カンターラ・イニシアティブにおける分科会の取組み事例

伊藤　宏樹
日本電信電話株式会社
NTT情報流通プラットフォーム研究所

本日のアジェンダ

1. カンターラ･イニシアティブにおける分科会活動

2. Concordia DG
3. Identity Assurance Framework WG
4. User Managed Access WG
5. P3 (Privacy and Public Policy) WG
6. eGovernment WG

7. まとめ

1. カンターラ・イニシアティブにおける分科会活動

分科会活動

- 2009年11月 6日現在、14 のワークグループ、4つのディスカッショングループが活動中ないしは組織化準備中。

ワークグループ

- Clients
- Consumer Identity
- eGovernment
- Healthcare Identity Assurance
- Identity Assurance
- IdP Selection
- ID-WSF Evolution
- Information Sharing
- Japan
- Privacy and Public Policy
- Universal Login Experience
- User Managed Access
- (Liberty Spec Maintenance)
- (Telecommunications Identity)

ディスカッショングループ

- Concordia
- Identity Community Update
- Japan
- (Multi-Protocol Identity Selector)

() 内のグループは現在組織化準備中

http://kantarainitiative.org/confluence/dashboard.action

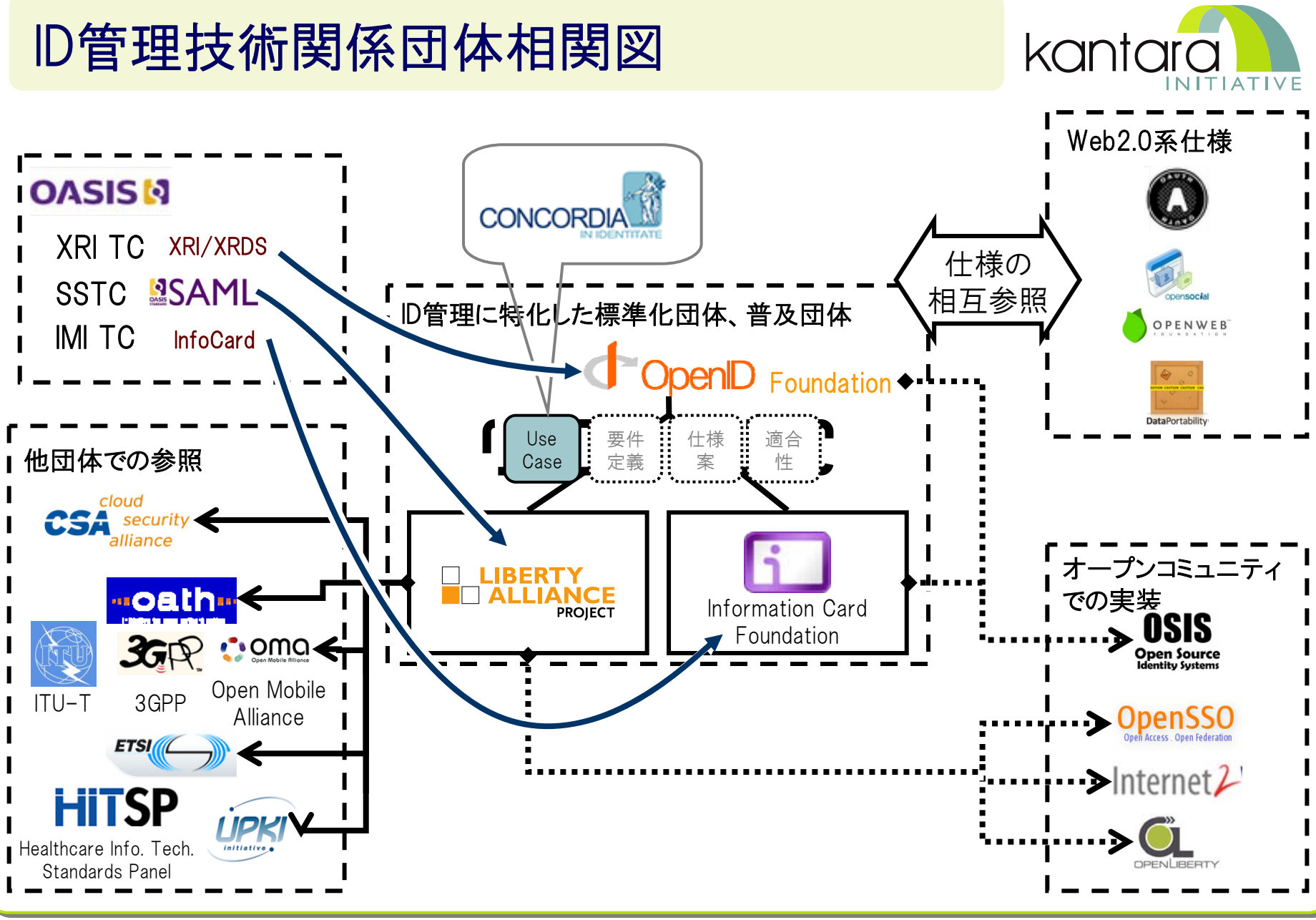
2. Concordia DG

Concordia DG

kantara INITIATIVE

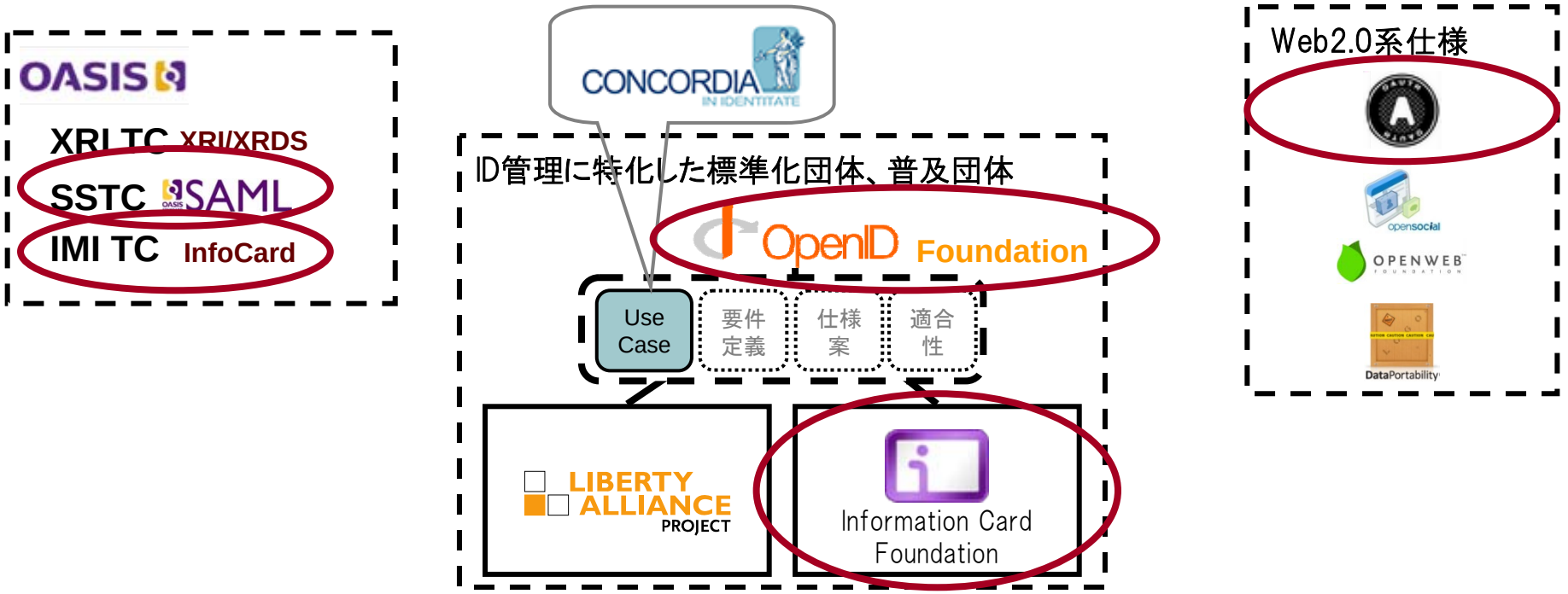
- 分科会の概要
  - 異なるID管理方式で構築されたシステムに跨がるサービスを提供する際に必要となる、技術要件／仕様間のコンテキスト変換方式等について議論を行うとともに、参加者向けに成果のアピールの場を設ける
- ワークショップ参加例
  - Burton Catalyst Conference Identity Public Workshop (2007-2009)
  - Digital ID World Workshop (2007, 2008)
  - RSA Conference Identity Workshop and Interop Demo (2008, 2009)
- これまでの主要参加メンバ
  - Microsoft, Oracle, Sun Microsystems, Cisco, NEC, GM, Boeing, Chevron
  - Google, PayPal, AOL, VeriSign, Ping Identity, Internet 2, NRI, NTT
  - 米連邦政府一般調達庁 (GSA)、米国陸軍、カナダ州政府機関、ニュージーランド政府

ID管理技術関係団体相関図



これまでの Concordia での取り組み例

kantara INITIATIVE



- SAML ⇔ CardSpace 相互運用 （2008年公開デモ実施）
  - デモ参加メンバ: Microsoft, Oracle, Inernet2, GSA, ニュージーランド政府 など
- SAML ⇔ OpenID 相互運用 （2009年公開デモ実施）
  - デモ参加メンバ: Oracle, NRI, NTT
- SAML ⇔ OAuth などの相互運用 （現在検討中）
- SAML Metadata の他のID管理方式への適用（現在検討中）

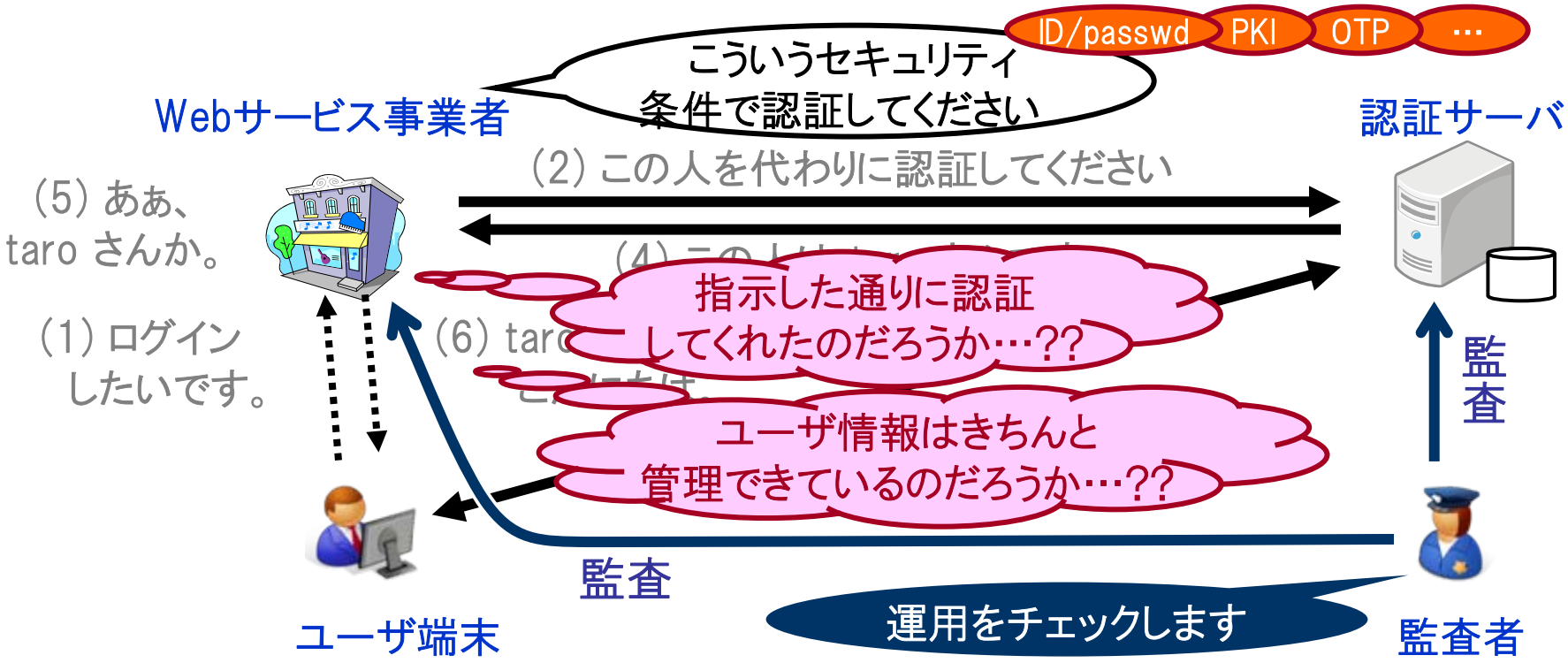
3. Identity Assurance WG

Identity Assurance WG

kantara INITIATIVE

❑ グループの概要

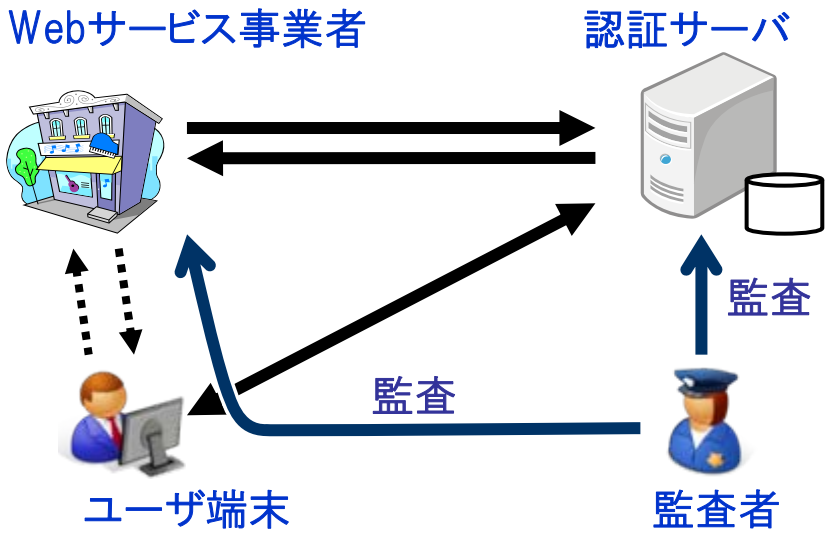
- ウェブサービス間の認証、アクセス制御の相互運用時の信頼性を担保する認証レベルの保障基準を策定する。
- 同基準の相互運用性を担保する為、同基準に基づく検証テストを実施、対応するサービスを認定する(予定)。



IAFで規定される基準

- 「認証(という行為)の保障レベル」の記述方式の規定
  - レベル1(ポータルへのログイン) ～ レベル4(医療情報等へのアクセス)

- 各保障レベルに応じて必要となる実装／管理運用体制に関する規定
  - サービス提供者が満たすべきアセスメント要件
    - **組織**が満たすべき要件
    - **組織が提供するサービス**において満たすべき要件
    - 組織が**クレデンシャルを発行する場合**に満たすべき要件
  - アセスメント事業者の要件
  - IAF の相互運用にあたって当事者間で必要な契約の要件
    - 参加者の役割や、参加者が負う義務等



4. P3 (Privacy and Public Policy) WG

Privacy & Public Policy WG (P3WG)

kantara INITIATIVE

グループの概要

- ネットワーク上で利用されるユーザのプライバシーを適切に管理する為のフレームワーク、ガイドラインを検討する。

現在のステータス

- プライバシー管理フレームワーク作成に向けた検討に着手済。
- IAF同様、ユーザアイデンティティの相互運用に際し必要となるプライバシー保証レベル(Level of Privacy（仮称))、およびプライバシー保護基準（Privacy Assurance Framework（仮称））を規定し、サービスおよびサービス事業者の監査、評価を行うことが検討されている。

		Level of Assurance			
		1	2	3	4
Level of Privacy	1				
	2				
	:				
	n				

Matrix of Assurance and Privacy

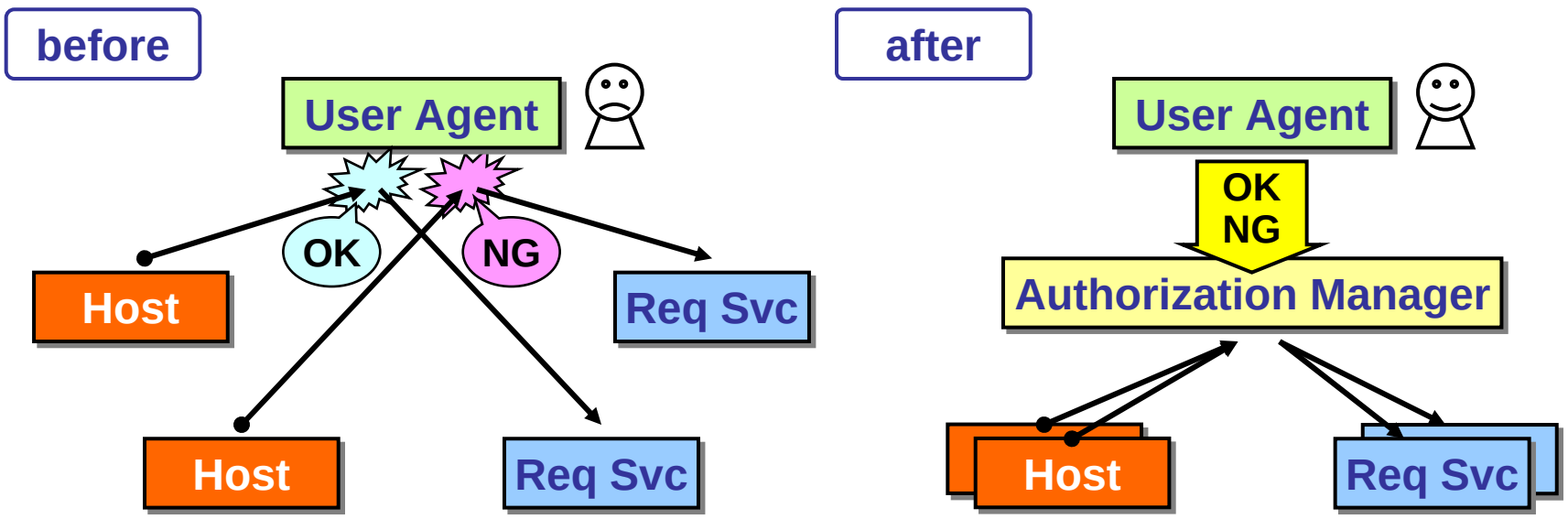
kantara INITIATIVE

5. UMA (User Management Access) WG

User Management Access (UMA)

kantara INITIATIVE

- グループの概要
  - 属性情報の第三者への提供可否等を判断するサービスを外部に移管し、ユーザが簡単かつ確実に管理できる環境を提供する方式を提案する。

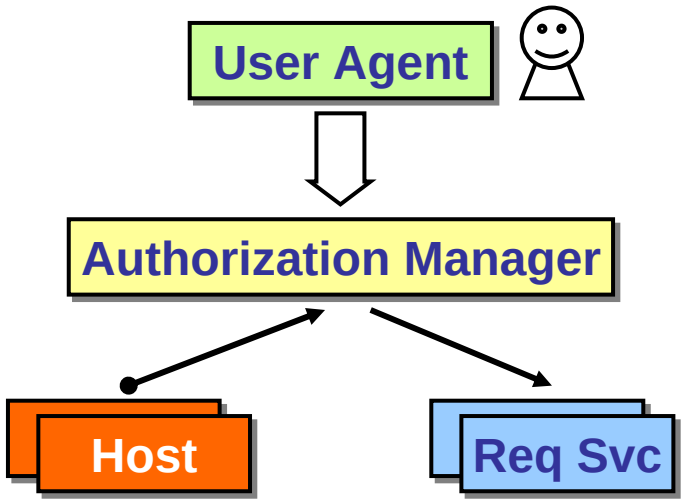


個々のサービスに対して
アクセスコントロールの判断が必要

アクセスコントロールを AM に集約し、
用語やインタフェイスを統一可能

UMA WG の活動状況

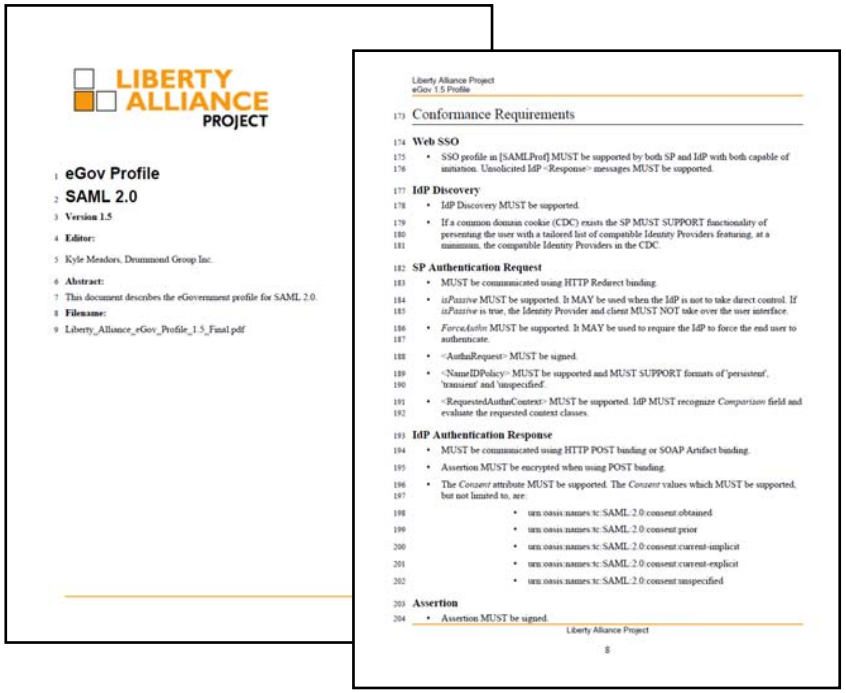
- 現在のステータス
  - 仕様策定に必要なユースケース、要求条件の収集
- 要求事項例
  - 個々のリソースのポリシー制御
  - Webベースのアクセス管理ポリシーの配布
  - ユーザによるアクセス管理ポリシーの設定
  - 認可管理サーバ（Authz Manager）による ユーザのアクセス証跡（audit log）の管理
- ユースケース例：
  - カレンダーの共有
  - eコマース
  - ローンの照会
  - 位置情報
  - 分散処理....



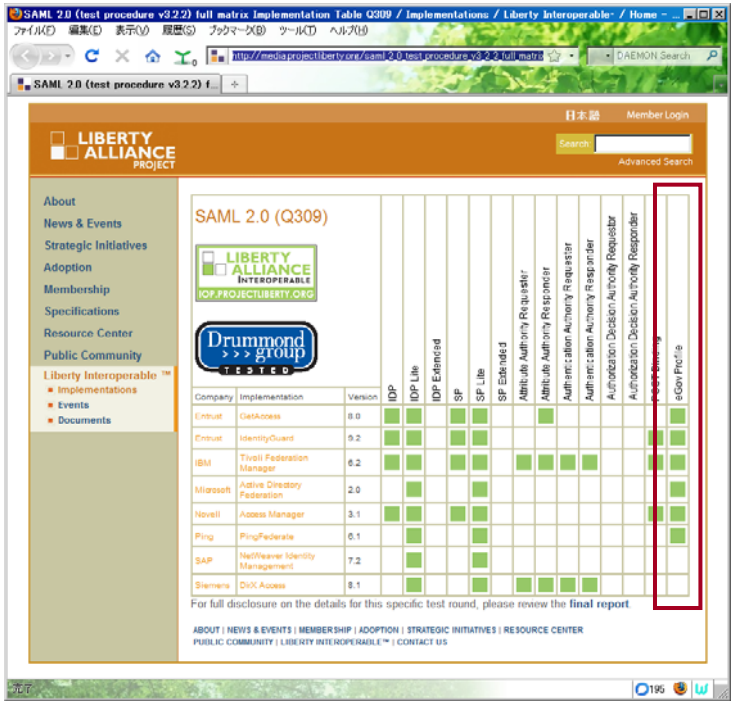
6. eGovernment WG

eGovernment WG

- グループの概要
  - 電子政府へのID管理技術の導入にあたって必要となる事例の収集、ホワイトペーパー、ガイドライン等の策定を行う



SAML 2.0 eGovernment Profile*



SAML 2.0 相互運用性テスト結果**

* http://www.projectliberty.org/liberty/liberty_interoperable/documents
** http://media.projectliberty.org/saml_2_0_test_procedure_v3_2_2_full_matrix_implementation_table_q309/

7. まとめ

本日のまとめ

- カンターラ･イニシアティブの分科会

- Concordia DG
- Identity Assurance Framework WG
- UMA (User Management Access) WG
- P3 (Privacy and Public Policy) WG
- eGovernment WG

おまけ

kantara INITIATIVE

@ITフォーラムにて連載させていただくことになりました

http://www.atmarkit.co.jp/fsecurity/rensai/kantara01/kantara01.html


kantara
INITIATIVE