

AWS設定監査サービス紹介

EGセキュアソリューションズ株式会社

設定監査とは

設定監査って必要？

AWS設定監査について

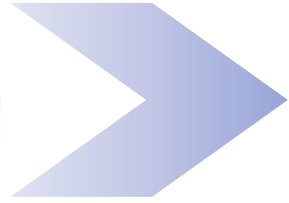
AWS設定監査の実施イメージ

監査結果の成果物

設定監査って必要？

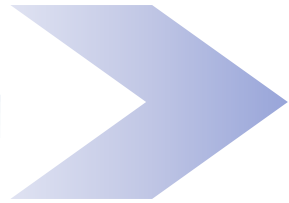
ウェブアプリケーション脆弱性診断

ウェブアプリケーションのバグ、脆弱性の検出



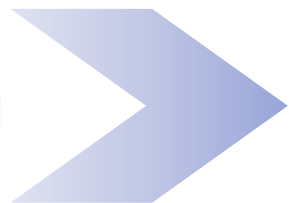
プラットフォーム脆弱性診断

OS、ミドルウェアの設定不備や古いバージョンの検出



AWS設定監査

AWSのアカウントや権限の設定不備やログの取り扱いなどが適切に成されているか監査



EGセキュアソリューションズが提供するシステムに対するセキュリティアセスメントにおける区分として左図のようなメニューをご用意しております。それぞれ診断/監査する**対象**により適切なサービスを選定いたします。

一般的なウェブアプリケーションやプラットフォームの診断では、AWSの設定を監査し設定不備を発見することは困難な為、AWS固有の設定に対する設定不備は、"**AWS設定監査**"にて洗い出します。

AWS設定監査について

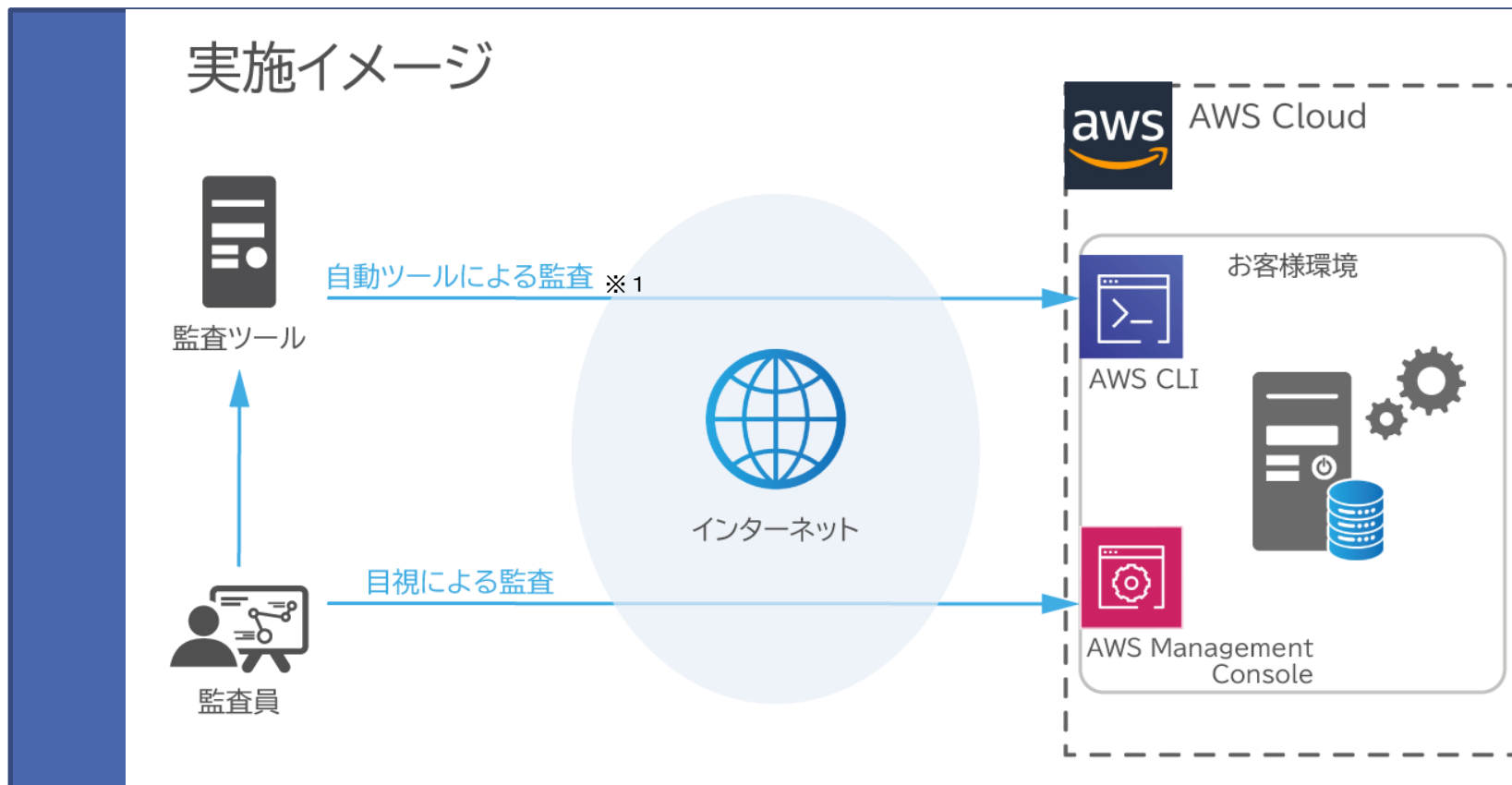
本サービスは、AWSの設定状況についてセキュリティ上の不備がないか監査を行い、その結果を監査結果報告書としてお客様へ提供するものです。

EGセキュアソリューションズのAWS設定監査サービスでは、米国のCIS(Center For Internet Security)が開発した「CIS Amazon Web Services Foundations Benchmark v5.0.0」を基準として準拠状況の確認を行います。CIS Amazon Web Service Foundations Benchmark v5.0.0は下表の5つの項目となっております。

監査項目	
項目	監査概要
Identity and Access Management	AWSのアカウントを適切に保護しているか、過大な権限を割り当てていないかなどの監査を行います。
Storage	AWSの各ストレージ設定において、暗号化設定が適切に行われているか、非暗号化通信を拒否しているかなどの監査を行います。
Logging	AWSによる各種ログの取得が行われているか、ログの暗号化が行われているかなどの監査を行います。
Monitoring	AWS上の変更が発生した場合に備えて、検知する仕組みがあるか、通知する設定があるかなどの監査を行います。
Networking	AWSのネットワーク設定において、アクセス制御が設定されていない箇所がないか監査を行います。

AWS設定監査の実施イメージ

Tenable社のセキュリティ監査ツールである「Nessus」を用いてAWSへ接続し設定監査を行う他、監査員がAWSマネジメントコンソールにログインし、目視確認(監査)を行います。



※ 1 :Security Hub補完監査プランを除く

監査結果の成果物

監査を行った結果として「CIS Amazon Web Services Foundations Benchmark v5.0.0」への準拠率と総合評価、非準拠である項目の概要、改善方法などをまとめた「AWS設定監査報告書」をPDFファイルで納品いたします。

1. エグゼクティブサマリー

1.1. 総合評価

判定状況	説明
B	監査の結果、CIS AmazonWebServices Foundations Benchmark レベル1への準拠率が66.7%の結果となりました。

1.2. 評価基準

判定状況	説明
A	CIS AmazonWebServices Foundations Benchmark レベル1への準拠率が80%以上であり、安全な設定状況です。
B	CIS AmazonWebServices Foundations Benchmark レベル1への準拠率が60%～79%の間であり、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 AmazonWebServices Foundations Benchmark レベル1への準拠率が40%～59%の間であり、一部、設定の見直しが必要です。
D	CIS AmazonWebServices Foundations Benchmark レベル1への準拠率が20%～39%の間であり、注意を要する設定状況のため、早急な対策が必要です。
E	CIS AmazonWebServices Foundations Benchmark レベル1への準拠率が0%～19%の間であり、非常に危険な設定のため、対策を実施する必要があります。

©EG Secure Solutions Inc.

Confidential

1.3. 総評

CIS Amazon Web Services Foundations Benchmark v4.0.1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は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出ています。また、ログの出力やモニタリング設定についても改善点があります。万が一、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、脆弱性、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策優先度となります。この基準は弊社独自の基準となりますが、セキュリティの観点上から各推奨事項を優先して対応していただいております。

優先度	説明
緊急	セキュリティ上、早急に対応が必要で、深刻な被害の発生につながる可能性があります。早急に対応を要する事項を推奨する項目です。
高	セキュリティ上、早急に対応を推奨しています。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しますが、被害の発生につながる可能性が低いと考えられる項目です。運用を円滑に進めるために設定する事項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、早急な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。

©EG Secure Solutions Inc.

Confidential

2.3. 指摘一覧

No.	区分	レベル	不適切項目	対策優先度
1	IDおよびアクセス管理	レベル1	アカウント連携機能	高
			セキュリティチームの連絡機能	低
			セキュリティの監視	低
			ユーザーのロケーション	高
			アクセスキーのローテーション	中
			IAM インスタンスロール	中
			IAM アクティバイザー	低
2	ストレージ	レベル1	バックアップ	中
			データの暗号化	低
			データの公開	低
3	ログ設定	レベル2	EB ログ出力	中
		レベル1	CloudTrail	低
		レベル2	CloudWatch ロググループ	低
4	モニタリング	レベル1	CloudWatch	中
		...	...	中
		レベル2	...	中
		...	...	中

©EG Secure Solutions Inc.

Confidential

3. 不適切詳細(レベル1)

本書では、「CIS AmazonWebServices Foundations Benchmark レベル1」で不適切となった項目について記載します。

3.1. IDおよびアクセス管理

3.1.1. アカウント連携機能

利用規定に違反する、またはセキュリティインシデントの可能性を示す事象が AWS Abuse チームによって報告された場合、AWS はアカウント所有者に連絡をとりませんが、連絡先が登録されていない場合、連絡先が登録することができなくなります。

不適切の理由

管理アカウントを利用して連携機能を確認した結果、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 アカウントの停止または凍結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 アカウントの停止または凍結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。

対策優先度

高

対策方法

- AWS マネジメントコンソールでの設定方法
 - 請求およびコスト管理コンソールを開きます。
 - 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。
 - [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。
 - 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。
 - 変更を入力したら、[変更を保存]を選択します。
 - 変更を加えたら、[完了]を選択します。
 - 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。
 - 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。

©EG Secure Solutions Inc.

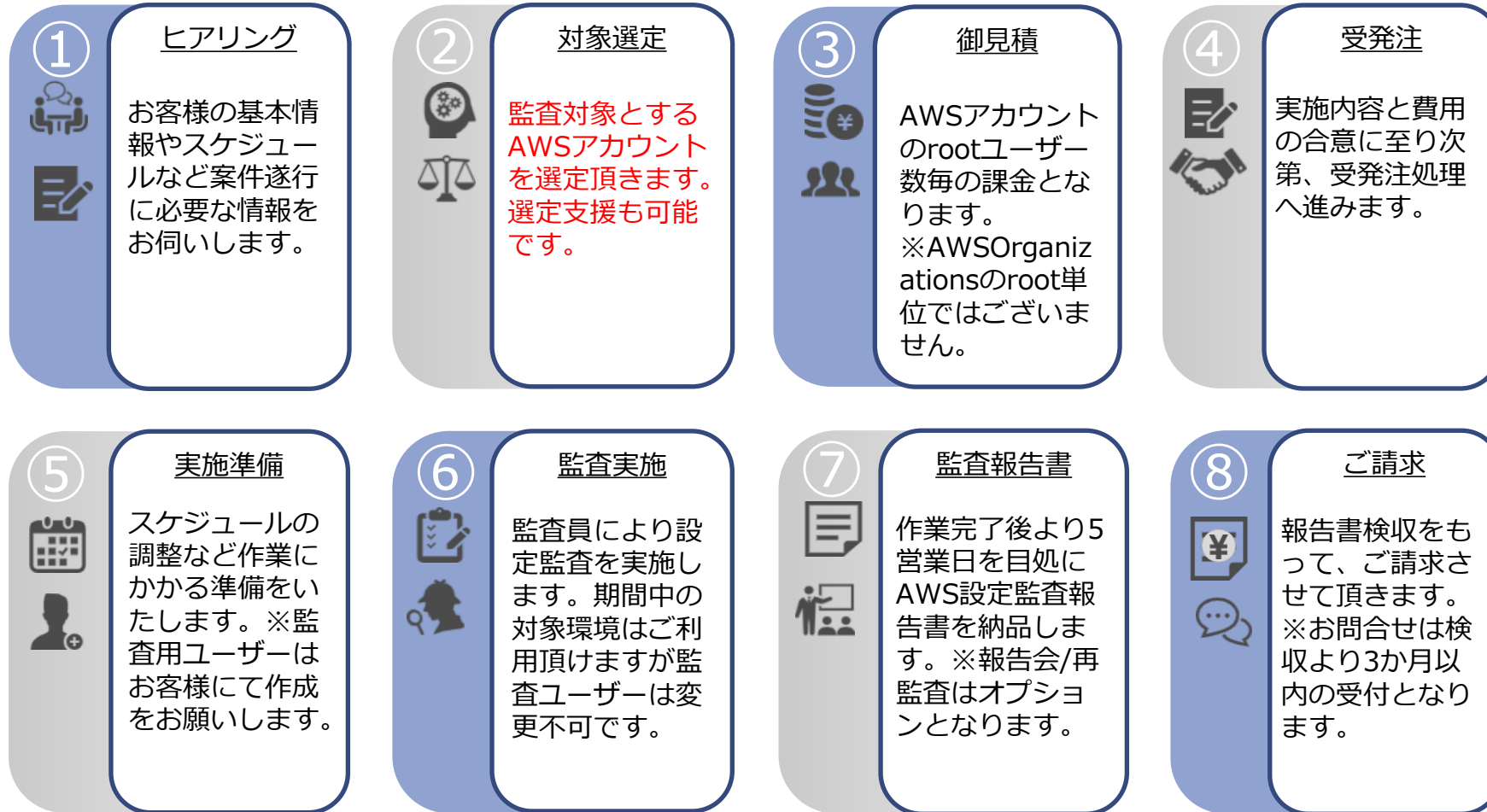
Confidential

サービスご提供までの流れ

AWS設定監査サービスご提供までの流れ

お見積に必要な情報

AWS設定監査サービス ご提供までの流れ



プランと費用

	スタンダード監査プラン	クイック監査プラン	Security Hub補完監査プラン
監査概要	CIS Amazon Web Services Foundations Benchmarkの全63項目を基に、お客様のAWS利用にかかる設定値を監査	スタンダード監査の63項目をもとに当社が項目を選定抽出し納期や費用を抑えたコンパクトな監査	Security Hub で「CIS AWS Foundations Benchmark v3.0.0」を設定済みのお客様向けに、手動監査が必要な項目のみ抽出したコンパクトな監査
導入場面の想定	Security Hubの設定を自社で実装するのは難しく対応できていないが、現状よりもセキュアなAWS環境にしたい	全量63項目の監査を依頼すると予算やスケジュールが計画にあわないが、セキュリティチェックはしたい	Security Hub は設定しているがツールでわかる範囲の監査しかできていないので、その他の監査項目も確認したい
監査項目	63	12	28
監査費用	rootアカウント 1 つ毎に110万円 ※再監査は別途見積	rootアカウント 1 つ毎に30万円 ※再監査は別途見積	rootアカウント 1 つ毎に55万円 ※再監査は別途見積
報告会		 開催回数毎に10万円	

御見積に必要な情報

ヒアリングシート

クラウド設定監査ヒアリングシート（基本情報）

1) お申込み者情報					
お申し込み					
記入者					
サービス約款への同意	☐ サービス約款について確認し、同意します。				
2) 納品先情報					
会社名					
部署名					
担当者名					
メールアドレス					
3) 請求先情報					
会社名					
部署名					
担当者名					
ご連絡方法					
メールアドレス					
住所					
4) 監査対象リージョン					
リージョン名					
5) 監査対象環境情報					
No.	AWSアカウントID	監査用IAMのID	監査用IAMのパスワード	監査用IAMのAPIキー	監査用IAMのAPIシークレット
例	123456789	egsskase	QweZwYtHspwEASjSKUFG3YYUKSmlB	AKIAVKNWTAUYY66S73V	bnfD7SqacTghw4Rfu0VfEUJZDdSSin
1					
2					
3					
4					
5					
6) 監査対象時期					
監査開始または終了希望日					
7) その他ご連絡事項					

ヒアリング項目

企業情報

監査希望rootアカウント数

ご担当者様情報

希望スケジュール

請求書送付先情報

会社概要

名 称	EGセキュアソリューションズ株式会社
本 社	〒105-0001 東京都港区虎ノ門1-2-8 虎ノ門琴平タワー 8F
設 立	2008年4月2日
代 表	齊藤 和男
株 主	イー・ガーディアン株式会社 (プライム市場/証券コード：6050) 100%
事業内容	1. 情報セキュリティ、情報システムに関する監査、コンサルティング 2. 情報セキュリティに関する調査、研究、執筆 3. 情報セキュリティ関連の教育及びコンテンツ制作 4. セキュリティ製品の開発、販売、サポート



IS575950 / ISO27001:2013

情報セキュリティサービス基準適合（情報セキュリティ監査サービス）

2024年12月20日登録

https://sss-erc.org/iss_books/020-0012-10/



020-0012-10

取締役CTOプロフィール

徳丸 浩（とくまる ひろし）



略 歴

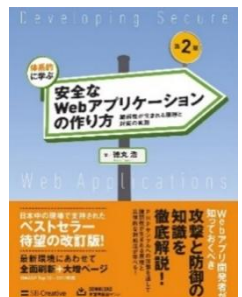
1985年京セラ株式会社に入社後、ソフトウェアの開発、企画に従事。1999年に携帯電話向け認証課金基盤の方式設計を担当したことをきっかけにWebアプリケーションのセキュリティに興味を持つ。2004年同分野を事業化。

2008年独立、Webアプリケーションセキュリティを専門分野とするHASHコンサルティング株式会社（現EGセキュアソリューションズ株式会社）を設立。

2015年イー・ガーディアングループに参画。2019年よりイー・ガーディアン子会社のグレスアベイル株式会社取締役を兼任。2021年取締役CTO就任。

独立行政法人情報処理推進機構（IPA）非常勤研究員
技術士（情報工学部門）

著 書



実 績 等

相次ぎ発生する預貯金の不正引き出しについて、テレビ東京ワールドビジネスサテライト等メディアでの解説や東洋経済、産経新聞他、ITmedia等IT系メディアの取材実績多数。
その他、セキュリティイベントでの基調講演やゲスト講演も多数。

著書『体系的に学ぶ 安全なWebアプリケーションの作り方 第2版』を教材、出題範囲とする民間試験「ウェブ・セキュリティ基礎試験」（徳丸基礎試験）が2019年より開始。

本サービスに関するお問合せ・お見積のご依頼

- 公式サイト <https://www.eg-secure.co.jp/contact/>
- メール contact@eg-secure.co.jp