Confidential

サンプル株式会社 御中

AWS クラウドセキュリティ診断

結果報告書

EG セキュアソリューションズ株式会社

2023 年 8 月 1 日

目次

1. エグゼクティブサマリー

1.1. 総合評価

設定状況	説明
B	診断の結果、CIS AWS Foundations Benchmark レベル 1 への適合率が 66.7%の結果となりました。

1.2. 評価基準

設定状況	説明
A	CIS AWS Foundations Benchmark レベル 1 への適合率が 80%～100%で、安全な設定状況です。
B	CIS AWS Foundations Benchmark レベル 1 への適合率が 60%～80%で、比較的安全な設定状況ですが、一部、設定の見直しが必要です。
C	CIS AWS Foundations Benchmark レベル 1 への適合率が 40%～60%の間であり、問題を含む設定であるため、対策が必要な状況です。
D	CIS AWS Foundations Benchmark レベル 1 への適合率が 20%～40%の間であり、問題を多く含む設定であるため、早急な対策が必要です。
E	CIS AWS Foundations Benchmark レベル 1 への適合率が 0%～20%の間であり、非常に危険な設定であるため、至急、対策を実施する必要があります。

1.3. 総評

CIS AWS Foundations ベンチマーク v.2.0.0 に準拠したセキュリティ診断を実施した結果、適合状況はレベル 1 で 66.7%、レベル 2 で 55.0%の結果となりました。

基本的な構成については大きな問題がありませんでしたが、一部、Web サーバー等の構成やハードディスクの暗号化設定などに改善点が検出されています。また、ログの出力やモニタリング設定について過不足があるため、万一、セキュリティインシデントが発生した場合に、原因を特定することができない可能性があります。

現状の運用状況を確認の上、本書で指摘している内容について対応可能なものから対策を実施していくことを推奨いたします。

1.4. 対策優先度

以下の表は弊社が推奨する対応優先度となります。この基準は弊社独自の基準となりますが、セイキュリティの観点上から各指摘に対して割り振らせていただいております。

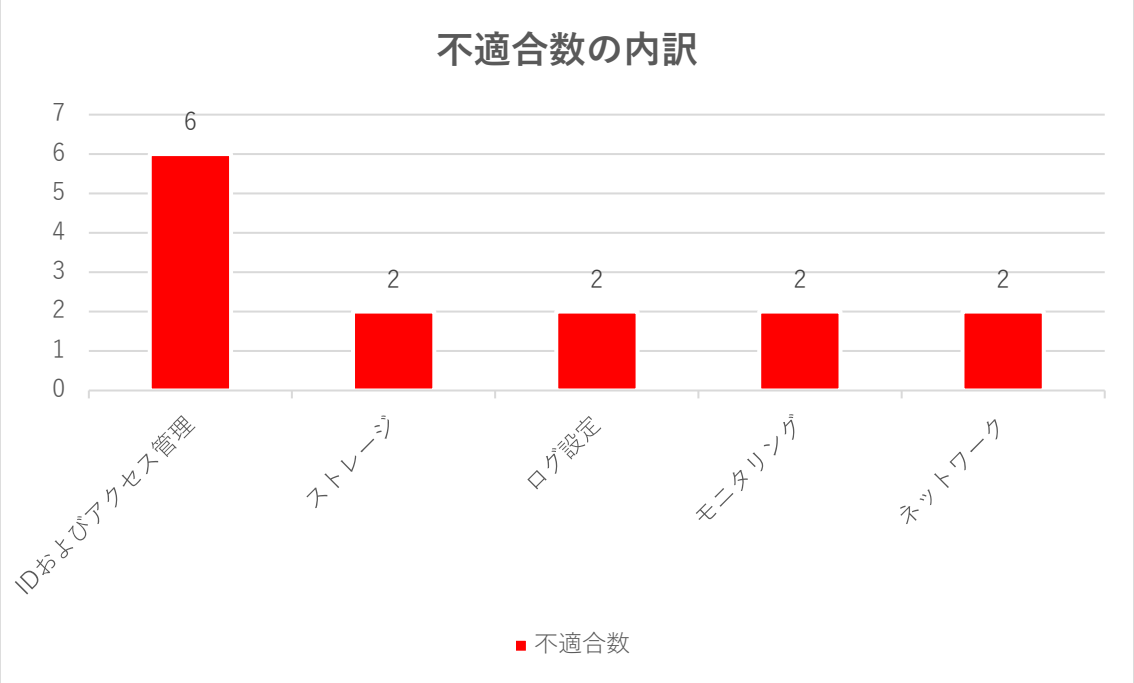
設定状況	説明
緊急	セキュリティ上、早急に対応が必要な項目です。 暫定的な内容でも良いので早急に意思決定する事を推奨する項目です。
高	セキュリティ上、早めの対応を推奨していますが、運用状況等の考慮が必要と考えられる項目です。
中	セキュリティリスクとしては存在するが、運用の検討を行った上で設定変更する事を推奨する項目または、セキュリティリスクはかなり小さいが、運用を円滑に進めるために設定する事を推奨する項目です。
低	セキュリティ上、対応優先度は低い項目ですが、できれば対策を実施することが望ましい項目です。
情報	運用においてセキュリティリスクを回避できると考えられるため、対応優先度は低い項目です。

2. 診断結果

2.1. CIS AmazonWebServices Foundations Benchmark レベル 1

適合率				
66.7%				
No	**区分**	**診断項目数**	**適合数**	**不適合数**
1	ID およびアクセス管理	19	13	6
2	ストレージ	6	4	2
3	ログ設定	4	2	2
4	モニタリング	9	7	2
5	ネットワーク	4	2	2
合計		**42**	**28**	**14**
割合		**100%**	**66.7%**	**33.3%**

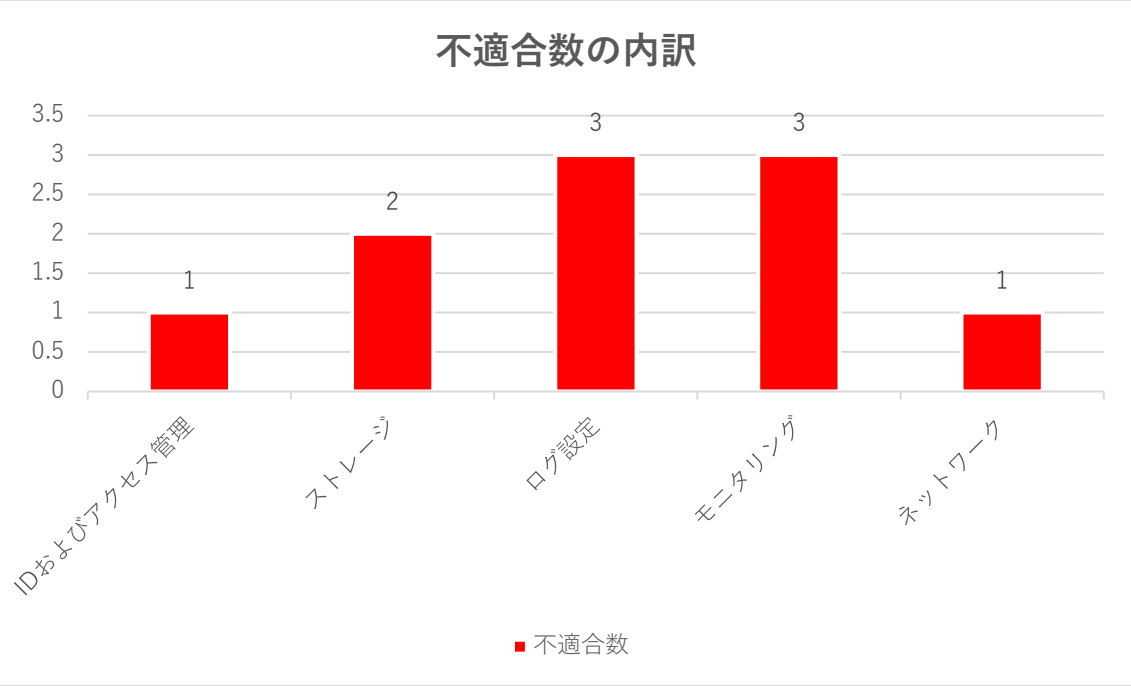
※ 適合率は不適合数÷診断項目数から全体に対する割合を計算して算出しております。



2.2. CIS AmazonWebServices Foundations Benchmark レベル 2

適合率				
55.0%				
No	**区分**	**診断項目数**	**適合数**	**不適合数**
1	ID およびアクセス管理	3	2	1
2	ストレージ	3	1	2
3	ログ設定	7	4	3
4	モニタリング	7	4	3
5	ネットワーク	2	1	1
合計		**22**	**12**	**10**
割合		**100%**	**54.5%**	**45.5%**

※ 適合率は不適合数÷診断項目数から全体に対する割合を計算して算出しております。



2.3. 指摘一覧

No	区分	不適合項目
1	ID およびアクセス管理	アカウント連絡情報
		セキュリティチームの連絡情報
		セキュリティの質問
		管理ユーザーのタスク
		アクセスキーのローテーション
		IAM インスタンスロール
		IAM アクセスアナライザ
		アカウントガバナンス
2	ストレージ	S3 バケットの暗号化
		S3 パケットの公開
		EBS の暗号化
3	ログ設定	CloudTrail の有効化
		CloudTrail のログ公開
		CloudWatchLogs
		…
		…
		…
4	モニタリング	…

3. 不適合詳細

3.1. ID およびアクセス管理

診断項目名
アカウント連絡情報
診断内容の説明
利用規定に違反している、またはセキュリティインシデントの可能性を示す挙動が AWS Abuse チームによって観察された場合、AWS はアカウント所有者に連絡をとりますが、連絡先が登録されていない場合、コンタクトすることができなくなります。
不適合の根拠
管理アカウントを利用して連絡先情報を確認した結果、連絡先が登録されていないことを確認しました。
主なリスク
連絡先が登録されていない状態で AWS アカウントが禁止または疑わしい方法で動作していることが確認された場合、AWS アカウントの所有者に連絡されることなくアカウントの凍結や利用停止などの事態に陥る危険性があります。
設定変更による影響
AWS 環境に対する影響はありません。
対策優先度
高

対策方法

■ AWS コンソールでの設定方法

1. 請求およびコスト管理コンソールを開きます。
2. ナビゲーションバーで、アカウント名を選択してから、[マイアカウント]を選択します。
3. [アカウント設定]ページの[アカウント設定]の横にある[編集]を選択します。
4. 更新する必要があるフィールドの横にある[編集]を選択します。
5. 変更を入力したら、[変更を保存]を選択します。
6. 変更を加えたら、[完了]を選択します。
7. 連絡先情報を編集するには、[連絡先情報]で[編集]を選択します。
8. 変更するフィールドに、更新した情報を入力し、[更新]を選択します。

※ 連絡先にはメーリングリストなど複数名とコンタクトが取れる連絡先を指定することを推奨いたします。

診断項目名

セキュリティチームの連絡情報

診断内容の説明

セキュリティチームの連絡先情報を指定すると、AWS から送信されたセキュリティアドバイザリ情報が指定した連絡先に届くようになります。

不適合の根拠

管理アカウントを利用して確認した結果、セキュリティチームの連絡先が登録されていないことを確認しました。

主なリスク

最新の AWS からのセキュリティアドバイザリ情報が受け取れなくなります。

設定変更による影響

AWS 環境に対する影響はありません。

対策優先度

低

対策方法

■ AWS コンソールでの設定方法

1. コンソールの右上隅にあるアカウント名をクリックします。
2. ドロップダウンメニューから[マイアカウント]をクリックします。
3. [代替連絡先]セクションまで下にスクロールします。
4. [セキュリティ]セクションに連絡先情報を入力します。

■ CLI での設定方法

なし

3.2. ストレージ

・・・省略・・・

3.3. ログ設定

・・・省略・・・

3.4. モニタリング

・・・省略・・・

3.5. ネットワーク

・・・省略・・・

3.6. その他

・・・省略・・・

4. 監査情報

環境	Amazon Web Services
アカウント情報	アカウント名 アクセスキー
監査方法	当社エンジニアによるマニュアル診断 専用ソフトウェアによるツール診断
監査項目	CIS Amazon Web Services Foundations Benchmark v2.0.0 のレベル 1 およびレベル 2
稼働状態	本番稼働前環境
アクセス方法	インターネット経由
診断実施者	徳丸 浩
診断期間	2022/03/01 ～ 2022/03/31
診断時間	10:00 ～ 18:00

5. 免責

5.1. 診断の正確性

本診断は診断対象のクラウドサービスにアクセスし、ベースライン（AWS セキュリティホワイトペーパー・AWS セキュリティベストプラクティス及び IAM ベストプラクティス）に適合しているか否かを機械的に判断しております。

診断の特性上、本報告書に記載する指摘については再現性・網羅性を完全に保証するものではありません。本書の内容をもとに対策を行なわれる場合、貴社の責任で行なって頂きますようお願いします。

5.2. 本報告書に関するお問合せ

本報告書に関するご質問・その他お問い合わせは、本報告書のご提出日より起算して 3 ヶ月間承ります。ただし、本報告書をもとにお客様がプログラム修正などの対策を実施される場合については、個別の実装方法についてのご質問にはお答えしかねますことをご了承ください。

期間終了後のお問い合わせについては、別途ご相談ください。

お問合せ先：contact@eg-secure.co.jp