現場で役立つ

セキュア・アーキテクティング・レビュー

のポイント

― AWS Well-Architected Framework ―

一般社団法人 日本クラウドセキュリティアライアンス（CSA ジャパン）
クラウドセキュリティワーキンググループ

目次

CSA ジャパン成果物の提供に際しての制限事項

日本クラウドセキュリティアライアンス（CSA ジャパン）は、本書の提供に際し、以下のことをお断りし、またお願いします。以下の内容に同意いただけない場合、本書の閲覧および利用をお断りします。

1．　責任の限定

CSA ジャパンおよび本書の執筆・作成・講義その他による提供に関わった主体は、本書に関して、以下のことに対する責任を負いません。また、以下のことに起因するいかなる直接・間接の損害に対しても、一切の対応、是正、支払、賠償の責めを負いません。

(1) 本書の内容の真正性、正確性、無誤謬性
(2) 本書の内容が第三者の権利に抵触しもしくは権利を侵害していないこと
(3) 本書の内容に基づいて行われた判断や行為がもたらす結果
(4) 本書で引用、参照、紹介された第三者の文献等の適切性、真正性、正確性、無誤謬性および他者権利の侵害の可能性

2．　二次譲渡の制限

本書は、利用者がもっぱら自らの用のために利用するものとし、第三者へのいかなる方法による提供も、行わないものとします。他者との共有が可能な場所に本書やそのコピーを置くこと、利用者以外のものに送付・送信・提供を行うことは禁止されます。また本書を、営利・非営利を問わず、事業活動の材料または資料として、そのまま直接利用することはお断りします。

ただし、以下の場合は本項の例外とします。

(1) 本書の一部を、著作物の利用における「引用」の形で引用すること。この場合、出典を明記してください。
(2) 本書を、企業、団体その他の組織が利用する場合は、その利用に必要な範囲内で、自組織内に限定して利用すること。
(3) CSA ジャパンの書面による許可を得て、事業活動に使用すること。この許可は、文書単位で得るものとします。
(4) 転載、再掲、複製の作成と配布等について、CSA ジャパンの書面による許可・承認を得た場合。この許可・承認は、原則として文書単位で得るものとします。

3．　本書の適切な管理

(1) 本書を入手した者は、それを適切に管理し、第三者による不正アクセス、不正利用から保護するために必要かつ適切な措置を講じるものとします。
(2) 本書を入手し利用する企業、団体その他の組織は、本書の管理責任者を定め、この確認事項を順守させるものとします。また、当該責任者は、本書の電子ファイルを

適切に管理し、その複製の散逸を防ぎ、指定された利用条件を遵守する（組織内の利用者に順守させることを含む）ようにしなければなりません。

(3) 本書をダウンロードした者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、そのダウンロードしまたは複製した本書のファイルのすべてを消去し、削除し、再生や復元ができない状態にするものとします。この要求は理由によりまたは理由なく行われることがあり、この要求を受けた者は、それを拒否できないものとします。

(4) 本書を印刷した者は、CSA ジャパンからの文書（電子メールを含む）による要求があった場合には、その印刷物のすべてについて、シュレッダーその他の方法により、再利用不可能な形で処分するものとします。

4. その他

その他、本書の利用等について本書の他の場所に記載された条件、制限事項および免責事項は、すべてここに記載の制限事項と並行して順守されるべきものとします。本書およびこの制限事項に記載のないことで、本書の利用に関して疑義が生じた場合は、CSA ジャパンと利用者は誠意をもって話し合いの上、解決を図るものとします。

その他本件に関するお問合せは、info@cloudsecurityalliance.jp までお願いします。

本書執筆編集メンバー
井上 淳
面 和毅
釜山 公徳
森田 翔
※五十音順

- 変更履歴

日付	版数	変更内容
2023 年 12 月 26 日	1.0	初版発行

1. はじめに

クラウドコンピューティングを意味する「クラウド」。このクラウドは日々使われる用語として市民権を得て、様々なビジネスシーンで登場するようになりました。クラウドの提供形態は様々で、利便性の高い多種多様なサービスが存在し、日々進化し続けています。

クラウドの利用者は増加し続けていますが、その一方でサイバーセキュリティインシデントも増加し続けており、単純に利用者の増加に比例しているわけではありません。

なぜクラウドでセキュリティインシデントが増加するのか。それを紐解くためにはクラウドの利用形態とは何かを抑える必要があります。クラウドは、クラウドサービス事業者が自動化や標準化、共通化などを行って IT リソースを抽象化し、その抽象化された IT リソースをサービスとして利用できるプロダクトを指します。クラウドサービスの提供形態は、NIST SP 800-145 で IaaS、PaaS、SaaS の 3 つのサービスモデルとして定義されており、多くの場合はこの 3 つのサービスモデルを用いて責任共有モデル(Shared Responsibility Model)を定義し、クラウドサービス事業者と利用者との責任範囲を可視化します。しかし、この 3 つのサービスモデルは大まかな提供形態をモデル化しているだけに過ぎず、実際に提供されているクラウドサービスは個々のサービスによって責任範囲が異なり、クラウドサービス事業者間で同様のクラウドサービスでも責任範囲が異なることがあります。

クラウドは IT リソースが抽象化されたことにより簡便に利用可能になった一方で、多種多様の責任範囲が異なるサービスが公開されており、「誰が」、「どのように」、「何をすればよいか」も抽象化されているのが現状です。さらには、クラウドを安全かつ効果的に利用するためには様々なサービスを組み合わせるため、環境が複雑になって攻撃可能領域を作りやすく、セキュア・アーキテクティングの難度があがります。こういったクラウド利用の課題により、本来のクラウドのメリットが享受できず、設定ミス(Mis-Configuration)によるリスクが生じ、このリスクをついた攻撃により多くの深刻な情報窃取が発生しております。

クラウドを安全に利用するためには、ネイティブサービスを含めた様々なセキュリティプロダクト、AWS Well-Architected Framework といったベストプラクティス集によるセキュア・アーキテクティング、SecOps を支援するソリューションがあります。本書で AWS Well-Architected Framework をより効果的に利用することにより、よりセキュアにする活動の一助になれれば幸甚です。

日本クラウドセキュリティアライアンス
クラウドセキュリティワーキンググループ　リーダー
釜山 公徳

2. 本書執筆における前提事項・留意事項

- AWS 社による既存の評価、内容、改善計画に対し、それぞれの項目を実務の視点で捉え、現場で検討する可能性がある項目を挙げております。
- 本書は、ワーキンググループにて独自に解釈したものとし、正確性や網羅性の保証は無く、執筆者による粒度の相違があります。
- 本書の執筆は、2022 年末であるため、最新の AWS Well-Architected Framework とは一部相違がありますが、検討の視点としては有効です。

3. AWS Well-Architected Framework セキュリティの柱

3.1. SEC1

AWS における SEC1 の質問は以下が挙げられています。

質問	ワークロードの認証情報と認証をどのように管理していますか？

3.1.1. SEC1-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	アカウントを使用してワークロードを分ける
内容	会社のレポート構造をミラーリングするのではなく、機能または共通のコントロールセットに基づいて、ワークロードを別々のアカウントに整理し、アカウントをグループ化します。セキュリティとインフラストラクチャを念頭に置いて、ワークロードが増大するにつれて組織が共通のガードレールを設定できるようにします。
改善計画	・AWS Organizations を使用する: AWS Organizations を使用し、複数の AWS アカウントにポリシーベースの管理を一元的に適用します。 ・AWS Control Tower を検討する: AWS Control Tower では、ベストプラクティスに基づいて、新しいセキュアなマルチアカウントの AWS 環境を容易にセットアップおよび管理できます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
ワークロードの定義	・ ワークロードが何であるかの定義を具体的に行っているか。	・ ワークロードの定義に関する要件定義書、設計書を確認する。
アタックサーフェス(攻撃可能領域)の定義と可視化	・ 対象システムにおけるセキュリティポリシーで、アタックサーフェスの定義、可視化を行っているか。	・ 同上
複数の AWS アカウント利用時におけるベストプラクティス適応	・ AWS アカウントでそれぞれ何を行っているかを把握し、俯瞰的に管理できているか。	・ 「ワークロードの定義」の行動例に加え、AWS Trusted Advisor の Organization View を活用する。
アクセス権限付与の適切な設計	・ ワークロードに割り当てられた AWS アカウントへのアクセス権限	・ 同上

	を付与する対象とそのルールを定義しているか。	

3.1.2. SEC1-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	AWS アカウントのセキュリティを確保する
内容	たとえば、MFA を有効にしてルートユーザーの使用を制限したり、アカウントの連絡先を設定したりすることで、アカウントへのアクセスを保護します。
改善計画	・AWS Organizations を使用する: AWS Organizations を使用し、複数の AWS アカウントにポリシーベースの管理を一元的に適用します。 ・AWS ルートユーザーの使用を制限する: 特定のルートユーザーを必要とするタスクについては、当該ルートユーザーのみを使用します。 ・ルートユーザーの MFA を有効にする: AWS Organizations がルートユーザーを管理していない場合は、AWS アカウントのルートユーザーで MFA を有効にします。 ・ルートユーザーパスワードを定期的に変更する: ルートユーザーのパスワードを変更することにより、保存したパスワードが使用できる状態となっていることによるリスクが軽減されます。AWS Organizations を使用しておらず、あらゆるユーザーが物理的にアクセスできる場合に特に重要です。 ・AWS アカウントのルートユーザーが使用された場合に通知を送信するようにする: 通知を受け取ることで、リスクは自動的に軽減されます。 ・新しく追加されたリージョンへのアクセスを制限する: 新しい AWS リージョンについて、ユーザーやロールなどの IAM リソースは、有効にしたリージョンのみに伝播されます。 ・CloudFormation StackSets について検討する: CloudFormation StackSets を使用すると、IAM ポリシー、ロール、グループなどのリソースをさまざまな AWS アカウントとリージョンに承認されたテンプレートからデプロイできます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
AWS アカウントの権限について	・ AWS アカウントが大きな権限を有していることを明文化しているか。	・ 設計書で明記する。
AWS アカウントの使用制限	・ 一部の管理者しか使用出来ないように制限しているか、または AWS アカウントを使用不可にしているか。	・ AWS アカウントを利用できる要員を限定する。 ・ AWS アカウントを使用不可にする場合、パスワードが記載された媒体を物理的に金庫で保管する。 ・ リセラーとの契約によ

		り AWS アカウント自体を保有しない。
特権を有するアカウント認証の多重化	・ MFA(Multi Factor Authentication : 多要素認証)を実装しているか。	・ AWS IAM で MFA を有効化する。
MFA の選定	・ 要件に応じてハードウェアトークンかソフトウェアトークンかを選定しているか。	・ 業務用のスマートフォンが存在し、かつ MDM といった端末を管理するソリューションがある場合はソフトウェアトークン。そうでない場合は、ハードウェアトークンを選定する。
MFA の冗長化	・ MFA の冗長化を検討したか。 ・ ソフトウェアトークンの場合、複数のアプリケーションを利用することや、スマートフォン自体の冗長化を検討したか。	・ 同左
MFA のバックアップ(エクスポート)	・ 有事の際に備えて、MFA のバックアップ(エクスポート)を定期的に行なっているか。	・ 同左

3.1.3. SEC1-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	管理目標を特定および検証する
内容	脅威モデルから特定されたコンプライアンス要件とリスクに基づいて、ワークロードに適用する必要がある管理目標および管理を導き出し、検証します。管理目標と管理を継続的に検証することは、リスク軽減の有効性を測定するのに役立ちます。
改善計画	・コンプライアンス要件を特定する: ワークロードが準拠する必要のある組織要件,法的要件,規制要件を確認します。 ・AWS コンプライアンスリソースを確認する: コンプライアンスを支援するために使用できる AWS のリソースを特定します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
業界の標準やベストプラクティスへの準拠の確認	・ システムに応じた業界の標準(クレジットカードの場合、PCI DSS)やベストプラクティスへの準拠を確認し、要件に応じた適切なセキュリティが実装されているか。	・ AWS Audit Manager や AWS Security Hub などを使用して、継続的に評価する。
セキュリティリファレンスの参照	・ 当該システムに有用なセキュリティリファレンスを整理し、標準化された情報を取り込んでいるか。	・ CSA のセキュリティガイダンスや NIST Cybersecurity Framework を参照する。
監査レポートの確認	・ 監査レポートで AWS におけるセキュリティの評価を確認しているか。	・ AWS Artifact を使用して、対象コンプライアンスの監査レポートを入手して確認する。

3.1.4. SEC1-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	セキュリティ脅威に関する最新情報を入手する
内容	最新のセキュリティ脅威を常に把握して攻撃ベクトルを認識し、適切な管理を定義して実装できるようにします。
改善計画	・脅威インテリジェンスソースを購読する: ワークロードで使用しているテクノロジーに関連する、複数のソースからの脅威インテリジェンス情報を定期的に確認します。 ・AWS Shield Advanced サービスについて検討する: ワークロードがインターネットにアクセスできる場合、インテリジェンスソースについてのほぼリアルタイムでの可視性を提供します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
継続的な脅威情報や脅威インテリジェンスの収集	・ 情報とインテリジェンスの違いを理解しているか。OSINT を効果的に行っているか。	・ 6 つの基本的なインテリジェンス(SIGINT、IMINT、MASINT、HUMINT、OSINT、GEOINT)を踏まえた上

		での OSINT の運用を設計する。 ・ 脅威インテリジェンスの専門企業から情報やインテリジェンスを収集する。
社外組織との情報共有	・ 自助、共助、公助の観点に基づき、自組織における体制構築と他組織との連携による情報共有するスキームがあるか。	・ 共助：所属する業界の団体との連携。 ・ 公助：監督省庁や警察庁、NISC 等との連携。
脅威インテリジェンスの活用	・ 脅威インテリジェンスを自組織で作成する、もしくは脅威インテリジェンス事業者から提供されているか。 ・ 自組織で脅威インテリジェンスを活用できる体制はあるか。	・ TLPT(Threat-Led Penetration Testing : 脅威ベースのペネトレーションテスト)で、脅威インテリジェンスを活用する。

3.1.5. SEC1-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	セキュリティのレコメンデーションに関する更新情報を入手する
内容	AWS と業界の両方のセキュリティのレコメンデーションを常に最新に保ち、ワークロードのセキュリティ体制を進化させます。
改善計画	・AWS の更新情報をフォローする: 新しいレコメンデーション、ヒント、コツをサブスクライブまたは定期的に確認します ・業界ニュースを購読する: 複数のソースから、ワークロードで使用しているテクノロジーに関連するニュースフィードを定期的に確認します

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
AWS 社が公開する情報の収集	・ AWS における複数の情報源(AWS 社発信の公式情報、パートナー企業による情報、ユーザーグループでの発	・ AWS 社の公式情報(サービスアップデート情報、ブログ)を確認する。 ・ JAWS-UG(AWS Users

	信)を活用しているか。	Group – Japan)といったユーザーグループに参加する。
セキュリティ関連テクノロジーの情報収集	・ セキュリティ専門組織による AWS や AWS に関する情報を収集しているか。	・ CISA(Cybersecurity and Infrastructure Security Agency)から専門的な情報を収集する。
業界団体や業界誌による情報の収集	・ 業界特有の情報を収集しているか。	・ 業界団体に所属し、当該業界におけるサイバーセキュリティ情報を収集する。(金融であれば FISC や金融 ISAC)

3.1.6. SEC1-6

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	パイプラインのセキュリティコントロールのテストと検証を自動化する
内容	ビルド、パイプライン、プロセスの一環としてテストおよび検証されるセキュリティメカニズムの安全なベースラインとテンプレートを確立します。ツールとオートメーションを使用して、すべてのセキュリティコントロールを継続的にテストおよび検証します。たとえば、マシンイメージやインフラストラクチャなどの項目をコードテンプレートとしてスキャンして、セキュリティの脆弱性、不規則性、およびドリフトを各ステージで確立されたベースラインから確認します。
改善計画	・設定管理を自動化する: 設定管理サービスやツールを使うことで、自動的に安全性の高い設定を適用および検証します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
ヒューマンエラーを極小化するための施策	・ 人手による作業を必要最小限に抑える施策があるか。	・ 自動化やパッケージ製品の活用、AWS のネイティブサービス(AWS Config など)を活用する。
自動化によるセキュリティコントロール	・ 当該システムにおける設定変更時の管理や検証などを自動で行なっているか。	・ 同上
ヒューマンエラーのリスク	・ ヒューマンエラーが起	・ 規定類でリスク対応を

対応	こり得る箇所で、事故発生を想定したリスク対応策を整理しているか。	整理する。 ・ インシデント対応フローを整備する。
合理的な CI/CD の実装	・ AWS のネイティブサービスや、OSS の活用を適材適所で検討して利用しているか。	・ AWS のネイティブサービス： Code ファミリー ・ OSS：Git、Jenkins, Ansible, Maven、SonarQube

3.1.7. SEC1-7

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	脅威モデルを使用してリスクを特定し、優先順位を付ける
内容	脅威モデルを使用して潜在的な脅威を特定し、その登録を最新の状態に維持します。脅威に優先順位を付け、セキュリティコントロールを調整して防止、検出、対応を行います。進化するセキュリティ環境の状況に応じてセキュリティコントロールを再確認および維持します。
改善計画	・脅威モデルを作成する: 脅威モデルは、潜在的なセキュリティ脅威を特定して対処するのに役立ちます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
脅威モデリングの実施	・ 脅威モデリングを自組織で実施、または他組織による提供があるか。	・ 設計(Design)、分解(Break)、修正(Fix)、検証(Verify)を経て脅威モデリングを行う。
脅威の優先順位付け	・ 脅威モデルをベースにした脅威の優先順位付けができているか。	・ 規定類や設計書などで整理する。

3.1.8. SEC1-8

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	新しいセキュリティサービスと機能を定期的に評価および実装する
内容	AWS および APN パートナーは、ワークロードのセキュリティ体制を進化させることができる新しい機能とサービスを継続的にリリースしています。
改善計画	・定期的なレビューを計画する: コンプライアンス要件、AWS の新しいセキュリティ機能とセキュリティサービスの評価、業界の最新ニュースの入手を含むレビューアクティビティのカレンダーを作成します。 ・AWS のサービスと機能について調べる: 使用中のサービスで利用可能なセキュリティ機能について調べ、新しい機能がリリースされた時には、それについて確認します。 ・AWS のサービスの導入プロセスを定義する: 新しい AWS サービスの導入プロセスを定義します。新しい

AWS のサービスの機能とワークロードのコンプライアンス要件を評価する方法を含めます。
・新しいサービスと機能をテストする: 新しいサービスと機能がリリースされたら、本稼働環境に近いかたちで複製する本稼働環境ではない環境でテストします。
・その他の防御メカニズムを実装する: ワークロードを保護するための自動化されたメカニズムを実装し、利用可能なオプションを確認します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
継続的なセキュリティ機能の評価	・ 収集した情報に基づき、継続的にセキュリティ機能に関する評価と実装を行なっているか。	・ 同左
定期的なサイバーレジリエンスの評価	・ 脆弱性評価、ペネトレーションテスト(レッドチーム演習を含む)を実施しているか。	・ 同左
体制に関する実効性の評価	・ 自組織で 3 ラインモデルを活用し、セキュリティに関する組織体制を整備したか。 ・ 組織要件に応じて CSIRT、SOC、CCoE、サイバーセキュリティ CoE が構成されているか。 ・ 継続的にセキュリティオペレーションの実効性を評価しているか。	・ 同左

3.2. SEC2

SEC2 の質問について、AWS では以下が挙げられています。

質問	ユーザー ID とマシン ID はどのように管理したらよいでしょうか?

3.2.1. SEC2-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	強力なサインインメカニズムを使用する
内容	パスワードの最小長を適用し、一般的なパスワードやパスワードの再使用を避けるようにユーザーを教育します。ソフトウェアまたはハードウェアのメカニズムを使用した Multi-Factor Authentication (MFA) を義務化することで、セキュリティを強化できます。
改善計画	・MFA サインインを強制する IAM ポリシーを作成する: ユーザーが [My Security Credentials] ページでロールを引き受け、自分の認証情報を変更し、MFA デバイスを管理できるようにするものを除いて、すべての IAM アクションを禁止するカスタマー管理 IAM ポリシーを作成します。 ・ID プロバイダーで MFA を有効にする: 使用する ID プロバイダーまたはシングルサインオンサービス (AWS Single Sign-On (SSO) など) で MFA を有効にします。 ・強力なパスワードポリシーを設定する: IAM やフェデレーテッド ID システムで強力なパスワードポリシー

を設定し、総当たり攻撃から守ります。
・認証情報を定期的にローテーションする: ワークロードの管理者が、パスワードとアクセスキー (使用されている場合) を定期的に変更するようにします。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
特権 ID 管理	・ AWS アカウントのルートユーザーなど、個人に紐づかずに高い権限レベルを持つユーザーについては一般のユーザーと異なる管理を行っているか。	・ ルートユーザーは MFA を必須とする。 ・ ルートユーザーの使用は、IAM ユーザーの作成など、必要な場合のみに限定する。
特権 ID 以外の ID 管理	・ パスワード侵害に対するリスクアセスメントを実施し、費用対効果に応じて適切な認証強化方法を選択しているか。	・ パスワードポリシーの徹底や定期的なパスワード変更、従業員教育などの対策も併用してリスク低減を図る。
不要な ID の削除	・ 退職者や異動により職務を離れた従業員のユーザーアカウントによるトラブル防止を考慮しているか。	・ 不要になった ID は、要件に応じて直ちに削除か無効化する。 ・ 定期的に ID の棚卸を実施する。

3.2.2. SEC2-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	一時的な認証情報を使用する
内容	一時的な認証情報を動的に取得するために ID を要求します。人員 ID の場合、AWS Single Sign-On、または IAM ロールによるフェデレーションを使用して AWS アカウントにアクセスします。マシン ID の場合、長期的なアクセスキーではなく IAM ロールの使用を要求します。
改善計画	・最小権限ポリシーを実装する: IAM グループおよびロールに最小権限のアクセスポリシーを割り当てて、定義したユーザーのロールまたは機能を反映します。 ・必要でないアクセス許可を削除する: 不要なアクセス許可を削除して、最小権限を実装します。 ・アクセス許可の境界を考慮する: アクセス許可の境界は、アイデンティティベースのポリシーが IAM エンティティに付与できるアクセス許可の上限を設定する管理ポリシーを使用するための高度な機能です。エンティティのアクセス許可の境界では、アイデンティティベースのポリシーとそのアクセス許可の境界の両方で許可されているアクションのみを実行できます。 ・アクセス許可のリソースタグを検討する: タグを使用して、タグ付けをサポートする AWS リソースへのアクセスを制御できます。また、IAM ユーザーとロールにタグ付けして、ユーザーがアクセスできる内容を制御することもできます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
運用ルールの整理	・ 運用ルールを遵守することにより、不要なアクセス権限が残ってしまうリスクを考慮しているか。	・ 組織外のメンバーに対し、一時的に特権を与える場合の権限付与について、規定とフローを文書にする。
運用の自動化	・ 権限付与をシステムで自動的に行うことで、人的ミスの防止やセキュリティ監査への対応を図っているか。	・ 権限付与の申請/承認をワークフロー等との連携によって自動化する。
不要権限の削除	・ 不要なアクセス許可を削除しているか。	・ 不要になった権限は、要件に応じて直ちに削除か無効化する。 ・ 定期的に権限の棚卸を実施する。

3.2.3. SEC2-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	シークレットを安全に保存して使用する
内容	サードパーティーアプリケーションへのパスワードなどのシークレットを必要とする人員 ID とマシンの ID については、専門的なサービスの最新の業界標準を使用して自動ローテーションを使用して保存します。
改善計画	・AWS Secrets Manager を使用する: AWS Secrets Manager は、機密情報の管理を容易にする AWS のサービスです。シークレットとは、データベース認証情報、パスワード、サードパーティー API キー、任意のテキストなどです。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
管理下におけるシークレットの明確化	・ 保持するシークレット情報を網羅的に把握しているか。	・ システム間連携のためにシステム上で保持する必要があるシークレットを網羅的に把握し、定期変更などの運用を検討する。
シークレット管理方法の見直し	・ クラウドで利用可能な、より安全なシーク	・ オンプレミスの資産をクラウドへ移行する場

	レット管理方法を採用しているか。	合、設定ファイルなどに埋め込まれたシークレットをそのまま移行するのではなく、AWS Secrets Manager への移行を検討する。

3.2.4. SEC2-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	一元化された ID プロバイダーを利用する
内容	人員 ID の場合、一元化された場所で ID を管理できる ID プロバイダーを利用します。これにより、1 つの場所からアクセスを作成、管理、取り消すことができるため、アクセスの管理が容易になります。これにより、複数の認証情報の要件が軽減され、HR プロセスと統合する機会がもたらされます。
改善計画	・管理アクセスを一元化する: IAM ID プロバイダーエンティティを作成して、AWS アカウントと ID プロバイダー (IdP) の間に信頼関係を確立します。IAM は、OpenID Connect (OIDC) または SAML 2.0 (Security Assertion Markup Language 2.0) と互換性のある IdP をサポートします。 ・アプリケーションアクセスを一元化する: アプリケーションアクセスを一元化するために Amazon Cognito を検討します。ユーザーのサインアップやサインイン、アクセスコントロールをモバイルアプリやウェブアプリに簡単に追加できます。Amazon Cognito は、数百万人のユーザーにスケールし、Facebook、Google、Amazon などのソーシャル ID プロバイダー、SAML 2.0 を介したエンタープライズ ID プロバイダーによるサインインをサポートします。 ・古い IAM ユーザーとグループを削除する: ID プロバイダー (IdP) の使用を開始したら、不要になった IAM ユーザーとグループを削除します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
統合 ID 管理の導入に必要な手段	・ 統合 ID 管理の導入により HR プロセスとの連携など運用の自動化を図っているか。	・ 未統合状態のアプリケーションが乱立している場合、手始めに組織内の ID リソースや ID 体系の把握を行い、重要度の高いシステムから段階的に ID 統合を進める計画を立て、中長期的な取り組みによって組織内の ID 統合を進化させる。

3.2.5. SEC2-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	定期的に認証情報を監査およびローテーションする
内容	一時的な認証情報を利用できず、長期的な認証情報を必要とする場合、認証情報の監査を行い、定義されているコントロール (MFA など) が義務化されているか、定期的にローテーションされているか、アクセスレベルが適切かどうかを確認します。
改善計画	・認証情報を定期的に監査する: 認証情報レポートと IAM Access Analyzer を使用して、IAM 認証情報とアクセス許可を監査します。 ・アクセスレベルを使用して IAM アクセス許可を確認する: AWS アカウントのセキュリティを向上させるには、各 IAM ポリシーを定期的に確認してモニタリングします。ポリシーが、必要なアクションのみを実行するために必要な最小権限を付与していることを確認します。 ・IAM リソースの作成と更新の自動化を検討する: AWS CloudFormation を使用すると、テンプレートを検証してバージョンを管理できるため、ロールやポリシーを含む IAM リソースのデプロイを自動化して、人為的ミスを減らすことができます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
CSPM 導入の検討	・ 特に大規模組織において、CSPM の利用を検討しているか。	・ 改善計画の記載事項において、一律に統制を取ることが難しい場合、組織の規模に応じて CSPM の導入を検討する。

3.2.6. SEC2-6

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ユーザーグループと属性を活用する
内容	一般的なセキュリティ要件を持つユーザーを ID プロバイダーによって定義されたグループに配置し、アクセスコントロールに使用される可能性のあるユーザー属性 (部署や場所など) が正確で、最新の状態に保たれるようにするメカニズムを導入します。アクセスを制御するには、個々のユーザーではなくこれらのグループと属性を使用します。これにより、ユーザーのアクセスニーズが変化したときに多くの個別のポリシーを更新することなく、ユーザーのグループメンバーシップや属性を 1 回変更することで、アクセスを一元管理できます。
改善計画	・AWS Single Sign-On (SSO) を使用している場合は、グループを設定します。: AWS SSO では、ユーザーのグループを設定し、必要なレベルのアクセス許可をグループに割り当てることができます。 ・属性ベースのアクセスコントロール (ABAC) について: 属性ベースのアクセスコントロール (ABAC) は、属性に基づいてアクセス許可を定義する認証戦略です。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
グループや属性の割り当ての自動化	・ 外部システムとの連携による、グループや属性の割り当ての自動化	・ AWS のネイティブサービスでの対応が難しい場合、

	を検討する。	IDaaS(Microsoft Entra ID(旧 Azure Active Directory)、Okta、OneLogin など)との連携を検討する。

3.3. SEC3

SEC3 の質問について、AWS では以下が挙げられています。

質問	人とマシンのアクセス許可はどのように管理すればよいでしょうか?

3.3.1. SEC3-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	アクセス要件を定義する
内容	ワークロードの各コンポーネントまたはリソースには、管理者、エンドユーザー、またはその他のコンポーネントからアクセスする必要があります。各コンポーネントにアクセスできるユーザーや内容を明確に定義し、適切な ID タイプと認証および承認の方法を選択します。
改善計画	・職務と責任に必要な権限を定義する: ユーザーの職務、ロール、または責任に基づいて、アクセスする必要のあるリソースと適用される条件を定義します。共通の要件を持つユーザーをグループ化して、ポリシーの委任を容易にします。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
アクセス要件を定義した規定類の整理	・ 最小権限の原則に基づき、誰が、何を、どのようにアクセス出来るかを整理した規定類の有無を整理する。	・ 同左
IAM ユーザーと利用者との紐付け	・ インシデント発生時の追跡性を確保するため、1 つの IAM ユーザーにつき 1 人を割り当てているか。(1 つの IAM ユーザーを複数人で共有していないか)	・ 同左
共有アカウントの制限	・ 要件により、やむを得ず IAM ユーザーを共有せざるを得ない場	・ 左記に加え、AWS IAM での利用状況を確認する。

	合、IAM ユーザー利用時に誰が、いつ、何を実施したかの監査証跡を残す仕組みはあるか。	

3.3.2. SEC3-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	最小権限のアクセスを付与する
内容	特定の条件下で特定の AWS リソースに対する特定のアクションを行えるようにして、ID に必要なアクセスのみを付与します。グループと ID 属性を利用して、個々のユーザーのアクセス許可を定義するのではなく、規模に応じてアクセス許可を動的に設定します。たとえば、開発者のグループに、扱うプロジェクトのリソースのみを管理することを許可できます。これにより、開発者がグループから削除されると、アクセスポリシーに変更を加えることなく、そのグループがどこでアクセスコントロールに使用されたかを問わず、開発者のアクセスが取り消されます。
改善計画	・最小権限ポリシーを実装する: IAM グループおよびロールに最小権限のアクセスポリシーを割り当てて、定義したユーザーのロールまたは機能を反映します。 ・必要でないアクセス許可を削除する: 不要なアクセス許可を削除して、最小権限を実装します。 ・アクセス許可の境界を考慮する: アクセス許可の境界は、アイデンティティベースのポリシーが IAM エンティティに付与できるアクセス許可の上限を設定する管理ポリシーを使用するための高度な機能です。エンティティのアクセス許可の境界では、アイデンティティベースのポリシーとそのアクセス許可の境界の両方で許可されているアクションのみを実行できます。 ・アクセス許可のリソースタグを検討する: タグを使用して、タグ付けをサポートする AWS リソースへのアクセスを制御できます。また、IAM ユーザーとロールにタグ付けして、ユーザーがアクセスできる内容を制御することもできます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
アクセス権限付与に関する規定類	・ アクセス権限の付与は攻撃可能領域の拡大に繋がることを認識の上で規定類を整備しているか。 ・ 規定類で個別のサービス単位で最小限のアクセス権限を付与するように明記されているか。 ・ リスク分析に基づいたアクセス権限設定が定義されているか。	・ 同左

データクラシフィケーション	・ IT 資産管理やインシデントレスポンスの効率化のため、リスクベースアプローチに基づき、データの識別や区分を行ったか。	・ 同左
タグの命名規則	・ タグの命名規則について、実用的かつ合理的に整理の上で、文書化できているか。	・ 同左
AWS IAM の管理者	・ AWS IAM 設定の運用ルールやワークフローが定義されて、いつ誰が設定変更を実施したか追跡できるようになっているか。	・ 同左

3.3.3. SEC3-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	緊急アクセスのプロセスを確立する
内容	自動プロセスまたはパイプラインの問題が発生した場合に、ワークロードへの緊急アクセスを許可するプロセス。これにより、最小権限のアクセスを利用しながら、ユーザーは必要なときに適切なレベルのアクセスを取得できます。たとえば、管理者がリクエストを確認して承認するプロセスを確立します。
改善計画	・事前プロビジョニング緊急アクセス: 信頼されたアカウント（セキュリティチームに使用されるアカウントなど）から緊急アクセス用のロールを事前にプロビジョニングすると、すばやくアクセスを得ることができます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
緊急アクセス実施時のプロセス	・ 緊急アクセス用の AWS クロスアカウントロール、管理者が緊急リクエストの検証と承認を行う際の特定のプロセスなどを要件に応じて整備しているか。	・ 同左

	・ 緊急アクセスは通常時と緊急時の両方において運用上でリスクがあることを踏まえ、適切にプロセスを設計しているか。 ・ 緊急アクセスを実施する際の監査証跡はあるか。	
緊急アクセス用のアカウント	・ 緊急アクセス用のアカウントを AWS アカウント(ルートアカウント)にしていないか。 ・ IAM ポリシーを高権限のプリセットルール(AdministratorAccess など)をそのまま使っていないか。 ・ 通常時に不正利用の有無の検証ができているか。	・ 同左

3.3.4. SEC3-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	アクセス許可を継続的に削減する
内容	チームとワークロードが必要とするアクセスを決定したら、不要になったアクセス許可を削除し、最小権限のアクセス許可を達成するためのレビュープロセスを確立します。未使用の ID とアクセス許可を継続的にモニタリングし、削減します。
改善計画	・IAM Access Analyzer を設定する: AWS IAM Access Analyzer は、組織内のリソースや外部エンティティと共有しているアカウント (Amazon S3 バケットや IAM ロールなど) を特定するのに役立ちます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
継続的なアカウント権限の見直し	・ アクセス権限とアカウントの放置によるリスクの顕在化を防止するため、定期的にアカウント権限の見直しを行	・ AWS IAM のサービスコンソールや IAM Access Analyzer でアカウントの状況を把握し、必要に応じて見直

	っているか。	す。
イベント発生前後でのアカウントの取り扱い	・ アカウントの不正利用を防止するため、退職、異動などのイベントが発生する際に、アクセス権限の削除やアカウントそのものの削除を行なっているか。	・ 同上

3.3.5. SEC3-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	組織のアクセス許可ガードレールを定義する
内容	組織内のすべての ID へのアクセスを制限する共通コントロールを確立します。たとえば、特定の AWS リージョンへのアクセスを制限したり、中央セキュリティチームが使用する IAM ロールなどの一般的なリソースをオペレーターが削除できないようにしたりできます。
改善計画	・すべての ID に適用される共通の制限を定義する: 特定の AWS リージョンへのアクセスに限定するなど、組織固有の要件に基づいて、AWS Organizations を使用して適用できる制限をいくつも作成します。 ・AWS Control Tower を使用してガードレールを管理する: 特定の AWS リージョンへのアクセスに限定するなど、組織固有の要件に基づいて、AWS Organizations を使用して適用できる制限をいくつも作成します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
ガードレールの定義	・ 当該組織におけるガードレールの定義を明文化しているか。 ・ リージョンの法的要件やカントリーリスクを踏まえてアクセス権限を付与する範囲が定義されているか。	・ 同左
ガードレールの設計	・ 定義したアクセス権限の適用範囲と AWS IAM、AWS Organizations、Control Tower がそれぞれ意図した通りにマッピングされているか。	・ 同左

	・ IAM Permissions Boundary によるアクセス境界設定を検討したか。	

3.3.6. SEC3-6

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ライフサイクルに基づいてアクセスを管理する
内容	アクセスコントロールをオペレーター、アプリケーションのライフサイクル、一元化されたフェデレーションプロバイダーと統合します。たとえば、ユーザーが組織を離れるとき、またはロールを変更するときに、ユーザーのアクセス権を削除するとします。
改善計画	・ユーザーアクセスのライフサイクル: 新しいユーザーの参加、職務の変更、退職するユーザーに対するユーザーアクセスライフサイクルポリシーを実装して、現在のユーザーのみがアクセスできるようにします。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
ライフサイクルに関するリスク分析	・ ライフサイクルによるセキュリティリスクを踏まえた上で、ユーザーをコントロールしているか。	・ 従業員に対する辞令の発令による転属や、従業員が退職する際に、適切なアクセス権の付与や削除を行わないことによるリスク評価を行う。
ライフサイクルイベントでの内部不正の防止	・ 退職予定者が退職するまでの間のアクセス権限の極小化や、アカウントの削除を実施しているか。 ・ 証拠保全のためにユーザーの無効化と削除のタイミングをずらしているか。	・ 同左
ライフサイクル管理	・ ライフサイクルイベントへの対応漏れを防止するために、定期的に棚卸しを実施しているか。	・ 同左

3.3.7. SEC3-7

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	パブリックおよびクロスアカウントアクセスの分析
内容	パブリックおよびクロスアカウントアクセスに焦点を当てた結果を継続的にモニタリングします。パブリックアクセスとクロスアカウントアクセスを減らして、このタイプのアクセスを必要とするリソースのみへのアクセスに限定します。
改善計画	・IAM Access Analyzer を設定する: AWS IAM Access Analyzer は、組織内のリソースや外部エンティティと共有しているアカウント (Amazon S3 バケットや IAM ロールなど) を特定するのに役立ちます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
意図しないパブリックアクセスのコントロール	・ 意図しないパブリックアクセスの許可による、情報漏洩の可能性を認識するとともに、対策を講じているか。 ・ IAM Access Analyzer を「誰が」「いつ」実施するかを定義しているか。	・ S3 のサービスコンソールや 3rd party ツールを使用し、意図せず公開しているバケットの有無を確認する。 ・ IAM Access Analyzer を利用してアカウントを特定する。

3.3.8. SEC3-8

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	リソースを安全に共有する
内容	アカウント間または AWS 組織内の共有リソースの消費を管理します。共有リソースをモニタリングし、共有リソースへのアクセスを確認します
改善計画	・AWS Resource Access Manager を使用する: AWS Resource Access Manager (RAM) は、AWS リソースを任意の AWS アカウント間または AWS 組織内で簡単かつ安全に共有できるサービスです。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
リソース共有のコントロール	・ リソースの共有はリスクが発生することを認識した上で実施しているか。 ・ 共有範囲を最小限にした上で成文化しているか。	・ AWS Resource Access Manager によるリソースの可視化と共有を実施する。

3.4. SEC4

SEC4 の質問について、AWS では以下が挙げられています。

質問	セキュリティイベントをどのように検出し、調査していますか？

3.4.1. SEC4-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	サービスとアプリケーションのログ記録を設定する
内容	アプリケーションログ、リソースログ、AWS のサービスログを含め、ワークロード全体でログ記録を設定します。例えば、組織内のすべてのアカウントで AWS CloudTrail、Amazon CloudWatch Logs、Amazon GuardDuty、AWS Security Hub が有効になっていることを確認します。
改善計画	・1.AWS のサービスのログ記録を有効にする:要求事項を遵守するため AWS のサービスのログ記録を有効にします。ログ記録機能には、VPC フローログ、ELB ログ、S3 バケットログ、CloudFront アクセスログ、Route 53 クエリログ、Amazon RDS ログを含みます。 ・2.オペレーティングシステムとアプリケーション固有のログ機能を評価して有効にする: オペレーティングシステムとアプリケーションごとのログ機能を評価して有効にし、不審な動作を検出します。 ・3.ログに適切なコントロールを適用する:ログには機密情報が含まれている場合があるため、承認されたユーザーにのみログへのアクセス権を与えるようにします。S3 バケットと CloudWatch Logs のロググループに対するアクセス権を制限することを検討します。 ・4.Amazon GuardDuty を設定する: Amazon GuardDuty は脅威検出サービスです。悪意のある動作や不正な動作を継続的に検索し、AWS のアカウントとワークロードを保護できるようにします。GuardDuty を有効にし、ラボを使用して E メールの自動アラートを設定します。 ・5.CloudTrail でカスタマイズされた証跡を設定する:証跡を設定するとデフォルトの期間よりも長くログを保存し、後で分析できます。 ・6.AWS Config を有効にする:AWS Config は、AWS アカウントの AWS リソースの設定を詳細に表示します。このビューには、リソース間の関係と設定の履歴が含まれるため、時間の経過とともに設定と関係がどのように変わるかを確認できます。Lab:Automated Deployment of Detective Controls ・8.AWS Security Hub を有効にする:AWS Security Hub では、AWS のセキュリティ状態の包括的なビューが提供され、セキュリティ業界の標準とベストプラクティスへの準拠を確認するのに役立ちます。Security Hub は、AWS アカウント、サービス、およびサポートされているサードパーティーのパートナー製品からセキュリティデータを収集し、セキュリティの傾向を分析し、最も優先度の高いセキュリティ問題を特定するのに役立ちます。

SEC4-1 では、Cloud(AWS)へのアクセス、アクティビティの把握および、インシデント発生時に即座に調査が行えるように各情報を収集・整理することが重要であると定義されており、この目的を達成するためには、以下の検討も必要になると考えている。

SEC4-1：追加検討要素

検討項目	検討の視点	行動例
調査・分析要件の検討	・ どのようなケースを想定した調査を行うかを	・ 利用環境の把握 ・ 想定リスクの分析

	整理し、必要な情報の特定から収集方法の検討を実施しているか。	・ 分析対象・目的の決定 ・ 調査要件の整理 ・ 情報収集方法の検討 ・ 情報集約要否の検討
調査・分析対象とする情報の正規化	・ 複数の情報を利用して調査を行う場合は、横断調査が行えるように情報の正規化を行っているか。	・ 同左
資産・リソース情報の収集	・ 問題が発生したアセット（インスタンス）やユーザーを特定できるように資産情報を分析に利用できるようにしているか。	・ 集めるべき資産情報の精査
外部情報の活用	・ 内外通信の不審性を確認するために脅威インテリジェンス等外部情報の活用を検討しているか。	・ 必要とする脅威情報の特性の理解 ・ 入手先の検討 ・ ・運用方法の検討

3.4.2. SEC4-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ログ、結果、メトリクスを一元的に分析する
内容	異常や不正なアクティビティの兆候を検出するため、すべてのログ、メトリクス、テレメトリーを一元的に収集し、自動的に分析する必要があります。ダッシュボードを使用すると、リアルタイムの状態に関する洞察に簡単にアクセスできます。例えば、Amazon GuardDuty と Security Hub のログがアラートと分析のためにあるロケーションに一元的に送信されるようにします。
改善計画	・1.ログ処理機能を評価する:ログの処理に使用できるオプションを評価する ・2.CloudTrail ログの分析の最初の作業として Amazon Athena をテストする ・3.AWS での集中ロギングを実装する:複数のソースからのログ記録を一元化する AWS のサンプルソリューション。 ・4.パートナーで集中ロギングを実装する:APN パートナーは、ログを一元的に分析するためのソリューションを提供しています。

SEC4-2 では、特性の異なる情報を横断的に分析調査できるようにし、アクセスイベントの総合的評価を行えるようにすることを重要としている。また、期待する結果を得るための情報の整理や分析方法の検討が前提として必要になると考える。

SEC4-2：追加検討要素

検討項目	検討の視点	行動例
調査・分析要件の検討	・ SEC4-1 と同じ	・ SEC4-1 と同じ
調査・分析対象とする情報の正規化	・ SEC4-1 と同じ	・ SEC4-1 と同じ
集約方法の検討	・ ログをどこにどのように集めるか検討しているか。	・ 一元管理の方法の検討 ・ 保管期間の確認 ・ 一元管理時のビューや検索方法の確認 ・ ログの収集方法の確認
出力結果の確認	・ 結果がどのような形式で確認できるか。 ・ 結果を受けてどのような対応がとり得るかを事前に検討しているか。	・ ソリューションの仕様確認 ・ 結果および内容の確認方法の検討 ・ 期待する結果に対する想定行動の検討
運用ワークフローの検討	・ 迅速な調査を行うため、「A が発見された場合に B を調査する」といったワークフローを整理しているか。 ・ ※手順化ではない	・ 運用体制の確保 ・ 運用者の役割決定 ・ 運用方法の決定

3.4.3. SEC4-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	イベントへの応答を自動化する
内容	自動化を使用してイベントを調査および修正することで、人為的な労力やエラーが軽減され、調査機能をスケールできます。定期的なレビューは、自動化ツールを調整するのに役立ちます。継続して繰り返し行います。例えば、最初の調査ステップを自動化して Amazon GuardDuty イベントへの応答を自動化し、同様の作業を繰り返して、人間の労力を徐々に排除します。
改善計画	・Amazon GuardDuty で自動アラートを実装する: Amazon GuardDuty は脅威検出サービスです。悪意のある動作や不正な動作を継続的にモニタリングし、AWS のアカウントとワークロードを保護できるようにします。GuardDuty を有効にし、自動アラートを設定します。 ・調査プロセスを自動化する: 時間を節約するため、イベントを調査して情報を管理者に報告する自動化されたプロセスを開発します。

SEC4-3 では、アラート（インシデント）発生時の対処をどのように行うべきか、如何にして迅速に行うか、その対応の必要性について記されている。

一口に自動化といってもどのように自動化するか、自動化することでどのような問題が

解決するかなどシステムに頼り切ったものではなく事前の計画が必要と考えられる。

SEC4-3：追加検討要素

検討項目	検討の視点	行動例
自動化実現に向けた計画	・ 自組織内のサービス特性やセキュリティ運用を理解し、自動化可能な対応と不可能な対応を整理しているか。	・ どのような運用（ワークフロー）を自動化すべきか検討する。 ・ 実現の可能性を検討する ・ 自動化メリットを検討
自動化に向けたインシデントレスポンス計画	・ 業務影響を考慮して自動化可能なインシデントレスポンスを計画する。	・ 自動化後の運用ワークフローを整理する。

3.4.4. SEC4-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	実用的なセキュリティイベントを実装する
内容	チームに送信され、チームによるアクションが可能なアラートを作成します。チームがアクションを実行するための関連情報がアラートに含まれていることを確認します。例えば、Amazon GuardDuty と AWS Security Hub のアラートが、アクションを実行するためにチームに送信されたり、オートメーションフレームワークからのメッセージによってチームが通知される状態を保ちつつ、レスポンスオートメーションツールに送信されたりするようにします。
改善計画	・AWS のサービスで利用可能なメトリクスを検出する: 使用しているサービスについて CloudWatch を通じて利用できるメトリクスを確認します。 ・Amazon CloudWatch アラームを設定します: 。

SEC4-4 では、必要なアラート（セキュリティイベント）を設定し、チーム内で共有すると記されている。このアラートについて理想とする内容は意味のある情報を取得できることであると考える。アラートの量が多いと運用コストの増加や取りこぼしに繋がるため、ノイズとなる情報は極力減らすことが重要である。

SEC4-4：追加検討要素

検討項目	検討の視点	行動例
分析要件の検討	・ どのような事象を確認すべきか、分析要件を事前に検討する。	・ リスク分析 ・ 分析の目的決定 ・ 分析環境の理解 ・ 収集する情報の決定
インシデントレスポンス計画	・ インシデントレスポンスに必要な情報を精査する。	・ どのような情報を元にIRを行うか検討

運用改善	・ 意味のあるセキュリティイベントを発見するためのアラート等を設定後も継続的に結果の見直しを行い、精度を高めるための取り組みを検討する。	・ 定期的な運用見直し ・ KPI の設定

3.5. SEC5

SEC5 の質問について、AWS では以下が挙げられています。

質問	ネットワークリソースをどのように保護しますか?

3.5.1. SEC5-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ネットワークレイヤーを作成する
内容	到達可能性要件をレイヤーに共有するコンポーネントをグループ化します。たとえば、インターネットアクセスを必要としない VPC 内のデータベースクラスターは、インターネットへのルート、またはインターネットからのルートがないサブネットに配置する必要があります。VPC を使用せずに稼働するサーバーレスワークロードでは、マイクロサービスを使用した同様の階層化とセグメント化でも同じ目標を達成できます。
改善計画	・VPC にサブネットを作成する: (複数のアベイラビリティーゾーンを含むグループで) 各レイヤーのサブネットを作成し、ルートテーブルを関連付けてルーティングを制御します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
攻撃可能領域の極小化	・ マイクロセグメンテーションによる適切な区画の設計により、攻撃可能領域の極小化と影響範囲の最小化を図っているか。	・ ネットワーク概要図、アーキテクチャ図、システム設計書などを確認する。
ネットワーク設計	・ セグメント単位でワークロードを定義し、適切にワークロードを分離しているか。 ・ パブリックサブネットの利用を最小限、もしくは全てをプライベー	・ 同上

	トサブネットにしているか。 ・ VPC 外と VPC 内のサービスを、要件に応じて適切に使い分けているか。	

3.5.2. SEC5-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	すべてのレイヤーでトラフィックをコントロールする
内容	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の両方について、多層防御アプローチでコントロールを適用します。たとえば、Amazon Virtual Private Cloud (VPC) の場合、これにはセキュリティグループ、ネットワーク ACL、サブネットが含まれます。AWS Lambda の場合は、VPC ベースのコントロールを使用してプライベート VPC で実行することを検討してください。
改善計画	・VPC 内のネットワークトラフィックを制御する: VPC ベストプラクティスを実装してトラフィックを制御する ・エッジでのトラフィックを制御する: Amazon CloudFront などのエッジサービスを実装して、追加の保護レイヤーやその他の機能を提供します。 ・プライベートネットワークトラフィックを制御する: ワークロードのプライベートトラフィックを保護するサービスを実装します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
ネットワークレイヤーに応じたセキュリティ設計	・ 仮想ファイアウォールにおいて、セキュリティグループとネットワーク ACL とで、ステートフルとステートレスの違いがあることを理解した上で使い分けているか。 ・ 要件に応じて、仮想ファイアウォール以外にネットワークファイアウォールや WAF を実装しているか。	・ ネットワーク概要図、アーキテクチャ図、システム設計書などを確認する。 ・ 当該システムを OSI 参照モデルに照らし合わせ、アタックベクターに対応したレイヤーのファイアウォールを実装する。(例:Web アプリケーション通信であれば WAF を実装する。)
ロケーションの特性を活かしたアーキテクチャ	・ エッジロケーション、リージョン、AZ でのそれぞれのトラフィック	・ 同上

	と、要件に応じたセキュリティ設計ができているか。 ・ 静的 Web サイトを運営する場合、オリジンを秘匿しているか。	

3.5.3. SEC5-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ネットワーク保護を自動化する
内容	保護メカニズムを自動化し、脅威インテリジェンスと異常検出に基づく自己防御型ネットワークを提供します。たとえば、現在の脅威にプロアクティブに適応し、その影響を軽減できる侵入検知および防止ツールなどです。
改善計画	・ウェブベースのトラフィックの保護を自動化する: AWS では、AWS CloudFormation を使用して、一般的なウェブベースの攻撃をフィルタリングするために設計された AWS WAF ルールセットを自動的にデプロイするソリューションを提供しています。ユーザーは、AWS WAF ウェブアクセスコントロールリスト (ウェブ ACL) に含まれるルールを定義する事前設定された保護機能から選択できます。 ・APN パートナーソリューションを検討する: APN パートナーは、オンプレミス環境の既存のコントロールと同等、同一、またはそれらと統合される、業界をリードする多くの製品を提供しています。これらの製品は既存の AWS サービスを補完します。包括的なセキュリティアーキテクチャーをデプロイして、クラウド環境およびオンプレミス環境全体にさらにシームレスなエクスペリエンスを得ることができます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
アプリケーション層での防御	・ 要件に応じて WAF をネイティブサービスか 3rd パーティ製品かを選択しているか。 ・ ネイティブサービスを利用する場合、どのロケーション(エッジ、パブリック)で動作させるかを検討の上で選択しているか。	・ ネイティブサービスを利用する場合、AWS WAF(マネージドルールを含む) を実装する。
ネットワーク層での防御	・ 要件に応じて IDS/IPS などをネイティブサービスか 3rd パーティ製品かを検討の上で選択しているか。	・ ネイティブサービスを利用する場合、AWS Network Firewall を実装する。

ネットワークの自動遮断、自動隔離	・ セキュリティ侵害が発生する場合の被害拡大抑止を想定しているか。	・ ラテラルムーブメントによる攻撃の拡大を抑止するため、ネットワークの自動遮断を実装する。

3.5.4. SEC5-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	検査および保護を実装する
内容	各レイヤーでトラフィックを検査し、フィルタリングします。たとえば、ウェブアプリケーションファイアウォールを使用して、アプリケーションネットワークレイヤーでの意図しないアクセスから保護します。Lambda 関数の場合、サードパーティーのツールは、アプリケーションレイヤーのファイアウォールをランタイム環境に追加できます。
改善計画	・Amazon GuardDuty を設定する: Amazon GuardDuty は脅威検出サービスです。悪意のある動作や不正な動作を継続的にモニタリングし、AWS のアカウントとワークロードを保護できるようにします。GuardDuty を有効にし、自動アラートを設定します。 ・VPC フローログを設定する: VPC フローログは、VPC のネットワークインターフェイス間を行き来する IP トラフィックに関する情報をキャプチャできるようにする機能です。フローログデータは、Amazon CloudWatch Logs および Amazon S3 に公開できます。フローログを作成した後、選択した送信先でデータを取得したり表示したりできます。 ・VPC トラフィックのミラーリングを検討する: トラフィックミラーリングは、Amazon EC2 インスタンスの Elastic Network Interface からネットワークトラフィックをコピーし、コンテンツ検査、脅威のモニタリング、トラブルシューティングのために帯域外セキュリティおよびモニタリングアプライアンスに送信するために使用できる Amazon VPC の機能です。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
不正アクセスのモニタリングと追跡	・ VPC フローログ、CloudWatch(Metrics/Logs)、CloudTrail、Route 53 の利用とモニタリング設計を検討したか。	・ 同左
脅威検出サービス	・ Amazon GuardDuty やサードバーティ製品の利用を検討したか。	・ 同左
S3 のログ記録オプション	・ 「サーバーアクセスログを使用したリクエストのログ記録」、「AWS CloudTrail を使用した Amazon S3 API コールのログ記録サーバーアクセス	・ 同左

	ログ」を要件に応じて利用しているか。	

3.6. SEC6

SEC6 の質問について、AWS では以下が挙げられています。

質問	コンピューティングリソースをどのように保護していますか?

3.6.1. SEC6-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	脆弱性管理を実行する
内容	コード、依存関係、インフラストラクチャ内の脆弱性のスキャンとパッチ適用を頻繁に実施し、新しい脅威から保護します。
改善計画	・Amazon Inspector を設定する: Amazon Inspector は、Amazon EC2 インスタンスのネットワークアクセシビリティと、それらのインスタンスで実行されるアプリケーションのセキュリティ状態をテストします。Amazon Inspector は、アプリケーションの露出、脆弱性、ベストプラクティスからの逸脱を評価します。 ・ソースコードをスキャンする: ライブラリや依存関係をスキャンして脆弱性に対応します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
パッチ管理	・ 脆弱性管理とパッチ管理が異なることを認識しているか。 ・ AWS Systems Manager Patch Manager で OS とアプリケーションの両方にパッチを適応できるが、公開する前にパッチをテストしないことを認識しているか。	・ AWS Systems Manager Patch Manager と AWS IAM、AWS CloudTrail、Amazon EventBridge と連携して、イベント通知や使用状況の監査などを行う。 ・ パッチコンプライアンスレポートを生成する。
脆弱性管理	・ サードパーティーの脆弱性管理ソリューションの要否を検討したか。 ・ 定期的にセキュリティパッチ適応以外の脆弱性の有無を確認してい	・ Amazon Inspector や AWS Trusted Advisor で脆弱性の有無を確認する。

	るか。	
セキュリティテスト	・ セキュリティテストを脆弱性診断、ペネトレーションテスト、レッドチーム演習、TLPT などに分類して特徴を把握しているか。その上で要件に応じて適切な手段を採用しているか。 ・ Amazon Inspector のスキャン対象は限定的であることを認識しているか。(EC2 と ECR)	・ 同左
コードスキャンツール	・ ソースコードの脆弱性をスキャンしているか。	・ ネイティブサービスであれば Amazon CodeGuru Reviewer、OSS であれば SonarQube などを利用する。

3.6.2. SEC6-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	攻撃領域を削減する
内容	オペレーティングシステムを強化し、使用するコンポーネント、ライブラリ、外部から利用可能なサービスを最小限に抑えることで、攻撃対象領域を縮小します。
改善計画	・オペレーティングシステムを強化する: ベストプラクティスを満たすようにオペレーティングシステムを設定します。 ・コンテナ化されたリソースを強化する: セキュリティのベストプラクティスを満たすよう、コンテナ化されたリソースを設定します。 ・AWS Lambda 関数を使用する際のベストプラクティス: AWS Lambda のベストプラクティスを実装する

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
責任共有モデルに基づく攻撃可能領域の把握	・ 責任共有モデルを基に、サービスの抽象度を高くすることでクラウド利用者における責	・ Trusted Advisor による不要なオープンポートの有無などの評価により、攻撃可能領域の削

	任範囲と攻撃可能領域が削減されることを前提とし、要件に応じたサービス選定と、サービスの抽象度に合わせたセキュリティ設計を行っているか。 ・ 利用するサービスの攻撃領域の把握と、実装するセキュリティを定義し、最小権限の原則に基づく設計と設定を行っているか。	減を行う。

3.6.3. SEC6-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	マネージドサービスを活用する
内容	Amazon RDS、AWS Lambda、Amazon ECS などのリソースを管理するサービスを実装し、共有責任モデルの一部としてのセキュリティメンテナンスタスクを減らします。
改善計画	・利用可能なサービスを調べる: Amazon RDS、AWS Lambda、Amazon ECS などのリソースを管理するサービスを調査、テスト、実装します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
マネージドサービス活用による責任範囲の最小化	・ 選定するサービスの抽象度を高くすることでクラウド利用者における責任範囲が縮小することを前提に、抽象度の高いマネージドサービスを選定しているか。 ・ 抽象度と自由度は反比例するため、抽象度の高いサービスにおいては機能の概要レベルではなく、具体的な動作における制限事項やパ	・ 該当するマネージドサービスにおける制限事項や利用可能な機能を確認し、要件が制限事項に該当するかを確認する。

	ラメーターに関しても設計時点で把握しているか。	

3.6.4. SEC6-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	コンピューティング保護を自動化する
内容	脆弱性管理、攻撃対象領域削減、リソース管理などのコンピューティング保護メカニズムを自動化します。
改善計画	・設定管理を自動化する: 設定管理サービスやツールを使うことで、自動的に安全性の高い設定を適用および検証します。 ・EC2 インスタンスのパッチ適用を自動化する: AWS Systems Manager Patch Manager は、セキュリティ関連および他のタイプの更新の両方を使用して、マネージドインスタンスにパッチを適用するプロセスを自動化します。Patch Manager を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用できます。 ・侵入検知と防止ツールを実装する: 侵入検知と防止ツールを実装することで、インスタンス上の悪意のあるアクティビティをモニタリングし、停止できます。 ・APN パートナーソリューションを検討する: APN パートナーは、オンプレミス環境の既存のコントロールと同等、同一、またはそれらと統合される、業界をリードする多くの製品を提供しています。これらの製品は既存の AWS サービスを補完します。包括的なセキュリティアーキテクチャーをデプロイして、クラウド環境およびオンプレミス環境全体にさらにシームレスなエクスペリエンスを得ることができます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
パッチ適応	・ パッチ適応により攻撃可能領域の削減に繋がっていることを認識しているか。 ・ EC2 やオンプレミスのサーバーがある場合、迅速なパッチ適応と管理を行なっているか。	・ AWS Systems Manager Patch Manager を活用してパッチ適応を行う。
防御策の実装	・ 環境に応じて WAF や IDS/IPS(ホスト型、ネットワーク型の両方)といったソリューションを選定しているか。	・ WAF であれば AWS WAF、IDS/IPS であれば AWS Network Firewall を実装する。
セキュリティ侵害時の自動隔離	・ 要件に応じて、セキュリティ侵害時の EC2 インスタンスを自動隔離するといったソリュー	・ 同左

	ションを検討しているか。	

3.6.5. SEC6-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ユーザーが遠距離でアクションを実行できるようにする
内容	インタラクティブアクセスの機能を排除すると、人為的ミスのリスクが軽減され、設定や管理が手動で行われる可能性が低くなります。たとえば、変更管理ワークフローを使用して、Infrastructure as Code によって EC2 インスタンスをデプロイした後、直接アクセスや踏み台ホストを許可する代わりに、ツールを使用して EC2 インスタンスを管理します。
改善計画	・コンソールアクセスを置き換える: インスタンスへのコンソールアクセス (SSH または RDP) を AWS Systems Manager Run Command に置き換えて、管理タスクを自動化します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
IaC(Infrastructure as Code)の導入	・ インフラストラクチャをコードで定義することによって人為的ミスを削減し、有事の際の追跡性を向上させる。	・ AWS CloudFormation や AWS OpsWorks を利用する。
管理タスクのリスク軽減	・ 管理コンソールへのアクセスを必要最小限に留めているか。 ・ 被管理インスタンスには直接アクセスしていないか。 ・ 要件に応じて、予め、有事の際にアクセス権限を付与するフローの策定や、緊急アクセス用のアカウントを準備する。	・ 要件に応じて、踏み台サーバー経由、AWS Systems Manager Session Manager の利用、AWS Systems Manager Run Command の利用を検討する。

3.6.6. SEC6-6

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ソフトウェアの整合性を検証する
内容	ワークロードで使用されるソフトウェア、コード、ライブラリが信頼できるソースからのものであり、改ざんされていないことを検証するメカニズム (コード署名など) を実装します。
改善	・メカニズムを調査する: コード署名は、ソフトウェアの整合性を検証するために使用できるメカニズムの 1

計画	つです。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
コード署名	・ コードに変更がないことや、信頼できる発行元からのコードであることを確認する。	・ AWS Lambda を利用している場合、AWS Signer によるコード署名を行う。
コードレビューの自動化	・ 予めコードレビューを自動化しておき、整合性の検証をする前のコード保守を行う。	・ Amazon CodeGuru Reviewer、Security Detector を活用する。

3.7. SEC7

SEC7 の質問について、AWS では以下が挙げられています。

質問	どのようにデータを分類していますか?

3.7.1. SEC7-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ワークロード内のデータを特定する
内容	これには、データのタイプと分類、関連するビジネスプロセス、データ所有者、該当する法的要件およびコンプライアンス要件、データの保存場所、および結果として実行が必要な統制が含まれます。これには、データが一般公開されることを意図しているかどうか、データが顧客個人識別情報 (PII) などの内部使用のみかどうか、データが知的財産である、法的な秘匿特権がある、機密性が高いと特記されているなど、より制限されたアクセス用であるかどうかを示す分類が含まれます。
改善計画	・Amazon Macie を使用したデータの検出を検討する: Amazon Macie は、個人識別情報 (PII) や知的財産などの機密データを認識します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
法的要件の確認	・ 地域や業界に特化したデータ保存に関する法的要件を確認する。	・ 同左

3.7.2. SEC7-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	データ保護コントロールを定義する
内容	分類レベルに従ってデータを保護します。たとえば、関連するレコメンデーションを使用してパブリックと

	して分類されたデータを保護すると同時に、追加のコントロールで機密データを保護します。
改善計画	・データの識別および分類スキーマを定義する: データの識別と分類は、保存するデータの潜在的な影響とタイプ、およびデータにアクセスできるユーザーを評価するために実行されます。 ・利用可能な AWS のコントロールを確認する: 使用しようとしているか、使用を計画している AWS サービスについて、セキュリティコントロールを確認します。多くのサービスには、ドキュメントにセキュリティセクションがあります ・AWS コンプライアンスリソースを確認する: サポートに役立つ AWS のリソースを確認します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データ配置	・ 機密情報に関するデータ配置の設計を行っているか。	・ 個人情報など機密情報として扱うべきデータは極力分散させないように設計段階で考慮する
リージョン設計	・ データの物理配置場所と法的要件に注意する。	・ 高可用性が求められるシステムにおいては、データ分類に応じて、法的要件を満たしながら可用性を確保可能な複数リージョンにまたがるネットワーク設計を行う。
長期保管データの扱い	・ 業界のコンプライアンスに準じて機密情報の保持期間を設計しているか。 ・ データを暗号化のみではセキュリティコントロールが不十分となるケースがあることを考慮しているか。	・ 同左

3.7.3. SEC7-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	識別および分類を自動化する
内容	データの識別と分類を自動化して、手動操作による人為的ミスのリスクを軽減します。
改善計画	・Amazon S3 インベントリを使用する: Amazon S3 インベントリは、オブジェクトのレプリケーションと暗号化ステータスの監査とレポートに使用できるツールの 1 つです。

・Amazon Macie を検討する: Amazon Macie は、機械学習を使用して Amazon S3 内に保存されているデータを自動的に検出、分類、保護します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データ配置	・ 機密情報に関するデータ配置の設計を行っているか。 ・ 機密情報を過剰に分散して管理不能に陥っていないか。 ・ データ所在地を把握しているか ・ データ所在地に応じたコンプライアンスに対応しているか。	・ 同左

3.7.4. SEC7-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	データのライフサイクル管理を定義する
内容	定義されるライフサイクル戦略は、機密性レベル、また法的および組織の要件に基づいている必要があります。データを保持する期間、データ破壊、データアクセス管理、データ変換、データ共有などの側面を考慮する必要があります。
改善計画	・データタイプを識別する: ワークロードに保存または処理するデータのタイプを特定します。そのデータは、テキスト、イメージ、バイナリデータベースなどです。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データサイクルの定義	・ 各サイクルをコンプライアンスや自組織の要件に合わせて定義しているか。	・ CSA セキュリティガイダンスなどガイドラインになる情報を参考にしながら、自組織に合わせて定義する（生成/保存/利用/共有/アーカイブ/破棄など）

3.8. SEC8

SEC8 の質問について、AWS では以下が挙げられています。

質問	保管時のデータをどのように保護していますか?

3.8.1. SEC8-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	安全なキー管理を実装する
内容	暗号化キーは、AWS KMS などのキー管理サービスを使用するなど、厳格なアクセスコントロールで安全に保存する必要があります。異なるキーを使用し、AWS IAM およびリソースポリシーと組み合わせて、データ分類レベルと分離要件に合わせて、キーに対するアクセスコントロールを検討してください。
改善計画	・AWS Key Management Service (AWS KMS) を実装する: AWS Key Management Service (AWS KMS) では、キーを作成および管理し、さまざまな AWS のサービスおよびアプリケーションで暗号化の使用を制御することを容易にします。AWS KMS は、FIPS 140-2 で検証されたハードウェアセキュリティモジュールを使用してキーを保護する、安全で弾力性のあるサービスです。 ・AWS Encryption SDK を検討する: アプリケーションでクライアント側でのデータ暗号化が必要な場合、AWS KMS が統合された AWS Encryption SDK を使用します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
実装要件の検討	・ どの様なデータ分類レベルがあるのか、分離要件にはどのようなものがあるのか、ケースを想定しながら検討を実施する。	・ データ分類レベルをまとめる。 ・ 分離要件を洗い出す ・ 洗い出したレベル・要件を取りまとめる
実装の選択	・ 実装方法に対しての要件をまとめ整理する。	・ 厳格なアクセスコントロールの選択 ・ 鍵の操作履歴が取得できるものを選択する ・ HSM も対象に含めて検討する。

3.8.2. SEC8-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	保管中に暗号化を適用する
内容	最新の標準やレコメンデーションに基づき、暗号化要件を適用することは、保管中のデータの保護に役立ちます。
改善計画	・Amazon S3 の保管時の暗号化を強制する: S3 バケットのデフォルト暗号化を実装します。 ・AWS Secrets Manager を使用する: AWS Secrets Manager は、機密情報の管理を容易にする AWS のサー

	ビスです。機密情報とは、データベース認証情報、パスワード、サードパーティー API キー、任意のテキストなどです。 ・新しい EBS ボリュームのデフォルトの暗号化を設定する: 新しく作成したすべての EBS ボリュームを暗号化形式で作成することを指定します。AWS が提供するデフォルトキーを使用す>るか、作成したキーを使用するかを選択できます。 ・暗号化された Amazon Machine Image (AMI) を設定する: 暗号化を有効化して既存の AMI をコピーすると、自動的にルートボリュームとスナップショットが暗号化されます。 ・Amazon RDS の暗号化を設定する: 暗号化オプションを有効化して、保管中の Amazon RDS DB クラスターとスナップショットに対して暗号化を設定します。 ・追加の AWS のサービスで暗号化を設定する: 使用する AWS のサービスについて、暗号化機能を特定します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データ保護の選択	・ データ保護に対して要件をまとめ整理しているか。	・ データの暗号化の要／不要を洗い出す。 ・ 暗号化実施による速度等パフォーマンスへの影響を確認する。
障害発生時の確認作業	・ データ保護機構でインシデントが発生する場合に検討すべき事項を整理する。	・ 暗号化鍵漏洩時に鍵を変更した再度暗号化が可能か確認する。 ・ アルゴリズム危殆化時にアルゴリズムを変更した再暗号化が出来るか否かを確認する。

3.8.3. SEC8-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	保管時のデータの保護を自動化する
内容	自動化ツールを使用して保管中のデータの保護を継続的に検証し、提供します。たとえば、すべてのストレージリソースが暗号化されていることを確認します。
改善計画	・すべての EBS ボリューム が AWS Config Rules を使用して暗号化されていることの検証を自動化できます。AWS Security Hub は、セキュリティ標準に対する自動チェック機能を通じて、さまざまな制御を検証することもできます。さらに AWS Config Rules は、自動的に 非準拠のリソースを修復できます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データ保護の確認	定期的にデータが適切に保護されているかを確認す	・データの暗号化の定期的な確認方法を調べておく

	る。	・データに不整合が生じていないかの定期的な確認方法を調べておく ・使用されている暗号化アルゴリズムの一覧を定期的に確認できるようなツールを使用する
障害時復旧方法の確認	データ保護機構にてなんらかの障害（鍵の漏えい等を含む）が発生した場合に検討しなくてはならない箇所をまとめ整理する。	・障害時にデータ復旧を行う際の手順を確認する

3.8.4. SEC8-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	アクセスコントロールを適用する
内容	最低限の権限によるアクセスコントロールや、バックアップ、分離、バージョニングなどのメカニズムを適用することは、保管中のデータの保護に役立ちます。オペレーターがデータへのパブリックアクセスを許可しないようにします。
改善計画	・アクセスコントロールを適用する: 暗号キーへのアクセスを含め、最小権限を用いたアクセスコントロールを適用します。 ・さまざまな分類レベルに基づいてデータを分離する: AWS Organizations によって管理されるデータ分類レベルには、さまざまな AWS アカウントを使用します。 ・AWS KMS ポリシーを確認する: AWS KMS ポリシーで付与されるアクセスのレベルを確認します。 ・S3 バケットおよびオブジェクトに対するアクセス許可を確認する: Amazon S3 バケットのポリシーで付与されるアクセスのレベルを定期的に確認します。ベストプラクティスは、バケットを公開で読み取りまたは書き込み可能にしないことです。AWS Config を使用して公開されているバケットを検出し、Amazon CloudFront を使用して Amazon S3 からコンテンツを提供することを検討します。 ・Amazon S3 バージョニングとオブジェクトロックを有効にする ・Amazon S3 インベントリを使用する: Amazon S3 インベントリ Amazon S3 インベントリは、オブジェクトのレプリケーションと暗号化ステータスの監査とレポートに使用できるツールの 1 つです。 ・Amazon EBS と AMI の共有アクセス許可を確認する: 共有アクセス許可は、イメージとボリュームをワークロード外の AWS アカウントに共有することを可能にします。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
アクセスコントロールの監査方法の検討	・ 定期的にアクセスコントロールが適切に行われているかの監査方法を検討しているか。	・ 権限の侵害および変更等がなかったかどうかを定期的に検査する監査方法を検討しておく。

		・ アカウントの作成時、権限の変更時などで成功した操作のログ・レポートが出力できるような監査方法を確認する。 ・ 共有アクセス許可などの、アクセス許可を与えているボリュームやAWS アカウントを確認する方法を考慮する。

3.8.5. SEC8-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	人をデータから遠ざけるメカニズムを使用する
内容	通常の運用状況で、すべてのユーザーが機密データおよびシステムに直接アクセスできないようにします。たとえば、クエリを実行するデータストアに直接アクセスする代わりにダッシュボードを提供します。CI/CD パイプラインを使用しない場合は、通常無効になっている特権アクセスメカニズムを適切に提供するために必要な制御とプロセスを決定します。
改善計画	・人をデータから遠ざけるメカニズムを実装する: メカニズムには、Amazon QuickSight などのダッシュボードを使用して、直接クエリを実行する代わりにユーザーにデータを表示することが含まれます。 ・設定管理を自動化する: 設定管理サービスまたはツールを使用して、リモートでアクションを実行し、安全な設定を自動的に適用および検証します。踏み台ホストを使用したり、EC2 インスタンスに直接アクセスしたりすることを回避します。 ・通常の運用状況で、すべてのユーザーが機密データおよびシステムに直接アクセスできないようにします。たとえば、変更管理ワークフローを使用して、直接アクセスや踏み台ホストを許可する代わりに、ツールを使用して EC2 インスタンスを管理します。これは、タスクを実行する手順を含むオートメショントドキュメントを使用する AWS Systems Manager Automation を通じて 達成できます 。これらのドキュメントはソース管理に保存し、実行前にピアレビューを行い、シェルアクセスと比較してリスクを最小限に抑えるために徹底的にテストできます。ビジネスユーザーは、データストアに直接アクセスする代わりにダッシュボードを使用し、クエリを実行できます。CI/CD パイプラインを使用しない場合は、通常無効になっている特権アクセスメカニズムを適切に提供するために必要な制御とプロセスを決定します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
アクセス方法の限定化	・ 通常の運用状況では機密データやシステムに直接アクセスできないようにし、ユーザーからのデータ入力の入口	・ 機密データやシステムにアクセスする必要のある操作を予め確認しておく。 ・ 必要なアクセス権を予め

	を限定しているか。	全て洗い出しておく。 ・ 通常時はダッシュボード等でのみアクセスが可能なようにユーザーのアクセス権を限定する。 ・ ダッシュボード使用時にも、アクセスしたアカウントや時間等が操作ログに残るようにする。 ・ 機密データやシステムにアクセスする必要がある場合には、抑止方法を考慮に入れた手順を作成しておく。 ・ 機密データやシステムにアクセスする場合には、アクセスしたユーザーや時間等が操作の許可／不許可を問わずログに残るようにする。

3.9. SEC9

SEC9 の質問について、AWS では以下が挙げられています。

質問	転送時のデータをどのように保護していますか?

3.9.1. SEC9-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	安全な鍵および証明書管理を実装する
内容	AWS Certificate Manager (ACM) などの証明書管理サービスを使用するなど、厳格なアクセスコントロールを適用して、暗号化キーと証明書を安全に保管し、適切な時間間隔でローテーションします。
改善計画	・安全な鍵および証明書管理を実装する: 定義された安全なキーおよび証明書管理ソリューションを実装します。 ・安全なプロトコルを実装する: 認証と機密性を提供する安全なプロトコル (Transport Layer Security (TLS) や IPsec など) を使用し、データの改ざんや損失のリスクを軽減します。使用しているサービスに関連するプロトコルとセキュリティについては、AWS ドキュメントを参照してください。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例

暗号化方法の選択	・ それぞれの箇所で必要とする暗号化の要件と実装方法をまとめ整理しているか。	・ 鍵及び証明書のローテーション間隔を検討し、実装時にその間隔が選択できることを確認する。 ・ システム上の構成要素で必要とする暗号化の実装方法を簡潔に整理する。 ・ 鍵や証明書の利用場所を明瞭に管理する。
障害時の確認	・ データ保護機構にてなんらかの障害（鍵の漏えい等を含む）が発生した場合に検討しなくてはならない箇所をまとめ整理する。	・ 暗号化鍵や証明書が漏洩時に対応すべき箇所を確認する。 ・ アルゴリズム危殆化時にアルゴリズムを変更した場合の影響を確認する。

3.9.2. SEC9-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	伝送中に暗号化を適用する
内容	組織的、法的、コンプライアンスの要件を満たすために、適切な基準とレコメンデーションに基づいて定義された暗号化要件を適用します。
改善計画	・伝送中に暗号化を適用する: 定義された暗号化要件は、最新の標準とベストプラクティスに基づいて、安全なプロトコルのみを許可するものである必要があります。たとえば、Application Load Balancer または EC2 インスタンスには、HTTPS プロトコルを許可するセキュリティグループのみを設定します。 ・エッジサービスで安全なプロトコルを設定する: Amazon CloudFront と必要な暗号で HTTPS を設定します。 ・外部接続に VPN を使用する: ポイントツーポイント接続やネットワーク間接続を IPsec VPN で保護し、データのプライバシーと整合性の両方を提供することを検討してください。 ・ロードバランサーで安全なプロトコルを設定する: ロードバランサーへの接続を保護するために、HTTPS リスナーを有効にします。 ・インスタンスで安全なプロトコルを設定する: インスタンスで HTTPS 暗号化を設定することを検討します。 ・Amazon Relational Database Service (Amazon RDS) で安全なプロトコルを設定する: SSL/TLS を使用してデータベースインスタンスへの接続を暗号化します。 ・Amazon Redshift で安全なプロトコルを設定する: SSL/TLS 接続を必須とするようにクラスターを設定します。 ・その他の AWS のサービスで安全なプロトコルを設定する: 使用する AWS のサービスについて、転送中の暗号化機能を特定します。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
暗号化方法の選択	・ SEC9-1 と同じ	・ SEC9-1 と同じ
障害時の確認	・ SEC9-1 と同じ	・ SEC9-1 と同じ

3.9.3. SEC9-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	意図しないデータアクセスの検出を自動化する
内容	GuardDuty などのツールを使用して、データ分類レベルに基づいて定義された境界の外部にデータを移動する攻撃 (DNS プロトコルを使用して不明または信頼されないネットワークにデータをコピーするトロイの馬など) を自動検知します。
改善計画	・意図しないデータアクセスの検出を自動化する: ツールまたは検出メカニズムを使用し、定義された境界の外側にデータを移動する試みを自動的に検出します。たとえば、認識されていないホストにデータをコピーしているデータベースシステムを検出します。 ・Amazon Macie を検討する: Amazon Macie では、データアクセスアクティビティの異常が継続的にモニタリングされ、不正アクセスの危険や不注意によるデータ漏えいが検出された場合には詳細なアラートが生成されます。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
データ境界の決定	データ分類レベルに基づいてデータ境界を確定する。	データ分類に基づいた境界を決定する。
不正アクセスモニタリングの決定	不正アクセス検出等のモニタリングの詳細を決定する。	・不正アクセスを検出した場合にアラートの通知方法、例えばメールや SNS、Slack 等での通知方法と通知先を決定する。 ・アノマリー検知を使用する場合には、異常時に通常時との差異の詳細が通知されるようにしておく。 ・不正アクセス検出後の処理フローにおいて、一次対応の範囲とエスカレーションルールを整備する。

3.9.4. SEC9-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ネットワーク通信を認証する
内容	Transport Layer Security (TLS) や IPsec など、認証をサポートするプロトコルを使用して、通信の ID を検証します。
改善計画	・安全なプロトコルを実装する: 認証と機密性を提供する安全なプロトコル (Transport Layer Security (TLS) や IPsec など) を使用し、データの改ざんや損失のリスクを軽減します。使用しているサービスに関連するプロトコルとセキュリティについては、AWS ドキュメントを参照してください。

CSA では、更に以下の評価ポイントを挙げます。

検討項目	検討の視点	行動例
暗号化方法の選択	・ SEC9-1 と同じ	・ SEC9-1 と同じ
障害時の確認	・ SEC9-1 と同じ	・ SEC9-1 と同じ

3.10. SEC10

SEC10 の質問について、AWS では以下が挙げられています。

質問	インシデントの予測、対応、復旧はどのように行いますか?

3.10.1. SEC10-1

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	重要な人員と外部リソースを特定する
内容	組織がインシデントに対応するのに役立てるため、社内外の担当者、リソース、法的義務を特定します。
改善計画	・組織内の主要な人員を特定する: インシデント対応と復旧に必要な組織内の人員の連絡先リストを保持します。 ・外部パートナーを特定する: 必要に応じて、インシデント対応と復旧を支援できる外部パートナーと連携します

SEC10-1 では、インシデント対応に関わる組織（人々）の確認、それぞれの役割を定義することが重要と定義されている。また人員配置に関しても IR プロセスが円滑に行えるような考慮を行う必要がある。(適切な人、適切な人数、適切な体制を考える)

本 WG では当検討項目を一段掘り下げて検討してみる。

SEC10-1：追加検討要素

検討項目	検討の視点	行動例
関係者間の連携方法の確認	・ 有事の際のコミュニケーションやエスカレーションの方法を確認しているか。	・ 各チーム（組織）の窓口を設定する。 ・ 窓口への連絡方法を確認する。(日中/夜間) ・ ・各チーム（組織）内の役割を明確にする。

定期的なトレーニング	・ 定期的にインシデント対応の演習・訓練を実施しているか。 ※ 参加者は実際に対応を行うものに限らず、インシデント対応に関係する人すべてを対象に検討することが望ましい。	・ 自組織のリスクに対応したシナリオの検討を行い、机上/実地訓練を計画する。 ・ 関係各所とのコミュニケーション計画を計画する。
外部組織との連携	・ 調査や対応において、自組織内に対応リソースがない場合外部組織との連携を検討する	・ ・自組織内で対応できない内容を検討し、必要に応じた外部支援を検討する。

3.10.2. SEC10-2

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	インシデント管理計画を作成する
内容	インシデントへの応答、インシデント時の伝達、インシデントからの復旧に役立つ計画を作成します。たとえば、ワークロードと組織にとって起こる可能性が最も高いシナリオで、インシデント応答計画を作成してみましょう。内部および外部に伝達およびエスカレーションする方法を含めます。
改善計画	・利用可能なリソースを確認する: AWS および業界のリソースを使用できます。 ・インシデント対応プレイブックを策定する: わかりやすいプレイブックには、インシデントに対応して復旧するための手順が詳しく記述されている必要があります。 ・エスカレーションおよびコミュニケーション計画を策定する: エスカレーションおよびコミュニケーションには、インシデント中の各ステージで連絡する必要がある組織内の人員と外部関係者が含まれている必要があります。 ・外部広報計画を策定する: インシデントに関する情報をリリースするための広報計画を策定します

SEC10-2 では、SEC10-1 と同様の内容でありインシデント発生時に以下に迅速に行動できるかに焦点を当てている。

体制面の検討に加え、事前準備としてどこまで対応できるか次第で、インシデント発生時に迅速にことを運べるかが決まってくる。

SEC10-2：追加検討要素

検討項目	検討の視点	行動例
記録の管理	・ 発生事象や記録の管理が行えるように準備しているか。	・ チケット管理システム等や対応記録システムを準備して運用方法を決定する。
KPI の設定	・ 以下のインシデント対応にお	・ 設定した KPI のチェックを行

	ける KPI を検討しているか。 ➢ サービスデスクで解決された割合（初回解決） ➢ 解決までの平均経過時間 ➢ インシデント処理の平均コスト ➢ 総インシデント数に対する暫定対応の割合 ➢ 合意済みの期間内に解決したインシデントの割合 ➢ 重大なインシデントの数と割合	い、運用改善検討を定期的に行う。

3.10.3. SEC10-3

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	フォレンジック機能を備える
内容	外部のスペシャリスト、ツール、オートメーションなど、適切なフォレンジック調査能力を特定し、準備します。
改善計画	・フォレンジック機能を確認する: 組織のフォレンジック調査機能、利用可能なツール、外部スペシャリストを調査します。

インシデント発生時に侵害の痕跡等、詳細調査が求められるケースがあるため、フォレンジック調査が行えるように事前準備しておくことが重要

SEC10-3：追加検討要素

検討項目	検討の視点	行動例
専門業者との連携	・ 有事の際に即座に調査が行えるように専門業者（外部機関）との連携を検討しているか。 ・ 迅速にインシデントレスポンスを行うために、データの受け渡し方法を整理しているか。	・ 同左
証跡の保管	・ フォレンジック調査を行う上での証跡（ログ）の保管方法を検討	・ 例 ➢ 保管場所：S3 ➢ アクセス権：セキュリ

	しているか。	ティチーム、フォレンジックベンダーのみがアクセス可能な領域 ➢ 保管期間：1 年間
想定される調査の検討	・ 当該システムがフォレンジック調査を実施するか検討し、必要である場合に適切な方法を選択しているか。 ・ 適切な製品やサービスを検討しているか。	・ 以下を整理し、要件に応じて実施の要否を決定する。 ➢ コンピュータフォレンジック ➢ モバイルデバイスフォレンジック ➢ ネットワークフォレンジック

3.10.4. SEC10-4

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	封じ込め機能を自動化する
内容	インシデントの封じ込めおよび復旧を自動化し、対応時間を短縮するとともに組織的影響を軽減します。
改善計画	・封じ込め機能を自動化する

インシデント対応の重要なファクターとして、如何に迅速に被害を極小化できるかが挙げられる。その手段の一つとしてレスポンスのオートメーション化を行うことが被害の極小化につながる場合がある。ただしオートメーション化は現状正しく運用フローが整備されていることが条件となるため、自組織でどのような方法が適切かを理解して検討する必要がある。

SEC10-4：追加検討要素

検討項目	検討の視点	行動例
レスポンス自動化の範囲の検討	・ 自動化には様々な方法があることを認識し、自組織に最適な方法を選択しているか。 ・ インシデント発生時、どのように対応しているかを精査し、運用フローの再確認を行い、自動化の検討を行っているか。	・ 要件に応じて次の防止措置を採用する。 ➢ 通信遮断 ➢ 悪意あるプロセス・サービスの停止 ➢ 論理抜線/論理隔離 ➢ パッチ適応 ➢ 侵害されたインスタンスの自動リビルド（ロール

		バック）

3.10.5. SEC10-5

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	アクセスを事前プロビジョニングする
内容	インシデント応答者が AWS に事前プロビジョニングされた正しいアクセス権を持っていることを確認しておき、調査から復旧までの時間を短縮します。
改善計画	・アクセスを事前プロビジョニングする: セキュリティ担当者がインシデントに適切に対応できるように、セキュリティ担当者に AWS への適切なアクセス権が事前に設定されていることを確認します。

運用においては職務分掌の考え方は重要となるが、これはインシデント対応でも同じである。対応時に役割に応じた権限がない場合、対応の遅れへとつながる場合があるため、適切な人に適切な権限を与えられるように事前にアクセス権等の設定は適切に行っておく必要がある。

SEC10-5：追加検討要素

検討項目	検討の視点	行動例
職務分掌によるコントロール	・ 部門ないし個人のそれぞれが担当する仕事の内容や権限、責任の範囲を簡潔・明確に定義しているか。	・ 同左
アカウントにおけるアクセス権の整備	・ 利用システムに対して、インシデントレスポンダーに必要な権限を精査し、適切に付与しているか。	・ 同左

3.10.6. SEC10-6

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ツールを事前デプロイする
内容	復旧までの調査時間を短縮できるように、セキュリティ担当者は適切なツールを AWS に事前にデプロイしておきます。
改善計画	・ツールを事前デプロイする: セキュリティ担当者がインシデントに適切に対応できるように、セキュリティ担当者に適切なツールが AWS で事前デプロイされていることを確認します。 ・リソースのタグ付けを実施する: インシデント時にリソースを特定できるように、調査対象のリソースのコードなどの情報をリソースにタグ付けします。

インシデント対応において、必要と考えられるツールを事前に準備し、またまた影響のあるリソースを即座に特定できるようにする。

SEC10-6：追加検討要素

検討項目	検討の視点	行動例
運用ワークフローの整備	・ インシデントレスポンスにおけるプロセスのワークフローを定義し、必要なツールを事前に準備しているか。	・ インシデント対応において、誰がどのような手段で何をするか、想定する事象は何かをシミュレーションし、必要なツール類を整備する。
分析要件の検討	・ SEC4-1 と同様	・ 同左
資産・リソース情報の収集	・ SEC4-1 と同様	・ 同左
外部情報の活用	・ SEC4-1 と同様	・ 同左
調査・分析対象とする情報の正規化を行う	・ SEC4-1 と同様	・ 同左

3.10.7. SEC10-7

評価、内容、改善計画について、AWS では以下が挙げられています。

評価	ゲームデーを実施する
内容	インシデント対応ゲームデー（シミュレーション）で定期的に訓練し、そこで得られた教訓をインシデント管理計画に組み込み、継続的に改善します。
改善計画	・ゲームデーを実施する: さまざまな脅威について、インシデント対応イベントのシミュレーション（ゲームデー）を実施します。このゲームデーには、主要なスタッフや管理者を参加させてください。 ・教訓から学ぶ: ゲームデーの実行から得られた教訓は、プロセスを改善するためのフィードバックに含まれている必要があります。

事前にインシデント対応訓練を実施し、いざという時に迅速に動けるようにすることが重要である。

SEC10-7：追加検討要素

検討項目	検討の視点	行動例
定期的なトレーニング	・ SEC10-1 と同じ	・ 同左
演習・訓練の振り返り	・ 演習・訓練のフィードバックを受け、対応計画を練る。必要に応じてセキュリティ施策の input としても活用することが望ましい。	・ 演習・訓練における課題の抽出が重要となるため、参加者で振り返りの機会を設け、見直しに向けた

		計画を検討する。
外部演習等の検討	・ 自組織内では難しい演習・訓練（複雑な環境を準備した高度な訓練）は外部演習などに参加する。	・ セキュリティ企業が開催している講義やサイバー演習を活用する。

4. 参考・引用文献

AWS Well-Architected Framework

- https://docs.aws.amazon.com/ja_jp/wellarchitected/latest/framework/welcome.html