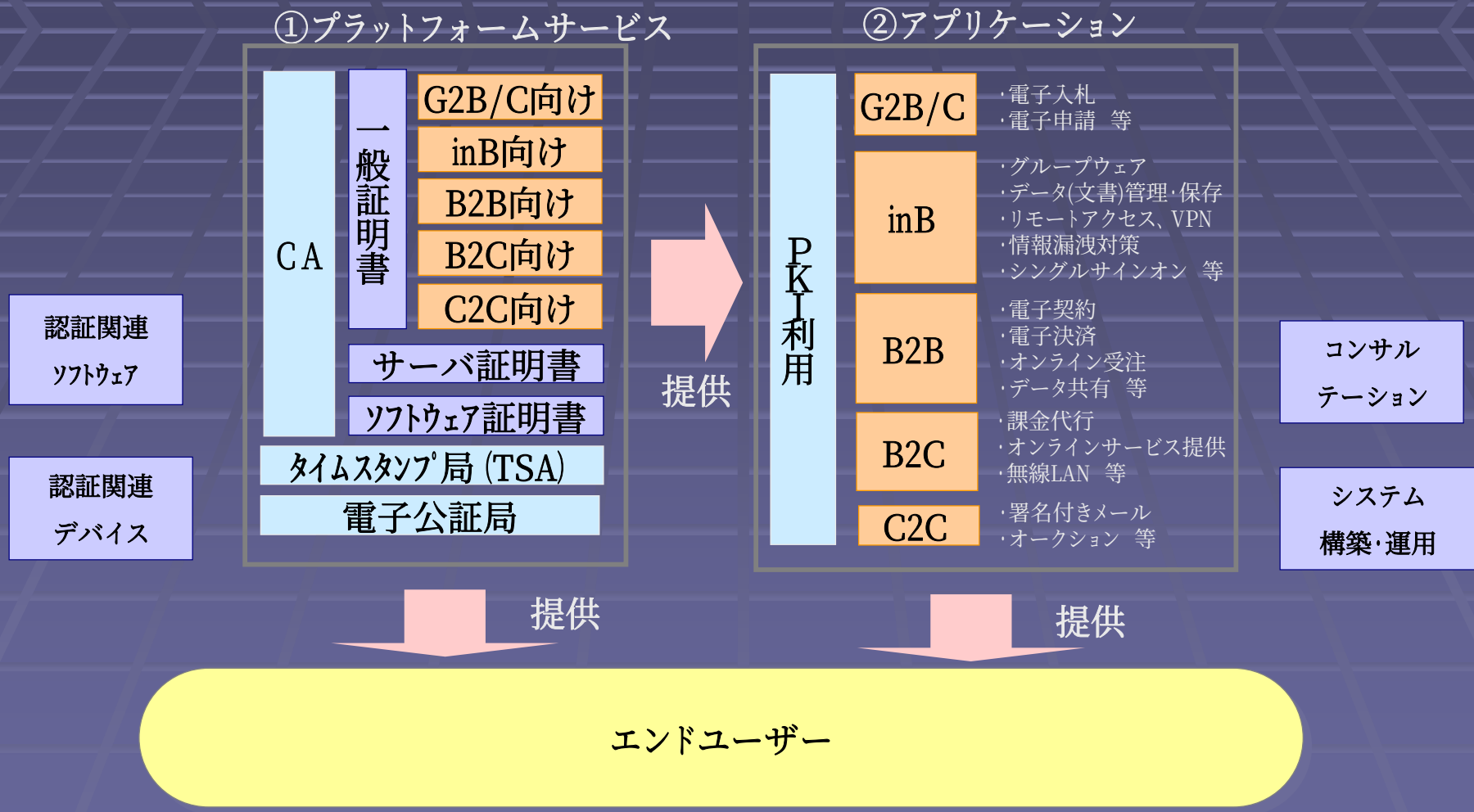
認証プラットフォーム事業の現状と今後

工藤 明彦
NTT情報流通プラットフォーム研究所

本日の概要（ポイント）

- 電子認証ビジネスの市場構造
- 電子認証関連サービスの現況
- PKIの課題
- 今後の展望
- UPKIへの期待

電子認証ビジネスの市場構造



電子認証関連サービスの現況

- 電子認証サービス
  - GPKI（府省認証局）/LGPKI
  - 公的個人認証サービス
  - 法務省商業登記認証局
  - 民間認証局、士業認証局
  - サーバ証明書発行サービス
- タイムスタンプサービス
  - 時刻配信サービス
  - 時刻認証サービス
- 電子公証サービス
  - 公証制度に基礎を置く電子公証サービス（指定公証人）
  - 民間の公証サービス（電子データのやりとりなどを証明）
  - e-文書法に対応した署名文書保存サービス

PKIの課題 -普及が進まない要因（例）-

- 導入コスト・運用コストに見合う“効果”
  - セキュリティに対する経営層の認識
  - 法律等に強制力・義務付けがない
  - ネット利用によるコスト削減、BPRとの連動によるシナジーへの期待
- 適用範囲が限定された証明書、相互認証/認証局連携が困難
  - 証明書の有効範囲（利用用途）が限定・・・行政・企業・学校・病院・・・
  - 公的個人認証サービスも用途限定
  - 証明書の普及とサービスの創出が“鶏と卵”の関係に陥っている
  - 汎用的で使い勝手の良い証明書（言わば“三文判”）がない
- “電子的”だけでは完結しない電子行政プロシージャ
  - 申請は電子化されたが添付文書等は別途郵送、など

（PKIの普及阻害要因ではないが）これ以外に、

- 暗号アルゴリズムの危殆化（DES/1024-bit RSA/SHA-1）
  - NISTによる移行勧告：暗号アルゴリズムの2010年問題

今後の展望 -期待を込めて-

- 利用シーン拡大による認証ビジネス市場の成長
  - e-文書法施行（2005.4）
  - ＥＣ（ネットオークションなど）/情報交換サイト（Blogなど）
  - ユビキタス社会（認証対象機器拡大、FMC認証など）
  - 日本版SOX法整備に伴うディジタルフォレンジクスの要求
- 課題解決に向けた技術面の進歩
  - 相互認証/運用・・・SSO（Single Sign On）の活用・融合
  - 暗号危殆化対策（暗号強度）・・・国策としての対応
- 施策（制度・運用面の改善）への期待
  - IT新改革戦略（2006.1）
  - 日本版SOX法（？）
  - 改正・電子署名法（？）

UPKIへの期待

- これまで述べてきた諸課題解決への第一歩
- 新たな技術･ビジネス創出の機会
  - 危殆化に備えた新暗号アルゴリズム
  - 利便性など、訴求力の大きいPKIサービスモデル

プロファイル

工藤 明彦（くどう あきひこ）

1977.4　日本電信電話公社（現NTT）入社
2005.7　現職（NTT情報流通プラットフォーム研究所長）

- 主として、オペレーティングシステム、分散処理ミドルウェア、サービスオペレーションアーキテクチャ、企業システム向けサービス管理技術、電子入札システム等の研究開発に従事。この間、NTTの事業部門において、社内情報システムの設計・開発・全国展開等も担当。
- 電子情報通信学会・情報処理学会・IEEE各会員