

# Salesforce Certified Identity and Access Management Architect (Japanese Version)

1. ID アーキテクトは、外部システムから Salesforce へのユーザーのプロビジョニングとプロビジョニング解除をどのように自動化する必要がありますか？

A. ユーザー オブジェクトで SOAP API upsertQ を呼び出します。

B. 着信 SAML アサーションで Security Assertion Markup Language Just-in-Time (SAML JIT) を使用します。

C. 着信 OAuth 応答で登録ハンドラーを実行します。

D. 有効なアクセス トークンを使用して OpenID Connect (OIDC)-userinfo エンドポイントを呼び出します。

Answer(s): C

---

2. ユニバーサル コンテナ (UC) には、認証に Facebook を使用するカスタマー コミュニティがあります。UC は、Facebook プロファイルの変更が適切な顧客コミュニティ ユーザーに反映されるようにしたいと考えています。この要件はどのように満たすことができますか？

A. 登録ハンドラ クラスで updateuser() メソッドを使用します。

B. Facebook と Salesforce の間で SAML ジャストインタイム プロビジョニングを使用する

C. Facebook から受信した署名付きリクエストの情報を使用します。

D. 毎晩 Facebook を呼び出すスケジュール ジョブを開発します。

Answer(s): C

---

3. ユニバーサル コンテナ (UC) は、自己登録ページを使用すると、「ボット」または意図しないオーディエンスがユーザー レコードを作成する手段を提供し、それによってライセンスが消費され、ダーク データが追加されることを懸念しています。自己登録プロセス中に不正なフォーム送信を防止するために UC が取るべき 2 つのアクションはどれですか? 選ぶ

A. 自由回答式の秘密の質問と複雑なパスワード要件を使用する

B. 主に自己登録ページのルックアップ フィールドとピックリスト フィールドを使用します。

C. 自己登録プロセスの最後にキャプチャを要求します。

D. 自己登録ページの Java スクリプト イベントによって入力された非表示フィールドを使用します。

**Answer(s): C,D**

---

4. ユニバーサル コンテナ (UC) は、パートナー コミュニティを実装したいと考えています。実装の一環として、UC は、パートナー コミュニティ ユーザー向けのカスタム ブランディングを使用して、パスワードを忘れた場合とパスワードを変更するエクスペリエンスの両方を変更したいと考えています。アーキテクトが UC に推奨すべき 2 つのアクションはどれですか? 2 つの答えを選択してください

A. パスワード変更エクスペリエンス用のコミュニティ ビルダー ページと、パスワードを忘れた場合のカスタム Visualforce ページを作成します。

B. パスワードの変更とパスワードを忘れた場合の両方のエクスペリエンスのカスタム Visualforce ページを作成します。

C. パスワード変更エクスペリエンス用のカスタム visualforce ページと、パスワードを忘れた場合のコミュニティ ビルダー ページを作成します。

D. パスワードの変更とパスワードを忘れた場合の両方のエクスペリエンスのコミュニティ ビルダー ページを作成します。

**Answer(s): B,C**

---

5. Universal Containers (UC) は、ID プロバイダーとして機能し、Salesforce へのログインに使用される SAML アサーションを生成するカスタム アプリケーションを使用しています。UC は、SAML アサーションにカスタム パラメーターを含めることを検討しています。これらの属性には機密データが含まれており、ユーザーを認証するために必要です。アサーションは、プラ

ウザ フォーム ポストを介して Salesforce に送信されます。大多数のユーザーは UC の企業ネットワーク経由でのみ Salesforce にアクセスできますが、一部の管理者と幹部はモバイル デバイスで企業ネットワークの外部からアクセスできます。転送中に機密データが改ざんされたり、誰もアクセスできないようにするためにアーキテクトが検討すべき 2 つの方法はどれですか？

A. ID プロバイダーの証明書を使用してデジタル署名し、Salesforce の証明書を使用してペイロードを暗号化します。

B. Salesforce の証明書を使用して、ユーザーのモバイル デバイスで SAML アサーションとモバイル デバイス管理クライアントにデジタル署名します。

C. ID プロバイダーの証明書を使用してデジタル署名し、ID プロバイダーの証明書を使用してペイロードを暗号化します。

D. アサーションに属性を含めずに、カスタム ログイン フローを使用して、Apex コールアウトを使用して機密データを取得します。

**Answer(s): C,D**

---

6. Universal Containers (UC) には、Idp を使用した SP 開始 SAML SSO 用に構成された既存の Salesforce 組織があります。2 番目の Salesforce 組織が環境に導入されており、IT チームは新しい組織に同じ Idp を使用できるようにしたいと考えています。2 番目の組織を実装する際に、IT チームはどのようなアクションを実行する必要がありますか？

A. 最初の組織と同じ SAML ID の場所を使用します。

B. 最初の組織とは異なるエンティティ ID を使用します。

C. 最初の組織と同じ要求バインディングを使用します。

D. Salesforce ユーザー名を SAML ID タイプとして使用します。

**Answer(s): B**

---

7. Identity Connect が可能な 2 つのステートメントはどれですか？ 2 つの答えを選択してください

A. Salesforce 権限セットのライセンス割り当ての同期。

B. ID プロバイダーが開始する SSO とサービス プロバイダーが開始する SSO の両方をサポートします。

C. 複数の Active Directory サーバーに接続する複数の組織をサポートします。

D. 自動化されたユーザー同期と無効化。

**Answer(s):** B,D

---

8. Universal Container's (UC) は、Salesforce Experience Cloud のサイトをコンテナ卸売事業に使用しています。ID アーキテクトは、新しいサイトの認証プロバイダーを必要としています。

A. カスタム登録ハンディを設定できます。

B. カスタム エラー URL を設定できます。

C. デフォルトのログインユーザーを設定できます。

D. デフォルトの認証プロバイダ証明書を設定できます。

**Answer(s):** A,B

---

9. Northern Trail Outfitters (NTO) には、セキュリティ アサーション マークアップ言語 (SAMI) や OAuth などのシングル サインオン標準をサポートしていない既存のカスタムの企業対消費者 (B2C) Web サイトがあります。NTO は、Salesforce Identity を使用して、Web サイトで新規顧客を登録および認証したいと考えています。

A. Identity Connect

B. 代理認証

C. 接続されたアプリ

D. 埋め込みログイン

**Answer(s):** B,D

---

10. Universal Containers (UC) は、自社開発の従業員ポータルを使用して、従業員が共同作業を行っています。UC は、Salesforce Ideas を使用して、従業員が従業員ポータルからアイデアを投稿できるようにすることにしました。ユーザーが従業員ポータルのリンクの一部をクリックすると、ユーザーは Salesforce にリダイレクトされ、認証され、関連するページが表示されます。このシナリオに最適な OAuth フローはどれですか？

A. Web アプリケーション フロー

B. SAML ベアラー アサーション フロー

C. ユーザーエージェントフロー

D. Web サーバーの流れ

Answer(s): D

---

11. ある不動産会社は、顧客が室内装飾のオプションを設計できるデジタル スペースを提供したいと考えています。

A. 宣言型の登録ハンドラー プロセス ビルダー/フローを使用して、ユーザーと連絡先を作成、更新します。

B. ソーシャルサインオン プロバイダーごとに認証プロバイダーの構成が必要です。コミュニティで認証プロバイダーを有効にします。

C. OIDC をサポートするには、セキュリティ アサーション マークアップ言語 (SAML) とジャスト インタイム プロビジョニング (JIT) および OAuth 2.0 を有効にする必要があります。

D. 登録ハンドラーがユーザーを作成および更新するには、Apex コーディングのスキルが必要です。

Answer(s): B,D

---

12. Universal Containers (UC) のセキュリティ チームは、レポートのエクスポートがリスクの高いアクションであると認識しており、その際、ユーザーが Active Directory (AD) 資格情報を使用して Salesforce にログインすることを要求したいと考えています。Salesforce の他のすべてのユーザーについては、AD 資格情報または Salesforce 資格情報を使用できるようにする必要があります。Salesforce 資格情報でログインしたときにレポートを表示する機能を維持しながら、AD 資格情報を使用してログインした場合を除き、レポートのエクスポートを防ぐために推奨されるソリューションはどれですか？

A. SAML Federated Authentication を使用し、Standard Assurance セッションを介してアクセスされたときにレポートへのアクセスをブロックします。

B. SAML フェデレーション認証とカスタム SAML JIT プロビジョニングを使用して、レポートのエクスポート アクセス許可を付与するアクセス許可セットを動的に、または削除します。

C. SAML フェデレーション認証を使用し、SAML セッションを高保証として扱い、レポートのエクスポートに必要なセッション レベルを上げます。

D. ログイン フローで SAML フェデレーション認証を使用して、レポートのエクスポート権限を付与する権限セットを動的に追加または削除します。

**Answer(s): C**

---

**13.** Universal Containers (UC) には、マーケティング キャンペーンのリードを収集するためのデスクトップ アプリケーションがあります。UC は、このアプリケーションを拡張して Salesforce と統合し、見込み客を作成したいと考えています。デスクトップ アプリケーションとセールスフォースの統合はシームレスである必要があります。アーキテクトが推奨する承認フローは？

A. JWT Bearer Tokenの流れ

B. Web サーバー認証の流れ

C. ユーザー エージェント フロー

D. ユーザー名とパスワードの流れ

**Answer(s): B**

---

**14.** Containers (UC) には既存のカスタマー コミュニティがあります。UC は、顧客が登録プロセス中に提供するデータに基づいて異なるコミュニティ体験を受け取ることができるように、自己登録機能を拡張したいと考えています。アーキテクトが UC に推奨すべき推奨アプローチは何ですか？

A. ユーザ オブジェクトに After Insert Apex トリガを作成して、特定のカスタム権限を割り当てます。

B. さまざまなコミュニティ ユーザー ペルソナに対応する個別のログイン フローを作成します。

C. コミュニティ ページを変更して、ユーザー レコードと連絡先レコードの特定のフィールドを利用します。

D. 既存のコミュニティ登録コントローラーを変更して、異なるプロフィールを割り当てます。

**Answer(s): C**

---

15. Universal Containers (UC) は、Force.com プラットフォーム上に新しい高機密アプリケーションを構築することを決定しました。UC のセキュリティ チームは、このアプリケーションに対する認証のために、ユーザー名とパスワードに加えて指紋も提供することをユーザーに求めることを決定しました。アーキテクトは、Salesforce 認証の識別形式として指紋をどのようにサポートできますか？

A. サードパーティの指紋スキャン アプリケーションへのコールアウトで Salesforce Two-Factor Authentication を使用します。

B. サードパーティの指紋スキャン アプリケーションへのコールアウトで委任認証を使用します。

C. ネイティブの Salesforce ID 確認で指紋スキャンを実行する AppExchange 製品を使用します。

D. サードパーティの指紋スキャン アプリケーションへのコールアウトを含むカスタム ログイン フローを使用します。

**Answer(s): D**

---

16. SAML を使用したシングル サインオン設定での ID プロバイダーの役割の 1 つは何ですか？

A. トークンの検証

B. トークンを作成

C. トークンを消費

D. トークンを取り消す

**Answer(s): B**

---

17. Northern Trail Outfitters (NTO) には、すべてのユーザー ログインに単一の多要素認証 (MFA) プロンプトが含まれるようにする必要があります。現在、ユーザーは、ユーザー名とパスワードを使用してログインするか、組み込みの MFA を含む NTO の企業 ID プロバイダーに対してシングルサインオンを介してログインするかを選択できます。

A. 「ユーザー インターフェイス ログイン用の MFA」を含む権限セットを作成し、すべての従業員に割り当てます。

B. MFA を適用するカスタム ログイン フローを作成し、権限セットに割り当てます。次に、権限セットをすべての従業員に割り当てます。

C. [設定] -> [本人確認] から組織の「ユーザー インターフェイス ログインの MFA」を有効にします。

D. すべての従業員プロファイルについて、[ログイン時に必要なセッション レベル] を [高保証] に設定し、企業 ID プロバイダーを組織のセッション セキュリティ レベルの [高保証] リストに追加します。

Answer(s): C

---

18. ID アーキテクトは、ユーザーが Experience Cloud サイト (以前のコミュニティ) ホームページに到達する前に、管理者がユーザーにパーソナライズされたアラート メッセージを構成できるようにするソリューションを推奨するよう求められました。

A. 登録ハンドラの Apex クラスをカスタマイズして、ユーザ プロファイルに基づいてさまざまなホームページに移動するルーティング ロジックを作成します。

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. カスタムアラートを表示するホームページ用の Lightning Web コンポーネント (LWC) を作成します。

D. ユーザー アラートを格納するカスタム 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。

Answer(s): B

---

19. Northern Trail Outfitters (NTO) は、Salesforce Experience Cloud に実装された Customer 360 Platform を使用しています。担当の開発チームは、連絡先情報のないユーザーを作成することで、顧客やパートナーの管理のオーバーヘッドを削減できる非接触型ユーザー機能について知りました。



A. 新しく登録された非接触型ユーザーに外部 ID またはコミュニティ ライセンスを正しく割り当てるには、カスタム登録ハンドラーが必要です。

B. 非接触ユーザーがコミュニティ ライセンスにアップグレードされた場合、連絡先レコードが自動的に作成され、ユーザー レコードにリンクされますが、アカウントには関連付けられません。

C. 非接触型ユーザー機能は、External Identity ライセンスでのみ使用できます。これにより、ユーザーが使用できる Experience Cloud 機能が制限される可能性があります。

D. ワンタイムパスワード (OTP) を受信する携帯電話は、連絡先レコードの番号と一致する必要があるため、パスワードレス認証はサポートできません。

**Answer(s): B**

---

20. 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。

A. Apex Just-in-Time ハンドラを使用して、標準の SAML 属性をクエリし、権限セットを設定します。

B. Apex Just-in-Time ハンドラを使用して、カスタム SAML 属性をクエリし、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 属性をクエリし、権限セットを設定します。

D. ログイン フローを使用して、標準の SAML 属性をクエリし、権限セットを設定します。

**Answer(s): B**

---