トピックス

インターネットとプライバシー・個人情報保護

郵政事業庁総括専門官　大寺　廣幸

1　はじめに

EU各国の個人情報を保護し、大西洋をはさむ欧米間のデータ流通の障害を取り除くセーフ・ハーバー（避難港）が昨年11月１日完工し供用が始まった。

セーフ・ハーバー構築に米国商務省等を駆り立てた天候異変の原因は、1992年、欧州評議会（Council of Europe）で検討を始め、95年成案を得、そして、98年10月25日施行された「個人データの処理における個人保護と当該データの自由移動に関する指令（Directive 95/46/EC)」である。この指令第25条に基づき、欧州委員会は、EU域外国におけるデータ保護の妥当性（Adequacy）を判断する権限、責務をもつ。妥当性を欠くと考えられるプライバシー保護の仕組みしか持たない域外国へは、個人データの流出を禁止することができる。EUから個人が特定できる情報を取得したいと考える企業などは、「妥当な」プライバシー保護を行う必要があるのだ。

米国は、EU加盟国との間で膨大なデータ流通があり、2000年のEUとの貿易額が約3,850億ドルにのぼる。データの流通は企業の血流であり、特に電子商取引では基盤そのものである。多国籍企業や国際的に事業展開を行う企業にとっては、国境を越えオフィス間で個人情報を共有しあっているのが実態だ。それらの情報とは、たとえば、個人の電話・ファクス番号、電子メールアドレスもあれば、秘密性の高い個人情報もある。保険金請求のための生命保険加入情報、クレジットカードの請求情報、新薬開発に必要な試験投与患者の情報もある。

米国側は、プライバシー保護、個人情報保護は、民間セクターの自主規制によることを原則とし、法規制はやむを得ない分野に限るべきだと主張する。EU側は、基本的人権を守るため国が包括的な法規制を行うべきだと主張する。米商務省、欧州委員会第15総局を中心に両者の間で、米国の法制度の枠組みに合うようなかたちで、この「プライバシー保護の妥当な水準（adequate level of privacy protection)」をどのように担保していくかをめぐって折衝が続いた。

昨年５月、ようやくEU・米データ保護セーフ・ハーバー協定案が定まった。ところが、７月はじめ、欧州議会は、投票総数279に対し反対票が259と、圧倒的多数で否決。本来、この協定は議会の議決を要せず、すでにEU加盟の15か国の政府がすべてこの協定を了承していたので、議会の指摘した疑問点などを書簡交換で明らかにして協定は11月発効した。

このセーフ・ハーバー協定は、この数年の爆発的なインターネットの普及発展の前に策定されたEUの個人データ保護指令を前提としているが、当然、インターネットも対象とする。

米国と欧州委員会は、データの自由流通と個人データの効果的保護をはかるためハイレベルでの

非公式対話を重ねてきた。この対話からセーフ・ハーバー（Safe Harbor、避難港）の枠組みが作られた。プライバシー保護に対する米国と欧州の規律の相違を踏まえた現実的な妥協案である。

この小稿では、昨年11月動き始めたセーフ・ハーバー協定までのプライバシー・個人報保護の枠組み構築の歩みをたどってみたい。

2　公正情報基準

2.1　個人情報とは何か。

個人情報には、個人の名前、住所、電話番号、家族状況、個人を特定する番号（例：健康保険証番号）といった基本的なものがある。さらに、資産・負債状況（預貯金・ローン）、病歴・入院歴などの健康状況などの重要な個人情報がある。

2.2　枠組みの基本

個人情報の収集・利用に関し個人の関与を確保するため、約30年にわたり米、カナダ、EU加盟国等の世界各国やOECD（経済協力開発機構）などの関係国際機関で、公正情報基準（Fair Information Practices）と一般的に言われるガイドラインが模索されてきた。個人情報を扱うプロセスは、1）収集、2）蓄積、3）分析・加工と4）配布の4つに分けることができ、各プロセスでプライバシー問題が生まれる。また、プライバシー問題は、個人どうしの間、企業などの民間部門とのかかわり、国、自治体などの公共部門との関係の3つに分けて考えると便利だ。この基準を検討するうえで考慮すべき「ものさし」は、1）データの質、2）透明性、処理のオープン性、3）特に慎重な対応が必要な健康状態、人種・民族、宗教的信条、セックスなどのデータの取扱い、4）プライバシー・個人情報保護を具体的に担保する仕組みである。

プライバシー・個人情報保護に関する公正情報基準は、世界的にコンセンサスがほぼできているが、次のようなものに要約化できる。

1）団体は、その保有する個人情報すべてに関し説明できるようにしなければならない。
2）団体は、情報を処理ないし収集する目的を特定すべきである。
3）団体は、原則として個人情報を収集するときは必ず個人の了知・同意を要する。
4）団体は、特定の目的の達成に必要な個人情報の収集に限るべきである。
5）団体は、個人の同意がある場合を除き、特定目的以外の目的のため個人情報を利用ないし開示すべきではない。（利用・開示特定原則finality principle）
6）団体は、情報を不必要に長い期間保有すべきではない。
7）団体は、個人情報を正確・完全・最新なものにしておくべきである。
8）団体は、個人情報に関し適切なセキュリティ保護措置を講じなければならない。
9）団体は、プライバシー・ポリシーをオープンにし非公開情報システムをもつべきではない。
10）団体は、データの客体たる個人がその個人情報にアクセスできるようにし、必要に応じ訂正できるようにすべきである。

2.3　欧米各国の歩み

OECDは、1980年9月、「プライバシーの保護と個人情報の国際流通を規律するガイドライン」を策定し、公正情報原則を国際的に一般化したが、その動きをリードしたのが欧米である。

⑴　米　国

米国における公正情報原則は、1973年に健康・教育・福祉省（Department of Health, Education and Welfare：HEW）がコンピュータの利活用と

個人のプライバシーとの調和をはかるため策定したものが最初である。この公正情報原則は、データ処理の透明性、蓄積個人情報へのアクセス、個人情報の二次利用の制限、誤った情報の訂正、正確性、セキュリティ・セーフガードを定めている。

公正情報基準は、米国では主として、民間企業、業界団体などによる自主規制（self-regulation）のルールの中で具体化され、さらに、特に法的にプライバシー・個人情報保護が必要な分野での立法措置の中で具体的に盛り込まれていった。（なお、個人情報の処理の透明性、二次利用に関する規定ぶりが不十分な立法例もある。）米国では、歴史的にみて民間セクターによるプライバシー侵害よりも公的機関のそれを憂慮してきた。たとえば、連邦議会は、1974年プライバシー法を成立させたが、それは、米国市民の情報を収集する政府機関を規制するものである。民間セクターへの規制は、包括的に網をかぶせるのではなく、たとえば公正信用報告法（Fair Credit Reporting Act）のように、規制範囲を限り特定の業種を対象としている。なお、個別分野ごとに規制法を定めていく方式を「Sectoral Approach」という。この米国方式は例外的で、世界的に見ると包括的なプライバシー保護法が一般的である。

⑵ EU（欧州連合）

EU（欧州連合）において公正情報基準がどのように具現化してきたか概観してみよう。

EU加盟国は、米国同様、プライバシー・個人情報の保護に熱心であるが、その規律のあり方は異なっている。プライバシー関連法の制定に慎重な米国に対し、欧州各国は、民間セクターも対象とする関連法の立法化に積極的に取り組んできた。これは、国家は、社会的危害から市民・国民を保護するため積極的な役割を果たすべきであるという伝統的な思想があるからであろう。1970年、ドイツ・ヘッセン州で世界初のデータ保護法が成立した。民間セクターにおける個人情報の取扱いの実態が十分把握できていなかったため、国レベルのデータ・プライバシー法制定は遅れた。1973年にスウェーデンが、世界で初めてデータ・プライバシー法を制定した。その後、プライバシー関係訴訟を受け、1977年ドイツで連邦データ保護法が、1984年英国でデータ保護法が成立した。このような立法過程で公正情報基準がさまざまな観点から検討され条文化されていった。

① EUデータ保護指令

また、欧州評議会（Council of Europe）では、1981年、「個人データの自動処理に関する個人保護条約（the Convention for the Protection of

図表１

制定年	法律	内容
1970	公正信用報告法（Fair Credit Reporting Act）	クレジット報告を規制
1974	プライバシー法（Privacy Act）	政府のデータ処理を規制
1984	ケーブル通信政策法（Cable Communications Policy Act）	CATV加入者のプライバシーを保護
1986	電子通信プライバシー法（Electronic Communications Privacy Act）	電子通信のプライバシーに適用
1988	ビデオ・プライバシー保護法（Video Privacy Protection Act）	ビデオ・レンタル利用者のプライバシーを規制

Individuals with Regard to Automatic Processing of Personal Data)」を採択した。さらに、OECDが「情報システムのセキュリティ・ガイドライン（Guidelines for the Security of Information Systems)」を採択した1992年、欧州評議会では、「個人データの処理における個人保護と当該データの自由移動に関する指令（EUデータ保護指令）（Directive 95/46/EC)」の作成を始めた。1995年に策定され1998年10月施行されたこの指令に基づき、欧州委員会（European Commission）は、法令の提案、政策の具体化などの作業を進めている。また、調査権限を持ち、関連条約などに違反する加盟国に対し法的制裁措置を講じるよう要請することができる。

EUデータ保護指令は、プライバシー問題に対し規制的・包括的アプローチをとっている。指令の目的は、1）個人情報の処理に関し個人を保護することと、2）国内法の調整手続を通しEU域内での個人情報の自由な流通を確保することである（第1条)。

個人情報は、特定の自然人に関する情報である。特定の自然人と直接、間接に推定できる情報を含む。たとえば、個人識別番号やその個人の属性、すなわち、身体的、生理的、精神的、経済的、文化的、社会的な個人識別の特性などの情報である（第2条)。

指令の範囲は広い。データ処理の形態は、オンライン、オフラインを問わず、手作業、機械自動処理を問わない。個人データをもつすべての組織、団体を対象にする。純粋に個人や家庭の活動を通じて利用されるデータは除かれる（第3条)。指令は、個人情報の処理に関し厳格なガイドラインを設けている。「処理」は、個人情報にかかわるすべての作業をいう。処理から例外となるのは、単純な送達だけであると解されている（第2条)。たとえば、情報をコピーすることやファイル化することも処理とみなされる。この指令のプライバシー保護の公正情報基準は、1981年にOECDで採択された「プライバシー保護と個人データの国際流通に関するガイドライン」を受けて策定された。

指令によれば、すべての個人情報は公正かつ適法に処理されなければならない。たとえば、個人は、自らの情報が収集・利用されることを知らされるべきであり、そのため、その個人に利用目的を告知しなければならない。さらに、個人情報の利用は、最初に明らかにされた目的や関連する目的に限定される。情報は、収集目的を満たすに足る必要最低限のものに限られる。たとえば、個人が電話加入に際して自らの情報を提供する場合、その情報は、バカンス旅行へ個人を勧誘することなどに使ってはいけない。また、電話加入に際し、バカンス旅行に興味があるかといった情報を要求してはならない。情報は、正確で最新のものにしておかなければならない（第6条)。

指令は、「正当な」データ処理を求めている。特別の例外の場合を除き一般的に、情報が処理されるに先立ってデータの客体たる個人の同意を得なければならない（第7条)。さらに、一定の情報については、その個人情報が処理されるときデータ客体の個人にその情報が提供されなければならない（第10条)。たとえば、データを見たり、不正確な情報を訂正したり、あるいはデータを受け取る者を知る権利を、個人が有しているような場合である（第12条)。

秘匿性の高いデータについては特則がある。「秘匿性の高い」データとは、人種・民族、政治的信条・信教、健康などについての情報である。これらのデータは、個人が明示的に同意する場合などきわめて限られたとき以外は、処理ができない（第8条)。

また、指令は、セキュリティ確保の観点から、破壊や破損、変更、無断開示・アクセスに対し、

「データを保護する適切な技術的・組織的措置」を求めている（第17条）。

さらに、指令では、データの処理にさまざまな要件の充足を要請している。データ処理に責任をもつ「データ管理者」を指名しなければならない。データ管理者は政府機関に登録し（第19条）、データ処理の前に最小限、次の事項を通知しなくてはいけない。義務的通知事項としては、1）処理の目的、2）データの客体たる個人に関すること、3）データの開示を受ける者ないしその範疇、4）第三国への情報移転の予定、5）処理のセキュリティ要件が満足しているかの事前確認に関すること（第19条）

指令に基づき、加盟国の政府機関は、データ処理活動を監督する権限・責務をもつ。各国は、独立の公的機関を置き個人データの保護を監督する。この「データ保護委員会」の権限は次のとおりである。1）データ処理活動の調査と指令の実行状況の監視、2）データ処理に介入し、データの封鎖、抹消、破壊の命令や、処理の禁止、3）データの客体たる個人からきた苦情の処理、4）委員会活動に関する定期報告の作成・発表（第28条）。

米・EU間でセーフ・ハーバー協定を締結する契機となったEU域外へのデータ移転については、指令は次のように定めている。すなわち、加盟国は、「プライバシー保護の妥当な水準」を確保できない域外国への個人データの移転を禁止する法律を制定しなければならない（第25条）。保護水準が不適当と判断されると、加盟国は当該域外国へのデータ移転を阻む措置を講じなければならない。加盟国やデータ保護委員会は、域外国が保護の妥当な水準を確保していないとみとめる場合は、相互に通報する義務を負う。

② EU加盟国

この指令を受けて加盟国は、所要の措置を講じつつある。具体的な措置としては、一定の政府機関を「データ保護コミッショナー（data protection commissioner）」として指定し、個人情報を収集する者はこの指定機関に登録しデータ保護方針を明らかにする義務を法定化するなどの措置である。

③ インターネットとの関係

これらの法規制は、もともとインターネットを視野に入れていたわけではない。しかし、インターネットも対象とするものであることを明らかにするため、1999年2月、欧州評議会は、「情報ハイウェイ上の個人データの収集と処理に関する個人保護ガイドライン（Guidelines for the Protection of Individuals with Regard to the Collection and Processing of Personal Data on the Information Highways）」を採択した。

3 インターネット時代のプライバシー・個人情報保護の問題

個人情報の収集は、インターネット登場以前ずっと昔から行われてきたことでそれ自体目新しくはない。発信者の電話番号を受信者に知らせる発信者番号通知制度（Caller ID）が導入されてから、消費者の電話番号は秘密ではなくなった。消費者の行動パターンは、通販のオーダーやクレジットカードの使用、診療カードへの記入、お客様優待クラブへの加入などを通じ把握されてきた。

しかし、インターネットの出現で、個人データの収集、蓄積などはきわめて容易になった。ウェブサイトは、広い範囲のインターネットユーザからアクセスでき、それらの人たちからサイトへの登録や調査表への記入といったかたちで、様々なデータを得ることができるようになった。さらに、ウェブ・ブラウザは、データを追跡できるようになった。ブラウザは、ユーザのパソコンのハード・ドライブに「クッキー」をつける。これはあたかも商店街の買い物客を追跡しどの店に入った

かをチェックするマーケット調査員を雇ったようなものだ。ユーザがどのようなウェブサイトにサーフィンするのか、オンラインショッピングでどのような商品・サービスを購入するか、といったことがクッキーのタグに記録され、そのクッキーを付けたウェブに送信される。ウェブサイトは、個々のユーザのインターネット利用情報にアクセスできるのだ。データの蓄積が非常に廉価にできるようになったので、より多くの企業が、より多くの人たちのより多くの情報を集めることができ、情報をより長期間保持できる。データ収集の制約であったコストをあまり気にする必要はなくなった。

3.1　クッキーとは

クッキーについて、少し詳しく述べてみよう。インターネットの技術革新が新たなプライバシー・個人情報の問題を生み出した。それは「クッキー」の存在である。

消費者の多くは、インターネットの特異点は「匿名性」だと思っている。しかし、これは多くの場合真実ではない。多くのサイトは、サイトを訪れる消費者の情報をクッキーのような技術を使って集めている。クッキーは、一種の電子タグで、インターネットを通じ訪問したサイトが、その訪問者のパソコンのハードディスクに貼り付けるのだ。クッキーは、ユーザの名前、クレジットカード番号、訪問サイト、メールアドレス、利用・購入パターンなどの情報を蓄積していく。これらの情報は、パソコンのハードディスクのクッキー・ファイルに保存され、ユーザがサイトを一層便利に使うため活用されるのが一般的だが、しばしば、ユーザが同意せず知らぬ間に集められる。いったんクッキーが貼り付くと、ユーザのパソコンのブラウザは、ユーザが訪れるサイトすべてに対し、常にそのサイトのクッキーがあるか否かをチェックする。そのサイトのクッキーがあるとわかると、ブラウザは、クッキー情報をそのサイトに送信する。

Cookie Centralは、企業がクッキーをどう活用しているかをそのホームページに掲載している。（http://www.cookiecentral.com）

①　ターゲット・マーケティング

クッキーを使えば、個人がどのサイトを訪ね、どの広告をクリックし、どのようなことに関心を持っているのか、のプロフィールをサイトが作ることができる。このプロフィールを活用し、個々の消費者に特定の広告をうつことができる。

②　ウェブサイトの追跡

クッキーを使えば、消費者がどのサイトを訪ねたか、そのサイトに幾人訪れたか、関心を引くリンクがないのでサイトから立ち去ったのはどのようなユーザか、などがわかる。

③　オンライン・オーダー

クッキーの中には、個人の購買傾向を示す情報を蓄積するものがある。時間をかけて商品・サービス（アイテム）を選んだあげくオーダーせずに立ち去ったとしても、ショッピング・バスケットにそのアイテムを入れた段階でその記録をクッキーに残すことができる。

④　サイトの個人向け特別仕様化（カスタマイズド化）

クッキーは、ニュースサイトに見られるように、ウェブサイトを個々人向けに再編集するのに利用できる。クッキーの機能を使って、個人が特に関心をもつ分野のニュースを優先的に画面に表示されることができる。

以上のような用途にクッキーは広く用いられ様々な便宜をもたらしているが、他方で、好ましくない利用の仕方も報告されている。たとえば、特定の医学情報を入手するためインターネットをサーフィンしたことを記録としてクッキーに残す

ように仕組んだ場合、そのデータは秘匿されるべき個人情報であるが、当人の了解なしに収集され第三者に売られるおそれが出てくる。

クッキーの存在をインターネットユーザは認識し、その便益とともに危険性も十分知っておく必要がある。繰り返して言えば、インターネットサーフィンの足跡、痕跡が知らぬ間に誰かに「盗まれ」、悪用される危険があるのだ。個人の名前、IPアドレス、ブラウザ、OSの種類、訪問サイトなどの情報が、簡単に集積、加工分析され、個人のプライバシーを脅かす用途に使われ、第三者に渡される危険があるのを知りその対策を講じておく必要がある。

4　インターネットでの公正情報基準

インターネットでは公正情報基準は一層重要になる。インターネットの技術特性から、特に配慮すべき点は、1）データ収集の目的の特定、2）個人情報の取扱いにかかる個人の同意、3）個人に対するデータの扱いの透明性（データ収集と蓄積個人情報へのアクセスを個人に周知することを含む)、4）慎重な扱いを要するデータへの特別の保護、5）損害賠償・復旧の仕組みの構築、である。

4. 1　連邦取引委員会の公正情報基準

インターネットを視野に入れた連邦取引委員会（Federal Trade Commission：FTC）の公正情報基準を見てみよう。

FTCは、5つの区分（告知、選択、アクセス、セキュリティ、コンタクト）に分けて原則を策定している。この基準にしたがうことで、個人はデータ収集の危険性を事前に理解し自らの情報を管理できるようになる。これらの原則は、技術革新がどのように進もうと、また、データがどのような種類のものであっても適用できる普遍性を有する。

「告知」は、個人がデータ収集のプロセスを知り自らの情報を管理するためのスタートラインとなるものであり、いわば公正情報基準の基本ともいえるものである。データを収集する者は、「どのような情報をどのような方法で収集し、どのような用途に使い、さらに、誰と共有するのか。」を明確に示す義務を負う。

この基準は、収集の事実があいまいになりがちなオンラインでは特に重要だ。ウェブサイトは、クッキーの利用の有無と使用目的を明らかにすべきである。理想をいえば、サイトは、そのホームページや情報収集ページから容易にアクセスできるかたちでリンクを張って、自らのプライバシー・ポリシーをウェブユーザに閲覧できるようにすることが望ましい。

個人は、「選択」によって、そのデータの利用を実際に管理できるようになる。選択とは、ウェブユーザが、ウェブサイトからの電子メールを受信するか否かを選択し、ユーザ自身の情報をサイトが他の企業と共有しないよう要求することができるようにすることである。選択には大別して二つの方式がある。オプト・イン（opt-in）とオプト・アウト（opt-out）である。オプト・インとは、サイトが、データを利用する前に明確な承諾をユーザから得る方式だ。他方、データ収集者であるサイトに対し、自らの情報を利用しないよう告げる方式が、オプト・アウトだ。一般的に、オプト・インのほうが、サイトがデータを利用しようとする前に個人に諾否を尋ね、ユーザがその利用の応諾を判断しなければならないので、情報保護に有用である。

また、個人は、「アクセス」によって、収集された自分の情報をたやすく検証できるようになり、また、不正確な情報を訂正させることも可能になる。プライバシー・ポリシーにおいては、個人が

どのようにすれば訂正を申し入れることができるか明らかにすべきである。アクセスが可能になることで、個人はデータ収集者のデータベースなどをモニターし自らの情報が最新のものになっていることを確認できる。

「セキュリティ」の義務づけにより、データ収集者は、データの流通・蓄積の過程でのデータへの加害行為を防止する義務を負う。窃取、消滅、破壊、改変、無許可アクセスを防ぐ措置などである。セキュリティは、ハッカーがデータベースに侵入する危険性があるので、特にオンラインでは重要だ。

公正情報基準は、データ収集者がデータ元の個人に信頼できる「コンタクト」情報を提供することを求めている。データ収集者との間に意思疎通ができることで、個人は、選択、アクセスの権利を有効に行使できるのだ。さらに、コンタクト規定があるということは、個人が苦情や質問を容易に行う手段があるということで、この仕組みの存在によりデータ収集者は、より一層の説明責任を負うことになる。インターネットでは、電子メールがユーザとサイトとの間を手軽に結び意思疎通をはかる手段になる。

5　プライバシー・個人情報保護に関するインターネット利用者へのアンケート

電子商取引の目覚しい発展とともに、消費者は、オンライン・ビジネスが個人データを収集・利活用していること、そしてプライバシーへの侵害の危険が増加していることを理解し始めた。1999年実施の調査「Personalized Marketing and Privacy on the Net：What Consumers Want」によれば、消費者の92%がオンラインでの個人情報の誤った利用を心配している。IBMの「Multi-National Consumer Privacy Survey」という調査では個人情報の誤った利用に対し一般的には不安を覚えない人でもその76%がインターネットでのプライバシー侵害を憂慮している。オンラインで個人情報がどう扱われるか不明なことが不安を掻き立て、電子商取引（B２C）に二の足を踏む原因になっているのであろう。「Cyber Dialogue E-Commerce Survey」によれば、インターネットがプライバシーに脅威を与えていると考えている人だと、オンラインでオーダーする割合は20%にも達しない。昨年４月の「Survey Shows Few Trust Promises on Online Privacy」では、インターネットを使っている家庭の92%が、オンライン企業は個人情報を機密扱いしているとは思っておらず、82%の家庭が、政府はオンライン企業の個人情報利用を規制すべきだと回答した。

5. 1　AT＆Tの「Beyond Concern：Understanding Net User's Attitudes about Online Privacy」等の調査結果

1999年４月公表されたAT&Tの「Beyond Concern：Understanding Net User's Attitudes about Online Privacy」がプライバシー・個人情報保護に関し詳しくアンケート調査を行っているのでその結果を概観してみよう。

○インターネットユーザは、自らを特定する情報を求められる時よりもそうでない時のほうが情報を提供する。

○データの種類によって慎重な取扱いが必要だ。クレジットカード番号や社会保険（social security）番号をウェブサイトに出すことに不快を感じる人が多い。また一見同じような種類のデータでも微妙な差違があるようである。たとえば、郵便の受取り住所と電話番号、電子メールアドレスでは、ほとんどの回答者が電話番号の提供を嫌うのに対し、宛先住所の提示には違和感はなく、電子メールアドレスはその中間、という結果が出た。

○ユーザは、情報開示を応諾するときにはさまざ

まな要素を考慮していることがわかった。最も重要なのは、情報が第三者と共有されるか否かである。次に大切な判断要素は、情報が個人を特定できるような方法で利用されるのか、どのような種類の情報が収集されるのか、その情報の利用目的は何か、といった点である。サイトがプライバシー・ポリシーを掲げているか、サイトがシール・プログラムの承認を受けているか、なども重要であるが、前記の事項ほど、ユーザの判断において大きな比重をもっていないようだ。

○ユーザが、クッキーのような持続的な特定コードを受け入れるか否かは、その使用目的次第であるとの結果が出た。回答者の52%は、クッキーに憂慮を示している。12%の人はクッキーとは何かを知らなかった。クッキーを理解している回答者の56%は、クッキーが自らのパソコンのブラウザに自動的に貼り付くを防ぐよう、パソコンのセッティングを変更していた。しかしながら、回答者の78%は、持続的な特定コード、特にクッキーをユーザの利用目的に合ったサービス（カスタマイズド・サービス）を受けるため必要だとして肯定的にとらえている。60%が自らの嗜好にあった広告を受けるためこのような特定コードを容認している。

○インターネットユーザは、データの自動送信を好ましくないと思っている。ウェブを一層便利に利用するためのソフト・ツールへの関心が高い一方で、大半のユーザは自らの情報をウェブサイトに自動的に送るツールを望んでいない。ユーザの関与なしに情報をサイトに送る自動送信機能をもつブラウザ・ソフトに対し、86%の回答者は、「ノー」と答えた。

○また、インターネットユーザは、自らが求めもしないコミュニケーションを強いられることに嫌悪感を抱いている。回答者は、ウェブサイトに情報を送ることによって、一方的に情報が送られるようになることに強い忌避反応を示した。たとえば、自らの名前、郵便の受取り住所をサイトに知らせ、その結果、無料のパンフレットやクーポンが送られてくることに肯定的な回答者の61%が、もし、それらの情報が他の企業にも共有され、そこからダイレクト・メールなどが送られてくるようならば、情報提供はしないだろうと答えた。

○インターネットユーザは、プライバシー・ポリシーを自らのサイトに掲載し、著名なプライバシー・シール・プログラムへ登録する自主規制と法規制のいずれが適当か、との質問に対し、興味深い結果が出た。情報提供の際に告知された目的を外れて勝手に情報が利用されることについては、48%の人が法的に禁止することに賛成した。28%は、目的外使用をサイトが定めるプライバシー・ポリシーで禁止するほうを選択。そして、58%が、サイトが定めるプライバシー・ポリシーと、Better Business BureauやAAAのような著名な団体によるシール・プログラム認定の双方で担保されることを選んだ。

このほか、Jupiter Communicationsが行った調査「Proactive Online Privacy, Scripting an Informed Dialogue to Allay Consumers' Fears」では、消費者のほぼ3人に2人（64%）は、たとえ、ウェブサイトがプライバシー・ポリシーをホームページに掲載していてもそのサイトを信用しないと答えている。クレジットカードの情報のセキュリティが不安と答えた人が78%、第三者への個人情報の販売が最も心配だという人が58%にのぼる。FOX News Opinionが昨年6月に行った調査では、回答者の69%は、医療・金融データなどを秘密にしておくことはできないのではないかと大いに心配し、90%の人は、ますます秘匿が困難になっていると答えた。

6　プライバシー・個人情報保護のためのソフト技術

インターネットでは、クッキーのように便利な反面、個人情報を個人の知らぬ間にウェブサイトに収集する技術が猛スピードで開発される一方で、個人を特定できる情報を保護するため様々なソフト技術、サービスも日々生まれている。インターネット上でのプライバシー・個人情報保護を論ずる場合、当然、その技術革新の動向を把握しておくことが必要である。代表的事例を紹介してみよう。

6. 1　クッキー撃退法

クッキーは一種の電子タグであるが、その撃退法は、1）クッキーがパソコンのハード・ドライブに付いたときにそれを知らせる、2）クッキーの付着をブロックする、3）ユーザのパソコンからクッキーを除去する、という各段階のものがある。

現在、インターネットユーザは、クッキーがパソコンに植え付けられたかを知り、それを受け入れるか拒否するかが選択できる。Netscape NavigatorやInternet Explorerといったブラウザでは、サーバがパソコンのブラウザにクッキーを貼り付けようとするときは常にその情報をスクリーン上で警告する仕組みを選択することができる。

また、インターネットユーザは、ウェブサイトから送られてきたクッキーを一個所にまとめてあるので一挙に削除できる。たとえば、Netscape Navigatorでは、クッキーはユーザのプロフィールを保存するユーザ辞書の中の「cookies.txt.」というファイルに蓄積されている。削除したければ、この「cookies.txt.」を探し出し削除すればよい。特定のクッキーの削除も可能だ。

不要なクッキーをパソコンから掃除するソフトは多数出ている。たとえば、America Onlineが開発したNetscape Cookie Managerは、Netscapeブラウザの機能だが、ユーザが個々のプライバシー・プレファレンスに基づきクッキーを探しブロックし削除できる機能を持っている。

6. 2　特定性除去サービス（Identity Scrubber）

様々なユーザの情報は、ウェブサイトを訪れた瞬間にそのサイトにパソコンから情報が送られサイトでその情報を把握できるようにプログラムすることができる。この特定性除去サービスは、インターネットを匿名のままサーフィンできるようにする機能をもつものだ。多種多様なサービスが実用化されているが、たとえば、ネットワーク・サービス・プロバイダー用に開発されたPrivadaControlは、ユーザのパソコンで機能し、ユーザのウェブページのリクエストは暗号化されてPrivada Networkに送られ、そこで、復号化される。いわば、自らのパソコンのほかに匿名性をもった第二のパソコンを持つようなものだ。これによって、ユーザはPrivada Networkを使って匿名性を保ったまま電子メールの送受やクッキーの利点であるカスタマズド・ブラウジングの便益を享受できるようになる。

6. 3　ウェブサイト・シール・プログラム（Website Seal Program）

シール・プログラムとして知られている第三者機関による実施プログラムは、企業の公正情報基準をモニターしプライバシー・ポリシーが実践されるように誘導する機能をもつ。企業等のウェブサイト上のTRUSTe、BBBonline、Webtrustなどのシールをクリックすると、ユーザは、サイトのプライバシー規約に飛ぶことができる。シール・プログラムの目的は、そのサイトがプライバシー・個人情報保護の観点で信用に足るところか

否かをシールで簡単に判別できるようにすることである。シール・プログラムは、ウェブ企業のプライバシー・ポリシーの標準化にも役立っている。その代表的なものがTRUSTeである。このシールを獲得するには幾つかの要件をもつプライバシー・ポリシーを持つ必要がある。どのような個人情報が消費者から収集されるのか。情報はどのように利用されるのか。情報は第三者と共有されるのか。消費者は、収集された情報の利用に関しどのような選択ができるのか。このような事項が開示されなくてはいけない。さらに、TRUSTeは、消費者を情報の滅失、誤用、変更から守るセーフガードを設定し、また、消費者が自らの情報を最新のものにし不正確を正す方法を開示することをウェブサイトに義務づけている。シールが承認されると、サイトは毎年、プライバシー・ポリシーとTRUSTeの要求条件に合致しているかをチェックしなければならない。TRUSTe自体もモニターするが、違反やプライバシー侵害の不安といったユーザからの情報も積極的に受け付けている。

6. 4　プライバシー・プレファレンス技術（Privacy Preference Technology）

プライバシー・プレファレンス技術とは、ユーザが個人情報の開示の許容範囲をあらかじめ決め、この条件と合ったサイトのプライバシー・ポリシーを自動的に識別する技術である。たとえば、AT&T ResearchがMicrosoftと組んで開発中のものは、MicrosoftのInternet Explorerに組み込まれる。このソフトをインストールするとブラウザ・ウインドウ上にプライバシー・ボタンが表示される。このボタンをクリックすると、ユーザは自分の情報開示の許容範囲を設定でき、ウェブサイトのプライバシー・ポリシーが自らの条件に合うかのチェックが可能になる。

また、World Wide Web Consortiumが開発中のPlatform for Privacy Preferences（P３P）は、注目すべきプロジェクトである。このコンソーシャムは、America Online、AT&T、IBM、Microsoft、Nokia、Hewlett Packard、日本電気、Citigroup、Direct Marketing Association、Center for Democracy and Technology、Privacy Alliance[1)]、TRUSTeなどさまざまな企業、業界・公益団体が参加している。ウェブを通じて収集されるデータに関し公正情報基準の開示を促進することにより、ユーザのプライバシー保護とインターネットの信頼性を向上させようとすることが狙いの技術だ。P３Pのアプリケーションによって、サイトは、ユーザのブラウザにユーザが理解できる方法でサイト自らの公正情報基準を自動的に明らかにする。この基準はウェブサイトに組み込まれており、ユーザは、その条件を判断した上でウェブサイトへのアクセスを決定できるのだ。このようにP３P技術によって個人は、自己の情報を管理し自らの情報開示条件に合ったサイトの選定が可能になる。P３Pプロジェクトのメリットは、標準フォーマットで公正情報基準を明らかにすることによりユーザがパソコン内で自動的かつ容易にその条件を照合できる点だ。本年中に、P３Pの勧告案が固められる予定である。

1）プライバシー保護の観点から自主規制の実効性を高めるため、シール・プログラムのほかに、プライバシー保護を遵守しているか否かをモニターする団体が誕生している。たとえば、Online Privacy Allianceは、個別企業や業界団体がメンバーの組織で、個人のオンライン上のプライバシー保護にかかる環境整備を推進するものである。この団体は、自主規制をさらに促進するため、会員にプライバシーの技術開発の進展状況を知らせ、議論のためのフォーラムを提供し、個々のウェブサイトが告知、選択、アクセス、セキュリティ等を内容とするプライバシー・ポリシーを構築する支援を行う。この団体には、AT&TやeBay、Disney、Yahooなどが会員になっている。

7　プライバシー・個人情報保護の枠組み構築とその推進

欧米各国では、プライバシー・個人情報保護のため多種多様な仕組みが工夫され稼動している。ここでは、米国内の自由放任主義や自主規制の状況を概観してみよう。

7. 1　自由放任主義

市場への政府の関与を最小限にし「見えざる手」が需給の最適解をもたらすという自由放任主義によれば、オンライン・プライバシーの世界においても、外部からの干渉自体は消費者の求めるプライバシー保護の水準を生み出すものにはならない。自由放任アプローチは、最大限の自由度をもたらすゆえ電子商取引の関連産業から多くの支持を集めている。自由放任はもっとも理想的なプライバシー保護の環境を生み出すと賛成派は主張する。ビジネスの成功は、消費者の選好、つまりマーケットシェアの増加しだいであり、プライバシーに関しても消費者の意向を考慮して必要な措置を各企業は自発的に講じる。何も外的な規制を加えなくとも企業は自ずからプライバシー保護に努力する。また、インターネットは本質的に急速な変貌を遂げており、すべてのサイトはプライバシー保護措置を含めその公正情報基準をその変化に迅速かつ絶え間なく合わせなくてはいけない。外的な規制はその変化に適応が難しい場合もある。このように主張する。

他方、自由放任に反対する立場からは、ビジネスは消費者の憂慮に適切に応えておらず、また、プライバシー・ポリシーを策定したとしてもそれは公正情報基準に完全に対応しているとは言い難いとの批判がなされている。消費者が十分な情報を持っていない場合、自由放任主義は本当に最適解を生み出すか疑問だ、との声もある。

理論的には、消費者がプライバシーを重視するなら、プライバシー保護に配慮するサイトを評価し、そうでないサイトの利用はやめるであろう。公正情報基準がなかったり、あったとしても遵守していないサイトから消費者が遠のけば、そのサイトは自ずと市場から退場しなくてはならない。逆に消費者の立場を尊重した基準をもつサイトは、消費者から評価されヒット数は増加するであろう。競争の激しいコマーシャルサイトでは、プライバシー重視の姿勢が消費者を魅了すると判断すれば、プライバシーに一層配慮するであろう。消費者がハイレベルのプライバシー保護を期待すれば、公正情報基準は、サイトの市場参入の必要条件になるのである。

事実、優良企業の多くがプライバシー保護を重視することのメリットを認識し始めているようだ。Electronic Privacy Information Center（EPIC）とOnline Privacy Alliance（OPA）の研究によれば、プライバシー・ポリシーをもつ人気サイトが増加している。消費者の圧力が企業行動に影響を与えているのは事実であるが、そのプライバシー・ポリシーの質となると公正情報基準の域まで達しているか否か疑問のものもあるとのことである。

1999年OPA調査（対象：94のサイト）によれば、全サイトの93%は少なくとも部分なりと「告知」し、83%が「選択」の機会をユーザに与えている。しかし、「アクセス」は50%、「セキュリティ」は51%、「コンタクト」は59%しか関連情報をサイトに掲載していない。1999年実施のGeorgetown Internet Privacy Policy Study（GIPPS）の調査結果は、なお悪い。調査した363のサイトのうち65%、236がなんらかの情報公開をしており、そのうち、89%は「告知」、62%は「選択」の情報をサイトに掲載している。しかし、「アクセス」は40%、「セキュリティ」は46%、

「コンタクト」は49%のサイトしか関連情報を出していない。公正情報基準の５つの条件を満たすのはわずか13.6%（調査全体ではわずか９%）に過ぎない。これらの調査結果からすると、自由放任は公正情報基準遵守に十分応えているとは言えないようだ。

「告知」は、掲出割合がもっとも多いものだが、その情報の質は不十分である。EPICの1999年の調査では、わずかに51%のサイトがホームページからプライバシー・ポリシーのページへリンクし、また、情報収集を行うページからのリンクはわずかに35%に過ぎない。同じ調査によれば、「告知」の質の面をチェックしてみると、たとえば、わずか58%のサイトが情報収集の理由を明示しているだけだ。クッキーを使っていることを明らかにしているのは１サイトで、EPICは、他の多くのサイトもクッキーを利用していると見ている。プライバシー・ポリシーの多くはわかりにくく、理解困難な法律用語を多用し近寄りがたい。

完全で明快なプライバシー・ポリシーがまだないということは、自由放任アプローチの限界を示している。自由放任主義は、消費者がその選好に基づき選択する能力を前提にしている。しかし、消費者がそのような決定を行えるのは信頼に足る十分な情報がある場合である。消費者が完全な情報を欠いているとき正しく選好がなされるとはいえず、したがって市場メカニズムが働いて理想的なプライバシー保護が実現するとはいえないであろう。なんらかの外からの力に促されなければ自由放任アプローチは有効に機能しないようである。

7.2　自主規制

個々のウェブサイトのレベルでは自由放任であっても、産業界レベルでは多数のサイトが自治的組織を作って自主規制が行われている。産業界の自主規制は、自由放任と同様、企業にプライバシー基準の採用に弾力度を与え、プライバシー保護への有効なアプローチと言われてきた。自主規制は、産業界の専門家やプライバシー保護の有識者が自主規制の枠組みづくりに参画でき、この枠組みを基準に各ウェブサイトのプライバシー・ポリシーの当否を判断することが可能になる。自主規制に批判的な人は、公正情報基準の実践の有効性が自主規制によって担保されないと指摘する。特に、自主規制は、プライバシー・ポリシーの質を保証するものでなく、プライバシー保護を有効に強制するメカニズムを欠いていると指摘する。

クリントン政権下この数年間は、連邦政府も産業界、公益団体も自主規制こそプライバシー問題への妥当なアプローチであるとみなしてきた。連邦政府はプライバシー保護の必要性とインターネットの急激な変化の両面を勘案し、オンライン関連産業が、政府の過度の関与を受けることなく自らのイニシャティブでプライバシー問題を解決するのがベストであるとの姿勢を貫いてきた。クリントン大統領は、1997年の「電子商取引に関する指令」の中で次のように述べている。「電子商取引の発展のため民間セクターがリーダーシップをとるべきだ。連邦政府は、産業界の適切な自主規制を促し、インターネットの成長・成功に資する技術や商取引ルールの開発に対する民間セクターの努力を支援すべきだ。」

1998年議会報告の中で、FTCは、オンライン・プライバシー保護のため、政府規制よりも自主規制のほうが効果的・効率的な手段であると述べた。(注) このスキームは、消費者、ビジネス双方のニーズをすばやく充足させる利点をもつといえよう。自主規制としては、シール・プログラム、産業界のガイドライン、プライバシー関係団体、米・EUセーフハーバー・イニシャティブなどがある。

(注)　なお、昨年５月のFTCの議会報告では、

公正情報基準を遵守する自主規制は実効性の点で問題があり、インターネットプライバシーへの消費者の憂慮がさらに強まった結果、何らかの包括的な立法措置が必要であると述べている。

⑴ シール・プログラム

シール・プログラムは、プライバシー遵守を判定するものさしとなる。ウェブサイトのプライバシー・ポリシーがプログラムの要件を満足すればサイトはプログラムのシールを有料でホームページ上に掲示することができる。消費者は、シールを見て、そのサイトがプログラムの要件に合致していることを認識し、また、シールの部分をクリックすればその要件を閲覧できる。品質を保証するシール・プログラムが広く普及しウェブユーザがたやすくわかるようになれば、シールは、サイトのプライバシー基準遵守を知らせる手早く信頼性のある判別方法になろう。ほとんどのシール・プログラムは、米国で開発され、最近、欧州のサイトにも用いられ始めた。

よく知られているシール・プログラムはTRUSTeである。1996年に構想が発表され、97年から98年にかけてすべての大手のポータルサイトの協力を得てプライバシー・パートナーシップを打ち上げた。また、Microsoft、Netscape、America Online、IBMなどの主要企業がスポンサーになっている。TRUSTeは、現在もっとも大きなシール・プログラムである。ただ、欧州からの参加はオンライン・オークションのQXL.comなどまだ少数にとどまっている。

Council of Better Business Bureausは、1998年、BBBOnlineシール・プログラムを始めた。TRUSTeに比して参加メンバーの数は少ないが、Council of Better Business Bureausの名声に裏打ちされこのシール・プログラムへの信頼は高い。AT&T、Dell Computers、American Airlines、eBayがこのプログラムに参加している。

ほとんどのプライバシー関連のシール・プログラムは、公正情報基準をカバーしており、その参加者に対し消費者へ次の事項を告知することを求めている。情報の用途、第三者との共有の有無、情報共有・提供の場合のオプト・アウトの方法、データ内容の変更方法、データ保護の方法、ウェブサイトとのコンタクト方法などである。また、シール・プログラムは、苦情処理・解決の手続を定めており、シール・プログラムが消費者とウェブサイトとの間の斡旋・仲介者となる。必要があれば苦情の調査も行う。

1999年後半に始まった新しいシール・プログラム、SecureAssureは、さらに厳しい条件を課している。他のプログラムが、消費者に明示的に告知する限り第3者との情報共有を認めているのに対し、SecureAssureは、第一次利用をこえる目的のための利用や情報共有を禁止している。また、他の多くのプログラムがオプト・インとオプト・アウトのいずれかを求めているのに対し、SecureAssureは、明示的なオプト・インの許可を得ることを条件にしている。

シール・プログラムは、公正情報基準に準拠しプライバシー問題に効率的な自主規制の枠組みを提供しているように見える。しかし、この方策にも2つの大きな問題がある。シール・プログラムへの参加が任意であり、また、公正情報基準を強制できないことだ。もっとも知られたシール・プログラムであるTRUSTeとBBBOnlineのメンバーはまだ少数にとどまっている。EPICの1999年の調査では、上位100のショッピングサイトのうちわずかに20が、このいずれかのプログラムを導入しているにすぎない。シール・プログラムは充実してきてはいるが、比較的新しくプライバシー保護にはなお完全なものとはいえない。

シール・プログラムは、その規定を強制する手段は現在もないし将来的にもないだろう。紛争解決や調査の手段はあるが、違反からの十分な原状回復には程遠い。もっとも厳しい制裁は、シールを無効にすることだ。確かに違反したサイトに対する悪評とはなろうが、プログラムそれ自体は、直接的な制裁はできない。

TRUSTeは、プロファイルの苦情事例に対するアクションに消極的な姿勢を示してきた。1998年、FTCは、ウェブサイトのGeoCitiesにかかるプライバシー侵害事件を審査したが、その審査の過程で、GeoCitiesは、プライバシー遵守基準に違反しながら、一方でTRUSTeへ申請しシールを付与されていたことが明らかになった。TRUSTeは、FTCの審理終了まで沈黙を守った。また、1999年3月、Microsoftは、そのソフトウエアに追跡可能な独自の識別符号を埋め込みTRUSTeのシールに違反した。しかし、「Microsoftは、消費者のプライバシーに配慮すべきだが、TRUSTeとの契約違反はない。」とTRUSTeは判断し、この事実を荒立てなかった。さらに、1999年後半、ハッカーが、MicrosoftのHotmailのセキュリティ上の欠陥を見つけ、何千もの個人の電子メール・アカウントが侵入の被害にあったが、問題が公になるまでTRUSTeは、事態を放置し、その後もMicrosoftが問題を解決する手助けに、外部の会計事務所を雇っただけであった。Microsoftの事例は、MicrosoftがTRUSTeの有力なスポンサーであることから特に問題となった。TRUSTeがMicrosooftを譴責しようとしないのは、利害の衝突から来るのではないかとの見方もあった。

⑵ 産業界のガイドライン

産業界のガイドラインは、その産業に特有の基準を設けようとするもので、ダイレクト・マーケティング協会（DMA）やバンカーズ円卓会議（Bankers Roundtable）のような業界団体を通じて設定されている。これらの団体は、個々の産業の事情に精通しているので、会員企業にふさわしいプライバシー・ガイドラインを決めることができる。理論上は、ウェブサイトすべてを対象とするものよりも個別ビジネス事情を勘案して定めるプライバシー保護基準のほうが実効性もあり効率的である。

いくつかの業界団体が、会員企業のためプライバシー・ガイドライン、行動指針を作成した。DMAは、1999年、「プライバシー誓約」（Privacy Promise）を定め、その中で、会員企業は、「情報共有や勧誘のときにその情報を利用されないよう求める消費者の権利」を、消費者に告知することを定めている。DMAは、会員企業向けにオンラインでそのガイドラインの解説を提供している。1999年、財務省の貯蓄金融機関監督室（Office of Thrift Supervision：OTS）は、その監督下のS&Lなどの金融機関がオンライン取引を行うウェブサイトにプライバシー・ポリシーを掲げることを求める規則を公表した。OTSは、金融機関に次のような義務を課した。1）利用者にその情報がどのように使用されるか告知すること。2）金融機関が情報使用を制限する権利を利用者に与えること。3）利用者の情報が正確で安全に保護されること。

残念ながら、産業界のガイドラインの多くは、公正情報基準を完全に満たしていない。FTCは、議会への1998年報告のため9つの業界向けガイドラインを調べた。その結果は次のとおりであった。情報収集の告知義務はすべてのガイドラインが明示している。大半のガイドラインが、情報共有の可否について個人の同意を求めている。ところが、アクセスやセキュリティへの言及は事実上どのガイドラインにも見当たらない。特に重要な点は、

どのガイドラインも、業界のガイドラインの実効を確保する強制の仕組みを用意していないことだ。Magazine Publishers of Americaのようなところは、単に参考資料、模範としてプライバシー原則を掲げるだけで、その会員に原則の採用を要求していない。会員に業界のガイドラインに従うことを要求するものもあるが、その義務づけの程度は弱い。最悪、業界団体は、除名処分をすることが可能でその企業が評判を落とすことにあろう。しかし、このような制裁も違反企業にとって苦痛になるとは必ずしも言えず、侵害された個人へ損害賠償となることにはならない。

8　セーフ・ハーバー協定

冒頭述べたように、セーフ・ハーバー（Safe Harbor：避難港）は、「プライバシー保護の妥当な水準」を確保できない域外国への個人データの移転を禁止するEUのデータ保護指令と、プライバシー・個人情報保護は、民間セクターの自主規制によるとする米国の間で作られた知恵の産物である。

セーフ・ハーバー協定は、米国・EUの行政当局間の取決めとして、データ保護指令の「プライバシー保護の妥当な水準」を確保するフレームワークをとりあえず構築し、国際公法レベルではこれで指令の条件を充足したことにする点にまず意義があったように見える。

EUの立場を尊重し、米国企業等へ好ましくないデータ移転を避けるため、EUが裁量的に執行権限を行使するというEUの政治的合意（セーフ・ハーバーの一時中断）は有効である。また、セーフ・ハーバー協定は、今年半ばにその履行状況を検証することになっている。そのとき、前記の一時中断も検討対象になる。

他方で、米国の理念である自主規制の建前が工夫して協定に組み入れられている。セーフ・ハーバーの枠組みに入るか否かは、米国企業・団体の任意とし、この枠組みから脱退することも任意にしてある。米国企業・団体は、この枠組みに入るに際しセーフ・ハーバーが求める条件に合致していることを自己診断しその旨を公告することが条件だ。商務省は、その企業等のリストを公表する。セーフ・ハーバーによって、EUから米国へのデータ移転に関わる欧米企業等には予見可能性と継続性のメリットが生まれる。セーフ・ハーバー協定が定めるプライバシー原則は、指令の妥当性基準に適合するものとみなされる。セーフ・ハーバーに参加すれば、データ移転の事前承認が不要になり自動的に承認されるようになる。このプライバシー原則の違反行為は、一般的には具体的な個人からのプライバシー侵害の訴えをもって顕在化し、その問題解決は裁判外の調停・和解手続きの活用が期待されるようだ。プライバシー原則の違反行為は、一般的に連邦取引委員会法第5章の不公正取引（詐欺・欺もう行為）とみなされる。連邦取引委員会法がプライバシー原則遵守の担保として機能する仕組みとなっているのだ。ただ、連邦取引委員会法の管轄外の通信事業者などに関する取扱いには不明瞭な点が残っているようである。

9　終わりに

連邦取引委員会は、昨年5月の議会への報告「Privacy Online：Fair Information Practices in the Electronic Marketplace」の中で、次のように強く包括的なプライバシー・個人情報保護法の制定を強調している。

9.1　報告書の要点

電子商取引は、急速に発展を遂げている。同時に技術革新は、ウェブサイトに訪れる消費者の膨大な情報を収集・蓄積・移転・分析する企業の能

力を飛躍的に高めている。このデータ収集・利用の増大はプライバシーへの消費者の不安をさらにかきたてている。電子商取引への消費者の信頼を確保し、電子商取引市場を発展させるため、この消費者の不安に対し対策が必要だ。

連邦取引委員会は、インターネットを含むオンラインでの公正情報基準をより一層実効性あるものにするため、立法措置が必要であるとの結論に達した。

1998年の議会報告では、ほとんどすべてのウェブサイト（92%）が消費者の個人情報を収集し、その一方で程度の差はあるにせよなんらかの形で情報基準を開示しているサイトはわずかに14%に過ぎないことを明らかにした。この報告では、告知、アクセス、セキュリティの公正情報基準の原則を詳述し、プライバシー保護のため、行政的措置や自主規制の枠組みを推奨した。

1999年、Georgetown大学のMary Culnan教授が行ったGeorgetown Internet Privacy Policy Surveyでは、プライバシーの開示頻度で顕著な改善傾向が見られたが、４つの公正情報基準をすべて開示しているのはわずか10%のサイトであった。この結果から、1999年の報告では、自主規制がうまく機能するか否かの見極めにはなお時間が必要で、民間企業等の公正情報基準の実践への努力を喚起した。

2000年２・３月行った連邦取引委員会の調査では、ほとんどすべてのサイトが電子メールアドレスやその他の個人を特定する情報を収集していた。335のサイト中20%のみが４つの公正情報基準を開示しているに過ぎなかった。確かにアクセス、セキュリティ原則の遵守は困難と考え、告知、選択に限ってその原則の実行状況を調べたが、335サイト中41%しか守っていなかった。主要な自主規制の手段であるシール・プログラムについて調査したところ、わずかに８%しかシールを表示していなかった。

このような調査結果を踏まえれば、確かに将来的にも自主規制は大きな役割を果たすであろうが、連邦取引委員会としては、自主規制とともに消費者のプライバシー保護のための立法措置が必要だと結論せざるを得ない。

9. 2　プライバシー・個人情報保護に対する我が国の取り組む視点

わが国では、今国会に個人情報保護法案が審議される予定だ。米国においても、このような連邦取引委員会の見解を受けて、包括的なプライバシー・個人情報保護法が誕生するかどうか注目が集まっている。

また、今後、電子商取引のみならずさまざまな形態でのインターネット利用が国境を超えて進んでいく。個人情報の保護の枠組みは、国際的な協調を視野にいれなければ一歩も前進しない状況である。Information Heavenや治外法権を生みださない工夫が必要だ。公正情報基準は、その大枠が収斂化しているといっても、個人情報の範囲、透明性基準、告知条件などに関し解釈はEU加盟国内でも微妙に異なる。その実効性を担保する法的強制メカニズムは、管轄権、裁判外の紛争処理手続き、復旧・損害賠償措置などの面で、各国で多種多様である。ますますの国際連携が求められるであろう。他方で、インターンネットが優れて技術指向であり、その技術革新が、コインの表と裏のように、経済社会、生活に多大な恩恵をもたらすとともにプライバシー侵害も拡大する危険性を内在していることに留意することが大切だ。

個人・民間セクターの自由競争の優位と国家・社会秩序の安定のいずれに優位に置くかなど、大西洋をはさんで大きな価値観の相違がある米国とEUがセーフ・ハーバー協定を作り上げた両者の努力は、十分吟味すべきである。インターネット

を通じての情報交流や電子商取引が国境を超えてますます進展する21世紀、国際的なプライバシー・個人情報保護の新たな枠組みづくりにわが国も積極的な参画ができるよう、国際対話・協力、政策提言、技術革新等、官民協力して進めていくべきだと考える。