SAMLの基本技術・実装技術

2004年12月9日

日本電気株式会社

遠藤　由紀子

⟨**y-endo@ah.jp.nec.com**⟩

Empowered by Innovation NEC

目次

1. 背景と動向
   - 背景
   - 動向
2. **SAML**とは
   - **SAML**の概要
   - **SAML**の概念モデル
   - シングルサインオンモデル
3. **SAML**の仕様
   - **SAML**アサーション
   - ⑴付録⑵ ブラウザ**SSO**プロファイル
   - ⑴付録⑵ **SAML**プロトコル
4. **Liberty Alliance**
   - **Liberty** の概要
   - **Liberty ID-FF1.2**
5. システム構築
   - システム構築にあたって
   - システム構成例
6. おわりに

背景と動向

背景

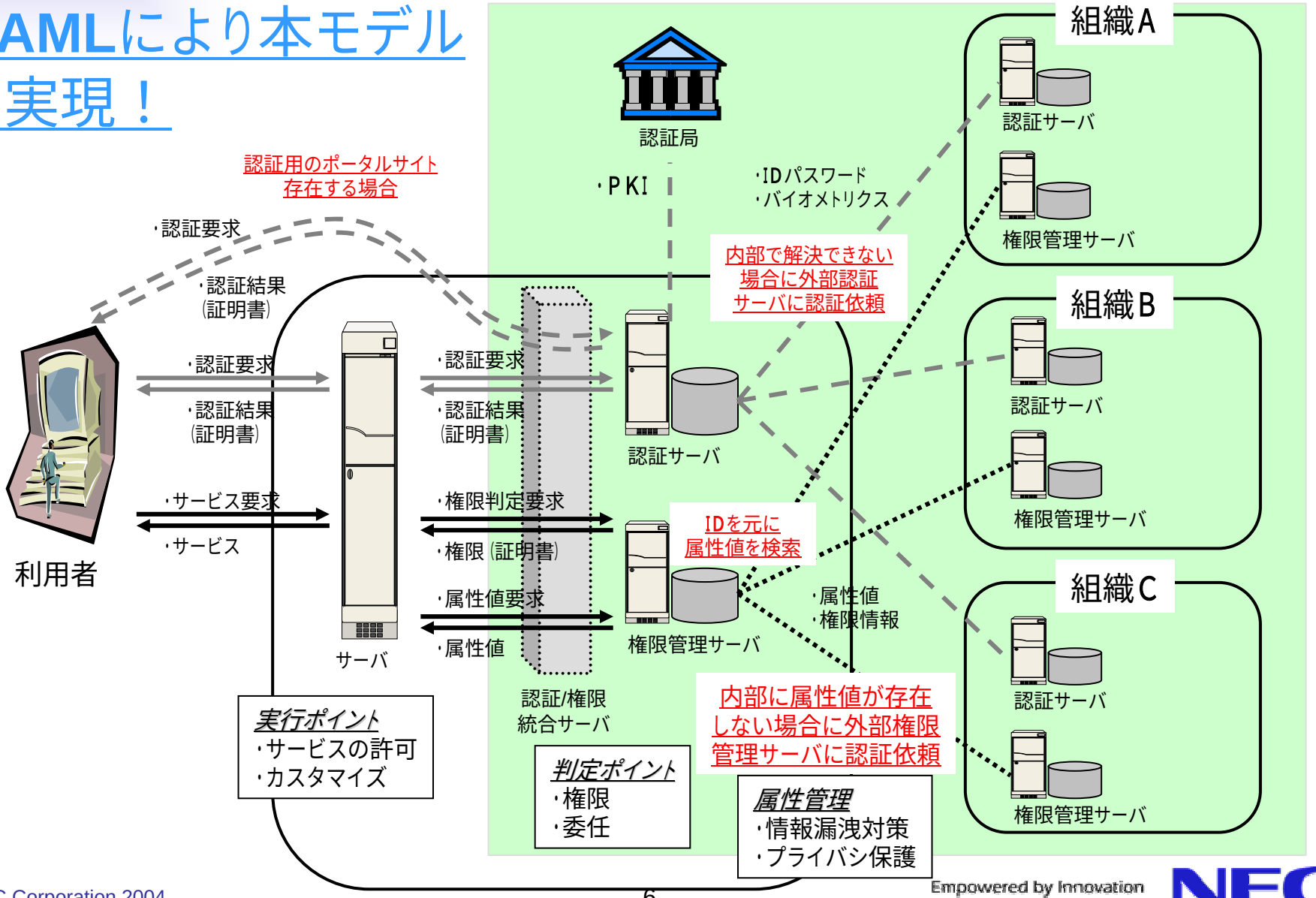
- サービスプロバイダのセキュリティ対策の負担が増加
  - インターネット上のセキュリティ要求レベルが高くなり、本業システム以外でのシステム構築の負担が増加
- ユーザの認証/属性/権限の処理において**PKI**の利用が進んでいない
  - **ID**/パスワードは今も一般的
  - バイオメトリクスへの注目が高まっている
  - 属性証明書が普及していない
- いくつかのサービスにおいてユーザの動的な属性情報を必要とする
  - プレゼンスサービス
  - 位置情報サービス

動向

- 認証/属性/認可の処理をアウトソーシング
  - サービスプロバイダが本業のサービス構築に注力することで、ユーザによりよいサービス提供を可能に
- 認証レベルに応じた認証方式の選択および認証ポリシの統一化
  - **PKI**
  - バイオメトリクス
  - **ID**/パスワード
  - それぞれの組み合わせ
- 信頼できる動的な属性情報の入手を可能に
  - 動的な属性情報を基にした権限情報を生成

認証基盤イメージ

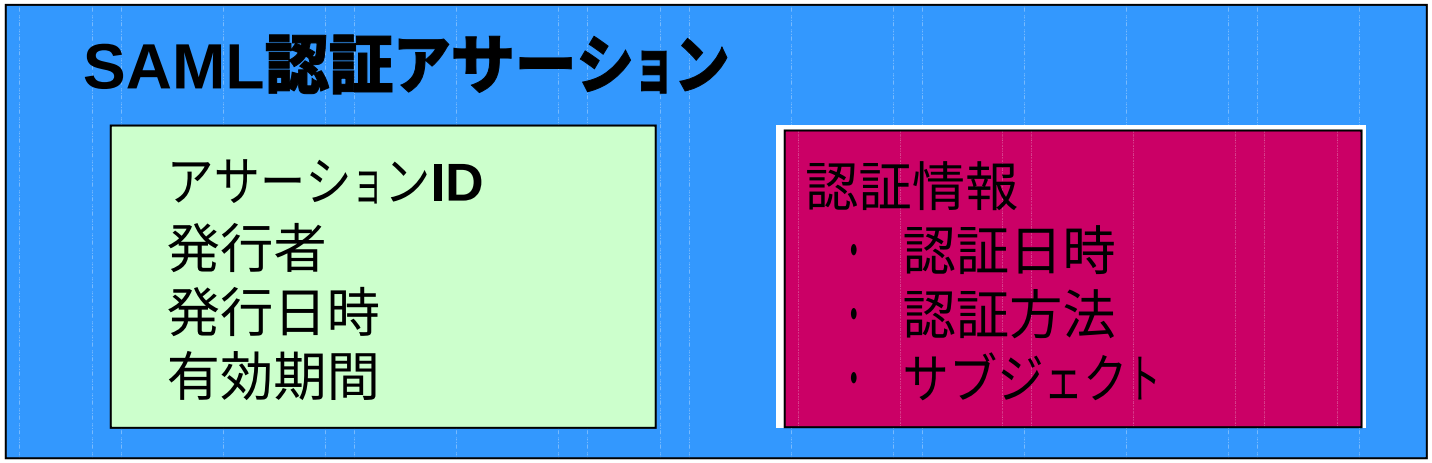
SAMLにより本モデルを実現！



SAMLとは

SAML （Security Assertion Markup Language）

- **XML**を基盤としたセキュリティ情報交換のための標準仕様
  - セキュリティ情報をサブジェクト(人、機器など)に対するアサーションという形態で表現
    - 認証・属性・認可情報を**XML**で記述
  - メッセージの書式の他、プロトコル、プロトコルバインディング、プロファイル、…**etc**を規定



SAMLの特徴

- **XML**

  ⇒ **XML**を用いたセキュリティ標準との高い親和性

  （**XML**署名、**XML**暗号、**XACML** … **etc**）、

  Webサービスへの適用

- 標準仕様

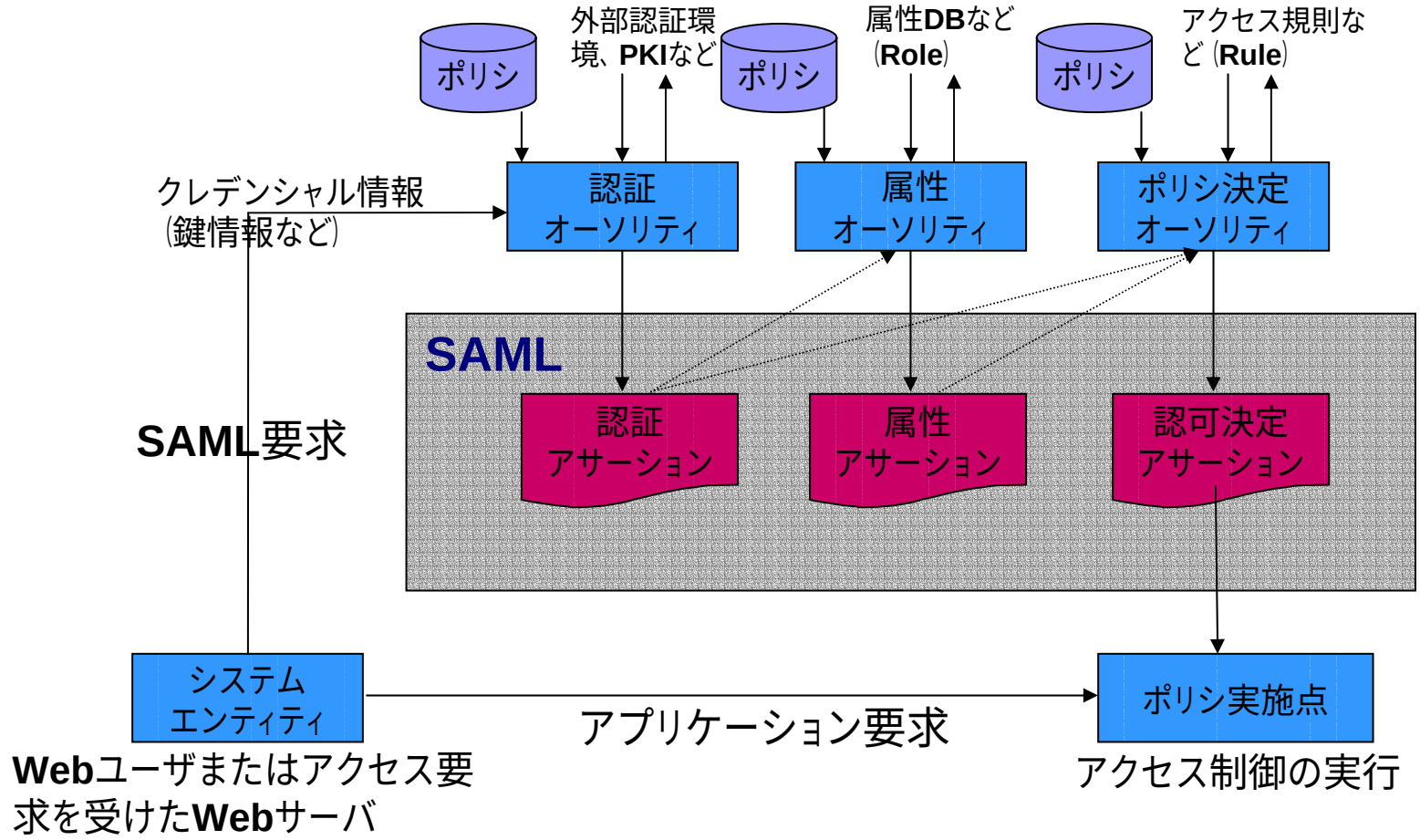
  ⇒ 高い相互運用性

- **SAML**を利用して、**SSO**（シングルサインオン）を実現
- 幅広い認証方式（**ID/PW**、**PKI**、**Kerberos**、 … **etc**）をサポート

（参考**URL**: **http://www.oasis-open.org/committees/security/**）

SAML概念モデル

- 3種類のSAMLオーソリティ*がアサーションを発行してアクセス制御を行う



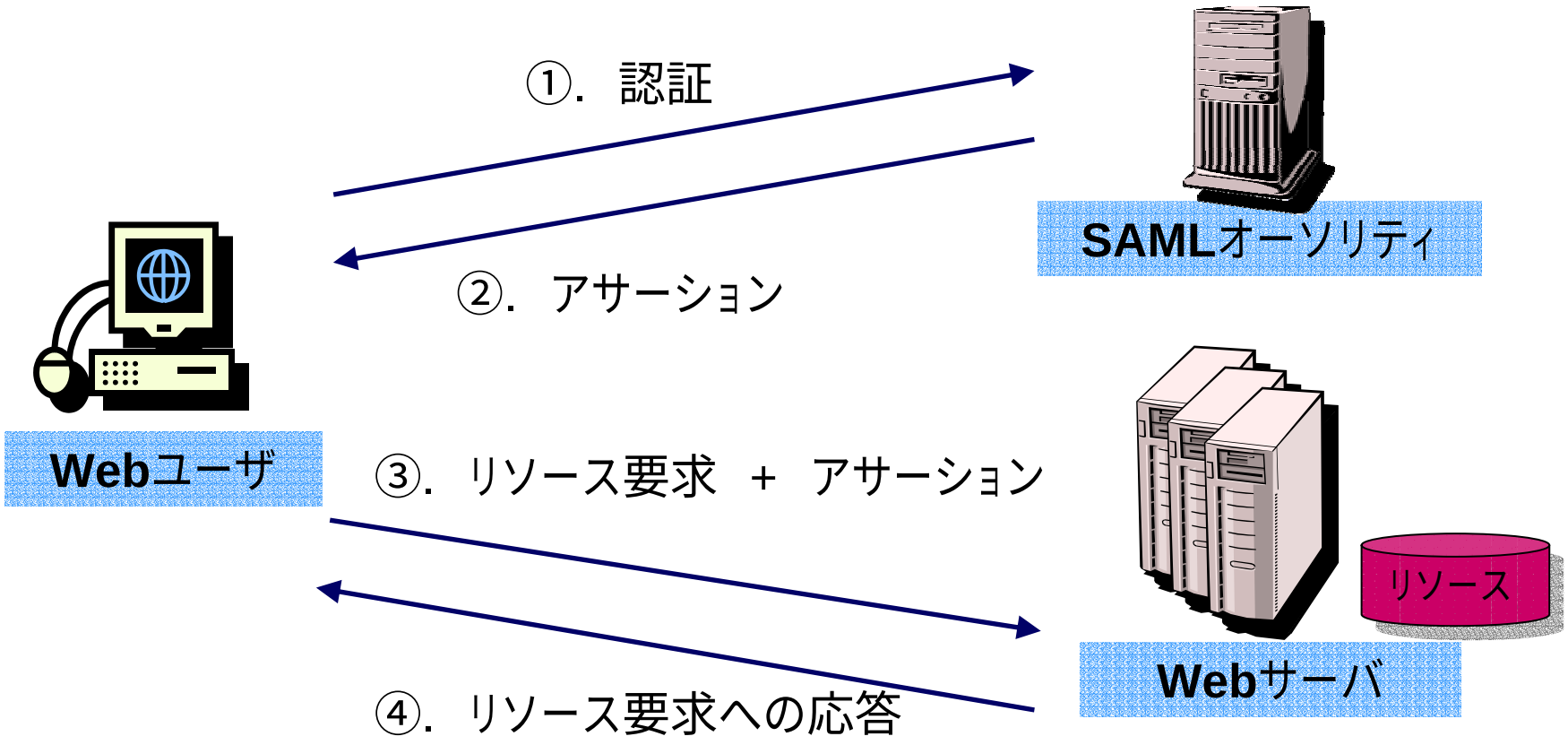
*SAMLオーソリティ ： 自らが正当性を証明するアサーションを発行するエンティティ

SAMLを用いるメリット

- **SSO** (シングルサインオン)
  - 一度認証すると、再認証の必要がない
  - **Web**ブラウザベースの**2**つの方式をサポート
  - **SAML**という標準仕様により相互接続性が向上
- ID管理
  - **ID**統合：**ID**の一元化 (組織内)
    - 重複した**ID**管理のコストを削減
    - 情報漏えいのリスク削減
  - **ID**連携：緩やかな**ID**の統合 (組織間)
    - 別々に管理されている**ID**に関連を持たせる
- 認証機構のアウトソーシング
  - **ID/PW**や**PKI**などの認証機構をアウトソーシング
  - セキュリティポリシを統一した認証が可能になる

シングルサインオンモデル1

- 認証情報をフォームPOSTの形でWebサイトへ転送

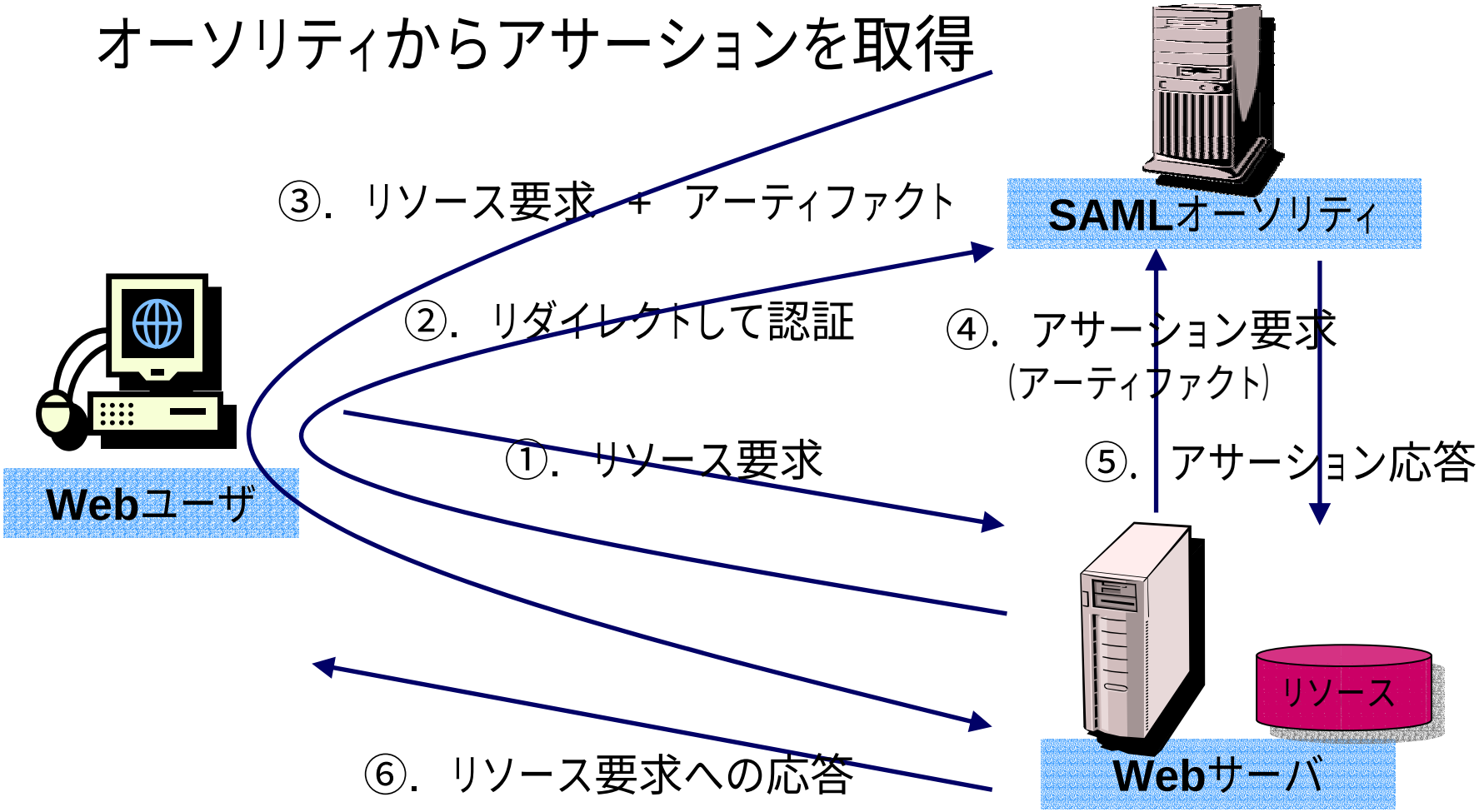


シングルサインオンモデル１の特徴

- メリット
  - アサーションを自在に提出することができる
  - 処理フローがシンプル
- デメリット
  - ブラウザのプラグインを作りこむ、もしくはクライアントのアプリケーションを作りこむ必要がある

シングルサインオンモデル2

- ブラウザが**URL**のクエリの後ろに付加されたアーティファクト文字列を運び、**Web**サーバは**SAML**オーソリティからアサーションを取得



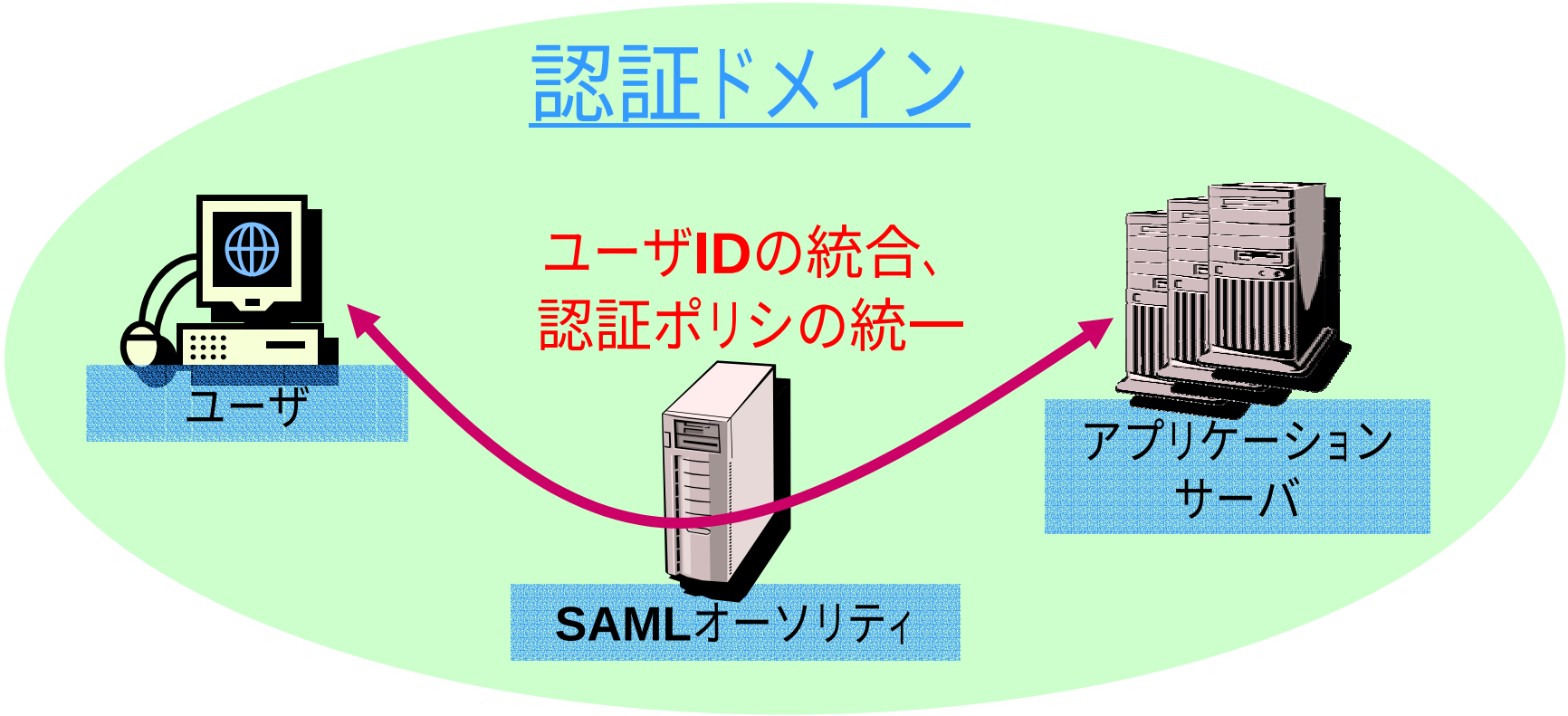
シングルサインオンモデル2の特徴

- メリット
  - アーティファクトの仕組みを使っているため、一般的なブラウザがあれば実現可能
  - **Web**ユーザにはプラグインや専用アプリケーションを用意する必要がない
- デメリット
  - **Web**サーバと**SAML**オーソリティ間のやり取りが必要

※ブラウザを用いるため、ユーザの観点からモデル2によるシステム構築が一般的

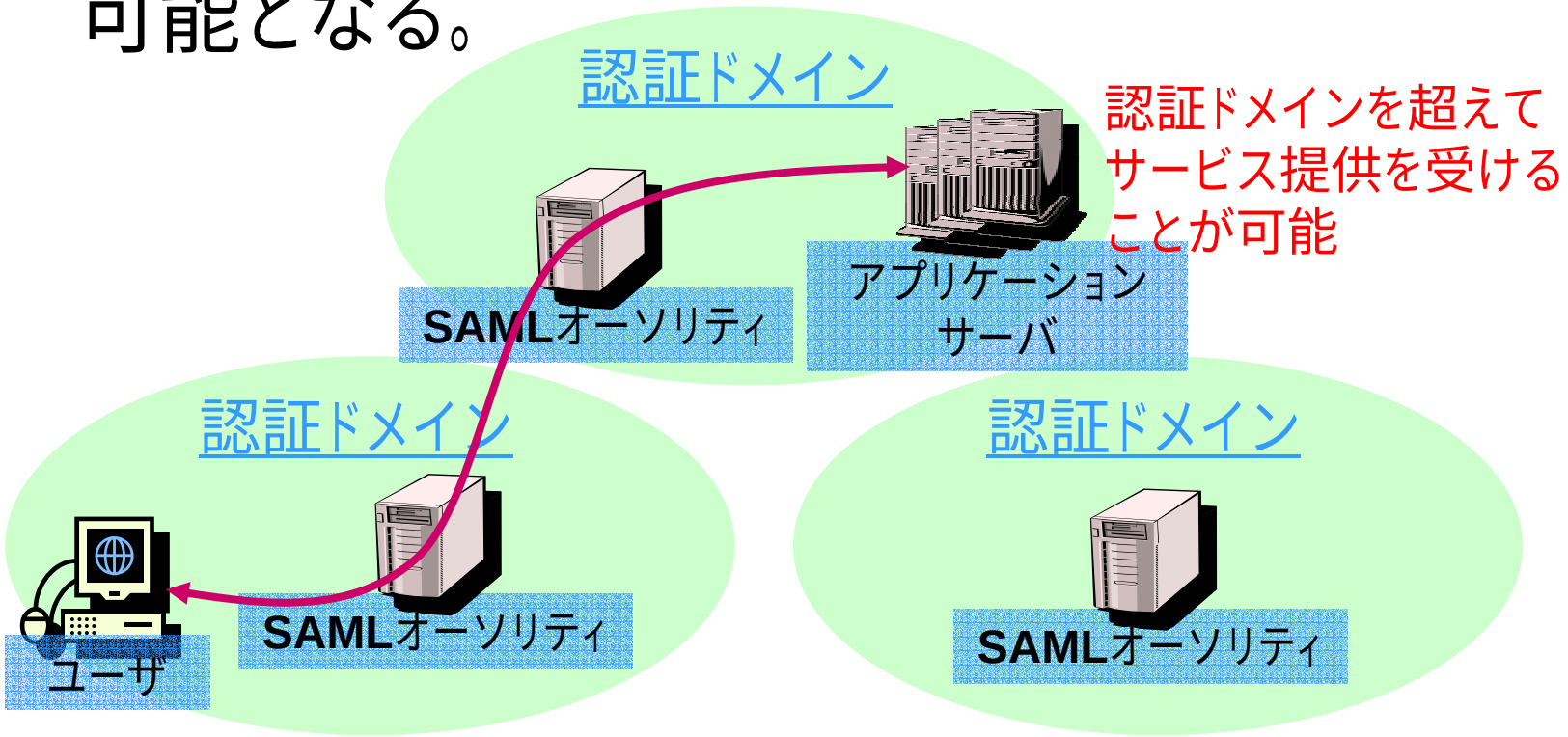
ID統合

- 認証ドメイン内において、**SAML**オーソリティが認証することにより、ユーザ**ID**の統合や、認証ポリシの統一化が可能となる。



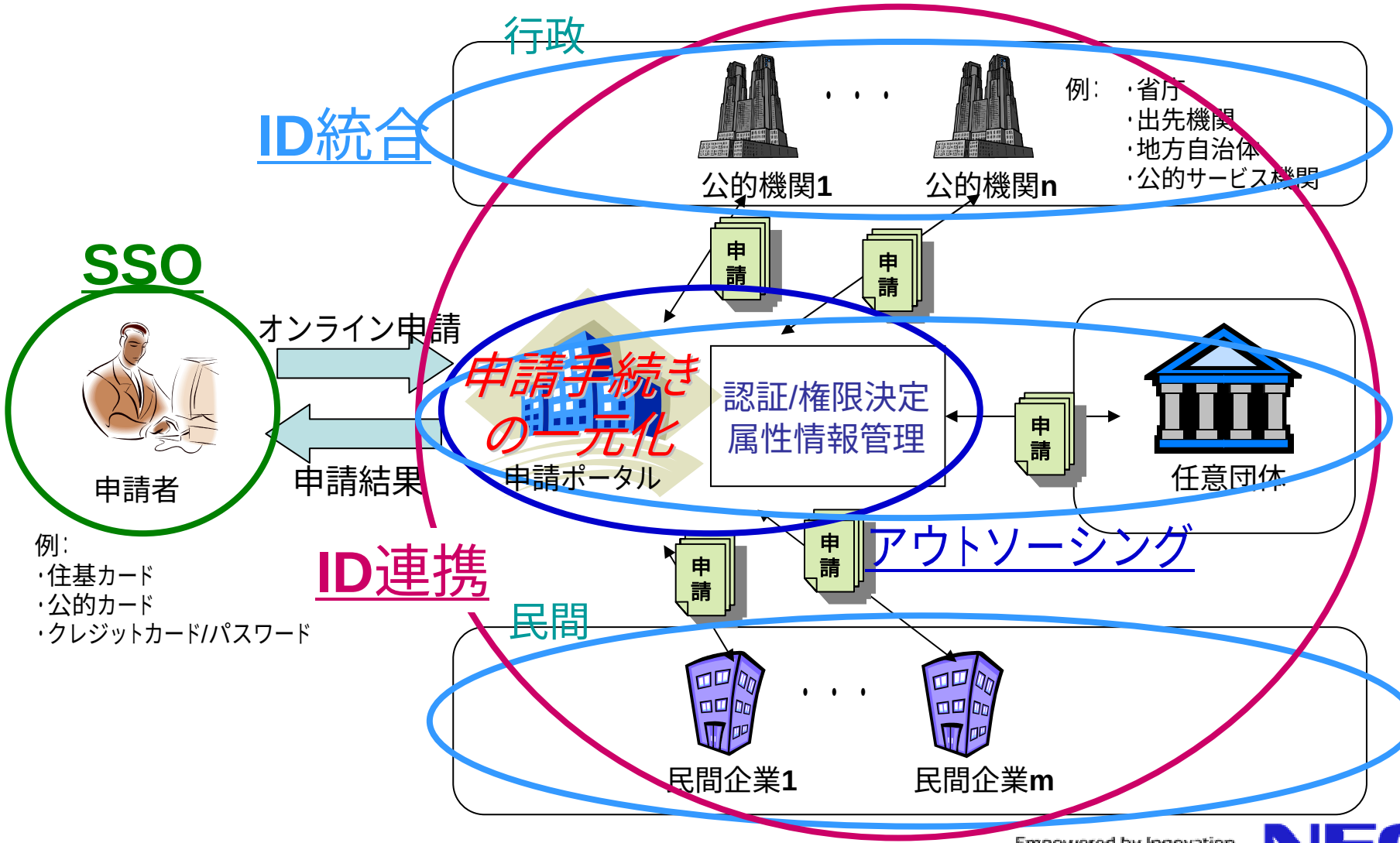
ID連携

- 認証ドメイン間において、信頼関係を確立することで、ユーザは認証ドメインを超えてアプリケーションサーバからサービスを受けることが可能となる。



ワンストップサービスによる例

ワンストップサービスは関連する申請手続きを一元化することにより、
申請手続きの効率化を図る

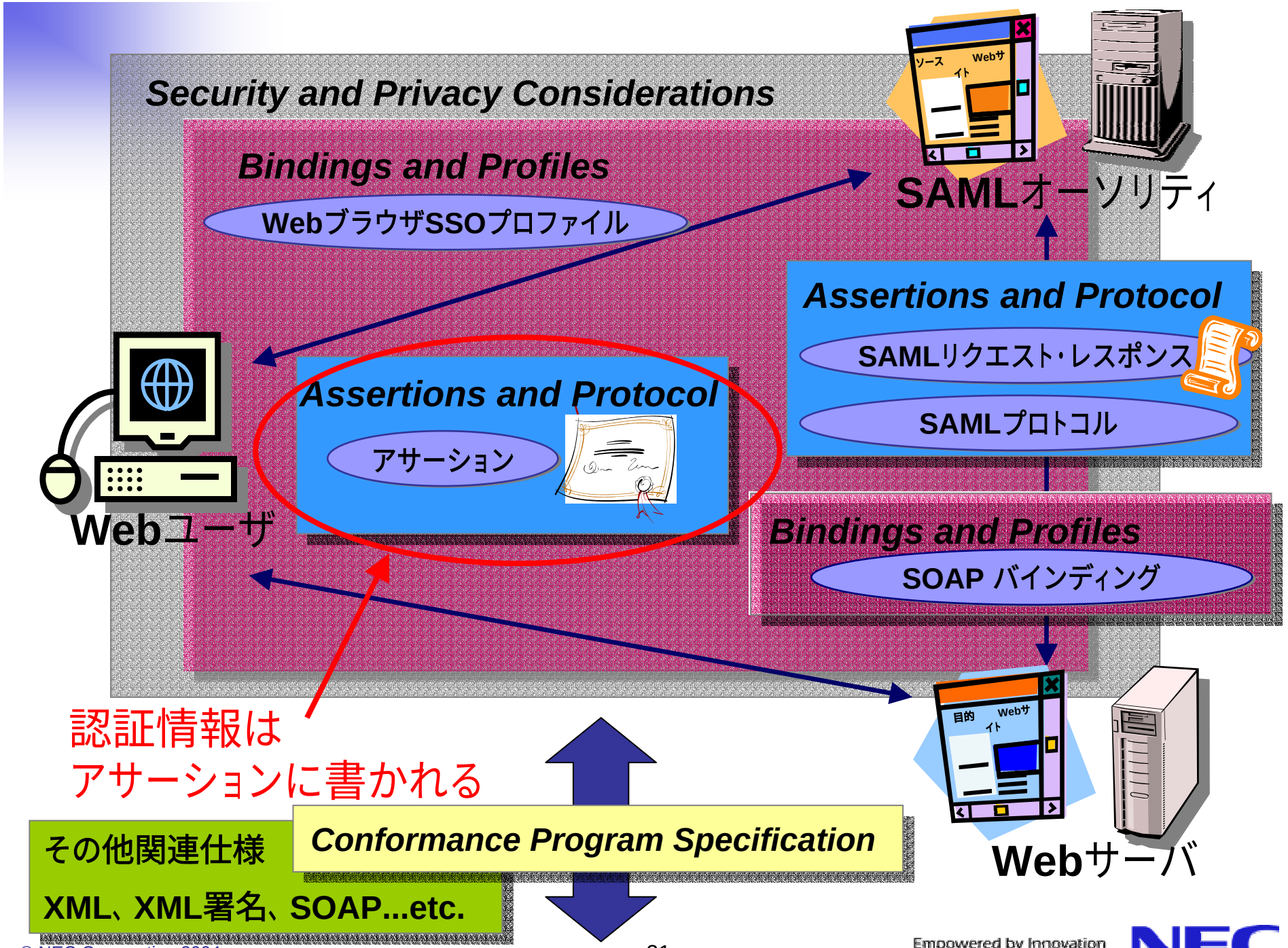


ＳＡＭＬの仕様

SAML仕様書

SAMLのコアはアサーション

仕様名	内容
Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1	アサーションとプロトコルのデータフォーマット
Binding and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1	**SOAP**バインディングの規定とブラウザプロファイルの規定
Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML) V1.1	相互運用性を確保するための適合性要件のまとめ
Glossary for the OASIS Security Assertion Markup Language (SAML) V1.1	用語集
Assertion Schema	アサーションの**XML**スキーマの規定
Protocol Schema	プロトコルの**XML**スキーマの規定
Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V1.1	セキュリティ、プライバシ要件の考察



SAMLアサーション

- **SAML**アサーションとは**SAML**オーソリティが作成するセキュリティ情報のパッケージ
- **SAML**仕様では**3**種類のアサーションを規定
  - 認証アサーション (**SSO**アサーション)
    - サブジェクトが特定の時間に特定の手段によって認証済であることを示す
  - 属性アサーション
    - サブジェクトの属性を示す
  - 認可決定アサーション
    - サブジェクトが特定のリソースに対してアクセスを許可されているかどうかを示す

SAMLアサーションの例（認証アサーション）

```
<saml:Assertion
 MajorVersion="1"
 MinorVersion="1"
 AssertionID="b75gts68-35f8-92gs-15gs-sfe3538aergd"
 Issuer="AuthServer.nec.co.jp"
 IssueInstant="2004-10-20T08:20:02Z"
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Conditions
   NotBefore="2004-10-20T08:20:02Z"
   NotOnOrAfter="2004-10-20T08:30:02Z">
    <saml:AudienceRestrictionCondition>
      < saml:Audience>http://www.aaa.nec.co.jp </saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AuthenticationStatement
   AuthenticationInstant="2004-10-20T08:20:02Z"
   AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
        y-endo@ah.jp.nec.com
      </saml:NameIdentifier>
    </saml:Subject>
  </saml:AuthenticationStatement>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#”>
   ・・・
  </ds:Signature>
</saml:Assertion>
```

アサーションのバージョン

アサーションの識別ID

アサーションの発行者と発行時間の指定

条件の指定

有効期間の指定

アサーションを利用する
Webサーバの指定

認証ステートメント

認証した時間

認証方法（パスワード、**Kerberos**、**SRP**、**IC**カード、**SSL/TLS**クライアント認証、**X.509**公開鍵、未定義、**etc**.）

サブジェクトの指定　（未定義、電子メールアドレス、**X509SubjectName**、**Windows**ドメイン限定名）。**SubjectConfirmation**の**ConfirmationMethod**を指定することも可能

XML署名(任意)

SAMLアサーションの例（属性アサーション）

```
<saml:Assertion
 MajorVersion="1"
 MinorVersion="1"
 AssertionID="a3254sit-65tg-gt58-hu36-5sg2sf6sgt0h"
 Issuer="AuthServer.nec.co.jp"
 IssueInstant="2004-10-20T08:40:02Z"
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Conditions
  ・・・
  </saml:Conditions>
  <saml:AttributeStatement >
   <saml:Subject>
    <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
      aaa@bbb.jp.nec.com
    </saml:NameIdentifier>
   </saml:Subject>
   <saml:Attribute   AttributeName="NEC役職"   AttributeNameSpace="http://nec.co.jp">
     <saml:AttributeValue>
      課長
     </saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
   ・・・
  </ds:Signature>
</saml:Assertion>
```

アサーションのバージョン

アサーションの識別ID

アサーションの発行者と発行時間の指定

条件の指定

属性ステートメント

サブジェクトの指定

属性の記述

XML署名(任意)

SAMLアサーションの例（認可決定アサーション）

```
<saml:Assertion
 MajorVersion="1"
 MinorVersion="1"
 AssertionID="ckj59d32-jh83-62vl-l58s-32llksn652ok"
 Issuer="AuthServer.nec.co.jp"
 IssueInstant="2004-10-20T08:50:02Z"
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Conditions
  …
  </saml:Conditions>
  <saml:AuthorizationDecisionStatement  Resource="http://foo.com/foo.txt"  Decision="Permit" >
   <saml:Subject>
    <saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:email
      aaa@bbb.jp.nec.com
    </saml:NameIdentifier>
   </saml:Subject>
   <saml:Action  Namespace="urn:oasis:names:tc:SAML:1.0:action:rwedc">
    Read Write
   </saml:Action>
   <saml:Evidence>
    <saml:AssertionIDReference>
     b75gts68-35f8-92gs-15gs-sfe3538aergd
    </saml:AssertionIDReference>
   </saml:Evidence>
  </saml:AuthorizationDecisionStatement>
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#”>
  …
  </ds:Signature>
</saml:Assertion>
```

アサーションのバージョン

アサーションの識別ID

アサーションの発行者と発行時間の指定

条件の指定

認可決定ステートメント

対象リソースへのアクセス認可の可否（Permit、Deny、Indeterminate）

サブジェクトの指定

行動の指定

認可決定の根拠となったアサーション

XML署名(任意)

アサーションの利用の現状

- 認証オーソリティの実用化
- 属性オーソリティの検討
  - 属性の整理
    - 固定的な属性
    - 動的な属性
- ポリシ決定オーソリティ
  - **XACML**
    - アクセスコントロール

Liberty Alliance Project

Empowered by Innovation NEC

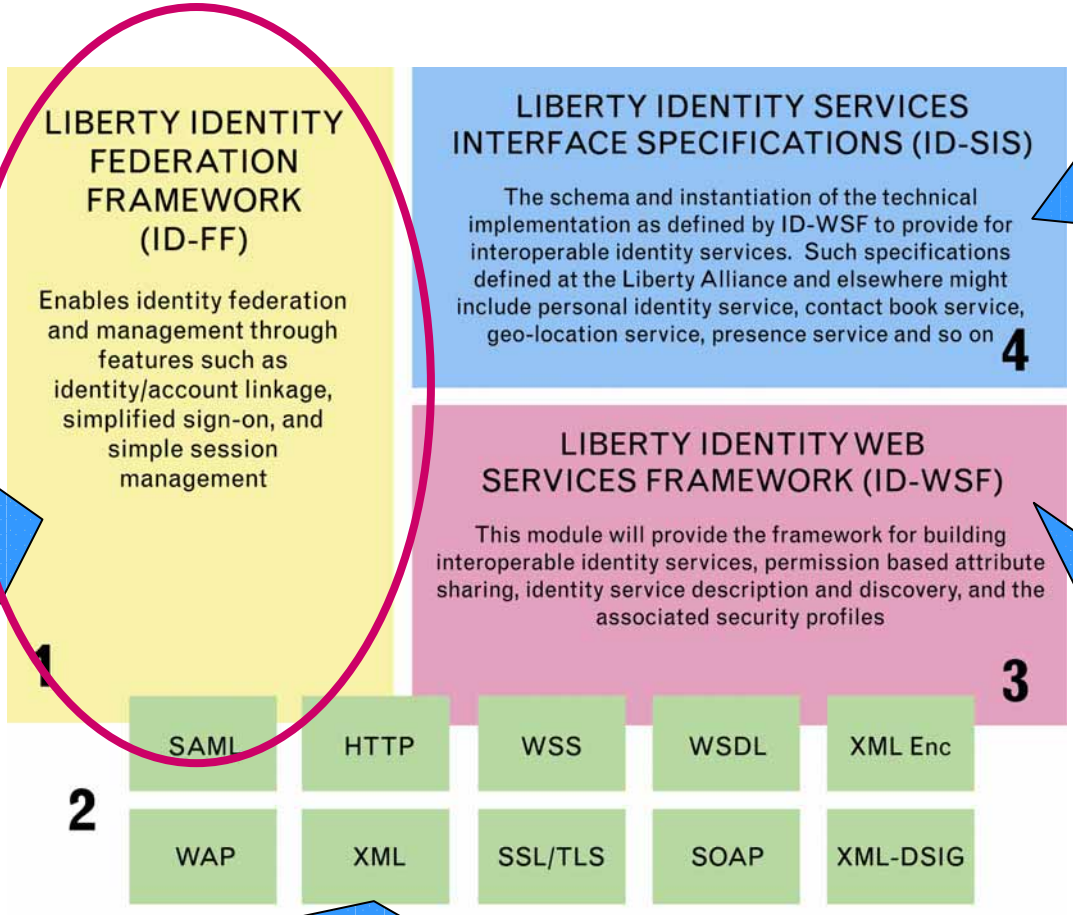
Liberty Alliance Projectとは

- インターネット上においてシングルサインオンのサービスの提供を目的に活動
  - 世界中の**160**以上の企業･政府機関等から構成
  - ビジネス部会と技術部会の連携
  - 仕様化活動
  - 相互接続の認定試験
  - **Liberty**仕様の普及活動

（参考**URL: http://www.projectliberty.org**）

Libertyの活動領域

IDとIDを結びつけるための認証連携技術
- **SAML**をベースにして、**SSO**のための**Assertion**のやりとりを規定
- 連携の登録/停止、サインオン/オフの方法を規定
- ブラウザからの**POST/GET**などのプロファイルを規定
- **IDP**間で**ID**を連携させる方法は含まれない



個人情報に関わる基本サービス群
- 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、カレンダー、財布、アドレス帳などを検討

個人情報交換のためのWebサービス基盤
- 個人情報の登録と検索の仕様
- 個人情報を管理するサーバのディレクトリの仕様

参照する他の標準
- **SAML**の拡張として、**ID-FF**を規定し、**ID-FF**の成果を**SAML**に提供
- **HTTP**のリダイレクト、クッキーを用いた実装のガイドライン
- **SSL/TLS** を用いた情報の隠蔽

Libertyの仕様について

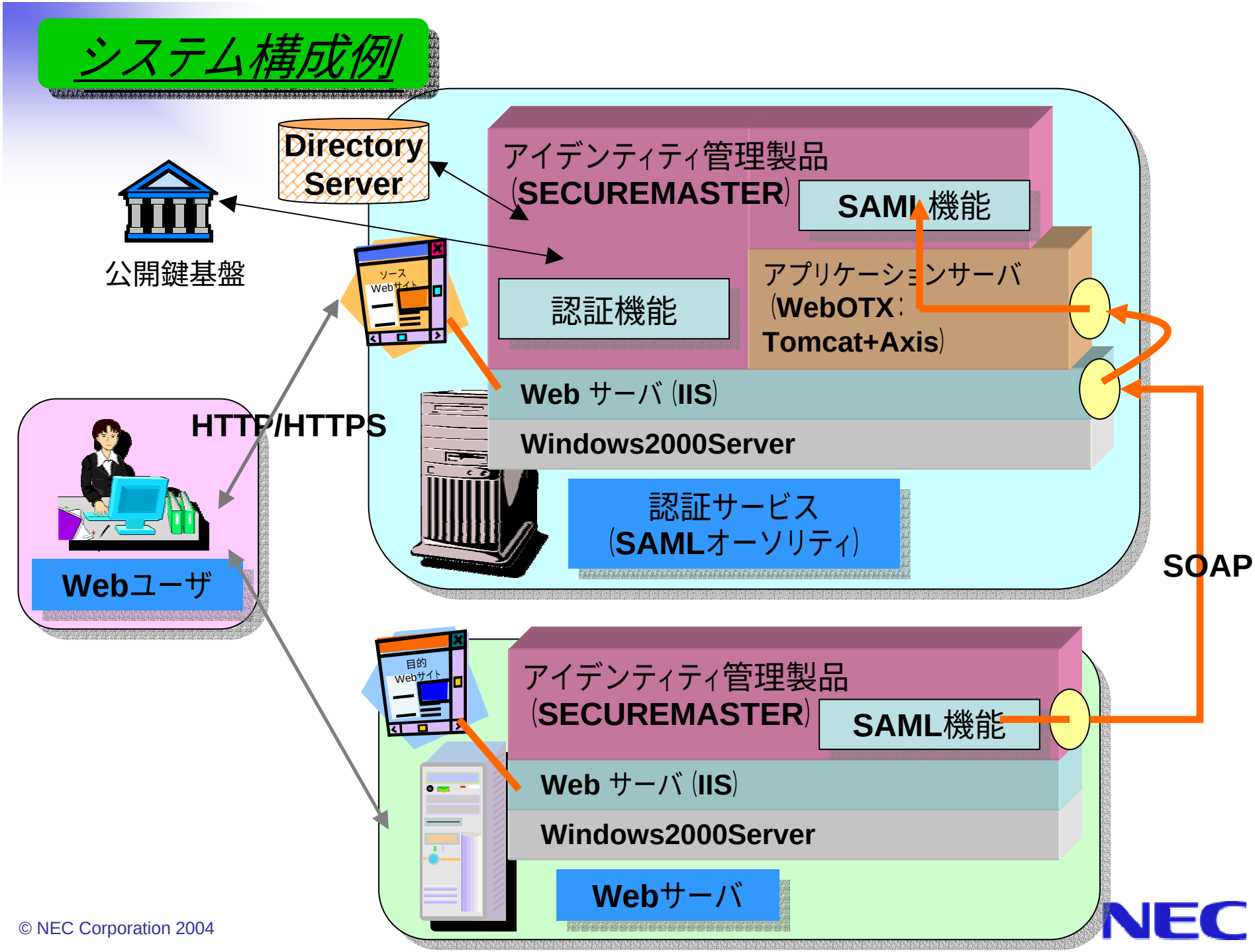
- **Liberty ID-FF1.2の機能**
  - **SAML**をベースに**SSO**機能を強化
    - **Identity Provider Introduction**
      - ユーザがどの**IdP**（**SAML**オーソリティ）を利用しているのかを検索する
    - シングルログアウト
      - 1度のログアウトで、シングルサインアウト可能
  - アイデンティティ連携
    - **ID**の連携
      - 異なる**ID**をマッピングして緩やかなID統合を実現
      - **Name Identifier Mapping**
    - 連携解除
  - 認証コンテクスト
    - **SP**（**Web**サーバ）が**IdP**（**SAML**オーソリティ）に自らのセキュリティポリシを提示
  - メタデータ
    - **SP**（**Web**サーバ）、**IdP**（**SAML**オーソリティ）間で事前に交換するポリシ情報の記述方式

システム構築

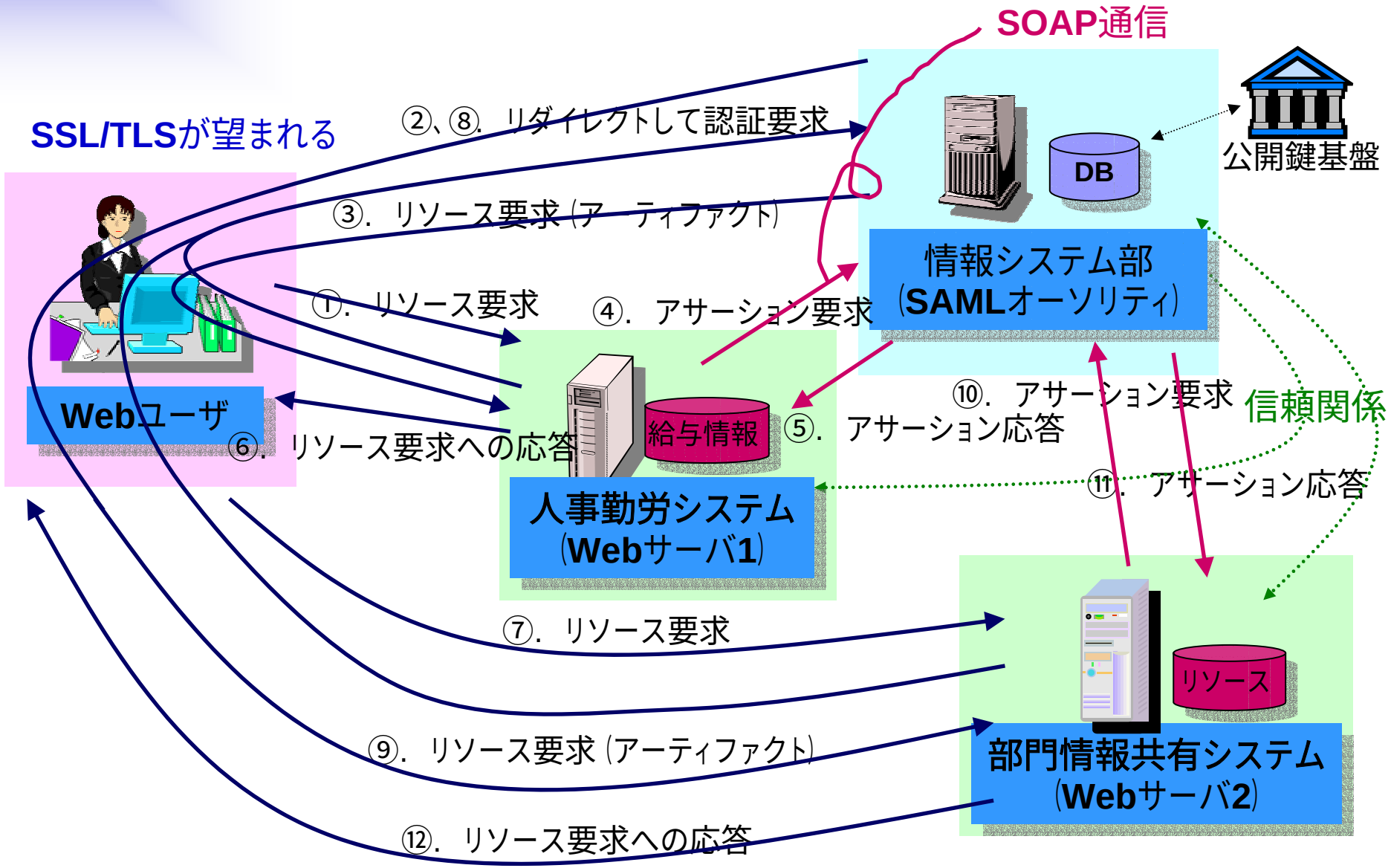
システム構築にあたって

- **SAML**を利用して、**SSO**システムを実現する際にサービス事業者と**SIer**で決めること
  - **Web**ブラウザ**SSO**プロファイルの選定
    - プロファイル：アーティファクトプロファイル、**POST**プロファイル
  - アサーションの設計
    - 認証方式： **ID/PW**、**PKI**、**IC**カード、バイオメトリクス・・・
    - 有効期限：（例）数分～1日程度 5分
    - **Subject**：（例）電子メールアドレス、社員番号
    - 含めたい情報は何かあるか？：（例）役職、部署名
  - セキュリティに関する項目
    - **SSL/TLS**、**IPSec**（ネットワークセキュリティ）
    - **XML**署名、**XML**暗号（メッセージセキュリティ）

システム構成例



社内システムSSOフロー



おわりに

- 本日のまとめ
  - 認証処理部分のアウトソーシング
  - 複数の認証方式の利用
  - **SAML**の利用
    - **SAML**のコアはアサーション
    - シングルサインオン、**ID**統合、**ID**連携
  - **SAML**のシステム構築例
    - 社内システム間のシングルサインオン
  - **Liberty Alliance Project**のご紹介
    - **Liberty**は**SAML**をベースにしたアーキテクチャを仕様化
  - **SAML2.0**、**e-Authentication**に注目
    - 認証基盤技術としてキャッチアップしていく必要あり

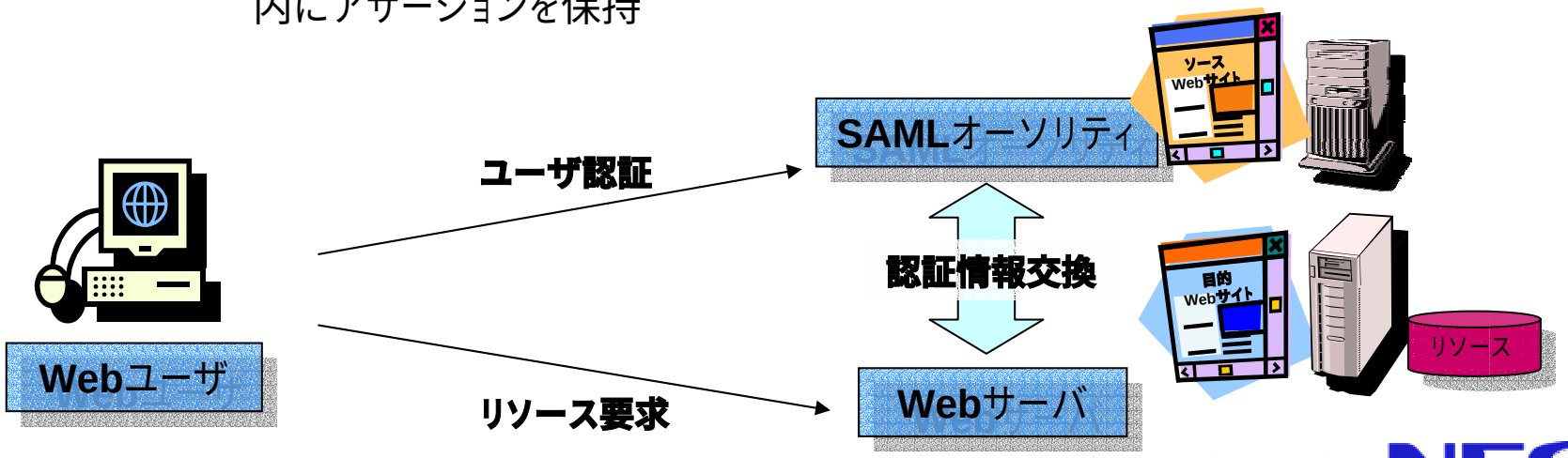
付録

SAML標準化動向とLibertyAllianceProject

- **2000 / 11 : OASIS SSTC結成**
  - **Security Services Technical Committee(SSTC)**を結成。インタネット上のセキュリティ情報の交換とサービスのための**XML**標準の開発開始
- **2001 / 01 : S2ML**と**AuthXML**の統合を決定
  - **OASIS**は**AuthXML**の提案を受け入れ、**S2ML**に統合し、仕様策定を行うことに(この時期に仕様の名称を**SAML**とすることに決定)
- **2001 / 09 : Liberty Alliance Project発足**
- **2002 / 07：フェーズ1 ID-FF1.0 発表**
- **2002 / 11：SAML V1.0 仕様化**
- **2003 / 01：ID-FF1.1 updated 発表**
- **2003 / 04 : SAML 2.0の検討のために、フェーズ1仕様をOASISに提供**
- **2003 / 09：SAML V1.1仕様化**
- **2003 / 11：フェーズ2 ID-FF1.2 、ID-WSF1.0発表**
- **2004 / 10：SAML V2.0 Committee Drafts仕様レビュー**

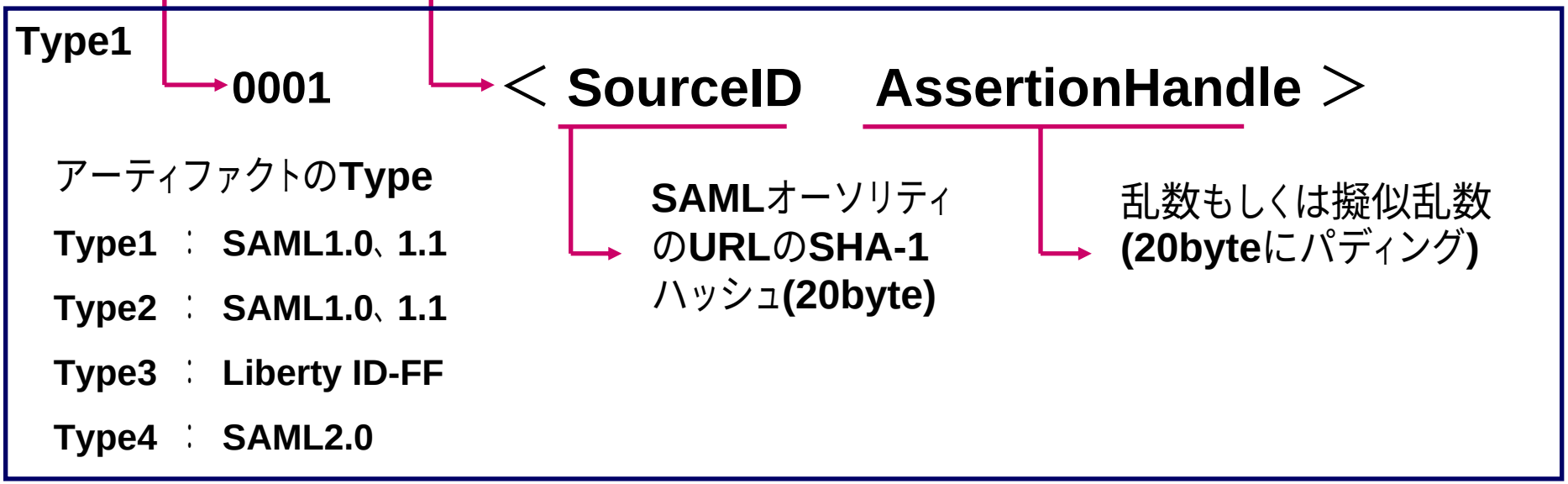
プロファイル

- **Web**ブラウザ**SSO**をサポートする**2**つのプロファイルを規定
  - ブラウザ/アーティファクト・プロファイル
    - **SAML**アーティファクト方式:
      - **URL** クエリ文字列中に埋め込まれる**SAML**アーティファクト内にアサーションへの参照を保持
      - 目的**Web**サイトへのリダイレクトを用いて運搬
  - ブラウザ/**POST**プロファイル
    - フォーム**POST**方式:
      - **HTTP POST**により目的**Web**サイトへアップロードされる**HTML**フォームデータ内にアサーションを保持



アーティファクトの例

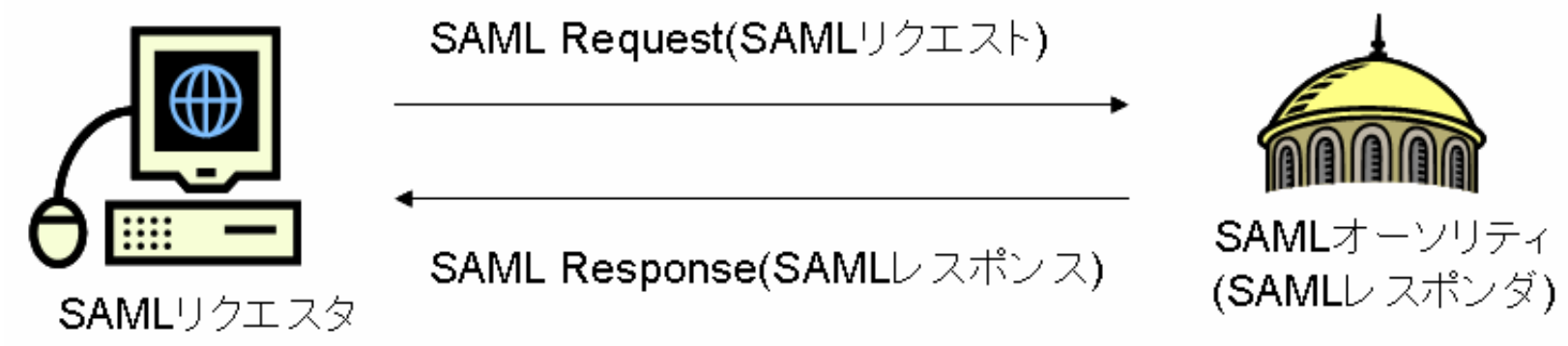
＜ TypeCode　RemainingArtifact ＞のBase64変換



AAGMn1Wa68XRZrJQY9pg0HVrFODV1ZPpGAtkRe5cmh4KSWTkW76nVMUp

SAMLプロトコル

- アサーションを取得するためのプロトコル
- メッセージフォーマットを規定
  - **SAML**リクエスト
  - **SAML**レスポンス
- **SAML**リクエスト、**SAML**レスポンスにも**XML**署名の付加が可能



SAMLリクエストの例

```
<samlp:Request
 MajorVersion="1"
 MinorVersion="1"
 RequestID="_192.168.16.51.1024506224022"
 IssueInstant="2004-10-20T08:21:30.022Z"
 xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
 xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
 xmlns:xsd="http://www.w3.org/2001/XMLSchema"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  …
  </ds:Signature>
  <samlp:AssertionArtifact>
  AAGMn1Wa68XRZrJQY9pg0HVrFODV1ZPpGAtkRe5cmh4KSWTkW76nVMUp
  </samlp:AssertionArtifact>
</samlp:Request>
```

リクエストのバージョン

リクエストの識別ID

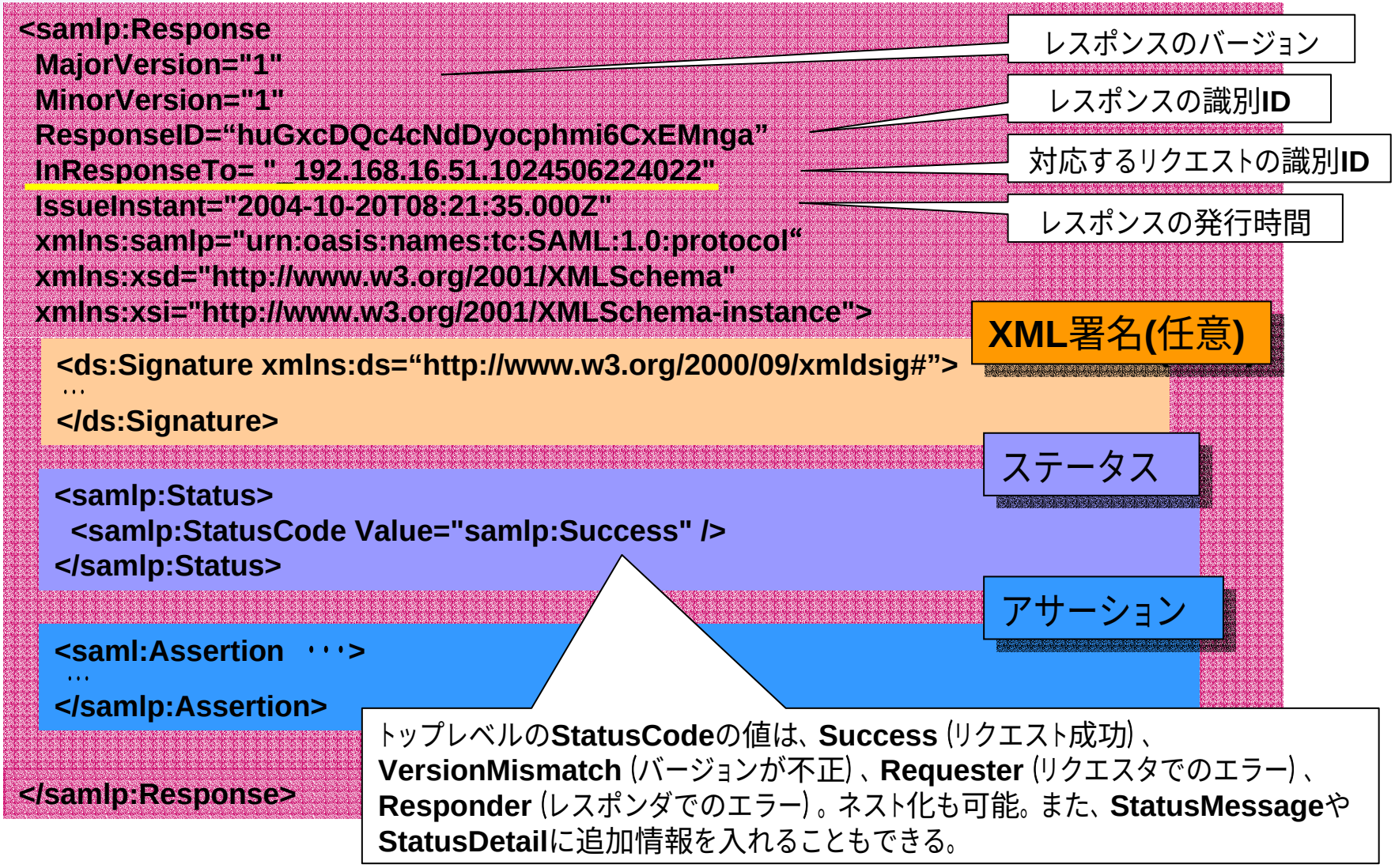
リクエストの発行時間

XML署名(任意)

アーティファクト

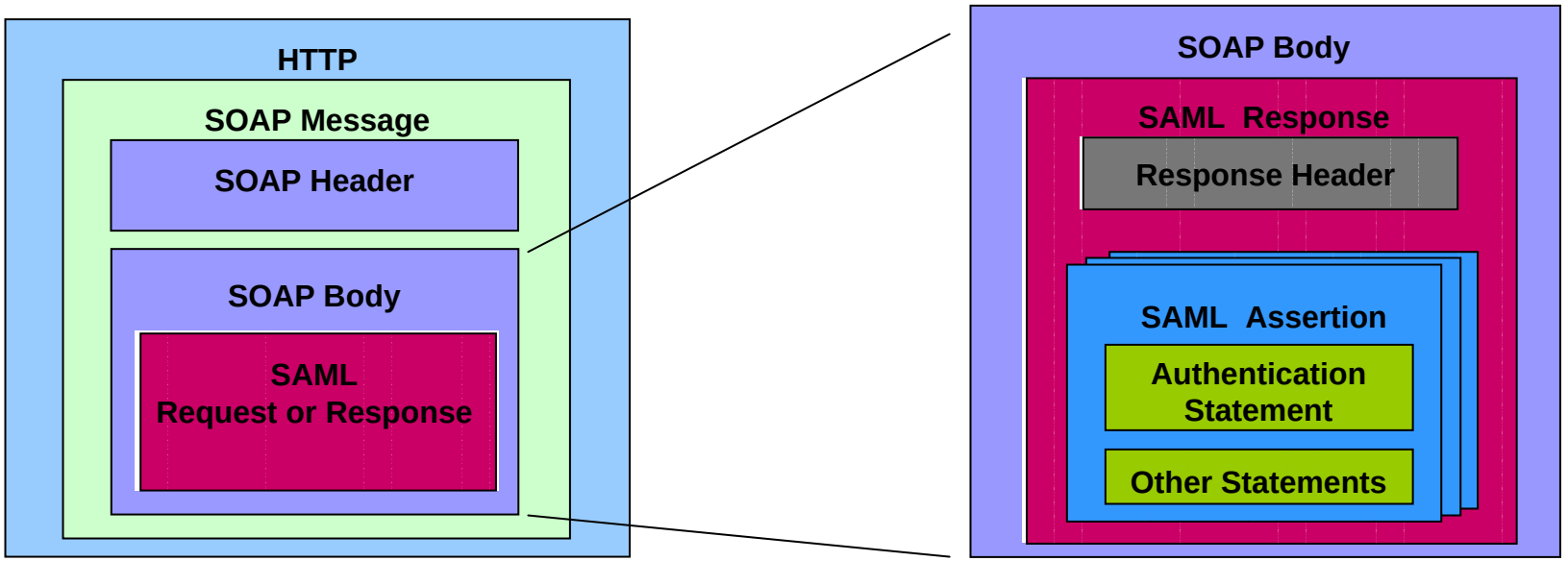
AuthenticationQuery（認証情報の問い合わせ）、**AttributeQuery**（属性情報の問い合わせ）、**AuthorizationDecisionQuery**（権限情報の問い合わせ）、**saml:AssertionIDReference**（指定した**AssertionID**を持つアサーションの問い合わせ）、**AssertionArtifact**（指定したアーティファクトに結びつくアサーションの問い合わせ）から**1**つ選択

SAMLレスポンスの例



SOAPバインディング

- バインディングとは**SAML**のリクエスト、レスポンスのメッセージ交換を、実際の標準的なメッセージ交換/通信プロトコルでどう実現するかを規定したもの
  - **SOAP**バインディング<唯一規定されているバインディング>
    - **SAML**リクエスト、レスポンスをやり取りする際の**SOAP**の利用方法を規定
    - **SAML over SOAP over HTTP**の実装を必須と規定



Empowered by Innovation