AWS Builders Online Series

今日からスタート！ AWS セキュリティ 初めの一歩

勝原 達也

アマゾン ウェブ サービス ジャパン合同会社
AWS 技術統括本部 技術推進本部
セキュリティ ソリューションアーキテクト

自己紹介

勝原 達也（かつはら たつや）

セキュリティ ソリューション アーキテクト

・SIer でデジタル・アイデンティティと認証・認可セキュリティ
・セキュリティ専門会社で Web、工場・プラント、IoT・自動車のセキュリティ
・AWS 活用におけるセキュリティ課題解決をサポート

好きな AWS サービス：

Amazon Cognito、AWS Single Sign-On、AWS IoT

このセッションでお話しすること

Builders Online では、お客様のビジネスに活用いただけるサービスを、
多数ご紹介するセッションをご提供しています

本セッションでは、みなさまが安心して各サービスをお試しいただくためにも、
AWS アカウントを取得したらすぐに取り組んでいただきたい、
AWS セキュリティの「初めの一歩」について、厳選してご紹介します

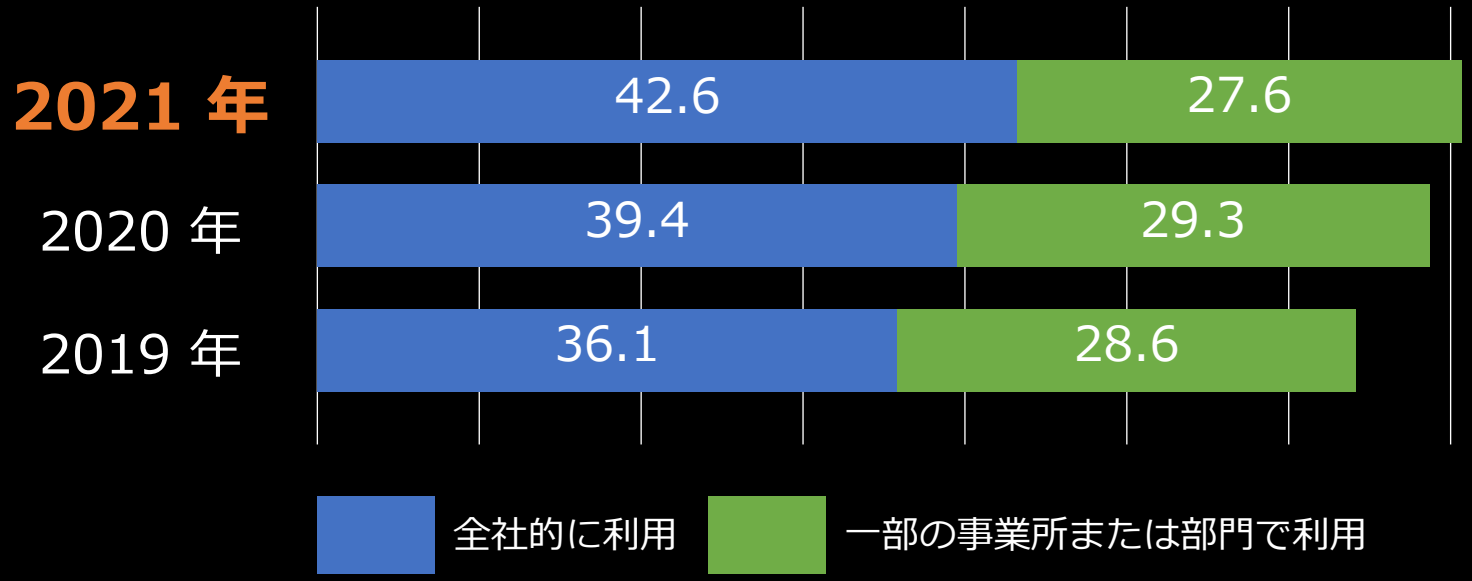
関連する AWS サービスのポイントやメリットにフォーカスして
お届けするため、サービスの機能詳細については各サービスの公式ドキュメントを
合わせてご確認ください

アジェンダ

- AWS におけるセキュリティの考え方
- 実施していただきたい初めの一歩
  - AWS アカウントをセキュアにしよう
  - AWS で起きた事実を記録しよう
  - セキュリティ脅威を自動的に検知しよう
  - コスト面での「安心」を確保しよう
  - 継続的な改善へ取り組もう
- まとめ

AWS における
セキュリティの考え方

クラウドサービスの利用は継続して増加



クラウドを利用している企業

約 70 %

- 半数以上の企業が利用
- 利用企業数は年々増加

クラウドを活用して、ビジネス変革を進める企業が増えている

出所：総務省 令和 3 年通信利用動向調査 (企業編)

クラウド未利用企業が抱える課題

クラウド利用に踏み切れない要因としてセキュリティへの不安が挙げられている

クラウドサービスを利用しない理由 (n=317)	回答割合
情報漏えいなどセキュリティに不安がある	**27.3 %**
クラウドの導入に伴う既存システムの改修コストが大きい	26.7 %
ネットワークの安定性に対する不安がある	15.6 %
通信費用がかさむ	10.3 %
ニーズに応じたアプリケーションのカスタマイズができない	8.6 %
クラウドの導入によって自社のコンプライアンスに支障あり	4.8 %
法制度が整っていない	4.1 %

出所：総務省 令和３年通信利用動向調査 (企業編)

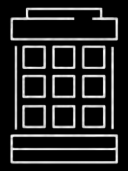
クラウド利用企業はセキュリティの優位点を認識

クラウドはセキュリティに関連する高い評価を得ている

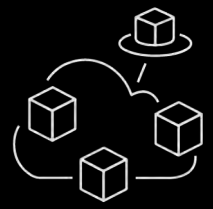
クラウドサービスを利用している理由 (n=1757)	回答割合
場所、機器を選ばずに利用できるから	49.2 %
資産、保守体制を社内に持つ必要がないから	40.9 %
安定運用、可用性が高くなるから	36.8 %
災害時のバックアップとして利用できるから	32.8 %
サービスの信頼性が高いから(情報漏えいなど対策)	**28.8 %**
システム容量の変更などに迅速に対応できるから	26.7 %
システムの拡張性が高いから(スケーラビリティ)	22.1 %
既存システムよりもコストが安いから	19.4 %

出所：総務省 令和３年通信利用動向調査 (企業編)

クラウドのセキュリティに関するギャップを埋めていくためにお伝えしたい 3 つのこと



クラウドをまだ
利用していない企業



既にクラウドを
利用している企業

クラウドのセキュリティ
に対する懸念

クラウドのセキュリティに
対する信頼と活用

**セキュリティは
AWS の最優先事項**

**AWS における
責任共有モデル**

**AWS を活用したお客様
セキュリティ統制の実現**

セキュリティは AWS の最優先事項

セキュリティ、ID、コンプライアンスのための
包括的なサービスと機能を提供

AWS クラウドセキュリティ
https://aws.amazon.com/jp/security/

独立した監査人による継続的な
セキュリティとコンプライアインスの確認を実施

コンプライアンスプログラム例

AWS コンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

▶ お客様は AWS を活用することで、柔軟かつセキュアなクラウドコンピューティング環境を実現することが可能

AWS における責任共有モデル

お客様と共に、優れたセキュリティを素早く実現するための理想的なアプローチ

AWS を活用したお客様セキュリティ統制の実現

複数の軸でセキュリティを高めながら、改善するメカニズムも組みこんでいく

予防的統制		発見的統制
あらかじめリスクを想定し それが発生しないように 予防できる対策を行うこと	＋	あらかじめリスクを想定し それが発生した場合に検知し 影響を抑える対策を行うこと

セキュリティ初めの一歩はここからはじまる

AWS アカウントをセキュアにしよう

AWS のセキュリティの根幹
AWS Identity and Access Management (IAM)

AWS Identity and Access Management (IAM)

- AWS リソースをセキュアに操作するための認証・認可を行う
- AWS の 200 以上のサービスについて同一の枠組みでアクセス管理が可能

AWS アカウントの保護において最初に実施すべきプラクティス

AWS Identity and Access Management (IAM)

ルートユーザーを通常の作業に使わない

多要素認証 (MFA) を利用しよう
※Multi Factor Authentication

ルートユーザーのアクセスキーを使わない

AWS アカウントの保護において最初に実施すべきプラクティス

AWS Identity and Access Management (IAM)

ルートユーザーを通常の作業に使わない

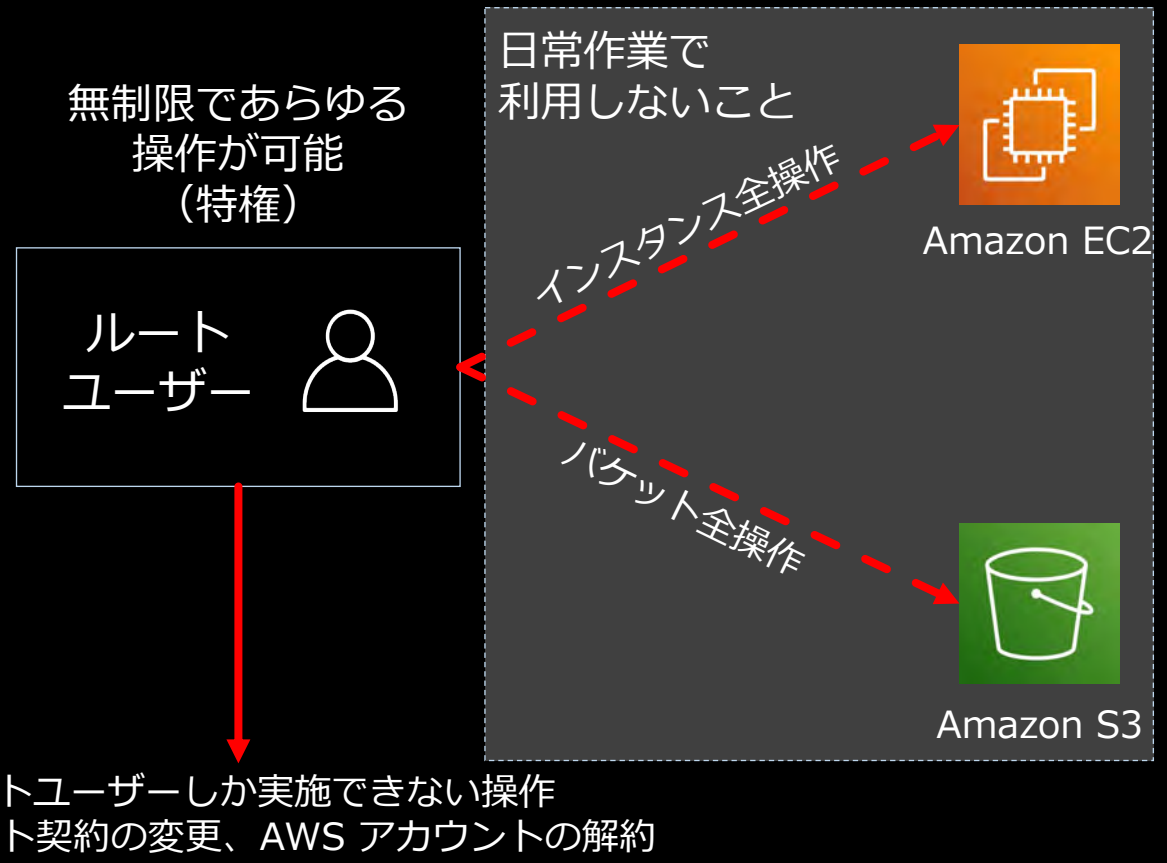
多要素認証 (MFA)を利用する
※Multi Factor Authentication

ルートユーザーのアクセスキーを使わない

特権を持つユーザー (ルートユーザー)は特別な作業を行うときだけに利用しよう

ルートユーザー

- 特権ユーザーで、全 AWS サービスとリソースに無制限のアクセス権限を持つ
- 日常作業には利用せず、ルートユーザーしか実施できない一部のタスク※を行う際に利用する

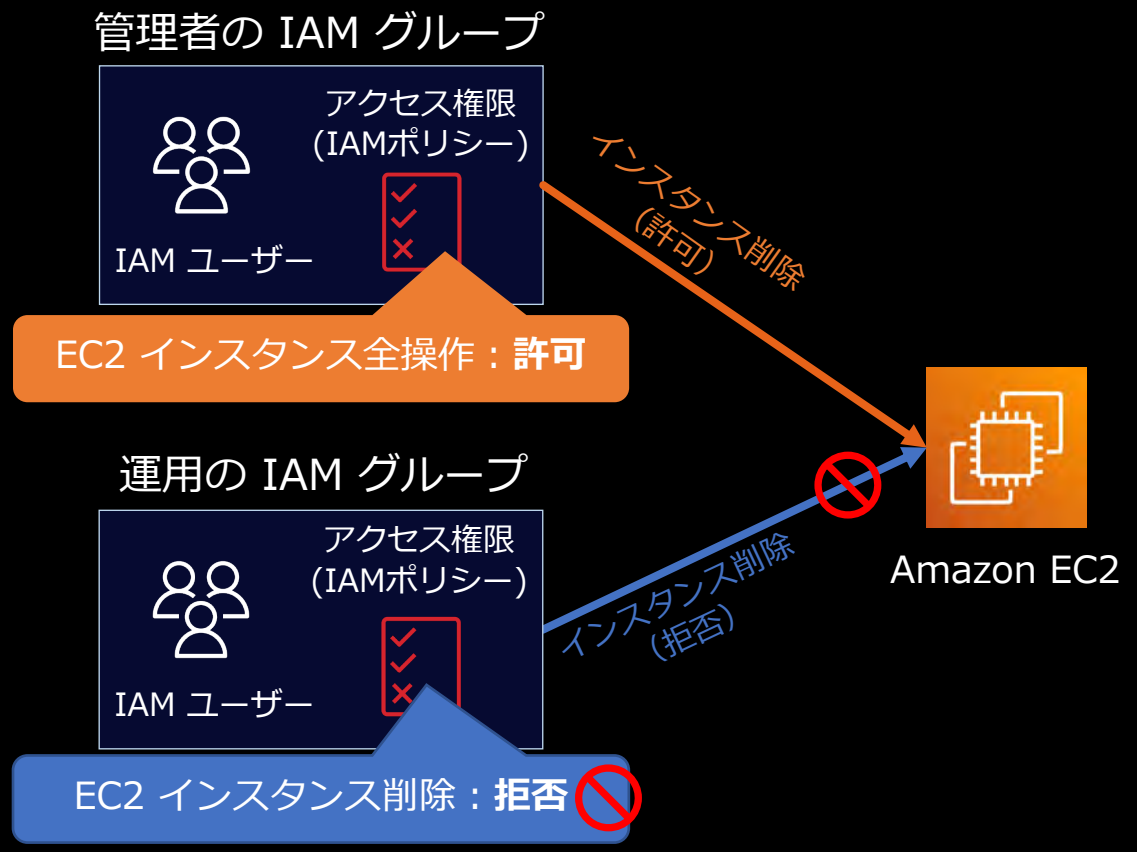


※ルートユーザーしか実施できないタスクはこちらを参照

日常作業には一般ユーザー（IAM ユーザー）を用途に合わせて作成・利用しよう

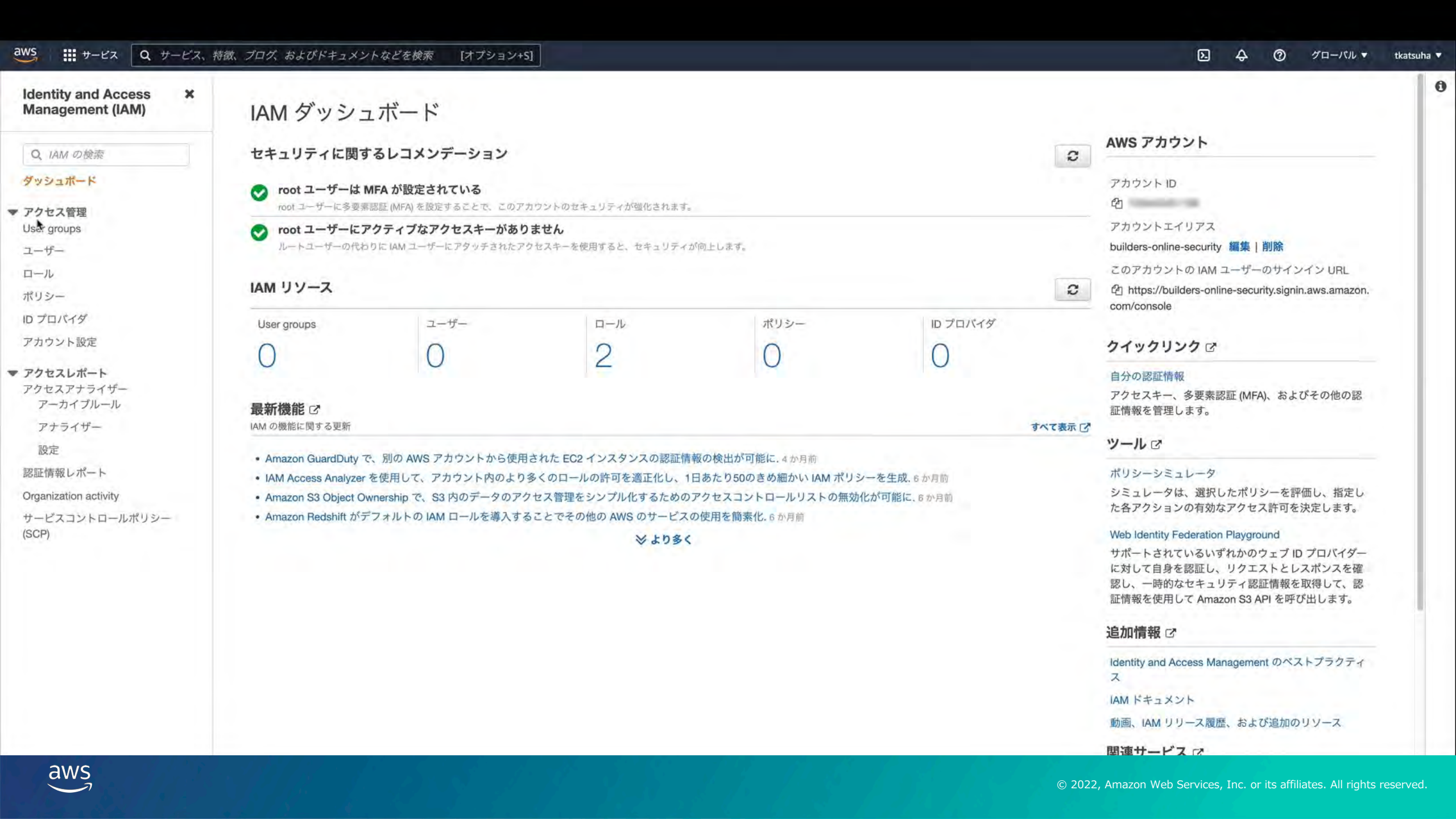
IAM ユーザー

- 日常作業に利用するユーザーのことで、IAM の機能で簡単に作成・管理※1ができる
- 管理を容易にするためにユーザーはグループ（IAM グループ）に所属できる
- 事前に許可されたアクセス権限（IAM ポリシー※2）の範囲で操作が可能



※1 初の IAM 管理者のユーザーおよびユーザーグループの作成

※2 AWS Identity and Access Management (IAM) におけるアクセス権限ついて記述するドキュメント。詳細はこちら



AWS アカウントの保護において最初に実施すべきプラクティス

AWS Identity and Access Management (IAM)

ルートユーザーを通常の作業に使わない

多要素認証 (MFA)を利用する
※Multi Factor Authentication

ルートユーザーのアクセスキーを使わない

多要素認証（MFA※）

※Multi Factor Authentication

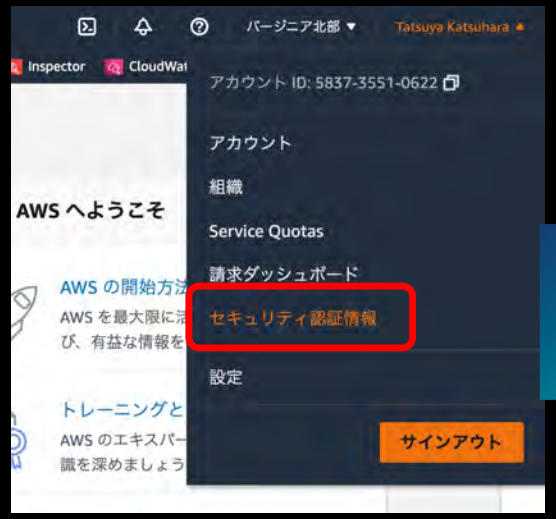
- ID/PW + ワンタイムパスワードのように複数の「要素」を組み合わせた認証のこと

- 多要素認証は AWS アカウントを保護するための強力な手段

- お客様の AWS 環境を守る
  - ルートユーザー / IAM ユーザーを守る
  - ワークロードを守る
  - その先にいるエンドユーザーを守る

簡単に設定して利用開始
ルートユーザーには必ず MFA を設定しよう

1. ルートユーザーの
「セキュリティ認証情報」を選択



2.「MFA の有効化」を押下

3. 利用する MFA デバイスのタイプを
選択してセットアップ

※IAM ユーザーにも MFA を設定することが望ましい。
詳細は「IAM でのベストプラクティス – MFA の有効化」参照

幅広い MFA デバイスサポート、豊富な選択肢

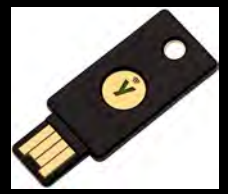
物理 MFA デバイス

ワンタイムパスワード(OTP)方式

SafeNet IDProve 700
OTP Card

SafeNet IDProve

Security Key
(WebAuthn または FIDO U2F 方式)

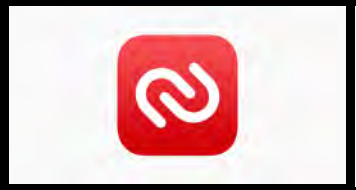


Yubico Yubikey

https://aws.amazon.com/jp/iam/features/mfa/

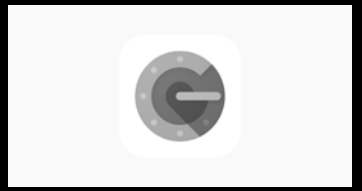
仮想 MFA デバイス
(スマートフォンアプリ)

ワンタイムパスワード(OTP)方式

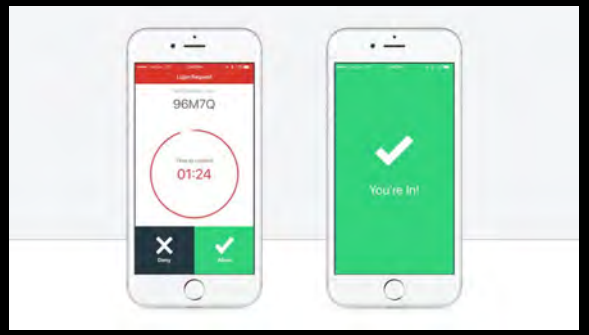


Authy

Microsoft
Authenticator



Google
Authenticator



LastPass Authenticator

Duo Mobile

aws

サインイン

◉ **ルートユーザー**
無制限アクセスを必要とするタスクを実行するアカウント所有者。詳細はこちら

○ **IAM ユーザー**
日常的なタスクを実行するアカウント内のユーザー。詳細はこちら

ルートユーザーの E メールアドレス

次へ

お客様は、続行することにより、AWS カスタマーアグリーメントまたは AWS のサービスに関するその他の契約、およびプライバシー通知に同意することになります。このサイトは必須の Cookie を使用します。詳細については、Cookie に関する通知をご参照ください。

AWS のご利用は初めてですか?

新しい AWS アカウントの作成

AWS でのワークロードの起動に役立つリソースセンター

どなたでも簡単にAWSを開始できるチュートリアルや
中・上級者向けのユースケース別ガイド、トレーニング等を
ご活用ください

詳細はこちら »

日本語

AWS アカウントの保護において最初に実施すべきプラクティス

AWS Identity and Access Management (IAM)

ルートユーザーを通常の作業に使わない

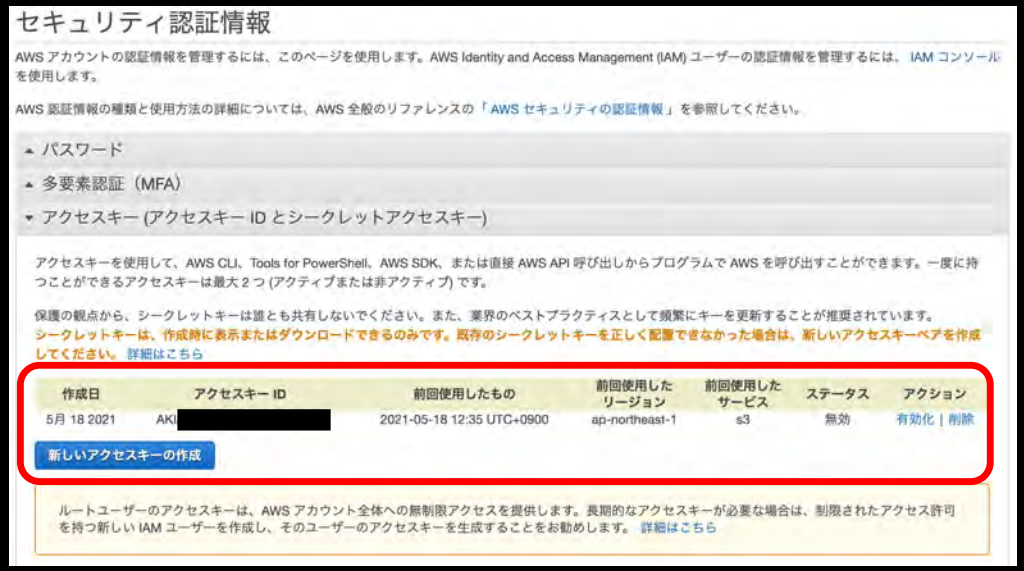
多要素認証 (MFA)を利用する
※Multi Factor Authentication

ルートユーザーのアクセスキーを使わない

ルートユーザーのアクセスキーは使わない、よりセキュアな手段を利用しよう

- アクセスキーはプログラムなどからAWS 環境を操作するための認証情報
- ルートユーザーのアクセスキーを、日常作業で使うユースケースはなく、もし作成していれば削除※1
- よりセキュリティを高める手段を使おう（例：一時的な認証情報※2）

ルートユーザーのアクセスキーが
存在している場合は、影響に注意して削除する
（デフォルトでは存在しない）



IAM でのベストプラクティス
※1 AWS アカウント ルートユーザーのアクセスキーをロックする
※2 ロールを使用してアクセス認可を委任する

「いつ・どこで・だれが・なにを・どのように」したか

AWS で起きた事実を記録しよう

AWS で起きた事実を記録するための プラクティス

AWS CloudTrail
AWS 環境における操作履歴を記録

AWS Config
AWS 環境におけるリソースの構成変更履歴を記録

AWS で起きた事実を記録するための プラクティス

AWS CloudTrail
AWS 環境における操作履歴を記録

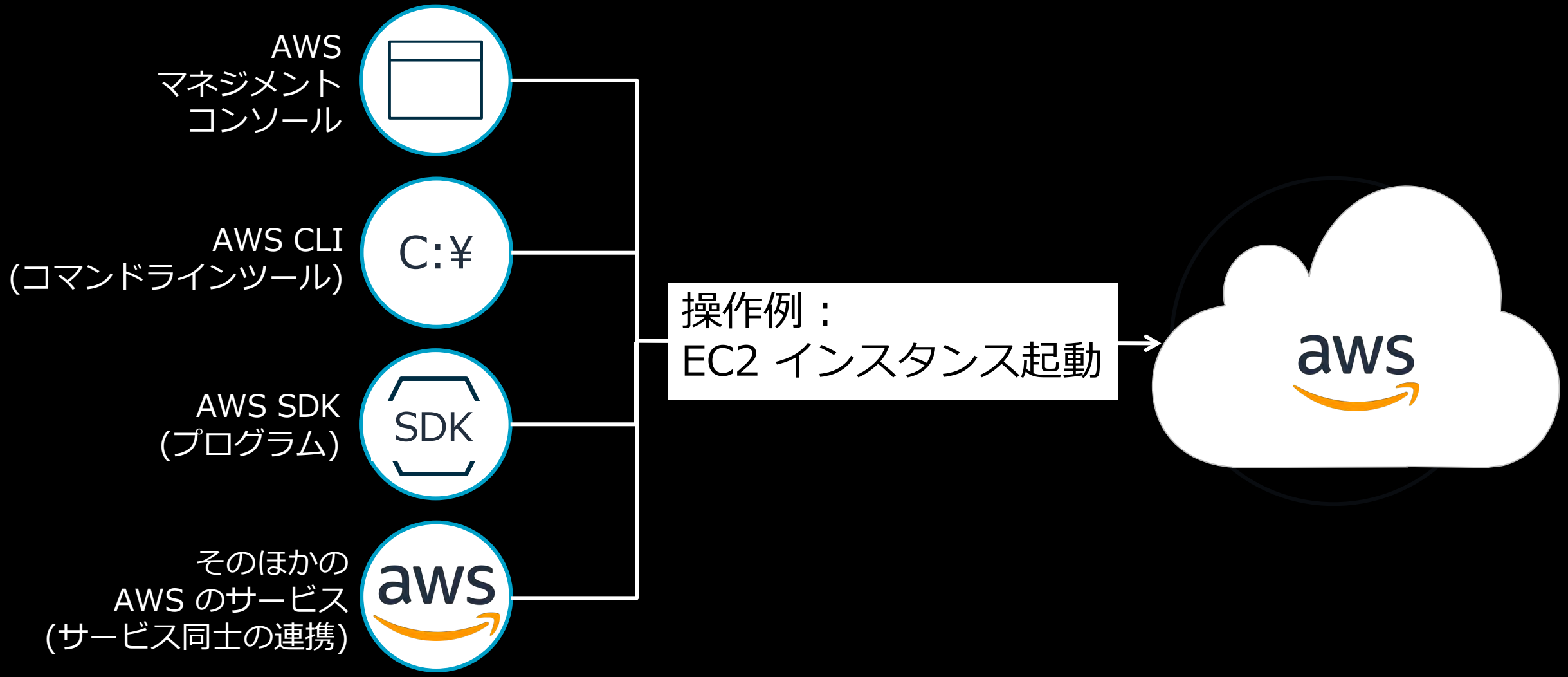
AWS Config
AWS 環境におけるリソースの構成変更履歴を記録

AWS CloudTrail

AWS CloudTrail

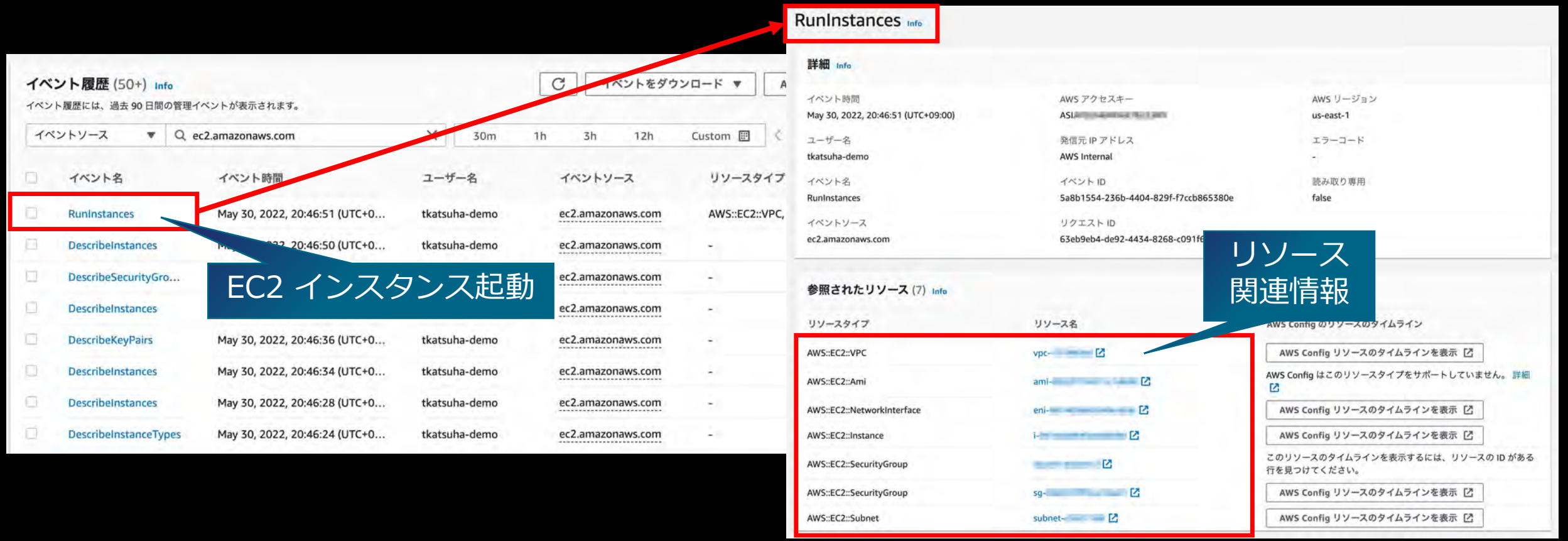
- AWS アカウントにおける各種操作の
  ログ記録、継続的なモニタリング、保持が可能
- いつ、どこから、誰が、どんな操作を実行したか
  を記録し、セキュリティ分析など容易に
- 設定により Amazon S3 に証跡を自動保存する

様々な経路で AWS に対して行われる操作を記録



AWS CloudTrail が記録する操作履歴を見よう

- AWS CloudTrail コンソールで、過去 90 日間のイベント（操作履歴）を無料で参照、ダウンロード可能※
- 単一の属性キーに対するフィルタリング機能を有する



※AWS の主要な操作履歴である管理イベントのみ。他のイベントについてはこちらを参照。

操作履歴を長期間保存するために証跡の作成を実施しよう

監査や長期的な視点でのセキュリティ分析のために、ログを長期間保存するとよい

1つ目の証跡ログの Amazon S3 への配信は無料※なので設定しよう（Amazon S3 の料金発生）

1. AWS CloudTrail のトップ画面で「証跡の作成」ボタンを押下

2.クイック証跡の作成を完了し、Amazon S3 への証跡ログの保存開始

3. 証跡ログが Amazon S3 バケットに配信されていることを確認

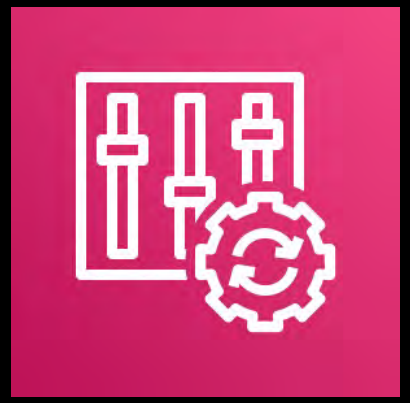
※ AWS の主要な操作履歴である管理イベントのみ。

AWS で起きた事実を記録するための プラクティス

AWS CloudTrail
AWS 環境における操作履歴を記録

AWS Config
AWS 環境におけるリソースの構成変更履歴を記録

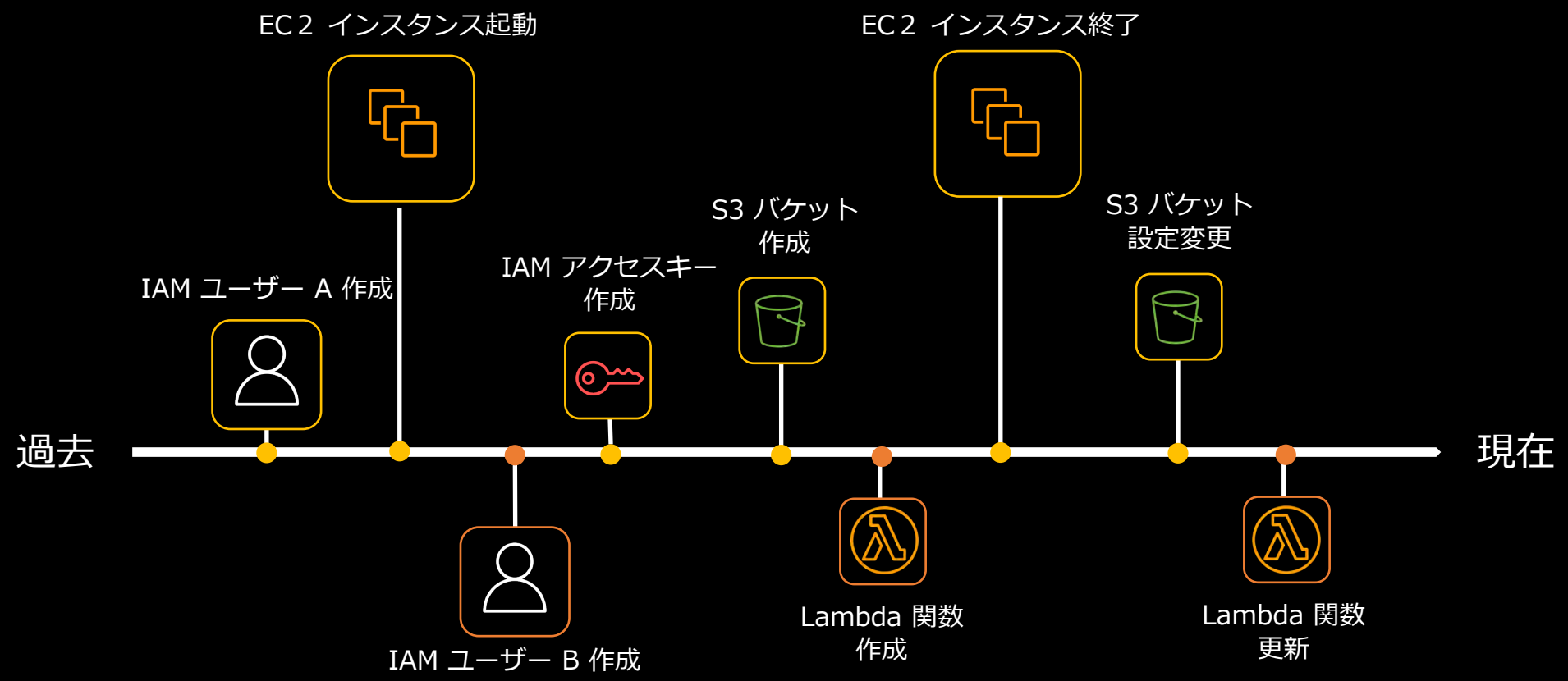
AWS Config



AWS Config

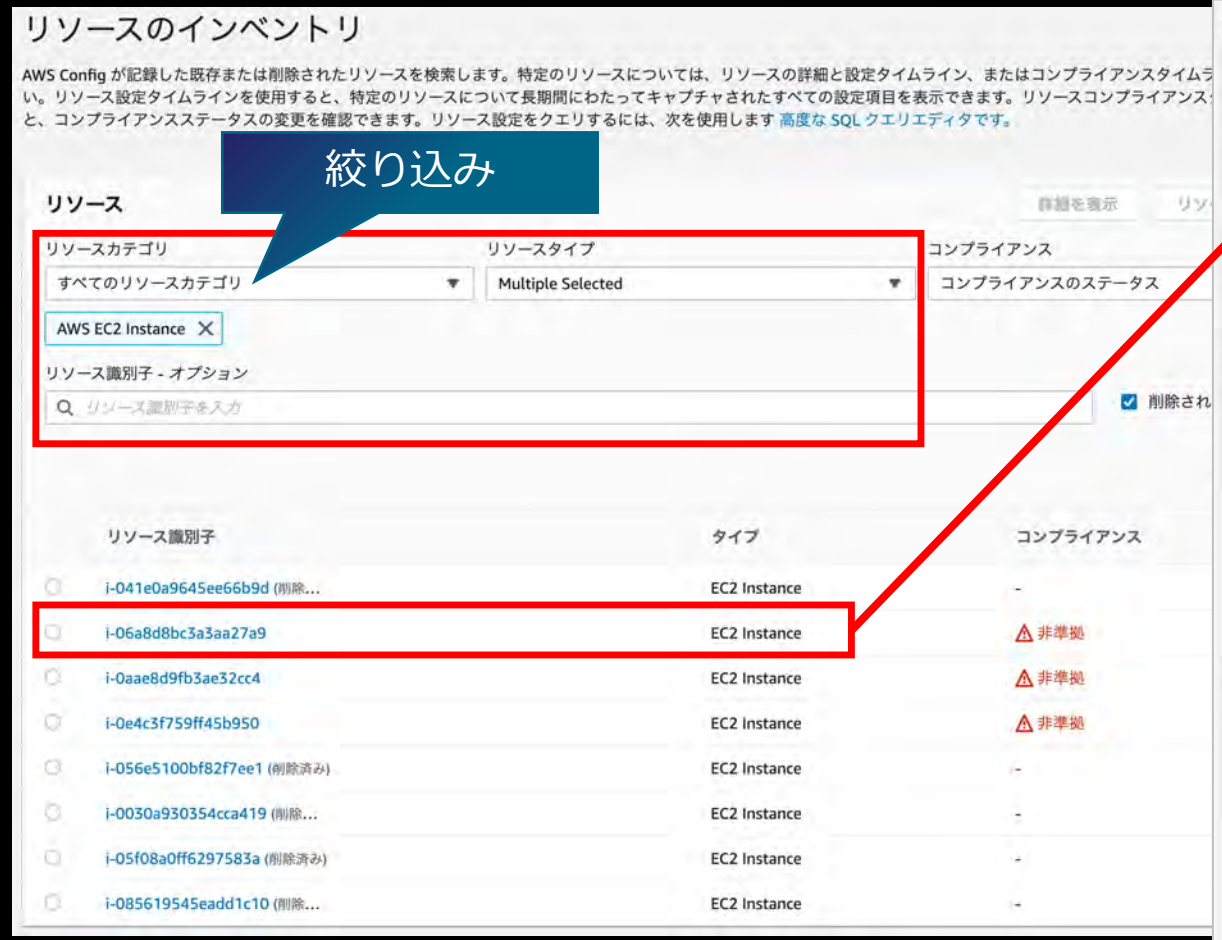
- AWSリソース構成情報の一元管理、および構成変更管理のためのフルマネージド型サービス
- AWS リソースの構成変更履歴をロギング
  - 保持期間はデフォルト７年間 （30日間～７年間で設定可）
- 構成変更の追跡で、セキュリティ分析などを容易に

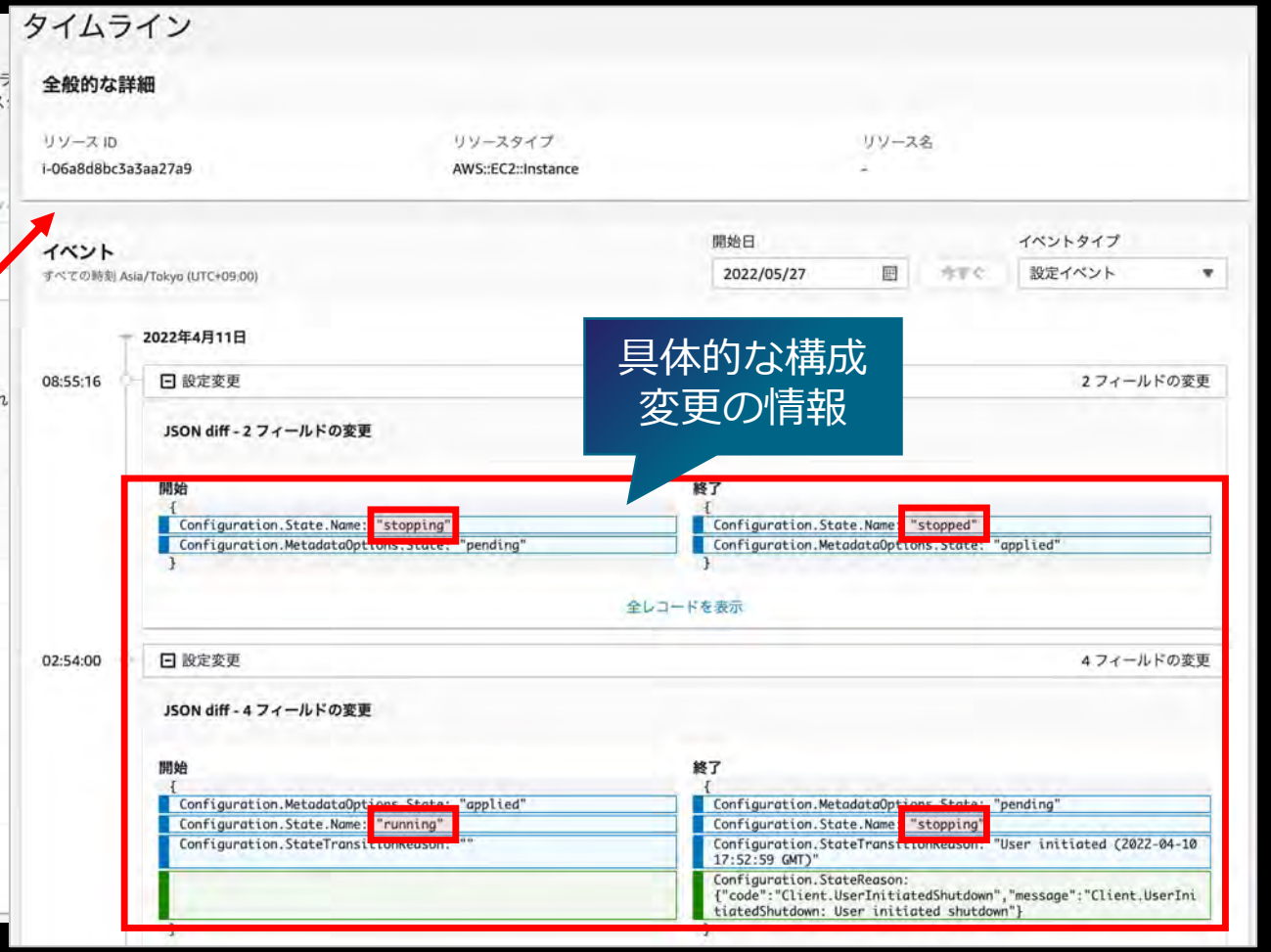
AWS Config が記録する履歴はセキュリティ面で「どのような構成だったか」の把握に役に立つ



構成変更履歴の検索とタイムラインを見てみよう

AWS リソースを管理・一覧する画面（インベントリ）で、リソースを絞り込み
必要に応じて個別のリソースの詳細・タイムラインを確認





AWS リソースの構成変更履歴の記録を有効化しよう

構成変更履歴は、監査やセキュリティ分析・トラブルシューティングなどに役立つ

保持期間（デフォルト 7年）は要件に応じて調整可能

1. AWS Config のトップ画面で「1-Click セットアップ」を押下

2. レビューで記録の配信バケットを確認しておく

3. ダッシュボードが表示され、記録状況を確認できる

※無料期間はありません。料金はこちらを参照。

AWS がお客様環境の脅威を常時監視

セキュリティ脅威を自動的に検知しよう

セキュリティ脅威検知を行うためのプラクティス

Amazon GuardDuty
　専門家がいなくても始められる高度な脅威検知を活用

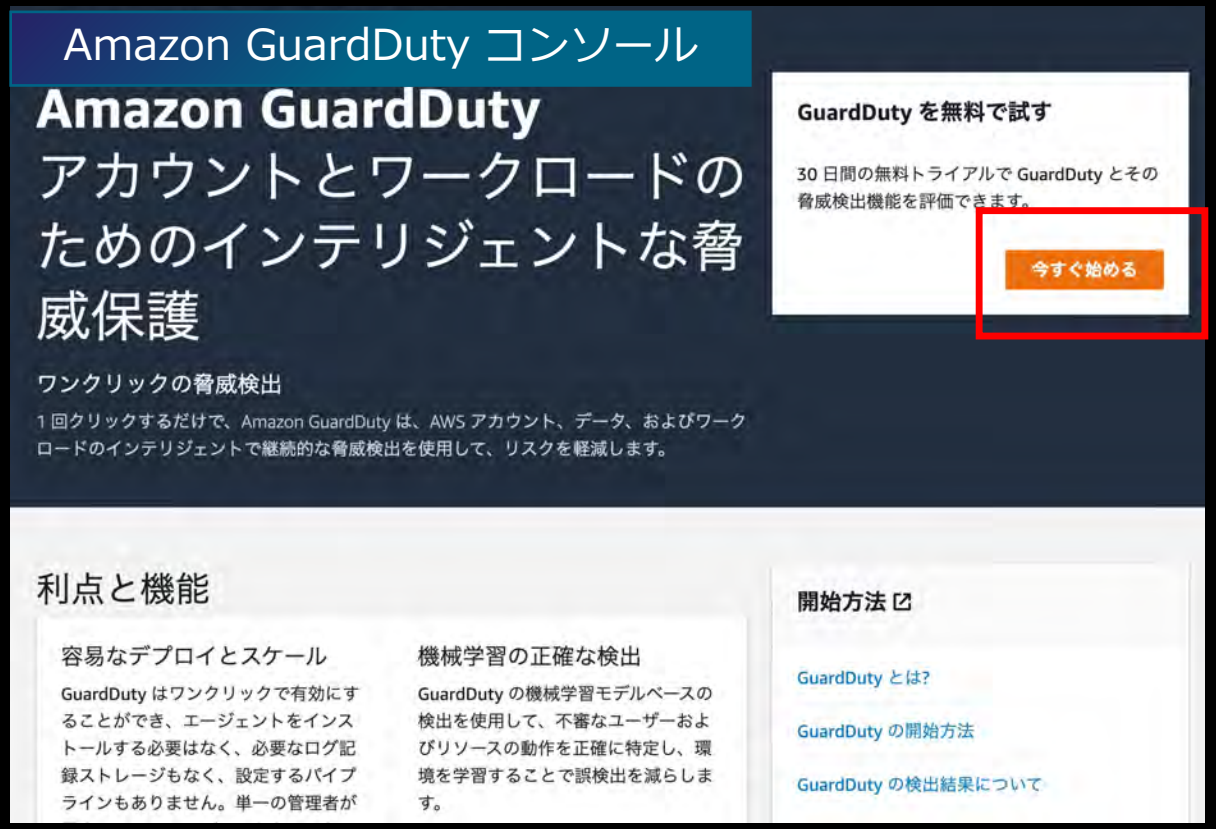
Amazon GuardDuty

Amazon GuardDuty

- 機械学習と豊富な脅威情報に基づいた脅威検知で、お客様の AWS 環境を保護
- AWS が管理する基盤で動作し、導入時の構成変更不要 & 性能影響なし
- 脅威検知手法は AWS が継続的に改善

簡単に高度な脅威検知を始めることができる

Amazon GuardDuty のコンソール画面に遷移し、数クリックするだけ
セキュリティ専門家に代わって AWS が高度な脅威検知と対策に役立つ機能を提供
30日の無料トライアル※でコスト感を把握しよう



※無料期間後の料金はこちらを参照

クラウドを安心して使うためにコストは重要

コスト面での「安心」を確保しよう

コストが急増する要因はさまざま

運用うっかりミスの例
- 大きな EC2 インスタンスタイプの
- 検証環境を立ち上げて放置

不具合作り込みの例
- Lambda 関数で無限ループ発生

意図しないアクセスの例
- 公開リポジトリにアクセスキーをコミット、悪用され仮想通貨のマイニング用インスタンスを大量に作成された

コストの急増は、請求されるまで気づけないことも
（安心を確保できていない）

コスト面で「安心」を確保するための プラクティス

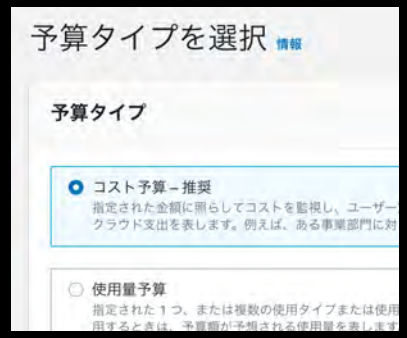
AWS Budgets
　請求アラートで、コスト急増の兆候を早期に掴む

AWS Budgets 請求アラート

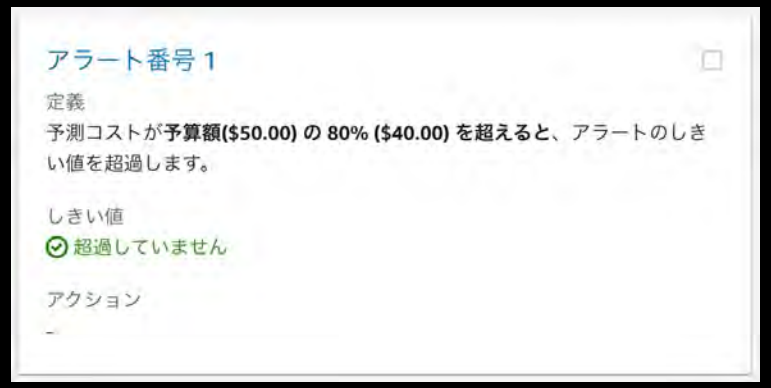
コストが高額になる兆候を知らせてくれる

- 実績/予測コストが、予算に対する「しきい値」を超えると警告メール
- 予算の監視とアラート通知の受信は無料

1. AWS Budgets コンソールで「予算を作成する」ボタンを押下



2.予算タイプの選択と、予算、対象サービスなどを選択



3. 予算に対するしきい値を指定、アラートを作成し登録

※ AWS Budgets の料金詳細はこちらを参照。
※ 同様のコストに関するアラートとして、機械学習を用いた AWS Cost Anomaly Detection はこちら

AWS Budgets 請求アラート

AWS Budget Notification / 請求アラート メールサンプル

AWS Budget Notification
AWS Account *672701140642*

Dear AWS Customer,

You requested that we alert you when the **cost** associated with your *Monthly EC2 Budget for Project Beta* budget **exceeds $31.50** this budget is **$33.35**. You can find additional details below and by accessing the AWS Budgets dashboard.

Budget Name	Budget Type	Budgeted Amount	Alert Type	Alert Threshold	FORECASTED Amount
Monthly EC2 Budget for Project Beta	Cost	$35.00	FORECASTED	> $31.50	$33.35

Go to the AWS Budgets dashboard

設定した予算

予測 or 実績

アラートしきい値

AWS がお客様の改善活動を強力にサポート

継続的な改善へ取り組もう

継続的な改善へ取り組むためのプラクティス

AWS Trusted Advisor
　AWS のセキュリティベストプラクティスを改善に活かす

AWS Trusted Advisor

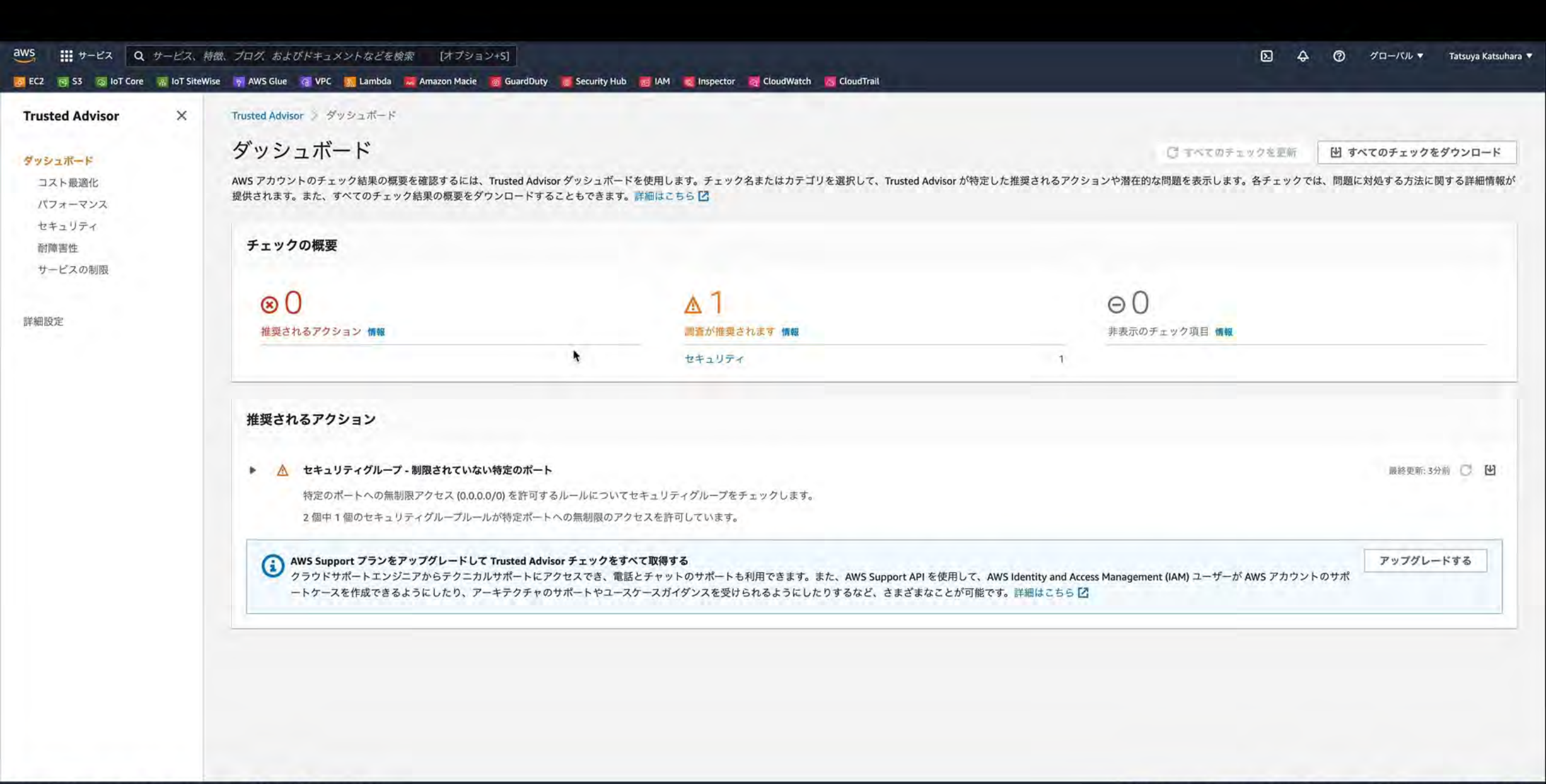
AWS Trusted Advisor

- お客様の AWS 環境を自動的に検査し、AWS のベストプラクティス※に基づく改善を提案する
- 以下の軸での推奨事項を提示

※AWS Well-Architected Framework についてはこちら

AWS Trusted Advisor セキュリティチェック

- IAM の使用　無料利用枠
- IAM パスワードポリシー
- IAM アクセスキーローテーション
- ルートアカウントの MFA　無料利用枠
- 露出したアクセスキー
- セキュリティグループ — 制限されていない特定のポート　無料利用枠
- セキュリティグループ — 無制限アクセス
- Amazon S3 バケット許可　無料利用枠
- AWS CloudTrail ロギング
- セキュリティに関する AWS Well-Architected のリスクの高い問題
- 非推奨のランタイムを使用する AWS Lambda 関数
- Amazon EBS のパブリックスナップショット　無料利用枠
- Amazon RDS のパブリックスナップショット　無料利用枠
- Amazon RDS セキュリティグループのアクセスリスク
- Microsoft SQL Server を使用した Amazon EC2 インスタンスのサポートの終了
- Amazon Route 53 MX リソースレコードセットと Sender Policy Framework
- IAM 証明書ストアの CloudFront 独自 SSL 証明書
- オリジンサーバーの CloudFront 独自 SSL 証明書
- ELB リスナーのセキュリティ
- ELB セキュリティグループ



まとめ

お客様のセキュリティ統制環境 – 初めの一歩

予防的統制

AWS Identity and Access Management

AWS アカウントのセキュリティ強化

+

発見的統制

Amazon GuardDuty

脅威検知

AWS CloudTrail

操作履歴

AWS Budgets

請求アラート

AWS Config

構成変更履歴

継続的な改善

AWS セキュリティ
ベストプラクティス & 改善提案

AWS Trusted Advisor

Amazon GuardDuty

脅威検知手法の
自動改善

おすすめしたいハンズオン

本セッションでご紹介した内容を、
具体的な画面とデモを見ながら進めることができるハンズオンです

最後に

- AWS にとってセキュリティは最優先事項

- 数多くのセキュリティ施策から厳選した「初めの一歩」を紹介
  - AWS アカウントをセキュアにしよう / AWS Identity and Access Management
    - ルートアカウント未使用、多要素認証利用、アクセスキー削除
  - AWS で起きた事実を記録しよう /AWS CloudTrail、AWS Config
  - セキュリティ脅威を自動的に検知しよう / Amazon GuardDuty
  - コスト面での「安心」を確保しよう / AWS Budgets
  - 継続的な改善へ取り組もう / AWS Trusted Advisor

- 今回ご紹介したサービスと機能は、お客様が今後もセキュリティを高めるための「基礎」となる重要なものです。

- これらのセキュリティ施策が、お客様が安心してAWS サービスを活用し、ビジネス変革を実現する一助となれば幸いです。

参考

AWS クラウドセキュリティ

https://aws.amazon.com/jp/security/

AWS コンプライアンス

https://aws.amazon.com/jp/compliance/

責任共有モデル

https://aws.amazon.com/jp/compliance/shared-responsibility-model/

IAM のベストプラクティス

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/best-practices.html

AWS アカウントのルートユーザー 認証情報が必要な AWS タスク

https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_tasks-that-require-root.html

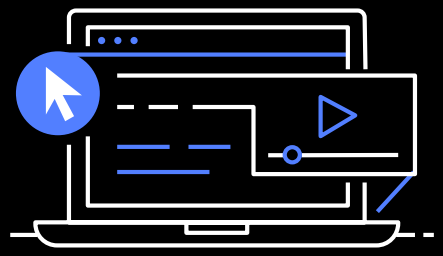
AWS Hands-on for Beginners - Security #1 アカウント作成後すぐやるセキュリティ対策

https://pages.awscloud.com/event_JAPAN_Ondemand_Hands-on-for-Beginners-Security-1_LP.html

Amazon CloudWatch Events を使用した GuardDuty の検出結果に対するカスタムレスポンスの作成

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_findings_cloudwatch.html

AWS デジタルトレーニング



実力、自信、信頼性を高め、業界で認められた資格で差をつけよう

デジタル学習

- スキルビルダー – AWS のエキスパートが開発した数百のデジタルトレーニングを自分のスケジュールで学習できます
- Cloud Quest - AWS Cloud Quest は、実践的なクラウド経験を積み、AWSクラウドのスキルを身につけることができる、初めてで唯一のロールプレイングゲームです

認定試験準備ためのリソース

- Cloud Practitioner - AWS Certified Cloud Practitioner 取得に役立つリソースをご紹介します
- Developer – Associate – AWS Certified Developer – Associate 取得に役立つリソースをご紹介します

aws

aws.amazon.com/jp/training

AWS Builders Online Series に
ご参加いただきありがとうございます

楽しんでいただけましたか? ぜひアンケートにご協力ください。
本日のイベントに関するご意見/ご感想や今後のイベントについての
ご希望や改善のご提案などがございましたら、ぜひお聞かせください。


aws-apj-marketing@amazon.com


twitter.com/awscloud_jp


facebook.com/600986860012140


https://www.youtube.com/user/AmazonWebServicesJP


https://www.linkedin.com/showcase/aws-careers/


twitch.tv/aws

Thank you!