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

本村憲史[†] 橋本誠志[†]
井上明[††] 金田重郎[†]

ネットワーク上にあふれている個人情報は，デジタルデータであるがゆえに，複数ソースからのデータを統合できる．このため，紙に書かれた個人情報と比べ，個人のプライバシー侵害を招く危険性が大きい．欧米には，この種の情報統合の危険性を視野に入れたプライバシー保護法制が存在する．たとえば，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おり，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大きく異なっている．ただし，先進的な欧米のプライバシー保護法制といえども，ここで想定されているのは，キー属性による統合である．しかし，非キー属性であっても，複数属性を併用すれば，実質的にキー属性と等価に働くことに注意をすべきである．いずれにせよ，デジタルデータ化された個人情報は，統合が容易であり，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．特に，インターネットで広く利用されている Cookie は，この情報統合の有力な手段であり，米国のみを視野に入れた仕様であるために，わが国では情報統合の危険がより大きい．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えない．わが国でも，情報統合を前提とする法制度の確立と，あわせて，データ主体が個人情報の存在をつねに把握しうる，個人情報流通管理システム/データ監察官の設置が必要である．

Privacy Protection against Infringement by Combination of Personal Data

Kenji Motomura,[†] Satoshi Hashimoto,[†] Akira Inoue[††] and Shigeo Kaneda[†]

This paper discusses data combination, which is a new type of privacy infringement in a computer network. It is someone combines plural data in the network according to a key attribute and gets complete profiles of a target person. It is one of the most effective means of Database marketing in the present information society. But it has a risk of serious privacy infringement at the same time. This paper tries to show positive policies to this problem. Firstly, it surveys West European privacy protection law systems, which suppose data consolidation and discusses how to evaluate the possibility of privacy infringement. Thirdly this article clarifies the functions of "Cookie" in the Internet, experimentally. Our experiment shows we can easily exchange "user ID" between two companies in Japan. Because there are no privacy protection law systems, which suppose a private sector, data combination and privacy infringement with "Cookie" are to be more serious in Japan. As a conclusion this article suggests necessities of positive counterplans: construction of law and information systems supporting personal data exchange and protection fitted to data consolidation.

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☆．そのうえ，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．本論文においては，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，さら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あり方を考察する．

以下，2 章では，プライバシー保護制度の流れを概観する．次に，3 章では，HP 上の個人情報を統合す

† 同志社大学大学院総合政策科学研究科
Graduated School of Policy and Management, Doshisha University
†† 聖泉短期大学情報社会学科
Seisen College

☆ 本論文執筆時点．包括的個人情報保護法の議論は行われている．

ることによるプライバシー侵害の危険を示す．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触れる．5 章では，複数属性の併用による統合の危険度を示す目安として,「データ弁別度」を導入する．6 章では，インターネットの WWW ブラウザの利用に際して広く利用され，情報統合の有力な手段である Cookie の問題に言及する．7 章では，情報統合を視野にいれたプライバシー保護政策を論じ，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．8 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

最初に，プライバシー保護制度の流れ[18),19)]を概観する．

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」として定義づけて以来，プライバシー権は,「私的」生活上の利益また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まった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いったことが指摘されるようになった．そのため，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（自己情報がどのよう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）権利としてとらえるべきであることが，ウェスティン[29)]やミラー[30)]ら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」ととらえるいわゆる「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，(1) プライバシー保護を結果不法から考えないこと，(2) 秘匿性の強弱を一応捨象して個人情報すべてを一応権利の射程内にとらえること，(3) 個人情報の収集・蓄積・利用のすべての過程に対して，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．

ただし，これらの法律は，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，多くのばらつきが見られた．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とって現れた．そのため，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[41)]．

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．ただし，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．

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[33)]．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かかわらず個人データに対して行われる作業または一連の作業を意味するものとする」（第 2 条 b 項）と規定する等，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．そのうえ，この指令はその名称が示すとおり，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[19)]．

1980 年代に入るとこのよう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「個人情報処理にともな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，そのため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☆．

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」[35]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．そして，さらに，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[38]．

それ以降，通産省や郵政省等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．ガイドラインも多数存在し，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，登録している団体の数も少なく，一般に広く知られているとはいい難い[36),40)]．

以上のように，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，通産省をはじ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．しかし，民間部門を対象とするプライバシー保護法制は，本論文執筆時点では，存在しない．世界におけるプライバシー保護制度と比較すると，現状では大きな差異がある．

☆ 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[6),7)]．ただし，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．

3. 情報統合によるプライバシー侵害

以上見てきたように，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．このような状況では，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，前述のよう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．

(StepI) 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．

(StepII) 各情報（ab，ac，ad）を収集．

(StepIII) 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ほどの情報を得る．

すなわち，個々のホームページの情報は,「a と b」「a と c」「a と d」といったように，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，このとき,「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いう）[12]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1つである．

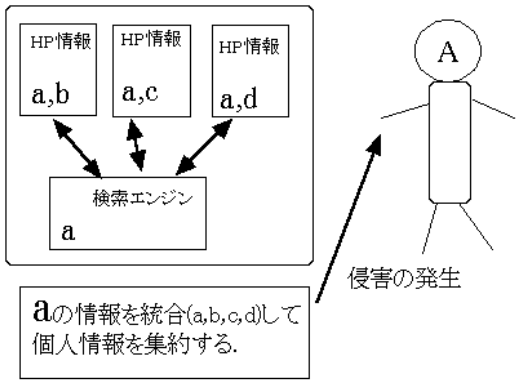

図1 侵害のモデル
Fig. 1 Privacy infringement by combination of personal data.

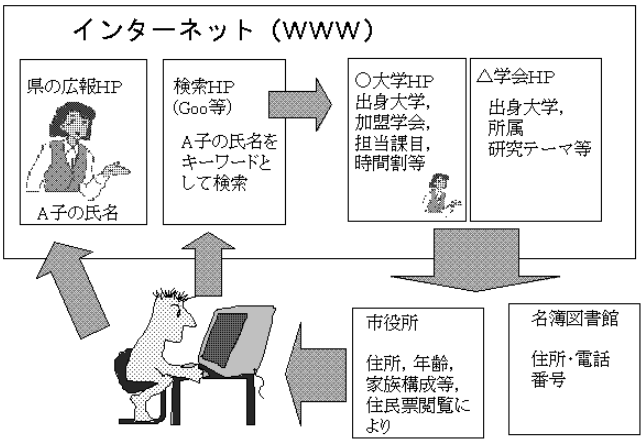

図 2 情報統合による侵害実行例
Fig. 2 An Example of privacy infringement.

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☆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 すべ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．

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 HP で公開されるようになっている．このような状況では，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．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）．ただし，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，

(Step1) goo 等のサーチエンジンで A の氏名で検索し，

(Step2) 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．

(Step3) これにより，県広報に載った女性が (Step2) の助手と分かる．

(Step4) 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，適当な人物になりすまし，戸籍や住民票の写しを請求），

(Step5) 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か否かが問題となる．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

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 1** に示す．人物 A，D，F，G については，すべてターゲットである本人の情報が検索された．したがって，検索された HP の情報を統合して，当該個

☆ 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が分からない（準拠法の問題），問題が生じたときに，どこの国の裁判所が事件を審理するのかが分からない（管轄権の問題）がしばしば生じる．

表 1 実在人物による検索実験（検索は goo による）
Table 1 Search experiment using real name (http://www.goo.ne.jp).

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	△

人の全体像を把握できる．

ありふれた姓であっても，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，ほとんどがターゲット人物以外の情報が収集されてしまった．姓，名ともにありふれた氏名については，予想されたことではあるが，ほとんどが他人の情報であった．

3.4.2 統計的な推計

次に姓の分布データを用いて，解析を行ってみる．日本ユニバックによれば[44]，約 100 の姓で姓全体の 37%を占める．100 万人の被検索対象がある場合に，上位 100 種の姓で，1 つの姓に平均

$$370,000/100 = 3,700$$

人がひしめく．一方，名前の分布は，姓よりも分布が広いと思われるが，安全側にとって，姓と同様とする．この場合，上位 100 種の名前と姓の組合せで，特定氏名を持つ同姓同名の人数は，

$$3,700 \times 3,700/1,000,000 = 13.69$$

人と少ない．しかし，これでは，情報統合はできない．

一方，姓の 500 位から 1,000 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．したがって，この 500 位から 1,000 位にある範囲にある名前と，ありふれた 100 位までの姓を組み合わせると，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，姓または名前の少なくとも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．

3.5 わが国固有の問題点

このよう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 (Step4) のように，ある程度，個人を特定できれば，収集可能な情報量も多く，実際にこのようなプライバシー侵害が行われやすい．

では，(Step4) 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．しかもこのよう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，いま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[23]．

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いは，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，諸外国なみの総合的なプライバシー保護制度の成立が急務である．

4. 諸外国の法制度

では，ここで，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[5),16),26)]．

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」[33] 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，情報統合に関係した記述がある．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[15]．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，もっぱら ID カード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したり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・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・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等，興味深い．詳細は文献 5)，26) 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ことはできない．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えない．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等，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☆．
- **キー属性による結合（JOIN）のみを想定してよいか：**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，氏名等という，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，氏名と生年月日の双方を利用すると，かなり，特定個人が絞り込める．

同様な現象はインターネットでも存在する．たとえば，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，サーバ側には秘匿できる．しかし，ユー

☆ W3C コンソーシアムのプライバシー保護施策である P3P[42] 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．このあたりにも，米国とヨーロッパの立場の違いが感じられる．

ザごと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合せがキー属性を構成している．このような，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．

さらに，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 → サラ金というように，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，知る術もほとんどない．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こと，(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，サーバ会社の公的機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．

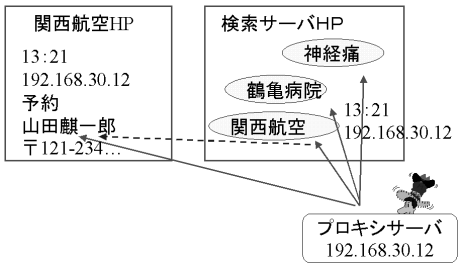

図 3 タイムスタンプによる情報統合
Fig. 3 Privacy data integration using time-stamp.

5.2 データ弁別度

データ統合の危険性を測る尺度として，データ弁別度を導入する．データモデルはリレーショナルモデルとする．

リレーション $R1(A_1, A_2, \ldots, A_n)$ および $R2(B_1, B_2, \ldots, B_m)$ を考える．このとき，$R1$ のあるタプルと，$R2$ のあるタプルが同一個人のデータであることを，その属性値または属性値の組から推定できるとき，これを**統合可能**であると呼ぶ．

一般に考えられているデータ統合とは，この 2 リレーションの統合であろう．しかし，本論文では，さらに，以下の複数リレーションの統合を考える．

【定義 1】複数リレーション統合

3 個のリレーション $R1(A_1, A_2, \ldots, A_n)$，$R2(B_1, B_2, \ldots, B_m)$，$R3(C_1, C_2, \ldots, C_p)$ を考える．このとき，R1，R2，R3 が互いに統合不能とする．すなわち，R1 上のあるタプル t を考えるとき，t と JOIN 可能なタプルが R2 にも複数個（これらを，「R2 候補タプル」と呼ぶ），R3 にも複数個（R3 候補タプル）あるとする．R2 候補タプルと R3 候補タプルの中で，統合可能なタプルが唯一あるとき，最終的に，各リレーションから唯一のタプルが選定される．ここでは，3 リレーションの例を示したが，さらに多数のリレーションに対しても同様の操作を実行可能なとき，これを「複数リレーション統合」と呼ぶ． □

上記の複数リレーション統合を，**図 4** により具体的に示す．

【前提条件】 名簿業者甲は，購入者リスト（表 B），および○△学会の会員名簿（表 C）を保有している．一方，公開情報として，年齢，勤務先，趣味が記録されたデータベース（表 A）が公開されていた．この表 A は，統合に配慮して，氏名やキー属性が存在しないの

公開情報（プライバシーを考慮して，住所・氏名は削除）

表 A

年齢	勤務先	趣味
58	NTT	ギャンブル
20	資生堂	ハイキング
34	日立	音楽鑑賞

表 B

趣味	氏	年齢
ギャンブル	山田尚久	58
お茶	山田祥子	21
ギャンブル	藤原紀香	58
ギャンブル	鈴木憲花	58
ギャンブル	田中晃一	58

購入者名簿

表 C

氏	年齢	勤務先	住所	電話番号
山田尚久	58	NTT	東京	XX-XXX
加藤俊文	43	東芝	仙台	YYY-YY-
田中尚久	32	日立	大阪	ZZ-ZZZZ-
鈴木まみ	58	NTT	和歌山	ZZZ-ZZ-
藤原花子	58	NTT	京都	ZZZ-ZZZ-

○△学会名簿

図 4 複数リレーション統合による個人データ抽出
Fig. 4 Privacy data extraction using integration of multiple relations.

で，問題なしとして公開したデータである．一方，甲は，競馬の予想業者乙から依頼を受け，予想紙の講読会員募集の DM 送付先リストを作成することとなった．なお，乙からは，58 歳で NTT に勤務する人のリストが特に欲しいと要請が出ている． □

上記前提のうえで，以下の処理により情報統合が可能である．

(1) 甲は，B 表から A 表にある年齢 58 歳に該当する人を検索し，山田尚久，藤原紀香，鈴木憲花，田中晃一の 4 人が該当することが分かった．

(2) 次に，甲は，C 表から A 表にある年齢 58 歳，NTT 勤務のデータに該当する人を検索，山田尚久，鈴木まみ，藤原花子の 3 名が該当する．

(3) B，C 表の対応関係を考えると，山田尚久氏のデータが共通している．一方，C 表の鈴木，藤原については，B 表中に存在しないので排除される．

(4) 以上のように 3 の表を統合的に観察して，統合を行えば，公開情報に氏名，住所がなくても，山田尚久氏は，東京都に在住し，NTT に勤務するギャンブル好きな 58 歳の男性であることが判明し，結果として，住所も分かる．

上記の例で注目したい点は，公開されるリレーションと他リレーションの間では，完全な統合ではなく，あいまい性がある点である．**完全なキー属性を持たないデータであっても，プライバシー侵害の危険がある**ことになる．そこで，この統合の危険性を測る目安として，以下のデータ弁別度を導入する．

【定義 2】データ弁別度

属性 P がとりうる値の集合を，ドメイン DP と呼び，そのサイズ $|DP|$ をドメインサイズと呼ぶ．このとき，当該リレーション中の全属性に対するドメインサイズの積 $Descri$ を**データ弁別度**と呼ぶ．

$$Descri = |D_0| * |D_1| * , \ldots , * |D_i| * , \ldots , * |D_{n-1}|$$

□

データ弁別度を最も素直に計算できるのは，属性値が数値で，かつ，分布がランダムな場合である．たとえば，生年月日については，データ弁別度は $Descri = 50 * 12 * 31 = 18,600$ である．ただし，ここでは，個人データを保有する期間を 50 年とした．

氏名のような非数値データの場合には，データ弁別度の計算はやっかいである．きわめて珍しい氏名であると，事実上，1 億 3,000 万のデータ弁別度に等しくなる．一方，比較的ありふれた氏名であると，そこまでのデータ弁別度とは見なせない．氏名のような固有名詞の場合には，平均的なデータ弁別度しか議論できない．たとえば，極論であるが，名字も名前も 500 通りしかないとすると，氏名のデータ弁別度は，$Descri = 500 * 500 = 250,000$ である．

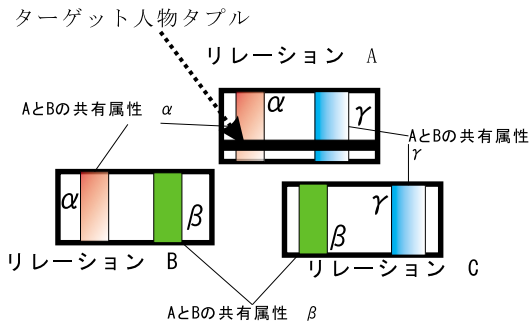

図 5 複数リレーション統合とデータ弁別度
Fig. 5 Multiple relation integration and data discrimination power.

この結果，氏名と生年月日の組合せは，$Descri = 250,000 * 18,600 = 4,650,000,000$ となって，国民人口総数をはるかに超える．厳密な議論ではないが，よほどありふれた氏名の組合せでないかぎり，氏名と生年月日で，ほぼ，個人が特定できることがこのデータ弁別度からも分かる．

5.3 データ弁別度と統合可能性

次に，複数のリレーションを統合することにより，ターゲット人物の情報を得る場合を考える．リレーションの統合は，制約充足問題[21] で，2 つの制約表（リレーション）が統合されて，より大きな制約表を構成する状態に相当する．この問題を**図 5** を用いて考察する．図 5 には，3 つのリレーション A，B，C があり，以下の前提条件を設ける．

【前提条件】

- A と B が属性 α，B と C が属性 β，そして，C と A が属性 γ を共有している．
- A には，ターゲット人物のタプルが含まれている．B，C には，ターゲット人物のデータが含まれていることは分かっているが，どのタプルがそれであるかは特定できていない☆．
- A がデータ管理者により新たに公開される情報である．B，C は，侵害者が有する情報である．B，C については，非公開情報であるか，公開情報であるかはここでは問わない． □

上記の前提で，A の公開により，侵害者が A，B，C を統合するとする．A 中のターゲット人物のタプ

☆ すなわち，A，B，C の全リレーションにターゲット人物のタプルが含まれている．これは，かなり厳しい前提条件である．当該前提条件が成立しない場合については，後述する．

ル，B，そして C が統合されて全体の制約表を構成する．

まず，リレーション B，C のみを統合する．当該制約表中にターゲット人物のタプルが 1 個あるはずである．しかし，属性 β のみによる統合では，データ弁別度が低いため，タプルは絞り込まれていない．すなわち，どれがターゲット人物かは不明である☆．この状態は，図 4 で下 2 つのリレーションの統合を行った状態に相当する．

次に，ターゲット人物の新たな情報（リレーション A）が公開されたとする．侵害者は，リレーション A 中の特定タプルをターゲットとする．このタプルを，先ほどのリレーション B，C の統合結果と統合する．これは，B，C から生成された制約表と，別の制約表（ターゲット人物のタプル）との統合である．加えられた制約表（A 中のタプル）が有する属性（α，γ）は，すでに B，C に含まれている．新たな制約表の統合は，タプルの個数を増加させない．解を刈り込むのみである．

ここで，新規公開情報である A が含む，ターゲット人物の属性として既知な属性は，α，γ のみである☆☆．一般的にいって，心あるデータ管理者であれば，プライバシー侵害に生じないように，属性 α，γ が構成するデータ弁別度を意識的に，低めに制御するはずである．たとえば，250,000 を選択したとする．公開される個人情報が持つ生年月日等の属性から得られるデータ弁別度が 250,000 程度ならば，全国民 1 億 3,000 万人には，500 人程度該当者がいるので，プライバシー侵害の原因にはならないと考えたわけである☆☆☆．

これに対して，侵害者は，リレーション A を公開したデータ管理者側には不知であるリレーション B，C を有している．この制約表のサイズが，250,000 以下であった場合には，この新たな個人情報の公開は，プライバシー統合のキーとなりうる．この場合，データ管理者は，どの程度のサイズの制約表を第三者が持っているかを知ることができないので，データ弁別度の制御によりプライバシー侵害の防止をすることは難しい．

以上から，以下の結論を得る．

【分析結果 1】データ弁別度許容限界の推定不能性
新たに公開されるデータが低い弁別度しか持たない場合であっても，他のデータをそれにより刈り込むことが可能となり，実質的にキーを構成する場合がある．この限界許容値は，データ統合対象データを有しないデータ管理者側には，それを推定できない． □

たとえば，現状の情報公開法では，「他の情報と結合して個人を特定可能なものを除く」として，プライバシー保護に配慮している．しかし，他の情報の存在が不知である場合には，この規定は，技術的にも実務上も意味を持たない．

以上の議論では，ターゲット人物のデータが含まれていることを前提としていた．ターゲット人物のデータが含まれていることが分かっていると，リレーション中のタプルの個数が少ないので，小さなデータ弁別度でもターゲットを特定できる．言い換えると，所属学会や出身大学等の情報は，年齢等の個人属性とはまた別の意味で，重要な個人情報である．たとえば，勤務先として従業員が 20 名しかいない企業名が表示されていれば，その 20 名の中から，個人を特定すればよい．この場合，データ弁別度が 50 程度のごくありふれた属性（年齢，本籍等）であっても，個人特定のためのキー属性となる．

また，3.4.2 項で論じたように，固有名詞属性の問題として，その分布が一様でない点がある．姓にしても，名前にしても，分布には偏りがある．したがって，自明な以下の性質がある．

【分析結果 2】固有名詞のデータ弁別度計算不能性
リレーションのデータ弁別度が，数学的に推定可能なのは，リレーションを構成する属性が，すべて数詞・一般名詞により構成され．かつその分布がランダムなときに限定される．その場合，データ弁別度は，定義 2 に従う．しかしながら，属性として，固有名詞を含む場合には，平均的には大きなデータ弁別度を有する場合でも，ある固有の姓名等が大きなデータ弁別能力を有する場合がありうる． □

以上の議論では，ターゲット人物のデータが，必ず統合対象のリレーションに含まれていることを前提としていた．しかし，図 5 で，ターゲット人物のタプルがリレーション B，C に含まれていることが保証されていない場合には，B，C の双方にターゲット人物のタプルが含まれている確率は非常に低い．したがって，公開情報と統合されて得られたタプルをターゲット人物のものと判定することはかなり難しい．その意

☆ この際の属性 β のデータ弁別度が小さいと，B と C から生成される制約表のサイズが巨大となる．この場合，後ほど，リレーション A と統合しても刈り込みが難しい．属性 β のデータ弁別度は大きい方が望ましく，後述のユーザ ID，IP アドレス，Cookie 値等が効果的である．

☆☆ 属性 β は，B と C の統合には利用しているが，この段階では，ターゲット人物がどんな属性値を持っているかは分かっていないものとしている．

☆☆☆ ここでの議論で，数字 500 には特段の根拠があるわけではない．データ管理者が感覚的に選択したと考えていただきたい．

味からも，ターゲット人物が所属している団体名等の情報の扱いには注意が必要である．

統合に利用する属性のデータ弁別度は大きいほど，結果として生成される制約表のサイズを絞り込める．たとえば，コンピュータの世界でよく利用されるユーザ ID は，キー属性であり，かつ，探索範囲が絞り込まれるため，強力な統合手段である．Intel の PSN☆や Cookie がこれに該当する．次章では，Cookie の問題について考えてみたい．

6. わが国における Cookie の問題

個人 ID は有力なデータ統合キーであり，その危険性は，外部データの有無にかかわらず，大きなものがある．その ID をネットワーク上で取得する有力な方法に Intel の PSN と Cookie[43] がある．PSN については，パソコン雑誌等でも取り上げられている．しかし，Cookie の詳細は，ほとんど紹介されていない．

特に問題なのは，Cookie を利用すれば，**複数の企業で，利用者の ID を共有できる**ことである．これにより，どちらかの企業のホームページで氏名，住所等を入力した瞬間に，それらのデータは他社のデータと統合可能となる．以下，この問題点について，実験的に明らかにする．

6.1 Cookie とは何か

Cookie は，Netscape 社により提案され，Internet Explorer，Netscape Navigator に実装されている．ホームページ側から送信された変数名と変数値を，クライアント側 Cookie ファイルに保存する[31),32),39)]．クライアント側の内部ファイルを読み取ることを目的とするものではない☆☆．

Cookie データは，設定したサーバからは読み取れる．サーバは Cookie 値設定の際，自分自身のドメイン名の上部概念部分（たとえば，サーバが「foo.hoo.com」であれば，「.hoo.com」といった上位部分）を同時に設定している．この場合，「x.hoo.com」「y.hoo.com」といった，同一企業内サーバならば，Cookie 値を読み取れる．しかし，「z.zoo.com」といった，他社のサーバからは読めない．あまり上位のドメイン名を登録できると問題があり，Netscape 社[32)] は，「.foo.com」は許容するが，「.co.jp」は認めず，「.ntt.co.jp」は認める仕様を公開している．これにより，米国においても，わが国においても，Cookie に設定したユーザ ID を共有できるのは，同一企業内部のサーバに限定される．

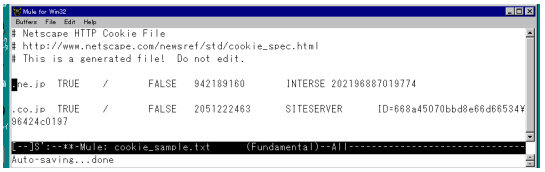

図 6 設定されていた Cookie
Fig. 6 An example of Cookie file.

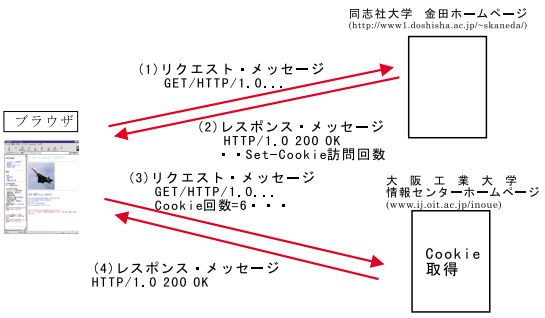

図 7 Cookie の読み取り実験
Fig. 7 Experimental block diagram for Cookie extraction.

しかし，上記の Netscape 社の仕様は，W3C の正式な Cookie 仕様 RFC2109[43] には反映されていない．わが国では，「.ac.jp」といった，複数の団体から自由に参照できる Cookie が設定できる．実際，著者らのパソコンにも，このような Cookie が設定されていた（**図 6**）．

6.2 実験による確認

Cookie の機能を確認するため，以下の実験を行った．実験の構成を**図 7** に示す．

(1) 同志社大学のホームページ（doshisha.ac.jp）に Cookie を設定するために JavaScript プログラムを設定した．設定するドメイン名は「.ac.jp」．

(2) 上記ホームページをある大学（doshisha.ac.jp でも oit.ac.jp でもない）にアクセス依頼した．これにより，Cookie 値がセットされた．

☆ Intel 社が Pentium III プロセッサに内蔵した，個々のチップを識別するための ID 番号である．Pentium III の発売当時に大きな話題となって，米国のプライバシー保護団体の圧力により，Intel 社は，出荷時には，この機能を止めて出すこととなった．ただし，わが国では，プライバシー保護への意識が薄いためか，あまり議論になったとはいい難い．すべての Pentium III には内蔵されて出荷されているものと思われ，大規模な企業等でのパソコンの管理を考えると，技術的には魅力的な機能である．

☆☆ 最初にホームページを参照した瞬間に，Web ブラウザを立ち上げている側のパソコン内部に，変数名と変数値がホームページから書き込まれる．たとえば，変数名として，ユーザ ID であることを宣言し，あわせてユニークな値をこの変数にセットする．後日，同一パソコンが当該ホームページをアクセスするたびに，この変数名と数値が読み取られる．すなわち，ユーザ ID を参照することにより，同一人がアクセスしてきたことをサーバ側は認識できる．ユーザ ID は情報統合の手段（属性）として利用できることとなる．

(3) 次に，クライアントには，大阪工業大学（oit.ac.jp）のホームページを参照してもらった．大阪工業大学のホームページには，上記の Cookie 値を読み取るプログラムを設定しておいた．

実験の結果，読み取りうることが確認できた．実際には，同志社のホームページを参照した回数を読み取った．以下の問題が提起される．

- 異なる企業の間で，ユーザ ID を共有できる．これは，Intel の PSN と同様の効果を生む．たとえば，検索エンジンで（本人は匿名のつもりで）検索を行い，別途，ある企業のホームページに入り，そこでは懸賞応募等に参加して，住所・氏名・電話番号を登録したとする．この場合，誰がどのような検索を実行したかを特定できる☆．また，情報統合の立場からすると，異なる企業が得た情報を統合するための属性として，Cookie を利用できる可能性が，わが国にはあることになる．
- Netscape には，Cookie に関する設定があり，「Cookie を拒否する」「Cookie の設定を確認する」「設定したサーバのみに Cookie を返送する」を選択できる．ここで，「設定を確認する」とすると，確かに Cookie の設定時には確認するが，Cookie 値を送信するときには，環境変数値として返送するので，ユーザには警告しない．しかし，現状の日本語の確認メッセージは，あたかも，メッセージが出ているときに確認するかのごとき印象を与える．
- ブラウザのデフォルトでは，上記 Cookie に関する確認画面は示されない．このため，理系ユーザであっても，多くのユーザは Cookie の存在すら知らない．一方，データをインターネット上で送信するときには，警告はデフォルトで表示される．同様に，ファイルダウンロードでも，デフォルトで警告が出る．これらの条件に従うなら，Cookie 確認をデフォルトとすべきである．

Cookie は Netscape 社の主張のとおり，基本的には便利なツールである．バナー広告が，自分の興味に合致したものとなることはむしろ望ましいし，ホームページを久しぶりに参照しても，以前の投入データが残っていることは，ユーザインタフェースとしても快適である．Cookie そのものを否定するつもりは著者らにはない．

しかし，一方，懸賞募集と Cookie を組み合わせて，個人データの収集が本人の認知しない範囲で行われているとすれば，これは，個人データは本人に告知して行うべきであるとする通産省ガイドラインにも合致しない[38]．

6.3 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，いか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．

6.3.1 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，データ主体の認証がない限り，記憶してはならない．ただし，個人情報は，次々と転記される場合もあると思われるので，その場合には，転記元の認証でよいとする．

【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ことを，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．

6.3.2 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 8** 参照）．

☆ わが国には，プライバシー保護の法律はないので，企業間で，個人データを流通することはまったく自由である．これは，マーケティング上は，興味深いデータである．

☆☆ 本節で提案する個人情報流通管理システムは，あくまで，データ主体自らが，プライバシー情報がどこに存在するかを知りうるように保証するものであり，統合そのものを防ぐものではない．しかし，いかなる個人情報が流布しているかを認識できることが，統合の可能性をデータ主体が判断するためには必要と考える．

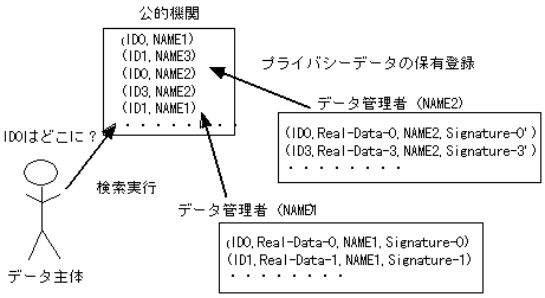

図 8 個人情報流通管理システム
Fig. 8 Block diagram of privacy management system.

【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

MD：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☆

で表すとき，

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

として，データ管理者において保存されるものとする．ただし，$S(ID_i + D_p + MD)$ は，ID_i，D_p および MD 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 ID 番号は，きわ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．なお，ここでは省略しているが，データとともに，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ときには，自分で認証をする．すなわち，この場合の受け取り側が管理するデータは，

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

となる．ただし，ここで，MD' は受け取り側のデータ管理者名であり，$S'(ID_i + D_p + MD')$ 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，コピー元データ管理者の公開鍵に対する証明書である．なお，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できない．

なお，以上のシステム構成案では，データの二次流通の場合において，ソース側であるコピー元データ管理者が，ID 番号を改竄することは考慮に入れていない．コピー元データ管理者は，適当な ID 番号 ID_i を創出し，これに個人情報をつけて，全体に，コピー元データ管理者がデジタル署名することが可能である．この場合，ID 番号が適当な番号なので，データ主体が自己のデータがどこに存在するかを確認できなくなる．したがって，このようなケースにも対応するには，個人情報として，データ主体がつけた署名を含む個人情報全体を，個人情報のように扱い，コピー元データ管理者は，これに自分の名前を付加して，そこに署名する方法を用いる必要がある．この場合，データ管理者の手を経るごとに，署名の個数が増えるが，基本的には，上に述べたシステム構成で対応可能である．

【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．ただし，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 ID 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, MD) あるいは (ID_i, MD') である）．なお，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．たとえば，ID のビット列の部分値を検索条件として，きわ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，すなわち，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．なお，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，いうまでもなく，どのデータを誰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いうまでもない．データ

☆ 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[11]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．

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．

7. 現実的な対応策

以上，(1) 個人データについては，流通させれば，どんなデータでも，プライバシー侵害のきっかけとなる危険があること，(2) わが国では，Cookie を用いて，企業間でユーザ ID を共有可能であることを明らかにした．本章では，このような状況に対して，どのような対処（政策）が可能かを考察したい．

7.1 教育のあり方として

著者らの簡単な聞き取り調査の範囲でも，わが国にはプライバシー保護の法律があると考えている IT エンジニアが数多く存在した．一方，企業の中では，業務用電話の利用量・宛先を上司が参照しようとするときにも「プライバシーの侵害である」との反発がある場合があり，そもそも，プライバシーが何であるかについて，IT エンジニアの間に，まったくコンセンサスがない．一方，IT エンジニアの多くが，自分のパソコンだけは，Cookie ファイルを消去したり，受付けを禁止している．

ほとんどの IT エンジニアは，自己情報コントロール権[13),24),25)] 等には，知識も興味もない．しかし，一般のユーザとは異なり，彼ら IT エンジニアは，Cookie を利用したホームページの設計やサーバ管理，あるいは，個人データを大量に扱うシステムの設計を行う立場である．プライバシーの考え方，法制度等について無関心であるのは問題である．

一方，一般のユーザは，プライバシー保護の法律の現状についても知らず，Cookie によるデータ収集自体にも不知である．著者らは大学で生活している立場なので，教育の場についていえば，以下の対策が考えられる．著者の所属する研究科では，ネチケット等とともに，カリキュラムに取り入れている．

- **エンジニア教育：**近年では工学部でも知的所有権についての科目が設けられている．大変に意義深いことと思われるが，この中で，プライバシー権の現状，法制度等についても，紹介してもらえると効果的である．
- **コンピュータリテラシー教育：**近年は文系の学生に対しても，広く，情報リテラシー教育が実施されている．しかし，情報を提供する側に将来なるであろう，これら文系の学生については，Word, Excel，ネチケットだけでなく，ウイルスやプライバシー保護について紹介してゆく必要がある．

7.2 法制度の制定

現行の法律では，企業が収集した個人データを販売することに対して，何らの規制はない．実際，ある名簿業者が，以前,「購買データ買います」との広告をインターネットの HP のトップに掲示していたことがある．CD レンタルショップ等で，会員のデータをアルバイト学生が半ばおおっぴらにコピーして小遣いを稼いでいる話もよく聞く．前述したように，どのような個人データでも，それが漏れてしまえば，プライバシー侵害の危険を増大させる．情報が増えると，それだけ解が絞り込まれるからである．

このような状況にあって，良心的な IT エンジニアがいて，プライバシー保護に配慮したシステムを提案しようとしたとする．この場合でも，(1) プライバシー保護は儲からないので，企業としては優先順位が低い，(2) もともと，IT エンジニアは顧客から発注を受けて仕事をしており，立場上，コストアップ要因となる提案は出しにくいに違いない．しっかりしたコンピュータシステムをエンジニアが提案できるためにも，プライバシー保護の法律が必要である．

また，本論文で示したように，どのような低いデータ弁別度を持つ個人データであっても，それを開示したために，個人が特定されてしまうケースがどこかで生じる恐れがある．その意味では，自分にとってセンシティブなデータを含む個人データは，絶対にデータ管理者以外には流通してはならない．そのためにも，法的な規制は必須である．そして，ドイツ法のように，データ統合を禁止する条項を法的に規制することも，今後は，視野に入れる必要がある[5),10),26)]．

一方，1999 年 3 月にプライバシー保護のための JIS Q 15001 が制定をみた[1)]．この JIS は，ISO14000 のように，絶え間ない見直しと改善を主旨とする．おそらくは，今後，プライバシーに関するコンサルティング・教育を，ビジネスチャンスとしてみる団体が現れるであろう．しかし，それが，一部エージェンシーやコンサルティング会社の利益のみに終わり，インターネット利用者全体のプライバシー保護の意識が変化しないなら，JIS Q15001 の意義は薄いものとなる．

自分の Cookie ファイルを消してよしとするエンジニアが多いのも，多少気になる現象である．あまり，前向きの態度とはいえない．JIS Q 15001 が手本とした環境分野では，環境対策を前向きにとらえて，むしろ，ビジネスチャンスとして生かすことを考えている．プライバシー保護を,「一部のうるさい人が言っていること」ではなく，顧客の囲い込み手段，サービスの向上施策として，活かすべきである．

8. 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．さらに，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わが国では，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．

次に，データ統合に向いたデータを取得する手段である Cookie に注目した．わが国では，異なる企業間で，インターネットユーザを識別するための個人 ID を Cookie 経由で共有できる．この Cookie の問題は，ドメイン名構造が同一の EU 諸国でも生じるが，明確なプライバシー保護法やデータ監察官を持つ EU とは異なり，民間部門を対象とする保護法制すら持たないわが国では，より危険である．

一方，わが国には，通産省等のガイドラインが存在する．これらガイドラインの果たしてきた役割は大きいものと思われる．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（＝業界ごとのガイドライン）のみで，全体としての実効性を確保できるか否かは十分に議論する必要がある．

図 9 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[9]．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 1999 年 2 月に成立をみた．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．

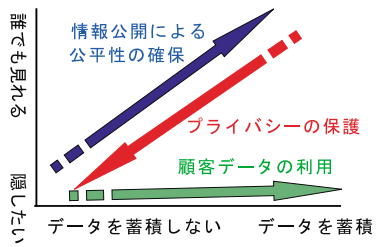

図 9 情報公開・プライバシー保護そしてデータベースマーケティング
Fig. 9 Open policy, privacy protection and database marketing.

ホームページを利用して商品購入した経験のあるユーザなら分かるように，相手の顔や店構えを見られない状況で，住所・氏名・クレジットカード番号等の個人情報をインプットするのは，恐いものである．しかし，このことは，どんな情報を取得しているかをユーザに開示できれば，より大きな安心をユーザに与えうることを示唆している．収集した個人情報は他の目的に利用しませんとホームページに掲示するだけではなく，取得したデータそのものをユーザに開示するアプローチを想定しうる．そのようなアプローチの方が，自己情報コントロール権の立場にも合致する．

周知のように，環境保護分野では，「もうからない環境対策」から，「ペイする環境対策」へと，大きく流れが変化している[17),28)]．コンピュータ・エンジニアは，「自分のパソコンの Cookie ファイルを消してよしとする」ような，後ろ向きの取組み姿勢から一歩進んで，広くプライバシー保護の法制度に興味を持ち，そのありようを考えるべき時代に入りつつあると思われる．そして，日本人が新しいプライバシー保護と流通の観点に立てるような，新たなプライバシー収集・活用のビジネスモデルの構築へと，企業エンジニアの意識が変革することを，強く念ずるものである．

謝辞　本論文に関し，有益なコメントをいただいた査読委員に感謝します．ただし，本論文では，反映できていない部分があります．今後の研究課題とさせていただきたいと考えます．また，本研究は，電気通信普及財団・研究助成（1999.4–2000.3）によります．あわせて，深謝いたします．

参　考　文　献

1) 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.
2) 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 (1999). http://www.ipsj.or.jp/magazine/interessay.html
3) 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).
4) 岡本龍明，山本博資：現代暗号，産業図書 (1997).
5) 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).
6) 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).
7) 神奈川県個人情報保護条例については，たとえば http://www.pref.kanagawa.jp/osirase/kensei/Homej.htm
8) 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).
9) 東京都情報公開制度研究会（編）：情報公開制度実務便覧，ぎょうせい (1998).
10) 斎藤貴男：プライバシー・クライシス，文春文庫 (1999).
11) Stinson, D.R.（著），櫻井幸一（監訳）：暗号理論の基礎，共立出版社 (1996).
12) 鈴木健司：データベースがわかる本，オーム社 (1998).
13) 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).
14) 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).
15) 平松　毅：情報公開と個人情報保護，公法研究，No.60, pp.1–24 (1998).
16) 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).
17) シュミット・ブレーク（著），佐々木建（訳）：ファクター 10 エコ効率革命を実現する，シュプリンガー・フェアラーク，東京 (1997).
18) 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).
19) 堀部政男：プライバシーと高度情報化社会，岩波書店 (1988).
20) 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).
21) 制約充足問題については，筑波大学・第三学群・西原清一教授のホームページが詳しい．
22) 松尾　直：情報法とプライバシー権，文眞堂 (1995).
23) 三井　優：データレイプ—衝撃の個人情報裏ビジネス，山下出版・山下書店 (1998).
24) 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).
25) 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).
26) 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).
27) 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いわれる．たと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
28) エルンスト・ワイツゼッカーほか（著），佐々木建（訳）：ファクター 4 豊かさを 2 倍に，資源消費を半分に，省エネルギーセンター (1998).
29) Westin, A.F.: *Privacy and Freedom*, Galahad Book (1967).（堀部政男：プライバシーと高度情報処理社会，岩波書店 (1988) p.27 より引用）．
30) Miller, A.R.: *The Assult on Privacy*, University of Michigan (1971)（堀部政男：プライバシーと高度情報処理社会，岩波書店 (1988) p.28 より引用）．
31) Netscape 社の cookie についての説明．
http://home.netscape.com/legal/_notices/cookies.html（2000.4.16 現在）．
32) Netscape 社の cookie 仕様．
http://home.netscape.com/newsref/std/cookie_spec.html（2000.4.16 現在）．
33) EU 指令，Directive 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/）．
34) Fayyad, U.M., Piatetsky-Shapiro, G., Smith, P. and Uthrusamy, R.: *Advances in Knowledge Discovery and Data Mining*, AAAI Press and MIT Press (1996).
35) 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（1999 改訂）．
http://www.fisc.or.jp/ippan.htm（2000.4.16 確認）(1999).
36) 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（2000.4.16 現在）．
37) 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（2000.4.16 現在）．
38) 平成 9 年 3 月 4 日通商産業省告示第 98 号，通産省ガイドライン，日本情報処理開発協会（JIPDEC）．
http://www.jipdec.or.jp/security/privacy.htm（2000.4.16 現在）(1997).
39) St. Laurent, S.（著），(株) クイック（訳）：Cookies 入門，アスキー出版 (1998).
40) プライバシーマーク制度（JIPDEC）．
http://www.jipdec.or.jp/security/MarkSystem.html/（2000.4.16 現在）．
41) OECD ガイドライン，Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
http://www.oecd.org//dsti/sti/it/secur/prod

/PRIV-EN.HTM（2000.4.16 現在）(1980).（邦訳は，ECOM の HP, http://www.ecom.or.jp/）
42) P3P. http://www.w3.org/Privacy/（2000.4.16 現在）.
43) RFC2109. http://www.w3c.org/
44) 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).
45) 松浦康彦：デジタル世紀のプライバシー・著作権，日本評論社 (2000).

(平成 12 年 4 月 20 日受付)
(平成 12 年 9 月 7 日採録)

本村　憲史

1996 年 3 月同志社大学法学部政治学科卒業．1998 年 3 月同大学大学院総合政策科学研究科修士課程修了．修士論文において個人情報保護法制について研究．同年（株）ジオン商事入社．2000 年 3 月第 15 回電気通信普及財団賞（テレコム社会科学学生賞）受賞．

橋本　誠志

1996 年 3 月関西学院大学法学部卒業．1999 年 3 月同志社大学大学院総合政策科学研究科修士課程修了．同年，同大学院総合政策科学研究科博士課程入学，在学中．コンピュータ法専攻，特に消費者保護に関する法律に興味を持つ．2000 年 3 月第 15 回電気通信普及財団（テレコム社会科学学生賞）受賞．

井上　　明（正会員）

1992 年 3 月大阪工業大学工学部経営工学学科卒業．2000 年 4 月同志社大学大学院総合政策科学研究科修士課程修了．同年，同大学院総合政策科学研究科博士課程入学，在学中．1992 年住友金属情報システム（株）入社．大阪工業大学情報センターを経て，2000 年 4 月聖泉短期大学情報社会学科専任講師．デジタル技術とコミュニティー形成過程に興味を持つ．2000 年 3 月第 15 回電気通信普及財団賞（テレコム社会科学学生賞）受賞．

金田　重郎（正会員）

1974 年 3 月京都大学工学部電気第二学科卒業．1976 年 3 月同大学大学院修士課程修了．同年，電電公社武蔵野電気通信研究所入所．以後，主記憶装置の実用化，高信頼化技術の研究，ならびにエキスパートシステムの研究・実用化に従事．1997 年より，同志社大学大学院総合政策科学研究科教授，同工学部教授．工学博士（京都大学），技術士（情報処理部門）．電子情報通信学会，人工知能学会，経営情報学会，IEEE 各会員．人工知能学会全国大会優秀論文賞（1992, 1995），経営情報学会全国研究発表大会発表賞（1999）．2000 年 5 月より情報処理学会関西支部幹事．