

OpenID Connectによる Shibboleth IdPとEntra IDの認証連携 ～学認の認証をさらにセキュアにするために必要なこと～

2024年12月11日

サイオステクノロジー株式会社

プロフェッショナルサービス サービスライン



Noriyuki TAKEI

武井 宜行



Information

- サイオステクノロジー株式会社
- Microsoft MVP for AI Platform

blog

<https://tech-lab.sios.jp/>

Twitter

@noriyukitakei

Favorites

- Azure
- スカッシュ
- スキー
- ライブ配信
- 甘いもの
- 走ること
- ストリートファイター6

core skill

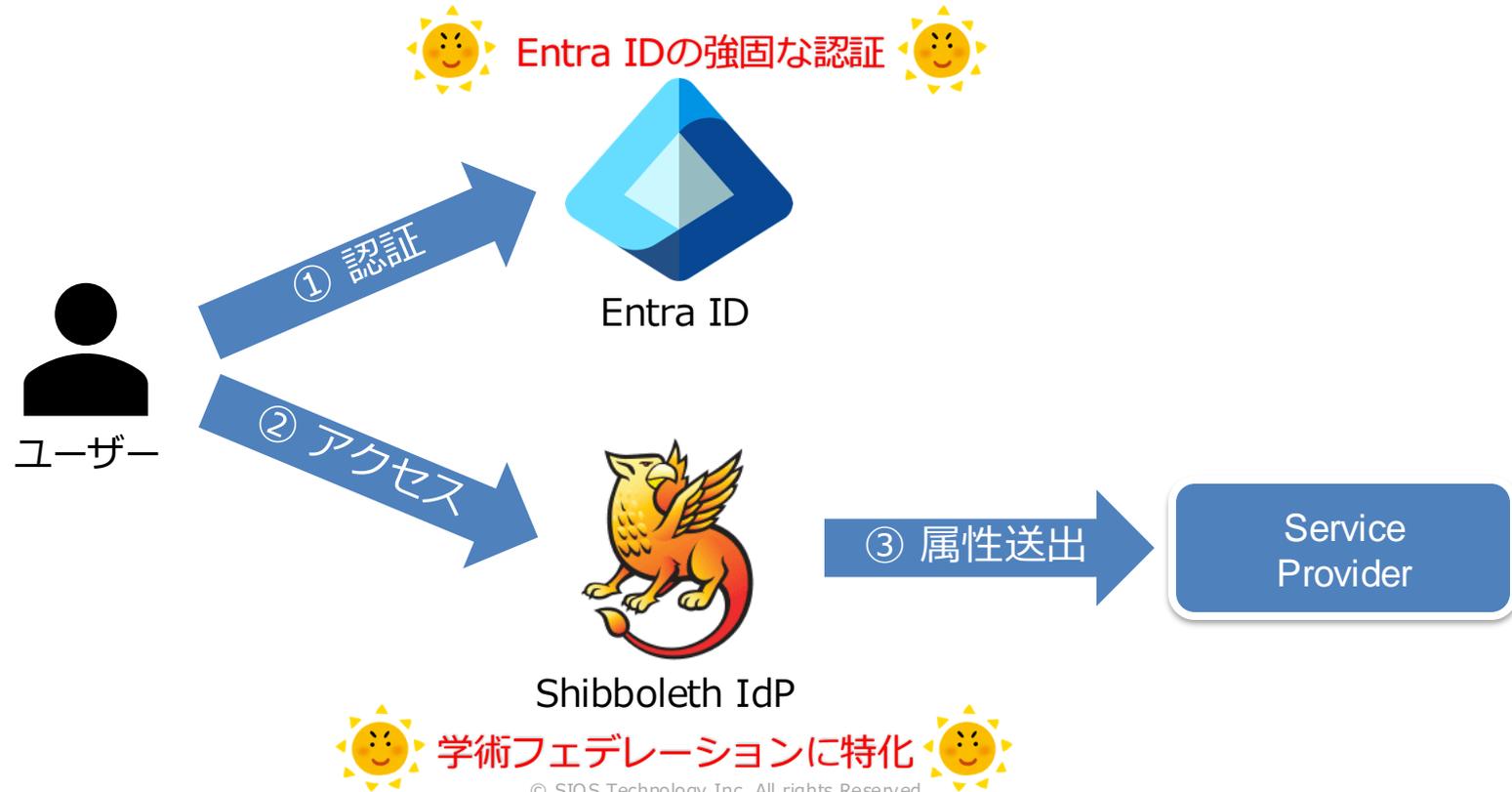
Azureによるクラウドネイティブな
アプリ開発



1. Shibboleth IdPとは？
2. Entra IDとは？
3. OpenID Connectとは？
4. Shibboleth IdPにおける課題と解決策
5. 解決のためのコアテクノロジー(ExternalAuthnConfigurationとOpenID Connect)
6. SIOS Authn Module for Azure AD

本セッションの目的

Shibboleth IdPとEntra IDをOpenID Connectで連携をして、Shibboleth IdPの認証をより強化にする方法をお伝えします。



Shibboleth IdPとは？

Shibboleth IdPの3つの特徴

1 標準規格への準拠

SAMLやOpenID Connect、CAS等の標準的な認証プロトコルをサポートしており、他のシステムとの互換性が高いです。

2 柔軟で高度なカスタマイズ

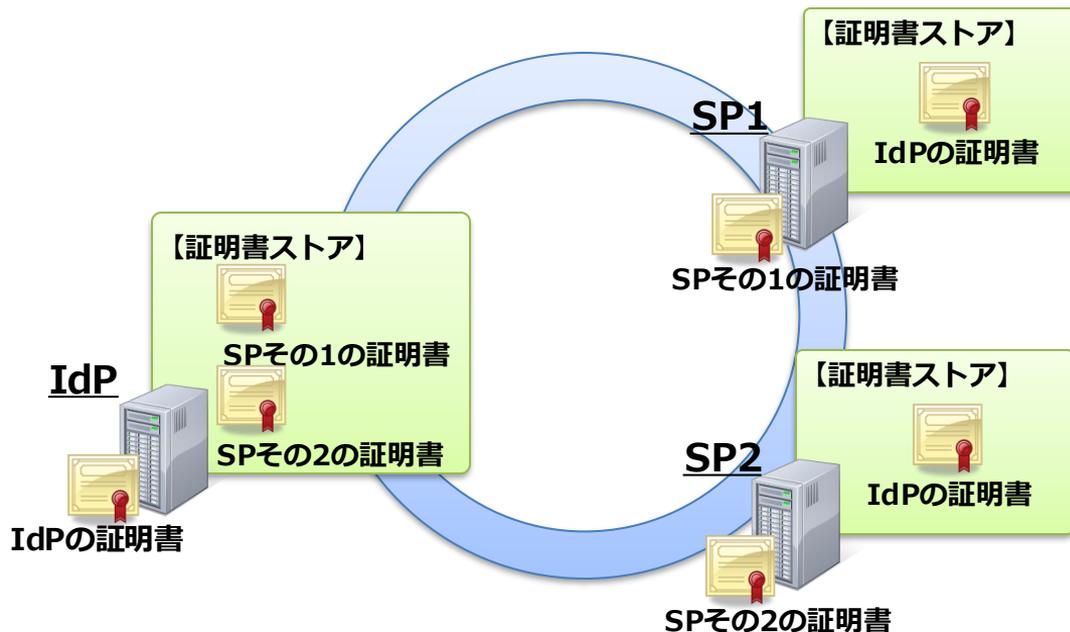
認証フローのカスタマイズや、LDAP、データベース、外部認証システム（例：MFA、OAuth）など、様々なバックエンド認証ソースを利用可能。

3 学術フェデレーションに特化

認証フェデレーション環境で必要となるSAMLメタデータを公開リポジトリ（例：学認やeduGAINのメタデータリポジトリ）から定期的を取得・更新する機能を提供します。これにより、新しいサービスプロバイダー（SP）やIDプロバイダー（IdP）が追加・変更された場合でも、最新情報を自動的に反映できます。

Shibboleth IdPとは？

シングルサインオンを行うためには、SSOサーバ(以降IdPと呼ぶ)とサービスプロバイダ(以降SPと呼ぶ)の間で信頼関係が結ばれてないといけません。「信頼関係を結ぶ」とは、IdPとSPが互いの公開鍵証明書を交換し、それをそれぞれの「証明書ストア」に登録することを指します。これにより、認証情報が正しいものであることを確認し、安全なシングルサインオンが実現されます。



Shibboleth IdPとは？

世の中には、全ての大学向けに色々なサービス(論文検索サービスなど)が存在します。これを学生だけに使うためには、各大学でIdPを立てて、各サービスにシングルサインオンすればいいという発想になります。でもこれでは不都合が生じます。それは次のページで説明します。

論文検索サービス



eラーニング



ファイル共有サービス



A大学



IdP

B大学



IdP

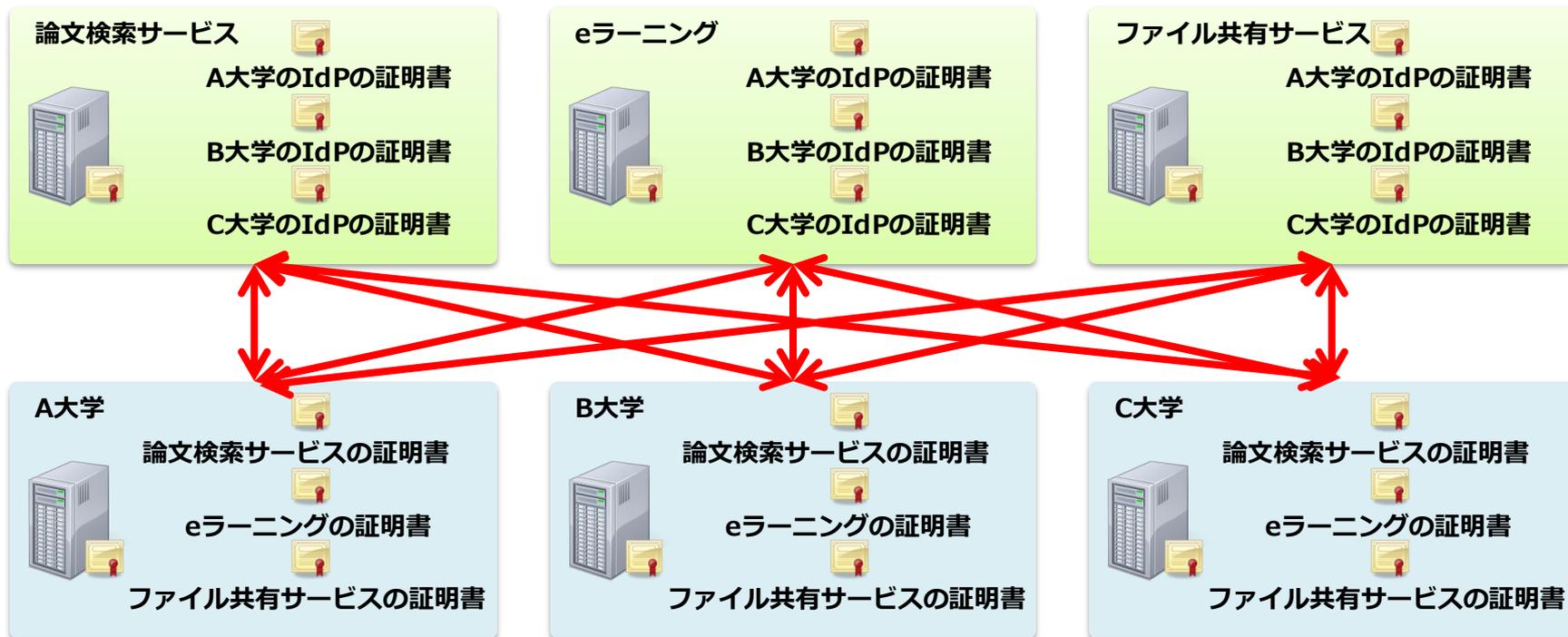
C大学



IdP

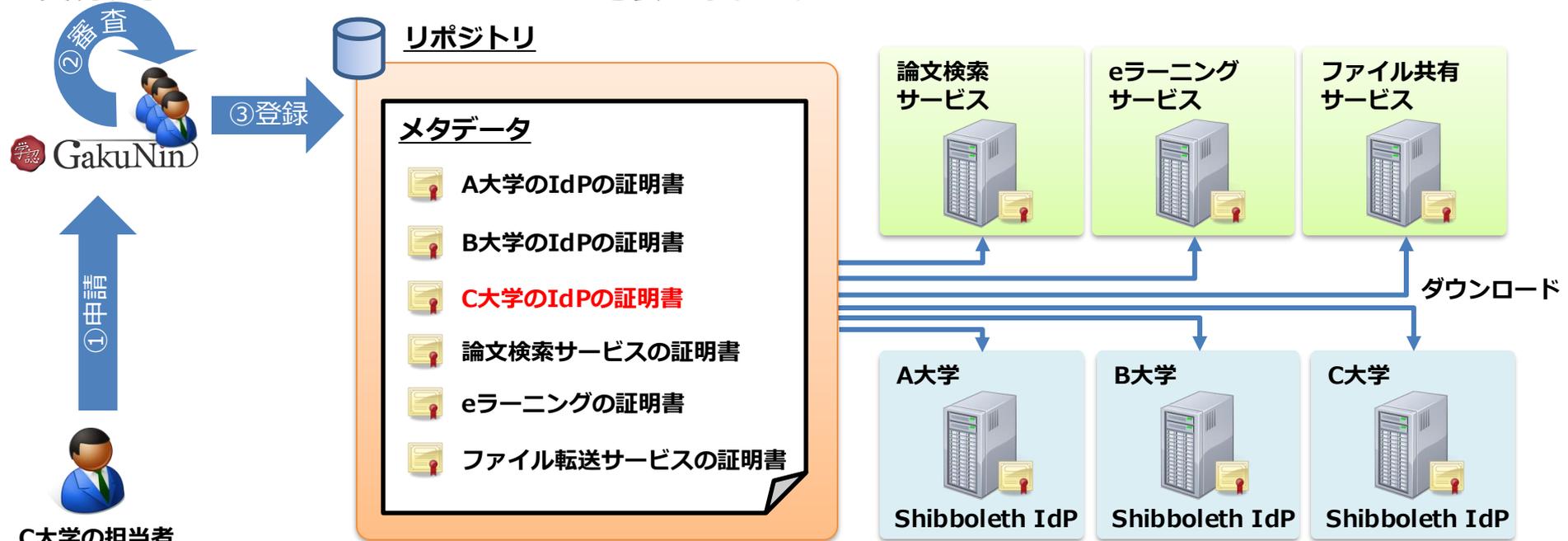
Shibboleth IdPとは？

シングルサインオンするためには、先ほど説明したようにお互いの証明書を交換しあって、トラストサークルを構築しなければなりません。各大学と各サービスがお互いの証明書を交換しあうというのは現実的ではありません。下記のように膨大な組み合わせになってしまいます。



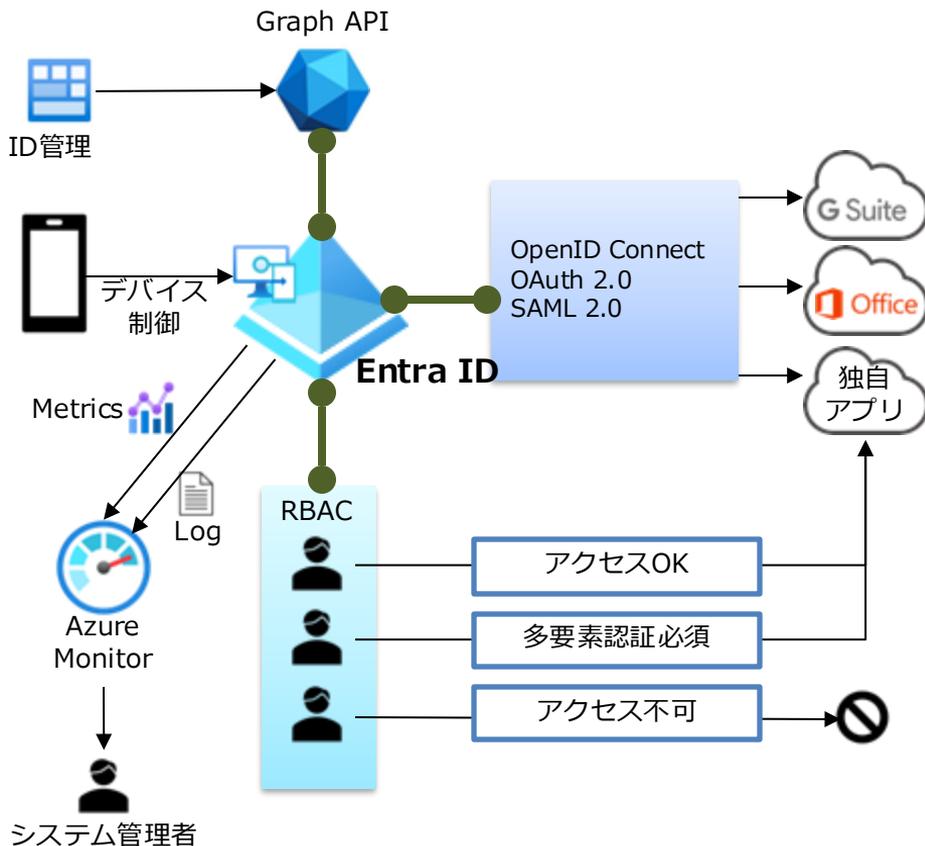
Shibboleth IdPとは？

そこで下記のような仕組みを構築します。まず、大学の担当者が「学認」という団体に申請します(①)。学認が責任を持って大学を審査し(②)、問題無いと認められれば、リポジトリ内のメタデータに大学の証明書を登録します(③)。そのメタデータを各大学のIdPと各サービスがダウンロードします。このようにして、各大学と各サービスがお互いの証明書を交換しあわなくても、トラストサークルが構築できるわけです。この仕組みを実現するためにShibbolethというものが必要になります。



Entra IDとは？

Entra IDとは？



概要

Entra IDは以下の特徴を持つクラウドベースのアイデンティティとアクセス管理サービスです。

- SaaSであり、処理性能はほぼ無限にスケールする。
- Open ID Connect、SAML 2.0、OAuth 2.0などの様々な認証プロトコルに対応している。
- ユーザーやグループ単位で認証方法を制御するルールベースのアクセス制御(RBAC)を提供する。
- Azure Monitorとの連携により、監視やログデータの取得・分析が可能である。
- さまざまなAzure サービスとの親和性が高い。

Entra IDは安全かつ柔軟なアイデンティティとアクセス管理を実現し、組織のセキュリティと効率性を向上させます。

導入の効果

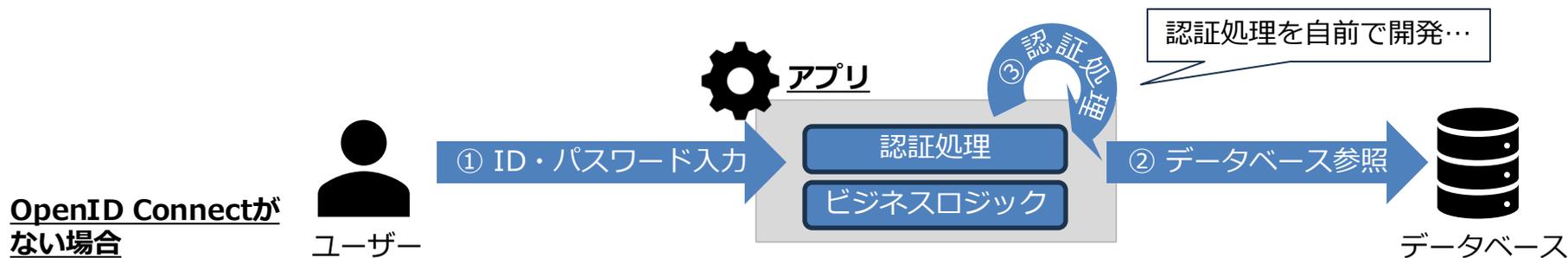
Microsoft Entra IDは、SaaSベースのサービスであり、その処理性能はほぼ無限にスケーリングするので、授業開始前などのアクセスが集中する際の負荷に耐えることが可能です。

また、ブラウザベースのGUIにより、SPの追加・削除が容易であり、運用管理面でのサービス向上が期待されます。

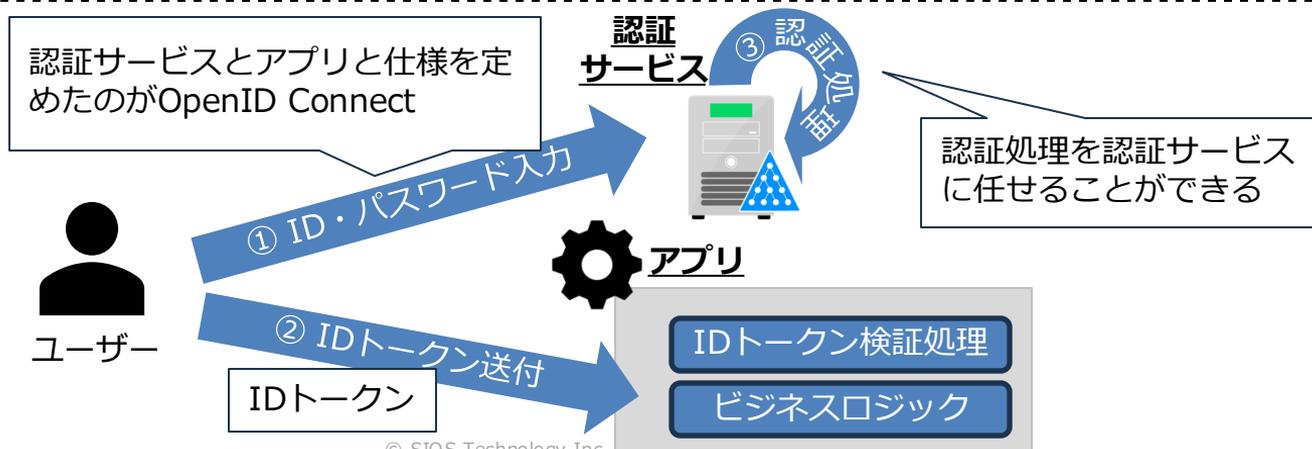
OpenID Connectとは？

OpenID Connectとは？

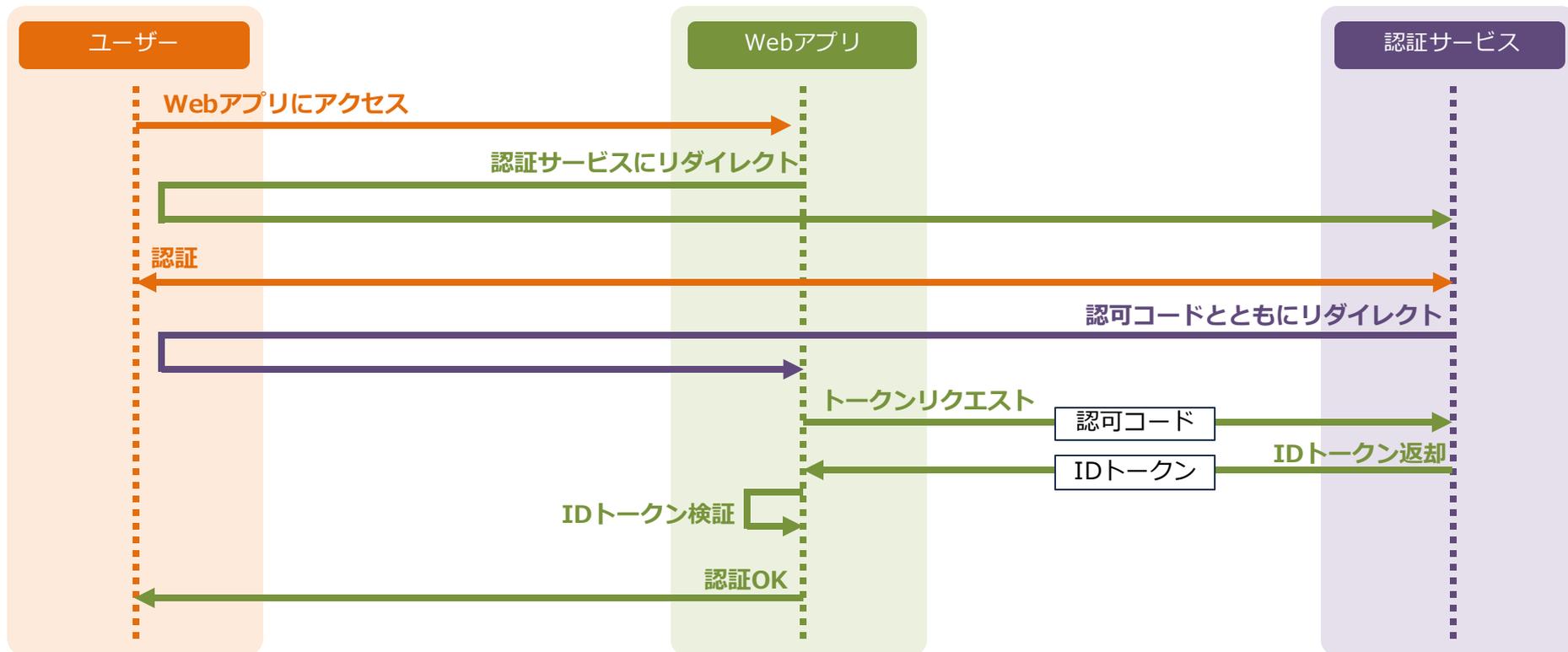
小生が若いころは自前で認証処理を開発することが当たり前でしたが、SAMLやOpenID Connectが登場して、認証処理を認証サービスに委任することができる機会が多くなりました。



OpenID Connectがある場合



認可コードフロー



IDトークンを構成するJSON Web Token

ヘッダー

```
{  
  "kid": "1e9gdk7",  
  "alg": "RS256"  
}
```

BASE64URLエンコード

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTJ5In0=

ペイロード

```
{  
  "sub": "248289761001",  
  ...  
}
```

BASE64URLエンコード

eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0Ijoi

シグニチャ

```
eyJhenAiOiIxOTkzODM0MzIwNjUta2dqbzJmc2hsMTd0aGNpODNwN2IydGJ...  
ydGJ...
```

BASE64URLエンコード



暗号鍵で署名

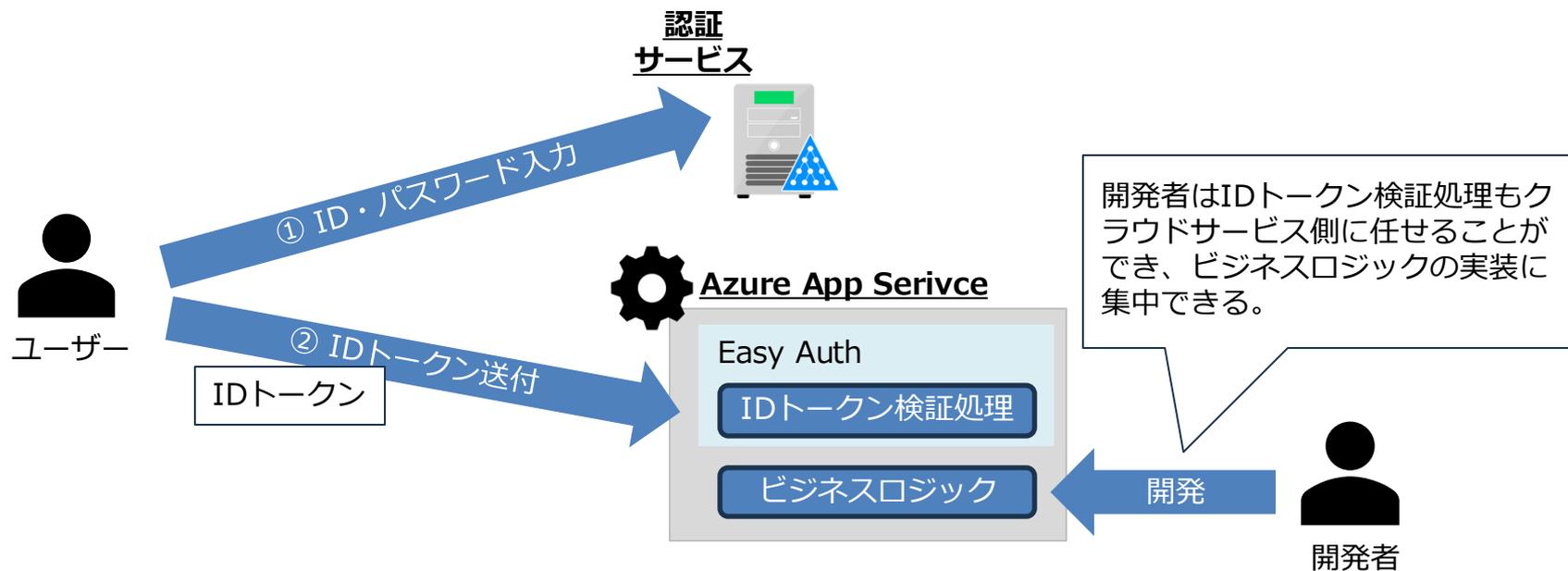
SflKxwRJSMeKKF2QT4f...

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXLTJ5In0= . eyJzdWIiOiIxMjM0NTY3ODkwIiwiaWF0Ijoi . SflKxwRJSMeKKF2QT4f...

JSON Web Token

OpenID Connectに対応したクラウドサービス

OpenID Connectに対応したPaaSサービス(Azure App Serviceなど)を導入すると、IDトークン検証処理もクラウド側に任せることができ、開発者はビジネスロジックの実装に集中できる。



Shibboleth IdPにおける課題と解決策

Shibboleth IdPにおける課題と解決策

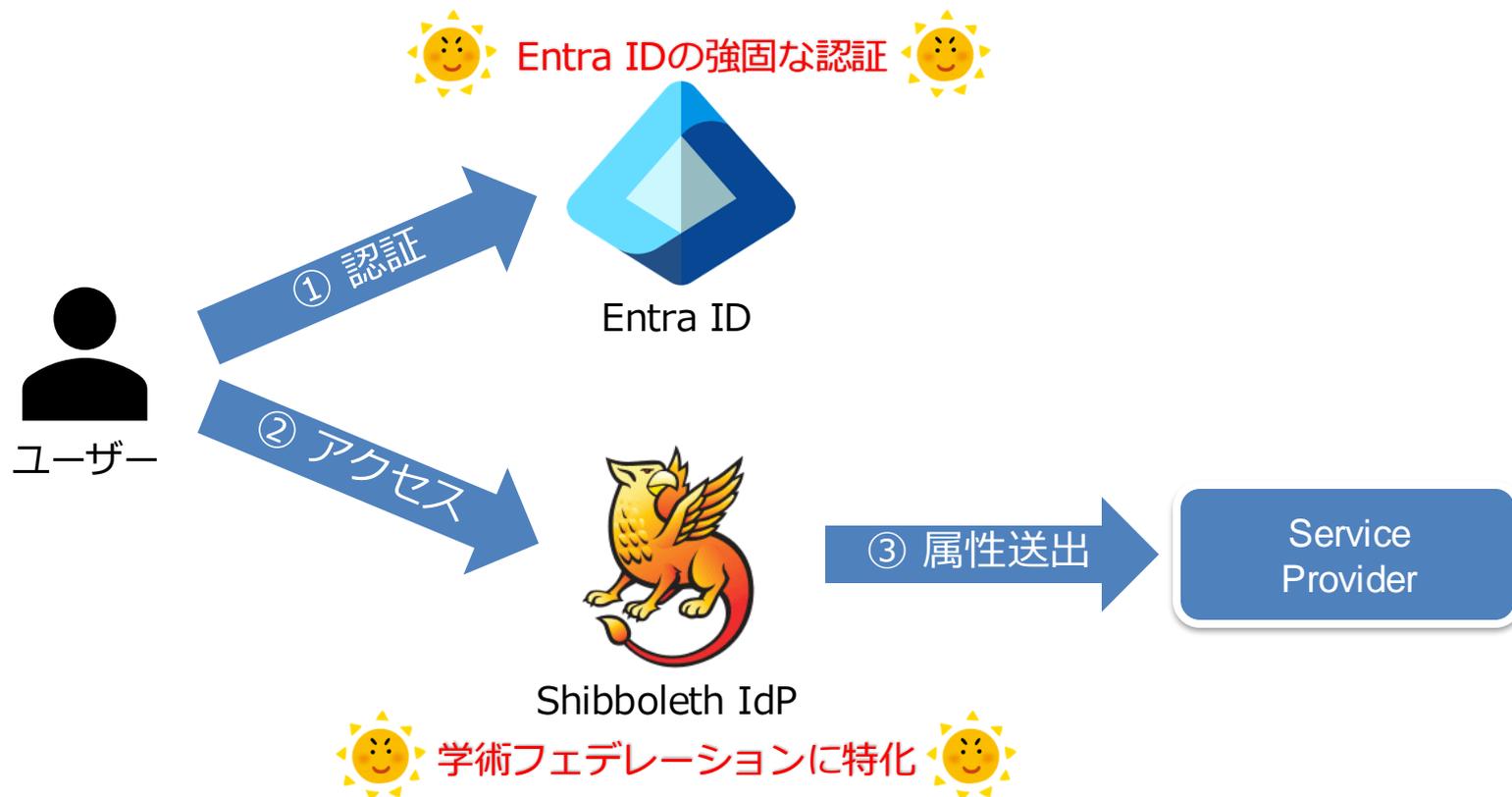


Shibboleth IdPとEntra IDにはそれぞれ、得意とする部分が異なる。

	Shibboleth IdP	Entra ID
認証方式の多様さ	×	○
	TOTPのみとなり、種類は少ない。	TOTP、生体認証、Push通知認証と多様な認証方式が利用できる。
学術フェデレーションへの対応	○	×
	メタデータの自動取得、SPごとへの柔軟な属性リリースとポリシー設定等、学術フェデレーションに特化している。	Shibboleth IdPが備えているような、学術フェデレーションに特化した機能はない

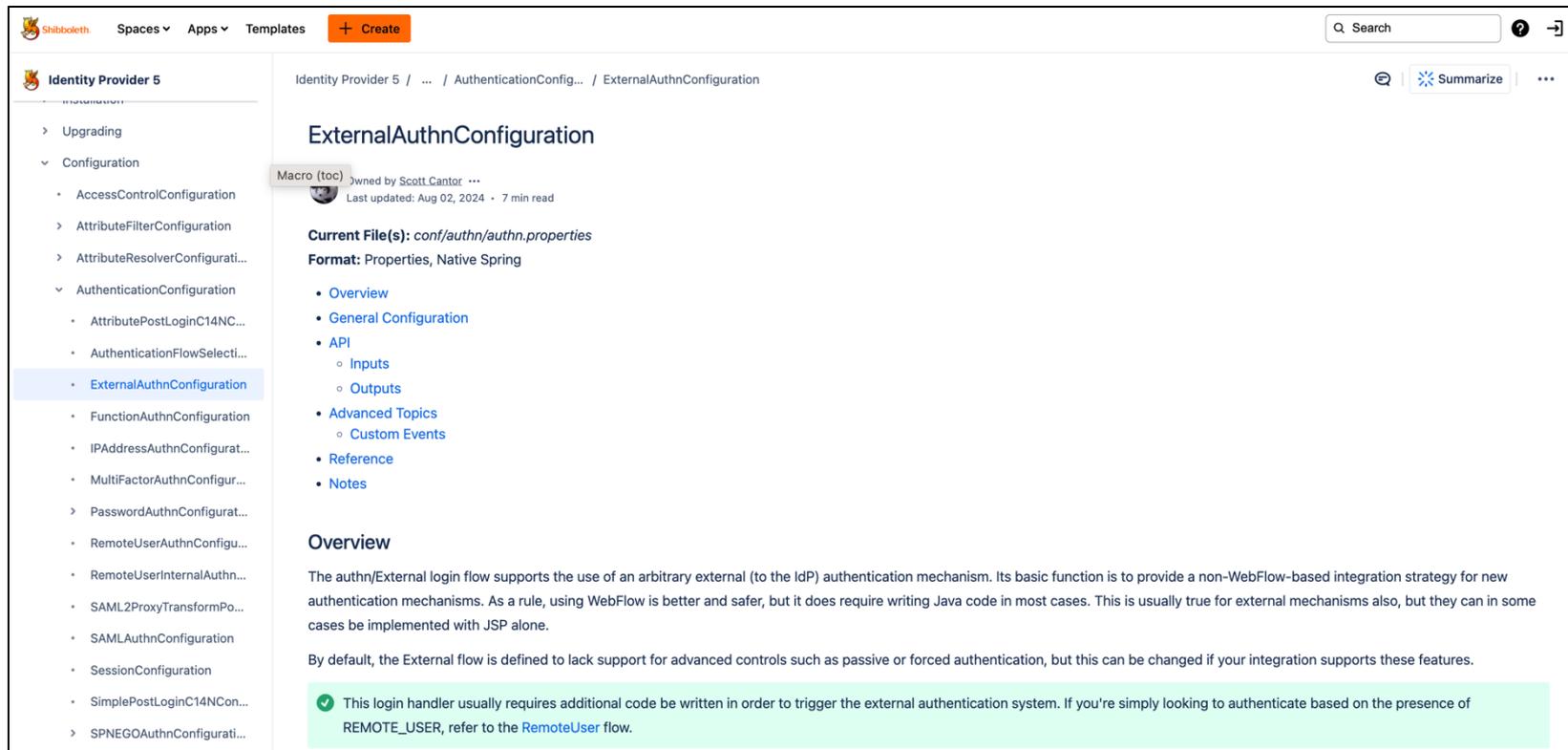
Shibboleth IdPにおける課題と解決策

Shibboleth IdPとEntra IDを連携させ、お互いの得意な部分を活かす！！



解決のためのコアテクノロジー (ExternalAuthnConfigurationとOpenID Connect)

ExternalAuthnConfiguration



The screenshot shows the configuration page for ExternalAuthnConfiguration in the SIOS Identity Provider 5. The page is titled "ExternalAuthnConfiguration" and is part of the "AuthenticationConfig..." section. The current file is identified as "conf/authn/authn.properties" in "Properties, Native Spring" format. A table of contents is provided, listing sections such as Overview, General Configuration, API (Inputs, Outputs), Advanced Topics (Custom Events), Reference, and Notes. The Overview section is currently selected and contains the following text:

The authn/External login flow supports the use of an arbitrary external (to the IdP) authentication mechanism. Its basic function is to provide a non-WebFlow-based integration strategy for new authentication mechanisms. As a rule, using WebFlow is better and safer, but it does require writing Java code in most cases. This is usually true for external mechanisms also, but they can in some cases be implemented with JSP alone.

By default, the External flow is defined to lack support for advanced controls such as passive or forced authentication, but this can be changed if your integration supports these features.

A green callout box at the bottom of the Overview section states: "This login handler usually requires additional code be written in order to trigger the external authentication system. If you're simply looking to authenticate based on the presence of REMOTE_USER, refer to the RemoteUser flow."

ExternalAuthnConfigurationのメリット

1 Shibboleth IdP以外の外部のIdPに認証を委任できる

Shibboleth IdPの認証を他のIdPに委任できるので、認証の強固なIdPで認証をしつつ、Shibboleth IdPの学術フェデレーションに強いというメリットも活かせる。

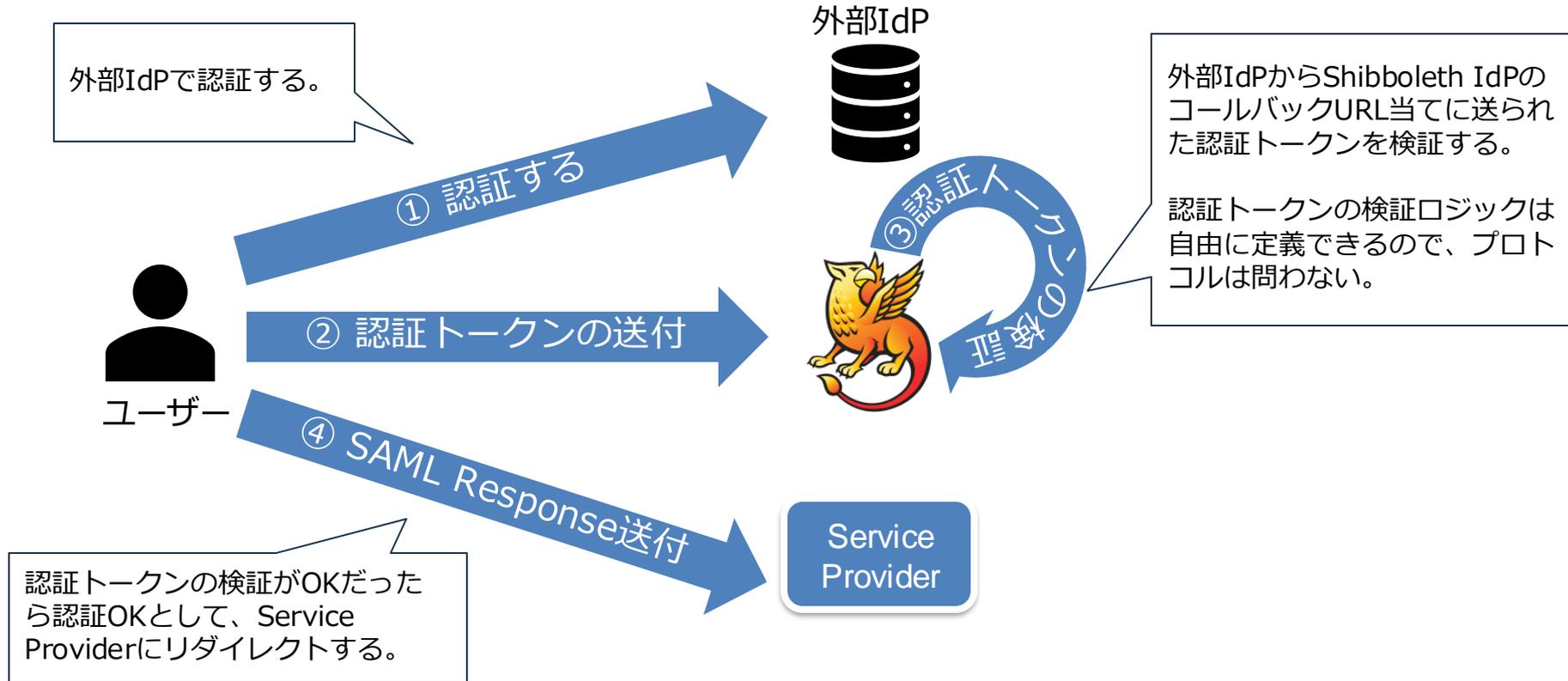
2 多様なプロトコルに対応可能

外部のIdPで認証を行った後、その結果をShibboleth IdPに戻す仕組みである。具体的には、認証後にShibboleth IdPが用意した特定のコールバックURLにアクセスし、その内容を検証する。この仕組みは認証プロトコルに依存しないため、SAMLやOpenID Connect (OIDC) など、どのプロトコルでも利用可能となる。

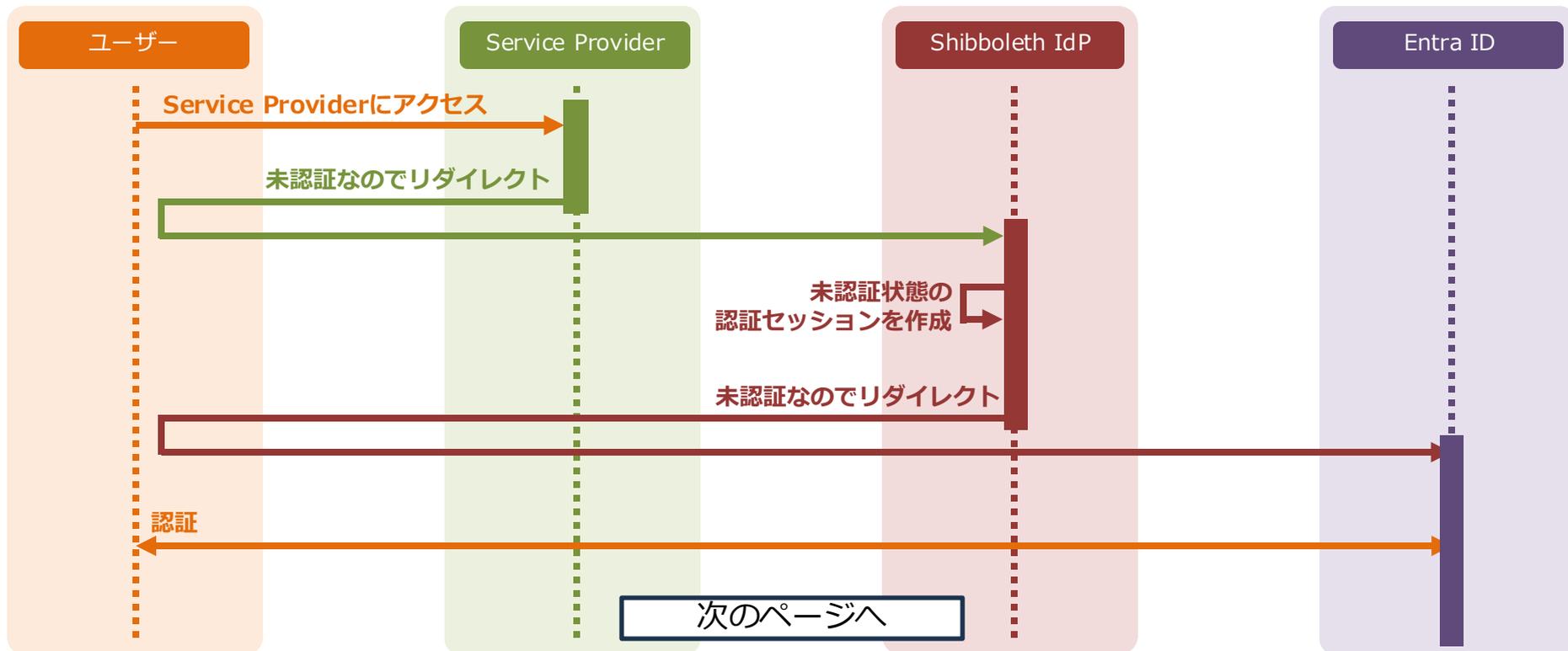
3 他の認証処理との組み合わせが可能

ExternalAuthnConfigurationはShibboleth IdPの認証フローの1つであるため、他の認証(ワンタイムパスワードやX509証明書認証など)と組み合わせることが可能であり、その組み合わせにより、さらに強固な認証が可能となる。

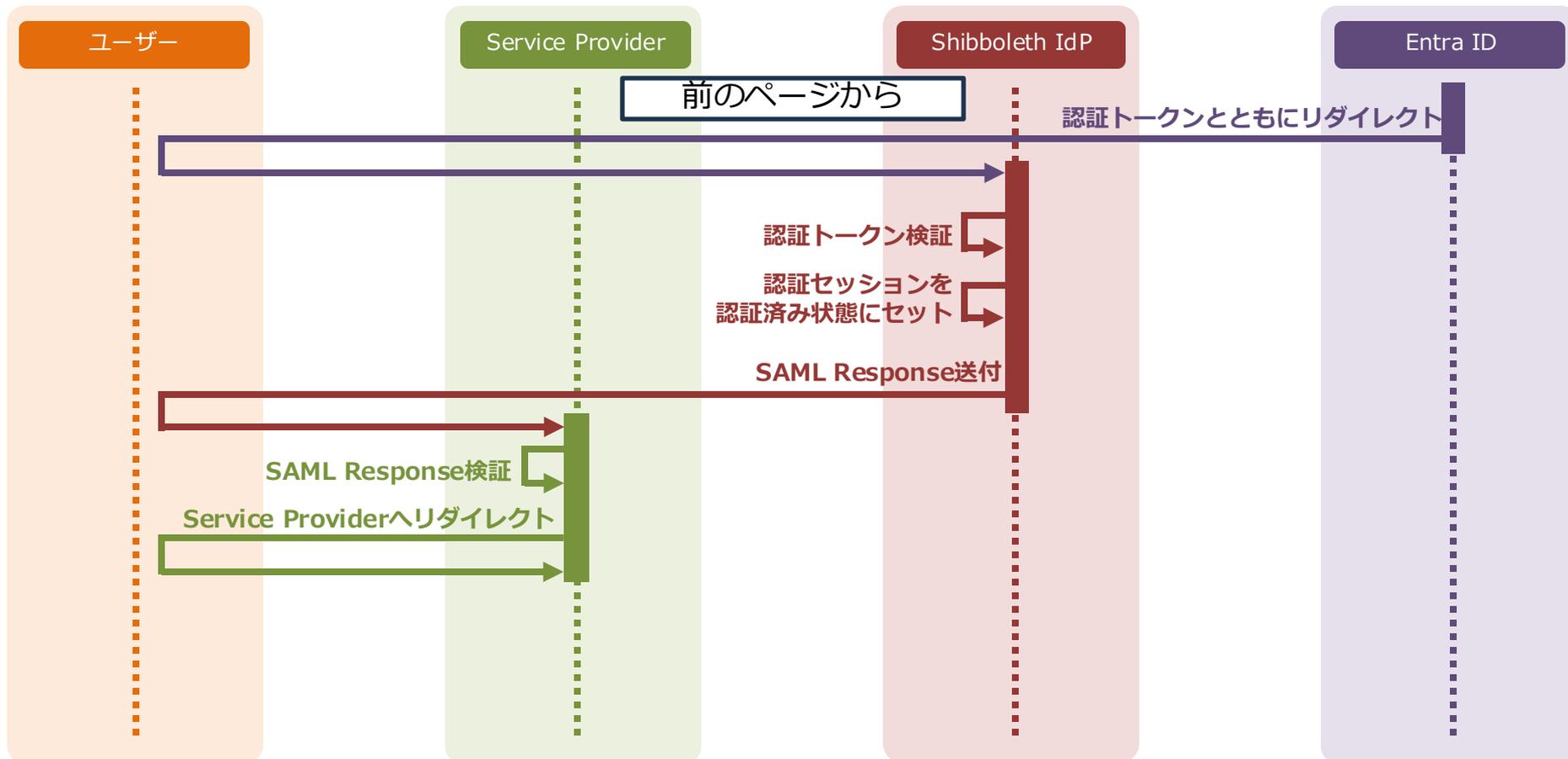
ExternalAuthnConfigurationの概要



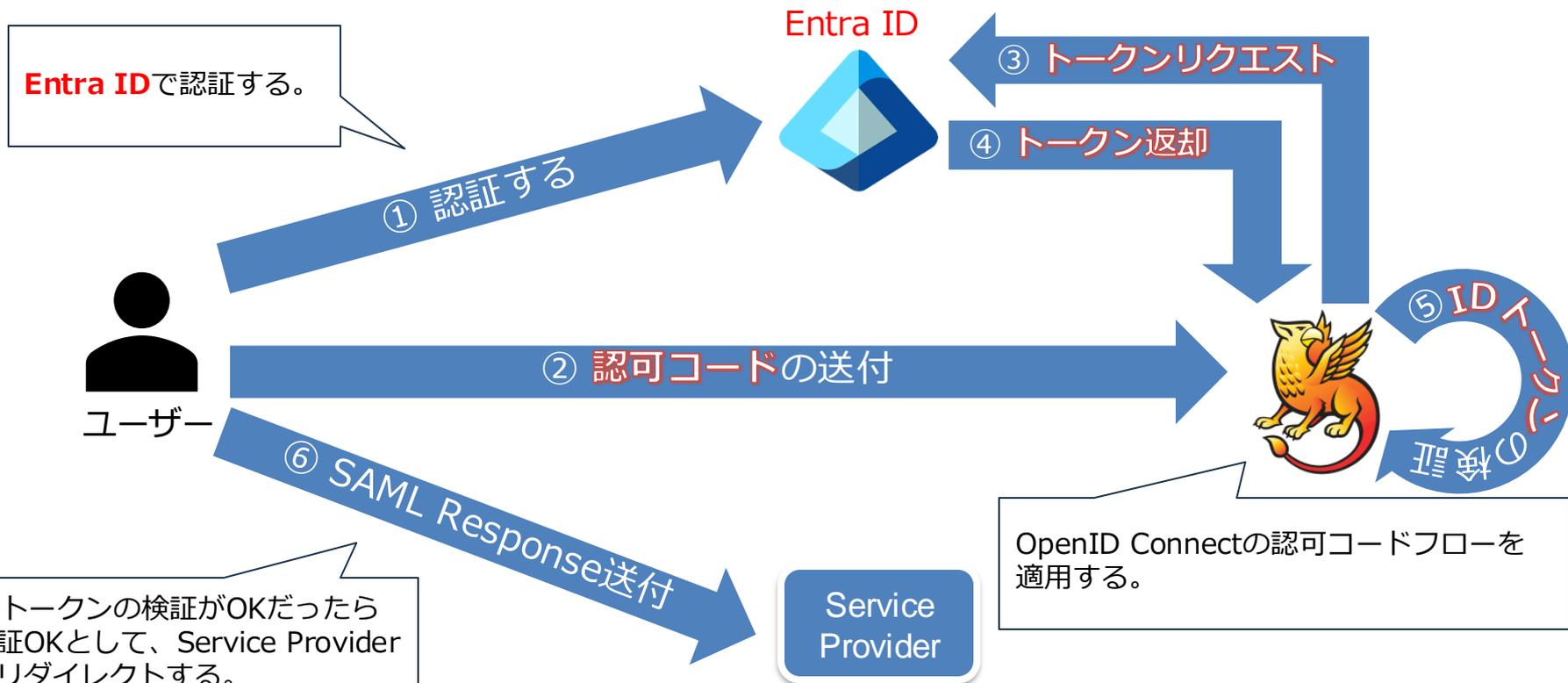
ExternalAuthnConfigurationの認証フロー



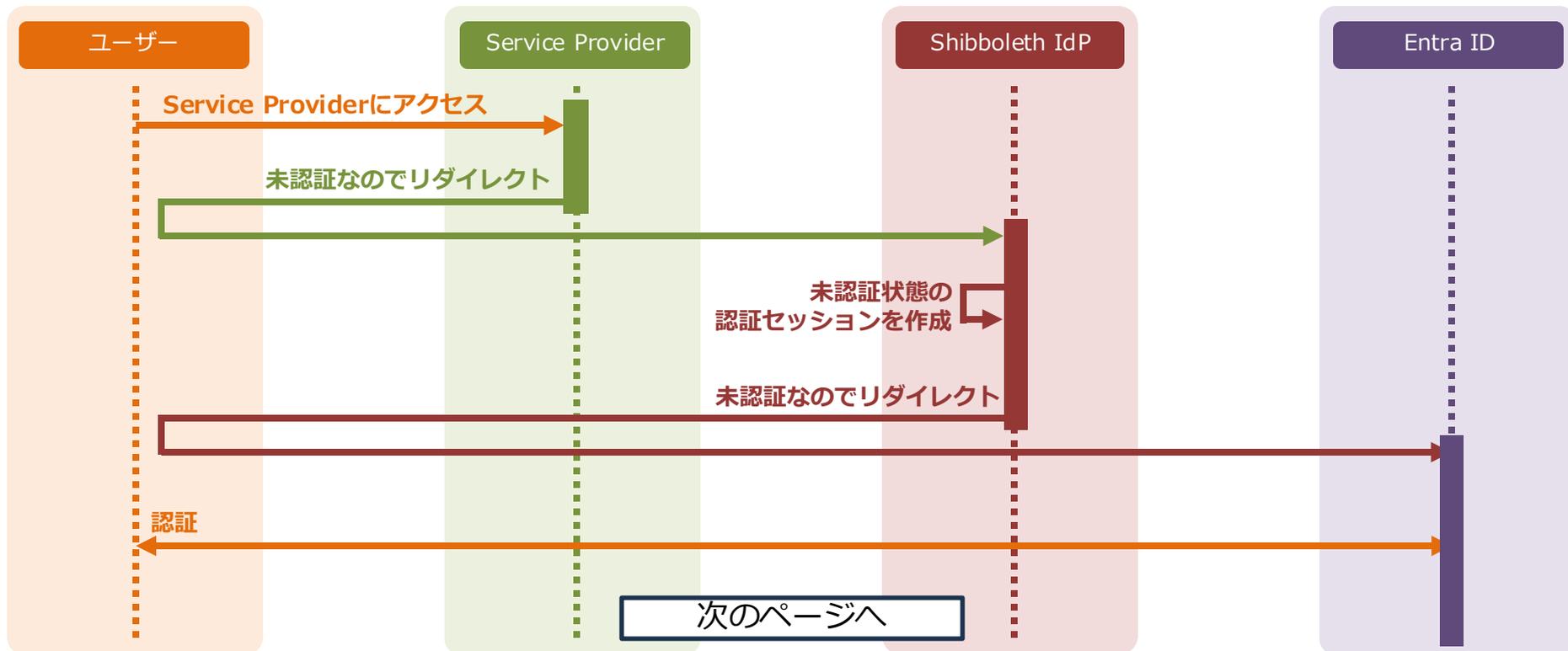
解決のためのコアテクノロジー



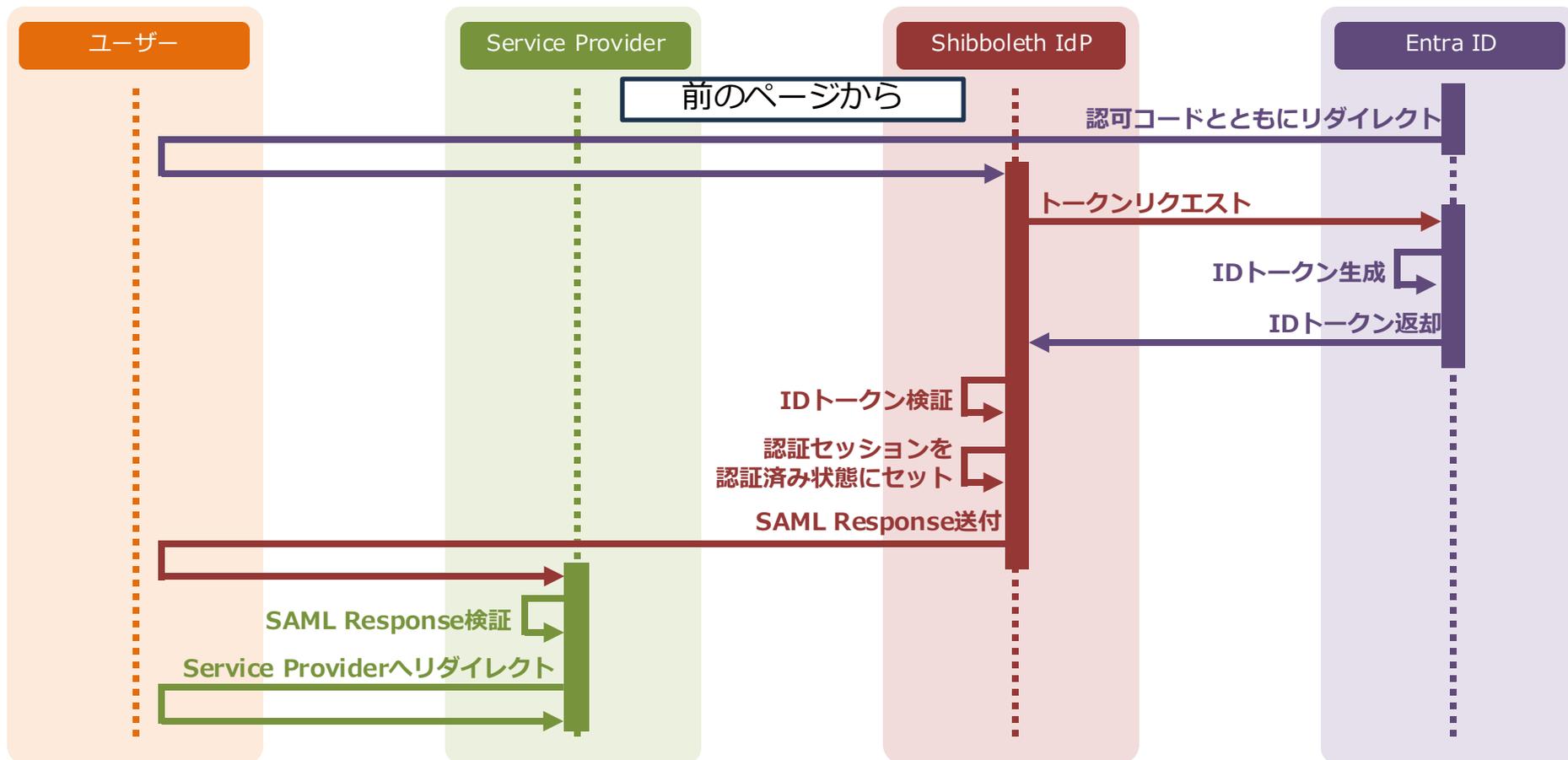
ExternalAuthnConfiguration + OpenID Connect



ExternalAuthnConfiguration + OpenID Connectの認証フロー



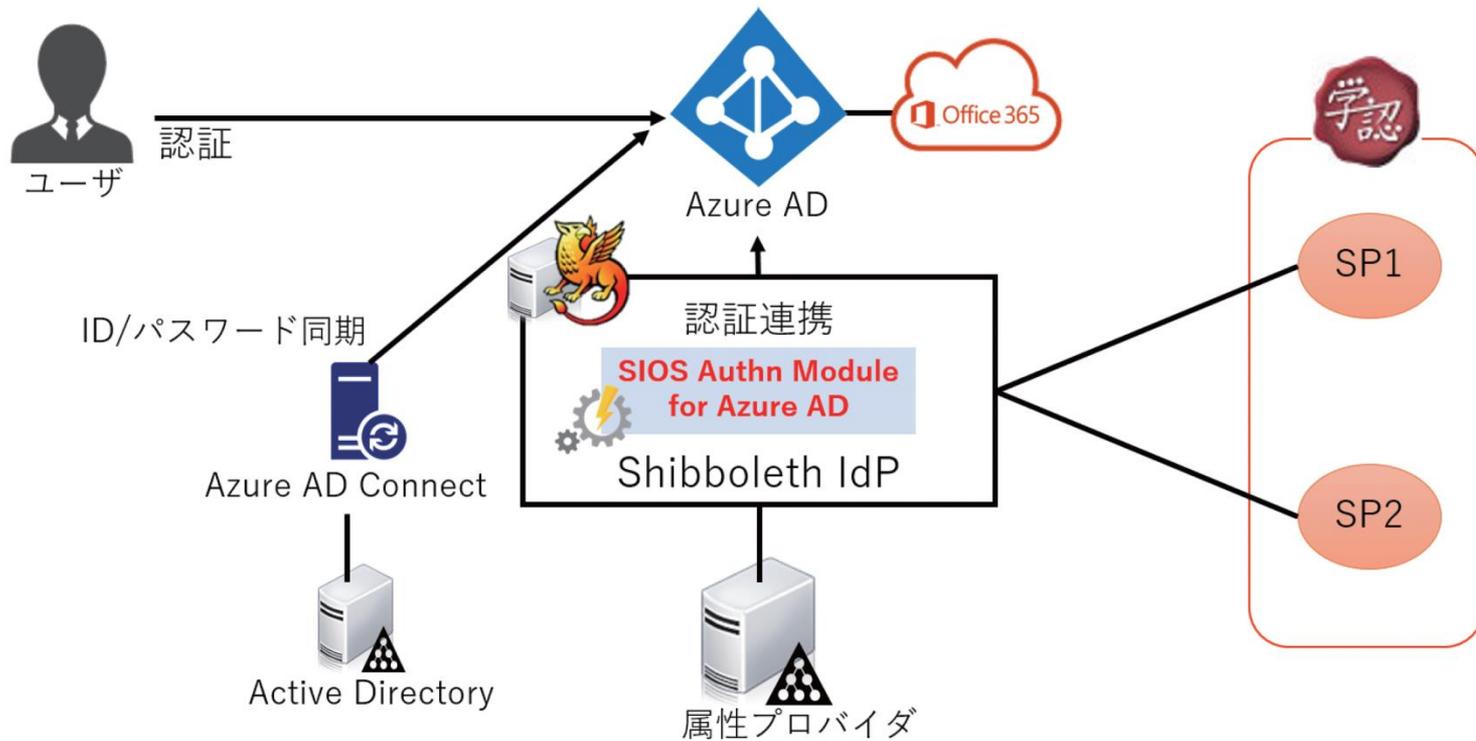
解決のためのコアテクノロジー



SIOS Authn Module for Azure AD

SIOS Authn Module for Azure AD

Entra IDの強固な認証とShibboleth IdPの学術フェデレーションに特化した機能を組み合わせたモジュールを提供しています。



Shibboleth周辺ソリューションのご紹介

1 Shibboleth Management Portal

Shibboleth SPの追加やメタデータの管理などができるWebインターフェースを備えたアプリケーション

2 ワンタイムパスワード認証モジュール

TOTPベースの認証をShibboleth IdPで実現するための追加モジュール

3 代理認証モジュール

SAMLに対応していないレガシーなWebアプリケーションへのシングルサインオンを可能にする追加モジュール

4 IDプロビジョニング

導入が簡易でシンプルなIDプロビジョニングツール(同期元はCSV/MySQL/LDAP、同期先はLDAP、Active Directoryに対応)

5 ユーザープロフィール管理

ユーザープロフィールやパスワードの変更を行うWebインターフェースを備えたアプリケーション

