



[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



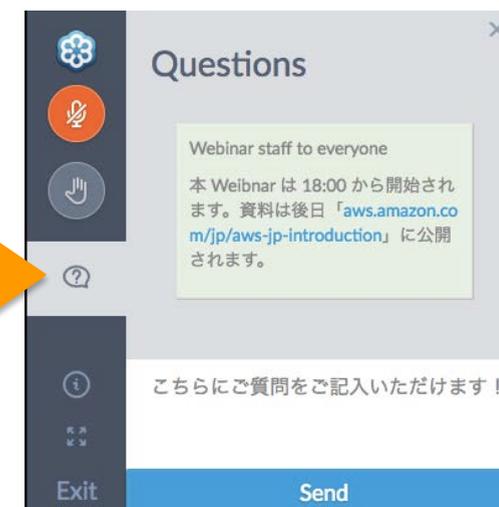
AWS Black Belt Online Seminar とは

「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おります。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

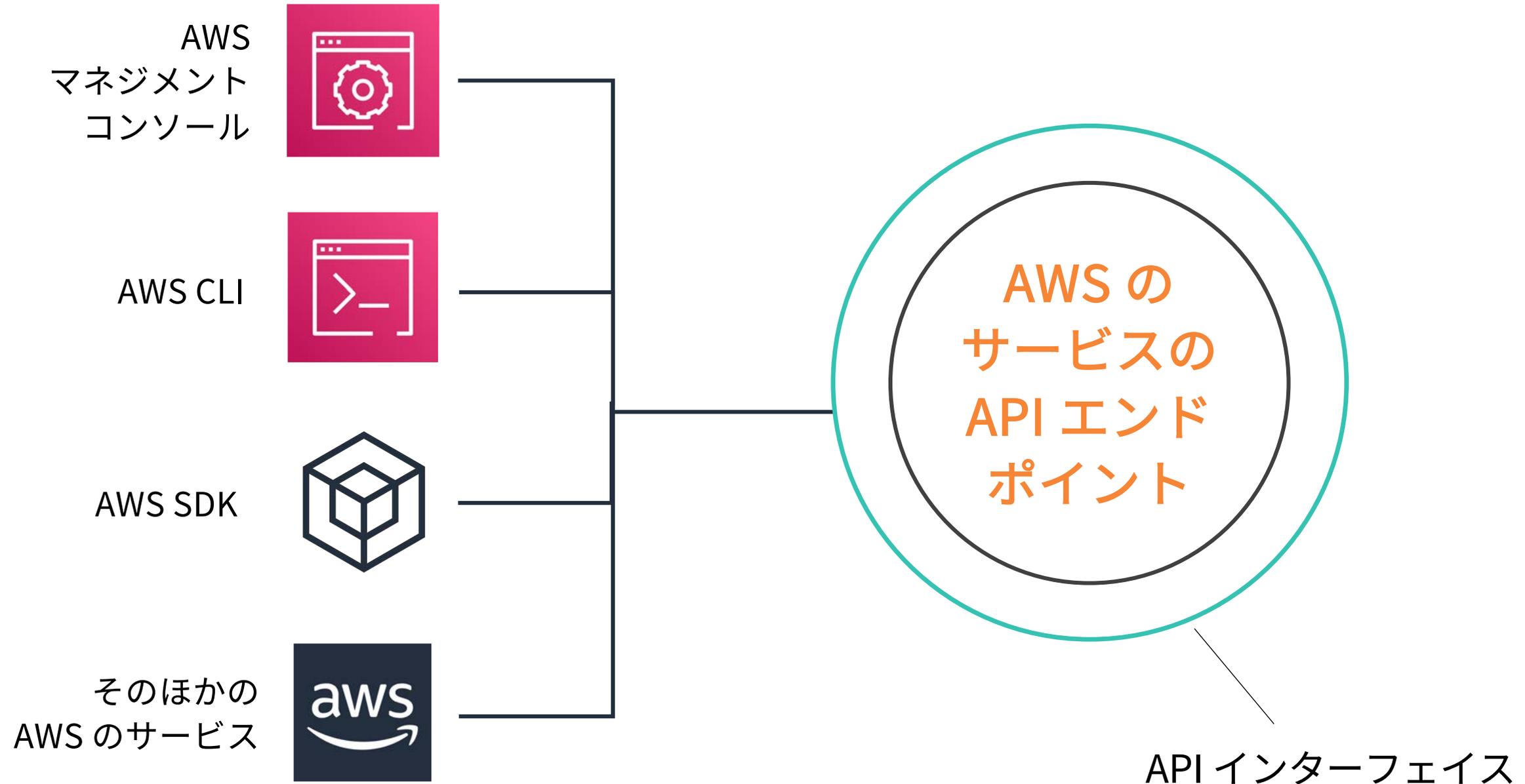
- まずベースラインとして「ログの保全と脅威検知の有効化」から始める
 - すべてのAWSリージョンでAWS CloudTrailの証跡の有効化
 - Amazon GuardDutyの有効化
- 次に「AWS CloudTrail でのセキュリティのベストプラクティス」を取り込む
- さらに「調査、モニタリング、脅威検出」の体制を整備する

Agenda

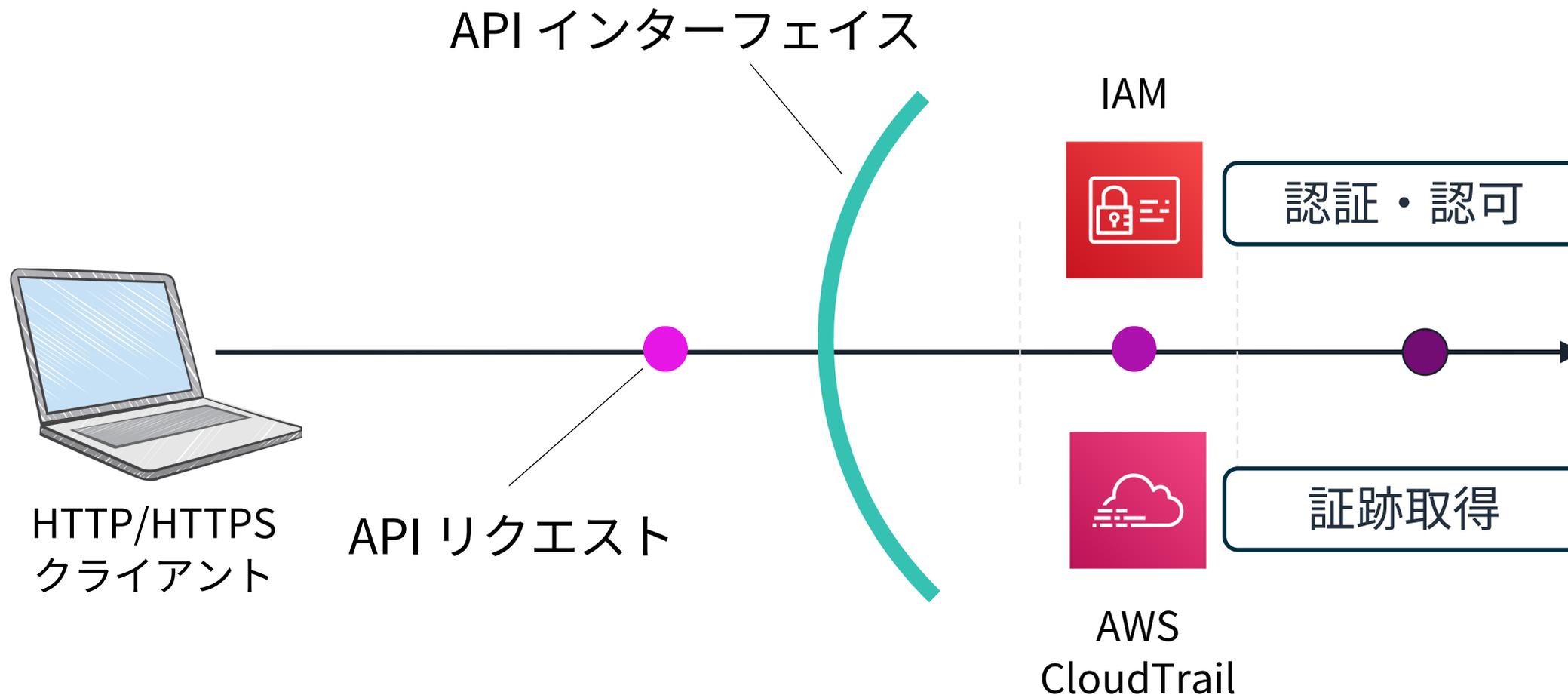
1. AWS CloudTrailの基本
2. 証跡ログの保存、保護
3. コスト最適化
4. 証跡ログの調査
5. 証跡ログのモニタリング、脅威検出
6. ふりかえり

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

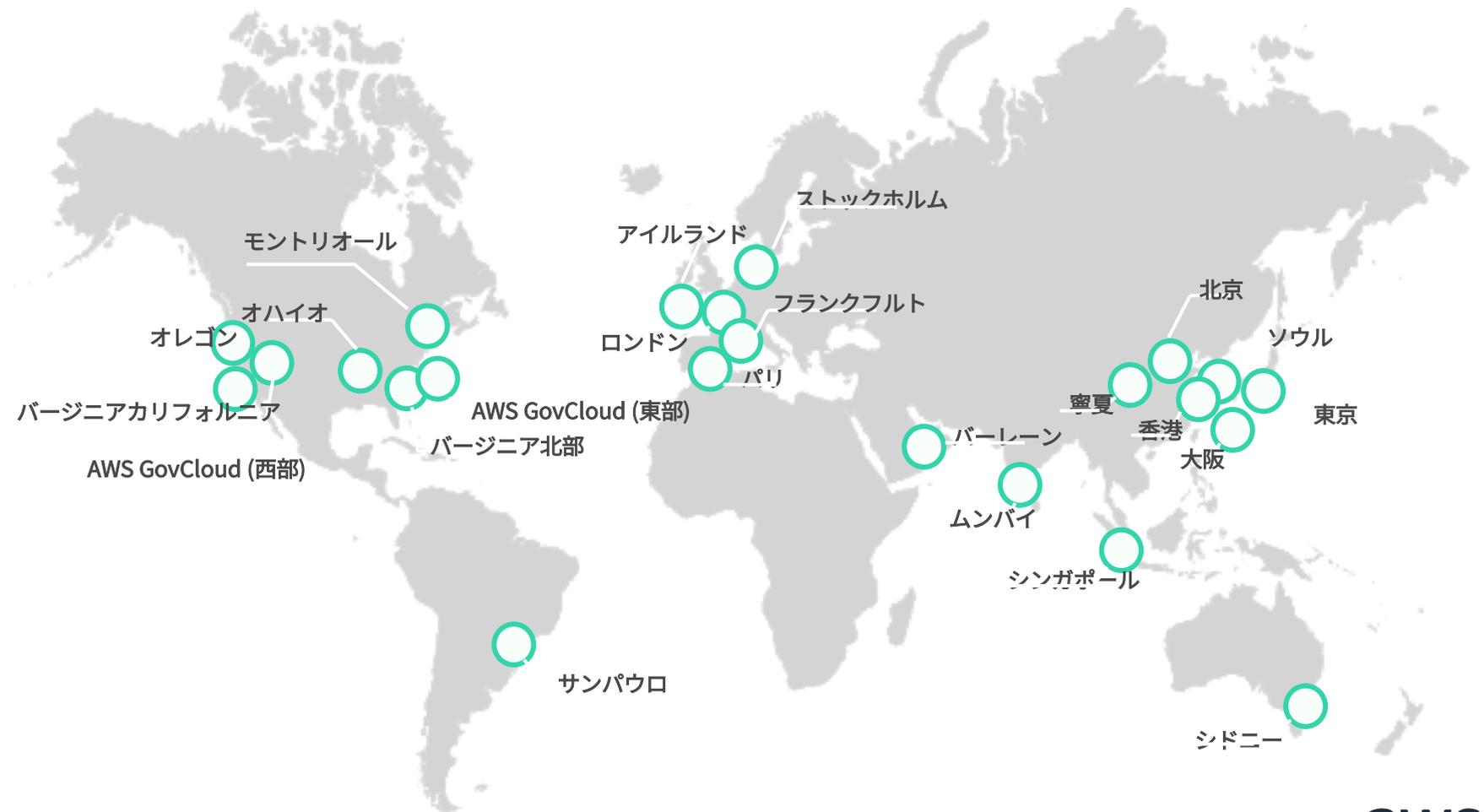


AWS サービスの
API エンドポイント

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

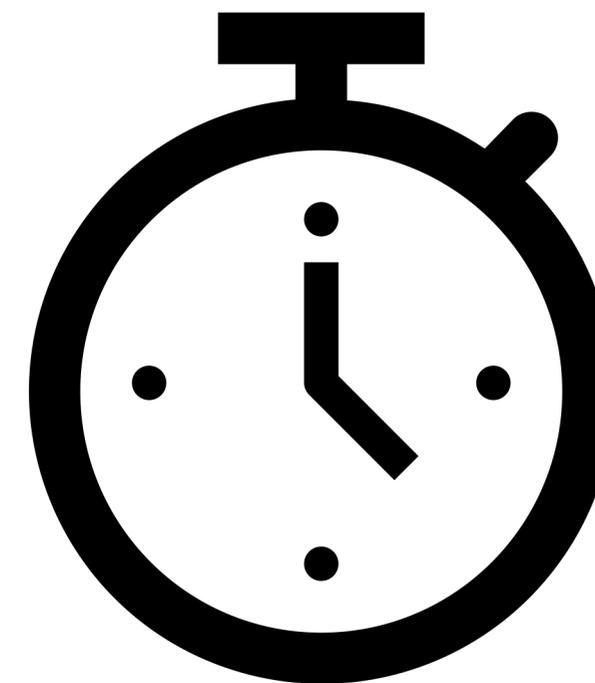
https://docs.aws.amazon.com/ja_jp/awscloudtrail/latest/userguide/cloudtrail-aws-service-specific-topics.html

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



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

CloudTrail

- ダッシュボード
- イベント履歴
- Insights
- 証跡

- 料金表
- ドキュメント
- フォーラム
- よくある質問

古いコンソールを使用する

CloudTrail > ダッシュボード > 証跡の作成

ステップ 1
証跡属性の選択

ステップ 2
ログイベントの選択

ステップ 3
確認と作成

証跡属性の選択

全般的な詳細

コンソールで作成された証跡は、マルチリージョンの証跡です。 [詳細](#)

証跡名
証跡の表示名を入力します。

3~128 文字。文字、数字、ピリオド、アンダースコア、ダッシュのみを使用できます。

組織内のすべてのアカウントについて有効化
組織のアカウントを確認するには、AWS Organizations を開きます。 [すべてのアカウントを表示](#)

ストレージの場所 [情報](#)

新しい S3 バケットを作成します
証跡のログを保存するバケットを作成します。

既存の S3 バケットを使用する
この証跡のログを保存する既存のバケットを選択します。

証跡ログバケットおよびフォルダ
ログを保存する新しい S3 バケット名とフォルダ (プレフィックス) を入力します。バケット名はグローバルに一意である必要があります。

ログは aws-cloudtrail-logs-123456789012/AWSLogs/738463627792 に保存されます

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

ライフサイクルの例

短期間

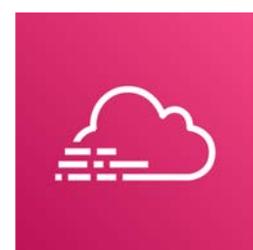
～14日

中長期間

～90日

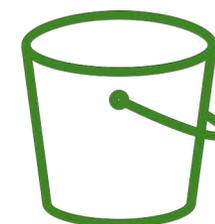
長期間

～2年



AWS
CloudTrail

S3バケットへ出力



Amazon S3
バケット



Amazon Glacier
ボールド

CloudWatch Logsへ出力
(オプション)



Amazon
CloudWatch Logs

ログデータのエクスポート

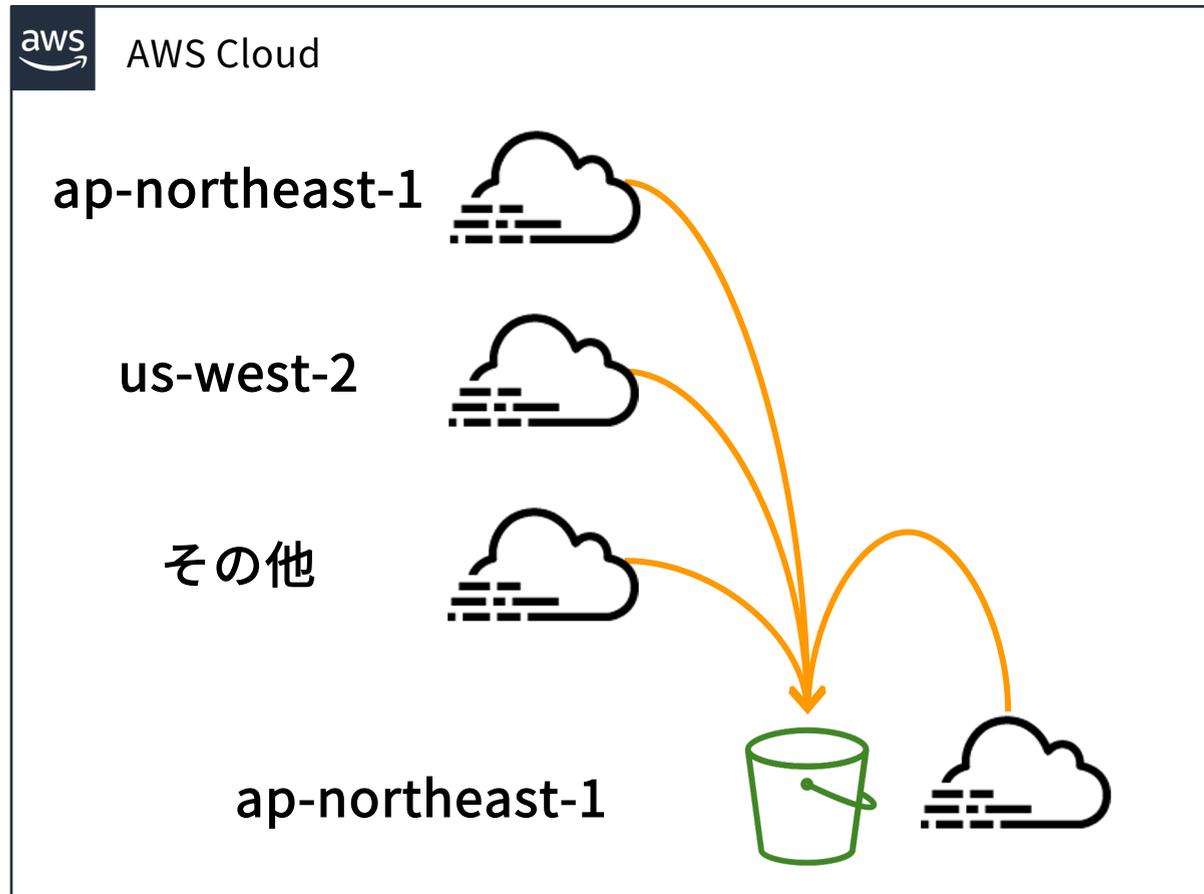


KMS暗号化された
S3バケットへの出力を
サポートしない点に留意

証跡ログの集約

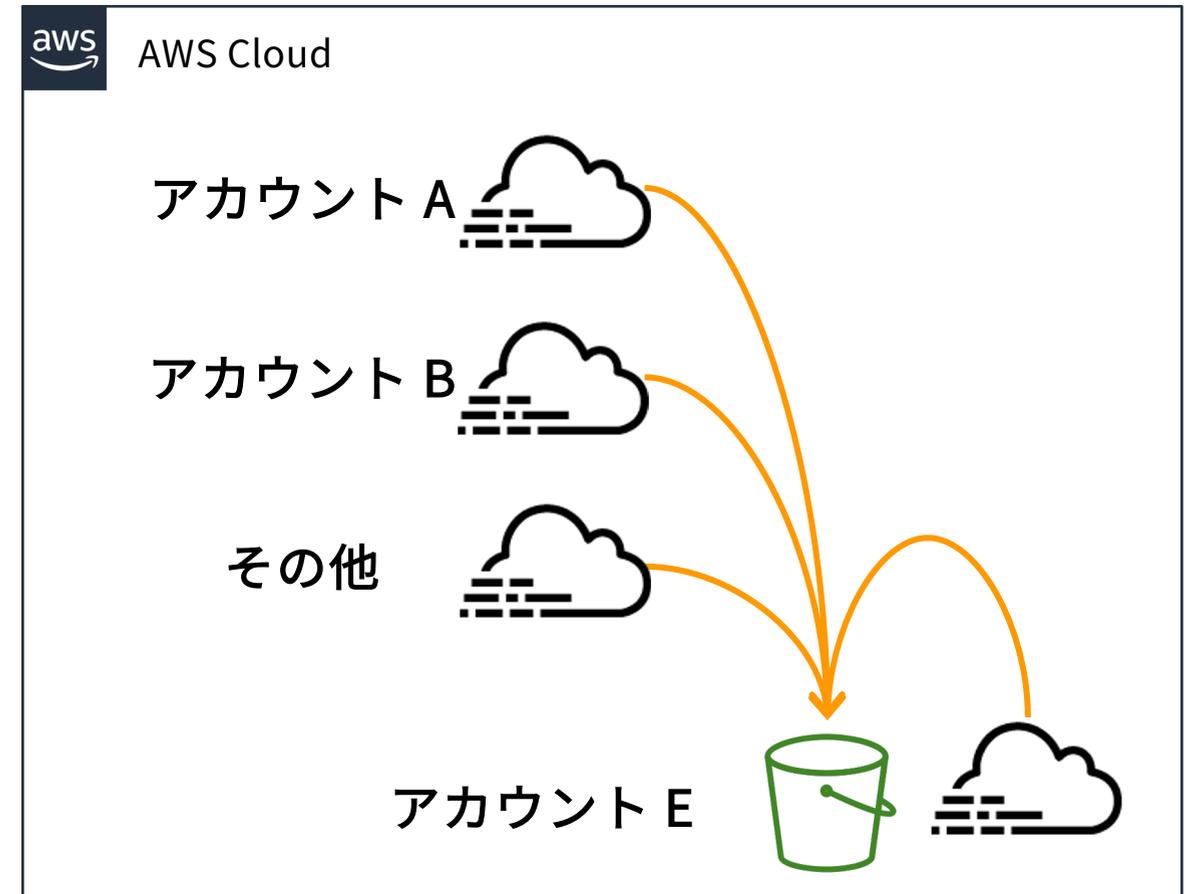
リージョンやアカウント毎の証跡ログを集約することで運用を容易にする

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

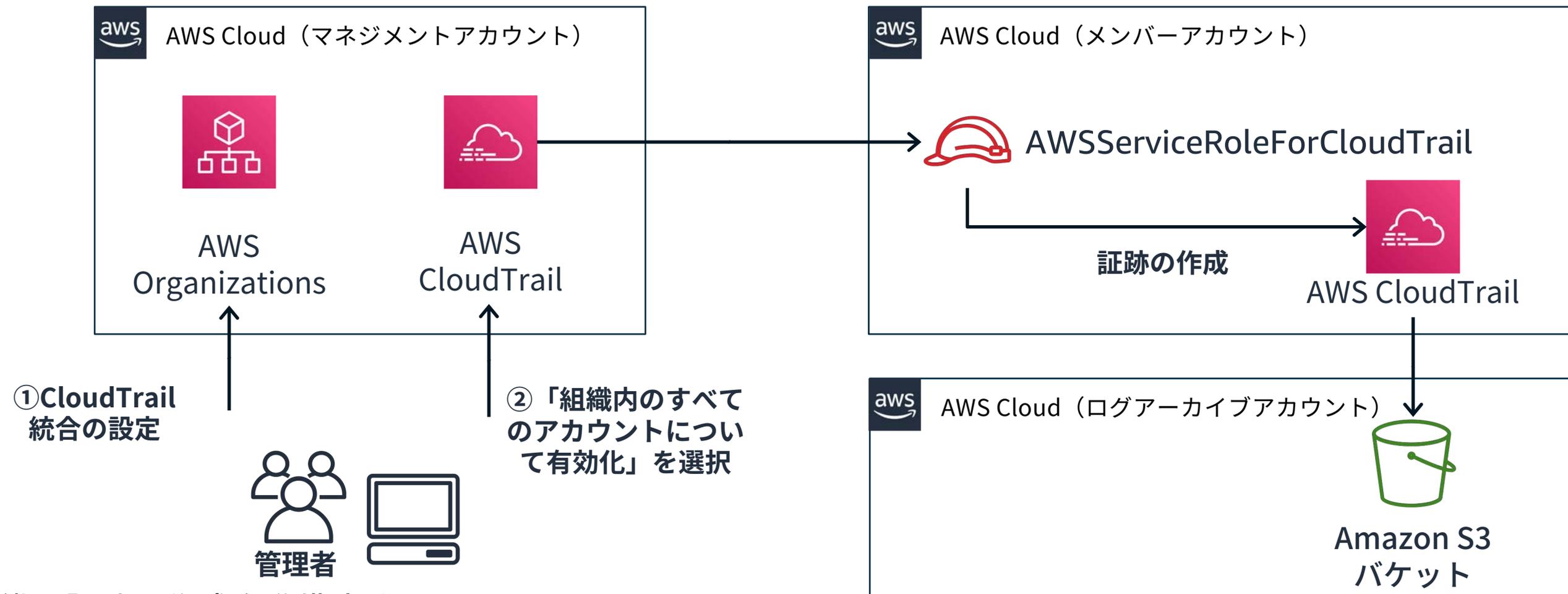
すべてのアカウントのログを
1つのアカウントへ



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/awsccloudtrail/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

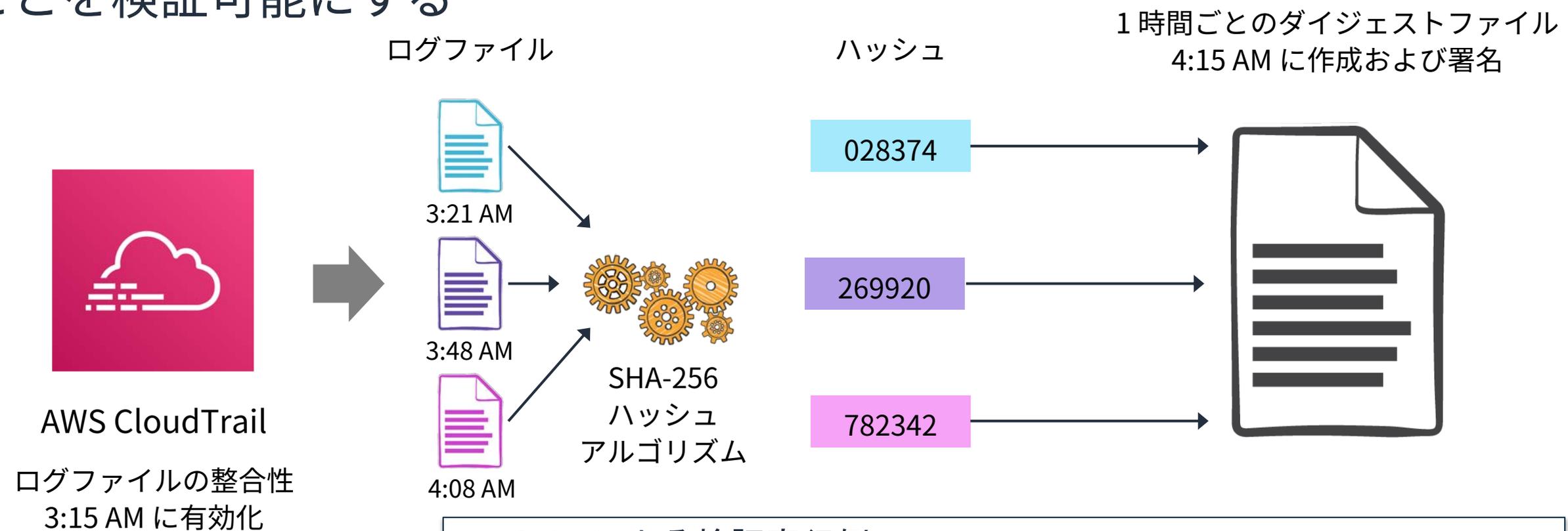
証拠の証明力は、裁判官の自由な判断に委ねる。

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) ボールドロック(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

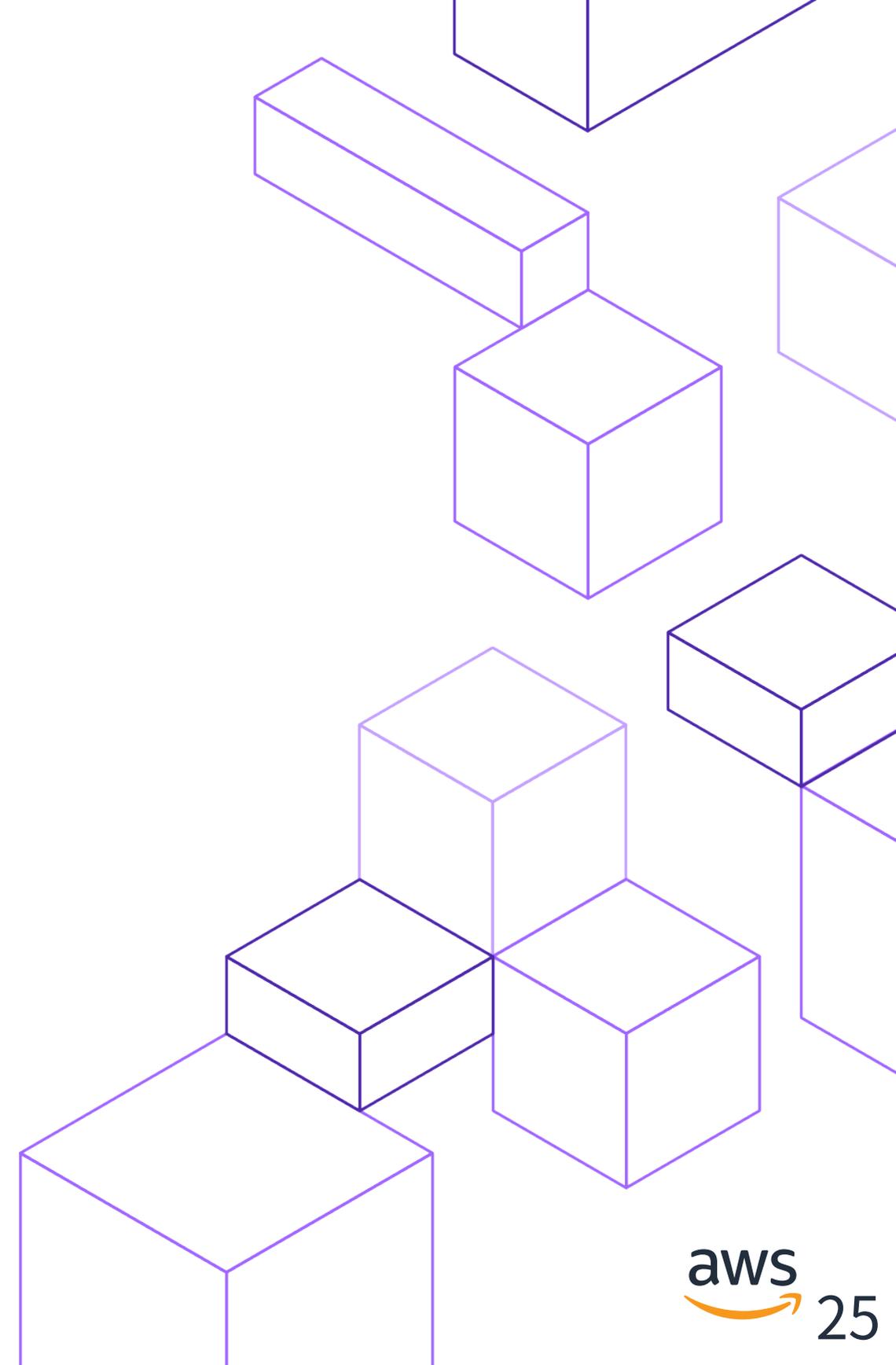
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/replication-what-is-not-replicated.html

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に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

データイベント 情報

追加料金が適用されます [?](#) データイベントは、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についての情報を表示します。

高度なデータイベントセレクター

高度なデータイベントセレクターを使用すると、証拠別にキャプチャされるイベントをより詳細にコントロールできます。高度なデータイベントセレクターでは、イベント内の eventName、eventSource、readOnly、eventCategory、resources.type、および resources.ARN の各フィールドについてきめ細かなコントロールが提供されます。これらの新しいコントロールは、お客様にとって重要なデータイベントを制限することで、コストを調整するのに役立ちます。

▼ データイベント: S3

データイベントタイプ
ログ記録するデータイベントのソースを選択します。

S3

ログセレクターテンプレート
カスタム

基本的なイベントセレクターに切り替える

セレクター名

名前を入力
1,000 文字未満

イベントの収集
すべてのイベントをログに記録するか、特定のイベントのみを記録するかを選択できます。後で編集できます。

高度なイベントセレクター 情報
特定のリソース、オブジェクト、ユーザー、またはロールからイベントを記録または除外します。

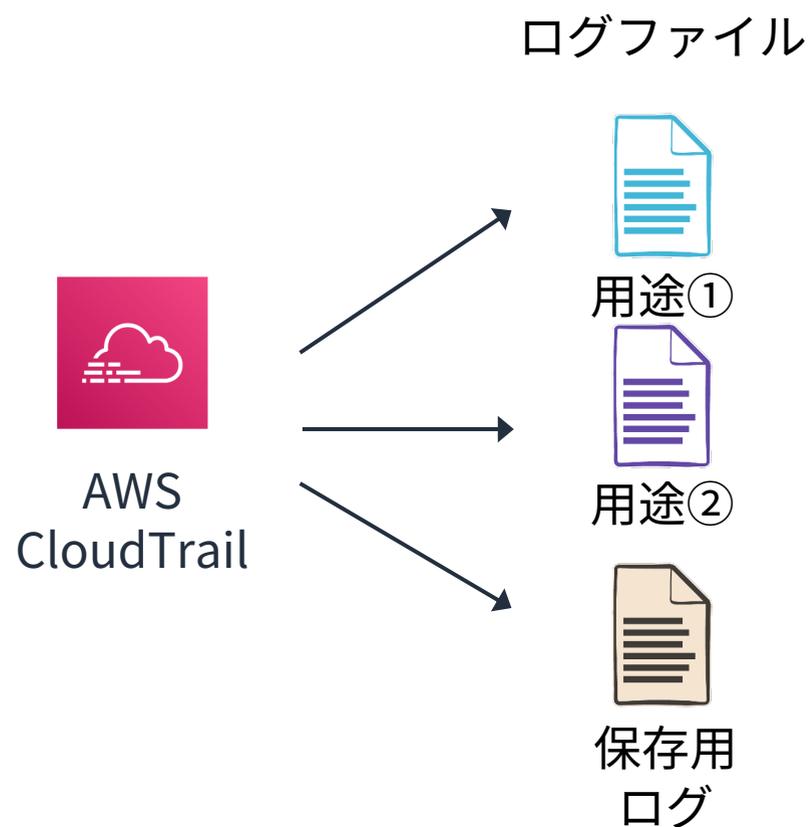
Amazon S3のデータイベントを限定して保存する例

フィールド	オペレーター	Value	
eventName	次で始まる:	Put	×
	次で始まる:	Delete	×
+ 条件			
AND			
resources.ARN	次で始まる:	arn:aws:s3:::my_bucket/	参照 ×
+ フィールド + 条件			

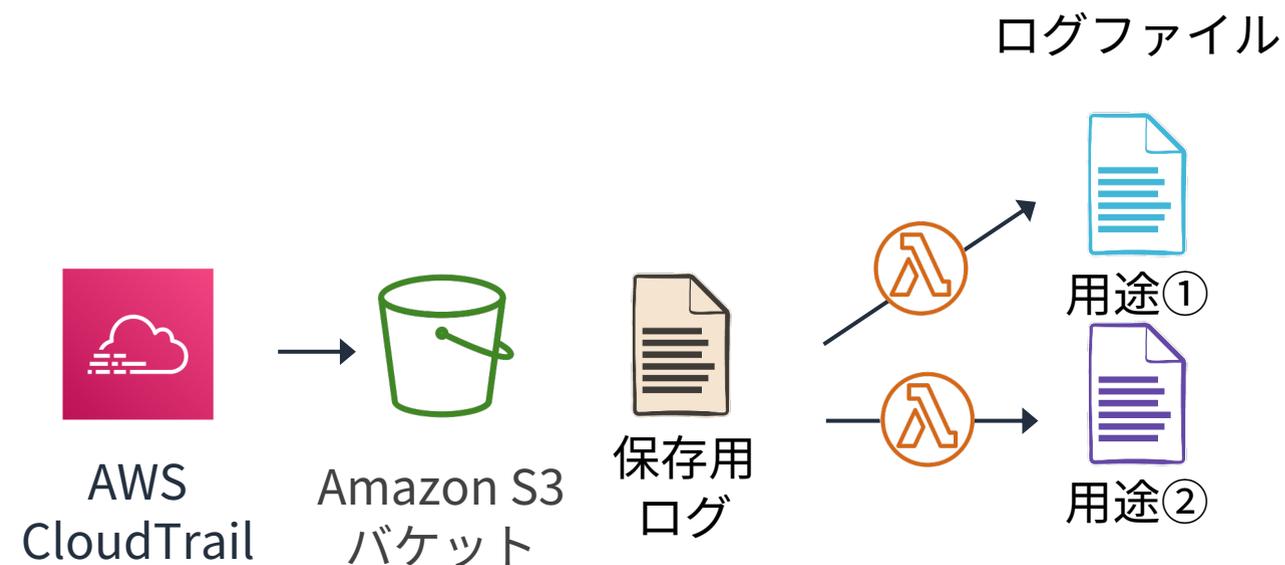
注：選択的保存が出来るのはデータイベントのみ

デザインパターン

用途毎に証跡を設定するパターン



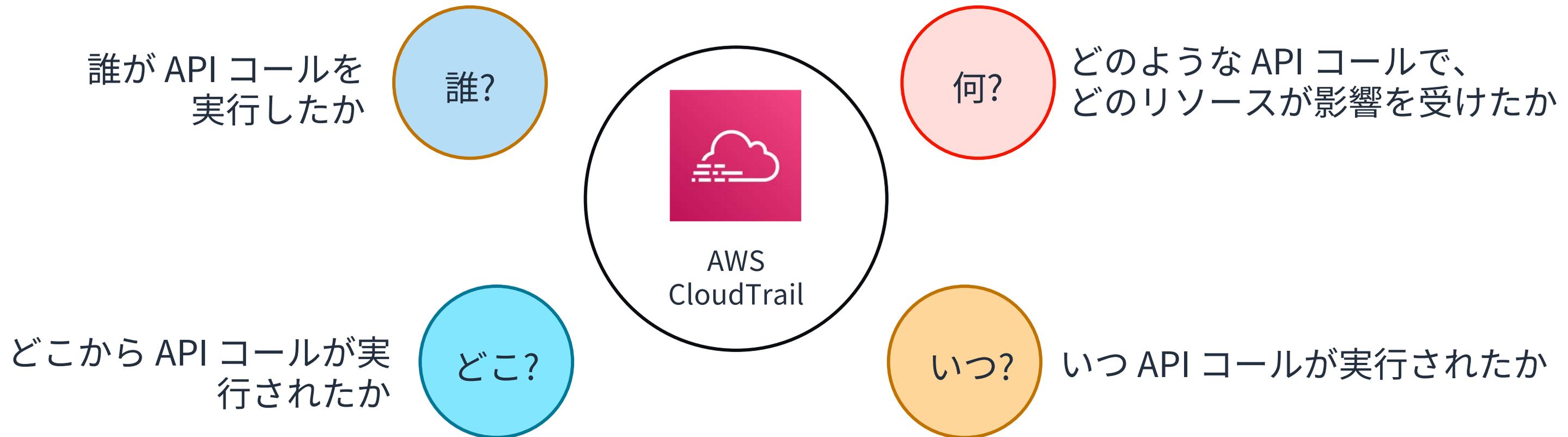
集約した証跡を用途毎にロードするパターン



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



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"  
    },  
    }
```

何がリクエストされたか

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

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",
```

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

The screenshot displays the AWS CloudTrail console interface. On the left is a navigation sidebar with options like 'ダッシュボード', 'イベント履歴', 'Insights', and '証跡'. The main content area shows the 'イベント履歴 (50+) 情報' page, which includes a search bar and a table of events. One event, 'BatchGetResourceConfig', is highlighted with a red underline and a blue arrow pointing to its details pane on the right. The details pane shows various attributes such as 'イベント時間', 'AWS アクセスキー', 'AWS リージョン', 'ユーザー名', '発信元 IP アドレス', 'イベント ID', and 'リクエスト ID'.

イベント名	イベント時間
BatchGetResourceConfig	January 17, 2021, 21:24:32 (UTC+09:00)
BatchGetResourceConfig	January 17, 2021, 21:24:32 (UTC+09:00)
BatchGetResourceConfig	January 17, 2021, 21:24:32 (UTC+09:00)
BatchGetResourceConfig	January 17, 2021, 21:24:32 (UTC+09:00)
BatchGetResourceConfig	January 17, 2021, 21:24:32 (UTC+09:00)

詳細	情報
イベント時間	AWS アクセスキー
January 17, 2021, 21:24:32 (UTC+09:00)	ASIA2X364XIIMI3CWY5D
ユーザー名	AWS リージョン
securityhub	us-west-2
イベント名	発信元 IP アドレス
BatchGetResourceConfig	securityhub.amazonaws.com
イベントソース	エラーコード
config.amazonaws.com	-
	イベント ID
	01d7ac2f-3cf6-46c7-b40f-a3e68eec78bf
	読み取り専用
	false
	リクエスト ID
	0078b8ee-a942-4f47-9285-3630dc55aed5

AWS Cloud Trail イベント履歴 (マネジメントコンソール)

The screenshot displays the AWS CloudTrail console interface. At the top, the breadcrumb navigation shows 'CloudTrail > イベント履歴'. A dark blue callout box with white text 'イベントの条件フィルタリング' points to the search and filter area. This area includes a dropdown menu set to '読み取り専用', a search box containing 'false', and a time range selector with options for 30m, 1h, 3h, 12h, and Custom. A gear icon for settings is also visible. Below this is a table of event history with columns for 'イベント名', 'イベント時間', 'ユーザー名', 'イベントソース', 'リソースタイプ', and 'リソース名'. The first row is selected. A second dark blue callout box with white text '表示カラムの追加 (オプション)' points to the gear icon. Below the table is the 'イベント詳細を比較' section, which allows comparing 2-5 events. Two event comparison cards are shown, each with a close button. The first card is titled 'イベント 1' and the second 'イベント 2'. Both cards show details for an 'UpdateInstanceInformation' event, including the event name, ID, time, user name, and AWS access key. A third dark blue callout box with white text 'イベント比較表示' points to these comparison cards. A 'すべての選択をクリア' button is located at the top right of the comparison section.

イベント履歴 (2/5) 情報

Event history shows you the last 90 days of management events.

読み取り専用 | false | 30m | 1h | 3h | 12h | Custom

イベント名	イベント時間	ユーザー名	イベントソース	リソースタイプ	リソース名
<input checked="" type="checkbox"/> UpdateInstanceInfor...	January 13, 2021, 20:22:...	i-0a56fc8c920eeae90	ssm.amazonaws.com	-	-
<input type="checkbox"/> UpdateInstanceInfor...	January 13, 2021, 20:17:...	i-0a56fc8c920eeae90	ssm.amazonaws.com	-	-
<input type="checkbox"/> UpdateInstanceInfor...	January 13, 2021, 20:13:...	i-0a56fc8c920eeae90	ssm.amazonaws.com	-	-

イベント詳細を比較 情報

詳細を比較するイベントを 2~5 個選択します。

すべての選択をクリア

イベント 1		イベント 2	
イベント名	UpdateInstanceInformation	イベント名	UpdateInstanceInformation
イベント ID	dbed352e-7b2d-4d5f-aec8-19326b9c9f5f	イベント ID	d21bd4c8-8e2a-470a-9d9d-c8dfe8a11431
イベント時間	January 13, 2021, 20:07:19 (UTC+09:00)	イベント時間	January 13, 2021, 20:22:19 (UTC+09:00)
ユーザー名	i-0a56fc8c920eeae90	ユーザー名	i-0a56fc8c920eeae90
AWS アクセスキー	ASIA2X364XIIPA2WGEE4	AWS アクセスキー	ASIA2X364XIIPA2WGEE4

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

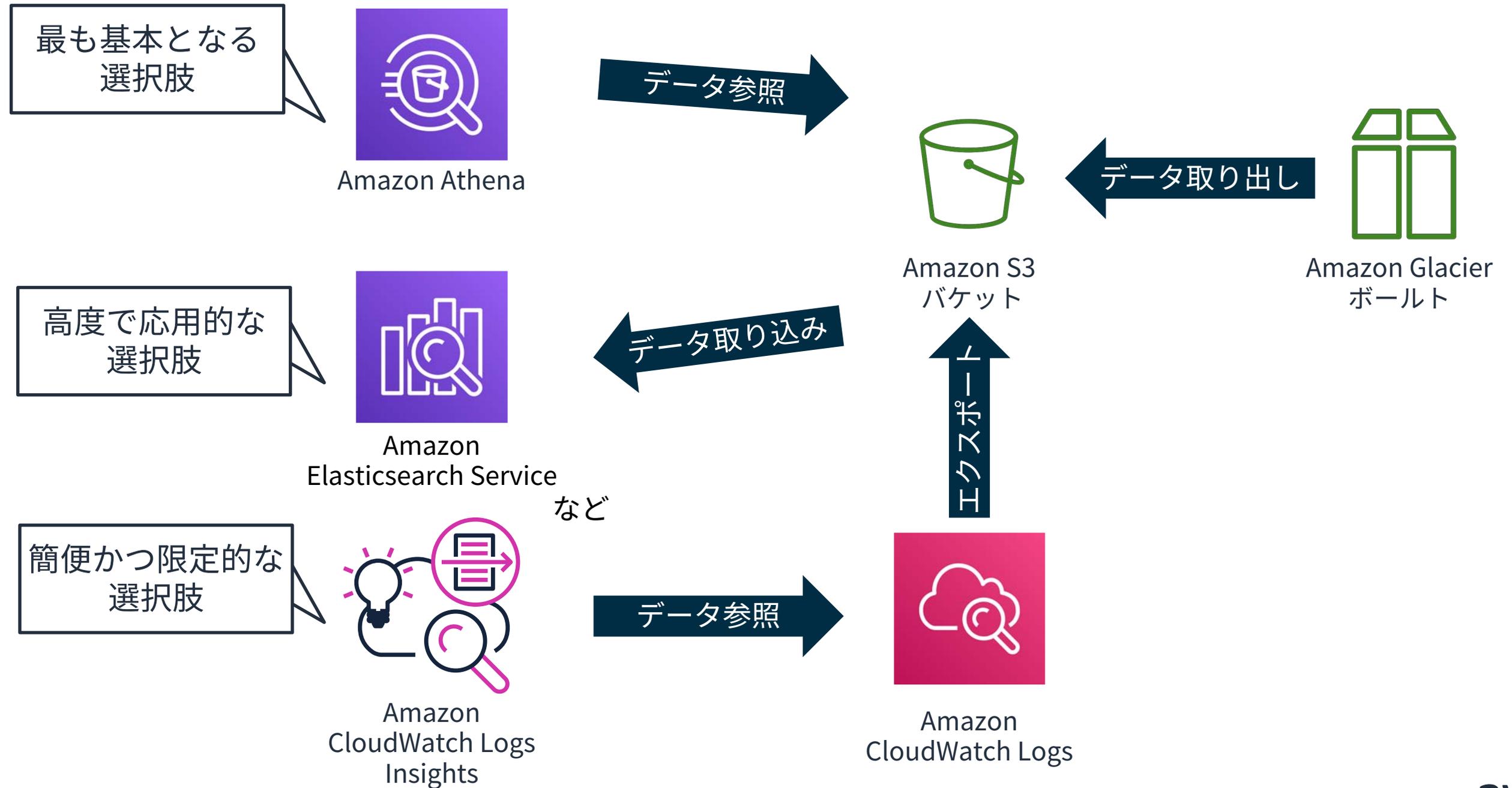
AWS CLI を使用して CloudTrail イベントを表示する

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

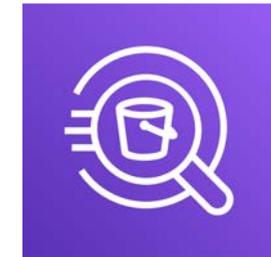
保存場所ごとの適した調査手法



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



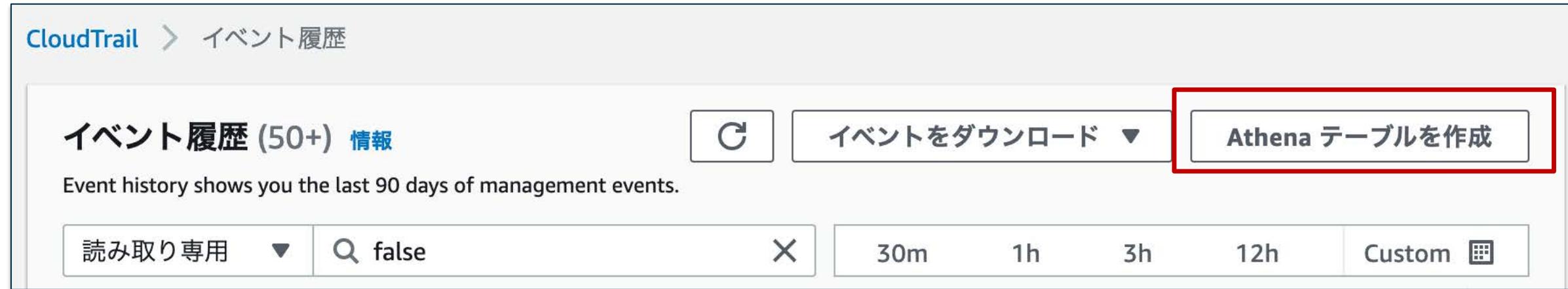
Amazon
Athena

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

データソース [データソースを接続する](#)

AwsDataCatalog

データベース

default

テーブルとビューのフィルタリング...

▼ テーブル (1) [テーブルの作成](#)

▼ cloudtrail_logs

- eventversion (string)
- useridentity (struct<type:string,principalId: eventtime (string)
- eventsourcesource (string)
- eventname (string)
- awsregion (string)
- sourceipaddress (string)
- useragent (string)
- errorcode (string)
- errorMessage (string)
- requestparameters (string)
- responseelements (string)
- additionalEventData (string)
- requestid (string)

新しいクエリ 1 +

```
SELECT useridentity.username, sourceipaddress, eventtime, additionalEventData
FROM cloudtrail_logs
WHERE eventname = 'ConsoleLogin'
and eventtime >= '2021-01-01T00:00:00Z'
and eventtime < '2021-01-18T00:00:00Z';
```

クエリの実行 名前を付けて保存 作成 (実行時間: 4.1 秒, スキャンしたデータ: 14.68 MB) クエリのフォーマット Clear

Athena engine version 1 [Release versions](#)

クエリの実行には Ctrl + Enter、オートコンプリートには Ctrl + Space を使用します

結果

username	sourceipaddress	eventtime	additionalEventData
1	203.0.113.1	2021-01-17T15:28:47Z	{"MobileVersion":"No","MFAUsed":"No"}
2	203.0.113.1	2021-01-17T15:27:58Z	{"MobileVersion":"No","MFAUsed":"No"}
3 alice	203.0.113.1	2021-01-17T19:30:15Z	{"LoginTo":"https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode"}
4	203.0.113.1	2021-01-17T23:25:51Z	{"MobileVersion":"No","MFAUsed":"No"}

SQL文で調査クエリを記述

対象期間内のコンソールログインを抜粋し全て表示した例

テーブルの定義はいつでも確認可能

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

検索条件、フィルタリング条件の指定

The screenshot displays the Amazon Elasticsearch Service console interface. At the top, there are navigation options: 'New', 'Save', 'Open', 'Share', and 'Inspect'. Below this is a search bar with a 'Search' button and a 'KQL' dropdown. To the right of the search bar, there is a date range selector set to '~ 7 months ago' to 'now' and a 'Refresh' button. Below the search bar, several filters are applied: 'eventSource: s3.amazonaws.com', 'eventName: PutObject', 'NOT sourceIPAddress: delivery.logs.amazonaws.com', 'NOT sourceIPAddress: cloudtrail.amazonaws.com', and 'NOT sourceIPAddress: athena.amazonaws.com'. A '+ Add filter' button is visible to the right of these filters.

On the left side, there is a 'log-aws-cloudtrail-*' dropdown menu. Below it, there is a 'CHANGE INDEX PATTERN' section with a search box for 'Filter options'. A list of index patterns is shown, with 'log-aws-cloudtrail-*' selected. Below this list, there are several filter options: 'event.action', 'event.ingested', and 'event.module'. A blue arrow points from the 'event.action' filter to a dark blue callout box.

The main area of the console shows a search result with '42 hits'. The time range is '06/22 09:28:31 - 01/18 09:28:31' with an 'Auto' refresh rate. A bar chart on the right shows the distribution of hits over time. Below the chart, a log entry is displayed with the following details:

```
2020-07-01 2020-08-01 2020-09-01 2020-10-01 2020-11-01 2020-12-01 2021-01-01
@timestamp per day

eventSource: s3.amazonaws.com eventName: PutObject eventVersion: 1.08 userIdentity.type: IAMUser userIdentity.principalId: AIDAR52N3XG6JBPO467NK
userIdentity.arn: arn:aws:iam::123456789012:user/blackbelt-admin userIdentity.accountId: 123456789012 userIdentity.accessKeyId: AKIAIOSFODNN7EXAMPLE
userIdentity.userName: blackbelt-admin eventTime: 01/16 15:34:14 awsRegion: ap-northeast-1 sourceIPAddress: 203.0.113.1 userAgent: [aws-sdk-nodejs/2.804.0
darwin/v14.15.3 aws-cdk/1.80.0 callback] requestParameters.bucketName: cdktoolkit-stagingbucket-11a3yvzxo3lfb requestParameters.Host: cdktoolkit-stagingbucket-
11a3yvzxo3lfb.s3.ap-northeast-1.amazonaws.com requestParameters.key: cdktoolkit-stagingbucket-11a3yvzxo3lfb.s3.ap-northeast-1.amazonaws.com requestParameters.key: cdktoolkit-stagingbucket-11a3yvzxo3lfb.s3.ap-northeast-1.amazonaws.com responseElements.x-
```

At the bottom of the console, there are links for 'View surrounding documents' and 'View single document'. Below the log entry, there are fields for '@id' (bc1ca4f0-6835-42f8-921a-806c1aef2c34) and '@log_s3bucket' (aes-siem-132770412988-log).

Amazon S3のPutObjectイベントから
特定の条件を除外し抽出した例

複数ログの
横断的分析指定

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

CloudWatch > CloudWatch Logs > Logs Insights

① ロググループを選択 (複数選択可)

② 期間を選択

ロググループを選択

2020-05-01 (00:00:00) > 2021-01-18 (23:59:59)

クリア aws-cloudtrail-logs-123456789012 X

```
1 filter eventName="CreateUser"
2 | fields awsRegion, requestParameters.userName, responseElements.user.arn
```

クエリの実行 保存 履歴

③ クエリを記述

ログ 可視化

結果をエクスポート ▼ ダッシュボードに追加

1 の 1 の一致したレコードの表示 ⓘ

22,685 レコード (34.3 MB) が 4.2s @ 5,341 records/s (8.1 MB/s) でスキャンされました

ヒストグラムを非表示

#	awsRegion	requestParameters.userName	responseElements.user.arn
▼ 1	us-east-1		
フィールド	値		
@ingestionTime	1610912812229		
@log	123456789012:aws-cloudtrail-logs-123456789012		
@logStream	123456789012_CloudTrail_us-west-2		
@message	{"eventVersion": "1.08", "userIdentity": {"type": "AssumedRole", "principalId": "AROAIIDPPEZS35WEXAMPLE:alice", "arn": "arn:aws:iam::123456789012:role/IamAdminRole/alice"}, "eventTime": "2020-05-01T00:00:00Z", "eventName": "CreateUser", "awsRegion": "us-east-1", "errorCode": "AccessDenied", "errorMessage": "User: arn:aws:sts::123456789012:assumed-role/IamAdminRole/alice is not authorized to perform: iam:CreateUser on resource arn:aws:iam::123456789012:role/IamAdminRole/alice"}.		
@timestamp	1610912812177		
awsRegion	us-east-1		
errorCode	AccessDenied		
errorMessage	User: arn:aws:sts::123456789012:assumed-role/IamAdminRole/alice is not authorized to perform: iam:CreateUser on resource arn:aws:iam::123456789012:role/IamAdminRole/alice		

対象期間内のユーザー作成イベントを抜粋し可視化した実行例

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

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

この値からロールを利用したプリンシパルを確認

※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

プリンシパルを特定したいロールが実行したイベント

```
"userIdentity": {  
  "type": "AssumedRole",  
  "principalId": "AROAI DPPEZS35WEXAMPLE:MySessionName",  
  "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",  
  "accountId": "123456789012",  
  "accessKeyId": "AKIAI...",  
  "sessionContext": {  
    "attributes": { "m..."},  
    "sessionIssuer": {  
      "type": "IAMUser",  
      "principalId": "AIDAAAAAAAAAAAAAAAAAAAA",  
      "arn": "arn:aws:iam::123456789012:user/Alice",  
      "userName": "Alice",  
      "eventSource": "AssumeRole",  
      "responseElements": {  
        "assumedRoleUser": {  
          "assumedRoleId": "AROAI DPPEZS35WEXAMPLE:MySessionName",  
          "arn": "arn:aws:sts::123456789012:assumed-role/RoleToBeAssumed/MySessionName",  
        }  
      }  
    }  
  }  
}
```

※一部要素省略

AssumeRoleイベント

※一部要素省略

① 対応するIDを探索

② UserIdentityを参照

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

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
GuardDuty



AWS CloudTrail
Insights

など



Amazon CloudWatch
Logs



Amazon
Elasticsearch
Service

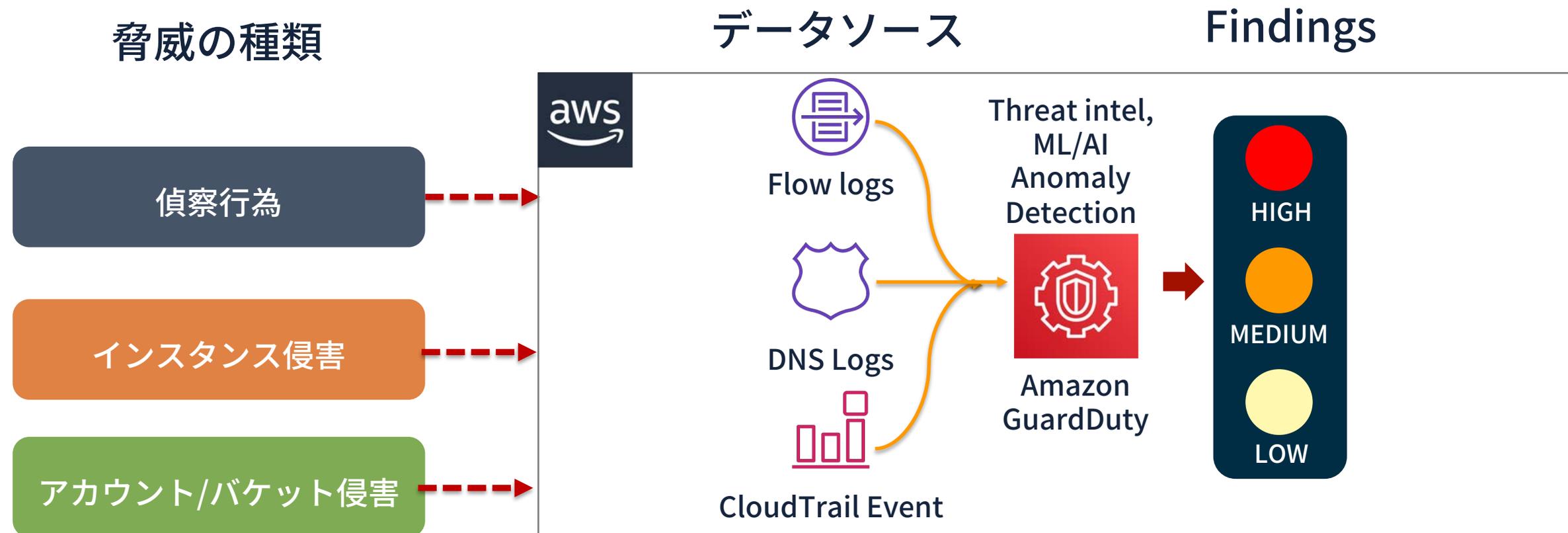
など

サービスを有効化するのみで
自動的にモニタリング

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

RunInstances APIの
コールレート上昇を
検知し確認した例

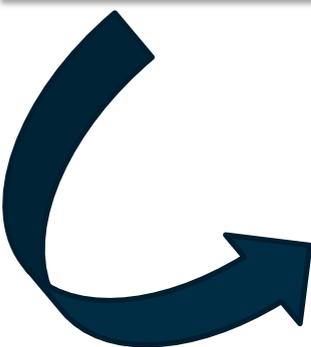
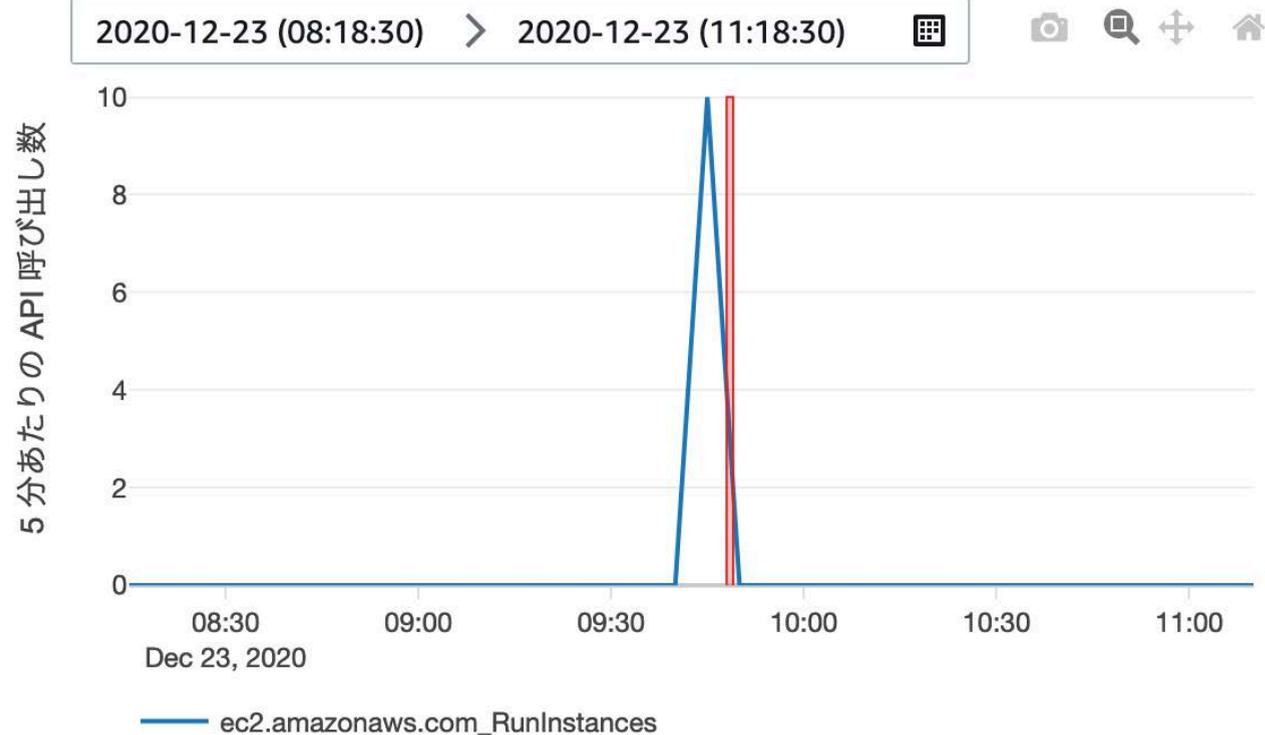
Insights (7) 情報

ルックアップ属性キーを選択 ▼ 🔍 ルックアップ値を入力

30m 1h 3h 12h Custom 1

イベント名	イベント開始時刻	イベントソース	API コールレートの...
TerminateInstances	December 23, 2020, 10:10:00 ...	ec2.amazonaws.com	300% ↑
PutEvaluations	December 23, 2020, 09:50:00 ...	config.amazonaws.com	120% ↑
RunInstances	December 23, 2020, 09:48:00 ...	ec2.amazonaws.com	500% ↑

Insights グラフ 情報



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

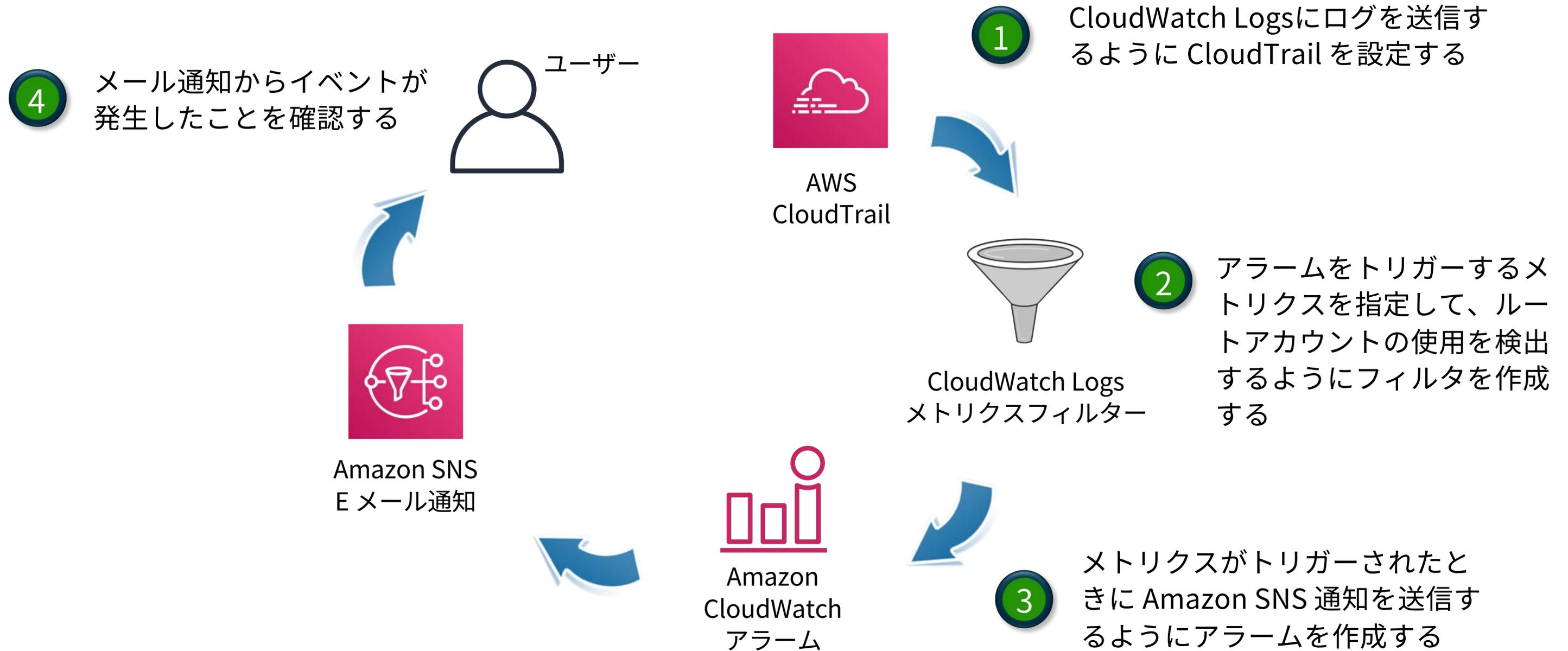
CloudWatch > Log Groups > PostgreSQL1 > PostgreSQL-Logs

Expand all Row Text   

“LOG” all 30s 5m 1h 6h 1d 1w custom ▾

Time (UTC +01:00)	Message
▶ 16:17:43	2019-05-17 ::: @ >LOG: database system was shut down at 2019-05-17 16:17:42 EST
▶ 16:17:43	2019-05-17 ::: @ >LOG: MultiXact member wraparound protections are now enabled
▶ 16:17:43	2019-05-17 ::: @ >LOG: database system is ready to accept connections
▼ 16:17:43	2019-05-17 :: [unknown] : [unknown] @ [unknown] >LOG: connection received : host=12...
2019-05-17 :: [unknown] : [unknown] @ [unknown] >LOG: connection received : host = 120.154.68.29 port = 56329	

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

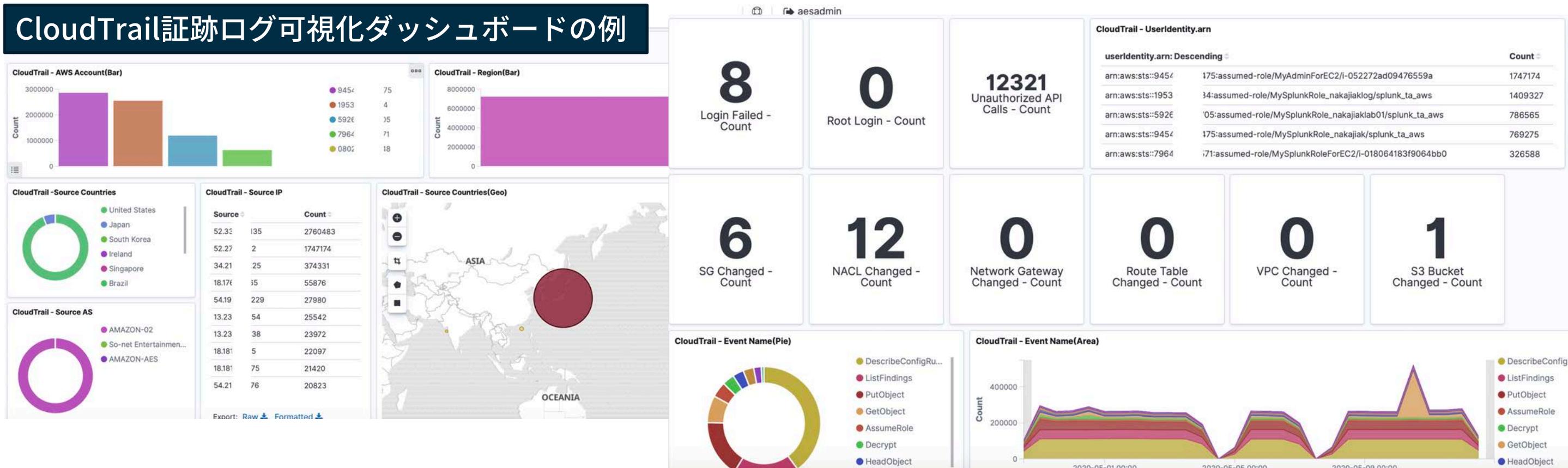
ネットワーク構成変更

- AttachInternetGateway
- AssociateRouteTable
- CreateRoute
- DeleteCustomerGateway
- DeleteInternetGateway
- DeleteRoute
- DeleteRouteTable
- DeleteDhcpOptions
- DisassociateRouteTable
- CreateNetworkAcl
- CreateNetworkAclEntry
- DeleteNetworkAcl
- DeleteNetworkAclEntry
- ReplaceNetworkAclEntry
- ReplaceNetworkAclAssociation

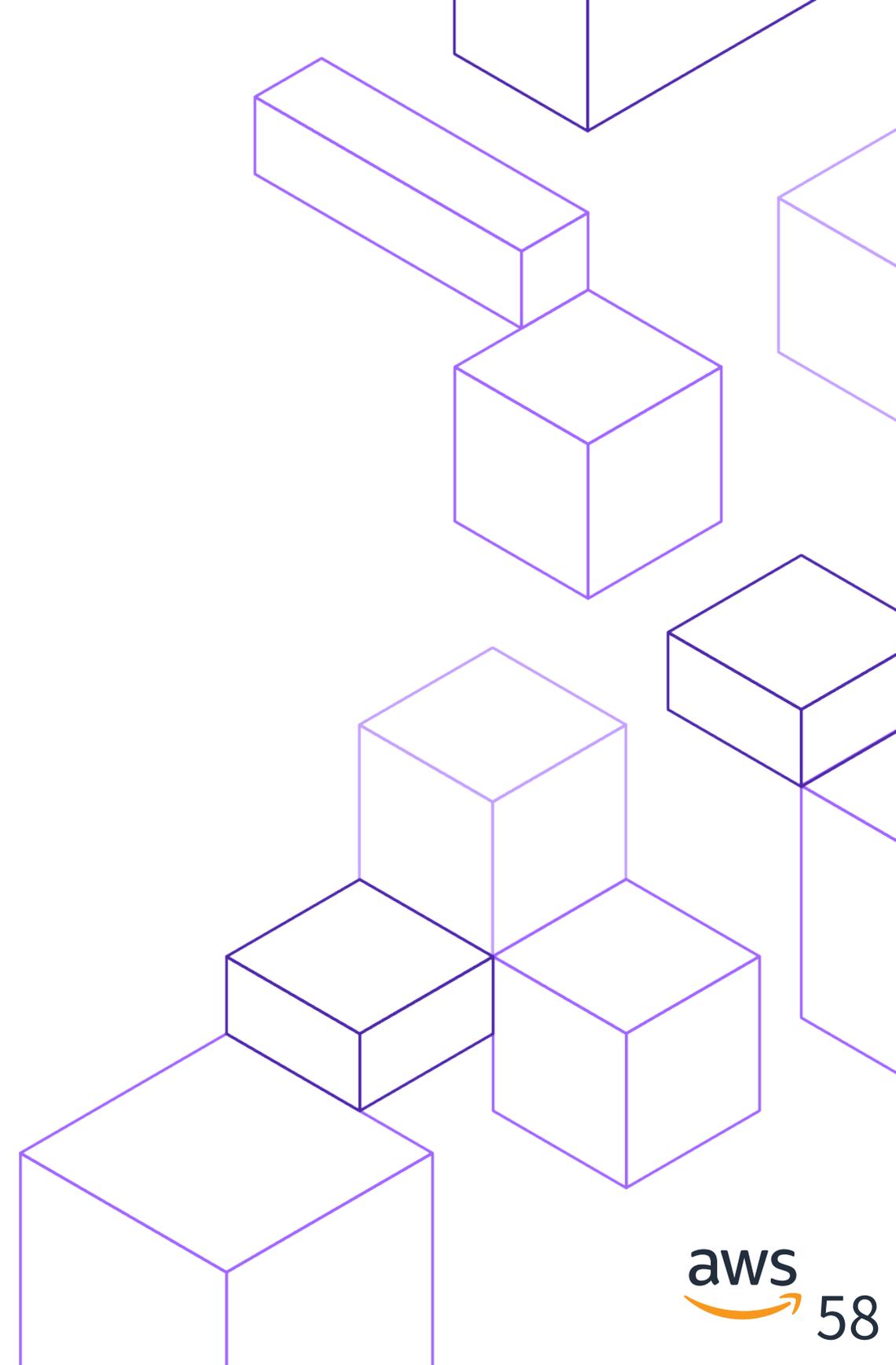
SIEM on Amazon Elasticsearch Service (Amazon ES)

- 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



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 GuardDuty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

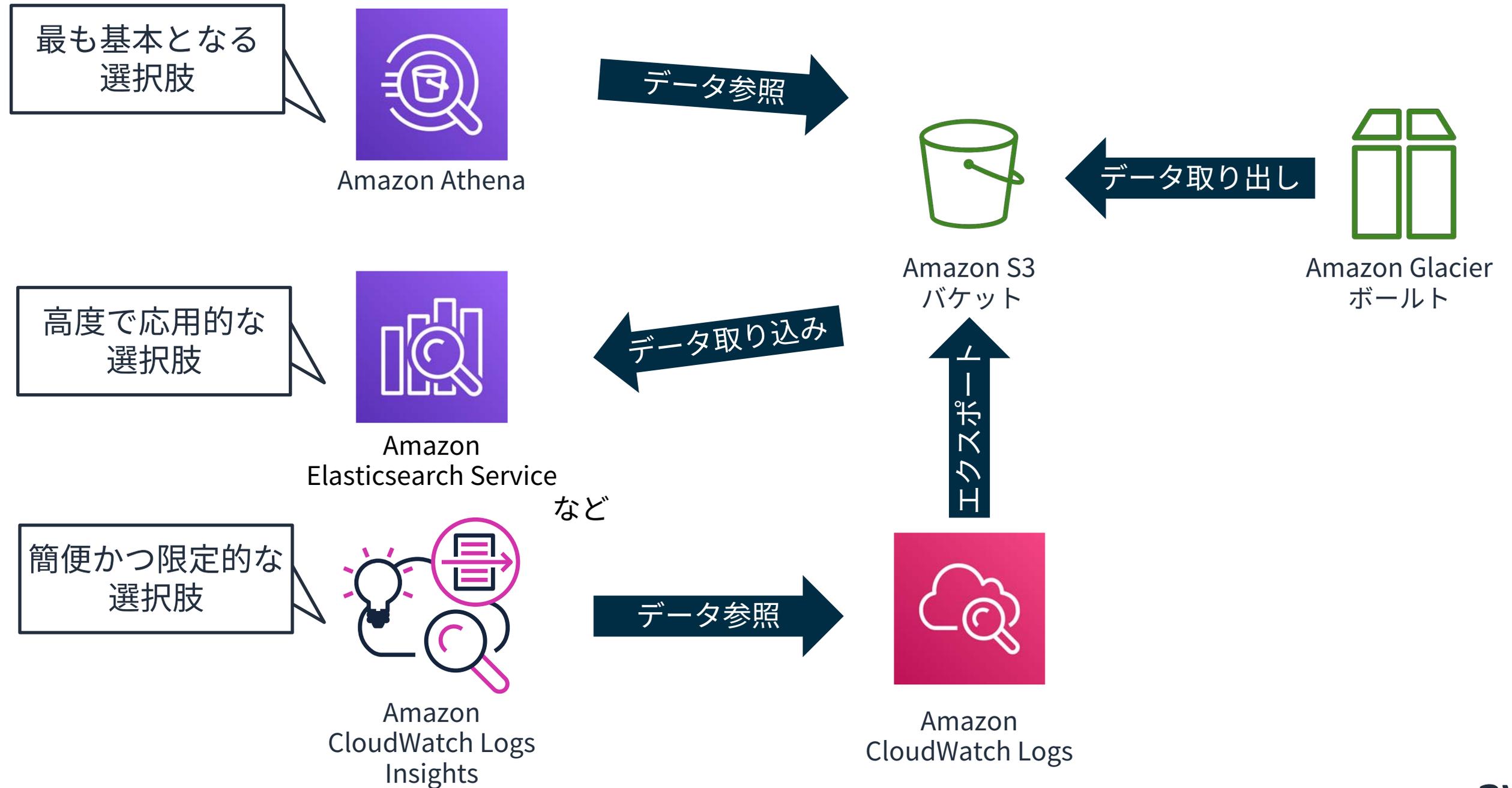
AWS CloudTrail セキュリティのベストプラクティス抜粋

- 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

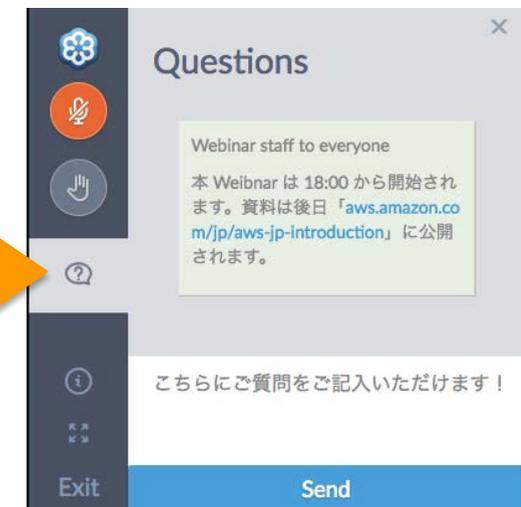
AWS Japan Blog 「<https://aws.amazon.com/jp/blogs/news/>」にて後日掲載します。

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



The screenshot shows the AWS Japanese website header with the AWS logo, navigation links for '製品', 'ソリューション', '料金', 'ドキュメント', '学習', 'パートナー', 'AWS Marketplace', and 'その他', and a search icon. The main heading is 'AWS クラウドサービス活用資料集トップ'. Below it is a paragraph of introductory text in Japanese. At the bottom, there are four buttons: 'AWS Webinar お申込', 'AWS 初心者向け', '業種・ソリューション別資料', and 'サービス別資料'.

aws

日本担当チームへお問い合わせ サポート 日本語 ▼ アカウント ▼ コンソールにサインイン

製品 ソリューション 料金 ドキュメント 学習 パートナー AWS Marketplace その他 Q

AWS クラウドサービス活用資料集トップ

アマゾン ウェブ サービス (AWS) は安全なクラウドサービスプラットフォームで、ビジネスのスケールと成長をサポートする処理能力、データベースストレージ、およびその他多種多様な機能を提供します。お客様は必要なサービスを選択し、必要な分だけご利用いただけます。それらを活用するために役立つ日本語資料、動画コンテンツを多数ご提供しております。(本サイトは主に、AWS Webinar で使用した資料およびオンデマンドセミナー情報を掲載しています。)

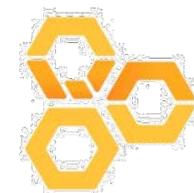
AWS Webinar お申込 » AWS 初心者向け » 業種・ソリューション別資料 » サービス別資料 »

<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



AWS Well-Architected

- 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>

