# ネットワーク上での情報統合に対するプライバシー保護システム

金田 重郎 ・ 本村 憲史 ・ 橋本 誠志


## あらまし

ネットワーク上に溢れている個人情報は、デジタル化されているが故に、統合され、個人のプライバシーが侵害される恐れがある．情報統合を視野に置くプライバシー保護法制は、欧米には存在する。ドイツ身分証明書法は、個人IDによる情報統合を禁止している。民間部門に対するプライバシー保護法制自体が存在しないわが国と比較すれば、このような法律があるだけでも、西欧諸国の状況は大きく異なっている。しかし、これら既存の法律で想定されているのは、キー属性（いわゆる国民背番号等）による統合である。キー属性でなくても、複数属性を併用すれば、結果として、キー属性として利用できる。その結果、データ主体・データ管理者の予知範囲を超えて侵害が発生する恐れがある。情報統合によるプライバシー侵害は、個々のデータ管理者の善良なる管理監督のみでは防ぎ得ない。わが国でも、情報統合を前提とする法制度の確立と、併せて、データ主体が個人情報の存在を常に把握し得る、個人情報流通管理システム／データ監察官の設置が必要と思われる。


## １．はじめに

わが国では、プライバシーの保護に対する意識が薄く、総合的なプライバシー保護規制は存在しない。その上、インターネットの普及により、WWW上のホームページ（以下HP）の情報を収集・統合することによって、個人のプライバシーが侵害される恐れが生じている。本稿においては、ネットワーク上の情報を統合することよって生まれる新しいプライバシー侵害の形態を示し、更にそれがプライバシー保護規制のないわが国で起こった場合の特有の問題を具体例によって明らかにする。そこから今後のプライバシー保護規制の在り方を考察する。

以下、第２章では、プライバシー保護制度の流れを概観する。わが国では、民間部門を対象とするプライバシー保護法制が存在しないことを、欧米と比較して明らかにする。本章は、プライバシー保護法制にあまり詳しくない読者へのイントロダクションを兼ねている。

次に、第３章では、HP上の個人情報を統合することによるプライバシー侵害の危険を示す。本論文の主要な主張点である。とりわけ、民間部門に対するプライバシー保護法制の存在しないわが国では、民間の名簿業者（いわゆる「名簿屋」）の存在により、プライバシー侵害の危険が増大していることを、簡単な実験・数値的解析を交えて明らかにする。

続いて、第４章では、情報統合に関する諸外国（特にドイツ）の法制上の扱いについてまとめる。情報統合への配慮は、ヨーロッパ諸国に存在するが、キー属性（国民背番号のように、当該属性値で、一意に個人が特定できるものを言う。）のみを念頭においた法制度となっている。しかし、第３章の実験が示すように、キー属性のみではなく、複数の属性を併用することにより、事実上、キー属性のように利用できる。この種の問題に対して、ドイツ法制、ならびに、ガイドラインは何ら考慮していないことを明らかにする。

さらに、第５章では、上記の情報統合までも視野にいれたプライバシー保護のための対策を示す。法律制定自体について論ずることは研究

論文の範囲を超えるので、本論文では、デジタル署名を用いた、プライバシー情報の登録機関のシステム構成を提案する。本章の理解には、デジタル署名とCA証明書のごく基本的な知識を前提とする。

最後に、第６章では、本論文の結論をまとめる。

## ２．プライバシー保護制度

本章では、プライバシー保護制度の流れを文献［堀部88、堀部96］に従って整理する。

### ２．１　プライバシー保護制度成立までの流れ

1890年にウォーレンとブランダイスが、「プライバシーの権利」という論文を『ハーバード・ロー・レビュー』に発表し、プライバシー権を「ひとりで放っておいてもらう権利」として定義付けて以来、プライバシー権は、「私的」生活上の利益又は自由の権利として、私法上、特に不法行為法上の保護法益として発展してきた。

しかし、その後1960年代中頃からのコンピュータの発達により個人の情報が大量に蓄積、処理されるようになると、データ主体である個人と全く関係のないところでその全体的イメージが作り出されるのではないかと言ったことが指摘されるようになった。その為、プライバシー権を従来の受動的な（「私的」情報を公開させない）権利から、能動的な（自己情報がどの様に利用されているかを知る、また間違っていれば訂正できる）権利として捉えるべきであることが、A・ウェスティンやA・ミラー等によって提唱されるようになり、そこからプライバシー権を「自己に関する情報の流れをコントロールする権利」と捉えるいわゆる「自己情報コントロール権」が生まれた。

そしてこれらの権利の保護には、⑴プライバシー保護を結果不法から考えないこと、⑵秘匿性の強弱を一応捨象して個人情報全てを一応権利の射程内に捉えること、⑶個人情報の収集・蓄積・利用の全ての過程に対して、防御的でない積極的・能動的な性格を付与すること、といった要請に応えることが必要不可欠であるとして、「自己情報コントロール権」を保護法益とするプライバシー保護法やデータ保護法が、1974年アメリカにおいて制定された「プライバシー法（Privacy Act of 1974）」を皮切りに欧米を中心とした世界各国において制定された。

但し、これら法律は、それぞれの国内事情を反映した独自の規制対象、規制方法を持つため、多くのばらつきみられた。そして、この問題は、個人情報の国外処理規制条項を有するヨーロッパ各国と、世界規模の情報ネットワークを保有する情報産業を抱えるアメリカとの対立といった形を取って現れた。その為、1970年代の終わりには、その調整をOECD（経済開発協力機構；Organization for Economic Cooperation and Development）に委ねた。これにより、OECDは、1980年に「プライバシー保護と個人情報の国際流通についてのガイドラインに関する理事会勧告」（以下OECD理事会勧告）を採択した［OECD80］。

### ２．２　OECD理事会勧告

上記のOECDによって示されたガイドラインは現在の世界のプライバシー保護の共通の原則となっている。但し、この原則に基づく制度化だけでプライバシー保護が達成されるのではなく、あくまでミニマム・スタンダードである。

**【OECD理事会勧告８原則】**

以下にOECD理事会勧告の和訳[1]は、その８原則のみを抜き出すと以下のようなものである。

**収集制限の原則：**個人データの収集には、制限を設けるべきであり、いかなる個人データも、適法かつ公正な手段によって、かつ適当な場合には、データ主体に知らしめ又は同意を得た上で、収集されるべきである。

**データ内容の原則：**個人データは、その利用目

[1] この８原則の和訳は、ECOMプライバシー問題検討ワーキンググループの訳をECOMホームページから引用させて頂いたものである［OECD80］。

的に沿ったものであるべきであり、かつ利用目的に必要な範囲内で正確、完全であり最新なものに保たれなければならない。

**目的明確化の原則：**個人情報の収集目的は、収集時よりも遅くない時点において明確化されなければならず、その後のデータの利用は、当該収集目的の達成又は当該収集目的に矛盾しないでかつ、目的の変更毎に明確化された他の目的の達成に限定されるべきである。

**利用制限の原則：**個人データは、第９条により明確化された目的以外の目的のために開示利用その他の使用に供されるべきではないが、次の場合はこの限りではない。(a)データ主体の同意がある場合、又は、(b)法律の規定による場合

**安全保護の原則：**個人データは、その紛失もしくは不当なアクセス・破壊・使用・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

**公開の原則：**個人データに係る開発、運用及び政策については、一般的な公開の政策が取られなければならない。個人データの存在、性質及びその主要な利用目的とともにデータ管理者の識別、通常の住所をはっきりさせるための手段が容易に利用できなければならない。

**個人参加の原則：**個人は次の権利を有する。

(a)データ管理者が自己に関するデータを有しているか否かについて、データ管理者又はその他の者から確認を得ること。

(b)自己に関するデータを、(I)合理的な期間内に、(II)もし必要なら、過度にならない費用で、(III)合理的な方法で、かつ、(IV)自己にわかりやすい形で、自己に知らしめられること。

(c)上記(a)及び(b)の要求が拒否された場合には、その理由が与えられること及びそのような拒否に対して異義を申立てることができること。

(d)自己に関するデータに対して異義を申立てること、及びその異議が認められた場合には、そのデータを消去、修正、完全化、補正させること

**責任の原則：**データ管理者は、上記の諸原則を実施するための措置に従う責任を有する。

また、現在においてはこのOECD理事会勧告によるプライバシー保護原則の適用範囲を、さらに広範囲にかつ明確に規定したガイドラインとしてEU指令がある［EU95］。この指令は、定義において、「『個人データの処理』を自動的な手段であるかどうかに係わらず個人データに対して行われる作業又は一連の作業を意味するものとする。」（第２条ｂ項）と規定するなど、従来のガイドラインよりも広範囲にわたる個人情報の保護を求めている。その上、この指令はその名称が示す通り、個人情報のEU域外の第三国に対する移動に対しても規定していることからも、今後の個人情報保護とデータ流通の世界的なガイドラインとなると考えられる。

## ２．３　わが国におけるプライバシー保護政策

わが国のプライバシー権は、1959年の「宴のあと」事件によってその最初の一歩を示す。この事件は、プライバシー権という、過去に争われたことのない新たな権利のため各方面から大きな注目を集めたが、東京地方裁判所判決において、「私生活をみだりに公開されないという法的保障ないし、権利」としてその権利を認めた。この事件をきっかけにして1960年代にはわが国においてもプライバシー権が活発に議論されるようになったが、それはあくまでプライバシー権を「ひとりで放っておいてもらう権利」とする伝統的プライバシー権に関する議論でしかなかった［堀部88］。

1980年代に入るとこの様な閉塞的な状況に変化がみられるようになる。その最大の原因は、前節において示したOECD理事会勧告の採択である。1981年１月から1982年７月にかけて行政管理庁においてプライバシー保護研究会が開催された。そこでは「個人情報処理に伴うプライバシー保護対策について新たな制度的対応が必要」であることを明確化し、10項目の具体的方

策を示した。この方策はOECD理事会８原則に則って打ち出されたものである。しかし、「自己情報コントロール権」を法制度的に確立するための総合的なガイドラインを示したことの意義は大きかった。

そして、1987年度の行革大綱において「行政機関の保有する電子計算機処理に係る個人情報の保護の制度的方策については、法的措置を講ずる方向で、その為の具体的検討を行う。」とし、1988年に「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が成立する。本法律が、わが国における唯一のプライバシー保護法制である[2]。

また民間企業における個人情報の保護については、1987年に(財)金融情報システムセンター（FISC）が、「金融機関等における個人情報保護のための取扱指針［FISC87］を、1988年には(財)日本情報処理開発協会（JIPDEC）が、「民間部門における個人情報保護のためのガイドライン」を策定した［JIPDEC88］。そして、更に、JIPDECのガイドラインは、1989年の通商産業省の情報化対策委員会個人情報保護部会での審議の後、「民間部門における電子計算機処理に係る個人情報処理保護について（指針）」として公表され、業界関係者に同指針の遵守を通達した。その後EU指令への対応を念頭に、同指針の改訂作業を行い、1997年１月に新たなガイドラインを発表している。

それ以降、通産省や郵政省などにおいて行政指導や、通達によって自主規制の方向で個人情報の保護対策は行われている。これらのガイドラインの中で、主要と思われるものを表１に示す。また、ガイドラインにそって、何種類かのプライバシーマークの発行が行われているが、1998年末現在、登録している団体の数もすくなく、一般に広く知られているとは言い難い［Mark, JISA］。

## ２．４　わが国の個人情報保護制度の問題点

以上の様に、わが国でも、個人情報保護制度の一定量の確立はみており、また、通産省を初めとするガイドラインについても、その果たした役割も大きいと思われる。しかし、世界におけるプライバシー保護制度と比較すると、その原則を同じOECDの理事会勧告に求められるとはいえ、現状では大きな差異がある。以下にわが国の保護制度の問題点を示す。

（１）目的の相違（プライバシー保護を目的とせず）

諸外国立法例において、プライバシー保護制度の目的はスウェーデン法「個人のプライバシ

**表１　日本国内の主要ガイドライン**

| ガイドライン名称 | 対象者 | 制定時期 | 制定組織 |
|---|---|---|---|
| 金融機関等における個人情報保護のための取り扱い指針 | 金融関係 | 昭和62年 | 金融情報センターガイドライン |
| 民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン | 民間企業等 | 平成１年策定,<br>平成９年改訂 | 通産省/JIPDEC |
| 発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン | 発信者情報通知サービスの利用者 | 平成８年 | 郵政省 |
| 情報サービス産業個人情報保護ガイドライン | 情報サービスに係る事業を営む者 | 平成９年 | 社団法人情報サービス産業協会 |
| 電子ネットワーク運営における「個人情報保護に関するガイドライン」 | インターネット運用・サービス提供業者 | 平成９年 | 電子ネットワーク協議会 |
| サイバービジネスに係る個人情報の保護に関するガイドライン | 電子商取引 | 平成９年 | サイバービジネス協議会 |

[2] 実際には、福岡県春日市、神奈川県等、地方自治体の中には、プライバシー保護条例を設けている場合があるが、本論文ではその詳細は割愛する［春日96、神奈川98］。但し、春日市の例でも、対象は市が所有する個人情報に限定される。

ー」の保護、アメリカ法「個人のプライバシーの侵害に対する個人の保護」、ドイツ法「保護に値する当事者の利益」の保護 、そしてフランス法「人間の同一性、私生活、公的および私的自由」等となっており、明確にプライバシーの保護を挙げている。

これに対して、わが国の個人情報保護法は、行政における電子計算機処理の分野の拡大を踏まえた「行政の適正運営」を第一の目的とし、「個人の権利利益」についても、「自己情報コントロール権」の内容の一部の権利しか認めていない点や、プライバシー権の保護を明確に示していない点からも、この個人情報保護法がプライバシー保護のための他の国におけるプライバシー法などと目的を同じにする制度であるとはいえない。

この様な個人情報保護法に対する「行政の適正運営上の個人情報の適切な取り扱い」だけを重視し、明確なプライバシー保護規定を行わない姿勢は、一部の自治体条例を除き、民間部門ガイドラインや、住民基本台帳法の情報化に伴う一部改正案においても共通してみられることからも、現在のわが国の個人情報保護制度は、その目的において既に諸外国のプライバシー保護制度とは根本的な違いがある。

（2）適用範囲の相違（政府機関のみが対象）

本来、情報主体の権利侵害の態様は、処理機関（官庁・民間）・処理形態（自動処理・マニュアル処理）を問わず共通である。その為、諸外国においては、一つの法律を公民両部門に適用する例が数多くみられ、たとえ、公的部門と民間部門を異なる法律によって規制する場合においても、その時期はほぼ同時期にプライバシー権の保護という同じ原則に則って成立している。また、マニュアル処理も含めた法制化がなされており、現時点において自動処理のみにしか規定のない国においても、EU指令への対応もあり、OECD加盟国の日本を除くほとんどの国々において、EU指令の国内制度の発効期限である1998年の10月までには、マニュアル処理を含むプライバシー法案が成立（もしくは改正）していると考えられる。

しかし、わが国の制度的対策は、各対応省庁によってそれぞれの場合に分割され、限られた範囲内における個人情報の保護の達成のみを目的とする。その為、現在のわが国における個人情報保護政策は、国の個人情報保護法は総務庁主導において制定され、地方自治体に関しては自治省、民間企業活動に対する個人情報保護は通産省、信用情報等に関しては経済企画庁、そしてインターネットなどの新たなメディアにおける個人情報保護は、郵政省というように 、プライバシー保護の原則達成のための総合的政策ではなく、それぞれの状況に応じた別個の対応策として捉えられ、検討されている。

従って、個人情報保護法は、わが国唯一の個人情報保護に関する法律であるにも係わらず、民間部門に対する規定はなく、公的部門の範囲である地方公共団体においてさえもその適用はなされていない。

その上、処理形態においても、その対策は一部地方自治体を除いては、自動処理に限られた形で進められ、未だマニュアル処理に対しての対応策は全く打ち出されておらず、マニュアル処理に係わる唯一の規定は、公務員の守秘義務だけである。

（3）保護方法の相違（データ管理者の処罰規定なし）

わが国の個人情報保護法は、その保護の方法においても諸外国と大きな違いがある。特に問題と考えられるのは、データ主体の権利に関わる問題と、ファイル設置の事前通知とそれに係わる監督機関に関する規定と、罰則規定という実際の制度の施行に関わる問題の二つである。

**・個人の権利に関わる規定に関する問題：**

「自己情報コントロール権」を保護法益とするプライバシー保護法において、アクセス権と訂正権を権利として保障することは、この法律の本質的な目的といえる。わが国の個人情報保護法においては、アクセス権は、「情報開示請求権」として第13条に明確に規定しているものの、「訂正権」に関しては、「訂正の申し出」として第17条に「保有機関の長は、第13条第3項の規定による開示を受けた者から、書面により、開示に係る処理情報の訂正等の申出があったときは、（中略）ファイル保有目的の達成に必要な範囲内において遅滞なく調査を行い、その結果を申出をした者に対し、書面で通知するものとする。」とされるに

とどまり、権利としての明確な規定はされていない。

**・制度の施行に関わる問題：**

まず、ファイル設置の事前通知については、わが国におけるその規定はファイルが設置された後の総務庁による公示義務を果たすためだけの規定にすぎず、ファイルに対しての事前審査やチェック等といった事柄に関する規定がないために、総務庁の位置づけが、本来のプライバシー保護制度の監督機関ではなく単なる受理機関としての意味合いが強くなる。その結果、実際の個人情報制度における義務を果たさせる拘束力が非常に弱いものになってしまう。

また、この監督機関を行政機関内の総務庁と定めていることもこの法律の実効性を失わせる大きな要因となる。諸外国においては、スウェーデンのデータ検査委員、ドイツのデータ保護監督官等のように、第三者的な監督機関をたてるか、もしくは行政機関の所属であっても独立した権限を与え、その法律の実効性の確保を図っているのに比べ、自らも規制される立場にある総務庁において、個人情報保護法の実効性の確保を図るのには限度があると考えられるからである。

次に、罰則規定についてであるが、わが国の個人情報保護法は、情報開示請求における不正行為についてしか規定されておらず、諸外国におけるファイル管理者と利用者に対しても罰則規定を設け、しかもファイル管理者（及び利用者）に対する規制を重視するプライバシー保護法とは異なる。これは、個人情報保護法が行政機関を対象にしているため、データ管理者やデータ利用者の不正については、国家公務員法の守秘義務によって十分責任を問えるとの判断があるからである。

しかし、現在のような情報化時代においては、データ管理者によって引き起こされる犯罪の方が一般的であり、その損害も深刻なものになる。その為、データ管理者に対しては大きな責任を課せられるべきであり、世界的な流れはこれに対応するものとなっている。にもかかわらず、わが国の管理義務違反に対する罰則が国家公務員法の罰則規定だけというのはあまりにも軽微であり、その点から考えても個人情報保護法にファイル管理者（及び利用者）に対する罰則が存在しないことは非常に問題である。

## 3．情報統合によるプライバシー侵害

以上見て来たように、わが国の個人情報保護制度は、本来の意味においてのプライバシー保護制度としては機能しない。一方、インターネットの広範な普及とともに、ある特定個人の情報が、断片的に、複数のHPで公開されるようになっている。この様な状況では、インターネット上の情報を統合することにより発生する新たなプライバシー侵害の可能性が生じている。そして、前述の様なプライバシー保護法制の不備なわが国では、より深刻な問題となる。以下、まず、情報統合によるプライバシー侵害について示す。

### 3．1　発生形態

HP情報を利用したプライバシー侵害は以下の手順で行われる。概念化して図１に示した。

（**Step I**）サーチエンジンでターゲットとなる人物Aに関する情報を検索。
（**Step II**）各情報（ab, ac, ad）を収集。
（**Step III**）これらの情報を統合（a, b, c, d）し、ターゲットAのプライバシーを侵害する程の情報を得る。

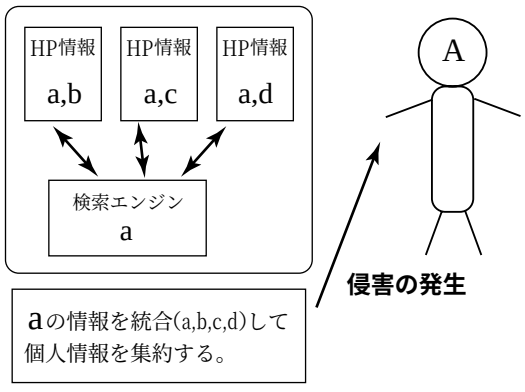


**図１　侵害のモデル**

即ち、個々のホームページの情報は、「aとb」「aとc」「aとd」と言ったように、限定されていても、それらを総合すると、結局、「aとbとcとd」なる全プロフィールが判明してしまっている。

一般には、この時、「a」はキー属性（国民背番号のように、その値で、一意に当該データ主体が特定できるものを言う）［鈴木98］でなければならないと思われがちである。しかし、後述するように、この際、「a」は、国民背番号のようなキー属性である必要はない。それが、本論文の主要な論点のひとつである。

## 3.2 問題点

インターネット情報の統合によって起こるプライバシー侵害には、従来からインターネットにおける問題点として指摘される準拠法と管轄権の問題[3]や、オープンネットワークの特性からの従来のプライバシー保護規制における規制対象となる情報管理者の不在の問題も含まれる。しかし、ここにおける最大の問題は、それぞれにおいては合法的なHPを統合的に利用して、プライバシー侵害が行われた場合、HPの責任を問えるのか、という問題である。

しかも、たとえ責任を問うとしても、該当人物の個人情報を掲載したHP全てに責任を問うのか、それとも時間的にみてプライバシーを侵害するに至る最後の情報を掲載したHPのみの責任を問うのかといった、責任の所在の範囲の問題までもが含まれる。しかもわが国においては、これ以外にも、総合的プライバシー保護規制がないことから更なる問題が指摘される。

上記の問題は、事実上、プライバシー保護制度のないわが国では、さらに大きくなる。インターネットの広範な普及とともに、ある特定個人の情報が、断片的に、複数のホームページ（以下、HPと略記する。）で公開されるようになっている。この様な状況では、情報を統合することにより発生する新たなプライバシー侵害の可能性がある。

特に問題なのは、各々が合法的なHPを統合的して、プライバシー侵害が行われた場合、HPの責任を問えるのか、という問題である。以下、具体的に示す。

## 3.3 侵害実行の具体イメージ

図2には、侵害実行のより具体的な例を示した。以下、順に説明する。

**前提：**

女性Aは、大学の助手であり、最近、県HPに、受賞者として写真と名前のみが掲載された（自宅住所、自宅電話番号、年齢、生年月日等は掲載せず、プライバシー保護に配慮している）。

但し、Aに関する情報は、所属大学HPにおいて、出身大学、加入学会が掲載されていた。

**侵害の実行：**

県広報HPのAに興味を持った人物Bが、

（**Step 1**）goo等のサーチエンジンでAの氏名で検索し、

（**Step 2**）ヒットした大学や、学会のHPから、Aの出身大学、所属、加盟学会等の情報を得る。

（**Step 3**）これにより、県広報に載った女性が（Step 2）の助手と分かる。

（**Step 4**）名簿屋に行き大学職員名簿から自宅住所、電話番号等が判明する。そして市役所で住民票を閲覧すれば、（閲覧規制があれば、適当な人物に成りすまし、戸籍や住民票の写しを請求）

（**Step 5**）Aが一人暮らしであることや、大学のHP中に表示されたカリキュラムから自宅にいない時間まで割り出せる。

ここで注意しなければならないのは、各ホームページがそれなりにプライバシーに配慮して

[3] 1台のサーバマシンを世界中からアクセスできるインターネットの世界では、どこの国の法律を適用するか（準拠法）？そして、問題を生じたときに、どこの国の裁判所が事件を審理するのか（管轄権）が分からなくなることしばしば生じる。

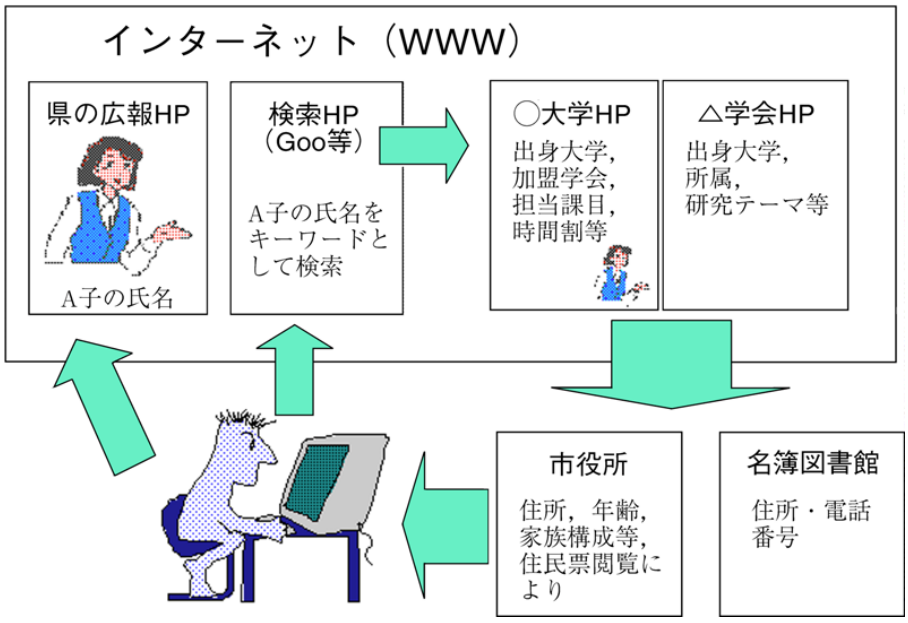


**図２　情報統合による侵害実行例**

いる点である。実際、名前だけで、このような情報統合が可能なのであろうか？この点を明確にするために、若干の実験と解析を行った。

## ３．４　数値的評価

### ３.４.１　検索サーバによる検索実験

まず最初に、著者らの周囲に実在する氏名を利用して、上記の手法で、個人情報の検索を行った。

結果を表２に示す。人物A、D、F、Gについては、全てターゲットである本人の情報が検索された。従って、検索されたHPの情報を統合して、当該個人の全体像を把握できる。

ありふれた苗字であっても、名前と組み合わされると、意外に特定が可能なようである。一方、人物B、Cは、殆どがターゲット人物以外の情報が収集されてしまった。苗字、名前共にありふれた氏名については、予想された事ではあるが、殆どが他人の情報であった。

### ３.４.２　統計的な推計

次に苗字の分布を持ちて、解析を行ってみる。

日本ユニバックによれば［UNIVAC71］、約100の苗字で苗字全体の37%を占める。100万人の被検索対象がある場合に、上位100種の苗字で、一つの苗字に平均

$$370{,}000 \div 100 = 3{,}700$$

人がひしめく。一方、名前の分布は、苗字よりも分布が広いと思われるが、安全側に取って、苗字と同様とする。この場合、上位100種の名前と苗字の組み合わせで、特定氏名を持つ同姓同名の人数は、

$$3{,}700 \times 3{,}700 \div 1{,}000{,}000 = 13.69$$

人と少ない。しかし、これでは、情報統合はで

**表２　実在人物による検索実験（検索はgooによる）**

| 氏名 | 検索結果数 | 該当情報数 | 結果判定 |
|---|---|---|---|
| A | 7 | 7 | ○ |
| B | 89 | 3 | × |
| C | 34 | 2 | × |
| D | 15 | 15 | ○ |
| E | 5 | 3 | △ |
| F | 7 | 7 | ○ |
| G | 25 | 25 | ○ |
| H | 53 | 10 | △ |

きない。

一方、苗字の500位から1000位までの人数は、全体の10.79%である。この場合、同一の性を持つ人数は、

$$0.1079 \times 1{,}000{,}000 / 500 = 215.8$$

人にまで減少する。従って、この500位から1000位にある範囲にある名前と、ありふれた100位までの苗字を組み合わせると、同姓同名の人数は、

$$215.8 \times 3{,}700 / 1{,}000{,}000 = 0.798$$

人となり、個人を特定できる確率が高い。実際の名前の分布は、さらに広がりが激しいものと思われ、被検索人数が100万人から増加しても、苗字又は名前の少なくとみ一方が多少珍しいなら、氏名による情報統合が十分に可能と思われる。

では、前述の（Step 4）はどの点において問題といえるのか。まず、名簿屋等の民間業者における個人情報の二次利用の問題がある。名簿情報は、流通に何ら法的措置は講じられていない。次に、未だに戸籍や住民票といった個人情報そのものに対してさえ、制度的なプライバシー保護措置が弱いことも問題であろう[4]。

以上のようにわが国のプライバシー保護制度の未整備は、すでに顕在化している問題とともに、ネットワーク上のプライバシー侵害をもより深刻なものにする。諸外国並の総合的なプライバシー保護制度の成立が急務である。

## 3.5 わが国固有の問題点

この様にプライバシー保護規制がなされていないわが国においては、（前述の侵害の実行におけるステップ）（Step 4）の様に、ある程度、個人を特定できれば、収集可能な情報量も多く、実際にこの様なプライバシー侵害が行われやすい。

では、（Step 4）はどの点において問題といえるのか。まず、名簿図書館等の存在に代表されるような民間業者における個人情報の二次利用の問題である。わが国では、ある程度の特定さえできれば簡単に住所や電話番号が分かってしまう。しかもこの様な民間データベース業も電子マネーの普及によって、インターネット上においてサービスを行うことも想定され、ますます容易に、侵害者は、自らの名前／顔を明かさずに、情報を収集できる。

しかし、各種名簿の情報は、本来一般に公表を目的としたものとはいえず、JIPDECのガイドラインにおいても、公開情報とは考えにくいとしている。にもかかわらず、現時点においてこれらの流通に何ら法的措置は講じられていない。次に、未だに戸籍や住民票といった個人情報そのものに対してさえ、制度的なプライバシー保護措置を講じていないという行政機関の対応の甘さがある［三井98］。

現在、個人情報保護条例によってプライバシー保護の対策は一見進んでいるかに見える。しかし、戸籍や住民票の取扱は、戸籍法や住民基本台帳法のために保護条例の対象外とされ（現在その公開に規制をかける自治体も増えたものの）、原則として何人にもその請求を（住民票は閲覧も）認めており、戸籍・住民票がプライバシー保護の対象となる個人情報とは法律的には考えられていない。

以上のようにわが国のプライバシー保護制度の未整備は、すでに顕在化している問題とともに、ネットワーク上のプライバシー侵害をもより深刻なものにする。その被害を最小限にとどめるためにも、諸外国並の総合的なプライバシー保護制度の成立が急務である。

## 3.6 増大する個人情報の収集

以上見てきたように、インターネットでは、個々のホームページがプライバシーに配慮していても、それらの情報が統合されて、結果的に、侵害と呼ぶに足る情報が収集される危険がある。

[4] 名簿等については、プライバシー保護のために、一応、著作権の主張等を行い、プライバシーに配慮しているケースも多いようである。しかし、現在では、電子データで名簿屋にプライバシー情報が提供され、それが紙打ち出しで販売されているケースが多いのではないだろうか？この場合、名簿等に著作権表示をしても、紙への打ち出し結果から、その侵害を確認することは難しい。

しかし、ネットワーク技術の進展により、個人情報は大規模に蓄積されてゆく。具体的には、以下のような技術要素がある。

- **データマイニング技術：**購買データから、顧客を選別するデータベースマーケティングへの期待は大きい［江尻96、神山95］。また、これら顧客データを統合的に分析して、新たなマーケティング戦略をたてるデータマイニングへの期待も大きい［Fayyad96］。ポイントカード等を利用した、個人の購買記録の収集は、今後、更に広がる可能性が高い。当然、この種の顧客データは、名簿屋等の商品となることも予想され、また、データの集積先である名簿屋自身が、データの商品価値を高めるために、プライバシーデータの統合に乗り出して、統合結果を販売することも予想される。

- **HP数の増大とXML の登場：** HPの個数が増加するのみでなく、SGML（Standard Generalized Markup Language）［SGML95］の一種であるXML（eXtensible Markup Language）［XML 1, XML 2, XML 3］によって、データベースがインターネットを流通する。XMLは、今後のインターネットを支える最も重要な技術であるが、データベースがそのままインターネット上を流通することに他ならず、統合精度を向上させることが危惧される。

- **企業内ネットワーク化の進展：**電子メールのログはすべて保存されている。POPサーバ[5]管理者なら、容易に読み出し・検索が可能である。また、近年のイントラネット化に伴い、扶養、年休等の総務系処理もネットワーク化される。また、今後、社員用電話が構内PHS化された場合には、原理的に社員の位置情報がセンターに集約される[6]。また、社内のセキュリティ管理のため、カードによる認証（バッチシステム）が行なわれ、扉の開閉データはすべてセンターに送信・保存される可能性がある。これらはすべて個人情報である［平松98］［労働省］。

このため、例えば、ネットワークサーバ上のデータを統合して、労組役員や要注意人物の監視、不倫関係の摘出(電子メールでの不倫を思わせる連絡を抽出)が可能となる。総務系システムでは、同時に年休を取得する妻帯者と若い女性社員のペアを簡単にリストアップできる。しかし、彼と彼女は、たまたま同時に、あるNGOで奉仕活動をしていただけだったかもしれない。

何より問題なのは、「名簿屋」が、購買データや、インターネット上のデータ等を販売するようになる可能性があることである。最初から電子化されたデータは、買い手にとっても魅力的である。あるいは、名簿屋自身が、ここにのべる情報統合を実行して、データの付加価値を高めてゆくものと思われる。そして、民間部門に対するプライバシー保護法制のないわが国で、これらの行為をどこまで、法的に規制し得るかは疑問である。

但し、本来の目的であるEC（電子商取引：Electronic Commerce）やポイントカード等の、経済的利点を妨げてはならない。顧客の購買行動を広く収集できれば、設計・製造・物流・資源回収のサプライチェーンを効率化・迅速化できる可能性がある。そして、このようなSCM（Supply Chain Management）により、企業の競争力を強化し、併せて限りある資源の有効利用を図る事は、経済活性化のためにも、「環境にやさしい持続できる経済的発展」にも重要である。

藤原は、プライバシー法と環境法の類似を指摘している［藤原97］。興味深い指摘である。

上記のような、多様なサービスが実現されるなかで、各々のサービスの利点を生かしながら、一方、プライバシーを保護し、しかも必要な官庁等の情報公開を進める必要がある。環境問題の解決には、情報公開が不可欠であるとの議論もなされているようである[7]。どれをどう情報統合すると、プライバシーが漏洩するかの分析は容易ではない。これらを総合的に満足する個人情報流通と保護のあり方は現在未だ得られていない。

---

[5] 電子メールを発信・受信する専用のサーバコンピュータ。

[6] 今後は、社内電話がすべてコンピュータテレフォニー化し、LANですべての通話が処理される可能性がある。この場合も、PBXにくらべて社員間の通話ログ取得は容易なはずである。

[7] 以上の議論では、プライバシーは個人に関するもののみであるように論じてきた。しかし、企業等の法人にとっても、決済情報や、企業活動の詳細を統合されることは、法人にとってのプライバシー（秘密）を犯される危険をはらんでいる。

## 4. 諸外国の法制度

では、ここで、すこし目を転じて、海外の法制度が、情報統合に対して、どのような対策を考慮しているかを概観したい。具体的には、この種の配慮があるのは、ドイツを中心とするヨーロッパ諸国である［米丸97、藤原97、小澤98］。

### 4.1 EU指令

海外には、不十分ながらも、情報統合への配慮を行っている法制が存在する。1995年、ヨーロッパ連合（EU）は、1998年10月までの域内各国の法的対応を義務づけた、プライバシー保護のための指令「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」［EU95］を出した。EU指令は、今後の世界各国のプライバシー保護政策の指針となるものと考えられ、以下の通り、情報統合に関係した記述がある。

> 「個人データの処理」（処理）とは、自動的な手段であるかどうかに関わらず、個人データに対して……（中略）……開示、もしくは連結、ブロック化、消去又は破壊が含まれる。

上記「連結(combination)」のなかに、情報統合を含めるのが自然であろう。一方、最も進んだ法制度を有するのは、ドイツである。情報統合を意識した条文が存在する。次にドイツ法について紹介する。

### 4.2 ドイツにおける個人情報保護法制

#### 4.2.1 ドイツのIDカード

ドイツでは、住民の氏名、住所等の情報を記録したIDカードの携帯が義務づけられている［平松98］。IDカードには、各行政機関が住民に対してなした行政サービスの履歴を記録できる仕様のものがあり、これと国民背番号制が結合され、インターネットによる情報統合が絡めば、個人情報は丸裸同然となる。

しかし、1986年の身分証明書法の中で、IDカード記載事項は、専らIDカードを作成以外の目的では利用してはならず、使用後ただちに消去しなければならない(第３条第３項)。

一連番号は、電子計算機ファイルから個人情報を呼び出したり、データベースを結合するために利用してはならない(第４条第１項)。と規定している。キー属性であるIDカード番号の利用に歯止めをかけている。

また、IDカードの有効期限は10年（26歳未満は５年）として、更新時には、別番号を振って、個人識別に利用できないように配慮している点からも、立法時の配慮が感じられる

しかし、この法律は、あくまでIDカードに関するものであり、より、一般的なプライバシー保護は、次のテレサービスデータ保護法に見られる。

#### 4.2.2 テレサービスデータ保護法

1997年に制定されたこの法律は、テレサービスで流通する個人情報が加工、利用される際、データ主体がそのことを把握できない状況に鑑み、従来の個人情報保護法規を補完するために、制定されたものであり、「ユーザー・プロフィールの形成・開示の回避」を狙いとする。

取得された情報の分散保存を要求することで、ネットワーク上での情報統合によるユーザー・プロフィールの醸成に歯止めをかけようとの主旨である。本法のテレサービス提供者を対象とした規定の適用に、業務性の有無は関係しない。テレサービス提供者は、サービス提供に用いる技術においても、最低限 の個人情報で稼働するようシステムを構成する「省個人情報型システム」への転換を要求しているなど、興味深い。詳細は文献［米丸97、小澤98］に譲るが、情報統合に関して特徴的なのは、以下の部分である。

- **テレサービス利用データの抹消義務：**ユーザーのテレサービスへの接続その他利用について提供者が取得 した情報は、利用料金請求のために必要とされない限り、当該ユーザーの利用終了後、ただちに抹消されねばならない。そして、同一ユーザーによる多種のサービス利用に関して生じた個人データは、利用料金

請求目的以外に統合できない。

・**仮名よる利用履歴の蓄積：**利用履歴の作成は、仮名でのみ可能。当該利用履歴と仮名と本名の情報を同一に保存する事はできない。これは、誰のものかを抹消して、データを流通させようとするものである。

## 5．情報統合への対策

### 5．1　現行法制の分析

以上紹介したドイツ法の制定によっても、なお、準拠法の問題等を解決するための手段は提起されていない。しかし、マルチメディア法は、情報通信における企業活動促進のための出発点となる枠組みを提供した点で評価しうる。特に、個人と特定できる情報の消去を迫るドイツ法は、民間部門に対するプライバシー保護法制を持たないわが国とは大きな差がある。

しかし、情報技術的に考えると、多少の疑問を感じざるを得ない。以下に列挙する。

・**データ主体のプライバシー情報確認のための具体的手段の不明確さ：**ドイツマルチメディア法は、データ主体のプライバシー情報提供了承においても、マウスクリックの利用を忌避するなど、厳密である。しかし、具体的に、どこにどんなデータが存在するかを報知するシステムの構成については未検討である[8]。

・**キー属性による結合（JOIN）のみを想定して良いか？：**どの法制度でも、結合は、その属性値により一意に個人を特定できるキー属性を前提として考察している。しかし、氏名などという、非キー属性であっても、高い確率で、情報を統合できる。さらに複数属性の併用が効果的である。たとえば、7桁郵便番号と氏名を利用すると、対象となる母集団が、前述の100万人ではなく、1万人程度に低下する。抽出される人数の期待値は、上位100種の苗字でも、単一の苗字に僅か

$$3,700 / 100 = 37$$

人となり、上位100種の名前と苗字の組み合わせでも、

$$37 \times 37 / 10000 = 0.1369$$

人しかいない。つまり、複数属性を利用すると、ID番号なしに個人特定が可能と思われる。しかし、このような手法への配慮は、現行法制には見られない。

・同様な現象はインターネットでも存在する。例えば、インターネットユーザがプロバイダや企業内部のネットワークからインターネットへアクセスしている状況では、実際のクライアントマシンそのもののIPアドレスは、サーバー側には秘匿できる。しかし、ユーザ毎にプロキシサーバのIPアドレスは特定である。図3には、このユーザが、ある検索サーバから一般のホームページへとサーフィンした場合を模式化した。このケースでは、利用者はプロキシサーバのIPアドレス以外では識別できないが、時刻が正確なので、航空会社へのアクセス記録と、検索サーバへのアクセス記録は簡単に統合できる。これにより、氏名・住所が分かった人物の興味の範囲を簡単に検索サーバのアクセス記録から特定できる。つまり、IPアドレスとタイムスタンプの組み合わせがキー属性を構成している。この様な、非キー属性による統合への配慮は、現行法制には存在しない。

更に、日本では、業界団体ごとに独自の管理機関が存在し、個人の信用情報は、銀行→サラ金と言うように、業種を越えて交換される。しかし、登録された信用情報のその後の流通 について、利用者は、知る術もほとんど無い。

少なくとも社会制度の面からは、(1)情報統合そのものを禁止する事、(2)利用者が自己に関する情報を検索しやすくなる（個人情報に関する相談コーナー設置、ドイツの法制にあるデータ保護観察官制度の導入、サーバー会社の公的機

[8] W3Cコンソーシアムのプライバシー保護施策であるP3P［P3P］は、クライアント側での定型化された個人情報の準備と、マウスクリックによる承諾を前提としている。ここらにも、米国とヨーロッパの立場の違いが感じられる。

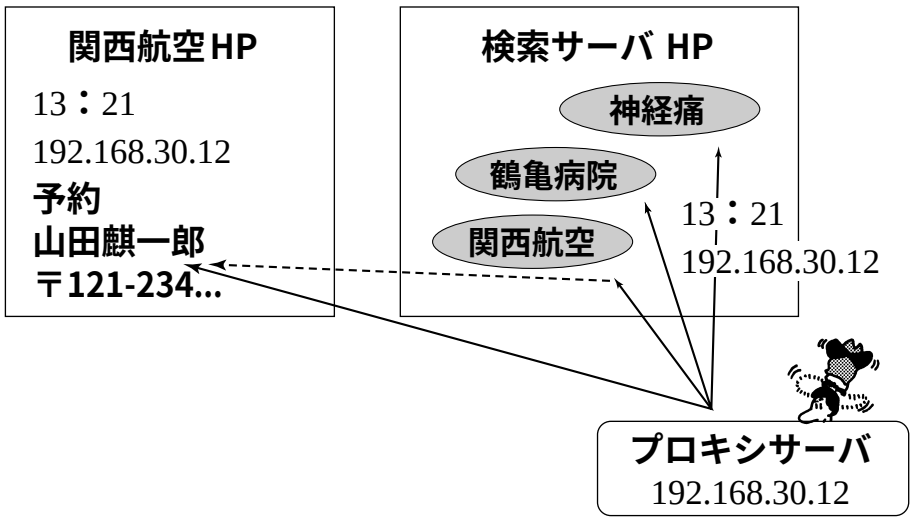


**図3　タイムスタンプによる情報統合**

関への登録義務とレイティング等）制度を考える必要がある。

一方、近年、名簿等がCD-ROM化される事も多い。たとえ、内部データを読み出す所まではやらなくても、CD-ROMのまま、システムの一部に組み込み、電子的な操作により、内部の情報を大量に取り出せる可能性を否定できない。更に、この様なシステムへの組み込み利用には、データベース著作権上の疑義があり、規制できたとしても、オペレータが画面上で、手操作により、情報を検索して販売する場合には、どこまでデータベース著作権でガードできるかについて疑問が残る。

CD-ROM形式の名簿については、掲載される個人に対して、情報統合による流出の可能性があることを警告するとともに、出版にあたっては、テキストコピー禁止や印刷禁止形式のPDF［PDF97］を用いて名簿を出版する等の配慮も必要と思われる。

## 5.2　個人情報流通管理システムの提案

情報統合によるプライバシー侵害を防ぐには、データ主体が、自己のデータの所在場所を知ることが重要である。所在が分かれば、開示請求でき、如何なる情報統合が可能であるかも判定できる。そこで、本節では、データ主体が認証したデータ管理者以外にはデータが流通せず、かつ、自分のデータがどこに存在するかを確実に認識できるシステムの一構成法を提案する。

### 5.2.1　前提条件

個人情報流通管理システム構成の検討の前提として、以下の条件を設定する。

**【要件1】データ主体による認証：**
個人情報は、データ主体の承認が無い限り、記憶してはならない。但し、個人情報は、つぎつぎと転記される場合もあると思われるので、その場合には、転記元の認証で良いとする。

**【要件2】データ存在場所の確認：**
データ主体は、いつでも、自分のデータがどこにあるかを確認できなければならない。

この実現手段として、本システムでは、個人情報を保持するデータ管理者は、データ保持している事を、公的機関に開示する必要がある。言い換えれば、認証された個人情報の存在は、公的機関にデータの存在が開示されていないと罰則を受けるものと想定している。認証されていようがいまいが、公的機関に開示されていないデータが発見されれば、それ

は違法である。

**【要件３】データ具体値の守秘：**
上記公的機関は、誰のデータがデータ管理者により保持されているのか、それが、いかなるデータ値であるかを登録されたデータから解析できない必要がある。これは、公的機関自身による、プライバシー侵害を防止するものである。

### 5.2.2 システム構成

上記３要件を満たすシステムの一例として、以下の構成を提案する（図４参照）。

**【個人情報の保存方法】**
個人情報は、
$ID_i$：データ主体 $i$ が作成した秘密の ID 番号
$D_p$：個人情報
$Co$：データ管理者名（企業等の名称)
$S(d)$：データ d へのデータ主体 $i$ のデジタル署名[9]
で表す時、

$$ID_i, D_p, Co, S(ID_i + D_p + MD)$$

として、データ管理者において保存されるものとする。但し、$S(ID_i + D_p + Co)$ は、$ID_i$、$D_p$ 及び $Co$ 全体に対するデータ主体によるデジタル署名［18］である。これにより、データ主体の了承のもとに、個人情報がデータ管理者に渡されていることが認証される。データ主体の識別番号は、極めて大きな桁数の整数からランダムに選択する。これにより、ID 番号の衝突の危険は、限りなくゼロに近づくことになる。尚、ここでは省略しているが、データと共に、データ主体の公開鍵の CA 証明書を添付する。

データ管理者は、あらかじめデータ主体との契約により、他データ管理者に写しを渡すこともある。写しを作成するたびに、データ主体の署名を受けるのは実際的ではないので、データ管理者が他のデータ管理者にデータを転送する時には、自分で認証をする。即ち、この場合の受け取り側が管理するデータは、

$$ID_i, D_p, Co'S'(ID_i + D_p + Co')$$

となる。但し、ここで、$Co'$は受け取り側のデータ管理者名であり、$S'(ID_i + D_p + Co')$ は、コピー元データ管理者によるデジタル認証を意味する。添付される CA 証明書は、コピー

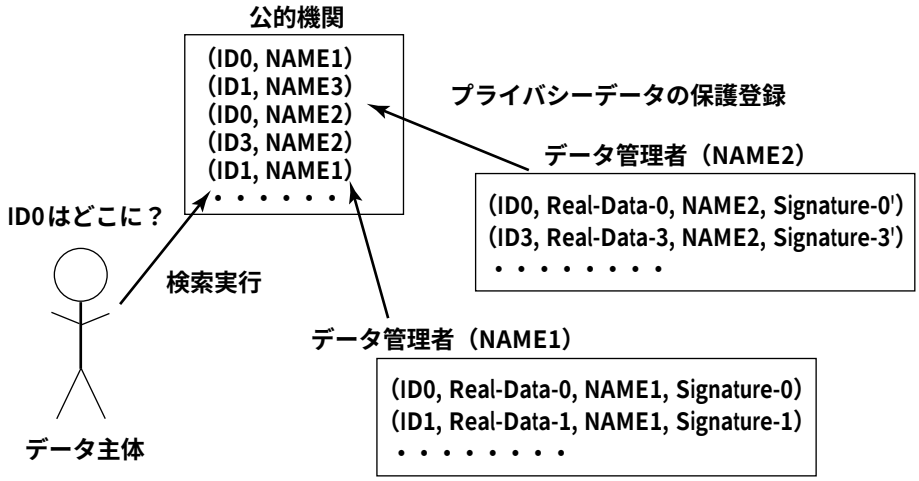


**図４　個人情報流通管理システム**

[9] 個人のデジタル署名を付すことは、結果として、不正に当該データが流出したときに、それを否認できない。この問題を解決するには、認証に、かならず個人に戻る必要がある否認不可署名［櫻井96］の利用が効果的である。以下の議論は、否認不可署名であると考えても、同様である。

元データ管理者の公開鍵に対する証明書である。尚、このようなデータ管理側による署名は、データ管理者以外の（データ参照があらかじめ許可された）企業等が検索を実行した際に、検索結果に付加して送られるべきものでもある。以上のデータ形式以外の個人情報保存を認めないこととすれば、認証できるのはデータ主体のみであるから、データ管理者が勝手にデータを作成することは出来ない。

**【公的機関への個人情報存在の登録】**

データ管理者は公的機関に個人情報を登録しなければ違法とする。但し、実データを登録すると公的機関にプライバシー漏洩するので、データ主体の識別番号である$ID_i$をデータ管理者識別名称とともにペアとして登録する（($ID_i$, $Co$）あるいは（$ID_i$, $Co'$）である）。尚、何個のデータを保持しているかはデータ管理者の法人プライバシーであるとも考えられ、データ管理者は適当に生成したIDによる偽データを登録してもよい。

データ主体は、自己のID番号で、公的機関のデータを検索する。ただし、この際、データ主体は、自分のID番号で直接検索することはしない。例えば、IDのビット列の部分値を検索条件として、極めて冗長なデータを取得し、真のIDにより選択する。この際、偽の部分値を入力してもよい。

以上の対策により、公的機関は、データ主体の真のIDが何なのか、即ち、どこにデータ主体の個人情報があるのかを知ることはできない。そして、データ主体は、データ管理者に開示請求をして、その具体値を確認できる。尚、ここで論じたのはデータのありかを確認するシステムであり、言うまでもなく、どのデータをだれが参照しているかを登録・表示するホームページも必要であることは言うまでもない。データベースとして保有していなくても、参照可能であれば、その参照値を統合に利用できるからである。

## 6．終章

ネットワーク上の情報を統合することによるプライバシー侵害の可能性について問題提起した。そして、情報統合のために利用する属性として、ドイツ法で想定しているようなキー属性（ドイツ法では国民背番号に相当する個人ID）を利用しなくても、氏名や複数属性による統合が可能であることを明らかにした。更に、民間部門を対象とするプライバシー保護法制の存在しない我が国では、特に、いわゆる「名簿屋」の存在が問題となることを指摘した。

情報統合の危険を予知するには、(1)個人情報の所在をデータ主体が知り得るシステム、(2)個人情報が誰から見えているかを知り得るシステムが必要である。その実現法のひとつとして、本論文では、デジタル署名による個人情報流通管理システムを提案した。

ネットワーク化により、電子商取引（EC: Electronic Commerce）、ポイントカード等による顧客データの蓄積等、個人情報を収集するシステムは膨張を続けている。これらは、わが国経済の発展のためにも普及させるべき技術である。しかし、民間部門を対象として、何らの法的規制もないわが国では、このデータが「名簿屋」に流れない保障はない。

通産省等のガイドラインが果たしている役割は大きい。しかし、プライバシー侵害が、複数ソースからの情報の統合によって行われ始めようとしている今、個々のソースに対応する規制（＝業界毎のガイドライン）のみで、全体としての実効性を確保しようとすることは、はたして可能だろうか？

ヨーロッパ式の厳しい法制度によるプライバシー情報の流通を選択するか、アメリカのように業種毎の法規制にまかせるかは国民の選択の問題である。しかし、個人情報の利用が、複数ソースからの統合により行われ始めようとしている現在、国民背番号のようなキー属性のみを見て、プライバシー保護を論じても、技術の実体に合わない。また、データ監察官を設置を前提として、業界毎の規制で対処している国から、業界毎の規制のみを取り込んでも、プライバシー保護の全体思想を取り込んだとは言えない。

図５にも示したように、情報公開、データベースマーケティング（顧客データベースを利用した販売促進）、そして、プライバシー保護は相互に相矛盾する側面を有し、相互に関係が深い。東京都条例、大阪府条例等、情報公開条例はプライバシー保護に配慮している［公開法 98］。

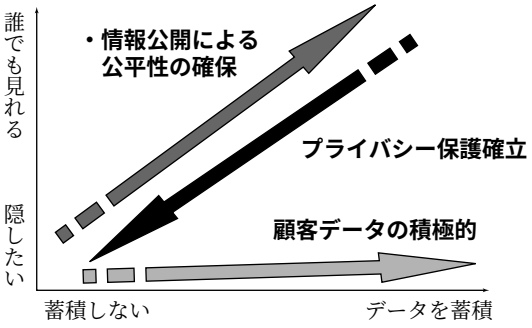


**図５　情報公開・プライバシー保護そして データベースマーケティング**

都情報公開条例では、「個人に関する情報で特定の個人が識別できるもの」とある。国の情報公開法も平成11年２月に成立を見た。しかし、そもそも、「特定の個人が識別できる情報」が、当該情報のみでは決まらないのである。

以上見てきたように、プライバシー保護の問題は、環境問題にも似た、総合的な取り組みを必要とする。そして、それは、法研究のみでは達成できず、技術のみでも達成できない。より、総合政策的な研究が必要である。そして、環境問題にも似て、総合的な対策のために残された時間は少ない。そのことが、本論文をまとめて行く中で、最も強く残った印象である[10]。

## 参考文献

［JIS］JIS Q 15001、「個人情報保護に関するコンプライアンス・プログラムの要求事項」、1999, 3, 20制定、日本規格協会。

［鈴木98］鈴木健司、「データベースがわかる本」、オーム社、1998。

［堀部88］堀部政男、「プライバシーと高度情報化社会」、岩波書店、1988。

［堀部96］堀部政男（編）、「情報公開・プライバシーの比較法」、日本評論社、1996。

［堀部98］堀部政男（編著）、「発信電話番号表示とプライバシー」、NTT出版、1998。

［神山95］神山敏雄、堀部政男、坂本昌成、松本恒雄、「顧客リスト取引をめぐる法的諸問題」、成文堂、1995。

［春日96］春日市個人情報保護審議会専門研究会編、『「知る権利」「知られない権利」－春日市「情報二条例」の回顧と展望－』、信山社、1996。

［神奈川98］神奈川県個人情報保護条例については、例えば http://www.pref.kanagawa.jp/osirase/kensei/Homej.htm

［公開法98］東京都情報公開制度研究会編集、「情報公開制度実務便覧」、ぎょうせい、1998。

［松尾95］松尾直著、「情報法とプライバシー権」、文眞堂、1995。

［藤原97］藤原静雄、「個人データの保護」、岩波講座現代の法（10）情報と法、岩波書店、1997。

［米丸97］米丸恒治、「ドイツ流サイバースペース規制」、立命館法学、No.255, pp.141-194, 1997.

［小澤98］小澤哲郎、「ドイツマルチメディア法～情報及び通信サービスの枠組みを定める法律～」、国際商事法務、Vol.26, No.3, pp.277-287, 1998.

［平松98］平松毅、「情報公開と個人情報保護」、公法研究、No.60, pp.1-24, 1998.

［本村98a］本村憲史、金田重郎、「ネットワーク上での情報統合によるプライバシー侵害とその対策」、電子情報通信学会技術研究報告 OFS98-5, pp.29-36, 1998.

［本村98b］本村憲史、金田重郎、「ネットワーク上での情報統合によるプライバシー侵害とその対策」、経営情報学会1998年春季全国研究発表大会、D-1-2, pp. 65-68, 1998.

［橋本99a］橋本誠志、金田重郎、「ネットワーク上での情報統合に対するプライバシー保護システムのあり方」情報処理学会・電子化知的財産・社会基盤研究会、情報処理学会研究報告 99-EIP-3, 3-3, pp.17-24, 1999.

［井上99a］井上明、金田重郎、「何故にCookieは論じられないのか？」情報処理学会インタラクティブ・エッセイ、Vol.40, No.4 http://www.ipsj.or.jp/magazine/interessay.html, 1999.

［橋本99b］橋本誠志、金田重郎「個人データ流通・保護のための法とシステム」経営情報学会1999年春期研究発表大会、A-5-2, 1999.

［井上99b］井上明、橋本誠志、金田重郎、「個人データ流通における保護システムのあり方」情報処理学会・電子化知的財産・社会基盤研究会、99-EIP-4-8, pp.49-56, 1999.

[10] 尚、本論では、論じていないが、インターネットでユーザIDをクライアントのパソコンに打ち込むCookieも、情報統合の強力な手段である。我が国でもCookieは、多くのホームページで日常的に利用されている。しかし、一般ユーザには、その存在や役割がほとんど知られていない。Cookieの詳細、問題点については、文献［橋本99a、橋本99b、井上99a、井上99b］を参照されたい。

［三井98］三井優、「データレイプー衝撃の個人情報裏ビジネス」、山下出版・山下書店、1998。
［斎藤99］斎藤貴男、「プライバシー・クライシス」文春文庫、1999。
［荒川95］荒川圭基、「データベース・マーケティングの進め方」、PHP出版、1995。
［OECD80］OECDガイドライン、1980 “Organization for Economic Cooperation and Development Guidelines on Privacy and Transborder flows”, http://www.oecd.org/dsti/iccp/legal/priv-en.html, 1980, （邦訳は、ECOMのHP、http://www.ecom.or.jp/）。
［EU95］EU指令、“irective 95. EC of the European Parliament and of the Council of On the protection of individuals with regard to the processing of personal data and on the free movement of such data”, 1995, （邦訳は、ECOMのHP、http://www.ecom.or.jp）。
［FISC87］財団法人・金融情報システムセンター編、「金融機関等における個人データ保護」、金融情報システムセンター発行、1991（但し、FISCはガイドラインの改定を進めている）。
［JIPDEC88］日本情報処理開発協会（JIPDEC）ガイドライン（http://www.jipdec.or.jp/security/privacy.htm）。
［Mark］プライバシーマーク制度（JIPDEC）http://www.jipdec.or.jp/security/MarkSystem.html/
［JISA］（財）日本データ通信協会「プライバシーマーク制度の創設・運用開始について」http://www.dekyo.or.jp/hogo/center.htm/
［P3P］P3P, http://www.w3.org/Privacy/
［SGML95］（株）日本ユニテックSGMLサロン編著、「はじめてのSGML」、技術評論社、1995。
［XML1］富士通XML推進チーム編、「はじめてのXML」、日経BP社、1997。
［XML2］村田真、「XML入門」、日本経済新聞社、1998。
［XML3］日経バイト、「究極のデータ表現XML」、日経バイト、1999年1月号特集。
［PDF97］株式会社ユニット広田健一郎著『日本語PDF＋Acrobat入門』、工学図書、1997。
［江尻96］江尻弘著、「データベース・マーケティング」、中央経済社、1996。
［UNIVAC71］丹羽基二（監）、日本ユニバック（編）、「日本の苗字」、日本経済新聞社、1971。
［岡本97］岡本龍明、山本博資、「現代暗号」、産業図書、1997。
［櫻井96］D.R.Stinson著、櫻井幸一監訳、「暗号理論の基礎」、共立出版社、1996。
［JISALIST］社団法人・情報サービス産業協会（JISA）のリンク集に国内のリンクがよくまとめられている。http://www.jisa.or.jp/privacy/link-j.html/
［労働省］企業内部の個人情報の扱いについての個人情報に関する関心も薄いと言われる。例えば労働省の報告を参照。http://www.jil.go.jp/kisya/daijin/980629_01_d/980629_01_d.html/
［Fayyad96］Usama M. Fayyad, Gregory Piatetsky-Shapiro, Pradhraic Smith, and Ramasamy Uthrusamy, “Advances in Knowledge Discovery and Data Mining”, AAAI Press and MIT Press, 1996.

**〔付記〕**
本研究は、電気通信普及財団の助成による。