



salesforce

知っているようで意外と知らない？ Salesforceの認証

シングルサインオン 編

株式会社セールスフォース・ドットコム

プラットフォーム・スペシャリスト 塚本 直人

2020年06月22日

A stylized illustration of a forest scene. In the foreground, there are green bushes and small orange flowers. In the middle ground, there are several green coniferous trees. On the right side, a large, dark brown tree trunk is visible. The background is a light blue sky with soft white clouds.

Forward-Looking Statements



"Safe harbor" statement under the Private Securities Litigation Reform Act of 1995: This presentation contains forward-looking statements about the company's financial and operating results, which may include expected GAAP and non-GAAP financial and other operating and non-operating results, including revenue, net income, diluted earnings per share, operating cash flow growth, operating margin improvement, expected revenue growth, expected current remaining performance obligation growth, expected tax rates, stock-based compensation expenses, amortization of purchased intangibles, shares outstanding, market growth, environmental, social and governance goals and expected capital allocation, including mergers and acquisitions, capital expenditures and other investments. The achievement or success of the matters covered by such forward-looking statements involves risks, uncertainties and assumptions. If any such risks or uncertainties materialize or if any of the assumptions prove incorrect, the company's results could differ materially from the results expressed or implied by the forward-looking statements it makes.

The risks and uncertainties referred to above include -- but are not limited to -- risks associated with the effect of general economic and market conditions; the impact of geopolitical events, natural disasters and actual or threatened public health emergencies, such as the ongoing Coronavirus pandemic; the impact of foreign currency exchange rate and interest rate fluctuations on our results; our business strategy and our plan to build our business, including our strategy to be the leading provider of enterprise cloud computing applications and platforms; the pace of change and innovation in enterprise cloud computing services; the seasonal nature of our sales cycles; the competitive nature of the market in which we participate; our international expansion strategy; the demands on our personnel and infrastructure resulting from significant growth in our customer base and operations, including as a result of acquisitions; our service performance and security, including the resources and costs required to avoid unanticipated downtime and prevent, detect and remediate potential security breaches; the expenses associated with our data centers and third-party infrastructure providers; additional data center capacity; real estate and office facilities space; our operating results and cash flows; new services and product features, including any efforts to expand our services beyond the CRM market; our strategy of acquiring or making investments in complementary businesses, joint ventures, services, technologies and intellectual property rights; the performance and fair value of our investments in complementary businesses through our strategic investment portfolio; our ability to realize the benefits from strategic partnerships, joint ventures and investments; the impact of future gains or losses from our strategic investment portfolio, including gains or losses from overall market conditions that may affect the publicly traded companies within our strategic investment portfolio; our ability to execute our business plans; our ability to successfully integrate acquired businesses and technologies; our ability to continue to grow unearned revenue and remaining performance obligation; our ability to protect our intellectual property rights; our ability to develop our brands; our reliance on third-party hardware, software and platform providers; our dependency on the development and maintenance of the infrastructure of the Internet; the effect of evolving domestic and foreign government regulations, including those related to the provision of services on the Internet, those related to accessing the Internet, and those addressing data privacy, cross-border data transfers and import and export controls; the valuation of our deferred tax assets and the release of related valuation allowances; the potential availability of additional tax assets in the future; the impact of new accounting pronouncements and tax laws; uncertainties affecting our ability to estimate our tax rate; uncertainties regarding our tax obligations in connection with potential jurisdictional transfers of intellectual property, including the tax rate, the timing of the transfer and the value of such transferred intellectual property; the impact of expensing stock options and other equity awards; the sufficiency of our capital resources; factors related to our outstanding debt, revolving credit facility and loan associated with 50 Fremont; compliance with our debt covenants and lease obligations; current and potential litigation involving us; and the impact of climate change.

Further information on these and other factors that could affect the company's financial results is included in the reports on Forms 10-K, 10-Q and 8-K and in other filings it makes with the Securities and Exchange Commission from time to time. These documents are available on the SEC Filings section of the Investor Information section of the company's website at.

Salesforce.com, inc. assumes no obligation and does not intend to update these forward-looking statements, except as required by law.

Third party trademarks are the property of their owners.



THANK YOU

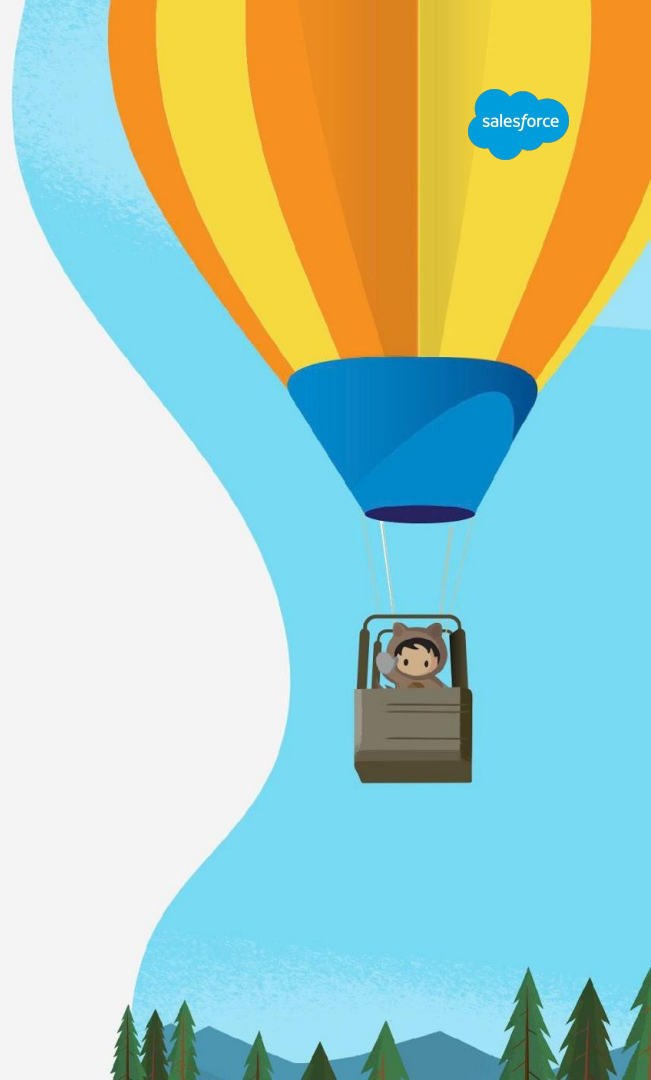


本ウェブセミナーの対象者

- これからSalesforceの管理者・開発者を始める方
- ID管理に携わる、携わる予定があるシステム管理者

本日のアジェンダ

1. 認証・認可について理解する
2. なぜシングルサインオンが必要なのか
3. Salesforce Identityの紹介
4. Salesforceのシングルサインオン
5. デモンストレーション



認証: 利用者が誰であることを確認すること



The image shows a Salesforce login interface. At the top is the Salesforce logo. Below it are two input fields: 'ユーザー名' (Username) and 'パスワード' (Password). Each field has a small icon on the right side. Below the password field is a blue 'ログイン' (Login) button. At the bottom, there is a checkbox for 'ログイン情報を保存する' (Save login information) and two links: 'パスワードをお忘れですか?' (Forgot your password?) and 'カスタムドメインを使用' (Use custom domain).

「誰？」

ユーザ名やメールアドレスなどシステムで一意に認識できる情報(ID)で、自分が誰であることを知らせる

「本当に〇〇さん?(確認)」

パスワードや生体認証など本人しか知り得ない・持ち得ない情報で本人であることを証明する

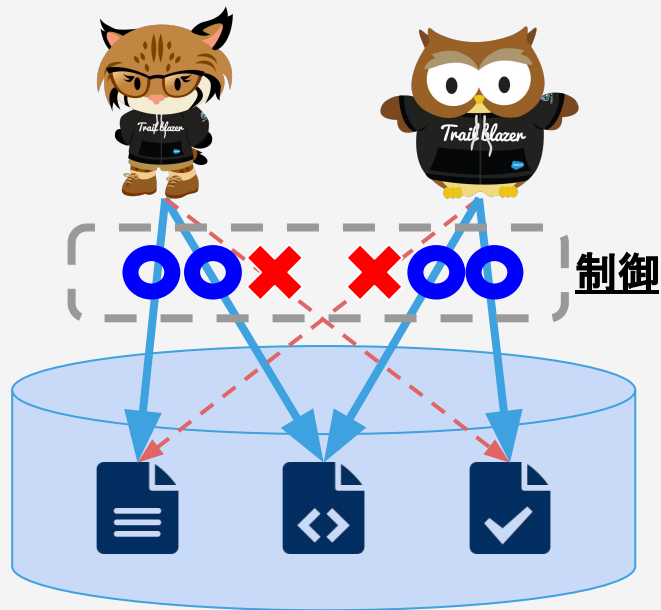
※2要素認証・多要素認証:

パスワードだけだと漏えいや総当たりによる「なりすまし」を防止するために複数の認証要素で多段的に認証を行う機能

例: YubiKey, SMSによる確認コード, Authenticator など

認可とは

認可: サービスの利用やリソースへのアクセス権限を与えること

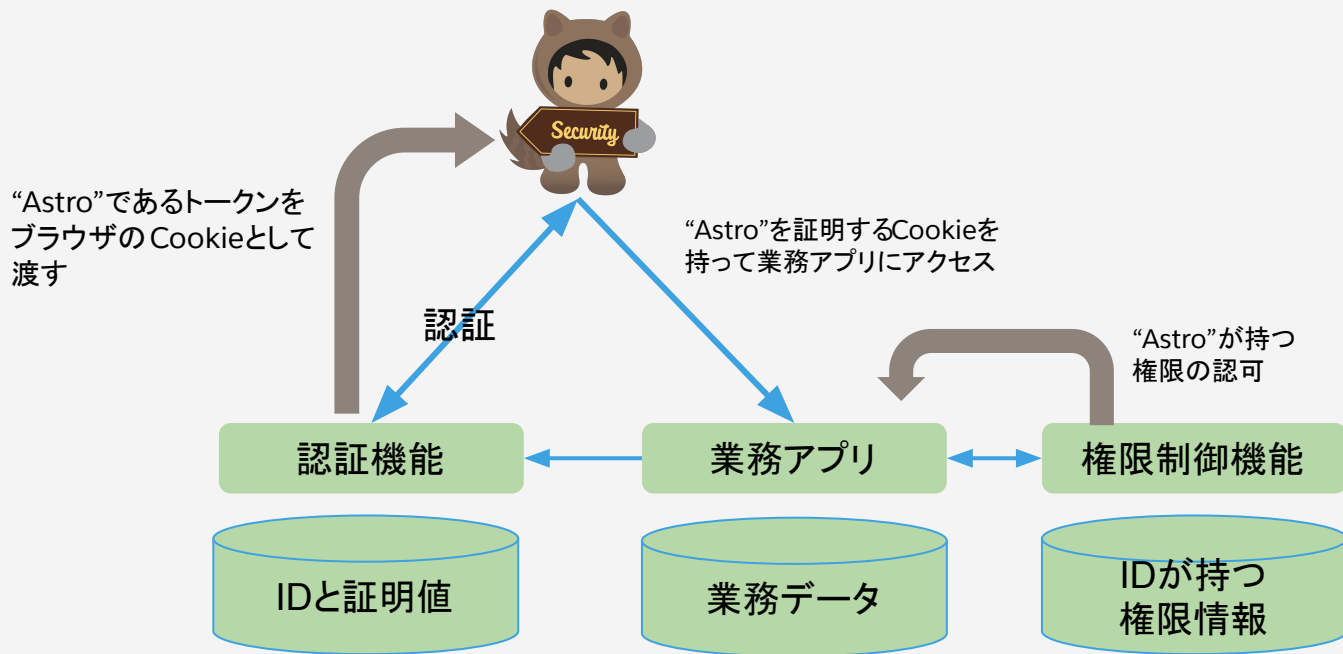


「認可」は制御の仕組み自体ではなく、仕組みに則って権限を「与える」こと



認証・認可とWebアプリケーションの仕組み

色々認証アーキテクチャはありますが、一つの例です

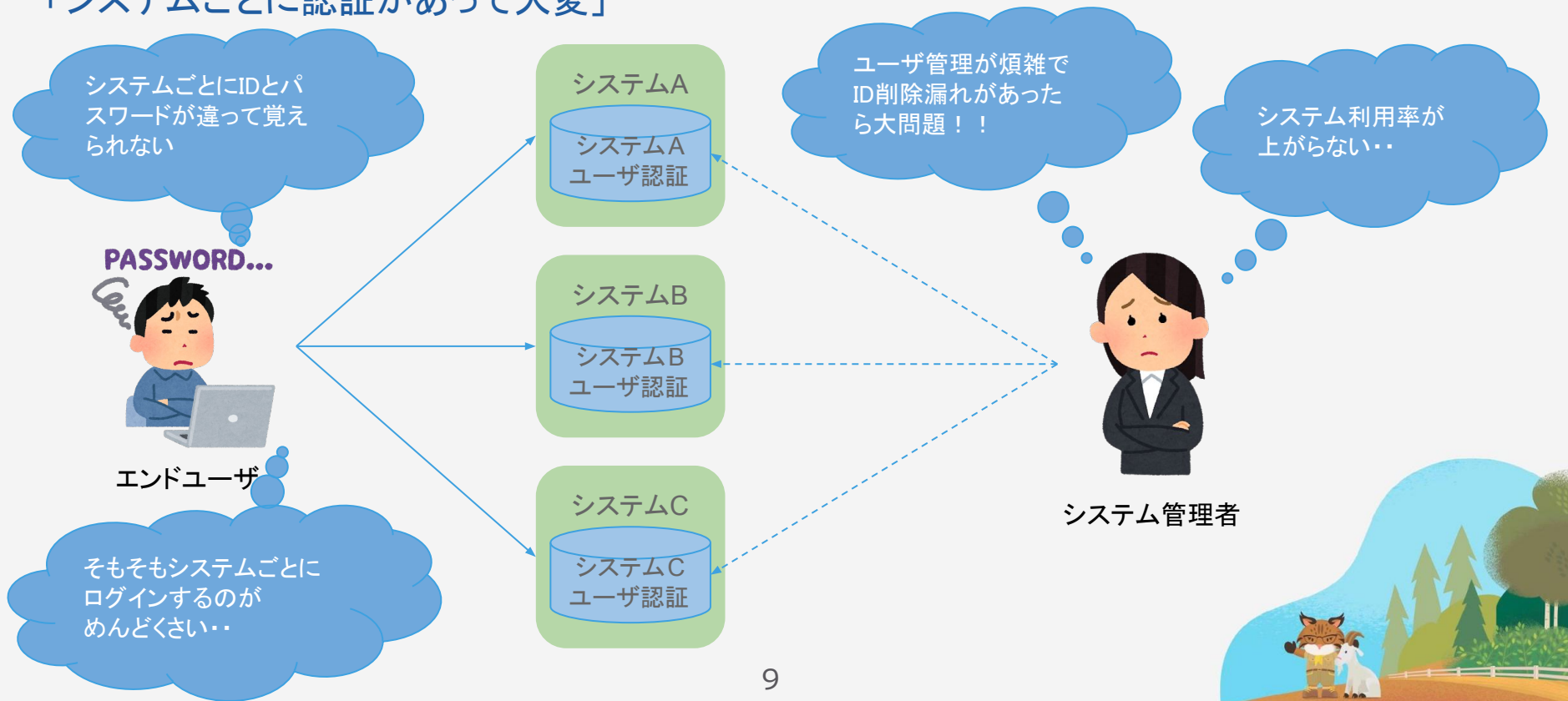


ユーザリポジトリ・ディレクトリ

認証・認可にまつわる課題

salesforce

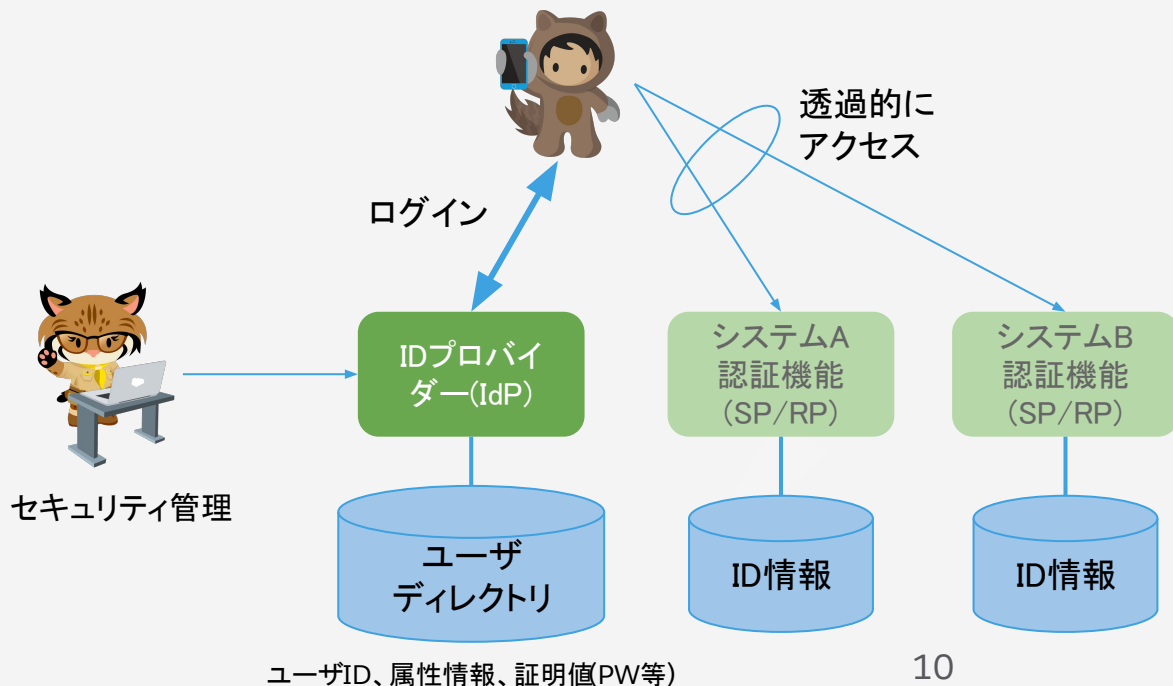
「システムごとに認証があって大変」



シングルサインオン (SSO / Single Sign-On)

煩雑なID・認証管理の課題を解決

ユーザは一度の認証作業で複数のサービスへアクセス可能



ユーザビリティ
管理効率性
セキュリティ

IdP: Identity Provider
SP: Service Provider
RP: Relying Party

シングルサインオンの実現方法

フェデレーション型がクラウド時代の主流

実現方法	特徴
エージェント型	SPとなるWebサーバに認証エージェントをインストール
リバースプロキシ型	SPとなるWebサーバの前段に認証サーバを配置
代理認証型	各認証システムのID/PW入力を代行
フェデレーション型	IdPとSP間でユーザ情報を連携



標準プロトコル

- SAML (Security Assertion Markup Language)
- OpenID connect



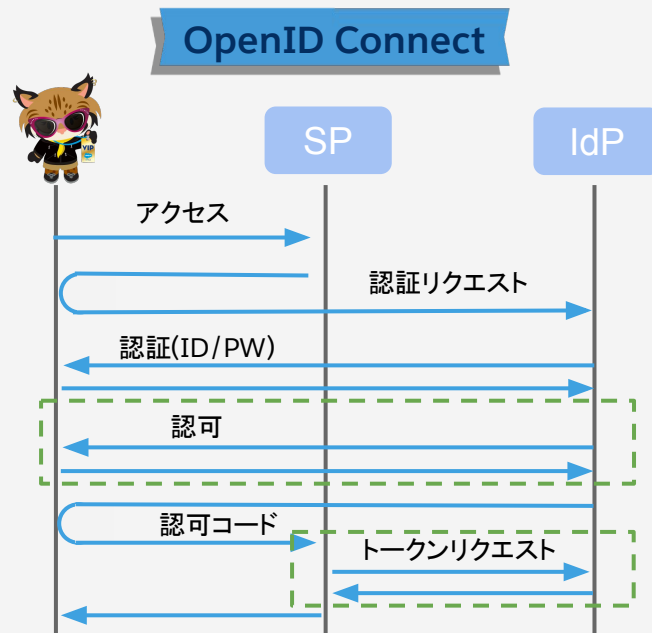
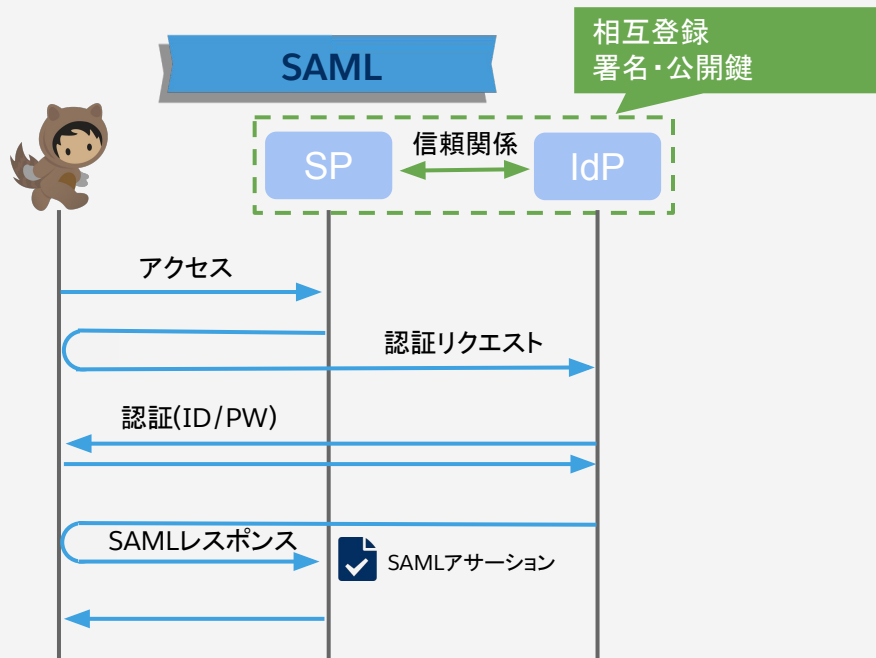
Salesforceでサポート

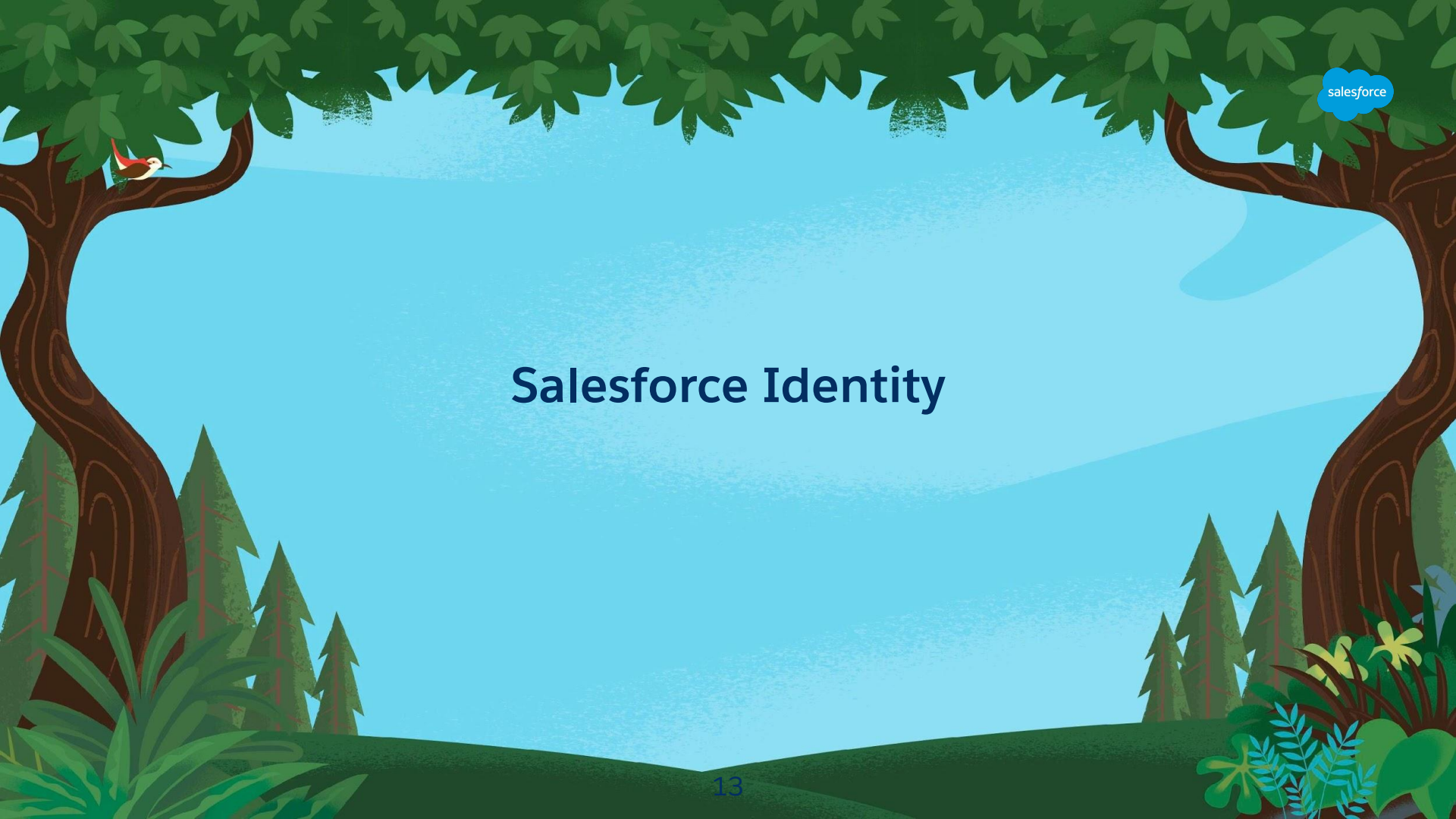
- 代理認証型
- フェデレーション型

SAMLとOpenID Connect



大きな違いは事前に信頼関係を作るかどうか



A stylized illustration of a forest scene. Two large, leafy green trees frame the top and sides of the image. In the background, there are rolling green hills and several tall, thin evergreen trees. The sky is a clear, light blue. The overall style is clean and modern.

Salesforce Identity

Salesforce Customer 360

salesforce

信頼・スマート・柔軟・持続可能



プラットフォーム



Identity for Employees

従業員にはシンプルさを、管理者にはセキュリティと制御を提供します



強化されたセキュリティ

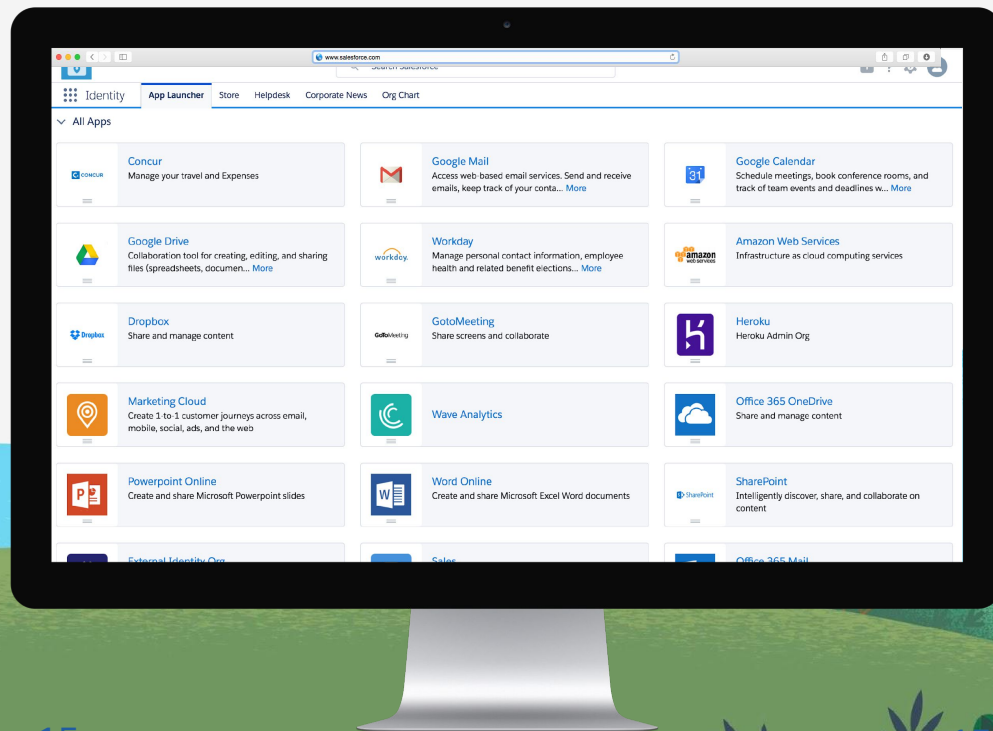
サードパーティアプリケーションとセキュアな統合

管理コストの削減

ユーザは1つのパスワードのみで各サービスへアクセス

Salesforce資産を活用

シングルロケーションからユーザ情報の
プロビジョニングと解除



Identity for Customers & Partners

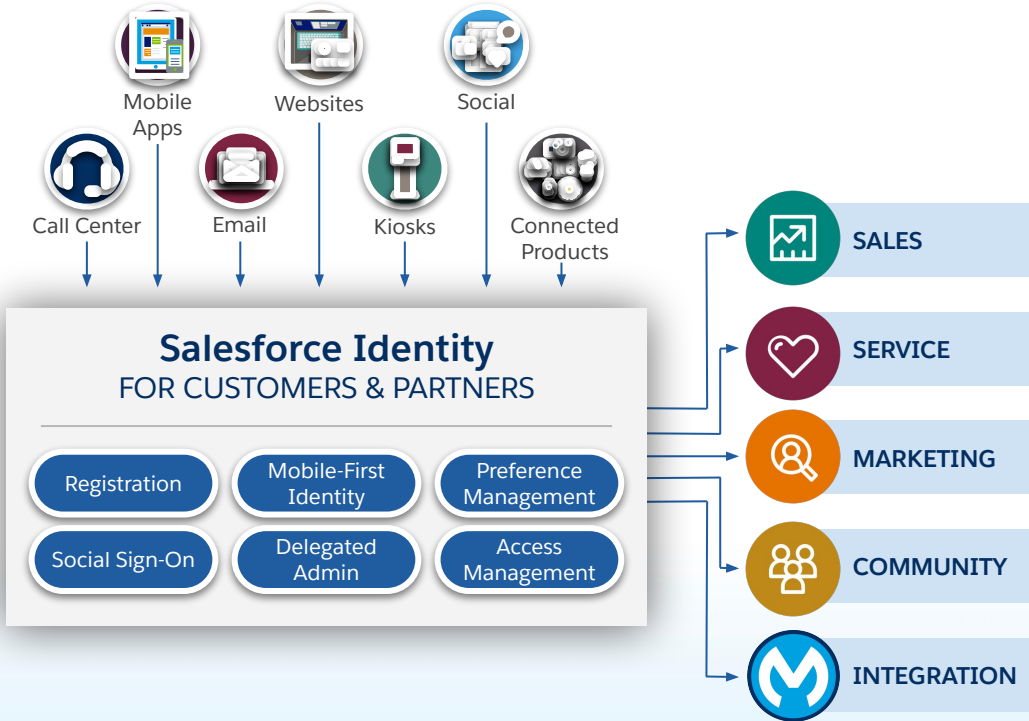
サイロ化されたIdentityデータの橋渡し

Consolidate 接続されたデバイスを含む複数のデータからIDを統合

Manage Salesforceで顧客IDとプロフィールを管理

Integrate 登録された顧客プロフィールとログインをSalesforceでのビジネスプロセスと統合

Personalize セールス、サービス、マーケティング全体でカスタマージャーニーをパーソナライズ

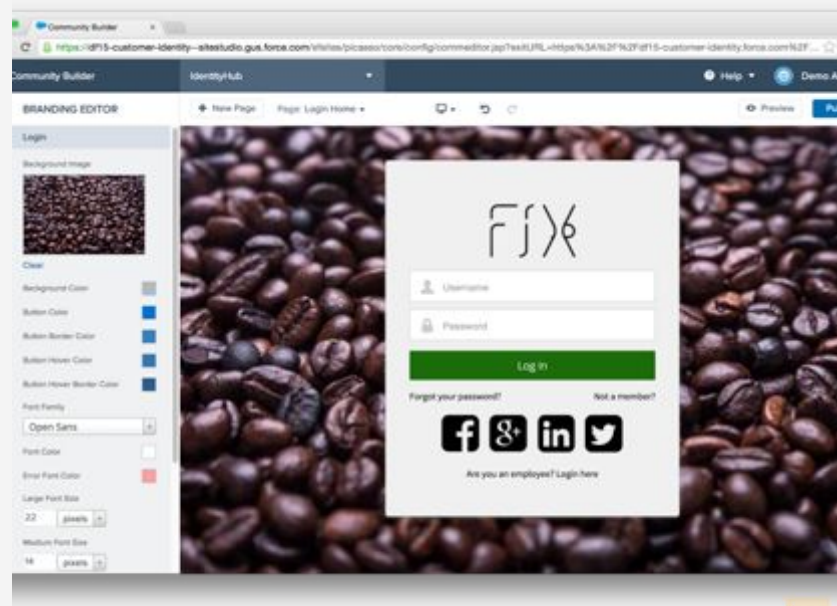


優れたユーザ・エクスペリエンス

ユーザ・ジャーニー全体でブランディング



- 宣言的およびプログラムによるブランディング
- ブランディングされたログイン画面
- ページビルダーを使用したポイント&クリックによる操作
- ウェルカムメニュー (“App Launcher”)
- セルフサービスプロフィール管理
- モバイルアプリからのログイン
- サービスEmailテンプレート (password reset…)
- カスタムドメイン設定 (URLs)



アプリケーションランチャーメニュー

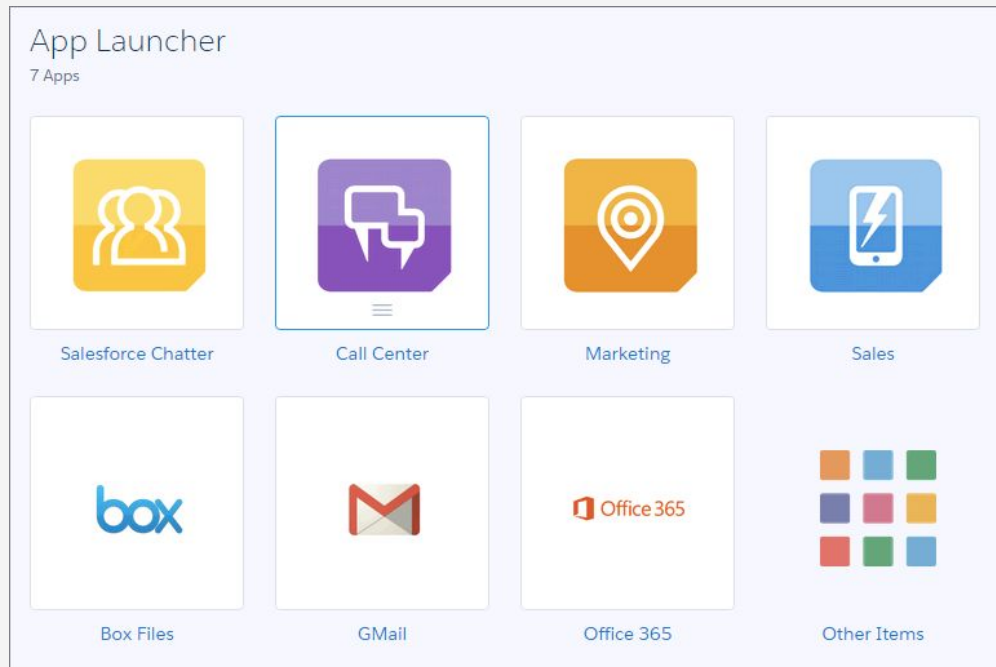
使いたいアプリケーションにすばやくアクセス

■ 利用の効果

- 使いたいアプリにすばやくアクセス(SSO)
- プロファイルor権限セットに紐付いた接続アプリケーションを表示
- タイルの並びはユーザーが自由に変更可能
- ユーザーはAppカタログの中から自分が利用したいアプリを選択し、メニューに追加することが可能
- 利用申請 & 承認処理も組み込み可能

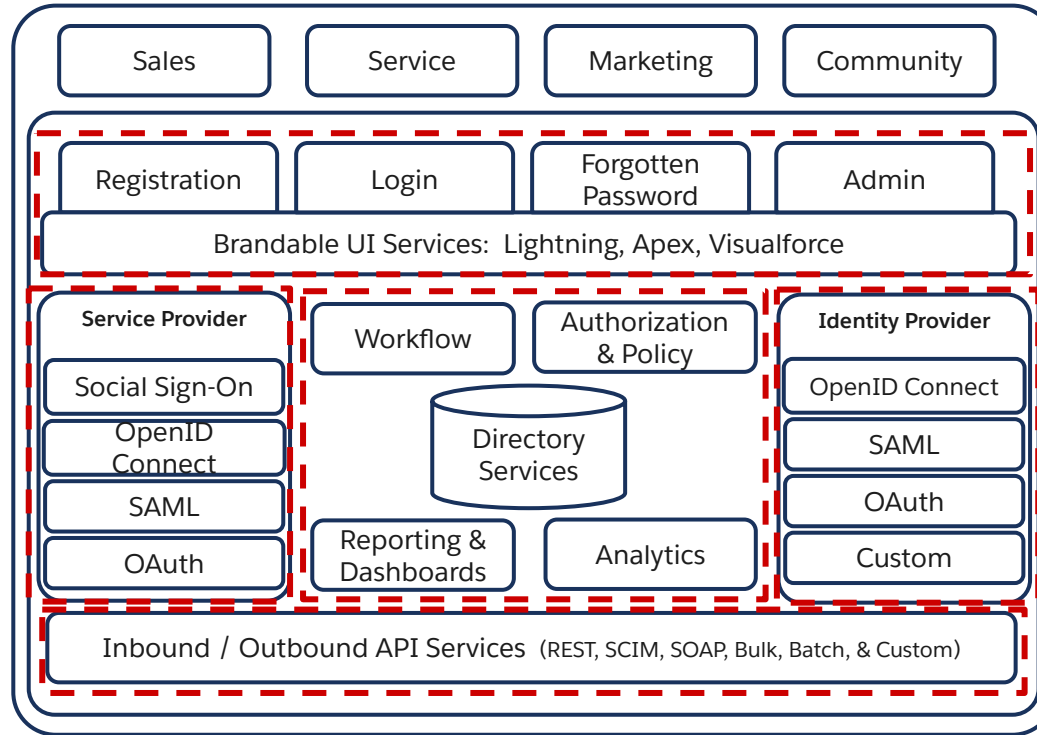
■ 注意点

すべての Lightning Experience ユーザーは、アプリケーションランチャーを使用できます。Salesforce Classic ユーザーには「Identity 機能を使用」権限が必要であり、ユーザープロフィールの「アプリケーションランチャー」オプションが**【参照可能】**に設定されている必要があります。

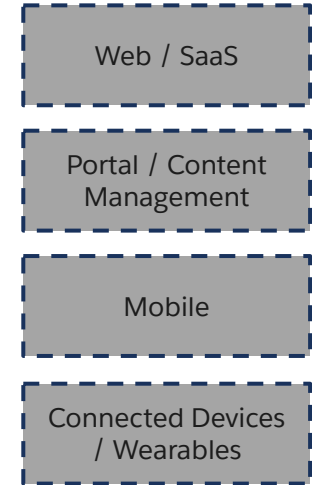


Salesforce Platform

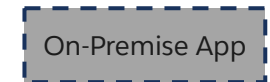
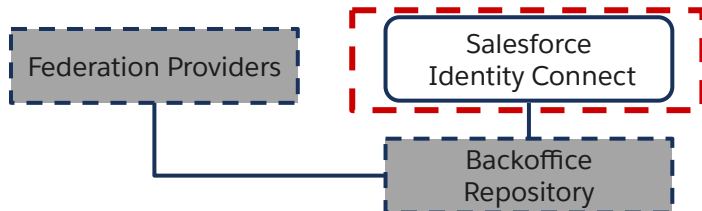
Identity Sources



Identity Targets



Cloud
On-Premise



サポートしている認証プロトコル

さまざまな標準プロトコルに対応

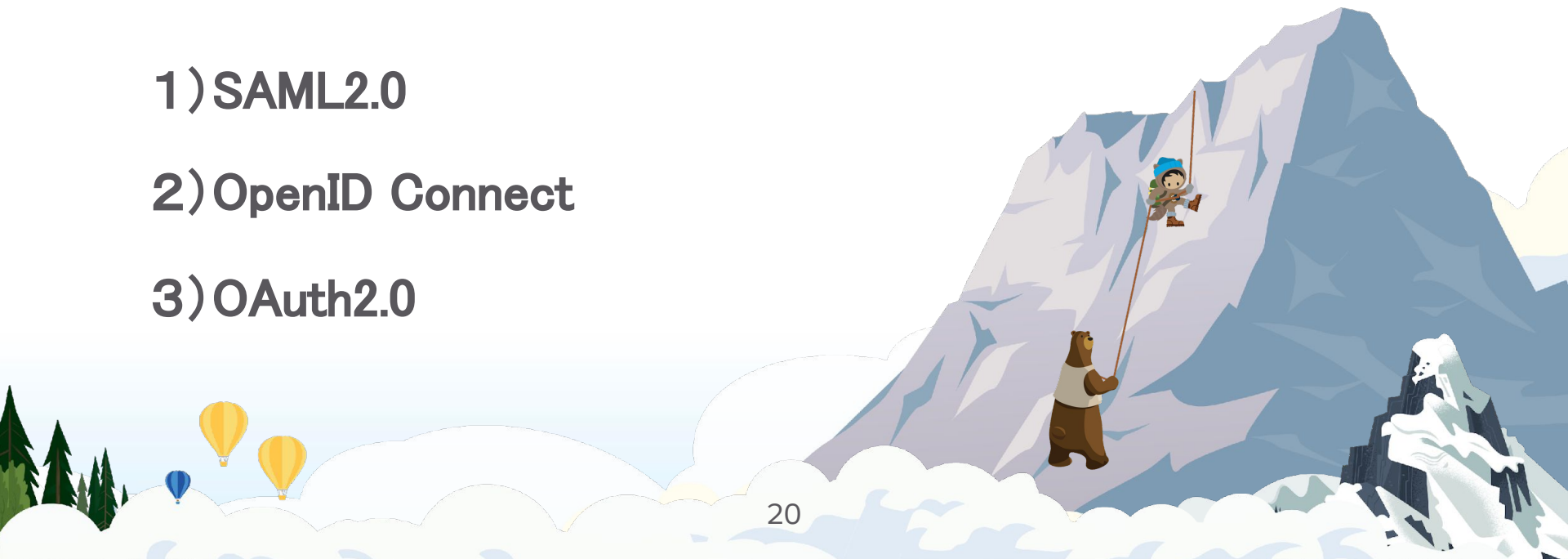


Salesforceの認証機能は、現在以下の標準プロトコルをサポートしています。
これらを使って外部システムとの双方向の認証連携が可能です。

1) SAML2.0

2) OpenID Connect

3) OAuth2.0



ユーザアカウントのプロビジョニング標準技術



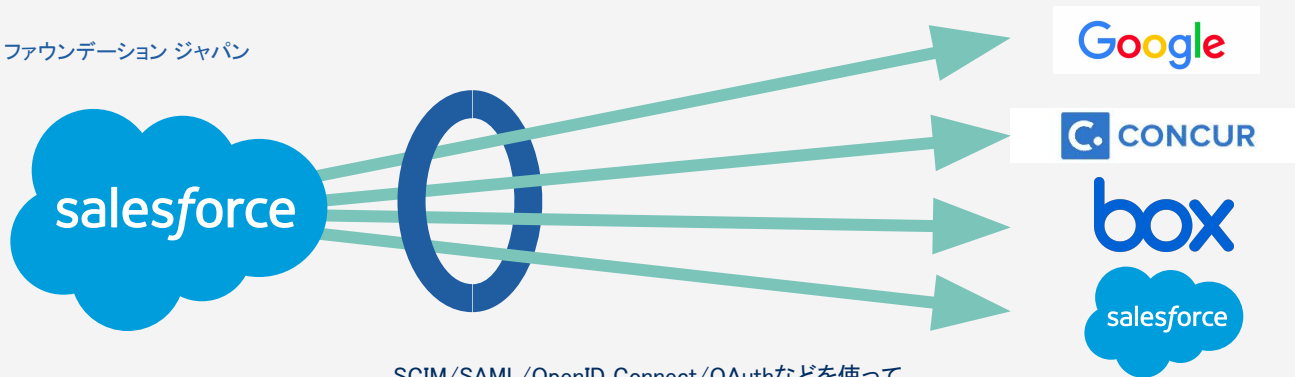
Salesforceは、現在SCIM2.0をサポート

■ SCIM (System for Cross-Domain Identity Management)とは

SCIM (System for Cross-domain Identity Management) とは、クラウドベースのアプリケーションやサービスのユーザー情報の管理を容易にすることを目的に、IETF (Internet Engineering Task Force) で標準化中の仕様です。クラウドサービス事業者は同仕様を採用することにより、ユーザー企業向けにオープン標準準拠のアイデンティティ・プロビジョニングAPIを提供することが可能となり、サービスの付加価値向上が期待できます。

また、同仕様はRESTfulなAPIを指向し、かつメッセージ形式にJSONを採用していることから、開発者にとって理解しやすいものとなっています。

出典: OpenID ファウンデーション ジャパン



SCIM/SAML/OpenID Connect/OAuthなどを使って
アカウント情報を配信

プロビジョニング実行トリガー



Salesforceから外部のサービスプロバイダにユーザ情報を配信するきっかけ

イベント	操作	オブジェクト
ユーザの作成	Create	User
ユーザの更新(選択した属性)	Update	User
ユーザの無効化	Deactivate	User
ユーザの有効化	Activate	User
ユーザの凍結	Freeze	UserLogin
ユーザの凍結解凍	Unfreeze	UserLogin
ユーザの再有効化	Reactivate	User
ユーザプロフィールの変更	Create / Deactivate	User
ユーザへの権限セットの割り当て／割り当て解除	Create / Deactivate	PermissionSetAssignment
接続アプリケーションへのプロフィールの割り当て／割り当て解除	Create / Deactivate	SetupEntityAccess
接続アプリケーションへの権限セットの割り当て／割り当て解除	Create / Deactivate	SetupEntityAccess



プロビジョニングが処理されるタイミング



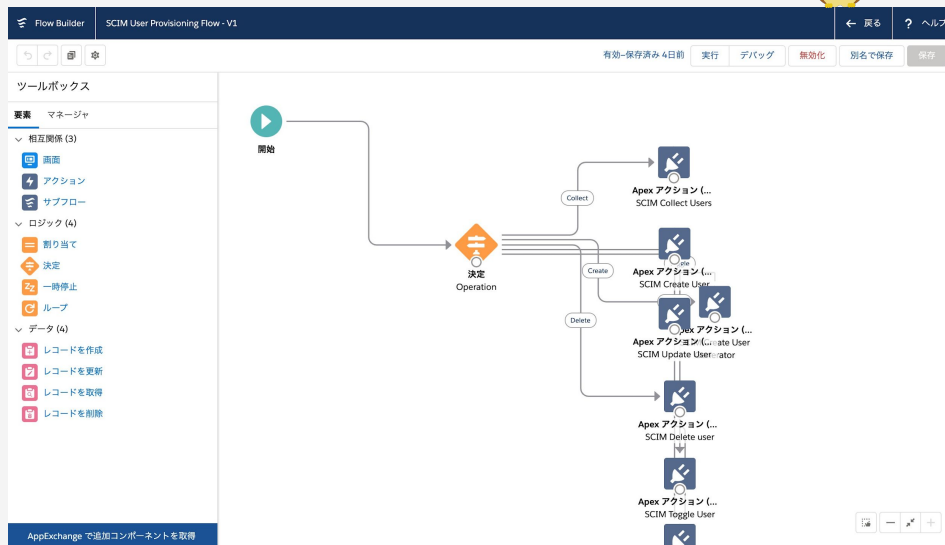
Salesforceから外部のサービスプロバイダにユーザ情報が配信されるタイミング

■ フローと承認処理

- ・ 即時実行 or スケジュール実行
- ・ グラフィカルワークフロービルダーで設定
- ・ 一括/繰り返し実行
- ・ サブワークフローやプラグイン差し込み
- ・ 多段階承認処理
- ・ メールやフィードでの承認実行

■ コネクターの拡張

- ・ Apexワークフロープラグイン
- ・ 外部データベース
- ・ パッケージ化



ジャストインタイム(JIT)・プロビジョニング



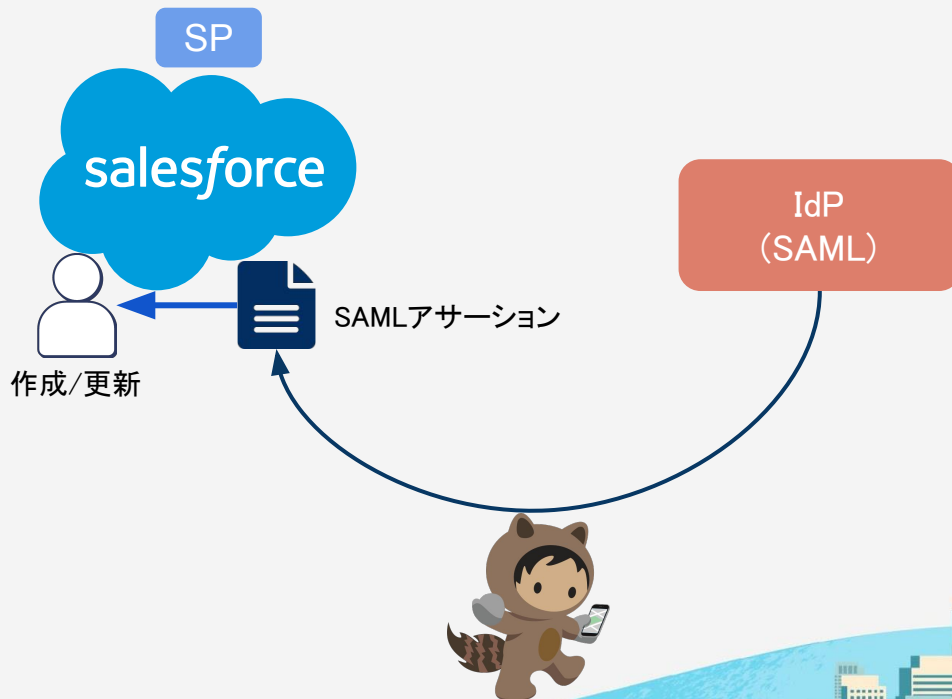
SAMLアサーションを利用した自動ユーザ作成・更新

管理コストの削減
ユーザの採用の増加
セキュリティ向上

必須属性

- Email
- LastName
- ProfileId
- Username

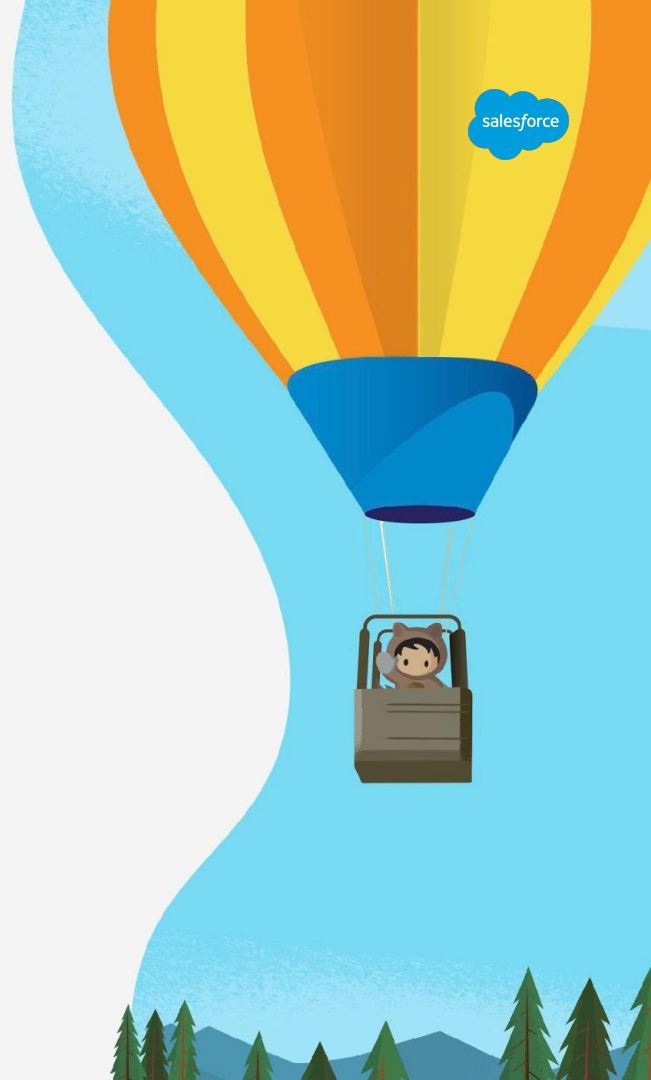
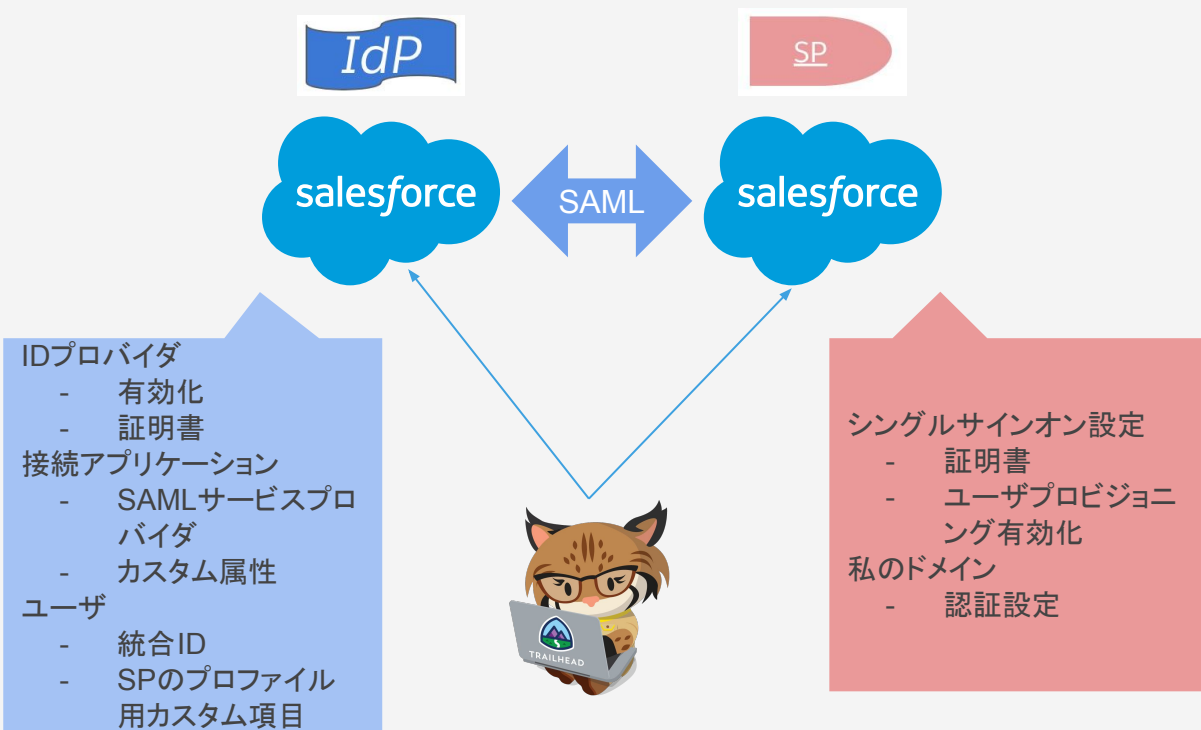
その他の属性を含めることが可能



シングルサインオン デモンストレーション

デモンストレーション

Salesforceのシングルサインオンとプロビジョニング

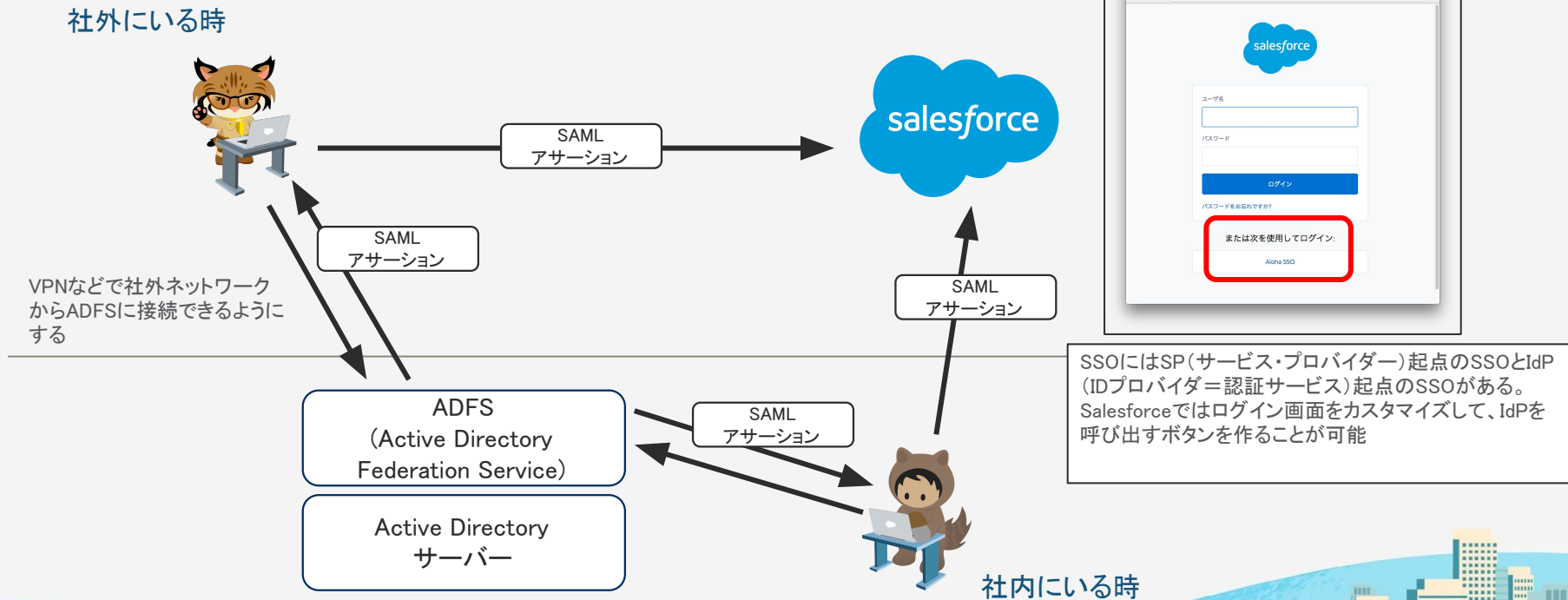


シングルサインオン ユースケース

SSOユースケース 1(イントラのActive Directoryと連携)



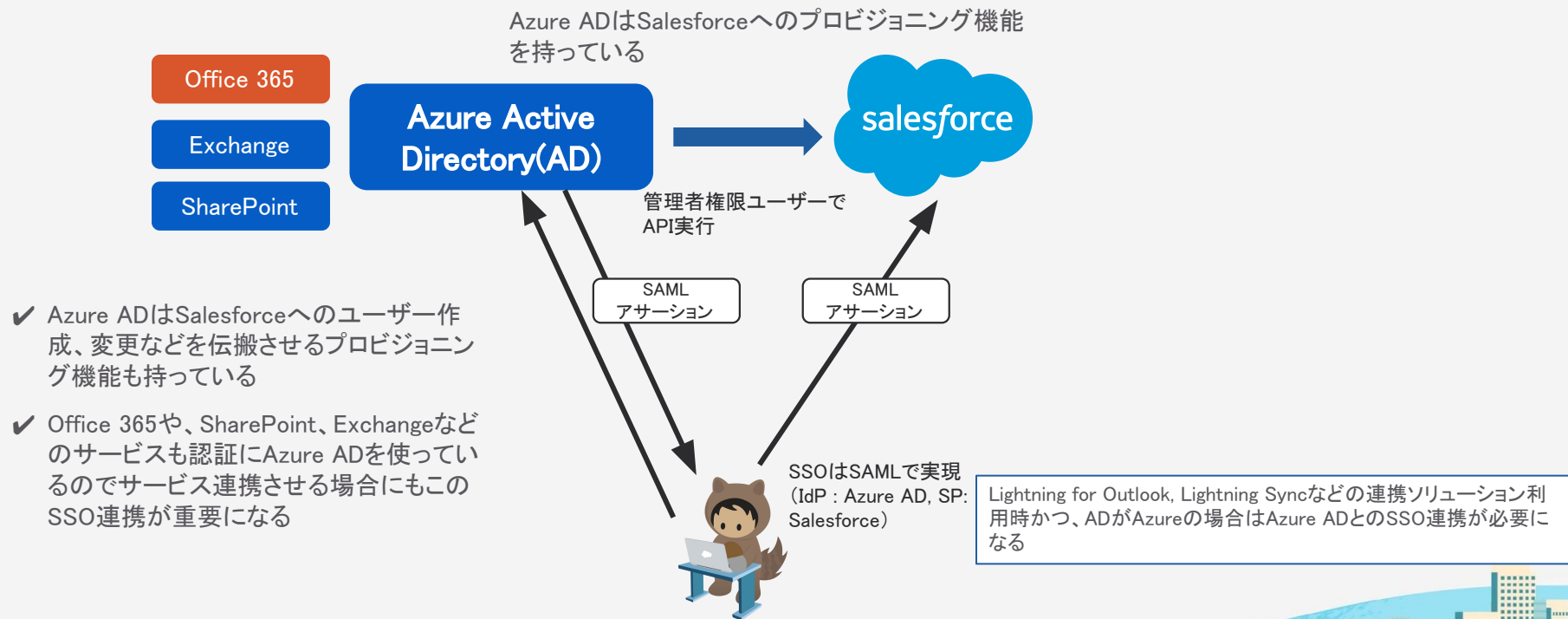
ADFSを介してActive DirectoryとSAMLで認証連携する



SSOユースケース 2(Azure Active Directory連携)



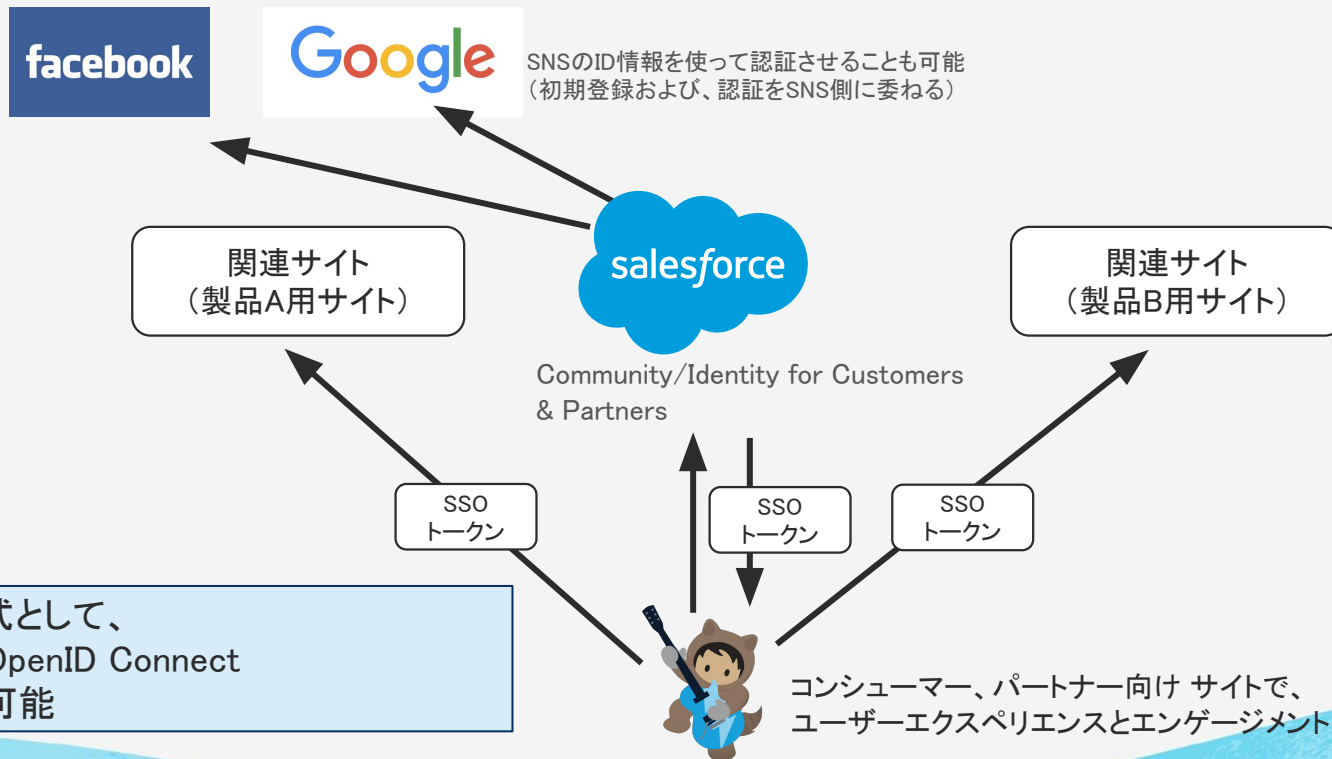
クラウド上のIDaaSを利用



SSOユースケース 3(SalesforceをIdPとして活用)



Salesforceを中心に利用者が関連して利用するサービスにSSOを提供



Salesforce Identityを使うために

Identity系ライセンスと提供機能

コアサービスにはIdentity機能が含まれます



オンプレミスのActive Directoryのユーザー情報を
Salesforceに反映するためのコネクターソフトウェア。クラウド
上で動くのではなく、オンプレミス環境にインストールする
ソフトウェアなのでインプリメンテーションが必要



さらなる高みへ



学習コンテンツや開発者ドキュメントの活用



Trailhead トレイル「安全なIDとアクセスの管理」

<https://trailhead.salesforce.com/ja/content/learn/trails/identity>



シングルサインオン実装ガイド

https://developer.salesforce.com/docs/atlas.ja-jp.sso.meta/sso/sso_about.htm

Identity実装ガイド

https://developer.salesforce.com/docs/atlas.ja-jp.identityImplGuide.meta/identityImplGuide/identity_overview.htm



まとめ

- 「認証」「認可」を理解
- 効率的でセキュリティの高いID管理のためのシングルサインオン
- Salesforceの認証でID管理の課題を解決

