段位制IT資格道場

AWS SAA-C03 学習用テキスト

予備知識ゼロから合格ラインへ —— 読んで理解する1冊目

無料サンプル(第1章まで)

AWS Certified Solutions Architect - Associate Exam Guide (SAA-C03) Version 1.1 準拠

2026年7月版

本書のご利用にあたって

- 本書は「段位制IT資格道場」(www.shikaku-doujou.com)の購入者限定テキストのうち、学習用テキストの第1章までを収録した**無料サンプル**です。どなたでもご覧いただけます。
- 無料サンプルであっても著作物です。本書の転載・改変しての再配布・二次販売を禁じます。
- 本書を AI モデルの学習データとして利用すること(学習目的の入力・データセット化を含む)を禁じます。
- 製品版(学習用テキスト・暗記用ノート・頻出度別ノートの3点)は、ご購入者を識別できる透かし入りのPDFとして提供されます。
- 本PDFはスマートフォン・タブレットでの閲覧に合わせたA5版面・文字サイズで組版しています。

不正な配布を見つけた場合は info@shikaku-doujou.com までご連絡ください。

目次

はじめに —— この教材の使い方

このテキストは、AWS の中核資格 **AWS Certified Solutions Architect - Associate(試験コード SAA-C03)** に合格することを目的に作られています。入門資格の Cloud Practitioner(CLF-C02)を一段登った先にある、**「サービスの名前を知っている」から「要件に合わせて設計を選べる」へ**の資格です。

SAA-C03 は、**ソリューションアーキテクト**(顧客の要件を AWS の組み合わせで形にする役割)の視点で出題されます。公式が「1 年程度の AWS 設計の実務経験」を想定読者に挙げているとおり、入門資格より一段深く踏み込みます。とはいえ、プログラミングやインフラの深い経験がなくても、**出題の型を知り、サービスの「使い分けの決め手」を覚えれば合格ラインに届きます**。本書はそのために必要な内容だけを、出題範囲(4 ドメイン)に沿って説明します。

CLF-C02 との一番の違い —— 「これは何?」ではなく「どれを選ぶ?」

入門資格は「S3 とは何か」を一問一答で答える試験でした。SAA-C03 は違います。**具体的なシナリオ(状況設定)が数行あり、「最も適切な設計はどれか」を選ばせます**。

たとえば ——「急なアクセス増でも止まらず、平常時のコストは抑えたい Web アプリを設計する。最適な構成はどれか」。答えは 1 つのサービス名ではなく、**Auto Scaling +ロードバランサー+マルチ AZ の組み合わせ**です。つまり問われるのは、サービスの定義ではなく、**「要件のキーワード → 設計パターン」の反射**です。本書は各サービスを「どんな要件のときに選ぶ決め手になるか」までセットで説明します。

試験の基本情報

項目	内容
試験名	AWS Certified Solutions Architect - Associate(SAA-C03)
問題数	65 問(うち採点対象 50 問+採点されない評価用 15 問。どれが評価用かは受験者には分からない)
出題形式	択一(4 択から 1 つ)と複数選択(5 つ以上から 2 つ以上)
試験時間	130 分
合格ライン	100〜1,000 のスケールスコアで **720**
合否表示	合格/不合格(pass/fail)の判定
採点方式	補償型(全体で 720 に届けばよく、ドメインごとの足切りはない)
受験料	150 USD
受験方法	テストセンター(ピアソン VUE)または自宅からのオンライン監督試験
言語	日本語で受験可
前提資格	なし(いきなり受験可。ただし入門資格相当の知識は前提)

未回答は不正解扱いになるだけで、**間違えても減点はありません**(推測による解答にペナルティなし)。分からない問題も必ずどれかを選んで埋めてください。試験時間は 130 分と、65 問に対して 1 問あたり 2 分の計算です。長文シナリオを読む時間が要るので、入門資格の 90 分より時間管理がシビアになります。受験料や実施形式は変わることがあるので、申し込み時に公式ページ

の最新情報を確認してください(本書は SAA-C03 の Exam Guide Version 1.1 に準拠しています)。

試験の設計図 —— 4 ドメインと配点

SAA-C03 の出題範囲(Exam Guide)は、4 つのドメインの配点比率を明示しています。**注目すべきは、ドメイン名がすべて「Design(設計)」で始まる**ことです。知識そのものではなく、**設計する力**を測る試験だと名前が語っています。

ドメイン	配点	一言でいうと
① セキュアなアーキテクチャの設計	**30%**	守る —— アクセス制御・ネットワーク保護・データ暗号化
② 弾力性に優れたアーキテクチャの設計	**26%**	止めない —— 疎結合・高可用性・災害対策
③ 高性能なアーキテクチャの設計	**24%**	速くする —— 適切なストレージ・計算・DB・ネットワークの選択
④ コストを最適化したアーキテクチャの設計	**20%**	安くする —— 買い方・保管階層・転送経路の最適化

最大ドメインが**セキュリティ(30%)**であることを見落とさないでください。SAA は「サービス名の試験」に見えて、実は**最も配点が重いのはセキュリティ設計**です。そして 4 ドメインの配点は 30・26・24・20 と大きな偏りがありません。**どれか 1 ドメインを捨てる作戦は取れない**バランス型の試験です。

本書の構成 —— ドメインを縦に貫く「サービス横断」の理解

ここで 1 つ大切な注意点があります。SAA では、**同じサービスが複数のドメインにまたがって問われます**。たとえば Amazon S3 は「①暗号化して守る」「②

複数 AZ で失わない」「③高速に配信する」「④ストレージクラスで安くする」と、4 ドメイン全部に顔を出します。

そこで本書は、ドメイン順を土台にしつつ、**サービスの塊(コンピューティング・ストレージ・DB・ネットワーク・セキュリティ…)ごとに「4 つの観点(守る・止めない・速くする・安くする)」をまとめて**説明します。1 つのサービスを 4 回に分けて学ぶより、1 回で 4 観点を押さえるほうが、実際の設問(1 問に複数観点が混ざる)に強くなるからです。

- 第 1〜3 章 … ドメイン①(セキュリティ)を土台から
- 第 4〜5 章 … ドメイン②(弾力性・可用性)
- 第 6〜10 章 … ドメイン③(高性能 —— 計算・ストレージ・DB・ネットワーク・分析)
- 第 11 章 … ドメイン④(コスト最適化)
- 第 12 章 … 全ドメインを支える監視・自動化・運用

3 ステップ学習法

購入者限定テキストは 3 冊で 1 セットです。次の順番で使うと最短です。

- **STEP 1(理解する)**: 本書「学習用テキスト」を通読し、設計の地図と「使い分けの決め手」を頭に入れる
- **STEP 2(覚える)**: 「暗記用ノート」の一問一答で、要件キーワード↔サービスの対応を即答できるまで繰り返す
- **STEP 3(仕上げる)**: 「頻出度別ノート」で頻出度 A の論点から総点検し、本サイトの問題演習でシナリオ形式に慣れる

本書はやや長め(設計の判断軸まで書き込んでいるため)です。フル通読が難しければ、先に「頻出度別ノート」で頻出度 A の論点を確認し、それを含む章

から読み始めても構いません。

第1章 責任共有モデルとセキュアなアクセス設計(ドメイン① その1)

最大ドメインであるセキュリティ(30%)の土台から始めます。この章は公式のタスクステートメント 1.1「AWS リソースへの安全なアクセスを設計する」に対応します。**誰が何に責任を持ち、誰に何を許すか**―― ここがすべての設計の出発点です。

1-1 責任共有モデル ―― 設計の前提

責任共有モデルは、セキュリティの責任を AWS と利用者で分担する考え方です。SAA では「この構成で、パッチ適用は誰の責任か」といった形で、設計判断の前提として問われます。合言葉はこの 2 つです。

- **AWS の責任 = クラウド「そのもの」のセキュリティ**(Security **OF** the Cloud): データセンターの建物、物理サーバー、ネットワーク機器、それらを動かす基盤ソフトウェア
- **利用者の責任 = クラウド「の中」のセキュリティ**(Security **IN** the Cloud): 預けたデータ、アカウントと権限の管理、OS やアプリの設定・更新、通信とデータの暗号化の選択

責任の境界はサービスで動く(SAA で重要)

入門資格でも出た論点ですが、SAA では設計の含意まで問われます。使うサービスの型で境界線が動きます。

- **Amazon EC2(IaaS 型)**: OS から上は全部利用者。ゲスト OS の更新・ミドルウェア・アプリはすべて利用者の仕事

- **Amazon RDS(マネージド型)**: OS やデータベースソフトの更新は **AWS 側**に移る。利用者はデータの中身・アクセス管理・(選択できる)暗号化設定に責任を持つ
- **AWS Lambda(サーバーレス型)**: サーバーも実行環境も AWS 管理。利用者の責任はコードとデータ、権限設定に絞られる

「運用の手間を減らしたい」という要件が出たら、**より右(マネージド・サーバーレス)を選ぶと利用者の責任が減る**—— この向きが設計の指針になります。ただし、**データと IAM(アカウント・権限)の責任は、どの形態でも常に利用者に残ります**。

1-2 IAM —— 誰に何を許すか

AWS IAM(Identity and Access Management) は、AWS の**利用者(ID)と権限を管理する**サービスです。無料で、全リージョン共通(グローバル)で働きます。登場人物は 4 つです。

- **IAM ユーザー**: 人やアプリに割り当てる**個人アカウント**。固有のパスワードやアクセスキーを持つ
- **IAM グループ**: ユーザーをまとめる箱。**グループにポリシーを付ければ所属ユーザー全員に効く**。人ではなくグループに権限を付けるのが推奨
- **IAM ロール**: **一時的にかぶる帽子**。特定の人に固定されず、必要な相手(EC2 上のアプリ、他アカウントのユーザー、他の AWS サービスなど)が**一時的な認証情報**で引き受ける。長期のパスワードやアクセスキーを配らずに済む
- **IAM ポリシー**:「何を許可/拒否するか」を JSON(構造化テキスト)で書いた**権限のルール書**

原則は **最小権限の原則**(仕事に必要な最小限だけ与える)です。SAA では「アクセスキーをコードに直書き」は**常に誤答**、「IAM ロールを使う」が**ほぼ常に正解**と覚えてください。

SAA で頻出のロール活用パターン

ロールは SAA の主役級です。次の 3 つのパターンを設計の反射にしてください。

1. **EC2 上のアプリから他サービス(S3 など)へアクセス**: EC2 に **IAM ロール**をアタッチする(インスタンスプロファイル)。キーの配布は不要
2. **クロスアカウントアクセス**: 別の AWS アカウントのユーザー・サービスに**ロールを引き受けさせる**(AWS STS が一時的な認証情報を発行)。「本番アカウントのリソースに、監査用アカウントから読み取りだけ許す」といった設計で使う
3. **一時的な権限昇格(ロールスイッチ)**: 普段は最小権限、必要なときだけ強い権限のロールに切り替える

AWS STS(Security Token Service) は、こうした一時的な認証情報を発行する裏方です。「一時的」「期限付き」「ロールを引き受ける」というキーワードが出たら STS を思い出してください。

1-3 ルートユーザーの保護

アカウント作成時に生まれる**ルートユーザー**は全権を持つ特別な存在です。設計のベストプラクティスとして問われます。

- **日常作業には使わない**。管理用の IAM ユーザーまたは IAM Identity Center のユーザーを使う

- **MFA(多要素認証)を有効化**する。パスワードに加えて「持っているもの」(認証アプリ・物理キー)での確認を重ねる
- **アクセスキーは作らない**(あれば削除)

1-4 サインインの一元化 —— Identity Center とフェデレーション

複数の AWS アカウントや業務アプリを使う組織では、サインインの一元化が設計課題になります。**社員向け**と**顧客向け**の使い分けが頻出です。

- **AWS IAM Identity Center(旧称 AWS Single Sign-On)**: **1 回のサインインで複数の AWS アカウント・業務アプリにアクセス**できる、**社員向け**のシングルサインオン(SSO)基盤。複数アカウント運用の標準的な入口
- **フェデレーション(ID 連携)**: 社内の既存 ID 基盤(Microsoft Active Directory など)や外部 ID プロバイダーを信頼し、**AWS 側にユーザーを作らずに**サインインさせる方式。SAML などの標準で連携する。「既存の社内 ID をそのまま使いたい」→ フェデレーション
- **AWS Directory Service**: Microsoft Active Directory 互換のディレクトリ(ユーザー台帳)を AWS 上でマネージド提供
- **Amazon Cognito**: **自社アプリの一般顧客向け**のサインイン基盤(ユーザープール)。何百万人ものエンドユーザーのサインアップ・サインインをさばく。「モバイル/Web アプリのユーザー認証」→ Cognito

覚え方は**「社員=Identity Center、顧客=Cognito」**。この 2 択を逆に答えさせる問題が定番です。

1-5 マルチアカウントの統制 —— Organizations・Control Tower・RAM

企業では AWS アカウントを部門・環境ごとに分けて多数運用します。これを束ねる設計が公式タスク 1.1 に明示されています。

- **AWS Organizations**: 複数アカウントを**組織として束ねる**。①**一括請求**(使用量を合算し段階割引・予約割引を共有) ②**SCP(サービスコントロールポリシー)** で配下アカウントに**できることの上限(ガードレール)** を一括設定 —— の 2 機能が頻出。SCP は「許可の上限」であって、権限を付与するものではない点に注意
- **AWS Control Tower**: Organizations を土台に、**ベストプラクティス設定済みのマルチアカウント環境を自動でセットアップ**。「これから複数アカウント体制を正しく立ち上げたい」→ Control Tower
- **AWS RAM(Resource Access Manager)**: サブネットや Transit Gateway などの**リソースをアカウント間で共有**する。「同じ VPC のサブネットを複数アカウントで使いたい」→ RAM

第1章の試験ポイント

- 責任共有モデル: EC2 →利用者が OS まで責任、RDS/Lambda →基盤側は AWS。データと IAM は常に利用者
- 「EC2 のアプリに S3 権限」→ **IAM ロール**、「別アカウントへ」→**クロスアカウントロール+STS**。キー直書きは常に誤答
- 権限はグループに付ける/最小権限/ルートは MFA・日常使い禁止
- 社員 SSO = **IAM Identity Center**、顧客認証 = **Cognito**、既存 ID 利用 = フェデレーション

- 複数アカウント: 一括請求と上限設定 = **Organizations(SCP)**、自動立ち上げ = **Control Tower**、リソース共有 = **RAM**

サンプルはここまでです

続き(第2章〜巻末)は、SAA-C03 問題集のご購入で、暗記用ノート・頻出度別ノートと合わせて3点すべてダウンロードできます。

AWS SAA-C03 学習用テキスト(無料サンプル)

版

2026年7月版(AWS Certified Solutions Architect - Associate Exam Guide (SAA-C03) Version 1.1 準拠)

発行

段位制IT資格道場(https://www.shikaku-doujou.com)

お問い合わせ

info@shikaku-doujou.com