なぜOpenID Connectが必要となったのか
その歴史的背景

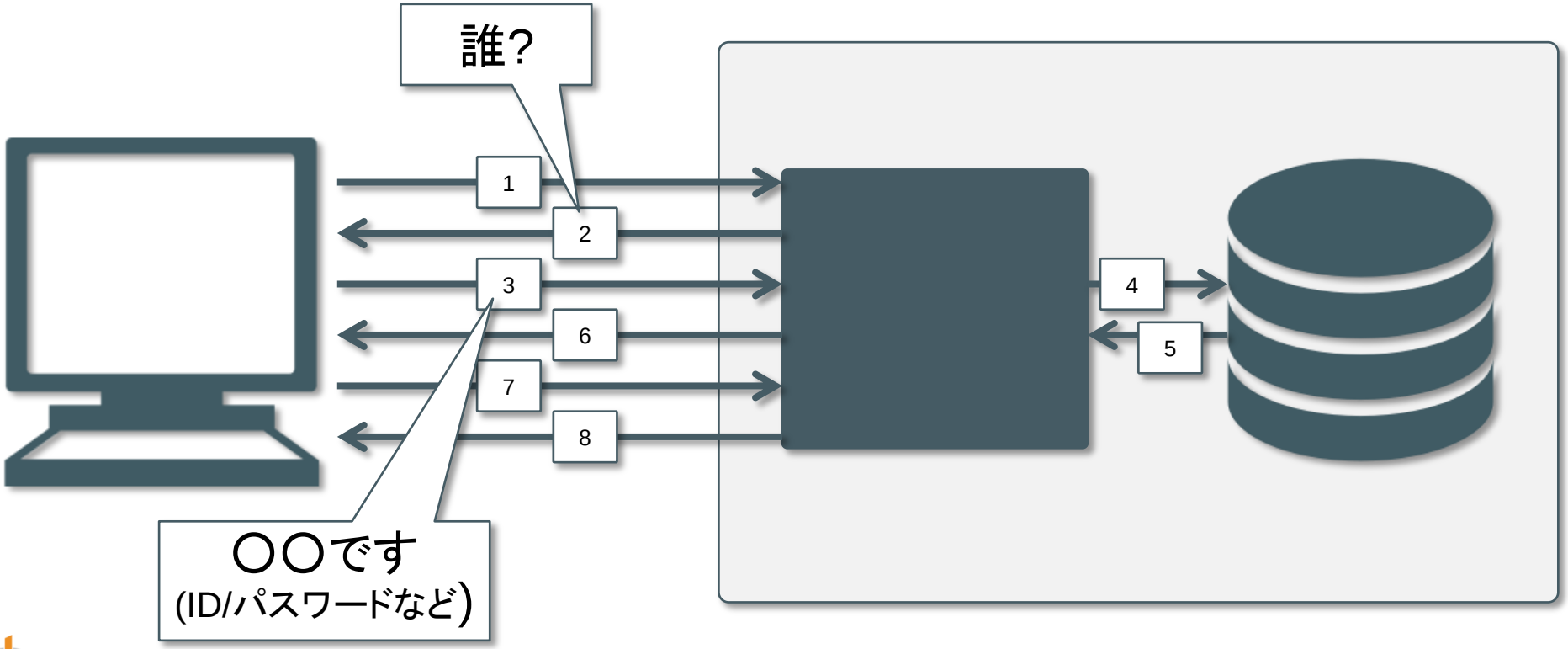
工藤達雄

OpenIDファウンデーション・ジャパン

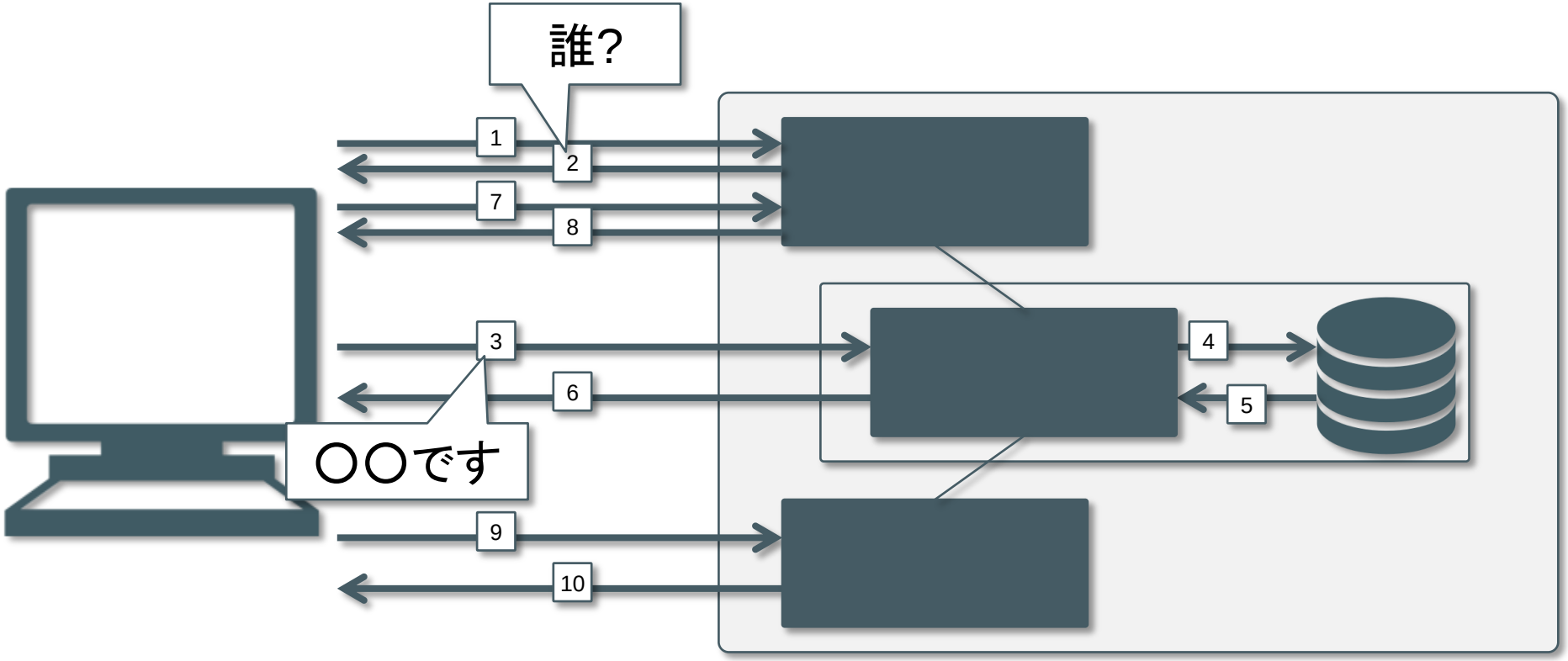
自己紹介

- 工藤達雄 http://www.linkedin.com/in/tatsuokudo, @tkudos
  - サン・マイクロシステムズ (1998~2008)
    https://blogs.oracle.com/tkudo
  - 野村総合研究所 (2008~)
  - OpenIDファウンデーション・ジャパン (2013~)
    http://openid.or.jp/blog

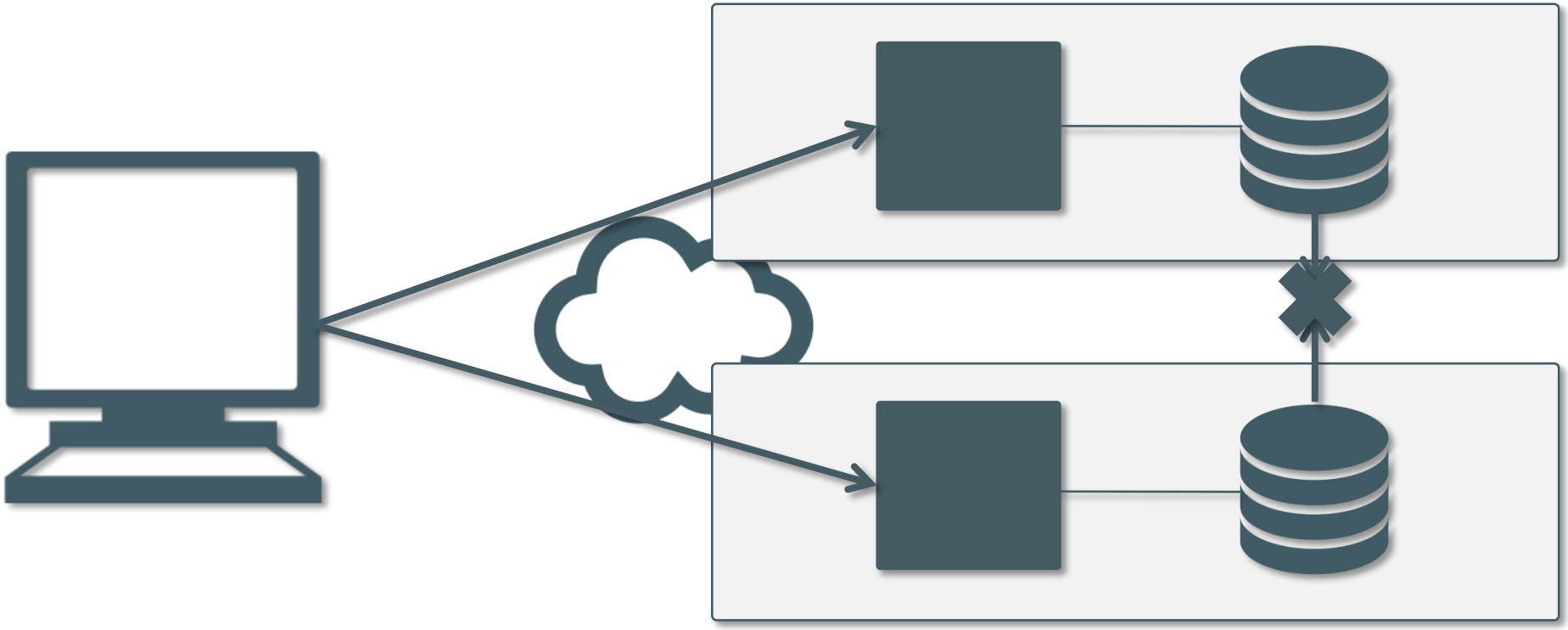
Webアプリケーションのユーザー認証



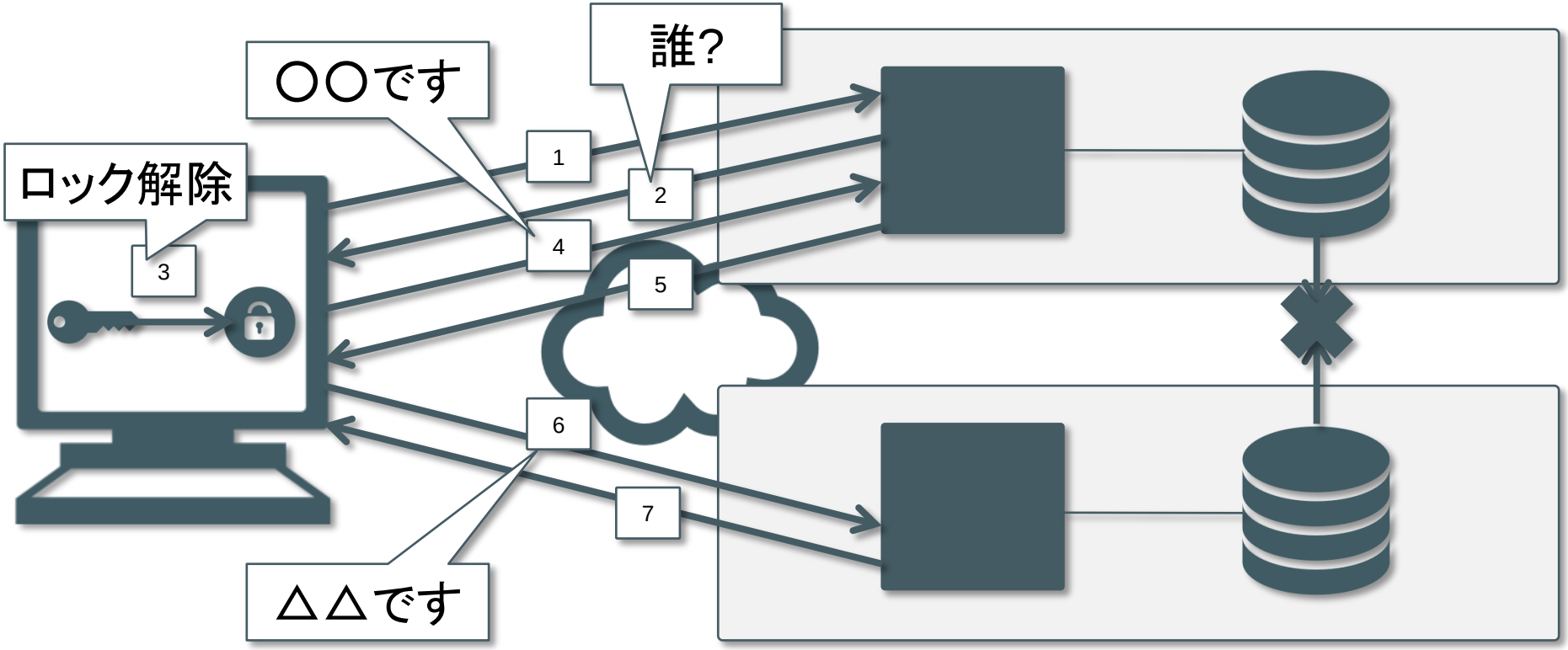
SSO
(エスエスオー; Single Sign-On)



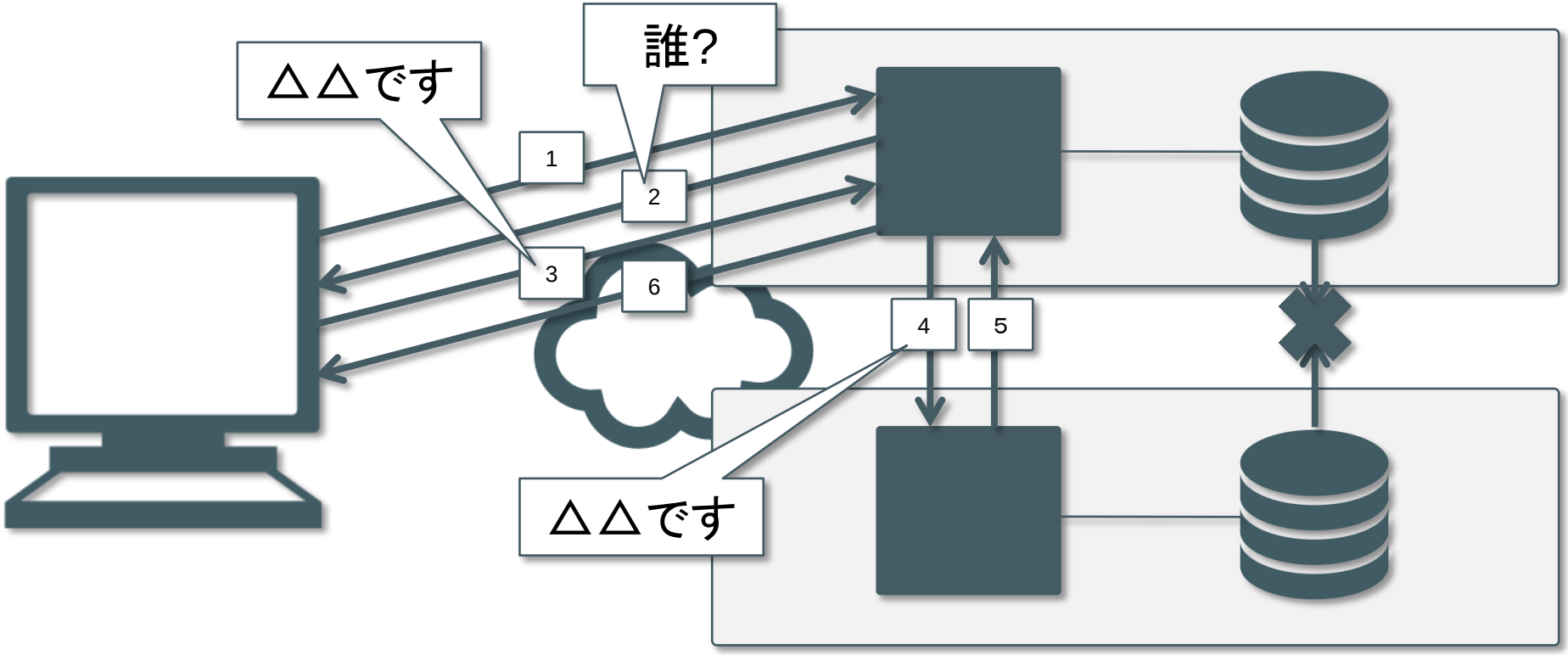
複数アイデンティティ・リポジトリ間のSSO



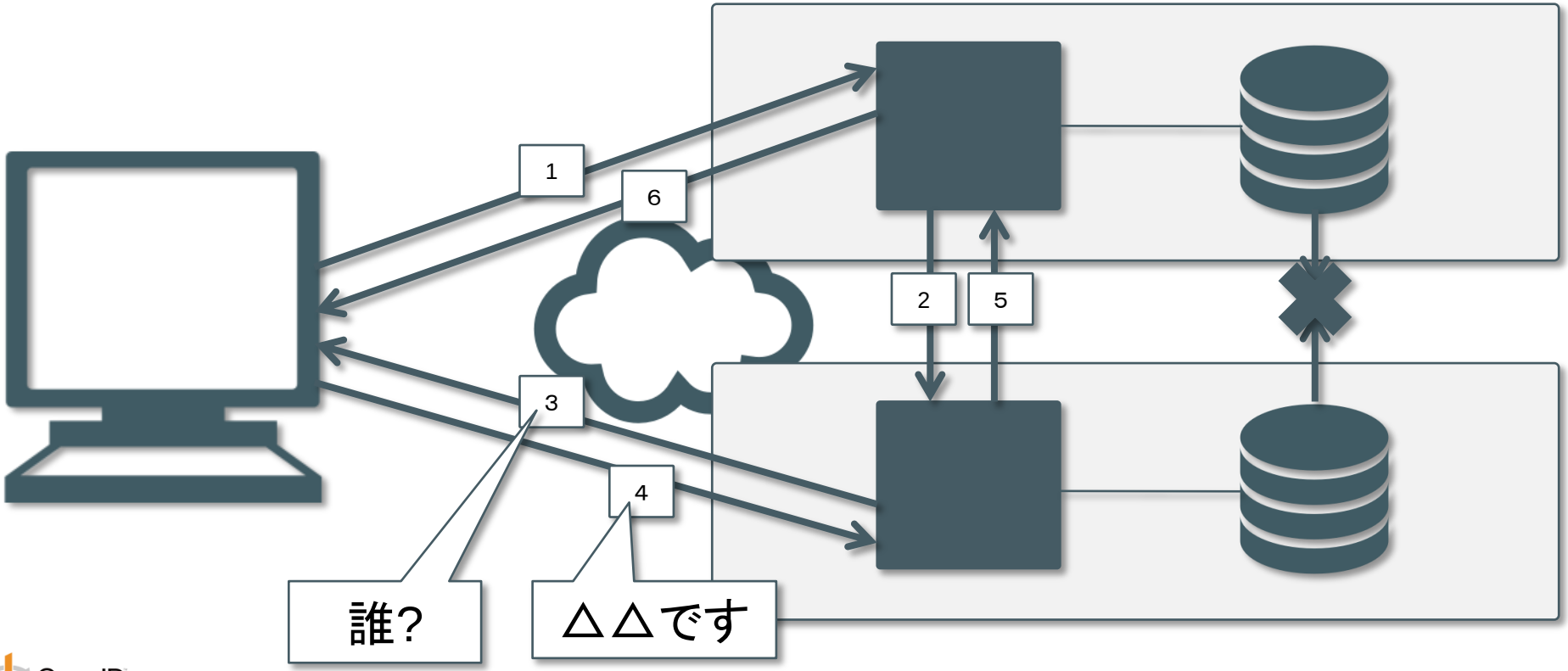
方法その1: クライアント側ががんばる



方法その2: クレデンシャルを横取り

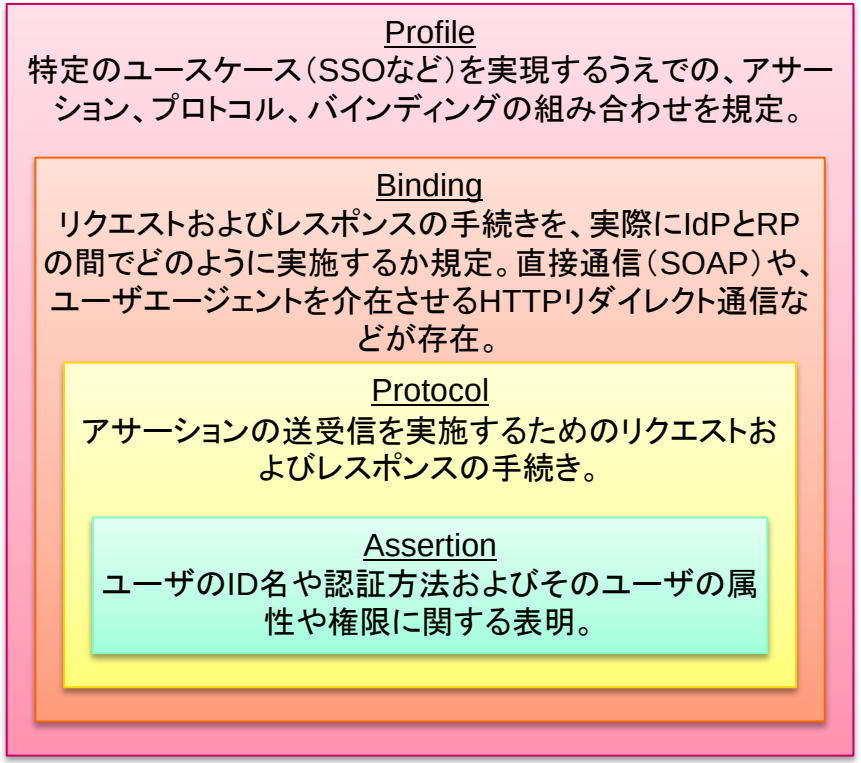


方法その3: アイデンティティ連携



SAML
(サムル; Security Assertion Markup Language)

- アイデンティティ情報を安全に流通させるためのXML形式および通信仕様
- ID連携を実現する主要要素を4つに分解
  - 「アサーション」「プロトコル」「バインディング」「プロファイル」

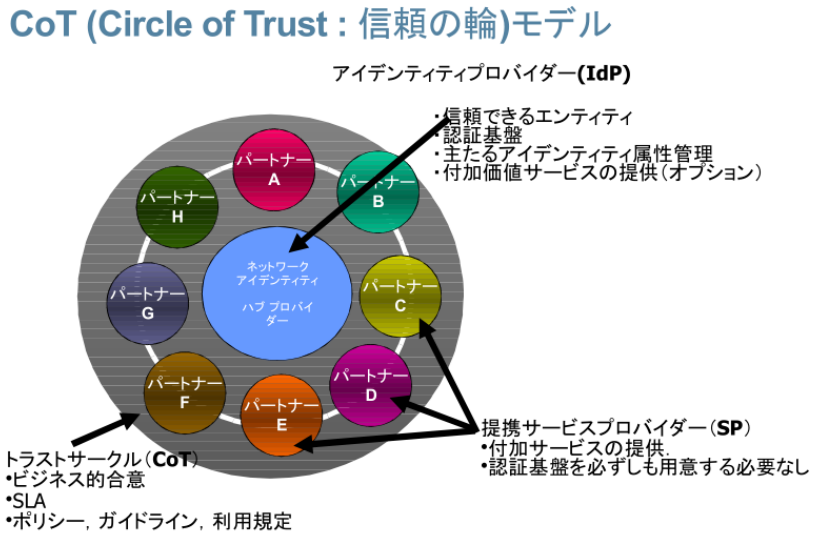


SAMLのコアは「アサーション」

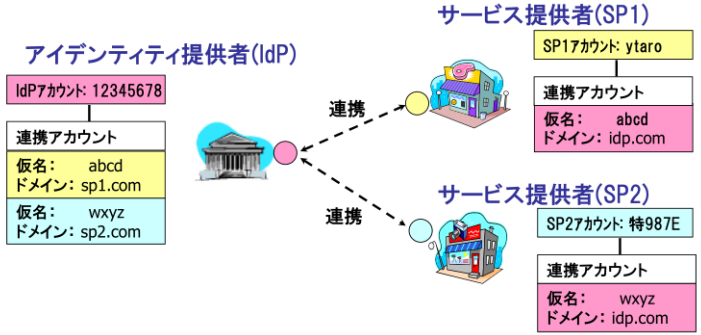
```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Version="2.0" IssueInstant="2005-01-
31T12:00:00Z">
 <saml:Issuer>www.example.com</saml:Issuer>
 <saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress">j.doe@example.com</saml:NameID>
 </saml:Subject>
 <saml:Conditions NotBefore="2005-01-31T12:00:00Z" NotOnOrAfter="2005-01-
31T12:30:00Z"></saml:Conditions>
 <saml:AuthnStatement AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="0">
  <saml:AuthnContext>
   <saml:AuthnContextClassRef>
    urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
   </saml:AuthnContextClassRef>
  </saml:AuthnContext>
 </saml:AuthnStatement>
</saml:Assertion>
```

Source: Federated Identity Management http://www.xmlgrrl.com/publications/177-maler-fed-id.html

Liberty Alliance



Source: Web2.0時代のアイデンティティ関連技術と OpenID
http://www.slideshare.net/schee/t2



Source:リバティ・アライアンスの取組みについて
http://www.kantei.go.jp/jp/singi/it2/nextg/meeting/dai7/siryou4.pdf

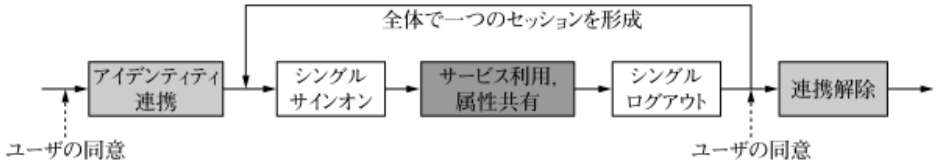
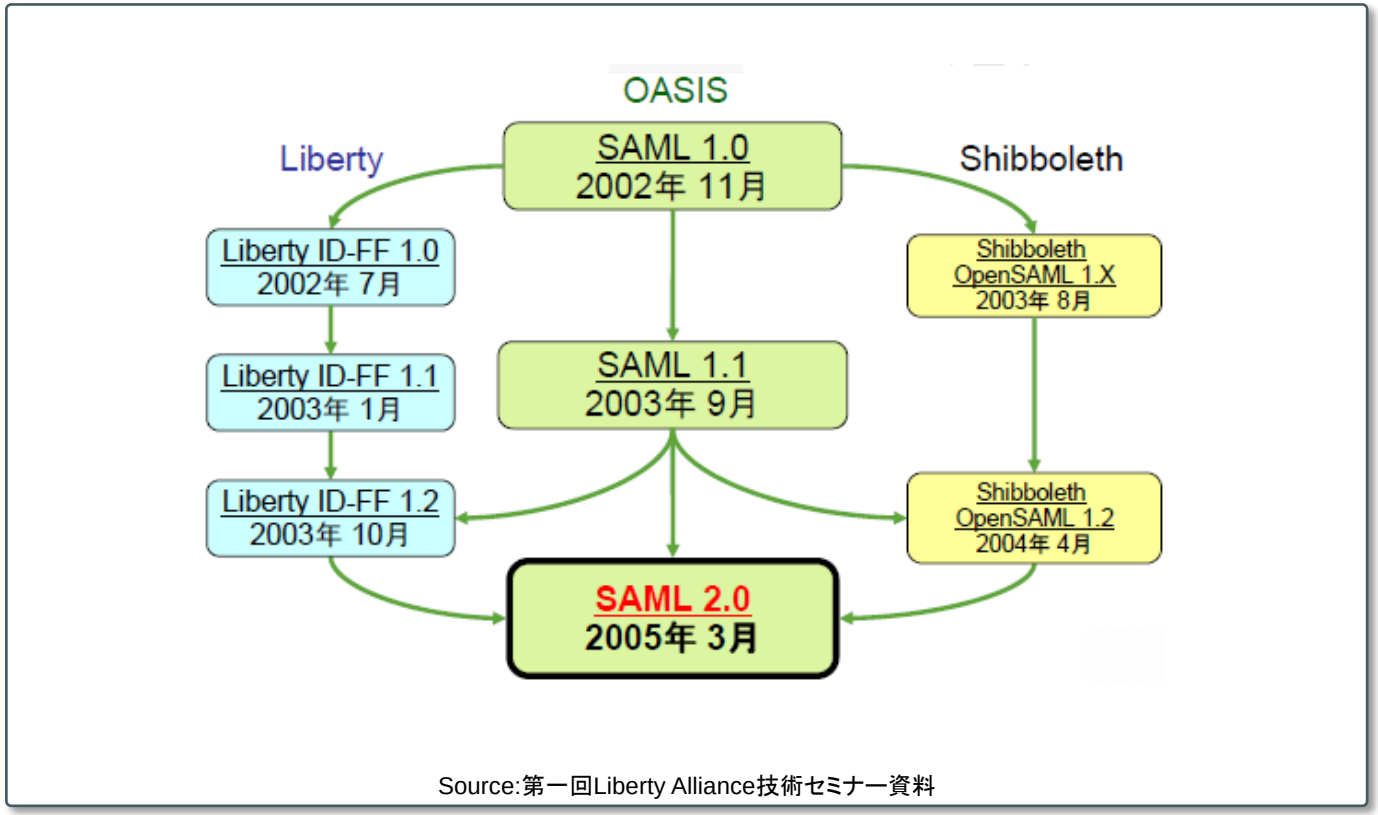


図2 アイデンティティ連携方式における処理手順の概要

Source: 高橋健司. "アイデンティティ管理の現状と今後." *信学誌* 92.4 (2009): 287-294.
http://ieice.or.jp/jpn/books/kaishikiji/2009/200904.pdf

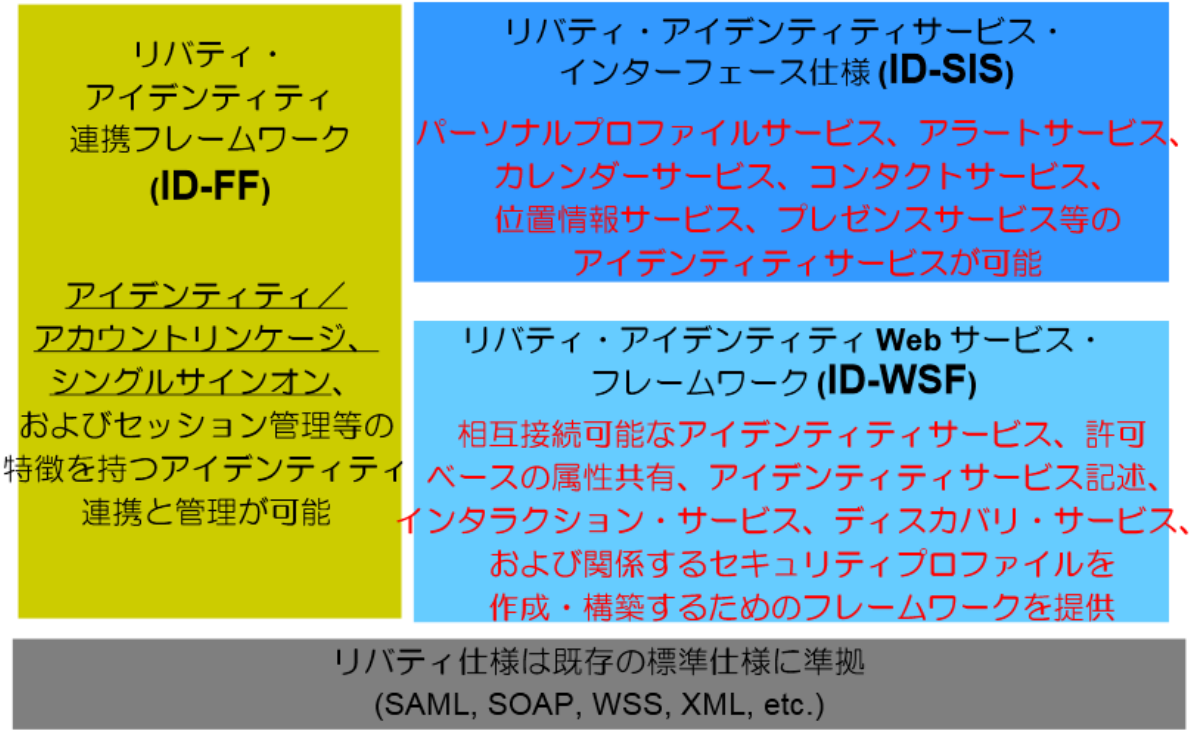
SAML 2.0

(aka Liberty ID-FF (Identity Federation Framework))



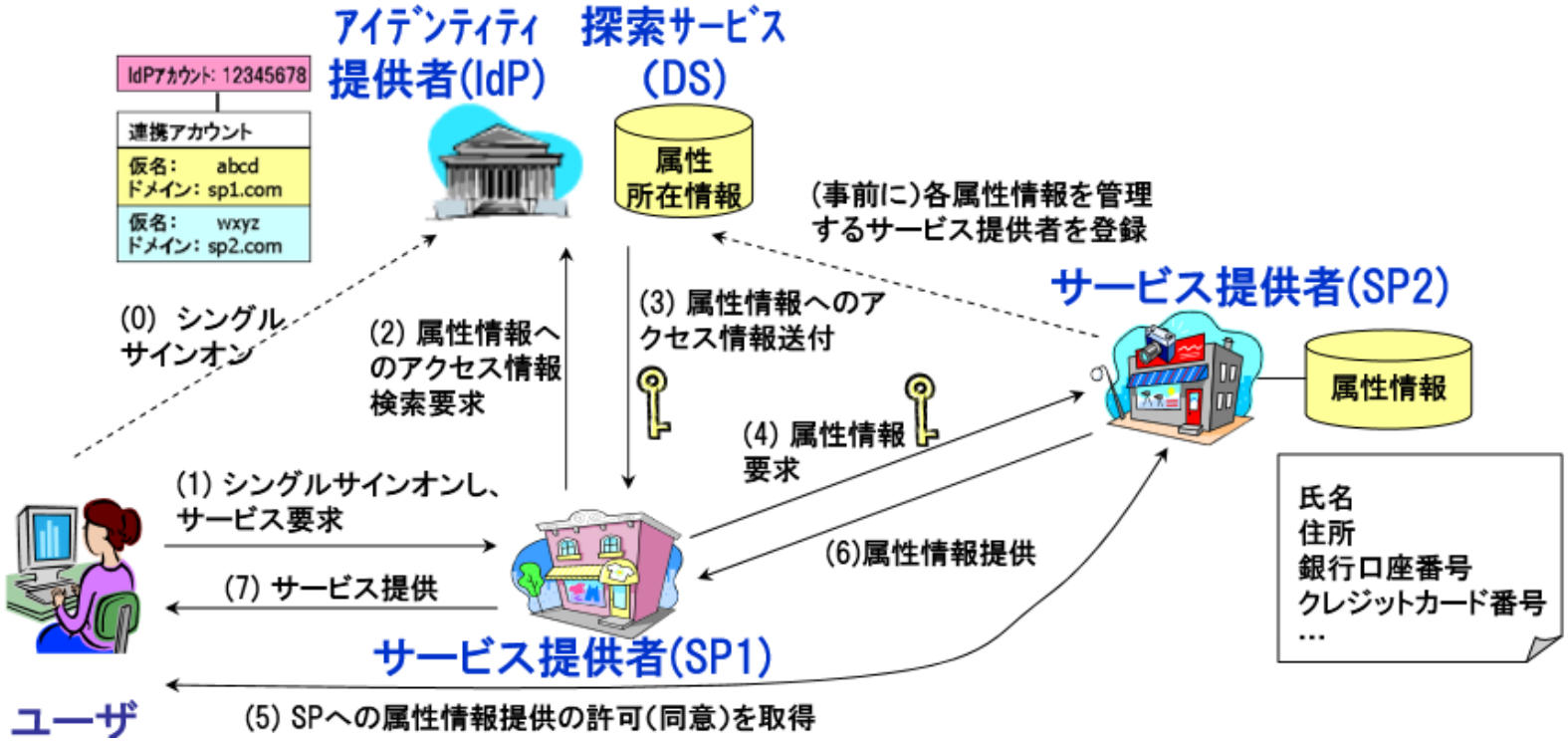
Source:第一回Liberty Alliance技術セミナー資料

Liberty ID-WSF
(アイデンティティWebサービス・フレームワーク)



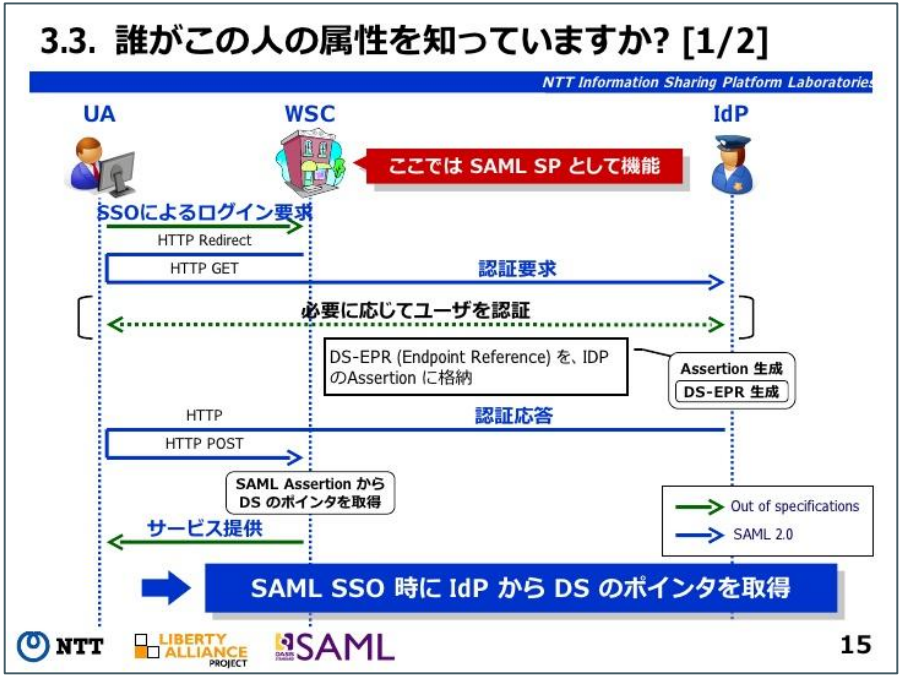
Source: クラウド間連携へ向けてのアイデンティティ管理技術 カンターラ･イニシアティブ概要と技術標準化の動向
https://itmedia.smartseminar.jp/static/upload/itmedia.smartseminar.jp/seminar/110/shared/pdf/Com-3.pdf

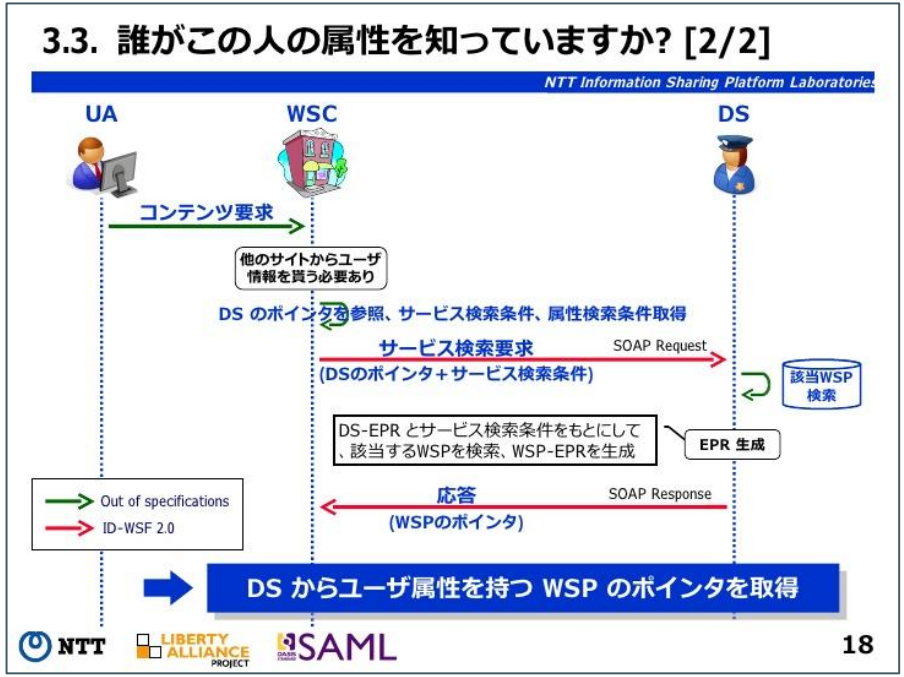
ID-WSFが目指していたもの



Source:リバティ・アライアンスの取組みについて http://www.kantei.go.jp/jp/singi/it2/nextg/meeting/dai7/siryou4.pdf

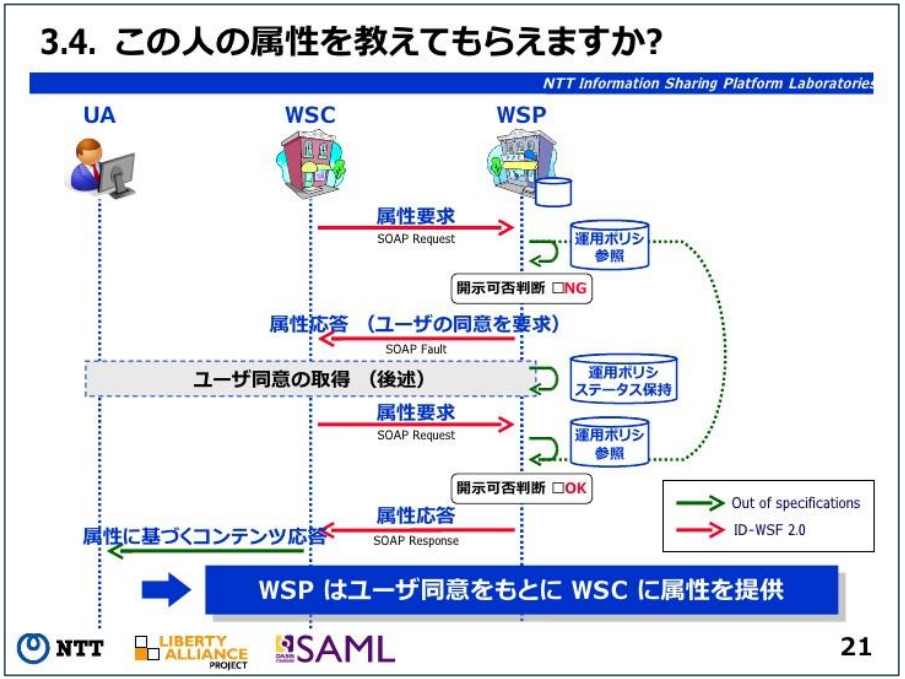
ID-WSFのシーケンス

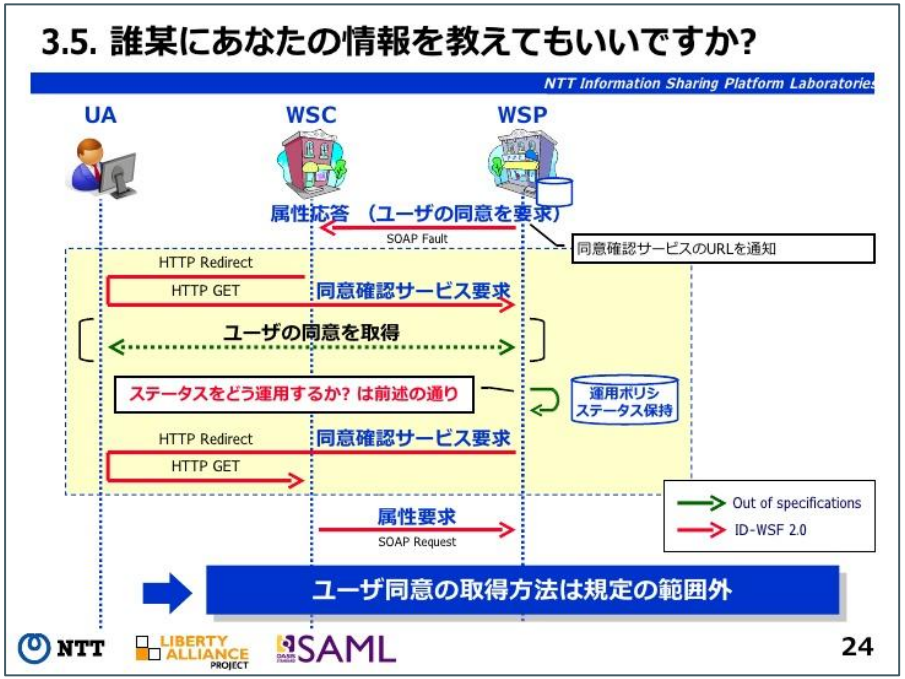




Source: Liberty Alliance ID-WSF2.0 仕様 について http://www.slideshare.net/hiroki/080620-identity-conference-2-hiroki

ID-WSFのシーケンス (cont.)



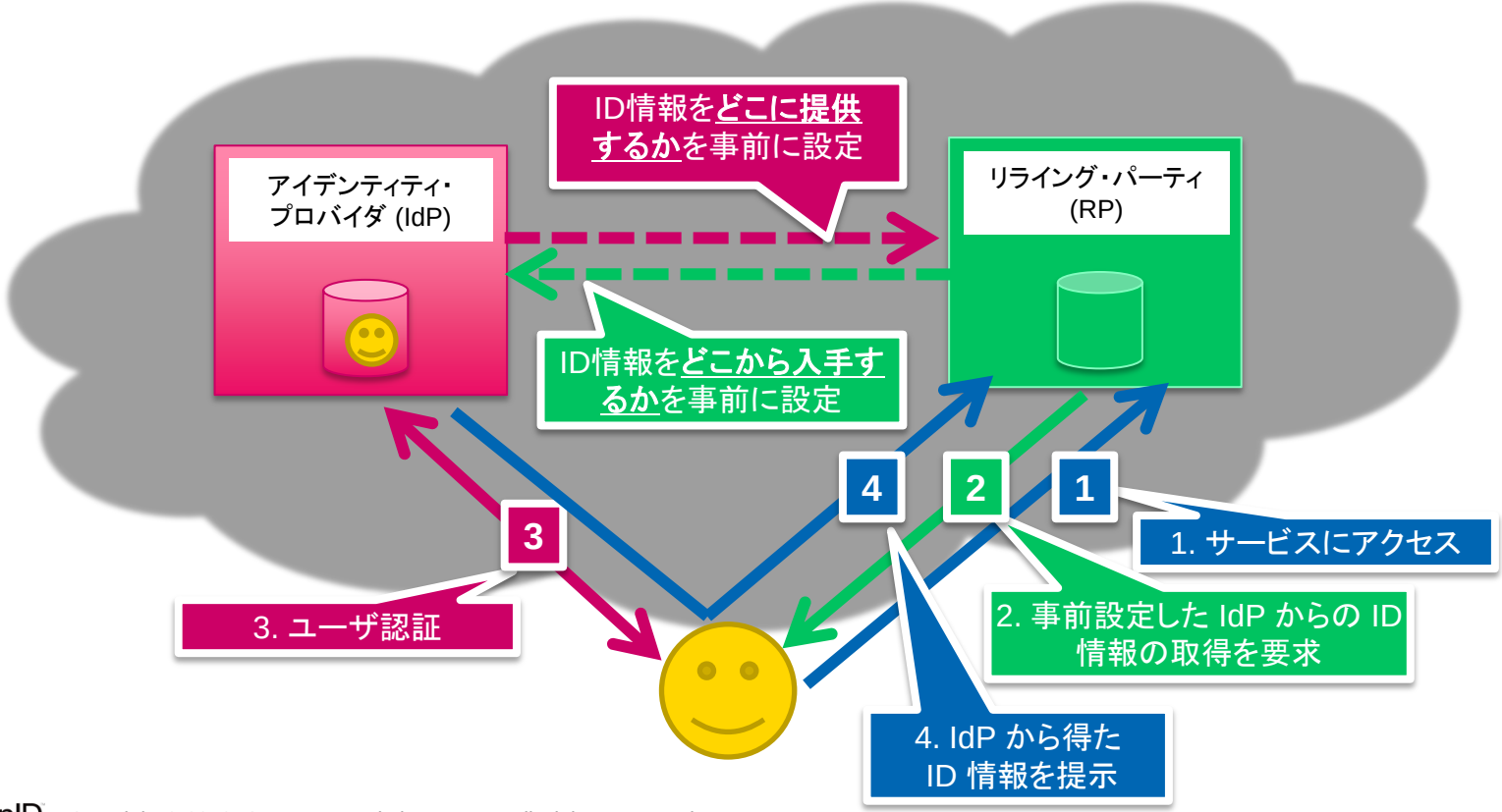


Source: Liberty Alliance ID-WSF2.0 仕様 について http://www.slideshare.net/hiroki/080620-identity-conference-2-hiroki

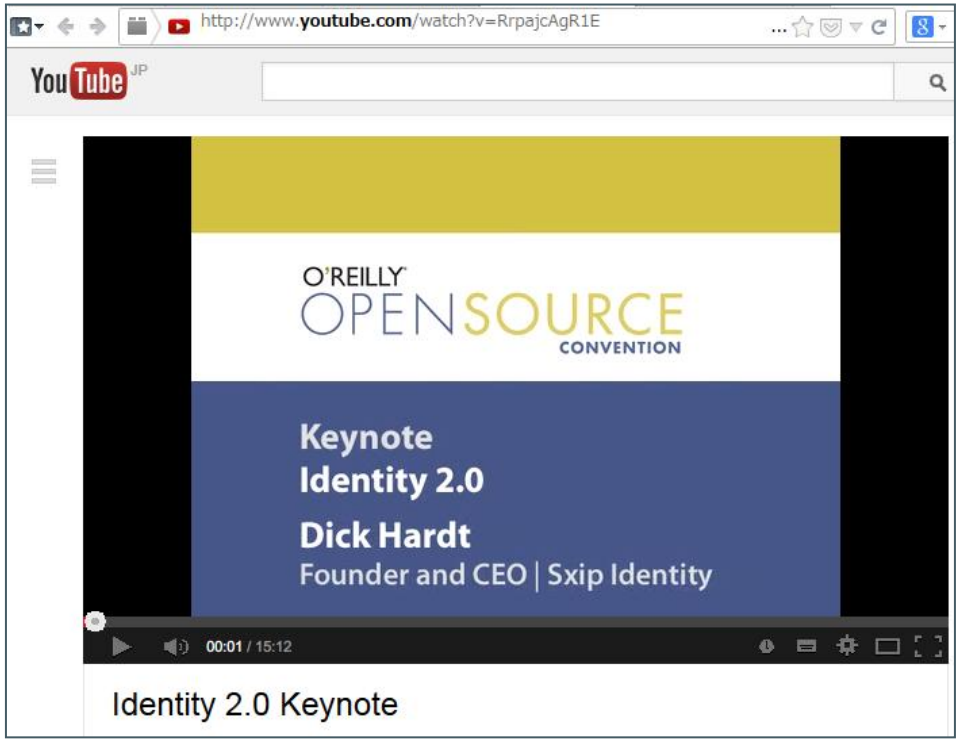
けっきょくID-WSFは普及しなかった

- 一言で言うと「やりすぎ」
- サービス仕様まで定義しようとした
- ついていけないので普及が進まない → 普及が進まないので流行らない → 流行ってないのでついていかない → （以下繰り返し）

SAMLは「事前の信頼関係に基づく連携」



“Identity 2.0”



Source: Identity 2.0 Keynote http://youtu.be/RrpajcAgR1E

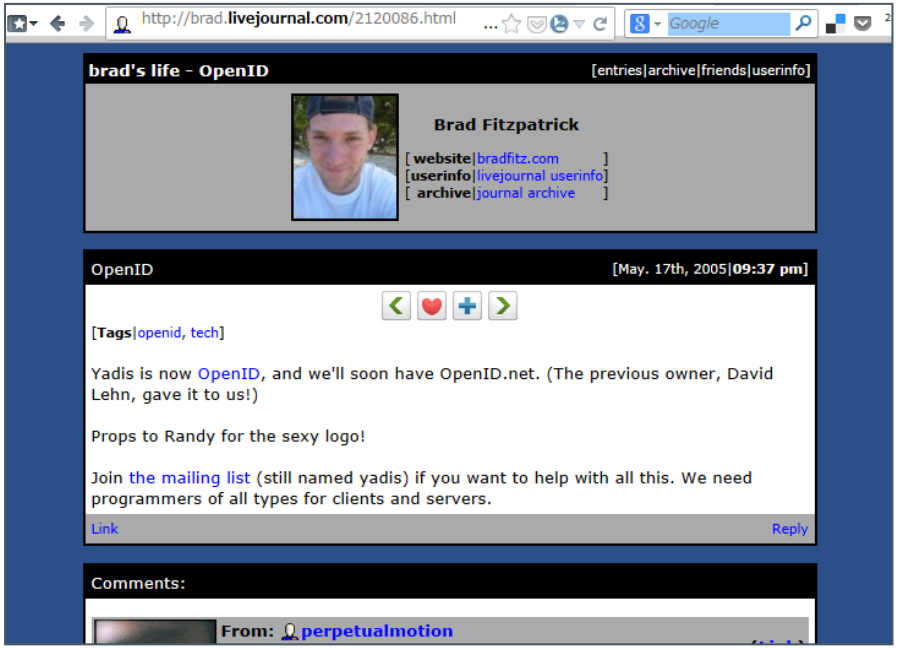
“The Laws of Identity”

Source: IdentityBlog - Digital Identity, Privacy, and the Internet's Missing Identity Layer http://www.identityblog.com/?p=1065

「ユーザーセントリック・アイデンティティ」

- ユーザーがコンテクストに応じて決める
  - どのIDを使うか（名乗るか）
  - どの属性を連携するか
  - …

OpenID



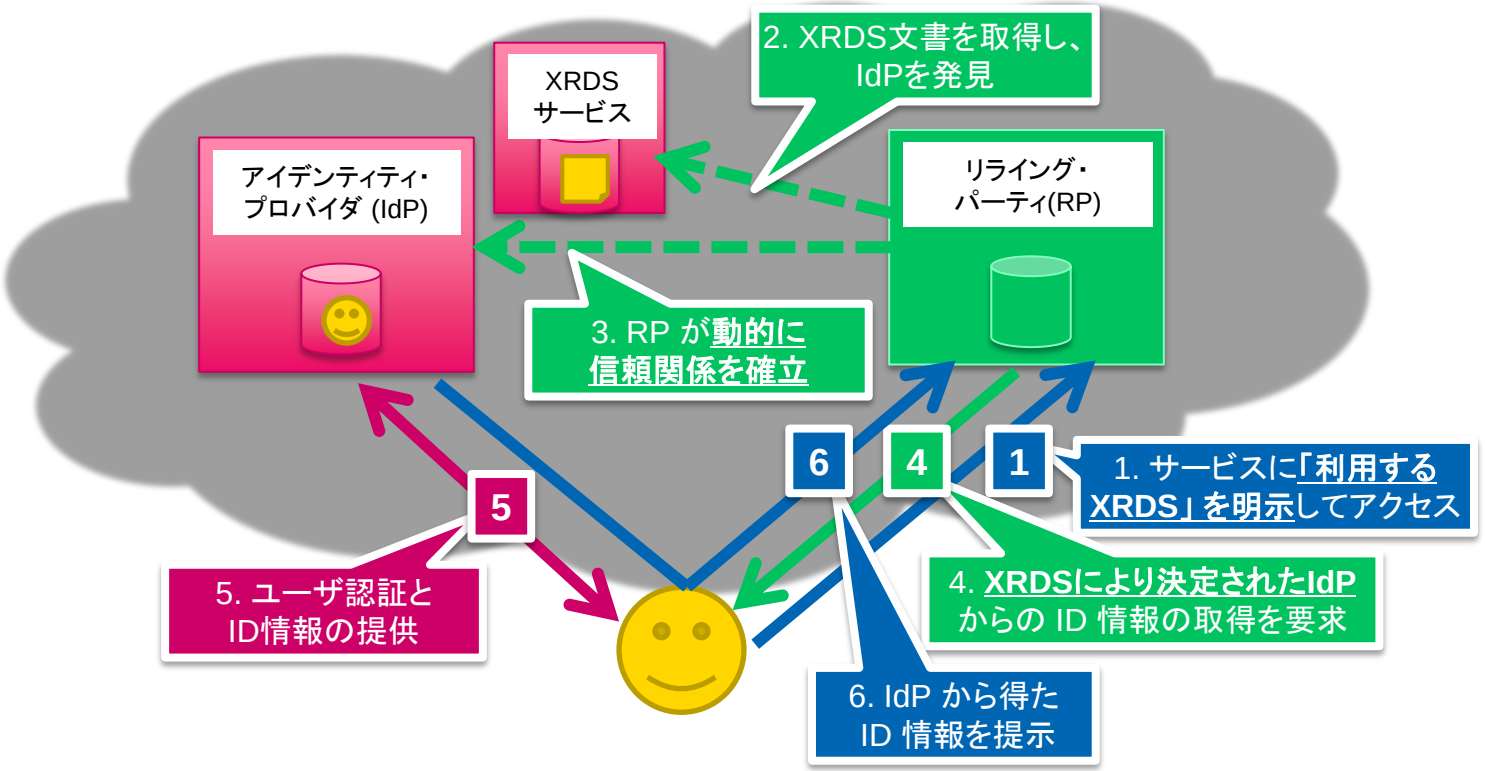
Source: brad's life - OpenID http://brad.livejournal.com/2120086.html

OpenIDとは

- OpenIDにおけるIDとはURLのことである。
- End Userは自分のClaimed IdentifierをConsumerに対して認証してくれるIdPに加入していなければならない。
- End UserはどのIdPに加入していても良く、ConsumerはいずれのIdPであっても協調してEnd UserのClaimed Identifierの認証手続きを行わなければならない。
- IdPがConsumerに対して認証するのはEnd UserのClaimed Identifier、即ちURLが、End Userが確かに所有しているかどうかということである。

Source: OpenIDの仕様と技術（1）：仕様から学ぶOpenIDのキホン (3/3) - @IT
http://www.atmarkit.co.jp/ait/articles/0707/06/news135_3.html

OpenIDはサービス同士の連携を「ユーザ」が決定



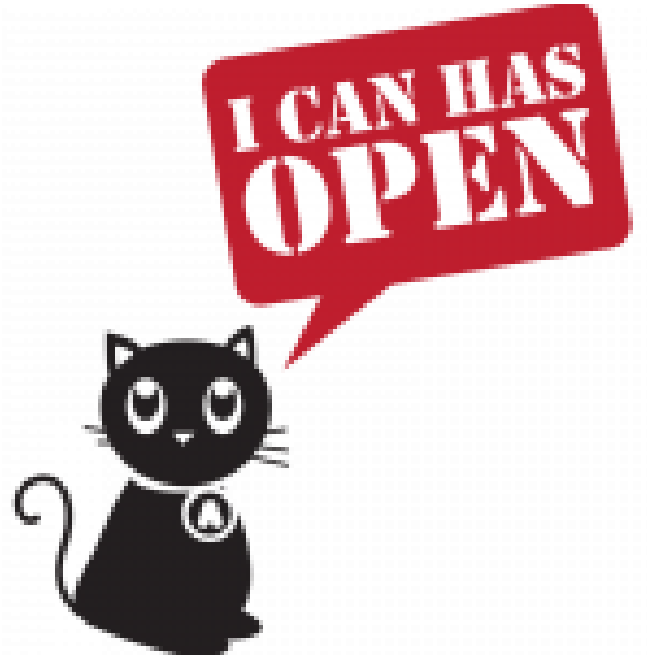
OpenIDをAPIのアクセス認可にも使えないか?

- We want something like Flickr Auth / Google AuthSub / Yahoo! BBAuth, but published as an open standard, with common server and client libraries, etc. The trick with OpenID is that the users no longer have passwords, so you can't use basic auth for API calls without requiring passwords (defeating one of the main points of OpenID) or giving cut-and-paste tokens (which suck).

  -- Blaine Cook, April 5th, 2007

Source: History « hueniverse http://hueniverse.com/oauth/guide/history/

OAuth

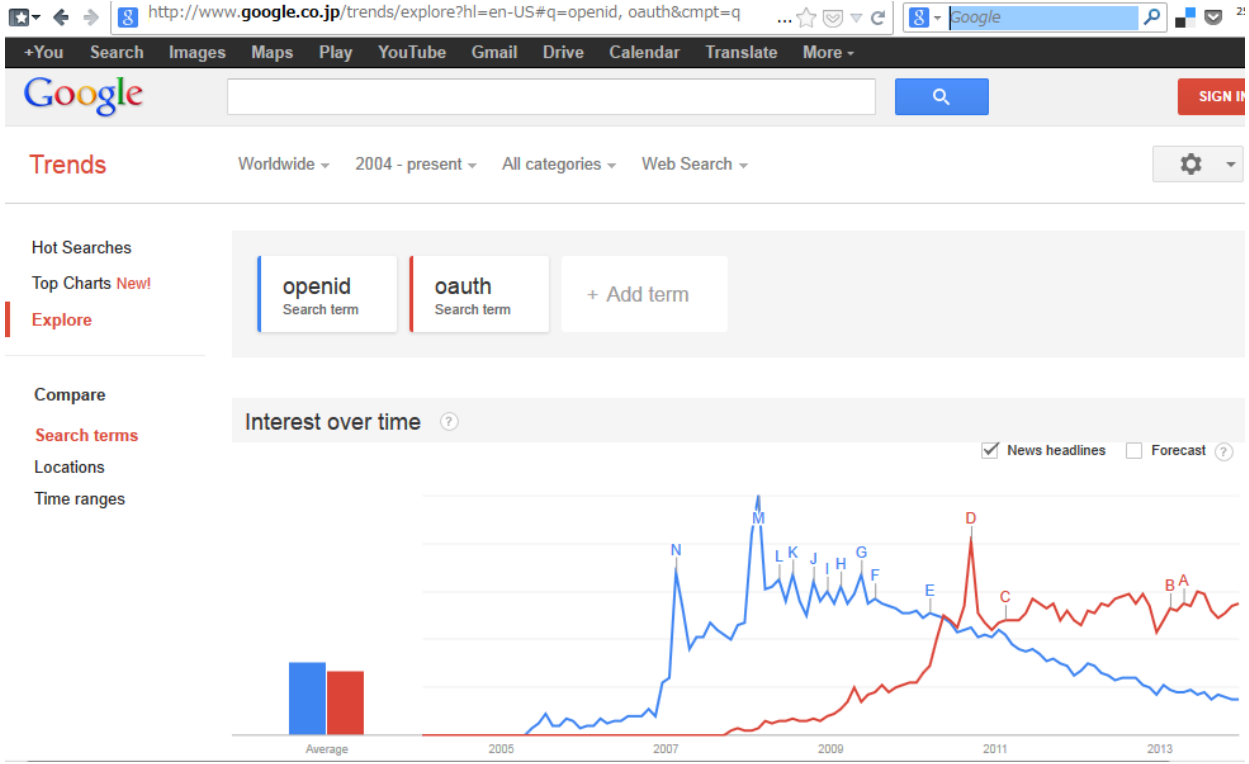


I CAN HAD OPEN: OAuth First Summit a Hit! « hueniverse
http://hueniverse.com/2008/07/i-can-had-open-oauth-first-summit-a-hit/

そこかしこでOAuthが使われるように

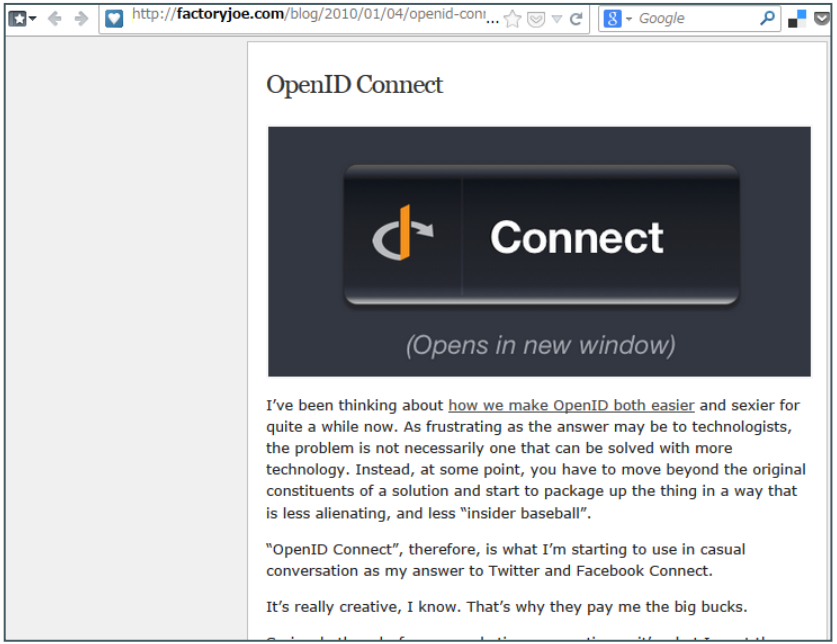
- ユーザー認証に使うケースも
  - OAuth+OpenIDよりも、OAuth+独自ユーザー認証APIのほうが提供しやすい
- さらに発展
  - OAuth WRAP → OAuth 2.0へ
  - Facebookも乗ってきた

OpenID < OAuth

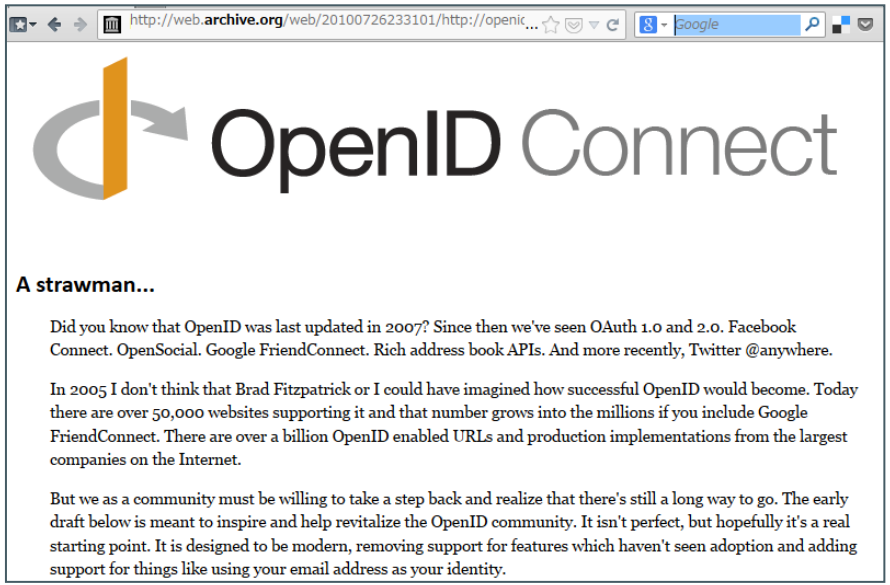


Source: Google Trends - Web Search interest: openid, oauth - Worldwide, 2004 - present http://goo.gl/2M2MJp

「(旧) OpenID Connect」

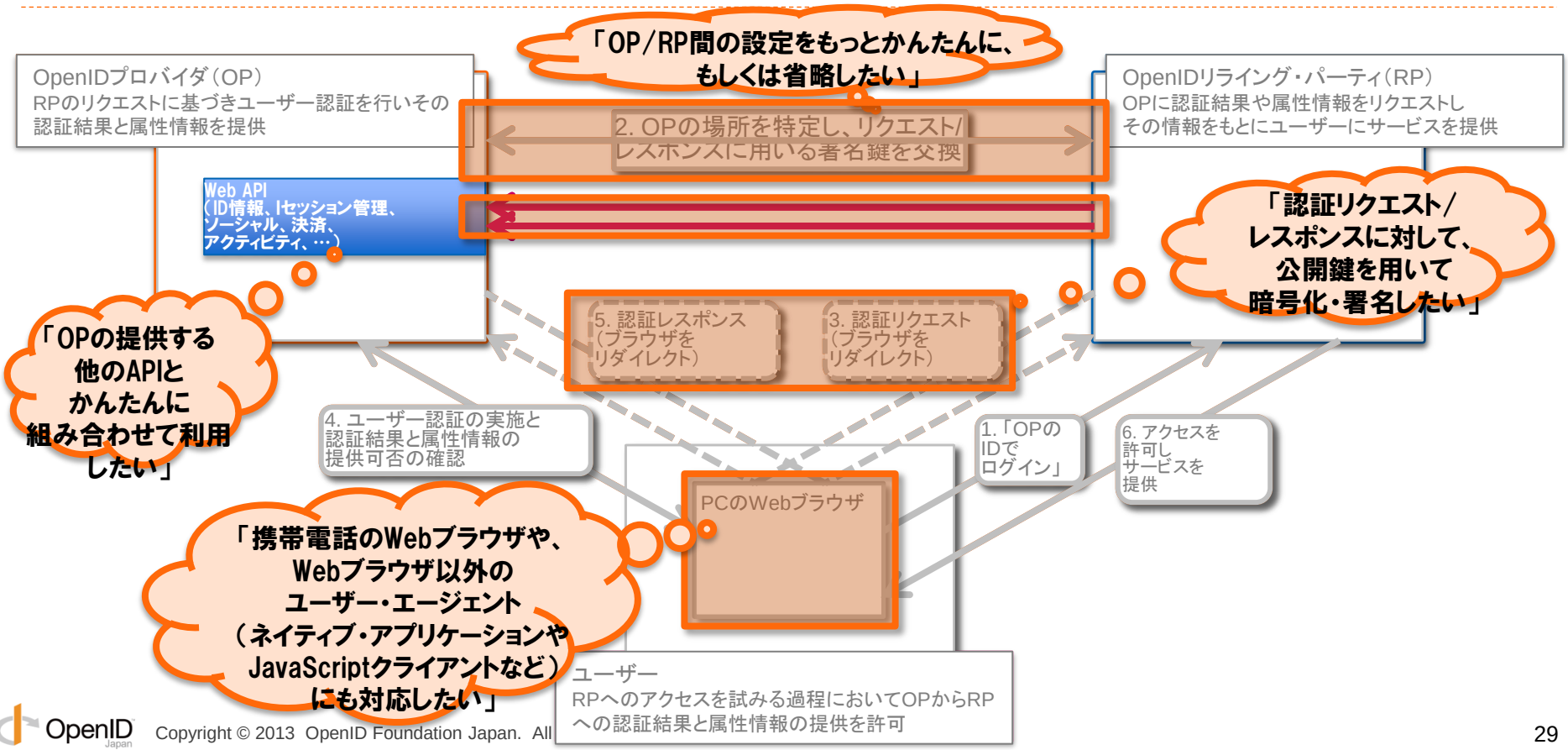


Source: FactoryCity » OpenID Connect
http://factoryjoe.com/blog/2010/01/04/openid-connect/

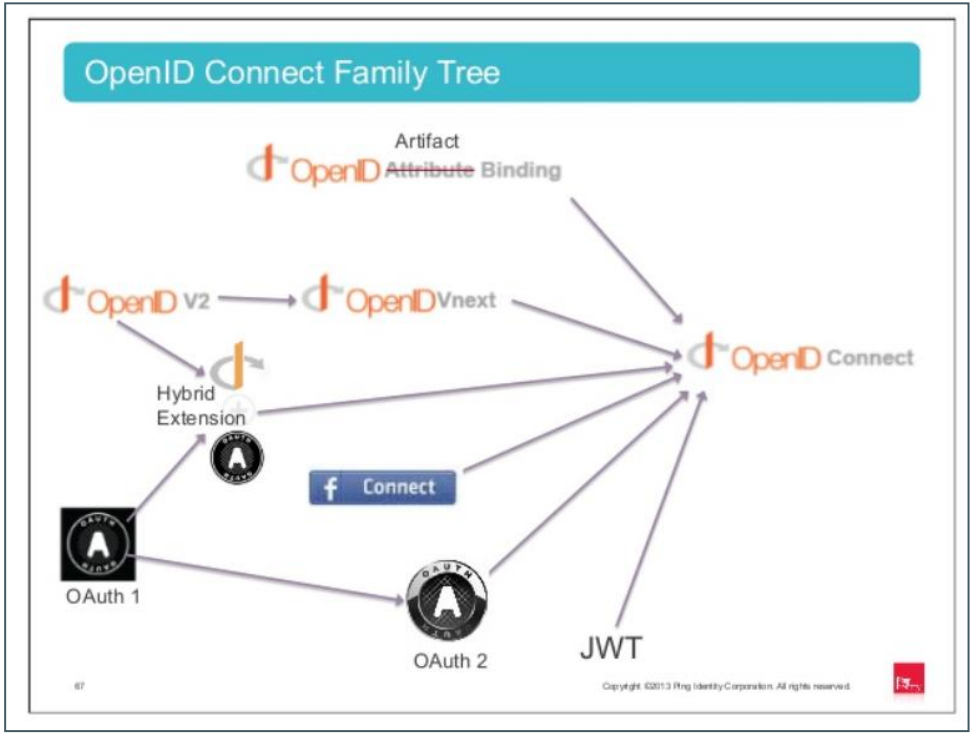


Source: OpenID Connect
http://web.archive.org/web/20100726233101/http://openidconnect.com/

OpenID 2.0の課題



現在のOpenID Connectへ



Source: CIS13: Bootcamp: Ping Identity OAuth and OpenID Connect In Action w...
http://www.slideshare.net/CloudIDSummit/cis13-bootcamp-ping-identity-oauth-and-openid-connect-in-action-with-pingfederate-handson

OpenID Connect

アイデンティティ・プロバイダ

(IdP: ID情報提供側)

SSO / アクセス管理システム

“Self-issued IdP”

OpenID Connect 対応製品が続々登場

携帯端末がIdPに!

OAuth 2.0による API認可と統合

認可リクエスト/APIアクセス

OpenID Connect

認証結果/属性情報提供

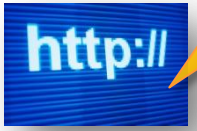
JWT * によって セキュアにID情報を提供

*** JSON Web Token**

リライング・パーティ

(RP: ID情報要求側)

Webアプリケーション

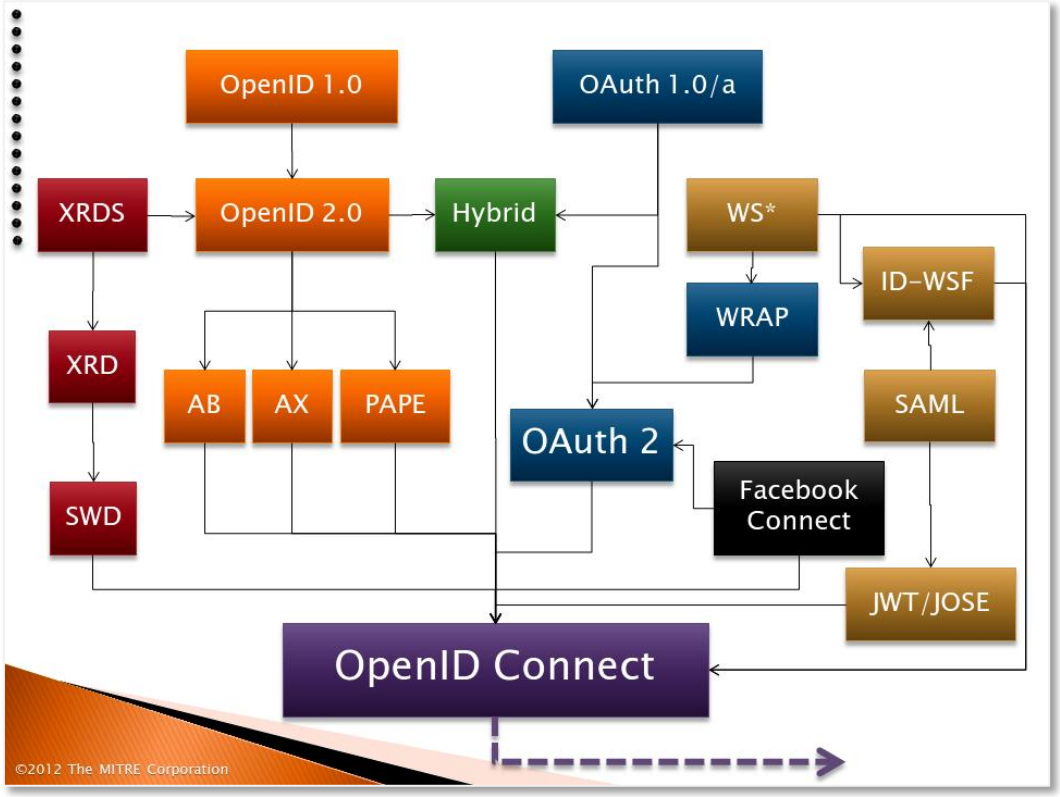


ライブラリやパッケージの導入が不要

モバイルアプリケーション

ネイティブ(non-Web)アプリでも利用可能

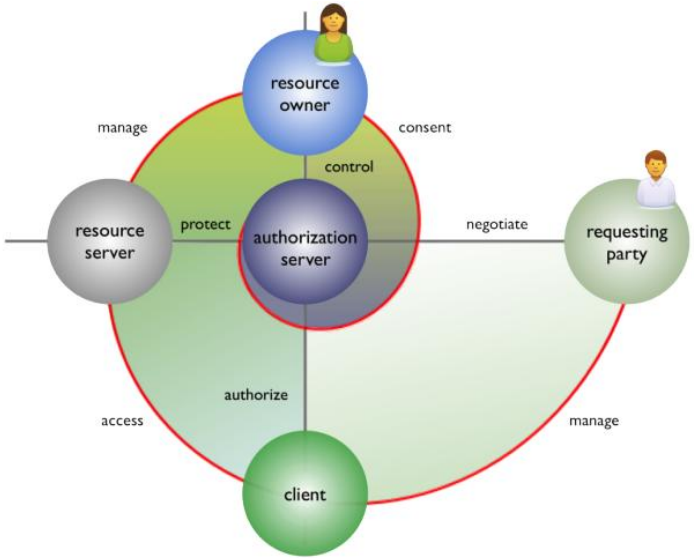
主要ID/API連携仕様がすべてOpenID Connectに収斂



Source: http://civics.com/OpenID-connect-webinar/

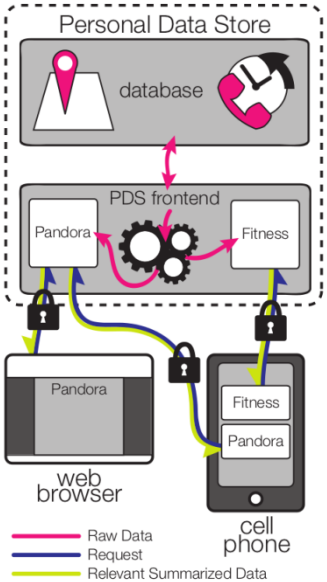
再び Identity First へ

- UMA (User Managed Access; ウーマ)



Source: [WG-UMA] New "UMA 101" slides available on the wiki
http://kantarainitiative.org/pipermail/wg-uma/2013-September/002486.html

- OpenPDS (Open Personal Data Store)



Source: openPDS - The privacy-preserving Personal Data Store
http://openpds.media.mit.edu/

まとめ

- ふたつの考えかたがある
  - サービスのひとつとしての「アイデンティティAPI」
  - アイデンティティが中心にあってこそのサービス


OpenID™
Japan