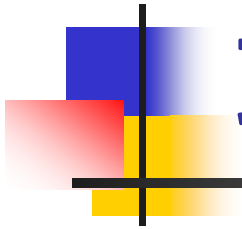
九州大学学術情報リポジトリ
Kyushu University Institutional Repository

「価値」と「信用」を取り扱う情報技術に向けて

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/2324/9140

出版情報：SLRC プレゼンテーション, 2006-07-19. 九州大学システムLSI研究センター
バージョン：
権利関係：



「価値」と「信用」を取り扱う情報技術に向けて

安浦寛人
九州大学システムLSI研究センター
2006.7.19

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

社会システムと情報技術

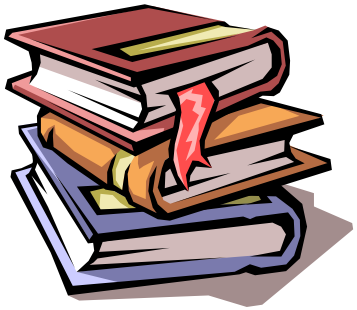
- 20世紀後半は既存の社会システムの中に情報通信技術を部分的に導入し、サービスの高度化、高速化を進める時代であった。
- 通信速度、情報処理速度の向上は、システムの設計時に想定しなかった事態を生み出すようになった。
- 21世紀は情報通信技術を前提として社会システム自身を再設計する時代。
  - 社会情報基盤(Social Information Infrastructure)
  - ユビキタス社会、 e-Japan、u-Japan

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
- 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
- **情報技術を前提とした社会システムの再構築**
  - **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

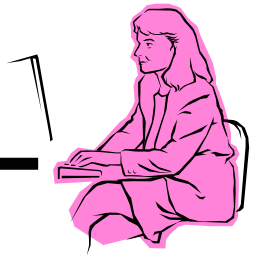
書く（100文字/分）



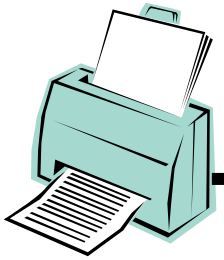
読む（1000文字/分）

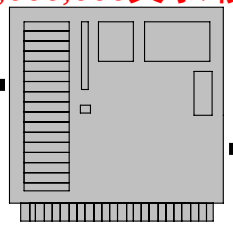
話す（500文字/分）

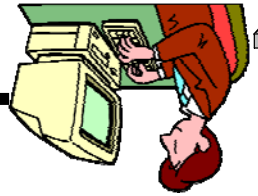
ファクシミリ（2000文字/分）

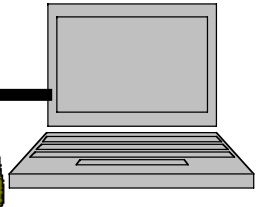


インターネット
（1,000,000文字/秒）

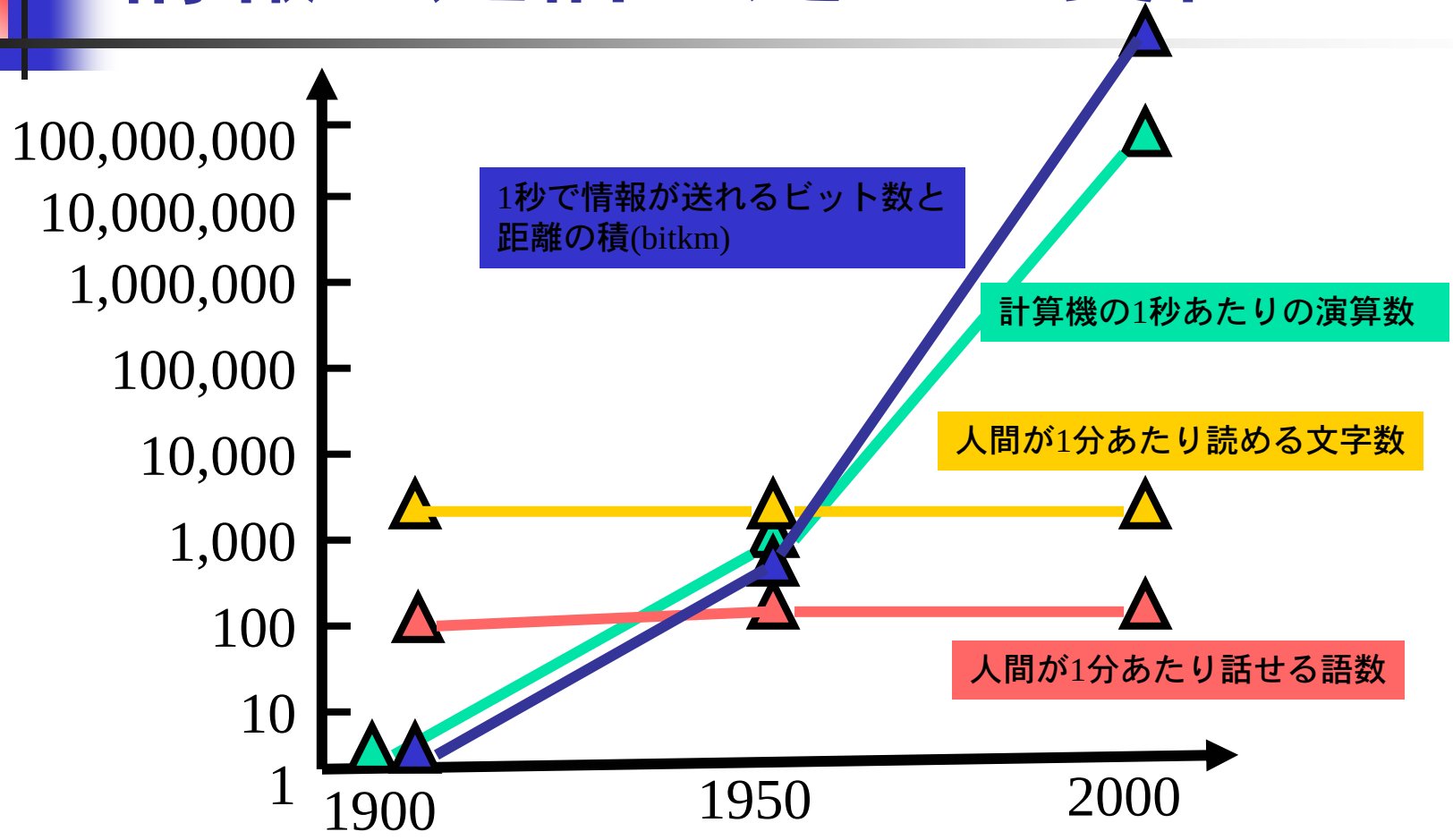




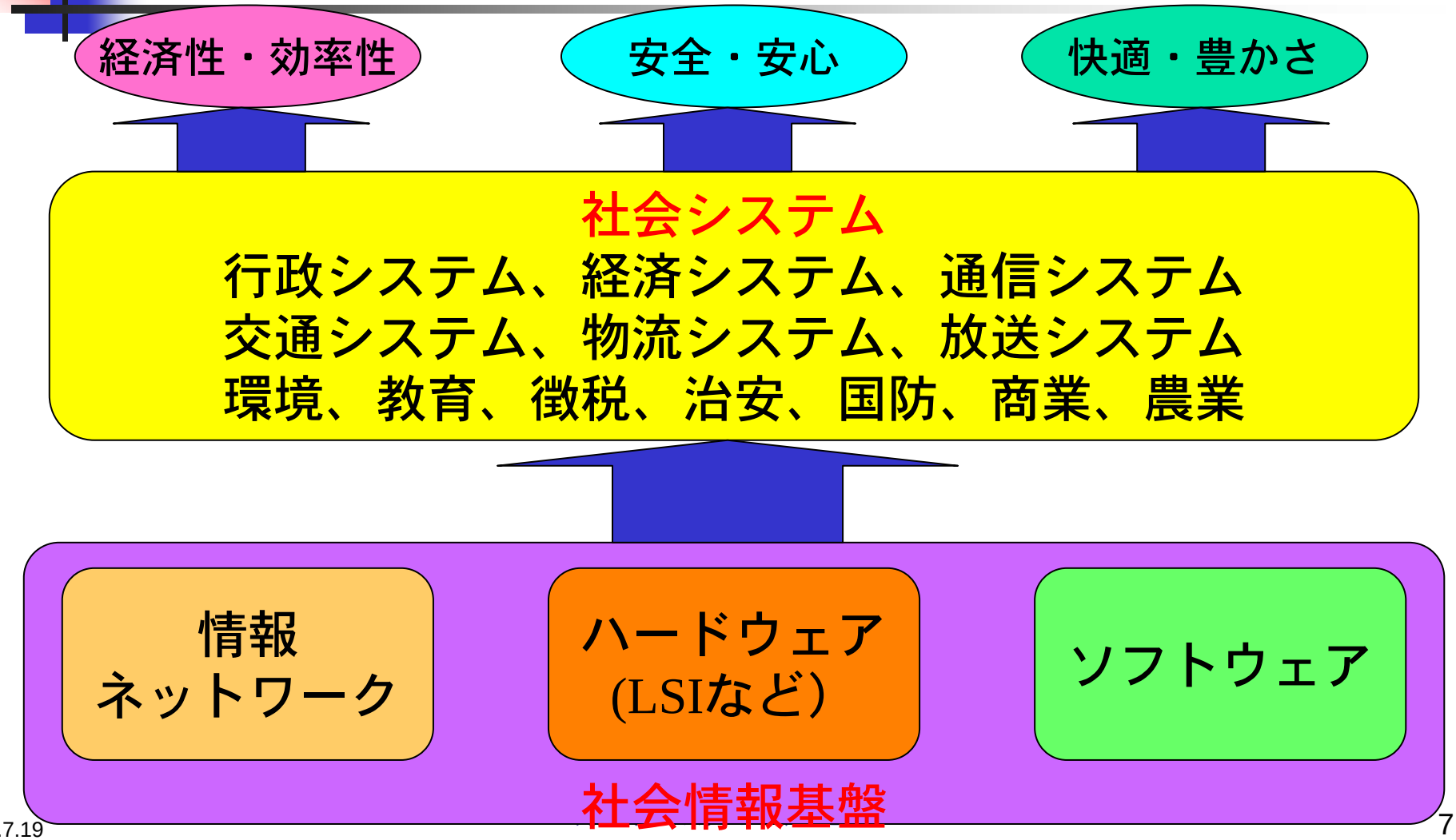




情報の通信・処理の変化


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

システムLSI研究センターの役割

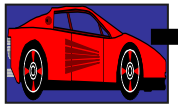
九州大学システムLSI
研究センターの対象範囲

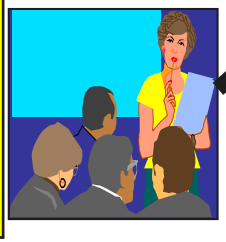
東京大学大規模集積
システム設計教育センター
(VDEC)の対象範囲

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

QUBE: Q-shu University hardware/software Borderless system design Education program

QuickTimeý Ç²
TIFFÂiLZWÂj êLIÉÉvÉçÉOÉãÉÂ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾â©ÇÉÇ2Ç½Ç…ÇÒÍKóvÇ·ÇÍÂB

対象とする受講者層

先端レベル
入社10年目程度対象

応用レベル
入社3～4年目対象

基礎レベル
新入社員、大学院生対象

入門レベル
学部生、高専生対象

「システムLSI設計人材養成実践プログラム」

専任：教授：築添明、講師：久住憲嗣、助手：林田隆則、研究員：大石淳子
担当（研究院所属）：安浦寛人、福田明、中西恒夫

ハードウェア設計

HW/SW コデザイン

組込みソフトウェア設計

システムLSI設計技術習得コース

先端設計技術習得コース

設計教育ノウハウの提供
スタッフによるバックアップ

連携講座「実エンベデッドソフトウェア開発工学講座」

福岡知的クラスター創成事業

システムLSI研究センター「設計手法研究部門」

21世紀COEプログラム

九州大学システムLSI研究センター
九州大学大学院システム情報科学研究院

上級者向け講座を編入

応用課程・実践課程等

基本課程

若年者人材育成プロジェクト講座

福岡システムLSIカレッジ

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

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
  - 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）

QuickTimeý Ç²
TIFFÅiàlèkÇ»ÇµÅj êLí£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÕïKóvÇ-Ç⁄ÅB

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

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

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(90兆円)
    - 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
- 発行者への信用をベースとした集団幻想

QuickTimeý Ç²
TIFFÅiàÌèkÇ»ÇuÅj ëLíÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÉÇžÇ½Ç…ÇÕïKóvÇ·ÇÍÅB

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

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？

現金貨幣の情報モデル

目的：現金貨幣の電子化のための技術的基盤を作る

1. 現金の情報科学的モデル（仕様）を作る
2. 既存の電子マネーをこれに当てはめて違いを確認
3. 違いの部分は技術的に克服可能か？
   - Yes：どのような技術が必要なのかを明確にする。必要ならば制度や法律の変更も考える。
   - No：現金とは異なる概念の社会制度として「電子マネー」を設計する必要がある。

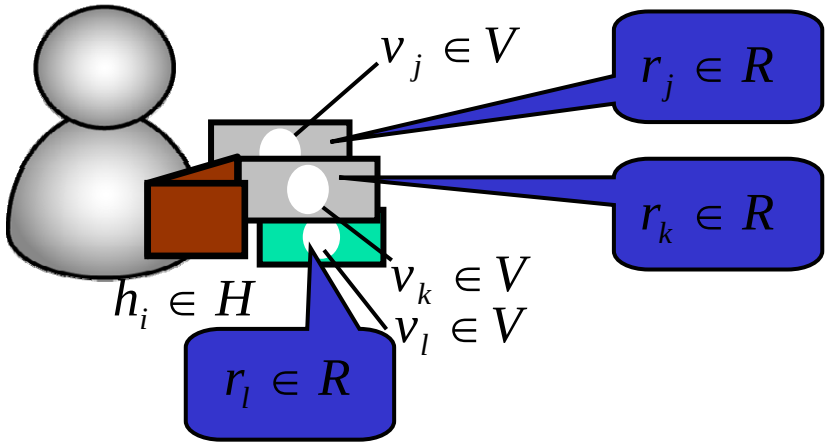
基本要素の集合

- 価値トークン(Rights)．価値や権利などを証明するものでありそれ以下に分割できない最小要素．偽札に対応する価値トークンはない．
- 媒体(Vehicle)．現金の集合．紙幣や硬貨のことを指す．偽札も含まれる．
- 保持者(Holder)．人が持つ財布など．

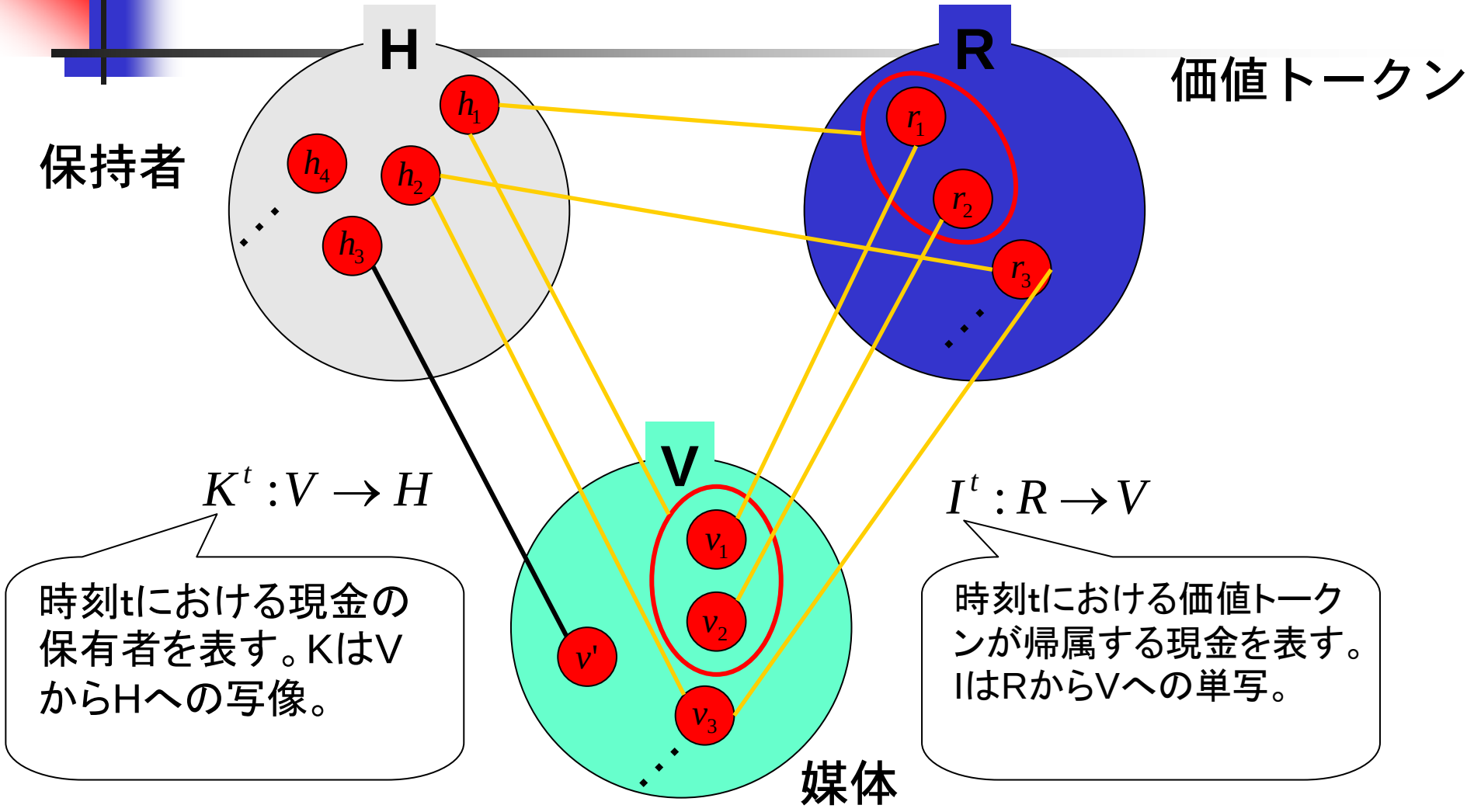
$$R := \{r_1, r_2, \ldots r_n\}$$

$$V := \{v_1, v_2, \ldots v_m\}$$

$$H := \{h_1, h_2, \ldots h_l\}$$



集合間の関係


H
R
価値トークン
保持者
h_1
h_2
h_3
h_4
r_1
r_2
r_3
V
v_1
v_2
v_3
v'
$K^t : V \to H$
時刻tにおける現金の保有者を表す。KはVからHへの写像。
$I^t : R \to V$
時刻tにおける価値トークンが帰属する現金を表す。IはRからVへの単写。
媒体

集合の時間的変化

- 現金の譲渡（時刻tにおいて保持者h_iからh_jへ媒体v_kが譲渡される場合）

$$V_{h_i}^{(t+1)} = V_{h_i}^{(t)} - \{v_k\}, V_{h_j}^{(t+1)} = V_{hj}^{(t)} \cup \{v_k\}$$

$$\forall x \neq i, x \neq j, V_{h_x}^{(t)} = V_{h_x}^{(t+1)}$$

- 現金の発行（時刻tにおいて新しい媒体v_iが発行される場合）

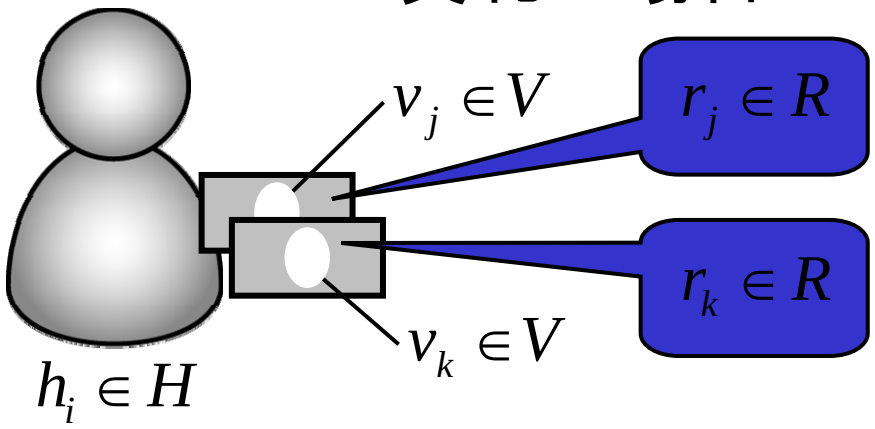
$$V^{(t+1)} = V^{(t)} \cup \{v_i\}, R^{(t+1)} = R^{(t)} \cup \{r_i\} \quad \left(v_i = I^t(r_i)\right)$$

- 現金の回収（時刻tにおいて媒体v_iが回収されて廃棄される場合）

$$V^{(t+1)} = V^{(t)} - \{v_i\}, R^{(t+1)} = R^{(t)} - \{r_i\} \quad \left(v_i = I^t(r_i)\right)$$

判別関数

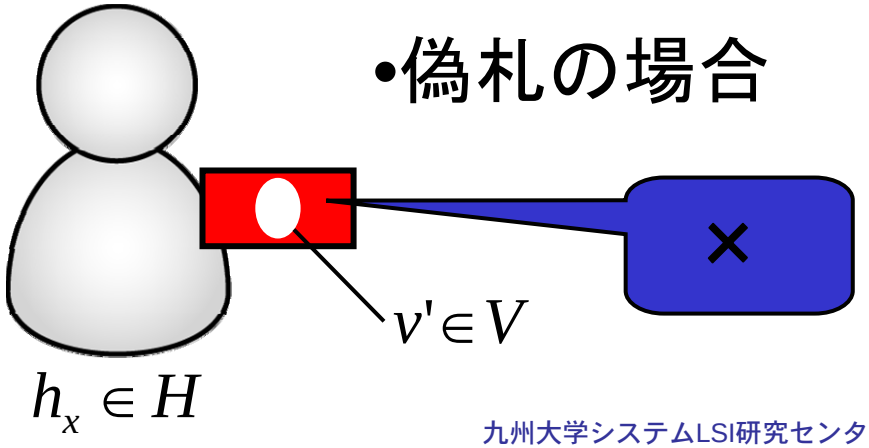
•真札の場合



$D(v_j) = true$

$D(v_k) = true$

•偽札の場合



$D(v') = false$

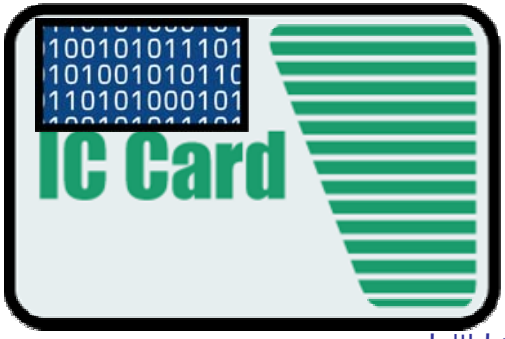
現金通貨の性質

- 判別関数Dの周知
- 判別関数の適用（市民、機械、銀行、中央銀行）
- 転々流通性
  - 第三者を介することなく当事者同士のみで現金の譲渡ができる
- 価値トークンの総量の保存
  - 発行者による発行や回収以外では価値トークンの総量は変化しない（現在の現金では物質の保存則に依存している）

$$\sum_{k=1}^{n} R_{h_k}^{(t+1)} = \sum_{k=1}^{n} R_{h_k}^{(t)}$$

電子マネーは現金貨幣か？

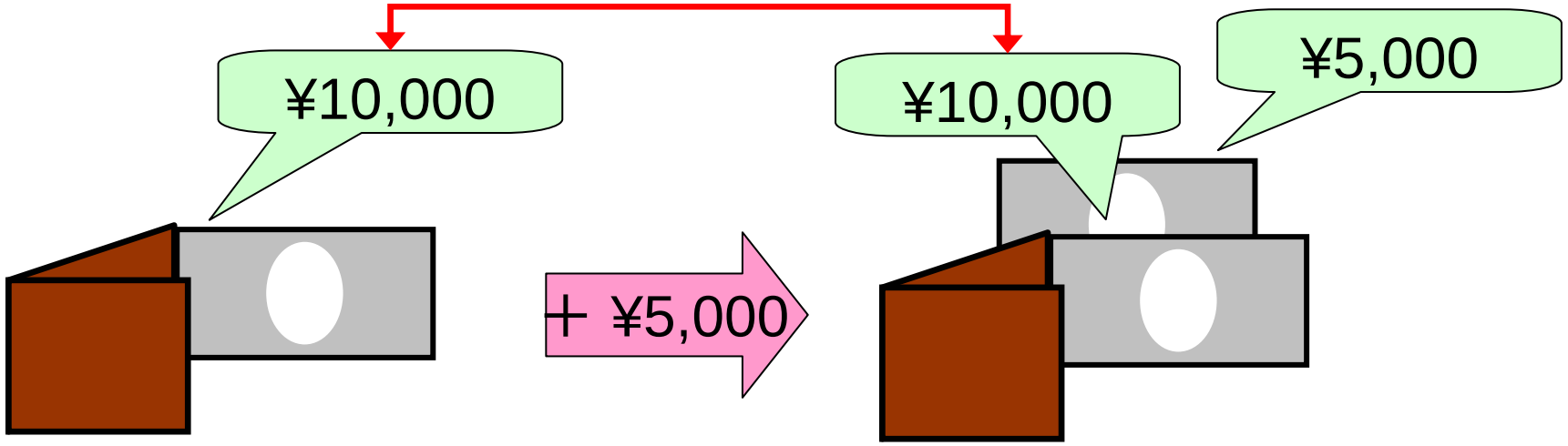
- EdyやSuicaは現金通貨の仕様を満たすか？
  - ディジタルデータを媒体として用いる
  - 保持者はICカードを用いる
  - 価値トークン
    - ローカル内で、残高金額として保持される
    - 移動は電子的な通信により行われる
    - 発行者間とユーザ間のみで移動が行われる



媒体集合の問題(1/3)

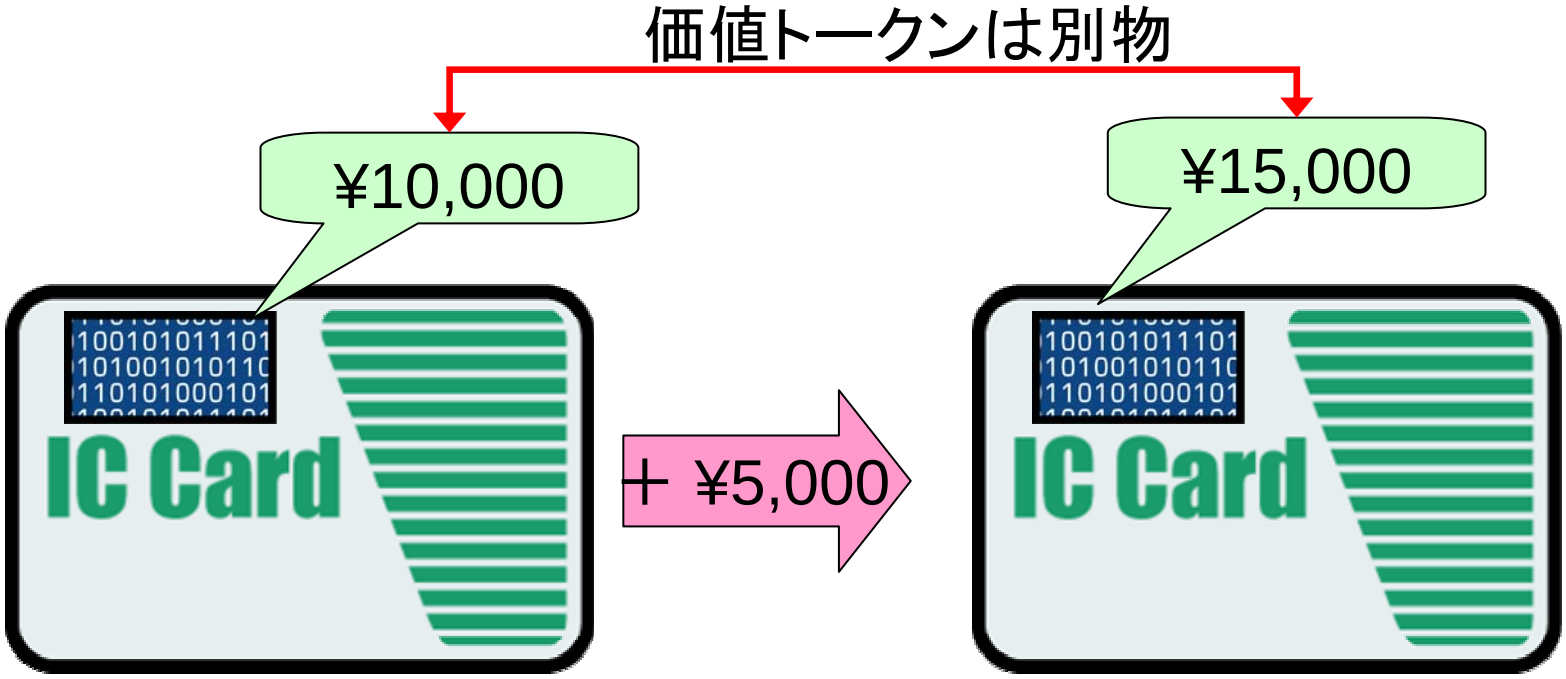
- 現金における媒体は、物理的制約から分割できない最小要素からなる

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)

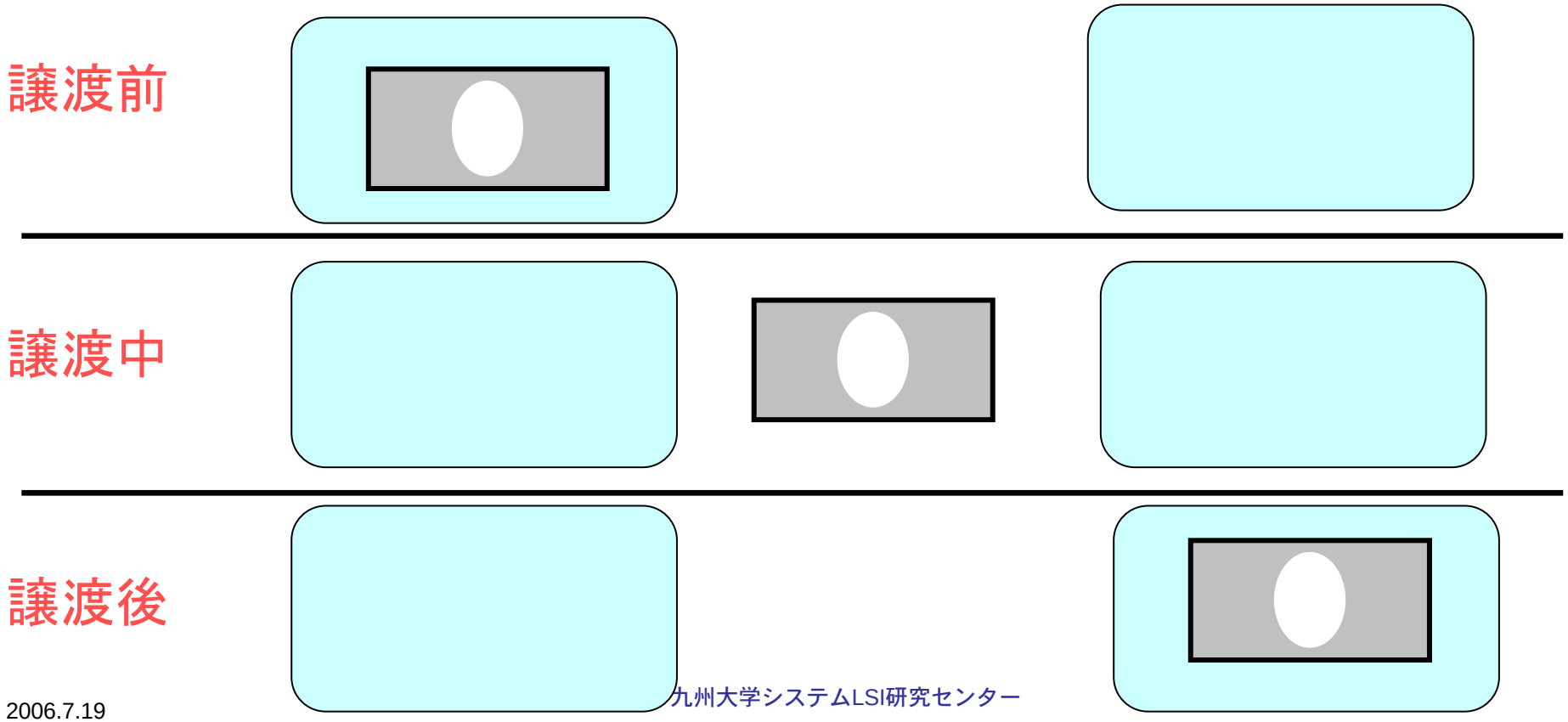
- 価値トークンの集合と媒体の集合の関係をどうやって保つ？
  - 偽造されたデータが混入した場合、すべて無効になる？
  - 関係があいまいであるがゆえに匿名性を確保できる?

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？

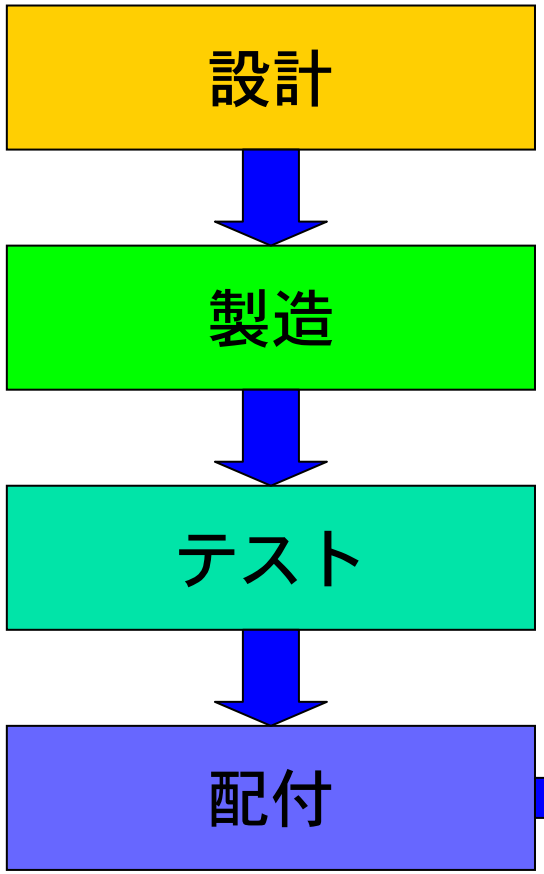
- 財布であるなら
  - 偽物でも入っている「価値」が本物なら許せる
  - ブランド品と安物の差はあっても、中身の「価値」とは無関係
- 貨幣であるなら
  - 偽物は許されない
  - 政府の通貨発行権や徴税権と密接に関係する
  - 財務省印刷局LSI部門が必要？
  - 暗号だけで済む話ではない

QuickTimeý Ç²
TIFFÅiàÌèkÇ»ÇµÅj êLÍÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾â©ÇÉÇ2Ç½Ç…ÇÕÍKóvÇ-ÇìÅB

QuickTimeý Ç²
TI FFÅiàÌèkÇ»ÇµÅj ê LÍÉÉvÉçÉO ÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾â©ÇÉÇ2Ç½Ç…ÇÕ ÍKó vÇ-ÇìÅB

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

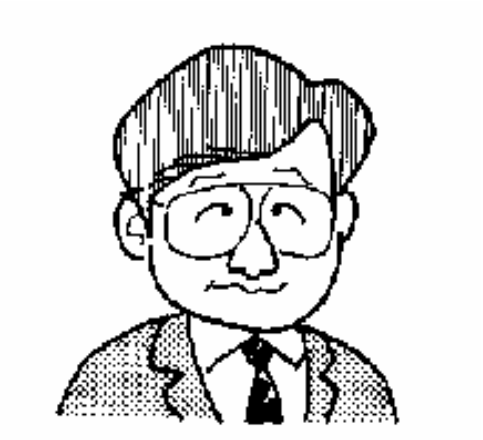
運用

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

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）

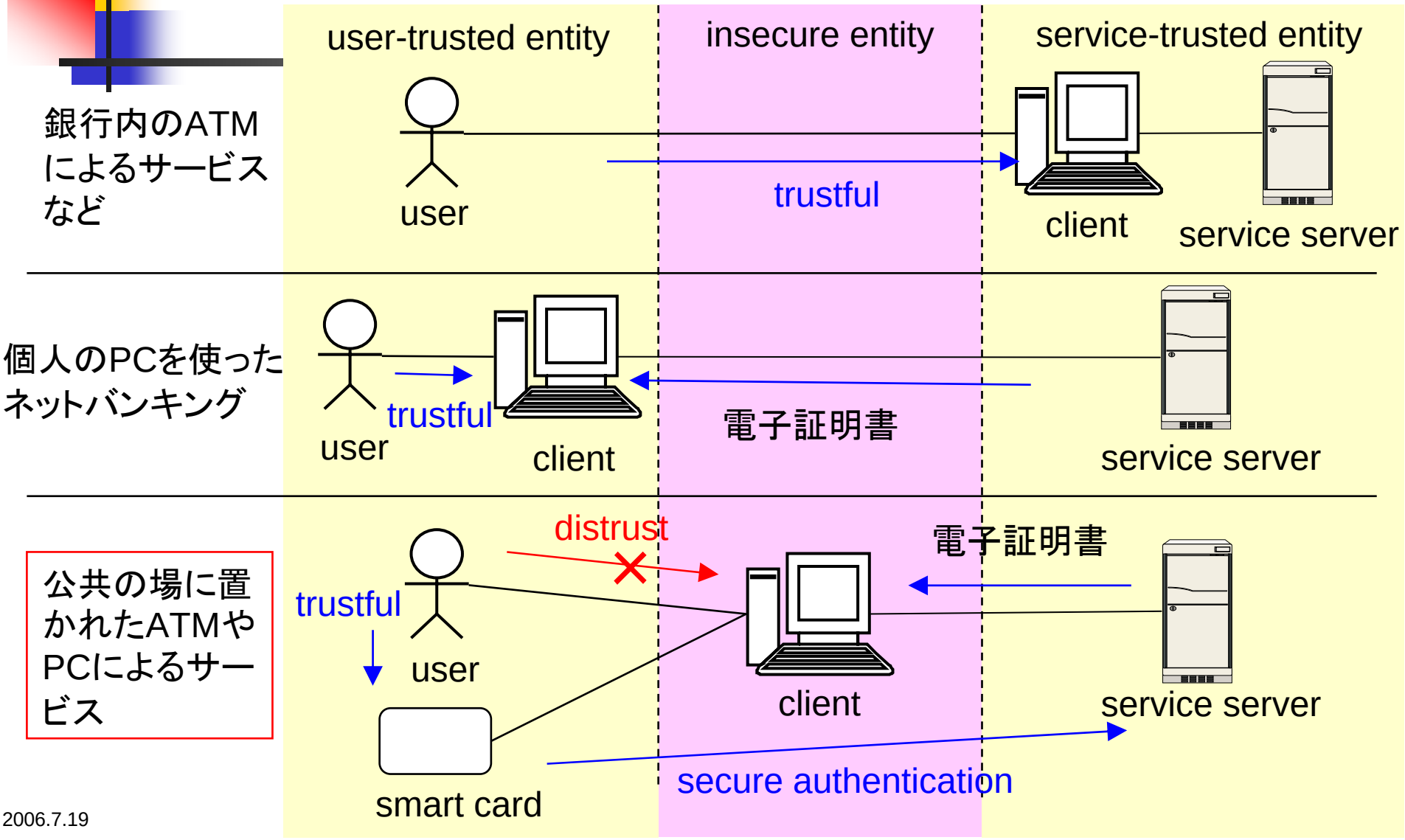
QuickTimeý Ç²
TIFFÅiâÌêkÇ»ÇµÅj ëLÍÉÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÆsÉNÉ ÉÉÇ¾â©ÇÉÇžÇ½Ç…ÇÒÍKóvÇ-ÇlÅ

QuickTimeý Ç²
TIFFÅiâÌêkÇ»ÇµÅj ëLÍÉÉvÉçÉOÉâÉÄ
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

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

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

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。

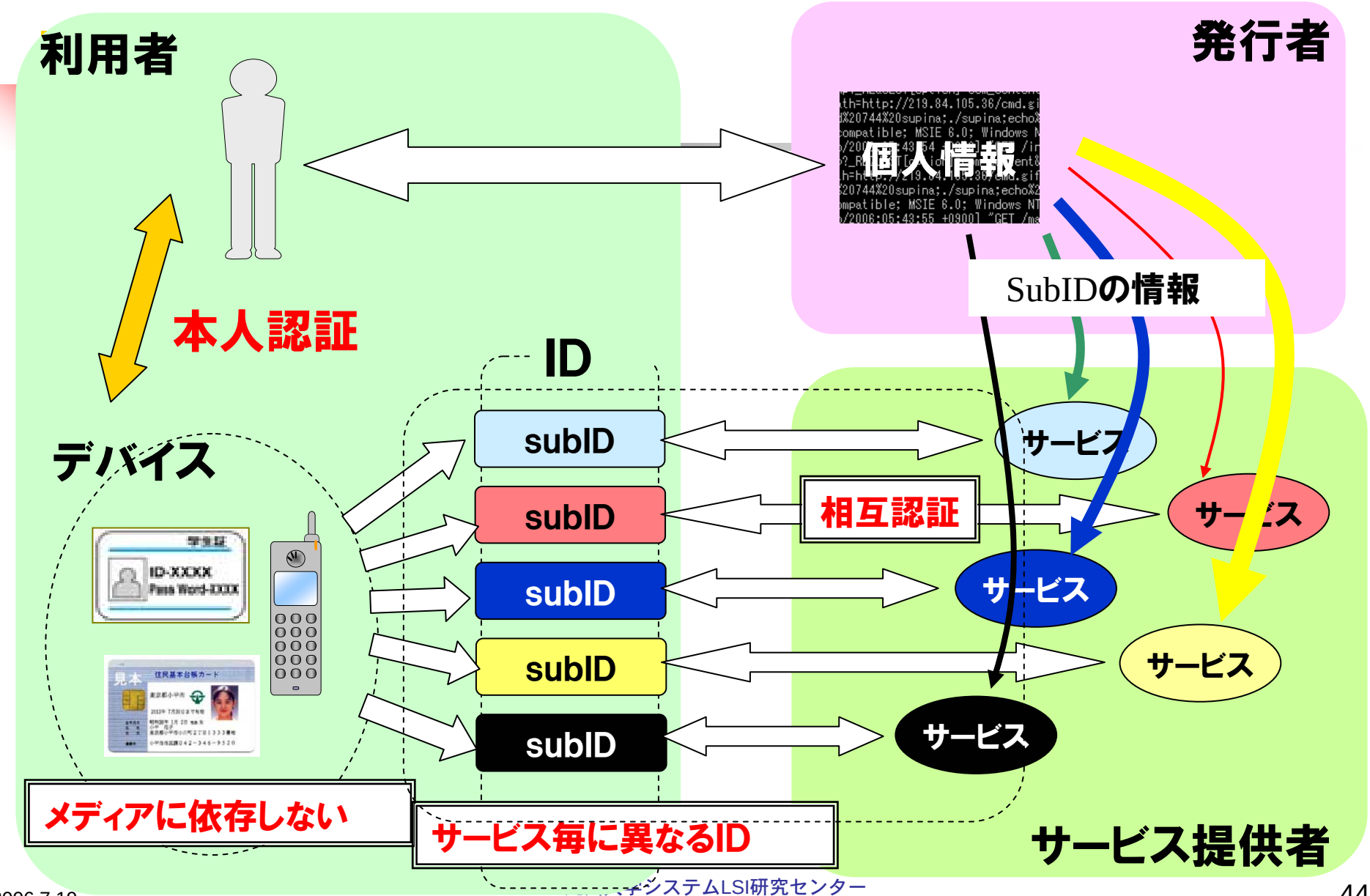
3 相互認証などの柔軟な認証方式

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

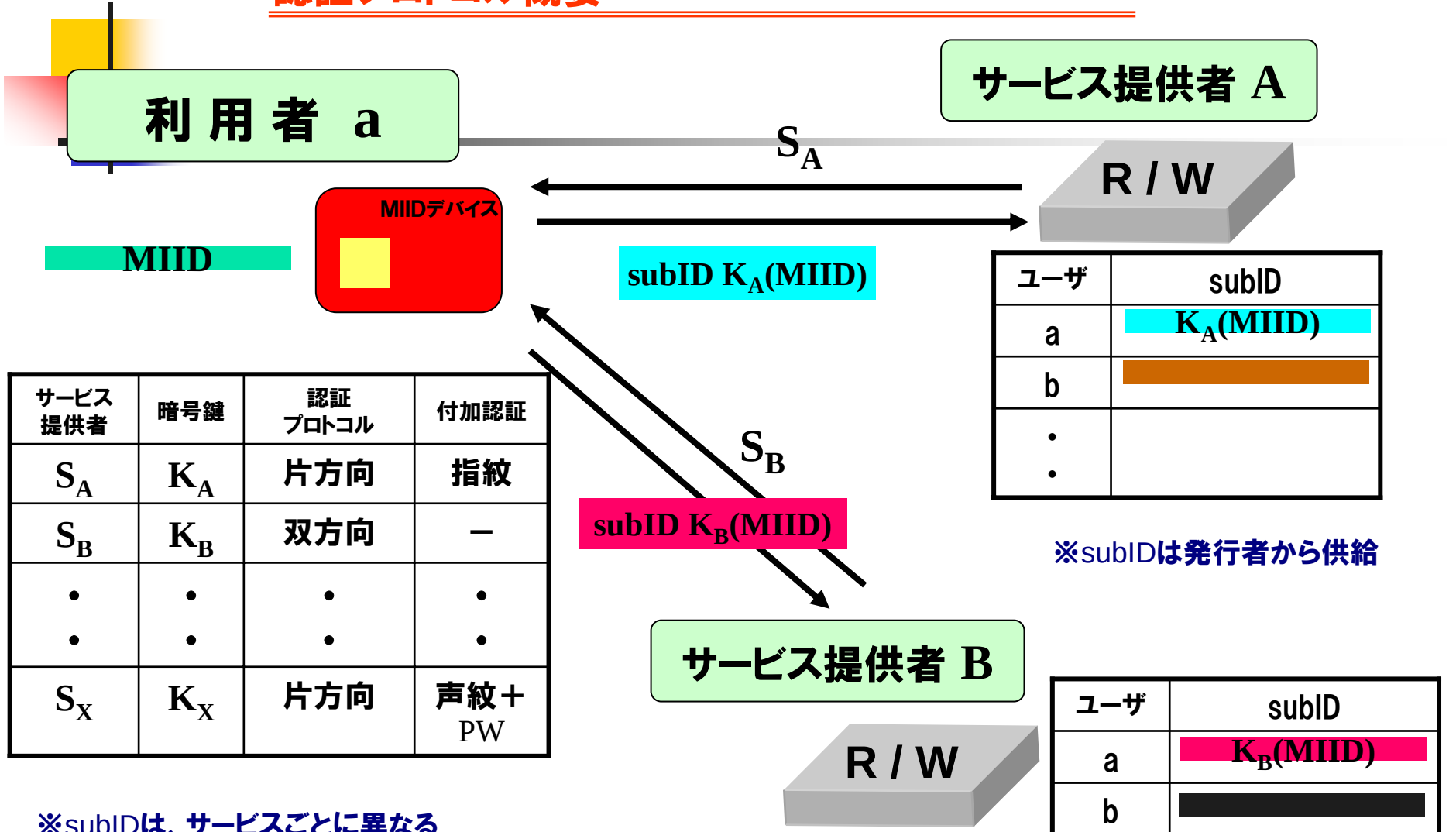
サービス提供者が個人情報を持つ必要がなく、情報を持つリスクを回避。個人情報の分散管理が可能。

MIIDシステム全体像



MIID管理システム

認証プロトコル概要

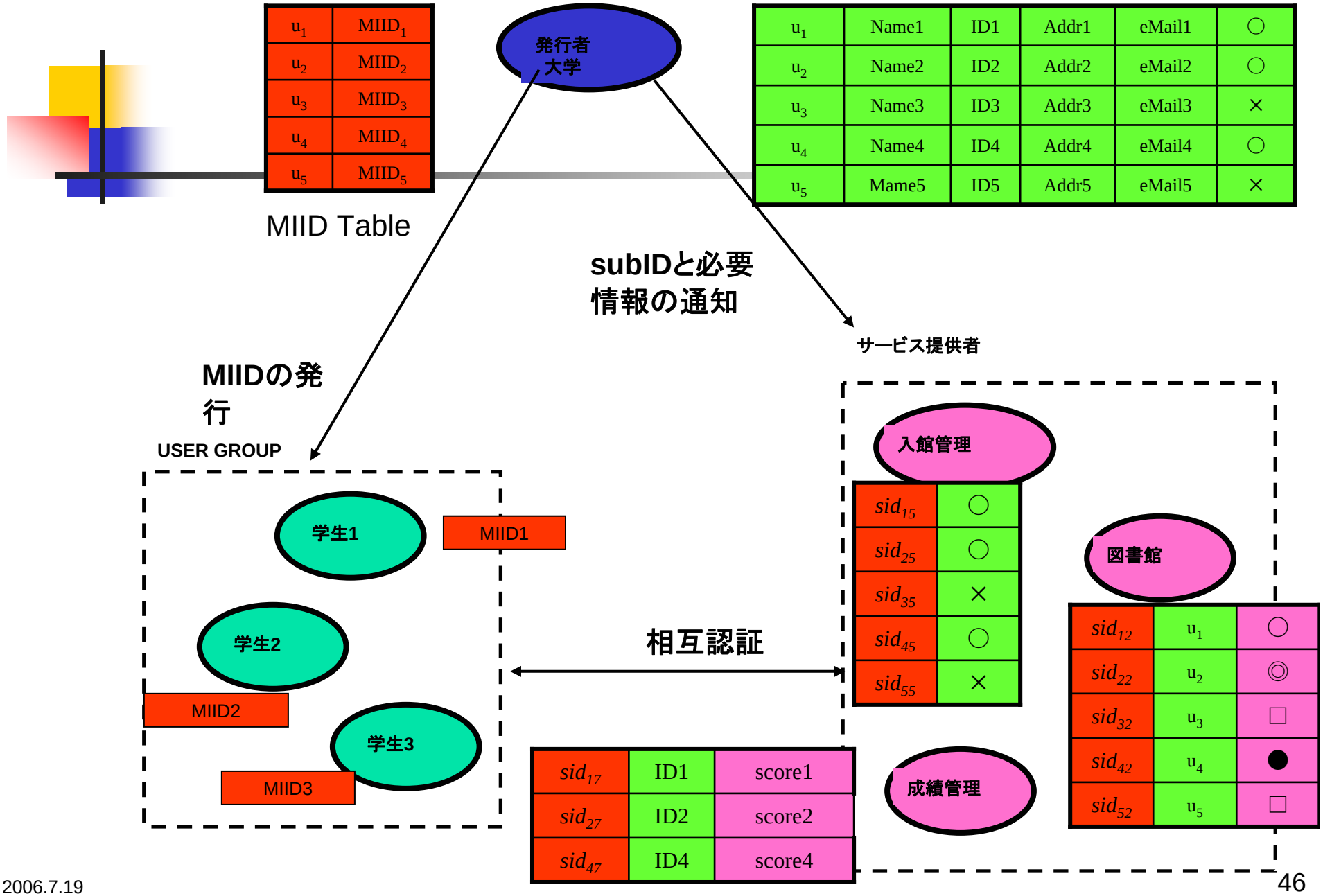


サービス提供者	暗号鍵	認証プロトコル	付加認証
S_A	K_A	片方向	指紋
S_B	K_B	双方向	−
・ ・	・ ・	・ ・	・ ・
S_X	K_X	片方向	声紋＋ PW

※subIDは発行者から供給

※subIDは、サービスごとに異なる
※あるサービスの事故時にはその暗号鍵の変更で対応
※実現時には暗号やセキュリティ技術と組合わせて実現

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)

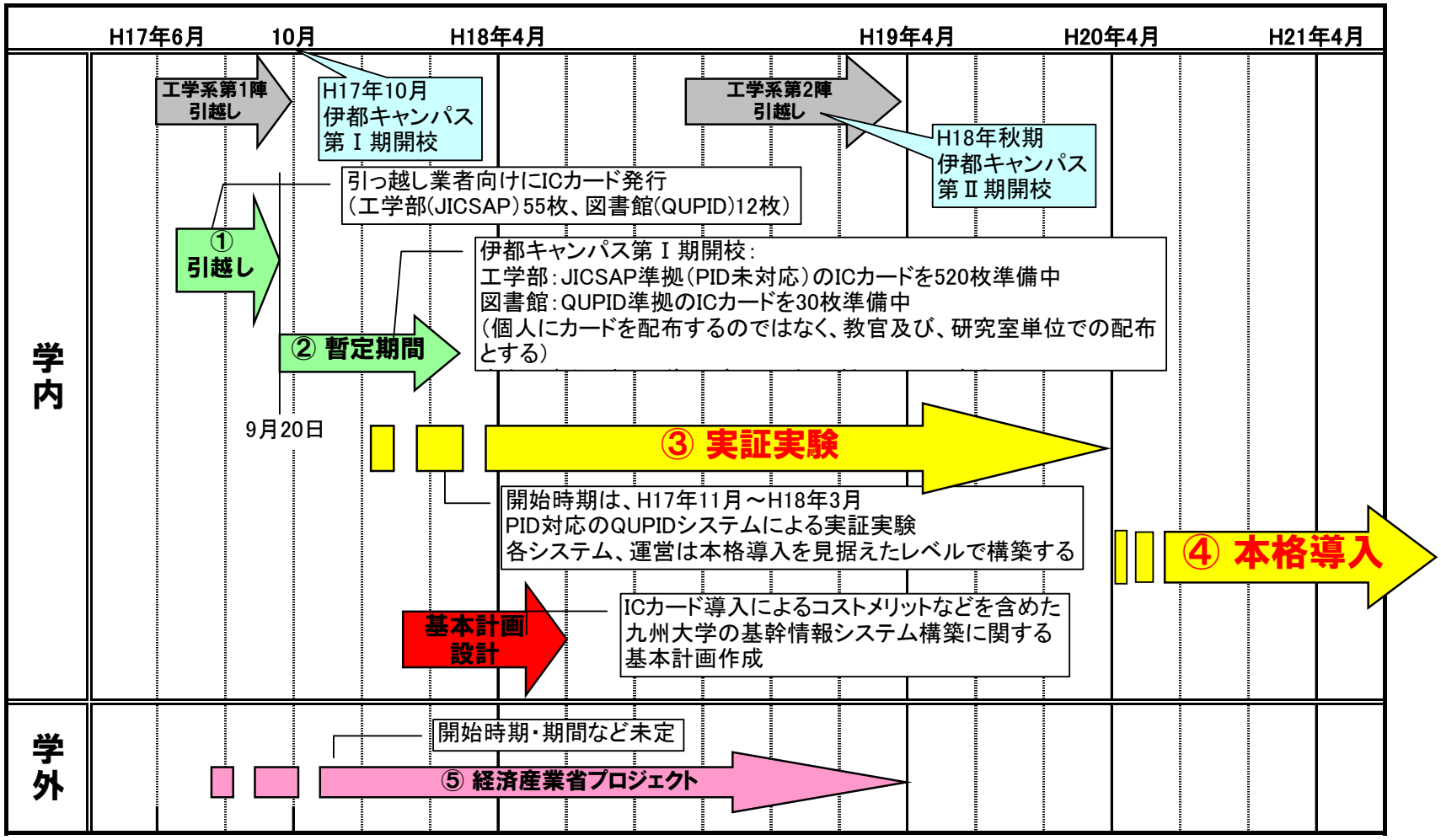
- 安全で安心な社会基盤システムを構築するための情報インフラを新キャンパスにおいて構築し、実運用して、技術のみならず社会科学的な視点も考慮した未来の社会基盤システムの方向性についての提言を行う。
- 新しい情報インフラを基盤とした、効率的で機能的かつ柔軟な大学運営体制を確立する。

九州大学システムLSI研究センター

これまでのICカード導入推進の経緯

2004年1月	全学共通ICカード導入推進室および同会議を設置
2004年2月	パートナー企業公募
2004年3月	パートナー企業選定 西日本電信電話（株）、松下電器産業（株）、（株）クマヒラ （株）キューデンインフォコム、（株）セキュアードコミュニケーションズ
2004年8月～	月１回のペースでステアリングコミッティ（SC会議）を開催。 導入のための各種工程の管理および協議を行ってきた。
2005年3月	（株）セキュアードコミュニケーションズが退会
2005年5月	松下電工（株）がSC会議に加入（新キャンパス研究教育棟の電子鍵）
2005年6月	実験用システムの完成と公開実験
2005年8月	新キャンパスで部分的に運用開始（新キャンパス理系図書館の電子鍵）
2005年9月	研究棟の電子鍵運用開始（松下電工仕様）
2006年1月	経済産業省・平成17年度「我が国のIT利活用に関する調査研究」の受託
2006年3月	経済産業省受託の実証実験（電子鍵、図書館貸出）
2006年5月	経済産業省・平成18年度「ディジタルコミュニティ実証実験」の受託

基本計画(平成17年６月策定)
ー見直し中ー



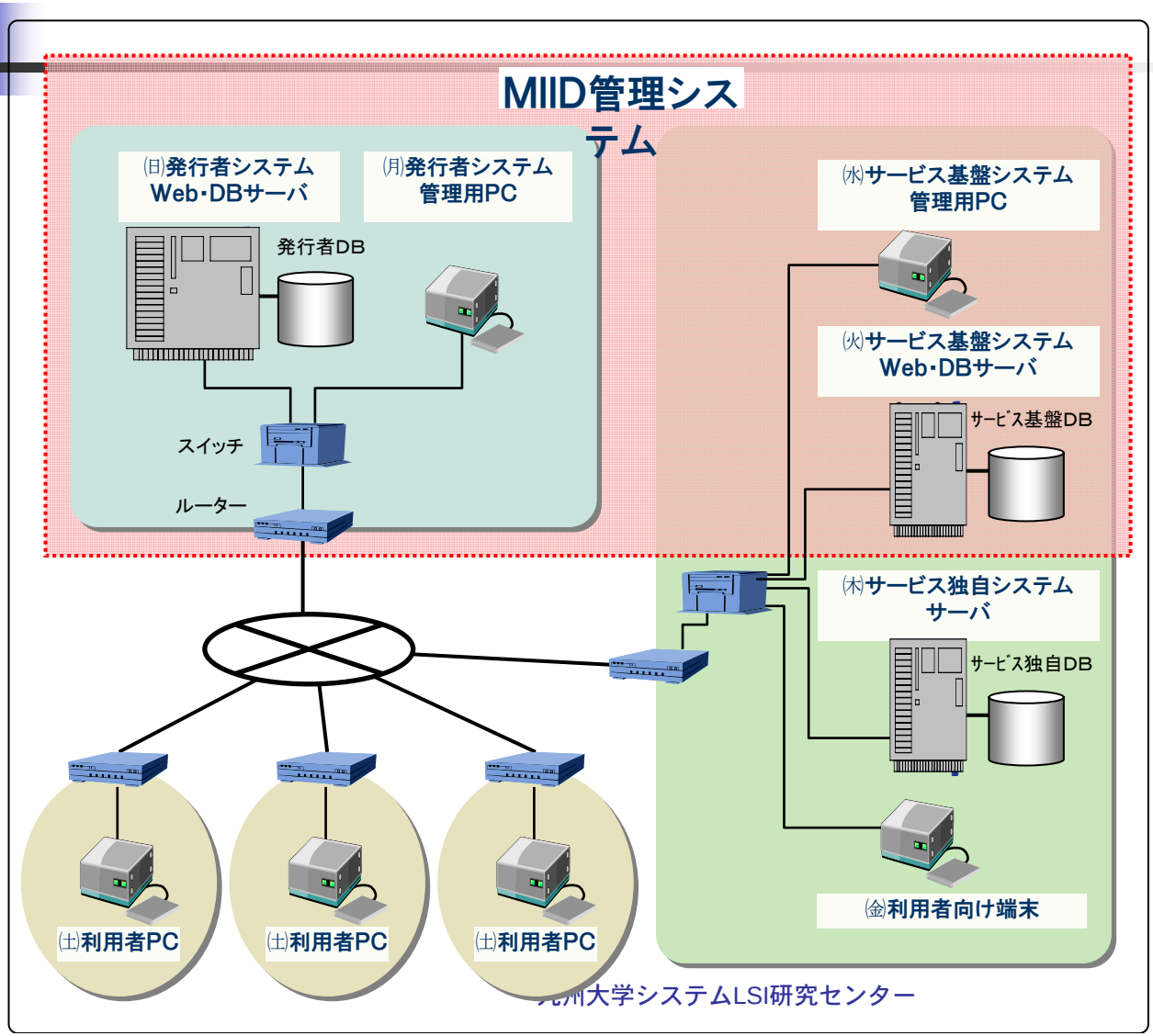
種々のMIID
デバイス

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

QUPID管理システム



MIIDの利用と展開

- 顧客、職員、学生、住民などの情報管理
  - 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
- 各種サービス
  - 交通カード、地域カード、地域マネーなどへの発展

「価値」と「信用」を取り扱う情報技術に向けて

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」の問題
4. 「信用」の問題
5. MIIDプロジェクト
6. Dependableな技術を目指して

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？＝＞Life、Property、Privacy
  - 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

Dependability Chain

- 社会→システム→
  サブシステム→
  デバイス
- 車の例
  - 社会：交通システム
  - システム：自動車、道路、信号系、交通規則
  - サブシステム：エンジン、制動系、ステアリング
  - デバイス：機械系、電子系、材料系

QuickTimeý Ç²
TIFFÅiàÎèkÇ»ÇµÅj êLÍ£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÕïKóvÇ-ÇÎÅB

QuickTimeý Ç²
TIFFÅiàÎèkÇ»ÇµÅj êLÍ£ÉvÉçÉOÉâÉÄ
Ç™Ç±ÇÃÉsÉNÉ`ÉÉÇ¾å©ÇÈÇžÇ½Ç…ÇÕïKóvÇ-ÇÎÅB

揺らぎと不確実性への増大

物理的揺らぎの
設計による吸収
- DFM
- Variation Tolerant Design

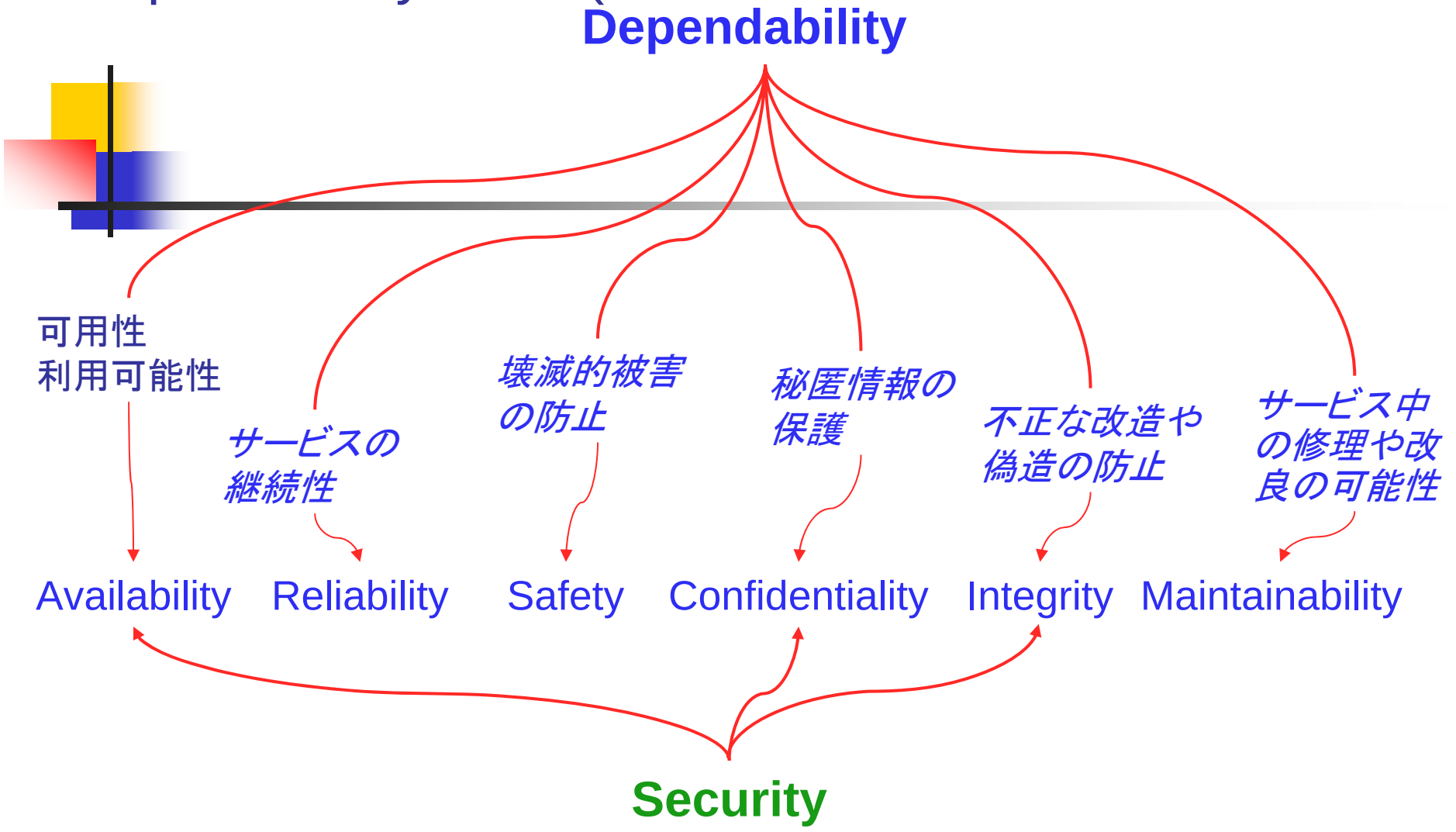
問題のシステム全体への波及の阻止

各層で発生する問題をいかにシステム全体の致命的な問題にせずに済ませるかという問題

Dependabilityとは

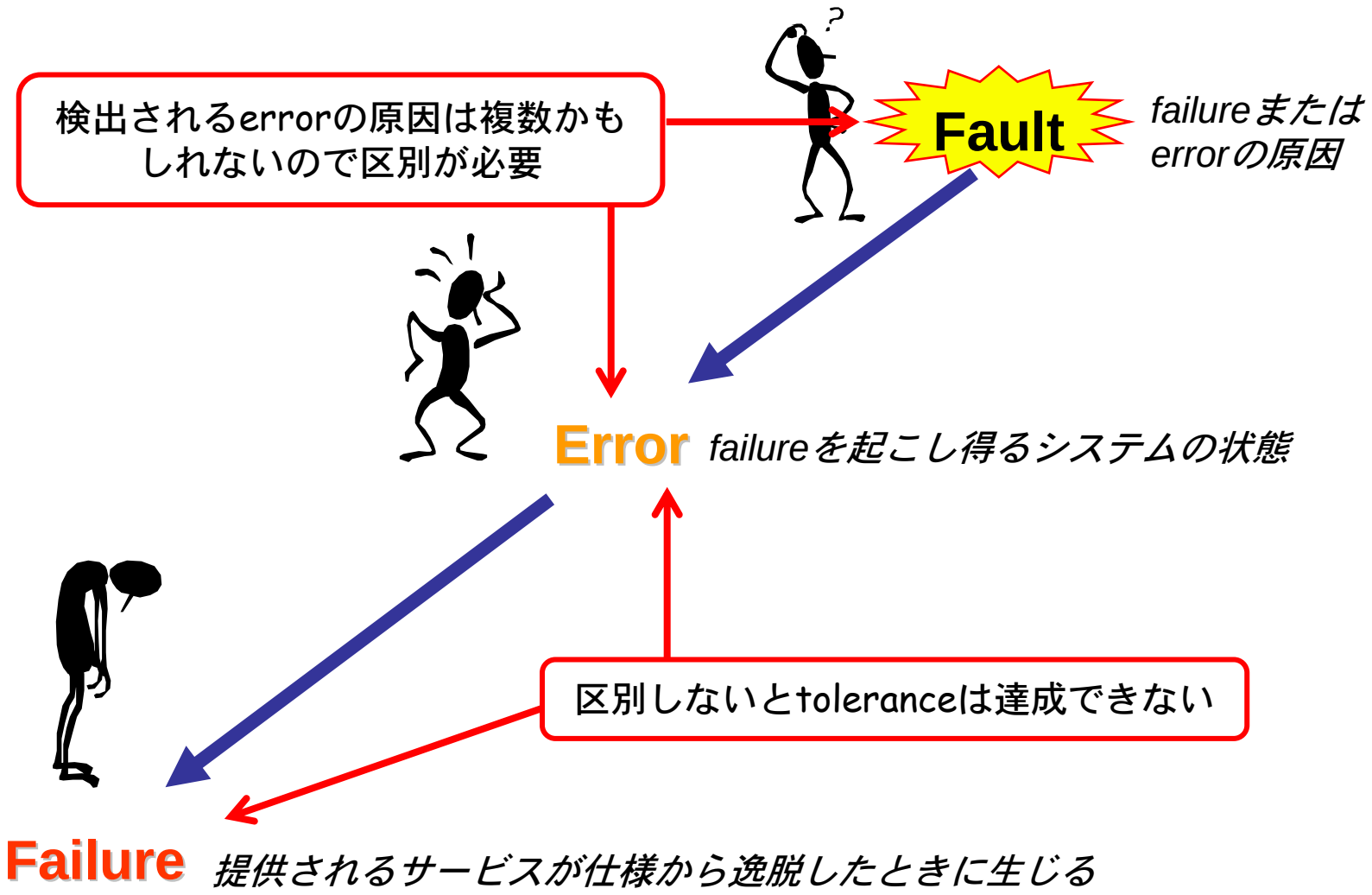
- ユーザ視点の概念
- 予測不可能性（想定外事象）を秘めた系において、システムに期待されるサービスが許容範囲内で提供されることが保証されること。あるいは、その保証の度合。
  - 合理的な有限責任をユーザに宣言するための基礎となる性質
  - 無限責任を負うべきシステム（原子力など）については、極めて厳しいレベルで要求される
- DependabilityのMetricsが定義されていないことが問題
  - 参照システムとの比較
  - 絶対基準における定義
  - 人命、財産、プライバシーなどユーザが託す対象によっても基準が異なる

Dependabilityとは？(IEEEでの議論から)



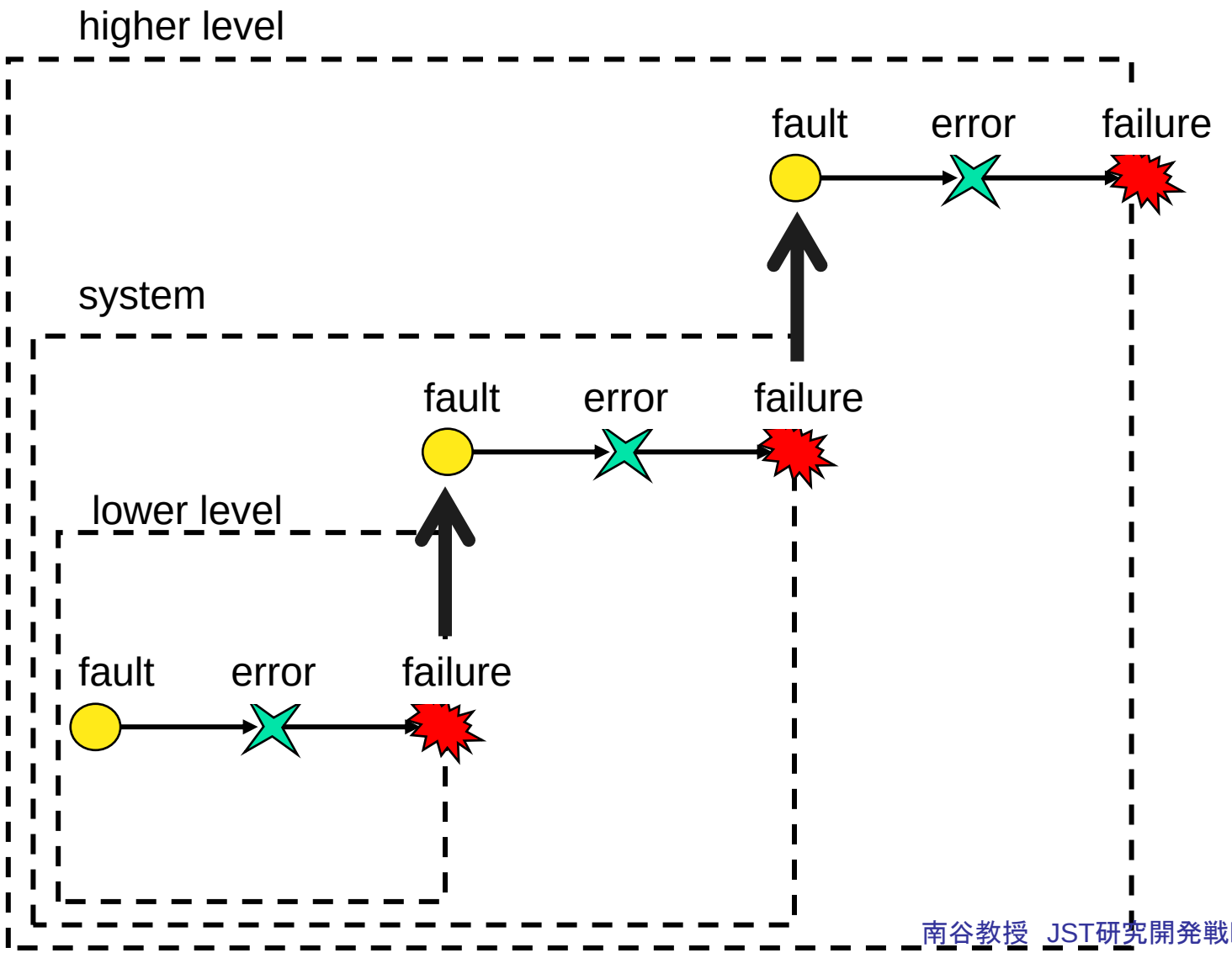
Absence of unauthorized access to, or handling of , system state

Dependability 阻害要因の因果関係



南谷教授　JST研究開発戦略センター
ディペンダビリティワークショップ資料

Classical Fault Model: Recursion

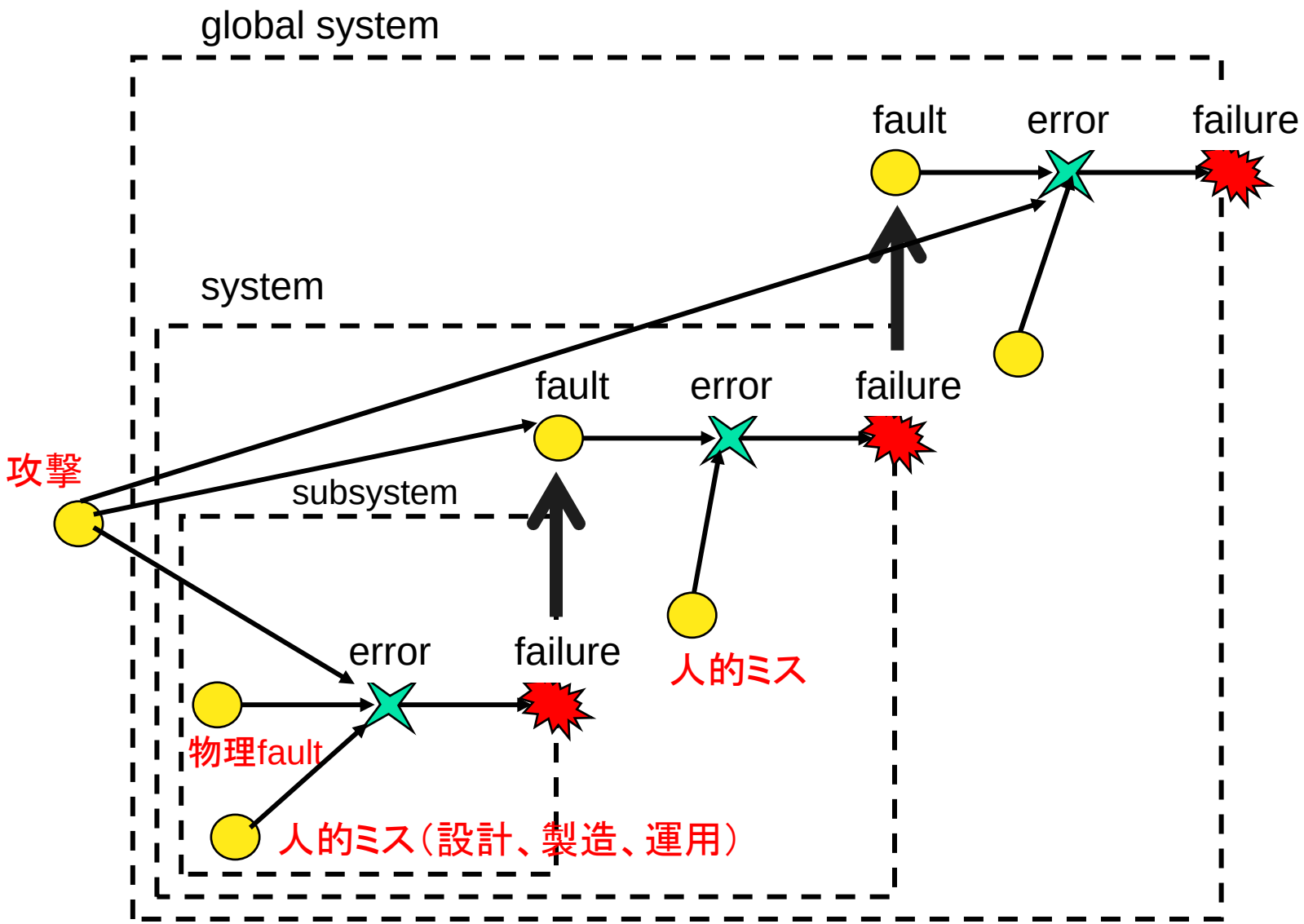


南谷教授　JST研究開発戦略センター
ディペンダビリティワークショップ資料

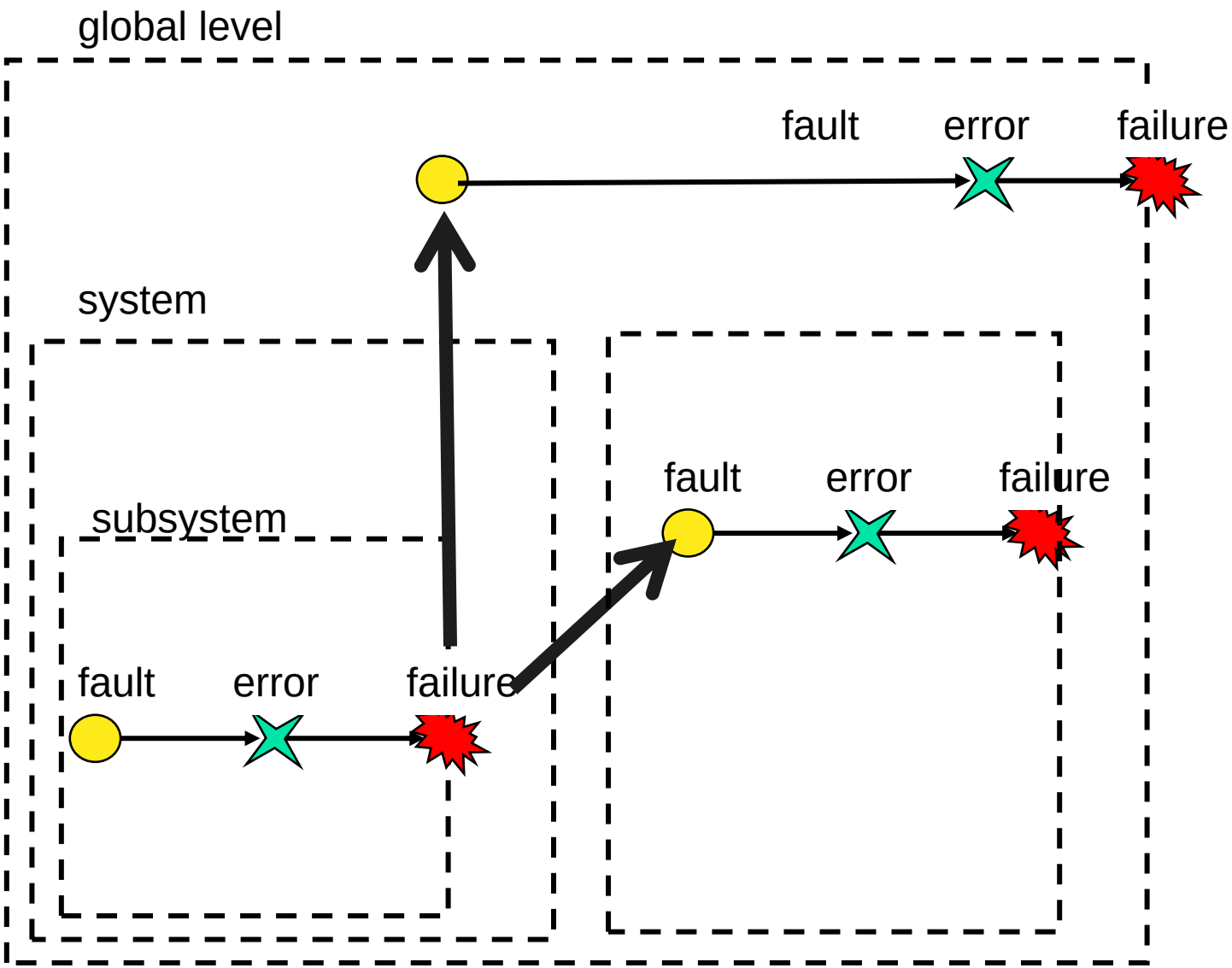
現代的な問題

- Faultの多様化
  - 自然現象中心から人間の誤りや攻撃によるものへ
- FaultとFailureの関係の多様化
  - 階層を飛び越えた影響
  - 複数のFaultの組み合わせ効果
- Failureの定義の変化
  - システム仕様の動的な変化

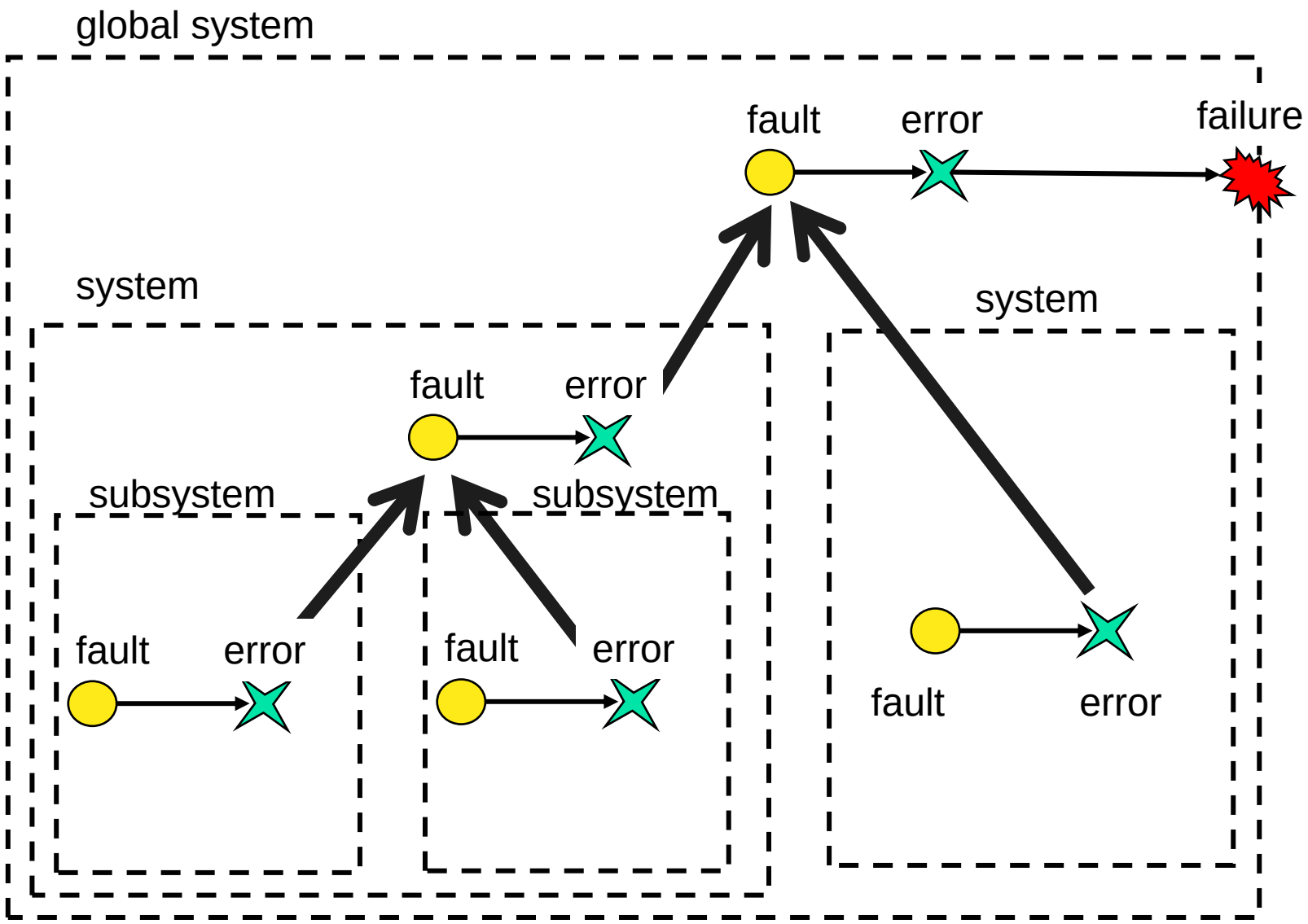
Modern Fault Model: Faultの多様化



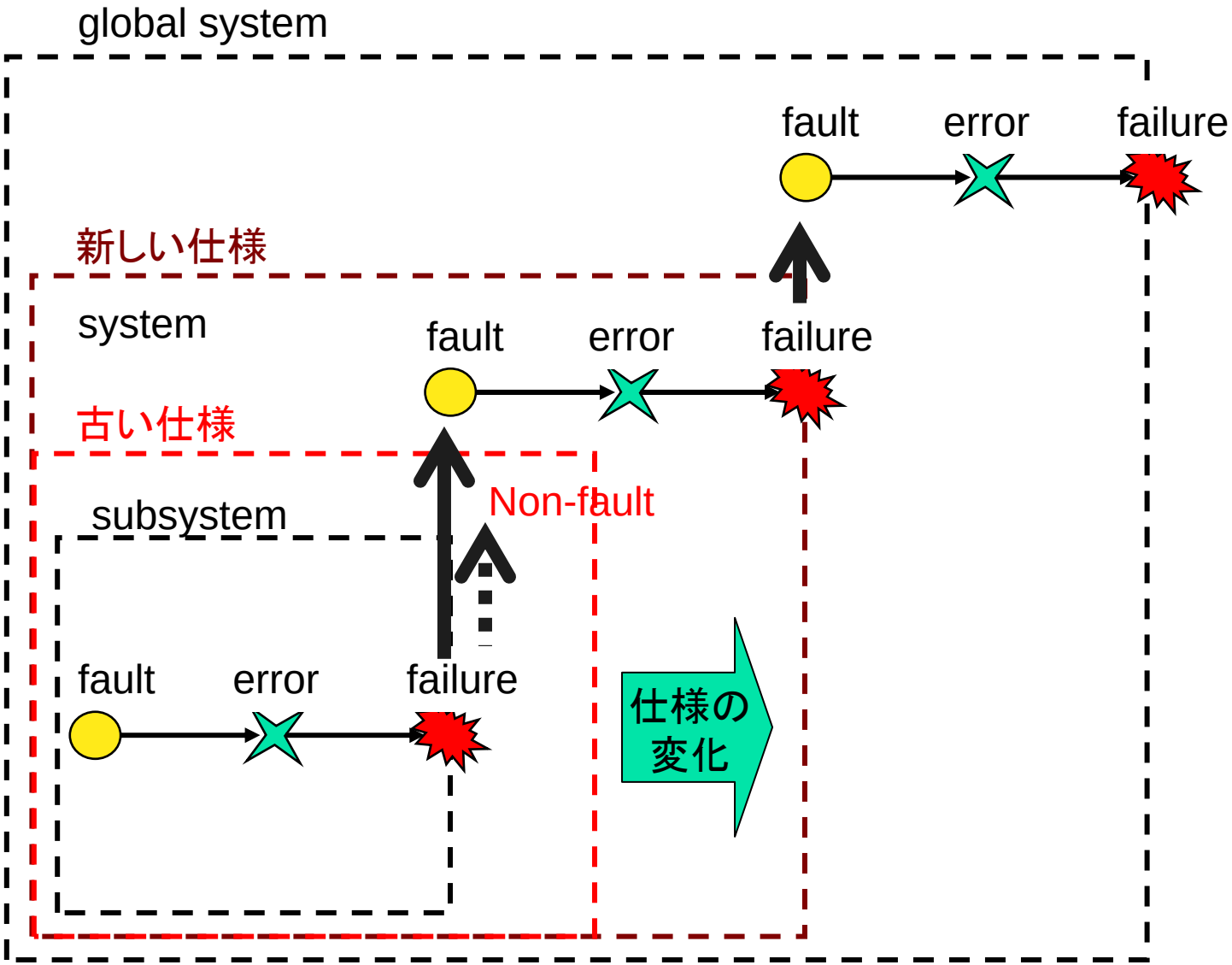
Modern Fault Model:階層の透過



Modern Fault Model:相互作用



Modern Fault Model:仕様の変更



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）

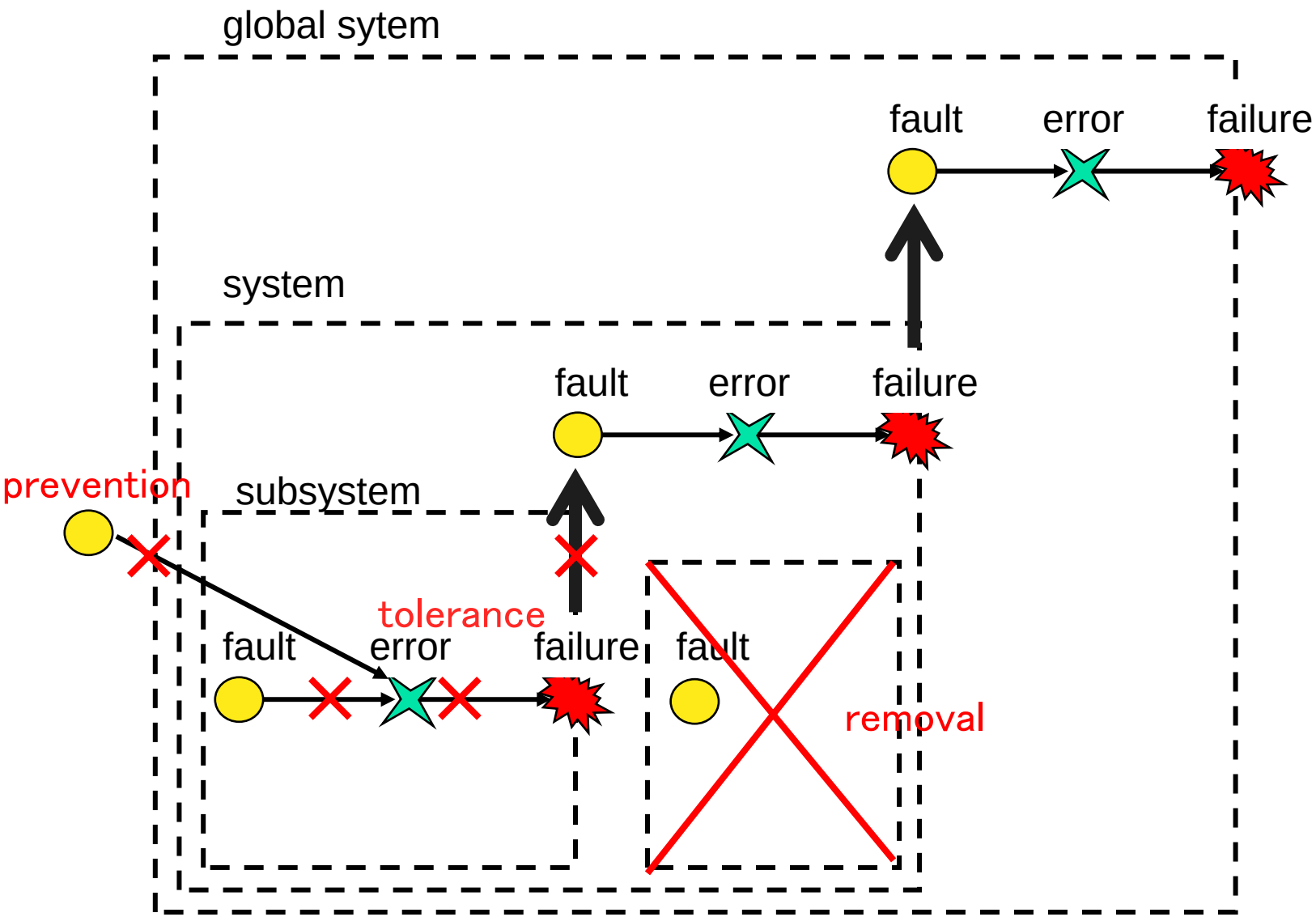
	自然現象	人的ミス	人的攻撃
企画		仕様不備 交換時への配慮不足	企画の盗難
設計		設計ミス、バグ 利用環境の想定ミス	設計の盗難 不正回路挿入
製造	製造ばらつき	製造ミス	違法な生産による横流し
検査	間欠故障	見逃し	良品横流し
流通	運搬・保存中の環境変化	運搬等の事故	盗難、横流し
運用	経年変化 宇宙線・環境	利用事故	Phishing、virus 盗聴、不正利用
廃棄・更新		更新時不整合	情報抜取・解析

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

ディペンダビリティの実現手段

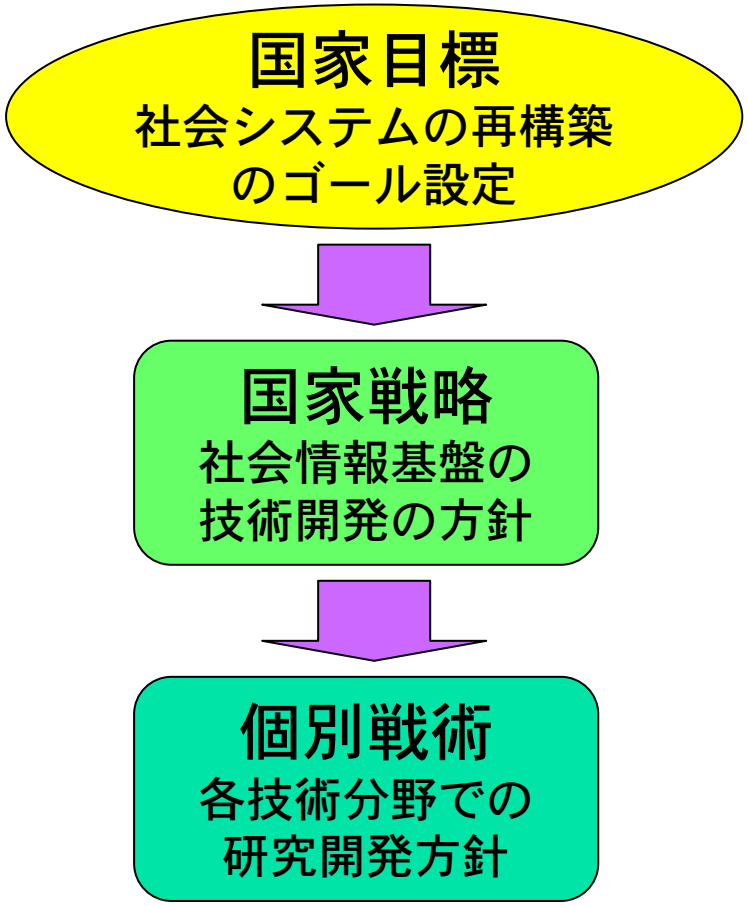


何故Dependabilityか？

- 社会システムが急速に発達した情報技術に大きく依存するようになり、社会システム自身の再構築が必要となっている。
- Openなシステムが世界規模で実用化され、Closed Loopを前提としたシステム開発手法が適用できず、新たな工学手法が必要である。
- 技術の微細化・高速化・高集積化による種々の物理的限界、システム複雑化や相互接続による設計ミスや運用時のエラー、悪意ある攻撃者による各種の攻撃などによってシステムの安全性・信頼性・安定性などが脅かされている。
- さらに、システムのオープン化により従来の意味での「仕様（製品と社会の契約）」が定義できなくなった。
- 上記の各種のFault（人間のエラーや攻撃を含む）は不可避なので、その存在を前提として安全で安心な社会システム構築のための技術開発が必要である。
- Commodity部品により構築される社会システムの信頼性や安全性が危惧されている。
- ユーザ・製造者・設計者・運用者・許認可権者の責任の明確化も重要である 。
- このような状況で、安全・安心を保証するための新しい指導原理と技術が必要となっている。

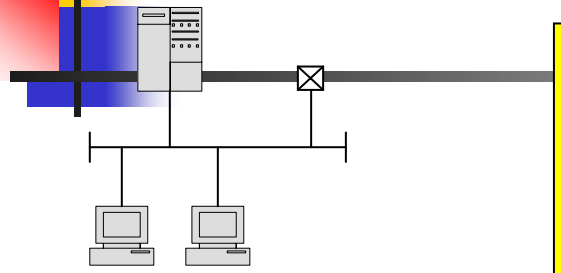
何が求められているのか？

- 新しい情報技術と方法論
  - 社会や個人がDependableな社会情報基盤の構築手法とその要素技術
  - 社会制度や規則と連携した社会システムの再構築への技術側からの参画
- 社会システムの再構築を担う人材の育成



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

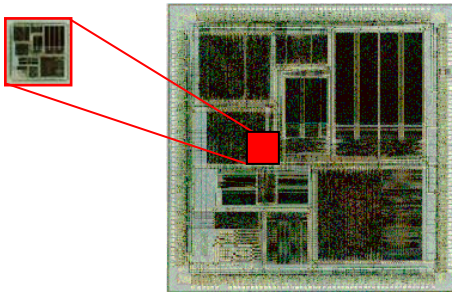
デバイスレベル

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

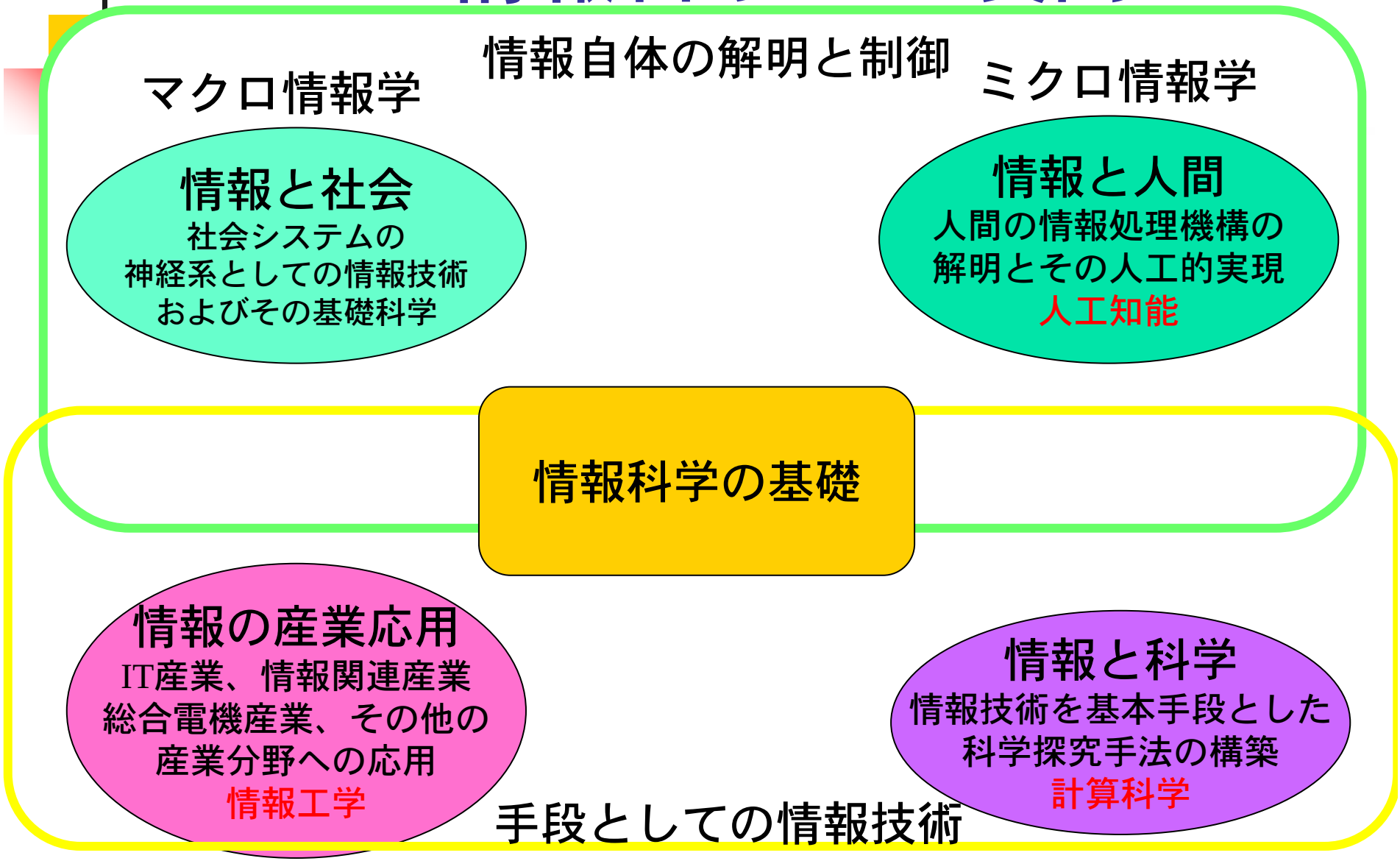


電子経済時代の通貨・徴税の仕組みの構築

電子的通貨基盤の構築の意味

- 国家の基盤である通貨・徴税システムの電子化の基礎技術の構築
- 匿名性を維持した現行決済システムの継続によるプライバシー保護
- 「価値」を載せられる「安全なシリコン技術」による各種応用分野での競争力の確立
- 経済システム基盤技術の世界への供給による国家的安全保障
- 世界的な標準化・技術競争に対する指導的立場の確立

マクロ情報科学への展開



「価値」と「信用」を取り扱う情報技術に向けて

- ミクロ的視点の情報科学から社会全体を把握し、社会情報基盤を設計するマクロ的情報科学へ
- 情報科学と社会科学の新しい融合による社会基盤システムの設計問題
  - 社会SystemのModel化
  - DependableなSystem構築の技術
  - Quality, Reliability, Securityを対象とした理論
- 次世代の国家及び社会の基盤の方向を情報技術の立場から発信する事業の展開
  - 大学キャンパスを実験場へ
  - 実証の中からの思想と技術の創成