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

新キャンパスにおける未来型情報経済インフラの実験

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

https://hdl.handle.net/2324/9124

出版情報：SLRC プレゼンテーション, 2006-02-15. 九州大学システムLSI研究センター
バージョン：
権利関係：

新キャンパスにおける
未来型情報経済インフラの実験

九州大学システムLSI研究センター

安浦　寛人

背景

21世紀COEプログラム
社会基盤としての情報技術

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

システムＬＳＩを核にした社会基盤システム構築を通して *i and e* の理念の実現

情報通信技術
•衛星通信（立居場光生）
•モバイル通信（赤岩芳彦）
•インターネット（荒木啓二郎）
•回路網理論（香田徹）

情報科学
•発見科学(有川節夫・竹田正幸・正代隆義)
•認知科学（志堂寺和則）
•マルチエージェントシステム（雨宮真人）
•画像データベース（牧之内顕文）

情報・通信基盤技術プロジェクト

デジタルシステム設計
•システムLSI設計（安浦寛人・村上和彰）
•セキュリティー技術（櫻井幸一）
•組込みソフトウェア（福田晃）

回路設計とデバイス技術
•RF回路設計（吉田啓二）
•ナノ集積化加工技術（白谷正治・興雄二）
•システムインディスプレイ（宮尾正信）
•味・においセンサー（都甲潔）

システムLSIプロジェクト

システム情報科学での社会基盤システム形成

電気電子システムプロジェクト

電子デバイス
•高感度SQUID （園福敬二）
•超伝導電力機器（船木和夫・原雅則）

電気システム
•スイッチング電源（二宮保）
•インテリジェントロボット（長谷川勉）

光エレクトロニクス
•次世代リソグラフィ光源（岡田龍雄）

研究プロジェクト体制

実践プロジェクト

遠隔教育・研究基盤構築
荒木、有川、立居場

全学共通ICカード導入
安浦、有川、櫻井、村上、吉田

システムLSI関連プロジェクト

SLRC

システムLSI研究センター
九州大学戦略的教育研究拠点（時限教員ポスト）
教員3名増員　H17-22
CREST:低消費エネルギーシステムLSI（名大と共同研究）

科学技術振興調整費
新興分野人材養成
「システムLSI設計人材
養成実践プログラム」
3億円、教員4名増員
H17-21

21世紀COEプログラム
システムLSIアーキテクチャ
組み込みソフトウェア開発技術
低消費エネルギー化設計手法
無線通信用CMOS回路技術
セキュリティ技術
味・においセンサー
微細加工技術・新材料
システムLSIを用いた社会基盤システム
6億円　H14-18

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
3.4億円　H14-18

シリコンシーベルト福岡
＊福岡システムLSI総合開発
センタービル（30億円）
＊知的クラスタ創成事業
＊システムＬＳＩカレッジ
総額100億円
H13-

知的クラスタ創成事業
H14-18
総額25億円
研究者20名雇用
６つのプロジェクト

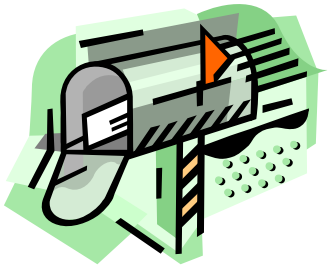
**全学共通ICカード
導入プロジェクト**
H15-18
経済産業省実証実験
8000万円　H17

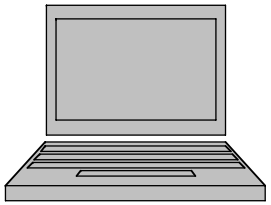
システムLSI
リサーチコア

次世代スーパーコンピュータ

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。





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（基幹システムと組込みシステム）
- 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（社会の神経系）

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
  - 距離の克服ー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
  - 必要ならば社会のルールを変更する必要がある

◆ **情報技術を前提とした社会システムの再構築の必要性**

◆ **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」の媒体となりえるか？**

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
- 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

認証基盤の確立

IDシステムの構築

MIIDシステムとQUPID

現在の認証基盤

- 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
  - ログインID、電子商取引など新しい形態
- 一方向認証が主流（相互認証でない）
- 偽造や詐欺の脅威
- 電子化・デジタル化による新しい問題
- 仕組みや原理の複雑さ

現在の認証基盤の問題点

SLRC

利用者

- 複数のサービスを利用する際、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
- マルチサービスにおいては、利用履歴などのトレースが懸念される
- パスワードなど記憶しておく事項が多い
- 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

- 発行者の役割を兼務することが多く、管理コストがかかる
- 個人情報を集めるとそれの管理コストがかかる
- 新たな認証デバイスを用いてサービスを行おうとすると、認証の仕組みまで自前で用意する必要がある
- 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
- 個人に対してIDが付与されており、個人単位での管理しかできない
- マルチサービスにおいては、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
- 個人に対してIDが付与されるため複雑な権利・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

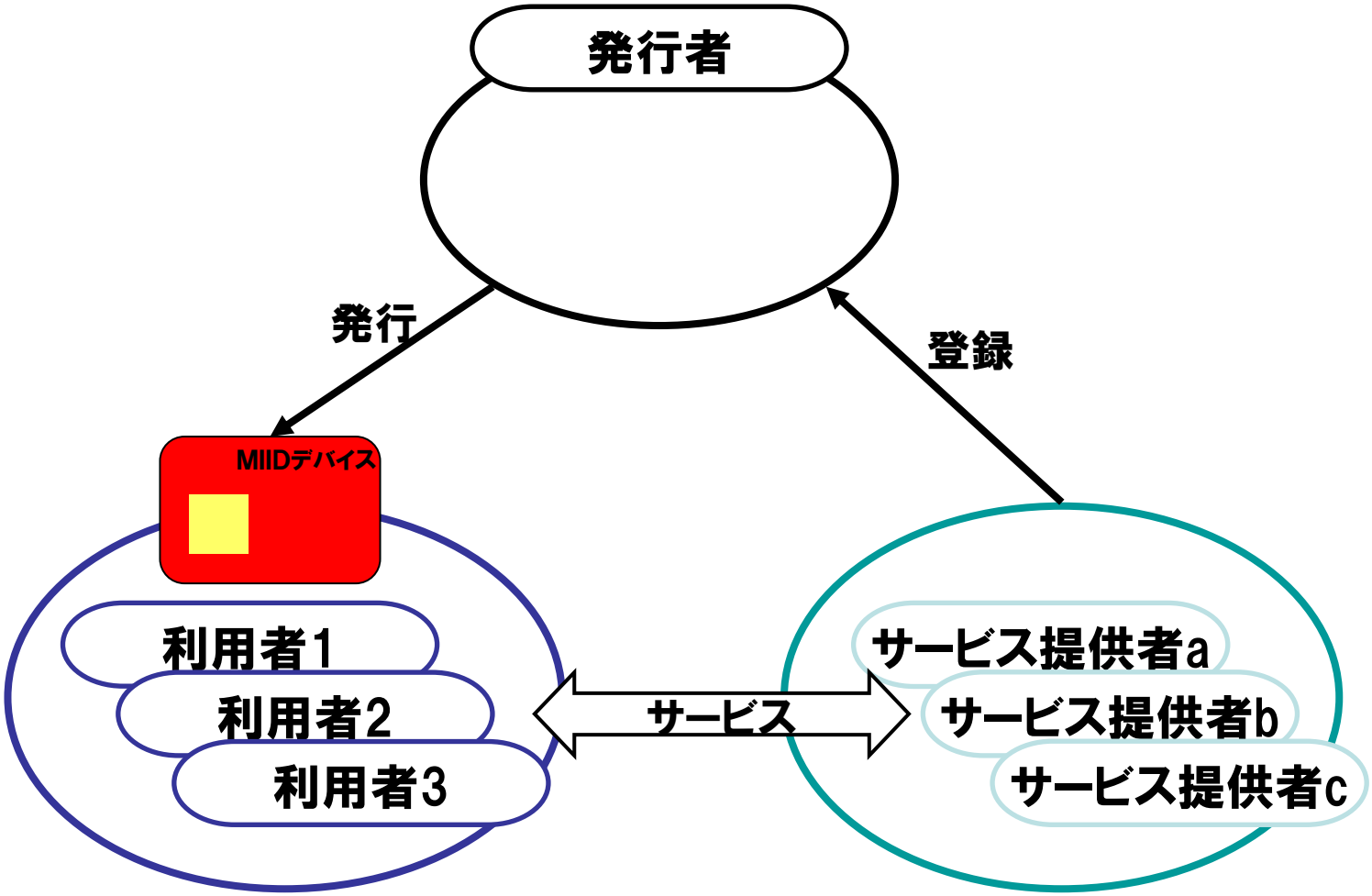
相互認証や複雑な認証要求に対応する機能を搭載

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管理システム

MIID管理システムの3者モデル



MIID管理システム

MIID管理システムの特徴１～メディアに依存しない～

今まで

データフォーマットの異なる多くの種類の認証デバイス（カードや携帯電話など）が出回り、互換性に乏しい

◆データフォーマットを統一し、TypeBカード、FeliCaカード、FeliCa携帯など多くのメディアでのサービス利用を可能に
◆IDシステムを技術変革の早いデバイスから分離

今まで

サービス提供者が新たなメディアに対してサービス提供をするためには大きな投資が必要であった

◆共通の認証基盤を構築することで、サービス提供者がMIIDシステムを利用することが容易に
◆発行者システムおよびサービス提供者の利用する共通基盤システムを共有化
◆サービス提供者は従来のシステムに簡単に接続可能

MIID管理システム

MIID管理システムの特徴2～サービス毎に異なるID～

ひとつのIDで複数のサービスを利用するため、サービスごとに独立した管理・運用が難しい

◆利用するサービス毎に異なるIDを利用するため、個々のサービスごとに独立したポリシーでの運用が可能
◆発行者による個人の確認と個々のサービスによる認証は独立であるので、サービス間の連携・協調が柔軟に実現可能

ひとつのIDで複数のサービスを利用するため、ひとつのサービスでIDが漏洩した場合、被害が広範囲に及ぶ

◆利用するサービス毎に異なるIDを利用するため、ひとつのサービスにおいて問題が起こっても他のサービスには影響がない

個人に対してIDを付与していたため、複雑な権利・権限管理が困難

◆役職や所属など複数の属性に対してIDを付与することができ、複雑な権利・権限管理が可能

MIID管理システム

MIID管理システムの特徴3～相互認証などの柔軟な認証方式～

今まで

現在、ネットワークを介さないサービスはほとんどが片方向認証によって提供されている。偽ATMなど新たな危険に対する対応が必要。

◆銀行ATMなど双方向認証の必要があるサービス場合には相互認証を選択的に導入可能
◆一般の利用者にも分かりやすい相互認証のしくみを提供

今まで

ひとつのIDで複数のサービスを受ける際、どのサービスに対しても同様の認証を行っていた

◆基本的な認証機能の上に本人確認(生体認証など)や高度な認証方式を組み合わせることができ、セキュリティレベルに応じた認証方法の実現が可能

MIID管理システム

MIID管理システムの特徴4～Unlinkabilityとリスク対応～

今まで

サービス提供者は個人情報を持つことにより常に情報漏洩リスクを抱えている

◆基本的な個人情報は発行者が保持し、サービスは必要最低限の個人情報のみを持つので、情報漏洩リスクを下げられる
◆複数のサービスが連携するときに、それぞれの持つ個人情報を交換する必要がなく、情報の漏洩無しにサービスの連携・融合が可能

今まで

同一のIDで複数のサービスを受けるため、利用情報のトレースが可能

◆サービス毎に異なるIDを利用するため、サービス提供者同士が結託しても利用者のリンクが不可能

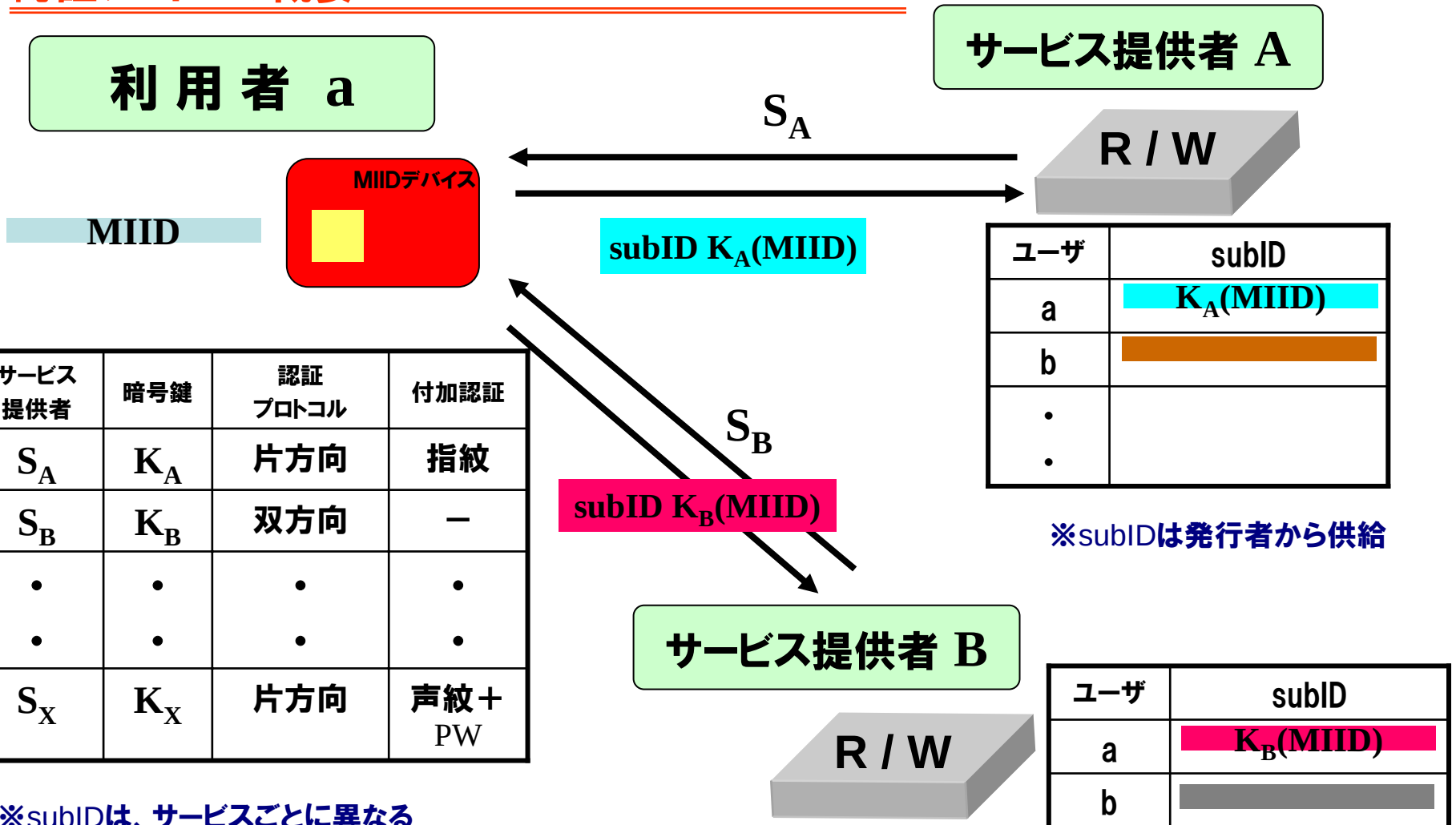
MIID管理システム

各プレーヤーのメリット・デメリット

	利用者	サービス提供者	発行者
メリット	•一つのデバイスで複数のサービスを受けることができ、何枚ものカードなどを持つ必要がない •複数のサービスを統一された手続きで利用可能 •個人情報変更や紛失の際の連絡は発行者に対してのみ行えばよい •個人情報の漏洩リスクが少ない •サービス毎に異なるIDを利用するので、情報がトレースされない •原理が単純で理解しやすい	•不要な個人情報を持つ必要がなく、情報漏洩リスクが低い •提供するサービスに必要な安全性に合った認証プロトコルでサービスを提供可能 •異なるサービスと簡単に連携が可能 •事故時の影響が他のサービスに波及しにくい •導入のコストが低い	•情報の一元管理により柔軟で安全な管理が可能 •複雑な権利・権限管理が可能 •事故時には被害の限定と低コストの回復が可能
デメリット	•MIIDデバイスを紛失した場合の被害が甚大	•顧客の囲い込みにおいて、従来の方法とは異なる手法が必要	•すべての情報を管理するため責任が重大で、大きな信頼が必要 •発行者に問題が発生した場合、問題は全体へ波及する

MIID管理システム

認証プロトコル概要



ユーザ	subID
a	K_A(MIID)
b	
・ ・	

※subIDは発行者から供給

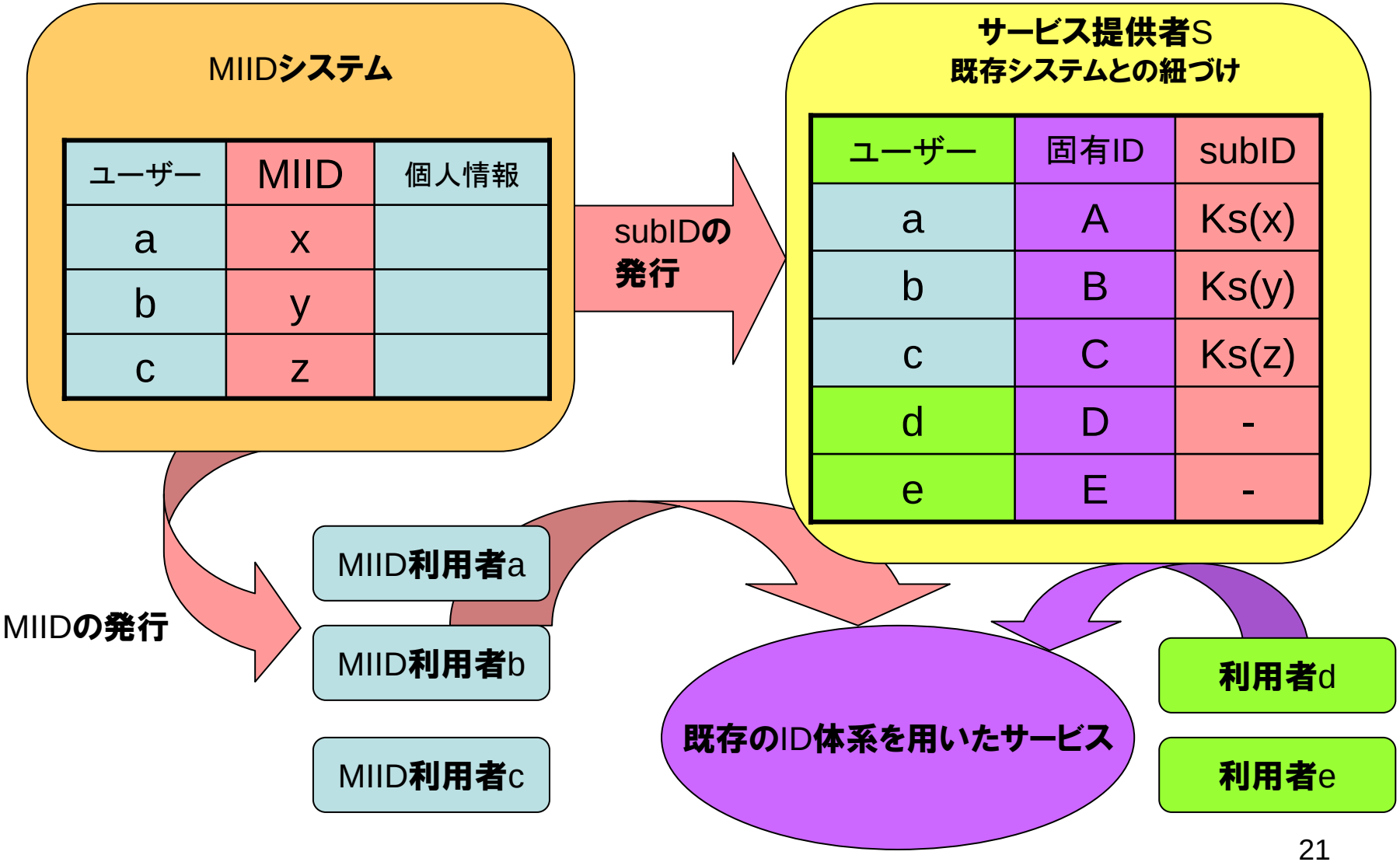
サービス提供者	暗号鍵	認証プロトコル	付加認証
S_A	K_A	片方向	指紋
S_B	K_B	双方向	―
・ ・	・ ・	・ ・	・ ・
S_X	K_X	片方向	声紋＋ PW

ユーザ	subID
a	K_B(MIID)
b	
・ ・	

※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

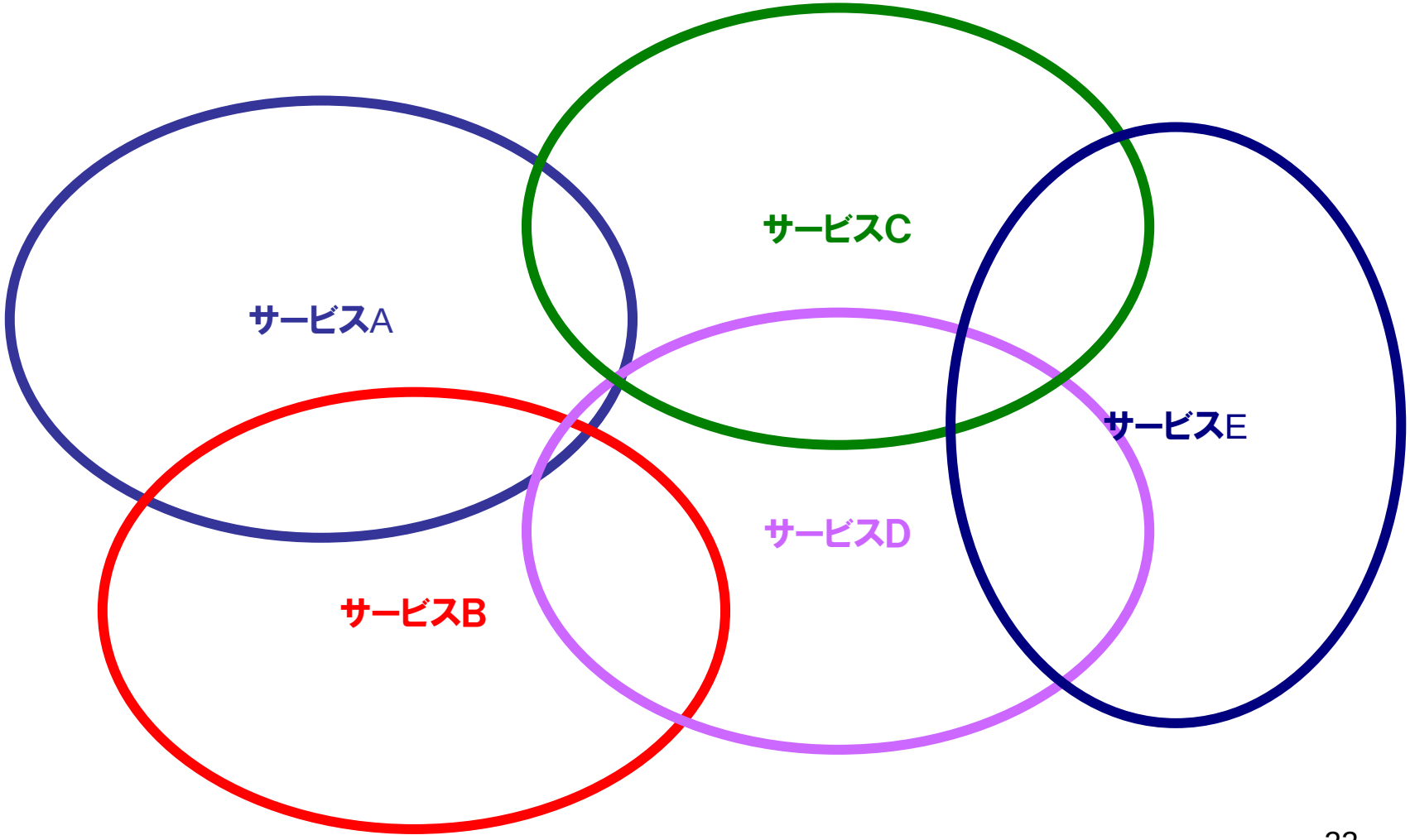
MIID管理システム

既存のID管理システムとの結合



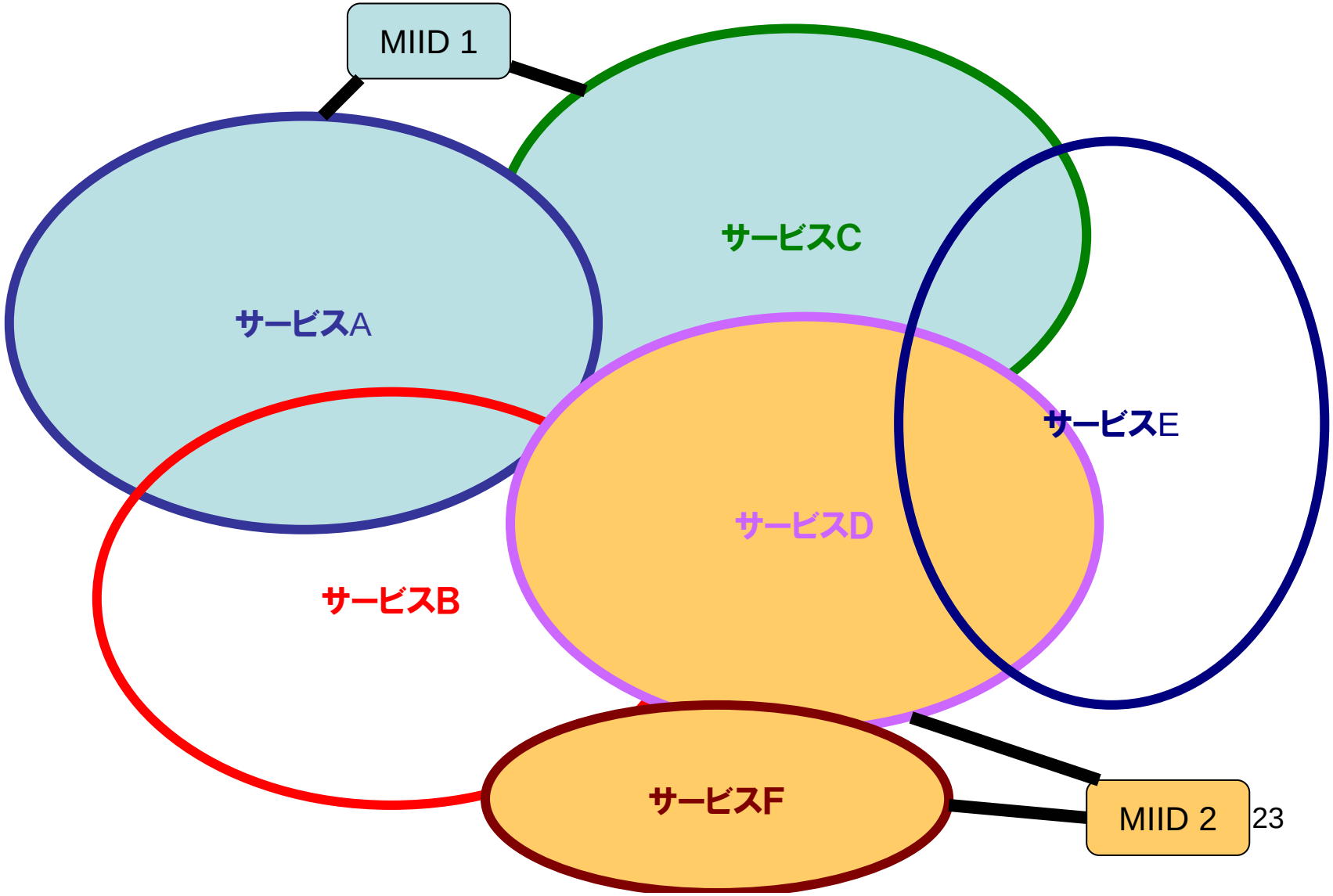
MIID管理システム

MIIDシステムの拡大（個々のIDシステムの混在（現状））



MIID管理システム

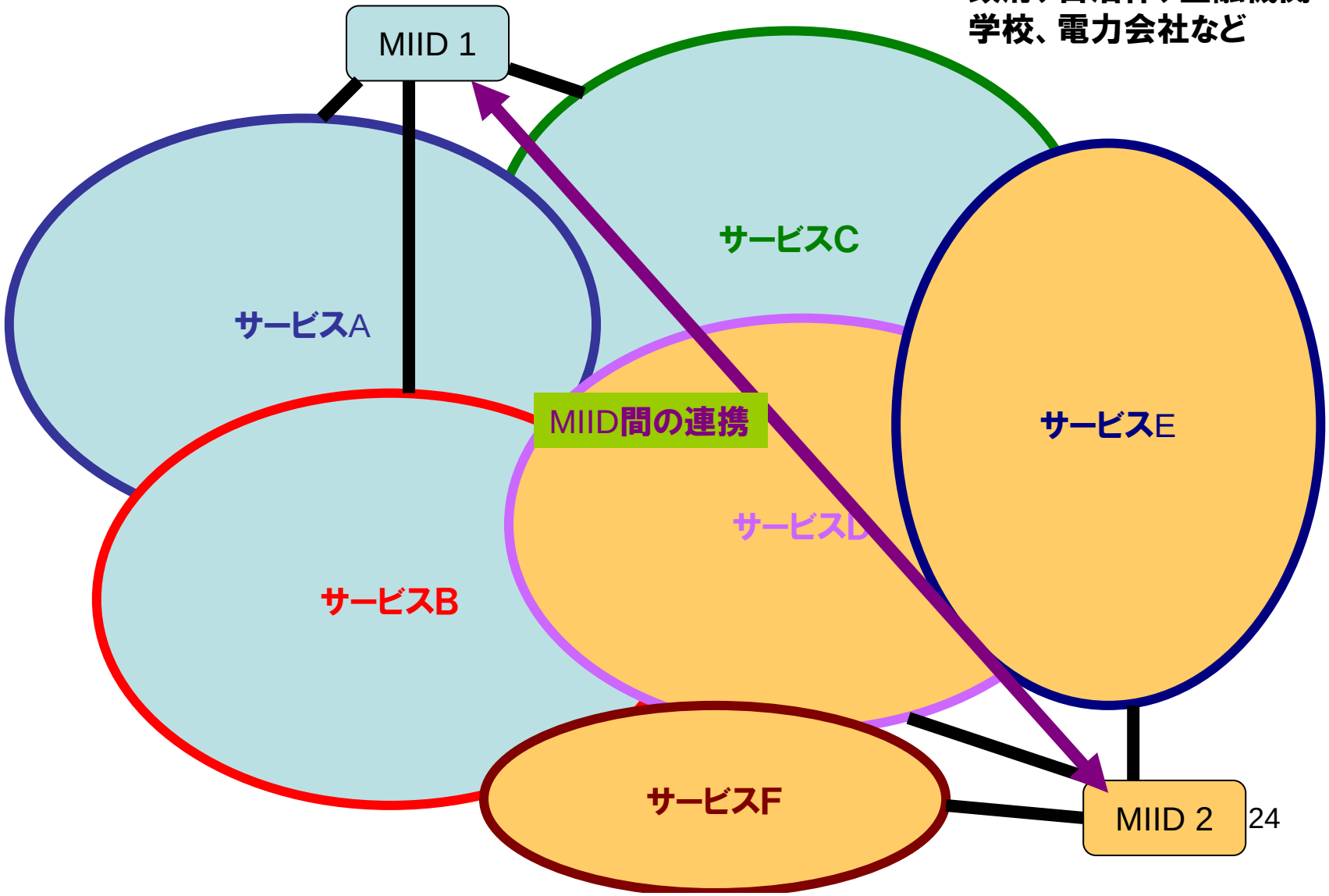
MIIDシステムの拡大（小さなMIID連合の形成期）



MIID管理システム

MIIDシステムの拡大（大規模MIIDへの集約期）

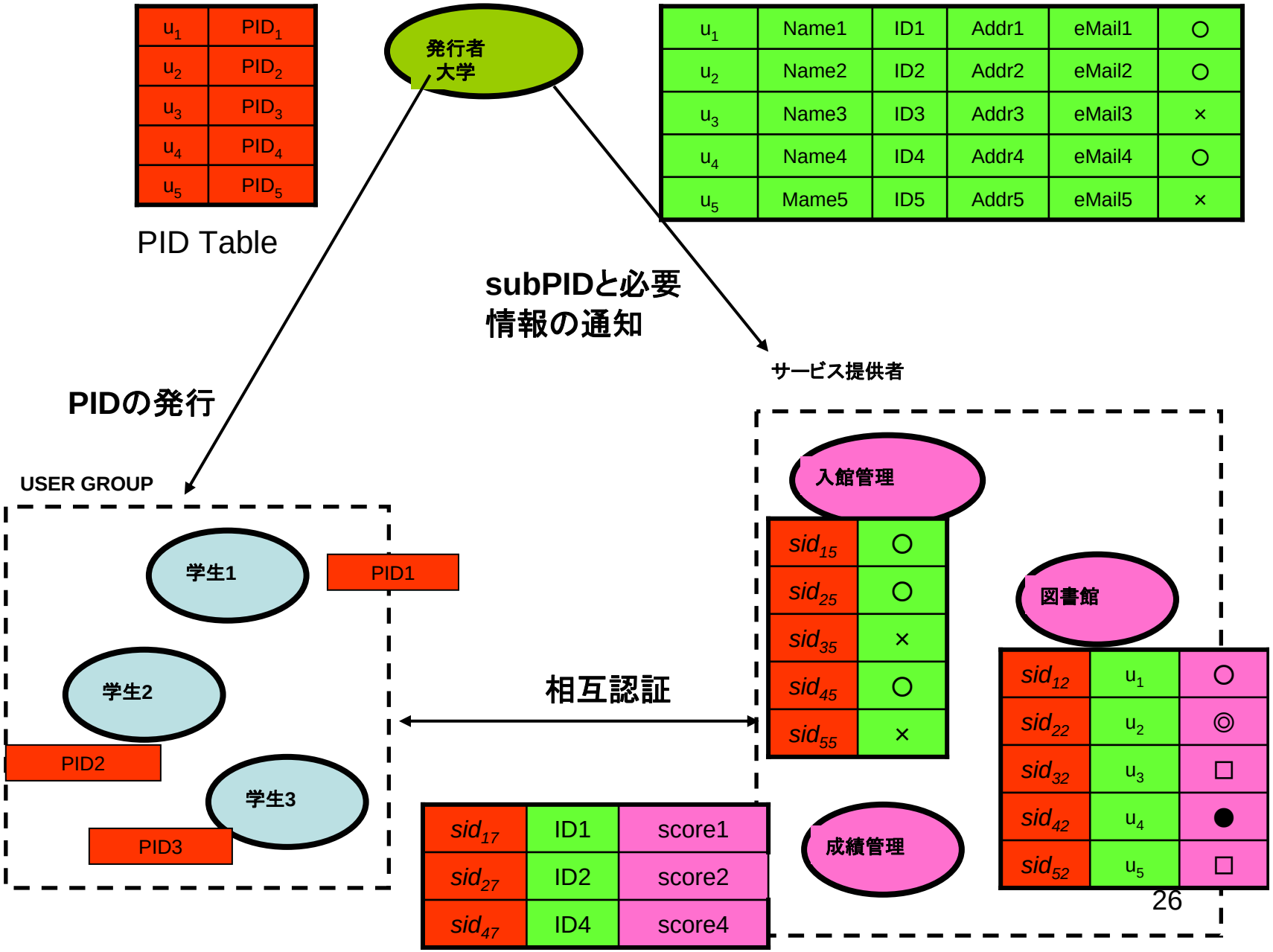
MIID発行者の集約
社会的な信用のある機関
政府、自治体、金融機関
学校、電力会社など



九州大学全学共通ICカード
QUPID：(Q-shu Univ. Personal ID)

- MIIDの九州大学学生証・職員証での実現
- 平成18年7月までに実現予定のサービス
- 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書（券面印刷／写真）
  - 電子的に確認が可能な証明書
- 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

個人に関する情報の分散管理



実証実験プロジェクト

情報家電等のネットワーク化技術の相互運用性及び有効性に関する実証実験事業

全体概要

採択事業名

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
「情報家電等のネットワーク化技術の相互運用性及び有効性に関する実証実験事業」

申請者

（代表者）　国立大学法人　九州大学　総長　梶山　千里
（プロジェクトリーダー）国立大学法人　九州大学　副学長　有川　節夫
（プロジェクトマネージャー）九州大学システムLSI研究センター　センター長　安浦　寛人

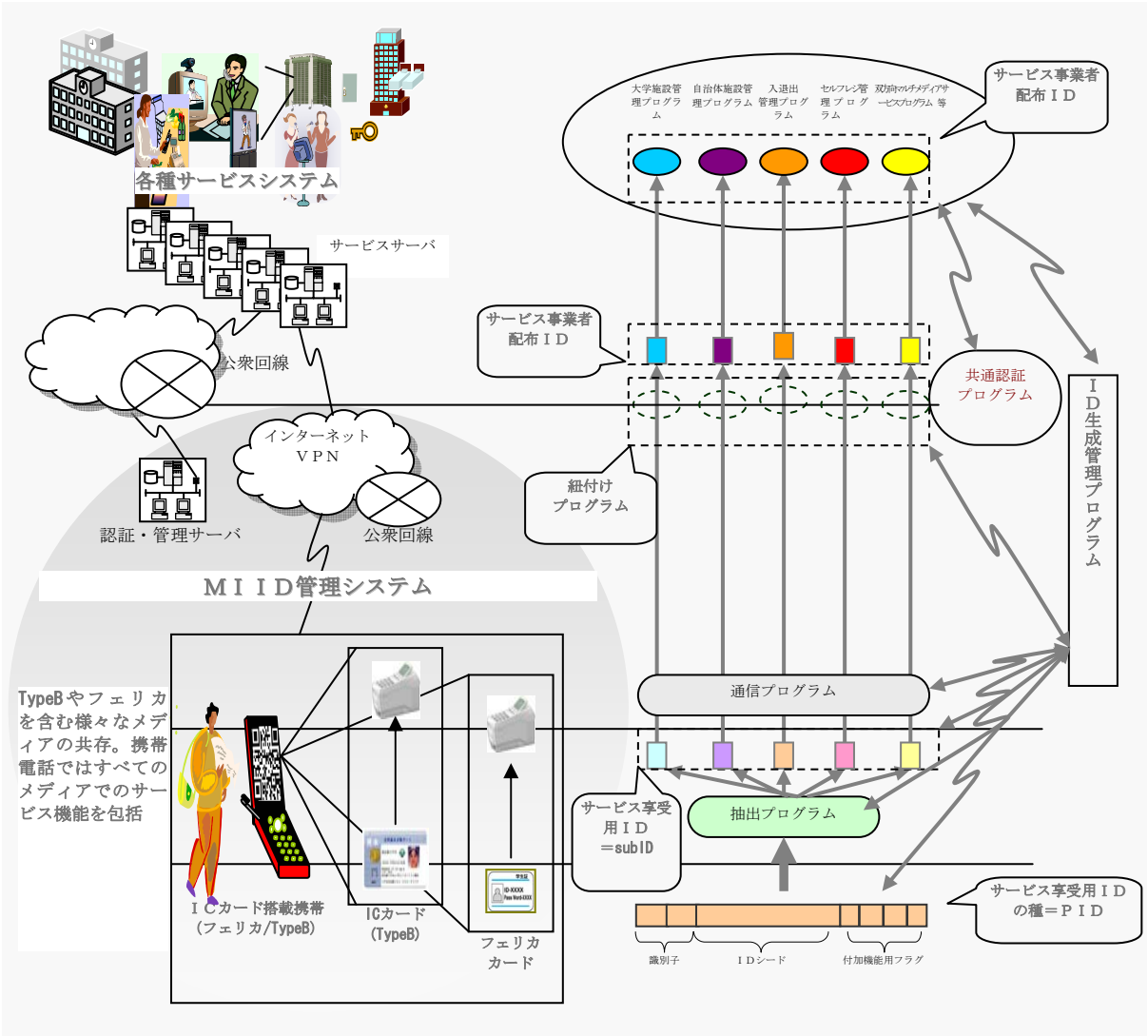
事業概要

情報家電ネットワーク化時代における、ネットワーク上でサービスを実施する事業者の競争力強化と消費者の安全性・利便性向上ならびに負担軽減のための施策立案用情報収集を主目的とするものである。
事業では、九州大学の新キャンパス及び周辺地域に、今後活用が見込まれる新技術を盛り込んだ情報通信ネットワークを施設し、そのネットワーク上にITとサービス融合のための必要な共通情報基盤を構築、そこにおいて実際に様々なサービス提供実験を行うことにより、新技術の有効性と共通情報基盤の装備すべき機能・能力について検証を行う。

共通情報基盤・・・九州大学発の、ICカード・携帯電話等のメディアの違いを吸収して共存を可能とするID管理技術であるMIID（Media Independent ID）管理システムが稼動するインフラ。

核となる技術～Media Independent ID(MIID)管理システム～

MIID管理システムの基本構造



ID照合・認証が完了したら
サービス開始

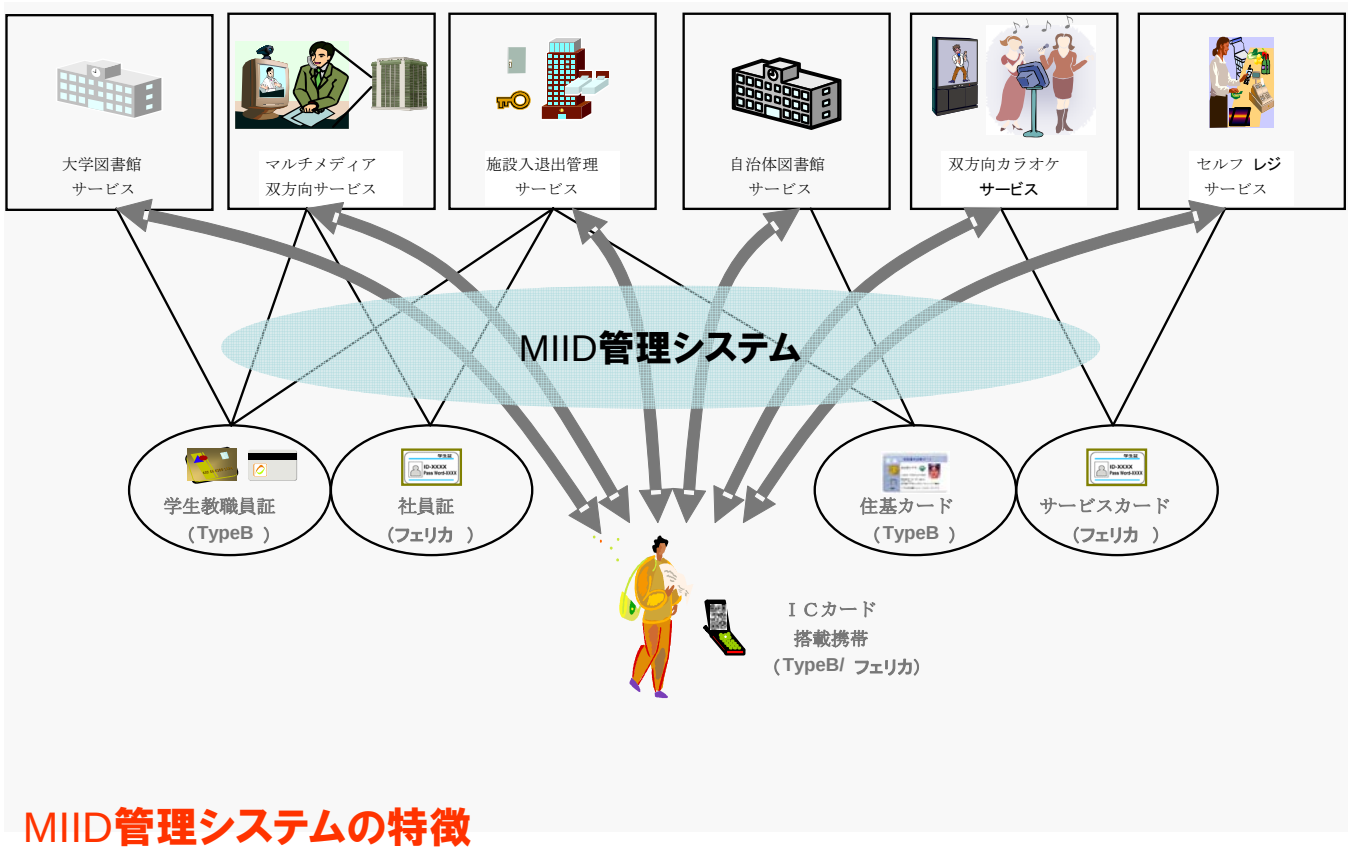
紐付けプログラムによりサービス業者
独自の利用者IDとsubIDを対応付け

抽出プログラムにより、サービス毎の
subIDを動的に生成

利用者は発行者に個人登録。
発行者より各利用者へPIDを発行。

MIID管理システムの利用イメージと特徴

MIID管理システムの利用イメージ



会員制・非会員制に関わらず既存ビジネスを展開しているサービス業者に接続可能

相互認証による高いセキュリティを実現。また、サービス毎のセキュリティ強度設定も可能

カードのタイプ、媒体の違いをMIID管理システムにより統合化。一つの媒体で全てのサービスが利用可能

MIID管理システムの特徴

①独立性・・・サービス毎にsubIDを割り当てることによるID体系の独立化→ID漏洩被害の最小化
②安全性・・・サービス毎に認証方法やID長を変更することが可能→サービス内容に適した安全対策を提供
③共通性・・・メディアに依存しないことによる利用シーンの共通化→利用者の利便性向上
④接続性・・・既存サービスは自社のサービス体系をほとんど崩すことなく対応可能→事業者の負担軽減と個人情報免除
⑤匿名性・・・サービス事業者と利用者の間はsubIDによる結びつきのみ→利用者の匿名性を維持した上でのサービスが成立

今年度事業概要

今年度の事業スキームと体制

実験の検証と将来に向けた提案WG

今年度開発する基盤システムの検証や、それを活用した新しいビジネスモデルの創出等7つの検討項目を設置し、それぞれWGを行う。

サービス実証実験

MIID管理システム上でのサービス提供実験。①複数の管理システム融合実験 ②複数の権利権限の効果的管理実験 ③非対面型サービス付加価値実験 ④対面型サービス無人化支援実験(リアル、バーチャル)

MIID管理システム実証実験

MIID管理システムの構築と検証。メディア非依存性の検証と、利用者は匿名性を維持しながらサービスを享受でき、サービス事業者は個人情報保護を意識しつつも、余分な顧客情報を保有しないで顧客を囲い込むことができるかの検証を行う。

ネットワーク新技術有効性実験

情報家電をネットワーク化する有力技術であるPLC(Power Line Communication)技術の有効性実験を行う。

今年度事業規模

- 九州大学新キャンパス等の九大キャンパス内、およびその周辺地域が対象
- 九州大学の学生・教職員、福岡市・前原市の一般モニターで構成される2,000人以上の実験対象者

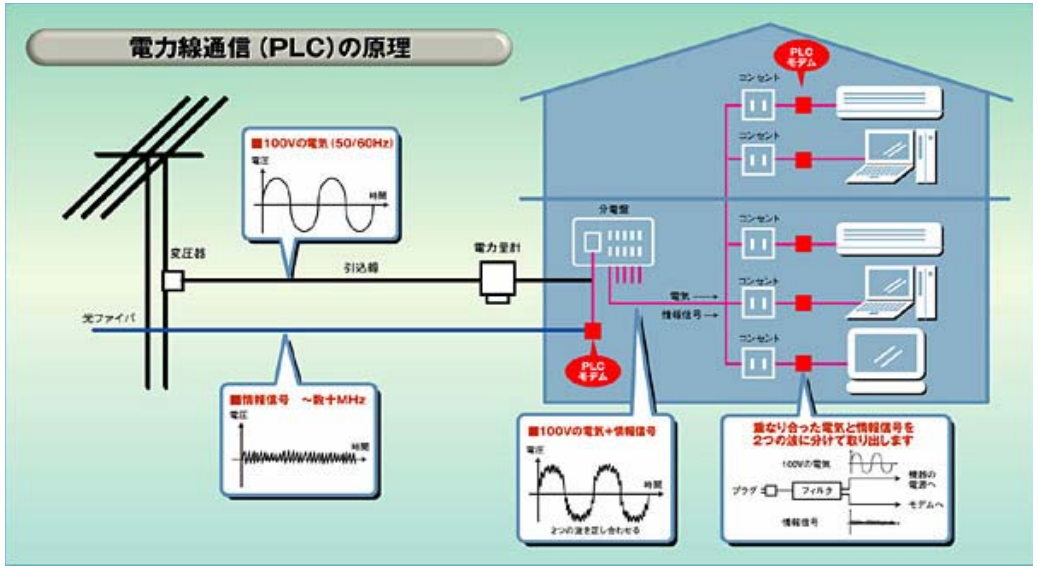
ネットワーク新技術有効性実験

PLC（Power Line Carrier Communication＝電力線搬送通信）実験

次世代ネットワークインフラとして活用が見込まれる新技術としてPLCに着目。現在の法律で可能な範囲の電力・通信混合実験はPLC実験ネットワーク環境で行い、不可能な範囲実験は、実験通信ネットワーク環境で実施する。
（大学としては日本で初めて高周波設備許可申請を申請中）

PLCとは・・（高速電力線通信協議会資料より）
電力線通信とは、100V（50/60Hz）の電力線に高周波信号を重畳し、電力線を伝送路として双方向の通信を行う方式であり、以下のような利点がある。

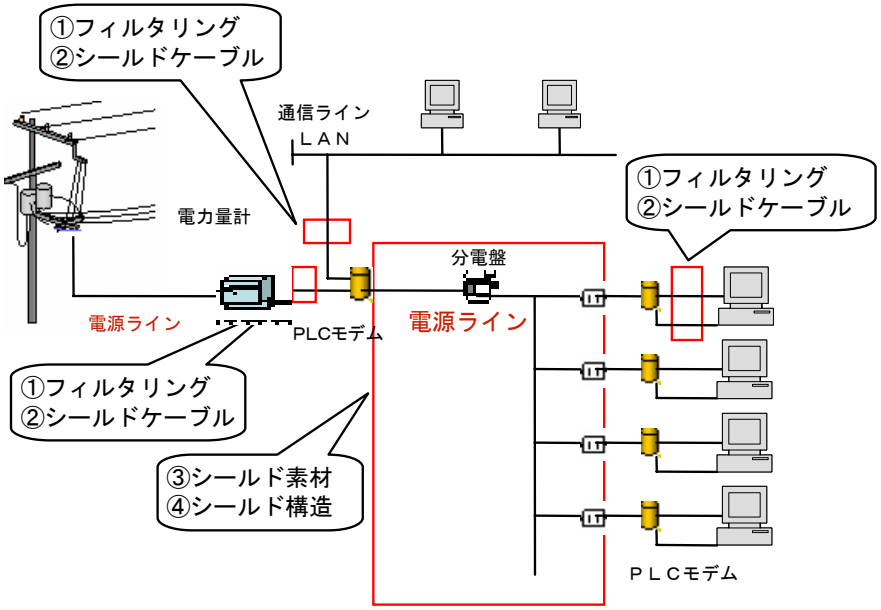
・既存の電灯引込線・コンセントがそのまま利用できるので、新規の配線工事が不要　→　経済的
・プラグをコンセントに差し込むだけで接続でき、すぐに利用可能　→　プラグ&プレイ
・各家庭内の各部屋間でホームネットワークの構築が可能　→　どこでも使える



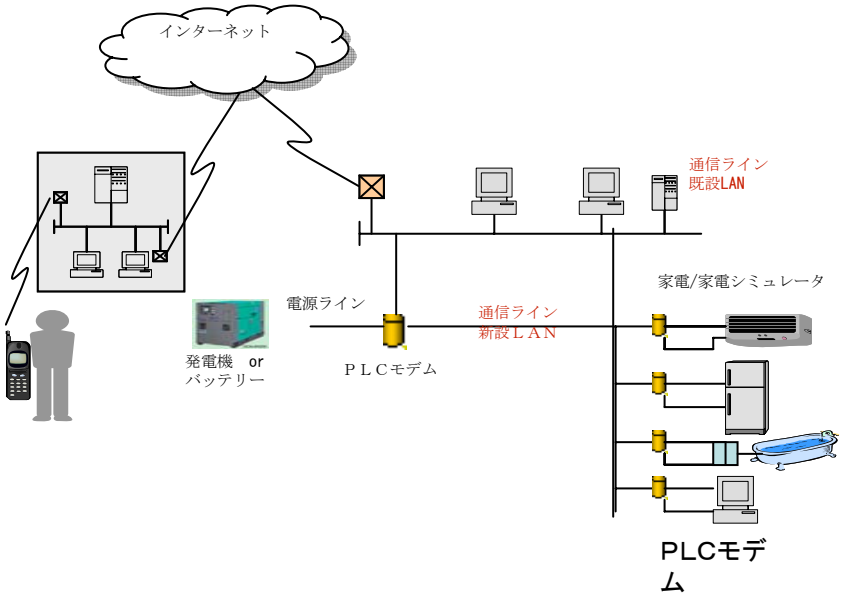
ネットワーク新技術有効性実験

PLC実験概要

①電源ラインにおける通信・電力混合及び輻射低減実験



②通信ラインにおける通信・電力混合及びアプリケーション実験

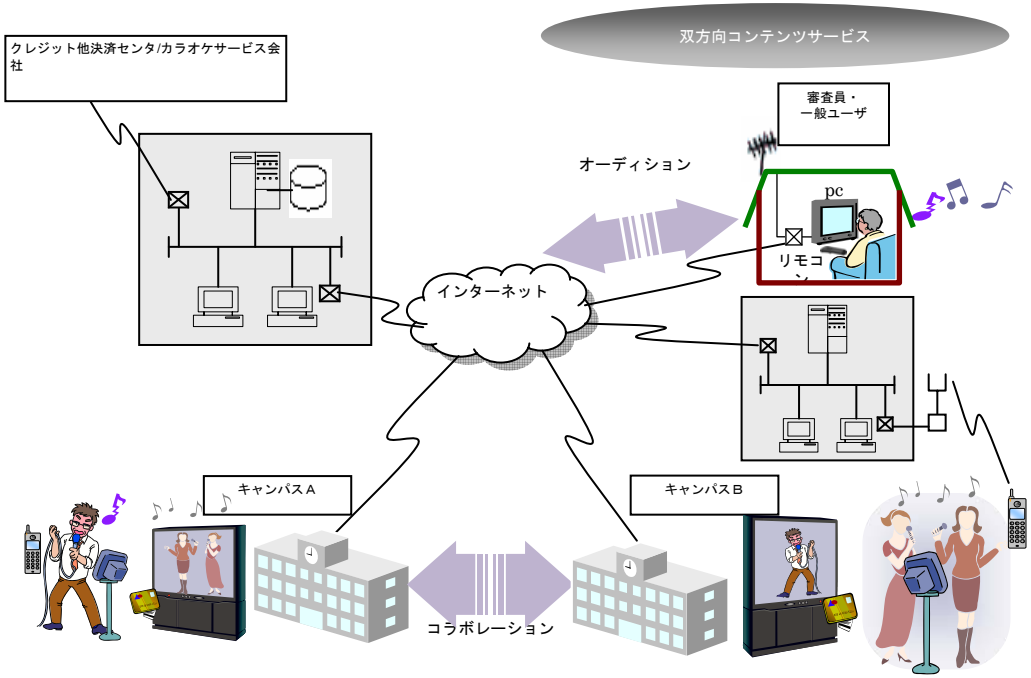


【実験概要】
新キャンパス内にPLCの実験環境を構築。
そこにおいて通信方法の他、ハードウェアによるフィルタリング、
電力線の素材・被服方法、引き回し方法、電飾線が配置される
周辺環境(壁等)の構造・素材等による総合大学ならではの、
総合力を活かした輻射低減対策実験を実施する。

【実験概要】新キャンパス内に電力を流すことが可能な特殊な
通信環境を構築、そこにおいて、情報家電の制御、
マルチメディアコミュニケーションを想定したアプリケーションを動作させ、
環境条件を変化させることで問題点や課題を明らかにし、
それに対する対策を立てる。

サービス実証実験例

非対面型サービス付加価値実験～マルチメディアコンテンツ提供サービス～

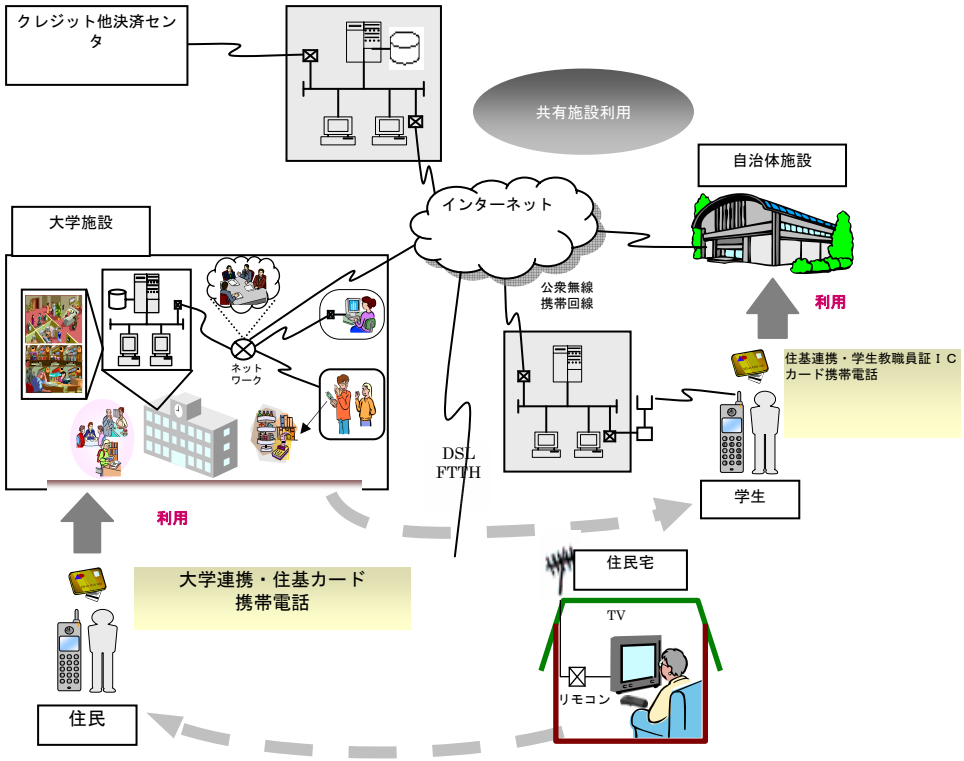


MIID管理システムと、セガが提供するネットワークカラオケサービスを結合する実験。

【検証項目】
非対面の双方向コンテンツビジネスのあるべき姿模策
・双方向配信管理
・個人情報の保護とサービス付加価値化
・サービス課金のあり方

サービス実証実験例

異なるメディアを用いた管理システムの融合実験～大学・自治体の施設サービス融合～

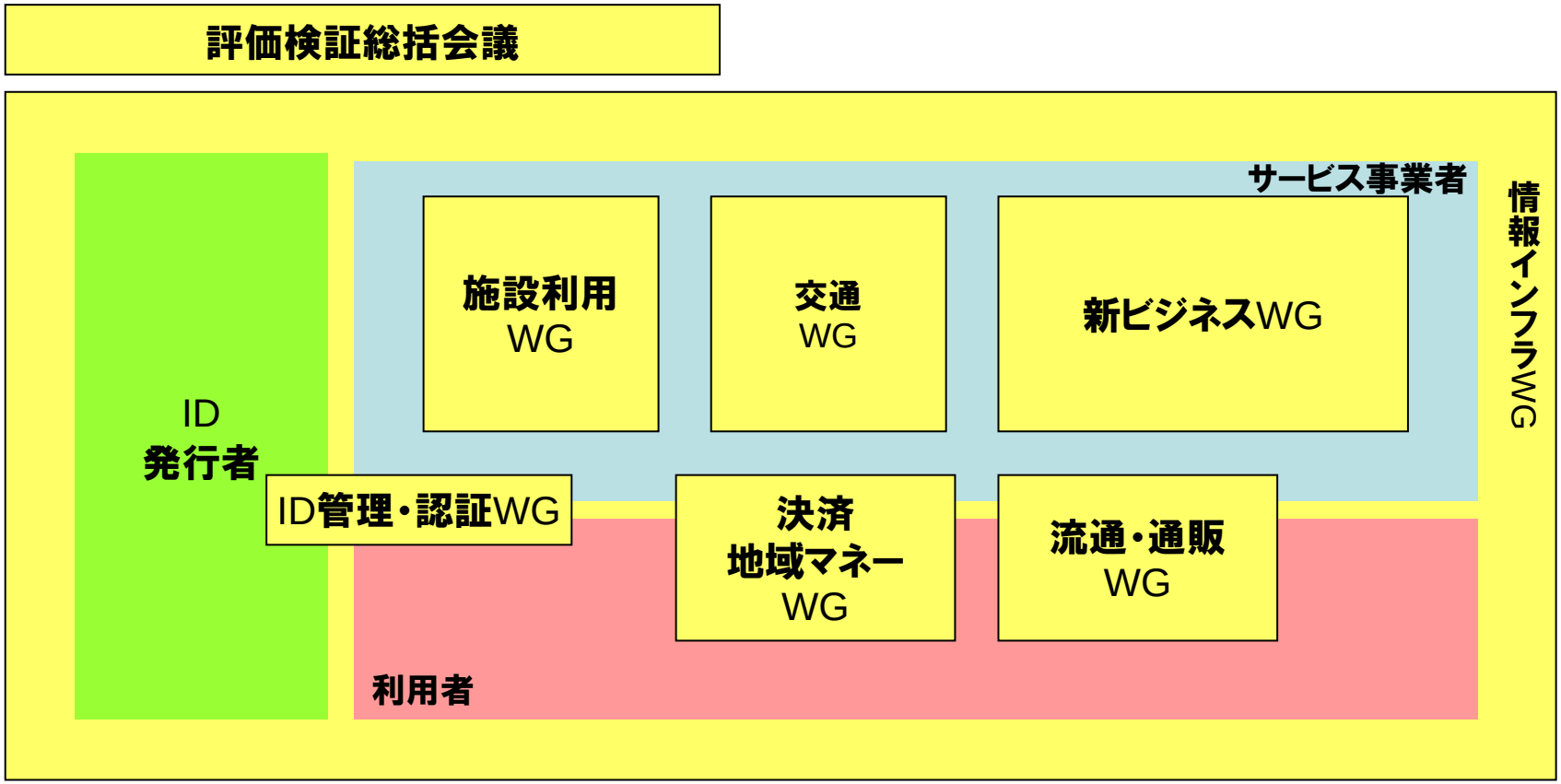


MIID管理システムと、大学の図書館サービス、自治体が運営する図書館・体育館等の公共サービスを融合し、相互運用を検証する実験

【検証項目】
大学・自治体で行っている
サービス融合のあるべき姿模策
・サービスの融合による高付加価値化
・メディアリーダ氾濫防止による
管理効率向上
住基カード、学生教職員証、フェリカ携帯が混在する新しい施設サービスの
機能検証
・予約/入退出/書籍貸出し/顧客管理/
付加価値情報提供

実験の検証と将来に向けた提案WGの構成

WGの構成について



評価検証総括会議議長・・安浦　寛人（九州大学システムLSI研究センター　センター長）
ID管理・認証WGリーダー・・安浦　寛人（九州大学システムLSI研究センター　センター長）
決済・地域マネーWGリーダー・・原　徳登（（財）九州大学学術研究都市推進機構　事務局長）
施設利用WGリーダー・・藤井　恵介（（株）KESAKAシステム　専務取締役）
交通WGリーダー・・武津　義行（（株）キューデンインフォコム e-ビジネスグループマネージャー　部長）
流通・通販WGリーダー・・野原　佐和子（（株）イプシ・マーケティング研究所　代表取締役兼CEO）
新ビジネスWGリーダー・・久保　善博（（財）福岡県産業・科学技術振興財団　専務理事）
情報インフラWGリーダー・・岡村　耕二（九州大学大学院システム情報科学研究院　助教授）

まとめ

- 情報技術は社会基盤の基本構成要素
- 認証基盤の構築と実証実験
  - MIIDシステムの開発とQUPIDの運用
    - メディアとID体系の分離
    - サービスごとに異なるID
    - 柔軟で多様な認証方式
    - 事故の波及の最小化と復旧
    - 既存システムへの容易な接続
    - 個人情報の分散管理と保護
  - 実用的なサービスシーンでの実証実験
  - 新しいシステム構築への提案
- 大学を新しい社会基盤の実験場へ

ミクロ的視点の情報科学から

社会全体を把握し、
社会基盤システムを設計する
マクロ的情報科学へ