H12-消費者 WG 個人情報保護 SWG

ＥＣで取り扱われる個人情報に関する調査報告書（ver.3.0）

平成 13 年 3 月

電子商取引推進協議会

消費者WG個人情報保護ＳＷＧ

目次

1　電子商取引（ＥＣ）の可能性と個人情報保護から見た課題

1.1　はじめに（EC ビジネスの現状と展望）

わが国のインターネット利用者数は、2000 年 11 末時点で 3,900 万人。人口普及率 30.5%に達しており、携帯電話など非 PC 端末の普及で、日本における一般消費者へのインターネットの普及、さらには電子商取引（BtoC・EC）の可能性は急速に広がっている。

EC 先進国である米国でもオンラインショッピングの急速な普及が見られたのは 1998 年のことである。一方、日本でも 1999 年後半に入り、米国を中心とした先進ビジネスモデル事業者の参入、大企業の EC への再参入、携帯電話等の非 PC インターネット端末の登場、等により、BtoC・EC の急速な実ビジネス化がみられる。日本でも、1999 年後半に「EC 元年」への助走期を迎え、翌 2000 年には、いよいよ本格的な普及期に突入したと言えよう。

同時に、ｅマーケットプレイスに代表されるオープンな企業間（BtoB）EC の展開も、2000 年度に入り、にわかに注目されている。現在、その多くが初期段階であり、ビジネスとしての定着や規模については今後の展開を見る必要があろう。しかし、今後インターネットを通じて、相対的に不特定多数に対してよりオープンな企業向け電子商取引（「オープン BtoB・EC」）は着実に拡大する傾向にあると考えられる。

1.2　電子商取引(B to C EC)のチャンネル拡大と市場規模

従来のパソコンを使ったオンラインショッピングから、最近ではそれ以外の端末機器を利用した電子商取引が新しいチャンネルとして登場している。その代表がｉモードに代表されるモバイルＥＣである。この携帯電話という、いつでも、どこでも、自分の好きな時にインターネットにアクセスできる機器をベースにした新チャンネルはその加入者数の増加（2000 年 12 月末で 6,300 万人突破）に伴い国民の二人のうち、一人がこれを利用する時代に突入すると共にＥＣ人口の拡大と参入年齢の低下という大きな変化をＥＣにもたらした。

これからは、モバイルバンキングの進展やショッピング決済インフラの充実それにセキュリティ面の対策等の条件が揃えば、将来の BtoC・EC はこのモバイルをキーワードに発展すると言っても過言ではないであろう。

次に端末機器の普及台数と言う点で、ＥＣの新チャンネルとして期待されるのが、家庭用ゲーム機器である。現時点ではこれを使用しての一般的な電子商取引推進には制約条件

も多いが、少なくともゲームコンテンツのダウンロード（コンテンツ取引）には大いに活用されるであろう。すなわち現行のメディア（ＣＤ／ＤＶＤ）を経由したゲームソフト購入からインターネットからゲーム機への最新バージョンのダイレクトダウンロードに移行していく方向である。

それから今後、さらなるＥＣ発展の為の大きなプラットフォームの一つとして期待されているのが「ＴＶコマース」である。特に 2000 年の年末から本格化したＢＳデジタル放送を追い風に、デジタルＴＶがＥＣの主役になる日が近いとの見方がある。

特徴としては、大画面・精細画像を活かした、まるで実物を見るかのような製品情報や家庭電化製品の一つとして馴染み深いＴＶを使用するために、パソコン操作が苦手なお年寄りから子供にまでにも電子商取引の参加ユーザー層が拡大する事が挙げられる。

実際に、電子商取引(ＥＣ)の取扱い高はここ数年、前述の携帯端末の普及や情報通信技術の発展等により、目覚ましい勢いで延びてきている。

とくに国内の事業者―消費者間（Ｂ to Ｃ ）ＥＣの市場規模推移（2001 年１月ＥＣＯＭ調査）をみると、2000 年に 8,240 億円と推計されたものが、2005 年には 13.3 兆円になると予測されている。

しかし、こうしたＥＣの発展に伴ない、消費者と事業者間のトラブルも増加してきており、全国の消費生活センターなどへ寄せられたＥＣ関連の苦情・相談件数は徐々に増える傾向にある。

こうした中で、消費者はＥＣに利便性を感じながらも潜在的な不安を抱いている為に、積極的な利用を躊躇している様子が、ＥＣＯＭの行なった「ＥＣに関する意識調査」でも明らかになっている。その主なものとしては、

① 自己データが漏洩するのではないか
② 代金を誤請求されるのではないか
③ 商品確認がよくできない

といった事項で、どれもＥＣが隔地間取引で、相手が見えない為の不安であることがわかる。

1.3 電子商取引上の情報の特徴

つづいて電子商取引上の取扱い情報･データの特徴、そしてそれがもたらすメリット・デメリットについて見てみる。

1.3.1　デジタルデータの特性から来る加工・データベース化の容易さ

オンラインデータでは再インプットの必要無しで、データベース化ソフトを使ってそのままの加工や大容量データベース化が可能である。つまりハードコピー上のデータと違い、デジタルデータの特性を活かして、今日既に流通しているデータ･マイニングやデータウェアハウスという各種プログラムソフト･手法を用いて、生データから目的別のデータ集計・加工やデータベース化が瞬時の内に、本当に容易にできると言う事である。このことは、後から出てくる消費者個人情報の統合データベース化である「コンシューマープロファイアリング」を可能にした大きな要素の一つでもある。

1.3.2　ダイレクトで継続的な顧客接点と情報獲得の容易さ

顧客のアフターフォローや利用アンケート集計等が簡単にできて、国や地域のエリア制限無しで広範囲・確実な見込み客情報の蓄積が出来る。これはオンラインデータの特性としてダイレクトに顧客のパソコンと企業側サーバーが連結されており、それこそ継続的な顧客接点の確保とそれに伴う最新情報の入手がアクセスログも含めてきわめて簡単である点からくるメリットである。

このことはまた、メール･アドレスその他の個人特定情報を元に、いろいろな形でのマーケティングが低コストで大ボリュームにしかも地理的にはグローバルな範囲で可能になるということであり、その付加価値たるやマーケティングの担当者からすると従来の非効率的なダイレクトメール手法に比べれば各段の違いがあると言っても過言ではないであろう。

1.3.3　購入前に無意識に提供・収集されている情報

購入意志決定に至るまでのプロセス情報であるアクセスログやブラウザ情報をサーバー側に自動送信する cookie と呼ばれるプログラムがある。

これらは一般に無意識提供情報と呼ばれ、まずアクセスログについては消費者が通常、インターネット･サービス･プロバイダー等を経由して各企業サイトのサーバーに接続されることから、その接続履歴がプロバイダー企業のサーバーには蓄積されていく。

つまりあるＵＲＬから次のＵＲＬへとネットサーフィンするたびに、克明にその経過・到着・離脱及び滞在時間等が記録されていることに殆どの消費者は気付いていない。

これ以外に消費者のパソコンハードディスクに蓄積された訪問ウェブサイトでのブラウザ

情報を企業サイトのサーバーに送り返すプログラムである cookie の存在についても、その実態やメリット･デメリットについても、同様に名前程度しか聞いた事がないといったケースが比較的に多いのが実態であり、企業側の意図が優先され、消費者保護の立場からすると、課題が多い。

1.3.4　ＥＣデータの特徴まとめ

1.3.4.1　メリット：「One to One Marketing」(欲しい人に、欲しいその物を)

つまりインターネットマーケティングは企業側にとって前述の様に、それまでの旧来手法をコスト面･ボリューム面・対象地域エリア等に関して、革新的に凌駕するリサーチ手法であるし、消費者にとってもその特定個人情報の使われ方が全く気にならないタイプの人間にとっては欲しい時に、欲しいものが、欲しい人に届けられるという究極の便利ツールであろう。

1.3.4.2　デメリット：「ＥＣ上の情報流出・漏洩（容易に・大量に・一瞬に・知らぬ間に）」

ただ恐ろしいのは、その裏返しとして、それだけ加工･データベース化が容易なところからくるデジタルデータの特性として、その情報流出･漏洩が容易にしかも大量に、そして情報主体の知らぬ間に一瞬にしして起こり得る事である。そしてこの大量･瞬時の漏洩がオンライン上の個人情報保護にとっては一番の脅威である。

1.4　電子商取引における個人情報保護について

次にそういった電子商取引上の取扱情報の中でも、昨今新聞・マスコミ等でも話題となった個人情報保護に関する基本法に関連してこういった法規制の背景となっているＥＣ上の個人情報保護の現状について述べてみる。

1.4.1　個人情報保護についての現状

ＥＣにおける個人情報保護についての現状として、よくある事例では、個人情報の流出が挙げられる。これには、「なりすまし」・「盗用」と「情報漏洩」・「誹謗中傷」といったパターンがある。それぞれの対策としては、まず「なりすまし」・「盗用」に対しては、やはり個人管理の徹底がポイントで、パスワード・カード番号の取扱い、接続時間等利用状況のチェック、オートログインの回避など消費者自身の自己管理のレベルアップが

必要である。

そして「情報漏洩」・「誹謗中傷」のケースについても、ここにきて相次いで企業･業者の内部からの個人情報の意図的漏洩が起こっているのが現状である。これについては、個人としての対策としては、なかなか有効な事前防止は困難であるため、通信履歴の保存、接続業者・公的機関への相談、警察への被害届などで対応せざるを得ない状況である。ただ企業側としては、こういった状況を深刻に受けとめて、社内の情報保護管理体制の強化や委託契約内容に保護内容を明記する等による漏洩防止のための具体策を講じるべきであろう。

また一般に、この個人情報に関するプライバシーの権利は「情報の主体が自己に関する情報をコントロールする権利である（自己情報コントロール権）」と解釈される。

つまり、現代のような以前までは考えられないようなレベルのオープンネットワーク社会においては、膨大な情報を入手できるというメリットを享受できる裏返しとして、個人情報の自己管理の重要性についての充分な理解と認識を、我々ネットワーク社会に生きる市民“ネチズン”は持たねばならない。

1.5　海外におけるオンライン個人情報保護の新段階での現状と課題

一方、国内だけでなく海外においてもオンライン上の個人情報保護の課題については、従来から様々な形で、問題提起され議論の的となっている。そして近年、海外とくに米国で顕著な傾向として出ているものに、個人情報の単純な漏洩の問題だけでなく、いわゆる「コンシューマー（ユーザー）プロファイリング」のついての課題認識がまずある。

また、もう一つの課題としてはその「コンシューマープロファイリング」の技術的な裏付けとなっている cookie をはじめとしたユーザー追跡プログラムの存在である。実際にプロファイリングに利用されているかどうかは別としても、それが可能となるテクニカルなアプローチにはプライバシー保護団体はじめ多くの見識あるユーザーは危惧の念を抱いているのが実情である。

その面で米国ではネット上の個人情報保護については、ある意味でネットマーケティングの新局面として、また漏洩事件の性格からしても第二段階に突入しているといっても過言ではないであろう。以下その事例を見ていくものとする。

1.6　海外における最近のオンライン個人情報保護漏洩事件（代表事例・抜粋編）

前述のように明らかに新しいフェーズに突入したと思われるネット上の個人情報取扱い・プライバシー保護の実態について、最新（2000 年度以降に発生）のニュース・事件の代表事例・抜粋編を以下に見ていくものとする。

1.6.1　プライバシー侵害で集団訴訟　米トイザラスが相手

玩具販売大手の米トイザラスを相手取り、同社サイトの利用者が 11 件の集団訴訟を起こしていたことが、同社が米証券取引委員会（SEC）に 11 日（米国時間）に提出した書類で明らかとなった。同日付けのロイター通信が伝えた。訴えによると、トイザラスがオンライン利用者の行動を追跡して、第三者と個人データを共有していたという。

原告側は、これらの訴訟はトイザラスのウェブサイトを訪れ、オンラインで商品購入したか、既に個人データを不正に「傍受」「監視」「転送」または「利用」された全利用者を代表した訴訟だと主張している。

11 件のうち 6 件の訴訟はニュージャージー州で起こされたもの。これらのうち多くの訴訟では、被告としてトイザラスと関連のトイザラス・コム Inc、トイザラス・コム LLC に加え、インターネット・マーケッティング企業のコアメトリクスが名を連ねている。この他、テキサス州やカリフォルニア州において集団訴訟が起こされている。

【米国記事】2000 年 9 月 13 日（Mainichi Daily Mail Internet）

1.6.2　シアトルの大学病院にハッカー、医療記録を盗む？

セキュリティ関連のニュースを配信する Web サイト SecurityFocus.com は 6 日、シアトルにある病院のコンピュータが今夏、ハッカーの侵入を受け患者の記録が盗まれたと報じた。侵入されたのはワシントン大学医療センターで、心臓病患者 4000 人以上の名前、住所、社会保障番号を含む記録、リハビリ中の患者の記録、同病院における 5 カ月間の入退院記録がダウンロードされたという。これを報じた同サイトの編集責任者 Kevin Poulsen 氏によると、同病院に侵入したハッカー「Kane」は今年夏、いくつかの病院のコンピュータに侵入を試み、ワシントン大学医療センター以外にニューヨークとオランダの病院に侵入したという。だが記録を持ち出せたのはワシントン大学医療センターのみとのことだ。Poulsen 氏は Kane が持ち出したという記録も見ているという。一方、ワシントン大学医療センター側は、侵入を受けたことは認めながらも、病院の記録が盗まれた事実はないとしている。

【米国記事】2000.12.8（MSNBC　December 7, 2000）NEXT NEWS

1.6.3　AOL の IM サービスで「アカウント漏洩」の指摘

America Online（AOL）のインスタントメッセージサービス AOL Instant Messenger（AIM）にサインアップするのために使われるサーバをめぐってセキュリティホールが指摘されている。nside-AOL.com と AOL-Files.com という、AOL ユーザーが作っている 2 つのサイトは 29 日、「AIM ユーザーのアカウントがハッカーによって盗まれている」と報告した。これらサイトが共同で掲載した文書には「われわれがこの情報を公開するずっと前から AOL は問題の存在を知っている」とも記されており、セキュリティホールを即座に埋めようとしない AOL の態度を批判している。このセキュリティホールは 1 カ月以上前から、AIM のアカウントを乗っ取るハッカーによって使われているが、特に頻繁に「ハイジャック」が行われるようになったのはここ数週間のことだという。AOL からのコメントは得られていない。（その後修復にかかっている事がを明らかにした。）

【米国記事】2000.12.1（ZDNN/USA　November 30, 2000）NEXT NEWS

1.6.4　生保サイトでユーザーの個人情報が露出

3 月 21 日から 22 日にかけて，オンライン生命保険サイトの SelectQuote で計算表をリクエストしたユーザーは、「期待以上の」結果を被ることになった。ソフトウェアの欠陥が原因で、ユーザーの個人情報が同サイトに残され、その後サイトを訪れたあらゆる人の目にさらされるという事態が発生した。

問題は、ユーザーが生命保険の計算表を得るために情報を入力した場合に発生。入力された情報は最後に画面からクリアされるはずが、そのままサイトに残り、氏名や住所、両親の病歴などが、次に入力しようとしたユーザーの画面に表示されていた。

【米国記事】　2000.3.22　（Mike Brunker, ZDNet/USA）

1.6.5　過去最大規模のクレジットカード情報オンライン漏洩――事件の詳細が明らかに

コンピュータへの不法侵入者が，電子商取引サイトから 48 万 5000 件ものクレジットカード情報を盗むという，インターネット上の窃盗としては過去最大の犯罪が発生，その大量の情報が，なんと米政府機関の Web サイトに置かれていたことが分かった。クレジット

カード各社は，この事件について既に提携金融機関に連絡ずみだが，3 月 17 日現在，情報漏洩した口座の多くは，まだ閉鎖されていないか利用者への盗難の通知が行われていない。

この盗難事件は昨年 1 月に起きた。だがこれまでは，ごく一部の詳細しか明らかにされていなかった。

盗難の事実は昨年 12 月 27 日，VISA USA が金融機関に送った手紙によって表面化することとなった。シークレットサービス（米財務省秘密検察局）の広報担当官 JimMacken 氏は，事件の存在を認め，インタビューに応えて 3 月 16 日，さらなる詳細をいくつか明らかにした。

銀行やクレジットカード会社がよく指摘するのは，盗まれたカードを他人に使われて請求を受けた場合,本来のカード保有者の支払い義務は 50 ドルまでであり,ほとんどの場合,このルールの適用を受けることができるという点だ。

だが，盗まれたクレジットカード情報は，インターネット上で商品を売る他の販売業者を標的とした詐欺行為に使われることもある。盗んだ個人情報を使って，新たなクレジットカードを取得したり，あるいは借金したり，高額商品の入手したりといったやり口だ。この場合，だまされた販売業者が損害や，犯人追跡のためのコストを負わされることが多い。

【米国記事】　2000.3.17（Mike Brunker, MSNBC & ZDNet/USA）

1.6.6　オンライン銀行を不正利用――他人の口座から現金引き落とし

1 月半ばのある日，Imad Khalidi 氏はメイン州ポートランドで自身が経営する自動車販売店 Auto Europe に出勤し， 2 万 1000 ドルが同社の銀行口座から引き出されていることに気がついた。サンフランシスコの Gucci に注文した商品の代金として，口座から自動的に引き落とされたものだった。それからの 10 日間は同社にとって地獄のような日々だった。設立間もない Web 銀行の X.com に絡むオンラインバンキングの悪夢に巻き込まれたのだ。そして，この Web 銀行にかかわる預金横領事件はこれだけにとどまらなかった。

誰かが Auto Europe の銀行口座情報を入手し，不正な引き出しを何回か試みた後，その情報をインターネット上に掲示していた。

「この口座を自分の X.com と Wingspan への振り込みに利用するといい」。犯人はニュ

ースグループに口座番号を列挙した後，不敵にもこのように書き込んでいる。「口座には数百万ドルもの残高があり，週に 2 万 5000 ドルくらいの引き出しなら気づかれることはない。明細は 3 カ月に 1 回しか発行されないのだから」

Khalidi 氏によれば，その後 10 日間にわたって犯人は，X.com または競合するオンライン銀行 Wingspan を利用して，1 日に 4? 5 回，違法な自動引き落としを試みたという。

最初の Gucci からの請求，およびその後 Auto Europe の口座に課金された請求のいくつかは，オンライン料金支払代行業者 CyberBills.com を通じて請求されたものだった。Auto Europe の経験は，他の企業にとっても教訓になるはずだと同氏は言う。インターネット上で全く取引を行っていなくても，インターネット詐欺の犠牲者になる可能性があるという。

【米国記事】　2000.1.30　（Bob Sullivan, MSNBC & ZDNet/USA）

1.7　プライバシー擁護団体と企業側の新マーケティング手法

米国では、インターネット上でショッピングやウェブサーフィンを楽しむ消費者から、cookie 等を使用して、無断でその個人が特定可能な各種の情報を収集している企業に対する批判が、プライバシー保護団体を中心に既に１９９９年くらいから始まっている。

特に、近年マーケティング手法の高度化・コンピュータシステムの高速化に伴い、この種のデジタル化された個人特定情報の付加価値は更に高いものとなり、これを利用しようとする企業とプライバシー保護の取組みとの軋轢は頂点に差し掛かっているのが現状である。この傾向を物語る関連記事（抜粋編）を以下順に見ていくものとする。

1.7.1　「コンシューマー・プロファイリング」に対して高まる批判――プライバシー擁護団体が廃止を訴え

Web マーケティング会社が行うコンシューマー情報のオンライン収集をめぐって論争が高まっている。

米連邦取引委員会（FTC）と米司法省は 11 月 8 日、企業がコンシューマーの情報をオンラインで集めること――いわゆるコンシューマー・プロファイリング――をどう捉えていくかを討議する公開ワークショップを開いた。これは，ターゲットを絞り込んだオンライン広告を打つために企業が行っているコンシューマー・プロファイリングに対し，規制をか

けていく方向へのお膳立てともいえる動きだ。

プライバシー擁護団体はこれに先だって 5 日，米連邦取引委員会（FTC）に対し，同委員会が調査中のコンシューマー・プロファイリング行為すべてを即刻中止させ，迅速に法規制を敷いて，コンシューマーのプライバシーを保護するよう求めている。

コンシューマー・プロファイリングには，ユーザーのネットサーフィン習慣に関する情報収集が伴う。オンライン上で広告宣伝活動を行う会社は，その情報をもとに，個々のユーザーの関心事に合ったターゲット広告を展開するわけだ。

だが，プライバシー擁護組織 Junkbusters Corp.の Jason Catlett 社長はこう指摘する。「過去 2 年のあいだに，Web サーファーの情報を収集しプロファイルを作成する技術は極めて侵略的になり，消費者のプライバシーを侵害する受け入れ難い行為となっている。消費者の同意や監視体制なくこうした情報を収集することに，米政府は歯止めをかける必要がある」。

オンライン広告業者は、ユーザーの個人情報を収集させないために、ユーザー自身がクッキーを解除できることをしばしば指摘している。クッキーとは、Web サイト上でユーザーが誰で、何を見て、いつ接続したかなどの情報を集めるために使われる機能。ユーザーはブラウザオプションでその機能をオフにすることができる。しかし、プライバシー擁護団体 Electronic Privacy Information Center（EPIC）のポリシーアナリスト、Andrew Shen 氏は、ユーザーがクッキーの解除の仕方を知っていると期待するのは現実的とは思えないとしている。

「プライバシー保護の負担を消費者側に押しつけている。利用者が自分自身を守らなければならないのはおかしい」と Shen 氏は指摘する。

（Jennifer Mack & Steven Vonder Haar，ZDNN/USA & Inter@ctive Week）

1.7.2　米消費者団体が「cookie」悪用によるプライバシー侵害を警告、FTC に請願書

【米国発】　'99.12.3　5:21 PM PT――

米国の消費者擁護団体とプライバシー擁護団体の一団が 12 月 3 日、電子メールソフトの“抜け穴”を埋めるよう求める請願書を米連邦取引委員会（FTC）に提出した。この“抜け穴”を使えば、電子ダイレクトメール配信業者が「cookie」技術を使い、消費者を特

定できてしまう危険があるとしている。これらの団体によると、大量の電子メールを配信する業者は、電子メールメッセージに cookie を添付して配信する可能性がある。cookie は、通常は電子メールではなく Web ブラウザで利用されているユーザー識別のための小さなファイルだ。セキュリティコンサルタントの Richard Smith 氏によると、もし誰かが Web ブラウザを使って電子メールを読み、この電子メールに Web から取ってきたグラフィックスが含まれていた場合、cookie をユーザーの PC に植え付けることができる。このユーザーがその後、インターネットを閲覧すると、特定のサイトからそのユーザーの cookie を読むことができ、ユーザーの電子メールアドレスと照合可能だという。

世界最大のオンライン広告サービス会社 DoubleClick は先日、電子メールマーケティング会社の Opt-In Email.com を買収している（12 月 2 日の記事参照）。このような合併によって、企業は cookie データを基にした匿名プロファイルと電子メールアドレスとの照合がたやすく行えるようになるという。

プライバシー擁護団体は、こうした業種オーバーラップへの危機感が、今回 FTC に請願書を出した理由の 1 つであることを認めている。

プライバシー擁護組織 Junkbusters の Jason Catlett 社長は、「プライバシーに対するこうした非常に危険な脅威に対処できないとなると、米国の消費者保護機関は全く機能していないということになってしまう」と語る。

今回 FTC に請願書を提出した団体は、Junkbusters, Electronic Privacy Information Center（EPIC）, Electronic Frontier Foundation（EFF）, Ralph Nader 氏率いる Consumer Project on Technology（EPT）, Privacy Rights Clearinghouse など。

（Margaret Kane, ZDNet/USA）

1.7.3 EPIC が実施した調査「Surfer Beware III」がオンラインショッピングによる個人情報流出の危険を警告

米国の記事によると、プライバシー擁護団体の Electronic Privacy Information Center（EPIC）は、大手ショッピングサイトが個人のプライバシーに関わるデータ収集技術を採用しており、この年末商戦中にオンラインショッピングを行う消費者は、提供した以上の個人情報を取られる可能性があると警告している。EPIC が実施した調査「Surfer Beware

III」によると調査対象となった 100 件の電子商取引サイトのうち 87 件が cookie を採用していた。また 35 のサイトがユーザープロファイルを使った広告技術＝「コンシューマプロファイリング」を利用していることも明らかになった。ユーザープロファイル収集に対しては、その技術的手法について米国では近年、複数の団体から非難の声が上がっている。（.zdnet/news/9912/18）

1.8　個人情報保護の在り方についての課題検討

さて、次にＥＣ上の個人情報保護の問題は、前述のような米国の実態及びそれがまた国内でもやがて現実となるであろうという状況を踏まえて、さらに大きく分けて二つの観点から、早急に検討しなくてはならない問題である。

一つは国際的な要請つまり外圧的要素である。インターネットの世界的な普及により、これまで各国毎に異なった対応となっていた個人情報保護についての世界的規範を目指す動きが始まっている。

特に欧州で 1998 年の 10 月に発効した個人データ保護のいわゆる「ＥＵ指令」の 25 条には域外国へのデータ移転規制条項があり、ＥＵ域外国の個人データ保護の水準が適切でない場合に、ＥＵ加盟国からのデータ移転を禁止できる。このため例えば、ヨーロッパでアメリカのカード会社が蓄積した顧客情報を、アメリカに持ち帰る事が出来ないという事態が実際に起こる可能性がでてきた。

これに対して米国側の反応は早く、従来からのセーフハーバー（妥協点）政策に加えて、マーク制度等を中心とした自主規制策を次々と立ち上げ、ここにきて民間企業の方もデータ保護への意識を益々強め、以前と比べて自主規制の効果が着実に上がってきたというのが米国の政府系機関・業界団体も含めた認識となっている。

それに比べ、この件に関する日本国内での認識は、特に民間レベルでまだまだの感は否めない。その反映として、インターネット上に開店しているサイバーショップのうち、この個人情報の保護を意識して実践しているサイトが、これまでは一部の先進優良サイトに限られている点からも明白である。今回の個人情報保護の立法化による規制だけでなく、もっと民間の企業自身がデータ保護に関する危機感をもたねばならない必要性がそこにある。

二つ目の個人情報保護に関する検討が必要な観点は、日本国内でのＥＣ普及を阻害している要因の除去というポイントである。

前述の様に 2000 年 5 月にＥＣＯＭがおこなった、「ビジネスショウ 2000 東京」における「ＥＣ意識調査のアンケート集計結果」（有効回答 2,400 名）によると、ＥＣ参入への不安の最大要因は、去年と同じくやはり〔自己データの漏洩〕の項目である。今回の結果についても、これまでの調査と比べてその割合が若干減ったとはいえ、依然として 70%を超える高率であった。

この点からも国内での消費者ＥＣのさらなる発展のためには、現状の自主規制のレベルアップはもとより、個人データ保護における今回の法整備も含めたネット環境･インフラの整備が急務であることは論をまたない。

1.8.1　具体的課題の解決について

前述の課題解決には具体的に次の 3 つの項目が不可欠と考えられる。

(1) ＥＣ上の消費者情報・プライバシー保護のための立法策検討（個別法含む）

(2) 消費者が安心してＥＣに参入できるようなネット環境の整備（インフラ・技術面）

(3) 消費者・企業双方に対するＥＣ上のプライバシー保護リテラシー

また従来からも、民間の自主規制を支援する行政の取組みとしては次にあげる三つがなされている。

一つは 1997 年に改訂された、民間の自主規制主体である業界団体が採用するガイドラインの雛型となる「旧通産省個人情報保護ガイドライン」の策定。

二つ目は適正な個人情報保護を行っている事業者に対してＰマークを付与する、1998 年から導入されたプライバシーマーク制度（（財）日本情報処理開発協会）の導入。

三つ目は事業者のプライバシー保護マネジメントの確立を目指して 1999 年に制定された、前述のプライバシーマーク制度と連動したコンプライアンス・プログラムの実践を認定する日本工業規格（JISQ15001）の設定である。

一方、法規制という課題について、政府は 1999 年に高度情報通信社会推進本部の下に個人情報保護検討部会を設置、同年 11 月には官民両分野を包括して個人情報を保護する基本法制定を促す中間報告をまとめた。

また 2000 年には個人情報保護法制化専門委員会を設置し、2001 年の通常国会提出を目指して個人情報保護基本法の大綱案を策定した。

そして 2001 年 3 月の閣議で民間分野も対象とした、初の「個人情報保護法」が決定されて国会の議決を待つ事となった。

この法案骨子となった大綱は、個人情報の適切な取扱いを求める「基本原則」と守らなければ罰則の対象とする「義務規定」の二つの柱からなっている。その基本原則は情報取扱いの基本的考え方である 5 項目からなり、義務規定は個人情報の取扱い事業者が守るべき必要最小限の 9 規定からなっている。

また、基本法の罰則は事業者の義務違反に対して直罰規定ではなく、まず、義務違反があり、主務大臣の中止・是正措置の勧告・命令がありその命令に違反した場合に罰則適用になるというステップ規定となっている。

そして、基本法にはこのように情報の窃盗や漏洩に対する直罰規定がないため、従来よりの「情報窃盗に罰則規定を」という立場からこれを意図した個別法の議論の余地もまだ残っていると言わざるを得ない。

2　民間個人情報保護の法制度のあり方についての検討

一般的に言って個人情報保護の問題は、広く国民等全般に及ぶ問題であるとともに、国民一人一人にも深く関わる問題であるので、あまねく各界、各層からの意見等を聞くことが、今後の検討に不可欠であると考えられる。

このため、政府においては、いわゆるパブリック・コメント手続に準じて、国民等の意見を聴取する手続を実施するよう要請し、各場面で次の様に実施されている。

特に今回の個人情報保護法は、わが国初の、民間分野の個人情報保護を対象とした法規制であり、民間の個人情報取扱い事業者に与える影響はきわめて大きいと言わざるを得ないし、また業界内でのそれまでの商慣習や常識等で当たり前とされていた事項が新しい法規制によって根底から覆ること自体もあり得る事である。

そのような劇的変化を伴う可能性のある強制力を持ったシステマチックな環境変化については、その方向性について行政側の一方的な意図だけでなく、民間企業側の実ビジネスをベースにした民意の吸上げが必須となる。それが為の、パブリックコメントであり、これが為の実務ベースに立った民間側の意見反映が大きなポイントとなることは言うまでもない。

2.1　「我が国における個人情報保護システムの在り方について（個人情報保護検討部会中間報告）」に対する国民等の意見の概要

標記中間報告について、1999 年 12 月から 2000 年 1 月 20 日まで、国民等から意見を募集。意見の総数は計 57 件で、個人から 27 件、企業等の法人及び団体からは 30 件となっている。意見は主に以下の項目に関するものとなっている。（個人情報保護担当室資料より）

●意見の概要

1. 個人情報を保護するに当たって考慮すべき視点としての、個人情報の保護あるいは利用面の有用性に関する意見－15 件
2. 個人情報保護の目的について、個人情報の保護と憲法との関係に関する意見－14 件
3. 保護対象となる個人情報保護の範囲について、電子計算機等処理情報等に関する意見－17 件
4. 適用除外を検討する分野や収集、利用等、管理等、開示等、管理責任及び苦情処理の在り方に関する意見－40 件

企業の保有する従業員の人事情報等（インハウス情報）、疾病登録、疫学調査等の

取扱いに関する意見も寄せられる。

5. 罰則等の要否、実効性確保、監督機関に関する意見－15 件

6 個別法等の整備に関する意見－12 件

7.その他：複層的な救済システムの在り方、苦情処理・相談窓口の整備、第三者的な窓口の設置

2.2 法制化委員会の答申（中間整理）に対するパブリックコメント作成に向けた民間企業からのあり方提言

次は 2000 年度 6 月の個人情報保護法制化委員会の答申（中間整理）に対して、ＳＷＧとしてのパブリックコメント作成のベースとなった、各メンバー企業より提出されたコメントのうち主要なものをまとめて紹介する。

2.2.1 ＥＣＯＭＳＷＧの主要メンバー企業よりのコメント

(1) 「個人情報保護基本法制に関する大綱案（中間報告）」について（コメント）

：富士通株式会社

標題中間報告につき、以下の通り考える。

① 対象となる個人情報の範囲

対象個人情報の範囲が広範である一方で、これに対する適正な管理義務等を課されると、事業者にとって非常に大きな負担となり、遵守が事実上不可能になりかねない。

⇒定義において(1)個人情報の範囲を限定する、(2)個人情報自体は広範なものとしたままで、具体的な義務等が想定される局面においては一定の限定を行う、という選択肢がありうるが、基本法であることに鑑み、(2)の選択肢のほうが望ましいと考える。その場合、「組織的に管理されている、電子計算機で自動処理される情報又は検索可能な情報」に限定することが妥当と考える。

② 受託者の規則

第三者への委託に係る規定はあるが、これは委託者側につき規定するものであり、受託者側の対応を定める規定はない。自ら利用する目的で個人情報を収集・取得した者と同等の負担を課すことが妥当かどうか、検討する必要があるのではないか。

⇒「事業者が遵守すべき事項」で掲げられた事項につき、(3)内容の正確性、(7)関連

事項の公表、(8)開示・訂正、(9)苦情処理については、その性質上、委託者側が負担すべき事項であり、受託者が負うべきものではないと考える。他方、(1)利用目的制限、(5)安全保護措置などは受託者も遵守すべき事項と考える。

③　委託先の開示

第三者委託を行っている場合、委託理由及び委託先の名称を公表することとなっているが、委託先の変更やセキュリティ上の理由からの未公表が考えうる。

⇒委託先を公表する目的が、自己のデータがどこに流れているか確認するためなら、「公表」まで必要ない（「開示」で十分対応できる）と考える。また、選択的に、委託先は公表／開示せず、事故の際は委託者が責任を負うことも考えられる。

④　公表の必要性

事業者はその保有する個人情報の処理等に関する情報を公表することが求められている。

⇒直接利害関係を有さない公衆にも公開することが求められているが、必ずしも必要ないのではないか。利害関係者（＝その個人情報を保有されている個人）への開示は必須とし、それ以外への公表については、各事業者の裁量に委ねることで足りるのではないかと考える。（ただし、公表すべき情報の範囲にもよる）

⑤　公表の効果

事業者が公表を行った場合の法的効果につき、引続き検討するとしているが、検討の方向性がわからない。

⇒公表した際の何らかの免責を考えているのか（何の免責か？）、それとも虚偽の公表を行った場合の制裁（景表法違反等）を考えているのか？

⑥　開示・訂正等の対象となる情報の範囲

保有する個人情報に対する本人開示につき、一定の場合にはこれに応じ、訂正等を求められた場合には原則これに応じることとされている。本人から収集した情報についてはこれでかまわないと考えるが、保有者が自ら追加したもの（評価情報等）については取扱いを異にするべき場合があるのではないか。

⇒①で述べたとおり、具体的な義務等を伴う場合には対象となる個人情報の範囲を合理的に限定すべきであり、(1)開示対象とする個人情報を、当該本人から直接又は間接に収集したものに限定する、(2)事業者の適正・円滑な業務遂行に支障ある場合は開示等の対象としない、のいずれかの方策が考えられる。

⑦　個人情報安全管理者に関する公表

事業者が公表すべき事項のひとつに、安全管理者の氏名及び連絡先が挙げられており、ここが事業者に対する請求等の窓口となると規定されている。しかし、管理者が一人とは限らず、また、当該管理者が窓口を兼ねているとは限らない。

⇒責任者の明確化の必要性・必然性がどの程度と考えるかにもよるが、まずは問合窓口の設置を求め、責任者（あるいは責任部門）の公表については各事業者の裁量に委ねることで足りるのではないかと考える。

⑧　地方公共団体の措置

地方公共団体はその保有する個人情報の取扱いにつき、必要な条例等の整備を行うものとしているが、その際、各地方公共団体の自律性を尊重しつつ、基本法制との整合を図る観点から検討するとしている。

⇒ここでの「地方公共団体の自律性」とは何を想定しているのか不明。各自治体で取扱いを変える必然性・合理的理由はあるか？　また、条例の規定が民間部門保有の個人情報にも及ぶ場合、各自治体ごとの対応を求められることになり、負担が大きい。基本法制の枠内で条例化すべきと考える。

(2)　「個人情報保護基本法制に関する大綱案（中間整理）」に対する意見（2000 年 6 月 23 日：日本アイ・ビー・エム株式会社）

「基本的な考え方」

個人情報は、原則として、民間の自主的な取組みによって保護され、法律による保護は信用情報、医療情報といったセンシティブな特定情報にのみ適用されるべきである。しかしながら、諸外国と比較して民間部門における自主規制も含めた制度的枠組みが十分に確立していない我が国では、基本法により基本原則を定めることは、個人情報保護に対する意識と実効性を高める有効なひとつの解決策であると考えている。

個人情報保護の基本法制では、情報経済の発展、ビジネス・モデルやテクノロジーの革新を阻害することがないように、法規制は必要最小限に留め、民間の自主的な取組みを十分に尊重、促進する枠組みの構築が必要である。こうした観点から、基本法は次のような前提で法制化すべきである。

「個人情報」「事業者」「利用」「開示」などの用語や範囲の定義は簡潔であり、かつ柔軟性が確保されること

基本原則、遵守事項の具体的措置等については詳細を規定せず、事業者の自主性

を最大限に確保すること

関係主体に不必要なあるいは過度な義務を課すものでないこと、また過度なコストを課すものでないこと

また、情報経済のグローバル性を前提に、国際的に支持された原則を採用し、諸外国の制度との整合性を確保することが必要である。この観点からは、特に米国・ＥＵ間の交渉の状況を視野に入れるべきである。セーフ・ハーバー・アグリーメントにおいて、米国とＥＵは、民間事業者が一定のプライバシー原則の適用を証明、厳守、実行することを前提に民間の自主規制を認めている。ここで合意された次のような原則は我が国の基本法でも採用すべきである。

どのような個人情報が収集され、何に使われるかを当該個人が知る権利

個人情報が第三者に開示されてよいか、また、される場合には、どのように開示されるかを当該個人が選択できる権利

収集された個人情報が当該個人に開示され、また、不正確な個人情報は当該個人が訂正、変更、削除できる権利（但し、この権利は、それに要する費用と負担が加味され制限されうる。）

「主な論点に対する考え方」

大綱案（中間整理）で示された各論点についての意見は次の通りである。

①　定義

用語や対象範囲等の各定義は、簡潔であり、かつ柔軟性が確保されるべきである。例えばＯＥＣＤガイドラインなど、国際的にコンセンサスの得られた定義を採用すべきである。

②　利用目的による制限

個人情報が収集目的外の目的に利用される場合、どのように利用されるかについて当該個人が選択できよう、オプトアウトできる機会が提供されるべきである。

③　第三者に対する目的外の提供の制限

個人は自己の個人情報を収集される際に、第三者への提供の可能性についてあらかじめ知らされ、この提供についてオプトアウトの機会が与えられるべきである。また、個人情報の第三者への目的外の提供についても、当該個人にオプトアウトの機会が与えられ、また、かかる第三者への提供にあたってはオプトイン等の手段により当該個人の同意を得るべきである。

④　安全保護措置の実施

事業者は、個人情報保護のための適切な措置をとり、また、個人情報の紛失、誤用、改竄等を防止する合理的な措置を取るべきである。しかし、セキュリティ技術やデータベース管理システム等が急速に進歩しており、技術革新を阻害することがないように、安全保護措置の具体的な方策は詳細を規定せず事業者に委ねるべきである。また、「個人情報の保護に関する規程」は法的強制ではなく、事業者が自主的に策定すべきものである。

⑤　透明性の確保／開示、訂正等

事業者は不正確な個人情報が訂正されるよう合理的な処理プロセスや仕組みを確立すべきである。しかし、基本法では、開示、訂正の手続きを詳細に規定すべきではない。当該情報がセンシティブな情報であれば事業者は必ず訂正すべきであるが、そうでない場合には、その実行に要する費用と負担を加味できるようにすべきである。

⑥　政府の措置及び施策

政府は、民間の自主規制の促進、事業者および個人の意識向上に継続的に取り組むべきである。「個人情報の保護に促進に関する方針」はこのような観点から策定されるべきで、詳細な規定や義務づけにより事業者の自主性を拘束するものであってはならない。

⑦　苦情等の処理

苦情等の処理に政府機関が関与する仕組みを設けるとしても、まず当該事業者自身、簡易な第三者機関による苦情処理を先行させるべきである。政府機関を第一の苦情申立先にすることは、当該政府機関はもとより、申立てられる事業者、申立てる個人にとっても、事務処理、時間、コストが大きくなると想定される。政府が行う調査は、被調査事業者の日常の事業活動を阻害しないよう配慮すべきである。また、救済措置は、賠償ではなく、情報の訂正や謝罪といった実際的で迅速な方策がより重要である。苦情処理プロセスは、申立人、事業者の双方にとって簡便でコスト効果の高いものであるべきである。

⑧　第三者への委託

個人情報の取扱いについて、事業者が情報処理の委託先との間で個々に独自の取決めを行うことを制限すべきではない。例えば、ＩＴアウトソーシング契約では、お

客様毎に個人情報の取扱いに関する要求事項を調整しており、このような当事者間の取決めを尊重すべきである。事業者と委託先との関係は当事者間の取決めが基本であり、基本法では、事業者に過度な監督責任や義務を課したり、委託先に過度な責任を求めるべきではない。

⑨　個人情報の処理等に関する事項の公表

個人情報の処理等の委託先の公表は、事業者および委託先との責任関係が個々の委託業務毎に異なるため、一律とせず、当事者が判断すべきである。

⑩　地方公共団体の措置

地方公共団体によって講じられる事業者や住民に対する措置は、個人情報保護に関する啓蒙や民間の自主規制の取組みを促進することを目標とするべきである。これら措置は、基本法と一貫性があり、事業者に追加負担を課すべきではない。

⑪　国民の役割

国民に対しては基本法について十分な啓蒙を行い、その際、自己に関する個人情報の管理は自己責任が基本であることを周知徹底すべきである。

⑫　罰則の可否

現行の刑事法制等で対処可能な行為に追加的な罰則措置を講じる必要はないと考える。基本法は基本原則を定めるもので、罰則を設けるべきではない。

「今後の進め方」

公表された大綱案には不確定な要素が多く、今回の意見募集を踏まえて法制化案を策定された時点で、再度の意見聴取の機会が与えられ、経済活動の主体である民間の意見が反映されることを要望する。

また、法制化に先立って、欧米等との事前調整により、国際的に整合性のとれた個人情報保護の枠組みが構築されることを要望する。

(3)　「個人情報保護基本法制に関する大綱案」への意見（2000.6.28：電子商取引安全技術研究組合）

- はじめに

社会における急速なIT普及に伴う個人情報の保護については、「行政サービスと民間市場」、「目的外利用と漏洩・盗用」、「所有権と対価」等の視点から、正確な整理を行う必要がある。この大綱案を一読する限りこれらの整理がきわめて曖昧であり、法制化の基本姿勢が何処にあるのかよくわからない印象を受ける。

電子商取引推進の観点から見ても、個人情報の適正な活用を促進する姿勢は見えず、単なる利用の制限としか思えない表現も散見され、憂慮すべき内容と思う。

以下、気づいた項目について、出来るだけ要点を整理して申し述べる。

① 行政サービスと民間市場における個人情報の活用

国及び地方公共団体が行う行政サービスの場合、従来いわゆる縦割りの制度のために、個人情報は個別の機関内に蓄積され、他機関が利用することは比較的困難であった。行政コスト削減のため、これを機関横断的に活用するニーズと、いわゆる国民総背番号制への国民の危惧（個人情報の同意なき、目的外利用への不安）に応える適切な運用とのバランスをいかにとるかが課題である。この大綱案においては、民間事業者に対して求められている個人情報保護の内容は、原則として全て、行政機関に求められるべきものであるにもかかわらず、特に国の保有する個人情報については「別に法律の定めるところによる」とするなど、全く法制の対象外に置いており、著しく相当を欠くものである。基本法制においては、行政サービスも民間事業者のサービスも全体を通して、「個人情報の目的外の同意なき利用は不可」の原則を定めるべきと考える。

いわゆる、「one to one marketing 」の発展に見られるごとく、民間事業者の適正な個人情報の活用は、電子商取引等の進展を促し、ひいては、社会の発達を推進する重要な要素である。その一方で、個人の権利を侵害するような個人情報の活用が、かえって消費者の不安と嫌悪を招来し、社会の発達を阻害することも論をまたない。民間市場においては、このバランスを如何にとるかが課題である。大綱案は、個人情報「活用」の実体を想定せずに、単なる保護の発想に終始している印象を受ける。将来社会において、どのような個人情報活用がなされ、したがってどのような問題が生じるかを十分に予測していないのではないかと考えざるを得ない。

② 個人情報が財産であることの確認

大綱案に見られる上記のような矛盾ないし混乱の理由は、究極すれば、以下の視点が欠如していることにある。

即ち、個人情報が個人に帰属する財産であり、所有者の同意によって、財貨ないし便益の対価として、他者に制限付きで使用を許諾する性質ものであるという視点がそれである。

大綱案における個人情報とは、本来の所有者に帰属するが、他者に「知られてしま

う」、経済的価値のない、「個人にとって大切なもの」としてしか取り扱われていない。

行政サービスにおいても、民間市場においても、個人情報とはその所有者に帰属する無形の財産であり、所有者の益のために適切に活用されるべきものであるとの視点から、その保護を論ずれば、自ずから適切な運用のガイドラインが生まれるものと考える。

③　個人情報の目的外利用と漏洩・盗用

大綱案においては、個人情報の目的外利用と漏洩・盗用とを同列に論じているきらいがある。個人情報侵害の主体が誰であるか（本来の所有者に許諾を得た者か、使用許諾の関係にない第三者か）を明確に区分した上で、個人情報の所有者から使用許諾を得た者（行政機関または民間事業者）が、個人情報を「侵さない」ことと「侵させない」ことを、そしてそのために何をなすべきかを、それぞれの場合について整理して規定すべきである。

大綱案の各項目は、個別にはこれらを満たしているが、「誰が、何のために」を明確には述べていない。

④　所有権と対価

個人情報は、財産であるから、所有者は財貨や便益などの対価を得て、他者にその使用を許諾することが出来る。

個別の個人情報の価値は、「公開の場でどれだけ入手が困難か」「どれだけ他者にとって有用か」によって決まる。

第三者が容易に知りうる個人情報は、「プライバシーではない」のではなく、財産として価値の少ない個人情報なのである。

個人情報は原所有者の許諾なく使用されてはならず、使用の許諾を得た者は、許諾の範囲内でこれを利用しなければならず、利用に際して原所有者の権利が、第三者に侵害されないような措置をとらなければならない。大綱案は、この観点から再整理されるべきと考える。

2.3　大綱案(中間整理)に対する「ＥＣＯＭ個人情報保護ＳＷＧパブリックコメント」

次に前述の 3 団体の意見とそれ以外の各ＳＷＧメンバーよりのコメント等をもとに作成

し、個人情報保護法制化委員会あてに提出した当ＳＷＧのパブリックコメントを見ていくものとする。このコメント作成の過程でＳＷＧ内の意見が分かれて、統一的な見解に至らなかった事項については両論併記として記載している。

2.3.1　個人情報保護ＳＷＧパブリックコメント内容

●個人情報保護基本法制に関する大綱案(中間整理)]に対する意見書

＜個人情報保護法制化専門委員会 御中

内閣官房内閣内政審議室　個人情報保護担当室 御中＞

「電子商取引推進協議会　個人情報保護 SWG」

2.3.1.1　定義・適用範囲関連について

- **「個人情報」に検索可能な状態で保有されているマニュアル処理のものを含むの点については、とくに「検索可能な状態で保有」の表現を保持して頂きたい。**
- **事業者間取引における取引相手の個人情報利用（名刺による得意先情報の利用）は範囲外とさせて頂きたい。**
- **その他「事業者」・「個人情報」等の用語・対象範囲等の各定義については明確化をした上で簡潔性かつ柔軟性及び国際的コンセンサスの確保をお願いしたい。**
- **個人情報の「利用」・「提供」といったその「流通性」における行為規制的な考え方も適用範囲にいれて検討すべきであると思われる。**
- **事業者が保護（遵守）の対象とすべき「個人情報」は、電子データの形のものと、速やかに電子化して活用することが予定されたデータに限ることが必要と考える。**
- **ＯＥＣＤ8 原則との整合性を図り、個別法（分野別）の整備を行い他の分野については自主規制。**
- **対応して実行担保として第三者認証制度の確立をすべきであると考える。**
- **ハイリーセンシティブな情報についての考え方を明確にすべきであると思われる。**

2.3.1.2　基本原則関連

(1) **利用目的による制限について**

利用目的の変更可能な範囲について今後の検討事項としている点につき、当初の目的に限定されるのでは実際的ではないケースが多い事を想定した表現にして頂きたい。

(2) 透明性の確保

「開示請求権」・「異議申立権」等の具体的かつ明確な個人権利の明記をした方が良いのではないかと思われる。

地方公共団体や紛争解決機関と事業者間または個人間において、抽象的な権利確保の主張が行われる事が懸念される。これらの排除のためにも、権利内容の明記必要と思われる。

開示・訂正手続きの詳細規定については基本法で規定するべきではないという観点から、またセンシティブな情報については、事業者は必ず訂正をするべきだが、センシティブでない情報については、その実行に要する費用と負担を加味できるようにするべきであると思われる。

2.3.1.3 政府の措置及び施策について

(1) 個人情報の保護の推進に関する方針の策定

民間の自主規制の促進・保護意識の向上がポイント、事業者の自主性を拘束しないような配慮が必要と思われる。

(2) 苦情等の処理

利便性･費用対効果を考えて、簡易な第三者機関による苦情処理を基本として検討頂きたい。

政府機関が関与することを認める表現について、事業者側の日常業務活動を阻害しない範囲での調査実施実施等の配慮が必要と思われる。

「 政府は勧告を行うという仕組みも考えられる」という表現で、行政の介入のレベルがＦＴＣ等の活動と比較して「勧告」のレベルで十分かの検討が必要と思われる。

2.3.1.4 「事業者が遵守すべき事項」

(1) 利用目的による制限

具体的な利用目的の通知等の表現は、限定的過ぎるので同意を求める為の明示という表現ではどうか検討頂きたい。

本人以外からの間接収集については、かなり広範囲に「本人同意取得不要」等の簡便化が認められるべきと思われる。また第三者にすでに公表されている情報については本人同意取得不要と考える。

収集目的外の目的に利用される場合、どのように利用されるかについて当該個人が選択できるように拒否すれば中止できる機会が付与されるべきと思われる。

(2) 第三者への提供

第三者に対する目的外の提供制限について、まず個人に第三者提供への可能性の明示とその同意があればこれを実行できるようにして、かつ目的外提供時については拒否すれば中止できる機会が付与されるべきであると思われる。

(3) 安全措置の実施

技術革新の進歩を考慮して場合、安全保護措置の具体的方策については詳細を規定せずに、これを事業者に委ねるべきと思われる。

「個人情報の保護に関する規定」については、法的強制ではなく事業者が自主的に策定すべきものと思われる。

(4) 第三者への委託について

委託先も本基本法制の対象範囲内であり、委託元の事業者に対する規制は過重な保護措置の要請となるため不必要ではないか。

受託者側についての規定はないが、委託者側と同等の負担を課すことが妥当かどうかの判断が必要と思われる。

事業者と委託先の関係は当事者間の取り決めを基本とする考え方もあると思われる。

(5) 個人情報の処理等に関する事項の公表について

第三者に委託している場合や第三者に提供して使用させている場合の、その理由及び第三者の氏名又は名称の公表については、委託先の変更やセキュリティ上の問題があると思われる。

事業者が公表を行った場合の法的効果について、免責事項となるかどうかを検討頂きたい。

基本的に個人情報に関する公表という概念導入に反対であるという意見もあり。

公表の必要性について、その範囲にもよるが、利害関係者への開示のみ必須としてはという意見もあり。

委託先公表は、事業者及び委託先との責任関係が個々の業務毎に異なるため当事者判断に委ねるた方がいいのではないかの意見もあり。

特に電子商取引の場合、委託主体者と技術面をカバーする複数の受託者が存在するケースが容易に考えられ、公表した場合は消費者の混乱を招くと思われる。

個人情報安全管理者に関する公表については、問い合わせ窓口の設置がポイントで、責任者等の公表については各事業者の裁量とする事の検討をお願いしたい。

同管理者はドイツのように従業員の中から、「個人データ保護受託者」の配置を法律で義務付ける事を意図するものか検討頂きたい。情報処理の外部委託については同意不要と考えるが、第三者への提供は同意に範囲内に限られるべきであり、公表は必要である。

(6) 開示、訂正等

保有者自ら追加したもの（評価情報等）の取扱いについては別途検討が必要ではないかと思われる。いわゆるアクセス権について単純な開示訂正ではなくいくつかの条件付がなされるべきで、データの構造やシステムと関係する問題でもあり、現在のコンピュータでは個人情報を開示することを前提にプログラムが作られていないのが現状。このため別途プログラムの開発が必要となり事業者にとっては負担増となる。

2.3.1.5 地方公共団体の措置

「地方公共団体の自立性を尊重」した場合、各団体の制定する条例に格差が発生した時の対応時に全国規模の業者は混乱、基本法制の枠内で法制化すべきと思われる。

事業者や住民に対する啓蒙や民間の自主規制促進を目標とすべきものであり、事業者への追加負担は課すべきでないと思われる。

2.3.1.6 国民の役割

基本法についての十分な啓蒙と個人情報は自己管理が基本である事を周知徹底させるべきと思われる。

2.3.1.7 罰則の可否

基本法は基本原則を定めるもので罰則規定は必要ない（現行刑事法制にて対応）と思われる。

きわめて悪質な行為に対する厳格な罰則規定の検討は別途必要との意見もあり。

特定分野だけに対する過重な保護規制は該当分野の活力を失わせる可能性あり慎重な対応が必要と思われる。

法への罰則導入には反対で、義務創設的規定よりも理念的規定にして自由度を高めにする必要との意見あり。

2.4 個人情報保護法制化委員会：関係団体別ヒアリング資料

次に個人情報保護法制化専門委員会が 2000 年に行なった関係団体別ヒアリングのうちで、7 月のＥＣＯＭに対するヒアリング向け資料（個人情報保護ＳＷＧとして作成）を見て

いくものとする。これは行政側に対してＥＣに関わる民間企業側としての個人情報の取扱の実態を把握してもらうという点でとくに意義深いものがあった。

2.4.1　関係団体別ヒアリング事項「電子商取引における個人情報の取扱の実態」（電子商取引推進協議会：個人情報保護ＳＷＧ）

2.4.1.1　結合データベース化による個人の特定

インターネットを使ってバーチャルショップやポータルサイトのホームページにアクセスすると、本人が自ら個人情報を入力しない場合であっても、サーバー側には、アクセス・ログ、接続履歴という形でアクセスした側の情報が送信・蓄積されているのが実態である。またインターネットを利用する殆どのケースにおいて、いわゆる cookie というデータの自動送信の仕組みを使って、パソコンのブラウザ側の情報（アクセスサイトのコーナー・商品・興味分野等）は匿名性をもってサーバー側に送られている。

これらの蓄積データと氏名・住所・メールアドレスなどのインプットされた個人情報を結合すると、本人の知らない間に特定可能な結合個人情報データベースを容易に構築することができる。この手法が前述の様に米国で問題となっている「コンシューマー･プロファイリング」とよばれるものである。

こうした取扱のメリットとしては、いわゆるワン・ツー・ワン・マーケティング（欲しい個人に、その欲しい商品・情報を）という事業者側・ユーザー側の双方にとって非常に効率的なビジネス展開が可能になる。

反面、そのデメリットとしては、デジタル情報であるが故の特性を悪用されて、大量の個人情報が容易な手段で、情報主体の知らない間に、しかも瞬時に流出、漏洩してしまう危険性をはらんでいるという点が挙げられる。

2.4.1.2　情報収集時における目的の通知、同意の取得の程度

それぞれの企業規模・業態によってバラツキあるのが実態。

(1) 大手企業サイト・有名モール・通信プロバイダー等

プライバシーポリシー及び個人情報保護に対する方針・考え方をウェブ上に掲載して、同意の上で取引開始・情報収集に至る。

特に cookie（前述のブラウザ側からの自動送信データ）の使用をホームページ上に公開して、オプトイン（事前同意）で了解を得てアクセスさせるサイトも多い。

(2) その他及び個人経営サイト等

単一ショップでプライバシーポリシーをウェブ上に掲載している例もあるが、現実には保護方針等の明示や事前同意なく個人情報を収集するケースが大半。

2.4.1.3　ネット上で収集される個人情報の管理について

データベース化した電子媒体での保存が基本であるが、その保管場所・対策については様々である。

(1) 大手企業・情報処理関連企業サイト

ホストコンピュータやメインサーバーのハードディスクに蓄積されている個人情報について、パスワード・アクセス制限等により厳重に管理し、外部からの不正アクセスについてもファイアウォールの設定等のセキュリティ対策がなされているケースが多い。

(2) その他のショッピングサイト等

一部にはデータ保護意識を強く持ち、社内体制も含めて整備されているサイトもあるが、多くはコストとのからみで厳重なセキュリティ対策とまでは行かずに、サーバーのハードディスク保管以外にMO・フロッピーディスク等の可搬電子媒体に収納、キー付き保管等を行う程度。

2.4.1.4　ネット取引における個人情報保護の取組状況

インターネット上での個人情報の保護については、現状として下記の項目が挙げられる。

(1) ガイドライン等による規制

「通産省個人情報保護ガイドライン」等をベースにした各関連団体による保護ガイドラインの策定。

（例）ＥＣＯＭの「電子商取引における個人情報保護ガイドライン」

(2) 個人情報保護マーク制度のオンライン運用

ＪＩＰＤＥＣのプライバシーマーク（JIS 規格）

日本データ通信協会の個人情報保護マーク

その他民間業者によるオンラインデータ保護マーク

(3) 技術的なアプローチ

Ｗ３ＣによるＰ３Ｐ（プライバシー提供ランク自動設定）の取組み

ＯＥＣＤによるプライバシー・ポリシー・ジェネレータ（生成器）導入

各種暗号技術による通信データの保護（ＳＥＴ・ＳＳＬ等）

(4) 先進企業による自主規制

プライバシーポリシー・個人情報保護方針のウェブ掲載

プライバシー保護不充分企業サイトに対する自社広告自粛

個人情報保護プログラム（社内遵守規定）の策定

(5) 国際的な取組

プライバシー規制に対する企業側意識の高まりを反映してＪＩＰＤＥＣのプライバシーマークの申請が増加

このＪＩＰＤＥＣと米国のＢＢＢオンラインのマーク制度との相互承認に向けての取組み

米国を代表として、プライバシー保護の民間団体の活動が活発化

世界的にもオプトイン（事前同意あれば可）ビジネスが台頭してきており、これまでのオプトアウト（事前拒否なければ可）ビジネスに対する個人情報取扱いの差別化要因として機能

2.4.2 インターネットを利用したワン・ツー・ワン取引における個人情報の活用に利用目的制限を課した場合の実ビジネスへの影響

2.4.2.1 一般収集情報について

情報収集時の本人「同意」の取得について、わが国の一般的な商慣行からしても、妥当なレベルで本人「同意」の事後取得や本人「同意」の推定規定といった考え方を導入しないと事業活動に支障をきたす恐れが強い。

- プロバイダーへの加入時に受けるＥＣ上の会員制サービスの提供の場合、サービス内容の改善や新サービスメニューの追加を行う場合に当初目的に限定されるのは、現実的でない。（相当程度包括的な目的が認められるべき。）
- グループ企業内で複合的にネット上での個人情報を収集・利用している場合、窓口企業がその利用目的を示し､本人から同意を取り付けただけでは不十分となると、各企業が個別にその個人の同意を取らなければならなくなり、かえって面倒な事態を招来する。
- プロバイダー企業の合併・再編及び会社機能のネット分社化（本体から分離）等があるたびに、その都度、個別の顧客に利用目的の同意を取り直すのは非現実的。

2.4.2.2 付随・特殊情報について

- アクセスログ（前述）からその商品・コンテンツの人気度（ヒット件数）を把握して、結果としてその個人に詳細情報・関連グッズの紹介に及ぶ場合、アクセス毎に利用目的の通知や同意の取得は困難である。
- ネットショッピングしていただいた商品のアフターサービスの情報や修理内容等の情報について、当初の利用目的だけに限定されると逆に顧客に対するサービス低下のおそれあり。

2.4.3　取扱いの透明性を確保する為の手段の在り方

2.4.3.1　消費者側にとっては

- 開示請求権・異議申立権等の基本的な考え方として、個人権利の範囲を明確にして上で、ネット上のアクセス可能手段・方法の明示。
- 同上の権利を行使できるような苦情窓口の設定と窓口責任者の配置。

2.4.3.2　事業者側にとっては

- 取引上不必要な開示請求権の行使等は、アクセス件数の増大につながり、サーバーの本来目的でない負担増につながるため、情報ランク・アクセス可能要件の設定等が必要。
- 消費者ニーズと対策コストを考慮した上での合理的・必要な範囲でのネット上の検索・閲覧・開示プログラムの作成。

2.5　民間分野にも初めて法の網　大綱の”個人情報保護”の課題について

前述の様々な民間からのパブリックコメント・意見等を受けて、情報通信技術（ＩＴ）戦略本部：個人情報保護法制化専門委員会が 2000 年 10 月 11 に内閣に対して、まとめ作業を完了して提出した、「個人情報保護基本法制に関する大綱」（今回の法案のベース）についての課題を検討するものとする。

今回の大綱については、民間分野をも対象にした初めての個人情報保護法という位置付けから様々な課題も内包しているのが実情である。ここで順にその検討すべき点について毎日新聞関連のウェブ掲載記事を見ていく。　＊（　）内は記事・出所ＵＲＬ関連情報。

2.5.1　個人情報保護大綱の決定と通常国会への法案提出の課題

政府の情報通信技術（IT）戦略本部が設置した個人情報保護法制化専門委員会＝園部逸

夫委員長（元最高裁判事）＝は 2000 年 10 月 11 日、最終会合を開き、個人情報保護基本法の下敷きとなる「個人情報保護基本法制に関する大綱」を正式決定した。専門委は同日、IT 戦略本部の本部長を務める森喜朗首相（当時）に報告した。政府は専門委の報告を受け、通常国会への法案の提出、成立を目指すこととなった。民間分野を主対象にした個人情報保護法は初めて、しかし、大綱は一部の規定を報道目的にも適用し、政府の介入の余地を残すなど課題も残った。

大綱は、個人情報を取り扱うすべての者が守るべき規定を示した 5 項目の「基本原則」と、一定の規模以上の個人情報データベースを運用する企業や団体を「個人情報取扱い事業者（仮称）」と位置づけ、事業者が個人情報の開示を求められたり、訂正や利用の停止を求められたりした場合は、これに義務として応じるなど 9 項目の規定「義務等」や、「政府の措置及び施策」などで構成されている。

事業者を監督する主務大臣に対し、苦情・紛争処理に当たり事業者に対して、必要に応じて「報告」を求め、「助言」もしくは「改善の指示」の権限を付与、さらに事業者が改善の指示に従わない場合は、「改善」または「中止」命令を出す権限を与えた。さらに、これらの命令に従わず違反した時には行政罰を科せられる仕組みだ。

一方、大綱づくりでは報道の自由など憲法上の他の権利との調整をどう図るかが大きな焦点となった。この日の大綱では、基本原則の各規定をどう報道の自由に配慮する文言が盛り込まれるかが注目を集めていた。この日最終的に決まった大綱では、この基本原則の趣旨について「公益上必要な活動や正当な事業活動等を制限するものではない。この趣旨は、報道分野における取材活動に伴う個人情報の取扱い等に関しても同様である」などと、法的な拘束力が弱いことを明記した。

また、園部委員長は森首相への報告後、官邸内で会見した。園部委員長は焦点となっている報道の自由との調整について「我が国の歴史、経験を踏まえれば報道の自由の現れとしての活動に行政が事前に直接介入することには慎重であるべきだ」と述べ、事業者の義務などから除外した理由を説明した。しかし大綱では「基本原則」については、「表現の自由にも自ずと限界がある」として適用することになった。

また、園部委員長は「大綱が表現の自由を侵害することにはならないと考えるか」との質問に対し、「表現の自由や学問の自由、宗教など憲法上の自由が侵害されるような法律が作られたり、そうした法律が運用されたりするようなことはないであろう」と述べた。

（.mainichi.co.jp/digital/netfile/archive/200010/11 の記事より引用･一部改変）

2.5.2　報道機関にも「原則」を適用か？

政府の個人情報保護法制化専門委員会（園部逸夫委員長）が 2000 年 9 月 29 日にまとめた、「個人情報保護基本法」の大綱案について、日本新聞協会などが「言論の自由・国民の知る権利に重大な支障をきたす」として言論･報道･学術分野を「基本法」の適用除外とするよう求めていたが、大綱案は取扱事業者に課す「情報の開示」や｢透明性の確保｣など義務規定の一部適用を除外するものの、｢目的｣および｢基本原則｣は適用対象にしている。欧米諸国では、ジャーナリズムや言論・表現活動は除外している。この種の法律の運用が民主主義の根幹にかかわるとの認識からである。

（以下 mainichi.co.jp/digital/netfile/archive/200009/29 の記事より抜粋引用･一部改変）

2.5.2.1　義務規定から報道を除外　個人情報保護法で専門委

前述の様に焦点となっていた報道目的の個人情報の取扱いについては、宗教、学術目的の個人情報とともに報道機関は事業者の義務としての適用を除外された。しかし、努力義務として定めた 5 項目の「基本原則」は、一部の規定で報道に配慮した文言を加えた上で、適用されることになった。日本新聞協会などメディア側は、「法の適用対象外」にすることを求めていたが、大綱案は、これと真っ向から対立する内容となった。

大綱案は、一定規模以上の個人情報を蓄積したデータベースを運用する事業者を「個人情報取扱い事業者」（仮称）と規定。第 3 章「個人情報取扱い事業者（仮称）の義務等」を設け、業務上での利用に関し、利用目的内での個人情報の取得制限や、第三者に対して無断で個人情報を提供することを禁じている。

この第 3 章の規定は、報道目的の個人情報に関しては、適用しないことにした。このため主務大臣が関与する苦情・紛争処理システムの枠外に置かれることになり、「個人情報の保護」を口実にした政府の報道機関への干渉は、一応は回避されることになった。

一方、基本原則が定める「利用目的による制限」「適正な方法による取得」など 5 項目に関しては、報道目的の個人情報を適用除外としなかった。メディア側は「努力目標として掲げるだけでも、権力者の不正を暴く過程で影響を免れない」（日本新聞協会）として基本原則も対象としないことを主張してきた。

しかし大綱案は、5 項目のうち本人からの開示・訂正請求などを内容にした「透明性の確保」について、「公益上の理由を除き」との表現を追加する方向で大綱をまとめる方針で、報道に一定の配慮を示した格好となった。しかし、苦情・紛争処理システムの整備を、自主

的に講じる努力義務としてあえて設けるなど、事実上の義務規定ともとれる内容となっている。

2.5.3 ”個人情報保護”システムを検証

前述の様に、官民両分野を対象にした個人情報保護基本法の下敷きとなる「個人情報保護基本法制に関する大綱案」が大綱としてまとまったのを受けて、ネット上に本人に無断で個人情報が流出したり、名簿を勝手に売買されるなどの事件が相次いでいたのに、これまで規制できなかった民間事業者の情報取扱いにも初めて法の網が被せられることになる。

（以下 mainichi.co.jp/digital/netfile/archive/200010/02 の記事より抜粋引用･一部改変）

2.5.3.1 民間分野を 3 段階で規制

大綱案は、官民両分野に共通した 5 項目の「基本原則」を設けている。旧通産省や旧郵政省が個人情報を取り扱う通信業界、訪問販売業界などの個人情報保護ガイドラインを作成する際に、参考にしている経済協力開発機構（ＯＥＣＤ）が策定した 8 原則をふまえたもの。大綱案ではこの 8 原則を、▽利用目的による制限▽適正な方法による制限▽内容の正確性の確保▽安全保護措置の実施▽透明性の確保に集約した。この原則は個人を含めた「個人情報を取り扱う者」すべてが守らなければならない。この基本原則の下に、特定の民間事業者を対象にした「個人情報取扱い事業者（仮称）の義務等」を定めるとともに、政府が個人情報保護で果たすべき役割を定めている。

これに、医療や電気通信、クレジットカード取引などの信用情報、さらに行政の個人情報など、より保護の必要性が高い分野を規制する個別法が組み合わせられる 3 段階の構造が大綱案の”個人情報保護”だ。個別法は、今後法整備されることになっている。この法律の実効性を担保する仕組みとして、民間事業者に対して苦情・紛争処理機関の自主的な設置を求めるとともに、主務大臣の関与と、命令に従わない場合は、罰則を課すシステムとした。

2.5.3.2 「基本原則」についての議論

前述した様に、大綱案の策定過程では憲法上の他の権利との調整をどう図るかの適用除外が最大の焦点となった。特に「表現・報道の自由を大きく制約する」として、法の対象外を求めるメディア側との考え方の差は、最後まで埋まらなかった。大綱案は、報道、宗教、学術目的の個人情報の取扱いに関しては、一定規模以上の個人情報データベースを運用す

る事業者の義務などを定めた規定から除外することにしたものの、「基本原則」は適用することになった。

基本原則をめぐる論点の一つは、各規定がどの程度の法的な拘束力を持つかだった。具体的には、基本原則違反を根拠に、裁判所に訴えたり、裁判所が違反を認定する際の根拠となる高い「規範性」を認めるかどうか、ということになる。規範性が高い、ということになれば、表現の自由との調整がなお求められるが、そうでなければその他の権利との調整の必要性は低くなる、というわけである。

しかし、強い規範性を念頭に、委員長代理の小早川光郎・東大法学部教授や上谷清弁護士（元大阪高等裁判所長官）、西谷剛・横浜国立大学大学院国際社会科学研究科教授らは、5項目のうち本人による情報開示や訂正など本人関与を規定した「透明性の確保」に「公益上の目的の場合などを除き」などの配慮規定を盛り込むことを主張した。これに対して、高橋和之・東大法学部教授や新美育文・明治大学法学部教授らは、いわばすべての国民が基本原則の対象となることや、基本原則違反に対する罰則などの規定を大綱は講じていないことなどから特に配慮規定を設ける必要のない考えを述べていた。

園部委員長は「基本原則の法的拘束力はあまり強くない」との認識を示すものの最終的には、透明性の確保の事項に関しては、配慮規定を置くことになった。法案化作業を行うことになる内閣内政審議室は「基本原則違反を根拠に訴訟を提起することは難しいだろうが、裁判官が事案を判断する際の参考にする程度の規範性は有していると考えている」と位置づけているが、そのイメージは固まっていない。いずれにしろ、メディアに限らず国民一人一人がかかわることになる重要な内容だけに十分な議論は必要となる。

2.5.3.3　開示・訂正請求への対応を義務化

大綱案は、民間事業者が守るべきさまざまな規定を定めている。大綱は、民間事業者のうち電子計算機を用いて個人情報を検索することができるデータベースを運用する事業者を「個人情報取扱い事業者」（仮称）と規定し、さまざまな義務を課した。ただし「小規模」なデータベースは権利侵害の程度が小さいことを考慮して除外されている。「小規模」の程度に関しては法案化作業の中で今後決められることになる。

本人の個人情報を開示させ、誤っていれば訂正を求められる「開示・訂正請求権」、中でも関心の高い項目だ。大綱案は「本人からの求め」に対して開示したり、訂正することは事業者の義務と規定した。しかし、「正当な利益を害するおそれ」や「業務の適正な実施に支障」がある場合は応じないでもいいことになっている。ただし、応じない理由の明示

や説明を事業者の努力義務として、実効性を担保した。

開示するかどうかは、第一義的には事業者自身が判断することになるため、適正な運用が期待できないケースも予想される。大綱案では業界団体や政府が定めるガイドラインを活用し、客観性を明確にすることを求めている。

2.5.3.4　苦情・紛争処理システムの整備

大綱案の特徴の一つは、個人情報の保護をめぐる苦情の受付や紛争を処理するための救済システム整備を事業者の努力義務として法的に求めた点にある。この苦情処理システムが機能せずに本人に対する権利の侵害が放置された場合には、事業者による義務規定違反を根拠に行政が解決に乗り出す仕組みとなっている。現行の裁判制度では、多額の訴訟費用や判決までに長期間を要するなどの弊害があり、「救済機関として十分機能していない」との認識から盛り込まれた。ただし大綱案では、行政改革の流れを受け、公正取引委員会のような独立した紛争処理機関を設けることは提起していないが、「将来的に検討すべき課題である」と指摘した。

大綱案は、こうした苦情処理システムの実効性を確保できる仕組みとして、罰則規定も設けている。罰則に関しては、関係省庁だけでなく、民間事業者や消費者からの要望が強かった規定の一つだ。具体的には、本人に無断で第三者に個人情報を提供するなど悪質なケースを念頭に、業界を監督する主務大臣に対して「改善・中止命令」を付与した。さらに一歩、踏み込んだ「改善命令」を発し、それが守られない場合について罰則を適用することにした。この仕組みは、個人情報や権利侵害の内容で処罰することは一般法では困難であることから命令違反に対する処罰として設けた。さらに、大綱案は個別法ではより具体的な被害の実態にあった罰則制度の導入を求めた。

2.5.3.5　行政への規制に対する大綱案の課題

専門委員会では、行政機関が所有する個人情報の保護に関する議論は、ほとんど行われなかった。大綱案でも「政府の措置及び施策」の中で、「本基本法制の趣旨にのっとり、別に法制上の措置を講ずるものとすること」と言及しているだけだ。特に今回の法制化のきっかけとなった、すべての国民に 11 ケタの住民コード（番号）を付与する「改正住民基本台帳法」（1999 年 8 月成立）については触れられなかった。

わずかに触れたのは、行政部門を対象にした現行の「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」に関してだけである。大綱案の解説文の中で、その見直しを求めた。同法には施行（1988 年）後、5 年後の見直しが規定されているが、これ

まで先送りされていた。大綱案は論点として、同法が対象としていない「マニュアル情報」の取扱いや適用除外となっている個人情報、さらに開示・訂正請求の手続きを挙げた。しかし、見直し時期は「速やかに」とするだけで具体的に明示しなかった。ある有力委員は「行政機関の個人情報の取扱いは、民間に比べればきちんと対応してくれる」と「官」にはやや甘い評価との評価もあり、民間分野への規制が目立つ大綱案となったとの意見も一部にはある。

2.6　個別法の検討とその他課題について

今まで述べてきた包括的・全体的な基本法制の枠組みに関する課題とは別に、以前の法制化検討組織である「個人情報保護部会」時からの課題である「個別法の検討とその他課題」について見ていくものとする。とくに今回はそのなかでも、個別分野課題の検討が進んでいる「電気通信分野」・「個人信用分野」・「医療分野」の3分野について順に検討していく。

2.7　電気通信分野について

まず、最初に従来からもコンピュータ・ネットワーク関連分野の個人情報のうち、特にその保護の必要性が叫ばれて久しい電気通信分野については、一般的な基本法制だけでは充分にカバーしきれない特殊性がある。この分野については個別法の検討が必要な理由がここにある。参考として、その特殊性についての記述が詳しい旧郵政省電気通信局からの関連報告書・資料を以下に見ていくものとする。

2.7.1　電気通信分野における個人情報保護の現状

以下「電気通信分野における個人情報保護法制のあり方に関する研究会中間報告書」（抜粋編・一部改変）よりこの分野における保護の現状を見ていく。

2.7.1.1　法制度

(1) 通信の秘密

通信の秘密は、憲法第 21 条第 2 項により基本的人権の一つとして保障され、電気通信事業法は、これを受けて、電気通信事業者の取扱中に係る通信の秘密の保護を規定している。その趣旨は、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、思想表現の自由の保障を実効あらしめ、自由闊達

な通信がなされることを保障することにある。

① 「通信の秘密」（第 4 条第 1 項）

通信の秘密とは、通信の内容にとどまらず、通信当事者の住所、氏名、発信場所等通信の構成要素や通信回数等の通信の存在の事実の有無を含む概念であり、個人にかかわる通信の秘密は、個人識別情報としての当該通信当事者の個人情報に包摂される。

通信の秘密を侵す行為は、処罰の対象となり（第 104 条第 1 項）、電気通信事業に従事する者に対しては、特に罰則が加重されている（同条第 2 項）。ここに「通信の秘密を侵す」とは、通信当事者以外の第三者が積極的意思をもって「知得」しようとすることのほか、第三者にとどまっている秘密をその者が「漏洩」（他人の知り得る状態にすること）すること、及び、「窃用」（本人の意思に反して自己又は他人の利益のために用いること）することを含むと解されている。

また、電気通信事業者の従業員等が、その業務に関して通信の秘密を侵した場合には、当該電気通信事業者も罰金刑の対象となる（第 112 条）。

② 「通信に関して知り得た他人の秘密」（第 4 条第 2 項）

通信に関して知り得た他人の秘密とは、「通信の秘密」のほか、通信当事者の人相、言葉の訛やプッシュホンに記憶された相手番号等、直接の通信の構成要素とは言えないが、それを推知させ得るものを意味する。これは、通信の秘密を含み、当該通信当事者の個人情報に包摂される。電気通信事業に従事する者は、通信に関して知り得た他人の秘密を「守らなければならない」とされ、その「漏洩」及び「窃用」が禁じられる。禁止行為の態様として、「知得」行為が含まれていないのは、電気通信事業に従事する者は、業務上、「通信の秘密」を含め、通信に関する他人の秘密を積極的に知得することが当然予想されるところ、これらの業務上の正当な行為としての知得行為は、第 4 条第 2 項及び第 1 項の違反とならず、その後これを第三者に漏洩し、又は窃用することがこれらの規定の違反となることを明確にするとの趣旨によるものである。

また、通信の秘密に該当する部分を除き、上記の禁止行為について罰則はないが、このような規定が設けられたのは、他人の通信を取り扱う電気通信事業の公共性に鑑み、その職務に従事する者には、訓示的にせよ、より幅広い義務を課して、通信の秘密の保護に万全を期したものと解されている。

(2) その他の法制度

以上のとおり、電気通信事業者が取り扱う個人情報のうち、「通信の秘密」については罰則を伴う保護規定が、それ以外の「通信に関して知り得た他人の秘密」については罰則を伴わない保護規定が、それぞれ定められているが、これらを除く個人情報一般の保護に関しては、何ら法整備がなされていないのが現状である。現行法下においても、例えば、日本電信電話株式会社（以下「ＮＴＴ」という。）の従業員等が、顧客の個人情報を漏洩する見返りとして金銭等を受領していた場合には、日本電信電話株式会社等に関する法律（以下「ＮＴＴ法」という。）第 19 条が定める収賄罪、個人情報が記録された用紙やフロッピーディスク等の有体物を盗み出すなどの行為については窃盗罪（刑法第 235 条）ないし横領罪（同法第 252・第 253 条）、会社の社員等がその任務に違背して自己若しくは第三者の利益を図り又は本人に損害を加える目的で個人情報の漏洩行為等を行い、これにより会社に財産上の損害を与えたときには背任罪（同法第 247 条）、コンピュータに対する不正アクセスの手段を用いた個人情報の漏洩等についてはその手段につき不正アクセス行為の禁止等に関する法律（一部を除き 2000 年 2 月施行。以下「不正アクセス禁止法」という。）の不正アクセス行為の罪（第 3 条・第 8 条）の適用の余地をそれぞれ考えることができるが、いずれも個人情報の保護を直接の目的とした規定ではなく、これらによりカバーできる範囲は極めて狭い。

2.7.1.2　電気通信分野における個人情報保護に関する個別法法制化の必要

電気通信分野においては、電気通信事業そのものの公共性に加え、通信の秘密というこの分野に特徴的な事項も含めた個人情報保護が図られる事に対するニーズは大きなものがあり、前述の様に、昨今マスコミ等で取り上げられる問題事例の発生でも、この分野が大きな比重を占めていることから見ても法制化に対する国民の期待は大きい。

2.7.1.3　ガイドラインの有用性とその限界

個人情報保護ガイドラインは、「この法律は、電気通信事業の公共性に鑑み、その運営を適正かつ合理的なものとすることにより、電気通信役務の円滑な提供を確保するとともにその利用者の利益を保護し、もって電気通信の健全な発達及び国民の利便の確保を図り、公共の福祉を増進することを目的とする。」と規定する電気通信事業法第 1 条の趣旨に基づき制定されたものであり、まさに、電気通信の健全な発達及び国民の利便の確保を図ることをその目的とするものである。

このようなガイドラインによる保護措置は、電気通信分野の業務実態に即した迅速かつ柔軟な対応が可能であることや、規制の遵守等の監視・管理にかかわる行政コストが小さいことなど、積極的に評価すべき面は大きい。

しかしながら、他方で、ガイドラインの実効性を巡っては、ガイドラインはそもそも自主規制の準則となるべき指針であり、これに違反する行為の是正についても自主規制の枠組みでの対応に委ねられており、その性質上、ガイドライン遵守のための強制力がないという問題点が指摘されている。電気通信事業者の保有する個人情報漏洩の事案が相次ぐ現状を踏まえ、こうした指摘を謙虚に受け止める必要がある。

そもそも、ガイドラインの遵守について自覚と意識に乏しい事業者に対し、これが有効な規律となり得ないことは当然であるし、業界団体に加盟していない事業者に対しても、業界団体としてのガイドラインの継続的周知活動に触れる機会が少ないため、どうしても有効な規律が及ばないという問題もある。

なお、ガイドラインが有効に機能するためには、ガイドラインに反する問題事例の発生に対して、速やかに対応策が講じられることが不可欠であるが、問題事例における各社の対応の過程では、法的に違法とされていない行為に関しどこまで強硬な社内調査が可能なのかというジレンマもあり、事実関係や発生原因について社内的に有効な調査を行うことが必ずしも容易ではないという現状も明らかとなっている。

2.7.1.4　諸外国等における法整備の進展

諸外国等においても個人情報保護に関する法整備が進められてきている。1995 年に採択された「個人データの処理に係る個人の保護及びその自由な流通に関する欧州議会及びＥＵ理事会指令」（以下「ＥＵ「個人データ保護指令」」という。）においては、個人データに対する十分なレベルの保護が確保されていない第三国に対し、そのデータの移転を禁止する旨が定められており、このような状況を踏まえ、諸外国における個人情報保護に関する法整備は更に促進されている。先進諸国における電気通信分野の個人情報保護にかかわる法制の概要は次の通りである。

(1) アメリカ「1996 年電気通信法」

連邦行政機関における個人情報保護一般について、1974 年プライバシー法が制定されているが、電気通信分野における顧客のプライバシー保護を図るため、1996 年電気通信法により、電気通信事業者が保有する顧客情報の取扱いに関する規定が設けられ、1934 年通信法（合衆国法典第 47 編）に第 222 条が追加された。ここでは、電気通信

事業者の守秘義務、サービスの提供上知り得た情報の利用制限、顧客のアクセス権、集計顧客情報の取扱い、加入者リスト情報の取扱い等について規定されている。なお、これらの規定に対する違反行為には罰則が定められている。

(2) ＥＵ「電気通信個人データ保護指令」

デジタル技術の公衆電気通信ネットワークへの導入により、利用者の個人データやプライバシーに関する特別要件を求める声が高まっていることを背景に、1997年12月、「電気通信分野における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の指令」（以下「ＥＵ「電気通信個人データ保護指令」」という。）が採択された。これは、ＥＵ「個人データ保護指令」を具体化し補完するものとして、通信の秘密の保護、トラヒック・データ及び課金データの取扱い、通話明細、電話番号情報等の取扱いについて規定されている。

(3) イギリス「1999年電気通信（データ保護及びプライバシー）規則」

貿易産業省（ＤＴＩ）は、ＥＵ「電気通信個人データ保護指令」をイギリス国内で実施するため、1999年、法律としての効力を有する「電気通信（データ保護及びプライバシー）規則」を策定した。同規則では、トラヒック・データ及び課金データの取扱い、電話番号情報の取扱い、通話明細、発信電話番号通知サービスの提供のための条件等について規定されている。なお、個人情報保護に関する一般法である1999年データ保護法には、違反行為に対する罰則が定められている。

(4) ドイツ「電気通信事業者データ保護令（ＴＤＳＶ）」

1996年に制定された電気通信法第89条において、連邦政府は、ドイツ議会の承認を得た上で、電気通信にかかわる個人データの保護に関し、法的効力を有する令を制定することとされているのを受け、同年6月、電気通信事業者データ保護令を制定した。同保護令では、通信履歴の収集・処理・利用制限、発信電話番号通知サービス提供のための条件、電話番号情報の取扱い等について規定されている。なお、個人情報保護に関する一般法である「データ保護法（ＢＤＳＧ）」には、違反行為に対する罰則が定められている。

(5) フランス「電気通信規制法及び関連デクレ（政令）」

1996年の電気通信規制法及び関連デクレ（政令）において、ＥＵ「電気通信個人データ保護指令」に定められた事項が規定された。特に、1996年デクレ第96－1175号において、通信内容の秘密の保護、電話番号情報の取扱い、発信電話番号通知サービス

提供のための条件、その他データの収集・利用・外部提供に関する事項が規定されている。なお、個人情報保護に関する一般法である「情報処理、ファイル及び個人の諸自由に関する法律」に対する違反行為は、刑法により処罰される。

2.7.2　電気通信分野における「個別法」の制定に向けた取組み

個人情報保護に関する「基本法」の検討状況にも十分配意しながら、電気通信分野における「個別法」策定に向けて検討を進め、「基本法」と同時期の法案の国会提出を目指す方向で検討された。（以下：第３回個人情報保護法制化委員会資料「電気通信分野における個別法の検討状況」旧郵政省版より抜粋･一部改変）

2.7.2.1　「個別法」策定に当たっての基本的な観点

- 従来のガイドラインに基づく自主規制の運用実態を踏まえ、実効性ある個人情報保護のシステムを構築する。
- ネットワーク社会における電子商取引の発展等を促進するためには、情報の自由な流通が不可欠であることから､利用面の有用性にも配意した個人情報保護の在り方を検討する。
- 「基本法」に規定される内容等との整合性を図る。
- 他分野における個人情報保護の状況との整合性にも配慮する。
- 電気通信事業者等の個人情報保護に向けての自主的な取組みについて、法制を補完するものと位置付け、引き続きその促進に努める。

2.7.3　電気通信分野「個別法」のイメージについて

2.7.3.1　個人情報保護の目的

個人情報の保護は、個人の尊厳という価値に根ざした重要な要請であり、また、電気通信事業の公共性に鑑み、電気通信分野における個人情報を保護することは、電気通信サービスの利用者の保護、ひいては電気通信事業の健全な発達、公共の福祉の増進にも資する。

2.7.3.2　個人情報保護の必要性

1. 近時相次ぐ問題事例の発生が示しているように、強制力を伴わないガイドラインの実効性には疑問を呈する声が強まっており、法的な規制を求める意見も多数にのぼっている。また、現在の法制の下では、「通信の秘密」以外の個人情報を保護する規定はなく、「通信の秘密」に含まれる事項か否かで大きく異なる結果が導かれる

が、実際上その区分が明確でない場合もあり、このような法制の在り方の合理性も問われている。

2. こうしたことなどからすると、電気通信事業者が保有する個人情報保護の在り方について、従来の枠組みにとらわれず、より良いシステムの構築を目指すという観点から、法制化に向けた検討を行う必要がある。

2.7.3.3 個人情報保護の法制化の方向性

(1) 電気通信分野において保護すべき個人情報の範囲

電気通信事業者が保有する電気通信サービスの利用者（加入契約者のみならず、その通信の相手方、加入契約に係る端末を利用するもの等も含む）に関する個人情報を全て保護の対象とし、電子計算機処理に係るもの等の条件による限定は不要と考えられるが、なお、電気通信事業者が保有する個人情報の実態や他分野とのバランス等も考慮しつつ、検討を行う必要がある。

(2) 個人情報保護の原則

電気通信分野における個人情報保護の原則は、ＯＥＣＤ8 原則に基づく「電気通信事業における個人情報保護に関するガイドライン」の諸原則（①個人情報の収集、②利用及び提供、③適正管理、④開示及び訂正等、⑤責任の明確化）に従うのが適当である。

(3) 個人情報保護のための規制手法

① 個人情報の不正な漏洩等を行う個人（行為者）に対する規制

A. 罰則により保護すべき個人情報の範囲

従来の立法例では、個人情報のうち、罰則により保護すべき個人情報の範囲は「秘密」として整理され、「秘密」を漏洩する行為等が罰則の対象とされている。

電気通信分野においても、このような「秘密」に相当する個人情報を罰則により保護するのが適当であると考えられるが、さらに広い範囲に罰則の網をかけようとする場合には、合理的に構成要件を画定する必要があり、こうした従来の立法例との整合性を図る必要があること、他分野とのバランスにも配慮する必要があること等を踏まえつつ、なお検討が必要である。

B. 罰則による規制の対象となる者の範囲

特に携帯電話事業者の場合には、顧客の個人情報を取り扱う業務を広く代理店に業務委託している実態があり、実効性確保の観点からは、こうした業務委託先の業務に従事する者に対しても規制の対象とすることが適当であるが、法制的にどのよう

な規定が考えられるかは、さらに検討を要する。

C. 第三者が個人情報を不正に入手する行為に対する規制

第三者が、電気通信事業者の従業員等とともに、あるいはこれをそそのかすなどして不正に個人情報を入手する行為等については、当該従業員等に犯罪が成立する限りにおいて、当該第三者にも共犯規定の適用が可能である。

それ以上に第三者に対する独立の処罰規定を設けることについては、情報一般が保護の対象とされていない現行法下においては、困難な問題がある。

② 電気通信事業者に対する規制

電気通信事業者に対しては、個人情報の適正管理義務を負わせた上で、郵政大臣がその具体的な「指針」を定めるとともに、必要な場合には、郵政大臣が指導・助言、さらには業務改善命令を行うことができることとし、この命令に対する違反には罰則を科するというスキームが考えられる。

なお、電気通信事業者の従業員等が前記で処罰される場合には、これに両罰規定を設けることにより、当該電気通信事業者も罰則の対象となる。

③ 届出・登録制度について

届出・登録制度を導入しても、届出・登録にかかわる個人情報の全てを罰則の対象とすることは、前記の検討を踏まえると困難であり、必ずしも罰則を設ける際の構成要件の明確化にはつながらない。

なお、電気通信分野においては、事業そのものに関し、第一種電気通信事業者に対しては許可制、第二種電気通信事業者に対しては登録又は届出制が採用されており、また、情報主体にとって、自らサービスを利用し自己の個人情報が蓄積されている電気通信事業者の所在等は特に紛れがない。 したがって、電気通信分野への届出・登録制度の導入は、積極的な意義に乏しい。

2.8 個人信用分野

次に個別法検討分野の 2 番目として、個人信用情報保護・利用の在り方について、実務的な立場も踏まえて、具体的に金融審議会や産業構造審議会等で行われた検討についての整理内容を見て行く。

2.8.1 「個人信用情報保護・利用の在り方について」

●個人信用情報保護・利用の在り方に関する論点・意見の中間的な整理

（以下旧大蔵省・金融審議会、旧通産省・産業構造審議会、割賦販売審議会：個人信用情報保護・利用の在り方に関する作業部会作成資料 1999 年 7 月 6 日：より抜粋・一部改変）

2.8.1.1　検討の背景

近年、一部の与信業者や信用情報機関からの情報漏洩が社会問題化しているが、わが国の民間部門における個人信用情報を含む個人情報の個別保護法制は未整備の状況にある。また、顧客の返済能力を判断するために与信業者が収集・蓄積・利用している情報（個人信用情報）に関しては、多重債務問題解決等の観点から、業態ごとに設置されている信用情報機関相互間での情報交流の推進が必要ではないかとの指摘もなされている。

こうした問題を背景に、1997 年 4 月、旧大蔵省・旧通産省共同の「個人信用情報保護・利用の在り方に関する懇談会」が設置された。同懇談会が 1998 年 6 月に取りまとめた報告書では、個人信用情報保護・利用に関する制度整備の必要性が提言される一方、「今後、学界、関係業界、消費者保護団体、関係省庁等によって、新法整備の方向性を念頭に置きつつ、各業法、刑事法、民事法との関係等の法律面や情報システムの開発等の技術面、民間における自主ルール等を含めた多様な観点から検討が行われることを期待したい、また、法的措置のタイミングにかかわらず、新たな研究会などを設け、更に検討していくことが必要」とされている。

具体的な措置に向けて掘り下げた議論を行っていくためには、消費者、与信業者及び信用情報機関等の実態を十分に踏まえることが重要である。こうした観点から、旧大蔵省・金融審議会並びに旧通産省・産業構造審議会、割賦販売審議会では、1999 年 1 月、学識経験者のほか、弁護士、消費者団体関係者、マスコミ関係者に加え、金融機関、貸金業者、信販業者及びクレジット業者等実務者をメンバーとする「個人信用情報保護・利用の在り方に関する作業部会」を設置し、法的整備を含めた具体的な制度整備の在り方について検討した。

2.8.2　これまでの検討状況

(1) 法制化について

①　個人情報の中での位置づけについて

個人信用情報保護の法制化を検討するに当たっては、他の個人情報の保護の在り方

の中での位置づけが問題となると考えられる。

懇談会報告書では、個人信用情報は与信時に半ば強制的に提供を求められ、その内容も個人の信用力を判断するため、個人生活に係る詳細な、かつセンシティブな情報が中心であり、いわゆる与信業者のみが信用情報機関を通じて登録された情報を利用することができ、与信業者間で共有されることが多いほか、情報のもつ経済的な価値が大きいため、実際に情報の不正入手・目的外利用の事件が発生している、とし、他の個人情報に先駆けて措置する可能性も含め、立法をできるだけ早期に図るべきである、とされている。

本作業部会では、懇談会報告書の基本的認識を踏まえ、個人信用情報保護の法制化を視野に置いた議論を進めていく必要がある、との意見が多く出された。

他方、民間部門の個人情報全般を規制対象とする個人情報一般を保護する法律を立案することが先決である、との意見もあった。

なお、個人情報一般の保護については、法整備を含めたシステムを整えるため、政府の高度情報通信社会推進本部が設置する検討部会において、総合的に検討が進められる予定である。

② 法制化を検討する際の留意点

また、本作業部会では、法制化に当たっての留意点として、

（イ）罰則や行政的な規制は極力拡大しないこととし、民事的なところで広く規制をかけていくべきである。

（ロ）消費者金融業務における新規サービスの展開を阻害するべきではないこと等を考え、現状固定的になりやすい法規制への依存を必要最小限とした上で、与信業者に個人信用情報保護を手厚くするインセンティブが生じるような制度的フレームワークの構築が必要である。

（ハ）多重債務発生の防止や適正与信の観点から必要な個人信用情報の一層の利用促進には十分な個人信用情報保護が前提となるが、保護のための法的措置は過度なものとならないようにすべきである。

（ニ）すでに高いレベルで個人信用情報を保護している業態があることを踏まえ、法制化に当たっては、個人信用情報の収集、管理、提供及び利用等の取扱いに関する実務の現状を十分考慮すべきである。

（ホ）採用する規制手段に応じて保護・規制の対象は異なるはずで、例えば、刑罰

により保護されるべき個人信用情報はかなり絞り込んでよいが、刑罰により保護されるもののみを規制対象とするのでは範囲が狭すぎるといった意見が出された。

(2) 法的な保護・規制の対象となる個人信用情報の範囲について

① 対象範囲について

個人信用情報の保護に当たっては、まず個人信用情報の範囲を明確にすることが必要であると考えられる。与信業者が与信を実施する際には、顧客の氏名、住所のほか収入、借入状況等個人の経済状況に関する情報や、今後の商品の購買予定や趣味等アンケート的な情報を収集している場合がある。

懇談会報告書では、保護の対象となる個人信用情報を、「与信との関連で収集・保有・利用される情報で返済能力・支払能力を判断するための情報」とすることが考えられるとされている。

(3) 個人信用情報の概念について

作業部会では、法的な保護・規制の対象となる個人信用情報の範囲が、法的な整備を図っていく上での基本となる重要事項であることから、意見聴取を精力的に行い、議論を重ねたところである。本論点については、以下のとおりいくつかの考え方が示された。

① 信用情報機関への登録情報等に限定すべきとの意見

返済能力・支払能力の判断に利用する情報の範囲は各社個別の判断で決められており、個人情報一般と個人信用情報との判別も実務上困難であることから、法の実効性を確保するためには、法的な保護・規制の対象を信用情報機関に登録すべき情報と与信業者が信用情報機関から入手した情報に限定し、その他の情報については当面自主ルールによって保護すべきであるとの意見が出された。

② 与信判断に利用する情報以外も対象とすべきとの意見

一方、消費者のプライバシーに配慮すれば、上記の個人信用情報の定義の範囲を超えて、与信判断に利用する情報以外もできるだけ広く保護・規制の対象とすることが望ましいとの意見が出された。

また、事業者が保有する顧客情報の中で対象範囲を区分するのは困難であるので、まず個人信用情報保護の義務主体となる事業者の範囲を定め、その事業者がもつすべての顧客情報を保護・規制の対象とすべきとの意見も出された。

③ マニュアル情報の扱いについて

法的な保護・規制の対象となる個人信用情報の範囲を定める際の切り口として、マニュアル情報の扱いがある。

懇談会報告書では、マニュアル情報についても、与信業者の過重な負担とならないよう配慮しつつ保護の対象とすべき、とされている。

また、マニュアル情報を法的保護の対象とすることの当否について議論したが、以下のような意見が出された。

A. マニュアル情報を法的保護の対象外とすべきとの意見

マニュアル情報を電算情報と同列に扱うことは実務上負担が大き過ぎるとの指摘があり、マニュアル情報は自主ルールで保護することとし、法的な保護・規制の対象は、電算情報あるいはそれが印字された物とすべきであるとの意見が出された。

B. マニュアル情報も法的保護の対象とすべきとの意見

一方、消費者のプライバシー保護の観点からは、マニュアル情報も電算情報と同様に重要な位置づけにあり、法的な保護・規制の対象に含めるべきとの意見が出された。

(4) 罰則の在り方とその適用範囲について

① 罰則の在り方について

個人信用情報の漏洩事件や外部者からの不正取得が発生していることを考えると、罰則によって保護の実効性を担保していくことも考えられる。

懇談会報告書では、刑罰の適用により個人信用情報の漏洩、不正取得等の抑止を図ることが必要であるが、現状では個人情報一般について、その侵害行為が刑罰の対象とされていないこととのバランスや補充性の原則（他の手段で抑止が可能であれば、まず、それを用い、刑罰は補充的に用いるとの考え方）を考慮する必要があり、刑罰適用による保護の対象もハイリーセンシティブ情報（国籍、信教、政治的見解、保健医療、犯歴等個人の機微に深く関わる情報）や信用判断に直結する情報等重要な情報に限定すべきであるとも考えられるとされている。

作業部会でも、悪意を持った者による情報漏洩、不正入手等に対しては社会的影響から見ても自主ルールでは不十分であることから、情報を保有する主体からの漏洩や不正利用のほか、外部からの不正アクセスには刑罰で対応すべきであるが、その

場合でも、他の個人情報に先駆けて個人信用情報保護のための刑罰を新設するのであれば、罰則の構成要件については厳密にすべきであり、罰則適用の必要性・公平性、明確な適用条件、量刑等について慎重かつ十分な検討が必要である、との意見が出された。また、運用における公平性を確保するため、禁止行為を明確に定めることが望ましいとの意見も出された。

② 行為規制の対象者について

個人信用情報の保護を担保するために罰則を用いるのであれば、行為規制の対象者を明確にする必要があると考えられる。

懇談会報告書では、行為規制の対象者として、業務として個人信用情報を組織的に取扱うものを一般的に取り込むべきとの考え方が大勢であるとされ、具体的には、信用情報機関（業として、加盟している与信業者から個人信用情報を収集し、加盟業者のために利用又は提供を行うもの）、業として与信を行う与信業者（銀行・保険会社等の金融機関、貸金業者、クレジットカード会社、割賦販売業者等）、及びこれらに係わる与信業者に準ずるものとして保証会社、債権回収代行組合等が挙げられている。また、情報の漏洩の防止の観点から、信用情報機関等から情報提供を受けるもの（業務委託先、その他債権譲渡先、グループ企業等）に対して、また、情報の正確性の確保を図る観点から、信用情報機関に情報提供を行うもの（不払い情報を提供する電話会社、通信販売業者等）に対しても一定の行為規制の対象とする必要があろうとされている。

作業部会では、行為規制の対象者として具体的な業態名を挙げるまで議論が及んでいないが、業務として個人信用情報を組織的に取り扱う者すべてとすべきあり、電算処理等の業務委託先についても含めるべきであるとの意見が出された。

③ 罰則の対象となる情報・行為について

罰則を適用していくに当たっては、その対象となる情報・行為についても明確にしておく必要があると考えられる。

懇談会報告書では、前述のとおり、刑罰の対象となる情報について、個人情報一般への侵害行為がすべて刑罰の対象とされているわけではないという現状とのバランスを考慮し、ハイリーセンシティブ情報や与信判断に直結する情報等の重要な情報に限定すべきとされている。また、刑罰の対象となる行為としては、情報保有者による行為として、情報の漏洩、不正提供、不正利用を挙げ、外部のものによる行為

として、窃取、詐欺、強迫その他不正の手段による情報取得が挙げられており、不正取得又は不正提供された情報であると知りつつ情報を入手し、その利用・提供を行うことに対しても措置する必要があるとされている。

作業部会では、刑罰の対象となる情報の範囲について、ハイリーセンシティブ情報や与信判断に直結する情報等の重要な情報に限定すべき、との意見が出された。また、刑罰の対象となる行為について、(イ)個人信用情報を違法な手段で入手する行為、(ロ)守秘義務を負わされている者がそれに違反して悪意をもって個人信用情報を第三者に漏らす行為、(ハ)違法な入手行為や守秘義務違反行為が介在しない限り出てくるはずのない個人信用情報をそれとわかって入手する行為、及び(ニ)個人信用情報システムの外部者が詐取、詐欺、強迫等によって不正に取得する行為等とすべきとの意見が出された。

④　両罰規定について

情報保有者による不正行為を抑止するためには、両罰規定が必要な場合があると考えられる。

懇談会報告書では、情報保有者による不正行為があった場合には、両罰規定によって、法人に対しても刑罰（罰金）を課すことが考えられるとされている。

作業部会では、両罰規定を「組織的な犯罪」や「重大な管理・監督を怠った場合」等に限定すべきである、との意見があった。一方で、「組織的な犯罪」や「重大な管理・監督を怠った場合」等にのみ企業、組織が両罰規定により刑事責任を負うという考え方は狭すぎるのではないか、企業、組織の側に落ち度があるといってよい場合（過失責任が認められる場合）には基本的に刑事責任を免れないとすべきであり、そのために自然人行為者と法人に対する罰金額に差を設けるべきとの意見が出された。

⑤　自主ルールとの関係について

個人信用情報については、法的措置の対象になじむ情報と、自主ルールの対象になじむ情報があると考えられる。

懇談会報告書では、自主ルールについて、個人信用情報の保護・利用のためのルールは、法的措置のほかに自主ルール等において重層的に手当てすることが望ましく、与信業者等は個別業者が収集・保有・利用する個人情報全般を対象に、できるだけ早期に自主ルールの一層の整備を図り、そのルールに則った対応を行っていくこと

が求められるとされている。

作業部会でも、個人信用情報の保護には、法制化になじむ領域と自主ルールになじむ領域が存在することから、自主ルールを拡充して法律との重層的な保護を図る必要がある、との意見が出された。

また、刑罰を含む法整備とあわせて、自主ルールや紛争解決的機能を持つ監視機関の設置も視野に入れた制度作りを進めることが適切である、との意見や、行為規制の内容については、基本原則は法定し、細目に及ぶ具体的な内容は自主ルールで補完するような制度とすべきであるとの意見が出された。

(5) ポジティブ情報の交流について

与信業者が与信を行う際に利用する個人信用情報は、利用者本人による提供のほか、信用情報機関の情報の照会等によって行われているが、ネガティブ情報（延滞、代位弁済、破産といった事故情報）はもとより、ポジティブ情報についても、利用者本人から正確な情報を入手することは困難であると考えられる。

懇談会報告書では、個人信用情報の保護と利用の関係について、信用情報機関間のポジティブ情報の交流は、多重債務問題の軽減や効率的な与信業務につながる効果を持つ一方、与信業者や信用情報機関の負担増、交流を進めた場合の消費者のプライバシーへの影響、漏洩の危険性拡大等の可能性が存在することから、それらを総合的に勘案しながら交流を段階的に進めていくべきであるとされている。

作業部会では、個人信用情報の利用には、社会問題化している多重債務問題の軽減にも一定の効果があると考えられることから、信用情報機関間のポジティブ情報交流の当否について、意見聴取を精力的に行い、議論を重ねたところである。

その際、議論を進める上での視点として、ポジティブ情報の交流を法律で義務づけることの当否を議論するに当たっては、「多重債務問題の解消」の法目的との関係を検討することが必要である、との意見や、多重債務発生防止のためのポジティブ情報交流を制度化する場合には、当該情報を交流される必要性が消費者側に無いにもかかわらず、消費者の財産状況が借入先ではない与信業者や信用情報機関等にまでチェックされるということに対して消費者が抱く不安と公共的な利益との比較衡量が必要であるとの意見が出された。

(6) 消費者に対する与信業者への正確な情報提供の義務づけについて

個人信用情報は、与信業者が与信判断を行う材料であることから、適正な与信を実施

するためには消費者が正確な情報を提供することが求められると考えられる。

懇談会報告書では、消費者にも正確な情報の提供義務を課すべきとの意見があった一方、是非とも与信を受けたいと考えている消費者に正確な情報提供を義務づけ、これに法律的な効果をもたせること（例えば虚偽の申告により与信を受けた借手については、破産の際にも免責を受けられない等）までは困難である、悪質なケースについては詐欺罪等を適用することで対応すべきである、との慎重論があったとされている。

作業部会では、正確な情報提供は適正与信のために不可欠であることから、正確な情報を提供しない消費者は不利益な扱いを受ける仕組みを整備する必要がある（注記）、との意見があった一方、自分に不利益になる事実を相手に正直に告げることを法律が強制できるのは、原理的にはよほど重要な公共的利益の実現にかかわっている場合のみであり、基本的に取引上弱者である借り手側をして取引上の強者に正直に告げることを法が強制するということはありえない発想であり、法制化にはなじまないとの意見が出された。

(注記)　不利益な扱いとして、虚偽の申告により与信を受けた借手について現行法を活用（例えば破産法 366 条の 9 の免責不許可事由の周知徹底）していくほか、虚偽の情報提供によって与信を受けた場合には、破産手続上不利益に取扱うことも考えられるとの意見が出された。

また、消費者に正確な情報提供を義務づける前に、与信業者や信用情報機関が、内部の情報管理、本人情報の取扱いに関して消費者への周知を図るよう努力することで消費者の自覚を促すとともに、消費者・事業者間の信頼関係を構築していくことの方が先決ではないかとの意見も出された。

これに対し、一部には、消費者からの正確な情報提供は与信業者にとって極めて重要であり、これを法的に義務づけることは意義がある（ただしその場合でも、義務づける情報の範囲は個人を特定する項目など必要最小限に止め、消費者教育を徹底すること等が必要）との意見があった。

2.8.3　今後の検討課題

今後は、こうした前述の論点のほか、これまで十分議論が及んでいない下記のポイントも合わせて要検討課題としていくものとする。

- 法的措置の対象とするのが適当な個人信用情報の範囲と自主ルールの対象とす

るのが適当な範囲の整理

- 誤情報を訂正する権利等情報主体の権利
- 情報漏洩等の早期発見のための施策
- 民事訴訟手続による救済の在り方
- 行政機関の監督の在り方
- 信用情報機関への加盟与信業者による個人信用情報の登録・照会の在り方
- 信用情報機関の定義や在り方

以上についても検討を深めていく必要があると思われる。

2.9 医療分野

つづいて個別法検討の３つめの分野であるハイリーセンシティブという位置付けの医療分野の個人情報保護について、旧厚生省の検討内容を見ていくものとする。とくにこれからは前述の様に医療ネットワークの拡大進展により、今まではハードコピー上のマニュアルデータであった医療関連情報がデジタル化されてオンライン上を行き交うケースが当たり前となってくる。つまりカルテやレセプトの電子化、それに遠隔地医療の進展等がもたらすインパクトは絶大なだけに、その暗部である

医療情報の漏洩は他分野の情報とは、また違ったアプローチが必要とされている。

以下第 3回個人情報保護法制化専門委員会資料 医療分野における個人情報保護について検討報告」2000 年 2 月 16 日旧厚生省作成より抜粋･一部改変）

2.9.1 基本的考え方

患者に対する適切な診断・治療等を行うためには、医師等の医療従事者が患者等から正確かつ詳細な情報を得ることが不可欠である。 特に近年科学技術の進歩や生活習慣病等の慢性疾患の増加などにより、医療分野における個人情報の範囲は広範囲なものとなってきている。

また、医療現場におけるチーム医療の進展、医療関連サービスの外部委託化の進展、介護サービス等他サービスとの連携、医療分野における情報化の進展等により、個人医療情報が流通する範囲は、医療機関内外において拡大しつつある。

これらの情報の多くは極めて個人的な情報であり、また、その漏洩等が直接的に患者の社会的な評価等に関わるおそれもあるため、個人医療情報については、その保護を一層図っ

ていく必要がある。
しかし、一方で、医学・医術の進歩や公衆衛生の向上及び増進のためには、診断・治療等を通じて得られた個人医療情報を活用して研究等を行い、新たな治療法・医療技術の開発・普及等を進めていくことが不可欠であり、個人医療情報については適正な情報の利活用を図っていく必要がある。

2.9.2　医療分野における個人情報保護の現状

医療分野における個人情報については、主として、刑法及び医療関係法規において、資格又は業務に着目した守秘義務規定を広く設けることにより、その保護を図っているところである。
このほか、民間の取組みとして、日本医師会等が倫理規定等を定め、個人医療情報の保護を図っている。

2.9.2.1　守秘義務規定

守秘義務規定は、個人の秘密の保護を目的とすると同時に、医療関係者が患者の秘密を漏泄するおそれがあれば、患者が安心して情報を提供できなくなり、結果として有効・適切な医療が行われなくなることから、患者の医療関係者に対する信頼を確保することを目的としている。
守秘義務規定は、個人の秘密の保護を目的とすると同時に、医療関係者が患者の秘密を漏泄するおそれがあれば、患者が安心して情報を提供できなくなり、結果として有効・適切な医療が行われなくなることから、患者の医療関係者に対する信頼を確保することを目的としている。

(1) 資格に着目した守秘義務規定

① 刑法

●刑法第 134 条（秘密漏示）

医師、薬剤師、医薬品販売業者、助産婦、弁護士、公証人又はこれらの職にあった者が、正当な理由がないのに、その業務上取り扱ったことについて知り得た人の秘密を漏らしたときは、6 月以下の懲役又は 10 万円以下の罰金に処する。

医師の刑法上の守秘義務規定に関する特別規定

精神保健及び精神障害者福祉に関する法律（第 53 条）

1.精神病院の管理者、指定医、地方精神保健福祉審議会の委員若しくは臨時委員、精神医療審査会の委員若しくは第 47 条第 1 項の規定により都道府県知事等が指定した医師又はこれらの職にあった者が、この法律の規定に基づく職務の執行に関して知り得た人の秘密を正当な理由がなく洩らしたときは、1 年以下の懲役又は 50 万円以下の罰金に処する。

2.（略）

3.このほか、感染症の予防及び感染症の患者に対する医療に関する法律（第 67 条）、麻薬及び向精神薬取締法（第 58 条の 19）に同様の規定がある。

② 個別の資格法上の守秘義務規定

●診療放射線技師法第 29 条（秘密を守る義務）

診療放射線技師は、正当な理由がなく、その業務上知り得た人の秘密を漏らしてはならない。診療放射線技師でなくなった後においても、同様とする（罰則 30 万円以下の罰金）。

●その他

このほか、臨床検査技師、衛生検査技師、理学療法士、作業療法士、視能訓練士、言語聴覚士、臨床工学技士、義肢装具士、救急救命士、歯科衛生士、あん摩マッサージ指圧師、はり師、きゅう師、柔道整復師及び精神保健福祉士について、各資格法に同様の守秘義務規定が置かれている。

(2) 業務の特性に着目した守秘義務規定

① 精神保健医療関係

●精神保健及び精神障害者福祉に関する法律（第 53 条）

1.（略）

2.精神病院の職員又はその職にあった者が、この法律の規定に基づく精神病院の管理者の職務の執行を補助するに際して知り得た人の秘密を正当な理由がなく洩らしたときも、前項と同様とする。

② 感染症医療関係

●感染症の予防及び感染症の患者に対する医療に関する法律 （第 68 条）

感染症の患者であるとの人の秘密を業務上知り得た者が、正当な理由がなくその秘密を漏らしたときは、６ヶ月以下の懲役又は 30 万円以下の罰金に処する。

③ 臓器移植関係

●臓器の移植に関する法律（第 13 条）

前条第 1 項の許可を受けた者（以下「臓器あっせん機関」という。）若しくはその役員若しくは職員又はこれらの者であった者は、正当な理由がなく、業として行う臓器のあっせんに関して職務上知り得た人の秘密を漏らしてはならない（罰則 50 万円以下の罰金）。

●その他、結核予防法、薬事法、医薬品副作用被害救済・研究振興調査機構法、麻薬及び向精神薬取締法、母体保護法、原子爆弾被爆者に対する援護に関する法律、国民健康保険法、社会保険診療報酬支払基金法に同様の規定がある。

(3) その他の関連規定

このほか、医療分野における個人情報の保護については、関係法規において、個人情報の適正な管理、本人等への情報提供等を規定し、その保護を図っているところ。

(4) 個人情報の保護に関するその他の関連規定の例

① 医療法（情報提供、適正管理）

●第 1 条の 4

1. （略）

2. 医師、歯科医師、薬剤師、看護婦その他の医療の担い手は、医療を提供するに当たり、適切な説明を行い、医療を受ける者の理解を得るよう努めなければならない。

●第 21 条

病院は、厚生省令の定めるところにより、次に掲げる人員及び施設を有し、かつ、記録を備えて置かなければならない。ただし、政令の定めるところにより、都道府県知事の許可を受けたときは、この限りでない。

② 医師法（適正管理）

●第 24 条

1. 医師は、診療をしたときは、遅滞なく診療に関する事項を診療録に記載しなければならない。

2. 前項の診療録であって、病院又は診療所に勤務する医師のした診療に関するものは、その病院又は診療所の管理者において、その他の診療に関するものは、その医師において、5 年間これを保存しなければならない。

・　臓器の移植に関する法律（適正管理、情報提供）

●第 10 条

1.　医師は、第 6 条第 2 項の規定による臓器の摘出又は当該臓器を使用した移植術（以下この項において「判定等」という。）を行った場合には、厚生省令で定めるところにより、判定等に関する記録を作成しなければならない。

2.　前項の記録は、病院又は診療に勤務する医師が作成した場合にあっては当該病院又は診療所の管理者が、病院又は診療所に勤務する医師以外の医師が作成した場合にあっては当該医師が、5 年間保存しなければならない。

3.　前項の規定により第 1 項の記録を保存する者は、移植術に使用されるための臓器を提供した遺族その他の厚生省令で定める者から当該記録の閲覧の請求があった場合には、厚生省令で定めるところにより、閲覧を拒むことについて正当な理由がある場合を除き、当該記録のうち個人の権利利益を不当に侵害するおそれがないものとして厚生省令で定めるものを閲覧に供するものとする。

(5) 民間での取組み例

①　日本医師会

「医師の倫理」（1951 年）において、「患者に接するには、慎重なる態度を持して、忍耐と同情の誠を示し、その診療所の一切の秘密は絶対に厳守すべきである。」旨規定する。

また、診療情報の提供については、医師・患者の相互信頼関係を樹立し、治療効果を上げるために極めて重要であるとの考えから、「医師が患者に積極的に診療記録の開示等を含めて懇切な診療情報の説明・提供する」ことを求める「診療情報の提供に関する指針」（1999 年 4 月）を医師の倫理規範として策定するとともに、苦情処理機関として 2000 年 1 月から全都道府県医師会に診療情報に係る相談窓口を設置する。

②　日本薬剤師会

「薬剤師倫理規定」（1968 年）において、「薬剤師は、職務上知り得た患者等の秘密を、正当な理由なく漏らさない」旨規定する。

③　日本看護協会

「看護婦の倫理規定」（1988 年）において、「看護婦は、対象のプライバシーの権利を保護するために、個人に関する情報の秘密を守り、これを他者と共有する場合

については、適切な判断のもとに対応する。」旨規定する。

3 ネット環境整備の為の自主的取組み課題の検討・整理

次に行政側の法制化への取組みと平行して、ＥＣの今後益々の発展のために不可欠であり、民間企業として自主的に取り組まねばならないネット環境整備の為の課題について検討・整理していく。

3.1 オンライン上のプライバシー保護の為の自主的取組みツール（W3C：P3Pプログラム）について

まず、オンライン上のプライバシー保護の為の自主的取組みの代表的ツールとしてW3Cで有名なP3P（Platform for Privacy Preferences）の民間への普及について見ていくものとする。

3.1.1 Microsoftが「Privacy Wizard」でP3Pバックアップ

米国記事（Maria Seminerio, ZDNet/USA）によると、米Microsoftは1999年4月6日、World Wide Web Consortium（W3C）のP3P（Platform for Privacy Preference Project）に基づくオンラインプライバシー保護ツールの利用促進に向けた、新たな標準を後押ししていく姿勢を明らかにした。

米国ワシントンD.C.で開かれたComputers, Freedom and Privacy（CFP）'99のパネルディスカッションに出席したMicrosoftプライバシーイニシアチブ担当ディレクターのSaul Klein氏は、「われわれは、どんなサイトでも簡単に、それぞれのガイドラインに即したプライバシーポリシーを設定できるP3P手法を開発した」と語った。

P3P（Platform for Pravacy Preference Project）を使ったこの新標準は、Microsoftが Electronic Frontier Foundation (EFF) とともに開発したもので、正式認可を求めてW3Cに提出された。Klein氏によればこの新標準は、オンラインプライバシーポリシーの導入プロセスを簡易化する。

P3Pの仕様そのものは、目新しいものではない。W3Cによるこの技術は、インターネットユーザーがWebサイトを訪れた際、そこで開示する個人情報をユーザーが特定できるようにするためのフレームワークを提示する。

だが、P3Pの実際の導入には技術的に困難な作業が伴うため、これまでこの技術は、コンシューマー向けのWebサイトでは普及してこなかった、とMicrosoftとEFFは説明している。MicrosoftとEFFの提案のもとでは、P3P仕様は「Privacy Wizard」と呼ばれるWeb

ベースのツールを介して Web サイトに取り込まれる。Privacy Wizard は、インプリメンテーションプロセスの特定要素を自動化する。

EFF の会長兼エグゼクティブディレクターを務める Tara Lemmey 氏は、ユーザーがプライバシーの範囲を特定し、そしてサイトがプライバシーポリシーを掲載するという、この 2 つの重要なプロセスの促進は、電子商取引の成長と、米政府からの規制圧力の回避のために不可欠なことだとしている。

同氏はこう述べている。「人々の個人情報を収集する Web サイトはすべて、その情報の利用状況について告知する義務を負っている。だがユーザーによる個人情報の管理を可能にしながらも、さまざまな個々のサイトのポリシー条件に準ずるに十分な柔軟性を持ち合わせた、信頼性のあるフレームワークを開発することは、真に挑戦的な作業だ。われわれの提案する標準は、これを実現するための、次なるステップだと考えている。」

3.1.1.1　普及までに「数カ月から数年」

Privacy Wizard は、Microsoft が TRUSTe とともに開発した技術で、今週中に MSN LinkExchange のサイトでリリースされる。

Privacy Wizard によってサイトオペレーターは、P3P 利用のブラウザが自動的に評価できるようなプライバシーポリシーを作ることができるという。ただし Microsoft は、この技術が普及するには、数カ月あるいは数年はかかるだろうとしている。ブラウザアップグレードが必要というのが理由の 1 つだが、P3P 技術の一部について、特許をめぐる争いが絡んでいるせいもあるようだ。今年、シアトルのソフトウェアメーカー、Intermind が P3P 関連の技術について特許を取得している。

Privacy Wizard によって、一般のインターネットユーザーは、電子メールアドレスやオンライン上でのショッピング習慣など、サイトが自分についてどんな種類の情報を欲しがっているかを簡単に見つけることができるようになる。このウィザードを含む Web ブラウザの将来バージョンでは、ユーザーがプライバシーポリシーを持たないサイトを訪れたり、ユーザーが共有を許可していない情報をサイトが収集したりすると、警告が表示されるという。

米議会の Internet Caucus の共同議長を務めた経験のある弁護士、Rick White 氏は、Associated Press に対してこうコメントしている。「今回発表された技術は、おそらく最終的な答えにはならないだろうが、真に前向きなステップではある。これがすべての問題を解決するかどうか分からない。法的手段で解決すべきギャップは残るだろう」

一方、プライバシー擁護組織 Junkbusters の Jason Catelett 会長は、これまで P3P プロジェクトには長い時間がかかっていることから、今後の成功にも障害があるだろうと見ている。

「具体的導入までに数年かかるのなら、それはすべてのユーザーのプライバシー問題を解決するソリューションとは言えない」と同氏。

Microsoft と EFF はまた、電子商取引に対応した、新たな P3P データスキーマを W3C に提出する計画だ。このスキーマには、プライバシーポリシーの公開や、Better Business Bureau などの業界団体が設置した基準に準じたプライバシーの設定など、電子商取引サイトが顧客からの信用を高めるためのガイドライン案が含められている。

3.1.2 Microsoft、次期 Windows「Whistler」に P3P 対応プライバシー保護機能

米 Microsoft が米国時間 2000 年 6 月 21 日に、Windows の次期バージョン（開発コード名は「Whistler」）で「Platform for Privacy Preferences (P3P)」対応のプライバシ保護機能を組み込むと発表した。ニューヨークで開催された World Wide Web Consortium（W3C）の「P3P Interoperability Session」で明らかにしたものである。

Microsoft 社は P3P Interoperability Session の開催中に、消費者と WWW サイト運営者向けのプライバシー保護技術をテストした。2001 年に市場投入する Whistler で P3P 対応を実現する予定である。同社が P3P Interoperability Session で行ったデモの内容は以下の通りである。（bizit2.nikkeibp.co.jp/wcs/usn2/article/20000622 より）

・「Privacy Statement Generator」：WWW サイト運営者にプライバシ・ポリシに関する一連の質問を行い、自動的に Extensible Markup Language (XML)で記述した P3P 準拠のプライバシ・ステートメントを作成するツール。同社のプライバシ・ポリシ作成支援ツール「Privacy Wizard」をベースにしている。Privacy Statement Generator は今年後半に利用可能になる。

・Internet Explorer の P3P 対応機能：消費者のプライバシ・プリファレンスと WWW サイトが提示するプライバシ・ステートメントの比較を行う。P3P 対応の Internet Explorer は Whistler に組み込む。

・P3P 対応の Microsoft Privacy Statement：XML で記述されており、既存の同社プライバシ・ステートメントを Microsoft 社の「Browser Helper Object」、P3P 対応ブラウザやツールで読めるようにする。

P3P は、WWW のサーバとクライアントの間での個人情報の受け渡し方法を定めた仕様。ユーザは個人情報がどのように使われるかを把握でき、その内容に応じて入力する個人情報のレベルを決められる。

3.2　ＯＥＣＤ プライバシー・ポリシー・ジェネレータの概念

オンラインショップ側がプライバシー・ポリシーを作成しようとした場合に、参考となるサンプルとしては、何を基準に作成したら良いかの一つの答えとなるツールがある。それが「ＯＥＣＤ プライバシー・ポリシー・ジェネレータ Ｖｅｒ.1（オンライン「ウィザード」）」である。

これは個人情報保護方針＝プライバシーポリシーの各要件について、その「ＯＥＣＤの保護ガイドライン 8 原則」をベースに、1998 年のオタワでの「プライバシー保護に関する宣言」等を踏まえて、まさにその大元であるＯＥＣＤから出ている自動作成ツールであり、今回はその内容（最新雛型をＥＣＯＭにて和訳）について見ていく。

（以下ＯＥＣＤのホームページに掲載分http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm）

3.2.1　プライバシー･ポリシーを策定し、プライバシー・ステートメントをポスティングする

●理由

インターネットに関する調査では、多くの消費者が電子ビジネスの利用に二の足を踏む 1 つの理由として、個人データのプライバシー保護に不安を覚えることが指摘されている。プライバシー・ポリシーを策定し、そのポリシーについてのステートメントを正確に伝えることは、電子商取引についての公開性および信頼を、Web サイトのユーザーの間に広める重要なステップである。また、ユーザーは、組織に個人情報を委託し、その個人情報を利用して取引する場合に、詳細な情報に基づいて選択できる。

3.2.2　OECD ジェネレーターの背景

OECD プライバシー・ガイドラインとは、効果的なプライバシー保護と自由な個人情報の流れの間でどのように最適のバランスを取るかについて、国際的に形成されたコンセンサスである。公開は、ガイドラインの重要な原則であり、柔軟性を持ち、しかも様々なプライバシー保護手段に対応が可能となる。

電子商取引の世界で、このガイドラインを実施するために、OECD は産業界、プライバシー保護専門家、消費者グループの協力を受けて、OECD プライバシー・ポリシー・ステートメント・ジェネレーターを開発した。このジェネレーターは、OECD の 29 の加盟国から支持されており、ガイドライン準拠に関するガイダンスを提供している。また、組織がプライバシー・ポリシーおよび Web サイトで公開するためのステートメントを作成することを助けるものである。

オンライン上でジェネレーターを自由に入手できることが望ましい。これは、次のことを促進する。

- Web サイトの所有者の間にプライバシー問題についての認識を広める。
- 閲覧する Web サイトのプライバシー・プラクティスについての、ユーザーの認識を高める。
- グローバル・ネットワークおよび電子商取引に対する、ユーザーおよび消費者の信頼を高める。

しかし、OECD ジェネレーターを利用することは、必ずしも、Web サイトが OECD プライバシー・ガイドラインに準拠していることを意味しない。

3.2.3 プライバシー・ポリシー・ステートメント・ジェネレーターの概念

ジェネレーターとは、まず第一に教育用ツールである。

ジェネレーターは、既存の個人データ・プラクティスの内部調査を実施し、プライバシー・ポリシー・ステートメントを作成するためのガイダンスを提供する。また、プライバシー・ポリシーを策定するための専門知識を持つ民間組織へのリンクも備えている。さらに、関連する規則についての情報を提供する政府機関、非政府組織および民間団体へのリンクも用意されている。

ジェネレーターは、質問を利用して個人データ・プラクティスについて学習する。「ヘルプ」の章では、説明の注記および実行のガイダンスについて説明する。該当する場合は、警告フラッグを表示する。回答は、あらかじめフォーマットされているドラフト・ポリシー・ステートメントに送られる。このステートメントが、個人データ・プラクティスおよびポリシーを正確に反映しているか、評価する必要がある。

このようなドラフト・ポリシー・ステートメントが、適切な法律要件あるいは自己規制要件を満たすことを、OECD は保証しないことに注意する必要がある。このステートメント

は、ジェネレーターの質問に対する回答を反映しているに過ぎない。しかし、プライバシー・プラクティスが、どの程度 OECD プライバシー・ガイドラインに準拠しているかを示すことはできる。

3.2.4　OECD ジェネレーターの制限および利用条件

あらゆる民間団体および公的機関は、OECD の Web サイトから、または加盟国あるいはそれ以外の国へのリンクによって、ジェネレーターを自由に入手できる。政府機関あるいは類似組織の Web サイト上のジェネレーターには、該当する国の特殊な国家的要件に準拠させるために考案されたセクションが追加されている場合がある。

OECD は OECD ジェネレーターをユーザーがプライバシー・ポリシーおよびステートメントを作成するさいに有効な情報を得るためのツールとしてつくられた。

ユーザーにはジェネレーター及びジェネレーターで作成するステートメントの内容を適切かつ誠実に取り扱うことが求められる。

ジェネレーターを使用してユーザーがプライバシー・ポリシー及びステートメント作成したからといって、OECD がそこに認証や支持を与えることはないし、またそうすべきでもない。しかし、ユーザーはプライバシー・ポリシーおよびステートメントを作成するにあたって OECD ジェネレーターを使用したということを明示することができる。その場合は下記 URL をリンク先として表記しなくてはならない。

：http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

- プライバシー・ポリシー・ステートメントの作成を最初に読む。
- 質問を開始する。

3.3　プライバシー・ポリシーおよびステートメントの作成

3.3.1　プライバシー・ポリシーを作成する方法

●ステップ 1.　ジェネレーターに含まれている質問に正確に答えるためには、御社の個人データ・プラクティスについて認識する必要がある。したがって、質問に答える前に、現在の御社の個人データについて詳細な内部調査を実施することが重要である。

- 個人データを収集しているか？
- どのような種類の個人データを収集しているか？
- データをどのような方法で収集しているか？ 個人、第三者、公的機関あるいは

政府機関のいずれかからか？ 該当する個人は、個人データが収集されていることを認識しているか？

- どの個人データをどのように収集するかを決定しているのは、組織内の誰か？
- なぜ、個人データを収集するのか？
- 個人データをどのように利用しているか？
- 個人データを収集した後、誰が管理しているか？
- 個人データは第三者に公開されているか？ 公開されているとすれば、それはなぜか？
- 個人データはどのような方法でどこに格納されているか？
- 個人データの収集および利用に適用される標準、ガイドラインおよび規則を定めているか？
- ユーザーは、自分に関する個人データを利用できるか？
- ユーザーが自分の個人データを照会するとどうなるか？ また、その結果にユーザーが満足しない場合はどうなるか？
- 内部調査の実行についての詳しいガイダンスは、SIIA、USCIB、あるいは CSA
- Model Code CAN/CSA-Q830 の Web サイトを参照できる。または、次の Web サイトを参照できる。
- http:///.jipdec.or.jp/security/privacy/index-e.html
- http://www.research.att.com/projects/p3p/propgen
- http://www/the-dma.org
- http://www/truste.org/wizard

●ステップ 2. 現在のデータ・プラクティスを調査した後は、次のことを実行する。

- 個人データの収集および利用に適用される可能性がある、法律あるいは（自己）
- 規制案の概要について調査する必要がある。この点については、政府機関、非政府組織あるいは民間団体から情報を得ることができる場合がある。
- 現在のプラクティスをそのような規則と照らし合わせて調査し、確実に準拠させる必要がある場合は修正することを推奨する。

3.3.2 ジェネレーターによるプライバシー・ポリシー・ステートメントの作成

●ステップ 3. 現在の個人データ・プラクティスを決定し、そのプラクティスを該当する規則要件と照らし合わせて調査した後は、ジェネレーターの質問を実行できる。「ヘルプ」の節では、使用されている用語の説明、OECD プライバシー・ガイドラインに準拠する項目についてのガイダンス、さらに該当する場合は、国、地域あるいは国際的な文書についての追加情報を、提供している。回答する前に説明の注記を読むことが必要である。
できる限り正確に質問に解答した後は、ドラフト・プライバシー・ポリシー・ステートメントが自動的に作成される。この結果、あらかじめフォーマットされた文章が、回答および選択に基づいて表示される。

3.3.3 ドラフト・プライバシー・ポリシー・ステートメントの評価

●ステップ 4. 次に、以下のことを確認する。

- ドラフト・プライバシー・ポリシー・ステートメントが、組織の個人データ・プラクティスを正確に反映している。
- ドラフト・プライバシー・ポリシー・ステートメントが、該当する国、地域および国際的な法律あるいは（自己）規制の概要に準拠している。
- 誤りが修正されており、プライバシー・ステートメントをスムーズに読める。
-

3.3.4 プライバシー・ポリシー・ステートメントの Web サイトへの配置

●ステップ 5. プライバシー・ポリシー・ステートメントが個人データ・プラクティスを正確に反映し、該当する規則に準拠することを確認した後は、ポリシー・ステートメントを利用する方法を検討する必要がある。準拠する規則によっては、ステートメントに対し、ホームページあるいは個人データが収集される場所など、特定のロケーションが必要な場合がある。特定の規則要件が存在しない場合は、ホームページおよびプライバシー・ステートメントとの間、あるいは個人データを収集するページおよびプライバシー・ステートメントとの間にリンクを作成することを検討する必要がある。OECD プライバシー・ガイドラインでは、個人が時間、知識および費用について過度な努力を強いられることなく、個人データ・プラクティスに関する情報にアクセスできることを推奨している。また、ユーザーが、該当するすべての規則を認識できるように、関連する Web サイトへのリンクを作成することが必要である。

注記：いったんプライバシー・ステートメントが公的に掲示されると、プライバシー・ポリシー・ステートメントに準拠しない場合、あるいはそのステートメントが地域の法律に準拠していない場合は、法的に責任を問われる可能性がある。
前述のステップに従えば、確実に、ポリシー・ステートメントにプライバシー・プラクティスを反映させ、あるいは、該当する規則に準拠させることができる。

3.3.5　プライバシー・ポリシー・ステートメントの例

OECD オンライン・プライバシー・ポリシー・ステートメントは、ドラフト OECD ジェネレータを利用して改訂中である。この例は「モデル」ステートメントを目的とするものではない。これは最終的なプライバシー・ステートメントの予想図を示すものに過ぎない。

- OECD ジェネレーターとは何か？
- 制限および利用条件
- 質問の開始

3.4　ログイン

3.4.1　新規ステートメント

下記に示されたステートメント ID をメモしてください。作成したステートメントを修正する際に必要となります。
ステートメントが他人に見られることを防ぐためにパスワードを決めて入力して下さい。
パスワードを決めたらメモしておいてください。作成したステートメントを修正する際に必要になります。

- ステートメント ID:3590
- パスワード：****
- パスワード確認：****

●前に戻る　　次に進む

3.4.2　御社組織および Web サイトについての情報

この情報は御社の HP にアクセスした人が御社を知ることができるように御社のプライバシー・ステートメントの中で公開されます。

3.4.2.1　このプライバシー・ステートメントを作成する御社組織および Web

サイトについての情報

- 組織名：
- 住所：
- 市町村：
- 都道府県：
- 郵便番号：
- 国：
- データ管理者の名前
- 組織の主要業務
- （1 つの欄に 1 つの業務を明記してください）
- Web サイトの URL

●前に戻る　次に進む

3.4.2.2　このステートメントを適用する御社の子会社とその Web サイトについての情報

子会社 1　　子会社 2

- 子会社名：
- 住所：
- 市町村：
- 都道府県：
- 郵便番号：
- 国：
- データ管理者の名前
- 組織の主要業務
- （1 つの欄に 1 つの業務を明記してください）
- Web サイトの URL

●前に戻る　次に進む　プレビュー

3.4.3　ユーザーへの匿名アクセスの提供

3.4.3.1　御社 Web サイトでは、ユーザーが（標準的な HTTP ログ情報など、

システム管理に必要な情報以外に）自分の個人データを開示しないで、ホーム・ページにアクセスし、サイトを閲覧することができますか？

- はい　いいえ

●前に戻る　　次に進む　プレビュー

3.4.4　Web サイトのリンク特性

3.4.4.1　御社 Web サイトでは、ユーザーが他のユーザーと通信したり、あるいは Web サイト経由で他のユーザーもアクセスできるようにデータをポスティングすることができますか？

- はい　いいえ

3.4.4.2　御社 Web サイトでは、ユーザーの個人データを収集するために、第三者の Web サービス・プロバイダー（個人データを収集し広告を配信する企業など）を利用していますか？

- はい　いいえ

(1)　「はい」の場合、第三者の具体的な名称を挙げてください。

1

2

3

- 前に戻る　次に進む プレビュー

3.4.5　情報の自動収集

3.4.5.1　Web サイトでは何らかの理由でクッキーを使用していますか？

- はい　いいえ

3.4.5.2　御社の組織あるいは Web サイトでは、クッキーに個人データを保存したり、クッキーに保存されている非個人情報を特定の個人についての個人データに関連付けていますか？

- はい　いいえ

(1)　回答が「はい」の場合、目的は何ですか？

- Web サイトの技術的管理
- 調査および開発

- **顧客管理**
- **マーケティング**
- **個人データの売買**
- **その他。具体的に説明してください**

1

2

3

3.4.6 データ収集および目的の明確化

御社組織あるいは Web サイトでは、Web サイトのユーザーが御社のサービスを利用する場合に、ユーザーの自発的な意志により、Web サイトのユーザーについての個人データを収集していますか？

- **はい　いいえ**

3.4.6.1 御社組織あるいは Web サイトでは、Web サイトのユーザーについての個人データを、他のソース（公開の記録、公共機関あるいは民間団体など）から収集していますか？

- **はい　いいえ**

● 前に戻る　次に進む プレビュー

質問で御社が個人データの収集を行っていることが示されました。以下の表の当てはまるもの全てをチェックして下さい。

3.4.7 基本的な個人データ/ビジネス情報

- 各ユーザーが自発的意志で提供
- 公開の記録または公共機関から収集
- 民間団体から収集

基本的な個人データ	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
名前	-	-	-	-	-
性別	-	-	-	-	-
住所	-	-	-	-	-
E-Mail アドレス	-	-	-	-	-
電話/ファックス番号	-	-	-	-	-
その他（具体的に）					
ビジネス情報	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
事業主/組織	-	-	-	-	-
肩書き	-	-	-	-	-
住所	-	-	-	-	-
E-Mail アドレス	-	-	-	-	-
電話/ファックス番号	-	-	-	-	-
その他（具体的に）					

3.4.8 その他の個人詳細およびプロファイル・データ

- 各ユーザーが自発的意志で提供
- 公開の記録または公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
個人詳細	-	-	-	-	-
身体の記述	-	-	-	-	-
家族構成	-	-	-	-	-
教育およびスキル	-	-	-	-	-
生活様式または趣味嗜好	-	-	-	-	-
財務の詳細	-	-	-	-	-
その他（具体的に）					

3.4.9　識別子

- 各ユーザーが自発的意志で提供
- 公開の記録または公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
オンライン識別子	-	-	-	-	-
財務識別子	-	-	-	-	-
公共機関の割り当てる識別子	-	-	-	-	-
生物測定識別子	-	-	-	-	-
その他（具体的に）					

3.4.10 特定のデータ

- 各ユーザーが自発的意志で提供
- 公開の記録または公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
人種または民族的な出身	-	-	-	-	-
政治的意見	-	-	-	-	-
宗教的または哲学的信条	-	-	-	-	-
組合員	-	-	-	-	-
健康/医療データ	-	-	-	-	-
性生活	-	-	-	-	-
本人が提起した、または本人に対して提起された民事、刑事訴訟などの警察/司法データ	-	-	-	-	-

● 前に戻る　次に進む　プレビュー

3.4.11 前記以外に、個人データを利用あるいは収集する目的がありますか？

- はい　いいえ

3.4.11.1　5.4.1 回答が「はい」の場合は、個人データを収集あるいは利用するその他の目的を入力してください。(例：弊社では、この他の目的、す

なわち次の目的のために個人データを収集あるいは利用する)

1

2

3

3.4.11.2 御社が、この質問の前述のセクションで示した目的以外のために、個人データを利用する場合、この新しい目的に同意する機会をユーザーに与えていますか？

- はい いいえ

3.4.11.3 ユーザーにこの新しい目的に同意する手段を提供する場合、ユーザーは自分の選択をどのようにして表現することができますか？

- 個人データを収集するサイト上のポイントでボックスをクリックする
- E-Mail を送信する（送信先 E メールアドレス）
- 特定の URL にアクセスする（アクセス先ホームページアドレス）
- 特定の住所に郵便を送る（郵送先住所）
- 特定の電話番号に電話する（電話番号）
- その他（具体的に）

● 前に戻る 次に進む プレビュー

3.4.12 児童のプライバシー

3.4.12.1 御社では、児童の個人データを故意に収集していますか？

- はい いいえ

3.4.12.2 御社が故意に収集している個人データについて、児童のプライバシーを保護するために、特殊な手段を講じていますか？

- はい いいえ

(1) 「はい」の場合、児童のプライバシーを保護するために講じている特殊な手段について説明するために、次の該当するボックス（項目）すべてに印を付けてください。

- 弊社では、保護者が児童の個人データを収集することに同意していることを確認するために、相応の努力をしている。
- 弊社では、社内で使用するための児童の個人データの収集および利用について、同意する場合のオプションを保護者に提供している。

- 弊社では、第三者に公開するための児童の個人データの収集および利用について、同意する場合のオプションを保護者に提供している。
- その他。具体的に入力してください。（弊社のWebサイトで、児童のプライバシーを保護するために、弊社では・・・）

1

2

3

(2) 御社では、児童についての個人データ・プラクティスを説明する情報を、ホームページおよび御社が故意に児童から個人データを収集している場所で、提供していますか？

- はい　いいえ

●前に戻る 次に進む プレビュー

3.4.13 公開およびユーザーによる選択

3.4.13.1 御社 Web サイトあるいは御社組織では、Web サイトのユーザーについての個人データを子会社あるいはその他の組織に公開していますか？

- はい　いいえ

● 前に戻る　次に進む プレビュー

3.4.14 機密保持/セキュリティ

3.4.14.1 御社 Web サイトでは、弊社に個人データを送信する場合に安全な転送方式を利用するオプションをユーザーに提供していますか？

- はい　いいえ

3.4.14.2 御社が、ユーザーに対し、安全な転送方式を利用して送信することを許可しているデータの種類を示してください。該当するチェック・ボックス（項目）をクリックしてください。

- 基本的な個人データ（名前および連絡情報など）
- その他の個人およびプロファイル・データ（身体の記述、レジャー活動など）
- 識別子（クレジット・カードの詳細、Web サイトのパスワードなど）

- 特定の個人データ（人種または民族的な出身、宗教的な信条、医療データなど）
- その他具体的に入力してください。テキスト・ボックスのスクロール。

3.4.14.3 御社 Web サイトでは、御社の管理下にあるユーザーの個人データを、次に示すことから保護するために、セキュリティ・ポリシー、規則あるいは技術的な手段を適切に講じていますか？

(1) 許可されていないアクセス　はい　いいえ

(2) 不適切な利用あるいは公開　はい　いいえ

(3) 許可されていない修正あるいは変更　はい　いいえ

(4) 不法な破棄あるいは偶発損失　はい　いいえ

3.4.14.4 御社の従業員およびデータ処理業者に、ユーザーの個人データの機密保持を尊重する義務を課していますか？

- はい　いいえ

3.4.14.5 御社組織および Web サイトでは、法律その他の規制により要求される場合を除いて、ユーザーの個人データが国および自治体などの機関に公開されないようにしていますか？

- はい　いいえ

●前に戻る 次に進む プレビュー

3.4.15 個人の参加/アクセス

3.4.15.1 ユーザーは、御社が保管している自分のデータを、御社組織あるいは Web サイトから検索できますか？

- はい　いいえ
- ユーザーは、御社の組織あるいは Web サイトが自分についてのデータを保管しているかどうか、どのようにして検索できますか？
- E-Mail を送信する（送信先 E メールアドレス）
- 特定の URL にアクセスする（アクセス先ホームページアドレス）
- 特定の住所に郵便を送る（郵送先住所）
- 特定の電話番号に電話する（電話番号）
- その他（具体的に）

3.4.15.2 ユーザーは、御社が保管している自分についての個人データのコピー

を、わかりやすい形で入手することができますか？

- はい いいえ

3.4.15.3 「はい」の場合、ユーザーは、どのようにして、御社が保管している自分についての個人データのコピーを、わかりやすい形で入手することができますか？

- E-Mail を送信する（送信先 E メールアドレス）
- 特定の URL にアクセスする（アクセス先ホームページアドレス）
- 特定の住所に郵便を送る（郵送先住所）
- 特定の電話番号に電話する（電話番号）
- その他（具体的に）

3.4.15.4 ユーザーがその情報を入手するまでに、通常どれくらいの時間がかかりますか？

- オンラインでほぼ瞬時に
- 1 週間以内
- 1 カ月以内
- それ以上（具体的に）

3.4.15.5 一定の料金を請求しますか？

- はい いいえ

3.4.15.6 料金を入力してください。

3.4.15.7 ユーザーは、御社が保管している自分のデータについて変更を要求できますか？

- はい いいえ

3.4.15.8 要求できる場合、ユーザーは次のどの措置を講じることができますか？（要求が妥当であるとされる場合）

- 消去
- 修正あるいは変更
- 完全化

3.4.15.9 御社では、データの提供を拒否する権利を留保していますか？

- はい いいえ

3.4.15.10 「はい」の場合、御社では、データの提供を拒否する理由をユーザー

に知らせますか？

- **はい　いいえ**

3.4.15.11　**御社がデータの提供を拒否することに対して、ユーザーは異議を申し立てることができますか？**

- **はい　いいえ**

3.4.15.12　**御社では個人データを提供する前に、自己証明を要求しますか？**

- **はい　いいえ**

●前に戻る 次に進む プレビュー

3.4.16 **プライバシー保護の順守**

御社ではどのような手段を用いた個人データの収集も行われていないと示されました。もしこれが御社が情報に関して行っている慣例と異なっている場合は前述の関連質問をもう一度検討してください。これらの質問のうち、一つでも「はい」と回答すれば、質問の全てに回答することができます。

3.4.16.1　**御社の HP もしくは組織は、国内のプライバシー保護法あるいは自己規制制度の適用下にありますか？**

- **はい　いいえ**

(1) **「はい」の場合、御社のプライバシー・ポリシーは適用される国内のプライバシー保護法あるいは自己規制制度に準拠していますか？**

- **はい　いいえ**

(2) **御社のポリシーが準拠している主なプライバシー制度を挙げてください。（それぞれのタイトルおよび国名）**

1

2

3

3.4.16.2　**御社の HP もしくは組織は、国際的なあるいは地域のプライバシー規制制度、または自己規制プライバシーの適用下にありますか？**

- **はい　いいえ**

(1) **「はい」の場合、御社のプライバシー・ポリシーは適用される国際的なあるいは地域のプライバシー規制制度あるいは自己規制プライバシー制度に準拠しています**

か？

(2) 御社のポリシーが準拠している主な国際的なあるいは地域のプライバシー制度、または自己規制制度を挙げてください。（それぞれのタイトルおよび出所）

1

2

3

3.4.16.3 御社のプライバシー・ポリシーが前述の該当する規則を順守していることを示すために、次の手続きを行っていますか？

- 自発的な自己評価手続き
- 自発的な第三者組織の認定
- 政府機関による監督
- 独立データ保護機関による監督

前記で該当するものすべてについて、次の詳細を記入してください。

3.4.16.4 自己評価手続き

- プライバシー・ポリシー担当者あるいはサービスの名前もしくは名称
- URL
- 住所
- 国名

(1) 第三者組織の認定

- 第三者組織の名称
- URL
- 住所
- 国名

(2) 政府機関による監督

- 政府機関の名称
- URL
- 住所
- 国名

(3) 独立データ保護機関による監督

- データ保護機関の名称

- URL
- **住所**
- **国名**
- **はい　いいえ**

3.4.17 プライバシー・サポート

3.4.17.1 Web サイトのユーザーに対する.プライバシー・サポート：御社では、Web サイトのユーザーに対して、プライバシーに関する疑問あるいは問題が発生した場合に、連絡する担当者についての情報を提供していますか？

- **はい　いいえ**

(1) **以下の連絡先（当てはまるものはすべて記入）を記入してください。**

- **名前/名称　　連絡先** 1　　**連絡先** 2
- **部門**
- **住所**
- **電話番号**
- Fax **番号**
- E-Mail **アドレス**
- URL

3.4.17.2 御社では、ユーザーが、問題に対する御社の対応に満足しない場合、その問題を解決する別の手段を推奨していますか？

- **はい　いいえ**

3.4.17.3 御社では、ユーザーの問題を解決するどのような別の手段を推奨していますか？

(1) **御社の組織あるいは HP がユーザーに、御社が収集もしくは私用した特定可能な個人情報に関して第三者組織による調停、和解あるいは仲裁を提供している場合、その第三者組織名および連絡先の詳細を入力してください。**

- **名称：**
- **連絡先（URL など）：**
- **条件（費用など）：**

(2) 該当する政府機関あるいは部門に連絡する。機関あるいは部門名および連絡の詳細を入力してください。

- 名称：
- 連絡先（URL など）

(3) 該当するデータ保護機関に連絡する。機関名および連絡の詳細を入力してください。

- 名称：
- 連絡先（URL など）

(4) その他。具体的に入力してください（ユーザーが、問題に対する御社の対応に満足しない場合、ユーザーが連絡することを推奨している。名前および連絡の詳細を入力してください）。

- 名称：
- 連絡先（URL など）

●前に戻る　次に進む プレビュー

3.5　<ドラフト>　鈴木カンパニーのプライバシー・ステートメント（ステートメント No 3640：インプット結果出力表）

3.5.1　弊社の組織および Web サイトについての情報

近代的な情報および通信技術が、鈴木カンパニーのような組織の業務では基本的な役割を果たします。弊社は日本に本社を置いています。

弊社の主要業務は小売業です。

弊社のプライバシー・ポリシーは鈴木カンパニーに適用され、その Web サイトについての情報は次の通りです。

- 組織名: 鈴木カンパニー（仮名）
- 住所:　霞ヶ関 1-3-1
- 市町村、郵便番号:　千代田区 100-8901
- 都道府県:　東京都
- 国:　日本
- データ管理者の名前：　鈴木孝（仮名）
- Web サイト(複数):

弊社のプライバシー・ポリシーは弊社の子会社にも適用され、その Web サイトについての情報は次の通りです。

3.5.2　ユーザーへの匿名アクセスの提供

ユーザーは自分の個人データを開示しないで、弊社の Web サイトのホーム・ページにアクセスし、サイトを閲覧することができます。

3.5.3　弊社の Web サイトのサービスおよびリンク特性

弊社の Web サイトでは、ユーザーは他のユーザーと通信することも、他のユーザーもアクセスできるように情報をポスティングすることもできません。

弊社の Web サイトには、第三者の Web サービス・プロバイダーへのリンクは含まれていません。

3.5.4　情報の自動収集

弊社の Web サイトでは、クッキーは使用していません。

弊社では、自動的に個人データを保存することも、その他の手段で自動的に保存されている情報を、特定の個人についての個人データに関連付けることもしていません。

3.5.5　データ収集および目的の明確化

弊社では、ユーザーが弊社のサービスをご利用する場合に、ユーザーの自発的な意志により提供される個人データを収集します。

弊社では、ユーザーについての情報を、公開の記録、公共機関あるいは民間団体などのその他のソースからは収集しません。

収集されている個人データの一覧表にアクセスする時に、またそれらのデータを利用する時に、ここをクリックしてください。

弊社では、以下の表に明記されている以外の目的で、個人データを収集することも利用することもありません。

弊社が新しい目的でユーザーの個人データを利用したい場合は、ユーザーにこの新しい目的に同意する手段を提供しています、すなわち、個人データを収集するサイト上のポイントでボックスに表現します。

3.5.6　児童のプライバシー

弊社では、児童から個人データを故意に収集したりしません。

弊社では、弊社に個人データを公開している児童のプライバシーを保護するために、特殊な手段を講じていません。

弊社では、児童についての個人データ・プラクティスを説明する情報を、ホーム・ページおよび弊社が個人データを収集する弊社の Web サイト上の場所では提供していません。

3.5.7　公開およびユーザーによる選択

弊社では、ユーザーの個人データを弊社の子会社にもその他組織にも公開していません。

3.5.8　機密保持/セキュリティ

弊社では、弊社に下記の種類の個人データを送信する場合に、安全な転送方式を利用するオプションをユーザーに提供しています。

- 基本的な個人データ(名前および連絡情報など)

弊社では、弊社の管理下にあるユーザーの個人データを、次に示すことから保護するために、セキュリティ・ポリシー、規則および技術的な手段を講じていません。

- 許可されていないアクセス
- 不適切な利用あるいは公開
- 許可されていない修正
- 不法な放棄あるいは偶発損失

個人データにアクセスし、個人データの処理に関係するすべての弊社の従業員およびデータ処理業者に、ユーザーの個人データの機密保持を尊重する義務を課しています。

弊社では、法律あるいはその他の規則により要求される場合を除いて、ユーザーの個人データが国および自治体などの機関に公開されないようにしています。

3.5.9　弊社が保管しているユーザーについての個人データへのアクセス

ユーザーは、弊社が自分についての個人データを保管しているかどうか、以下の方法で弊社に問い合わせることができます。

- E-Mail を送信する(suzuki-takashi2@meti.go.jp)

弊社では、弊社が保管しているユーザーについての個人データのコピーを、わかりやすい形で提供していません。
弊社では、ユーザーは弊社が保管している自分のデータについて変更を要求することができ、要求が妥当であるとされる場合、ユーザーはデータに次の措置を講じることができます。

- 修正あるいは変更
- 完全化

弊社では、ユーザーに自分の個人データのコピーを提供することを拒否する権利を留保してはいますが、データの提供を拒否する理由を知らせます。

弊社では、しかしながら、ユーザーの個人データのコピーの提供を拒否する決定に対して、ユーザーは異議を申し立てることができます。

3.5.10 プライバシー保護の順守

弊社のプライバシー・ポリシーはプライバシー規則 JIS Q 15001 に準拠しています。
弊社の Web サイトあるいは組織には、国際的なあるいは地域のプライバシー規制制度、または自己プライバシー規制制度は適用されていません。
弊社のプライバシー・ポリシーが前述のプライバシー規則を順守していることを示すために、弊社では、次の手続きを行っています。

- 自発的な第三者組織の認定

3.5.11 第三者組織の認定

3.5.11.1 第三者組織の名称　JIPDAC

- URL　http://www.jipdac.or.jp
- 住所　日本国東京都港区芝公園 4-5-8
- 国名　日本

3.5.12 プライバシー・サポート

弊社のプライバシー・ポリシーに関する疑問あるいは問題が生じた場合は、下記までご連絡ください。

- 連絡先 1
- 名前/名称　　鈴木孝（仮名）
- 部門　　情報プロジェクト室（仮名）
- 住所　　東京都千代田区霞が関 2-3-1
- 電話番号 81-3-4501-2964
- Fax 番号 81-3-4580-6403
- E-Mail アドレス suzuki-takashi2@mieti.go.jp
- URL

弊社では、ユーザーの問題を解決する別の手段を推奨しておりません。

3.5.13 収集している個人データの一覧表およびデータの利用目的

3.5.13.1 基本的な個人データ/ビジネス情報

- 各ユーザーが自発的意志で提供
- 公開の記録あるいは公共機関から収集
- 民間団体から収集

基本的な個人データ	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
名前	-	-	-	X	-
性別	-	-	-	X	-
住所	-	-	-	X	-
E-Mail アドレス	-	-	-	X	-
電話/ファックス番号	-	-	-	X	-
その他（具体的に）					
ビジネス情報	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
事業主/組織	-	-	-	-	-
肩書き	-	-	-	-	-
住所	-	-	-	-	-
E-Mail アドレス	-	-	-	-	-
電話/ファックス番号	-	-	-	-	-
その他（具体的に）					

3.5.13.2 その他の個人詳細およびプロファイル・データ

- 各ユーザーが自発的意志で提供
- 公開の記録あるいは公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
個人詳細	-	-	-	X	-
身体の記述	-	-	-	-	-
家族構成	-	-	-	-	-
教育およびスキル	-	-	-	-	-
生活様式または趣味嗜好	-	-	-	-	-
財務の詳細	-	-	-	-	-
その他（具体的に）					

3.5.13.3 識別子

- 各ユーザーが自発的意志で提供
- 公開の記録あるいは公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
オンライン識別子	-	-	-	X	-
財務識別子	-	-	-	-	-
公共機関の割り当てる識別子	-	-	-	-	-
生物測定識別子	-	-	-	-	-
その他（具体的に）					

3.5.13.4 特定のデータ

- 各ユーザーが自発的意志で提供
- 公開の記録あるいは公共機関から収集
- 民間団体から収集

	Web サイトの技術的管理	調査および開発	顧客管理	マーケティング	個人データの売買
人種または民族的な出身	-	-	-	-	-
政治的意見	-	-	-	-	-
宗教的または哲学的信条	-	-	-	-	-
組合員	-	-	-	-	-
健康/医療データ	-	-	-	-	-
性生活	-	-	-	-	-
本人が提起した、または本人に対して提起された民事、刑事訴訟などの警察/司法データ	-	-	-	-	-

3.6 プライバシーポリシー雛型作成と基本法制の趣旨反映

まず今回の法制化に伴い、消費者側に対して法遵守の立場を明らかにし、具体的に各企業がどのような対応を取らなければならないかについて指針となり、また各企業がサイトに掲載すべきプライバシーポリシーの雛型となるものをＥＣＯＭのＳＷＧが、あるメーカー（製造業）のプロトタイプ案をベースに作成したものを紹介する。

■プライバシーポリシー ガイドライン風）雛型 案）■

ECOM個人情報保護SWG　　2001.1.19

3.6.1 対象となる「個人情報」の定義

3.6.1.1 対象となる「個人情報」とは、お客様である特定個人を識別することが可能な情報

- 個人を識別することが可能な情報とは次のような情報をいう。

  例）氏名、住所、電話番号
- その情報から直接個人を識別できないような情報であっても、上記情報と照らし合わせることによって個人を識別することが可能となり、プライバシーに関わるような場合にはここでいう「個人情報」にあたる。

例）家族構成、年収、学歴、メールアドレス、

- **例えば、メールアドレスは、それ自体では個人を識別することはできないが、当該メールアドレスを利用するお客様は原則として特定の人に限られているので、個人情報に準じた取扱をする。**
- **弊社は次のような「個人情報」は取得、利用、提供しないものとする。**

・思想、信条及び宗教に関する事項

・人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴、その他の社会的差別の原因となる事項

3.6.2 個人情報を取得する場合の留意点

3.6.2.1 お客様から個人情報を取得するときには、適法かつ適切な方法で取得する事を約束

- **弊社が個人情報を取得する場合には、お客様などの情報の主体者が個人情報を取得されることを認識できるような状況、手段によって行なわれることを約束する。**
- **取得の際には、取得し個人情報の利用目的や第三者への提供の有無などを明確にして、これをお客様本人に通知、公表する。**

①　「取得の具体的場面」

アンケート・モニター募集

懸賞・プレゼント募集

各種会員の会員登録

愛用者カードの回収

ユーザー登録カードの回収

保証書の回収

電話、電子メールによる問い合わせ受付

②　「通知、公表しておくべき事項」

利用の目的

例）当社取扱商品、サービスに関する情報提供のため

提供しているサービス向上のため

賞品発送のため

第三者への提供の有無、提供する場合の提供先

自己の個人情報の開示、訂正などに関する連絡先

個人情報を提供しなかった場合に生じる不利益

（一部のサービスが受けられないことなど）

③ 「通知、公表の方法」

本人への直接の通知

例）個人情報登録フォーム等への記載

会員規約などにおける個人情報の取扱いに関する規定

常にアクセスすることができる方法による公表

例）ホームページ上やパンフレットへの記載または問い合わせ窓口におけるお客様本人からの問合せへの回答

④ 「同意を取る方法」

個人情報登録フォーム等への同意欄、同意ボタンの設置

会員規約への同意

3.6.2.2 第三者が取得した個人情報を提供してもらう場合、提供を受けた者は個人情報の利用・管理・提供について個人情報を直接取得した者と同等の責任を負うことを約束

- 個人情報を保有している業者から個人情報の提供を受ける場合には、当該業者が個人情報を弊社（または当該業者以外の第三者）に提供する旨を予め告知等していたのか確認しておくことを約束する。
  告知がなされていない場合、新たな同意を得ることなく個人情報の提供を受け、これを利用等することはしない。
- 第三者が取得した個人情報の提供を受ける場合、その利用は取得の際に告知していた利用目的の範囲内でしか利用しない。
  取得時の利用目的を超えて利用する必要がある場合には、改めてお客様の同意を得ることとする。
- ＜要検討：公になっている個人情報を取得する場合に何らかの制約を受けるのか電話帳に掲載されている。（氏名・電話番号・住所の利用など）＞

3.6.3 個人情報の利用における留意点

3.6.3.1　個人情報は利用の目的を明確にし、その目的の範囲内において取り扱うことを約束

- 取得した個人情報は、お客様に告知した目的を達成するために必要な範囲においてのみ利用し、告知した目的以外に個人情報を利用することはしない。
- なお個人情報の取得時に利用目的を告知していない場合、当該個人情報は通常合理的に考えられる目的のために提供されたものであるとお客様に理解される下記のような目的を超えて利用することはしない。

保証書　・・・品質事故時の対応

アフターケア申込・・・修理依頼への対応、当該修理に関する事後フォロー

電話問合せ・・・問合せへの対応、当該問合せに関する事後フォロー

懸賞募集・・・当選時の賞品発送

① 「取得後の利用目的の変更」

個人情報を取得した後に、通知、公表していた利用目的を原則として変更しない。個人情報を取得した後に利用目的を変更する必要が生じ、その変更が一般的に合理的であると思われる範囲を超えるものである場合には、既に保有している個人情報をそのまま利用はしない。変更後の利用目的をお客様本人に改めて通知するなどの措置をとる。

例）賞品発送のために取得した個人情報を新製品情報の送付に使おうとする場合

② 「利用目的の変更の程度」

＜要検討：提供する情報の性質が変更される場合、取待目的の範囲外となって新たな告知等が必要なのか。：製品Aに関する製品情報の送付一用途等全く異なるB関連商品情報の送付＞

③ 「同一法人内における取得部門以外の部門の利用」

＜要検討：同一法人内において、ある部門が取得した個人情報を他の部門が利用する揚合、取得目的の記載の仕方にもよるが、お客様のような情報主体者が想定しうる部門が利用する限りにおいては取得目的の範囲内と考えることにする。

例）同一企業（法人）内A部門が新商品情報の送付のために取得した個人情報を企業（法人）内B部門が同一の目的で利用する場合。

＜要検討：しかしながら、お客様である情報主体者が想定し得ないような部門が

利用するような場合には、たとえ同一企業（法人）内であっても取得目的の範囲外であると解せられるので、改めてお客様である情報主体者の同意が必要となり、改めて新しい利用目的をお客様本人に通知するなどの措置をとる。このような部門の利用が想定される場合には取得目的に予め盛り込んでおき、告知するようにする。＞

④ **「グループ内における取得会社以外の会社の利用」**

＜要検討：グループ内のある会社が取得した個人情報を他の会社が利用する場合には法人格は別なので形式的には「第三者」に該当するため、取得目的の範囲外となる。その為グループ内の他の会社が利用する可能性がある場合には、その旨を予め取得目的に予め盛り込んでおき、告知しておくことにする。

例）A社が取得した個人情報を同一企業グループ内（別法人）のB社が利用する場合

＜要検討：同一ブランドを扱っている複数会社でひとくくりと評価して構わないかについては「当サイトでご登録いただいた個人情報に基づき、弊社およびその子会社・関係会社より、各社が取り扱っている商品・サービスに関する情報を送付させていただきす。」との告知をしておくものとする。＞

⑤ **「事務処理代行の実施」**

次のような揚合には個人情報の「利用」にはあたらないが、個人情報の保護に必要な管理体制を整えることとする。詳細は個人情報の管理における留意点の項に従うものとする。

個人情報のデータ処理代行

顧客データベースの管理

送付物の発送代行

⑥ **「統計資料等の作成」**

マーケティング分析や統計資料等を作成する場合など、個人が識別・特定できないように加工した上で、利用・提供する場合には、個人情報としての保護の対象から外すものとする。

3.6.4　個人情報の管理における留意点

3.6.4.1　取得した個人情報の内容は、利用目的の達成に必要な範囲において、

正確かつ最新の内容に保つことを約束

- **保有している個人情報が誤っていたり、古いものであったりした場合、これを利用することによって情報の主体者が不利為を受ける恐れがある。**
- **したがって、利用に必要な範囲において、個人情報の正確性を確保するとともに、登録した個人情報の更新を行うことを約束する。**

①　「正確性確保のための仕組み」

個人情報登録時に入力内容確認のための画面の設置

個人情報の登録受付後に登録内容確認のためのメール、登録証などの送付

②　「情報更新のための仕組み」

ホームページ上での登録内容変更のためのページの設置

送付物への同梱等による登録内容の変更手続の通知

本人への定期的な登録内容確認の実施

3.6.4.2　個人情報は、適切な安全保護措置を講じた上で取り扱うことを約束

- **弊社は、個人情報を取り扱っている部門あるいは部署単位で、管理責任者をおき、その管理責任者に適切な管理に努める。**
- **保有している個人情報が、外部に持ち出されるなどして不正に流出することのないよう厳重に管理する。**
- **第三者によるハッキングなどによって個人情報が外部に流出したり、改竄、破壊などされることのないように、コンピュータの不正アクセス対策、ウイルス対策、データのバックアップ体制などを整えておくことをお約束する。**

3.6.5　第三者への提供

3.6.5.1　個人情報を情報の主体者であるお客様に無断で第三者に提供せず

- **取得の目的が第三者への提供である場合あるいは取得した個人情報を第三者への提供の可能性がある場合には、予めその旨および提供先を通知、公表しておくことを約束する。**
- **例）他社と提携して提供しているサービスにおいて個人情報を取得する場合「サービスの向上を図るため、ご提供頂いた個人情報を本サービスの提携先である○○株式会社に提供することがある。」**
- **「当サイトでご登録いただいた傭人情報は当サイトの登録各社に提供され、各**

登録会社から商品情報等の案内が送られることがある。」

- 個人情報の取得代行を行う場合
- 「当サイトのアンケートでご登録いただいた個人情報は、マーケティング調査のために○○株式会社に提供される。」
- 提供は、取得目的の範囲内でのみ行うものとする。
- 提供先は、個人情報の保護への配慮を行っている会社・メンバーに限定する。提供先から個人情報が流出した場合、個人情報を取得し、これを当該提供先に提供した当社の信用も損なわれることとする。
- 提供に際しては、個人情報の取扱いに関する機密保持義務を課すなど必要な契約を締結するなどして、提供先から個人情報が不正に流出する事がないように、必要な保護を図るものとする。
- 「提供」とは、個人情報の利用を目的とする者に情報を開示することや利用させることを指すものとする。
- 取得情報のデータ処理を行わせるために情報処理業者にデータを引き渡す場合には、ここでいう「提供」には該当しないものとする。「外部業者への委託」の項にしたがった取扱いをするものとする。

3.6.6 外部業者への委託

3.6.6.1 個人情報の取扱いを第三者に委託する場合には、委託先の選定に配慮し、必要な監督等を行うことを約束

- 外部の情報処理業者などに個人情報のデータ処理などを委託する場合には、個人情報保護への配慮を行っている業者を選定するものとする。
- 委託に際しては、個人情報の取扱いに関する機密保持義務を課すなど、必要な契約を締結するなどして、委託先から個人情報が不正に流出する事がないように、必要な保護を図るものとする。

例）機密保持契約書や業務委託契約書の締結

- 機密保持規約遵守の誓約書

① 「規定すべき条項」

機密保持義務、目的外利用の禁止

事前に同意のない再委託の禁止

処理終了時の個人情報の返却

- 委託先における個人情報保護の確保を図るために、必要に応じて委託業務の監視、監督を行うものとする。

  例）廃棄処理時の立会い

- 委託先における個人情報の保護体制を定期的に監査するなどして、守秘の徹底を図るものとする。

② 「外部業者への委託が想定される場面」

個人情報の入力業務委託

個人情報を利用するシステムの開発委託・運用委託

取得した個人情報に基づくマーケティング分析などデータ処理の委託一個人情報が記載されている書類、記録媒体等の廃棄処理

3.6.7 公表

3.6.7.1 個人情報を取得する者として、利用目的など一定の事項を公表しておくことを約束

① 個人情報の取得に当たっては、次のような事項を公表

利用目的

個人情報の保有について責任を有する事業者名（部署名）

自己の個人情報の開示、訂正を求める際に必要となる手続

苦情等の受付窓口

個人情報の取扱い方針

② 「公表の方法」

ホームページ上への掲載

愛用者カードやユーザー登録カードとともに同封するパンフレットへの記載

3.6.8 情報の主体者であるお客様からの開示請求などに対する透明性の確保

3.6.8.1 情報の主体者であるお客様から自己の個人情報について開示を求められた揚合には、原則としてこれに応じることを約束。

- 個人情報の取扱いについての透明性を高めるために、情報の主体者であるお客様は自己に関する個人情報の内容について開示を求めることができるものとさ

れている。

- 情報の主体者が開示要求や訂正・削除要求を行うために必要な連絡先や手順等を明示しておくこととする。
- 開示の求めがあった場合には、弊社の正当な利益が害される場合や業務遂行に支障が生じる場合など正当な事由がある場合を除き、原則としてこれに応じることを約束する。
- 求めに応じることができない場合には、その理由を情報の主体者に説明するように努めるものとする。
- 開示要求の対象となった個人情報のうち、当社による当該個人に対する特定の評価、判断、分析など取得した個人情報に付加された情報は開示の対象にはしない。

3.6.8.2　開示の結果、保有していた個人情報の誤りなどを指摘され、これを訂正、削除等するように求められた場合には、原則としてこれに応じる。

- 開示した個人情報に関して、その内容が誤っているなどして、正確かつ最新の事実を反映させるよう訂正の求めがあった場合には、その内容が妥当であると認められる場合には、原則としてこれに応じるものとする。
- 開示した個人情報に関して、これを削除するように求めがあった場合には、その内容が妥当であると認められる場合には、原則としてこれに応じるものとする。

3.6.8.3　情報の主体者であるお客様から、自己の個人情報の利用・提供の中止を求められた場合には、原則としてこれに応じる。

- 情報の主体者であるお客様から自己の情報の利用や提供の中止、削除などの求めがあった場合には、その内容が妥当であると認められるときには、原則としてこれに応じるものとする。

3.6.9　苦情処理対応窓口の設置と規範遵守

3.6.9.1　個人情報の取扱いに関する苦情に対応するために必要な体制を整備

- 個人情報の取扱いに関する苦情への対応や、開示請求などの窓口となる連絡先を明確にする。

  例：全社共通の受付窓口、メールアドレスの設定
- ＜要検討：社内、グループ内に複数の対応窓口が設けられる場合には、連携強

化の仕組みを取るようにする。＞

3.6.9.2　弊社はお客様の個人情報の保護に関係して、社員に対する教育啓蒙活動を実施する他、日本の法令その他の規範を遵守し、本ポリシーの内容を継続的に見直し、その改善に努める。

以上が参考作成したプライバシーポリシーの雛型条文である。

3.7　個人情報保護ハンドブックについて

次に旧通産省が作成した個人情報保護の基本的考え方をまとめた「個人情報保護ハンドブック」について見てみるものとする。

これは「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」(1997 年 3 月 4 日旧通産省告示第 98 号）として告示された通称「旧通産省の個人情報保護ガイドライン」について、企業側（個人情報を取り扱う事業者）が、その自主的な取組み支援ツールとしていかなる対策をとるべきかを詳細に示して幅広い関係者に配布することとしたものである。（以下同＜**解説書＞平成１０年６日：旧通商産業省；機械情報産業局資料より抜粋・一部改変**）

3.7.1　ハンドブック策定の背景と経緯

1．近年における情報処理技術の著しい発展は、電子計算機（コンピュータ）による大量かつ迅速な情報処理を可能とし、個人指向のクレジットローン等の消費者信用取引、ダイレクトマーケティング等において、ニーズの多様化・個性化に対応した効率的な事業活動の展開を容易にしている。

しかし一方で、個人に関する情報が本人の知らない間に収集・蓄積され、また、本人の予想外の目的に利用されているという事態も見受けられるようになってきていることから、各方面で個人情報の適正な保護について関心が高まってきており、また各種の取組が進められている。

旧通産省においても、1989 年 4 月に、機械情報産業局長の懇談会である「情報化対策委員会個人情報保護部会」の報告として、「民間部門における電子計算機処理に係る個人情報の保護について（指針）」をとりまとめ、財団法人日本情報処理開発協会が昭和 63 年に策定した「民間部門における個人情報保護のためのガイドライン」を当部会のガイドラインとして改めて広く関係者に提示した。あわせて、1989 年 6 月 28 日付けで、本指針に基づいてガイドラインの策定を行うよう、関係事業者団体に対する通達を発信し、指導を行

った。

さらに、1989 年 7 月 7 日には、通商産業大臣告示により、「電子計算機処理に係る個人情報の保護のための措置等についての登録簿に関する規則」を定め、事業者及び事業者団体等が実施している個人情報保護のための措置の概要等に関する申告内容を登録する「個人情報保護措置登録簿制度」を創設し、12 団体からの登録を受けてきた。

2. しかし、昨今の情報処理技術の進歩は目を見張るものがあり、特にダウンサイジング、エンド・ユーザー・コンピューティング等により、従来の大型コンピュータを用いた大量・定型業務の処理に伴うもののみならず、中小を含めた様々な事業者等が情報システムを利用して個人情報を取り扱うことが可能となった結果、個人情報が分散した形で蓄積・利用される可能性が高まり、正当な権限のないものによる情報の不当な利用、改竄、加工等が行われるおそれも強まってきている。実際に、個人情報の漏洩事件は散見されてきており、個人情報保護に対する不安感の高まりから、消費者団体からも個人情報保護の強化が求められているところである。

また、最近のインターネットの爆発的な拡大に代表されるオープンなコンピュータ・ネットワークの世界的な発展等により、いったんネットワーク上に乗せられた個人情報は、一瞬のうちに国境をも越えて広範囲に流通することが可能となっていることから、より大規模な個人情報の侵害事例の発生のおそれが強まるとともに、個人情報保護の国際的な調和が必要となってきている。

3. さらに、海外先進諸国においては、従来から、個人情報保護法が制定され、1980 年に経済協力開発機構（ＯＥＣＤ）が採択した「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（いわゆるＯＥＣＤプライバシー・ガイドライン）をもとに、その後も個人情報保護法が制定されている。さらに近年の情報技術の進展に伴い、各国において個人情報保護の強化へ向けた取組みが開始されている。

特に、ＥＵにおいては、1995 年 10 月に「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令（以下、ＥＵ指令と略す。）」が採択され、域内各国は当該指令に適合するよう 3 年以内に法制化を含めた検討を行うよう求められている。当該指令によれば、個人情報の第三国への移転について、第三国が十分なレベルの保護措置を講じていない場合にはその移転が禁止されるほか、第三国が十分なレベルの保護措置を講じていないとＥＵ委員会が認定した場合には、第三国と交渉できることとなっており、我が国においても「個人情報の十分なレベルの保護」を確保するこ

とが求められているところである。

4. 以上に述べたような状況の変化を踏まえ、旧通産省においては、1995 年度から、機械情報産業局長の研究会である「プライバシー問題検討ワーキンググループ」（座長：堀部政男一橋大学教授＜当時＞）において、抽象的であった 1989 年のガイドラインを具体的かつ詳細にするような改正、民間事業者の自主的な取組みを補完する諸制度の整備、消費者（情報主体）の苦情等に対応する窓口機能の充実等の点に関する検討を開始し、1996 年 4 月には、我が国民間企業等の事業活動の実態を踏まえ、また、ＥＵ指令採択等の国際的動向をも視野に入れた改正ガイドライン第 1 案が完成した。

そして、1996 年 5 月からは、改正案に関する関係者説明及び意見照会を、旧通産省に登録を行っている 12 の事業者団体及び結婚相談業、学習塾業界等の対個人サービスを提供する業界や地方公共団体等に対して実施し、さらに、1996 年 12 月には、旧通産省公報及びインターネットホームページを通じて、国民に対し広く意見照会を行った。

このような過程を経て、「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（1997 年 3 月 4 日旧通産省告示第 98 号）として告示するに至った。

5. 旧通産省としては、1989 年指針のときと同様に、この改正ガイドラインが、関係業界団体やそれを構成する各企業等において、個人情報保護のための自主的ルールが作成される際の指針として利用されることを期待して、普及啓発活動を実施してきた。しかしながら、ガイドライン告示の後も個人情報の漏洩事例が発生している。特に、1998 年に入ってからは、漏洩事例が急増し、その規模も大きなものが見られる。

これは、1989 年のときと比較して、めざましい情報技術の進展が見られたため、個人情報を扱う事業者の範囲が大きく拡大するとともに、その処理量も増大してきていることも大きな要因となっていると考えられる。このため、改正ガイドラインに即し、個人情報保護策として留意すべき点を事例なども活用しながら整理し、個人情報を取り扱う事業者がいかなる対策をとるべきかを詳細に示した本「個人情報保護ハンドブック」を策定し、幅広い関係者に配布することとしたものである。本ハンドブックが事業者のみならず、消費者、研究者等広く国民に利用され、個人情報保護の重要性について認識がより深まることが期待される。

6. さらに、今後は、個人情報保護について、事業者と消費者の間で紛争・トラブルが発生することも懸念される。旧通産省としては、改正ガイドライン及び本ハンドブックは、紛争・トラブルの解決の規範の一つとして活用することが可能と考えているところである。

司法機関、消費者相談所等での活用により、円滑な紛争解決が図られることが期待されるところである。

4　消費者リテラシーへの取組み及び普及ツール導入に伴う課題と対応策

ここでは消費者に対して、オンライン上のプライバシー保護についての啓蒙・教育を実践するのためのツール・施策を見ていくものとする

4.1　啓蒙用「プライバシー保護プロモーション・アニメ」の作成について

このツールは、オンライン上のプライバシー保護において、ネットショッピングの経験のある一般消費者として注意しなければならないポイントを、線画アニメでビデオ化したもので、ＥＣＯＭの個人情報保護ＳＷＧがイベント等の啓蒙用として作成した「プライバシー保護プロモーション・アニメ」を紹介する。

4.1.1　タイトル「それゆけ！EC くん！エピソード２＝安全なＥＣライフのために＝」

プライバシー保護プロモーション・アニメ「それゆけ！EC＜ん！エピソード 2～安全な EC ライフのために～」（VP　4 話オムニバス形式）については、４話構成（時間割）でネットショッピングをする際の個人情報保護についての大切さを比較的解りやすく解説している。時間的には合計で約 4 分 30 秒の線画アニメビデオである。

4.1.2　構成概要

下記のような内容構成となっている。

(1) 第 1 話「大切な個人情報」・・・70 秒

これについては、資料ストーリー1、2、3、4 からなっており、まず電子商取引上での個人情報の大切さを見せている。

(2) 第 2 話「安心な店」・・・70 秒

これについては、資料ストーリー5、6 からからなっており、ネットショッピングにおいての安心できるお店の選び方を見せている。

(3) 第 3 話「チルドレンプロテクション」・・・65 秒

これについては、資料ストーリー8 からからなっており、オンライン上での子供から収集される個人情報についての留意点が解説されている。

(4) 第 4 話「豊かな EC ライフ」・・・65 秒

これについては、資料ストーリー7 及び 9 からからなっており、ネットショッピングを消費者が安心して楽しめるにはどういった基準でお店を選べばいいか、どんな事に注意してショッピングしたら良いかをまとめている。

4.1.3　基本設計・狙い目

昨年の EC 入門アニメ『それゆけ！ EC くん！』の続編として、今回の作品は既に e－コマースを体験されている中級者（ネットショッピング経験者）を対象に、プライバシー保護意識の普及とその具体策の紹介を目的としている。

前作に引き続き、ブルーのバックを背景とした線画キャラクターによるアニメーション（一部、赤色の背景などを内容により使用）を基本に、より具体的な説明を必要とする箇所に HP やマークの実写映像、各種文字情報を加えて展開している。

用途としては、各種のイベントでの啓蒙用や各種研修会での教育（貸出し含む）用ビジュアルツールとしての活用を考えている。

5　プライバシー保護に関するその他課題への取組み

つぎに個人情報保護に関するその他課題である、国際的な動向やネット上のプライバシー保護団体の取組み及び児童オンラインプライバシー等について見ていくものとする。

とくに今回の個人情報保護法制の適用によって、プライバシーをめぐるＥＵとわが国政府との交渉は新しい局面を迎えたと言えよう。

今までの政府間交渉においては、ガイドライン・ＪＩＳ規格・マーク制度のセット活用・実施による自主規制がポイントであったが、これからは基本法の成立を受けてかなりの論点をここに集中して交渉出来そうである。

5.1　サイバースペースのプライバシーを守る業界の取組みで陣頭に立とうとする「オンライン･プライバシー連合（ＯＰＡ）」

次に紹介するのは、1998 年 6 月 22 日に米国の企業や協会による業種をこえた連合組織が、共同で決意を表明し、新しいプライバシー推進計画を発表するにいたった内容である。特にこの「オンライン･プライバシー連合（ＯＰＡ）」のプログラム指針については、後のＥＵと米国の交渉のポイントとなった「セーフ･ハーバー・ポリシー」のベースとなるものとして有名である。（以下はＯＰＡより 2000 年 12 月に直接入手の資料をＥＣＯＭにて抜粋翻訳したものを一部引用。）

5.1.1　「オンライン･プライバシー連合」の創設

ワシントン D.C.にて、米国の 50 近い企業や協会が、「オンライン･プライバシー連合」の創設を発表した。サイバースペースにおける個人のプライバシー保護に取り組む、業種をこえた有力な連合組織である。

同グループは自らの使命の宣言や、オンライン･プライバシー方針の詳細なガイドライン、子供たちのプライバシーを安全に守る一連の原則を公表した。

「これら企業や協会が、個別におこなったり、この連合の一員として行うプライバシーの実践が、今後何年にもわたりインターネット上のあらゆるビジネスの運営方法に影響を与えるだろう」と、連邦取引委員会（FTC）前コミッショナーで同グループのアドバイザーを務めるクリスティン・バーニーは述べた。

同連合は約 3 ヵ月前から正式な会合を始めたが、加盟するメンバーの多くは、米商務省主催で今週開かれるインターネットのプライバシーに関する 2 日間の首脳会議に参加する予

定である。この会議は、新メディアの開発に関連するコンテンツやプライバシーなどの問題への方針を明確にしようとする、米政府の継続的取組みの一環である。
同連合に加わるメンバーは、民間部門全体にとって有効なプライバシー方針を明らかにし、それを促進すること、プライバシー保護に役立つ技術に加え、自己規制の実施メカニズムや活動について、その開発と利用を支援し、助長すること、法律や規則の遵守や強力な執行を支援することに同意した。さらにメンバーは、子供たちのプライバシーを守る慣行や方針を支援し、助長すること、企業、非営利団体、消費者などが連合の取組みを広く認知し、参加するよう促すこと、消費者、企業、大学関係者、市民団体などに連合の取組みに対する意見や支援を求めることで合意した。
「オンライン・プライバシー連合」は、プライバシーを尊重するオンライン環境を生み出すために産業界が手がけたこれまでで最も広範な取組みとなる。
加盟企業や協会（電子商取引に携わる他の数千社の企業を代表する）のリスト（増加中）はhttp://www.privacyalliance.orgで見ることができる。
「連合のメンバーは、いくつかの非常に複雑な問題について共通の基盤を見出そうと著しい努力を払ってきた。またプライバシー保護の基準設定にリーダーシップを発揮している」と、バーニー女史は述べた。
同連合の子供のための方針では、子供向けサイトが、事前に親の同意を得ることなく、または収集する情報の性質や使用目的を親に直接通知することなく、13 歳未満の子供からオンライン連絡先情報を収集してはならないと述べられている。
ガイドラインには、通知と開示、選択権、データ・セキュリティ、データ品質およびアクセスといった問題に対処するプライバシー方針を連合のメンバーが実行するための要件が含まれている。
これに加えて同グループは、100 万社の企業を対象に連合の方針や実践方法を採用するよう働きかけるという教育キャンペーン計画を発表した。消費者向けキャンペーンでは、個人データを保護する方法を人々に教える予定である。連合のメンバーは実施と消費者救済の方針について最後の詰めに入っており、計画完了のスケジュールを決めた。
オンライン・プライバシー連合のメンバーは以下の通り。
Acxiom、アメリカ広告業連盟、アメリカ電子工学協会、American Online, Inc.、AT&T、Bay Networks、Bell Atlantic、CASIE（全米広告主協会およびアメリカ広告代理店協会の代表）、Cisco、Compaq、Dell、ダイレクトマーケティング協会、Disney、Dun & Bradstreet、

Eastman Kodak, Co.、eBay Inc.、EDS、E-LOAN、Equifax、Ernst and Young、Ford、Hewlett Packard、IBM、個人照会サービスグループ、情報産業協会、アメリカ情報技術協会、情報技術産業協議会、双方向サービス協会、LEXIS-NEXIS、Lucent Technologies、MatchLogic、MCI、Microsoft、NationsBank、NCR、NETCOM Onlin ECOMmunications Services, Inc.、Netscape、Oracle、Preview Travel、Price Waterhouse、Procter & Gamble、Sun Microsystems、Time Warner、国際ビジネス合衆国会議、Viacom、Xerox

5.1.2　オンライン・プライバシー連合の自己規制の効果的な実施について

5.1.2.1　概要

オンライン・プライバシー方針の効果的な実施は、オンライン上の個人識別情報の収集・利用・公表についての自らのプライバシー方針を組織が確実に守ることと、消費者からの苦情の解決を図ることを意図している。自己規制の効果的実施は、それを管理するのが第三者のプライバシー検印プログラムであれ、ライセンス許可プログラムであれ、メンバーシップ協会であれ、（1）検証と監視（2）苦情解決（3）教育と活動の拡大、が必要である。一般市民の信頼を得る最善の方法は、容易に認識できるシンボルや検印をもつプログラムへの参加を通じて、各組織が消費者やその他の個人に対して自らの実践方法や手順への注意を喚起することであると、オンライン・プライバシー連合は考える。

5.1.2.2　第三者による実施プログラム

独立した信頼できる第三者により、各組織が有意義なオンライン・プライバシーの自己規制に従事していると確認されることが、消費者の信頼を増すために必要であろう。こうした確認がなされたことは、例えば検印やその他のシンボルを通じて、消費者が容易にわかるようにすべきである。このシンボルや検印は、プライバシー方針の遵守を意味するとともに、検印を与えた者に消費者が連絡をとる容易な方法を示すためにも利用できる。このようにオンライン・プライバシー連合は、第三者の実施プログラムにより、ウェブサイト、オンラインサービスなどのオンラインビジネスの所有者や事業者が、オンライン・プライバシー連合の表明した要素を含むプライバシー方針を導入し、それらの方針に確実に従うための手順を整え、消費者の苦情解決策を提供していることを消費者に知らせるための、識別可能なシンボルを授与する仕組みを応援する。

5.1.2.3　プライバシーシールプログラム

こうしたプライバシーシールプログラム（以下「シールプログラム」と呼ぶ）では、客

観性を維持し、消費者に対する正当性を確立するのに必要なメカニズムを実現すべきである。シールプログラムでは、その方針を策定するにあたり、ビジネス界、消費者・市民団体や、大学関係者からの意見を請い、考慮するような管理組織を活用すべきである。またシールプログラムでは、その手順を実行する一貫した予測可能なフレームワークを生み出す努力をすべきである。このシールプログラムは独立した活動として、すべてのオンライン事業に入手可能なシールをなるべく受け取らせる努力をすべきである。

シールプログラムには以下の特徴が含まれるべきである。

- **遍在性：** 混乱を最小限に抑え、消費者の信頼を高めるため、至る所で同時に導入されるようにし、ブランド化（例えば、企業や協会との共同ブランドにするなど）を通じてシールを確実に知ってもらう努力をするものとする。
- **包括性：** シールプログラムは、秘密に関わる情報とそうでない情報のいずれに関連する問題にも十分対処できる柔軟性を備えるべきである。
- **わかりやすさ：** シールは利用者が容易に気づき、利用し、理解できるものであるべきだ。
- **入手しやすさ：** シールの価格や構造は、幅広い使用を助長すべきものであり、中小企業にとって負担が大きすぎてはならない。シールの価格は、検査の範囲や複雑さ、事業の規模、収集・利用・配布される個人識別情報の量や種類などを含む、数多くの要因により様々に異なるだろう。
- **完全さ：** シールを与える者は、商標権の執行措置など、そのシールの完全さを維持するのに必要なあらゆる手段を追求できるようにすべきである。
- **奥深さ：** シールを与える者は、オンライン・プライバシー方針への違反が万一発生した場合に、消費者の問い合わせや苦情の数や幅広さに対応できる能力を備えるべきである。またそうした問い合わせや苦情に対処する一連のメカニズムを確立しておくべきである。

5.1.2.4 検証と監視

シールプログラムは、参加者がオンライン・プライバシー連合の支持する原則に適合するプライバシー方針を採用するよう要求しなくてはならない。この要求の範囲は、参加組織にのみ適用され、関連会社のウェブページや参加組織のウェブページとの間でリンクする他のウェブページには適用されない。これら指針となる原則は標準化されるべきだが、シールを与える者が認める個々の方針では、その部門に特有のバリエーションを考慮すべ

きである。そこでシールプログラムは、シールの授与に先立ち、組織が自己査定システムを整備するか、シールプログラムの遵守検査を受入れるかのいずれかを要求しなくてはならない。

自己査定システムを選択する場合、それは厳格で、一定不変で、明確に示され、一般に開示されたシールプログラム方法論に従うものでなければならず、それに基づいて組織は、すでに公表したプライバシー方針が的確で、包括的で、目立つように表示され、完全に実行されており、わかりやすいことと、苦情処理のための消費者苦情解決メカニズムについて消費者に十分知らせていることを、検証するよう要請される。自己査定を検証する申告書には、その企業の役員または誰か権限を与えられた代表者が署名すべきである。その上でシールプログラムが検査して、自己査定が上記方法論にしたがっていることを確かめるべきである。企業が自己査定システムの実施方法を改善する場合や、さらなる手段を導入する場合の明確な基準や、第三者のチェックが必要となる状況は、シールプログラムにおける容認できる自己査定の方法論の一部に含まれるべきである。

シールを表示している組織が自らのプライバシー方針を守り続けていることや、その方針が連合の原則と一致し続けていることを確かめるために、シールプログラムは定期的な検査を義務づけるべきである。こうした定期検査には、表明されたプライバシー方針を各サイトが厳守していることを確かめるのに適切と思われる、監査、無作為抽出検査、「おとり」の使用、または技術ツールの使用などの方法があるだろうが、これらに限定されない。

会社が自らのプライバシー方針を守っていない証拠がある場合、シールを与える者はその会社を保護観察下に置くか、またはシール取消しの手続を始める明確な基準を定めるべきである。シールを与える者は、会社のシールを取消すことができる場合や方法について明確に示した基準を定めるべきである。会社側には通知がなされるとともに、シールが取消される前に外部の検査を要請する機会が与えられるべきである。シール取消しは、公的な記録として残すべきである。シールを与える者は、取消しの根拠を明確に記述し、取消し後の上訴の手順を確立すべきである。シールを与える者は上記の基準に加え、濫用や悪用を監視することにより、シールの完全さを確保することにも努力を払うべきである。

5.1.2.5　消費者からの苦情の解決

第三者による効果的な実施メカニズムは、参加企業や消費者に対して、苦情を解決する仕組みを提供し、解決に失敗した場合の結果を示さなくてはならない。そこでシールプログラムでは、苦情解決プロセスにしたがって苦情の範囲を明らかにし、苦情を処理するシス

テムを整備し、大量の苦情を処理するのに必要なスタッフを用意し、それらを解決する組織上の奥深さを備える必要がある。シールプログラムは、消費者が容易に苦情を申立てたり質問したりできるようなメカニズムを多様な形で提供しなくてはならない。シールを授与された者は、苦情解決手続きに応じなければならない。

苦情解決システムのもとでは、シールプログラムの苦情解決メカニズムの利用を許可する前に、まず消費者が自分を不当に扱ったと考える企業に苦情の救済を求めることを義務づける必要がある。その企業が苦情を適切に処理できない場合や、消費者と企業が合意に向けた誠実な努力を続けられなくなった場合に、その企業は苦情解決メカニズムに従うよう求められるべきである。

苦情解決の成果は、その参加企業の現在の法的義務に反するものであってはならない。シールプログラムの苦情解決の成果を企業が受入れない場合は、その企業に対して事前に定められた結果に従うことになる。苦情解決プロセスとは関係なく、消費者、企業およびシールを与える者が、他の可能な法的償還請求権を追求することになるだろう。

5.1.2.6　教育と活動の拡大

シールプログラムは、オンライン・プライバシーについて消費者や企業を教育するための方針を考え出し、実行しなければならない。

シールプログラムは、消費者の側も企業の側もそのプログラムやオンライン・プライバシー問題に対する認識を高めるための方針を考え出し、実行しなければならない。その手法として以下のようなものが挙げられる。参加企業への広報活動、具体的な非遵守またはシール取消しの情報開示、監視・検査手続の結果を定期的に公表すること、非遵守企業を適切な政府機関に付託すること。

5.1.3　オンラインのプライバシー促進に取り組むグローバル企業および協会による連合の使命について

5.1.3.1　使命宣言

オンライン・プライバシー連合は、信頼できる環境を生み出すとともに、オンラインおよび電子商取引における個人のプライバシー保護を助長する、自己規制の推進計画を先導し、支援するものである。

本連合は今後、以下のことを行う。

- 民間部門全体に有効なオンライン・プライバシー方針を明らかにし、それを促

進する。

- ユーザの能力を高める技術ツールに加え、個人のプライバシー保護を目的とする自己規制の実施メカニズムや活動について、その開発と利用を支援し、助長する。
- 適用される法律や規則の遵守や強力な執行を支援する。
- 子供たちのプライバシーを守る慣行や方針の策定と利用を支援し、助長する。
- 企業、非営利団体、政策立案者、消費者が連合の取組みを広く認知し、参加するよう促す。
- プライバシー保護という共通の問題に関わっている消費者、企業、大学関係者、市民団体やその他の組織に、連合の取組みに対する意見や支援を求める。

5.1.3.2 メンバーとしての誓約

連合のメンバーとして、以下のことを誓約する。

- 我々は連合の使命を支持する。
- 我々は連合のガイドラインに矛盾しないオンライン・プライバシー方針を実行することを約束する。
- 我々は効果的で適切な自己規制の実施活動やメカニズムに参加することを約束する。

5.1.3.3 オンライン・プライバシー方針のガイドライン

オンライン・プライバシー連合への加入時に、各メンバーは、オンラインまたは電子商取引環境における個人識別情報を保護する自らの方針が、少なくとも以下の要素に対処する（メンバー自身のビジネスや業種にとって適切な変更や改善点を加えた上で）ことに同意する。

(1) プライバシー方針の導入と実行

オンライン活動や電子商取引に従事する組織は、個人識別情報のプライバシーを保護する方針を導入し、実行する責任を負う。また各組織は、例えばビジネス・パートナーと最善の実践方法を共有するなど、業務で協力し合う相手の組織が効果的なオンライン・プライバシー方針を導入し、実行するよう助長する手段を講じるべきである。

(2) 通知と開示

ある組織のプライバシー方針は、容易に見つかり、容易に読め、容易に理解されるものでなければならない。その方針は、個人識別情報が収集または請求される時点かそ

れ以前に入手可能でなければならない。

この方針は、次のことを明確に述べていなくてはならない。どのような情報を収集しているのか、その情報の使用目的、その情報を第三者が配布する可能性、収集された情報の収集・利用・配布に関して個人に与えられる選択肢、その組織がデータ・セキュリティに取り組む姿勢の宣言。データの品質とアクセスを確保するために組織がいかなる手段を講じるか。

この方針では、個人が情報提供を拒否した場合の結果（もしあれば）を明らかにすべきである。またこの方針には、その組織への連絡方法など、組織がいかなる説明責任メカニズムを用いるかという明確な宣言が含まれるべきである。

(3) 選択権／同意

個人からオンラインで収集した個人識別情報を、その情報が収集された目的と関係のない用途に利用してもよいかに関して、個人に選択権を行使する機会を与える必要がある。少なくとも、個人にそのような利用を拒否する選択の機会を与えるべきである。

加えて、個人からオンラインで収集した個人識別情報を、収集された目的とは関係なく第三者が配布する場合、大多数の状況において、個人にそれを拒否する選択の機会を与えるべきである。

そのような用途への利用または第三者の配布について、技術ツールを通じてまたは許可を選択することにより、同意を得ることもできる。

(4) データ・セキュリティ

個人識別情報を生み出したり、維持したり、利用したり、広めたりする組織は、信頼性を保証する適切な手段を講じるべきであり、情報の損失、濫用または変更を防ぐために妥当な予防措置を講じるべきである。また上記の組織は、こうした情報の伝達先である第三者がこれらのセキュリティ実践方法を承知し、第三者の側でも伝達された情報を守るために妥当な予防措置を確実に講じてくれるような、妥当な手段をとるべきである。

(5) データの品質とアクセス

個人識別情報を生み出したり、維持したり、利用したり、広めたりする組織は、データがその利用される目的にとって正確かつ完全であり、時機が適切なことを保証する妥当な手段を講じるべきである。

組織は、具体的な個人識別情報の誤り（口座情報や連絡先など）を訂正できるように、

適切な手順またはメカニズムを確立すべきである。これらの手順やメカニズムは簡明で利用しやすく、誤りが訂正されたという保証を与えるものがよい。データの品質を保証するこれ以外の手続としては、信頼できる情報源や収集方法の利用、妥当かつ適切な消費者アクセスと訂正方法、偶発的または許可のない変更からの保護、などがある。

これらのガイドラインは、専有情報、一般に入手可能な情報、または公的に記録された情報に適用されることを意図しない。また、法令、規則または法的手順により課せられる義務に取って代わることを意図しない。

プライバシー方針を考えるときに連合のメンバーが利用できる他の貴重な情報源としては、経済協力開発機構（ＯＥＣＤ）の「プライバシー保護と個人データの国境を越えた流出に関するガイドライン」、米商務省の「プライバシー自己規制に関する審議報告書」および各種の業界団体プログラムなどがある。

5.2　児童オンラインプライバシー保護法について

次に2000年4月21日から有効となった児童オンラインプライバシー保護法を紹介する。同法律は、13 歳未満の児童からのオンラインでの個人情報収集に適用される。この新しい規則では、ウェブサイトの運営者がプライバシー方針として取り入れるべきことは何か、何時、どのようにして親から証明可能な同意を得るべきか、また、オンラインでの児童のプライバシーと安全を保護するためにどんな義務を負うべきかが詳しく述べられている。

このガイドは、連邦取引委員会（FTC）のスタッフ、ダイレクト・マーケティング協会、インターネット・アライアンスによって、人々がこのオンラインにおける児童のプライバシー保護のための新しい規制を遵守し、FTC の持つ執行権を理解する助けとなるよう制作されたものである。（以下ＦＴＣにて 2000 年.12 月に入手の資料から「1998 年成立の米国児童オンラインプライバシー保護法」関連の翻訳を抜粋引用）

5.2.1　対象となる人

児童オンラインプライバシー保護法（COPPA）を遵守しなければならないのは、13 歳未満の児童を対象とし、児童から個人情報を収集している商用ウェブサイトまたはオンラインサービスを運営している場合、もしくは一般用ウェブサイトを運営していても、児童から個人情報を得ていることが実際にわかっている場合である。

- ウェブサイトが児童を対象としたものかどうか判断するために、FTC はいくつかの点を考慮している。例えば主題、視覚的・聴覚的内容、サイト上のモデルの年齢、用語のほか、ウェブサイト上の広告が児童を対象としたものかどうか、実際のまたはターゲットとする利用者の年齢に関する情報、アニメのキャラクターなど子供向きの工夫がサイトで用いられているかなどである。
- サイトで収集される情報の「運営者」に該当するかどうかを判断するために FTC が考慮するのは、その情報を所有し、収集しているのは誰か、その情報の収集・メンテナンスにかかる費用を出しているのは誰か、情報に関してどのような契約関係が事前に結ばれているのか、情報の収集やメンテナンスにおいてそのウェブサイトがどんな役割を果たしているのかなどである。

5.2.2 個人情報

児童オンラインプライバシー保護法および規則は、オンラインで収集された情報で、児童を個別に特定できるものに適用される。例えば氏名、住所、E メールアドレス、電話番号のほか、その児童を特定したり児童と連絡をとったりすることが可能になる情報である。同法はその他のタイプの情報も対象としている。例えば趣味、関心事、cookie その他のトラッキング方法を使って収集した情報などで、それらが個人を特定できる情報につながっている場合は対象となる。

5.2.3 基本条項

5.2.3.1 プライバシーに関する告示

(1) 設定

運営者はその情報の利用に関する告示へのリンクをウェブサイトやオンラインサービスのホームページ、さらに児童から個人情報を収集する各エリアに張らなければならない。児童向けのエリアが別についている一般向けサイトの運営者は、その児童向けエリアのホームページ上に告示へのリンクを張らなければならない。

プライバシーに関する告示へのリンクははっきりと目立つものにする必要がある。フォントのサイズを大きくしたり、背景とは対照的な色を使ってもよいであろう。リンクがページの一番下に小さく書かれていたり、サイト上の他のリンクと区別できないような場合、はっきり目立つとは見なされない。

(2) 内容

告示は明確にわかりやすく書かれていなければならない。関係のない事柄や誤解を生むような記述を入れてはならないのである。告示には次の情報が含まれることとされている。

そのウェブサイトやオンラインサービスを通じて児童の個人情報の収集やメンテナンスを行っている運営者全員の名前と連絡先（住所、電話番号、Eメールアドレス）。そのサイトで情報を収集している運営者が複数いる場合は、そのサイトのプライバシー方針に関する親からのあらゆる問い合わせに対応する運営者を一人選んで、連絡先を掲載することもできる。その場合も、運営者全員の名前を告示に載せなければならない。

児童から収集される個人情報の種類（例えば名前、住所、Eメールアドレス、趣味など）およびその情報がどのように収集されるのか、すなわち、児童から直接収集するのか、あるいは例えば cookie などを通じて間接的に収集されるのか。

その個人情報は運営者によってどのように利用されるのか。例えば児童に商品を販売するためか？　コンテストの入賞者を知らせるためか？　児童がその情報をチャットルームを通じて公開することを許可するためか？

運営者は児童から収集した情報を第三者に公開するのかどうか。公開する場合は、運営者はその第三者が従事しているビジネスの内容も公開する必要がある。すなわち、その情報を利用する主な目的、および第三者が情報の秘密性やセキュリティの保持に同意しているかどうかである。

親には児童の情報の第三者への公開には同意せずに、情報の収集・利用に同意するという選択肢があること。

運営者は、児童が企画に参加するための条件として、道理的に参加のために必要であるとされる以上の情報を児童に要求してはならないこと。

親は児童の個人情報を閲覧し、その削除を要求したり、それ以上の情報の収集や利用を認めることを拒否したりすることができること。また告示には親がとるべき手順についても記載しなければならない。

5.2.3.2　親への直接の告示

(1) 内容

親への告示にはウェブサイト上の告示と同じ情報が盛り込まれていなければならない。

さらに、運営者は親に対し、児童から個人情報を収集したいこと、その情報の収集、利用、公開にあたっては親の同意が必要なこと、同意を与えるにはどのようにすればいいのかを通知しなければならない。親への告示は明確、かつわかりやすい文章を心がけ、関係のない事柄や紛らわしい情報が含まれないようにする。運営者は親への通知にあたり、Ｅメールでのメッセージの送付または郵送など、どんな方法をとってもかまわない。

(2) 証明可能な親の同意

児童の個人情報を収集、利用、または公開する前に、運営者はその児童の親から証明可能な同意を得なければならない。すなわち、運営者は（利用できる手段を考慮したうえで）しかるべき努力を払い、児童から個人情報を収集する前に、その児童の親が運営者による情報の取扱いや、これらの取扱いに対する同意に関する告示を確実に受け取るようにしなければならないのである。

2002 年の 4 月まで、FTC は親の同意について「スライディングスケール」法を適用するが、ここでは必要とされる同意の方法が、運営者がその児童の個人情報をどのように利用するかによって違ってくる。つまり、運営者がその情報を内部的な目的で利用する場合は、それほど厳格でない同意方法が必要とされる。運営者が情報を他者に公開する場合は、児童に対してより大きな危害が及ぶことも考えられ、より信頼性の高い同意方法が求められる。スライディングスケール法は、2001 年 10 月に予定されている委員会の再検討の結果にしたがって、2002 年 4 月に終了する。

(3) 内部利用

運営者は個人情報の内部的な利用に対する親の同意を得るのにＥメールを使うことができる。内部的な利用とは、例えば、その児童の好みに合わせて商品を販売したり、営業目的でサイトの内容についての最新情報を流したりすることであるが、これは、親が実際に同意を与えたことを確認するために運営者が追加的な手段を講じる場合に限られる。例えば、後から確認のＥメールによって親から確認をとったり、文書や電話で同意を確認することもできる。

(4) 公開

運営者が児童の個人情報を第三者に公開したり、一般に利用できるようにしたい場合（例えばチャットルームやメッセージボードを通じて）、スライディングスケールでは次のようなより信頼性の高い方法をとることを求めている。

郵送やファックスで親からの署名入りの書類を入手する。

取引に使われるクレジットカードの番号を入手して照合する。

訓練を受けた者が応対する無料電話番号を設置して、親からの電話を受け付ける。

デジタル署名の入ったＥメール。

ただし、モニターつきのチャットルームの場合、個人を特定できる情報が公開前にすべて掲載からはずされ、さらにその情報が運営者の記録から削除されている場合は、運営者は事前に親の同意を得る必要はない。

(5) 第三者への公開

運営者は親に対し、第三者への情報の公開に同意することなしに、児童の個人情報の収集と利用に同意するという選択肢を与えなければならない。しかし、親が児童の個人情報の収集と利用に同意した場合、運営者はその情報をウェブサイトやサービス内部の運営のサポート、例えば技術的なサポートやその他の業務などの目的でのみ利用する者に与えることができる。

(6) 例外

この規則には、運営者が事前に親の承諾を得ることなく児童のＥメールアドレスを収集することを許可する、いくつかの例外がある。これらの例外には、コンテスト、オンラインニュースレター、宿題の手伝い、電子ポストカードなど、子供に人気のあるオンラインのプログラムの多くが該当する。

次のような場合、事前の親の承諾は必要ない。

運営者が告示を出し、同意を求める目的で児童やその親のＥメールアドレスを収集する場合。

運営者が児童からの一回限りのリクエストに応じるためにＥメールアドレスを収集し、その後そのアドレスを削除する場合。

運営者が児童からニュースレターの購読などの特定のリクエストに数回にわたって応じるためにＥメールアドレスを収集する場合。この場合、運営者は児童に定期的に情報を送っていることを親に通知し、その情報を 2 回目に送付または配達する前に親がそれを差し止めることができる機会を与えなければならない。

運営者がそのサイトに参加している児童の安全を守るために、児童の名前またはオンラインの連絡先を収集する場合。この場合、運営者は親に通知を出して、その情報のそれ以上の利用を差し止める機会を与えなければならない。

運営者がサイトのセキュリティや信頼性を守るため、あるいは必要に応じて法の執行に対応するために児童の名前またはオンライン連絡先を収集し、それ以外の目的には利用しない場合。

(7) スライディングスケール法の終了

2001 年 10 月、委員会は技術が進歩したかどうか、証明可能な親の同意を得るための安全な電子媒体が広く利用可能になっているのかどうか決定を下すために、一般からのコメントを求めることになっている。委員会の再検討に従い、スライディングスケールは 2002 年 4 月に失効する。その時まで、運営者はすべての児童の個人情報の利用に対し、より信頼性の高い同意の方法をとることを奨励されている。

(8) 新たな同意を求める告示

運営者はすでに親から承諾を得ている情報の収集、利用、または公開方法に大きな変更があった時には、親に対し新たな告示と同意の申請を送付する必要がある。例えば、児童が一定の個人情報を提出することが求められるコンテストに参加することに対し、その親からすでに同意を得ている運営者が、今度は児童にチャットルームを提供したいとする場合を想定してみる。あるいは、当初の同意の対象とされていたのとは大きく種類の異なるビジネス—例えば、ぬいぐるみの販売から今度はダイエット薬品の販売など—に従事する第三者に対し、児童の情報を公開したいとする運営者の場合はどうであろうか。これらのケースでは、規則により新たな通知と同意が必要とされる。

5.2.3.3 アクセス

(1) 確認

運営者は親の求めに応じて、サイトを訪れる児童から得た特定の情報だけでなく、児童からオンラインで収集した一般的な個人情報（例えば名前、住所、電話番号、Ｅメールアドレス、趣味など）も開示しなければならない。運営者は児童の特定の情報へのアクセスを親に与える前に、それが確かにその児童の親であることを確認するため、しかるべき手順をとる必要がある。

運営者は親の身元を確認するために様々な方法をとることができる例としては

親から郵送またはファックスで署名入りの文書を取り寄せる。

クレジットカードの番号を入手して照合する。

訓練をうけたスタッフが応対する無料電話番号で、親からの電話を受け付ける。

デジタル署名が入ったＥメール。

上記の確認方法を通じて得られたPIN（個人識別番号）またはパスワードのついたＥメール。

親からのアクセスに対する要望に対し、運営者がこれらの手順のいずれかに従い、誠意を持って行動した場合、児童の親を名乗る人物に間違って情報を流してしまっても、連邦および州の法律のもとに責任を問われることはない。

(2) 取り消しおよび削除

児童の親は同意を取り消したり、運営者がその児童の個人情報をそれ以降利用・収集するのを拒否したり、運営者に情報の削除を指示したい時、何時でもそうすることができる。そのかわり、運営者はいかなるサービスであれ、その児童に提供されているサービスを終了させることができる。ただしそれは、問題となっている情報が、そのプログラムに児童が参加するにあたってどうしても必要である場合に限る。例えば、運営者はチャットルームに参加する児童に対し、児童がチャットルームで不適切な行為をとった時に連絡をとれるよう、Ｅメールアドレスを提出するよう求めることができる。そして、児童の親が運営者に同意を与えた後で、その児童の情報の削除を求めた場合、運営者はその児童がそれ以降チャットルームに参加するのを拒否することができるのである。ウェブサイト上の他の企画ではその児童のＥメールアドレスが必要でない場合は、運営者は児童がそれらの企画にアクセスするのを許可しなければならない。

5.2.3.4 タイミング

この規則は、それまでの運営者と児童との関係にかかわりなく、2000年4月21日以降に収集されたすべての個人情報を対象としている。例えば、運営者が児童の名前とＥメールアドレスを2000年4月21日より前に収集していても、児童の住所に関する情報を4月21日以降に得ようとした場合、これは規則の要件を満たさなければならなくなる。さらに、2000年4月21日以降、運営者が児童からの継続的な情報収集を行う企画（例えばチャットルームなど）を続けようとする場合、あるいはそのような企画を新たに開始する場合、それに参加するすべての児童について、児童がそのサイトに登録済みであるかどうかにかかわりなく、告示と同意が必要となる。

5.2.3.5 セーフ・ハーバー

業界団体などで自主規制プログラムを作成し、その参加者に児童オンラインプライバシー保護法の遵守について指導することもできる。これらのガイドラインには独自の監視お

よび懲戒方法を導入し、委員会の承認を得るために提出する必要がある。ガイドラインの認可にあたっては、委員会はそれを公開し、一般からのコメントを求める。運営者が委員会に認可された自主規制ガイドラインを遵守することは、主に規則違反に対する法の執行のセーフ･ハーバー「安全港」としての役目を果たすことになる。

5.2.3.6 執行

委員会は規則違反に対し、FTC 法に基づく他の規則の違反に対するのと同じように執行権を行使して、民事罰を課することができる。委員会はまた FTC 法の第 5 節のもとに、情報の取扱い方に詐欺や不正がないかを検査する権限を持つが、この取扱い方には規則が有効となる日より前のものも含まれる。FTC 法の第 5 節の解釈として、委員会は表現方法や省略、取扱いが以下のようである場合、それらが詐欺に相当するとしている。

- 消費者に誤解を与える。
- 消費者の行動、またはその製品やサービスについての判断に影響を与える。

特に、ウェブサイトが児童から単一の目的（例えば賞品を獲得するためのポイントを稼ぐなど）のために個人を特定できる情報を収集しているように装いながら、その情報を親が重大視するような他の目的で利用すること、そしてその目的をはっきりと開示しないことは、第 5 節のもとでは詐欺行為とされる。

さらに、ある行為や慣行が損害をもたらしたり、またはもたらす可能性がある場合、その損害が以下のような場合、不正行為となる。

- 重大である。
- 他の利点と比べて大きすぎる。
- 道理的に避けることが不可能である。

例えば、児童からＥメールアドレスや住所、電話番号などの個人を特定できる情報を収集したうえ、親に対してしかるべき告示およびその情報の収集・利用を抑制する機会を与えることなく情報を第三者に公開した場合、その行為は第 5 節の違反という不正行為であるとされる可能性がある。

5.2.4 GO.comが子供のプライバシー保護のために親のクレジットカード確認を要求

The Walt Disneyのインターネットビジネス部門であるGO.comは21日、子供がGO.comのネットワークサイトで、掲示板への投稿やチャットへの参加、メールアカウントの取得

など、コミュニケーション機能を使おうとする場合に、親のクレジットカード番号を提供してもらい、認証作業を行なうことを発表した。
この作業が必要となるサイトには GO.com、Disney.com、ESPN.com、ABCNEWS.com、ABC.com、が含まれる。
昨年の 1 月以来、GO.com と Disney Online は子供がオンラインで活動する際に親に対してメールで確認をとっていたが、今回規制を厳しくしたのは 4 月 21 日に施行される児童オンラインプライバシー保護法（Children's Online Privacy Protection Act：COPPA）を遵守するためだ。
この法律では Web サイトは 1)プライバシーポリシーを掲示しなければならない 2)子供に関する個人的な情報を集めたり開示したりする場合には親の了解を得なければならない 3)情報の中身が実質的に変化する場合には新しく同意を取り付けなければならない 4)子供に関して集められた個人的な情報は親が見ることができなければならない 5)親が同意を取り消し、これまでに集められた個人情報を削除する権利を与える、などの法律的な義務を負うことになっている。
ネットの匿名性故に、ネットにアクセスする子供がこうした GO.com のような規制を守るかどうかは難しい問題だが、まじめな子供にとって親のクレジットカード番号を要求されることは実質的に心理的な障壁となるだろう。子供を巻き込んだネット犯罪が多発する中で新法が施行され、今後こうした規制をするサイトが増えてくるかもしれない。
(2000/4/24 taiga@scientist.com)

5.2.5 The Children's Online Privacy Protection Act of 1998 (COPPA)の詳細

米国のＦＴＣ(Federal Trade comission)が 1998 年秋に成立し、2000 年 4 月施行の Children's Online Privacy Protection Act を実施するための細則(rule)を発表した。本体は pdf ファイルで 90 ページあるのでプレスリリースを見ていくものとする。
この法律では子どもの個人情報をオンライン上で取得することについて様々な制限を課している。
細則として最も注目されていたのは"verifiable parental consent"とはどのような方法を指すかであった。子どもの個人情報を取得するには「証明可能な親の同意」が必要なのであるが、具体的にはどのような方法が必要かは法は規定していないからである。
ニューヨークタイムス(By JERI CLAUSING)が指摘しているように、産業界は電子メール

での確認が確実であり、他の方法は費用がかかり過ぎると言い、人権保護の立場からは親よりパソコンに詳しい最近の子どもたちは簡単にごまかしてしまうと主張するという問題があるわけである。

この点についてＦＴＣのルールは「スライド制」という方法を採用した。

つまり、2 年間に限って、2 つの異なる方法をとっている。まず、個人情報をサードパーティーに渡す場合とチャットなどの利用のように子どもに危険な場合は、もっと信頼性の高い同意方法が必要である。次にその情報を内部的に使用するに過ぎない場合は、親の同意を確認する付加的ステップが取られる限り、電子メールを使うことが許される。

ニューヨークタイムスによればこの方法は人権派も産業界も受け入れているようである。

つまり現状では、その場で親の確実な同意を得る手段が技術的にも制度的にもないため、危険の程度に応じて同意の方法を変え、しかも技術の発展を期待して 2 年間という据え置き期間を認めるという方法がより現実的かつ両者が受け入れうる妥協点というわけである。

このほかにこの細則では、いくつかの例外を定めている。

例えば宿題のためなどのように 1 回限りのリクエストのためにメールアドレスを収集すること、あるいはコンテストやニュースレターについてはそれについて親が知らされることと親がそれ以上の使用を止める機会が与えられる限り親の同意がなくても良いとされている。

また、学校の活動については. 教師に親を代理する権限あるいは仲介者としての地位を認めている。ここでも現実的な選択をしているわけである。

実はこれを単なる妥協というのは実は正確ではなく、ここにプライバシーの本質の一部が表れていると見るべきである。つまり、個人情報を厳格に守るだけでは、実際の社会的活動が困難になってしまう。プライバシーの権利も合理的な必要性とのバランスの上で認めなければならないという権利としては当然の性質を持っているわけである。但し、このバランスは非常に難しく、判断を誤ると人権侵害に陥いるが、今回のＦＴＣのルールは合理的なものと言えるであろう。

このほかに細則ではプライバシーの告知の掲示の仕方についても言及している。

つまり、まずホームページ(トップページである。)に明確かつ目立つように掲示するとともに、個人情報を収集する各ページへの掲示も要求している。また、そこにはオペレータの名前とコンタクト方法、子どもから集める個人情報の類型と使用方法、サードパーティに開示されるかどうかについて書かねばならない。

さらに、告知には合理的に必要な範囲を超えて子どもが個人情報を打ち明けることをそこへの参加の条件としてはならないことを明記しなければならない。また、親が収集した子どもの個人情報を検閲し、それを削除できること及びそれ以上の収集・使用を拒否することができることも明記しなければならない。

このことは最近わが国でもプライバシーポリシーを掲載するサイトが増えており、その際の参考になると考える。

この細則がただちにわが国のインターネット界に影響を与えるとは考えにくいのであるが、わが国のポルノ業者が脱法的(実は違法)に米国にサイトを移動したように、米国の業者がサーバをわが国に移転するなどの状態が生じた場合には、わが国の子どもの個人情報の取扱いについて議論が生ずる可能性がある。

（asahi-net.or.jp/~lg9h-tkg/news991022 より抜粋引用）

.

5.2.6 子供のオンラインプライバシー保護法、過半数の子供が規制は必要と感じる

米連邦取引委員会（FTC）は「子供のオンラインプライバシー保護法（COPPA）」に関する最終的な法規を公開する予定である。この保護法では、Web サイトが 13 歳以下の子供の個人情報を収集する場合、親の同意を必要とする。それを前にして、米 SmartGirl.com が、16,528 人の少年少女を対象に、オンラインプライバシーを保護する最適な方法について調査を行なった。

調査によると、プライバシー保護が必要ないと答えたのはわずか 5%。少年少女の 64%は、インターネットは危険なものになりうると感じている。58%は、子供が個人情報を渡す前に両親の許可を得るべきだと答えている。

また、少年少女の 49%が、子供から収集した情報をどのように使用するかについて、厳重な法律で規制すべきだと答えた。一方で、チャットルームや掲示板に参加する自由を失いたくないと考えており、チャットルームに参加する前に親の許可が必要だと答えたのは 15%、掲示板への書き込みに許可が必要と答えたのはわずか 8%だった。また、10～12 歳の子供の 67%が、13 歳以上でなければ Web サイトにアクセスできないとしたら、自分は 13 歳と答えると回答した。

企業が親の同意を得たことを証明できる方法として、挙げられた上位 3 つの方法は、政府が「インターネットの運転免許」を作成する（12%）、両親が許可を与えた Web サイトに

メールを送る（10%）、両親にフリーダイヤルの番号を与える（9%）。

（watch.impress.co.jp/internet/www/article/1999/1020 の記事より）

5.3　児童プライバシー保護課題のまとめ

以上見てきたように、米国では米連邦取引委員会（FTC）が「子供のオンラインプライバシー保護法（COPPA）」に関する最終的な法規を公開し、この保護法では、Web サイトが 13 歳以下の子供の個人情報を収集する場合、親の同意を必要とすることを求めている。

それに比べて、わが国ではインターネット上の子供に対する個人情報の保護については、基本法制のカバーはあるものの、社会的な関心事としての位置付けはまだまだ低く、この分野に特化した法規制の動きはまだ何もない状態である。

ところが周知の様に、わが国におけるインターネット人口は近年爆発的に増加の一途であり、またその参入年齢も低年齢化及び広範化が益々進行している。この状況を鑑みるとやはり、オンライン上の子供の個人情報保護は喫緊の課題の一つと言えるであろう。

つまりわが国においては、民間分野を含む全体･総括的な法規制が確立した後に、残る課題としては、個別法分野の課題の一つとして「子供及び高齢者にたいする個人情報保護」が検討されるべきであると思われる。

5.4　全体課題まとめ

今回の法制化といった行政的な施策とは別に現在の、個人情報保護の取組み全般について言えば、特定少数の先進企業群は、すでに自主的な取組みを始めているのが現状である。

つまりこういった企業では個人情報保護という取組みが全社の経営マネジメントの一要素として、その一環に組込まれており、その重要性の自覚と言う点で他企業と際立った違いを見せている。

当然。社内遵守規定であるコンプライアンスプログラム（JIS 規格準拠）策定・実施等を通して、この個人情報保護のコンセプトそのものが、社内監査・マネジメント体制 へ反映されており、それが当該先進企業群の企業システムの改善・対外競争力強化に役立っているといっても過言ではない。

こういった企業の実態を見ていると、会社としての個人情報保護つまりプライバシーの遵守・保護の考え方は、現在の企業戦略から、近い将来すぐに重要な経営課題となり、やがて現在の環境保護と同じく、いわゆる企業理念へと昇華して行くのではないかと思われ

る。

そして米国では、もうその兆候がはっきりと現れており民間企業が生き残る為の必須施策のひとつにプライバシー保護が認知されて、個人情報保護の専門担当役員であるＣＰＯ（Chief Privacy Officer）の存在が、ＣＥＯ／ＣＩＯと並んで先進企業では当たり前の役職として登場してきている。つまり米国ではプライバシー問題だけで一人の役員を抱えてまでその課題解決に邁進させるだけの価値のある経営課題として、その重要性の認識が高いと言う証左に他ならない。

またもうひとつの忘れてはならない大きなポイントとしては、ＣＳ（Customer Satisfaction）の問題がある。つまり、プライバシー保護や個人情報保護の取組みはＣＳの実現とイコールであると言う事実である。それはいろいろなアンケート記事やインタビューデータからも分かる様に、顧客（カスタマー）の最大不安解消に繋がる喫緊の経営課題である。

将来方向としては、顧客としてこれだけ関心の高いパーソナルデータの安全保護管理については、既に米国の一部企業でビジネスとして始まっている個人識別可能情報（ＰＩＩ＝Personal Identifiable Information）の一括管理が主流になると言う見方もある。

つまり「インフォミディアリー（情報仲介人）」市場の形成である。プライバシーも財産と同じく、自己とは別な管理人をおいてまで保護に値する個人にとって貴重な物と言う認識が米国ではもう既に始まっている。別な言い方をすればプライバシー権の財産権的権利化がすでに起こり始めていると言っても良いであろう。

そこまで国民の認識が高まっていないわが国においても、個人情報・プライバシーに関してはやっと近年マスコミ等でもその話題が頻繁に取り上げられる様になってきた。新たに加わる法規制による制約としての、わが国初の民間分野対象した個人情報保護法の影響である。

今までは、法律という規制枠が無く、ある意味で無法地帯であったわが国の個人情報保護の分野について、法の網が掛かると言うのは、民間の個人情報取扱い事業者にとって非常にインパクトのある出来事であるに違いない。従来から一部では取り組まれてきた、業界別ガイドラインや企業別プライバシーポリシーの掲載等の対象範囲が着実に広がる事を意味する。つまり前述の様に個人情報保護の重要性についての認識を、これまでの様に会社の法務関連部門の社員だけでなく、社長から平社員に至るまでのあらゆる階層の従業員が認識しなければならない状況になる事に他ならない。特に個人情報・プライバシー保護

の問題はモラルベースでの意識が必要な懸案だけに、単に上部からの指示ベースとしての命令等だけでなく、それこそボトムアップとしての意識改革が必要でありこの全社員に均質な品質レベルを求められる課題である。またその取組み効果は、情報システムの改革や決裁上限枠の改訂などと違って、一長一短に組織に浸透するような性格のものではないだけに、その醸成期間を含めた推進の困難さはある意味で他に類を見ないと言っても過言ではないであろう。

それだけトップからボトムまでの一気通貫なモラル維持体制が必要となることはいうまでもない。また当然の帰結として、従来であれば、特定の先進企業が取り組んでいた個人情報保護のマネジメントやそれに対するパブリシティについても、一民間企業として当たり前に取り組まねばならない課題として浮上してきている。

つまり、法律遵守の立場からはそのマネジメントは民間企業として必須であり、かつ前述の様に社員ボトム層からのモラル面での納得性が必要となる。そして内なる取組みとしての企業の自己満足レベルから社会的に糾弾されないための実質保護レベルを維持する為にも、更に、それだけの取組みを企業としてコストを掛けてやっていると言う事実の世間へのパブリシティも必要となって来る訳である。これが、ビジュアルな面でそのアピールとしてのその企業としてのプライバシーポリシーの掲載であり、シールプログラムへの参画という形になるであろう。

一方、その表面的にアピールする外ズラ部分だけでなく、そういったポリシーステートメントを掲げる事について発生する当該企業としての倫理・法的責任についても十分留意する必要がある。

つまり、そういった看板を掲げながら、実態としてそこまでのマネジメントや保護レベルで無かった事が、何らかの事件・事故等で露見してしまった時はその企業が受ける実務的損害・イメージ的損失は莫大なものがあるといっても過言ではないであろう。

しかし、厄介な事にそのビジュアル表示をすることから逃れる事は企業にとってもっと大きいダメージを早期に蒙る可能性があることを画面パブリシティ慎重派の方々は認識せねばならない。

それはオンライン消費者から他社とのホームページ画面との比較をされると言う事である。つまり競合他社がプライバシーポリシーを掲げて、アクセスした初期画面からその保護を大アピールしているのに比べて、それに乗り遅れる事は、今後特に法規制浸透後は、ある意味でビジネスチャンスを失う事を意味する。

実態として、従来より日本国内において平均的に７０％～８０％の消費者が、この個人情報の漏洩が購買意志決定アクセスの一番大きな阻害要因であると言う事実がある。
つぎに最新状況を踏まえたこれからの課題であるが、まず第一が今回の法制化（H13）に伴う分野別課題（個別法の検討と要対象課題）である。具体的には前述の様に
（１）信用情報・金融分野・・・電子マネー・決済&ネットバンキング関連
（２）医療情報分野・・・電子カルテ・遠隔地医療診断等関連
（３）電気通信分野他・・・オンライン・ネットワーク全般含む課題等
である。
これは、それぞれの分野で現状に比して、益々ＥＣのカバー範囲が拡大する事を示している。それによって今回の法制化（H13）の時点の一部積み残し課題を含めて、各分野毎に今までの議論の俎上に上がらなかった様々な課題が出てくる可能性は否定できない。
次に民間分野を初の対象とする個人情報保護法を受けて、民間自主規制のさらなる推進の為の課題として
（１）EC 関連個人情報保護ガイドライン（ＥＣOM含む）見直し・改訂
（２）オンラインＰマーク&チルドレン(高齢者)マーク本格立上・相互乗入
（３）苦情処理・紛争解決手段・窓口検討（ＡＤＲ＝裁判外紛争解決）
が上げられる。
これらの効果は、法制化即ち行政の介入を最小限にとどめる為の抑止力として機能する。つまり法の基本理念を民間企業の従業員ボトム層まで徹底しようとする際の、個別企業への落し込みツールとしても最適である。特に社員が自分達の会社の属する業界団体の特徴を体したガイドライン文面や自社ホームページに掲載されているプライバシー・ポリシーを見るにつけ、内部からの自然な保護モラル浸透効果が期待できる点が挙げられる。
またマーク制度に関しては、やはりウェッブ環境の整備の為の、取得数の増大・普及によるビジュアル面での安心効果という点で重要であり、これからは子供及び高齢者を対象としたスペシャルマーク制度や一部で始められている、国際間での各国独自マークとの連携・相互乗入れがポイントとなってくるのは言うまでも無い。
そしてＡＤＲについては電子商取引の件数・金額の拡大に伴って、クレーム・トラブル件数は益々増加する事が予想されており、行政的・法的な解決ではない、迅速な消費者保護が可能という観点からも特に早期の制度確立が望まれる。
またこれからのＥＣ環境の整備を考えた場合、今回の法規制により、益々、企業に対する

リテラシー＆啓蒙が必要になってくるのは前述の通りである。具体的にＥＣＯＭとしては次のような課題に取り組んでいきたい。

（１）EC の参入Ｇブック（個人情報保護編）＆PP ジェネレーター普及

（２）モバイル分野における個人情報保護と自主規制＆環境整備

これからのＥＣ環境を考えた場合、オンライン消費者（ユーザー側）の拡大と共に、やはり新規のウェッブ企業参入者数の増大推進は発展の重要ポイントである。その為の施策として、新規にＥＣの参入しようとする企業に、今回の法制化を踏まえた個人情報保護の観点から実施せねばならない事柄について分かり易くポイント解説したパンフレット（小冊子）を検討していきたい。また中小のオンラインショップ等でも、ウェッブ上のＱ＆Ａに順に答えていくだけで簡単に情報保護ポリシー＆ステートメントが作成できるツールである PP（プライバシー・ポリシー）ジェネレーターの普及にも取り組む予定である。

また、今後は定置パソコン・インターネット以上に急速に進展・拡大・進展しつつあるモバイル・コマースの分野での個人情報保護は、その位置（ロケーション）情報の認識という特殊性から来る課題を踏まえて、喫緊の課題として浮上してくるのは間違いないと言えるであろう。このため医療分野とも重複する将来のバイオ・プライバシー保護と並んで、電気通信分野と関連したこのモバイル・プライバシーの保護は、今から早急に取り組まねばならない課題の一つと言えるであろう

以　上

■引用・参考記事、資料、文献、ＵＲＬ一覧■（順不同）

●Mainichi Daily Mail Internet :インターネット関連米国記事

●MSNBC　NEXT NEWS :同米国記事

●ＺDNN/USA　NEXT NEWS :同米国記事＆ZDNet/ＵＳＡ関連記事

●, MSNBC & ZDNet/USA）

Copyright (c) 2000 by SOFTBANK ZDNet Inc. All rights reserved

●ZDNN/USA & Inter@ctive Week）

Copyright (c) 1999 by Softbank Publishing Inc. All rights reserved.

●.mainichi.co.jp/digital/netfile/archive **記事&**bizit2.nikkeibp.co.jp **記事**

●個人情報保護担当室関連資料

●個人情報保護法制化専門委員会関連資料

● 電気通信分野における個人情報保護法制のあり方に関する研究会中間報告書」

● 個人信用情報保護・利用の在り方に関する作業部会」作成資料

●経済産業省（情報プロジェクト室）資料「OECD プライバシー・ポリシー・ジェネレーター」について

●ＯＥＣＤホームページ http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm

●国内新聞記事 :その他のネット犯罪及びプライバシー・個人情報漏洩関連事件

●同上 :個人情報保護法関連の動き・事件

●ＥＣ上の消費者情報・プライバシー保護関連についてのオンライン記事（INTERNET Watch／Biz　IT／Biz　Tech／ ITニュース等）

● 通産省の個人情報保護ガイドライン」についての**＜解説書＞：旧通商産業省；機械情報産業**局資料より）

●オンラインプライバシー連合（OPA）関連翻訳資料　URL :http://www.privacyalliance.org

●米国連邦取引委員会(FTC)「1998 年成立の米国児童オンラインプライバシー保護法」関連翻訳資料

●taiga@scientist.com関連資料

●asahi-net.or.jp/news 関連記事＆watch.impress.co.jp/internet/www/article 関連記事

●その他ＥＣ及びプライバシー関連のネット記事・資料及び関連プレスリリースやニュース報道（関連英文記事の翻訳）等

■消費者WG個人情報保護ＳＷＧ名簿（敬称・役職略、企業名５０音順）

委員　金子 稔 アコム(株) 経営戦略部

委員　渡辺 真史(株)エヌ･ティ･ティ･データ 開発本部 ビジネスモデル開発部

委員　真田 幸博 沖電気工業(株) ビジネスソリューション事業部 ソリューション企画部

委員　吉元 利行 (株)オリエントコーポレーション 法務部

委員　野中 雅彦 近畿日本ツーリスト(株) 営業企画室 ﾏﾙﾁﾈｯﾄｾﾝﾀｰ

委員　保倉 豊 グローバルフレンドシップ(株)

委員　石井 忠晴 (株)小松製作所 e-KOMATSU 推進本部 IT 部

委員　大西 雅春 佐川急便 (株) 商品企画部

委員　菅佐原 健一(株)シー･アイ･シー 電子取引研究ﾌﾟﾛｼﾞｪｸﾄ

委員　大野 文治 (株)ジェーシービー 情報通信営業部

委員　本田 拓 大日本印刷(株)Ｃ＆Ｉ企画開発センター･ネットワークソリューション企画開発室

委員　岸本輝昭 電子商取引安全技術研究組合

委員　祝 壮吉 東京電力(株) ｼｽﾃﾑ企画部

委員　横田 博行 (株) 東芝 法務部 法務第二担当

委員　塚本　恵　日本アイビーエム(株)　公共渉外

委員　上野 正之　日本信販(株) 審査本部 個人情報部

委員　野田 泉　日本ユニシス(株)　asaban.com 事業部 ﾋﾞｼﾞﾈｽ開発室

委員　橋本 博喜　株式会社野村総合研究所 社会ｼｽﾃﾑｺﾝｻﾙﾃｨﾝｸﾞ二部

委員　小林 千寿　ぴあ(株)　経営企画本部 EC 推進室

委員　河野 敬幸　日立キャピタル株式会社 株)本社 社長室

委員　伊藤 文隆　株)日立製作所 ﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝ開発本部

委員　赤松 耕治　富士通(株) 法務･知的財産権本部 法務部ビジネス支援部

委員　若林 茂男　三井海上火災保険 株) 総務部 総務グループ

委員　小林 正弘　松下電器産業 株)企業システム本部 ＥＣビジネス推進室

●オブザーバー

関本 貢　財団法人 日本情報処理開発協会 情報ｾｷｭﾘﾃｨ対策室

渡辺 明宏　財団法人 金融情報システムセンター 調査企画部

●ECOM 事務局

事務局　植原総一郎　　電子商取引実証推進協議会 主席研究員

事務局　合原英次郎　　電子商取引実証推進協議会 主席研究員

■文献翻訳　：株）インターグループ

■報告書製作：同　上

2001 年 3 月発行

発行 :電子商取引推進協議会

東京都江東区青海 2－45

タイム 24 ビル 10 階

Tel　03-5500-3600

E-mail　info@ecom.or.jp