翻訳

インターネットのプライバシー問題の解決には政府の介入も必要だ

オンラインプライバシーに対する一般の人々の信頼感は
インターネットの拡大に伴い低下している．
法制化を含む保護の枠組みが救済措置として求められる．

Roger Clarke　Roger.Clarke@anu.edu.au
翻訳：安藤　進　sando@twics.com

原文: "Internet Privacy Concerns Confirm the Case for Intervention"
Communications of the ACM, Vol.42, No.2, pp.60-67 (Feb. 1999) より許可を得て翻訳

サイバースペースがプライベートな空間に侵入している．スパム，クッキー，クリックストリームの是非をめぐる議論は注目されているが，これは氷山の一角にすぎない．裏ではリアルタイムで個人情報が密かに収集されている．たとえば，高度交通システム（ITS），地図検索，生体識別法による本人確認，ハード認証技術，プラスチックのカードに埋め込まれた小型のプロセッサ，アンクレット，時計，リング，製品そのもの，製品の包装，家畜，ペット，人間などがある．

社会的な信用が得られなければ，消費者電子商取引（e-commerce）が進展しないことは明らかだ．問題は単にセキュリティの問題というよりはむしろ，情報社会に対する信頼性の問題である．

これまで，インターネットと法律はあまり関係がないと考えられていた．これに対して本論文は，プライバシーとインターネットをめぐる現在の議論がプライバシーを保護するための本格的な動きに向かっていることを論証したい．米国では長期間にわたり一般的なプライバシー保護を寄せ付けなかったので，ヨーロッパ諸国より大幅な変更が必要になるだろう．

プライバシーは倫理的な権利あるいは法的な権利と見なされることが多い．しかし，個人が他人や組織からの干渉を受けないような自分の空間を保持する権利と見なした方が分かりやすいだろう．

個人空間にはいくつかの次元がある．特に，個人のプライバシー（個人の身体の統合性に関係する），個人の振舞いの秘匿，個人の通信の秘匿，個人情報の秘匿が重要である．情報の秘匿は，個人が自分の情報を他人や組織に利用されないようにすることであり，情報を第三者が処理する場合，個人が情報そのものと情報の用途をかなりの程度でコントロールできるようにすることである（言葉の定義については文献6）を参照）．

情報の秘匿は，高価な監視装置が，本誌で10年以上も前に提唱した情報監視（dataveillance）に急速に置き換わることに伴い，ますます脅威になってきた．serveillance（監視）から造語した情報監視（dataveillance）は，人間の行動や通信を調査あるいは監視するために個人情報システムを体系的に使用することである[2]．

個人情報をくまなく収集することは，公共団体や民間企業が個人をコントロールするための土台になる．プロファイル情報を送信者駆動型の技術に組み合わせることで，カスタマイズした情報を各個人にプッシュする．こうすると，個人の振舞いは大きな影響を受け，個人の考え方や行動の自由が制約される．

インターネットは社会的経済的な価値にプラスの影響を与えるが，プライバシーの点では情報技術がマイナスの影響を与えている（インターネットのプライバシーについては文献7）を参照）．マーケティング，技術，プロバイダの要請で，これまで匿名で行われたことが身元を明示した取引に代わる傾向がでてきた．その結果，情報量はますます増加した．情報の整理統合を容易にするために，政府と民間企業は多目的の国民総背番号制を強制し

ようとしてきた[3]．たとえば，米国当局は1998年，多目的の国民総背番号制として2つの制度を強力に推進した．1つは運転免許証に基づくもので，もう1つは健康保険に基づくものである．

プライバシーの保護と社会的信用の危機

プライバシーを規定するときに重要なのは，個人の権利，他人の権利，グループや社会全体の権利というそれぞれ相反する側面を持つ多くの権利のバランスをとる必要があることだ．バランスをとるプロセスはもともと政治的な色彩が濃いものであり，当局，市場，そのほかの関係者による権力の行使を伴う．

技術主導型のプライバシー侵害に対して，ただ単に防衛するというだけでは不十分である．情報の収集量は増加し，しかも個人名のついた情報も増えている．情報の格納技術が情報の継続利用を保証し，情報ベース技術が検索を可能にし，電気通信技術が情報のネットワーク化を可能にする．組織は，職業倫理や業界規定で多少の制約を受けるだけである．

コストの制約は急速に解消されつつある．いずれにせよ，経済的な制限は制約としては働かなくなった．たとえば，公共部門の情報照会制度の場合，コスト／利益分析が自発的になされることはめったにない．現在公開されているいくつかの分析には多くの重大な欠陥がある．明らかに赤字である制度が生き残っている．民間部門では，プライバシーの侵害行為が日常的に行われている．その理由は自社の狭い観点ではその方が経済的だからというだけにすぎない．自然に任せれば，効率を追求する企業の権利の方が消費者の権利より強いので，企業が人間を支配するようになる．

これに対して個人が反撃してもその効果は薄い．現在のところ，むしろ何もしないことの方が効果的な場合が多い．先進国の業界や政府は，電子商取引が遅々として進まない理由として，消費者や小規模会社が大手企業や政府を信頼していないことを挙げている．電子商取引の信頼性が確立できるかどうかには，消費者の権利，表現の自由，社会的な公平さなど，相互に関連し合う複数の複雑な要因がある．本論文は，プライバシーの中心的な要素だけに的を絞って述べる．

先進国の業界や政府は，電子商取引が遅々として進まない理由として，消費者や小規模会社が大手企業や政府を信頼していないことを挙げている．

社会的な価値としてプライバシーを放棄すべきか

政府高官や企業幹部の中には，保護の枠組みに問題が多いことを根拠として「プライバシーなんか不要だ，そんなものは捨ててしまえ」と主張する者もいる．大衆は信頼できないものであり，個人情報へ組織がアクセスする力を実質的に強化する見返りとして現代社会の恩恵を与えてやるのだというのだ．この議論は，国庫の収入，信用供与機関，保険会社での不正防止，税金の効果的な徴収，製品やサービスの効果的なマーケティングなどの文脈で語られる．法律の強化や国防も蒸し返される．

この種の議論はネットワーク化された世界の現状とは関係がないように見える．多国籍企業のパワー，リージョナリズム，グローバリズム，情報インフラ，情報社会と

情報経済の新しい形態によって，国家の影響力は弱まりつつあると見られている．

昔は，管轄権外（取引が主として異なる国で行われる）および特別管轄権（取引が主として法定ヘイブンで行われる）にアクセスできるのは金持ちだけに限られていた．一方，先進国では，インターネットのコストが大幅に減少したので，組織や個人がそれほどお金をかけないでもインターネットの利益を享受できるようになった．

インターネットは効果的な超管轄権（管轄権の規制を受けない）も可能にしている．公海は常に特別な法的措置を必要とするが，宇宙法（地球軌道で発生した事件の責任分担など）が新たな課題を提供している．インターネットの世界では，事件の発生地を特定するのが困難なので，（大国や向こう見ずな国でも）管轄権を主張できる裁判所はない．

その結果，自国の意思を国民に強制するこれまでの政府権力が弱まり，巨大企業や大富豪の方が強くなってしまった．

一方，企業は，アウトソーシングやダウンサイジング，テレコンピューティング，バーチャル化などの形態で分散化を開始している．その目的は，小さな組織の柔軟性や順応性，さらにできるだけ安くしかも残業をいとわない個人経営者を有利に利用するためだ．しかし本当にそうなるかどうかは必ずしも明白ではない．財務的な統制権を過度に集中するあまり，組織のプロセスや構造の変化が見えにくくなる傾向があるからだ．この傾向が続けば，欧米経済圏内での力関係は，単一の企業ではなく企業間提携の規模と説得力で決まるだろう．

一方，インターネットを利用すると，消費者や市民が企業や団体の動きに関する情報を交換し組織的な対抗措置を講じることが可能になる．談合協定を維持しようとする企業は政府の圧力には耐えられるが，インターネットで組織化された消費者グループの要求は無視できなくなる．

要するに，政府職員には官僚的な経済処世訓が説得力を持ち，企業幹部には事業の効率化が錦の御旗なのだが，いずれも市民や消費者には説得力を持たない．21世紀中頃に，圧倒的な力を持つ大衆がプライバシーの保護を要求すれば，必ず実現できるだろう．だれも人間性を喪失させることはできない．志があれば道は拓けるのだ．

すべてオープンにすることだけで解決できるのか

プライバシーの重要性に対する反論の中で透明性の向上に関する議論がある．その要点はBrin[1]に明瞭に述べられている．インターネットの場合と同じく有視界監視（visual surveillance）が無秩序に拡大していることを踏まえて，Brinは，技術の圧倒的な力には勝てないので，プライバシーの保護はムダであると述べている．プライバシーを維持するには，万人に向かって情報の自由を強調するしかない．プライバシーは，秘密にするのではなく自由にすることで実現できるというのである．

Brinの要旨を簡単に紹介しておく．

Q: 監視人を監視するのはだれだ．
A: 監視される人だ．

Brinの対抗手段は，すべてを完全オープンにして，権力者の行為をだれでも自由に監視できるようにすることだ．警察官が他人を監視すれば，インターネットを利用して警察官の行為を監視し，その行為の妥当性を判断する．

Brinは，監視人が他人から監視されるのを防止する目的で政治力は使わないことを前提にしている．歴史を振り返れば，権力の分配は公平ではなく，権力者は権力を行使する動機と力を持っており，権力を維持しようとする．Brinの透明社会が実現するのは，数千年間にわたり繰り返されてきた人間の行動様式が一朝にして崩壊する場合しかあり得ない．

Brinは，力の弱い者は自分より力の強い者より強くなれるので，だれも特権的な地位を築くことはできないし，すべての人々の行動がすべての人々によって監視されるということを暗黙の前提にしている．この点についてBrinは，権力者が他人からの監視を防止できるのは，自分の利害を損なうプライバシー保護法に抵抗している場合に限られる，と再度反論している．

プライバシー保護に関するさまざまな提案を簡単に紹介したが，いずれも現在焦眉の急である問題の解決には役立たない．インターネットの急速な成長と桁違いの影響力によって浮上してきた情報技術（IT）に対する社会的な信頼が揺らいでいる．これが問題なのだ．

企業革新で解決できるのか

一般消費者は電子商取引に消極的なので，一部の業界団体では，行動規範と商標を確立し，監査や契約条件の修正などの追加措置を行った．業界全体として重要なのはTRUSTe（Benassiの項を参照）である．もう1つは北米会計協会のWeb Trustイニシアティブである．

こうした動きと並行して，技術的な手段もいくつか提案されている．たとえば，匿名および仮名のメーラー，Webサーフィン支援ツールがある．その背景には，自分の行動を会社や組織の監視から守りたいという要望がある．しかしそのほかのツールは，バスに乗り遅れると業務や管理にマイナスだという企業の思惑から出ているものである．これらのツールについては，後述する．

以前よりもっと本格的なものとしてWWWコンソーシアム（W3C）が開発した規格がある．P3P（Platform for

Privacy Preferences）は，アーキテクチャの革新として特筆すべきである（ReagleとCranorの記事を参照）．

これらのさまざまなイニシアティブを眺めてみると，個人の情報に知的所有権（IP）とでもいうべきものを認めようとする動きが表面化していることが分かる．これは個人に与えられる権利であり，個人が個人情報を売買できる性質を持つ．このような特徴を持つ知的所有権は，著作権や特許，商標，意匠などの従来の権利とは大きく異なるものにする必要がある．個人規制のデフォルトを設定する必要はあるが，情報の使用権は個人によって付与され，その条件は個人の選択に任される．法務当局によって慎重に検討されたあいまい性のない妥協案があれば，それも認める必要がある．

IP権が売買できるという考え方は，人間の見方について社会的な存在より経済的なモデルの優位を暗黙に認めることになるので，神聖な個人という純粋主義的な考え方と対立する．しかし，この新しい考え方の方が個人の権利を保護するうえで従来よりはるかに効果があるかもしれない．さらに，財産権は経済的な諸関係を対象にするが，政府との関係においても速やかに実行に移しやすい．政府に対する国民の信頼が重大な脅威にさらされているのは，国民を情報監視の対象にしようとする政府の権限がますます強くなっているからである．これを所有権と考えれば，立証責任が逆転する．IPに対してどのような譲歩が法律上必要であるかは，政府が明示しなければならない．その結果，法的な侵害事件ごとに提示される判例が脚光を浴びるようになるだろう．

先進諸国では，FIP（Fair Information Practices）と呼ばれる包括的な慣行が徐々に法制化されてきている．経済開発協力機構（OECD）の1980年版ガイドラインが成文化されたのは20年ほど前である（このページの「OECD原則」と文献10）を参照）．ヨーロッパ連合（EU）は規制強化の必要性を認め，1998年10月に通達（Directive）が発効した[8]．経済先進国の大半，特にヨーロッパ内では，OECDに準拠した法律が公共部門に適用され，さらに民間部門にも適用された国が多い[9]．

さて，米国の有力民間部門についてみると，歴代の政府は企業の要望には耳を傾けてきたが，プライバシー保護法を求める国民の声は無視してきた．このような政府の立場は，経済効率は上がれば上がるほどよく，市場がすべての問題を解決してくれ，業務効率がプライバシーの保護者であり，企業の責任ある行動を求めるにはエコノミストのいう「道義的勧告（moral suasion）」に訴えるだけでよい，ということだ．

国民の目を引く問題を取り上げても，一貫した枠組みがなければ，気まぐれで行き当たりばったりの法律しか生まれない．米国には，連邦レベルと大半の州[12]でプライバシーを規制する制定法が非常にたくさんあるが，内容に一貫性がない．たとえば，ビデオ-レンタルレコードは，手厚い保護を受けるが，もっと大切な個人情報は保護の対象にならない．

規制が必要だ

市場原理は万全なものではない．個人には経済的な私利私欲があり，企業がこれにつけこんで，新たな問題が生まれる．歴史的に自己規制が適切であったことはなく，特定の文脈で法律が制定された場合しか有効でなかったのも当然である．インターネットの登場で消費者と市民が共同して立ち上がるという期待がないわけではないが，組織と個人との間の権力の不均衡がすぐにでも逆転するとは思えない．つまり，政府機関や市場の動きの介入なしでプライバシーが適切に保護できると考えるのは現実的ではない．

企業がインターネット上でマーケティング活動を展開することでその必要性が急に注目を浴びるようになった．米連邦取引委員会（FTC）は，1995年から1998年にかけて企業のWebサイトの振舞いを調査した．FTCは1998年6月「効果的な自己規制システムが登場しているようには

OECD原則（抜粋）

個人情報の収集には制限を設けるべきであり，個人情報を取得する手段は合法的かつ公正でなければならない．また，できる限り，収集する情報の内容について知っているか同意を得ていることが望ましい．

個人情報は，使用目的に適合しており，かつその目的に必要な範囲に限定されており，さらに正確で完全であり，最新状態に更新されていなければならない．

個人情報を収集する目的は，事前に明示しなければならない．収集した情報の使用はその目的を実現するための範囲に限定される．

個人情報の開示，利用，ほかの目的での使用は認められない．ただし，情報に関連した人物の同意または法律の権限がある場合を除く．

個人情報は，適正な安全予防手段で保護しなければならない．

個人情報に関する開発，慣行，方針を規定する一般的でオープンなポリシーを作成しなければならない．

個人は，自分自身に関する情報を取得する権利および自分自身に関する情報に異議を申し立てる権利を持つ．

情報の管理者は，原則に則った措置を講じなければならない．

見えない」と結論付けた．そして「12歳以下の児童から個人情報を収集する場合は，両親にその旨を通知して両親の同意を得ることを商用Webサイトに義務付ける法律の制定」を議会に勧告した．法案を支持する上院議員をFTCが見つけるのはさほど困難ではないので，これはほんの手始めに過ぎないだろう☆1．一方，クリントン政権はその姿勢を徐々に変えてきた☆2．米国で法律よるプライバシーの保護を主張することは，これまで政治的には大きな危険を伴う賭けだった．ところが1998年に，法律によるプライバシーの保護は政治的に望ましいという立場に突然変わってしまった．

主権国家の法執行力が低下しているときに法の介入を主張するのは，時代錯誤な意見といわれるかもしれない．確かに法執行力が低下しているのは事実だが，決してなくなってしまったわけではない．情報社会経済においては，場所と同じく法律も重要であることに変わりはない．21世紀初頭はかなりの紆余曲折が予想されるが，個人も企業も，自分あるいは自社の営業拠点として，自分の家族あるいは社員が比較的安全でかつ法治状態も比較的信頼できる場所を選ぶことになるだろう．

プライバシーを保護するには，多様なアプローチが必要である．個人や組織，業界団体，政府が同じ法的な枠組みの中で活動することが前提になる．そこで，法律や手続き，技術も含む包括的な対策が必要になる．さらに，法律に準拠しない組織を規制できる機構で補強しなければならない．自己規制を促進するには法律の強化が必要である．1つには，「善良なる市民」になるための経済的社会的な動機を与えることで，遵法活動を促進することである．もう1つは，コスト構造の上昇など社会的経済的な面で不利になり，法的な制裁を受けることを説明して，法不遵守を断念させることである．このようなモデルの概要をこのページ下段に紹介する．これは「相互規制(co-regulatory)」と読んだ方がよいだろう．このモデルの実施例は，ニュージーランドにある☆3．

☆1 www.ftc.gov/reports/privacy3/toc.htm
☆2 www.epic.org/privacy/laws/gore_release_5_14_98.html
☆3 プライバシー法は1993年に制定．次のサイトを参照．
www.knowledge-basket.co.nz/privacy/legislation/legislation.html

プライバシーの相互保護体制を実現するための要件

企業は，これまで自分の取引先に責任を合法的に押し付けていた．プライバシーの問題は建設的に取り組む必要がある．建設的というのは，企業幹部の知恵の活用，資源の確保，スタッフの適応訓練，ビジネスプロセスの修正，苦情処理窓口の準備と運用，企業顧客とのやりとり，適合を保証するための規制および監査機構などが手段として含まれる[4]．

業界団体は，それぞれの守備範囲でプライバシー保護活動の中心となって働く必要がある．このレベルで重要なのは，一般的なプライバシー原則に基づいて特定業界内の企業に適用するガイダンスとして具体化した行動規範である．加盟企業内に苦情処理窓口の設置．プライバシーの保護と強化のための技術を実現するインフラの整備．使いやすいユーザインタフェースの開発．啓蒙と研修の展開．

法律の遵守を奨励し，不正な行為を思いとどまらせるには，議会の役割が見逃せない．業界団体の力を強化する法律を制定すれば，各団体が自業界内の秩序を維持し，過激分子の行動を抑えてくれる．

包括的なプライバシー保護原則に基づいた情報プライバシー原則を確立する必要がある．あえて抽象的な表現になっている原則を実行可能にするために，行動規範の修正や整備も必要になる．これらの諸原則の適用対象は，特定の業界分野（銀行，保険，債権回収，公益事業，医療など）および特定分野では一般的な慣行（テレマーケティング，遠隔有視界監視など）である．原則を適用する際には，相手の立場を配慮する必要がある．個人の権利を守る必要性を認識し，原則準拠に伴う経費が合理的に納得できる範囲を超えないようにしなければならない．

最後に，適切な資源と権限を持つプライバシー保護局が必要である．制裁規定も強化したい．一般市民が企業を提訴することだけに頼るのは，費用対効果の面でも現実的ではない．不法行為監視局は，適切な相談サービスを提供しなければならない．そのほか，行動規範の取扱いと承認，遵守しているかどうかの監視，不履行者への制裁，違反者の提訴，技術の研究，情報クリアイングハウスとしての行動，行動規範の普及や技術開発の中心となる活動もある．

人々に権限を委譲し，自分たちで適切な行動をとれるようにする．これを実現するには，啓蒙と研修が必須である．（比較的非公式の）苦情処理を企業や業界団体レベルで制度化する．（比較的公式の）苦情処理，強制執行，損害額の裁定は裁判所で行う．米国のように独立独歩を高く評価する国もあるし，そうでない国もある．規模や権力，資金力などの点ではるかに大きな政府の規制がある国では，個人の役割は小さくなる．

ここで紹介するのは代替機能ではなく，それぞれ相互に依存した機能である．ネットワーク世界の市民になり小規模会社を経営するには，大手企業や政府との電子商取引を信頼するだけでよい．

情報の公平な運用慣行を超えて

FIP原則は，1960年代の後半に生まれたものであり，その当時の情報処理機能に適したものだったようだが，技術の進歩にはまったく適合できないことが明らかになった．2000年代の情報技術（IT）はネットワークが中心で現在よりはるかに強力になることが予想される．したがって，FIP原則そのままではまったく使い物にならない．21世紀に向けてプライバシー保護のための基盤を構築するには，FIP原則を超えなければならない．

OECDの1980年版ガイドラインをインターネットに適用する是非が現在議論されているが，OECDはガイドラインの修正は不要だと主張している[11]．OECDの動機は社会的なものではなく主として経済的なものであるのが常であり，個人情報の保護を強化するのではなく，個人情報へのアクセス規制の緩和を要求する周囲の圧力を受けている．

したがって，現在のOECDの立場は容認できない．規制体制が依拠すべき情報プライバシー原則は，単なるFIPではなく，次のように拡張すべきである．

- 組織や団体はプライバシーを侵害する情報システムを正当化する根拠，使用目的，情報の用途を公開する．
- 匿名サービス，仮名サービス，個人を特定するサービス[5]の中から選べるようにする（ただし，匿名サービスの中で，実際に実行するのが不可能であったり，匿名での行為が法的に禁止されている取引を除く．仮名から本名を割り出す行為を組織的，技術的，法的に保護する）．
- IDを多重使用を禁止する．経済的な効率は明らかに犠牲になるが，複数の情報源から個人情報の照合を困難にする必要がある[3]．
- 本人の身元確認と認証用のトークン（チップカードやデジタル署名など）を個人がコントロールし，トークンの発行元を選択できるようにする．
- プライバシー保護の範囲を拡大しプライバシーのすべての側面を包括する．有視界監視や情報監視，さらにストーキング，情報検索サービス，生体識別法どの脅威に個人空間が曝されている．

まとめ

プライバシーという概念を歴史的にたどると，19世紀末に発表された米最高裁判事らによる論文にたどりつく[訳注]．この論文が注目されるようになったのは20世紀半ば以降であり，その理由は急速に進化する情報技術により情報を中心とする社会慣行が広まったことである．

訳注　翻訳執筆時点で著者の確認は得られなかったが，次の文献を指していると考えられる．Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harvard Law Review 193, 213（1890）．この論文は，http://chnm.gmu.edu/aq/photos/texts/4HLR193.htmに記載されている．

20世紀末にインターネットが人間の生活のさまざまな局面に重大な影響を与えるようになった．これに伴い，活動の場所，仕事のパターン，通信の手段，通信の相手，生活や文化も多様化した．自由という概念，法律の基礎的な概念に与えたインターネットの影響も非常に大きい．

インターネットの影響を受ける情報関連の事柄がいくつかあるが，その中の1つにプライバシーがある．情報経済という今や定着した概念および情報法という新たに登場した概念の中で，情報関連の事柄を再検討する必要がある．自分自身に関する情報が知的所有権の対象になるという考え方を急速に広める必要がある．

プライバシーは決して抽象的な権利ではない．情報法は所有とアクセスとの間の条件のバランスをとるものになるだろう．一方に，知る自由，出版する自由，表現する自由があり，他方に，あるがままである自由，隠す自由，拒否する自由がある．情報経済は信用に依存する．信用は獲得するものであり，不法侵入を許容し可能にするような制度から信用は生まれない．

プライバシーは保護可能であり情報社会の要でもある．維持可能というのは，人間の商品化への抵抗手段としてプライバシーを保護するという意味である．情報社会の要というのは，電子商取引と電子サービスを実現する手段としてプライバシーがカギになるという意味である．業界の自己規制やプライバシー強化技術の開発と適用は必要であるが，それだけでは不十分である．本論文はプライバシー保護に必要な枠組みの概略を提示した．

この枠組みの中心となる原則は，情報技術（IT）の機能と可能性がこの四半世紀にわたり大幅に向上した事態に対処するために，1980年版ガイドラインの時代遅れの規定を乗り越えなければならないということだ．

インターネットはさまざまな領域で堰を切ったように大量のエネルギーを放出し続けている．たとえば，個人相互の関係，地域社会の進展（地域社会という概念そのもの），商取引の進展などだ．プライベートな空間を維持しようとする個人の力は，インターネットの脅威には風前の灯にすぎない．ダムは壊れ始めているのだ．情報社会と情報経済に対応するプライバシー保護のための枠組みには，法制化と公共の監視機構の設置が不可欠であるとの認識を，米国が率先して諸外国と共有する必要があるだろう．

謝辞　新潟工科大学の青山幹雄先生には原稿を査読していただき貴重なアドバイスをいただきました．また，原著者のRoger Clarke氏にも電子メールでいくつか訳者の質問に答えていただいた．この誌面をお借りして感謝申し上げる．

参考文献

1) Brin, D.: The Transparent Society, Addison-Wesley, Reading, Pa. (1998).
2) Clarke, R.: Information Technology and Dataveillance, Commun. ACM 31, 5 (May 1988); www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html
3) Clarke, R.: Human Identification in Information Systems: Management Challenges and Public Policy Issues, Info. Tech. & People 7, 4 (Dec. 1994); www.anu.edu.au/people/Roger.Clarke/DV/HumanID.html
4) Clarke, R.: Privacy and Dataveillance, and Organizational Strategy, In Proceedings of EDPAC '96, Perth, Australia (May 28, 1996); www.anu.edu.au/people/Roger.Clarke/DV/PStrat.html
5) Clarke, R.: Identification, Anonymity and Pseudonymity in Consumer Transactions: A Vital Systems Design and Public Policy Issue, In Proceedings of the Conference on Smart Cards: The Issues, Sydney, Australia (Oct. 18, 1996); www.anu.edu.au/people/Roger.Clarke/DV/AnonPsPol.html
6) Clarke, R.: Introduction to Dataveillance and Information Privacy and Definitions of Terms (Aug. 1997); www.anu.edu.au/people/Roger.Clarke/DV/Intro.html
7) Clarke, R.: Information Privacy on the Internet: Cyberspace Invades Personal Space, Telecomm. J. Australia 48, 2 (May/June, 1998); www.anu.edu.au/people/Roger.Clarke/DV/IPrivacy.html
8) European Commission: The Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Brussels (July 25, 1995); www2.echo.lu/legal/en/dataprot/directiv/directiv.html
9) Global Internet Liberty Campaign: Privacy And Human Rights: An International Survey of Privacy Laws and Practice (Sep. 1998); www.gilc.org/privacy/survey/
10) Organization for Economic Cooperation and Development (OECD): Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris (1980); www.oecd.org/dsti/sti/it/secur/prod/PRIVen/HTM
11) Organization for Economic Cooperation and Development (OECD): Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet, Committee for Information, Computer, and Communications Policy, Paris (May 1998); www.oecd.org/dsti/sti/it/secur/news/
12) Smith, R. E.: Compilation of State and Federal Privacy Laws, Privacy J., Providence RI (1997).

(平成11年5月6日受付)