# ぎりぎり20分で話しきる
# Amazon GuardDuty による脅威検知

小森谷 健太
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 合同会社
2022/04/28

# ぎりぎり20分で話しきること

- Amazon GuardDuty とは
- 有効化する前に知っておきたいこと一問一答
- 次のステップ

# 自己紹介

## 小森谷 健太 こもりや けんた

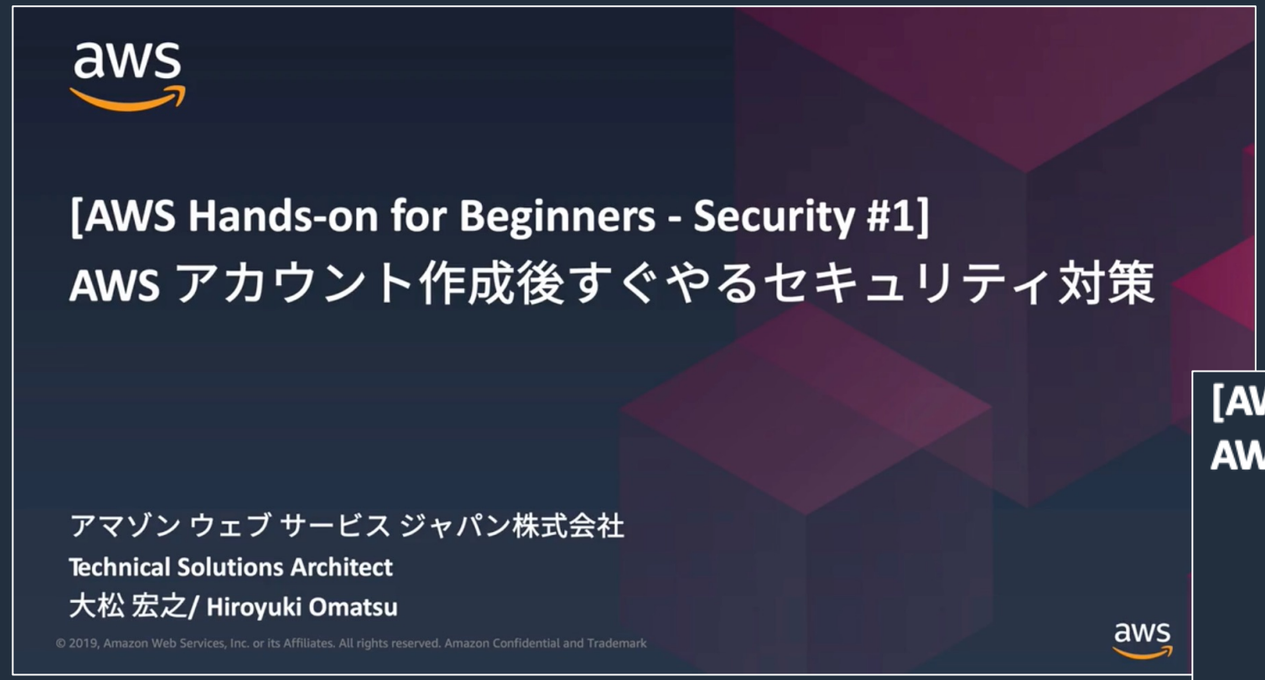
- Amazon Web Services Japan G.K.
- Solutions Architect
- 前職: SIer
  - 金融機関様向けシステムの構築, 運用
- 好きな AWS サービス
  - Amazon GameSparks, Amazon GuradDuty
- 趣味：ビアバー巡り🍺, ハンバーガー🍔🍺

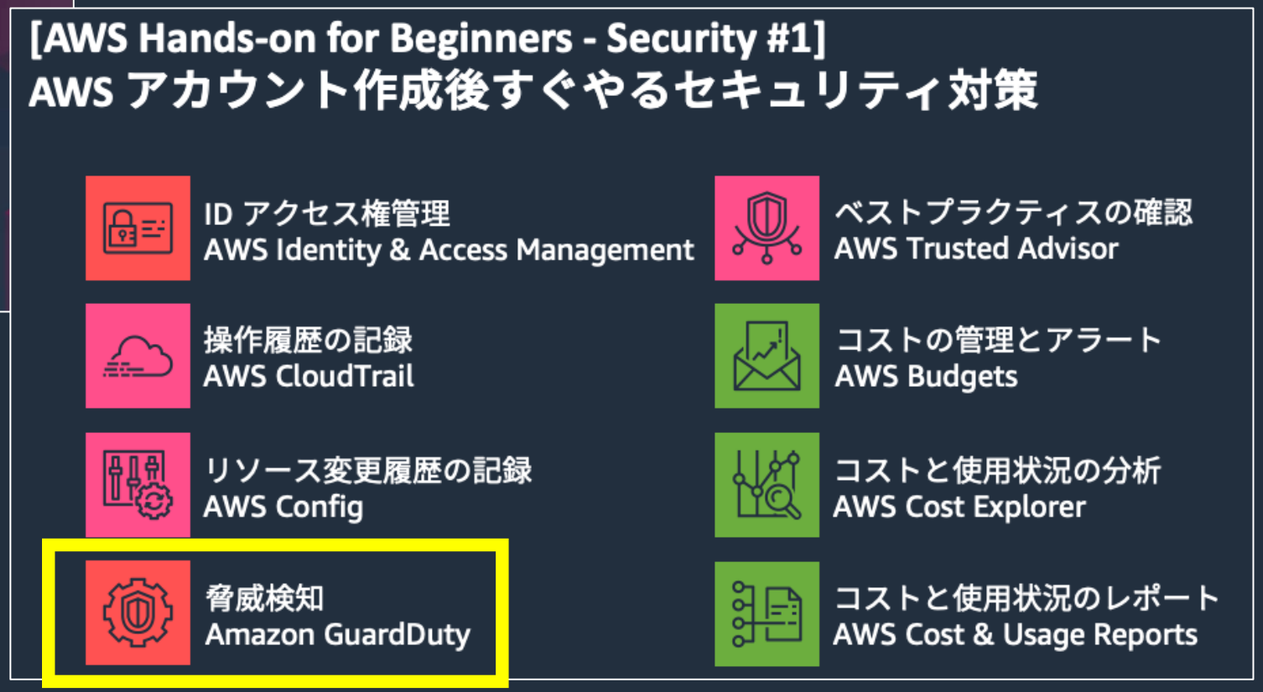



aws

# Amazon GuardDuty とは

# すべてのAWSアカウントで有効化することを推奨しています




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

# AWS セキュリティ サービス

## ID とアクセス管理

AWS Identity and Access Management (IAM)

AWS Single Sign-On

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

## 発見的統制

AWS Security Hub

Amazon GuardDuty

Amazon Inspector

Amazon CloudWatch

AWS Config

AWS CloudTrail

VPC Flow Logs

AWS IoT Device Defender

## インフラ保護

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF – Web application firewall

Amazon Virtual Private Cloud

AWS PrivateLink

AWS Systems Manager

## データ保護

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Secrets Manager

AWS VPN

Server-Side Encryption

## インシデント対応

Amazon Detective

Amazon EventBridge

AWS Backup

AWS Security Hub

CloudEndure Disaster Recovery

## コンプライアンス

AWS Artifact

AWS Audit Manager



aws

# Amazon GuardDuty

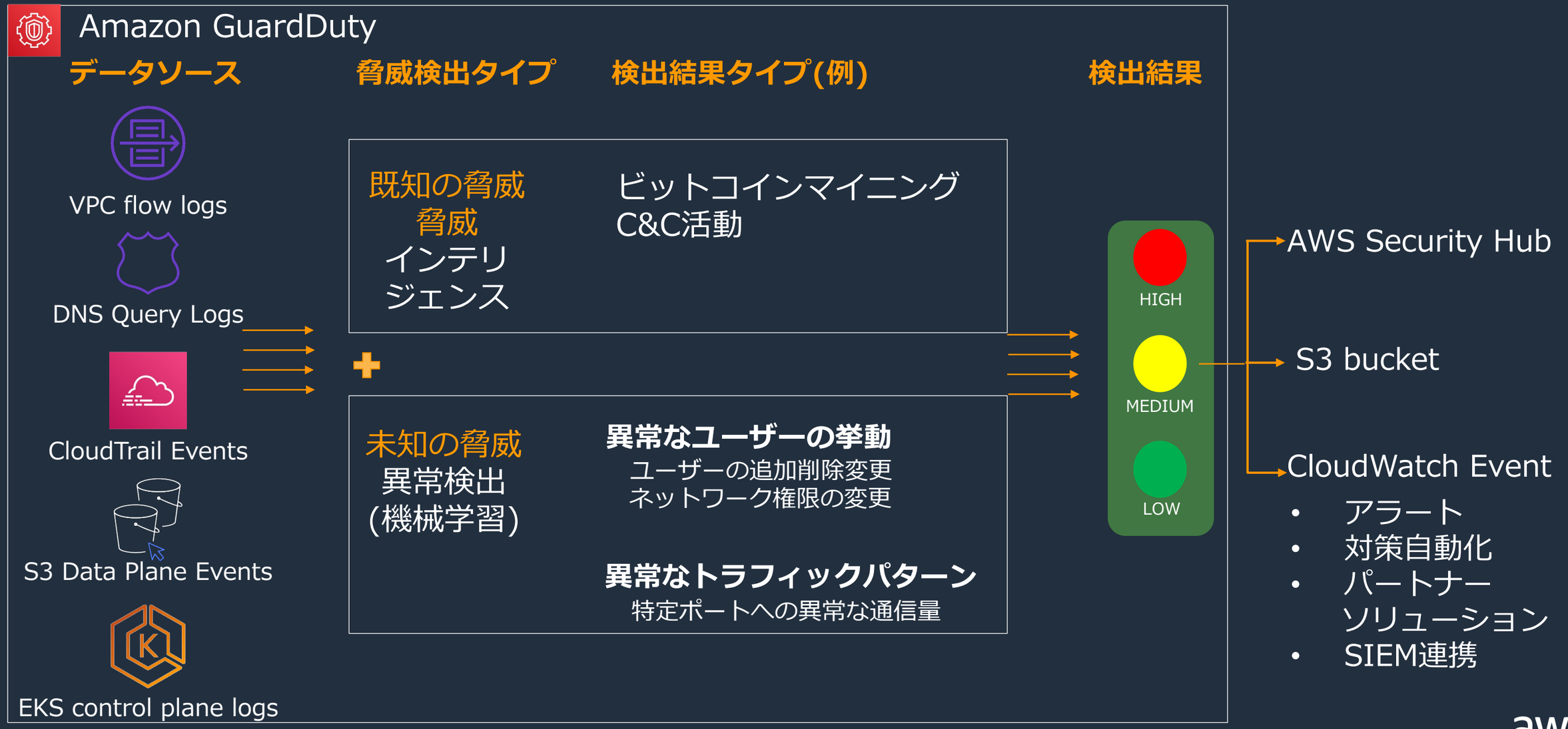
Amazon GuardDuty

- セキュリティの観点から脅威を検知する AWSマネージド・サービス
- 機械学習、異常検出、脅威インテリジェンスを使用して脅威を継続的に監視
- 悪性で強く疑わしい挙動を特定
- IDS / IPS などで検出が難しい AWS のアカウントや S3 バケットの侵害も検出



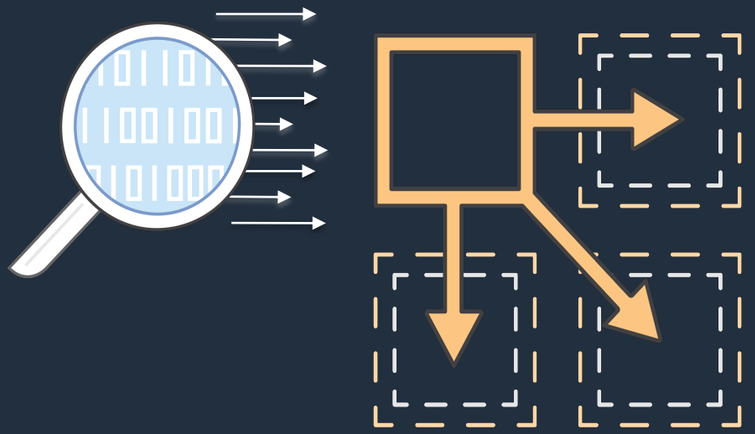
aws

# 脅威の検出方法



# 脅威インテリジェンスによる既知の脅威検出

- 様々な脅威インテリジェンスの活用
  - AWSセキュリティのインテリジェンス
  - AWSパートナーの CrowdStrike と Proofpoint
  - ユーザーが登録したインテリジェンス



- 脅威インテリジェンスにより識別できる脅威
  - 既知のマルウェアに感染したホスト
  - 匿名プロキシー
  - マルウェアおよびハッキングツールをホストしてるサイト
  - 暗号資産(仮想通貨)のマイニングプールとウォレット



aws

# S3 プロテクション

## Amazon S3 内のデータに対する脅威のプロアクティブな検出

### ポリシー

- バケット公開
- S3パブリックアクセスブロックの無効化
- ロギング停止
- ルートアカウントの使用

### 不正アクセス

- データの探索、取得、変更の送信元が
  - Tor (匿名通信)
  - 漏洩した認証情報使用
  - 不正なIPアドレス

### 異常なふるまい

- 通常時と違うロケーション
- 通常時と違うバケット
- 異常な転送量
- 異常な転送失敗

- アカウント内の全ての S3 バケットを、自動的に継続的に監視
- 新規に GuardDuty を有効化すると、S3 プロテクションも自動的に有効化されます



aws

# Kubernetes プロテクション

## Amazon EKS クラスターへの不正なアクティビティを監視

### ポリシー

- ダッシュボードの公開
- デフォルトのサービスアカウントへの管理者権限付与
- Anonymous ユーザーへの権限付与

### 不正アクセス

- データの探索、取得、変更の送信元が
  - Tor (匿名通信)
  - 漏洩した認証情報使用
  - 不正なIPアドレス

### 疑わしいふるまい

- Kubernetes の System Pod内で実行
- 機密性の高いホストパスへマウント
- 特権権限のコンテナ起動

- 既に　GuradDuty が有効化されている場合、デフォルトでは無効化されているため、手動で有効化することで利用できます
- 新規に GuardDuty を有効化すると、Kubernetes プロテクションも自動的に有効化されます



aws

# 有効化する前に知っておきたいこと一問一答

# Q1. 料金はどれくらいかかりますか？

# A1. GuardDuty の料金はこちら

CloudTrail Events: 分析されたCloudTrailイベントの数量（1,000,000イベントあたり）

VPC Flow Logs/DNS Logs: 分析されたAmazon VPC Flow LogおよびDNS Logデータの量（GBあたり）

S3 Data plane Events: 分析された CloudTrail S3 データイベントの数量（1,000,000イベントあたり）

Amazon EKS 監査ログ: 分析された EKS 監査ログの数量（1,000,000イベントあたり）

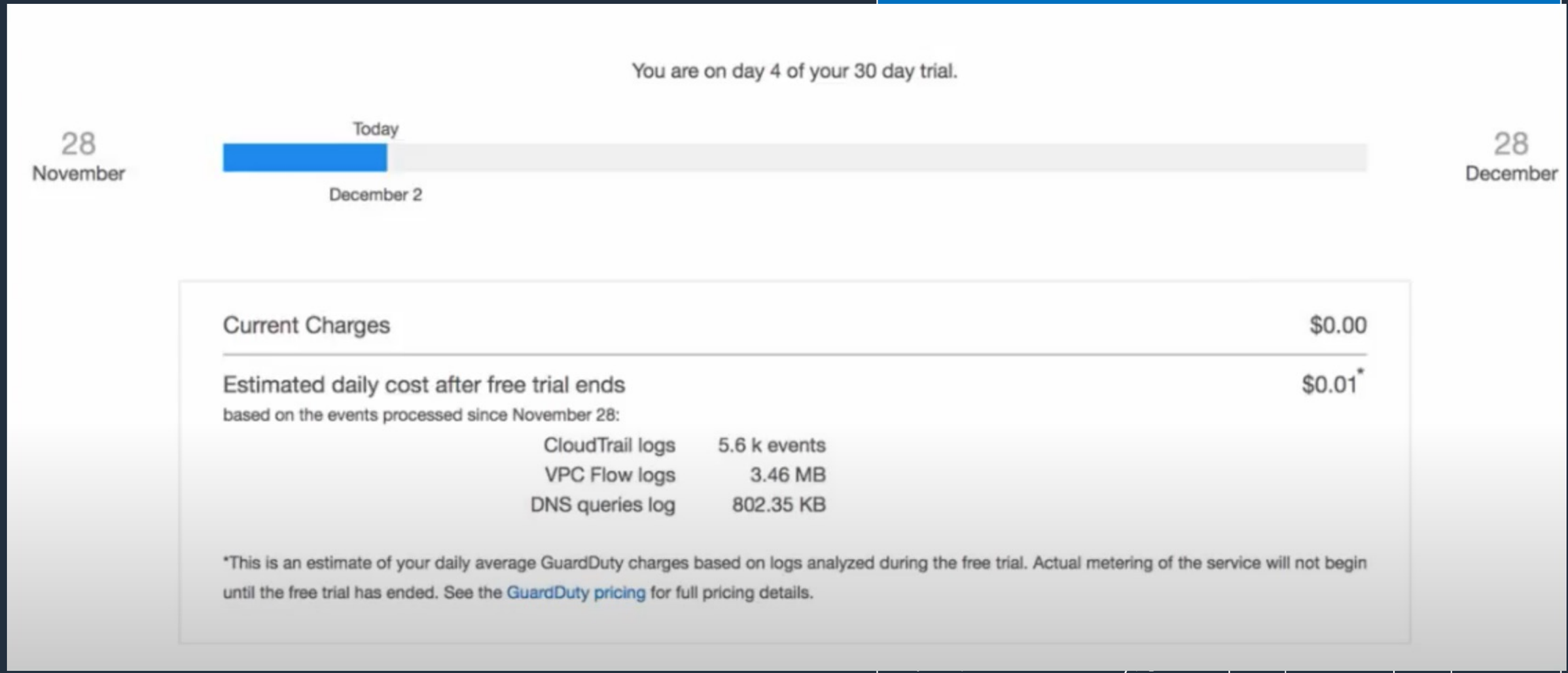
30日間の無料トライアルで料金試算が可能

https://aws.amazon.com/guardduty/pricing/

| | 東京 | 大阪 |
|---|---|---|
| VPC フローログと DNS ログ分析 | | |
| 最初の 500 GB/月 | $1.18 | $1.29 |
| 次の 2000 GB/月 | $0.59 | $0.645 |
| 次の 7,500 GB/月 | $0.29 | $0.3225 |
| 10,000 GB/月を超えた場合 | $0.17 | $0.1935 |
| AWS CloudTrail 管理イベント分析 | | |
| 100 万イベント/月 | $4.72 | $5.00 |
| AWS CloudTrail S3 データイベント分析（100万イベント毎） | | |
| 最初の 5 億イベント/月 | $1.04 | $1.032 |
| 次の 45 億イベント/月 | $0.52 | $0.516 |
| 50 億を超えるイベント/月 | $0.26 | $0.258 |
| AWS CloudTrail S3 データイベント分析 (100万イベント毎) | | |
| 最初の 1 億イベント/月 | $2.48 | $2.48 |
| 次の 1 億イベント/月 | $1.24 | $1.24 |
| 2 億を超えるイベント/月 | $0.31 | $0.31 |

# A1. GuardDuty の料金はこちら

| | 東京 | 大阪 |
|---|---|---|
| VPC フローログと DNS ログ分析 | | |




https://aws.amazon.com/guardduty/pricing/

# Q2. パフォーマンス影響はありますか？



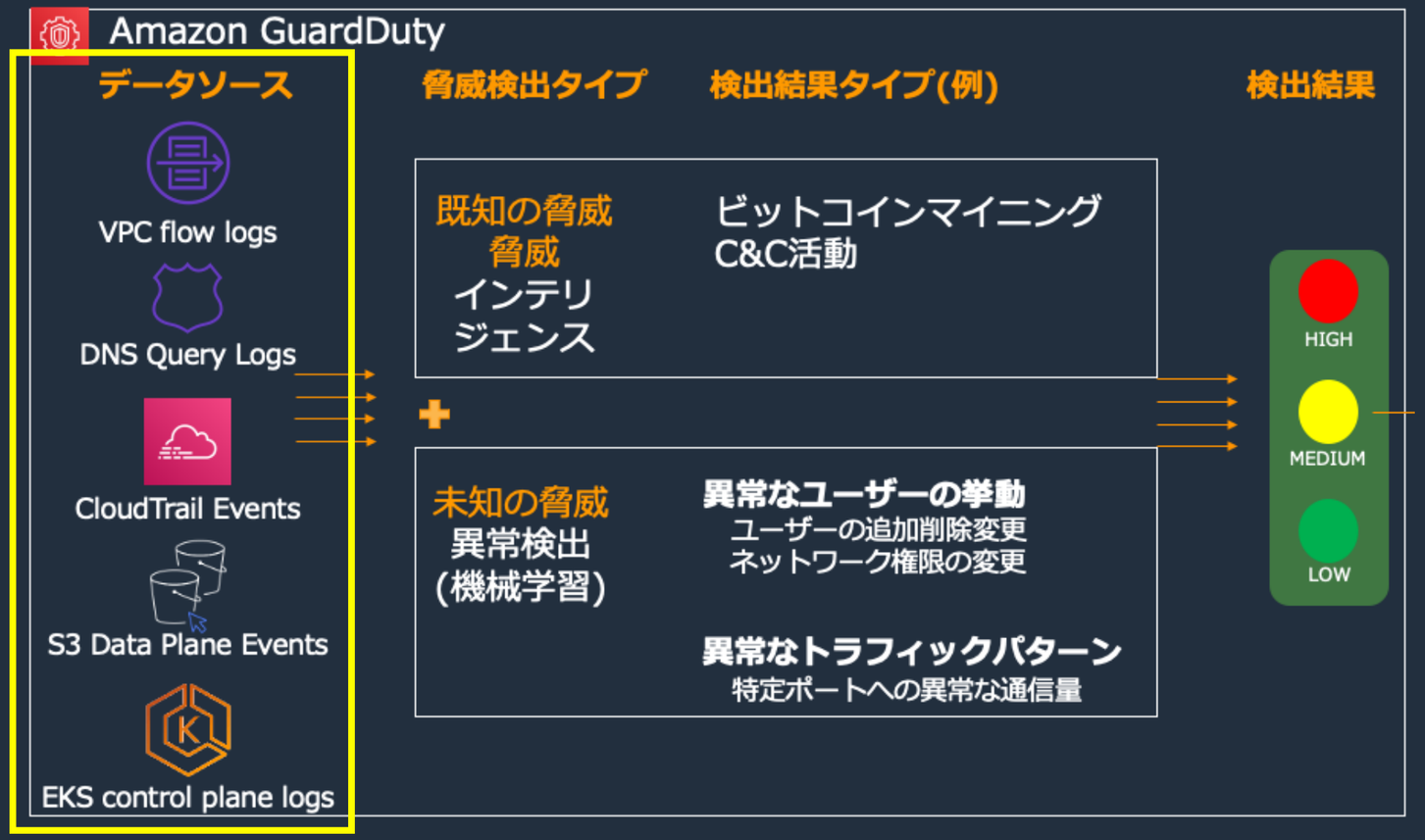
aws

# A2. パフォーマンス影響はありません！



aws

# Q3. CloudTrail など GuardDuty の分析対象となるデータソースのログ出力を事前に設定する必要はありますか？

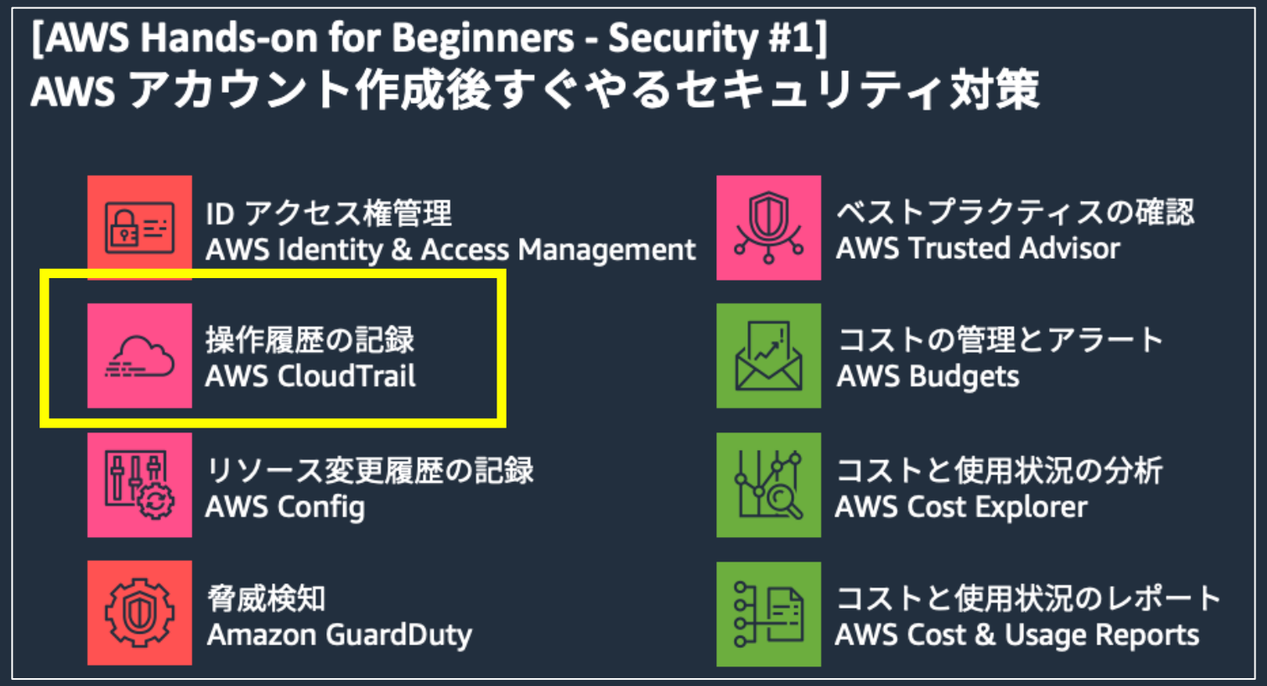


# A3. いいえ。CloudTrail などGuardDuty の分析対象となるデータソースのログ出力を事前に設定する必要はありません。



aws

# A3. いいえ。CloudTrail などGuardDuty の分析対象となるデータソースのログ出力を事前に設定する必要はありません。




GuardDuty 利用上の観点とは関係ないですが、 CloudTrail ログの S3 バケットへの保存は推奨しています。

# Q4. どうやって有効化すればいいの？

# A4.（デモでご案内）

# Q5. 全リージョン一括で有効化したいんだけど、コンソールでポチポチする以外に方法ないの？



aws

# A5. 本日時点で、GuardDuty の全リージョン一括で有効化する機能は提供されておりません。

# A5. 本日時点で、GuardDuty の全リージョン一括で有効化する機能は提供されておりません。

1. CLI でスクリプトを組む
2. CloudFormation テンプレートを書く



aws

# Q6. log4j に関連する脅威を検知することはできますか？



aws

# A6. log4j に関連する問題の特定に役立つ検出結果タイプがアップデートされています。

## Document history for Amazon GuardDuty

PDF | RSS

| Change | Description | Date |
|---|---|---|
| Added Kubernetes protection content for GuardDuty | GuardDuty can now generate findings for your Amazon EKS resources through the monitoring of Kubernetes audit logs. To learn how to configure this feature see Kubernetes protection in Amazon GuardDuty. For a list of findings GuardDuty can generate for Amazon EKS resources, see Kubernetes findings. New remediation guidance has been added to support remediating these findings in the Kubernetes finding remediation guide. | January 25, 2022 |
| Added 1 new finding | A new finding UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS has been added. This finding informs you when your instance credentials are accessed by an AWS account outside your AWS environment. | January 20, 2022 |
| Updated the finding types to help identify issues related to log4j | Amazon GuardDuty has updated the following finding types to help identify and prioritize issues related to CVE-2021-44228 and CVE-2021-45046: Backdoor:EC2/C&CActivity.B; Backdoor:EC2/C&CActivity.B!DNS; Behavior:EC2/NetworkPortUnusual. | December 22, 2021 |
| Finding Changes | UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration has been changed to UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. This improved version of the finding learns the typical locations your credentials are used from to reduce findings from traffic routed through on premise networks. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS | September 7, 2021 |
| Update to GuardDuty SLR | The GuardDuty SLR has been updated with new actions to improve finding accuracy. | August 3, 2021 |
| Added data source information for each finding type. | Finding descriptions now contain information on which data source GuardDuty uses to generate that finding. | May 10, 2021 |
| Retired 13 finding types. | 13 findings have been retired to be replaced with new AnomalousBehavoir findings. Persistence:IAMUser/NetworkPermissions, Persistence:IAMUser/ResourcePermissions, Persistence:IAMUser/UserPermissions, PrivilegeEscalation:IAMUser/AdministrativePermissions, Recon:IAMUser/NetworkPermissions, Recon:IAMUser/ResourcePermissions, | March 12, 2021 |

The following table describes important changes in each release of the *GuardDuty* User Guide.

# A6. log4j に関連する問題の特定に役立つ検出結果タイプがアップデートされています。

## Document history for Amazon GuardDuty

PDF | RSS

| Change | Description | Date |
|---|---|---|
| Added Kubernetes protection content for GuardDuty | GuardDuty can now generate findings for your Amazon EKS resources through the monitoring of Kubernetes audit logs. To learn how to configure this feature see Kubernetes protection in Amazon GuardDuty. For a list of findings GuardDuty can generate for Amazon EKS resources, see Kubernetes findings. New remediation guidance has been added to support remediating these findings in the Kubernetes finding remediation guide. | January 25, 2022 |
| Added 1 new finding | A new finding UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.InsideAWS has been added. This finding informs you when your instance credentials are accessed by an AWS account outside your AWS environment. | January 20, 2022 |
| Updated the finding types to help identify issues related to log4j | Amazon GuardDuty has updated the following finding types to help identify and prioritize issues related to CVE-2021-44228 and CVE-2021-45046: Backdoor:EC2/C&CActivity.B; Backdoor:EC2/C&CActivity.B!DNS; Behavior:EC2/NetworkPortUnusual. | December 22, 2021 |
| Finding Changes | UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration has been changed to UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS. This improved version of the finding learns the typical locations your credentials are used from to reduce findings from traffic routed through on premise networks. UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration.OutsideAWS | September 7, 2021 |
| Update to GuardDuty SLR | The GuardDuty SLR has been updated with new actions to improve finding accuracy. | August 3, 2021 |
| Added data source information for each finding type. | Finding descriptions now contain information on which data source GuardDuty uses to generate that finding. | May 10, 2021 |

※ GuardDuty はあくまで、脅威検知のサービスなので、脆弱性の検出には Amazon Inspector も併用することをお勧めします。
また、根本的なリスク軽減のためには当該脆弱性のパッチ適用等が必要です。

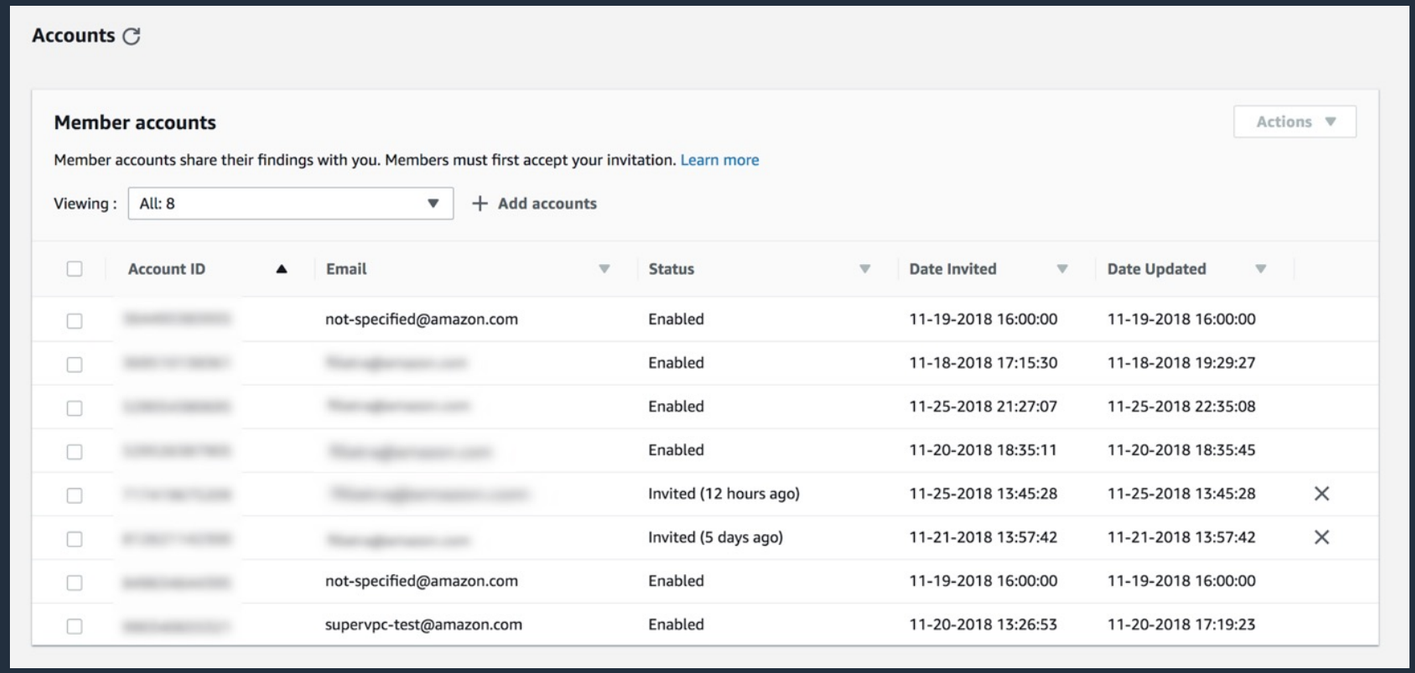
# Q7. AWS Organization を使ってマルチアカウント管理しているのだけれど、GuardDuty も一元管理できる？



aws

# A7. 管理者アカウントで一元管理できます

・管理者アカウントからメンバーアカウントを一元的に管理、検出結果を集約して監視
・AWS Organizations にてマルチアカウントの管理も可能

# Q8. GuardDuty のログの保存期間は？

# A8. コンソールで過去90日間の検出結果を確認できます

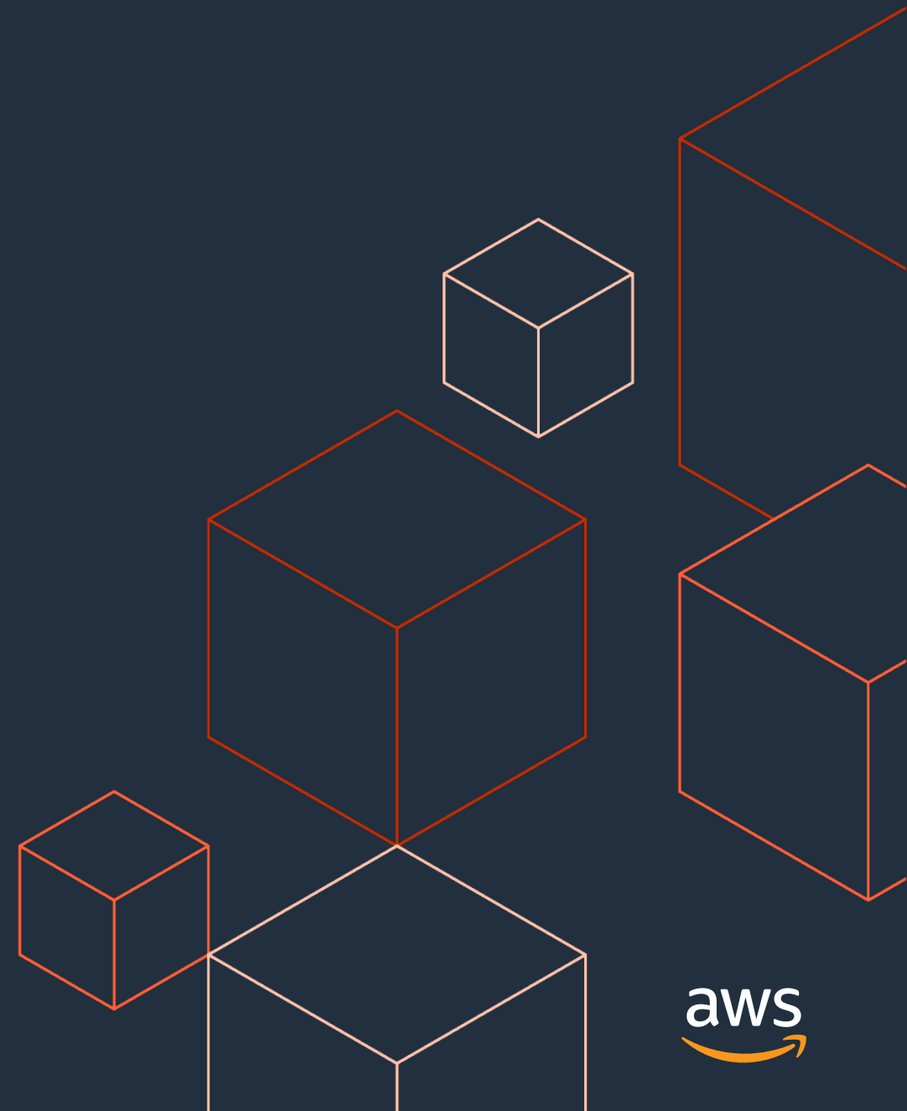

- 90日を超えて、ログを保存したいときは S3 バケットにログをエクスポートしておく
- 長期保存目的の他、外部の分析基盤へのログ連携のためにファイル出力しておく
  - e.g.; SIEM on OpenSearch Service

# SIEM on Amazon OpenSearch Service

- AWS サービスのセキュリティ監視をするためのダッシュボードやログ分析システム
- オープンソースソフトウェアとして公開。テンプレートは無料で利用可能
- マネージドサービスとサーバーレスのみ
- マルチアカウント/マルチリージョン対応
- CloudFormation/CDK によるデプロイ。約30分で完了


https://github.com/aws-samples/siem-on-amazon-opensearch-service

# 次のステップ



# 次のステップ

- GuardDuty の有効化
- 脅威検出結果の確認、対処
  - 「Appendix.検出結果の調査・対応方法」を参照ください。
- AWS Security Hub への情報集約, 可視化
  - 5/12 (木) AWS Security Hub Activation Day 参加を！

# AWS Security Hub Activation Day

- Amazon Web Services Japan G.K.
- 2022/05/12

**AWS Security Hub を使ってセキュリティリスクの可視化をしてみたくなりましたか？**

**以下のイベントによければ参加してください！**

次回おすすめセキュリティセミナー

## AWS Security Hub Activation Day

日時: 2022/05/12 (木) 17:00 ～ 18:00

参加費用: 無料

概要:

Solutions Architect のガイダンスの下、AWS Security Hub をお客様のAWSアカウントで実際に有効化するイベントです。さらに、有効化後、どのように Findings が表示されるのか？どのように対応するべきなのか？など、他サービスとの連携も踏まえてデモを交えてご紹介するイベントです。

参加方法:

申し込みページはございません。お時間になりましたら以下のリンクにアクセスしてください。
https://chime.aws/8954394106

# Thank You!

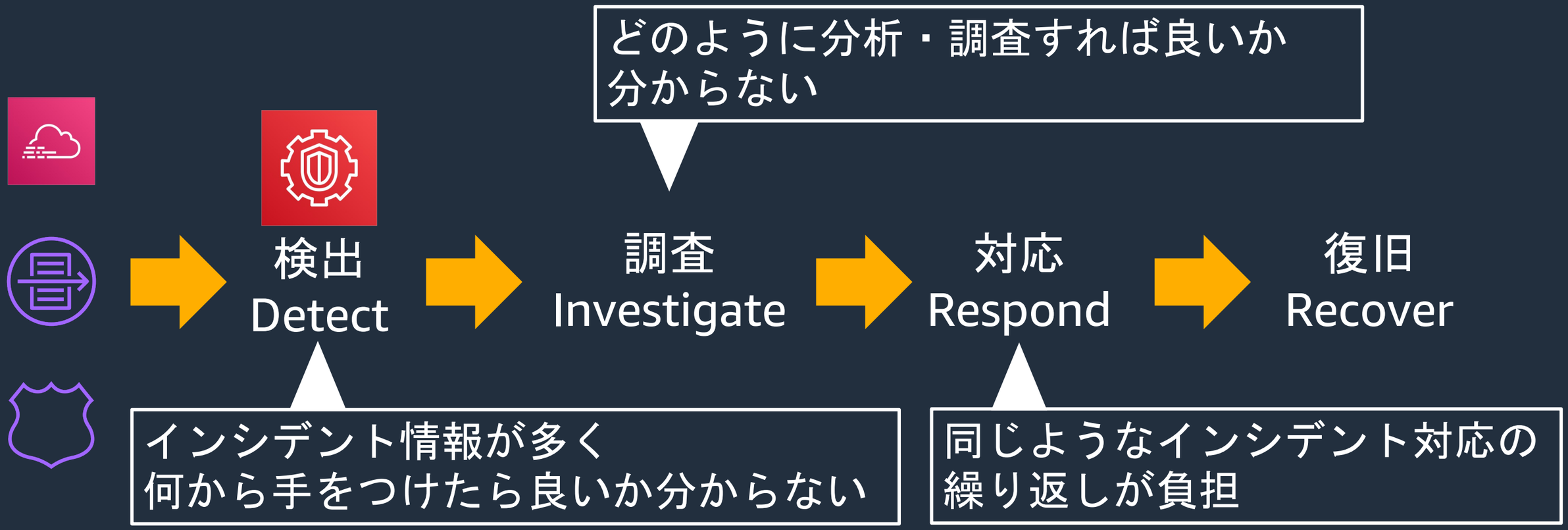
# Appendix. 検出結果の調査・対応方法

# AWS セキュリティ サービス

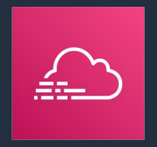


# 脅威を検出してからのワークフロー

# お客様からよくご相談いただく
# セキュリティインシデント対応の課題



# お客様からよくご相談いただく
# セキュリティインシデント対応の課題



どのように分析・調査すれば良いか
分からない

検出結果の見方を理解する

検出
Detect

調査
Investigate

対応
Respond

復旧
Recover

インシデント情報が多く
何から手をつけたら良いか分からない

優先度をつけて対応
フィルター機能を活用

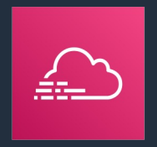
同じようなインシデント対応の
繰り返しが負担

問題ない検出結果の抑制
自動化による運用の効率化



aws

# お客様からよくご相談いただく
# セキュリティインシデント対応の課題



検出
Detect

調査
Investigate

対応
Respond

復旧
Recover

どのように分析・調査すれば良いか
分からない

検出結果の見方を理解する

インシデント情報が多く
何から手をつけたら良いか分からない

優先度をつけて対応
**フィルター機能**を活用

同じようなインシデント対応の
繰り返しが負担

問題ない検出結果の抑制
自動化による運用の効率化



aws

# インシデント情報に優先度をつける

最初から全てのインシデントに対応しようとせず優先度をつける

- 重要度が 高 の検出結果に注目する
- 重要なリソースの結果のみにフィルターする

初期調査で推奨の GuardDuty 検索タイプ

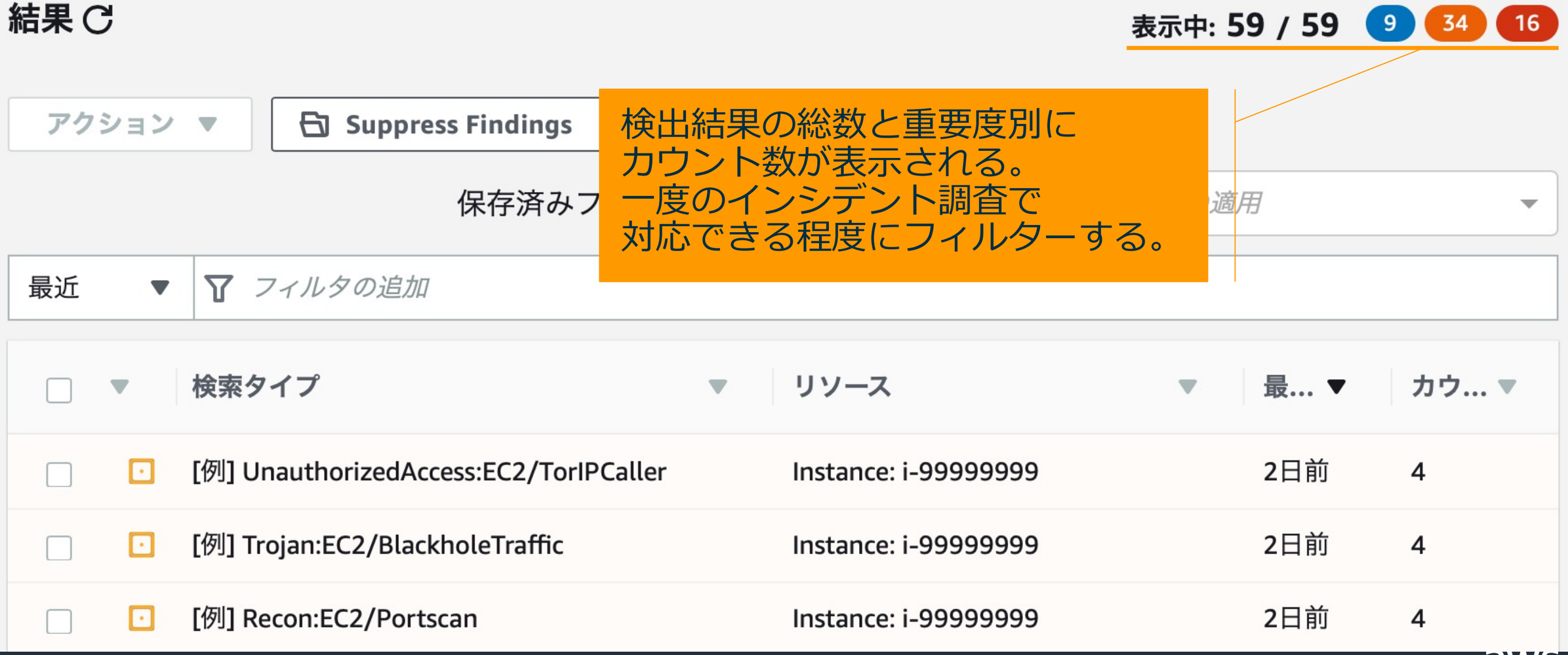
- UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration
- UnauthorizedAccess:IAMUser/TorIPCaller
- CryptoCurrency:EC2/BitcoinTool.B!DNS
- CryptoCurrency:EC2/BitcoinTool.B
- Recon:EC2/PortProbeEMRUnprotectedPort
- UnauthorizedAccess:EC2/TorClient
- UnauthorizedAccess:EC2/TorRelay



aws

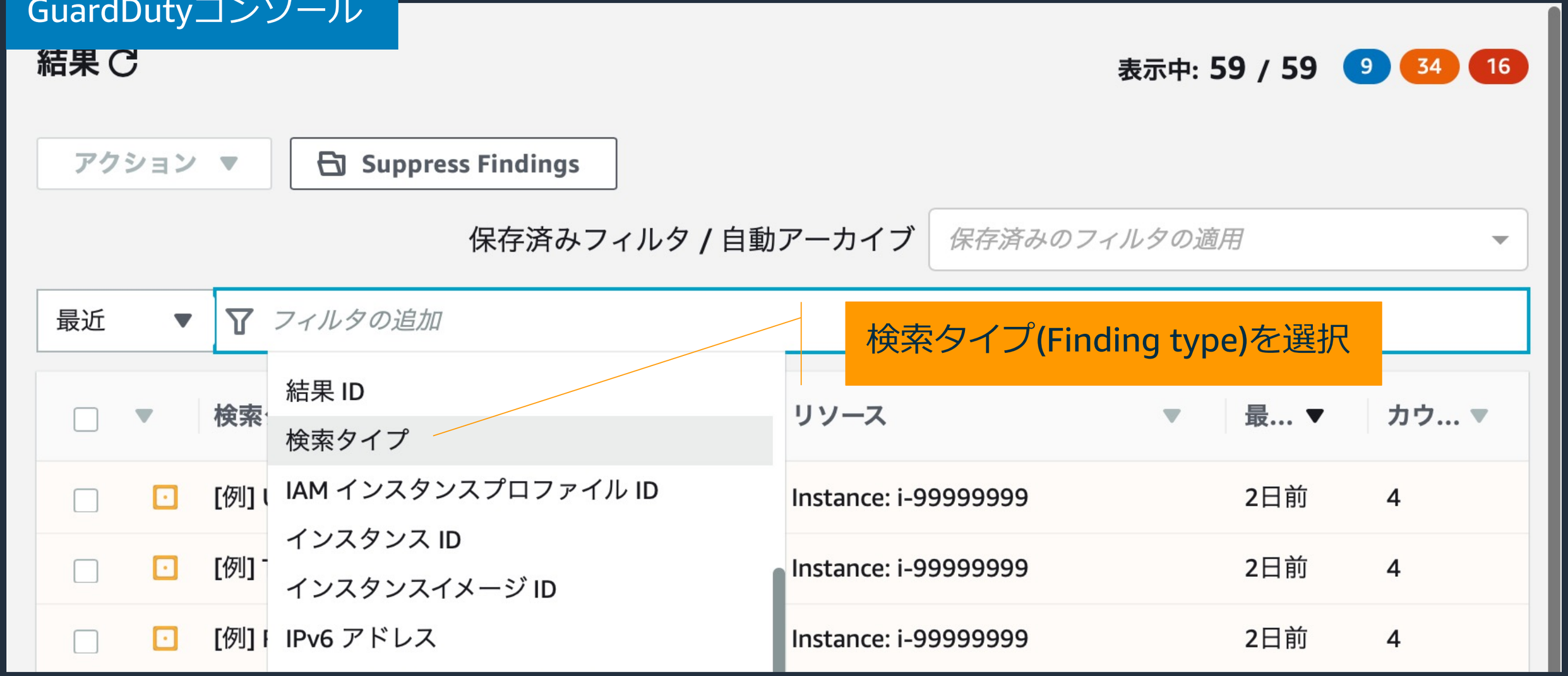
# 【例】複数条件のフィルターの方法(1)

GuardDutyコンソール



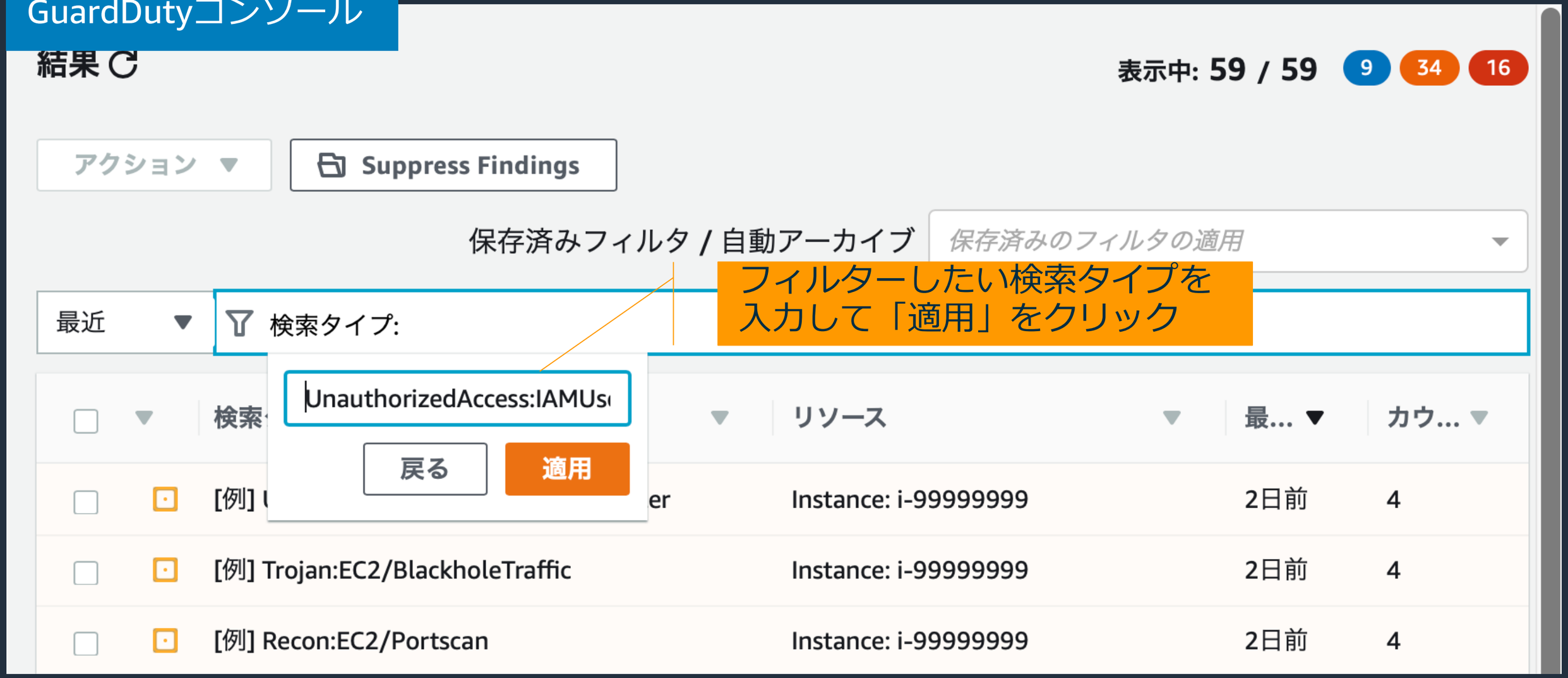
# 【例】複数条件のフィルターの方法(2)

GuardDutyコンソール



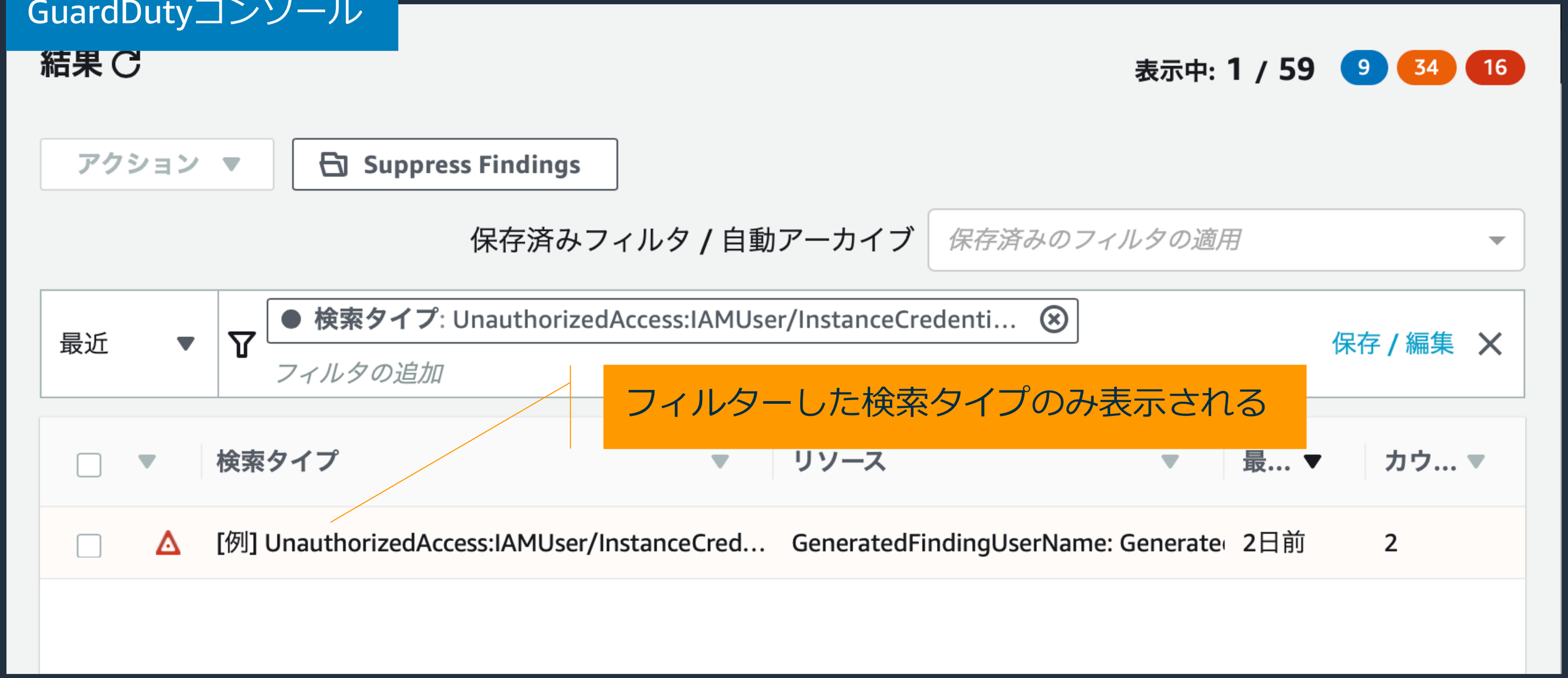
# 【例】複数条件のフィルターの方法(3)

GuardDutyコンソール



# 【例】複数条件のフィルターの方法(4)

GuardDutyコンソール

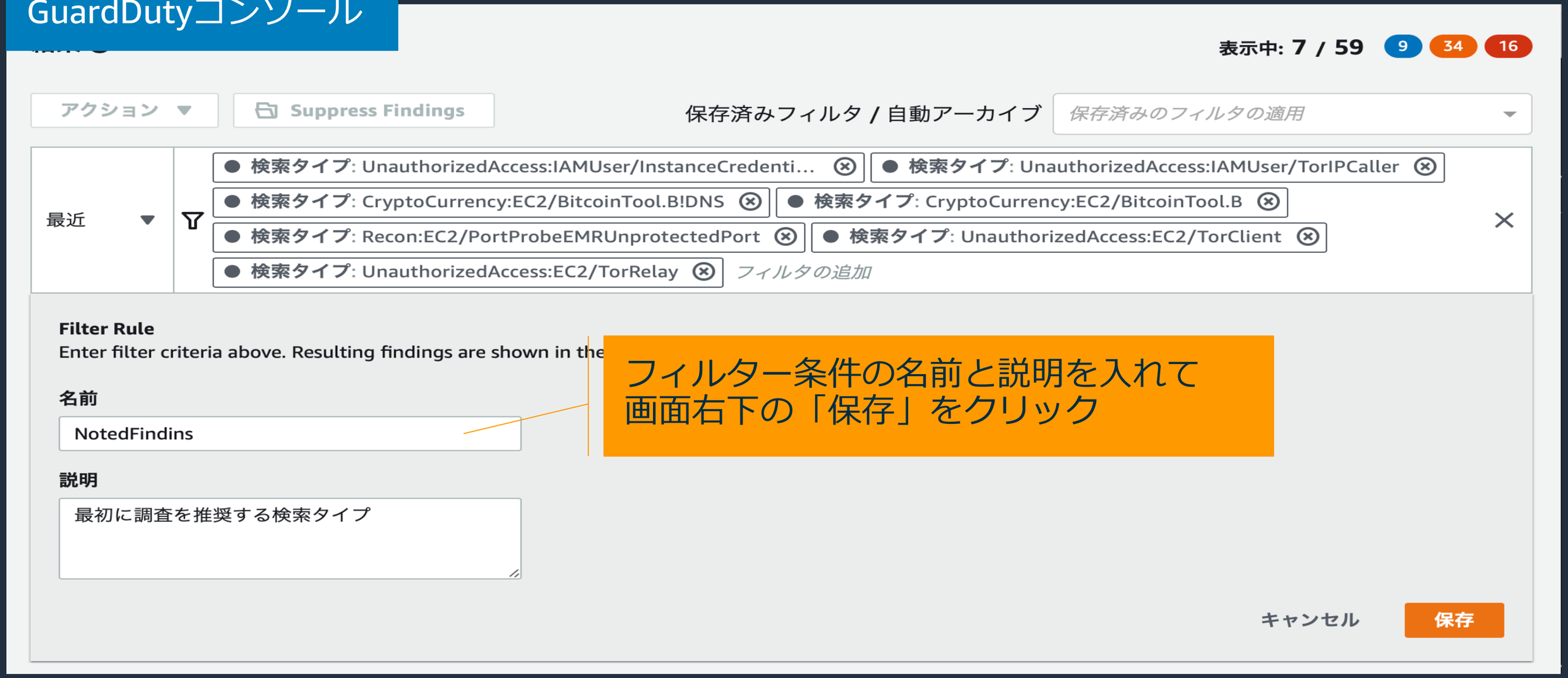


# 【例】複数条件のフィルターの方法(5)

GuardDutyコンソール

# 【例】複数条件のフィルターの方法(6)

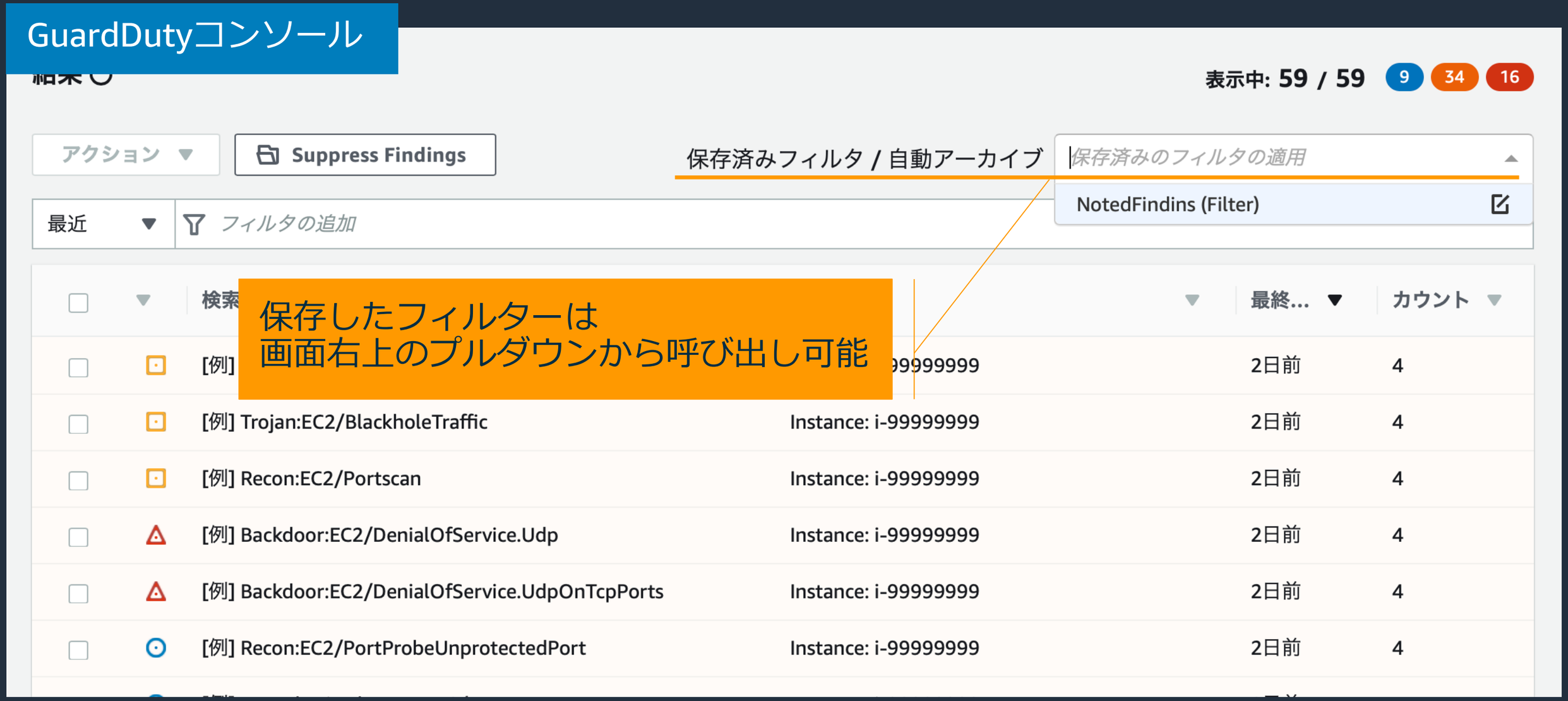
GuardDutyコンソール



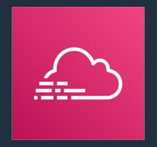

フィルター条件の名前と説明を入れて
画面右下の「保存」をクリック

# 【例】複数条件のフィルターの方法(7)

GuardDutyコンソール



# お客様からよくご相談いただく
# セキュリティインシデント対応の課題



どのように分析・調査すれば良いか
分からない

検出結果の見方を理解する

検出
Detect

調査
Investigate

対応
Respond

復旧
Recover

インシデント情報が多く
何から手をつけたら良いか分からない

優先度をつけて対応
フィルター機能を活用

同じようなインシデント対応の
繰り返しが負担

問題ない検出結果の抑制
自動化による運用の効率化

# 調査の観点とプロセス

1. 検出結果タイプが示す事象を理解する
2. 誤検出または受容できるリスクかを判断する
3. 本格調査をする
4. 完了した調査をクローズする

次の検出結果の分析を例に説明
「UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration」

※ InstanceCredentialExfiltration は OutsideAWS と InsideAWS の2種類があります。
資料作成時点では InsideAWS がなかったので OutsideAWS と読み替えてください。



aws

# 1. 検出結果タイプが示す事象を理解する

迅速かつ正確に調査し、セキュリティインシデントの詳細把握をするには、
検出した検索タイプそのもの理解が不可欠です

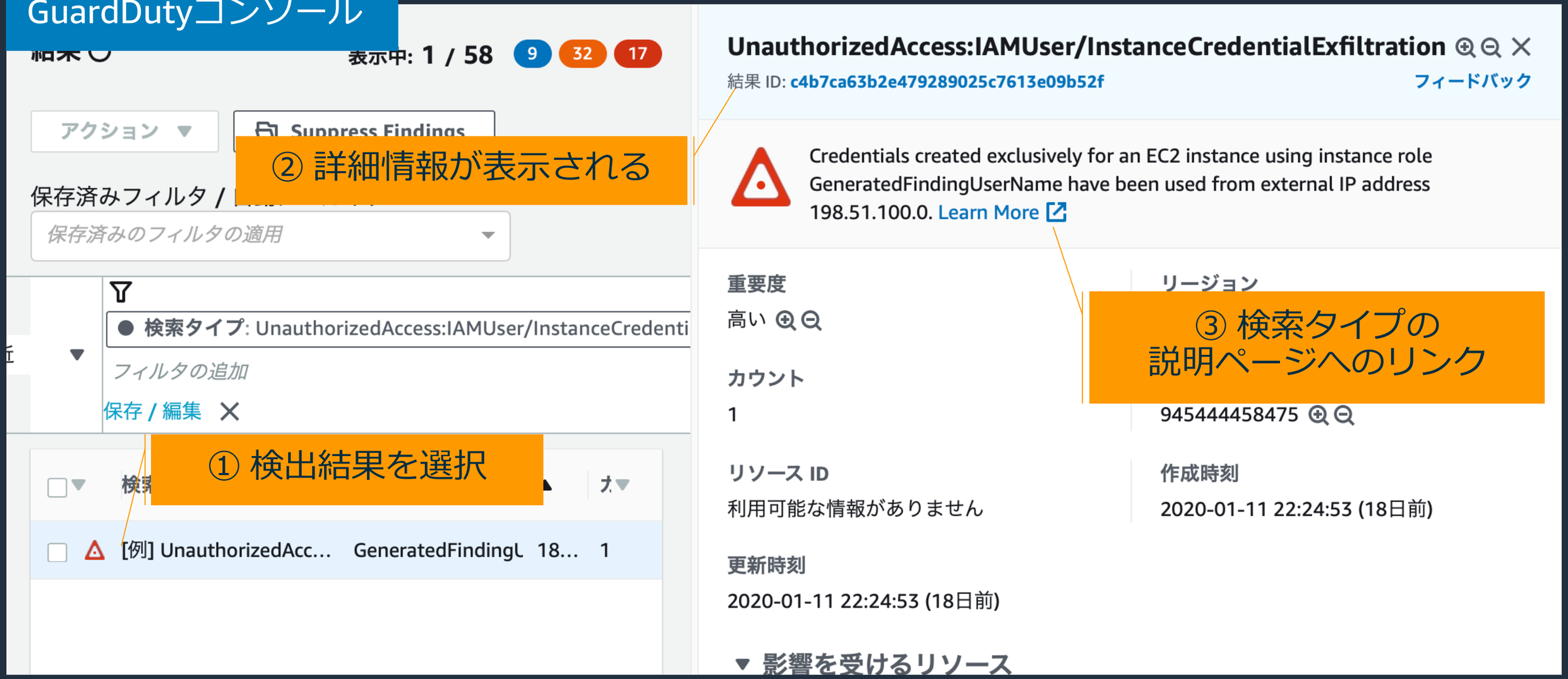
理解後にできることの一例
- なぜ検出したかのロジックの把握
- 正常通信を誤って検出(誤検出)したかの判断
- お客様環境でのリスク評価
- 関連ログの特定



aws

# 検出結果の詳細を確認する

GuardDutyコンソール



# 検出結果の説明ページから読み取れること

AWS > ドキュメント > Amazon GuardDuty > Amazon Guard Duty ユーザーガイド　フィードバック

## UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration

### 結果の説明

検出ロジック

**インスタンス起動ロールを通じて EC2 インスタンス専用に作成された認証情報が外部 IP アドレスから使用されています。**

この結果では、AWS アカウントの EC2 インスタンスで作成された一時的な AWS 認証情報を使用して、EC2 外のホストから AWS API オペレーションを実行しようとしている試行について知らせます。EC2 インスタンスが侵害されていて、このインスタンスの一時的な認証情報が密かに AWS 外のリモートホストに抽出されている可能性があります。AWS は、一時的な認証情報を作成したエンティティ (AWS アプリケーション、EC2、Lambda など) 外にその認証情報を再配布することはお勧めしません。ただし、承認されたユーザーは EC2 インスタンスから認証情報をエクスポートして正当な API コールを行うことができます。攻撃の可能性を排除してアクティビティが正当であることを確認するには、これらの認証情報を割り当てる先の IAM ユーザーに問い合わせてみます。詳細については、「侵害された AWS 認証情報の修正」を参照してください。

この結果が生成されるのは、VPC インターネットゲートウェイ (IGW) からではなく、オンプレミスゲートウェイからエグレスされるという方法で、インターネットトラフィックがルーティングされるように、Amazon VPC ネットワークが設定されている場合です。AWS Direct Connect、AWS Outposts、VPC VPN 接続の使用といった一般的な設定では、この方法でトラフィックがルーティングされる可能性があります。この予期され
動アーカイブ 構成されるル 最初のフィル
UnauthorizedA iltration であ 条件は、オンプレミスインターネットゲートウェイの IP アドレスまたは ASN です。IP ベースのフィルタの場合、「API caller IPv4 Address (API 発信者の IPv4 アドレス)」条件を使用します。ASN ベースのフィルタの場合、「API caller ASN name (API 発信者の ASN 名)」または「API caller ASN ID (API 発信者の ASN ID)」を使用します。GuardDuty は引き続き、自動アーカイブフィルタルールに一致する結果を生成します。ただし、このルールにより、これらの結果は結果アーカイブに直接移動されます。CloudWatch イベント ルールのイベントがトリガーされたり、他のダウンストリーム統合に送信されたりしません。詳細については、「結果のフィルタリング」を参照してください。

被害時の対応方法

誤検出のパターン

誤検出有無の確認方法

### デフォルトの重要度: 高



aws

# 説明ページから得られたこと

- EC2の認証情報を窃取され悪用された可能性あり
  - EC2が生成した認証情報が外部からのAPIコールで利用された
- デフォルトの危険度：高
- 誤検出するケース
  - オンプレ経由でグローバル IP による API 呼び出しを行う 等
- 誤検出の確認方法
  - 認証情報を使用した IAM ユーザーに問い合わせる
- 誤検出ではない場合の対応方法
  - AWS アカウントが侵害された場合の説明ページを参照

# 2. 誤検出または受容できるリスクかを判断

想定できる、または受容可能なリスクのイベントかを判断する

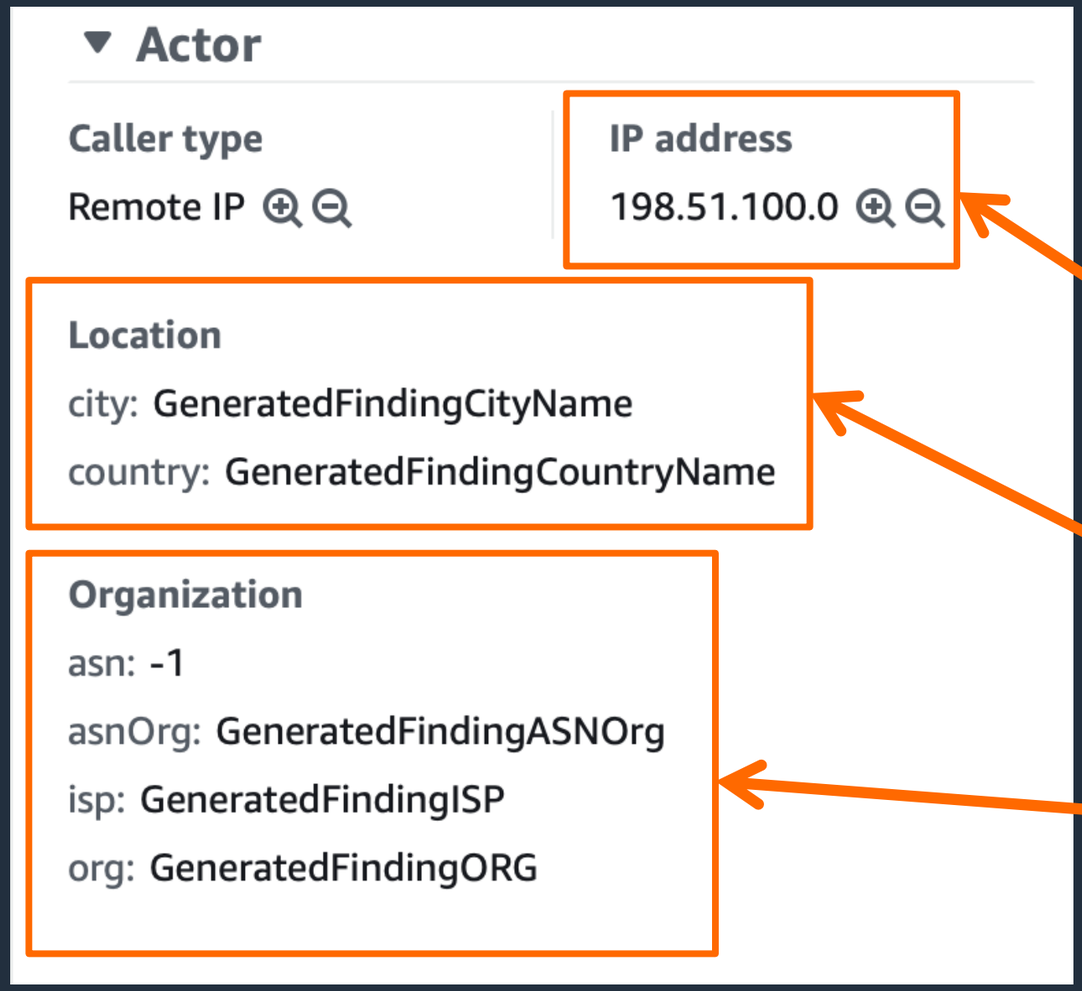
判断基準例）
- 脆弱性診断ツールによるポートスキャン
- 要塞化されたホストへのSSHの総当たり攻撃
- インターネットに公開しているサービスへのポート調査
  (Webサーバーなど)

問題ない検出結果と断定できない　⇒ 次のプロセスへ
問題ない検出結果である　⇒ 次はのプロセスはスキップ



aws

# 正常な通信の誤検出であるかを確認する




**Actor**を確認
今回の場合は通信元の情報

- IP Addressはお客様のIPか？
- お客様拠点の所在地か？
- 契約しているISPか？

※ 参考：GuardDuty 結果の検索と分析

# 3. 本格調査

問題ない検出結果と判断できなければより深い調査を行う

準備：構成図等からインシデントが発生したシステムを把握
　　痕跡の残るログを収集し結びつける

ログ分析・調査の仮説検証アプローチの例
- 調査目的を決め、仮説を立てる
- 特定のキー(特に異常値/外れ値)で関連ログを抽出
- 抽出した関連ログを分析し、仮説の検証を繰り返す

最終の調査目的：影響・被害範囲・根本原因に対する結論を得る



aws

# 【例】攻撃の最初の時間を特定する(1)

【目的】攻撃の最初の時間を特定したい
【仮説】IP(198.51.100.0)で抽出すれば判明するはず
【調査】GuardDuty、CloudTrail、VPC Flow LogsをIPで検索

■ GuardDutyで検索する場合
検索式：「API 発信者の IPv4 アドレス」198.51.100.0でフィルター

■ CloudTrailをCloudWatch Logs Insightで検索
検索式：filter sourceIPAddress="198.51.100.0"



aws

# 【例】攻撃の最初の時間を特定する(2)

■ VPC Flow LogsをCloudWatch Logs Insightで検索

検索式：filter srcAddr="198.51.100.0"

■ VPC Flow LogsとCloudTrailをCloudWatch Logs Insightで串刺し検索

検索式：

filter srcAddr="198.51.100.0” or sourceIPAddress="198.51.100.0”



aws

# 4. 完了した調査をクローズする

- 調査・対応が完了したセキュリティインシデントはクローズする
  - 未対応のインシデントと区別できるようにする
  - 新規に発生したインシデントに迅速に対応
- GuardDutyではアーカイブ機能を使うことで実現できる



aws

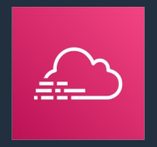
# 対応完了した検出結果をアーカイブする(1)

GuardDutyコンソール

# 対応完了した検出結果をアーカイブする(2)

GuardDutyコンソール

# お客様からよくご相談いただく
# セキュリティインシデント対応の課題



どのように分析・調査すれば良いか
分からない

検出結果の見方を理解する

検出
Detect

調査
Investigate

対応
Respond

復旧
Recover

インシデント情報が多く
何から手をつけたら良いか分からない

優先度をつけて対応
フィルター機能を活用

同じようなインシデント対応の
繰り返しが負担

問題ない検出結果の抑制
自動化による運用の効率化



aws

# インシデント対応の効率化

- 繰り返し発生する問題ない検出結果の抑制

- 自動化による運用の効率化
  - 脅威を検知したら自動で通知する
  - 脅威を自動で修復する仕組みを構築する



aws

# インシデント対応の効率化

- 繰り返し発生する問題ない検出結果の抑制

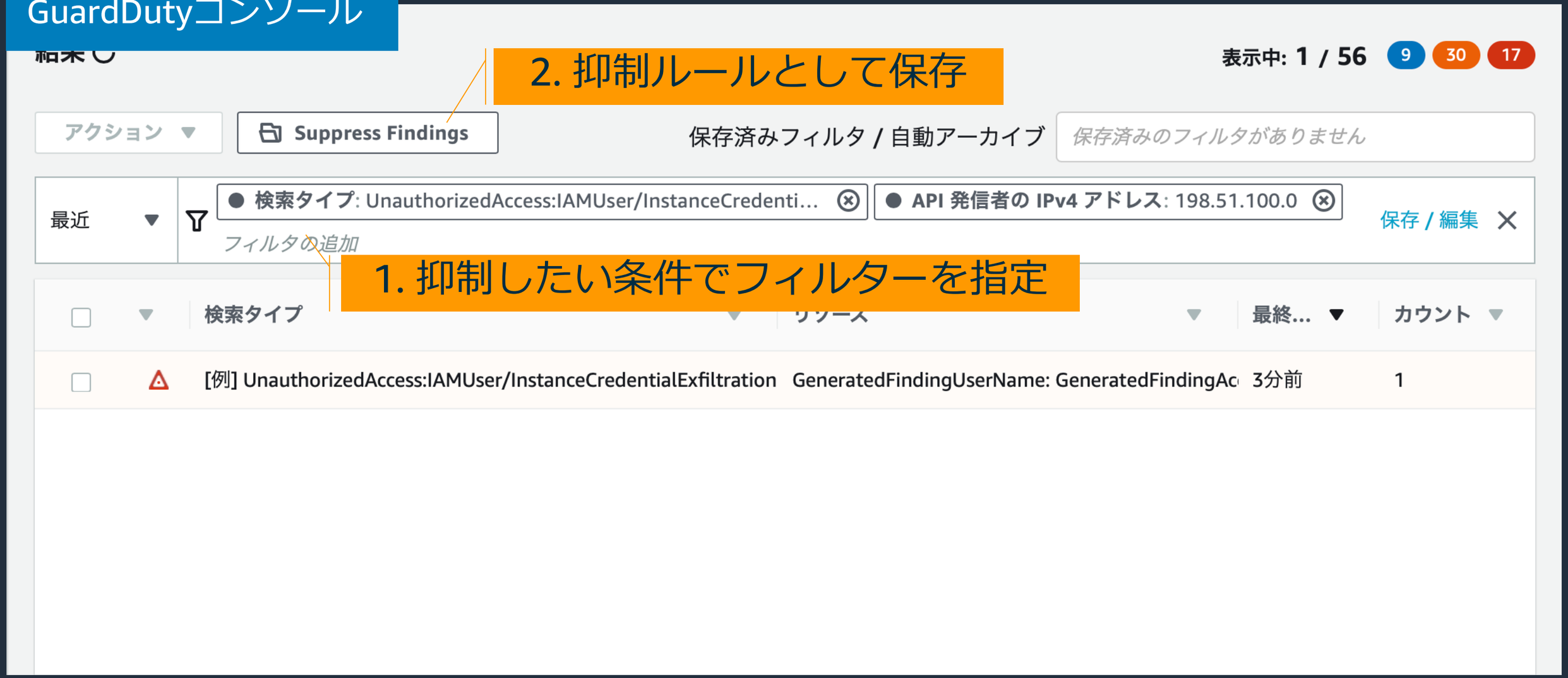
- 自動化による運用の効率化
  - 脅威を検知したら自動で通知する
  - 脅威を自動で修復する仕組みを構築する



aws

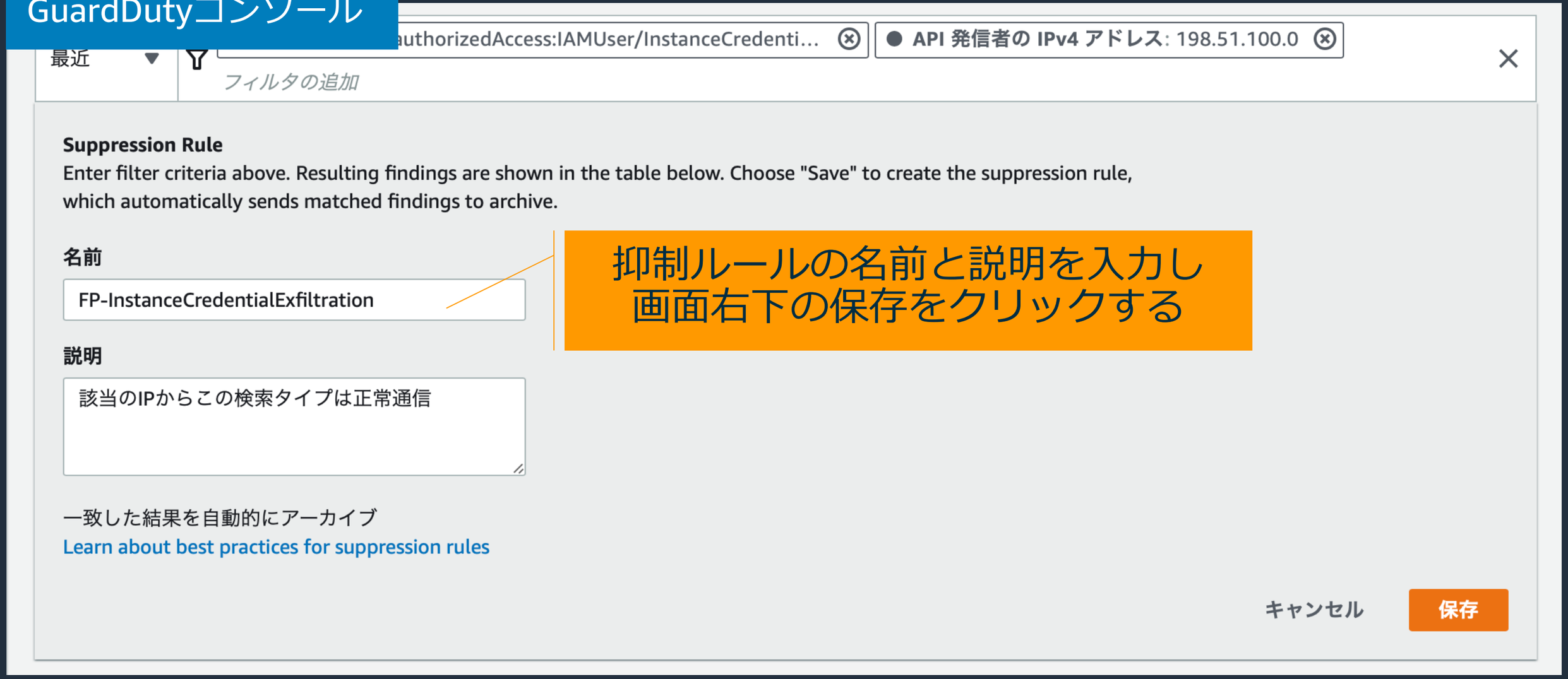
# 【例】GuardDuty検出結果の抑制方法(1)

GuardDutyコンソール



# 【例】GuardDuty検出結果の抑制方法(2)

GuardDutyコンソール




抑制ルールの名前と説明を入力し
画面右下の保存をクリックする