NTT

NTT Information Sharing Platform Laboratories
NTT 情報流通プラットフォーム研究所

UPKIシンポジウム2009

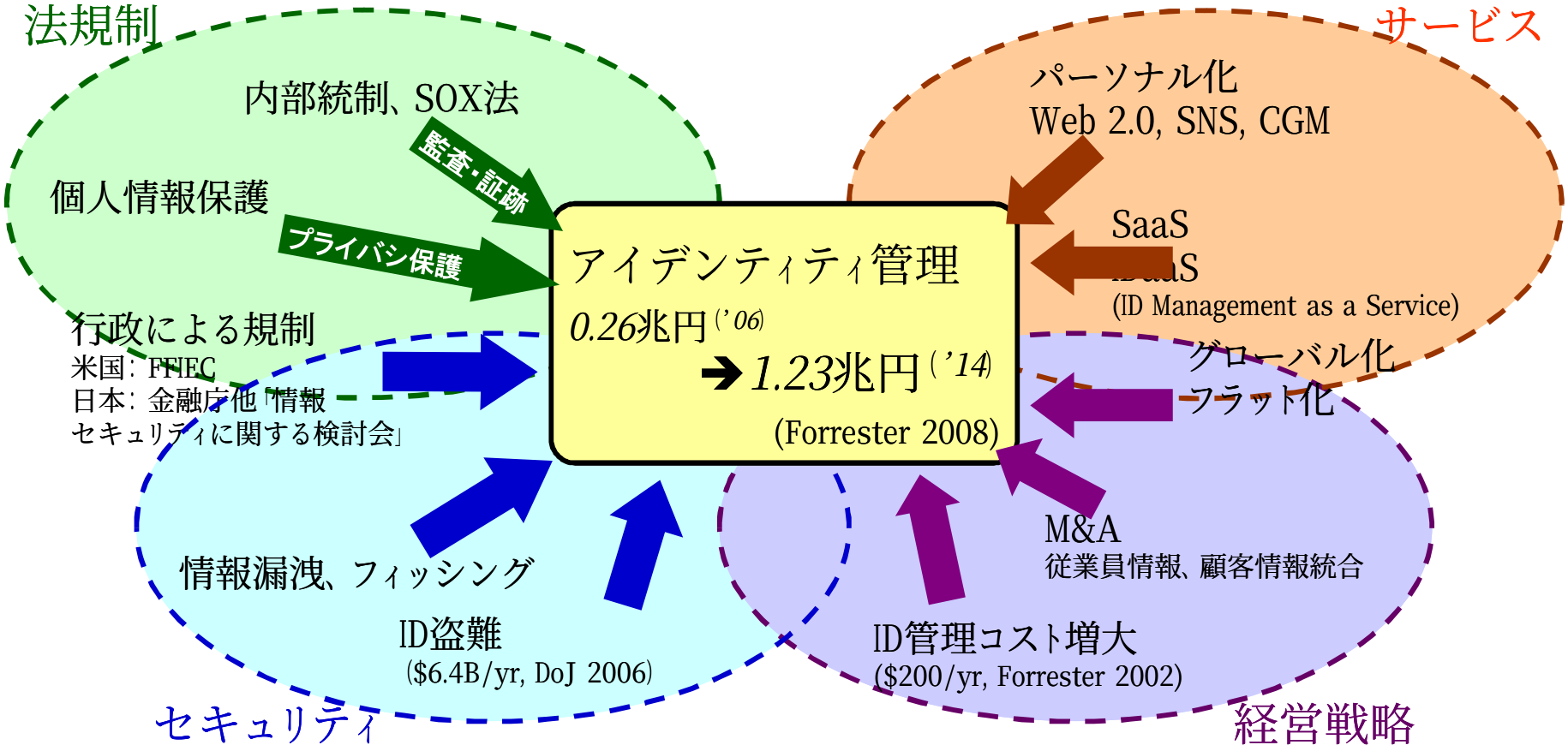
アイデンティティ管理技術の現状と今後
～リバティ・アライアンスに関して～

2009年2月23日

NTT 情報流通プラットフォーム研究所
下村道夫

高まるアイデンティティ管理の重要性

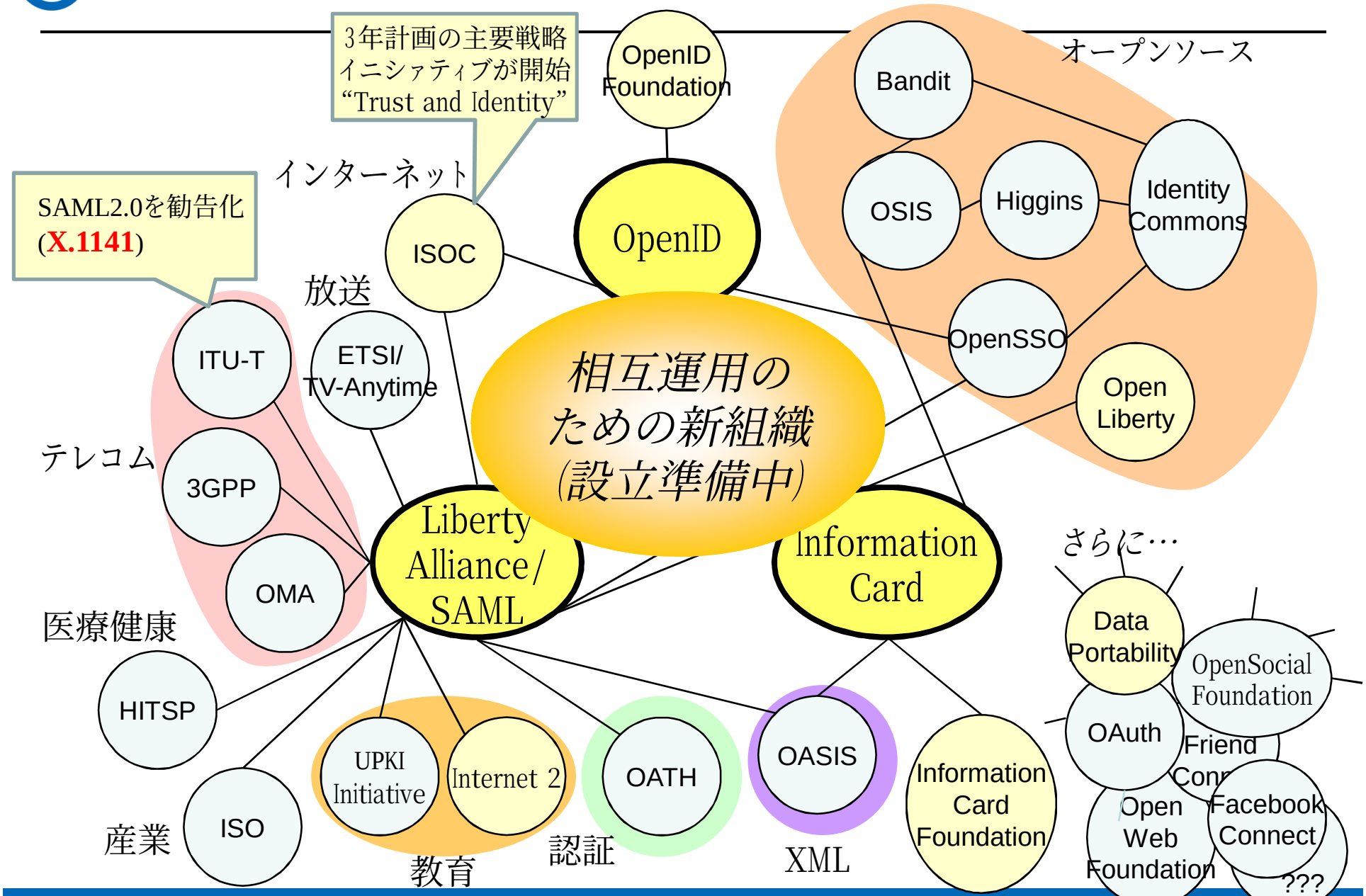
規制強化、セキュリティ被害の深刻化、経営効率化、オンラインサービスの普及拡大、といったトレンドを背景に、アイデンティティ管理の重要度が高まる見込み



アイデンティティ管理をめぐる3つの動き

方式	概要	主なプレイヤ
Liberty Alliance / SAML	「連携」モデルに基づくアイデンティティ管理の技術仕様	Liberty Alliance参加メンバ (AOL,BT, Internet Society, Intel, Oracle, Sun, GSA, Citigroup, Novell, France Telecom, Internet2, NEC, NHK, NTT他)
OpenID	URL / XRIをID(個人識別子)として用いるアイデンティティ管理技術仕様	OpenID Foundation参加メンバ (Microsoft, Verisign, IBM, Yahoo!, Google, Six Apart、Facebook等)
CardSpace	「カード」のメタファでアイデンティティ情報を管理する技術の総称	Information Card Foundation 参加メンバ (Equifax, Google, Microsoft, Novell, Oracle, Paypal, etc.)

アイデンティティ管理技術仕様の状況



リバティ・アライアンス

プライバシを保護した安心安全なアイデンティティ管理の実現のために、公開標準仕様の策定、普及、相互運用性の確保を推進するグローバルな業界団体

■ 2001年9月設立、150以上の企業・組織・団体が参加
- ITベンダ、テレコム、金融機関、政府組織、放送事業者、製造業等

■ 取組内容
- 様々なネットワークやデバイスに対応した公開標準仕様、ビジネスガイドライン、規制対応に関する白書等の提供
- 分野別の話題を議論する分科会(SIG：Special Interest Group)の運営
  - 日本, 医療情報, 電子政府, ID盗難防止, テレコム、人事教育等
- 相互運用性試験の運営実施
  - 米国では連邦調達庁 (GSA) が政府機関への調達条件として採用

リバティ・アライアンスの主なメンバ

http://www.projectliberty.org/liberty/membership/current_members

ボードメンバ

AOL, BT, ca, Fidelity Investments, Internet Society, intel, Novell, NTT, ORACLE, Sun

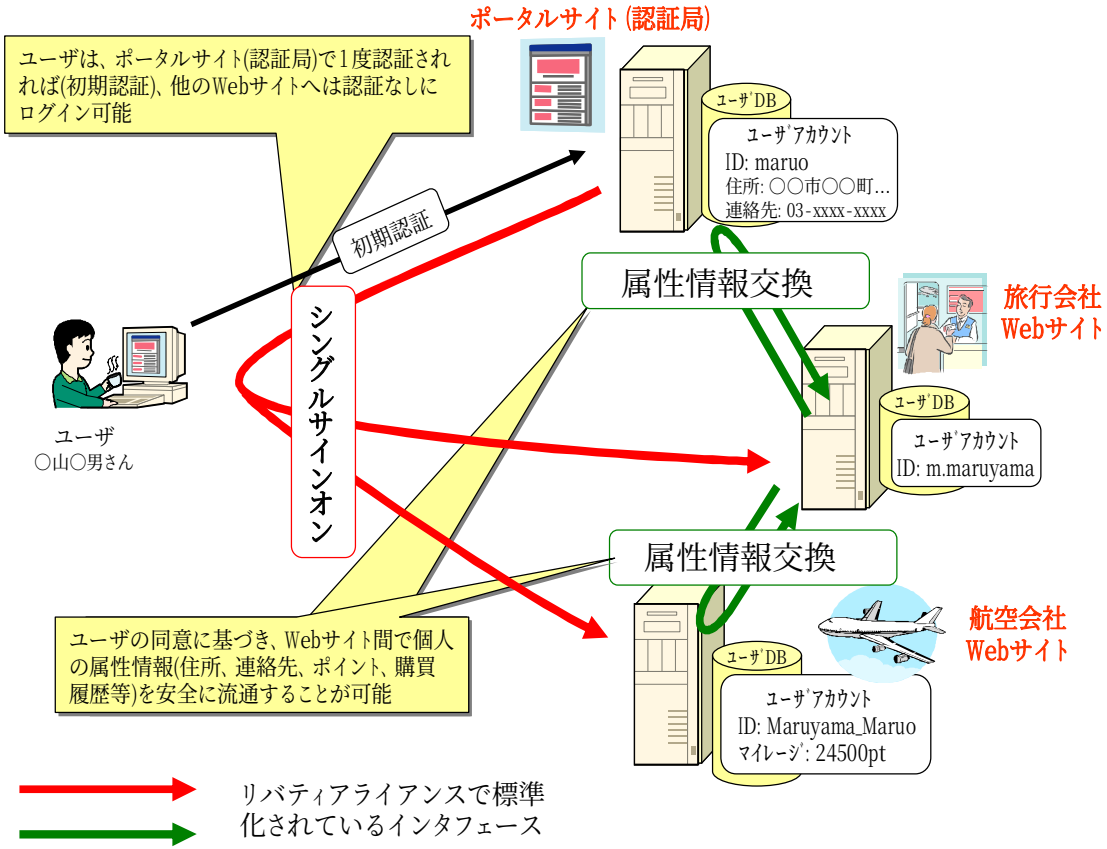
スポンサーメンバ

Adobe, BIPAC, 2e Prosperity Project, CATCert Agència Catalana de Certificació, citi, Clareity Security, T-..., Drummond group, EIFEL, ERICSSON, france telecom, FuGen Solutions, gemalto, GSA, kantega, Mortgage Bankers Association Investing in communities, NEC, NeuStar, NHK, NORTEL, PingIdentity, reach, SanDisk, State Services Commission Te Komihana O Ngā Tari Kāwanatanga, symLABS Identity Management Infrastructure, THALES, UNINETT, VeriSign, Zenn New Media, INTERNET 2, ...

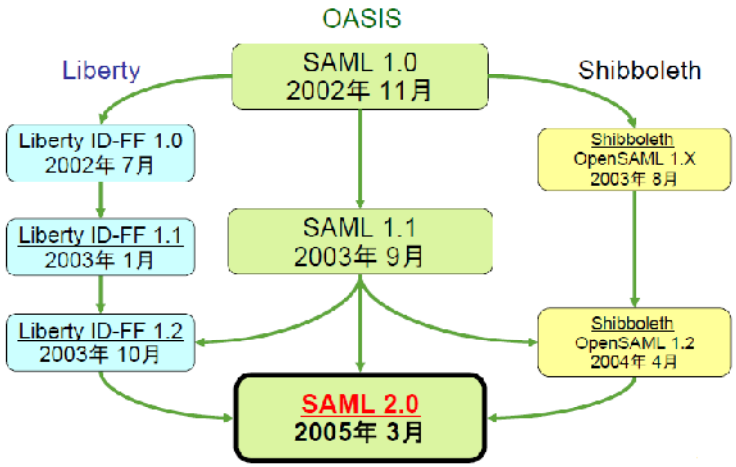
NTT シングルサインオン、属性情報交換の概要

- リバティアライアンスでは、複数のサイト間でID連携をベースとするシングルサインオン(認証結果情報の伝達)や属性情報交換等を行う技術仕様を策定している。
- 策定済み仕様例
  - ① SAML.2.0： Webサイト間でユーザID同士を連携し、シングルサインオンを実現する
  - ② ID-WSF2.0：Webサイト間で個人の属性情報をユーザの了解のもと、安全に交換する

SAML：Security Assertion Markup Language
ID-WSF：Identity Web Services Framework



SAMLの進化

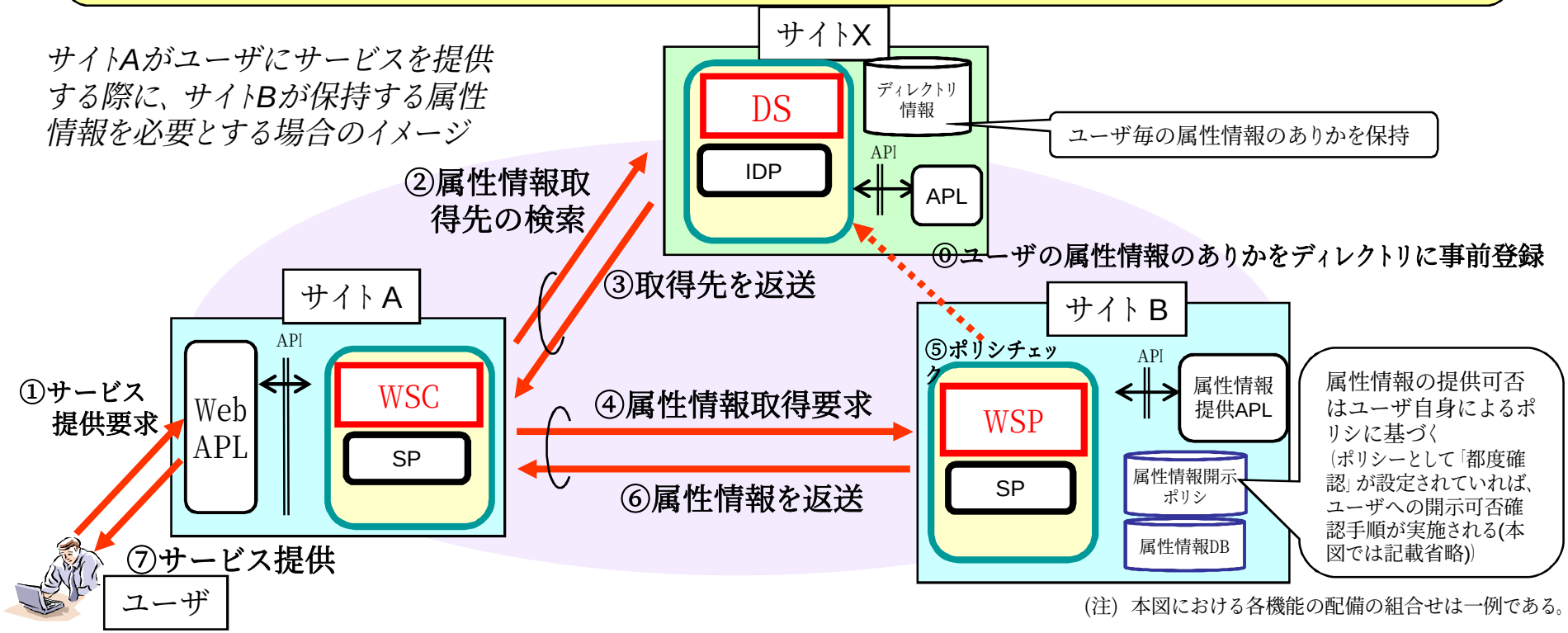


※出典：
http://wiki.projectliberty.org/images/9/94/080215_JapanSIG_Technical_Seminar.pdf

ID-WSF2.0 （属性情報交換）

・安全な属性情報の交換を実現するプロトコル
⇒属性情報管理サイトの発見、ユーザの了承の下でのサーバ間の属性情報の要求と応答、ポリシベースの開示制御、グループ（人間関係）の管理など

サイトAがユーザにサービスを提供する際に、サイトBが保持する属性情報を必要とする場合のイメージ



（注）本図における各機能の配備の組合せは一例である。

DS　Discovery Service：個人の属性情報のありかを提供する

WSP　Web Service Provider：個人の属性情報を提供する

WSC　Web Service Consumer：個人の属性情報を他のWebサイトから入手しユーザにサービスを提供する

属性情報交換に関する能力		SAML2.0	ID-WSF2.0
方向	IDP⇒SP	○	○
	SP⇒SP	×	○
	SP⇒IDP	×	○
オペレーション	生成	×	○
	通知	○	○
	更新	×	○
	削除	×	○
	更新時の通知	×	○

海外の具体的事例 (B2E, B2B, B2C)

主体	概要
企業内･企業間システム	･Boeing, Fidelity Investments, American Express, GM, Intel, HP, Sun, Star Alliance ⇒従業員向けに、企業内およびパートナー企業との業務効率化のためのポータルを提供。顧客向けのサービスへの展開も検討中。
モバイル＆テレコム事業者	･Orange/France Telecom, T-Online, Telefonica Moviles, TeliaSonera/Telenor, Bluewin (Swiss Telecom) ⇒外部サービス事業者連携や自社内のオペレーションコスト削減 ･T-Online (独テレコムの小会社) ⇒1200万のISPユーザに対し、SSO、アグリゲーション、個人情報管理、年齢証明サービスを実現。
Nokia	主力の携帯電話シリーズにリバティアライアンス標準対応のOSを組み込んで発売中
Google	Google AppsのAPIとしてSAML2.0を利用。
Microsoft Geneva	ActiveDirectoryの後継版で、SAML2.0サポートを表明
Salesforce.com	SAMLによるSSOを提供

海外での具体的事例（公共/教育系）

主体	概要
英国	各種電子政府システムへのSSOを実現（登録済ID：800万）。電子政府の各サイトへの国民の誘導と、各サイトでのユーザ登録システムとの連携とを狙う。
米国	・EduTechシステムによりNY州の公立学校（約７００校）システムのSSOを実現。教師1万人が登録済。 ・一般調達局(GSA)で政府システム間の連携標準技術として採用。
フィンランド	オンライン納税や公的文書の一元管理
ノルウェー	個人情報にアクセスする政府系マイページポータルをLiberty対応に移行へ
イタリア	運転免許更新サイトへのSSOを提供
オーストリア	市民認証カードによるオンラインバンキングのユーザ認証をLiberty対応に移行へ
NZ	電子政府サービスに省庁を越えたＳＳＯを提供
Internet2	Shibboleth 2.1 にて OpenSAML を採用し、SAML2.0に対応 ⇒導入例：英国高等教育機関の情報システム

日本国内での具体的事例

主体	概要
UPKI	UPKI認証連携基盤を用いたSSO実験。7大学が参加
公共系	・経産省、NiCT等の研究開発プロジェクトにおけるＳＳＯに利用 ⇒コンビニで源泉徴収等が印刷できるサービス実験を実施 ・EduMart ⇒総務省実証実験。教育コンテンツの流通システムへのSSO
NHK	デジタル放送受信機向け認証連携技術の研究開発
NTTデータ	・JAL ONLINE と出張旅費申請システムとの連携によるSSO ・イントラネット(2万ID、２００システム)とグループ企業ネットワーク(3万2千ID、２０ システム)との連携によるSSO
NTTコミュニケーションズ/NTTレゾナント	NTTコミュニケーションズ社のマスターIDと、NTTレゾナント社のgooIDとのSSO
NTTドコモ	Mydocomo IDを中心に、imode.net, DCMXminiとのSSO

検討中のトピック例

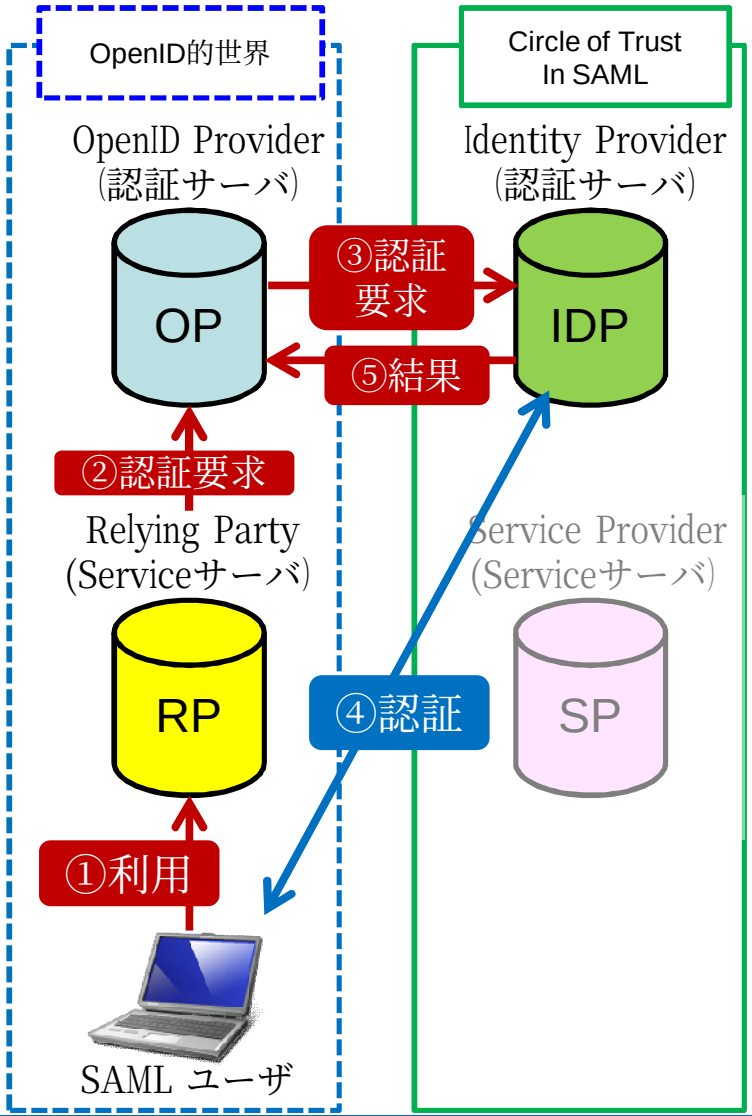
IAF（Identity Assurance Framework）

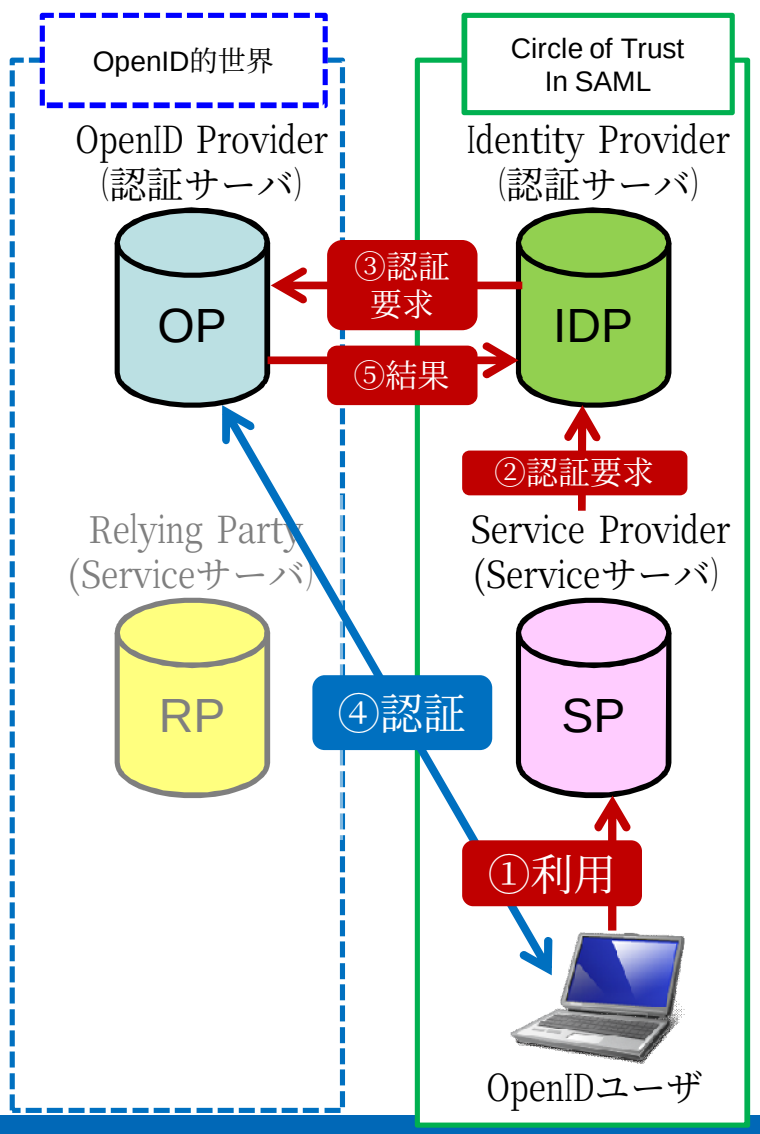
ID連携を行うWebサービス事業者間において、情報の信頼性等の相互確認等をより簡素化するための、ID情報の保証レベル、保証レベル毎に各事業者が満たすべき認証方式等の統一基準を規定する標準仕様。

章	見出し	概要
2	Assurance Levels （保証レベル）	個別のID情報に必要とされる信頼性を、用途から4段階に分類
3	Service Assessment Criteria （サービス評価基準）	ID情報を管理する上でサービス提供者が満たすべきアセスメント要件を • 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おいて満たすべき要件 の観点から4段階の Assurance Level 毎に規定
4	Accreditation and Certification Rules （認定と証明のルール）	IAF を満たした実装、運用を行っているか認定、証明を行う、アセスメント事業者が満たすべき要件を規定
5	Business Rules （ビジネスルール）	IAF の相互運用にあたって当事者間で必要な契約の要素（参加者の役割や、参加者が負うべき義務等）を規定

検討中のトピック例

コンコーディア：相互運用のユースケースの例





まとめ / 課題

■ 今後もさらなる導入が進む。

・仕様／ガイドライン／白書の充実化
・導入実績の積み重ね
・シングルサインオンに加えて属性情報交換も
・異種ID管理方式の相互接続

＜主な課題＞

・認知度向上
　エンドユーザ： セキュリティリスク／不便の認識
　サービス提供側： 費用対効果、適用領域の正しい認識
・費用対効果の共有、検証（⇒導入判断の材料）
・導入コスト削減
・強力で利便性の損なわれない初期認証手段の利用
　例：回線認証、ロケーション認証、ハードウェアトークン、PKI、バイオメトリクス
・IDの価値向上に伴う、攻撃の標的化への備え
・異種仕様間の相互運用性の確保

URLs

情報	URL
Liberty Alliance	http://www.projectliberty.org/
Liberty Alliance仕様書	http://www.projectliberty.org/liberty/resource_center/specifications
Liberty Alliance Japan SIG	http://wiki.projectliberty.org/index.php/JapanSIG
Liberty Alliance相互接続認定実装	http://www.projectliberty.org/liberty/liberty_interoperable/implementations
OASIS SSTC	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
SAMLチュートリアル	http://wiki.projectliberty.org/images/9/94/080215_JapanSIG_Technical_Seminar.pdf http://wiki.projectliberty.org/images/2/26/080718_LA_Technical_Workshop_SAML.pdf http://www.ntts.co.jp/publish/column/index.html#security
ID-WSFチュートリアル	http://wiki.projectliberty.org/images/1/13/Japan-sig-seminar-2-1_r1.pdf http://wiki.projectliberty.org/images/4/4b/Japan-sig-seminar-2-2.pdf
Concordia	http://projectconcordia.org/index.php/Main_Page
Web記事	「ID管理の案内人リバティ」(Open Enterprise Magazine、2006年10月号～2007年10月号) http://japan.zdnet.com/sp/feature/07liberty/
	「アイデンティティ管理の現在と未来」(Zdnet Japan特集、2007年9月～同年11月) http://www.sociusjapan.co.jp/OEM/OEM_IdentityTop.html
	「ID管理三国志時代の幕開けか」 http://www.atmarkit.co.jp/news/200808/05/id.html
	アイデンティティ管理の相互運用に向けて主要団体が取り組みを開始 http://www.sociusjapan.co.jp/OEM/200812/Sample_TP200812.pdf

情報	URL
LA,SAML製品例	Trust Bind/Federation Manager（NTTソフトウェア社） http://www.ntts.co.jp/products/trustbind/
	VANADIS SSO（NTTデータ社） http://bs.nttdata.co.jp/vim/relativesol/
LA、SAMLオープンソース例	http://www.openliberty.org/
	https://opensso.dev.java.net/ja/
	http://rnd.feide.no/simplesamlphp
	https://spaces.internet2.edu/display/OpenSAML/Home/
	http://www.eclipse.org/higgins/
	http://www.softwareborsen.dk/projekter/softwarecenter/brugerstyring
SAMLとOpenIDの比較例	http://identitymeme.org/doc/draft-hodges-saml-openid-compare.html
	http://www.xmlgrrl.com/blog/archives/2007/03/28/the-venn-of-identity/
	http://www.xmlgrrl.com/blog/archives/2007/08/07/the-three-faces-of-user-centricity/
	http://www.xmlgrrl.com/publications/fed-id-tech-27jul2007.pdf
	http://www.terena.org/activities/eurocamp/may08/slides/20080508-culloch-openID.pdf
SAMLのセキュリティ分析例	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
OpenIDのセキュリティ分析例	http://www.jisc.ac.uk/media/documents/programmes/einfrastructure/openid-finalreport-v1.0.pdf