OpenID Summit Tokyo

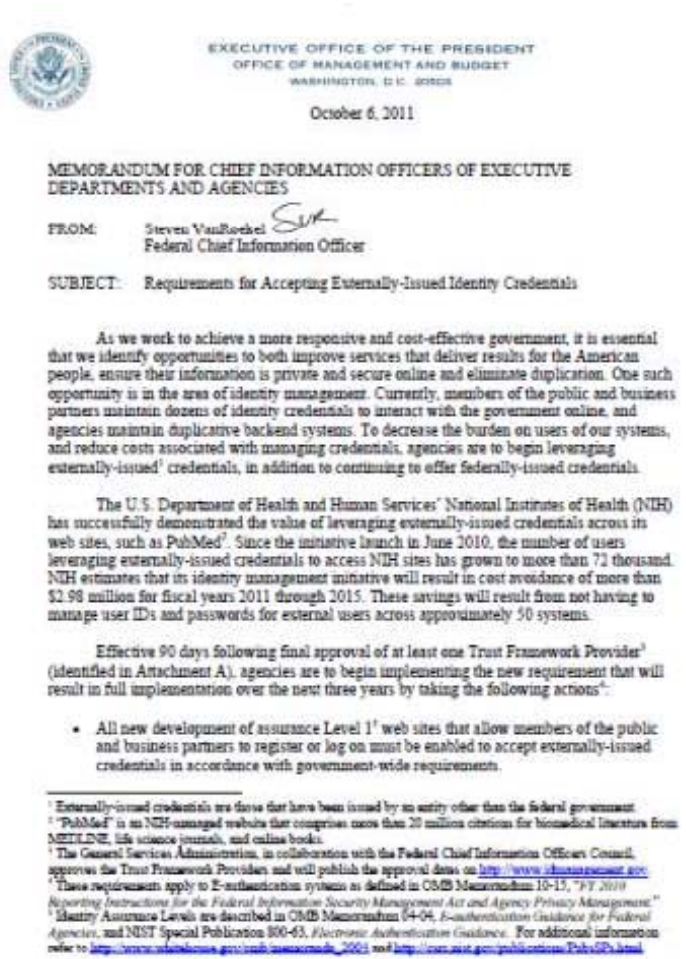
Policy Track (B)

Introduction

Shingo Yamanaka
OpenID Foundation Japan
@shingoym

OMB（米国連邦政府 行政管理予算局）

“Requirements for Accepting Externally-Issued Identity Credentials”



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

October 6, 2011

MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Steven VanRoekel
Federal Chief Information Officer

SUBJECT: Requirements for Accepting Externally-Issued Identity Credentials

As we work to achieve a more responsive and cost-effective government, it is essential that we identify opportunities to both improve services that deliver results for the American people, ensure their information is private and secure online and eliminate duplication. One such opportunity is in the area of identity management. Currently, members of the public and business partners maintain dozens of identity credentials to interact with the government online, and agencies maintain duplicative backend systems. To decrease the burden on users of our systems, and reduce costs associated with managing credentials, agencies are to begin leveraging externally-issued[1] credentials, in addition to continuing to offer federally-issued credentials.

The U.S. Department of Health and Human Services' National Institutes of Health (NIH) has successfully demonstrated the value of leveraging externally-issued credentials across its web sites, such as PubMed[2]. Since the initiative launch in June 2010, the number of users leveraging externally-issued credentials to access NIH sites has grown to more than 72 thousand. NIH estimates that its identity management initiative will result in cost avoidance of more than $2.98 million for fiscal years 2011 through 2015. These savings will result from not having to manage user IDs and passwords for external users across approximately 50 systems.

Effective 90 days following final approval of at least one Trust Framework Provider[3] (identified in Attachment A), agencies are to begin implementing the new requirement that will result in full implementation over the next three years by taking the following actions[4]:

- All new development of assurance Level 1[5] web sites that allow members of the public and business partners to register or log on must be enabled to accept externally-issued credentials in accordance with government-wide requirements.

[1] Externally-issued credentials are those that have been issued by an entity other than the federal government.
[2] "PubMed" is an NIH-managed website that comprises more than 20 million citations for biomedical literature from MEDLINE, life science journals, and online books.
[3] The General Services Administration, in collaboration with the Federal Chief Information Officers Council, approves the Trust Framework Providers and will publish the approval dates on http://www.idmanagement.gov
[4] These requirements apply to E-authentication systems as defined in OMB Memorandum 10-15, *"FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."*
[5] Identity Assurance Levels are described in OMB Memorandum 04-04, *E-authentication Guidance for Federal Agencies*, and NIST Special Publication 800-63, *Electronic Authentication Guidance*. For additional information refer to http://www.whitehouse.gov/omb/memoranda_2004 and http://csrc.nist.gov/publications/PubSPs.html

- 2011/10/6 政府CIO要求
  - KundraからVanRoekelになっても、基本路線に変更なし
- “3年以内に、連邦政府のすべてのWebサイトは既存のものも新規のものも外部のIDを受入れることを必須とする”
  - まずはLoA1から。随時LoA 2, 3, 4も対象に
- 本要求の意図
  - コスト削減
  - セキュリティ／プライバシー対策
  - NSTICの実現

Policy Trackのテーマ

- 国内・海外のTrust Framework の普及、標準化動向

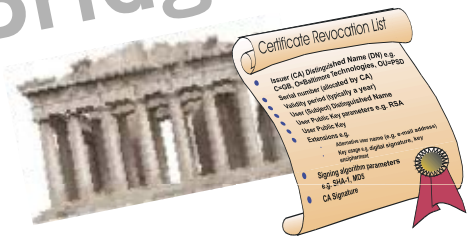
- なぜ信頼（Trust）が必要なのか？
- Trust Framework のメリットは？
- Trust Framework はどうやったら構築できるのか？

トラストフレームワークとは？

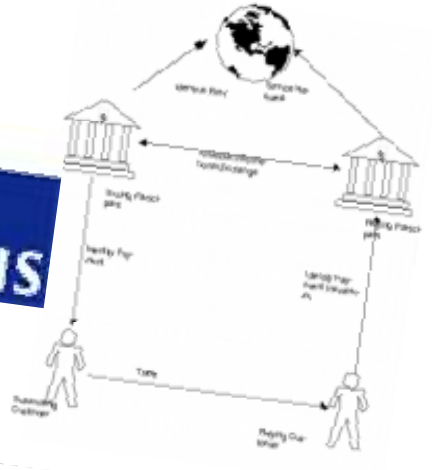
オンラインで
パーソナル・データを
認定された事業者(Entity)の間で
利用者本人の同意に基づき
安全に流通させる
ガバナンスの枠組み

これまでも様々なトラストフレームワークがあった

Bridge CA?

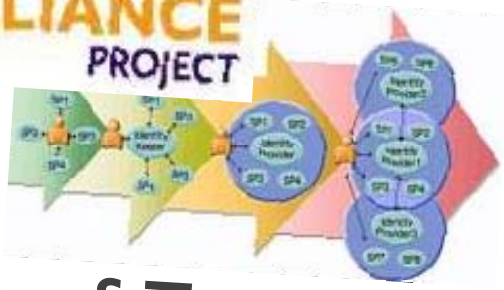


identrus



5-Corner Model?

LIBERTY ALLIANCE PROJECT



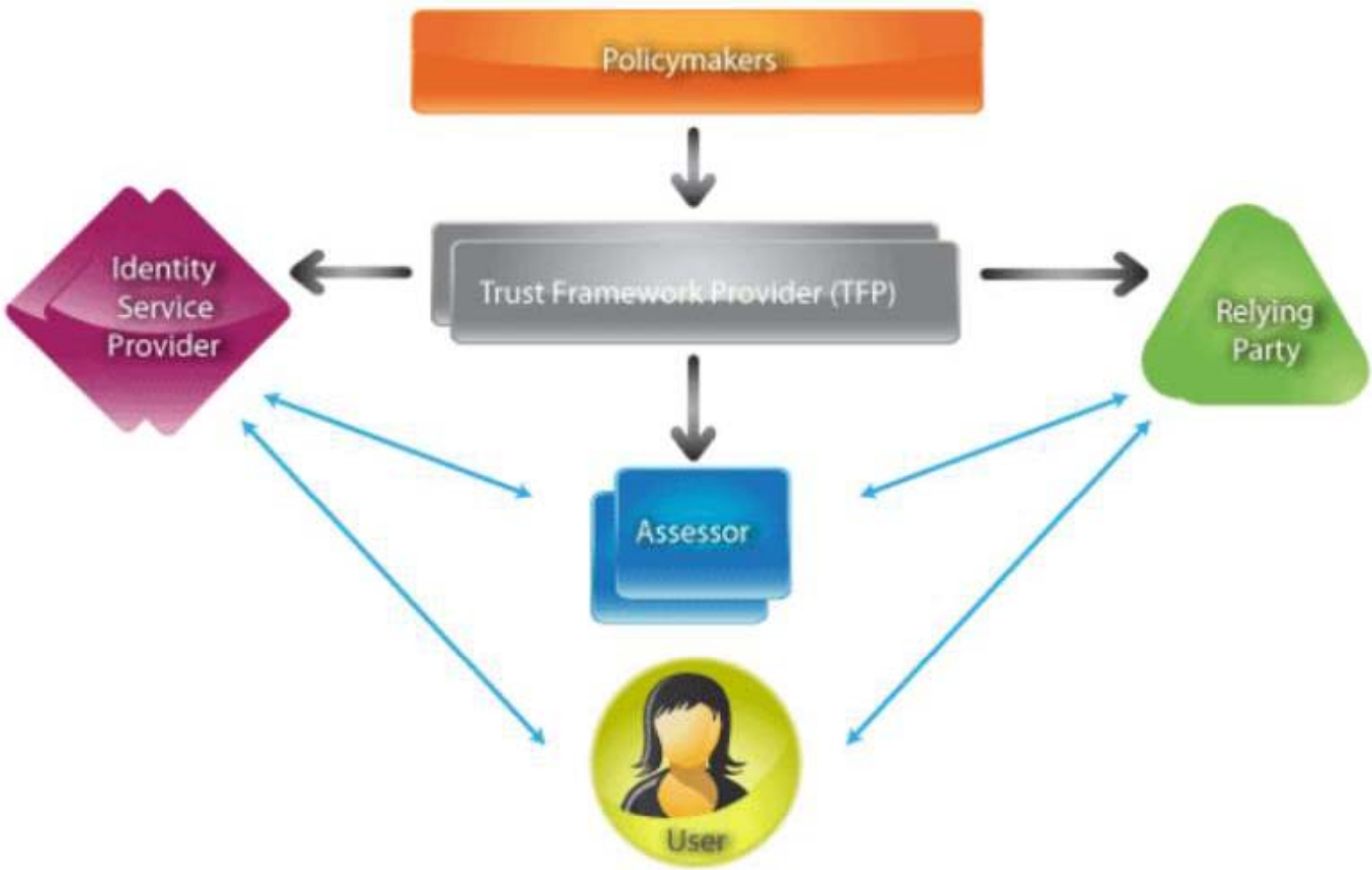
Circle of Trust?

WS-I WEB SERVICES INTEROPERABILITY ORGANIZATION

WS-Trust?

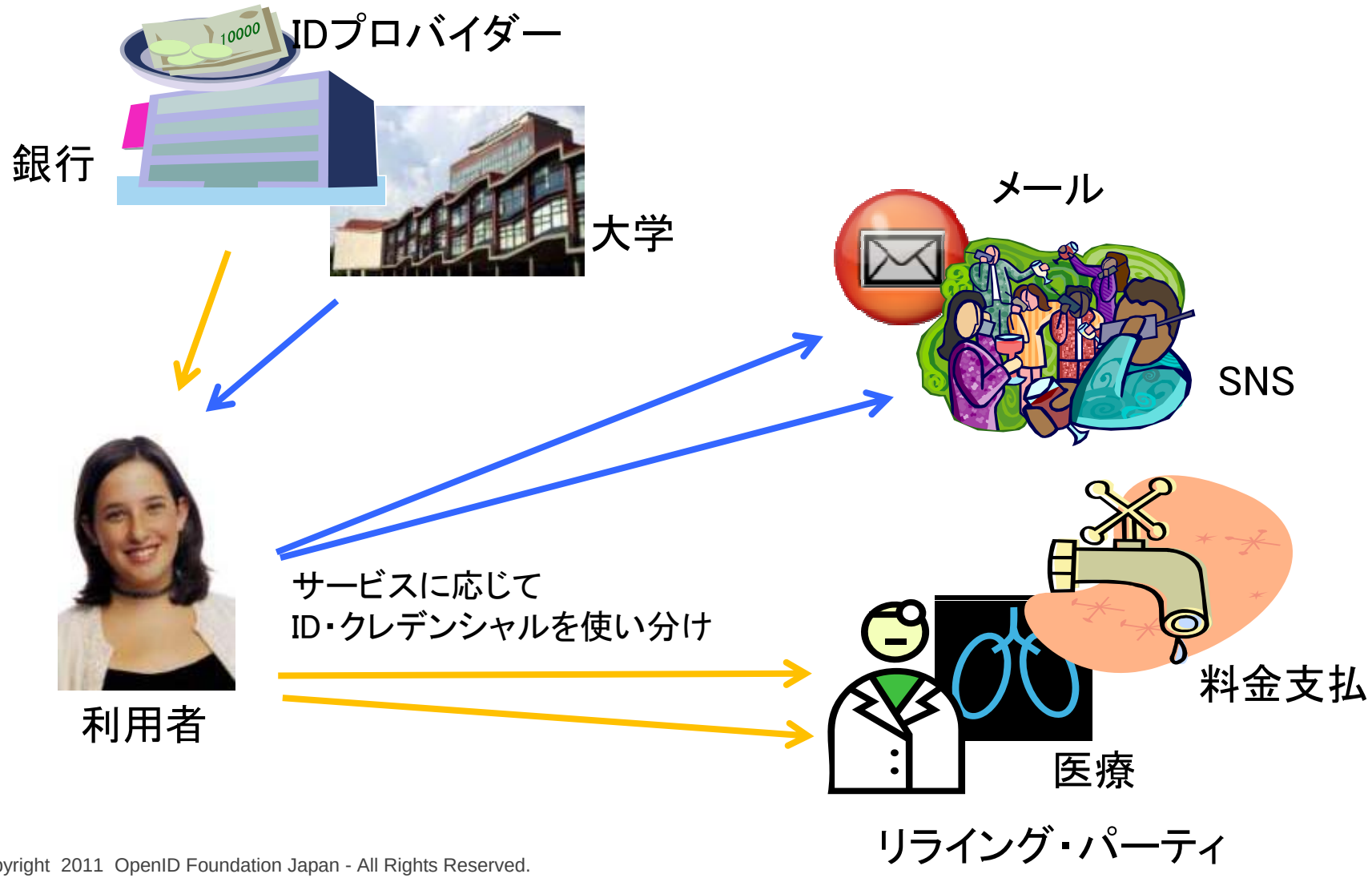
トラストフレームワークの代表例

Open Identity Trust Framework



トラストフレームワークのユースケース ＃1

サービスにあったクレデンシャルの選択



トラストフレームワークのユースケース #2

必要な資格情報のみ取得し匿名でアクセス

学校

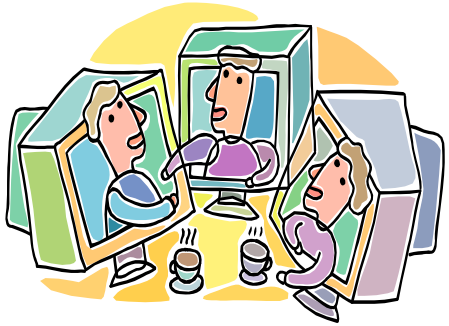
属性プロバイダー

12歳～17歳の証明

子供向けチャットルーム

利用者

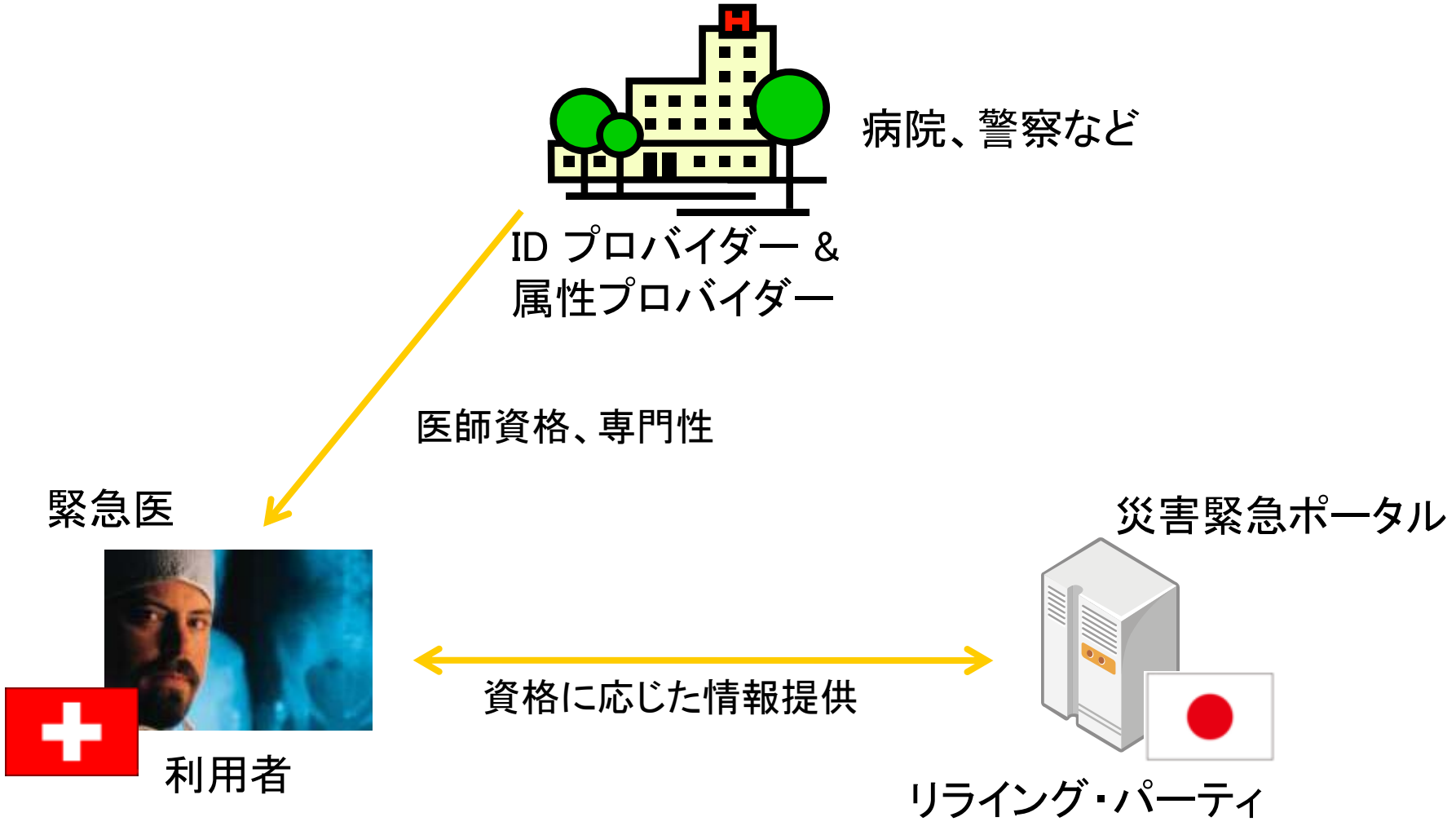
匿名での利用
（利用資格のみ証明）



リライング・パーティ

トラストフレームワークのユースケース ＃3

資格証明と非常時のアクセス許可



トラストフレームワークのユースケース ＃4
IDプロバイダーの許可によって第三者から属性を提供

PHRサイト

IDプロバイダー

ミネソタ州の病院
（過去のかかりつけ）

属性プロバイダー

利用者

電子カルテの提供

マサチューセッツ州の病院（現在のかかりつけ）

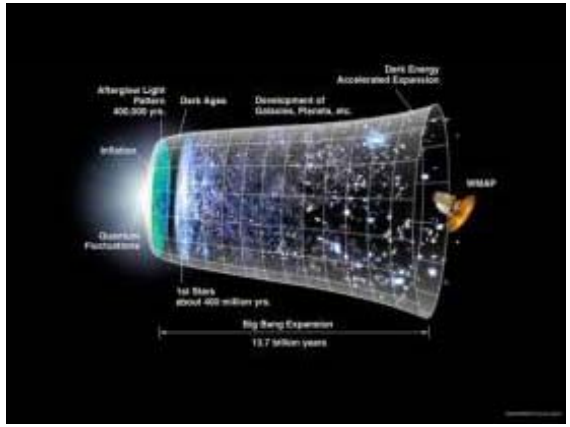
リライング・パーティ

日本の国民ID制度の文脈で考えると

- 属性の利用
  - マイナンバー（税と社会保障の共通番号）を使って、政府の持っているアイデンティティ情報（基本4情報）が欲しい
  - 特定の事業者（上場企業？金融機関？）だけがOK？
- IDの配布
  - 公的認証、民間利用でのハードル、任意だと広がらない
  - ICカード＋ICカードリーダー＋ドライバインストール
  - リテラシー教育と多様なデバイスでの対応
- コスト
  - なんでも高レベルでのIDを使うと青天井にカネがかかる
  - マイナンバーのICカード配布をオンライン利用、数千億円
- プライバシー
  - 自己情報コントロールの確保
  - 不当な名寄せの防止
- 分野ごとの課題
  - 電子政府の官民連携、スマートグリッド、EHR／どこでもMY病院…

Envision it!

Big Bang
&
Invention



Policy Panel Speeker

- Sessions
  - Don Thibeau – Chairman, OIX
  - John Bradley – Kantara, OpenID Foundation
  - Valter Nordh – eduGAIN, NORDUnet
  - Kick Willemse – OpenID Foudation
  - Tony Nadalin – Microsoft
- Panel
  - 東京大 佐藤先生、JIPDEC 小林様、Ian Glazer – Gartner、Hal Warren – OpenID Society/APA
  - 京都大 岡部先生

Q&A

1. 特定の企業に属性情報が多く集まると個人が特定出来る可能性がある。どう対応するのか？
   - IdPに情報が集約するのはしかたないか？どうデータ分散させることができるのか？
   - 逆にAPからSPに情報を提供するモデルでは、AP側にどのSPを利用してるかバレてしまうが？
2. Trustフレームワークを形成する上で国と民間の役割はどう考えればいいか？
   - 民主導だとしても、法律などの整備は国の役割
3. 日本でTrustフレームワークは普及するか？
   - その普及ドライバーは？
4. OITFのAssessorの信頼確保はどのように行うのか
   - Assessorの信頼性に全体の信頼性が決まるのではいか？

Q&A

5. プライバシー法、個人情報保護法の各国の制度違いをOITFはどう吸収するのか？
6. IDPの参加者として、銀行や通信業者がよくあげられる。検討プロセスにこれらの企業がどのように関与しているか？
7. 理想型のOITFの普及のマイルストーンはどんなものか？
   - 2～3年後なのか、5年～10年後か？