

OpenAMで実現するアイデンティティ 連携技術を使った認証基盤



ThemiStruct
デミストラクト

株式会社オージス総研
八幡 孝



認証基盤をとりまく動向

企業の認証基盤プロジェクトが変化

- 社内システムの認証基盤(SSO、ID管理)



- クラウド利用時の認証強化
- 顧客向けサービスの認証基盤

ビジネスのデジタル変容への対応

- モバイル、クラウド、ソーシャルの活用
- ユーザー情報の活用、分析
- ビジネスプロセスの自動連携
- 多様なデバイスとの連携、活用

- 
- ユーザー毎に最適化されたサービスの提供
 - 業務効率の向上、提供スピードの向上

認証基盤の技術要求が変わる

	従来の認証基盤	今後の認証基盤
利用端末	統一されたPC	多様な端末の利用
対象システム	フロントシステム(Web)の認証	フロントシステムの認証とAPIアクセスの認証 SPA、モバイルアプリ対応
利用形態	社内、VPN経由での利用	社内外からのシステム利用、APIアクセスを想定
その他	—	社内外システムとのAPI連携

アイデンティティ連携技術

アイデンティティとは？

■ 主体 (Entity | Subject)

- 人、組織、PC、デバイス、サービス、リソース、...

■ アイデンティティ (Identity)

- 主体にかかわる属性の集合体
- ひとつの主体に、コンテキストに応じたIdentity

認証とは？

■ 主体(人)を Identity に紐付けること

- アクセスをしている主体が、
- サービス・システムが認識している、どの Identity と紐付いているか、
- 本人だけが知り得る、所有する情報をもって確認する

アイデンティティ連携とは？

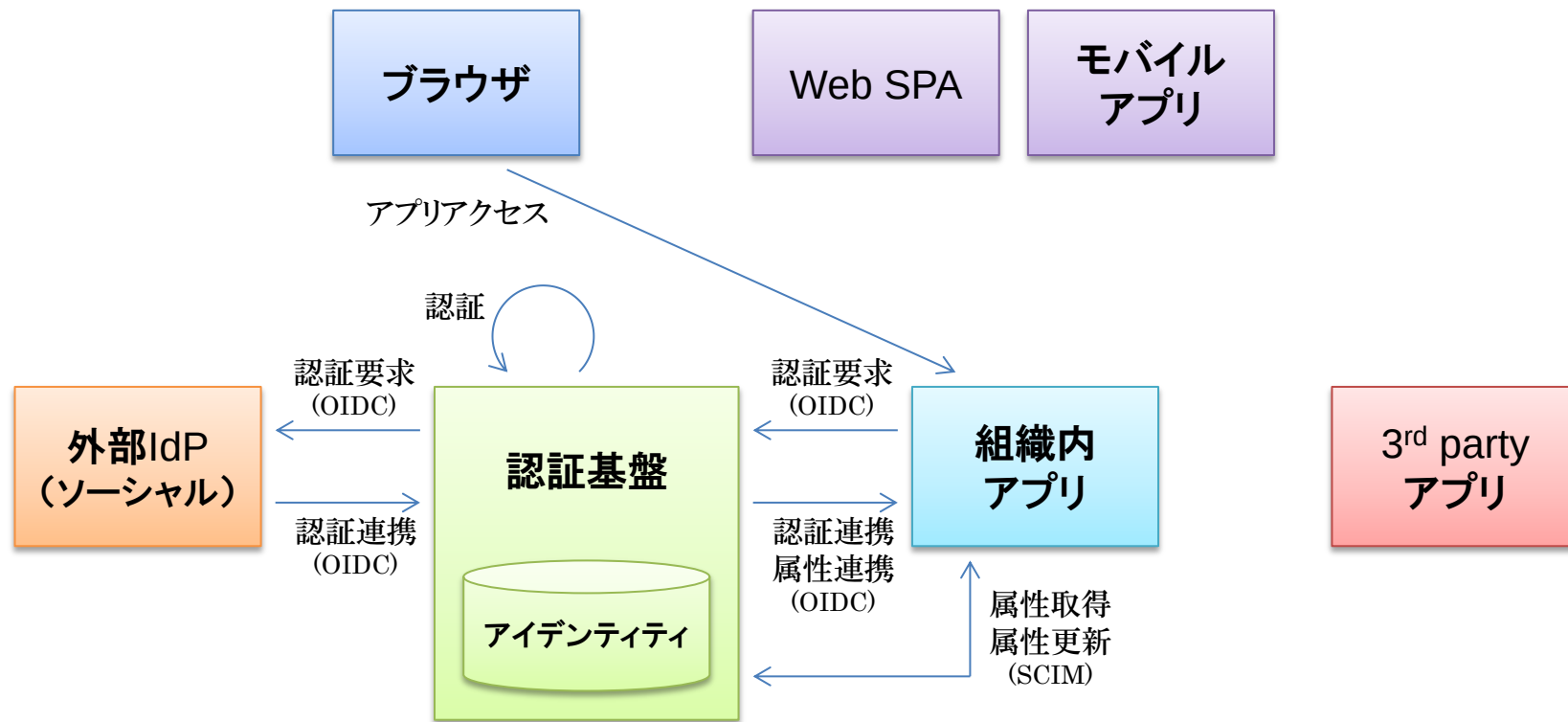
- 認証連携 + 属性連携 = ID連携
- 複数の組織、ドメインでアイデンティティを利用する

アイデンティティ連携技術の標準

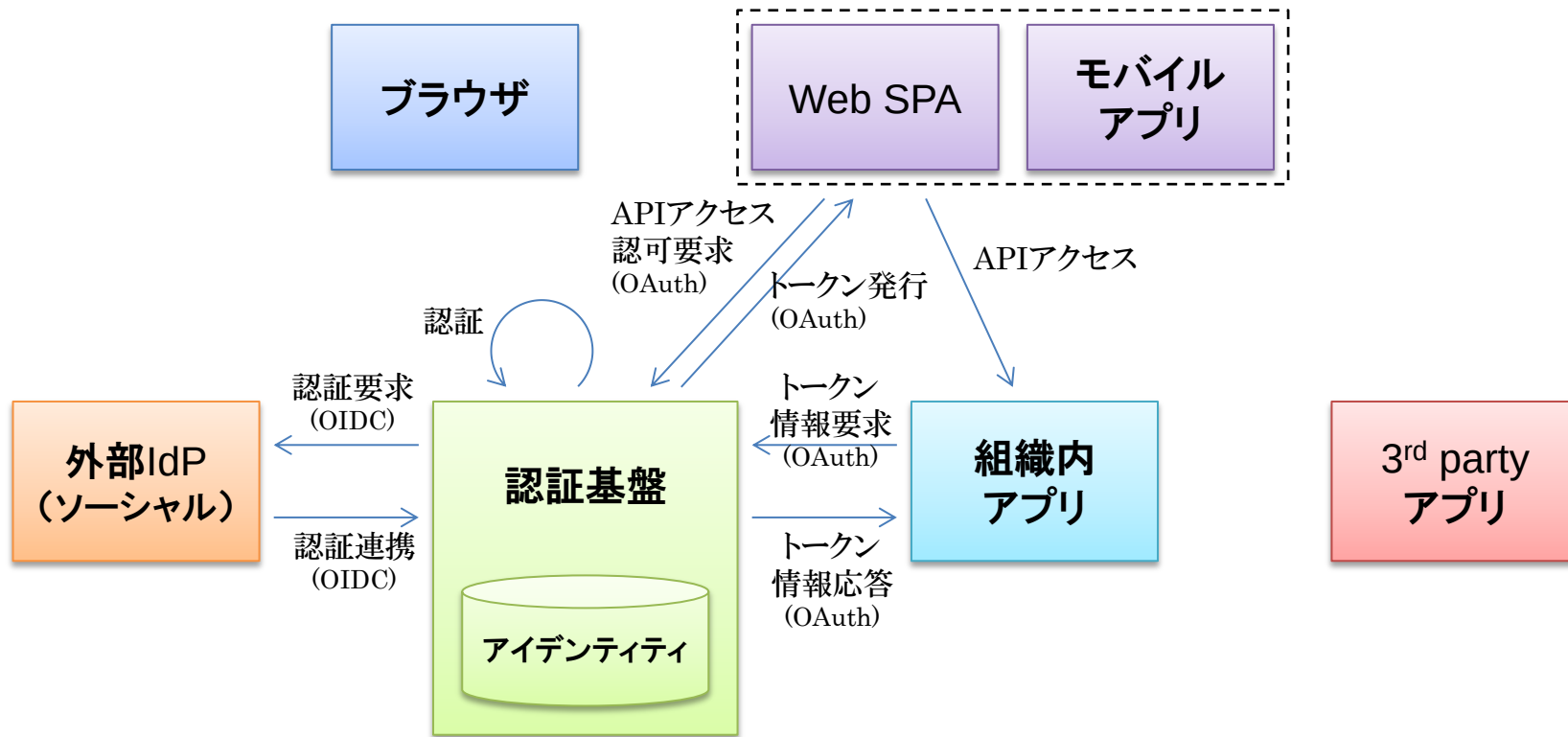


アイデンティティ連携技術を使った認証基盤

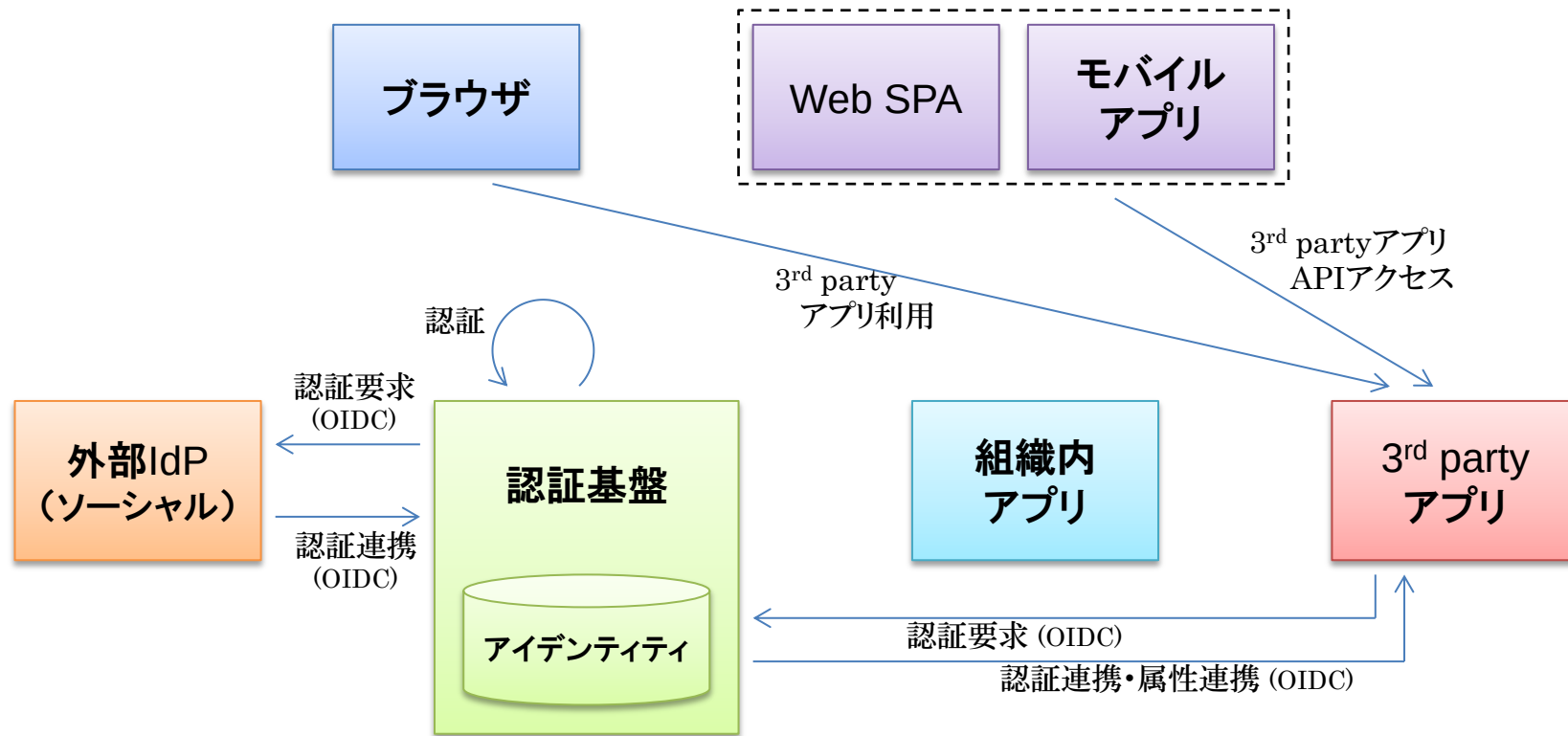
アプリケーションへのSSO



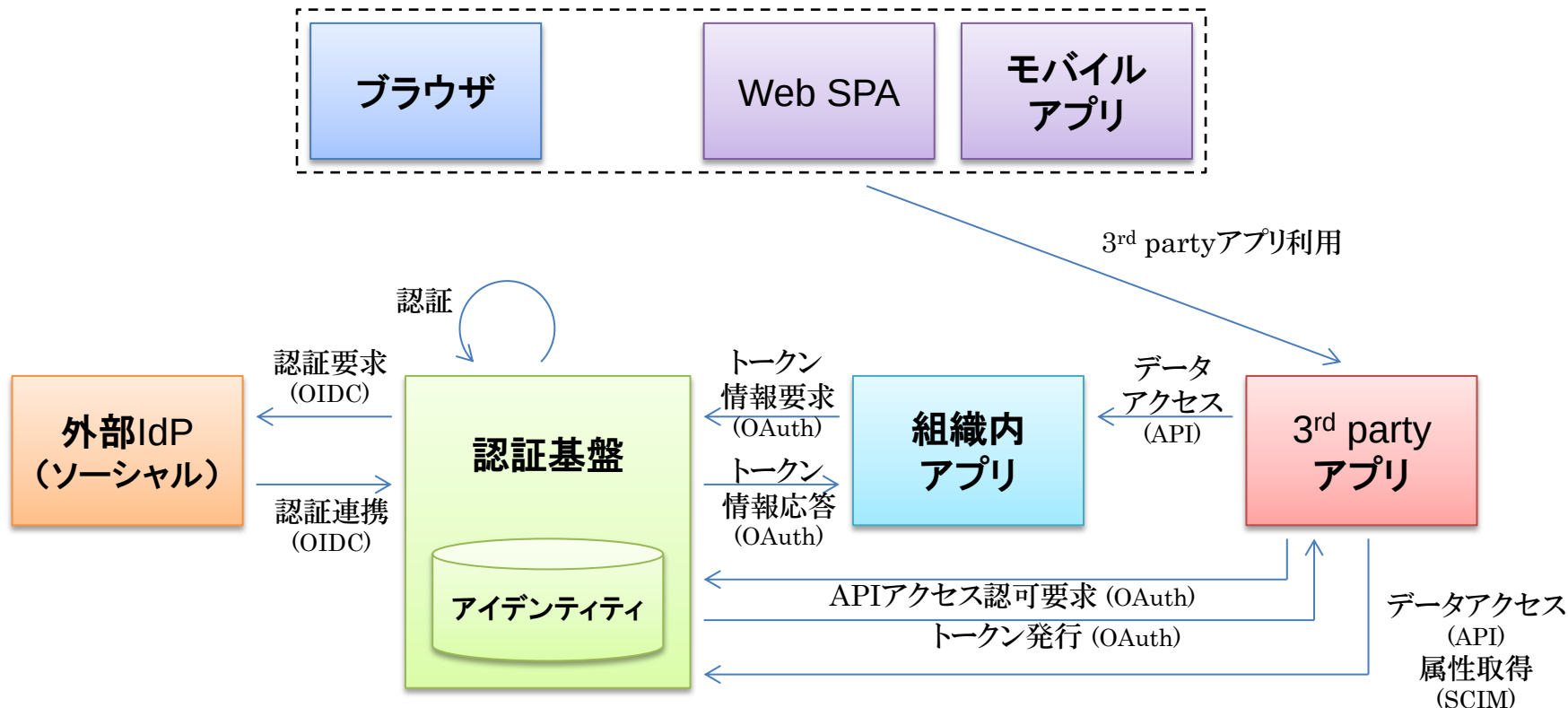
SPA, モバイルアプリからのAPI利用



3rd partyアプリへのSSO

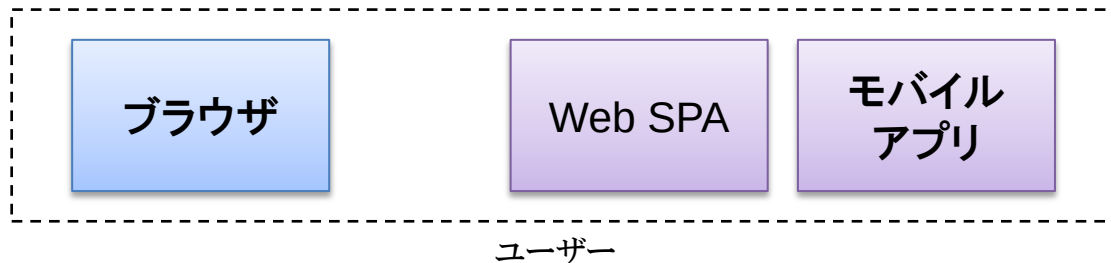


3rd partyアプリへのデータ提供



顧客向けサービスへの適用例

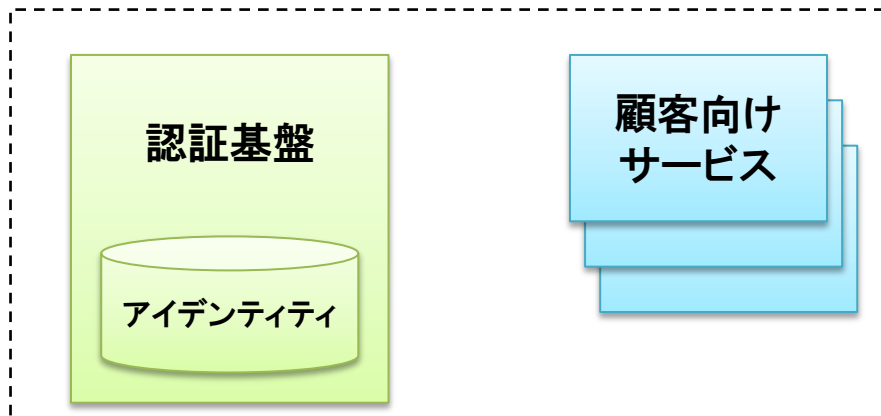
顧客向けサービスの全体構成



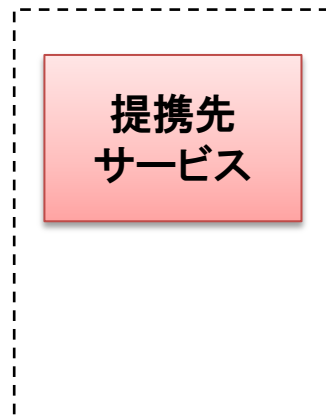
ソーシャルIDの活用



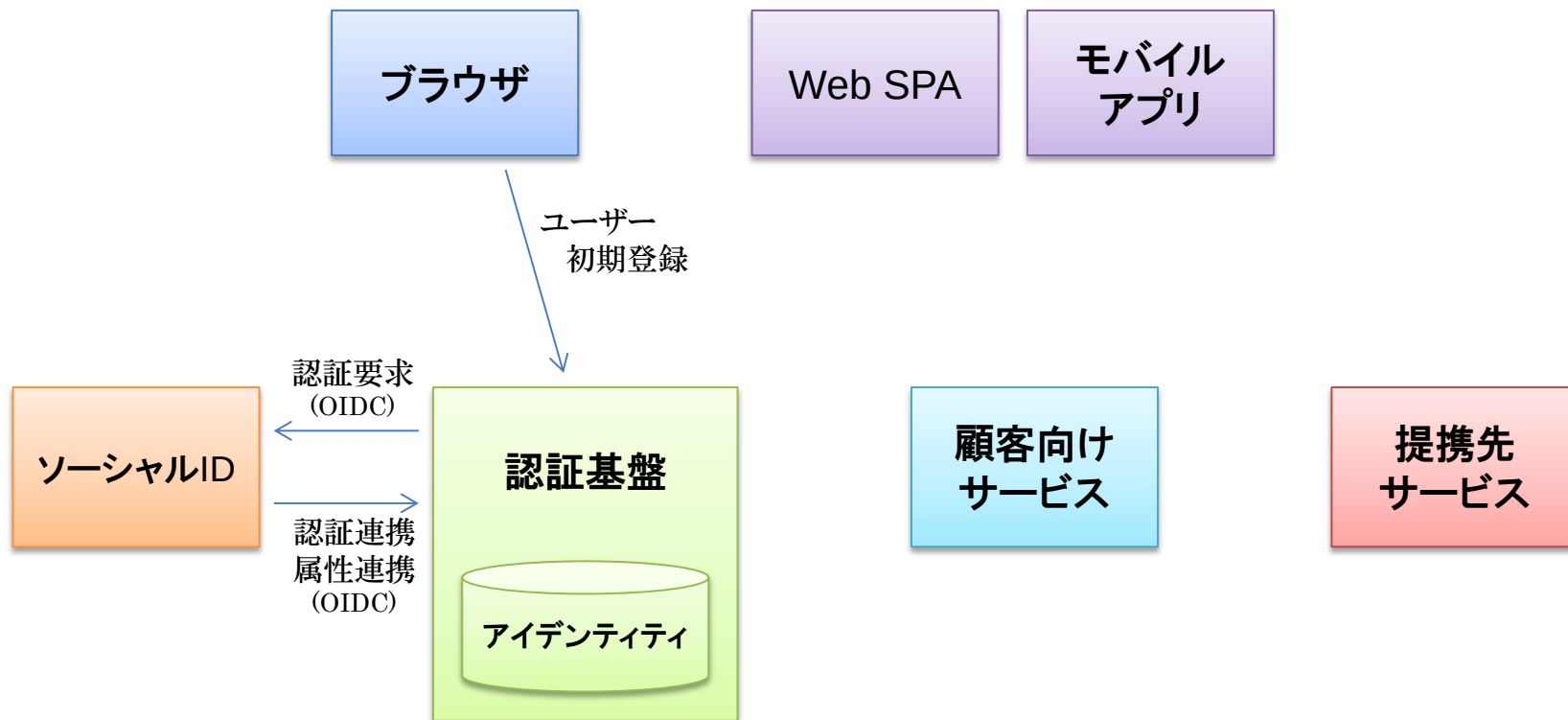
顧客向けサービス基盤



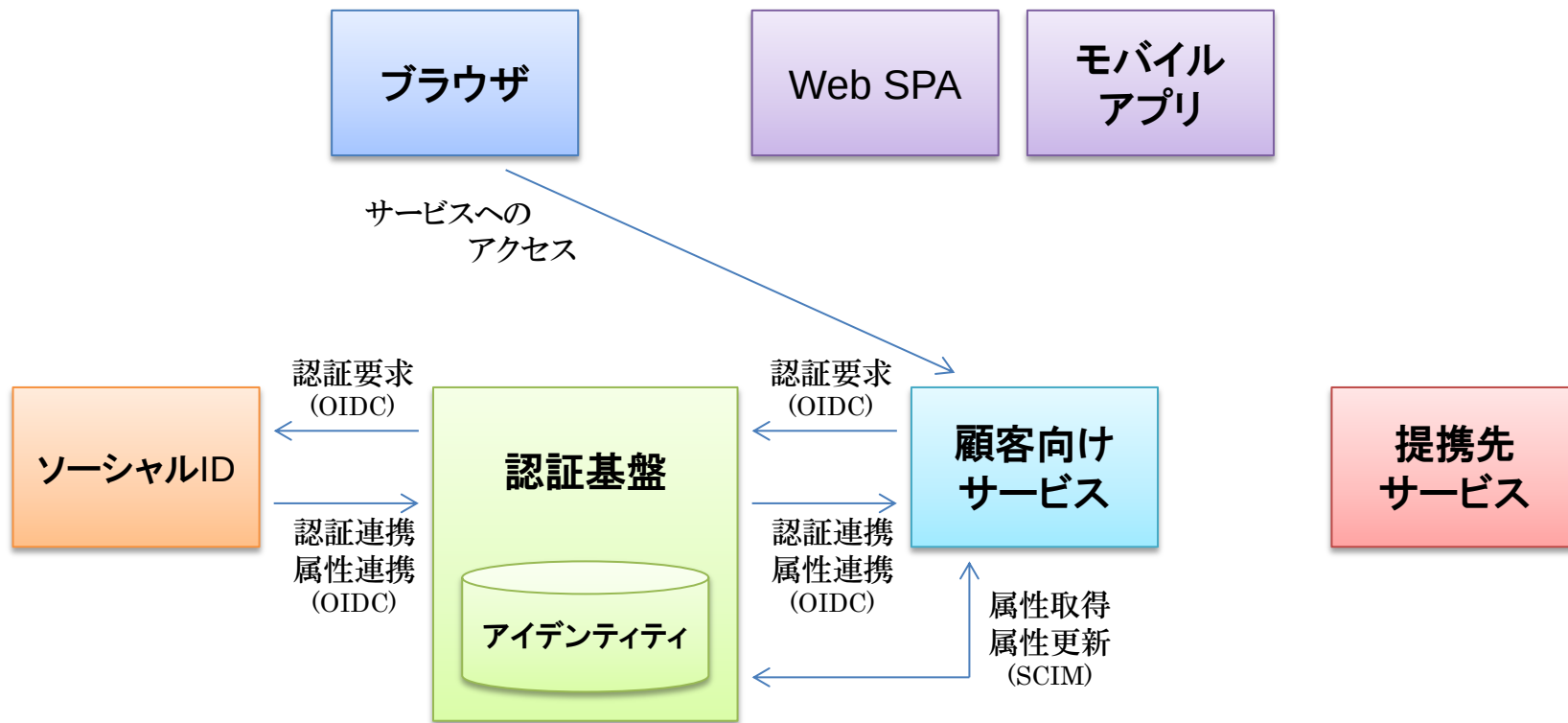
業務提携先/関連サイト



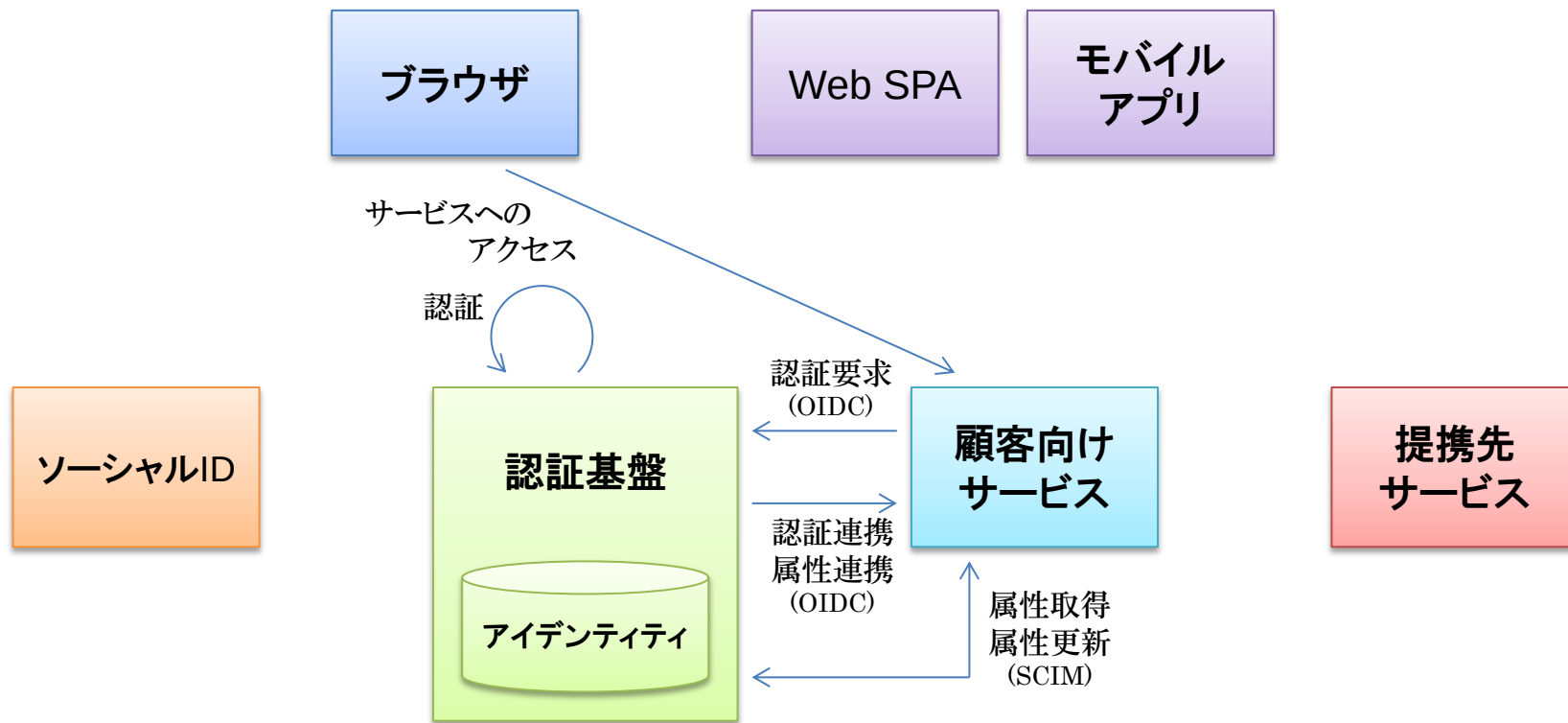
ソーシャルIDを使ったユーザー登録



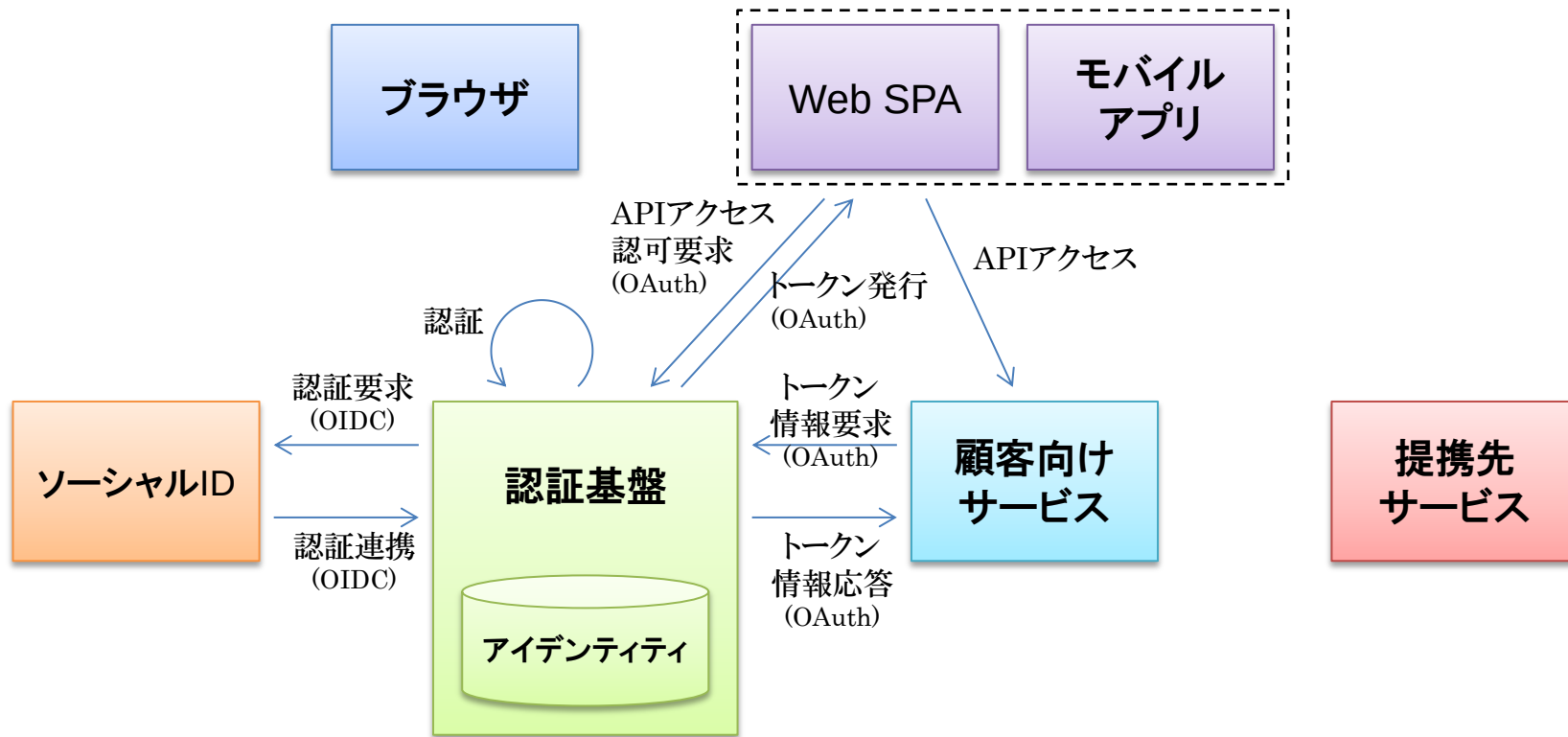
ソーシャルIDを使ったサービスへのサインオン



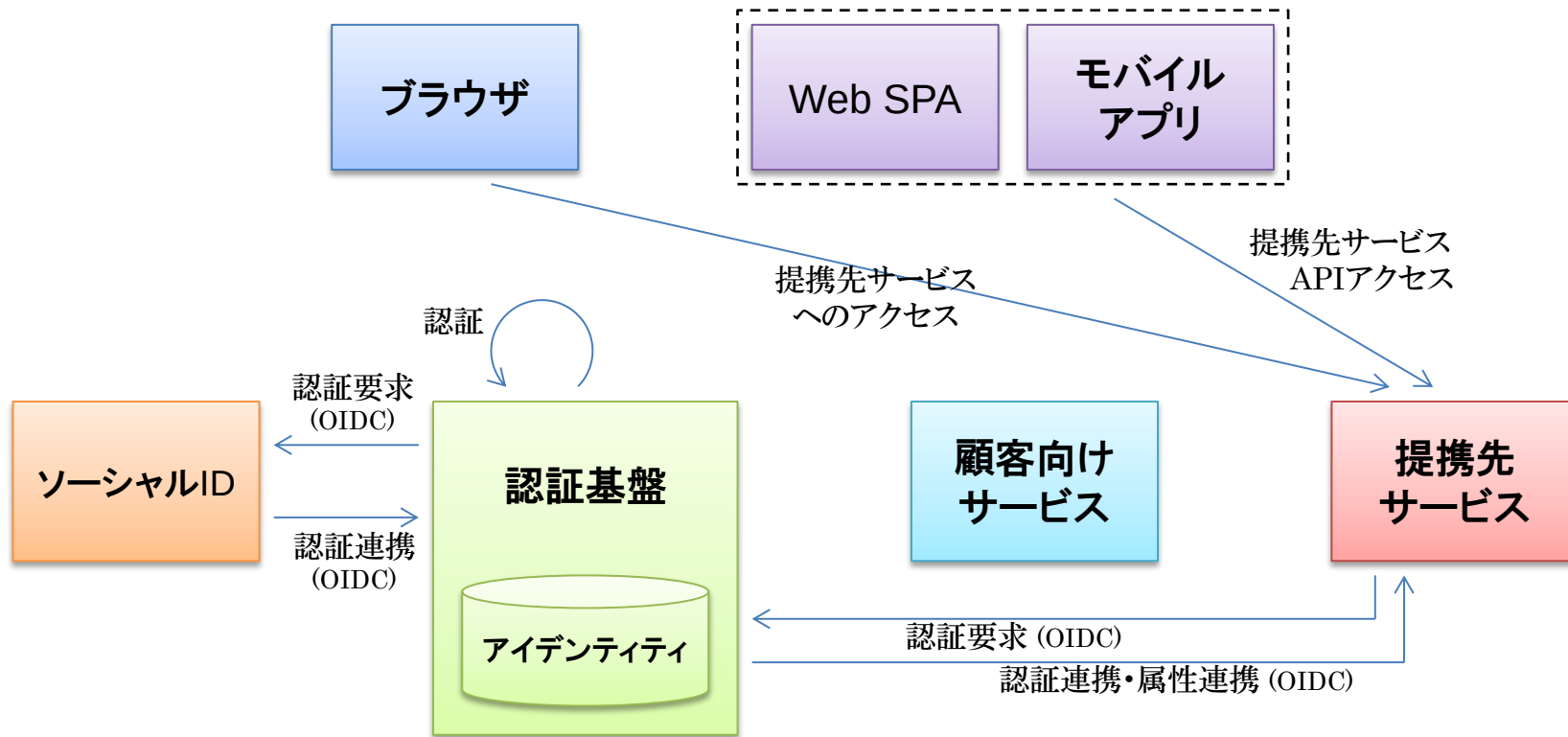
ローカルIDを使ったサインオンにも対応



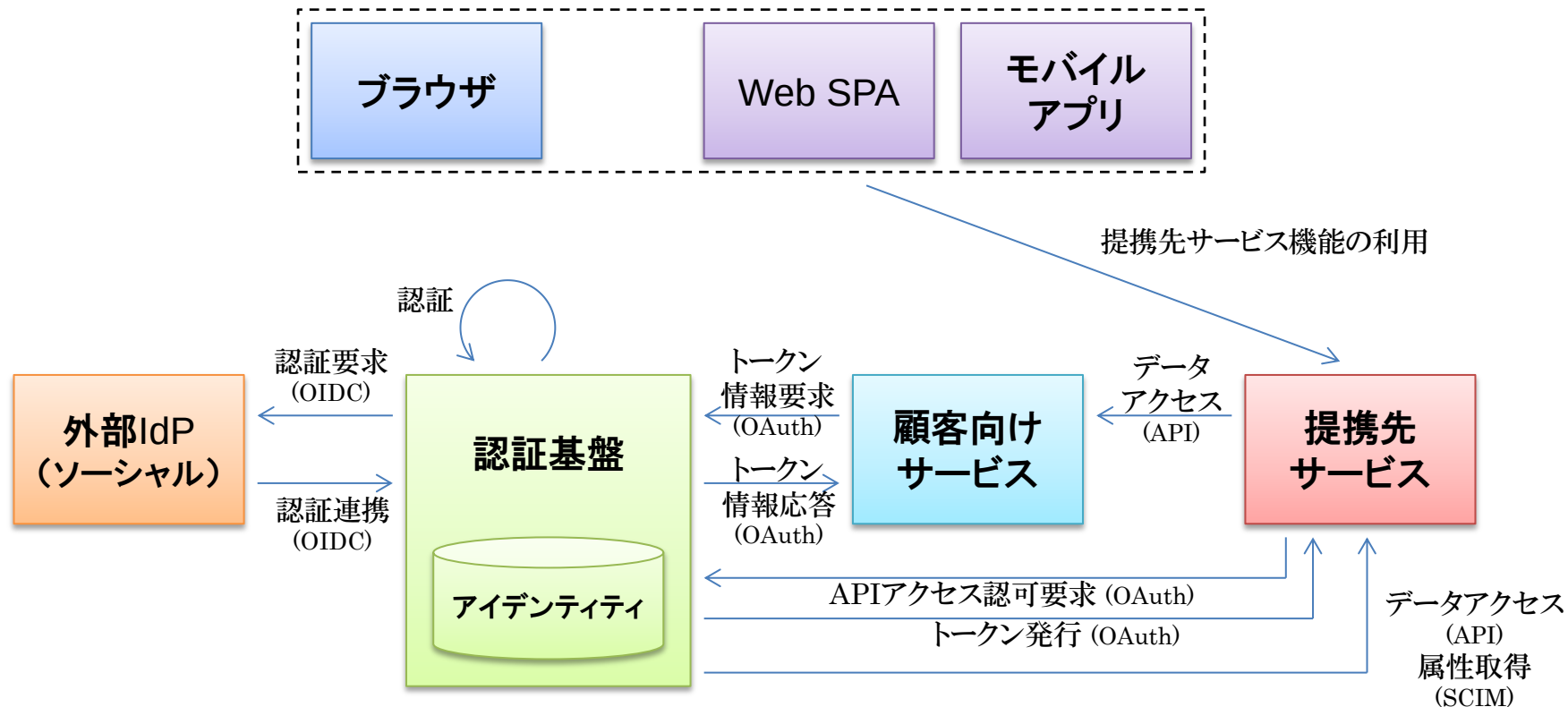
SPA, モバイルアプリを使ったサービスへ展開



提携先サービスへのシームレスなアクセス

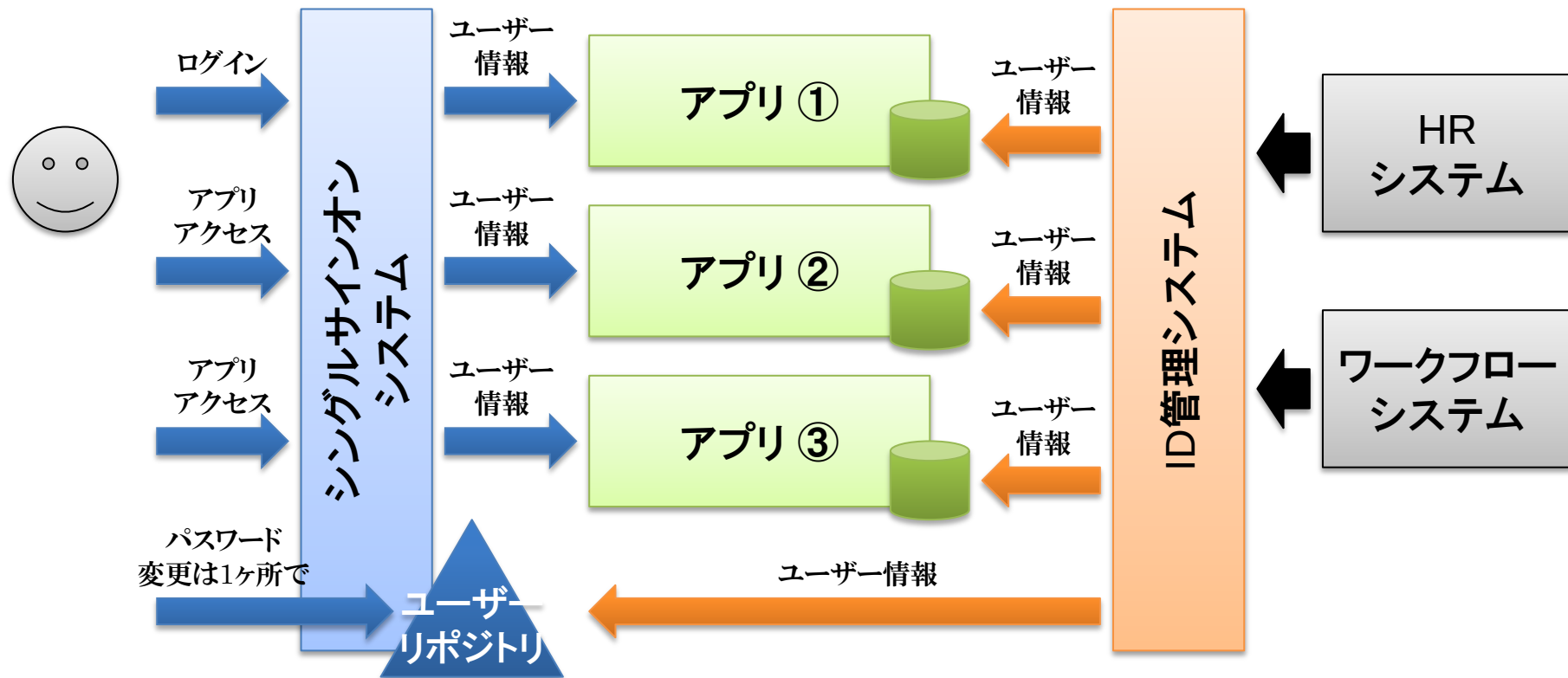


提携先と連携した新しいサービスの提供



社内システムの認証基盤への応用

社内システムの認証基盤の一般形



アプリへの属性連携はSSOから? IDMから?

- 企業でのアイデンティティは、異動により変化する
- スケジューラ、コラボレーションアプリでは、全ユーザー、全組織の情報が事前に登録されている

IDMを使った一括反映で対応

- アプリとIDMの接続は個別設計が必要。費用、期間が課題となる

IDMだけの対応ではアプリの認証基盤活用が進まない

属性の特性に合わせて対応

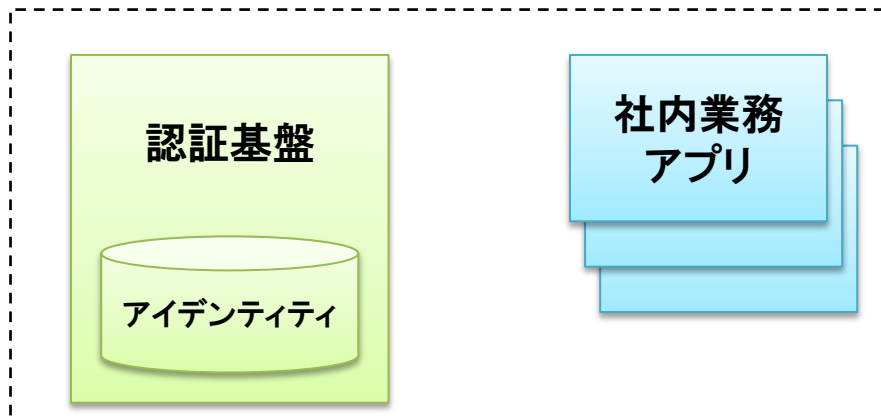
- ログイン可/不可 は認証基盤(SSO)で対応
- ログインしたユーザーに関連する属性はSSOから
 - 表示用属性、属性ベースのアクセス制御、など
 - そのユーザーが属する組織の情報も
- アプリデータとしての特性を持つ属性はIDMを使って
 - 全社員ユーザーの登録、全組織の登録が事前に必要な場合に限る
- アカウントの事前作成、遅延削除を併用して

社内システムの認証基盤の全体構成

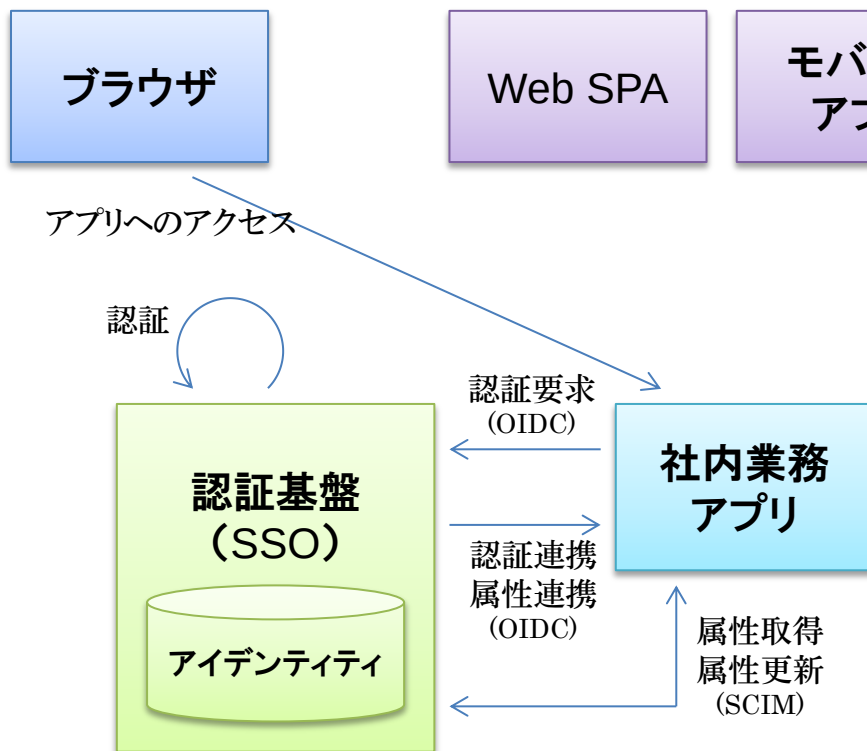


ユーザー

社内システム



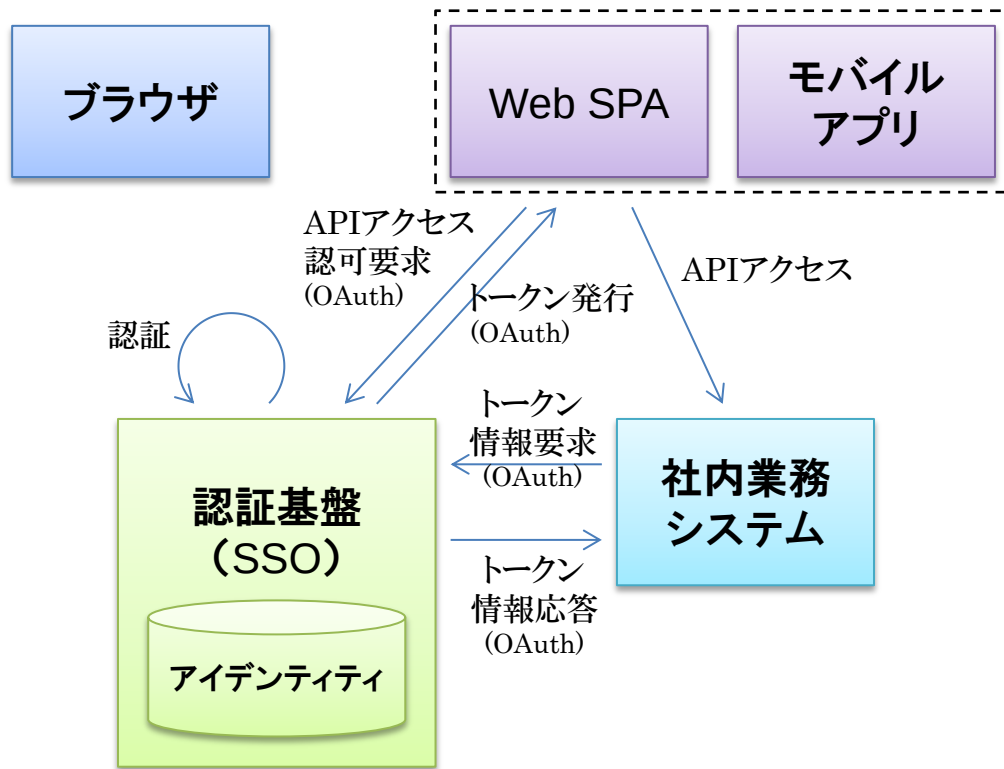
社内業務アプリにシングルサインオン



社内業務アプリでのアイデンティティの扱い方

1. 社内業務アプリではアイデンティティ情報を保持しない。OIDCでの属性連携、SCIMを使った属性取得で動作させる。
2. 社内業務アプリではOIDCでの属性連携時に、動的にアカウントの作成、属性の更新を行なう。
3. 社内業務アプリは、ユーザー、組織の情報をデータとして必要とするためIDMを使った定期メンテナンスを行なう。

SPA, モバイルアプリを使ったシステムへ展開

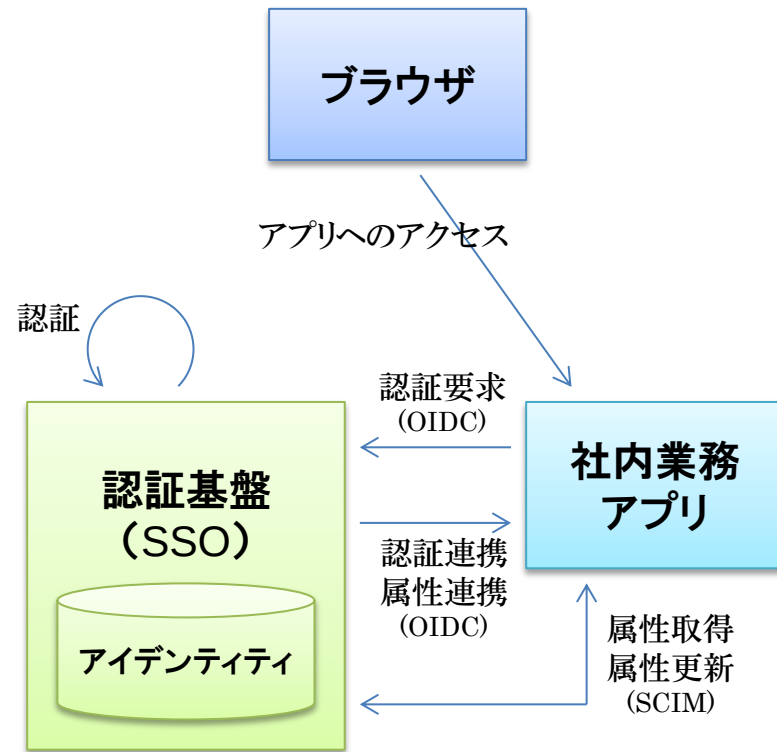


OpenAMを使ったコンセプト実装のデモ

コンセプト実装

■ 社内システムのSSOを コンセプト実装

- 認証基盤: OpenAM
- 社内業務アプリ: スクラッチ



実装の概要

■ OpenAM 14.0.0-SNAPSHOT

- OpenID Connect OP として構成
 - profileスコープで企業ユーザーの属性をclaimとして応答するように設定
- embedded OpenDJ を SCIM Server として構成
 - SCIM Schema 2.0 っぽく応答するように

■ スクラッチで作ったアプリをRPとして接続

- Python3 + bottle framework + pyoidc

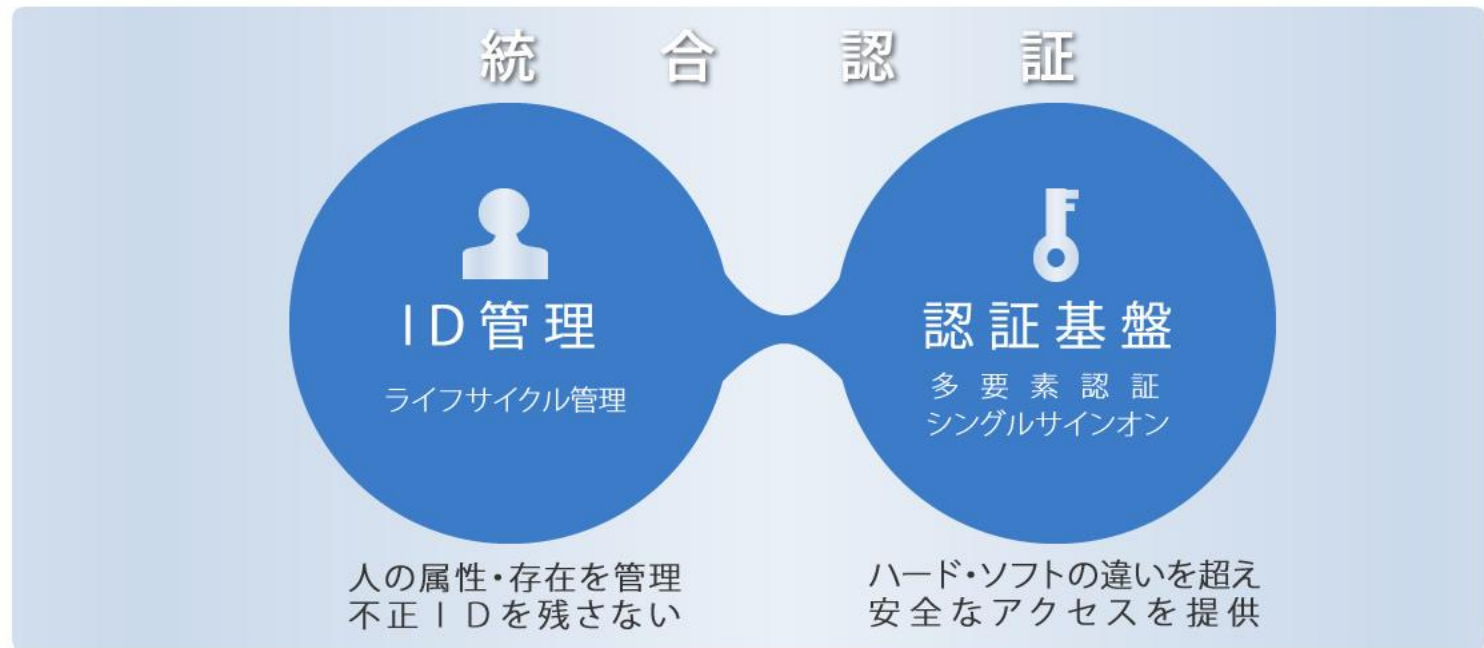
まとめ

まとめ

- ビジネスのデジタル変容という潮流の中にある
- アイデンティティ連携技術への対応が不可欠
- 顧客向けの基盤のみならず社内基盤も変化が必要
- OpenAMがコアコンポーネントとなる

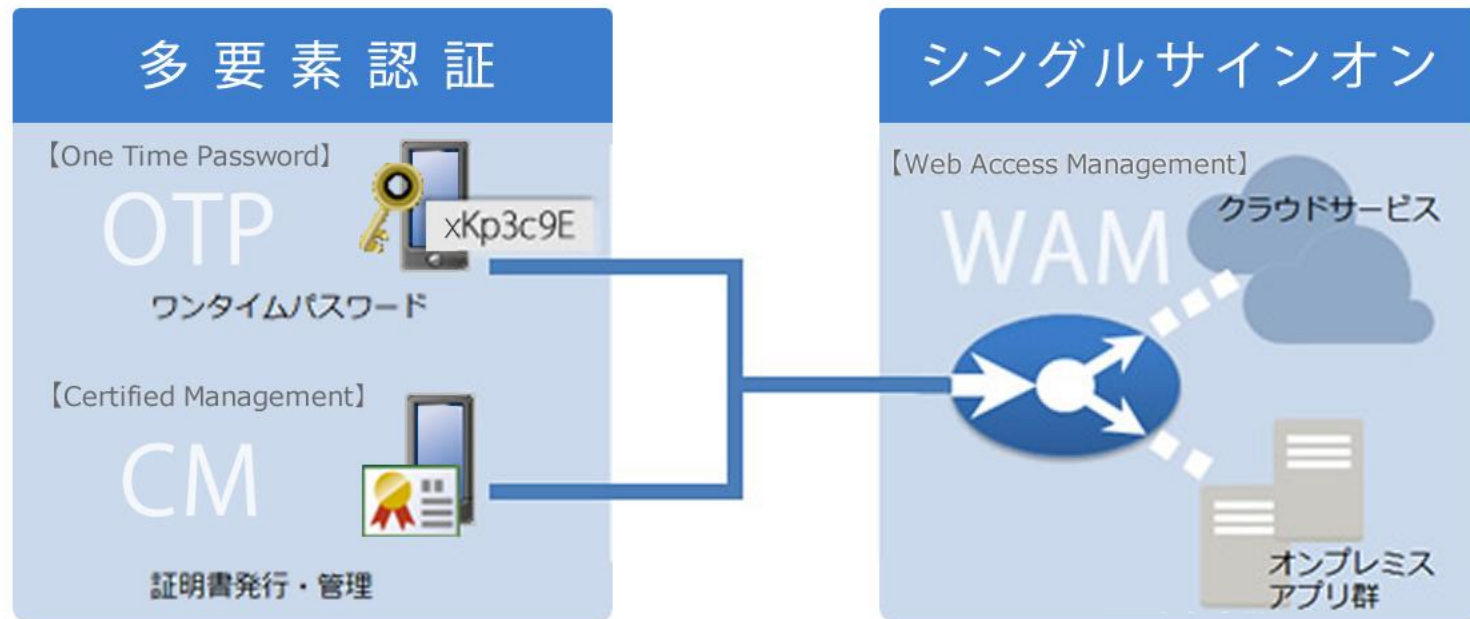
当社ソリューションの紹介

ThemiStruct は統合認証ソリューション



1. 認証基盤ソリューション

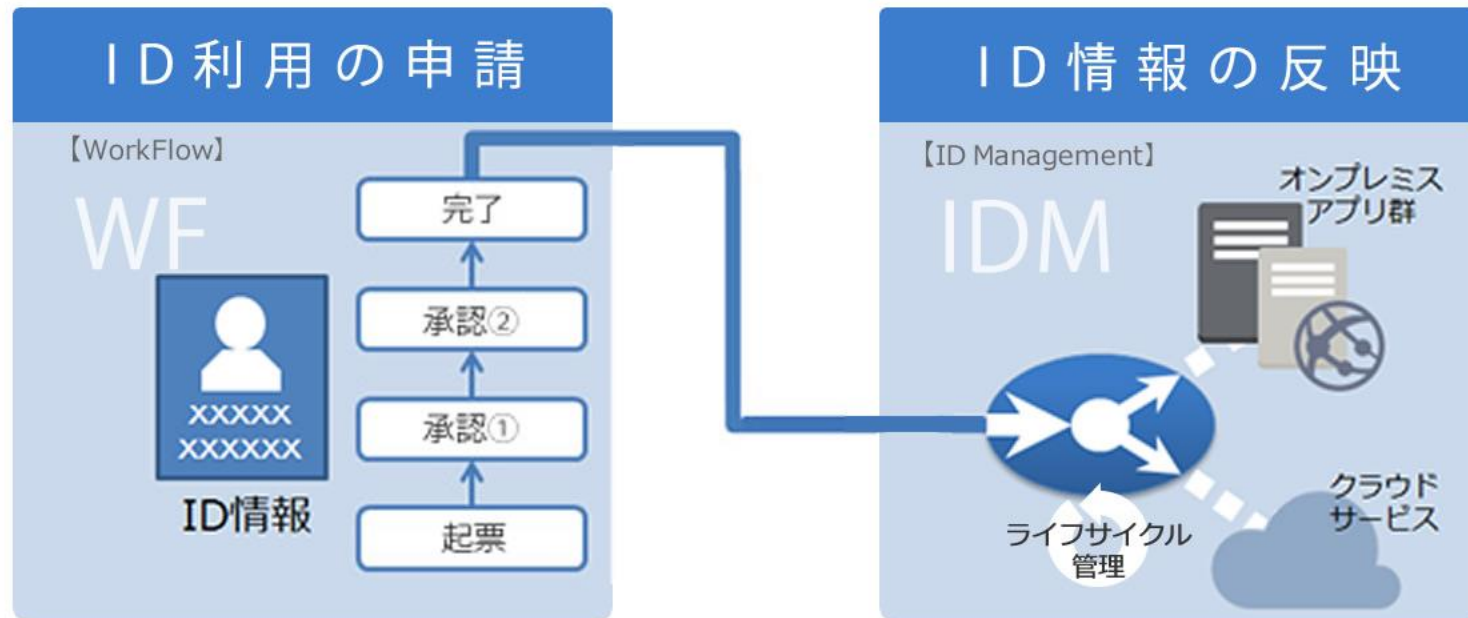
クラウド×スマートデバイスを多要素認証でセキュリティ強化し
シングルサインオンで利便性を向上します





2. ID管理ソリューション

ID情報を申請フローを用いて収集し対象システム群へ反映
有効期限による管理および人事異動などにスマートに対応可能です



5つのソリューションを提供



ThemiStruct-WAM

シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM

ID管理ソリューション

ThemiStruct-CM

電子証明書発行・管理
ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

ThemiStruct-WAM

- OpenAM (trunk) がベース
- 専用のインストーラー
- 当社オリジナルの日本語マニュアル
- スマートデバイスに対応するレスポンスUI
- パスワード管理強化のためのアドオンモジュール群
- 高度なリスクベース認証を実現するインベントリ認証オプション
- ...

ThemiStruct-IDM

- OpenIDM (trunk) がベース
- 専用のインストーラー
- 当社オリジナルの日本語マニュアル
- 権限委譲に対応した専用のWebUI (SSI)
- 組織、グループ、ロールの管理
- プロビジョニングのスケジューリング、予約への対応
- ...

ThemiStruct-CM

- EJBCA (Enterprise版) がベース
- 当社オリジナルの日本語マニュアル
- 証明書の一括登録、一括ダウンロード
- 秘密鍵がエクスポートできない証明書発行への対応
- デバイスアクセスコントロールへの対応
- ...



当社は PrimeKeySolutions AB 社の
パートナー です。

OSSを活用するメリット

- 技術標準の早期実装
- 公開されている仕様
- ソースコードを使った問題調査、修正

ThemiStructで提供する3つのサービス

テクニカルサポート サービス

- 利用方法などの問合せへの回答
- 障害時の調査、回避策や代替案の提示、復旧の技術支援

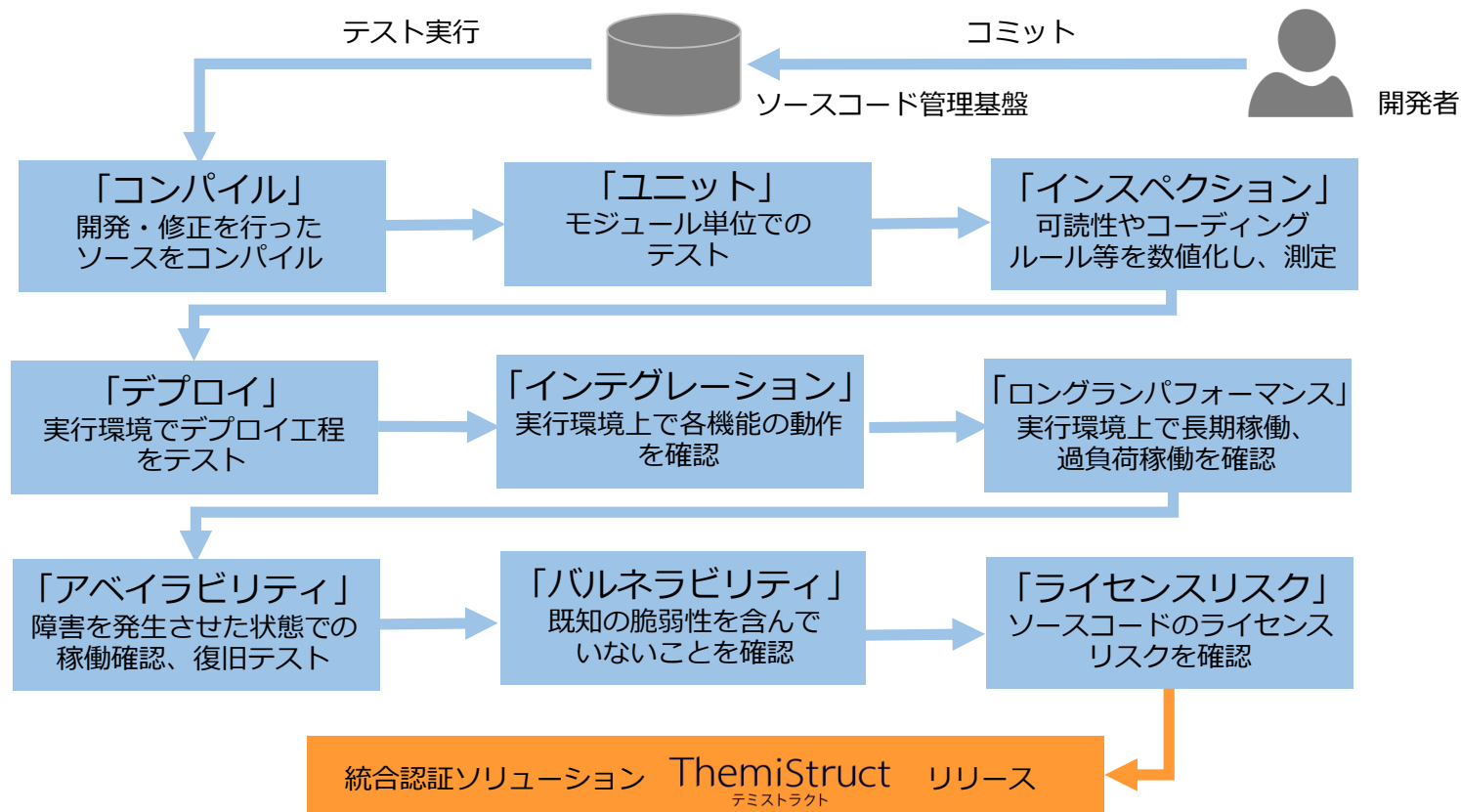
プロフェッショナル サービス

- 要件実現方法の相談、回答
- 技術検証の支援
- 自社で実施する開発、構築の技術支援

システムインテグ レーションサービス

- お客様の要望に応じたシステムを構築

OSSを安心して活用いただくための取り組み



AWS上に展開されたテスト基盤

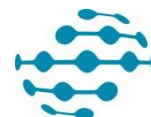
- テストターゲットの自動デプロイによる
クリーンなテスト環境の構築
- 自動化インテグレーションテスト
 - 自動化率向上のための取り組みを継続
- スポットインスタンスを活用した
パフォーマンステスト
- etc...



当社は APN (AWS Partner Network)
コンサルティングパートナー です。

ライセンスリスクの確認

- 使用しているOSS、著作権者、
ライセンス条件を正しく把握
- 権利の瑕疵の発生を予防
- OSS自動検出ツール
「Palamida™」を使用



PALAMIDA™

Application Security for Open Source Software

当社は 米国PALAMIDA社の
パートナー です。

サポート力向上のための更なる挑戦

■ ソースコード静的解析ツール 「コベリティ®」を使った、不具合 発見と修正へトライ中。

- クラッシュ
- リソースリーク
- 脆弱性
- ...

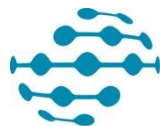


当社は 米国シノプシス社(旧:コベリティ社)の
販売代理店 です。

本日紹介した当社ソリューション



ThemiStruct
テミストラクト



PALAMIDA™
Application Security for Open Source Software



ご清聴ありがとうございました。



ThemisStruct
テミストラクト

【お問合せ先】

株式会社オージス総研

TEL: 03-6712-1201 / 06-6871-7998

E-mail: info@ogis-ri.co.jp

