# 全学共通IC カードの学内実証実験報告とその基盤技術について

池田, 大輔
全学共通IC カード導入推進室, 大学院システム情報科学研究院, 附属図書館研究開発室

安浦, 寛人
全学共通IC カード導入推進室, 大学院システム情報科学研究院, システムLSI 研究センター



出版情報：九州大学情報統括本部ITマガジン. 1 (1), pp.13-21, 2007-06. 九州大学情報統括本部広報委員会
バージョン：
権利関係：

# 全学共通 IC カードの学内実証実験報告とその基盤技術について

池田 大輔* 安浦 寛人†

## 1 はじめに

九州大学の学内サービスの向上，学内業務の効率化，およびこれらの情報化に対応する共通的な個人認証基盤を構築するために，九州大学では情報政策委員会の下で下記のように全学共通 IC カード導入の準備作業を行ってきました.

**平成 15 年 6 月** システム LSI 研究センター開発の PID を用いた独自仕様による全学共通 IC カードの実現を決定（情報政策委員会）

**平成 16 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

**平成 16 年 2 月** IC カードの基盤技術の共同開発のためのパートナー企業の公募

**平成 16 年 3 月** パートナー企業を選定

**平成 16 年 8 月〜** 月１回のペースでステアリングコミッティーを開催．学内での導入を目指した実証実験の為の各種工程の管理及び協議を行う

**平成 17 年 6 月** 実験用システムの完成と公開実験

**平成 17 年 8 月** 新キャンパスで部分的に運用開始（入館の電子鍵）

**平成 17 年 9 月** 学内実証実験の承認（情報政策委員会）

**平成 18 年 1 月** 経済産業省から情報家電等のネットワーク化技術の相互利用性および有効性に関する実証実験事業」の受託

**平成 18 年 7 月** 経済産業省から「ディジタルコミュニティ実証実験事業」の受託

本稿では，九州大学が取り組んできた全学共通 IC カードの全学的導入を目指した学内実証実験[1]の報告と，全学共通 IC カードの技術的な背景について説明します.

## 2 学内実証実験報告

全学共通 IC カードの全学導入向けた準備として，平成 17 年度と 18 年度には認証のための基本的な枠組みといくつかのサービスへの適用を行いました[2].

*全学共通 IC カード導入推進室，大学院システム情報科学研究院，附属図書館研究開発室 mailto:daisuke@i.kyushu-u.ac.jp
†全学共通 IC カード導入推進室，大学院システム情報科学研究院，システム LSI 研究センター mailto:yasuura@c.csce.kyushu-u.ac.jp

[1]平成 17 年度と 18 年度の 2 つの経産省の委託事業は，新たなビジネスモデルの創出に関する実証実験であり，本稿で述べる学内の実証実験とは異なります．また，このための実験協力者も別途モニタを募っています.

[2]予定では平成 19 年度まで学内における実証実験は続けられます.

### 2.1 平成 17 年度

平成 17 年 10 月の伊都キャンパス開校にあたり，キャンパス内の主な建物の入館の電子鍵および理系図書館の入退館や貸出業務（限定的なユーザのみ）のサービスを開始しました（図 1 参照）．発行したカードは約 1200 枚ですが，各個人への個人カードとしての発行までは実現できていませんでした．これは，人事や学務のデータを

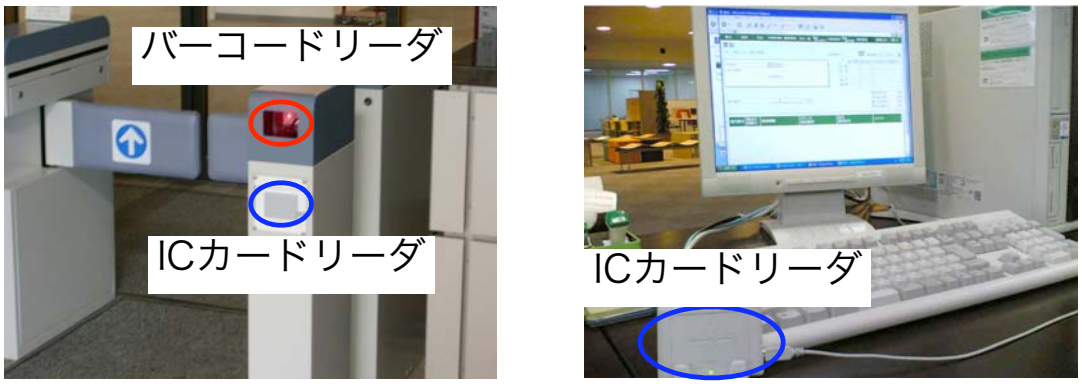


図 1: 理系図書館ゲート（左）と貸出用リーダ（右）

共有する体制的な仕組み作りが遅れたためです．

### 2.2 平成 18 年度

平成 18 年秋から，伊都キャンパスの学生及び教職員約 3500 人に「デジタルコミュニティ証」と呼ぶ IC カードを発行しました．また，伊都キャンパスにおけるほとんどの建物の入退館と，理系図書館における図書貸出と入退館でデジタルコミュニティ証が利用できます．

昨年度は実現していなかった個人データの受け渡しを行う体制を作り，個人カードとして発行することができました．また，附属図書館や工学部等事務部の協力により，これらのサービスも個人ごとに登録しました．これにより様々な利点が生じます．図書館サービスについて言えば，従来は利用者ごとに別途図書館への登録の必要があった教職員も，デジタルコミュニティ証で図書館サービスを利用することも可能になりました[3]．鍵サービスで言えば,「ある部門の人はウェスト 2 号館の出入口の鍵を開閉できる」や「教授のみが実験棟の鍵を開閉できる」など，IC カードの特徴を活かした利用が可能になりました．

その他，経産省の委託事業として，伊都キャンパスの生協売店や紀伊国屋書店での電子マネーによる買い物，福岡市営地下鉄・JR 九州・昭和バスなどの交通系の利用などの実証実験も行ないました．

## 3 PID (Personal ID) モデル

本節では全学共通 IC カードの基盤技術である PID (Personal ID) モデルを，プレイヤーとカード内の情報に分けて説明します．PID モデルは本学システム LSI 研究センターが提案・開発を行っている ID 管理のためのモデルです．

> ✔ 現在，PID ではなく MIID (Media Independent ID; メディアに依存しない ID) とも呼んでいます．MIID という時は，ID を運ぶ媒体（様々な種類の非接触 IC カード，携帯電話，USB トークンなど）に依存しない点を強調しています．一方で，以下で説明するプレイヤー間の関係や複数 ID を利用に側面に焦点を当てる時に PID と呼んでいます．

### 3.1 PID モデルのプレイヤー

まず，PID モデルを構成するプレイヤーは**発行者**と**サービス提供者**と**利用者**です（図 2 参照）．発行者は利用

[3]伊都キャンパスで働く教職員のみです．

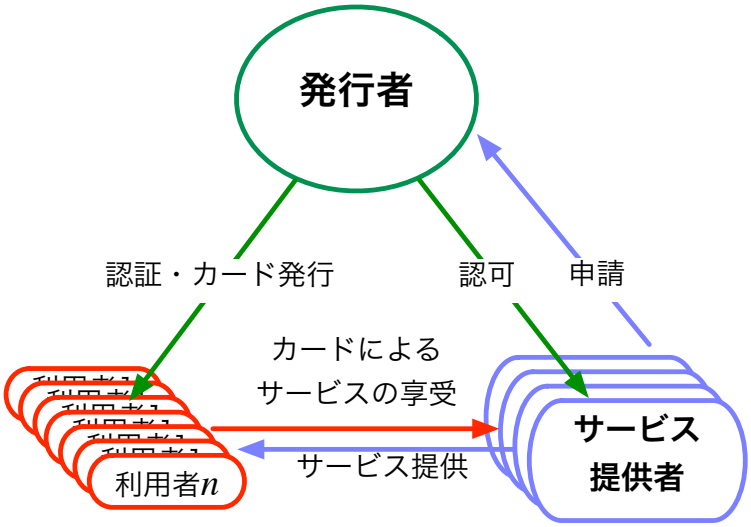


図 2: PID モデルにおけるプレイやーである発行者，サービス提供者，利用者の関係

者の個人情報などを確認した上で，利用者に IC カード[4]を発行します．通常はこの IC カードが身分証明証の役割を果たすことが多いでしょう．サービス提供者は，利用者にサービスを提供したい旨発行者に連絡し，発行者はサービス提供者としての適正やサービスの有用性を判断した上で，必要な情報をサービス提供者に渡します．利用者はサービスを利用するときに IC カードを提示します．サービス提供者は IC カードの情報と発行者から渡された情報を照合し，サービスを提供します．この情報がどのようなものであるかの詳細は後述しますが，基本的にはカードから個人を識別する番号が読み出れされ，サービス提供者が持つ ID 番号と照合されます．

本学の場合，発行者は総長で，利用者は学生及び教職員です．サービス提供者はそれぞれのサービスを行う部局や組織になります．図書館利用者カードを全学共通 IC カードに載せる場合は，附属図書館がサービス提供者です．また，ドアのカードキーを全学共通 IC カードに載せる場合は，その建物を管理する組織がサービス提供者になるでしょう．学外の組織もサービス提供者になることが可能です．

> ✔ PID は基本的にデバイスを用いるモデルであり，デバイスを「持つ」人を適切な利用者と考えます．しかし，デバイスを持つ人が正当な利用者かどうかは実際には分かりません．一方で，パソコンのログインによく用いられる ID とパスワード認証では，秘密の情報を「知る」人を適切な利用者と考えます．覚えられるパスワードはそれほど長くなく，そのため十分安全とは言えません．これらを組み合わせることでより安全な運用が可能になります．言い方を変えると PID モデルは人の認証方法とは独立したモデルであると言え，必要に応じて適当な強度の認証方法と組み合わせて運用する必要があります．

クレジットカード会社や銀行など，現在でも個人情報を保持してサービスを提供し，かつ，社会的な信用があるような組織は，自然な発行者の候補になります．実際，クレジットカード会社は単独でカードを発行するのではなく，様々な企業と提携してカードを発行しています．例えば，ガソリンスタンドの会員証にクレジットカード機能が付いています．PID モデルでは，提携するサービスは複数あってよいことになります．このようにすることで，カード発行にかかるコストやマーケティングに活かせる利用者の情報などを共有できます．ここでいう情報は「20 代の女性」や「A 学部の教授」などといった属性情報で，個人が特定されないことを想定しています．どのような情報が発行者からサービス提供者へ渡るのかについて，利用者には十分な周知が必要でしょう．

さらに，PID では利用者のプライバシーを保護するしくみが備わっています．これについては 3.2 節と 4 節で詳しく述べます．

住民に対して自治体が身分証明証を出している場合は，自治体の首長が発行者となり，公共図書館や住民票発行サービス，地域の企業が提供する会員制サービスなどを共通のカードで受けるモデルも考えられるでしょう．地場企業や地元の商店がサービス提供者になれば，自治体は地域振興の役割を果たすこともできると期待できます．

[4]もちろん IC カードでない媒体でもよいのですが，ここでは IC カードに統一して説明します．

### 3.2 PID と subPID

まず，PID に対応しない一般の IC カードや磁気カードを用いたサービスの利用について考えます．IC カードや磁気カードをカードリーダに読ませた時にどのような情報がサービス提供者に渡されるのでしょうか．厳密にはサービス提供者ごとに異なるはずですが，基本的には利用者（またはカード）に固有の番号や文字列（ここでは ID 番号と呼びます）が渡されているでしょう．つまり，ID 番号があれば個人情報やその他の情報はカード内にある必要はなく，サービス提供者のシステム内のデータベースで ID 番号とそのような情報を紐づけることができます．

PID モデルでは複数のサービスを受けることができますが，それを可能にするには各サービス提供者に ID 番号を渡す必要があります．ある利用者が持つ ID 番号は全サービス提供者で共通にすることもできますが，共通の ID では利用者の行動をサービスをまたいで追跡可能となり，プライバシー保護の観点から望ましくありません．そのため PID モデルではある利用者の ID 番号をサービスごとに違ったものを使うようにしています．

具体的にはカードの中身は以下のようになります．まず，発行者がカードを発行するときに *PID* と呼ぶ長いビット列を利用者に割りあててカードに格納します．次に，サービスを受けるときに，カードリーダからサービスに関する ID を受けとり，これを用いて PID を変換し別の ID 番号（*subPID* と呼ぶ）を生成します．これをサービスを利用するための利用者 ID 番号とします．もちろん PID はユニークな番号で，あるサービスにおいては subPID もユニークな番号です．変換方法は工夫してあり，subPID からは元の PID を復元することは非常に困難です．

この subPID の考え方と，発行者とサービス提供者の機能分離により，利用者にとって以下のような利点があります．

- 一枚のカードで複数のサービスが受けられる
- 発行者への申請のみで，複数のサービスが利用可能になる
- 一つのサービス提供者が持つ subPID のデータベースから情報が漏洩しても，他のサービスには影響を与えない
- ある利用者の subPID はサービスごとに異なるため，サービスをまたいだ個人の行動追跡が不可能になる
- サービス提供者側に個人情報が存在しないため，個人情報と購買履歴などのログが分離可能である[5]

サービス提供者側にも様々なメリットが生まれます．

- 発行者の機能を持たずにすむため，発行にかかるコストを軽減できる
- 個人情報を持たずにすむため，セキュリティに関するコストを軽減できる
- 身分証明書であるカードに相乗りできるので，どのサービス提供者のカードも持ち歩いてもらえる

一方で，以下のような欠点が考えられます．

- 1 枚のカードに多くのサービスが集約されるため，1 枚のカードを紛失した時のリスクが増大する
- あるカードでどのサービスが受けられるのか，カードリーダにかざして見るまで分からない
- 発行者が持つ利用者データベースが複数のサービスに対応するため，情報漏洩した時のリスクが増大する
- あらかじめ subPID をサービス提供者に渡しておく必要があるため，利用者の判断なしに subPID がサービス提供者に渡る

一番上とその次の欠点は，1 枚のカードで複数のサービスを享受できることの裏返しです．また，多くのサービスで個人情報を 1 箇所に集約することで，1 箇所のみでセキュリティ対策を行なえばよいという利点はあるものの，もし万が一情報漏洩が発生すると，一度に全てのサービスに影響してしまう，という欠点もあります．また，

[5]個人情報が必要なサービスもあるでしょう．その場合は，利用者に明示した上で発行者からサービス提供者へ個人情報が渡されます．

最後に挙げた欠点を一言で言えば「PID または subPID は誰のものか」ということになります．これについては，直感的に欠点だということが分かりにくいので少し詳しく説明します．

PID そのものはカード内に格納されており，個人と紐付いた情報です．逆に言えば，PID は各個人のものと言ってもよいでしょう．そうであればこそ，耐タンパー性のある IC カードなどに格納し，安全を期すわけです．

一方で，PID をサービスごとに変換して得られる subPID は，各利用者の同意なしに，サービス提供者に渡ります．したがって，必ずしも個人のものとは言えませんが，個人のものである PID から生成されており，いいかげんな変換の仕方であれば，subPID から PID が推測される可能性もあります．よって，この変換の仕方には十分に気をつける必要があります．現在の実装では，1 方向関数と呼ばれる性質を持つ変換方法を使っており，subPID から PID を推測することは困難です．

subPID は利用者の同意なしサービス提供者に渡されるものの，この情報だけでは利用者に関する情報はありません．したがって，利用したこともないサービス提供者から請求書が送りつけられる，といった事態は起きません．

# 4　図書館における PID モデルの実際と可能性

この節では，具体的なサービス提供者として附属図書館を考え，PID モデルが図書館の利用や運営にどのような影響を与えるかを，プライバシーと図書館運用の面から説明します．また，PID を用いることで可能になる新たな図書館サービスを示します．

## 4.1　プライバシー保護

本学の附属図書館に限らず，一般に図書館を利用するためには，利用者登録をする必要があります．つまり，図書館には利用者の個人情報が存在し利用者 ID に紐づけられています．また，図書館における行動，例えば，貸出履歴や演習室などの利用時に利用者 ID が用いられることが多いため，誰が何をしたかという情報が図書館に蓄積されることになります．つまり，個人情報と行動履歴が同時に図書館にあります．このような状態では，悪意ある図書館職員がいたり，操作ミスやシステムのバグの存在などにより，プライバシーの侵害につながる可能性は否定できません．PID モデルでは個人情報が図書館に蓄積されないため，このような危険性が原理的になくなります．

一方で，個人情報を図書館から分離しているのは，運用としてそうしているだけであり，技術的に運用していることが保証されているわけではありません．従って，利用者から見れば，サービスを享受するときに，本当に個人情報がそこにないかどうかを確認する手段がありません．そのため，PID モデルで運用する場合は，プライバシーポリシーや発行者からサービス提供者へどのような情報が何のために渡されているのかなどを明確にし，利用者からの信頼を得るような運用体制の構築が必要でしょう．

### 4.1.1　情報の取り過ぎ

PID モデルを用いることにより個人情報と行動履歴の分離が可能になるだけでなく，従来の図書館サービスにおける個人情報に関する問題点も明らかになりました [1, 2]．図書館に個人情報，特に連絡先が必要なのは，返却期限を過ぎても図書を返却しない利用者に連絡を取るためです．そのため，教職員からは申請時に，学生からは図書を借りる時に，図書館職員が連絡を取る必要があるからと説明した上で連絡先情報を取得していました．

このやり方では，仮にいつも返却期限内に返す立派な利用者がいたとしても，この利用者の連絡先も取得しないわけにはいきません．つまり，モノを貸しだすという性質上，返却してくれそうかどうかにかかわらず，情報を取る必要があるのです[6]．

[6]本を貸す前に保証金を取り，本を返したら保証金を戻す，ということも考えられますが，金銭の授受と保管にかかるコストを考えると現実的とは言えません．

表 1: 必要な個人情報に合わせた subPID と個人情報の対応表

| 貸出用 subPID | 個人情報 | 入館用 subPID | 個人情報 |
|---|---|---|---|
| 0000000001 | 池田 大輔 (642-4422) | 0000000208 | 附属図書館 |
| 0000000007 | 安浦 寛人 (583-7620) | 0000000093 | システム情報科学研究院 |
| … | … | … | … |

図書館ではこのような状況は当たり前のことでしたが，PID モデルを図書館に適用した場合と比較してみると，現在の状況は真面目な人間が情報の取られ損をしている，ということができます．PID モデルでは連絡先を含む個人情報は発行者側にあり，返却期限内に図書を返す限り図書館がその情報を取得する必要はありません．しかし，万が一本を返さなかった場合，図書館から発行者に申請の上その利用者の連絡先を教えてもらう，という運用が可能になります．つまり，返却が遅れた場合のみ，個人情報を取得する，という運用が可能です．

ただし，この場合，一度でも延滞してしまうと情報が図書館に渡ってしまい，PID を用いる利点が薄れてしまいます．4.3 節で詳しく述べるメッセージ転送機能を用いれば，図書館が連絡先を知ることなく，連絡を取ることも可能になります．

#### 4.1.2 図書館内のサービス分割

大学図書館では貸出以外にも入館時にゲートに利用者カードのバーコードを読ませる必要があります．現在の入館ゲート設置の目的は大きく二つあり，一つは有資格者だけに入館を制限すること，もう一つは部局ごとの入館者数の統計を取るためです．この目的のためには個人名が分かる必要はありません．しかし，普通の図書館における運用方法では図書館利用者カードには個人情報が関連づけられているため,「誰」がいつ入館したか分かります．つまり，ここでも情報の取り過ぎが発生しているわけです．

PID モデルでは複数のサービスを扱うことが可能で，しかも，カードは一枚ですから図書館内のサービスを分割することで情報の取り過ぎを防ぐことできます．まず，図書館内のサービスを全部まとめて考えるのではなく，必要な個人情報の粒度に応じて複数のサービスに分けます．例えば，個人情報はとりあえず必要ないけど督促の時には必要になる「貸出サービス」，個人情報は最後まで必要ないけど所属学部の情報が必要な「入館サービス」，著作権の関係から個人名が必要な「ILL サービス」という具合です．

> ✔ ILL (Inter Library Loan; 図書館間相互貸出) による複写は，図書館間という名前ですが，著作権の観点から言うとあくまで利用者が複写を依頼していることになります．そのため，現行の ILL の運用においては利用者の名前が依頼先の図書館に渡る必要があります．

従来のサービスとカードの関係では，このようにサービスを分けるとそれに応じてカードが必要になり，ひいてはカードに対応した別の利用者データベースが必要になります．また，全ての ID を一つにすると利用者データベースは一つで済みますが，最も情報を必要とするサービスに合わせる必要があるため，本来必要のないサービスでの個人情報を取得する必要がでてきます．

PID モデルでは 1 枚のカードで複数のサービスが受けられるため，発行者が持つ subPID と利用者情報の対応表を少し変えるだけで，必要な個人情報のみを提供してサービスを受けられる仕組みができます．つまり，入館サービスの subPID に対応する個人情報は学部名のみに，貸出サービスの subPID に対応する個人情報は氏名や連絡先などに，ILL サービスを受ける場合は subPID と個人情報を図書館に渡します（表 1 参照）．このようにしても，各 subPID は別ですので，ILL の利用履歴と入館の利用履歴からある特定の利用者の動きを追跡することはできません．また，入館用の subPID には個人情報は対応づけられていないので，誰が入館したかは分かりませんが，統計情報を計算するために必要な情報はあります．

### 4.2 図書館運用におけるメリット・デメリット

上述したプライバシー保護に関する PID のメリットは，どちらかといえば利用者に対するメリットでしょう．しかし，図書館側から見てもメリットはあります．学生証に図書館利用者 ID がバーコード印字されているため，

学生は入学と同時に図書館を利用することができます．一方で，教職員は図書館利用者カードを各自作成する必要があります．全学共通 IC カードが導入されれば，教職員も新たな申請の手間がなくなり，図書館員もカード発行の手間やコストが不要になります．

また，個人情報を保持しないメリットもでてきます．現在は本部事務から提供を受ける学生に関する個人情報と，申請してもらった教職員の情報を適切に管理する必要がありましたが，PID モデルではその必要はなくなります．

> ✔ 学外の人も図書館を利用できます．そのため，外部利用者に対する利用者カードの発行や外部利用者の氏名，連絡先などは図書館が管理する必要があるでしょう．

PID と subPID の考え方により，最小限のコストで全学共通 IC カードを導入できます．通常，複数のサービスを使う場合は，ID を統一するなどの工夫が必要です．単に同じ ID を使えばよいではないか，と思われる方もいらっしゃるかもしれませんが，利用者データベースの作り直しになり，莫大なコストが発生します．しかし，PID モデルでは各サービスごとに別の ID を利用することが可能ですので，すでにサービス提供者が利用している ID 体系（ここでは独自 ID と呼びます）を利用することができます．実際には，subPID はあくまで発行者が作りますので，subPID から独自 ID への変換までを行い，独自 ID を図書館システムに渡します．そのため，図書館システムから見ると全学共通 IC カードを使われたのか，旧来の利用者カードを使われたのか判別できません．別の言い方をすれば，IC カードと利用者カードを混在した環境で利用でき，徐々に導入することも可能です．そのため，すでに稼働している図書館システムに大規模な変更を加える必要もありません．実際，伊都キャンパスの理系図書館の入館と貸出は，実験的に配布している IC カードでも利用できますが，従来の利用者カードも問題なく使えます．

一方でデメリットとしては（図書館に限らず）カードが壊れた場合の対応が困難なことが挙げられます．バーコードであれば，多少印字面が汚れても読みますし，仮にバーコードリーダが読みとれなくても，番号を手で入力すれば運用が可能です．しかし，PID モデルの場合はカードに入れてある情報と発行者から図書館に渡されている情報を符合させて，個人情報を照合せずに利用者であると認証します．そのため，カードそのものが読めない場合は利用者認証が行なえません．また，カード内の情報は秘密情報ですから，バーコードのように数字として印字しておく，という運用も不可能です．よって，PID モデルでは，以前に増して障害対策を十分に考慮しないといけないでしょう．

## 4.3 新たなコミュニケーションサービス：ハブとしての図書館

4.1 節と 4.2 節で述べた PID の利点は，PID の設計や開発段階から予想された利点でした[7]．本節では，図書館という具体的なサービスに適用を考えた時に新たな見えてきた PID の可能性について説明します．

図書館のように貸出を行うサービスでは督促が必須であり，そのため利用者の連絡先が必要です．4.1.1 節で簡単に述べたように，PID モデルではあらかじめ連絡先を図書館が取得するのではなく，メール転送機能を使って人手を使わずに利用者にメールで督促を行うことが可能です．

具体的には以下のようにします（図 3 左参照）．まず，図書館は督促したい利用者の ID (subPID) と実際に送りたいメッセージを発行者に送信します．発行者は ID をメールアドレスに変換し，メッセージを利用者に送ります．この手続きはシステムとしてほぼ自動で行うことが可能です．つまり，各サービス提供者は利用者の個人情報を得ることなくメッセージを送ることが可能です．

督促は通常電話で行っており，非常にコストのかかる作業です．これに対し，うっかり忘れてしまった利用者にメールにより延滞を知らせることができれば，督促にかかるコストを抑えることが可能になると予想されます．

また，このメール転送機能をより積極的に使うことも可能です．例えば，図書館で行う利用者講習会などのイベント情報を知らせたいとします．無差別に利用者全員に送るのではなく，特定学年の利用者や別イベントへの出席経験者などにターゲットを絞ってメールを送るほうがよいでしょう．どのような属性の人に送りたいかを決

[7]ただし，プライバシー保護については個人情報をサービス側から分離することのみが利点として認識されており，情報の取り過ぎなどについては，実際に図書館に適用後に新たに認識された PID の利点です．

め，該当する人の subPID と送りたいメッセージをメール転送サーバに送れば，効果的にイベントの案内を行うことができます．

さらに，メール転送機能を使えば，誰が借りたかは知らなくても，同じ本を借りた人に発行者経由で連絡できる可能性があります（図 3 右参照）．

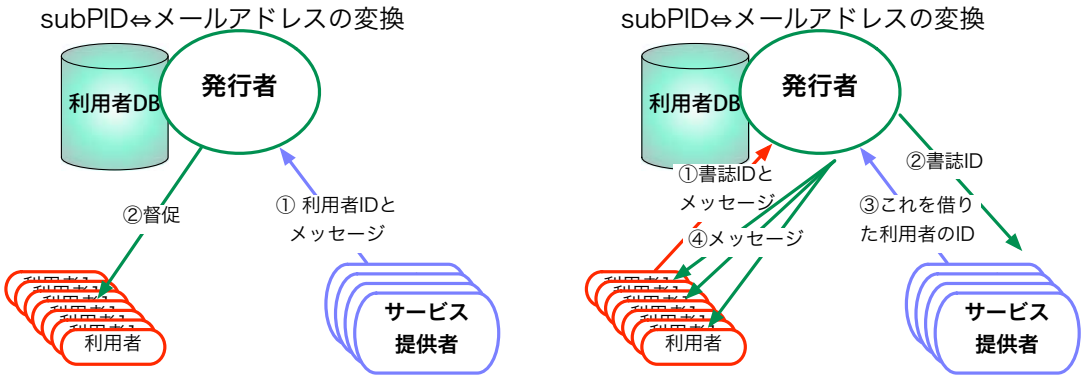


図 3: メール転送機能を応用した督促（左）と利用者間のコミュニケーション（右）

利用者は書誌 ID と自分の利用者 ID (subPID) を図書館に通知します．具体的なイメージとしては，書誌 ID を読み込むバーコードリーダと利用者 ID を読み込む IC カードリーダが付属したキオスク端末のようなものに本と IC カードを載せます．次に利用者はメッセージを入力します．書誌 ID と利用者 ID，メッセージは発行者に送信されます．発行者は書誌 ID のみを図書館に転送し，図書館は書誌 ID に関連のある利用者，例えば，最近その本を借りた人などを抽出し，その ID を発行者に返信します．発行者は利用者の ID をメールアドレスに変換し，最初の利用者のメッセージを添えて各利用者に送ります．

このように，特に複雑な機能や仕組みを仮定せず，プライバシーを保護した上で図書館をハブとした知的なコミュニケーションが可能になります．このようなコミュニケーションは従来は不可能でした．例えば，以前は図書に図書カードが挟んであり，借りるときにカードに名前を書いていました．図書カード世代の方には，図書館で本を手に取った時に知りあいが同じ本を借りたことを知って親近感を覚えた経験があるのではないでしょうか．あるいは，知り合いではないけれども自分が借りた本と同じ本をよく借りる人の存在を知り，自分はまだ借りていないがこの人が借りた本を教えてもらえないか，と思ったことがある人もいるのではないでしょうか．しかし，個人のプライバシーを守る観点から，図書館がこのようなコミュニケーションの仲介をすることは考えられないでしょう．

ここでは図書館で説明しましたが，一般の企業でも有用なマーケティングツールとなる可能性があります．企業でマーケティングを行う際は，個人名まで必要とするようなデータマイニングや統計解析をすることはなく，ほとんどは属性で処理をしています．例えば，ある製品は 20 代の女性によく利用されている，などで十分な場合が多いでしょう．個人情報は管理のためのコストが高いばかりで，特にマーケティングに役立つわけではありません．このような場合でも PID モデルを用いると，個人情報を持たずに効率的にマーケティング可能です[8]．

しかし，解決すべき問題もあります．この仕組みでは，メッセージが必ず発行者を通るため，別のプライバシー侵害の問題が発生する可能性があります．これは，発行者には個人情報があり，行動の一部がメッセージとして発行者を通るため，個人情報と行動を結びつけることが可能になります．

これに対して，一度別の利用者と連絡を取りあい，互いの連絡先を交換した後は，発行者を通さない方法でメッセージを交換する，という方法も現実的でしょう．しかし，一度でも発行者にメッセージの内容を見られる可能性は排除したい場合は，例えば公開鍵暗号を用いた暗号化などにより，発行者からメッセージの中身を秘匿するような仕組みが必要かもしれません．

[8]企業がサービス提供者になる場合は，発行者は例えば自治体や金融機関が考えられます．

## 5　おわりに

本稿では全学共通 IC カードの学内実証実験について報告し，コア技術である PID モデルを説明しました．そして，主に図書館での例を用いて，どのような影響があるかを説明しました．

学内実証実験はまだ続いています．この期間で，ここまでの実証実験を通して明らかになった問題点を解決して，より良い全学共通 IC カードとして全学的な導入が可能になるように努力していきます．

## 参考文献

[1] 池田大輔, 安東奈穂子, 田中省作．ディジタルライブラリにおける履歴・個人情報の保護及び利用．http://rd.cc.kyushu-u.ac.jp/~daisuke/paper/08-Mar-05-DLW.pdf, 3 2005．（ディジタル図書館ワークショップ講演）．

[2] 安東奈穂子, 池田大輔, 田中省作. 電子図書館と利用者のプライバシー――履歴・個人情報の保護と利用の両立を目指して――. デジタル図書館, No. 30, pp. 62–71, 3 2006.