aws partner network | competency

AWS 小売コンピテンシー
テクノロジーパートナー検証チェックリスト

2019 年 12 月
バージョン 1.0

目次

はじめに

AWS コンピテンシープログラムの目標は、専門的なソリューション分野で習熟した技術と顧客を成功に導いた実績を持つ AWS パートナーネットワークパートナー (「APN パートナー」) を認定することにあります。コンピテンシーパートナー審査チェックリスト (「チェックリスト」) は、AWS コンピテンシーへの申し込みを希望する APN パートナーを対象としています。このチェックリストでは、AWS コンピテンシープログラムの認定基準を示しています。APN パートナーは特定のコンピテンシーに申請する際に、その能力の審査を受けることになります。AWS は、この審査を円滑に行うために社内の専門家と外部企業を活用します。AWS はこのドキュメントを随時変更する権利を有します。

当事者に求められること

APN パートナーは、前提条件をすべて満たしている場合であっても、AWS コンピテンシープログラムへの申し込む前にこのドキュメントを熟読する必要があります。このドキュメントについて不明点がある場合や詳しい説明が必要な場合は、まず AWS パートナー開発担当者 (「PDR」) または AWS パートナー開発マネージャー (「PDM」) に問い合わせてください。さらにサポートが必要な場合は、PDR/PDM がプログラム事務局に連絡します。

APN パートナーはプログラムの申込書を提出する準備が整ったら、このドキュメントの以下に記載されているチェックリストの「パートナー自己診断」表に必要事項を記入する必要があります。

申込書の送信方法

1. APN パートナーセントラル (https://partnercentral.awspartner.com/) にアライアンスリードとしてログインします。
2. ページの左側で [View My APN Account] を選択します。
3. [Program Details] セクションまでスクロールします。
4. 申し込みたいと考えている AWS コンピテンシーの横にある [Update] を選択します。
5. プログラム申込書に必要事項を入力して [Submit] をクリックします。
6. 必要事項を入力した自己評価を E メールで competency-checklist@amazon.com に送信します。
    - 自己診断には次の内容を含める必要があります。
        - ソリューションのカテゴリ (カスタマーエンゲージメント、企業商品と計画、サプライチェーンと流通、実店舗とデジタルストアおよび仮想ストア、高度な小売データサイエンス、およびコアとなる小売ビジネスアプリケーション)
        - デプロイのタイプ (SaaS、または顧客が AWS にデプロイ)
        - AWS の導入事例のドキュメント (下記の定義を参照)

上記の手順に関して質問がある場合は、PDR/PDM にお問い合わせください。
AWS は、可能な限り 5 営業日以内に審査スケジュールの開始や追加情報のリクエストを行い、質問があればあわせて回答します。

APN パートナーは、チェックリストを読み、チェックリストを使用して自己評価を実施し、審査日に審査員に示す客観的な証拠資料を集めて整理し、審査に備えてください。

AWS では、APN パートナーが審査時に要件について詳しく述べることのできる担当者を決めておくことをお勧めします。APN パートナーにとっては、審査には高度な技術を持つ AWS 認定エンジニア/設計者を 1 名以上、運用およびサポート機能の責任者である運用担当者、概要説明を行う事業開発エグゼクティブを指名し同席できるようにしておくことがベストプラクティスです。APN パートナーは、審査のスケジュールを設定する前に、客観的な証拠資料やデモンストレーションに含まれるすべての情報が審査員に (AWS かサードパーティーであるかにかかわらず) 共有されることに対し、確実に同意する必要があります。

AWS 小売コンピテンシープログラム

AWS 小売コンピテンシーパートナーは、カスタマーエンゲージメント、企業商品と計画、サプライチェーンと流通、実店舗とデジタルストアおよび仮想ストア、高度な小売データサイエンス、およびコアとなる小売ビジネスアプリケーションにまたがるソリューションを小売業に提供します。

小売コンピテンシーカテゴリ

APN パートナーは、以下のうち自社ソリューションが合致するセグメントカテゴリも明らかにする必要があります。

- **カスタマーエンゲージメント:** ロイヤルティ、ソーシャルチャネル管理、顧客関係管理 (CRM)、コールセンター、広告 (デジタルおよびダイレクトメール)、小売マーケティングリーダーが購入前と購入後の顧客をプロアクティブに魅了し、維持することを可能にする SEO および視聴者エンゲージメントソリューション。

- **企業商品と計画:** 商品化計画、補充、品揃え計画、プラノグラム/スペースプランニング、プロモーションと価格設定の最適化、カテゴリ管理、企業の商品化計画および計画チームが活用するベンダーコラボレーションソリューション。

- **サプライチェーンと流通:** ウェアハウス管理システム (WMS)、エンタープライズリソース計画 (ERP)、ウェアハウスオートメーション、輸入/輸出、運輸、およびロジスティクスをカバーするサプライチェーンと流通ソリューション。

- **実店舗とデジタルストアおよび仮想ストア:** POS、注文管理システム (OMS)、ユニファイドコマース、e コマース、ラストマイルデリバリー、バウンドネス (摩擦のない) ストアエクスペリエンス、デジタルイノベーション (AR/VR、ESL、IoT、Beacons、Voice、Recognition、Digital Kiosk、Smart Mirrors、インタラクティブディスプレイ)、デジタルアセット管理 (DAM)、および決済をカバーするオンラインまたはオフラインショッピングエクスペリエンスに変革をもたらすソリューション。

- **高度な小売データサイエンス:** 小売データレイク、運用効率と顧客インサイトおよびカスタマーエンゲージメントを向上させる AI/ML、分析ソリューション。

- **コアとなる小売ビジネスアプリケーション:** C-Suite、財務、調達、人事、従業員管理、法務、および IT 向けの、コアとなる小売エンタープライズソリューション。

APN パートナーは、以下のうち自社ソリューションが合致するデリバリーカテゴリも明らかにする必要があります。

1. **SaaS:** 共有 AWS インフラストラクチャから複数の顧客にサービスを提供する。すべての AWS アカウントは APN パートナーによって管理される。

2. **顧客デプロイ型:** 顧客の AWS 環境にデプロイされる。すべての AWS アカウントは顧客によって管理される。

AWS 小売コンピテンシープログラムの前提条件

以下の項目が AWS コンピテンシープログラムマネージャーによって検証されます。情報が不足しているか不完全な場合、技術検証レビューのスケジューリングに先立って対処する必要があります。

1.0 APN プログラムメンバーシップ		適合の有無
1.1 テクノロジーパートナー階層	APN パートナーは、小売コンピテンシープログラムに申し込む前に、プログラムのガイドラインと定義を読む必要があります。プログラムの詳細はここをクリック	
1.2 テクノロジーパートナー階層	APN パートナーは、AWS 小売コンピテンシープログラムへの参加を申し込む時点で、アドバンスト階層の APN テクノロジーパートナーである必要があります。	
1.3 ソリューションカテゴリ	APN パートナーは自社ソリューションのセグメントカテゴリを明らかにします。 □ **カスタマーエンゲージメント** □ **企業商品と計画** □ **サプライチェーンと流通** □ **実店舗とデジタルストアおよび仮想ストア** □ **高度な小売データサイエンス** □ **コアとなる小売ビジネスアプリケーション** APN パートナーは自社ソリューションのデリバリーカテゴリを明らかにします。 □ **SaaS** □ **顧客デプロイ型**	
1.4 顧客の導入状況	APN パートナーは、自社のソリューションを利用している顧客の総数を記述します。	
2.0 導入事例		**適合の有無**
2.1 小売特有の導入事例	APN パートナーは、レビュー対象の小売ソリューションに固有に対応した 4 件の導入事例を用意しなければなりません。4 件の導入事例はそれぞれ、6 つのセグメントカテゴリ (カスタマーエンゲージメント、企業商品と計画、サプライチェーンと流通、実店舗とデジタルストアおよび仮想ストア、高度な小売データサイエンス、およびコアとなる小売ビジネスアプリケーション) のいずれかで使用される APN パートナーソリューションの例に関連する必要があります。 AWS デジタルカスタマーエクスペリエンス (DCX)、データ & 分析、IoT、移行、機械学習コンピテンシーを保有する APN パートナーは、小売業界に固有の独自のセグメントドメイン知識を与える、業界特有の課題とコンサルティング業務に高度にターゲットを絞ったソリューションを提供するプロジェクトに対して、お客様の導入事例を最大 4 つまで再利用できます。 導入事例ごとに、APN パートナーは以下の情報を提出する必要があります。 ▪ 顧客の名前 ▪ 顧客のウェブサイト ▪ 顧客の課題 ▪ 課題に対処するためにソリューションをデプロイした方法 ▪ 使用したサードパーティ製のアプリケーションまたはソリューション ▪ リファレンスが実稼働した日付 ▪ 成果や結果 ▪ 特定のアーキテクチャ図、デプロイガイド、その他の資料 (ソリューションの種類により異なる。次のセクションで説明)	

	この情報は、APN パートナーセントラルのプログラム申し込みプロセスで必要になります。この導入事例に付随する情報は非公開として提供することができ、その場合は公開されることはありません。 提出された 4 件の導入事例はすべて、技術検証のドキュメントレビューで審査されます。チェックリストの各項目について導入事例を評価するために必要なドキュメントを APN パートナーが提出できない場合、またはチェックリスト項目のいずれかに適合していなかった場合、その導入事例はコンピテンシーの検討対象から除外されます。 導入事例は、過去 18 か月以内に実施されたデプロイを説明するものであり、「パイロット」や PoC (概念実証) ではなく顧客の本番プロジェクトである必要があります。	
2.2 公開導入事例	公開導入事例は、コンピテンシーへの組み入れが承認されると AWS によって使用されます。その使用目的は、ソリューションの測定可能な KPI に基づいてパートナーの成功実績を紹介すること、また、顧客の目的を達成するソリューションを開発して提供するために必要な経験と知識が APN パートナーにあることの根拠を顧客に提示することです。 APN パートナーは、導入事例と関連付ける 4 件の顧客デプロイのうち 2 件を、公開導入事例とする必要があります。公開導入事例は、公式な導入事例、ホワイトペーパー、ブログ記事のいずれかの形式でなければなりません。	
	APN パートナーのホームページに公開導入事例へのナビゲーションの設定をしたり、公開導入事例へのリンクをアプリケーションに組み込んだりするなど、公開導入事例は APN パートナーのウェブサイトから簡単に閲覧できる必要があります。	
	公開導入事例には、以下を含める必要があります。 ▪ 顧客名、APN パートナー名、AWS が言及されていること ▪ 顧客の課題 ▪ 課題に対処するためにソリューションをデプロイした方法 ▪ ソリューションの一部として AWS サービスをどのように使用したか ▪ 成果や結果	
3.0 AWS 小売ウェブプレゼンスとソートリーダーシップ		**適合の有無**
3.1 APN パートナーの AWS ランディングページ	APN パートナーは、AWS 小売ソリューション固有のインターネットプレゼンスによって、自社の能力と経験についての根拠を顧客に提示します。 APN パートナーは AWS ランディングページを設置し、AWS 小売ソリューションの説明、公開導入事例へのリンク、テクノロジーパートナーシップの一覧を掲載する必要があります。また、小売業に関連した APN パートナーの専門知識を裏付け、AWS との連携を示すその他の関連情報を提供する必要があります。 この AWS 向けの小売ページは、APN パートナーのホームページからアクセスできる必要があります。APN パートナーが小売テクノロジーに特化した会社であり、小売を専門に扱っていることがホームページに反映されている場合に限り、ホームページそのものが AWS ランディングページとして認められます。	
3.2 小売に関するソートリーダーシップ	AWS 小売コンピテンシーパートナーは、AWS のサービスを活用する革新的なソリューションをこれまでに開発しており、小売分野において深い専門知識を持っていると見なされます。	

	APN パートナーは、小売における重点的な取り組みと専門知識を示す資料 (ブログ投稿、プレス記事、動画など) を一般公開する必要があります。過去 12 か月以内に公開した資料例へのリンクを提供する必要があります。	
4.0 ビジネス要件		
4.1 営業用ツールキット	APN パートナーは、営業担当者がすぐに使えるドキュメンテーションおよび販促ツールキットを用意しなければなりません。これには、AWS 日本担当チームの組織に説明できる明確な製品バリュープロポジション (価値提案) と、顧客のセールスチャンスへの適合性を判断するために必要なすべての関連情報 (販促資料、プレゼンテーション、顧客ユースケースなど) が含まれます。 エビデンスは、プレゼンテーション、1 ページの要約資料、導入事例チェックリストを含む販促資料の形態でなければなりません。	
4.2 製品サポート/ ヘルプデスク	APN パートナーはウェブチャット、電話、またはメールで顧客に製品サポートを提供します。 エビデンスは、製品またはソリューションについて顧客に提供するサポートを説明したものでなければなりません。	
4.3 AWS Marketplace に製品を掲載	APN パートナーは AWS Marketplace でソリューションを提供します。 □ はい □ いいえ 「はい」の場合、APN パートナーは AWS Marketplace の当該ページへのリンクを提供しなければなりません。「いいえ」の場合、これ以降の情報は不要です。	
4.4 共同 AWS ディールに対する販売報酬	APN パートナーには、共同 AWS 案件での販売に関する販売報酬プランがあります。 □ はい □ いいえ □ 理由説明：_____ 証拠は APN パートナーに対する報酬プランの簡潔な説明の形式で示す必要があります。	
4.5 共同 AWS/ APN パートナー成功事例	APN パートナーには共同成功事例を記録し公表するプロセスがあります。 証拠は、口頭説明の形で示す必要があります。	
5.0 APN パートナー自己診断		**適合の有無**
5.1 AWS コンピテンシーパートナープログラム検証チェックリストの自己診断	APN パートナーは、AWS 小売テクノロジーパートナー検証チェックリストの要件への準拠について、自己診断を実施する必要があります。 ▪ APN パートナーは、チェックリストのすべてのセクションに記入する必要があります。 ▪ 自己評価に必要事項を記入したら、件名を「[APN パートナー名], Retail Competency Technology Partner Completed Self-Assessment」とし、**competency-checklist@amazon.com** に E メールで送信します。 ▪ 必要事項を記入した自己診断は、AWS に提出する前に、パートナーソリューションアーキテクト、パートナー開発担当者 (PDR)、またはパートナー開発マネージャー (PDM) に確認してもらうことをお勧めします。この目的は、APN パートナーの AWS チームがプロセスに関与し、審査に先立ってアドバイスを提供し、審査のプロセスを生産的なものにすることにあります。	

小売コンピテンシーテクノロジーパートナー検証チェックリスト

次の項目がサードパーティー審査員と AWS パートナーソリューションアーキテクトのどちらかまたは両方によって検証されます。情報が不足しているか不完全な場合、技術検証レビューのスケジューリングに進む前に対処する必要があります。

		申込先:		
技術検証		SaaS	顧客による AWS へのデプロイ	適合 はい/ いいえ
アーキテクチャ図	デプロイカテゴリによっては、1 枚以上のアーキテクチャ図が必須です。 各アーキテクチャ図は次のものを示していなければなりません。 □ アーキテクチャの主な要素と、それらの組み合わせによってパートナーソリューションを顧客に提供する方法 □ 使用するすべての AWS のサービス。適切な AWS サービスのアイコンを使用すること。 □ AWS のサービスのデプロイ方法。Amazon Virtual Private Cloud (VPC)、アベイラビリティーゾーン (AZ)、サブネット、AWS の外部システムへの接続など。 □ オンプレミスコンポーネントやハードウェアデバイスなど、AWS の外部でデプロイされる要素を含める。	はい – ソリューション全体で 1 つ、各導入事例ごとに 1 つずつ。	はい – 各導入事例ごとに 1 つずつ。	
デプロイガイド	デプロイガイドでは、パートナーソリューションを AWS にデプロイするためのベストプラクティスを提供し、デプロイガイドの基本要件に記載されているすべてのセクションを含めなければなりません。	いいえ	はい – ソリューションに 1 冊	
完了した検証チェックリスト	パートナーソリューションに対して提供する 4 つの導入事例ごとに、APN パートナーは次のチェックリストの完成版を提出して、どのチェックリスト項目が満たされているかを示さなければなりません。	はい	はい	
1.0 セキュリティ **セキュリティの柱では、情報とシステムを保護することに焦点を当てます。重要なトピックには、データの機密性と整合性、誰が何を実行できるかを権限管理によって特定および管理すること、システムの保護、セキュリティイベントを検出するための統制の確立があります。**				
1.1 AWS アカウントの root ユーザーを日常的なアクティビティに使用していない	AWS アカウントの root ユーザーは日常的なアクティビティに使用しない。AWS アカウントの作成後、すぐに AWS Identity and Access Management (IAM) ユーザーアカウントを作成し、すべての日常的なアクティビティにはこれらの IAM ユーザーアカウントを使用する必要があります。IAM ユーザーアカウントを作成したら、AWS のルートアカウントの認証情報を安全な場所に保存し、AWS アカウントのルートユーザーの権限が必要な一部のアカウントおよびサービス管理タスクの実行のみに、その認証情報を使用してください。日常的に使用する IAM ユーザーアカウントおよびグループのセットアップ方法については、「最初の IAM 管理者のユーザーおよびグループの作成」を参照してください。	はい	いいえ	
1.2 AWS アカウントの root ユーザーに対して Multi-Factor Authentication (MFA) が有効になっている	AWS アカウントの root ユーザーに対して Multi-Factor Authentication (MFA) を有効にする必要があります。AWS アカウントの root ユーザーは AWS アカウントで機密性の高い操作を実行できるため、新たな認証レイヤーを追加するとアカウントのセキュリティ強化に役立ちます。仮想 MFA やハードウェア MFA など、複数の種類の MFA が利用可能です。	はい	いいえ	

1.3 すべての日常的なアクティビティに IAM ユーザーアカウントを使用している	AWS アカウントの root ユーザーは、root 権限が不要なタスクに使用してはなりません。代わりに、管理者アクセスが必要な担当者ごとに新しい IAM ユーザーを作成します。次に、このユーザーを管理者グループに配置し、管理者アクセスマネージドポリシーを付与することで、ユーザーを管理者に設定できます。その後、管理者グループのユーザーは、AWS アカウントのグループ、ユーザーなどを設定できるようになります。これ以降の対話操作はすべて、root ユーザーではなく AWS アカウントのユーザーとそのユーザー自身のキーを使用して行う必要があります。ただし、一部のアカウントおよびサービス管理タスクを実行するには、root ユーザーの認証情報を使用してログインしなければなりません。	はい	いいえ	
1.4 すべてのインタラクティブ IAM ユーザーに対して Multi-Factor Authentication (MFA) が有効になっている	すべてのインタラクティブ IAM ユーザーに対して MFA を有効化しなければなりません。MFA では、一意の認証コード (ワンタイムパスワード: OTP) を生成するデバイスをユーザーが所持します。ユーザーは通常の認証情報 (ユーザー名とパスワード) および OTP の両方を入力しなければなりません。MFA デバイスは、特別製のハードウェアのほか、(スマートフォンで実行できるアプリのような) 仮想デバイスでも構いません。	はい	いいえ	
1.5 IAM 認証情報を定期的に更新している	パスワードおよびアクセスキーを定期的に変更するとともに、アカウント内のすべての IAM ユーザーにも変更を促さなければなりません。そうすることにより、知らない間にパスワードまたはアクセスキーが漏れた場合でも、その認証情報を使ってリソースにアクセスされる期間を制限できます。パスワードポリシーをアカウントに適用することで、すべての IAM ユーザーにパスワードの変更を要求できます。また、ユーザーに要求するパスワードの変更頻度を選択することもできます。IAM ユーザーのアクセスキーの更新については、「アクセスキーの更新」を参照してください。	はい	いいえ	
1.6 強力なパスワードポリシーを IAM ユーザーに適用している	IAM ユーザーに対して強力なパスワードポリシーを構成しなければなりません。ユーザーが各自のパスワードを変更できるようにする場合は、強力なパスワードを作成しそのパスワードを定期的に変更するようユーザーに要求します。IAM コンソールの [Account Settings] ページから、アカウントのパスワードポリシーを作成できます。パスワードポリシーを使用して、最小文字数、アルファベット以外の文字が必要かどうか、義務付ける変更頻度など、パスワードの要件を定義できます。詳細については、「IAM ユーザー用のアカウントパスワードポリシーの設定」を参照してください。	はい	いいえ	
1.7 IAM 認証情報を複数のユーザーで共有していない	AWS アカウントにアクセスする必要があるすべての担当者に対して、個別の IAM ユーザーアカウントを作成しなければなりません。自分自身にも IAM ユーザーを作成してそのユーザーに管理者特権を付与し、その IAM ユーザーをすべての作業で使用するようにします。アカウントにアクセスする個人に個別の IAM ユーザーを作成することにより、固有のセキュリティ認証情報をそれぞれの IAM ユーザーに付与することができます。それぞれの IAM ユーザーに異なったアクセス許可を付与することもできます。必要な場合には、いつでも IAM ユーザーのアクセス許可の変更または取り消しができます(root ユーザーの認証情報をいったん譲渡してしまうと、その取り消しが難しくなります。また、root ユーザーのアクセス許可を制限することはできません)。	はい	いいえ	
1.8 IAM ポリシーのスコープを最小権限に下げている	「最小権限を付与する」の標準的なセキュリティアドバイスに従わなければなりません。つまり、タスクの実行に必要なアクセス許可のみを付与しなければなりません。ユーザーが何をする必要があるのかを決定し、それに沿ったポリシーを作成して、ユーザーが決め	はい	いいえ	

	られたタスクのみを実行できるようにします。最小限のアクセス許可から始めて、必要に応じて追加のアクセス許可を付与します。この方法は、寛容なアクセス許可から始めて後から制限を厳しくしていくよりもはるかに安全です。必要なアクセス許可を正しく定義するには、ある程度の調査が必要です。特定のタスクに必要な権限、特定のサービスがサポートする操作、それらの操作を実行するために必要なアクセス許可ついて判断します。			
1.9 ハードコードされた認証情報 (アクセスキーなど) を使用していない	AWS アクセスキーを管理するためのベストプラクティスに従い、ハードコードされた認証情報の使用を避けなければなりません。AWS にプログラムでアクセスする場合、アクセスキーを使用して自身の ID とアプリケーションの ID を検証します。アクセスキーを持っていれば誰でも、キーの被発行者の AWS リソースに同じレベルでアクセスできます。したがって、AWS ではアクセスキーの保護に細心の注意を払っており、責任共有モデルに基づいて、キーの被発行者も同等の注意を払う必要があります。	はい	はい	
1.10 すべての認証情報を暗号化して保存している	基本要件は、認証情報が暗号化されて保存されていることを保証することです。	はい	はい	
1.11 インタラクティブユーザーのみが AWS アクセスキーを使用している	以下の場合を除き、AWS アクセスキーを使用できません。1. AWS サービスにアクセスする人物がキーを使用しており、その人物が管理するデバイスにキーが安全に保存されている場合。2. 以下の限られた条件下で、サービスが AWS のサービスにアクセスするためにキーを使用している場合。a) Amazon EC2 インスタンスロール、Amazon Elastic Container Service (Amazon ECS) タスクロール、または同様のメカニズムが使用できない場合。b) AWS アクセスキーを週 1 回以上更新している場合。c) IAM ポリシーのスコープが次のように厳しく設定されている場合。i) 特定のメソッドおよびターゲットへのアクセスのみ許可する。ii) リソースへのアクセス元であるサブネットにアクセスを限定する。	はい	はい	
1.12 すべてのリージョンのすべての AWS アカウントに対して AWS CloudTrail が有効である	AWS CloudTrail はすべてのリージョンのすべての AWS アカウントに対して有効である必要があります。AWS アカウントアクティビティの可視性は、セキュリティと運用のベストプラクティスの重要な側面です。AWS CloudTrail を使えば AWS インフラストラクチャ全域にわたって視聴、検索、ダウンロード、アーカイブ、分析、アカウントアクティビティへの応答が可能です。誰が、何が、どんなアクションを取ったか、何のリソースが使われたか、いつそれが起きたのか、また、AWS アカウントに対するアクティビティを分析し、それに対応するのに役立つその他の詳細情報を特定することが可能です。	はい	いいえ	
1.13 別の AWS アカウントが所有する S3 バケットに CloudTrail のログを保存している	AWS CloudTrail のログは、監査やリカバリに限定するなど、ごく限られたアクセスのために構成された別の AWS アカウントが所有するバケットに配置する必要があります。	はい	いいえ	
1.14 CloudTrail S3 ログバケットでバージョニングまたは MFA Delete が有効である	AWS CloudTrail ログバケットの内容は、バージョニングまたは MFA Delete によって保護する必要があります。	はい	いいえ	

1.15 Amazon EC2 セキュリティグループのスコープを厳しくしている	すべての Amazon EC2 セキュリティグループは、最大限までアクセスを制限する必要があります。これには少なくとも、次のことが含まれます。1. インターネットと Amazon VPC 間のトラフィックを制限するようにセキュリティグループを実装する。2. Amazon VPC 内部のトラフィックを制限するようにセキュリティグループを実装する。3. どのような場合でも、最も限定的な設定のみを許可する。	はい	はい	
1.16 アカウント内部の Amazon S3 バケットが適切なレベルのアクセス権を持っている	必ず、各 Amazon S3 バケットへのアクセスを制御するための適切な統制を適用する必要があります。AWS を使用する場合、本当に必要とするユーザーのみにリソースへのアクセスを制限するのがベストプラクティスです (最小権限の原則)。	はい	はい	
1.17 パブリックアクセスを許可するように Amazon S3 バケットを誤って構成していない	パブリックアクセスを許可してはならないバケットが、パブリックアクセスを防ぐように正しく構成されていることを確認しなければなりません。デフォルトでは、すべての Amazon S3 バケットはプライベートであり、明示的にアクセスが許可されたユーザーのみがアクセスできます。パブリックなアセット (一般公開ウェブサイトで使用する画像など) をホストするために Amazon S3 を使用している場合を除き、ほとんどの導入事例では広い範囲のパブリックアクセスを許可しなくても Amazon S3 バケットからのファイル読み取りには支障がないため、アクセスを決してパブリックにオープンにしないのがベストプラクティスです。	はい	はい	
1.18 S3 バケットまたはオブジェクトがパブリックになった時点で検出するモニタリングメカニズムが有効である	Amazon S3 バケットがパブリックになった時点で、それを識別するモニタリングまたはアラートを有効にする必要があります。そのオプションの 1 つは AWS Trusted Advisor の使用です。AWS Trusted Advisor は、オープンなアクセス許可を持つバケットが Amazon S3 にないかチェックします。List アクセスを全員に許可するバケットのアクセス許可により、予想より高い料金が発生することがあります。具体的には、意図しないユーザーがバケット内のオブジェクトのリストを取得する頻度が高い場合です。バケットのUpload/Delete アクセスを全員に許可すると、誰でもバケット内のアイテムを追加、変更、または削除できるため、セキュリティ脆弱性の原因となることがあります。Trusted Advisor のチェックは、バケットの明示的なアクセス許可を検証します。また、バケットに関連付けられたポリシーで、バケットのアクセス許可を上書きする可能性があるものについても検証します。	はい	いいえ	
1.19 Amazon EC2 インスタンスとコンテナの変更を検出するモニタリングメカニズムが有効である	Amazon S3 インスタンスまたはコンテナの変更は不正アクティビティである可能性があり、将来の法的捜査に備えて、少なくとも耐久性のある場所にログを残す必要があります。この目的で採用するメカニズムには、少なくとも次の機能が必要です。1.ソリューションで使用する Amazon S3 インスタンスまたはコンテナ内の OS、あるいはアプリケーションファイルの変更を検出する。2. これらの変更を記録したデータを、Amazon S3 インスタンスまたはコンテナの外部の耐久性のある場所に保存する。適切なメカニズムの例は以下のとおりです。a. Chef、Puppet などのスケジュール化された構成管理、または OSSEC、Tripwire などの特殊なツールによるファイル整合性チェックのデプロイ。b. 構成管理ツールの拡張機能によって Amazon S3 ホスト構成を検証し、重要な構成ファイルまたはパッケージの更新を「canary」(ログに記録された no-op) イベントで警告する。これはランタイム中にすべてのスコープ内ホストでサービスの稼働継続を保証するための構成です。c. OSSEC と ElasticSearch および Kibana のようなオープンソースソリュー	はい	いいえ	

	ションなどのホスト侵入検出システムをデプロイするか、パートナーのソリューションを使用する。次のメカニズムはこの要件を満たさないことに注意してください。a.Amazon S3 インスタンスまたはコンテナの頻繁なサイクル。			
1.20 すべてのデータが分類されている	ワークロードで処理および保存するすべての顧客データに検討を加えて分類し、データの機密性と、データの処理時に使用する適切な方法を決定します。	はい	はい	
1.21 すべての機密データが暗号化されている	機密と分類したすべての顧客データを、転送中および保存中に暗号化します。	はい	はい	
1.22 暗号化キーが安全に管理されている	保存中および転送中のすべての暗号化キーを暗号化し、キーを使用するためのアクセスは、AWS Key Management Service (KMS) などの AWS ソリューションや HashiCorp Vault などのパートナーソリューションを使用して制御します。	はい	はい	
1.23 転送中のすべてのデータが暗号化されている	Amazon Virtual Private Cloud の境界を越えて送信されるすべてのデータは暗号化されます。	はい	はい	
1.24 セキュリティインシデント応答プロセスを定義し、リハーサルしている	AWS アカウントの侵害などのインシデントを処理するセキュリティインシデント応答プロセスを定義しなければなりません。インシデント応答プロセスをリハーサルする手順を実装することによって (たとえば、セキュリティ GameDay 演習を完了することによって) このプロセスをテストしなければなりません。以下を確認するためのリハーサルが最近 12 か月以内に行われていなければなりません。a.適切な担当者が環境にアクセスできる。b.適切なツールが利用可能である。c.対策プランに記載された各種セキュリティインシデントに対応するために何をすべきか、適切な担当者が知っている。	はい	いいえ	
1.25 Payment Cart Industry (PCI) データセキュリティスタンダード (DSS) – 認定あるいは SAQ	カード所有者のデータが存在する e コマース、ユニファイドコマース、および POS アプリケーションの場合、ワークロードに対する Payment Card Industry (PCI) データセキュリティスタンダード (DSS) 範囲の年次評価を実行するプロセスが確立されます。スコープの評価に基づき、PCI DSS 認定または SAQ が必要に応じて実施されます。証拠は PCI DSS 認定のコンプライアンスレポートまたは記入済みの自己評価調査票 (SAQ) の形式で提示する必要があります。	はい	はい	
1.26 PCI データのエンドツーエンド暗号化	カード所有者のデータが存在する e コマース、ユニファイドコマース、および POS アプリケーションの場合、データは Amazon VPC 内であっても転送中に暗号化されます。	はい	はい	
1.27 分散サービス拒否 (DDoS) 攻撃に対する適切な保護	開放型システム間相互接続 (OSI) モデルのすべてのレイヤーに対して、分散サービス拒否 (DDoS) を軽減するインフラストラクチャとサービスを提供します。	はい	いいえ	
1.28 Open Web Application Security Project (OWASP) のトップ 10 攻撃を緩和するためのメカニズム	Open Web Application Security Project (OWASP) の脆弱性を軽減するインフラストラクチャとサービスを提供します。	はい	いいえ	

2.0 信頼性 信頼性の柱では、ビジネスや顧客の要求に応えるための障害の防止や、障害からの迅速な復旧を行う能力について焦点を当てます。主要なトピックには、設定、プロジェクト間の要件、復旧計画、および変更に対処する方法についての基礎的な要素が含まれます。				
2.1 ネットワーク接続の高い可用性	ソリューションへのネットワーク接続の可用性が高い必要があります。VPN または AWS Direct Connect を使用して顧客のネットワークに接続している場合、顧客が必ずしも冗長接続を実装していなくても、ソリューションは冗長接続をサポートする必要があります。	はい	はい	
2.2 インフラストラクチャのスケーリングメカニズムがビジネス要件と合致している	次のいずれかの方法で、インフラストラクチャのスケーリングメカニズムはビジネス要件と合致する必要があります。1.自動スケーリングメカニズムをアーキテクチャの各レイヤーに実装する。2.コスト要件やユーザーの予想増加率など、現在のビジネス要件下では自動スケーリングメカニズムが不要であること、そして、手動でのスケーリング手順が完全に文書化され頻繁にテストされていることを確認する。	はい	はい	
2.3 AWS とアプリケーションのログが集中管理されている	アプリケーションおよび AWS インフラストラクチャのすべてのログ情報を 1 つのシステムに統合する必要があります。	はい	いいえ	
2.4 AWS とアプリケーションのモニタリングとアラームが集中管理されている	アプリケーションと AWS インフラストラクチャを集中的にモニタリングし、アラームを生成して適切な運用スタッフに送信しなければなりません。	はい	いいえ	
2.5 インフラストラクチャのプロビジョニングと管理が自動化されている	ソリューションでは、AWS CloudFormation や Terraform などの自動化ツールを使用して、 AWS インフラストラクチャをプロビジョニングおよび管理する必要があります。AWS コンソールは、稼働中の AWS インフラストラクチャに定型的な変更を加えるために使用できません。	はい	はい	
2.6 定期的なデータバックアップを実行している	耐久性のあるストレージサービスへの定期的なバックアップを実行しなければなりません。バックアップは、管理、論理、または物理エラーの状況からのリカバリ能力があることを保証します。Amazon S3 および Amazon Glacier はバックアップやアーカイブに適したサービスです。どちらも耐久性があり、低コストのストレージプラットフォームです。どちらも容量無制限で、バックアップデータセットが大きくなってもボリュームまたはメディアの管理が不要です。従量制の料金モデルと GB/月あたりの低コストにより、これらのサービスはデータ保護の導入事例に最適です。	はい	はい	
2.7 リカバリメカニズムを定期的に、またアーキテクチャの大きな変更後にテストしている	リカバリのメカニズムと手順を定期的に、またクラウド環境を大きく変更した後にテストしなければなりません。AWS では、データのバックアップと復元の管理に役立つ多くのリソースを提供しています。	はい	いいえ	
2.8 アベイラビリティーゾーンの中断に対してソリューションが弾力的である	1 つのアベイラビリティーゾーン内のサービスがすべて中断した場合でも、ソリューションが稼働し続けなければなりません。	はい	はい	

2.9 ソリューションの弾力性がテスト済みである	1 つのアベイラビリティーゾーンの中断に対するインフラストラクチャの弾力性が、実稼働環境で、Gameday 演習などによって最近 12 か月以内にテスト済みです。	はい	いいえ	
2.10 災害対策 (DR) 計画が定義されている	目標復旧ポイント (RPO) と目標復旧時間 (RTO) を含む、綿密な災害対策計画が定義されています。すべてのスコープ内サービスの RPO と RTO を定義し、この RPO と RTO が顧客に提案する SLA と整合していなければなりません。	はい	はい	
2.11 目標復旧時間 (RTO) が 24 時間未満である	基本要件は、コアサービスの RTO が 24 時間未満であることです。	はい	いいえ	
2.12 災害対策 (DR) 計画が適切にテストされている	DR 計画を定期的に、また大規模な更新の後にテストして、目標復旧ポイント (RPO) および目標復旧時間 (RTO) を達成しなければなりません。AWS APNアドバンスト階層の申請承認前に、少なくとも 1 回の DR テストを完了しなければなりません。	はい	いいえ	
2.13 別のリージョンへのリカバリが災害対策 (DR) 計画に含まれている	別の AWS リージョンへのリカバリ手順を DR 計画に含め、定期的なリカバリテストでこのシナリオをテストしなければなりません。別の AWS リージョンへのリカバリを含めた DR 対策の完全テストを、最近 12 か月以内に少なくとも 1 回は完了済みである必要があります。注意: テスト環境にデータを復元する、またはユーザーのデータをエクスポートするプロセスは、バックアップを検証するための有用な方法ですが、これらのプロセスは別の AWS リージョンへの完全復元テストを実行するという要件を満たすものではありません。	はい	いいえ	
3.0 運用上の優秀性 運用上の優秀性の柱では、ビジネス価値を提供するためのシステムの実行とモニタリング、および継続的にプロセスと手順を改善することに焦点を当てます。主要なトピックには、変更の管理と自動化、イベントへの対応、日常業務を適切に管理するための標準の定義が含まれます。				
3.1 コード変更のデプロイが自動化されている	ソリューションでは、AWS インフラストラクチャにコードをデプロイする自動化された方法を使用しなければなりません。AWS インフラストラクチャに更新をデプロイするために、対話型の Secure Shell (SSH) あるいは Remote Desktop Protocol (RDP) セッションを使用することはできません。	はい	いいえ	
3.2 ランブックとエスカレーションプロセスが定義されている	ランブックを作成し、各種のアプリケーションイベントや AWS イベントへの対応に使用する標準的な手順を定義しなければなりません。システムによって生成されるアラートやアラームに対処したり、顧客から報告されたインシデントに対応したりするためのエスカレーションプロセスを定義しなければなりません。エスカレーションプロセスには、必要に応じた AWS サポートへのエスカレーションを含めなければなりません。	はい	いいえ	
3.3 AWS アカウントに対して AWS ビジネスサポートが有効である	ビジネスサポートが有効でなければなりません。ビジネスサポート (または、より上位のサポート) は、AWS パートナーネットワークでアドバンスド階層のテクノロジーパートナーの認定要件です。アドバンスド階層の資格を満たすためには、少なくとも 1 つの AWS アカウントでビジネスサポートを有効にしなければなりません。	はい	いいえ	

4.0 パフォーマンス効率 パフォーマンス効率の柱では、IT とコンピューティングリソースの効率的な利用に焦点を当てます。主要トピックには、必要なワークロードに基づく適切なリソースのタイプやサイズの選択、パフォーマンスのモニタリング、ビジネスニーズの変化に応じて効率性を維持するための情報に基づく意思決定などが含まれます。				
4.1 デプロイ後にパフォーマンステストが有効化される	測定可能なパフォーマンス目標を定義し、パフォーマンステストを実施して、本番稼働へのリリース前にパフォーマンス目標が満たされていることを確認します。	はい	はい	
4.2 所定のしきい値をモニタリングする	アプリケーションのパフォーマンスをモニタリングし、しきい値に違反したときにアラームをトリガーするメカニズムを用意します。	はい	はい	

AWS リソース:

タイトル	説明
プラクティスランディングページの構築方法	プログラムの前提条件を満たす、プラクティス/ソリューションページを構築する方法についてのガイダンスを提供します。
公開導入事例について記述する方法	プログラムの前提条件を満たし、公開するお客様導入事例を作成する方法についてのガイダンスを提供します。
アーキテクチャダイアグラムを構築する方法	プログラムの前提条件を満たす、アーキテクチャ図を作成する方法についてのガイダンスを提供します。
パートナー準備に関するドキュメント	プログラムの前提条件のガイダンスおよびベストプラクティス例を提供します。
AWS Well-Architected ウェブサイト	Well Architected ベストプラクティスを網羅