新個人認証システムPersonal IDが変える図書館の個人情報管理 ： 個人情報やプライバシーに配慮した一歩先行く図書館サービスとは

安東，奈穂子
九州大学法学研究院学術研究員（協力研究員）

池田，大輔
九州大学システム情報科学研究院准教授

出版情報：大学図書館研究. 81, pp.26-41, 2007-12-31. 学術文献普及会
バージョン：
権利関係：

新個人認証システムPersonal IDが変える図書館の個人情報管理

－個人情報やプライバシーに配慮した一歩先行く図書館サービスとは－

安 東 奈穂子，池 田 大 輔

大学図書館研究81号別冊
2007年12月発行
（pp.26～41）

新個人認証システムPersonal IDが変える図書館の個人情報管理
－個人情報やプライバシーに配慮した一歩先行く図書館サービスとは－

安 東 奈穂子，池 田 大 輔

抄録：個人情報漏洩事件が相次ぐなか，図書館にも，図書館利用者の個人情報やプライバシーに対するいっそうの配慮が求められている。そこで，現在多くの図書館において行われているような，個人情報の取得を半ば当然としたうえで取得後のセキュリティを重視する個人情報管理が，果たして十分な情報保護を実現しているのか検証し，それに対して，画期的な新個人認証システムPersonal IDシステムの下では個人情報管理にどのような変化がもたらされるのかを比較検討する。さらに，当該システムを活用した，図書館利用者の情報主権者としての立場をより尊重した情報取得のあり方や，それに基づく，図書館利用者自らが主導権を握る利用者指向のサービスについて考察する。

キーワード：個人認証，個人情報管理，個人情報漏洩，PIDシステム（Personal IDシステム），MIID（Media Independent ID），図書館利用者，図書館サービス，個人情報，プライバシー，履歴

第1章　はじめに

第1節　図書館の個人情報管理の見直し

2005年4月の個人情報保護法全面施行以来，個人情報の取り扱いをめぐっては，今まで以上に社会的な関心が寄せられている。特に，個人情報が流出した場合には，情報管理者は厳しい批判にさらされ，法的な責任[1]を問われることはもとより，積み上げてきた社会的な信用を一瞬にして失うことにもなる。

これは図書館においても決して例外ではない。2004年10月には，三重県立図書館の全利用者約133,000人の個人情報が漏洩する事件[2]が報告されており，社会的に大きな問題となったことは今なお記憶に新しい。現在の図書館には，従来にも増して図書館利用者（以下，利用者）の個人情報やプライバシーに対する配慮[3]が求められており，なかでも個人情報管理の見直しは急務であるといえよう。

第2節　個人情報を“取得する時”への視点の必要性

図書館としては，できる限り不要な個人情報の取得および保管は避けたいところであるが，現在提供しているサービスの維持を考えれば，利用者から取得する情報を減らすという方向性よりは，取得した情報をいかに安全に保管するか，具体的には，セキュリティ強化や職員への情報モラル教育などに力点が置かれている[4]ように思われる。すなわち，図書館が個人情報を“取得する時”に着目するよりも，“取得した後”のことの方がどちらかといえば重要視されている向きがある。

けれども，取得時という早い段階から，あらかじめ個人情報漏洩のリスクを軽減できたり，仮に漏洩した場合でも被害を最小限にとどめたりできる手立てがあるならば，それを講じない積極的な理由は見当たらない。また，図書館が利用者に個人情報の提示や提供を要求するような場面での，利用者に不安を与えない，納得してもらえる個人情報の取得方法を導くためには，何より情報取得時に焦点を当て，それぞれの個人情報の利用目的を改めて問うことが重要な鍵を握っている。さらに，図書館が利用者の情報を取得する正にその時に，個人情報やプライバシーに配慮した誠意ある図書館の姿勢を具体的なかたちで示すことができれば，利用者の図書館に対する信頼もさらに深まるであろう。

このようなことから，図書館の個人情報管理のより効果的な見直しを図るためには，情報取得後の対策もさることながら，この取得時への視点も決して欠かすことはできないものと考えられる。

第2章　問題提起と本論文の目的

第1節　個人情報取得時の視点からみた問題点

それにしてもなぜ，ここ最近は，図書館における個人情報の取得時を検証する試みがあまり見られないのであろうか。それは，利用者の個人認証という個人情報の取得と深く関わり，代表的な図書館サービスでもある貸出返却業務において，現在ほとんどの図書館が，横並びで類似のコンピュータ“技術”や“システム”を取り入れている[5]ことと少なからず関係しているように思われる。

このような現状では，現に導入されている技術やシステムに疑問を抱くことは稀かもしれない。また，そうした技術やシステムに対し，周辺の一般的な図書館とは違う独自性や変革を強いて望まない限り

は，図書館利用者カードの作成にあたって取得しコンピュータに保管する個人情報の種類や，実際に貸出カウンターにおいて利用者カードのバーコード読み取り作業といった認証プロセスを通じて取得する貸出記録を含めた個人情報の質やレベルについて，改めて吟味する必要性も感じられにくいのかもしれない。

しかし，今やコンピュータを用いた個人認証の技術やシステムは目覚しく進歩し多様化している。従って，カード作成時や図書貸出時に，利用者の名前や連絡先以外の個人情報を取得する可能性も考えられる[6]。さらに，技術やシステムの選択が広がってきている今だからこそ，利用者の認証に際して名前など“直接に”個人が特定される情報を取得する必要が本来あるのかを検証したり，サービス提供に際して必要とされる最小限の個人情報を再考したりして，図書館における個人情報取得の現状を，取得時の段階から見直す時期に来ているといえるだろう。

第2節　本論文の目的とするところ

今こそ図書館は，現状より望ましい個人情報取得のあり方 —— 例えば，同じ個人情報であっても漏洩のリスクや被害が軽減されたうえでの取得，あるいは，サービスごとに要求される個人情報に限ったうえでの取得 —— の実現に向け，新しい技術やシステムの導入，ならびに当該技術やシステムの最大限の活用方法を積極的に検討する必要があると考える。

その具体的な検討には，まず現在の図書館において，提供されているサービスごとにどのような個人情報やプライバシーに関わる情報が図書館に取得され保管されているのかを検証する。次に，各サービスとそれが本来要求している情報を厳密に分析し，先の検証と比較して，現在の取得方法では，個人情報が漏洩した場合に被害が甚大化するおそれのあること，さらに図書館が必要以上の個人情報を取得する傾向にあることを指摘する（**第3章**）。

そのうえで，九州大学システムLSI研究センターで提案され，このたび一部キャンパスで実証的に導入された，新たな個人認証システムであるPIDシステム（Personal IDシステム）[7]を紹介したい。そして，図書館はこのPIDシステムによって情報漏洩のリスクや被害を軽減できることなど，具体的にどのような影響や作用が及ぶのか，また適用範囲や限界についても言及したいと考える（**第4章**）。

最後に，この新しい認証システムの効用をさらに活用することによって，いかなる可能性が広がるかについていくつかの提案を行いたい（**第5章**）。

第3節　予想される結果

この一連の検討作業を通じて，図書館における個人情報やプライバシーに一層配慮した新しい情報管理モデルの提示，さらには，利用者の自己情報コントロールを尊重した情報取得のあり方が明らかになるものと確信している。そして，このようにして導かれる提示や提言は，後に第5章で具体的に述べるような，利用者と図書館とが協力して情報の付加価値を創造する関係の更なる発展に貢献し，また図書館以外の情報管理者にとっても示唆深いものになると考えている。

第3章　想定する現在の図書館

本論文では，貸出手続きおよび個人情報の管理に際して，コンピュータが導入されている図書館を想定する。

第1節　図書館がサービスを通じて取得する図書館利用者の個人情報

図書館では，実に様々なサービスが利用者に提供されている。その核ともいえる貸出サービスはいうまでもなく返却と表裏一体である。すなわち，貸出サービスを円滑に行うためには，利用者からの返却が確実に行われなければならない。仮に返却が遅滞するような場合には図書館は当該利用者に対し督促を行う。このような必要性からも，図書館は利用者の名前や連絡先（電話番号やメールアドレス）といった個人情報を取得しデータベースに保管している。

また，貸出サービスや予約サービス[8]などの提供にあたっては，貸出記録や予約記録を通じて，利用者が“何を借りているのか”や“何を読みたいのか”というような，利用者と本との結びつきを垣間見ることのできる情報も取得し，一定期間，保管している。例えば貸出記録については，何を，誰に，いつまで貸したかを把握するために保管しており，返却処理の後は速やかに消去する図書館が多い[9]。

さらに，利用者が図書館において体験する，本を“借りる”または“予約する”という出来事，言わば利用者のイベントから図書館が取得する情報も，同じ利用者において複数回蓄積すれば，当該利用者が“今までどのような本を借りてきたのか”という読書履歴や，“どういったジャンルに興味があるのか”という読書傾向を示す情報へと転化する可能性がある。特にこのような読書履歴や読書傾向となって現れる情報は，利用者の思想や信条[10]に深く根ざすプライバシー情報[11]といえよう。

すなわち図書館は，名前や連絡先といった直接に個人が特定される情報，ならびに図書館における利

用者の個々の読書イベント（来館する，閲覧する，借りる，予約する，図書館から資料提供を受けるなど）から取得する情報，ひいては，読書履歴や読書傾向といったプライバシーに至るまで，利用者に関する幅広く多様な情報を取得しうる立場にある。

このような状況のなかで図書館は，行動規範となる「図書館の自由に関する宣言」（1979年改訂）や「図書館員の倫理綱領」（1980年）のなかで，職務上知り得た情報の秘密保持や利用者のプライバシーを尊重することを定め，個人情報保護法が施行されるかなり以前より，サービスを通じて取得した利用者の個人情報とプライバシーに対して慎重な取り扱いを心がけてきた[12]。

第2節　図書館がサービス提供に必要とする最小限の情報

ではここで，特に図書館から利用者に対し個人情報の提示や提供を要求するようなサービスや場面について，それぞれに対応する必要最小限の情報について考えてみたい。そこで一つ確認しておこう。先で見てきたように，図書館が利用者の個人情報を取得する主な理由は，利用者からの本の返却を徹底するための個人認証ゆえにほかならない。すなわち図書館は，個人認証を通じて，利用者の“信用”を確認すること，および連絡先を“担保”することによって，返却を確保しているのである。

＜貸出サービス＞

やはり利用者からの返却を確保するためには，利用者の“信用”確認と連絡先の“担保”が必要不可欠である[13]。しかし，そのために果たして図書館は，“直接に”個人が特定されるような情報を利用者より取得する必要があるのであろうか。

直接に名前を利用しない場合，一般的に行われている方法として利用者カード番号がある。図書館は利用者カード番号と利用者の名前との対応表を持つが，対応表がない限りは番号だけで直接に個人を特定することはできない。これによって図書館は，貸出のたびに名前や連絡先を利用者から取得する必要はなくなる。ただし，利用者カード番号発行の際に信用確認のため個人情報を取得しなければならないのはもとより，利用者カード番号の管理[14]や督促を考えると，取得した個人情報はその後も保管し続けなければならない。

このほかにも例えば，大学図書館や公共図書館の場合，同じように利用者の個人情報を取得していて，かつ，当該図書館と縦なり横なりの繋がりのある大学の事務局や自治体が，図書館に代わって利用者の信用を確認してくれるならばどうだろう。そうすれば当該図書館は，そもそも利用者カード作成の際のように，“独自に”利用者の個人情報を取得しデータベースに保管する必要がなくなる。さらに，利用者の信用確認に現状ほど厳格な個人認証を要しなくなり，連絡先もあらかじめ取得しておかなくても，督促時に，大学の事務局や自治体のデータベースに保管されている情報に速やかに辿り着ければ良くなるのではないだろうか。

以上のようなことから，貸出サービスに最小限必要な情報とは，利用者からの返却を確保するための情報であり，逆に言えば，貸出期限内に返却する利用者の個人情報は必要なく，督促時において初めて直接に個人が特定される情報に辿り着くことが担保された情報であれば十分といえよう。ここにいう，“直接に個人が特定される情報”を「第1レベルの個人情報」，“直接に個人が特定される情報に速やかに辿り着くことが担保された情報”を「第2レベルの個人情報」と呼ぶことにしたい。

＜予約サービス＞

予約された本が返却されれば直ぐに，次の予約者に連絡する必要がある。そのため，予約の段階で，利用者の連絡先（電話番号やメールアドレス）は明確にしておくことが要求されよう（「第1レベルの個人情報」）。しかし名前は，「第2レベルの個人情報」でも良いのではないだろうか。

＜ILL（Interlibrary Loan）サービス＞（図書館間相互協力サービス）

ILLサービスとは，図書館間で行なう図書の貸借（Interlibrary Loan）と文献複写の取り寄せ（Document Delivery）を指す。ただし文献複写の場合は，表向きは図書館間のやり取りではあるものの，本質的には著作権法第31条の図書館等における複製の規定[15]に則り，利用者が資料を持つ図書館に依頼するかたちをとることを要す。よって依頼館も受付館も，申込者である利用者が確かにいることを確認することが要求されるため，「第1レベルの個人情報」が必要となる。

＜施設[16]利用サービス＞

館内の施設の利用を誰にどの程度認めるかは，図書館の運営方針によるところが大きい。緩やかな運用では，「第2レベルの個人情報」で十分であろう。一方，厳格な運用で，建物の管理上，特に火気管理などの安全性の問題から利用者の責任を重たくしておく必要があると考える場合には，施設利用の申請の際に，少なくとも代表者の「第1レベルの個人情報」が要求されよう。

＜入館ゲート＞

当該図書館の利用者として適格かどうかを判断する情報が要求される。例えば大学図書館であれば，

大学の構成員であるかどうか，所属（学部や院など）を示す情報のみで良いはずである。よってここでは，利用者の「第1レベルの個人情報」も「第2レベルの個人情報」も必要ないであろう。ただし無人開館の場合には，安全性に特に配慮することが求められるため，「第1レベルの個人情報」もしくは「第2レベルの個人情報」が必要となろう。

第3節　現在の取得方法が抱える問題点

これまでの叙述を踏まえたうえで，図書館における現状の個人情報の取得方法が抱えている問題点について，3つほど挙げておきたい。

まず，果たして図書館が現状で取得している個人情報が，サービス提供に必要な最小限の情報かどうか検証したい。前述のとおり，図書館サービスにおいて「第1レベルの個人情報」が要求されるのは限られた場合のみである。これと現状を比較すると，図書館は必要以上の個人情報を取得しているという感が否めない。特に貸出サービスでは，返却をきちんと行う利用者もあらかじめ「第1レベルの個人情報」が取得されていることが指摘できる。すなわち，サービスが要求する情報と実際に図書館が取得している情報が釣り合っていないのである。これは，現状の取得方法における問題点の1つに挙げられよう。この問題は，図書館が利用者の信用確認および連絡先の担保を，“独自に”行うことを前提としていることから生ずる，現状の個人認証システムにおける限界ともいえるかもしれない。よって，この問題を打開するには，前節でも少し触れたように，このような前提をとらない個人認証システムの構築を考える必要がありそうである。

次に問題の2点目として，図書館において，直接に個人が特定される情報と貸出記録や読書履歴などのプライバシーとが切り離されないまま取得されていることが挙げられる。仮に利用者カード番号を割り当てるとしても，番号と利用者を直接に特定できる情報との対応表は，図書館が持っている。その図書館が，現状では，さらに，利用者の思想や信条が反映された貸出記録や読書履歴というプライバシーも取得しうる立場にある。よって，たとえ図書館がプライバシーに配慮していると説明を繰り返しても，現に図書館がその意思さえあれば見られる状態にあること，さらに，図書館が情報を持っている限りは，システム障害やクラッキング[17]などにより意図せずそうした情報が漏洩する危険性も孕んでいることなど考えれば，利用者の不安を拭いさるのは到底容易ではない。

最後に3点目として，現状のように図書館が，利用者の名前や連絡先といった個人を特定できる情報をはじめ，“何を借りたのか”や“何を読みたいのか”というような，利用者と本との結びつきを垣間見ることのできるプライバシー情報に至るまで取得する方法は，図書館が単独で一括して情報を管理できるという利点はあるものの，いったん情報が漏洩した場合には，被害が甚大化してしまう問題がある。

これら3つの問題点からいっても，図書館における個人情報の取得方法の現状は，利用者に不安を与えない，納得してもらえる個人情報の取得のあり方を十分に実現していると言うことはできず，見直されるべき余地があると言わねばなるまい[18]。

第4章　新個人認証システムPID（Personal ID）の導入

第1節　図書館に求められる新しい個人認証システム

前章で指摘したように，図書館における現在の個人情報の取得方法では，

①サービスが要求する利用者に関する最小限の情報の内容と，実際に図書館が取得しているそれらとが一致していないこと＝**「過剰な情報取得」**，

②直接に個人が特定できる情報と，利用者の内面が反映される貸出記録や読書履歴というセンシティブ情報[19]とが一つの建物内において切り離されないまま取得されていること＝**「情報の不分離」**，

③個人情報を一括して取得保管し独自に個人認証を行うことが，漏洩した場合に大きな危険性をはらんでいること＝**「単独で情報管理を行うことのリスク」**

など，いくつかの問題があることが分かった。

これらの問題は，利用者にとって図書館を利用する際の弊害とまで意識されていなくとも，図書館に対する不安や緊張に結びついていることに異論はあるまい。よって，現状より望ましい図書館と利用者との関係を指向するならば，これらの問題を解決することが必須といえよう。では，これらの問題を解決する糸口はどこにあるのだろうか。

まず，これらの問題に共通しているのは，どれも情報の取得時に端を発しており，図書館が利用者に関する情報を取得するプロセスと深い関係を有していることである。そして，その情報が取得されるプロセスを実際に左右しているのは，図書館が個人情報を取得する根拠ともなる利用者認証を行う際，現に実動しているコンピュータによる個人認証システムがどのような情報を必要とするかである。よって，コンピュータシステムの改良が問題解決の糸口になりそうである。

一方で，これらの問題を単なるコンピュータの問

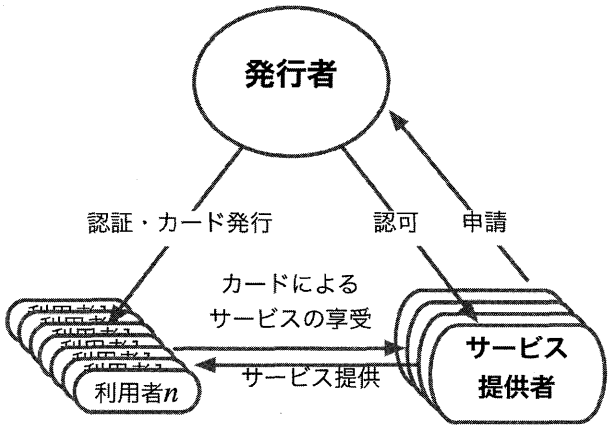

図1

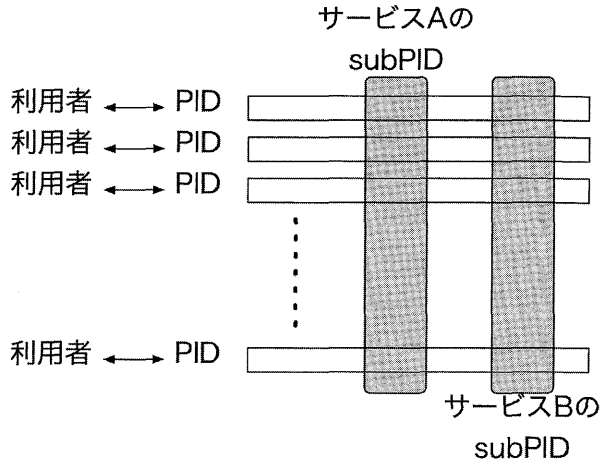

図2

題[20]として片付けてはならないだろう。なぜなら，それらは実はコンピュータの問題であると同時に，何よりシステムを支えている認証の手法，すなわち，「誰とまたは何処との関係性において，どのような情報をやり取りすることによって信用を確認するのか」という問題だからである。そこで考えてみるに，現在ほとんどの図書館では，利用者との二者関係において，直接に利用者を特定できるような情報（第1レベルの個人情報）によって信用を確認する手法をとっている。さらに，図書館と利用者との間の認証は，図書館から利用者への一方向のみ行われている。このような認証の手法においては，図書館が独自に，個人情報を取得，保管し，認証を行うことを前提とせざるを得ない。このことは，前述の特に②や③の問題と深く関連している。

以上のことから，問題解決のために図書館に求められる個人認証システムとは，そもそもの認証の手法が全く異なる，新しい認証システムであるといえよう。

第2節　新個人認証システムPID（Personal ID）とは？

そこで紹介したいのが，新しい個人認証システムであるPID（Personal ID）システム[21]である。

PIDシステムは，九州大学で提案された新しい個人認証システムで，現在ではMIID（Media Independent ID）と呼ばれ[22]，キャンパスの一部ではすでに導入されており，2009年の本格的な導入を目標としている[23]。ICカードの持つ情報記憶や情報処理機能といった特性を活用した，実用的でかつ信頼できる認証基盤の構築を可能にし，社会や組織全体における情報管理の安全性の維持，および個人のプライバシー保護と多様なサービス[24]の安定的な提供の両立を目指すものとして注目されている。

具体的には，［発行者］，［サービス提供者］，［利用者］の三者関係における相互認証が基本となる（**【図1】**参照）。［発行者］は，まず［利用者］にPID（個人識別子）として十分に長いビット系列を与え，それをICカード等の記憶媒体に格納して［利用者］に渡す。さらに［発行者］は，［サービス提供者］が［利用者］にとって適切かどうかを判断し，適切であると判断した場合には，［サービス提供者］に対しサブPID[25]（［利用者］のPIDを分割したもの）を渡して認証の許可を与える。この際，［サービス提供者］に渡されるサブPIDは，個々のサービスごとにユニークなものである（**【図2】**参照）。こうして［利用者］はサービスを受ける際，［発行者］の許可を得た［サービス提供者］と，サブPIDによって相互認証を行う[26]。

例えば九州大学附属図書館では，［発行者］は九州大学総長であり，学生や教職員などの構成員が［利用者］，図書館が［サービス提供者］となる。この場合，学生や教職員の個人情報は，総長がPIDの発行に伴う身元と信用の確認のために提供を受け保存するにとどまり，図書館にはサブPIDのみで直接に個人が特定できる情報は渡されない。

第3節　PIDの特徴と効果

PIDシステムの最も大きな特徴の一つは，サブPIDにある。サブPIDとは，前述のとおり，PIDが分割されたものであって，それだけで個人を特定することはできない。しかしながらサブPIDは，一方では確かに，［サービス提供者］と［利用者］との関係において直接に個人を特定できない情報（第2レベルの個人情報）ではあるものの，［発行者］という，［サービス提供者］と［利用者］とを前もって認証する者が加わることによって，［サービス提供者］が［利用者］を認証するに十分な情報となりうる。

このようなサブPIDを特徴とするPIDシステムの

効果は，以下の２点が主要なものとして挙げられよう。

まず１点目は，**「情報の分離」を可能にする**ことである。

PIDシステムにおいて，直接に［利用者］を特定できる第１レベルの個人情報を取得および保管し，かつ［利用者］に割り当てられたPIDとの対応表を有しているのは［発行者］だけである。さらに［発行者］は，PIDを分割し，それだけでは個人を特定することができない第２レベルの個人情報（サブPID）にまでレベルを下げたうえで［サービス提供者］に渡す。そのため，［サービス提供者］の手元には，第１レベルの個人情報とは切り離された情報が取得されるにとどまる。すなわち，PIDシステムによって個人情報をレベルの異なる二つの情報に分離することが可能となる。例えば，［サービス提供者］に，サービスの提供に伴って［利用者］に関する私的な情報が入手されたとしよう。しかし，［サービス提供者］には，［発行者］からサブPIDという，直接には［利用者］を特定することはできない第２レベルの個人情報しか渡されていないため，入手された私的な情報が直接に［利用者］を特定することのできる第１レベルの情報と結びつけられるおそれはない。これを［サービス提供者］の側から言い換えるなら，サービス提供に付随して得た［利用者］の私的な情報を第１レベルの個人情報と分離して取得することが実現可能となる。

また，このような情報の分離は，［サービス提供者］の内部にも生じる。例えば，同じ［サービス提供者］内でも，提供するサービスごとに［利用者］の認証に必要な最低限の情報の内容（Aサービスでは年齢と性別，Bサービスでは名前と連絡先，Cサービスでは所属，Dサービスでは一切不要･･･）は異なる。さらに，名前や連絡先を必要とするサービスのなかでも，これらの情報が認証の際に敢えて明確にされる必要はなく，その後場合によっては必要となるときのために担保しておきたいというような，第２レベルの個人情報で十分なサービスもある。サブPIDはこのように様々なサービスごとにそれぞれ独特のものを割り当てることができる。よって，個々のサービスに見合ったバリエーションに富んだ認証を行うことが可能となる。そのうえ，異なる［サービス提供者］を跨ぐ［利用者］の行動の追跡を不可能にするのは言うまでもなく，同じ［サービス提供者］内の異なるサービスを跨ぐ追跡も防ぐことができる。

次に２点目は，**「情報漏洩リスクおよび被害の軽減」を可能にする**ことである。

そもそもなぜ情報が漏洩するのか，そして情報漏洩がこれほど危険視されるのか。もちろんセキュリティ管理の不十分さや情報モラル教育の後れなどを指摘できようが，何よりも情報が価値を有しているからこそ狙われたり漏洩の危険を恐れたりしなければならないといえるだろう。どんなにセキュリティを強化し情報モラル教育を施したとしても，管理する情報が価値を有している限り，情報盗難のおそれおよび何らかの理由で情報が漏洩した際の悪用の危険性に，常に神経をすり減らさなければならない[27]。かたやPIDシステムにおいて，［サービス提供者］が管理している情報は，直接に［利用者］を特定できない情報であるために，第三者から見た個人情報としての利用価値は格段に低い。よって，個人情報の漏洩の危険性は従来に比べ明らかに減少し，漏洩した情報が悪用されることへの懸念も軽減される。

さらに，［サービス提供者］は，PIDシステムにおいて，サブPIDによって［利用者］を認証することができるので，今までのように独自に第１レベルの個人情報を取得して保管する必要がない。よって，仮に［サービス提供者］の管理する情報が漏洩したとしても，漏洩した情報により個人が特定される危険性はほとんどないと言ってよく，従来の情報漏洩事故に比べて［利用者］に及ぶ被害が極めて小さい。そのうえ，PIDシステムでは，それぞれの［サービス提供者］が異なるサブPIDによって認証を行っているため，一つの［サービス提供者］の情報漏洩事故が他の［サービス提供者］の［利用者］の認証に影響を及ぼして被害が広がってしまうおそれもない。後に［発行者］が，情報漏洩事故を起こした［サービス提供者］の［利用者］にサブPIDの再割当てを行うだけでよい。すなわち，個人情報の漏洩の被害を最小限にくいとめることが可能となる。

第４節　図書館へのシステム導入

では，このPIDシステムが図書館に導入された場合，具体的にどのような作用や変化が起こるであろうか。以下に３つほど述べたい。

第１に，今までのような図書館と利用者との二者関係から，［発行者］が加わった三者関係へと移行する。

PIDシステムでは，図書館は［サービス提供者］，利用者は［利用者］，それに対して［発行者］は，図書館と同じ組織に所属して縦なり横なりの繋がりがある機関の長や，目的を同じにしたり物理的に繋がりがあったりする団体の代表者などが考えられる。例えば，大学図書館においては大学の総長，公共図書館においては，自治体の長が［発行者］として相当である。このほかにも，複数の図書館が集合

したなかを代表する図書館の館長や，図書館とともにビルを共用している団体の代表者などもあてはまるであろう。

第2に，図書館の個人情報管理の安全性がさらに向上する。

PIDシステムにおいて，［サービス提供者］である図書館は，直接に利用者を特定できてしまうような情報を独自に取得して管理する必要がない。よって，前節でも述べたように，従来に比べて情報漏洩の危険性は減少し，仮に図書館が情報漏洩事故にあっても被害が最小限に抑えられる。また仮に，他の［サービス提供者］が情報漏洩事故にあってサブPIDが流出しても，それとは異なるサブPIDによって認証を行っている図書館には事故の影響は及ばないため，安定したサービスの提供が実現できる。⇒**「単独で情報管理を行うことのリスク」が無くなる**（本章第1節の問題③の解決）。

第3に，従来よりも利用者のプライバシーに配慮したサービスが可能となる。

例えば現状の図書館では，貸出サービスにおいて返却をきちんと行う利用者もあらかじめ第1レベルの個人情報が取得されてしまっている。一方PIDシステムにおいては，図書館には第2レベルの個人情報しか渡されておらず，なおかつ，図書館が貸出サービスの提供に伴い利用者を認証するためには，督促時において初めて直接に個人が特定される情報に辿り着くことが担保された第2レベルの個人情報で必要十分である。また，図書館では貸出サービス以外にも様々なサービスが提供されているが，そのそれぞれにユニークなサブPIDが割り当てられサービスごとに必要な情報と対応しているため，個々のサービスに適応した適切な情報の取得を実現できる。⇒**「過剰な情報取得」の解消**（本章第1節の問題①の解決）。

さらに貸出サービスを通じて図書館には，利用者の貸出記録が取得される。従来の貸出記録は，貸出された本の情報とその本を借りた利用者を特定できるような第1レベルの個人情報とが結びついたプライバシー情報である。それに対し，PIDシステムにおいては，利用者の本を“借りる”または“予約する”というイベントを通じて図書館に入手される情報は，前節でも述べたように，取得時の段階から第1レベルの個人情報と分離されている。よって，PIDシステム導入下での貸出記録は，その本を借りた利用者を直接に特定できる個人情報とは結びつかない[28]。また，例えば仮に図書館において，サービスの性質上からどうしても個人の特定を必要とするサービスがあって第1レベルの個人情報などが取得されても，その情報と他のほとんどの第2レベルの個人情報で必要十分なサービスから取得される情報とが結び付けられるおそれもない。すなわち，図書館にPIDシステムが導入されることは，利用者の個人情報の保護ばかりでなく，プライバシーに配慮することにも繋がる。⇒**「情報の不分離」からの脱却**（本章第1節問題②の解決）。

第5節　PIDの適用範囲とその限界

ところで，ここまでは主にPIDシステムの有用性について述べてきたが，果たしてPIDシステムは，あらゆる場面で適用可能な万能なモデルとまで言い切ることはできるだろうか。そこでこの節では，PIDシステムを実際に運用する際に予想される問題点を指摘し，現時点で考えうる解決方法や，今後に考察が必要となる課題などを示しつつ，PIDシステムの適用範囲について議論することとする。

第1款［発行者］と［サービス提供者］／［利用者］の関係

個人認証システムを要するサービスにおいては，［サービス提供者］と［利用者］の二者モデルが通常である。一方PIDシステムは，その二者に［発行者］が加わった三者モデルの形態をとる。こうした三者モデルで予想される問題のまず一つは，通常の二者モデルには存在しない［発行者］の責任が大きくなることである。

実際，三者モデルにおける［発行者］は，［利用者］との関係では，［利用者］の身分や素性の確認，ICカードなどの安全な媒体の配布が必要となり，さらに，［サービス提供者］との関係では，新規に［サービス提供者］が加入する際の適切な確認作業，定期的なサブPIDリストの更新などが必要となる。そのため，大学における大学と大学図書館／大学の構成員のように，従来から自然に，PIDシステムの下での［発行者］に近い業務が三者のなかで行われている場合にはスムーズに導入できると予想される。けれども逆に，そのような関係にないサービスに適用する場合はどうだろうか。以下，そのようなサービスの例として，電子マネー[29]とポイントサービス[30]の二つを挙げて考えてみる。

まず，電子マネーだが，例えば，大学が［発行者］で，公共交通機関用の電子マネーを発行する企業を新規に［サービス提供者］として加える場合を考えてみる。地域によっては，すでにICカードで公共交通機関を利用する人々が多数いるところもあり[31]，現実にこのような連携が実現する可能性は十分にある。こうした公共交通機関向けの電子マネー用ICカードは，種類によっては本人確認なしに購入することもできるが[32]，PIDシステムの下でも，［サー

ビス提供者］は直接に個人が特定される情報を保有する必要はなく，その点を考慮すればシステム導入は十分可能といえよう。まして，［発行者］によって身分や素性が確認された，身元のしっかりした潜在的な顧客が増えるという利点もある。

一方で，ポイントサービスを提供している店舗を新規に［サービス提供者］として考える場合には，個々の店のマーケティング等における個人情報の利用方針の如何により，PIDシステムを導入できる場合とそうでない場合があるだろう。すなわち，ダイレクトメールなど，［利用者］に直接アクセスするマーケティング手法に重きを置いている場合には，［サービス提供者］が［利用者］を直接に特定する情報を取得できないようなPIDシステムは利用できないことになる。ただし，このような直接的なマーケティングは，［利用者］が望んでいない場合も多く，スパムメールや迷惑メールに対する近年の苦情の高まりを踏まえれば，そのあり方を考える時に来ているといえるだろう。このような状況に対応して，氏名や連絡先の情報を用いずに，例えば「20代の男性」といった属性情報によるマーケティング手法を構築することや，［利用者］の側から積極的に自分の目的に適った広告情報を取得するモデルとPIDシステムを組み合わせることなどが求められており，今後の考察に値する。

第2款　コストの問題

PIDシステムでは，ICカードなどの安全な媒体の存在を仮定している。このことは，カードの発行やリーダ／ライタの設置などに多大なコストがかかることを意味している[33]。

大学や企業において身分証明書としてICカードを発行することは不自然ではない。そのため，大学図書館や企業内の図書室で，このICカードをそのまま利用者カードとして利用することも自然である。しかし，一つの大学や企業の中だけでは，十分に多くのサービスがあるとは限らない。もしサービスの数が不十分であれば，多くのサービス間で認証基盤を共有するメリットが生まれず，多大なコストを掛けるだけの価値も乏しくなり，PIDシステムを導入することは実質的に不可能になる。よって，PIDシステムの導入にはサービスが多数あることが必須であり，そのためには，大学における大学図書館のようなサービスだけでなく，大学組織とは直接に関係のないサービスとの間でもPIDシステムを共有して利用できることが望ましい。ただしその一方で，それを可能にするためには，多くのPIDの［発行者］の存在が，あらかじめ，もしくは同時に必要になってしまう。このことを具体例で考えてみよう。

例えば上述したような公共交通機関（企業A）が現実問題として［サービス提供者］になるためには，企業Aから見て，あらかじめ多くの人々がPIDの発行を受けPIDシステムを利用している環境がなくてはならない。なぜなら，仮に一つの大学（大学B）だけでPIDシステムを導入し，大学Bの構成員がシステムを利用しているくらいでは，［利用者］の数に限りがあり，多大なコストを掛けてまで自動改札機にリーダを設置するだけの価値は生じないからである。つまり，［発行者］の大学Bとは異なる組織の企業Aが［サービス提供者］になる場合には，すでに大学Bのほかにも多くの組織でPIDシステムが採用されており，PIDの［発行者］が複数存在して，多くの人々がサブPIDを持つ状況になければ，［サービス提供者］として加入する価値がないことになる。したがって，サービスの数が多くなければPIDシステムの導入は難しいが，反面で，サービスの数を増やすにはPIDシステムを導入している組織が多く必要であるというジレンマに陥る。

これを解決する方法として，携帯電話や，住基カードのような既存のICカードなど，発行コストがかからない媒体を採用することが考えられる。これらの媒体において，PIDからサブPIDを生成するプログラムを載せることが可能になれば，発行コストを低く抑えた発行業務が実現できる。

第3款　督促の問題

確かに，PIDシステムの下で図書館の貸出手続の際に取得される情報は，当該サービスに最低限必要な，直接に個人が特定される情報に速やかに辿り着くことが担保された情報（第2レベルの個人情報）のみである。よって，現状の図書館のように，貸出期限内に返却をきちんと行う利用者までもが，あらかじめ直接に個人が特定される情報（第1レベルの個人情報）を取得されてしまうことや，それが貸出記録と結びつけられプライバシー情報として蓄積されてしまうことなどを回避できる。

ただし，仮に返却が遅滞し督促の必要性が生ずれば，その折は，当該利用者に対して，電話番号やメールアドレスを通じて，借りたままになっている本の速やかな返却を促さなければならない。もちろん督促の際，未だ返却されていない本の借り手が誰なのかを確認し，その本人の連絡先に返却を催促することは当然のことといえるが，しかしながらこのとき，当該利用者について，貸出記録と，直接に個人が特定される情報とが結びついてしまうことが問題となる。すなわち，貸出時には，図書館において，当該利用者の貸出記録と第1レベルの個人情報は明らかに分離していたが，ひとたび督促を行うとなれ

ば，これらの情報は結合しプライバシー情報を図書館が取得してしまう事態となる。

たとえ，図書館に代わって，［発行者］である大学の事務局や自治体が督促を行うとしても，当該利用者にとって，自己の行動履歴と個人情報が結びつけられ，プライバシー情報が他者に取得されてしまうことに変わりはない。また実際には，手間を伴う督促の作業を，およそ［発行者］が図書館に代わって行うとは考えにくく，従来どおり図書館が行うと考えるのが妥当であろう。

こうしたことから，現状の督促のあり方では，ある利用者にいったん督促の必要性が生ずれば，依然として図書館において，当該利用者の貸出記録と直接に個人が特定される情報が結びついてしまうことを否定できない。よって，今後の課題として，図書館がこのような第１レベルの個人情報を取得せずとも，有効で，かつ，あまり手間のかからない督促を可能にする新サービスを構築するなどにより，解決策を講じていくことが求められよう。

第５章　PIDの更なる活用を図書館利用者の視点から考える

これまでに説明したとおり，図書館にPIDシステムが導入されることにより，個人情報の取得後はもとより取得時の段階から，情報漏洩の危険性や漏洩被害が軽減され，さらには，利用者のプライバシーに配慮したサービスも可能となる。だが，PIDシステムが可能にすることは，これだけに尽きるのであろうか。PIDシステムの可能性をもう少し探ってみよう。

第１節　PIDが図書館利用者に与える心理的な影響

PIDシステムの導入によって，［サービス提供者］である図書館は，直接に個人が特定される情報を取得する必要はなくなる。このことを，利用者の視点から考えてみる。

直接に個人が特定される情報を他者に取得されるということは，当該個人に大きな精神的重圧を与える。また，前にも述べたとおり，図書館にあっては，貸出サービスや予約サービスを通じて，読書履歴や読書傾向といったプライバシー情報も取得されてしまうおそれがある。

それがPIDシステムによって，図書館に取得される情報が依然として個人情報であるとしても（「第２レベルの個人情報」），直接に個人が特定される情報ではない（「第１レベルの個人情報」ではない）ということによって，貸出手続きなどにおける情報の提示や提供に際して，利用者の精神的負担や抵抗感が軽減されると考えられる[34]。

第２節　図書館の信頼性の向上と図書館利用者との良好な関係作り

図書館は，PIDシステムという利用者に分かりやすいシステムを導入することによって，個人情報の取得や管理の透明性を確保することができる。そのうえ，情報漏洩の危険性や漏洩被害が軽減された個人情報管理が可能となり，利用者に安心感を与えるであろう。これらは，図書館の信頼性の向上に繋がるものと思われる。

さらに図書館の，利用者に対する日ごろからの個人情報やプライバシーに配慮する姿勢がPIDシステムによって具体化，明確化されることは，図書館と利用者との間にある，個人情報を取得する側と取得される側という一方的な関係を緩和してくれるであろう。

第３節　図書館でPIDを活用した提案

図書館にPIDシステムが導入されることにより，指摘した現状の問題点も解決され，より望ましい情報取得のあり方が可能になると考えられる。しかしながら，やはり利用者からどのような情報を取得するかは図書館の方針に任されているため，図書館の指示に従って個人情報などを提供する利用者の立場はあくまで受身の感が否めない。そこで提案したいのが，利用者の自己に係わる情報を提供する側としての，すなわち情報の主権者としての立場をより尊重した情報取得のあり方であり，さらにそれに基づいた，利用者自らが主導権を握る利用者指向のサービスである[35]。

図書館はかねてより利用者のプライバシー権[36]に配慮してきたが，そのプライバシー権が発展した権利として，近時，自己情報コントロール権が注目を浴びている。自己情報コントロール権は，プライバシー権と同様，明文化されておらず，その定義自体も必ずしも確定しているとはいえないが，一般的には，「本人が自己に係わる情報を保有する者に対してその情報の開示・変更・消去を請求することができる権利」と解されている[37]。その意味でこの権利は，旧来のプライバシー権よりも個人の自己に係わる情報への主権者としての積極的な関与を保障しようとするものである。個人情報保護法も，このような自己の情報に対する個人の一定の利益を尊重し，「公表等，開示，訂正等，利用停止等」（第24条～27条）を定めている[38]。またこの権利を簡潔に分かりやすく，より積極的に表現するならば，「自己に関する情報を，いつ，どのように，また，どの程度他人に伝えるかを自ら決定できる権利」ということもできよう[39]。このような考え方を反映した図書館の個人情報の取得のあり方がPIDシステムの活用を

通して可能となる。

例えばまず一つに，サービスごとに要求される個人情報を細かく限ったうえで取得する方法である。大学図書館において，貸出手続きの際は，督促時に速やかに個人を特定できる情報に辿り着ける情報をあらかじめ利用者より取得しておく必要があるが，入館して閲覧するだけなら，大学の構成員であることを示す所属（学部や院など）の情報のみで良いはずである。これにPIDシステムを活用することにより，個々のサービスに必要な情報ごとにサブPIDが対応付けられるので，入館ゲートと貸出カウンターでは，それぞれ種類の異なる情報が取得され認証が行われる。このようにすることで，利用者は，自己が受けようとするサービスの範囲内で，かつそれに適った最小限の自己に係わる情報を図書館に伝えることが可能となる。

第1款　現在の具体的な導入例

そこで，PIDシステムの具体的な導入例として，現在，九州大学の新キャンパスである伊都キャンパスにおいて運用されているケースを図に示す（**【図3】**参照）。附属図書館におけるサービス以外にも，建物や部屋の鍵として，また，電子マネーの利用などにも活用されている。

九州大学附属図書館では，分館の一つである理系図書館において，ICカードや携帯電話を用いたPIDを運用している。そして，実際に理系図書館においては，一つの［サービス提供者］が複数のサブPID集合を用いることが可能なことを活用し，“入館用サブPID”と“貸出用サブPID”を別にすることによって，前述したような，サービスごとに要求される情報を最小限に限定したうえで取得する方法を実現している（**【図4】**，**【図5】**参照）。

なお，理系図書館では，従来の図書館利用者カードも利用可能である（**【図4】**参照）。また，他館においては，今のところ従来の利用者カードで運用しているため，個人情報は，従来どおり図書館システム内に保管する運用形態がとられている。この点は，今後予定されているICカードの本格導入時や，図書館システムのリプレース時などに合わせて，変更されると考えられる。

九州大学でのPIDシステムの導入は今のところ部分的であり，九州大学附属図書館におけるPIDの特徴を活かした具体例も，将来的には次に述べるとおりサービスも充実すると考えられるが，現状では上述のとおり，分館の一つで実施されている入館ゲートと貸出サービスにとどまっている。また，実際に運用してみて，具体的に現場でどのような効果が得られているか，あるいは問題点が浮上しているかについては，導入から日が浅いこともあるが，検証は不十分である。ぜひこうした点は，次稿での考察に譲りたいと思う。

第2款　将来的なサービス

九州大学では，2009年のPIDシステムの本格的な導入に向けて，今後ますます様々な図書館サービスをPIDに対応させていくことが積極的に考えられている。

例えば，九州大学附属図書館で“MyLibrary”と呼ばれているような，パーソナライズドWebページへのログインや，機関リポジトリへ登録するためのログインなど，コンピュータシステムの対応である。これらのサービスがPIDに対応することによって，利用者は異なるIDとパスワードを覚える手間から解放されるとともに，高いセキュリティの確保も期待できるようになる。

また，コンピュータシステムだけでなく，予約システムと連動した館内のセミナー室や会議室などの鍵や，ICカードをリーダにかざすと必要な個人情報部分があらかじめ記入された種々の申請書などが出力される帳票サービスなども考えられる。帳票サービスのように，個人情報が必須のサービスが存在すると，仮に全て共通のIDで運用されている場合には，他のサービスに対してもIDと個人情報の紐づけが可能になってしまうおそれが生ずる。しかしPIDシステムの下では，異なるサブPIDを割り当てることにより，このような紐づけが不可能となる。

さらに，PIDの後継規格として研究開発および実証実験が進められているMIID[40]には，電子マネーや決済機能も付加されている。一方，図書館では現在，コピー機の利用やILLサービスの利用の際などに現金の授受が行われているが，こうした現金の管理に要する手間はとても大きい。そのため，小さな分館では，研究費でのみ利用可能といった制限が設けられているところもあり，学生の利便性を損なっているという問題が指摘されている。PIDまたはMIIDでは，これらのサービスにも，プライバシー保護を実現したまま対応することが可能であり，利用者にとっての利便性向上はもちろんのこと，図書館職員にとっての負荷軽減も期待できるようになる。

第3款　更なる活用に向けての提案

そのうえ，現代のような高度情報化社会においては，利用者のなかにも，図書館に自己に係わる情報を提供することにより，図書館の情報処理能力を経由してさらに付加価値の向上した情報を得たいと考える者も少なくないと思われる。このような，自己に係わる情報を積極的に利用しようとする利用者を

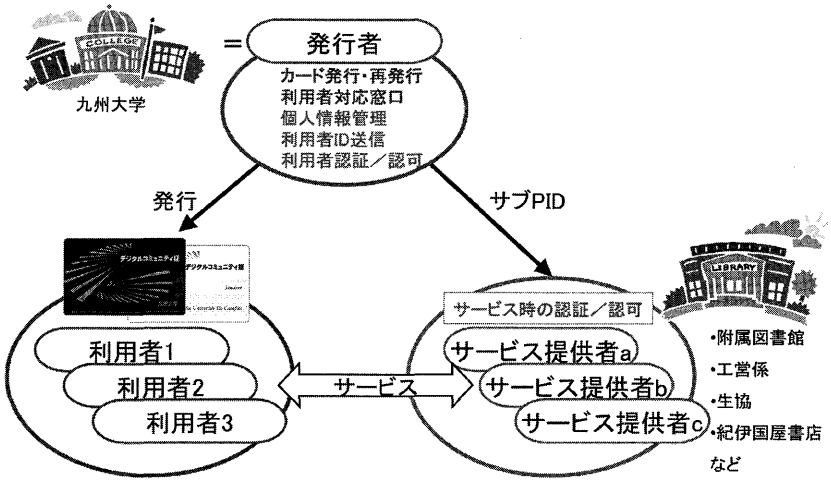

図3

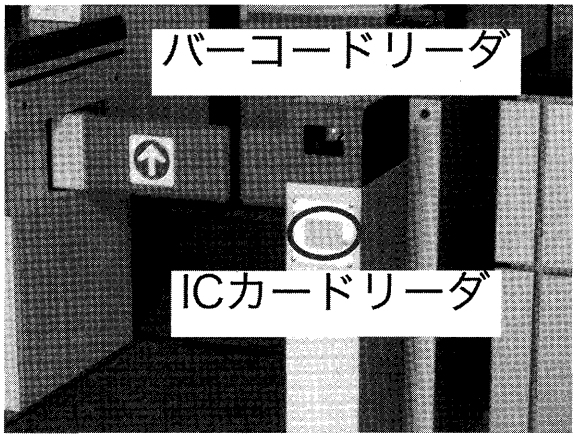

図4

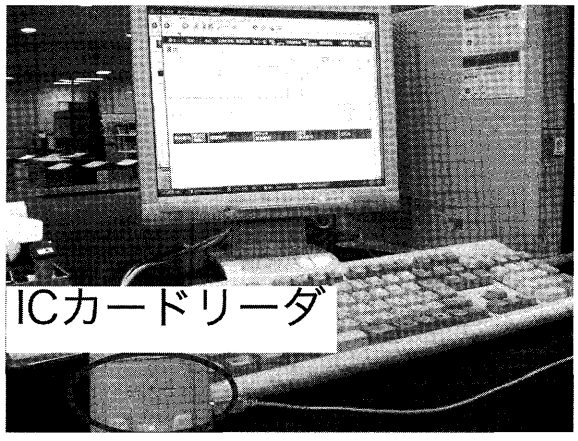

図5

視野に入れた，独自性ある利用者指向のサービスの開発もPIDシステムの活用によって実現可能となるであろう。

すなわち例えば，読書履歴という自己に係わる情報は，特に短期間の間に大量の図書や雑誌に当たる大学の研究者などにとって，重複して資料を集めてしまうミスを防ぎ，長期間にわたる読書履歴もまた，自己の研究の流れを客観的に示す貴重な材料にもなる。よって，このような情報を自己のために利用したいと考える利用者は少なくないと思われる。しかしながら現状では，読書履歴は個人情報と分離されていないために，プライバシー情報を取得することなく，図書館が履歴を作成してサービスとして提供したり，利用者の問合せに応じたりすることも難しい状況にある。無論，利用者が自ら作成するにも手間を伴う。ここにPIDシステムが導入されることによって，図書館においては個人が特定されなくなることから，利用者のなかには，図書館の協力を得ながら読書履歴を作成したいと希望する者も現れるかもしれない。このような場合，図書館は利用者に対し，十分な理解と許諾を得たうえではあるが，PIDシステムを活用した読書履歴の提供[41]を検討しても良いと考える。

また利用者は，PIDシステムによって，今までにはなかった半匿名性（PIDシステムの下での［利用者」は，直接に個人を特定されないが，明確に特定できる存在として保証されていること）とでもいうべき自己表現を手に入れることができる。図書館もこれに呼応して，図書館の利用の幅をさらに広げる新たな独自性ある図書館サービスを構築することができよう。

例えば大学において，学際的な研究も多くなっているなか，分野の垣根を越えて出会いの機会を求めている研究者は少なくないと思われる。図書館の本こそ，実際に分野の垣根を越えて流通しているものの一つであり，同じ本を介して情報を共有している研究者が必ず存在するのである。しかし実際の大学図書館のなかでは，様々な分野の研究者たちが言葉も交わすことなくすれ違っているにとどまっている。このような状況が，PIDシステムを活用するこ

とにより，研究者が自己のサブPIDを利用して，一定のプライバシーを留保しながら図書館に情報を寄せたり，知らない研究者同士で本について情報を交換し合ったりすることが可能になると考えられる。この際，サブPIDに基づいて利用者から寄せられる情報には，たとえ互いに知らない者からであっても，前述した半匿名性ゆえの信憑性が確保されている。PIDシステム導入下での図書館には，こういった本を介しての利用者のコミュニケーションをサポートするような，新しい視点でのサービスの提供が望まれよう。具体的には，Web上で書誌情報とともに当該図書についての利用者のコメントが参照できるようにしたり，希望する利用者の間で，直接に個人が特定されないようなかたちでメールなどを通して情報のやり取りができるような環境を作ったりすることである。

以上のように，利用者と図書館とが協力しながら，日々の読書によって蓄積する情報が読書履歴として秩序立てて整理されることにより，また，一般には無味乾燥な書誌情報に読者の体験に基づいたコメントが付けられることにより，さらに，単なる本の流通から知的な交流へと発展していく流れを作ることにより，基となる情報に新たなる価値が付加された，すなわち付加価値の向上した情報を利用者は享受することができるようになる。このような，PIDシステム導入がもたらす安心・信頼をベースにした利用者の新しい自己表現の可能性と，それに依拠した固有のコミュニケーションの世界を支援していくのも，これからの図書館の役割といえるのではないかと考えている。

謝　辞

本研究は，財団法人日本証券奨学財団（The Japan Securities Scholarship Foundation）の平成18年度研究調査助成を受けて行ったものです。

1）例えば，東京地判平19・2・8判時1964号113頁「TBC個人情報漏洩」事件（原告団14名のうち13名其々に対し35,000円，残り1名に対し22,000円の支払いを命じた。控訴審の東京高判平19・8・28では，TBC側の控訴も，被害者側の附帯控訴も棄却され，第一審判決が維持された。控訴審の判決文は，〈http://homepage3.nifty.com/tbc-higai/kousai.pdf〉，（参照2007-10-12）．から読むことができる），大阪地判平18・5・19判時1948号122頁「Yahoo! BB顧客情報流出」事件（原告5名其々に対し，慰謝料として5,000円，弁護士費用として1,000円の，計6,000円の支払いを命じた），京都地判平13・2・23判自265号17頁「宇部市住民基本台帳データ流出」事件（原告3名其々に対し，慰謝料として10,000円，弁護士費用として5,000円の，計15,000円の支払いを命じた。その後，大阪高判平13・12・25判自265号11頁では，宇部市側の控訴を棄却。最判平14・7・11判自265号11頁では，宇部市側の上告を棄却，確定）。また，漏洩を引き起こした企業は，自主的にお詫びとして漏洩被害にあった顧客に対し，500～1,000円の金券を送るなどして対処している。

2）図書の貸し出し業務の新システム開発を委託された中部日本電気ソフトウェアの男性社員が，全利用者約133,000人の氏名，性別，生年月日，住所，電話番号，利用者カード番号，図書貸出記録などが入ったノートPCを自宅から盗まれた。図書館側の説明では，書名は登録番号が記録されており，書名自体は分からないようになっているとのことだった。この事件の後にも，2004年12月には近畿大学中央図書館利用者情報漏洩事件（職員共用のノート型パソコン7台が盗まれ，そのうち1台には，図書館を利用した学生など約40,000人分の個人情報が入っており，利用者の氏名，住所，生年月日，貸出図書名などが記載されていた），2005年2月には高槻市立中央図書館利用者名簿盗難事件（利用者89人の氏名，住所，電話番号，生年などが記された名簿が盗まれた）が起きている。最近でも，2006年3月末には越前市武生図書館でメールの誤送信により，図書館利用者152人のメールアドレスが流出する事件が起き，2007年7月には，杉並区の区立南荻窪図書館において，図書館利用者の個人情報が記載された紙（確認されたところでは，4人分の氏名，電話番号，年齢が記載されていた）の裏面を，利用者向けのメモとして提供していたことが利用者からの指摘を受けわかり，同区の立ち入り調査および個人情報の適正管理の指導が行われている。

3）図書館が取り組んでいる利用者のプライバシー保護について，例えば，「図書館の自由に関する宣言」（日本図書館協会1979年改訂〈http://www.jla.or.jp/ziyuu.htm〉，（参照2007-10-12）．）では，利用者の秘密を守ることを確認し，「図書館員の倫理綱領」（日本図書館協会1980年6月4日総会決議〈http://www.jla.or.jp/rinri.htm〉，（参照2007-10-12）．）では，利用者の権利を守る職業上の倫理を明確化している（塩見昇，山口源治郎編．図書館法と現代の図書館．日本図書館協会，2003，p.86.）。また，東村山市図書館設置条例第6条に見られるように，自治体独自に条例の中で明文化しているところもある（同p.9.）。

4）栗山正光．図書館コンピュータのセキュリティ対策．図書館雑誌．2004年11月号，p.832-834．などを参照。

5）公共図書館では，2000年4月の時点で，80％が貸出返却業務にコンピュータを使用している（日本の図書館2000年版．日本図書館協会.）。また大学図書館では，2005年5月時点で，実に99％以上が

コンピュータを導入している（平成17年度学術情報基盤実態調査結果報告（文部科学省研究振興局情報課）〈http://www.mext.go.jp/b_menu/toukei/001/index20/07012502/001.htm〉，（参照2007-10-12）.）。コンピュータ方式が主流となる以前は，ブラウン方式や逆ブラウン方式，中小レポート方式が多数を占め，それぞれの方式ごとに，貸出手順や貸出記録の保管および返却後の取り扱いが異なっていた。

6）例えば，独立行政法人国立環境研究所の環境情報センターの図書館では，指紋認証による管理システムが導入されており（〈http://www.nies.go.jp/kanko/nenpo/h12/3.html〉，（参照2007-10-12）.），茨城県那珂市の市立図書館では，非接触型の手のひら静脈認証がカード代わりに採用されている（〈http://www.lib.city.naka.ibaraki.jp/icity/browser?ActionCode=content&ContentID=1165626334411&SiteID=0000000000000&FP=search&RK=1187489918577〉，（参照2007-10-12）.）。

7）システムLSI研究センター（〈http://www.slrc.kyushu-u.ac.jp/index-j.html〉）で開発。浜崎陽一郎，安浦寛人．“PIDを用いた安全な社会システムの構想”．〈http://www.c.csce.kyushu-u.ac.jp/lab_db/papers/paper/pdf/2002/hamasaki02_2.pdf〉，（参照2007-10-12）．および，安浦寛人．“九州大学全学ICカード導入プロジェクト”．〈http://www.c.csce.kyushu-u.ac.jp/lab_db/papers/paper/pdf/2004/yasuura04_1.pdf〉，（参照2007-10-12）．などを参照。

8）利用したい図書がすでに他の利用者に貸し出されているような場合，利用者は貸出の予約をすることができる。図書館は，予約が入っている図書が返却されると，予約順に利用者に連絡を入れる。このサービスによって，利用者は図書の返却を確かめるために来館する必要がなくなり，人気のある図書でも順番を待てば確実に読むことができる。

9）コンピュータが導入されている図書館の実務的運用の指針となっている「貸出業務へのコンピュータ導入に伴う個人情報の保護に関する基準」（日本図書館協会1984年5月25日総会決議（〈http://www.jla.or.jp/privacy/kasidasi.html〉，（参照2007-10-12）.）では，本が返却されたら貸出記録をできるだけ速やかに消去しなければならないと述べられている。

10）人の思想や信条は，憲法によってその自由と尊重が明文化されている（憲法第19条「思想及び良心の自由は，これを侵してはならない。」）。

11）個人情報とプライバシーの関係については，新保史生．個人情報保護法に基づくバイオメトリクスの利用．情報メディア研究．第4巻，第1号，p.60．などを参照。

12）特集・個人情報保護と図書館．図書館雑誌．2005年8月号，p.500-527．または，坂井暉．図書館利用者のプライバシーの保護について．龍谷法学．2001，p.1-16．および，松本克美．名誉・プライバシー侵害図書の閲覧制限措置請求権について．早稲田法学．1999，p.575-596．などを参照。

13）ただし，個人情報を全く取得しないで物の貸出と返却を確保することも不可能ではない。例えば，保証金のような制度である。しかし，比較的規模の大きな図書館でこのような制度を導入することは，サービスを煩雑にさせるばかりかコストもかかるうえ実用的でない。

14）例えば，カードの再発行やカード申請が重複して行われていないかどうかなどの管理。

15）著作権法第31条は，図書館等において著作物を複製できる場合を定めている。その一つとして，「図書館等の利用者の求めに応じ，その調査研究の用に供するために，公表された著作物の一部分（略）の複製物を一人につき一部提供する場合」を挙げている。

16）例えば，AVルーム，セミナー室，会議室など。

17）悪意をもって他人のコンピュータのデータやプログラムを盗み見たり，改ざんまたは破壊などを行なったりしてコンピュータを不正に利用すること。多くはインターネットなどのネットワークを通じて外部から侵入し，悪事を働く。

18）無論，現状のように，図書館がサービスの提供に際し個人情報やプライバシー情報を取得すること自体は，法律や条令に抵触したりプライバシー権を侵害したりするものではない。しかし，例えば，個人情報の保護に関する法律の第15条は，個人情報の利用目的をできるだけ限定することを求め，第16条は，利用目的の達成の範囲を超えた個人情報の取り扱いを禁じている。また，独立行政法人等の保有する個人情報保護に関する法律の第3条第1項でも，個人情報の保有を，法令の定める業務を遂行するため必要な場合に限り，かつ，その利用の目的をできる限り特定しなければならないと定めている。よって，図書館が現状で取得している情報を今一度見直し，できるだけ取得する個人情報を限定してプライバシー情報に繋がるような情報をそもそも取得しないよう努めることは，このような法的要請にも沿うものといえよう。

19）プライバシー情報の中でも特に慎重な取り扱いが求められる情報。JIS Q 15001では，このような「特定の機微（センシティブ）な個人情報」として，a）思想，信条及び宗教に関する事項，b）人種，民族，門地，本籍地（所在都道府県に関する事項を除く），身体・精神障害，犯罪歴，その他社会的差別の原因となる事項，c）勤労者の団結権，団体交渉及びその他団体行動の行為に関する事項，d）集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項，e）保健医療及び性生活，を挙げて定義している。

20）たとえ改善の必要性が認識されていても，経済的な理由から，コンピュータが旧式のままであった

り，ソフトのバージョンアップができなかったりすることなどが考えられよう。

21) 注7参照。

22) PIDは，九州大学全学共通ICカードシステム（QUPID：KYU（Q）shu University Personal ID）の基本概念であり，現在ではMIID（Media Independent ID）と呼ばれる。MIIDとは，携帯デバイスの種類や通信の規格といったメディアに依存しない個人識別のことで，IDの種であるPIDと抽出プログラム，サブPID（PIDより生成され，サービスに使用されるID）と紐付けシステム，およびID管理システムより構成される（〈http://www.kyushu-u.ac.jp/pressrelease/2006/2006-04-07.pdf〉，（参照2007-10-12）.）。安浦寛人．“「九州大学新キャンパス」未来型情報経済インフラ構築プロジェクト”．〈http://www.slrc.kyushu-u.ac.jp/japanese/presentation/p_yasuura060313.pdf〉，（参照2007-10-12）．を参照。

23) 2005年夏より，新キャンパス（伊都キャンパス）の建物の入館管理について部分的に稼働開始され，2006年秋には，伊都キャンパスの学生および教職員約3000人にICカードが発行されている。

24) 例えば大学では，教務サービス（学生の証明書自動発行など），設備・施設の利用（建物の入館，図書館サービス，情報基盤センターの計算機利用サービスなど），防犯および安全管理，事務の情報化，入構管理，学生や職員に対する商用サービスなど。さらに，九州大学が2006年春から進めている「e-World FUKUOKAプロジェクト」（〈http://www.kyushu-u.ac.jp/pressrelease/2006/2006-04-07.pdf〉，（参照2007-10-12）.）では，このICカードの活用範囲をキャンパス内にとどめず，周辺の商業施設での支払いや交通機関利用に役立てることや，携帯電話やクレジットカードといった他の媒体との連携なども図られる（〈http://www.miid.kyushu-u.ac.jp/project.html〉，（参照2007-10-12）.）。

25) 実際にはPIDと提供されるサービスから適当な関数を用いてサブPIDが生成される。

26) こうした認証方法は，ICカードが耐タンパー性に優れていることから可能となる。耐タンパー性とは，ソフトウェアやハードウェアが備える，内部構造や記憶しているデータに対する外部からの非正規な手段による読み取りや解析を防ぐ能力のこと。

27) 例えば，大学や図書館の情報漏洩の中で，特に，お茶の水女子大学個人情報盗難事件（2004年6月），近畿大学・中央図書館利用者情報漏洩事件（2004年12月），秋田大学個人情報盗難事件（2005年4月），熊本学園大学個人情報盗難事件（2005年6月）では，建物内部に無断で侵入され，個人データの入ったパソコンそのものが盗難されている。また，ウィルス感染およびファイル交換ソフトを介する大学の情報流出では，近畿大学個人情報漏洩事件（2006年4月，「山田オルタナティブ」感染），甲南大学個人情報漏洩事件（2006年9月，ファイル交換ソフト「Share」），九州大学個人情報漏洩事件（2007年8月，ファイル交換ソフト「Share」）などがある。

28) 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－新たな電子図書館サービス構築に向けた個人情報保護モデル－”．〈http://www.dl.slis.tsukuba.ac.jp/DLjournal/No_27/4-ikeda/4-ikeda.pdf〉，（参照2007-10-12）．および，池田大輔．“PID：プライバシーを考慮したIDマネジメントシステム”．〈http://www.lib.kyushu-u.ac.jp/event/20060829/D_Ikeda.pdf〉，（参照2007-10-12）．などを参照。

29) 電子マネー（electronic money）。貨幣価値をデジタルデータで表現したもの。クレジットカードや現金を使わずに買い物ができ，インターネットを利用した電子商取引の決済手段としても使われる。専用のICチップに貨幣価値データを記録するICカード型電子マネーと，貨幣価値データの管理を行なうソフトウェアをパソコンなどに組みこんでネットワークを通じて決済を行なうネットワーク型電子マネーの2種類がある。

30) 買い物をした金額や来店回数等に応じてポイント（点数）を顧客に与え，次回以降の買い物でポイント分の金額を値引きするなどのサービス。デパート，スーパー，チェーンストア，ホテル，クレジットカード会社などで多く行われている。

31) 2007年3月18日には，首都圏の私鉄・地下鉄やバスで利用できる共通IC乗車券「PASMO」のサービスが開始した。さらに同日，Suica／PASMOの相互利用サービスもスタートし，首都圏在住者はSuicaかPASMOのどちらかを所有していれば，現金いらずで公共交通機関が利用できるうえに，駅や駅周辺の商業施設でもキャッシュレスで買い物できることになった。すでにJR東日本のSuicaは，カード型のSuicaとおサイフケータイ向けのモバイルSuicaを合わせて1900万枚以上の発行数があり，PASMOは今後3年間で800万枚以上の発行を目標としている（〈http://business.nikkeibp.co.jp/article/tech/20070312/120837/〉，（参照2007-10-12）.）。

32) 「Suicaカード」（〈http://www.jreast.co.jp/suica/about/type/index.html〉，（参照2007-10-12）.）や「無記名PASMO」（〈http://www.pasmo.co.jp/pasmo/type.html〉，（参照2007-10-12）.）は，購入時に個人情報の登録の必要が無い。一方，「My Suica」や「記名PASMO」の購入時には名前・性別・生年月日・電話番号などの登録が必要だが，これも，それらの情報が紛失時の再発行や払い戻しの際に備えて必要となることに着目すれば，実際に購入時に必要十分な情報とは，紛失時の再発行や払い戻しに際して初めて直接に個人が特定される情報に辿り着くことが担保された「第2レベル

の個人情報」（第3章第2節参照）で良いということになろう。なお，九州大学が進める「e-World FUKUOKAプロジェクト」の「e-Traffic」では，決済を鉄道系では行わず，ID認証と決済機能を共通のプラットフォーム化した決済システムを利用することにより，請求行為の簡略化を実現する（〈http://www.miid.kyushu-u.ac.jp/project.html〉，(参照2007-10-12).）。

33) 磁気カードの単価は100円程度であるのに対し，接触型のICカードは300～400円程度，非接触型のICカードは数千円程度する。さらに，ICカードの導入には，ICカード対応のリーダ／ライタ，リーダ／ライタに接続するネットワークや処理システムなど，ICカードを受け入れるためのインフラも加えて必要となる。

34) 国立国会図書館が，1995年の地下鉄サリン事件後に，裁判所の押収令状に応じて警察に延べ53万人分の図書館利用者の貸出記録などを渡していたことは，社会に大きな衝撃を与えた（坂井暉．図書館利用者のプライバシーの保護について．龍谷法学．2001，p.1-16.）。確かに「図書館の自由に関する宣言」にもあるように，図書館は令状を確認した場合には例外的に情報を提供することになっている。しかし，当該令状は具体性を欠き憲法違反の可能性が大きい。にもかかわらず，膨大な個人情報およびプライバシー情報が提供されたことは，国民の図書館に対する不信感を生む結果となった。さらに，北九州市立大学附属図書館の監視カメラ設置をめぐっては，学内だけでなく社会的にも議論となり，図書館のプライバシーへの配慮に一抹の不安を抱かせたのも事実であろう（西河内靖泰．公共図書館への防犯カメラ（監視カメラ）設置の現状と課題．図書館雑誌．2004年11月号，p.835-837.）。

35) 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－”．ディジタル図書館．No.30，p.62-71，Mar.2006.

36) プライバシー権は，ウォーレンとブランダイスによって1890年，一人で放っておいてもらう権利として初めて提唱された（Warren and Brandeis. The Right to Privacy. 4 Harv. Law Rev. 1890, p.193.）。日本の裁判例では，1964年の「宴のあと」事件以降，プライバシー権について言及されるようになり，その概念を実質的に承認している。ただし，権利をどのように定義するかでは，i）私生活への侵入・私事の公開をプライバシー権侵害とする立場，ii）個人の自己情報へのコントロール権を認め，その侵害をプライバシー権侵害とする立場，iii）私事についての自己決定権をプライバシー権とする立場，iv）宗教的または心の静穏をプライバシー権の保護の対象とする立場，など学説は多岐に渡る（竹田稔，堀部政男編．名誉・プライバシー保護関係訴訟．青林書院，2001，p.129.）。なお，プライバシー権の対象となることがらは，一般的に，①私生活上の事実又は事実らしく受け取られるおそれのあることがら，②一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められることがら，③一般の人にいまだ知られていないことがら，と解されている（東京地判昭39･9･28判時385号12頁「宴のあと」事件判決より）。

37) プライバシー権の誕生の地アメリカでは，1960年代に入り，コンピュータが普及するのを受けて，自己の情報をコントロールする権利として，より積極的に解されるようになっている（五十嵐清．人格権法概説．有斐閣，2003，p.195.）。日本では，1980年代から，自己情報コントロール権という言葉を直接には用いないものの，その旨の主張がなされるようになり，裁判所も，「逃亡」事件（一審：東京地判昭59･10･30判時1137号29頁，控訴審：東京高判昭63･3･24判時1268号15頁）や，「逆転」事件第一審判決（東京地判昭62･11･20判時1258号22頁）などにおいて，そうした概念への前向きな姿勢を示している。特に近時では，住民基本台帳ネットワークシステムの差止めなどを求める訴訟において盛んに主張され，「住基ネット制度にはデータマッチングや名寄せに利用される危険があるなど個人情報保護対策に欠陥がありプライバシー権（自己情報コントロール権）を侵害する」とした裁判例（大阪高判平18･11･30判時1962号11頁）や，「住基ネットからの離脱を求める原告らに対して適用する限りにおいて改正法の住基ネットに関する各条文は憲法13条に違反する」としてシステムの運用差止めを認容したケースもある（金沢地判平17･5･30判時1934号3頁，ただし，控訴審の名古屋高金沢支判平18･12･11判時1962号40頁では，システムの運用差止めの請求は排斥された）。また，日弁連などでは，自己情報コントロール権を，「自己の情報が予期しない形で，あるいは無限定に収集･管理･利用･提供されることを防止し，自己の情報がどこにどのような内容で管理され，誰に利用･提供されているかを知り，これら管理された情報について誤りがあれば，これの訂正を，また不当に収集された情報については，その抹消を求めることができる」権利として，積極的に位置づけている。一方，定義や射程が不明確な自己情報コントロール権に対しては，裁判例や学説において，批判的または慎重な立場も見られる（竹田稔，堀部政男編．名誉・プライバシー保護関係訴訟．青林書院，2001，p.132-139.）。

38) 独立行政法人等の保有する個人情報保護に関する法律の第4章では，「開示，訂正および利用の停止」（第12条～44条）が定められている。

39)「プライバシーとは，個人，グループまたは組織が，自己に関する情報を，いつ，どのように，ま

た，どの程度他人に伝えるかを自ら決定できる権利である」(Alan F. Westin. Privacy and Freedom. 1967, p.7.)。このWestinの見解は，アメリカにおける各種のプライバシー法に影響を与えている。

40) 注22参照。

41) 例えば，サブPIDによって，Web上にある読書履歴にアクセスするIDとパスワードを取得する。Web上の読書履歴には利用者の名前は表示されないものとする。さらに，いつまで読書履歴を残しておくかも利用者が選択できるようにするとよい。

＜2007.10.18 受理 あんどう なほこ 九州大学法学研究院学術研究員（協力研究員），いけだ だいすけ 九州大学システム情報科学研究院准教授＞

Nahoko ANDO, Daisuke IKEDA

Development of library services using a new identification and authentication system: a study of library personal information management

Abstract: As incidents of identity theft become more frequent, libraries are becoming more concerned with ways to protect the personal information and privacy of their users. They must begin by asking themselves whether the library's current system of personal information management is really performing adequately, and then consider how it would compare to the way they could manage personal information using the innovative personal authentification system Personal ID. Furthermore, the authors posit that by implementing this new system, more respect is given to the library users who are in the position of controlling information, and this in turn provides a framework for developing user-centered services in which library users are able to take the initiative themselves.

Keywords: personal authentication / personal information management / identity theft / Personal ID System, MIID (Media Independent ID) / library users / library service / personal information / privacy / personal history