CloudShift

Stylez

株式会社スタイルズ

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

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るべき？

・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

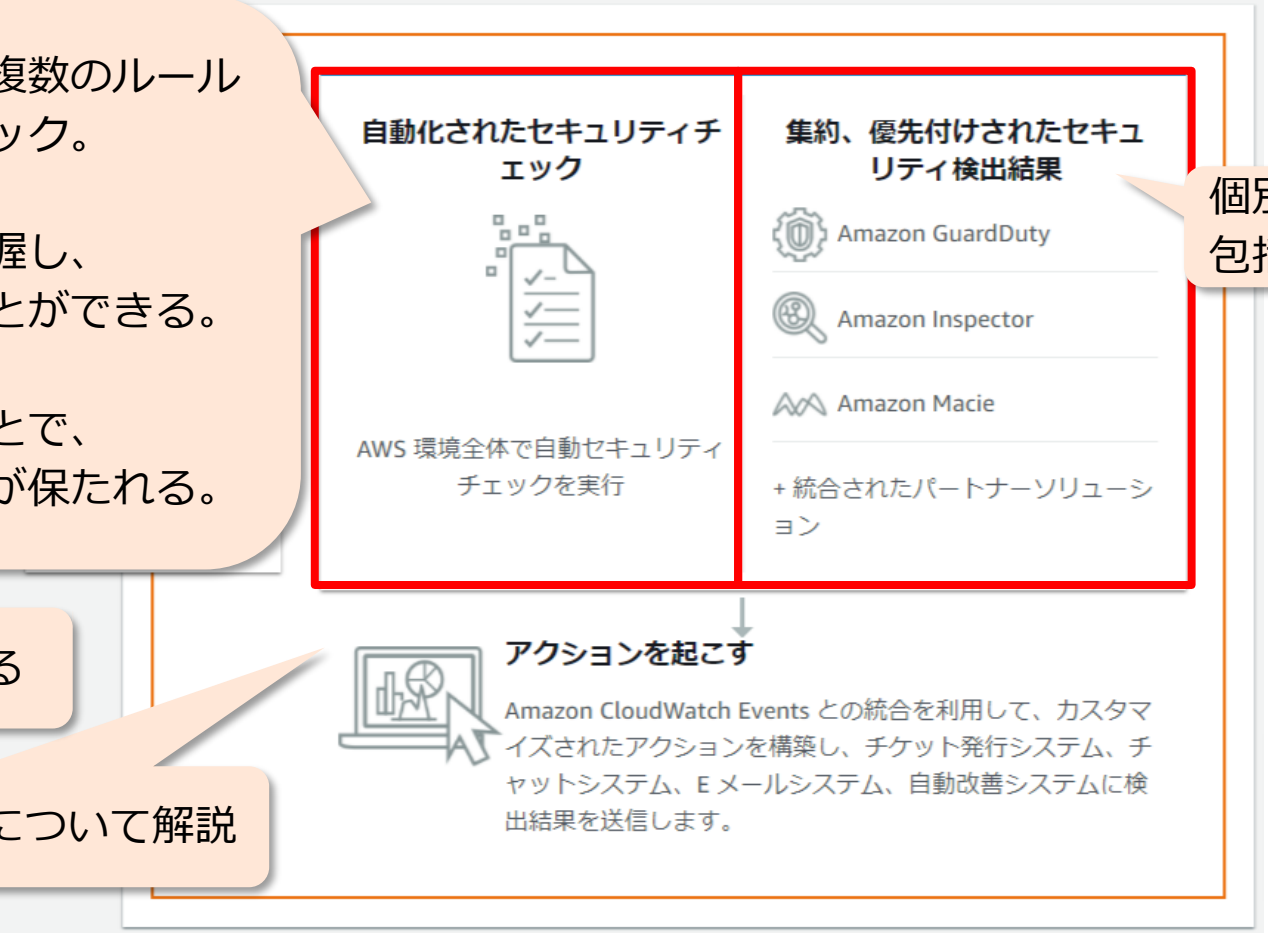
AWS SecurityHubとは

- **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。



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

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

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

「Security Hub に移動」

AWS SecurityHubの有効化

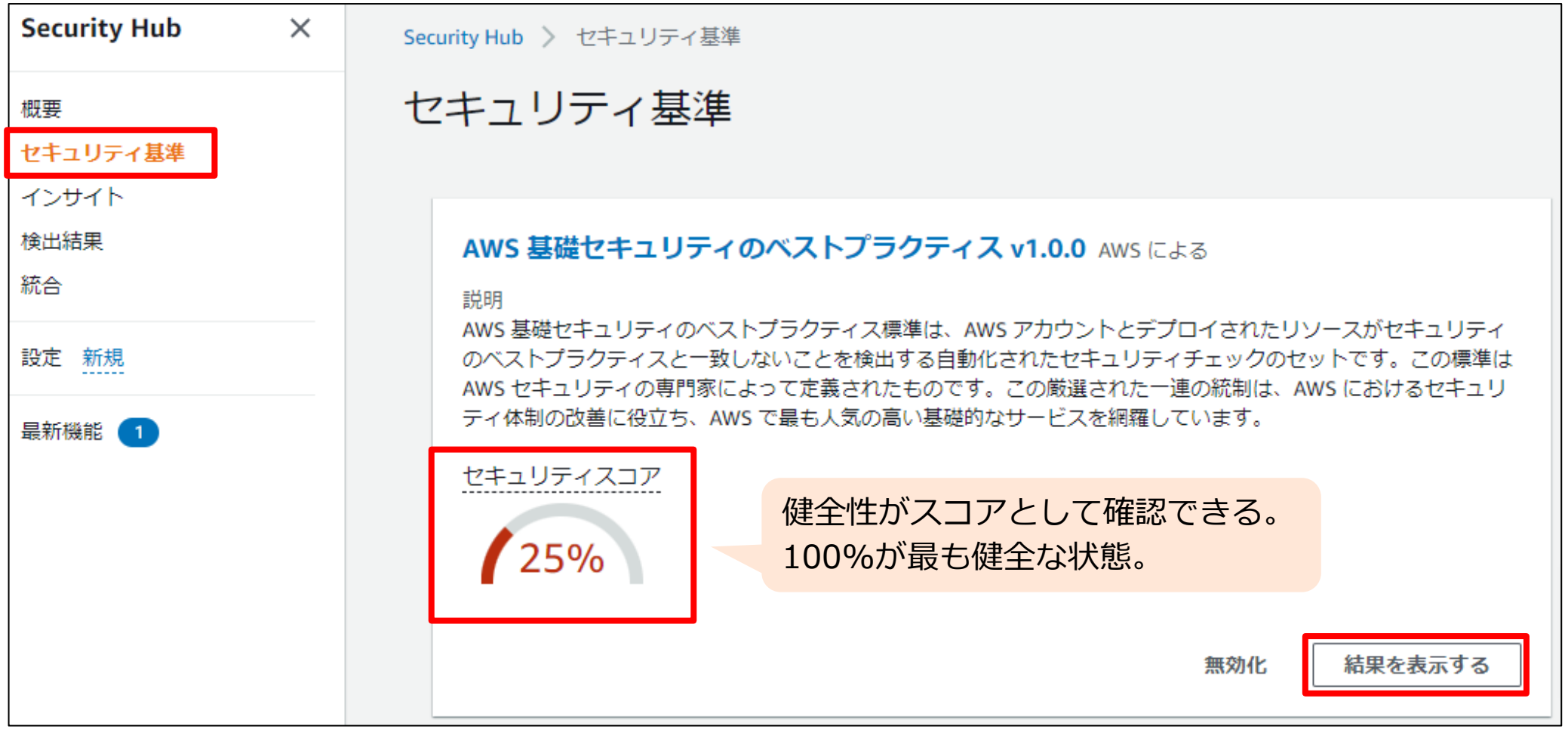
利用するSecurityHubと同じリージョン内で
AWS Configが有効化されている必要がある。

「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
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

状況確認


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

【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

【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。

【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
25%
202 of 2,057 チェック 失敗
10% 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
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

現状、ELBカテゴリで４つ失敗検出

改善

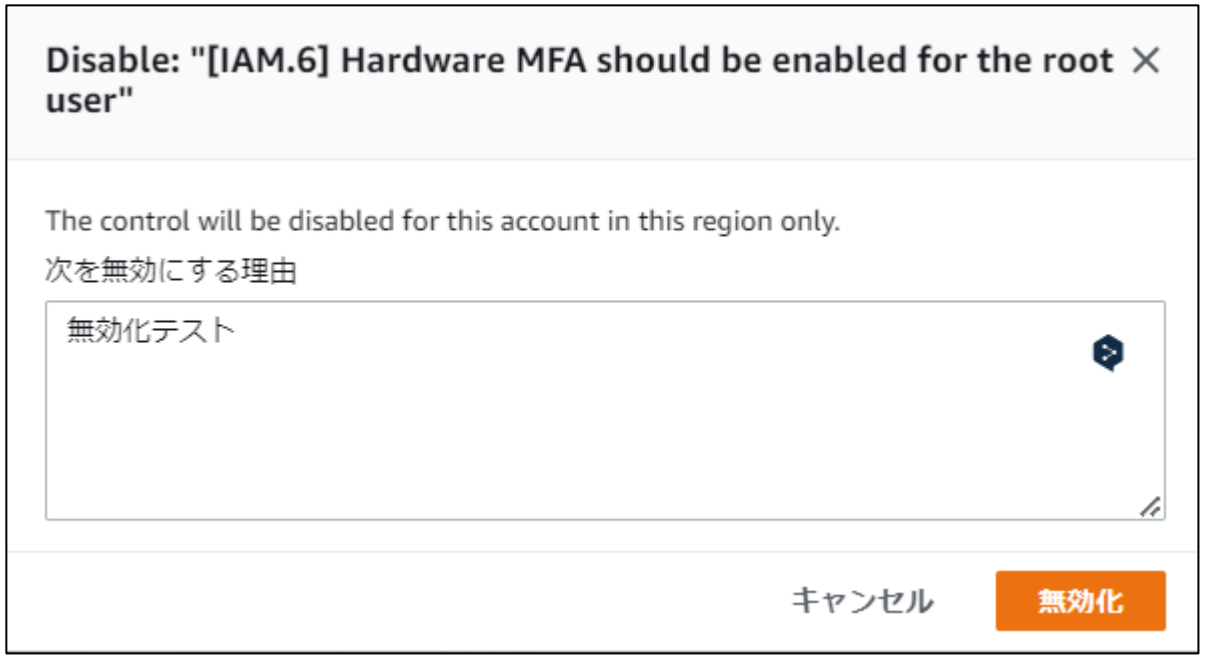

属性
削除保護 無効
アイドルタイムアウト 60 秒
HTTP/2 有効
削除保護を有効化
属性
削除保護 有効
アイドルタイムアウト 60 秒
HTTP/2 有効


すべて有効 136
失敗 40
不明 0
データなし 81
成功 15
無効 0
該当項目が「成功」になり、
失敗数が 41 から 40 に。
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
フィルター 失敗 コントロール
"elb"
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

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
71%
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
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



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

「失敗」件数が1件減り、「無効」に移動した。

AWS SecurityHubの運用

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

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