Salesforce.Identity-and-Access-Management-Architect-JPN.v2026-09-24.q45

試験コード：	Identity-and-Access-Management-Architect-JPN
試験名称：	Salesforce Certified Identity and Access Management Architect (Identity-and-Access-Management-Architect日本語版)
認証ベンダー：	Salesforce
無料問題の数：	45
バージョン：	v2026-09-24
ページの閲覧量：	108
問題集の閲覧量：	605

https://www.jpnshiken.com/shiken/Salesforce.Identity-and-Access-Management-Architect-JPN.v2026-09-24.q45.html

質問: **1**
ノーザン -トレイル -アウトフィッターズ(NTO)は、新しい顧客サービスポータルを構築する予定で、パスワード不要のログイン方式を採用したいと考えています。これにより、顧客はメールまたはSMSで送信されるワンタイムパスコードを使用してログインできるようになります。
必要な本人確認クレジットの数量はどのように見積もるべきでしょうか？
A. 本人確認クレジットは、送信される確認ごとに消費されるため、本人確認チャレンジが発生するログイン回数に基づいて見積もる必要があります。
B. 各コミュニティには毎月 10,000 の本人確認クレジットが付与されており、月間ログイン回数が 10,000 を超える顧客のみが、追加の SMS 認証が必要になることを見積もる必要があります。
C. 本人確認クレジットは、送信される各SMS(ベストメッセージ)ごとに消費され、SMS認証ユーザーのログイン認証チャレンジの数に基づいて見積もる必要があります。
D. 本人確認クレジットは、既存のメンバーベースまたはログインベースのコミュニティライセンスの数に基づいて直接追加されるライセンスです。
正解: **(**正解を表示します**)**
Identity Verification Credits are consumed when Salesforce sends verification challenges through the configured channel, and SMS-based passwordless login specifically depends on SMS verification activity.
Therefore the right estimation approach is to forecast how many SMS verification events the portal will generate, not how many community licenses exist. Some Salesforce identity offerings include baseline entitlements, but capacity planning still centers on expected

verification traffic. If the portal intends to let customers log in with one-time passcodes sent by text, then every challenge can consume credits. The architecture question is really an operational one: estimate the expected volume of SMS-based login verification and size the verification-credit requirement to match that demand. This is why option C is the best answer in Salesforce terms.

質問: **2**
Universal Containersは複数のSalesforceインスタンスを運用しており、ユーザーはそれぞれ異なるインスタンスからメールを受信します。
ユーザーがSalesforceレコードへのメールリンクをクリックする際には、ユーザーは自身のIDプロバイダーによって認証された正しいSalesforceインスタンスにログインしている必要があります。
Salesforceで前提条件として有効にしておくべきことは何ですか？
A. 外部識別子
B. 私のドメイン
C. 多要素認証
D. IDプロバイダー
正解: **(正解を表示します)**
My Domain is a prerequisite for many modern Salesforce identity capabilities because it gives the org a unique and predictable login domain. In multi-org environments, that matters when users click record links from emails and must be routed into the correct instance and authentication path. Without My Domain, identity routing and branded login behavior become harder to control, especially when multiple orgs and external identity providers are involved. MFA and Identity Provider settings address other aspects of security, but they do not provide the unique domain-level entry point required here. The architectural role of My Domain is both technical and user-facing: it standardizes the login endpoint and helps ensure that generated links take users to the proper org context. This is why option B is the best answer in Salesforce terms.

質問: **3**
ユニバーサル ・コンテナーズ(UC)は、輸送用コンテナにWi-Fi対応のGPS追跡装置を搭載し、追跡装置からカスタムAPIを介してSalesforceの運用組織にGPS座標データを送信する計画を立てています。このGPS装置には、ユーザーによる直接的な入力や出力機能はありません。
アイデンティティアーキテクトは、要件を満たすためにどのOAuthフローを推奨すべきでしょうか？
A. 接続されたデバイスを保護するためのOAuth 2.0アセットトークンフロー
B. Webアプリ統合のためのOAuth 2.0 Webサーバーフロー
C. サーバー間統合のためのOAuth 2.0 JWTベアラーフロー
D. 特殊なシナリオ向けのOAuth 2.0ユーザー名/パスワードフロー

正解: **A (**コメントを発表する**)**
The OAuth 2.0 Asset Token Flow is Salesforce's purpose-built answer for connected devices and IoT-style integrations. It is designed for assets that need to act on behalf of a physical device or asset record rather than a human user. That makes it the correct fit for sensors, GPS trackers, or smart devices that must securely post telemetry or create service actions in Salesforce. User-agent, web-server, or username-password flows are built around user identity or generic application access, not around a registered device/asset relationship. The architectural advantage of the asset token model is that it ties the authorization context back to the asset, which is exactly what you want when the platform must know which device generated the event or maintenance alert. This is why option A is the best answer in Salesforce terms.

質問: **4**
Salesforceにログインするユーザーは、頻繁に本人確認を求められます。
本人確認設計者は、迅速な本人確認の頻度を減らすための提言を行う必要がある。
アイデンティティアーキテクトは、この要件を満たすためにどのようなことを推奨すべきでしょうか？
A. 外部IDプロバイダーを使用してSalesforceのシングルサインオンを実装します。
B. 組織の信頼できるIPアドレス範囲を設定します。
C. Salesforce 組織に 2FA 認証を実装します。
D. Salesforce 組織に多要素認証を実装します。
正解: **(**正解を表示します**)**
Frequent identity verification prompts in Salesforce are often a session security issue rather than an SSO design defect. One of the standard administrator controls for reducing repeated verification in known corporate environments is to define trusted IP ranges. When a login originates from a recognized network, Salesforce can apply lower-friction verification behavior consistent with the org's policies. Simply enabling MFA or 2FA does not reduce prompts; those controls often introduce stronger verification requirements. Similarly, moving to an external identity provider changes the sign-in architecture but does not automatically tell Salesforce to trust the user's network context. The trusted IP model is the documented way to reduce unnecessary verification challenges while keeping the org's perimeter assumptions explicit. This is why option B is the best answer in Salesforce terms.

質問: **5**
ある大学が卒業生向けの本人確認システムを導入する計画を立てている。シングルサインオンにはサードパーティの本人確認プロバイダーを利用し、記録システムにはSalesforceを使用する予定だ。しかし、ユーザーがログインしようとするとエラーメッセージが表示されるという問題が発生している。
この問題のデバッグには、Salesforceのどの機能を使用すればよいですか？

A. ニュースレッグス
B. Webアプリ監査証跡
C. ログイン履歴
D. 例外メールについて
正解**: (**正解を表示します**)**
When users report SSO login errors, Login History is the first Salesforce-native place to look for the failure details. It records authentication attempts, statuses, timestamps, source information, and failure reasons that help narrow down whether the problem lies in the identity provider, the assertion, or the Salesforce configuration. Setup Audit Trail is for admin changes, not runtime authentication troubleshooting, and exception email is not the primary way to debug SSO. The practical reason architects start with Login History is that it tells you what Salesforce actually received and how Salesforce evaluated it. That makes it a reliable first checkpoint during alumni portal, workforce SSO, or community login investigations. This is why option C is the best answer in Salesforce terms.

質問**: 6**
Universal Containersは、OpenID Connectを使用して、新しいモバイルアプリから本番環境のSalesforce組織への接続を実現しています。
OpenID Connect接続のアクセストークンステータスを取得できるようにするには、どのような手順を踏むべきですか？
A. OpenID Connectトークンのイントロスペクションを活用します。
B. OpenID Connect ディスカバリエンドポイントを使用したクエリ。
C. /services/oauth2/token エンドポイントに対してクロスオリジンリソース共有 (CORS) を有効にします。
D. カスタム OAuth スコープを作成します。
正解**: A (**コメントを発表する**)**
Salesforce documents token introspection as the standards-based way to ask the authorization server about the current state of an OAuth token after it has been issued. That is exactly what this scenario requires: checking whether an OpenID Connect access token is still active, expired, or revoked. The discovery document only advertises endpoints and capabilities; it does not return runtime token status for a specific token. Likewise, enabling CORS on the token endpoint affects browser access patterns, not token validation, and creating a custom scope changes authorization boundaries rather than token-state lookup. In other words, when the requirement is "retrieve token status," token introspection is the platform feature designed for that purpose.
This is why option A is the best answer in Salesforce terms.

質問**: 7**

Universal Containers社は、ユーザーがActive Directoryのパスワードを使用してSalesforceモバイルアプリにログインできるようにしたいと考えています。従業員はモバイルVPNを使用できません。
アイデンティティアーキテクトは、要件を満たすためにどの2つの選択肢を推奨すべきでしょうか？
2つの回答を選択してください
A. プラグイン以降のActive Directoryパスワード
B. Salesforce Identity Connect
C. 取引先責任者オブジェクトのSalesforceトリガーとフィールド
D. クラウドプロバイダーロードバランサーの設定
正解: **(**正解を表示します**)**
If users must log in to the Salesforce mobile app with their Active Directory credentials and cannot rely on a mobile VPN, the architecture usually combines Salesforce Identity Connect with the appropriate Active Directory authentication plug-in or federation integration that allows Salesforce to honor those AD credentials without direct VPN dependency. Identity Connect helps bridge AD user management into Salesforce, while the directory-side authentication component handles password validation against Active Directory. Custom triggers or load balancers do not solve the identity problem. The important architecture idea is that workforce users should continue using their corporate directory password, and Salesforce should trust that directory- driven authentication path in a mobile-friendly way. This is why options A, B work together as the correct solution.

質問: **8**
Salesforceの顧客企業が、コールセンターのエージェント向けにSales Cloudとカスタム価格設定アプリケーションを導入している。
エンタープライズ向けシングルサインオンソリューションを使用して、すべてのアプリケーションへのユーザー認証とサインインを行います。顧客は以下の要件を掲げています。
1. 開発チームは、価格設定アプリケーションをエージェントに公開するためにCanvasアプリを使用することを決定しました。
2. エージェントは、価格設定アプリケーションにログインすることなく、Canvasアプリにアクセスできる必要があります。
アイデンティティアーキテクトは、Canvasアプリがユーザーのログインを開始できるようにするために、どの2つの選択肢を検討すべきでしょうか？
2つの回答を選択してください
A. Canvasアプリを接続済みアプリとして構成し、管理者が承認したユーザーを事前承認済みとして設定します。
B. 接続済みアプリの設定で「Canvasパーソナルアプリとして有効にする」を選択します。
C. 料金設定アプリケーションに必要な OAuth スコープを使用して、接続済みアプリで OAuth 設定を有効にします。

D. 接続されたアプリで SAML を有効にし、Security Assertion Markup Language (SAML) 開始方法をサービスプロバイダー開始に設定します。
正解: **A,D (**コメントを発表する**)**
A Canvas integration relies on a connected app to establish trust between Salesforce and the external application. To let agents open the pricing application without a second login, the connected app should be pre-authorized for the intended users so consent is not prompted at runtime. When the external application participates in enterprise SSO, SAML settings on the connected app can also support the federated sign-in pattern expected by the pricing service. The key Salesforce design principle is that Canvas is not only an iframe placement technology; it also depends on connected app security and identity configuration. Pre- authorization controls user access, while SSO settings determine how the external app accepts the Salesforce- initiated identity context. This is why options A, D work together as the correct solution.

質問: **9**
Universal Containers (UC) は、カスタマーサービス担当者向けに Salesforce を使用しています。UC は、SAML (Security Assertion Markup Language) ベースのシングルサインオンをサポートする独自の注文追跡システムを持っています。カスタマーサービス担当副社長は、Salesforce 内でのみ表示される注文追跡システムには、アクティブな Salesforce ユーザーのみがアクセスできるようにしたいと考えています。
要件を満たすためには、何をすべきでしょうか？
2つの回答を選択してください
A. 注文追跡用のIDプロバイダー(IdP)として企業IDストアを設定します。
B. ログイン後にSalesforceでユーザーを検証するためのREST呼び出しを開始するように注文追跡をカスタマイズします。
C. 注文追跡用のIDプロバイダー(IdP)としてSalesforceを設定します。
D. Salesforce の Canvas アプリとして注文追跡を設定し、IdP が開始した SAML アサーションを POST します。
正解: **(**正解を表示します**)**
If the order-tracking application supports SAML SSO and should only be accessible to active Salesforce users from inside Salesforce, the clean approach is to make Salesforce the identity provider and expose the app through Salesforce as a Canvas-style embedded experience or equivalent app launch pattern. Using Salesforce as the IdP ensures that only valid Salesforce users can obtain the SAML identity needed to enter the external system. A separate corporate identity store or a custom REST validation step introduces more moving parts than needed. The architectural goal is to let Salesforce govern access to the application that is surfaced from within Salesforce. That points to Salesforce-led federation and an in-platform application entry point. This is why options C, D work together as the correct solution.

質問: **10**
あるテクノロジー企業が、従業員向けに外部ベンダーのウェルネスアプリケーションと連携したIDソリューションを構築している。ユーザー属性はIDトークンとしてウェルネスアプリケーションに返される必要がある。
アイデンティティアーキテクトは、要件を満たすためにどの認証メカニズムを推奨すべきでしょうか？
A. ユーザーエージェントフロー
B. OpenID Connect
C. JWTベアラートークンフロー
D. Webサーバーフロー
正解: **(正解を表示します)**
If the external wellness application needs user attributes returned in an ID token, the mechanism must be OpenID Connect. OIDC extends OAuth with identity semantics and introduces the ID token as the standard carrier for authenticated user information. A plain user-agent or web-server OAuth flow by itself does not guarantee an ID token, because OAuth alone is about authorization, not identity. JWT bearer flow is also for noninteractive token exchange, not end-user identity assertion to a relying party. The architecture requirement points directly to the artifact being requested: an ID token. In Salesforce identity design, once the requirement says "return attributes in an ID token," the answer is to use OpenID Connect. This is why option B is the best answer in Salesforce terms.

質問: **11**
アイデンティティアーキテクトの顧客は、自社開発のアイデンティティプロバイダー(IdP)を使用しています。サービスプロバイダー(SP)としてはSalesforceが使用されています。IT部門の責任者は、SPが開始するシングルサインオン(SSO)の際に、セキュリティアサーションマークアップ言語(SAML)リクエストの内容が変更されるのではないかと懸念しています。
アイデンティティアーキテクトは、サービスプロバイダー(SP)とアイデンティティプロバイダー(IdP)間の信頼関係をさらに強化するために、どのような対策を推奨すべきでしょうか？
A. IDPとSPの間でHTTPS接続が確立されていることを確認してください。
B. 認証局 (CA) 署名付き証明書を使用して SAML リクエストを暗号化し、IdP で復号します。
C. SPとIDPの間で発行者およびアサーション消費者サービス(ACS)URLが正しく構成されていることを確認してください。
D. SSO設定ページで、 署名証明書の要求」フィールドに自己署名証明書が設定されていることを確認してください。
正解: **(正解を表示します)**
If the concern is that an SP-initiated SAML request could be altered on the way to the identity provider, the additional control is request signing. Salesforce supports signing the

SAML request with a request-signing certificate so the IdP can verify integrity and origin. HTTPS protects the transport channel, but it does not provide the same message-level assurance that a signed request provides inside the SAML trust model. Issuer and ACS configuration are necessary for setup, yet they do not prove that the request was not modified. The architecture principle here is layered trust: transport security protects the channel, while signature validation protects the SAML message itself. That is why the request-signing certificate is the feature that directly addresses tampering concerns. This is why option D is the best answer in Salesforce terms.

質問**: 12**
Salesforceプラットフォーム上でマルチブランドの顧客IDおよびアクセス管理ソリューションを設計する際、IDアーキテクトはSalesforce内で特定のブランド体験が適切に提供されるようにするにはどうすればよいのでしょうか？
A. エクスペリエンスID。OAuth/Open IDフローおよびSecurity Assertion Markup Language (SAML)フローにURLパラメータとして含めることができます。
B. 共有クッキーに設定できるオーディエンスID。
C. サービスプロバイダの OAuth/SAML 呼び出しにカスタムパラメータを追加し、そのログインページにロジックを実装して、パラメータの値に基づいてブランディングを適用します。
D. エンドユーザーがSalesforceにアクセスした際に、サブブランドを選択できるブランドピッカーを提供します。
正解**: (**正解を表示します**)**
Salesforce supports dynamic branding for Experience Cloud login journeys through the Experience ID parameter. The Experience ID tells Salesforce which branded experience to render, allowing a single identity implementation to serve multiple brands or sub-brands without building separate authentication stacks. This is more scalable than asking users to pick a brand after arrival or inventing custom parameters and branding logic outside the standard experience framework. It also works cleanly with OAuth and SAML-based sign-in patterns, which is why it is commonly recommended in multi-brand CIAM designs. When the requirement is to reliably present the correct branded Salesforce experience during login, the Experience ID is the built-in mechanism intended for that routing and presentation layer. This is why option A is the best answer in Salesforce terms.

質問**: 13**
あるメーカーは、ディスプレイ入力や機能が制限されたIoT(モノのインターネット)デバイスの登録機能を提供したいと考えている。
どのSalesforce OAuth認証フローを使用すべきですか？
A. OAuth 2.0 User-Agent
B. OAuth 2.0 アセットトークンフロー
C. OAuth 2.0 WiT ベアラーフロー

D. OAuth 2.0 デバイスフロー
正解: **(**正解を表示します**)**
The OAuth 2.0 Device Flow is intended for devices that have limited input or display capabilities and therefore cannot easily support a standard browser-based login interaction. Instead of collecting full credentials on the device, the user completes authorization on a secondary device using a verification code and URL. That is why Salesforce recommends device flow for TVs, appliances, kiosks, and similarly constrained hardware. Asset Token Flow solves a different problem: it authorizes a registered asset or device to call Salesforce as a connected thing. Here the requirement is about registration and user authorization from a constrained device, so the device flow is the correct match. The design distinction is between human sign-in on limited hardware and secure machine identity for an asset. This is why option D is the best answer in Salesforce terms.

質問: **14**
アイデンティティアーキテクトは、ユーザーがExperience Cloudサイト(旧称Community)のホームページにアクセスする前に、管理者がユーザーに対してパーソナライズされたアラートメッセージを設定できるソリューションを推奨するよう依頼されました。
この要件を満たすために、最小限のカスタマイズで済む方法はどれでしょうか？
A. ユーザープロファイルに基づいて異なるホームページに移動するルーティングロジックを作成するために、登録ハンドラーApexクラスをカスタマイズします。
B. ログインフローを使用して、パーソナライズされたアラートを表示する画面を追加します。
C. ユーザーアラートを保存するカスタムメタデータを作成し、LWCを使用してアラートを表示します。
D. カスタムアラートを表示するホームページ用の Lightning Web Component (LWC) を作成します。
正解: **(**正解を表示します**)**
Login Flows are the least-custom way to present user-specific messaging before a user lands on an Experience Cloud home page. Salesforce designed login flows to insert screens into the authentication journey, which makes them a strong fit for pre-homepage alerts, acknowledgments, and decision points. A custom homepage component can display alerts after login, but it does not satisfy the "before they land on the homepage" requirement as directly. Custom metadata with LWC or a specialized registration handler introduces more build effort than needed. The important platform distinction is timing: login flows run during authentication and can show a screen before the session continues to the destination page. That is why they are commonly chosen for policy notices, onboarding prompts, and personalized pre-entry messages. This is why option B is the best answer in Salesforce terms.

質問: **15**

ある組織のエグゼクティブスポンサーから、Salesforceが、よりシームレスなユーザーエクスペリエンスを実現するために、ログインウィジェットをサービスプロバイダーに埋め込む機能をサポートしているかどうかを問い合わせがありました。
Salesforceプラットフォーム上でソリューションとして推奨する前に、どのような点を考慮し、どのような対策を講じるべきでしょうか？
A. 埋め込みログイン。サービスプロバイダーの外観や操作感に合わせるために、どの程度のUIカスタマイズが必要になるかを特定します。
B. Salesforce REST API。統合にはセキュアソケットレイヤー(SSL)接続が使用されていることを確認してください。
C. OpenID Connect Webサーバーフロー。サービスプロバイダーがクライアントシークレットを保存するのに十分なセキュリティを備えているかどうかを判断します。
D. 埋め込みログイン。ブラウザの互換性の問題を引き起こす可能性のあるサードパーティCookieに依存しているかどうかを検討してください。
正解: **(**正解を表示します**)**
Salesforce Embedded Login exists specifically to place a Salesforce-backed login experience inside another application or service provider, which makes it the right feature to consider for a seamless sign-in widget.
However, the architectural caveat is browser behavior. Embedded login can rely on third-party cookies, and modern browser privacy controls can affect how that experience behaves. That dependency is often the deciding consideration before recommending it.
REST APIs and generic OAuth flows are part of the broader identity toolbox, but they don't answer the executive sponsor's question about embedding a login widget directly into another application. The recommendation should therefore focus on Embedded Login and on whether the target browser landscape will tolerate the cookie model it depends on. This is why option D is the best answer in Salesforce terms.

質問**: 16**
Universal Containersは、Salesforce IdentityのQAuth 2.0ユーザーエージェントフロー(このフローではQAuth 2.0の暗黙的許可タイプを使用)によって保護されるモバイルアプリケーションを開発しています。
このフローに適用される3つのQAuth概念はどれですか？
3つの回答を選択してください
A. リフレッシュトークン
B. クライアントID
C. 確認コード
D. 認証コード
E. スコパス
正解: **(**正解を表示します**)**
Salesforce's user-agent flow implements the OAuth 2.0 implicit grant model for browser-based or mobile applications that obtain authorization through a browser. In that flow, the

client uses a client ID and requests specific scopes. The user authorizes the app, and the resulting token is delivered through the browser-based redirect. In Salesforce identity examples, refresh-related behavior is often part of the mobile discussion, while an authorization code is not a characteristic of the implicit model. That is the key concept to remember:
implicit or user-agent flow is centered on browser-mediated authorization without a back-end code exchange.
So the valid concepts align with client identity and requested access, not with the server-side authorization- code step used in the web server flow. This is why options A, B, E work together as the correct solution.

有効的な**Identity-and-Access-Management-Architect-JPN**問題集はJPNTest.com提供され、**Identity-and-Access-Management-Architect-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**Identity-and-Access-Management-Architect-JPN**試験問題集を提供します。JPNTest.com Identity-and-Access-Management-Architect-JPN試験問題集はもう更新されました。ここで**Identity-and-Access-Management-Architect-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/Identity-and-Access-Management-Architect-JPN-mondaishu ﬁ**12**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **17**
ノーザン・トレイル・アウトフィッターズ(NTO)は、顧客が購入した商品に関する問題を報告・管理できる機能を提供したいと考えています。NTOにとって、顧客がAmazonのアカウント情報でログインできる機能を提供することは重要です。
これらの要件を満たすために、アイデンティティアーキテクトはどのようなことを推奨すべきでしょうか？
A. Amazon 用のカスタム外部認証プロバイダーを作成します。
B. Amazonを接続済みアプリとして構成します。
C. Amazon 用の OpenID Connect 認証プロバイダーを設定します。
D. Amazon 用の事前定義済み認証プロバイダーを設定します。
正解: **(**正解を表示します**)**
When an external brand such as Amazon supports OpenID Connect and the requirement is to let customers use those credentials to sign in to Experience Cloud, the straightforward Salesforce approach is to configure an OpenID Connect authentication provider. A connected app represents an app trust relationship, not the external identity source for community login. A predefined provider can be used only when Salesforce offers that exact template; otherwise standards-based OIDC is the general answer. Building a custom provider would be unnecessary if the external source already speaks OpenID Connect.

The architectural decision is simply to use the standard protocol that the provider supports and let Salesforce consume that identity through an authentication provider. This is why option C is the best answer in Salesforce terms.

質問: **18**
Universal Containersは、お客様にSalesforce Experience Cloud上に構築されたポータルへの登録とログインをお願いしています。お客様は、利便性を考慮して、FacebookまたはLinkedInの認証情報を使用できるはずです。
アイデンティティアーキテクトがソーシャルサインオンを実装するために取るべき3つのステップは何ですか？
3つの回答を選択してください
A. ユーザーの作成と更新を行うためのデフォルトの登録ハンドラを更新します。
B. 「SAML を使用したフェデレーション シングル サインオン」を有効にする。
C. ログインページ設定で「Facebook」と「LinkedIn」を有効にします。
D. FacebookとLinkedInの両方の認証プロバイダーを作成します。
E. FacebookとLinkedInの両方を接続済みアプリとして登録します。
正解: **A,C,D (**コメントを発表する**)**
To enable social sign-on for Experience Cloud, Salesforce expects the architect to create an authentication provider for each social identity source, expose those providers on the login page, and use the registration handler logic that creates or updates the external user in Salesforce. SAML federation is not required for Facebook or LinkedIn sign-in. Connected apps are not how those social providers are registered for Experience Cloud login; the trust is established through authentication providers. The architect also needs the login page to actually show the provider buttons so users can choose those sign-in methods. In short, the implementation has three moving parts: provider setup, login-page exposure, and user-provisioning logic through the registration handler. This is why options A, C, D work together as the correct solution.

質問: **19**
Northern Trail Outfittersは、アプリケーションの機能権限をActive Directoryグループとして一元的に管理しています。
CRM_SuperUserグループとCRM_Reporting_SuperUserグループは、それぞれSalesforceにおいてユーザーにSuperUser権限とReporting_SuperUser権限を付与する必要があります。Salesforceは、SAML(Security Assertion Markup Language)IDプロバイダーへのサービスプロバイダーです。
アイデンティティアーキテクトは、ユーザーがSalesforceにアクセスする際に、Active Directoryグループが正しく反映されるようにするにはどうすればよいでしょうか？
A. Apex の Just-in-Time ハンドラーを使用して、カスタム SAML 属性を照会し、権限セットを設定します。
B. ログインフローを使用して標準の SAML 属性を照会し、権限セットを設定します。

C. ログインフローを使用してカスタム SAML 属性を照会し、権限セットを設定します。
D. Apex の Just-in-Time ハンドラーを使用して、標準 SAML 属性を照会し、権限セットを設定します。
正解: **(**正解を表示します**)**
When Salesforce receives a SAML assertion and needs to translate external directory group membership into Salesforce entitlements at login, Apex Just-in-Time provisioning is the right hook. A JIT handler can read custom SAML attributes, interpret the incoming group values, and then create or update the user record and assign the appropriate permission sets. Login flows run after authentication and are not the normal mechanism for parsing assertion content into provisioning logic. Standard SAML attributes also don't carry every organization-specific group mapping, which is why custom attributes are typically used for permission translation. The design goal is to make access decisions based on identity-provider claims at sign-in, and the JIT Apex handler is where Salesforce expects that provisioning and entitlement logic to be implemented. This is why option A is the best answer in Salesforce terms.

質問: **20**
世界的なフィットネス機器メーカーがフィットネストラッキングデバイスの販売を計画しており、以下の要件があります。
1) 顧客がデバイスを購入する。
2) 顧客はモバイルアプリを使用してデバイスを登録します。
3) デバイスが追跡に関する問題を記録した場合、Salesforceにケースが自動的に作成され、顧客のアカウントに関連付けられる必要があります。
これらの要件を満たすには、どのOAuthフローを使用すべきでしょうか？
A. OAuth 2.0 ユーザーエージェントフロー
B. OAuth 2.0 アセットトークンフロー
C. OAuth 2.0 デバイスフロー
D. OAuth 2.0 SAVLサーバーアサーションフロー
正解: **(**正解を表示します**)**
The OAuth 2.0 Asset Token Flow is Salesforce's purpose-built answer for connected devices and IoT-style integrations. It is designed for assets that need to act on behalf of a physical device or asset record rather than a human user. That makes it the correct fit for sensors, GPS trackers, or smart devices that must securely post telemetry or create service actions in Salesforce. User-agent, web-server, or username-password flows are built around user identity or generic application access, not around a registered device/asset relationship. The architectural advantage of the asset token model is that it ties the authorization context back to the asset, which is exactly what you want when the platform must know which device generated the event or maintenance alert. This is why option B is the best answer in Salesforce terms.

質問: **21**
Northern Trail Outfitters(NTO)は最近、Microsoft Active Directory(AD)とSalesforce Sales Cloud全体にわたるユーザープロビジョニングを効率化するために、Salesforce Identity Connectを購入しました。
NTOは、どのSalesforceセキュリティ設定がADの権限に対応できるかを特定するよう、アイデンティティアーキテクトに依頼した。
Salesforceのどの3つの権限をADの権限にマッピングできますか？
3つの回答を選択してください
A. 共有ルール
B. 公開グループ
C. パーミッションセットライセンス
D. 役割
E. プロファイルと権限セット
正解: **(**正解を表示します**)**
Identity Connect can synchronize several Salesforce security constructs from Active Directory-driven administration, particularly the identity and authorization artifacts attached to users. Profiles and permission sets are directly relevant because they define user capabilities in Salesforce. Roles also matter because they shape record access and hierarchy behavior. Public groups can participate in permission design and assignment patterns as well. By contrast, sharing rules and permission set licenses are not the core mapping focus in the same way. The main architectural takeaway is that Identity Connect is about translating directory- based user management into Salesforce access structures, especially those that determine who a user is, what they can do, and where they sit in the org's access model. This is why options B, D, E work together as the correct solution.

質問: **22**
Northern Trail Outfitters (NTO) は、Salesforce Experience Cloud を使用して設計・構築された新しいデジタルポータルへのログインに、顧客に電話番号を使用するよう求めています。ポータルにアクセスするには、ユーザーは以下の手順を実行する必要があります。
1. 電話番号またはメールアドレスを入力してください
2. メールまたはSMSで送信される確認コードを入力してください。
この要件を満たすための推奨されるアプローチは何ですか？
A. 認証プロバイダを作成し、自己登録ハンドラクラスを実装します。
B. Apex コントローラーを使用してカスタム ログイン ページを作成します。コントローラーには、ID を送信して検証するためのヒントがあります。
C. ログイン発見ページを作成し、ログイン発見ハンドラーApexクラスを提供します。
D. Apex コントローラーを使用して、会社の認証サービスで電話番号を検証するカスタム ログインフローを作成します。
正解: **C (**コメントを発表する**)**

For a portal that wants users to enter a phone number or email address first and then receive a one-time verification code, Salesforce's recommended pattern is a Login Discovery page backed by a Login Discovery handler. This supports identifier-first authentication and lets the org decide how to route or verify the user once the identifier is known. Building a custom login page and controller can work, but it bypasses the purpose-built experience Salesforce provides for this exact passwordless entry pattern.
Authentication providers and login flows solve different phases of the login journey. The architectural advantage of Login Discovery is that it cleanly supports phone-or-email identification before the platform or handler triggers the verification step. This is why option C is the best answer in Salesforce terms.

質問: **23**
Universal Containers社は新しいExperience Cloudサイトを導入しており、アイデンティティアーキテクトはログインプロセスの一部として動的なブランディング機能を利用したいと考えている。
サイトのダイナミックブランディングをサポートするために、アイデンティティアーキテクトはどの2つのオプションを推奨すべきでしょうか？
2つの回答を選択してください
A. 動的なブランディングを使用するには、コミュニティを Audience + Salesforce Tabs テンプレートで構築する必要があります。
B. 動的なブランディングを使用する場合、コミュニティは顧客アカウントポータルテンプレートを使用して構築する必要があります。
C. Experience Cloud サイトで動的なブランディングを行うには、外部のコンテンツ管理システム (CMS) を使用する必要があります。
D. ブランドを表すために、URL にはエクスペリエンス ID (expid) またはプレースホルダーパラメータを使用する必要があります。
正解: **(**正解を表示します**)**
Dynamic branding in Experience Cloud relies on the Experience ID, sometimes carried as the expid parameter or equivalent placeholder in the URL, so Salesforce can render the right login experience for the selected brand. This is the scalable way to vary the look and feel without duplicating entire identity stacks. The community template choice can matter because not every template exposes branding capabilities the same way, but the central concept is still the Experience ID. External CMS tools are not required just to route the login experience by brand. From an architecture standpoint, this keeps the login framework centralized while letting the entry experience adapt to whichever brand, campaign, or sub-experience the user selected before authentication. This is why options B, D work together as the correct solution.

質問: **24**

Universal Containers社は、Salesforceへのシングルサインオンプロセスをサポートする既存のSecurity Assertion Markup Language(SAML)構成を使用して、Salesforce APIのセキュリティを強化したいと考えている。
どのSalesforce OAuth認証フローを使用すべきですか？
A. OAuth 2.0 JWTベアラーフロー
B. OAuth 2.0 SAML ベアラーアサーションフロー
C. OAuth 2.0 ユーザーエージェントフロー
D. SAMLアサーションフロー
正解: **(正解を表示します)**
If the organization already has a SAML setup and wants to obtain OAuth access to Salesforce APIs based on that existing federation trust, the correct bridge is the OAuth 2.0 SAML Bearer Assertion Flow. This flow allows a client to present a SAML assertion and exchange it for an OAuth access token. That is different from standard user-agent or JWT flows, and it is more specific than simply saying "SAML assertion" without naming the OAuth flow. The exam point is that SAML is being reused to obtain API authorization, not merely to log a person into the user interface. Salesforce documents this pattern specifically for environments that already depend on SAML and want to extend that trust into API access. This is why option B is the best answer in Salesforce terms.

質問: **25**
Universal Containers(UC)は、営業チームが社内ポータルにシームレスにログインできるように、CRMおよびIDプロバイダー(IdP)としてSalesforceを使用しています。
UCのITチームは現在、残りの従業員向けのIDプロバイダーとしてSalesforceを評価している。
この要件を満たすには、どのSalesforceライセンスが必要ですか？
A. 本人確認
B. 識別接続
C. 識別のみ
D. 外部識別子
正解: **(正解を表示します)**
The Identity Only license is designed for users who need Salesforce Identity services without broad CRM object access. Salesforce documentation positions it for scenarios where employees or other internal users need to authenticate with Salesforce credentials and access connected applications, but they do not require the full set of standard Salesforce business objects. That makes it a good fit for benefits portals, employee hubs, or third-party workforce apps that rely on Salesforce for identity rather than for CRM usage. External Identity is aimed at external audiences such as customers or partners, while Identity Connect is synchronization software rather than an end-user license. The licensing decision follows the user population and the scope of application access more than the authentication protocol itself. This is why option C is the best answer in Salesforce terms.

質問: **26**
管理者がSalesforce内のカスタムWebアプリケーション用の接続済みアプリを作成しましたが、このアプリはアプリランチャーにタイルとして表示される必要があります。しかし、Salesforceのすべてのユーザーのアプリランチャーに、このカスタムWebアプリケーションのタイルが表示されません。管理者は、この問題を解決するために、アイデンティティアーキテクトに支援を依頼しました。
この問題の原因となっている2つの理由は何ですか？
2つの回答を選択してください
A. この接続済みアプリのセッションポリシーは 高信頼性セッションが必要」に設定されています。
B. 接続されているアプリがアプリメニューで 「アプリランチャーに表示」に設定されていません。
C. 接続済みアプリの規約が接続済みアプリの設定で設定されていません。
D. 取得スコープに openid」が含まれていません。
正解: **(**正解を表示します**)**
For a connected app to appear as a tile in the Salesforce App Launcher, two things generally matter: the app must be marked visible in the App Launcher, and the connected app configuration must include the required launch details such as the start URL or equivalent launch settings. High-assurance session requirements or OIDC scopes do not by themselves control whether the tile shows up. The absence of a launch target can keep the app from being presented meaningfully to users even when the connected app exists. From an architecture and administration perspective, discovery in the launcher depends on app-visibility settings plus a valid launch configuration. Without those, users can be entitled to the app and still not see it in the launcher. This is why options B, C work together as the correct solution.

質問: **27**
Northern Trail Outfittersは、Salesforceプラットフォームを IDプロバイダー(IdP)と統合することで、シングルサインオン(SSO)を実現したいと考えています。
SalesforceとIDプロバイダー(IdP)間の信頼関係を確立するために、どの手順を実行すべきですか？
A. 安全な通信のために、SalesforceとIDプロバイダー間のVPN(仮想プライベートネットワーク)トンネルを設定します。
B. IDプロバイダーの認証コードをSalesforceのソースコードに直接埋め込む。
C. SalesforceとIdP間でメタデータXMLファイルを交換することにより、信頼関係を構成します。
D. ユーザー認証のためにSalesforceプラットフォーム内にカスタムログインページを作成します。
正解: **(**正解を表示します**)**

Trust between Salesforce and an identity provider is established by exchanging the metadata and certificates that define each side of the federation relationship. In Salesforce SAML setups, this commonly means importing or exchanging metadata XML so each side knows the issuer, endpoints, and signing certificate of the other. A VPN tunnel or custom login page does not create protocol-level trust for SSO. Embedding authentication code into Salesforce is not how federation is configured. The key concept from Salesforce documentation is that SAML trust is declarative and certificate-based: the two parties agree on metadata, endpoints, and certificates, and then assertions are validated against that trust configuration. That exchange is the foundation of a working Salesforce-IdP federation. This is why option C is the best answer in Salesforce terms.

質問: **28**
ユニバーサル ・コンテナ(UC)は、コンテナ卸売事業にSalesforce Experience Cloudサイトを利用している。
アイデンティティアーキテクトは、新しいサイトに認証プロバイダーを利用したいと考えている。
認証プロバイダーを作成する際に利用すべき2つのオプションはどれですか？
2つの回答を選択してください
A. デフォルトのログインユーザーを設定できます。
B. カスタムエラーURLを設定できます。
C. デフォルトの認証プロバイダー証明書を設定できます。
D. カスタム登録ハンドラを設定できます。
正解: **(**正解を表示します**)**
When creating an authentication provider in Salesforce, architects can configure operational settings that shape the user experience and downstream provisioning behavior. A custom error URL is supported so failed sign-ins can be routed to a branded or informative destination. A custom registration handler is also supported, giving the org control over how incoming identities are mapped to Salesforce users and related records. By contrast, options like a "default login user" or a generic default certificate setting do not describe the primary provider-creation controls in the same way. The important architecture concept is that an authentication provider defines both the trust with the external source and the user-lifecycle handling logic inside Salesforce. This is why options B, D work together as the correct solution.

質問: **29**
Northern Trail Outfitters (NTO) は、営業機会管理に Salesforce を使用しています。最近、NTO ユーザーのアプリケーションへのジャストインタイム (JIT) プロビジョニングと認証のために Okta が導入されました。Salesforce ユーザーは、Okta を使用して、予測 Web アプリケーションがユーザーに代わって Salesforce レコードにアクセスすることを承認しています。

Salesforceはどのような2つの役割を果たしていますか？
2つの回答を選択してください
A. OAuthリソースサーバー
B. SAMLサービスプロバイダー
C. OAuthクライアント
D. SAML IDプロバイダー
正解: **(**正解を表示します**)**
In this design, Salesforce plays two separate identity roles. Because Okta authenticates the workforce and sends users into Salesforce via federation, Salesforce is acting as the SAML service provider. At the same time, when the forecasting web application asks users to authorize access to Salesforce records, Salesforce is the OAuth resource owner's platform and the external application is the client. From Salesforce's perspective in that authorization exchange, it participates as the OAuth authorization platform and the ecosystem around it treats Salesforce as the protected resource. The important exam distinction is that one platform can play different identity roles in different flows. Here, Salesforce accepts a SAML assertion for login and also participates in an OAuth pattern for delegated data access. This is why options B, C work together as the correct solution.

質問: **30**
大手消費財企業がコミュニティの構築を計画しており、顧客のソーシャルIDによるログインを必須とする予定です。以下の要件を満たす必要があります。
1. 顧客は自身のソーシャルIDのいずれかを使用してログインできる必要がありますが、Salesforceでは顧客ごとに1人のユーザーのみが許可される必要があります。
2. 顧客がソーシャルIDで識別された後は、Salesforceへの承認は不要となるべきである。
3. 顧客がソーシャルIDを使用してSalesforceにログインする際に、ソーシャルサインオンから顧客の個人情報を取得する必要があります。
3. 顧客がソーシャルサイトで個人情報を変更した場合、その変更はSalesforceにも反映される必要があります。
アイデンティティアーキテクトが要件を満たすことができる2つの選択肢はどれですか？
2つの回答を選択してください
A. ログインフローを使用して認証登録ハンドラーを呼び出し、コミュニティにユーザーをログインさせる前にユーザーをプロビジョニングします。
B. カスタム登録ハンドラーを使用して、ソーシャル ID を Salesforce ID にリンクします。
C. ソーシャルサインオンには認証プロバイダーを使用し、個人情報の挿入または更新にはカスタム登録ハンドラーを使用します。
D. ユーザーをカスタムページにリダイレクトし、ユーザーが既存のソーシャルIDを選択してログインできるようにします。
正解: **(**正解を表示します**)**

When customers can authenticate with multiple social identities but Salesforce must maintain only one user record per person, the logic belongs in the authentication provider and registration-handler pattern.
Authentication providers handle the external trust with the social platforms, while a custom registration handler can locate an existing Salesforce identity, link the new social identity to it, and update profile details if the source data changes. Login flows are not the primary mechanism for social identity linking, and forcing the user through an extra selection page creates unnecessary friction. In Salesforce CIAM, the registration handler is the lifecycle control point: it decides whether to create, update, or link the user so the portal maintains a single consolidated identity per customer. This is why options B, C work together as the correct solution.

質問**: 31**
Northern Trail Outfitters (NTO) の部門が Salesforce を買収しました。NTO は、サードパーティの ID プロバイダー (IdP) を使用して、ユーザーの認証情報を自社の軽量システムと照合して検証しています。
ディレクトリアクセスプロトコル(LDAP)ディレクトリ。NTOは、従業員が覚えるパスワードの数をできるだけ少なくすることを支援したいと考えています。
アイデンティティ ·アーキテクトは何を推奨すべきでしょうか？
A. Salesforce Connect を使用して LDAP パスワードを Salesforce に同期します。
B. Salesforce を既存の IdR の認証プロバイダーとして設定します。
C. Salesforce を IdP として設定し、LDAP ディレクトリに対して認証を行います。
D. 既存の IdP に対して Salesforce をサービス プロバイダーとして設定します。
正解**: (**正解を表示します**)**
When a third-party enterprise identity provider already validates users against LDAP and the organization wants employees to remember as few passwords as possible, Salesforce should be configured as the service provider. That lets the existing IdP remain the authoritative login system while Salesforce trusts the resulting assertion. Salesforce Connect is unrelated to password synchronization, and making Salesforce the IdP would invert the current enterprise architecture. This is a classic workforce SSO pattern: the corporate identity layer owns credentials, and Salesforce consumes that identity through federation. The architectural win is reduced password sprawl. Users authenticate once against the enterprise identity provider and then reach Salesforce without maintaining a separate Salesforce password. This is why option D is the best answer in Salesforce terms.

有効的な**Identity-and-Access-Management-Architect-JPN**問題集はJPNTest.com提供され、**Identity-and-Access-Management-Architect-JPN**試験に合格することに役に立

ちます！JPNTest.comは今最新**Identity-and-Access-Management-Architect-JPN**試験問題集を提供します。JPNTest.com Identity-and-Access-Management-Architect-JPN試験問題集はもう更新されました。ここで**Identity-and-Access-Management-Architect-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/Identity-and-Access-Management-Architect-JPN-mondaishu　**112**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」

質問: **32**
Northern Trail Outfitters(NTO)は、従業員のユーザー名、パスワード、アクセス権限、および資産へのアクセス管理にMicrosoft Active Directory(AD)を活用しています。また、NTOはサードパーティ製のシングルサインオン(SSO)ソリューションも所有しています。このサードパーティ製SSOソリューションは、Salesforceを含むすべての企業アプリケーションで使用されています。
NTOは、Salesforceにおけるユーザーの自動プロビジョニングおよびデプロビジョニングのために、Salesforce Identity Connectの活用を検討するよう、アーキテクトに依頼した。
提示された要件において、Identity Connectはどのような役割を果たしますか？
A. シングルサインオン
B. IDプロバイダー
C. サービスプロバイダー
D. ユーザー管理
正解: **(**正解を表示します**)**
Identity Connect can synchronize several Salesforce security constructs from Active Directory-driven administration, particularly the identity and authorization artifacts attached to users. Profiles and permission sets are directly relevant because they define user capabilities in Salesforce. Roles also matter because they shape record access and hierarchy behavior. Public groups can participate in permission design and assignment patterns as well. By contrast, sharing rules and permission set licenses are not the core mapping focus in the same way. The main architectural takeaway is that Identity Connect is about translating directory- based user management into Salesforce access structures, especially those that determine who a user is, what they can do, and where they sit in the org's access model. This is why option D is the best answer in Salesforce terms.

質問: **33**
Universal Containers(UC)は現在、Salesforce Sales Cloudと外部の請求アプリケーションを使用しています。Salesforceと請求アプリケーションはどちらも、顧客管理のために1日に複数回アクセスされます。UCはシングルサインオンを設定し、SalesforceをIDプロバイダーとして活用したいと考えています。さらに、Salesforceから請求アプリケーションにアクセスできるようにしたいと考えています。リダイレクトでも構いません。
要件を満たすために、アイデンティティアーキテクトはどの2つのSalesforceツールを推奨すべきでしょうか？

2つの回答を選択してください
A. Salesforce Canvas
B. エイジランチャー
C. アイデンティティコネクト
D. つながりの時代
正解: **B,D (**コメントを発表する**)**
When Salesforce is acting as an identity provider and the goal is to make a third-party application available from within Salesforce, two standard tools work together: a connected app to define trust and single sign-on behavior, and the App Launcher to give users a discoverable entry point. The connected app handles the identity relationship and protocol settings, while the launcher exposes the application from the Salesforce UI.
Delegated Authentication and external data sources solve different problems and don't provide the same app- launch experience. In Salesforce Identity architecture, this combination is common because it aligns governance and usability: the app is centrally configured through a connected app and then delivered to users as part of their Salesforce app catalog. This is why options B, D work together as the correct solution.

質問: **34**
Universal Containers(UC)は、自社開発の顧客ポータルをSalesforce Experience Cloudに置き換えることを決定しました。UCは、顧客およびパートナーの認証情報をすべて保存するサードパーティ製のシングルサインオン(SSO)ソリューションは引き続き使用します。
顧客が初めてシングルサインオン(SSO)経由でExperience Cloudサイトにログインする際には、ユーザーレコードが自動的に作成される必要があります。
ログイン時にSalesforceでユーザーを自動的にプロビジョニングするために、アイデンティティアーキテクトはどのソリューションを推奨すべきでしょうか？
A. サードパーティのAppExchangeソリューション
B. カスタムミドルウェアとウェブサービス
C. ジャストインタイム(JIT)プロビジョニング
D. カスタムログインフローとApexハンドラー
正解: **(**正解を表示します**)**
Just-in-Time provisioning is designed for exactly this onboarding pattern: a user authenticates through an external identity provider, and Salesforce creates the user automatically on first successful login. That avoids preloading every external user into Salesforce before they ever visit the site. Middleware and custom web services can do similar work, but JIT is the native, lower-complexity mechanism built into Salesforce federation. Login flows by themselves do not create the user record during the authentication handshake. The architectural value of JIT is that it keeps the source of identity external while letting Salesforce create and update the user only when the person actually needs access. It is efficient, standard, and commonly used with Experience Cloud. This is why option C is the best answer in Salesforce terms.

質問: **35**
Universal Containers社は、Salesforce IdentityとOAuth 2.0ユーザーエージェントフローを使用してセキュリティを確保するモバイルアプリケーションを開発しています。アプリケーションユーザーは、ユーザー名とパスワードを使用して認証を行います。モバイルアプリ内でAPIアクセスを承認したり、3か月間再認証を求められたりすることはありません。
このユースケースを満たすために、接続されたアプリのオプションのうち、どの2つを設定する必要がありますか？
2つの回答を選択してください
A. Sealstonタイムアウト値を3ヶ月に設定します。
B. 許可されたユーザーを すべてのユーザーが自己承認できます」に設定します。
C. 許可されたユーザーを 管理者が承認したユーザーは事前承認済み」に設定します。
D. リフレッシュトークンポリシーを設定して、リフレッシュトークンを3か月後に期限切れにします。
正解: **(**正解を表示します**)**
For a mobile app using the user-agent flow, two connected-app controls work together when the business wants a long-lived session without repeated approval prompts. First, the app should be set to Admin Approved Users Are Pre-Authorized so users are not asked to approve API access inside the mobile experience. Second, the refresh-token policy should be configured for the required lifetime, such as three months, so the app can keep renewing access without forcing the user to log in again. A session timeout controls the UI session but not the refresh-token lifecycle in the same way. The architectural point is that user consent suppression and durable reauthentication behavior are governed by separate connected-app policies.
This is why options C, D work together as the correct solution.

質問: **36**
ある広告会社の最高マーケティング責任者(CMO)が、Salesforce Experience Cloud上で同社のログインおよび登録エクスペリエンスを構成するためのSalesforceの標準機能について話し合うため、アイデンティティおよびアクセス管理(IAM)の専門家を招いた。
最高マーケティング責任者(CMO)は、ログインページに会社のロゴ、背景色、ログインボタンの色、および外部URLからの動的な右フレームを反映させたブランドイメージを構築したいと考えています。
IAMスペシャリストは、どの2つの解決策を推奨すべきでしょうか？
2つの回答を選択してください：
A. ログインページと登録ページは、コミュニティ管理設定でブランド化できます。
B. パスワードのリセットとパスワードを忘れた際の機能のためのカスタムサイトページを作成します。
C. 経験豊富なクラウドとして要件を処理するためのカスタムページを作成します。

D. Experience Builder を使用して、ブランド化されたパスワードリセットおよびパスワード忘れページを作成します。
正解: **(**正解を表示します**)**
Salesforce Experience Cloud includes out-of-the-box branding options for login and registration experiences, and those can be extended through Experience Builder for related pages such as forgot-password and reset- password journeys. The standard site administration and branding controls can cover logos, colors, and certain visual treatments of the login page. Where the business wants branded password-management pages as well, Experience Builder is the supported way to build those experiences consistently. That is better than creating fully custom pages for everything unless the requirement truly goes beyond what the platform supports. The architecture point is to use the built-in branding framework first and extend through Experience Builder where branded identity pages are needed. This is why options A, D work together as the correct solution.

質問: **37**
Northern Trail Outfittersは、Experience Cloud上に構築されたB2C(企業対消費者)ポータルで、顧客が自分で登録できるようにしたいと考えています。アイデンティティアーキテクトは、個人アカウントを使用することを推奨しています。
個人アカウントを使用した自己登録を有効にするには、どの3つの手順を設定する必要がありますか？
3つの回答を選択してください
A. 設定ページでビジネスアカウントを有効にします。
B. 設定ページで個人アカウントを有効にします。
C. ログインと登録の設定で、デフォルトのアカウントフィールドが空であることを確認してください。
D. 公開アクセス設定で、個人およびビジネスアカウントレコードタイプへのアクセスを有効にします。
E. 連絡先の組織全体のデフォルト共有を 公開読み取り専用」に設定します。
正解: **(**正解を表示します**)**
For Experience Cloud self-registration with Person Accounts, Salesforce requires the org and site configuration to line up with how external users are created. Person Accounts must first be enabled at the org level. On the site, the default account field must be left blank so the self-registration process doesn't force users into a shared business account model. Public access settings also need access to the relevant Person Account and business account record types so the registration process can create the right record. This is the documented pattern when self-registration is meant to create people as customers rather than contacts under a standard account. The key idea is that registration must be allowed to create the correct account model from the start. This is why options B, C, D work together as the correct solution.

質問: **38**
ある消費財メーカーは、注文情報を含む顧客情報の管理にSalesforceを利用しています。同社はSalesforce Experience Cloudを使用して顧客向けポータルソリューションを導入し、顧客は自身の認証情報でログインできるようになりました。同社は、ユーザーがFacebookまたはLinkedInの認証情報でログインできるようにすることも検討しています。
有効化されると、Salesforceはどのような役割を果たすのでしょうか？
A. FacebookとLinkedInがこのSPになります。
B. FacebookとLinkedInはLIPSとSPとして機能します。
C. Salesforce がサービスプロバイダー (SP) になります。
D. Salesforce が ID プロバイダー (LIP) になります。
正解: **(正解を表示します)**
When customers sign in to an Experience Cloud site with Facebook or LinkedIn credentials, Salesforce is consuming identity from those providers. In federation terms, that means Salesforce is the service provider and the social platforms are acting as the identity providers. This is a foundational identity concept and helps explain why the configuration happens through authentication providers in Salesforce. Salesforce is not issuing the social credential; it is trusting the identity assertion or token from the external provider and then creating or locating the user locally. Understanding that role assignment is important because it determines where trust is configured, where profile data originates, and how the registration handler fits into the login process. This is why option C is the best answer in Salesforce terms.

質問: **39**
Northern Trail Outfitters (NTO) は、セキュリティアサーションマークアップ言語 (SANL) ベースのアイデンティティプロバイダー (IdP) を使用して、すべてのシステムで従業員の認証を行っています。IdP は、軽量ディレクトリアクセスプロトコル (LDAP) ディレクトリに対してユーザーを認証し、ユーザー情報にアクセスできます。NTO は、Salesforce を必要とするユーザーはごく一部であるため、Salesforce ライセンスの使用を最小限に抑えたいと考えています。
新入社員が既存のIDプロバイダーを使用してSalesforceにすぐにアクセスできるようにするには、どのような対策が推奨されますか？
A. 定期的に LDAP を消去し、Salesforce に新しいアクティブ ユーザーを作成する統合を構築します。
B. SANL属性を使用して自動時間プロビジョニングを設定し、新しいユーザーがSalesforceにログインしようとしたときに必要に応じて新しいSalesforceユーザーを作成します。
C. 管理者がSalesforceで新しいユーザーを手動で作成するプロセスを定義します。
D. LDAP を消去し、Salesforce に新しい非アクティブ ユーザーを作成し、ログイン フローを使用して初回ログイン時にユーザーをアクティブ化する統合を構築します。
正解: **(正解を表示します)**

Just-in-Time provisioning is designed for exactly this onboarding pattern: a user authenticates through an external identity provider, and Salesforce creates the user automatically on first successful login. That avoids preloading every external user into Salesforce before they ever visit the site. Middleware and custom web services can do similar work, but JIT is the native, lower-complexity mechanism built into Salesforce federation. Login flows by themselves do not create the user record during the authentication handshake. The architectural value of JIT is that it keeps the source of identity external while letting Salesforce create and update the user only when the person actually needs access. It is efficient, standard, and commonly used with Experience Cloud. This is why option B is the best answer in Salesforce terms.

質問: **40**
アイデンティティアーキテクトが、外部ユーザー向けにモバイルファーストの消費者向けアイデンティティアクセス管理(CIAM)を実装している。
ユーザー認証のみが必須要件です。ユーザー名として、ユーザーのメールアドレスまたは携帯電話番号がサポートされている必要があります。
この要件を満たすために必要なライセンスはどれですか？(2つ選択)
2つの回答を選択してください
A. 外部IDライセンス
B. メール認証クレジット
C. Identity Connect ライセンス
D. SMS認証クレジット
正解: **A,D (**コメントを発表する**)**
For a mobile-first external identity use case, Salesforce requires both the right base license and the right verification channel entitlement. External Identity licenses support authentication for external users such as consumers, while SMS verification credits support sending one-time verification codes to mobile phones for passwordless or verification-based login experiences. Email verification credits would address email delivery, not SMS-based verification. Identity Connect is unrelated because it is an AD synchronization product for workforce identity, not a CIAM licensing option. The architecture requirement here is straightforward:
external users authenticate to Salesforce-backed digital experiences, and mobile number verification is part of the sign-in model. That combination points to External Identity plus SMS verification capacity. This is why options A, D work together as the correct solution.

質問: **41**
Universal Containers社は、Salesforceと外部ディレクトリサービスを統合するIDアーキテクチャを設計しています。この外部ディレクトリサービスは、組織内の複数のシステムにわたるユーザー認証と認可のための中央リポジトリとして機能します。

Salesforceと外部ディレクトリサービス間の信頼関係を確立するために、どの手法を評価すべきでしょうか？
A. システム全体でユーザー認証にメールベースの検証を利用します。
B. 2 つのシステム間でユーザー認証情報を同期するために、共有データベース テーブルを使用します。
C. Salesforce および外部ディレクトリ サービスに対する IP ベースのアクセス制限を適用します。
D. SANL (Security Assertion Markup Language) に基づくフェデレーション型アイデンティティソリューションを実装します。
正解: **(**正解を表示します**)**
When an external directory service is intended to remain the central source for authentication and authorization across systems, the right architecture to evaluate is federation rather than password synchronization or database sharing. SAML is one of the standard ways Salesforce establishes that federated trust with an enterprise identity system. Email verification and IP restrictions can complement security, but they do not create single sign-on or shared identity trust. A shared credential table is also not an acceptable identity architecture. The important design principle is that Salesforce should trust the external identity service through standards-based federation and allow that system to remain authoritative for authentication.
That is precisely the problem SAML-based federation is designed to solve. This is why option D is the best answer in Salesforce terms.

質問: **42**
Universal Containersは、ハイブリッドモバイルアプリを使用して、従業員がモバイルデバイスからSalesforceにアクセスし、日常業務を行うことを可能にします。このアプリはモバイルソフトウェア開発キット(SDK)を使用し、必要に応じてリフレッシュトークンを活用してアクセストークンを再生成し、プライベートアプリとして配布されます。
最高セキュリティ責任者は、従業員が過去1週間以内にそのデバイスからログインしていない場合、デバイスの再認証を義務付ける組織全体のコンプライアンスポリシーを展開している。
このポリシー変更に対応するために、どの接続済みアプリ設定を利用すべきでしょうか？
A. スコープ - この接続済みアプリの refresh_token スコープを拒否します。
B. 許可されたユーザー - 管理者に、最終ログイン日に基づいて許可されたユーザーのリストを維持するように依頼します。
C. セッションポリシー - 接続されたアプリのタイムアウト値を 7 日に設定します。
D. リフレッシュトークンポリシー - 7日間使用されなかった場合、リフレッシュトークンを失効させます。
正解: **(**正解を表示します**)**
When a mobile application uses refresh tokens to preserve login state, the strongest control for forcing re- verification after inactivity is the refresh token policy. Salesforce lets

administrators define when refresh tokens expire, including inactivity-based expiration. That is more aligned with the stated requirement than a generic session timeout, because the app renews access through the refresh token even after individual access tokens expire. Denying refresh_token scope would break the usability requirement, and manually maintaining permitted users would be operationally weak. The architecture question is about reauthentication after the device has been idle from an OAuth perspective. In Salesforce connected apps, that control sits with the refresh token policy, especially the "expire if not used for X days" style setting. This is why option D is the best answer in Salesforce terms.

質問: **43**
あるテクノロジー企業は、ユーザー向けにシングルサインオンログインを導入する計画を立てています。ユーザーがSalesforceにログインすると、ユーザーオブジェクトのカスタムフィールドにデータが自動的に入力されるようにする必要があります。
アイデンティティ ·アーキテクトは、どの2つのステップを推奨すべきでしょうか？
2つの回答を選択してください
A. 登録/処理インターフェースを実装します。
B. SessionManagement クラスを実装します。
C. Auth.SumIDHandler インターフェイスを実装します。
D. メソッドの作成と更新。
正解: **C,D (**コメントを発表する**)**
To populate custom fields on the User record during SSO, Salesforce expects the architect to use the SAML Just-in-Time handler pattern. That means implementing the appropriate JIT interface and supplying create and update methods that map incoming assertion data into Salesforce user attributes. Session management classes and generic registration-handler interfaces solve different problems. The JIT handler exists specifically so that user creation and user updates can occur at login time based on federation data. This is useful when the identity provider is the source of truth for workforce attributes and those values must be refreshed without manual administration. In short, the interface gives Salesforce the entry point, and the create/update methods carry out the field population logic. This is why options C, D work together as the correct solution.

質問: **44**
大手フィットネストラッカーメーカーが、顧客コミュニティの立ち上げ準備を進めている。同社は、顧客にコミュニティにログインしてもらい、フィットネスデバイスをプロフィールに接続してもらうことを目指している。顧客はコミュニティ内で、運動の詳細情報やフィットネスに関するアドバイスを得られるようになる予定だ。
この要件を満たすには、どちらを使用すべきでしょうか？
A. 名前付き認証情報
B. ログインフロー

C. OAuthデバイスフロー
D. OAuthアセットトークンフロー
正解**: (**正解を表示します**)**
The OAuth 2.0 Asset Token Flow is Salesforce's purpose-built answer for connected devices and IoT-style integrations. It is designed for assets that need to act on behalf of a physical device or asset record rather than a human user. That makes it the correct fit for sensors, GPS trackers, or smart devices that must securely post telemetry or create service actions in Salesforce. User-agent, web-server, or username-password flows are built around user identity or generic application access, not around a registered device/asset relationship. The architectural advantage of the asset token model is that it ties the authorization context back to the asset, which is exactly what you want when the platform must know which device generated the event or maintenance alert. This is why option D is the best answer in Salesforce terms.

質問**: 45**
Universal Containers社は、IDプロバイダーとしてSalesforceを、従業員経費管理システムとしてConcurを使用しています。人事部長は、従業員のConcurアカウントがSalesforce組織内で適切な承認を得た後にのみ作成されるようにしたいと考えています。
アイデンティティアーキテクトは、この要件を実装するために、どの3つのステップを用いるべきでしょうか。
3つの回答を選択してください
A. プロビジョニングフローに関連付けられたカスタムオブジェクトの承認プロセスを作成します。
B. プロビジョニングフローに関連付けられた UserProvisioningRequest オブジェクトに対する承認プロセスを作成します。
C. SalesforceでConcur用の接続済みアプリを作成します。
D. 接続されたアプリのユーザープロビジョニングを有効にします。
E. プロビジョニングフローに関連付けられたユーザーオブジェクトの承認プロセスを作成します。
正解**: (**正解を表示します**)**
Salesforce connected-app user provisioning can be combined with internal approval so downstream accounts are created only after the right business authorization is complete. The connected app must have user provisioning enabled, and the target application must be represented as a connected app in Salesforce. To control timing, the approval process should be associated with the provisioning request object that participates in the provisioning lifecycle rather than with the generic User object. That allows the organization to hold or approve the provisioning action itself. This pattern is useful when HR or compliance wants a formal checkpoint before external accounts are created. The architecture separates identity eligibility from final outbound provisioning execution. This is why options B, C, D work together as the correct solution.

有効的な**Identity-and-Access-Management-Architect-JPN**問題集はJPNTest.com提供され、**Identity-and-Access-Management-Architect-JPN**試験に合格することに役に立ちます！JPNTest.comは今最新**Identity-and-Access-Management-Architect-JPN**試験問題集を提供します。JPNTest.com Identity-and-Access-Management-Architect-JPN試験問題集はもう更新されました。ここで**Identity-and-Access-Management-Architect-JPN**問題集のテストエンジンを手に入れます。最新版のアクセス、https://www.jpntest.com/shiken/Identity-and-Access-Management-Architect-JPN-mondaishu ↑**112**問、３０%ディスカウント、特別な割引コード: **JPNshiken**」