

カンタラ・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

□ 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

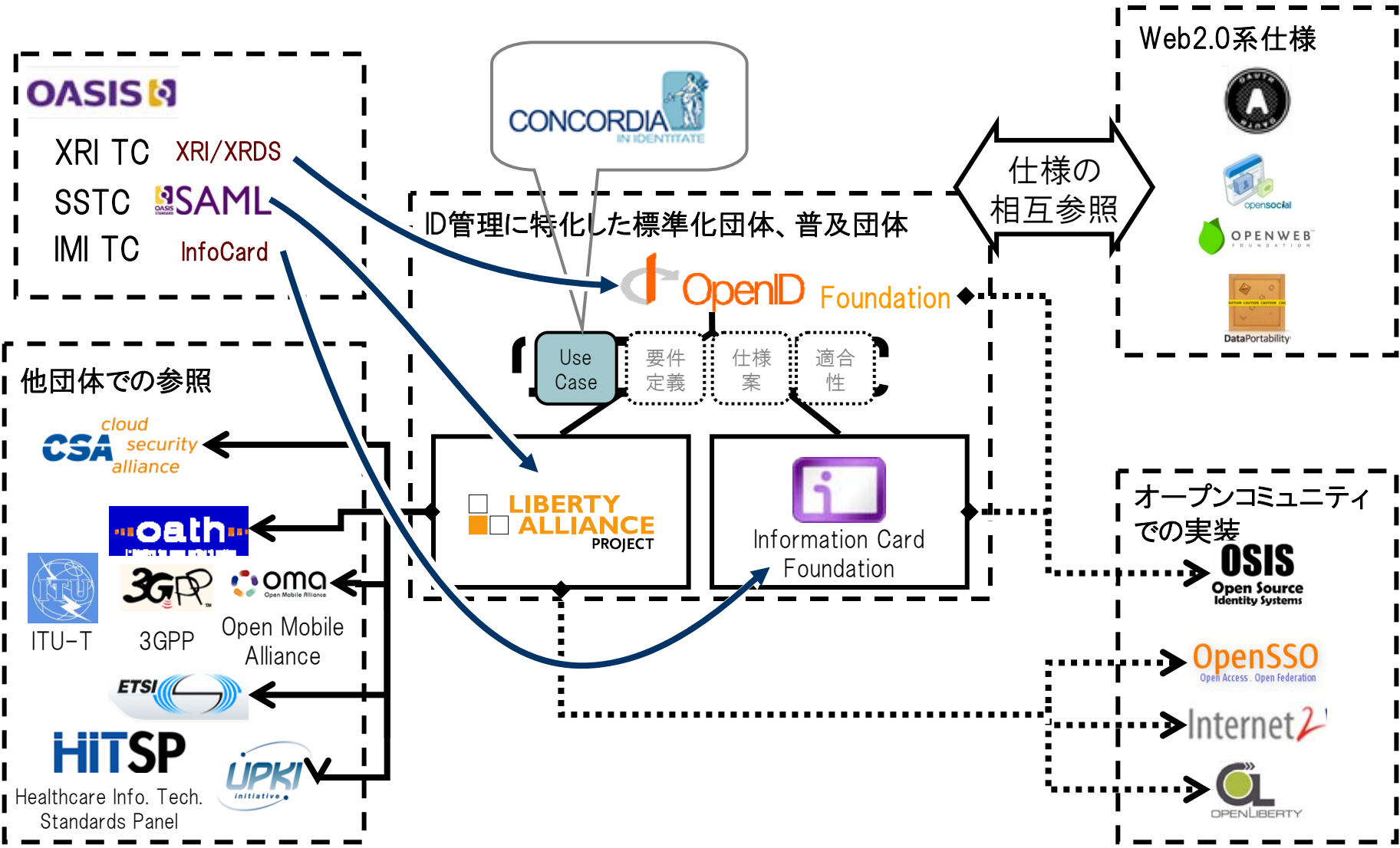
□ ワークショップ参加例

- Burton Catalyst Conference Identity Public Workshop (2007-2009)
- Digital ID World Workshop (2007, 2008)
- RSA Conference Identity Workshop and Interop Demo (2008, 2009)

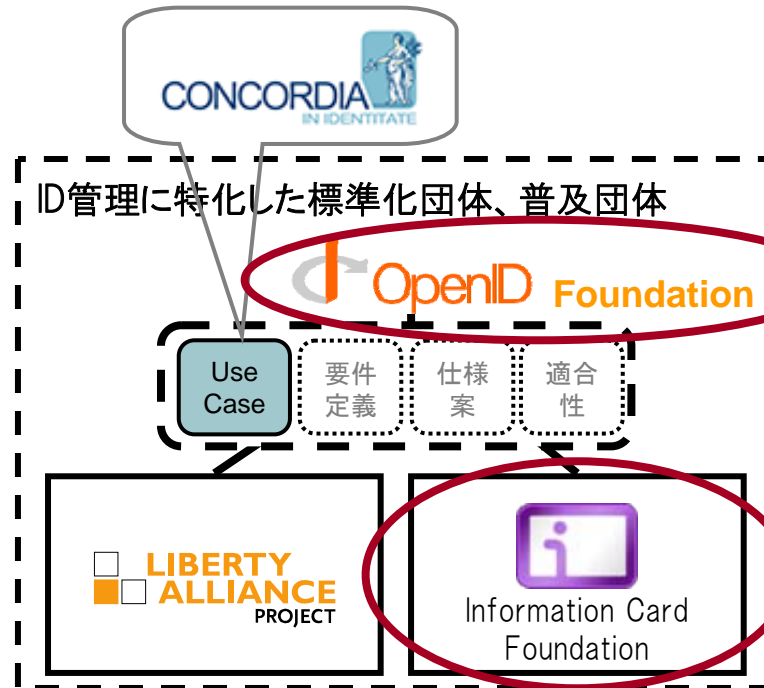
□ これまでの主要参加メンバ

- 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

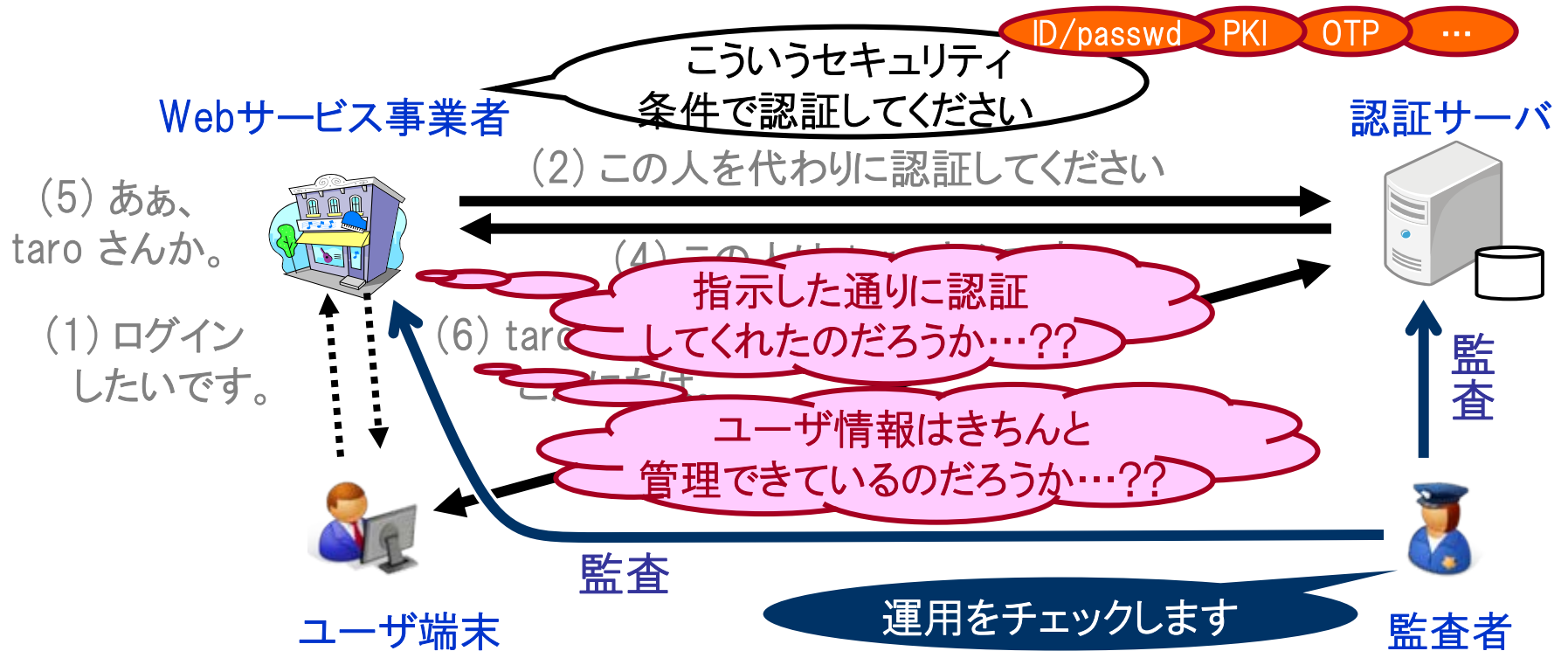


- ❑ SAML ⇔ CardSpace 相互運用（2008年公開デモ実施）
 - デモ参加メンバ: Microsoft, Oracle, Inernet2, GSA, ニュージーランド政府 など
- ❑ SAML ⇔ OpenID 相互運用（2009年公開デモ実施）
 - デモ参加メンバ: Oracle, NRI, NTT
- ❑ SAML ⇔ OAuth などの相互運用（現在検討中）
- ❑ SAML Metadata の他のID管理方式への適用（現在検討中）

3. Identity Assurance WG

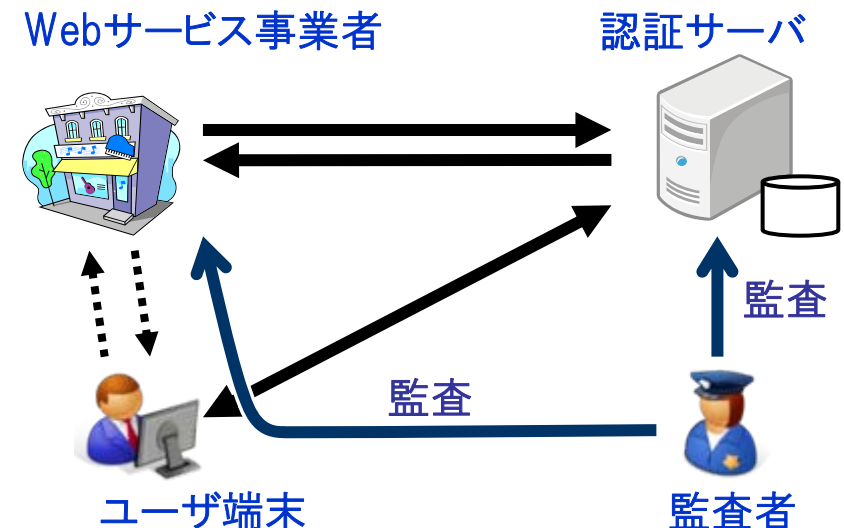
□ グループの概要

- 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

□ 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

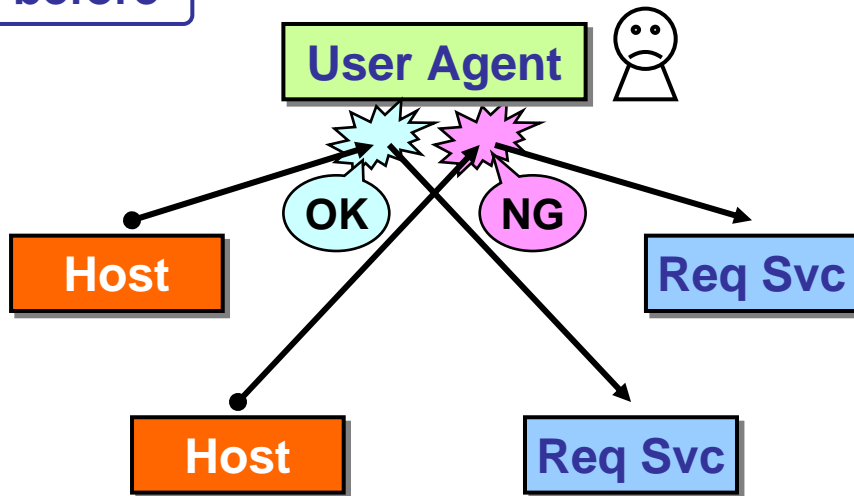
5. UMA (User Management Access) WG

User Management Access (UMA)

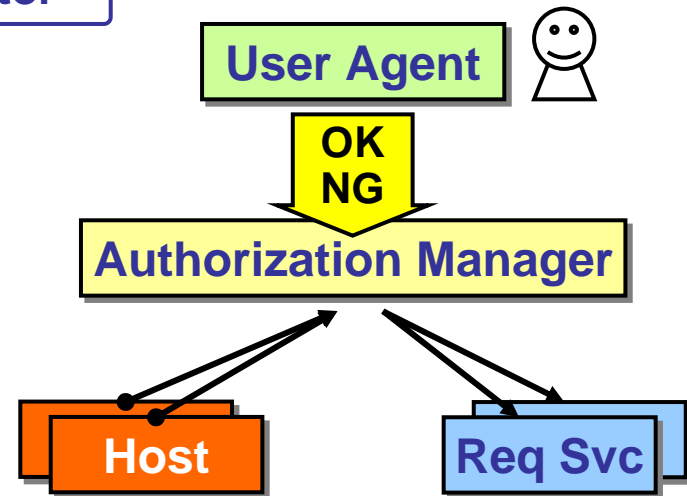
□ グループの概要

- 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。

before



after



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

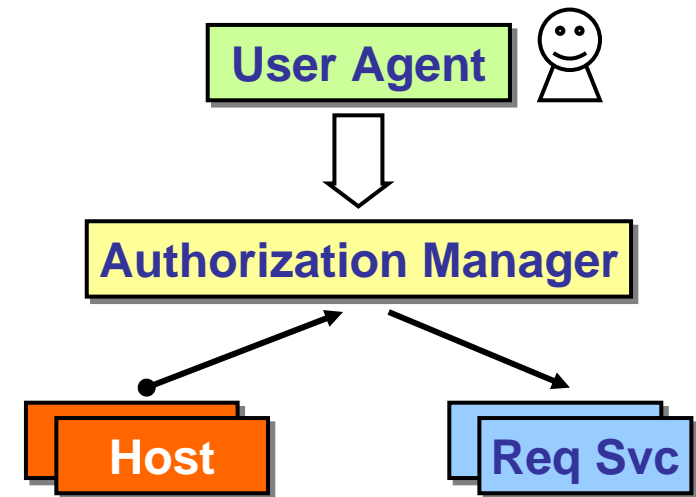
- 仕様策定に必要なユースケース、要求条件の収集

□ 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

□ 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

LIBERTY ALLIANCE PROJECT

eGov Profile
Version 1.5

174 Conformance Requirements

174 Web SSO

- 175 • SSO profile in [SAMLProf] MUST be supported by both SP and IDP with both capable of initiation. Unsolicited IDP ->Response- messages MUST be supported.

177 IDP Discovery

- 178 • IDP Discovery MUST be supported.
- 179 • If a common domain cookie (CDC) exists the SP MUST SUPPORT functionality of presenting the user with a tailored list of compatible Identity Providers featuring, at a minimum, the compatible Identity Providers in the CDC.

182 SP Authentication Request

- 183 • MUST be communicated using HTTP Redirect binding.
- 184 • idPassive MUST be supported. It MAY be used when the IDP is not to take direct control. If idPassive is true, the Identity Provider and client MUST NOT take over the user interface.
- 185 • ForceAuthn MUST be supported. It MAY be used to require the IDP to force the end user to authenticate.
- 186 • -AuthnRequest- MUST be signed.
- 187 • -NameIDPolicy- MUST be supported and MUST SUPPORT formats of 'persistent', 'transient' and 'unspecified'.
- 188 • -RequestedAuthnContext- MUST be supported. IDP MUST recognize Comparison field and evaluate the requested context classes.

193 IDP Authentication Response

- 194 • MUST be communicated using HTTP POST binding or SOAP Artifact binding.
- 195 • Assertion MUST be encrypted when using POST binding.
- 196 • The Consent attribute MUST be supported. The Consent values which MUST be supported, but not limited to, are:
- 197 • urn:osis:names:tc:SAML:2.0:consent:obtained
- 198 • urn:osis:names:tc:SAML:2.0:consent:prior
- 199 • urn:osis:names:tc:SAML:2.0:consent:current-implicit
- 200 • urn:osis:names:tc:SAML:2.0:consent:current-explicit
- 201 • urn:osis:names:tc:SAML:2.0:consent:current-implicit
- 202 • urn:osis:names:tc:SAML:2.0:consent:unspecified

203 Assertion

- 204 • Assertion MUST be signed.

Liberty Alliance Project
8

SAML 2.0 eGovernment Profile*

SAML 2.0 (Q309)

Company	Implementation	Version	IDP	IDP Life	IDP Enhanced	SP	SP Life	SP Enhanced	Attribute Authority Requester	Attribute Authority Responder	Authentication Authority Requester	Authentication Authority Responder	Authentication Decision Authority Requester	Authentication Decision Authority Responder	eGov Profile
Entrust	GetAccess	0.0	■	■	■	■	■	■	■	■	■	■	■	■	■
Entrust	IdentityGuard	0.2	■	■	■	■	■	■	■	■	■	■	■	■	■
IBM	Trust Federation Manager	0.2	■	■	■	■	■	■	■	■	■	■	■	■	■
Microsoft	Active Directory Federation	2.0	■	■	■	■	■	■	■	■	■	■	■	■	■
Novell	Access Manager	3.1	■	■	■	■	■	■	■	■	■	■	■	■	■
Ping	PingFederate	0.1	■	■	■	■	■	■	■	■	■	■	■	■	■
SAP	NetWeaver Identity Management	7.2	■	■	■	■	■	■	■	■	■	■	■	■	■
Siemens	DXX Access	0.1	■	■	■	■	■	■	■	■	■	■	■	■	■

For full disclosure on the details for this specific test round, please review the **final report**

ABOUT | NEWS & EVENTS | MEMBERSHIP | ADOPTION | STRATEGIC INITIATIVES | RESOURCE CENTER
PUBLIC COMMUNITY | LIBERTY INTEROPERABLE™ | CONTACT US

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

@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



「アイデンティティ管理」の周辺事情を整理しよう - @IT - Mozilla Firefox

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

「アイデンティティ管理」の周辺事情を整理しよう

アイデンティティ管理の新しい教科書

第1回「アイデンティティ管理」の周辺事情を整理しよう

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
伊藤 宏樹
2009/11/5

OpenIDにSAM-L、Liberty AllianceにInformation Card……。ここでもう一度、アイデンティティ管理をイチから学んでみませんか。ID管理の周辺情報をまとめ、新しい教科書として使える連載をスタートします(編集部)

ID管理って何だったっけ？

昨今のOpenIDの台頭や、マイクロソフトによる Windows CardSpaceの本格展開を契機として、「シングルサインオン (Single Sign-On)」や「連携アイデンティティ管理 (連携ID管理)」といった単語がようやく日の目を見るようになってきました。また、いまあるID管理技術をどう使い分けるか、あるいは異なるID管理技術同士の相互運用は可能なのかといった議論がまさに起きつつあるところ です。

本稿では、これからWeb上の複数サービスを束ねるID管理である「連携ID管理」(以下、ID管理)を勉強する人向けに、ID管理とは何か、またID管理技術に関する最近の状況、今後の展望、そして2009年6月に生まれたID管理に関する新しい団体、「カンタラ・イニシアティブ」の目指すところを簡単にまとめてみたいと思います。

完了

197

Security & Trust

スポンサーからのお知らせ

- ▶ 組込みもWindows 7! 今日から使える最新機能
マイクロソフトとユニタックスの講演、デモを
オンライン配信でいつでもどこでも見られます
- ▶ 【FW/UTM製品シェアNo1】FortiGateならCTCSP
最大60%OFF! 特価キャンペーン実施中!
自営オンサイト保守で安心のサービス品質
- ▶ その対策で、情報漏えいを防げますか?
エンドポイント、ストレージから
ネットワークまで包括的に根拠情報を保護!
- ▶ ユーザーに負担をかけず IT をリスクから保護
Microsoft Forefrontなら、
仕事の効率性を下げず、管理コストも削減!
- ▶ 製造業のERP組立・加工やERPプロセス最新事例
日配食品製造業事例(IBM)、医療機器メーカー
ERP導入事例(沖電気)、他多数→(11/19(木))

- PR -

オンライン・セミナー unidux

組込みだってWindows 7!!

今日からすぐ使える 最新機能 大活用

- 配信期間 2009/11/24 (火) ~11/30 (月)
- 定員 100名

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

