野村総合研究所

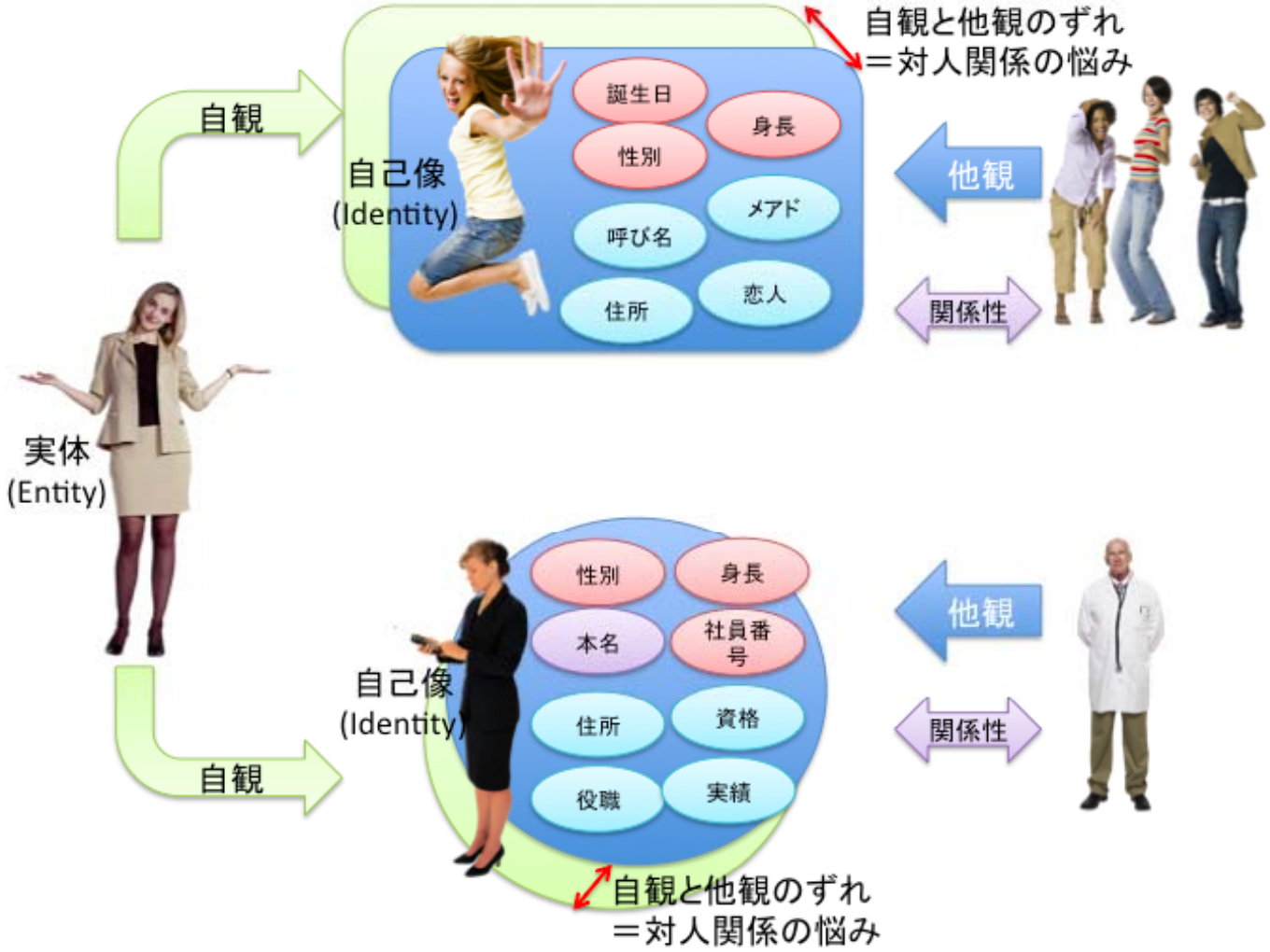
Internet Week 2011S5

デジタル・アイデンティティに関するホットトピック

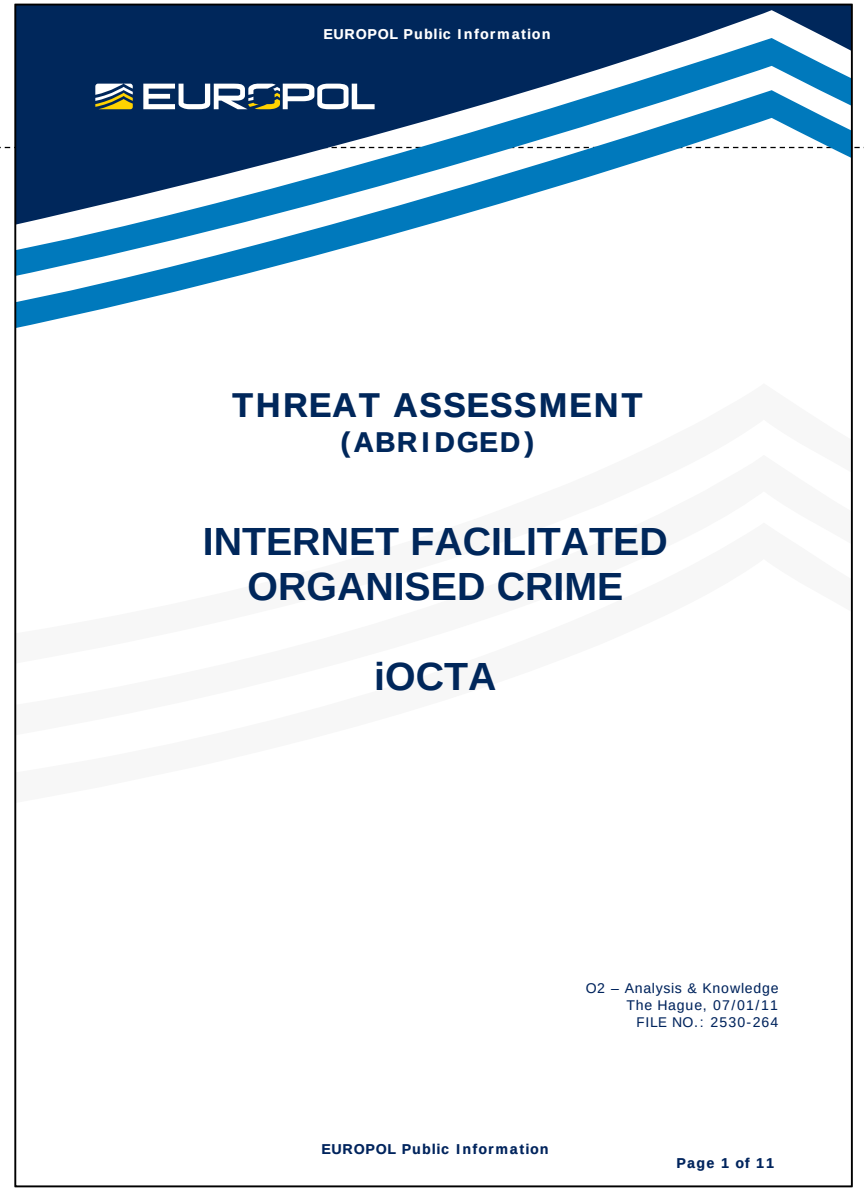
2011年11月30日

株式会社野村総合研究所
崎村 夏彦
（米OpenID Foudation理事長）

「Identity」＝そのEntityに関係する属性の集合



重要なの？



ID詐欺＝EUの主要な犯罪要因

McAfeeの試算(2009)＝$1兆（約100兆円）の被害

英国だけの被害＞€700億

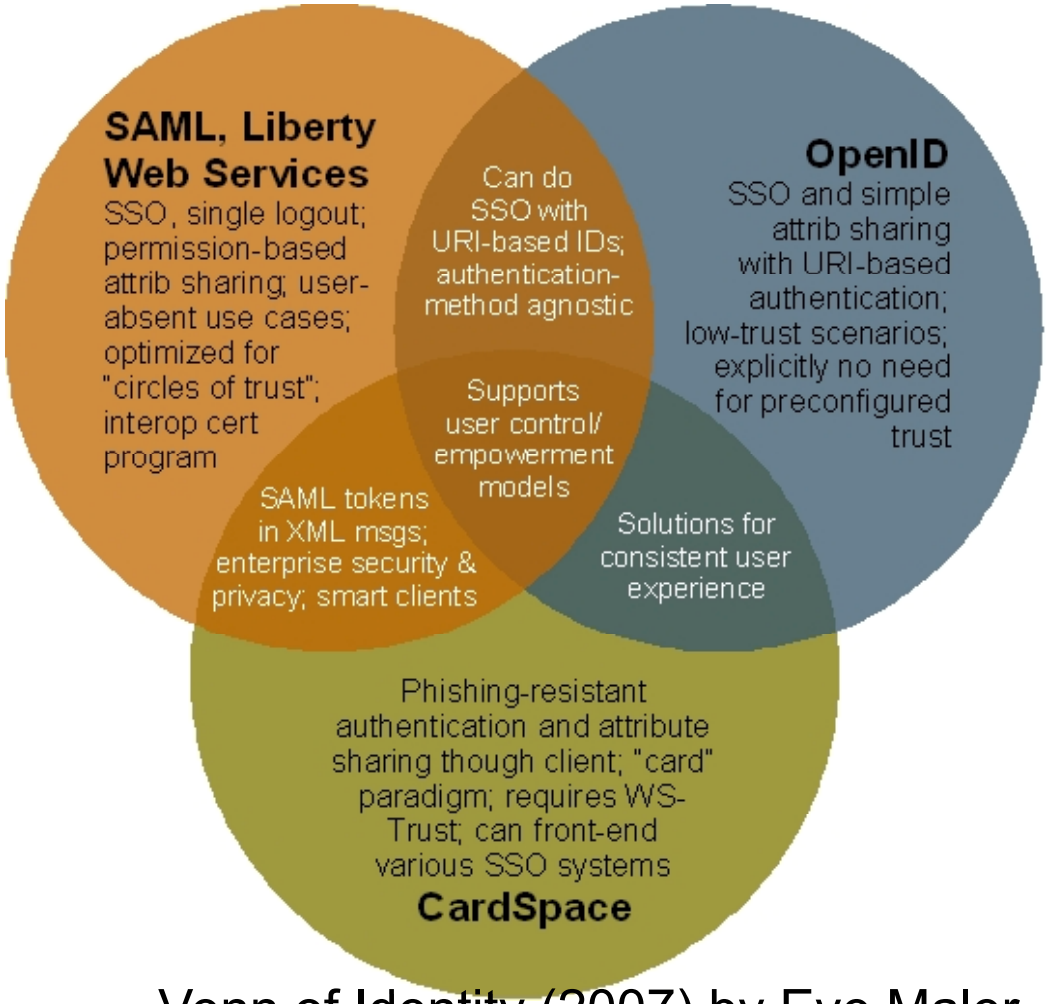
EU全体の被害＞ギリシャ＋ポルトガル+の救済費用

なんとかしなきゃ！

（出所）Europol “Threat Assessment – Internet Facilitated Organised Crime”(2011) File No. 2530-264

アイデンティティ三国志？

- SAML 2.0
- OpenID
- InfoCard



Venn of Identity (2007) by Eve Maler
http://www.xmlgrrl.com/blog/2007/03/28/the-venn-of-identity/

OpenID Connect Heralds the “Identity Singularity”

TABLE OF CONTENTS

- Security Pros Face An Increasingly Diverse Access Management Challenge
- OpenID Connect Stuffs Many Identity Features Into A Single Simple Package
- SAML Will Fade Away, But The Process Won’t Be Painful

by Eve Maler
Forrester

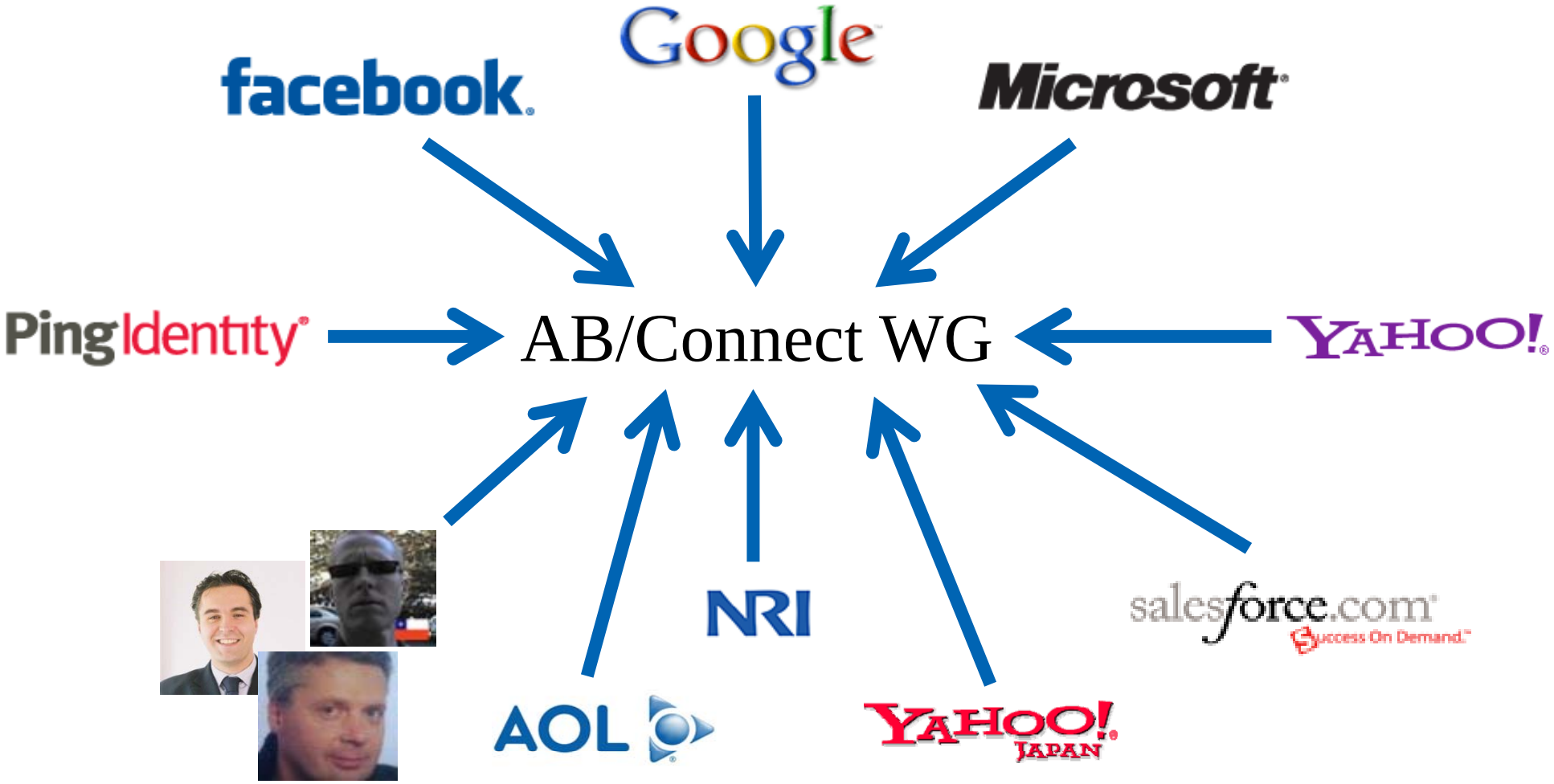
RECOMMENDATIONS

- Look To OpenID Connect When SAML Doesn’t Do The Trick
- WHAT IT MEANS
- Evolution Is Healthy For Federated IAM And Other Loosely Coupled Things

中華統一の声が
聞こえる？

http://www.forrester.com/rb/Research/openid_connect_heralds_identity_singularity/q/id/60893/t/2

Working Together



設計方針

簡単なことは簡単に

複雑なことも可能に

モジュラー・デザイン

簡単なことは簡単に

標準化された UserInfo APIを通じた シンプルな “Connect” 機能

モバイル環境のサポート

どうやって簡単に？

- OAuth 2.0ベース
- JSONの活用
- JSON Web Token（JWT）claims 形式

- Goal: 全ての現代的なWebプラットフォームで容易に実装できること

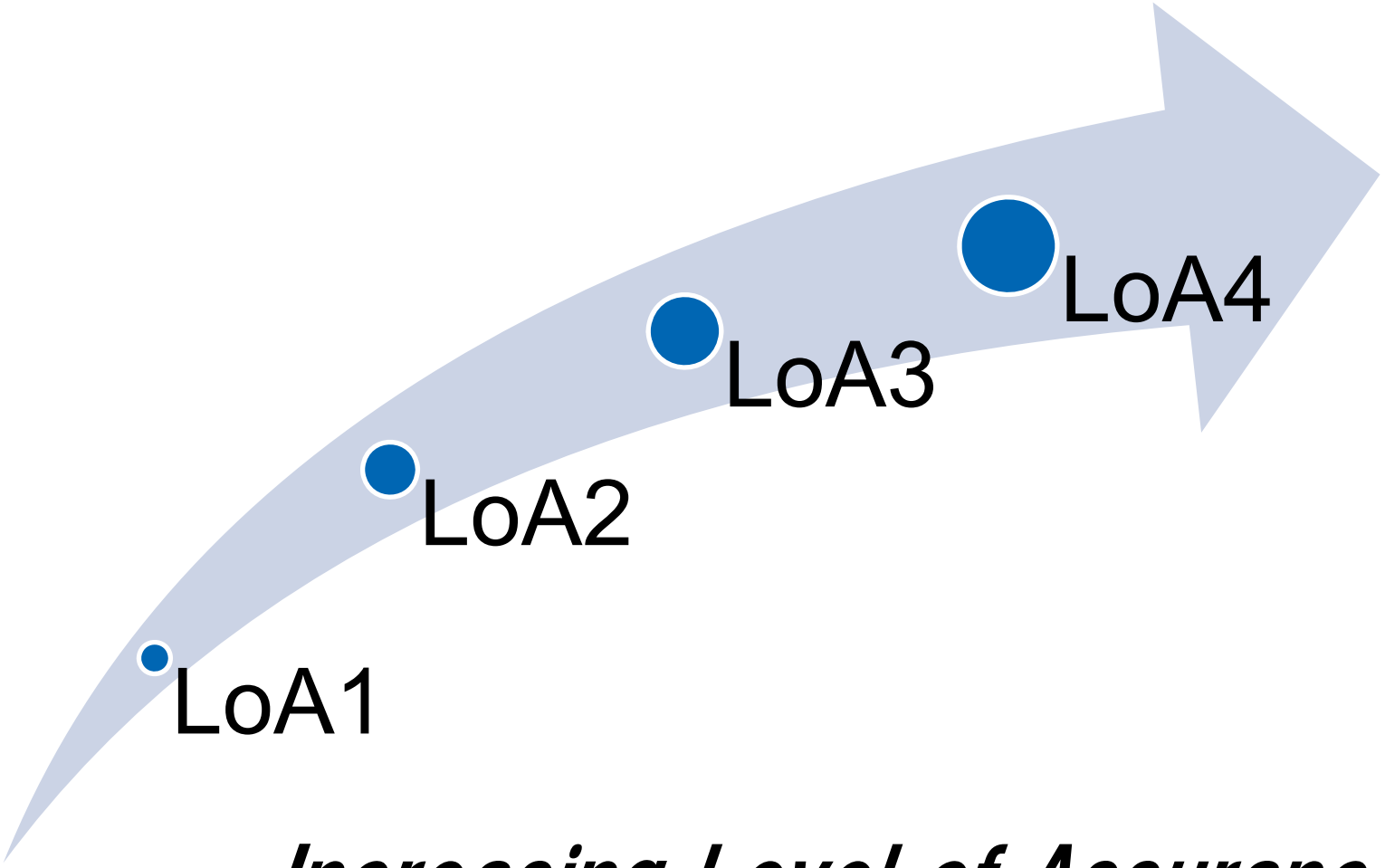
複雑なことも可能に

幅広いセキュリティレベルへの対応

Claims 集約

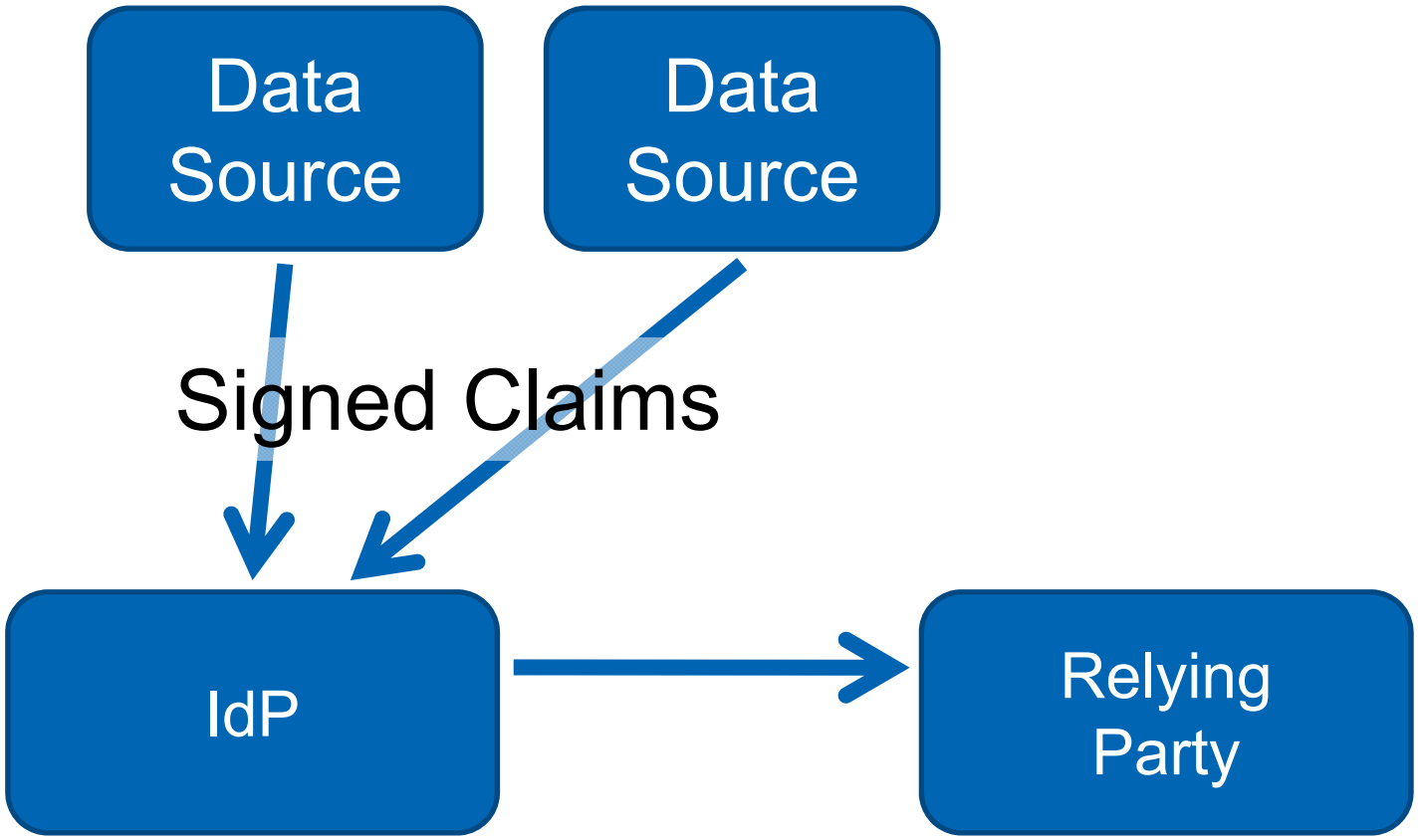
分散 Claims

幅広いセキュリティレベルへの対応

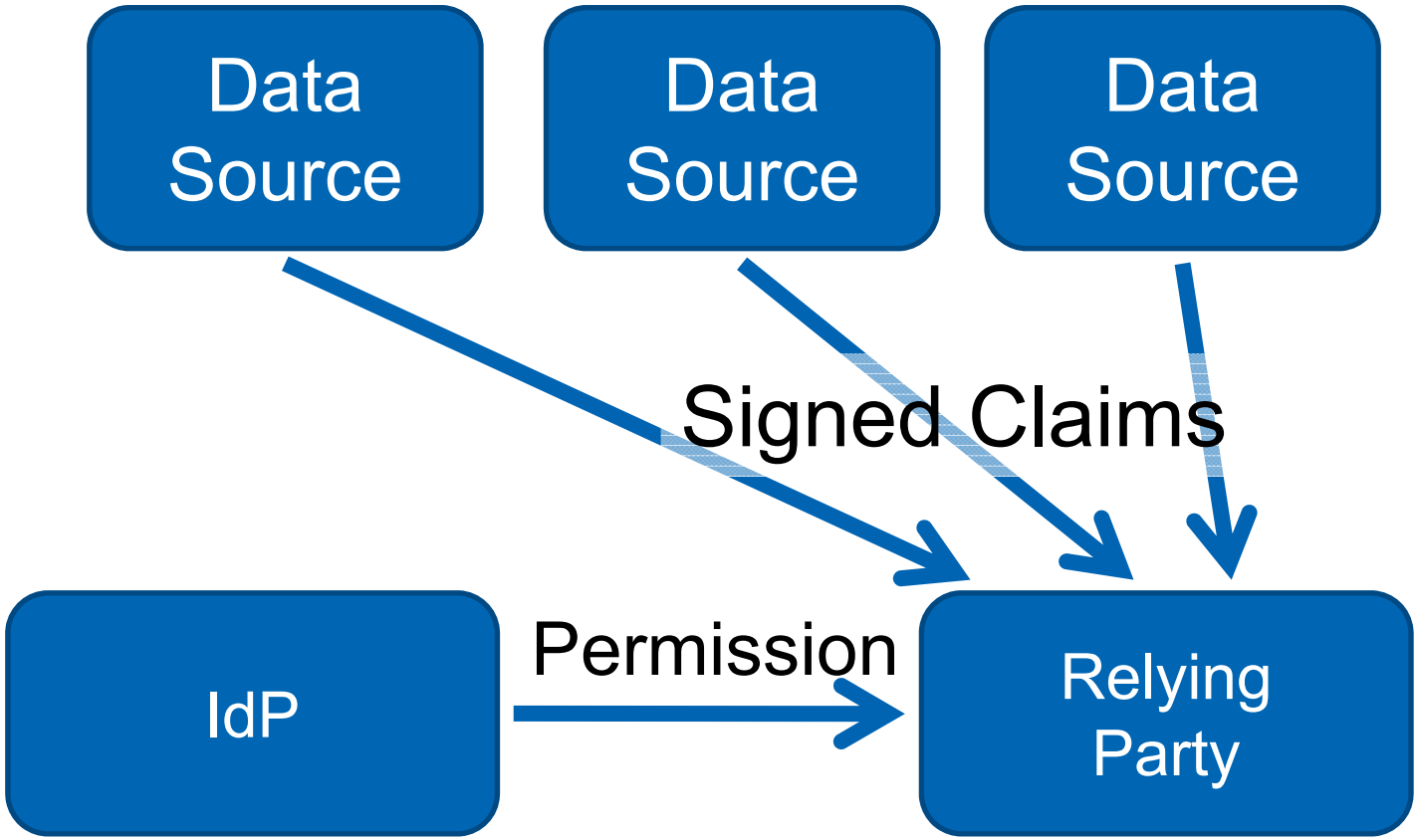


Increasing Level of Assurance →

Claims 集約



分散Claims



Better scalability, etc.

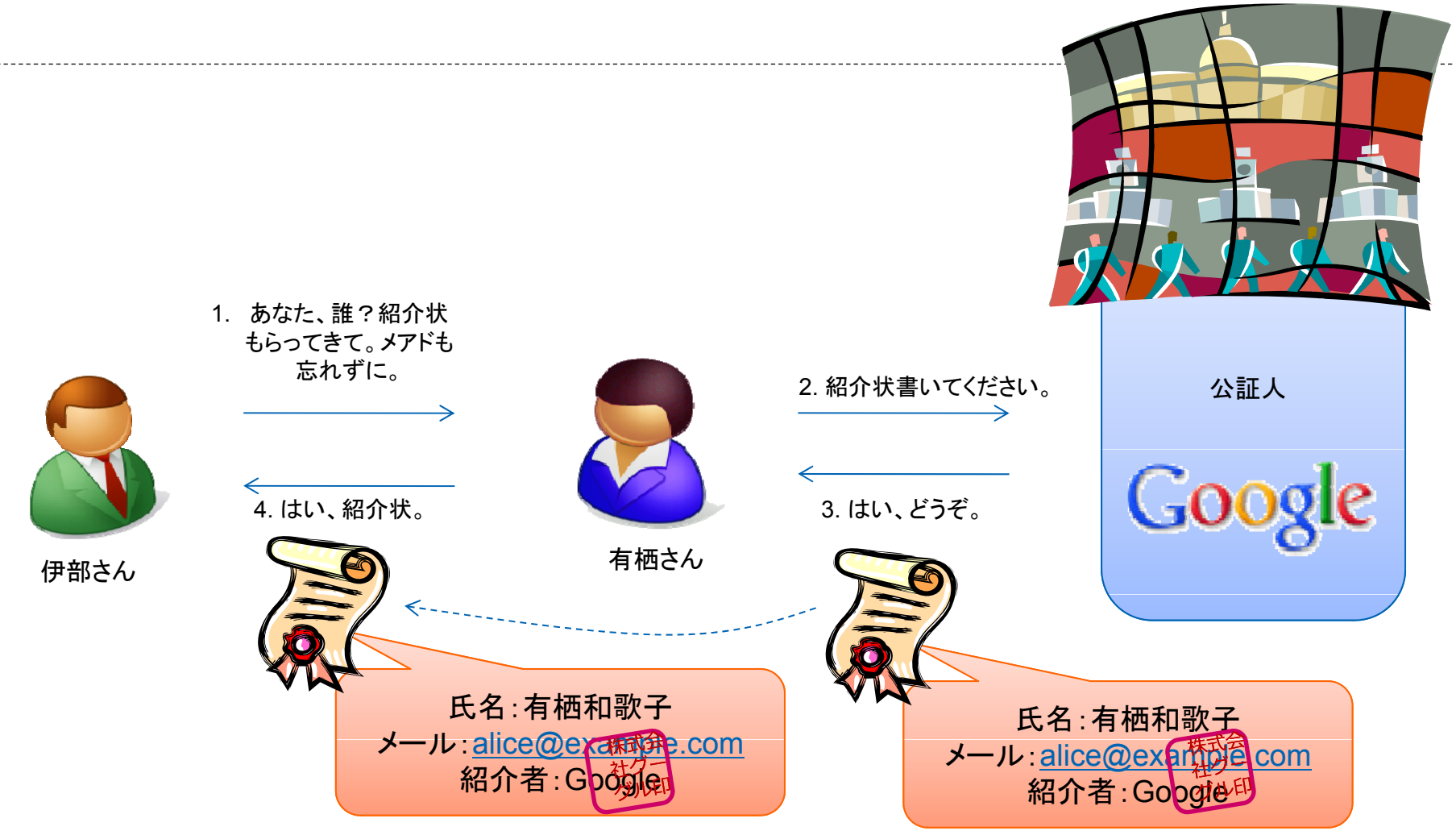
Connect Suite

- Messages（End point とメッセージを定義）
- Standard（OAuth 2.0 Core Binding）
- Basic Client Profile
- Registration
- Discovery

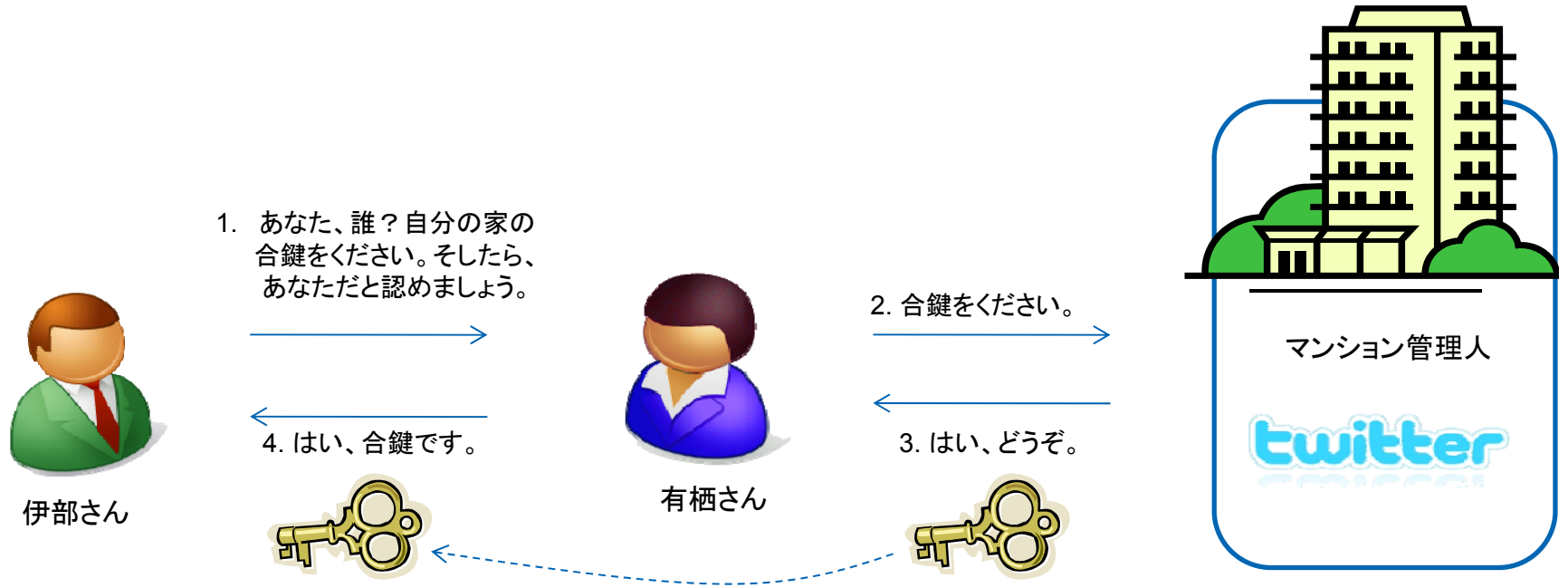
WHY NOT JUST OAUTH 2.0?

http://www.sakimura.org/2011/05/1087/

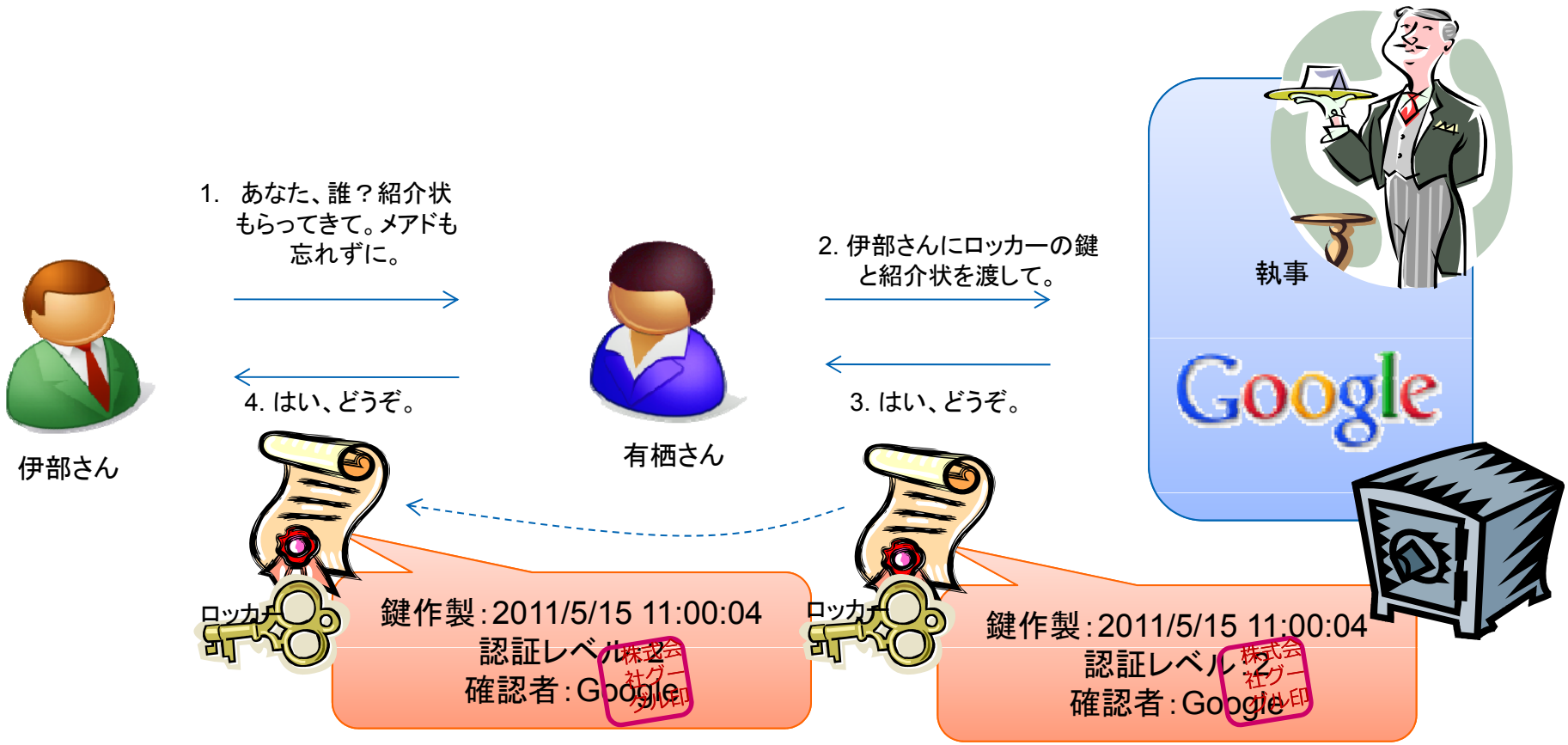
OpenID認証(身元確認)の場合



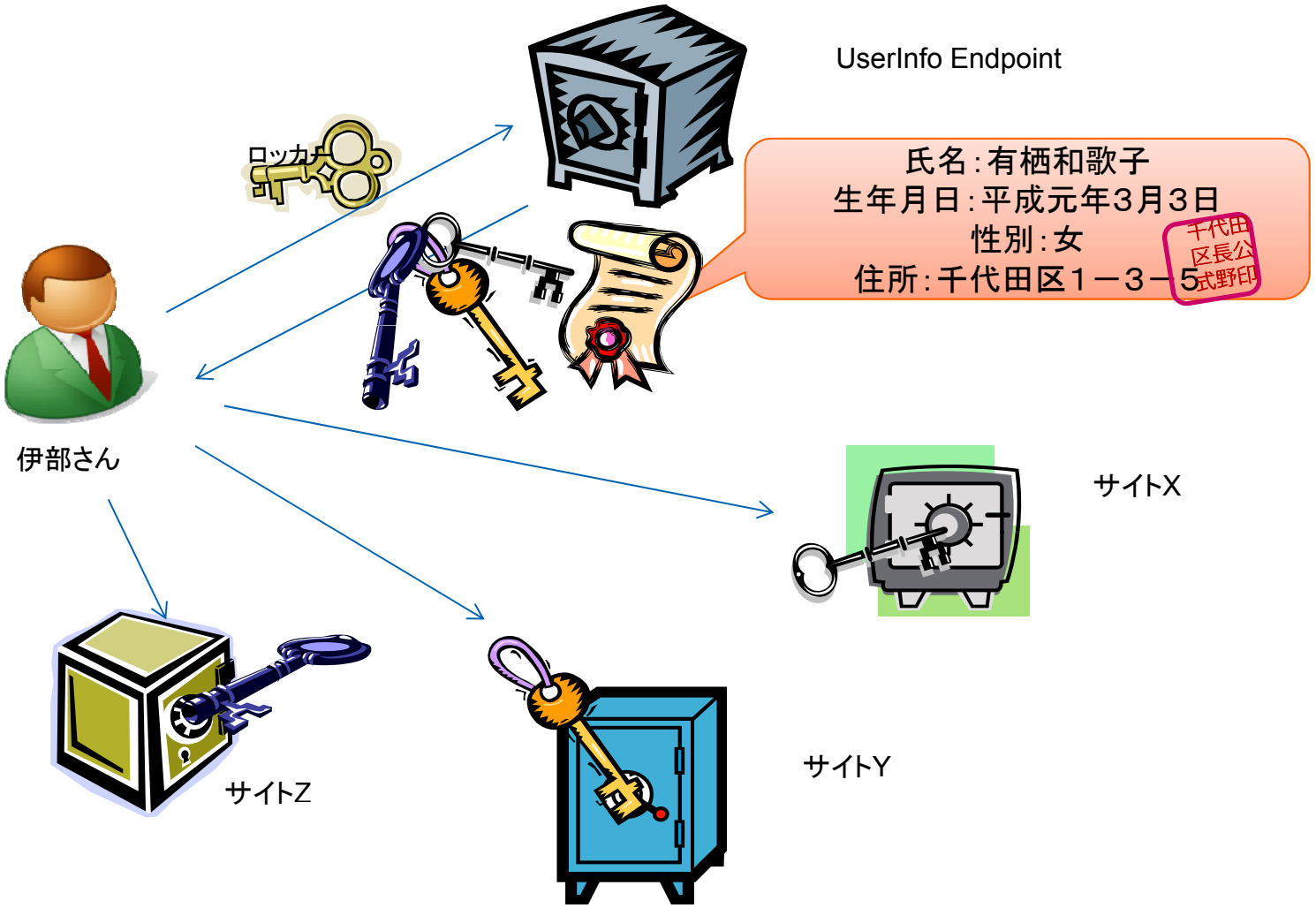
OAuthで身元確認もどきをする場合



OpenID Connectの場合



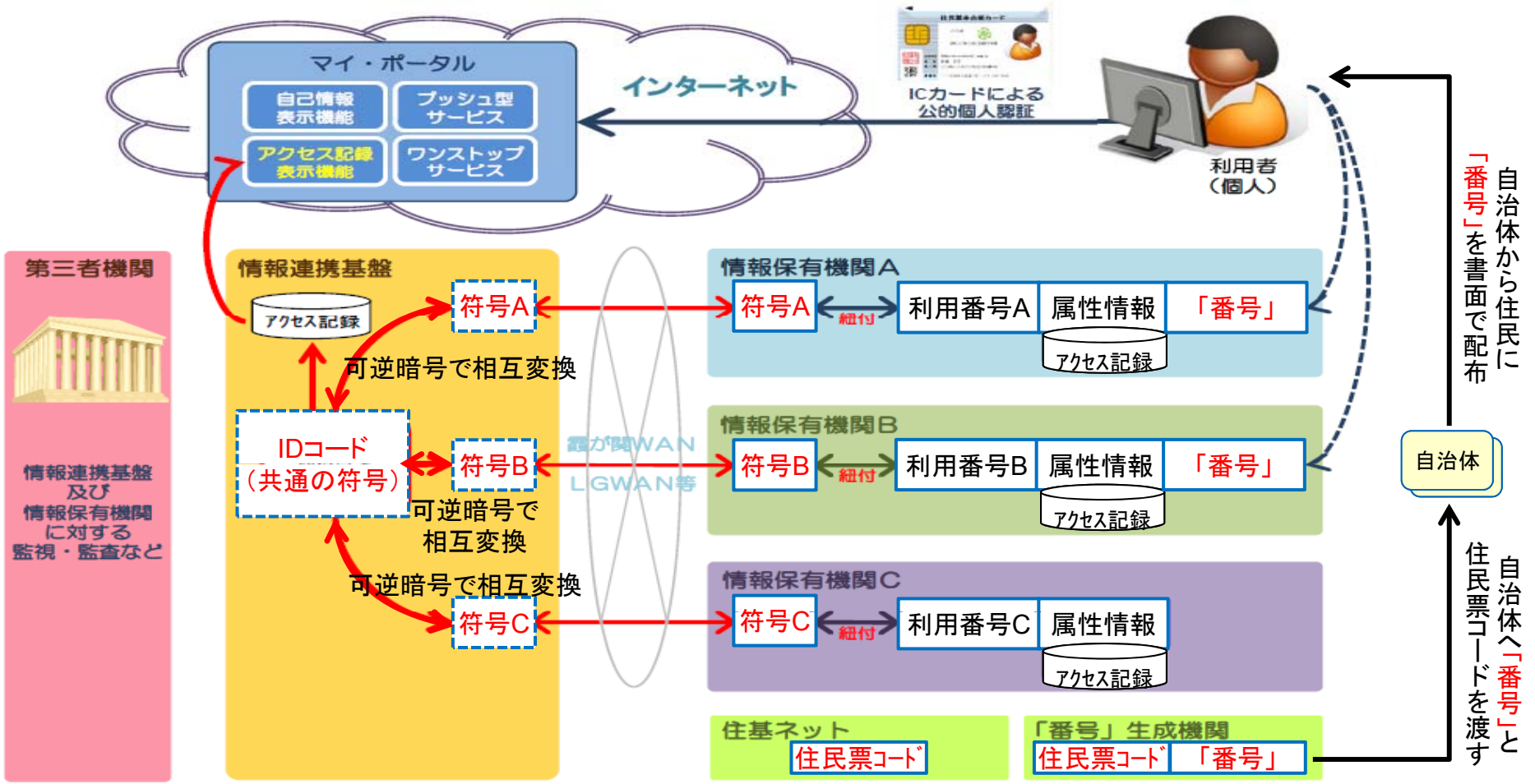
OpenID Connectのクレーム集約、分散クレーム



バックエンドもできます

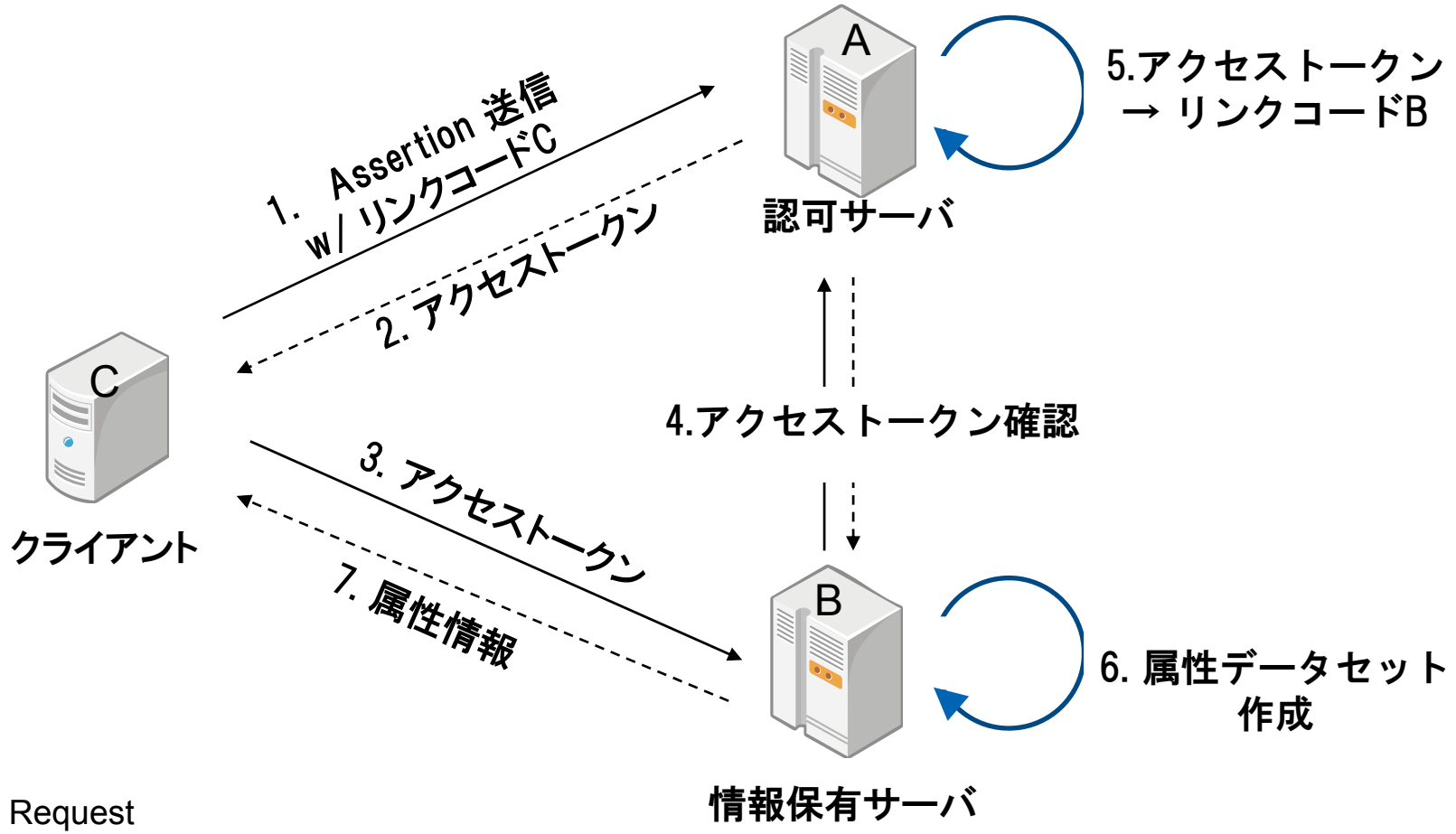
例えば、今話題の情報連携基盤で考えると…

情報連携基盤とは？



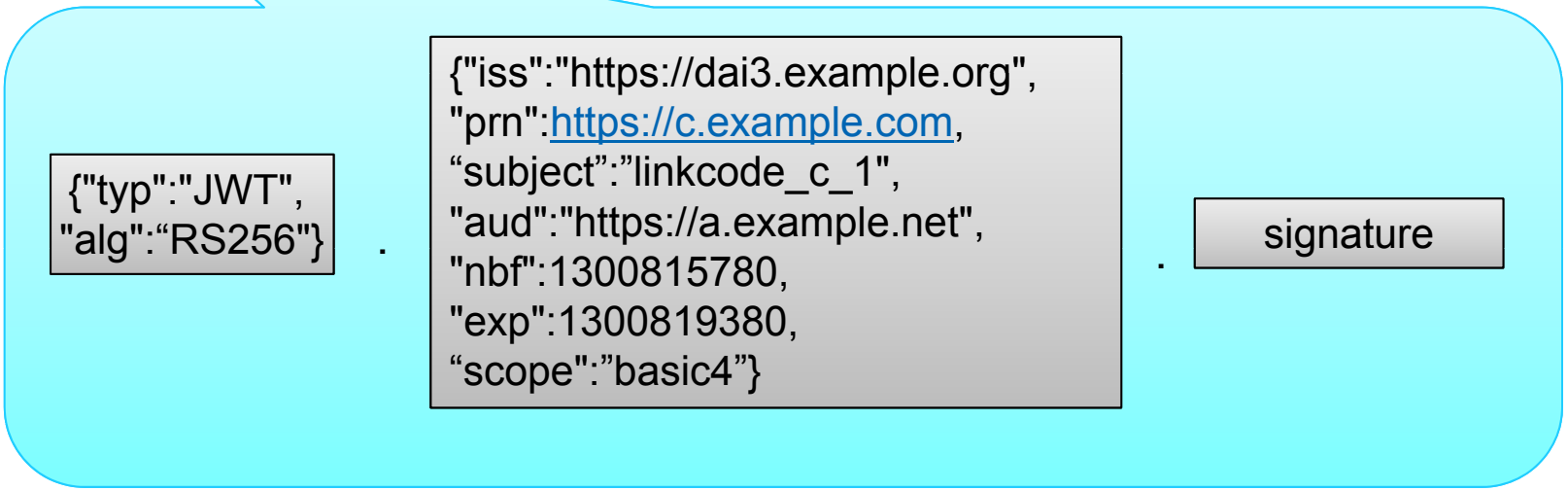
（出所）内閣官房資料

まずは、データ取得フロー



1. access_token request

```
POST /token HTTP/1.1
Host: a.example.net
Content-Type: application/x-www-form-urlencoded

client_id=https%3A%2F%2Fc.example.com&
grant_type=urn%3Aietf%3Aparams%3Aoauth%3Agrant-type%3Ajwt-bearer&
assertion=jwt.assertion.here
```



みたいな…

2. Access Token Response

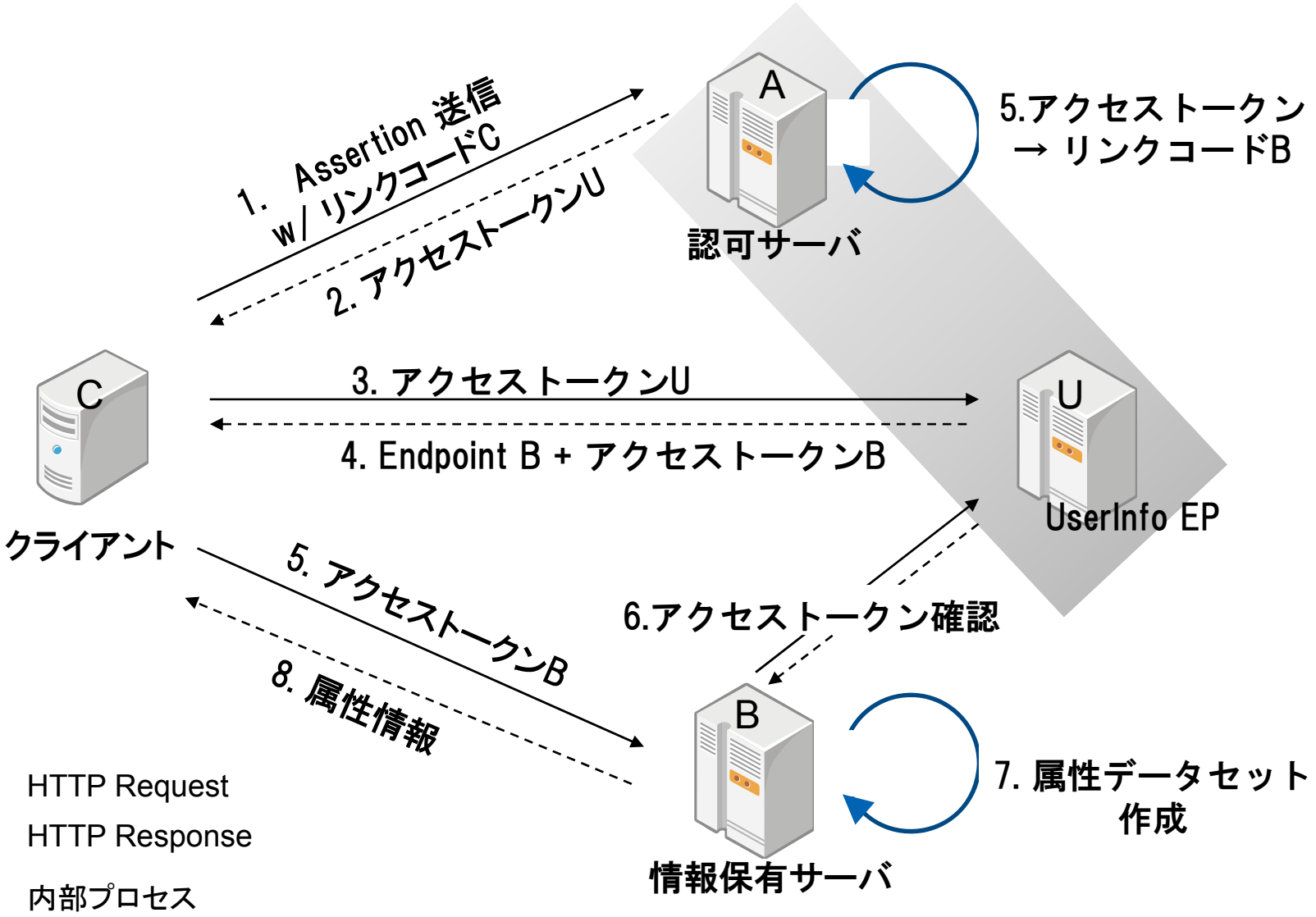
```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Cache-Control: no-store
Pragma: no-cache

{ "access_token":"2YotnFZFEjr1zCsicMWpAA",
"token_type":"example",
"expires_in":3600}
```

サーバがState を持ちたくない場合、ここに必要な情報を埋め込んでしまってOK。

みたいな…

あ、でも どこにデータがあるか分からないや…

ConnectのDistributed Claim を使えばOK



4. UserInfo Response

```
HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8

{
  "_claim_names": {
    "name": "src1",
    "address": "src1",
    "birthday": "src1",
    "gender": "src1" },
  "_claim_sources": {
    "src1": {
      "endpoint": "https://b.example.com/data",
      "access_token": "ksj3n283dke"}
  }
```

これらのデータは

ここから取れますよ！

みたいな…

なんか、できそう！

他に何がいるか？

Client関係

- Client Registration（初期/変更）→ Connect Registration 使えそう
- Assertion 取得 → これは新規
- Log 書き出し → Syslog で良い？

市民Lifecycle関係

- 新規登録（出生時、海外からの転入）
- 住民票コード変更
- 居住市町村変更（IAA*変更）
- ステータス変更：active/archived/suspended

識別子情報関係

- リンクコード取得：基本4情報ないしは住民票コードを使って取得
- マイナンバー取得：同上

Etc.

* Identity Attribute Authority (cf. ISO/IEC 27460-1)

その他の関連規格

- IETF OAuth WG
  - OAuth Assertion Profile
  - JSON Web Token（JWT）
  - Simple Web Discovery（SWD）
  - Request by JSON for OAuth 2.0
- IETF JOSE WG
  - JSON Web Signature and Integrity（JWS）
  - JSON Web Encryption（JWE）
- Portable Contacts（PoCo）
- Simple Cloud Identity Management（SCIM）

ISO/ITU-T関連

- ISO/IEC 29100 Privacy Framework (FDIS)
- ISO/IEC 29101 Privacy Reference Architecture (CD4)
- ITU-T X.1251 | ISO/IEC 29115 Entity Authentication Assurance Framework (FDIS)
- ISO/IEC 24760 A framework for identity management Part 1: Terminology and Concepts (FDIS)
- ISO/IEC 24760 A framework for identity management Part 2: Reference framework and requirements (WD2)
- ISO/IEC 24760 A framework for identity management Part 3: Practice (WD2)
- ISO/IEC 29146 A framework for access management (WD6)
- ISO/IEC 29190 Privacy Capability Assessment Model (WD3)
- ISO/IEC 29191 Requirements for partially anonymous, partially unlinkable authentication (CD4)
- X.OITF Open Identity Trust Framework

ご清聴有り難うございました