野村総合研究所

OpenIDのモバイル対応
～ 認証基盤連携フォーラムの取組み他から

Nat Sakimura
Vice Chair, OpenID Foundation
Board Member, Kantara Initiative
Advisory Board Member, OIX

株式会社野村総合研究所
上級研究員　崎村夏彦

自己紹介

■OpenIDな人？

XRI(OpenID): =nat
Twitter: _nat
Web: http://www.sakimura.org/

■確かに…

- OpenID Foundation (米国)副理事長
- OpenIDファウンデーション・ジャパン発起人代表
- OpenID/PAPEの共同著者
- OpenID for Mobile (Artifact Binding) の共同著者

実際には

- 2000年くらいから Digital Identity に取り組む
- XDI.org 副理事長
- OASIS Open Reputation Management Systems TC共同議長
- Kantara Initiative 発起人＆ゴッドファーザー w
- Infocard Foundation のEDの Drummond Reed とは10年来の戦友
- Open Identity Exchange, Advisory Board Member
- 総務省：電子政府推進対応WG構成員

目的：

（自分のDigital Identity を自決する）

Power to the People を現実に！

OpenIDって、何？

OpenID（オープンアイディー）とはウェブサイトによらず使用できる認証システムの標準、およびそこで使用される識別子である。(wikipedia)

Digital Identity

- Subject/Entity に対応する、属性（形質、狭義の属性、関係性）の集合
  - Phill Windley著「Digital Identity」より

じぶん情報（Identity Attributes）

身元確認＝クレデンシャルなどを用いて、形質情報と本人とを比較して、本人と情報を結びつけること。

クレデンシャル（識別子）＋（パスワード、公的個人認証証明書、指紋、虹彩など）

自分だけが
・知っているもの
・持っているもの
・形質

Credential: An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person. Electronic Credential: Digital documents used in authentication that bind an identity or an attribute to a Subscriber's token.

Source: SP800-63rev1

生年月日、出生地 性別 苗字（出生時）・名前 肌の色・目の色・髪の色 身長・体重		形質 (traits)
戸籍 住所（住民票登録） 住民票コード パスポート番号 免許証番号	識別子 (Identifier)	属性 (attributes)
電話番号 メールアドレス ユーザー名	識別子 (Identifier)	属性 (attributes)
位置情報		属性 (attributes)
好きな食べ物 好きな音楽		趣味・好み （Preference）
ブログ・twitter 交友関係 購買履歴 旅行履歴		関係性 (relationships)
・ ・ ・		

例：Wii でいうところの mii

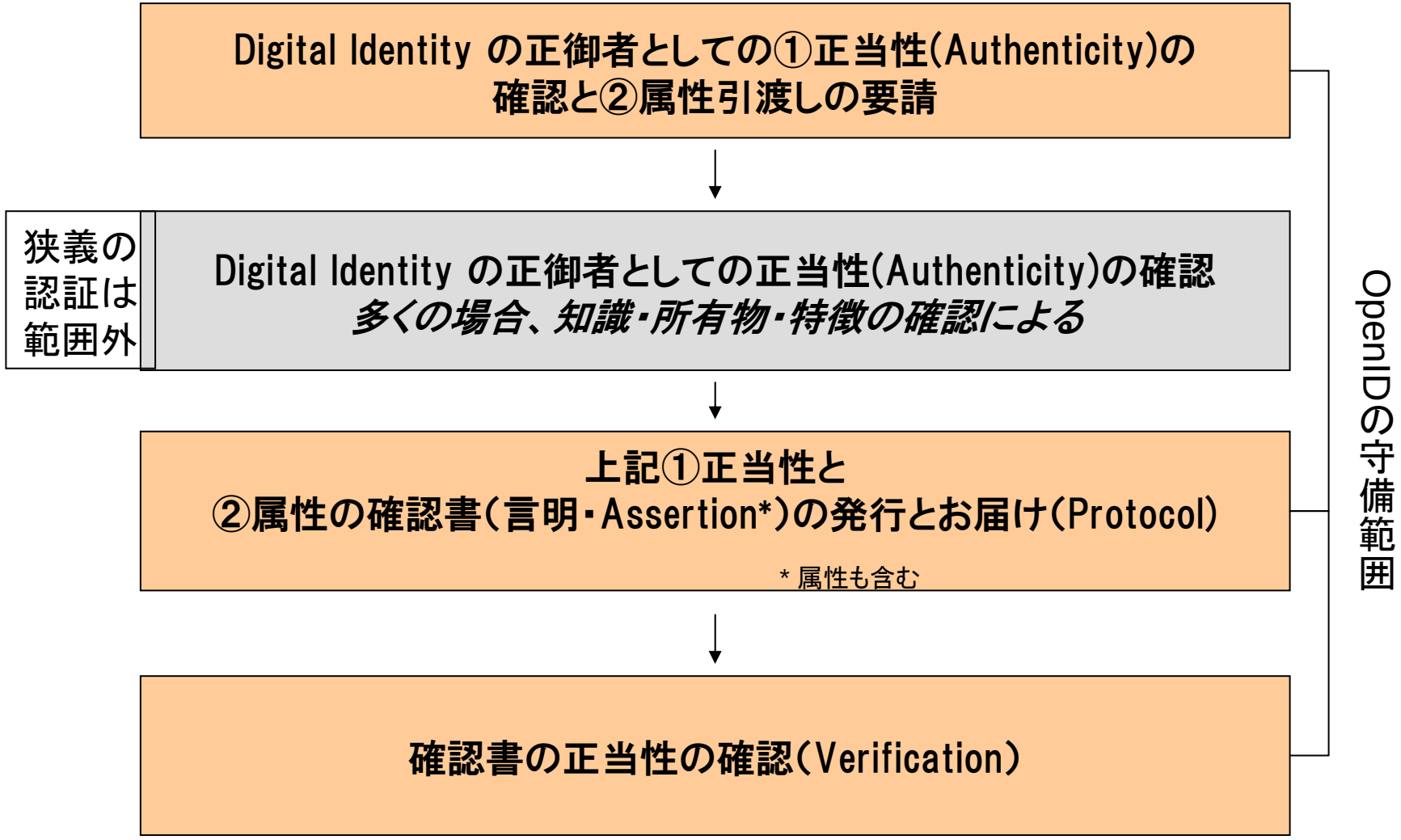
しかし、mii は wii の中でしか生きられない

インターネット全般で生きられるように

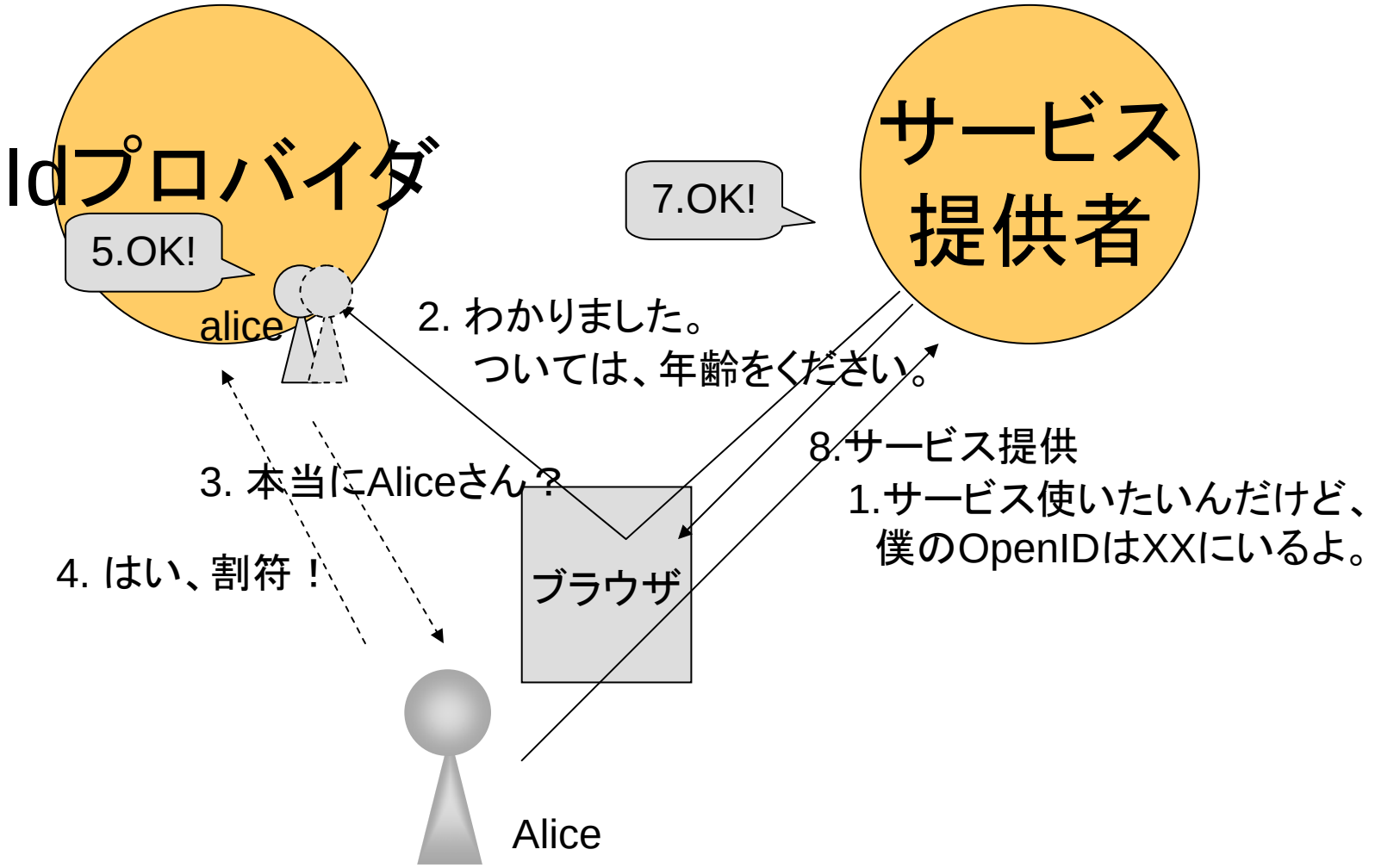
標準化・Open化

Open mii ⇒ OpenID

認証プロセスとOpenIDの守備範囲



OpenIDの基本モデル



まとめ

- OpenIDは、URLを識別子として使う、デジタル・アイデンティティフレームワークです。
  - 識別子にはURLを利用
  - Assertion は、Tag=Value/JSON 形式
  - 属性提供と同意取得フレームワークを持つ
  - WGプロセスが規定されており、どんどん追加仕様を提案可能
  - Facebook, Google, Yahoo!, Microsoft, IBM, Verisign, Salesfoce.com, Amazon, MySpace, NRI, JanRain, OIDF-J などが推進

認証基盤連携フォーラム

認証基盤連携フォーラム

■総務省・通信プラットフォーム研究会報告書「通信プラットフォームのあり方について」(2009/1) で規定

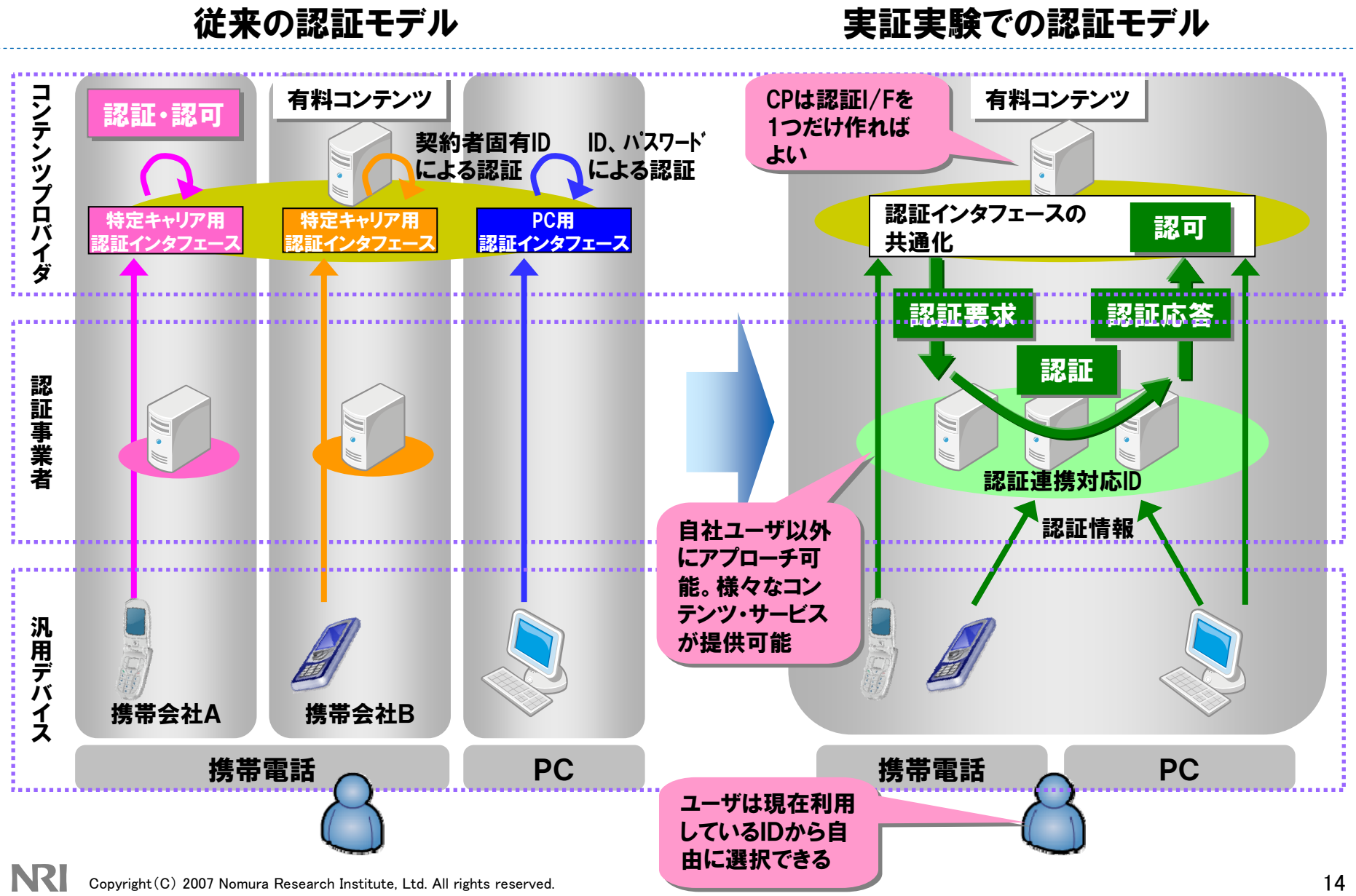
- 分散＆連携
  - 統合ではなく相互運用性の確保によって、サービスを一つのIDで利用できるように。
  - 複数のID間にバーチャルIDを介在させるなどの変換構造を導入し、各事業者は自社に関わる情報のみを取り扱う仕組み
- ユーザー中心
  - 利用者自らの意思でID管理ができるような仕組み
  - 利用者側はサービスを利用する事業者にのみ必要最低限の情報を渡し（利用者が承諾した程度に応じて属性情報が取扱われることを確保）
- 高可用
  - （相互運用性の確保による）特定の認証基盤で支障が発生した場合であっても、他の認証基盤によって代替を行うなど堅牢性の高い認証システムの構築
- 信頼＆評判
  - IdPの責任分担の在り方やIdPのレーティング（評価）の手法等についても併せて検討

認証基盤連携フォーラムのミッション

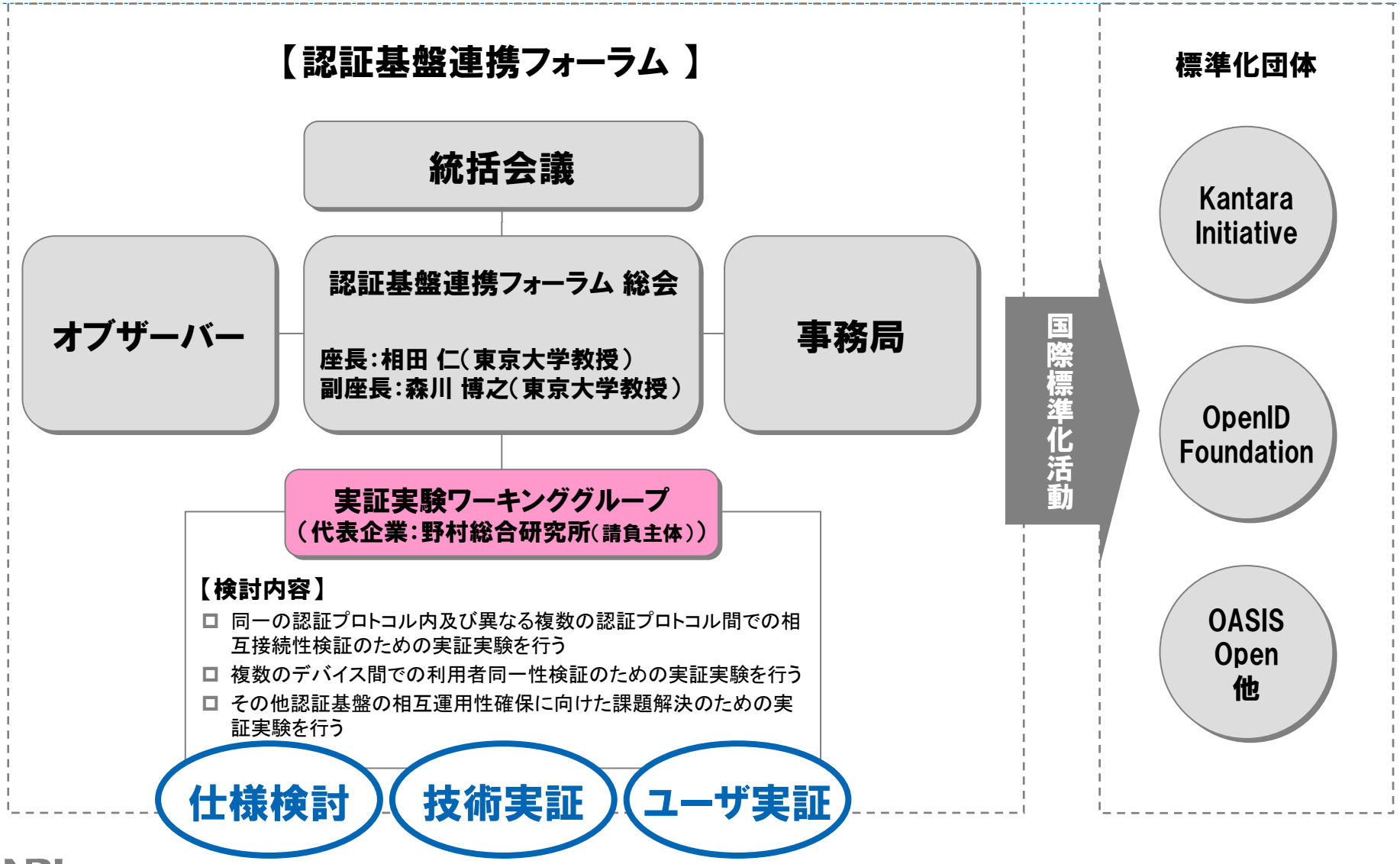
- 認証基盤の相互運用性の確保に向けたインターフェースの在り方等について、セキュリティの確保など利用者の安心・安全を確保するために講じるべき措置を含め、具体的な検討を進める。

- 認証基盤の相互運用性の確保に向けた実証実験を行うなど、関係事業者等が連携した取組を行う。

目的は、ユーザーセントリックIDの実現。



フォーラム傘下のワーキンググループで実施。



１３社が参加。

注）左から五十音順

コンテンツプロバイダ

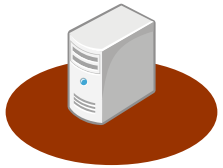
グルメサイト
（ユーザ試験用）

医療サイト
（デモ用）

検証サイト

ハードウェア（クラウド）

認証基盤



認証技術

（携帯電話）　（携帯電話）　（FeliCa）　（SyncLock）　（個体認証）　（SecuSURF）（BlueTooth）　（ICカード）

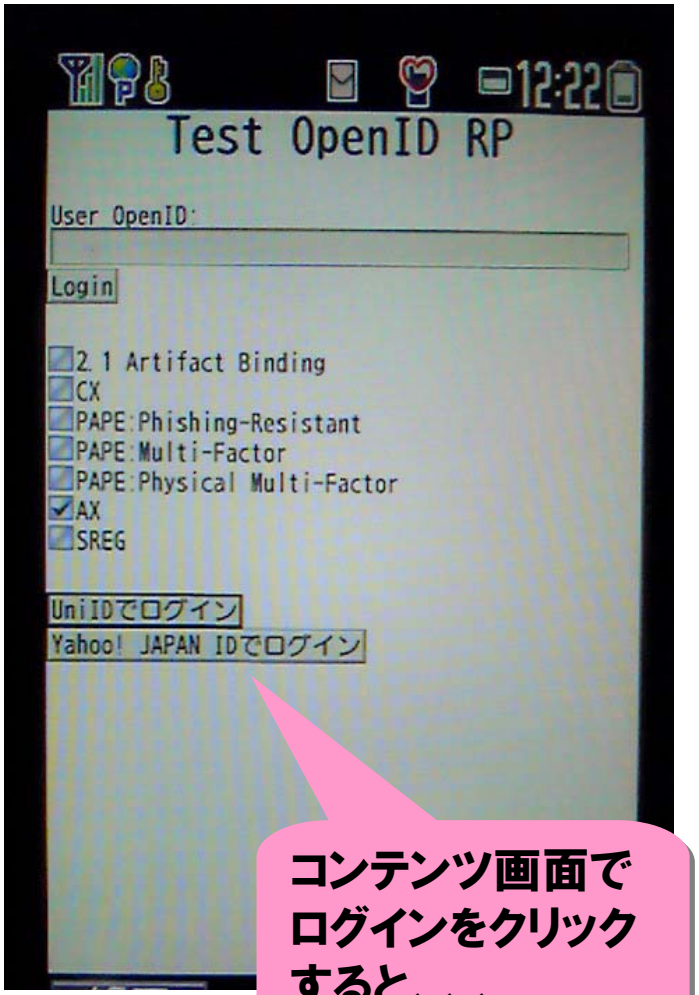
※上記企業に加え、NTTコミュニケーションズ、ウィルコムが仕様検討に参加

2009年度の取り組み

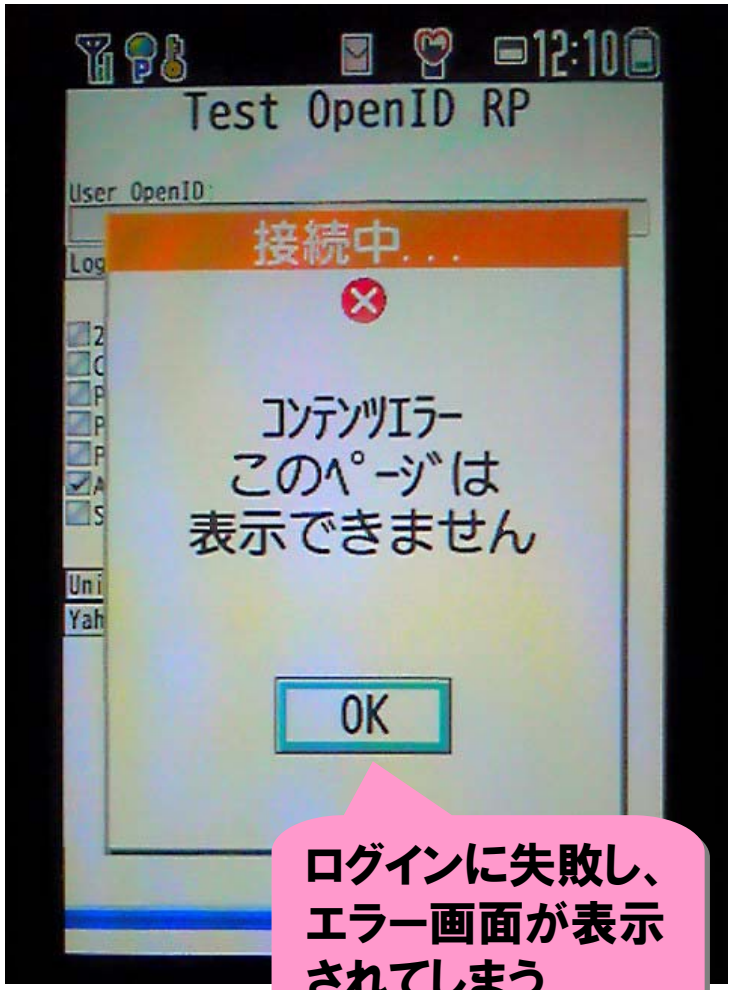
- OpenIDとSAMLの相互運用性確保
  - Yahoo! OpenID で Google Apps (SAML SP)にログイン、など
- OpenIDのモバイル対応方式の検討
- 属性表現の統一の検討
  - 属性URL
  - 言語・スクリプト表現
- IdP間のIdentity移行の課題の検討
- 利便性検討
  - デバイス間セッション引継ぎ（携帯電話, PC, etc…）
  - 属性情報連携
- 信頼性情報提供へのニーズ調査
- 上記にかかわる実験　他

OpenIDはモバイルでは…

「携帯電話」でのOpenID利用の課題



コンテンツ画面でログインをクリックすると、、、



ログインに失敗し、エラー画面が表示されてしまう

GET URLが長すぎる

■リクエスト例：
https://example.com/op_endpoint?openid.ns=http://specs.openid.net/auth/2.0/&claimed_id=http://specs.openid.net/auth/2.0/identifier_select&identity=http://specs.openid.net/auth/2.0/identifier_select&openid.mode=checkid_setup&...

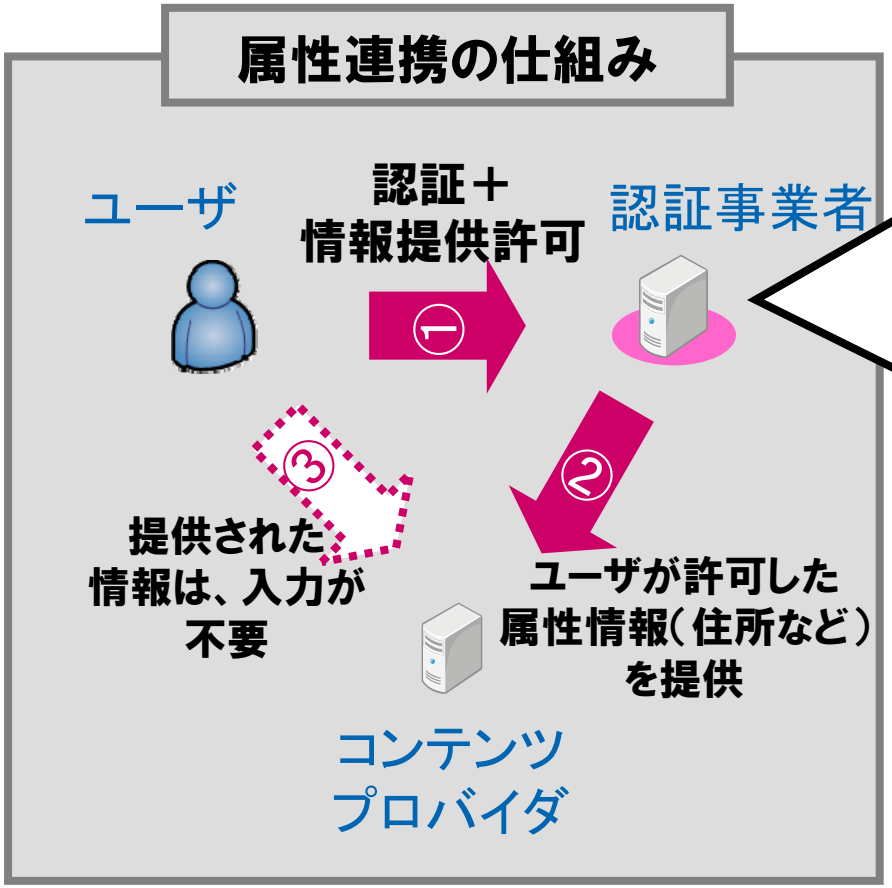
■POSTにすれば通るが、javascriptが無い端末だと、ユーザーがクリックしなければならず、「成功率」が落ちる

■レスポンスは、Assertion が全部乗ってくるので、さらに大きい

→URL長制限の無いブラウザーでも遅くなり、ユーザー利便性が落ちる

～ユーザ実証結果～

属性連携は、ユーザ利便性を高めることが検証された。



～ユーザ実証結果～

属性連携は、ユーザ利便性を高めることが検証された。

属性連携によって、時間短縮がされるとともに、入力エラーの発生率が削減した。

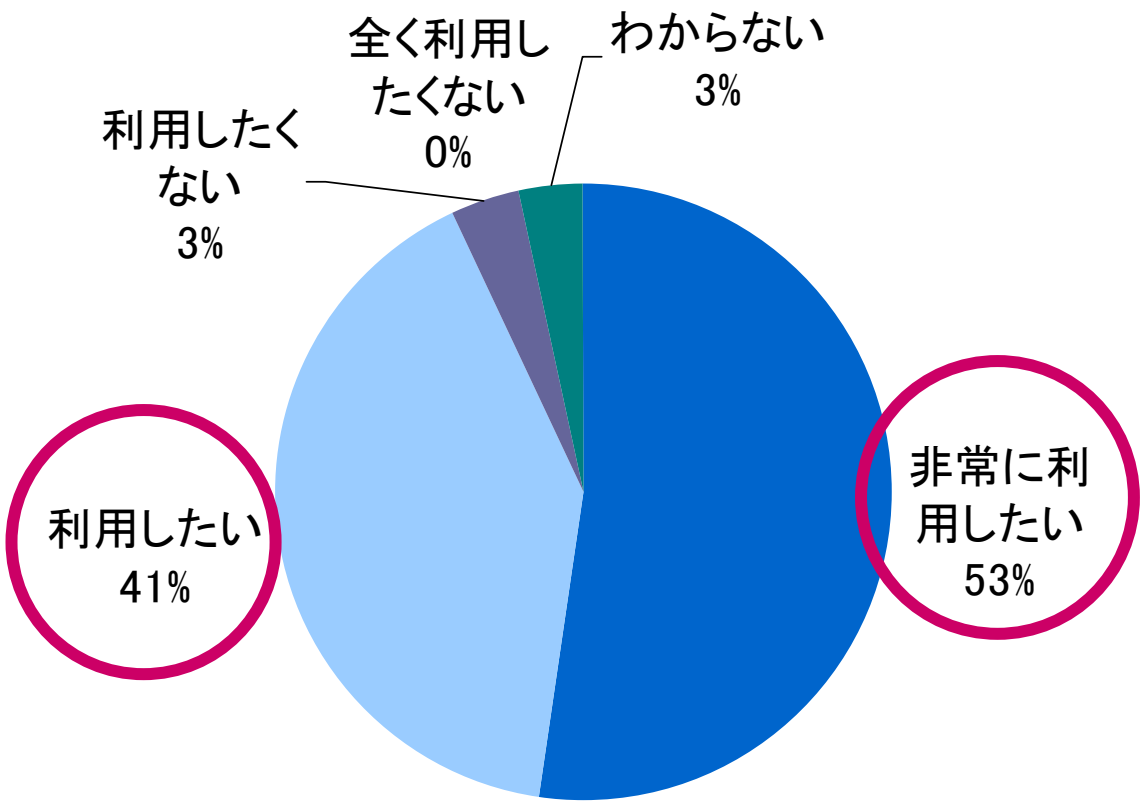
	属性連携を使わない場合	属性連携を使った場合
1サイトあたりの情報登録に必要な時間	1分33秒	19秒 （80%短縮）
入力エラーの発生率	19．6%	7．1% （65%減少）

※会場調査（N＝117）の結果。
調査においては、仮想的な懸賞応募サイトを作成。

～ユーザ実証結果～

調査参加者のうち9割以上が属性連携サービスを利用したいと回答。

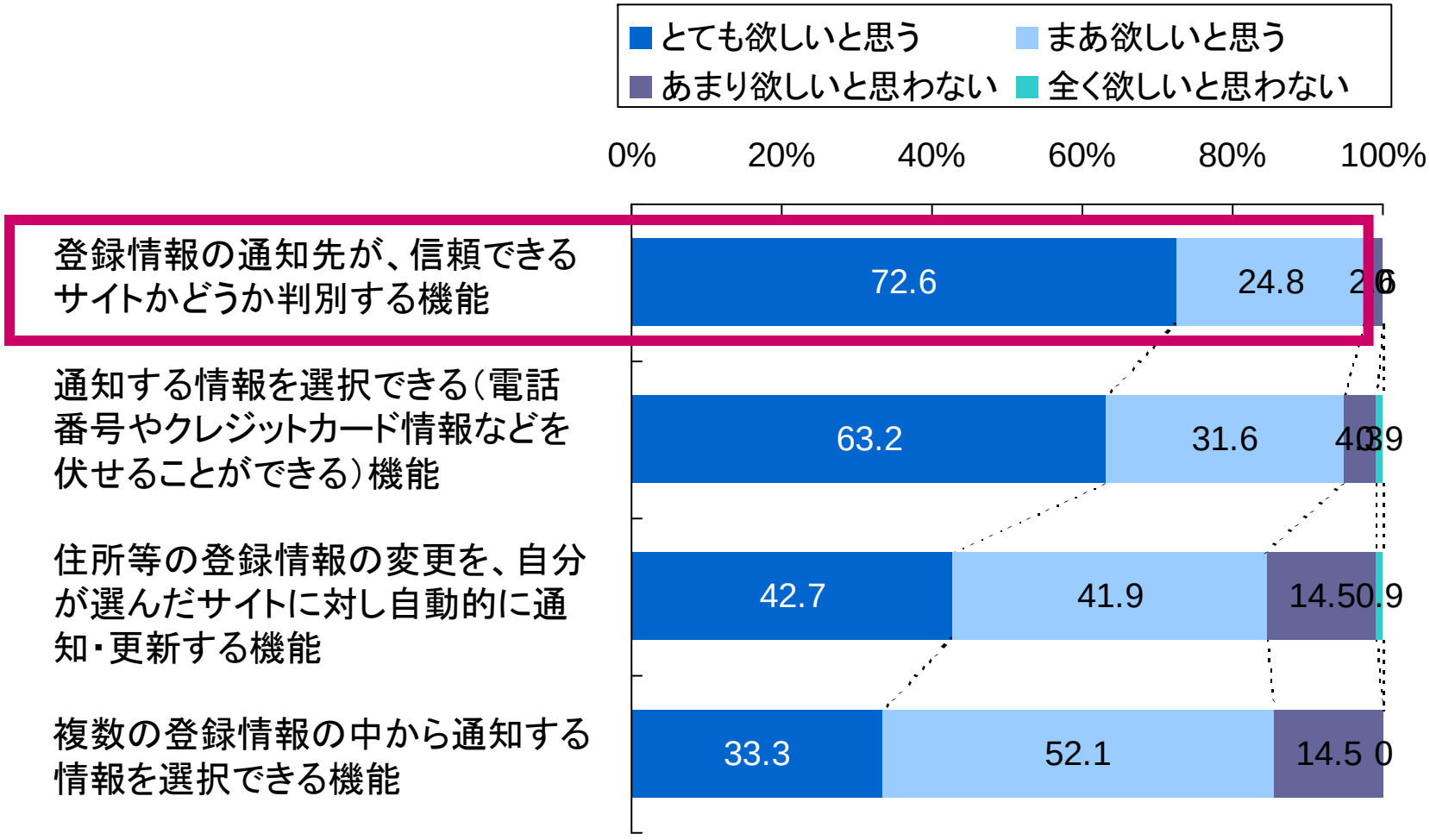
属性連携サービスへの利用意向



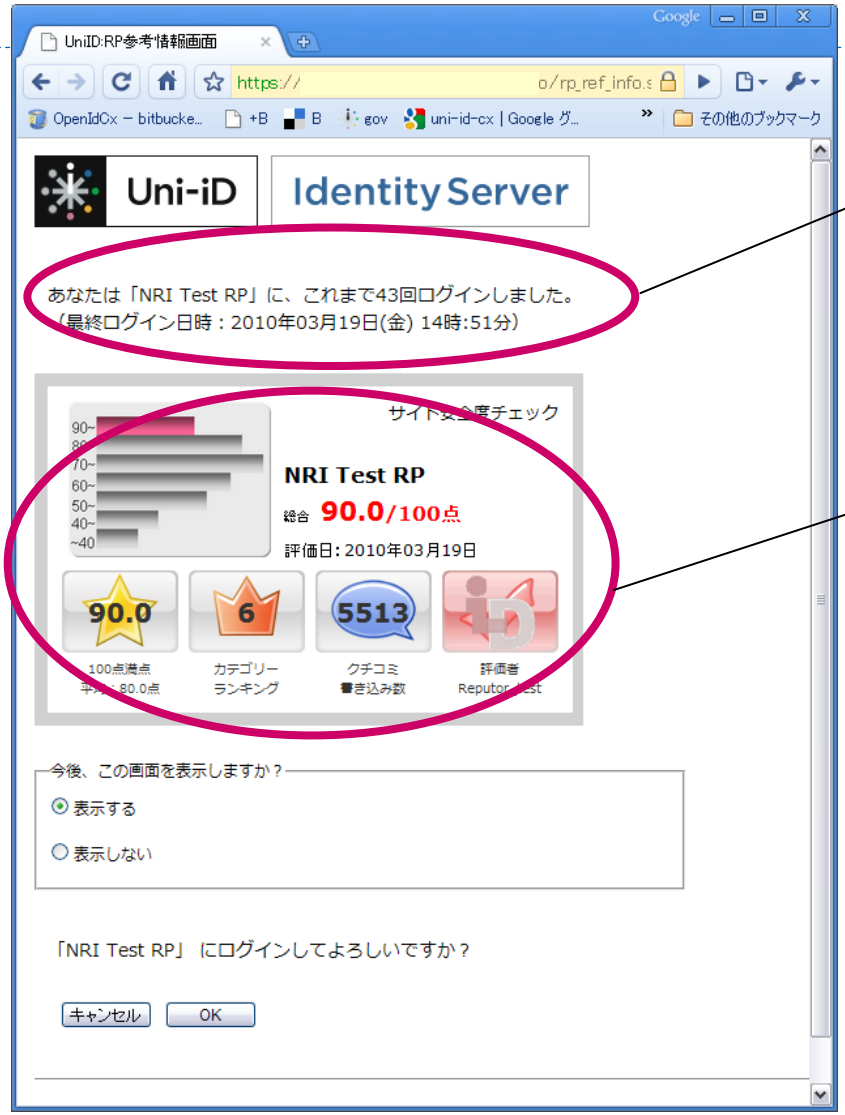
～ユーザ実証結果～

情報通知先の信頼性を判別する機能の利用意向は97％。

属性連携の付加機能への利用意向



認証参考情報～Level of Protectionの例



過去、そのRPにログインしたことがあるか？いつか？何回か？

どのくらいの評価を受けているサイトか

OASIS

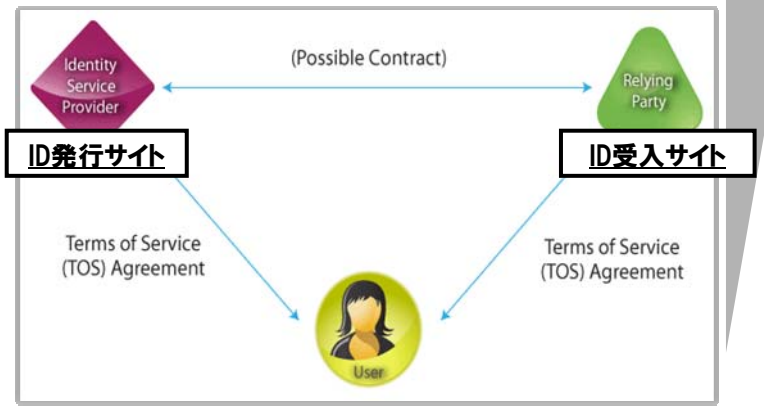
Open Reputation Management Systems (ORMS)

参考）Level of Assurance認定の必要性

■ 事業者間でのID連携の基礎となる信頼関係の構築促進を目指すOpen Identity Trust Framework (OITF) を提唱し、OITFにおける信頼フレームワーク・プロバイダー(TFP) 業務を行う非営利団体

従来のモデル

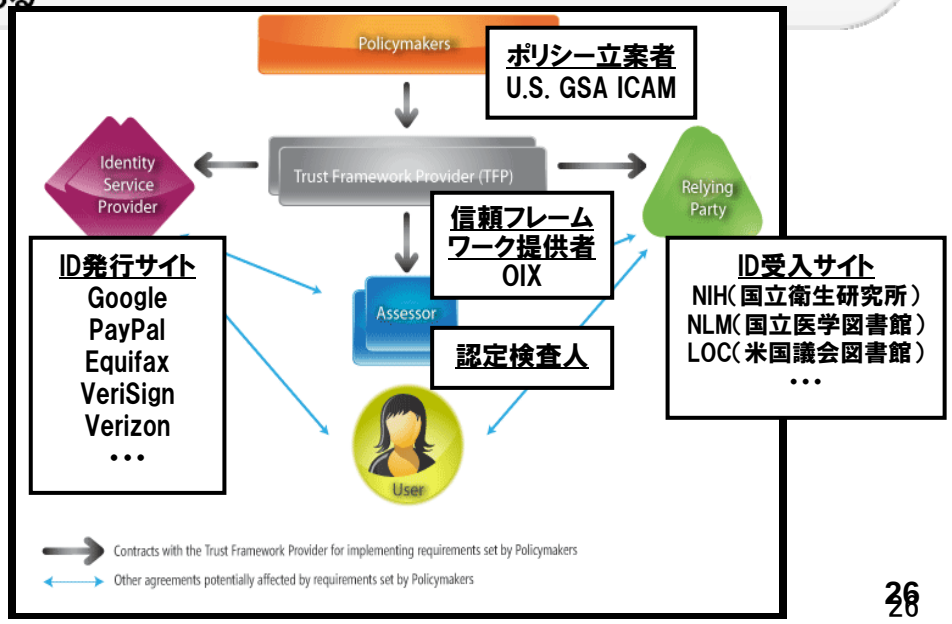
- 事業者同士が個別に信頼関係を結ぶ必要があるため、様々な課題が存在
  - 信頼関係を結ぶ度に毎回事業者間の交渉が必要となるため、コストと時間がかかる
  - 結果的にスケーラビリティに限界がある（参加する事業者を爆発的に増やすことができない）



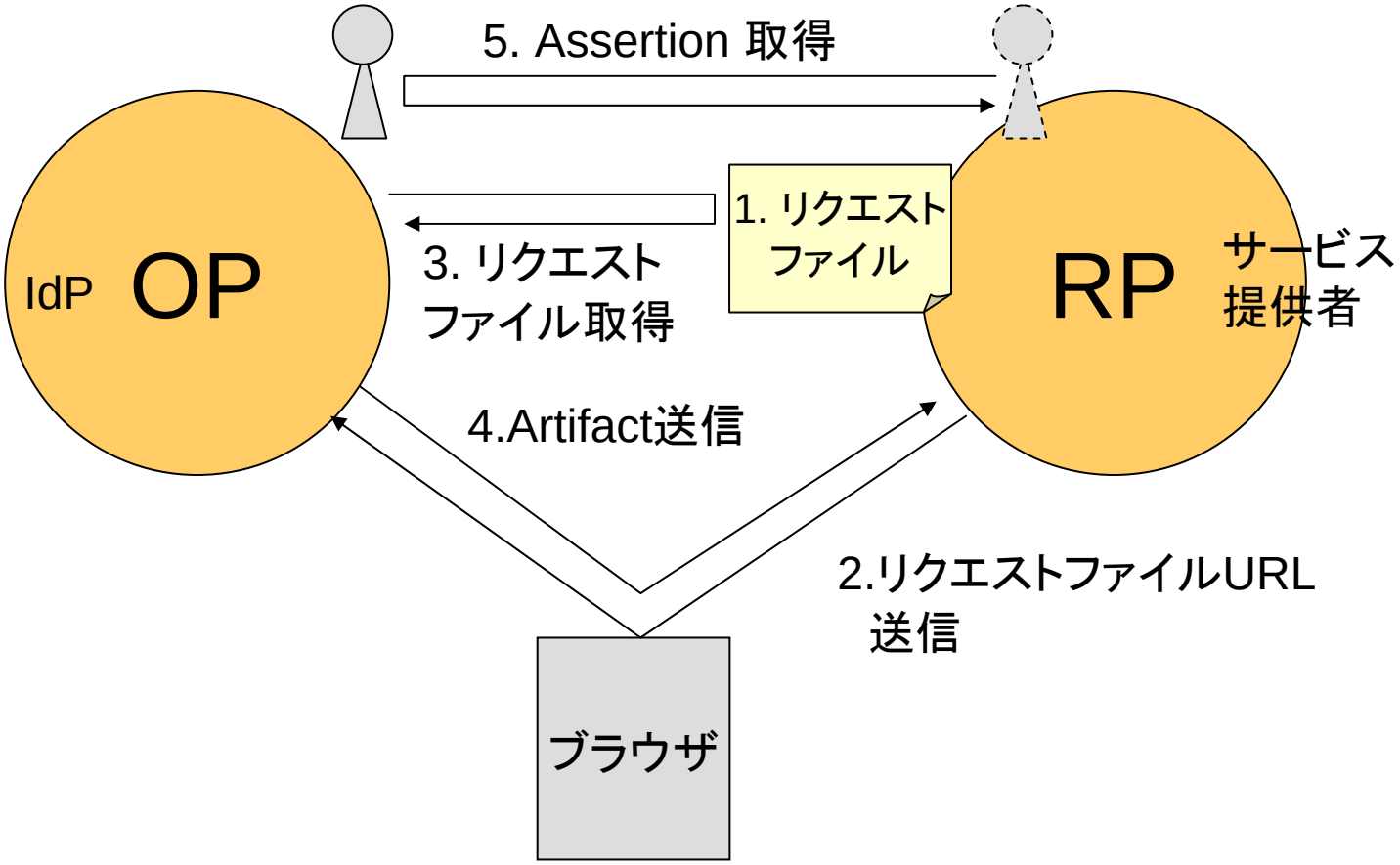
※ 図は OIXのWebサイトより引用

OITFモデル

- ポリシー立案者（Policymaker）の認定をうけた「信頼フレームワーク提供者（Trust Framework Provider: TFP）」が、各事業者を認定するモデル
  - 事業者はTFPの認定のみを受けるだけで済むようになり、コストと時間が大幅に短縮され、その結果スケーラビリティが向上する
  - ポリシー立案者は複数のTFPを認定することで、TFP同士の競争を発生させ、市場原理によるサービス向上が期待できる
- OIXはこのTFP業務を行う企業・団体のひとつとなる
  - 独占的なものではなく、他にも「カンターラ・イニシアチブ」等のTFP団体がある



OpenID for Mobile（Artifact Binding）



Spec Home: http://bitbucket.org/openid/ab/
解説＆デモ: https://openid4.us/

リクエストファイル

JSON

例 :

```
{
   "openid": {
      "type": "http://openid.net/specs/ab/1.0#req",
      "immediate": "false",
      "mode": "checkid_setup",
      "claimed_id": "http://specs.openid.net/auth/2.0/identifier_select",
      "identifier": "http://specs.openid.net/auth/2.0/identifier_select",
      "pem_url": "https://openid4.us/abrp/certs.pem",
      "enctype": "AES-128-CBC",
      "ns:ax": "http://openid.net/srv/ax/1.1",
      "ax:mode": "fetch_request",
      "ax:avatar": "",
      "ax:nickname": "",
      "ax:email": "",
      "ax:lastname#ja_Hani_JP": ""
   },
   "client_id": "https://openid4.us/abrp/",
   "redirect_url": "https://openid4.us/abrp/index.php",
   "grant_type": "authorization_code"
}
```

Asserti

■JSON


```
{
        "openid":{
        "ns":"http:¥/¥/openid.net¥/specs¥/ab¥/1.0¥/",
        "mode":"id_res",
        "claimed_id":"https:¥/¥/openid4.us¥/=alice#1234",
        "identity":"=alice",
        "ns:ax":"http:¥/¥/openid.net¥/srv¥/ax¥/1.1",
        "ax:mode":"fetch_response",
        "ax:avatar":"http:¥/¥/costumzee.com¥/view¥/wp-content¥/uploads¥/2007¥/07¥/alice.jpg",
        "ax:nickname":"alice",
        "ax:lastname#ja_Hani_JP":"¥u5c71¥u7530",
        "ax:lastname#ja_Kana_JP":"¥u30e4¥u30de¥u30c0",
        "ax:firstname#ja_Hani_JP":"¥u4e9c¥u7406¥u7d17",
        "ax:firstname#ja_Kana_JP":"¥u30a2¥u30ea¥u30b5",
        "ax:lastname":"Yamada",
        "ax:firstname":"Alice",
        "ax:telephone":"+1-999-999-9999",
        "ax:email":"alice@example.com",
        "ax:gender":"female",
        "ax:birthYear":"2000",
        "ax:link":"http:¥/¥/alice.in.wonderland.example.com¥/",
        "op_endpoint":"https:¥/¥/openid4.us¥/abop¥/op.php",
        "pape":null,
        "type":"http:¥/¥/openid.net¥/specs¥/ab¥/1.0#id_res"
},
        "server_id":"https:¥/¥/openid4.us¥/abop¥/",
        "client_id":"https:¥/¥/openid4.us¥/abrp¥/",
        "request_url":"https:¥/¥/openid4.us¥/abrp¥/rfs¥/rf_ax.json",
        "issued_at":1283244080,
        "expires_in":3600,
        "signature":"2f4daa1d0f58a4e283918d336361e82e41596e53b4e9c8dd77683b5171f1982d"

}
```

Artifact Request

- 302 Redirect で送信。OP Endpoint は https のみ。
- パラメータ
  - mode: “art_req”
  - rurl: リクエストファイルURL
  - immediate: (Opt) true or false. ユーザー確認画面の表示可否
  - claimed_id: (Opt) identifier_select でない場合

Artifact Response

- 302 Redirect で送信
- パラメータ
  - mode: “art_res”
  - code: Artifactの値

Assertion Request

- OP の https End Point に対して GET で送信
- パラメータ
  - mode：”direct_assertion_req”
  - code: 受け取った Artifactの値
  - sig: (opt.)
    base64url_encode(“mode=direct_assertion_req&code=_artifact_value_”) を RSA-SHA256 し、base64url_encode したもの。秘密鍵には、リクエストファイルに入れた公開鍵に対応するものを使う。

Assertion Response

- https response body に JSON ないしは JSONP として入れる。
- 署名をかける場合は、magic signatures.

メリット

- ブラウザー経由で渡されるGETリクエストを小さくできる
- Server to Server でほとんど通信するので高速
- Assertion Disclosure の防止
- OPの完全ステートレス化も可能
- NISTのLevel of Assurance (LoA) 4 まで対応可能（Holder of Key利用時）
- Signed Assertion Request を使えば、繰り返し属性の取得が可能（ユーザーのパーミッションがあれば。）
- OAuth2.0 の token の受け渡しも同時に可能
- 実装が簡単:
  - 今からデモするものはOP300行、RP100行程度（含HTML）
  - LoA1のRPなら、RPはページにjavascript を貼り付けるだけでOK
- おまけ:
  - OPがサポートすれば、SAMLやWSSも返せます…。

実際に動いているサイト

- 経産省-オープンガバメントWiki :
  - http://wiki.openlabs.go.jp/
- 陸別町アイディアボックス:
  - http://rikubetsu.openlabs.go.jp/
- OpenID/AB 技術デモサイト:
  - https://openid4.us/

今後の展開(みこみ…)

- 現在のDraft 13 ないし次の 14で凍結→投票
- OpenID Connect のベースドキュメントに。
- 派生仕様としての、OAuth Artifact Binding および OAuth Signature を同時並行
- Facebook, Google 他での採用を目指す

属性をどう表現するか？

- Type URI で表現するのが主流と思うが…
- どのType URIを共通に使うかのコンセンサスは無い
  → 属性連携がスケールしない
  - AXSchema
  - Portable Contacts etc.
- アメリカで作っているので、フリガナなどは当然無い（スクリプトの概念が無い。

スクリプト表現案

- Type_URL#言語_スクリプト_国

- 例：カタカナ氏名
  http://axschema.org/namePerson#ja_Kana_JP

TypeURL案

ARIB-MC 部会の属性項目	相対 TypeURI (http://axschema.org/～)	和名ラベル	説明	Example	Formatting (http://www.w3.org/2001/XMLSchema#～)
	namePerson/friendly	ニックネーム	ニックネーム、愛称	"Johnny5"	normalizedString
名前	namePerson	氏名	氏名（アルファベット表記）	"John Smith"	normalizedString
	namePerson/prefix	敬称	敬称	"Mr.", "Mrs.", "Dr."	normalizedString
	namePerson/first	名	名前	"John"	normalizedString
	namePerson/last	姓	名字	"Smith"	normalizedString
	namePerson/middle	ミドルネーム	ミドルネーム	"Robert"	normalizedString
	namePerson/suffix	名（接尾語）	対象の名前の接尾語（3 世、jr など）	"III", "Jr."	normalizedString
所属組織	company/name	会社名	会社名	"Springfield Power"	normalizedString
所属組織役職	company/title	役職	役職	"Engineer"	normalizedString
職種	company/occupation	職種	職種	"Company Employee"	normalizedString
所属識別子（社員番号、会員番号等）	company/EmployeeID	社員番号	社員番号	"0123456789"	normalizedString
生年月日	birthDate	誕生日	誕生日	"1979-05-31"	date
	birthDate/birthYear	誕生年（西暦）	誕生年（西暦）	"1979"	gYear
	birthDate/birthMonth	誕生月	誕生月	"05"	gMonth
	birthDate/birthday	誕生日（日のみ）	誕生日（日のみ）	"31"	gDay
	contact/phone/default	電話番号	連絡先電話番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
自宅電話番号	contact/phone/home	電話番号（自宅）	自宅電話番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
所属組織電話番号	contact/phone/business	電話番号（勤務先）	勤務先電話番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
携帯電話番号	contact/phone/cell	電話番号（モバイル）	携帯電話番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
	contact/phone/fax	FAX 番号	連絡先 FAX 番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
自宅 FAX 番号	contact/phone/home/fax	FAX 番号(自宅)	自宅 FAX 番号（RFC3966 の表記形式に従う。）	"+1-800-555-1234"	normalizedString
住所	contact/postalAddress/ho	町域、番地、	町域、番地、建物名（自宅）	"#42 135 East 1st Street"	normalizedString

今後の国際展開

- Kantara Inititative Concordia DGに提出、議論
  - 最終的な標準化団体はこの中で決める
- Higgins Project とも連携

Q&A