



2022年3月8日

30分でわかる！
Amazon SecurityHubによる
セキュリティチェック



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各サービスのセキュリティ関連設定を最善な形にしたい方

□ゴール

- ▶ AWS SecurityHubはどのようなサービスなのかを理解する
- ▶ AWS SecurityHubを利用して、AWSの推奨設定に基づくチェック方法を把握する。

AWS上のセキュリティ対策

どのような対策をすべきか？

➤ 対策をしないと・・・

- ・ 情報流出、攻撃の踏み台、マルウェア感染、システム停止 といった被害に。

➤ 対策検討における疑問・不安

- ・ 従来のオンプレミスの対策と同じで良いのか？
- ・ マネージドサービスの設定はどうすべき？
- ・ そもそも何をしたら良いかわからない。



「AWS SecurityHub」を利用することで、
AWS全般における最善なセキュリティ設定を知ることができる。

AWS SecurityHub

AWS SecurityHubとは

- AWS内のセキュリティ状態を包括的に把握し、様々な設定が推奨設定に準拠しているかどうかを確認できるサービス

セキュリティ基準となる複数のルールに準拠しているかをチェック。

準拠していない項目を把握し、推奨される設定を知ることができる。

定期的にチェックすることで、最善なセキュリティ設定が保たれる。

脆弱性診断とは異なる

今回はこちらの機能について解説



個別のセキュリティサービスの結果を包括して確認できる



アクションを起こす

Amazon CloudWatch Events との統合を利用して、カスタマイズされたアクションを構築し、チケット発行システム、チャットシステム、Eメールシステム、自動改善システムに検出結果を送信します。

AWS SecurityHubとは

➤ チェック可能なセキュリティ基準の一覧

明確な適用要件が無ければ、
AWS基礎セキュリティか CISを選択

- AWS 基礎セキュリティのベストプラクティス
 - AWSセキュリティの専門家によって定義された、汎用的で基礎的なルール
- CIS AWS Foundations Benchmark
 - 米国政府機関や企業、学術機関などが協力して、インターネット・セキュリティ標準化に取り組む目的で設立された団体（CIS）が提唱するセキュリティ基準をベースにしたルール
- PCI DSS
 - クレジットカード関連のデータを保存、処理、転送する仕組み向けのセキュリティ基準をベースにしたルール

AWS SecurityHubとは

➤ 料金

- ・ セキュリティチェック回数や検出結果の取り込みイベント数に依存

セキュリティチェック	
10万回まで/月	0.0010 USD / チェック
10万回～50万回/月	0.0008 USD / チェック
50万回以上/月	0.0005 USD / チェック

検出結果取り込みイベント	
1万イベントまで/月	無料
1万イベント以上/月	0.00003 USD / イベント

AWS SecurityHubの利用方法

AWS SecurityHubの有効化

セキュリティ、アイデンティティ、およびコンプライアンス

AWS Security Hub セキュリティ体制の管理と改善

AWS Security Hub では、AWS のセキュリティステータスを一括表示できます。セキュリティチェックを自動化し、セキュリティ検出結果を管理し、AWS 環境全体にわたってセキュリティで最優先すべき問題を洗い出します。

Security Hub の使用を開始する

- Try out Security Hub for free with a 30-day trial
- AWS 環境全体にわたって自動化されたセキュリティチェックを実行
- セキュリティ問題の優先順位付けと修復
- AWS およびパートナー製品のセキュリティ調査結果を、すべてのアカウントで標準形式で統合する

Security Hub に移動

30 日間の無料トライアル

「Security Hub に移動」

AWS SecurityHubの有効化

AWS Security Hub の有効化

AWS Config の有効化

Security Hub の標準およびコントロールを有効にする前に、まず AWS Config でリソースの記録を有効にする必要があります。すべてのアカウントと、Security Hub の標準およびコントロールを有効にするすべてのリージョンでリソースの記録を有効にする必要があります。最初にリソースの記録を有効にしない場合、Security Hub の標準およびコントロールを有効にしたときに問題が発生する可能性があります。AWS Config では、リソースの記録について個別に請求されます。詳細については、次をご参照ください: [AWS Config の料金ページ](#)。

リソースの記録は、[AWS Config コンソール](#)から手動で有効にすることができるほか、[ダウンロード]を選択して、AWS CloudFormation テンプレートを StackSet としてダウンロードしてデプロイできます。詳細については、[ドキュメント](#)をご参照ください。

ダウンロード

セキュリティ基準

AWS Security Hub を有効にすると、セキュリティチェックを実行する権限が付与されます。[サービスにリンクされたロール \(SLR\)](#) 以下のサービスがセキュリティチェックを実行するために使用されます: Amazon CloudWatch、Amazon SNS、AWS Config、AWS CloudTrail。

- ☒ AWS 基礎セキュリティのベストプラクティス v1.0.0 を有効化
- ☐ CIS AWS Foundations Benchmark v1.2.0 を有効化
- ☐ PCI DSS v3.2.1 を有効化

AWS 統合

Security Hub を有効にすると、有効にした AWS のサービスから結果をインポートするアクセス許可が付与されます。

[詳細はこちら](#)

キャンセル

Security Hub の有効化

利用するSecurityHubと同じリージョン内でAWS Configが有効化されている必要がある。

「ダウンロード」を押すと、AWS Configを有効化するためのCloudFormationテンプレートがダウンロードされる。

【AWS CloudFormationの開始方法】
https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/GettingStarted.html

「AWS基礎セキュリティのベストプラクティス v1.0.0 を有効化」を選択

Security Hub

×

概要

セキュリティ基準

インサイト

検出結果

統合

設定

新規

最新機能

1

Security Hub > セキュリティ基準

セキュリティ基準

AWS 基礎セキュリティのベストプラクティス v1.0.0 AWS による

説明

AWS 基礎セキュリティのベストプラクティス標準は、AWS アカウントとデプロイされたリソースがセキュリティのベストプラクティスと一致しないことを検出する自動化されたセキュリティチェックのセットです。この標準は AWS セキュリティの専門家によって定義されたものです。この厳選された一連の統制は、AWS におけるセキュリティ体制の改善に役立ち、AWS で最も人気の高い基礎的なサービスを網羅しています。

セキュリティスコア

25%

健全性がスコアとして確認できる。
100%が最も健全な状態。

無効化

結果を表示する

状況確認

Security Hub > セキュリティ基準 > AWS 基礎セキュリティのベストプラクティス v1.0.0

AWS 基礎セキュリティのベストプラクティス v1.0.0

概要

セキュリティスコア

202 of 2,057 チェック 失敗



10% 失敗

【セキュリティスコア算出方法】

= 成功項目数 (14) / 有効な項目数 (成功 : 14 + 失敗 : 41)
※データなしは除外

すべて有効	失敗	不明	データなし	成功	無効
136	41	0	81	14	0

【データなし】

未チェックの項目。初回チェックまで時間を要する。

すべて有効 (136)

Q フィルター 有効 コントロール

コンプライアンスのステータス	重要度	ID	
☐ ⊗ 失敗	■ 重要	IAM.6	
☐ ⊗ 失敗	■ 高	S3.8	
☐ ⊗ 失敗	■ 高	CloudFront.1	CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります 5 / 8
☐ ⊗ 失敗	■ 高	EC2.2	VPC のデフォルトのセキュリティグループはインバウンドトラフィックとアウトバウンドトラフィックを許可しない必要があります 2 / 2

【データ更新間隔】

12時間以内で更新。

リソース状況が変更した場合は、関連するルールは即時更新される。

改善

Security Hub > セキュリティ基準 > AWS 基礎セキュリティのベストプラクティス v1.0.0

AWS 基礎セキュリティのベストプラクティス v1.0.0

概要

セキュリティスコア

202 of 2,057 チェック 失敗



すべて有効 136	失敗 41	不明 0	データなし 81	成功 14	無効 0
--------------	----------	---------	-------------	----------	---------

「失敗」をクリック = 「失敗」のフィルタリング

すべて有効 (136)

無効化

ダウンロード

Q フィルター 有効 コントロール

コンプライアンスのステータス	重要度	ID	タイトル	不合格のチェック
○ 失敗	■ 重要	IAM.6	ハードウェア MFA はルートユーザーに対して有効にする必要があります	1 / 1
○ 失敗	■ 高	S3.8	S3 ブロックパブリックアクセス設定は、バケットレベルで有効になっている必要があります	10 / 11
○ 失敗	■ 高	CloudFront.1	CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	5 / 8
○ 失敗	■ 高	EC2.2	VPC のデフォルトのセキュリティグループはインバウンドトラフィックとアウトバウンドトラフィックを許可しない必要があります	2 / 2

改善

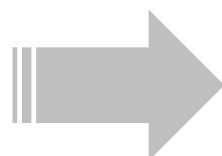
すべて有効 136	失敗 41	不明 0	データなし 81	成功 14	無効 0
失敗 (4)					
Q フィルタ ☐ 失敗 ☒ 中 ☐ 成功 ☐ 無効 ELB.6 Application Load Balancer の削除保護が有効になっている必要があります "elb" X フィルターをクリア					
コンプライアンスのステータス ▼		重要度 ▼	ID ▼	タイトル	
☐	失敗	中	ELB.4	Application Load Balancer は http ヘッダ	
☐	失敗	中	ELB.5	Application Load Balancer と Classic Load	
☐	失敗	中	ELB.6	Application Load Balancer の削除保護が	
☐	失敗	中	ELBv2.1	Application Load Balancer は、すべての	

現状、ELBカテゴリで 4 つ失敗検出

改善

属性	
削除保護	無効
アイドルタイムアウト	60 秒
HTTP/2	有効
Desync 緩和モード	防御的

削除保護を有効化



属性	
削除保護	有効
アイドルタイムアウト	60 秒
HTTP/2	有効
Desync 緩和モード	防御的

すべて有効 136	失敗 40	不明 0	データなし 81	成功 15	無効 0
失敗 (3)					
☐ ☒ 成功 ☐ 中 ELB.6 Application Load Balancer の削除保護が有効になっている必要があります					
Q フィルター失敗 コントロール					
"elb" X フィルターをクリア					
コンプライアンスのステータス ▼		重要度 ▼	ID ▼	タイトル	
☐	⊗ 失敗	■ 中	ELB.4	Application Load Balancer は http ヘッダ	
☐	⊗ 失敗	■ 中	ELB.5	Application Load Balancer と Classic Loa	
☐	⊗ 失敗	■ 中	ELBv2.1	Application Load Balancer は、すべての	

該当項目が「成功」になり、
失敗数が 41 から 40 に。

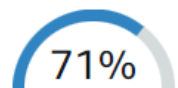
無効化

AWS 基礎セキュリティのベストプラクティス v1.0.0

概要

セキュリティスコア

200 of 2,138 チェック 失敗



9% 失敗

すべて有効

136

失敗

39

不明

0

データなし

0

成功

97

無効

0

失敗 (39)

無効化したい項目をチェック

無効化ボタンを押す

無効化

ダウンロード

		重要度	ID	タイトル	不合格のチェック
☒	⊗ 失敗	■ 重要	IAM.6	ハードウェア MFA はルートユーザーに対して有効にする必要があります	1 / 1
☐	⊗ 失敗	■ 高	S3.8	S3 ブロックパブリックアクセス設定は、バケットレベルで有効になっている必要があります	10 / 11
☐	⊗ 失敗	■ 高	CloudFront.1	CloudFront ディストリビューションでは、デフォルトのルートオブジェクトが設定されている必要があります	5 / 8
☐	⊗ 失敗	■ 高	EC2.2	VPC のデフォルトのセキュリティグループはインバウンドトラフィックとアウトバウンドトラフィックを許可しない必要があります	2 / 2
☐	⊗ 失敗	■ 高	ECS.2	ECS サービスには、自動的にパブリック IP アドレスが割り当てられてはなりません	1 / 1

無効化

Disable: "[IAM.6] Hardware MFA should be enabled for the root user" ×

The control will be disabled for this account in this region only.
次を無効にする理由

無効化テスト

キャンセル

無効化

無効化理由を記載し「無効化」ボタンを押す。

無効化された項目を後で確認した時に、
なぜ無効化したかの記録が残るので、
記載する事を推奨。

無効化



すべて有効 135	失敗 38	不明 0	データなし 0	成功 97	無効 1
無効 (1)					有効化
Q フィルター 無効 コントロール					
コンプライアンスのステータス ▼		重要度 ▼		ID ▼	タイトル
○	⊖ 無効	■ 重要	IAM.6	ハードウェア MFA はルートユーザーに対して有効にする必要があります	

「失敗」件数が1件減り、「無効」に移動した。

➤ 基本的な運用の流れ

- ・ 定期的に画面を確認して、新規の問題が出ていないか確認する。
※可能であればメール等への通知を推奨

【カスタムアクションを使用して検出結果とインサイト結果をEventBridgeに送信する】

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-cwe-custom-actions.html

- ・ 通知受信後は、内容を把握し、改善 / 無効化 を実施。
スコア100%に向けて調整していく。

まとめ

□ AWS SecurityHubによるセキュリティチェック

- ▶ 3種類のセキュリティ基準に基づいた準拠状況を確認できる。
- ▶ 他のAWSセキュリティサービスの検知結果を集約し、包括して確認できる。

□ AWS SecurityHub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
- ▶ 改善
- ▶ 無効化
- ▶ 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