NGNにおけるPKIおよび認証技術

NTT 情報流通プラットフォーム研究所
高橋健司

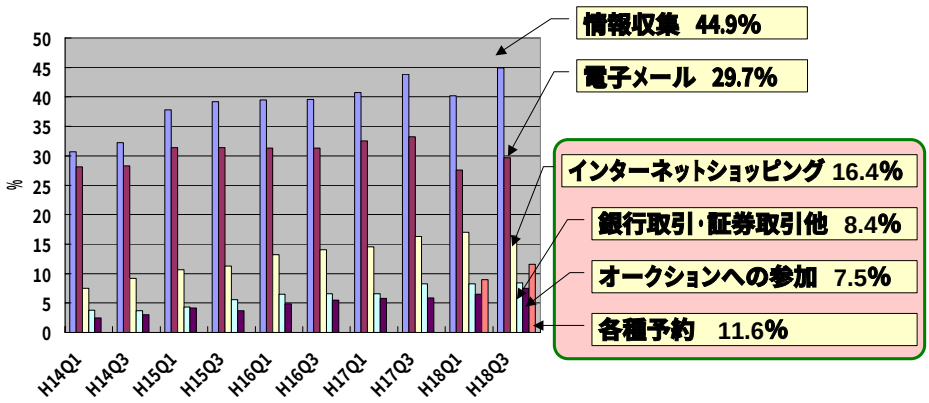
裸のセキュリティ表示？

オンラインバンキング利用者についての実験結果

- HTTPSの表示をなくしても、パスワードを入力
  →100%
- さらに、サイト認証用画像を省いても、パスワードを入力
  →92%
- さらに、セキュリティ警告画面を出しても、パスワードを入力
  →53%

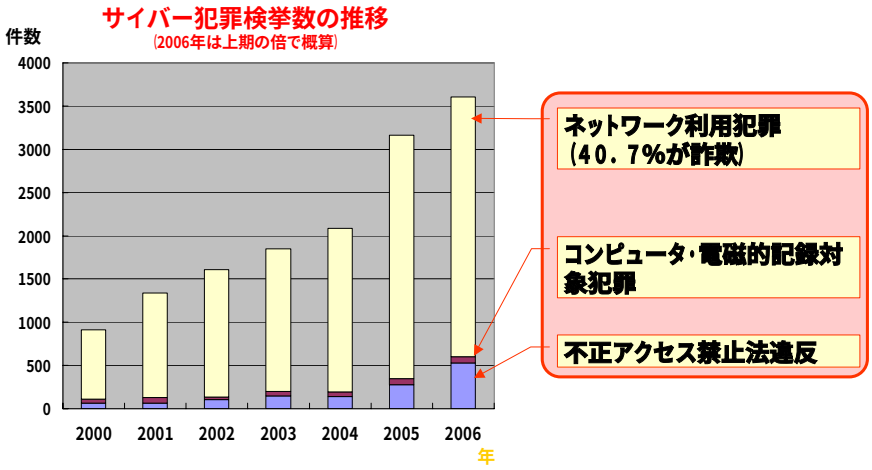
S. Schechter et al, "The Emperor's New Security Indicators," Proc. IEEE Symp. Security and Privacy, 2007

インターネットでの個人の経済活動が増加



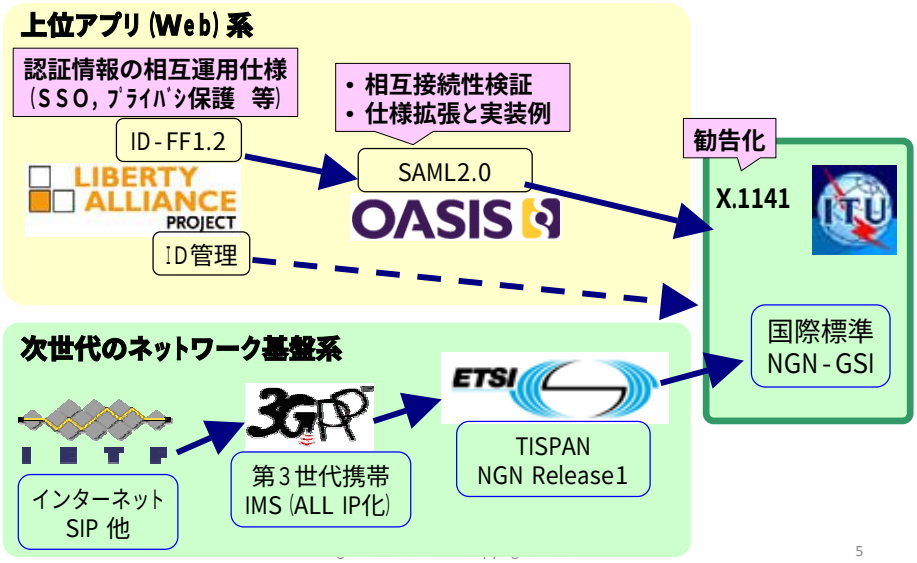
出典：総務省資料 http://portal.stat.go.jp/Guid/joukyou/joukyouit0201.html

サイバー犯罪の検挙数も増加



警察庁広報資料より http://www.npa.go.jp/cyber/statics/h18/pdf31.pdf

認証技術の標準化動向



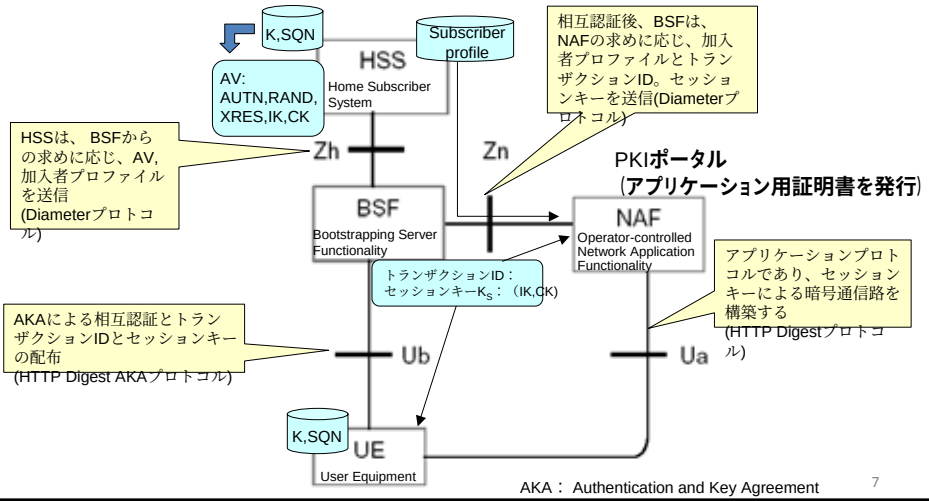
NW基盤系の認証技術の標準化

- NGNにおけるPKI (ITU-T) -

- SG13 Q15 (NGN セキュリティ)において、“Y.NGN Certificate Management” (NGN証明書管理) 勧告を議論中
- フォーマットはX.509バージョン3を利用
- 証明書の所有者に応じて3つに分類して運用方法を既定
  - NGN網内装置証明書
  - NGN加入者証明書
  - NGN利用者証明書

NW基盤系の認証技術の標準化
ー 3GPP(IMS)におけるPKI ー
General Authentication Architecture

•加入者情報をベースに、外部アプリケーション用の証明書を生成
•3GPP Release 8で仕様策定中(TS 33.220, TS 33.221)



AKA： Authentication and Key Agreement

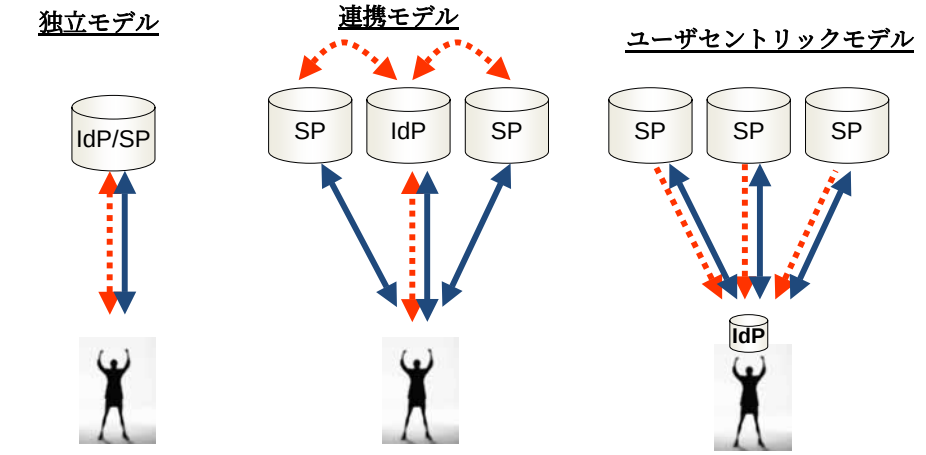
アイデンティティ管理をめぐる3つの動き

- **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
    - IE7に標準装備。オープンソース版もある
  - 主なプレーヤ：Microsoft, Novell, IBM他
- **Liberty Alliance/SAML** LIBERTY ALLIANCE PROJECT 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
  - 主なプレーヤ：Liberty Alliance参加メンバ(Oracle, Sun, GSA, Citigroup, NEC, NHK, NTT他)
- **OpenID** OpenID
  - URLをID(個人識別子)として用いるｱｲﾃﾞﾝﾃｨﾃｨ管理技術仕様
  - 主なプレーヤ：OpenID Foundation参加メンバ (Microsoft, Verisign, IBM, Yahoo!, Google, Six Apart等)

3つのアイデンティティ管理モデル

トラスト データ

SP: サービス提供者
IdP: アイデンティティ情報提供者

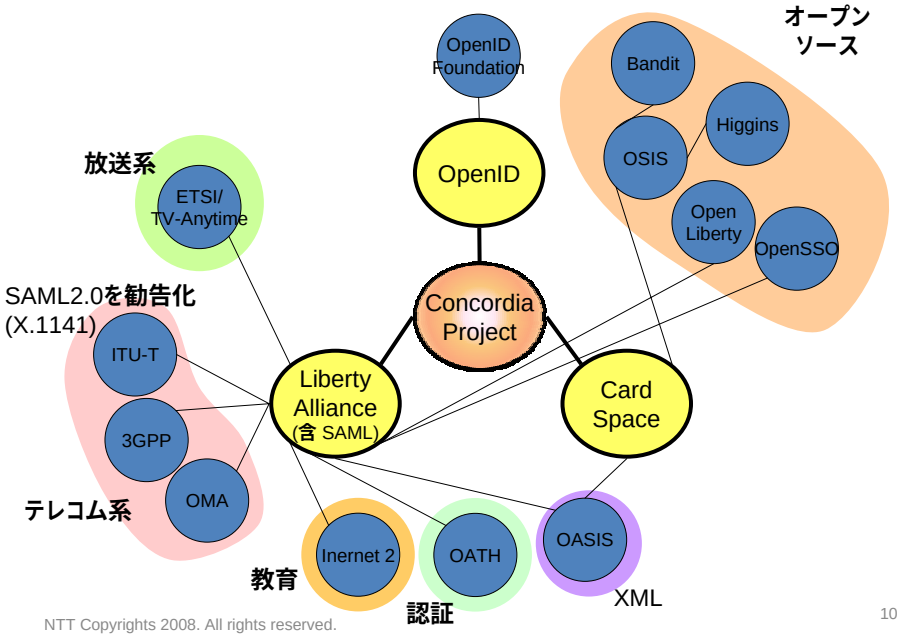


1アイデンティティー→1ＳＰ

1アイデンティティー→多ＳＰ
(IdP/ＳＰ間の事前連携あり)
LA/SAML

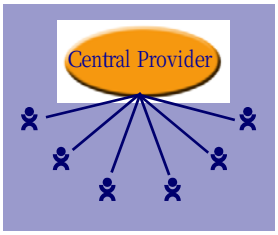
多アイデンティティー→多SP
(IdP/SP間の事前連携なし)
OpenID, CardSpace, LA/SAML

3つの技術と関連団体



連携アイデンティティモデル

- 集中型モデル
  - 単一レポジトリにおけるアイデンティティ情報 の管理
  - 集中コントロール
  - 類似システムのみ連携
- 連携型モデル
  - 様々なロケーションでのアイデンティティ情報の管理
  - 非集中コントロール
  - 類似 / 異種システムと連携

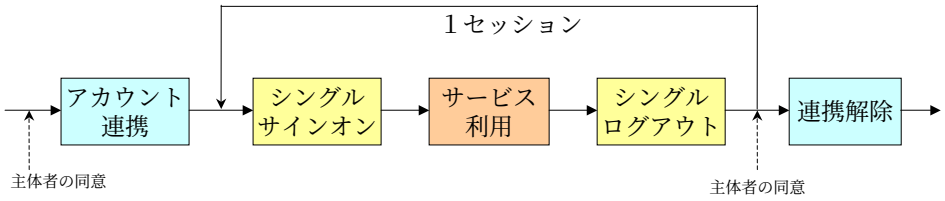


連携アイデンティティ管理の導入状況

- マスターID (NTTコミュニケーションズ) 及びgooID (NTTレゾナント) でSAMLを採用
- Google Appの公開インタフェースとしてSAMLを利用
- 欧米の政府機関での採用
  - 米連邦一般調達庁(GSA)が調達の要件としてSAML準拠を採用
  - フィンランド、ノルウェー、フランス、イギリス等でSAML採用
- 欧州テレコム(仏、独、スペイン等) でも採用が進む
- (世界で10億以上の機器やIDがSAML/Liberty仕様に対応)

アイデンティティ連携ライフサイクル

ユーザの立場から見たアイデンティティ連携の流れ

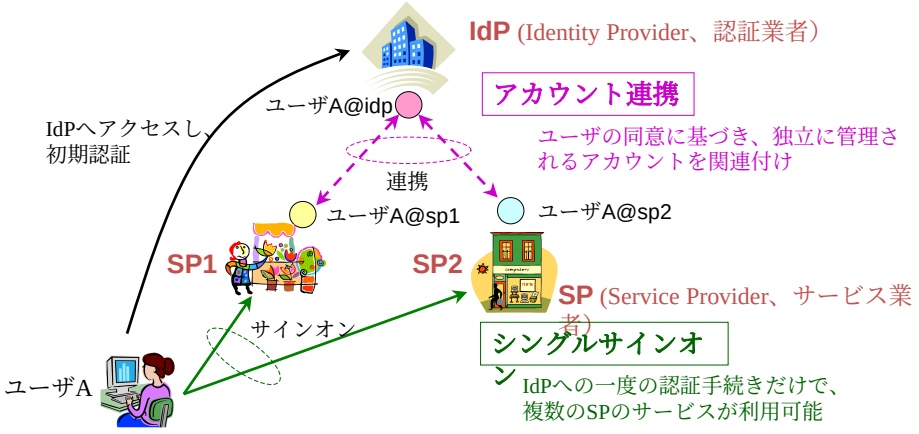


1. **ユーザがIdPとSPにそれぞれアカウントを開設。**
2. **ユーザが上記両アカウントを連携することを同意。**
3. **IdPとSPがアカウントの連携を確立。**
4. **ユーザがSSOし、SPのサービスを利用。**
5. **ユーザがSPのサービス利用終了時に、ログアウト。**
6. **その後、ユーザが上記アカウント連携の解除を要求。**
7. **IdPとSP間の連携が解除。**

SAML v2.0: アイデンティティ連携技術仕様

Security Assertion Markup Language v2.0

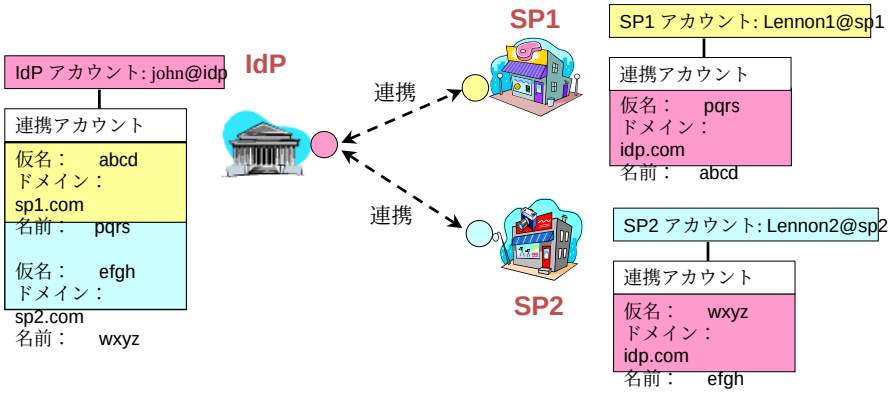
- **認証情報を安全に送付し、アカウント連携とSSO（シングルサインオン）を実現**
- **標準化団体(Liberty Alliance, OASIS)で仕様化され、公開中**



(Source: Liberty Alliance Project 2006)

仮名を使ったアカウント連携

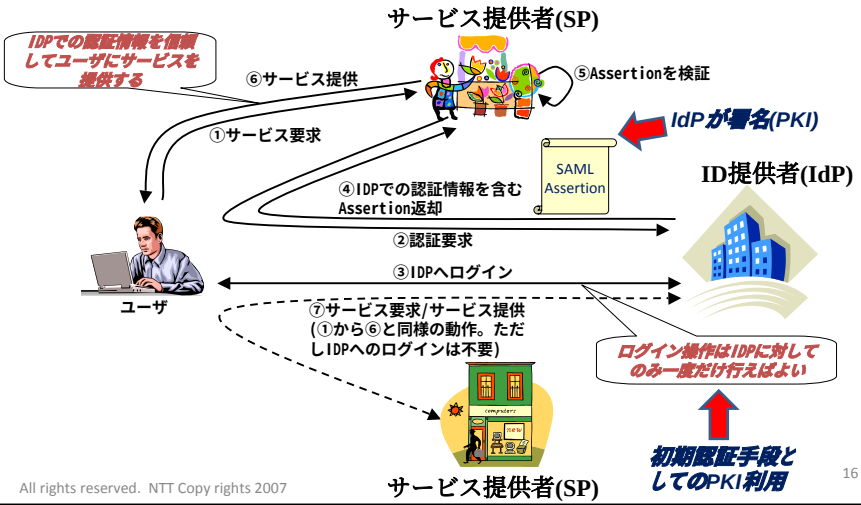
- ユーザに関して、IdPとSP間でのみ有効で、ユーザ個人を特定不能な仮名の利用
  - グローバルIDの必要性を排除、実際のアカウント名の流出を防止
  - 名寄せによるプライバシー情報漏洩を防止



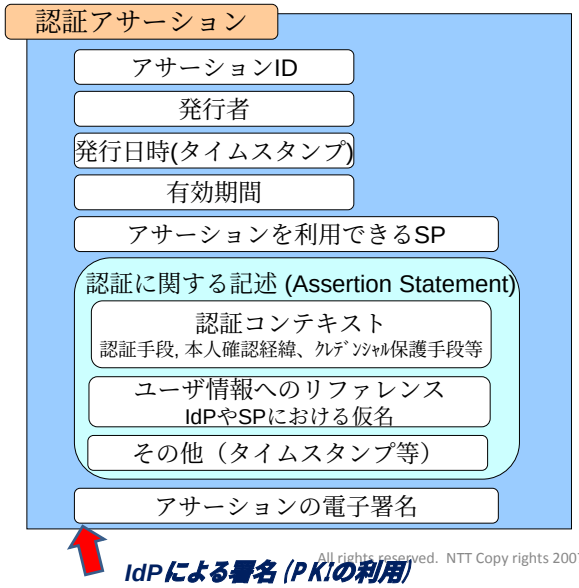
(Source: Liberty Alliance Project 2006)

シングルサインオン

- IDPで一度認証されれば、再度サインオンなしで複数のサービスを利用
- 認証結果情報(assertion)の受け渡しには様々な方法を利用可能
  - Assertionに属性情報や認可情報も含むことが可能



認証アサーション



- SAML (Security Assertion Markup Language) **を用いて表現。**
- **IdPとSP間でのみ有効な仮名を使ってユーザ個人を参照**

(Source: Liberty Alliance Project 2006)

認証コンテキスト

Authentication Context

認証コンテキストは、IdPからSPに伝える認証結果の背景情報。SPは、これを認証結果の確かさの判断材料に使う。以下の内容を記述することができる

- **本人確認** (Identification) – **ユーザ情報登録時の本人確認手段に関する記述 (例： 対面で免許証を確認)**
- **技術的保護** (Technical Protection) – **ユーザ認証のための秘密 (パスワードや秘密鍵等) がどのように保護されていたかの記述 (例：ICカードに格納)**
- **運用上の保護** (Operational Protection) – **IdP側でのセキュリティ運用に関する記述 (例：セキュリティ監査)**
- **認証手段** (Authentication Method) – **IdPにおけるユーザの (初期)認証手段に関する記述 (例：パスワード、PKI等)**
- **適用する契約** (Governing Agreements) – **認証に適用される契約に関する記述 (例：保証責任の範囲)**

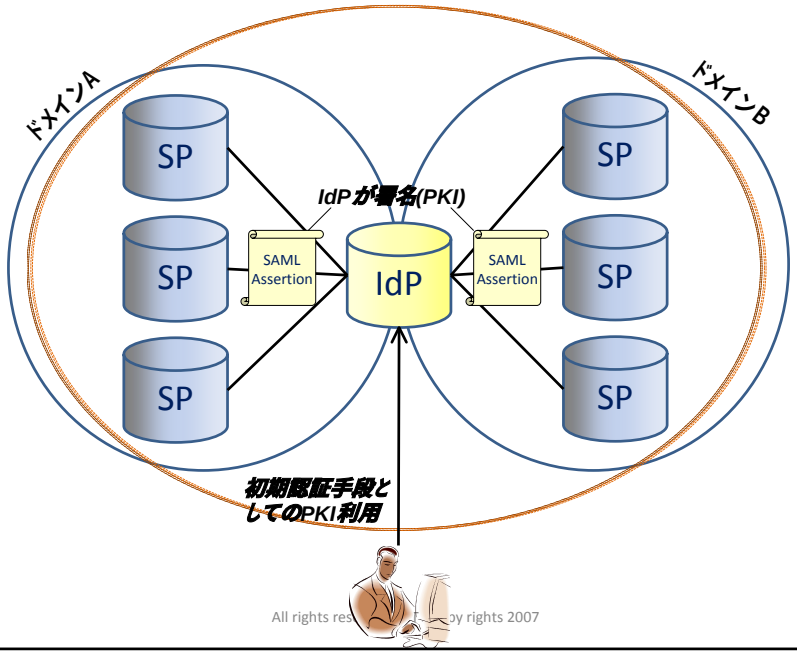
SAMLv2.0 の機能

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。

(Source: Liberty Alliance Project 2006)

SAMLとPKIの関係



新たなトレンド：User Centricアプローチ

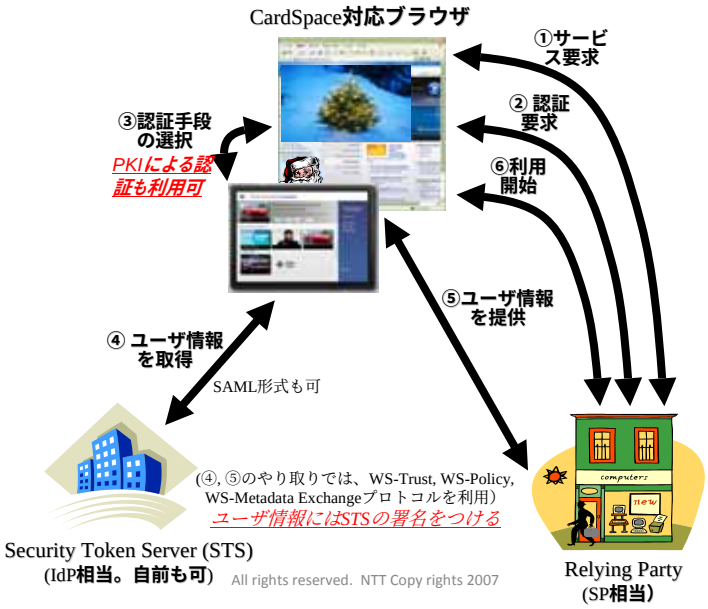
- ユーザによる個人情報のコントロールを重視
  - IdPやSP間の関係をフレキシブルにユーザが選択可能
  - User centricの定義は、まだ流動的。
  - 設計思想であり、特定の技術に結びついている訳ではない。
    - “The Law of Identity”
- 「簡易な」、「制限の緩い」実装が可能
  - 応用例：ブログやＳＮＳへの応用
- オープンソースコミュニティによる開発
- 代表的な実現例として、以下の3つがある
  - Microsoft CardSpace
  - OpenID 2.0
  - Liberty Alliance/SAML

CardSpaceとは？

「カード」を選択する感覚で、アイデンティティ情報を管理

- Microsoft Vista／IE7に標準搭載のID管理機能
  - SAMLをセキュリティトークンとして利用することも可能
    - Web Services Security SAML Token Profile v 1.0 and REL Token Profile v1.0
    - <http://www.oasis-open.org/specs/index.php#wssprofilesv1.0>
  - 関連仕様をOASIS等で標準化中
    - WS-SecureConversation, WS-SecurityPolicy, WS-Security, WS-Transaction, WS-Trust, WS-Federation
- オープンソース版も開発中
  - OSIS (Open Source Identity System)
    - Bandit, Higgins, OpenSSO等
    - Firefoxでも利用可能

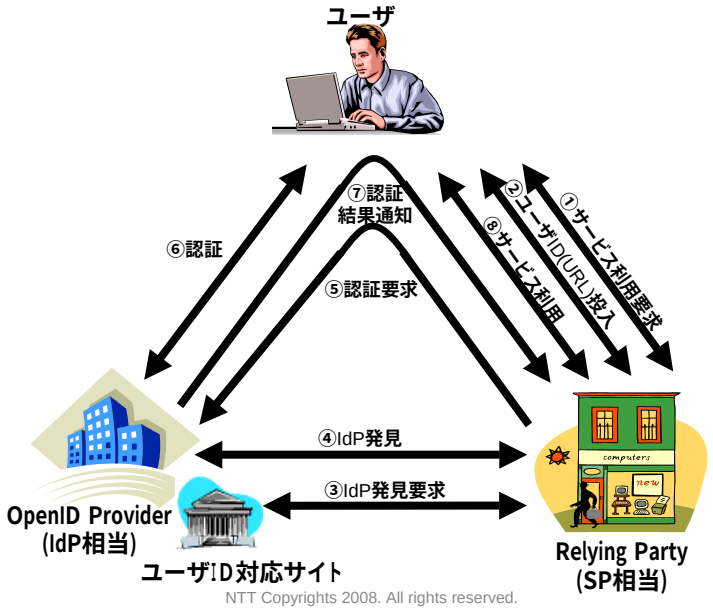
CardSpaceの基本動作



OpenID 2.0とは？

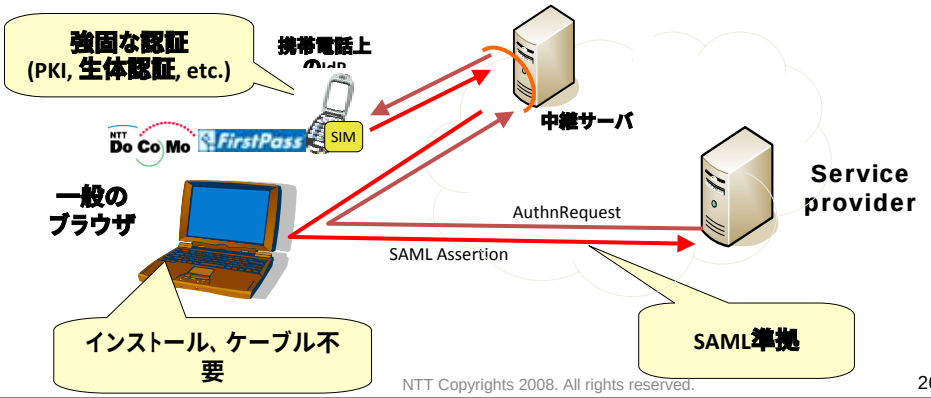
- アドレスベースのIDを用いたアイデンティティ管理技術。OSISで仕様を策定中。
  - Versign, Sxip, JanRain, Sxi Apartらが提案
- ユーザがあるアドレスを保有していることを証明することにより、認証を行う
- 「軽い」実装を目標に設計
  - SOAPを使わない。メッセージ形式も簡便化
  - 現在は、ブログやＳＮＳでの利用がメイン
- 複数のアドレスベース技術仕様(OpenID1.1, Yadis, XRI等) を統合。
- アドレスとして、URI及びXRIが利用可能。
  - XRI: eXtensible Resource Identifier
- シングルサインオン機能及び属性交換機能を規定。

OpenID 2.0の認証機能の基本動作



SAMLによるユーザセントリック型技術(SASSO)

- 携帯電話上にSAML IdPを実装し強固認証をどこでも簡単に利用
  - ユーザセントリックで使い勝手のよいアーキテクチャ
  - 大きな拡張性。携帯電話の持つ認証機能を汎用的に利用可能
    - 例：NTTドコモの認証サービス(FirstPass)
  - 高いユーザビリティ。携帯電話さえあれば、ＰＣ等にインストール不要
  - 強化されたプライバシ。仮名ID連携による名寄せの防止。

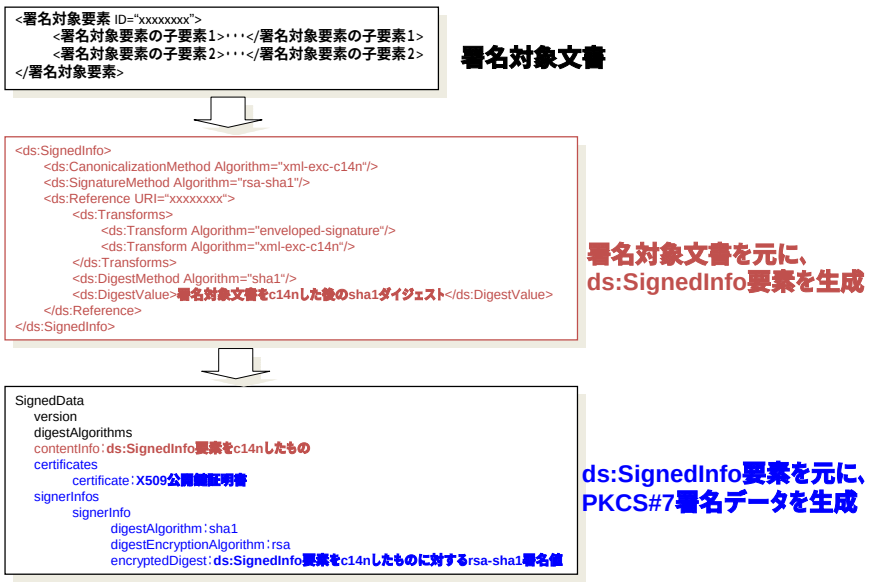


PKCS#7署名からXML電子署名へのフォーマット変換

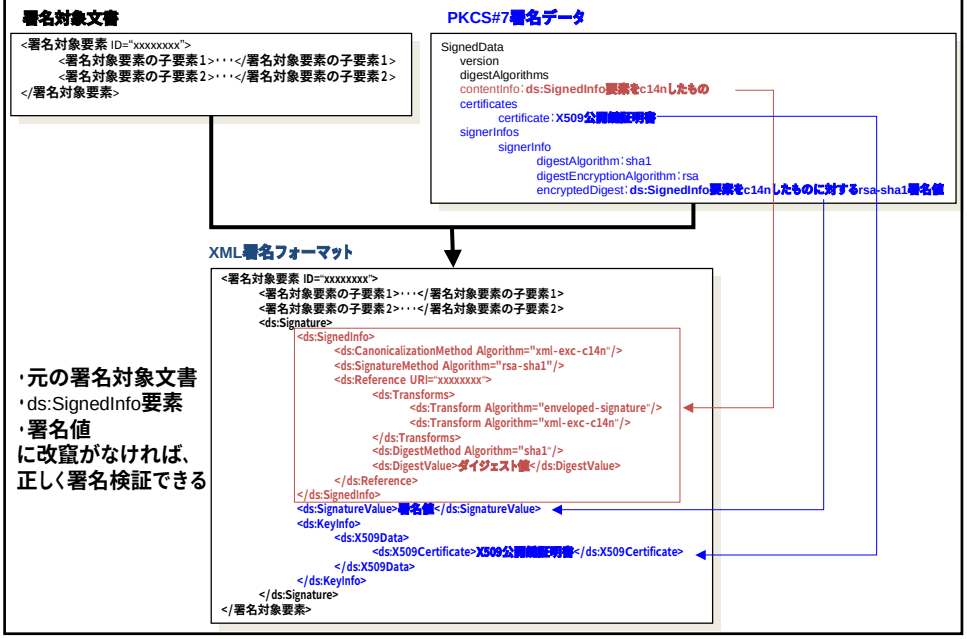
予め、署名対象文書に対して、ds:signedInfo要素を生成しておき、そのds:signedInfo要素をc14n化したものに対してPKCS#7署名データを生成すればよい。

	XML電子署名要素	PKCS#7署名データ
最終的な署名値計算のための元データ	ds:signedInfo要素をc14n化したもの	contentInfo
署名値	ds:signatureValue要素	encryptedDigest
X509公開鍵証明書	ds:x509Certificate要素	certificate

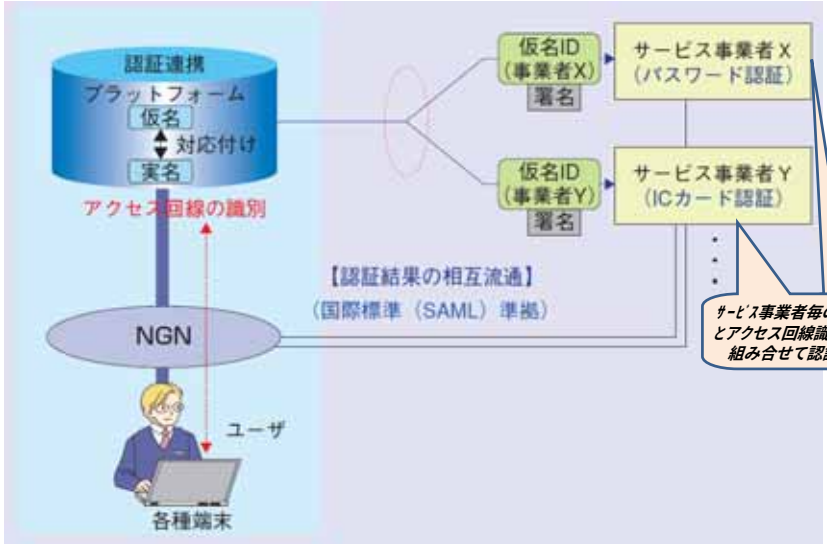
フォーマット変換の具体的手順その1： PKCS#7署名データの生成



フォーマット変換の具体的手順その2： XML署名フォーマットの構築



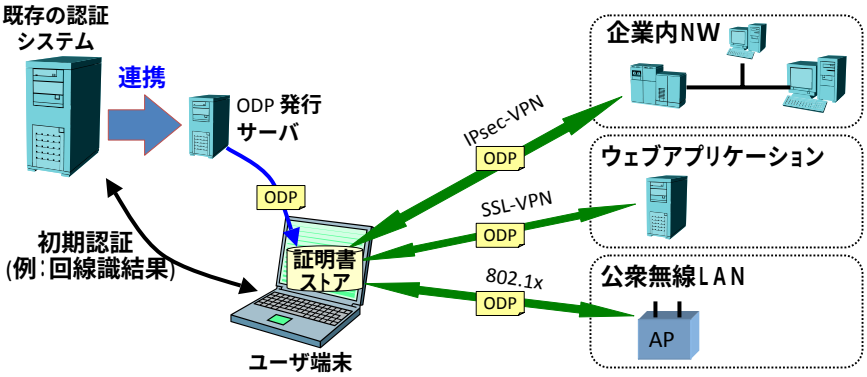
認証連携プラットフォーム
- アクセス回線識別情報の活用 -



(川添他、「次世代ネットワークを利用したプラットフォーム・アプリケーション技術」、NTT技術ジャーナル、Vol.19, No. 4) より

ODP(On Demand Pass)技術

- 認証結果をノマディック環境でも利用可能にする
  - 利用毎、目的別に短寿命の証明書を発行し利用



31

まとめ

- PKIと相互に補完しあう(認証／署名手段)、アイデンティティ管理技術の研究開発及び標準化が進めれられている
  - SAML, OpenID, CardSpace等
- PKI技術及びアイデンティティ管理技術の適用により、NGN向けの認証サービスのプライバシ及びセキュリティ強化が期待される

For more information…

- CardSpace
  - http://msdn2.microsoft.com/en-us/netframework/aa663320.aspx
- Concordia Project
  - http://projectconcordia.org
- Liberty Alliance
  - http://www.projectliberty.org
  - http://wiki.projectliberty.org/index.php/JapanSIG
- OpenID
  - http://openid.net
- OSIS
  - http//osis.idcommons.net