2002年7月24日

わが国の電子署名制度の発展の課題

須藤　修

Osamu Sudoh

Professor, phD.

The University of Tokyo

東京大学大学院情報学環教授

東京大学社会情報研究所教授

1 IT革命がもたらすもの

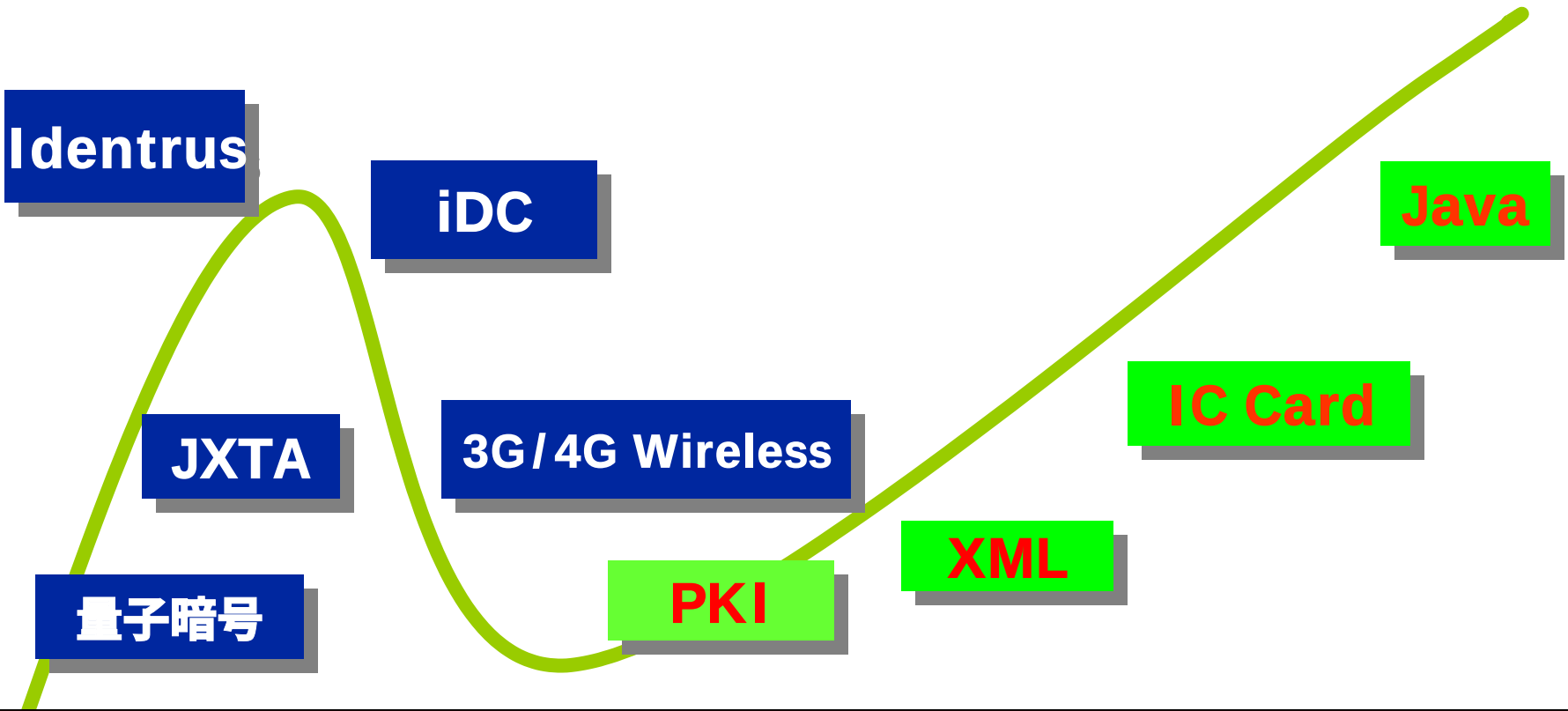
- ✓「デジタル革命はまだ始まったばかりだ。これから歴史を画する巨大なパラダイム･シフトが起こる。それは産業革命を凌ぐものになるだろう。」（アメリカ合衆国政府商務省）
- ✓不況を乗り越え、IT革命は第2段階に入った。
- ✓知識を活発に交流させながら民主的に進化していく「知識社会」の創造

インターネットと地域社会発展

- Silicon Valley（USA）
- Seattle（USA）
- Greater Washington（USA）
- Austin (Silicon Hills)（USA）
- Helsinki (Finland)
- Munich (Germany)
- Heidelberg (Germany)
- Singapore
- Greater Tokyo Area

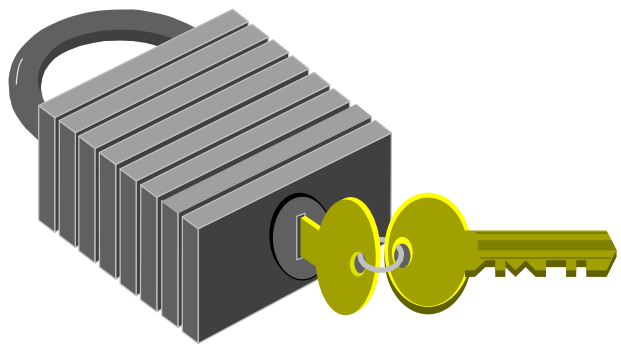
経験則：ムーブメントの波

- 新しい動向は普及・定着するまでに一度落ち込みを経験する！



2　セキュリティと認証

- 電子取引を本格的に実用化するには確実で安全性の高いICカード･システムを導入する必要がある。→暗号鍵の保管



What is Identrus ?

日米欧主要金融機関が出資･参加する電子認証プロジェクト

～ 世界的に汎用性のある電子認証サービスの提供を目指す

■ アイデントラス社(Identrus LLC, 本社 ニューヨーク)

･加盟金融機関共通の認証局運営ルールを制定

･世界標準の技術をもとにシステム要件を策定

･加盟金融機関を認証する最上位(ルート)認証局を運営

■ 加盟金融機関

･アイデントラスの仕様に準拠した電子認証局を運営

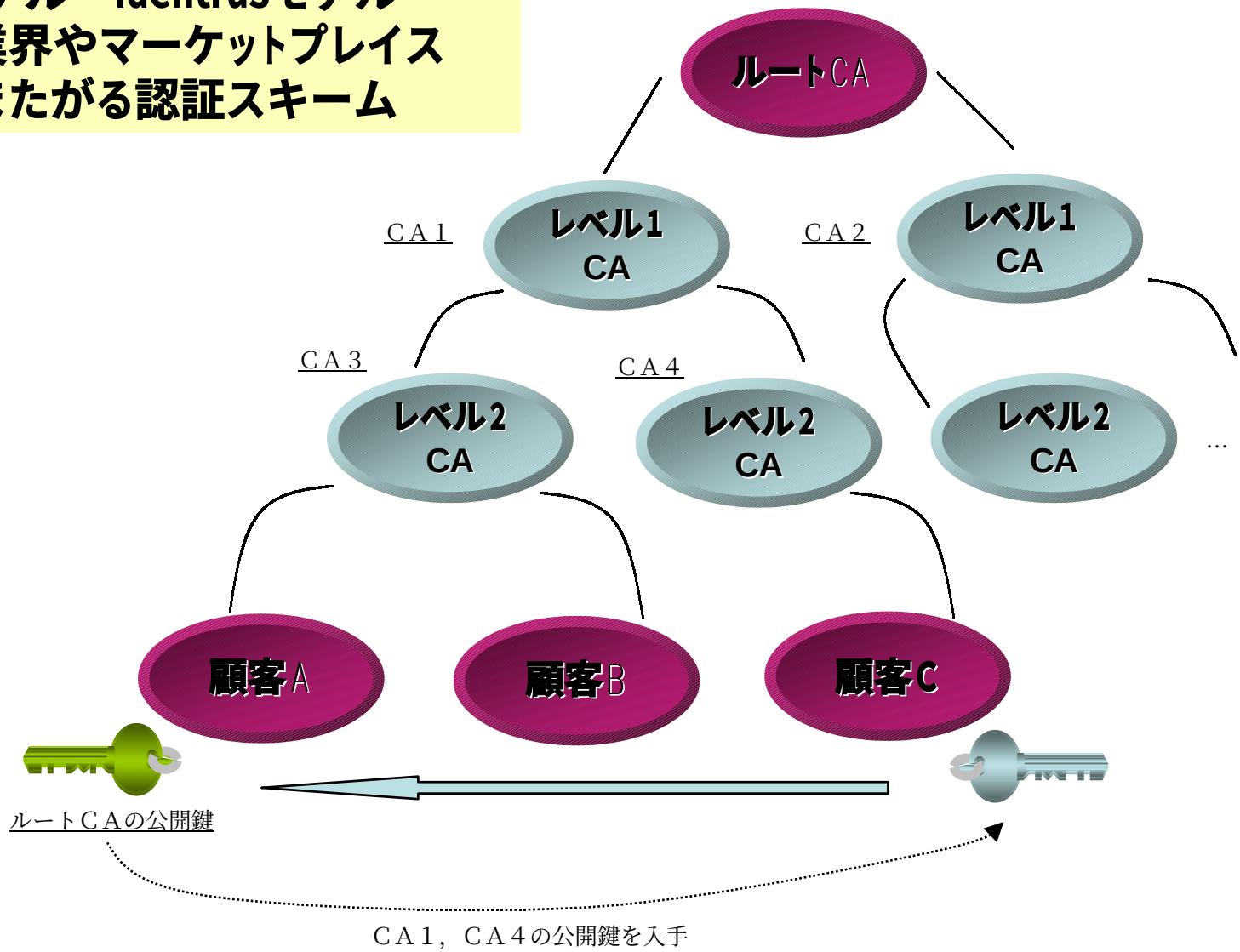
･アイデントラス規格のデジタル証明書を顧客企業に発行

･現在、金融機関６１社、ベンダー１５社が参加している。日本では邦銀に対してセコムが重要な役割を担っている。

認証モデル

Source：SUN Microsystems

階層型モデル＝Identrusモデル
・複数の業界やマーケットプレイス
各国にまたがる認証スキーム



Identrus

- Bank to BusinessとBusiness to Businessの**枠組みにおける組織属性認証と担当者属性認証を基本にする。**
- B2G**もサポートする－中央銀行及び指定金融機関**

3 電子政府・電子自治体とセキュリティ

- e-Japan戦略（2001年1月）
  - 2005年に世界最先端のIT国家になるための国家戦略
  - 電子政府の構築がそのための施策のひとつとして挙げられている
  - 電子申請や電子調達が全面的に可能になる環境を2003年に実現

E-Government Project in USA

◆連邦政府の取り組み

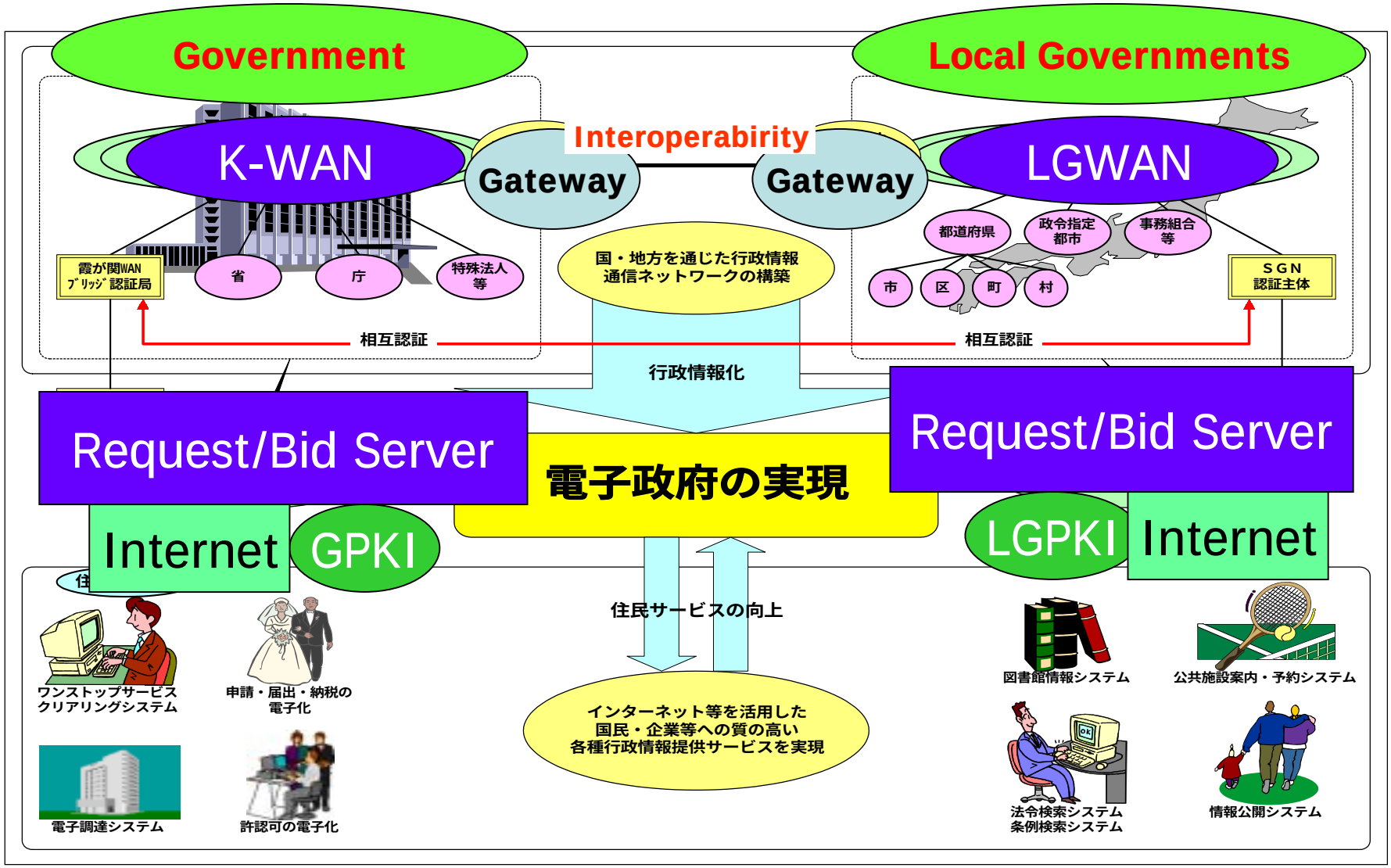
- ✓ Homeland Securityというコンセプトのもとに包括的なセキュリティ政策を構想。
- ✓ 国土安全省の創設（17万人規模）
- ✓ E-Gov：OMB (Office of Management and Budget)
- ✓ Federal PKI Steering Committee ：「2003年10月までにPKIを整える。さまざまなPKIをブリッジ認証局によって統合する方針である。」

Local E-Government in USA

◆サンホセ市役所（San Jose City Government）

- ✓私が見た限りにおいて最も先進的な取り組みを行っている。
- ✓PKIを基盤にした電子調達、電子申請を早くから実施している。
- ✓庁内各部局横断的な組織改革と技術標準化を行い、縦割りの弊害を克服している。

電子政府・電子自治体の基盤



電子自治体推進パイロット事業

- 2001年度より全国市町村の協力を得て、インターネットを活用した申請･届出等手続のための汎用システムを構築し、その利便性・有効性に関する検討を行う。
- 地方公共団体が規模・能力等にかかわらず住民サービスを行うことが可能となるよう、参加市町村が共同で利用できるシステム（ASP方式等）を構築し、申請･届出等手続のオンライン化を実施する。

地方公共団体における個人認証サービス

制度の仕組み

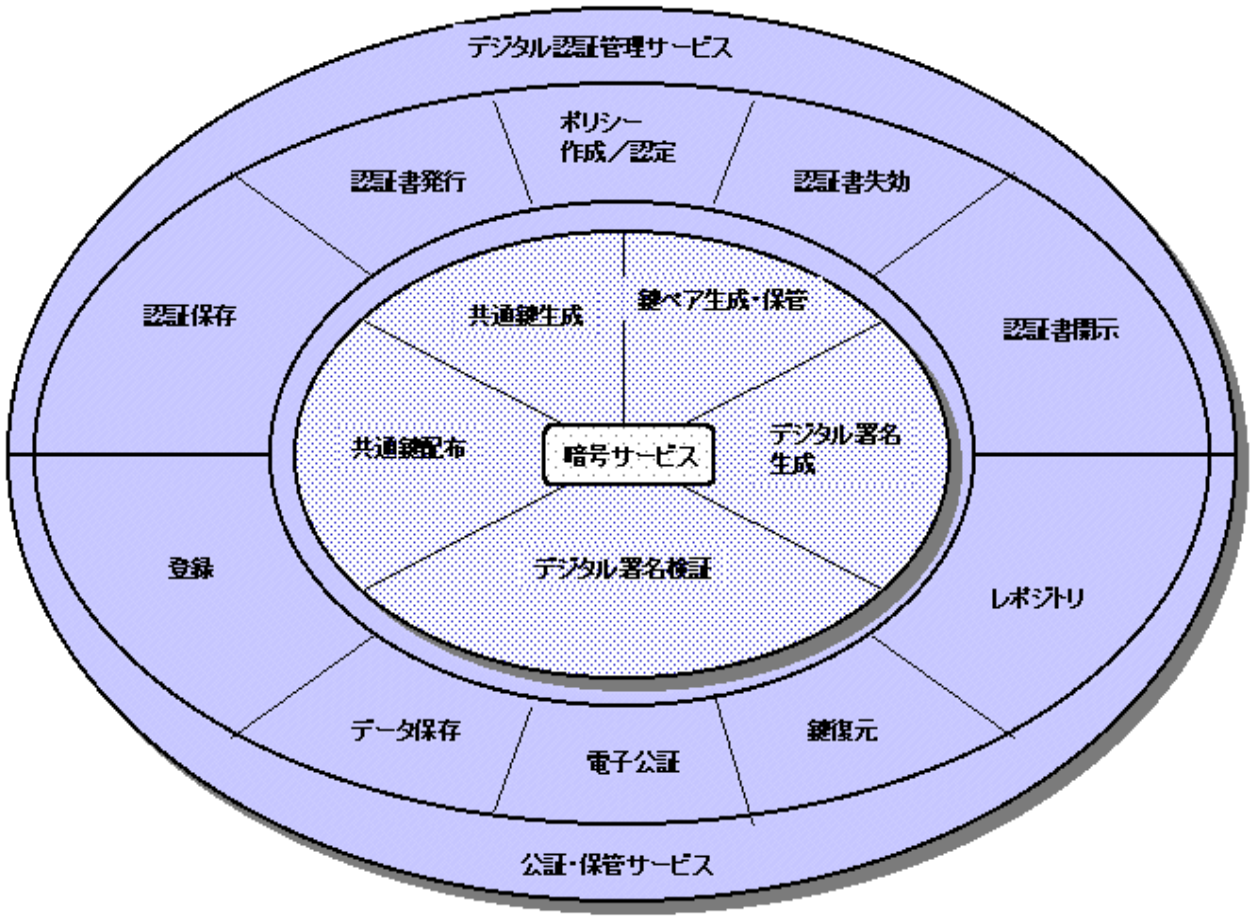
- 非対称鍵暗号方式による電子署名
- 本人確認機関：市町村
- 電子証明書発行機関：都道府県
- 電子証明書発行を受けることが出来る者：住民基本台帳に記録されている者
- 署名検証者：行政機関等、特定認証業務を行う民間認証事業者

地方公共団体における個人認証サービス

個人情報保護を最大限尊重する。

- ＯＥＣＤ８原則を遵守
- 実在証明のみ：氏名、生年月日、性別、住所
- 鍵ペアは利用者本人が作成し、秘密鍵のアーカイブシステムは採用しない。
- 電子証明書を受け取る署名検証者は、行政機関に限定する。
- 利用者から受け取った電子証明書を電子署名検証以外で利用することを禁止する。

認証局の業務



公開鍵基盤の構成

認証局運用ガイドラインV1.0版平成10年3月
電子商取引実証推進協議会認証局検討WG

公共事業における電子調達

電子調達：以下の３つの事柄からなる。

- **電子入札**
- **電子納品**
- **電子認証**

電子入札の動向：国土交通省の取組み

- フェーズ１（1996年ー1998年）
- 全職員のパソコン、インターネット利用環境整備
- 実証実験の開始
- フェーズ２（1999年ー2001年）
- 一部工事等に電子調達システムを導入
- 成果品の電子納品を開始
- 建設ＣＡＬＳ／ＥＣ推進本部の設置――2000年10月20日（本部長：事務次官）
- フェーズ３（2002年ー2004年）
- 旧建設省直轄事業のすべてのプロセスにＣＡＬＳ／ＥＣを実現
- それ以降（2005年ー2010年）
- 2010年までに地方自治体を含めたすべての公共発注機関においてＣＡＬＳ／ＥＣを実現

電子入札の動向：国土交通省の取組み

入札情報サービス

- 2001年4月より、国土交通省直轄事業において発注予定情報、発注情報、入札結果を一元的に集約、格納し、検索きる入札情報サービスの運用が開始された。

電子入札

- 2001年10月より一部の国土交通省直轄事業に採用される。
- 競争参加資格の確認申請／確認結果の通知／入札執行／札結果の通知／再入札など
- 公共調達電子認証局は、電子署名法にもとづく認定認証業者が行う。

成果物の電子納品

- 調査、設計、工事などの各業務段階の最終成果を電子データで納品する。

電子入札の動向：国土交通省の取組み

電子納品適用範囲

- 業務：河川事業、道路事業、公園事業、営繕事業
- 工事：暫時適用範囲を拡大する予定である。
- 2001年　３億円以上
- 2002年　２億円以上
- 2003年　６000万円以上

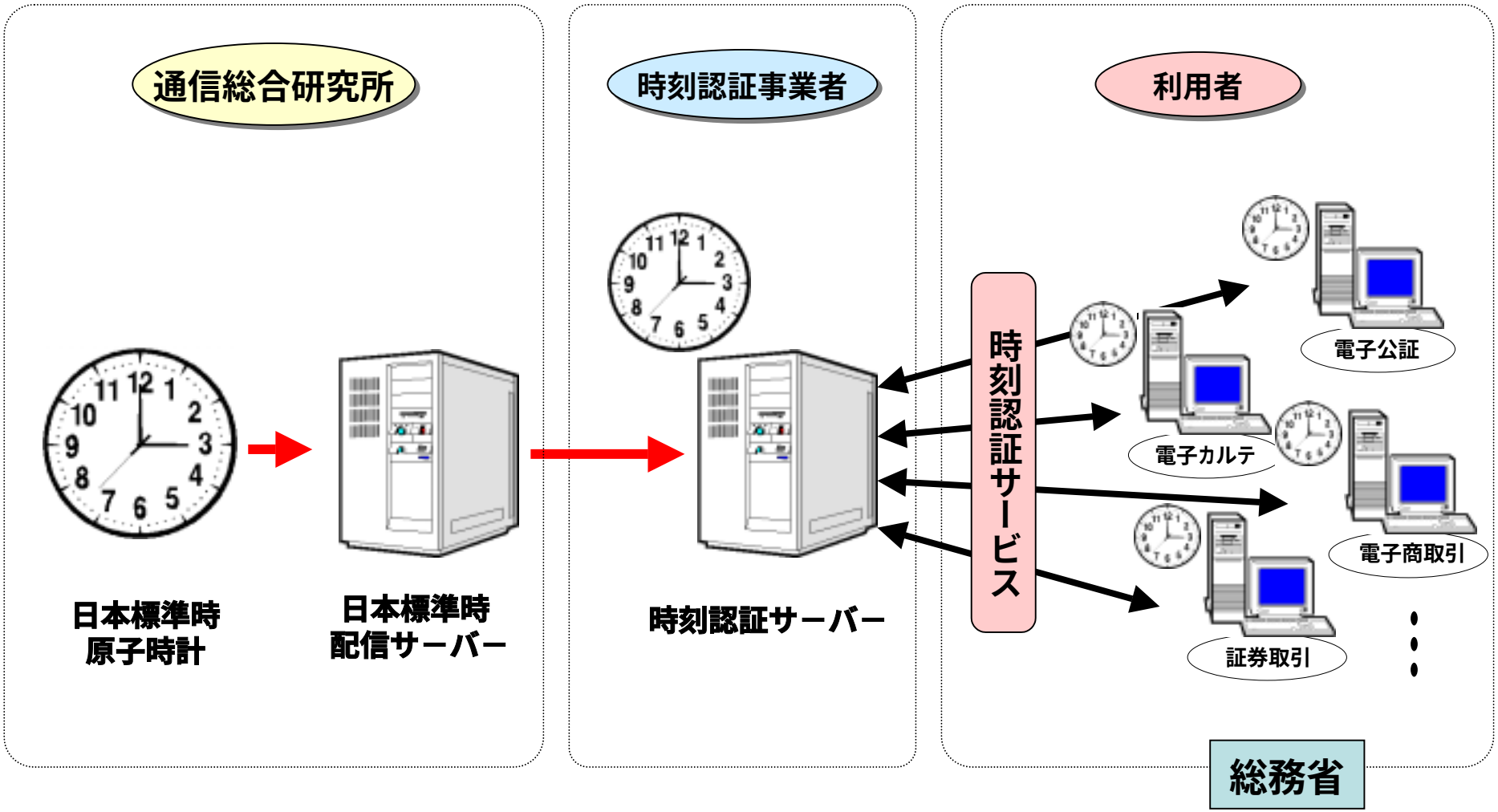
厚生労働省の電子申請実証実験

- 2001年度に労働災害申請に関して実証実験を行った。
- 2002年３月に報告書が公表される。
- 多重認証の処理方法等について有意義な検討がなされた。

厚生労働省の電子申請実証実験

- ✓ 申請方式、認証機能は実際の申請様式に即した組み合わせが必要である。
- ✓ 現在、行政の窓口で対面コミュニケーションにより解決されている申請内容の確認や職権訂正といった機能を、電子申請で実現する方法が必要である。
- ✓ 国民の利便性と申請の安全性の調和点を発見することの困難性。
- ✓ その他多くの解決すべき課題が明らかになった。

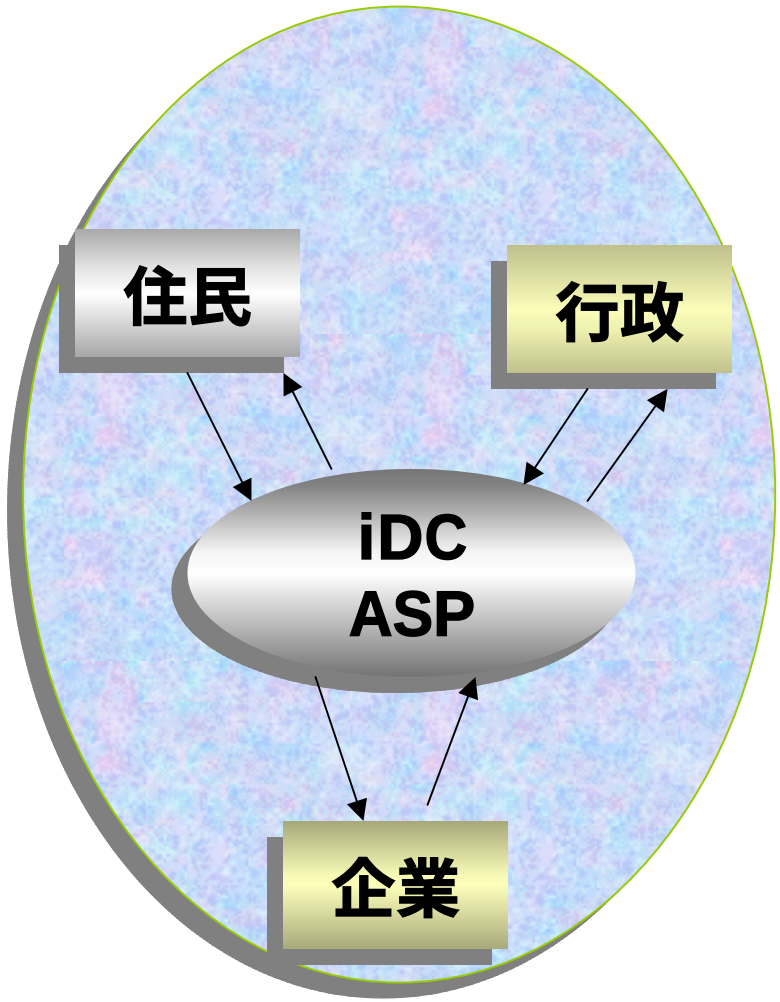
標準時配信・時刻認証サービスのイメージ



電子地域コミュニティの創造

Web Based Community

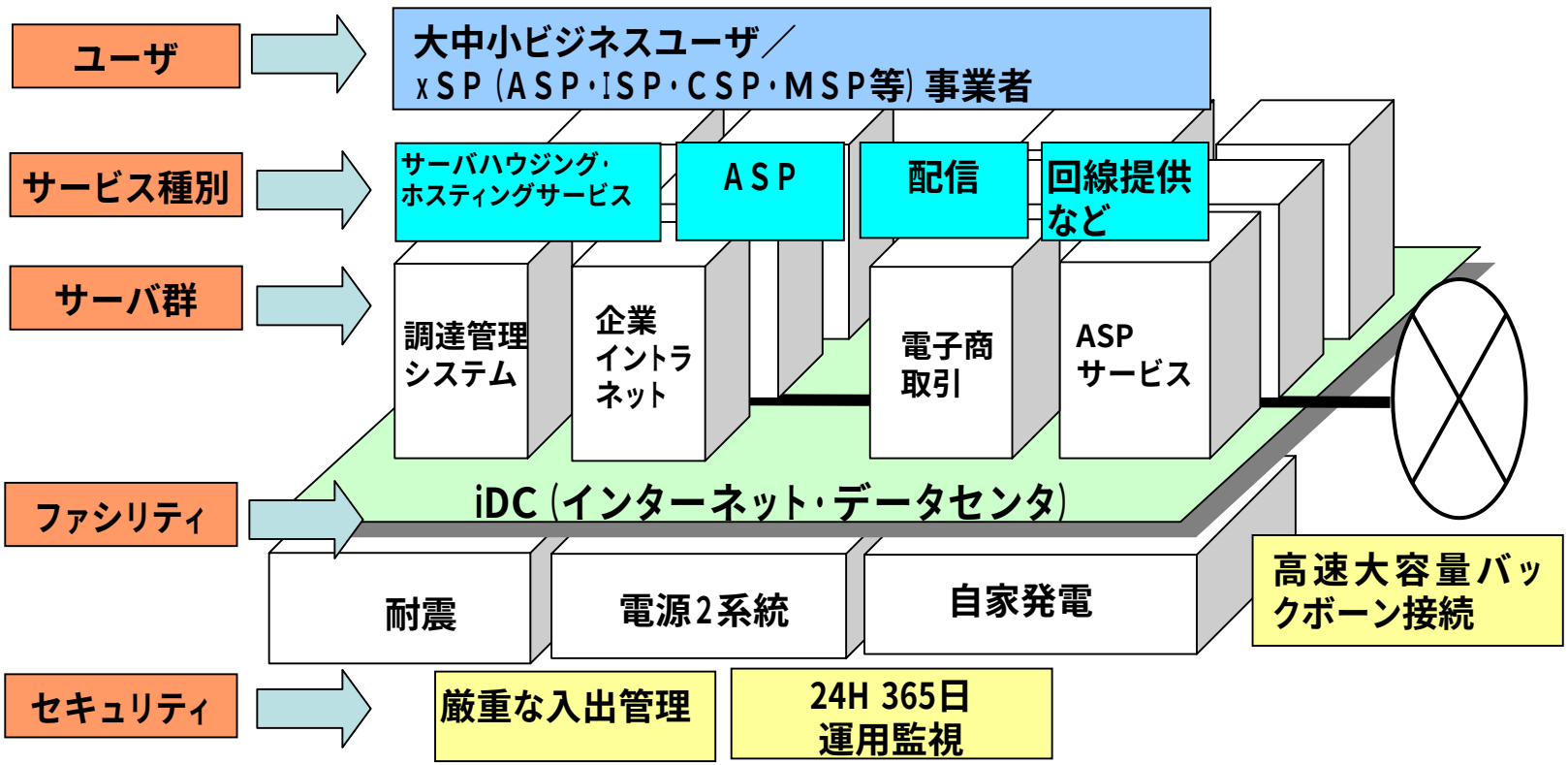
- 地方行政システムの官民による共同整備・共同運営（ASPなど）
- IT人材の養成とe-Learning
- 地域ポータルサイト



iDC（Internet Data Center）

資料：iDCイニシアティブ

セキュリティが高い環境を、低コストで利用でき、即座にインターネットビジネスが始められるために、災害に強く監視体制も整備された建物で、顧客のサーバ等のコンピューター式を預かったり必要なハードウェア・ソフトウェアを貸し出したりするビジネス拠点



ドイツにおける第三者監査

- TUVIT、デービス、BSIなど

  ソフトウェア品質検査、情報セキュリティ検査、設計検査、証明書発行業務などを行う。
- 情報セキュリティの証明：EU基準にもとづいて行われる。**認証機関の第三者監査！**
- CAビジネスのコンサルティングも行う。
- ドイツでは秘密鍵はICカードに保管される。したがってICカードの検査も行う。
- 99年にドイツテレコムが民間CA第1号を設立した。

多機能ICカード

- eCommerceへの対応
- mCommerceへの対応
- 電子行政化への対応
- ITS･ETCの整備普及
- ＪＩＣＳＡＰ
- ＮＩＣＳＳ
- ＥＣＳＥＣ

ご静聴ありがとうございます。
Thank you so much for your attentions !

Osamu Sudoh
Professor, ph.D.
The University of Tokyo
sudoh@isics.u-tokyo.ac.jp