AWS 請求代行サービス

セキュアカウント利用オプション

株式会社サーバーワークス

2024 年 8 月　Version 1.02

目次

1. はじめに

1.1. 概要

本ドキュメントは株式会社サーバーワークスが提供する AWS 請求代行サービスをご利用のお客様へのオプションサービスとなる [セキュアアカウント] について明記したドキュメントです。

1.2. サービス提供

AWS 請求代行サービスの新規アカウントをお申し込みいただく際に、「セキュアアカウントの有効化」の項目で「◉する」を選択頂いた場合に適用いたします。

1.3. 対象のお客様

AWS 請求代行サービスの新規アカウントをお申し込みいただく際に、「セキュアアカウントの有効化」の項目で「◉する」を選択頂いた方が対象です。
AWS Organizations を利用希望、または AWS Control Tower 利用希望の新規申し込みは対象外となります。

2. 用語

用語	説明
弊社	株式会社サーバーワークス
貴社	AWS 請求代行サービス契約主の個人もしくは法人
本サービス	AWS 請求代行サービスにおけるセキュアカウント
AWS Identity and Access Management (AWS IAM)	AWS リソースへのアクセスを安全に管理するためのサービス IAM により、誰を認証し、誰にリソースの使用を承認する (アクセス許可を持たせる) のかを制御する
Amazon EC2	サイズ変更可能なコンピューティング性能をクラウド内で提供するウェブサービス (仮想マシン)
Amazon Elastic Block Store (Amazon EBS)	Amazon EC2 向けに設計された、使いやすく、スケーラブルで、高性能なブロックストレージサービス

Amazon Simple Storage Service (S3)	任意の量のデータの保存と取得をどこからでも行えるように設計されたオブジェクトストレージ
AWS Organizations	複数の AWS アカウントを一元的に管理できる AWS のサービス
AWS CloudTrail	ユーザーアクティビティと API 使用状況をログ記録し後に追跡できるサービス
AWS Config	AWS リソースの設定状態を記録し、詳細や変更履歴を確認できるサービス
AWS Security Hub	セキュリティのベストプラクティスのチェックを行い、アラートを集約し、セキュリティ業界標準およびベストプラクティスに照らした AWS 環境評価を行うサービス
Amazon GuardDuty	AWS アカウントとワークロードを継続的にモニタリングして悪意のあるアクティビティがないかを確認し、可視化と修復のための詳細なセキュリティ検出結果を提供する脅威検出サービス
Amazon Athena	Amazon Simple Storage Service (S3) 内のデータを Python でシンプルに分析できるインタラクティブな分析サービス
AWS CloudFormation	AWS CloudFormation は、インフラストラクチャをコードとして扱うことで(infrastructure as code)、AWS およびサードパーティーのリソースをモデル化、プロビジョニング、管理することができるサービス

3. セキュアアカウント利用オプションとは

セキュアアカウントとは、AWS が推奨するセキュリティ設定をサーバーワークスが実施済の AWS アカウントとなります。
AWS アカウント新規発行後の状態で、AWS 基礎セキュリティのベストプラクティス v1.0.0 をベースに 100 または 100 に近い状態にて提供するサービスとなります。

※AWS Security Hub のコントロール更新タイミングによってはスコア 100 とならない可能性があります

3.1. 有効化するサービス

サービス名	詳細
AWS Security Hub	セキュアカウントは、AWS Security Hub の AWS 基礎セキュリティのベストプラクティス v1.0.0 をスコア 100 または 100 に近い状態にて提供するサービスである事と、各種 AWS サービスの通知を集約する機能(Hub)を利用する必要がある為、当サービスを有効化している。
Amazon GuardDuty	VPC Flow Logs や Amazon Route 53 のログ、CloudTrail ログなどからネットワークアクティビティ、AWS の操作から異常検出を特定し検出を行える。検出を行うことで、意図しない AWS 環境の操作や AWS 環境 のリソースから意図しない通信を特定することができる。 セキュリティインシデントの早期発見が望める為、有効化している。
AWS Config	AWS リソースの設定記録を保持することで、意図しない設定変更履歴を特定する。 また、設定状態に定義(Config Rules)を利用することで、ガバナンス、コンプライアンス要件に準じた設定を遵守するようにすることができる。万が一、要件外の設定を行った場合でも対象リソースの特定や自動修復なども行うことができる為、有効化している。
AWS CloudTrail	AWS 操作履歴を記録し、AWS 操作履歴の監査や不正利用時の調査で使用する為、有効化している。
IAM Access Analyzer	余剰権限がない事、例えば意図しない外部エンティティ(他 AWS アカウントなど)に共有されているリソースがないかを特定することで情報漏洩を未然に防ぐことができる為、有効化している。

AWS Identity and Access Management (IAM)	デフォルトで有効化、必ず利用されるサービス AWS のデフォルト設定から IAM ユーザーのパスワードポリシーの強化を実施している。
Amazon Elastic Block Store (EBS)	EBS のデータを暗号化する事で、AWS 側での物理的なストレージの盗難リスク等に対応できる。 常に新しい EBS ボリュームを暗号化する設定を実施している。
Amazon Virtual Private Cloud (VPC)	新規 AWS アカウント発行時から存在するデフォルト VPC は汎用的な設計であるが故にセキュリティ設計が甘く利用が推奨されない為、セキュアアカウントではデフォルト VPC の削除を実施済みの状態としている。
AWS Key Management Service (KMS)	セキュアアカウントでは、AWS Security Hub のスコア 100 の状態を目指す為、様々な AWS サービスで暗号化を行っておりその際に AWS KMS のキーを利用している。
Amazon Athena	Amazon Athena のデフォルトで存在しているワークグループが暗号化されておらず、AWS Security Hub のスコア要件を満たせない為、デフォルト暗号化設定を有効としている。

4. お客様にて実施いただく必要がある事

4.1. MFA の設定

IAM ユーザーの MFA を設定してください。

4.2. (任意) 通知の設定

AWS Cloud Formation を用いて通知を実装する為のテンプレートファイルをご用意しています。セキュリティ監視(通知設定)が必要なお客様はサーバーワークスマイスターズへログイン後、サーバーワークス サポートセンター内の「はじめてのセキュアアカウント」内の説明をご確認ください。

5. AWS アカウントに作成されるリソースについて

本オプション提供の際には以下のリソースがアカウントに作成されます。

関連 AWS サービス	リソース種別	リソース情報	用途
AWS Config	S3 バケット	cloudtrail-logs-[アカウント ID]	設定記録ログ保存用
	Config Recorder	default	リソース設定記録
	配信チャネル	default	設定記録データ送信用
AWS CloudTrail	S3 バケット	cloudtrail-logs-[アカウント ID]	操作履歴ログ保存用
	Amazon KMS カスタマー管理型キー	alias/trail_encrypt_key	CloudTrail 暗号化用
	証跡	cloudtrail	CloudTrail 証跡
AWS Identity and Access Management (IAM)	アカウント設定	Password Policy	Password Policy
	Access Analyzer	swx-iam-access-analyzer	IAM Access Analyzer
	アーカイブルール	swx-iam-access-analyzer-archiver	IAM Access Analyzer アーカイブ用ルール
AWS Security Hub	セキュリティ標準	arn:aws:securityhub:${AWS_REGION}::standards/aws-foundational-security-best-practices/v/1.0.0	セキュリティ標準

6. 申し込み方法

AWS 請求代行サービスの新規アカウントをお申し込みいただく際に、「セキュアアカウントの有効化」の項目で「◉する」を選択。

7. 注意事項

7.1. AWS Security Hub スコアについて

本サービスは AWS アカウント新規発行後の状態で、AWS 基礎セキュリティのベストプラクティス v1.0.0 をベースに 100 または 100 に近い状態にて提供するサービスとなります。

運用開始後のスコア管理は本サービスに含まれておりません。

アカウント運用時のスコア管理は、必要に応じて貴社にてご対応願います。

ベストプラクティスが更新された場合、更新直後の新規 AWS アカウントは既存の通りとし、新しいコントロールは無効の状態にいたします。有効化については貴社にてご検討ください。

更新の内容については可能な限り早く当社にて対応を検討し、新規 AWS アカウント発行分について適用します。

7.2. セキュアアカウントの利用料金について

セキュアアカウントを利用する際に発生する概算料金は以下となります。

68.18 USD /月

※上記料金は、想定される最低利用料金となります
※お客様の利用状況によって発生する料金は異なります

7.3. 本オプションの仕様変更について

本書は貴社の承諾なく更新いたします。本オプションで設定したリソースは適宜変更する可能性があります。ただし、貴社が重大な影響が想定される場合には事前にメールもしくはチケットにて報告の上で変更いたします。

弊社サポートセンターからのメールは以下のアドレスより送信いたします。こちらのアドレスからのメール受信ができる状態を常に維持してください。

support@ngmsp.serverworks.jp