



カンタラ・イニシアティブ -最近の動き-

カンタラ・イニシアティブ・ジャパン・ワークグループ
山田 達司

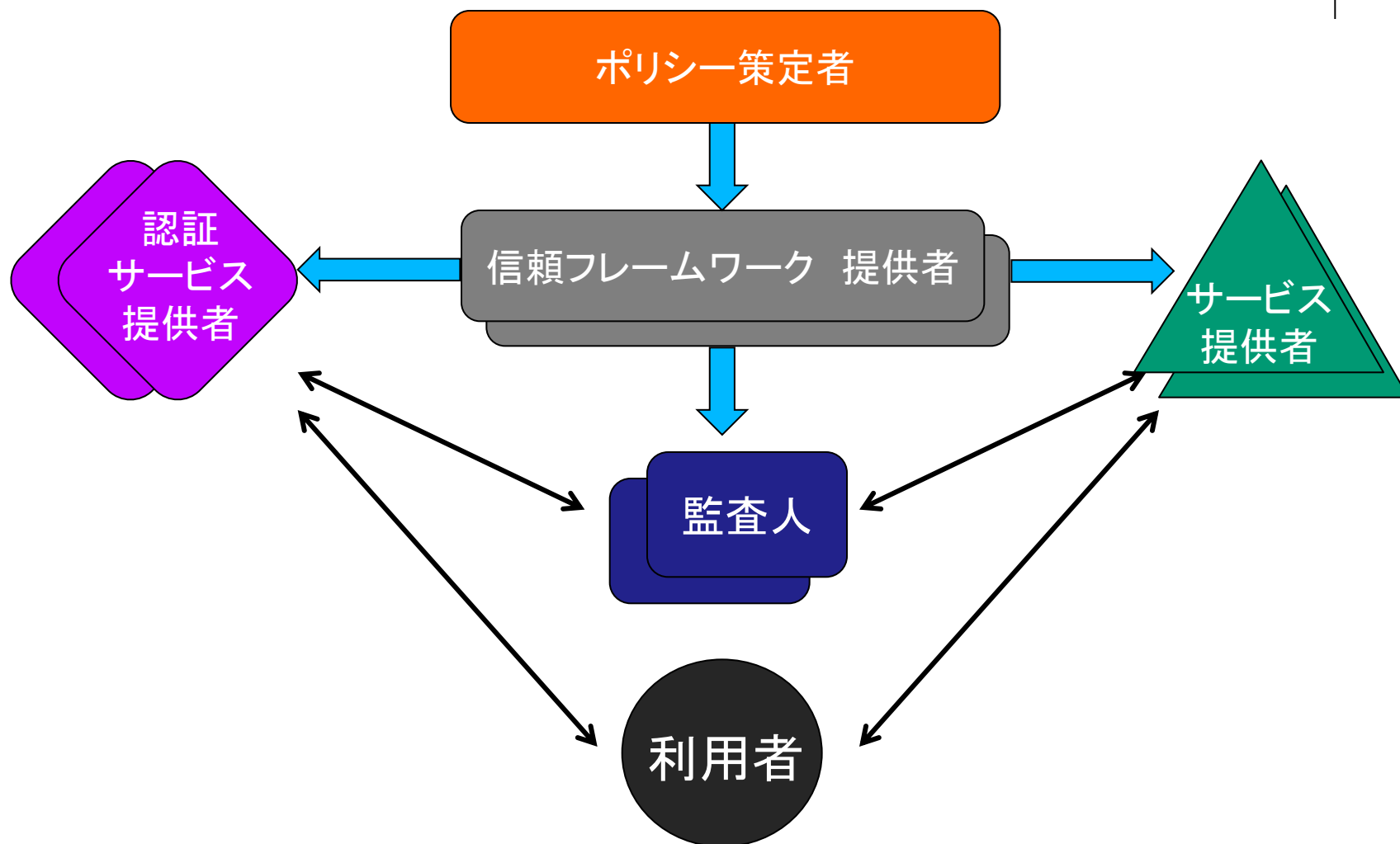
カンタラ・イニシアティブの信頼フレームワークに関する重要な発表

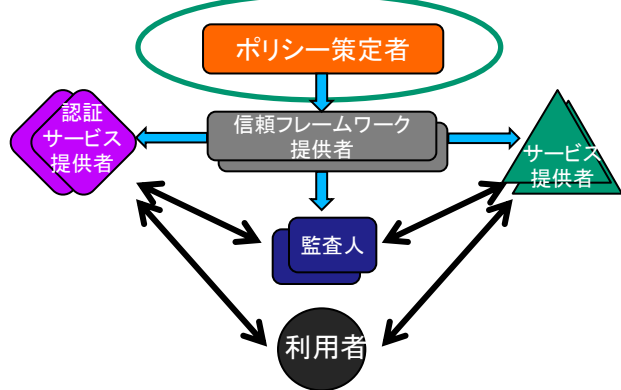


- ・OMB Memo (2011/10/6) によって以下が決定：
 - 米国連邦政府の新規開発される全ての外部向けLoA1サイトは認定を受けた外部認証プロバイダの認証を受け入れなければならない(既存サイトは改定のタイミング)
 - LoA 2 以上の認定認証プロバイダが出現した暁には、適切かつ可能な限り、同様に外部認証プロバイダの認証を受け入れるようにしなければならない。
- ・カンタラ・イニシアティブの信頼フレームワークプログラムである「Kantara Identity Assurance Accreditation and Approval Program」が米国連邦政府一般調達局(GSA)のIdentity Credential and Access Management(ICAM)からLevel of Assurance 1から3(non-PKI)の信頼フレームワークに認定(2011/11/1)
- ・カンタラ・イニシアティブがDeloitte & Touche LLP社とeValid8社をKantara Identity Assurance Accreditation and Approval Programにおける監査人に認定。またVerizon社のUniversal Identity ServiceをLevel of Assurance 3に認定(2011/12/5)

Trust Framework model

信頼フレームワークのモデル



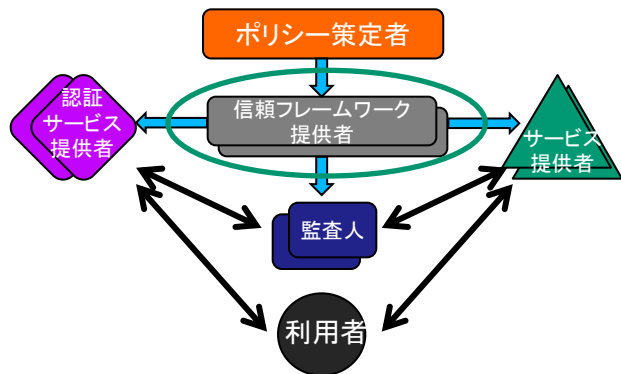


ポリシー策定者



トラストフレームワークにおけるポリシーを作成

- 連邦CIOカウンシルによるICAM(Identity Credential and Access Management): 米国連邦政府のオンラインサービス利用に関するポリシー。サービスの要求に合わせてLevel of Assurance (LoA)を1から3まで定義
- BIO-PHARMACEUTICAL Federation
- FINANCIAL SERVICES NETWORK
- HIGHER EDUCATION FEDERATION

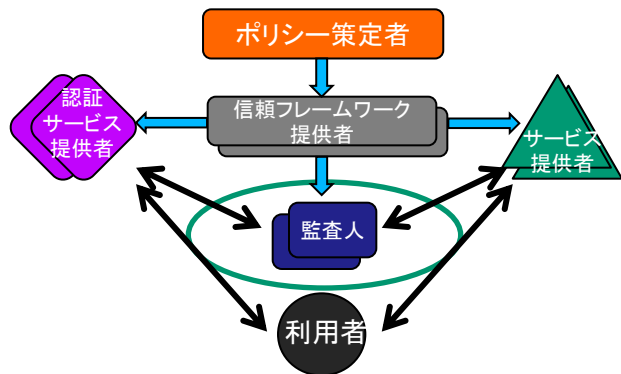


信頼フレームワーク 提供者



ポリシーに基づき、保証レベルを定義し、レベル毎に事業者が満たすべき技術、運用面での要件を作成。監査要件を作成し、監査人を認定。認定監査人の監査結果に基づき認定を実施。

- ・Open Identity Exchange: ICAM LoA 1に認定
- ・カンターラ・イニシアティブによるKantara Identity Assurance Accreditation and Approval Program: ICAM LoA 1~3(non-PKI)に認定
- ・学術認証フェデレーション(GakuNin): ICAM LoA1~申請予定
- ・InCommon(米国の学術認証フェデレーション): ICAM LoA1に認定

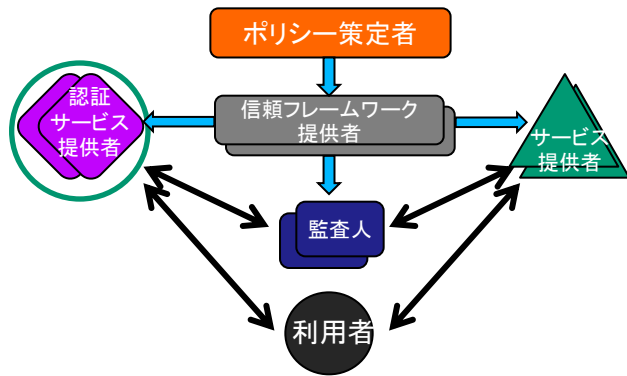


監査人

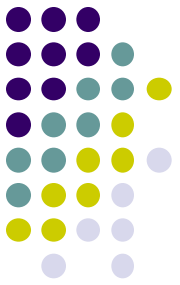


信頼フレームワークプログラムに基づき、認証サービス提供者およびサービス提供者の監査を実施。監査に合格すると、信頼フレームワーク提供者から認定が行われる。

- Open Identity Exchange: Spatial Dynamics Corporation
- Kantara Identity Assurance Accreditation and Approval Program: Deloitte & Touche LLP、eValid8
- GakuNin, InCommon: 別途定義された独立した監査人

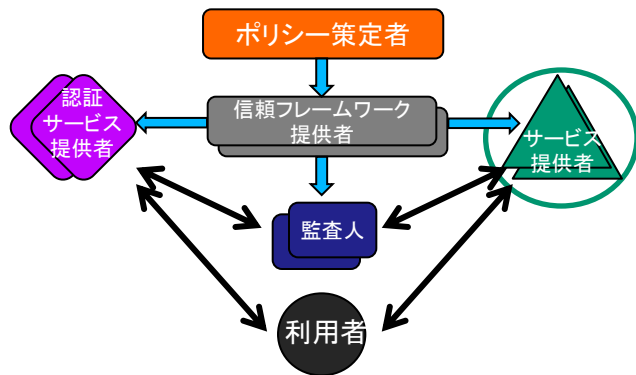


認証サービス提供者

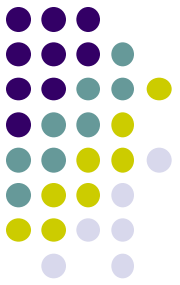


信頼フレームワークプログラムにより認定され、認証サービスを提供

- Google: Open Identity ExchangeによりLoA 1に認定
- PayPal: 同上
- VeriSign: 同上
- Verizon: Kantara InitiativeによりLoA 3(non-PKI)に認定
- GakuNin参加大学: GakuNinによりLoA 1の審査が行われる見込み



サービス提供者

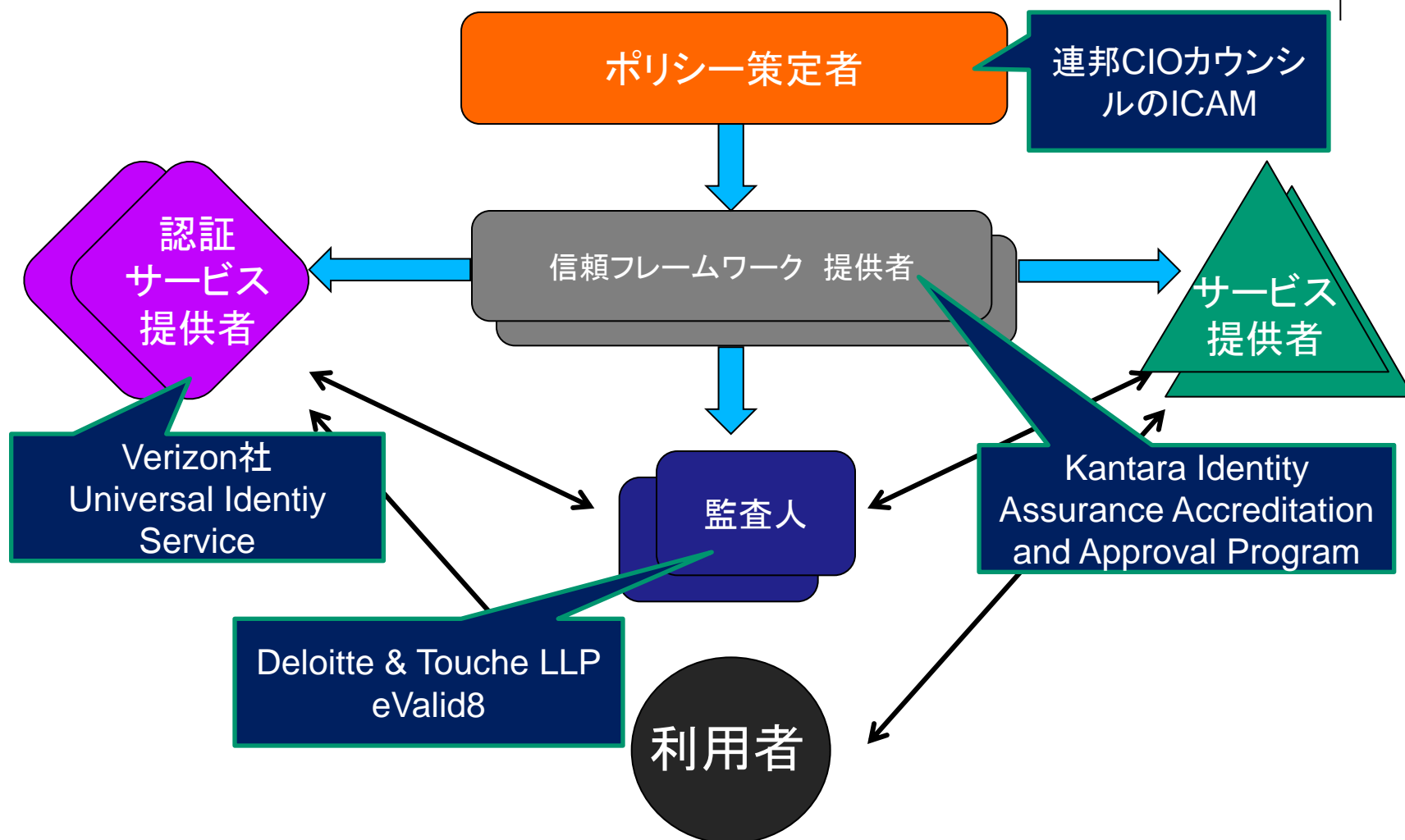


認証サービス提供者の認証に基づきサービスを提供。

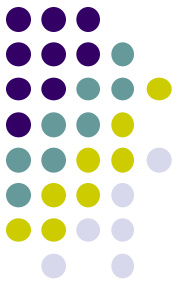
- 米国連邦政府のオンラインサービス:LoA1に相当するサービスはLoA1以上を所有する認証サービス提供者からのアクセスをサポートしなければならない。(2011/10~)
 - 例:PubMed(アメリカ国立医学図書館が提供する医学・生物学分野の学術文献検索サービス):認証サービス提供者にICAM LoA1を要求
- LoA 2 以上に関しても同様(2011/11~)



最近の発表の関係



カンタラ・イニシアティブの二つ目の事業



- Interoperability Certification Program
SAML2.0による製品間の相互接続性の認定プログラム
- Identity Assurance Accreditation and Approval Program
信頼フレームワークに基づく事業者、監査人の認定プログラム