財産権的アプローチを利用したインターネット上における個人データの保護

橋本　誠志

あらまし

ブロードバンドサービスの普及に伴い我が国は本格的なインターネット常時接続時代へと突入している。インターネットに長時間接続するユーザーが増加するにつれ、インターネット上にユーザーの個人データが流出する危険性は拡大する。精度の高い個人データが一旦、ネットワーク上に流出すれば、データ主体は、たとえ犯人が逮捕された後も私的生活の平穏を脅かされるリスクを常に背負う。個人データの流出予防策に加え、実際にデータが流出した際の被害拡散防止策の充実が今後のインターネット上の個人データ保護政策にとって不可欠である。

現在のプライバシー侵害の主な救済手法である不法行為構成には、要件上の限界が存在し、権利保護に費用と時間がかかるばかりでなく、①賠償額も低額しか認容されない、②立証責任、時効面で柔軟性に欠ける、③権利保護の程度が貧富の差に左右される等の問題がある。近時では、情報主体と事業者間において契約関係が存在する場合、事業者がデータ主体の同意した範囲を超えた情報取扱をした場合に債務不履行責任を認める契約アプローチが提唱され、米国では、既にインターネット上での個人データ保護政策のフレームワークとして利用されている。しかし、我が国では事業者のプライバシーポリシーの監視制度やプライバシー保護団体のサポートが機能しておらず、契約アプローチの実効性は期待できない。

本稿では、近時のプライバシー保護技術の動向に鑑み、インターネット上への個人データ流出した際の被害拡散防止手法として、財産権的アプローチの有効性を検討し、インターネット上での個人データの交換にライセンス制の導入を提案する。

１．はじめに

我が国のインターネットを取り巻く環境は、ブロードバンドサービスとIP接続機能が搭載された携帯電話の普及に伴って本格的な常時接続・モバイル接続時代へと突入している。こうしたネットワーク環境の整備により、インターネットに長時間接続するユーザーが増加するに従って、インターネット上にユーザーの個人データが流出するリスクは更なる拡大を見せている。特にインターネット利用者の低年齢化は今後、問題をさらに深刻化させる危険性がある。最近のインターネット上への個人データの流出事例を見てみると、情報統合によらずともそれだけで個人の全体像を十分把握しうる精度の高いデータが万単位という膨大な数で流出しやすい傾向を示している。デジタル情報の加工性とボーダレス性により、一旦、精度の高い個人データがインターネット上に流出すれば、データ主体は、犯人逮捕後も、執拗な迷惑電話や勧誘にさらされる等、その私的生活の平穏を脅かされるリスクに晒されることになる。個人データの流出予防策の更なる強化に加え、プライバシー侵害が実際に発生した際に備えての被害拡散防止策の充実が今後のインターネット上での個人データ保護政策にとって不可欠である。

我が国ではプライバシー侵害が発生した際の救済手法として、これまで、不法行為アプローチが主に利用されてきた。しかし、不法行為アプローチには、個人情報がプライバシー権の保護

対象になるか否かの点で要件上の限界が存在し、費用と時間がかかるばかりでなく、①賠償額が低額しか認容されない、②立証責任、時効面で柔軟性に欠けると言う難点がある。そこで、近時では、情報主体と事業者間において契約関係が存在する場合、データ主体の同意した範囲を超えて、事業者が第三者に対して情報を提供した場合に債務不履行責任を構成することで、被害者の立証責任を軽減しようとする契約アプローチも提唱されるに至り、米国では、既にインターネット上での個人データ保護政策のフレームワークとして広く利用されている。しかし、FTC（Federal Trade Commission）による監視やプライバシー保護促進団体、あるいはPrivacy Service Providerによる事業者へのコンサルティングや啓発活動が盛んな米国と異なり、我が国ではこうしたプライバシー保護問題に特化した団体による消費者に対するサポートが機能していない。そのため、契約アプローチの実効性は期待できない。

本稿では、インターネット上でのプライバシー侵害救済のための政策手法として第３のアプローチである財産権的アプローチの有用性を検討し、財産権的アプローチによる政策提言として、インターネット上での個人データの交換にライセンス制の導入を提言する。

２．わが国のインターネット環境の変化と個人データの流出

総務省が行った通信利用動向調査によれば、平成13年末における我が国のインターネット利用者数は5,593万人（対前年比18.8%増）と推計され、１年間で885万人の増加を示し、人口普及率は44.0%となっている。2005年には、インターネット利用者数は8,720万人に達すると見込まれている[白書]。近時、我が国のインターネット環境は大きな転換点を迎えている。第１に携帯電話等の非PC端末からインターネットに接続するユーザーが増加している。社団法人電気通信事業者協会のまとめによれば、2002年９月末時点での携帯電話契約数72,081,000回線のうち、IP（インターネット）接続サービスの加入数は57,112,700回線（79.2%）[1]を突破し、実に我が国総人口の約44%[2]が携帯電話を利用して、インターネットに接続することが可能となっている。こうしたモバイル端末の利用者増加と相俟って、インターネット利用者の年齢低下傾向は顕著に進行している。第２には、DSL等ブロードバンドサービスの普及に伴う本格的なインターネット常時接続時代の到来である。例えば、2002年８月末現在でADSL[3]接続サービスへの加入者は、3,915,740回線に達し、2001年１月実績との比較で242倍もの急激な増加傾向を示している（図１）。また、光ファイバーを利用した一般家庭向けFTTH（Fiber To The Home）インターネット接続サービスへの加入者数も2002年８月末現在で99,404回線を数えている[4]。

以上のように、我が国では本格的なインターネット常時接続時代に突入すると同時に、本格的なインターネット・モバイル接続時代に突入している。しかし、こうした本格的なインターネット常時接続・モバイル接続時代への到来に伴い、ユーザーの個人データがインターネット上へ流出するリスクは急速に拡大している。各ユーザーのインターネットへの接続が長時間化し、ユーザーの個人データを窃取しようと試みる攻撃者のアタック機会が増加したこととインターネットに長時間接続するユーザー数が増加することによるターゲット数の増加がパラレルに進行するためである。

今日、事業者にとって経済的価値をもたらすユーザーの個人データをターゲットに知られないようにインターネット上で収集する技術はより巧妙化している。これまで、インターネット上

---

[1] http://www.tca.or.jp/ (2002.10.9確認)

[2] 総務省統計局「人口推計調査結果・全国，年齢５歳階級別人口」平成13年10月確定値の１億2729万人により算出(http://www.stat.go.jp/data/jinsui/2.htm) (2002. ３．９確認)

[3] Asymmetric Digital Subscriber Line. 電話線を使って高速なデジタルデータ通信を行う技術(xDSL)の一形態であり、メタル電話回線に高周波信号を伝送させてデータ通信を行う。信号の伝送速度は電話局→利用者方向(下り)が1.5～９Mbps、利用者→電話局方向(上り)が最大16～640kbpsであることから「非対称(asymmetric)」の名がついている。最大伝送距離は5.5km(下り1.5Mbps)～2.7km(下り９Mbps)。xDSL技術の中で最初に実用化され、すでに一般家庭に広く普及している電話線を利用して、インターネットへの高速で安価な常時接続環境を提供する技術である。

[4] http://www.soumu.go.jp/s-news/2002/020930_7.html (2002.10.15確認)

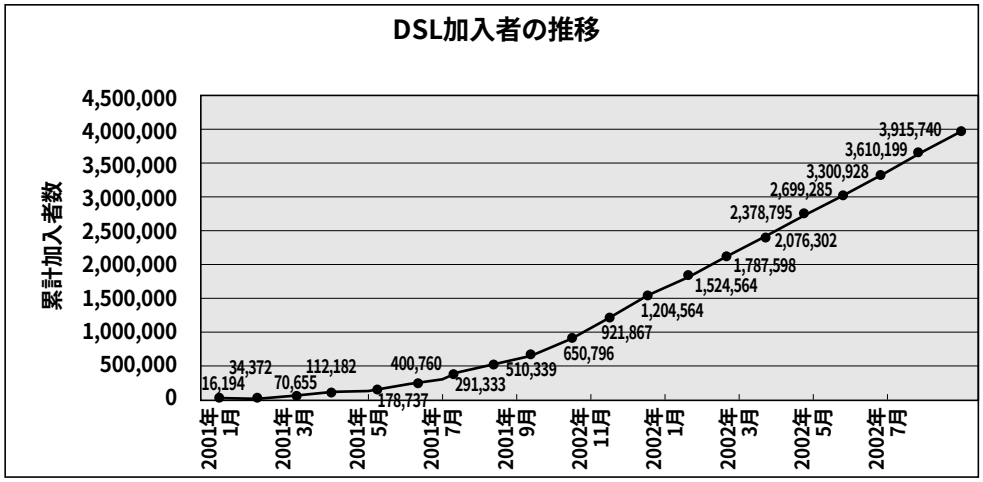

図１　ADSL サービス加入者数の推移（2002. 8 .31 現在）[5]

でユーザーのHPの利用動向を収集する技術としてPC内に変数名と変数値を打ち込み、これらPC内に登録されたIDをユーザーがサーバーにアクセスした際に読み取ることで、ユーザーのインターネットの利用動向を収集する技術であるCookieが知られている。現在では、Cookieによるプライバシー侵害に対する対策として、Cookieの動作をユーザーに制御させるシステムを組み込んだソフトウェアが実際に市場に投入されている。しかし、近時では、ディスプレイの画像ファイルにカモフラージュされ、PC内に痕跡を残さないWeb Bugと呼ばれる技術が新たに登場し、データの収集方法がより巧妙化している[前川2001][6][7]。また、Webブラウザーソフトや PCのオペレーティングシステム（OS）そのものにも個人データ流出の危険があるプログラム上の欠陥であるセキュリティーホールが多数発見されており、こうしたセキュリティーホールを悪用したコンピュータ・ウィルス等の不正プログラム群によりPC内に保管されたユーザーの個人データが第三者に流出する危険性が高まっている[8]。このようにインターネット上を流通するプライバシーに関する情報は、その加工の容易さとも相俟ってより傷つきやすいものへと変化している。

（表１）は、1999年以降の我が国における個人データのインターネット上への主な流出事例を抽出したものである。近年の流出事例を見てみ

[5] 総務省 DSL 普及状況公開ページ(http://www.soumu.go.jp/joho_tsusin/whatsnew/dsl/) (2002.9.30 確認)

[6] Web Bug は、一般的には１×１ピクセルの GIF 形式の画像データの形態を採っている。埋め込まれたページと同じ背景色でカモフラージュされており、ディスプレイ上からの視認による判別は不可能である。Web Bug にはアクセス履歴等ユーザーに関する情報を収集する HTML コード（実際のコーディング例は、付録を参照）が埋め込まれている場合があり、Web Bug が仕掛けられた Web ページとは全く異なるサイトに収集したデータを転送できる。具体的には、Web Bug が埋め込まれているサイトの URL と埋め込まれた位置、当該ページが読み込まれた日時、PC の OS の種類、ディスプレイ解像度、直前に設定された Cookie に関する情報等が収集・転送されることがある。

[7] 例えば、Microsoft 社のブラウザ、Internet Explorer 5.5 Service Pack 2(5.01SP2)以降のバージョン、及びビジネスプラットフォーム Office XP 等ではアプリケーションが動作停止した場合、エラー内容を Microsoft 社に報告するウィザードが搭載されている。こうしたエラー情報にはエラー発生時のコンピュータのメモリイメージが含まれることがあり、個人データ流出の恐れがあることが一部から懸念されている。http://cnet.sphere.ne.jp/News/2001/Item/011019-3.html (2001.10.23 確認)

[8] 2001 年 11 月には、Microsoft 社の Web ブラウザ Internet Explorer 5.5SP2 と IE6 に Cookie データがどのサイトにも流出しうる重大なセキュリティーホールが発見され、Microsoft 社は、修正プログラムをリリースする問題が発生した。同社の製品にはこれ以外にも多くのセキュリティーホールが発見されている。

表１　最近の我が国における主なインターネット上への個人データ流出事例

1999	5	京都府宇治市で住民基本台帳記載の 21 万人分の個人情報がインターネット上に流出
2000	3	大塚製薬のサイトから 9900名分の顧客情報が流出。住所、氏名、年齢、電話番号、メールアドレス、身長、体重、妊娠の有無と妊娠期間、睡眠時間や日常の運動量等が記録。
	4	ビデオレンタル店の延滞客情報 25,000人分のリストが収録された CD-ROM がインターネット上で売買されていたことが発覚
2001	7	ソニーシービーラボラトリーズ（化粧品製造）の顧客リスト１万人分の保管先 URLが流出
	7	サクセス（PC 関連機器販売）のサイトから顧客情報と購入商品情報数万人分が流出
	5	エステティックサロン大手「TBC」を運営するコミー（本社・東京都新宿区）のサーバーから資料請求・アンケート回答者 3 万 7810人分の個人データが流出。ボディサイズやエステに関心を持つ理由に関する情報も記載。
2002	6	原田泰治美術館（長野県諏訪市）のＨＰから、来館者などの住所や名前などの個人情報延べ約６７００人分が流出。
	8	カバヤ食品(本社･岡山市)の HP に 30回の不正アクセス。懸賞応募者の住所、氏名、年齢、性別、職業、電話番号、メールアドレスなどの個人データ 3244人分が流出。
	8	家庭用ソース大手のブルドックソース（東京・中央区）のＨＰ上で懸賞応募者やメールマガジン購読者の氏名、住所、電話番号や職業など約４万５千人分の個人情報が流出

（岡村久道「情報法学日記」http://www.law.co.jp/okamura/nikki/nik_now.htm を参考に作成）

ると、①１回の流出で万単位という多量のデータが流出する、②情報の精度がより高くなり、住所、氏名、年齢、電話番号、メールアドレスと言ったアクセス情報に加え、身長、体重と言った容姿を連想させる情報、妊娠歴、睡眠時間や日常生活での運動量、使用している化粧品の種類・数量等と言った情報主体の生活の全体像を情報統合[9]によらずとも直接暴き出しうるのに十分な情報が含まれやすいといった傾向がより顕著になってきている。このように個人の全体像を直接暴き出す内容を含んだ個人データがデジタル化された形で多量に流出しやすい状況下では、①たとえ、犯人を逮捕・処罰しえたとしても、コピーされたデジタル化データが拡散し、一人歩きすることにより、犯人逮捕後も執拗にかかる迷惑電話や勧誘にデータ主体は苛まれ続けることになる。②情報統合に要する手間とコストがこれまで以上に低下し、個人の全体像を容易に暴きうることになる。

３．我が国の個人データ保護政策の問題点

上述のように我が国においてもインターネット上へ流出する個人データは、今日、大量かつ詳細化している。[橋本2002]では、我が国の個人情

[9] インターネット上での情報統合によるプライバシー侵害に関しては、[橋本・本村・井上 2000]、[本村・橋本・井上・金田 2000]を参照

報保護政策を法規制アプローチ（政府機関を対象とした個人情報保護法、各個別法における限定分野での個人情報保護に関する規定、並びに各地方自治体の条例）、及び自主規制アプローチ（民間部門による自主規制と補助金制度）に分類して、その動向を整理した。例えば、JIPDECのプライバシー・マーク制度は、BBB-Onlineマークとの相互認証が2001年7月よりスタートするなど、国際連携の動きが広まる等、確実にそのレベルはアップしてきている。しかし、我が国の個人情報保護政策には、依然として多くの問題点がある。以下、特徴的な点を概観する[10]。

3.1 法人の「プライバシー的情報」

第1は、法人が有するプライバシー的情報が保護されていない点である。憲法学上、プライバシー権は、自然人の他、法人にも適用されうると解されている[芦部99][佐藤幸95]。しかし、現在、審議中の個人情報保護法案では、「個人情報」とは「生存する個人に関する情報」であることが必要とされている。（個人情報の保護に関する法律案2条1項）このため、法人は、個人情報取扱事業者としての義務は負わされているものの、自社のプライバシー的情報の侵害に対しては、同法案の保護対象に入っていない。この点、秘密として管理されている生産方法、販売方法其の他の事業活動に有用な技術上又は営業上の情報であって公然と知られていないもの（不正競争防止法2条4項）、例えば、顧客名簿やノウハウ等の情報は、営業秘密として、その不正な取得行為（同2条1項4号-9号）を営業秘密に係る不正行為として、不正競争防止法3条で差止請求を認めており、同13条1号により罰則が課される。しかし、企業の役員又は従業員の個人的なスキャンダルと言った情報に関しては、本法の保護対象外となっている[小野94]。また、営業秘密と認められる情報でも、インターネット上に散在したデータを合法的に収集し、マージする情報統合のように窃取・詐欺・強迫と言った信義誠実に反する手段でない情報の取得行為は、本法の適用対象外となる。そのため、事業者は、個人情報取扱事業者としての義務を負わされるのみで、自社のプライバシー的情報の保護手段は限定されている。

インターネットユーザーのプライバシー保護の観点からも法人の有する秘密情報保護法制が不十分である現状は、憂慮すべき事態である。現行法では、事業者が管理する顧客名簿等が窃取・詐欺・強迫と言った信義誠実に反する手段で流出した場合であっても、ユーザー自らが不正競争防止法に基づいて、法的救済を請求することができない。そのため、事業者の法人プライバシー情報の適切な保護はユーザーのプライバシー保護の観点からも喫緊の課題であり、法人プライバシー情報保護のための具体的な政策プログラムが提供されていない現状は問題である。

3.2 子どものプライバシー情報の保護

第2に我が国では、子供のオンライン・プライバシー保護政策が確立していない点がある。米国では、1998年10月に、“The Children’s Online Privacy Protection Act”（COPPA）が制定された[11]。本法では、13歳未満の子供から氏名、電子メールアドレス、電話番号、社会保障番号等個人について識別可能な個人情報[12]をインターネット上での収集に際して、子供から当該情報を収集する可能性があるすべてのWebサイトのオペレーターに以下の事項を義務づけている[13]。

---

[10] 2001年3月27日に衆議院に提出された個人情報の保護に関する法律案は、2002年1月21日、衆議院内閣委員会に付託された。また、2001年10月26日には行政機関等個人情報保護法制研究会による『行政機関等の保有する個人情報の保護に関する法制の充実強化について－電子政府の個人情報保護－』報告書が公表され、これを素に2002年3月15日、行政機関の保有する個人情報の保護に関する法律案、独立行政法人等の保有する個人情報の保護に関する法律案、情報公開・個人情報保護審査会設置法案等関連法案が衆議院に提出された。

[11] 子供のプライバシー情報の保護に関する米国での自主規制の取組に関しては、[橋本2002]で検討した。

[12] 15 USC § 6501(8)　その他、FTCが物理的に、またはオンラインで連絡を取りうると認めたその他身元に関する情報、ウェブサイトが子どもから収集し、上述した身元情報と照合しうる子どもまたは子どもの親に関する情報なども本法に言う個人情報に含まれる。

[13] 子供を主対象にしない一般のサイトでも子供を対象としたキャンペーン等を行うために子供の個人情報を収集する場合等には本法が適用される。

① 個人情報の収集、使用方法、開示方法の両親への告知
② 個人情報の収集、使用に際する検証可能な方法での親の同意
③ 保護者からの要請による当該情報の保護者への確認手段の提供
④ 情報の再収集、二次利用の防止機会の両親への付与
⑤ ゲームやコンテスト等の参加のための個人情報収集を当該活動の合理的範囲に限定
⑥ 収集情報のセキュリティーと保全性に関する手続の設定と維持

これらのうち、②の事前検証可能な方法での親の同意とは、子供から個人情報を収集する前に利用可能な技術を考慮し、親がWebサイト管理者から個人情報の収集・利用、開示慣行の通知を受けた上で同意を得ることができるように合理的な努力をすることを意味し、①郵送またはFAX、②同意画面へのクレジットカード番号の入力、③フリーダイヤル、④公開鍵方式の電子署名付きメール等を単独および相互に組み合わせた形態でなされることが必要とされている。[14]但し、以下の場合に例外がある。つまり、①親からの同意を取得、あるいはポリシーの通知を行うために必要な親または子へのインターネット上でのコンタクトに必要な情報、②子からの特定の要求に直接、1回限り応答するために必要で、当該コンタクト情報を再利用しない場合、③子からの特定の要求への直接応答するために必要で、2回以上コンタクト情報を利用し、親に再利用の中止要求機会を設けている場合、④子供の安全保護目的にのみ利用し、再利用・サイト上への開示をしない上で親への通知をした場合、⑤サービスの安全性や責任の警告、司法当局等への提供に必要な範囲での収集である[丸橋2000]。

上記通知の詳細な仕様を定めるものとして、COPPA施行規則であるChildren's Online Privacy Protection Rule, 16 CFR Part312でポリシーの掲示が義務づけられた。この掲示義務についての詳細は、文献[増田・舟井・アイファート＆ミッチェル法律事務所2002]に譲るが、子供の個人情報の収集を担当する可能性がある全オペレーターの氏名、住所、電話番号、E-mailアドレスの掲示を義務付けている点は、非常に特徴的である。

COPPAが適用された代表的な事件がToysmart事件である。オンライン玩具販売業者であったToysmart.com Inc.は自社のWebサイト上で収集した情報の第三者との共有を決して行わない旨のプライバシーポリシーを掲示したうえで、氏名、住所、メールアドレス、請求書情報、家族構成、子供の誕生日に関する情報等を収集していた。しかし、同社は経営不振に陥り、2000年7月、破産宣告を受けた。破産宣告を受けた同社は、保有資産の売却に関して、プライバシーポリシーで第三者への譲渡をしないと宣言していた個人情報データベースを保護者の同意なく売却しようとした。このため、FTCは、2000年7月、同社をプライバシー規則に関する不実表示を行ったものとして、FTC法違反により提訴した。提訴後、FTCは、Toysmart社に対して、家庭向け商品業界の適格な買主に会社毎売却される場合に限って、同社が有していた個人情報データベースのデータを譲渡できるとする和解案を提示した。しかし、2001年1月になっても同社の買主は現れなかったため、Toysmart社の大株主であるインターネット関連会社がToysmart社の有していたデータを買い受けた上で破棄する結果となった[増田・舟井・アイファート＆ミッチェル法律事務所2002_2]。

以上のように米国では、子供のオンライン・プライバシー保護について、親の本人確認の真正性確保に関する問題等今後の改善を要する事項は残されているものの、事業者に個人情報の収集手続を厳格化する対策がなされ、将来的には、子供の保護に限らず、より広範に制度が運用されてゆく可能性がある。しかし、我が国では、上述したように、携帯電話によるインターネット接続の普及により、インターネット利用者は、更に低年齢化しているにもかかわらず、子供の個人情報保護の問題に対しては、その認識が薄く、子供を対象とした個別法制を制定する動きは見られない。

3.3 事業者の経営破綻処理と個人データ保護

[14] これらの要件については、クレジットカード番号による親の同意確認による手法では、①子による親へのなり済まし、②親の重要な個人情報が子供により窃用される危険性、③親の本人確認の精度をどこまで担保すれば良いのかと言う問題が指摘されている。

第３は、我が国の個人情報保護政策は、事業者の経営破綻に対応していない点である。米国では、上述の Toysmart 社の経営破綻を機に倒産企業の個人情報利用ガイドラインを策定する動きが加速し、2001年10月11日には、米国でプライバシー認定マークを発行している非営利組織である“TRUSTe”が“Privacy Guidelines for Companies Undergoing Mergers, Acquisitions and Bankruptcies”を発表した。本ガイドラインでは、①企業が保有していた個人情報を譲渡する場合、委託を受けた第三者の管理を受け、プライバシー・ポリシーを変更する場合には、消費者にその旨を通知し、適切な選択肢を提供する、②企業が倒産した場合、そのプライバシー・ポリシーを変更しないように要求している[15]。また、改正破産法（Bankruptcy Reform Act of 2001）では、会社倒産時の収集済個人情報の売買に関して、個人識別情報を自社の関連会社以外の企業と共有しない旨のプライバシーポリシーが宣言され、破産手続申立時に当該ポリシーが有効である場合、管財人に当該企業の有する個人データの売買や貸借を禁止している[16]。

このように米国では、経営破綻時の個人情報の取扱について、その保護を強化する動きがある。それに比して、我が国では、個人情報保護法案では、小規模事業者は、個人情報取扱事業者から除外されるため、これら小規模事業者が経営破綻した場合、営業譲渡によらず、個人データだけが切り売りされても、個人情報保護法の適用から除外されることになる。一方、法的義務主体となる個人情報取扱事業者（個人情報の保護に関する法律案２条３項）に該当する事業者で清算型処理がなされ、当該事業者が保有していたデータが事業と分離して、売却される場合には本人の同意が必要となる（個人情報の保護に関する法律案28条４項２号）。しかし、①Toysmart 事件の例からもわかるように経営破綻状態に陥った企業は、目先の資産売却に主たる関心を置きがちで、プライバシーポリシーは無視される危険性が高い。②データ主体は倒産企業との関係において、破産債権者の立場に当然に立つものではないため、倒産処理過程に関与することは基本的に出来ない。③現代のように一人の消費者が無数の事業者と取引をする社会において、データ主体が自己の個人データが倒産企業に登録されていることすら記憶していない場合も多い。そのため、データ主体の同意を得る手続が煩雑となり、コストがかかる。④個人情報保護法案での罰則規定の上限は６月以下の懲役もしくは、30万円以下の罰金である。また、同法案は間接罰方式を採用しており、罰則の適用に時間がかかる。そのため、自社の評価額よりも高額でデータを買い受ける買主が現れた場合、罰則と目先の資金確保を天秤にかけ、後者を優先させてしまうことが考えられ、こうした場合、個人データ保護の実効性は期待できない。

一方、民間部門の自主規制アプローチによっても、我が国では、「倒産は悪である」との価値観が企業社会を支配しており、プライバシー・マークを取得した事業者でさえも策定されたプライバシー・ポリシーの中に、自社が経営破綻した際の収集済個人データをどのように取扱うかに関する方針については、全く宣言されていないし、JIS Q 15001 の中にも経営破綻時の個人情報の取扱指針は示されていない。このように、企業の経営破綻時における個人情報保護政策は、米国と我が国では、大きな温度差がある。企業の倒産は、当該企業が保有していた資産が激しく変動し、個人情報が流出する危険性が非常に高い事象である。そのため、倒産の場面では、平常時よりも更に強くデータ主体たるユーザーのコントロールが及ぼされなければならない。にもかかわらず、我が国では、プライバシーポリシーの監視制度すら存在しないなど、その保護は考慮されていない。

４．従来型のプライバシー侵害救済手法の限界

4.1　不法行為構成による保護の限界

上述したように、現在、我が国で取られている個人情報保護政策は、公的部門・民間部門の双方において侵害発生に対する予防措置を重視している。しかし、現状では、判断能力の低い子供の個人データ保護策や事業者の経営破綻と言った、

[15] http://www.truste.org/about/about_mabs.html (2001.11.10 確認)
[16] S.420ES/ H.R.333EAS

データ主体のコントロールが及びにくいケースを想定した予防施策とはなっていない。また、いくら個人データの流出予防対策を強化しても、パーソナル・データがインターネット上に流出・漏洩してしまう危険性を完全に排除することはできない。

実際にパーソナル・データのインターネット上への流出・漏洩被害が起こった場合に喫緊の課題となるのが、発生した被害の救済と速やかな被害拡散の防止である。

不法行為法アプローチはプライバシー権の生成当初から、その救済手法のフレームワークとして発展し、現在も、プライバシー侵害の救済手法のメインフレームワークとして、所与のものとされている。しかし、情報ネットワーク社会の進展によって、今日では、不法行為アプローチのみによっているだけでは解決できない問題が発生しているのが現状である。不法行為構成によるプライバシー保護の限界点として、(1)要件面の限界、(2)手続・効果面での限界を概観する。

4.1.1 要件面での限界

プライバシー権を「私生活をみだりに公開されない法的保障ないし権利」とする伝統的プライバシー権概念によれば、プライバシー権侵害の態様として、第三者による「公開」行為が重要であるとされる。この「公開」の要件は、侵害者が得た情報の第三者への伝達という狭義の「公開」のみに限定せず、本人以外の者に知られることと解する見解や「公開」は「侵害」に置き換えた方がよいとする見解[松本95]等のように拡張され、現在は、保護される利益の性質と侵害態様・価値との関連の中で判断する[四宮83]とされており、第三者への公開は違法性を高める要素に過ぎない。

一方、近時のプライバシー権の有力な考え方である自己情報コントロール権概念によれば、個人情報の収集、管理、利用、開示・提供は本人の意思に基づくことが基本とされ、閲覧請求権、訂正・削除要求権、利用・伝播統制権が認められる。これによれば、公表行為がなくとも、本人の同意を経ずに情報を収集すること自体がプライバシー権侵害を構成するとされる[吉野99]。しかし、ここで「情報」と「コントロール」の意義、そして究極的には、保護法益の実体が何かという点が問題となる。自己情報コントロール権概念によれば、既存の人格権との区別（例えばプライバシー権侵害と名誉毀損との区別）も曖昧なものとなるとの危惧がある[阪本95]。そこで、個人情報の閲覧、訂正・抹消請求権をプライバシー権から外して、プライバシー権概念は、伝統的プライバシー権概念として明確化し[竹田98]、情報コントロール権概念の持つ積極的側面は、憲法13条を根拠とした別の抽象的権利として構成する見解もある[吉野99_2]。このようにプライバシー権の定義について、伝統的なプライバシー権説、情報プライバシー権説のどちらに立っても、基本的個人情報が伝統的概念によれば「私生活上の事実」に、情報プライバシー権説によれば「情報」に該当するのか、そしてプライバシー権の保護範囲に含まれるのかという困難な問題に直面することになる[吉野99_3]。

この点、全ての情報をプライバシー権の保護対象にすることも考えられるが、これには、保護対象を拡大すればするほど、人格権概念からの乖離が進み、その実体が不明確になるほか、不法行為の成立に必要な違法性の認定には、個人情報の有する価値自体を個別に評価することになるとの批判がある[吉野99_4]。また、氏名・電話番号・住所については、個人を識別する符丁であり、他者に了知されることによる不利益は考えられないとの理由で私生活上の事実に含めないのが一般的である。センシティブな個人データとそうでないデータとの分類を行う考え方も可能であるが、そもそもセンシティブかどうかを判定することは、個人のプライバシー意識の差異の問題も絡んで、困難である[松本95_2]。また、個人識別の符丁に過ぎないとされる基本的情報でも、情報統合により、センシティブな情報とマージされれば、深刻なプライバシー侵害を引き起こす場合もある。つまり、基本的個人情報であるというだけで一刀両断的に保護を否定することは妥当ではないし、逆に保護範囲を拡大すれば、その実体が不明確となってしまうという問題が生じる[吉野99_5]。不法行為の成立に際しては、権利侵害ではなく、加害行為における違法性の有無が問題となる点を考慮して、情報の定義自体ではなく、侵害された個人情報の価値と侵害行為の態様との相関関係でプライバシー侵害の有無を判断する、つまり①個人情報の価値

が低い場合は侵害態様の不法性が高い場合に、②侵害行為の不法性が低い場合に個人情報の価値が高ければ、それぞれプライバシー侵害を認めるべきだとする見解も存在する[吉野 99_6]。

プライバシー侵害被害者の具体的な救済方法としては、①インターネット上での個人データ収集の事前差止、②原状回復、③金銭賠償が考えられる。①の事前差止については、「石に泳ぐ魚」事件の最判平成 14. 9 .24 において、最高裁判例上、初めてプライバシーの語が盛り込まれ、プライバシー権を名誉権と同様の排他性を有する人格権として差止が認められた。しかし、権利侵害者とその侵害態様を明らかにしやすい従来型のプライバシー侵害とは異なり、インターネット上でのプライバシー侵害の場合、どの情報とどの情報が統合されて、プライバシー侵害を惹起するかは、予測困難であり、権利侵害の態様も不定で類型化が困難であり、その請求は困難である[藤波 99]。②の原状回復に関しては、一端、個人データが流出してしまうと、回収は不可能であり、結局、③の金銭賠償によるところとなる。しかし、インターネット上に流出した個人データによって、どのデータとどのデータが結合されて、どの程度の二次被害が発生しうるかという予測はこれもまた困難である。ISP（Internet Service Provider）の責任を追及するにしても、特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律３条においては、「特定電気通信による情報の流通により他人の権利が侵害されたときは、（中略）これによって生じた損害については、権利を侵害した情報の不特定の者に対する送信を防止することが技術的に可能な場合であって」、①ISPが当該特定電気通信による情報の流通によって他人の権利が侵害されていることを知っていた場合、②ISPが当該特定電気通信による情報の流通を知っていた場合で、当該特定電気通信による情報流通によって他人の権利が侵害されていることを知ることができたと認められる相当の理由がある場合以外は、免責される。情報統合のように合法的な手段で各データを統合し、プライバシー侵害が発生した場合、本法によれば、ISPの責任を問うことはできない。

このように、個人データのインターネット上への流出によるプライバシー侵害が発生した場合、不法行為構成による解決を目指そうとしても、どの範囲の情報までを保護対象になるかが問題となる他、①誰がどのレベルで責任を負うかについて、流出したパーソナル・データの現状を把握できない以上、具体的にどのような損害が発生する可能性があり、誰の行為によって損害が発生したのかを確定することが、困難である。②「宴のあと」事件判決で示された (1) 私生活性、(2) 秘匿性、(3) 非公知性の３要件を満たす必要があり、場合によって保護が否定される [吉野 99_7]。これらの立証には、多大な時間的・金銭的コストを要する。そのため、提訴者に立証責任を負担させている現在の不法行為構成の枠組では、速やかな被害拡散の防止と言う観点からのユーザー保護は実現困難である。上述したように、たとえ現行法で犯人を検挙しえたとしても、一旦流出した個人データの利用による個人の私的生活の平穏を阻害する行為を防止することは現行の枠組みでは、デジタルデータの即時性、ボーダレス性、加工可能性から見た場合困難である。

4.1.2 手続・効果面での限界

不法行為構成により、プライバシー侵害の救済を得ようとした場合、訴訟手続・執行手続を通じて、不法行為に基づく損害賠償請求債権を実現するというステップを踏まなければならない。しかし、ネットワーク上に流出した個人データによって引き起こされるプライバシー侵害とその救済を考える際には、以下の特徴を検討する必要がある。

① １件当たりの損害額が低額である。
② 救済に長い時間が必要である。
③ 損害の程度・原因・加害者の特定とこれらの因果関係を被害者自身が立証することが困難である[17]。
④ 審理段階で二次的プライバシー侵害が発生する危険性がある。

[17] 個人データとは異なるが、インターネット上での知的財産権保護もファイル交換ソフトウェアの普及により、個人データと同種の情報拡散による権利侵害問題を抱えている。[中山97]では知的財産権保護を不法行為構成のみによっていたのでは、差止が認められない点、及び損害額立証の面で困難が伴い、保護が不十分になってしまう点を指摘している。

以上の①～④のうち、①・②について見る。①については、まず、プライバシー侵害の救済手法の主流となっている不法行為構成による救済について、裁判所が認めた認定額の状況を見てみる。竹田によれば、プライバシー侵害を原因とする不法行為損害賠償請求訴訟事件のうち、私生活への侵入、他人に知られたくない私生活上の事実、情報の侵害の成立を認めた30件の事案を見てみると、請求額50～2000万円に対し、認容額は2（1.7%）～500万円（83%）の範囲で認容されている[竹田98_2]。請求額の83%が認容額とされた事案もあるが、全体的な傾向としては、73%にあたる22件が請求額の20%以下しか認容されていない。我が国では、交通事故の事案については、損害賠償の認容額が高額化している傾向はあるものの、人格権侵害に対する賠償額は依然として低額にとどまっている[竹田98_3]。この点、「北方ジャーナル事件」最高裁判決（最大判昭和61年6月11日民集40巻4号872頁）の大橋裁判官補足意見は、「わが国において名誉既存に対する損害賠償は、それが認容される場合においても、しばしば名目的な低額に失するとの非難を受けているのが実情と考えられるのであるが、これが、本来表現の自由の保障の範囲外とも言うべき言論の横行を許す結果となっている」としている。

また、財産的損害賠償についても、③の侵害と損害の相当因果関係の立証が困難である点が障壁となり、小額の弁護士費用[18]のみが認められている例が大半である[竹田98_4]。更にプライバシー侵害被害の救済を求めるために司法手続を利用する場合、裁判所に納付する訴訟手数料・被告に対する訴状送達費用の他、弁護士費用（着手金・成功報酬）[19]、敗訴時の訴訟費用等を要する[20][相川99]。つまり、経済的に恵まれた富裕層に属する人々は、優秀な弁護士に依頼して、自己の権利保護を達成することが期待できる余地もまだあるが、そうでない場合、侵害された権利の救済を求めることは、著しく困難である。

次に②に関しては、近時の司法改革の動きを受けて、訴訟の迅速な解決に向けて、裁判所の積極的な取り組みがなされている。最高裁判所が1999年12月8日の司法制度改革審議会における法曹三者への意見聴取の際に委員に提出した「21世紀の司法制度を考える－司法制度改革に関する裁判所の基本的な考え方－」によれば、1989年～1998年の10年間の民事通常訴訟事件の平均審理期間（第一審・人証調べを行った事件の地裁全国平均）は23.1ヶ月から20.8ヶ月へと短縮されている[21]。しかし、インターネットの持つ即時性に即して言えば、裁判所、及び関係者の努力により達成された20.8ヶ月の審理期間でさえも、オンライン・プライバシー侵害被害者の権利保護には十分でない[22]。

4.2 契約アプローチによる個人データの保護

4.2.1 契約アプローチの位置づけ

以上、見てきたように、我が国の個人情報保護政策には、被害の救済という意識が薄く、具体的な救済プログラムが存在しない。現在、我が国では、上述したようにプライバシー侵害の救済として不法行為法による解決アプローチが多く用いられている。しかし、不法行為アプローチには、個人情報がプライバシー権の保護対象になるか否かの点で要件上の限界が存在し、費用と時間がかか

---

[18] 最高一小判昭和44年2月27日民集23巻2号441頁では、「不法行為者の被害者が自己の権利擁護のため訴を提起することを余儀なくされ、訴訟追行を弁護士に委任した場合には、その弁護士費用は、事案の難易、請求額、認容された額、その他諸般の事情を斟酌して相当と認められた範囲内のものにかぎり、右不法行為と相当因果関係に立つ損害というべきである」と判示している。

[19] 弁護士費用は、勝訴の場合でも請求認容額の10-20%しか相手方から回収できないことが多く、このことが、訴訟手続の利用を敬遠させる一因となっているとして、[意見書]では、一定の要件の下に弁護士報酬の一部を訴訟に必要な費用と認めて敗訴者に負担させる制度の導入を提言している。

[20] この点については、前掲注31資料p.28においても低額化を行う必要性が示され、司法制度改革推進本部司法アクセス検討会において、2003年通常国会への法案提出を目指して検討が進められている。

[21] http://www.courts.go.jp/pre21/08.gif (2002.9.5確認)

[22] 民事手続上は、訴額30万円以下の事案については、簡易裁判所において、1回の期日で判決を得られる少額訴訟手続や仮処分手続も設けられているが、いずれもインターネットの即時性をカバーする形での被害の拡散防止と被害者の権利保護を十分に達成しうるとは言えない。

るばかりでなく、①賠償額も低額しか認容されない、②立証責任、時効面で柔軟性に欠ける等の難点がある。こうした不法行為アプローチの限界に対応するための第２のアプローチとして考えられるのが、契約関係に基づいた債務不履行責任を問う契約アプローチである。

民法学上、プライバシー保護における契約アプローチは「情報主体と情報提供者間において何らかの契約が存在する場合、（中略）情報提供者の同意の範囲を超えて、情報提供者が第三者に対して情報提供した場合は債務不履行責任を構成する」[吉野99_8]事と考えられている。ある契約が締結された場合、債務者は債権者に当該契約の目的とされた給付義務の他に信義則に基づく付随義務（又は独立した保護義務）を負う。契約アプローチは、この付随義務に着目し、契約の目的となった範囲外の第三者に情報主体に無断で情報提供がなされた場合、付随義務に反した債務不履行責任を問うとするものである[吉野99_9]。例えば、クレジット契約において、信用供与契約時に信用情報が登録される旨を目的、登録機関名、登録情報内容、及び当該情報を参照する可能性がある範囲を提示した上で契約締結がなされたにもかかわらず、登録機関の加盟外企業や信用管理外目的で第三者に当該情報を提供した場合等が契約アプローチで想定される代表例である[23]。本アプローチでは、データ主体による同意の有無の一点が要件となり、不法行為アプローチによる保護で必要となる(1)私生活性、(2)秘匿性、(3)非公知性の３要件は不要となる。また、データ主体の同意を要件とする契約アプローチでは、当事者間の合意内容や契約の性質によって、情報の第三者提供行為がプライバシー侵害とされるか否かが決まる。そのため、データ主体の多様化したプライバシー保護意識に柔軟に対応できるメリットも存在する[吉野99_10][吉野2000]。

4.2.2　米国における Contractual Approach の展開

米国では、ネットワーク上での消費者のプライバシー保護政策に、すでにこの契約アプローチ（Contractual Approach）が政策の基本的なフレームワークとして採用されている。例えば、商務省国家情報通信局（The National Telecommunications and Information Administration of the U.S. Department of Commerce）により、消費者が情報通信サービスを利用する過程、及び情報通信サービスの利用の結果発生した個人情報の収集、利用、及び流通に関して事業者と消費者間での契約が行われるようにするための契約モデルが策定されている。米国の Contractual Approach では、事業者がマーケットからの評価を重視することで、プライバシー侵害企業であるとのレッテルを貼られないために個人データ保護に十分注意を払い、消費者も個人データ保護に関心を有することを前提に個人データ保護を重要な契約事項と位置づけている[Shaffer 2000]。

米国のContractual Approachでは、「告知」と「公正さ」の２原則を重視している。「告知」の原則は以下の５項目に関する情報をユーザーに適切に与えることを要求する。

① 情報の使用目的
② 当該情報の秘匿性、一体性、質を維持するために講じられる手段
③ 当該情報を提供する、または提供しないことによってユーザーが受ける影響
④ 契約が守られなかった場合の救済のための権利

その上で、個人情報利用者は、その利用が公共の利益が切迫して要求する場合以外は、ユーザー個人が理解している情報の利用方法に反して、情報を利用してはならないとする「公正」原則を掲げている[平野98]。米国でネットワーク上での消費者のプライバシー保護政策として契約アプローチが重用されている背景としては、政府による保護規制よりも Contractual Approach による市場的決定に委ねた方が効果的であると考えられているためである。Contractual Modelの下では、消費者は、取引企業のプライバシーポリシーの動向を監視し、不服があれば、当該企業との取引関係からの脱退をちらつかせながら、当該企業のプライバシー政策動向に影響力を行使

[23] 東京地判昭和56.11. 9判タ467号124頁、大阪地判平成２．７.23判時1362号97頁

することが可能である[Shaffer2000_2]。Contractual Approachの実効性を高めるためには、消費者が率先して、プライバシー問題に関心を持ち、日々事業者のプライバシーポリシーの動向を見極め、登録された個人データが他の目的に利用された場合、登録情報の抹消を求めるオプトアウトを行うことが期待される。この点、FTCやThe National Consumers League等は、プライバシー問題に関する子供用の教育サイトをインターネット上で展開するなど積極的な消費者教育活動を展開している[24]。

しかし、Contractual Approachは、事業者と消費者間のプライバシー問題に関する認識に非対称性が存在するという課題を抱えている。事業者は、日々、大量の消費者の個人データを継続的に管理・利用することで、各消費者の全体像を把握している。その一方、消費者は、多くの事業者とad hocな取引を行うため、消費者が個人レベルで取引を行う全ての事業者のプライバシーポリシーの動向をつぶさに監視することは困難であり、消費者の注意はしばしば、行き届かなくなりがちである。また、個人レベルで各事業者のプライバシーポリシーを収集・分析するにはかなりのコストがかかる。そして、こうしたコストの総計はしばしば、消費者のプライバシーに関する利益の価値を上回ることになる。このため、富裕層・高学歴層の人間と貧困層や教育レベルが低い階層の人間とでは権利保護の程度に大きな差が生じることになる[Shaffer2000_3]。

この問題に対して、米国では、プライバシー擁護団体（Privacy Advocates）が消費者のサポート的役割を果たしている。上述の様に多くの消費者はad hocに事業者と取引を行うため、事業者のプライバシーポリシーの動向を継続的に監視することは困難である。しかし、Privacy Advocatesは、事業者のプライバシーポリシーの動向を長期にわたって、継続的に観察し、消費者にとって不利益な方向にプライバシーポリシーが変更された場合に不買運動、議会へのロビー活動、提訴等の手段を用いて、事業者のプライバシーポリシーの水準を維持あるいは向上させる役割を果たしている。EUデータ保護指令（1998年10月発効）では、EU加盟国にEU指令と同水準の個人データ保護水準を達成しない国々への個人データ移転、および共有を禁止している。米国政府は、EU指令の保護水準を満たしていなかったため、EUが一定の条件を満たしたと判断した場合にEU指令規定の保護水準を満たしていない国にも例外的に個人データの移転を認めるEU指令25条5項のセーフハーバー条項の適用を求めて、外交交渉を行い、2000年5月31日、合意に達している。この交渉に際して、米国のPrivacy Advocatesは、商務省により厳格な保護水準を策定するように働きかけた他、FTCや他の団体とも連携して、企業に自社が宣言したプライバシーポリシーを忠実に遵守するように圧力をかけるなど積極的な役割を果たしている。また、米国のPrivacy Advocatesは他国のプライバシー擁護団体とも積極的な連携を行うなど国際的な活動を行っている。例えば、アメリカで主導的な地位にあるプライバシー擁護団体であるThe Electronic Privacy Information Center（EPIC）は、イギリスに拠点をもつPrivacy Internationalと連携して、①更なるプライバシー保護の充実を議会に働きかけ、②商務省ガイドラインへのコメントの発表、③アメリカ企業の行動を追跡（以上、EPIC担当）、④アメリカに拠点を置く多国籍企業のデータ移転を監視（Privacy International担当）する等の活動を行い、EU指令の実行性を高める役割を果たしている[Shaffer2000_4]。

一方、Privacy Service Providerの果たす役割も大きい。Alan Westinによって設立されたプライバシーシンクタンクである“The Center for Social and Legal Research”は、“Privacy and American Business”プログラム[25]を展開し、企業に国内外のプライバシー保護法制の動向について、個別にアドバイスや、企業や事業者団体を対象としてプライバシー保護問題を扱うConferenceの定期的な開催、あるいは“Privacy and American Business”と題される雑誌を発行するなど積極的な活動を見せている。“The Electronic Frontier Foundation”[26]は、IT企業と共同でインターネットWebサイトのプライバシー保護を評価するTRUSTe[27]プログラムを立ち上げている。Alan

[24] http://www.ftc.gov/privacy/index.html (2002. 3 .15確認)
[25] http://www.pandab.org/
[26] http://www.eff.org/
[27] http://www.truste.org

Westin教授は、Better Business Bureau Online（BBB Online）に対して、シールプログラムに基づいたコンサルティング・サービスを提供している。

4.2.3 我が国における契約アプローチの限界

我が国においても企業のWebサイトにプライバシーポリシーが掲示されるようになる他、プライバシー・マーク制度も運用される等、契約アプローチ確立への動きが高まっている。しかし、我が国の企業が掲示するプライバシーポリシーでは、個人データを提供する、または提供しないことによってユーザーが受ける影響や事業者側で契約違反のデータ取扱がなされた場合のユーザーの救済について、どのような権利が保障されるのかという点についての具体的な明示が全くなされていない。

ソフトウェアのライセンス契約や保険契約等の例からもわかるように近年の消費者契約では各消費者の意向を尊重した個別的な内容の契約を結ぶことは少なく、通常は約款等による符号契約の形態が採られるのが通常である。事業者は、経営破綻時の収集済個人データの取扱方針や、契約違反がなされた場合の具体的な救済措置のような自己に都合の悪い事項については宣言をためらう傾向にある。そのため、プライバシー・ポリシーのみに依拠した事業者主導による契約アプローチでは、企業－消費者間に存在する交渉力格差は解消されず、①契約違反時に具体的な救済措置が明示されない、②情報プライバシー権を消費者に放棄させる、あるいは個人データを提供しなければ、インターネット上のサービスを利用できなくなる等のようにユーザー側に一方的に不利な符号契約をエンド・ユーザーが飲まざるを得なくなる。また、たとえユーザーがこうした符号契約を変更させようと事業者と交渉することを決意したとしても、当該交渉には、時間・弁護士費用等金銭面の「取引費用」が多額に発生する。そのため、当該交渉は、結局、資金力の面で余裕がある事業者側に有利である、あるいは同じユーザー間でも金銭的に裕福な富裕層に属するユーザーのプライバシー権は保護され、貧困層のそれは保護されないという不公平が生じる[平野 98_2]。

我が国では、ようやくプライバシー情報の漏洩に関する保険方式による保護方式のビジネスモデル化と評価機関の設置を検討する研究が始められたに過ぎず[辰巳 2001]、米国のようにPrivacy Service Providerによるコンサルティング・サービスは市場化されていない現状にある。また、プライバシー擁護団体も我が国では、組織化された存在とは言えない[橋本 2002_2]。

ある規範が規制として有効に機能するためには、規範を強制する側のコミュニティに規制される側のコストを負担する者が参加していることが必要である。しかし、現状では、自主規制を行う事業者側は収集済データの使用に際して生じる関連コストやリスクを負担していない。こうしたコストやリスクはデータ主体である消費者が負担しているのが現状である[Lessig99]。米国の様にプライバシー擁護団体が組織化されていない我が国では、プライバシーコストを負担する消費者の代弁者すら存在しない。そのような環境下で我が国の契約アプローチの実効性は、米国に比してより薄いものに終わってしまうことが懸念される。

5．財産権的アプローチによるインターネット上の個人データ保護

5.1 ネットワーク上の個人データ保護における財産権的アプローチの有用性

以上を総合的に検討して、インターネット上でのパーソナル・データ取引に対するユーザー保護政策において、従来型の政策アプローチでは、限界があることを筆者は指摘する。本問題解決のためには、ユーザーの個人データに財産権を認定し、個人データの利用に際して、当該データの所有者たる情報主体に対し、明確な対価や承認を得る手続を取ることで、その保護を図る財産権的アプローチを新たに導入することが必要である。

財産権的アプローチが従来の損害賠償方式と異なる点には以下の諸点がある。第１に財産権的アプローチでは、権利者にコントロール権が付与されることから、データの移転前に交渉プロセスと同意の取得を踏むことが必要とされる。従来の損害賠償アプローチでは、プライバシー

ポリシーが掲示されていても、データの取得に際して、改めての交渉プロセスは踏むことはなく、データの移転そのものは認められることになる。また、財産権的アプローチによる場合、データ主体は、提供しようとするデータ毎に、あるいは提供先毎に個別のコントロール権を有することになる。インターネット上での個人データ保護に財産権的アプローチを導入する第１の意義が、この自律性にある[Lessig99_2]。

第２は、財産権的アプローチによれば、各データの経済的価値をデータ主体が独自に定めることができる点である。従来の契約アプローチでは、ユーザーは例えば航空会社のマイレージプログラムのように事業者が設定した価値や条件に従って個人データを提供することになる[28]。中にはシュリンクラップ（クリックラップ）契約により、プライバシーポリシーに同意を取引の条件とするサイトも存在する[吉川2001]。こうしたサイトでは、シュリンクラップ契約がなされるため、収集される個人データの価値についての交渉はなく、同意するか否かの二項選択を消費者は強いられることになる。また、不法行為アプローチにより、プライバシー権侵害に対する法的救済を求める場合は、法文、あるいは裁判官により、個人データの経済的価値が算定されることになり、データ主体は、何ら自己のデータの経済的価値をコントロールすることができない。財産権的アプローチによれば、事前の交渉プロセスで提供の対象となる個人データの経済的価値を決定することになり、プライバシーを他者より重要視する人も軽視する人も、どちらに対してもその意向に配慮した、つまりプライバシー意識の個人のレベル差に応じた保護を行うことができる[Lessig99_3]。

このように個人に関する情報に財産権性を認める概念の一つにパブリシティ権（The Right of Publicity）が存在する。20世紀後半、映像メディアの発達やスポーツ、コンサートといったイベントが盛んになり、こうした大衆娯楽文化を担う芸能人やスポーツ選手等の著名人（以下、セレブリティという）が多数登場し、彼らの氏名や肖像等のアイデンティティが広告宣伝上、絶大な顧客吸引力を発揮する事が明らかとなり、セレブリティに無断でその氏名や肖像が営利目的で第三者に利用される事件が増大した。パブリシティ権は、こうしたセレブリティの広告宣伝に関する経済的価値を保護する財産権として、1953年、ヘーラン判決[29]において、米国第二巡回控訴裁判所のフランク判事によって提唱された[豊田 2000]。

我が国では、パブリシティ権は「獲得された社会的名声、評価、知名度等からその氏名・肖像が独立した経済的な利益ないし価値として把握することができる俳優歌手等の芸能人、演奏家、プロスポーツ選手等公衆の人気に支えられ、その存在が広く社会に知られることを望んでいる者」[竹田 98_5]にとって、「独立した財産的価値を有し、各種の情報伝達手段によって商品の宣伝広告等に利用される（中略）氏名、肖像の有する財産的価値を利用する権利」[竹田98_6]と解されている[30][竹田 98_7]。

パブリシティ権論では、セレブリティの氏名、肖像の公開に関して排他的特権を認め、①他人の氏名、肖像の営利目的での利用、②特定人の氏名、肖像そのものやこれらを改変・使用していると商品取引者や需要者に認識可能な場合にパブリシティ権侵害が発生すると解されている[竹田98_8]。パブリシティ権は財産権であり、パブリシティ権の侵害者に対する救済手法として、損害賠償額を氏名・肖像使用料の対価相当額とする判決[31]や、パブリシティ権侵害の対象となった氏名・肖像を利用した製品の製造・販売の差止めを認めた判例[32]が存在する。

パブリシティ権と本稿で検討する財産権的ア

---

[28] 航空会社のポイント（マイレージ）プログラムの場合、例えば、東京－大阪間の１フライトあたりの加算基本ポイント（マイル）数は国内主要３社（日本航空、全日本空輸、日本エアシステム）とも一律 278 と設定されている。このように寡占状態や独占状態が形成された市場では、消費者は、自己の個人データの価値評価を事業者選定の条件にしえなくなる傾向にある。また、経済学的見地からは、消費者情報を用いて、事業者が第一種価格差別化を行うことで消費者の交渉力が損なわれる危険性が指摘されている。この点に関しては例えば、[Whinston&Stahl&Choi2000]を参照

[29] Haelan Laboratories Inc. v. Topps Chewing Gum Inc.,202 F 2d 866(2nd Cir. 1953)

[30] 我が国でパブリシティ権を実質的に認めた最初の判決として、東京地判昭和 51．６.29 判時 817 号 23 頁（マーク・レスター事件判決）が知られている。

[31] 東京高判平成３．９．２判時 1400 号３頁（「おニャン子クラブ」事件判決）

[32] 上述のおニャン子クラブ事件判決の他、東京地判平成１．９.27 判時 1326 号 137 頁(「光 GENJI 等氏名肖像表示物品販売禁止」事件判決)、東京地判平成４．３.30 判時 1440 号 98 頁（「加勢大周」事件判決）等を参照

プローチとの関係については、パブリシティ権は、セレブリティの氏名や肖像等のアイデンティティが有する顧客誘引力に基づく経済的価値を保護するために提唱された概念である一方、インターネット上での個人データ保護における財産権的アプローチは、データ主体の情報プライバシー権と私的生活の平穏を保護するために従来の救済手法を補完する手法であり、両者は基本的には異なる概念である。そのため、パブリシティ権で認められている相続性が財産権的アプローチによる個人データ保護では認められない等、実際の権利保護の手法にも両者には差異がある[33]。よって、パブリシティ権の保護方式のフレームワークをそのままインターネット上の個人データ保護に適用することは適切ではない。しかし、パブリシティ権は、個人の氏名や肖像を財産権として保護することで個人に関する情報に関する権利保護のメニューに多様性を与えることが可能であることを示している。こうした財産権の特性は、本稿で検討している実際に流出した個人データによる二次的プライバシー侵害被害の発生防止と言う観点から見たインターネット上での個人データ保護に関して、有効であると考える。

5.2　ライセンス制導入の有用性

本稿では、財産権的アプローチに立ったインターネット上での個人データ保護政策の一提案として、インターネット上で交換された個人データの利用にライセンス制の導入を提案する。インターネット上で交換された個人データの利用にライセンス制を導入するメリットとしては、以下の諸点を挙げることができる。

① 当事者間の個別事情に応じた個人データの利用条件を事前・個別に定めることが可能
② 司法手続を経ずにライセンス違反にあたる形態の個人データ取扱に対する初動的権利保護措置をオンライン上で瞬時に講ずることが可能
③ ライセンス上の利用条件違反やライセンスを有しない者の個人データ取扱に高額の損害賠償を請求することが可能
④ ライセンス処理の自動化により、データ主体の経済状況に左右されずにプライバシー保護を図ることが可能

①については、従来のプライバシー侵害の民事法上のメインフレームワークである不法行為構成の場合、問題となる個人データの取扱が違法であるかどうかは裁判官が最終的に決定することになる。しかし、裁判官の判断は、一般人の感受性が基準とされる[34]から、必ずしも、個々人のプライバシー保護意識に応じた判断がなされるとは限らない。また、事業者側の個人データ管理体制も個々の企業によって千差万別であり、社会的コストを考えた場合、不法行為アプローチによる権威的決定がされるよりも、個々の事情に合わせた個人データの利用条件を事前に定める方が安価である。この点から、ライセンス制は、従来の不法行為構成よりも、柔軟性のある個人データ保護形態を模索することが可能である点において有利である。

②については、違法な個人データ取扱がなされた場合でも、従来の不法行為構成では、訴訟手続によって、不法行為に基づく損害賠償請求債権の存在確認・損害額の認容と執行手続を踏まなければ、データ主体の権利は保護されない。これは、不法行為法は、契約法とは異なり、事前に具体的な権利義務関係が設定されているわけではなく、被害者側が加害者側の注意義務の内容と注意義務違反の存在を立証しなければならないという要件上の問題から、司法手続による解決が必須とされるためである。しかし、ライセンス制の場合、事前のライセンス契約によって、個人データの利用条件が定められているため、ライセンス条件に反した個人データの取扱が存在した場合、ライセンス許諾者は権利保護に際して、ライセンス違反者の故意・過失を立証する必要がない。実際、ソフトウェア著作権の分野でよく知られた事例では、Microsoft 社の Office XP（2001 年）以降に発売されたアプリケーション、及び Windows XP（2001 年）にライセンス認証システムが搭載され、規定されたライセンス数以上のソフトウェアが実行された場合、当該ソフ

[33] もっとも、プライバシーの権利・氏名権・肖像権について、遺族固有の権利の範囲で保護し、遺族の死者に対する敬愛追慕の情に関する法的利益によって保護する見解も存在する[竹田 98_9]。
[34] 「『宴のあと』事件」判決（東京地判昭和 39. ９ .28　判時 385 号 12 頁）

トウェアが機能制限モードでしか利用できなくなるなど、各ソフトメーカーで対策が進んでいる[35]。

③については、**4.1.2**で検討したように従来、人格権侵害に基づく不法行為の救済は、非常に低額しか損害賠償が認められなかった。しかし、財産権を基礎とするライセンス制では、契約条項にライセンス違反の際に懲罰的損害賠償を請求する旨を定めることが可能であり、不法行為構成に比べて、事業者に対する抑止力を維持することが可能である。

④についても、**4.1.2**で検討したように不法行為構成によれば、権利保護の程度がデータ主体の経済状況に左右される問題点がある。しかし、ライセンス制を導入すれば、費用のかかる司法手続を経ずに権利保護を図ることが可能である。端的に言えば、コンピュータ上でライセンスの自動処理を行うことも可能である。ブロードバンド技術の発達により、定額・常時接続環境が整備されている今日では、経済状況が比較的苦しいものであっても安価にプライバシー侵害の予防・救済を図ることができ、実質上、プライバシーが保護される者の範囲が大幅に拡大されることが期待できる。

5.3 カプセル化技術を利用したライセンス方式による個人データ保護

これまでは、財産権的アプローチ、特にライセンス制の導入がオンライン上の個人データ保護に有効であることを検討した。以下では、ライセンス制の実現に参考となる技術のうち、例として、オブジェクト指向技術の一部であるカプセル化技術を紹介する。

今日、ソフトウェア業界では、プライバシー保護を重視した開発動向がある。Microsoft 社は2001年8月に自社ブラウザーソフトの最新版であるInternet Explorer6をリリースした。本ブラウザにはP3P規格に準拠した新たなCookie管理システムが搭載されている。新たなシステムでは、アクセスしているサーバー以外のサーバーから送り込まれるいわゆる“Third Party Cookie”の存在をCookieの受け入れ前にユーザーに警告し、ユーザーの希望するレベルでCookieの活動をコントロールできる機能を搭載し、Cookieの削除ツールも新たに搭載されている。2002年1月には同社の製品にセキュリティーホールが相次いで発見されたことを踏まえて、同社のBill Gates会長は“Trustworthy Computing”構想を打出し、自社製品の開発方針を従来の新機能拡張型からセキュリティー重視型への転換を社員に対して表明した[36]。一方、我が国では、財団法人インターネット協会が、P3P規格に準拠したプライバシー情報管理システムとWebサイトをP3P対応にするためのポリシー作成支援ツールを無料で提供している[37][38]。

今日、MPEGのような符号化技術や情報通信技術が進歩することにより高品質の静止画、音声、動画情報等をネットワーク上で流通させることができるようになった。これに伴い、デジタルデータの大量コピーによる著作権侵害が問題視され、以下の2つの流れで技術的対策が行われている。

第1の流れは、デジタルデータに著作者情報を書き込むことで不正利用がなされた場合の証拠保全を行う電子透かし技術に代表されるPassive Safetyアプローチである。第2の流れは、不正利用の発生自身を未然に予防するActive Safetyアプローチである。Active Safetyアプローチによる技術的対策の例が、交換されるデータをカプセルの中にパッキングし、ライセンス違反等、一定の条件が認められた場合に、カプセルに内蔵された爆弾を作動させることで、当該データを使用不能にするカプセル化技術である。

カプセル化は「ディジタルデータとその利用方法を一体として、それを情報のハンドリングの単位として扱う考え方」[櫻井2001]であり、オブジェクト指向技術の典型例である[39]。NTTのMatryoshkaと呼ばれる技術の場合、①コンテン

[35] 2002年9月リリースのWindows XP Service Pack 1にはライセンス違反が認められる製品を実行しているコンピュータのWindows Update機能を利用不可能にする機能が搭載されている。

[36] http://www.zdnet.co.jp/news/dj/020117/e_ms.html (2002. 2 .28確認)

[37] http://www.nmda.or.jp/enc/privacy/index.html (2002. 3 .15確認)

[38] この支援ツールでは、タグ画面の質問に答えることで、XMLベースのP3Pポリシーが自動的に出力される。サイト構築者は、出力されたポリシーをWebサイトに組込むことで構築しようとするサイトをP3P対応とすることが出来る。

[39] オブジェクト指向は実世界のオブジェクトになぞらえてソフトウェアのプログラムを構成する考え方である。オブジェクト指向

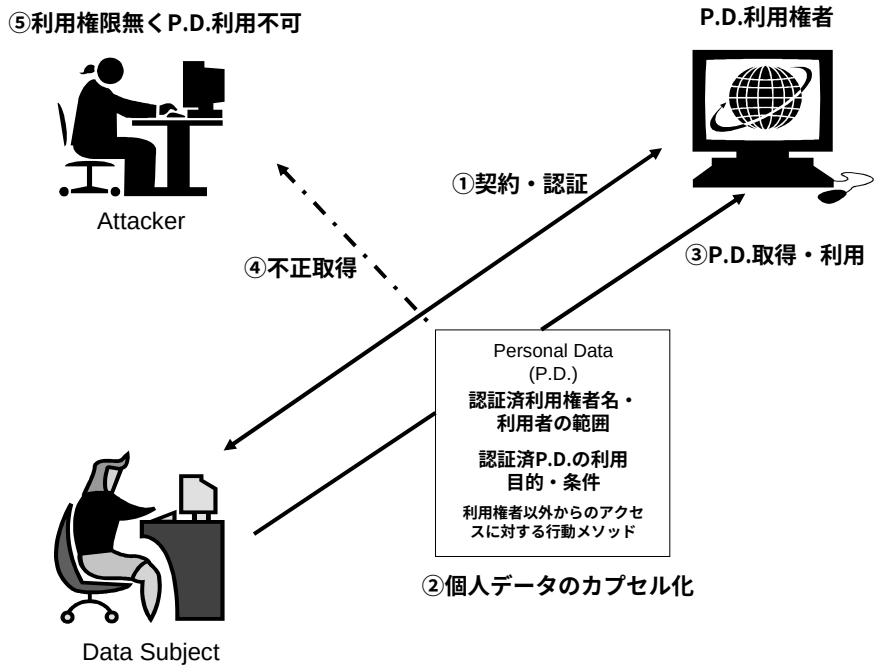

図２　カプセル化技術を用いた個人データ保護イメージ

ツ本体、②コンテンツ関連情報（利用制約条件・コンテンツの内容）、③カプセル全体の動作と利用制約条件に基づくコンテンツの表現機能が単一の格納単位（カプセル）に実行ファイル形式として内包される。ファイルを実行すると、カプセル内に実装されたコントロールが、カプセル内に内包されているコンテンツ関連情報を読み込み、実行環境を調査し、利用制約条件をチェックする。この利用制約条件には、端末限定がされている場合の利用者認証、使用時間、使用期限、使用回数を管理することが可能である。条件が適合する場合に実行されたコントロールは、履歴情報の更新処理後に制約条件に基づいてコンテンツを表示する。コンテンツ本体とその関連情報には、暗号化処理がなされており、カプセルに実装されるコントロールのみが、コンテンツの正常な表示を行えるようになっている[櫻井 2001_2]。

Matryoshka カプセルの場合は、自律性を重視した設計になっており、コンテンツ、コンテンツ実行アプリケーション（プレーヤー）、利用条件の監視システムがすべてカプセル内に内蔵されている。それ以外にもカプセル化技術には、利用者環境にすでにカプセル構造の認識、暗号化と復号が可能であるコンテンツ実行アプリケーションがインストールされ、カプセル自体には、利用制約条件とコンテンツ本体のみが実装されているタイプも存在する[40][櫻井 2001_3]。

カプセル化技術は、主にデジタルコンテンツにおける著作権保護を目的とした技術であるが、それ以外にインターネット上で交換される個人データの保護にも有用性を持っている。インターネット上では、流出したデータが転々流通することで、深刻なプライバシー侵害を惹起することになる。そこで、インターネット上に個人データが流出しても、アクセス権を有さない者が当該データにアクセス（閲覧・加工）できないようにすることで、プライバシー侵害へと発展しない手法が検討に値する。**（図２）**にカプセル化技術による個人データ保護のイメージを示し

におけるオブジェクトは、自身の状態に関する情報を保持し、与えられた刺激に従って、自身を操作するプログラムを有するものを指す。

[40] Windows Media Rights Manager(Microsoft)、MetaTrust Utility(InterTrust)、RightsEdge(ContentGuard)、RightsShell(NEC)、Cryptlope/EMMS(IBM)などが、実行アプリケーションとコンテンツが分離されているカプセル化技術の例である。

た。インターネット上でデータを取得・利用する者（例として事業者等）のプライバシーポリシーを評価し、ライセンス契約により、正当な利用目的を有するデータ取得・利用者のアクセス権を認証し、認証を受けた者のみに当該データ利用者のプライバシーポリシーを評価可能なメソッドでバインドしたカプセルの中に個人データをパッキングすることで、個人データへのアクセスを許可する開示制御を行う。この場合、正当な目的と評価・認証されない処理系や認証権限を持たないシステムから個人データへのアクセスがあれば、不正アクセスとして、正当なアクセス権を取得するまで、個人データへのアクセスを禁止したり、個人データそのものを消去し、データ主体から正当なアクセス権を取得ように要求することも可能である。個人データにアクセスする者の履歴を取得することも可能である [櫻井 2001_4]。

このようにカプセル化技術によれば、プライバシー保護政策のジレンマとして指摘されてきた個人データの不正流出によるプライバシー侵害からのデータ主体の保護とネットワーク社会における社会サービスの円滑な提供と企業の業務効率化という、相反する要請を満たすことが可能となる。こうしたプライバシー保護技術の開発と普及が進めば、これまで、事業者の意のままに個人情報を提供せざるを得なかったデータ主体が自分の意思で自己の個人情報の価値を設定できるようになると言う効果をもたらす。同時にデータ主体側がインターネット上で交換される個人データをコンピュータ・ソフトウェアと同視して、その使用条件を自由に設定できるようになる。

5.4 小括

上に述べたトレンドに鑑み、本研究では、インターネット上で交換される個人データ保護政策の具体的提案としてUniform Computer Information Transaction Act（UCITA・米国電子情報取引法）に規定されている電子的自力救済に類似した制度の導入により個人データを不適切な方法で取扱った事業者による当該個人データへの再アクセス（利用）をライセンス違反として排除する「オンライン・個人データ取引法制度」アプローチを提案する。電子的自力救済（Electronic-Selfhelp）とは、ユーザーによるライセンスの対象情報の利用を自動的に停止させる仕組みのことである（UCITA § 816）。既にUCITA § 102(a)(38)では、パブリシティ権を含む「排他的権利を与えるすべての法律の下で生じる情報についての一切の権利」を情報的権利として、その規律範囲に含めており、インターネット上での個人データ保護に対する適用可能性に配慮している。

今後の検討課題としては、ライセンス内容の条件をどう定めるのか、つまり、事業者により策定されるPrivacy Statementは、主観的な基準であり、破産した場合のデータの扱い方針など、都合の悪い事は、基本的に宣言しないため、客観性を担保する基準（実施体制に関する客観データ等）を別に考慮する必要があるのではないか。また、Privacy Statementを掲出しない事業者への対応に関して、このような事業者へのデータ移転をライセンス不存在として、排除することが適当なのかという点等に関して今後、検討の必要がある。

現在の我が国の知的財産法制上では、こうした電子的自力救済による権利者保護は認められていない。しかし、インターネット上での個人データ保護は、今日のネットワーク社会における我々の私的生活の平穏を保障するという観点からも必要不可欠なものである。即時性・ボーダレス性・複製の容易さという特徴を持った膨大な量のデジタルデータが流通するネットワーク社会における個人データ保護手法として、本稿で提案する電子的自力救済制度の導入は、コストパフォーマンス面で限界がある従来型の損害賠償アプローチに比して、より機動的で柔軟な保護を図ることが可能であるだけでなく、インターネット上でのプライバシー侵害の二次被害の拡大防止と言う観点からも必要である。

6．おわりに

本稿では、ブロードバンドサービスの普及による本格的なインターネットへの常時接続時代の到来により、消費者がこれまで以上のプライバシー侵害のリスクに晒される危険があることを指摘し、現在の我が国における個人情報保護政策の問題点として、①インターネットの持つ

即時性とグローバル性に対応しえるものではないこと、②事業者 - エンド・ユーザー間の交渉力格差の解消、及びエンド・ユーザー相互間での経済力格差を考慮した政策が不十分であること、③経営破綻企業の保有していた個人データに関するエンド・ユーザーの自己情報コントロール権の保護対策が不十分であること、④法人のプライバシー情報保護対策が不十分であり、結果として消費者のデータ保護が徹底されないこと、⑤子どものプライバシー保護対策が不十分である点を指摘した。

次にインターネット上での個人データ保護について、①従来の不法行為アプローチ、②契約アプローチについて、その概要を検討し、米国での取組みを検討した上で、プライバシー擁護団体や Privacy Service Provider が組織化されず、機能していない我が国での契約アプローチの実効性に疑問を呈した。その上で、第３のアプローチである財産権的アプローチの立場から個人データの利用にライセンス制の導入を提案した。個人データ保護手法としてライセンス制を導入する意義について、①不適切な個人データの取扱がなされた事業者に対して、その管理下にある個人データをライセンス違反として、一時的に制限することで、インターネット上での個人データ流出によるプライバシー侵害の被害拡散を一定限度で防止できる。②ライセンス違反の個人データ取扱を行った事業者に対して、懲罰的賠償による多額の損害賠償の可能性を示唆し、個人データの不適切な取扱によるプライバシー侵害への抑止力とすることができる。③ライセンス処理が自動化されることで、データ主体の経済状況に左右されることなく、オンライン・プライバシーを一定限度で保護することができる。④法人のプライバシー的情報の保護にも応用が可能である点を指摘した。

現在の複雑化した高度情報化社会の中で、個人は他者とどう向き合っていけばよいのか、その答えを我々一人一人が自問自答する素材のひとかけらに本稿が僅かでも寄与すれば、幸いである。

参考文献

[白書] 総務省編『情報通信白書　平成 14 年版』ぎょうせい , 2002, p.4

[前川 2001] 前川　徹「Web Bug とプライバシー問題」『情報処理』Vol.42, No.10, 情報処理学会 , 2001.pp.1014-1015

[橋本・本村・井上2000] 橋本誠志,本村憲史, 井上　明「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」『テレコム社会科学学生賞入賞論文集』No.9, 財団法人電気通信普及財団 , 2000.4, pp.1-36

[本村・橋本・井上・金田 2000] 本村憲史 , 橋本誠志 , 井上　明 , 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」『情報処理学会論文誌』Vol.41, No.11(2000)pp.2985-3000

[橋本 2002] 橋本誠志「ネットワーク社会における消費者保護の制度的枠組み―オンライン・プライバシー保護を中心に―」『同志社政策科学研究』（同志社大学）Vol.3, No.1, 2002, pp.73-94

[芦部 99] 芦部信喜『憲法　新版』岩波書店 , 1999, pp.87-88

[佐藤幸 95] 佐藤幸治『憲法　第三版』青林書院 , 1995, pp.424-427

[小野 94] 小野昌延『不正競争防止法概説』有斐閣 , 1994, p.201

[丸橋 2000] 丸橋　透「インターネットと子どもの保護」『法とコンピュータ』No.18, 法とコンピュータ学会 , 2000, pp.64-65

[増田・舟井・アイファート＆ミッチェル法律事務所 2002] 増田・舟井・アイファート＆ミッチェル法律事務所『米国インターネット法 - 最新の判例と法律にみる論点』ジェトロ、2002, pp.216-217

[増田・舟井・アイファート＆ミッチェル法律事務所 2002_2] 前掲著 , p.219

[松本 95] 松本恒雄「ダイレクト・マーケティングにおける顧客対象者リストの私法上の問題」神山・堀部・阪本・松本編『顧客リスト取引をめぐる法的諸問題』成文堂 , 1995, p.119

[四宮 83] 四宮和夫『不法行為（事務管理・不当利得・不法行為　中巻・下巻)』青林書院 , 1983(中巻), p.326

[吉野99] 吉野夏巳「民間における基本的個人情報の保護」『クレジット研究』No.22, 社団法人日本クレジット産業協会クレジット研究所 , 1999, p.139

[阪本 95] 阪本昌成「メイリング・リストの作成・販売およびダイレクト・メイルの法的規制」神山・堀部・阪本・松本編『顧客リスト取引をめぐる法的諸問題』成文堂 , 1995, p.9

[竹田 98] 竹田　稔『 [増補改定版] プライバシー侵害と民事責任』判例時報社 , 1998, p.166

[吉野 99_2] 吉野 , 前掲論文 , p.140

[吉野 99_3] 吉野 , 前掲論文 , p.140

[吉野 99_4] 吉野 , 前掲論文 , p.140

[松本 95_2] 松本 , 前掲論文 , p.123

[吉野 99_5] 吉野 , 前掲論文 , p.141

[吉野 99_6] 吉野 , 前掲論文 , p.141

[藤波99] 藤波 進「Cookies―その特質とプライバシー保護―」多賀谷一照・松本恒雄編集
代表『情報ネットワークの法律実務』第一法規 p.4356
[吉野99_7] 吉野, 前掲論文, pp.139-143
[竹田98_2] 竹田, 前掲著, pp.215-218
[竹田98_3] 竹田, 前掲著, p.218
[中山97] 中山信弘「財産的情報における保護制度の現状と将来」『岩波講座 現代の法10』岩波書店, 1997, p.275
[竹田98_4] 竹田, 前掲著, pp.219-220
[相川99] 相川忠夫「消費者信用取引に伴う情報流通」『クレジット研究』No.22, 社団法人日本クレジット産業協会クレジット研究所, 1999, p.109
[意見書] 司法制度改革審議会『司法制度改革審議会意見書―21世紀の日本を支える司法制度―』2001, p.28
[吉野99_8] 吉野, 前掲論文, pp.144
[吉野99_9] 吉野, 前掲論文, pp.144
[吉野99_10] 吉野, 前掲論文, pp.144-146
[吉野2000] 吉野夏巳「基本的個人情報の公開とプライバシー権」『クレジット研究』No.24, 社団法人日本クレジット産業協会クレジット研究所, 2000, pp.148-150
[Shaffer2000] Gregory Shaffer, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, The Yale Journal of international Law Vol.25, No.1, 2000 p.31
[平野98] 平野 晋, 牧野和夫『[判例] 国際インターネット法』プロスパー企画, 1998, p.134
[Shaffer2000_2] Shaffer, op.cit., pp.32-33
[Shaffer2000_3] Shaffer, Ibid., p.33
[Shaffer2000_4] Shaffer, Ibid., p.64-65
[平野98_2] 平野、前掲著, p.135
[辰巳2001] 辰巳丈夫、山根信二、白田秀彰「ネットビジネス業者の「プライバシー保護対策」評価の提案」『情報処理学会第62回全国大会』8F-4, 2001, pp.111-116
[橋本2002_2] 橋本, 前掲論文, pp.81-86
[Lessig99] Lawrence Lessig, CODE and other Laws of Cyberspace, Basic Books,1999（山形浩生、柏木亮二訳『インターネットの合法・違法・プライバシー』翔泳社, 2001）p.288
[Lessig99_2] Lessig, Ibid., p.290
[吉川2001] 吉川達夫「米国e-コマースにおける個人情報保護の動向」『国際商事法務』Vol.29, No.12, 2001, p.1439
[Whinston&Stahl&Choi2000] Andrew B. Whinston, Dale O. Stahl, and Soon-Yong Choi, The Economics of Electronic Commerce-The Essential Economics of Doing Businesses in the Electronic Marketplace, MACMILLAN TECHNICAL PRESS, 1997 (香内 力訳『電子商取引の経済学』ピアソン・エデュケーション, 2000), pp.328-345
[Lessig99_3] Lessig, op.cit., p.291
[豊田2000] 豊田 彰『パブリシティの権利』日本評論社, 2000, pp.2-8
[竹田98_5] 竹田, 前掲著, p.287
[竹田98_6] 竹田, 前掲著, pp.284-285
[竹田98_7] 竹田, 前掲著, p.288
[竹田98_8] 竹田, 前掲著, p.289
[竹田98_9] 竹田, 前掲著, p.288
[相川99_2] 相川, 前掲論文, pp.111-112
[櫻井2001] 櫻井紀彦「カプセル化コンテンツの動向と展望」『情報処理学会電子化知的財産社会基盤研究会』2001-EIP-12, 2001, pp.2
[櫻井2001_2] 櫻井, 前掲論文, p.4
[櫻井2001_3] 櫻井, 前掲論文, pp.3-4
[櫻井2001_4] 櫻井, 前掲論文, p.2
[佐藤英98] 佐藤英人『オブジェクト指向がわかる本』オーム社, 1998

【付録】Web bugの例

Web bugは、HTMLメールやWeb画像等、インターネットを介してユーザーの情報を取得する特殊なHTMLコーディングのことであり、以下のようなHTML-IMGタグとして表される。以下のWeb bugの例では、Quicken's社のHP(http://www.quicken.com)から、DoubleClick社とMatchLogic社(preferences.com)という2社のインターネット広告企業にQuicken's社のHPへアクセスしたユーザーのヒット情報を送信するように設定されている。ドキュメントを開くたびにWebへのアクセスが発生するため、ユーザーのドキュメント閲覧状況などがわかる。

基本的にはHTMLコーディングの創造的な応用であり，もともとはWebマスターが，自分のページ上にあるコンポーネントを別々の場所に置いておくために開発されたものであった。

```
<img src="http://ad.doubleclick.
net/ad/pixel.quicken/NEW"
width=1 height=1 border=0><IMG WIDTH=1
HEIGHT=1border=0SRC=
"http://media.preferences.com/ping?
ML_SD=IntuitTE_Intuit_1x1_RunOfSite_A
ny&db_afcr=4B31-C2FB-10E2C&event=
reghome&group=register&time=
1999.10.27.20.5 6.37">
```

(出所：Privacy FoundationHP (http://www.privacyfoundation.org/resources/webbug.asp)