CloudShift

Stylez

株式会社スタイルズ

2022年2月8日

# 30分でわかる！
# Amazon GuardDutyによる
# セキュリティ脅威検知

aws partner network

aws partner network Advanced Consulting Partner

RANCHER PARTNER NETWORK

ZABBIX CERTIFIED PARTNER

Nextcloud Gold partner

vmware PARTNER PROFESSIONAL SOLUTION PROVIDER

# 自己紹介

- 馬場 潤一（Junichi Baba）
- 株式会社スタイルズ
  - AWS上でのアプリ開発・インフラ構築
    チームリーダー
- 好きなAWSサービス
  - CloudFormation、Systems Manager、ECS(Fargate)

# 本日、お話しする内容

## 対象

- AWS上で発生する様々なセキュリティ脅威を検知したい方
- Amazon GuardDutyを導入しようか検討されている方

## ゴール

- Amazon GuardDutyはどのようなサービスなのかを理解する
- Amazon GuardDutyの基本的な利用方法を理解する

# AWS上のセキュリティ脅威と対策

# セキュリティ脅威とその兆候

## ➢ サイバー攻撃だけでも様々な種類がある

- DoS
- DDoS
- SQL インジェクション
- クロスサイト スクリプティング
- ゼロデイ攻撃
- パスワードリスト 攻撃
- マルウェア
- 不正アクセス
- その他

サイバー攻撃が実行される前には、不審な予備動作が発生していることが多い
　例）攻撃前にポートスキャンして攻撃可能なポートを確認する
　例）AWSコンソールへのサインインを様々なパスワード文字列で試す

このような攻撃につながる不審な動作を検知・通知するサービス
＝「Amazon GuardDuty」

# Amazon GuardDuty

# Amazon GuardDutyとは

## セキュリティ観点における様々な脅威リスクを検知するサービス

・細かい設定は不要。機能を有効化する程度で利用可能
・機械学習の仕組みにより不審な動作を分析・判断

不審な動作を見逃してしまったり、正常な動作を誤検知してしまう可能性はある

発見された脅威に対する対処は自分で実施する必要がある
※あくまで被害の早期検出や把握が目的のサービス

# Amazon GuardDutyとは

## ➢ 検知できる概要の例

2021/12/22 Log4jの脆弱性を狙う攻撃の検出をサポート！

・AWS上のリソースが攻撃を受けている　※DoSやリモートからのコマンド実行
・怪しい振る舞い　※通常とは異なるポートで通信している等
・暗号通貨関連のアクティビティ
・防御対策を回避する目的の挙動　※ログや通知の無効化
・脆弱性診断を受けている
・ポートスキャン等で脆弱性を探されている
・承認されていないユーザによる不審な挙動
・世界各地から同時に同じIAMユーザがコンソールログインした

詳細な検知内容の説明はこちらのURLを参照

【Amazon GuardDuty タイプの検索】
https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_finding-types-active.html

# Amazon GuardDutyとは

## 料金

保存されるイベントやログの費用は別途必要

・分析されたイベント数やログデータサイズ（データソース）に依存

東京リージョン価格

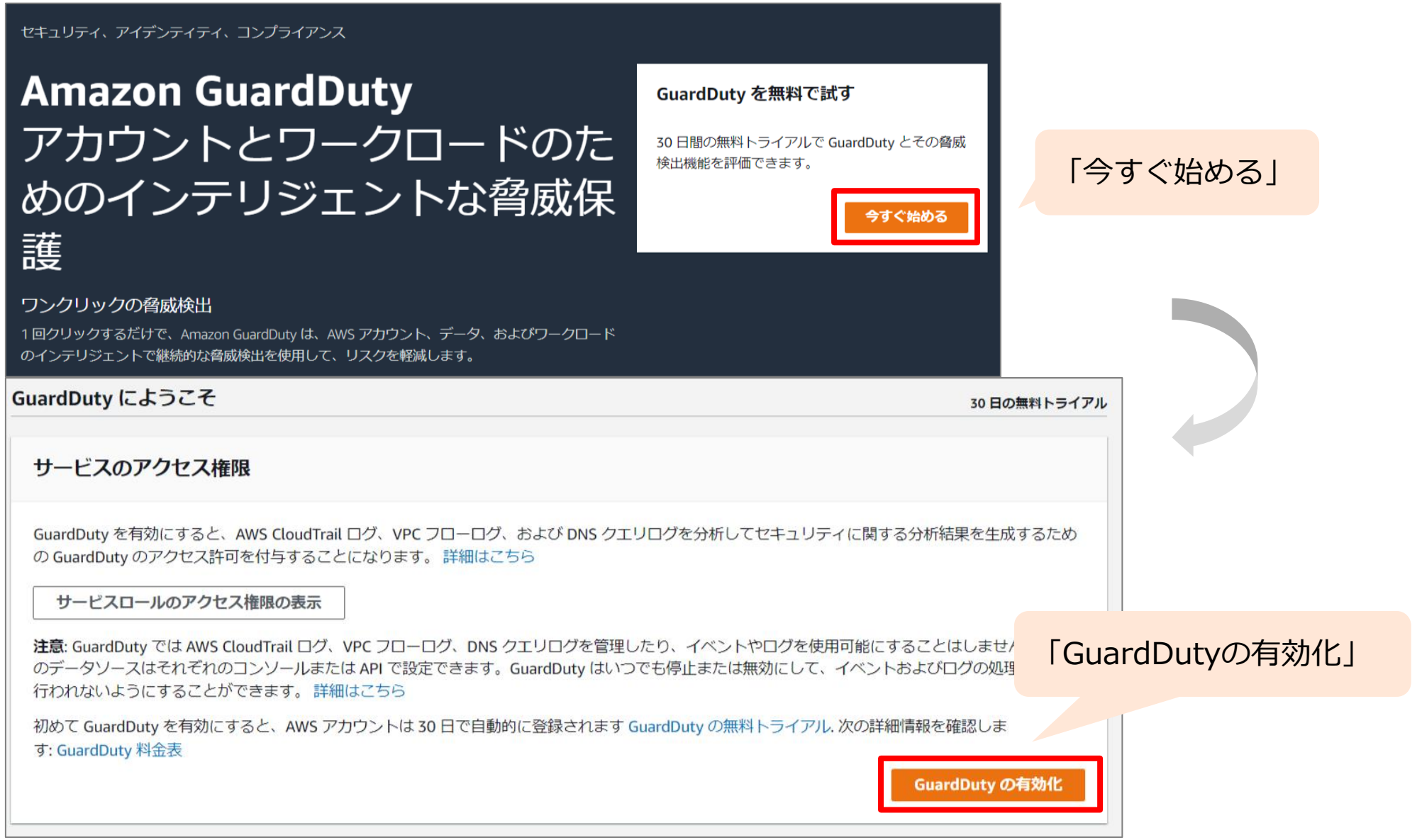
| CloudTrail 管理イベント分析 | |
|---|---|
| 100 万イベント/月あたり | 100 万イベントあたり 4.72USD |

| CloudTrail S3データイベント分析 | |
|---|---|
| 最初の5億イベント/月 | 100 万イベントあたり 1.04USD |
| 次の45億イベント/月 | 100 万イベントあたり 0.52USD |
| 50億を超えるイベント/月 | 100 万イベントあたり 0.26USD |

| VPCフローログとDNSログ分析 | |
|---|---|
| 最初の500 GB/月 | GBあたり 1.18USD |
| 次の 2,000 GB/月 | 0.59USD/GB |
| 次の 7,500 GB/月 | 0.29USD/GB |
| 10,000 GB/月を超えた場合 | 1GB あたり 0.17USD |

# Amazon GuardDutyの利用方法

# Amazon GuardDutyの有効化



# Amazon GuardDutyの有効化

# テストイベントの作成

本当に脅威が検出されるかを確認するために、下記の流れでイベントを作成・確認します。

あくまで動作検証用に実施するものであり、通常は実施する必要はない

1. 脅威リスト（悪意あるIP）として、自分のPCが利用するグローバルIPアドレスを登録

    - 脅威リストファイルの作成
    - 脅威リストファイルのアップロード
    - 脅威リストをGuardDutyへ登録

2. 自分のPCからAWSコンソールにアクセスし、どのようなイベントが生成されるかを確認

# テストイベントの作成　～脅威リストファイルの作成～

## ➢ 任意の場所で下記内容のファイルを作成

- untrustip.txt

```
49.58.159.251
49.58.159.0/24
```

グローバルIPアドレスを記載（サブネット単位でも可能）
※ 1 行：1 IP

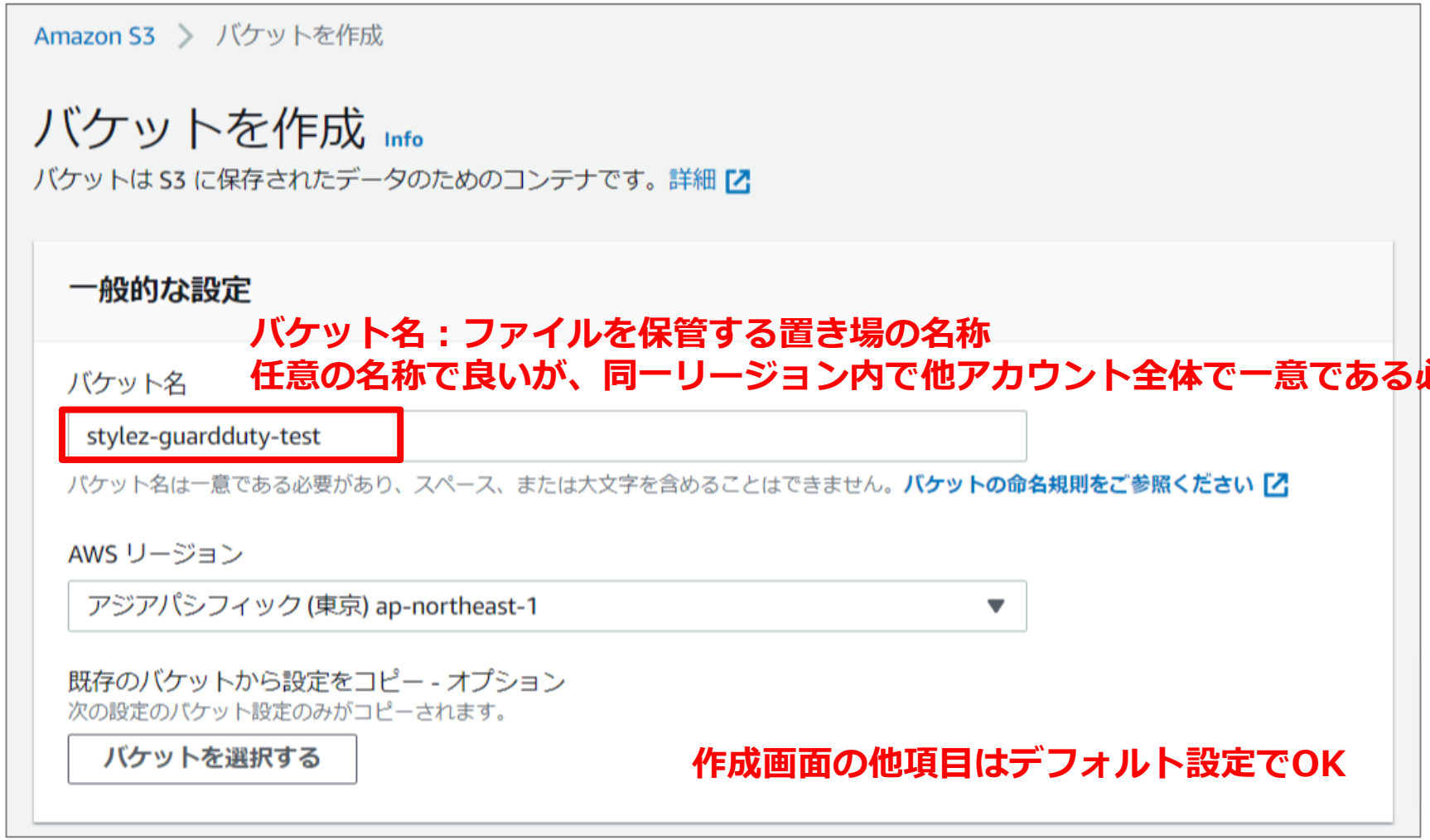
試す際はご自分のIPに置き換えてください。
https://checkip.amazonaws.com/

# テストイベントの作成　～脅威リストファイルのアップロード～

## ➢ ファイル格納用のS3バケット（ストレージ）を作成

# テストイベントの作成　～脅威リストファイルのアップロード～

- ファイル格納用のS3バケット（ストレージ）を作成



# テストイベントの作成　～脅威リストファイルのアップロード～

## S3バケットにファイルを格納

# テストイベントの作成　～脅威リストファイルのアップロード～

## S3バケットにファイルを格納

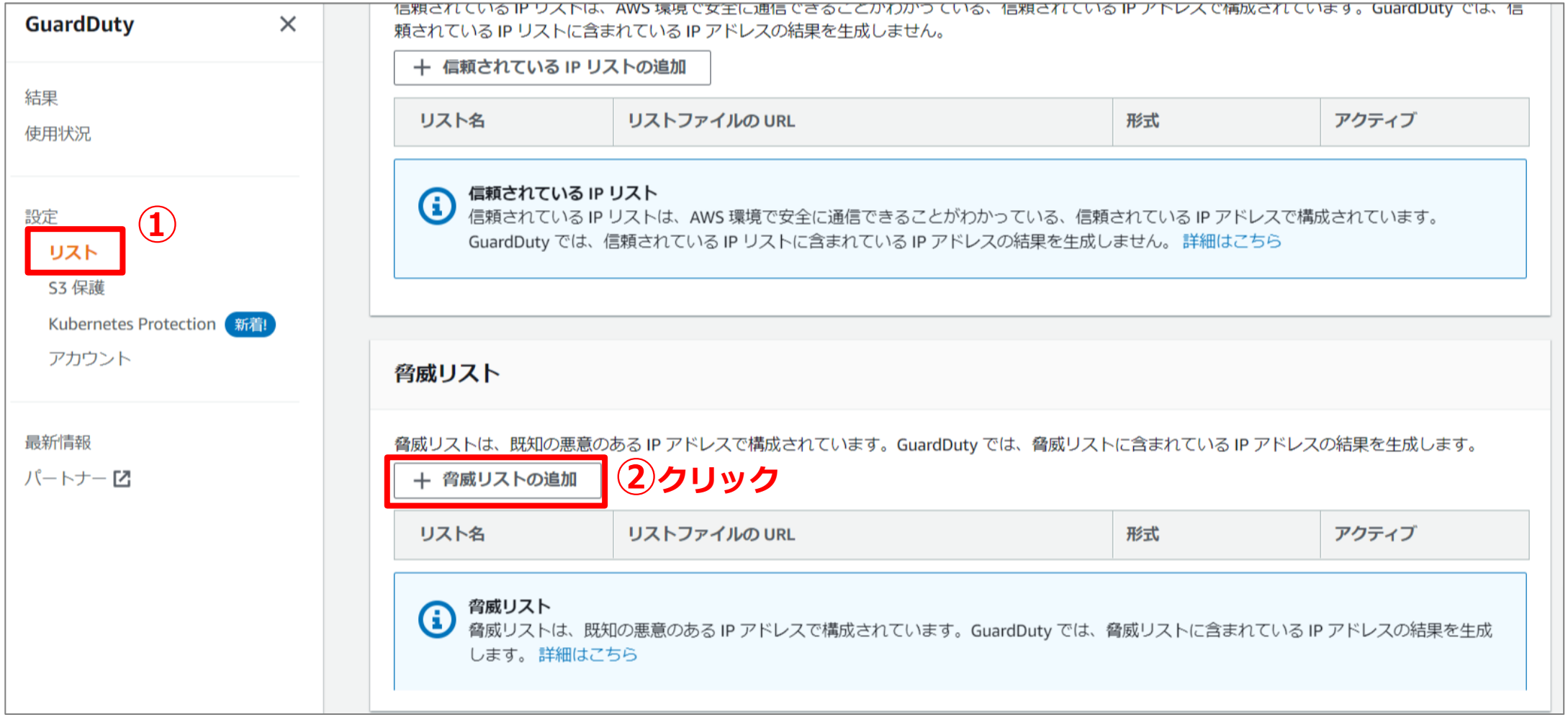

**ここを押すとファイルアップロード画面になるので、作成したuntrustip.txtを選択してアップロード**

# テストイベントの作成　～脅威リストファイルのアップロード～

## ➢ S3バケットにファイルを格納

# テストイベントの作成　～脅威リストをGuardDutyへ登録

## ➤ 脅威リストの登録



# テストイベントの作成　～脅威リストをGuardDutyへ登録～

## ➢ 脅威リストの登録


リスト名は任意：用途が分かる名称に

S3バケットにアップロードした際にコピーしたURLを貼りつけ

プレーンテキスト

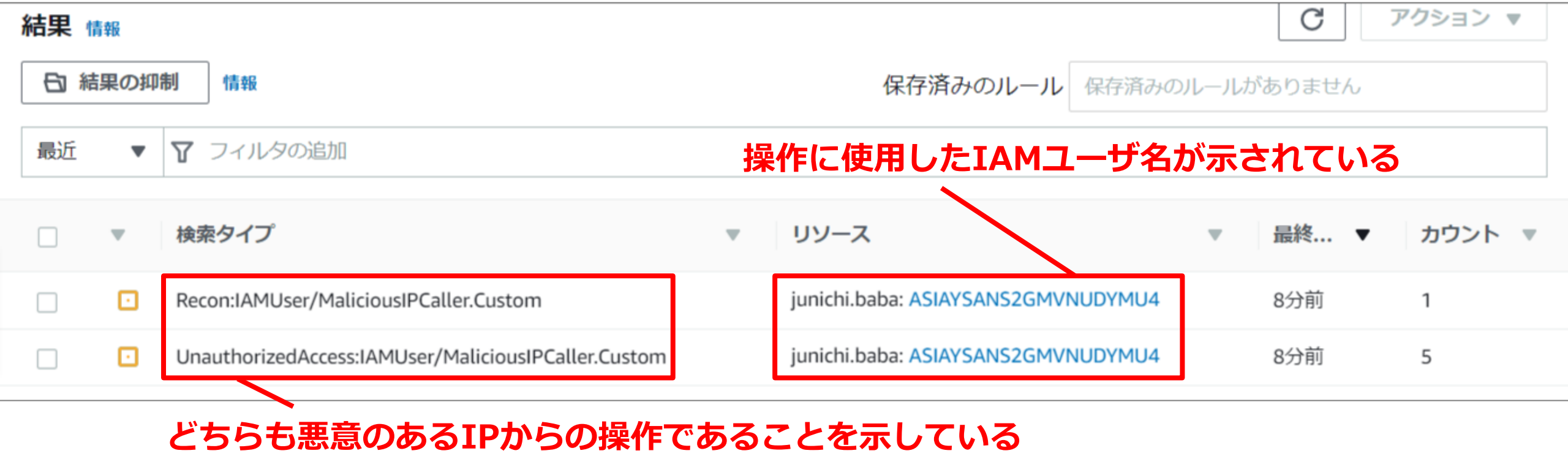
「同意します」にチェック

# テストイベントの作成　～脅威リストをGuardDutyへ登録

## ➢ 脅威リストの登録

**信頼されているIPリストに登録することで、検出されなくなる**

# テストイベントの作成　～検出結果～

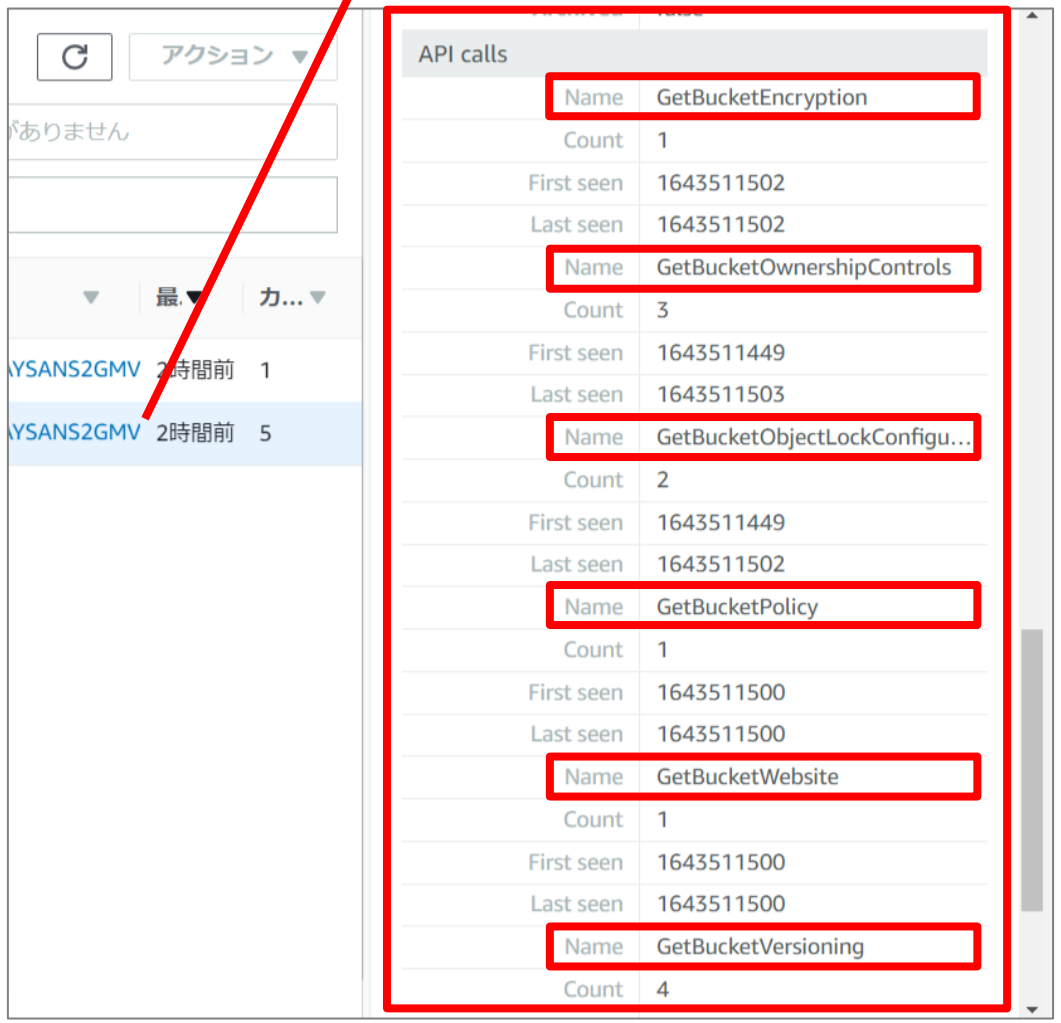



詳細な検知内容の説明はこちらのURLを参照

【Amazon GuardDuty タイプの検索】
https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_finding-types-active.html

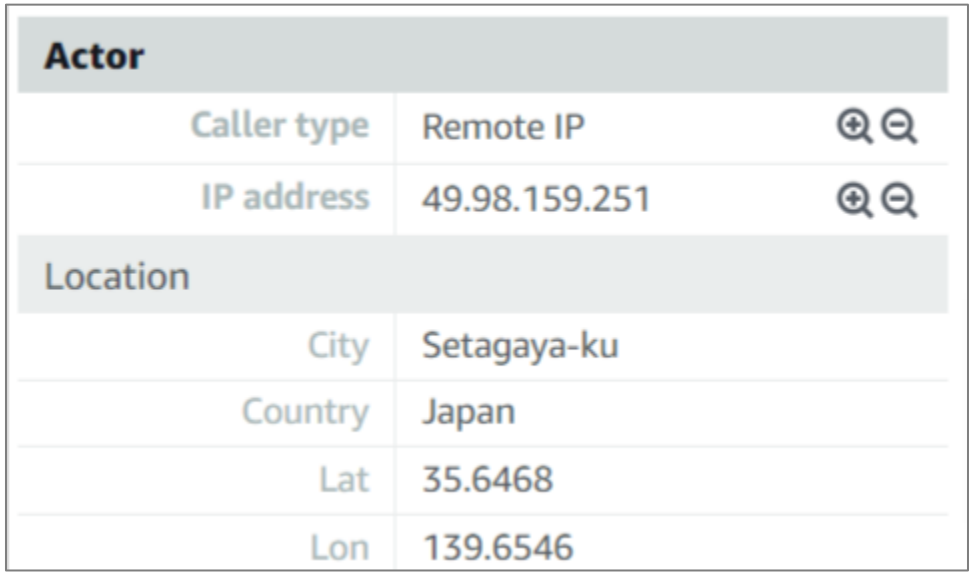
# テストイベントの作成　～検出結果～

**イベント行をクリックすると右画面に詳細が表示される**




**「API calls」にどのAPIを実行したか記載される**

**「Actor」の項目では、通信元IP等も表示される**
**明らかに怪しいIPで回数も多いようであれば**
**脅威リストへ追加登録するとよい**



# Amazon GuardDutyの運用

## 基本的な運用の流れ

・【前提】イベントが発生したら通知を受け取れるようにしておく

【AWS のサービスの特定のイベントタイプがトリガーされた場合にカスタム SNS 通知が送信されるように、GuardDuty 用に EventBridge を設定するにはどうすればよいですか。】
https://aws.amazon.com/jp/premiumsupport/knowledge-center/guardduty-eventbridge-sns-rule/

・通知受信後は、影響確認と対処

CallされたAPIを確認し、何をされたかチェック

IPアドレスのブロック、構成・設定変更

・対処不要な既知のアラートが多いと感じたら、
フィルタによる自動アーカイブにより通知を抑止する

# まとめ

# まとめ

## セキュリティ脅威とAmazon GuardDuty

- セキュリティ脅威は様々なケースが存在する
- 多くの場合、攻撃に至る前の予備動作が存在し、それを含めた脅威を検知・通知するサービスがAmazon GuardDuty
- 機械学習の仕組みで検知しにくい状況でも賢く分析してくれる

## Amazon GuardDutyの利用方法

- サービスの有効化
- 検出されたイベントの確認方法
- 運用の流れ

# 実績豊富なエンジニア集団の技術と開発ツールで「開発期間/コスト削減」「品質向上」を実現

株式会社スタイルズ

https://www.stylez.co.jp

東京都千代田区神田小川町1-2　風雲堂ビル6階

Tel:03-5244-4111

**オープンソースソフトウェア推進**