サーバー連携型
多目的ICカードシステム
ー耐タンパー技術の重要性ー

東京工業大学
像情報工学研究施設
大 山 永 昭

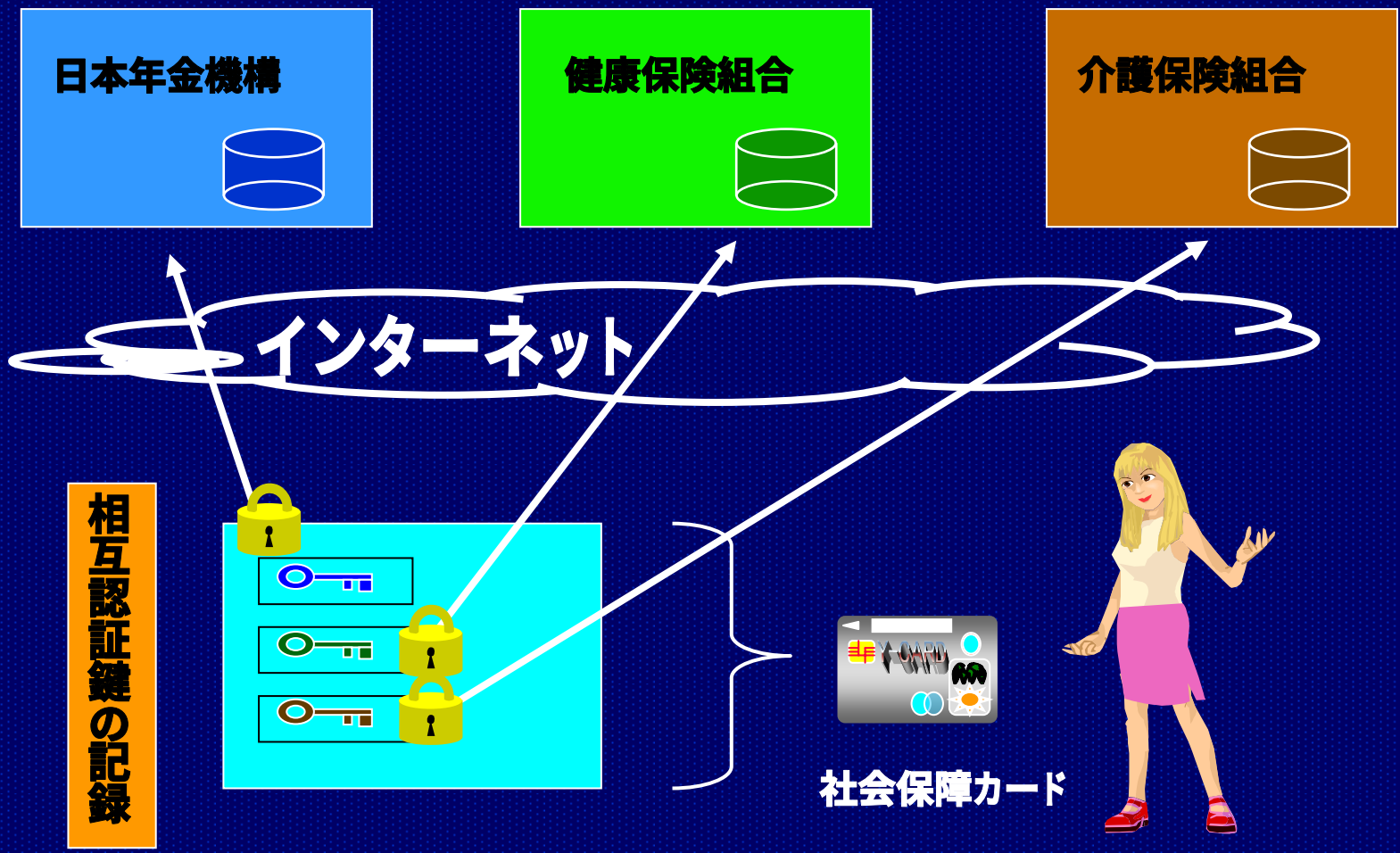
耐タンパーLSIについて

- 複合機能（CPU、RAM、ROM、通信機能等）を搭載した耐タンパーICチップで、ICカードに用いられている。
- 最先端のチップは、2階層PKIをサポートし、秘密鍵は読み出しが技術的にできなくしている。
- 住基カードで実用化され、Dynamic On-demand VPNにも利用される。
- ISO7816-13として、ISになっている（日本提案）
- GPの標準規格に採用されている。

従来型多目的カードの難点

- 2階層PKIの採用により、カードへのアプリ追加は許可証の利用できるが、各カードの状態を管理する機能も必要
- サービス提供者が多い場合、下層の鍵の廃止や更新に手間が掛かるとともに、高度なセキュリティレベルの維持が困難になる
- メモリ容量の制限から、搭載可能なアプリの数に限界がある
- バッテリー無しのICカードでは、自ら時間の流れを管理することができない ⇒ 期間指定のDRMの利用は困難

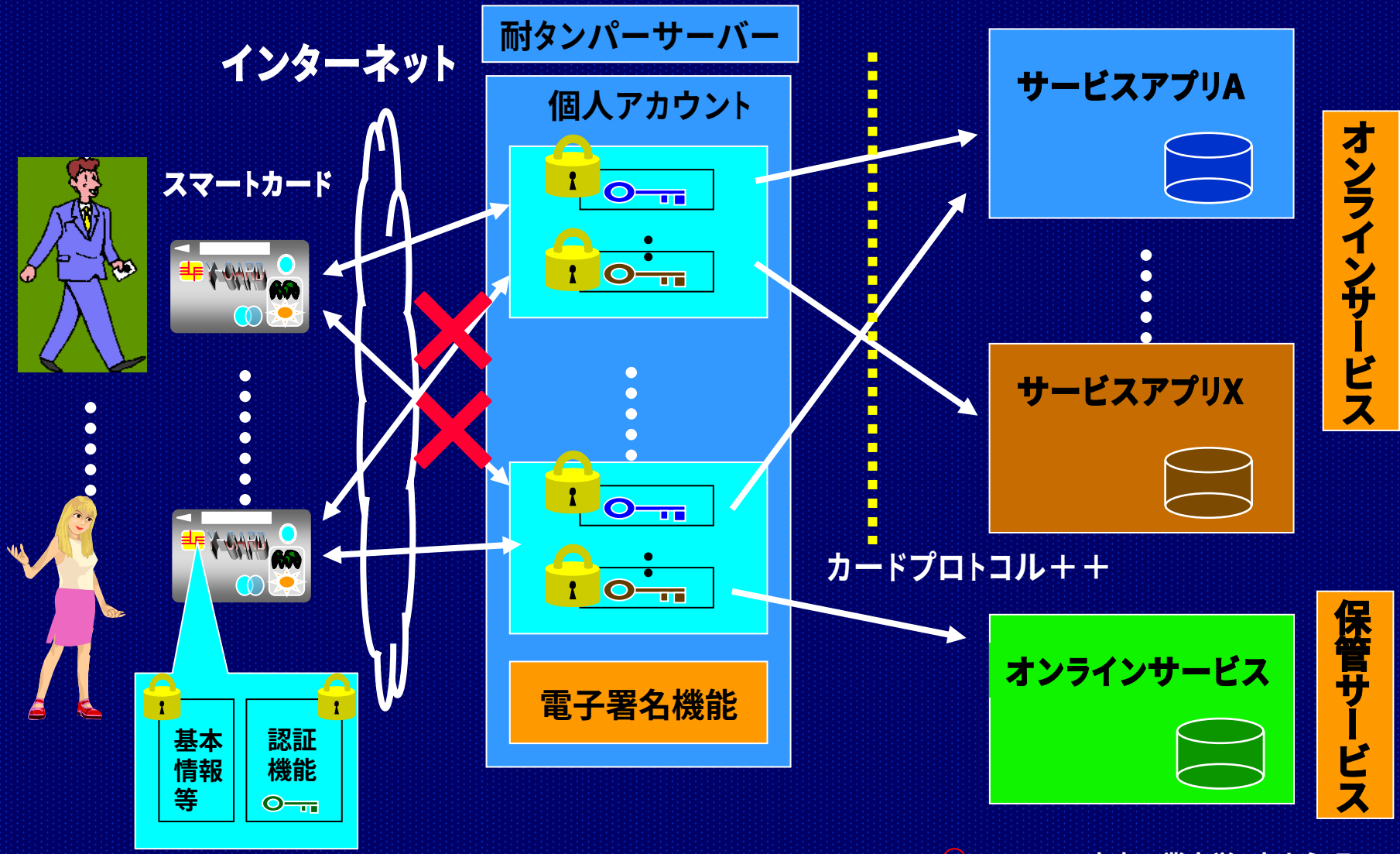
多目的カードの利用法（例）



サーバー連携型ICカードの開発

- サーバーにおかれる個人アカウントと連携する
- 個人アカウントは、データ実体へのアクセスキーを管理
- アカウントに記録される情報（アクセスキーと一部のデータ実体）は必要に応じて暗号化し、アクセスカードでのみ復号化可能とする
- サーバーに置かれる個人アカウントとアクセスキーで、従来の多目的カードを実現
- 耐タンパーサーバー（機能限定、秘密鍵の安全性確保）の開発が有望 ⇒ **耐タンパーVLSIが望まれる**

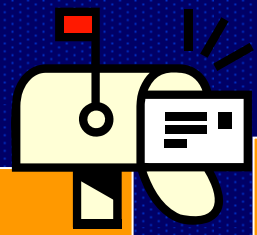
サーバー連携型ICカードシステム



電子私書箱への拡張

- 本人の意思で自己情報を取得、閲覧、活用することは、サーバー連携型ICカードシステムで基本的には可能になる
- 例えば、結婚、妊娠、出産、育児（評価専門調査会特別テーマ検討会資料参照）に要する各種の手続きは、一般の人には極めて難解かつ煩雑　⇒　手続きの順番や種類が多い
- 業務フローの簡素化やバックオフィス連携は、積極的に推進すべきであるが、実現にはかなりの時間を要する
- これらの手続きをガイドする（ナビゲーション）、一連の手続きを代行する（コンシェルジェ）機能が望まれる　⇒　電子私書箱の必要性
- これらから、サーバー連携型ICカードシステムに、ナビゲーション、コンシェルジェ等の機能追加したものが電子私書箱に　⇒　官民連携も可能？

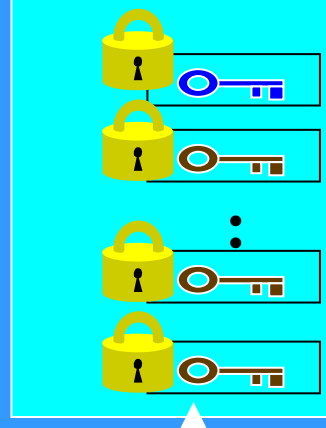
将来像（一案）



ナビゲーション・
コンシェルジェ
機能提供サーバー

耐タンパーサーバー

個人アカウント



アカウント　アカウント

モバイル

ID・パスワード

ICカード

アクセス手段の多様化

次世代電子行政：
ポータルサービス

社会保障関連

民間アプリ

保管サービス

：認証に要するID,鍵情報等