社会情報基盤の課題と新キャンパス周辺における実証実験

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

出版情報：SLRC プレゼンテーション, 2006-11-09. 九州大学システムLSI研究センター
バージョン：
権利関係：

社会情報基盤の課題と新キャンパス周辺における実証実験

安浦寛人
九州大学システムLSI研究センター
2006.11. 9

九州大学


0
3km
箱崎キャンパス
伊都キャンパス
百道浜サテライト
キャンパス
伊都地区
九州大学
病院地区
九州大学
六本松地区
九州大学
筑紫地区
貝塚RP
貝塚
箱崎RP
箱崎九大前
箱崎駅
新幹線
福岡IC
粕屋RP
伊賀
駅
JR香椎線
柚須駅
JR篠栗線
吉塚駅
県道607号線
原町駅
吉原駅
天神北RP
都市高速
中洲川端
百道RP
福岡ドーム
地下鉄
天神
天神南
博多
博多駅
空港RP
地下鉄
福岡空港
九州自動車道
姪浜
室見川
唐人町
大濠公園
西鉄天神
藤崎
西新
薬院
六本松
JR鹿児島本線
国道3号線
西鉄天神大牟田線
JR筑肥線
波多江
周船寺
九大学研都市
今宿
下山門
周船寺IC
今宿IC
西九州自動車道
大野城RP
南福岡駅
春日原
野多目RP
地下鉄
春日駅
白木原
太宰府IC
橋本
堤RP
(建設中)
都市高速
博多南駅
大野城駅
水城RP

福岡システムＬＳＩ総合開発センター

（九州大学連携型起業家育成施設）

QuickTimeý Ç²
TIFFÅià‰èkÇ»ÇµÅj êLÍ£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÕÏKóvÇ-Ç‰ÅB

SLRC:教員7名、職員2名、学生20名配置

CLUSSとシリコンシーベルトの推進の中核

知的クラスタ創成事業とFLEETS
システムLSIカレッジ
九州大学システムLSI研究センター
設計・試験・検証ラボ
インキュベーション施設

・規模　鉄骨コンクリート造７階建て
- 敷地面積　約３，２００㎡
- 延床面積　約７，７００㎡
- 事　業　費　３０億円

・所　在　地　福岡市早良区百道浜３丁目
・開設　平成１６年１１月4日

Silicon Sea Belt福岡プロジェクト

世界最大の市場
世界最大の半導体の生産力
世界最大の技術者の供給力

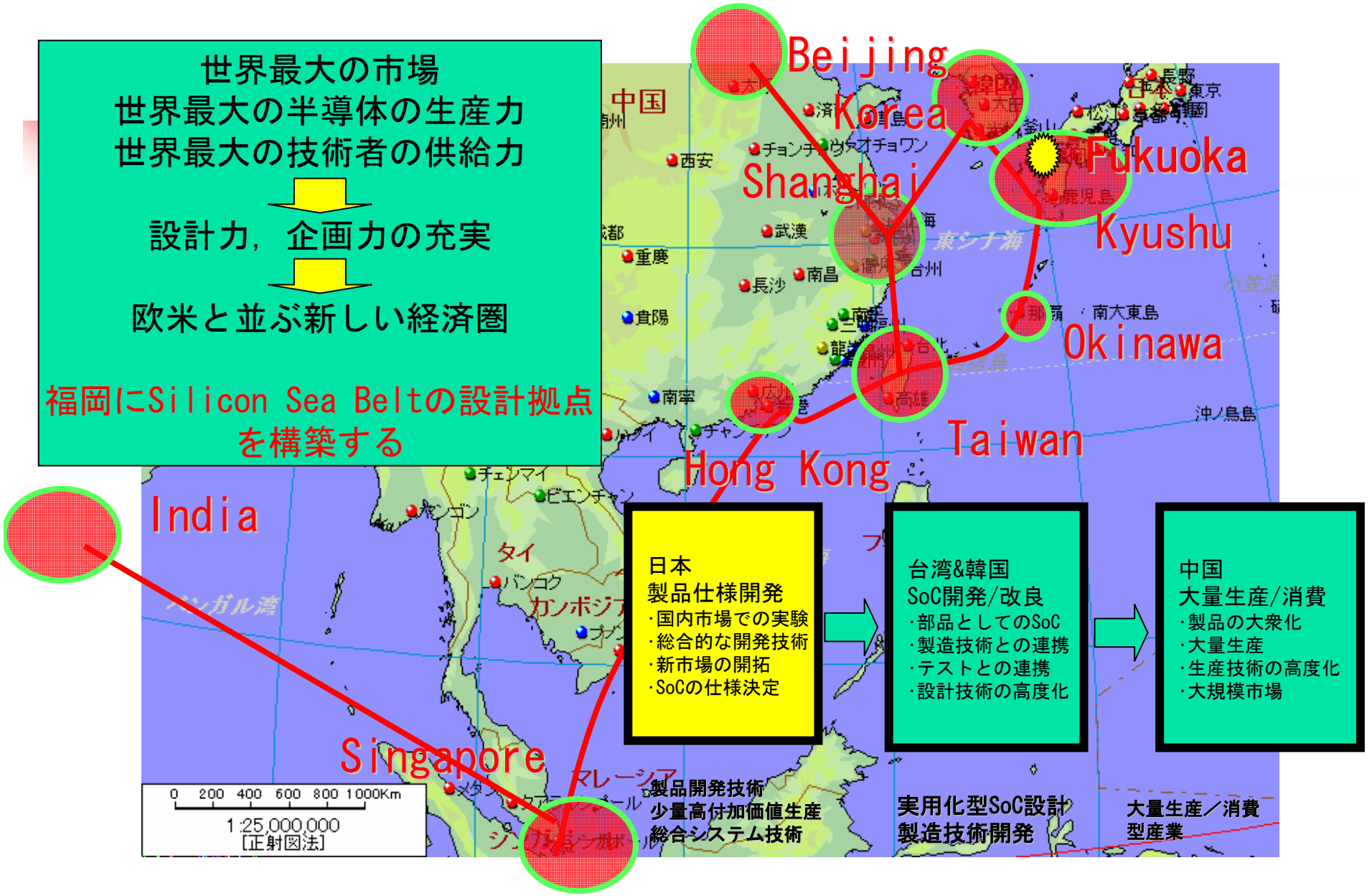
↓

設計力，企画力の充実

↓

欧米と並ぶ新しい経済圏

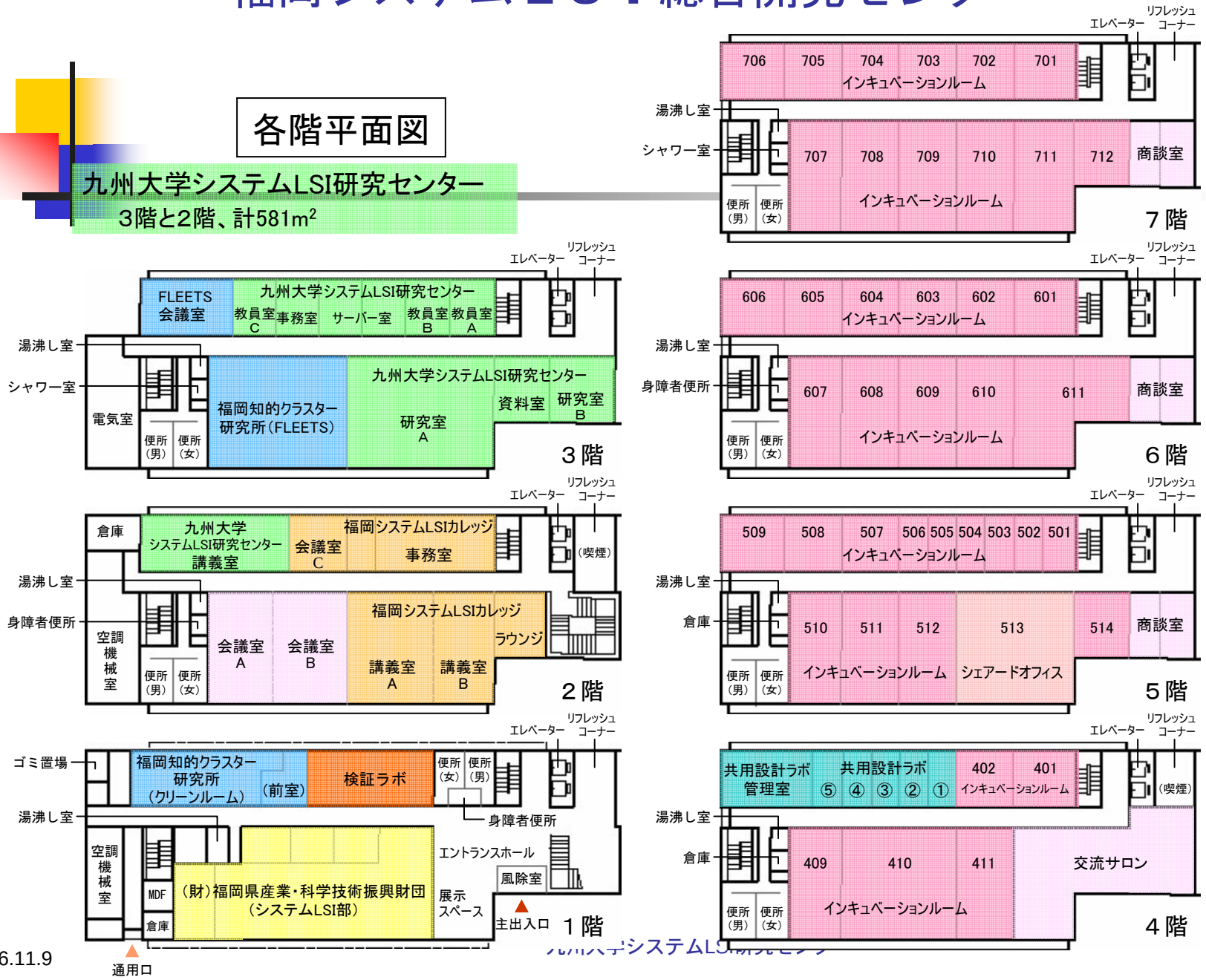
福岡にSilicon Sea Beltの設計拠点を構築する



福岡システムＬＳＩ総合開発センター

各階平面図

九州大学システムLSI研究センター
3階と2階、計581m²



システムLSI研究センターの役割

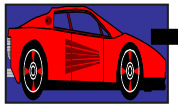
九州大学システムLSI
研究センターの対象範囲

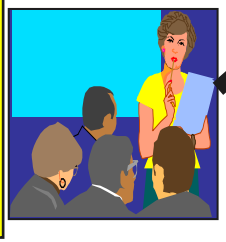
東京大学大規模集積
システム設計教育センター
(VDEC)の対象範囲

社会の種々の応用分野からの
要求に対し，システムLSIを
設計する先端技術の研究.
これからの中心的研究課題.

集積回路の仕様から集積回路を
既存の技術で設計し，安価に試作
する仕組み．全国の大学の設計教
育の充実と高度化を支援.

家電製品
ゲーム
情報機器
自動車
飛行機
鉄道
電子マネー
電子投票
医療機器
自動販売機
ロボット
通信システム
ライフライン





社会からの要求

システムLSIの設計

ソフトウェア

集積回路
の設計

ソフトウェア＋集積回路

九州工業大学の対象範囲
設計から製造までの総合的知識
を持った技術者の教育

集積回路の
製造

実際の
集積回路

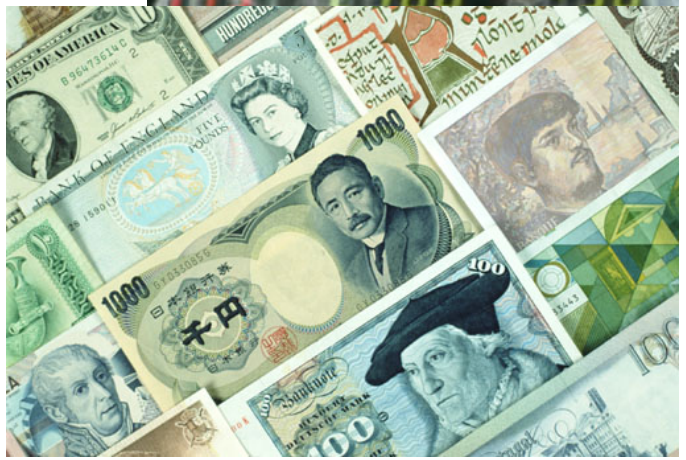
東北大学・広島大学の対象範囲
先端製造技術の研究

社会情報基盤の課題と新キャンパス周辺における実証実験

1. 情報技術と社会の変化
2. 社会情報基盤に求められるもの
3. 「価値」と「信用」
4. MIIDとe-Worldプロジェクト
5. Dependableな情報技術を目指して

社会システムと情報技術

- 20世紀後半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。
  - 社会情報基盤(Social Information Infrastructure)
  - ユビキタス社会、 e-Japan、u-Japan

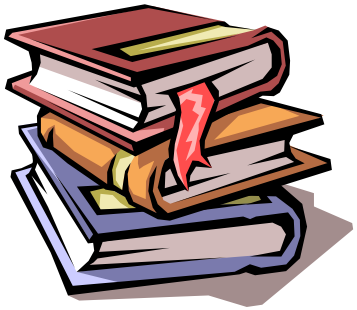


過去50年で何が変わったのか？

- 社会活動における物理的制約の削減
  - 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.
  - システムの安定性の危機
- Dependableな社会情報基盤の確立
  - 安心して生命、財産、プライバシーを預けられる仕組み
- **情報技術を前提とした社会システムの再構築**
  - **エレクトロニクスの故障率は10^{-9}、自動車は10^{-12}**
  - **情報化社会で「価値」や「信用」をどのように取り扱うか？**
  - **情報技術は「価値」や「信用」の媒体たりえるか？**

システムの不安定性の原因

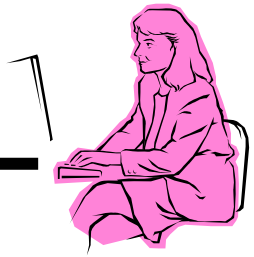
書く（100文字/分）



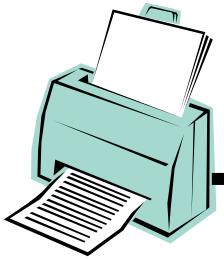
読む（1000文字/分）

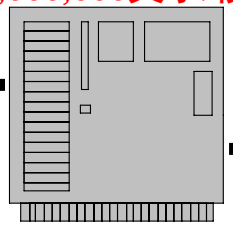
話す（500文字/分）

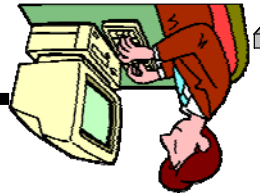
ファクシミリ（2000文字/分）

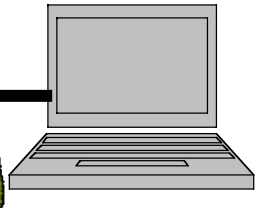


インターネット
（1,000,000文字/秒）

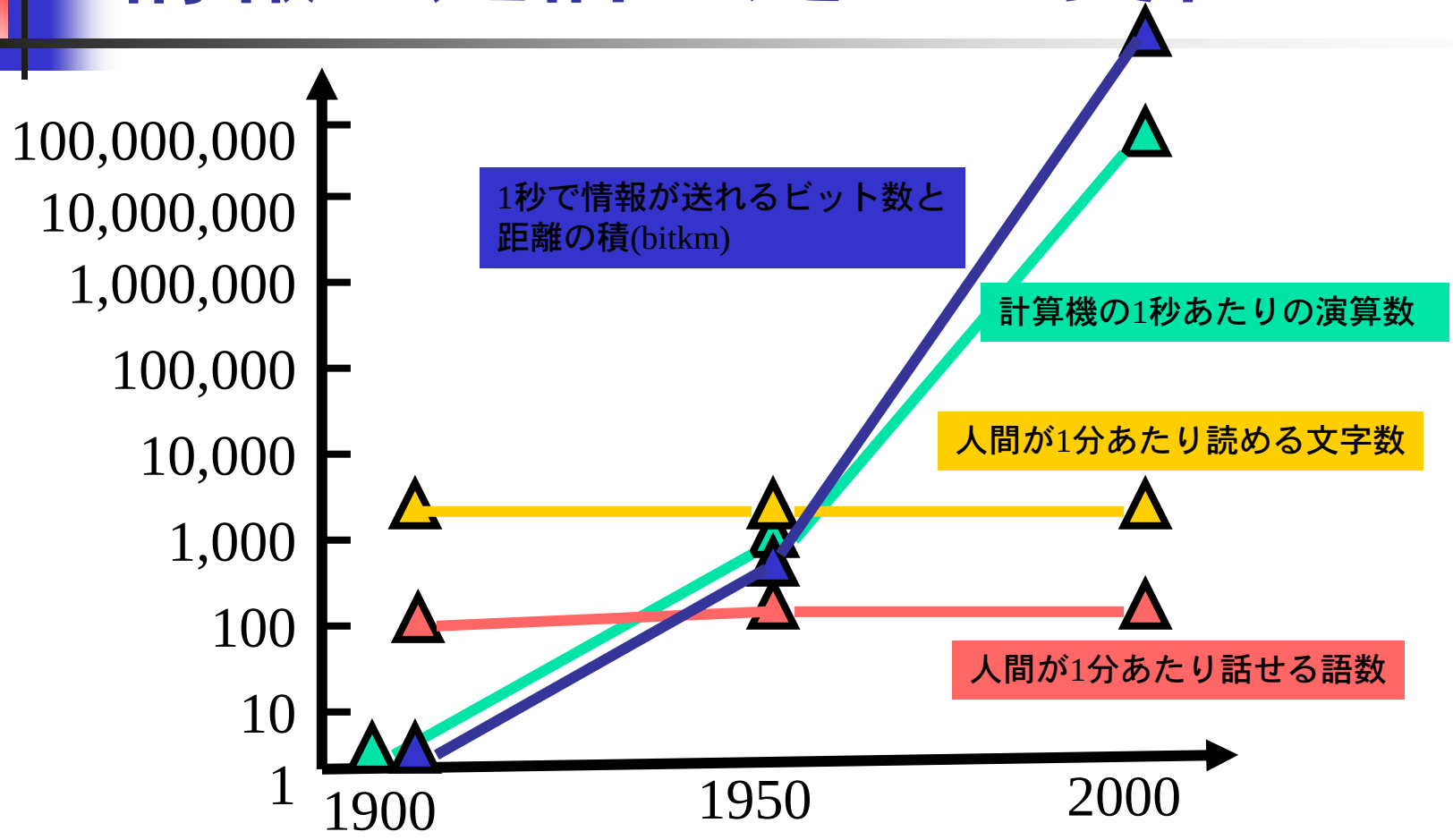




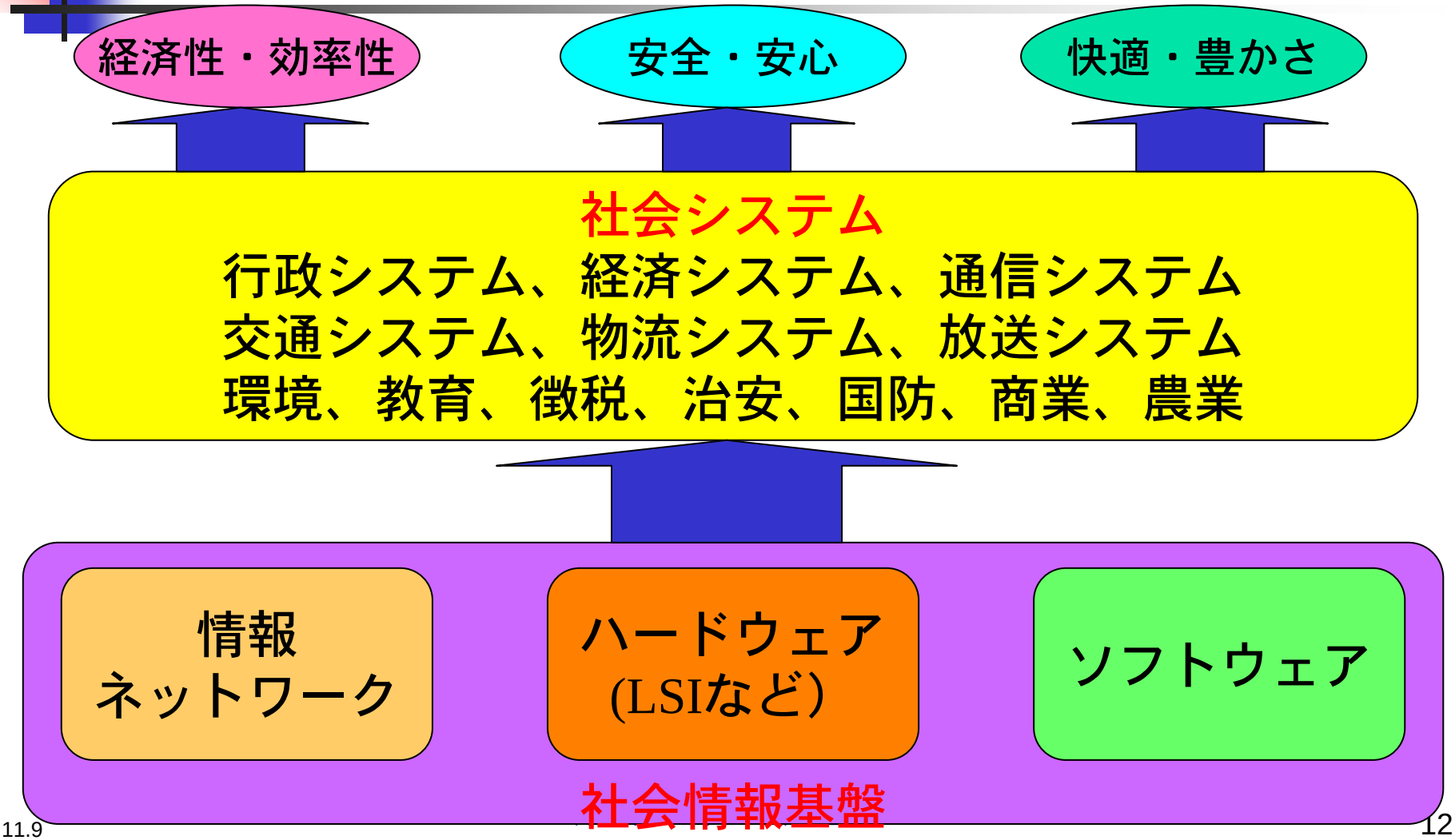




情報の通信・処理の変化


100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
1900
1950
2000
1秒で情報が送れるビット数と
距離の積(bitkm)
計算機の1秒あたりの演算数
人間が1分あたり読める文字数
人間が1分あたり話せる語数

社会情報基盤の構築


経済性・効率性
安全・安心
快適・豊かさ
社会システム
行政システム、経済システム、通信システム
交通システム、物流システム、放送システム
環境、教育、徴税、治安、国防、商業、農業
情報
ネットワーク
ハードウェア
(LSIなど)
ソフトウェア
社会情報基盤

社会情報基盤の課題と新キャンパス周辺における実証実験

1. 情報技術と社会の変化
2. 社会情報基盤に求められるもの
3. 「価値」と「信用」
4. MIIDとe-Worldプロジェクト
5. Dependableな情報技術を目指して

何が問題か？

- 情報化による環境と技術の変化
  - 産業構造の変化
    - サービス中心の産業構造への転換
    - 価値や信用の移動速度の劇的変化
  - システムの複雑化
    - 世界的なネットワーク接続（地理的拡大）
    - 異なる分野のシステムとの接続（異分野の統合）
    - 新旧の各種システムとの接続（時間軸での統合）
    - 微細化・大規模化による揺らぎや不確実性の増大
  - 予想外・想定外の事象の発生
    - Specification-basedの技術からPolicy-basedの技術への転換
    - 即時的な応急回復機能への要求（Instant Recovery)
    - 保険や責任体系の変化
    - 制度、法律、規則の整備や改変との連携

仕様が作れないシステム

- これまでのシステム設計は、「仕様」によって規定されていた（社会とシステムのインタフェース）
- 仕様が作れなくなった原因
  - システム境界の不明確化
    - ネットワークによる接続
    - 出荷後のソフトウェアのダウンロード
    - 時々刻々変化する外部環境
  - 技術の変化と拡大の速さ
    - 検証されない技術の更新
    - 大局が見えにくい局所的技術競争
  - 技術や規格のブラックボックス化
- 仕様からポリシーへ
  - 環境の変化への柔軟かつ即時的対応
  - 想定範囲の拡大
  - 責任の明確化（誰の責任か？運用者、設計者、許認可権限者）
  - 保険システムの変革（動的なリスク管理）

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
- 技術の変化に対応した新しいシステムへのスムーズな移行

何ができるかより
どうあるべきかを考えることが重要

社会情報基盤の課題と新キャンパス周辺における実証実験

1. 情報技術と社会の変化
2. 社会情報基盤に求められるもの
3. 「価値」と「信用」
4. MIIDとe-Worldプロジェクト
5. Dependableな情報技術を目指して

貨幣とは？

- 貨幣の役割
  - 決済手段
    - 売買，税や賃金などの支払い
  - 価値の貯蔵手段
    - 時間を越えた財産の貯蔵
  - 価値尺度（貨幣単位）
    - 物や労働の価値の評価尺度

- 決済の形態
  - 現金貨幣決済システム(150兆円)
    - 法貨規定された銀行券
    - 支払い完了性
    - 匿名性
    - 分散・オフライン・小口
  - 信用貨幣取引システム(290兆円)
    - 債務貨幣（債務の通貨化）
    - 預金通貨
    - 大きな金額の取引の手段
  - 電子マネー（1千億円）
- 発行者への信用をベースとした集団幻想

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

Edy Smart Shopping Style

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？

社会的な問題

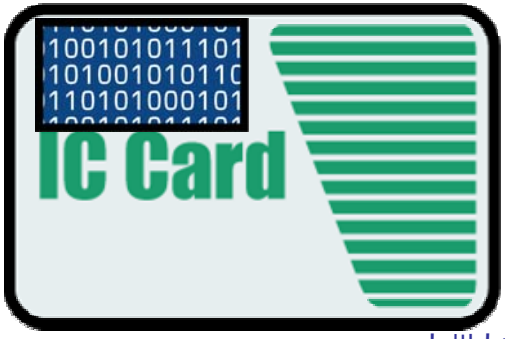
- 電子マネー発行機関の多様化
  - 中央銀行券以外の通貨
    - プライベートマネー（通貨発行権、徴税など）
      - （航空会社のマイレージ，クレジット会社のポイントなど）
    - 外国通貨の併用
    - 金融経済政策への影響
  - 徴税の問題
    - 電子取引への課税方法
    - プライベートマネーへの課税方法と法体系
    - 有力企業が賃金の一部を独自マネーで発行したら？
- 新しい社会体制と技術体系
  - 価値や信用を取り扱う情報技術は十分か？
  - 個人の財産管理（電子マネー内のデータは壊れないか？）
  - 新しい価値の流通システムをどのように構築する？
  - 貨幣の取引流通速度増加の問題（貨幣の数量方程式M×Ｖ＝P×Ｔ）
- 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。

現金貨幣の実現に必要な機能

- 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
  - 安全な媒体（デバイス）、システム、組織の構成
  - 信用性と教育

電子マネーは現金貨幣か？

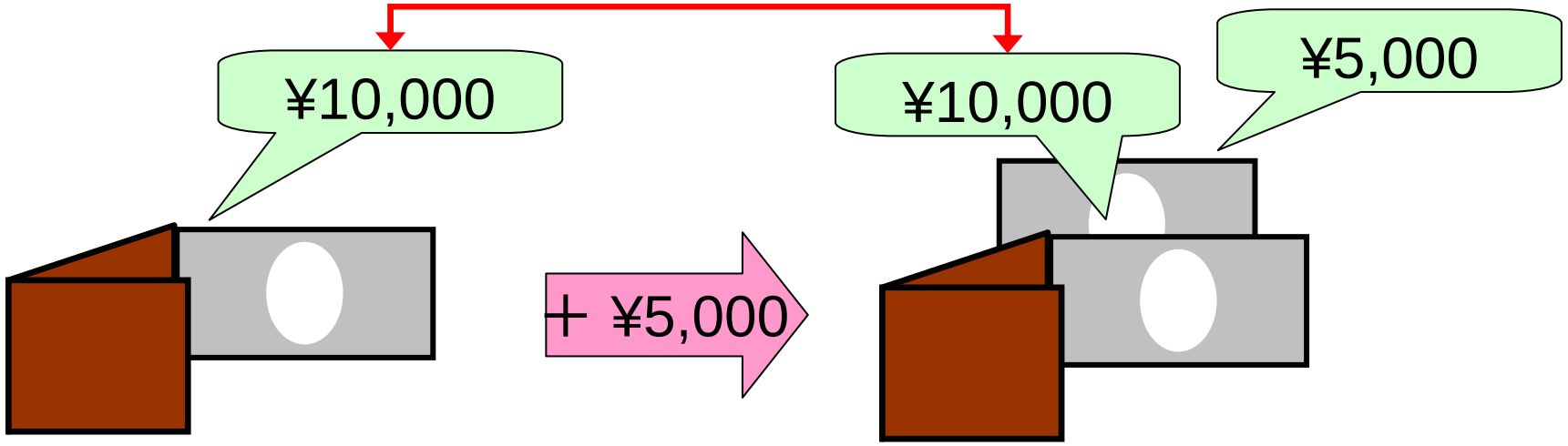
- EdyやSuicaは現金通貨の仕様を満たすか？
  - ディジタルデータを媒体として用いる
  - 保持者はICカードを用いる
  - 価値トークン
    - ローカル内で、残高金額として保持される
    - 移動は電子的な通信により行われる
    - 発行者間とユーザ間のみで移動が行われる



媒体集合の問題(1/3)

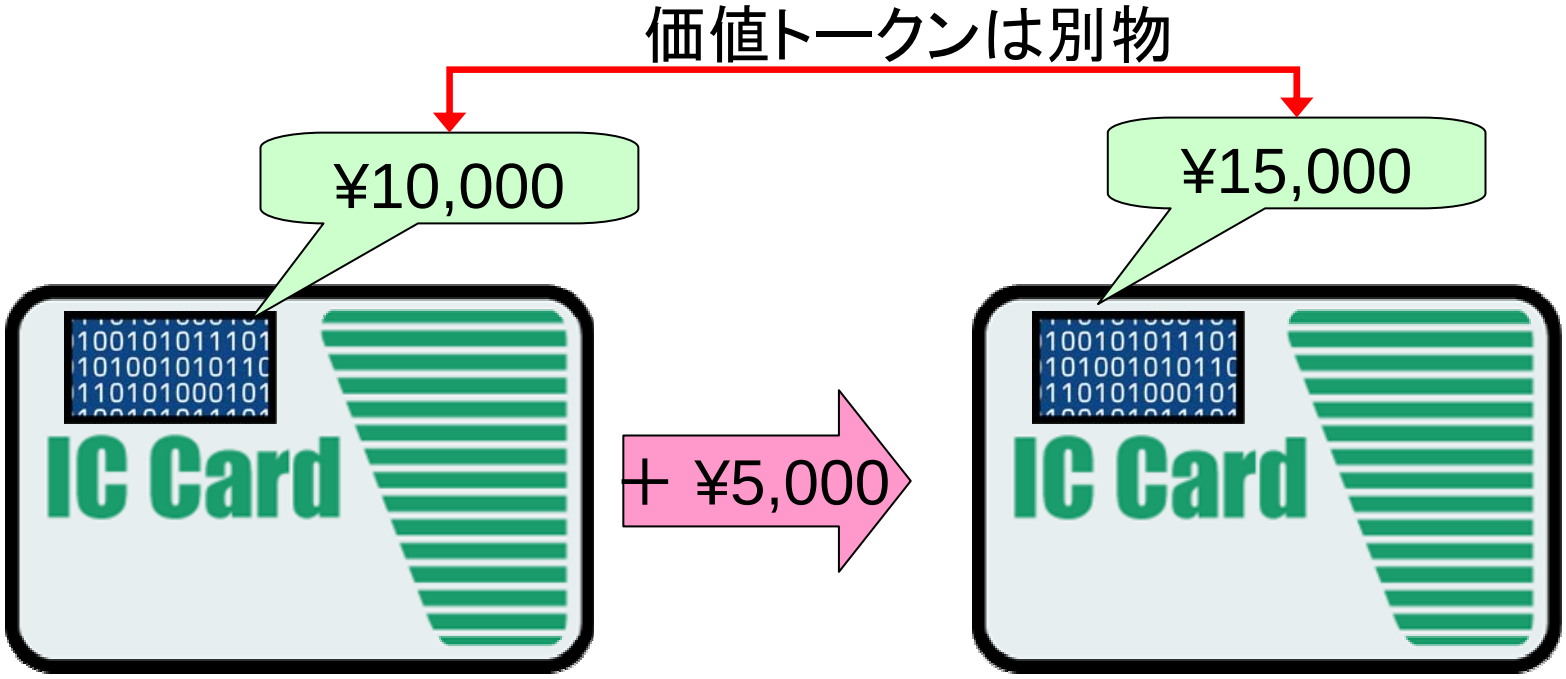
- 現金における媒体は、物理的制約から分割できない最小要素からなる

価値トークンは同一



媒体集合の問題(2/3)

- 電子マネーは、残高情報の上書き更新により媒体を管理



媒体集合の問題(3/3)

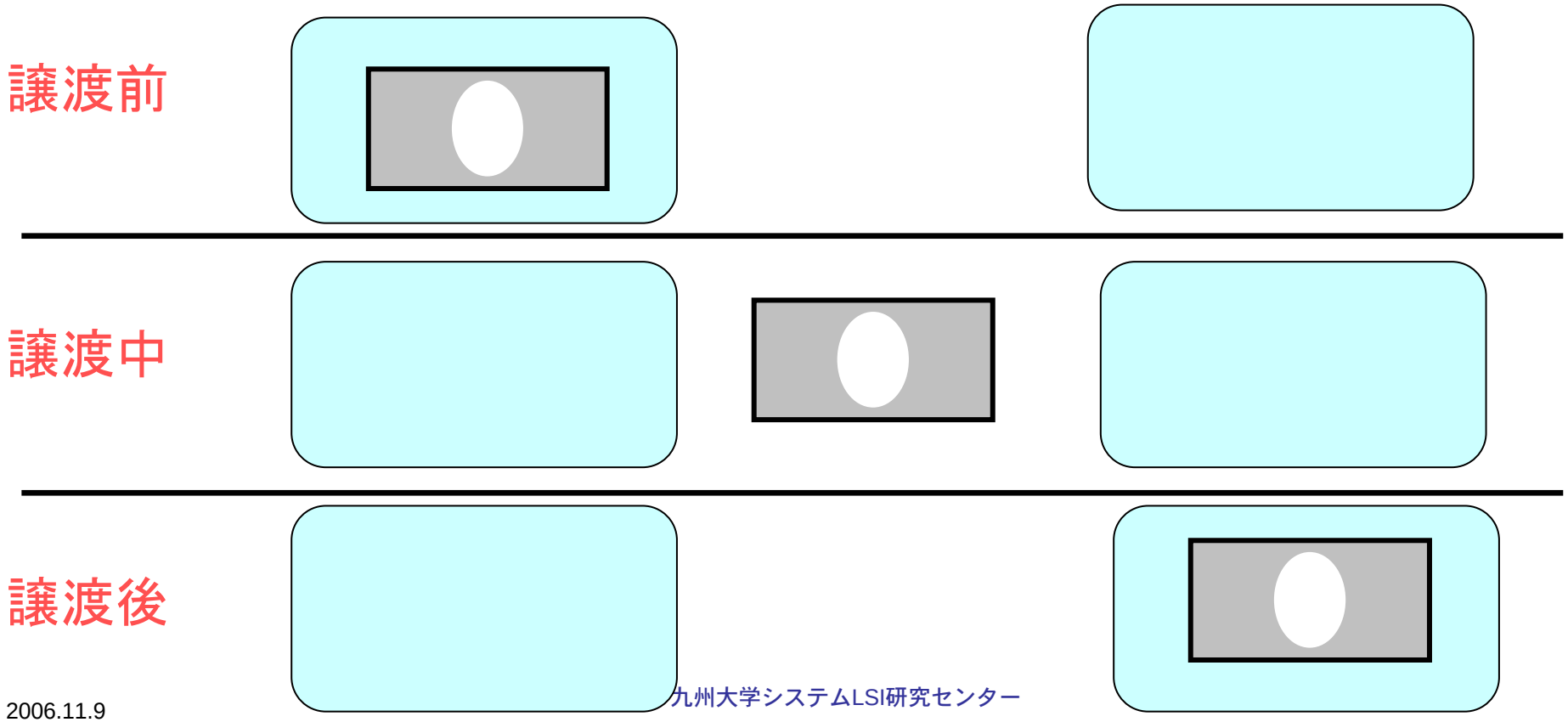
- 価値トークンの集合と媒体の集合の関係をどうやって保つ？
  - 偽造されたデータが混入した場合、すべて無効になる？
  - 関係があいまいであるがゆえに匿名性を確保できる?

譲渡の問題

- 電子マネーにおける価値の譲渡
  - ICカード内の現在残高を消去
  - ICカードに更新後の残高を追記
- 現金通貨モデルにおける価値の回収と発行に相当する！
- 価値の回収・発行は、今までは信頼できる第三者(中央銀行)のみが行っていた
- ICカードは財布ではない!

価値トークン総量保存則の問題

- 現金は物質の性質より、譲渡前・譲渡中・譲渡後においても価値トークンの総量は保存される



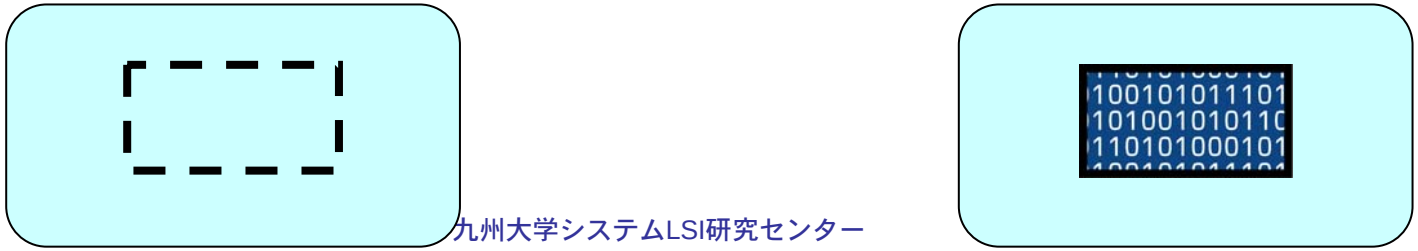
価値トークン総量保存則の問題

- 電子マネーでは価値トークンの総量が常に保存されるわけではない

譲渡前

譲渡中

譲渡後



価値トークン総量保存則の問題

- 通信途絶等が起こったら総量は変化しないのか？
  - ➔ Fair Exchangeの問題
- 一般の人に理解できるか？
  - 一般の人に信頼されることが通貨の絶対条件
- 子供達（次世代の市民）はこの問題を知っている(ポケモン交換)

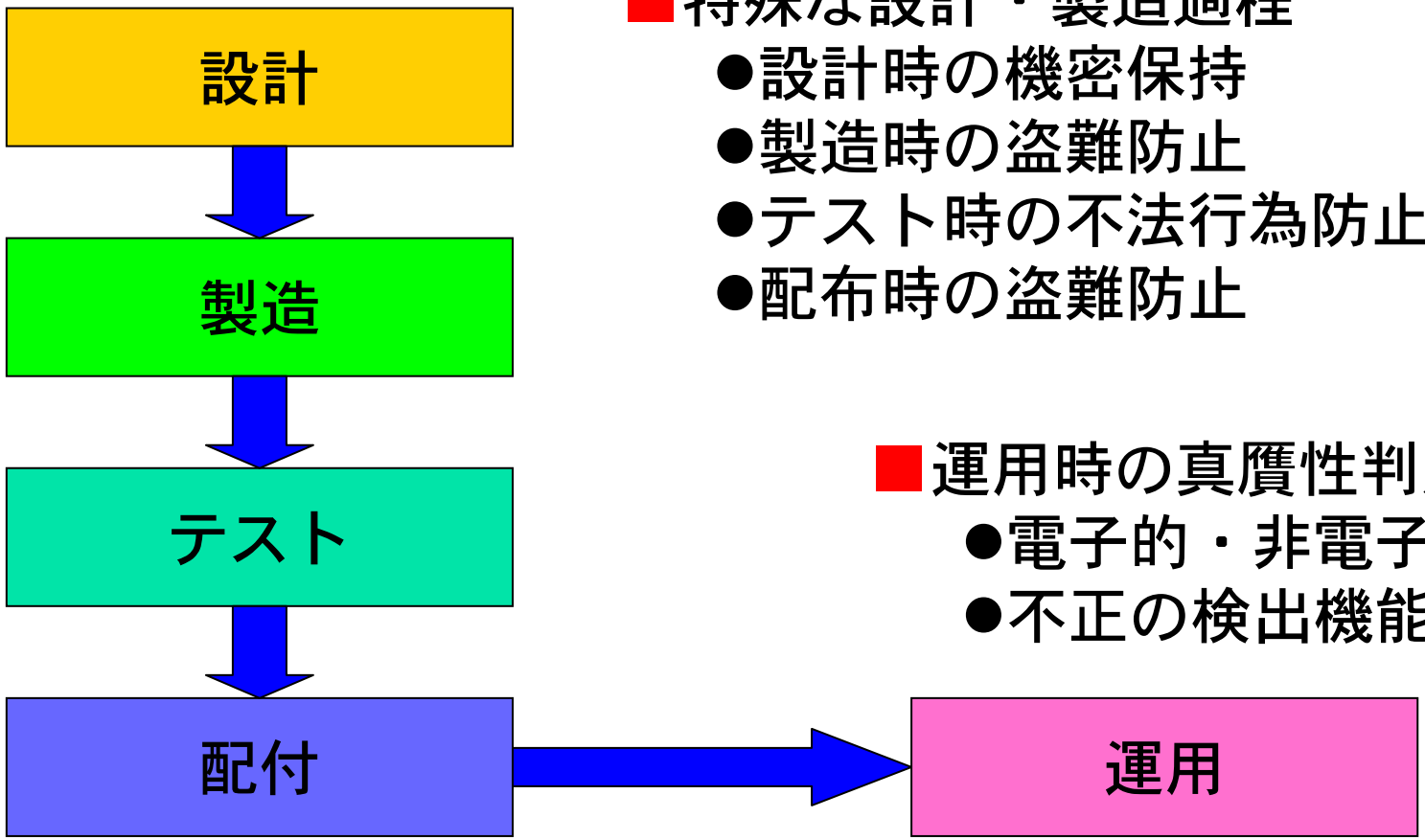
ICカードは財布か貨幣か？

- 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
  - 偽物は許されない
  - 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？
  - 暗号だけで済む話ではない

技術的課題

特殊性の実現
材料
加工方法
機能・性能

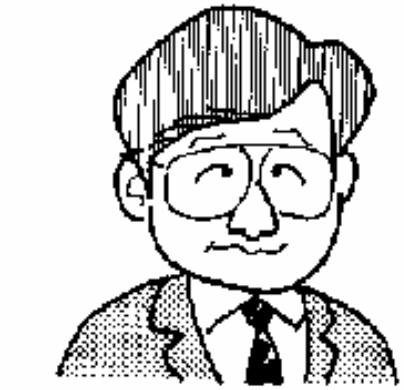
■特殊な設計・製造過程
- ●設計時の機密保持
- ●製造時の盗難防止
- ●テスト時の不法行為防止
- ●配布時の盗難防止



■運用時の真贋性判定
- ●電子的・非電子的
- ●不正の検出機能

信用の基盤（認証）

- 電子マネー、電子政府などと騒がれているが。。。
- ネットワークの先の相手は信用できる？
- 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？




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）
- 原理がわからないシステム(PKIなど)
- 個人情報の重さ（個人情報保護法）

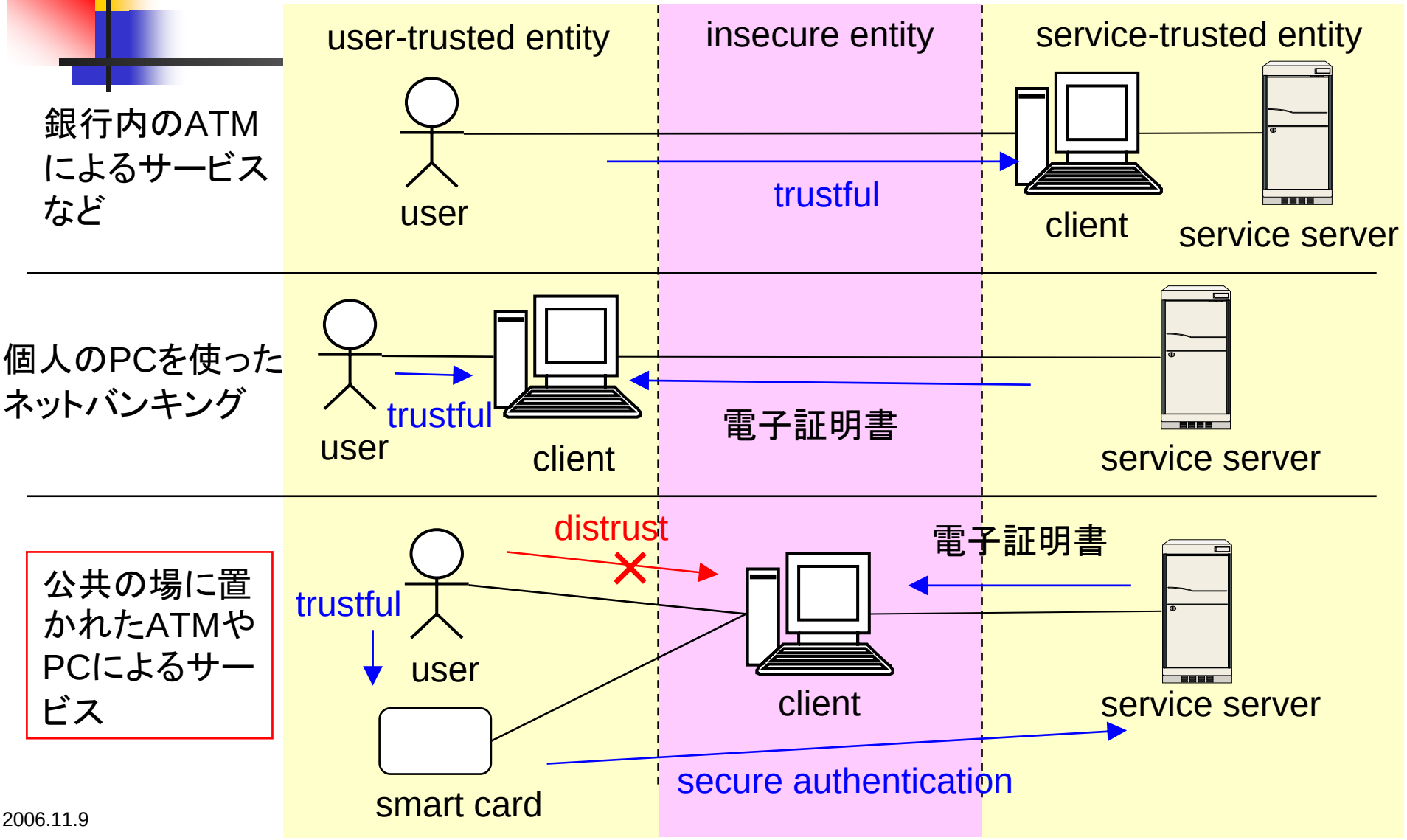
QuickTimeý Ç²
TIFFÅiâÌêkÇ»ÇµÅj êLÍÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÆsÉNÉ ÉÉÇ¾â©ÇÉÇžÇ½Ç…ÇÒÍKóvÇ-ÇlÅ

QuickTimeý Ç²
TIFFÅiâÌêkÇ»ÇµÅj êLÍÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÆsÉNÉ ÉÉÇ¾â©ÇÉÇžÇ½Ç…ÇÒÍKóvÇ-ÇlÅB

相互認証の必要性

- 従来の認証は組織や機関が個人を認証する一方向認証
- 個人が組織や機関を認証する仕組みが必要（相方向認証）
  - ATMなどの普及
  - ネットを通じた取引
  - Phishing
- 認証結果の表示方法
  - 携帯電話などの利用
  - ICカードへの表示機能追加

認証の危険の分類


user-trusted entity
insecure entity
service-trusted entity
銀行内のATMによるサービスなど
user
trustful
client
service server
個人のPCを使ったネットバンキング
user
trustful
client
電子証明書
service server
公共の場に置かれたATMやPCによるサービス
distrust
電子証明書
trustful
user
client
service server
smart card
secure authentication

現在の認証基盤の問題点

利用者

- サービス毎に異なるIDデバイス(カードなど)が必要となる
- サービスごとに認証の方法が異なり、対応が煩雑である
- 紛失した時に各デバイスの発行元へ連絡する必要がある
- 利用するサービスの数だけ個人情報を公開する必要がある
- 利用履歴などのトレースが懸念される
- 高いセキュリティを謳うサービスは原理が複雑で理解しづらい

サービス提供者

- 発行者の役割や個人情報の管理コストがかかる
- 他のサービスの連携を取るときのコストやリスクが大きい
- 事故が他のサービスに波及するリスクへの対応が必要

発行者

- サービス毎にセキュリティ管理の重みを変えることが困難
- 複雑で柔軟な権利・権限管理が難しい
- 各種の事故が大きな情報漏洩に波及する可能性がある
- 複数のサービスの柔軟で低コスト・低リスクでの融合が難しい

社会情報基盤の課題と新キャンパス周辺における実証実験

1. 情報技術と社会の変化
2. 社会情報基盤に求められるもの
3. 「価値」と「信用」
4. MIIDとe-Worldプロジェクト
5. Dependableな情報技術を目指して

九州大学全学共通ICカードプロジェクト
QUPID：(Q-shu Univ. Personal ID)

- 安全で安心な社会基盤システムを構築するための情報インフラを新キャンパスにおいて構築し、実運用して、技術のみならず社会科学的な視点も考慮した未来の社会基盤システムの方向性についての提言を行う。
- 新しい情報インフラを基盤とした、効率的で機能的かつ柔軟な大学運営体制を確立する。

QuickTimeÿ Ç³
TIFFÁILZWÁ ëLIëÉvÉçÉOÉãÉÁ
Ç™ÇsÇÅÉsÉNÉ ÉÉÇ¼âÇÉÇâÇ½Ç…ÇÖIKóvÇ-ÇÍÅB

九州大学システムLSI研究センター

提案するMIID(Media Independent ID) 管理システム

1 メディアに依存しない

TypeBカード、Felicaカード、携帯電話などメディアに依存しないID体系の実現。メディアとID管理システムの分離。

2 サービス毎に異なるID

サービス毎に異なるIDを利用し、複雑な権利権限管理に対応。また、情報漏洩などの被害を最小限に。

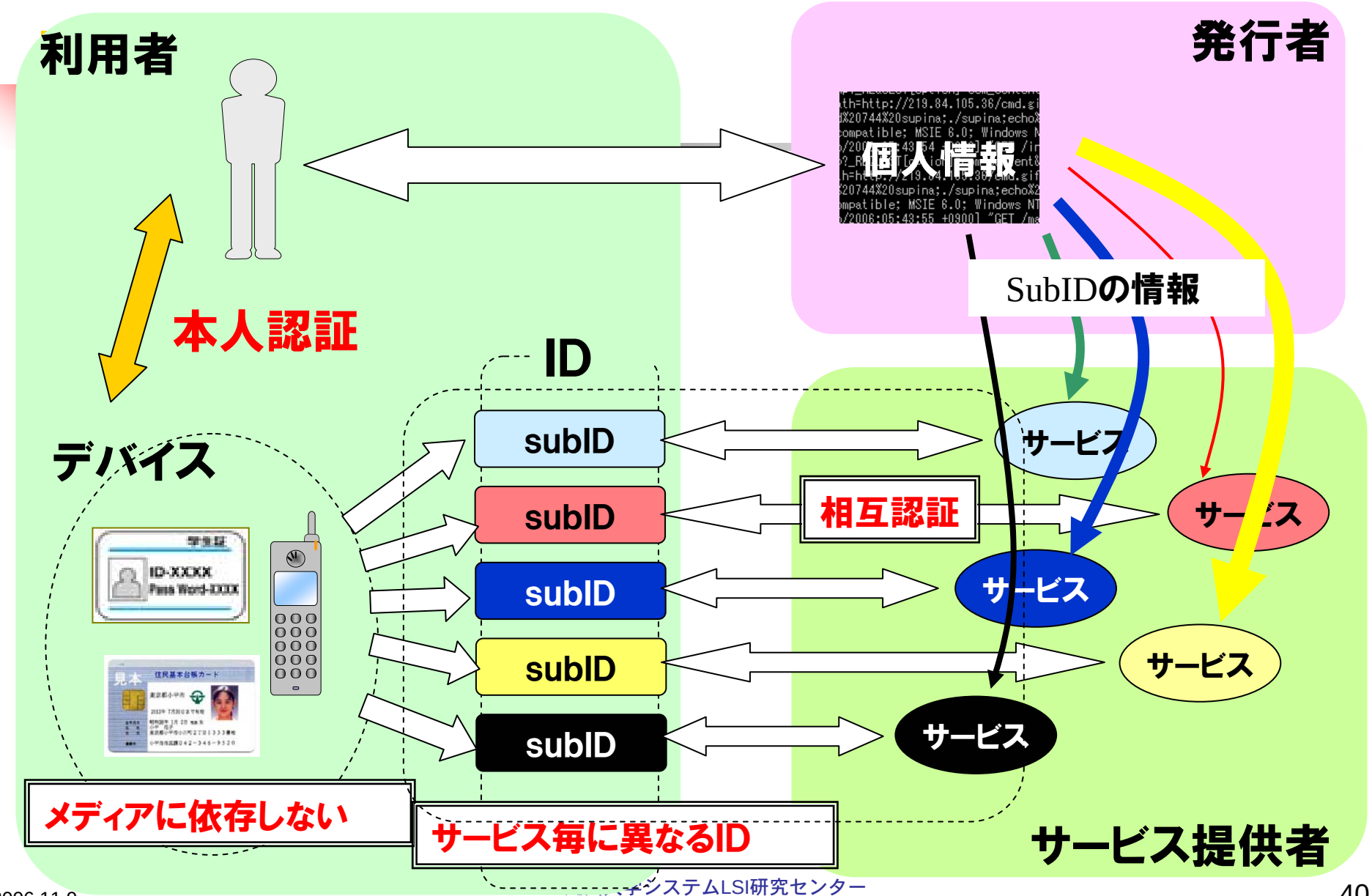
3 相互認証などの柔軟な認証方式

相互認証や複雑な認証要求に対応する機能を搭載

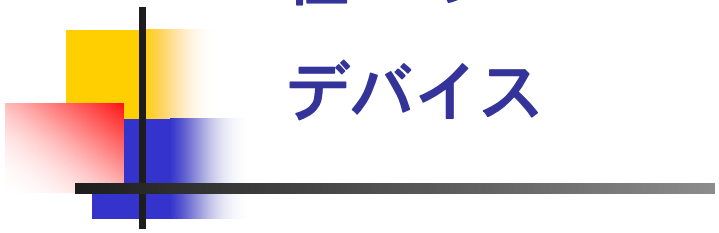
4 Unlinkabilityとリスク対応

サービス提供者が個人情報を持つ必要がなく、情報を持つリスクを回避。個人情報の分散管理が可能。

MIIDシステム概略図



種々のMIIDデバイス

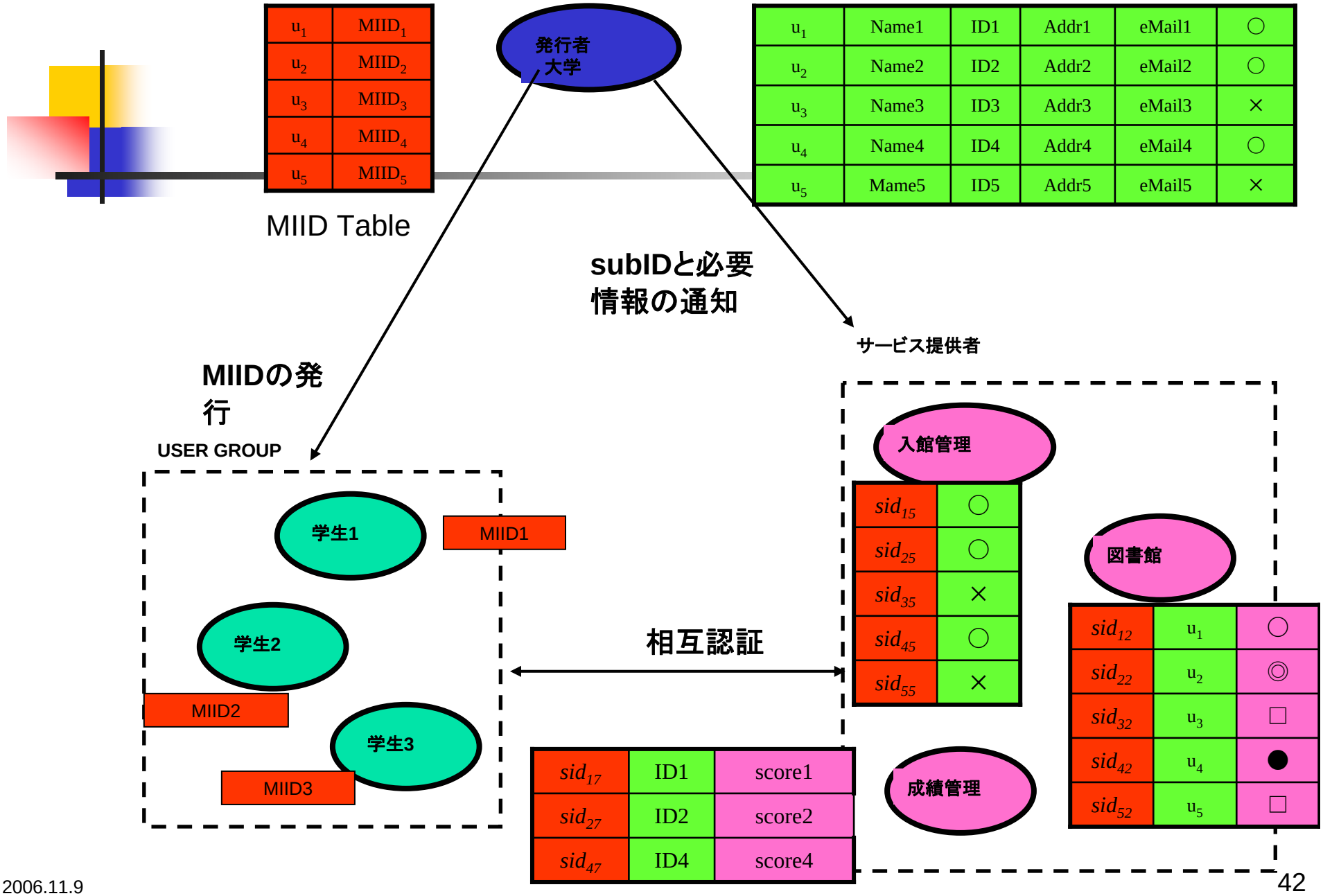


QuickTimeý Ç²
TIFFÃiLZWÃj êLíÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÉÇžÇ½Ç…ÇÖÍKóvÇ-ÇíÃB

QuickTimeý Ç²
TIFFÃiLZWÃj êLíÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÉÇžÇ½Ç…ÇÖÍKóvÇ-ÇíÃB

ICカード
携帯電話
USBデバイス

個人に関する情報の分散管理

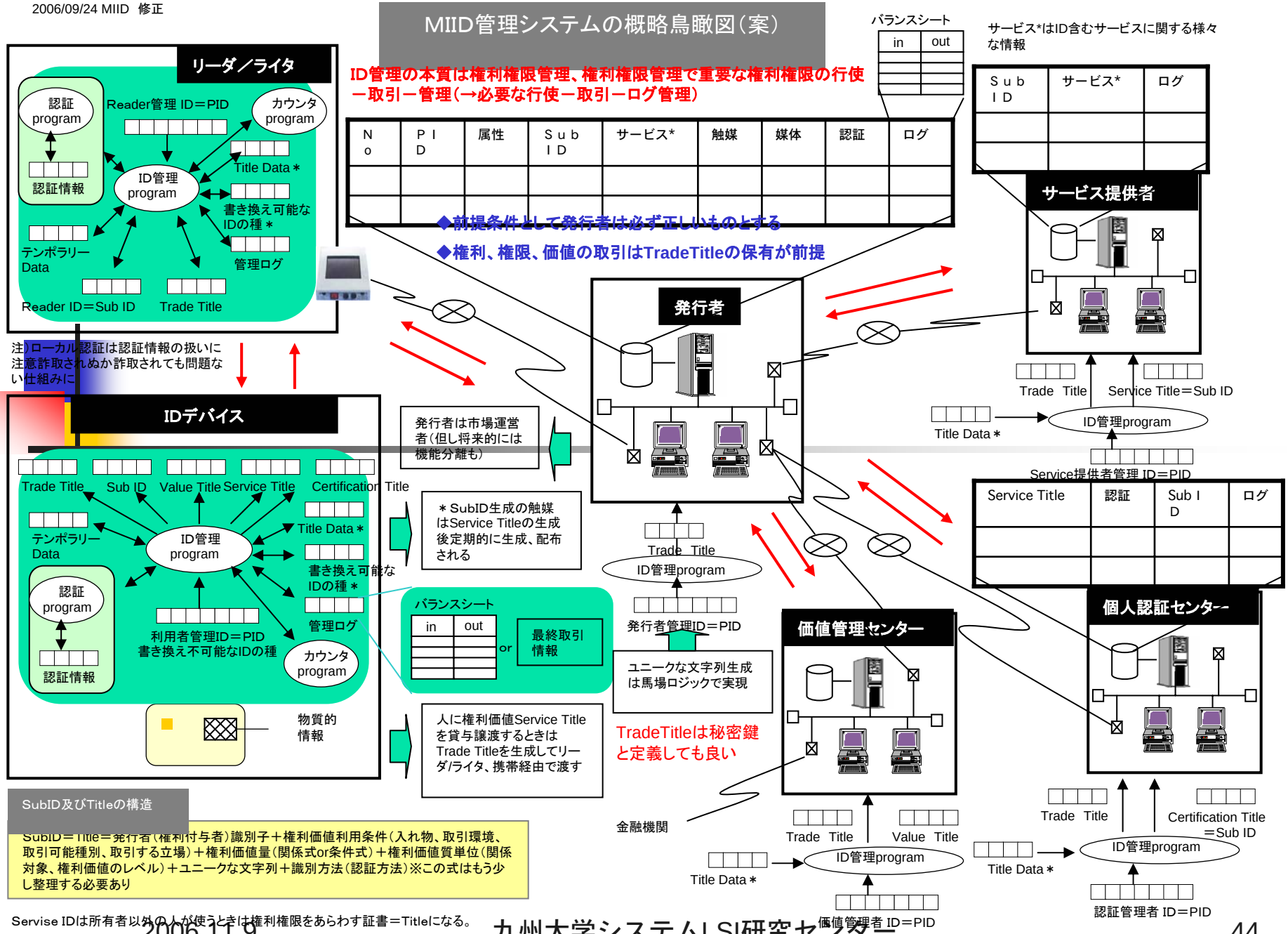


MIIDの利用と展開

- 顧客、職員、学生、住民などへの多様なサービスと情報管理
  - 個人情報の分散管理とプライバシー保護
  - 複数のサービスへの安全・安心なインフラ
  - 権利権限の柔軟な付与・譲与と制限
- 施設管理
  - 入退室や利用の柔軟な管理
  - 一時的な鍵の貸与（Portable Software Key）
- 通信販売
  - 生産者と消費者を結ぶ安全・安心な情報路
- アンケート収集
  - 回答者のプライバシー保護と調査の粒度の制御
- 新しいサービス事業
  - 交通カード、地域カード、地域マネーなどへの発展

2006/09/24 MIID 修正

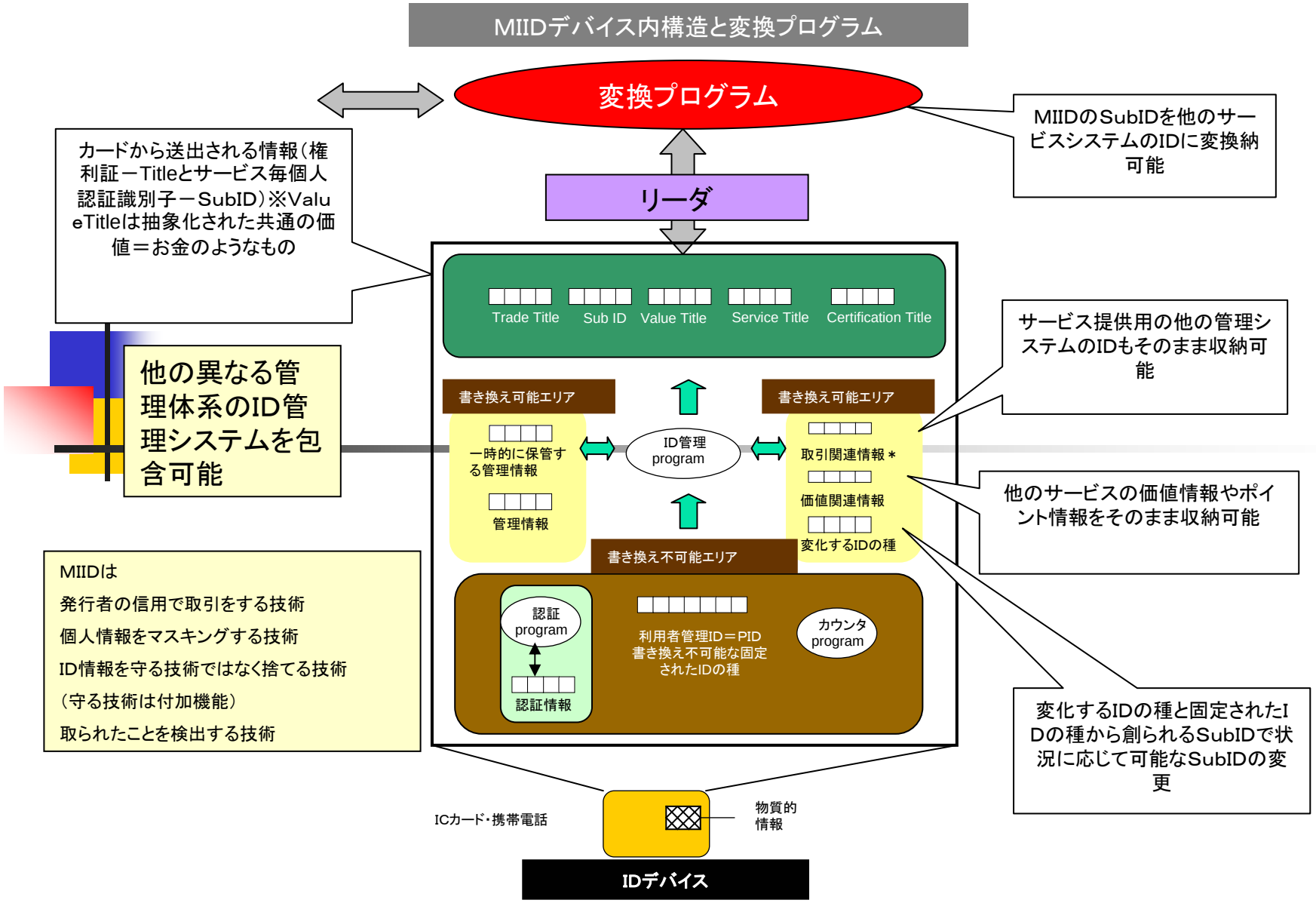
MIID管理システムの概略鳥瞰図（案）



SubID及びTitleの構造

SubID＝Title＝発行者（権利付与者）識別子＋権利価値利用条件（入れ物、取引環境、取引可能種別、取引する立場）＋権利価値量（関係式or条件式）＋権利価値質単位（関係対象、権利価値のレベル）＋ユニークな文字列＋識別方法（認証方法）※この式はもう少し整理する必要あり

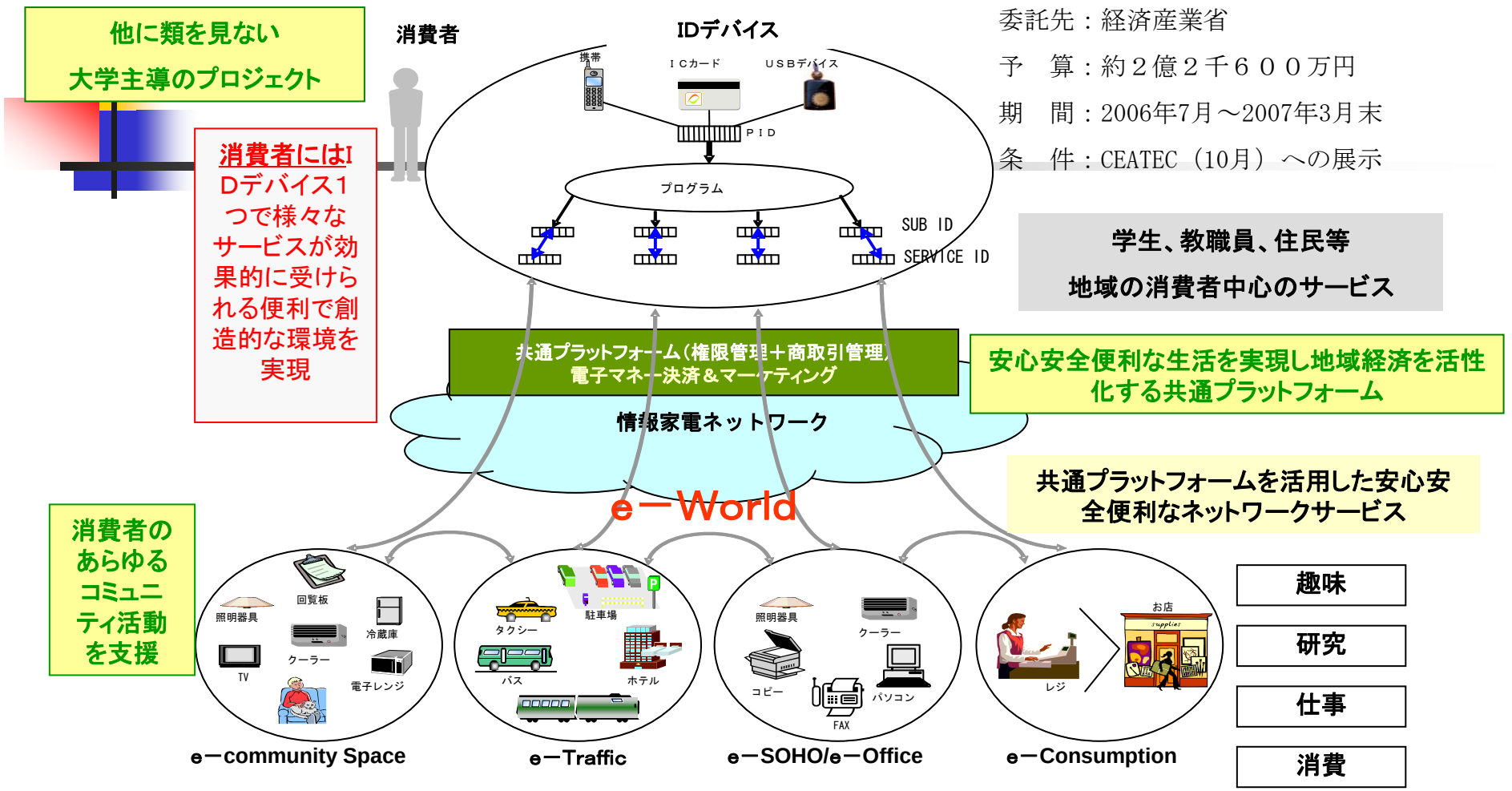
Servise IDは所有者以外の人が使うときは権利権限をあらわす証書＝Titleになる。


MIIDデバイス内構造と変換プログラム
変換プログラム
リーダ
カードから送出される情報（権利証－Titleとサービス毎個人認証識別子－SubID）※ValueTitleは抽象化された共通の価値＝お金のようなもの
MIIDのSubIDを他のサービスシステムのIDに変換納可能
Trade Title
Sub ID
Value Title
Service Title
Certification Title
他の異なる管理体系のID管理システムを包含可能
書き換え可能エリア
書き換え可能エリア
一時的に保管する管理情報
管理情報
ID管理program
取引関連情報＊
価値関連情報
変化するIDの種
サービス提供用の他の管理システムのIDもそのまま収納可能
他のサービスの価値情報やポイント情報をそのまま収納可能
書き換え不可能エリア
認証program
認証情報
利用者管理ID＝PID
書き換え不可能な固定されたIDの種
カウンタprogram
MIIDは
発行者の信用で取引をする技術
個人情報をマスキングする技術
ID情報を守る技術ではなく捨てる技術
（守る技術は付加機能）
取られたことを検出する技術
変化するIDの種と固定されたIDの種から創られるSubIDで状況に応じて可能なSubIDの変更
ICカード・携帯電話
物質的情報
IDデバイス

MIIDを利用した先行社会実験「e－World」プロジェクトの概要

他に類を見ない
大学主導のプロジェクト

委託先：経済産業省
予　算：約２億２千６００万円
期　間：2006年7月～2007年3月末
条　件：CEATEC（10月）への展示



サービス事業者には

既存サービスの高付加価値化と新しいサービス創出のチャンスを提供

九州大学では平行して学内で全学共通ICカード導入推進委員会による先進のICカードシステム導入を推進中


大学生協、2市3町、
イオン、ベスト電器
紀伊国屋、福岡銀行
クレジット会社5社
伊都キャンパス
箱崎キャンパス
百道浜サテライト
キャンパス
昭和バス
JR九州
福岡市営地下鉄
0
3km
N
貝塚RP
貝塚
箱崎RP
箱崎九大前
箱崎駅
新幹線
福岡IC
粕屋RP
伊賀
駅
JR香椎線
九州大学
病院地区
吉塚駅
柚須駅
JR篠栗線
吉原駅
県道607号線
原町駅
天神北RP
都市高速
中洲川端
百道RP
福岡ドーム
地下鉄
天神
天神南
博多
博多駅
空港RP
地下鉄
福岡空港
九州自動車道
姪浜
室見川
唐人町
大濠公園
西鉄天神
西新
薬院
六本松
九州大学
六本松地区
JR鹿児島本線
国道3号線
西鉄天神大牟田線
今宿
下山門
周船寺IC
今宿IC
西九州自動車道
橋本
地下鉄
野多目RP
大野城RP
南福岡駅
春日原
春日駅
白木原
太宰府IC
水城RP
大野城駅
堤RP
(建設中)
都市高速
博多南駅
九州大学
筑紫地区

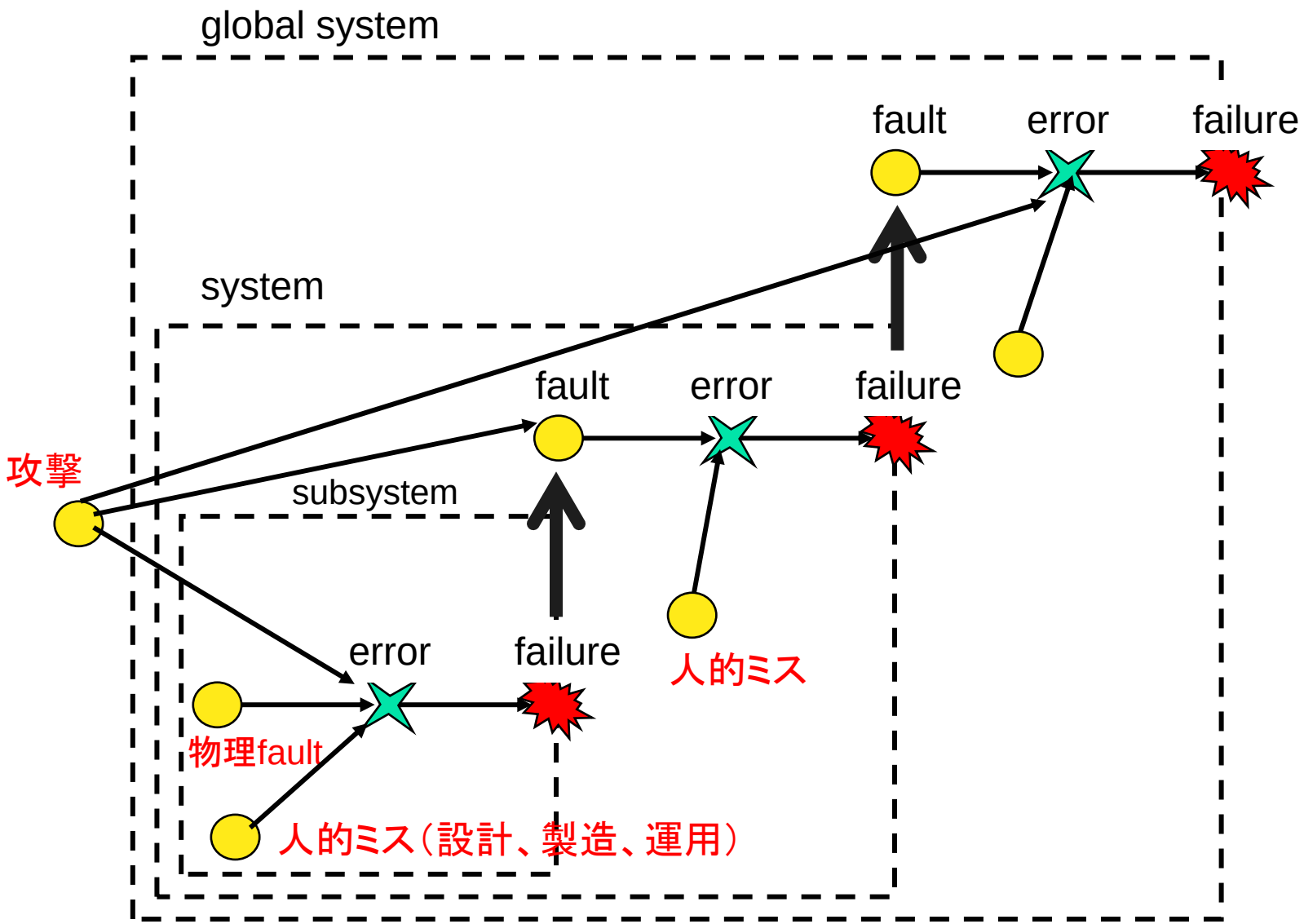
社会情報基盤の課題と新キャンパス周辺における実証実験

1. 情報技術と社会の変化
2. 社会情報基盤に求められるもの
3. 「価値」と「信用」
4. MIIDとe-Worldプロジェクト
5. Dependableな情報技術を目指して

Dependableな社会情報基盤を目指して

- 情報通信システムは社会の神経系である。
- 誰が何にDependするのか？
  - SystemがSW/DeviceにDependする。
  - 人や社会がSystemにdependする。
    - 何を守るのか？＝＞生命、財産、プライバシー
  - Dependability Chainの明確化
- SystemがDependableでなくなる原因は？
  - 自然現象による脅威
  - 人間活動（設計、製造、運用）における誤りやミス
  - 悪意ある攻撃による脅威
  - 「仕様」が規定できない
- SystemのLife Cycleの中での脅威の位置づけ
  - 設計者、製造者、販売者、運用者の責任の明確化

Modern Fault Model: Faultの多様化



阻害要因による分類

- 自然現象による脅威 (Natural Threat)
  - 自然界からの雑音
  - デバイスの故障・経年変化
  - 製造時の揺らぎ
- 人間活動（設計、製造、運用）におけるミス(Human Errors)
  - 設計や仕様上の誤り
  - 製造時の誤り
  - 運用上の誤り
- 悪意ある攻撃による脅威 (Human Attack)
  - 攻撃への耐性（設計時、製造時、運用時など）
  - 事故時の対応（波及の局所化、迅速な復旧）
  - 利用者の了解性、社会の受容環境
- 複数の要因の複合的効果
  - システム同士、システム対人、人同士のインタラクションに起因する不具合
  - 「仕様が規定できない」という本質的問題

Life Cycle Stagesの視点

- Dependabilityに影響するLife Cycle Stages
  - 企画 (Planning)
  - 設計 (Design)
  - 製造 (Fabrication)
  - 検査 (Test)
  - 流通 (Distribution)
  - 運用 (Operation)
  - 廃棄・更新 (Abandonment/Replace)

人命にかかわる例（自動車用LSI）

	自然現象	人的ミス	人的攻撃
企画		仕様不備 寿命設定ミス	企画の盗難
設計		設計ミス、バグ 利用環境の想定ミス	設計の盗難
製造	製造ばらつき	製造ミス	
検査	間欠故障の見逃し	見逃し	不良品混入
流通	実装中の環境変化	不良・偽造品混入	偽造品混入
運用	経年変化、温度環境	利用事故 保守のミス	無線による攻撃
廃棄・更新		更新不整合	情報抜取

赤字：原因

財産にかかわる例（電子マネー用LSI）

	自然現象	人的ミス	人的攻撃
企画		仕様不備 交換時への配慮不足	企画の盗難
設計		設計ミス、バグ 利用環境の想定ミス	設計の盗難 不正回路挿入
製造	製造ばらつき	製造ミス	違法な生産による横流し
検査	間欠故障	見逃し	良品横流し
流通	運搬・保存中の環境変化	運搬等の事故	盗難、横流し
運用	経年変化 宇宙線・環境	利用事故	Phishing、virus 盗聴、不正利用
廃棄・更新		更新時不整合	情報抜取・解析

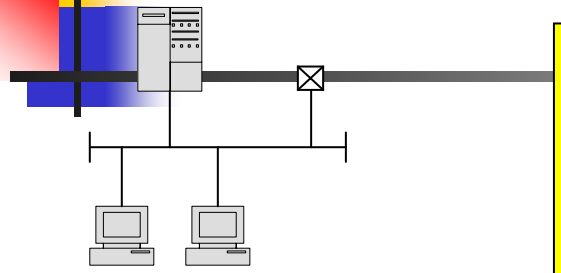
赤字：原因

Dependability向上の対策

	自然現象	人的ミス	人的攻撃
企画	製品寿命の見積もり 環境変化の予測	仕様の完備 ライフサイクルの予測	機密保持 攻撃の予測
設計	耐故障設計、雑音対策 DFM、DFT モニタ機能の組込み 単純なアーキテクチャ	設計検証 設計品質管理 テスト容易化 製品の操作性向上	設計データ管理 耐タンパ設計 Security-on-Chip 製品管理の仕組
製造	製造ばらつきの制御	工程管理の徹底	製品管理の徹底
検査	テスト精度向上 悪環境下のテスト	工程管理、自己テスト テスト精度向上	製品管理の徹底 モニタリング
流通	環境の保全・管理	物流の管理	物流の管理 トレース技術
運用	環境モニタリング Online Self Test	利用履歴モニタリング 利用者教育	利用者教育 監視、攻撃対策
廃棄・更新	自殺、異常通知機能	自動消去機能	無効化

国家的研究課題例

電子的通貨基盤の構築



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

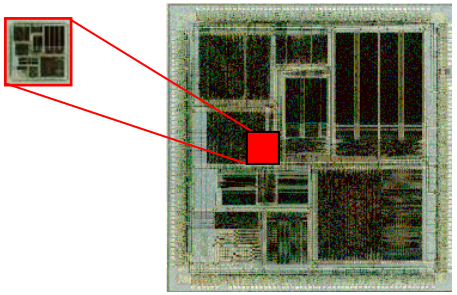
デバイスレベル

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

Secure Core



電子経済時代の通貨・徴税の仕組みの構築

マクロ情報科学への展開

情報自体の解明と制御

マクロ情報学

ミクロ情報学

情報と社会
社会システムの
神経系としての情報技術
およびその基礎科学

情報と人間
人間の情報処理機構の
解明とその人工的実現
人工知能

情報科学の基礎

情報の産業応用
IT産業、情報関連産業
総合電機産業、その他の
産業分野への応用
情報工学

情報と科学
情報技術を基本手段とした
科学探究手法の構築
計算科学

手段としての情報技術