

# 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>

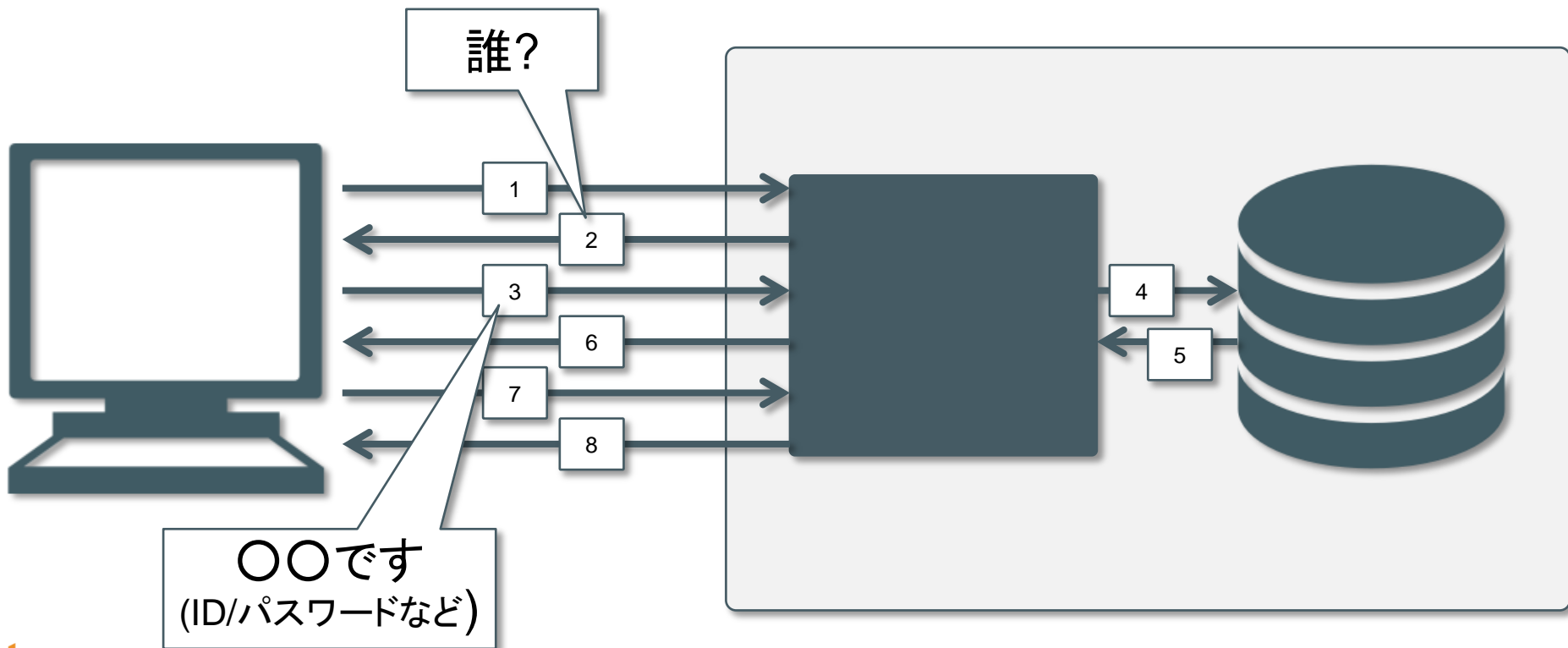
- 野村総合研究所 (2008~)

- OpenIDファウンデーション・ジャパン (2013~)

<http://openid.or.jp/blog>

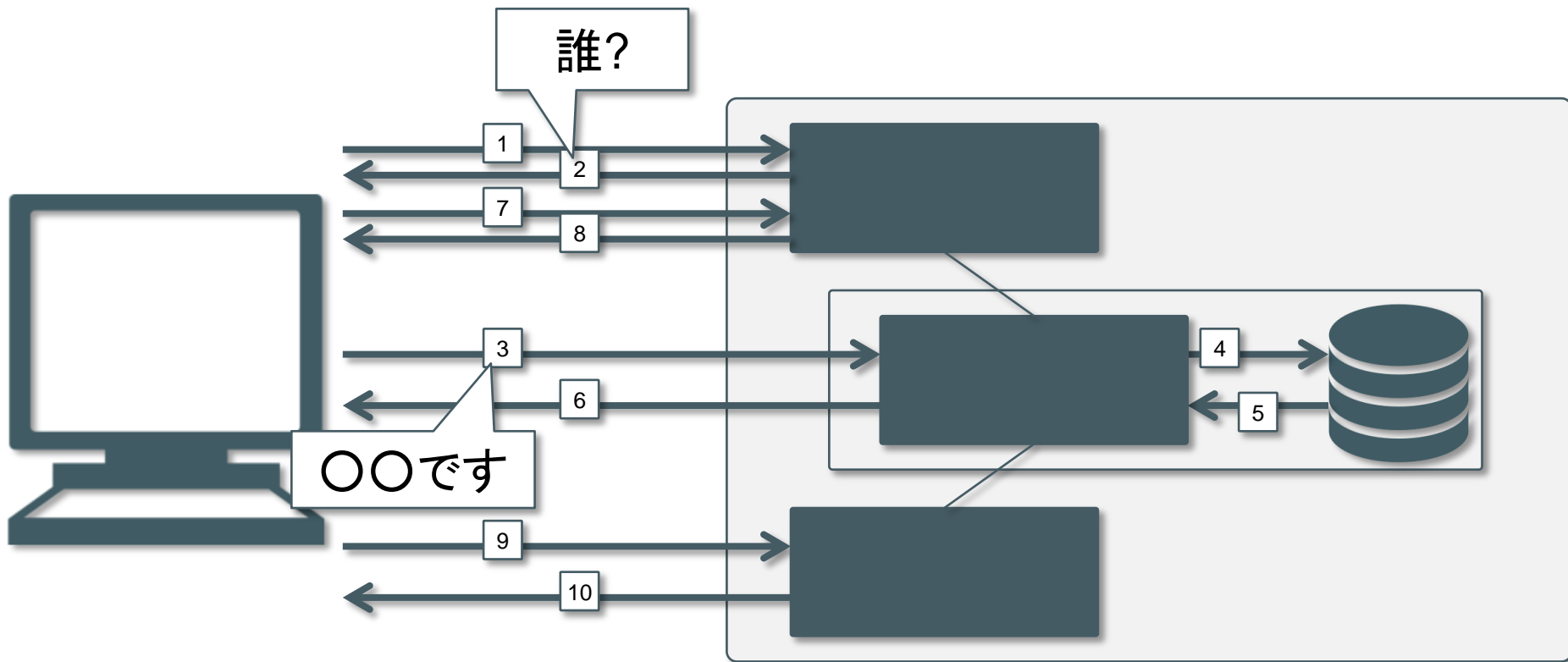


# Webアプリケーションのユーザー認証

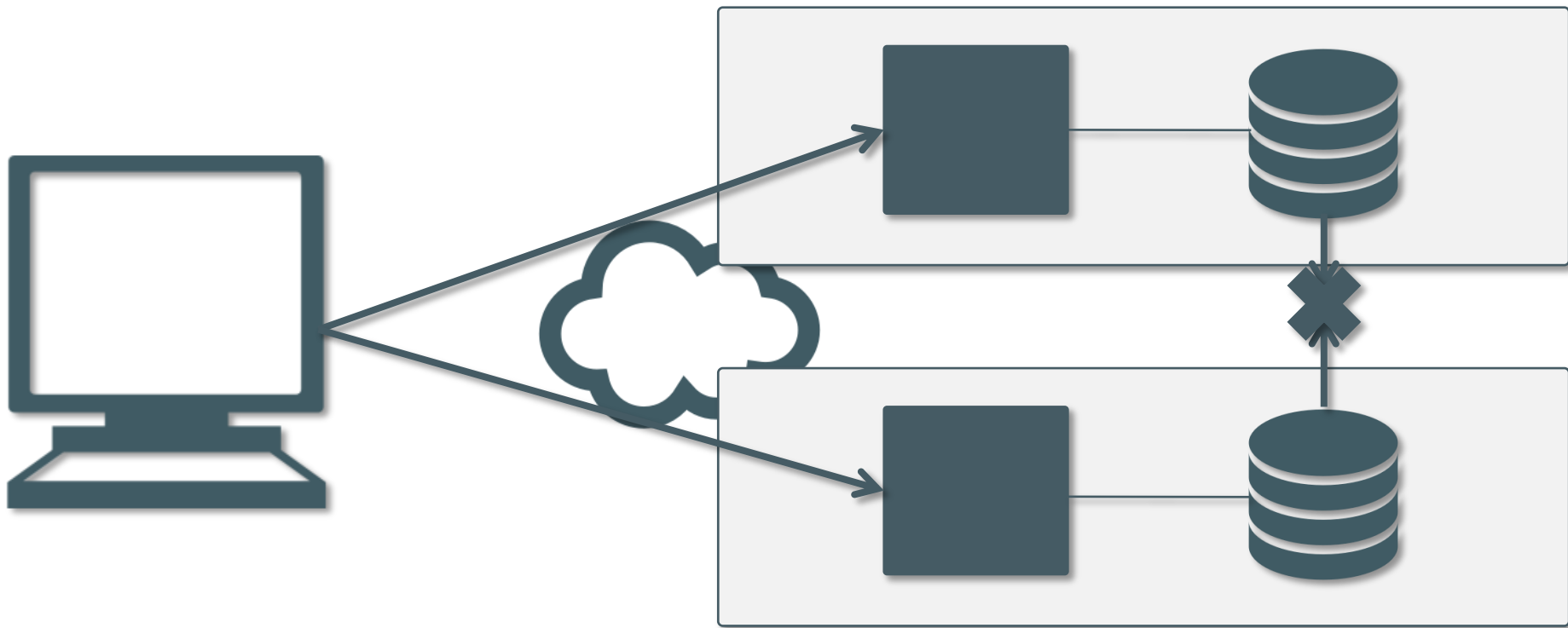


# SSO

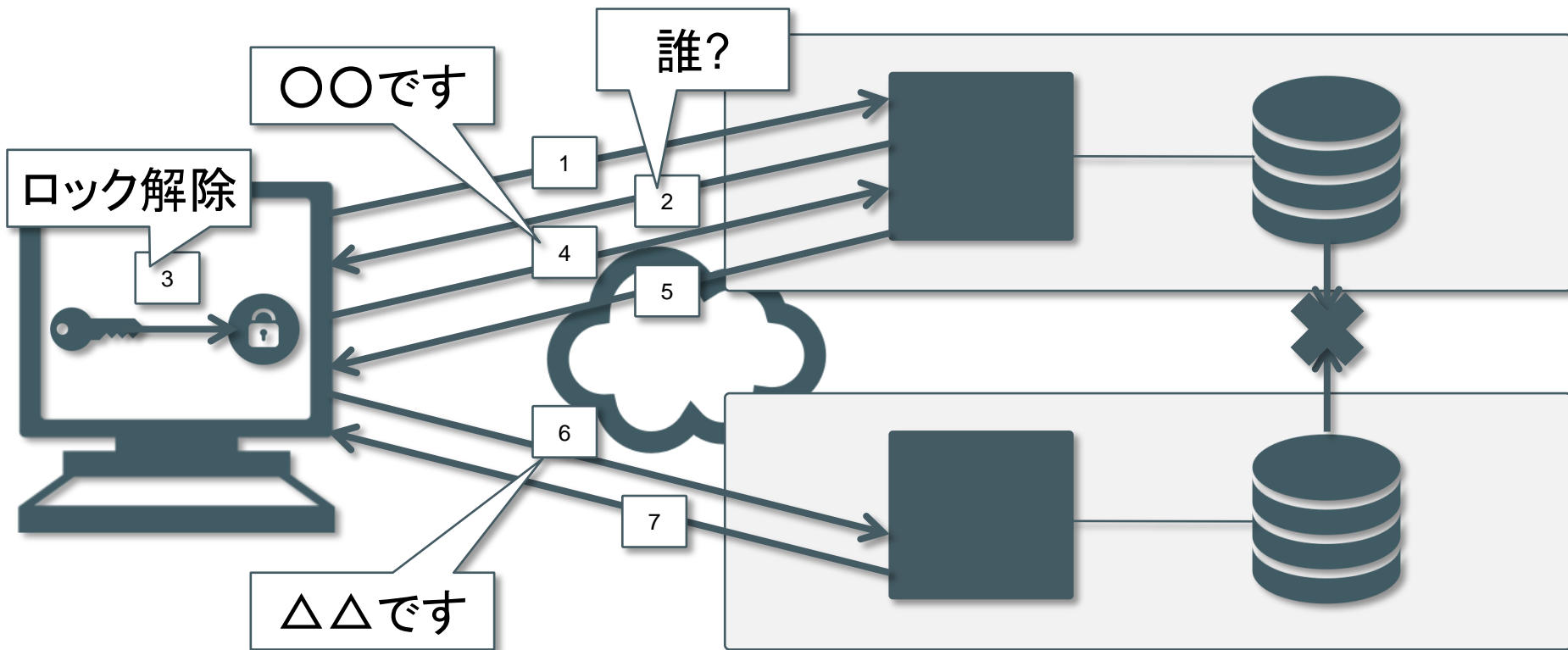
(एसएसオー; Single Sign-On)



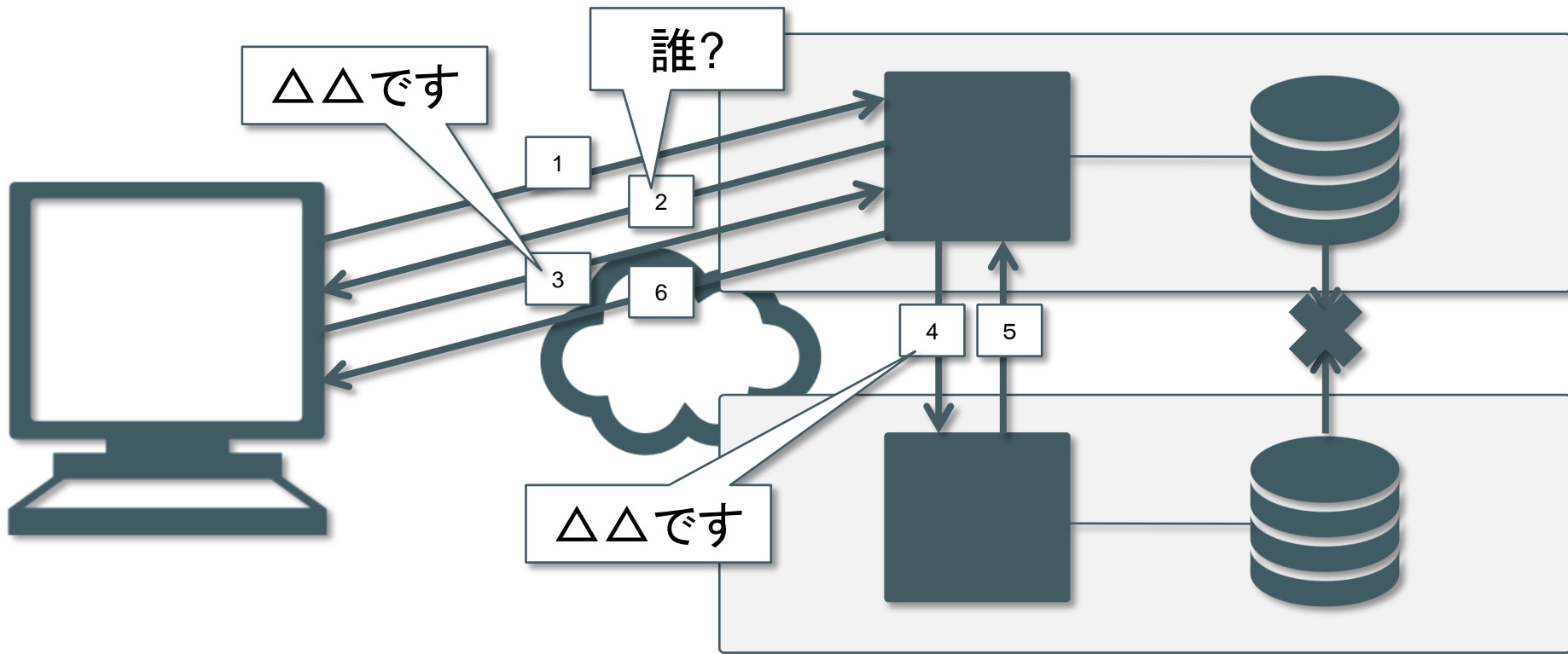
# 複数アイデンティティ・リポジトリ間のSSO



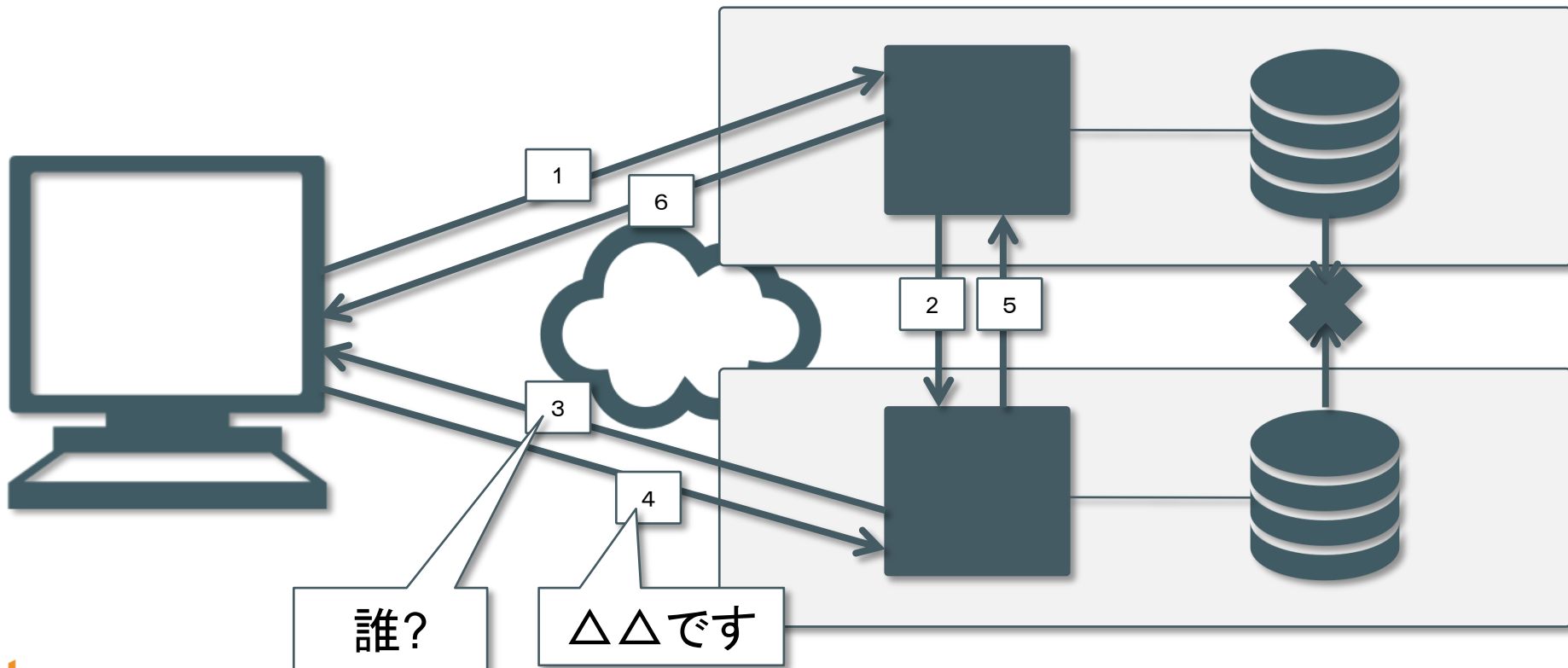
# 方法その1: クライアント側ががんばる



# 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

(サマル; 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」

## Profile

特定のユースケース(SSOなど)を実現するうえでの、アサーション、プロトコル、バインディングの組み合わせを規定。

## Binding

リクエストおよびレスポンスの手続きを、実際にIdPとRPの間でどのように実施するか規定。直接通信(SOAP)や、ユーザエージェントを介在させるHTTPリダイレクト通信などが存在。

## Protocol

アサーションの送受信を実施するためのリクエストおよびレスポンスの手続き。

## Assertion

ユーザのID名や認証方法およびそのユーザの属性や権限に関する表明。

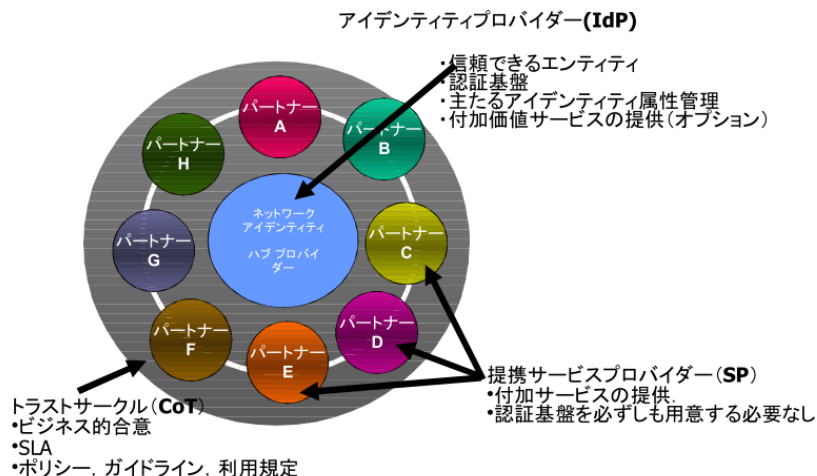
# SAMLのコアは「アサーション」

```
<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.xmlgrl.com/publications/177-maler-fed-id.html>

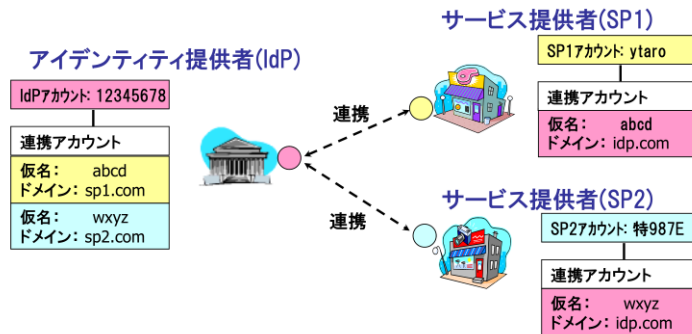
# Liberty Alliance

## CoT (Circle of Trust : 信頼の輪)モデル



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>

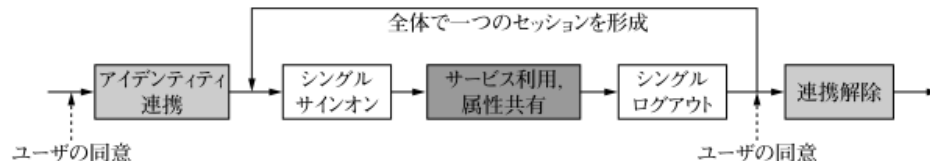


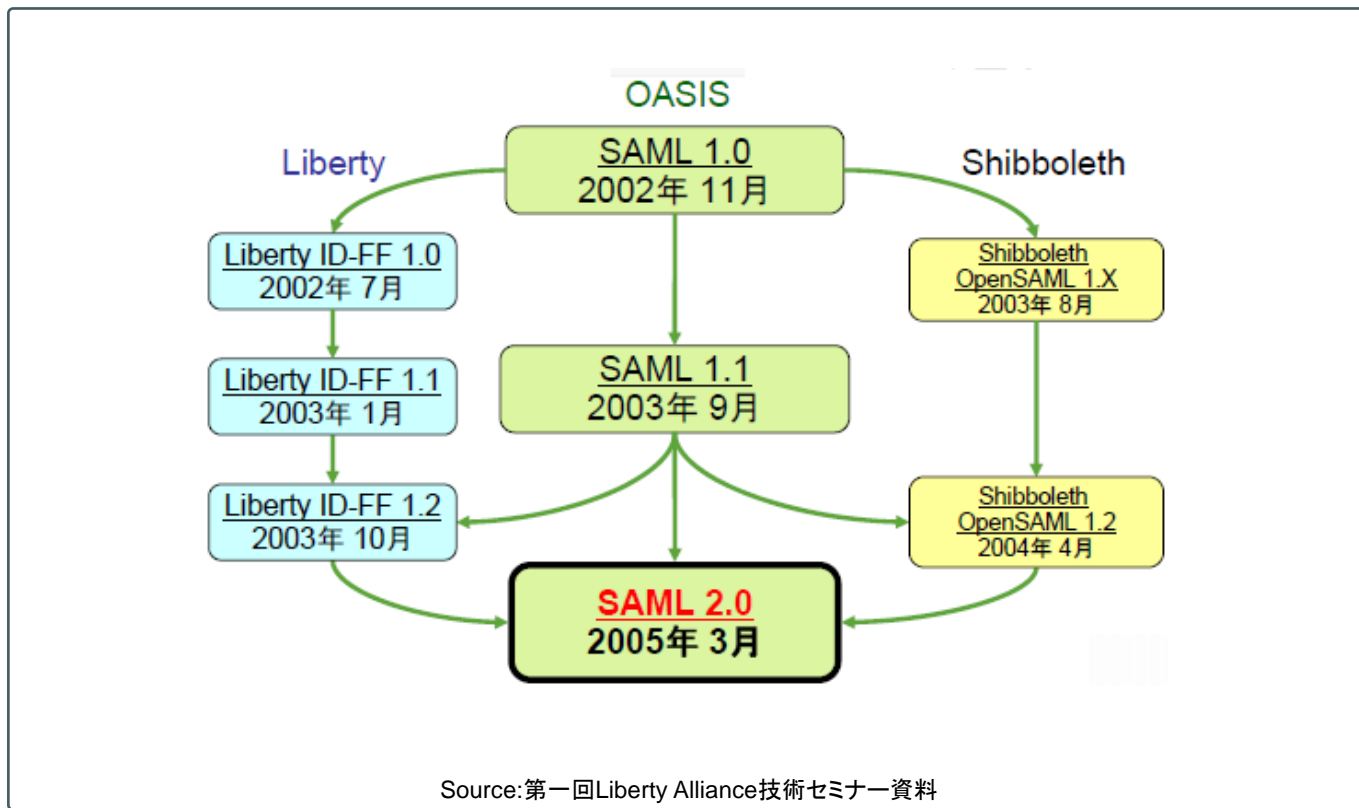
図2 アイデンティティ連携方式における処理手順の概要

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))



# Liberty ID-WSF

(アイデンティティWebサービス・フレームワーク)

リバティ・  
アイデンティティ  
連携フレームワーク  
(ID-FF)

アイデンティティ/  
アカウントリンケージ、  
シングルサインオン、  
およびセッション管理等の  
特徴を持つアイデンティティ  
連携と管理が可能

リバティ・アイデンティティサービス・  
インターフェース仕様 (ID-SIS)

パーソナルプロフィールサービス、アラートサービス、  
カレンダーサービス、コンタクトサービス、  
位置情報サービス、プレゼンスサービス等の  
アイデンティティサービスが可能

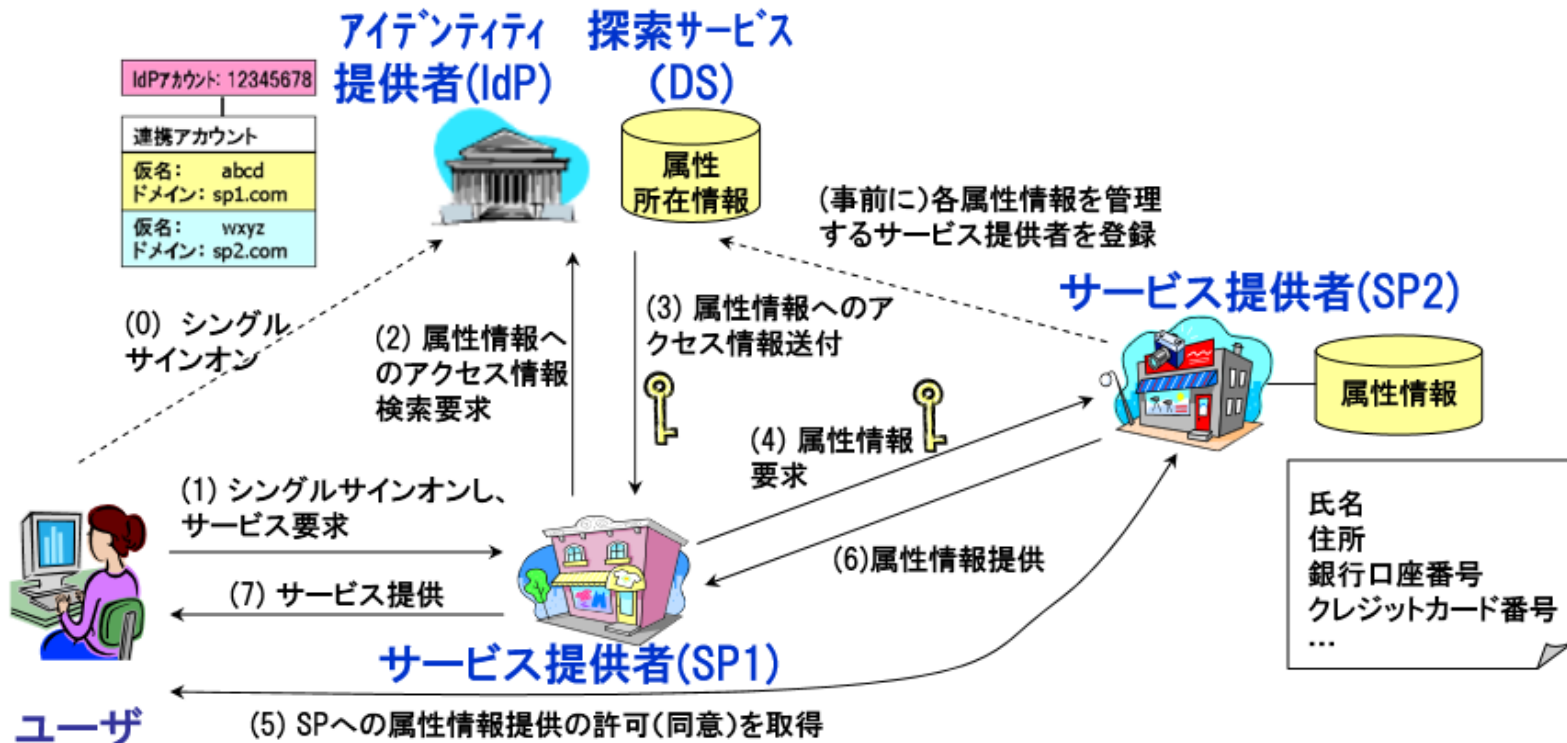
リバティ・アイデンティティ Web サービス・  
フレームワーク (ID-WSF)

相互接続可能なアイデンティティサービス、許可  
ベースの属性共有、アイデンティティサービス記述、  
インタラクション・サービス、ディスカバリ・サービス、  
および関係するセキュリティプロファイルを  
作成・構築するためのフレームワークを提供

リバティ仕様は既存の標準仕様に準拠  
(SAML, SOAP, WSS, XML, etc.)

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

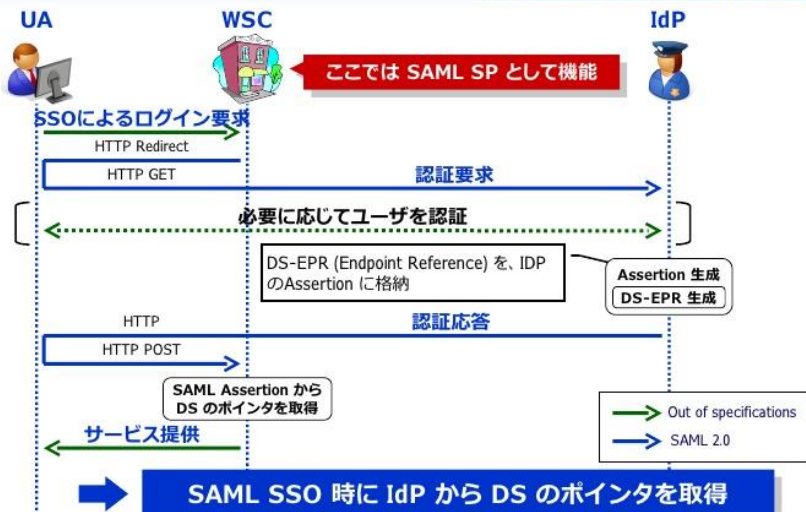


Source: リバティ・アライアンスの取組みについて <http://www.kantei.go.jp/jp/singi/it2/nextg/meeting/dai7/siryou4.pdf>

# ID-WSFのシーケンス

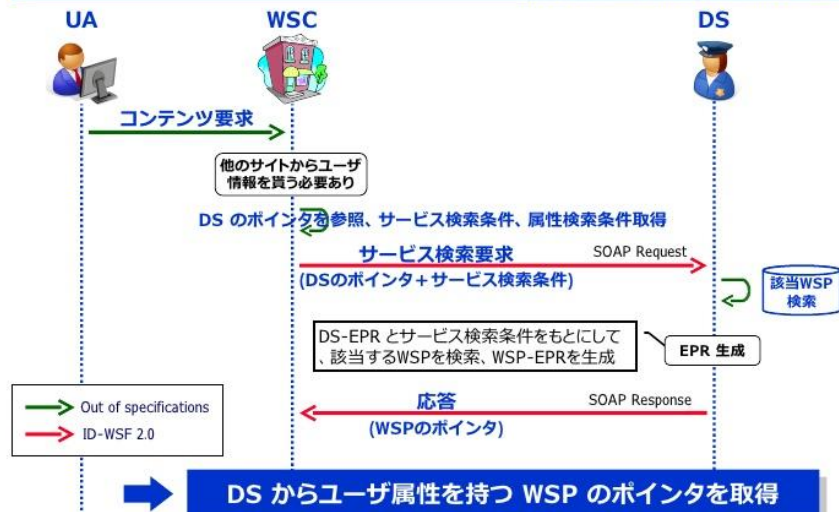
### 3.3. 誰がこの人の属性を知っていますか? [1/2]

NTT Information Sharing Platform Laboratories.



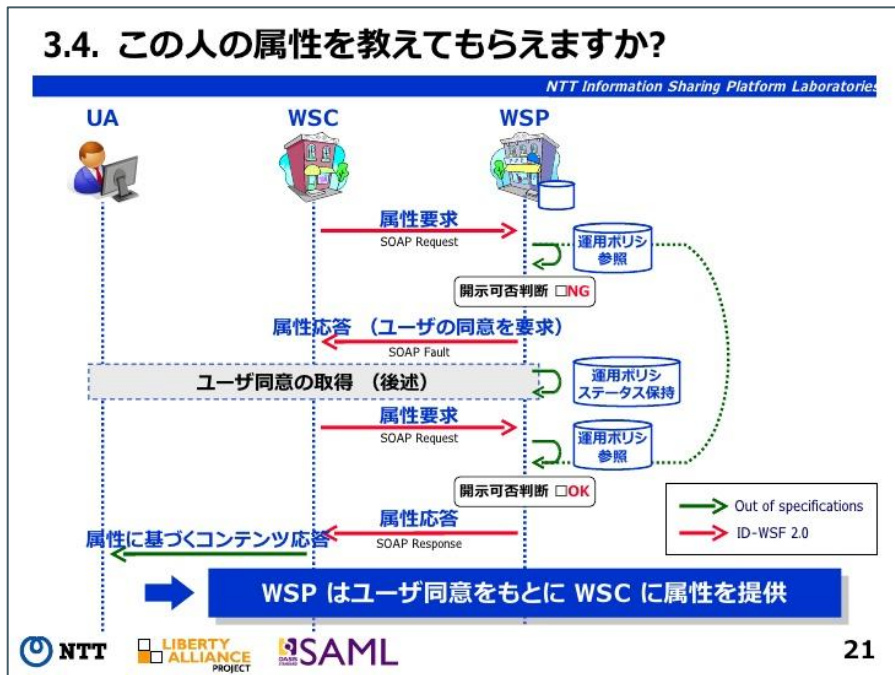
### 3.3. 誰がこの人の属性を知っていますか? [2/2]

NTT Information Sharing Platform Laboratories

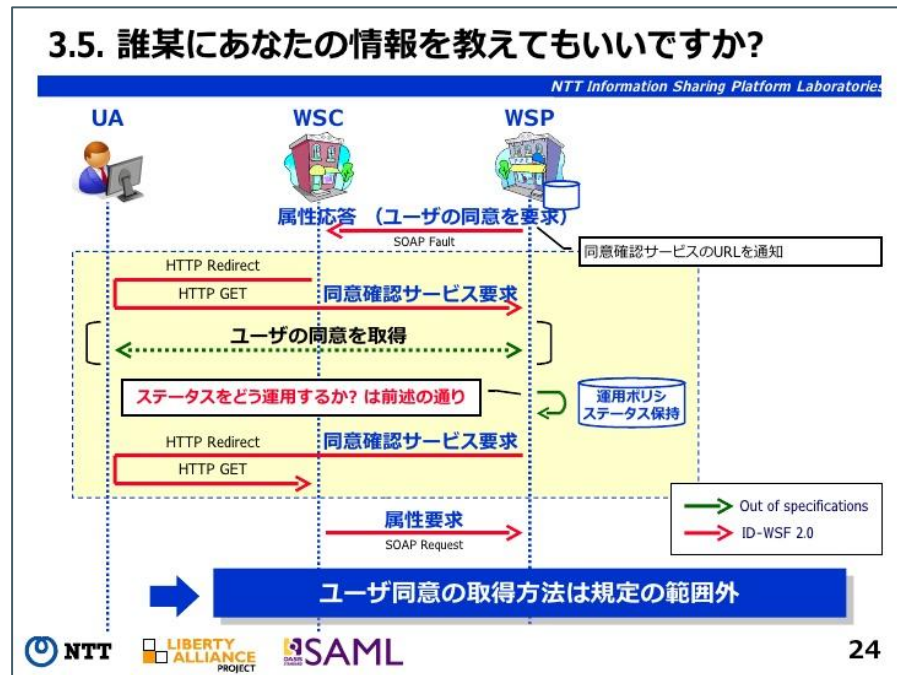


# ID-WSFのシーケンス (cont.)

## 3.4. この人の属性を教えてくださいか?



## 3.5. 誰某にあなたの情報を教えてもいいですか?



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

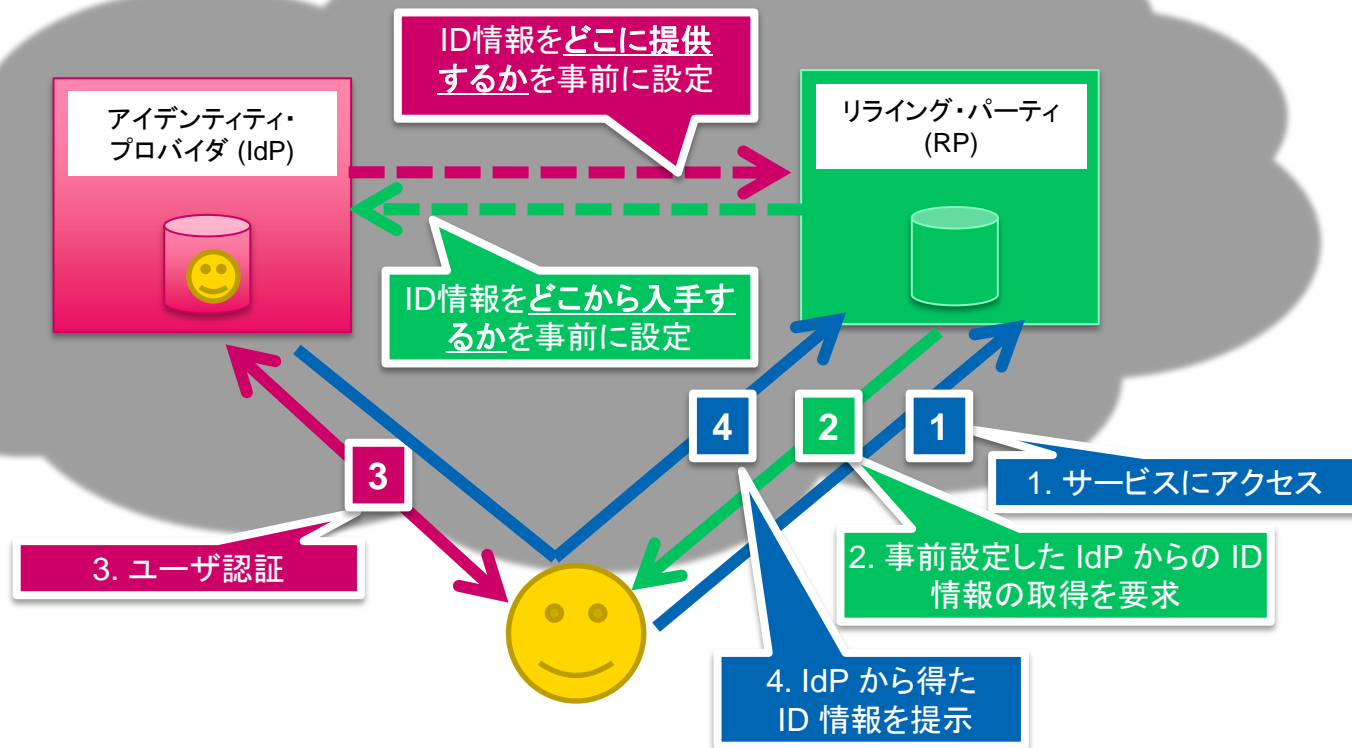


# けっきょくID-WSFは普及しなかった

---

- 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 → (以下繰り返す)

# 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”

Kim Cameron's

## Laws of Identity

### 1 User Control and Consent

Technical identity systems must only reveal information identifying a user with the user's consent.

### 2 Minimal Disclosure for a Constrained Use

The solution which discloses the least amount of identifying information and best limits its use is the most stable long term solution.

### 3 Justifiable Parties

Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship.

### 4 Directed Identity

A universal identity system must support both "omni-directional" identifiers for use by public entities and "unidirectional" identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

### 5 Pluralism of Operators and Technologies

A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers.

### 6 Human Integration

The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

### 7 Consistent Experience Across Contexts

The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.



Elkan / Alatan

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

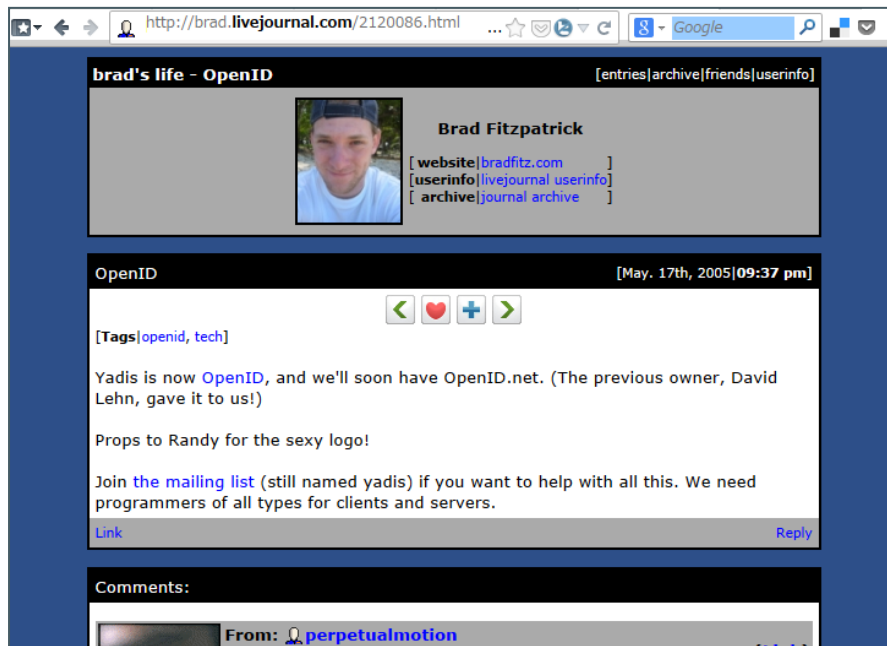
# 「ユーザーセントリック・アイデンティティ」

---

## ■ユーザーがコンテキ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

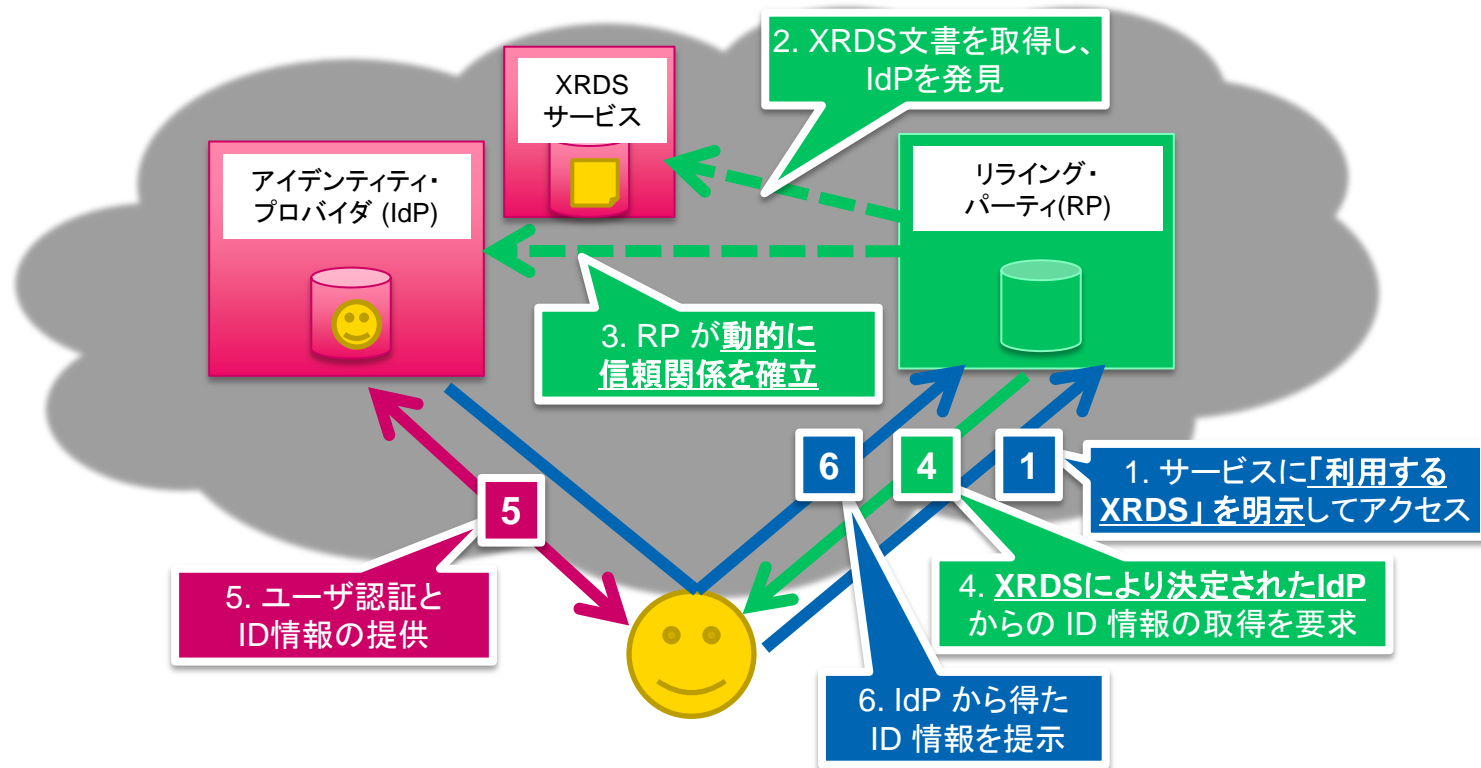
---

- 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](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？

---

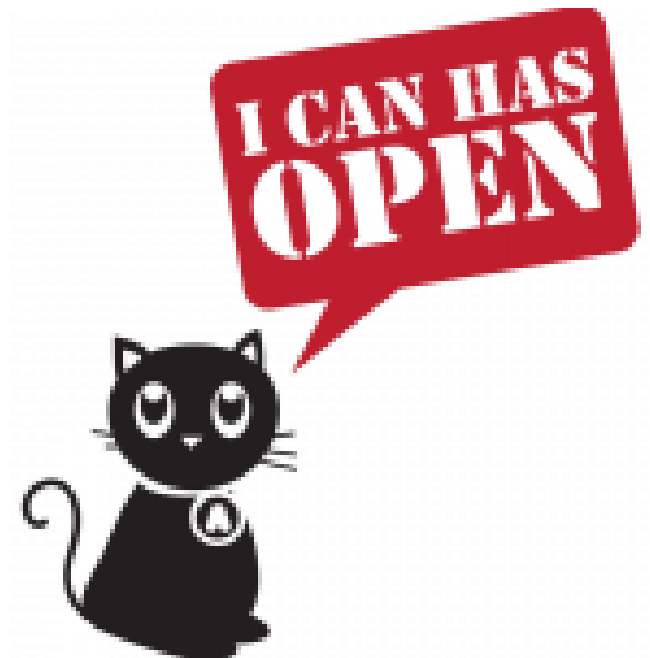
- We want something like Flickr Auth / Google AuthSub / Yahoo! BBAuth, but published as an open standard, with common server and client libraries, etc. The trick with OpenID is that the users no longer have passwords, so you can't use basic auth for API calls without requiring passwords (defeating one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

---

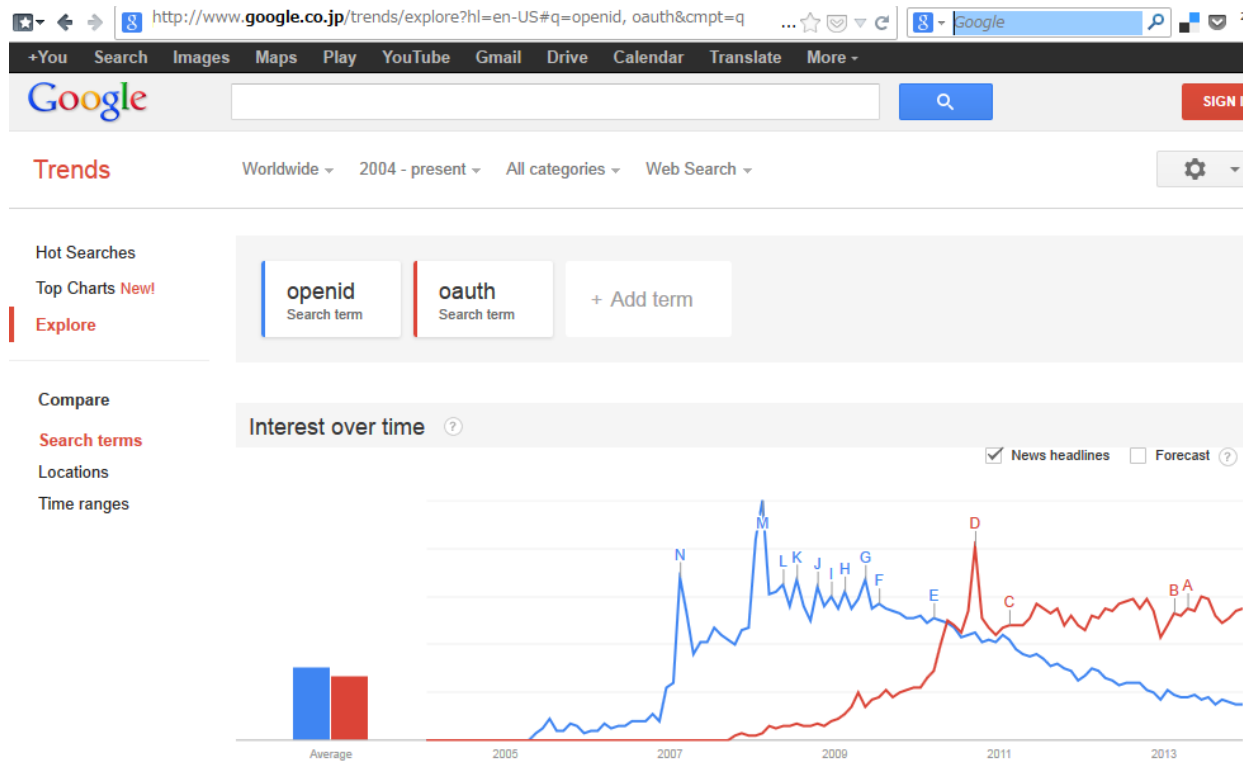
## ■ ユーザー認証に使うケースも

- 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

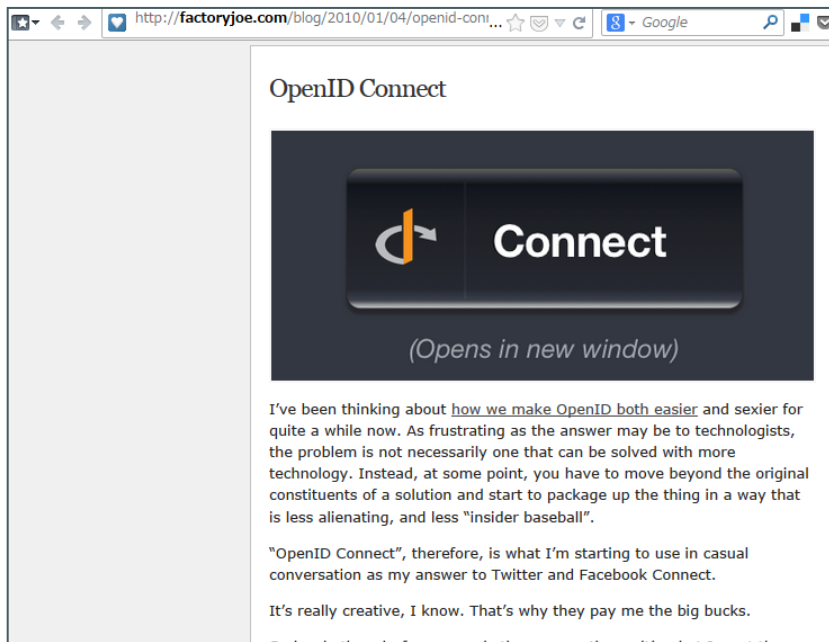
- OAuth WRAP → OAuth 2.0へ
- Facebookも乗ってきた

# OpenID < OAuth



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

# 「(旧) OpenID Connect」



Source: FactoryCity » OpenID Connect

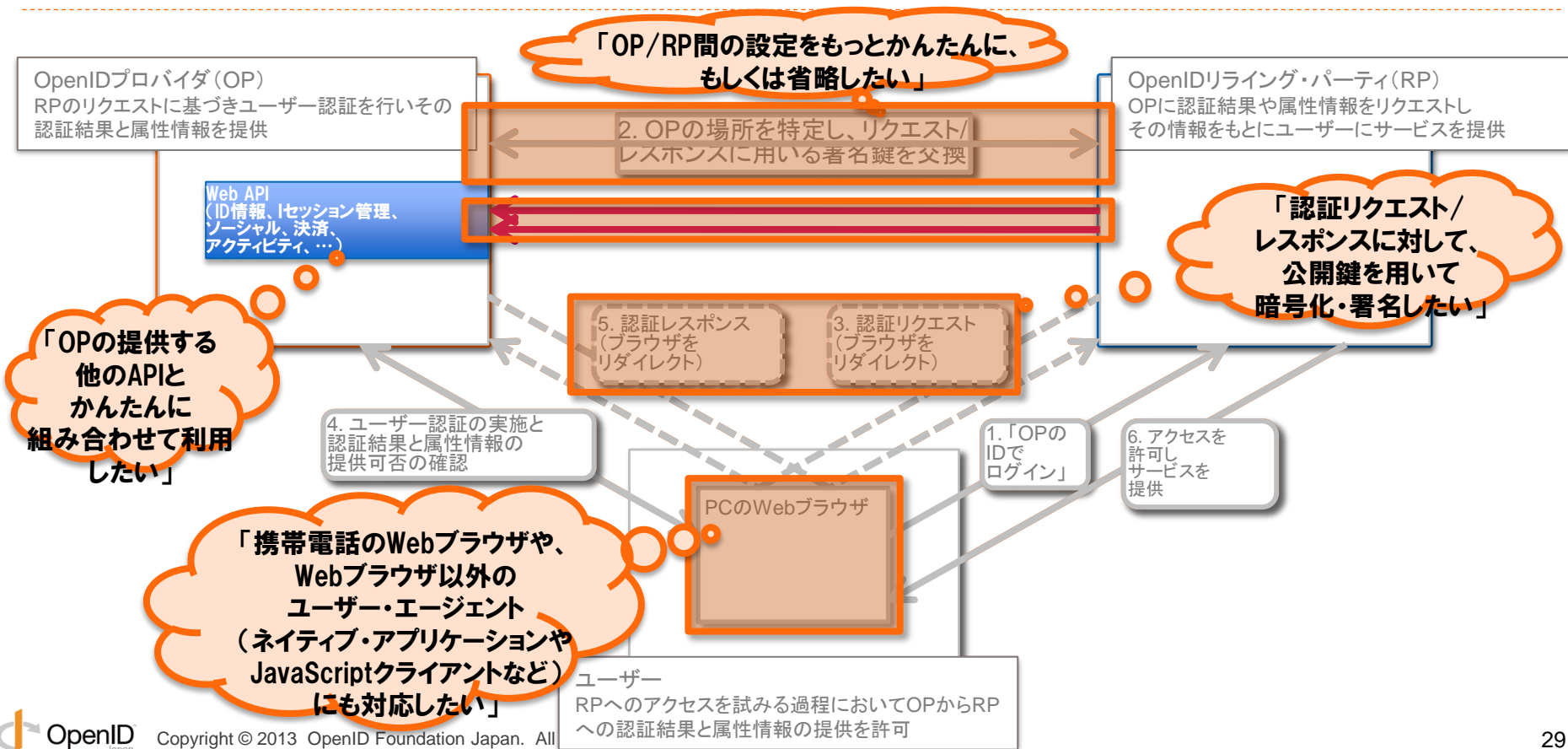
<http://factoryjoe.com/blog/2010/01/04/openid-connect/>



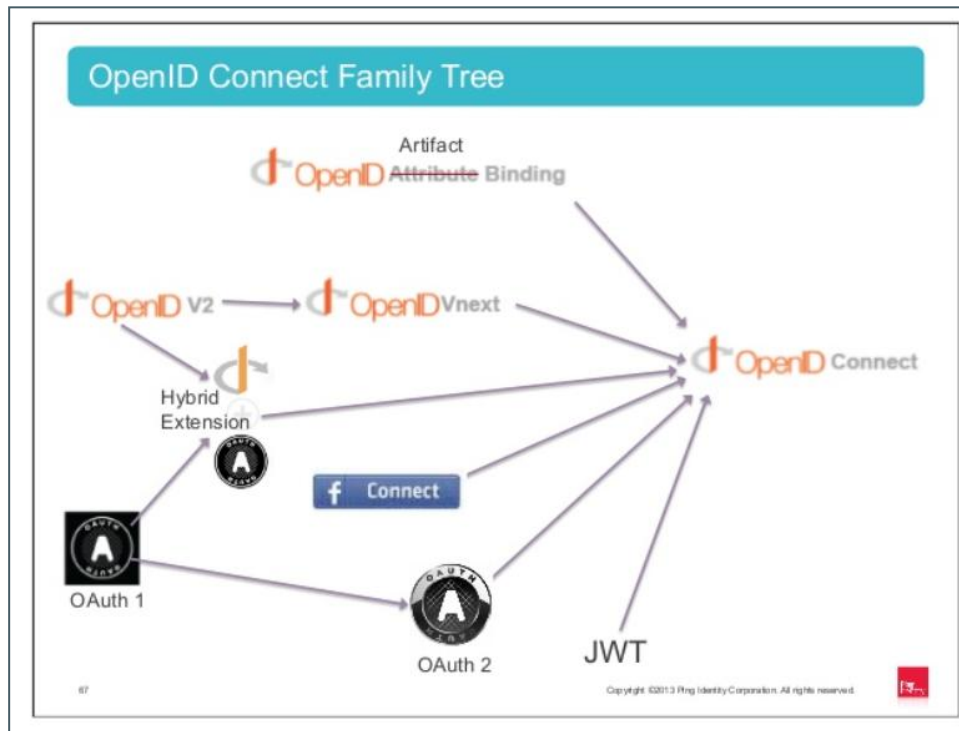
Source: OpenID Connect

<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”



OAuth 2.0による  
API認可と統合

認可リクエスト/APIアクセス



認証結果/属性情報提供

リライディング・パーティ  
(RP: ID情報要求側)

Webアプリ  
ケーション



モバイル  
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

JWT \* によって  
セキュアにID情報を提供

\* JSON Web Token

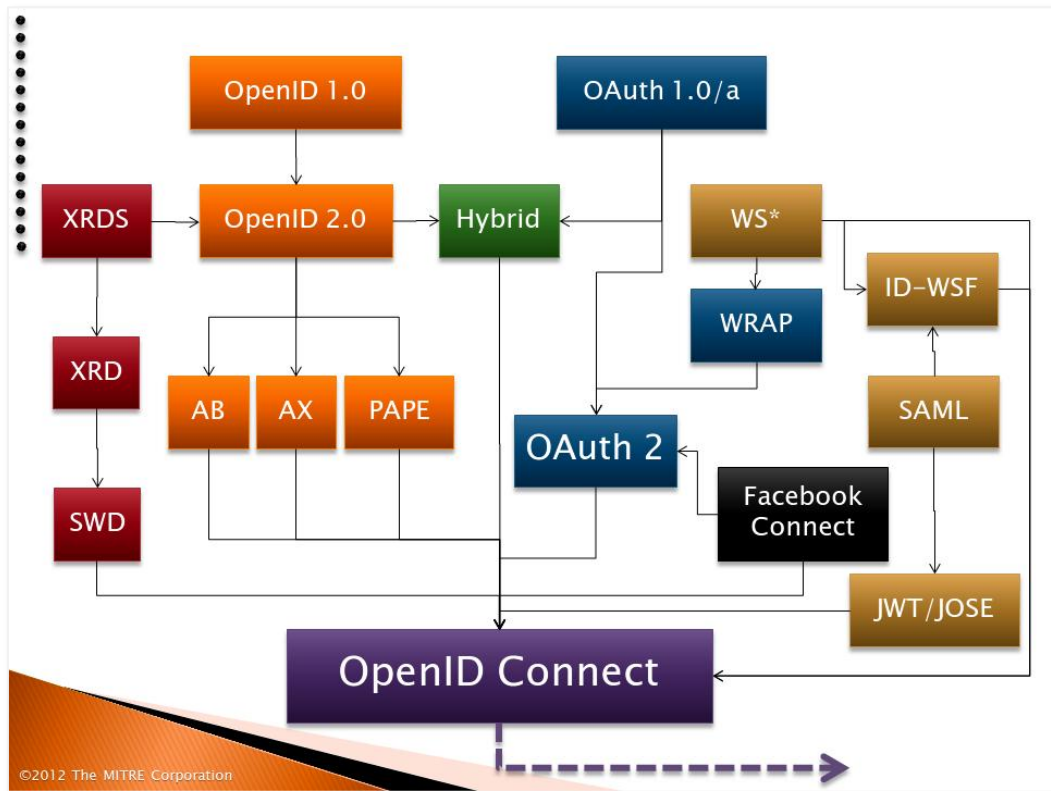
ネイティブ(non-Web)  
アプリでも利用可能

OpenID  
Connect  
対応製品が  
続々登場

携帯端末がIdPに!



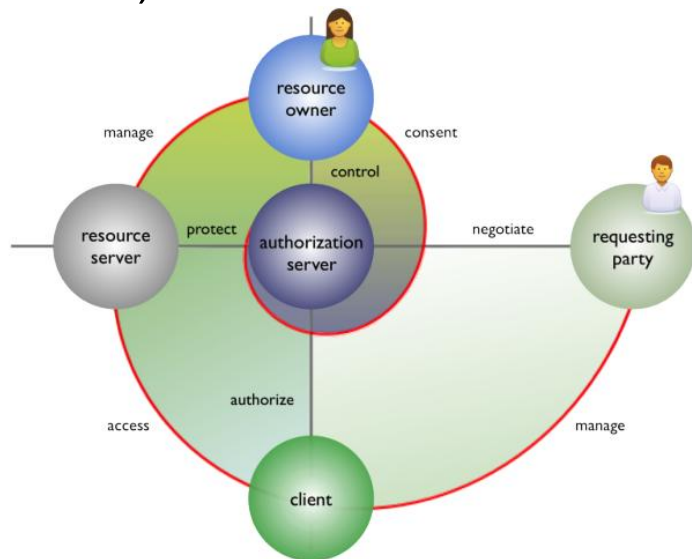
# 主要ID/API連携仕様がすべてOpenID Connectに収斂



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

# 再び Identity First へ

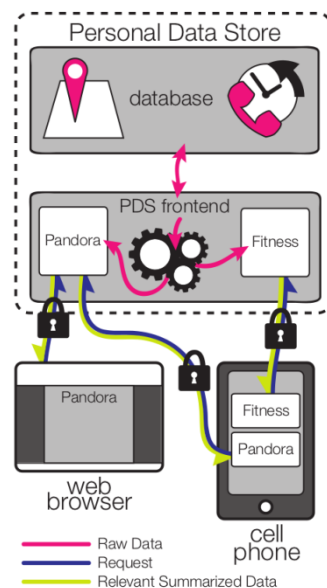
## ■ UMA (User Managed Access; ウーマ)



Source: [WG-UMA] New "UMA 101" slides available on the wiki

<http://kantarininitiative.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そのサービス





OpenID<sup>TM</sup>  
Japan