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

SIOS

© SIOS Technology Inc. All rights Reserved.

Noriyuki TAKEI

武井 宣行

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

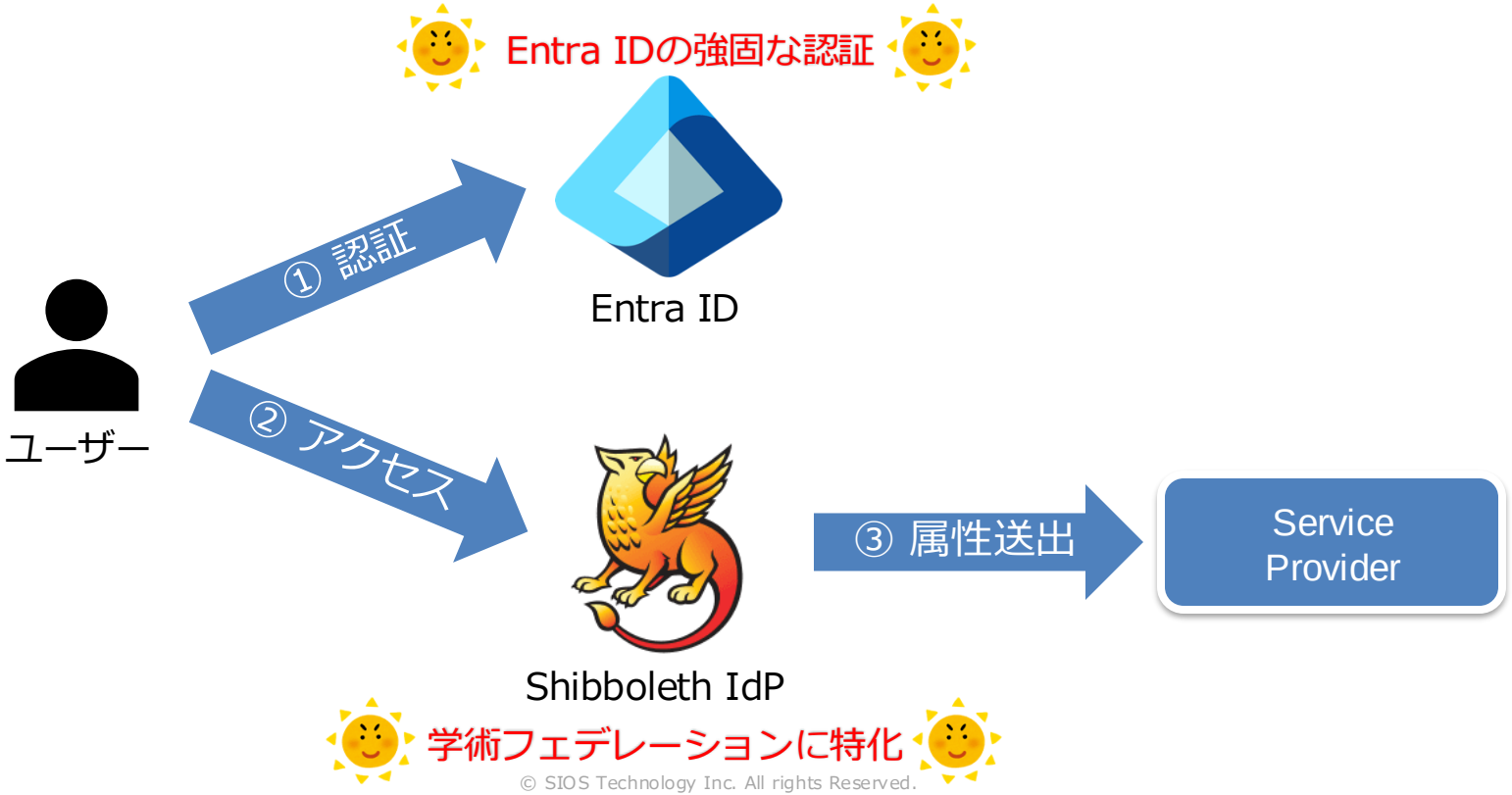
目次

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

© SIOS Technology Inc. All rights Reserved.

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。



© SIOS Technology Inc. All rights Reserved.

Shibboleth IdPとは？

© SIOS Technology Inc. All rights Reserved.

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。

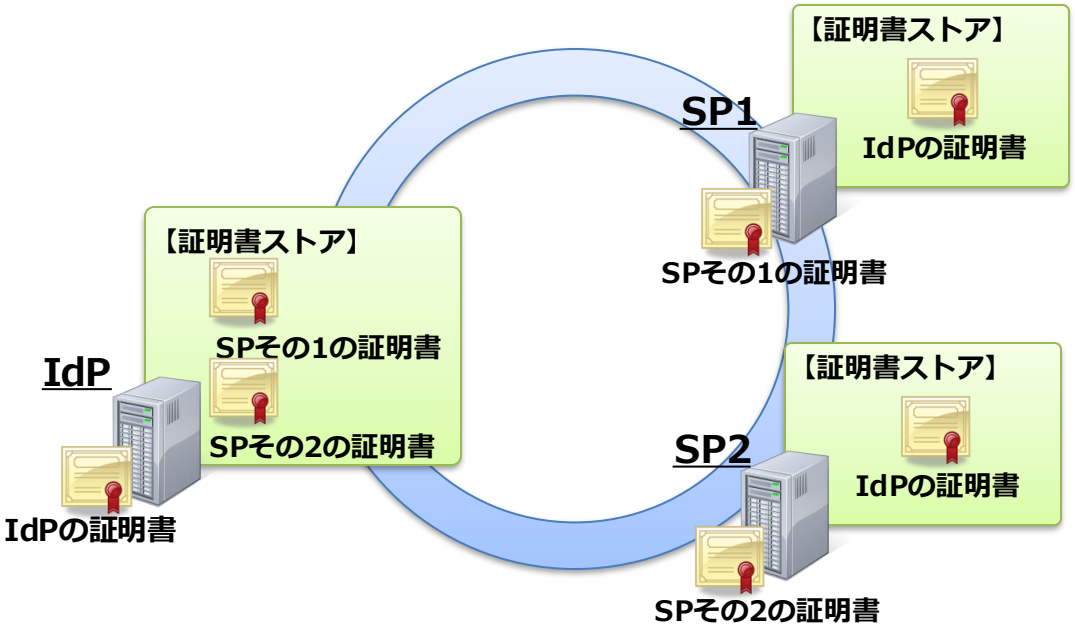
3 学術フェデレーションに特化

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）から定期的に取得・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。

© SIOS Technology Inc. All rights Reserved.

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。



© SIOS Technology Inc. All rights Reserved.

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わせるためには、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

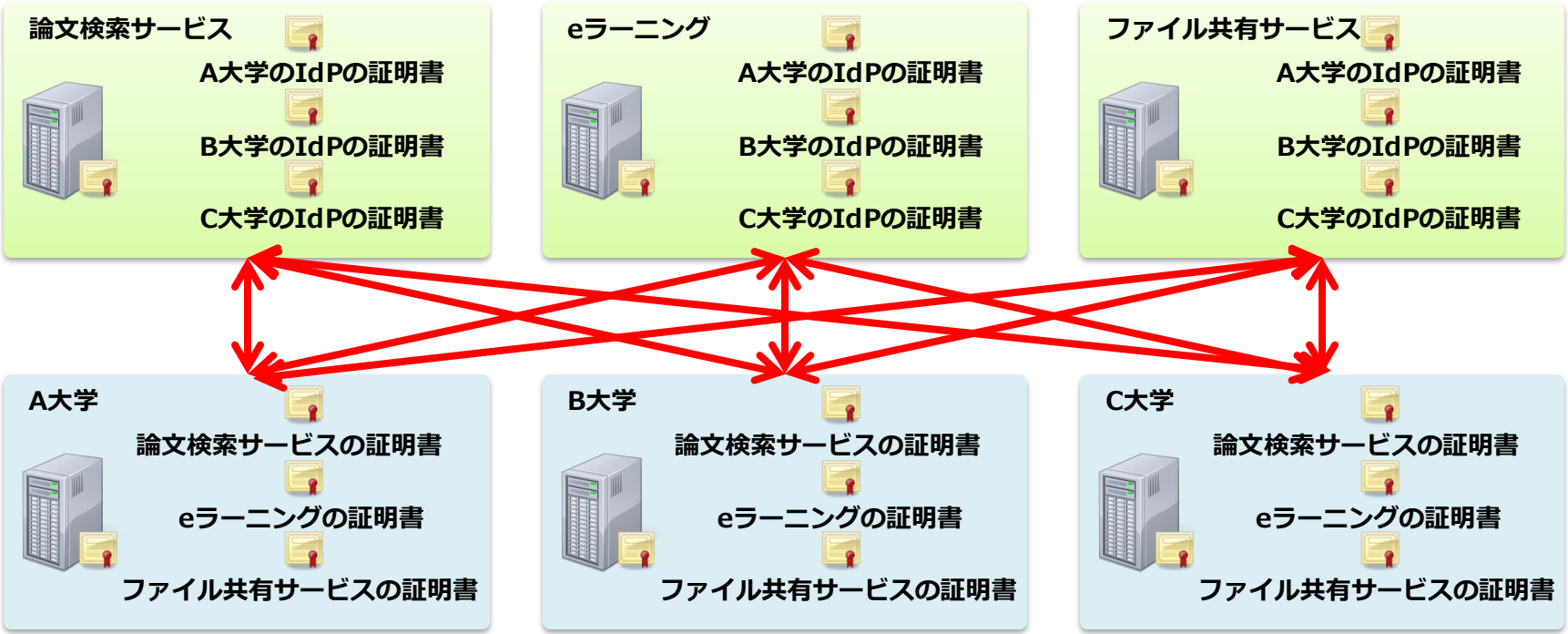
C大学

IdP

© SIOS Technology Inc. All rights Reserved.

Shibboleth IdPとは？

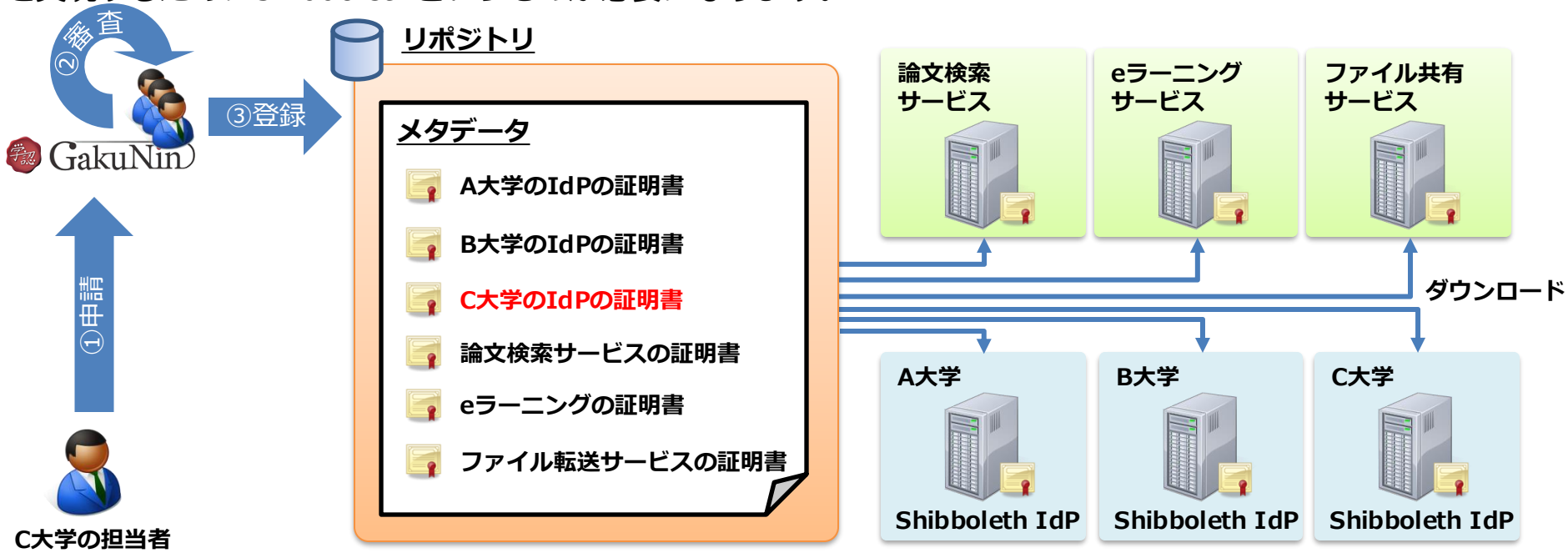
シングルサインオンするためには、先ほど説明したようにお互いの証明書を交換しあって、トラストサークルを構築しなければなりません。各大学と各サービスがお互いの証明書を交換しあうというのは現実的ではありません。下記のように膨大な組み合わせになってしまいます。



© SIOS Technology Inc. All rights Reserved.

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。この仕組を実現するためにShibbolethというものが必要になります。

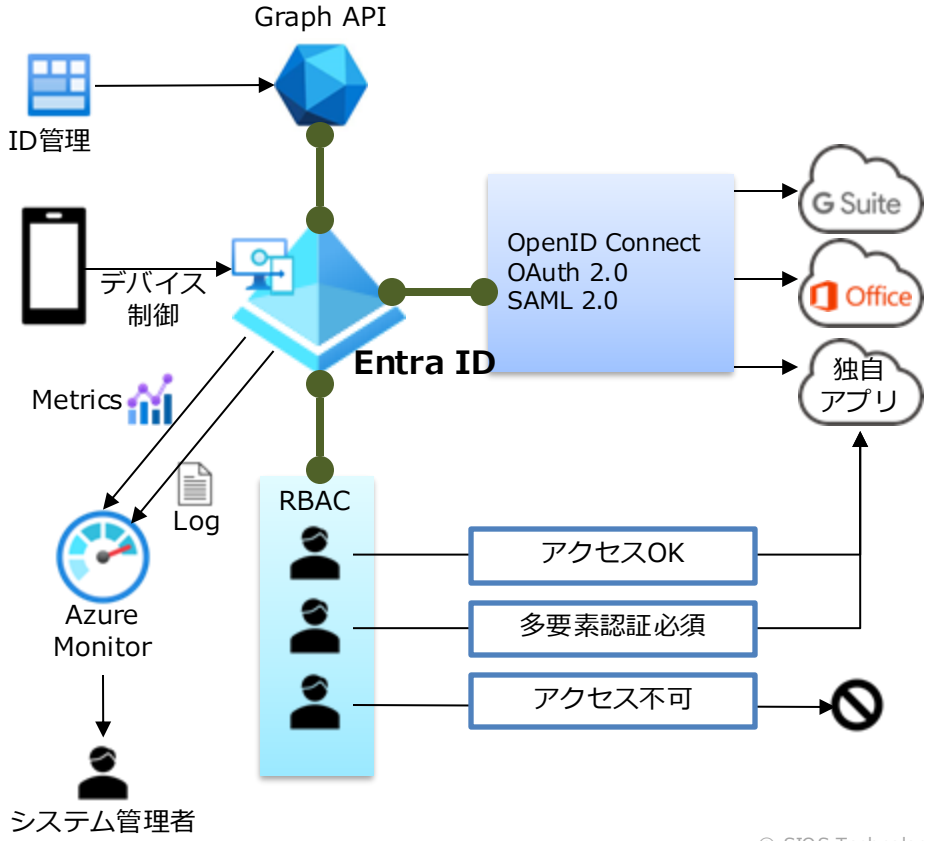


© SIOS Technology Inc. All rights Reserved.

Entra IDとは？

© SIOS Technology Inc. All rights Reserved.

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ロ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。
- ざまざまな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。

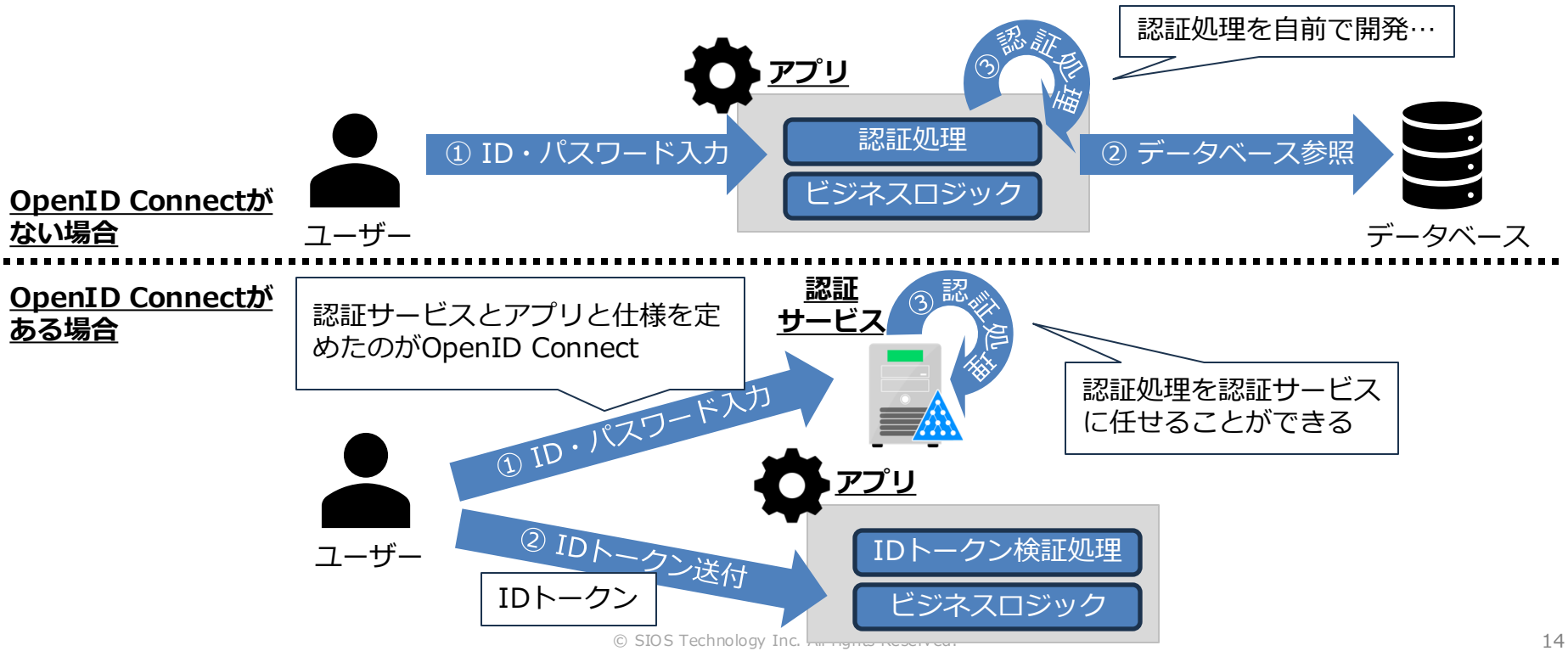
© SIOS Technology Inc. All rights Reserved.

OpenID Connectとは？

© SIOS Technology Inc. All rights Reserved.

OpenID Connectとは？

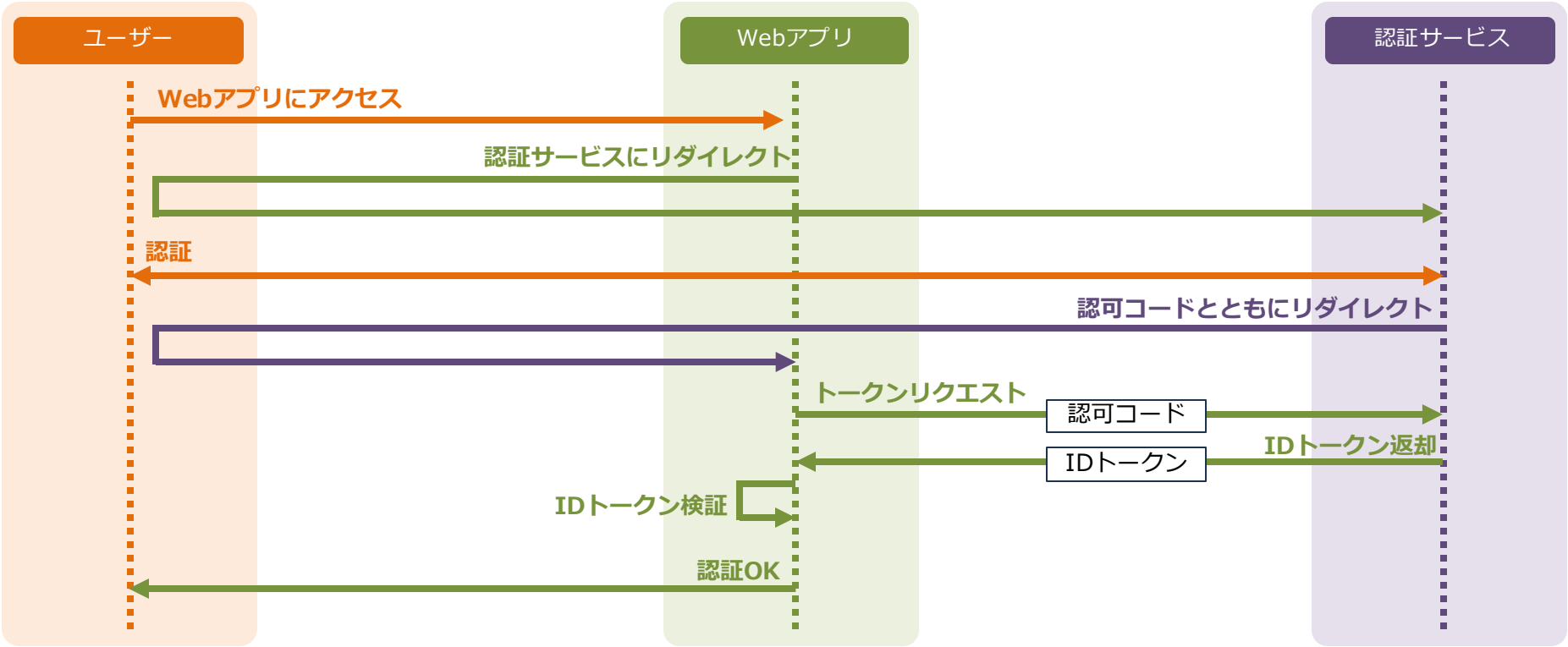
小生が若いころは自前で認証処理を開発することが当たり前でしたが、SAMLやOpenID Connectが登場して、認証処理を認証サービスに委任することができる機会が多くなりました。



© SIOS Technology Inc. All rights reserved.

OpenID Connectとは？

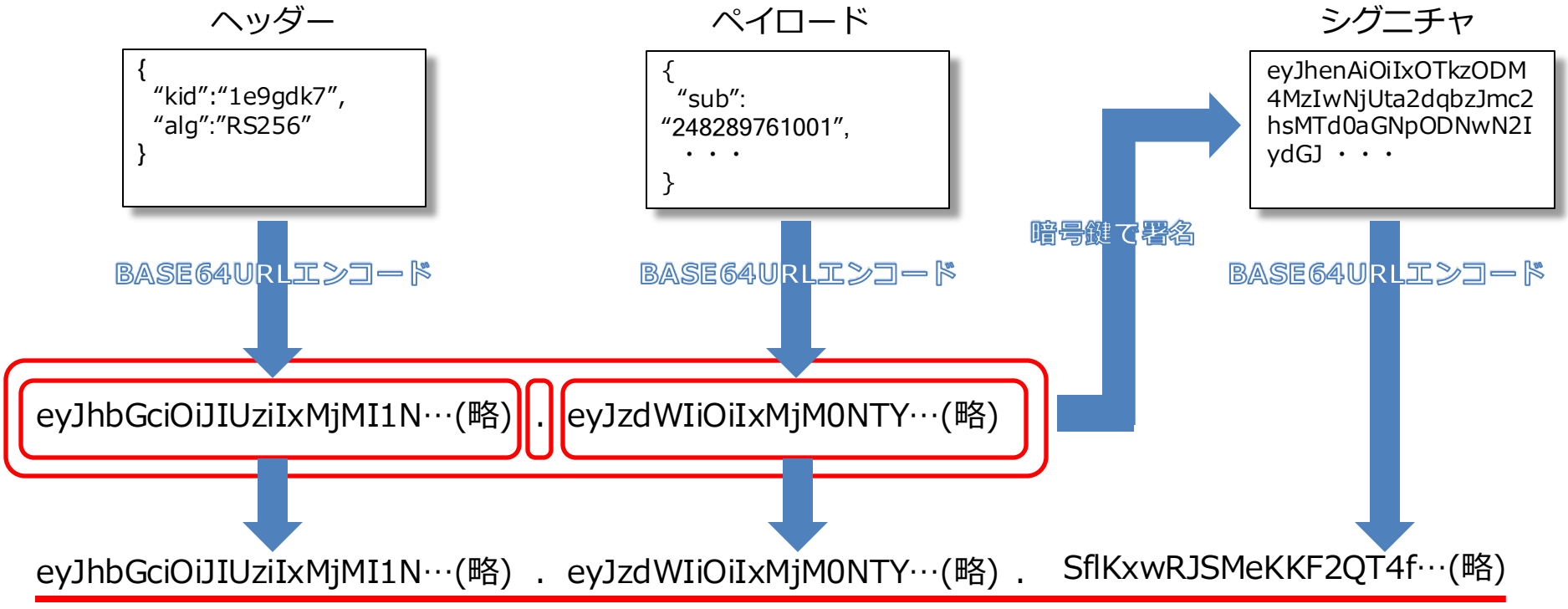
認可コードフロー



© SIOS Technology Inc. All rights Reserved.

OpenID Connectとは？

IDトークンを構成するJSON Web Token

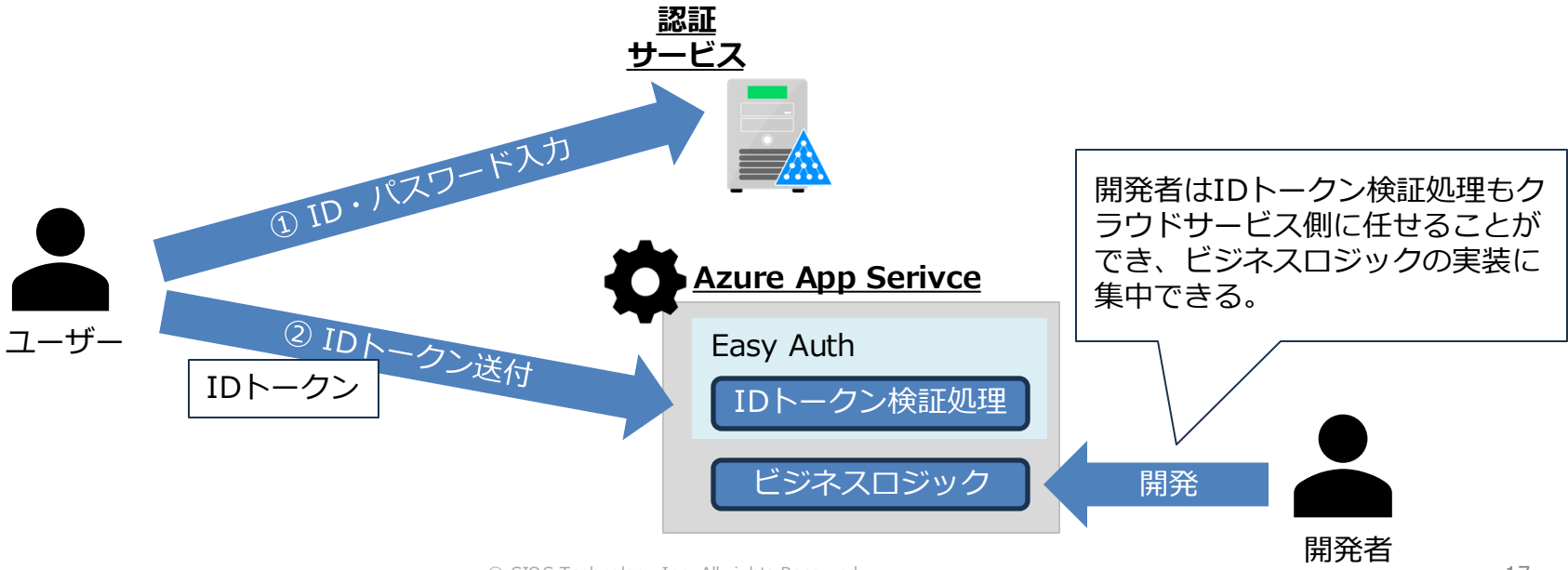


© SIOS Technology Inc. All rights Reserved.

OpenID Connectとは？

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。



© SIOS Technology Inc. All rights Reserved.

Shibboleth IdPにおける課題と解決策

© SIOS Technology Inc. All rights Reserved.

Shibboleth IdPにおける課題と解決策

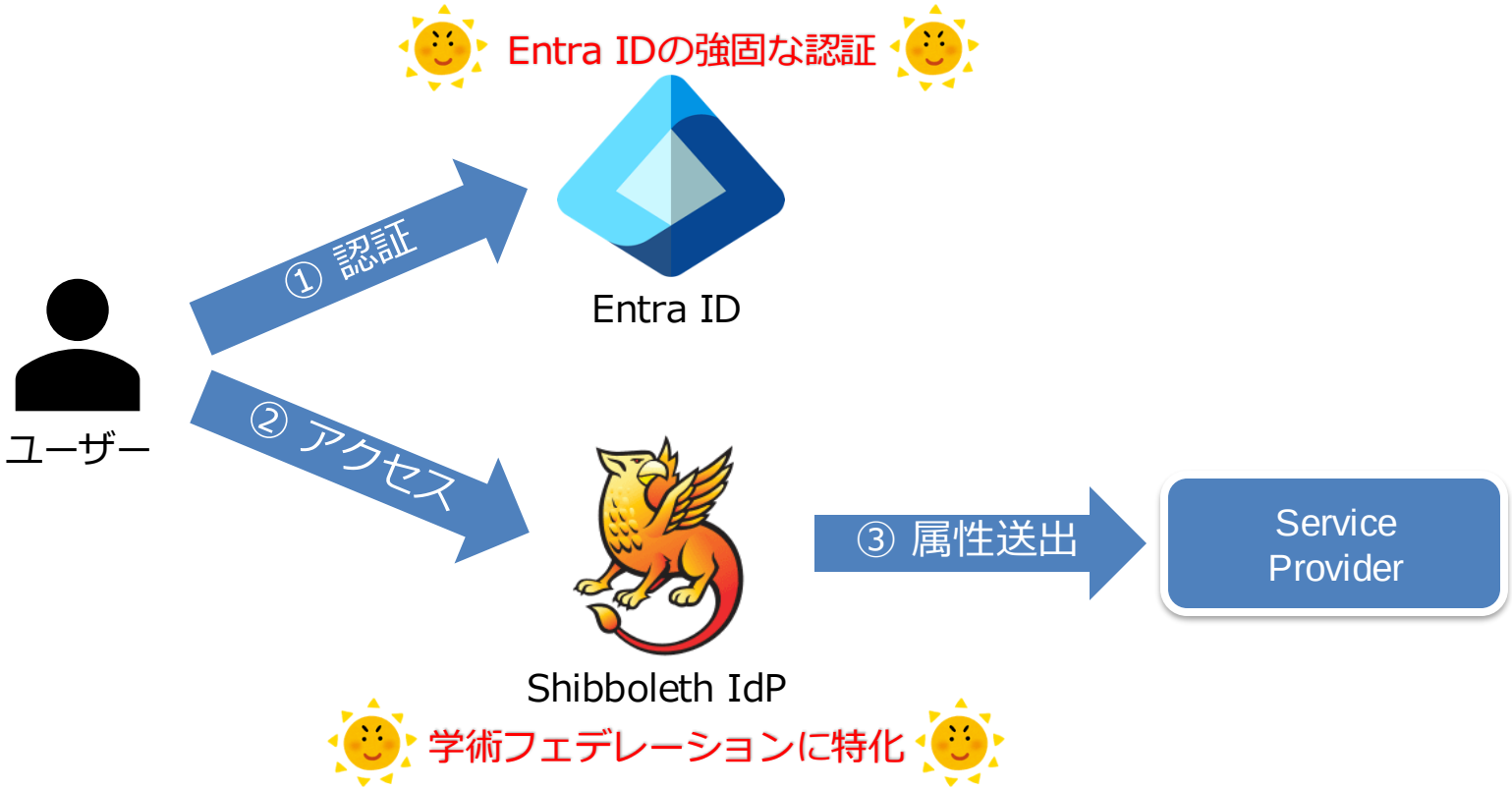
Shibboleth IdPとEntra IDにはそれぞれ、得意とする部分が異なる。

	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

© SIOS Technology Inc. All rights Reserved.

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！！



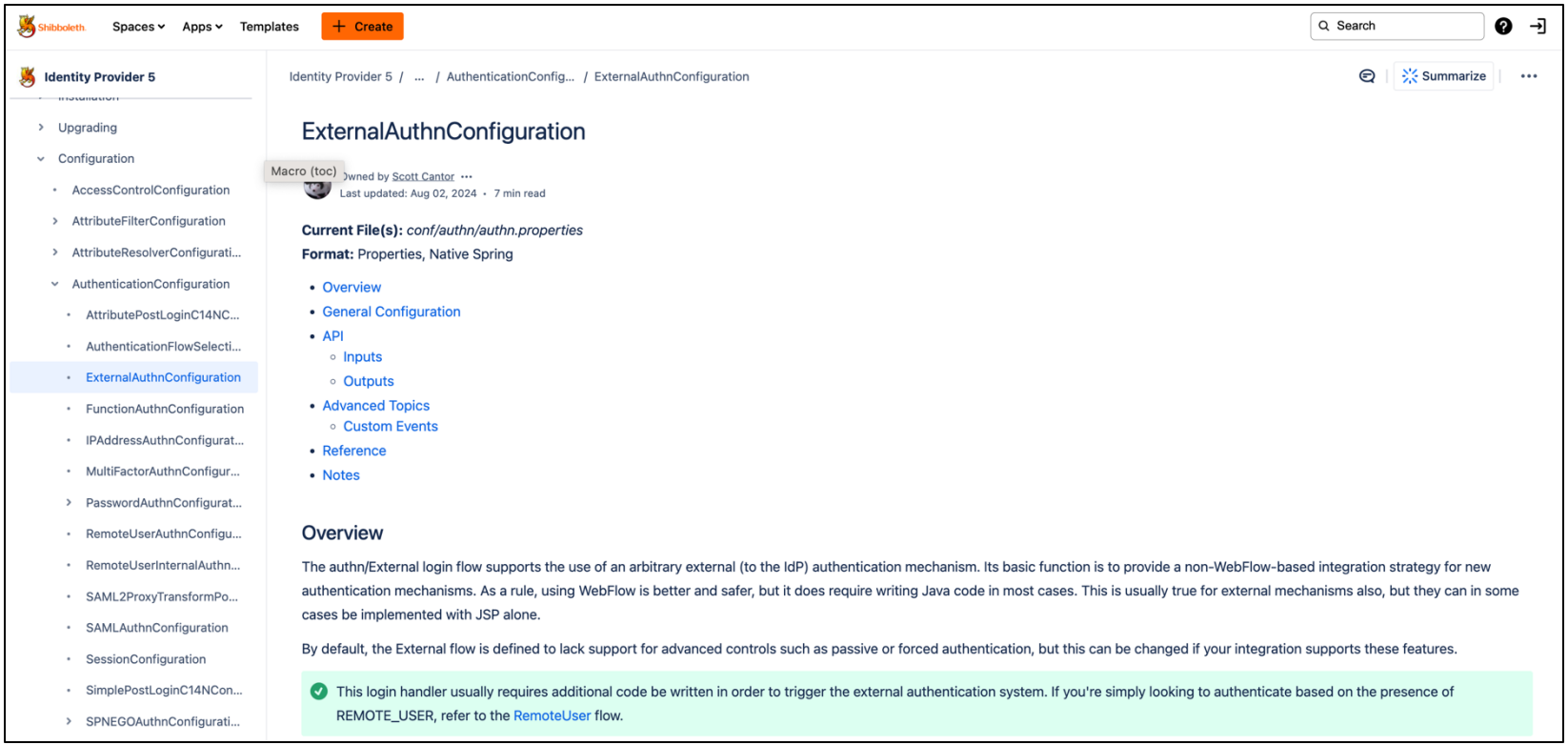
© SIOS Technology Inc. All rights Reserved.

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

© SIOS Technology Inc. All rights Reserved.

解決のためのコアテクノロジー

ExternalAuthnConfiguration



© SIOS Technology Inc. All rights Reserved.

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。

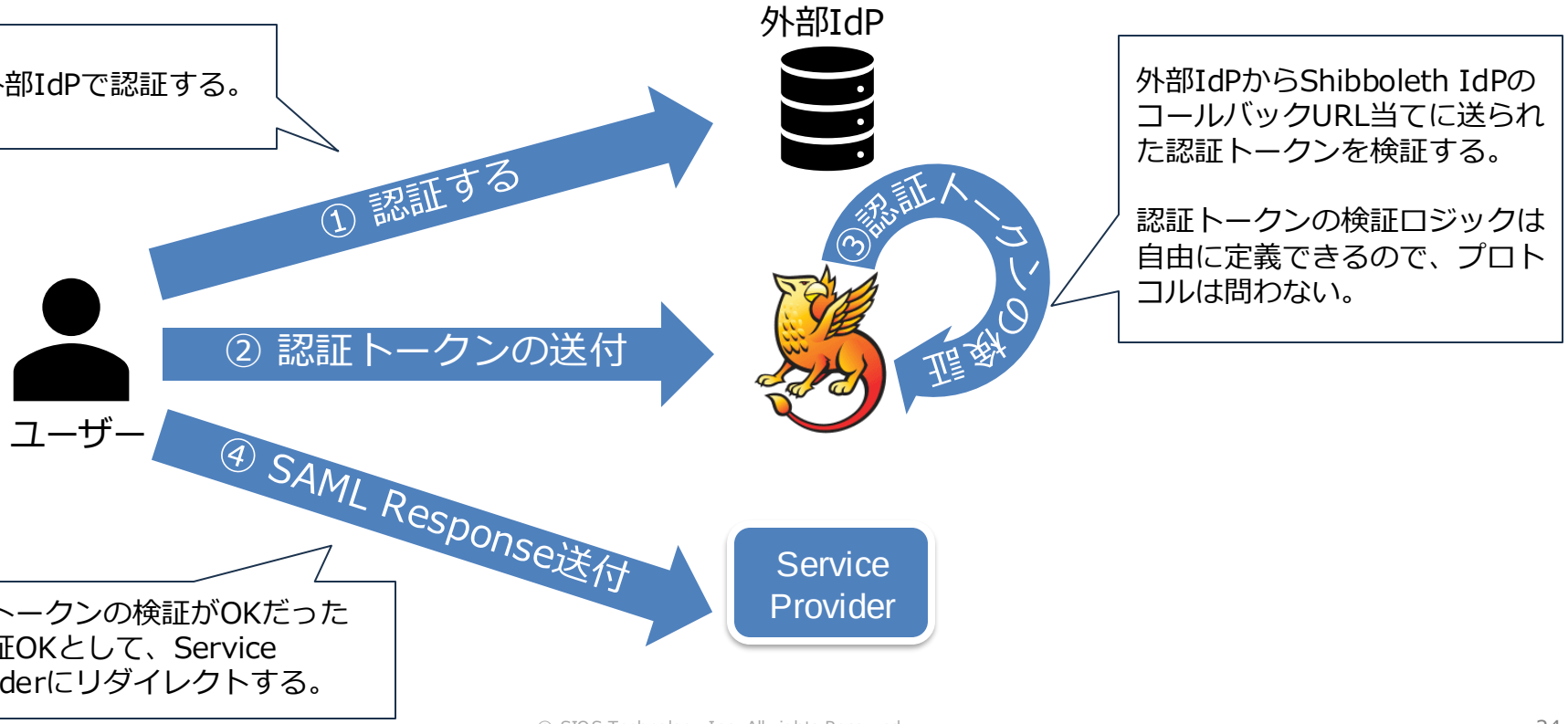
3 他の認証処理との組み合わせが可能

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。

© SIOS Technology Inc. All rights Reserved.

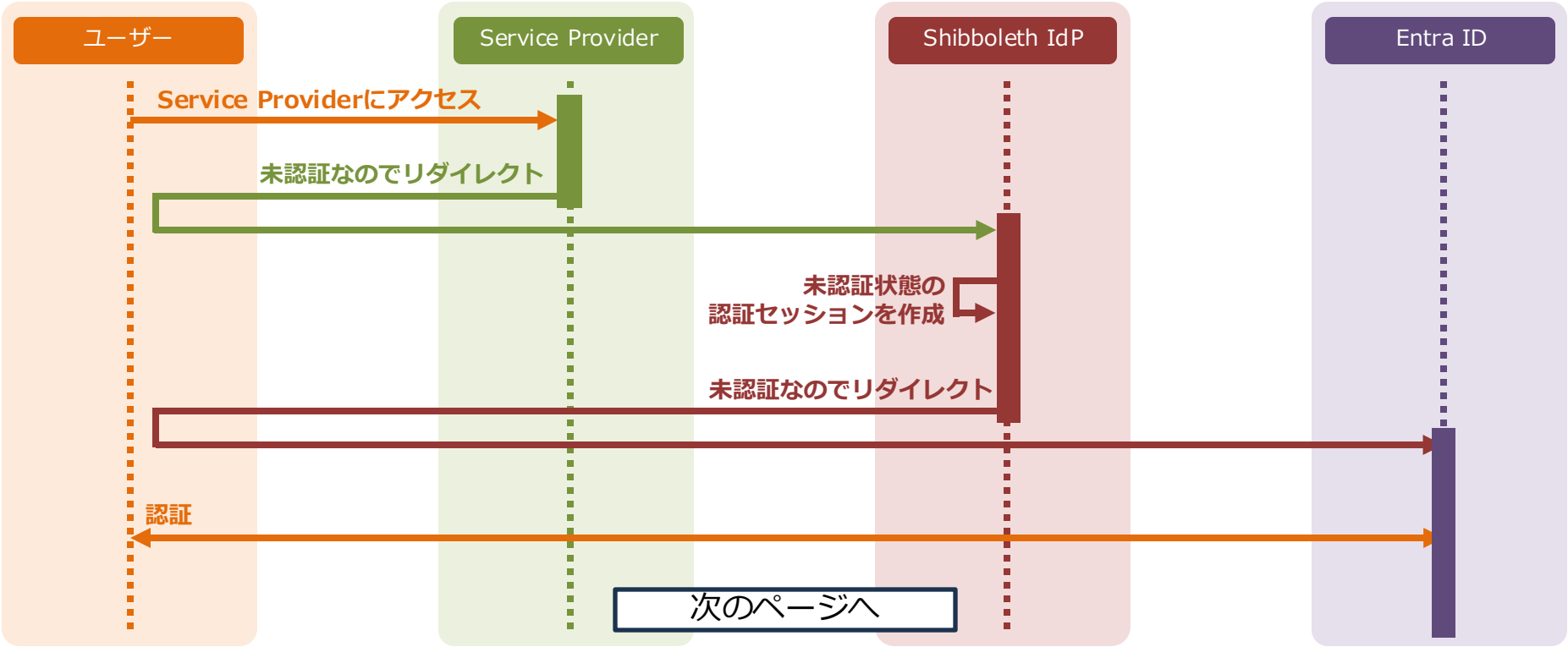
解決のためのコアテクノロジー

ExternalAuthnConfigurationの概要



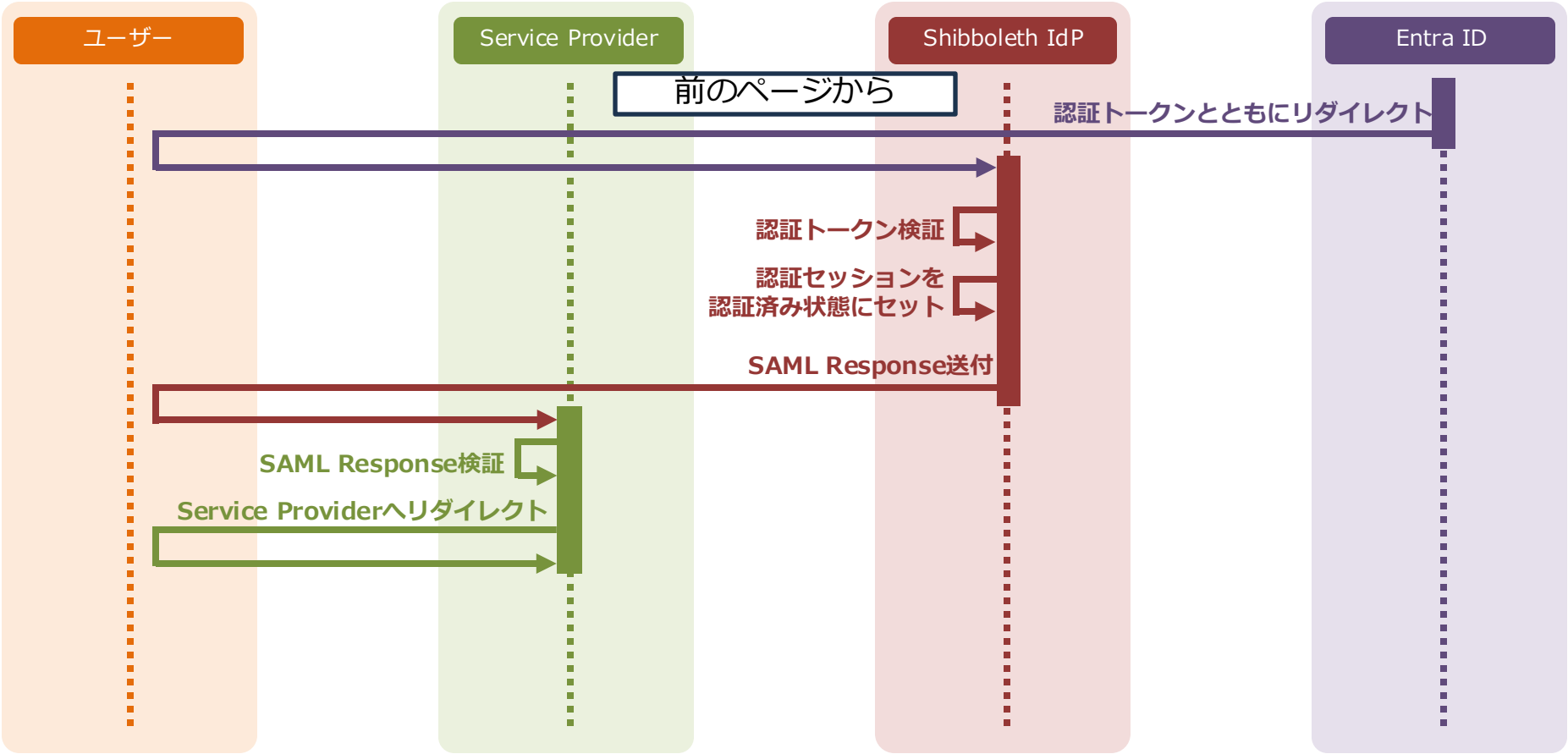
© SIOS Technology Inc. All rights Reserved.

ExternalAuthnConfigurationの認証フロー



© SIOS Technology Inc. All rights Reserved.

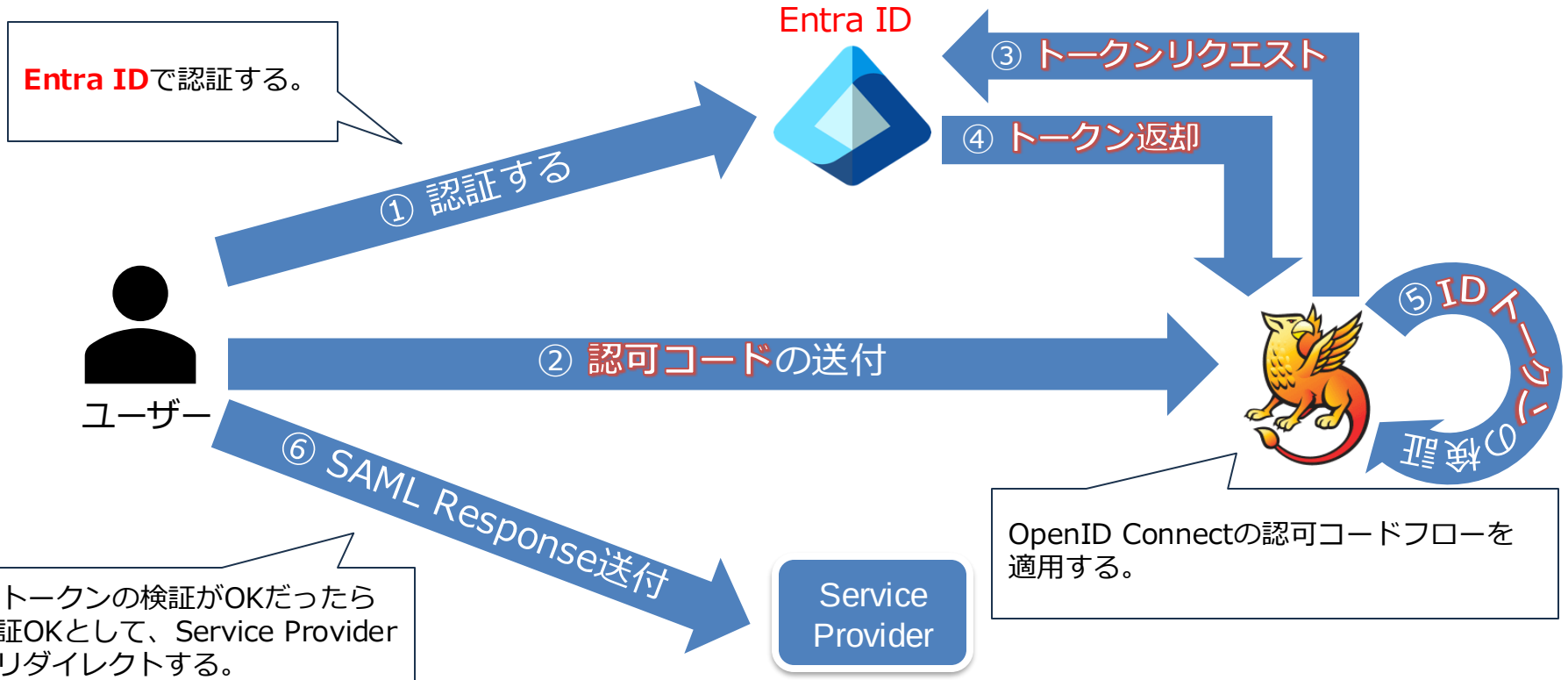
解決のためのコアテクノロジー



© SIOS Technology Inc. All rights Reserved.

解決のためのコアテクノロジー

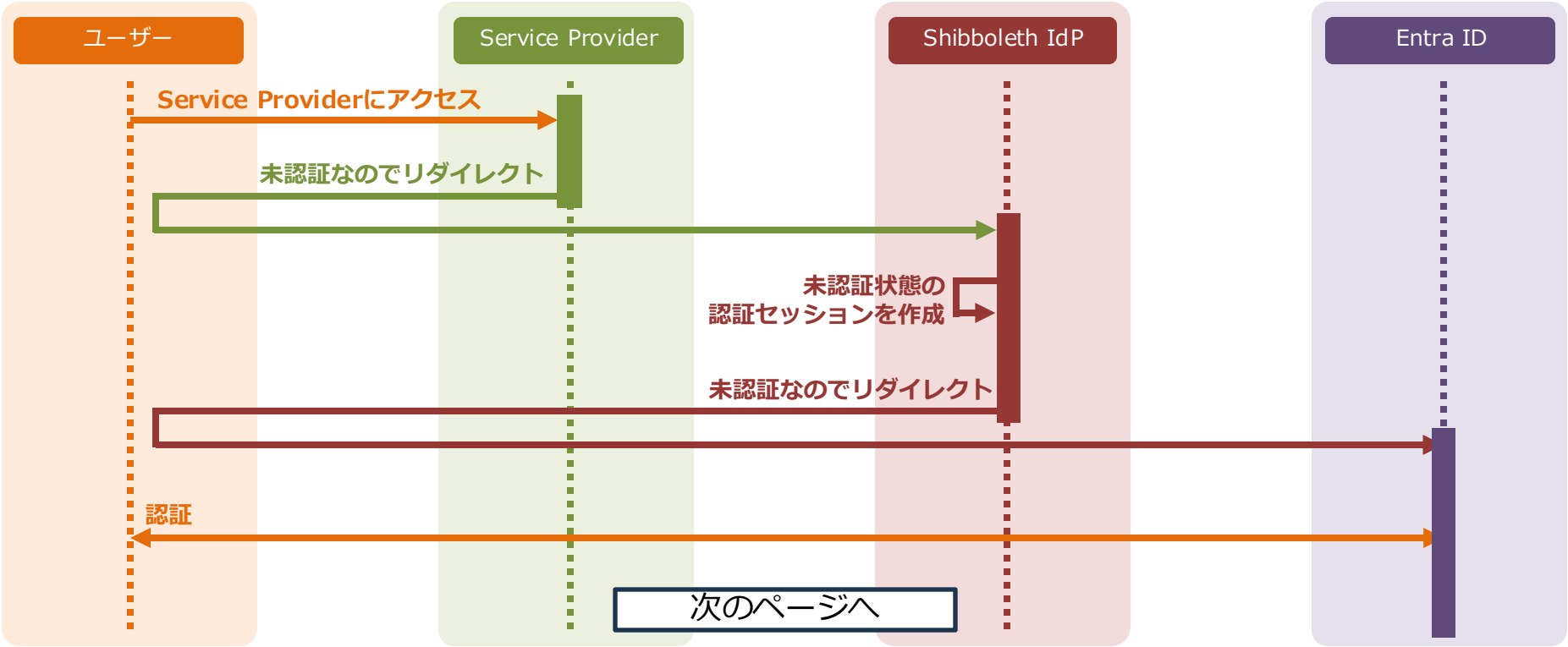
ExternalAuthnConfiguration + OpenID Connect



© SIOS Technology Inc. All rights Reserved.

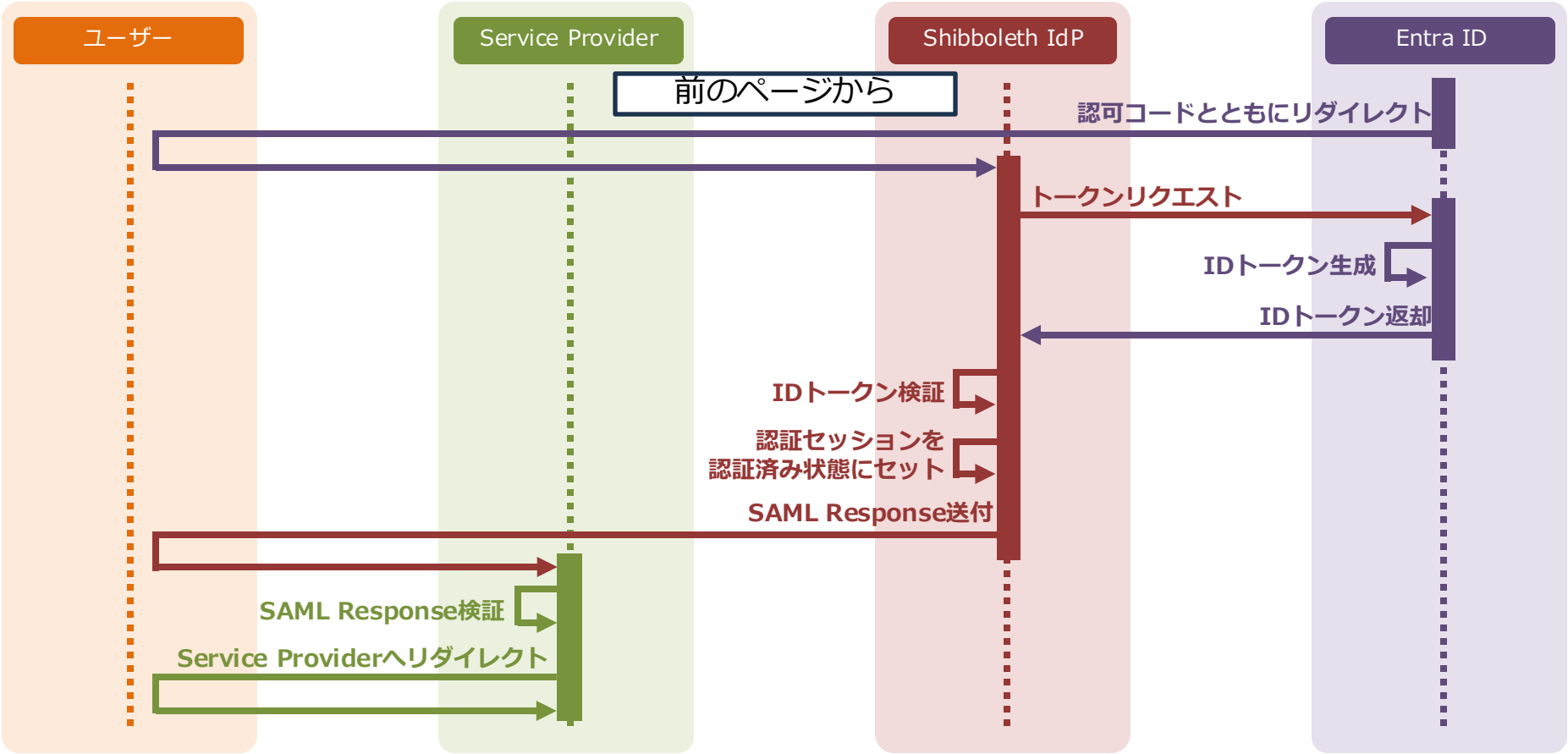
解決のためのコアテクノロジー

ExternalAuthnConfiguration + OpenID Connectの認証フロー



© SIOS Technology Inc. All rights Reserved.

解決のためのコアテクノロジー



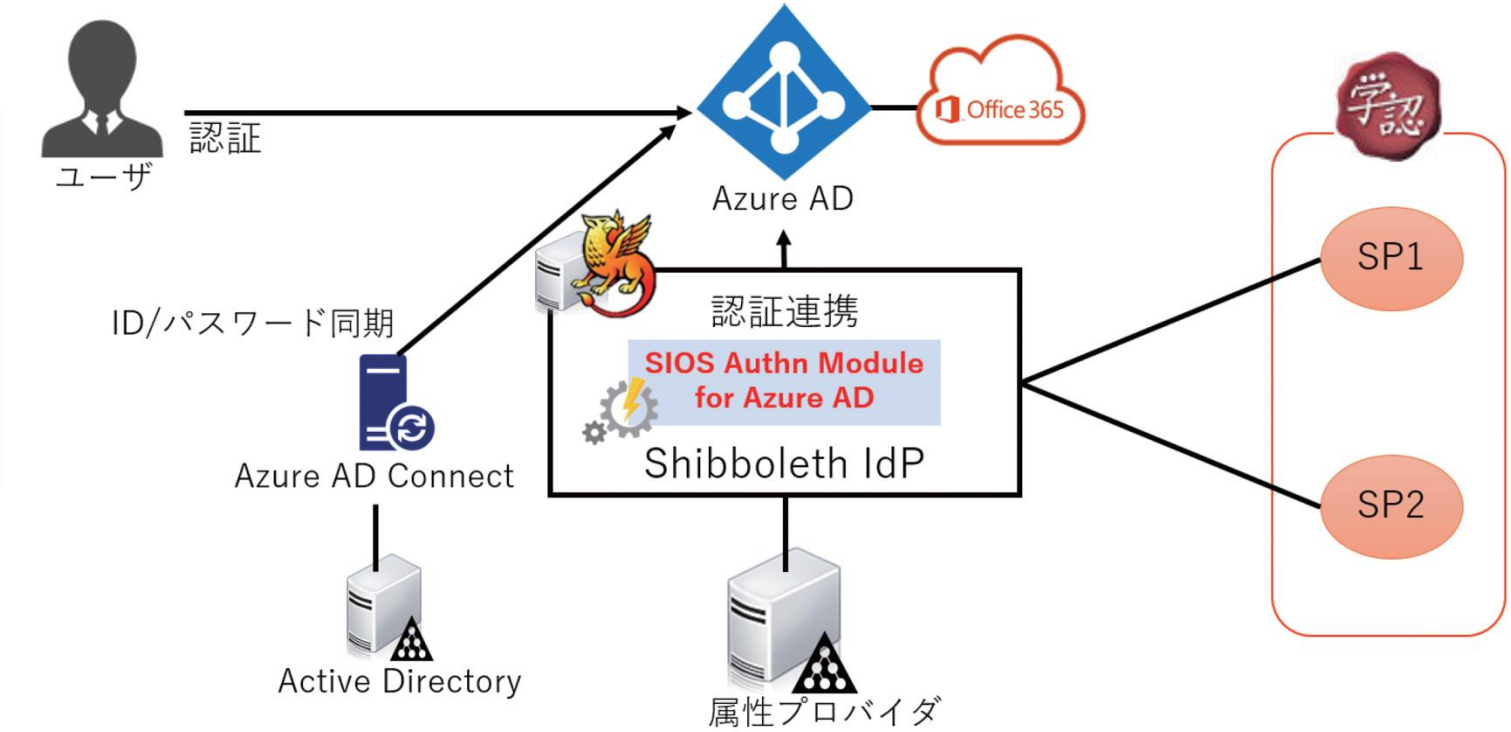
© SIOS Technology Inc. All rights Reserved.

SIOS Authn Module for Azure AD

© SIOS Technology Inc. All rights Reserved.

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。



© SIOS Technology Inc. All rights Reserved.

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. **ユーザープロファイル管理**
   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

© SIOS Technology Inc. All rights Reserved.


SIOS