



アイデンティティ管理技術と その利用事例

SACSIS2005:チュートリアル

2005年5月20日(金)

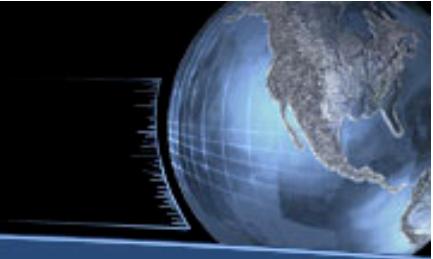
9時30分～11時00分

宮田・古賀

NTT

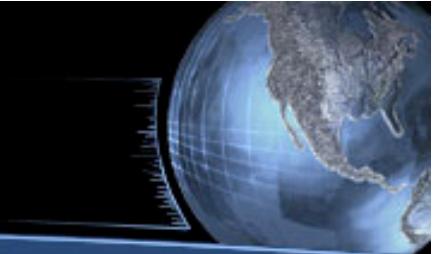
情報流通プラットフォーム研究所

発表者について



- NTT 情報流通プラットフォーム研究所
ユビキタスコンピューティング基盤プロジェクト
 - 宮田 輝子
 - 連携ID管理技術における標準化活動に従事。連携ID管理技術の導入事例拡大、関連標準化団体とのリエゾンを担当。普及促進活動の一環として技術チュートリアル発表および支援を行う(OASISチュートリアル2003、Liberty Alliance Tutorial 支援(2003))、ACM/CCS 2004 Tutorial “Identity Management”。

概要



本チュートリアルで目指すところ

1. 連携ID管理技術の概要

- はじめに
- SAML
- Liberty Alliance

2. ビジネス利用事例紹介

- 事例紹介: B2B, B2C
 - モバイル, ISP, およびデジタル放送



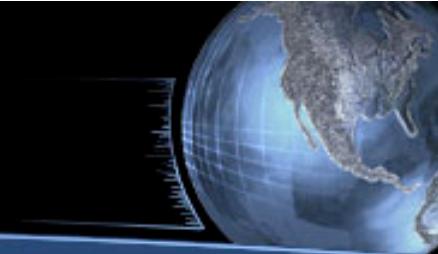
1. 連携ID管理技術 の概要

2005/05/20

SACSIS 2005

4

目次

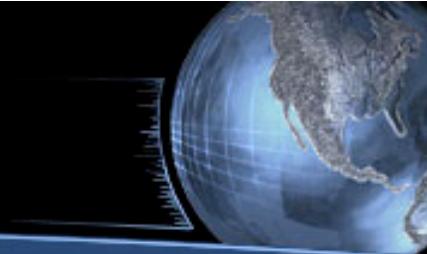


1. 連携ID管理技術の概要

- はじめに
- SAML
- Liberty Alliance

はじめに

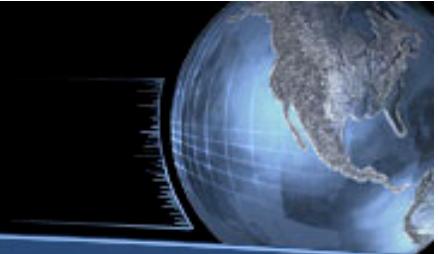
ID管理へのニーズの高まり



- アイデンティティ管理ソリューションの需要が企業間で高まる
 - 新規事業参入活発
 - 経費削減
 - 例: パスワード再設定要求依頼対応コストは6700円/1件
 - しかし利用者側ではプライバシやセキュリティに対する根強い懸念あり
- 広範囲にわたる事例拡大の障壁:
 - アイデンティティ管理技術の国際標準規格の不安
 - 製品およびサービスにおける相互接続性への不安
 - 連携モデルの不足
 - プライバシおよびセキュリティ実装の困難さ
 - ビジネス導入の難しさ

はじめに

ソリューションへの要求条件



- シンプル
- コスト削減
- セキュリティ
- プライバシ保護

はじめに

預託型ID管理と連携型ID管理

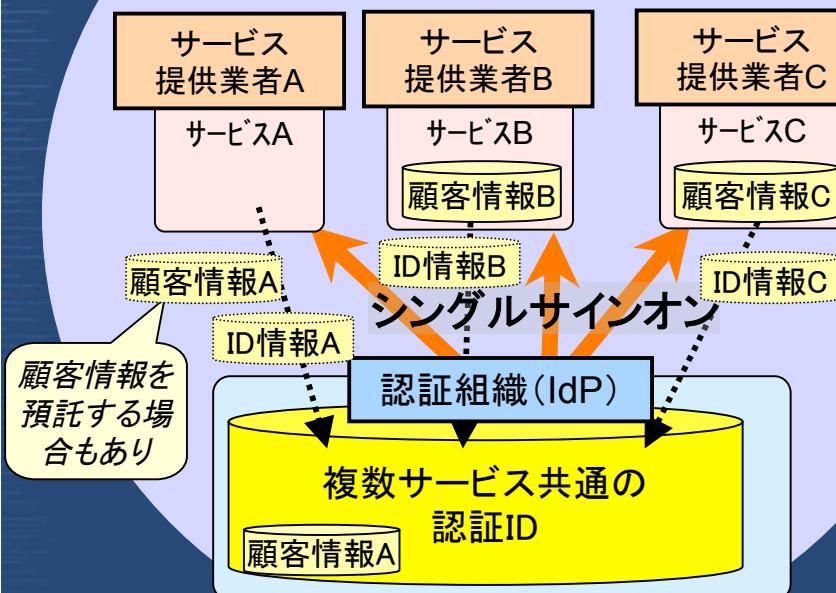
ID管理技術標準(リバティアライアンス)の「連携型のID管理」方式は、グループ会社の顧客ベースを仮想的に連携する事業戦略に適する

比較的小規模なサービス業者の囲い込み向け

独立したサービス業者間の柔軟な連携向け

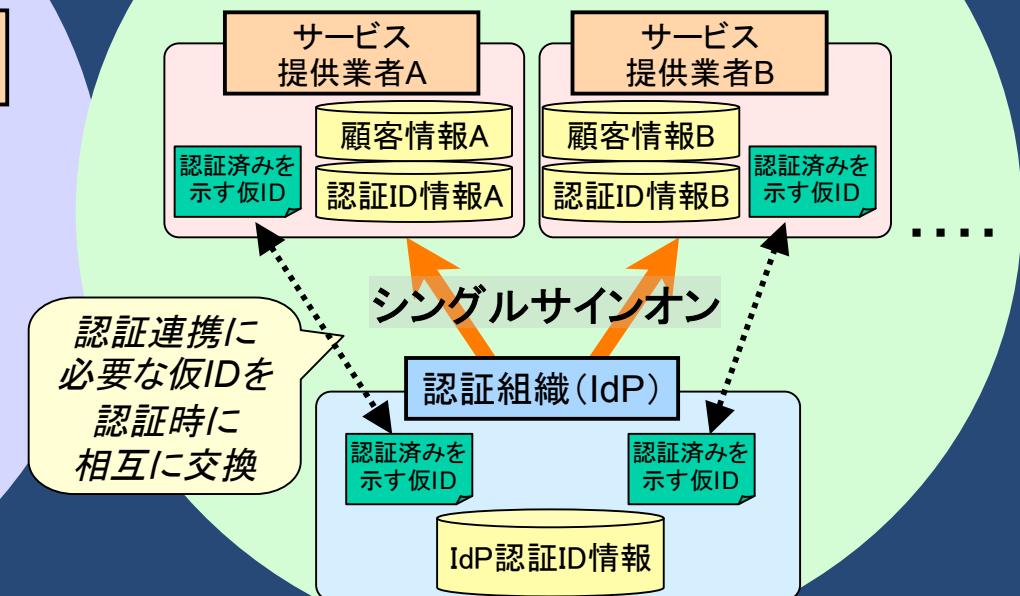
預託型ID管理

認証組織(IdP)にID情報を預託
複数サービス共通の認証用IDを利用



連携型ID管理

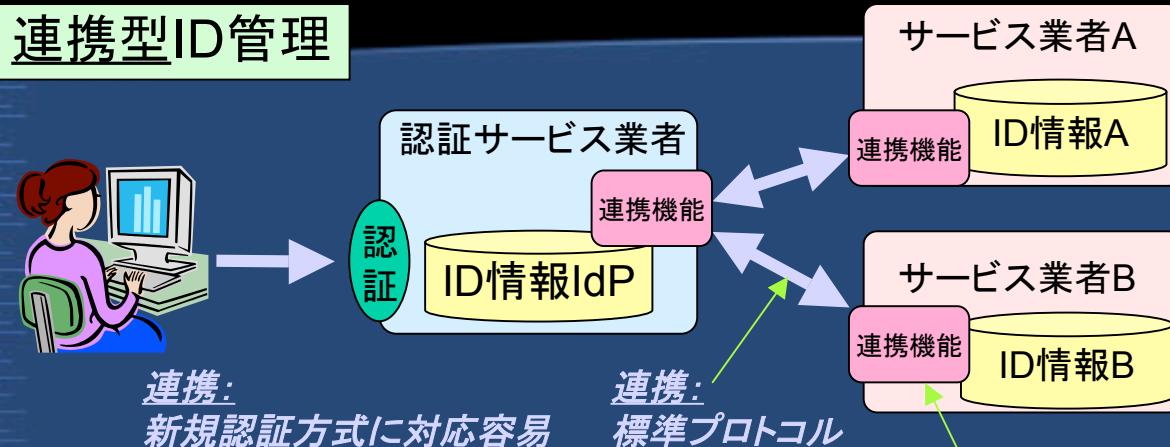
サービス提供者が(主体的に)ID管理
対等な立場で認証連携のみをIdPに委託



はじめに

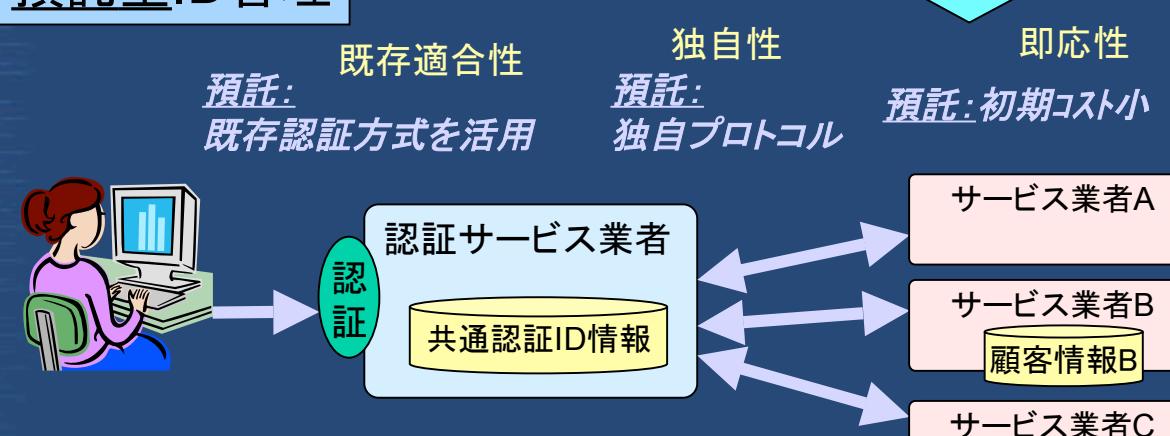
シングルサインオンサービス実現の判断ポイント

連携型ID管理



- 独立したグループ会社の連携向け
- 拡張性重視

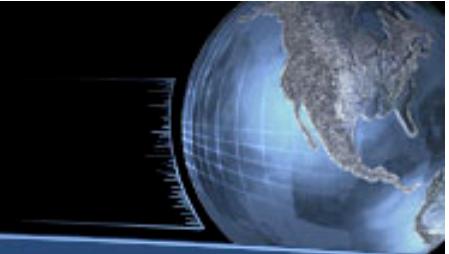
預託型ID管理



- 小規模業者の囲い込み向け
- 既存システム活用重視

はじめに

課題: 技術的観点から



- 國際標準策定団体の乱立
- 連携型アイデンティティ管理技術
 - SAML (OASIS SSTC)
 - Liberty Alliance

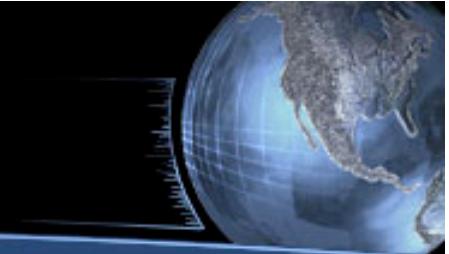
OASIS: Organization for the Advancement of Structured Information Standards

SSTC: Security Services Technical Committee

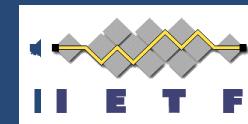
SAML: Security Assertion Markup Language

はじめに

国際標準策定団体



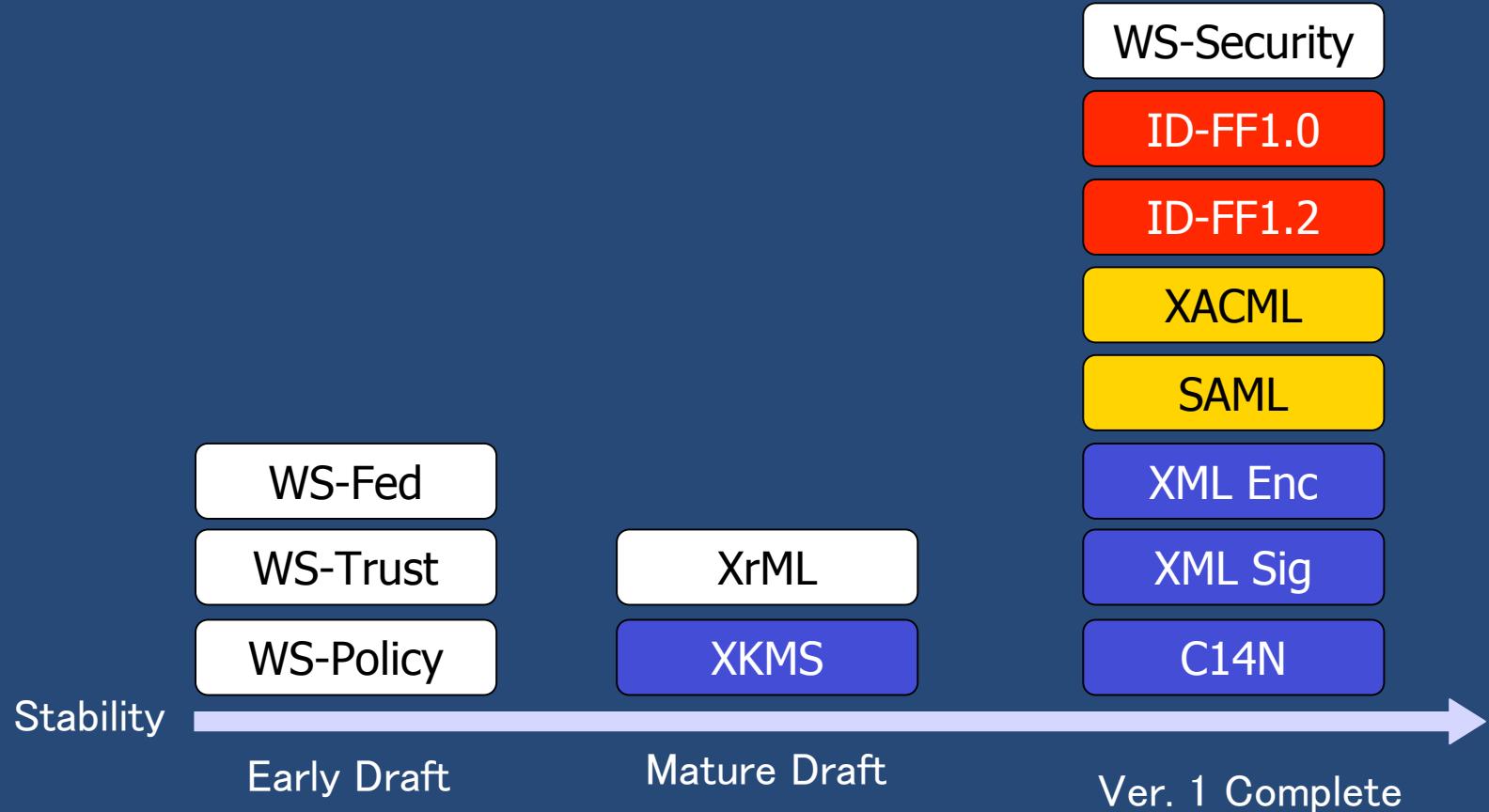
WPs



"Venn of Identity, Federation, and Secure Web Services",
Gary Ellison, Sun Microsystems

はじめに

国際標準仕様比較



"Venn of Identity, Federation, and Secure Web Services",

Gary Ellison, Sun Microsystems

W3C

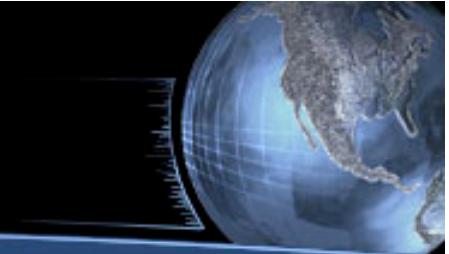
OASIS

Liberty

Private

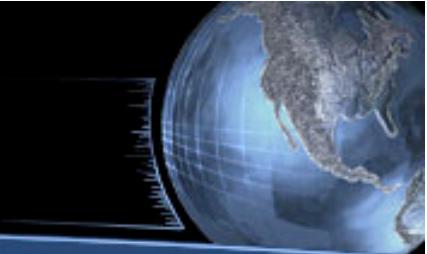
はじめに

課題：個人情報保護



- 預託型ID管理の場合
 - 複数のサービスを1つの共通IDで管理
 - 中央管理組織が必要。
 - オペレーションコスト増大
 - <名寄せ>リスク高
 - 個人情報・プライバシ保護への関心の高まり
 - ↓
 - 連携型ID管理への関心高まり。

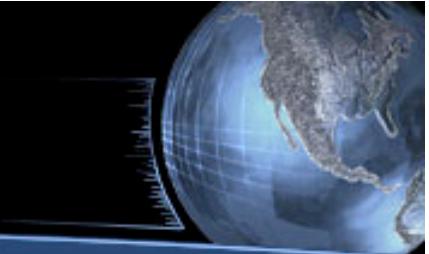
目次



1. 連携ID管理技術の概要

- はじめに
- SAML
- Liberty Alliance

OASISとは？

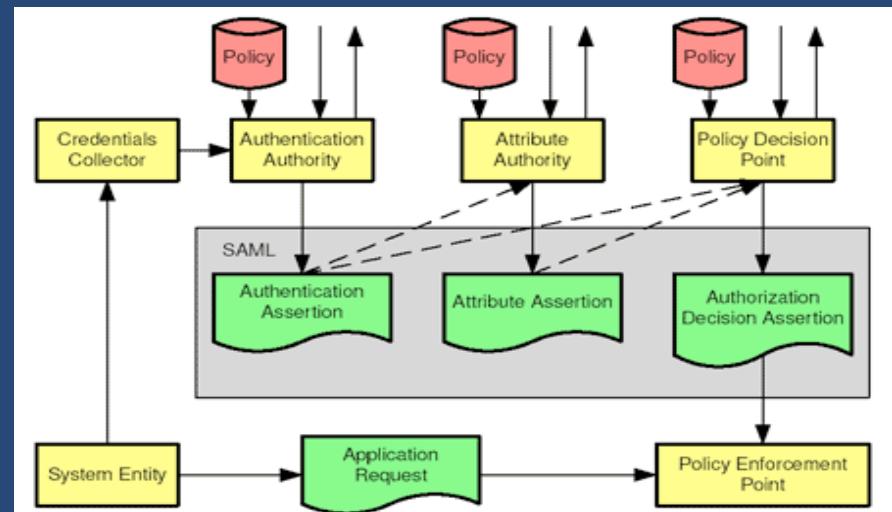


- e-businessを(主にXMLベースで)実現することを目的として、技術仕様を標準化している非営利の団体
 - ベンダニュートラルな印象が強い
 - 1993年に設立され、現在は600以上の組織体が加入している
- 主なボードメンバ
 - BEA Systems, Intel, Sun, Nokia, HP, Microsoft, Oracle, IBM
- 主な標準化技術
 - ebXML, SAML, SPML, UDDI, WSS, XACML

SAML: Security Assertion Markup Language, SPML: Service Provisioning Markup Language,
WSS: Web Services Security, XACML: Extensible Access Control Markup Language

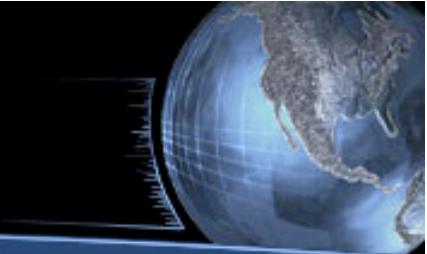
SAMLとは？

- 認証情報、属性情報、そして認可情報を運ぶためのXMLフレームワーク：
 - SAMLアサーション仕様：
 - 認証情報記述方式
 - SAMLプロトコル仕様
 - 認証/認可情報転送方式
 - OASIS SSTCで標準化
 - 主なメンバ
 - AOL, BEA Systems, Entrust, HP, IBM, Nokia, RSA Security, SAP, Sun
 - 状況
 - 現在SAMLv2.0公開(2005Q1)
 - 日米欧で注目される
 - 特に政府機関など
- 主にできること：認証/認可情報の相互運用
 - シングルサインオン
 - 認証/認可決定機関のアウトソーシング
 - 認可決定に他の機関を利用



SSTC: Security Services Technical Committee
SAML: Security Assertion Markup Language

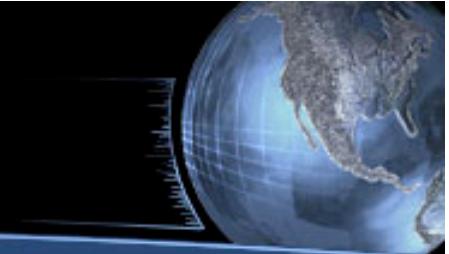
目次



1. 連携ID管理技術の概要

- はじめに
- SAML
- Liberty Alliance

Liberty Alliance



- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification

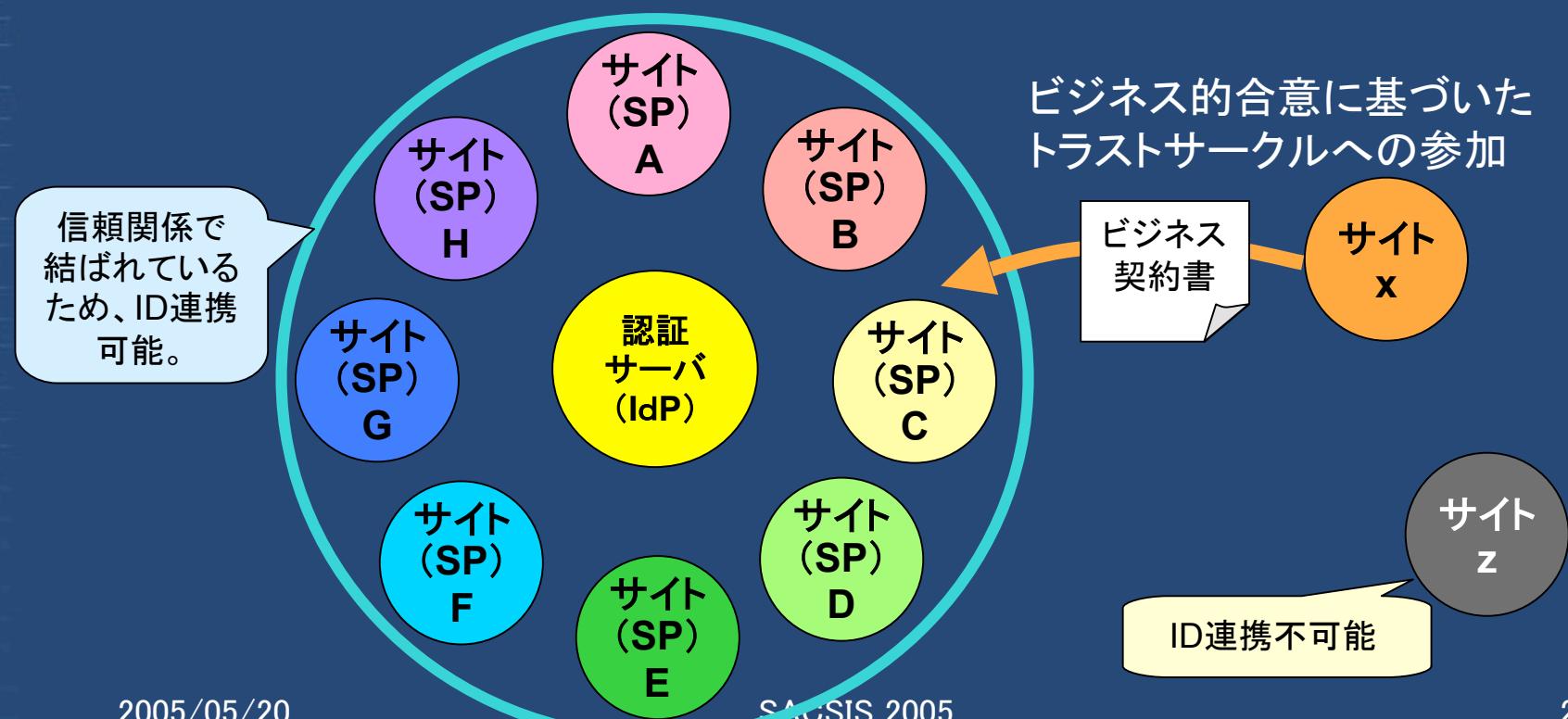
略語用語解説

Single Sign On (シングルサインオン)	一度の認証で複数のサービスへログインすることを指します。「SSO(エスエスオ一)」と略す場合がある。
Liberty Alliance (リバティアライアンス)	シングルサインオンを実現するID連携のプロトコルなどを規定した仕様。「Liberty(リバティ)」、「LA(エルエー)」と略す場合がある。
ID (アイディー)	個人を識別するための情報を指す。システムにおける「ユーザーアカウント」も狭義のIDの1種。「アイデンティティ」とも呼ぶ。
ID連携 (アイディーれんけい)	1個人が複数のサービス上で保有している各IDを互いに関連づけることを指す。これにより、シングルサインオンのような、複数サービスにまたがったサービスを提供することが可能。 リバティアライアンス仕様では狭義の意味で、IdPとSPの間で、SP自身が個別に管理しているIDと、IdP上のIDとを仮名を利用して関連づけることを指す。
IdP (アイディーピー)	アイデンティティプロバイダ(Identity Provider)の略。シングルサインオンのためのID情報を統合管理。文脈によって、認証組織を指す場合と、認証サーバそのものを指す場合がある。
SP (エスピ一)	サービスプロバイダ(Service Provider)の略。エンドユーザーにサービスや商品を提供。具体的にはECサイトなどのサービスサイトを指す。文脈によって、サービス提供組織を指す場合と、サービスサイトそのものを指す場合がある。
仮名 (かめい)	SPとIdPの当事者間でのみ仮のIDとして通用するランダム文字列。この仮名を利用することで、IdPとSPのそれぞれが保持する真のIDそのものをネットワークに流さずにID連携を実現可能。

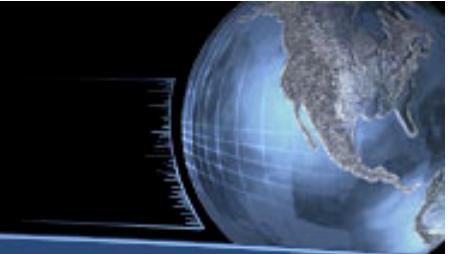
※ 詳細は、以下参照：「Liberty・アーキテクチャ用語集 v1.1」
[\(http://www.projectliberty.org/jp/resources/liberty-architecture-tech-glossary-v1.1-JP.pdf\)](http://www.projectliberty.org/jp/resources/liberty-architecture-tech-glossary-v1.1-JP.pdf)

Circle of Trust (CoT)

- ビジネス的な合意によるトラストサークル(信頼の輪)が形成された範囲内でのみ、ID連携が可能。
- ネットワークなど物理的に接続されている全てのサービスサイトが、ID連携する訳ではない。

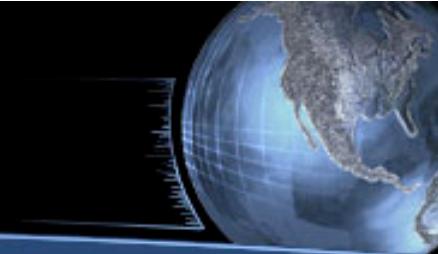


Liberty Alliance



- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification

Libertyアーキテクチャ



- Libertyアーキテクチャは複数階層の仕様の集合であり、それらはSAMLとSOAPに基づいている。Libertyには3つの主なコンポーネントから構成される。
 - ID-FF (Identity Federation Framework)
 - 複数のベンダによるアイデンティティ連携ネットワークを構築可能にするための、コアプロトコル、スキーマ、そして具体的なプロファイルを定義している。
 - 複数サイト間でのシングルサインオン(アイデンティティ連携)やシングルログアウト、サイト間の提携、認証ドメイン間の連携、そして匿名サインオン等が可能となる。
 - ID-WSF (Identity Web Services Framework)
 - アイデンティティサービスの生成、発見、そして利用(消費)というような基本的なフレームワークを提供するための、スキーマ、プロトコル、そして具体的なプロファイルを定義。
 - アイデンティティサービスで用いられる用語を提供する概念モデルをも定義。ディスカバリサービスといったようないくつかの基本的なアイデンティティサービスは、ID-WSF仕様の一部として規範的に定義されている。
 - パーミッションに基づくサービスサイト間での個人情報共有、アイデンティティサービスの発見、アイデンティティサービスの呼び出し等が可能となる。
 - ID-SIS (Identity Service Interface Specifications)
 - 具体的なアイデンティティサービスを利用するためのインターフェースを定義している。
 - 個人プロファイルサービス、プレゼンスサービス等が仕様化されている。

アーキテクチャ概要



Libertyアイデンティティ連携フレームワーク (ID-FF)

アイデンティティ/アカウントリンクage、シングルサインオン、およびセッション管理等の特徴をもつアイデンティティ連携と管理が可能

Libertyアイデンティティサービス・インターフェース仕様(ID SIS)

パーソナルプロファイルサービス、アラートサービス、カレンダーサービス、ウォレットサービス、コンタクトサービス、位置情報サービス、プレゼンスサービス等のアイデンティティサービスが可能

LibertyアイデンティティWebサービス・フレームワーク(ID-WSF)

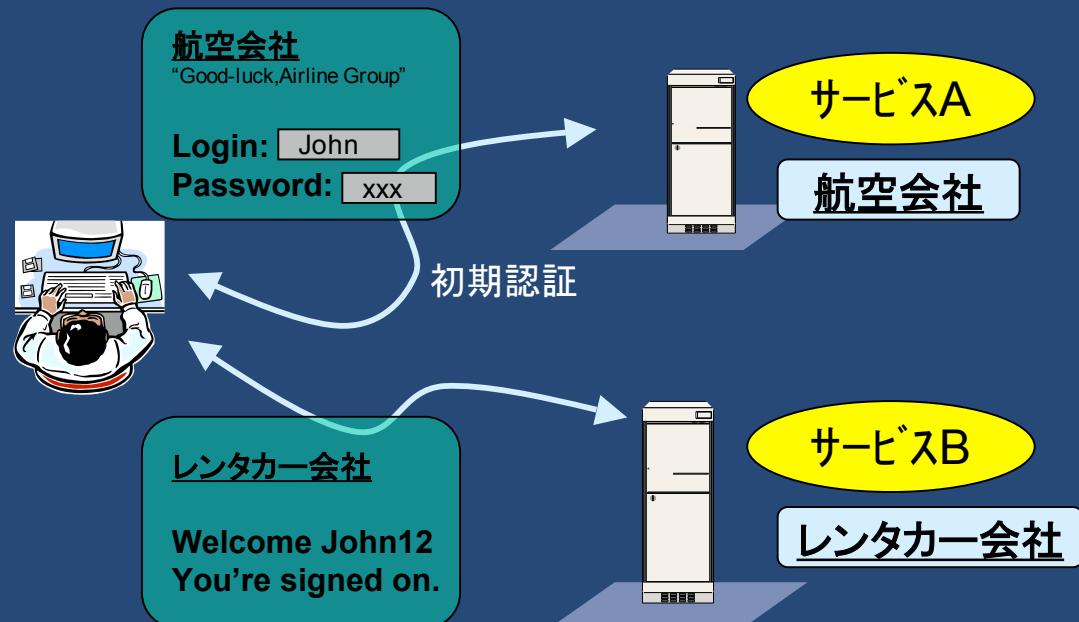
相互接続可能なアイデンティティサービス、許可ベースの属性共有、アイデンティティサービス記述、ディスカバリ、および関係するセキュリティプロファイルを作成・構築するためのフレームワークを提供

Liberty仕様は既存の標準仕様に準拠
(SAML, SOAP, WSS, XML, etc.)

Liberty Allianceでできること(1)

- 複数サービスサイトへのシングルサインオン
 - 一度の認証処理で複数のサービスサイトを利用可能.

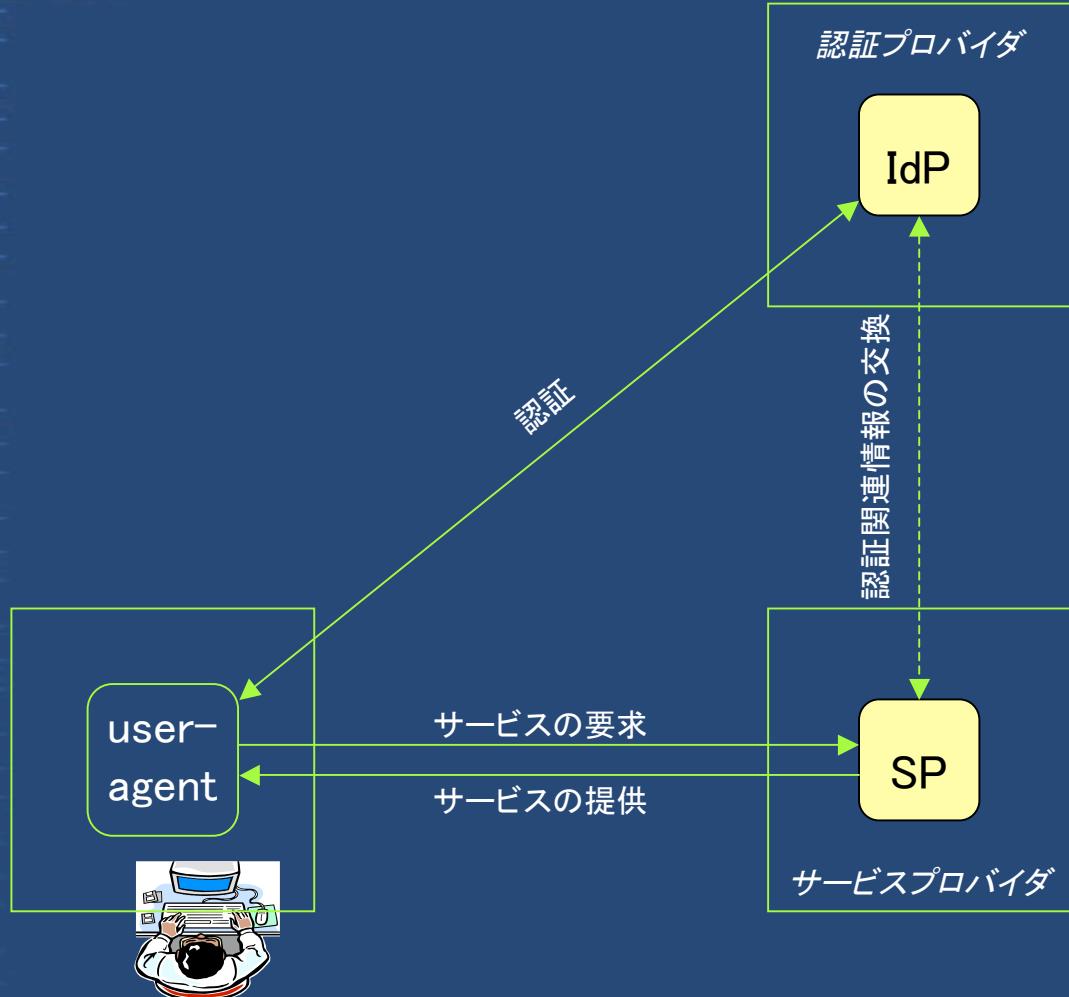
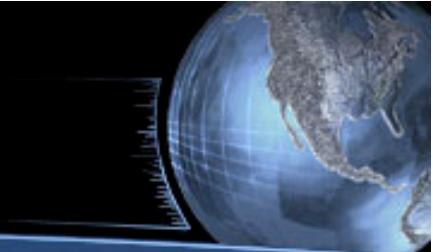
それぞれのサービスごとに認証を受ける必要はなく、一度認証を受ければ、他のサービスもそのまま利用が可能なシングルサインオンを実現.



[Liberty Allianceであることのメリット]

- ・標準化「シングルサインオン」のため、他社システムとの相互運用が可能です.

モジュール構成 (シングルサインオン)



IdP: Identity Provider, SP: Service Provider

SACSS 2005

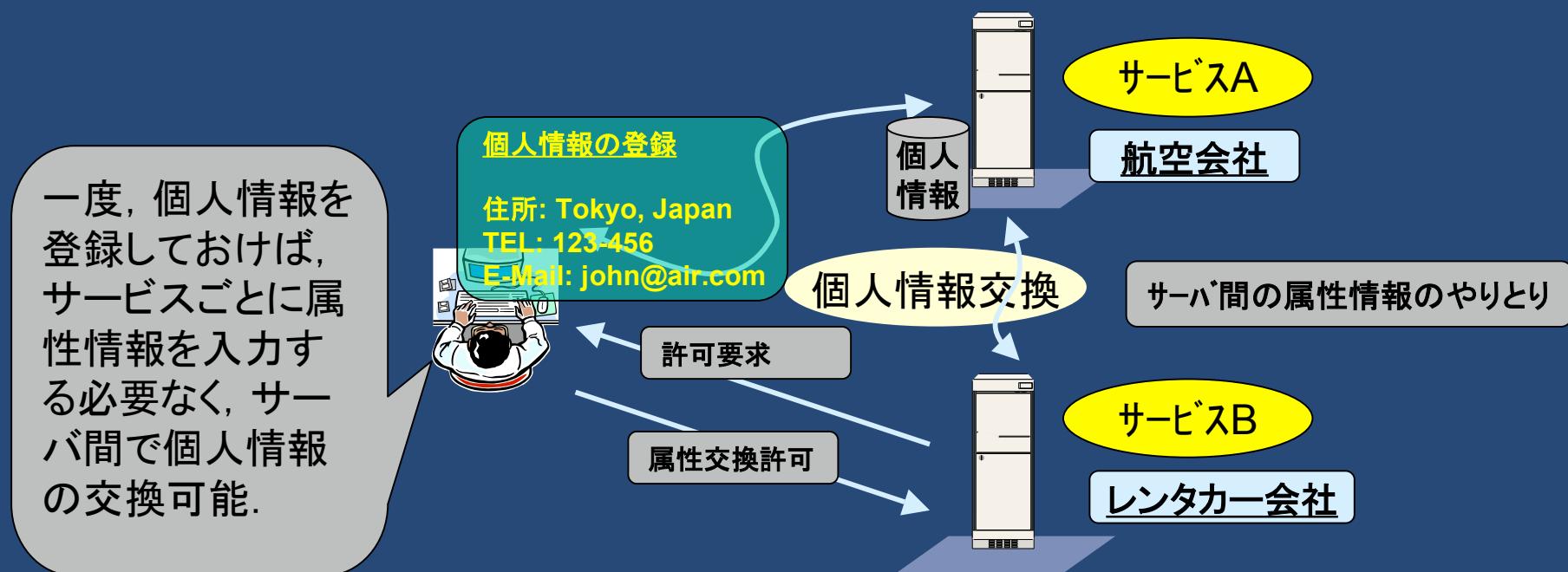
2005/05/20

NTT Platform labs.

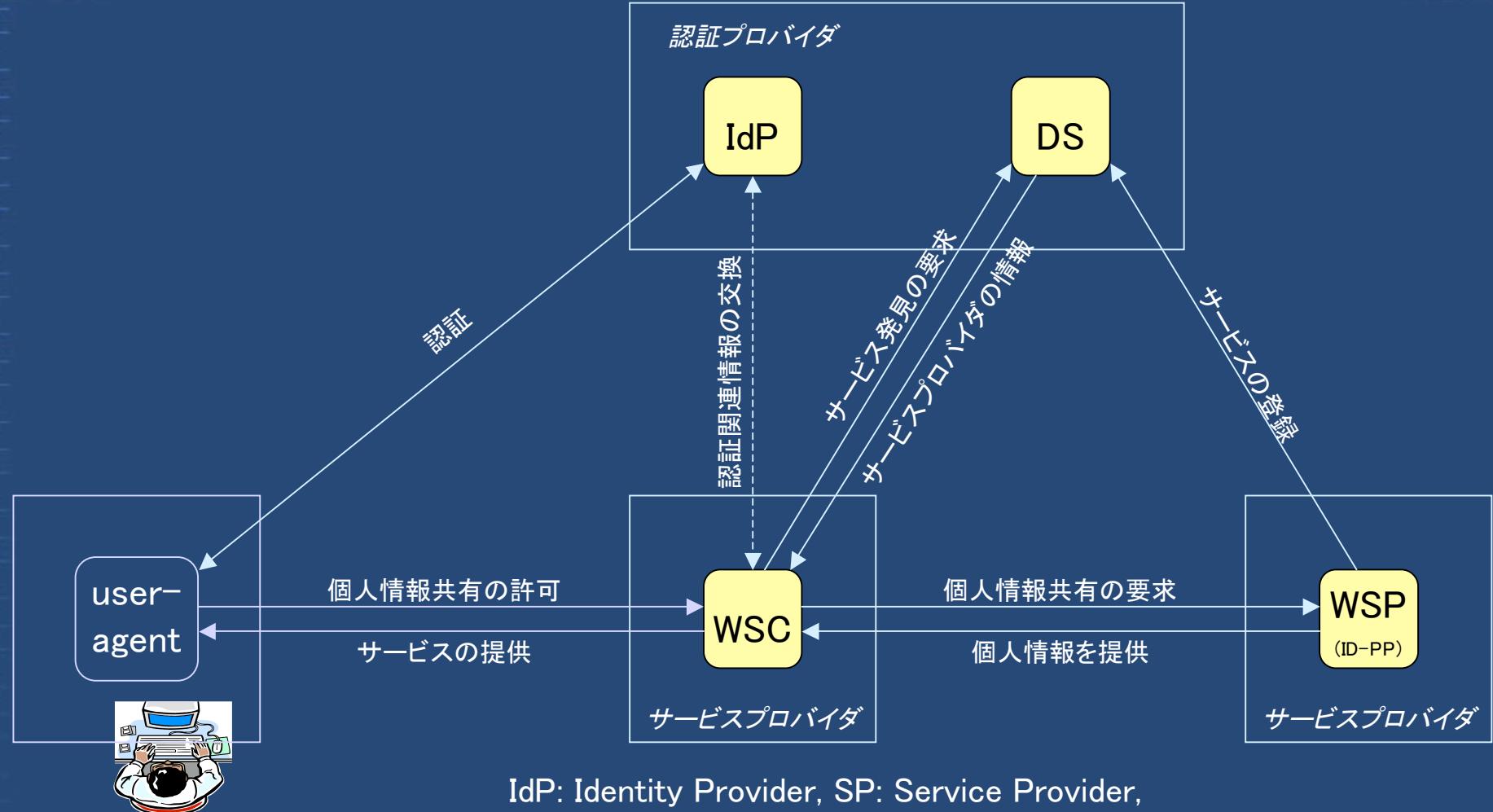
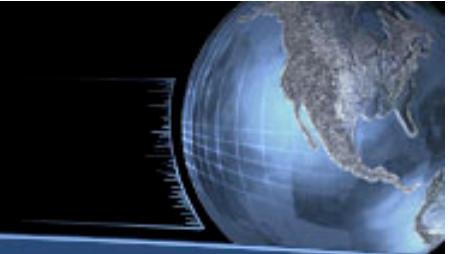
25

Liberty Allianceでできること(2)

- サービスサイト間での個人情報の共有
 - 住所や電話番号などの自分の属性情報を登録しておくことで、ユーザによる入力の手間を削減可能。
 - ユーザの許可に基づいて個人情報は共有されるため、プライバシが侵害されることはありません。



モジュール構成 (個人情報の共有)



IdP: Identity Provider, SP: Service Provider,

DS: Discovery Service,

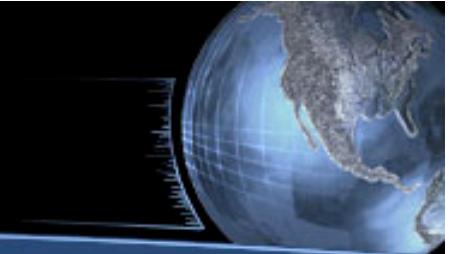
WSC: Web Service Consumer, WSP: Web Service Provider 27

Liberty Allianceでできること(3)

- 様々な個人情報サービスへの利用
 - 相互運用性をもつ総合的な個人情報サービスの世界

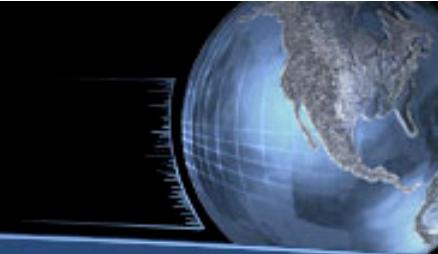


Liberty Alliance



- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification

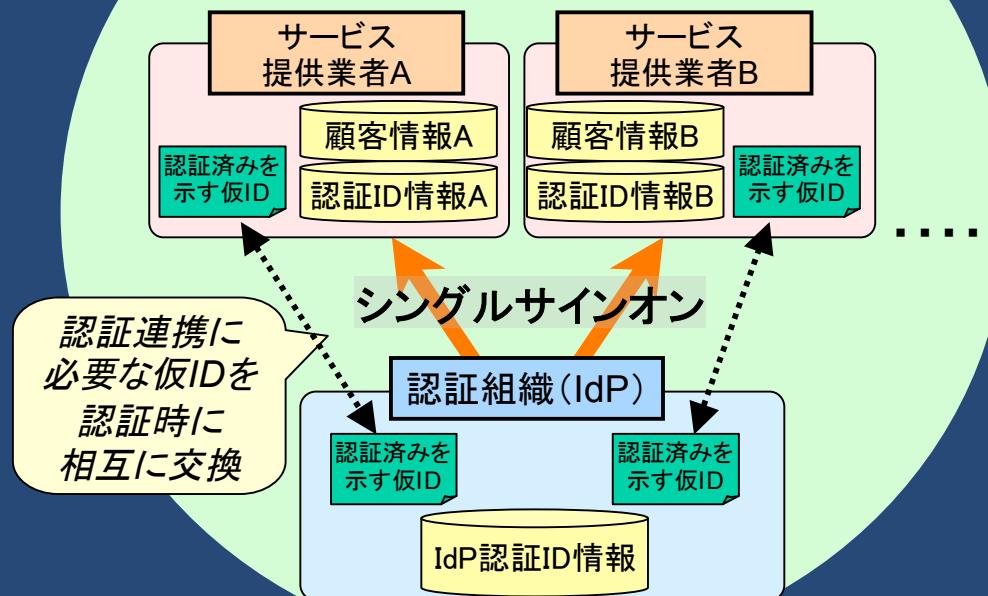
Liberty: 連携IDとは？ 連携型ID管理



独立したサービス業者間の柔軟な連携向け

連携型ID管理

サービス提供者が(主体的に)ID管理
対等な立場で認証連携のみをIdPに委託



Liberty: 連携IDとは？ 連携IDの特徴(1)

第三者への真のID情報の流出を防止

- 認証組織(IdP)とサービス提供組織(SP)間の連携は、お互いの間でのみ通じる仮名(ランダム文字列)を利用します。



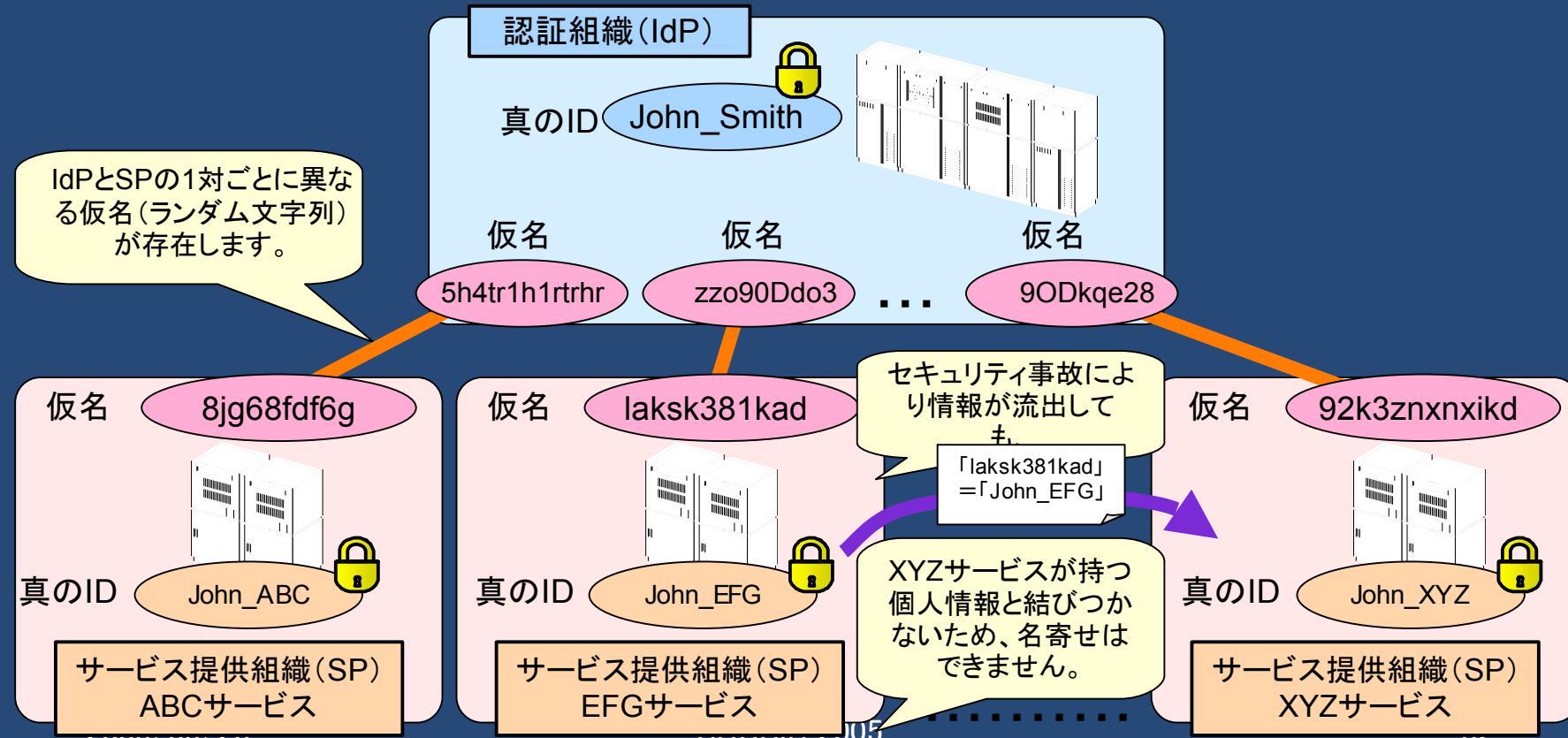
仮名は、当事者である認証組織Aとサービス提供組織Bの間でしか意味を持たないランダム文字列のため、万が一流出してもセキュリティの低下には結びつきません。

Liberty: 連携IDとは？ 連携IDの特徴(2)

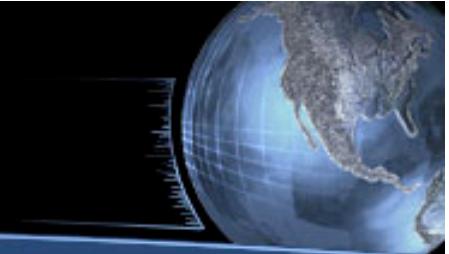
サービス提供組織(SP)ごとにプライバシーを担保

仮名(ランダム文字列)は、サービス提供組織(SP)ごとに異なります。

もあるサービス提供組織(SP)で仮名とIDの対が流出しても、仮名はそのサービス提供組織(SP)以外では意味を持たないため、他のサービス提供組織(SP)による名寄せは困難です。

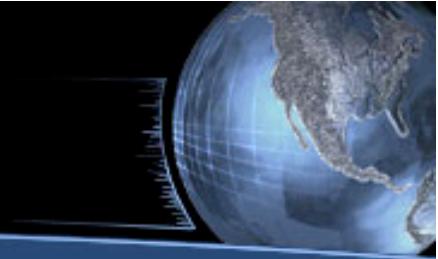


Liberty Alliance



- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification

ID-FFとは



連携ID管理基盤技術を規定。

1. Federated identity: single sign-on (ID-FF 1.1)
2. IdP Proxy (ID-FF 1.2)
3. Single federated identity (ID-FF 1.2)
4. Temporary anonymous account (ID-FF 1.2)
5. その他: 連携ID管理によるSingle Sign-on 技術の収束: SAML2.0

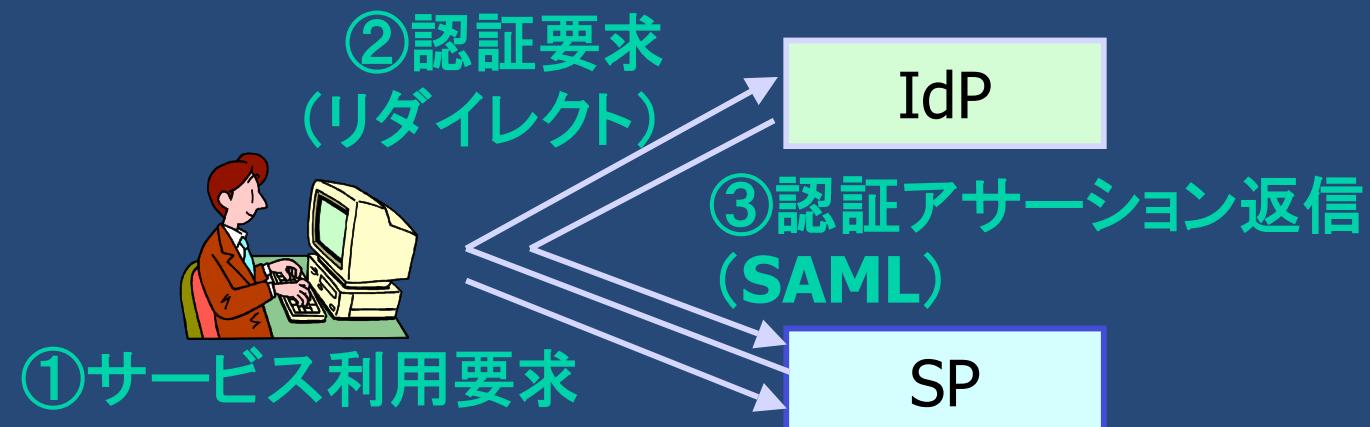


1. 連携IDによるシングルサインオン(ID-FF 1.1)

SAML認証アサーションによるシングルサインオンを実現

<関連機能>

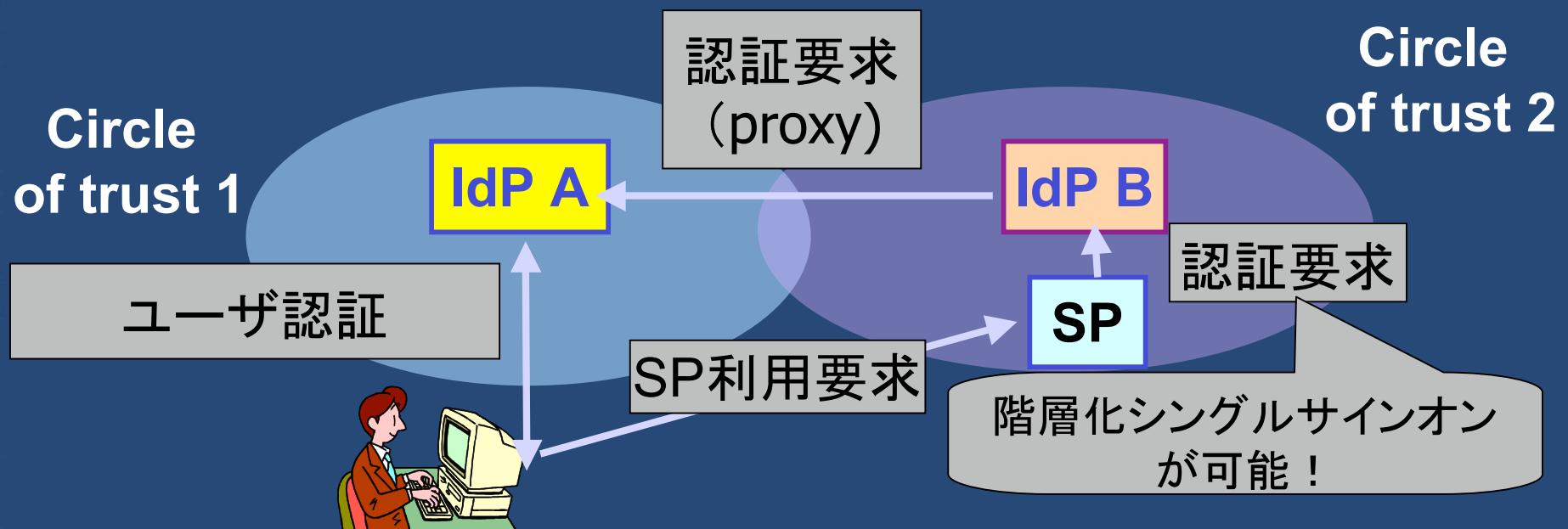
- ・連携ID機能
- ・連携解除機能
- ・シングル・ログアウト(利用SP一斉ログアウト)





2. IdP プロキシ (ID-FF1.2)

自分では認証をすることのできないユーザに関しては、他のIdPへのProxyとして動作することが可能。返信(リダイレクト)された認証情報を転送することで、SP上での認証行為が完了します。

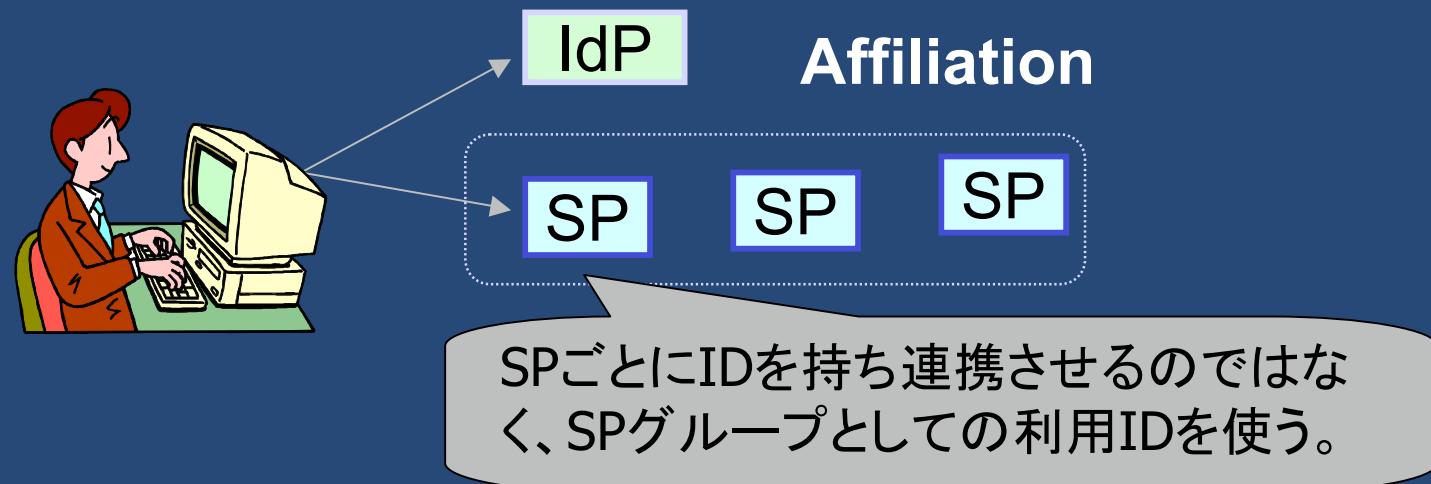




3. 一括アイデンティティ連携(ID-FF1.2)

グループによるくくりが可能です。

- SP内のAffiliation IDをもつことが可能。
- IdPをポータルとしたサービスグループ提供に便利。

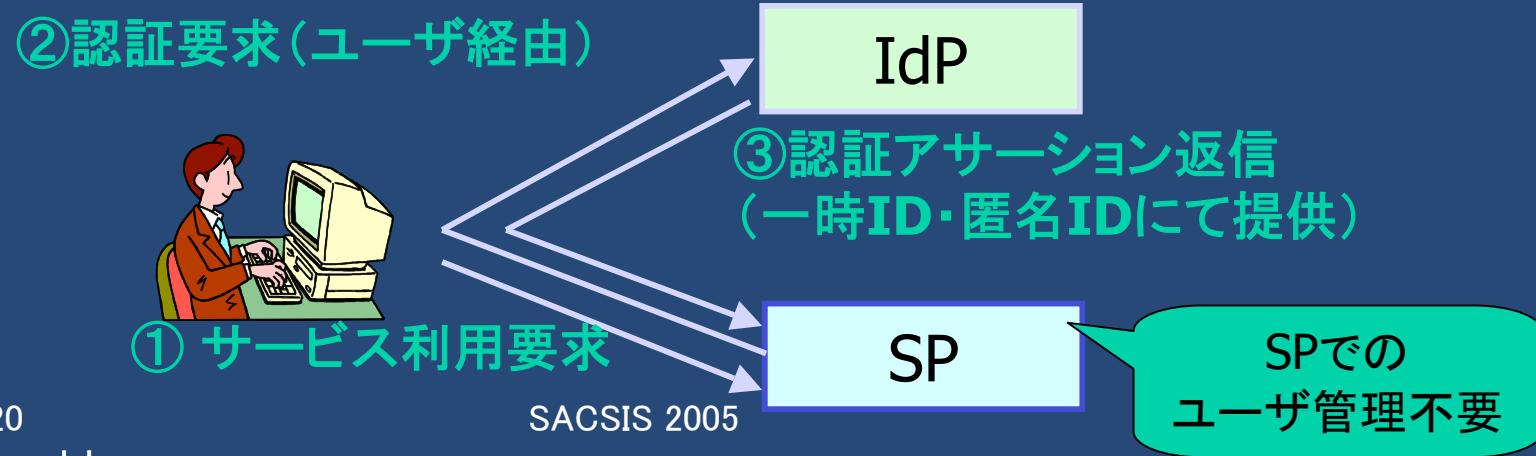




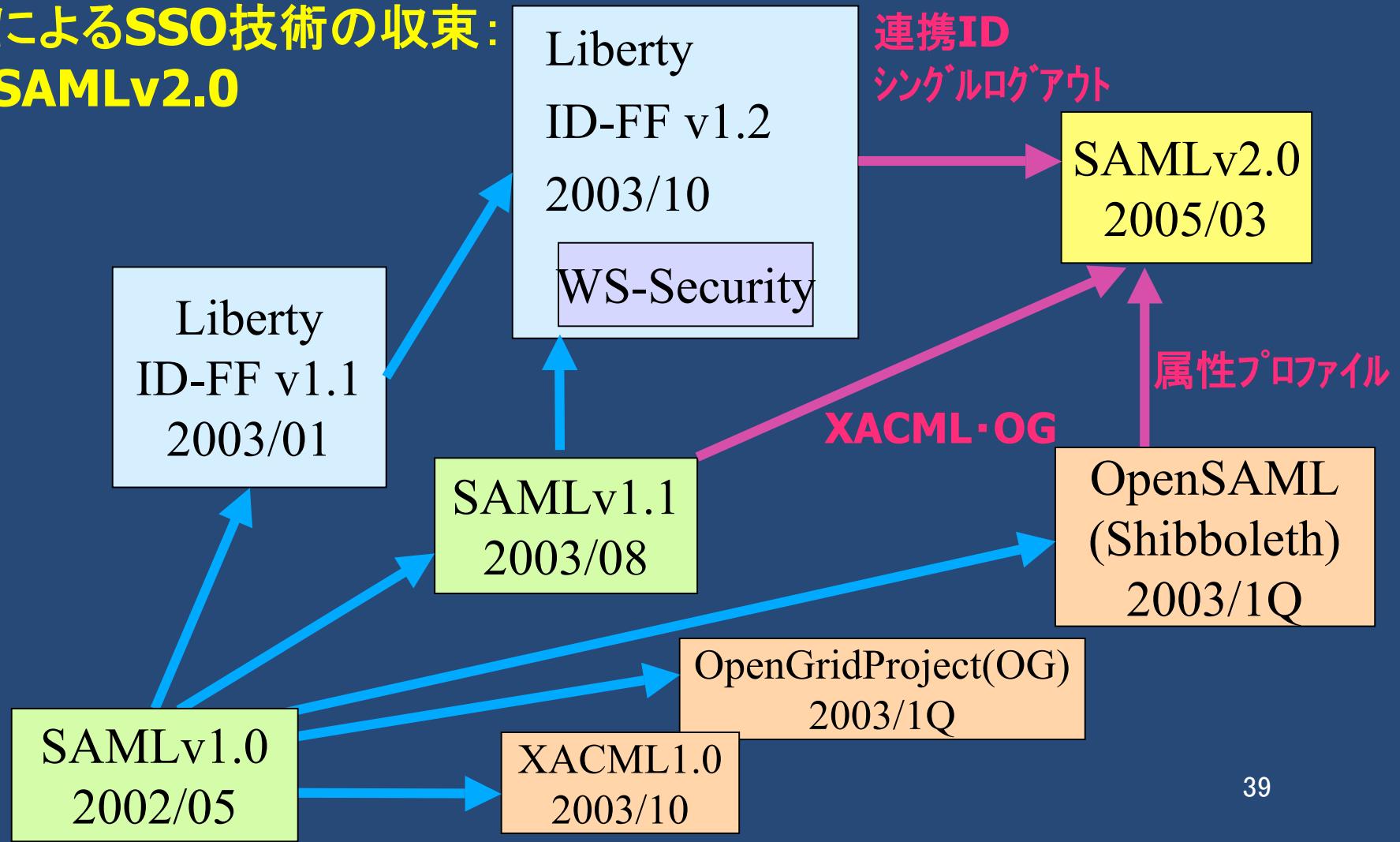
4. 一時・匿名アカウント(ID-FF1.2)

IdPの認証さえ受けていればSPでの利用を許す(匿名利用・一時利用)ことが可能です。

たとえば、SP側にアカウントがなくてもIdPの認証さえ受けていればサービス提供を許可します。すなわち、完全代理認証型のサービスを開拓することが可能です。



5. その他: 連携ID管理によるSSO技術の収束: **SAMLv2.0**



アーキテクチャ概要

OASIS
SAML v2.0

Libertyアイデンティティサービス・インターフェース
仕様(ID SIS)

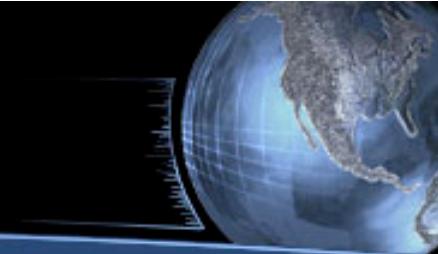
パーソナルプロファイルサービス、アラートサービス、
カレンダーサービス、ウォレットサービス、コンタクトサ
ービス、位置情報サービス、プレゼンスサービス等の
アイデンティティサービスが可能

LibertyアイデンティティWebサービス・
フレームワーク(ID-WSF)

相互接続可能なアイデンティティサービス、許可ベー
スの属性共有、アイデンティティサービス記述、ディ
スカバリ、および関係するセキュリティプロファイルを
作成・構築するためのフレームワークを提供

Liberty仕様は既存の標準仕様に準拠
(SAML, SOAP, WSS, XML, etc.)

Liberty Alliance



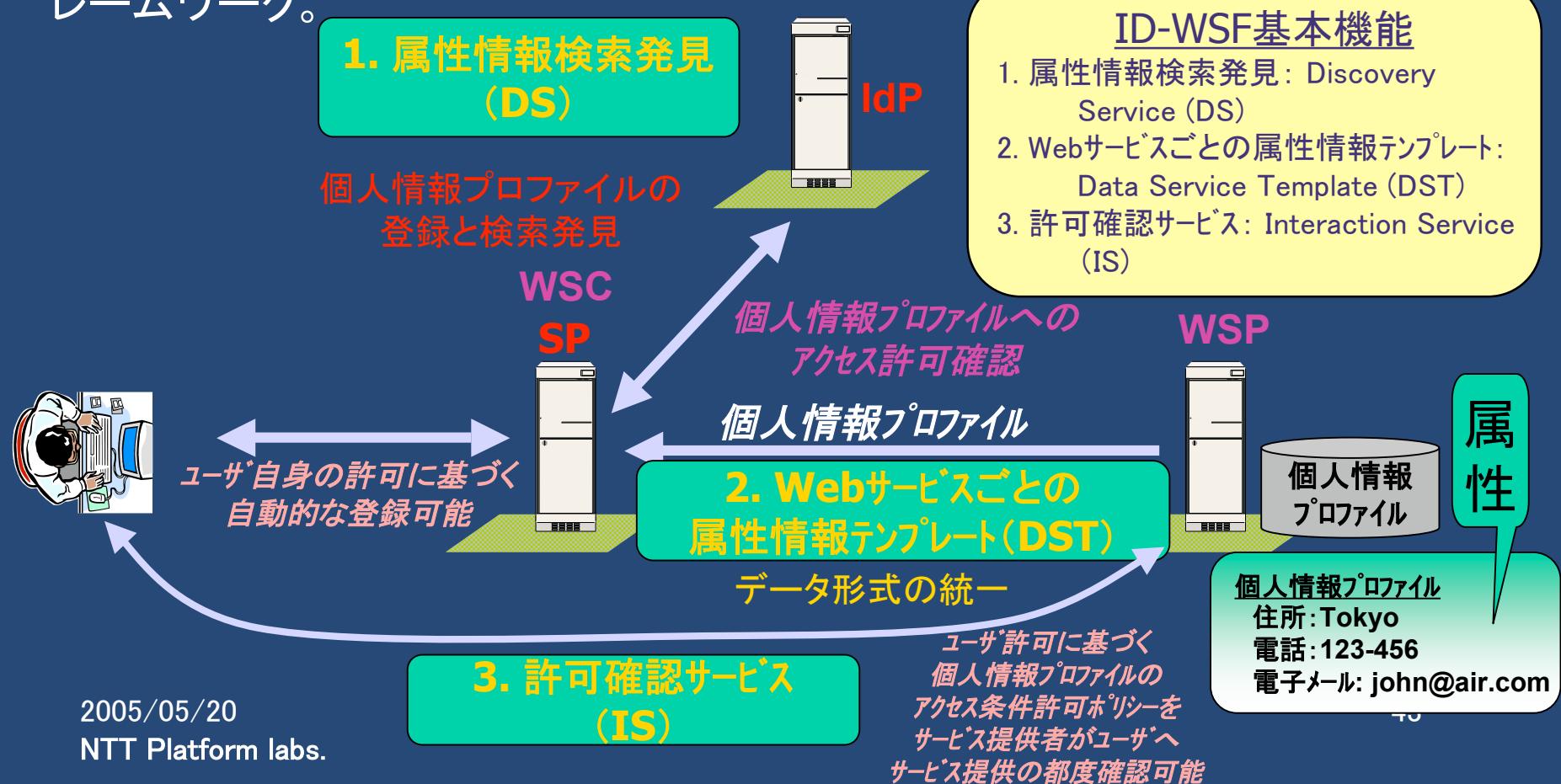
- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification



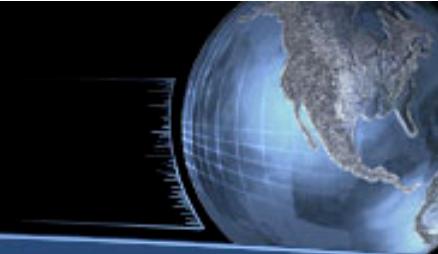
- ID-WSF: Identity-based Web Services Framework
- ユーザの属性情報をWebサービス提供サブ間で交換する仕様
- ID管理に基づくWebサービスとは
 - サービス利用者の属性情報と関連付けられたWebサービス
 - サービス利用者本人による属性情報提供ポリシーに基づくサービスの提供。
- 基本コンセプト: ユーザからの許可に基づく属性共有
 - 属性情報の検索発見サービス(DS: Discovery Service)、Webサービス提供者(WSP: WebService Provider)におけるユーザ属性利用サービスについて、サービス利用者本人からの許可に基づく、属性利用サービス開始処理手続

ID-WSF: コア要素技術概要

ID-WSFの目的: 属性交換についてパーソナライズ化されたサービス提供
 予め許可し合ったSP間において、異なるSPのサービスごとに登録情報入力作業を軽減するためにSP間で個人情報を含む属性情報交換可能にするフレームワーク。

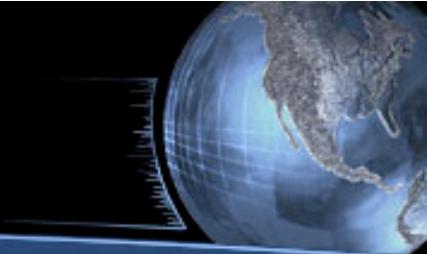


ID-WSF: コア要素技術



1. 属性情報検索発見: Discovery Service (DS)
2. Webサービスごとの属性情報テンプレート: Data Service Template (DST)
3. 許可確認サービス: Interaction Service (IS)

ID-WSF: コア要素技術



1. 属性情報検索発見: Discovery Service (DS)

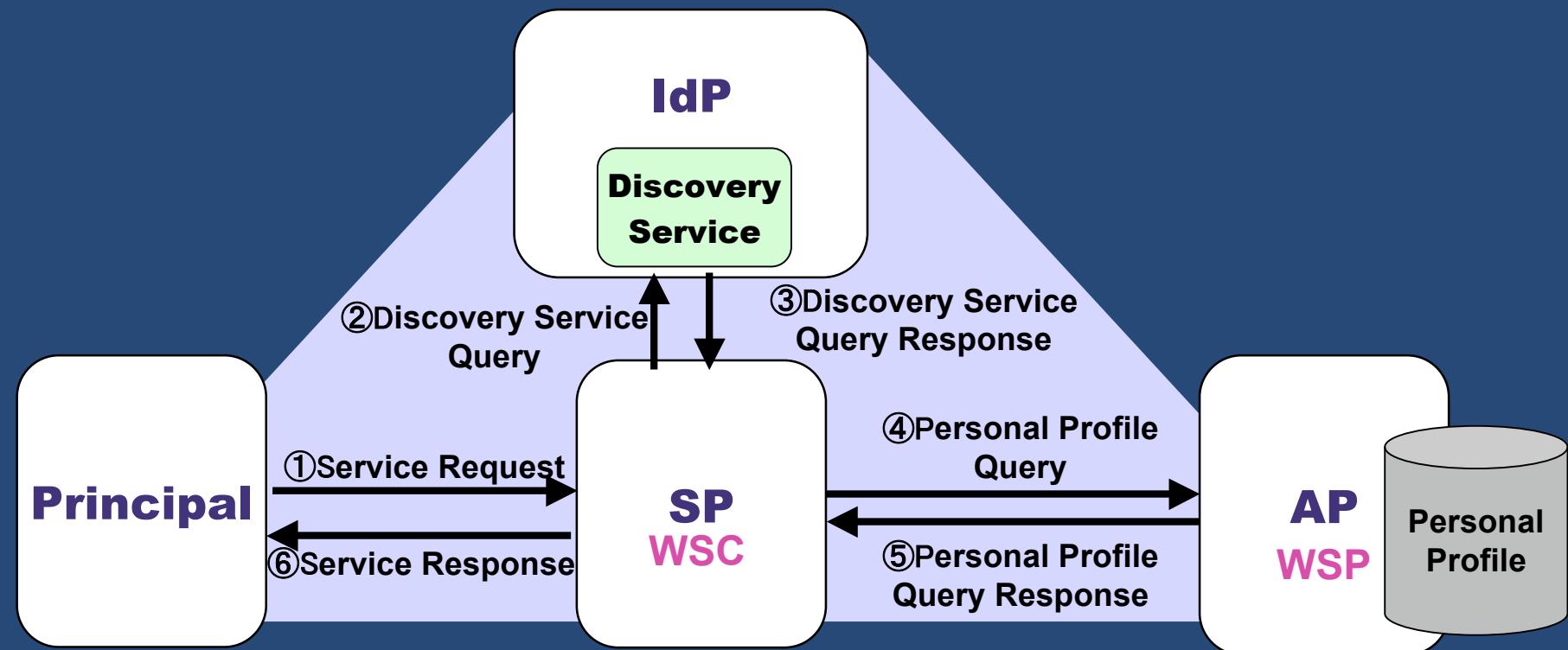
- 属性情報を利用したサービス提供のための「登録」
 - 属性情報の登録と検索発見サービス
 - 属性情報リソース提供 (Resource Offering (RO))
 - 属性情報の提供先
 - サービスごとに属性情報を指定可能
 - セキュリティメカニズム
- 属性情報交換時のセキュリティ保護規定
- 特定した属性情報の検索
 - 例) 「クレジットカード番号」を蓄積している属性情報の検索
 - 例) 「年齢情報」を蓄積している属性情報の検索

ID-WSF: コア要素技術

2. Webサービスごとの属性情報テンプレート: Data Service Template (DST)

- 本仕様は、（例えば個人アイデンティティプロファイルサービスといった）データサービスをアイデンティティウェブサービスフレームワークの上に実装する際に利用する、ビルディングブロックを提供。
 - データサービス内に蓄積されたデータへのクエリ方法・修正方法を定義。
 - データサービスで利用する共通属性を提供：
 - id [optional]: ユニークな識別子。
 - modificationTime [optional]: 最も最近に修正がかけられた時間。
 - modifier [optional]: 最後に修正をかけたプロバイダのID。
 - ACC [optional]: その情報が収集された方法(Attribute Collection Context)。
 - ACCTime [optional]: 上記ACC属性が与えられた時間。

ID-WSF: 実施例



ID-WSF: コア要素技術

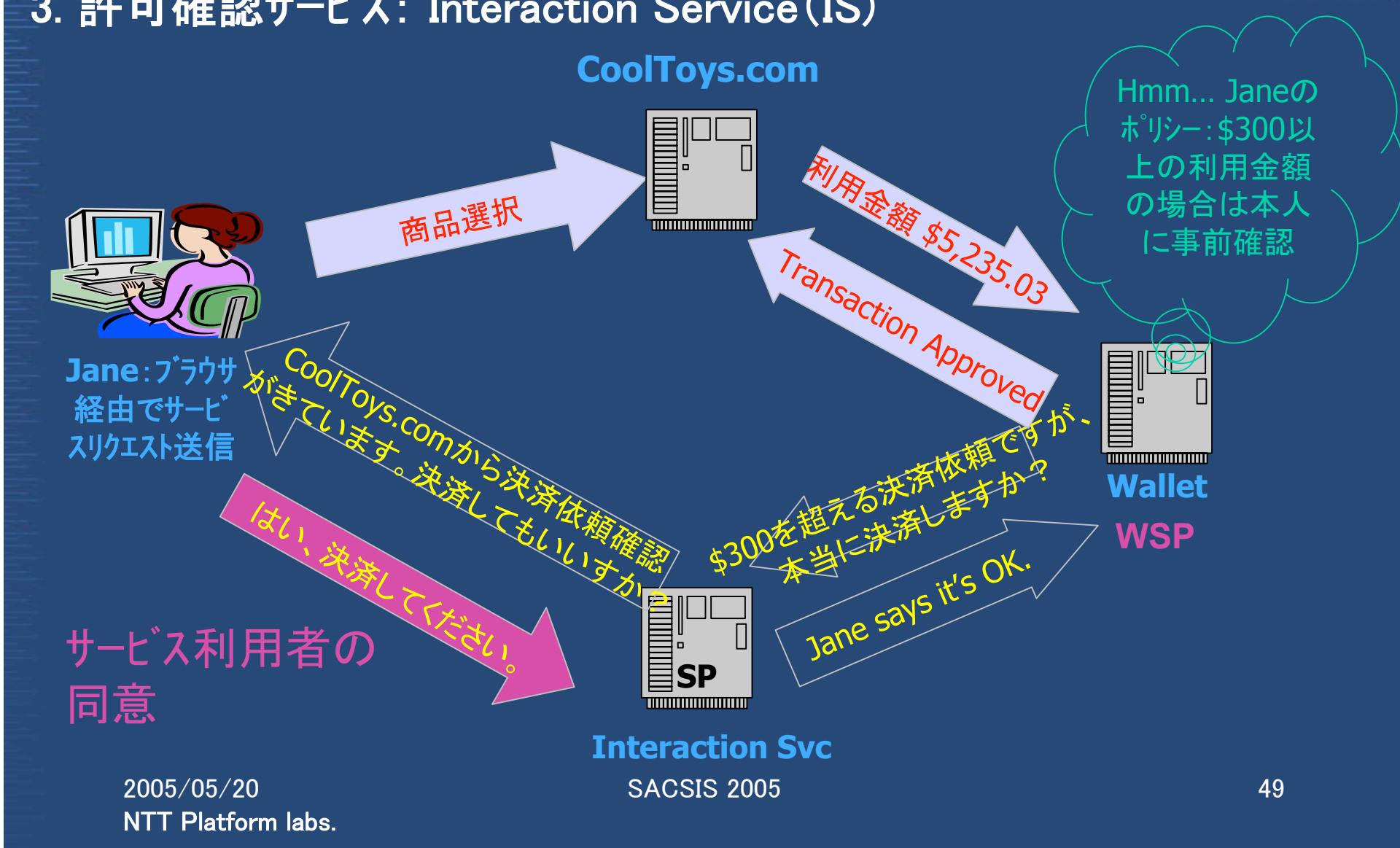
3. 許可確認サービス: Interaction Service (IS)

- WSPとサービス利用者を対話させる機能
 - 通常、WSPはサービス利用者に直接アクセスしない。
 - 実時間での、許可同意申請または提供する属性内容の確認
- 様々な実現手法
 - WSPに、SPがサービス利用者との対話を許可(中継)
 - WSPに、SPがサービス利用者のブラウザをリダイレクト
 - WSPが直接サービス利用者と対話する(SPを介さずに)

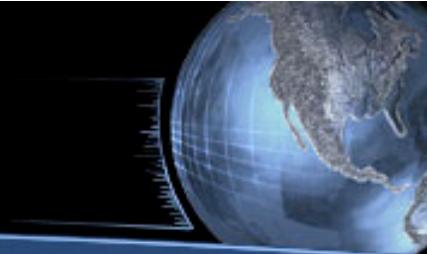
Liberty

ID-WSF: コア要素技術

3. 許可確認サービス: Interaction Service (IS)



セキュリティ・メカニズム



- ・ 本仕様は、アイデンティティサービスを、安全に、発見・利用するためのプロファイルや要求を記述。
 - ・ 主なセキュリティ要求：
 - ・ プライバシ保護要求
 - ・ サービスプロバイダ間のメッセージ交換の整合性や機密性を保証するためのセキュリティ要求。
 - ・ アイデンティティサービスを提供するための認証、署名、暗号化等の操作を規定。メッセージの認証と機密保護のための操作としてXML署名とXML暗号化を採用。

ID-FFとID-WSFの相関関係について



- ID-FFはID-WSFサービスへ誘導することが可能
 - ID-FFを実施すれば、SPはアサーションを入手でき、そのアサーションには属性情報検索発見サービスDSを呼び出すための情報が含まれている。
 - これにより、SPはID-WSFサービスの呼出を行うWSCとして動作可能。
- ID-WSFは認証サービス(Authentication Service (AS))を定義し、これによりID-FFに類似したオペレーションを実行するIdPへのSOAPインターフェースを提供可能。
 - ID-FFで獲得したトークンが認証サービス(AS)のクライアントへ提供される。
 - そのため、クライアントはDSを呼び出すことが可能。

ID-FF & ID-WSF

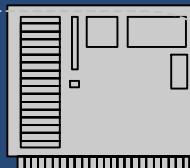
ID-FF: JaneのID証明書を得る手段としてブラウザを使い、SPはIdPと対話可能。



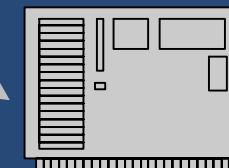
Jane: ブラウザからのサービス要求

It's Jane

SP/WSC



WSP

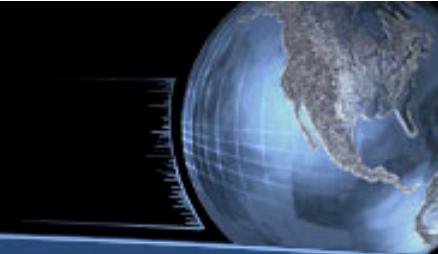


WSP

ID-FF

ID-WSF

Liberty Alliance



- 略語用語解説
- アーキテクチャ概要
- ID-FF: Identity Federated Framework
 - 連携IDとは？
 - ID-FFとは
- ID-WSF: Identity Webservice Framework
- ID-SIS: Identity Service Interface Specification



ID-SIS: Identity Service Interface Specification

- Libertyフレームワークと属性情報を用いた各種Webサービスとの間のサービスインターフェースを規定した仕様群
 - Personal Profile: サービス利用者の基本プロファイル情報(連絡先詳細・氏名)を提供するアイデンティティサービスのためのXMLスキーマに関する仕様。
 - Employee Profile: サービス利用者の従業員プロファイル情報(所属・役職)を提供するアイデンティティサービスのためのXMLスキーマに関する仕様。
 - Contact Book: サービス利用者のコンタクト・ブックに関する情報を提供するアイデンティティサービスのためのXMLスキーマに関する仕様。
 - Presence: サービス利用者のプレゼンスサービスに関する情報を提供するアイデンティティサービスのためのXMLスキーマに関する仕様。
 - Geo-Location: サービス利用者の位置情報サービスに関する情報を提供するアイデンティティサービスのためのXMLスキーマに関する仕様。

アーキテクチャ概要

OASIS
SAML v2.0

Libertyアイデンティティサービス・インターフェース
仕様(ID SIS)

パーソナルプロファイルサービス、アラートサービス、
カレンダーサービス、ウォレットサービス、コンタクトサ
ービス、位置情報サービス、プレゼンスサービス等の
アイデンティティサービスが可能

LibertyアイデンティティWebサービス・
フレームワーク(ID-WSF)

相互接続可能なアイデンティティサービス、許可ベー
スの属性共有、アイデンティティサービス記述、ディ
スカバリ、および関係するセキュリティプロファイルを
作成・構築するためのフレームワークを提供

Liberty仕様は既存の標準仕様に準拠
(SAML, SOAP, WSS, XML, etc.)



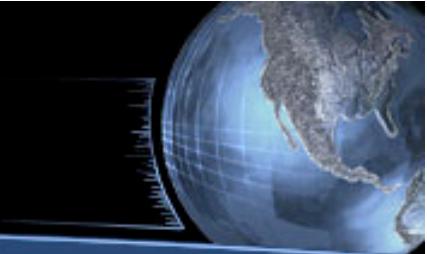
2. ビジネス導入 事例紹介

2005/05/20

SACSIS 2005

56

2. ビジネス導入事例紹介

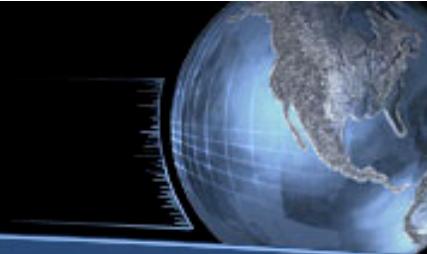


- 導入事例: B2B
- 導入事例: B2C
 - B2Cにおける連携ID管理ビジネスの強み
 - モバイルビジネス
 - Radio@AOL(米国)
 - Orange (France Telecom)
 - ISP
 - Wanadoo (France Telecom)
 - Bluewin (Swisscom)
 - MasterID (NTTコミュニケーションズ)
 - Digital TV

導入事例: B2B

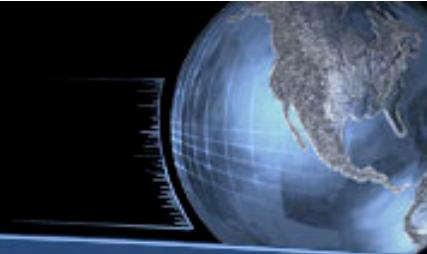
- NTTデータ: JAL ONLINE
 - NTTデータ: "JAL ONLINE"
 - SSOサービス: SAML 準拠
 - JAL航空券予約・発券と社内旅費申請システム間での連携ID管理サービス提供
- Communicator Inc.
 - 機関投資家へのSSOシステム提供(加入者数: 約4,000)。
- Neustar
 - 銀行、地方自治体、および権限保険会社の間で不動産権利証書の相互交換を実現するシステム提供。
- Niteo partners
 - JPMorgan、Wachovia、およびBank of Americaの間でそれぞれのアカウントを連携させるWebサービスを実現するシステムの提供。
- GM, American Express, Sun
 - それぞれの社内における社員属性情報交換システム提供。

将来導入が期待される事例



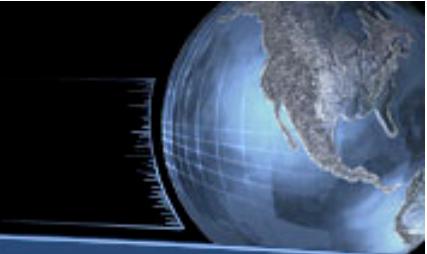
- 行政サービス
 - e-Authentication (米国), ADELE project (フランス)
- 医療サービス
 - HIPAA (Health Insurance Portability and Accountability、米国)
- 金融サービス
 - 401K, アカウント統合サービス
- セキュアで安全なビジネスおよび社会の実現
 - アイデンティティ盗難対策
 - 強い認証への需要
 - ICカード, セキュア・チップ等々.

2. ビジネス利用事例紹介



- 導入事例: B2B
- 導入事例: B2C
 - B2Cにおける連携ID管理ビジネスの強み
 - モバイルビジネス
 - Radio@AOL(米国)
 - Orange(France Telecom)
 - ISP
 - Wanadoo (France Telecom)
 - Bluewin (Swisscom)
 - MasterID (NTT Communications)
- On going use case:
 - Digital TV

B2Cにおける連携ID管理の強み



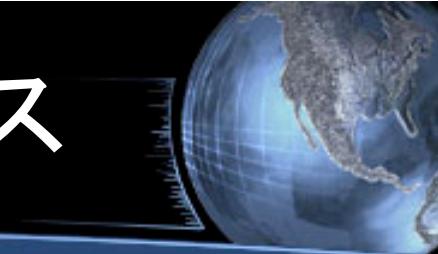
- 利用者のメリット:

- ログイン、サービス利用時の利用者プロファイルの作成、アカウント作成初期登録・更新などのための手続軽減、利便性向上
- 利用者主導による個人情報管理可能
- 最新のセキュリティおよびプライバシ保護法に対応した国際標準準拠サービスの利用

- ビジネス（サービス提供者）の強み:

- CoTによる連携により、新たな顧客獲得機会の増加
- 既存のID管理システムとの共存可能
- ハーネスサービスの提供により顧客満足度の改善と向上
- オープンで高い相互接続性を保障された国際標準規格に基づく実装により、導入コスト削減可能
- 様々なデバイスおよびプラットフォームへの導入可能
- アイデンティティ管理に関するヘルプデスクの問い合わせ（パスワードリセット等）の管理コスト削減

導入事例: B2C: モバイルビジネス



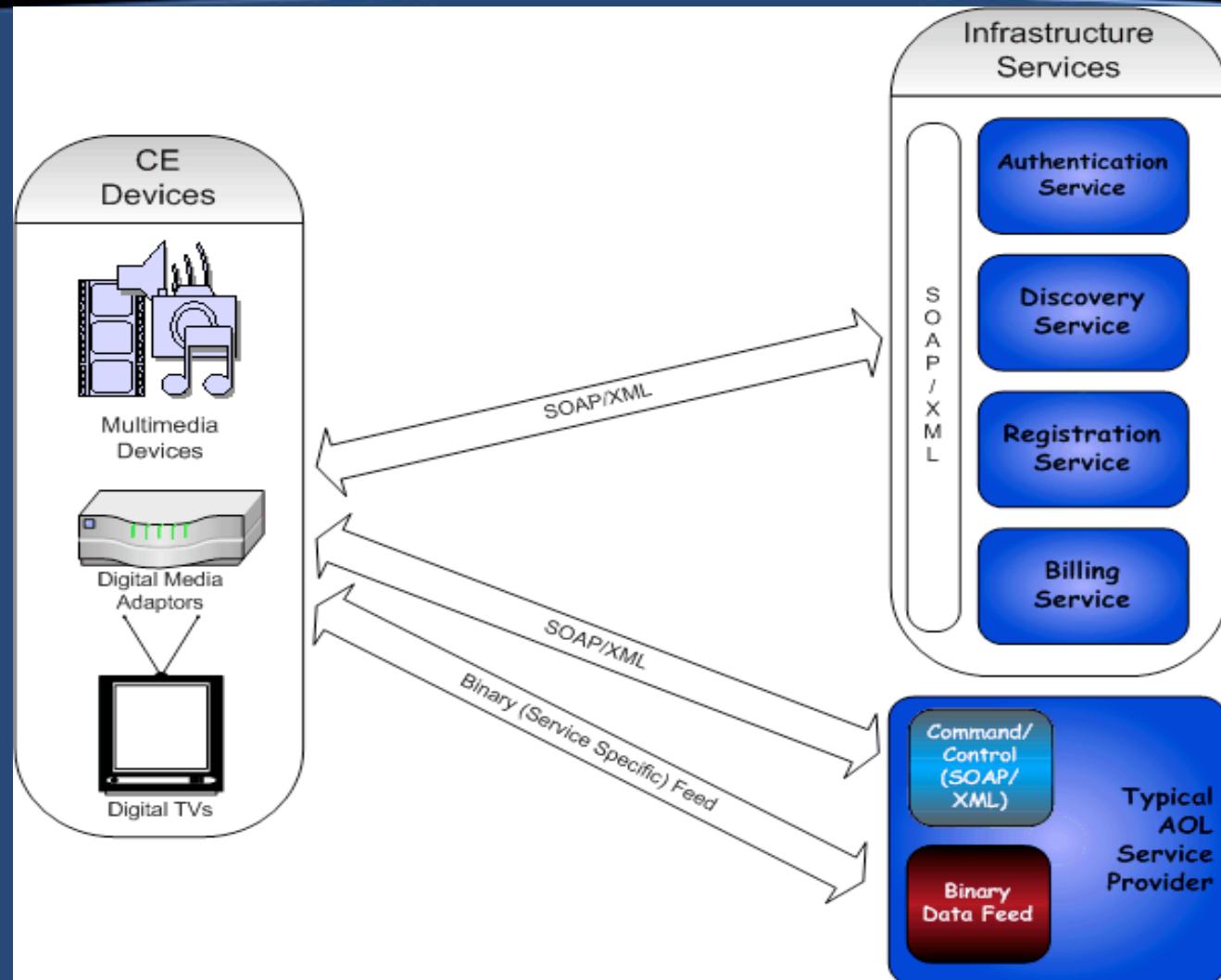
- AOL: ラジオコンテンツの携帯ダウンロードサービス“Radio@AOL”が米国で提供中。本サービスでは、Liberty属性交換仕様ID-WSFが用いられており、様々なデバイス(PC、携帯電話、携帯ストレージ音楽プレイヤなど)に対応し、利用者の嗜好情報を含む個人情報プロファイルを利用者の許可に基づいて提供利用するサービスを実現中。

Radio@AOL

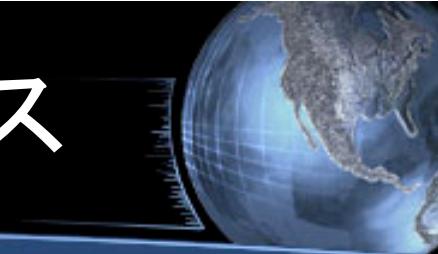
- Liberty ID-WSF(属性交換仕様群)準拠のWebサービス
 - 認証サービス
 - 属性情報発見サービス(Discovery Service)
- ラジオコンテンツや写真サービスの提供
- ネットワーク対応の高機能クライアントソフト:
 - 属性情報を直接デバイス間で交換することが可能
 - クライアント側で唯一設定することは、IdPのアドレス一つだけ。

導入事例: B2C: Mobile導入事例

Radio@AOL



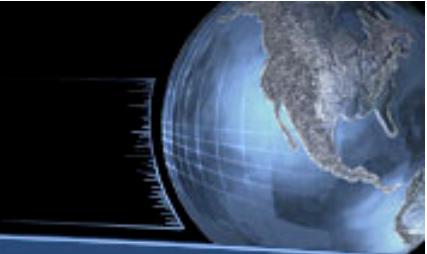
導入事例: B2C: モバイルビジネス



- 導入検討:

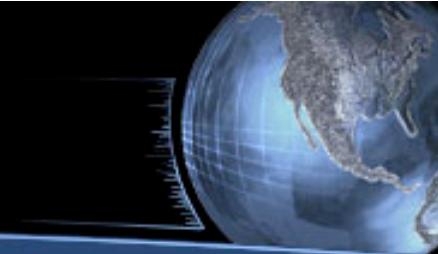
- Orange (France Telecomの携帯子会社): Libertyシングルサインオン機能ID-FF準拠システムを実サービスとして導入検討中。
- Nokia: 既存の携帯電話のためのLiberty準拠ゲートウェイを開発中。将来、Liberty準拠携帯電話のリリースを検討中。
- Vodafone Group: 携帯電話を用いたゲーム、着メロ、写真サービスにおけるLiberty準拠サービスの提供準備中。

2. ビジネス利用事例紹介



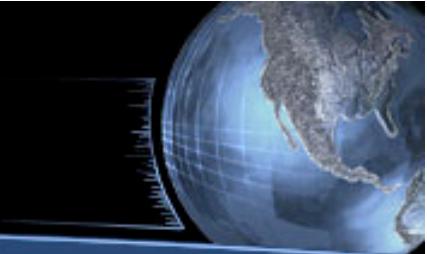
- 導入事例: B2B
- 導入事例: B2C
 - B2Cにおける連携ID管理ビジネスの強み
 - モバイルビジネス
 - Radio@AOL(米国)
 - Orange (France Telecom)
 - ISPなど
 - Wanadoo (France Telecom)
 - Bluewin (Swisscom)
 - MasterID (NTTコム)
 - Digital TV

導入事例: B2C: ISPなど



- NTT コミュニケーションズ: “マスターID”
 - SSOサービス: Liberty ID-FF1.1 準拠
 - 準ストレージサービスや請求書情報等間での連携ID管理サービス提供

2. ビジネス利用事例紹介



- 導入事例: B2B
- 導入事例: B2C
 - B2Cにおける連携ID管理ビジネスの強み
 - モバイルビジネス
 - Radio@AOL(米国)
 - Orange (France Telecom)
 - ISPなど
 - Wanadoo (France Telecom)
 - Bluewin (Swisscom)
 - MasterID (NTTコム)
 - Digital TV

デジタル放送における連携ID管理



● 背景:

– デジタル放送への期待

- デジタルTV:

- 新たな可能性: NWアクセス端末
- 双方向、パーソナライズ化
- 巨大市場といわれるT-コマース市場

- 視聴スタイルの変化: 好きなときに好きな場所で

- 大容量HDD付デジタルビデオ放送録画機 → いつでも
- 携帯端末での視聴: モバイル放送への期待 → どこでも

– 課題:

- リモコン操作のような限られた入力インターフェース:

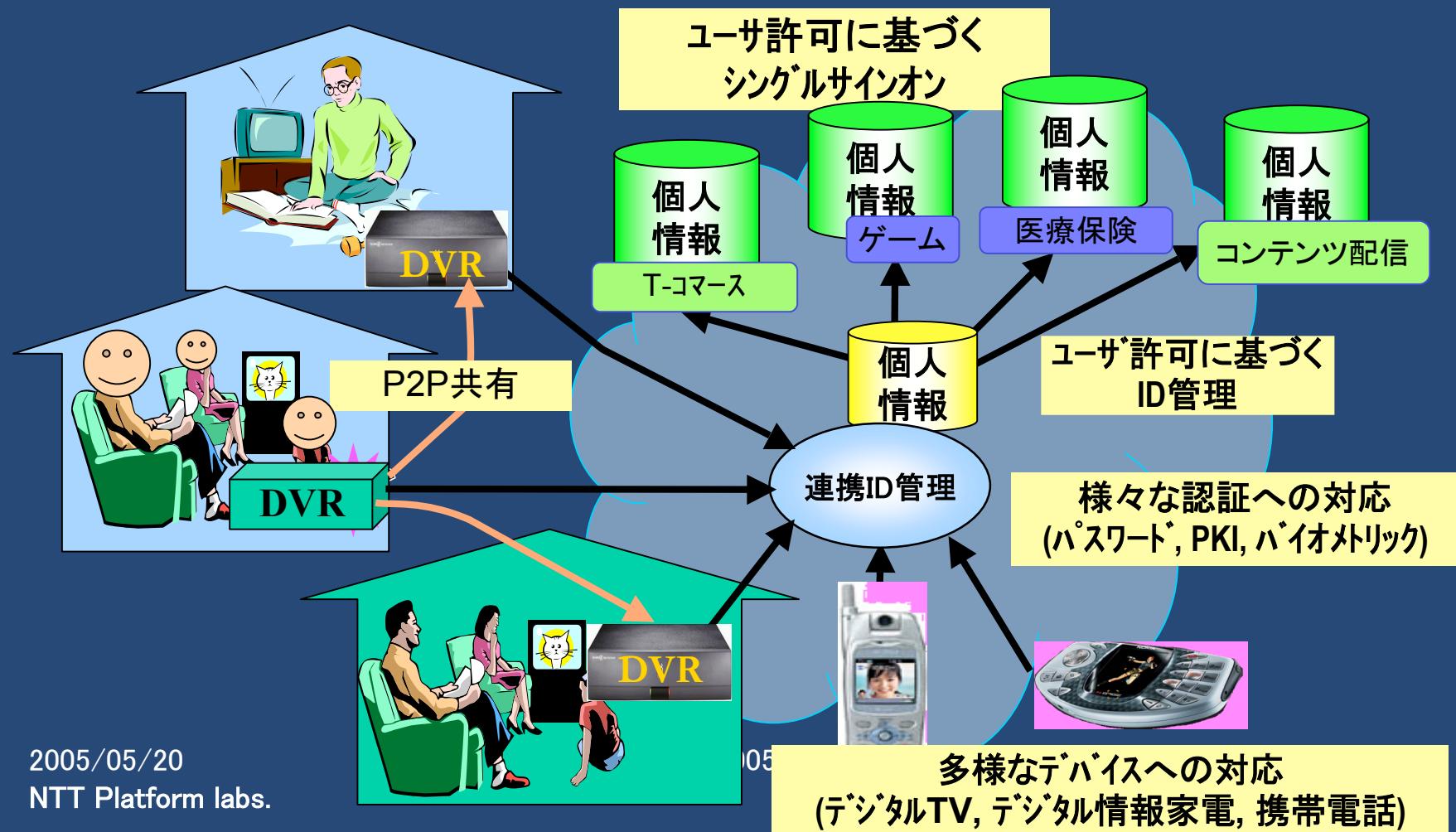
- 例) 配送情報、支払情報の入力、ID/パスワード入力

- セキュリティ・プライバシ保護

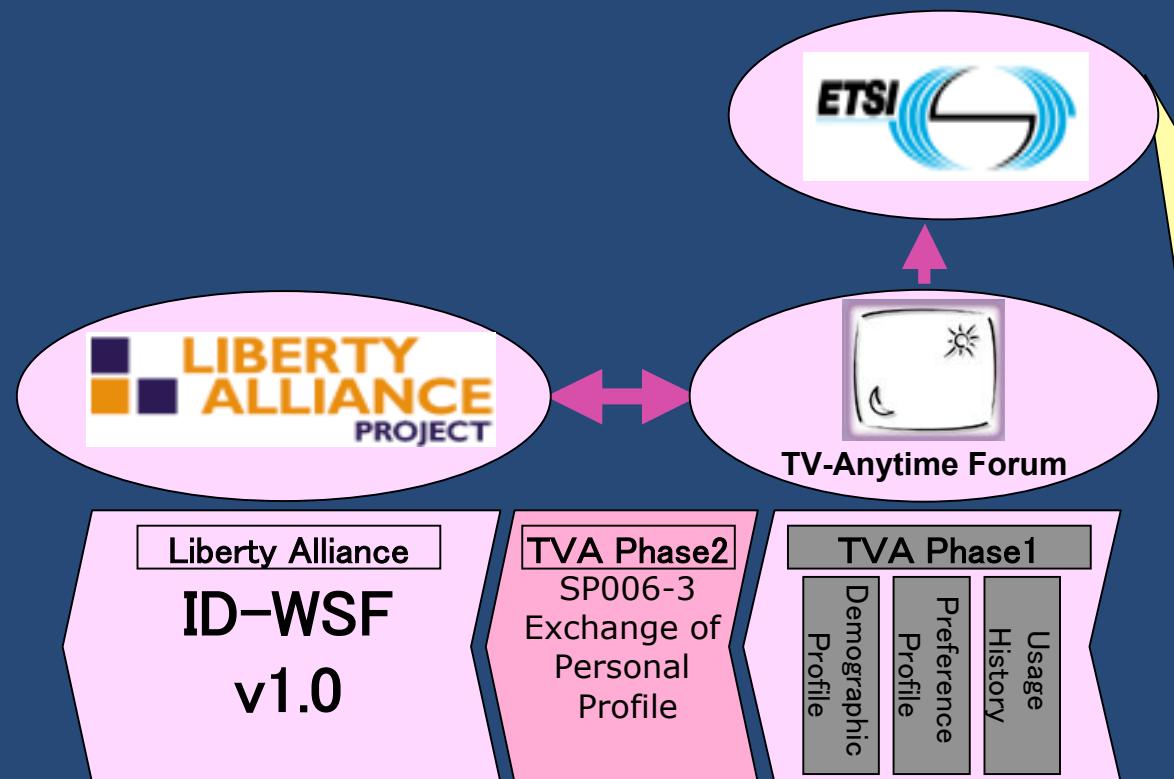
- オープン相互接続可能な国際標準仕様の確立。

デジタル放送における連携ID管理導入例

- 視聴履歴を含む個人情報の保護
- 利用者の許可に基づく属性交換



Liberty ID-WSFv1.0仕様、デジタル放送における個人情報交換として採択



(公開スケジュール: 2005/08予定)

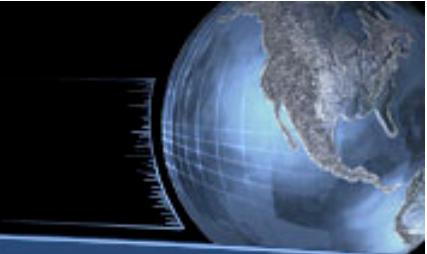
ETSI TS 102 822-6-3:

"Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime Phase 2");

Part 6: Delivery of metadata over a bi-directional network;

Sub-part 3: Exchange of personal profiles".

本日のまとめ

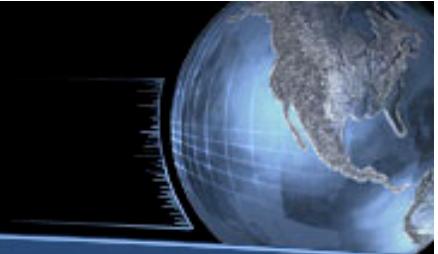


- 連携ID管理技術概要紹介
 - SAML
 - Liberty Alliance
- ビジネス導入事例紹介
 - B2B, B2Cユースケース
 - 今後の導入市場: Digital TV

参考情報

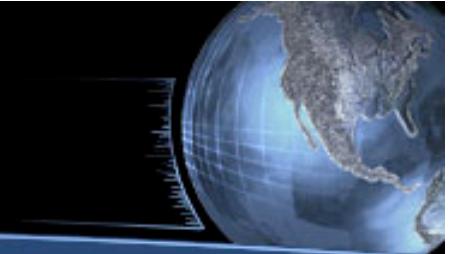
- Liberty技術チュートリアル(日本語),
http://www.projectliberty.org/jp/resources/LAP_DIDW_Oct_15_2003_jp.pdf
- 古賀他、“個人情報の管理・流通のための標準化団体「リバティアライアンス」の動向”、信学誌 Vol.87, No.6, p.504–507
- Teruko Miyata and Kenji Takahashi, Tutorial “Identity Management”, ACM CCS 2004, <http://www.acm.org/sigs/sigcac/CCS2004/tutorial.html#T3>
- 連携ID技術比較: Gary Ellison, The Venn of Identity, Federation, and SecureWeb Services, 9th Semiannual JA-SIG Conference Presentations, Dec 2003,
<http://web.princeton.edu/sites/isapps/jasig/2003winterMiami/presentations/ellisonkeynote.pdf>
- SAMLv2.0について: Paul Madsen, SAML 2: The building Blocks of Federated Identity, <http://www.xml.com/lpt/a/2005/01/12/saml2.html>
- Liberty Alliance 仕様, <http://www.projectliberty.org/resources/index.php>
- Liberty Alliance 仕様(日本語),
<http://www.projectliberty.org/jp/resources/index.html>

謝辞



- Gary Ellison
- Paul Madsen, NTT
- Conor P. Cahill, AOL
- NTT コミュニケーションズ
- NTT データ
- NTT プラットフォーム研究所

Call for Paper: ACM/CCS DIM Workshop 2005



● 投稿締切：2005年7月15日 ●

Call for Papers
ACM
CCS2005
Workshop
on Digital Identity Management

November 11, 2005,
Hilton Alexandria Mark Center, Alexandra, VA

ありがとうございました。



連絡先: 宮田 輝子
NTT プラットフォーム研究所
miyata.teruko@lab.ntt.co.jp