多要素認証MFA有効にする

管理者のIAMユーザーを作成する

AWS CloudTrail有効化

AWS請求アラート有効化

多要素認証MFA有効にする

IAMコンソール画面で多要素認証を有効化する

Google　Authenticator　インストールしてMFA用ツールとして設定する

IAMコンソール画面でパスワードポリシーを変更する

管理者のIAMユーザーを作成する

AWSマネジメントコンソールでIAMユーザを新規作成IAMポリシーにより管理者権限を実行する

IAM　（Identity　Access　Management）

個人用作成

認証情報タイプはどちらもチェックがベター

AWS管理者権限付与

既存のポリシーを直接アタッチ→[AdministratorAccess](https://console.aws.amazon.com/iam/home#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)

タグ

特定の情報を付与できる

分類わけなどの際に使おう

アクセスキーとシークレットアクセスキーはCLIでのログインで使う

CSVで保存可能

グループ用作成も可能

CloudTrail　ログを取得する

APIコールや　アクティビティログ

S３に暗号化されて保存

デフォ90日有効

クラウドウォッチ上で可視化できる

証跡を有効化

S3を設定

イベント履歴

アクティビティ履歴

証跡は自動でとられるが90日で消滅

インサイト

証跡に対して何らかの解析が出せる

S3はストレージ：データの保存場所

KMS暗号化とは

ログを暗号化すること

有効にしたらカギを設定すること　今回は無し

ログファイルの検証

ログファイルがしっかりしてるか検証してくれる

SNS 通知の配信

イベントが発生したときSNS通知してくれる

**CloudWatch Logs *- オプション***

　有料

　ログをCloud Watchに上げてくれる

ログイベント

管理イベント

データイベント

Insigtsイベント

基本的にはチェック

管理イベント

　読み取り書き取り　基本的にはチェック

　KMSイベントチェック無し

　RDSのイベントは応用

Insightは異常検知

　追加料金あり

請求アラートの設定

料金の使い過ぎを事前にキャッチ

ルートアカウントで実行

設定でIAMで設定できるようにしないといけませんよと

請求ダッシュボードで請求アラート設定を有効化

Cloud Watchでアラートを設定する

マイアカウントからIAMで可視化できるようになる設定あり

確認できず

Cost　Exproror

視覚的に使用容共を見れる

Budget

リソースごとに予算を決められるアラームできる

Cloud Watch

様々なクラウドサービスへのメトリクスを所持している

リソース立ち上げると自動で取得される