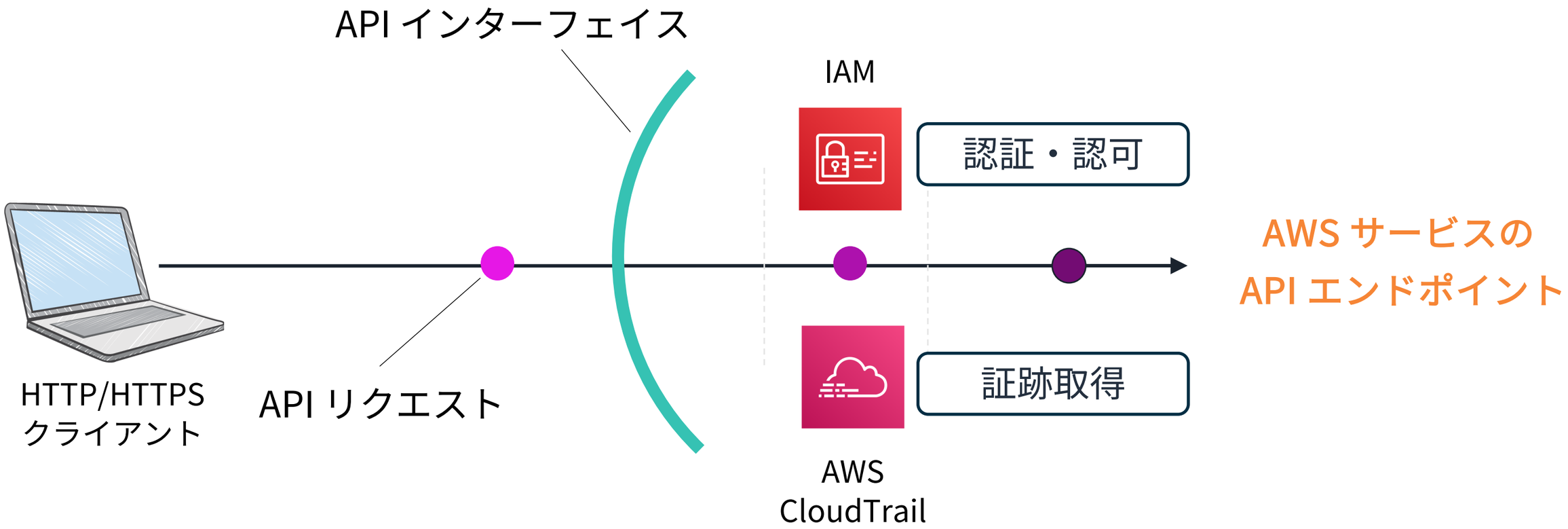
AWS CloudTrailの基本



AWSの操作はAPIを通じて提供される



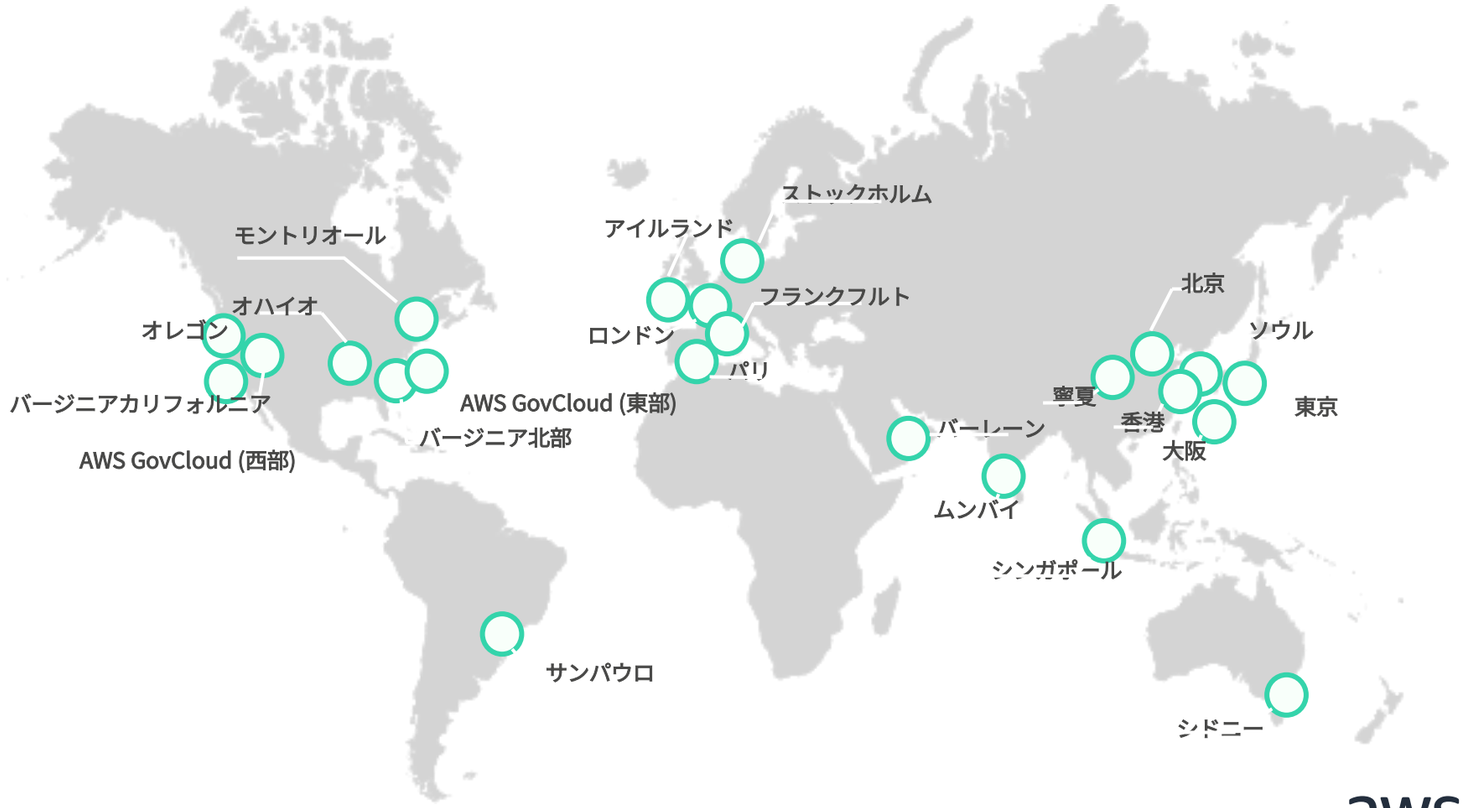
APIリクエストの認証認可、証跡取得



AWS CloudTrailはリージョン毎のサービス

証跡の保存はリージョン毎に有効化が必要（ただし一括有効化オプション有り）

AWS CloudTrail のリージョン別エンドポイントの例



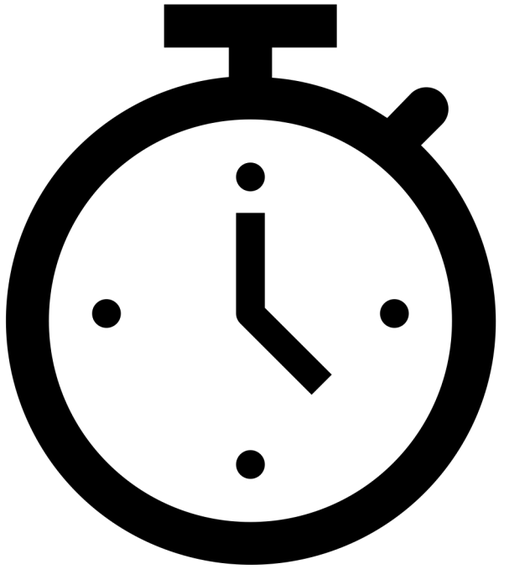
AWS CloudTrailが保存する証跡

- AWS CloudTrailがサポートする全てのサービスのAPIイベント
- API リクエストによって直接トリガーされない一部のイベント
    - AWS マネジメントコンソールへのログイン試行、
      AWS フォーラム、および AWS サポートセンター
    - すべての IAM ユーザーのサインインの試行
    - AWS アカウントのルートユーザーの成功したサインイン試行
      など

CloudTrail サポートされるサービスと統合
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-aws-service-specific-topics.html
CloudTrail でサポートされていないサービス
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-unsupported-aws-services.html

AWS CloudTrail 証跡ログの出力タイミング

- ログファイルは1 時間に複数回、約 5 分ごとに発行
- アカウントアクティビティは通常 15 分以内に配信
- デフォルトでは、ログファイルは永続的に保存
- インサイトイベント（後述）は
  異常なアクティビティから通常 30 分以内にバケットに配信



AWS CloudTrail ”の“セキュリティ＆コンプライアンス

複数の コンプライアンスプログラムの一環として、AWS CloudTrail のセキュリティとコンプライアンスの評価が行われています

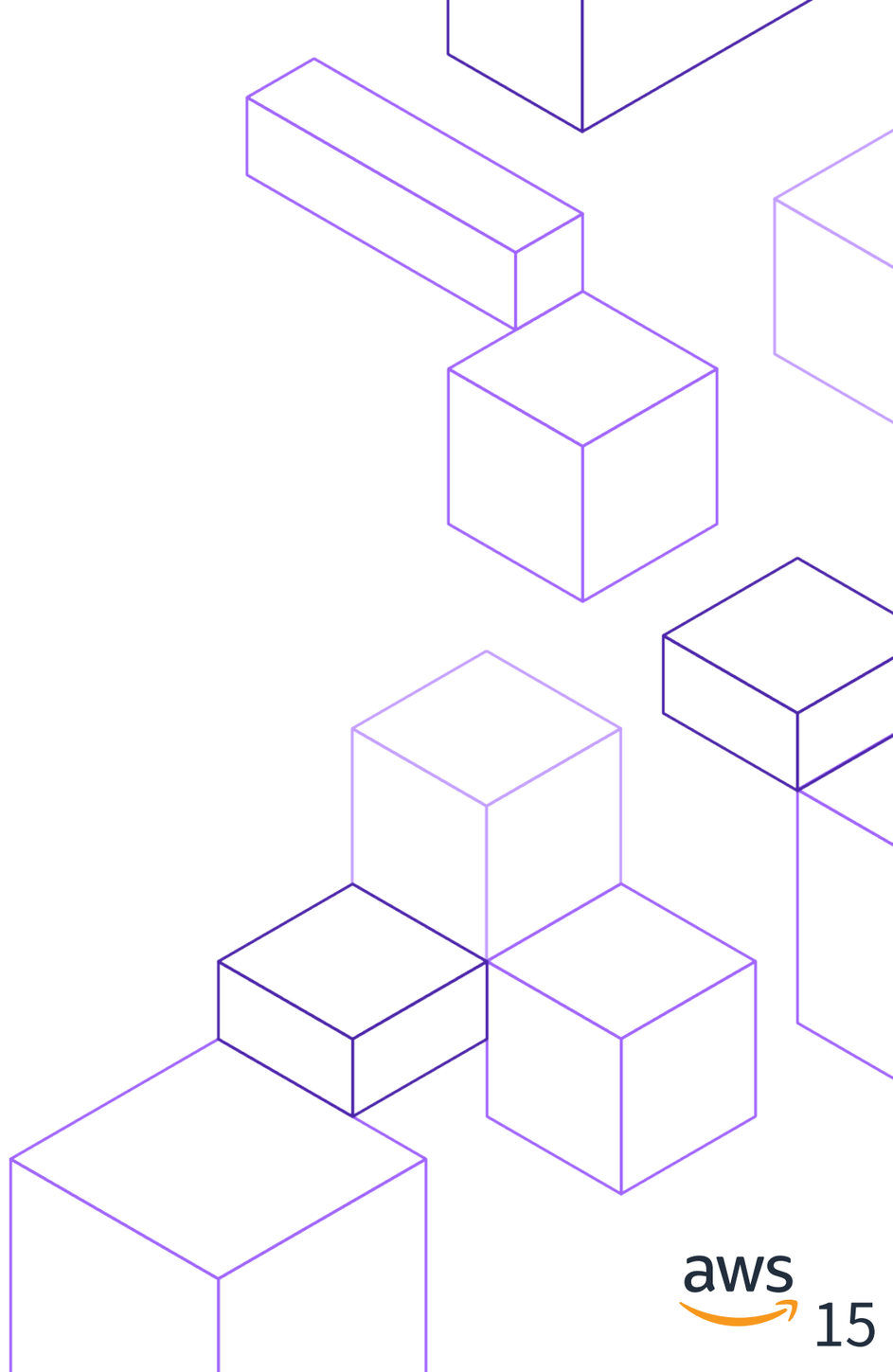
FedRAMP


など

すべてのプログラムを確認するには・・・

コンプライアンスプログラムによる AWS 対象範囲内のサービス
https://aws.amazon.com/jp/compliance/programs/

証跡ログの保存、保護



AWS CloudTrail 証跡の作成

証跡ログ 3つのイベント

管理イベント

コントロールプレーン
オペレーション

AWS アカウントのリソースで実行される管理オペレーション

例）
- ログ記録の設定
- ネットワーク構成変更
- コンフィグの参照
- デバイスの登録

データイベント

データプレーン
オペレーション

AWSアカウントのリソース上またはリソース内で実行されたリソースオペレーション

例）
- Amazon S3 オブジェクトレベルの API アクティビティ (GetObject、DeleteObject、PutObject APIなど)
- AWS Lambda 関数の実行アクティビティ (Invoke API)

インサイトイベント

読み取り専用ではない管理イベントの異常な傾向

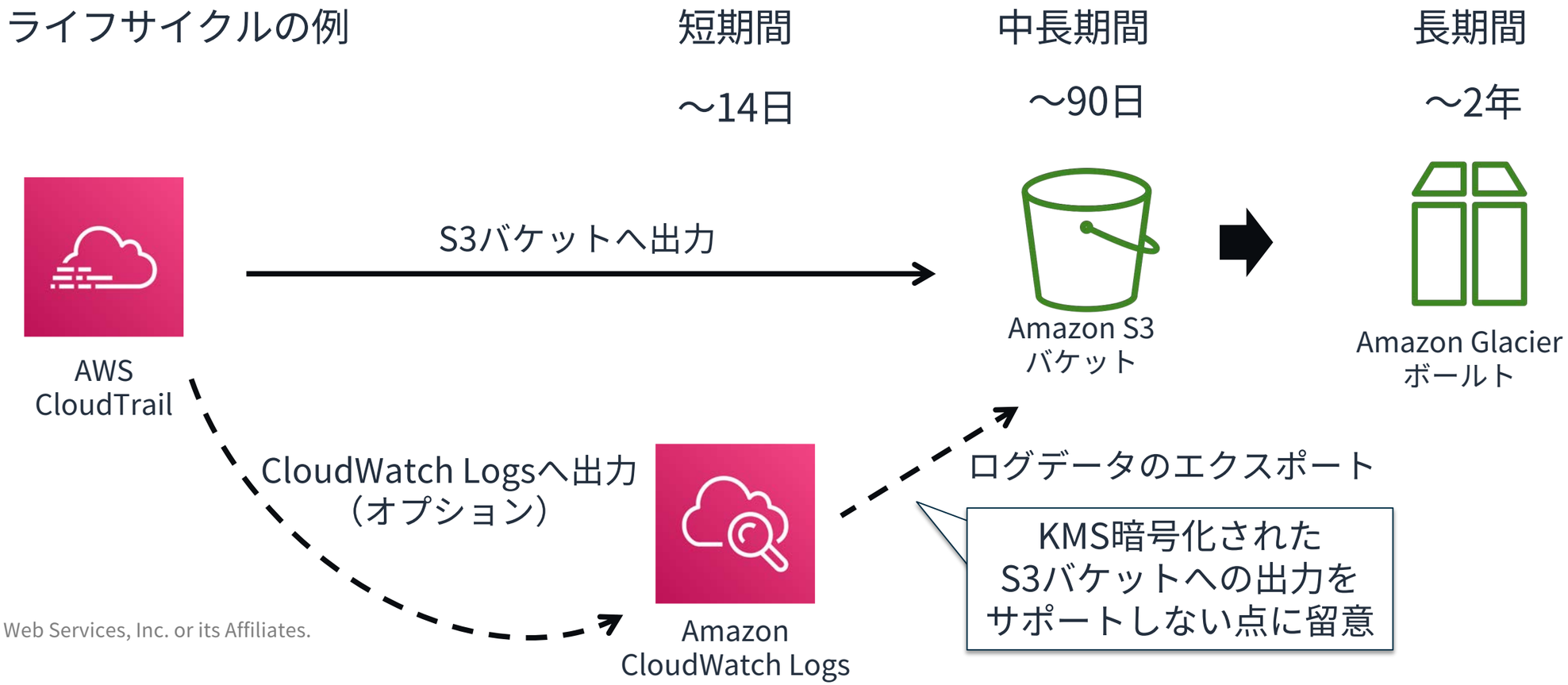
管理イベントのAPI コールボリュームの計測値が、通常のパターンから外れた場合に生成

例）
- リソースプロビジョニングの急上昇
- IAMアクションのバースト
- 定期的なメンテナンスアクティビティのギャップ

証跡ログの出力先とライフサイクル

Amazon S3 バケットを基本に、Amazon CloudWatch Logsへの出力もサポート

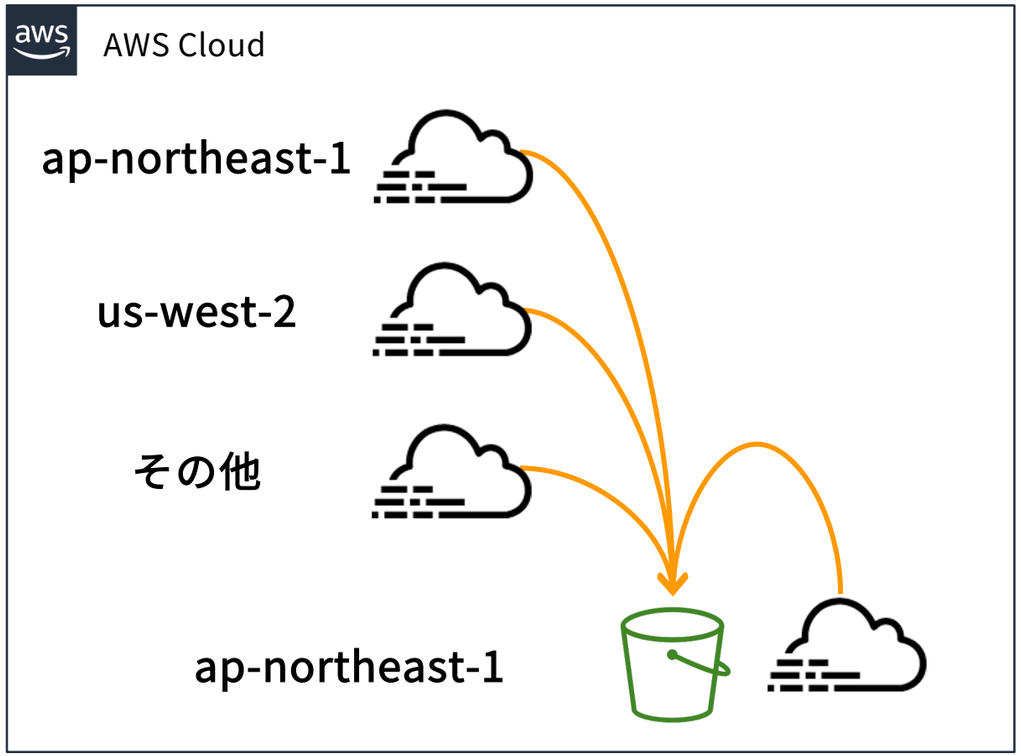
要件に応じた証跡ログのモニタリング、アーカイブ、バックアップを構成可能



証跡ログの集約

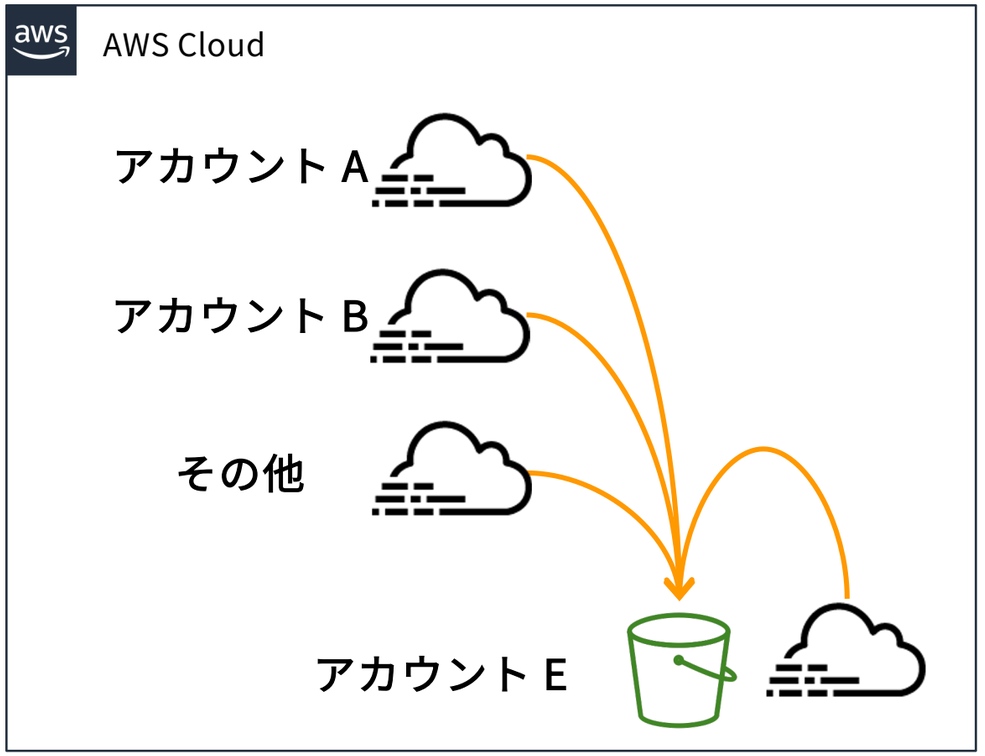
リージョンやアカウント毎の証跡ログを集約することで運用を容易にする

すべてのリージョンのログを
1 つのリージョンへ



アカウント A

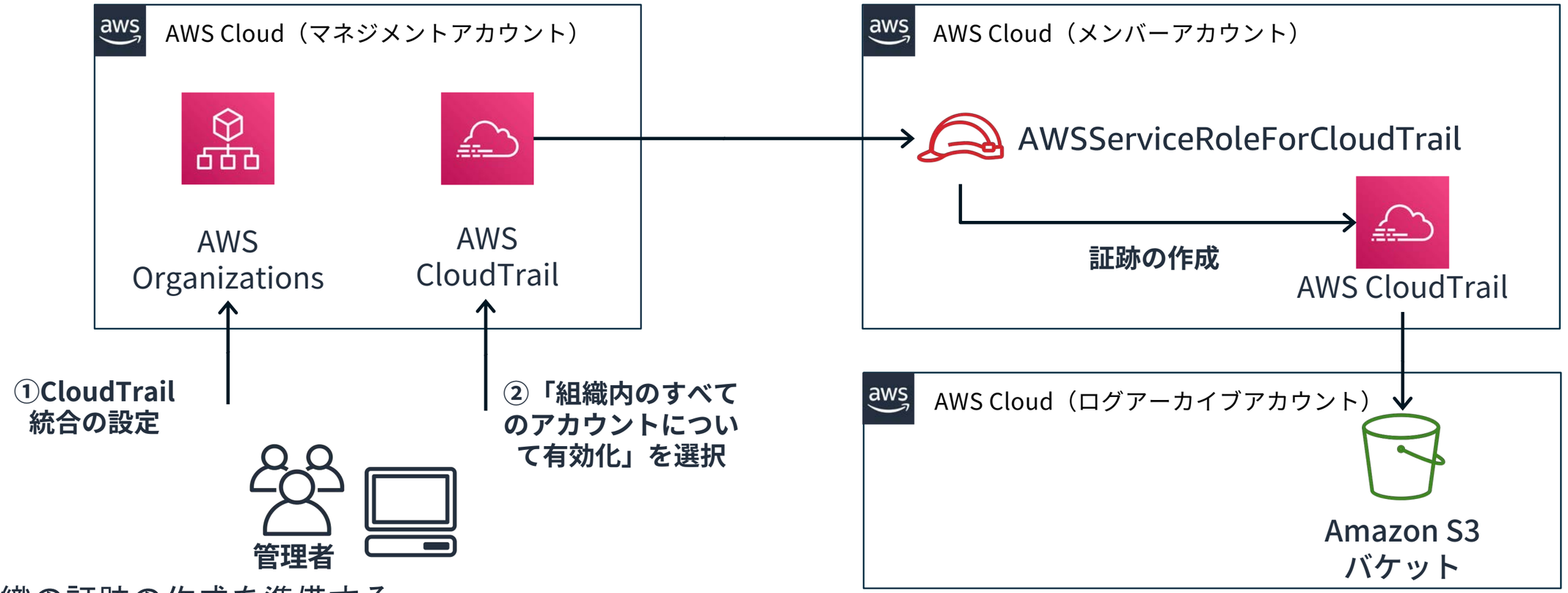
すべてのアカウントのログを
1 つのアカウントへ



ap-northeast-1

AWS Organizationsとの連携

組織毎に統合された証跡の作成を強制することが可能



組織の証跡の作成を準備する
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/creating-an-organizational-trail-prepare.html

証跡ログ 保護の重要性

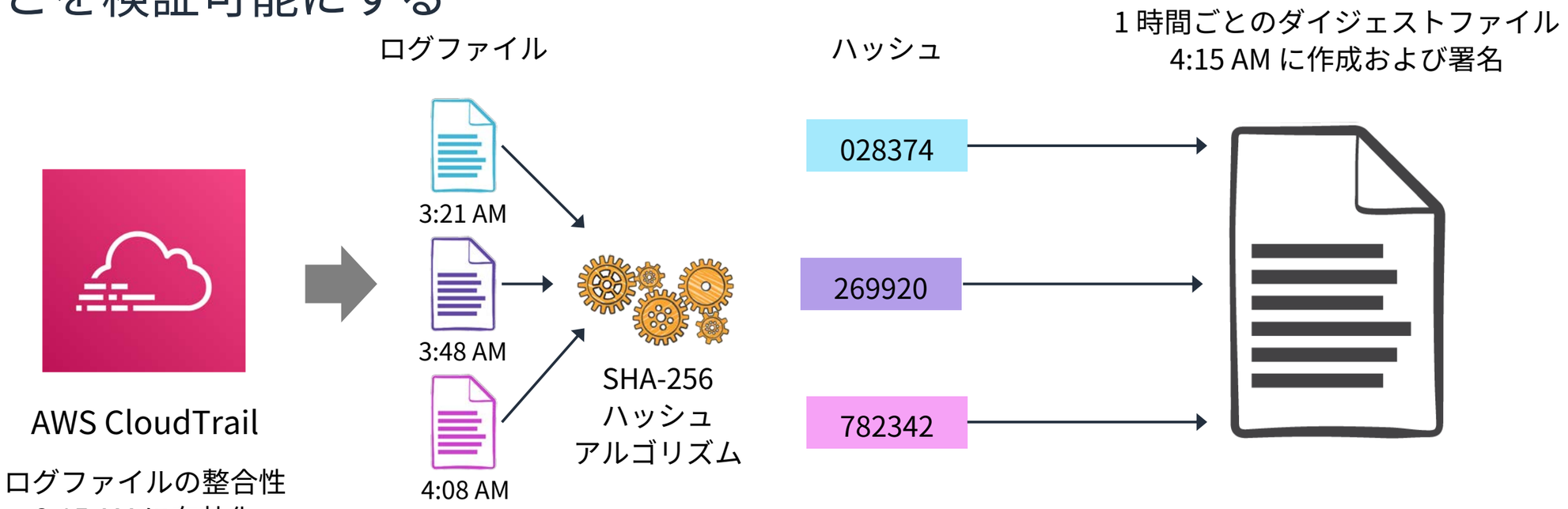
- コンプライアンス要件
    - データの耐久性、改ざん検知
    - “Write Once Read Many” (WORM)モデル など
- 係争時の説明、証拠能力の維持
    - 証跡が真正なものであることを説明するのはお客様の責任
    - 証拠裁判主義の下の自由心証主義（日本国の場合）

刑事訴訟法第318条
証拠の証明力は、裁判官の自由な判断に委ねる。

民事訴訟法第247条
裁判所は、判決をするに当たり、口頭弁論の全趣旨及び証拠調べの結果をしん酌して、自由な心証により、事実についての主張を採用すべきか否かを判断する

証跡ログの保護：AWS CloudTrail ログファイル整合性検証

電子署名のメカニズムにより証跡ログがAWS CloudTrail以外によって変更されていないことを検証可能にする



AWS CLIによる検証実行例

```
$ aws cloudtrail validate-logs --trail-arn arn:aws:cloudtrail:ap-northeast-1:123456789012:trail/example-trail-name --start-time 2021-01-01T00:00:00Z --end-time 2021-01-18T23:59:59Z
```

証跡ログの保護：Amazon S3/Glacierの保護設定

機能	概要	特記事項
KMS暗号化	鍵へのアクセス権を持たないユーザーや第三者からの意図しない参照を予防	バケットにデフォルト暗号化を設定しすべてのオブジェクトを暗号化
バージョニング	オブジェクトの更新ごとに新しいバージョンを作成、ユーザーの意図しない削除操作から保護し、削除されたオブジェクトの取得を容易にする	ライフサイクルポリシーを使用してコストをコントロール
MFA Delete	オブジェクトの削除にMFA認証を要求	バージョニングの有効化が必要
オブジェクトロック(S3) ボールトロック(Glacier)	“Write Once Read Many” (WORM)モデルによる保護	保護期間中にデータを削除したい場合は、AWSアカウントの解約によってデータの破棄が可能
レプリケーション	Amazon S3 バケット間でオブジェクトを自動で非同期的にコピー	Amazon S3の仕様に準ずる(※)

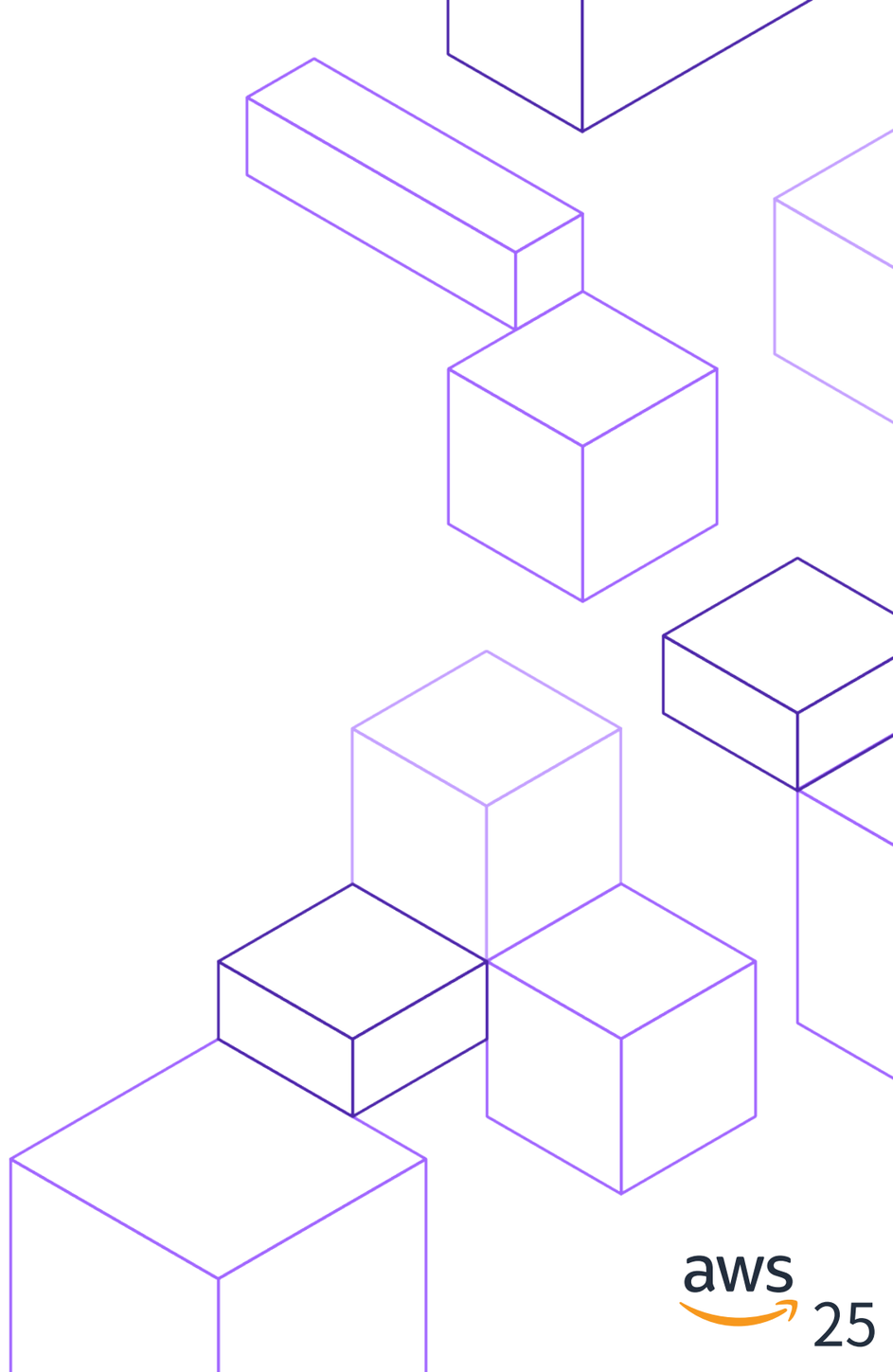
※ Amazon S3 レプリケーション
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/replication.html
Amazon S3 がレプリケートするもの
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/replication-what-is-isnot-replicated.html

証跡ログの保護を確実にするAWS Config Rules

AWS CloudTrailに関連するAWSマネージドルールを要件にあわせて有効化

機能	概要
cloudtrail-enabled	AWS アカウントで AWS CloudTrail が有効になっているかどうかを確認します。
cloud-trail-log-file-validation-enabled	AWS CloudTrail でログを含むダイジェストファイルを作成するかどうかを確認します。
cloud-trail-encryption-enabled	AWS CloudTrail がサーバー側の暗号化 (SSE) AWS Key Management Service (AWS KMS) カスタマーマスターキー (CMK) 暗号化を使用するよう設定されているかどうかを確認します。
cloudtrail-s3-dataevents-enabled	少なくとも 1 つの AWS CloudTrail 証跡がすべての S3 バケットの Amazon S3 データイベントをログ記録しているかどうかを確認します。
cloudtrail-security-trail-enabled	セキュリティのベストプラクティスで定義されている AWS CloudTrail 証跡が少なくとも 1 つあることを確認します。
multi-region-cloudtrail-enabled	マルチリージョン AWS CloudTrail が少なくとも 1 つあることを確認します。
cloud-trail-cloud-watch-logs-enabled	AWS CloudTrail 証跡がログを Amazon CloudWatch Logs に送信するように設定されているかどうかを確認します。

コスト最適化



コスト最適化の考え方

利用料金の仕組み

- 管理イベントの最初の配信のみ無料、2つめからは有料
- データイベント、インサイトイベントは、全ての配信が有料
- Amazon CloudWatchに配信した場合、Amazon CloudWatchの利用料が発生

すなわち、
配信する証跡を多く設定すると、同一のデータの出力であっても追加コストが発生

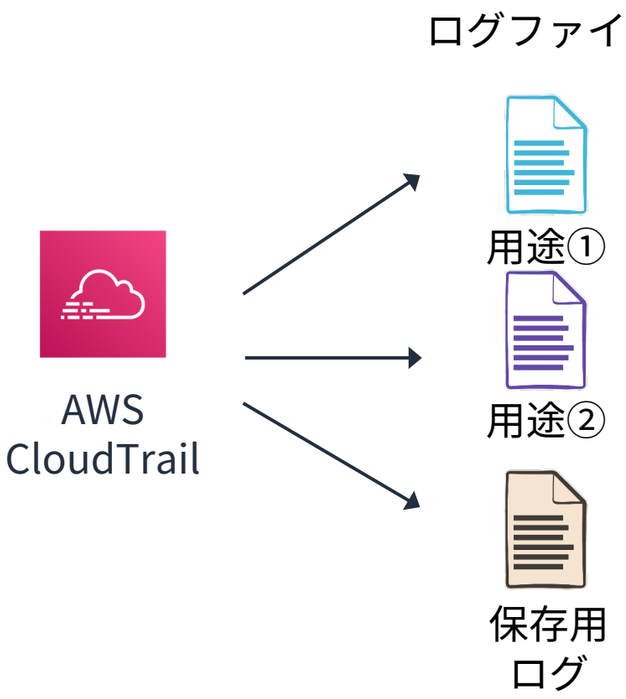
イベントセレクターやデザインパターンによってコストを最適化

イベントセレクター：データイベントログの選択的保存

注：選択的保存が出来るのはデータイベントのみ

デザインパターン

用途毎に証跡を設定するパターン

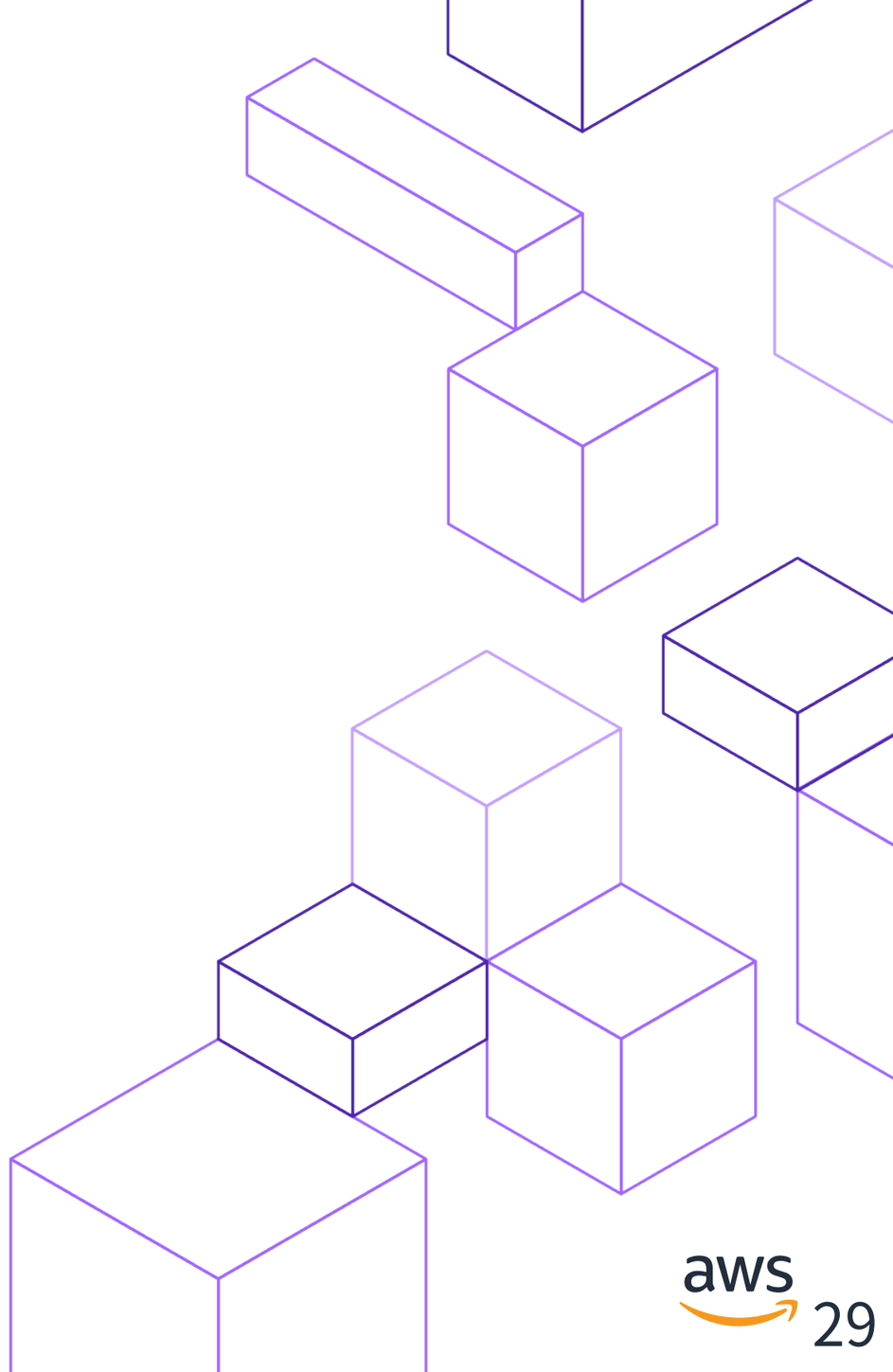


集約した証跡を用途毎にロードするパターン

AWS CloudTrailから出力する際の重複を少なくするとコストが節約できる

集約データを用途に応じてロードするのは柔軟性の高い一般的なアプローチ

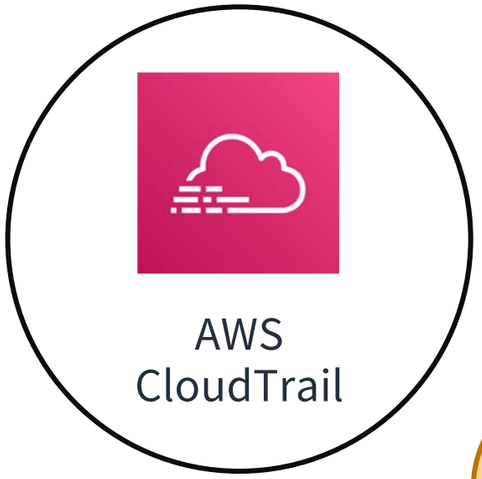
証跡ログの調査



証跡ログでわかること

誰が API コールを
実行したか

誰?



何?

どのような API コールで、
どのリソースが影響を受けたか

どこから API コールが実
行されたか

どこ?

いつ?

いつ API コールが実行されたか

証跡ログの例

誰がリクエストを行ったか

```
{
  "Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "EX_PRINCIPAL_ID",
      "arn":
"arn:aws:iam::123456789012:user/Alice",
      "accountId": "123456789012",
      "accessKeyId": "EXAMPLE_KEY_ID",
      "userName": "Alice"
    },
```

いつ、どこから

```
"eventTime": "2018-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
```

何がリクエストされたか

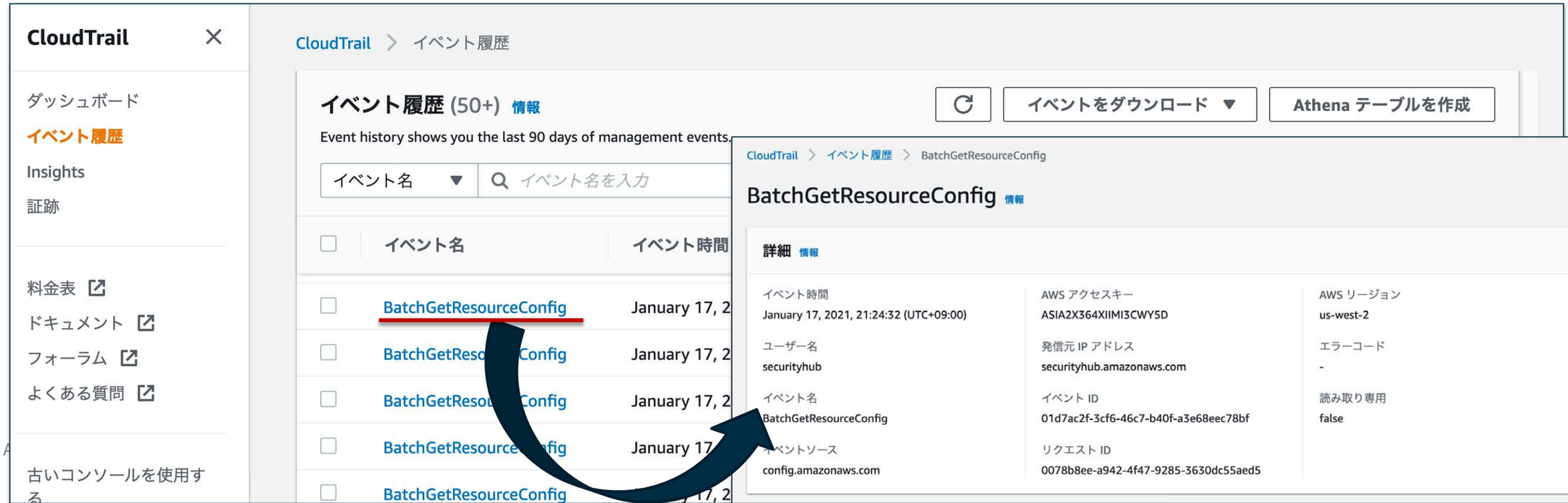
```
"requestParameters": {
    "instancesSet": {
      "items": [{
        "instanceId": "i-ebeaf9e2"
      }]
    },
    "force": false
  },
```

どんな応答があったか

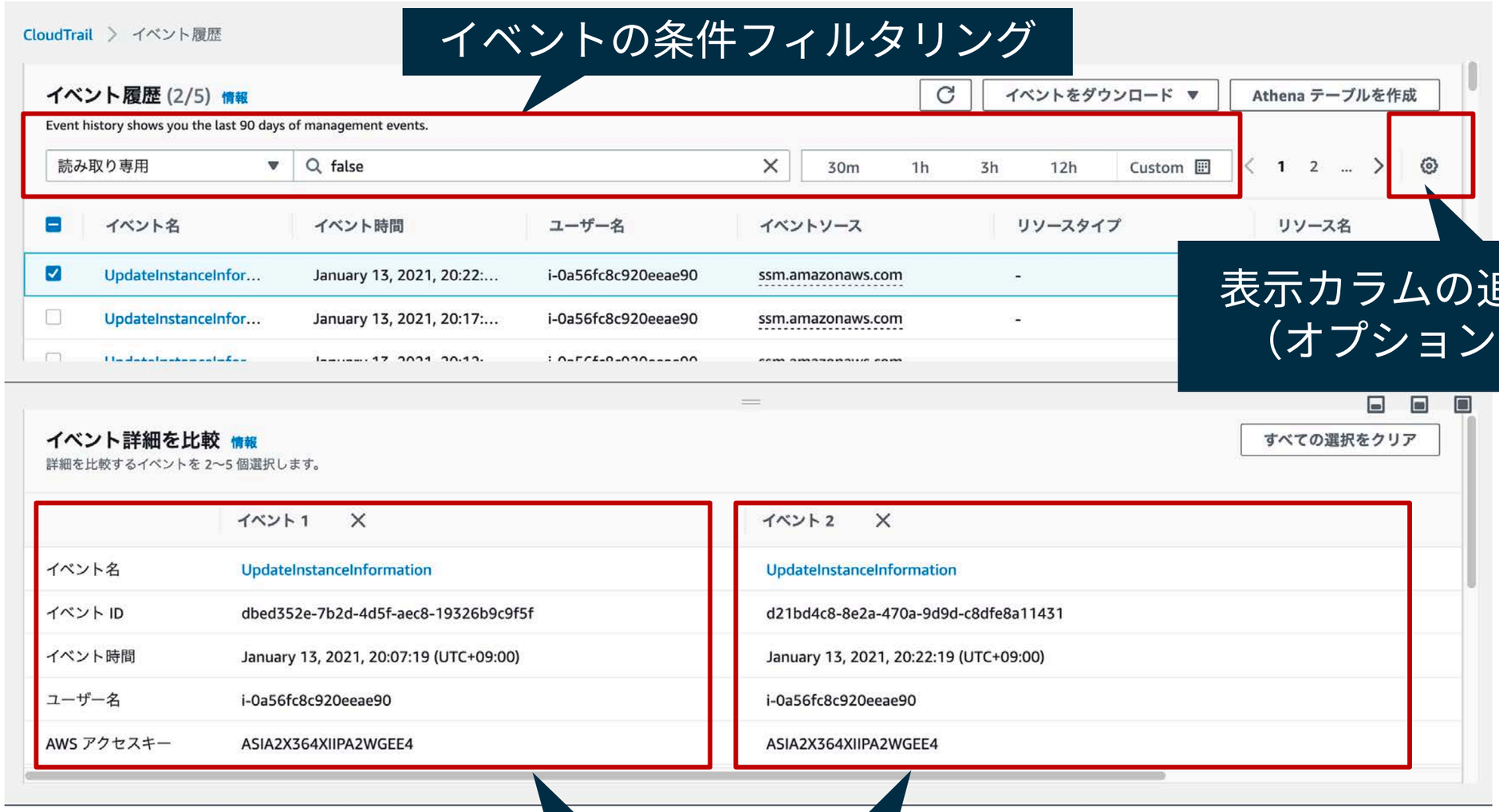
```
"responseElements": {
  "instancesSet": {
    "items": [{
      "instanceId": "i-ebeaf9e2",
      "currentState": {
        "code": 64,
        "name": "stopping"
      },
      "previousState": {
        "code": 16,
        "name": "running"
      }
```

AWS Cloud Trail イベント履歴

- 過去 90 日間のイベントを無料で参照、ダウンロード可能（管理イベントのみ）
- 単一の属性キーに対するフィルタリング機能を有する
- クエリなどを用いた高度な検索、調査機能はない



AWS Cloud Trail イベント履歴（マネジメントコンソール）



AWS Cloud Trail イベント履歴（AWS CLI / SDK）

属性キーでフィルタリングする

```
$ aws cloudtrail lookup-events --lookup-attributes AttributeKey=<attribute>,AttributeValue=<string>
```

タイムスタンプでフィルタリングする

```
$ aws cloudtrail lookup-events --start-time <timestamp> --end-time <timestamp>
```

フィルタリング条件の入力にJSONを利用する

```
$ aws cloudtrail lookup-events --cli-input-json file://LookupEvents.txt
```

コマンドラインのヘルプを取得する

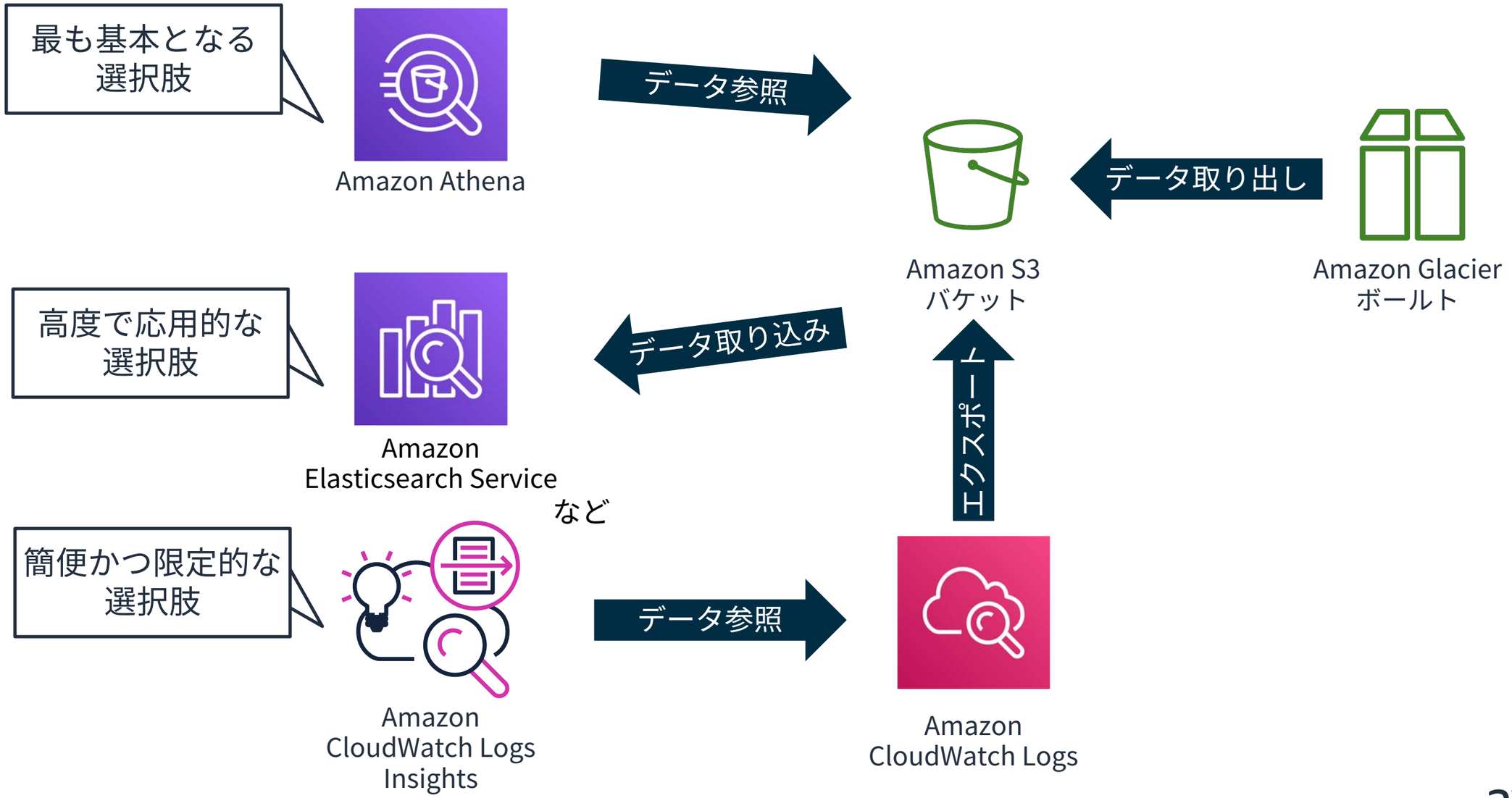
```
$ aws cloudtrail lookup-events help
```

指定可能な属性キー

- AccessKeyId
- EventId
- EventName
- EventSource
- ReadOnly
- ResourceName
- ResourceType
- Username

AWS CLI を使用して CloudTrail イベントを表示する
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/view-cloudtrail-events-cli.html
AWS CloudTrail lookupEvents
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/APIReference/API_LookupEvents.html

保存場所ごとの適した調査手法



Amazon Athena

Amazon S3 内のデータを SQL で分析できるインタラクティブなクエリサービス

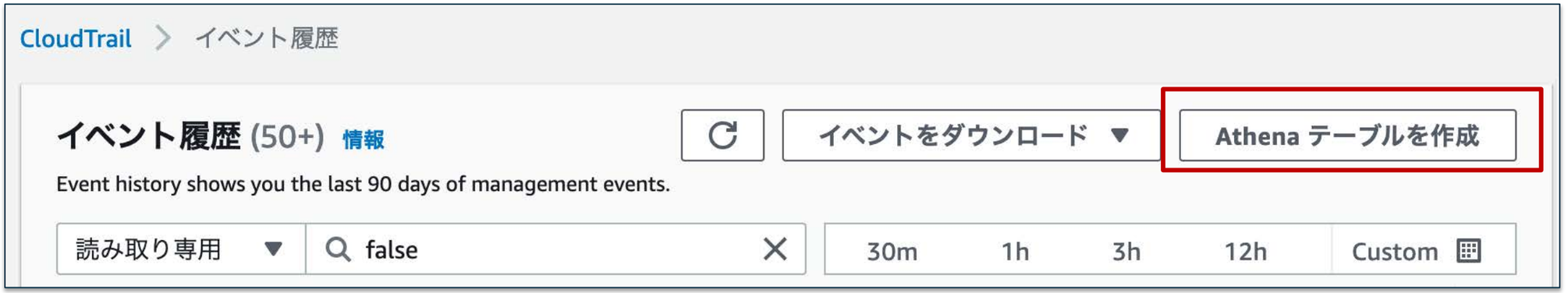
- データのロードや集約が不要
- サーバーレス/フルマネージド/従量課金

Amazon
Athena

利用手順

AWS CloudTrail 証跡ログのテーブルの作成

マネジメントコンソールを使用して自動作成



手動あるいはカスタマイズしたテーブルを作成するには・・・

手動パーティション処理を使用して CloudTrail で Athena ログのテーブルを作成する
https://docs.aws.amazon.com/ja_jp/athena/latest/ug/cloudtrail-logs.html

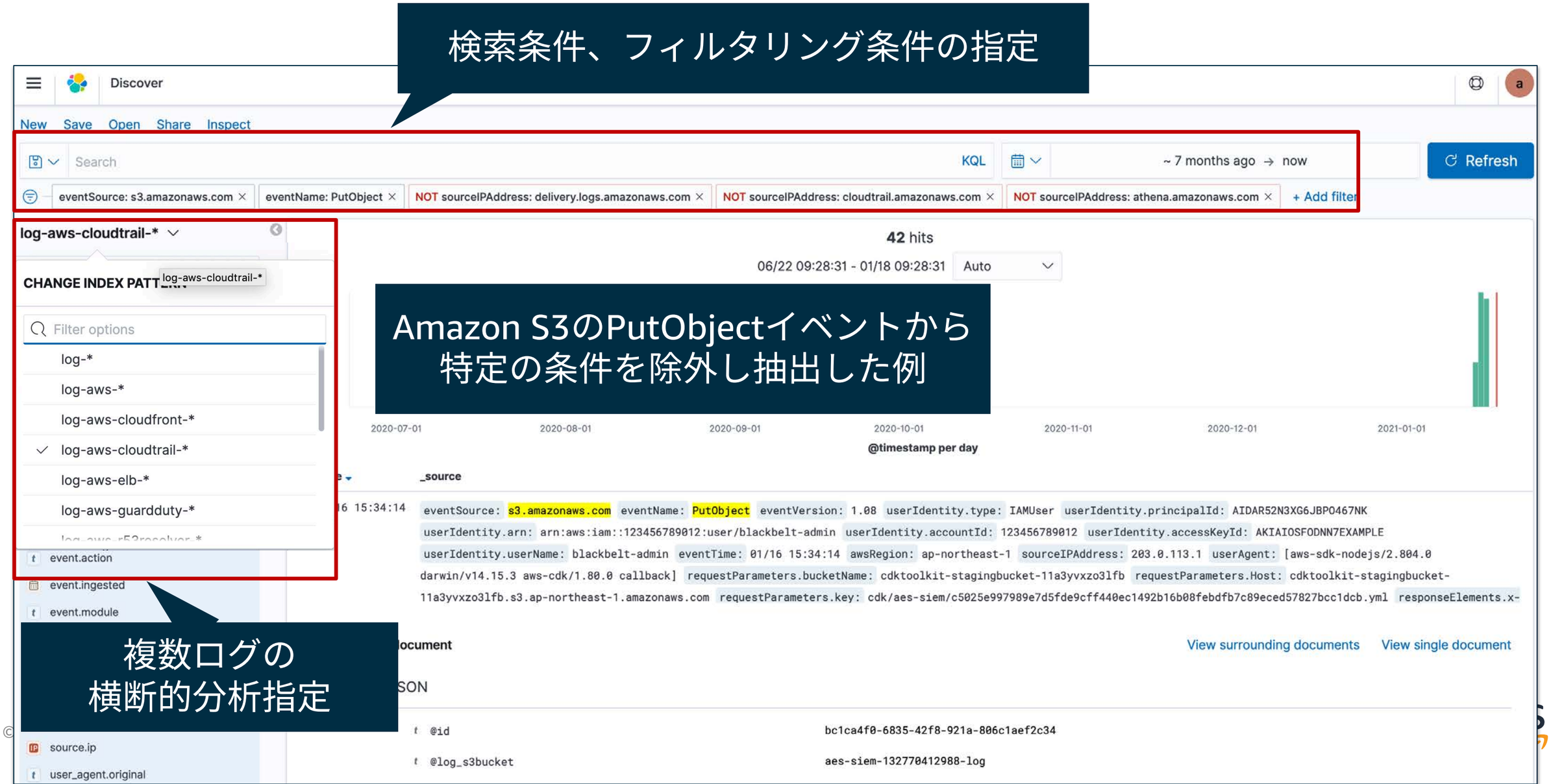
Amazon Athena 操作例

Amazon Elasticsearch Service

- RESTful 分散検索/分析エンジンElasticsearchのフルマネージドサービス
- 大規模かつ簡単でコスト効率の良い方法を使用してデプロイ、保護、実行
- インスタンスとストレージの維持に追加コストが発生
- Kibanaによる可観測性（オブザーバビリティ）をサポート

利用手順

Amazon Elasticsearch Service 操作例



Amazon CloudWatch Logs Insights

Amazon CloudWatch Logs内のデータを独自のクエリ言語を用いて分析できるインタラクティブなクエリサービス

- データのロードや集約が不要
- サーバーレス/フルマネージド/従量課金

Amazon CloudWatch Logs Insights

利用手順

Amazon CloudWatch Logs Insights 操作例

着目するフィールドは調査の目的によって異なる

調査目的の例

- アクションに失敗した原因を究明したい
- アラートの原因究明のため前後の挙動を確認したい
- 特定のユーザーや送信元IPアドレスからの操作を時系列に整理したい

など

ログ調査時に参照される典型的なフィールド

- userIdentity
- eventsource
- sourceIpAddress
- userAgent
- eventName
- requestParameters
- responseElements
- errorCode
- errorMessage

UserIdentity要素

- リクエストを行ったプリンシパルの種類(Type)と使用された認証情報を示す
- ロールを利用したプリンシパルを特定するには、さらに追加で要素の参照が必要

UserIdentity要素の例

```
"userIdentity": {
  "type": "IAMUser",
  "principalId": "AIDAJ45Q7YFFAREXAMPLE",
  "arn": "arn:aws:iam::123456789012:user/Alice",
  "accountId": "123456789012",
  "accessKeyId": "”,
  "userName": "Alice”}
```

Alice(IAMユーザー)
の操作であることが判る

CloudTrail userIdentity 要素
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-event-reference-user-identity.html

ロールを利用したプリンシパルを特定する（ケース1）

特定の条件下ではRoleSessionName値がロールを利用したプリンシパルを示す

- マネジメントコンソールを用いたスイッチロール
- AWSリソースにアタッチされたIAMロール（例：インスタンスプロファイル）
- RoleSessionNameにプリンシパルを含めるように構成されたSAML/Web ID フェデレーション
- Conditionにて“sts:RoleSessionName”に“${aws:username}”の指定を強制したIAMロール(※)
- その他RoleSessionNameにプリンシパルを含めてAssumeRoleされたケース

など

プリンシパルを特定したいロールが実行したイベント

この値からロールを利用したプリンシパルを確認

```
"userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAXXXXXXXEXAMPLE: RoleSessionName ",
    "arn": "arn:aws:sts::123456789012:assumed-role/role-name/RoleSessionName ",
    "accountId": " 123456789012",
    "accessKeyId": "ASIAXXXXXXXEXAMPLE
```

※IAM ロールを使用して実行されたアクションを担当する ID を簡単に特定
https://aws.amazon.com/jp/about-aws/whats-new/2020/04/now-easily-identify-the-identity-responsible-for-the-actions-performed-using-iam-roles/

ロールを利用したプリンシパルを特定する（ケース2）

いくつかの方法で特定可能、
たとえば、対応するAssumeRoleイベントを特定しUserIdentity要素を確認する

一意の識別子とフレンドリ名、ARN

IAM がユーザー、グループ、ロール、ポリシー、インスタンスプロファイルなどを作成するとき、各リソースには次のような一意の識別子が割り当てられる

IAMユーザーの一意の識別子例
AIDAJQABLZS4A3QDU576Q

IAMロールの一意の識別子例
AROAIDPPEZS35WEXAMPLE

プレフィクス4文字はリソースタイプを示す

多くの場合、“Alice”のようなフレンドリ名と ARNを用いて識別可能だが、一意の識別子は以下のようなケースにおいてもその各々を一意に識別することを可能とする

- IAM ユーザー名を再利用しているケースにおける、削除前のユーザーと再作成後のユーザー など

一意の識別子
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/reference_identifiers.html#identifiers-unique-ids

errorMessage/errorCode要素

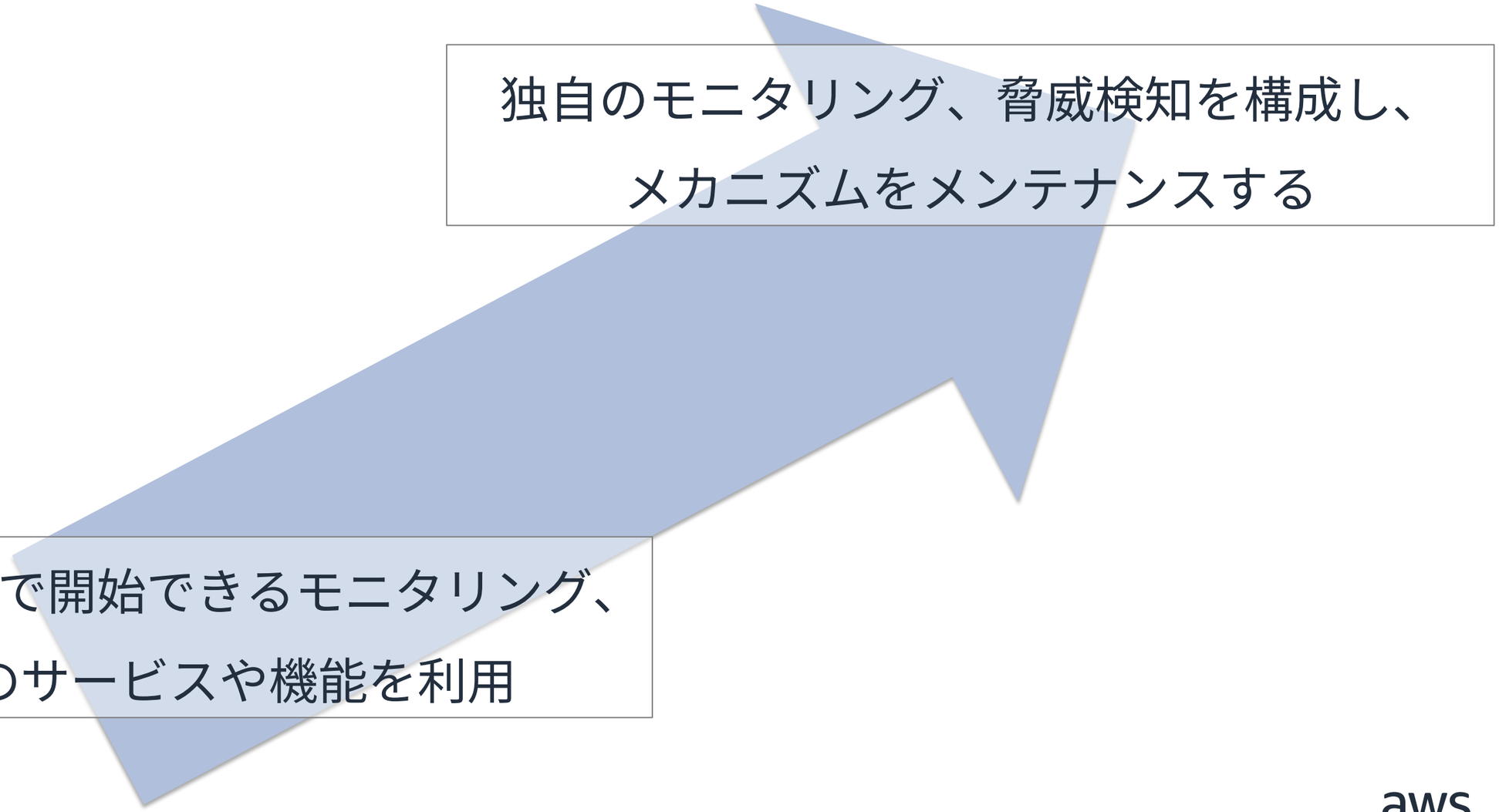
- リクエストがエラーを返す場合にその詳細を出力
- サービスによって出力するフィールドの階層が異なる
    - 最上位のフィールドとして提供するパターン
    - responseElements の一部として提供するパターン
- errorMessage/errorCodeが存在しないイベントはリクエストに成功している

権限不足によりアクセスキーの作成がエラーとなった例

```
"eventName": "CreateAccessKey",
"errorCode": "AccessDenied",
"errorMessage": "User: arn:aws:iam::123456789012:user/alice is not authorized to perform:
iam:CreateAccessKey on resource: user alice",
```

証跡ログのモニタリング、脅威検出

モニタリング、脅威検知のステップアップ



独自のモニタリング、脅威検知を構成し、
メカニズムをメンテナンスする

有効化するのみで開始できるモニタリング、
脅威検知のサービスや機能を利用

モニタリング、脅威検知に用いられるサービスや機能の例

機械学習、脅威インテリジェンスに基づく
モニタリング、脅威検知のサービスや機能

Amazon
GuardDuty

AWS CloudTrail
Insights

など

サービスを有効化するのみで
自動的にモニタリング

お客様独自のモニタリング、脅威検知を
実装可能なサービスや機能

Amazon CloudWatch
Logs

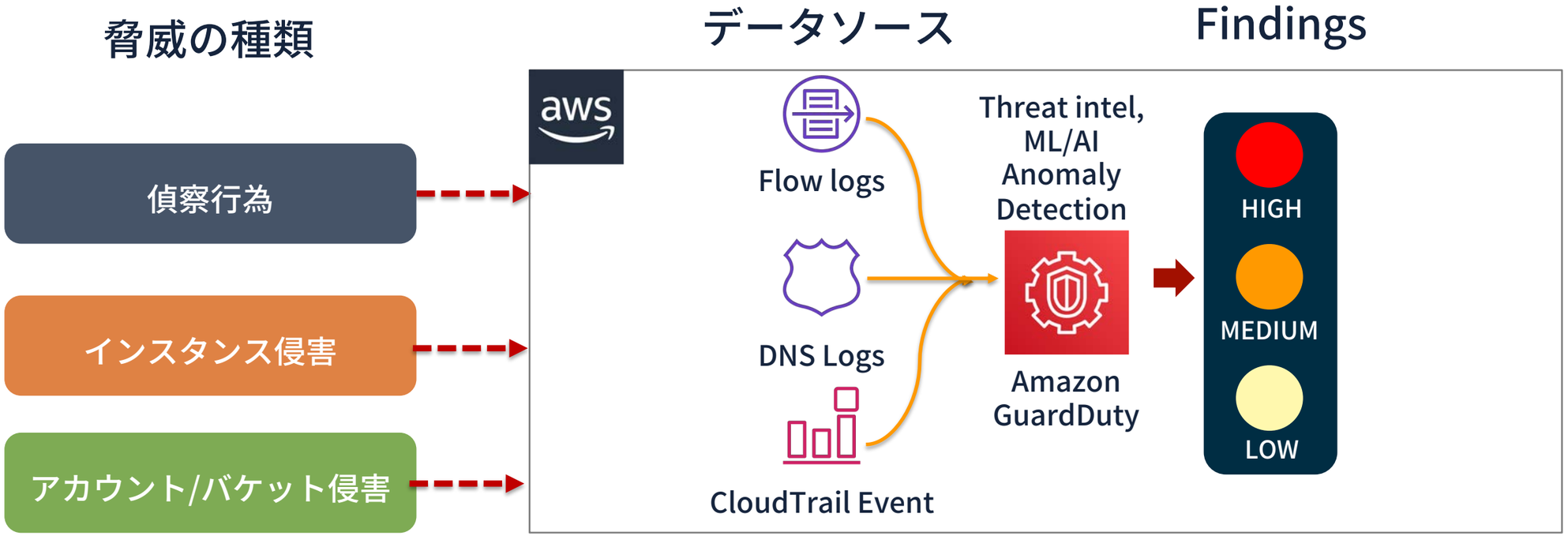
Amazon
Elasticsearch
Service

など

組織内モニタリングメカニズムの
メンテナンス体制が必要

Amazon GuardDutyとは

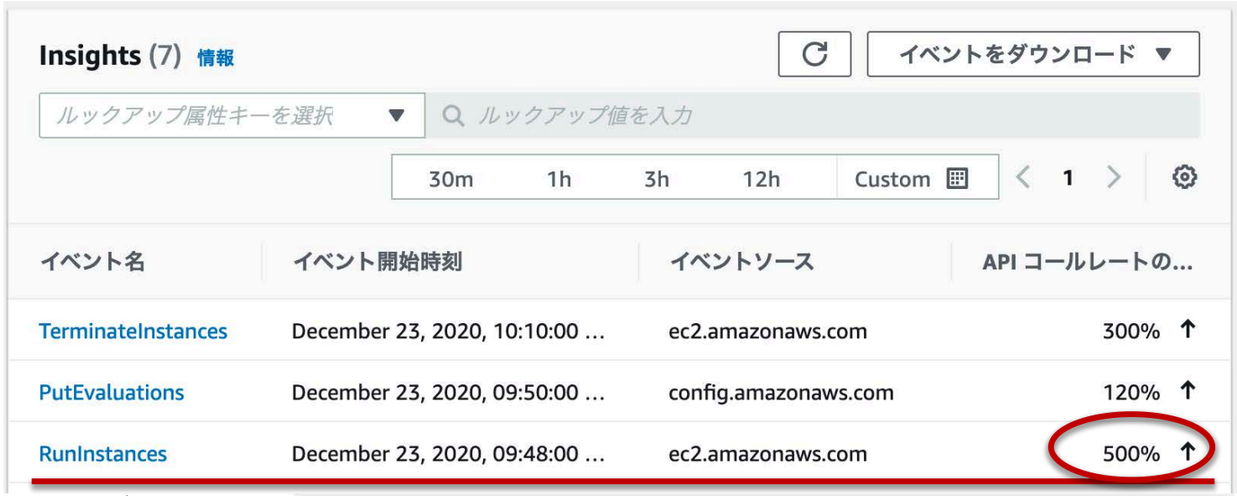
- セキュリティの観点から脅威を検知するAWSマネージドサービス
- 悪意のあるIPアドレス、異常検出、機械学習などの統合脅威インテリジェンスを使用して脅威を認識
- IDS/IPSなどで検出が難しいAWSのアカウントやバケットの侵害も検出する

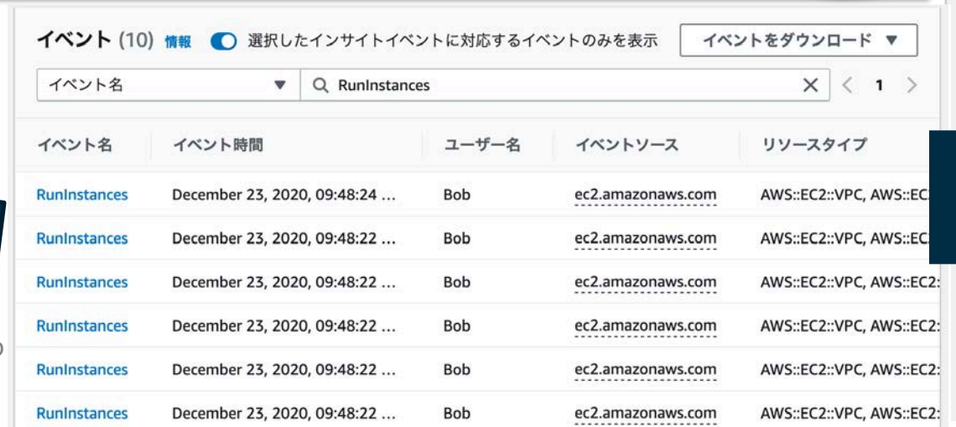


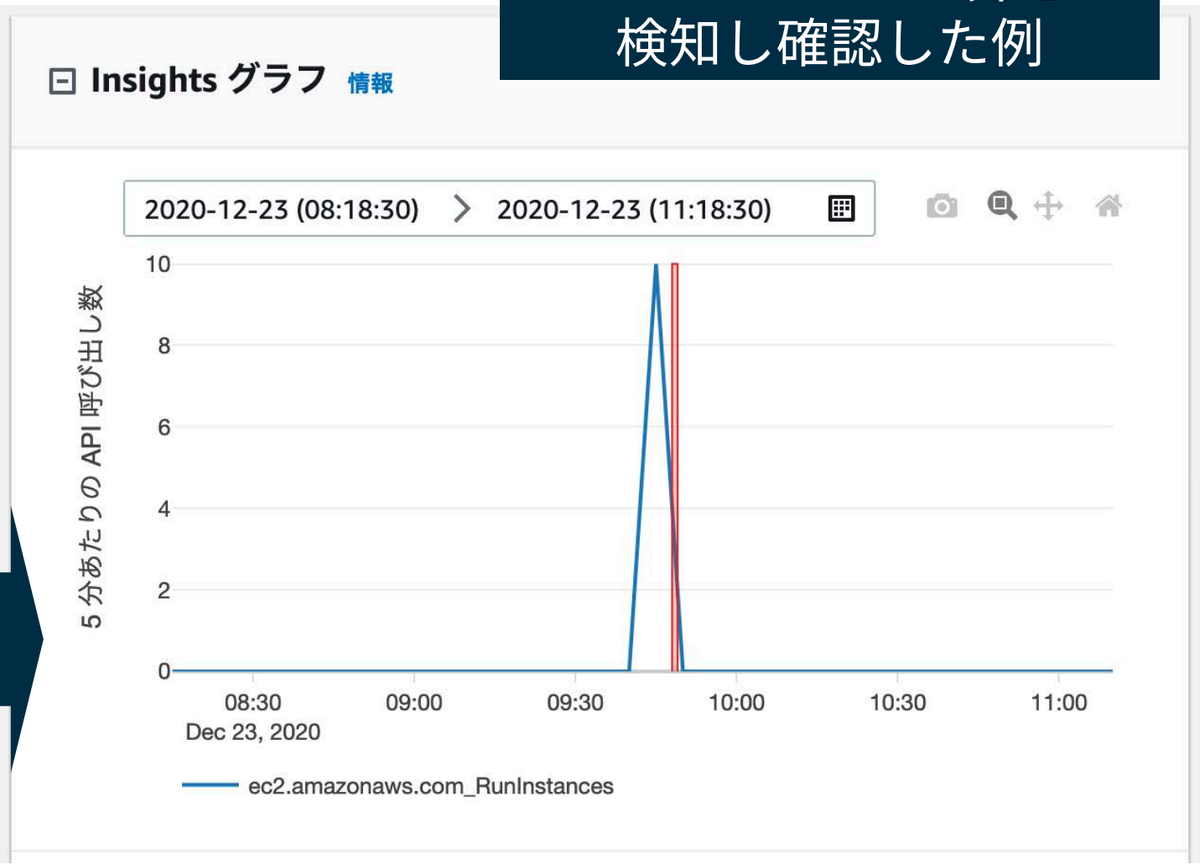
AWS CloudTrail Insights

管理イベントを自動的に分析して通常の動作のベースラインを確立、APIコールレートの異常なパターンを検出

RunInsntaces APIのコールレート上昇を検知し確認した例

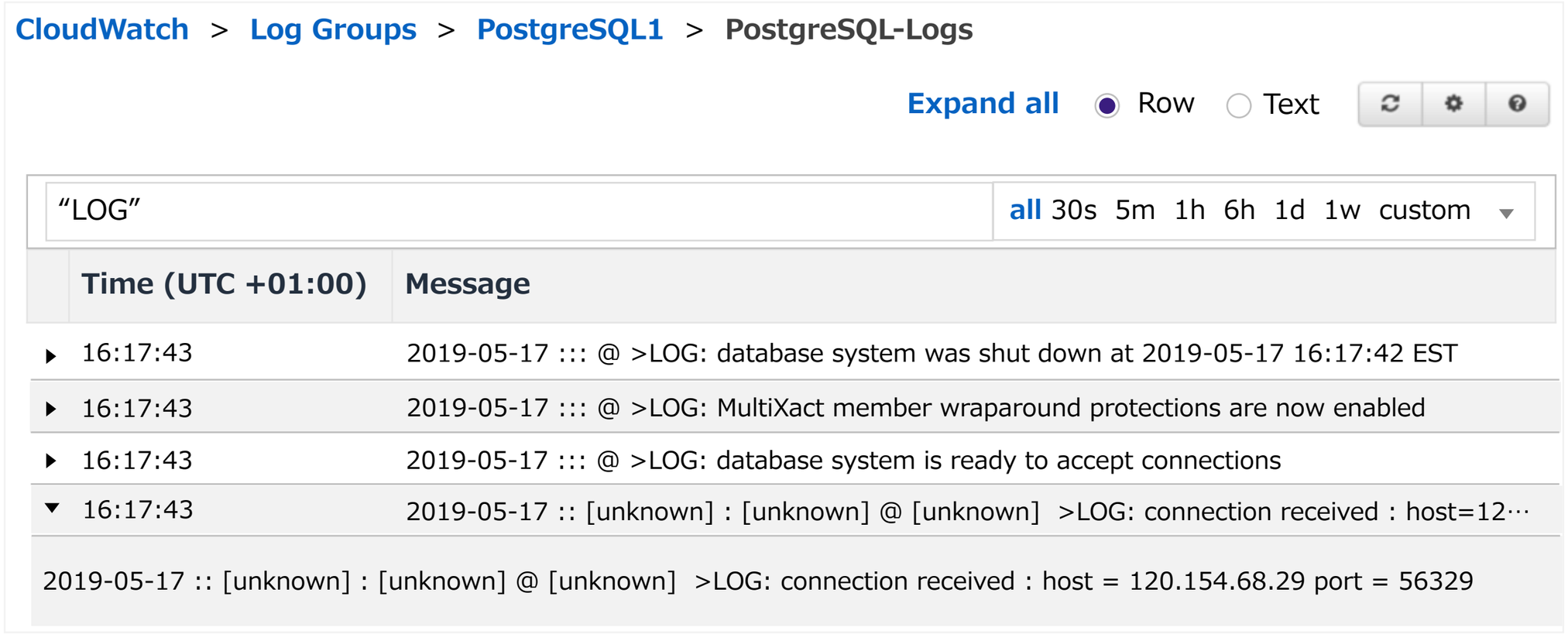




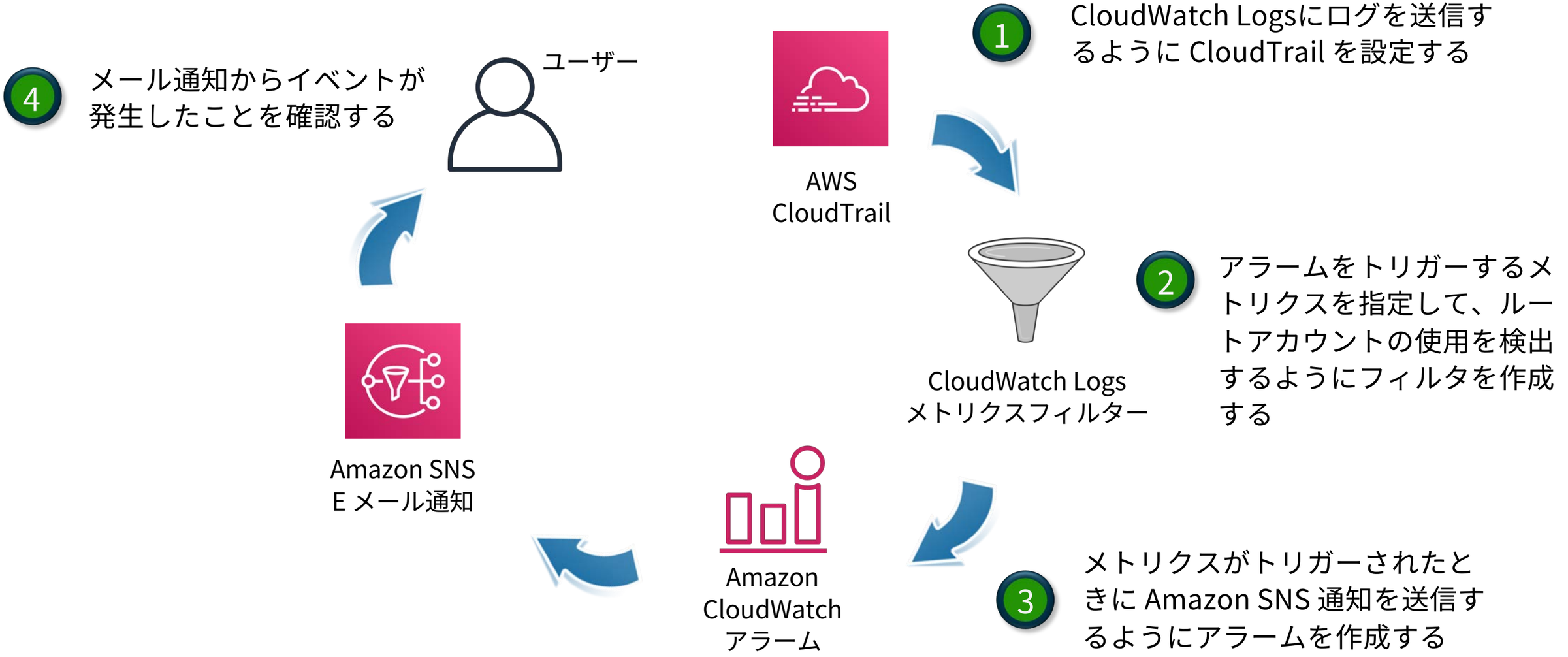


Amazon CloudWatch Logsとは

特定のフレーズ、値、またはパターンを見つけるためにログをリアルタイムでモニタリングするマネージドサービス



Amazon CloudWatch Logsによるモニタリング例



Amazon CloudWatch Logsによるモニタリングパターンの例

ルートアカウントでの操作
- "type":"Root"

CloudTrail構成変更
- StopLogging
- DeleteTrail
- UpdateTrail

操作の失敗、エラー
- Unauthorized*
- errorCode
- AccessDenied
- Failed authentication

IAMポリシーの削除、付与
- DeleteGroupPolicy
- DeleteRole
- DeleteRolePolicy
- DeleteUserPolicy
- PutGroupPolicy
- PutRolePolicy
- PutUserPolicy

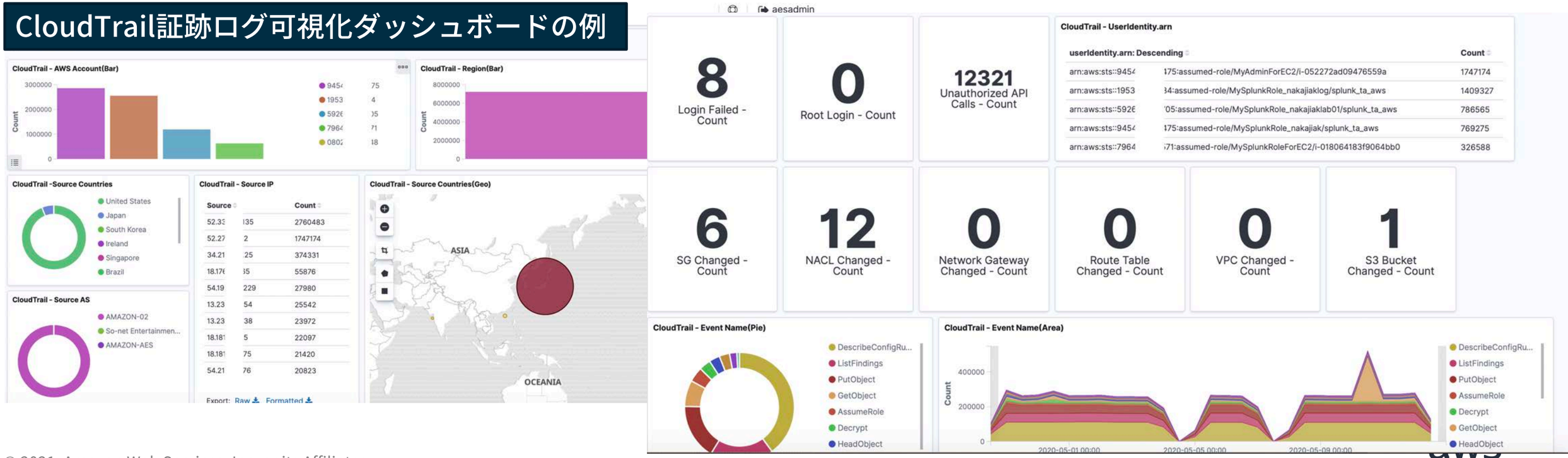
インスタンスの起動、終了
- RunInstances
- CreateInstances
- LaunchInstances
- TerminateInstances

ネットワーク構成変更
- AttachInternetGateway
- AssociateRouteTable
- CreateRoute
- DeleteCustomerGateway
- DeleteInternetGateway
- DeleteRoute
- DeleteRouteTable
- DeleteDhcpOptions
- DisassociateRouteTable
- CreateNetworkAcl
- CreateNetworkAclEntry
- DeleteNetworkAcl
- DeleteNetworkAclEntry
- ReplaceNetworkAclEntry
- ReplaceNetworkAclAssociation

SIEM on Amazon Elasticsearch Service (Amazon ES)

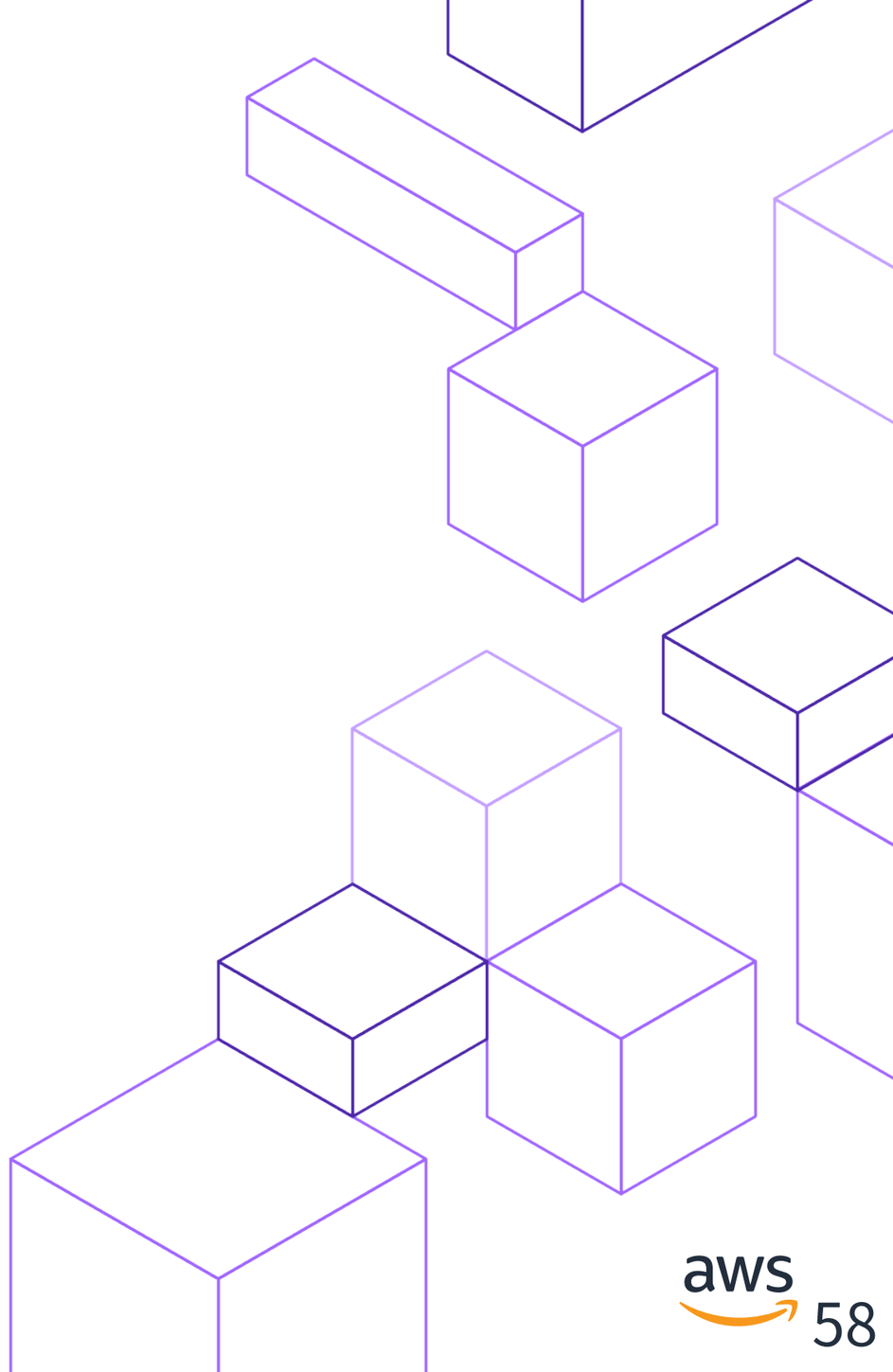
- AWS サービスのログの可視化やセキュリティ分析を実現するテンプレート
- デプロイはAWS CloudFormation を用い約20分で完了
- 分析対象のログを S3 バケットにエクスポートするだけで、複数種類のログに対する相関分析、作成済みのダッシュボードによる可視化が可能

CloudTrail証跡ログ可視化ダッシュボードの例



https://github.com/aws-samples/siem-on-amazon-elasticsearch/

ふりかえり



Key Takeaways

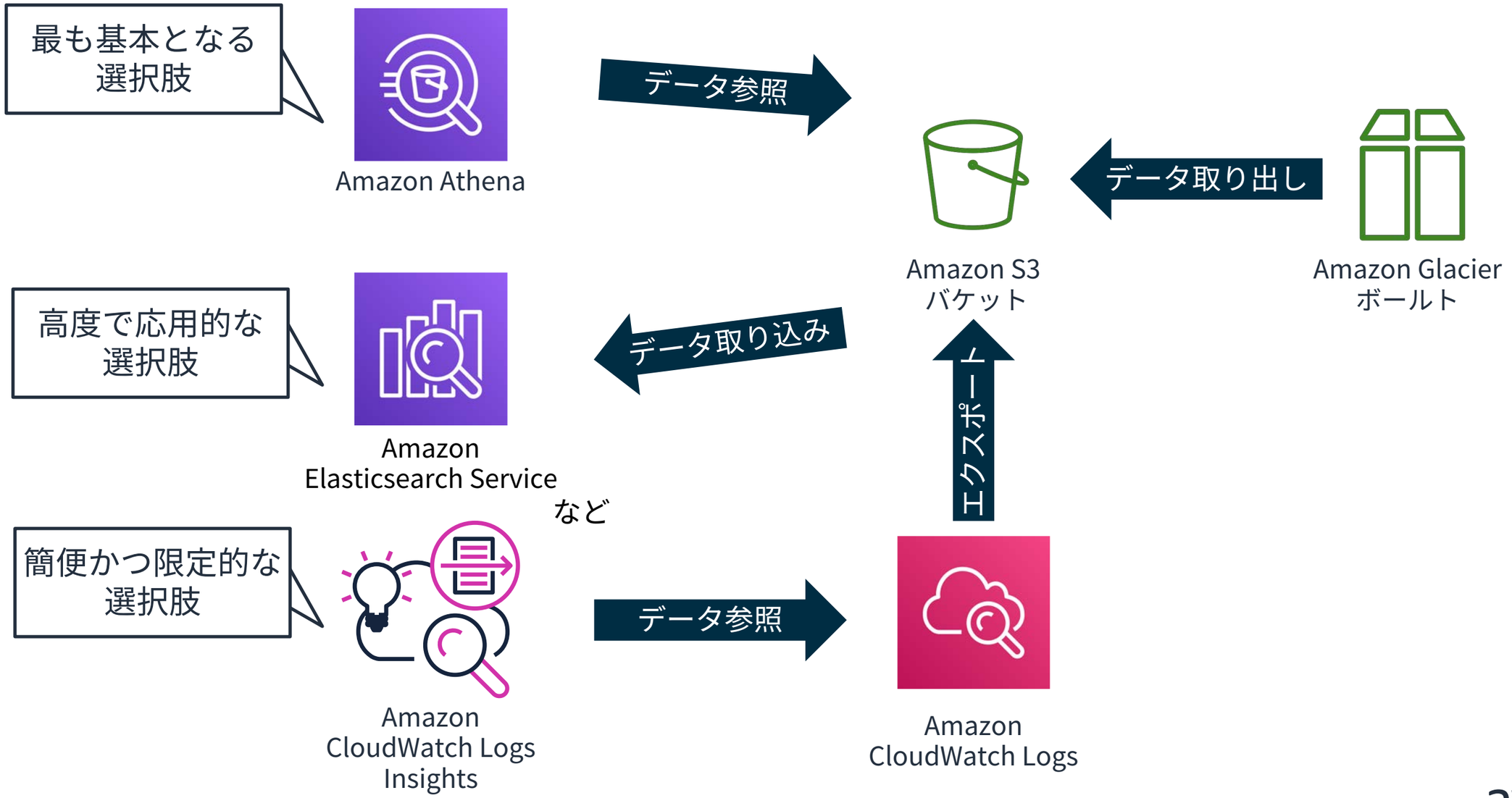
- まずベースラインとして「ログの保全と脅威検知の有効化」から始める
    - すべてのAWSリージョンでAWS CloudTrailの証跡の有効化
    - Amazon GuradDutyの有効化
- 次に「AWS CloudTrail でのセキュリティのベストプラクティス」を取り込む
- さらに「調査、モニタリング、脅威検出」の体制整備を進める

AWS CloudTrail セキュリティのベストプラクティス抜粋

- 専用および一元化されたAmazon S3バケットへのログ記録
- AWS KMSで管理されたキーを使用したサーバー側の暗号化
- ログファイルを保存するAmazon S3バケットで MFA Delete を有効にする
- ログファイルを保存するAmazon S3バケットでオブジェクトのライフサイクル管理を設定する
- ログファイルを保存する Amazon S3バケットへの最小限の特権アクセスを実装
- AWS CloudTrailへの特権アクセス（例：AWSCloudTrailFullAccessポリシー）を最小化

AWS CloudTrail でのセキュリティのベストプラクティス
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/best-practices-security.html

適材適所の調査手法の選択



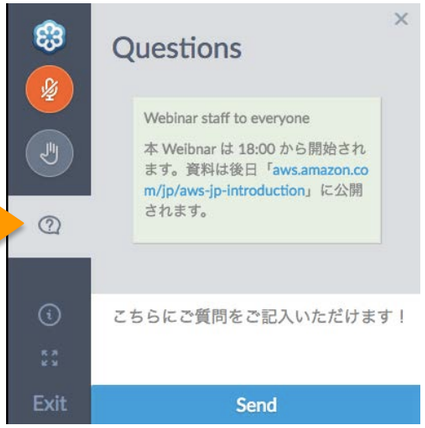
Q&A

ご質問への回答は
AWS Japan Blog 「https://aws.amazon.com/jp/blogs/news/」にて
後日掲載します。

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

AWS の日本語資料の場所「AWS 資料」で検索

https://amzn.to/JPArchive

AWS Well-Architected 個別技術相談会

毎週”W-A個別技術相談会”を実施中

- AWSのソリューションアーキテクト(SA)に対策などを相談することも可能

- 申込みはイベント告知サイトから

  (https://aws.amazon.com/jp/about-aws/events/)

AWS イベント で[検索]

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