

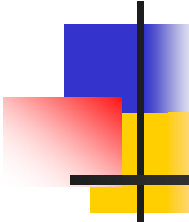
価値と信用を取り扱う半導体技術への要求

安浦, 寛人
九州大学大学院システム情報科学研究院 | 九州大学システムLSI研究センター

<https://hdl.handle.net/2324/9113>

出版情報 : SLRC プレゼンテーション, 2005-04-15. 九州大学システムLSI研究センター
バージョン :
権利関係 :



A decorative graphic on the left side of the slide, consisting of a black crosshair with a blue square in the top-left quadrant, a red square in the bottom-left quadrant, and a yellow square in the bottom-right quadrant.

価値と信用を取り扱う半導体技術への要求

安浦寛人

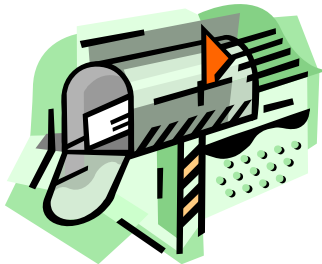
九州大学システムLSI研究センター

2005.4.16

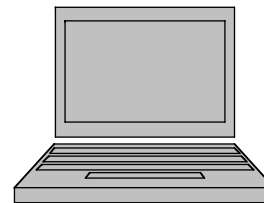
<http://www.slrc.kyushu-u.ac.jp>

社会基盤システムの再構築

- 20世紀は既存の社会システムの中に情報通信技術を部分的に導入し、サービスの高度化、高速化を進める時代であった。
- 通信速度、情報処理速度の向上は、システムの設計時に想定しなかった事態を生み出すようになった。
- 21世紀は情報通信技術を前提として社会システム自身を再設計する時代。



2005.4.16



Silicon Sea Belt





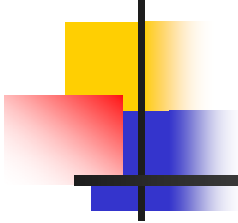
社会情報基盤とは？

- 各種社会システムの基盤となる基本的な情報技術(Social Information Infrastructure)
 - 情報ネットワークと情報通信技術
 - ハードウェア技術（主に半導体集積回路）
 - ソフトウェア技術
- エネルギーや土木、交通の基盤との違い
 - 基本技術の多くが民需ベースで発展
 - 大量の知財の集積の上に構築された技術
 - システムの開放性（インターネットやパソコン）
 - 社会の規則や制度への影響



ITによって何が変わったのか？

- 社会活動における物理的制約の削減
 - 距離の克服—情報通信ネットワークの整備
 - 価値情報や信用情報の移動に対する大きさ，重さ，時間の制約
- 社会システムにおける情報の影響が伝わる時間（時定数）
 - 人間の生理的情報処理能力は1000年前とほとんど変わらない.
 - 社会システムの時定数は50年で100万分の1 以下になった.
- 価値や信用の媒体とその裏付けの仕組み
 - 物質の保存則をベースにした過去の仕組みからの脱却
 - 完全なコピーが簡単にできるデジタル情報を利用した新しい仕組み
- ◆ IT技術を前提とした社会システムの再構築の必要性
 - ◆ ITで「価値」や「信用」をどのように取り扱うか？
 - ◆ 半導体は「価値」や「信用」の媒体となりえるか？

A decorative graphic consisting of overlapping yellow, red, and blue squares with a black crosshair.

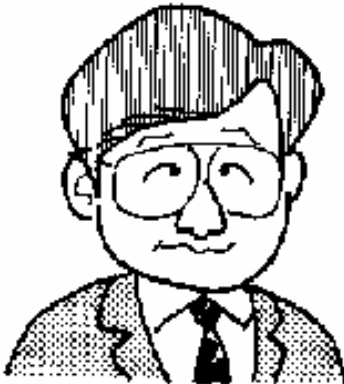
社会情報基盤の開発への要求

- 数十年有効なグランドデザイン
- 社会の安定と安全を確保する仕組み
- 一般の人に分かりやすい原理
- 個人を守るためのシステム
- 地球環境に負担をかけないシステム
- 開発、運用、保守のコストと効率

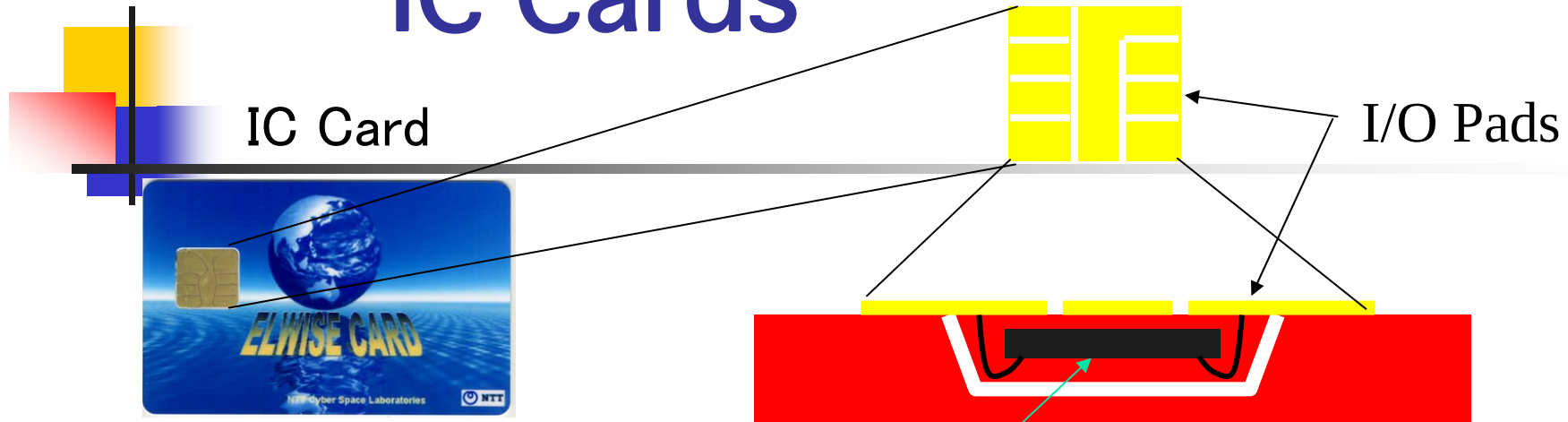
何ができるかより
どうあるべきかを考えることが重要

信用の基盤（相互認証）

- 電子マネー、電子政府などと騒がれているが。。
- 相手は信用できる？
- 自分が本人であることの証拠は？
- 電子化社会における「信用」の媒体は？

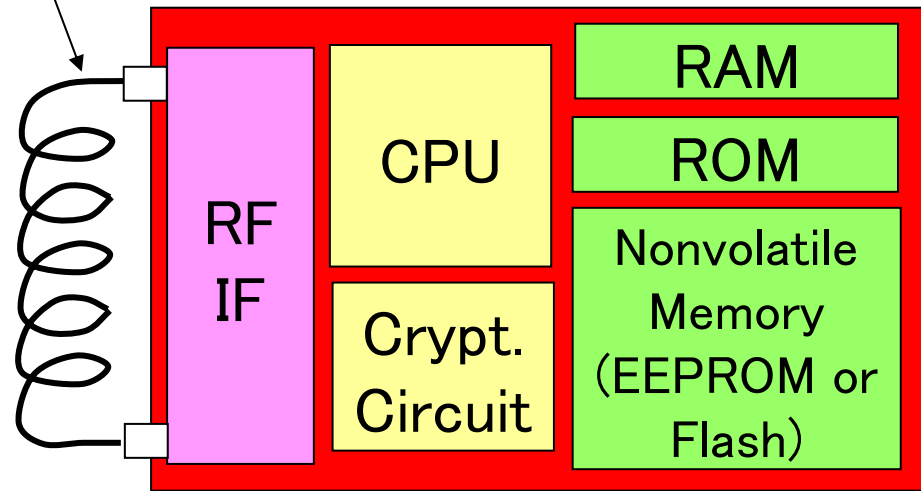


IC Cards

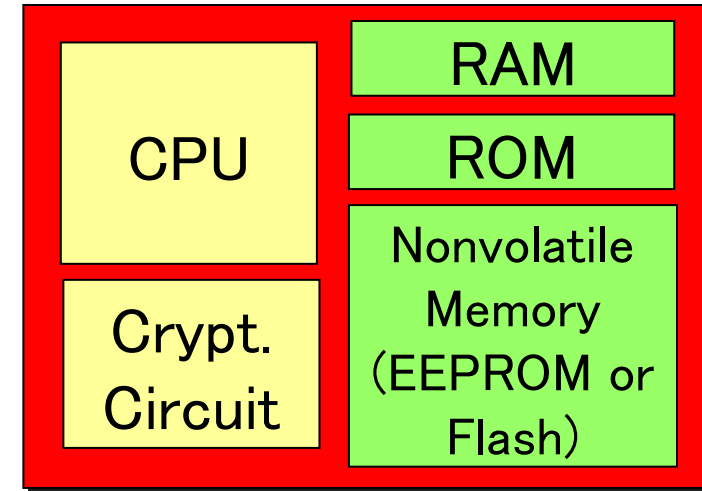


Antenna

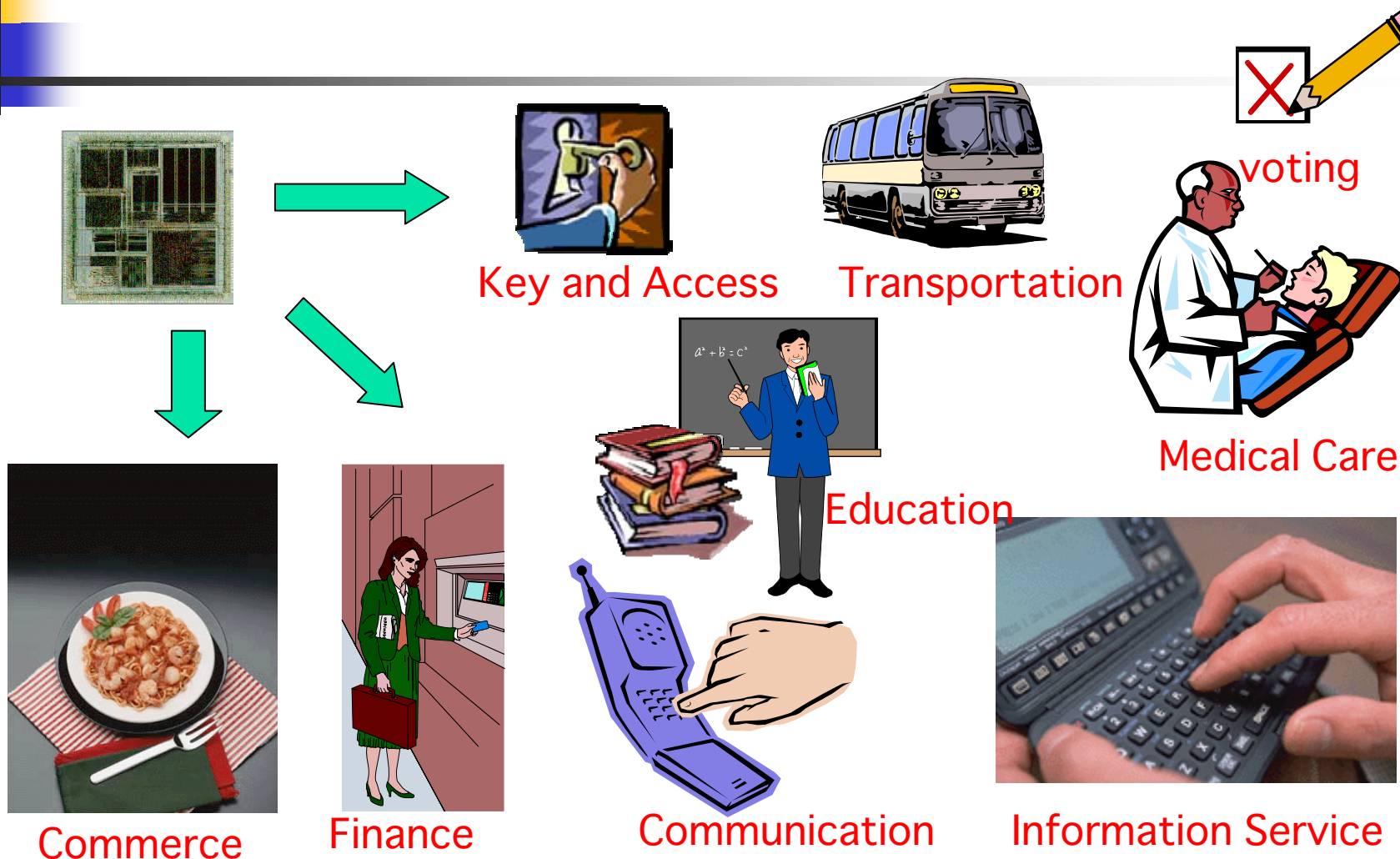
Non-Contact Type

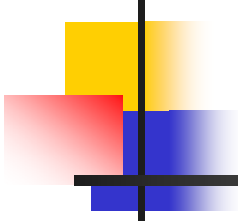


Contact Type



ICカードの利用





現在の認証基盤の問題点

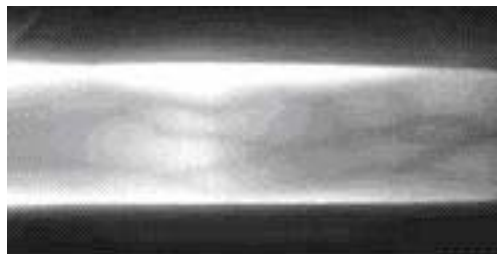
- 具体例
 - 身分証明書、ATMカード、クレジットカード、パスポート、免許証、印鑑など
- 相互認証ではない（一方向認証）
- 偽造に対する強さ
- 電子化・デジタル化による利点・欠点
- 仕組みや原理の複雑さ（PKI）

認証の落とし穴

- 盗まれたことがわからない情報（パスワード、指紋）
- 盗まれても変えられない情報（生体認証：指紋、静脈、虹彩、声紋、DNA）
- 個人情報の重さ（個人情報保護法）



2005.4.16



Silicon Sea Belt



価値媒体の基盤

- IT技術で「価値」を担えるか？
- コピー可能な電子情報が「価値」を媒介できるか？
- 偽造、窃盗の新しい手法への対応は可能か？
- 匿名性を保ったままの決済手段が構築できるか？
- 私的マネーや国外通貨の利用を阻止できるか？
- 徴税システムを維持できるか？（国家存続の危機）
- 給料をEdyでもらってうれしいか？



古代ローマの金貨
紀元前1世紀

2005.4.16



日本の最初の紙幣
16世紀



最初の円札 1872



?

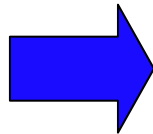
Silicon Sea Belt

歴史的な大問題

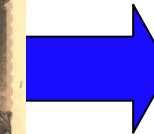
- 人類は、紙幣の発明に2000年かかった！



2,000 年



1,000年



電子マネー
21世紀？

金属貨幣

紀元前10世紀以前

- 価値は金属の希少性と不変性で保証

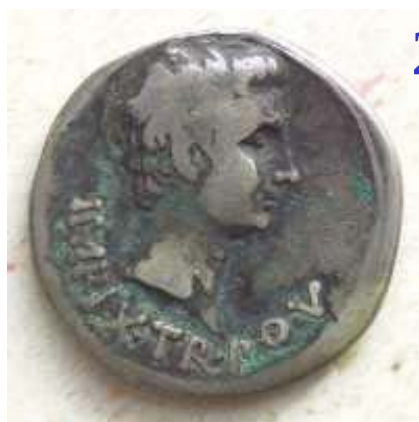
紙幣：10世紀中国で発明

- 価値は政府などの発行者の権威と社会制度で保証
- 物質不滅の法則

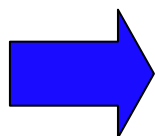
- 物理的保証の無い仕組み？

何が問題か？

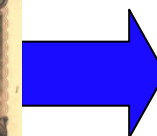
価値の量（大きさ）と保存則の保証



2,000 年



1,000年



金属貨幣

価値の量：物質（金属）

価値の保存則：物質保存則

紙幣

価値の量：情報（印刷）

価値の保存則：物質（紙）

電子マネー？

価値の量：情報

価値の保存則：情報

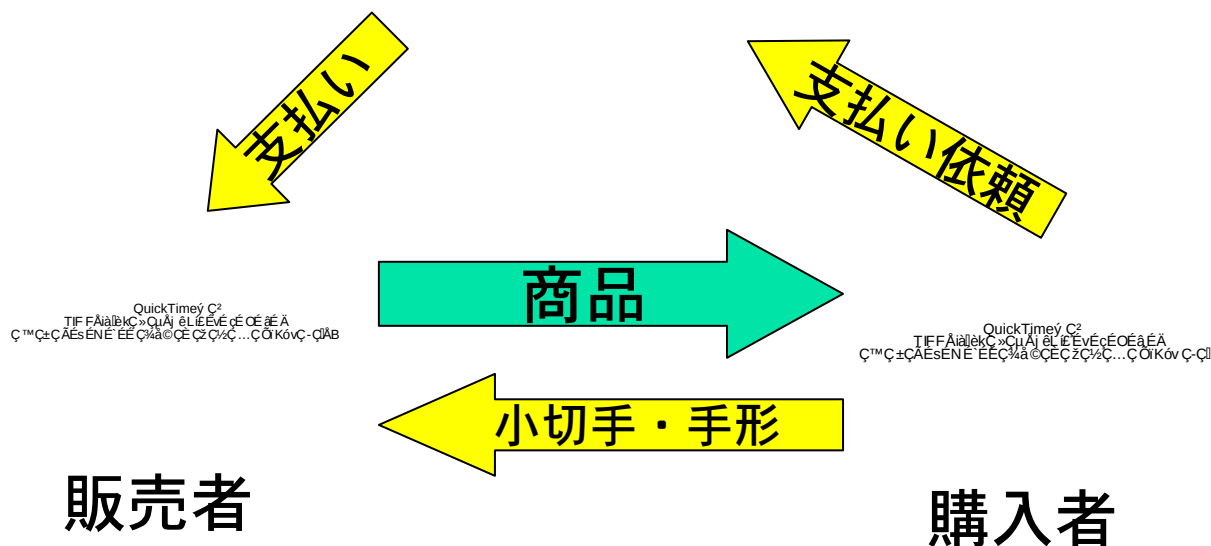
完全なコピーが可能な
情報で価値が保存できるか？

可能な解（信用取引）

金融機関
銀行・クレジット会社

第3者（金融機関）を介した
価値の移動

・価値の保存は第3者が保証



現金決済と信用取引

■ 現金決済システム(90兆円)

- 支払い完了性
- 匿名性
- 分散・オフライン
- 小口取引
- 電子化は可能か？

■ 信用取引システム(290兆円)

- 債務貨幣
- 大きな金額の取引の手段
- 電子化の鍵は認証技術

QuickTimey C2
TIF FÄiäÜkC»QuÄj èLüÉVÉ cÉ OÉ äÉ Ä
Ç™Ç±ÇÄEsENÉ EÉÇ4a©QE ÇZÇ¼Ç...ÇÖKóvÇ-QIÄB

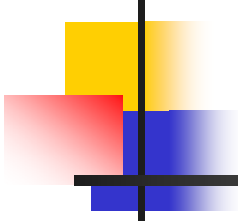
販売者

商品

現金

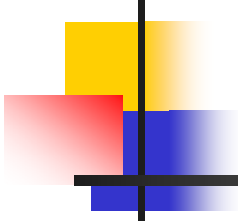
QuickTimey C2
TIF FÄiäÜkC»QuÄj èLüÉVÉ cÉ OÉ äÉ Ä
Ç™Ç±ÇÄEsENÉ EÉÇ4a©QE ÇZÇ¼Ç...ÇÖKóvÇ-QIÄB

購入者



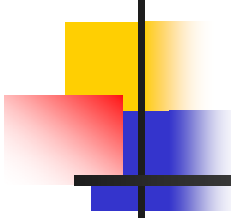
社会的な問題

- 電子マネー発行機関の多様化
 - 中央銀行券以外の通貨
 - プライベートマネー
 - （航空会社のマイレージ，クレジット会社のポイントなど）
 - 外国通貨の併用
 - 金融経済政策への影響
 - 徴税の問題
 - 電子取引への課税方法
 - プライベートマネーへの課税方法と法体系
 - どのように把握・検証するか？
- 新しい社会体制と技術体系
 - 価値や信用を取り扱う情報技術
 - 個人の財産管理
 - 新しい価値の流通システム
- 本質的な問題ーデジタルデータは完全なコピーが簡単にできる。



セキュリティとLSI

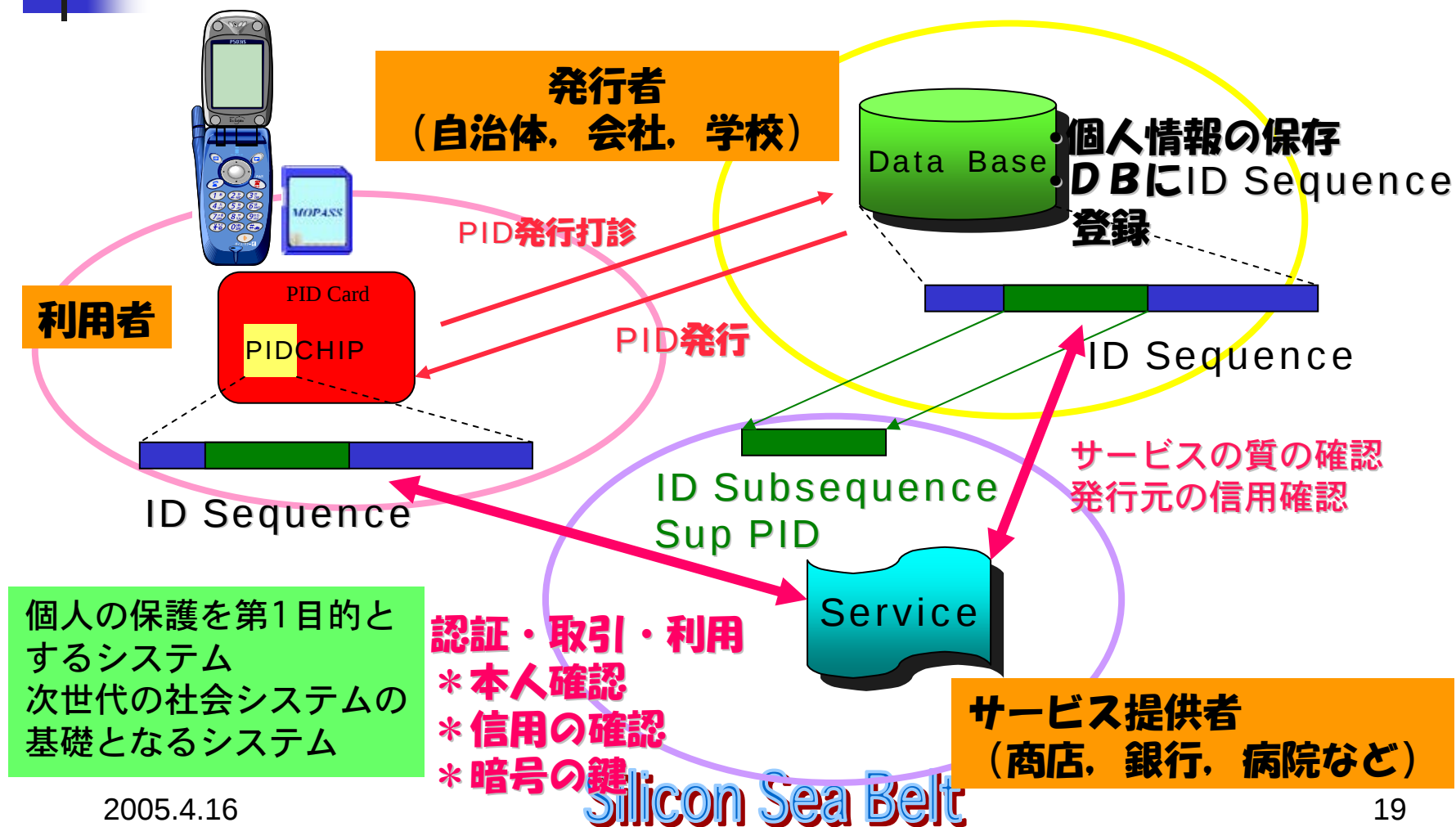
- LSIが「価値」や「信用」の媒体となる時代
- 暗号だけが問題ではない！社会システム自身に内在する危険を考えることが重要
- 攻撃者には格好の標的！



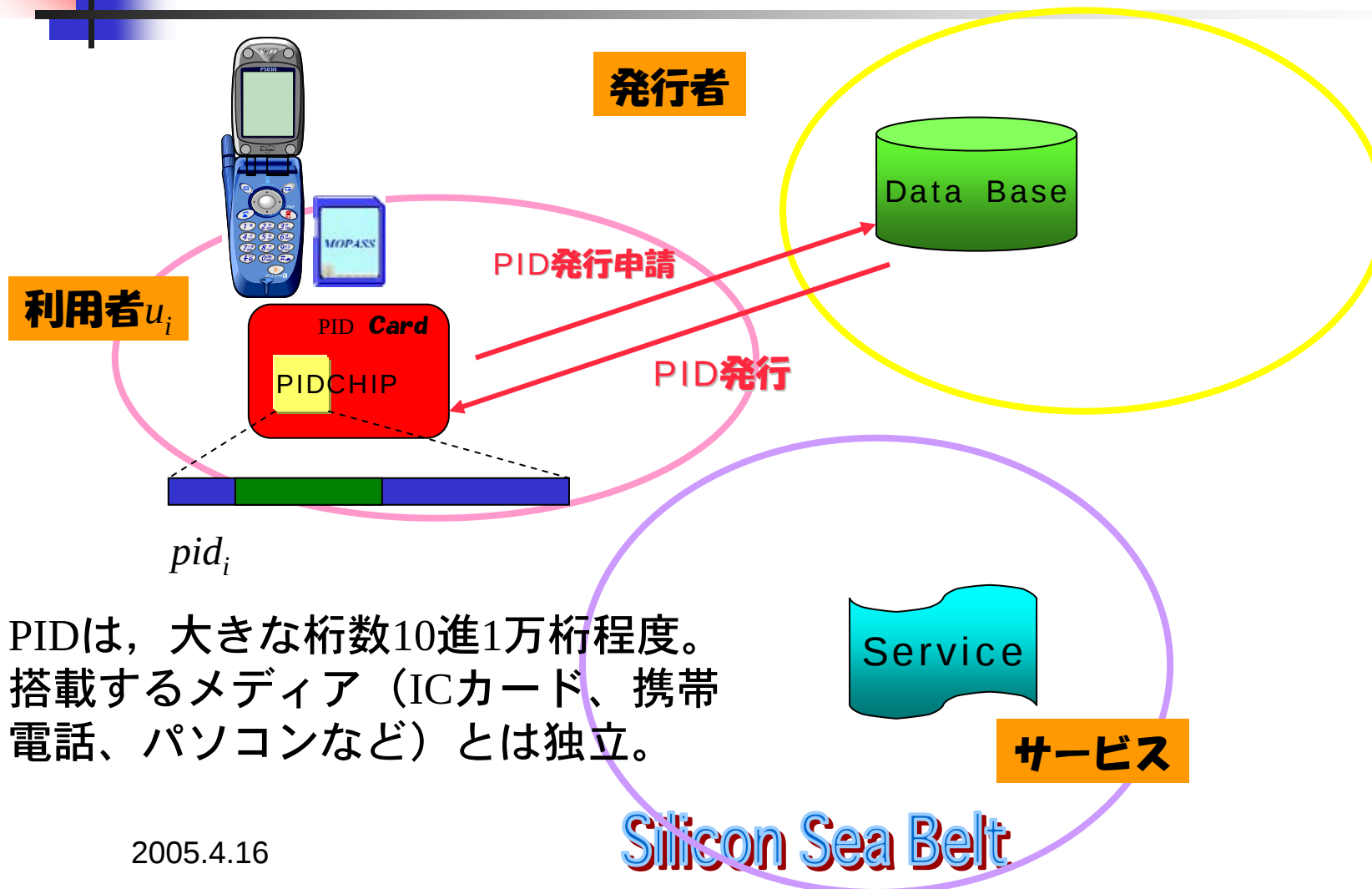
個人認証基盤

- 電子化社会における相互認証のしくみ
 - 電子化社会の基盤情報技術
 - 電子化した信用情報による相互認証のしくみ
 - 集積回路技術の利用（メモリ量，計算能力）
 - 単純な原理とメディア独立性
 - 社会的信用の電子化のしくみ
 - リスク分散，情報分散のしくみ
 - 個人情報を守るシステム（個人情報保護法）

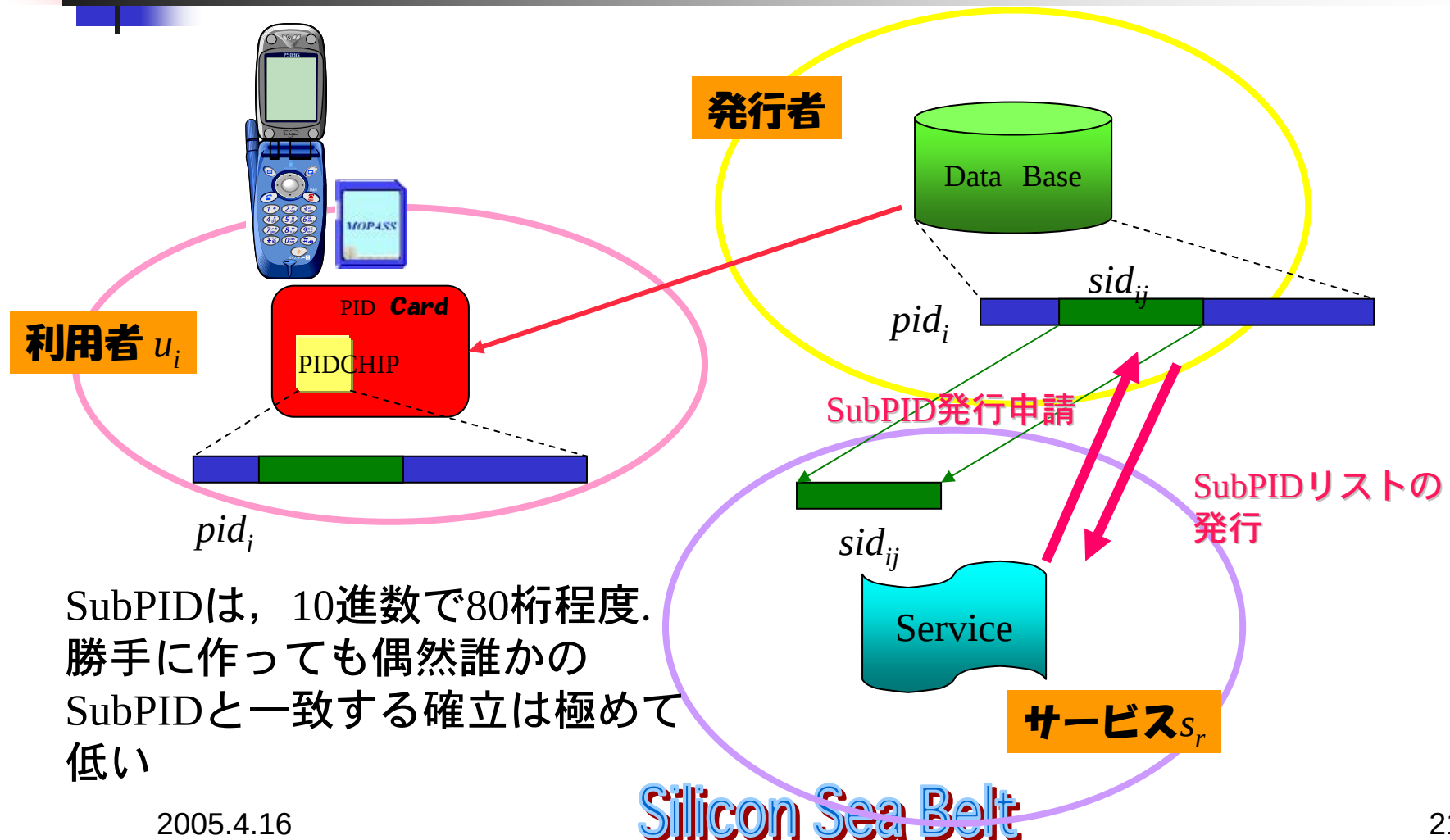
PIDとその利用



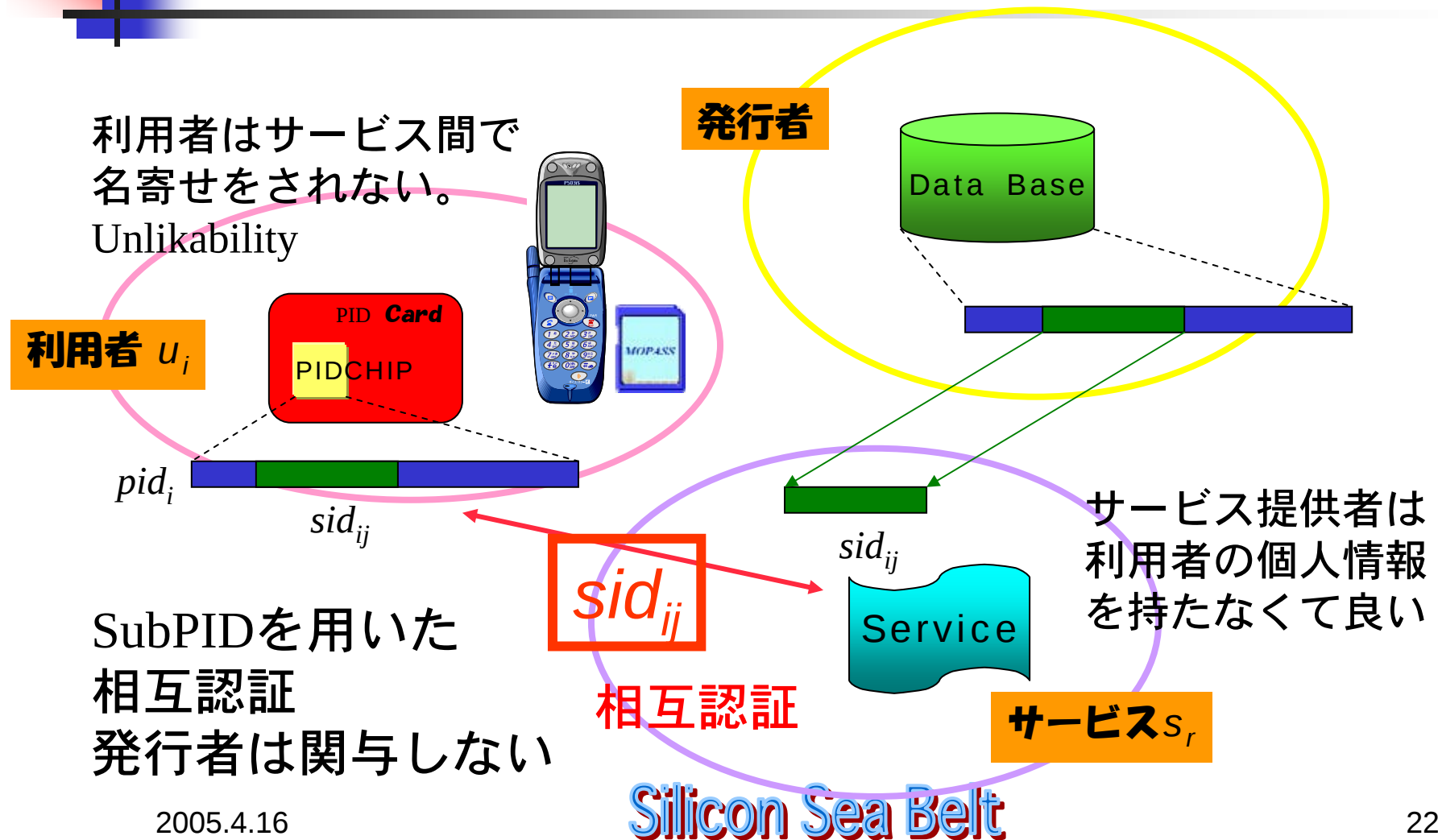
PIDの発行イメージ



サービスの認定イメージ

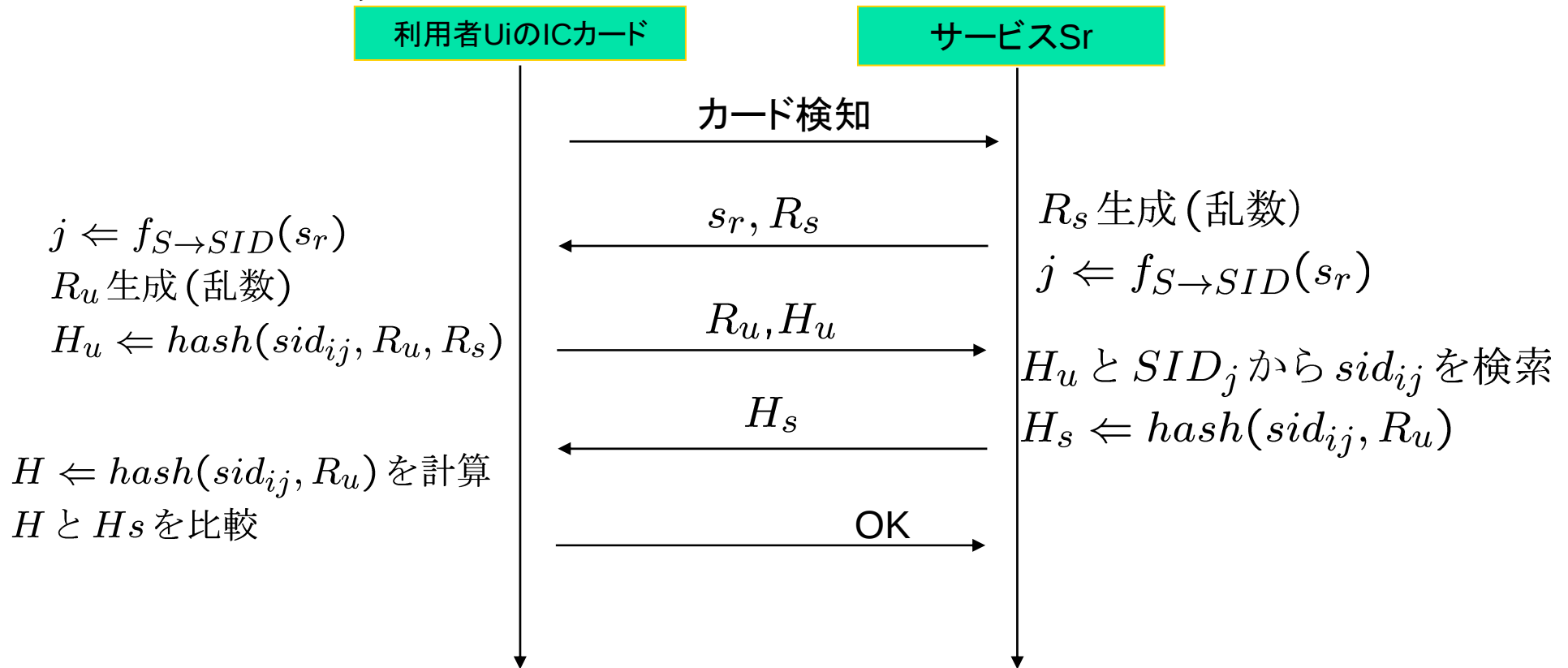


利用者とサービスのID照合

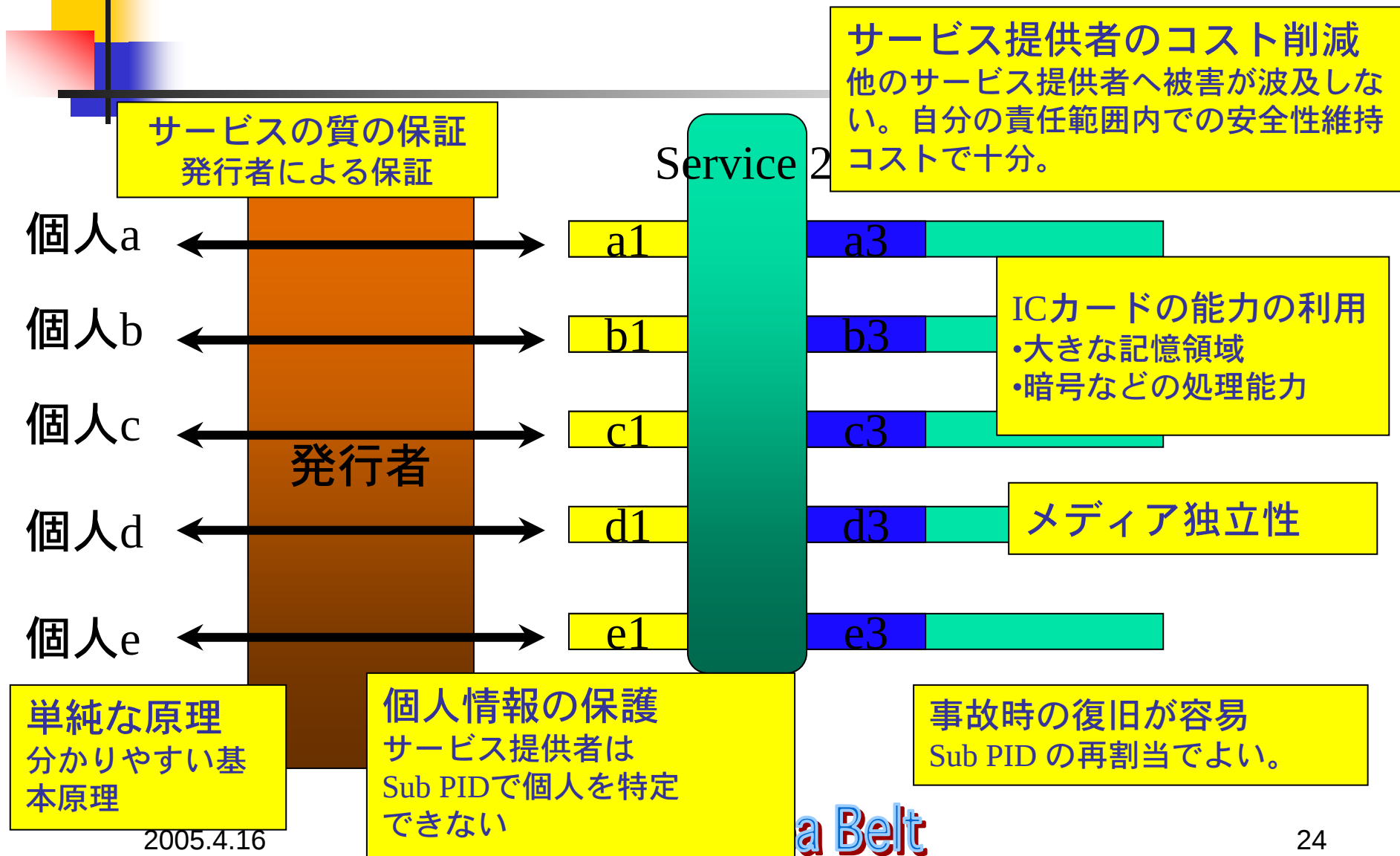


ID照合の Protokol 例

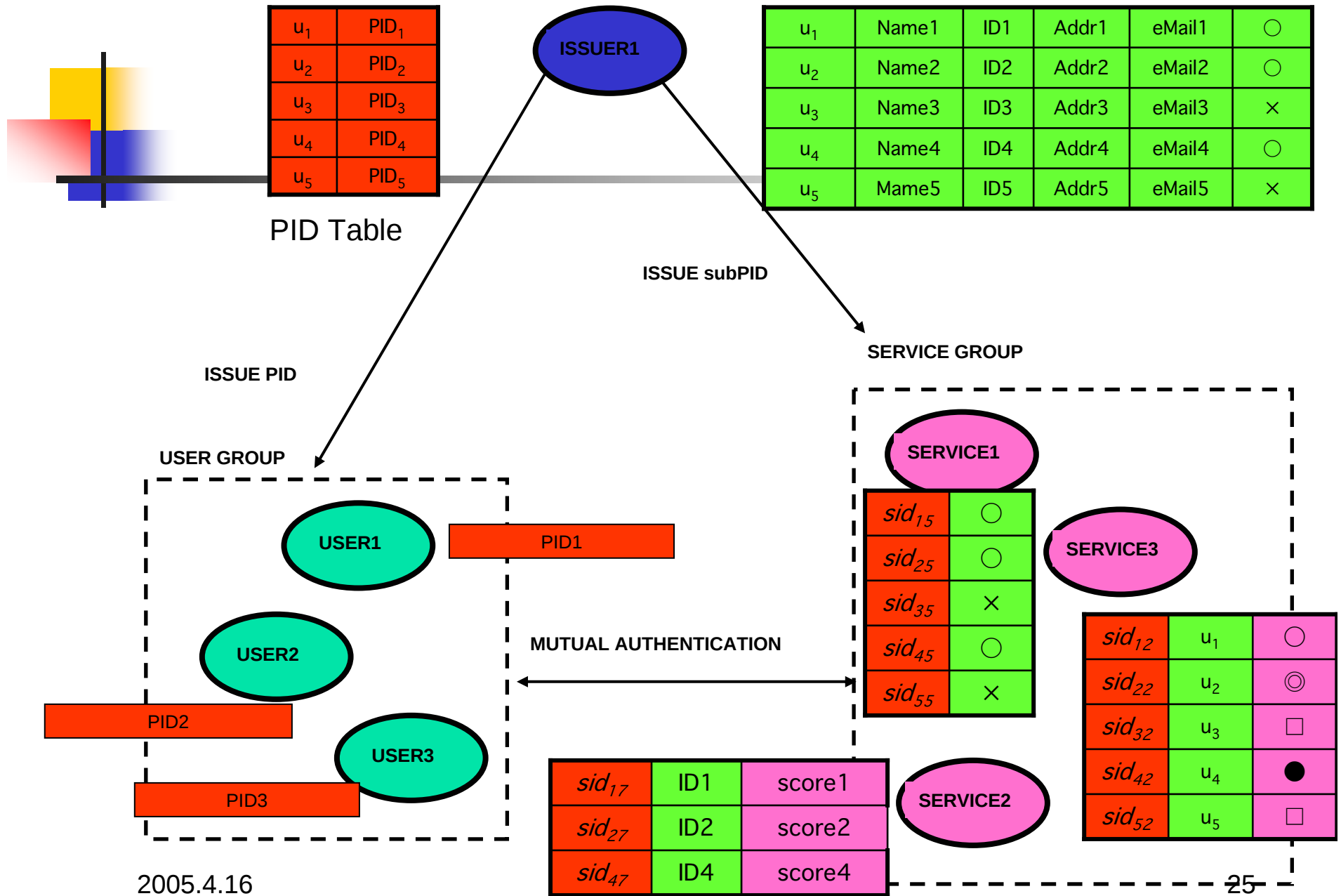
■ ハッシュ関数を使った方法



PIDの基本的構造



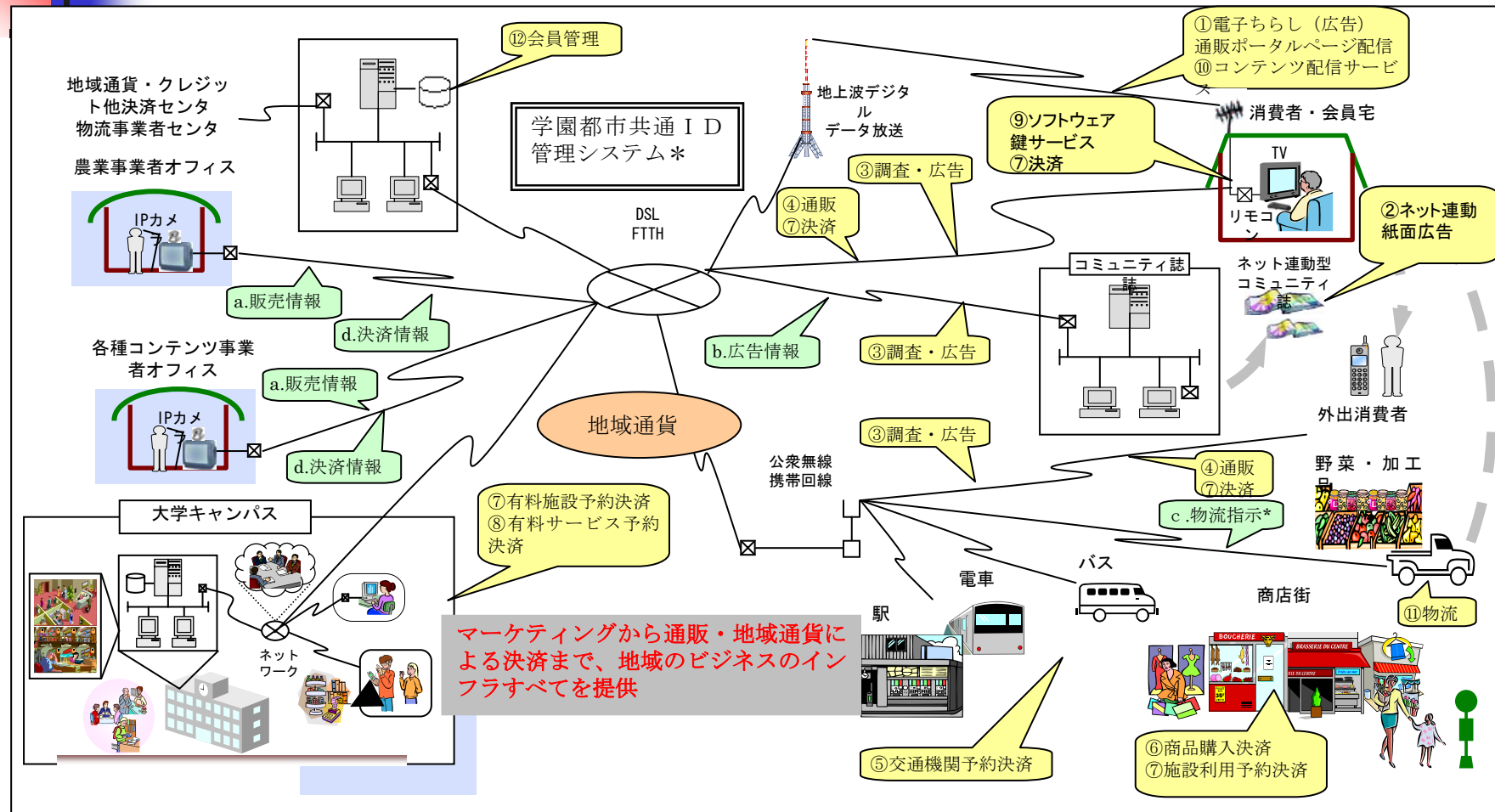
個人に関する情報の分散管理



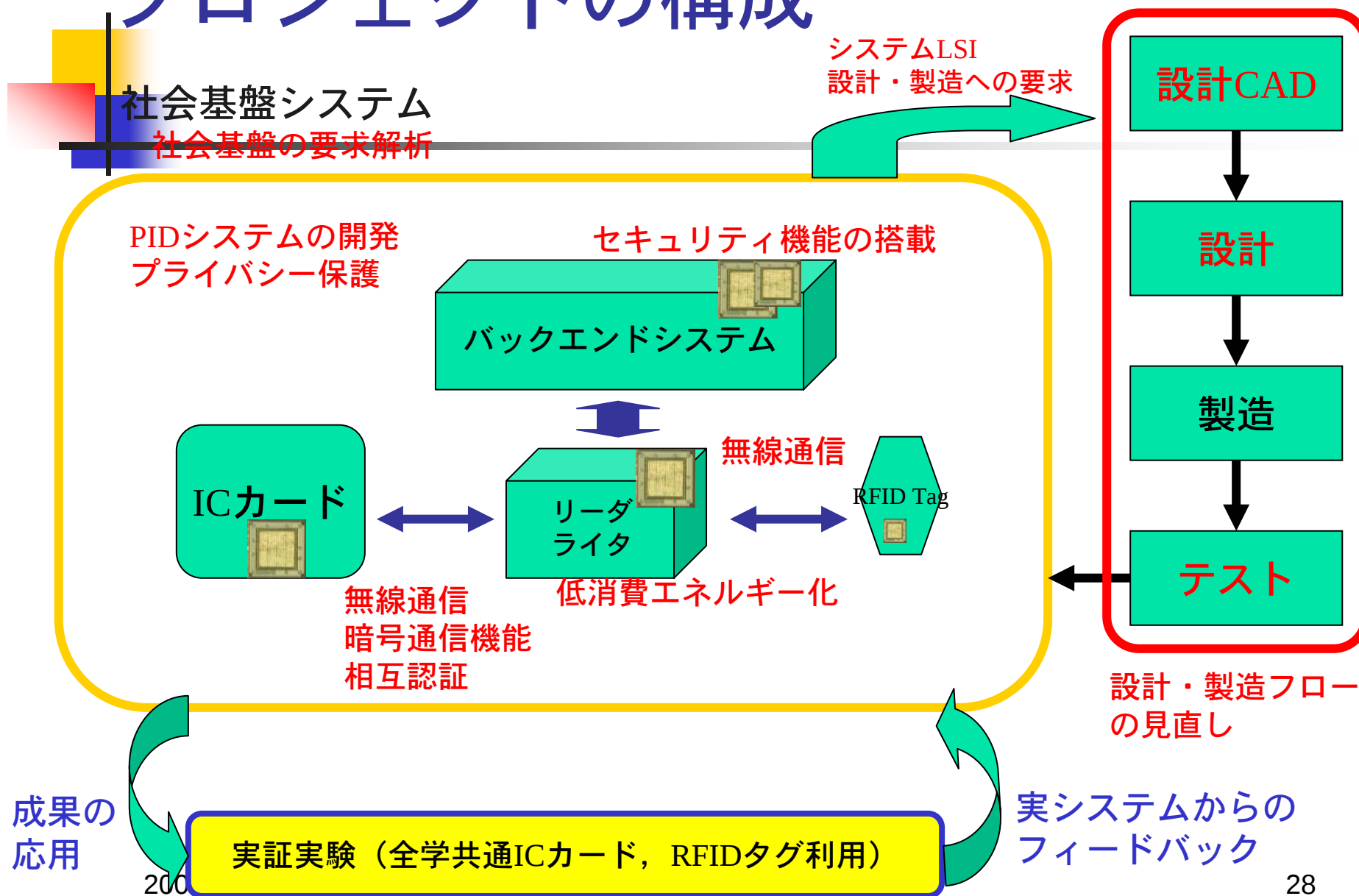
九州大学全学共通ICカード QUPID

- 平成18年4月までに実現すべきサービス
- 学生証および職員証としての機能
 - 視覚的に確認が可能な証明（券面印刷／写真）
 - 電子的に確認が可能な証明
- 建物への入館管理（新キャンパスH17夏より暫定運用）
- 図書館の入館および本の貸し出し管理
- 情報基盤センターの利用者ID
- 学生向け証明書自動発行機での利用

福岡カード(f-card)への発展



プロジェクトの構成

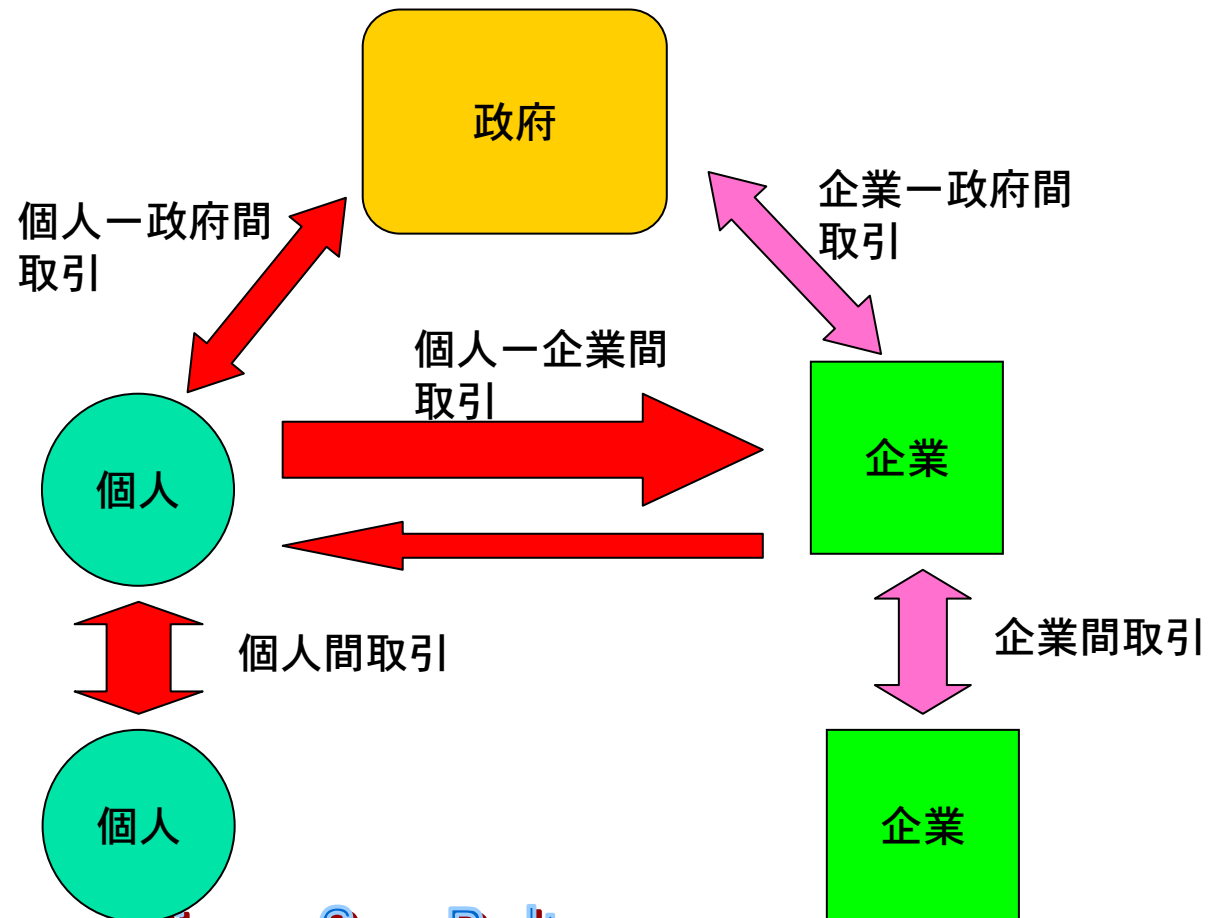


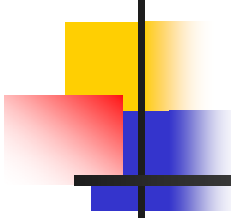
現金型電子化「価値」媒体の役割

必要な機能

- 価値保証性
- 支払い完了性
- 匿名性
- 転々流転性
- 小口決済機能
- オフライン性
- 直感的理解可能性
- 分散処理可能性
- 低コスト性
- 現金への換金性

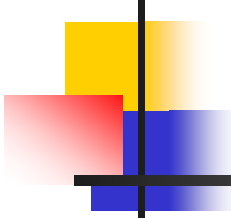
• すべての機能を実現しなくてもよい





電子的価値媒体の実現への条件

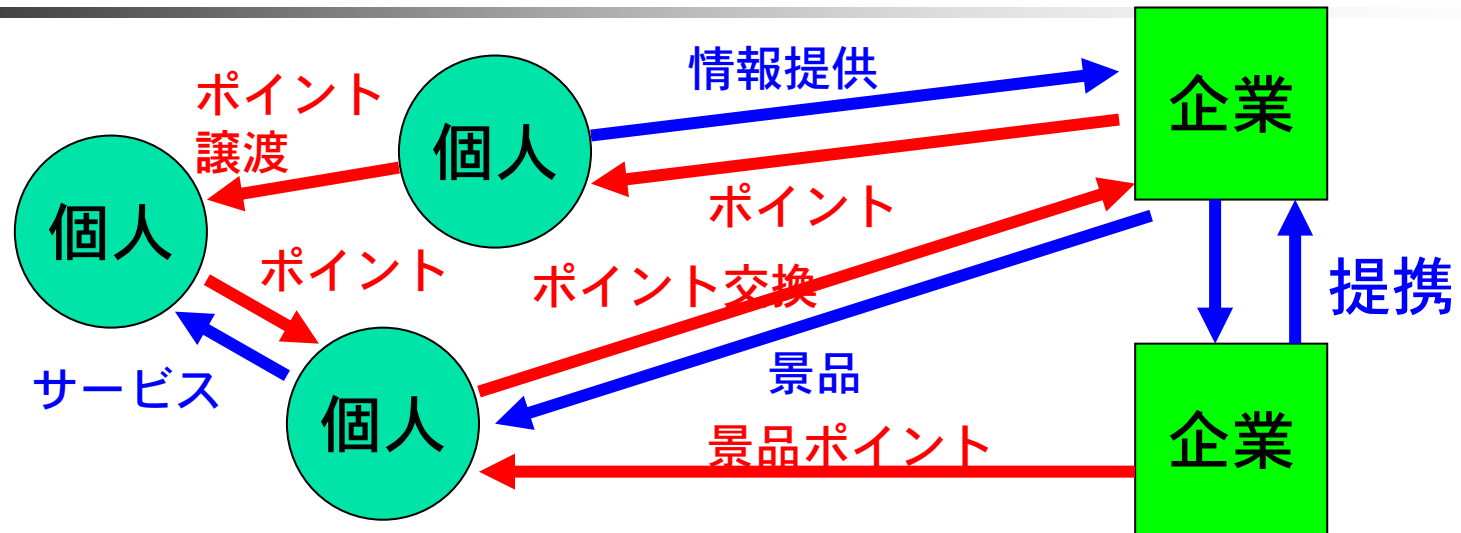
- 価値交換のしくみ
 - 支払った額＝受け取った額の保証
 - 支払い完了の確認手段
 - 取引の証拠性
- 価値保存のしくみ
 - 保存媒体
 - 残額確認手段
 - 証拠性
- 安全性
 - 贋「価値」の防止（予防、検知、抑制）手段
 - 媒体（デバイス）、システム、組織
 - 信用性と教育



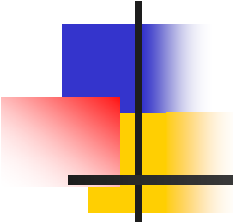
何が求められているか？

- 情報技術を用いた電子的価値媒体の原理の開発
 - 匿名性
 - 転々流転性
 - オフライン性
 - 直感的理解可能性
 - 低コスト性
- 上記原理を用いた実用システムの開発と実証実験
 - 現金とのリンクは必ずしも必要ではない
 - 低コストの静脈系

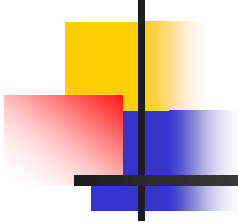
情報系サービスに対する静脈系



- 情報系のサービス（コンテンツ売買、計算サービス、資源貸与、付加的サービス、景品ポイント）などの還流系・利用経費回収系の構築
- 現金とのリンクは必ずしも必要でない（マイレージ、パチンコの玉）

A decorative graphic on the left side of the slide, featuring a black crosshair. The top-left quadrant of the crosshair is filled with a blue square, the bottom-left with a red square, and the bottom-right with a yellow square. The text "危険はどこに？" is positioned to the right of this graphic.

危険はどこに？

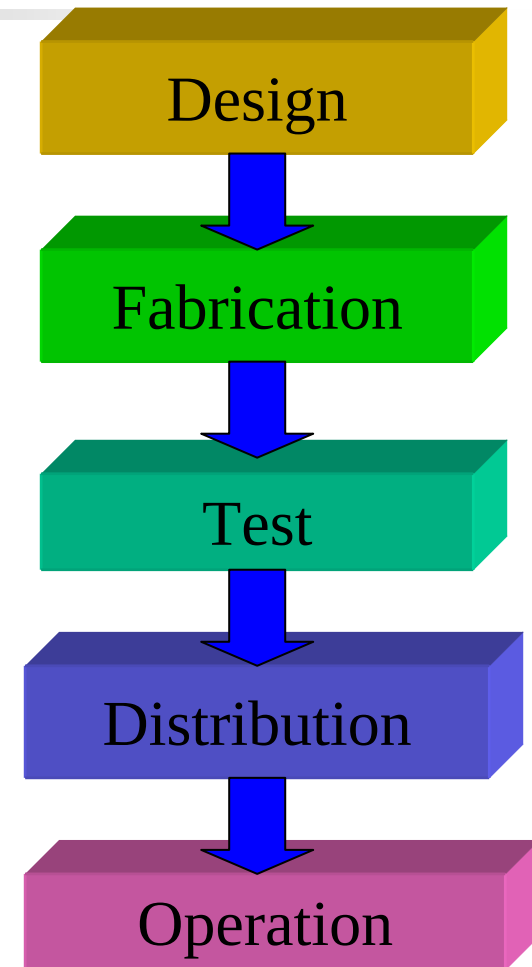


安全・安心を守るIT

- 暗号
 - 公開鍵暗号 (RSA, Elliptic Curve etc.)、共通鍵暗号 (DES, AES)
 - 設計法、解析手法の研究
 - 応用技術と標準化
- ネットワークにおける安全対策技術
 - 攻撃からの防御システム (Fire walls, Network structure)
- 通信内容の安全性確保
 - 安全な通信プロトコル
- ソフトウェアの安全対策
 - ウィルスやワーム対策技術
- ハードウェアの安全対策
 - 耐タンパ性
 - サイドチャネルアタック対策

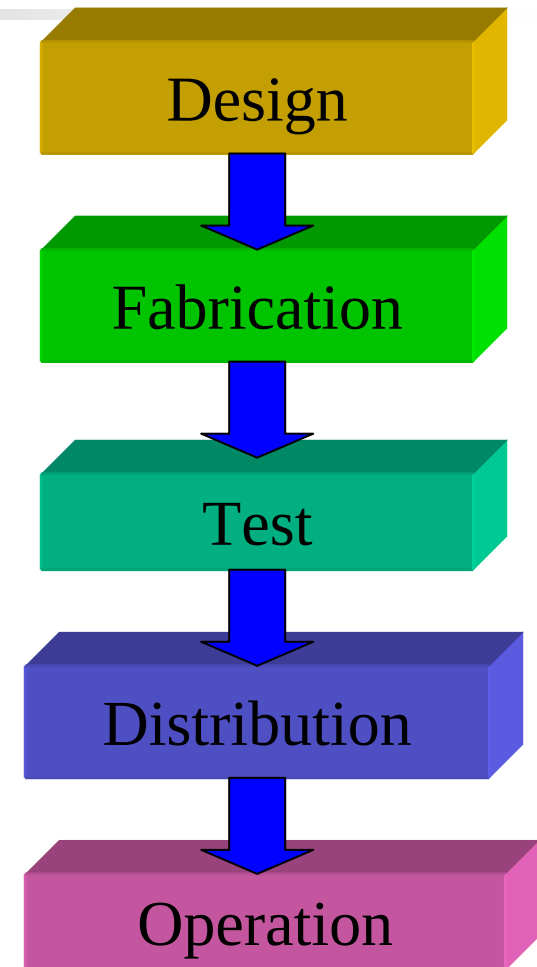
半導体デバイスへの攻撃

- 何が攻撃されるか?
 - デバイス上の情報（価値・信用情報）
 - デバイスの回路情報・プログラム
 - 社会システムや個人の財産
- いつ攻撃されるか?
 - 設計・製造段階
 - テストや流通の段階
 - 運用中
- なぜ攻撃されるか?
 - 不当な利益を得る為（主に隠れた攻撃）
 - 社会システムの破壊（テロリズム）



攻撃の可能性

- 設計データの漏洩・盗用
- EDAツールによる攻撃
 - スキャンパス自動挿入
 - 設計データの漏えい
 - 回路・レイアウトの変更
- チップの不正な増産
- テスト時の不正
 - 良品チップの横流し
 - テストデータや条件の漏洩
- パッケージなど後工程での盗難
- 搭載するソフトウェアからの攻撃
- 運用時の攻撃



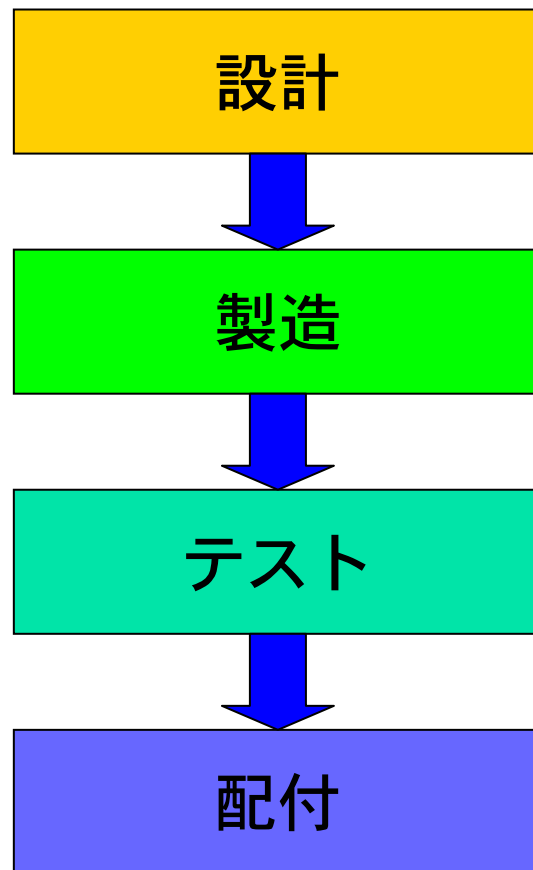
技術的課題

特殊性の実現

材料

加工方法

機能・性能



■ 特殊な設計・製造過程

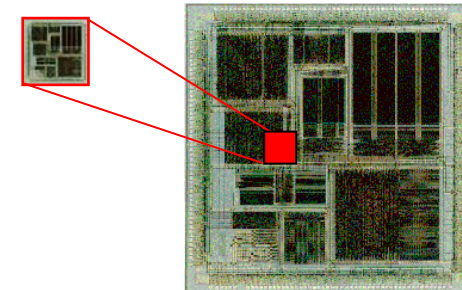
- 設計時の機密保持
- 製造時の不正防止
- テスト時の不法行為防止
- 配布時の盗難防止

■ 運用時の真贋性判定

- 電子的・非電子的
- 不正の検出機能

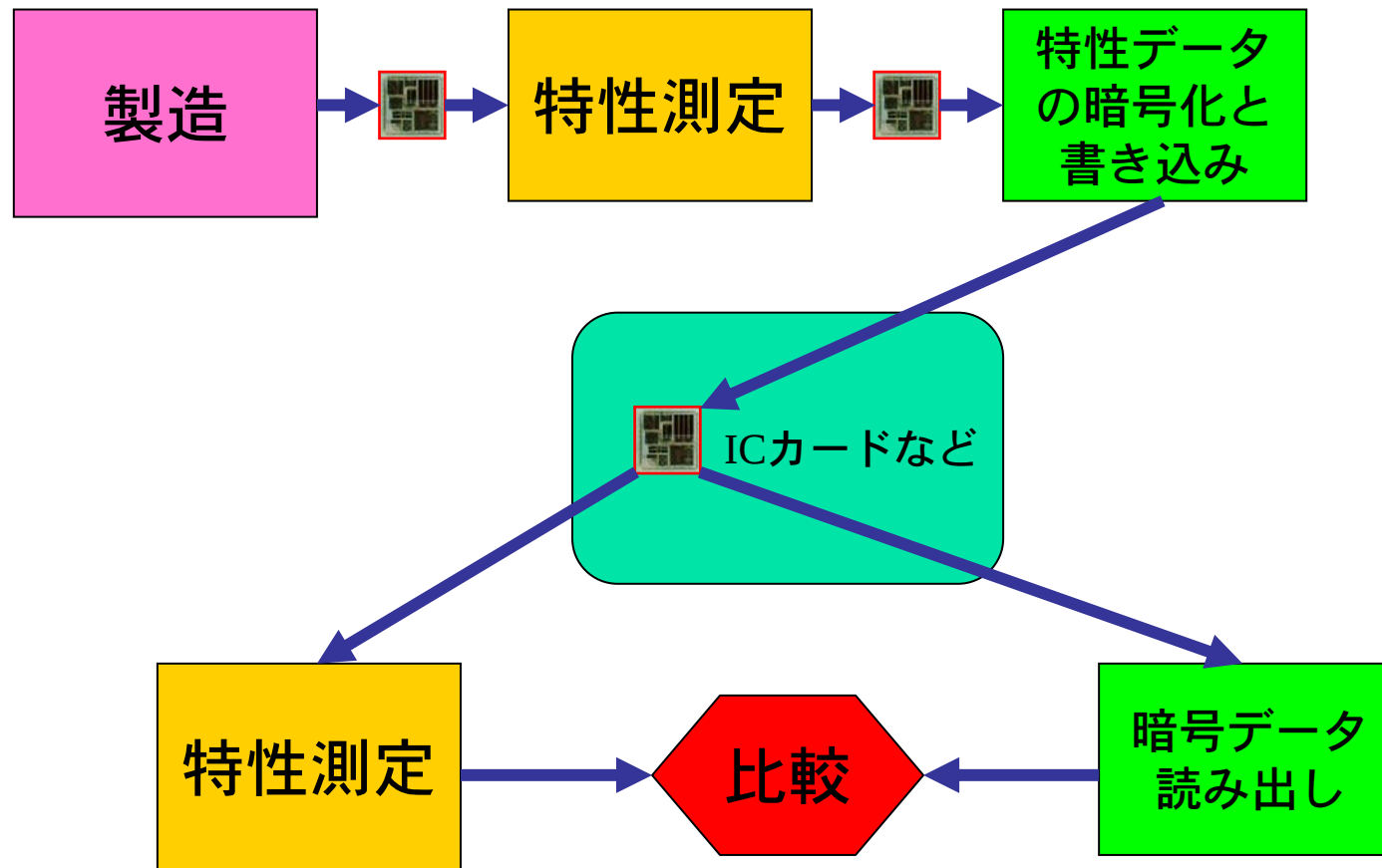
価値と信用を搭載するLSI

- 大半の機能は通常の半導体技術を使う（経済性）
- セキュリティに関する機能の部分だけを「特殊な方法」で設計・製造・テストする
- 付加価値の高いCoreとしてのSecurity Core
 - SWとして
 - IPとして
 - Chipとして(SiP技術の利用)
- 真贋性の判定方法
 - コストと有効性



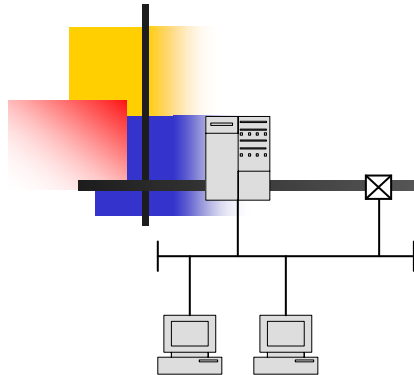
Security Core

真贋性保証の例

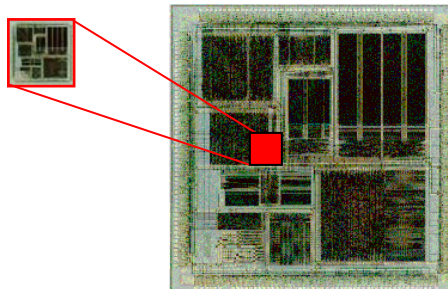


国家的研究課題例

電子的貨幣基盤の構築



Secure Core

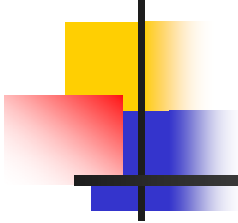


2005.4.16

システムレベル
社会システム（決済・徴税システム）
法体系、経済システム、通信・ネットワーク

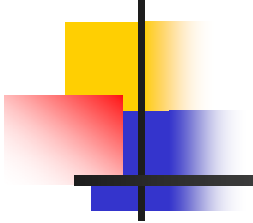
デバイスレベル
携帯電話・ICカード
発行・運用システム
セキュリティ技術（暗号）、プライバシー保護
組込みSW開発、危機管理

チップレベル
Security on a Chip（耐Tamper技術）
設計、製造、テスト段階での偽造防止技術
Secure Coreの分離、真贋性保証技術
「価値を載せられるシリコン」の技術



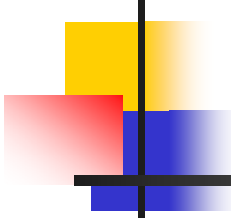
半導体関連企業への波及効果

- 半導体製造メーカー
 - 機密性の高い製造手法による製品への付加価値
 - 新しい応用分野（知財保護や信用取引）向け製品の開発
- 半導体製造機器メーカー
 - 特殊な製造装置と製造技術の開発
 - 一般端末における真贋判定機器への技術応用
- 半導体材料メーカー
 - 特殊な材料による安全性の確保
- マスクメーカー
 - 特殊なマスク技術の開発と安全管理技術の確立
- テスト機器メーカー
 - 耐タンパー性とテスト容易性を両立する技術
 - 一般端末における真贋判定機器への技術応用
- 設計ツールベンダー
 - 安全性の高い設計技術とそのためのツール
- 設計会社
 - 安全性を付加価値とするチップの製造技術
- システムメーカー
 - 価値や信用を搭載する機器の開発



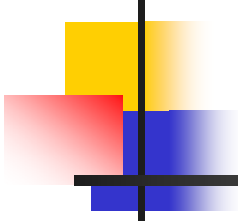
「価値」や「信用」を担えるIT技術

- 新しい半導体集積回路産業の応用分野の共通テーマ
 - 半導体業界の非競争的共通開発テーマの欠如
 - 情報通信やソフトウェアなどと不可分の技術開発
 - 大きな応用分野と経済効果
- 新しい社会の基盤技術
 - 経済システムの根幹
 - 知財立国政策の基礎となる社会システムの構築
- 国家の安全保障との関係
 - 通貨体制や徴税システムの基本
 - 諸外国への技術輸出による国家安全保障の確立



LSIは財布か貨幣か？

- 財布であるなら
 - 偽物でも入っている「価値」が本物なら許せる
 - ブランド品と安物の差はあっても、中身の「価値」とは無関係
- 貨幣であるなら
 - 政府の通貨発行権や徴税権と密接に関係する
 - 財務省印刷局LSI部門が必要？



最後に

- お金は，作るものである．半導体はお金を作る技術になろうとしている．
- 「価値」と「信用」は最も重要なコンテンツであり知財である
- 「価値」や「信用」と社会基盤を守る為の半導体知財の開発
- 本物を特定する技術と偽物を作らせない技術