セコムIS研究所
Intelligent Systems Laboratory

認証技術の現状の課題と今後の動向

セコム株式会社 IS研究所/
JNSA PKI相互運用技術WGリーダー
松本　泰

2004 年 12月 9日

セコムIS研究所
Intelligent Systems Laboratory

電子認証の現状と今後の課題

- e-Japan戦略の成果としてインターネットにおけるブロードバンドなどの普及が上げられている。そしてこれらのIT基盤の利活用が次の課題とされている。
- しかし、これまでのIT基盤は、利活用を進めるにふさわしい十分なユーザ認証（電子認証)、セキュリティを提供しているとはいえない。
- 特に、ネットワークにおける電子認証は、当たり前に利用されているにも限らず、インターネット上等で広く利用されている電子認証に対して何の評価基準もなく、実際、低レベルの電子認証が主流だと考えて間違いない
- IT基盤の利活用、様々な連携を進めるための電子認証のあり方について考察する

電子認証の現状と今後の課題

セコム IS 研究所
Intelligent Systems Laboratory

- NPO JNSAのChallenge PKIプロジェクト
- 認証のチュートリアル
- 現状の課題と今後の方向性
- 米国のe-Authentication Initiativeの例
- まとめ

NPO JNSAのChallenge PKIプロジェクト
プロジェクトの活動履歴

セコムIS研究所
Intelligent Systems Laboratory

2001	2002				2003				2004
4Q	1Q	2Q	3Q	4Q	1Q	2Q	3Q	4Q	1Q

Challenge PKI 2001 プロジェクト

Challenge PKI 2002 プロジェクト

Challenge PKI 2003 プロジェクト

☆ PKI関連相互運用性に関する調査報告を公開 (2002.5.16)

☆ JNSA主催 NSF2002での発表 2002.6.12

☆ 54th IETF 横浜ミーティングの PKIX WG において発表した。 2002.7.17

☆ 2002.11.20 55th IETF アトランタミーティングの PKIX WG において発表

☆ 2002.12.17 JNSA IW2002セミナ

☆ 2003.3.20 56th IETFサンフランシスコミーティングの PKIX WG において発表

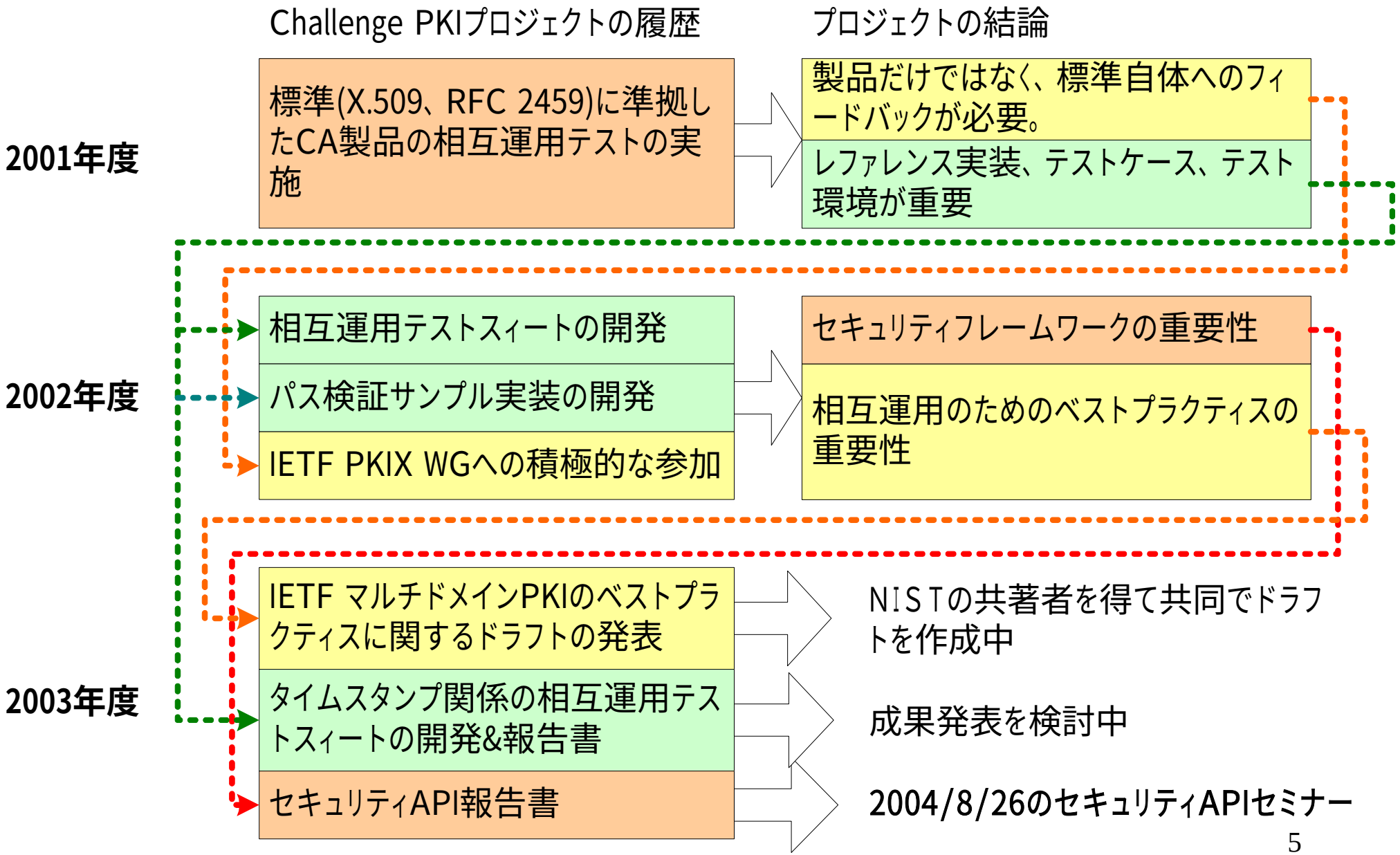
☆ 2003.7.17 57th IETFウィーンミーティングの PKIX WG において発表

☆ JNSA主催 NSF2003での発表 2003.10.24

☆ JNSA主催 ChallengePKI IETF参加等活動報告会 2004.4.27

NPO JNSAのChallenge PKIプロジェクト
プロジェクトの活動履歴(2)

セコムIS研究所
Intelligent Systems Laboratory

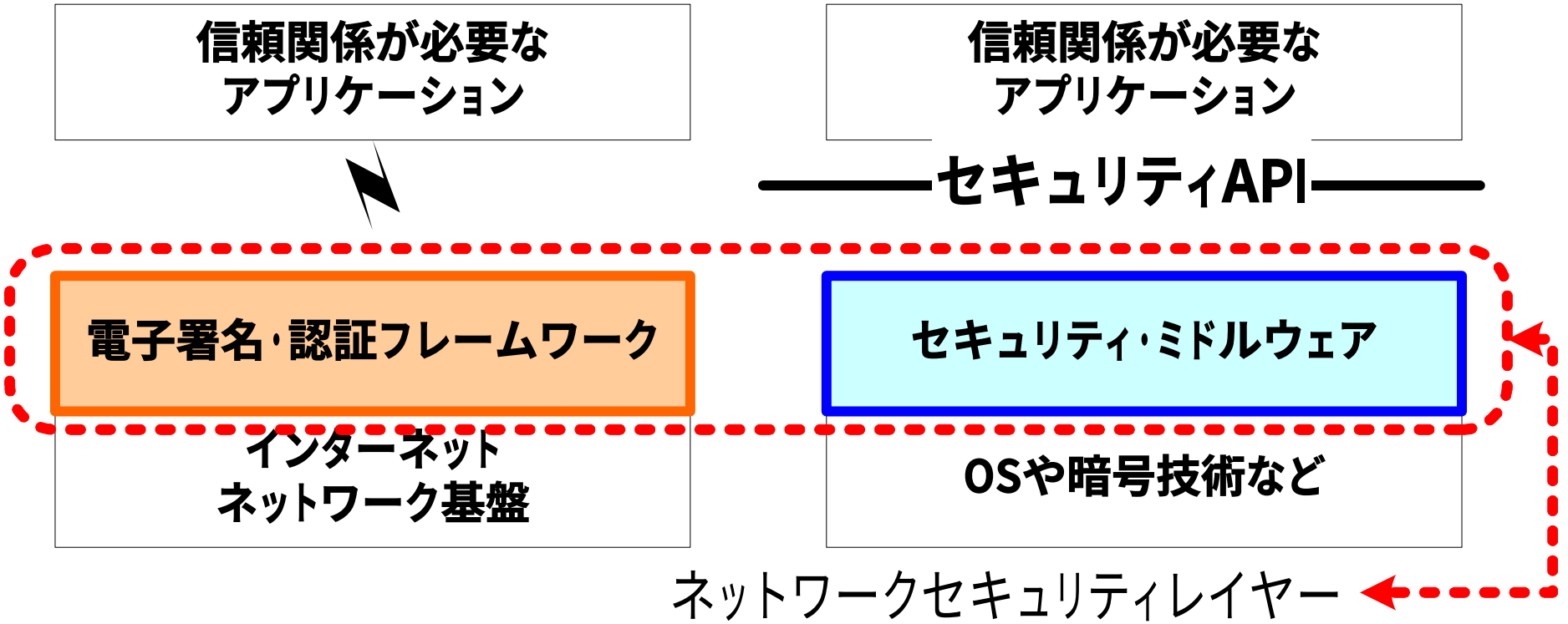


NPO JNSAのChallenge PKIプロジェクト
PKIプロジェクトの目標と課題

セコム IS 研究所
Intelligent Systems Laboratory

- プロジェクトの今後の目標
  - 実際に幅広く展開可能なセキュリティインフラの構築(= 幅広く相互運用可能なPKIの展開)
- 標準化の課題 (標準・実装から展開)
  - アイディアから仕様へ -> 多くの研究者が行っている
  - 仕様から標準、標準から実装 -> 学術系＆ベンダーなど
  - 標準・実装から展開 (相互運用) -> 誰が担うか
    - 標準と呼ばれる文書は山のようにある。しかし相互運用可能なものは極わずか…. これを解決して行かなければならない。
    - -> ベストプラクティスが重要。。。。ここに注力する。
- セキュリティフレームワークやミドルウェア重要性
  - 実際のアプリケーションにおいて、セキュリティ・ミドルウェアが、実行時のネットワーク上の信頼と複雑な相互運用の問題を吸収する

NPO JNSAのChallenge PKIプロジェクト
セキュリティフレームワークやミドルウェア重要性

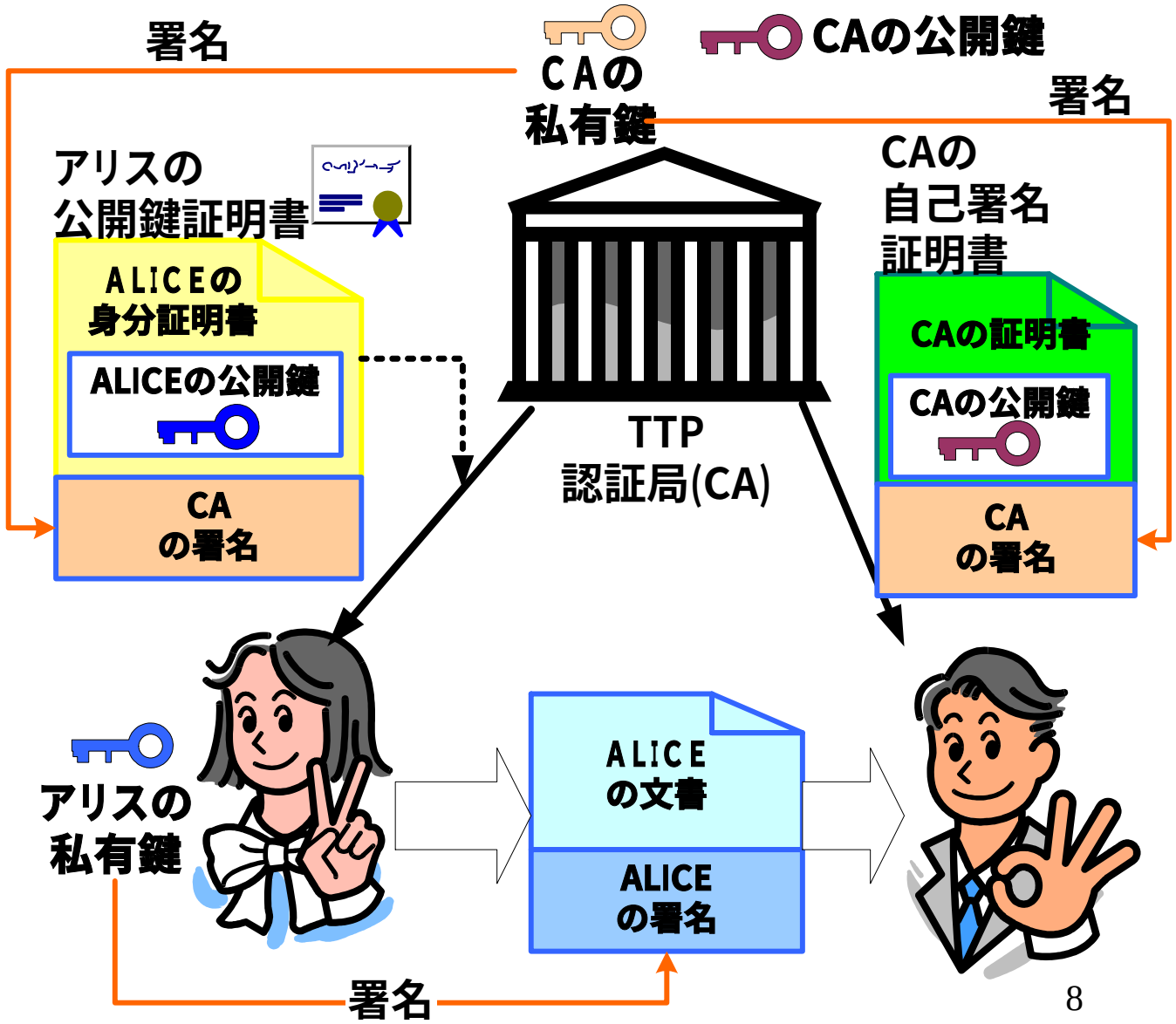


- 何処でも、何時でも、誰にでもつながるユビキタスネットワークにおいて信頼の拠りどころが求められる。。。。
- ネットワーク上の信頼を実現するセキュリティ・レイヤーの必然性
  - これらは、古典的なOSI参照モデルなどでは説明がつかない。。。

認証のチュートリアル
TTPよる署名（いかにアリスの公開鍵を信頼するか）

セコムIS研究所
Intelligent Systems Laboratory

- TTP(Trusted Third Party)とは
  - 信頼できる第三者機関
  - TTPによって署名されたデータは信用できるものとする
  - 代表的な例はCA（Certification Authority）
  - CAは印鑑証明を発行してくれる役所のイメージ
  - 公的個人認証サービスでは、都道府県CAが市民のための証明書を発行する。



認証のチュートリアル
リアル社会の証明書と電子証明書

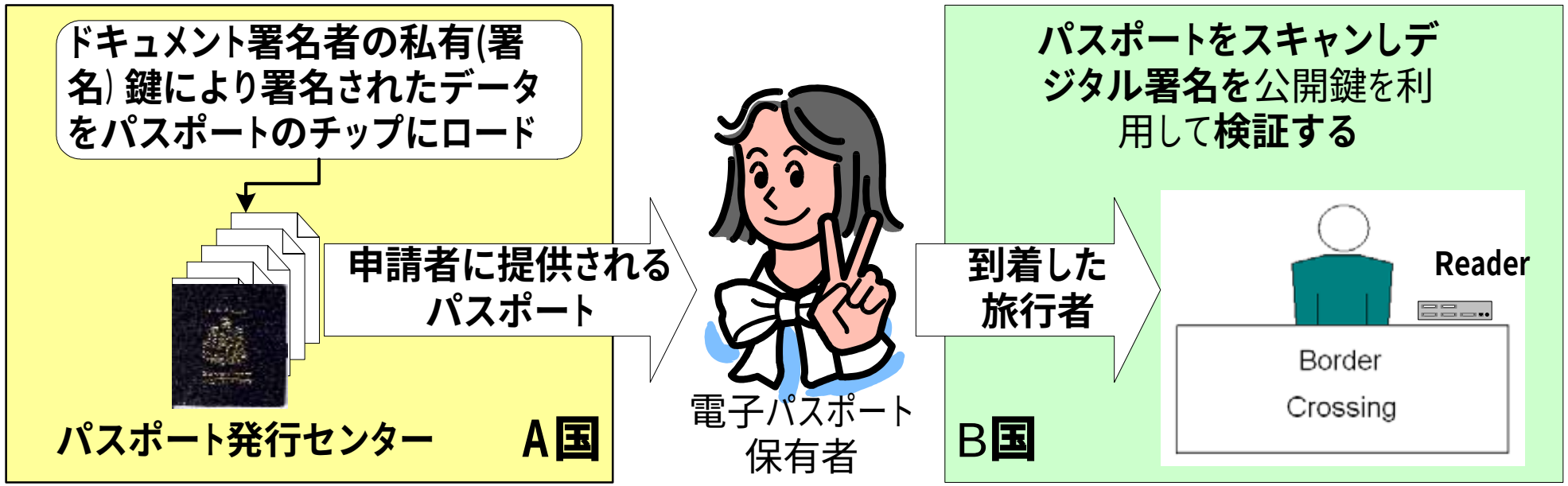
セコム IS 研究所
Intelligent Systems Laboratory

- リアル社会の証明書例
  - パスポート　-　「日本国外務大臣」が発行者
  - 運転免許証
  - 社員証、学生証、会員証
  - 発行者の何らかの「印鑑」が押されている。。
- 電子証明書
  - 公開鍵証明書　-　利用者が公開鍵に対応する私有鍵を持つ
  - 属性証明書　　-　電子許可証など
  - 電子パスポート　-　発行者（日本国外務大臣??)により電子署名が施されている。

認証のチュートリアル
典型的な電子署名の利用形態

セコムIS研究所
Intelligent Systems Laboratory

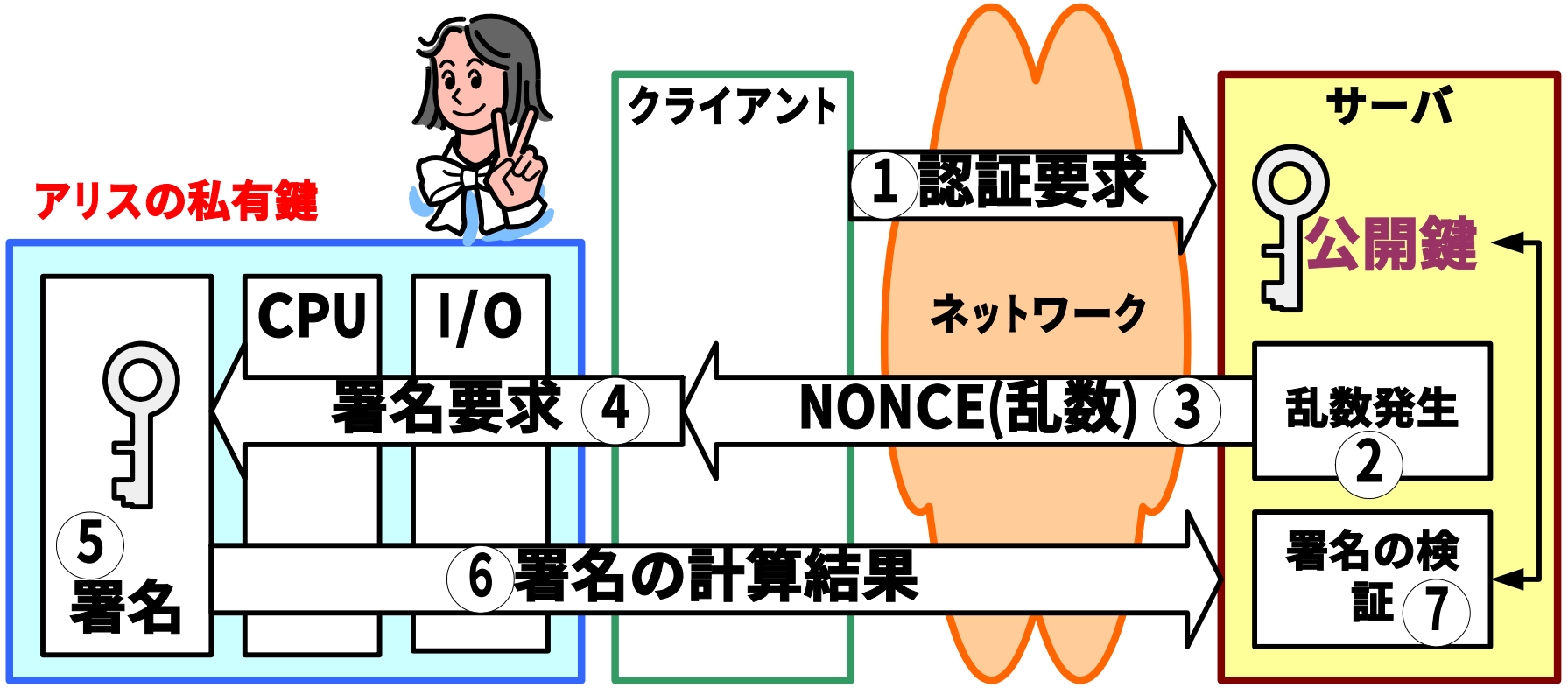
- 紙のパスポートから電子署名を施した電子パスポートへ
- 国際民間航空機関(ICAO)のNTWG (New Technology Working Group) PKIによるパスポートのデジタル署名の案
  - 機械可読な旅行文書(MRTD)のためのPKI電子署名
    - 電子署名 -> 不正を防ぐ　署名の意味=内容の証明
- #「不正を防ぐ=Big Brother」とならない情報公開、透明性が必要
  - 透明性の確保自体にも電子署名が重要



認証のチュートリアル
PKIを用いた認証 (Authentication) の例

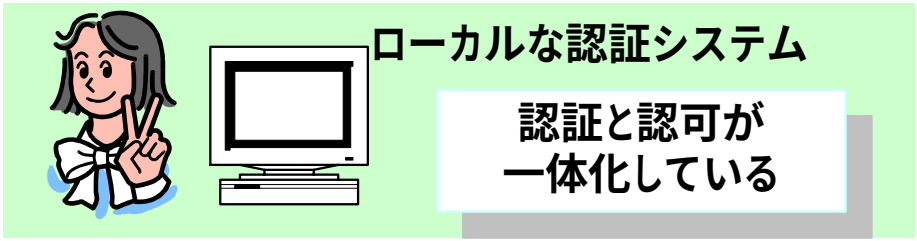
セコム IS 研究所
Intelligent Systems Laboratory

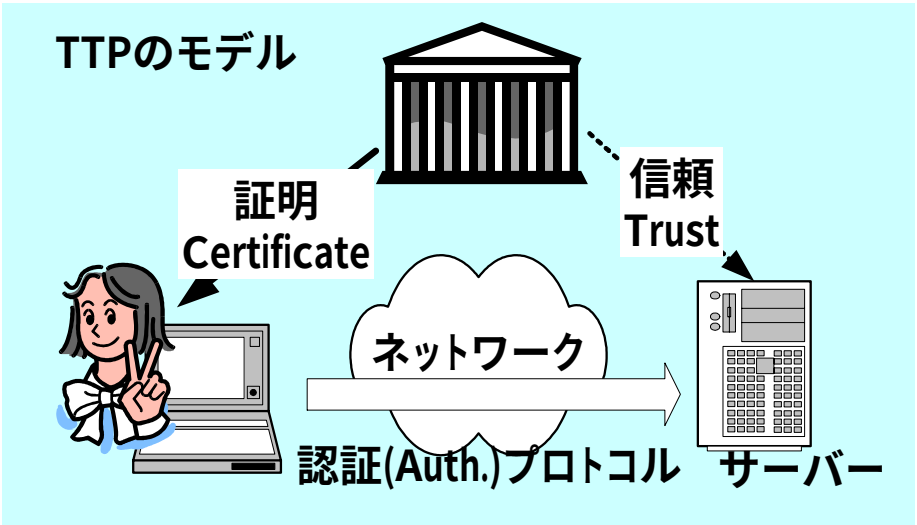
- チャレンジ・レスポンス認証の例
- アリスの秘密情報 (私有鍵) はハードウェアトークンから出ない
  - もちろんネットワークにも流れない
- アリスの秘密情報は、サーバには、格納されない
  - サーバは、アリスの秘密情報 (例えばパスワード) を預かる必要がない
  - これは、アリスとっても、サーバの運用者にとってもメリット

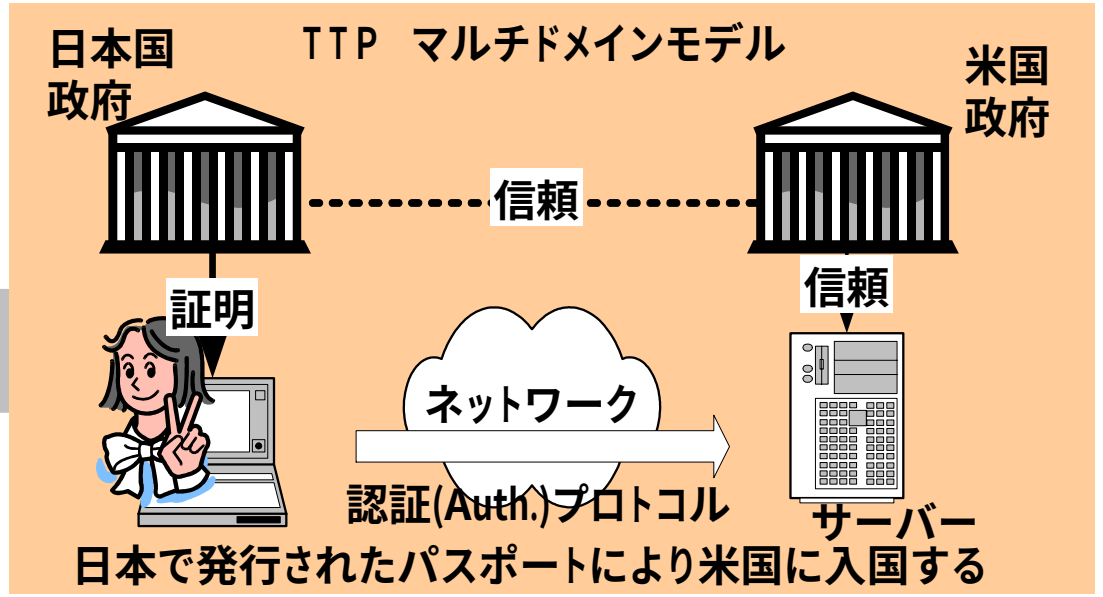


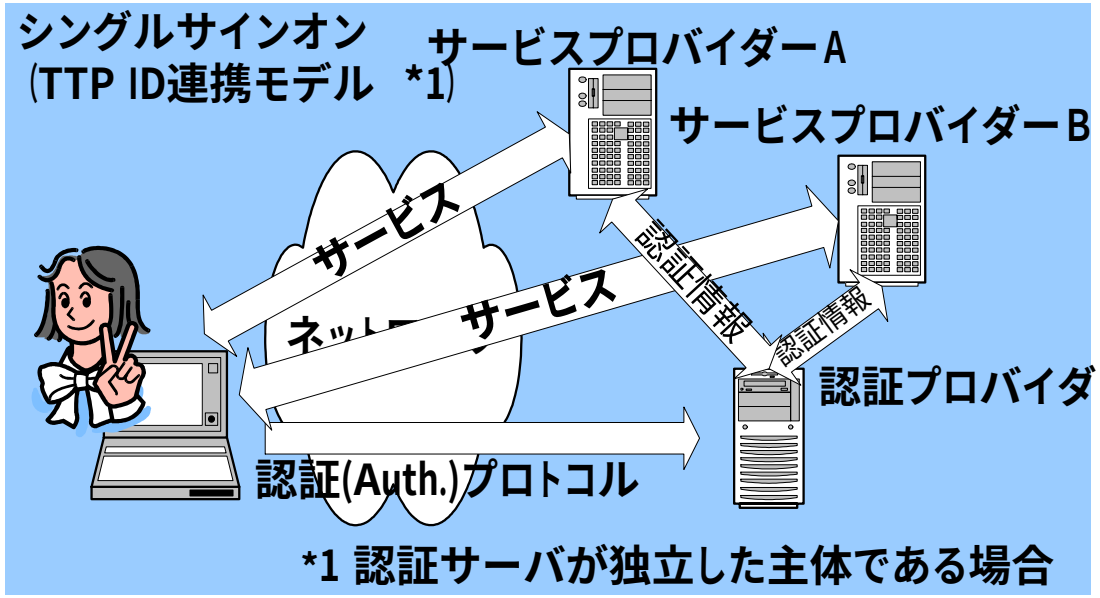
認証のチュートリアル
認証(Authentication)のモデル

セコムIS研究所
Intelligent Systems Laboratory

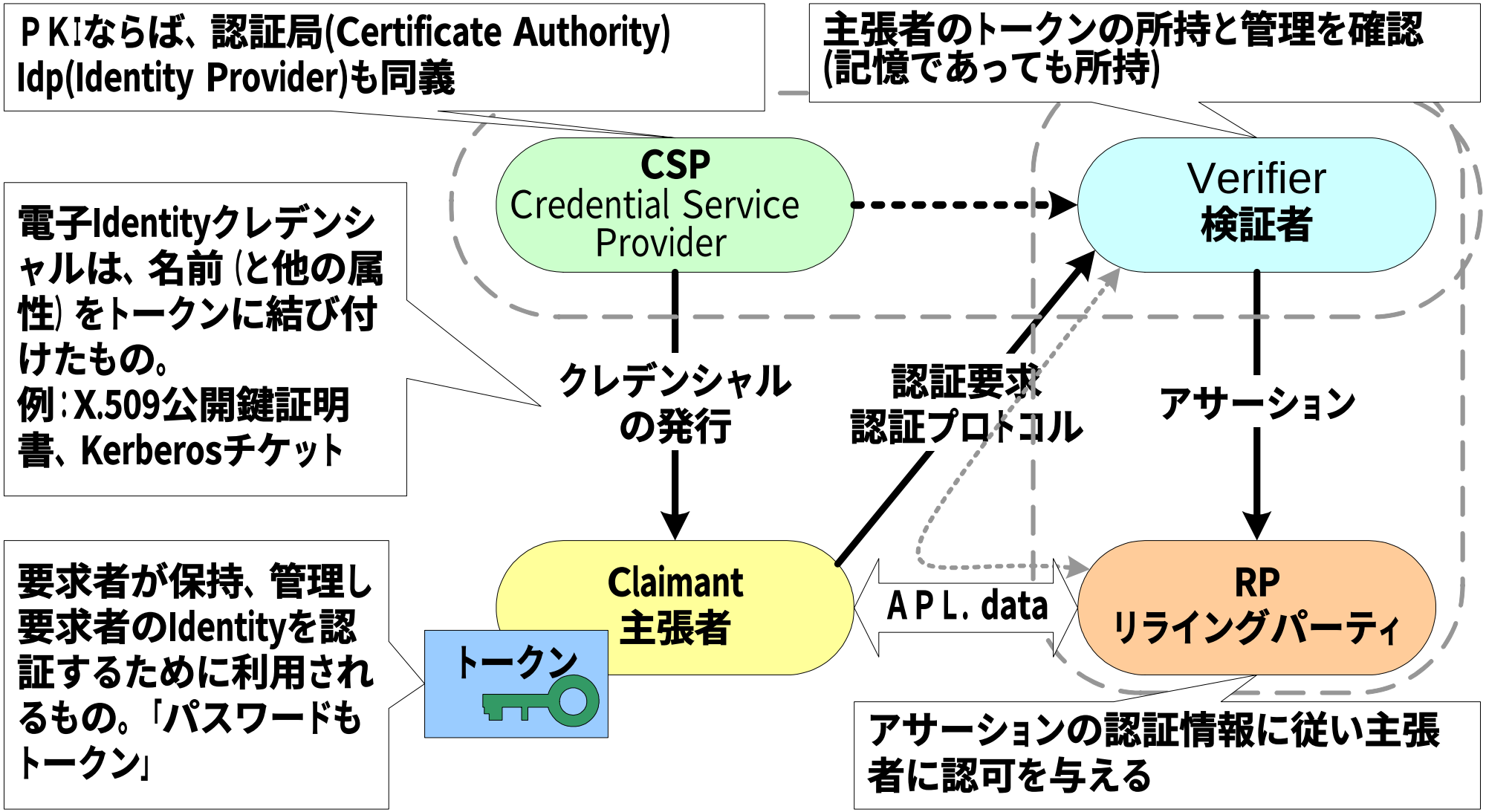








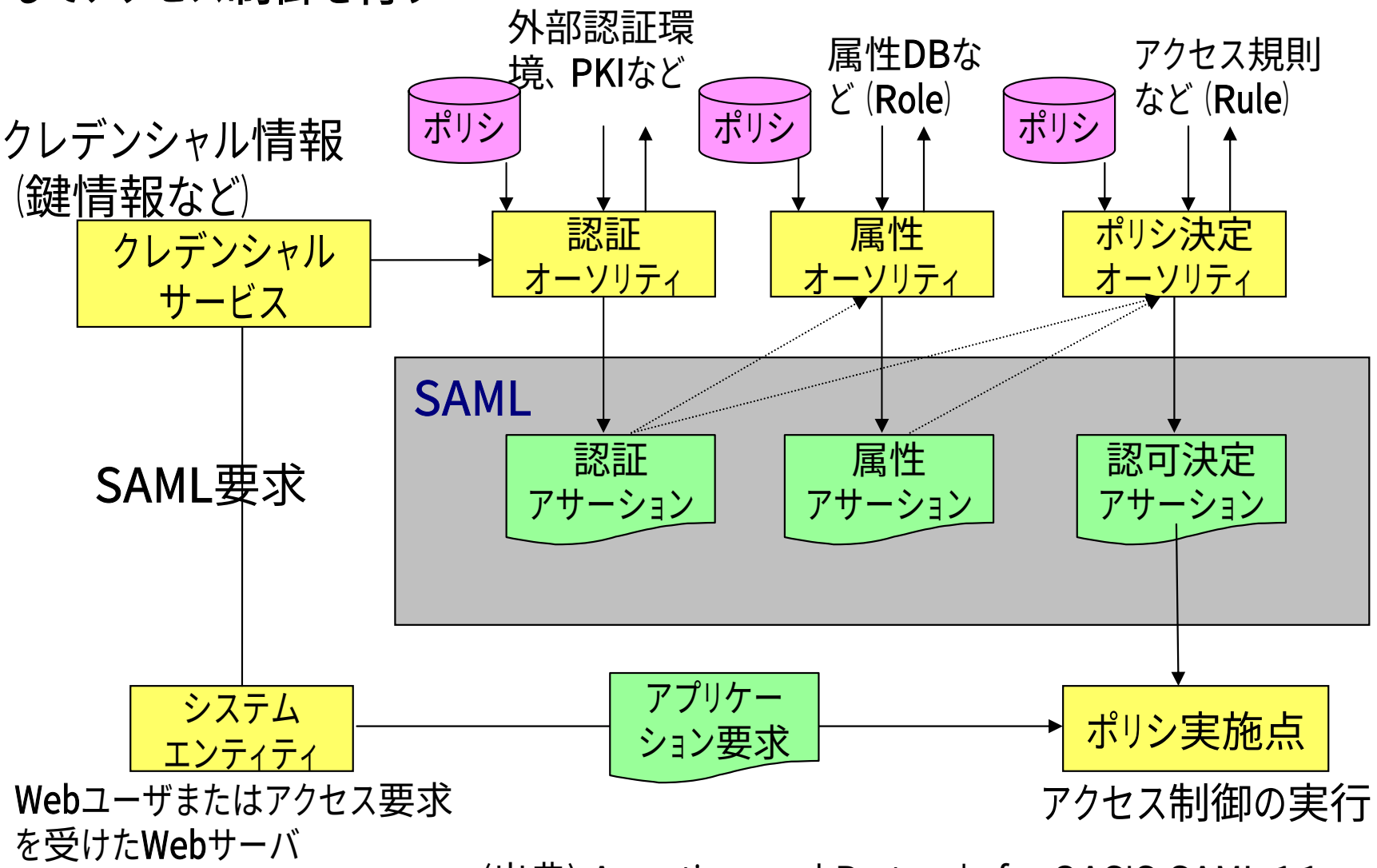
認証のチュートリアル
NIST SP800-63 電子認証ガイドラインの用語



認証のチュートリアル
SAMLの概念モデル

セコム IS 研究所
Intelligent Systems Laboratory

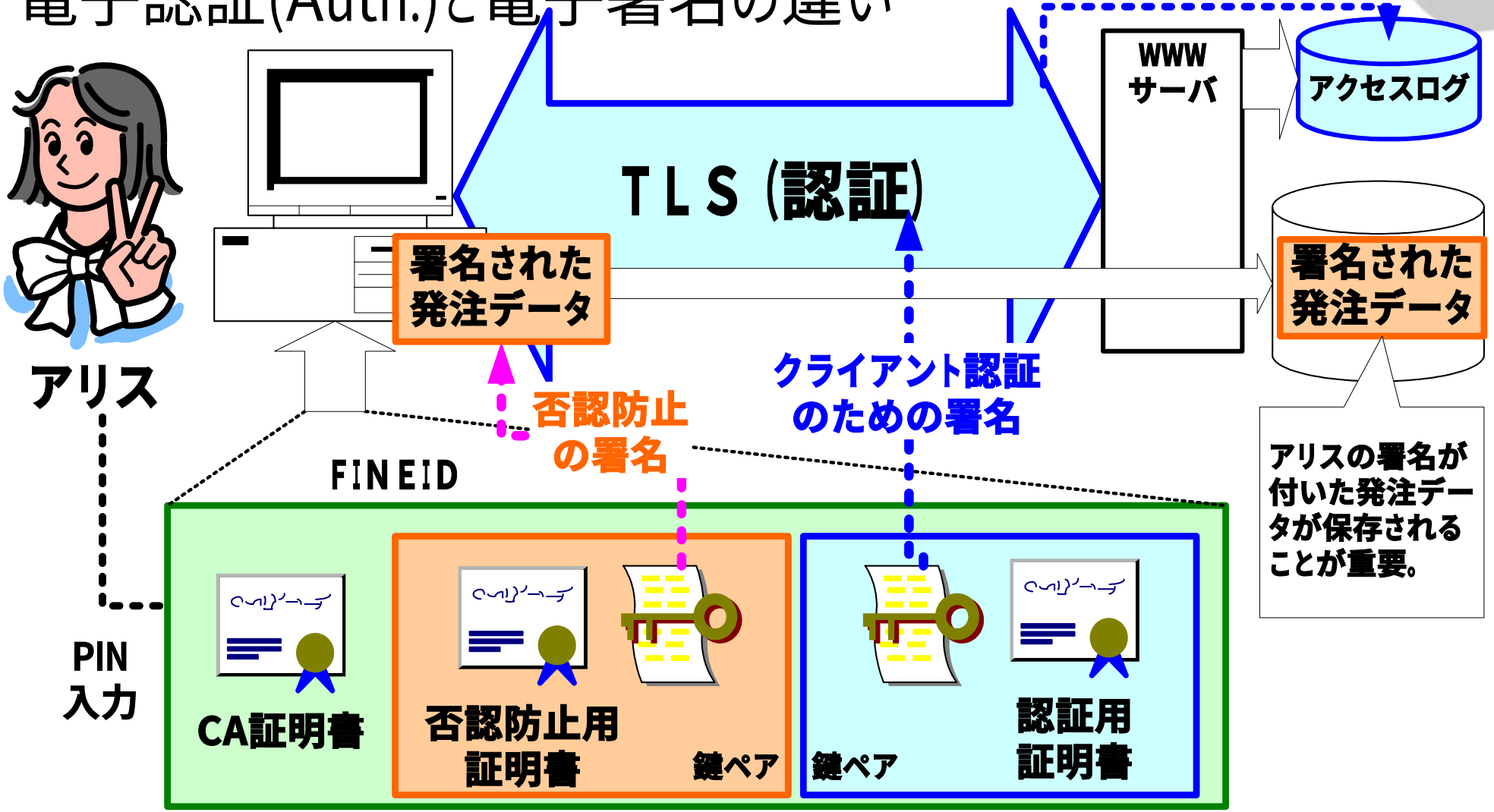
- 認証・属性・認可の結果を3種類のSAMLオーソリティがアサーションを発行してアクセス制御を行う



(出典) Assertions and Protocols for OASIS SAML 1.1

認証のチュートリアル
電子認証(Auth.)と電子署名の違い

セコムIS研究所
Intelligent Systems Laboratory



電子政府などでは、文書に署名され、署名された文書が保存されることが重要。欧州の市民カードは、2種類の証明書を使っている。

認証のチュートリアル
基本的な用語の理解

セコム IS 研究所
Intelligent Systems Laboratory

- CertificationとAuthentication
  - 共に「認証」と訳されることが多いが。。違う概念
  - Certification
    - 証明書により何らかの権威者が何事かを証明する
      - 会社が社員を。自治体が市民を。。
  - Authentication
    - 真正性の確認（正当な本人であることを確認する）
- 署名(Signature)と認証(Authentication)
  - 自然人による否認防止（Non Repudiation）の署名
    - 自分の意志で文書に対して内容を確認した上で署名　－ 自署名

認証のチュートリアル
電子認証(Auth.)と電子署名の違い

セコムIS研究所
Intelligent Systems Laboratory

	電子認証(Authentication)	電子署名(Signature)
手段	現状は色々な認証のメカニズムが乱立しておりユーザからは差が分らない(クライテリアが未整備)	電子署名はPKI以外の現実的な手段はない
法制度	現状、法制度との結び付きはなく、認証のレベルもバラバラ	電子署名法、e文書法など法制度との結び付きが深い
マーケット	比較的新しい業界に需要がある。今後のユビキタスネットワーク時代のユーザ認証、機器認証の需要は測り知れない	紙に依存した比較的レガシーな業界に需要が多い。効率化するために電子化、IT化を推進したいが電子署名などの敷居の高さが壁になっている。
普及の鍵	普及には新しいビジネススキームの創造が重要	普及には業務知識、そして効率化のためのＢＰＲが伴うことを理解する必要がある。
キーワード	ネットワーク上の安全、安心。ID管理、ID連携(Identity Federation)	e文書法対応、電子データ保存、電子契約、電子債権法(仮称)

同じPKIでも適用される業界、アプリケーションが大きく異なることが重要

現状の課題と今後の方向性
電子認証と電子署名の誤解

セコムIS研究所
Intelligent Systems Laboratory

- 平成12年施行の電子署名法の誤解??
  - 電子署名法 -> 紙文章における手書き署名や押印に対して、電子署名が同等の効力を持つ
    - このこと自体は非常に重要。既存の法制度の対応が目的
  - 電子署名法は、ネットワークにおける電子認証(Authentication)を促進している訳ではない。 – 技術的には、同じ技術(PKI)を使うが。。。
- 政府認証基盤(GPKI,LGPKI,公的個人認証サービス)の誤解??
  - 政府認証基盤(GPKI : Government Public Key Infrastructure) ― これは、電子認証(Authentication)の基盤ではない。やはり電子署名法の対応に重きを置いている。
  - 基本的には、否認防止の署名のための官職証明書(Certificate)を発行 – 官職に電子認証は不要。。。

現状の課題と今後の方向性
電子認証と電子署名の誤解

セコムIS研究所
Intelligent Systems Laboratory

- 電子署名
  - 電子社会への道　– そんなに簡単ではない….
  - 「紙と印鑑」の文化から「電子データと電子署名」の文化へ　– まずは、これまでの慣習の壁を越える必要がある
  - 透明性がありかつ効率的な社会の構築のためには電子署名は非常に重要な意味を持つ
    - これには変革も伴う。しかし、電子署名がなされた電子データは、これまでITの普及が困難だった業務を劇的に改善する可能性を秘めている。
  - #電子認証(Authentication)を当たり前に利用しているセキュリティ技術者は、意外に「電子署名」への理解がない。。。。
- 電子署名法特定認証業務認定制度
  - 良くも悪くも高い保証クラスの自然人に証明書を発行する認証局の認定。。。。
  - ユビキタス・ネットワーク時代に求められるのは、人による電子署名だけではない ー　電子署名法としては自然人は正しいが…

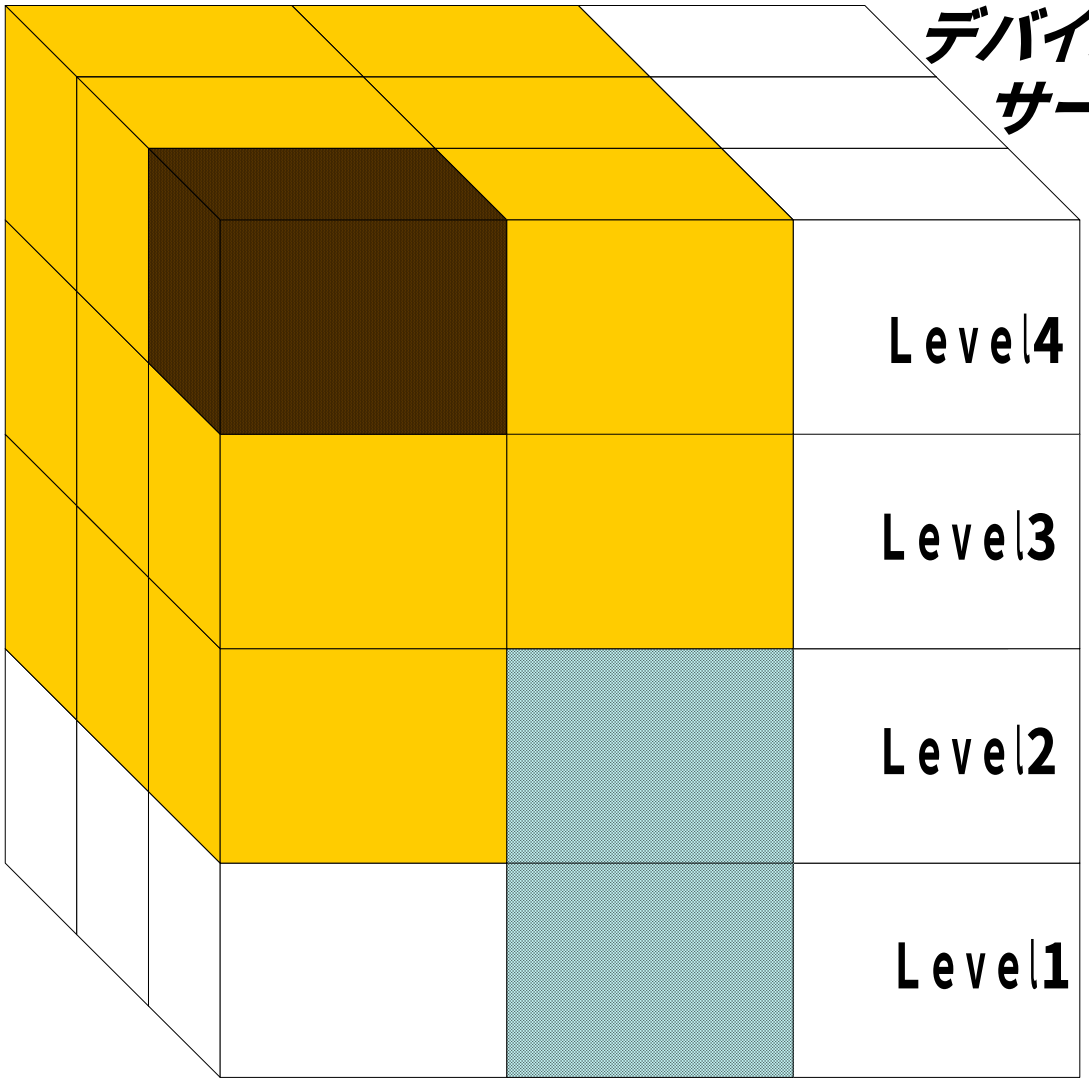
現状の課題と今後の方向性
電子認証と電子署名の誤解

セコムIS研究所
Intelligent Systems Laboratory

- **電子署名**の普及について
  - これまでところ普及しているのは、官の電子入札と、建設業界の電子契約
    - 強制力がある -> サービス – 顧客の関係ではない。。。
  - 電子署名は安全で便利だから普及するというよりは、法制度等からの**強制力**か、何らかの**インセンティブ**が必要
    - これは電子署名を使った提案には、業界に関する法制度とインセンティブ構造を理解していることが重要
  - 法制度のIT化対応はこれから。。。。(権利の電子化、証の電子化)
    - 電子署名法、e文書法等の通則法は、始まりにしか過ぎない。。。
  - ネットワークを使ったサービスというよりは、(保存な必要な) 紙から電子データの移行が重要 - 紙文書依存の業界がe-文書法で刺激されている。
- **電子認証**
  - ネットワーク上の安全、安心を提供するのは、むしろ電子認証。しかし実は、法制度、政策的なものは、なにもない??
  - 古い法律に縛られていない新しいビジネス(色々なインターネットサービス) の電子署名の要求は少ない。 -> 本来は、検討されるべきであるが。。。
  - しかし、高い付加価値のサービスを行うためには、**一定の保証レベル**を持った電子認証が必要

現状の課題と今後の方向性　－　電子署名法特定認証業務との既存の電子認証のギャップ

セコムIS研究所
Intelligent Systems Laboratory



高い保証レベル

低い保証レベル

電子署名法特定認証業務がカバーする領域

今後、社会的需要が大きいと思われる領域

現在、実際に多く使われている認証

現状の課題と今後の方向性
「元気・安心・感動・便利社会」を実現するアーキテクチャ

セコムIS研究所
Intelligent Systems Laboratory

感動、便利を提供するネットワークアプリケーション

個人情報を複数の組織が扱う 健康サービス

病病連携 病診連携 etc.. 医療APL

電子債権? Etc.. 金融APL

IP電話など P2P APL

--- Etc..

安全、安心を提供する電子認証基盤

技術
相互運用性
PKIなどセキュアな電子認証

ポリシー＆運用
本人確認手段などの基準
認証局など認定基準

ビジネスルール、基本的なビジネスモデル

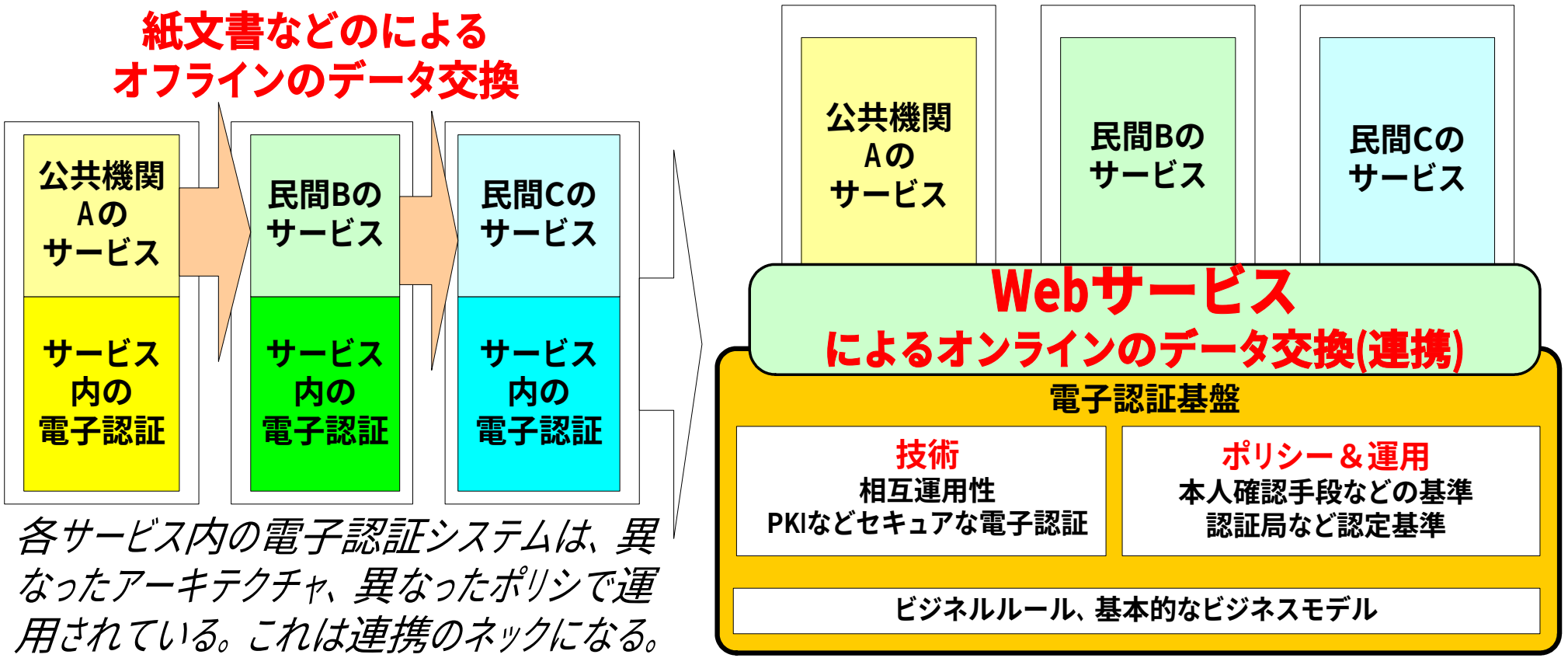
ネットワーク基盤のレイヤー

低価格なブロードバンドの普及
何処でも、何にでも、何時でもつながるユビキタスネットワーク

現状の課題と今後の方向性
「Webサービス」による連携と認証基盤

セコムIS研究所
Intelligent Systems Laboratory

–異なった公共機関や民間団体で連携が求められている
  –健康支援システム（ＥＢＨ:Evidence-Based-Health）、ワンストップ電子契約・電子調達、計算機リソースを共有するグリッドコンピュータ、etc　ー　これらの展開のためには、電子認証の連携も必須となる。

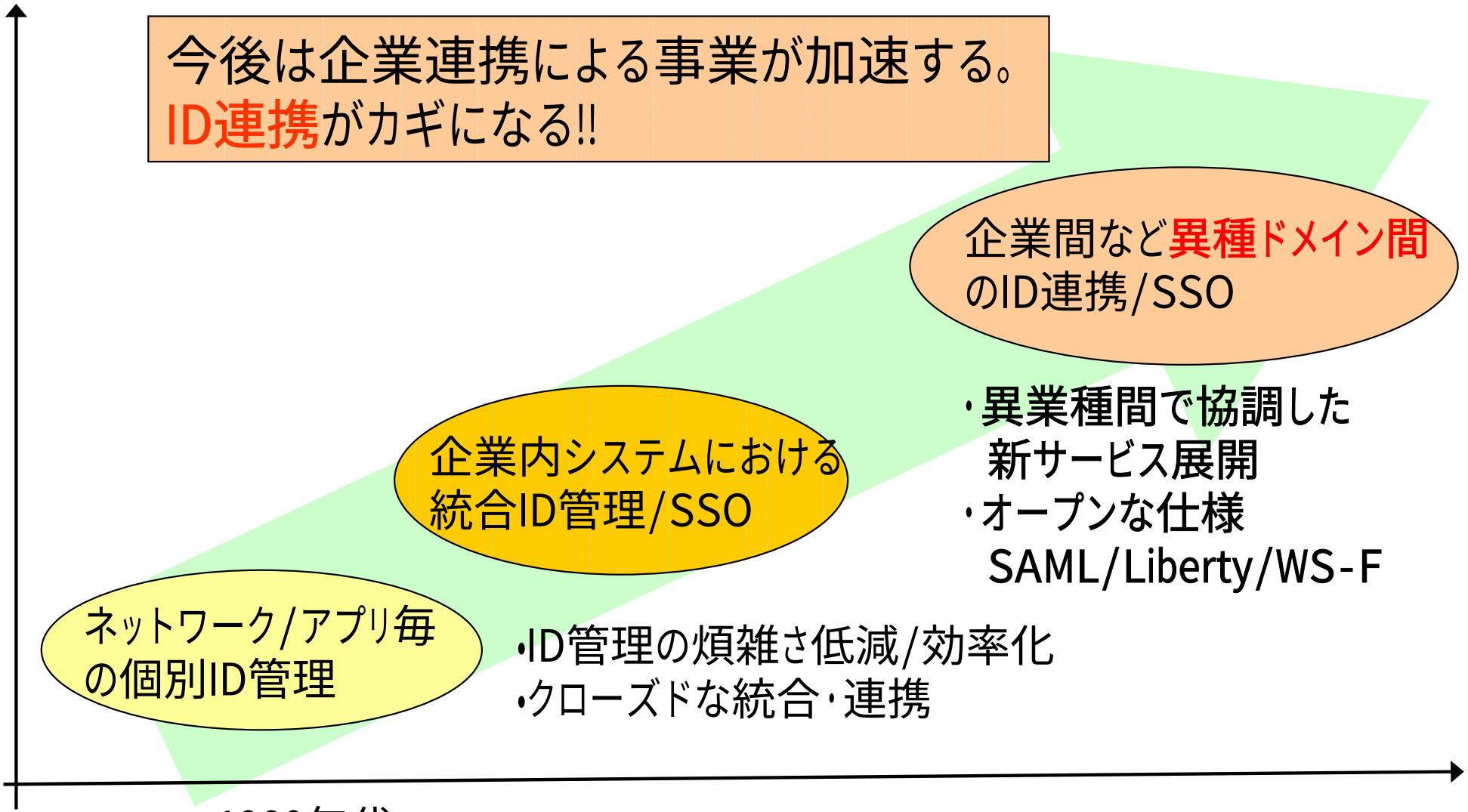


各サービス内の電子認証システムは、異なったアーキテクチャ、異なったポリシで運用されている。これは連携のネックになる。

現状の課題と今後の方向性
ID管理の変遷

セコムIS研究所
Intelligent Systems Laboratory

今後は企業連携による事業が加速する。
ID連携がカギになる!!



現状の課題と今後の方向性
セキュリティ・ミドルウェアの課題

セコムIS研究所
Intelligent Systems Laboratory

標準化、相互運用の課題

非常に複雑なセキュリティプロトコルの要求

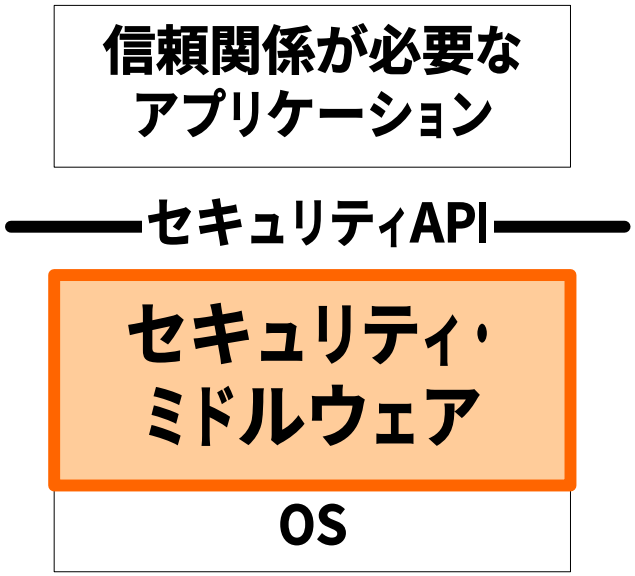
セキュリティに対応し切れていない標準化＆標準化組織

テスト環境、テストケース、相互運用テストが非常に重要だが、整備ができていない

実装上の課題

暗号技術等、基礎技術が、セキュリティ・フレームワーク＆ミドルウェアに組み込まれていかない
（日本の話し。。。。）

多くのバグが内在する可能性
(OpenSSLなどは典型的)



標準と実装のギャップ。何がどこまで正しく実装されているのか分からない。

複雑さを隠蔽するために、どんどん階層化されていく。そのことにより本質的な問題点も隠蔽されていく??

複雑さと問題点が集約されていく

米国のe-Authentication Initiativeの例

セコムIS研究所
Intelligent Systems Laboratory

- 米国電子政府のe-Authentication Initiative
  - 米国電子政府の最も重要な横断的イニシアチブのひとつ
  - 米国政府のEA(エンタープライズアークテクチャ) に対応した認証フレームワーク
  - 政府機関を横断したシングルサインオンの実現を目指している
    - SAML、Liberty Alliance などの技術を統合している
    - 複数のIDP(アイデンティティプロバイダー = 認証プロバイダー)、サービスプロバイダーが連携するモデル
  - 4つの保証レベルを定義
    - 脅威等に対応する保証レベルの認証を使い分け
    - PKI、パスワードなどの認証を保証レベルに応じて使い分け
- EAP (Electronic Authentication Partnership)
  - e-Authenticationイニシアチブのリソースを元に、官民、民民の連携のための電子認証スキームの確立を目指している

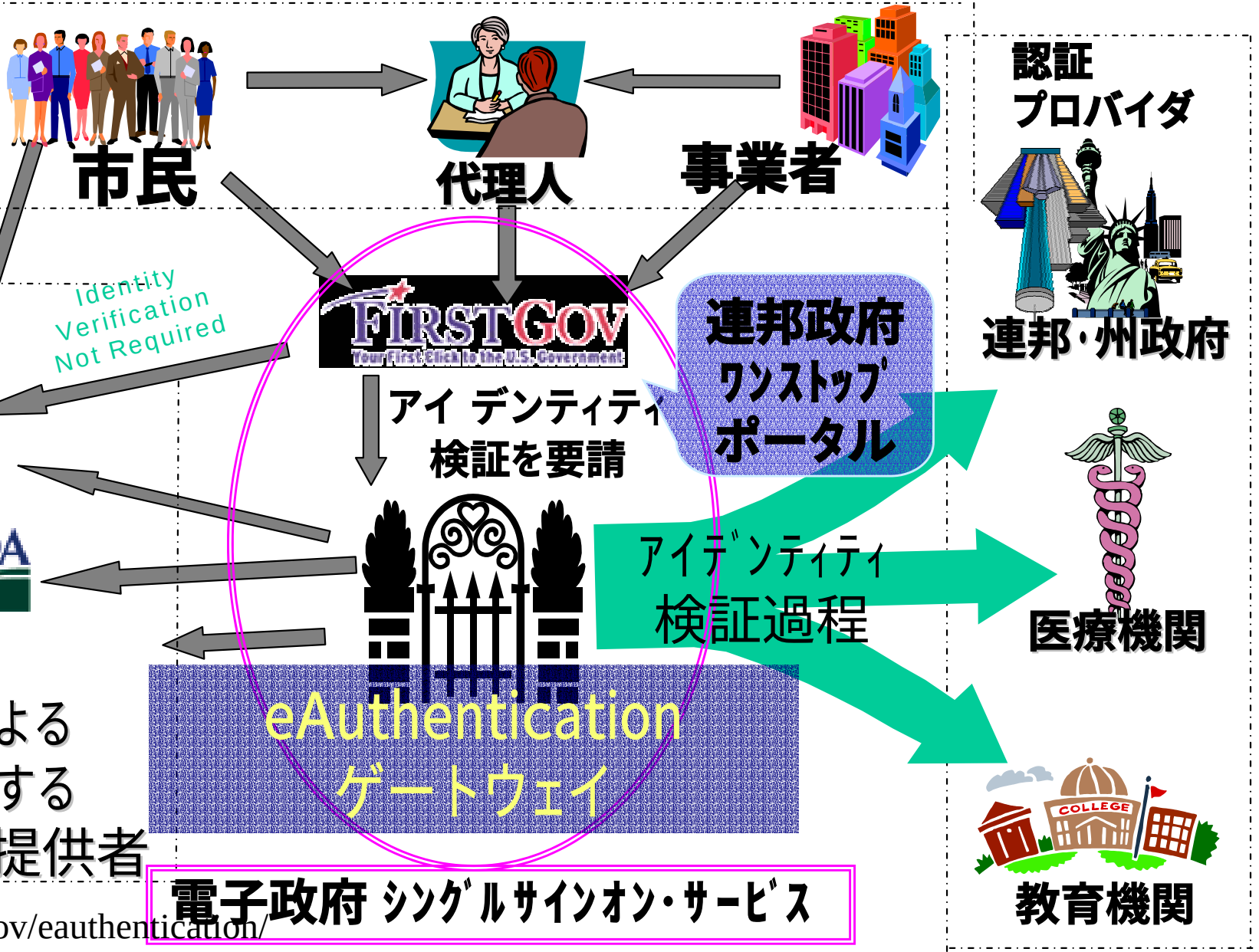
米国のe-Authentication Initiativeの例
米国電子政府の構成

セコムIS研究所
Intelligent Systems Laboratory

類型(ポートフォリオ)	目的	代表例＊
G2C（政府から市民に）	ワンストップ・サービス	Recreation one-stop (内務省)
G2B（政府から企業に）	企業負担の軽減。ワンストップ・サービス。XMLを使用したデジタル通信	One-stop business compliance （中小企業局)
G2G（政府から政府に）	連邦政府と、州、地方の政府との間の情報共有	Disaster Management (連邦緊急事態管理庁)
IEE（政府内部の効率と効果）	内部処理を合理化してコストを削減	E-Training (人事管理庁)
E-Authentication（電子認証）	民間企業、市民、政府の負担の軽減	全連邦機関共通の身元確認システム13を構築 (共通役務庁)

米国のe-Authentication Initiativeの例
米国電子政府のポータルとe-Authentication

セコムIS研究所
Intelligent Systems Laboratory



http://www.cio.gov/eauthentication/

米国のe-Authentication Initiativeの例
4つの保証レベル

セコムIS研究所 Intelligent Systems Laboratory

M-04-04:
e-Authentication Guidance for Federal Agencies
行政管理予算局(OMB)のガイダンスは4つの本人認証の保証レベルを確立

最低限の保証	低い保証	高い保証	最高の保証
レベル 1	**レベル 2**	**レベル 3**	**レベル 4**
Little or no confidence in asserted identity (**例** self identified user/password)	Some confidence in asserted identity (e.g. PIN/Password)	High confidence in asserted identity (**例 デジタル証明書**)	Very high confidence in the asserted identity (**例 スマートカード**)

NIST(国立標準技術研究所) SP-800-63
e-Authentication技術ガイドライン
NIST **技術ガイダンスはレベル実現に適合する技術を提示**

米国のe-Authentication Initiativeの例
NIST e-Authentication技術ガイドライン

セコムIS研究所
Intelligent Systems Laboratory

- NIST Special Publication 800-63
  - http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
- §7 アイデンティティ証明と登録、§8 認証プロトコルは、4つのレベル毎の記述になっている。
- 作者は、NISTのTim Polk、William BurrらFederal PKIの中心メバー

電子認証への勧告・目次

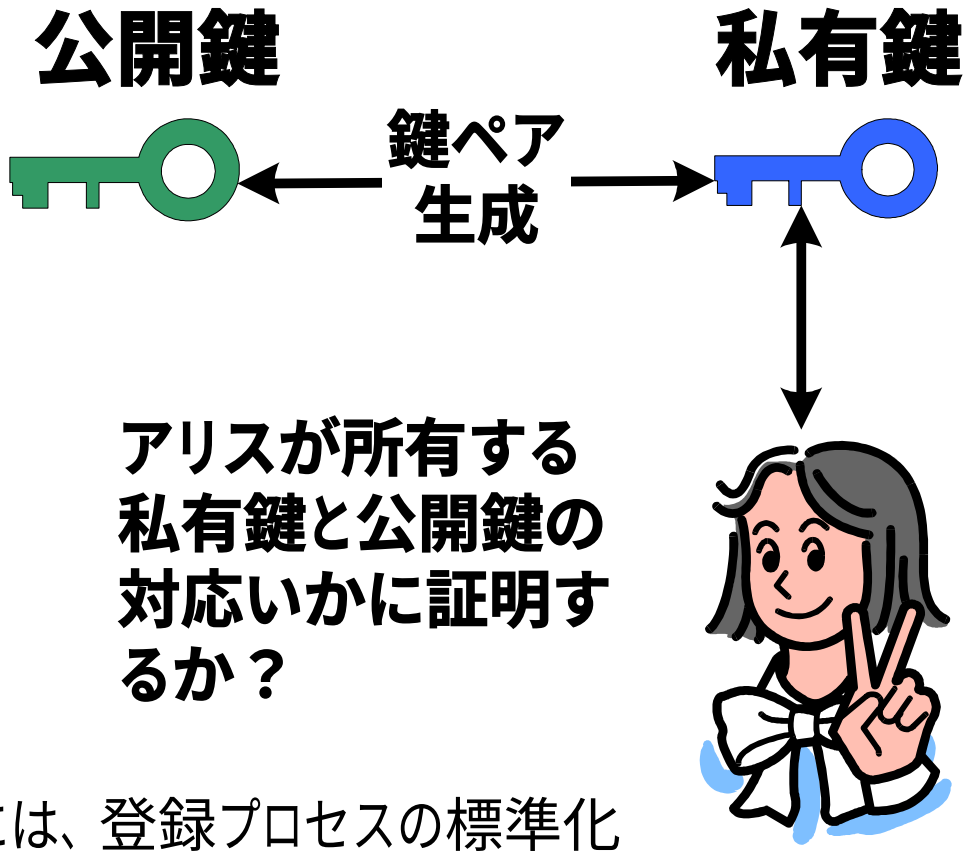
§1 目的
§2 オーソリティ
§3 導入
§4 定義と省略形
§5 電子認証モデル
§6 トークン
§7 アイデンティティ証明と登録
§8 認証プロトコル
§9 リファレンス
付録A パスワードのエントロピーと強さの推定

米国のe-Authentication Initiativeの例
SP800-63 アイデンティティ証明と登録
PKI的にはRFC 3647　4.3 識別と認証

セコムIS研究所
Intelligent Systems Laboratory

- ネーミングルール
  - 規約、解釈、ペンネームの可否．．．
  - ユニークであることの確保
- 識別、認証（個人、組織）
  - 本人又は組織の真偽の確認
  - 例：各種の公的証明書
- 初期登録／更新／失効後
  - 要求方法・手続
  - 認証方法・手続
- RFC 3647 4.3. I&A（識別と認証）
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html#043

POP: proof-of-possession
所有の証明



認証サービスを独立したサービスとするためには、登録プロセスの標準化や保証レベルといったことが最も重要な課題。。。

米国のe-Authentication Initiativeの例
NIST e-Authentication技術ガイドライン
各保証レベルでのトークンの種類

セコムIS研究所
Intelligent Systems Laboratory

トークンタイプ	レベル1	レベル2	レベル3	レベル4
ハードウェアの暗号学的トークン	○	○	○	○
ソフトウェアの暗号学的トークン	○	○	○	
ワンタイム・パスワード装置	○	○	○	
パスワード ＆PIN	○	○		

米国のe-Authentication Initiativeの例
保証レベルと認証技術の選択とE-RAツール

セコムIS研究所
Intelligent Systems Laboratory

**OMBの電子認証ガイダンスは、
政府を横断した電子認証の
一貫性のあるアプリケーションのために
4つの保証レベルを確立する**

レベル1	レベル2	レベル3	レベル4
Little or no confidence in asserted identity (e.g. self identified user/password)	Some confidence in asserted identity (e.g. PIN/Password)	High confidence in asserted identity (e.g. digital cert)	Very high confidence in the asserted identity (e.g. Smart Card)

E-RAツールは、認証要求を定義して、それらを適当な保証レベルにマップする機関をアシストする

NIST e-Authentication 技術ガイドラインは、保証レベルに合った認証技術のガイドラインを提供

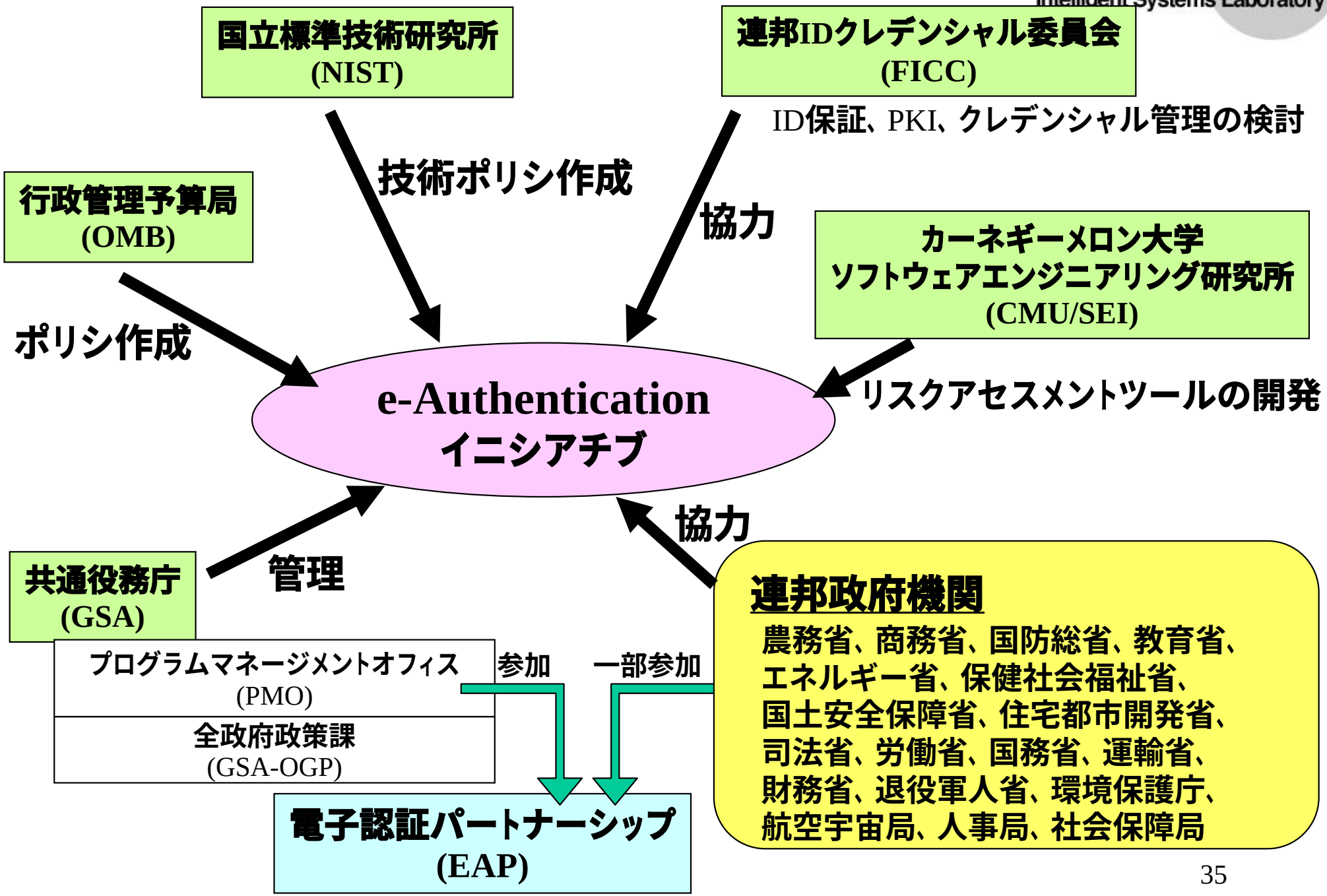
E-RA ツール ：E-Authentication Risk Assessment tool

米国のe-Authentication Initiativeの例
４つの保証レベルと認証プロバイダ

セコム IS 研究所
Intelligent Systems Laboratory

認証プロバイダ名	レベル	タイプ	備考
国防省PKIレベル4	4	PKI	
財務省PKIレベル4	4	PKI	
米国航空宇宙局(NASA)	3	PKI	
イリノイ州	3	PKI	
国民金融センター(USDA)	3	PKI	http://sig.nfc.usda.gov/pki/
農務省電子認証サービス	2	パスワード	WebCAAF (Web-based Centralized Authentication and Authorization Facility).
全米科学財団のFastLane	1	パスワード	オンライン研究補助金応募・審査システム

米国のe-Authentication Initiativeの例



米国のe-Authentication Initiativeの例
EAP (Electronic Authentication Partnership) の方向性

セコム IS 研究所
Intelligent Systems Laboratory

連邦政府

州政府・自治体

産業界

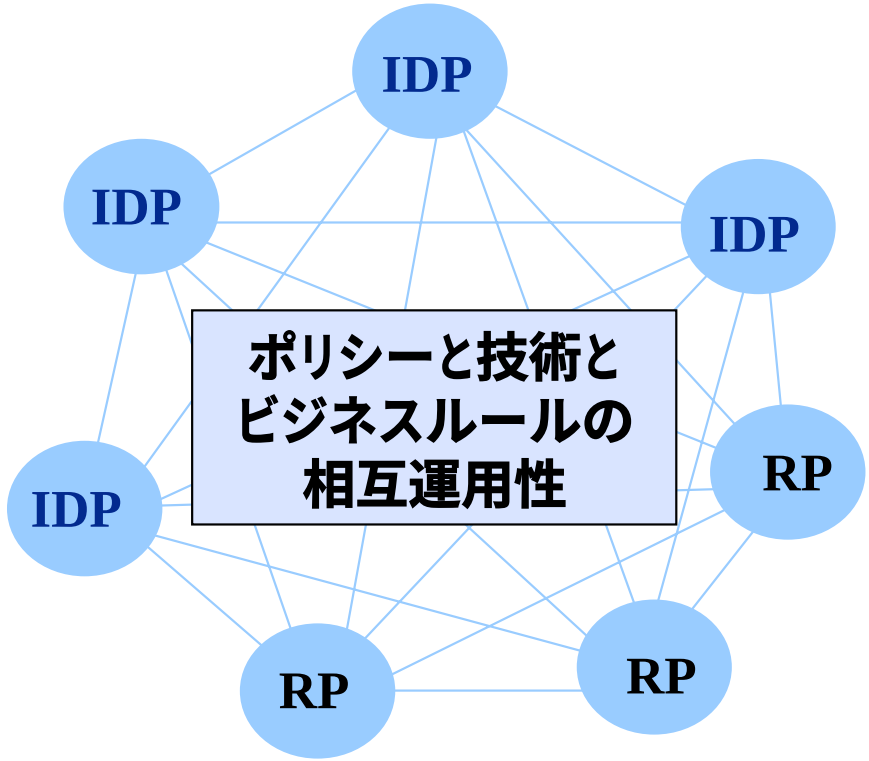
相互運用性

ポリシ
- 認証 (認定)
- 保証レベル
- プロファイル
- 認定
- ビジネスルール
- プライバシ・方針

技術
- Adopted schemes
- 共通仕様
- ユーザインターフェース
- API
- 相互運用性
- 商用製品
- 認可のサポート

商用の信頼保証サービス

共通のビジネスと運用のルール



http://www.eapartnership.org/

RP: Relying Party

出展: http://www.eapartnership.org/docs/EAP_Temoshok_2-12-04.ppt

まとめ　日本において検討すべき項目

セコムIS研究所
Intelligent Systems Laboratory

- 電子署名・電子認証の利活用を進めるには、組織・業態を超えた検討の場が必要
- 電子署名と電子認証の違いを理解して、それぞれの普及と利活用を目指すべき
- ユビキタスネットワーク時代の人、サーバ、デバイスが「どこでも、いつでも、何でも」接続される。この信頼をどう確立するか検討が必要
  - 人口よりもはるかに多い認証を要するデバイス
  - 人間が行なうよりもはるかに多いサーバによる署名
  - これらは、これまでの「電子署名法」などの枠組みだけではカバーできない。新たな枠組みが必要。

まとめ　日本において検討すべき項目　続き

セコムIS研究所 Intelligent Systems Laboratory

- 電子認証のクライテリアの整備
  - 個々の業界、管轄官庁に閉じた業界の電子認証への取り組みはあるが、これでは、連携ができない。「NIST e-Authentication 技術ガイドライン」に見られるような認証技術のクライテリアの整備がいそがれる
- ID連携(Identity Federation)
  - 組織内に閉じたこれまでの電子認証では、組織を超えた連携は困難。
  - ID連携が可能な電子認証基盤は、ビジネスの連携、官民の連携を加速する。
- Webサービス時代への対応
  - ネットワーク上での連携が求められている。有望な技術としてWebサービスがあるが、Webサービス自体も電子認証の連携が求められている。
  - 業界などを超えた、ID連携には、技術的な相互運用性だけではなく、ポリシー＆運用も含めた相互運用が重要

「認証技術の動向」セミナー

セコムIS研究所
Intelligent Systems Laboratory

- 「SAML の基本技術・実装技術」
  - 日本電気株式会社　ソリューション開発研究本部システム基盤ソフトウェア開発本部　遠藤　由紀子氏
  - ID連携とSAML
- 「電子認証基盤の技術動向」
  - 富士通株式会社　ソフトウェア事業本部　冨高 政治氏
  - 認証(Authentication)、認可(Authorization)、管理 (Administration)、監査・監査証跡　(Audit & Audit Trail)を中心に説明。
- 「IPアドレス認証局」
  - 社団法人 日本ネットワークインフォメーションセンター技術部インターネット基盤企画部　セキュリティ事業担当　　木村　泰司氏
  - インターネットのレジストリ情報の信頼性向上
  - アドレスブロックの証明書
- 「通信プロトコルの認証技術」
  - 松下電工株式会社 新事業企画室　福田　尚弘氏
  - 認証プロトコルの動向など

参考

セコムIS研究所
Intelligent Systems Laboratory

- マルチドメインPKI相互運用性プロジェクト- JNSA Challenge PKI
  - http://www.jnsa.org/mpki/index_j.html
- セコムIS研究所　サイバーセキュリティ読本
  - http://www.secom.co.jp/isl/j/cs_reader/index.html
  - PKI/電子署名と認証
    - http://www.secom.co.jp/isl/j/cs_reader/pki/digitalsignature/page01.html
      - 電子署名用証明書と認証用証明書の分離の必要性を説明している
  - Webサービス
    - Webサービスをセキュリティの観点から説明している
- 米国 e-authenticationのホームページ
  - http://www.cio.gov/eauthentication/
- 米国 電子認証パートナーシップのホームページ
  - http://www.eapartnership.org/