安心・安全な社会へのICT技術

中央大学

大橋　正和

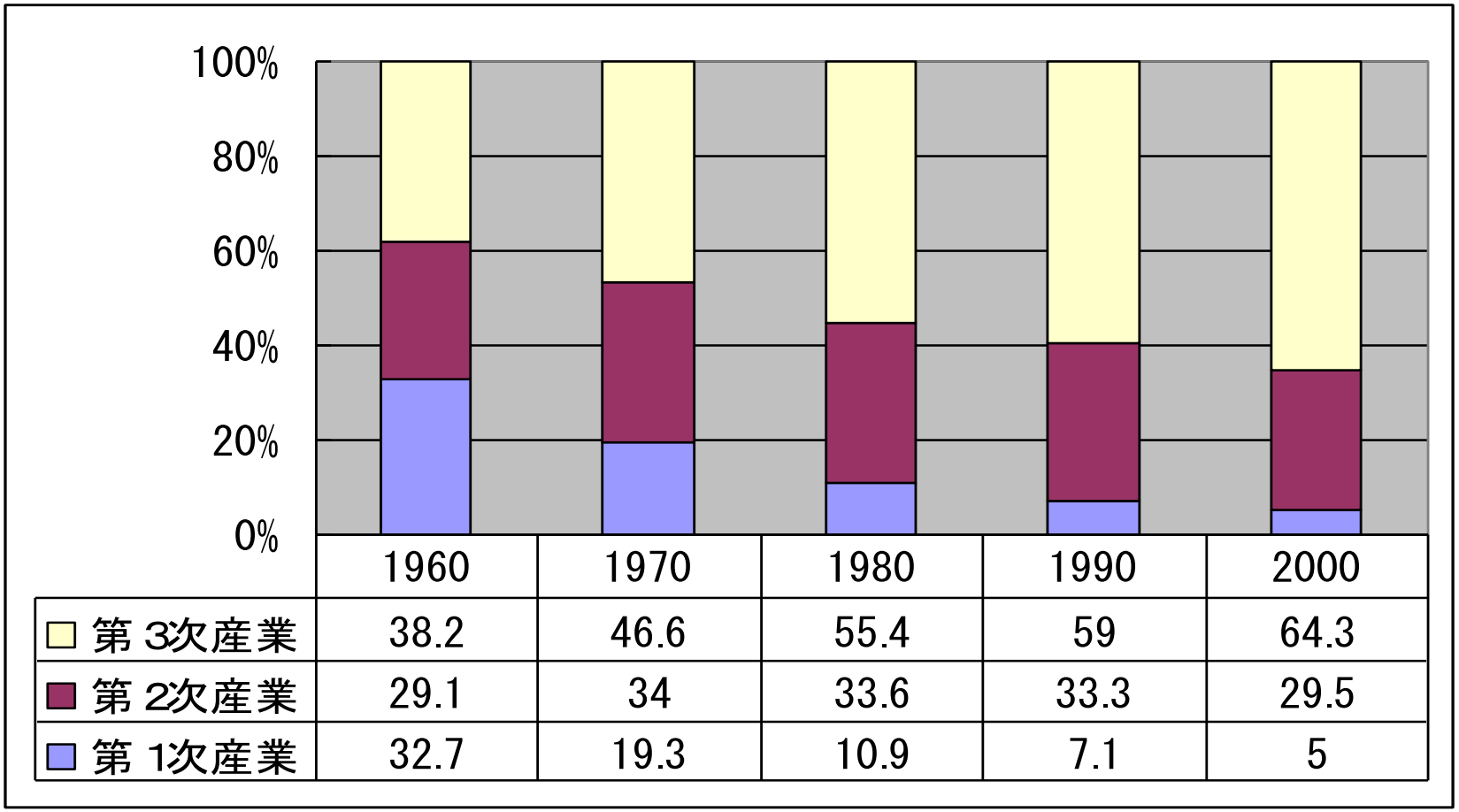
本日の話

- 安全・安心の考え方の変容
- 関連プロジェクト
  - iDC・クラウド関連
  - 認証関連(時刻認証・分散認証）
- 海外事例―国際動向
  - 米国
    - 3つの共通番号・電子政府
  - EU・インド他
- 方向性のまとめ

現代社会の変容

産業構造変化（日本）

（「国勢調査」「平成15年度労働経済白書」より
堀眞由美教授作成『ネットワーク社会経済論』紀伊國屋書店）



	1960	1970	1980	1990	2000
第 3次産業	38.2	46.6	55.4	59	64.3
第 2次産業	29.1	34	33.6	33.3	29.5
第 1次産業	32.7	19.3	10.9	7.1	5

第1次産業：農業、漁業、林業、第2次産業：鉱業、建設業、製造業、第3次産業：電気・ガス・水道、運輸・通信、流通、金融・保険、飲食、不動産、サービス業

「他人指向型社会」と「想像の共同体」

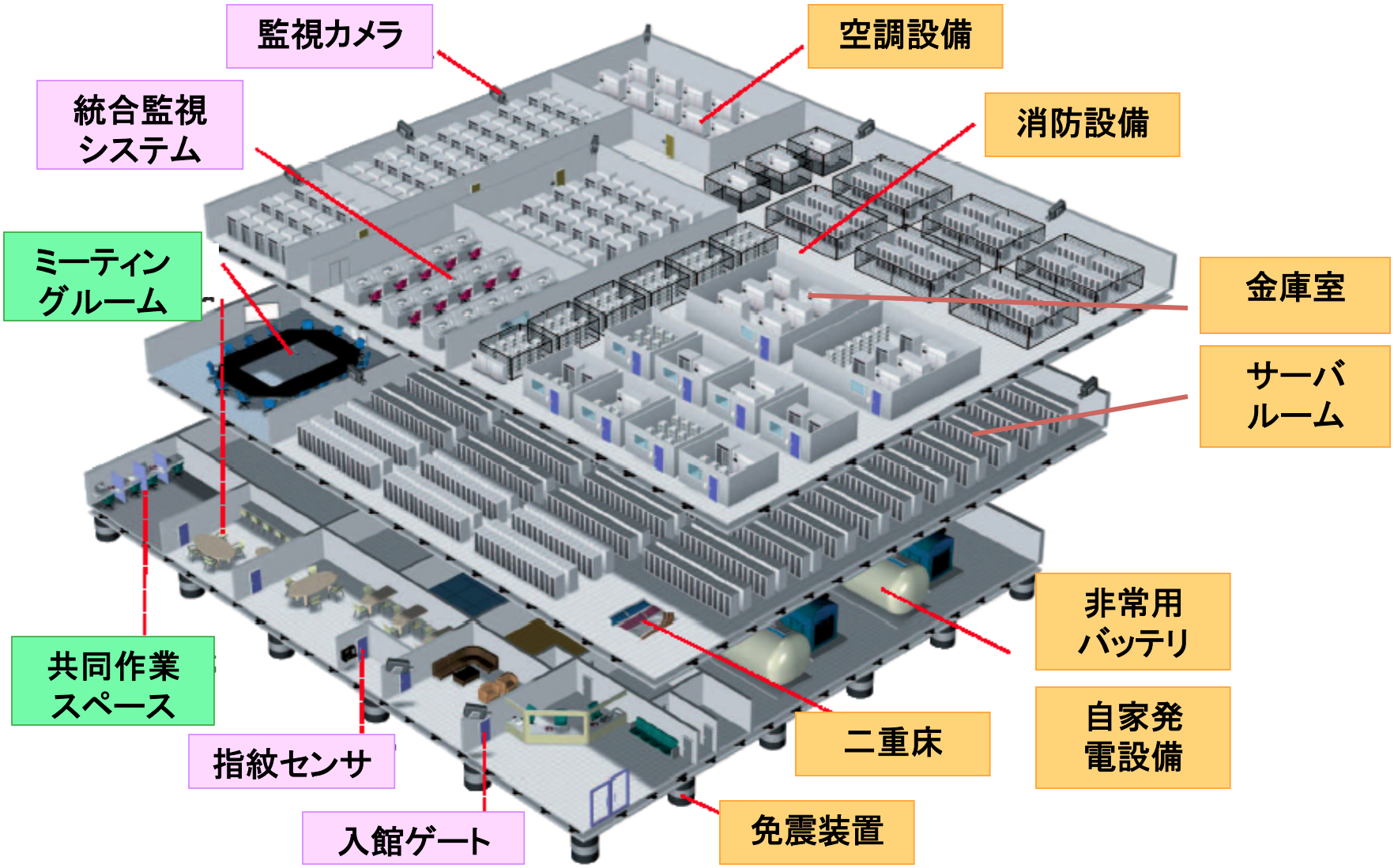
- リースマン
  - 農業社会　　伝統指向型　　「恥」
  - 工業化社会　　内部指向型　　「罪」
  - 脱工業化社会　　他人指向型　「消費社会」　「不安」
  - 他人指向型社会への移行
  - （facebook　18-35歳　Generation Y の加入率が約50%以上（EUデータ））
- ベネディクト・アンダーソン
  - 想像の共同体
  - Facebookはバーチャルな共同体ではない　「国家」や「民族」と同じ想像の共同体？
- ボードリアール
  - 消費の構造　差異　記号　としての消費
    - 消費対象　モノの意味作用は機能からの解放　　非本質的要素が「物の体系」を支配
  - 記号消費の終焉
  - シミュラークル
  - 「差異」から「他者」へのシフト
    - 差異自体のハイパーリアル化

自由と安全

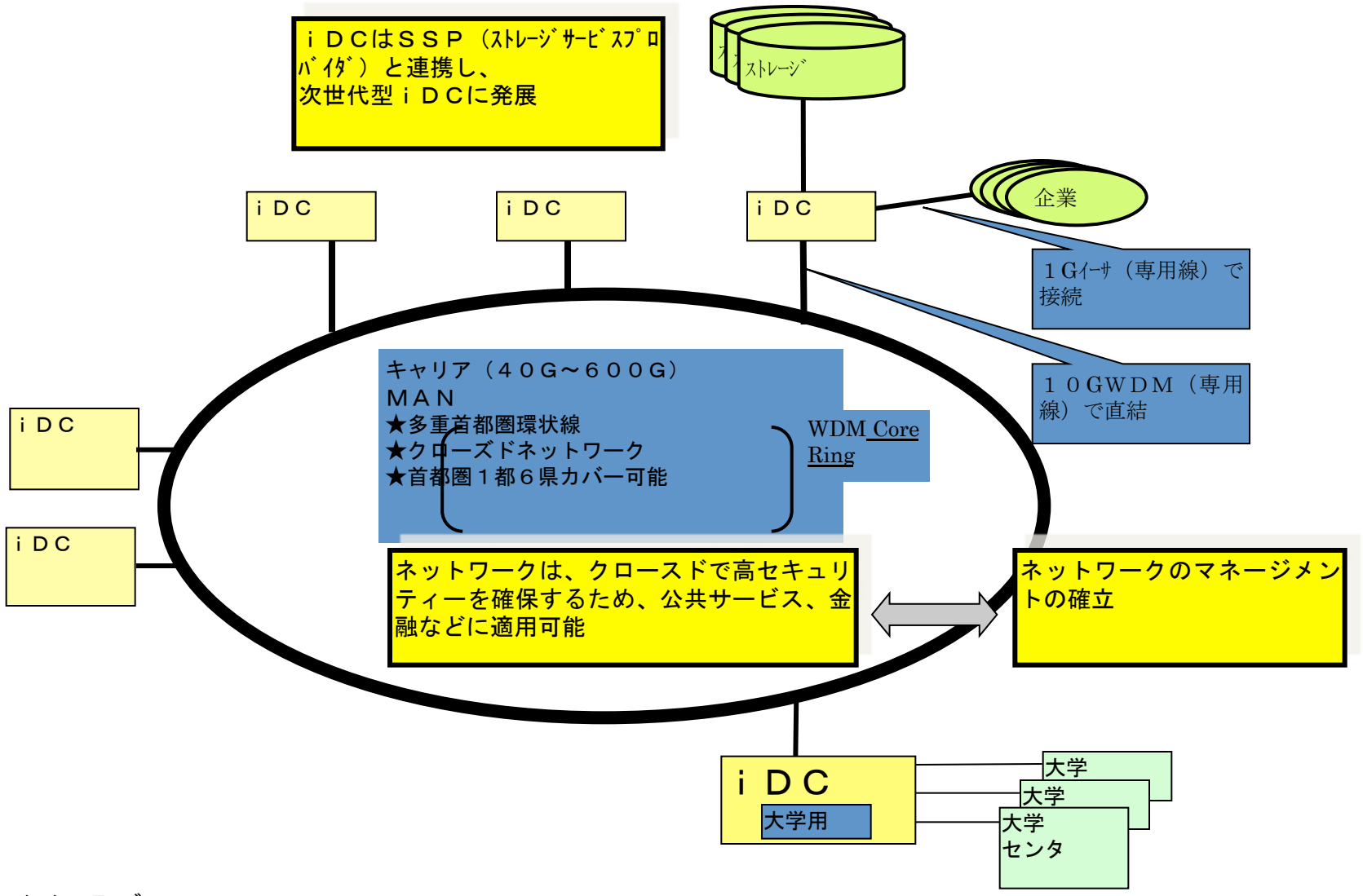
- アメリカ人
  - 自由とは自律性と結びついている
  - 自律には財産が必要
  - 富を蓄積すれば独立できるようになる
  - 人は自主独立し，他者から隔絶することによって自由になる
  - 富は排他性をもたら し，その排他性が安全をもたらす
- ヨーロッパ人
  - 自由とは帰属する ことである
  - 他者と無数の相互依存関係をもちそれにアクセスできること
  - アクセスできるコミュニティが増えるほど，満たされた有意義 な生活を送るための選択肢や機会が増える
  - 他者との関係が包括性をもたらし，
  - 包括性が 安全をもたらす
  - （包括性inclusivity　排他性の対極）

関連プロジェクト
技術動向

インターネット・データセンタとは



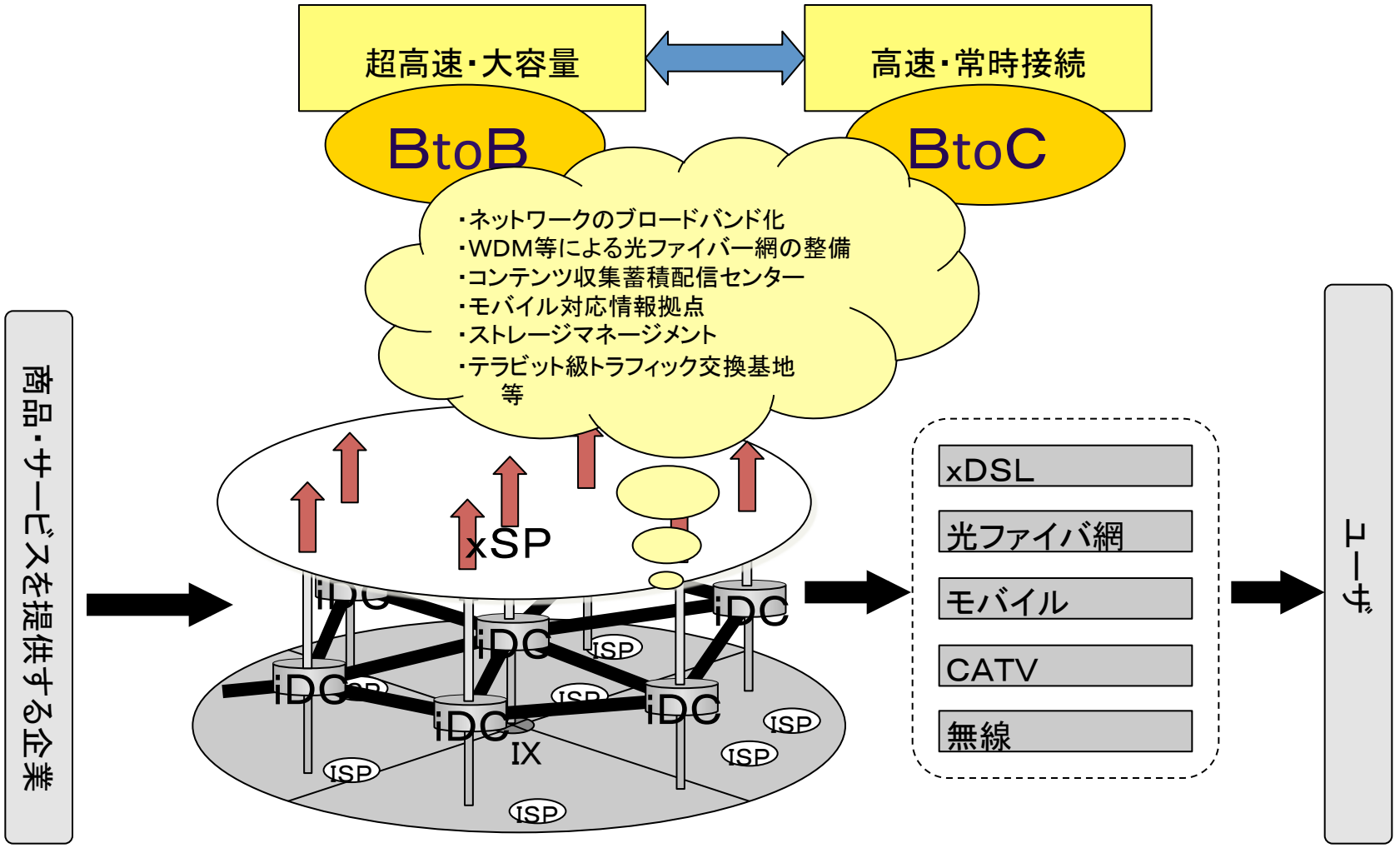
◆ＭＡＮプロジェクト全体概念図　2000年

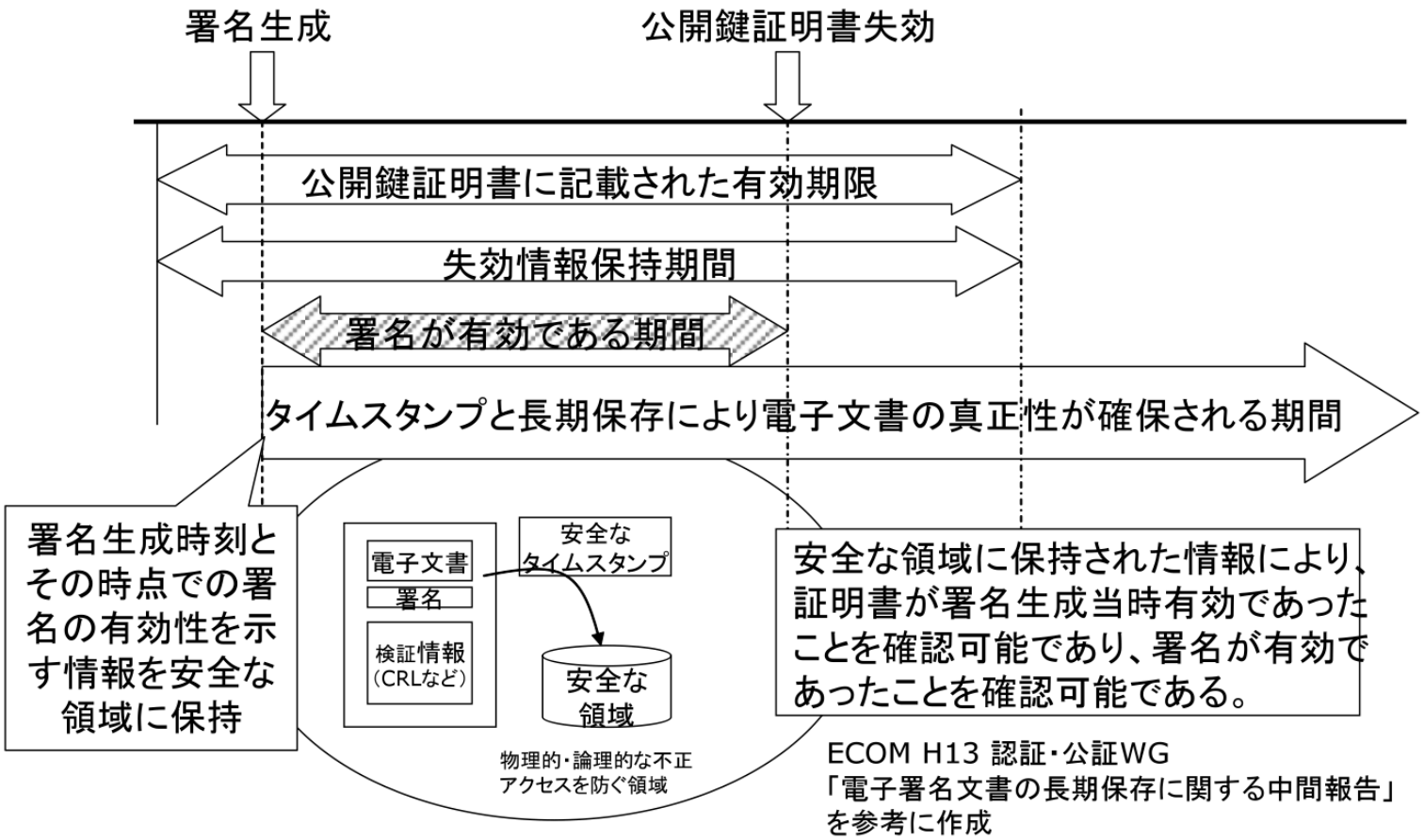


©iDCイニシアティブ、2001

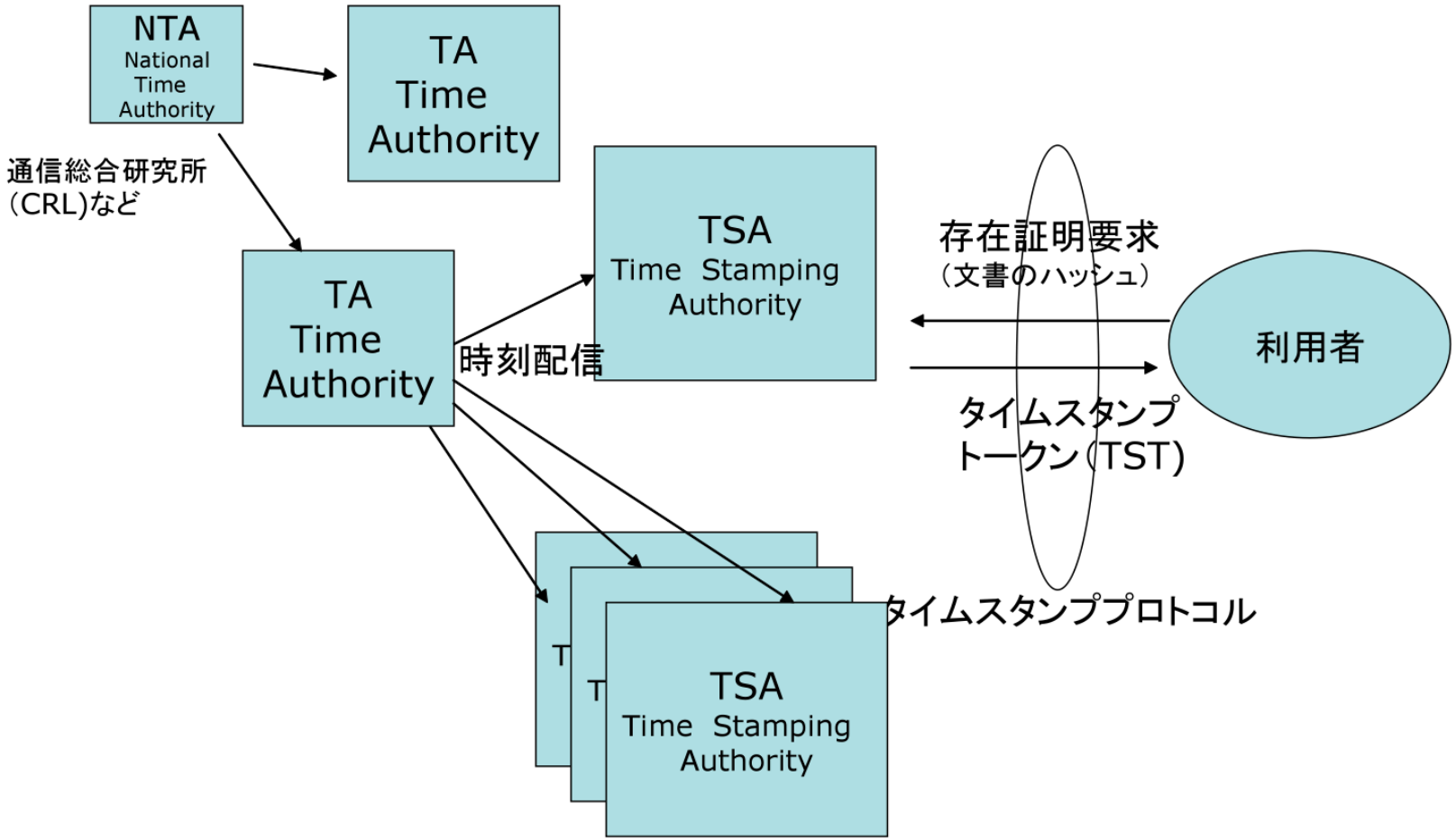
◆ビジネスプラットフォーム

クラウド



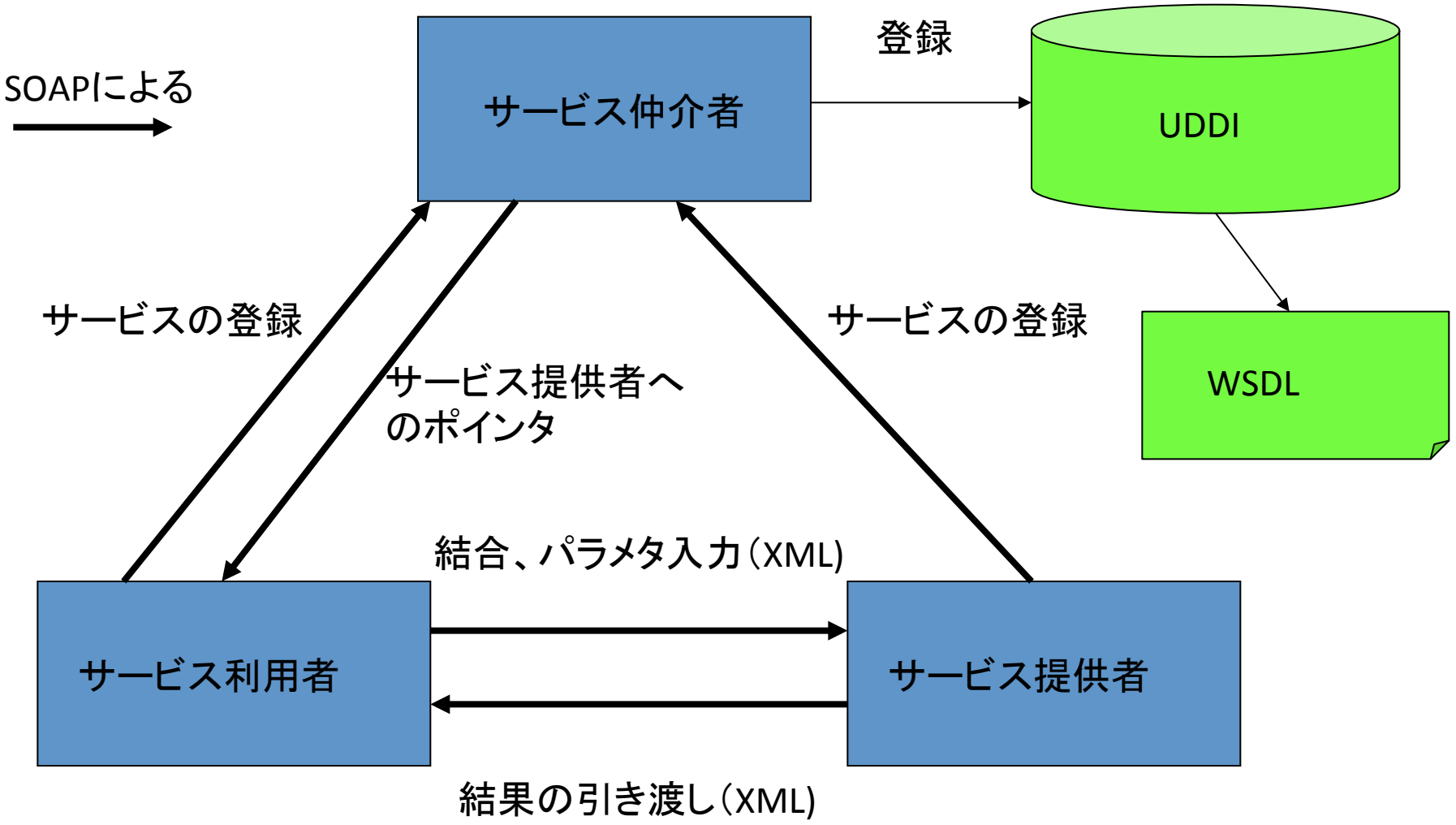


電子文書の真正性を保証する期間

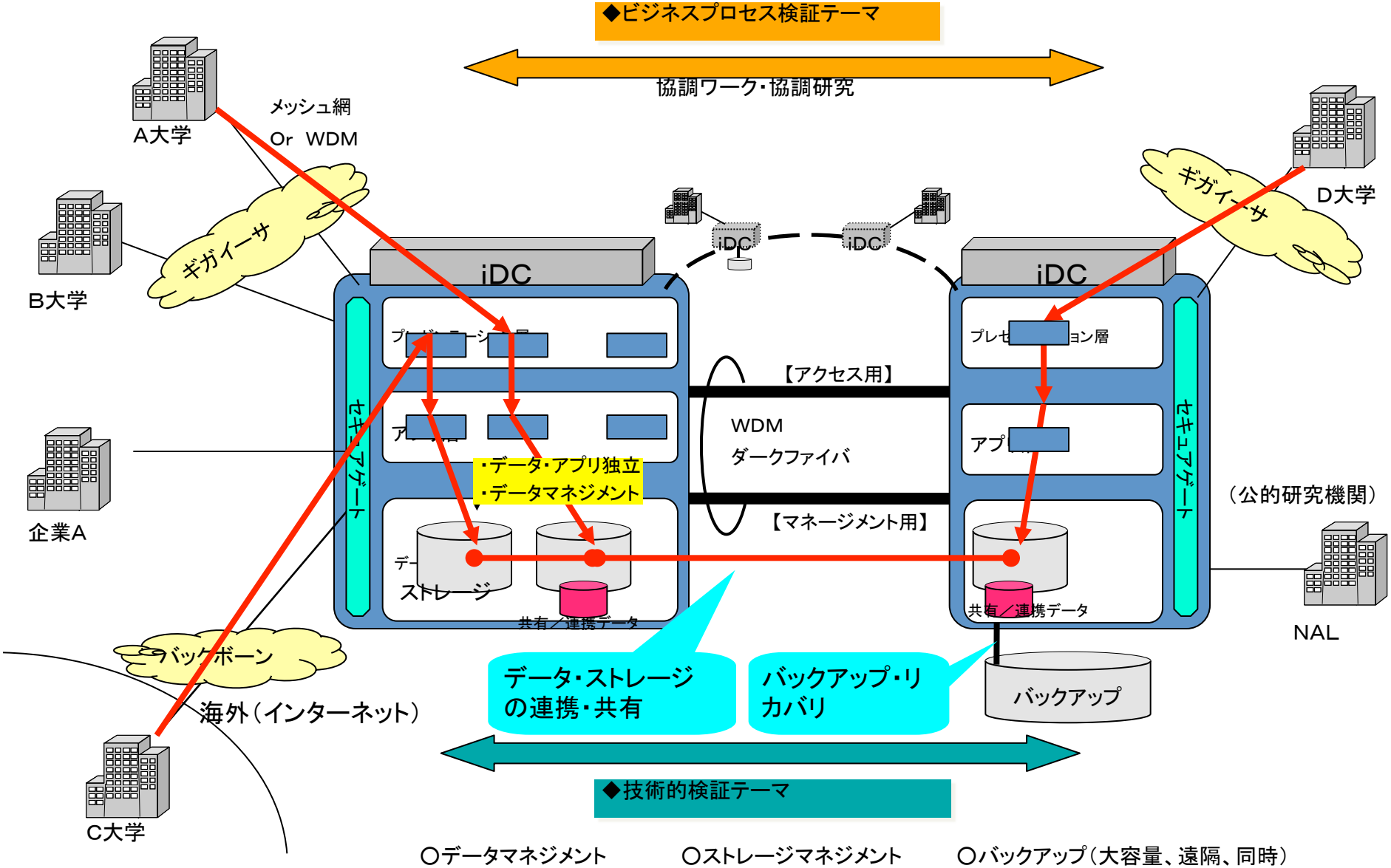


タイムスタンプサービスのモデル

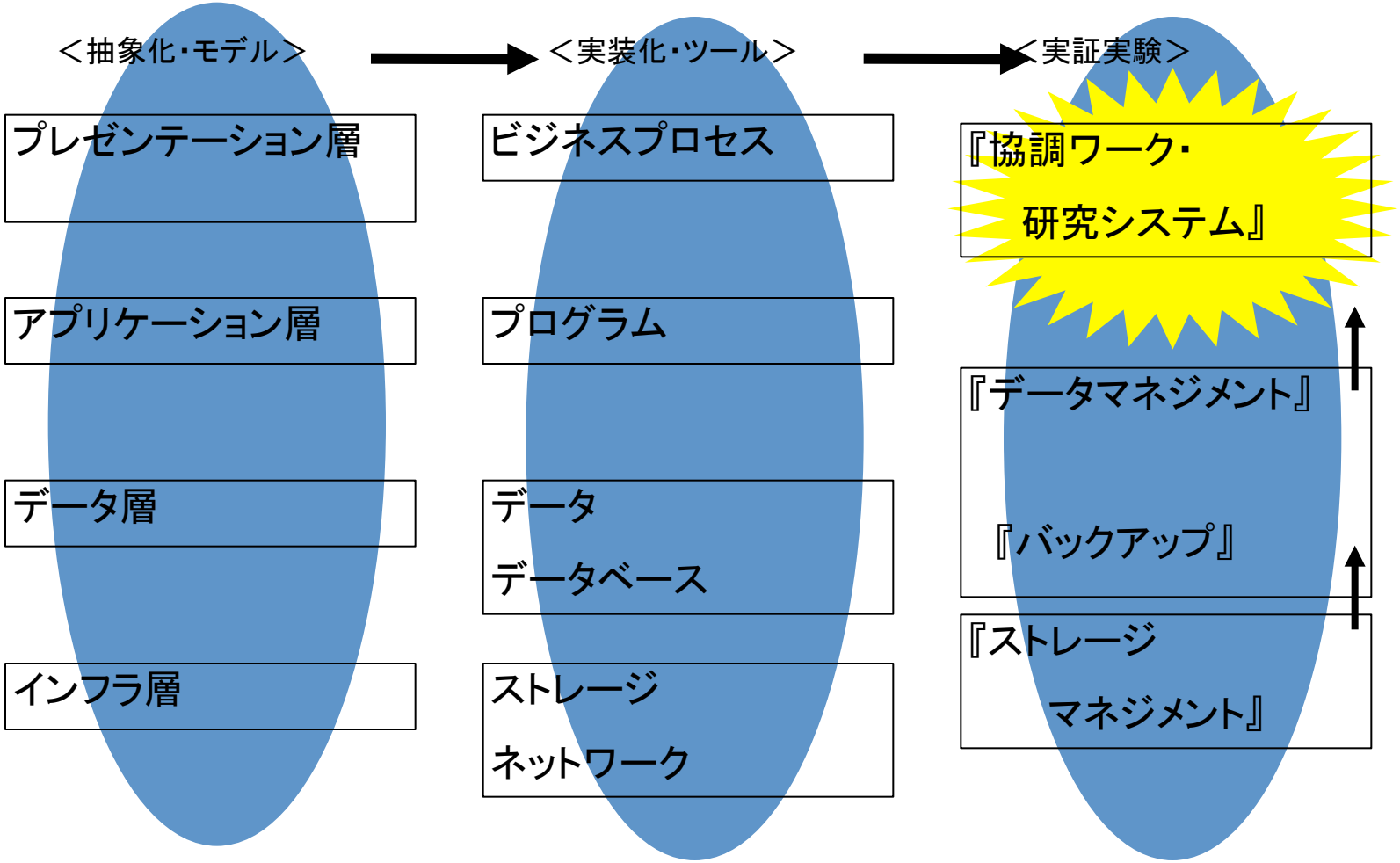
Webサービスのモデル



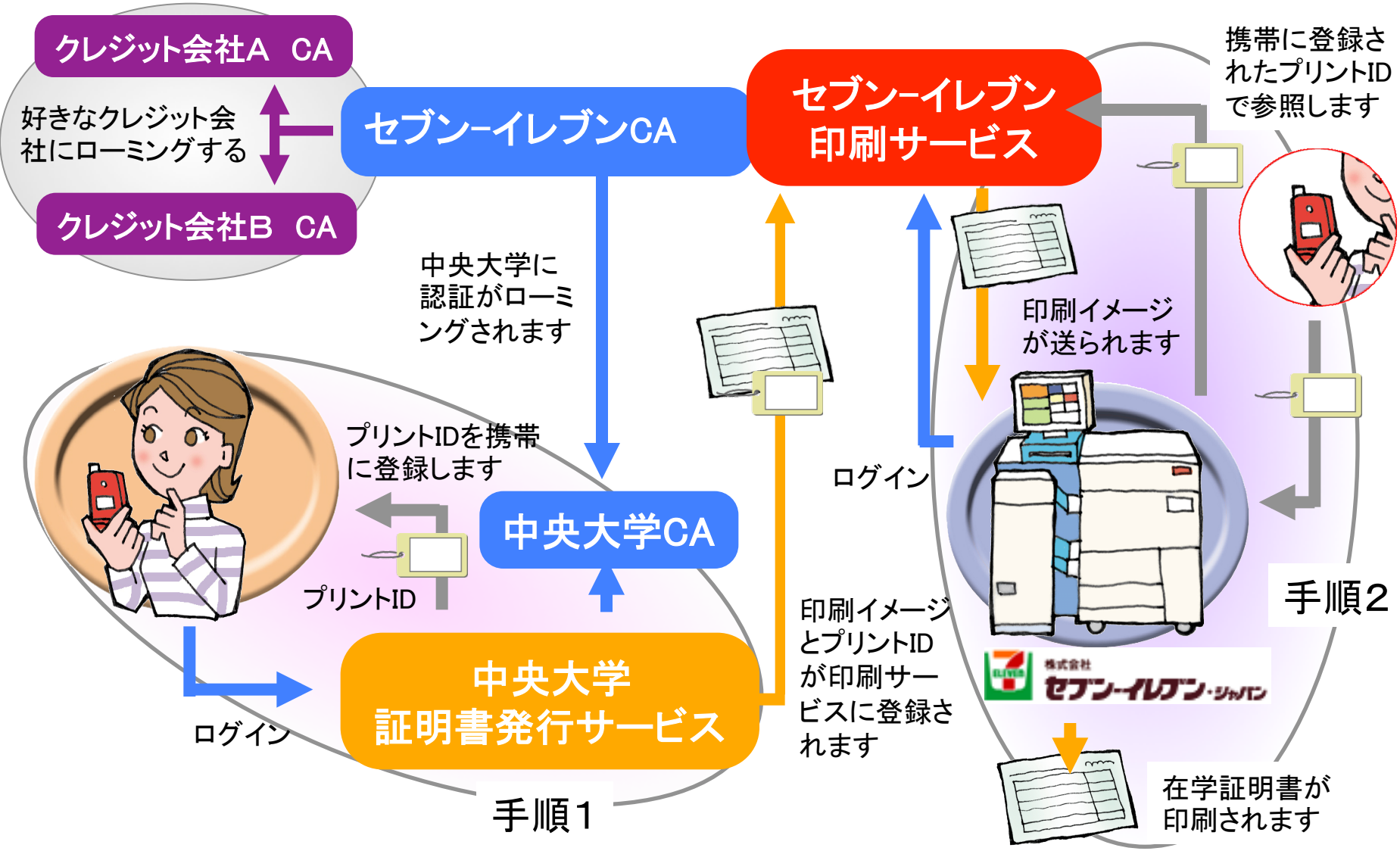
実証実験システム構成概念図　2003年



多階層モデルと実証実験構成



分散認証実証実験　2006年



クラウドとセキュリティ

- 安全利用
  - CIA（機密性、完全性、可用性）
  - 従来のアウトソースの利用の問題　同じ
- 境界の問題
  - パブリック―プライベート
  - 論理的な分離に対する境界（仮想化等も含む）
  - API（クラウドの制御）に関する
- 認証の問題
  - アイデンティティ基盤等　分散型認証
- デジタル・フォレンジック
  - 物理的な実態と論理的な実態の乖離（ログ追跡性）

信頼できる社会基盤としてのネットワーク

信頼性のあるネットワークを基盤とした安心・安全な情報社会を実現するためには、セキュリティ基盤、アイデンティティ基盤、サービス基盤の3つの基盤を確立する必要がある。特に、情報の適正な利用を図るためのアイデンティティ基盤とタイムスタンプが重要である。

・情報の適正な利用

① 情報システムを利用する全てのアイデンティティを漏れなく分散環境下で統合的に管理・運用すること（アイデンティティ基盤）
② 認証・許可・属性といった厳密な本人認証と、許可された必要な範囲内に限られた情報アクセス制御を行うこと（アイデンティティ基盤）
③ 誰がどの情報アクセスをいつ行ったのかをきちんと記録し、内容も含めて第三者による原本性の証明が可能なこと（タイムスタンプ）

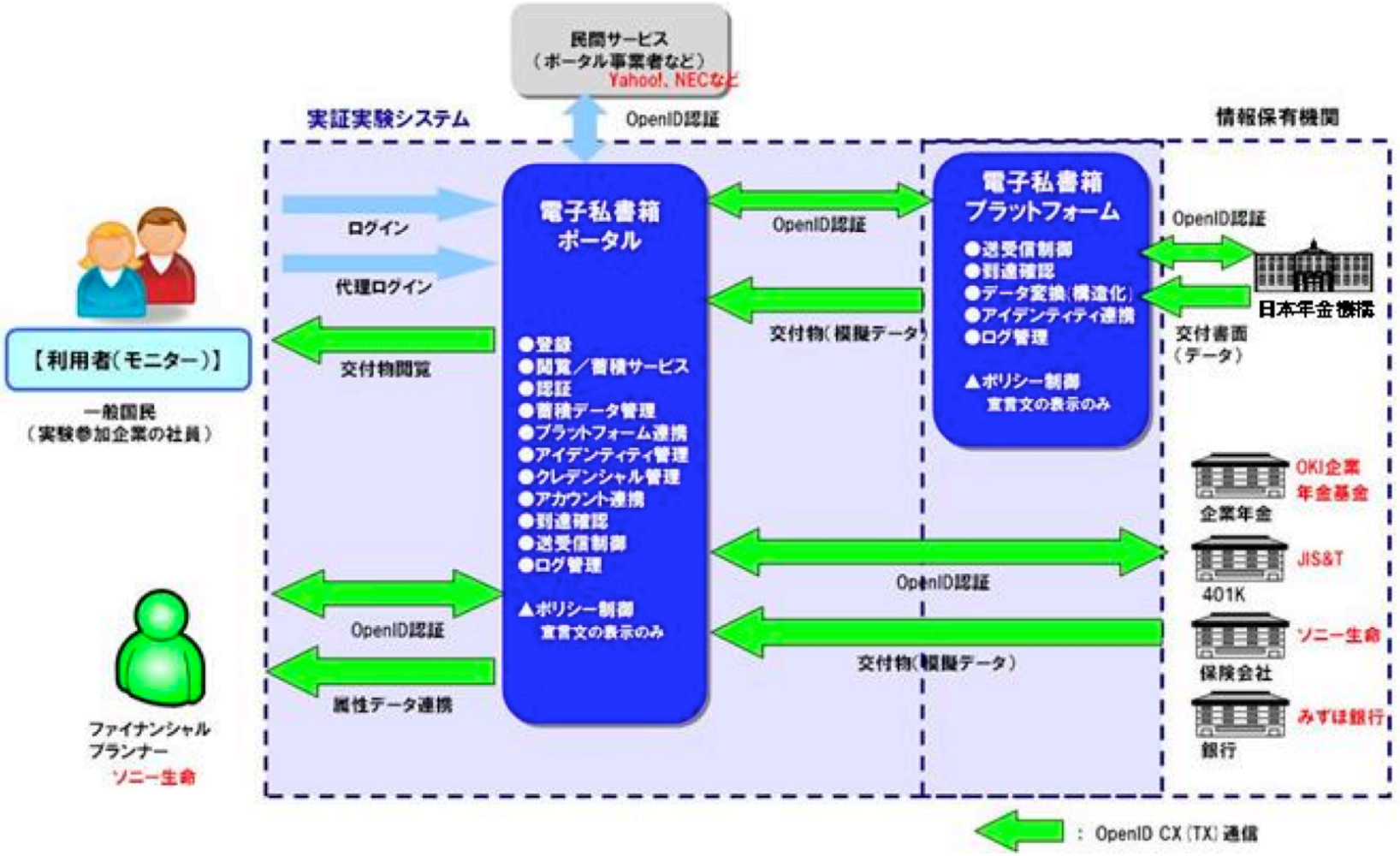
・アイデンティティの5A

① 認証（Authentication）…利用者をユニークに特定するための情報。
② 認可（Authorization）…利用者に与えられる権限情報（情報へのアクセス・操作許可）。
③ 属性（Attribute））…利用者の個人属性（所属、役職など）。
④運営・管理（Administration)…アイデンティティの適切な運営・管理
⑤監査・追跡（Audit） …セキュリティ上の問題がないことを保証・説明する（監査・追跡）

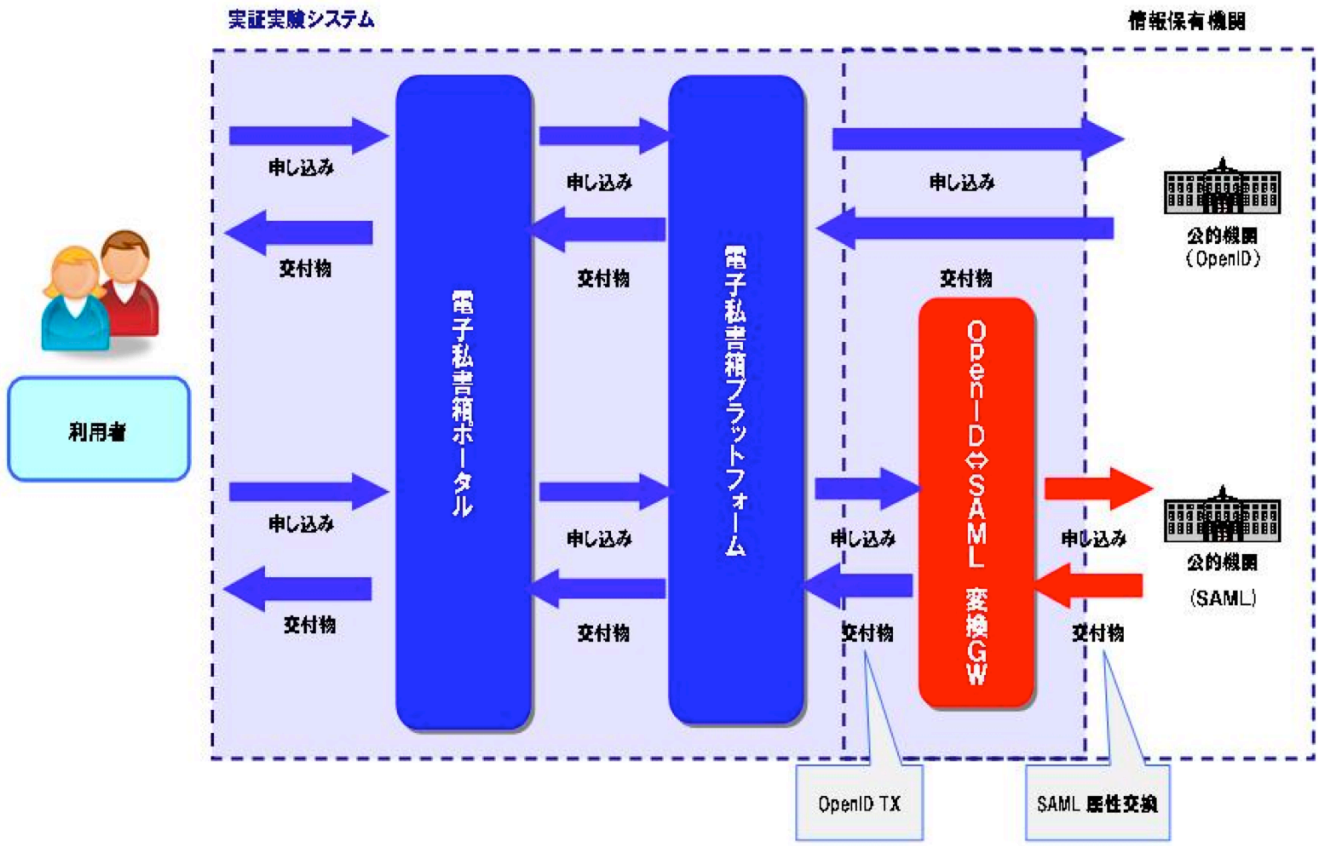
相互運用性：5A全てにおいて異なる認証主体間、サービス主体間で連携し、ワンストップサービスとそれに伴う認可、属性の交換、複数の認証主体にまたがる追跡・監査の実現が必要である。このアイデンティティ基盤は、RFIDなどの広範な普及によって航空手荷物のように荷物にも人のアイデンティティを付与したり、ユビキタス環境では、物品（生産者証明等）にも数々の情報を付与するときにはアイデンティティ基盤が重要な役割を果たすことになる。

認証の５Ａ

5A	現状	課題	課題概要	対策
認証	民間CA、公的CAが稼動しているものの、あくまで個別運用に留まっており、社会全体としての最適化という視点に欠けている	信頼性の確保	認証方式等によって、認証結果の信頼性には差が生じる。認証方式等に信頼性を与える仕組み（法制度含め）、認証における信頼レベルの統一的な基準が必要。	電子署名法の電子認証版の設立による法的信頼性付与 認証レベル統一基準の策定による安全水準の確保 認証レベルに対応したアイデンティティ管理技術の確立
		有効期間	認証に用いるクレデンシャルには有効期間を設定することが望ましい場合がある。このとき、信頼できる時刻に基づく運用が必要と	時刻認証による有効期間の厳密な運用
		画一的な保証レベル	電子署名法上、画一的な保証レベルの認証機能しか提供されていない	アプリケーション特性に応じた、複数の保証レベルの認証機能の提供
認可	本機能を提供する基盤は、現在存在しない	信頼性の確保	権限情報に改竄がないことを保証する必要あり。	署名やタイムスタンプによる改竄防止
		有効期間	権限情報を許容された期間を超えて使いまわせないようにする必要あり。	時刻認証による有効期間の厳密な運用
属性	本機能を提供する基盤は、現在存在しない	信頼性の確保	属性の正当性を確認できる必要あり。	署名やタイムスタンプによる改竄防止
		匿名性の確保	属性情報を必要以上に開示しないようにする必要あり。	仮名や匿名を可能とする属性管理
		有効期間	属性保証期間を厳密に管理する必要あり。	時刻認証による有効期間の厳密な運用
運営・管理	本機能を提供する基盤は、現在存在しない	信頼のレベルの統一	認証・認可・属性などの用語や基準が統一されている必要あり	統一基準を規定するガイドラインの策定
		安定性の確保	サービスの安定性は、個別主体に委ねられている	社会全体として、安定的なサービスを提供できる基盤の確立
追跡・監査	本機能を提供する基盤は、現在存在しない	証跡の信頼性の確保	証跡データに改竄や消失がないことを保証する必要あり。	署名やタイムスタンプによる改竄防止



2010　デジタル市民プロジェクト実証実験　経産省

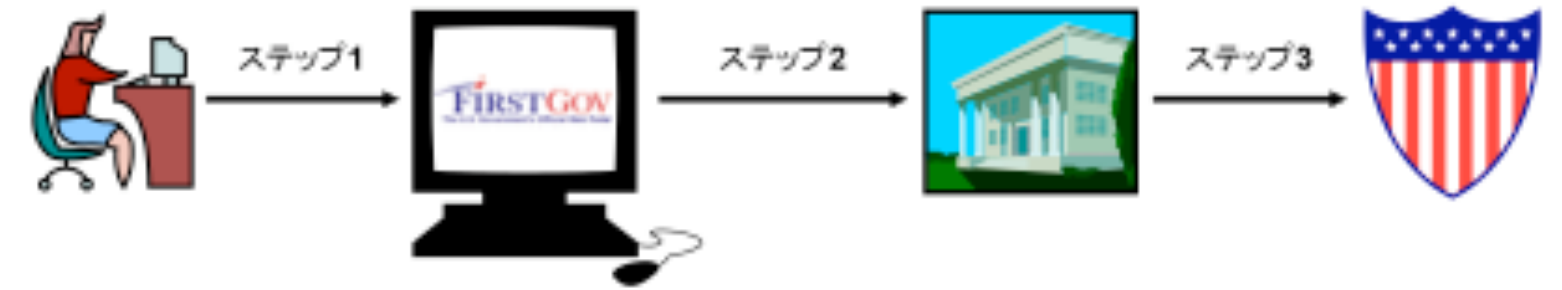


分散認証　Open−ID　SAML　変換システム実証実験

インターネット
ドメインネームサーバー　DNS

- インターネット　自律分散型
- ドメインネームサーバー　DNS
- ホスト名ー＞IPアドレスに変更
- 例　Webにアクセス（メール等も基本的に同じ）
  - URL：　http:www.chuo-u.ac.jp
  - DNSー＞IPアドレスを検索
  - アクセス可能
- ディレクトリーサービス

海外動向



ステップ1

ユーザは、アクセスポイントで※、政府機関アプリケーションとクレデンシャルサービスプロバイダを選択する。

※ アクセスポイントで

ポータル、政府機関のWebサイト、クレデンシャルサービスプロバイダのWebサイトなどが考えられる。

ステップ 2

ユーザは、選択したクレデンシャルサービスプロバイダへリダイレクトされる。

- もしユーザが既にクレデンシャルを持っていれば、ユーザはすぐに認証される。
- 持っていなければ、ユーザはクレデンシャルを取得してから認証される。

ステップ3

クレデンシャルサービスプロバイダは、認証したユーザを、彼女がアクセスポイントで選択した政府機関アプリケーションへハンドオフする。

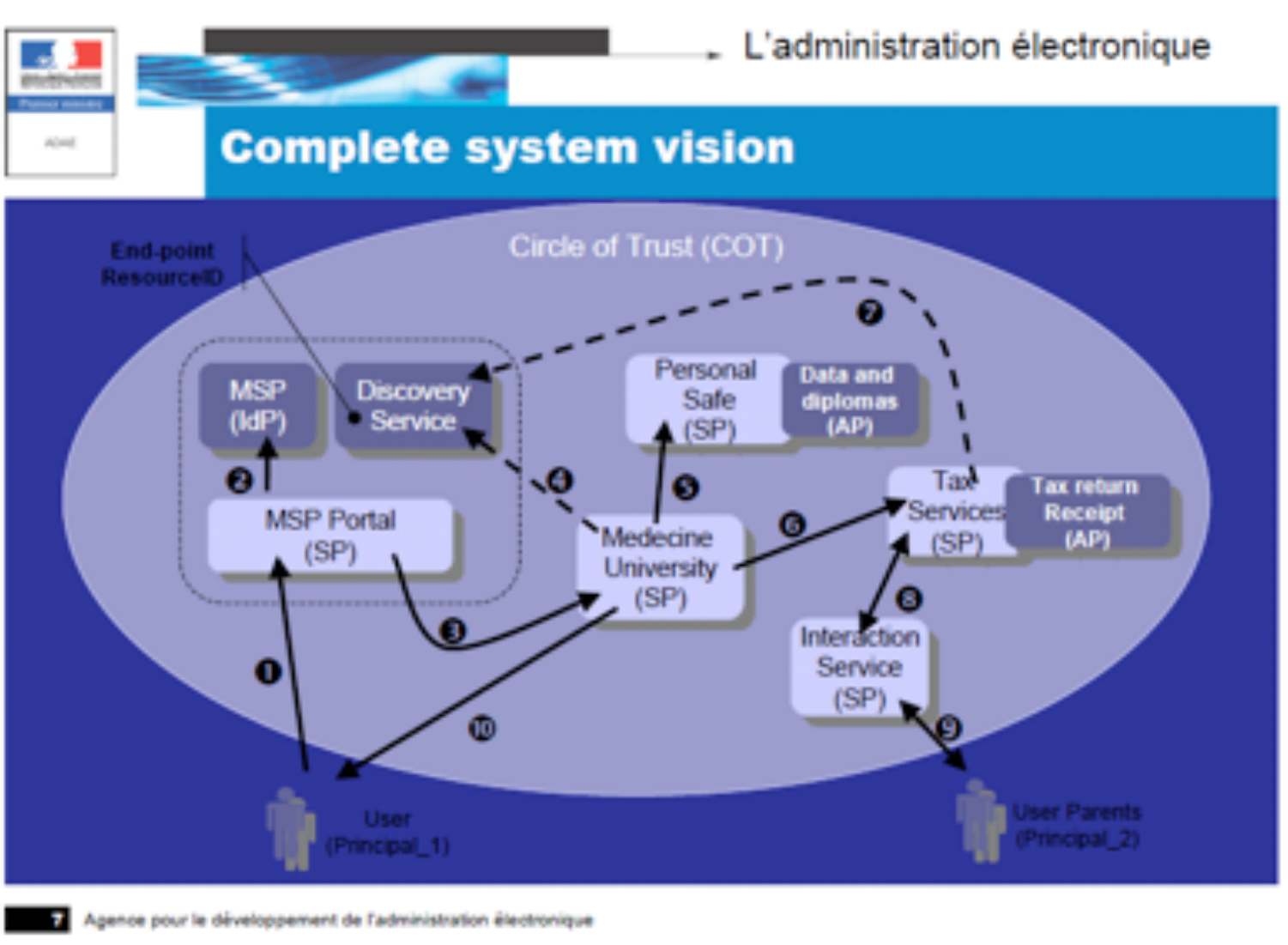
米国　e-Authentication サービスコンセプト
「次世代認証システムの在り方に関する調査研究」
総務省 情報通信政策局 情報通信政策課
受託　**学校**法人　中央大学　**平成19年3月**

米国の共通番号の構成

- 1.運転免許証
  - 形質情報の付与（写真） 身元証明に相当
- 2.SSN（社会保障番号）
  - 徴税用　 名寄せのための属性チェック
  - 真正性の確保　SSNVS
  - 負担と給付の公平性の目的
- 3.トラストフレームワーク（OITF）
  - 国民ID制度に相当
  - 民間企業のIDを利用

OITFの構成（民間ID利用）

- レベル1
  - 身元確認の必要なし　YahooID,Google,mixi,楽天
  - 公共施設予約等
- レベル2
  - 対面　公的な身分証明書番号、住所にクレデンシャルを送付
  - 非対面　公的な身分証明書、　金融機関の口座番号
    - 金融機関、携帯電話、特定認証局、公的個人認証サービス・パスポート
  - 給付金の申請等
- レベル3
  - 対面　写真付き証明書等、非対面　公的身分証明番号、　金融機関の口座番号等　住所にクレデンシャルを送付
    - Yahooワレット、Yahooプレミアム、生命保険、損害保険口座の開設
  - 給付金の振替依頼　（＋ワンタイムパスワード）
- レベル4
  - 対面のみ可　1.公的写真付き証明書＋2.別の公的証明書もしくは金融機関口座番号　両方を発行機関に検証　住所にクレデンシャル　送付



フランス情報産業局(ADAE : Agence pour le developpement de l'administration electronique)「次世代認証システムの在り方に関する調査研究」　**総務省 情報通信政策局 情報通信政策課**　受託　**学校**法人 中央大学　**平成19年3月**

まとめ

- 日本の実情
  - 戸籍・住民票等完備
  - 民間の様々なIDシステム稼働
- 課題
  - インフォームドコンセントについて
  - グローバルな仕組みとの連携？
    - 例：OITF　民間主導
  - 全体コストと地方自治体のコスト負担？
    - 負担が大きい？
  - 技術の進歩と暗号の危殆化？
- 技術的な方向性
  - ディレクトリーサービスで十分