



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



partner
network



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

セキュリティ、アイデンティティ、コンプライアンス

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。

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を評価できます。

今すぐ始める

「今すぐ始める」

GuardDuty によるこそ

30 日の無料トライアル

サービスのアクセス権限

GuardDuty を有効にすると、AWS CloudTrail ログ、VPC フローログ、および DNS クエリログを分析してセキュリティに関する分析結果を生成するための GuardDuty のアクセス許可を付与することになります。 [詳細はこちら](#)

サービスロールのアクセス権限の表示

注意: GuardDuty では AWS CloudTrail ログ、VPC フローログ、DNS クエリログを管理したり、イベントやログを使用可能にすることはできません。データのソースはそれぞれのコンソールまたは API で設定できます。GuardDuty はいつでも停止または無効にして、イベントおよびログの処理が行われないようにすることができます。 [詳細はこちら](#)

初めて GuardDuty を有効にすると、AWS アカウントは 30 日で自動的に登録されます [GuardDuty の無料トライアル](#)。次の詳細情報を確認します: [GuardDuty 料金表](#)

GuardDuty の有効化

「GuardDutyの有効化」

Amazon GuardDutyの有効化

GuardDuty

×

結果

使用状況

設定

リスト

S3 保護

Kubernetes Protection 新着!

アカウント

最新情報

パートナー

GuardDuty > 検出結果

000

結果 情報

アクション ▼

結果の抑制 情報

保存済みのルール

保存済みのルールがありません

最近 ▼

フィルタの追加

☐ ▼

検索タイプ ▼

リソース ▼

最.. ▼

カ... ▼

結果がありません。

GuardDuty は継続的に AWS 環境を監視し、結果をこのページで報告します。 [詳細はこちら](#)

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



The screenshot shows the Amazon S3 console interface. On the left sidebar, the 'バケット' (Buckets) option is highlighted with a red box and a circled '1'. The main content area displays the 'アカウントのスナップショット' (Account Snapshot) section, which includes a table with the following data:

ストレージの合計	オブジェクト数	平均オブジェクトサイズ	アドバンスドメトリクス
98.7 GB	6.1 M	17.0 KB	は、 [default-account- dashboard] の設定で有効 にできます。

Below the table, there is a note: '下のテーブルですべての列のソートを有効にするには、検索を使用してリストのサイズを 100 バケット以下に縮小します。'

At the bottom of the console, the 'バケット (108)' section is visible. It includes a search bar and several buttons: 'リフレッシュ' (Refresh), 'ARN をコピー' (Copy ARN), '空にする' (Empty), '削除' (Delete), and 'バケットを作成' (Create Bucket). The 'バケットを作成' button is highlighted with a red box and a circled '2'.

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

Amazon S3 > バケットを作成

バケットを作成 [Info](#)

バケットは S3 に保存されたデータのためのコンテナです。 [詳細](#)

一般的な設定

バケット名 **バケット名：ファイルを保管する置き場の名称
任意の名称で良いが、同一リージョン内で他アカウント全体で一意である必要がある**

stylez-guardduty-test

バケット名は一意である必要があり、スペース、または大文字を含めることはできません。 [バケットの命名規則をご参照ください](#)

AWS リージョン

アジアパシフィック (東京) ap-northeast-1 ▼

既存のバケットから設定をコピー - オプション
次の設定のバケット設定のみがコピーされます。

バケットを選択する

作成画面の他項目はデフォルト設定でOK

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



① バケット

Amazon S3

▼ アカウントのスナップショット
最終更新日: Storage Lens による 2022/01/28。メトリクスは 24 時間ごとに生成されます。詳細はこちら [🔗](#)

[Storage Lens ダッシュボードを表示](#)

ストレージの合計	オブジェクト数	平均オブジェクトサイズ	アドバンスドメトリクス
98.7 GB	6.1 M	17.0 KB	は、 [default-account-dashboard] の設定で有効にできます。

② 検索窓で作成したバケット名を入力すると下部にバケットが表示される

バケット (109) [Info](#)

バケットは S3 に保存されたデータのコンテナです。詳細 [🔗](#)

[🔄](#) [📄 ARN をコピー](#) [🗑️ 空にする](#) [🗑️ 削除](#) [📁 バケットを作成](#)

🔍 stylez-guardduty-test X 1 個の一致 < 1 > ⚙️

名前 ▲	AWS リージョン ▼	アクセス ▼	作成日 ▼
stylez-guardduty-test	アジアパシフィック (東京) ap-northeast-1	非公開のバケットとオブジェクト	2022/01/30 10:28:38 AM JST

③ クリック

S3 の AWS Marketplace

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

stylez-guardduty-test [Info](#)

オブジェクト

プロパティ

アクセス許可

メトリクス

管理

アクセスポイント

オブジェクト (0)

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。 [Amazon S3 インベントリ](#) を使用して、バケット内のすべてのオブジェクトのリストを取得できます。他のユーザーが自分のオブジェクトにアクセスできるためには、明示的にアクセス権限を付与する必要があります。 [詳細はこちら](#)



S3 URI をコピー

URL をコピー

ダウンロード

開く

削除

アクション ▼

フォルダの作成

アップロード

プレフィックスでオブジェクトを検索

< 1 >



名前 ▲

タイプ ▼

最終更新日時

サイズ

ストレージクラス

オブジェクト

このバケットにはオブジェクトがありません。

アップロード

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

Amazon S3 > stylez-guardduty-test

stylez-guardduty-test [Info](#)

[オブジェクト](#) | [プロパティ](#) | [アクセス許可](#) | [メトリクス](#) | [管理](#) | [アクセスポイント](#)

オブジェクト (1)

オブジェクトは、Amazon S3 に保存された基本的なエンティティです。 [Amazon S3 インベントリ](#) を使用して、バケット内のすべてのオブジェクトのリストを取得できます。他のユーザーが自分のオブジェクトにアクセスできるように、明示的にアクセス権限を付与する必要があります。 [詳細はこちら](#)

[🔄](#) [📄 S3 URI をコピー](#) [📄 URL をコピー](#) [📄 ダウンロード](#) [🔗 開く](#) [🗑️ 削除](#)

[アクション ▼](#) [フォルダの作成](#) [📁 アップロード](#)

🔍 プレフィックスでオブジェクトを検索

☒	名前 ▲	タイプ ▼	最終更新日時 ▼	サイズ ▼	ストレージクラス ▼
☒	 untrustip.txt	txt	2022/01/30 10:35:19 AM JST	13.0 B	スタンダード

③ファイルの接続URLがクリップボードにコピーされる

①ファイルがアップロードされた事を確認

②

テストイベントの作成 ～脅威リストをGuardDutyへ登録～ Stylez3

➤ 脅威リストの登録

GuardDuty

×

結果

使用状況

設定

リスト

S3 保護

Kubernetes Protection 新着!

アカウント

最新情報

パートナー

信頼されている IP リストは、AWS 環境で安全に通信できていることがわかっている、信頼されている IP アドレスで構成されています。GuardDuty では、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。

+

信頼されている IP リストの追加

リスト名	リストファイルの URL	形式	アクティブ
------	--------------	----	-------

信頼されている IP リスト
信頼されている IP リストは、AWS 環境で安全に通信できていることがわかっている、信頼されている IP アドレスで構成されています。GuardDuty では、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。 [詳細はこちら](#)

脅威リスト

脅威リストは、既知の悪意のある IP アドレスで構成されています。GuardDuty では、脅威リストに含まれている IP アドレスの結果を生成します。

+

脅威リストの追加

② クリック

リスト名	リストファイルの URL	形式	アクティブ
------	--------------	----	-------

脅威リスト
脅威リストは、既知の悪意のある IP アドレスで構成されています。GuardDuty では、脅威リストに含まれている IP アドレスの結果を生成します。 [詳細はこちら](#)

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

脅威リストの追加

GuardDuty では、脅威リストに基づいて結果を生成します。 [詳細はこちら](#)

リスト名

untrustip

場所

https://stylez-guardduty-test.s3.ap-northeast-1.amazonaws.c

形式

プレーンテキスト

シンプルな IP リストを含むファイルには TXT を使用します。

このリストを追加することにより、サードパーティーの脅威のインテリジェンスに関連するものを含む、GuardDuty のサービス条項に同意し、このリソースからデータを読み取るように GuardDuty を設定するものとします。

☒ 同意します

「同意します」にチェック

キャンセル

リストの追加

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

テストイベントの作成 ～脅威リストをGuardDutyへ登録～ Stylez3

➤ 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

信頼されている IP リスト

信頼されている IP リストは、AWS 環境で安全に通信できていることがわかっている、信頼されている IP アドレスで構成されています。GuardDuty では、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。

+ 信頼されている IP リストの追加

リスト名	リストファイルの URL	形式	アクティブ
------	--------------	----	-------



信頼されている IP リスト

信頼されている IP リストは、AWS 環境で安全に通信できていることがわかっている、信頼されている IP アドレスで構成されています。GuardDuty では、信頼されている IP リストに含まれている IP アドレスの結果を生成しません。 [詳細はこちら](#)

脅威リスト

登録直後は有効化されていないので、チェックボックスを押して有効化

脅威リストは、既知の悪意のある IP アドレスで構成されています。GuardDuty では、脅威リストに含まれている IP アドレスの結果を生成します。

+ 脅威リストの追加

登録されている事を確認

リスト名	リストファイルの URL	形式	アクティブ
------	--------------	----	-------

✔ untrustip

<https://stylez-guardduty-test.s3.ap-northeast-1.amazonaws.com>

TXT



テストイベントの作成 ～検出結果～



結果 情報

結果の抑制

情報

保存済みのルール

保存済みのルールがありません

最近

フィルタの追加

操作に使用したIAMユーザ名が示されている

☐	検索タイプ	リソース	最終...	カウント
☐	Recon:IAMUser/MaliciousIPCaller.Custom	junichi.baba: ASIAYSANS2GMVNUDYMU4	8分前	1
☐	UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom	junichi.baba: ASIAYSANS2GMVNUDYMU4	8分前	5

操作に使用したIAMユーザ名が示されている

どちらも悪意のあるIPからの操作であることを示している

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

アクション ▼	
がありません	
▼ 最 ▼ カ...	
YSANS2GMV 2時間前 1	
YSANS2GMV 2時間前 5	

API calls	
Name	GetBucketEncryption
Count	1
First seen	1643511502
Last seen	1643511502
Name	GetBucketOwnershipControls
Count	3
First seen	1643511449
Last seen	1643511503
Name	GetBucketObjectLockConfigu...
Count	2
First seen	1643511449
Last seen	1643511502
Name	GetBucketPolicy
Count	1
First seen	1643511500
Last seen	1643511500
Name	GetBucketWebsite
Count	1
First seen	1643511500
Last seen	1643511500
Name	GetBucketVersioning
Count	4

「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

Actor	
Caller type	Remote IP 🔍 🔍
IP address	49.98.159.251 🔍 🔍
Location	
City	Setagaya-ku
Country	Japan
Lat	35.6468
Lon	139.6546

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