XML コンソーシアム •セミナー

Liberty Alliance Project の技術と活動

2005年9月13日（火）
Liberty Alliance 日本SIG Co-Chair
NEC インターネットシステム研究所
五味 秀仁 <gomi@az.jp.nec.com>

はじめに

- 世界中から150以上の企業・団体が参加し、認証連携やプライバシー情報流通等の仕様策定を進める Liberty Alliance Project の活動を紹介致します。
- 近年、個人情報の漏洩に伴うプライバシーの侵害は深刻な社会問題になっています。
- 本講演では、今日のデジタル社会において、個人情報保護法制に遵守しつつ、個人情報を安全に管理し流通する技術とその取り組みをご説明致します。
- また、Liberty Alliance の最新動向や今後の方向性についてもご説明致します。

講演内容

- Liberty Alliance Project 概要
- Liberty Alliance の分散連携モデルと技術
- 先行事例と新たな適用分野
- Liberty技術の適用をサポートする取り組み

Liberty Alliance Project 概要

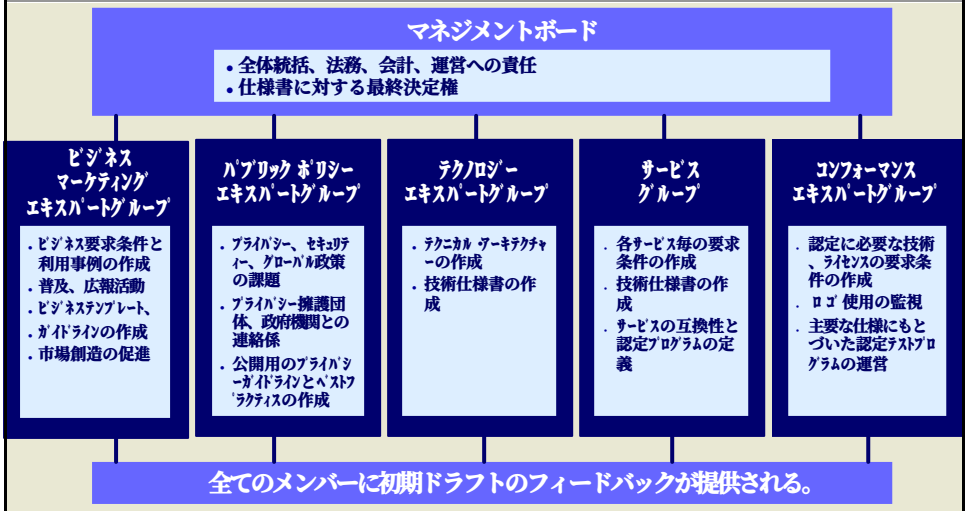
Liberty Alliance Project

- 2001年9月に設立されたビジネスアライアンス
  - 連携アイデンティティ管理とWebサービスのオープン標準仕様作成
- グローバルアライアンス
  - 150以上の企業、政府機関、非営利組織等から構成
- 目標
  - 様々なネットワーク・デバイスを対象としたオープンな標準仕様とビジネスガイドラインの提供
  - 分散的な認証・認可を実現する、アイデンティティ管理のための、オープンかつセキュアな技術標準の提供
  - 個人または企業が、安全に、かつ、柔軟に個人情報を管理する事を実現

Liberty Alliance スポンサーメンバー

：日本企業

Liberty Alliance 組織体制

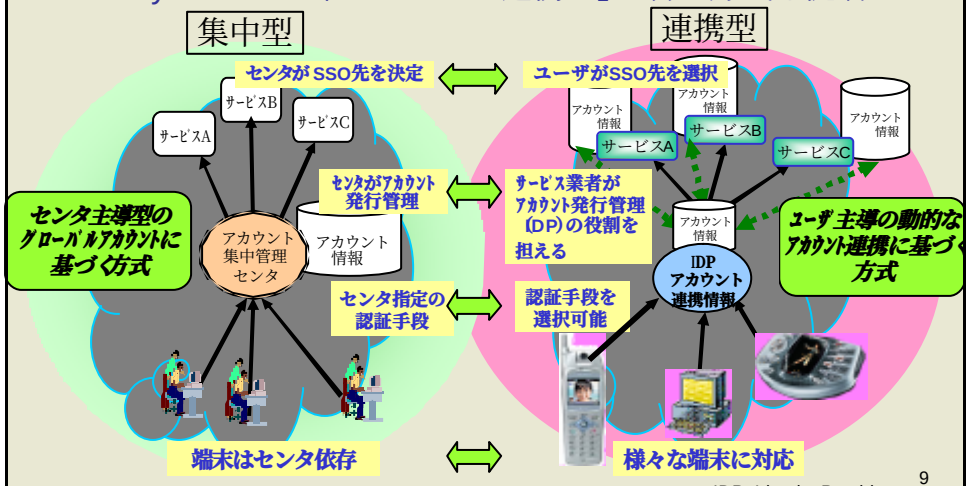


Liberty Alliance の 分散連携モデルと技術

ID-FF：アイデンティティ連携とシングルサインオン
ID-WSF: 個人情報の安全な交換と利用

連携型のアイデンティティ管理

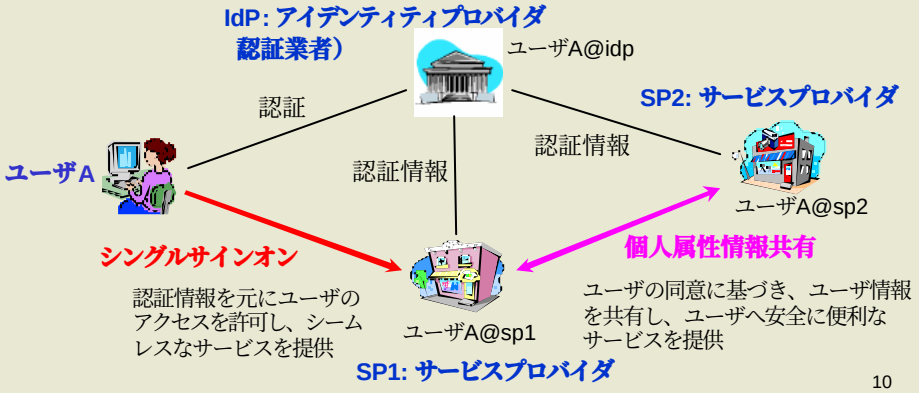
Liberty Allianceは、オープンな「連携型」の管理方式を提唱



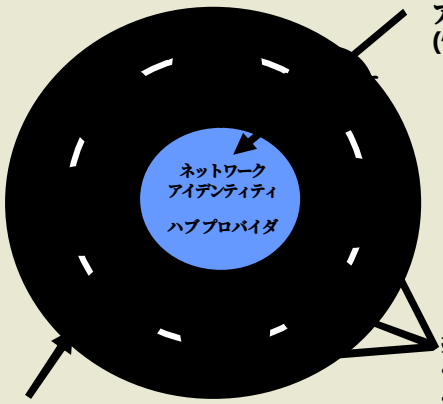
IDP: Identity Provider

アイデンティティ連携

- アイデンティティは、Webサービス連携のための構築基盤
  - シングルサインオン
  - 個人情報属性共有



トラストサークルモデル



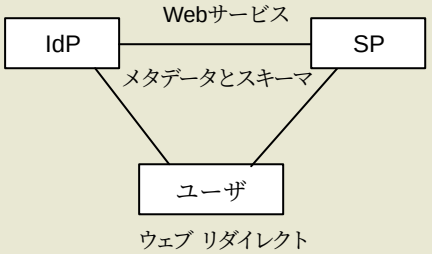
アイデンティティプロバイダー(IdP)
(例えば、金融機関や人事部)
- 信頼できるエンティティ
- 認証基盤
- 主たるアイデンティティ属性管理
- 付加価値サービスの提供 (オプション)

提携サービスプロバイダー (SP)
- 付加サービスの提供.
- 認証基盤を必ずしも用意する必要なし

トラストサークル (CoT)
- ビジネス的合意
- SLA
- ポリシー，ガイドライン，利用規定

Liberty アーキテクチャ

- IdPとSPは、ビジネス契約に基づき、メタデータ (メッセージ交換のためのサイトのURL等の基本情報を記述したXML文書) を事前に交換しておく。
- ユーザは、汎用的なWebブラウザを利用すればよく HTTPのリダイレクト機能を利用し、IdPとSPの両者と通信。IdPとSP間の直接通信は、SOAP のプロトコルを規定。



Liberty Alliance の技術フレームワーク

ID-FF (Federation Framework)
SSOと認証連携のフレームワーク

SAML ベースの認証情報交換プロトコルを規定

・アイデンティティ連携
・シングルサインオン
・シングルログアウト
・連携の解除
など

ID-SIS (Service Interface Specifications)
個人情報に関する各種サービスへのインターフェース仕様

・個人/従業員 プロファイル
・プレゼンスサービス
・位置情報サービス
・アドレス帳サービス など

ID-WSF (Web Service Framework)
個人情報交換のためのWebサービス基盤

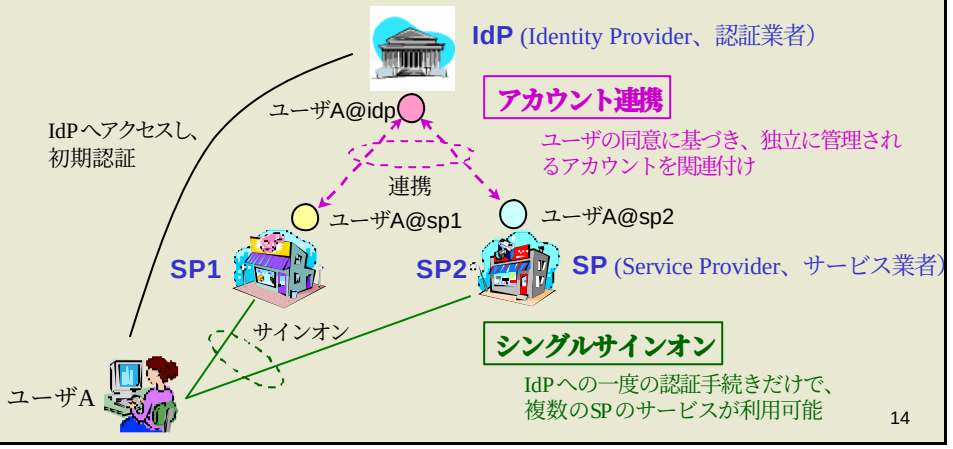
・相互接続可能なアイデンティティサービス
・許諾ベースの属性共有
・アイデンティティサービスの記述と発見
・セキュリティ機構

Liberty 仕様は既存の標準仕様に準拠
(SAML, SOAP, WAP, WS-Security, XML-Sig, XML-Enc, SSL/TLS, etc.)

SAML (Security Assertion Markup Language): 標準化団体
OASISで規定するセキュリティ情報交換のXML言語

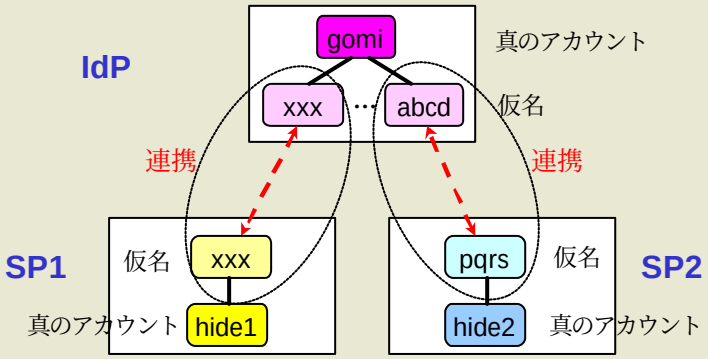
ID-FF (Identity Federation Framework)

- 認証情報を安全に送付し、アカウント連携とSSO（シングルサインオン）を実現



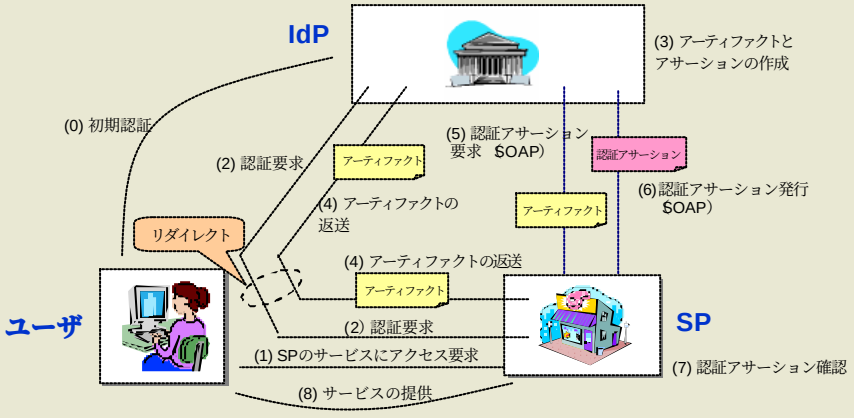
仮名を使ったアカウント連携

- ユーザに関して、IdPとSP間でのみ有効で、ユーザ個人を特定不能な仮名の利用
  - グローバルIDの必要性を排除、実際のアカウント名の流出を防止
  - 名寄せによるプライバシー情報漏洩を防止



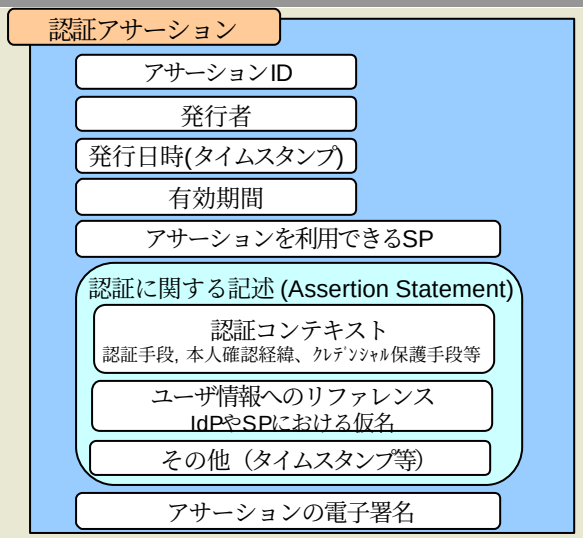
SSOのメッセージの流れ (アーティファクトプロファイル利用時)

- IdPからSPへ認証アサーション（ユーザの認証情報のXML記述）を送付。



（アーティファクト：アサーション取得のためのチケット）

認証アサーション



- SAML (Security Assertion Markup Language) をベースに拡張。
- IdP とSP間でのみ有効な仮名を使ってユーザ個人を参照
- ユーザ個人を識別可能な情報は記述されない。

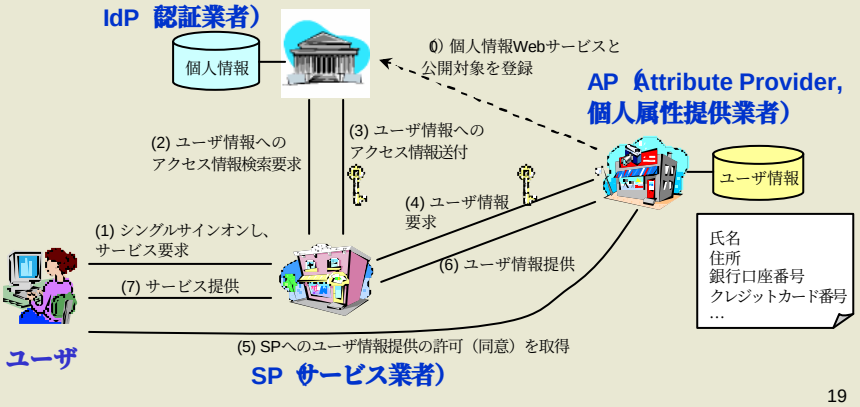
ID-FF の機能

- セキュリティとプライバシーのバランスを考慮し、策定

機能	内容
シングルサインオンと連携	ユーザのSP とIdPで管理されたアカウントの関連を確立する。また、その連携が確立後、一度のIdPへのサインオンだけで、SP のサイトが利用可。匿名アクセス機能もあり。
名前の識別子登録	SP とIdP が主体者に関して互いに交信する際に利用する仮名の識別子(Name Identifier)を登録、変更する仕組み。
連携の解除	SP とIdPが、あるユーザに関して、一旦確立したアイデンティティ連携を解除する仕組み。
シングルログアウト	IdPによって認証された，ある主体者に関する全てのセッションを一括してログアウトを行う仕組み.
IdPの照会	SP とIdPが、どのIdPをユーザが利用しているのかを検索する仕組み。
名前の識別子マッピング	あるユーザに関するIdP とSP間で交換される仮名を、他のSPが入手する仕組み。
名前の識別子の暗号化	SP とIdP間で交換されるユーザの名前識別子情報を暗号化する仕組み。

ID-WSF：個人情報の安全な交換・利用

- サーバに登録されている個人情報をサービス業者間で直接交換し、ユーザのサービス登録や利用時の手間を省いたり、サービスのパーソナライズを図る。

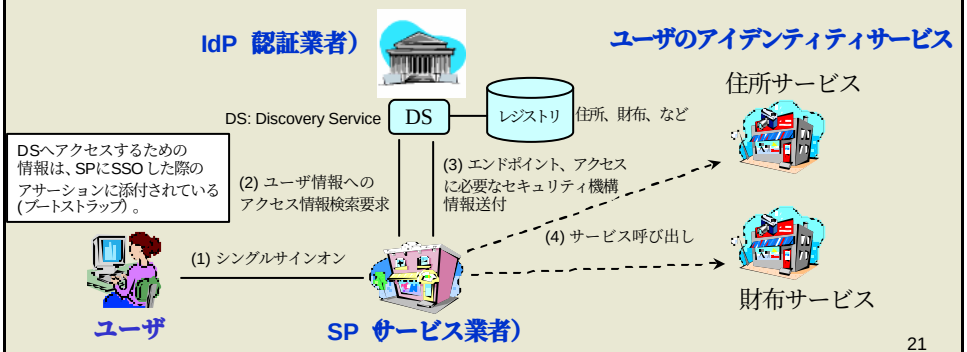


ID-WSF の機能

- アイデンティティサービス（個人情報公開サービス）の登録・検索
  - ID-WSFでは、アイデンティティの Webサービスとして、IdPに登録、管理され、不特定多数への公開を防止。
- 認証へのインターフェース
  - ID-FFのような SSOを利用し、ID-WSFを発動（ブートストラップ）。
  - SOAP によるSASL (Simple Authentication & Security Layer) ベースの認証サービス仕様も規定。
- データへの統一的なアクセスフォーマット
  - 個人情報へアクセスするためのプロトコルとスキーマを規定。
- ユーザとの個人情報取扱に関する対話機能
  - ユーザからオンデマンドで、情報提供に関する許可を取得可能。ユーザをプライバシー侵害から保護。
- アイデンティティサービスへのアクセス
  - 個人情報へのアクセスは、アイデンティティ情報がキーとなり、サービス呼び出しを行う機構を提供。アクセス主体の認証が必須で、厳密かつ柔軟なアクセス制御が可能。

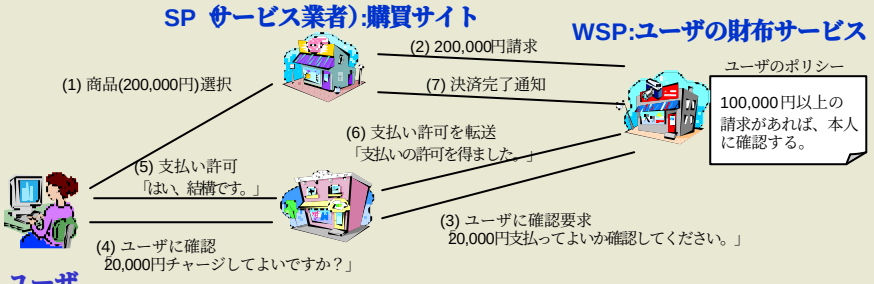
ID-WSF: Discovery Service

- アイデンティティに関連したサービスのレジストリ
  - サービスの登録と検索
  - サービス呼び出しのためのアクセス情報の提供



ID-WSF: Interaction Service

- WSPとユーザを対話させる機能
  - 一般的には、WSPはユーザに直接アクセスしない。
  - 実時間で、個人情報の取扱に関する許可や同意を得る。
- 複数の実現方法
  - WSPに、SPがユーザとの対話を許可し、中継する。
  - WSPに、SPがユーザのブラウザをリダイレクト。
  - WSPが直接にユーザと対話。



WSP: Web Service Provider

サービスインタフェース仕様群

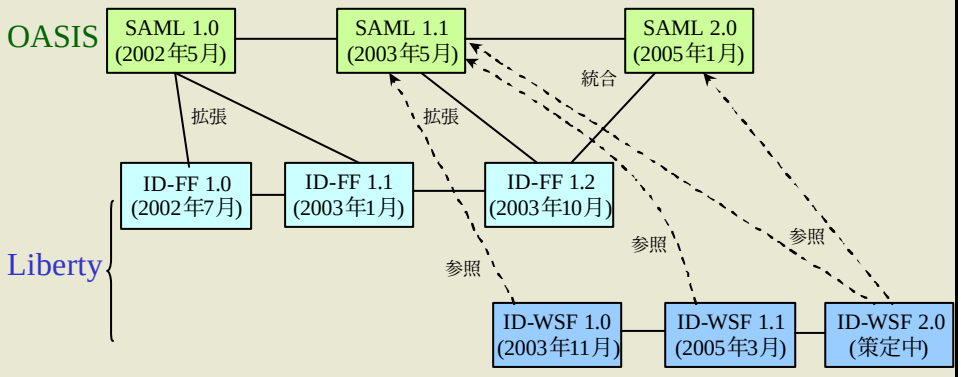
- ID情報を活用する各種サービスと、リバティのフレームワークとのインタフェースを仕様化 (ID-SIS: ID-Service Interface Specification)。4月に以下の3仕様を公開。
  - Contact Book：
    - 知人等の連絡先を運用管理するサービス
  - Presence：
    - 利用者間で互いの所在情報の共有を可能にするサービス
  - Geo-Location
    - 利用者の位置情報を提供するサービス
- 既存のサービス仕様を利用し、重複する新たな仕様を作るわけではない。むしろ、既存のサービス仕様における、セキュリティ・プライバシ強化や利便性の向上、サービス間の連携の促進がねらい。
- 以下のような検討も進行中。
  - ゲーム
  - 携帯電話向けコンテンツサービス

技術仕様の足取りとステータス

- ID-FF
  - 2002年7月ドラフト公開以来、改良を重ね、安定。
  - ID-FF 1.0 適合性試験開始（2003年11月）、現在のべ約30の認定ロゴ取得済み製品あり。
  - ID-FF 1.2 の成果は、OASISへ提供し、SAML 2.0 へ統合済（3月）。
- ID-WSF
  - 2003年4月ドラフト公開以来、仕様策定進行中。
  - ID-WSF 1.0 適合性試験開始（2004年10月）。
  - ID-WSF 1.1 仕様群一般公開（4月）。
  - ID-WSF 2.0 ドラフト仕様群（SAML 2.0 対応版）公開（2月）。
- ID-SIS
  - 個人・従業員情報プロファイル仕様の公開（2003年4月）。
  - プレゼンス、コンタクトブック、位置情報サービスの3仕様群を公開。（4月）、今後、適用サービスを拡充予定。

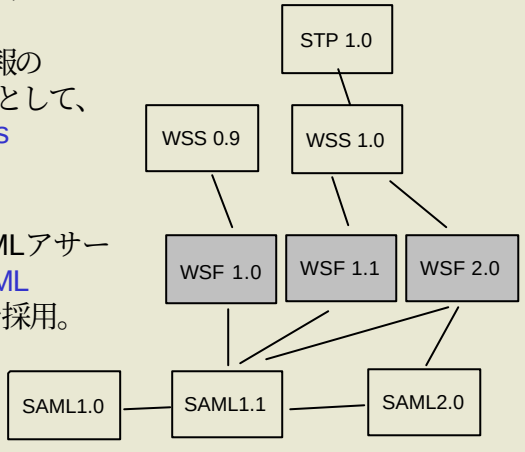
技術仕様策定の足取り

- SAML と Liberty ID-FF、ID-WSF との関係



ID-WSF & WSS & STP & SAML

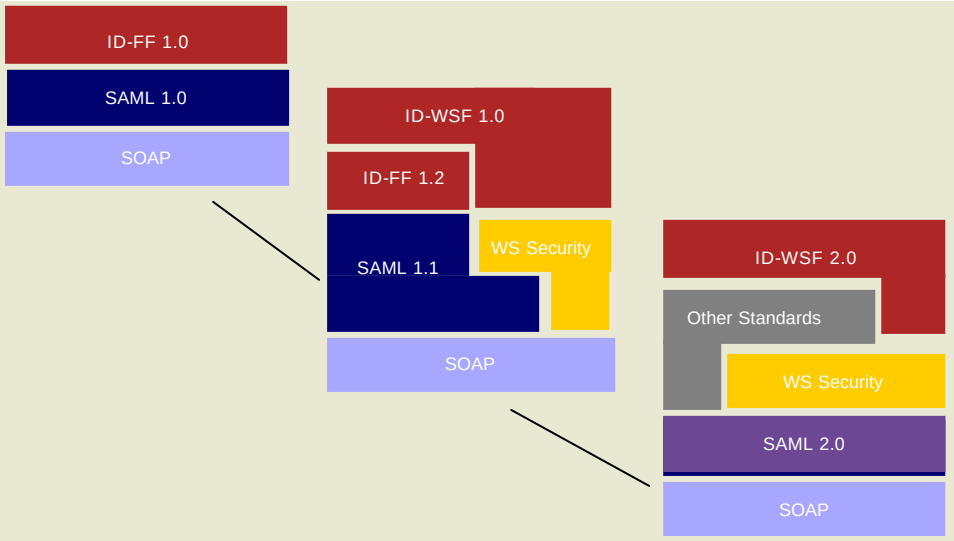
- ID-WSF はSAMLアサーションをセキュリティトークンのフォーマットの 1つとして利用。
- ID-WSF は、セキュリティ情報のSOAPヘッダーへの格納方法として、OASIS WSS (Web Services Security) を採用。
- さらに、ID-WSF は、WSS <Security>ヘッダー内のSAMLアサーションの格納方法として、SAML Token profile (WSS STP)を採用。



LIBERTY ALLIANCE PROJECT

NEC

Liberty とSAML の進展



LIBERTY ALLIANCE PROJECT

NEC

先行事例と新たな適用分野

海外での事例 (1)

- Communicator Inc.(BtoB)
  - 3500以上の機関投資家に対しシングル・サインオンによるボンド債取引システム
- Neustar (BtoB)
  - 銀行・権原保険会社・役所間の土地取引システム
- Niteo partners (BtoB)
  - JPMorgan, Wachovia, Bank of America 間でのアカウント共有Webサービスのシステム
- GM, American Express, Sun (BtoE)
  - 社内システム

海外の事例 (2)

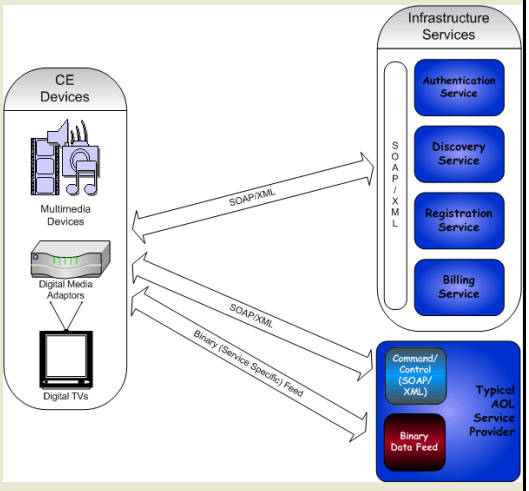
- AOL
  - 米国でRadio@AOLサービス提供中。ID-WSFを用いて、ユーザが同じ設定情報（音楽チャネル等）を様々な端末(PC、携帯電話、携帯音楽プレーヤ等)で利用可能。
- Nokia
  - 既存の携帯電話向けにリバティ対応ゲートウェイ(LEP)を開発中。リバティ対応の携帯電話も、将来の製品ロードマップ上にある。
- Vodafone
  - ゲーム、着メロ、写真メール等のサービスの利便性向上に向けて、ボーダフォンライブ！のリバティ対応を検討中。

日本国内での事例

- EduMart (G(B)toC)
  - 総務省実証実験。世界初のLiberty仕様を用いた教育コンテンツの流通システム。
- NTT コミュニケーションズ
  - Liberty仕様に利用したシングルサインオンサービスを提供中。
- NTT データ
  - Liberty仕様による JAL ONLINE と出張旅費申請システムとの連携。

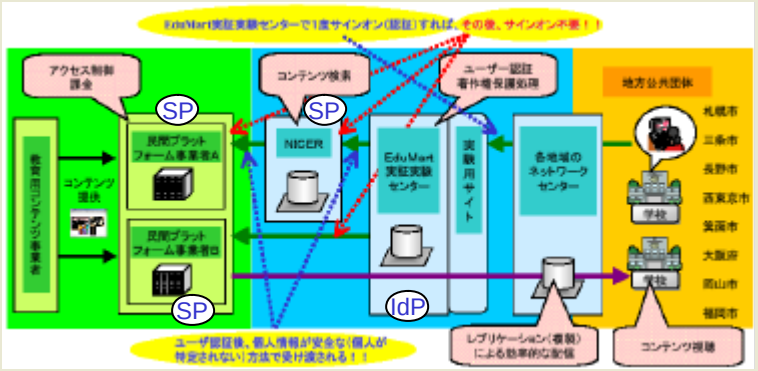
Radio@AOL

- ID-WSFに基づくサービス
  - 認証へのインタフェース（Authentication Service）
  - サービスの登録・検索（Discovery Service）
  - ラジオや写真サービスの提供



総務省 EduMart 実証実験

- 国・地方自治体・学校・民間事業者等が提供するユーザー認証やコンテンツ配信・視聴といった異なる機能を提供するシステムを一回のサインオン（認証）により連携し、シングルサインオン実現。
- 民間事業者が保有する動画等を含む教育用コンテンツを、日本全国に点在する小中高等学校へ配信できるようなインターオペラビリティを確保。



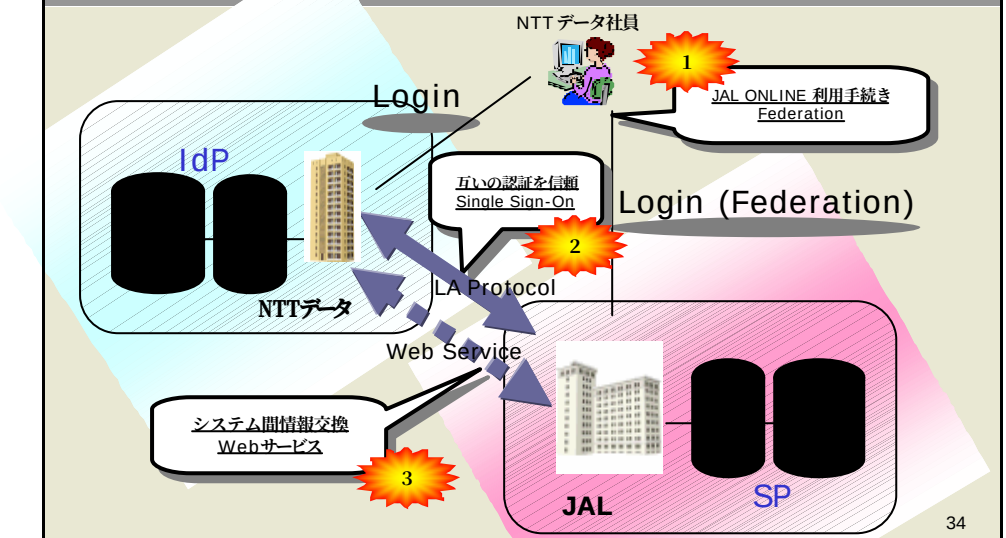
全国の小中高学校
計98校 計4610端末

コンテンツ事業者24社

* NICER : 教育情報ナショナルセンター

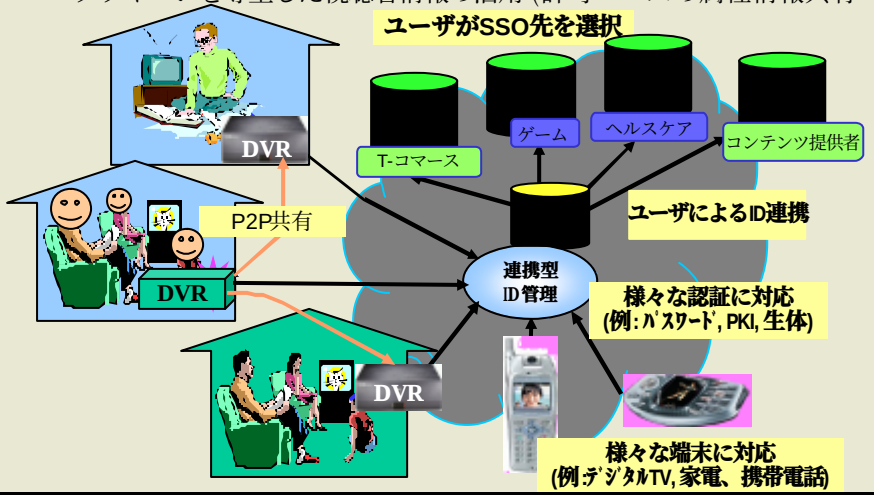
（総務省報道発表資料より）

JAL Onli と出張旅費申請システムとの連携



新たな適用分野 :デジタルTV

- コンテンツやサービスへの簡単アクセス (シングルサインオン)
- プライバシを尊重した視聴者情報の活用 (許可ベースの属性情報共有



Liberty 技術の適用を サポートする取り組み

プライバシーに関する取り組み

- Liberty プライバシー勧告：欧米諸国の既存のプライバシー保護法やガイドラインを元に公正な情報取扱に要する原則の基準を作成。これらを基本として、Liberty技術仕様は策定されている。
  - Notice　通知）
  - Choice　選択）
  - Principal Access to Personally Identifiable Information (PII)　主体者による個人識別情報へのアクセス）
  - Quality　品質）
  - Relevance　妥当性）
  - Timeliness　適時性）
  - Complaint Resolution　（クレーム解決）
  - Security　セキュリティ）

Liberty仕様と日本の個人情報保護法

- 個人情報取扱事業者の義務（第15条～第36条）の明記内容とLiberty仕様での取り組みの対応

個人情報保護法要件	Libertyプライバシー勧告	Liberty仕様
0) 本人同意の原則	a) Notice b) Choice	本人同意に基づくアイデンティティ連携／シングルサインオン(ID-FF)やインタラクションサービス (ID-WSF)など
1) 利用目的の明示・順守	a) Notice e) Relevance f) Timeliness	用途指示子(Usage Directives, ID-WSF)など
2) 不正取得の禁止	-	-
3) 適正管理	d) Quality h) Security	暗号鍵サイズの推奨や通信トランスポートにおけるSSL/TLS使用の推奨、Security Profiles(ID-WSF)など
4) 授受制限	直接対応する項目はないため、本人同意の原則に基づき対応	0) 本人同意の原則や1)利用目的の明示・順守の項を参照
5) 情報公開	a) Notice	-
6) 本人アクセスの提供	c) Principal Access to PII	-
7) 苦情処理	g) Complaint Resolution	-
8) 行政機関への対応	-	-

- Liberty技術の採用は個人情報保護法と干渉しない。
- Liberty技術の採用だけでは個人情報保護法を充足しない。
- Liberty技術の採用により個人情報保護を強化できる。

LIBERTY ALLIANCE INTEROPERABLE

NEC

Liberty適合性試験

- 各企業がLiberty技術仕様に基づいた製品を持ち寄って、仕様への適合性と相互運用性を検証する試験を実施。合格製品に対して認定ロゴを交付。
- エンドユーザの製品選択を助け、該当製品がすぐに利用可能な相互運用性を持ち、導入から運用開始までの時間を短縮し、生産性を高めコストを削減可能。
- 適合性認定ロゴ取得製品はLibertyの以下のURLで参照可能。
  http://www.projectliberty.org/about/enabledproducts.php
- SAML 2.0 向け適合性試験も開始。

LIBERTY ALLIANCE PROJECT

NEC

多様なアーキテクチャへの対応

- リバティには、様々な端末やNW、利用形態に適用するための仕様が用意されている。
- モバイルNWや端末、アプリ等への対応のためのプロキシ仕様
  - LECP: Liberty Enabled Client and Proxy

  ブラウザのかわりに、リバティ対応のクライアントやプロキシとしてサーバと通信
    - 例： 移動網とインターネットをつなぐゲートウェイへの応用
    - 例： メッセンジャー等のブラウザ以外のクライアントへの対応
- 端末主導型のアーキテクチャを実現するための仕様
  - LUAD: Liberty User Agent Device

  端末側がWebサービスのクライアントとして動作し属性情報等を取得
    - 例：音楽プレーヤがユーザ設定情報をサーバから直接取得
  - PAOS：SOAPの反対読み！

  端末側がWebサービスのサーバとして、属性情報等を提供
    - 例：携帯電話にユーザ情報を格納しておいて必要な時にサーバに送信

新たな取り組み

- Principal Referencing
  - ユーザが他のユーザの個人情報に対して アクセスするための技術。ユーザ間のセキュアな情報共有を促進する。
- ID Roaming
  - IdP（オペレータ）間の認証情報の転送。IdP間での認証情報を連携し、サービスの継続的利用と再認証機会の削減を意図する。
- Strong Authentication
  - あらゆる認証プロトコル、デバイスでもLiberty仕様が利用できるようにするための枠組みの検討。様々な業界団体と連携し、既存の認証プロトコルの利用を模索。
- Provisioning
  - アイデンティティ情報の自動的配置、アカウントの自動生成、更新など。
- iClient/Robust Client
  - 認証機能を強化した組み込みクライアント。
- CMS (Content Messaging Service)
  - SMS (Short Messaging Service)やMMS (Multimedia Messaging Service)などのサービスをLiberty のフレームワークを利用してWebサービス上で利用可能とするためのインターフェースを規定。

ビジネス要件を整理し、技術仕様の策定に進む予定

日本SIGでの活動内容

- 目的
  - 日本での知名度向上と普及活動の推進
  - ガイドラインや白書等の翻訳
  - 日本に即したガイドラインや白書の作成
- 参加企業
  - 日本の企業及び外資系の会社など10数社が参加
- 実施内容（2004年度）
  - 仕様書、白書等の日本語版の公開
  - RSA Conference Japan で講演（5月）
  - HP World で講演（7月）
  - リバティ「特別セミナー」開催（於品川、10月）
  - 「Liberty Alliance と日本の個人情報保護法」文書公開（3月）
  - 日本語版HPのリニューアル（3月）

ご参考

さらに詳細情報のために

- Liberty Alliance Webサイト
  - http://www.projectliberty.org/
- Liberty Alliance Webサイト日本向けHP
  - http://www.projectliberty.org/jp/
- Liberty Alliance 日本語文書リソース
  - http://www.projectliberty.org/jp/resources/
  - 以下のような文書を公開中
    - 「Liberty Alliance と日本の個人情報保護法」
    - 「プライバシーとセキュリティのベストプラクティス」
    - 「アイデンティティ連携による政府のメリット」
    - 「Libertyプロトコルとアイデンティティ盗用に関する白書」
    - Liberty仕様チュートリアル
    - など

連絡先

- リバティ・アライアンス広報担当
  (株)井之上パブリックリレーションズ
  - TEL: 03-5269-2301
  - FAX：03-5269-2305
  - E-Mail：liberty@inoue-pr.com

Liberty Alliance Day in Japan 2005

- 昨年に引き続き、Liberty Alliance主催セミナーを開催致しますので、是非、お越し下さい。
  - 日程：2005年10月24日（月）
  - 場所：東京カンファレンスセンター（品川）
  - 内容：「個人情報保護法時代におけるセキュアなサービス連携に向けて」
    - SOX
    - コンプライアンス
    - ID盗難対策
    - SAML
    - Etc.