社内のIdentityで AWSアカウントの管理を効率化

株式会社オージス総研

サービス事業本部 テミストラクトソリューション部

氏縄　武尊

自己紹介

氏縄 武尊 (Ujinawa Takeru)

Work

株式会社オージス総研
テミストラクトソリューション部　4年目
認証・認可・ID管理・PKI
OpenID Foundation Japan EIWGメンバー

Private

滋賀県彦根市 出身
Twitter: @uji52

Favorite

Spec: OpenID Connect, OAuth2.0, SCIM
AWS: IAM, CloudTrail, Lambda

私の仕事 ： ThemiStruct (テミストラクト)

ThemiStruct
テミストラクト

つくってます

ThemiStruct-WAM
テミストラクト

シングルサインオン
認証基盤

ThemiStruct-IDM
テミストラクト

ID管理

ThemiStruct-CM
テミストラクト

電子証明書発行・管理

IdentityPlatform AWS対応版

AWSのPaaS上で動く
アイデンティティ連携基盤

アジェンダ

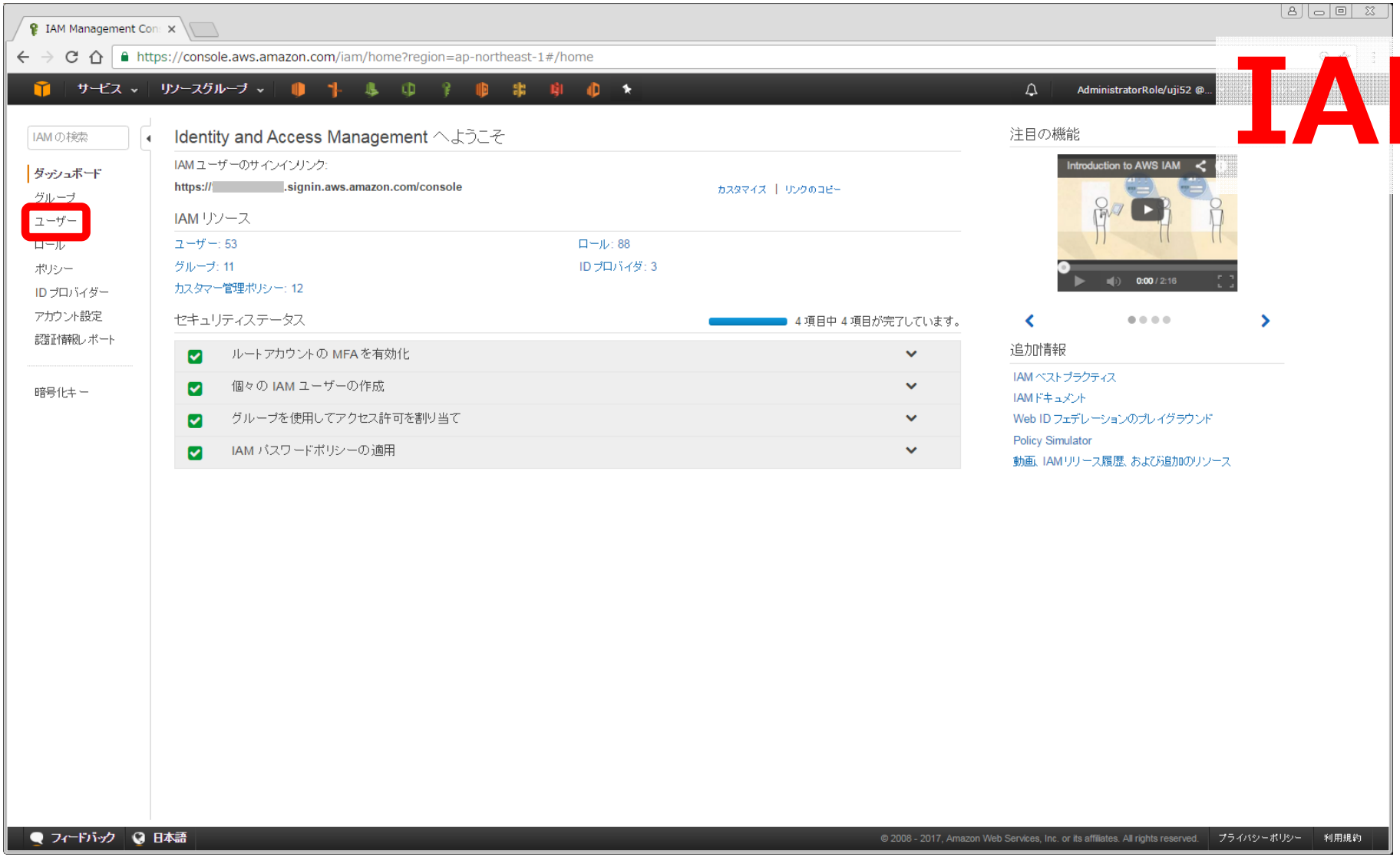
- AWSアカウント管理の苦労
- OpenAMとは
  - 認証連携方式
  - OpenAMをセットアップして使ってみる
- フェデレーションでアカウント管理効率UP
  - SAMLによるフェデレーション
  - OpenID Connectによるフェデレーション
- フェデレーション技術と今後ID管理について

AWSアカウント管理の苦労

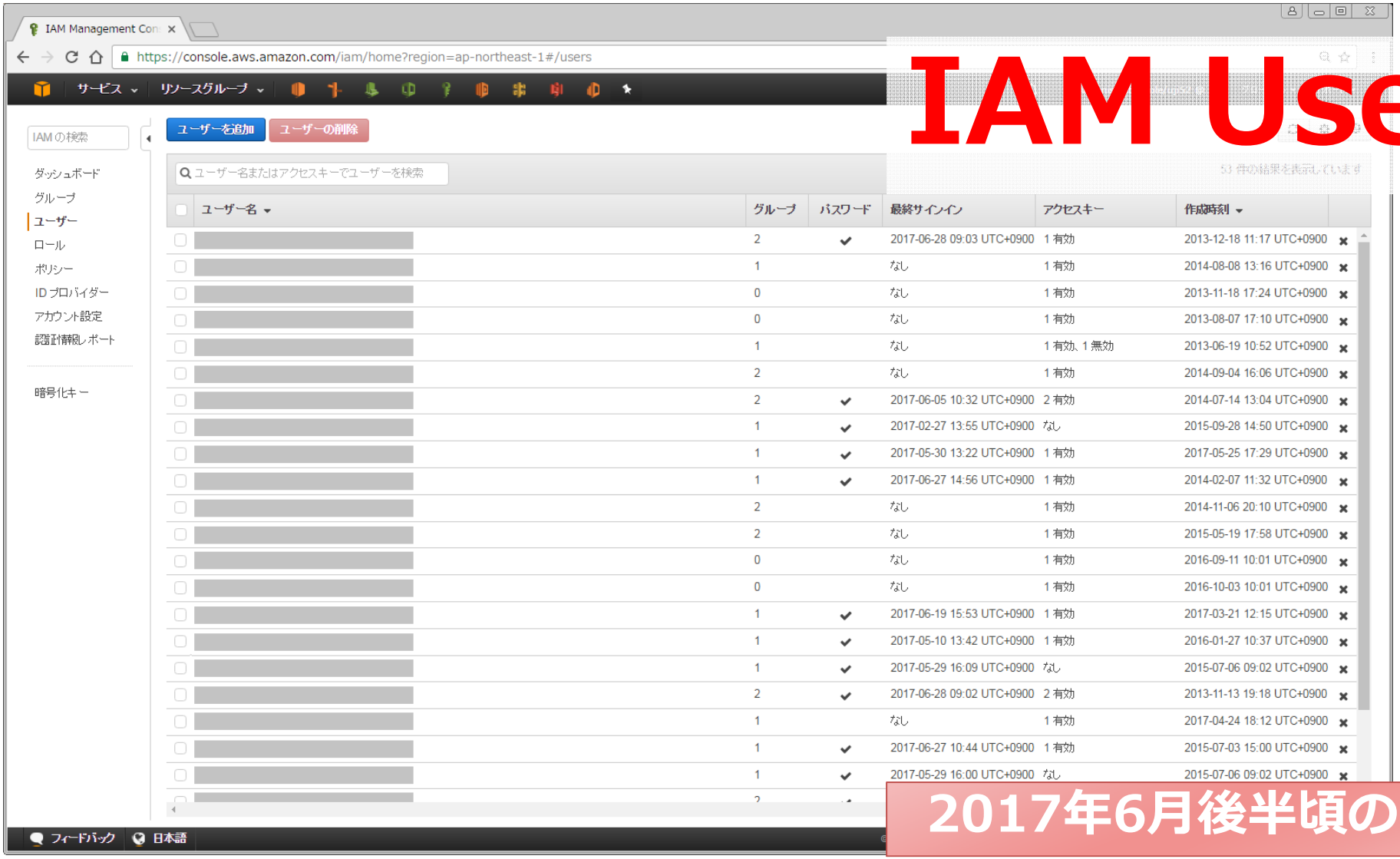
AWSアカウントの管理

ロアカウントの管理

- ユーザの追加・削除 (入社・退社)
- ユーザの属性変更 (異動)
- 所属グループの管理 (組織構成の変更)


IAM Management Con
https://console.aws.amazon.com/iam/home?region=ap-northeast-1#/home
サービス
リソースグループ
AdministratorRole/uji52 @...
IAM の検索
ダッシュボード
グループ
ユーザー
ロール
ポリシー
ID プロバイダー
アカウント設定
認証情報レポート
暗号化キー
Identity and Access Management へようこそ
IAM ユーザーのサインインリンク:
https://.signin.aws.amazon.com/console
カスタマイズ | リンクのコピー
IAM リソース
ユーザー: 53
ロール: 88
グループ: 11
ID プロバイダ: 3
カスタマー管理ポリシー: 12
セキュリティステータス
4 項目中 4 項目が完了しています。
ルートアカウントの MFA を有効化
個々の IAM ユーザーの作成
グループを使用してアクセス許可を割り当て
IAM パスワードポリシーの適用
注目の機能
Introduction to AWS IAM
0:00 / 2:16
追加情報
IAM ベストプラクティス
IAM ドキュメント
Web ID フェデレーションのプレイグラウンド
Policy Simulator
動画、IAM リリース履歴、および追加のリソース
フィードバック
日本語
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
プライバシーポリシー
利用規約

IAM



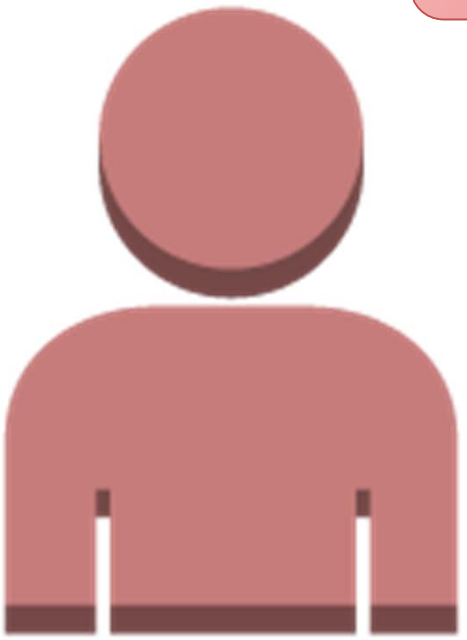
IAM User

2017年6月後半頃の画面

月初

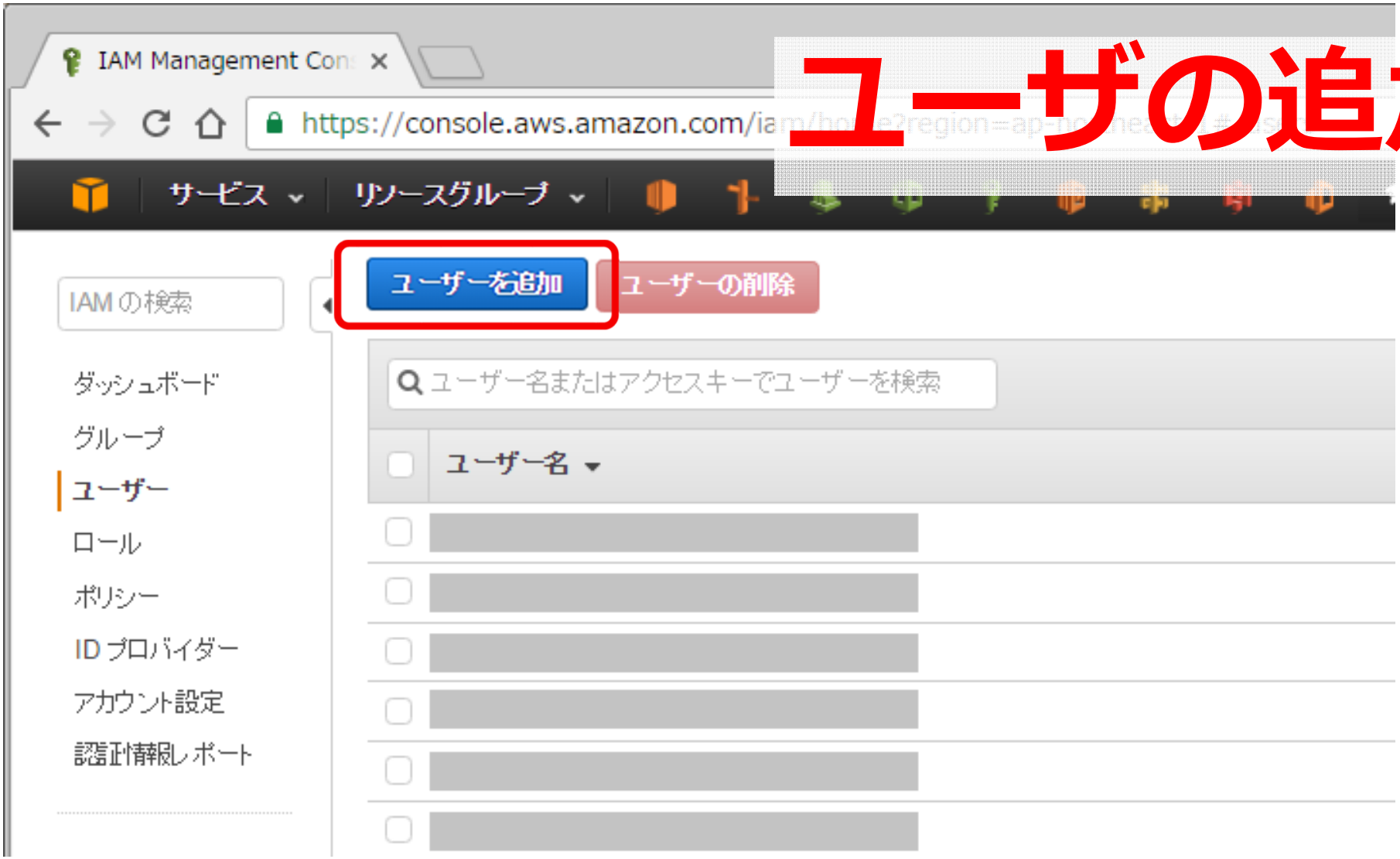
素早く対応しなきゃ
利用者に不便って言われる！

管理者



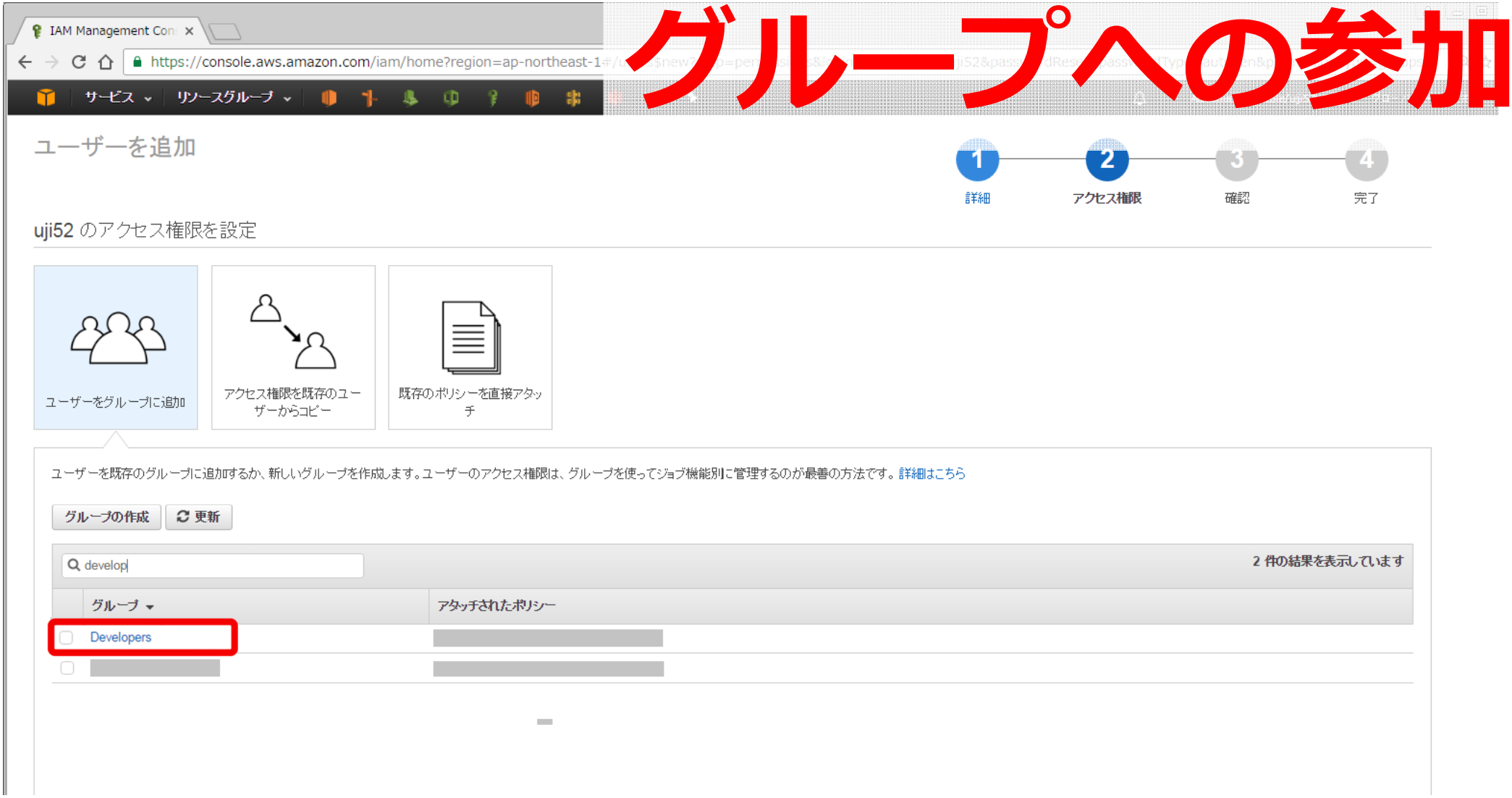
新メンバー加入

ユーザの追加

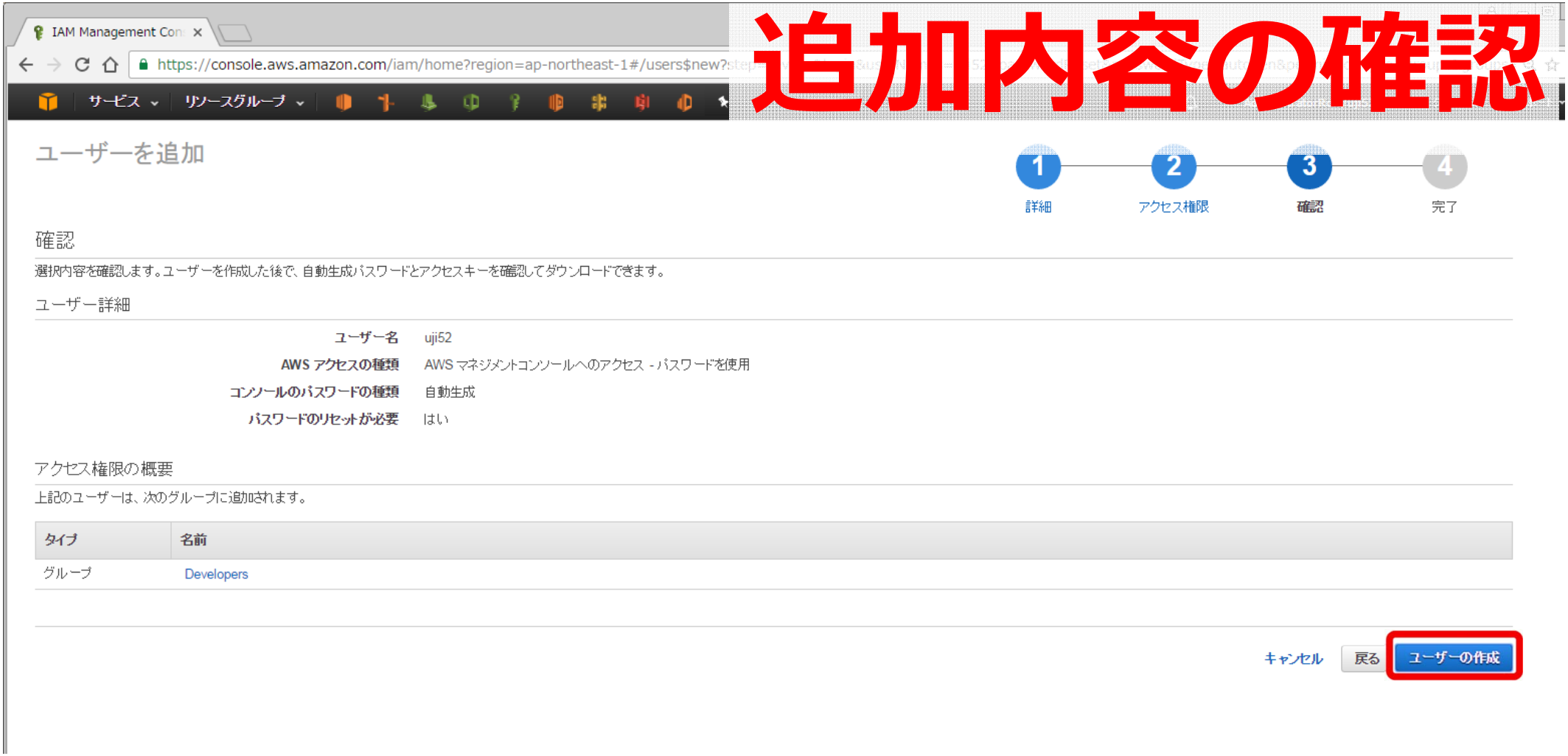


ユーザの追加

グループへの参加



追加内容の確認



OTPの設定

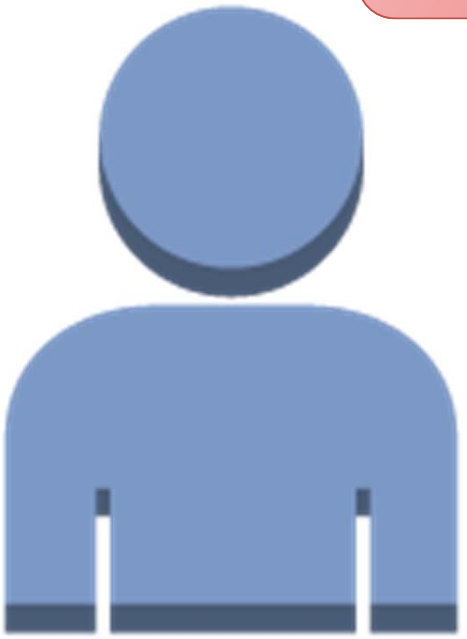
OTPの設定


ユーザーの ARN
パス
作成時刻
グループ (1)
認証情報
MFA デバイスの管理
仮想 MFA アプリケーションが QR コードのスキャンをサポートしている場合は、スマートフォンのカメラで次の画像をスキャンします。
手動設定のシークレットキーを表示
アプリケーションを設定したら、下のボックスに 2 つの連続する認証コードを入力し、[仮想 MFA の有効化] をクリックします。
認証コード 1
認証コード 2
キャンセル
戻る
仮想 MFA の有効化

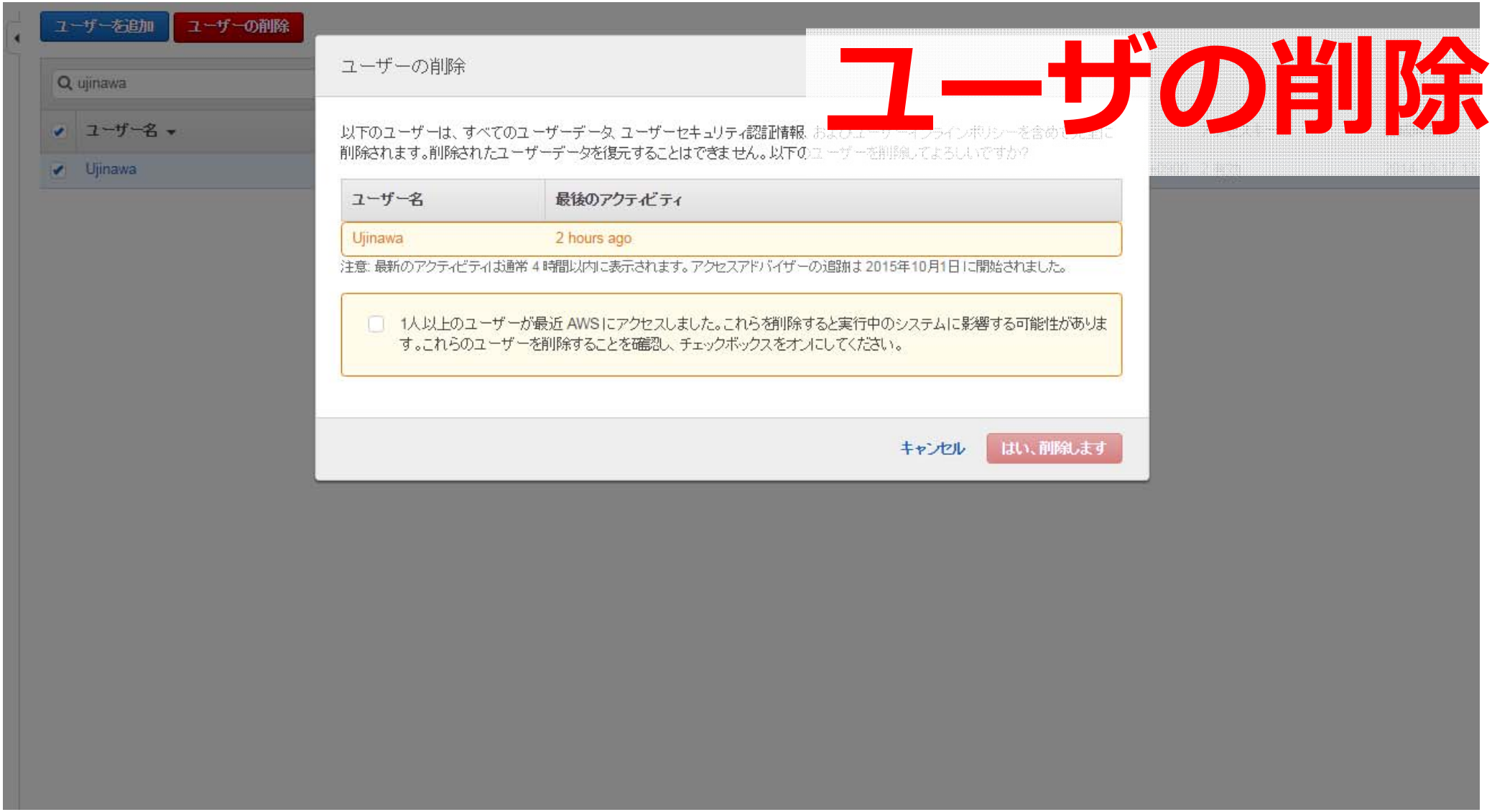
月末

素早く対応しなきゃ
辞めたのに入られてしまう！！
危ない！！

管理者



メンバー離脱



ユーザの削除

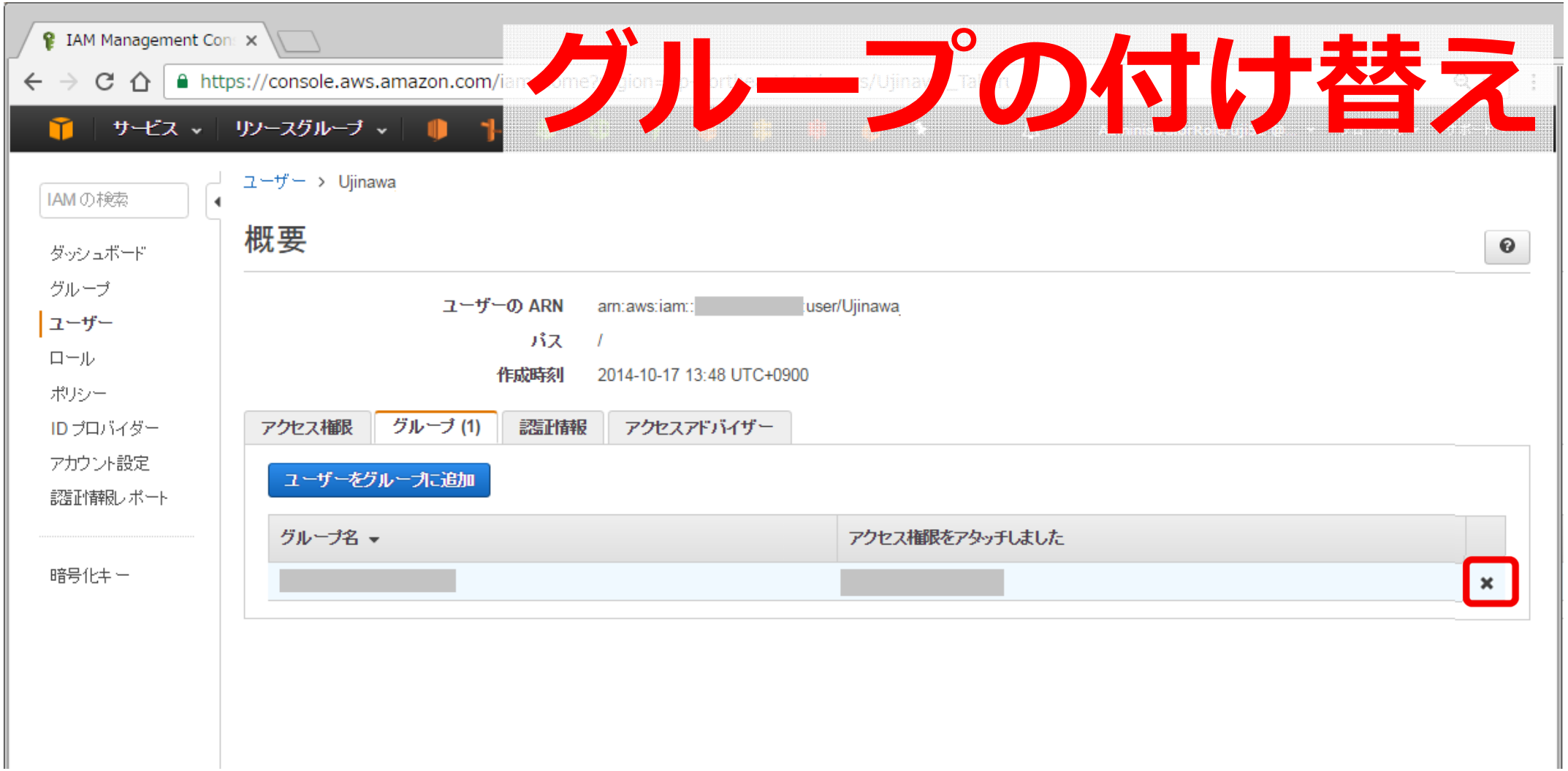
月末

早く対応しないと
不便だって言われる上に
権限が残ってて危ない！！

管理者

メンバー異動

グループの付け替え



月末月初の忙しい時期に
こんな処理ばっかり・・・
(作業漏れも許されない緊張感・・・)

アカウント管理上の課題

ユーザの不満 (不便！)

- 追加が遅れると不便だ
- MFA有効化が面倒だ
- そもそも認証するのが面倒だ

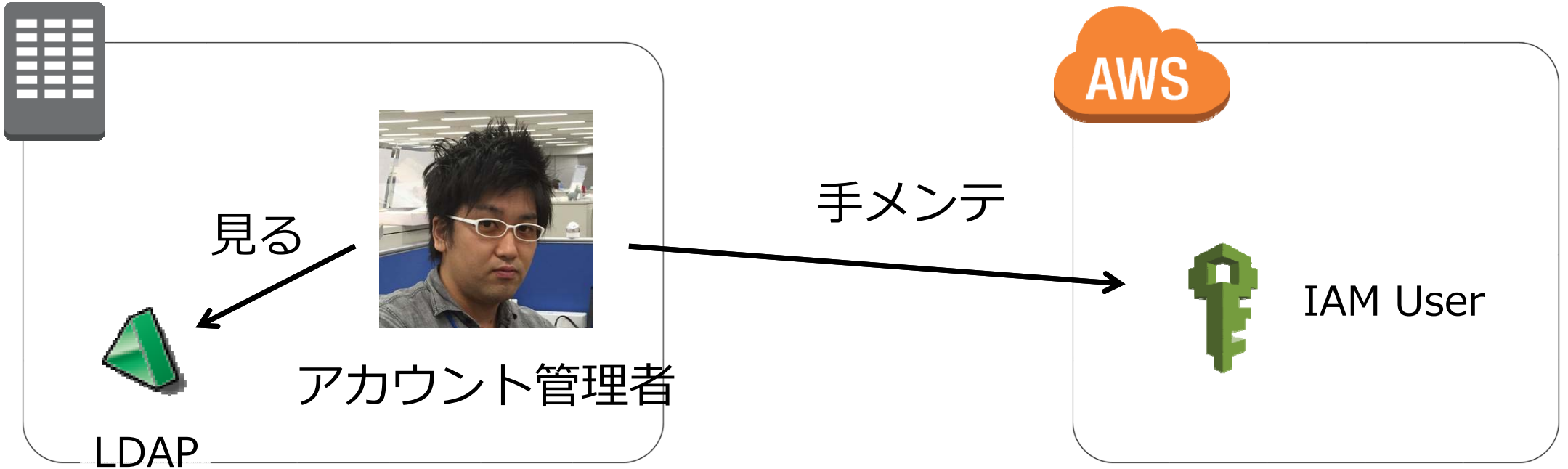
管理者の不満 (面倒！リスク！)

- 手作業が多い
- MFAを強制できない
- 作業を忘れたら企業に打撃を与える可能性がある

アカウント管理上の課題の元になっていること

◘社内に存在するユーザ情報のコピー

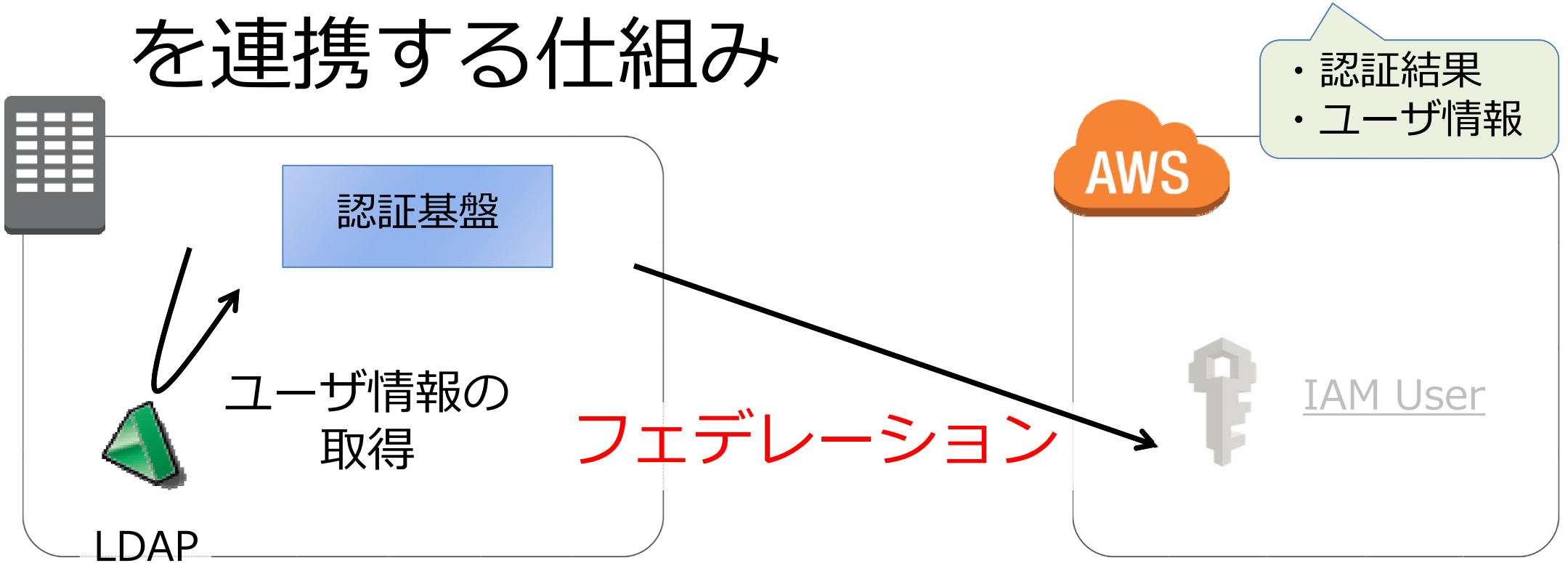
- ➢手作業でIAMユーザを追加



この問題
フェデレーションで
解決できる！！

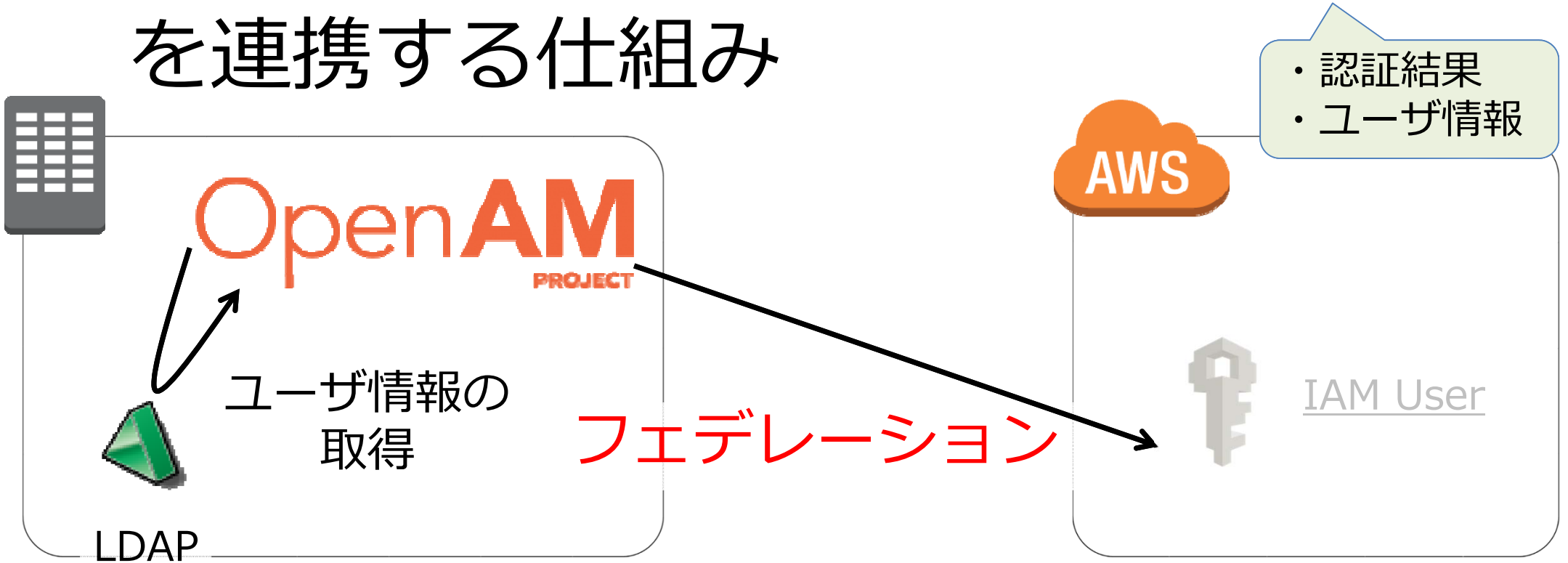
フェデレーション(ID連携)

□異なるシステム間で、安全にID情報を連携する仕組み



フェデレーション(ID連携)

- 異なるシステム間で、安全にID情報を連携する仕組み



アジェンダ

- AWSアカウント管理の苦労
- OpenAMとは
  - ID連携方式
  - OpenAMをセットアップして使ってみる
- フェデレーションでアカウント管理効率UP
  - SAMLによるフェデレーション
  - OpenID Connectによるフェデレーション
- フェデレーション技術と今後ID管理について

OpenAMとは(ざっくり)

◘ForgeRock社が開発元のOSS

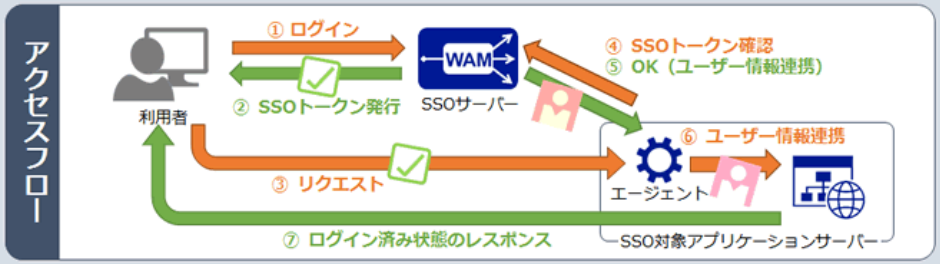
ID連携方式

- エージェント方式
- リバースプロキシ方式
- 代理認証方式
- フェデレーション方式

従来のID連携方式

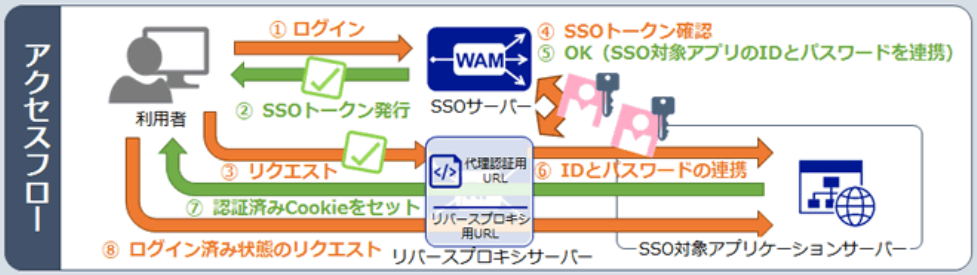
エージェント方式SSO

- Webサーバー、もしくはアプリケーションサーバーに「エージェント」ソフトウェアを導入することでSSOが実現可能です。
- インストール時はウィザードに従い、データを入力すれば、即座にSSOが可能です。



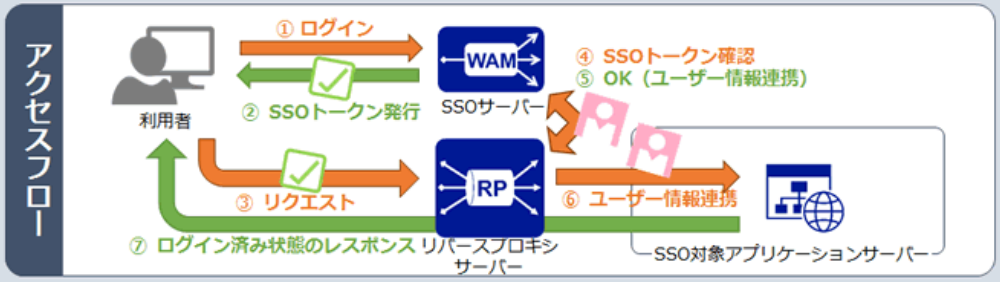
代理認証方式SSO

- 前述の「エージェント」ソフトウェアが連携するユーザー情報を取得できないアプリの場合、クライアントに代わって、リバースプロキシサーバーがIDとパスワードを送信することで、SSOが実現できます。
- 事前に、ID管理製品等を用いて、IDとパスワードを連携しておく必要があります。



リバースプロキシ方式SSO

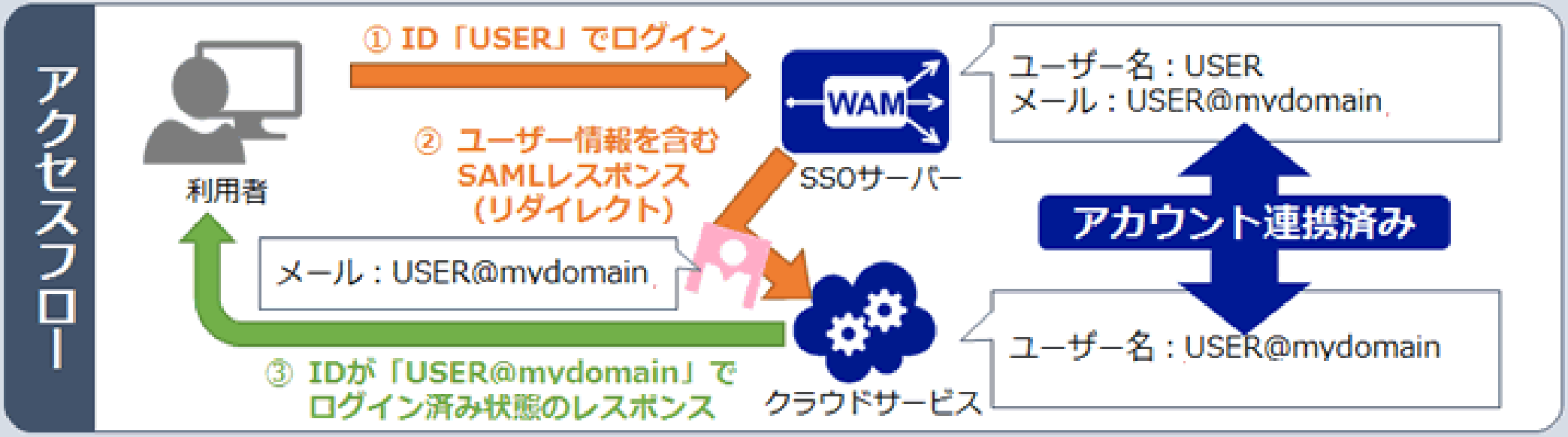
- 前述の「エージェント」ソフトウェアがインストールされた「リバースプロキシ」サーバーを経由することでシングルサインオンが可能となります。
- エージェントプログラムの導入が困難なシステムの場合でも、SSOが実現可能です。



http://www.ogis-ri.co.jp/pickup/themistruct/note/note_sso01.html

フェデレーション方式SSO

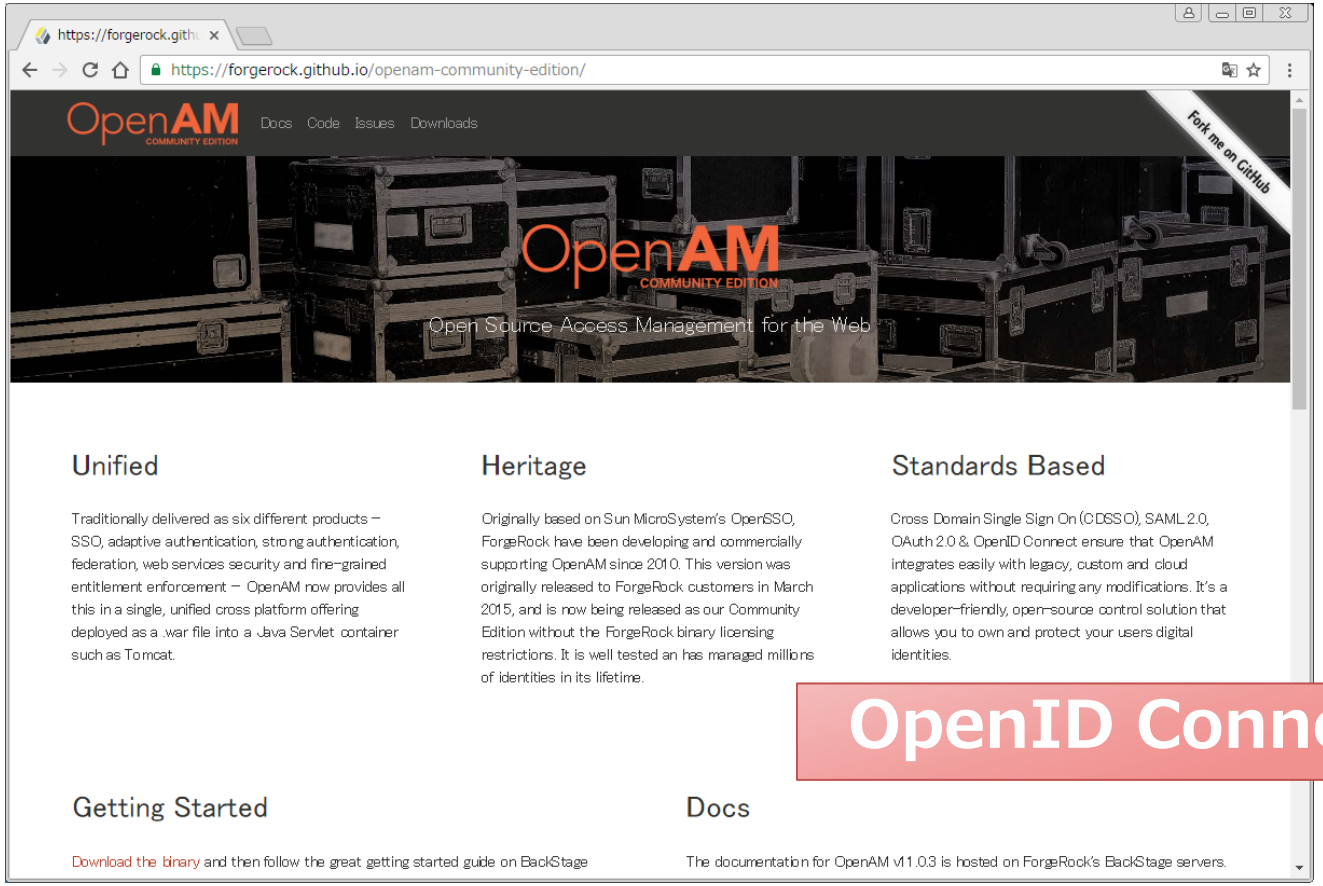
- Google AppsやSalesforce、Office 365をはじめとするクラウドサービスはSAMLやOpenID Connectなどの認証プロトコルに対応しています。
- SSOサーバー、および、クラウドサービスの設定のみで、SSOが実現可能です。



http://www.ogis-ri.co.jp/pickup/themistruct/note/note_sso01.html

OpenAMを
セットアップしてみよう

Community Edition

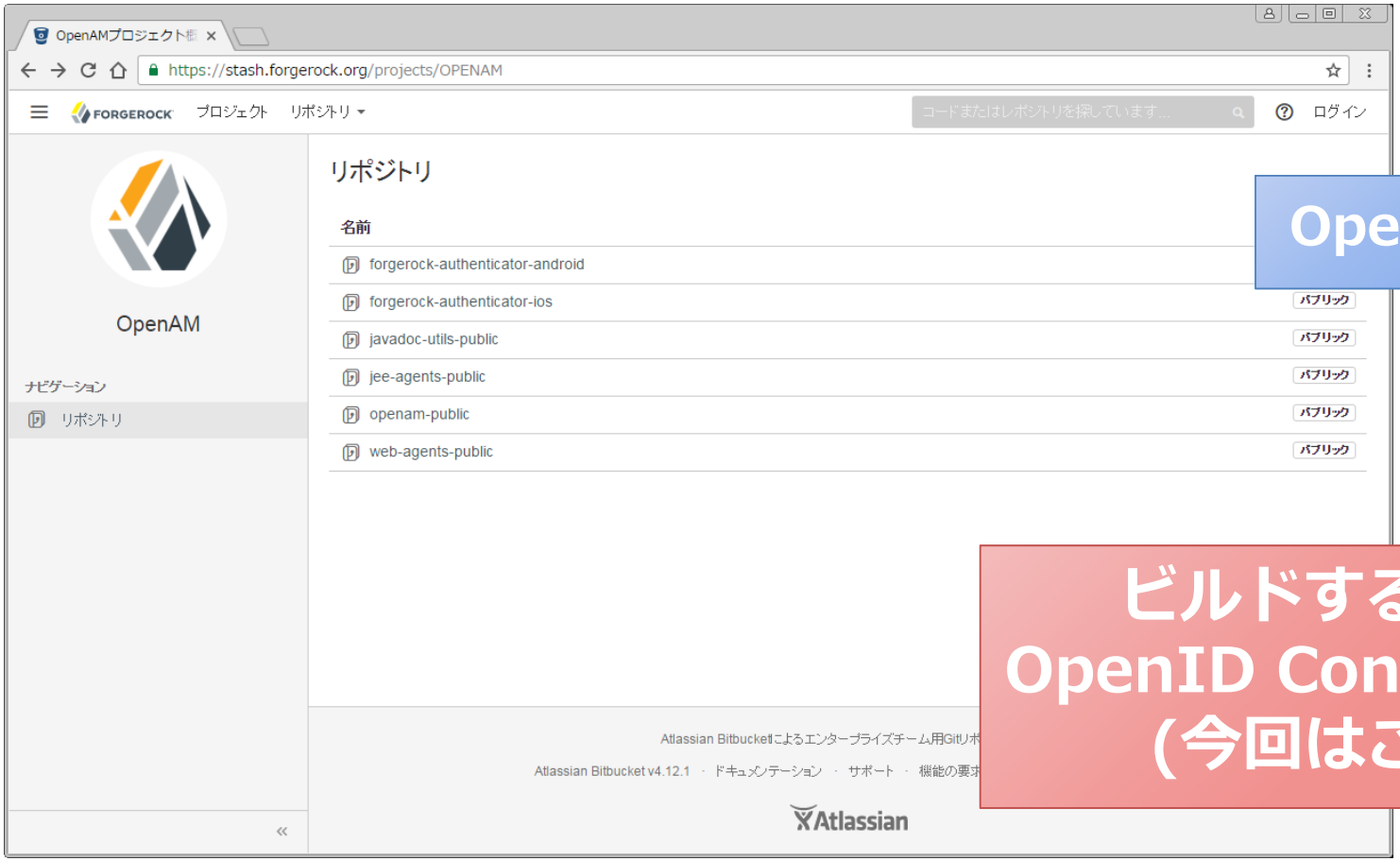


OpenAM 11.0.0

OpenID Connectの機能にやや不足アリ

https://forgerock.github.io/openam-community-edition/

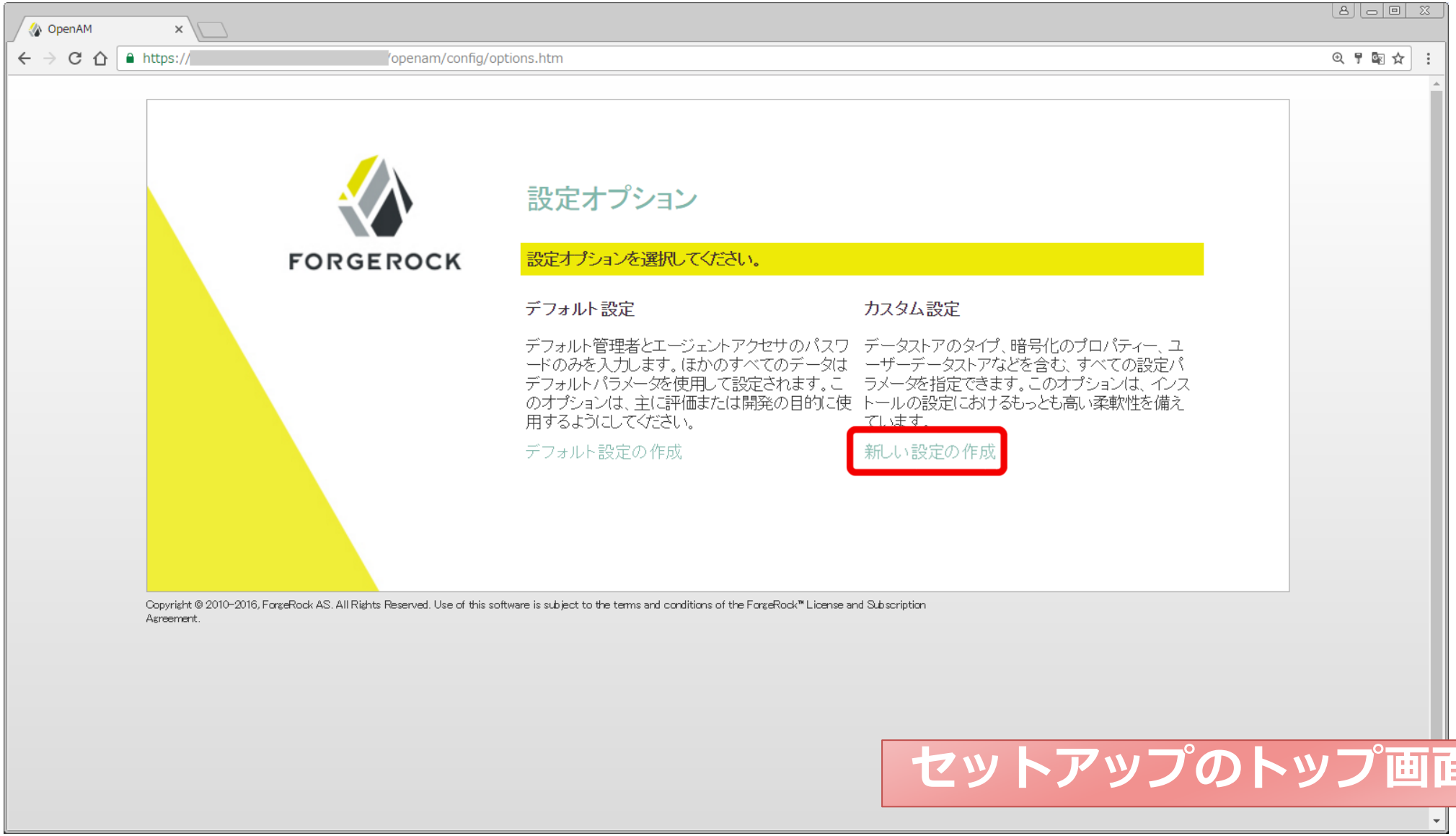
OpenAM パブリックリポジトリ



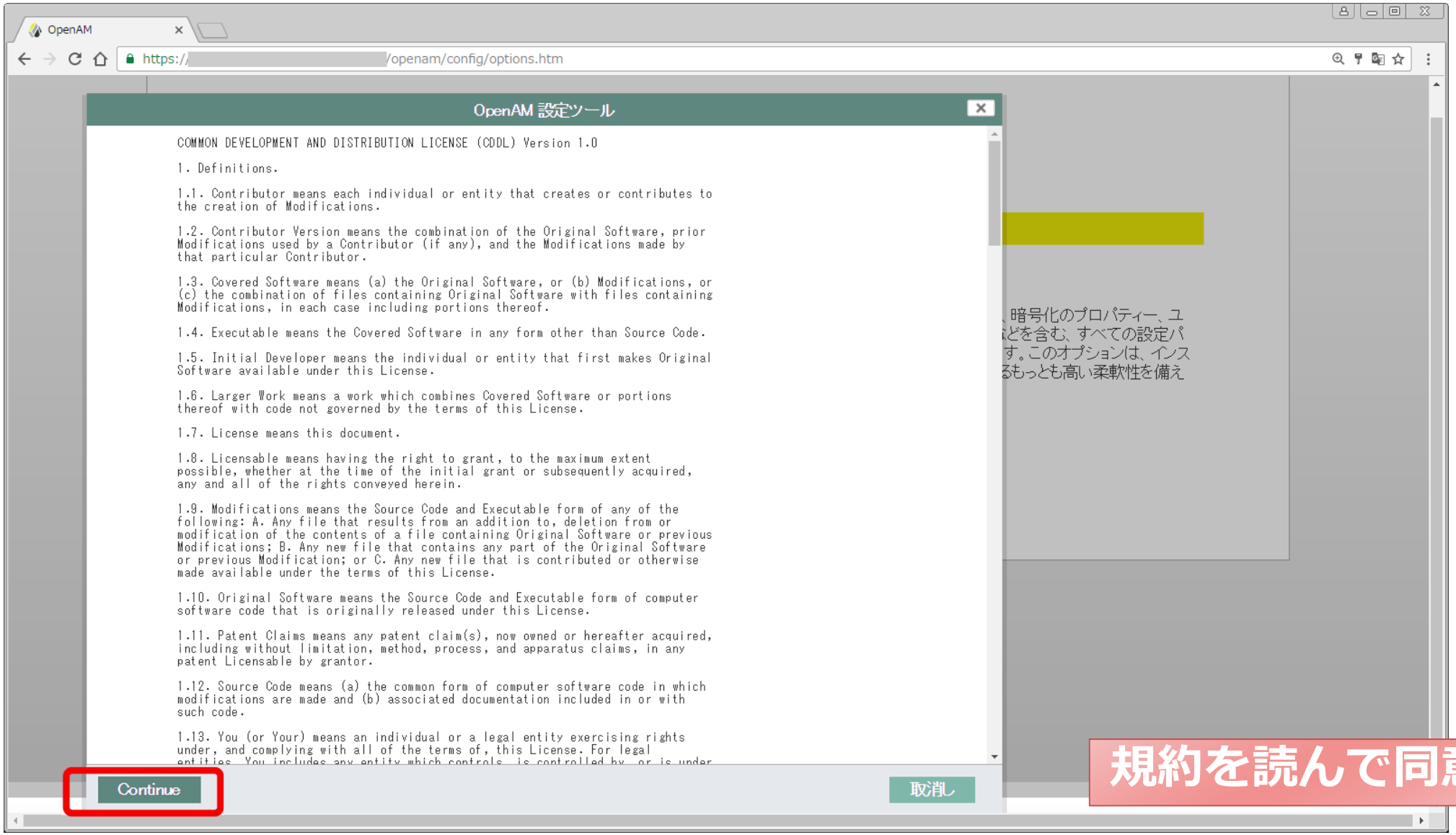
OpenAM 13.0.0

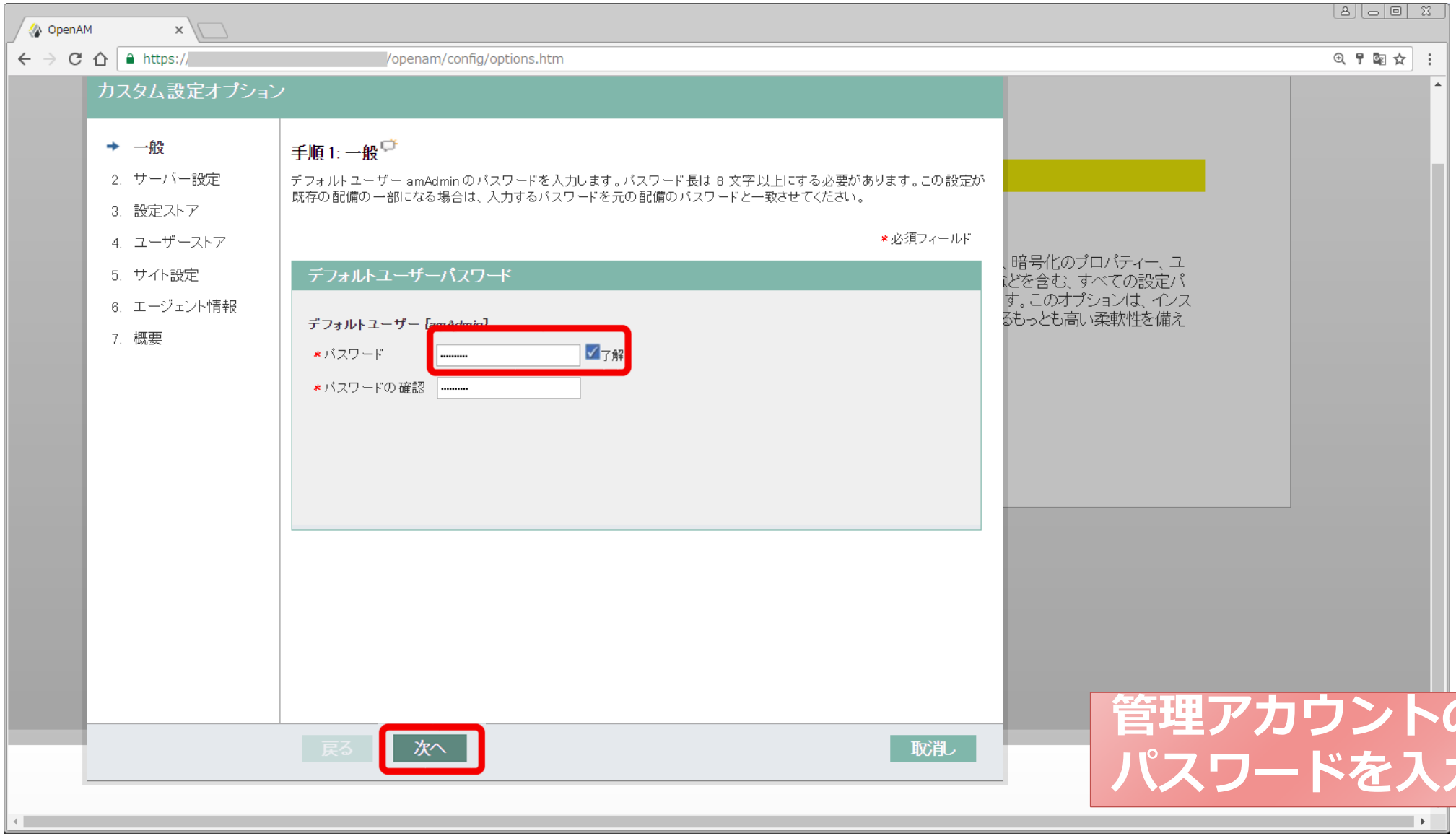
ビルドする必要があるが
OpenID Connectの機能は充実
(今回はこちらを採用)

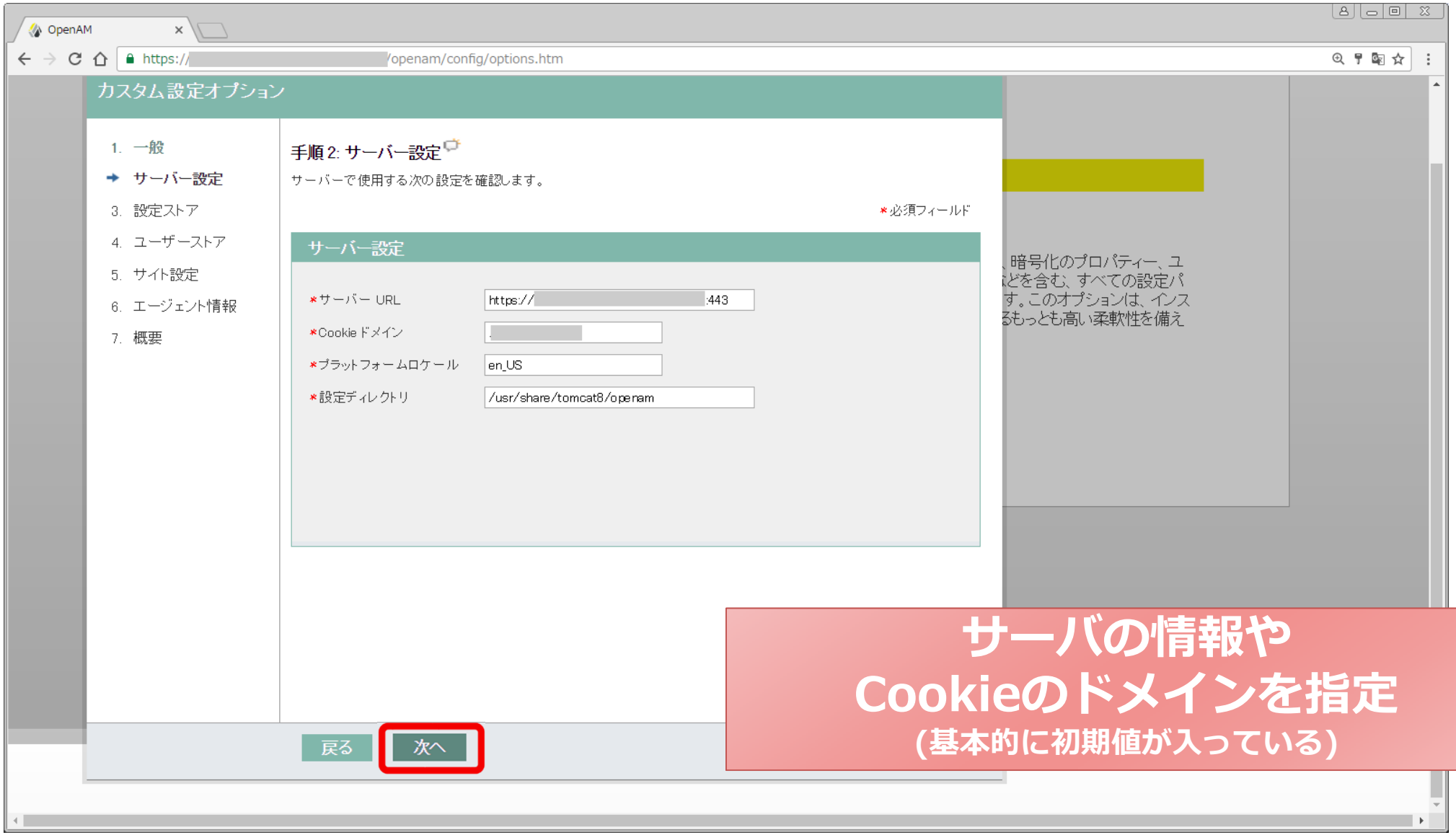
https://stash.forgerock.org/projects/OPENAM

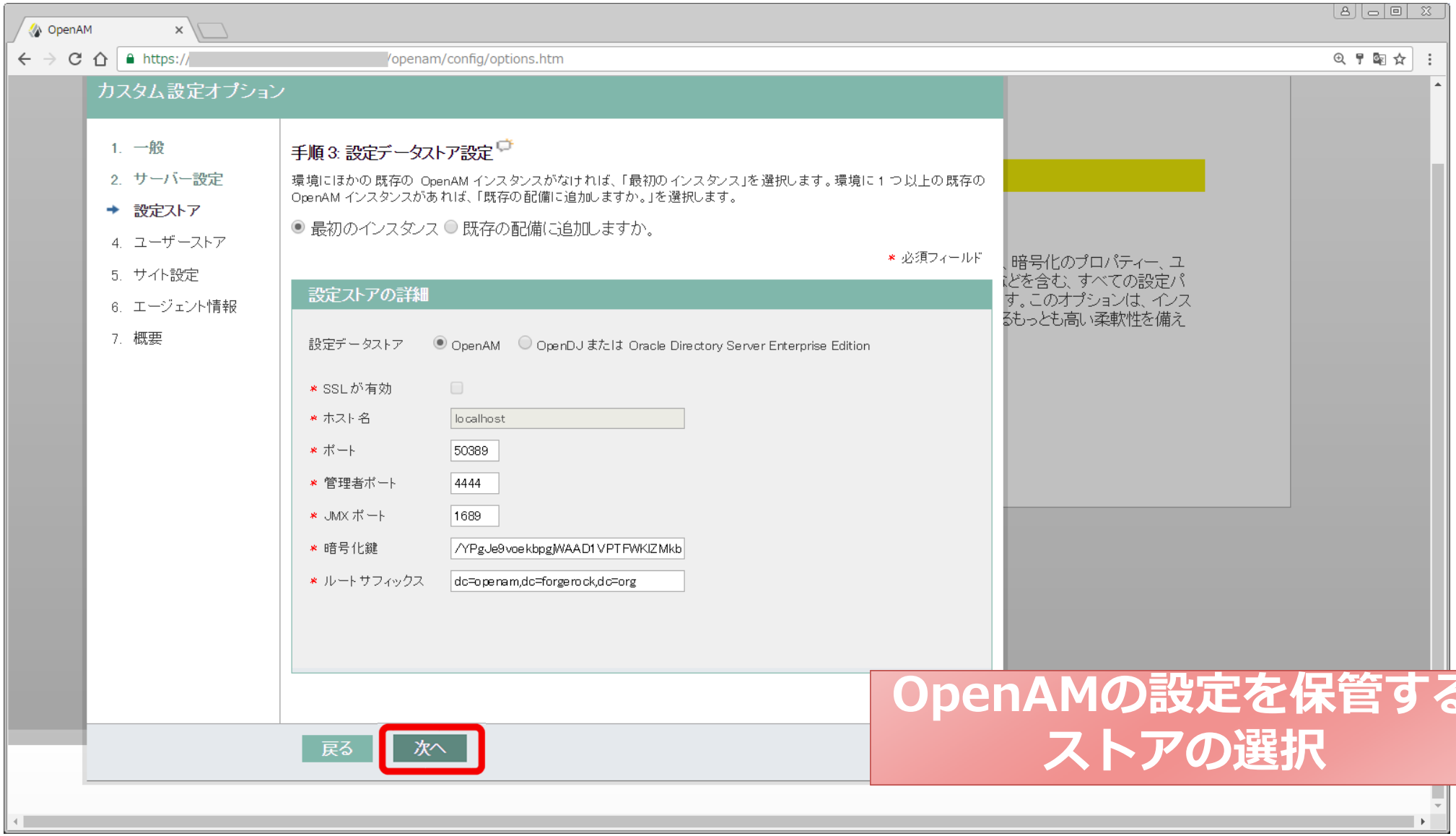


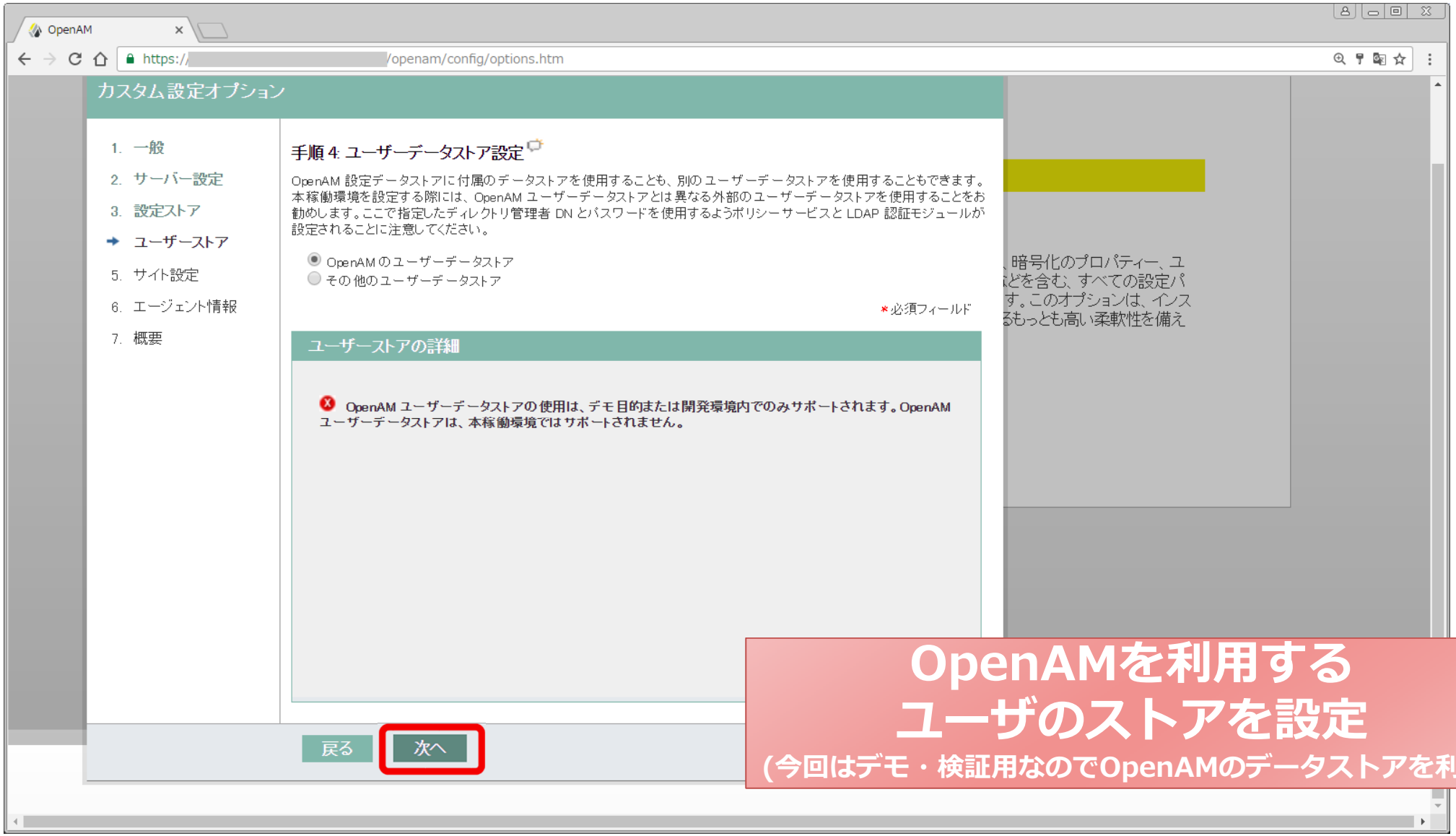
セットアップのトップ画面


OpenAM
https://
/openam/config/options.htm
OpenAM 設定ツール
COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0
1. Definitions.
1.1. Contributor means each individual or entity that creates or contributes to the creation of Modifications.
1.2. Contributor Version means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.
1.3. Covered Software means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.
1.4. Executable means the Covered Software in any form other than Source Code.
1.5. Initial Developer means the individual or entity that first makes Original Software available under this License.
1.6. Larger Work means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.
1.7. License means this document.
1.8. Licensable means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.
1.9. Modifications means the Source Code and Executable form of any of the following: A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications; B. Any new file that contains any part of the Original Software or previous Modification; or C. Any new file that is contributed or otherwise made available under the terms of this License.
1.10. Original Software means the Source Code and Executable form of computer software code that is originally released under this License.
1.11. Patent Claims means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.
1.12. Source Code means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.
1.13. You (or Your) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal
Continue
取消し
規約を読んで同意

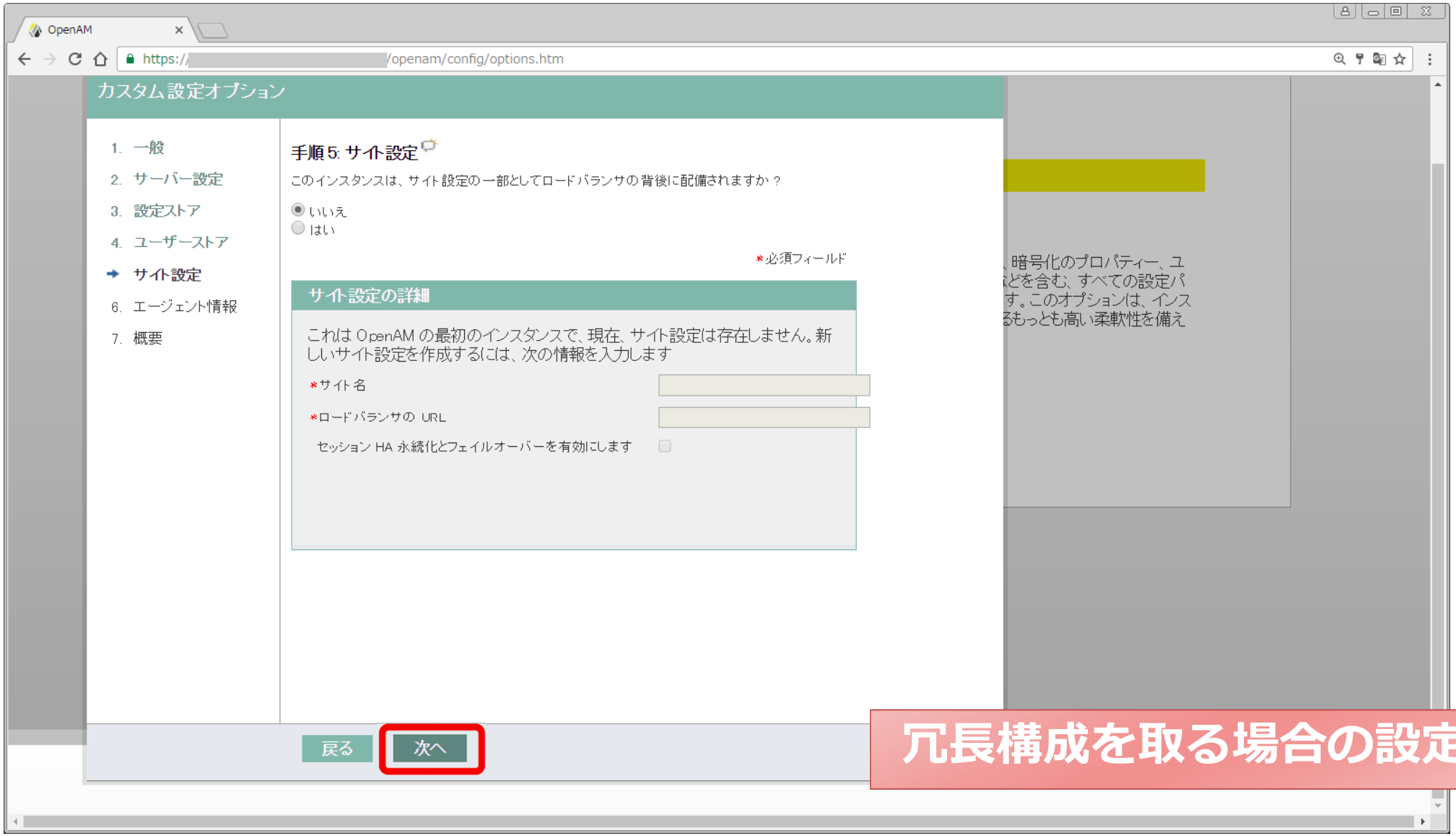


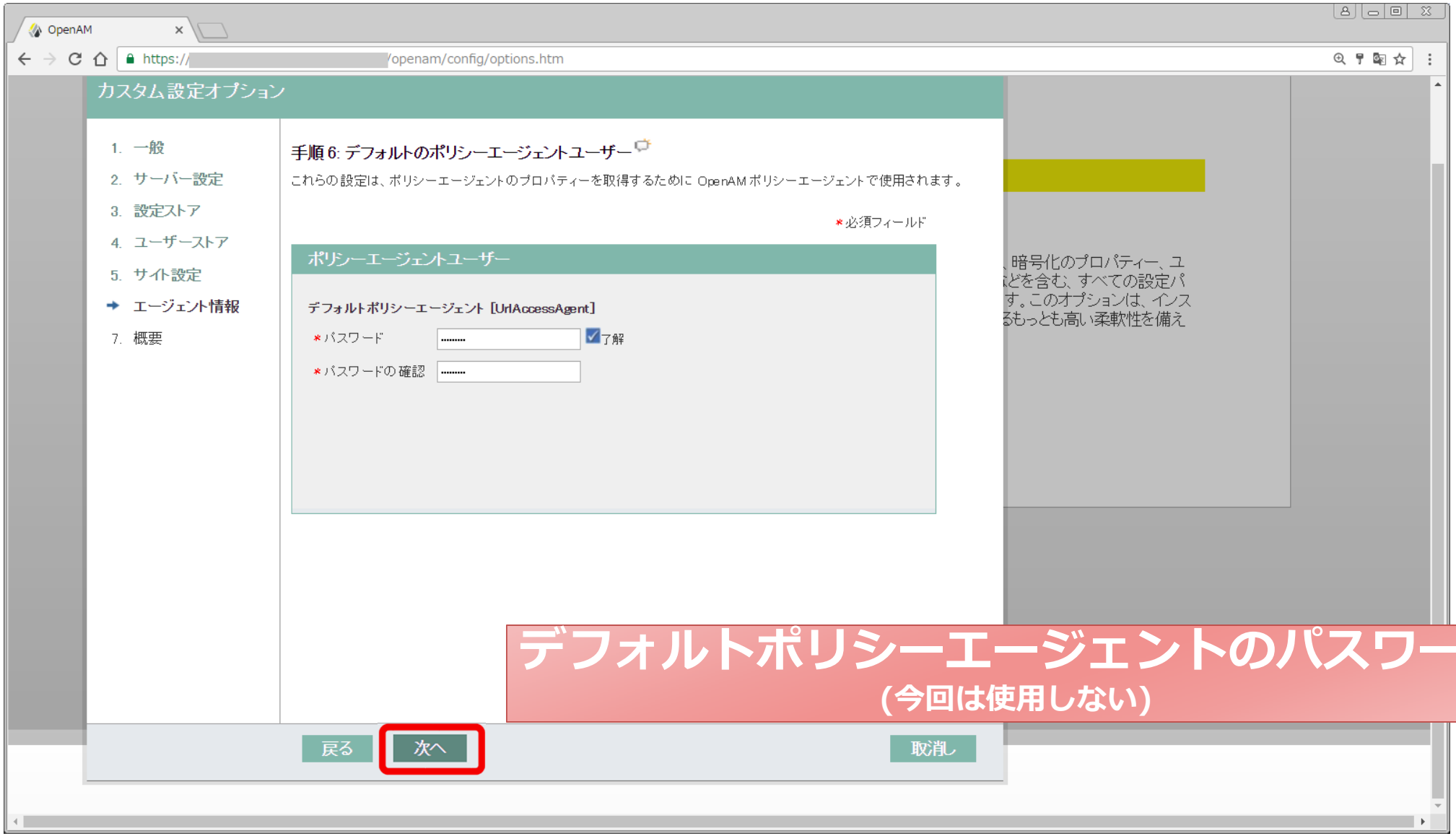


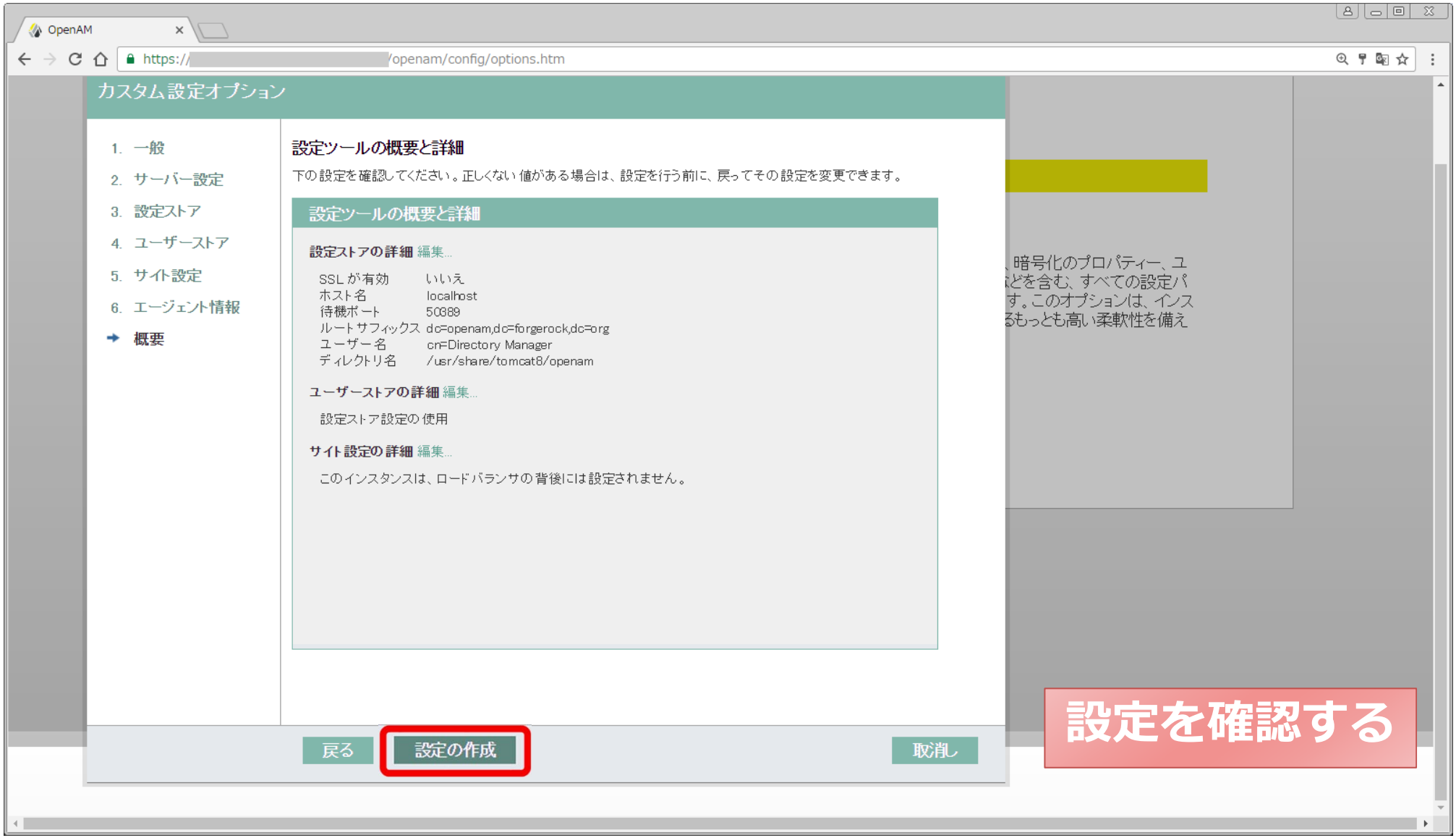

OpenAM
https://
/openam/config/options.htm
カスタム設定オプション
1. 一般
2. サーバー設定
設定ストア
4. ユーザーストア
5. サイト設定
6. エージェント情報
7. 概要
手順 3: 設定データストア設定
環境にほかの 既存の OpenAM インスタンスがなければ、「最初の インスタンス」を選択します。環境に 1 つ以上の 既存の OpenAM インスタンスがあれば、「既存の配備に追加しますか。」を選択します。
最初のインスタンス
既存の配備に追加しますか。
* 必須フィールド
設定ストアの詳細
設定データストア
OpenAM
OpenDJ または Oracle Directory Server Enterprise Edition
* SSL が有効
* ホスト名
localhost
* ポート
50389
* 管理者ポート
4444
* JMX ポート
1689
* 暗号化鍵
/YPgJe9voekbpgJWAAD1VPTFWKIZMkb
* ルートサフィックス
dc=openam,dc=forgerock,dc=org
戻る
次へ
OpenAMの設定を保管する
ストアの選択

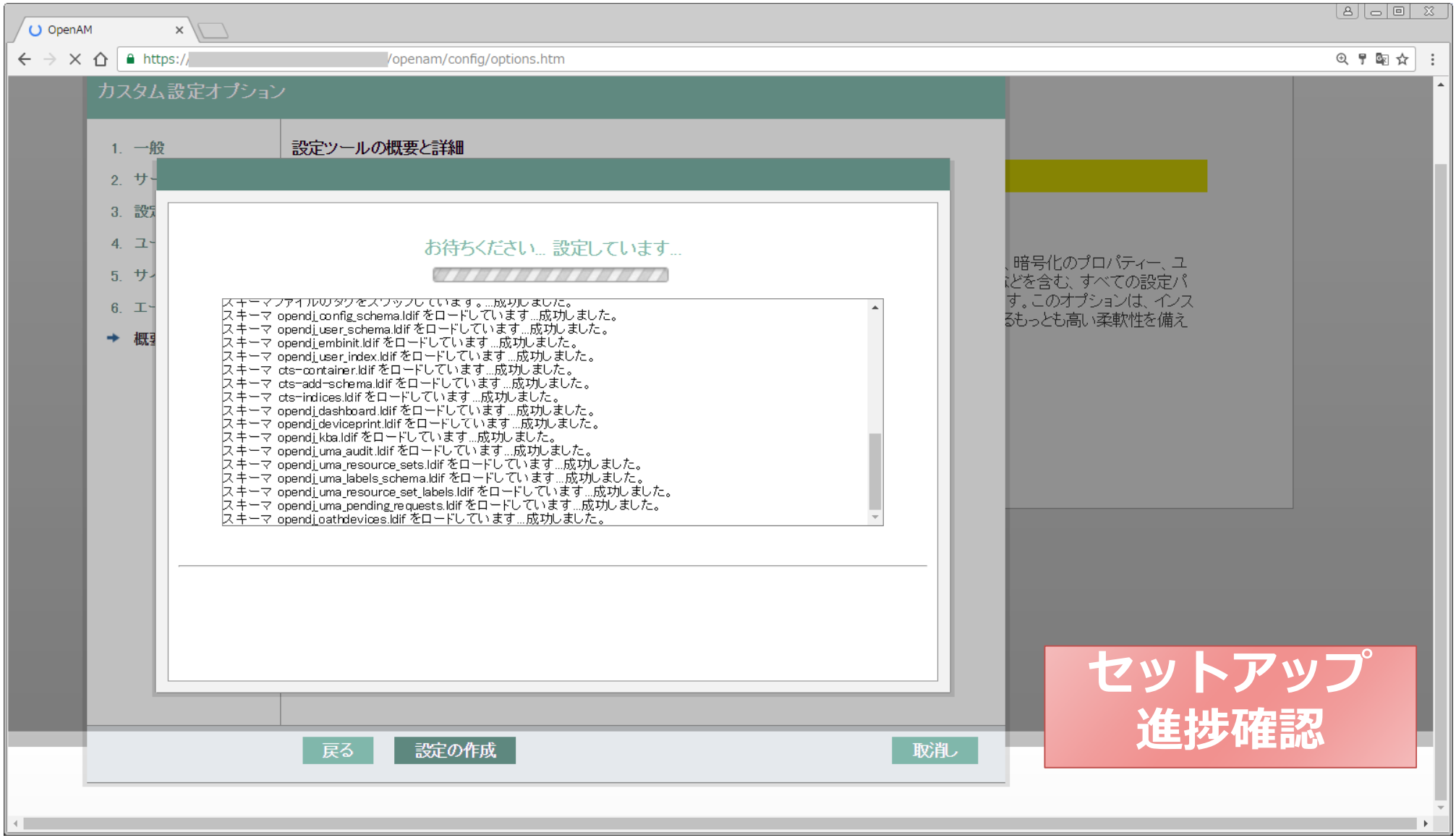


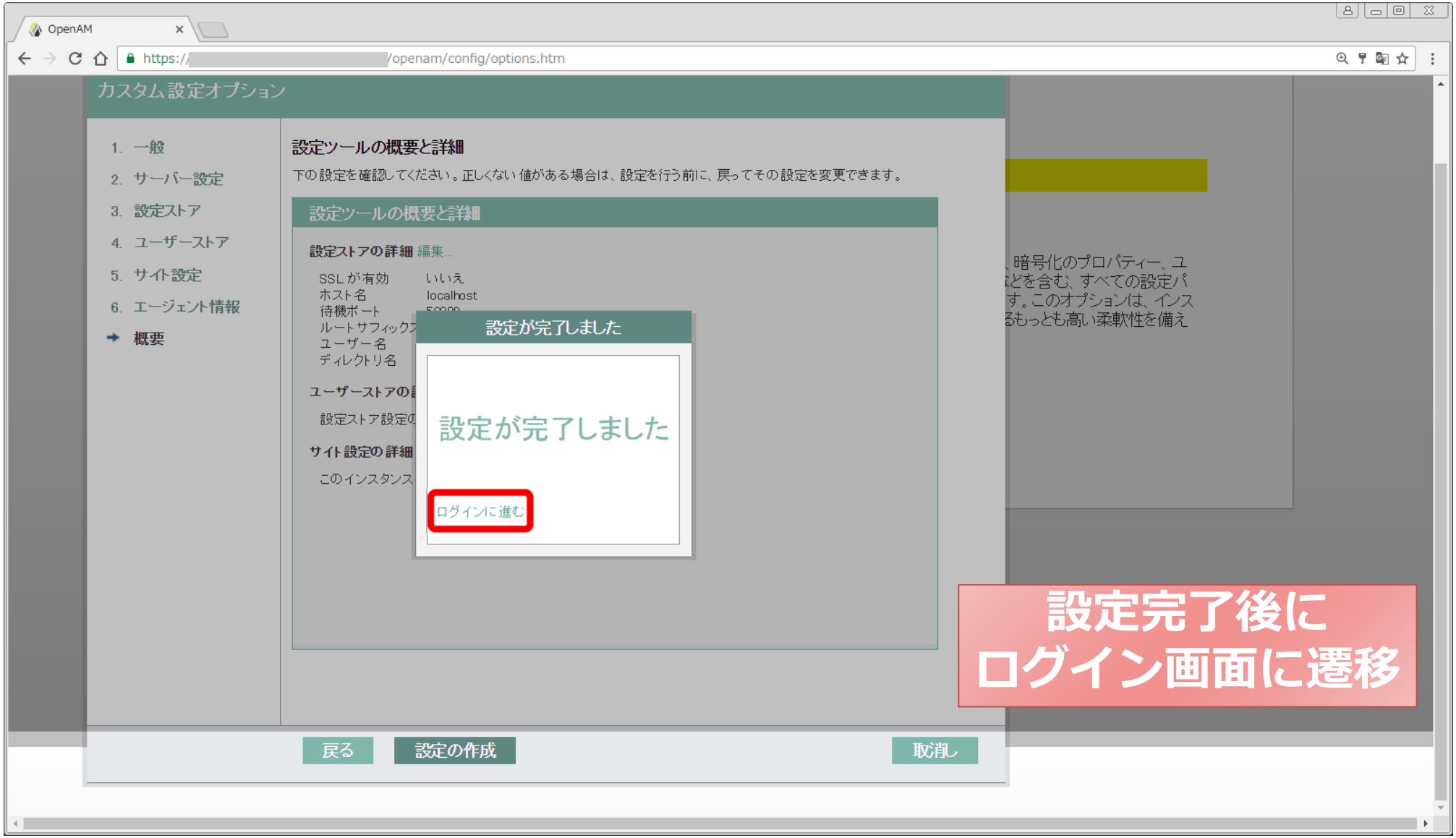
OpenAMを利用する
ユーザのストアを設定
(今回はデモ・検証用なのでOpenAMのデータストアを利用)

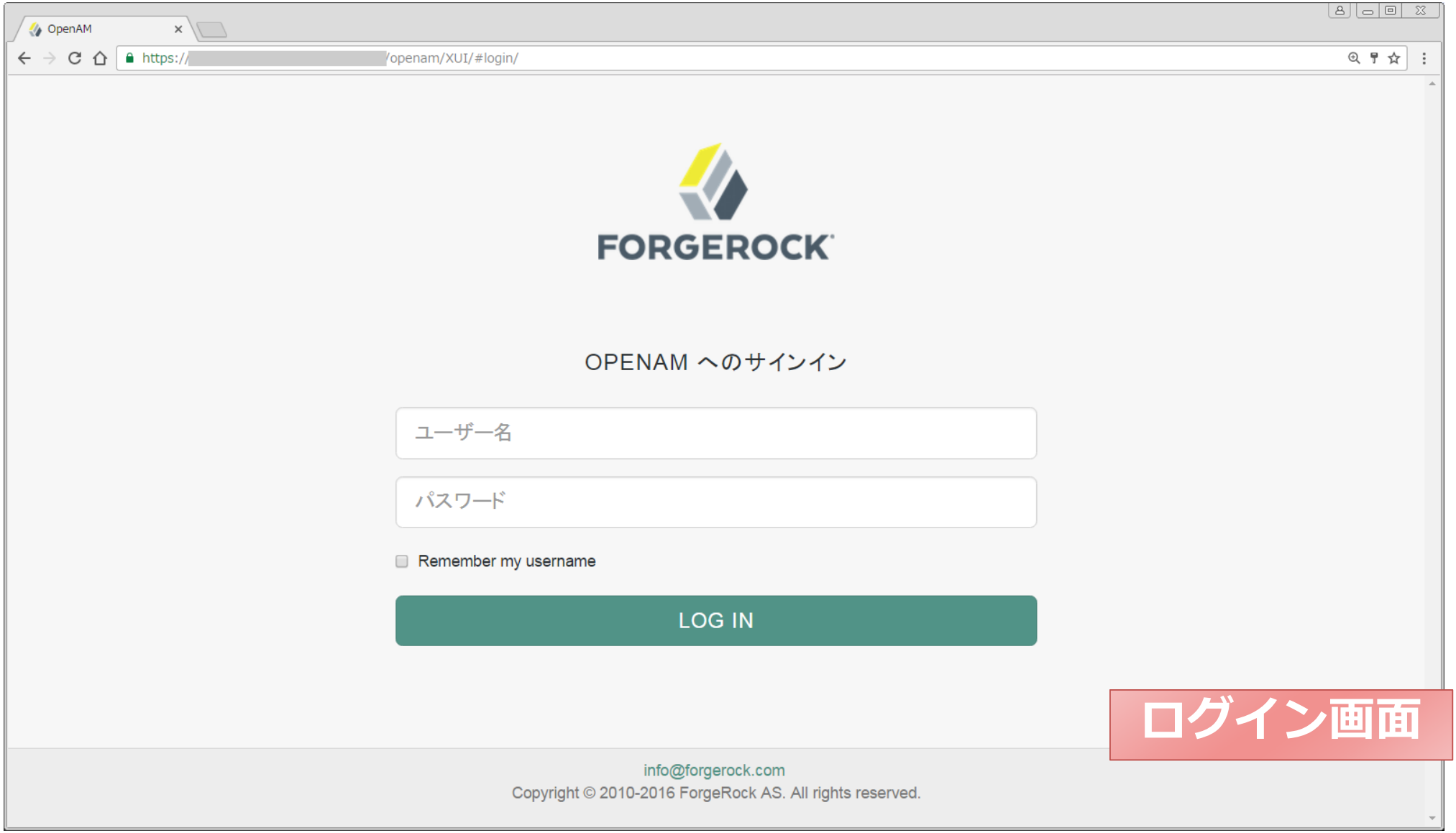




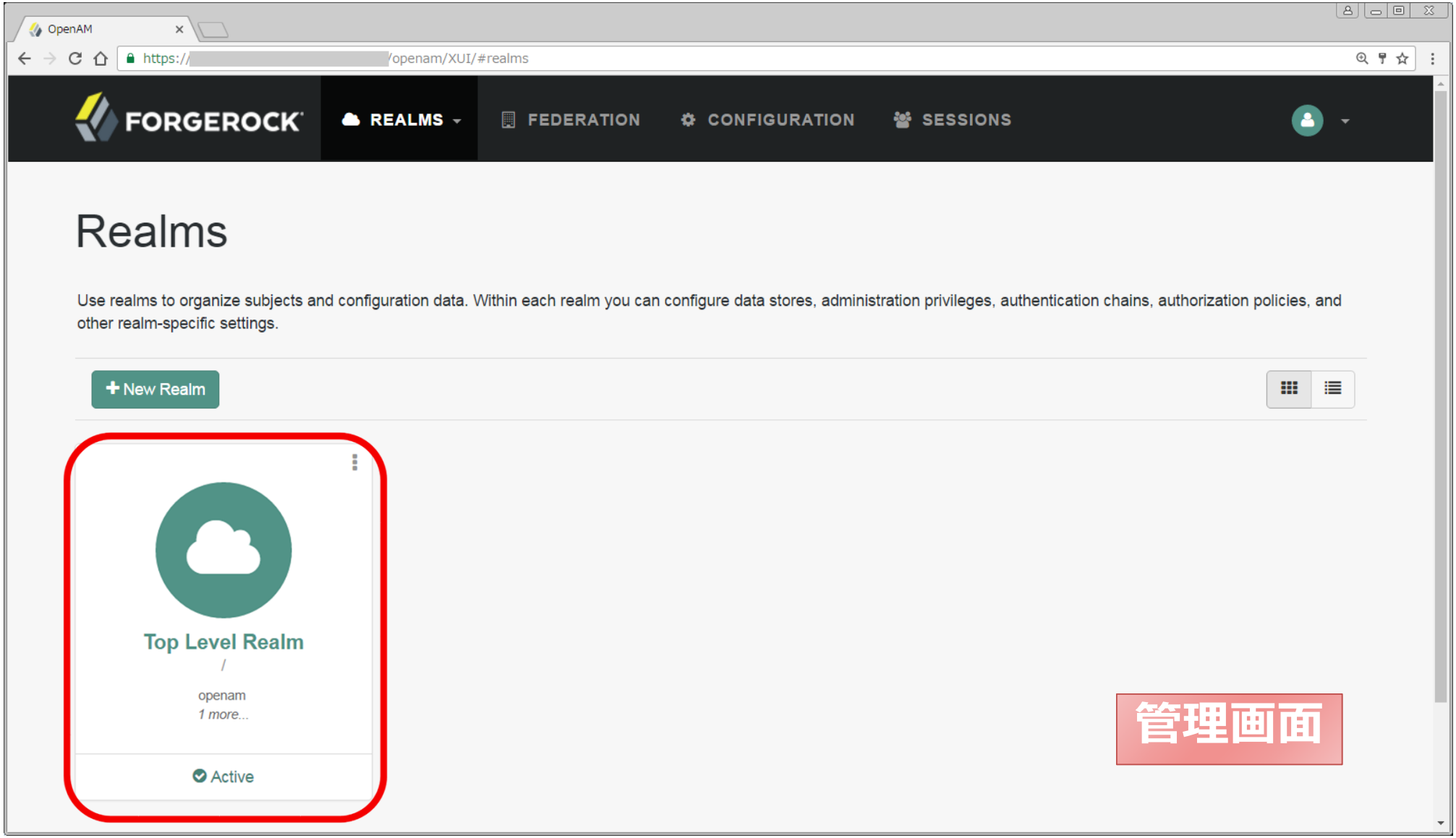


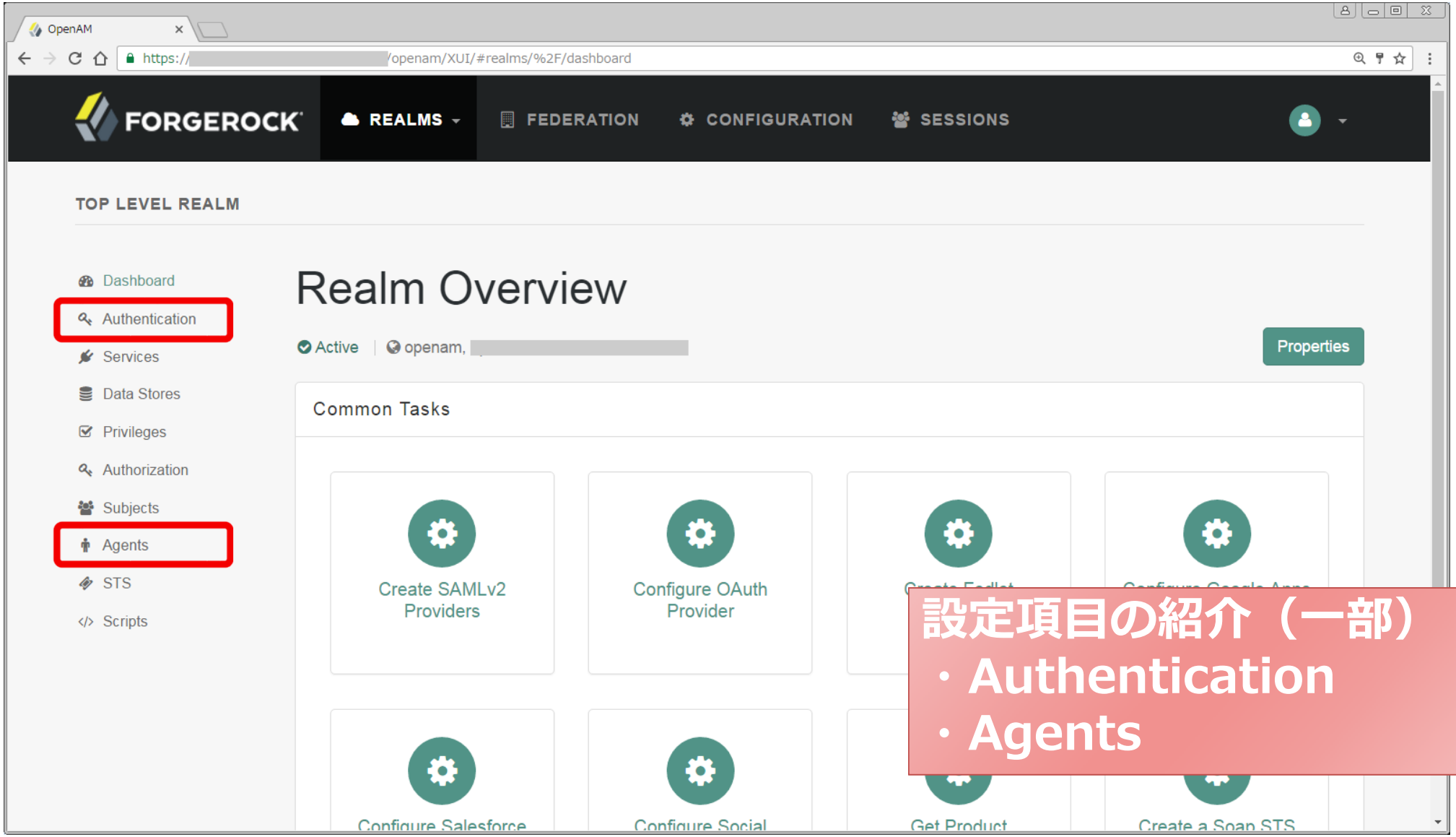


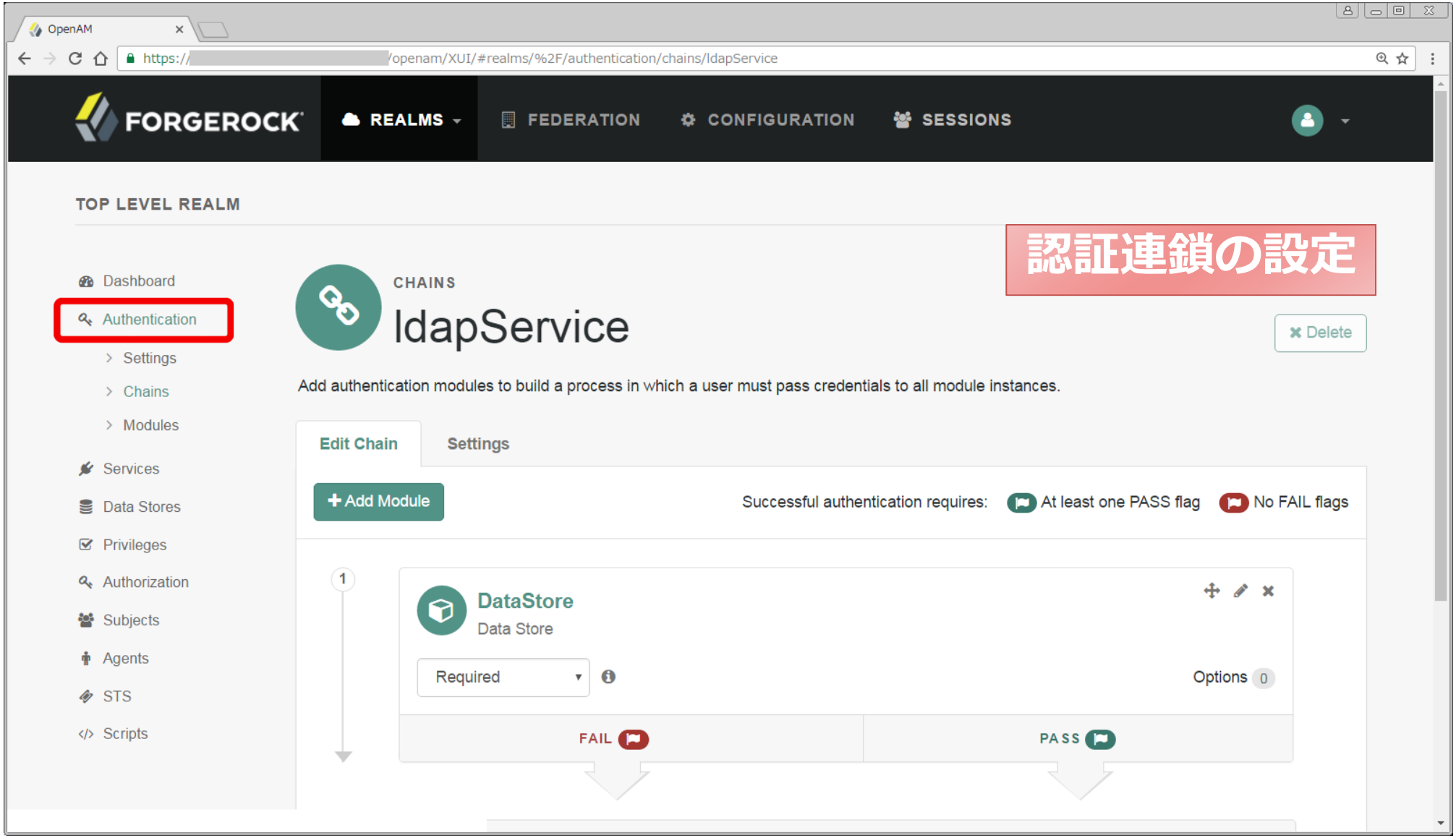



OpenAM
https://[redacted]/openam/XUI/#login/
FORGEROCK
OPENAM へのサインイン
ユーザー名
パスワード
Remember my username
LOG IN
info@forgerock.com
Copyright © 2010-2016 ForgeRock AS. All rights reserved.

ログイン画面







フェデレーション型(OIDC)を利用する際の注意点

◘13.0.0のバージョンにはバグがある

- ➢認証情報の連携同意画面が表示できない
- ➢XUI/libs/text.jsの21行目に改修が必要

```
defaultPort = hasLocation && (location.port || (defaultProtocol === 'https' ? '443' : '80')),
```

https://forum.forgerock.com/topic/openam-with-openid-service-provider-over-https/
https://bugster.forgerock.org/jira/browse/OPENAM-8371

アジェンダ

- AWSアカウント管理の苦労
- OpenAMとは
  - 認証連携方式
  - OpenAMをセットアップして使ってみる
- **フェデレーションでアカウント管理効率UP**
  - SAMLによるフェデレーション
  - OpenID Connectによるフェデレーション
- フェデレーション技術と今後ID管理について

フェデレーションで ID管理の悩み解決

アカウント管理上の課題

ユーザの不満 (不便！)

- 追加が遅れると不便だ
- MFA有効化が面倒だ
- そもそも認証するのが面倒だ

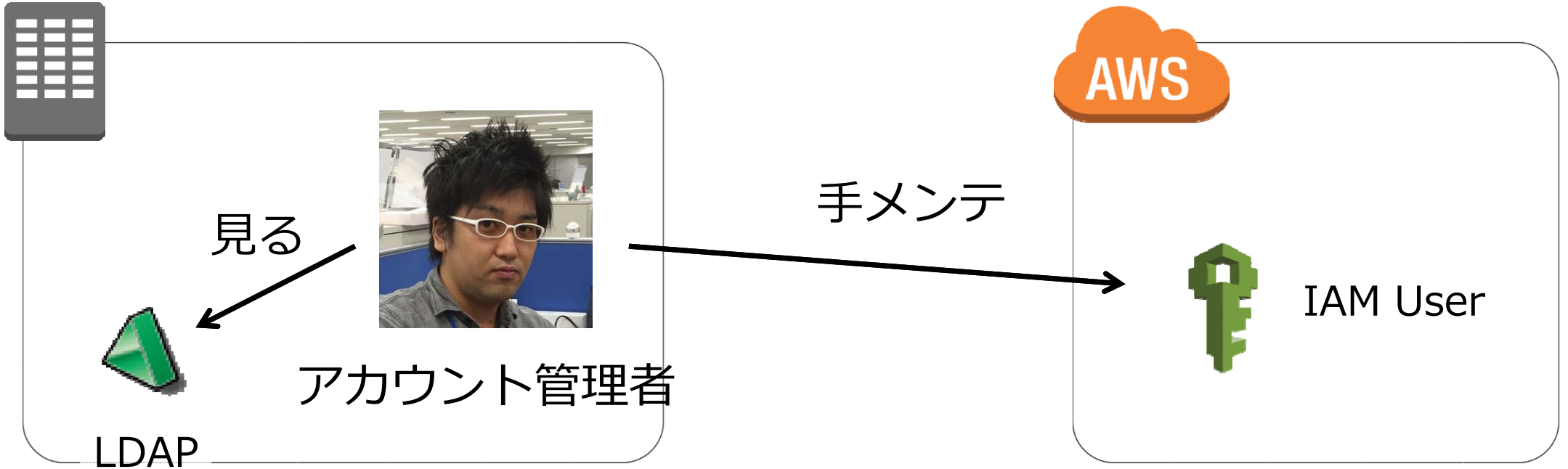
管理者の不満 (面倒！リスク！)

- 手作業が多い
- MFAを強制できない
- 作業を忘れたら企業に打撃を与える可能性がある

アカウント管理上の課題の元になっていること

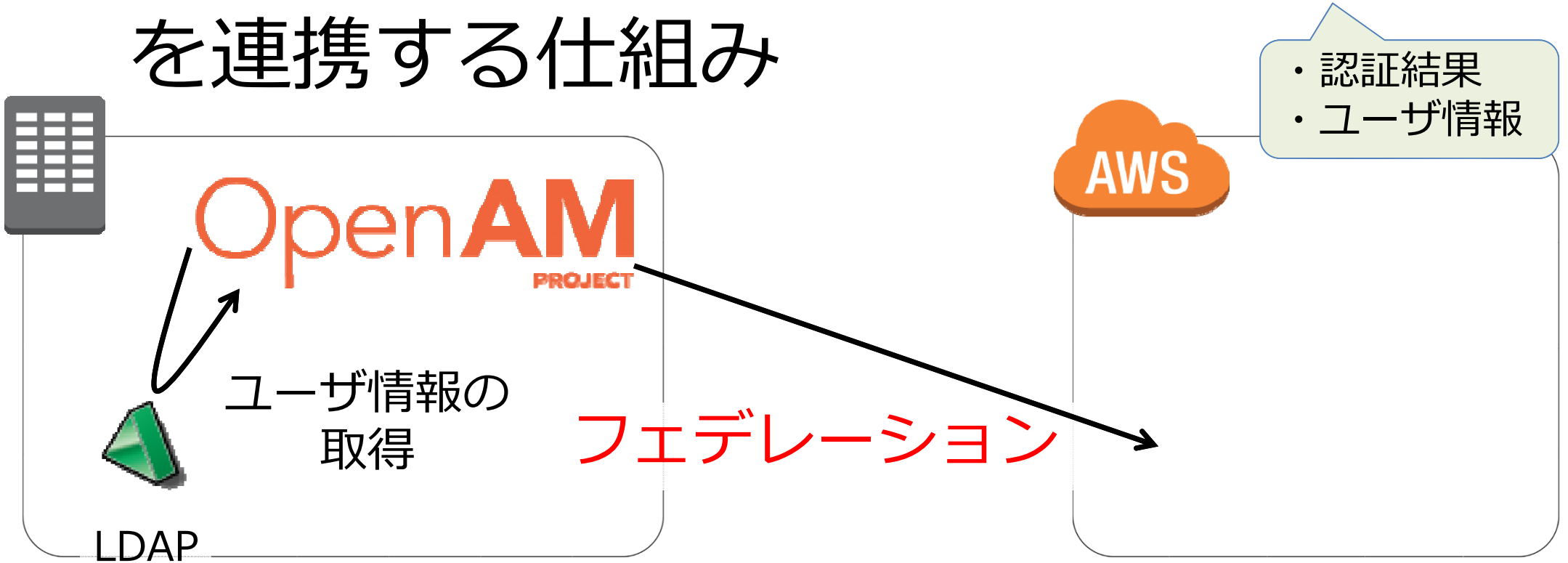
◘社内に存在するユーザ情報のコピー

- ➢手作業でIAMユーザを追加



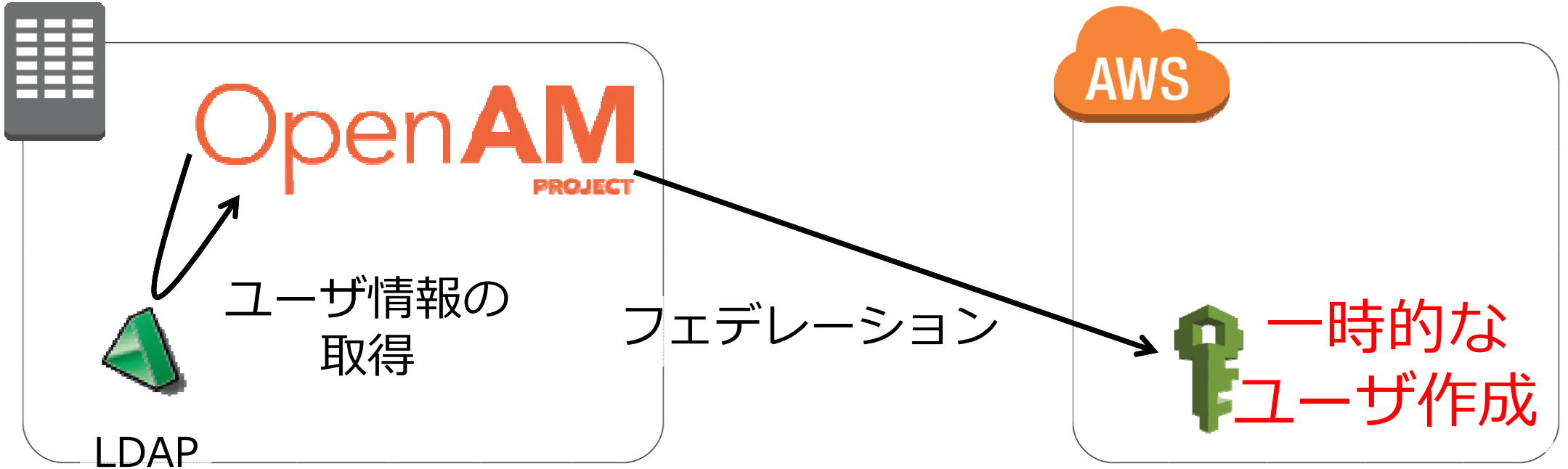
フェデレーション(ID連携)

- 異なるシステム間で、安全にID情報を連携する仕組み



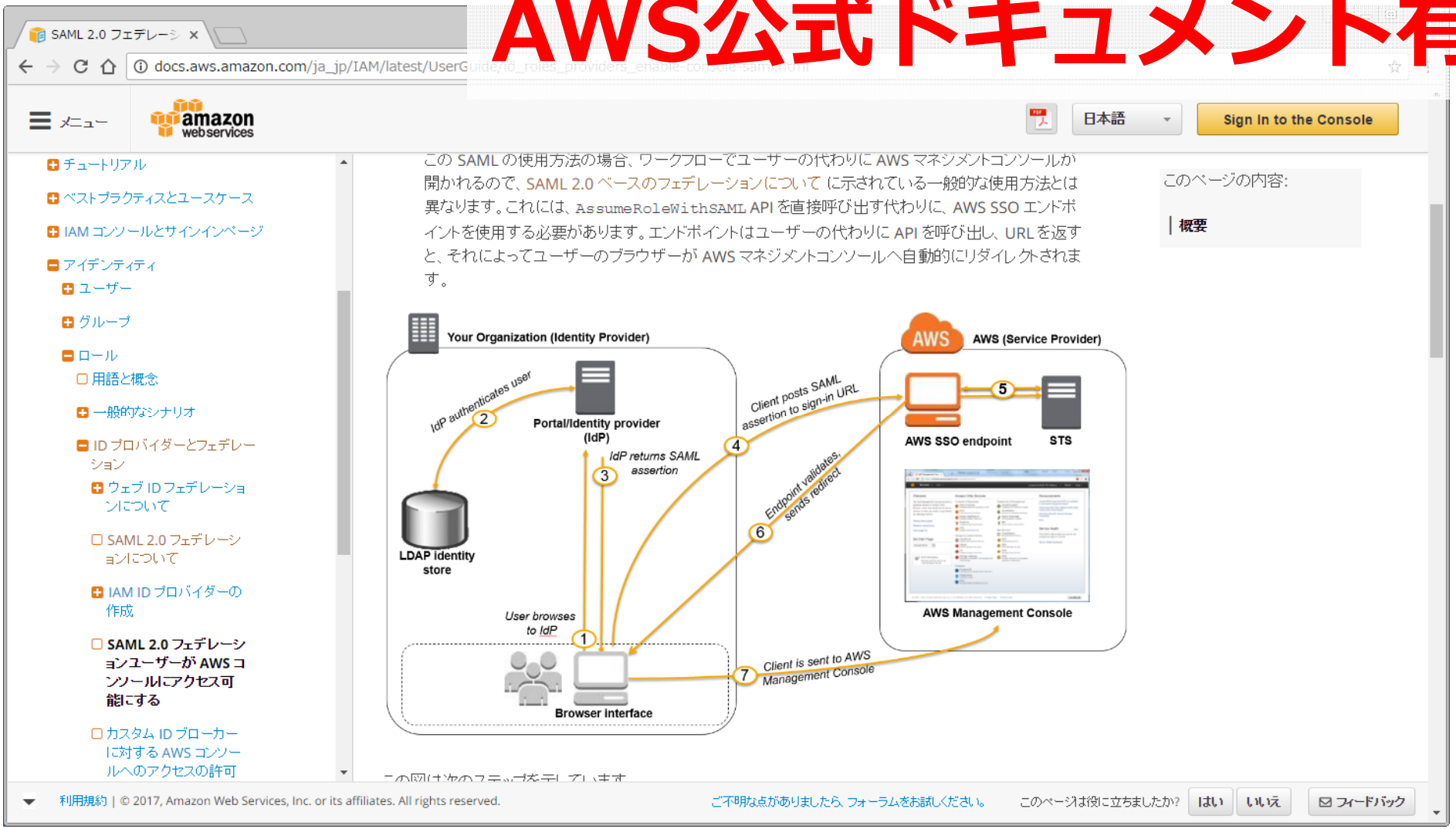
STS (Security Token Service)のAssumeRole

- 一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供



これらを組み合わせたら
社内のID情報で
AWSのユーザ管理を代用できる
(AssumeRoleWithSAML)

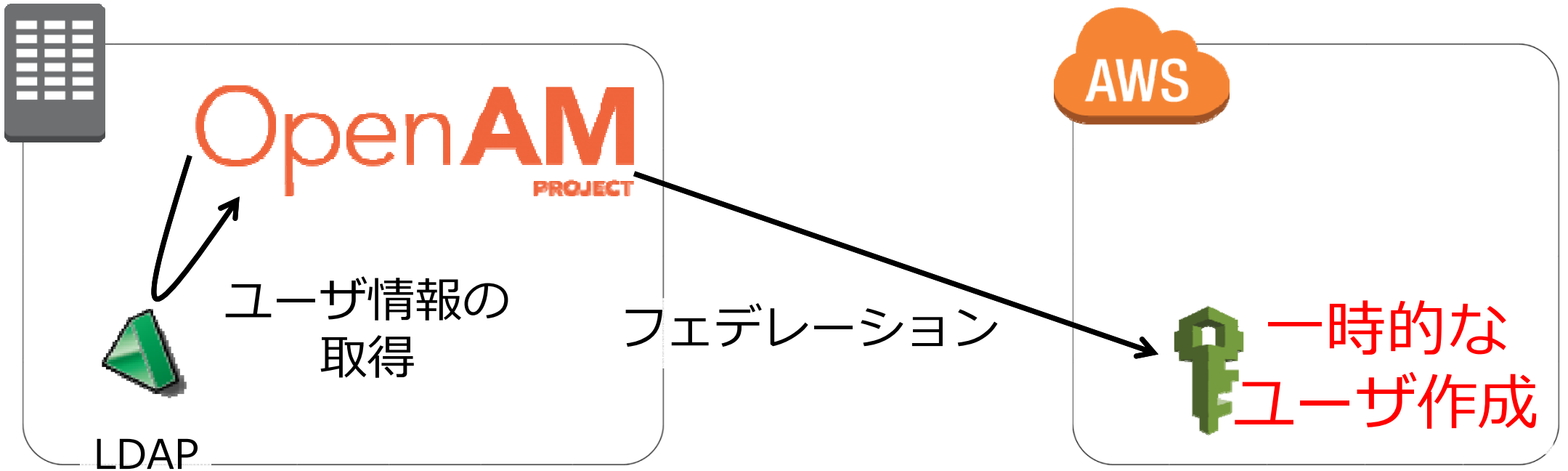
AWS公式ドキュメント有り



http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

SAML IdPとSAML SP

- SAML IdP (Identity Provider)
  - Identity情報の連携元(今回はOpenAM)
- SAML SP(Service Provider)
  - Identity情報の連携先(今回はAWS)

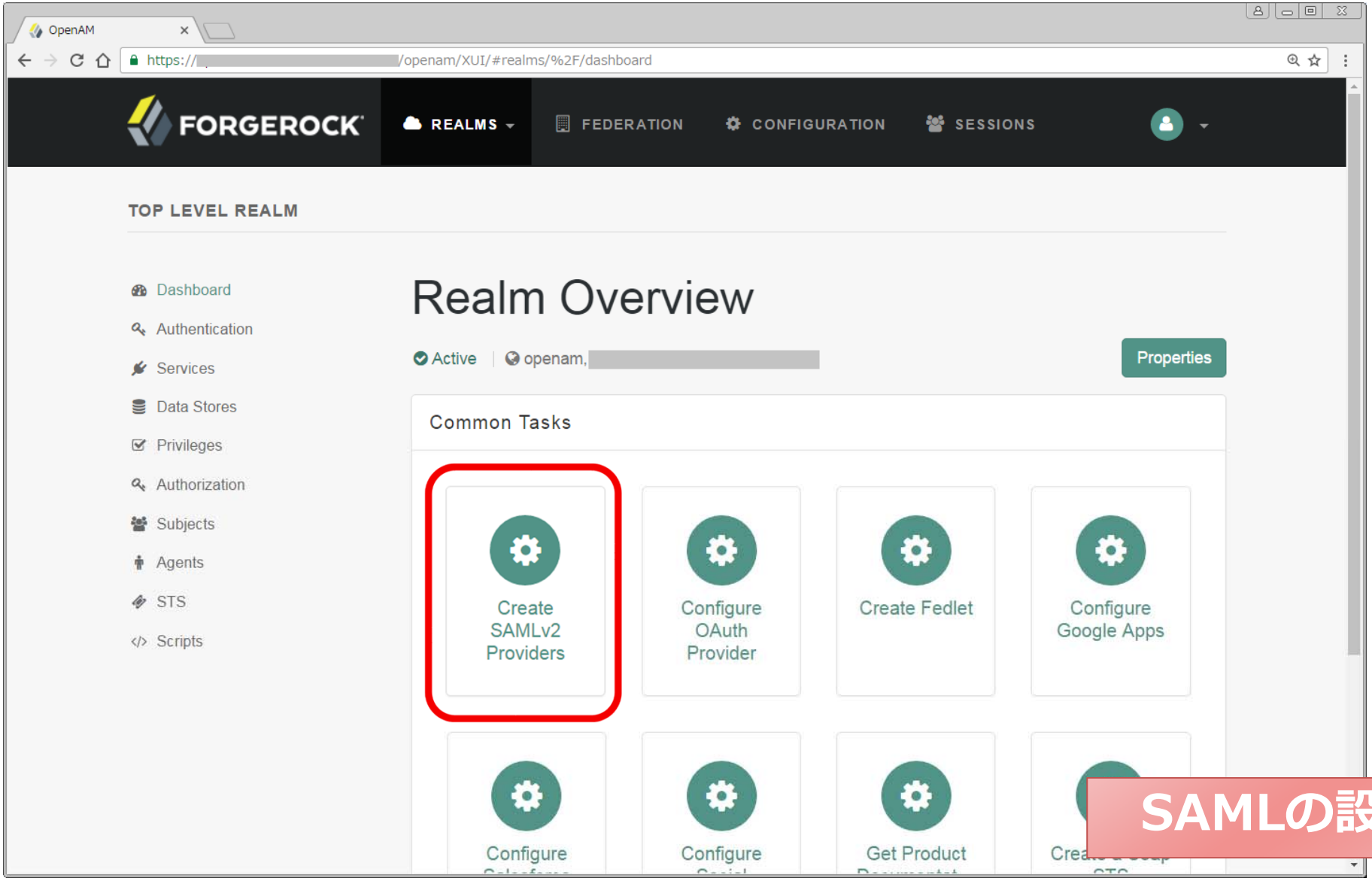


設定の流れ

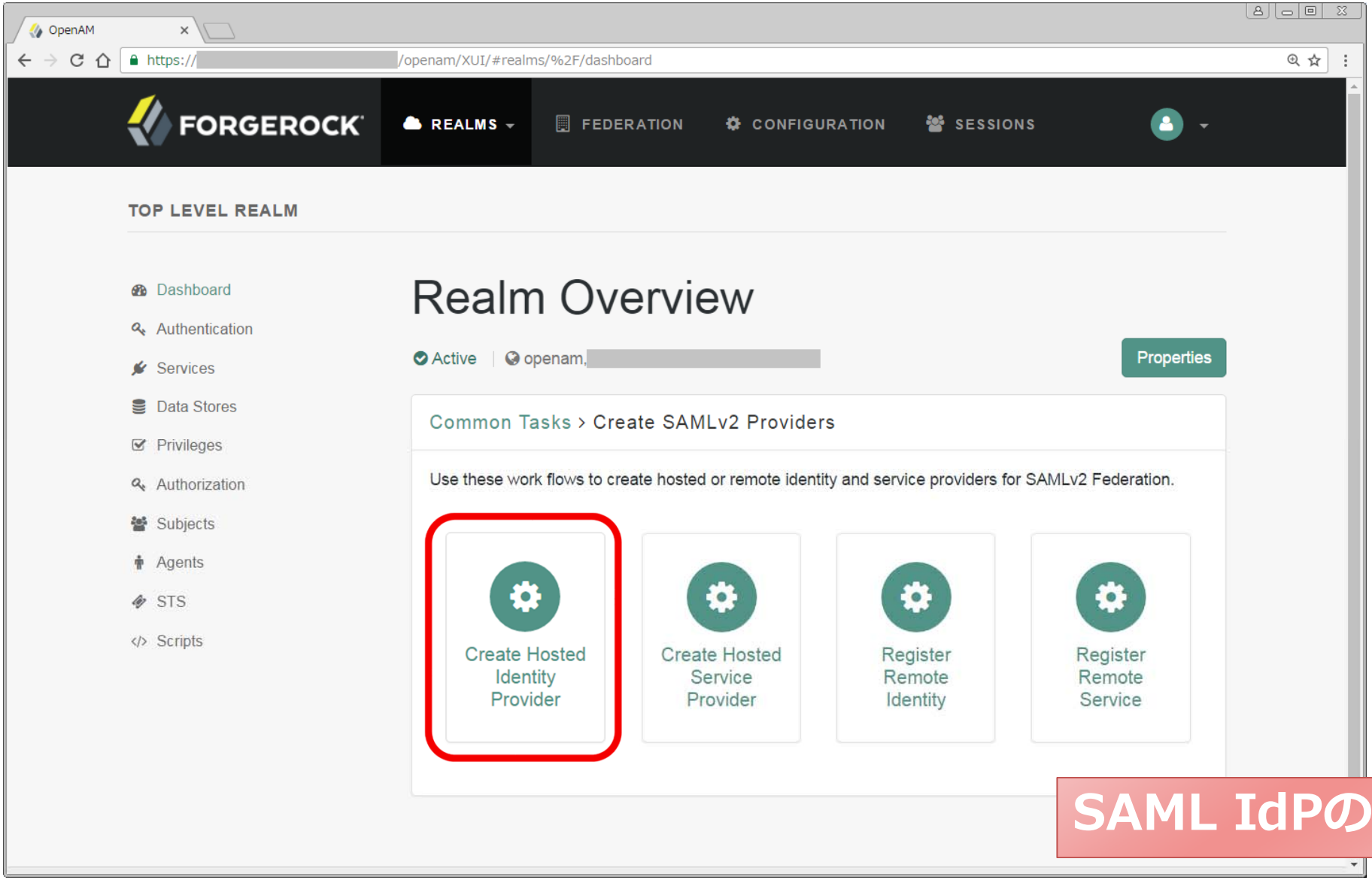
- SAML IdPを構成する
  - OpenAMをSAML IdPとして構成する
- SAML IdP, SPのメタデータを取得する
  - OpenAMのIdPメタデータを取得
  - AWSのSPメタデータを取得
- 互いに相手の設定を行う
  - OpenAMにSAML SP(AWS)を登録する
  - AWSにSAML IdP(OpenAM)を登録する

設定の流れ

- SAML IdPを構成する
  - OpenAMをSAML IdPとして構成する
- SAML IdP, SPのメタデータを取得する
  - OpenAMのIdPメタデータを取得
  - AWSのSPメタデータを取得
- 互いに相手の設定を行う
  - OpenAMにSAML SP(AWS)を登録する
  - AWSにSAML IdP(OpenAM)を登録する



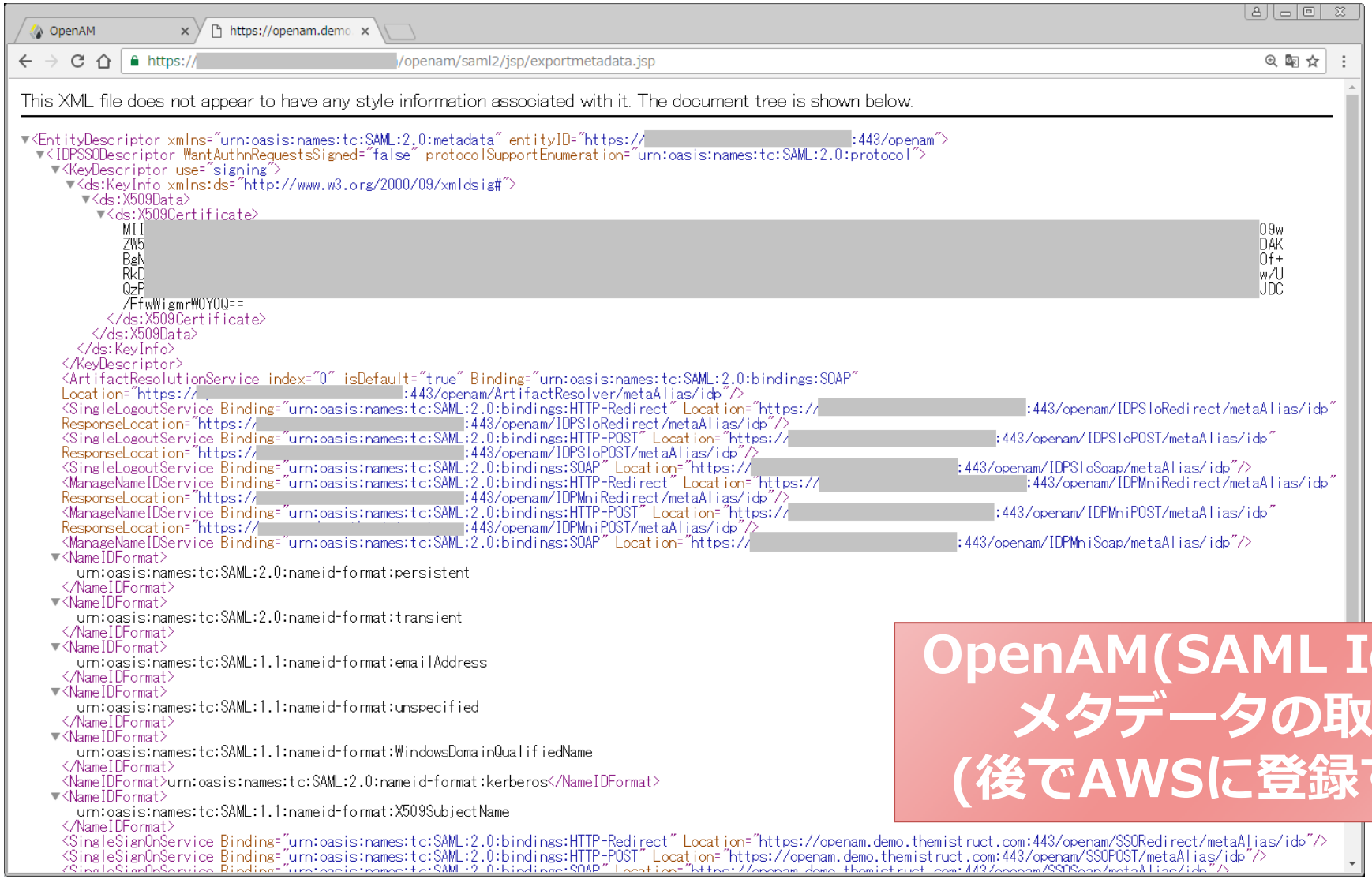
SAMLの設定



IdPの登録完了

設定の流れ

- ☑SAML IdPを構成する
  - OpenAMをSAML IdPとして構成する
- □SAML IdP, SPのメタデータを取得する
  - OpenAMのIdPメタデータを取得
  - AWSのSPメタデータを取得
- □互いに相手の設定を行う
  - OpenAMにSAML SP(AWS)を登録する
  - AWSにSAML IdP(OpenAM)を登録する



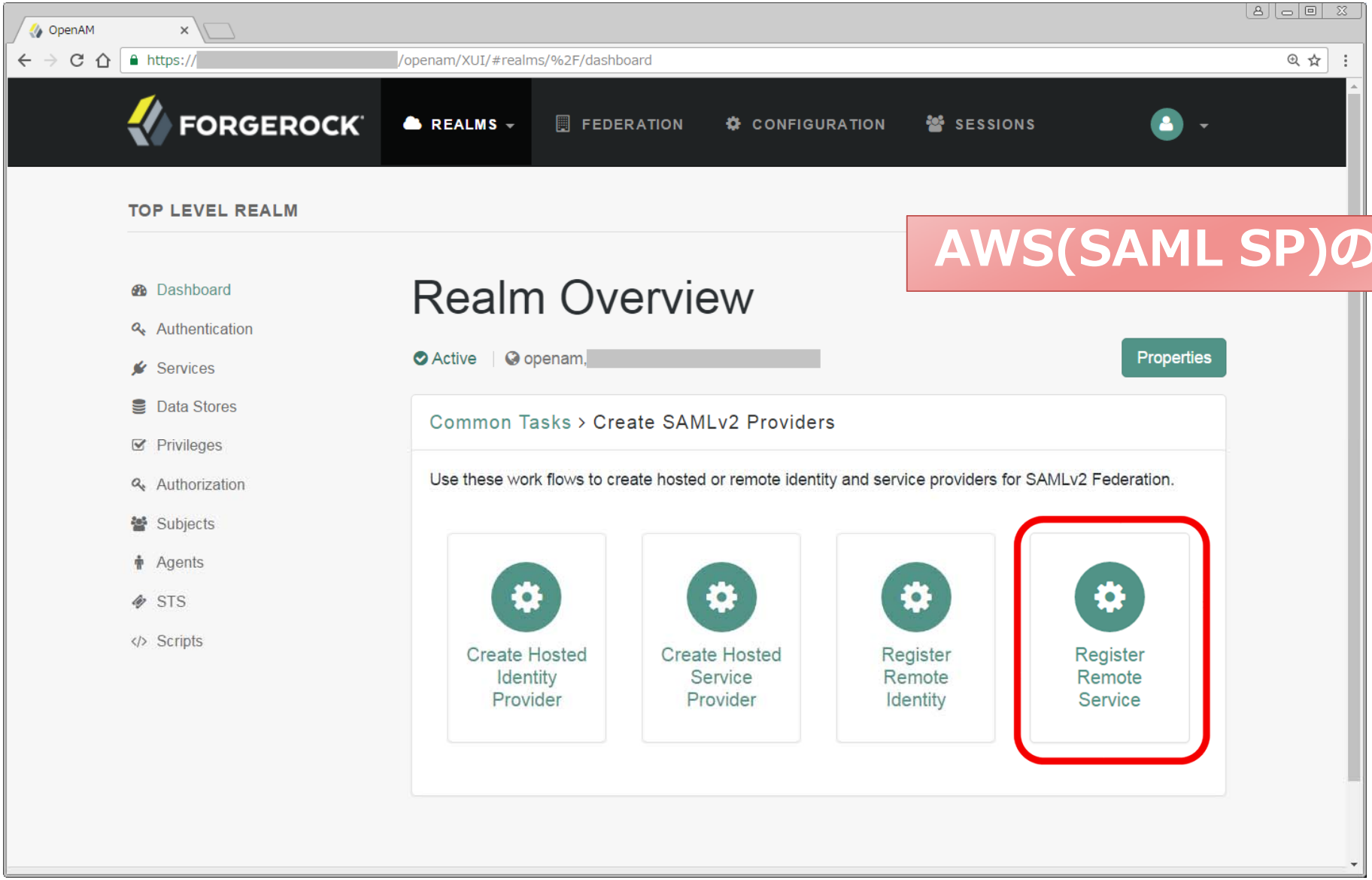
https://xxxxxxxxxxx/openam/saml2/jsp/exportmetadata.jsp

AWS(SAML SP)の
メタデータの取得
(後でOpenAMに登録する)

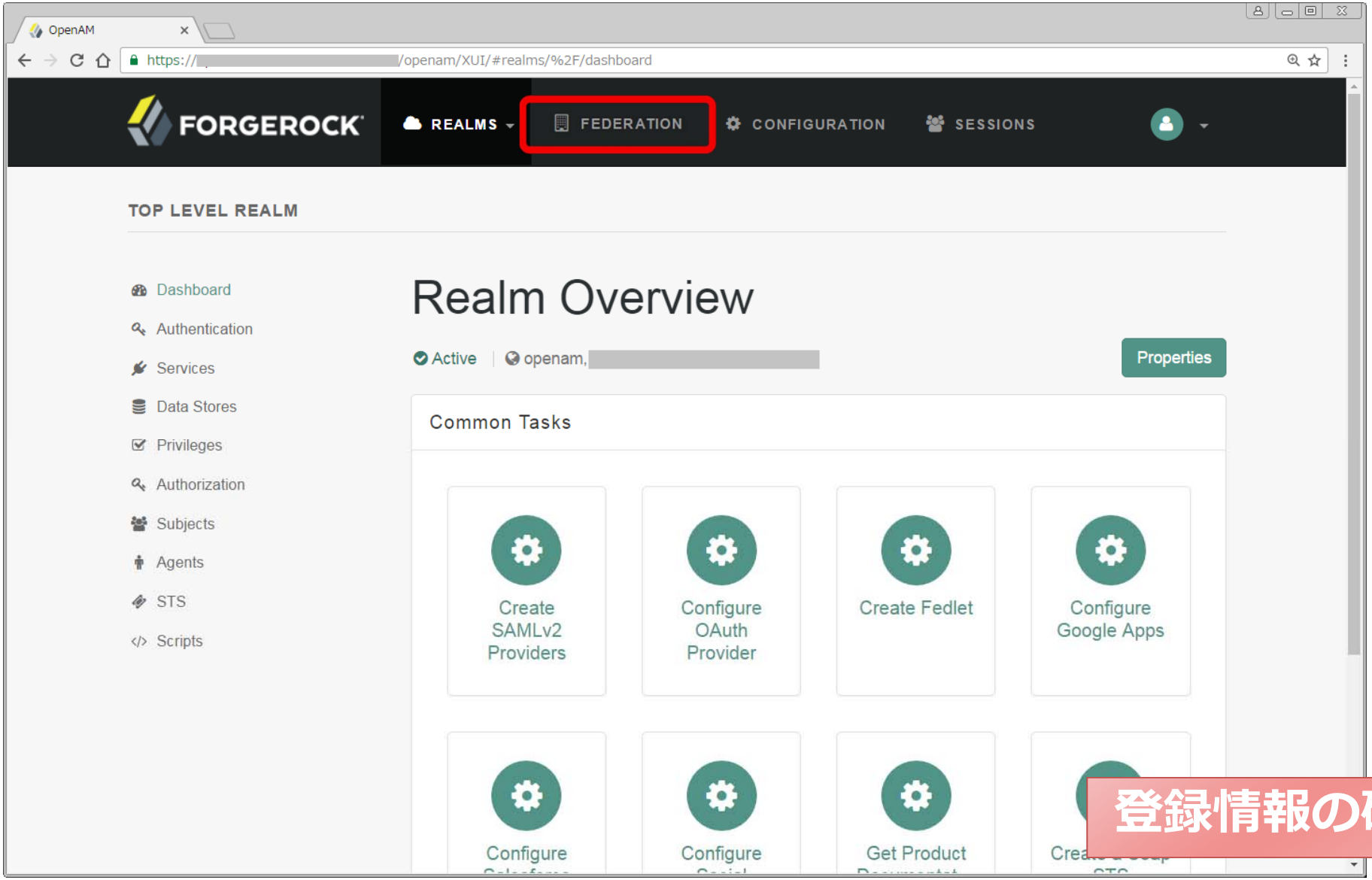
https://signin.aws.amazon.com/static/saml-metadata.xml

設定の流れ

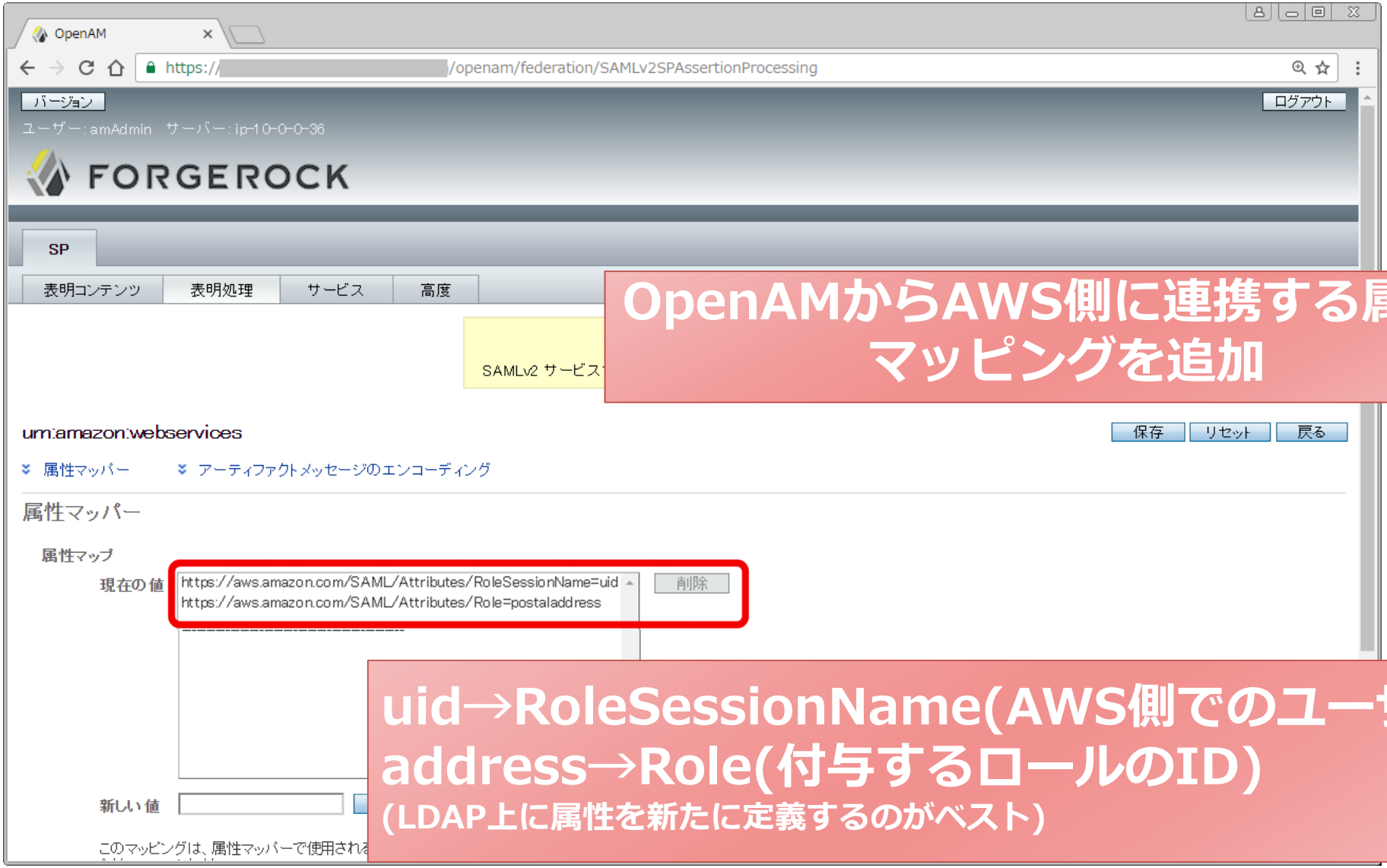
- ☑SAML IdPを構成する
  - OpenAMをSAML IdPとして構成する
- ☑SAML IdP, SPのメタデータを取得する
  - OpenAMのIdPメタデータを取得
  - AWSのSPメタデータを取得
- ☐互いに相手の設定を行う
  - OpenAMにSAML SP(AWS)を登録する
  - AWSにSAML IdP(OpenAM)を登録する

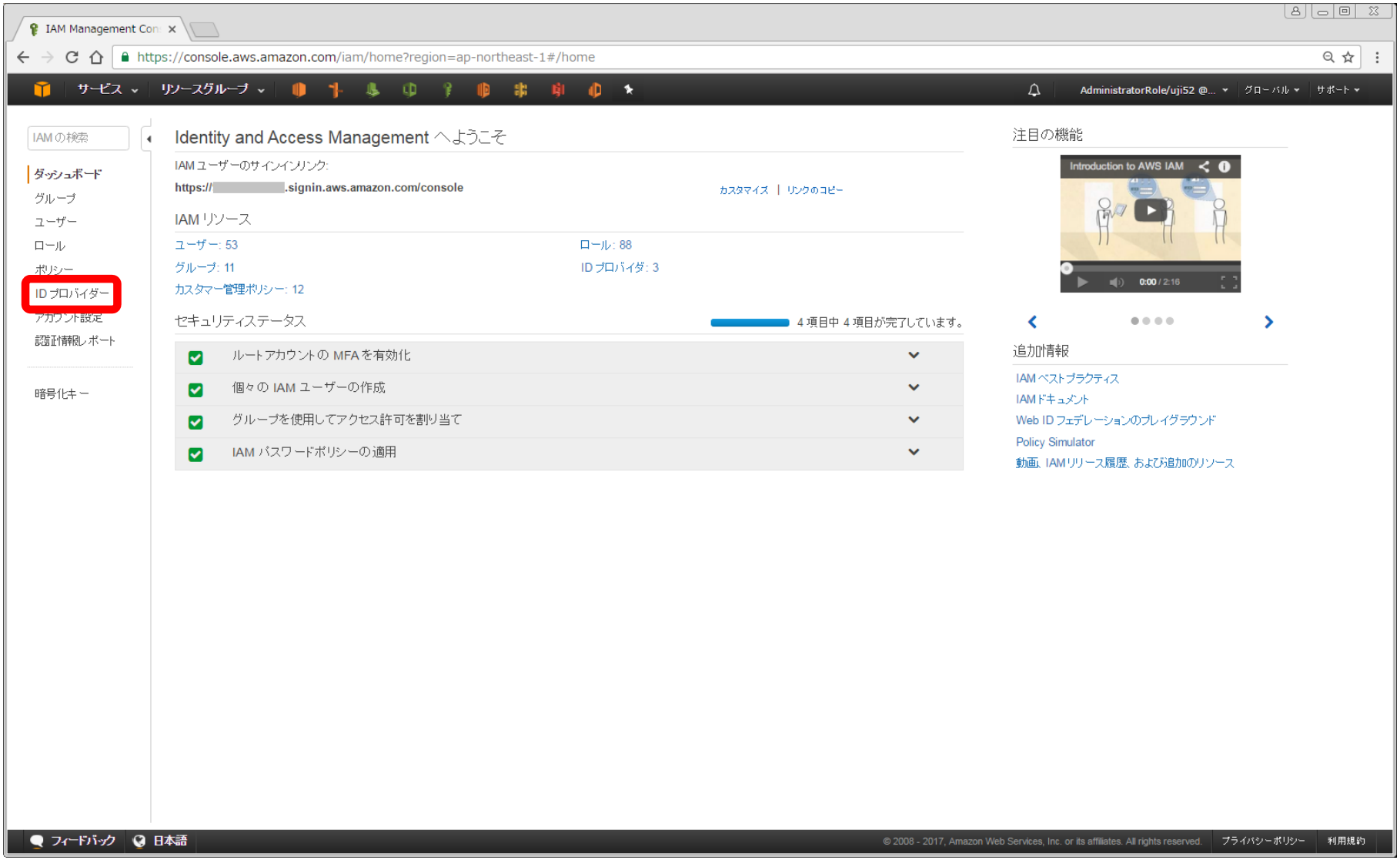


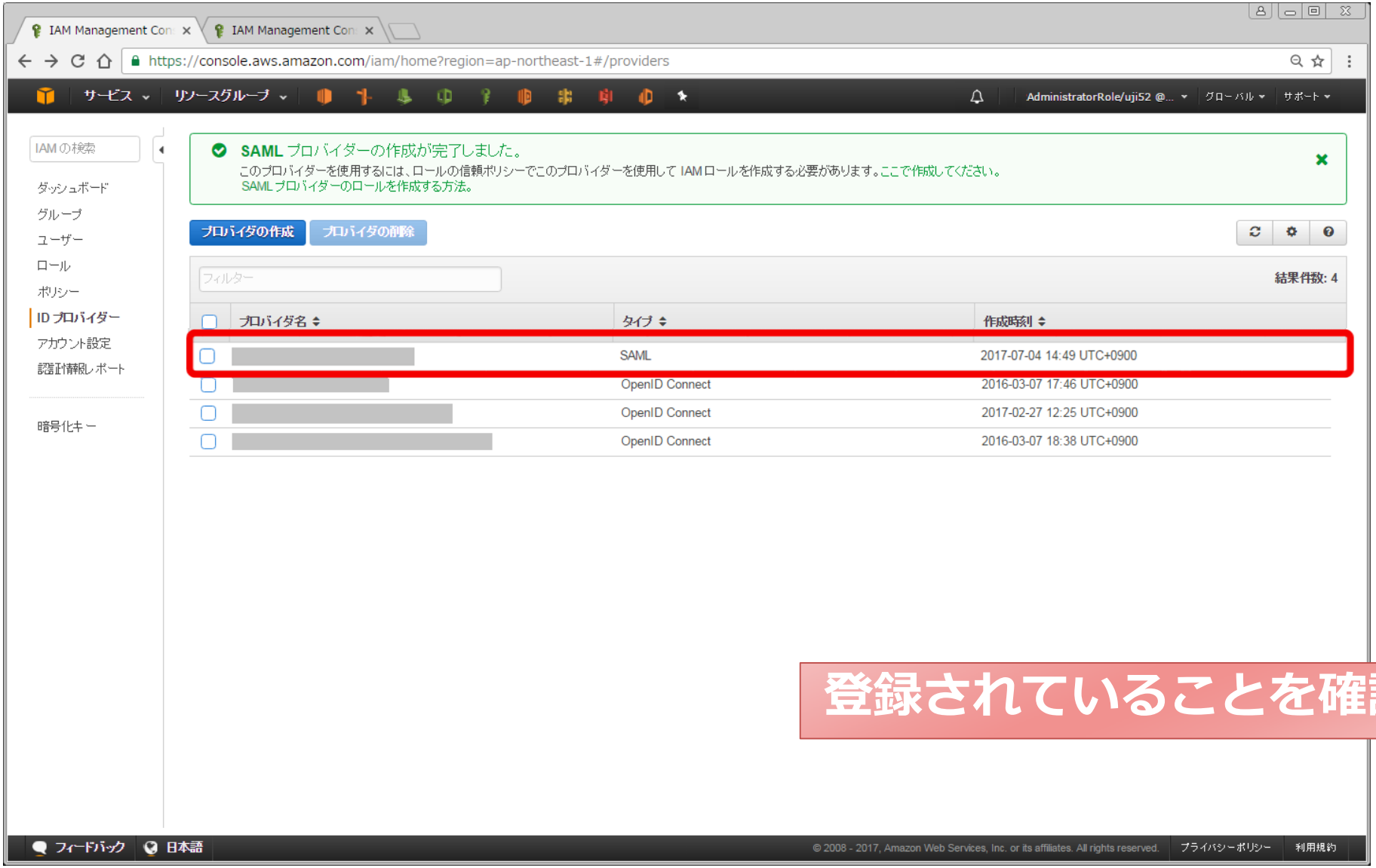
AWS(SAML SP)の登録

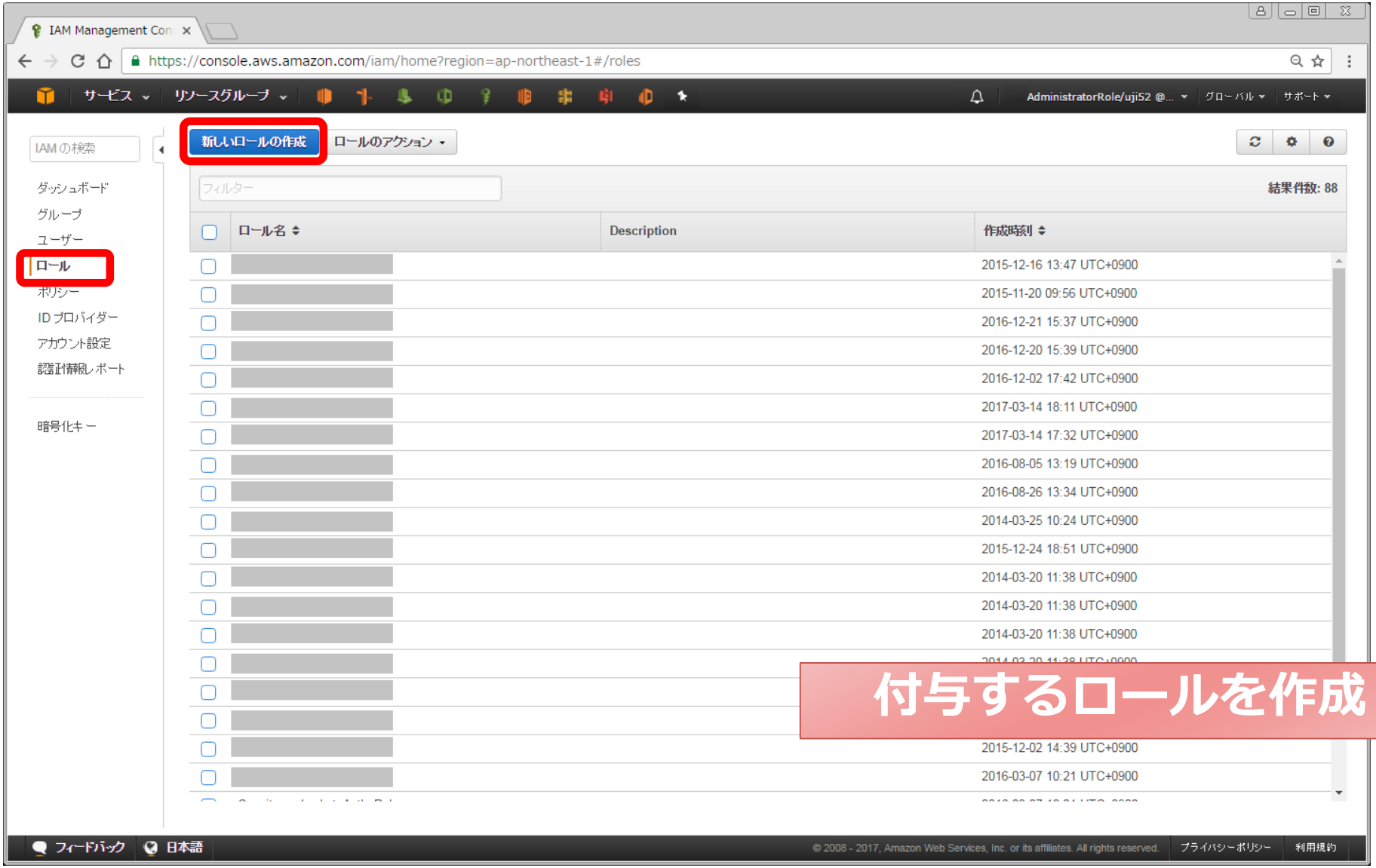


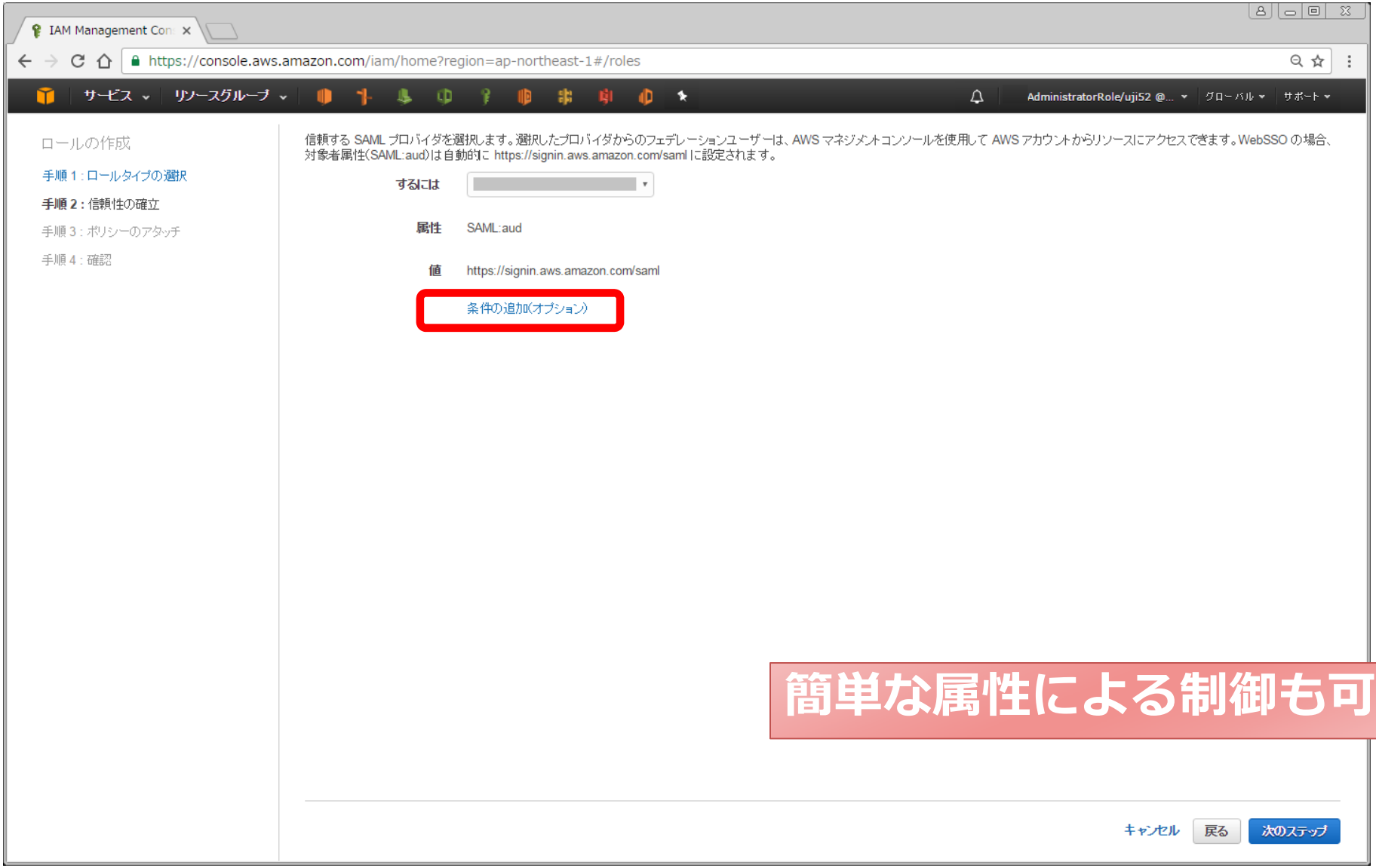
IdPとSPが登録されていることを確認

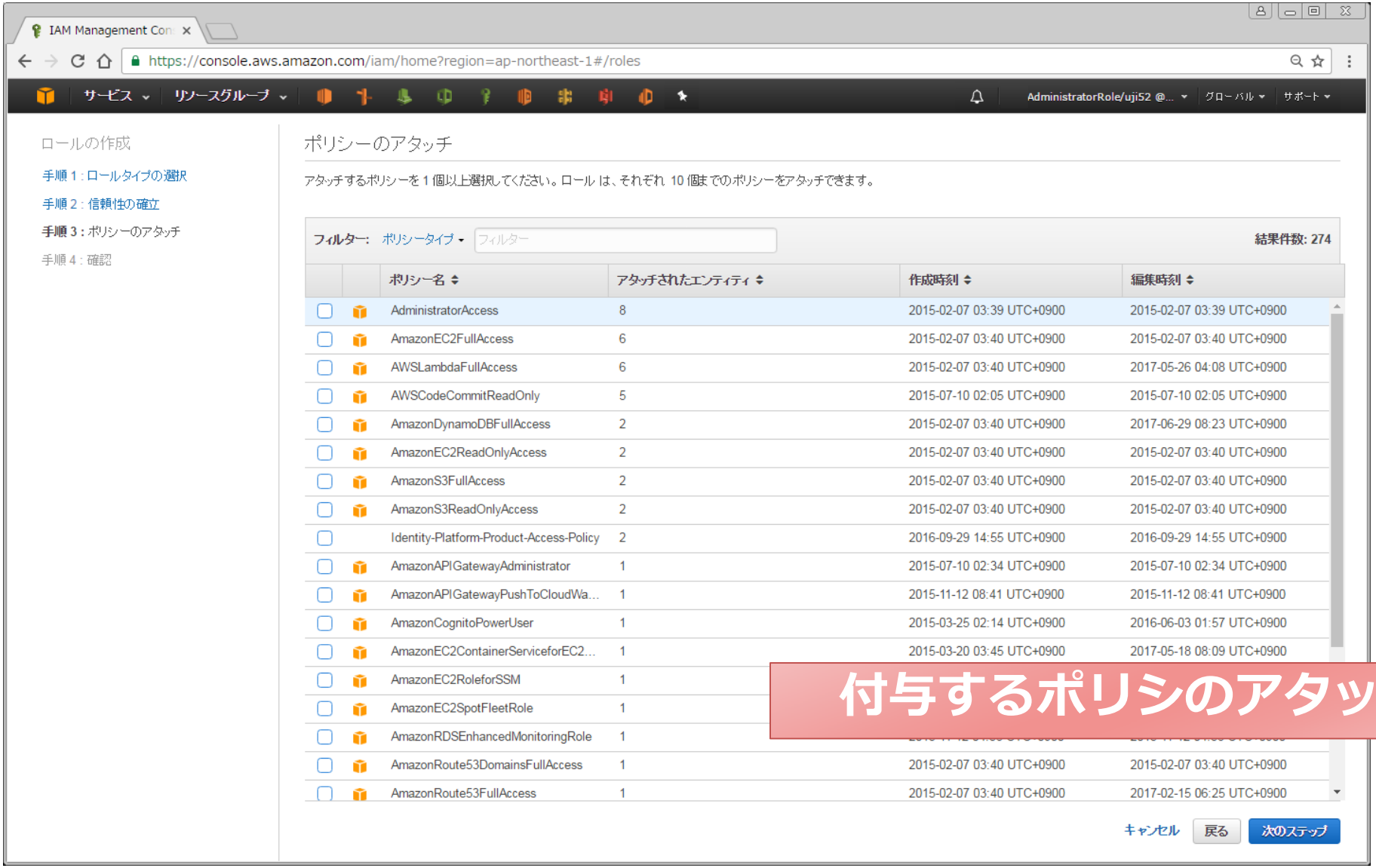


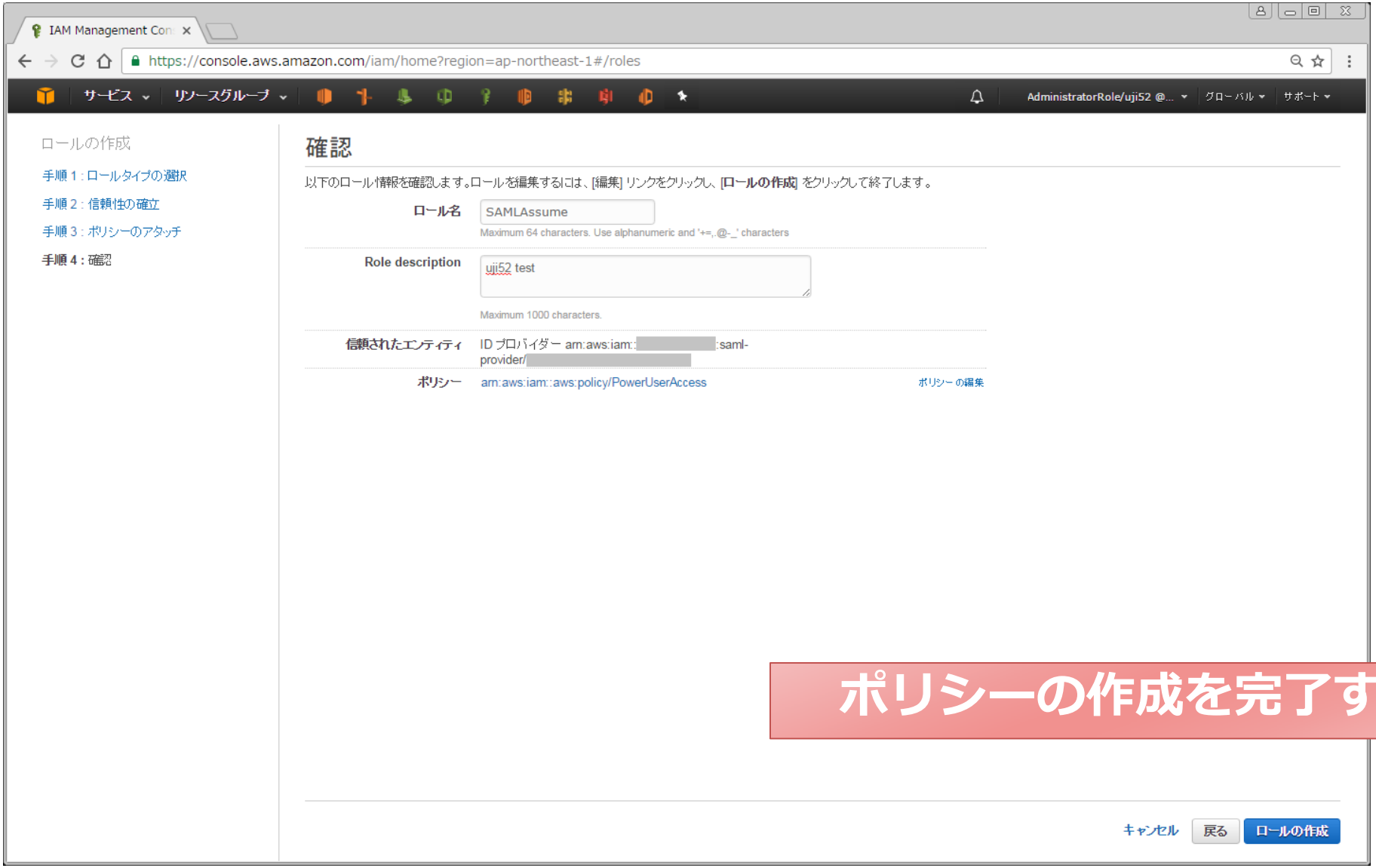

IAM Management Con
https://console.aws.amazon.com/iam/home?region=ap-northeast-1#/home
サービス
リソースグループ
AdministratorRole/uji52 @...
グローバル
サポート
IAM の検索
ダッシュボード
グループ
ユーザー
ロール
ポリシー
ID プロバイダー
アカウント設定
認証情報レポート
暗号化キー
Identity and Access Management へようこそ
IAM ユーザーのサインインリンク:
https://[redacted].signin.aws.amazon.com/console
カスタマイズ | リンクのコピー
IAM リソース
ユーザー: 53
ロール: 88
グループ: 11
ID プロバイダ: 3
カスタマー管理ポリシー: 12
セキュリティステータス
4 項目中 4 項目が完了しています。
ルートアカウントの MFA を有効化
個々の IAM ユーザーの作成
グループを使用してアクセス許可を割り当て
IAM パスワードポリシーの適用
注目の機能
Introduction to AWS IAM
0:00 / 2:16
追加情報
IAM ベストプラクティス
IAM ドキュメント
Web ID フェデレーションのプレイグラウンド
Policy Simulator
動画、IAM リリース履歴、および追加のリソース
フィードバック
日本語
© 2008 - 2017, Amazon Web Services, Inc. or its affiliates. All rights reserved.
プライバシーポリシー
利用規約







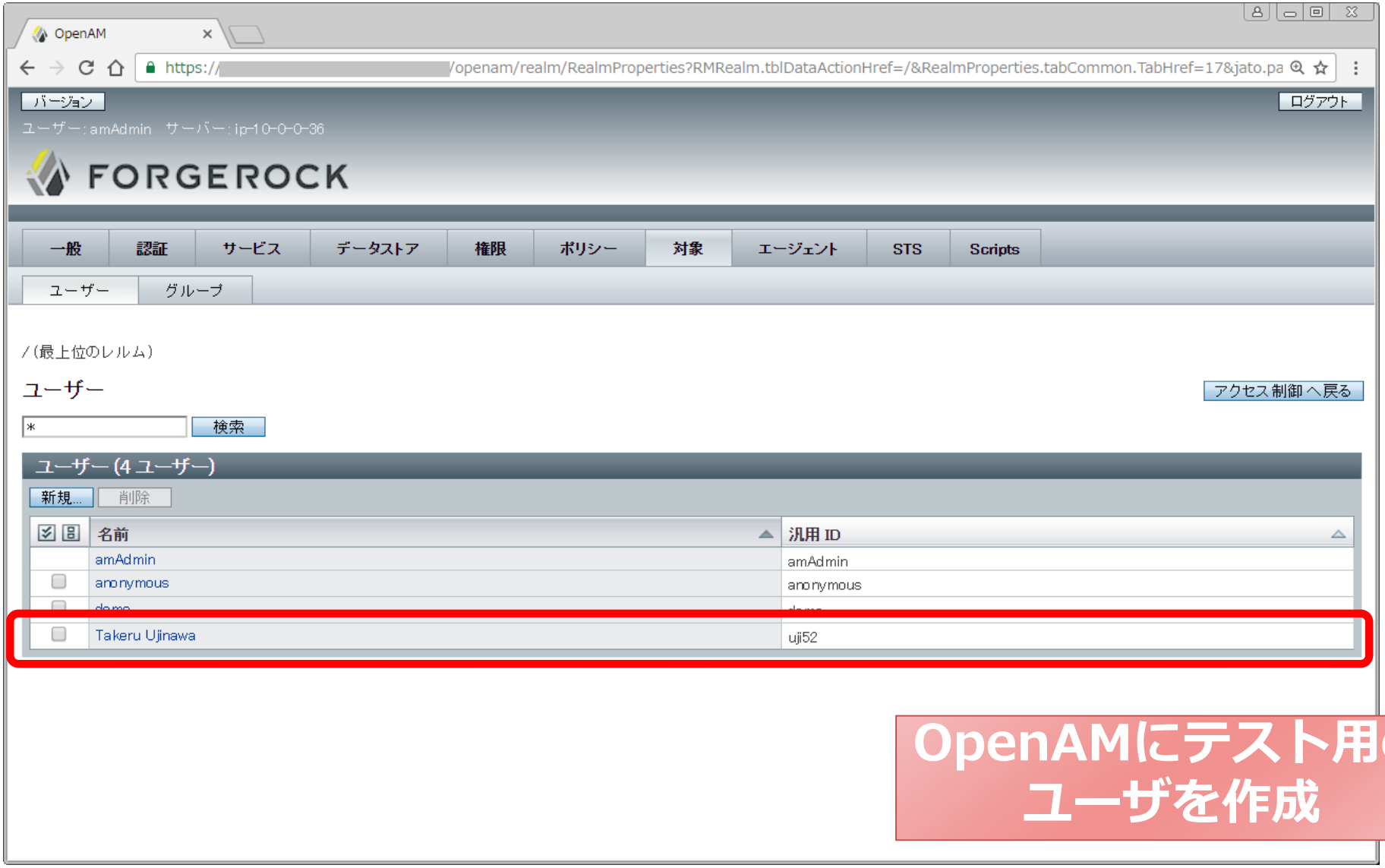




ポリシーの作成を完了する

設定の流れ

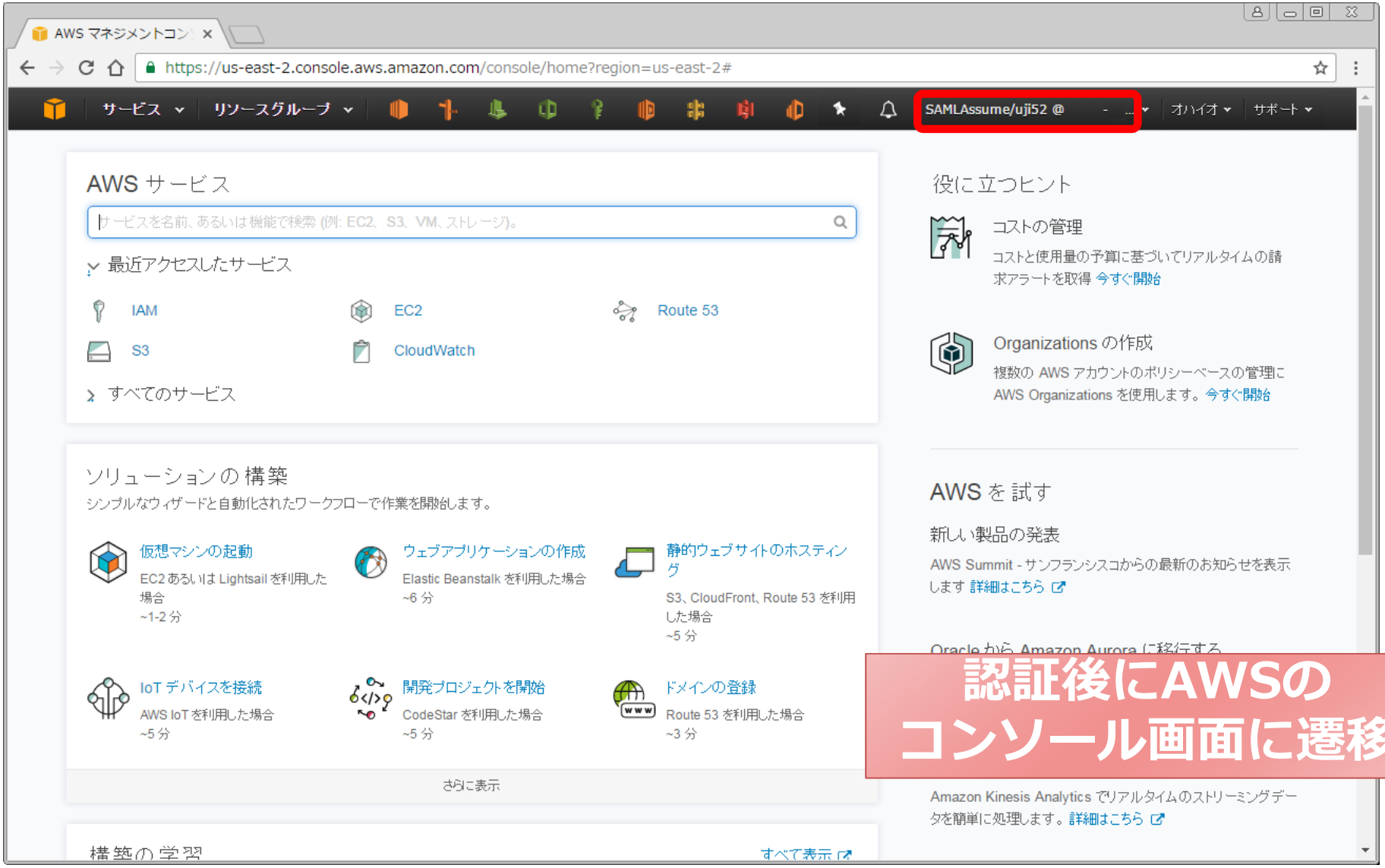
- ☑SAML IdPを構成する
  - ➢OpenAMをSAML IdPとして構成する
- ☑SAML IdP, SPのメタデータを取得する
  - ➢OpenAMのIdPメタデータを取得
  - ➢AWSのSPメタデータを取得
- ☑互いに相手の設定を行う
  - ➢OpenAMにSAML SP(AWS)を登録する
  - ➢AWSにSAML IdP(OpenAM)を登録する

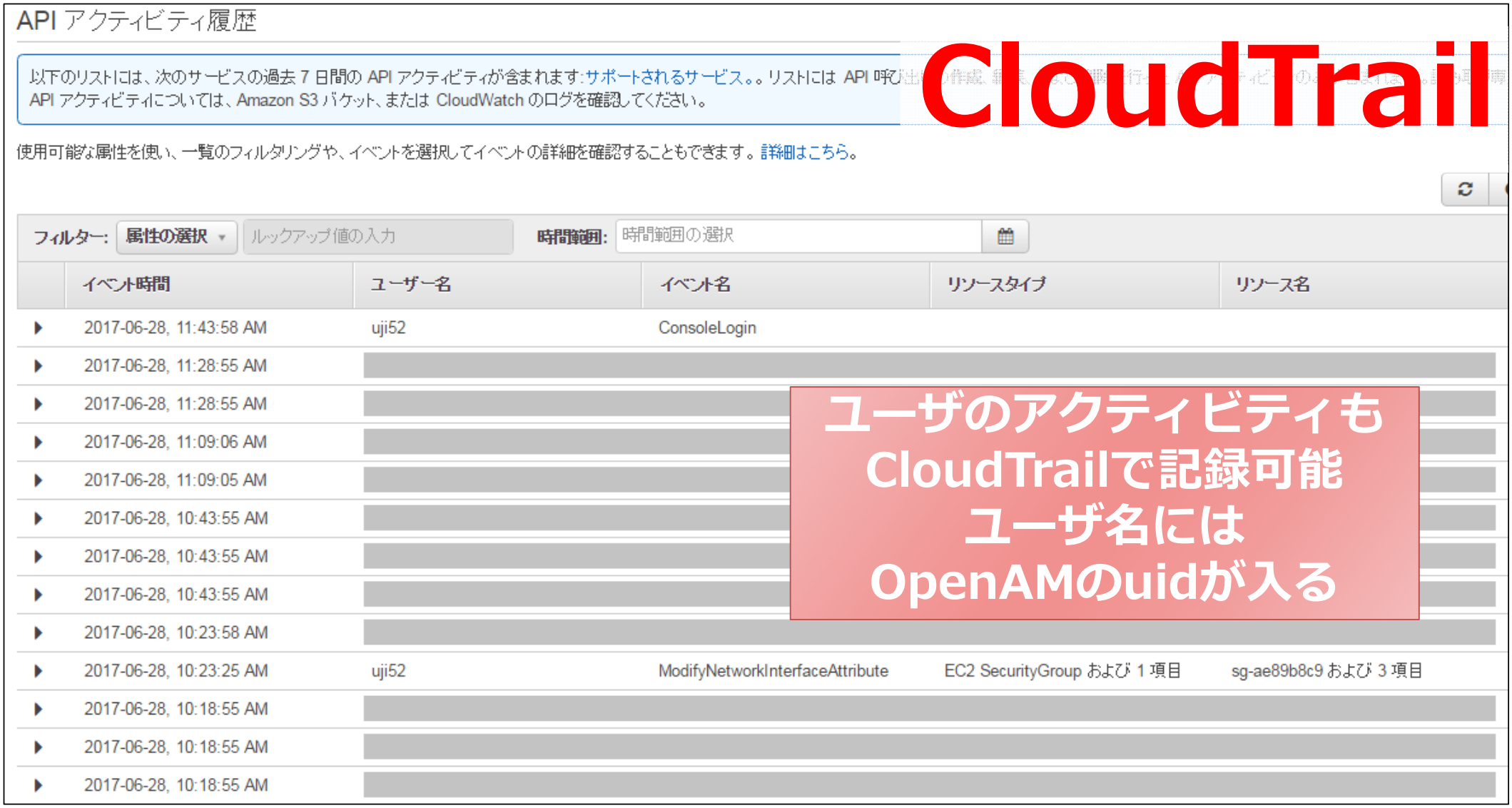


テストに使うユーザを作成
住所の属性にAWSのロール名を追加
(LDAP上に新たに定義した属性に差し込むのがベスト)

これで設定完了
OpenAMがSAML IdP
AWSがSAML SPになった

https://xxxxxxxxxx/openam/idpssoinit?metaAlias=/idp&spEntityID=urn:amazon:webservices

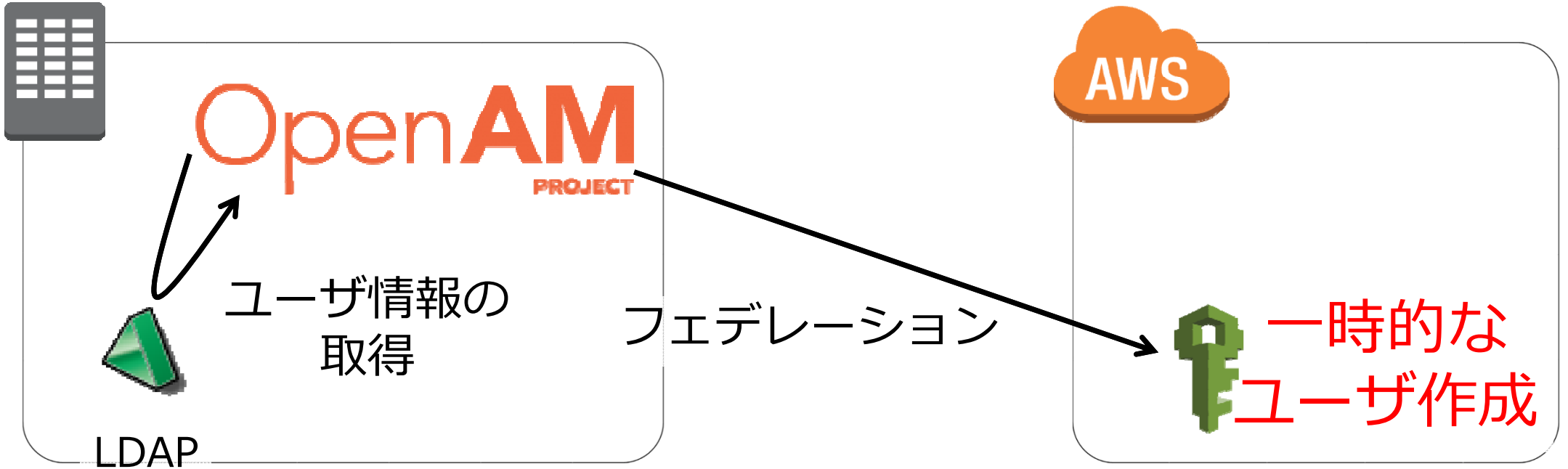




もっと細かい情報を元に
割り当てられるロールを判断し
最初のロールを与えたい

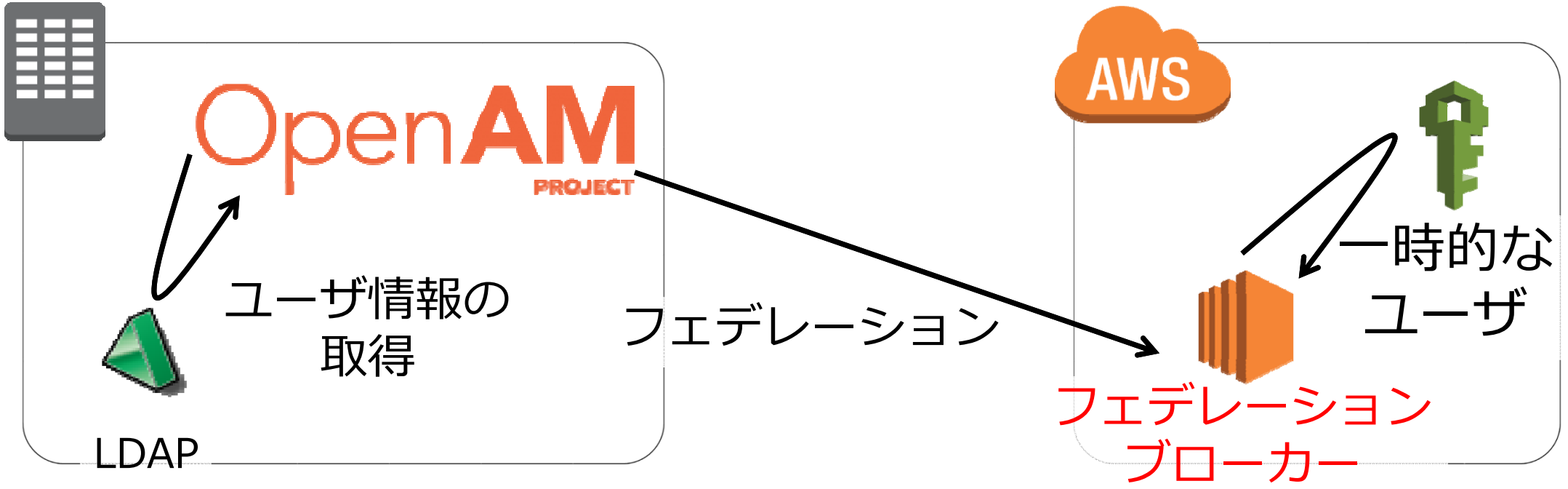
STS (Security Token Service)のAssumeRoleWithSAML

- 一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供



STS (Security Token Service)のAssumeRole

- 一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供



フェデレーションで渡る情報(SAML)


```xml
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
        ID="s2f01e008563013ee4043c33de620d7bb6c064f0a3"
        Version="2.0"
        IssueInstant="2017-07-04T09:28:17Z"
        Destination="https://signin.aws.amazon.com/saml">
 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  https://openam.demo.themistruct.com:443/openam
 </saml:Issuer>
 <samlp:Status xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <samlp:StatusCode xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
          Value="urn:oasis:names:tc:SAML:2.0:status:Success">
  </samlp:StatusCode>
 </samlp:Status>
 <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
         ID="s2f4af5fea34dafd4f098102dd07951d40832e2200"
         IssueInstant="2017-07-04T09:28:17Z"
         Version="2.0">
  <saml:Issuer>
   https://openam.demo.themistruct.com:443/openam
  </saml:Issuer>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="#s2f4af5fea34dafd4f098102dd07951d40832e2200">
     <ds:Transforms>
     <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
    </ds:Transforms>
    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
    <ds:DigestValue>
     nqlTXRSmseaMQu9/22W8vH5Ipk0=
    </ds:DigestValue>
   </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
   Mh9XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXkvG
   JsFXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX3jj
   O9LXXXXXXXXXXXXXXXXX=
  </ds:SignatureValue>
  <ds:KeyInfo>
   <ds:X509Data>
    <ds:X509Certificate>
     MIIXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXkNh
     bGlXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX09w
     ZW5XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXQsw
     CQYXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXDAK
     BgNXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXw0B
     AQEXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXOf+
     RkDXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXJNY
     Js0XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXw/U
     QzPXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXiDA
     cGyXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXJDC
     /FfXXXXXXXXXXX==
    </ds:X509Certificate>
   </ds:X509Data>
  </ds:KeyInfo>
 </ds:Signature>
 <saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
         NameQualifier="https://xxxxxxxxxxxxxxxxx:443/openam"
         SPNameQualifier="urn:amazon:webservices">
   6EubdGBN8rgKS27r6YC/zP9stl5U
  </saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
   <saml:SubjectConfirmationData NotOnOrAfter="2017-07-04T09:38:17Z"
                Recipient="https://signin.aws.amazon.com/saml"/>
   </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2017-07-04T09:18:17Z" NotOnOrAfter="2017-07-04T09:38:17Z">
   <saml:AudienceRestriction>
    <saml:Audience>
     urn:amazon:webservices
    </saml:Audience>
   </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement AuthnInstant="2017-07-04T09:24:38Z"
            SessionIndex="s28d49f5aa82b83dc41b6ebeb2cd49c1495e357601">
   <saml:AuthnContext>
    <saml:AuthnContextClassRef>
     urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
    </saml:AuthnContextClassRef>
   </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
   <saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/RoleSessionName">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="xs:string">
     uji52
    </saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/Role">
    <saml:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
             xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
             xsi:type="xs:string">
     arn:aws:iam::xxxxxxxxxxxx:role/SAMLAssume,arn:aws:iam::xxxxxxxxxxxx:saml-provider/xxxxxxxxxxxxxxxxx
    </saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
 </saml:Assertion>
</samlp:Response>
```


全100行

拡大

```xml
 <saml:AttributeStatement>
     <saml:Attribute
Name="https://aws.amazon.com/SAML/Attributes
/RoleSessionName">
        <saml:AttributeValue>
          uji52
        </saml:AttributeValue>
```

必要な属性の抽出がやや面倒

フェデレーションで渡る情報(OpenID Connect)

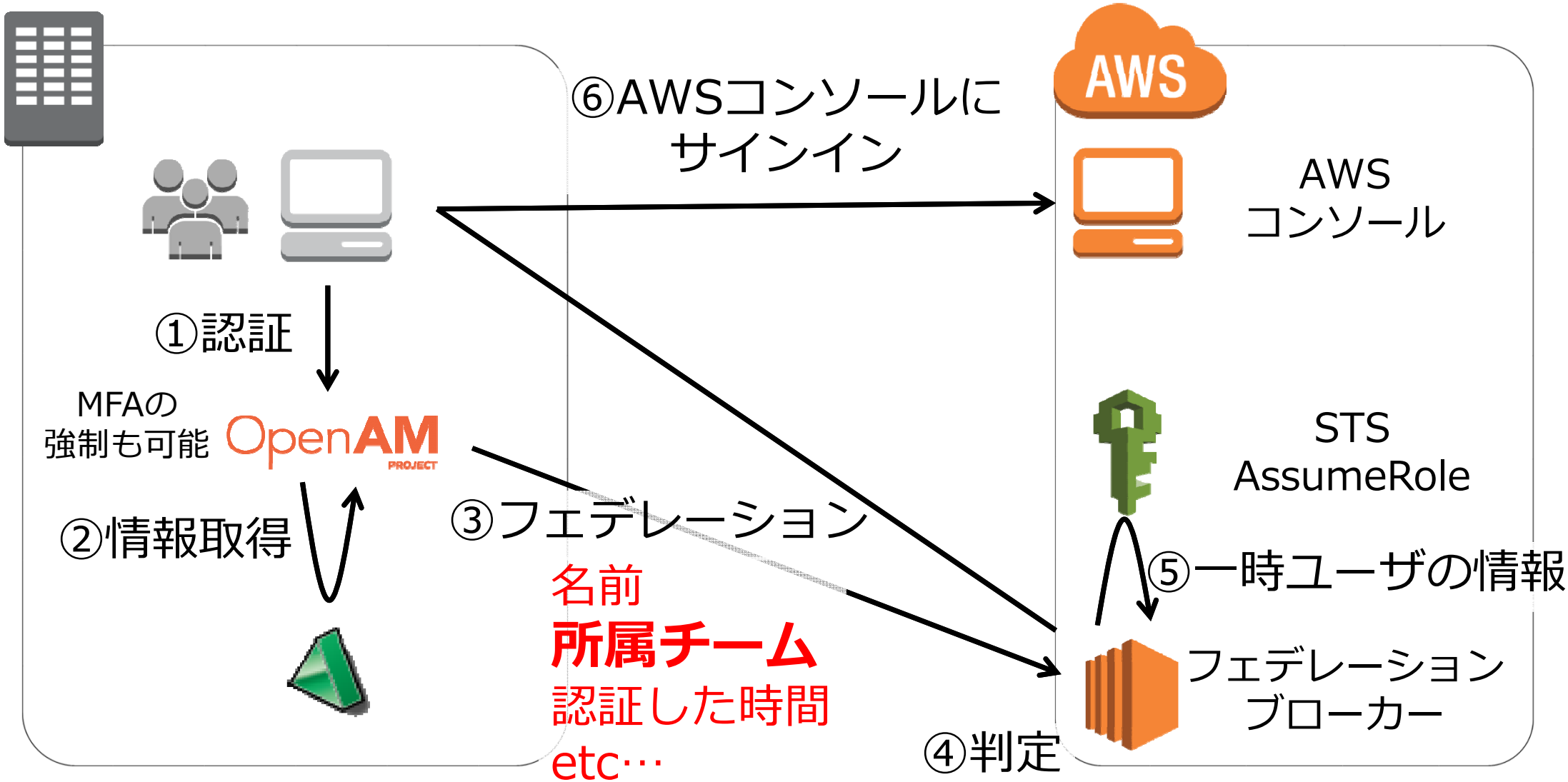
JSON形式で
必要な属性の抽出が
非常に簡単


```
{
  "iss": "http://server.example.com",
  "sub": "uji52",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970
}
```

OpenID Conectなら
認証情報の属性ベースで
権限のハンドリングがやり易い


OpenAM
https://openam.demo.themistruct.com/openam/XUI/?realm=%2F&goto=https%3A%2F%2Fopena
FORGEROCK
OPENAM へのサインイン
ユーザー名
パスワード


OpenAM
https://openam.demo.themistruct.com/openam/XUI/?realm=%2F&goto=https%3A%2F%2Fopena
FORGEROCK
OPENAM へのサインイン
ユーザー名
パスワード



アカウント管理上の課題

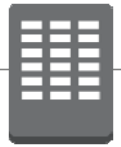
- ☑ユーザの不満 (不便！)
  - 追加が遅れると不便だ
  - MFA有効化が面倒だ
  - そもそも認証するのが面倒だ
- ☑管理者の不満 (面倒！リスク！)
  - 手作業が多い
  - MFAを強制できない
  - 作業を忘れたら企業に打撃を与える可能性がある

アカウント管理から開放された！

アジェンダ

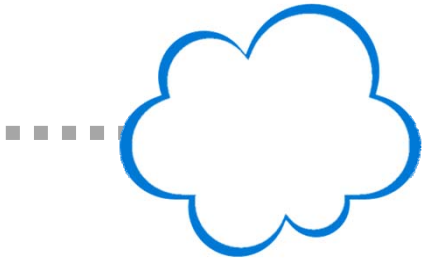
- AWSアカウント管理の苦労
- OpenAMとは
  - 認証連携方式
  - OpenAMをセットアップして使ってみる
- フェデレーションでアカウント管理効率UP
  - SAMLによるフェデレーション
  - OpenID Connectによるフェデレーション
- フェデレーション技術と今後ID管理について

ユーザーの属性情報を使ったコントロール



OpenAM PROJECT

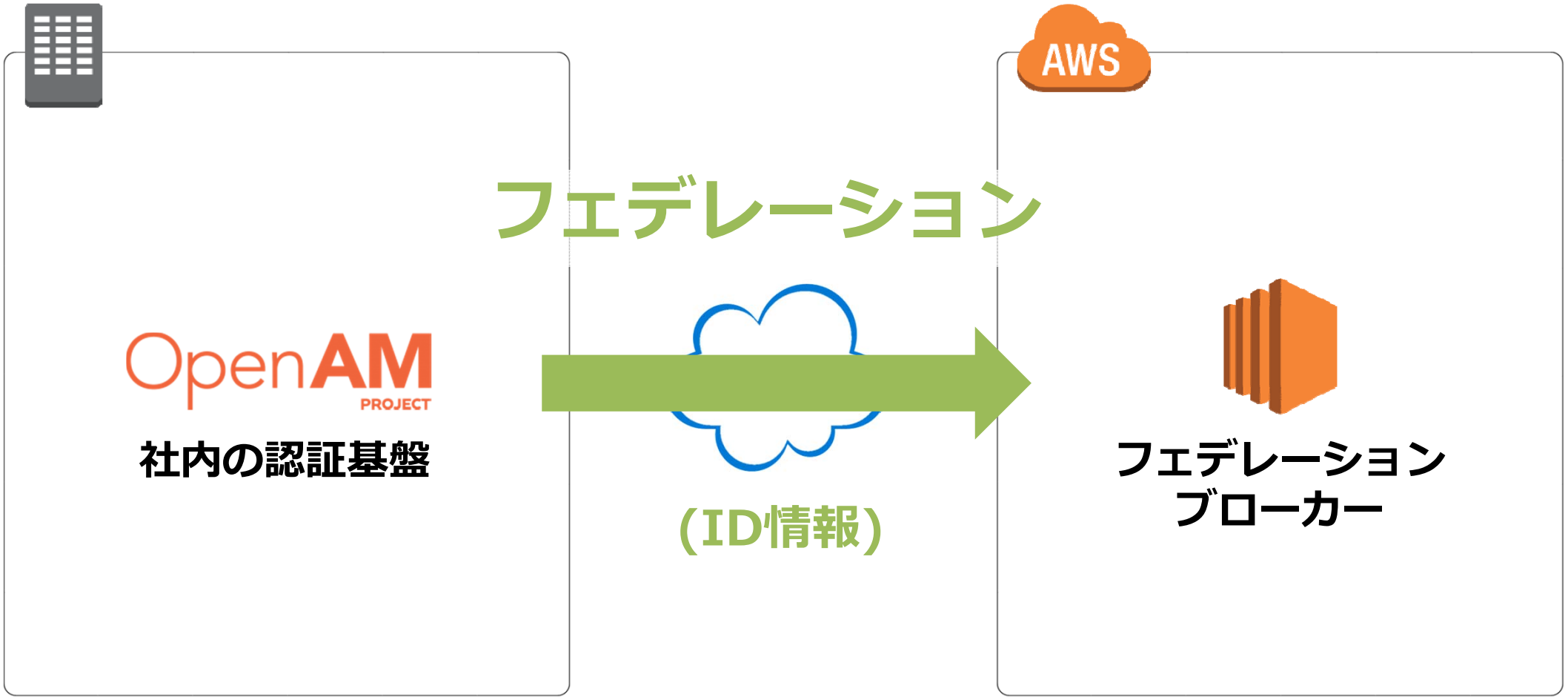
社内の認証基盤



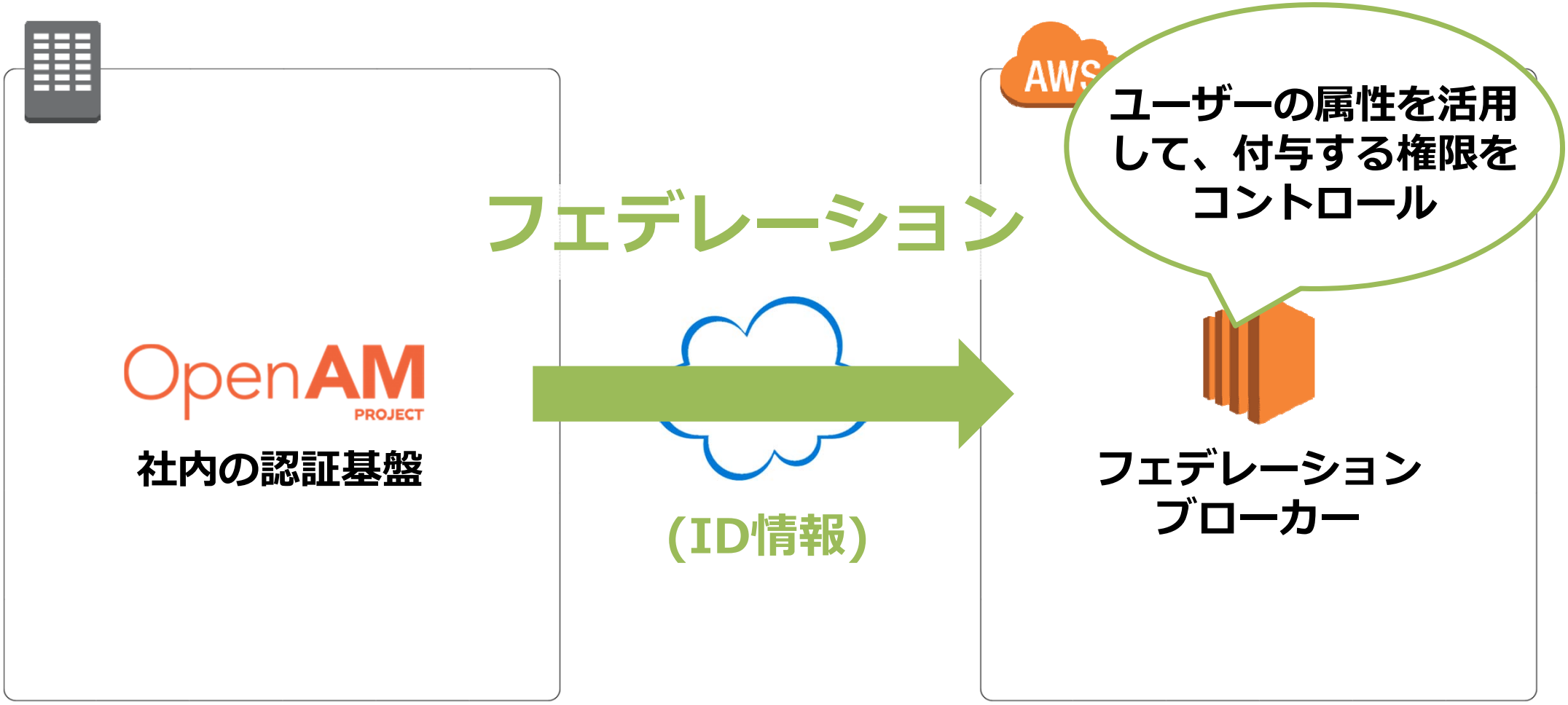
AWS

フェデレーション
ブローカー

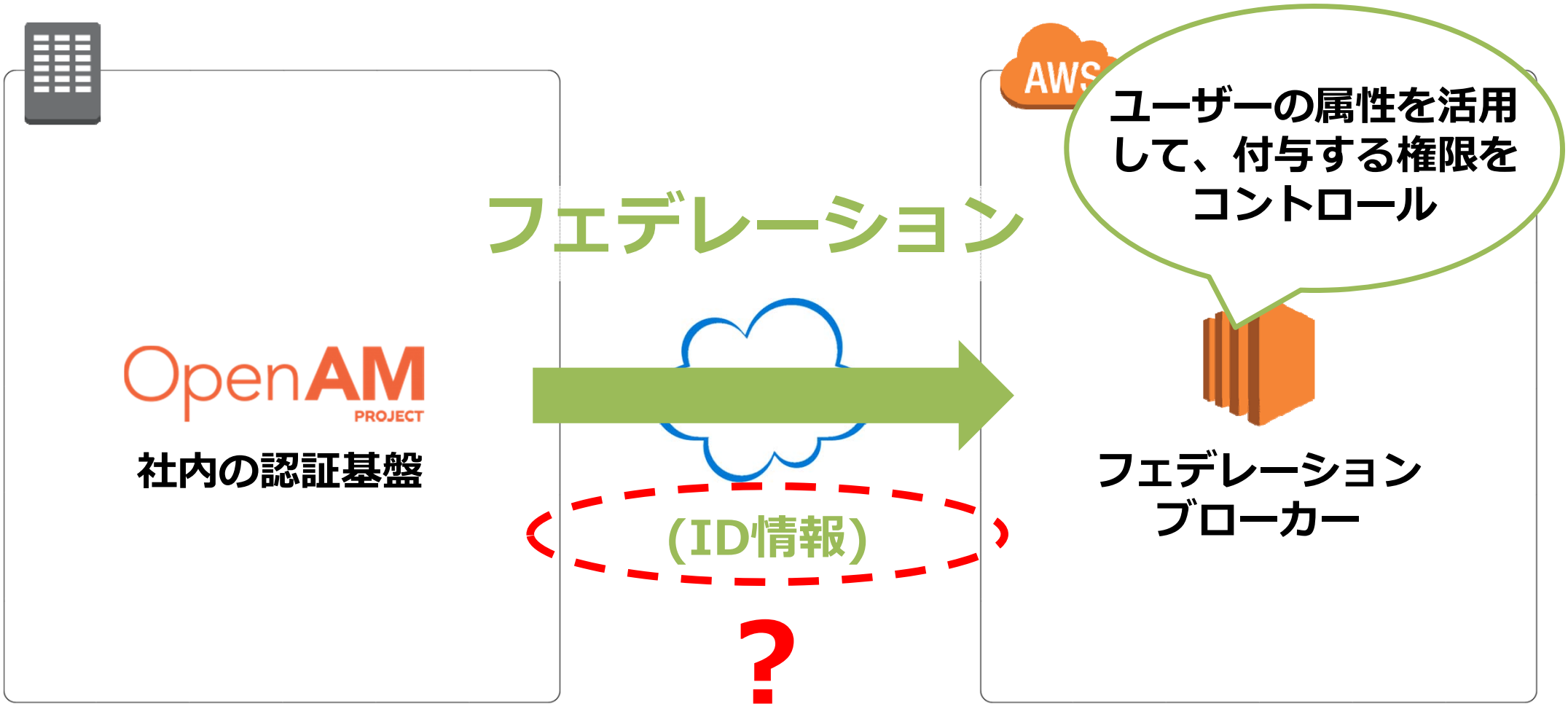
ユーザーの属性情報を使ったコントロール



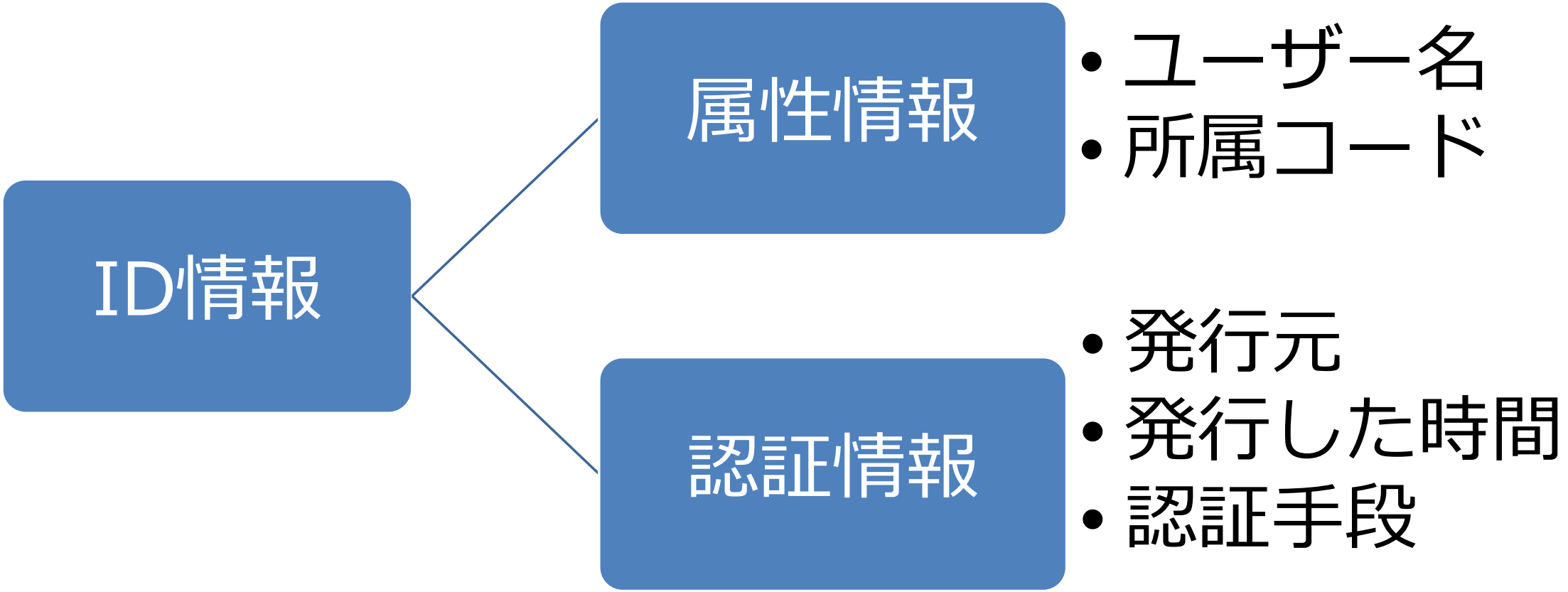
ユーザーの属性情報を使ったコントロール



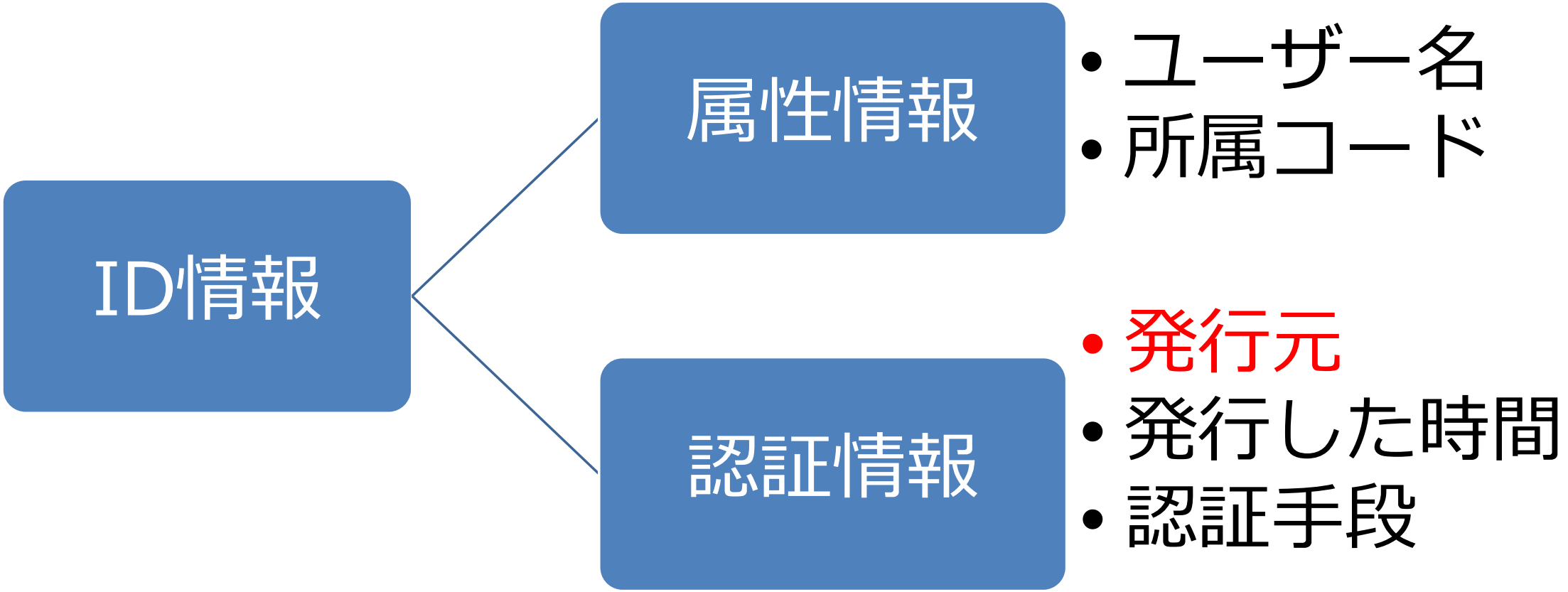
ユーザーの属性情報を使ったコントロール



フェデレーション技術で伝搬される情報

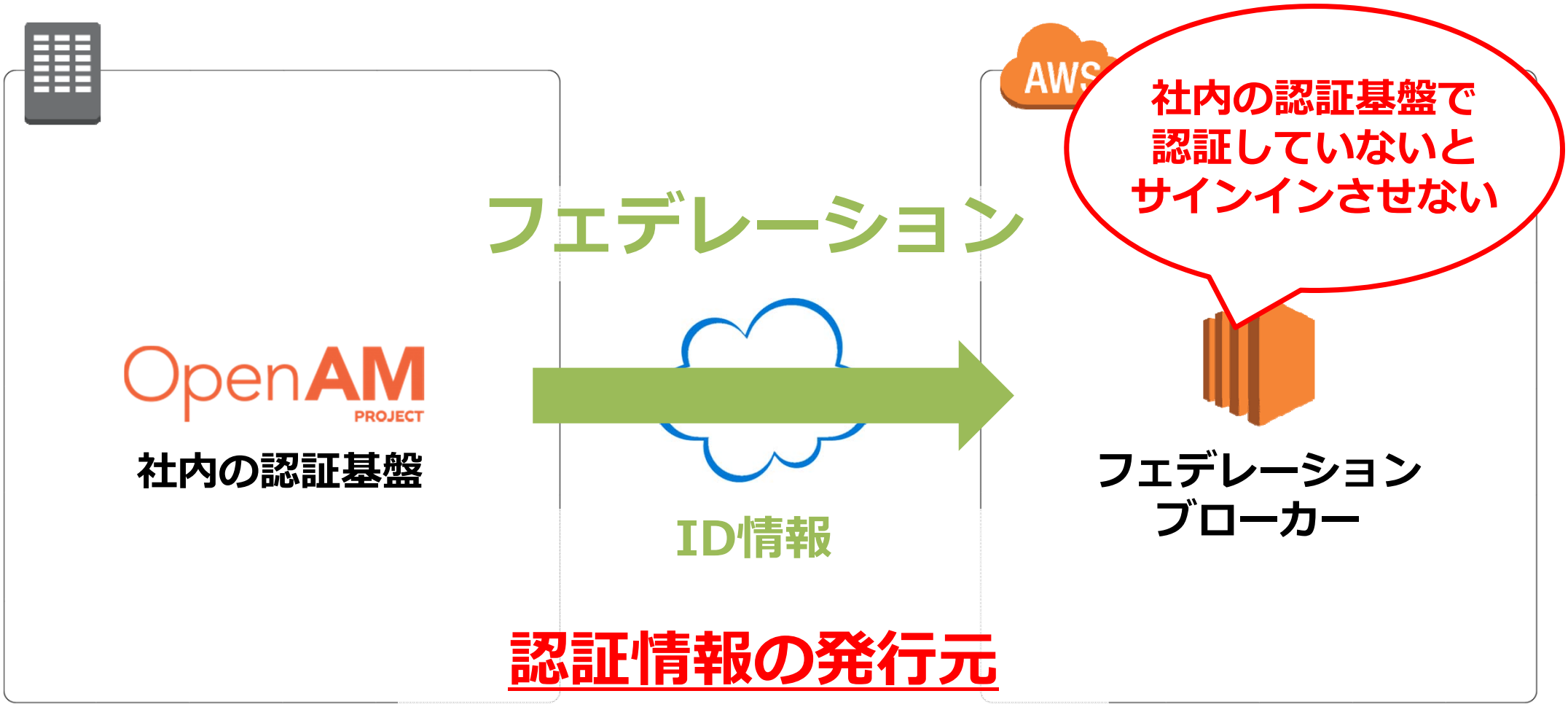


フェデレーション技術で伝搬される情報

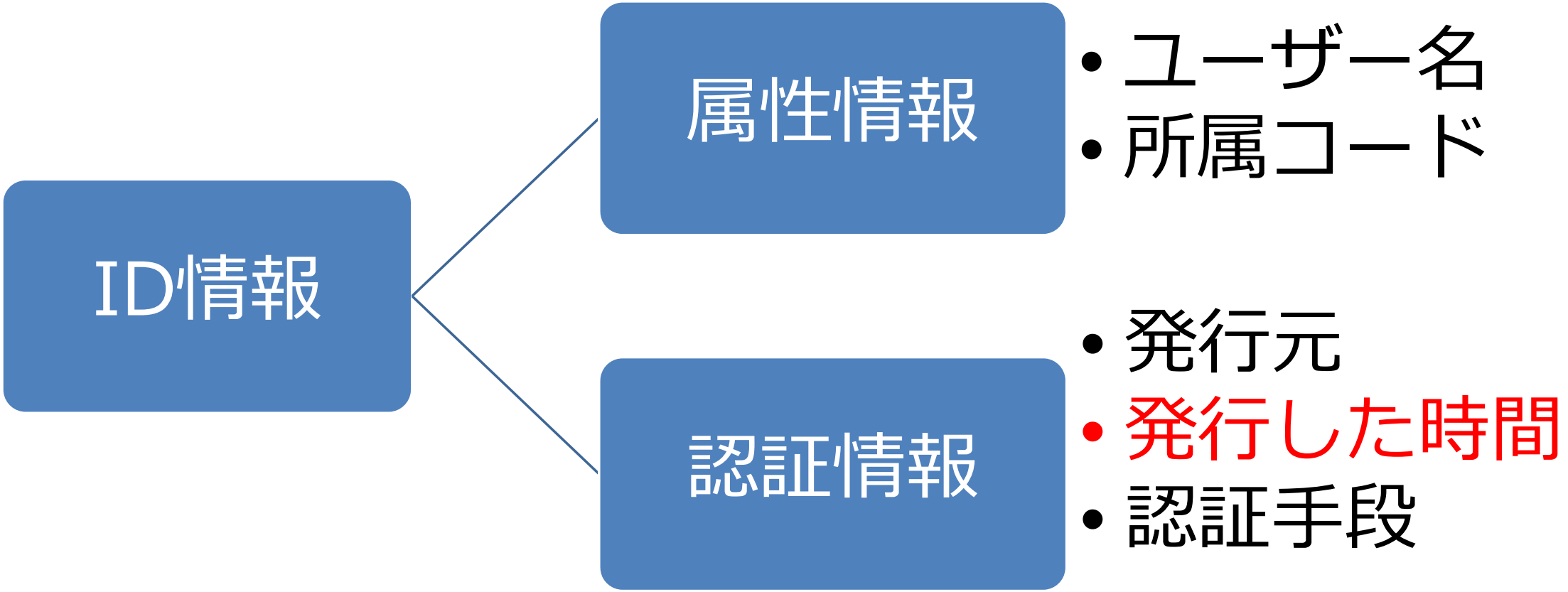


「認証情報の発行元 (issuer)」でコントロール

「認証情報の発行元 (issuer)」でコントロール

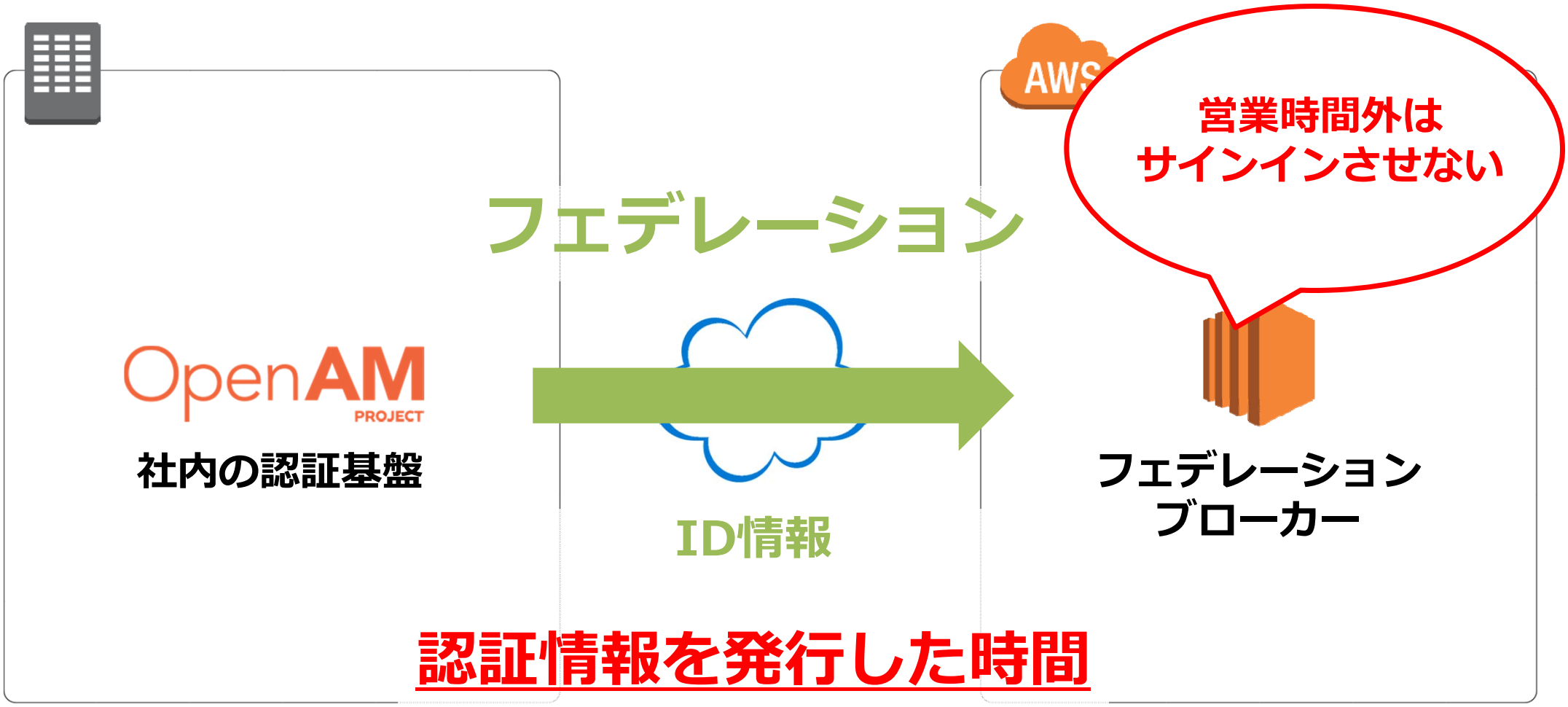


フェデレーション技術で伝搬される情報

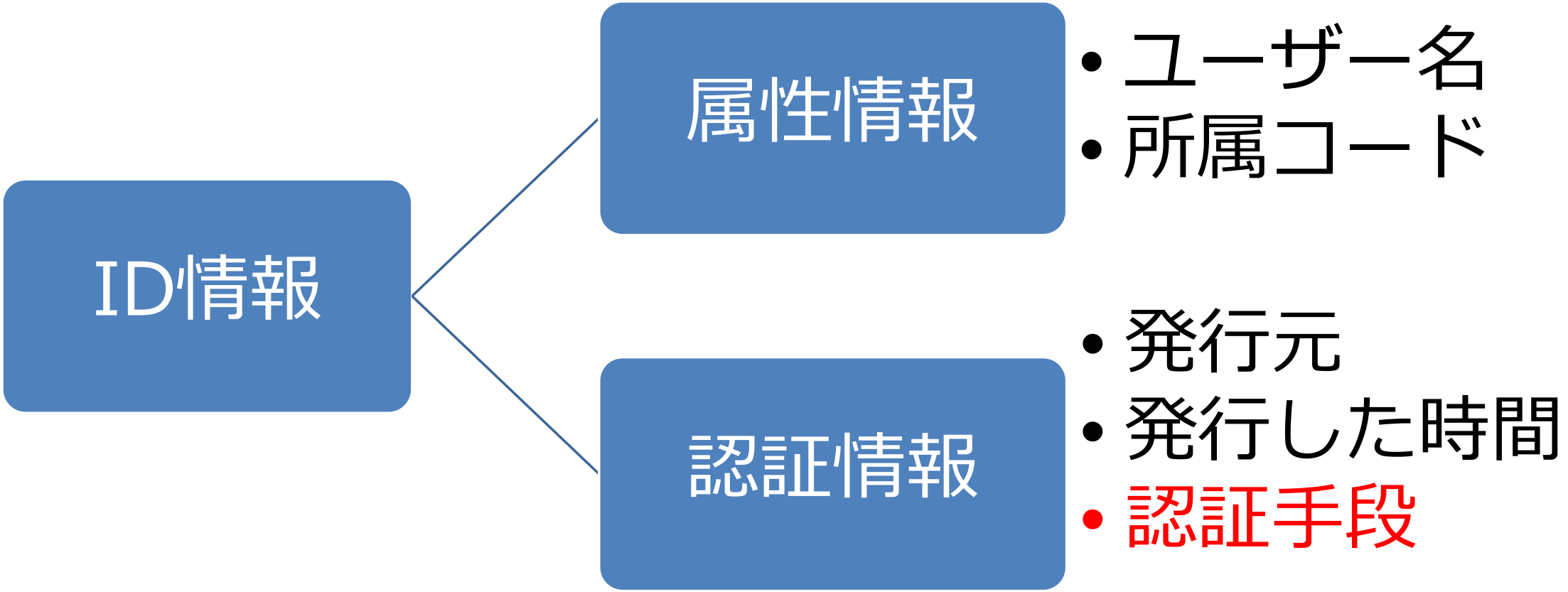


「認証情報を発行した時間 (iat)」でコントロール

「認証情報を発行した時間 (iat)」でコントロール

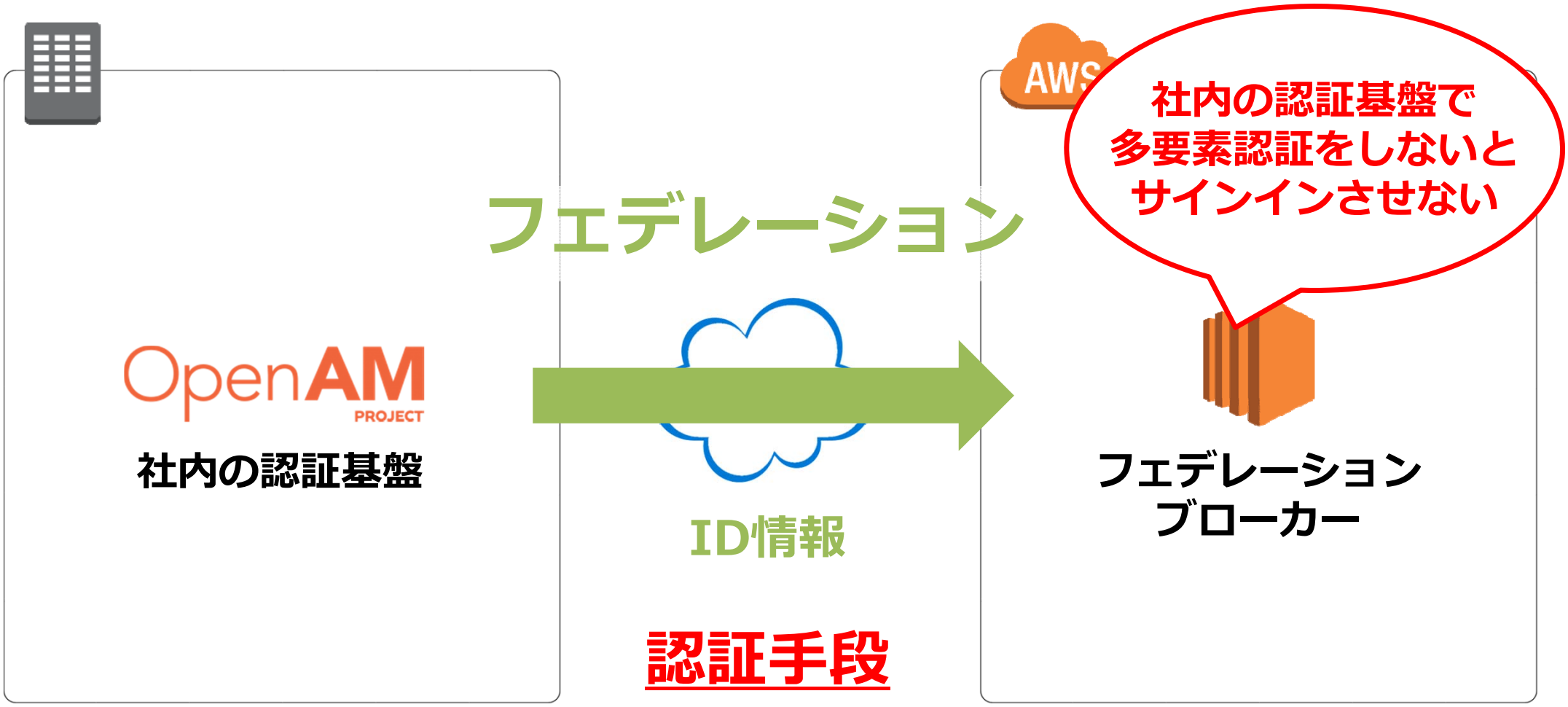


フェデレーション技術で伝搬される情報



「認証手段 (acrやamr)」でコントロール

「認証手段 (acrやamr)」でコントロール

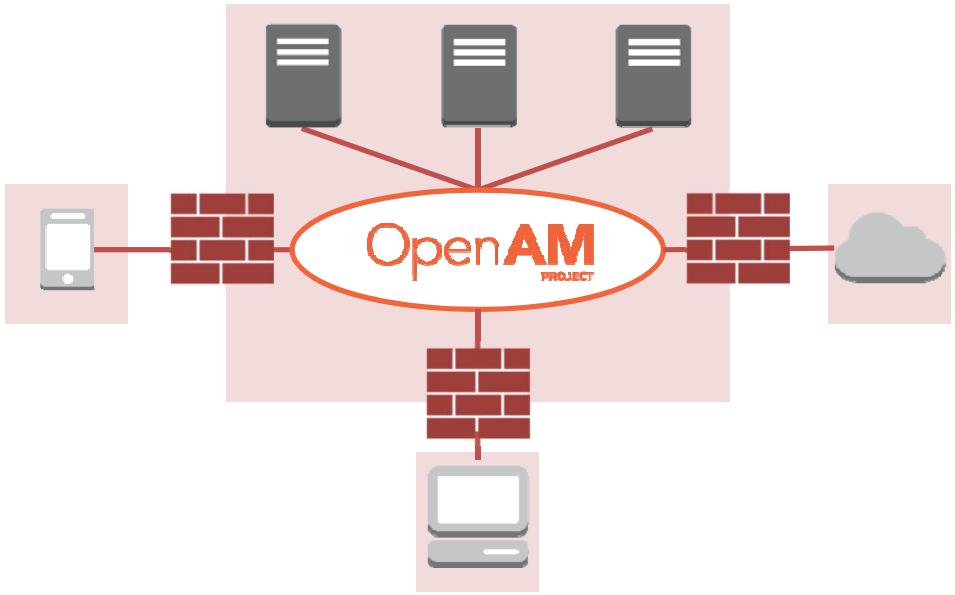


アイデンティティ情報を
システム間で連携できる

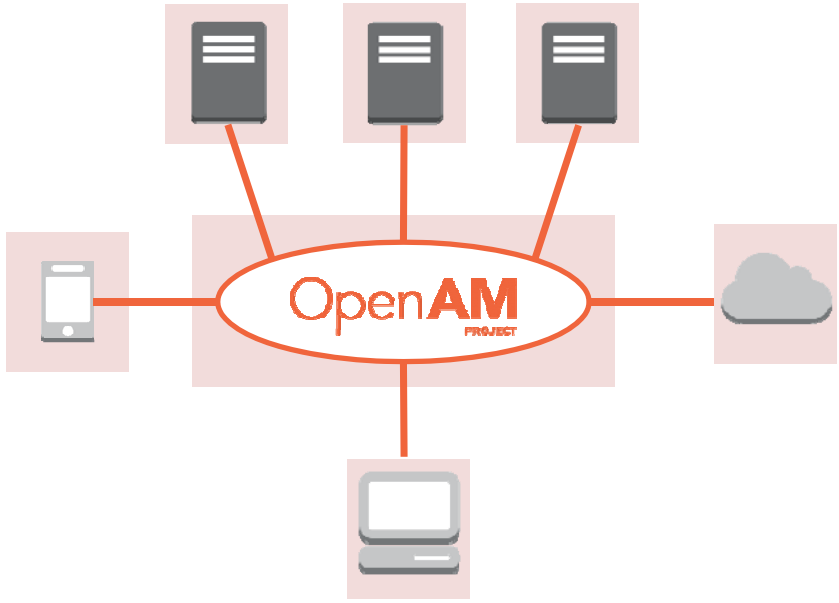
アイデンティティ情報で
セキュリティを実装できる

Identity Is the New Perimeter (ID業界話)

ネットワーク型の防御



アイデンティティ型の防御



おわりに

- 認証基盤 + フェデレーション + IAM
  - フェデレーションでアカウント管理の効率化
  - メンテナンス漏れによるインシデントを回避
- アイデンティティ
  - フェデレーションでセキュリティの実装ができる
  - Identity Is the New Perimeter

最後にちょっと宣伝

新しい統合認証プラットフォーム作ってます

ThemiStruct（テミストラクト）

Identity Platform AWS対応版

- ✓AWSのPaaS上で動くアイデンティティ連携基盤
- ✓≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓オージス総研自社商品

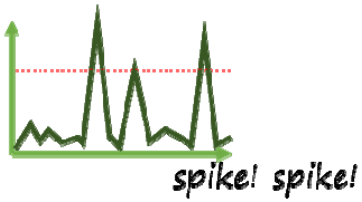
「非機能要求」のレベルがアップ

膨大なトラフィック

- 認証基盤の役割増加
- 提供するサービス・システムの増加
- ユーザー数・デバイス数の増加
- API利用の増加

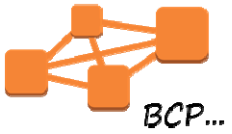
スパイクアクセス

- キャンペーンやニュースサイト掲載などにより定常的なアクセスと比較し、予想不可な大量のアクセスが発生する



システム停止を回避

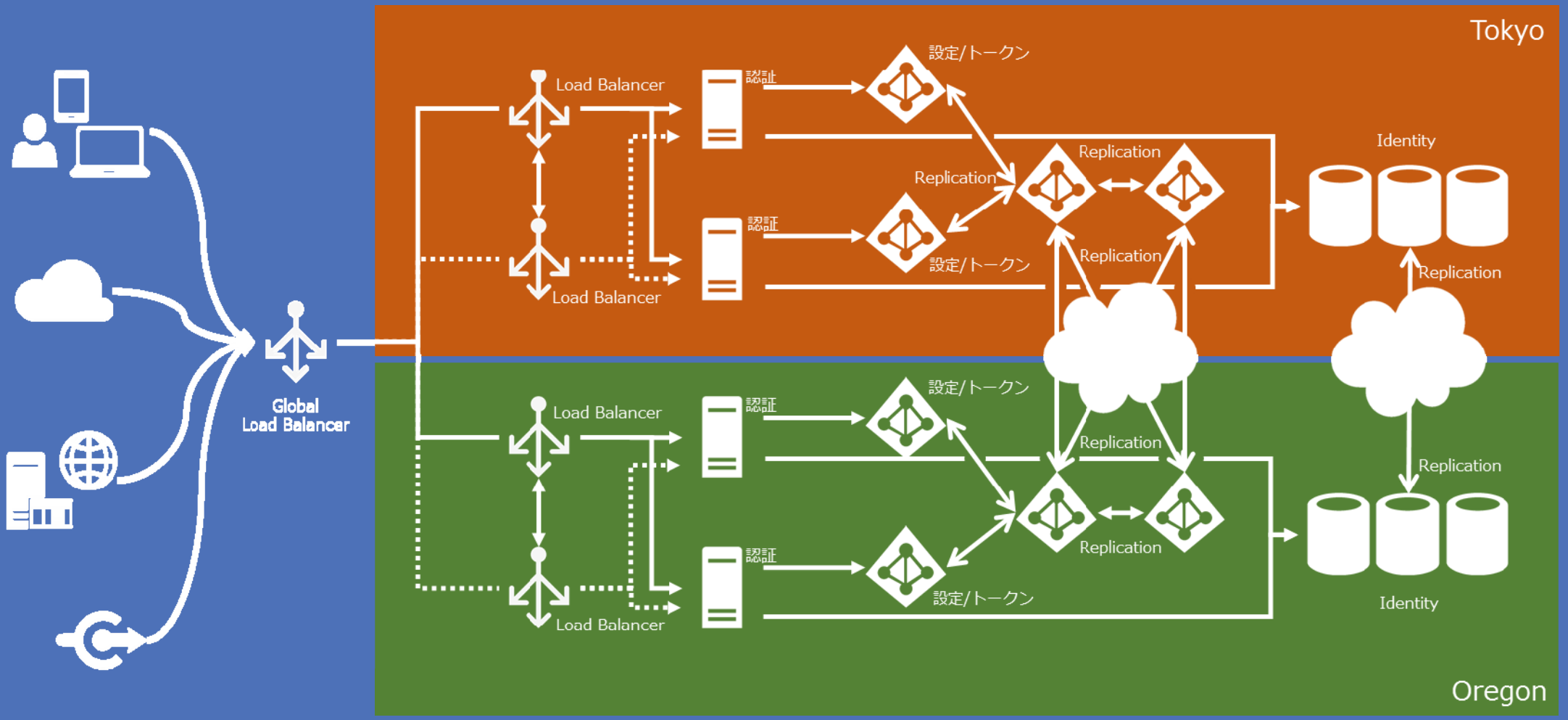
- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした



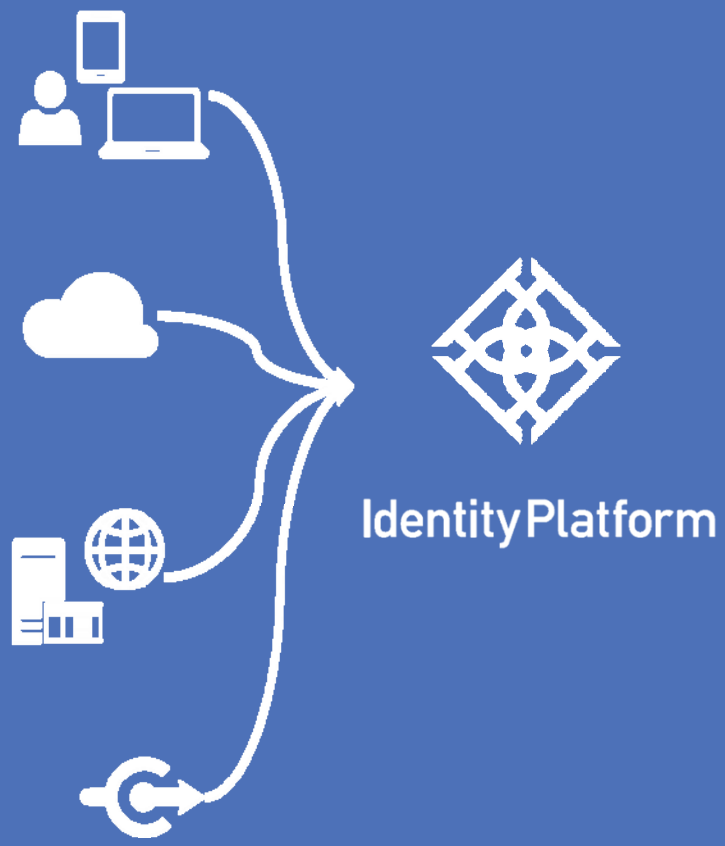
スピードスタート・スモールスタート

- 短期間でビジネスをスタートさせたり、事業規模に応じてスタート、柔軟にスケールできる必要がある

これまで： 高度な基盤設計。入念な可用性、性能のテスト。プロジェクトの巨大化。



これから： 基盤の設計、テストは不要。プロジェクトの迅速なスタートアップ。



OpenID Certified になりました。

ThemiStruct テミストラクト
Identity Platform AWS 対応版

オージス総研の ThemiStruct Identity Platform は OpenID Connect™ プロトコルの OP Basic, OP Implicit, OP Config の3つのプロファイルに適合した OpenID Certified™ 実装です。

http://openid.net/certification/

オブジェクトの広場は株式会社オージス総研グループのエンジニアによる技術発表サイトです

分野別記事　Books　About us

クラウド/Webサービス

OpenID Connectでつくる「アイデンティティ境界」

株式会社オージス総研
テミストラクトソリューション部
千野 修平, 氏縄 武尊

長年、組織領域とインターネット領域の境界で高価なセキュリティ製品を配備し、脅威から資産を守る手法が、世の中のデファクトスタンダードとして、多くの企業で採用されてきました。しかし、「モバイルデバイスの活用」、「クラウドサービス利用の浸透」、「ワークスタイルの変革」などのリクエス

Links

ご清聴ありがとうございました

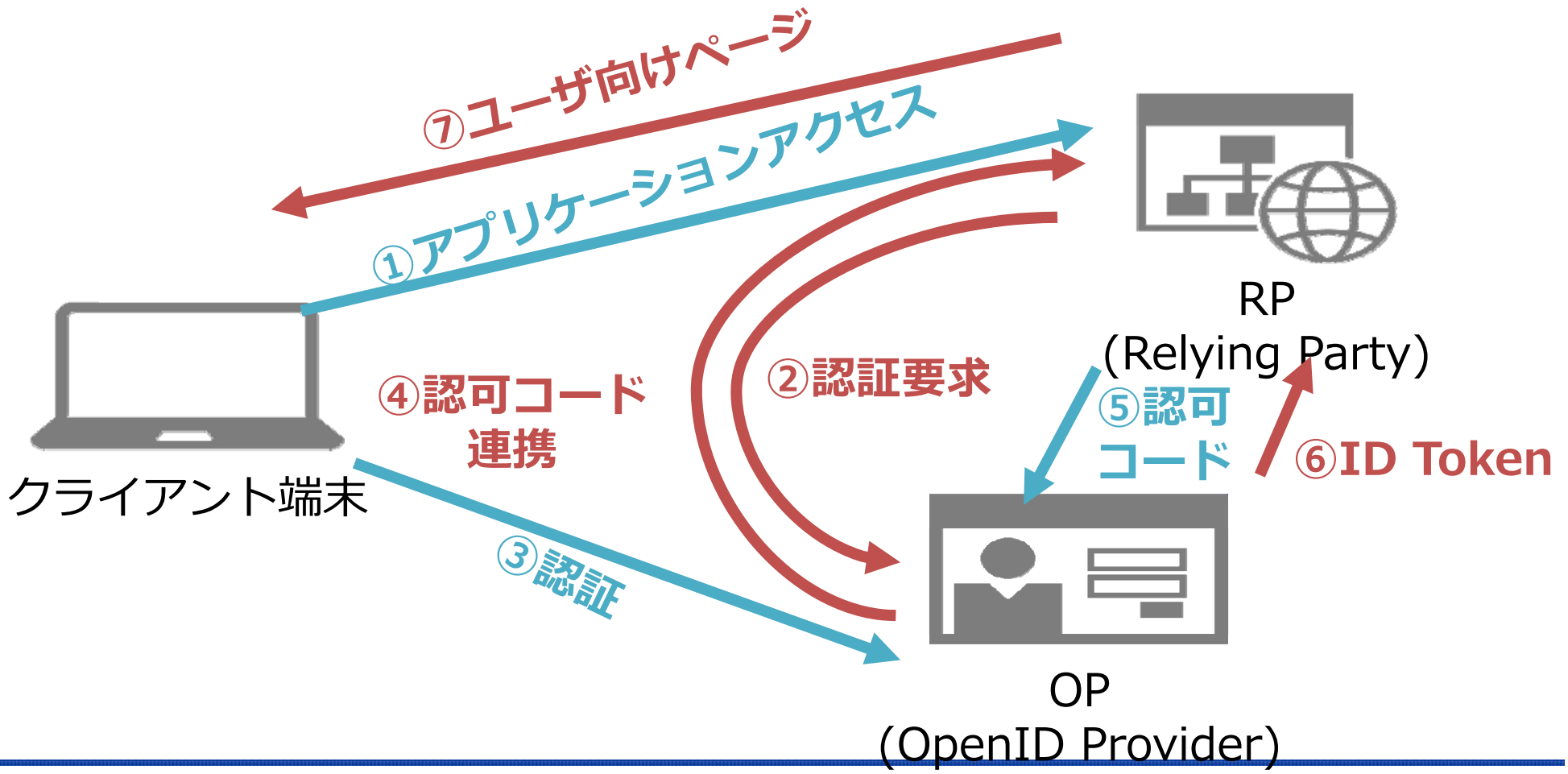
ThemiStruct
テミストラクト

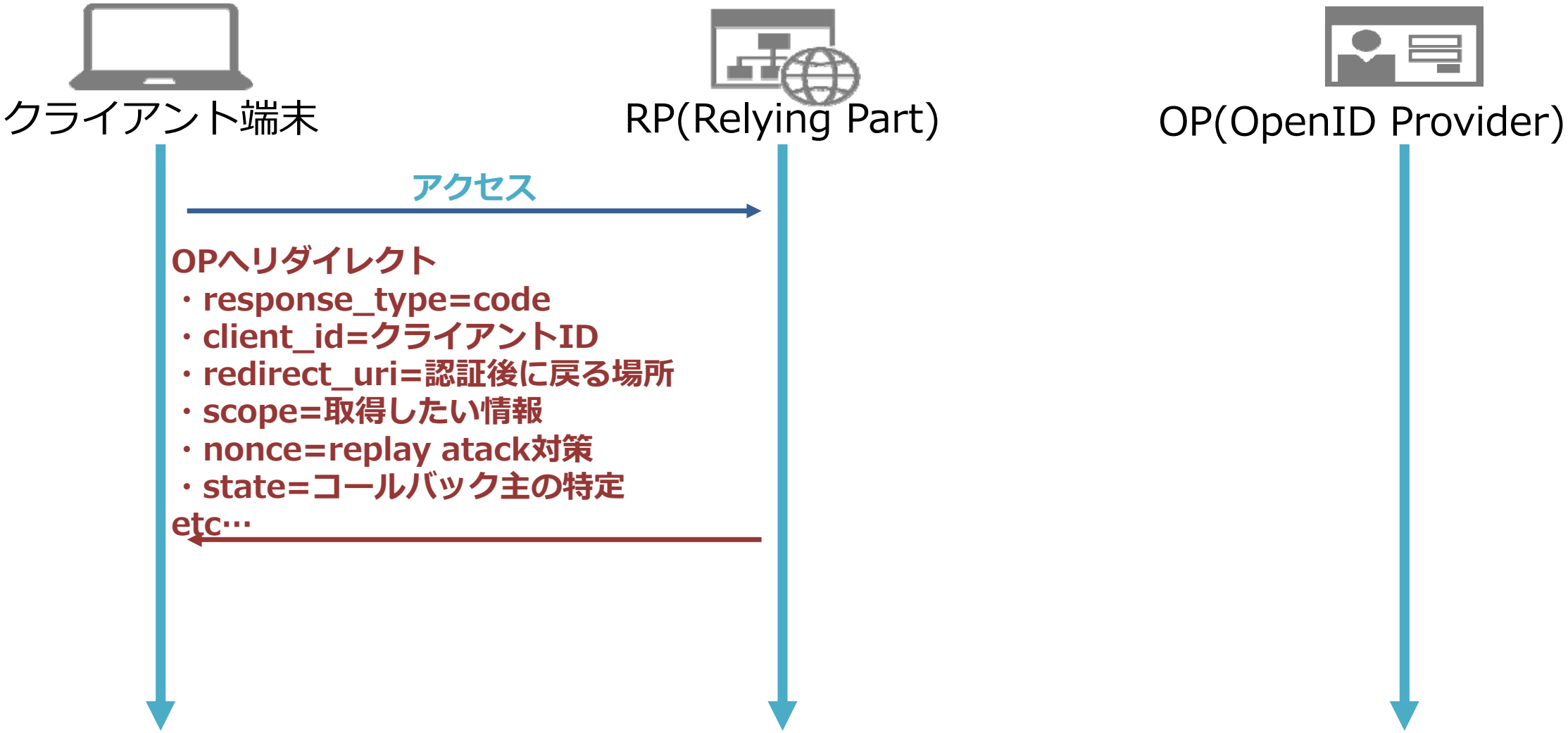
【お問い合わせ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-7998
mail: info@ogis-ri.co.jp

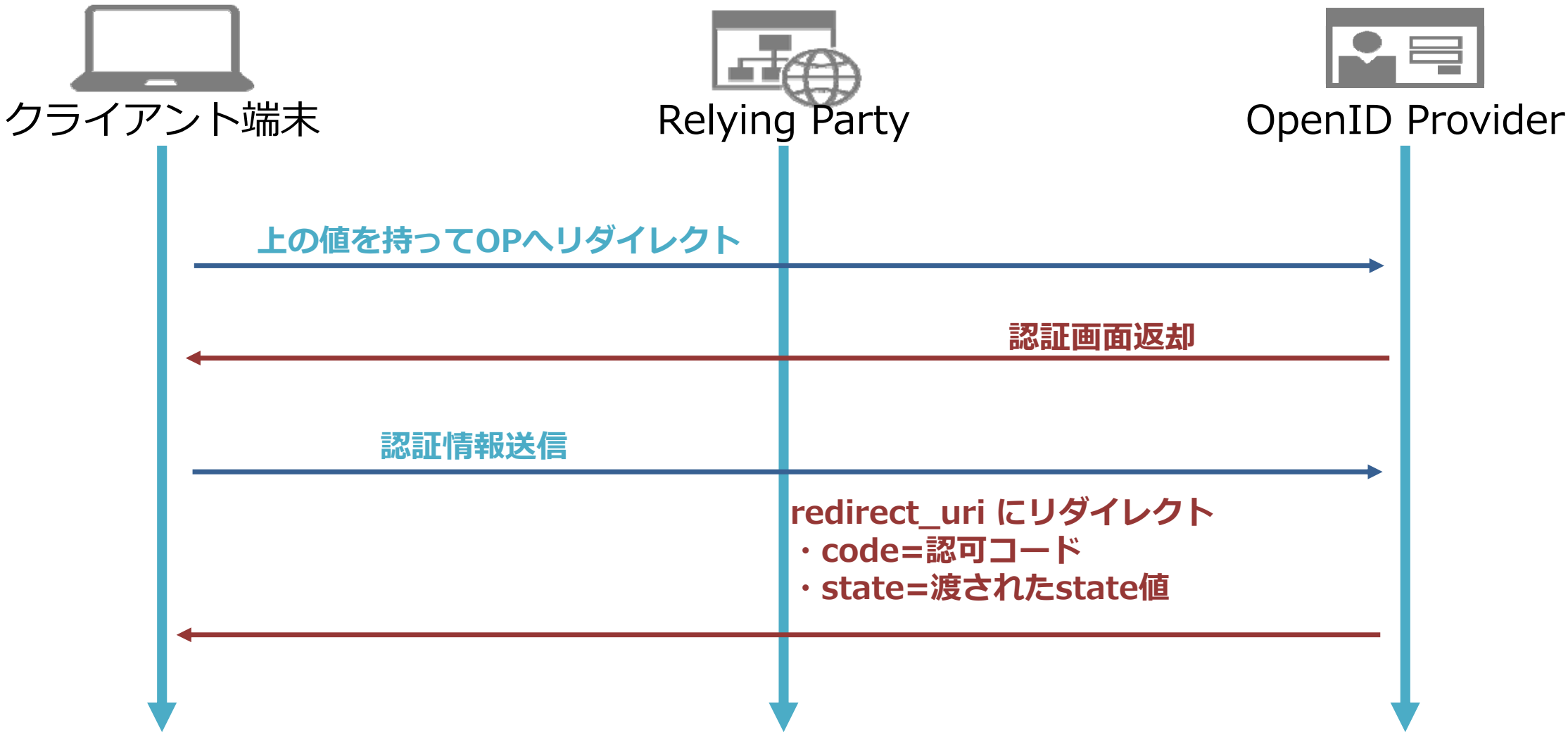
OGIS-RI

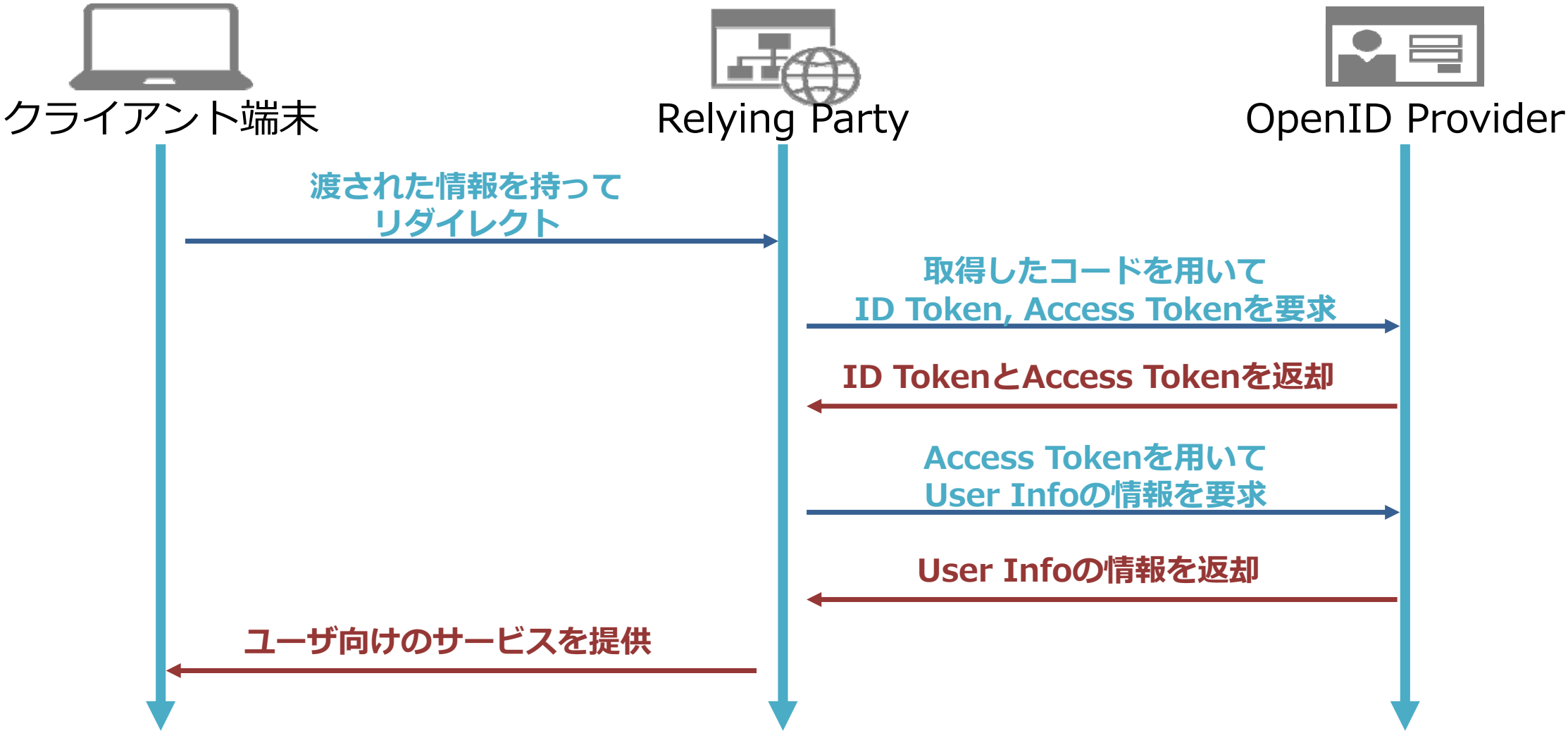
フロー補足

Code Flow









認証情報の正体（OpenID ConnectのID Token）

eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdWIiOiJ1amk1MiIsImF
1ZCI6ImNsaWVudF9pZCIsImlzcyI6Imh0dHA6Ly9vcC5leGFtcGxlLmNvb
SIsImV4cCI6IjE0Mzk5NDYzNjAiLCJub25jZSI6IkFCQ0QxMjM0IiwiaWF0
IjoiMTQzOTk0NjAwMCJ9.S2GTMObgH956hjE6Pf7LEL1+CyiobH8tVIm
vxsVqx1fAZkFNZGP4aVv5jjNj2Ldwt/LoGJs8Er0YZSfKPWI1cdmEr+Nt
YeRyljbQvCRhg3T4aZpBfzBcwABj8DQxbv0uNuV0s4eHS0OMM7LVJn
Xk/kzdCeM/cwlzz0Vor0aYdAg=

ヘッダ.ペイロード.署名

JWT(JSON Web Token)形式

引用 http://openid.net/specs/openid-connect-core-1_0.html

ID Tokenの中身(例)

ヘッダ(署名に用いる情報)


```
{
  "typ":"JWT",
  "alg":"RS256"
}
```


→ eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9

＋

ペイロード(ID Tokenの情報)


```
{
  "sub":"uji52",
  "aud":"client_id",
  "iss":"http://op.example.com",
  "nonce":"ABCD1234",
  "iat":  "1439946000"
  "exp":"1439946360"
}
```


→

eyJzdWIiOiJ1amk1MiIsImF1ZCI6ImNsaWVudF9pZCIsImlzcyI6Imh0dHA6Ly9vcC5leGFtcGxlLmNvbSIsImV4cCI6IjE0Mzk5NDYzNjAiLCJub25jZSI6IkFCQ0QxMjM0IiwiaWF0IjoiMTQzOTk0NjAwMCJ9

↓ 署名

S2GTMObgH956hjE6Pf7LEL1+CyiobH8tVImvxsVqx1fAZkFNZGP4aVv5jjNj2Ldwt/LoGJs8Er0YZSfKPWI1cdmEr+NtYeRyljbQvCRhg3T4aZpBfzBcwABj8DQxbv0uNuV0s4eHS0OMM7LVJnXk/kzdCeM/cwlzz0Vor0aYdAg=