

AWS Builders Online Series

T3-4

AWS セキュリティ入門 - 成長するスタートアップの セキュリティ戦略

柳 佳音

アマゾン ウェブ サービス ジャパン 合同会社
スタートアップ事業本部
シニアソリューションアーキテクト



自己紹介



柳 佳音 (やなぎ かいん)

スタートアップ ソリューション アーキテクト

好きな AWS サービス : AWS Lambda

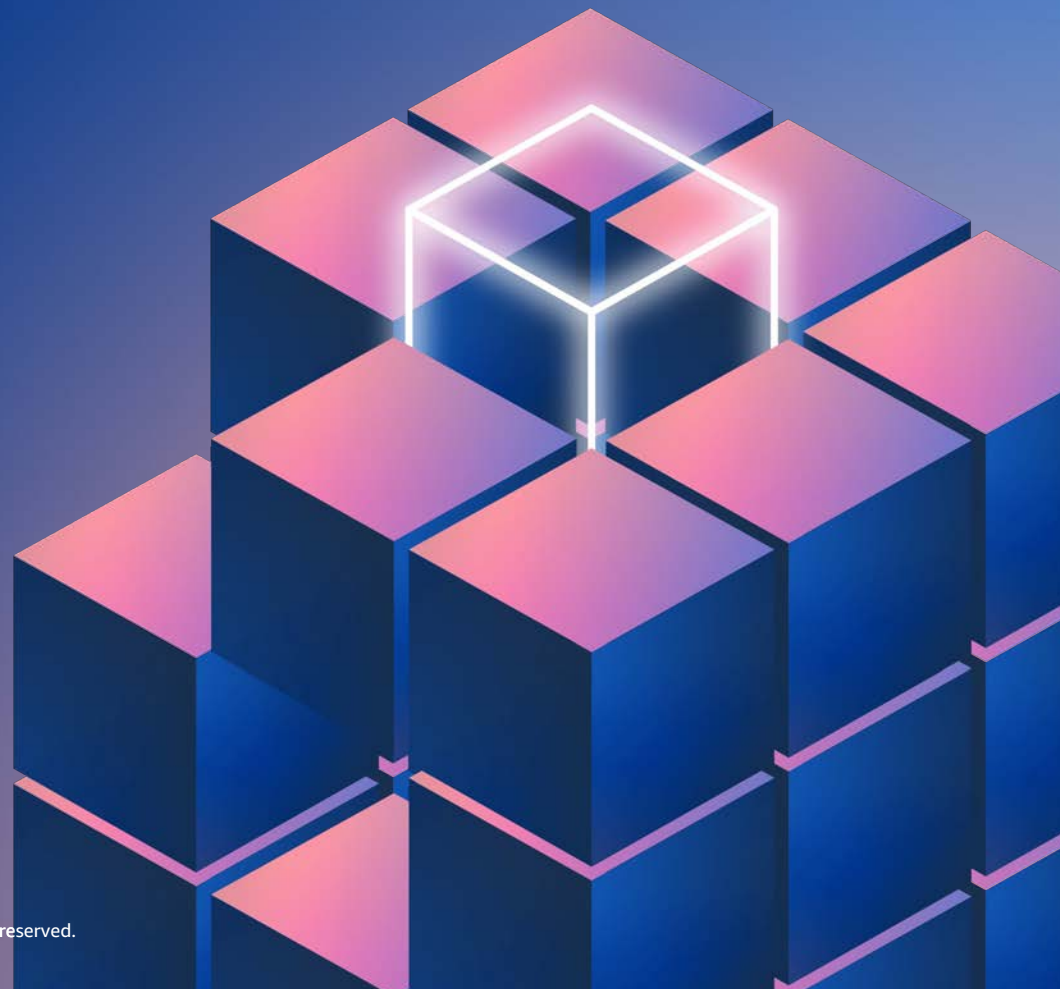
対象者、本セッションで学べること

本セッションは、AWS を使おうと思っている、あるいは使い始めたばかりの、主にスタートアップに所属しているお客様を想定しています。

本セッションでは、スタートアップが安全にビジネスを推進するための、セキュリティに取り組むための基本的な考え方、AWS におけるセキュリティの理解、まず取り組んでいただきたい施策についてお話しします。

アジェンダ

- スタートアップが直面する課題
- AWS におけるセキュリティの考え方
- 取り組んでいただきたい施策



スタートアップが直面する課題



事業の急成長がマストであり、 セキュリティの優先順位が低くなってはいませんか？

- 事業拡大が優先されコストをかけられない
- 規約・規定をゼロからつくらないといけない
- セキュリティの知見があるメンバーがいない
- 業務プロセスが複雑になり、業務効率が落ちる（と思われる）
- などなど…

「スタートアップだから」は通用しない

上場 or 売却時の監査対応

実際にセキュリティ起因で見送られるケースもある

後付けで対策しようとする、アーキテクチャーやデプロイパイプラインなどに大幅な変更が発生する可能性が高い

スタートアップの成長速度と時代の流れ

(SaaS など) 比較的早い時期にエンタープライズ企業を顧客として獲得するケースも増えている

AWS におけるセキュリティの考 え方

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

施策1: AWS アカウントを 分離しよう



AWS アカウントを用途に応じて使い分けること

セキュリティ・コンプライアンスまわりを主な理由に
マルチアカウント運用が主流になってきている

環境の分離

開発、テスト、本番などの環境をセキュリティやガバナンス、規制のために分離できる

請求の分離

部門単位やシステムの単位で、AWS のコストが明確に分離できる

権限の移譲

事前定義されたガバナンスフレームワークの中で、特定のビジネス部門に対する権限の委譲が行える

ワークロードの分離

外部向け/社内向けサービスや、リスクやデータ分類、顧客の違いなどに応じてワークロードを分離できる

施策2: 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

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 



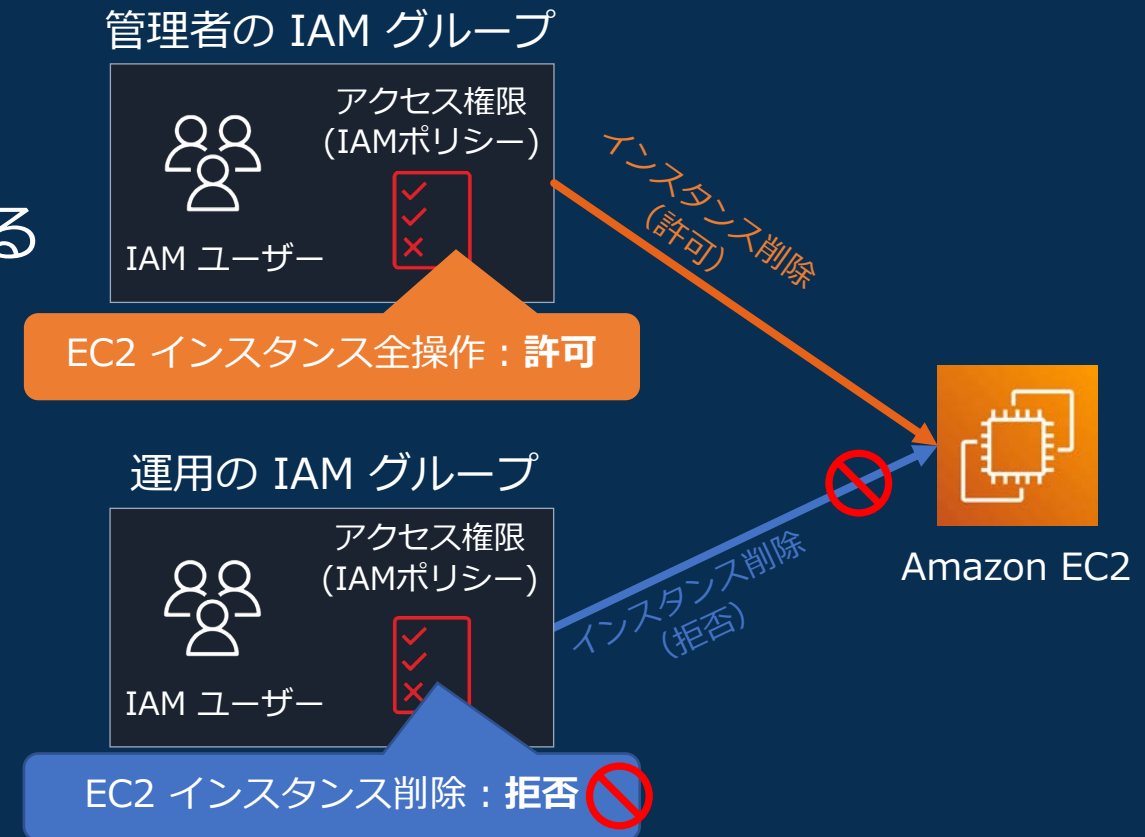
ルートユーザーしか実施できない操作
例：サポート契約の変更、AWS アカウントの解約

※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](#)

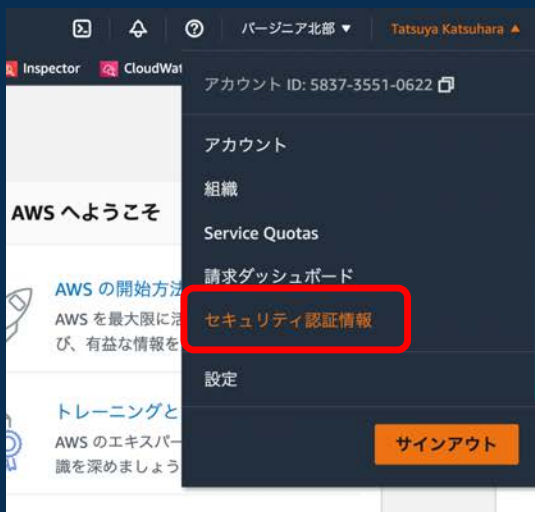
※2 AWS Identity and Access Management (IAM) におけるアクセス権限について記述するドキュメント。詳細は [こちら](#)

簡単に設定して利用開始 ルートユーザーには必ず多要素認証を設定しよう

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

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と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 [REDACTED]	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](#)



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

施策3: 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 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+) Info' section shows a list of events. The 'RunInstances' event is highlighted with a red box. A red arrow points from this event to the 'RunInstances Info' details panel on the right. A blue callout box with the text 'EC2 インスタンス起動' points to the 'RunInstances' event in the list. Another blue callout box with the text 'リソース 関連情報' points to the '参照されたリソース (7) Info' section in the details panel, which lists various resources like VPC, AMI, ENI, Instance, SecurityGroup, and Subnet.

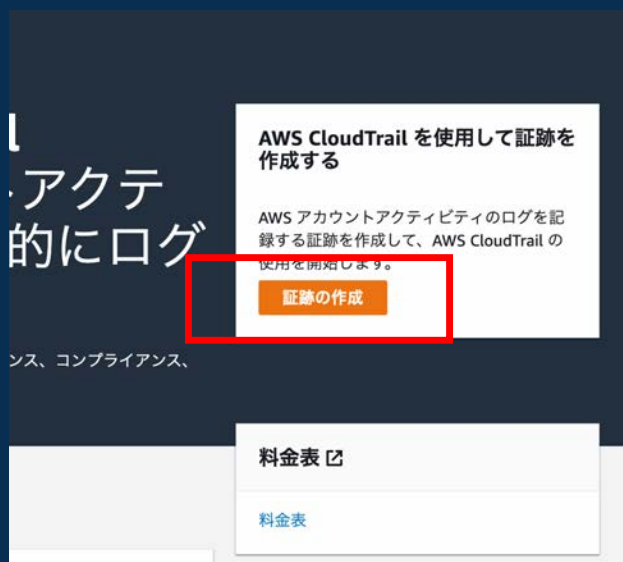
イベント名	イベント時間	ユーザー名	イベントソース	リソースタイプ
RunInstances	May 30, 2022, 20:46:51 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	AWS::EC2::VPC,
DescribeInstances	May 30, 2022, 20:46:50 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeSecurityGro...	May 30, 2022, 20:46:50 (UTC+0...)	tkatsuha-demo	ec2.amazonaws.com	-
DescribeInstances	May 30, 2022, 20:46:50 (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, 20:46:34 (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)

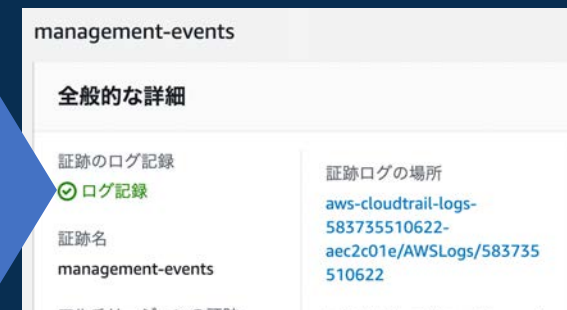
1. AWS CloudTrail のトップ画面で
「証跡の作成」ボタンを押下



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



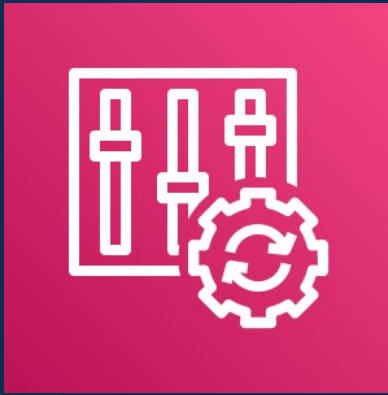
3. 証跡ログが Amazon S3
バケットに配信されている
ことを確認



※ AWS の主要な操作履歴である管理イベントのみ。

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

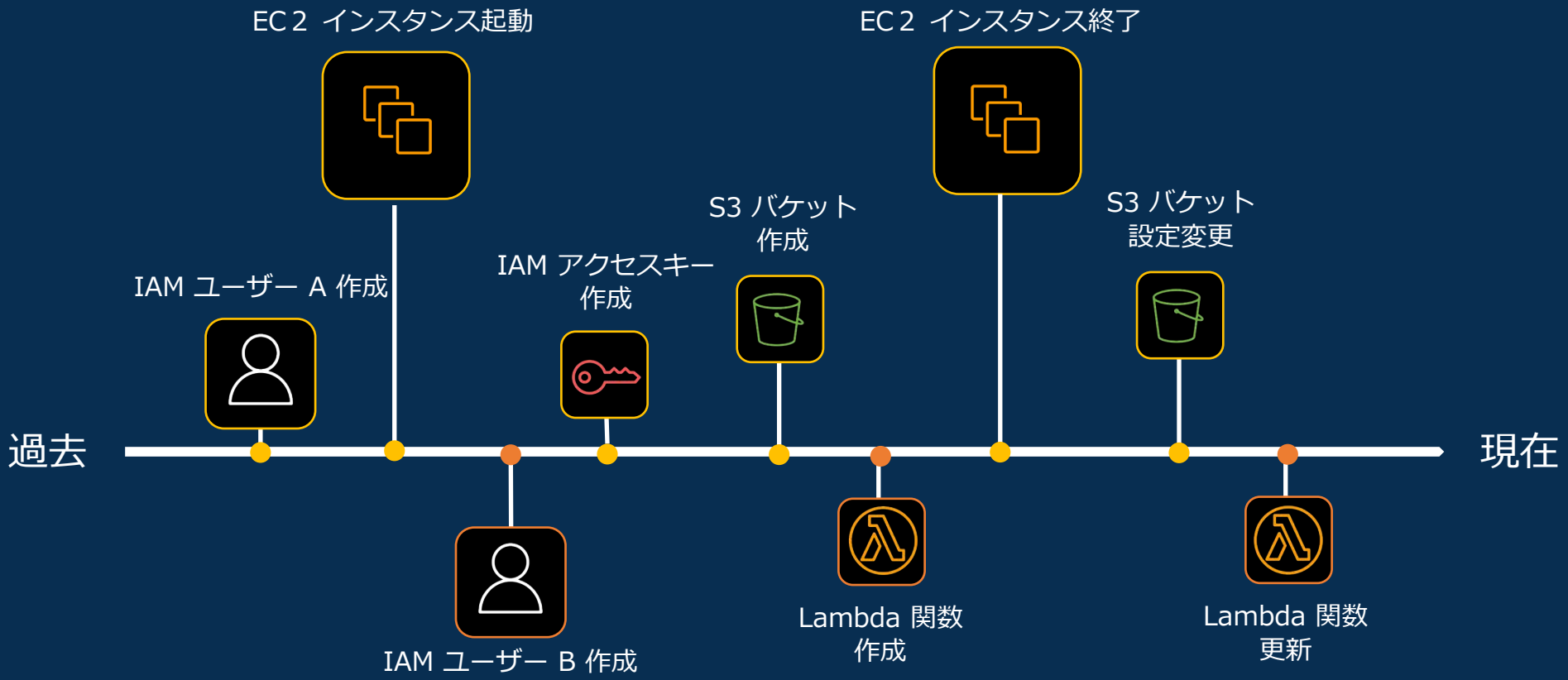
AWS Config



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

リソースのインベントリ

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ステータスと、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。

絞り込み

リソース

リソースカテゴリ: すべてのリソースカテゴリ

リソースタイプ: Multiple Selected

コンプライアンス: コンプライアンスのステータス

AWS EC2 Instance X

リソース識別子 - オプション

リソース識別子を入力

削除された

リソース識別子	タイプ	コンプライアンス
<input type="radio"/> i-041e0a9645ee66b9d (削除済)	EC2 Instance	-
<input type="radio"/> i-06a8d8bc3a3aa27a9	EC2 Instance	⚠️ 非準拠
<input type="radio"/> i-0aae8d9fb3ae32cc4	EC2 Instance	⚠️ 非準拠
<input type="radio"/> i-0e4c3f759ff45b950	EC2 Instance	⚠️ 非準拠
<input type="radio"/> i-056e5100bf82f7ee1 (削除済み)	EC2 Instance	-
<input type="radio"/> i-0030a930354cca419 (削除済)	EC2 Instance	-
<input type="radio"/> i-05f08a0ff6297583a (削除済み)	EC2 Instance	-
<input type="radio"/> i-085619545eadd1c10 (削除済)	EC2 Instance	-

タイムライン

一般的な詳細

リソース ID
i-06a8d8bc3a3aa27a9

リソースタイプ
AWS::EC2::Instance

リソース名
-

イベント

すべての時刻 Asia/Tokyo (UTC+09:00)

開始日
2022/05/27

イベントタイプ
設定イベント

具体的な構成変更の情報

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" }
```

全レコードを表示

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。



施策4: セキュリティ脅威を 自動検知しよう



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

お客様・専門家に代わり、継続的かつ高度な脅威検知を実施

データソース

-  VPC Flow logs
-  DNS Logs
-  CloudTrail Events
-  S3 Data Plane Events
-  EKS control plane logs & runtime activities
-  RDS Login events
-  EBS volumes

高度な脅威検知

-  「既知の脅威」検知
脅威インテリジェンス
(情報収集活動)に基づく検知
-  「未知の脅威」検知
機械学習による
普段と異なる振る舞い検知
-  「継続的」改善
脅威インテリジェンスや機械
学習、検出結果タイプ見直し

検出結果



-  AWS Security Hub
-  Amazon Detective
-  Amazon EventBridge
アラート・対応自動化、
パートナー
ソリューション連携

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

GuardDuty を無料で試す

30 日間の無料トライアルで GuardDuty とその脅威検出機能の評価ができます。

今すぐ始める

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 に基づいて検出結果サンプルが強調表示

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

GuardDuty > 検出結果

検出結果 情報

検出結果の抑制 保存済みのルール 保存済みのルールがありません

検出結果タイプ	リソース	重要度	アカウント	カ...
[明] CredentialAccess:Kubernet...	EKSCluster: GeneratedFinc	2ヶ...	5579597663...	1
[明] Impact:Kubernetes/Malicio...	EKSCluster: GeneratedFinc	2ヶ...	5579597663...	1
[明] Impact:Kubernetes/Malicio...	EKSCluster: GeneratedFinc	2ヶ...	5579597663...	1
[明] CryptoCurrency:EC2/Bitcoi...	Instance: i-99999999	2ヶ...	5579597663...	1
[明] Impact:EC2/SuspiciousDom...	Instance: i-99999999	2ヶ...	5579597663...	1
[明] Persistence:Kubernetes/Co...	EKSCluster: GeneratedFinc	2ヶ...	5579597663...	1
[明] PenTest:S3/PentooLinux	S3 Bucket: bucketName	2ヶ...	5579597663...	1
[明] Discovery:S3/TorIPCaller	S3 Bucket: bucketName	2ヶ...	5579597663...	1
[明] Discovery:S3/MaliciousIPCa...	S3 Bucket: bucketName	2ヶ...	5579597663...	1
[明] Backdoor:EC2/C&CActivity.B	Instance: i-99999999	2ヶ...	5579597663...	1

Backdoor:EC2/C&CActivity.B

検出結果 ID: 1abf68be8b46f6c84417c37b06ff65e

High EC2 instance i-99999999 is communicating outbound with a known Command & Control Server 198.51.100.0 located in GeneratedFindingCountryName.

Detective で調査する

概要

重要度	高い
リージョン	us-west-2
カウント	1
アカウント ID	557959766337
リソース ID	i-99999999
作成時刻	2022-03-22 20:57:19 (2ヶ月前)
更新時刻	2022-03-22 20:57:19 (2ヶ月前)

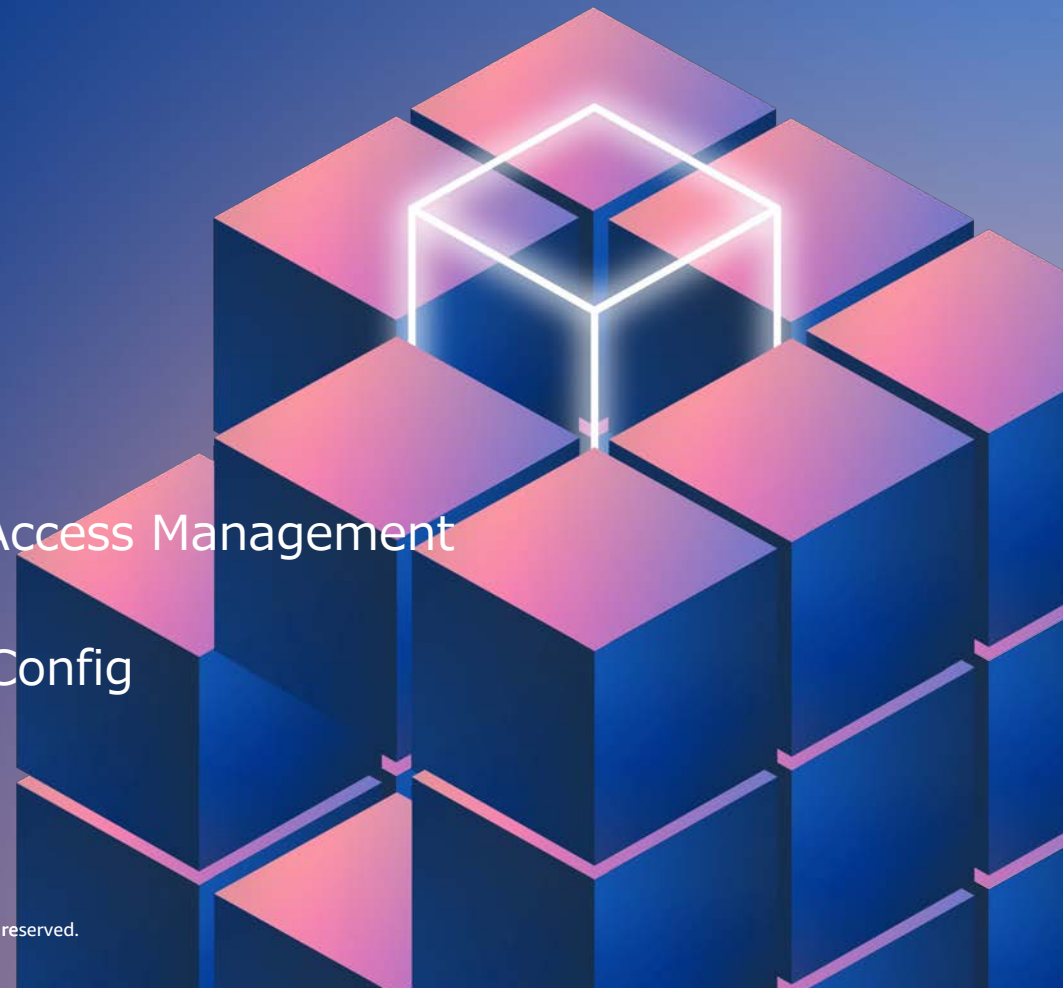
影響を受けるリソース

検出結果画面

※無料期間後の料金は[こちら](#)を参照

本セッションのおさらい

- 「スタートアップだからこそ」セキュリティは大事
- AWS にとってセキュリティは最優先事項
- 取り組んでいただきたい施策
 - AWS アカウントを分離しよう
 - AWS アカウントをセキュアにしよう / AWS Identity and Access Management
 - AWS で起きた事象を記録しよう / AWS CloudTrail、AWS Config
 - セキュリティ脅威を自動検知しよう / Amazon GuardDuty



今後に向けて

本セッションで紹介した内容を、
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



Thank you!

AWS TRAINING & CERTIFICATION

600+ ある AWS Skill Builder の無料デジタルコースで学ぼう

30 以上の AWS ソリューションの中から、自分にもっとも関係のあるクラウドスキルとサービスにフォーカスし、自習用のデジタル学習プランとランプアップガイドで学ぶことができます。

自分に合ったスキルアップ方法で学ぼう

[EXPLORE.SKILLBUILDER.AWS](https://explore.skillbuilder.aws) »



あなたのクラウドスキルを AWS 認定で証明しよう

業界で認められた資格を取得して、スキルアップの一步を踏み出しましょう。AWS Certified の取得方法と、準備に役立つ AWS のリソースをご覧ください。

[受験準備のためのリソースにアクセスしよう](#) »



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