
aws
SUMMIT
ONLINE

HOL-07

アカウント取得後すぐやるセキュリティ対策

大松　宏之
ソリューションアーキテクト
アマゾン ウェブ サービス ジャパン株式会社

aws SUMMIT ONLINE

Agenda

概要

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

ベストプラクティスの確認

注意事項

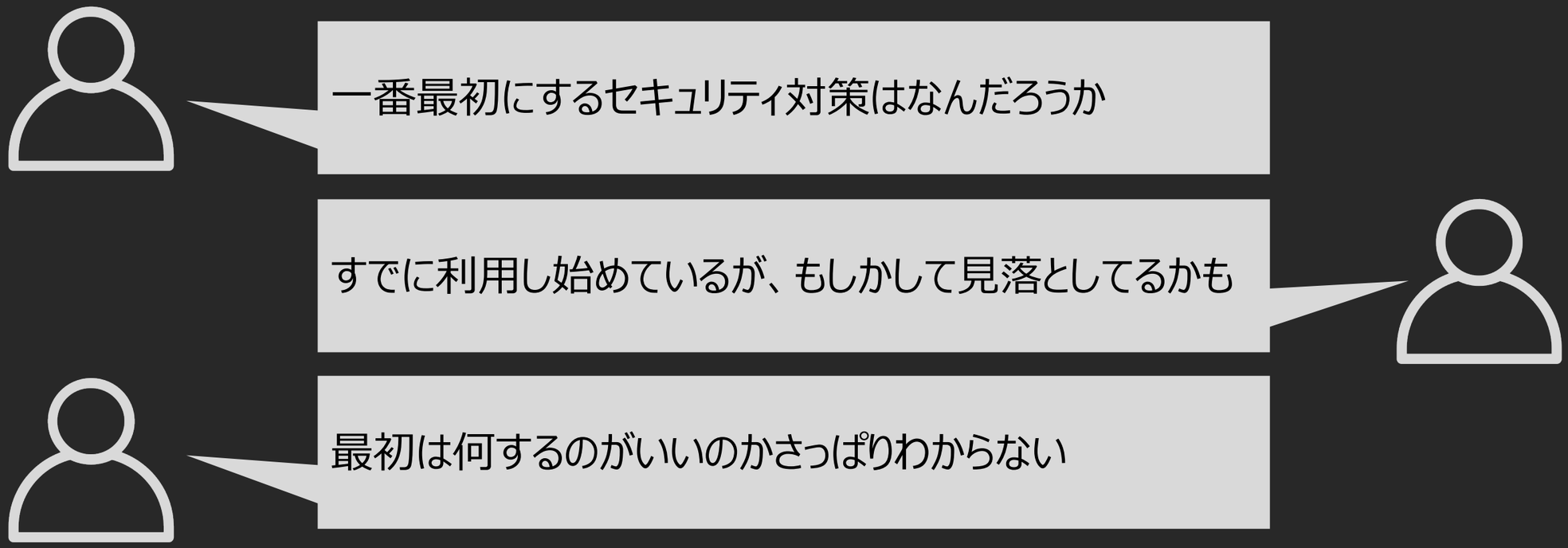
- 資料は07/10日時点のサービス内容および価格についてご説明しています。
  最新の情報はAWS公式ウェブサイト(http://aws.amazon.com)にてご確認ください。 資料作成には十分注意しておりますが、資料とAWS公式ウェブサイトとで記載内容に相違があった場合、AWS公式ウェブサイトの記載を優先させていただきます。
- マネージメントコンソールについても、収録時点のものとなります。
  差異がある場合がございますので、ご注意ください
- 学習後のリソースの削除は、お客様の責任でご実施いただくようお願いいたします。
- ハンズオンでは AWS の各種サービスの利用、リソースの作成を行います。
  無料枠を超えるハンズオンもございますが、その場合はご利用料金が発生することを
  あらかじめご認識ください。

概要

aws SUMMIT ONLINE

概要

こんなふうに思ったことはないですか？



概要

このハンズオンで利用するサービス

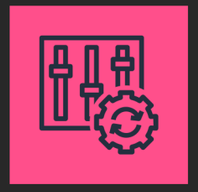
(注)一部のハンズオンでは、データの保存のために Amazon Simple Storage Service (Amazon S3) を利用

ID アクセス権管理
AWS Identity & Access Management

AWS Trusted Advisor

発見的統制
AWS CloudTrail

請求
AWS Budgets



発見的統制
AWS Config

請求
AWS Cost Explorer

発見的統制
Amazon GuardDuty

請求
AWS Cost & Usage Reports

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

ベストプラクティスの確認

IDアクセス権管理

aws SUMMIT ONLINE

ID アクセス権管理

- 不必要な権限を付与していると、情報の流出や破壊、不正閲覧や改ざん、不正使用、サービス自体の中断などが起こる場合がある

- 特権アカウントは厳重に管理し、利用者へ与える権限は必要最小限に絞り、アカウントへの不正アクセス対策を実施することは基本

ID アクセス権管理

AWS Identity & Access Management (AWS IAM)

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(*1)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(*1)に伝搬
- AWS IAM自体の利用は無料

(*1) 中国、GovCloudリージョンは除く

ルートユーザーとIAMユーザー

ルートユーザー

- メールアドレス+パスワードでログイン
- 全AWSサービスとリソースに対して完全なアクセス権限
- 日常的なタスクには使わない

IAMユーザー

- アカウントID + IAMユーザー名 + パスワードでログイン
- 紐づいている IAM ポリシー権限で許可された操作のみ可能
- 利用者ごとにIAM ユーザーを作成し、利用者はそのユーザーでログインし、作業を進めていく

AWS IAM のベストプラクティス

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

（参考）IAM のベストプラクティス
https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

ハンズオンで実施すること

1.ルートユーザーの多要素認証の有効化
2.ルートユーザーのアクセスキーの削除
3.IAMユーザー/ロールによる請求情報へのアクセス
4.IAMパスワードポリシーの適用
5.IAMグループの作成
6.IAMユーザーの作成
7.IAMユーザーのMFA有効化
8.IAMユーザー/ロールによる請求情報へのアクセス

ハンズオン

ルートユーザーでログインしてください

aws SUMMIT ONLINE

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

ベストプラクティスの確認

請求データの確認とアラート

aws SUMMIT ONLINE

セキュリティイベントの重要な指標

セキュリティ関連のイベントを検出する指標の例

ログとモニタリング

請求データ

脅威インテリジェンス

パートナーツール

連絡先

AWSからの連絡

セキュリティイベントの重要な指標

セキュリティ関連のイベントを検出する指標の例

ハンズオンするのはこちら

ログとモニタリング

請求データ

脅威インテリジェンス

パートナーツール

連絡先

AWSからの連絡

セキュリティイベントの重要な指標

セキュリティ関連のイベントを検出する指標の例

ハンズオンするのはこちら

ログとモニタリング

請求データ

脅威インテリジェンス

パートナーツール

連絡先

AWSからの連絡

セキュリティイベントの指標としての請求データ

AWS Budgets
一定額以上の利用が発生した場合にアラートを飛ばす

AWS Cost Explorer
コストと使用状況を分析

AWS Cost & Usage Reports
コストと使用状況レポートを保存

ハンズオンで実施すること

1. AWS Cost Explorer の有効化と確認
2. AWS Budgets を使った請求アラート
3. AWS Cost & Usage Reportsの設定

発生するコスト

AWS Budgets : 2つの予算までは無料で作成可能

AWS Cost & Usage Reports : レポートの保存先のS3の料金

ハンズオン

IAMユーザーでログインしてください

aws SUMMIT ONLINE

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

ベストプラクティスの確認

操作履歴とリソース変更履歴の記録

aws SUMMIT ONLINE

操作履歴とリソース変更履歴の記録

セキュリティ対策の一環として、利用者の操作ログを記録・管理することは不可欠

「いつ」「だれが」「どのリソースを」「どのように操作したか」「結果どうなったのか」といった情報などがログに適切に記録されている必要がある


ログとモニタリング


請求データ


脅威インテリジェンス


パートナーツール

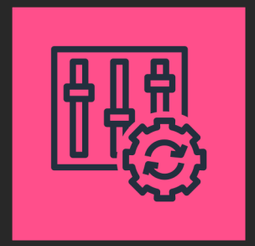

連絡先

aws
AWSからの連絡

操作履歴とリソース変更履歴の記録

AWS CloudTrail

AWSのサービスを利用する際の行動履歴をログに記録し、継続的に監視し、保持することが可能



AWS Config

リソースの変更履歴、構成情報を管理・監視することが可能

コンプライアンス準拠、運用監査、リスク監査、セキュリティ分析、変更管理、運用上のトラブルシューティングの負担を軽減できます

ハンズオンで実施すること

1. AWS CloudTrail の証跡の保存
2. AWS Config の有効化

発生するコスト

AWS CloudTrail : 証跡の保存先のS3の料金

AWS Config : 設定履歴ファイルの保存先のS3の料金

AWS Config : 記録された設定項目あたりの料金

ハンズオン

IAMユーザーでログインしてください

aws SUMMIT ONLINE

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

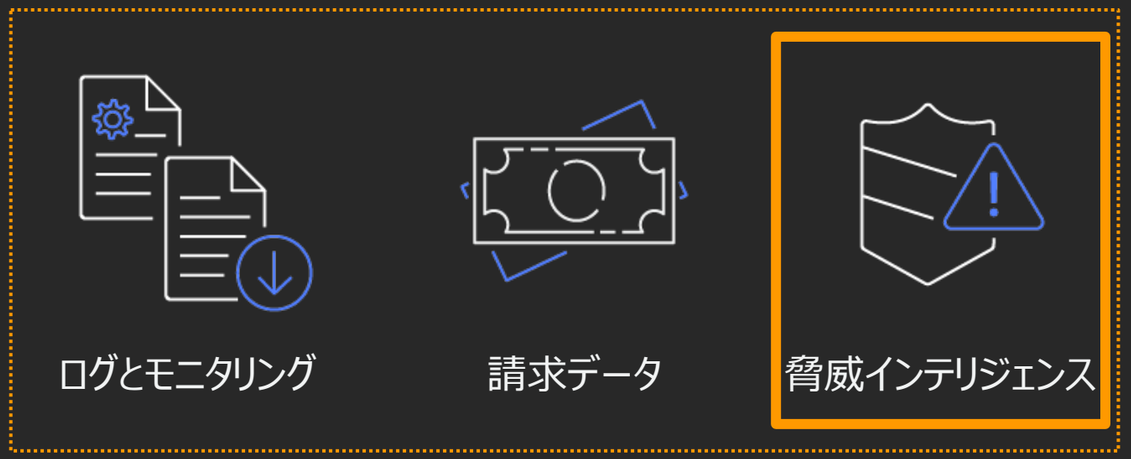
ベストプラクティスの確認

脅威検知

aws SUMMIT ONLINE

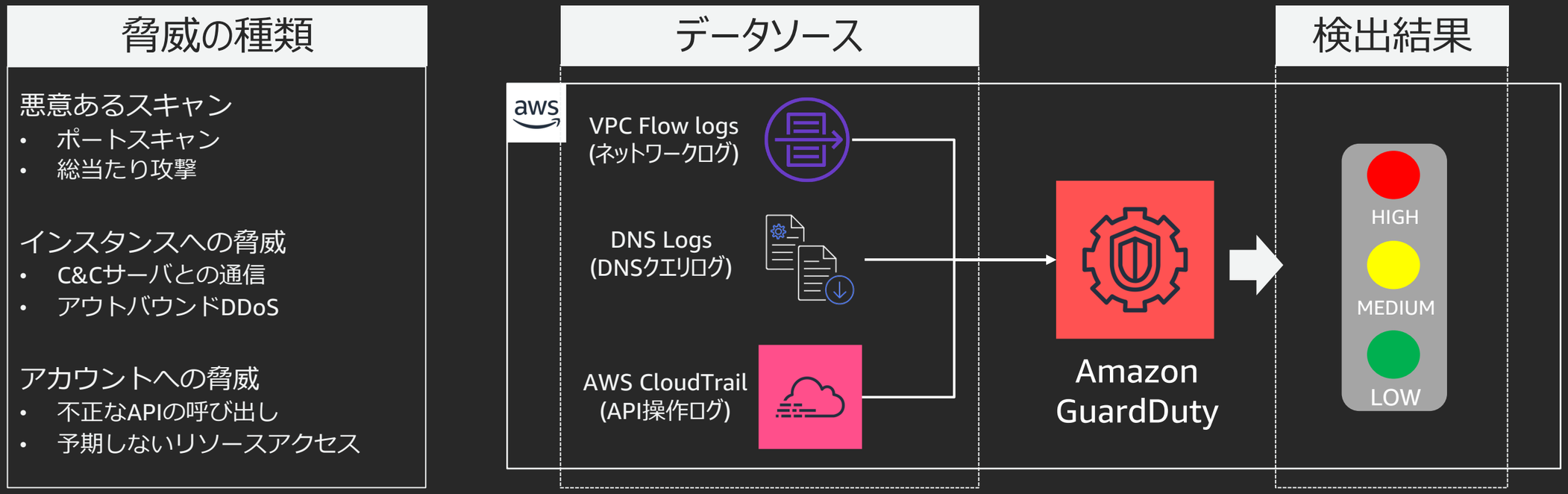
脅威インテリジェンスを利用した脅威検知

脅威インテリジェンスとは、脅威の防止や検知に利用できる情報の総称



継続的監視と脅威検知 – Amazon GuardDuty

機械学習を用いたクラウドネイティブな脅威検知サービス



（参考）検知可能な脅威
https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_finding-types-active.html

このハンズオンで実施すること

1. Amazon GuardDuty の有効化

発生するコスト

Amazon GuardDuty : 30日無料ののち、分析したログの量に応じた料金

ハンズオン

IAMユーザーでログインしてください

aws SUMMIT ONLINE

IDアクセス権管理

請求データの確認とアラート

操作履歴とリソース変更履歴の記録

脅威検知

ベストプラクティスの確認

ベストプラクティスの確認

aws SUMMIT ONLINE

ベストプラクティスの確認

こんな不安はありませんか？

自分たちの設定がAWSのベストプラクティスに沿っているのか心配

使っていないリソースがあれば、停止してリスクを減らしたい

他にもセキュリティ設定で見落としがないだろうか？

ベストプラクティスの確認

AWS Trusted Advisor

AWS 環境を自動監視、最適化するための推奨ベストプラクティスを提供

ベストプラクティスは五つのカテゴリに分類

- コスト最適化
- パフォーマンス
- セキュリティ
- フォールトトレランス
- サービス制限

このハンズオンで実施すること

1. AWS Trusted Advisor の確認

ハンズオン

IAMユーザーでログインしてください

aws SUMMIT ONLINE

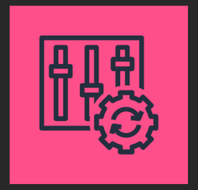
まとめ（再掲）

このハンズオンで利用したサービス

(注)一部のハンズオンでは、データの保存のために Amazon Simple Storage Service (Amazon S3) を利用

ID アクセス権管理
AWS Identity & Access Management

発見的統制
AWS CloudTrail



発見的統制
AWS Config

発見的統制
Amazon GuardDuty

AWS Trusted Advisor

請求
AWS Budgets

請求
AWS Cost Explorer

請求
AWS Cost & Usage Reports

作成したリソースの削除

aws SUMMIT ONLINE

作成したリソースの削除

実施した内容は、AWS環境を保護しリスクに対応するための重要な設定

継 続 し て 利 用 す る こ と を 推 奨

作成したリソースの削除

AWS Budgets

- 予算削除

AWS Budgets Report

- レポート削除

AWS Cost & Usage Reports

- レポート削除

AWS CloudTrail

- 証跡情報の削除

AWS Config

- 記録のオフ

Amazon GuardDuty

- 無効化

S3 バケット削除

- AWS Cost & Usage Report
- AWS CloudTrail
- AWS Config

Thank you!

aws SUMMIT ONLINE

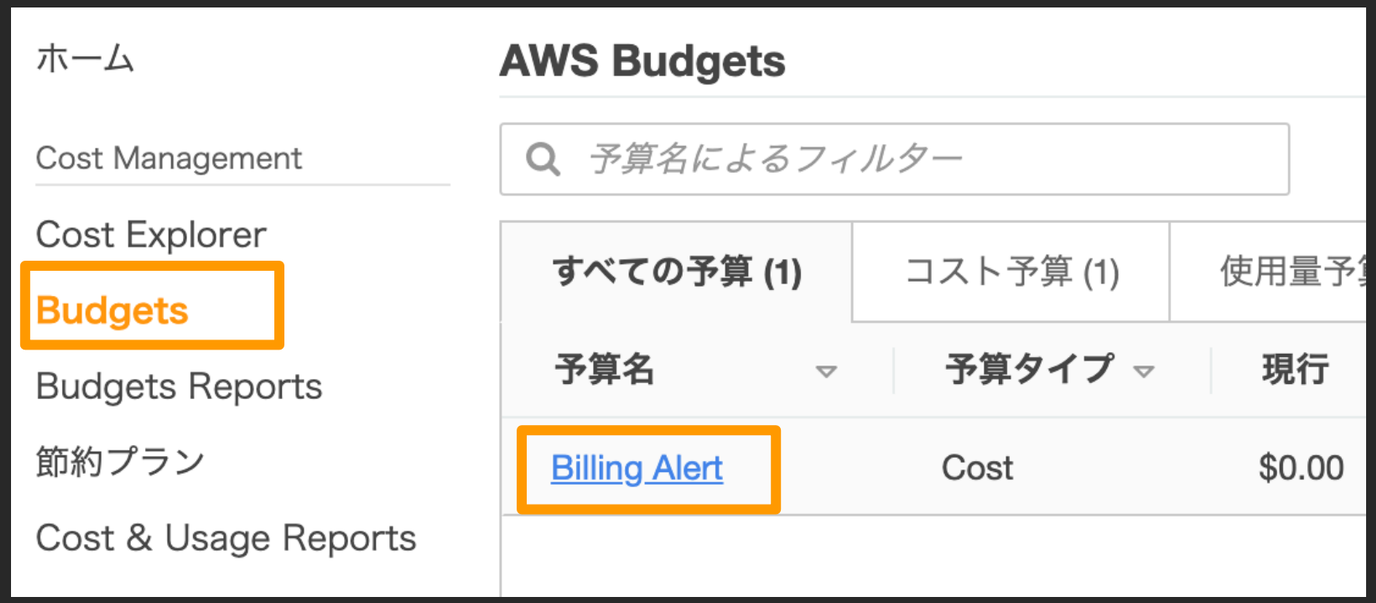
アンケートへの回答を
お願いいたします。

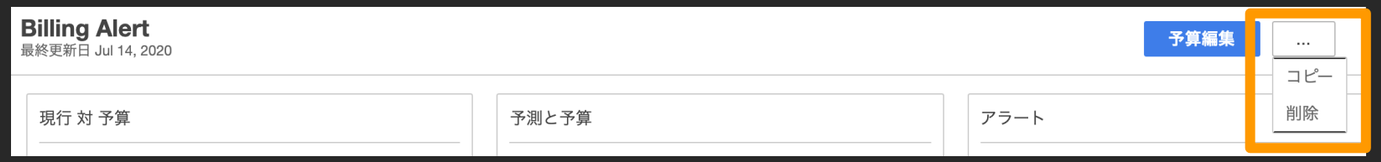
aws SUMMIT ONLINE

リソースの削除手順

aws SUMMIT ONLINE

AWS Budgets の削除





1. Billing の管理画面にアクセスし、Budgets をクリック
2. 作成した予算名をクリック
3. 右上の[...]をクリックして、削除を選択

AWS Budgets Report の削除

1. Billing の管理画面にアクセスし、Budgets Reports をクリック
2. 作成したレポート名の右にある[…]をクリックして、削除を選択

AWS Cost & Usage Reports の削除

1. Billing の管理画面にアクセスし、Cost & Usage Reports をクリック
2. 作成したレポート名をチェック
3. 削除ボタンクリックして、削除
4. 確認画面でもう一度削除をクリック

AWS CloudTrail の証跡を削除

1. CloudTrail の管理画面にアクセスして、証跡情報をクリック
2. 証跡情報から、作成した証跡名をクリック
3. 画面右上の[ゴミ箱]アイコンをクリック
4. 確認画面で削除ボタンをクリック

AWS Config の無効化

1. AWS Config の管理画面にアクセスして、設定をクリック
2. オフにするボタンをクリックして、無効化

Amazon GuardDuty の無効化

1. GuardDuty の管理画面にアクセスして、設定をクリック
2. GuardDuty の無効化ボタンをクリック
3. 確認画面で再度無効化をクリック

Amazon S3 のバケットを空にする

注意事項
- バケットを削除するためには一度空にする必要があります
- 収録時点でのS3のインターフェイスになり、差異がある場合がありますが、空にしてから削除する操作に変わりはありません

1. S3 の管理画面にアクセスして、以下の 3 つのサービスで利用したバケットを確認
    1. Cost & Usage Reports
    2. Cloudtrail
    3. AWS Config
2. 対象のバケットをチェックして、空にするボタンをクリック
3. 確認画面でバケット名を入力して、確認ボタンをクリック
4. 対象のバケット全てに2~3を行う

Amazon S3 のバケット削除

1. 対象のバケットをチェックして、削除ボタンをクリック
2. 確認画面でバケット名を入力して、確認ボタンをクリック
3. 対象のバケット全てに1~2を行う

リソースの削除手順

以上で、リソースの削除は終了です