

個人データ流通における保護システムのあり方

井上 明 橋本 誠志 金田 重郎

同志社大学大学院総合政策科学研究科, 京都市上京区
skaneda@mail.doshisha.ac.jp

あらまし プライバシーに配慮して公開した個人データであっても, 他の既存の個人データと統合すれば, 個人の全体的なプロフィールが暴かれる事がある。これをデータ統合によるプライバシー侵害と呼ぶ。本稿では, どのような性質のデータならば流通させても問題が生じないかを考察するため, 個人データに対する「データ弁別度」を導入する。そして, プライバシー侵害を生じる恐れがあるか否かを判定する事は, どのような個人データが世の中に流布しているかを完全に知っていないかぎり困難であることを示す。また, 一般には知られていない Cookie を利用すると, 複数の企業間で個人 ID を共有できることを実験的に示す。最後に, 当面の政策上の対策について考察する。

Privacy Protection Systems for Data Circulation

Akira INOUE, Satoshi HASHIMOTO and Shigeo KANEDA

Doshisha University, Graduate School of Policy and Management

Abstract Data combination is that someone combines plural personal data in the network according to a key attribute and gets complete profiles of a target person. This combination is one of the most effective means of Database Marketing. But it has a risk of privacy infringement at the same time. This paper dicusses how to evaluate the possibility of privacy infringement. The analysis shows that no one can evaluate the possibility without all privacy data in the world. Also, this paper clarifies the functions of "Cookie" in the Internet, experimentally. Our experiment shows that we can easily exchange "user ID" between two companies in Japan.

1 はじめに

プライバシーに配慮して公開した個人データであっても, 他の既存の個人データと統合すると, そこから個人の全体的なプロフィールが得られ, プライバシーが侵害される事がある。個人データの統合は, 犯罪捜査を見ても分るように, 個人のプロフィールをつかむために極めて効果的である。著者らも, 既に, ネットワーク上におけるデータ統合とプライバシー保護の関

係について論じている [5, 6].

EU圏では, データ統合 (combination) を視野におく法制度がある [7, 12, 13, 14, 15]. また, 我が国の情報公開法でも, 「特定の個人を識別することができるもの【他の情報と照合することにより, 特定の個人を識別することができることとなるものを含む】」¹とただし書きされ, デー

¹本稿執筆時点では, 情報公開法は参議院における与野党修正協議中である。情報公開法案 第5条第1項。

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	養生堂	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	田中昇一	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-7777-
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 1: 複数リレーション統合による個人データ抽出

タ統合に配慮している。しかし、この規定が具体的にどのような技術的内容を意味するのかは、未検討のように思われる。

以上の観点から、本稿では、データ統合を前提として、どのような性質のデータが公開可能かを考察する。また、このデータ統合の有力な手段であるにもかかわらず、必ずしも一般には知られていない“Cookie”の問題点を明らかにする。

以下、第2章では、「データ弁別度」を導入する。そして、許容できるデータ弁別度は、他の個人データに依存すること、結果として、「公開する側」単独では、データ統合の危険を予測できないことを明らかにする。第3章では、Cookieの問題に目を転じ、複数の企業間で個人IDを共有できることを実験的に示す。第4章では、以上の分析を踏まえて、当面の対策について考察する。第5章はまとめである。

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ンナルモデルとする。

リレーション $R1(A_1, A_2 \dots A_n)$ 及び $R2(B_1, B_2 \dots B_m)$ 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特定できる時、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、本稿では、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 $R1(A_1, A_2 \dots A_n)$, $R2(B_1, B_2 \dots B_m)$, $R3(C_1, C_2 \dots C_p)$ を考える。この時、 $R1$, $R2$, $R3$ が互いに統合不能とする。即ち、 $R1$ 上のあるタプル t を考える時、 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。

図1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)、及び○△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事となった。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。

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人が該当する事がわかった。
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歳の男性である事が判明し、結果として、住所も分る。

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が取り得る値の集合を、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。この時、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。

$$Descri = |D_0| \cdot |D_1| \cdots |D_i| \cdots |D_{n-1}| \quad (1)$$

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。例えば、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。但し、ここでは、個人データを保有する期間を

50年とした。

我々は、このデータ弁別度が1億くらいの大きな値でなければ、すなわち、キー属性に準じなければ個人データを公開しても問題ないように思いがちである。しかし、データ統合を想定する限り、そのような生やさしいものではない。

そもそも、データ統合は、複数のリレーションを統合する制約充足問題[4]であり、ある制約表中の1タプルを含む制約充足解が1個となることである。しかし、以下の点で、一般の制約充足問題と異なっている。

- リレーション同士を統合する際に、相互が間違いなくほぼ同一人のデータであることを確定する必要がある。このため、キー属性、あるいは、キーに近い属性（統合に複数属性を利用する場合には属性群）を必要とする。
- リレーションには、年齢、年・月・日、分・秒等の数詞・普通名詞属性と、所属企業名、商品名等の固有名詞属性がある。所属企業名のような固有名詞は、属性値として当該企業名が含まれていると、探索の範囲が、当該企業の従業員数まで、大幅に絞り込まれる。ユーザID等のID属性も、特定のアプリケーションで付与されているため、確実に対象とする人物をとらえており、固有名詞属性に近い性質を持つ。

特に問題なのは、上記2番目の固有名詞属性である。例えば、勤務先として従業員が20名しか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²となる。商品名（商品番号）も危険である。別に当該商品のユーザ登録情報が存在する危険がある。

つまり、データ弁別度で言えば、固有名詞属性値の存在により、キー属性になってしまうデー

²本稿で「キー属性」と言う場合、データベース理論でいう完全なキーではなく、ほぼキーに近いものを言う。全員のプライバシーが侵害されずとも、大半の人物のプライバシーが侵害されれば問題であるからである。それはまた、定義1からも裏付けられる。

タ弁別度が大幅に減少する。今から流通させようとしているデータ単独では、この限界値が本質的に分からない。実際の個人データでは、個人データに固有名詞を含まないことはまず、ないであろう。現状の法制が視野において「他の情報と結合して個人を特定可能なものを除く」との規定は、技術的にも実務上も意味を持たないものである。以上から、以下の結論を得る。

【定理1】統合可否の判定不能

リレーションが統合可能か否かが、当該リレーションのみで判定可能なのは、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時に限定される。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、当該リレーションのみでは、キー属性を構成するに至るデータ弁別度を推定できない。

【系1】データ弁別度許容限界

上記定理から、公開される個人データに固有名詞を含む場合には、公開する側にとっては不知のデータにより、対象人数が大幅に減少する危険がある。この場合、きわめて低い弁別度でも、キーを構成する。この限界許容値は、データ統合対象データを有しない公開側には、本質的に推定できない。

一方、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。

3 我が国におけるCookieの問題

以上のべたように、国民背番号を持つデータのみではなく、低いデータ弁別度でも、統合が実行できることがある。一方、個人IDは有力なデータ統合キーであり、その危険性は、外部データの生むに関わらず、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[10]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、あまり紹介されていない。

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。

3.1 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[8, 9, 11]。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位概念部分（例えば、サーバが「foo.hoo.com」であれば、「.hoo.com」と言った上位部分）を同時に設定している。この場合、「x.hoo.com」「y.hoo.com」と言った、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」と言った、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社は、以下の様に唱っている[9]。

Only hosts within the specified domain can set a cookie for a domain and domains must have at least two (2) or three (3) periods in them to prevent domains of the form: ".com", ".edu", and ".va.us". Any domain that fails within one of the seven special top level domains listed below only require two periods. Any other domain requires at least three. The seven special top level domains are: "COM", "EDU", "NET", "ORG", "GOV", "MIL", and "INT".

つまり、「foo.com」は許容するが、「co.jp」は認めず、「ntt.co.jp」は認める。これにより、米

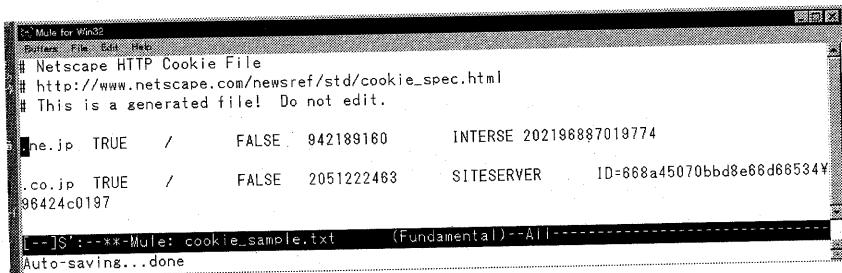


図 2: 設定されていたクッキー

国においても、わが国においても、クッキーに設定したユーザ 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。

しかし、上記の Netscape 社の仕様は、W3C の正式な Cookie 仕様 RFC2109[10] には反映されていない。わが国では、「.ac.jp」と言った、複数の団体から自由に参照できるクッキーが設定できる。実際、著者らのパソコンにも、このようなクッキーが設定されていた (図 2)。

3.2 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 3 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。
3. つぎに、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、上記のクッキー値を読みとるプログラムを設定しておいた。

実験の結果、読みとり得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とった。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。例えば、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³。

- Netscape には、Cookie に関する設定があり、「クッキーを拒否する」「クッキーの設定を確認する」「設定したサーバのみにクッキーを返送する」を選択できる。ここで、「設定を確認する」とすると、確かにクッキーの設定時には確認するが、クッキー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時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、上記クッキー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、多くのユーザはクッキー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、クッキー確認をデフォルトとすべきである。

クッキーは 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

³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。

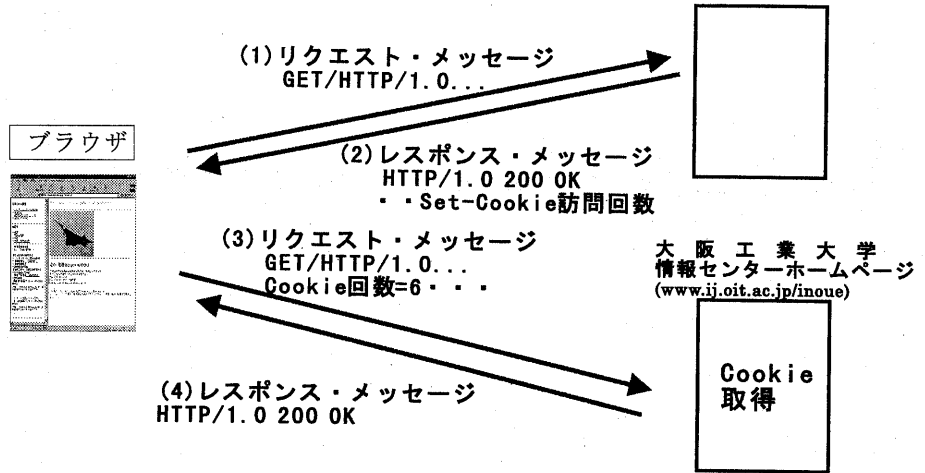


図 3: クッキーの読みとり実験

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、懸賞募集とクッキーを組み合わせ、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 [16]。

4 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。

4.1 教育のあり方として

著者らがプライバシー保護の研究発表をして来た中で、「えっ？プライバシー保護の法律って

無いんですか？」との反応がエンジニアから多くあった。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時にも「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、「プライバシーとは何か？」について、エンジニアの間に、全くコンセンサスがない。一方、コンピュータ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、受け付けを禁止している事を知ったのも驚きであった。

著者自身も、企業エンジニアの時には、自己情報コントロール権 [5, 6, 7] などには、知識も興味も無かった。しかし、一般のユーザとは異なり、コンピュータエンジニアは、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、教育の場について言えば、以下の対策が考えられる。著者の所属する研究科では、ネチケット等と共に、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、紹介していただくと効果的である。
- 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。

4.2 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、何らの規制は無い。実際、株式会社名簿図書館 [22] でも、「購買データ買います」との広告をインターネットで掲示している。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。基本的には、制約充足問題であるため、ひとつでも制約表が増加すれば、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、良心的なエンジニアがおり、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、コンピュータ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、本稿で示したように、どのような低いデータ弁別度をも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、自分に取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 [14, 15, 20]。

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 [3]。この JIS は、ISO14000 の様に、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、前向きな態度とは言えない。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。

5 終わりにあたって

「キー属性による統合」を利用しなくても、統合によるプライバシー侵害が生じ得る事を明らかにした。そして、危険度を定量化するため「データ弁別度」を提案し、どのような個人データでも、流通量が増えるほど、個人のプロフィールが明らかになる危険が増大することを示した。今後のプライバシー保護法の法制度設計にあたっては、従来法が想定する ID (キー属性) による「結合」のみを視野に入れるのではなく、一歩進んだ対応が必要である。

次に、データ統合に向けたデータを取得する手段である Cookie に注目した。我が国では、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我が国では、より危険である。

電子商取引において、未知のサイトに、住所・氏名・クレジットカード番号等を伝えるのは、勇気がいる。相手が信用できるか否かが分からないからである。顧客から収集した情報を、サイトがどのように利用し、管理しているかを利用者に情報開示してゆくことは、顧客の囲い込みの手段、商業活動の付加価値としても、活かし得ないだろうか？

既に環境分野では、「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 [23, 24]。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」様な、後ろ向きの取り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、その有りようを考えるべき時代に入りつつあるのではないだろうか？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、念ずるものである。

参考文献

- [1] 堀部政男, 「プライバシーと高度情報化社会」, 岩波書店, 1988.
- [2] 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.
- [3] 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.
- [4] 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.
- [5] 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.
- [6] 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.
- [7] 橋本誠志, 金田 重郎「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.
- [8] Netscape 社のクッキーについての説明 http://home.netscape.com/ja/legal_notices/cookies.html
- [9] Netscape 社のクッキー仕様 http://home.netscape.com/newsref/std/cookie_spec.html
- [10] RFC2109, <http://www.w3c.org/>
- [11] Simon St. Laurent 著, 株式会社クイック訳「Cookies 入門」, アスキー出版, 1998.
- [12] 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/>)
- [13] 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/>).
- [14] 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.
- [15] 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.
- [16] 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>).
- [17] プライバシーマーク制度 (JIPDEC) <http://www.jipdec.or.jp/security/MarkSystem.html/>.
- [18] (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/>.
- [19] 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/>.
- [20] 斎藤貴男, 「プライバシー・クライシス」文春文庫, 1999.
- [21] 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, 1998.
- [22] 株式会社名簿図書館, <http://www.meibo.com>
- [23] エルンスト・ワイツゼッカー他著, 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」, 財団法人省エネルギーセンター, 1998.
- [24] シュミット・ブレイク著, 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.