ITの利活用と社会

東京工業大学
フロンティア創造共同研究センター
大 山 永 昭

ITとは？

- ICT：Information Communication Technology
  ネットワークで接続された情報システム
- なぜ使う？
  - 生産性の向上、国際競争力の回復など
  - 多岐に渡る消費者ニーズに対応
  - 安全性と利便性の提供　など
- 何に使う？
  - 電子政府、遠隔医療、電子商取引などの新たなサービスを提供
  - 高度に情報化された社会の構築

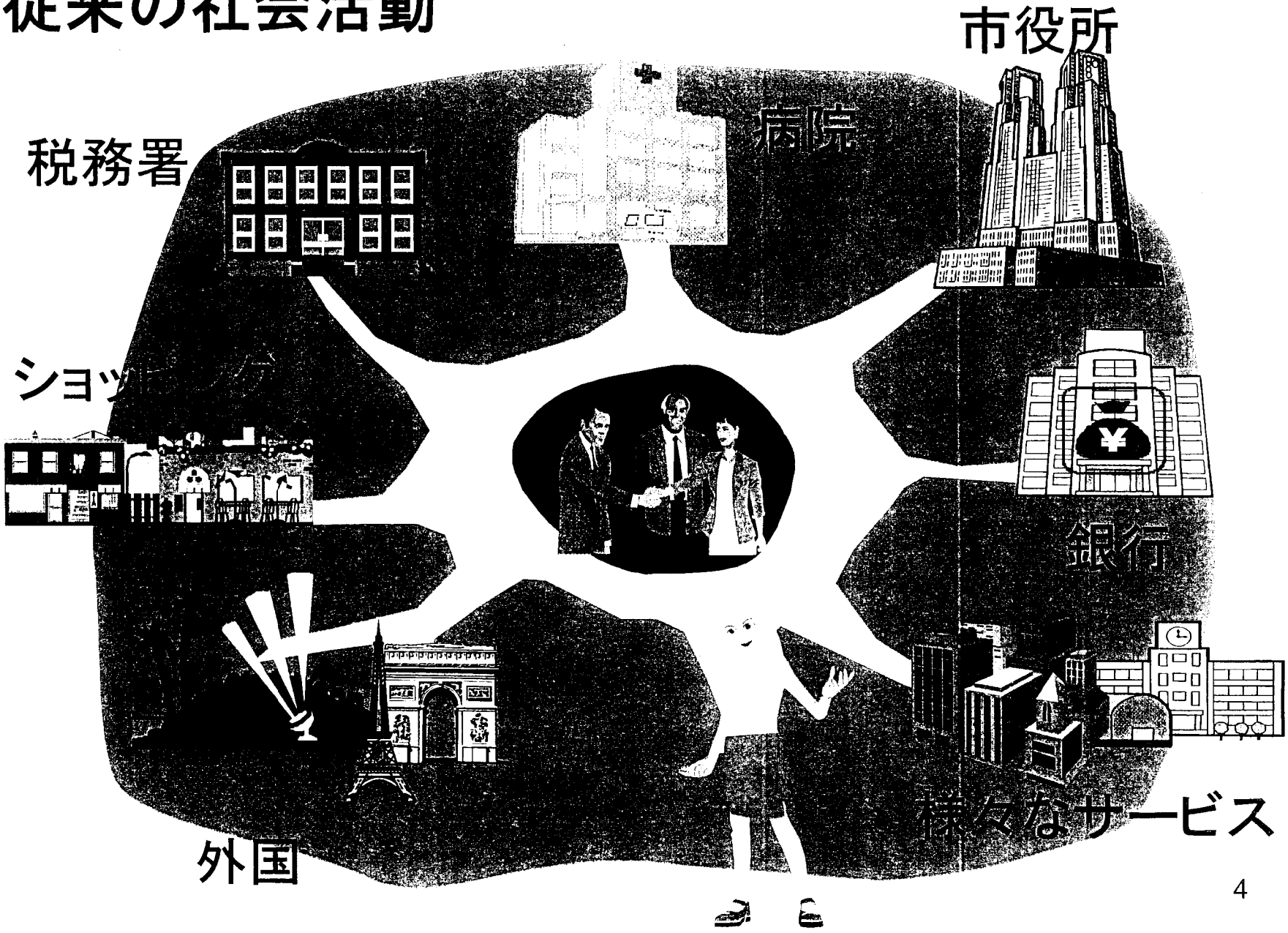
IT社会とは？

- 日々の社会活動が、ITにより支援される
- 社会活動がサイバースペースに拡大

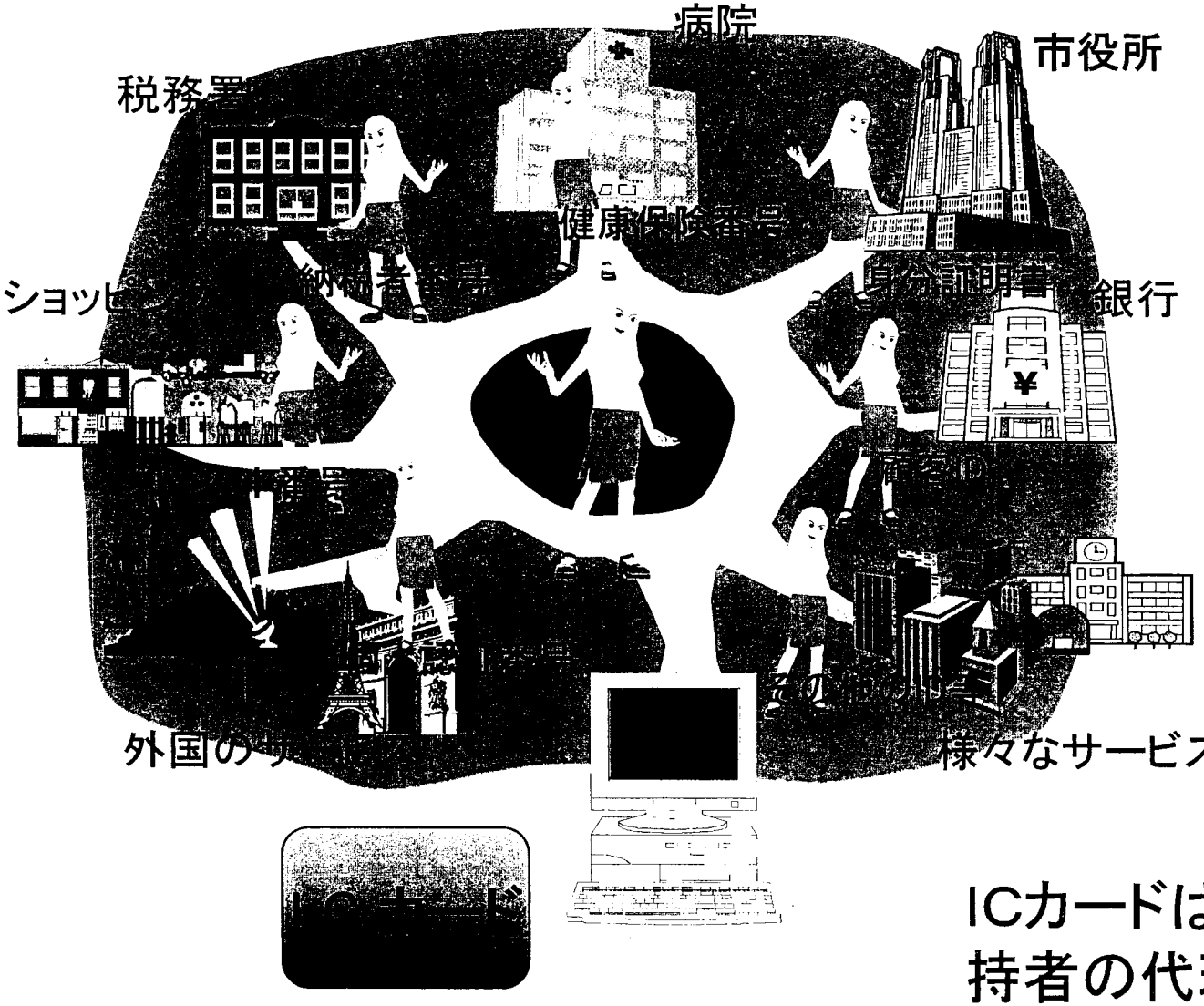
⇒ IT革命

- 活動空間は本人が自由に選択

従来の社会活動



サイバースペースにおける社会活動



公共分野

民間分野

ICカードは、カード所持者の代理機能

リアル空間と電子空間の整合

- 制度・法律
  - 個人、組織は、責任論で表裏一体　⇒　資格認証
  - 原則、同じでなければならない　⇒　個人情報保護にも適用
  - グローバル化は避けられない　⇒　日本のリーダーシップ
- 課題
  - 社会活動を行なうのに必要なものの機能の電子化
  - 有形物:　マネー、クレジットカード、各種証明書類　等
  - 無形物:　市民権　⇒　住民基本台帳　⇒　改正

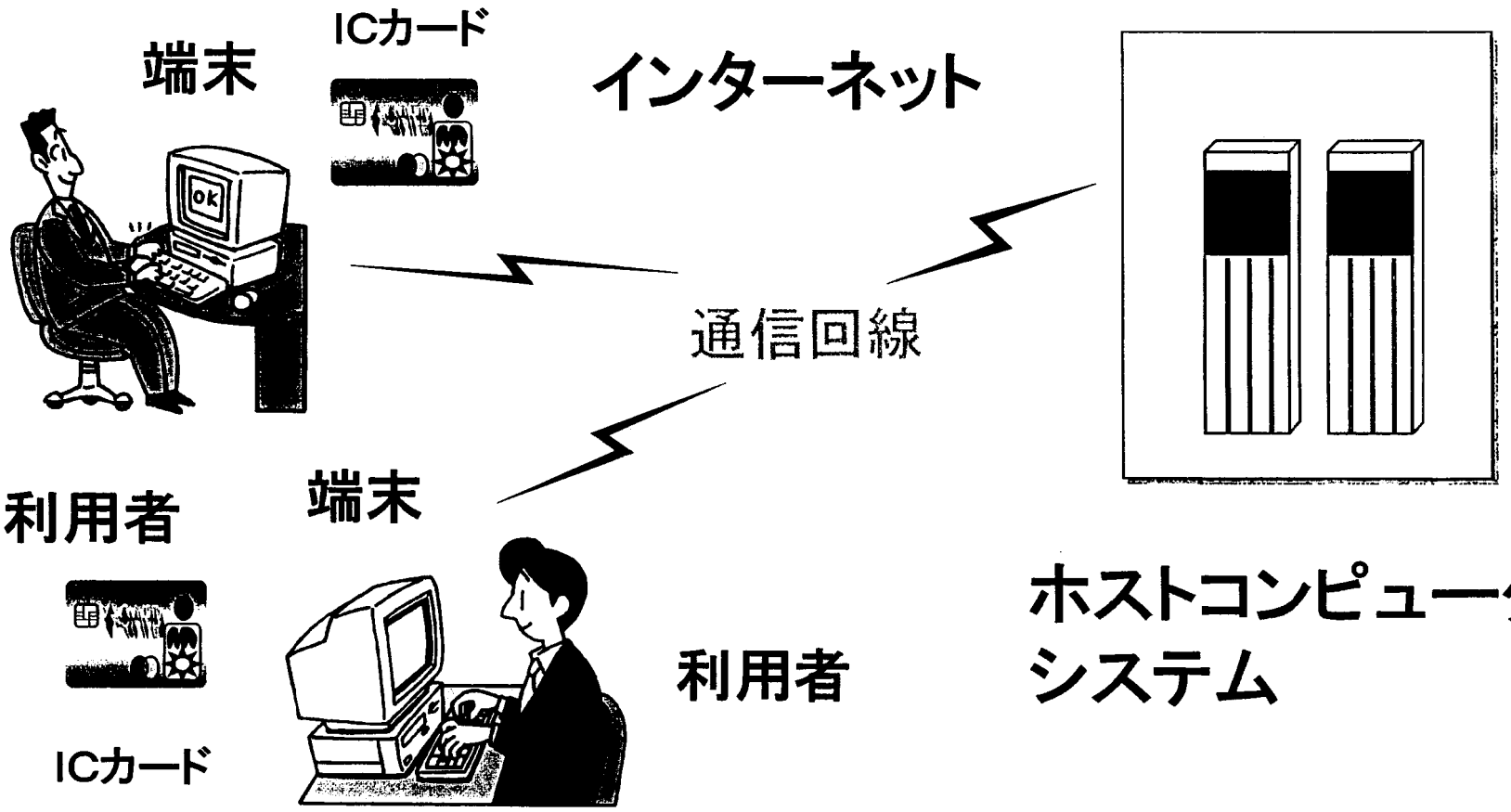
    ライセンス等　⇒　医師、税理士、行政書士等

    関連府省等の責任

セキュリティ技術について

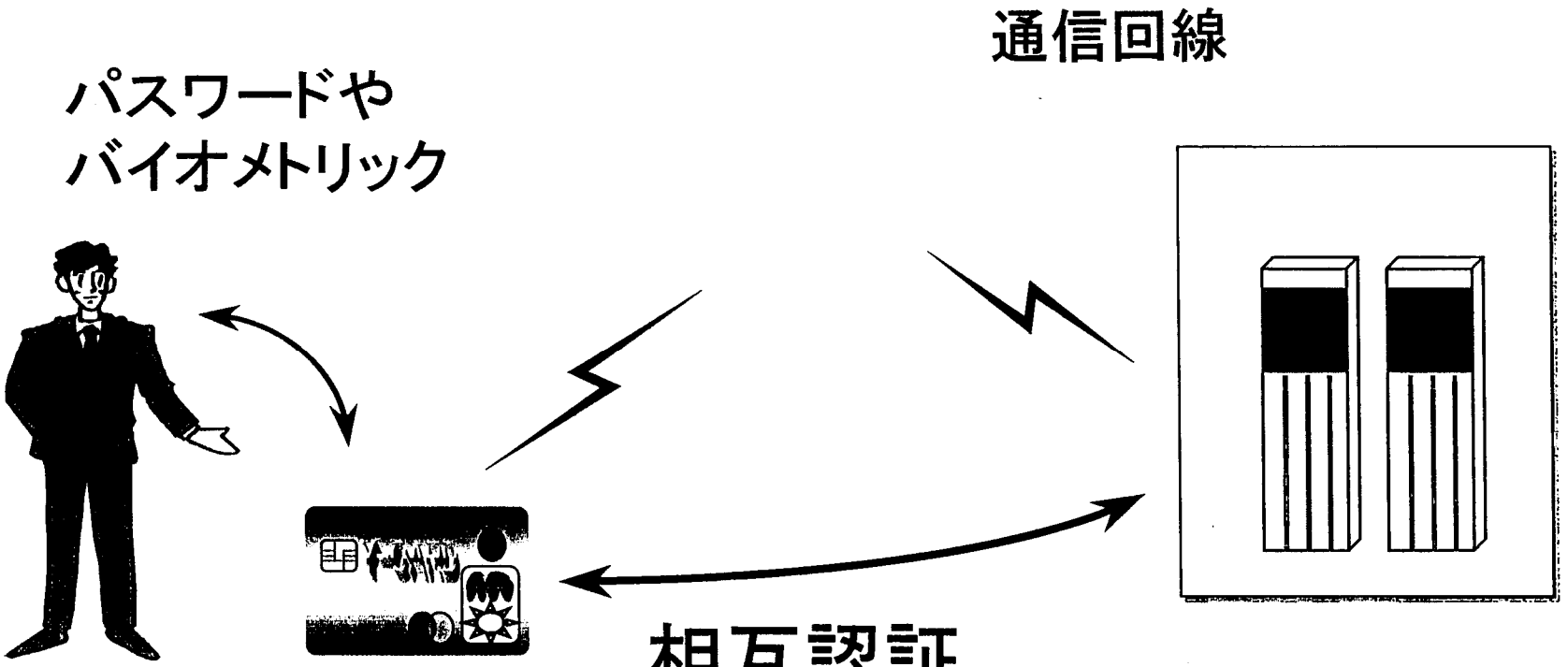
- 従来技術　⇒　例:金融系の情報システム
  - 情報システムを専用化する
  - 専用回線、専用端末、暗号技術などの利用
  - システムの仕様は非公開
- 近年の傾向　⇒　オープンシステムに対応
  - end to endの相互認証と暗号通信
  - 暗号手法は公開　⇒　客観的な強度評価
  - 暗号鍵の安全な管理・運用　⇒　スマートカード

ネットワークシステムの基本構成



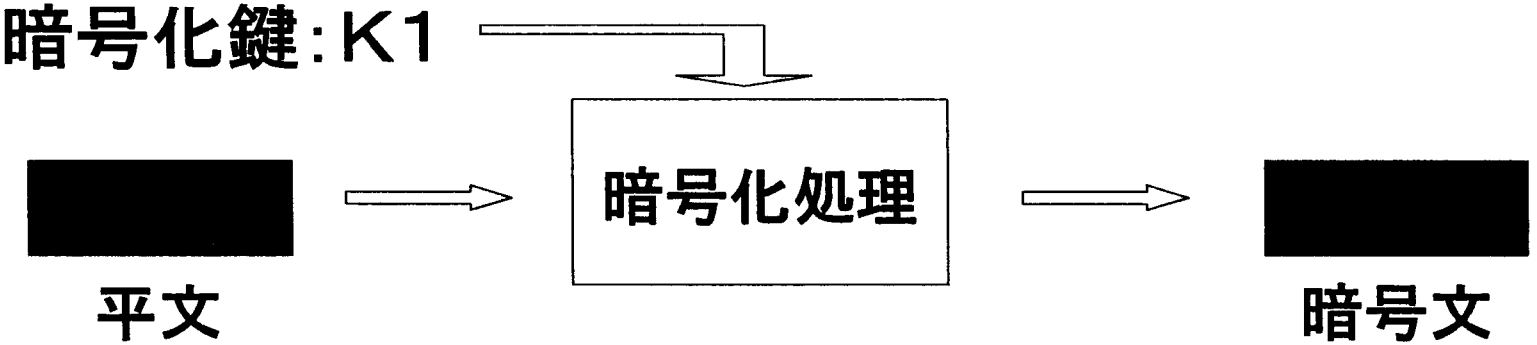
セキュリティを確保するためにend to endで相互確認

本人確認の考え方(オンライン)

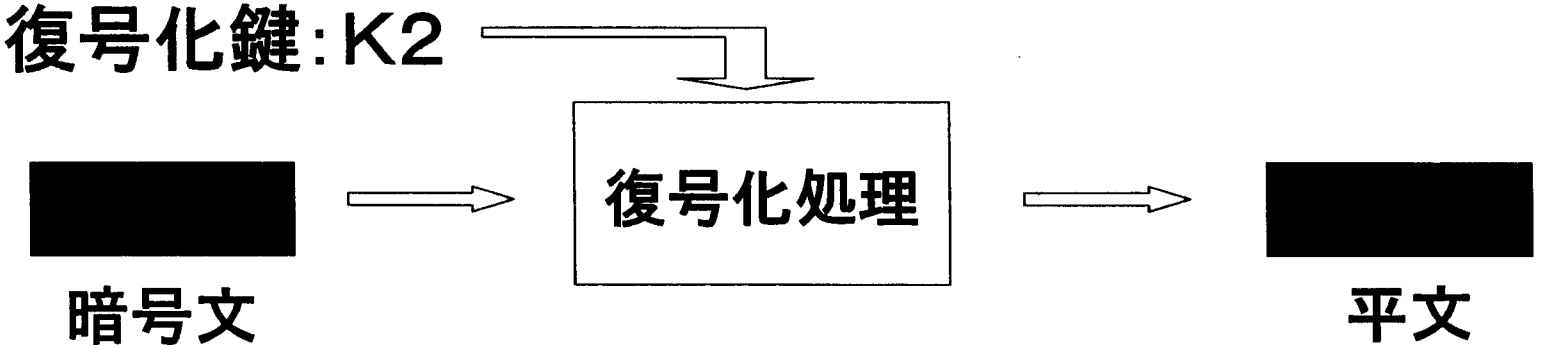


暗号手法について

暗号化鍵：K1



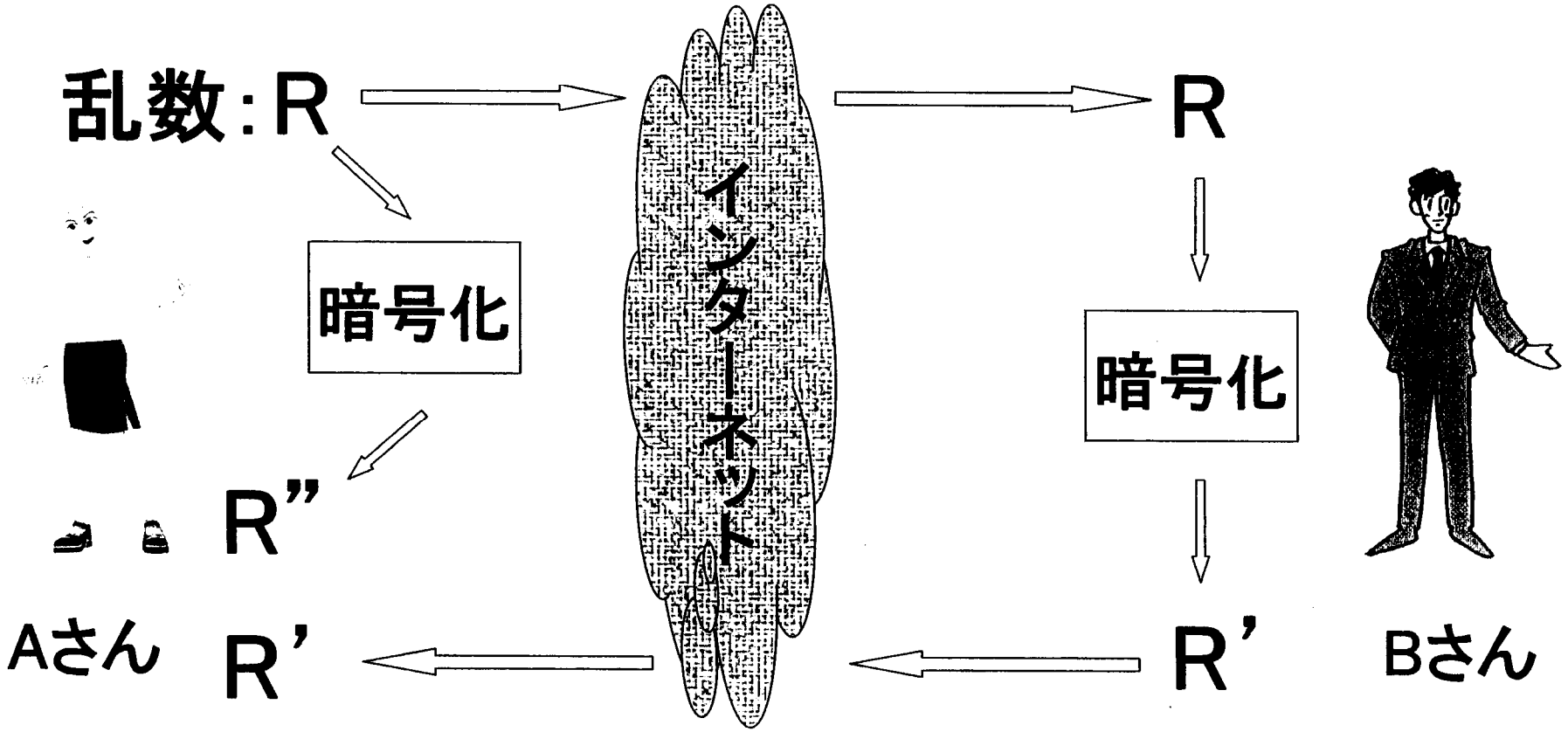
復号化鍵：K2



K1＝K2　；　秘密鍵共有（対称鍵）暗号方式

K1≠K2　；　公開鍵（非対称鍵）暗号方式　⇒　***電子署名***

暗号を用いた相互認証の手順



1. R'とR"が同じならば、Bさんは正しい鍵を知っている
2. 同じことをBさんからAさんに行なう ⇒ 相互認証

カードに関する基本知識(１)

- スマートカードって何？
  - CPU付きのICカードで、単なるメモリカードと区別するために欧米ではスマートカード呼んでいる
  - 数ミリ角のICチップにCPU、プログラム、暗号用補助演算装置、データ記録メモリが組み込まれている ⇒ 安全な超小型パソコン 等
- なぜ安全？
  - セキュリティ確保に必須な暗号演算を*カード内*で実施
  - 暗号鍵は、カードから取り出せない
  - 接続するコンピュータを相互に確認できる 等

カードに関する基本知識(2)

- どう使うの？
  - データキャリ
    - オフラインでの利用
    - 重要な情報をカードに記録する
    - 安全な記録が可能だが、容量に制限がある
    - 従来の保健医療カードなど
  - 認証デバイス
    - オンラインでの利用
    - 認証用の鍵を記録　⇒　各アプリのデータ量は少ない
    - ネットワークを必要とするが、容量に制限は無い
    - これからの利用法

これらの使い方を組み合わせた最適化が重要