

## 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

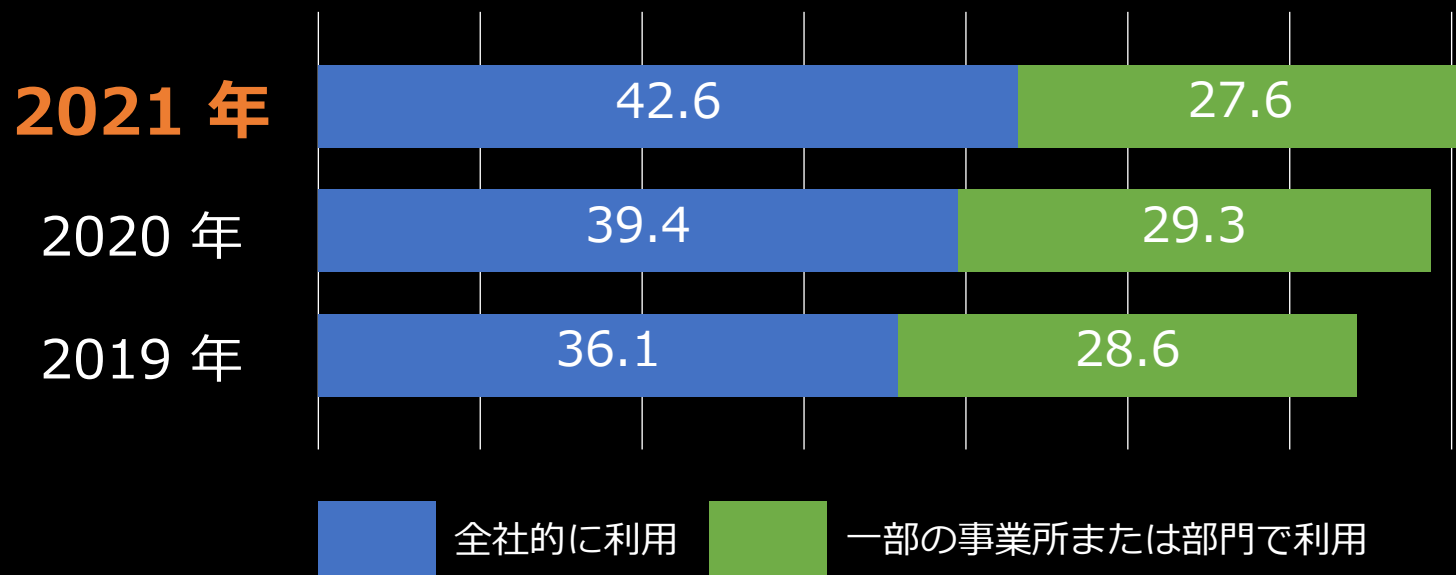
関連する AWS サービスのポイントやメリットにフォーカスしてお届けするため、サービスの機能詳細については各サービスの公式ドキュメントを合わせてご確認ください

# 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步
  - 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
<b>情報漏えいなどセキュリティに不安がある</b>	<b>27.3 %</b>
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

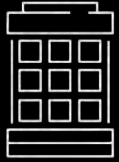
クラウドはセキュリティに関連する高い評価を得ている

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 %
<b>サービスの信頼性が高いから(情報漏えいなど対策)</b>	<b>28.8 %</b>
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 %

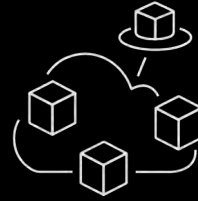
出所：総務省 令和3年通信利用動向調査(企業編)



# 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



アイデンティティ  
・  
アクセス管理



発見的統制



インフラストラクチャ  
防御



データ保護



インシデント  
レスポンス



コンプライアンス

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ンスの確認を実施

コンプライアンスプログラム例



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

## お客様のセキュリティ範囲

AWS を活用したお客様システムをセキュアに

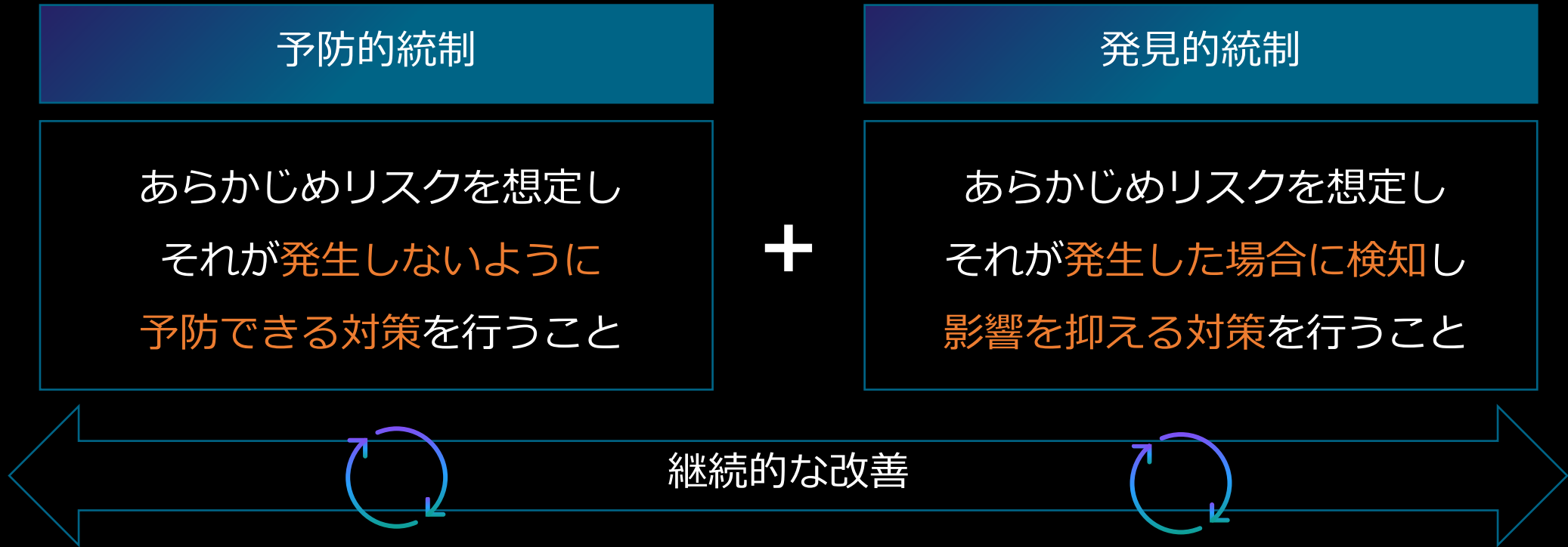
## AWS のセキュリティ統制範囲

AWS サービスが稼働するインフラをセキュアに

お客様  
AWS

# 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



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



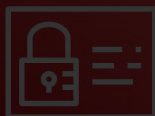
ルートユーザーのアクセスキーを使わない

# 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

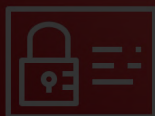
## AWS Identity and Access Management (IAM)



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

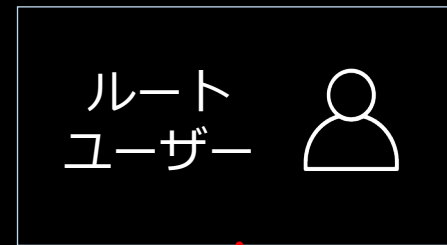


# 特権を持つユーザー（ルートユーザー）は特別な作業を行うときだけに利用しよう

## 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

無制限であらゆる操作が可能  
(特権)



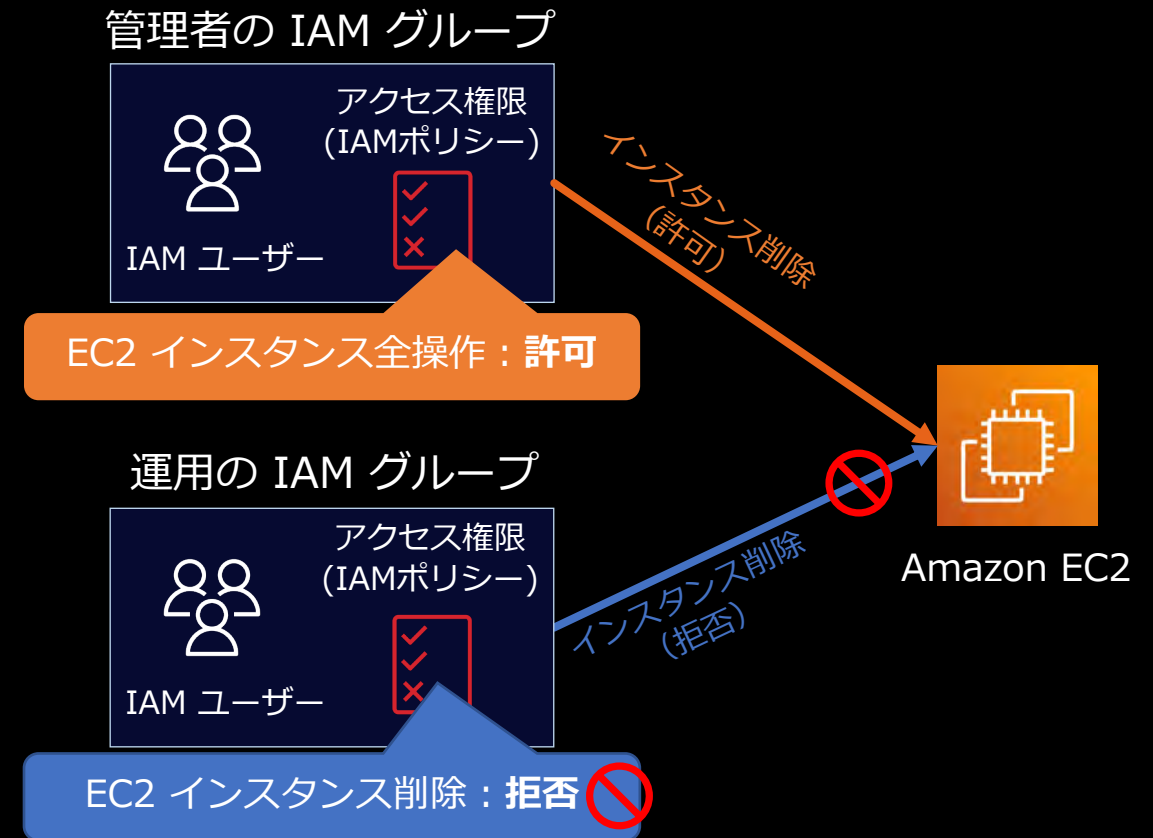
ルートユーザーしか実施できない操作  
例：サポート契約の変更、AWS アカウントの解約

※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について記述するドキュメント](#)。詳細は[こちら](#)

**Identity and Access Management (IAM)**

Q IAM の検索

ダッシュボード

- ▼ **アクセス管理**
  - User groups
  - ユーザー
  - ロール
  - ポリシー
  - ID プロバイダ
  - アカウント設定
- ▼ **アクセスレポート**
  - アクセスアナライザー
  - アーカイブルール
  - アナライザー
  - 設定
- 認証情報レポート
- Organization activity
- サービスコントロールポリシー (SCP)

# IAM ダッシュボード

## セキュリティに関するレコメンデーション

- root ユーザーは MFA が設定されている**  
root ユーザーに多要素認証 (MFA) を設定することで、このアカウントのセキュリティが強化されます。
- root ユーザーにアクティブなアクセスキーがありません**  
ルートユーザーの代わりに IAM ユーザーにアタッチされたアクセスキーを使用すると、セキュリティが向上します。

## IAM リソース

User groups	ユーザー	ロール	ポリシー	ID プロバイダ
0	0	2	0	0

## 最新機能

IAM の機能に関する更新

[すべて表示](#)

- Amazon GuardDuty で、別の AWS アカウントから使用された EC2 インスタンスの認証情報の検出が可能に. 4 か月前
- IAM Access Analyzer を使用して、アカウント内のより多くのロールの許可を適正化し、1日あたり50のきめ細かい IAM ポリシーを生成. 6 か月前
- Amazon S3 Object Ownership で、S3 内のデータのアクセス管理をシンプル化するためのアクセスコントロールリストの無効化が可能に. 6 か月前
- Amazon Redshift がデフォルトの IAM ロールを導入することでその他の AWS のサービスの使用を簡素化. 6 か月前

[≡ より多く](#)

## AWS アカウント

アカウント ID  
 アカウントエイリアス  
**builders-online-security** [編集](#) | [削除](#)

このアカウントの IAM ユーザーのサインイン URL  
<https://builders-online-security.signin.aws.amazon.com/console>

## クイックリンク

[自分の認証情報](#)  
 アクセスキー、多要素認証 (MFA)、およびその他の認証情報を管理します。

## ツール

[ポリシーシミュレータ](#)  
 シミュレータは、選択したポリシーを評価し、指定した各アクションの有効なアクセス許可を決定します。

[Web Identity Federation Playground](#)  
 サポートされているいずれかのウェブ ID プロバイダーに対して自身を認証し、リクエストとレスポンスを確認し、一時的なセキュリティ認証情報を取得して、認証情報を使用して Amazon S3 API を呼び出します。

## 追加情報

- [Identity and Access Management のベストプラクティス](#)
- [IAM ドキュメント](#)
- [動画、IAM リリース履歴、および追加のリソース](#)

## 関連サービス

# 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

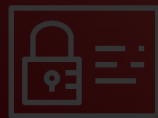
## AWS Identity and Access Management (IAM)



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. 使用する 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

## 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



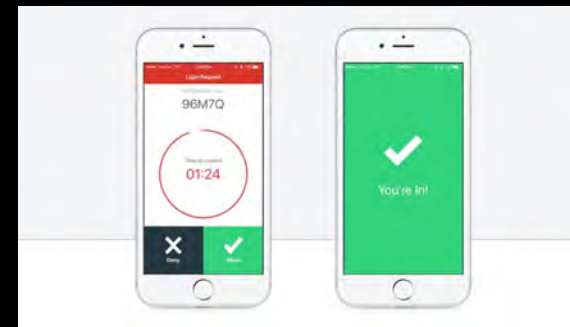
Authy



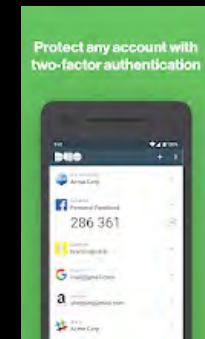
Microsoft  
Authenticator



Google  
Authenticator



LastPass Authenticator



Duo Mobile

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





## 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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

日本語 ▾

## 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 »



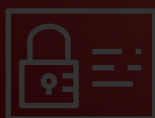


# AWS アカウントの保護において最初に実施すべきプラクティス

## 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)

セキュリティ認証情報

AWS アカウントの認証情報を管理するには、このページを使用します。AWS Identity and Access Management (IAM) ユーザーの認証情報を管理するには、IAM コンソールを使用します。

AWS 認証情報の種類と使用方法の詳細については、AWS 全般のリファレンスの「AWS セキュリティの認証情報」を参照してください。

- ▶ パスワード
- ▶ 多要素認証 (MFA)
- ▶ アクセスキー (アクセスキー ID とシークレットアクセスキー)

アクセスキーを使用して、AWS CLI、Tools for PowerShell、AWS SDK、または直接 AWS API 呼び出しからプログラムで AWS を呼び出すことができます。一度に持つことができるアクセスキーは最大 2 つ (アクティブまたは非アクティブ) です。

保護の観点から、シークレットキーは誰も共有しないでください。また、業界のベストプラクティスとして頻繁にキーを更新することが推奨されています。シークレットキーは、作成時に表示またはダウンロードできるのみです。既存のシークレットキーを正しく配置できなかった場合は、新しいアクセスキーペアを作成してください。詳細はこちら

作成日	アクセスキー ID	前回使用したもの	前回使用したリージョン	前回使用したサービス	ステータス	アクション
5月18 2021	AKI-██████████	2021-05-18 12:35 UTC+0900	ap-northeast-1	s3	無効	有効化   削除

新しいアクセスキーの作成

ルートユーザーのアクセスキーは、AWS アカウント全体への無制限アクセスを提供します。長期的なアクセスキーが必要な場合は、制限されたアクセス許可を持つ新しい IAM ユーザーを作成し、そのユーザーのアクセスキーを生成することをお勧めします。詳細はこちら

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

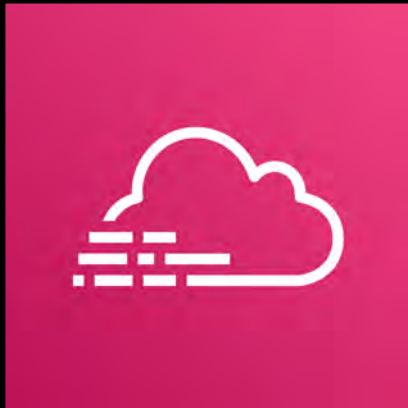


AWS CloudTrail  
AWS 環境における操作履歴を記録



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

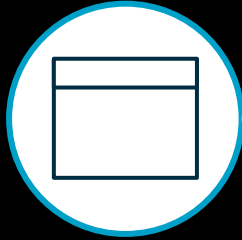


AWS CloudTrail

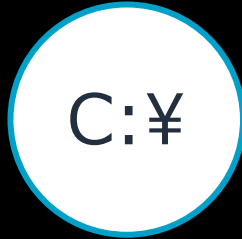
- AWS アカウントにおける各種操作のログ記録、継続的なモニタリング、保持が可能
- いつ、どこから、誰が、どんな操作を実行したかを記録し、セキュリティ分析など容易に
- 設定により Amazon S3 に証跡を自動保存する

# 様々な経路で AWS に対して行われる操作を記録

AWS  
マネジメント  
コンソール



AWS CLI  
(コマンドラインツール)



AWS SDK  
(プログラム)



その他の  
AWS のサービス  
(サービス同士の連携)



操作例：  
EC2 インスタンス起動



# 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

The screenshot displays the AWS CloudTrail console interface. On the left, the 'イベント履歴 (50+)' section shows a list of events. The 'RunInstances' event is highlighted with a red box. A blue callout box with the text 'EC2 インスタンス起動' points to this event. A red arrow points from the 'RunInstances' event to the 'RunInstances Info' panel on the right. This panel shows details for the event, including the event time, user name, and event name. Below this, the '参照されたリソース (7)' section lists resources associated with the event, such as VPC, AMI, ENI, Instance, SecurityGroup, and Subnet. A blue callout box with the text 'リソース 関連情報' points to this list. The right side of the console also shows 'AWS Config のリソースのタイムライン' with buttons to view timelines for each resource type.

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
RunInstances	May 30, 2022, 20:46:51 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	AWS::EC2::VPC,
DescribeInstances	May 30, 2022, 20:46:50 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeSecurityGro...	May 30, 2022, 20:46:50 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeInstances	May 30, 2022, 20:46:34 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeKeyPairs	May 30, 2022, 20:46:36 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeInstances	May 30, 2022, 20:46:28 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeInstanceTypes	May 30, 2022, 20:46:24 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-

リソースタイプ	リソース名
AWS::EC2::VPC	vpc-...
AWS::EC2::Ami	ami-...
AWS::EC2::NetworkInterface	eni-...
AWS::EC2::Instance	i-...
AWS::EC2::SecurityGroup	sg-...
AWS::EC2::SecurityGroup	sg-...
AWS::EC2::Subnet	subnet-...



# 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)

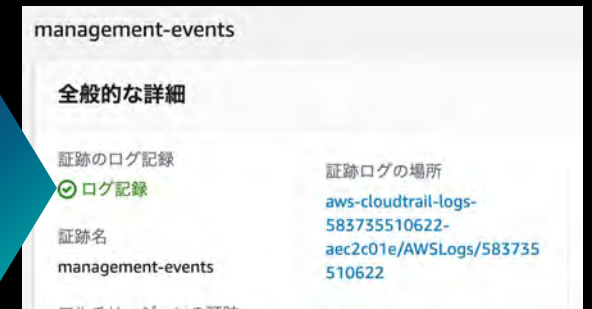
1. AWS CloudTrail のトップ画面で  
「証跡の作成」ボタンを押下



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

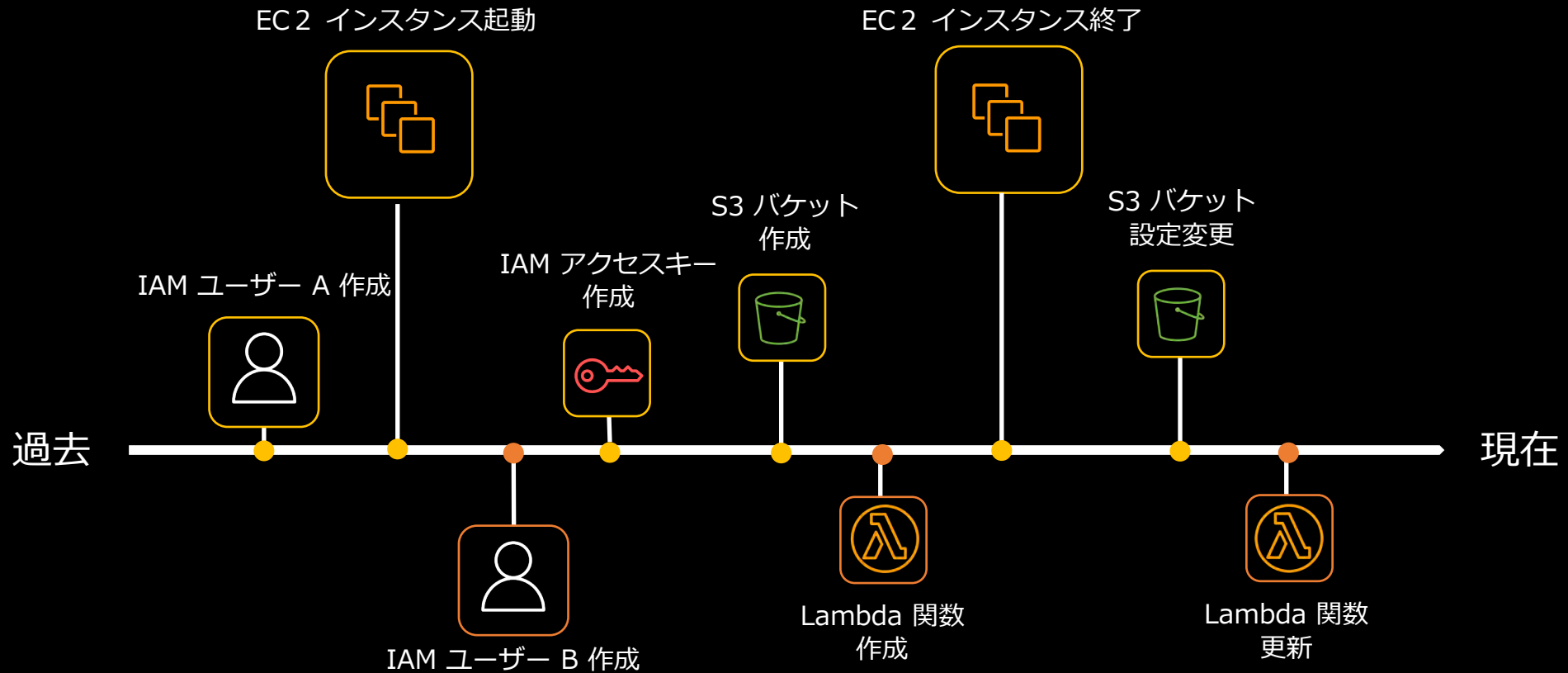
# AWS Config



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

The image shows two screenshots from the AWS Config console. The left screenshot is the 'Resource Inventory' page, and the right is the 'Timeline' page for a specific resource.

**Resource Inventory (Left):**

- Header: リソースのインベントリ
- Text: AWS Config が記録した既存または削除されたリソースを検索します。特定のリソースについては、リソースの詳細と設定タイムライン、またはコンプライアンスタイムライン。リソース設定タイムラインを使用すると、特定のリソースについて長期間にわたってキャプチャされたすべての設定項目を表示できます。リソースコンプライアンスと、コンプライアンスステータスの変更を確認できます。リソース設定をクエリするには、次を使用します [高度な SQL クエリエディタ](#)です。
- Filtering: A blue callout bubble labeled '絞り込み' (Filtering) points to the filter section. The 'Resource Category' is set to 'AWS EC2 Instance' and 'Resource Type' is 'Multiple Selected'.
- Table:

リソース識別子	タイプ	コンプライアンス
i-041e0a9645ee66b9d (削除...)	EC2 Instance	-
<b>i-06a8d8bc3a3aa27a9</b>	EC2 Instance	⚠️ 非準拠
i-0aae8d9fb3ae52cc4	EC2 Instance	⚠️ 非準拠
i-0e4c3f759ff45b950	EC2 Instance	⚠️ 非準拠
i-056e5100bf82f7ee1 (削除済み)	EC2 Instance	-
i-0030a930354cca419 (削除...)	EC2 Instance	-
i-05f08a0ff6297583a (削除済み)	EC2 Instance	-
i-085619545eadd1c10 (削除...)	EC2 Instance	-

**Timeline (Right):**

- Header: タイムライン
- General Info: リソース ID: i-06a8d8bc3a3aa27a9, リソースタイプ: AWS::EC2::Instance, リソース名: -
- Event: 2022年4月11日 08:55:16 設定変更 (2 フィールドの変更)
- JSON diff - 2 フィールドの変更:

```
開始 { Configuration.State.Name: "stopping", Configuration.MetadataOptions.State: "pending" }
終了 { Configuration.State.Name: "stopped", Configuration.MetadataOptions.State: "applied" }
```
- Event: 02:54:00 設定変更 (4 フィールドの変更)
- JSON diff - 4 フィールドの変更:

```
開始 { Configuration.MetadataOptions.State: "applied", Configuration.State.Name: "running", Configuration.StateTransitionReason: "" }
終了 { Configuration.MetadataOptions.State: "pending", Configuration.State.Name: "stopping", Configuration.StateTransitionReason: "User initiated (2022-04-10 17:52:59 GMT)", Configuration.StateReason: [{"code": "Client.UserInitiatedShutdown", "message": "Client.UserInitiatedShutdown: User initiated shutdown"}] }
```

# 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

Amazon GuardDuty コンソール

## Amazon GuardDuty

アカウントとワークロードのためのインテリジェントな脅威保護

ワンクリックの脅威検出

1回クリックするだけで、Amazon GuardDuty は、AWS アカウント、データ、およびワークロードのインテリジェントで継続的な脅威検出を使用して、リスクを軽減します。

### 利点と機能

- 容易なデプロイとスケール
- GuardDuty はワンクリックで有効にすることができ、エージェントをインストールする必要はなく、必要なログ記録ストレージもなく、設定するパイプラインもありません。単一の管理者が
- 機械学習の正確な検出
- GuardDuty の機械学習モデルベースの検出を使用して、不審なユーザーおよびリソースの動作を正確に特定し、環境を学習することで誤検出を減らします。

開始方法

- GuardDuty とは?
- GuardDuty の開始方法
- GuardDuty の検出結果について

検出結果のサンプル 情報

検出結果のサンプルは、GuardDuty が生成する検出結果のサンプルを生成すると、GuardDuty が生成した検出結果のサンプルが強調表示されます。

検出結果サンプルの生成

サンプルの脅威検知結果を生成

検出結果タイプ	リソース	アカウント	コスト
[例] CredentialAccess:Kubernet...	EKSCluster: GeneratedFinc...	2ヶ...	5579597663...
[例] Impact:Kubernetes/Malicio...	EKSCluster: GeneratedFinc...	2ヶ...	5579597663...
[例] Impact:Kubernetes/Malicio...	EKSCluster: GeneratedFinc...	2ヶ...	5579597663...
[例] CryptoCurrency:EC2/Bitcoi...	Instance: i-99999999	2ヶ...	5579597663...
[例] Impact:EC2/SuspiciousDom...	Instance: i-99999999	2ヶ...	5579597663...
[例] Persistence:Kubernetes/Co...	EKSCluster: GeneratedFinc...	2ヶ...	5579597663...
[例] PenTest:S3/PentoolLinux	S3 Bucket: bucketName	2ヶ...	5579597663...
[例] Discovery:S3/TorIPCaller	S3 Bucket: bucketName	2ヶ...	5579597663...
[例] Discovery:S3/MaliciousIPCa...	S3 Bucket: bucketName	2ヶ...	5579597663...
[例] Backdoor:EC2/C&CActivity.B	Instance: i-99999999	2ヶ...	5579597663...

検出結果画面



※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

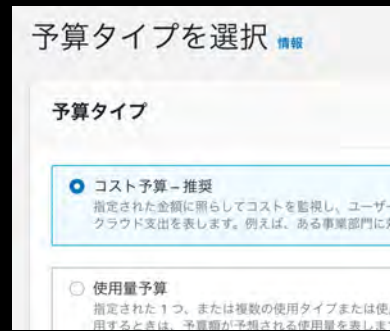
# AWS Budgets 請求アラート

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

**Trusted Advisor** ×

ダッシュボード

- コスト最適化
- パフォーマンス
- セキュリティ
- 耐障害性
- サービスの制限

詳細設定

## Trusted Advisor > ダッシュボード

# ダッシュボード

すべてのチェックを更新 すべてのチェックをダウンロード

AWS アカウントのチェック結果の概要を確認するには、Trusted Advisor ダッシュボードを使用します。チェック名またはカテゴリを選択して、Trusted Advisor が特定した推奨されるアクションや潜在的な問題を表示します。各チェックでは、問題に対処する方法に関する詳細情報が提供されます。また、すべてのチェック結果の概要をダウンロードすることもできます。 [詳細はこちら](#)

### チェックの概要

0

推奨されるアクション [情報](#)

1

調査が推奨されます [情報](#)

セキュリティ 1

0

非表示のチェック項目 [情報](#)

### 推奨されるアクション

▶ **セキュリティグループ - 制限されていない特定のポート** 最終更新: 3分前

特定のポートへの無制限アクセス (0.0.0.0/0) を許可するルールについてセキュリティグループをチェックします。  
2 個中 1 個のセキュリティグループルールが特定ポートへの無制限のアクセスを許可しています。



**AWS Support プランをアップグレードして Trusted Advisor チェックをすべて取得する**

クラウドサポートエンジニアからテクニカルサポートにアクセスでき、電話とチャットのサポートも利用できます。また、AWS Support API を使用して、AWS Identity and Access Management (IAM) ユーザーが AWS アカウントのサポートケースを作成できるようにしたり、アーキテクチャのサポートやユースケースガイダンスを受けられるようにしたりするなど、さまざまなことが可能です。 [詳細はこちら](#)

[アップグレードする](#)



# まとめ

# お客様のセキュリティ統制環境 – 初めの一步

## 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

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



# 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「初めの一步」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](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](https://docs.aws.amazon.com/ja_jp/general/latest/gr/aws_tasks-that-require-root.html)

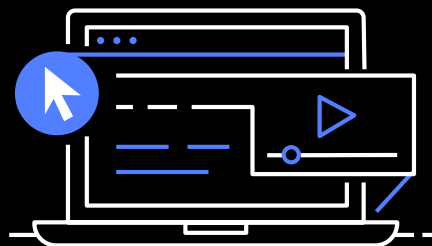
AWS Hands-on for Beginners - Security #1 アカウント作成後すぐやるセキュリティ対策

[https://pages.awscloud.com/event\\_JAPAN\\_Ondemand\\_Hands-on-for-Beginners-Security-1\\_LP.html](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](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 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](mailto:aws-apj-marketing@amazon.com)



[twitter.com/awscloud\\_jp](https://twitter.com/awscloud_jp)



[facebook.com/600986860012140](https://facebook.com/600986860012140)



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



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



[twitch.tv/aws](https://twitch.tv/aws)

# Thank you!

