SRA の技術情報誌
GS LetterNeo
Vol.177　2023 年 4 月

AWS Security Hub セキュリティ運用

佐川 喜昭

アドバンストクラウドエンジニアリング事業部

はじめに

AWS をマルチアカウント環境下で使用しているプロジェクトでのコンプライアンスの一環として、クラウド環境で発見的ガードレールを用いた検知の仕組みである AWS Security Hub を使用しています。

AWS アカウントを様々な用途で利用している利用者がいる中、検知されたガードレール違反に対して、利用者に歩み寄りながらどのように「検知の仕組み」や「検知対象の選別」などのルール作りをしているか、紹介します。

Security Hub を用いた発見的ガードレールの課題

プロジェクトで管理しているクラウド環境は、「クラウド共通基盤の管理者」と「AWS アカウント利用者」とで責任範囲が分かれています。クラウド環境のセキュリティレベルのベースラインを維持するために、共通基盤の管理者がセキュリティガードレールを管理しています。

プロジェクトで管理するクラウド環境：

- ✓ クラウド環境の共通基盤を管理者が提供している。
- ✓ AWS アカウントは管理者が初期構築している。
- ✓ 初期構築された AWS アカウントを利用者が使用している。

発見的ガードレールは、あくまでガードレール違反の発見をするための仕組みです。そのため、安全を保つには、ガードレール違反があった際の是正に向けたルール作りが必要です。

また、特定の利用ではなく、様々な用途で利用されている AWS アカウントのガードレール作りは、「利用者の自由度」と「安全性の確保」のバランスをどうとるかが難しいです。

是正に向けた仕組みづくりの課題：

- ✓ 共通基盤としてのガードレールの定義づくり。
  - ➢ 用途の異なる複数アカウントについて、自由度の確保が必要。
  - ➢ 一定のセキュリティレベルの確保が必要。
- ✓ ガードレール違反があった際の利用者への働きかけ。

発見的ガードレールの構成について

Security Hub では、 以下のセキュリティ標準をサポートしています。本プロジェクトで管理する環境では、「AWS 基礎セキュリティのベストプラクティス v1.0.0」を採用し、セキュリティガードレールの運用のベースにしています。

Security Hub でサポートしているセキュリティ標準：

- AWS 基礎セキュリティのベストプラクティス v1.0.0
- PCI DSS v3.2.1
- CIS AWS Foundations Benchmark v1.4.0
- CIS AWS Foundations Benchmark v1.2.0
- NIST Special Publication 800-53 Revision 5

Security Hub によるガードレールの構成は、下記のようになっています。

- 利用者アカウント側の Security Hub で検知を行う。
- 管理者アカウント側の Security Hub で検知内容を集約する。
- 管理者アカウント側から利用者に対して各種通知をする。

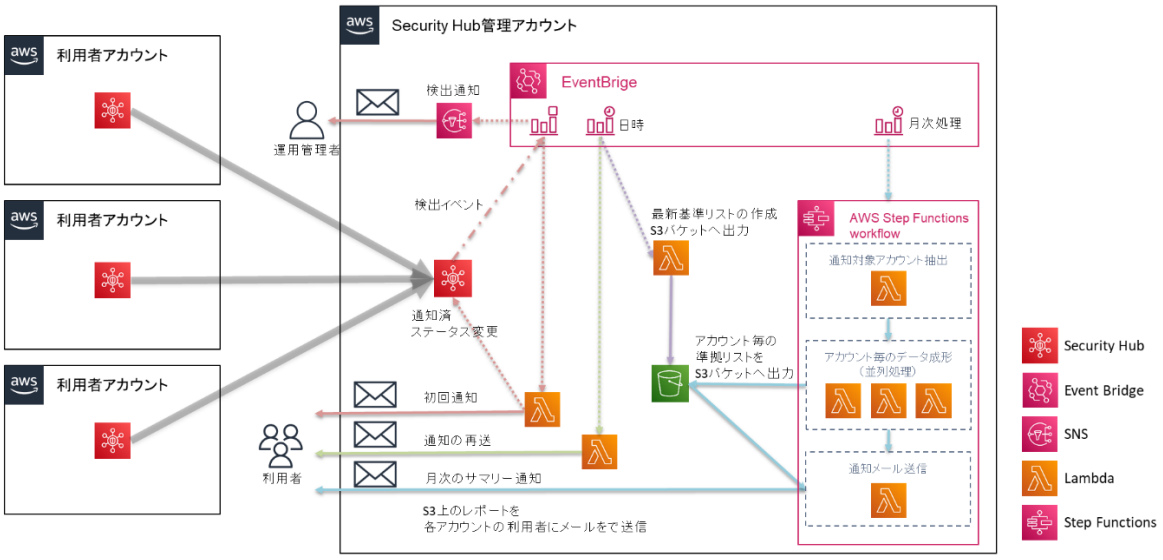

図 1. Security Hub によるガードレールの構成

課題に対する対応

「AWS 基礎セキュリティのベストプラクティス v1.0.0」には、以下のような実際の利用にはそぐわないコントロールも存在します。コントロールとは、セキュリティ標準で定義されている、アカウントおよびリソースに対する遵守事項です。

- ✓ 管理下にあるアカウントのすべてで遵守を必須としなくても良いと思われるコントロール
- ✓ 基盤側の構成で一定のセキュリティの安全性が担保されているコントロール
- ✓ システムの要件で AWS の基準に沿った方式で対応ができないコントロール

管理しているクラウド環境では、「共通基盤の管理者」として、下記 2 点を軸に全利用者アカウントに対する対応方針を定めています。

1. 共通基盤としての検出コントロールを定義
　重要性の高いコントロールに対するガードレール違反のみに限定することで、利用者が重要性の高いコントロールに対して意識して行動してもらう事を目指しています。

検出するコントロールの方針：

1. Low レベルのコントロールの無効化
2. 共通基盤で対策されているコントロールの無効化
3. 特定コントロールの無効化

※ セキュリティ標準は常に更新されており、内部のルールについても定期的な見直しを実施します。

2. 利用者に合わせた是正対応フローづくり

セキュリティ標準に沿った対応をしようとすると、検出したガードレール違反に対して、セキュリティ標準で定められた是正をする事になります。しかし、実際にはシステム要件により、セキュリティ標準に沿った是正が困難な場合もあります。そのため、利用者に対して報告を義務化し、「利用者からの報告」と、「ガードレール違反」の内容をもとに管理者で判断し、是正の要否を判断しています。

ガードレール違反に対する是正運用フローは、「初回検知」と「月次サマリー通知」から始まる２つのトリガーを設定しています。定期的な通知を行うことで、初回検知時に是正できない「ガードレール違反」の存在を防止します。

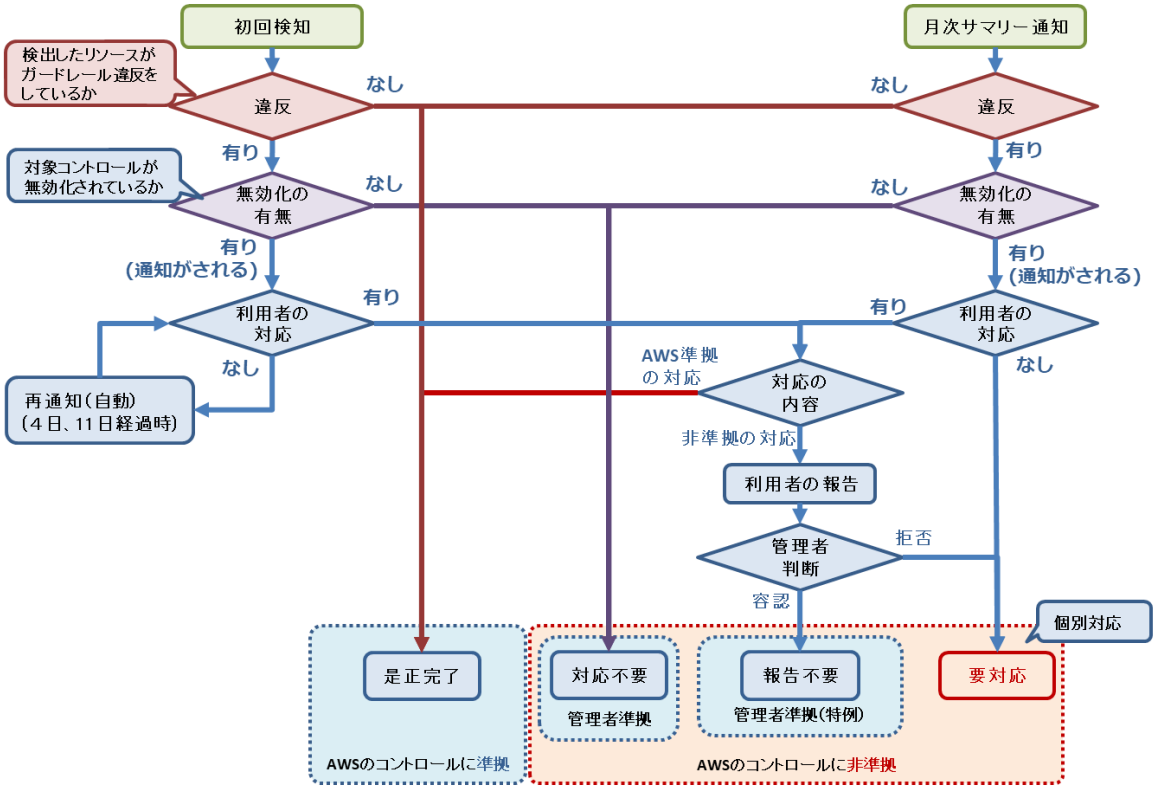

図 2. 是正対応フロー

おわりに

以上、マルチアカウント環境の発見的ガードレールで検知の仕組みとして AWS Security Hub を用いた、用途に合わせた AWS の基準に囚われない「コントロール」と「是正対応フロー」作りをしていることをお伝えしました。

今後は、「利用者への通知内容」や「利用者からの報告方法」の改善など、クラウド環境の利用者が違反に気づき改善するためのハードルを下げる仕組みを作ることが、クラウド環境のセキュリティガードレールの安全性の向上につながると考えています。

参考 URL

- AWS Security Hub のセキュリティ標準とコントロール：
  https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-standards.html

- AWS Security Hub で使用可能なセキュリティ標準：
  https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/standards-available.html

- コントロール結果への重要度の割り当て：
  https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/controls-findings-create-update.html#control-findings-severity

GSLetterNeo Vol.177
2023 年 4 月 20 日発行
発行者　株式会社 SRA 技術本部 先端技術研究室

編集者　熊澤努　方 学芬
バックナンバー https://www.sra.co.jp/public/sra/gsletter/
お問い合わせ　gsneo@sra.co.jp

株式会社SRA
〒171-8513 東京都豊島区南池袋 2-32-8

夢を。Yawaraka Innovation
やわらかいのべーしょん