応用技術部会　セキュリティWG活動報告
- SAMLの実装

2003年 6月 2日

XML Consortium 応用技術部会
セキュリティSWG
(株)NTTデータ 坂田 祐司
(株)日立製作所 坂田 匡通

本日の報告内容

- セキュリティSWGにおける活動内容
- SAMLの概要
- デモンストレーション
- デモの実装詳細
- 関連仕様

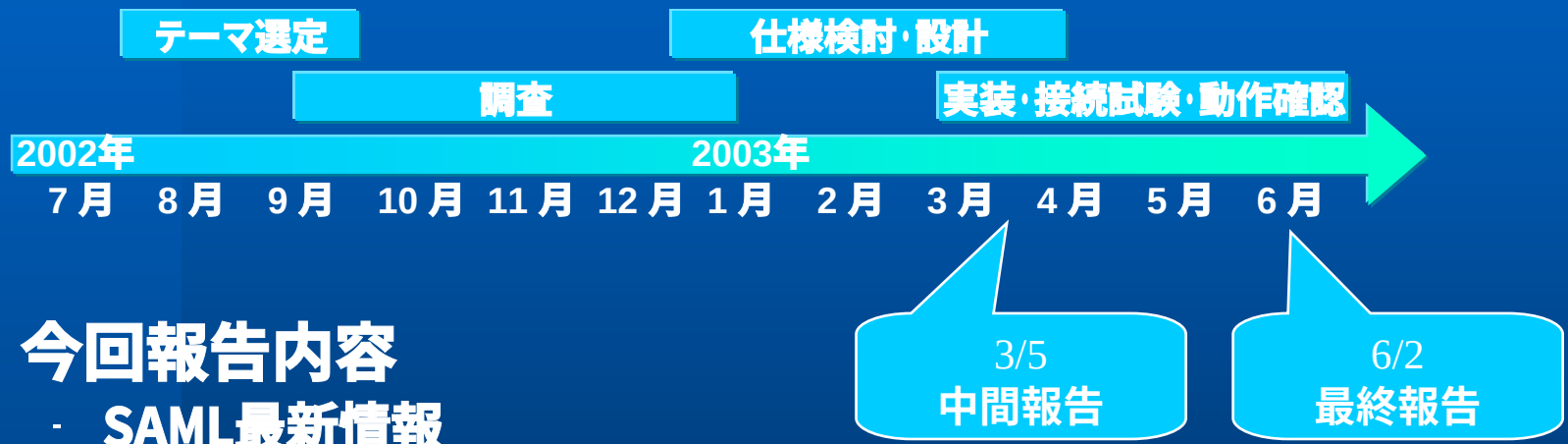
セキュリティ SWGの活動概要

- SAML サブサブWGの活動について
- 背景と目的
  - 企業間や複数WWWサイト間でのユーザ情報の共有の必要性
  - 需要の喚起, 利用方法の模索
  - SAMLの利用例の可視化のためのデモンストレーションの構築
    - WWWサイト間のシングルサインオン
    - WWWサイト間でのユーザ情報の共有
  - 実装ノウハウの獲得
  - 利用ライブラリの異なる実装における相互運用性の検証
    - 言語･ライブラリ
      - Java
      - ~~(.Net , Microsoft社)~~ 時間の関係で出来ず
      - OpenSAML
      - Trust Services Integration Kit(TSIK, Verisign社)

SAML:Security Assertion Markup Language

計画と今回の報告内容

- 計画
  - MLと月一回のミーティング



- 今回報告内容
  - SAML最新情報
  - デモンストレーション
  - 実装ノウハウ
    - 実装したライブラリによる差異
    - 相互接続における問題点

本日の報告内容

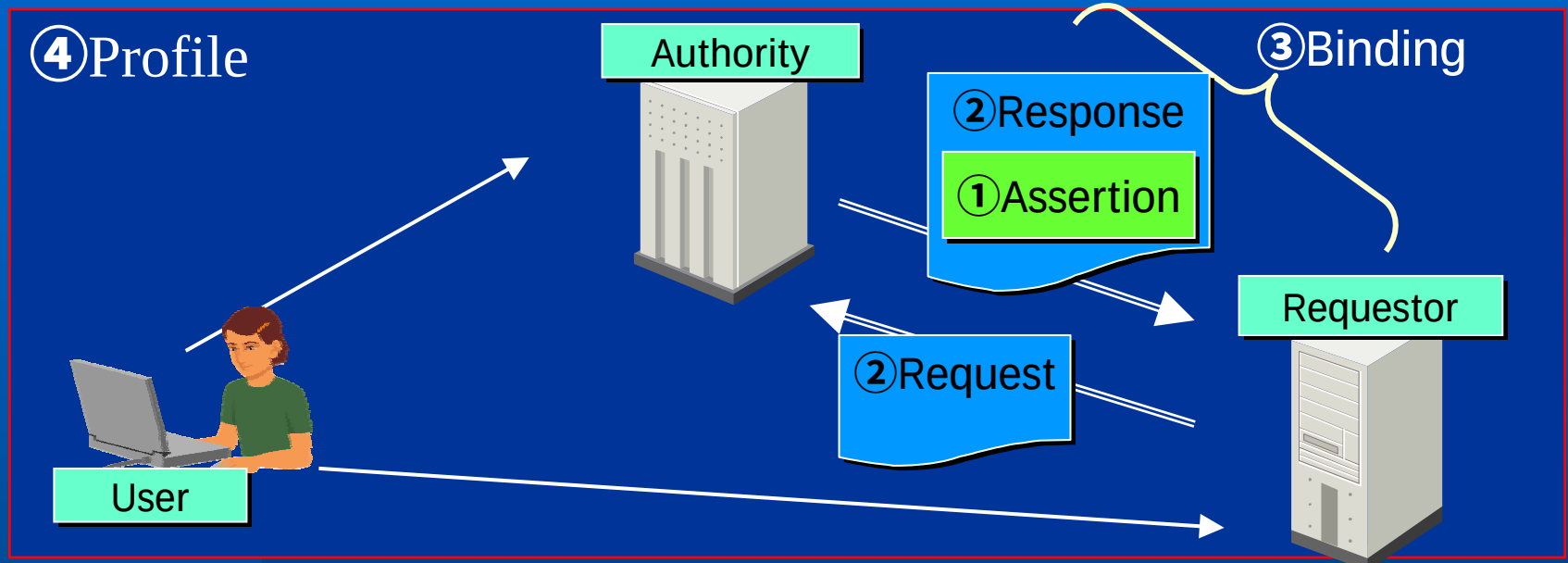
- セキュリティSWGにおける活動内容
- SAMLの概要
  - 仕様の概要
  - 利用アプリケーション例
- デモの実装詳細
- デモンストレーション
- 関連仕様

SAMLの概要

- Security Assertion Markup Language
  - ユーザの認証、属性、許可情報を表現するXML記述形式、発行者と利用者でのメッセージ交換プロトコル等を規定
- OASISによって標準化が行われ，現在OASIS Standardである(v1.0).
- 何を実現するものか?
  - 異なる組織間でユーザ情報を共有する
    - ユーザの認証状態 by Authentication Assertion
    - ユーザの属性 by Attribute Assertion
    - ユーザの持つ権利 by Authorization Decision Assertion
  - WWWサイト間のシングルサインオン(SSO)
    - Cookieが使えない場合

OASIS = Organization for the Advancement of Structured Information Standards
電子商取引に関する標準を決定し，その利用を促進する非営利団体

SAMLの仕様



① SAML アサーション　：認証、属性、許可情報を表現。
② SAML プロトコル　　：アサーションを交換するための交換プロトコル。
③ SAML バインディング: トランスポートプロトコルにどのように乗せるかを規定。
④ SAML プロファイル　：実際のサービスを実現するための一連のプロセス規定。

SAML アサーションの例

- SAML 認証アサーション例

JFBは
このユーザが
下田さんであると
保証します

```
<saml:Assertion
  MajorVersion="1" MinorVersion="0"
  AssertionID="128.9.167.32.12345678"
  Issuer="JFB Tourist"
  IssueInstant="2001-12-03T10:02:00Z">
  <saml:Conditions
    NotBefore="2001-12-03T10:00:00Z"
    NotOnOrAfter="2001-12-03T10:05:00Z" />
  <saml:AuthenticationStatement
    AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"
    AuthenticationInstant="2001-12-03T10:02:00Z">
    <saml:Subject>
      <saml:NameIdentifier
          Format="#X509SubjectName">
          cn=shimoda,o=jfbportal.c=jp</saml:NameIdentifier>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

○時×分、JFBが内容を証明しています.

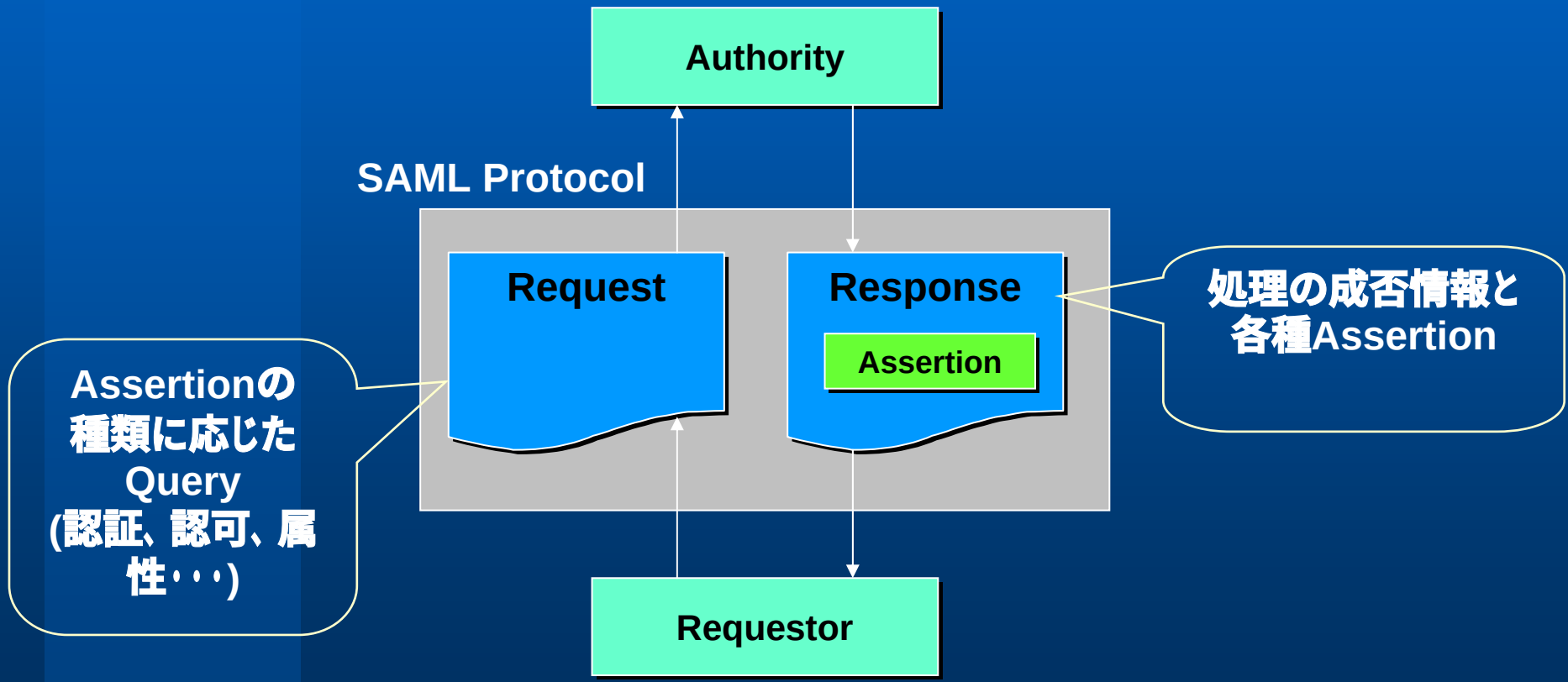
証明の 有効期限を示している

パスワード認証である

下田さんは認証されています.

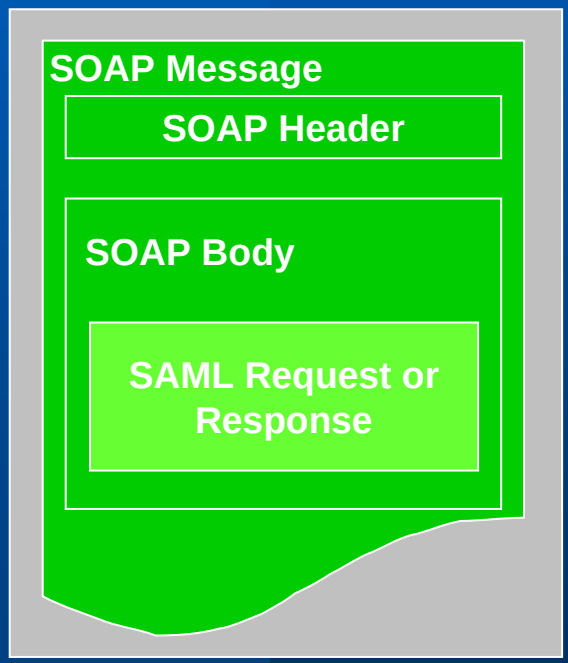
SAML protocol

- *SAML protocol* はSAML Assertionを獲得するための Request/Response型のメッセージプロトコルフォーマット



SAML binding

- トランスポート層にインターネット標準プロトコルを用いて，SAML ProtocolのRequestとResponseを交換するための方法を定義したもの
- SAML 1.0ではSOAP-over-HTTP bindingが定義されている。
- 今後、HTTP binding, TCP/IP bindingなどが定義される予定



SOAP-over-HTTP Binding

```
POST /SamlService HTTP/1.1
Host: www.example.com
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<SOAP-ENV:Envelope
xmlns:SOAP-
    ENV=”http://schemas.xmlsoap.org/soap/envelope/”>
  <SOAP-ENV:Body>
    <samlp:Request xmlns:samlp:=”…” xmlns:saml=”…
      xmlns:ds=”…”>
    <ds:Signature> … </ds:Signature>
      <samlp:AuthenticationQuery>
        …
      </samlp:AuthenticationQuery>
    </samlp:Request>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

SAML Profile

- 実際のサービスを実現するための一連のプロセス規定
  - アサーションをどのように利用するか。
  - プロトコルやシーケンスにマッピングするか。

- 現在，Webブラウザでシングルサインオンを実現するための，二つのProfileが定義されている．
  - Web Browser SSO Profiles of SAML
    - Browser/Artifact Profile of SAML
    - Browser/POST Profile of SAML

特徴：Cookieの仕組みは利用しない

今回のデモでは Browser/Artifact Profileを実装

- 今後以下のようなProfileが定義される予定
  - SOAP Profile of SAML
    - SAMLを用いてWebサービスをセキュアにするための”方法”

SAML1.1

- **基本的にはSAML 1.0の仕様の曖昧な点を変更**
- **SAML1.1は委員会標準としての承認を受けるための仕様の公開とコメントの受付が2003/5/16に終了**

SAML 1.0から1.1の主な変更点

- Assertion, Request, Responseの各要素の属性になるIDがXMLスキーマの文字列型からXMLスキーマのID型に
- DoNotCacheCondition要素の追加
  - 要素名のとおり、アサーションを保存せず一回の判断にのみ使うことを示す。 認証などの場合に用いられるものと思われる
- AuthorityBinding要素を非推奨要素に
- RespondWith要素を非推奨要素に
- XML署名方式の明確化
- バージョニングに関する詳細化
- 処理ルールの明確化
  - ex. Artifact のURLフォーマットをUTF-8に
- SOAP Bindingにおけるエラーでも SAMLのエラーとして扱う

SAML 1.1における電子署名

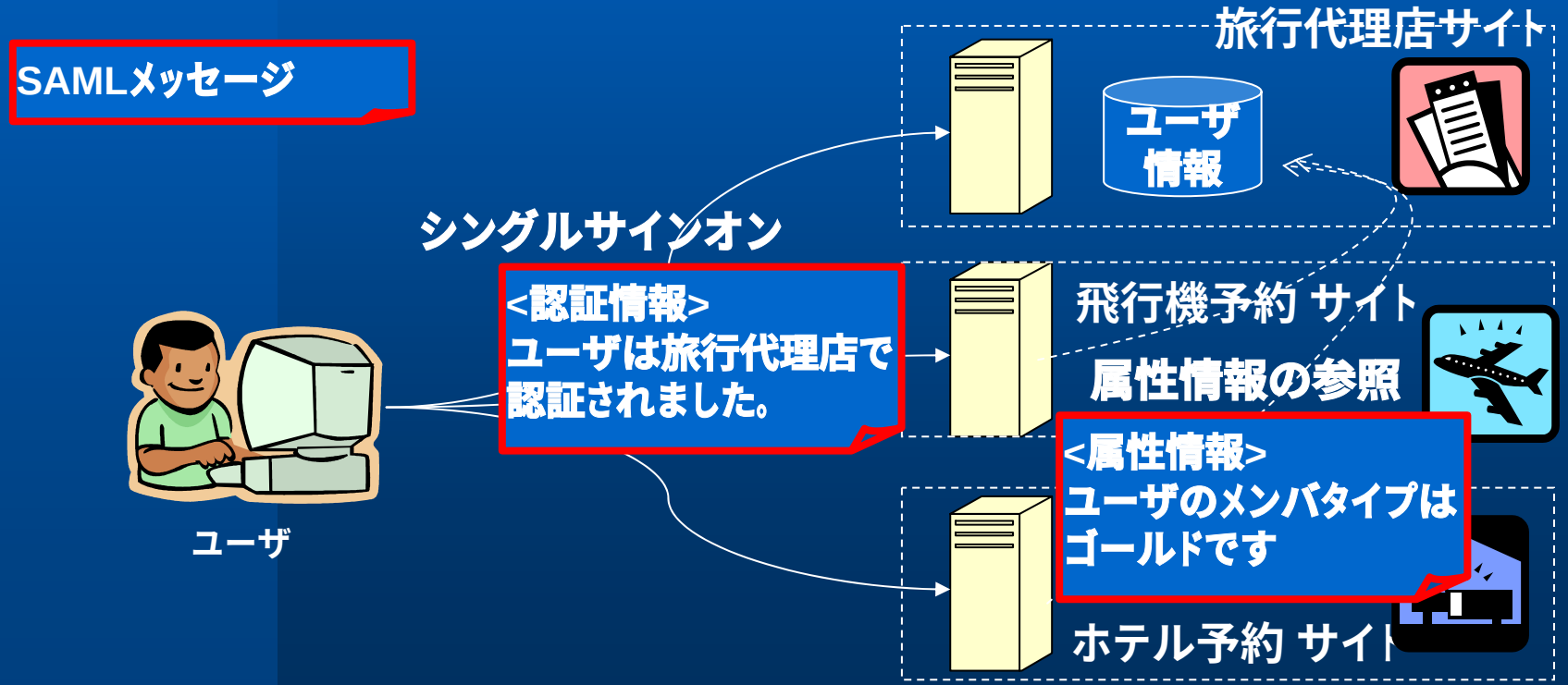
- SAML v1.1 Section 5
- SAML v1.0では電子署名の方式が曖昧で相互運用が困難であった。(5.4.7)
- 今回決めたこと

1. どのような場合にSAMLメッセージに署名すべきか
   - 署名付SOAPメッセージ、S/MIME,SSLなどでも良い場合がある。
     何を利用するかはProfileで決めるべきという指針を決めている
   - (指針として)SAMLリクエスタとオーソリティの間に別のエンティティが存在する場合はSAMLメッセージにXML署名をしたほうが良い。
2. もし、XML署名するならどのような形式にすべきか
   - 対象要素: Assertion, Request, Response要素
   - 方式: Enveloped Signature(必須), RSA-SHA1(推奨)
   - 参照方法: 対象要素のID属性によって指定
   - 正規化手法: Exclusive Canonicalization
   - 鍵情報: 特に制限なし

SAMLの利用アプリケーション例

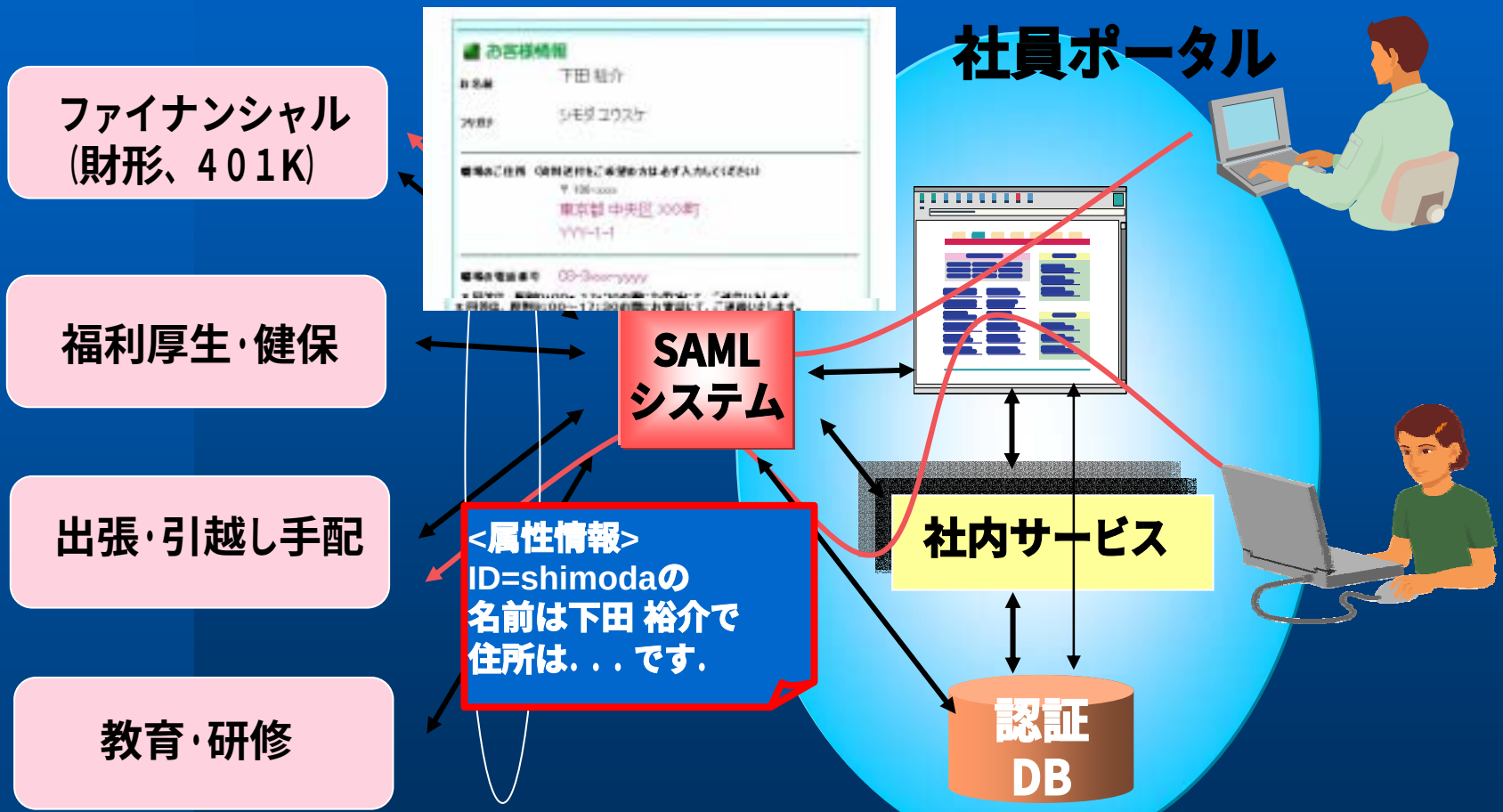
適用例：B2C

- ユーザが複数のサイトを用いて、旅行の予約を行う
  - シングルサインオン
  - ユーザ情報の共有



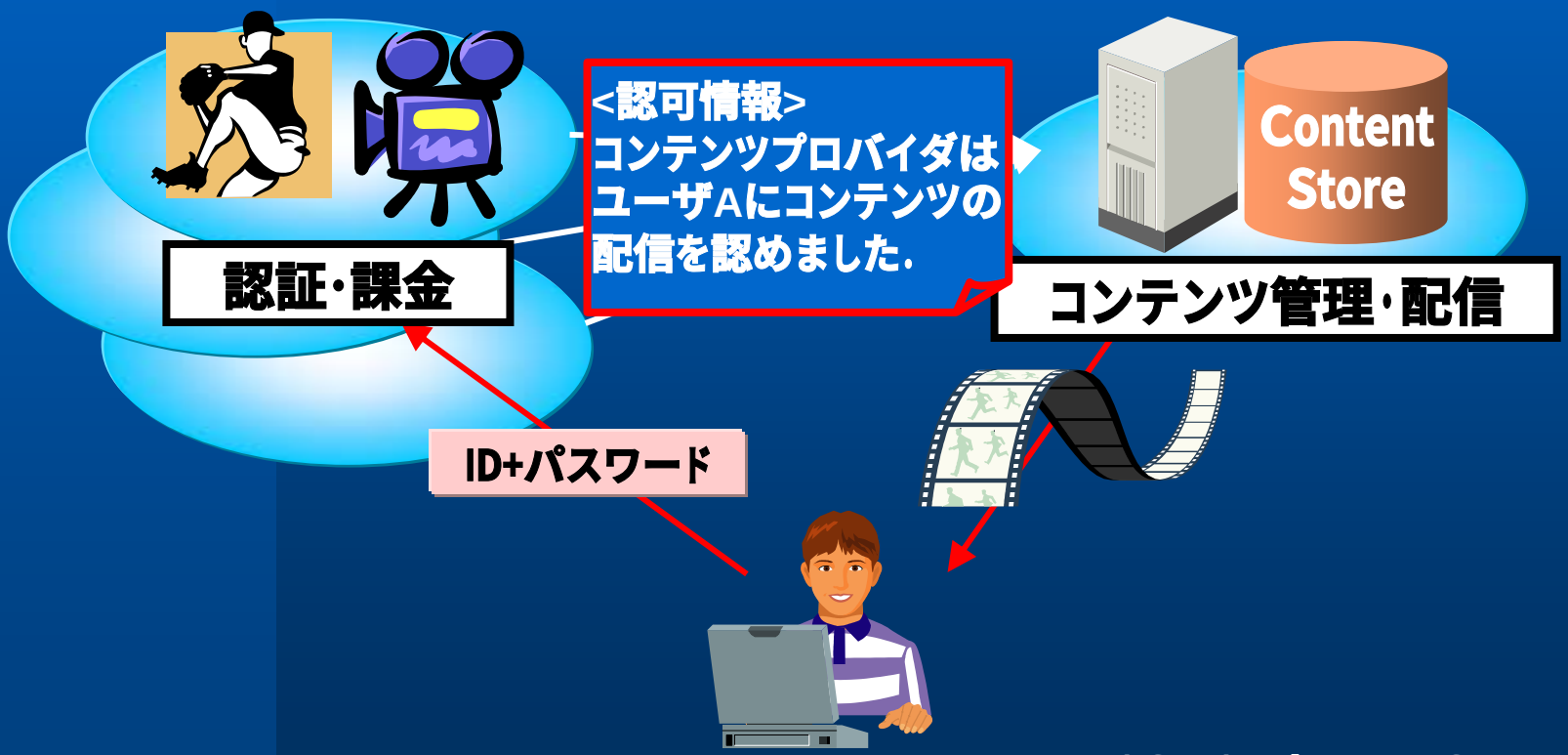
適用例：B2Eポータル

- 社外提携サービスへのシングル・サインオンや属性情報交換



適用例：ASP連携における認可情報提供

- コンテンツポータルとコンテンツ配信サービスとの連携



ASP:Application Service Provider

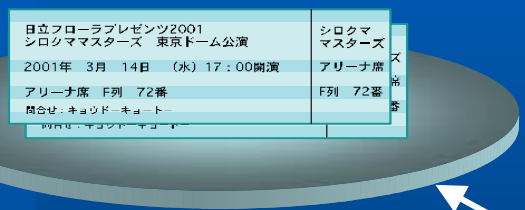
適用例：権限委譲

- コミュニティメンバ同士で権限委譲

SAML拡張

<権限委譲情報>
発行者名：坂田
対象者　：下田
権限　　：サッカーチケット購入
利用制限：1000円まで、決済機能付

署名



チケットサイト

日本代表応援
ネットコミュニティ

決済会社サイト

請求書

請求書

請求書

本日の報告内容

- セキュリティSWGにおける活動内容
- SAMLの概要
- デモの実装詳細
  - NTTデータ実装
  - 日立製作所実装
- デモンストレーション
- 関連仕様

SAMLオーソリティ,SAMLリクエスタの実装

～WebLogic 編～

㈱ NTTデータ 坂田祐司

作業実績

- 設計と実装
  - SAMLオーソリティ、リクエスタのプロトタイプの作成
  - オフラインでの互換性試験
  - オンラインでの接続試験

設計と実装 (続き)

- 環境
  - Windows XP Professional SP1
  - J2SDK 1.3.1
  - BEA WebLogic 7.0
    - WebLogic SSPI(Security Service Provider Interface)
  - JAAS (Java Authentication and Authorization Service)
  - Apache SOAP 2.1
  - Apache XML Security 1.05D2

設計と実装 (続き)

- **実装した主な仕様**
  - SAML Assertion
    (Authorization**にのみ必要な**Assertion**要素を除く**)
  - SAML Protocol
  - Browser/Artifact **プロファイル**
  - SOAP Binding
  - WebLogic**とのインタフェース部**
- **ステップ数**:**約**6Ks
- **その他にアプリケーション部**: HTML, JSP

SAMLオーソリティ，SAMLリクエスタの実装

～OpenSAML 編～

2003年6月2日
XML Consortium 応用技術部会
セキュリティSWG：坂田 匡通
（株式会社　日立製作所）

作業実績

- 調査：約20H
  - SAMLの調査
  - OpenSAMLの調査
- 設計と実装
  - OpenSAMLを用いたオーソリティ、リクエスタの作成
  - オフラインでの互換性試験
  - オンラインでの接続試験

設計と実装 (続き)

- 環境
  - Windows XP Professional SP1
  - J2SDK 1.4.0
  - Jakarta Tomcat 4.1.24
  - Apache Axis 1.1 Release Candidate 2
  - Apache XML Security 1.0.5D2
  - OpenSAML

設計と実装 (続き)

- OpenSAMLとは
  - オープンソースのSAMLライブラリ (Apache/BSD-styleライセンス。)
  - Internet2(UCAID) Shibbolethプロジェクト
  - Java and C++
  - SAML v1.0に対応。ドラフトv1.1に一部対応
  - SAML Browser/POSTプロファイルに対応
    - # Browser/artifactプロファイルには未対応

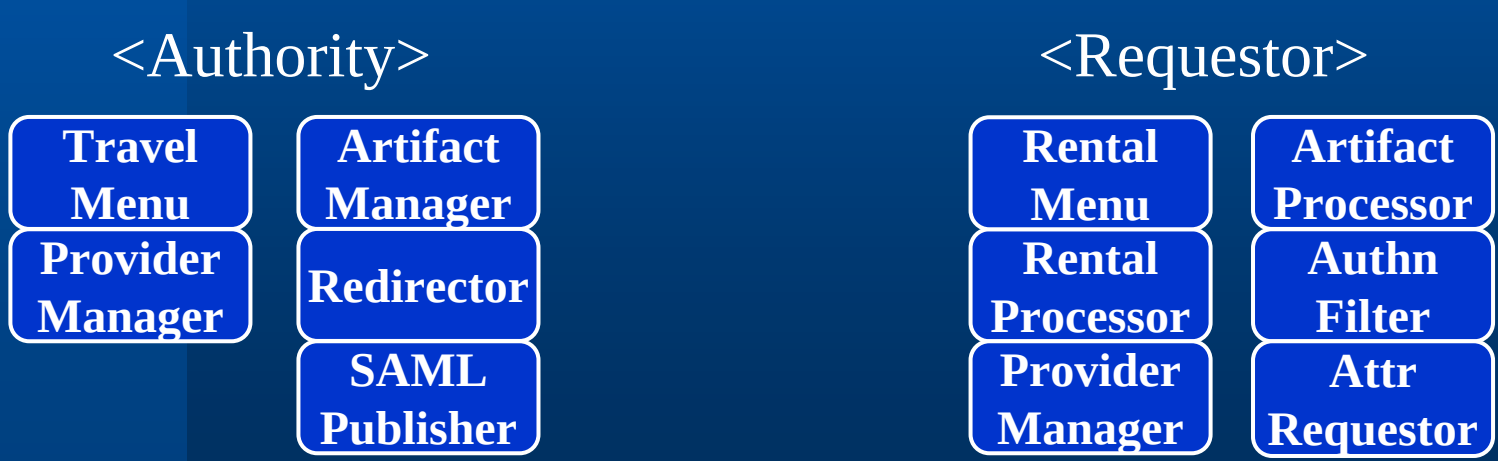
参考URL

OpenSAML : http://www.opensaml.org/

Internet2 Shibboleth : http://shibboleth.internet2.edu/

設計と実装（続き）

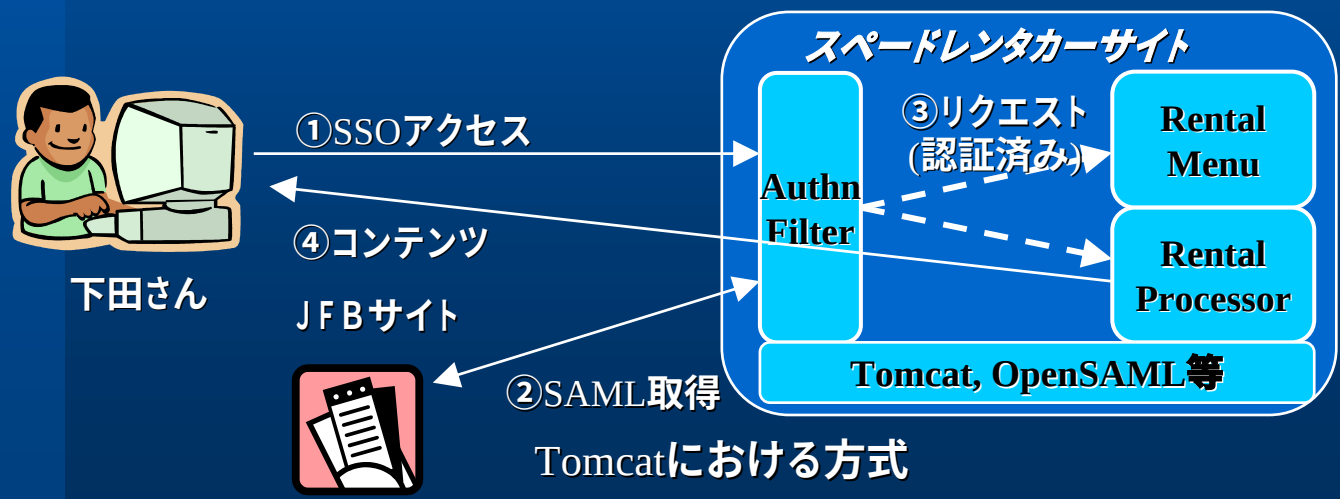
- **実装した機能**
  - Browser/Artifact **プロファイル**、SOAP Binding、**アプリケーション**
- **新規開発規模**
  - **ライン数**：**約**1.5ks
  - **クラス数**：11　**その他に**HTML, JSP



各実装における工夫点、考察・感想

障害となった点、工夫した点など

- 既存認証システムとの互換
  - SAMLを用いてシングル・サインオン（SSO）してきたユーザに、通常の認証処理（ID・パスワード等）と同等の権限を与える方法・機能を調査
  - OpenSAML(Tomcat)では、Servlet 2.3 Filter機能を利用して、全てのリクエストをキャプチャーし、認証情報をリクエストに付加して処理
  - WebLogicでは、WebLogic 7.0のSSPI,JAASを利用



Tomcatにおける方式

障害となった点、工夫した点など

- オーソリティやサービスプロバイダの設定情報
  - オーソリティやサービスプロバイダ設定に関する情報の持ち方
  - オーソリティやサービスプロバイダ間で交換されるべき情報
    - Metadata for ~ Profileとして今後は標準化されると思われる
  - 内部的な情報もある
    - ユーザ情報のデータソースや形式など
- 複数データソースを想定する場合の実装
  - LDAPサーバを想定したJNDIに経由での認証やユーザ取得(LDAPサーバ)
  - XML形式のユーザ情報(XMLファイル)
- 属性と値との関係、名前空間の扱いなど

障害となった点、工夫した点など

- 属性情報をContactXML等を使って定義。
- Liberty 1.2では基本的な個人情報をPersonal Profileとして定義している。ContactXML等の仕様とのマッピングが必要？

考察と感想

- SAML1.0仕様の疑問点
  - SAML Requestにリクエストサイトの情報を記述するタグがない。
    - Authorityサイトは、どのサイトからのリクエストかを別の方法で知る必要がある。
      (SSLクライアント認証、HTTP Basic、署名のKeyInfo)
  - SSOセッションを管理する機能がない。
    - 属性情報を要求するときに、属性Query情報としてSubject(誰の)、AttributeName,AttributeNamespace(何を)という情報しか記述できない。
      ⇔認証リクエストと属性リクエストが独立セッションになってしまう。

考察と感想

- SAML1.0仕様の疑問点
  - XML署名方式の規定があいまい
    - 1.0では正規化方式、署名タイプは規定されているが、Referencesの書式がきていされていなかった。
    - 今回のデモではdraft-sstc-xmlsig-guidelines-03で記されていたXPath Filter2を使った方式で作成。
    - SAML1.1ドラフトではXPath Filter2を使わない方式に変更されている。

考察と感想

- サービスへの適用性
  - SAMLはセキュリティデータの交換のための大きな枠組みを決めている。
    cf. Liberty 仕様ではかなり厳密な仕様となっている。
    -アカウントリンク、匿名アクセス、パーソナルプロファイル・・・
  - SAML1.0のSSOプロファイルを用いて簡単なSSOサービスは適用可能。
    今後、他のプロファイルの拡充が必要。
    (OASIS Security Services TC で検討が行われるかは疑問？？)
  - SAML1.0準拠製品を用いても、相互運用するためには事業者間の事前の検証が必要。
- OpenSAML
  - OpenSAMLは一部を除きSAML1.0基本的な部分はカバー
  - SAMLの世界を体験するには十分。
    (実際にサービスに適用するにはエラー処理、API等改良が必要)

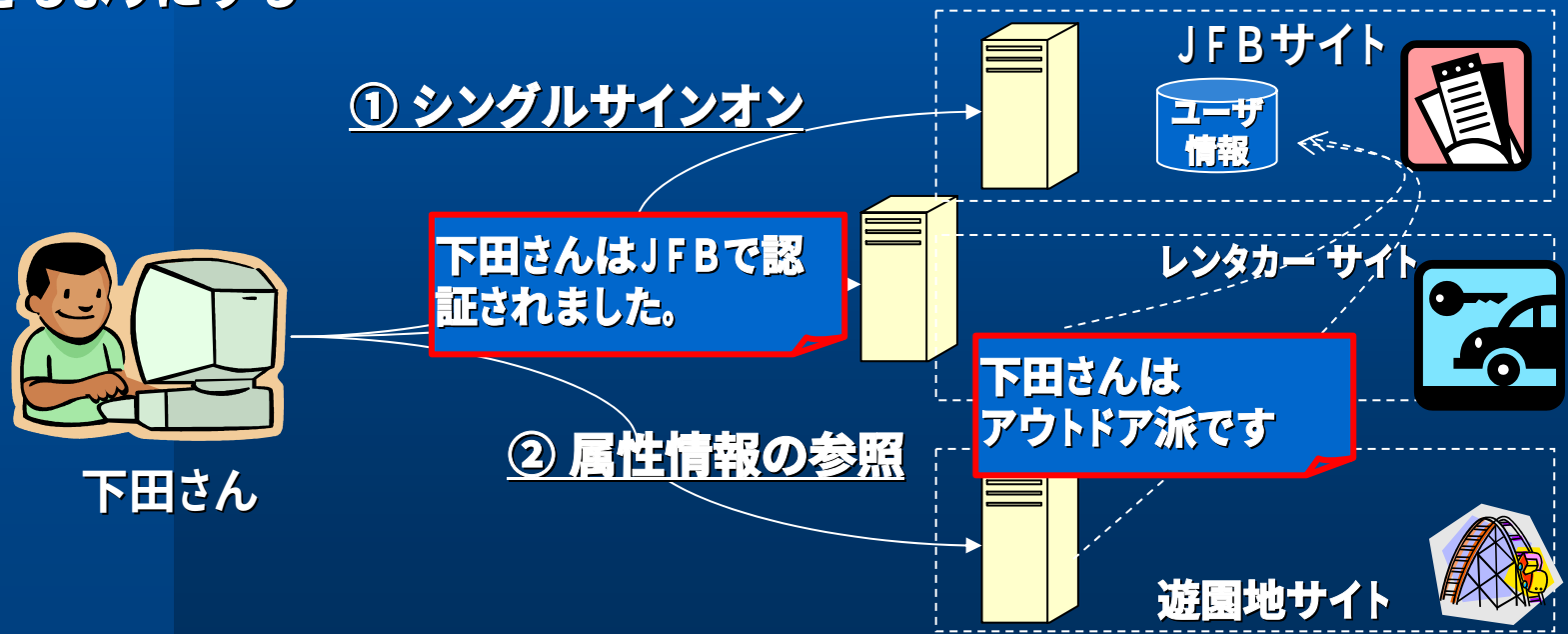
本日の報告内容

- セキュリティSWGにおける活動内容
- SAMLの概要
- デモの実装詳細
- デモンストレーション
- 関連仕様

デモでのSAMLの利用：認証と属性情報の共有

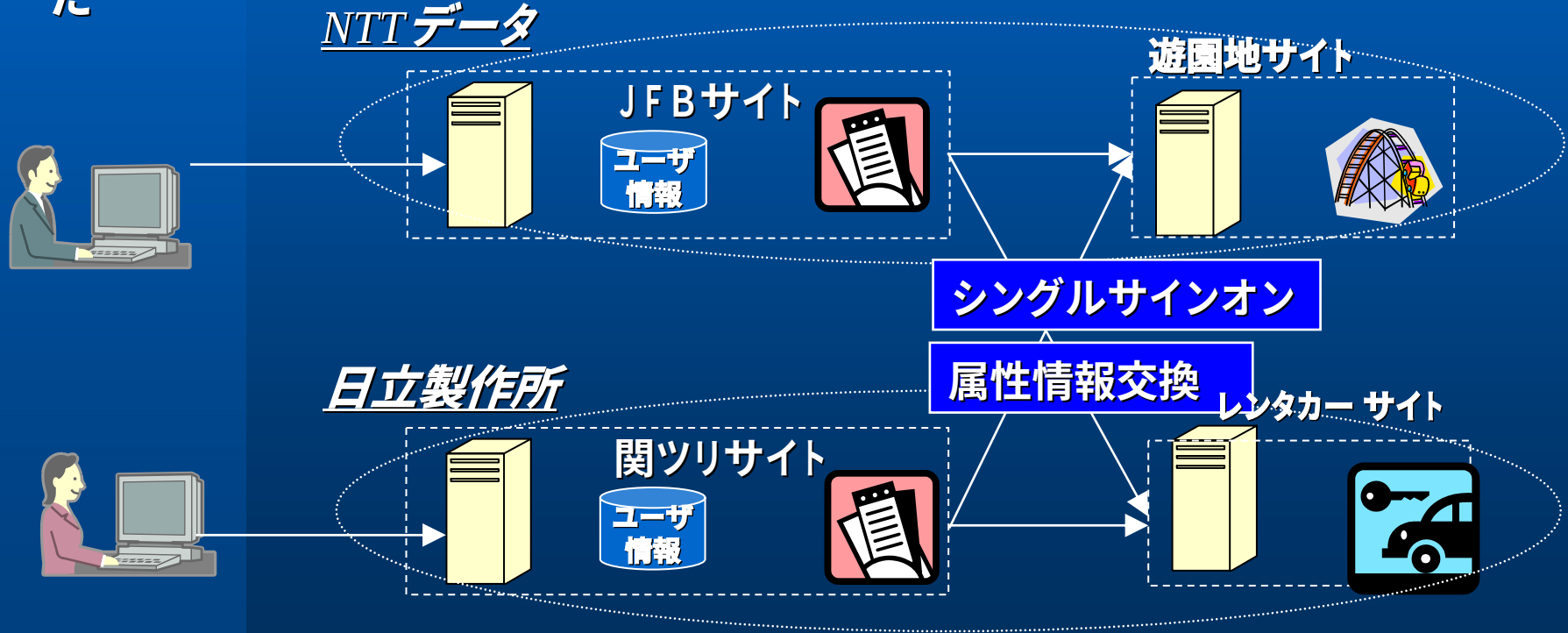
「下田さん」は、どのコンテンツサイトを最初に利用しても、「JFB」サイトによる認証を一回受ければその後はシングルサインオンでコンテンツサイトに認証される

「JFB」サイトで管理しているユーザ情報(住所やクレジット情報など)は適切なプライバシーを確保した上で、他のサイト(レンタカー、遊園地サイト)でも利用できるようにする



相互接続実験

- デモに先立ち相互接続試験を実施
- NTTデータで作ったプロトタイプと日立製作所で作ったプロトタイプで相互接続試験を実施
- 何点か仕様だけでは曖昧な部分に合意が必要であったが、最終的に成功した



デモンストレーション

デモのポイント

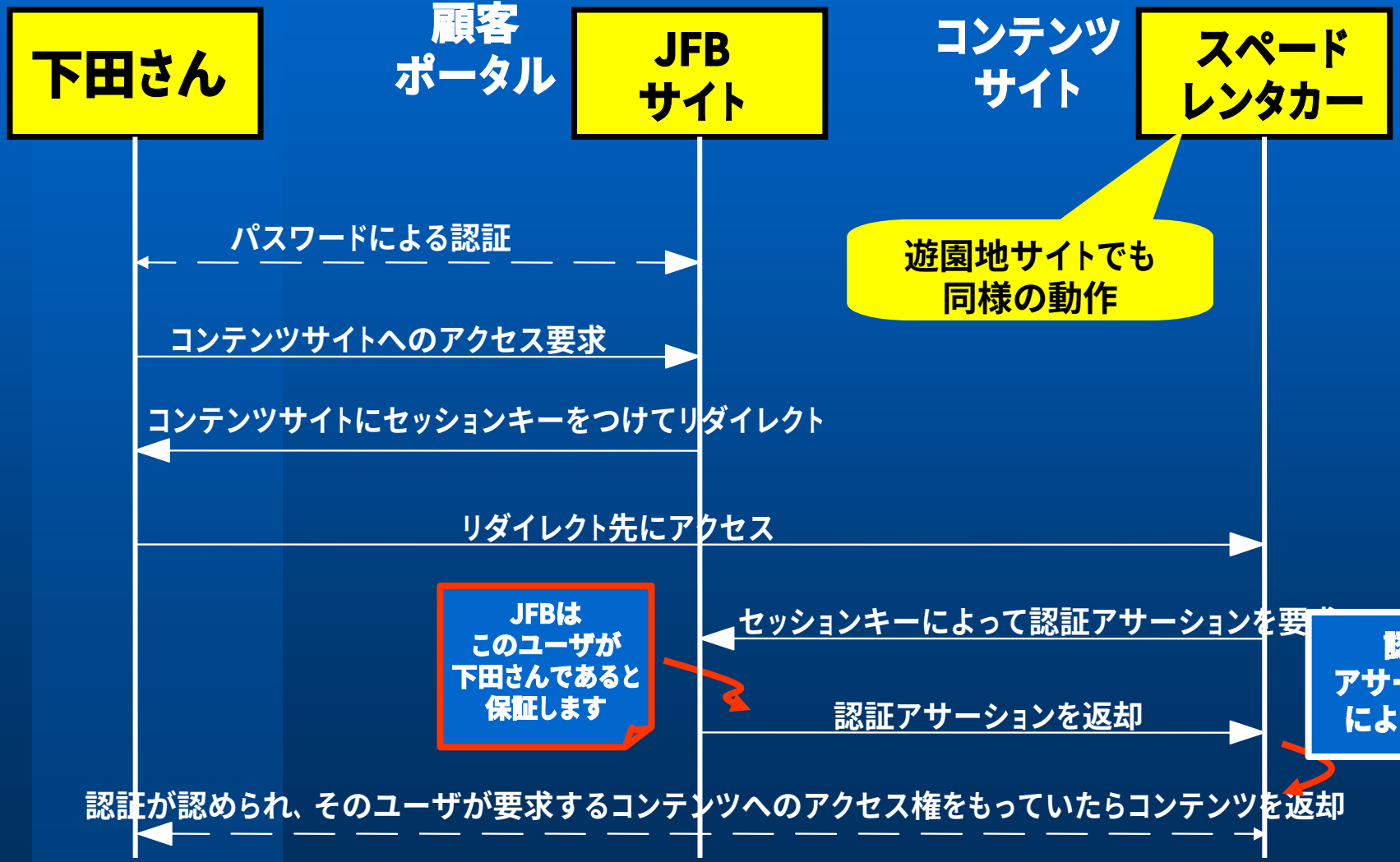
- JFB(旅行代理店サイト)における認証が、ドメインの異なる提携サイト(レンタカーサイト、遊園地サイト)で引き継がれる点 (Cookieを使わない)

- 提携サイトが、旅行代理店サイトで管理されているユーザ情報を利用し、ユーザ情報の補完やパーソナライゼーションを実現している点

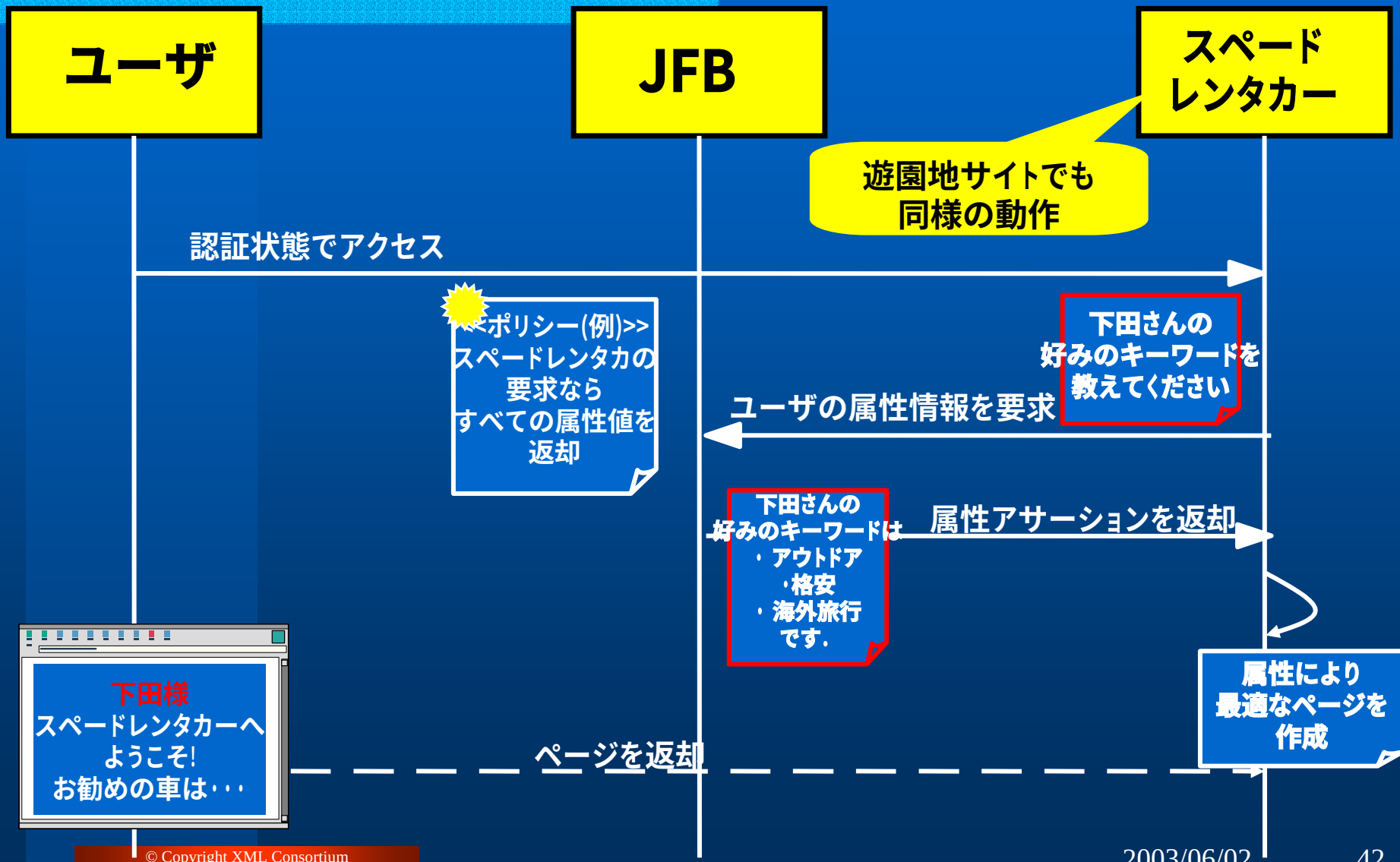
- 複数の旅行代理店サイトからの認証

- SAMLで動作!

デモでのデータフロー（認証）



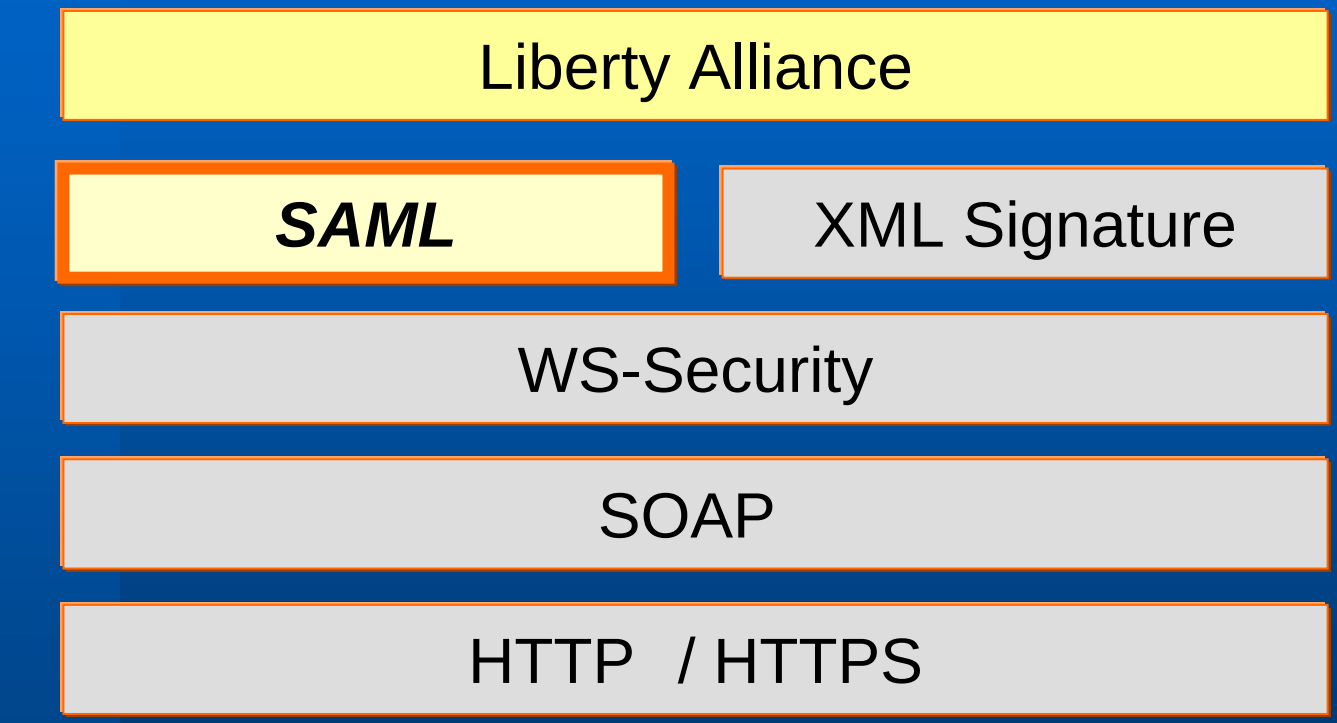
デモでのデータフロー (属性取得)



本日の報告内容

- セキュリティSWGにおける活動内容
- SAMLの概要
- デモの実装詳細
- デモンストレーション
- 関連仕様
  - Liberty Alliance Project

SAMLの位置づけ



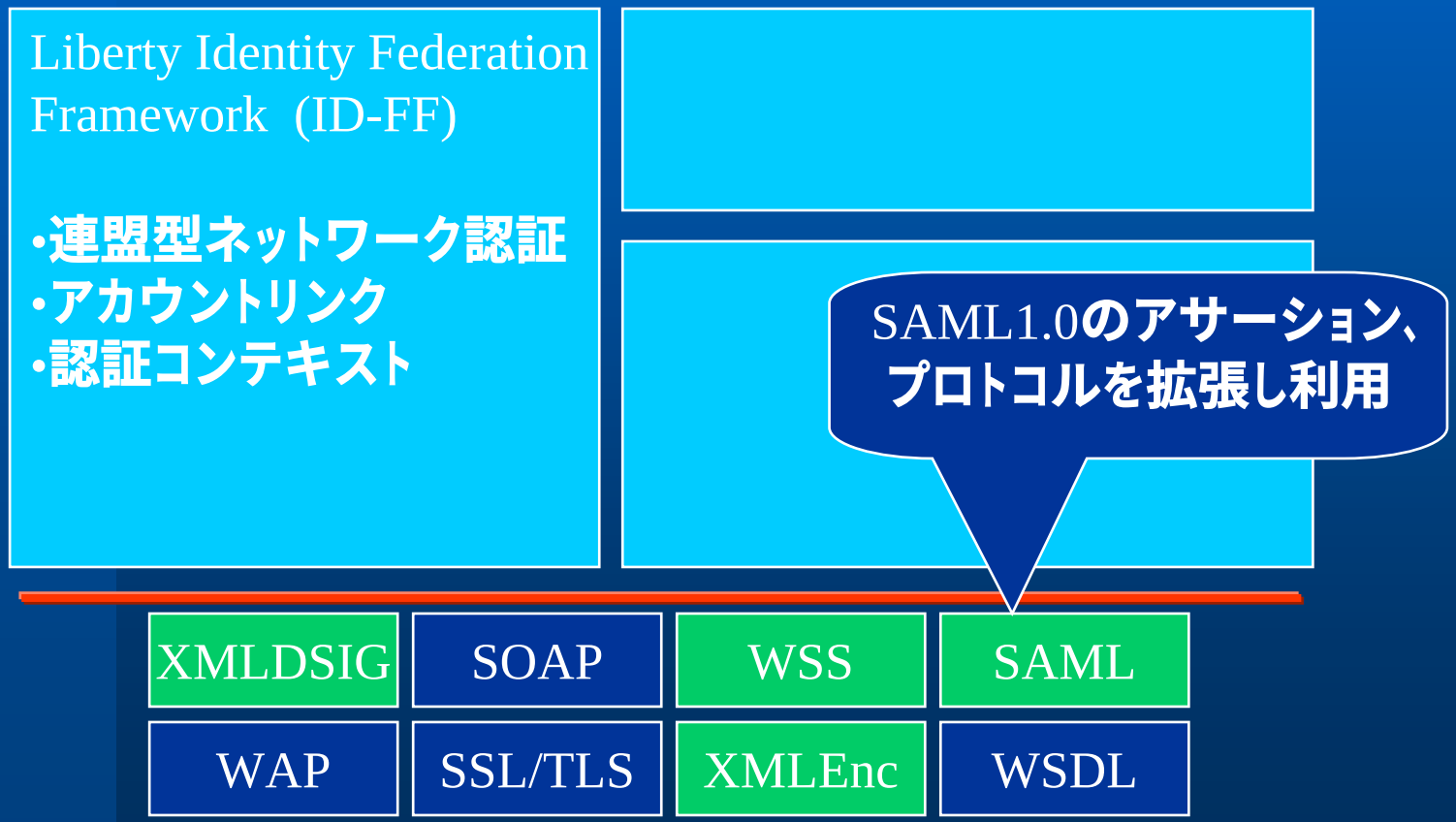
Liberty Alliance Project：ネットワーク上のアイデンティティ管理に関して、オープンな標準規格の策定を目的として設立された業界団体

Liberty Alliance Project

- ネットワーク上のアイデンティティ管理に関して、オープンな標準規格の策定を目的としてSun Microsystemsの主導により設立　(2001年10月)
- Cisco、VeriSign、ソニー、NTTドコモ、Bank of America、GM、United Airlinesなど各分野の企業現在約160社が参加
- 目的
  - シングルサインオン認証システムのためのオープンな標準規格
  - SAMLをベースに拡張し、協調型認証や管理機能などを備えたもの。
  - ユーザの了承のもとに複数のアカウントを「リンク」して“信頼の輪”を構築。　(Federated Network Identity)
  - 様々なデバイスや認証方式にも対応
    ID＋パスワード認証、IDカード、Java Card、指紋認証など

Liberty Spec. v1.0

- 2002/7/15「Liberty Alliance Version 1.0 Specification」公開



SAMLアサーションのLiberty拡張

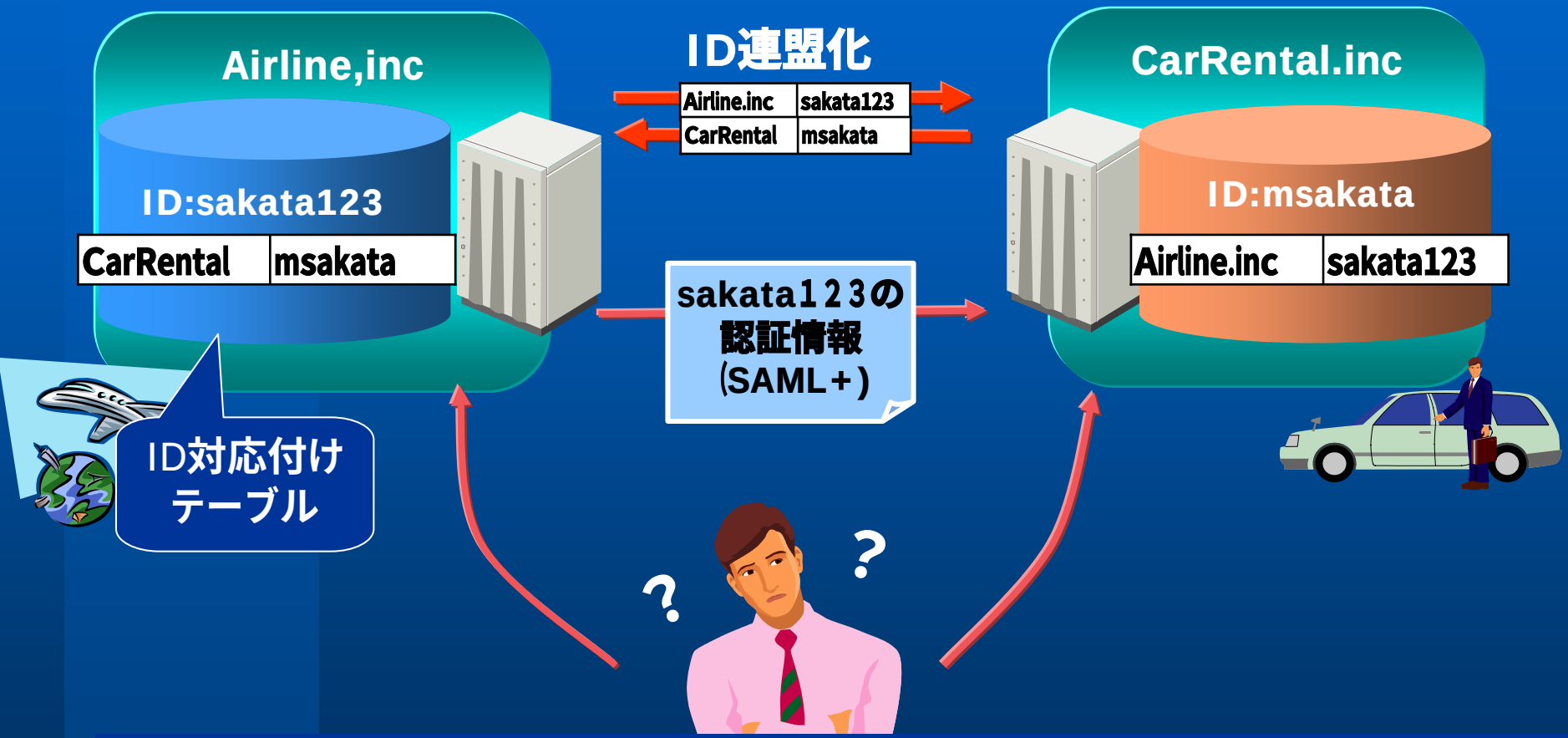
```
<saml:Assertion
 AssertionID="YdfOs8J0Xab“
 IssueInstant="2002-11-26T02:01:36Z“
 Issuer="http://www.kanturi.co.jp“
 ''' xsi:type="lib:AssertionType“
xmlns:lib=“http://projectliberty.org/schemas/core/2002/05”
>
<saml:AuthenticationStatement AuthenticationInstant="2002-
11-26T02:01:36Z"
xsi:type="lib:AuthenticationStatementType">
<saml:Subject xsi:type="lib:SubjectType">
<lib:IDPProvidedNameIdentifier>
   m0xk7wZQ2Sya4xe9tJGvarfN6R
</lib:IDPProvidedNameIdentifier>
<saml:NameIdentifier>
   Hnho/gm0xk7wZQ2Sya4xe9tJGvarfN6R
</saml:NameIdentifier>
</saml:Subject>
</saml:AuthenticationStatement>
</saml:Assertion>
```

Liberty拡張 AssertionTypeです。

Liberty拡張 認証Statement, Subjectです。

Liberty IDプロバイダ識別子は○○です。

Liberty Spec. v1.0



【使用イメージ】

- 選択可能なアカウント・リンク (Federation/Account Linking)
  → 異なるプロバイダにあるIDをユーザの同意の上でリンクする。

Liberty Phase 2 Draft Spec.

- 2002/7/15「Liberty Alliance Version 1.0 Specification」公開
- 2003/4/15「Liberty Alliance Phase 2 Draft Specifications」公開

Liberty Identity Federation Framework (ID-FF)
- *匿名アクセス*
- *アカウント暗号化*
- 連盟型ネットワーク認証
- アカウントリンク
- 認証コンテキスト

…

Liberty Identity Services Interface Specifications(ID-SIS)
- *IDパーソナルプロファイル*

Liberty Identity Web Service Framework(ID-WSF)
- *ディスカバリサービス*
- *サービステンプレート*
- *認証に基づく属性共有*

…

X

セキュリティ／プライバシ実装ガイドライン
「Privacy and Security Best Practices」

Liberty Phase 2 Draft Spec.

Airline,inc

③IDサービスアクセス

CarRental,inc

②ディスカバリサービスにより検索

④サービス

①サービスリクエスト

Discovery Service

IDサービスの記述、登録、検索等をID-WSFで定義

(Identity UDDI?)

ご清聴ありがとうございました

(参考) リンク

OASISのSAML標準化技術コミッティのWWWサイト
http://www.oasis-open.org/committees/security/

SAMLの仕様
SAML Assertions and Protocol
http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf
SAML Bindings and Profiles
http://www.oasis-open.org/committees/security/docs/cs-sstc-bindings-01.pdf

SAMLの日本語解説
「SAML技術解説」SAML技術解説，XMLコンソーシアム 技術解説書
http://www.xmlconsortium.org/websv/kaisetsu/C10/content.html
@IT
【連載】Webサービスのセキュリティ
第4回 強力なSSOを実現するXML認証・認可サービス（SAML）
http://www.atmarkit.co.jp/fsecurity/rensai/webserv04/webserv01.html

Liberty Alliance
http://www.projectliberty.org/
OpenSAML
http://www.opensaml.org/
TSIK(Trust Service Integration Kit)
http://www.xmltrustcenter.org/developer/verisign/tsik/index.htm

その他

- Windowsは，米国およびその他の国における米国Microsoft Corp.の登録商標です。
- Java 及びすべてのJava関連の商標及びロゴは，米国及びその他の国における米国Sun Microsystems,Inc.の商標または登録商標です。
- BSDは，米国Berkeley Software Design, Inc.の商品名称です。
- Apache Tomcat、Apache HTTP Serverの著作権はthe Apache Software Foundationに帰属します。
- BEA WebLogic ServerはBEA Systems, Inc.の商標または登録商標です。
- その他、記載されている会社名、製品名は各社の登録商標または商標です。