H11-消費者ＷＧ　消費者情報ＳＷＧ

ＥＣで取り扱われる個人情報に関する調査報告書（ver.2.0）

平成12年3月

電子商取引実証推進協議会

消費者WG消費者情報ＳWG

1　ＥＣで取扱われる個人情報に関する調査報告の内容について

この報告書の内容は、ＥＣＯＭ（電子商取引実証推進協議会）の消費者WG消費者情報ＳＷＧ（メンバー別途掲載）においての活動成果として、ＥＣにおける消費者に関する様々な課題の中でも、昨今の話題となっているプライバシー保護を含むオンライン上においての消費者の個人情報の取扱いについて、その調査及び分析を行った結果をまとめたものである。

1.1　前回報告書（ver1.0）との関連について

前回分（1999 年 3 月作成）と今回報告内容の兼ね合いであるが、前回報告では、オンライン上だけでなく、リアルの実商売上で取扱われる個人情報も含めて全体的・俯瞰的にこれらを収集することを目的として、

- 各種入会申込に見られる個人情報
- 各種商品購入時に見られる個人情報
- 各種法令・規約などに見られる個人情報の取扱い

を報告の主たる 3 本柱に据えて、いわゆる個人情報と一般に呼ばれているものが、具体的にはそれぞれについて、どのような項目の、どこまでの範囲を含むかを中心に取りまとめた。

そしてその個人情報がどのように収集・蓄積され、どんな利用をされているかについても、実際の各企業へのヒアリング等を通して分析・考察し、オンライン・リアルの双方に亘る項目を基にその一覧表を作成し，これを補完する形で、

- 医療行為に見られる個人情報
- 国際的な個人情報保護に関する技術的取組み

の 2 節を加えた。前者は広義の個人情報そのなかでもハイリーセンシティブ情報と呼ばれる他人に最も知られたくない情報の典型例を紹介した。後者は今後、国際的・技術的な分野での個人情報保護のアプローチでは中心的な存在になるであろう検討事例の紹介であった。

以上のような前回報告の内容を踏まえて、本報告である「ＥＣで取扱われる個人情報に関する調査報告書（Ｖer2.0）」では、その対象となる個人情報の範囲を、EC関連つまりオンラインネットワーク上の商行為で取扱われるものだけに焦点を絞って調査・考察するものとする。

1.2　本報告書「ＥＣで取り扱われる個人情報に関する調査報告書」（ver2.0）の概要とその目的

１．オンライン上の個人情報項目の調査・分析結果報告

第一のテーマとして「EC上の個人情報の抽出と課題整理」（オンライン上の個人情報項目の調査・分析）を行なった。これは具体的にＥＣ上でどのような個人情報項目が収集蓄積されているか

の実態を把握する目的で実施した。

●「ネットショッピング」で取扱われる情報項目調査内容

具体的には「オンラインショッピング」に見られる個人情報項目についての調査･分析について、以下の内容の詳細を記述した。

１．各サイト毎の手続き画面からの個人情報項目のピックアップと調査及び集計表の作成

２．要求項目の分類とモール・サイトのタイプ別・事業者の収集目的別のまとめ等

●「ネットショッピング以外のＥＣ」で取り扱われる項目の調査・分析

下記の項目で取扱われる個人情報について考察した。

１．オンライントレード（証券取引）及びオンラインオークションについて

２．オンライン保険加入について

●「プライバシーポリシー」の調査・分析

そして次にはサイト上に見られる「個人情報保護方針」の個別･具体内容の確認を目的として、有効な環境整備手段・自主規制の一環である、国内の企業サイトの掲示する「プライバシーポリシー」の調査・分析を行なった。次に「ＯＥＣＤ プライバシー・ポリシー・ジェネレーター」 について、その目的及び具体的内容・注意事項について記述している。これらは、これから「プライバシーポリシー」を作成･掲載しようとする企業にとって参考になると思われる。

２．消費者情報保護のための課題整理

二つ目の大きなテーマとして「電子商取引における消費者情報保護のための課題整理」を行なった。まず日弁連シンポジウム資料や（財）日本消費者協会ホームページ資料より、具体的な個人情報保護に関する苦情・相談事例と対策を分析、検討した上で、ネット犯罪及び個人情報漏洩関連事件や情報保護法関連の動き･事件の発生件数集計と内容分類を行なった。

これらが物語るのは、前述した様にＥＣ上の個人情報保護の現状では、やはりまだ不充分であり、行政･企業側も含めた早急な具体的解決策が必要であるということに他ならない。

そしてそれらを踏まえて、消費者情報保護の在り方についての課題検討を行ない、その背景・国際的要請から具体的課題とその課題解決の効果について検証して、下記の内容を記述した。

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

2. 消費者が安心してＥＣに参入出来るような情報保護環境の整備（インフラと技術アプローチ）

3. 消費者･企業双方に対するＥＣ上のプライバシー保護についてのリテラシーの必要性

これらは消費者・企業側の両方が、そのオンライン情報保護に対する意識をさらに高めねばならない事を示している。

３．海外におけるプライバシーマーク制度の調査

大きな活動テーマの三つ目として、海外におけるプライバシーマーク制度の調査を行ない、以下のようなシールプログラム（マーク制度）について翻訳を含めて報告としてまとめた。

●海外マーク制度について

1. BBB オンラインマーク制度
2. ＴＲＵＳＴｅプライバシーマーク
3. 米国公認会計士協会（AICPA）による「CPA ウェブトラストマーク」
4. 「スペインでのデータ保護マーク制度」
5. 韓国での授賞制度：優秀サイバーモール授賞制度

以上の各プログラムのミッションと目的それにプログラムの概要や申込み方法・手順等について紹介・考察した。また参考に国内の民間企業によるオンラインプライバシー保護関連マークについても一部例を取上げて紹介している。これについては、上記の先進事例を学ぶ事で、ＥＣを取り巻く情報保護の環境整備がいかに大切かを各企業の方々に認識していただくと共に、早急に消費者が国内でも安心してＥＣに参入できるインフラ整備の確立ができる事を切に望むものである。

４．全体のまとめ（個人情報保護という観点からの課題整理）

最後に今まで調査・分析及び考察してきた項目の全体のまとめとして

1. 昨今の個人情報の流出事件を見るに付け、やはり早急な法規制の検討の必要性
2. 自主規制については「個人情報保護に関するガイドライン」の周知・徹底と、これに基づく各業界団体による自主的な取組の推進が情報保護の根幹にあるとの認識
3. 国内の情報保護マーク制度が、ネットショッピングの消費者が一般に見るオンラインショップのウェブサイト上には、未だあまり見かけないことへの課題認識と一目見ただけで判る保護マーク等の必要性検討
4. 今後の課題等

を取上げて、消費者ＥＣの更なる発展をめざしての、個人情報保護という観点からの課題認識と提言という形で記述している。

これらのまとめが行政や企業における個人情報保護に向けたさらなる推進及び我々一般消費者の自覚と自己防衛の意識を高めることのご参考にになれば幸いである。

2 「EC上の個人情報の抽出と問題点及び課題整理」（オンライン上の個人情報項目の調査・分析）

2.1 調査･分析の目的について

1999年度の消費者情報ＳＷＧ（サブワーキング）では、まず1番目の活動テーマとして、「EC上の個人情報の抽出と課題整理」を取上げて、オンライン上の個人情報項目の調査・分析をおこなった。

具体的には、オンラインショッピングに見られる個人情報についての具体的調査･分析ということで、まず入会及び購入手続時にインプットもしくは要求する情報項目の調査・ピックアップと各サイト毎の要求項目の分類と一般･特殊（共通･独自）の区分け等のための分析及び集計である。

つまりオンライン上の個人情報に関する取扱い実態の把握のために、サイト上の情報項目やその保護関連データ・記述等の事例収集を行ない、その問題点と課題を整理するのが狙いである。

2.2 課題整理を行うにあたってのベースとなる考え方（「ＥＣＯＭ・個人情報保護ガイドライン」）について

オンライン上の個人情報抽出の前に、ＥＣＯＭ（電子商取引実証推進協議会）としては1998年に「電子商取引に係る個人情報保護の保護に関するガイドライン」を定めている。

このガイドラインが、これから課題整理を行うにあたっての考え方のベースになるものであり、その内容はOECDや通産省のガイドラインの基本要件を満たす内容となっている。

2.2.1 「民間部門における電子商取引に係る個人情報の保護に関するガイドライン」 の特徴（1998.3月策定）

まず「ＥＣＯＭ・個人情報保護ガイドライン」の特徴を、ＥＣ（電子商取引）の持つ特殊性も含めて現状の課題を踏まえて見ていくものとする。

2.2.1.1 「取引」のみならず、広告、宣伝等を一体として扱うことに留意した規定

電子商取引では、アクセスしただけでも個人情報を特定することができることから、単に取引だけに留意すると、個人情報の保護が不十分になる恐れも考えられる。 たとえば、新商品やイベントの案内等マーケティングに使用することを目的にした契約手続を伴なわないアンケート、抽選、懸賞への応募等のために入力された個人情報についても保護すべき個人情報であるととらえ、契約に係る商行為だけに限定せず、「誘引するための宣伝・広告」という契約の誘引に当たる行為も電

子的ネットワーク上で行われる場合は、電子商取引に含め、このガイドラインの対象としている。

2.2.1.2　個人情報の収集、利用及び提供を行う場合の要件と目的の明確化

電子商取引では、電子的ネットワーク上での情報のやり取りを前提として、情報主体（消費者）への通知方法については書面ではなく、ネットワーク上での通知を基本としている（但し、法的な規制のある場合を除く）。

また、個人情報の収集・利用・提供の目的を情報主体に画面上で表示し、同意を得た上で取引を進めることを基本とし、通知しなければならない事項を明確に定めている。また、情報主体以外からの間接的な情報収集及び収集目的内･目的外それぞれの利用･提供についても、それが可能となる場合を具体的に規定している。

2.2.1.3　センシティブな情報保護及び個人情報の開示・訂正・削除の権利と実現方法の明定

電子商取引においても、情報主体の権利の保護を明確にするために、特に情報の主体にとってセンシティブな情報の内容を明確にし、安易な収集を制限している。また、個人情報の収集を行う場合には、当該個人情報の開示･訂正･削除の各権利の存在と当該権利の行使方法を情報主体に通知しなければならないことを規定している。

例えば購入した商品の代金をすでに支払っているにもかかわらず、支払っていないことになっている場合、その誤った情報により情報主体の利益が阻害されることも想定されることから、当該事業者に対して自己の情報の開示を求め、誤った情報を訂正、削除することをもって、情報主体の利益を保護する手段を確保する必要がある。

2.2.1.4　個人情報の適正な管理及び実施責任の明確化

まず、安全な情報のやりとりができる技術的保証が必要である。 さらに、個人情報の取扱に直接関わる従業者に対する責務について規定するとともに、個人情報の管理者に対する責任についても具体的かつ詳細に規定している。 また、近年の情報化の進展に伴い、事業者における情報処理業務がますます多様化、複雑化していることから経営の効率化や顧客サービスの向上等のために情報処理業務を外部に委託するケースも多くなっている。これら外部委託の増加に伴い、情報処理の委託先における個人情報の処理に関してトラブルが生じることがないよう必要な措置を講ずるべきである。委託先の選定に当たっては、各省庁で規定している安全対策基準を遵守できる

など基準を設け、委託先との契約において、責任の範囲、秘密の保持、外部への提供の禁止、委託処理機間等の明記、処理終了後の個人情報の返還あるいは破棄等を取り決めることが必要である。

2.2.1.5　個人情報の取扱になれていない事業者を想定

電子商取引には新たに個人情報を取扱う事業者が参入してくることが考えられ、販売の主体が企業のみならず個人の場合も多いことに留意した規定となっている。

2.2.1.6　子供に関わる個人情報の保護

パソコン操作性の向上やパソコンが学校教育のカリキュラムへ組み込まれることに伴い、子供でも簡単に電子的ネットワーク上で商品・サービスの売買やアンケートへの回答を行うことが可能となる。こうした状況を利用し、子供から、本人や親の個人情報を収集することが生じる。子供は必ずしも個人情報の収集及び利用についての認識が十分ではないことから、なぜ情報が必要なのかわかりやすく誤解を生じない表現で説明するなどの慎重な取扱いを求めたものである。 さらに、子供やその親が、自分の知らないところで不利益を被る懸念があることから、「子供に個人情報の入力を求める場合」は、収集する前に保護者に事情を説明し、了解を得る機会を与える配慮も必要としている。 また、子供が入力した個人情報から子供及び親が不利益を被らないようにするために、保護者に対しても同等の権利を認める。

以上がＥＣＯＭの「電子商取引に係る個人情報保護の保護に関するガイドライン」（1998 年）の代表的な特徴項目であり、これからの様々な検討･考察のベースとなるものである。

2.3　オンラインショッピングに見られる個人情報項目についての具体的調査･分析について

次にオンライン上の個人情報の具体的な抽出作業にあたっては、インターネット上のモールやショップの申込み･購入画面を各々チェックしていった。以下はその手順である。

まずインターネット上でのショッピング時において入会や商品購買などの手続きを行なったときに、ネット上のモールまたはショップより要求される個人の属性項目情報の調査を行なった。

2.3.1　調査方法とその手順

現在、電子商取引を行なっているモールを任意に抽出し、日常的に消費者が、ショッピングする段階でモールもしくはショップに登録しているプロファイルがどんな内容なのかを調査した。

具体的には、モールへの入会や商品購入申込み等の段階でのサイトからの要求画面を収集調査することにより、モール企業・オンラインショップがどういった個人情報を求めており、また入手しているかを調査する。

- 入会及び購入手続時にインプットもしくは要求する項目の調査・ピックアップ
- サイト毎の要求項目の分類と一般･特殊（共通･独自）の区分け
- 調査及び集計

実際の調査の際は、 20 個所以上のモール・ショップの事例を収集する。収集結果を一覧表にまとめる。

- サイトの種類をキーにした個人情報属性項目のマッピング

調査及び集計で作成した一覧表を元に、サイトごとに共通して必要としている項目を明らかにし、どのような情報を必要としているかを明確にする。

- サイト側の収集目的をキーにしたと情報項目のマッピング

業界によって収集を行なっている情報の種類を分析すると共に、その傾向を明確にする。

- 上記の作業を通じた項目の一覧表作成と各業種・各目的別の考察・まとめ

2.3.1.1　入会及び購入手続時に個人情報を要求するサイトのリストアップ

ECOM ホームページにリンクしているショッピングサイトを中心に 20 サイト以上をネット上から任意抽出する。

内訳としては大手企業のモールから中小モール、それに単一ショップのサイトまでをカバーしてみた。

2.3.1.2　要求項目の分類と各サイトに共通かそのサイト独自かの検討及び必須項目か任意項目かの検討

- 共通→本人属性情報項目等（大体のサイト必須）
- 独自→職種・年収・世帯・最終学歴・勤務先項目等（任意のケースが多いもの）

その他、インターネットにアクセスする場所・パソコンの種類それに興味のある分野・商品の届け先情報等が独特項目となる。

2.3.1.3　その他オンライン独特のものかリアル（実商売）上も共通かの検討。

- オンライン（コンピュータ処理･ネットワーク関連）独特の項目
- リアル（オフライン･実商売上）でも見られる項目

  以上に分類して各項目の検討も行う。

2.3.2　ＥＣ上（オンラインショッピング時に収集・登録）の個人情報調査内容

実際の調査段階では、ＥＣＯＭホームページからリンク可能なサイトを中心に約25のモールと各モール 2～3 箇所のショップをピックアップして、その登録時や購買時の入力画面でのインプット項目を収集し、収集結果を一覧表にまとめた。

2.3.2.1　対象ショッピングサイト&モールのリストアップ〔ＥＣＯＭ／ＨＰリンク分〕

1.女性向けの素敵な街「まちこ」（Communication & Shopping Town）

2.CCC（サイバー・コマース・シティーコンソーシアム）

3.メディアポート日本（名古屋情報センター）

4.V-City（バーチャルシティ構想）

5.J-PLAZA（大和総研）

6.電活クラブ（野村総合研究所）

7.JUSTNET SHOPPING MALL（ジャストシステム）

8.Amazon.com

9.Nmart（富士通）

10.京都「アメリカ衣料の岸本屋」

11.生活情報館マリネットランド（丸紅）

12.栃木県物産店街（IBC）

13.&s（アンズ）（さくら銀行）

14.Max Market（伊藤忠インターネット）

15.TOPPAN SECURE MALL（凸版印刷）

16.サイバーウイングクラブ(東芝情報システム)

17.Curio City（三井物産）

18.InfoMarina（セコム）

19.fiesta（日本 IBM）

20.楽天市場（Ｒａｋｕｔｅｎ）

21.ショッピングワールドウェブ Shop（ＮＥＣ）

22.The Super Mall(フジサンケイ・エレクトロニック・コマース実験協議会)

23.わしたショップ（沖縄県物産公社）

24.Bargain America

25.EC ショップ沖縄（沖縄商工会議所）

2.3.2.2　調査及び集計表の作成

まず各個人情報項目毎に、それが大部分のサイトで共通な収集項目かそれともその一部サイト独自な項目かの分類が一つ。

それから二つ目は、その項目がリアルの商売（オンラインでない実社会上の商取引）でも共通かそれともオンラインショッピング独特の項目かの区分けを試みた。

以下がまとめた一覧表である。

項　　目	サイト共通	サイト独自	リアル共通	オンライン
1.氏名	○		○	
2.フリガナ	○		○	
3.郵便番号	○		○	
4.住所	○		○	
5.自宅電話番号	○		○	
6.Ｅ－メール アドレス	○			○
7.性別		○	○	
8.生年月日		○	○	
9.勤務先番号		○	○	
10.勤務先内線		○	○	
11.パスワード		○		○
12.配偶者有無		○	○	
13.子供		○	○	
14.サイトを 知ったきっかけ		○		○
15.インター ネット歴		○		○
16.利用通信 回線		○		○
17.生活の 関心事		○	○	
18.会員番号	○		○	
19.ＦＡＸ番号		○	○	

20.ショップからのメール受取		○		○
21.クレジット番号	○		○	
22.カード有効期限		○	○	
23.希望商品	○		○	
24.数量	○		○	
25.支払い回数	○		○	
26.登録電話番号		○	○	
27.連絡先電話番号		○	○	
28.ログイン名		○		○
29.カード会社		○	○	
30.カード名義		○	○	
31.希望ハンドル名		○		○
32.届日指定		○	○	
33.届け先氏名	○		○	
34.届け先住所	○		○	
35.届け先電話	○		○	
36.届け先Ｅメール		○		○
37.選択商品情報		○	○	
38.ご意見		○	○	
39.職業		○	○	
40.職種		○	○	
41.年収		○	○	
42.世帯		○	○	
43.最終学歴		○	○	
44.インターネットアクセス場所		○		○
45.使用コンピュータ		○		○
46.日中の連絡先（ＦＡＸ）		○	○	
47.勤務先名		○	○	
48.挙式（予定）年月日		○	○	
49.年齢		○	○	
50.業種		○	○	
51.年齢層		○	○	
52.趣味		○	○	
53.職位		○	○	
54.パソコン		○		○

利用経験				
55.使用接続サービス名		○		○
56.関心のある接続サービス名		○		○
57.よく使う検索エンジン		○		○
58.好きなホームページ		○		○
59.よく使うホームページ		○		○
60.興味のある分野		○	○	
61.希望する連絡手段		○	○	
62.呼び出し希望時間		○	○	
63.勤務先住所		○	○	
64.所属部署		○	○	

●以上の様に、個人情報項目としては「住所」・「氏名」といった基本的な属性項目から、「呼び出し希望時間」・「勤務先の住所、所属部署」にいたるまで、合計 64 項目におよぶ個人情報が任意インプットやアンケート形式も含めてサイト側から要求されている事が判る。

●次に上記の表の中でも特にオンライン（ＥＣ）に特有の情報項目について、次にさらに細かく見ていくものとする。

2.3.3　ＥＣにおける個人情報の特徴

ここでは、リアルの実商売ではなく、オンライン上の電子商取引で取扱われる個人情報に限って見ていくものとする。

2.3.3.1　パソコン関連情報

まず、当然の事ながらパソコンを通してのオンラインショッピングという事で、このＰＣ関連についての情報項目が挙げられる。

具体的にはEメールアドレス、パスワード、ＩＤ、ハンドル名や使用コンピュータ、アクセス場所、インターネット歴それに利用通信回線、接続サービス名、好きなホームページ名等である。

なかでもメールアドレスやパスワード、ＩＤ等は必須記入項目でその他の項目は任意記入項目と

なっているケースが多い。

2.3.3.2　購入前に収集される個人情報（無意識提供情報）

次に特にオンラインショッピングの特性を一番良く表す情報項目として、前述の一覧表の様に消費者に事前明示されずに、商品購入以前から、ユーザーの気付かないうちに収集されている（無意識提供している）情報項目を下記に列挙する。

(1) アクセスログ

これについては、ユーザーがネットサーフィン（カタログブラウジング）しながら買いたい商品に行きつくまでの過程がプロバイダーのコンピュータには記録されている。

つまり購入意思決定に至るまでのプロセス情報がユーザーの知らない間に蓄積されているという事実がある。

例えばオンラインサービスのプロバイダーであれば、加入の特定顧客の通信相手やログイン時刻、それにメール頻度などがアクセスログとして残り、またインターネットサービスのプロバイダーであれば、特定ユーザーのアクセスサイト・興味のある記事、それに購入に至るまでのネットサーフィンの順番が記録（アクセスログ）として蓄積されている。

(2) クッキー等の使用

さらにクッキー（サーバー側から送りこまれたプログラムでブラウザ側の情報を送り返すもの）等の使用により、ユーザー（ネットサーファー）がどの広告を見たかといった個別情報がサーバー側で分かる仕組みもある。これは即ち、マーケティング的観点から言って見込み客情報の事前把握に他ならない。

2.3.3.3　加工･データベース化の容易さ（デジタルデータの特性）

オンラインデータではユーザーからインプットされた個人情報がそのままデータベース化可能で、ハードコピーによる情報と違い、再インプットの必要がないというのも特徴の一つである。

またデジタルデータの特性として、蓄積情報の瞬時加工・検索・移転等が可能なのはもちろんであるが、その裏返しとして悪用された時の危険度はより一層高くなる事も認識せねばならない。

2.3.3.4　ユーザーとサイト（企業）側のダイレクトで継続的な顧客接点

生情報の把握、顧客のアフターフォロー、利用アンケートの集計等が容易でしかも低コストで可

能である。

つまり、広範囲･確実な見込み客（新規顧客予備軍）情報の蓄積が、国や地域の制限無しに可能になった画期的な手法といえよう。

2.3.3.5　まとめ

以上の様にＥＣ上の個人情報は、その取扱い方によっては顧客側も企業側にもメリットの出るいわゆる「One to One Marketing」（欲しい人に欲しいものを効率良くお知らせし、お届けする）が可能となる貴重なデータ源である。

その一方で、前述の様にＥＣ個人情報は、そのデジタルデータとしての特性が故に、容易に、大量に、一瞬にして、情報主体の知らない間に流出･漏洩する可能性もあるという事である。

つまり企業側としては、顧客情報の収集･管理にとくに注意すべきであるし、ユーザー側もそれらの光と陰を充分熟知していなければならない。

2.3.4　モール・サイト別考察

次に各モール及びショップが持つ性質からくる個人情報項目の特徴について見てみた。

A.　大規模モール

会員本人のアクセスのためのパーソナル情報（ＩＤ・パスワード等）と一般的な属性情報（住所・氏名等）・連絡先項目（Ｅ‐mail アドレス含む）の他に年齢・性別・既婚／未婚の別・職業などが求められる。

またオプションとして職種・年収・世帯・最終学歴などのプライバシー情報やアンケート形式で興味のある分野（ビジネス・ファッション・グルメ等）が聞かれる事もある。

またネットワークに関しても、インターネットへのアクセス場所・パソコンの機種・使用中や関心あるネットサービス名・よく使う検索エンジン・好きなホームページまで記入欄のあるサイトもあった。

B.　地域モール

大規模モールに比べて、モール会員への申し込み時に個人情報の要求項目が一般に少ない。

理由として考えられるのは、モール設立の目的がその地域性を活かした特定商店・商品の物販に限られており、大規模モールのような個人情報の 2 次利用（マーケッティングデータとしての活用）の意図が少ないからであろう。

C. 集合モール

地域モールと同じく、個々のショップの集合体のためモール全体としてのマーケッティング情報の収集とかいった意図は見られず、会員登録というより直接個々の店での登録が、そのまま次回の注文時に再活用されるパターンである。

D. 単一ショップ

基本的には地域モール等と同じだが、個人情報の取り扱いとして見た場合、特色としては会員登録というような手続きは必要でなく、注文・発注のための最低限の情報インプットという色彩が濃い。

但し、特定商品に関しての銘柄指定等、詳細な情報項目が求められるケースがある。またＥ‐mail のアドレスを必須記入項目にしているところも多い。

2.3.5 事業者の収集目的別考察のまとめ

カテゴリー	A	B	C	D
1．アクセス情報	○	○	○	○
2.連絡先	○	○	○	○
3.本人確認	○	○	○	○
4.職業・収入	○	○	△	×
5.興味分野	○	△	×	×
6.その他詳細	○	△	△	△

○＝必須の要求項目、△＝中には要求するケースありの項目、×＝要求ケース無しの項目

- カテゴリーA…アクセス情報の登録、入会申の手続き項目の中に、連絡先・本人確認レベル以外に任意ではあるが、マーケティング活用の為かかなり詳細な情報項目を求められる。（大規模モールに多い）
- カテゴリーB…Aよりも要求項目は少なく特定地域に限られた内容を求められる。（地域モールに多い）
- カテゴリーC…この場合、モール全体としてのマーケッティング意図はなく個々のショップの必要項目だけに限定。（集合モールのケース）
- カテゴリーD…入会手続ではなく即購買手続きとなる。さらに特定商品についてはかなり突っ込んだ情報項目が求められる。（単一ショップ）

2.3.6 個人情報保護に関する記述に対しての考察

今回の（1999年 5 月時点での調査情報）をベースに、その時のネットショッピングでの入会の手

続時に、モール・業者側から提示される個人情報の保護に関連した文面・約款の考察を試みた。

個人情報保護に関する記述があるサイトのうちで、この件に関して一番しっかりしていたのは、前記のカテゴリーでいうＤに属するの輸入衣料品を扱う単一ショップであった。

ここでは申込みの欄に〔個人情報保護〕というリンクを設けて、そこを開くと〔●お客様個人情報の保護、保全について〕というタイトルで下記の内容が記載されている。（詳細後述）

1. “どんなことがあっても絶対に外部にお客様個人情報を漏らしません”という項目欄にその会社の保護ポリシー・考え方を会社の代表者名で宣言している。
2. その他オンラインショップ初心者が抱く不安への対応、また望んでいないDMのストップ等、2 ページにわたって個人情報秘諾義務の遵守を明確にしている。

普通の例だとモールの会員規約の中に、会員情報の取扱いについての項目が入っており、そこに 5，6 行程度の個人情報保護の遵守規定が記載されている。

中には通産省の〔民間部門の個人情報保護のガイドライン〕を遵守すると明記しているモールもあった。

ただ集合モールのような寄り合い所帯的なところでは、そのモール全体を管轄するルール作りが出来ていないため、モール自体の個人情報保護の意思表示が見られないケースもあった。

また逆に個人情報を会員企業に提供する旨の同意を得る記述をしているモール規約も見受けられる。

特に注意を要するのは、自分個人の登録情報だけでなく、贈呈品の申込み等においては、送付先の連絡情報（他人の個人情報）が一緒に提供されていると言う事実も見逃してはならないポイントである。

2.3.6.1　クレジットカード情報等の提供について

次にやはり消費者にとって最も気に掛かる個人信用情報入力であり、カード会社名・名義・番号・有効期限等のインプットをさせる場合については、事前にほとんどのモール・ショップが採用セキュリティの方式（ＳＳＬ／ＳＥＴ）をオープンにしている。

但し、中には個人情報の保護方針やセキュリティレベルが明示されていないサイトもあり、消費者としてそういった所については、特に個人データのインプット前に充分な注意が必要である。

2.4　その他のネット取引で収集・蓄積される個人情報についての調査

続いてネット上の取引の中でショッピング以外のもので最近脚光を浴びている、オンライントレー

ド（証券取引）及びオンラインオークションそれに話題となっているオンライン保険を取上げて、そこで収集登録される個人情報について調査報告及び紹介するものである。

2.4.1　オンライントレード（証券取引）について

大和総研等の資料によると、1998 年末の手数料の完全自由化から、オンライン証券取引サービスがさらにビジネスチャンスとして注目されてきている。96 年 4 月に大和證券が日本で初めてオンライン取引を開始して以来、各証券会社では次々とサービス開始に踏み切り、その他の業界も含む参入企業は益々増加の一途である。特に証券と直接関係の無い異業種や外資系企業の参入が相次いで発表されるなど、業界の枠を越えた激しい競争が起こっている。オンライン取引が爆発的に普及した米国では、1999 年度ですでにリテール取り引きの約 3 割以上がオンライン経由で行われているといわれており、日本国内でもオンライン取引を実際に業務として行う証券会社がサービスの拡充やキャンペーンを頻繁に行う一方で、一般投資家などに対して情報提供を行うなどの周辺サービスも次々と誕生してきている。

2.4.1.1　日本のオンライン証券取引の概要

前述のように、インターネットを利用した個人のオンライン株式取引は、手数料自由化で急拡大しており、証券会社だけでなく、外資系企業や異業種企業からの参入、日系金融機関と外資系企業の提携など、規制緩和をバネにした動きが盛んである。９９年の 11 月現在でネット取引を取扱う証券会社の口座数を日本経済新聞が集計したところ、すでに９９年の 10 月末の時点で 30 万超と９月末に比べて 5 割強の増加である事がわかった。

このようなオンライントレードの特徴として、前述の大和総研等の資料によると

1.低コスト

通信回線としてインターネットを利用しているため、通信費が安価。

コンピュータによる受注のため人件費や間接部門の負担が小さい。

2.リアルタイム性

その時点での株価、ニュース等の情報をリアルタイムに提供できる。

注文、売買結果、資産内容などのその時点での取引情報を把握できる。

3.随時性

証券会社の店舗・営業時間に合わせる必要が無く、どこからでも 24 時間利用可能であるなど、時間･場所の制約がない。

4.情報処理能力

検索機能（企業の株価・企業情報・ニュースなどの多くの情報の中から必要な情報を瞬時に読み出す事のできる働き）を利用できる。

5.ハイパーリンク機能（ウェブ上にある様々な情報を利用可能とする働き）が使える。

過去のパフォーマンスの確認、資産内容のチェック等を記録しておく事が可能。

6.インタラクティブ性

一方的な情報提供でなく、顧客ニーズに合わせてカスタマイズしたサービスが提供できる。

マーケティング面で有効性を発揮する。（顧客の属性に基づいて、最も有効と考えられる商品を提示していくなど：One To One Ｍａｒｋｅｔｉｎｇへの応用など）。

このほか、全体の傾向で注目されるのは口座数と手数料収入が伸びてきたことで、オンライン取引サービスがすでに本格的なビジネスとして立ち上がってきたことを示しているという点だ。

以上のような状況から大和総研等の判断でも、オンライン証券サービスは個人向けのインターネットサービス（ISP 除く）のなかでもビジネス規模は群を抜いて大きく、日本の EC を牽引していく中心的な存在になりつつあるとみている。

2.4.1.2　情報項目の調査･分析

こういった背景からＥＣ上の個人情報保護を考える場合、ＥＣ全体への影響力という点から見て、これまでの「オンラインショッピング」だけのケースでなく、上記の「オンライン証券取引」及びその他のＥＣ新潮流についてもその中で取扱われる情報項目の調査・考察を加えるものとする。

まず、「オンライン証券取引」についてであるが、取引の前提としてまず消費者側として「口座開設」の登録があげられる。

そのための必要書類としては業務上、法規制を踏まえて揃える必要のある

1.証券総合取引口座申込書

2.実質株主報告名義届出書

3.上場株式等に係る譲渡所得の申請書または上場株式等に係る譲渡所得等の源泉分離課税の選択申告書（どちらか一方）

4.本人確認書類

- 運転免許証、住民票、印鑑証明書、健康保険証、転出証明書、
- パスポートのうちいずれか一通の写し

これら以外にオンライン上で申込み時にインプットする個人情報項目としては通常のオンライン

ショッピングでの項目以外にも

1.投資経験（株式・投資信託・中期国債ファンド等）

2.投資目的（元本安全性・安定収入・キャピタルゲイン等）

3.口座開設の動機（営業時間・取引コスト・非対面取引・初心者等）

4.口座開設者本人名義の銀行口座内容

5.自宅以外の連絡先（緊急時使用）

6.内部者登録

この 6. はインサイダー取引を防止するための登録で、会社関係者（当該組織の運営、業務、財産等の重要・未公開情報を知りうる立場の者）に該当する場合は、その会社名・株式銘柄コード・関係区分・役職名を記入するものである。

2.4.2　考察

以上の様にオンライントレードにおいては前述の様に、法律上の必要性から個人の金融・信用関連情報の一番詳細な内容がインターネット上でやり取りされることになる。そのため、その収集･蓄積情報についての安全な管理はもちろんのこと、事前登録時に情報主体に対して、その取扱い及び活用範囲等についてもきちんとした明示と同意を取付ける必要があろう。

特にマーケティング面から見て、収集情報内容をベースにしたオンライン以外の実商売（証券マンによるフェイス･トゥ･フェイス）への展開が可能な事から、サイト側はオンライントレード上で収集した個人情報について、収集･利用及び提供を行う場合の要件の明確化が前提条件となることは言うまでもない。

また当該サイト（事業主体）がシステム運営において、自社あるいはグループ企業のシステム部門で行っているケース以外にアウトソーシングという形で証券会社系以外のシステムベンダーに委託する場合など通常の取引以上に厳重に契約等により個人情報の適正な管理が求められる。

また現状での課題、苦情･クレーム等として挙げられるのは、Ｗｅｂファイナンスニュース等によると、

1.国内では「対応が遅い」：書類発送、口座開設、注文受付等に関して

2.同じく「つながらない」「画面が表示されない」「応答遅い」等

3.一方、海外では＜Ｅ*ＴＲＡＤＥ＞が 2 月に起こしたシステムダウンの法廷論争で、同社の「安全性・信頼性・迅速性」の欠如に関する契約不履行の訴訟で、4 万ドルの罰金を支払う命令が下った。

等である。

したがってまだオンライントレードという制度自体の勃興期にあたるため、個人情報保護についての直接的なクレームはないが、中には株取引の事を知らないコールセンターのオペレータが、「いくら入金したのですか？」とか「暗証番号は？」等々のあきれた質問が帰ってくるケースがあるという。

いずれにしてもオンライン証券会社側として、しっかりした個人情報保護の社内システムの整備及びプライバシー保護の為の「コンプライアンスプログラム」の実施等の早急な体制確立が急務な業界であろう。

というのもオンライントレード自体のビジネス規模の大きさに比例して、個人信用情報を中心にオンライン商取引（消費者ＥＣ）の中においても、最大の顧客データベース（個人情報項目の豊富さ）を有する可能性のある業界だからである。

2.4.3　オンラインオークションについて

次に同様にインターネット技術の活用により、これまでの口頭オークションの限界であった、参加者の制限、場所の制限、時間の制限を緩和し、だれでも、いつでも遠隔地からのアクセスを可能にしたオンラインオークションも発展の兆しを見せており、電子オークションというホームページにはすでに 15 以上のオークションサイトが名を連ねている（1999 年 6 月時点）。

このオンラインオークションについてであるが、このビジネスへの登録・申込みについて調べてみると、ほとんどの情報項目がオンラインショッピングでの個人情報インプット項目と同じである。

但し、オークションの特徴として入札（ピット）の登録時に、匿名に自分のわかる言葉を入力することにより指名を、主催者側以外に公開せずに参加することができるという制度がある。

ちなみに大手のオークションサイトはショッピングモールの一部として運営れている事から、モールへの会員登録画面と兼用しているケースも多い。

このことからオンラインオークションについては通常のオンラインショッピングと同程度の管理レベルのサイトがほとんどである事がわかる。

2.4.3.1　＜オンラインオークションの世界は危険がいっぱい＞の記事

ただ消費者保護という点では、次ぎのような警告記事　（ZDNet/USA）も出始めている。

サイバー詐欺の被害者は分刻みで生まれているという報道は嘘ではない。だが，オンラインオークションサイトの詐欺防止は，買い手と売り手だけに課せられた責任ではない。

信用しすぎてしまうオンライン入札者のために，大手のオークションサイトはどこもシステムに保護手段を組み込もうとしている。Amazon.com と eBay は 250 ドルまでの無料入札者保険を提供し，外部の第三者預託サービスも利用しやすくしている。

しかし、第三者預託サービスは 高額な場合が多く，取引額に数百ドルが加算されることもある。このため，ほとんどの入札者は，リスクが増えることになってもこのサービスを利用しないため、オークションサイト自らが，社内で第三者預託機能を用意し，低料金で利用できるようにするべきだとの意見もある。

米連邦取引委員会（FTC）の報告によると，この 1 年でオンラインオークション詐欺に関する苦情は 20 倍に増えたという。

2.4.4　考察

この記事を見ても解るように、現時点でのオンラインオークションにおいての緊急な課題は、個人情報保護というより、それ以前の問題としてサイト側の事業者適正の如何が詐欺･詐称等の増加と共に浮上している段階である。

ただプライバシー保護という観点からは、「どこそこの誰が何をいくらで買おうとしているか、また予算幅はこれだけ持っている」といったセンシティブな情報がサイト側に容易に蓄積されていると言う事実も見逃してはならない問題である。

そしてこの貴重な情報の二次利用と言う観点も含めて、オンラインオークションサイトとしての個人情報保護に対する考え方等に課題の中心が移るのもそれほど遠くない事であろうと思われる。

従って、今の段階から個人情報保護ポリシーの確立・運営及び暗号等によるシステム保護レベルの強化等が求められるのはもちろんである。

2.4.5　オンライン保険について

つぎにネット上での勧誘･申し込みが始まったオンライン保険での個人情報の取り扱いについて見てみる。

2.4.6　オンライン会員を対象としたネット完結型保険商品販売での個人情報

オンラインプロバイダーが、その提供オンライン上において、199 9 年後半から保険の販売サービス「オンライン保険」を開設している特例がある。

このオンライン保険では、クレジットカードで利用料金を支払っているオンライン会員を対象に、ID とパスワードを利用することで申込みから決済までオンラインで取引を完結できる。

このサービスはオンライン会員を対象に、簡単な手続きのみで保険商品を販売するものであるが、会員は保険契約の際に、オンラインのＩＤとパスワードを利用することで、保険会社との書類のやり取りが不要で保険代金の決済までオンラインで行える、ネットワーク完結型の保険商品の購入が可能となる。

即ちオンラインプロバイダーは、「オンライン保険」の提供により、従来は申し込みから契約まで時間と手間を要した保険購入のプロセスを簡便にし、利用者にとって身近な保険サービスの販売を可能とした。これは会員向けの保険商品を準備して他社との差別化を図り、新たな付加価値をオンライン会員に提供していくことで最大手プロバイダーとしての地位を確保しようとするものである。

また、この際のネット上での代金決済システムをについては、個人情報保護のための配慮がなされており、下記の特徴がある。

●オンライン利用料金と一緒に決済

ショッピングした代金は、オンラインの利用料金と同 じクレジットカードで決済される。

このため、サービスの利用はオンライン会員で料金の支払いにクレジットカードを指定されているメンバーとなる。

●インターネット上にカード番号の情報は暗号化されたもの以外流れない。

買い物時には、今使用中の ID、パスワードを用いるため、インターネットに大切なカード情報が流出する心配は一切ない。こういったシステムだから、安全にショッピングをすることができる。

セキュリティが保たれる。

セキュリティを保つために SSL（SecureSockets Layer protocol）を使用。利用にあたっては Microsoft Internet Explorer、NetscapeNavigator など SSL 対応ブラウザーを使用が条件である。

2.4.7　考察

この説明から解るのは、消費者にとっては「オンライン保険」という新商品をネット上でショッピングする事に等しい（ネット完結タイプ）わけなのである。

つまり文中にもあるように、会員は保険契約の際に、オンラインのＩＤとパスワードを利用することで、保険会社との書類のやり取りが不要で、クレジット番号等の個人情報がネット上に流れずに、保険代金の決済までオンラインで行える、ネットワーク完結型の保険商品の購入が可能となる。

ここで事前に収集されることが前提となる個人情報については、オンライン会員になる時に既に登録される情報項目と保険購入申込み時に再度インプットする情報項目からなる。

もちろん、オンライン保険が申込み可能なのは、既に会員の中でも会費の支払いをクレジット決済している消費者だけが対象である。

その前提となる会員申込み時に必要な個人情報項目は、氏名・性別・生年月日・自宅住所・電話番号等の一般的な属性情報に加えて、センシティブなカード情報（本人カードに限る）が必要である。すなわちカードの種別・カード番号・有効期限である。

このオンラインへの入会作業は、その申込み画面で一括して可能であり、会員規約を目視確認の上でボタンをクリックすればすぐその申込み画面となる。このやり取りには、やはりセキュリティの確保のため SSL を利用している。

またこのサイトでは入会案内と同じページに「個人情報の保護ポリシー」へのリンクがあり、自己情報の取扱いについて不安な消費者はその保護ポリシーを確認できる様になっている。

そして実際のオンライン保険初申込み時には、再度クレジット情報以外の個人一般属性情報の提供が求められる。

2.4.7.1　オンライン会員規約（参考＊代表例）の考察

次にオンライン保険に加入する要件として、オンライン会員入会申込みの段階で、消費者として事前確認することが前提である会員規約（特定会社の代表例）を考察する。

この中で、個人情報の保護という観点からいくつかの留意点があるのでそれを見ていきたい。

まず会員規約の「会員の義務」について「ＩD及びパスワードの管理責任」では「会員は自己のＩDおよびこれに対応するパスワードの使用および管理について一切の責任を持つものとします。」それと「オンラインプロバイダーは、会員のＩDおよびこれに対応するパスワードが他者に使用されたことによって当該会員が被る損害については、当該会員の故意過失の有無にかかわらず一切責任を負いません。」と明確に規定している会員規約が一般的である。

従って、自己のＩDおよびこれに対応するパスワードの盗難による責任は、基本としては建前上は、オンラインではすべて消費者側で負うものとなっている。

それから「個人情報・通信の秘密」については、会員の個人情報を、「別途オンライン上に掲示する“個人情報保護ポリシー”に基づき、適切に取り扱うもの。」として、また会員の個人情報を、「サービスの提供以外の目的のために利用しないとともに、第三者に開示、提供しないものとします。」と規定している。

ただ、問題はその第 5 項で「会員の個人情報の属性の集計、分析を行い、個人が識別・特定できないように加工したもの（以下「統計資料」という）を作成し、新規サービスの開発等の業務の遂行

のために利用、処理することがあります。また、オンラインプロバイダーは、統計資料を業務提携先等に提供することがあります。」と明記している点である。

さらに「通信の秘密」の項等で「会員のサービス利用記録の集計、分析を行い、統計資料を作成し、新規サービスの開発等の業務の遂行のために利用、処理することがあります。また、ニフティは、統計資料を業務提携先等に提供することがあります。」と規定しているのを見かけるが、何よりこの「統計資料」という定義が一番のポイントである。

その項の定義によると「当該個人情報を個人が識別・特定できないように加工したもの」とあるが、そのレベル・内容によっては、提供された側がマーケティングデータとして活用したいと意図する場合は、どうしても個人特定が必要なニーズが出てくる。

こういう場合には、当然の事として「個人情報の属性項目及び利用記録」のその“統計資料”としての加工レベル･内容の範囲が問題となってくる。

つまりどの程度までが“属性情報”で、どこからが“統計資料”かのボーダーライン・境目がポイントである。もちろん情報を提供されるマーケッティング側のニーズとしては、一般的な単なる統計資料ではなく、“One to One Marketing“の実現に向けて、より個人の属性情報に近い形でデータを入手したいのは当然であろう。

そこで“サービス利用記録の集計、分析”の内容が、マーケッティング側のニーズに屈することなく、その統計資料としての独立性をいかに保てるかを最大の焦点として、各プロバイダー業者はこれら顧客データの集計・加工・管理に充分、留意して欲しいものである。

2.4.8 「損害保険会社のオンライン直接購入商品」と個人情報

つぎにプロバイダーへの加入申込み及びそのネット上のオンライン商品としての損害保険の購入というパターンとは別に、その商行為自体としてプロバイダーを介さずに消費者が直接アプローチして購入・加入するパターンである「特定の損保会社のオンライン保険商品」の申込み時に収集される個人データについて見てみる。

損保会社の中には、見積りから申込みまでウェブサイト上で完了するスピーディーで簡単な契約手続きを実現しているところがある。 ユーザー登録をすれば、あとはすぐに見積り、そして納得すれば、そのまま申込みへということで、郵送による書類のやり取りは必要なく、支払い手続きも完了というものである。

コンテンツ確認には、ユーザー登録が必要。「GO」ボタンをクリックして、ユーザー登録後、自分の専用のページが表示。そこから再度「見積り・申込み」をクリック。ユーザー登録後は、見積り条件

を保存でき、保存してから約 1 年間いつでも確認可能というものである。

(1) インプットする情報項目内容

- 何をご見て、このサイトを知ったか。（ひとつだけ選ぶ）
  - インターネット
  - 新　聞
  - 雑　誌
  - テレビ衛星放送
  - その他
- あなたの E メールアドレス
  - （半角英数字）
  - 確認のためもう一度入力
- パスワード
  - （半角英数 6 文字まで）
  - 確認のためもう一度入力
- ウェブエージェントがあなたに呼びかけるニックネームを登録（全角可）
- 万が一、パスワードを忘れてしまった時も、入力した質問とその答えを登録しておくことで、いつでもご確認可能というパターン登録
  - 質問: 例）好きな言葉　、答え: 例）愛と信頼
- 今後、損害保険株式会社、及グループ各社より、E メールにてご案内をしていいか？（はい、　いいえ）

(2) 顧客のパーソナルライフにマッチした情報を届けるためのアンケート（追加記入情報）

- お客様について
  - 性別
  - ご職業
- 配偶者様について
  - ※ご結婚されている方のみお答え。
- ご職業
- お子様について
  - お子様がいらっしゃる方のみお答え。
  - 年齢　性別

(3) 「お客様に関する情報の取り扱いについて」の記述

弊社ではお客様により良い情報・サービスを提供させていただくため、お客様に関する必要最小限の情報を集めている。

弊社及び弊社グループ各社では、次の場合を除いては、お客様の情報を利用したり外部に提供するような事はない。

- お客様が同意されている場合
- 法令により必要と判断される場合

またダイレクトメールと電話による案内及び弊社グループ会社間でのお客様情報の共有について、お客様が希望されない場合は、窓口に申し出れば、取り扱いを中止する」。

当社ではお客様からの信頼を第一と考え、お預かりしたお客様に関する情報を、お客様のご希望に沿って取扱うと共に正確性・機密性の保持に努めている。

2.4.9 考察

このサイトの特徴は、まず「顧客のパーソナルライフにマッチした情報」のために記入する十数項目に亘るアンケート情報項目である。個人情報の保護という観点からすると、プライバシーポリシーにあたる＜お客様の情報の取り扱いについて＞という項目があり、この中である程度の保護要件を明記している点は評価できる。

またセキュリティの技術的側面でもベリサインのシステムを使用していることから、その保証レベルが理解できる。ただ保険加入というネット上の手続きの割には、収集する情報項目自体がアンケート内容を含めて多岐に亘っている感もある。

また同意のある場合のみ、情報主体へのアプローチ・収集情報の利用・グループ各社間での共有をするとの事だが、これもＥメールについては、確かにオプトイン（許可があれば実行＝許可が無ければ中止）方式で聞いてきているが、その他のダイレクトメールや電話による案内、それに一番のポイントであるグループ間企業同士での顧客情報の共有についてはオプトアウト（拒否が無ければ継続＝拒否があれば中止）方式を取っている。

2.5 サイト上に見られる個人情報保護ポリシーの調査について

次に実際に現状で、オンライン上に公開されている個人情報保護ポリシーがどんなものかを調査、分析して行くものとする。（プライバシーと個人情報という言葉は、厳密に言えば少し違う概念であるが，この章以降は同義語的な扱いをするものとする。）

構成としては、プライバシーの保護で先進国である米国の実態についてまず紹介した上で、実際の国内での調査内容について記述する。

2.5.1　プライバシー先進国である米国における最近の状況

日経金融新聞等の記事によると、米金融監督当局は米銀のインターネット取引における顧客のプライバシー保護状況に関する調査をまとめ、顧客情報の収集時に詳細なプライバシー保護方針を明記するなどの改善策を促した。同調査によると、調査対象の大手米銀五十行のうち、外部に情報を販売する際に顧客に販売を止める権利を認めているのは二十五行、顧客が情報販売禁止の通知を文書ではなくネット上でできるように認めている銀行は一行だけだった。

同調査は米連邦準備理事会（ＦＲＢ）、米通貨監督庁（ＯＣＣ）、米連邦預金保険公社（ＦＤＩＣ）、米貯蓄機関監督庁（ＯＴＣ）が 1999 年 5―6 月に銀行・貯蓄金融機関のホームページを対象に共同で実施した。

調査では、個人情報を収集するホームページでプライバシー保護方針に関する顧客からの疑問に回答する仕組みを設けている銀行は十一行だった。顧客に個人情報の確認・閲覧を認めている銀行は一行だけだった。当局は「今後も監督を続ける」と指摘し、プライバシー保護を強化する考えを示した。

一方、米国の IBM 社は、インターネットのウェブサイトに年間 6000 万ドルをかけて広告を出している。その IBM が同社の広告を掲載しているサイトに対して、明確な「プライバシーポリシー」を提出しなければ、広告を中止すると発表した。つまり、そのサイトを訪れたユーザーから、どんな情報を得て、どう処理しているのかということを開示するように要求したのだ。

オンラインショッピング経験のある消費者にとって最大の不安は、ショッピングの際に登録する氏名や電話番号などが悪用されないかということだ。各サイトが、「自分の所では、皆さんから得た情報はこのようにして保護しています」と明記してくれれば、消費者が、そこのサイトでショッピングを行うかどうかを判断できる。これが IBM の狙いだ。

つまり、消費者が個人情報の流出を恐れてオンラインショッピングを控えるようでは、結局は業界全体にと ってマイナスになるという判断をしたわけだ。IBM 以外にも、AOL（アメリカオンライン）やコンパック、マイクロソフトなどが中心になって、「オンラインプライバシーアライアンス」（OPA＝前述）を結成している。できるだけ多くの個人情報は欲しいが、一方でそれをあまりにも追求すると、逆に消費者が敬遠してしまうことになる。いま、多くのショッピングサイトはこのジレンマに悩んでいるようだ。

2.6　有効な環境整備手段・自主規制の一環＝「プライバシーポリシー」の調査について

上記のように米国でも話題となり、国内でも最近、かなりのサイトで見かけるようになった「個人情報保護ポリシー」もしくは「プライバシーポリシー」というものとは何かを見てゆく。

そして各サイトに掲げられているその実物を、業態毎に複数ピックアップの上で、代表例を取上げて一つ一つ調査・比較して、その内容から類推できる各サイト毎の個人情報保護への取組み姿勢といったものを考察していきたい。

現状のオンラインショッピングにおいて、企業側にとっても消費者側にとってもやはり主要な関心事である「プライバシーの保護」に対して、一つの有効な環境整備手段として、また民間企業としての自主規制の一環として普及・拡大しつつある取組みが、この各サイト企業側から提示される「プライバシーポリシー」である。

2.6.1　「OECD のプライバシー8 原則」との要件比較

この言わば、、プライバシーに関する企業側の姿勢・スタンスをストレートに表現した方針が、その基本となる「OECD のプライバシー8 原則」との比較で、どうその要件を満たしているかを、代表例を挙げて確認してみる。

その第一の対象として、国内最大のインターネットプロバイダーであり、おそらくかなりの部分でプライバシー要件を満たしていると思われる「オンライン/個人情報保護ポリシー」を取上げてその各項目について分析･比較を行うものとする。

2.6.2　「OECD のプライバシー8 原則」の各項目別内容

まず直接それを見る前に、基本ベースとなる「OECDのプライバシー8 原則」を再確認することにしたい。

●参考：

「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ＯＥＣＤ理事会勧告」 8 原則（正式名称）

(1)　収集制限の原則

個人データの収集は適法かつ公正な手段によるべきであり、適当な場合にはデータ主体に通知又は同意を得て行うべきである。

(2) データの正確性の原則

個人データは、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、完全、最新に保たれねばならない。

(3) 目的明確化の原則

収集目的は収集時より遅くない時期に明確されなければならず、その後の利用は収集目的と両立し、かつ明確化されたものにするべきである。

(4) 利用制限の原則

個人データは明確化された目的以外に使用されるべきではない。

(5) 安全保護の原則

個人データは紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

(6) 公開の原則

個人データに係る開発、実施、政策は一般に公開されなければならない。また、データ管理者を明示する手段を容易に利用できなければならない。

(7) 個人参加の原則

自己に関するデータの所在を確認し、知らしめられるべき。また、自己に関するデータについて異議申立ができ、異議が認められた場合には、データの消去、修正、完全化、補正ができなければならない。

(8) 責任の原則

データ管理者は、以上の様な原則を実施するための措置に従う責任を有するべきである。

2.6.3 代表事例オンライン/個人情報保護ポリシーについて

次に前述の様に、上記の各項目についてどれだけカバー、遵守する内容・範囲となっているかを確認するための代表サンプル・ポリシーとして、オンラインのそれを取上げて、その中身を各項目毎に 8 原則と対比・考察していくものとする。

2.6.3.1 本文 ：特定会社（代表事例）のオンライン/個人情報保護ポリシー

当社は、個人情報の重要性を認識し、以下の取り組みを実施いたしております。

1. 当社は、お客様個人に関する情報（以下「個人情報」といいます。）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置き、その管理責任者に適切な管理を行わせております。

- 考察

この条項は(8)「責任の原則」をカバーするものと理解でき、管理責任者を置いての管理を明示している。そしてこれは単にポリシーを宣言するに留まらず、その企業のマネジメントのレベルまでその保護スタンスが浸透している事を示すものである。

2. お客様から、お客様の個人情報を収集させていただく場合は、収集目的、お客様に対する当社の窓口、当社がお客様の個人情報を提供する会社の範囲等を通知したうえで、必要な範囲の個人情報を収集させていただきます。

- 考察

この条項は(1)「収集制限の原則」及び(3)「目的明確化の原則」(4)「利用制限の原則」の一部をカバーするものと理解でき、ポイントとしては事前通知を原則として収集・利用に当たる事である。

3. 当社は、お客様より収集させていただいた個人情報を適切に管理し、お客様の承諾を得た会社以外の第三者に提供、開示等一切いたしません。

- 考察

この条項は(2)「データの正確性の原則」の一部、(4)「利用制限の原則」及び(5)「安全保護の原則」をカバーするものと理解でき、事前承諾の無い限りは当初目的外にあたるデータ移転をしない事を明示している。

4. 当社が、上記 3. におけるお客様の承諾に基づき個人情報を提供する会社には、お客様の個人情報を漏洩や再提供等しないよう、契約により義務づけ、適切な管理を実施させております。

- 考察

この条項は上記 3. の(4)「利用制限の原則」及び(5)「安全保護の原則」に沿ってとくにデータ処理をアウトソーシングしたり、別な会社に移転する時の注意事項である。

5. 当社は、お客様に有益と思われる当社のサービス、又は提携先の商品、サ

ービス等の情報を電子メールでお客様に送信させていただく場合がございます。お客様は、当社にお申し出いただければ、このような電子メールの送信を中止させることができます。

- 考察

これは前述したオプトアウト（拒否が無ければ継続＝拒否があれば中止）による電子メール送信の確認である。通常は前述の様にこのオプトアウトパターンが多くの例で見うけられるが真の意味での消費者保護の観点からすれば、ケースにもよるが基本としてはオプトイン（許可があれば実行＝許可が無ければ中止）が望ましい姿である。

6. お客様が、お客様の個人情報の照会、修正等を希望される場合には、お客様に対する当社各窓口までご連絡いただければ、合理的な範囲ですみやかに対応させていただきます。

- 考察

この条項は(6)「公開の原則」の及び(7)「個人参加の原則」をカバーするものと理解でき、個人データに関しては開示、修正要望がすぐ受け入れられて正確性を保たねばならない事が基本である。

7. 当社は、当社が保有する個人情報に関して適用される法令、規範を遵守するとともに、上記各項における取り組みを適宜見直し、改善していきます。

- 考察

この条項は、全般にわたっての法的な遵守と各項目の実態に合わせた改良・修正を意図しており、プライバシーポリシー全体のまとめ的な文章となっている。

2.7 各企業のホームページの中にあるプライバシーポリシー

次に各企業のホームページの中からプライバシーポリシーを明確に宣言しているサイトを中心にそれぞれの業種・特徴別にこれを任意にピックアップしてみた。

2.7.1 京都「アメリカ衣料の岸本屋」の個人情報保護ポリシー

まず最初は単一オンラインショップという立場にもかかわらず、その店主の先見性及び経験則から判断して、いち早くそのサイトにプライバシーの考え方を宣言した前述した京都「アメリカ衣料の

岸本屋」の個人情報保護ポリシーである。

2.7.1.1　本文（別紙参照①：巻末参考資料に掲載…以下同様）

2.7.1.2　考察

このショップのプライバシーポリシーの素晴らしいところは、店主が消費者の立場にたっての自分の経験・反省・思いを反映させて作成されているところである。

普通にあるような、作成ベースとなる方針の雛型とか参考文献があって、それを修正したものではない為に、大変オリジナリティにあふれ、しかも示唆に富む内容となっている。

その点、もちろん画期的･独創的であるし、またプライバシーに関する感覚が大手企業とは異なる、こういった草の根企業において、想いを込めて宣言されたような上記ポリシーのもとにオンラインショップが運営されているのは特筆に値する。

しかもまた特別な意識をせずとも、基本ベースである OECD のプライバシーポリシーの要件をかなりのレベルで充足している点も、これからのオンラインショップのお手本となるべき要素の一つであろう。

2.7.2　NTT コミュニケーションズのプライバシーポリシー

次に通信関連会社の代表として NTT コミュニケーションズのプライバシーポリシーを見てみる。

2.7.2.1　本文（別紙参照②）

2.7.2.2　考察

ここのプライバシーポリシーの特徴としては、通常の個人情報保護の各要件に加えて、クッキー（Cookies）についてや、保証、及び責任制限それに準拠法等に付きわざわざ項目を設けて明記･言及している点である。

とくに準拠法については、インターネットの国際性から来る法律関連の複雑さを考慮して、日本国の法律及び東京都の条例に拘束される旨を謳っており、トラブル時の法規制の問題を充分に意識した内容となっている。

2.7.3　女性向のインターネットナビゲーションを標榜するウェブ Style のプライバシーポリシー

次に女性向及び子供向けサイトのサンプル事例としてウェブ Style のプライバシーポリシーを見ていくものとする。

2.7.3.1　本文（別紙参照③）

2.7.3.2　考察

ここのサイトポリシーの特徴は女性向らしい細やかな表現に加えて、何よりも“3歳から15歳までのインターネットが始まりました”と題する子供向けサイトの立ち上げと“保護者の方へ”と題したウェブ Style for Kids の設立経過・ポリシー・お願いの各項目がその特徴である。

また個人情報の保護という点から言えば、子供向けサイトポリシーについては、特にプライバシー保護だけが強調されているわけではないが、このサイト全体の運営方針を明示する事により、今まさにネット上の課題として問題視されようとしているチルドレンプライバシーの保護についての柔軟なアプローチがされている点でまさに画期的なウェブサイトである。

つまり、来るべきネット社会の入り口に立つ、我々自身が現在、一消費者としてとくに最重点課題として意識すべきものである、この“子供に対するネットの躾”をそのサイトポリシーに取上げているのが特筆される。

米国では、前述の様に民間企業の自主規制としてのチルドレンプライバシーマーク制度や行政による法規制という点での対応も進んでいるが、国内ではまだまだといった感は否めない状況のままである。

この子供のネット上での保護の問題は、官民ともに危機感を持って対応しなければならない時期に、すでに入って来ていると言う認識を持たねばならない。

2.7.4　オフィス京（有）のサイトポリシー

次に日本国内の年齢区分という点で、米国の18歳よりもさらに上の20歳未満のカスタマーに対しての適用方針を打ち出しているオフィス京(有)のサイトを紹介する。

2.7.4.1　プライバシー★本文（別紙参照④）

2.7.4.2　考察

このサイトは、小説・写真・絵･漫画や各種サービス･資料･実用書等の有料コンテンツのショッピングサイトである。従って著作権や会社情報及び成人向け内容等の法律的な取り扱いに関しての内容があるため、特にプライバシーポリシーの中に 20 歳未満の利用者に対する方針の項目を設けているものと思われる。

またこのサイトのホームページには「オンラインマーク実験」に参加しているとのコメントが記載されている。

この___部分をクリックすると現在（社）日本通信販売協会が行っている「オンラインマーク実証実

験参加中」（訪問販売法遵守の事業者に対してマークを付与）のページにリンクして、そこにあるナンバーのついた「オンラインマーク」をクリックすると次に認定された会社名、認定番号が現れて正しいかどうかの確認ができるようになっている。

そしてこのマーク制度の趣旨は、その企業サイトの信頼性確認の為のものであるが、その付与条件として、各業界毎の「個人情報保護ガイドラインの遵守」がその一つとなっていることは当然の事である。

2.7.5　住商情報システム（株）の個人情報保護方針

さて次は情報サービス業種の企業がオンライン公開している個人情報保護ポリシーを見ていきたい。ここでは初めて「コンプライアンス・プログラム」という表現が出てきている。

これの意味はいわば社内実践遵守計画（規定）であり、通産省及び業界の「個人情報保護ガイドライン」に準拠したもので、言いかえれば民間事業者が個人情報保護を自主的に取組むに当たっての体系的経営マネジメントシステムのことである。

2.7.5.1　本文（参考資料⑤）

2.7.5.2　考察

ここのサイトポリシーの全体を通して言える事は、情報サービス産業という職種柄、情報保護に対する意識が通常の職種と違いかなり高いレベルにあることがいえる。

そして特徴としてここではまず「プライバシーマーク制度」という言葉が出てくるが、これは財団法人の日本情報処理開発協会が

、前述の個人情報保護の為の「コンプライアンス･プログラム（以下ＣＰ）」を実践している民間の事業者（オンライン上に限らず）に対して「プライバシーマーク」を付与するものである。

またこのＣＰは＜個人情報保護に関するＣＰの要求事項（JIS Q 15001）＞準拠したもので、それに基づき個人情報の適切な取り扱いが行われ、併せて実施可能な体制が整備されている事がその条件である。

つまり、このマーク制度が米国等で実施されているプライバシープログラムと異なる点は、単に「プライバシーポリシー」を作成して、サイト上に掲げるだけでなく、その方針を遵守するための実行規定であるＣＰを策定・実施していることが、その条件となる。

またそれが JIS Q 15001 に準拠しており、その体制を管理する責任者の選定による定期的な社内監査も必要であるという点で、まさにこの「プライバシーマーク制度」がその企業の経営マネジメントの一環として組込まれなければならない事がわかる。

ただそれだけに一般のオンラインショップが簡単に取得するには、そのハードルが高すぎるという状況にることも確かであり、環境整備から見たより多くの企業への浸透・普及という点では課題がある事も事実である。

この「プライバシーマーク」も前述の「オンラインマーク」と同じく、そのマーク部分をクリックするとマーク付与機関のホームページの「プライバシーマーク許諾事業者」一覧にリンクし、それの真偽を確認できる様になっている。

2.7.6　富士通エフアイピー個人情報保護方針

次には今までの各情報保護ポリシーの要件（子供に対する規定以外）をほとんど集めて作られている代表的優良サイトのプライバシーポリシーの典型を見ていく。

このサイトもやはり情報サービス産業という職種から来る、情報保護に対する明確な意識とモチベーションの高さが感じられる内容である。また基本的考え方であるプライバシーのステートメントから始まり、基本原則としてのプライバシーポリシーへと続く表現形式となっている。

2.7.6.1　本分（別紙参照⑥）

2.7.6.2　考察

このサイトに関しては、今まで紹介した情報保護ポリシーの必要要件をかなりのレベルでクリアしているものであり、プライバシーステートメントも具備した言わばプライバシーポリシーのモデル事例に近いものと言っても良いくらいのレベルである。

特に前述の OECD8 原則に則った項目の表記が豊富であり、しかも外部委託時の注意事項、お客様窓口の明示等がきちんと掲載されているというベーシックな面がまずあげられる。

これはすべてのサイトに共通することだが、そのサイトのプライバシー・個人情報に関する基本的な考え方・認識度合いが出るのがこの部分である。

次に実施マニュアルであるコンプライアンス・プログラムの位置付けやその継続改善等についても、あくまで実行規定としての考え方が明示されている点が評価できる。

これは前述の様にマーク制度そのもののレベルアップ等にも繋がる、費用をかけた経営マネジメントの一環としての保護体制が、企業システムの中に組み込まれている事を意味するものと解釈できる。

背景としてこのサイトがステートメントの部分にもあるように、前述した情報サービス産業としての自覚もその一つの要因として、このような完成度の高いプライバシーポリシープログラムの実現を見たのであろう。

ただこれからは、このような好事例を先達に一般のネットショッピングモールやオンラインショップも是非こう言った具体的な、消費者にビジュアルで訴求できる情報保護の対応を積極的に進めて欲しいものである。

それがひいては、一部の企業の“点”での保護アピールがネットワーク全体の“面”での保護環境整備に繋がるものであり、消費者ＥＣの普及阻害主要因である“個人情報漏洩”の除去に貢献するものと確信する。

2.8　OECD プライバシー・ポリシー・ジェネレーター Ver.1（オンライン「ウィザード」）について

では具体的にオンラインショップがプライバシーポリシーを掲げようとした場合、前項で様々な業種のポリシーを分析・考察した結果、最後の企業（FIP）の情報保護ポリシーが一番ベストに近いという結論に達した訳である。

ではオンラインショップ側が一からこれを作成しようとした場合に、その様な参考となるサンプルポリシー以外に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・ジェネレーター Ｖｅｒ.1（オンライン「ウィザード」）」である。これは今まで見てきた個人情報保護方針＝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、本家本元の OECD から出ている自動作成ツールであり、今回はその第一次の最新雛型に付いて見てみる。

2.8.1　OECD プライバシー・ポリシー・ジェネレーター Ver.1（オンライン「ウィザード」）の内容について

それでは、これについて通産省の資料の抜粋をもとに、その内容について背景・目的・注意事項等の順番で紹介していくことにする。

2.8.1.1　背景

まず、この関連では 98 年 10 月に、カナダのオタワで、電子商取引に関する OECD の閣僚級会合が開催され、インターネット上などのオンラインにおいても OECD ガイドラインの 8 原則が基本となること、また、加盟各国の異なる保護手段を認め合い、様々なアプローチ間で橋渡し作業をすることなどを内容とする「プライバシー保護に関する宣言」が採択された。

具体的にはオタワ会議（1998 年 10 月 7 ～9 日）において、OECD の閣僚は、「重要な権利を

保証し、グローバル・ネットワークへの信頼を高め、個人情報の国境を越えた流通に対する不要な制限をなくするために、グローバル・ネットワークでのプライバシーの保護へのコミットメント」を再確認した。特に、彼等は、OECD のガイドラインに基づきグローバル・ネットワークでプライバシーを保護するために加盟国が採用しているアプローチの違いを調整するために努力すると宣言した。

情報、コンピューターおよび通信政策委員会（ICCP）が主催する情報セキュリティーおよびプライバシーの OECD 作業部会（WISP）は、オタワで閣僚が行ったコミットメントをさらに先へ進めている。WISP は、実際的なアプローチを採用し、特定の問題、特にモデル・プライバシー・ポリシー・ステートメントの作成を調べることを決定し、その調査の一環として、OECD プライバシー・ポリシー・ジェネレーター（オンライン「ウィザード」）を作成した。

2.8.1.2　OECD プライバシー・ポリシー・ジェネレーターの目的について

このOECD プライバシー・ポリシー・ジェネレーターは、ネットワーク上で商取引等のために個人情報を取り扱う主体が、ＯＥＣＤガイドラインにおける公開の原則をネットワーク上で実現するために情報主体に提示する自らのプライバシー・ポリシーの作成を支援するものである。

なお、今回のプライバシー・ポリシー・ジェネレーターはバージョン 1。現在、ＯＥＣＤにおいては、これを更に発展させたバージョン 2 の作成段階にあり、バージョン 2 が公表され次第、その変更点とともにこれを公開予定である。

この実験的なツールは、前述の様にウェブマスターおよび管理者が個人情報を処理するための自己の組織またはウェブサイト情報ポリシーに基づいて、1980 OECD プライバシー・ガイドラインの公開の原則をオンラインで実施するのを支援することを目的としているが目標は、実際的なものである。

つまり、ウェブマスターおよび管理者が自己のウェブ ページに掲げるプライバシー・ポリシー・ステートメントを作成するのを支援することである。

2.8.1.3　OECD プライバシー・ポリシー・ジェネレーターの具体的内容・注意事項

このツールではまずはじめに、自社サイト情報ポリシーに関して回答する必要がある一連の質問（詳細項目は後述）が出される。ハイパーリンクを通してアクセスすることができるすべての説明の注意書きを注意深く読むことが大切。また OECD プライバシー・ガイドラインを注意深く読んでおくこと。

それらの質問に完全に回答すると、プライバシー・ステートメント（プライバシーポリシーの前段と

して掲げるコメント）が自動的に生成される。また OECD は、このプライバシー・ポリシー・ジェネレーターを、企業および組織がプライバシー・ポリシーを作成する際に使用する教育ツールとして提供している。

そこで、OECD は、プライバシー・ポリシーの作成者にそれぞれの国・地域の適切な法律および規則による制約を参照すること、およびプライバシー・ポリシーの生成にはすべての部門などが関係する組織の中での広範な内部確認が必要になることを注意せねばならない。

2.8.2 実際のプライバシー・ポリシー・ステートメントの作成

ウェブサイトのプライバシー・ポリシー・ステートメントの草案を作成する前に、企業は、個人情報の収集（オンラインおよびオフラインの両方）および処理に関する現在および予想される活動を包括的に評価する必要がある。プライバシー・ポリシーの作成には、多くの部門にまたがるかなりの内部の議論と最終的に出来上がったものについての上級管理者による受け入れと参加が必要となることを企業が認識することが重要である。

プライバシー・ポリシーの作成において出てくるいくつかの主要な問題に関して全体的なガイダンスを提供するための様々な根拠と試みを総合するチェックリスト（後述）を確認すること。それには、ウェブ サイトが考慮すべき次の 5 つの領域が含まれる：

- 企業の背景情報
- 情報収集
- 情報の使用および保護
- 個人の参加
- 法律、規則、自主規制

たとえば、情報の収集（自動的と自発的の両方）およびその意図する使用に関して、ユーザーが行うことができる対話<単なるサイトのブラウズ、登録（メイリング・リスト）、調査、サイトの制限された部分へのアクセス、サイトへの E メール、またはオンライン取引の実施等>のタイプが異なると、ステートメントが異なることが明らかになっている。対話の各タイプに対して、匿名の異なるレベルを定義し、タイプの異なる情報使用を想定することができる。

基本的なプライバシー・ポリシーの概要を決めた後、ウェブ サイトにプライバシー・ステートメントを掲げる前に、下記の具体項目を考慮する必要がある。これらの問題には、別のチェックリスト（後述）に示すように、

- アクセス可能性（ユーザーは簡単にステートメントを見つけ、アクセスできるか？）

- ユーザー支援（ユーザーは簡単にサポートを得ることができるか？）
- 教育（このステートメントは、ユーザーに追加の情報を提供するか、またはプライバシー問題へのユーザーの認識を高めるか？）
- 法律面（ステートメントを掲げることにより、サイトはどのような責任を負うか？）

など各種のタイプの質問が含まれている。

さらに、プライバシー・ポリシー・ステートメントを生成した後、このステートメントが実際のデータ・プラクティスを反映し、ポリシーに表されている手順を遵守するように企業内で準備することを保証しなければならないことを認識すべきである。ウェブ サイトにプライバシー・ポリシー・ステートメントを掲げると、企業は、法律的な責任を負うことになることも認識しなければならない（たとえば、米国では、自ら掲げたプライバシー・ポリシーに従って行動しない会社は、不公正で人を欺く活動として FTC から訴えられることがある）。

2.8.2.1 プライバシー・ポリシー・チェックリスト

次に具体的にOECD プライバシー・ポリシー・ジェネレーターに沿ってプライバシー・ポリシーを作成するためのベースとなるチェック項目を見ていく。

(1) 会社情報
- 会社名は？
- 会社のビジネス／連絡先
- プライバシーについての連絡先
- データ管理者

(2) データ収集
- どの部門がデータを収集するか？
- 誰からデータを収集するか？
- ビジター
- 顧客
- どのようなタイプのデータをオンラインで収集するか？
- 個人データ
- 機微なデータ
- 子供から
- 集合

- どのようにデータを収集するか？
- ファーストハンド・ソース
- 登録／発注票、調査
- 取引データ
- トラッキング：ログ・ファイル、クッキー
- サードパーティー広告（バーナー）
- セカンダリー・ソース
- パブリック・ソース
- プライベート・ソース

(3) データの使用および保護

- なぜデータを収集するか？／それをどのように使用するか？
- ウェブ サイトの管理
- 顧客管理
- マーケティング／プロファイリング
- トレーディング
- 誰がアクセスするか？
- 内部
- 外部
- 子会社
- 第三者
- どのように保護するか？
- ポリシー、規則
- 技術的保護

(4) 個人の参加

- ユーザーは、どのように自らのデータを管理するか？
- オプトアウト
- オプトイン
- 記録へのアクセス
- 修正

(5) 法律、規則、自主規制

- どのような法律／規則に従うか？
- 国
- 法律
- 業界の習慣
- 商業上の取り決め
- 国外
- 国際
- 規則
- 自主規制
- サイトの監査／認証は行われているか？

2.8.2.2 「プライバシー・ポリシー・ステートメントのチェック・リスト」

(1) アクセス可能性／読取り可能性

- アクセス可能か？
- すべてのページからアクセス（アイコン）
- 情報が収集される前
- “FAQ”/Help セクションで
- 内部検索エンジンを使用して
- 簡単に理解できるか？
- 言語の種類

(2) ユーザー支援／サポート

- ユーザーはサポート／ヘルプを簡単に得ることができるか？
- 会社の連絡先
- 外部ソース
- 独立した第三者
- データ保護機関

(3) 教育／認識

- 教育ツールとなるか？
- 技術用語の定義
- 外部プライバシー・リソースへのリンク

- 既存の法律のテキストへのリンク

(4) 意味

- ステートメントを掲げることの意味は？
- プライバシー・ステートメントの適用範囲
- 法律上の責任

2.8.3 プライバシー・ガイドライン作成の為の「いくつかの既存のツール」

OECD プライバシー・ポリシー・ジェネレーター以外の既存のプライバシー・ガイドライン作成の為のいくつかのツールを以下に見ていく事とする。

2.8.3.1 いくつかの既存のツール

(1) Privacy Diagnostic

米国国際ビジネス委員会（USCIB）は、Privacy Diagnostic を開発した。これは、企業が「情報収集活動を評価し、プライバシー・ガイドラインを作成する」ときに使用する各種のチェックリストを提供する。自己調査質問事項を通して、Diagnostic は、情報の収集、処理、使用、移転、既存の規則、矯正メカニズム、および一般的なプライバシー原則（OECD ガイドラインから取り出された）などの問題を処理する。レビュー・プロセスに加えて、本文書は、企業がセクターの協会と相談し、セクター間に及ぶ全体の最小基準（オンライン・プライバシー同盟の「プライバシー原則」など）を考慮し、プライバシー拡張技術（PET）の新しい開発の情報を入手する必要があることを強調している。本文書は、国境を越える問題が重要であることおよびデータが中断されることなく保護されて流通することが必要であることを強調している。

(2) 「オンライン・プライバシー・ポリシーのガイドライン」

オンライン・プライバシー問題を処理するために作られた異業種間の連携である、オンライン・プライバシー同盟（OPA ）は、自己のステートメントを作成する商業サイトを支援するための「オンライン・プライバシー・ポリシーのガイドライン」を出版した。同盟のメンバーになる組織には、少なくとも次の 5 つの領域を処理することが求められている：

- 採用および実施、
- 通知および開示
- 選択／同意
- データ・セキュリティー

- データの質およびアクセス

これらのガイドラインに加えて、OPA は、消費者のプライバシーに対する自主規制アプローチを実施するためのフレームワークも提案している。これには、信頼された第三者が、たとえば識別可能なロゴ（プライバシー・シール・プログラム）を使用して順守を評価し、監視することが含まれる。さらに、この実施メカニズムは、消費者に各種の簡単にアクセスすることができる紛争解決システムを提供しなければならない。

(3) プライバシー・ポリシー・ステートメントステップガイド

Aftab & Savitt, P.C.、米国の「サイバースペース」法律会社は、ウェブ サイトにプライバシー・ポリシー・ステートメントを掲げようとしている企業のためにステップごとのガイドを出版した。最初に、それは、収集し、使用するデータのタイプについて企業が考慮すべき質問のリストを提供する。このチェックリストは、

- 子供からのデータの収集
- 個人の参加（記録へのアクセス、データの質など）
- ユーザー選択（オプトアウト）、
- セキュリティー手段

など各種のプライバシーの問題も取り扱う。

FTC の要求を参照して、それは、収集することができるデータの異なるタイプの定義（集合人口統計または個人識別可能）、およびこのデータの可能ないくつかの使用例もユーザーに提供する。ガイドは、個人識別可能データを収集するウェブサイトが内部または第三者のマーケティング活動から脱退するための簡単なメカニズムをユーザーに提供することを促している。集合情報だけを収集する企業には、ウェブ サイトでそのことを明確に述べるように促している。最後に、ガイドは、ユーザーとウェブ サイトの間の信頼が必要であることを強調している。

2.8.4 考察

以上見てきたように「OECD プライバシー・ポリシー・ジェネレーター（オンライン「ウィザード」）」は、サイト情報ポリシーに基づいて回答する必要がある一連の質問を通してプライバシーポリシー＆ステートメントが自動的に生成される機能を持つ実験的なツールである。

またそれには「プライバシーポリシー」の方で40 項目近く、「プライバシーステートメント」の方でも20 項目近くが、その作成に当たって要件として検討されねばならない。

これらすべてを網羅する事は、実用的に見て（ホームページ上の掲載という観点から）困難な面

もあるが、少なくともその中で原則的に見て絶対必要条件である項目は漏らさずに、しかもそれ以外の部分でそのサイトの独自色を出すのがポイントであろう。

また説明文中にもあるように、一旦プライバシーポリシー&ステートメントをウェブ上で公開する企業はある意味での法的責任を負う事になることも認識せねばならない。

但しそれでもオンライン企業は自主規制という観点からも、自らの個人情報保護に対する考えかたをきちんと持ち、またそれが社内での実践遵守規定として経営マネジメントに組み込まれる事を目指してのまずワンステップとしてプライバシーポリシーの作成が必要なのである。

そしてこの「OECD プライバシー・ポリシー・ジェネレーター（オンライン「ウィザード」）」以外にも米国国際ビジネス委員会・OPA・「サイバースペース」法律会社等の団体が、各企業のプライバシーポリシー策定の支援ツールを積極的に用意している事がわかる。

3 電子商取引における消費者情報保護のための課題整理

3.1 課題整理の方法について

1999 年度の消費者情報ＳＷＧ（サブワーキング）での、もうひとつの活動テーマとして、「電子商取引における消費者情報保護のための課題整理」を行なった。

具体的には、消費者の観点から見た個人情報の保護についての実態把握と対応策の検討ということで、消費者団体や各企業に寄せられた個人情報保護に関する消費者からの相談や苦情及び消費者アンケートの事例収集を行ない、その問題点と対処方法を把握する。

そしてこれを踏まえた上で、今後の消費者ＥＣのさらなる普及のために、収集事例以外にも、様々な関連資料を参考・参照した上でＥＣ上の消費者情報保護のあるべき姿の検討をしていくと事とする。

まず“日弁連　消費者問題対策委員会”での 1999 年 5 月に行われた“「インターネット取引をめぐる紛争の予防と解決」“というシンポジウム資料を参考として、その中の苦情・相談や消費者救済の問題などについてアンケート事例を取り上げて、消費者情報保護について検討・課題整理を行なうこととする。

また同じく“財団法人　日本消費者協会”が実際の消費者が経験したトラブル事例をホームページで紹介し、相談内容についても項目別に整理しているが、そのなかには個人情報の流出に関するものも含まれており、その対応策も含めて下記に整理した内容を記す。

3.1.1 苦情・相談の具体事例（1）～ 日弁連シンポジウム資料より

日弁連では、全国の消費者関連の協会・生活センターに対して、1997 年から 1998 年にかけて発生した電子商取引に関する苦情・相談の状況についてのアンケートを実施した。

寄せられた内容として消費者情報関連のものをあげると、内容的にはＩＤ番号やパスワード等が盗用され、注文していない商品代金や使用していないサービスの請求があったものがかなりの数発生している。

A. 具体例

- インターネットのパスワードを盗用された。一回目はプロバイダーが料金負担してくれたが、今回は負担してくれない。
- インターネットでクレジット番号などを悪用され、契約した覚えのない商品代金を請求された。
- インターネットの情報提供料を請求された。利用した覚えは無く、パスワードが盗見さ

れたと思う。

- クレジットカードの番号を悪用されて、全く身に覚えのない請求項目が載っていた。
- インターネットで通販を利用したところ、カード決済の後にこれを不正使用されて、請求をうけた。
- 3 月から毎月 19 ドル 50 セントがカードの口座から引き落とされていた。インターネット上でカードを使われたような気がする。信販会社に申し出たら、海外なので相手の会社が分からないと言われた。引き落としをとめたい。

＜＊特にこのケースはマスコミでも取上げられ、一躍、悪名高きネット犯罪の最前線となってしまった「Ｎ－Ｂｉｌｌ」事件として後述する。＞

- クレジットカード使用による支払いという事で、パソコンの通信料として 1 万 2379 円が口座から引き落とされていた。こちらの家にはパソコンは無く、利用した覚えもない。クレジット会社に電話して、インターネット会社の電話番号を教えてもらったので問い合わせようと思うが、プッシュホン式の電話でしかアクセスできないので連絡が取れない。
- 利用した覚えのないインターネット接続料金が、クレジットカードの請求の中に入っていた。
- インターネットで契約した覚えのない海外の業者の請求をカード会社から受取り、困ってしまった。
- 2 社のプロバイダー契約に名義冒用され、信販会社からの請求で発覚。入会した覚えはないのに脱会届を出せという。どの様に対応したらいいか。
- インターネットで教育に必要な情報を入手していたが、覚えのない買い物の請求がきた。買い物の内訳をカード会社に問い合わせたが、締切り前で判別不可能といわれ、パスワードは変更した。翌月 100 万円の以上の請求がきた。カード会社に紛失届けを出したが、使用した覚えのない外国の買い物に付いては払わなければならないか。

等である。

そしてネット上で勝手に個人情報を流されたり、実名で誹謗中傷されることも多い。またわいせつや暴力等の有害と思われるコンテンツも漏れており、ネットが一種の無法地帯化している状況も憂慮される。

3.1.2　苦情・相談の具体事例（2）と対策～（財）日本消費者協会ＨＰより

3.1.2.1　個人情報の流出（なりすまし、盗用、情報公開、誹謗中傷）

(1) 成りすまし･盗用

上記と同様にパソコン通信上でＩＤやパスワード・カードナンバー等を盗用されて、買った覚えのない物の代金請求を受けたり、送った事もないギフトの支払請求をカード会社から受けた事例。

A. 具体例

- パソコン通信会社に会員登録し利用しているが、注文した覚えのない９万円の有料のソフトウェアを購入した事になっていて、ソフトウェア会社から購入通知の電子メールがきた。パソコン通信会社に苦情を申し出たところ、盗用された立証は困難で、ＩＤ･パスワードの管理責任は規約に従って会員にもあるので基本的に代金請求は行うとの返事。またこれについての苦情相談はクレジット会社に言ってくれと言われた。
- パソコン通信会社の会員だが、ＩＤパスワードが間違いなく盗用されて、アクセスギフトという通信利用料の負担免除サービスを勝手に申込まれ、他人にプレゼントした事になってその代金を請求された。警察にも相談したが、パソコン通信の知識が少ないのか対応が悪い。

というような事例。

B. 対策：

個人管理の徹底（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の自己管理のレベルアップ）等。

(2) 情報公開･誹謗中傷

自分の知らない間に、パソコン通信の掲示板に自分の個人情報とわいせつな文書が書き込まれており、イタズラ電話・ジャンクメールが頻繁にある。

A. 具体例

- パソコン通信のフォーラムに、意図していないのに自分の名前・住所･写真等が掲載されて、電子掲示板に事実無根のわいせつな誹謗･中傷が書きこまれた。
- 知らない間に自分の連絡先・メールアドレスが、ネット上に流れたらしく、頻繁に広告の電子メールが来たり、勧誘電話がかかって来る。

B. 対策：

事前防止は困難だが、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。

3.1.3　N-BILL 事件について

N-BILL 事件は、全世界を舞台にした史上空前のクレジット詐欺事件であると言われている。

ウェブ 110 番等の資料によると、1998 年初夏にある日クレジットカードの請求書に「N-BILL』という身に覚えのない会社からの請求が掲載されていた。すぐクレジット会社に問い合わせをしても、「直接 N-BILL に問い合わせてください」との返事しかなく、金額が 19ドル95 セント (約 2000 円)と小額という事もあり大事にはならないかと思われていた。

しかし、この被害状況の報告が日本だけでなくアメリカでも行われている事が明らかになり、状況が一変した。当初は、インターネットの利用者がセキュリティの甘いホームページにて安易にクレジットカード番号を入力した為に被害に合ったのではないかと思われていたが、どうもインターネットを利用していない人も被害に合っているという事実がわかってきた。

1９９９年 1 月にはアメリカ連邦取引委員会（ＦＴＣ）が詐欺罪で N-BILL を告発。ＦＴＣによると、被害者は世界 20 ヶ国以上に約９0 万人いるという。さらに 5 月には主犯格の 2 人を発見し逮捕。これでとりあえず事件は解決したのだが、犯人の自供により恐るべき手口が判明した。

一番の疑問は「どうやってクレジットカード番号を入手したのか？」という事だが、これには何通りかの方法があった。まずひとつ目は、最初に挙げた「インターネット経由での顧客情報の盗用」そして「N-BILL が実際に運営してたオンライン上のサイト『NETFILL』の情報を不正に流用」したのだという。

だが、インターネットを使った事のない大部分の被害者は、どうして被害に合ったのか？ まず考えられたのが「悪質な他社から顧客番号を買い取り」だが、それでも割合から言うと少数と思われる。殆どは「カード番号をデッチ上げるソフト『カードナンバー・ジェネレーター』で番号を入手」したのだと言う。これなら今までインターネットはおろかクレジットカードを 1 度も利用してない人からも搾取できるのである。

こんな悪質極まりない手口で巻き上げた金額が、何と約50 億円以上（推計）！ 1 人当たり約2000 円の小額詐取も、全世界から搾取という『塵も積もれば山となる』式の典型的なマジックで、史上空前の詐欺事件となっていたのだ。

しかし一方では「カード番号だけで決済できる」という安易な仕組みも責任の一端である、とも言われている。

では、どうすれば防げるのかについては、今の所、対処療法しかない。「クレジット会社に支払い拒否」したり「クレジット会社に『N-BILL』からの請求を拒否」してもらうなどしかない。あとはカード番

号の悪用を金輪際されないよう、カードを解約。これで二次被害は確実に防げるのである。

最後に、これからも同様、もしくはもっと悪質な詐欺事件は増えていくと思われる。重要なのは、泣き寝入りするのではなく、第三者の相談窓口や公的機関に訴える等の行動に出る事である。

3.1.4　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

次にN‐ＢＩＬＬ事件以外で、1998 年あたりから頻繁に発生しているネット関連の犯罪と社会的影響も大きい個人情報の漏洩事件を、１９９９年の新聞等に掲載された項目を年間で合計した件数を分析して全体的な傾向を見てみる。

- ネット犯罪･個人情報漏洩関連合計：1999 年 1 月～1999 年 12 月まで合計 66 件

  ＜内訳＞

  - 顧客情報の漏洩関連：41 件（内なんと２１件が通信会社関連、また４件は医療情報）
  - プライバシー侵害・誹謗中傷等関連：１５件
  - 企業の無断個人情報収集等その他：10 件

ということで、顧客情報の通信会社からの漏洩事件が圧倒的に多い事がわかる。そして医療情報については、何とカルテ情報の漏洩という致命的な事件も入っている。またホームページ上での個人への誹謗中傷は５件含まれる。

3.1.5　個人情報保護法関連の動き･事件

続いてネット犯罪・情報漏洩の対策・防止策として、個人情報保護の法制化･プライバシー保護施策に関連した動きや事件・トピックス（海外含む）の項目別件数を取上げてみる。

- 1999 年 3 月～12 月まで合計 67 件

  ＜内訳＞

  - 個人情報保護の法制化関連：２１件
  - 不正アクセス・セキュリティ関連：１９件
  - プライバシー保護施策関連：１１件
  - 情報ポリシー掲示その他：１５件

やはり１９９９年１１月の内閣の高度情報通信社会推進本部における個人情報保護部会の中間報告に関連した法制化関連の記事が多く、それ以外にも不正アクセス・セキュリティに関連したものやプライバシー保護施策関連で大多数を占める。

3.2　消費者情報保護の在り方についての課題検討

電子商取引における個人情報の保護の問題は、現状の個人管理に依存する前記のような実態を踏まえて、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り、現在、各方面でプライバシー保護関連の議論が行なわれている。以下にその背景を述べる。

3.2.1　国際的要請

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の世界的規範を目指す動きが始まっており，ａＥＵと米国の交渉への注視も含め、日本が財産権保護だけの”プライバシー保護後進国”として孤立しないような対応が急務であること。

またこれに関連して、欧米各国ではすでに 70 年代から法整備が進んでいるｂ個人信用情報保護の義務化・2000 年以降の国内法制化等の動きに連動したＥＣ上での検討が不可欠である事。

＊記号･下線部は詳細を後述する。（以下同様）

3.2.2　国内でのＥＣ普及

ｃ消費者のＥＣ参入への大きな心理的阻害要因であり、また上記のように実害も頻発している”個人情報漏洩の問題”について、消費者保護の観点からも早急な対応が必要である事。

これからは”保護ガイドライン”レベルを超えたｄ実効性のある法的枠組みに対しての民間レベルでの要求結集及び行政への提言の必要性が上げられる。

3.2.3　具体的課題

- 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
- 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）
- 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

3.2.4　課題解決の効果

①個人情報保護のための立法策が検討され、部分立法していく事で、その罰則規定の強制力により、ＥＣ上でのプライバシー保護レベルに対する認識が高まり、国際的にも通用するＥＣインフラの構築につながる。

②その結果オンラインショッピング等において、消費者側からみて安心できる環境整備となりＥＣ人口の飛躍的増加が期待できる。

③特に企業側の方でも、一部先進企業で行われている、ｅプライバシー保護の為の投資が必要不可欠との認識にいたり、ｆ技術的取組み（P3P情報管理システム等）　やｇマネジメントへの組込み（ＪＩＳ規格）等が加速され、企業の内部情報管理レベルの向上に伴い、ＥＣの更なる発展に貢献すると思われる。

＊＜記号・下線部解説＞

a) ＥＵと米国の交渉

欧州連合（ＥＵ）と米国は、共通の個人情報保護手段を見出そうと交渉中である。ただ「電子商取引を円滑に進めるには、プライバシー保護への最低限の決まりが絶対必要」（欧州委員会：Ｓ・ベニニス局長）というＥＵ側の主張とあくまで自主規制にこだわる米国サイドとの溝は簡単には乗り越えられそうにない状態が続いていた。

一方 1998 年の 10 月に個人データ保護のいわゆる「ＥＵ指令」（個人データ処理に係る個人の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の９5／46／ＥＵ指令）がすでに発効している。

この中の 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りうることになった。

特にＥＵ側は米国のセーフハーバーのやり方では不充分であるとの認識を基本的には変えていない。これに対して米国側の自主規制ポリシーは一貫しており、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りつつあるというのが政府系機関・業界団体も含めた認識となっている。

またさらに最近の情勢として、新聞記事によると双方の歩み寄りが一部見られ、ＥＵの欧州委員会と米政府は、ＥＵ内にある企業がインターネット等を通じて海外に送信する個人情報を保護する新しい枠組みで 2000 年 2 月に大筋合意する方向との事である。

つまり個人データを悪用した業者の公表や「個人が自分のデータ削除を希望した場合に応じるなどの保護策を徹底する共同指針を作成、これを受けて米国側もＥＵ内の個人が情報保護に関する訴訟を起こした場合にきちんと対応する様に企業等に求めることとなる。

b) 日本の対応

国内での現状は、公的分野においては法規制（1998 年「行政機関の保有する電子計算機処理に係る個人情報保護に関する法律」）が行われており、地方自治体においても約 4 割が条例を制定している。

また民間分野においては、各業界･業態の特性に配慮しつつ、基本はその実態に沿った自主規制であるが、特定分野（信用情報・医療情報）においては法規制の導入も検討している。

特に民間の「個人信用情報保護」については、企業側の自主規制に委ねられていたが欧米各国･韓国等での法整備の現状を踏まえた国際的な信認確保の背景、それに昨今の信用情報機関からの大量の個人情報が引き出される等の不祥事発生をうけて、罰則規定を含む立法化を目指す事となっている。

そして自主規制を支援する政府の取組みとしては次の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「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）
- 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、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）。

以上のような自主規制の取組みももちろん大前提ではあるが、日本人一般の情報保護感覚レベルを鑑みた場合、ネットワークの国際的広がりの中で人権保護の観点からも包括的な個人情報保護法の必要性も平行して論議がなされるべきであろう。

c) 消費者ＥＣの阻害要因

ＥＣＯＭがおこなった、1999 年 5 月の「ビジネスショウ」（東京ビッグサイト）における「EC 意識調査」のアンケート集計結果（有効回答 2262 名）によると、

〔ＥＣで商品を購入したいと思う人〕は 80％を超えており消費者ＥＣへの期待度が高いことを物語っている。

しかし実際に〔購入経験ありの人〕はたったの 14％しかいないという現状がある。ＥＣのメリットは十分理解できるが、何かの参入阻害要因で躊躇している姿がこの集計からも浮かび上がってくる。

そのＥＣへの不安、短所の最大要因はやはり〔自己データの漏洩〕である。今回もこれま

での調査とは若干減ったとはいえ、依然として 70%近い高率となっている。

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、個人データ保護のおける法整備も含めた環境･インフラ整備が急務であることは論をまたない。

d) 実効性のある法的枠組み

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。

また情報化・ネットワーク社会においては、コンピュータの普及･インターネット人口の拡大により、個人情報の収集・蓄積・加工・流通などが**技術的**に従前と比較して極めて容易となった事及びこれに伴う不正アクセス等の頻発のため、特に個人情報に関するプライバシーの権利は極めて重要である。

現在の個人情報の法的な保護制度としては、前述の「行政機関の保有する電子計算処理に係る個人情報の保護に関する法律」（「個人情報保護法」と略称）がある。

一方、民間期間や事業者の保有する個人情報についての一般的な法規制は存在せず、個別法として、「割賦販売法 42 条の 4（信用情報の目的外使用禁止）」及び「貸金業の規制等に関する法律 30 条 2 項」が罰則を伴わない訓示規定として存在するだけである。また地方公共団体の条例には民間機関保有情報に関する規定を置くものもある。

これらを除くと一部の省庁による通達とガイドライン及び業界の自主規制により対応しているのが現状である。

これに対して先にも述べたような、ネット上のプライバシー侵害事件や顧客情報の流出・漏洩事例の頻発は、個人情報が侵害される機会が飛躍的に増大した事を如実に物語っている。

ここに現状では、個人情報保護制度は未だ不充分であるとした上で、現実にプライバシー侵害が発生した場合の被害救済に資する「実行性のある法制度」の整備を望む意見がでる所以がある。

2000 年は、前述の様に続出した電気通信事業者による顧客情報漏出事件などを反映し、個人情報の保護問題が大きくクローズアップされる年となりそうだ。このほか、某大学では外国要人の講演の際、住所、氏名などを記入した参加者リストを警察当局に 10 年以上にも渡って極秘に提出していたことが判明、個人情報保護の在り方に別の側面から一石を投じた。

このような背景の中で、政府は 1998 年 7 月に高度情報通信社会推進本部（本部長・小渕首相）の下に個人情報保護検討部会（座長・堀部政男中央大教授）を設置。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。政府は2000年1月に専門委員会を設置し、2001年の通常国会提出を目指す方針だが、報道機関や学問研究分野への法的規制問題などは未決着となっており、議論には今後も曲折がありそうだ。

e) プライバシー保護への先進企業の取組み事例

現在ネットワーク上でのコンシューマー（消費者）の信頼をいかに構築するかという点、つまりいわゆるｅ－ビジネス上での信頼関係の確立に向けてグローバル先進企業はすでに動き始めている。

「米マイクロソフト」は電子商取引における個人情報流出を防ぐために「プライバシー保護のガイドライン」を１９９９年 6 月に定めた。

例えばオンラインショッピングサイトの運営側が個人情報を入手･利用する際には利用者の同意を得、漏洩防止に万全を期すことなどが含まれる。

また特徴的なのは、オンライン上の年間広告予算が世界最大規模の同社が 2000 年 1 月以降、「プライバシー保護」を明記していないウェブサイトにはオンライン広告を掲載しないという方針である。

これについては一企業の取組みという範囲だけではなく、他のウェブページ運営者・電子商取引の事業者に対しても、同社の社会性・国際性からして、個人情報保護を徹底させる効果があるものと思われる。

また 1999 年に入り既に同様のプライバシー規定を作成している「ＩBM」についても同じ対応の可能性を示唆しており、さらに一歩進んで民間企業のイニシアティブによる「プライバシーコンサルティングサービス」の提供を開始している。

これはｅ－ビジネス上で導入されるプライバシーポリシー（政策）、プロシージャ（手順）、テクノロジーをヘルプする新たな方法論を示すものである。

これは別な言い方をすれば「プライバシーが商売になる時代の到来」をつげるものであり、国内の感覚とかなりのギャップをもって、グローバルな潮流はもうここまで来ているという事が実感できる話題である。

最近は国内でも「日経リサーチ」等を先頭にして、主要なネットプロバイダー及びシステムインテグレーターのうちのかなりの数のところが、サイト上に「個人情報保護方針」を公開す

る状況となっている。それぞれ各社の情報保護ポリシー・対応状況を広報資料及びウェブサイト上の関連コンテンツを通じて対外的に開示していく事を実践している。

この個人情報保護方針においては、一般的にはＯＥＣＤの 8 原則に沿った「利用・提供のルール化」「不正アクセス、紛失、破壊、改ざん、漏洩の予防･是正措置」「法令、団体綱領、社内規定の遵守」などが宣言されている。

こういった一連の動きは個人情報の保護に対する投資が不可欠であるとの認識が企業側に浸透しつつある証左であろう。

f) 保護に向けた技術的取組み

ネット上における個人情報保護の技術的アプローチの一つとして、前回報告書でも取上げた「WWWコンソーシアム（W3C）」によって開発された「プライバシー情報管理システムP3P（Platform for Privacy Preference）」がある。

これはウェブサイトがウェブブラウザ利用者の個人情報を入手する際に、その使用目的や開示する範囲を明確にし、利用者はそれに合意できた場合のみ個人情報をサイト側に渡す仕組みを自動化したシステムである。

具体的にはサイト側から利用者に対して、取得したい個人情報の種類・使用目的利用範囲などを提示し、これに対して利用者が全面合意・一部合意・拒否を逆提示する手順を自動的に行う。

機能的にはサイト側が組み込む「プロポーザル機能（情報要求内容提示用）」と利用者側ブラウザの 2 機能「プレファレンスビューロ機能（提供可能内容登録用）」及び「ユーザーエージェント機能（要求内容と提供可能レベルの自動照合用）」で構成される。

これによりネット上での個人情報のやり取りにおいて、サイト側がその取扱い内容を利用者側に明確に通知し、利用者側が自分の意思でその提供の可否を選択する事が自動的に可能となり、利用者プライバシーの保護がシステム化できる。

またこのシステムを導入したサイトは個人情報の取扱い方針を明確に公開することになる。

その他の技術的アプローチとしては、ネット上の個人情報そのものを高性能な暗号鍵により保護しようとする取組みがある。

つまり暗号鍵を保護するための情報量を飛躍的に増やして（例えば従来の 40 ビットから 128 ビットへ）、防衛機能を高めて、暗号解読に手間と時間がかかる様にしてネット上で流通する個人情報を保護しようとするものである。

g) マネジメントへの組込み

国内でも先進的なシステムインテグレーター及び電気・通信事業者による、前述のプライバシーマークの認定取得や同じくＪＩＳ規格（JIS･Q15001）認証に向けて活発な取組みがなされている。

これは個人情報保護の取組みを第三者機関に認知・公表してもらう事で、ライバル企業との差別化を図り、ユーザーの信頼性を確保しようとするものである。

例えばプライバシーマークの取得については、「個人情報保護に関するコンプライアンスプログラム（ＣＰ）の要求事項（JISQ15001）」に準拠したＣＰを申請時点で具備しなければならず、またそのＣＰに基づき個人情報の適切な取扱いが行われ、または実施可能な体制が整備されている事が絶対条件である。

加えて社内で年一回以上、個人情報の機密保持に係る周知徹底の措置（教育･研修）を講ずる事や、個人情報保護の状況を監査する事が義務付けられる。

こういった取組みの長所は、単にプライバシーポリシーを宣言するレベルに留まらずに、その保護活動を経営マネジメントに組み込んだところに実効性も含めて意義がある。これは即ち企業システムそのものの改善・対外競争力の強化につながる。

3.3　消費者情報保護に関する具体的課題の内容検討

次に今まで述べてきたような、個人情報保護について、そのまとめとして具体的課題である 3 項目（立法策・環境整備・リテラシー）について考察して行くものとする。

3.3.1　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

この課題については前述のように、民間の「個人信用情報保護」については、「医療情報分野」と「電気通信分野」の情報保護と共に 2001 年の通常国会で罰則規定を含む立法化を目指している。

ただ現状としてはこの分野毎（米国タイプ＝セグメント方式）立法化の動きの前提として、個人情報保護部会からの中間報告の様に、基本法としての包括的な（欧州タイプ＝オムニバス方式）個人情報保護の立法化が検討されており、今後も様々な紆余曲折が予想される。

そんな中で米国ではセグメント方式の一環として「金融プライバシー権法」等の法律を持っているが、これをベースにしてオンライン上の金融機関保有の顧客プライバシー保護について米金融監督当局がその調査に乗り出している。

また「個人信用情報」と並んで特にセンシティブ情報の代表であり、昨今デジタル医療の進展により、電子カルテ・遠隔地診療の分野において、また個人の病歴・治療歴等の漏洩事件等の発生によっても注目されている「医療情報」関連について検討してみる。

3.3.2　医療情報についての調査

ＥＣＯＭとしては 1998 年度の消費者情報ＳＷＧの前回活動報告書の中でも、この個人センシティブ情報の代表である医療情報についての考察を行っている。

3.3.2.1　「医療情報」の内容とは

通常下記の項目が挙げられる。

- 診療録（カルテ）：医師による
- 看護記録：看護婦・看護士による
- 処方箋：医師の指示により薬剤師が調剤した記録
- 検査記録：各種検査技師による検査の結果。テキスト・数値データのみならずX線写真や心電図などの画像データをはじめ、種々のアナログ・デジタルデータ等を含む
- 診療報酬請求明細書（レセプト）：病院の医療事務として患者の加入する健康保険組合に対する請求様式。

等である。

そのなかでも総括的に一番センシティブな個人情報が多いと思われる「診療録（カルテ）」については医師による診療記録であり、医師法と健康保険法による必須項目とそれ以外の任意項目とに区別できる。

必須項目としては、患者の住所、氏名、性別、年齢、診察年月日、病名及び主要症状、治療方法、処方及び処置について遅滞なく記録するように定められている。

また上記必須項目はあくまで最小限度のことで、実際のカルテには以下の例の様にいろいろなことが書いてあるのが実情である。

- 患者の現在の症状
- 精神的、身体的な状況を書きとめておく。
- 過去のエピソード
- 既往症
- 医師が受けた印象

- どのような可能性までを意識して治療したのか
- 患者の性格（例えば神経質、「誇大に症状を訴える」など）
- 患者の生活状況等

3.3.2.2　問題点

次に問題点としては医師として、今後の治療に必要とされる可能性を感じることは、すべてメモしておくという性格が強く、また、問題意識・注意の視点には医師の中でも非常に個人差が激しく、法令による最低限の記述項目を除けば一般化、標準化というのは非常に難しい。

但しこれが不統一のままでも、個々の医療機関毎にコンピュータ処理（システム化）される可能性は大いにあると考えなければならない。

またその情報の一部をベースに患者側から医療機関への支払いが発生し、病院側から健康保険組合に請求が発生することで実態としては情報流通がおき、商取引が成立する。

つまり“ｅ－メディカル（広義のＥＣ概念の中に含むとすれば）”これが今回の検討ポイントの一つである。

3.3.2.3　個人情報保護から見た課題

例えば医療機関内における医療情報のデジタル化・電子化の更なる進展である。そう遠くない将来に医師各人が今のハンド記入のカルテに替わって、「便利な携帯医療情報端末（ＰＤＡの一種）」を持ち、これでもって患者の個人医療情報を管理していく事は容易に想像できる。

そうなると必ず個人情報の中でも“ハイリーセンシティブ”と位置付けられるパーソナルな医療情報が、個別医療機関内でのカルテの電子化等を通して大量にストックされるデータベースの存在が浮かび上がってくる。

そしてこのデータベースにはカルテ以外の上記に上げた各種の専門医療情報がデジタル化され蓄積されていくわけである。

もしここにハッキングが起こったらどうなるか？、ご想像の通りである。例えばインターネット上に、エイズ患者全員のデータが公開されたりでもしたら、それは個人のプライバシー侵害を超えて、大パニック状態となり社会問題化するのではないだろうか。

もう一つ、もっと身近に起こる可能性のある個人医療情報の漏洩手段がある。これはもうすでに一部地域で始まっている「遠隔地診療」からのデータ流出である。

このケースも電子カルテほどではないが、それに近い患者の個人医療データが蓄積されると考

えられる。

また個別医療機関内の専用線等クローズドなネットワークではなく、インターネット等のオープンなネットワークを利用した場合は、より危険な事は言うまでも無い。

さらに遠隔地診療には診断の根拠となる画像データ（本人と特定できるものも含めて）は必須である。この情報量の多いまたプライバシー度が高い画像データが流出･漏洩したらどうなるか、想像に難くない。

3.3.2.4　高付加価値な医療情報

またこのような事態の発生可能性を高める要因がここに存在する。それは個人医療情報そのものの付加価値の高さである。

他の個人情報と比較しても信用情報と並んでハイリーセンシティブで個人としても出来るだけ守秘したいものであるだけに、通常の手段ではまず入手が困難であるからこそ、必要としている人に高く売れるという事実がある。

例えば病状は自覚しているものの、一度病院に行っただけで、こちらから望んでもいないのに、ある製薬会社から“One To One Marketing”と称して糖尿病の治療薬のダイレクトの電子メールが来たら受け取った本人はどう思うだろうか。

また人に一番知られたくないとの意識（何より貴重な情報）を逆手にとって、不正入手した個人の医療情報をウェブ上で悪意の個人攻撃の材料にする輩が出ない保証はどこにもないのである。

こうして見ていくと個人医療情報も特定分野における情報保護という観点から、その解決策としては、個人情報保護部会の中間報告通り、個人信用情報・電気通信分野と並んでその法制化を検討する時期に来ていると言えよう。

3.3.2.5　米国における医療関連のＥＣ業界動向

(1) Intel、全米医療協会とオンライン医療サービスを展開

Intel は全米医療協会（AMA）と協力して、信頼性が高く広範囲なオンライン医療サービスの提供を開始する。そのために、インターネット上で患者の検査結果など医療データが漏洩しないように、AMA 医師資格証明書を発行。これをオンラインで認識するほか、患者の本人認証も行なう。認証は Intel の「e-Health」サイトで行なわれ、これにより、消費者が医療機関からさまざまな医療情報を入手することや、医師と患者または医療機関同士のデータ交換などが高い信頼性をもって可能になるという。

e-Health は、資格証明書の発行を本年第 4 四半期に行ない、本格的には 2000 年第 1 四半期にサービス開始を見込んでいる。

これについては患者の検査記録や治療歴などを記録した電子カルテを医師が利用する際、情報が外部に漏れないように医師と患者の本人確認を確実に行うシステムであり、2000 年の稼動を目指すものである。

米医療関係者によると、医療機関同士でデータを交換していないために、医療データが得られず、検査を重複して実施する例は全検査の約 3 割に上ると推定されている。

全米医療協会（AMA）が三十万の会員医師に登録を勧めるということで医療情報にかかわる認証技術の基準の一つになりそうである。

また、一兆ドル強の市場規模といわれる米医療産業にネット企業の参入が相次ぐ一方でユーザー側からは情報の漏洩への不安やネットを導入した医療機関が少ないなどの不満の声も増えていた。この Intel の電子認証サービスは、登録者が本人であることを示す「デジタル証明書」を発行する事で、患者と医師のやり取りなどの医療機関内情報の外部漏洩を防ごうとするものである。

ちなみに米国では第二次世界大戦後生まれのベビーブーマー世代の高齢化が今後進む事から、医療ビジネスの高成長が予想されている。

Intel は、ネット事業の強化を経営戦略の柱に据えており、医療業界のネット活用をターゲットの一つに絞り、普及を促していく方針である。

(2) 米国の医療業界でのインターネット普及状況

- ９９年 7 月にネットを使って何らかの医療情報を得た成人の数…2480 万人（前年比 45%増）
- 医師と電子メールを介した情報交換を希望するネット利用者…全体の 48%
- 実際に医師と電子メールで連絡を取った事のあるネット利用者…全体の 3%
- 医師や医療機関の推薦があれば、ネット上の医療情報の信頼度が高まると思うネット利用者…74%
- 電子メールで連絡が取れる医師にホームドクターを変えてもいいと思うネット利用者…全体の 33%
- 患者の質問への電子メールでの応対が有効と考える医師…全体の 83%
- 実際に患者と電子メールで連絡を取り合っている医師…全体の 27%

（注）サイバー・ダイアローグ、ミシガン州立大、Intel などの資料をもとに作成

(3) ネット業界の動きに対しての米国での行政側緊急対応策の例

＜クリントン大統領、オンライン医療記録を保護する法律を提案＞

クリントン大統領は1999年10月29日、個人の医療情報を保護する法律を提案した。患者の同意なしに情報を公開することを制限するとともに、情報を何の目的で利用するか、誰に公開するかを患者に伝えなければならないとしている。これを不当に利用したり、不当に公開した者には罰則を適用する。電子的に記録されたオンライン上の医療情報も対象となる。

クリントン大統領は、オンライン医療情報の有用性を認めながらも、電子的に記録されることで「クリック一つで簡単に情報が引き出せる」状況になっており、プライバシーが流出する恐れが高まっていると指摘。規制の必要性を強調した。

個人情報保護について包括的な法規制をを取らない米国では、個人データの急速なデジタル化に対して個別の法規制で対処してきており、今回の法案もその一環といえる。

電子情報は紙の情報に比べ、複写や転送による売買が容易で、プライバシー侵害につながりやすい。今回の法案では、個人の電子医療情報が、雇用者や保険会社、製薬会社などに悪用されるのを防ぐ狙いがある。意図的な悪用に対しては、最高で5万ドルと禁固1年の罰則が課される。

電子医療情報の保護法については、連邦議会が制定する事になっていたが、期限内に合意案を作成できなかった為、法規定によりクリントン政権が作成した。国民への閲覧と意見収集を行い2002年2月以降に施行される。

3.3.2.6 国内の実態

一方国内においては、個人医療情報保護の法制化が遅々として進まない中、ついに1999年の11月にはなんと「病名付き病人リスト」なるものが売買されている事が発覚した。

朝日新聞によれば、これは氏名、年齢、住所、電話番号に「子宮ガン」「精神分裂病」「アトピー性皮膚炎」などの具体的な病名・病歴をセットにしたもので、まさにハイリーセンシティブな個人医療情報に他ならない。

同新聞によると、「全国医療情報センター」と称する業者が全国の薬局や健康食品販売会社にチラシをつけて購入者を募るといった大胆な手口である。またあろうことかそのリストは毎月更新されるという念の入り様である。

厚生省保険局によれば、なんとそのデータ自身が医療保険の「診療報酬明細書＝先のECOM報告書でも取上げた“レセプト”」の情報がベースになっていることも考えられるとの事であり通常で

は考えられない忌々しき事件である。

ただ問題はこの事件を犯罪とは呼べない事である、法の不備を確信的に突いたもので、この業者自身も「社会通念上は多少後ろめたい気もするが、個人情報の売買行為は違法ではなく、このリストで助かる会社もあるはず」という程度の認識レベルである。

その記事の解説にも、これまでの医療情報の流出の例では、ある程度流出ルートが特定できた。今回の様に広域且つ多岐にわたる情報が流出・売買され、しかも情報源の推測さえできない例は極めて稀である。

今回の例はあくまでネットワーク上でのやり取りではないが、チラシを送りつけて購入希望者を募る所をネット上でやれば立派なＥＣなのである。

前述の様に、自分の知らない間に自分自身の持病・既往症の特効薬のダイレクトＥメールが届く事が現実になった事であり、個人情報の売買に関する裏市場での進展は予想をはるかに越えて進行している事実が浮き彫りになった事件と言えよう。

またこの業者自身も法律の専門家に相談して、違法ではない事を事前に確認している事および「多数の個人情報が売買されているのに、今回の例だけが叩かれるのは納得がいかない」とまで言い切っているのである。

現状の医療情報保護の法規制の進展度合いは、いわゆる個人情報保護の基本法制に合わせて、厚生省も対応を検討している段階であり、守秘義務を課す職種を拡大するなどの部分的な対策から罰則規定の折込までを視野に入れた取組みを目標とする可能性が高いと思われる。

つまり民間企業も含めて、病院や医療保険の運営、審査機関等の個人医療情報が集まる所には、これを適正に管理・保護する施策を義務付ける必要が正に出てきた事に他ならない。

これからネットワーク社会の進展に伴い、電子カルテ・レセプトの電子化・遠隔地診断等個人医療情報がデジタルデータになって飛び交う世の中が、もうすぐそこまで来ているわけである。

今回の事件の流出経路・手段が果たしてハードコピーなのか電子媒体なのかは不明だが、業者がチラシという古典的媒体でのＰＲ活動に打って出た事と、ネット上での大量の情報流通がなかったのが、不幸中の幸いであったと言わざるを得ない。

もしこれがネット上で公募されていたら、まさしく日本のインターネットの歴史上の一大汚点となったの違いない。

3.3.3　子供のデータ保護に関して

つぎにインターネットの急速な普及に伴って、参入メンバーの拡大・低年齢化により、子供を通し

ての個人情報収集事例も増加してきており、これに対応しての環境整備が急務になってきた。

3.3.3.1　子供に関する特則

ECOM ではプライバシー問題検討ワーキンググループ（1998 年 3 月まで存続）において作成した「民間部門における電子商取引に係る個人情報の保護保護に関するガイドライン」のなかに、「子供に関する特則」を設けている。

その趣旨は次の通りである。

パソコン操作性の向上やパソコンが学校教育のカリキュラムへ組み込まれることに伴い、子供でも簡単に電子的ネットワーク上で商品・サービスの売買やアンケートへの回答を行うことが可能となった。

こうした状況を利用して、子供から、本人や親の個人情報を収集することが生じる。子供は必ずしも個人情報の収集及び利用についての認識が十分ではないことから、なぜ　情報が必要なのかわかりやすく誤解を生じない表現で説明するなどの慎重な取扱いが必要である。

さらに、子供やその親が、自分の知らないところで不利益を被る懸念があることから、「子供に個人情報の入力を求める場合」は、収集する前に保護者に事情を説明し、了解を得る機会を与える配慮も必要としている。

また、子供が入力した個人情報から子供及び親が不利益を被らないようにするために、保護者に対しても同等の権利を認める事が必要である。

例えば子供向けホームページでも、注文を受付ける前に消費者に対して何のために個人情報を収集したり、何のために利用するのかを表示している事がもちろん前提である。

また、自社で、商品やイベントの“案内サービス”をする場合は、利用目的を消費者に説明している。

もし、そのようなサービスがほしくない場合は、拒絶する仕組みを予め用意していることが必要である。

ただ収集した個人情報は原則提供することはないが、商品やイベントの案内サービスを受けたいと思う消費者の同意があれば、個人情報を保護している他のショップへ氏名・住所・電子メールアドレスを提供する事は可能である。

さらに、個人情報について登録内容の開示や誤登録についての訂正・削除を説明し、消費者からの問い合わせ先を電子メールや電話、ファックスで受け付けていることを説明する事も必要となろう。

具体的には情報の提供はあくまで任意で、必ずしも必須でない場合には「家族の名前は入れな

くてもこの申込みはできます。」などはっきりさせる事がポイントである。

それから「子供」という語句の定義であるが、年齢としては取扱う商品やサービスにより対象となる年齢層が決まるが、一般的には 13 歳未満・12 歳以下を指すのが普通である。

3.3.3.2　子供のオンラインに対する米国事情

一方米国ではまず 1998 年の 6 月に米連邦取引委員会（FTC）が、インターネットの子供向けホームページで氏名・住所・家族構成などの個人情報の提供を受ける際に、親の承諾を得る様に求めているホームページが調査対象全体（212 のチルドレンサイト中）の約 23％に留まり、「個人情報の保護」がチルドレンサイトでは極めて不充分だとの調査を公表した。

さらにその調査は全体の約 89％ものサイトが個人情報を何らかの形で子供達に求めており、その情報収集方針について説明しているには 54％、そのうちたったの 8％しか提供を受けた情報を親に知らせていなかったという結果であった。

これを受けて FTC では「オンライン上で子供から個人情報を収集、使用する際には親の管理が必要」と指摘し、12 歳以下の子供からの情報提供に親の承諾を義務付けるなどの規制強化案を提示した。

これを受けて米国では 1998 年 10 月に「子供のオンラインにおけるプライバシー保護法」（Children's Online Privacy Protection Act of 1998）が制定された。FTC の規制強化案の提示後わずか 4 ヶ月後の法律制定である。

翻って、わが国では種々のガイドライン・条例はあるものの、「子供のプライバシー」ひいてはそれに関連して引き出される可能性のある「家族のプライバシー」を保護する法律は現時点では未だ無いのが現状である。

逆にアダルトサイト・児童ポルノ等が氾濫している国内のサイト事情を考えると、子供向けネット事情の改善は、１９９９年１１月に施行された「児童ポルノ・児童買春処罰法」があるとはいえ、有害情報の「フィルタリング」・「レイティング」の問題を含めて、医療情報と並んで喫緊の課題ではないだろうか。

3.3.4　消費者が安心してＥＣに参入出来るようなネット上個人情報保護環境の整備（インフラと技術的アプローチ）

3.3.4.1　インフラの整備

(1) 日本の現状

ここではまず、消費者に対して安心できるサイトであることを表示する第三者機関によるネット上のインフラ整備として「情報保護マーク制度」について検討する。

現在、日本国内では前述の様にＥＣ上だけでなくコンピュータ処理に係る個人情報保護全般を目的とした、1998年4月から開始されたJIPDECによる“プライバシーマーク“制度の運用があり、また同様に同年 6 月より交付が開始された（財）日本データ通信協会による“個人情報保護マーク”（Trustmark）制度がある。

さらに本来は“信頼性”保証マークということで、個人情報の保護だけを目的としたものではないが、審査基準の中に個人情報保護のガイドラインの遵守をうたって、1999 年 8 月からテストスタートした“オンラインマーク（適性事業者認定マーク）”制度それから同様にその認定ハードルをより厳しくした監査法人トーマツが行う、米国公認会計士協会の個人情報保護基準をベースにしたもので“ウェブ Trust”マークによる認証サービス等がある。

この中では既に去年からスタートして、とくに国内に活動拠点を持つ民間事業者を対象としているJIPDECの“プライバシーマーク”については現在100社以上（1999年12月末時点）が取得しており、業種内訳は情報サービス・調査業を中心として学習塾、医療業、生活関連サービス業、メーリングサービス業、労働者派遣業、印刷業等となっている。

また同様に（財）日本データ通信の“個人情報保護マーク”については、対象が電気通信事業者及び発信情報通知サービス（ナンバーディスプレイ等）の事業用利用者であり、１９９９年 7 月末現在でインターネット接続サービス業者、携帯電話・ＰＨＳ・市外電話サービス業者を中心として 37 社が登録済である。

以上を見ても解るように、これらマーク取得の対象としては、情報サービス関連業者が中心であり、その取得意図も大量に抱えるデータベースについての管理・保護の信頼性確保が中心である。

よって個別のプライバシー・個人情報保護という、消費者が電子商取引に参入する時の一番の関心事については、一般にネット上で消費者からのアクセス対象であるモールやショップについても、もう少しこれらの個人データ保護制度の利用を検討する余地があるものと思われる。

(2) 米国の現状

ちなみに、次に米国の現状を概観してみる。（詳細はマーク毎に後述）

まずマーク制度として有名なものは、ネット上のＢＢＢオンラインのものがあり、現在これには 3 種類のマーク（シール）制度（子供保護シールを加えて）がある。

一つは従来からのネット上の取引事業者に対する“信頼性シール”で、連邦取引委員会（ＦＴＣ）の規制、モデルコード（ガイドライン）の遵守をチェックし、ライセンスされている。

日本のＪＡDMA等による“オンラインマーク制度”にあたるもので、1999年の 5 月現在 3,200 社が参加しており、内訳としては中小企業が多い。もう一つは“プライバシーシール”である。この認定マークを受けるためには、オンラインプライバシーについてのポリシーを明確にし、個人情報の収集方法やその用途に関する詳細、消費者にデータの正確さを確認させる機会を提供しなければならない。

このプライバシーシールプロジェクトの背景には、民間として政府の規制を回避することがあった。そのためＢＢＢに参加していない事業者もプライバシーシールには参加できることになっている。

また 26 社の大企業がスポンサーになっており、1999年3月にスタートしたばかりだが既に 5 月現在 300 社が申請している。なお同シールの取得料金は 150 ドルからとなっている。

次にオンラインプライバシー保護マークとして有名なものに、1997 年 6 月に発足した民間の非営利団体であるトラストｅが商業用のウェブサイトに個人情報の収集と利用に関するポリシーの公開を促す目的で行っている“トラストｅマーク”制度がある。

このプログラムはプライバシーポリシーに含まれるべき必須項目のガイドラインを設定し、参加サイトがポリシーに従い運営されているかどうかを年に 2 回監査しこれに合格したサイトに“トラストマーク”を交付する活動を行っている。

そしてこれもＢＢＢオンラインのプライバシーシールと同じく、政府による規制導入のプレッシャーを受けてにわかに大手企業がトラストｅの存在に注目して業界内の自主対応の取組みを示すために、1998 年の 5 月以降一斉に参加を表明した。この時に参加サイトは一気に 130 ヶ所以上に拡大した。

これによりトラストｅは、業界標準プログラムと言える規模を獲得してその活動も軌道に乗るに至った。

また現在ではその認定マーク（シール）の発行地域をヨーロッパまで拡大している。というのも欧州委員会では、法規制をベースとしたデータ保護が主流である実態を踏まえて 1998 年ＥＵ指令に基づき、前述の様に欧州連合（ＥＵ）と同等のプライバシー保護措置をとらない国との情報交流の差し止めを指示している。

今回のトラストｅの動きはもちろんこのようなＥＵ関連の情勢を考慮したものと考えられる。

その他にも消費者保護を目的としたＢＢＢオンラインの信頼性シールと同様のウェブ

Assurance Bureau のマークや前述した日本の監査法人トーマツのサービスベースとなっている、もっと保護範囲を広げてチェック項目を増やした米国公認会計士協会（ＣＰＡ）の“ウェブ Trust”マーク等がある。

またこのような海外におけるオンラインマーク（プライバシーマーク中心）制度の詳細については、別な章でその中身の詳細について言及していきたい。

(3) 国内の制度改善点

以上のように個人データ保護に対する世界の動きを見ると、法規制で一貫している欧州は別にして米国では民間団体が率先して、政府の規制を先回りして自主規制強化の名の元に次々に種々の情報保護マーク制度の立ち上げ、拡大を目指している事は消費者サイドから見ても評価に値する。

これに比して日本国内の現状では、確かに情報保護マーク制度自身は立ち上がってはいるが、そのカバー範囲・趣旨からして電子商取引の一般消費者からみた参入不安感の払拭に効果のある制度と言えるまでには、まだまだ改善･追加等の余地が大いにあるのではないだろうか？

またさらに米国では、法規制のところでも述べた様に1998 年 6 月のＦＴＣによる子供向けインターネットの規制強化に関する提案を受けて、トラストｅが子供の個人情報保護に関する「Children’ｓ Privacy Seal」プログラムを提唱している。

これは13 歳以下の子供が個人情報を提供する場合、親の同意を得る様に表示しているサイトに「トラストｅ Children’s Seal」のマークを貼る自主規制運動である。

またＦＴＣ自身も1999年4月 22 日に、政策的見地から 13 歳以下の児童から個人情報を収集する商用ウェブサイトに適用するための「Children’s Online Privacy Proposed Rule（児童オンライン個人情報ルール案）」を発表している。

一方日本国内では、１９９９年１１月に施行された「児童ポルノ・児童買春処罰法」以外には、この子供の一般的な個人情報保護に対しては、前述のように今のところ何の法制化も無い事に加えて、業界自身の自主規制の動きもあまりなく、児童に対するインターネットの普及率･環境が米国とは異なるとはいえ、現状はいわゆる野放しに近い状態である。

3.3.4.2 技術的アプローチについて

次にマーク制度以外で広い意味での取引環境整備に繋がる、米国の複数企業・団体の結束に

よる自主規制の代表事例「Open Profiling Standard(OPS)」と「OnlinePrivacy Alliance(OPA)」を見ていきたい。

(1)「Open Profiling Standard(OPS)」

まず1997年5月27日に米国のNetscape, VeriSign, Firefly Networkの3社が、インターネットで個人情報を安全にやりとりするために共同提案した規格案が「ＯＰＳ」である。

これは、インターネットに関する標準化団体であるＩＥＴＦに提案されていた電子ビジネスカードやデジタル認証等の標準的技術仕様に基づき、個人の名前やメールアドレス、住所、郵便番号、年齢、趣味などのプライバシーにかかわる項目で構成される個人情報（Personal Profile）を管理し、インターネット経由で受け渡しするものである。

情報収集・管理システムはFirefly Networkが提供し、認証サービスはVeriSignがが提供するというもので、Netscape以下60社がその当時でサポートを表明し、1997年6月にはWWWの標準化団体であるW3CにＯＰＳの仕様を提出し、ついでMicrosoftも支持を表明するに至った。これはプライバシー保護の環境整備に対する業界としての技術的アプローチの好例である。

(2)「Online Privacy Alliance(OPA)」

次に1998年6月23日、オンライン販売等に関連する米国の企業や団体が集まり、ネット空間のプライバシー保護を目的とした組織を結成したと発表した。（詳しくは後述のプライバシー保護関連の民間団体のところで詳細記述）

メンバーはAOL, Microsoft, IBM, Dell, Netscape, Bay Networks, AT&T等企業39社とAmerican Electronics Association等12の団体でスタートし,現在は85の営利･非営利団体から構成されている。

この「Online Privacy Alliance」では、業界が自主規制を行う事で消費者のプライバシー保護は可能だと強調、民間主導によるプライバシー保護に取組んで行くことにしている。

そしてそのホームページ上では、「Online Privacy Alliance」による、電子商取引におけるプライバシー保護の為のガイドラインや自主規制案を公開している。

具体的にはオンライン・プライバシー政策のための詳細なガイドライン（Guidelines for Online Privacy Policies）や子供のプライバシー保護（Safeguard The Privacy of Children）等を提唱している。

また1998年7月にはＦＴＣが消費者のオンライン上での個人情報保護のための対策を取るように業界に求めてきたのに対して、民間主導による個人情報保護施策（「EFFECTIVE

ENFORCEMENT OF SELF REGULATION」from OPA）を公開している。

それから1999年5月には設立以来の活動成果として「過去一年間でプライバシーの自主規制は大きな進展を見せた。」とする調査報告書を米連邦議会の小委員会に提出している。

「Georgetown Internet Privacy Policy Survey」と呼ばれるその調査は2つの項目からなっており、一つは上位100社のウェブサイトを対象とした調査、もう一つは人気のある7,500サイトの中からランダムに364のサイトを抽出して実施した調査である。

その結果によると、上位100サイトの94%が、少なくとも一つはプライバシーに関するポリシーを明記しており、1998年の74%より大幅に改善された。

またランダムの364のサイト中でも、66%が同じくプライバシーポリシーを表示しているという結果であった。

以上の様に米国では包括的な法規制がないとはいえ、各企業や民間団体が“ＥＵ指令“等を受けた政府規制に先んじてマーク制度以外にも、消費者から見た取引環境の整備の一環として様々な個人情報保護の取組みを行っている事がわかる。

それに対して日本国内では、こういったある意味で自分達の立場を追い込む、コストもかかる取組みに対する企業・業界団体の意識がまだまだ米国並には至っていない事がよくわかる。

しかし周知の通り、電子商取引の国際性から鑑みても、また真の意味での消費者のＥＣに対する参入不安を払拭するためにも企業自らが危機意識を持って、自主的に個人情報保護に取組まねばならない時期に既に来ている言えよう。

環境保護問題等と同じくこのプライバシー保護についての取組みを、すでに経営コストの中に折込む必要性を、一部の先端企業だけでなくＥＣにかかわるすべての企業が早く認識して欲しいものである。

3.3.5　企業・消費者双方に対するＥＣ上のプライバシー保護についてのリテラシー

この問題のポイントは、日本における企業・消費者双方のプライバシーに関する感覚・常識といったものが、欧米に比べて大きな差があることであろう。

3.3.5.1　企業側に対するリテラシーについて

これについては、前にも述べた様に法規制の有無にかかわらず、国内でも企業側が自主的にプライバシー保護の取組みを始めないと、特にＥＵ加盟国を中心として国際的な電子商取引が不可能になる時機がもうすぐそこまで来ている実態を早く認識すべきである。

特に日本企業を含む日本国全体の印象として、よく言われる経済的権利（財産権等）の保護には熱心であるが、個人情報のような人権保護には無頓着な国だと受け止められている現実がある。中でもプライバシー保護については、国内では未だに法規制や社会ルールといった社会的インフラが未整備であり、同時に前述の様に、「プライバシー」と言う概念そのものに対する日本的感覚・慣習が、欧米に比べて鈍感であるといわざるを得ない状況である。

つまりまだ一般消費者がプライバシー保護を、企業選別の一要因として捉えてない事が、現在の厳しい経済環境下では企業自身として情報保護関連の投資に、今これ以上に踏み込めない原因であろうと考えられる。

さらにはプライバシー保護への企業としての取組みは、まずプライバシー･ポリシーの確立が前提であるが、これだけでは実効性として不充分であり、やはり内部の企業マネジメントレベルにまで落とし込む事がポイントであろう。

昨今のデータ漏洩が外部からの不正アクセスよりも内部犯行によるものが圧倒的に多い事でも分かる様にコンプライアンス･プログラムの実践こそ求められる段階である。

またこれを通じた企業モラル・企業理念にまでの浸透こそ理想であるが、それまでには現実として、社内体制・インフラの整備等のコストがかかるのも事実である。

ただここで考えねばならないのは、電子商取引においては先に述べた様に、直接的にはＥＵを中心とした外圧がもうそこまで迫っている事がまずあげられる。

次に、それを受けてさらに間接的には、米 Microsoft，IBM 等の先進企業は、自社の自主規制の更なるアピールの為にプライバシー保護ポリシーを掲げていないサイトには、自らが世界最大規模の広告クライアントである事を武器に、広告を掲示しないと言う姿勢を明確にしている。

これら先進企業の選択は、当面の政府規制を逃れると言う側面と,それを逆手に取って、このプライバシー保護という項目が情報企業内において他社との“差別化”の手段として認知されていることに他ならない。

つまり前述の様に、環境問題と同じく受動的な規制クリアのための人道的経営コストという意味合いと同時に、積極的な意味での経営戦略の一環として組み込まれたことを意味すると言っても過言ではないと思われる。

いわば、プライバシー保護というのは企業にとっていろいろな意味で“金が出て行く木である”（必要コスト）と同時に今や“金になる木”（セールスポイント）なのである。

そして次の段階として、この企業のプライバシー保護への傾注が先進企業だけでなく一般企業にも広がっていくメリットは、その狙いである消費者にとってのＥＣ参入への大きな阻害要因である

個人情報漏洩の危惧を無くさせる普及効果である。

つまりプライバシー保護が一般企業に浸透した場合、その時点ではもう差別化は出来なくなるが、一方でそれが消費者の取引環境整備に繋がり、新しい購買層のＥＣへの積極的参入、即ち潜在顧客層の掘り起こし・ＥＣ市場の拡大に貢献する事である。

以上のように、消費者ＥＣの更なる発展のためには、このプライバシー保護に取組む企業としての社会貢献性・経営戦略面・消費者環境整備面でのメリットを各企業に良く認知してもらう事つまり企業リテラシーがポイントとなる。

そして具体的手段であるが、国内でもこういった動き・感覚に鋭敏な一部先進企業については既にもう取組みが始まっているおり、それに期待するとして、それ以外の企業についてはやはり、横断組織である業界団体としての役割遂行が求められる。

つまり主催する勉強会・研修･セミナー等様々な機会を通じての構成企業に対するリード役としてのパブリシティー及びリテラシーがあげられる。

もう一つとしては消費者団体等第三者機関によるプライバシー・ポリシーの掲載企業への応援キャンペーン、それに機関紙・マスコミ等のメディアを通じた企業名の公表･情宣等が有効と思われる。

3.3.5.2　消費者に対するリテラシーについて

まず電子商取引という場面に限らず、一般的なネット上での個人情報保護を考えてみたい。その延長線上にＥＣ上でのプライバシー保護に関する消費者リテラシーの課題があると考えられるからである。まずネット上の個人情報の漏洩・公開についての課題について検討する為、色々な文献を調査して見た。そのなかでも１９９９年5月に（財）ニューメディア開発協会から出されている「インターネット利用者のプライバシー保護へ向けて」（Needs of Privacy Protection on the Internet）という文書の一部を紹介・引用する。

(1) インターネット利用上の注意

ウェブ上の多数の業者から個人情報を要求されたり、利用者の個人情報がネット上に流出する事件が生じたりする現状では、消費者がインターネット利用中に何気なく入力した個人情報が業者によって悪用されたり、第三者に提供されたりする恐れもあります。

日本では公的機関が中心となって個人情報保護へ向けた取り組みを進めている段階ですが、プライバシーマークの掲載等の手段によって個人情報の取り扱い方針を利用者側に明示しているウェブサイトはまだ少なく、利用者はプライバシーを侵害されるリスクを負ってインタ

ーネット上のサービスを利用しているのが実状です。

そこで、利用者が安全にインターネットを利用するためには、不必要な個人情報の提供を避けること等、利用者側で自己防衛策をとることが必要となります。以下に、インターネットを利用する上で利用者が注意すべきいくつかの点を挙げます。

①ウェブサイトのサービスを利用する上で、ウェブサイトへの提供が不必要と思われる個人情報については提供しない。あるいは、必要最小限の個人情報のみを提供するようにする。例えば、「趣味・嗜好」、「興味ある分野」等は、多くの場合、ウェブサイト運営者がマーケティングへの利用を目的として収集している個人情報ですので、そのような利用を望まない場合には提供しないようにします。

②次に掲げる種類の内容を含む個人情報については提供しない。

・人種及び民族

・門地及び本籍地

・信教（宗教、思想及び信条）、政治的見解及び労働組合への加盟

・保健医療及び性生活

③ウェブサイト運営者が個人情報の収集目的等を明記しているかどうか、明記している場合にはその内容をチェックする。

④ウェブサイト運営者が、利用者からの問合せに対応するための対応窓口を設定しているかどうかをチェックする。

⑤パスワードなど利用者本人しか知り得ない個人情報については、他人に漏洩することのないよう、利用者本人が責任を持って管理する。

以上が、一般的な「インターネット利用上の注意」の項目から、考察の前提として参考になるネット上で個人情報の課題についてである。

(2) ＥＣ上での漏洩・公開の影響

その中で通常のオンラインショッピングにおいて、消費者側から相手の方に提供する個人情報としては実名、住所、電話番号、E－mail address ぐらいであろう。

但し,これとて上記の様にその程度のプライバシーレベルでさえ漏洩、公開されれば少なからず影響が出ると言う一例であり、ましてや個人の信用情報、医療情報等のセンシティブ個人情報が漏洩・公開されたりすれば、大問題になるという証左でもある。

(3) データ漏洩の実情

但し、現実の社会では個人情報の取り扱いについて実際にはもっと深刻で衝撃的なな状

況が水面下では進行している事を取上げた書籍も最近ではいくつか出版されている。

それらによると実名・住所・電話番号というもっとも基本的な個人属性情報が分ると、すぐに銀行の振込口座・給与・ローン・債務・本籍地・結婚歴から芋ずる式に破産者・犯罪歴まで一時間足らずで分るそうである。

それから、おそらく不正持ち出しによるものも含めて、街のいわゆる名簿屋で売られている一覧リスト・名簿関係は個人の趣味嗜好等の人物情報が入った個人情報の宝庫となっているそうであり、中には「結婚予定者名簿」もあるとのこと。

またネット上では会員制のビジネスサイトで流出した個人情報の売買が激増しているということで、例のテンプスタッフの登録女性名簿の売買はこういった会員制サイトだったそうである。それにネット上の商売としては「インターネット個人情報調査請負業」といって身元調査系のサイトがやはり個人情報を売買している実態がある。

(4) 自己防衛策

現在の個人情報に関する法的インフラの欠如やや企業管理レベルの低さといった危機的な状況下では、一消費者として出来る事はやはり米国並の自己情報の管理意識をもつ事と同時に自己が行使できる権利、例えば公開請求権やメールの拒否権の実行といったものを積極的に活用する事がまずあげられる。

次に注意しなければならない事項として、オンライン・ショッピング時の注意事項（自己防衛策）を列挙する（一部前述のインターネット利用上の注意と重複）

- クレジット情報・銀行口座情報等の個人信用情報のネット上取扱い要注意
- ネット上の懸賞・メールアンケートやダイレクトメール受け取り時の対応注意
- ショッピング時の申込みフォームの必須項目以外の記入注意
- 情報保護ポリシー・セキュリティレベルを明示していないサイトとの取引中止

等があげられる。

つまりは他の条件（商品的魅力）はいくら揃っていても、プライバシーポリシーや個人データ保護に関する規約が明示してなかったり、セキュリティ関連に対しての記述が見当たらない等の「個人情報管理を厳格にしていないと思われるサイト」とは一切付き合いしないことがまず前提であるが、上記の条件を満たす場合でも個人プライバシーの提供にはさらに細心の注意を払う事がポイントである。

(5) 子供へのリテラシー

次に注意すべきは、先ほども述べた子供達からの彼ら自身及び家族全体に及ぶ各人の個

人情報の流出である。特に子供達は大人に比べ射幸心が強く、興味あるサイトからの誘惑には負けやすい傾向なのは事実である。

また企業もそれを熟知しているがゆえに、豪華な懸賞グッズやお目当てのキャラクターを掲げたネット上のアンケートや懸賞募集などの申込みの際に、彼ら自身の個人情報のみならず、親や兄弟といった家族全体に及ぶ個人情報の記入を求めたりするケースがある。

これらの防止策は前述の様に、子供対象の法規制や子供専門サイト向けマーク制度の検討も必要であるが、それこそ学校教育の一環としてのインターネット教育の場においてネット社会の裏の部分である個人情報の流出・漏洩の怖さや影響の大きさも教育すべきであろう。

また家庭内教育においても、一般に個人情報に収集・利用についての知識が無く、またそれを提供したときに起こりうる自己のリスクについての判断も十分でない子供に関する情報リテラシーは、ネット社会では必須の現代版躾の一種ではないだろうか。

4 海外におけるプライバシーマーク制度の調査報告について

4.1 調査･収集内容について

いろいろな文献・資料を見ても現在、米国中心に展開されているオンラインマーク制度（とくにプライバシーマーク中心）について部分的に記述しているものは数多く見うけられる。

但しオンラインマーク制度全体として見た時には、その一項目としての記述に留まり、個々のプライバシープログラムの具体的内容といった種類の文献はほとんど見当たらないのが現状である。

そこでＥCOMとして、とくにオンラインマーク制度の中でも馴染みが薄いオンラインプライバシープログラム（マーク制度）を対象に、様々な文献・ニュース記事・ホームページの説明等を対象に独自調査を実施して、その全容紹介に翻訳も含めてチャレンジしたのがこの章である。

なおマーク制度の概観（現状）については、既に前述の章で触れた通りである。ここではまず、各マーク制度の運用に当たっている米国の民間団体が、その英語のホームページ及び英文記事等で紹介されている各種のオンラインマーク制度（プライバシーマーク中心）の中身についてECOM として独自に調査・翻訳及び解釈の上、これの考察を試みたものを以下に記載したい。

さらにアジアの代表として韓国において、既にスタートしている表彰マーク制度やスペインでの「Gマーク」制度についても調査をかけて、今までその実態が全く不明だったものについても、入手資料にこれも翻訳等を加えて、ECOM としてのネット環境整備の為の参考施策という観点から紹介・考察していきたいと思う。また参考に国内の民間のプライバシー関連シールの紹介も行なう。

以上まとめてみると今回の主要な調査報告対象としては

米国のでの

1.BBB オンラインマーク制度について

2.トラストｅマークについて

3.ＣＰＡウェブトラストマークについて

4.関連する行政機関のＦＴＣ及び民間団体のＯＰＡについて

それ以外の国として

5.スペインのGマークについて

6.韓国のオンラインマークについて

それに参考として

７.国内（民間）のプライバシー関連の各マーク制度である。

4.2　BBB オンラインマーク制度

まず有名な米国の BBB オンラインのマーク制度の紹介から始めるものとする。

4.2.1　ＢＢＢオンラインのミッションと各種シールプログラムの目的

ＢＢＢオンラインの使命は、健全で倫理的なオンラインビジネスを奨励することにより、インターネットにおける信頼と信用を高めることである。この BBB の高い水準を満たしている企業に対しては 3 種類のシール（信頼性シール、プライバシーシール、キッズプライバシーシール）を付与しているので、信用のおけるオンライン企業を簡単に見分けられる。このほかにも消費者教育資源や、一般消費者の苦情を処理する対応システムも用意している。

4.2.1.1　各シールプログラムの内容

(1) ＢＢＢオンライン信頼性シール

インターネットは、新しいアイディアを思いつけばほぼ誰でも、ウェブサイトを立ち上げて商売ができるエキサイティングな新しい媒体である。これはインターネットを非常に魅力あるものにしているものの一つであるいっぽう、消費者保護という分野において数多くの問題を提起しているものでもある。動きが速く、往々にして規制のないインターネットの世界では、評判の良いウェブサイトやオンラインサービスとそうでないものとを区別するのは難しい場合がある。信頼性シールは、信用できるウェブサイトやオンラインサービスを区別する簡単な方法を提供すると同時に、オンラインでの消費者の信頼や信用を高めるためのものである。

(2) ＢＢＢオンラインプライバシーシール

商品の注文やコンテストへの参加、サービスの登録、メーリングリストへの参加時に、多くのウェブサイトが消費者からデータを集めている。たいていは、その情報がどのように利用されるのか、あるいはどのような相手に公開されるのかは知らされないままである。オンライン上のプライバシーを守る一つの方法は、ＢＢＢオンラインプライバシーシールを探すことである。

(3) ＢＢＢオンラインチルドレンズプライバシーシール

子供たちから集められた情報は特別なプライバシー問題を提起するため、ＢＢＢオンラインプライバシーシールでは、子供に関係する固有のオンラインプライバシー問題を扱う広範囲の特別要件に従っているウェブサイトやオンラインサービス向けに、チルドレンズシールを用意している。

4.2.1.2　考察

このようにBBBオンラインは全部で3種類のシールプログラムを持っており、特にこのうちプラバシーシール及びチルドレンズシールは９９年の 3 月以降にスタートしたものである。大きな背景としては、ＥＵ指令ののデータ移転禁止条項の発効を受けた形での米国内での個人情報保護に対する民間ベースでの自主規制推進運動の高まりがある。

次に今まで紹介した各シールプログラムの内容に加えて、さらに詳細に各プログラムの概要･具体的要件等の中身について特に個人情報と言う観点からそのプライバシープログラムを中心に見ていきたい。

4.2.2　ＢＢＢオンラインプライバシープログラムの概要

インターネットが直面する数多くの課題の中でも、プライバシーはウェブユーザがオンライン接続しているときにあげられる第一の問題（そして障害）として最も大きく浮上している。BBBオンラインプライバシープログラムの参加企業は対応性の高い、効果的な自主規制によってこの問題に正面から取り組んでいる。責任ある情報の取扱いに同意することで、ＢＢＢオンラインプライバシープログラムの参加企業は自らのそして将来のインターネットでの成功にとって必要な、極めて重大な信用と信頼を高めている。

BBBが自主規制や紛争解決で駆使している際だった専門知識を活かし、ＢＢＢオンラインプライバシープログラムは、検証、監視と審査、消費者紛争解決、適合シール、施行機構、そして教育コンポーネントなどを特徴としている。消費者にはＢＢＢオンラインプライバシープログラムが、消費者がインターネットを安心して利用できる使いやすいツールであることがわかるであろう。企業にとってこのプログラムは、信頼できるオンラインプライバシー原則を遵守していることを証明する手頃な価格の、シンプルで何でも揃った、邪魔にならない手段となる。

4.2.3　BBB オンライン・プライバシー・シールの申請について

資格基準を含むプログラム、参加契約、価格設定情報の全詳細は、BBB のホームページ上で入手できる。事業申請書が提出されると、申込みの会社のユーザネーム、パスワード、「準拠性評価アンケート」の所要事項の書き入れに必要な指図事項を記載した e-mail を受け取ることになる。処理手数料の支払金を受領し、会社の準拠性評価アンケートの所要事項が書き入れられると、当該会社の準拠性評価アンケートとホームページは、BBB オンラインの準拠性アナリストによって審査されるという手順である。

4.2.3.1　注意事項

プライバシー方針と情報慣行について、実質的に複数の準拠性評価の審査が必要なほどに異なる内容のホームページ申請書を提出した場合には、処理手数料と年間使用料が別途課金される場合がある。

BBB オンラインの申請プロセスは、社外秘であり、申請処理に伴う秘匿性の保護条件を記載した完全な明細書を求める場合は、ホームページよりダウンロードのこと。

もちろん申請者は、BBBオンラインが申請者の準拠性について連絡するまでは、新聞発表その他で、みずからのホームページ上に、BBB オンライン・プライバシーのシールを表示したり、またはプライバシー・プログラムの準拠性に関してクレームしたりすることはできない。

また米国またはカナダ以外に本社のある企業の場合には、BBB の「世界企業申請書」に所要事項を書き入れること。

4.2.3.2　プライバシー・プログラムの作業について

BBB オンラインのプライバシー・プログラムには、たとえば BBB の全国広告部、その児童広告審査部門の「BBB オートライン」やBBBオンラインの信頼性プログラムなどの各プログラムを通じて、紛争の解決や自主規制で CBBB が掌握している重要なノウハウが利用されている。当信頼性プログラムには、現在、ホームページで、ある会社の歴史をチェックし、連絡情報を入手し、かつ当該会社がその広告クレームの保証に関する情報を消費者に提供するシールを表示している企業が 3,500 社以上もある。

BBB オンラインのプライバシー・プログラムの特徴は、確認、監視、審査、消費者の紛争解決、準拠性シール、執行のメカニズム、それに教育上の構成要素である。

4.2.3.3　BBB オンラインのプライバシー・プログラムの詳細項目。

- 開示、選択、機密保護などの、所要の「中核」原則を満足するプライバシー方針をオンラインで通知する企業に対して、容易に見分けがつきかつ容易に入手可能な「シール」を与える。
- 消費者にやさしい紛争解決に関する情報を提供する。
- 参加企業が、少なくとも年に 1 回、みずからのオンラインのプライバシー慣行の評価を引き受ける厳格な要件により、準拠性を監視する。
- 不準拠については、シールの撤回、政府執行機関への公表または照会など、具体的な論

理的結論を申し出る。

消費者には、BBB オンラインのプライバシー・プログラムが、インターネット上で消費者の快適性促進に役立つユーザフレンドリなツールであることがわかるはずである。また企業には、当プログラムが、信頼できるオンライン・プライバシー原則への準拠性を実証する、価格が妥当で、かつ単純、ワンストップ、非侵入的な方法であることがわかる。

4.2.3.4 申請費用について

申請者はすべて、シールの年間使用料以外に、申請書 1 件当り＄75 の一時的処理手数料を支払う。（処理手数料の払戻し不可）

企業の総売上高 （オンライン・オフライン混合）	BBB オンラインのプライバシー・シールの年間使用料
$1,000,000 以下	$150
$1,000,0001-$5,000,000	$300
$5,000,001-$10,000,000	$500
$10,000,001-$50,000,000	$750
$50,000,001-$100,000,000	$1,000
$100,000,001-$500,000,000	$1,500
$500,000,001-$2,000,000,000	$2,000
$2,000,000,000 超	$3,000

現地 BBB(ベター・ビジネス・ビュロー)に対する支持とその会員であることの報償として、BBB オンライン信頼性プログラムへの参加企業は、契約に署名する時点または更新する時点で年間使用料の 50%の割引を受ける資格がある。

非営利団体の場合、シールの年間使用料は、上記の価格設定一覧表を用いた年次予算に依拠する。ドメイン・ネームが複数の企業には、割引が適用される場合がある。

4.2.3.5 考察

まずこのプライバシープログラムの要件としては、申請企業が「開示、選択、機密保護などの、所要の「中核」原則を満足するプライバシー方針をオンラインで通知する」ことである。

そして所要事項を書入れ済みの当該企業の準拠性評価アンケートの審査が行われて、合格した企業に対して、容易に見分けがつきかつ容易に入手可能な「シール」が与えられる。

また参加企業にたいして、少なくとも年に 1 回、その企業のオンラインのプライバシー慣行の評価が行われることになっており、その厳格な要件により、準拠性を監視する。

不準拠については、シールの撤回、政府執行機関への公表または照会など、具体的な措置が講じられる。

また費用面では、年間のマーク使用料として各企業の負担は一律ではなく、その売上ランクにより 150 ドル～3000 ドルまでの幅を持たせている。

4.2.4　プライバシーシールの申込み方法・手順（ステップ・バイ・ステップガイド）概要

続いて上記の各項目の中から、シールの申込み方法について手順部分を紹介して、その項目内容について見ていくことにする。

（ステップ目次）

- ステップ 1：オンラインプライバシー指針を立てる
- ステップ 2：適格基準を見直す
- ステップ 3：文書や情報を集める
- ステップ 4：企業申込書を完成させる
- ステップ 5：査定質問用紙を完成させて提出する
- ステップ 6：ライセンス契約に署名する
- ステップ 7：申込み処理
- ステップ 8：ウェブサイトにシールをインストールする

4.2.4.1　考察

以上が９９年3月以降立ち上がったＢＢＢオンラインのプライバシーシールプログラムの申込み要領の概要である。次に同年 6 月から立ち上がったチルドレンズシールについても見ていく。

4.2.4.2　児童のプライバシー・シールについて

(1) 児童のシール要件を満足しなければならない企業

ホームページまたはオンラインのサービスのいずれかの部分が 13 歳未満の児童向けか、または現実に 13 歳未満であることが知られている訪問者から直接識別可能な情報を収集する企業は必ず、児童の補足的評価アンケートにも所要事項を書き入れること。

(2) 児童向けのホームページまたはオンラインのサービス

ホームページまたはオンラインのサービスが児童向けと見なされるのは、シールがカバーすべきホームページまたはオンラインのサービスのいずれかの部分に、児童を誘引しようとす

る構造を実証する明白な客観的特徴がある場合。これらの客観的特徴には、主題、視覚内容、モデルの年齢、言語、広告、周囲の状況などがある。ただし、それらに限定されない。

(3) 現実に知識のある児童から情報を収集するホームページまたはオンラインのサービス

児童向けではないが、現実に 13 歳未満であることがわかっている特定の訪問者から直接識別可能な情報を収集するホームページまたはオンラインのサービスまたはその一部を有する企業も、児童の補足評価アンケートに所要事項を書き入れ、かつ子供のシール要件に適合することが必要。

当該企業がみずからが 13 歳未満の特定の訪問者から目下情報を収集中であることを「現実に知っている」と見なされるのは、申請者が、訪問者の年齢または年齢区分を要求し、ホームページまたはオンラインのサービスの訪問者を年齢にしたがって分離し、ホームページまたはオンラインのサービスを、年齢を判定するか、または申請者が別途どの特定の訪問者が 13 歳未満であるかを知るかまたは聞き知った上で当該訪問者から情報を収集できるものと考えられる積極的な方法で行動するようなやり方で組み立てた場合。

申請者が訪問者から年齢を示唆する非請求情報を受け取り、かつ申請者が当該情報を積極的に引き出さなかった場合、申請者は、児童の補足評価アンケートに所要事項を書き入れたりまたは児童のシール要件に適合する必要はない。たとえば、児童のシール要件は、その掲示板のひとつで、年齢を判定しようと努力しなかったにもかかわらず、ある訪問者の e-mail アドレスならびに当該訪問者の年齢が 13 歳未満であることも表示されている非請求通知を受け取った、一般の人が興味をもつホームページには適用されない。

(4) 職員の判定事項

シールがカバーすべきホームページまたはオンラインのサービスのいずれかの部分が、児童向けであることがわかるかまたは現実に 13 歳未満である特定の訪問者から情報を収集していることがわかりながら、シールの申請者が児童の補足評価アンケートに所要事項を書入れていない場合には、BBB オンラインのプライバシー担当職員は、申請者に対して、そうするように、かつシールが与えられる前に児童のシール要件に適合するように、要求する。

(5) 児童のシールの表示の仕方及び選択について

前述の様に児童向けに、ホームページまたはオンラインのサービスまたはその一部を運用する企業は、原則として子供のシールを表示しなければならない。

児童向けにではなく、ホームページまたはオンラインのサービスまたはその一部を運用しているが、現実に 13 歳未満であることが知られている訪問者から直接識別可能な情報を収集

している企業には、子供のシールを表示する選択の自由がある。

子供のシールを与えられた場合、申請者は、児童のシールを単独で表示するかまたは子供のシールと BBB オンラインのプライバシー・シールの双方を表示することができる。

(6) 児童シールの要件と具体的な遵守事項

BBB オンライン・プライバシーの子供のシール要件は、カウンスル・オブ・ベター・ビジネス・ビュアローの児童の広告審査部門の指針、オンライン・プライバシー同盟、それに 1998 年の児童のオンライン・プライバシー保護法に依拠する。

これらの要件を満足するため、ホームページまたはオンラインのサービスの運用者は、下記を行なわなければならない。

- 直接識別可能な情報を収集、使用または開示できる前に、親の同意を得る。
- 児童に投函または他人と直接交信させる前に、親の同意を得る。
- わかりやすい言語で警告または説明を行う。
- 児童のゲームや活動をオファーする際には、必要以上の情報の収集を避ける。
- ハイパーリンクの提供方法に注意する。
- ｅ-mail を発信する際には、規則を厳守する。

また、シールの参加者はまた、親に対して、みずからの児童から収集した情報への合理的なアクセスやその情報を訂正したりまたは削除したりする権利も提供しなければならない。

4.2.4.3 考察

以上のように、米国では子供のオンラインプライバシーについて、法的な規制として 1998 年の児童のオンライン・プライバシー保護法があり、またオンラインプライバシー同盟等の保護規定等の要件をベースにして、このＢＢＢオンラインのチルドレンズプライバシーシールプログラム等が自主規制の一環として既に機能している訳である。

このプログラムの要件としては、そのサイトが児童（13 歳未満）から、直接識別可能な情報を収集、使用または開示できる前及び児童に投函または他人と直接交信させる前に、親の同意を得ることがポイントである。

またわかりやすい言語で警告または説明を行い、児童のゲームや活動をオファーする際には、必要以上の情報の収集を避ける等もその要件となっている。

4.2.5　関連プレスリリースやニュース報道の反応について

次に「ＢＢＢオンラインのプライバシーシール」全般関連のプレスリリースやニュース報道の幾つかについてその取上げ方を見てみると、特にCNET News.com及びＣＮＮ interactiveでは大きく取上げられて詳しく解説されておりニュース性の高さを物語っている。。

特に CNET News.com の記事は、それまで信頼性プログラムしかなかったＢＢＢオンラインがトラストｅなどと同じくオンライン上でのプライバシー・プログラムを立ち上げた事を大変高く評価する論調となっている。

4.2.5.1　BBB ウェブサイトプライバシープログラムが登場した背景とその意義

その記事によると商事改善協会（BBB）が、ネットサイトのプライバシープログラムをスタートするのは、行政機関による規制をくい止めて、データ収集に関する米国と欧州当局（ＥＵ）との間の衝突を和らげようとする一連の業界努力である自主規制の中で最も新しい動きであったとしている。

「待ちに待った」と言う表現で、このＢＢＢオンラインプライバシーシールの登場を伝えており、このシールプログラムの申込者が消費者の機密情報をいつ集めるか、これをどのように使用するか、そしてどのように保護するかを表示することを義務づける様になった事を紹介している。BBB プライバシーマークの付いたサイトはまた、ネットユーザに記録へのアクセスはさせるが、名前や電話番号、財務情報といったような個人的な詳細情報は収集を制限させる旨も掲載している。

また子供をターゲットにしたサイトは別のシール（チルドレンプライバシーシール）を掲示し、BBB の子供向け広告審査部門が規定するマーケティングガイドラインに従って、12 歳以下の子供からデータを収集する前には親の許可を得なければならない内容になった事も同様に紹介している。

また記事の中でＢＢＢオンラインはガイドラインを遵守しているかどうか監視し、ときにはランダムに実地調査する。つまり「このプログラムは、公正な情報収集に関する我々の基準に合格したウェブサイトに信用あるブランドネームを与えるようなものだ。」というＢＢＢオンラインの顧問弁護士の言葉を取上げている。

一方でこのような自主規制計画は過去にプライバシー擁護論者や米国当局から強制力に欠けるとして批判されたことがあるという経緯を踏まえて、ＢＢＢオンラインは９８ 年夏にプログラムを発表したとき、この要求に応えることを約束したことを伝えているが、これがこのような自主規制策の運営でポイントとなる実効性を担保した苦情処理制度の創設である。

即ちこの組織では消費者のネットプライバシーに関する苦情を集め、企業に対し、回答をして、

状況を是正するための 10 日間の期間を与えることを計画し、企業がそのプライバシー指針に背いていることがわかれば、ＢＢＢオンラインではシールを取り消して無効となったことを公表し、ことによれば連邦取引委員会（FTC）ないしその他の機関に問題を委託する場合もあることを紹介している。

また類似のシールプログラムとの比較と言う点では、ＢＢＢオンラインシールはこのマーケットでは有名なプライバシーの「信頼マーク」であるトラストｅや、会計事務所の「ビッグファイブ」を代表する米国公認会計士協会（AICPA）によって開発されたばかりの認定プログラム、ウェブ Trust と同様のものであるとしている。。

次に費用面での内容として、総売上高により企業はＢＢＢオンライン参加のために年間 150 ドルから 3,000 ドルを支払うこと、それにその参加企業スポンサーはその多くがトラストｅも後援しており、プログラム構築支援のためにそれぞれ 50,000 ドル以上を支払っていることを伝え、AT&T、ヒューレットパッカード、ネットスケープ・コミュニケーションズ、マイクロソフトなどの錚々たるメンバーが支援企業である事を紹介している。

またこのプログラムのスタート以前から、ＢＢＢオンラインはプライバシー団体から潜在能力をプログラムに十分活かしていないと非難されていた背景も説明している。

つまり、別のＢＢＢオンラインプログラムである信頼性シールなどはすでに存在しており、参加団体は 2,300（その時点で）ある。サイトにこのシールがあれば、ＢＢＢオンラインがこの企業を直接訪問しており、数ある検査の中でも特に、ウェブで売り出しているサービスをバックアップできることを確認したことを意味するのがこのプログラムである。

ただ、記事でも指摘している様に、この信頼性シールのある多数のウェブサイト、またオフライン世界において BBB メンバーであるより多くの企業に対して、このプライバシープログラムへの参加は義務付けや奨励策が講じられないかというのが、困難ではあるが最も大きな課題である。この組織の見積によると、270,000 メンバーのうちの 25 パーセントがウェブサイトを立ち上げている。つまり、約 68,000 の対象サイトのうち、これまでのところ、プライバシープログラムへの参加申込み企業はたったの 300 社（その時点で）である。

これに対して、ＢＢＢオンラインでは義務づけを決めてはいないが、奨励策を講じるつもりがあり、適格であれば信頼性プログラムのメンバーに対しては、相当期間の間無償でプライバシーシールを提供する案も持っているとの事である。

即ちこれが、既にリアルの多くの会員メンバーと既にスタートしている信頼性プログラムで実績のあるＢＢＢオンラインが、その持っている組織インフラという点で、そのネット環境整備に果たす役割

の期待値の高さを論じられる所以である。

4.2.5.2　考察

以上を見ても分かる様にオンラインユーザーにとっては、ある意味で待ちに待ったプライバシーシールプログラムの登場であった事が理解できる。ただやはりここにも日米間の自主規制活動について、財政面でのバックグラウンドに違いが浮き彫りにされている。

当然、民間の第三者団体についてはシールプログラムの運営等については、プログラム参加企業から徴収する会費をベースにするのが当たり前であるが、それに加えてＢＢＢオンラインのスポンサー企業からの多額な支援費がそのプログラム運営面で多大な影響を与えているの言うまでもない。それがまた BBB オンラインの支持者から期待される所以でもある。

そしてゼロからのスタートでなく、リアルの会員・信頼性プログラムの参加メンバー含めて、ネット環境整備の為の自主規制プログラム執行のインフラがこれほど整っている民間団体は、世界に類を見ないだろう。

4.2.5.3　BBB のオンライン・プライバシー認証マークの位置付け

次にCNN interactive の記事によると、Council of Better Business Bureaus の子会社としての Better Business Bureau Online(ＢＢＢオンライン)は、オンライン・プライバシー認証マーク制度が、ウェブサイトが消費者の個人情報をどのように扱っているか知るために役立つと述べている。98 年の政府による調査でプライバシーに関するポリシーを掲載しているウェブサイトの数が比較的少数であることが判明してから、インターネット業界は厳しい監視の目にさらされることとなったこと、及びインターネット業界の後援でジョージタウン大学のインターネット・プライバシー調査が始まり、企業のプライバシー・ポリシー開示に改善がみられたかどうか見直しの調査がなされた事も述べられている。

この記事によると、プライバシー情報開示の象徴となる認証のマークは青、黒、白の 3 色で地球が意匠化されている、と言うことである。

さらにＢＢＢオンラインでは、子供向けの広告のウェブサイトには、はっきりと異なる認証マークを付与し、毎年、企業のオンラインでのプライバシー管理制度を評価して、規定に従わない企業に対しては認証マーク使用の取消し又は政府機関への通知などの措置を取るということだ。消費者は、このプライバシー保護制度に加入している企業であるかどうかにはかかわらず、問題のある企業に対する苦情の申立てをすることが出来、同社ではその苦情に対する判定を公表するとしており、さ

らに、異議申立てを受け付ける中立の制度もあることも紹介している。

業界を監視している関連団体メンバーの中には、ＢＢＢオンラインでは、企業が自社のプライバシー・ポリシーを正直に開示することを奨励していくことを目標としているが、それが成功するかどうかは今後を見守る必要があるとして、この制度事態が「誤解を招く」ものであるとする意見もある。つまりウェブサイトにはプライバシーに関するポリシーが掲載されているかもしれないが、「それがプライバシーの保護となる適正な制度であるかどうか保証はない。」そしてこういった制度は、それが「真の法的保護の代わりとなる適正な制度」であることを証明していかなけらばならないという見解を紹介している。。

4.2.5.4　考察

紹介した記事の最後の内容には、一般的なシールプログラム制度に対する警鐘内容として、「法的保護の代わりとなるかのごとく誤解を生む制度」だという意見が紹介されているが、ここでいうプログラム制度は決して法制度を代替できるような拘束力・抑止力は必ずしも必要としない前提である事を全く理解していない意見となっている。

オンラインシールプログラムとは本来、民間自主規制の一環であり、行政施策の肩代わりをするものでなく、消費者にとってのよりベターな取引環境整備の為の自己防衛方策であり、法制度とは全く次元の違う話題であることを良く認識しなければならない。

また AT&T 研究所主導の調査記事では、回答者の 28%がサイトにプライバシー指針が掲示されていれば情報を提供する可能性が高くなり、サイトが請求処理以外の目的で情報を使用することを防ぐ規制があれば 48%が提供するが、サイトにプライバシー指針とＢＢＢオンラインプライバシーシールの両方があれば 58%が情報を提供するということがわかった。

これら一連の記事を読んでも分かる様に、BBB オンラインのプライバシーマークプログラムは米国内で高い評価を受けている。具体的には FTC ワークショップや米国情報技術協会（ITAA）それに家電品製造業者協会（CEMA）等のサポート表明や協力体制のオファーがあり、いわゆる世間的に認知されたマーク制度として機能していると言えよう。

また Kodak、AT&T 研究所、エキファックスといった主要な民間企業からも充分な評価を受けており、第三者機関だけでなく実質のスポンサーである民間企業自身の認知度が高い事がこの記事からも伺われる。

4.2.5.5　ＢＢＢオンラインの企業スポンサー

次はこういった BBB オンラインの活動を資金面からも支えている、主要スポンサー企業の一覧である。

以下の各社は、ＢＢＢオンラインがインターネットにおいて消費者を保護できるよう、指導および財政支援を提供し、各社ともＢＢＢオンライン取締役会に代表を送っている。

- Ａｍｅｒｉｃａｎ Ｏｎｌｉｎｅ
- Ａｍｅｒｉｔｅｃｈ
- AT&T
- Ｂａｎｋ ｏｆ Ａｍｅｒｉｃａ
- Ｄｕｎ＆ Ｂｒａｄｓｔｒｅｅｔ
- Ｅａｓｔｍａｎ Ｋｏｄａｋ
- GTE
- Ｈｅｗｌｅｔｔ－Ｐａｃｋａｒｄ
- IBM
- Ｍｉｃｒｏｓｏｆｔ
- Ｐｒｏｃｔｅｒ ＆ Ｇａｍｂｌｅ
- US WEST・Ｍｅｄｉａ・Ｇｒｏｕｐ
- 米国ＶＩＳＡ e.t.c.

4.2.5.6　考察

これらの企業名を見ても分かる様にネット・IT関連の主要企業が名を連ねている。ここにＢＢＢオンラインがそれらの企業の財政面での支援を受けて、一民間団体としてはなかなか困難な消費者保護の為の様々なシールプログラムを展開できる要因のひとつがあるのではないかと思われる。

つまりシールプログラムの運営に当たっては、各スポンサー企業からの支援のおかげで、そのプログラム参加企業からの収入だけに頼った形でなく、本来のプログラム趣旨を生かした展開が可能となり、様々な点で自由度が上がると言えよう。

そしてここにこそ、米国でのこういった自主規制シールプログラムの恵まれた環境がある。それに比較して、日本国内ではシールプログラムの運営自身が第三者機関に委ねられた場合、スポンサー企業をバックに持っている米国のそれと違い、その団体の財政面からしてそのプログラム自身での独立採算になる事が多く、そこに自ずから普及・展開の限界点（パブリシティや年間費用の費用設定等の課題）が出てくるものと思われる。

次にＢＢＢオンラインの連絡先及びシールプログラムについての問い合わせ先等をウェブ上に掲載し、苦情申し立てやサポートについてもホームページ上で対応できる様になっており、むろんの電子メールでのやり取りも可能である。参考に取上げてみた。

4.2.5.7　ＢＢＢオンライン連絡先

ＢＢＢオンラインもしくはシールプログラムに関する情報については、以下住所宛に連絡のこと。

- ＢＢＢオンライン, Inc.4200 Wilson Boulevard
  8th Floor Arlington, VA 22203
  ＢＢＢオンラインスタッフ
- 電話
  - 信頼性シールプログラム 703 247-9370
  - プライバシーシールプログラム 703 247-9336
  - オンラインプライバシー紛争解決受付センター 888 679-3353
- ファックス 703 276-8112
- 連絡フォーム
- 電子メールで連絡するときの使用フォーム
  - 名前：
  - 電子メールアドレス：
  - 会社名：
  - 電話：
  - 連絡理由：
  - 質問ないし意見

4.2.5.8　考察

以上がＢＢＢオンラインの連絡先及びシールプログラムについての問い合わせ先等のフォーム内容である。ここにこのシールプログラムの評価できるポイントが列挙されている。つまり一般消費者の苦情処理窓口としての機能を有する点である。

この苦情申し立てやサポートについての面倒な作業が、簡単にホームページ上で対応できる様になっており、むろんの電子メールでのやり取りも可能であるところが、何かあった時に非常に便利である。

やはりこういったシールプログラム（マーク制度）については、単なるマーク審査・付与業務だけでなく、この消費者の立場に立った苦情・紛争解決プログラムとの連動という面がその実効性の担保と言う観点からも見逃してはならないポイントであろう。

以上の様にＢＢＢオンラインのシールプログラムについては、当初は上記にもある様にWWW向け信頼性保証プログラム、ＢＢＢオンライン信頼性シールプログラムからスタートした経緯がある。

そして前述の様に1998年ＥＵのデータ移転禁止条項の発効を受けて、米国内で当局による規制をくいとめて民間の自主規制の弱点を補おうとする新しい動きとして、１９９９年の３月にプライバシープログラムが注目を集めてスタートした。

このプログラムのスタートは、既にこのマーケットでは有名なトラストｅの「トラストマーク」制度や最近開発されたばかりの米国公認会計士協会（AICPA）の「ウェブトラスト」プログラムとは別な意味でまた意義深いのは当然である。

というのも前述の様に270,000ものＢＢＢ加入メンバー（オフライン会員含む）のうち25％にあたる67,000以上がウェブサイトを立ち上げており、このオンラインメンバーが今回のプライバシー・シール・プログラムの対象となるからである。

例えば、信頼性シールプログラムのメンバーに対しては、相当期間、無償でプライバシー・シールを交付するとかの案がある。

つまり、加入メンバーの数量的なインフラの整った団体としてのプログラム制度立ち上げの効果が期待できるからである。ここが前述の様にＢＢＢオンラインのプライバシーシールプログラムの存在意義でもあり、またその位置付けの重要性の所以でもある。

これは即ち、消費者にとってより多くのサイトがプライバシー保護を意識して、このプログラムに参加することで、我々消費者にとってはオンライン上の個人情報保護環境がより改善される事を意味する。

4.3　トラストｅプライバシーマークについて

さて次に消費者のプライバシー保護の為の民間自主規制としては、前述のＢＢＢオンラインプライバシーシールプログラムより以前からスタートしているトラストｅのプログラムについて、調査･入手した各資料をベースに紹介していくものとする。このトラストｅは信頼性シールは持っておらずに、プライバシープロフラムオンリーの運用である。

4.3.1　トラストｅという団体について

トラストeはオンライン取引における国際的信用と信頼を創造することを唯一の目的とした非営利団体である。公正な情報慣行を指針として、トラストeシールプログラムはウェブパブリシャーに、トラストeの第三者監視プロセスに支えられた標準プログラムを提供する。各ウェブパブリシャーはこのプログラムを使用して、各サイトの情報収集および普及慣行に関する情報をユーザーに提供することができる。トラストeは定期的にサイトの検討を行い、消費者に問題解決メカニズムを提供する。トラストeのガイドラインに準拠したサイトには“トラストマーク”の表示が許可され、プライバシーシールプログラムに参加していることをユーザーに知らせることができる。

トラストeの優良企業後援者のネットワークには、America Online、Compaq、Ernst & Young、Excite、IBM、MatchLogic、Microsoft、Netscape および Novell 等が含まれる。

4.3.2　トラストｅの主要な 3 つの使命

インターネット上の消費者としてユーザーにはそれぞれの個人情報がどのように使用されているのかを知る権利がある。そしてトラストｅには主に次の 3 つの使命がある。

①インターネットが提供する全てを楽しみながら、ユーザーの意見に関してユーザーを啓蒙する。このウェブサイトはユーザーにオンライン上のプライバシーを守るために必要な資源、ツール、支援を提供することを目的とする。

②企業に対し、プライバシーに関する声明の掲示およびトラストｅの第三者監視“証印”プログラムへの参加を奨励する。

③必要に応じ、消費者とトラストｅのライセンシーとの仲介役を引き受ける。

4.3.3　オンライン上でのプライバシー保護

トラストeにおける基本的考え方として、ユーザーには、各ウェブサイトがそのプライバシー方針を公開することを期待する権利がある。さらに、ユーザーには個人情報の収集、使用および他のウェブサイトとの共有の方法、あるいは収集、使用および共有を許可するかどうかについても選択権を行使する責任がある。トラストeおよびトラストeのライセンシーは、相互信頼と公開性に基づく環境がインターネットを全てのユーザーにとって自由、快適かつ広範な多様性を持つ場にし、その状態を維持することに役立つものと考えている。

(1) Privacy Links and Resources（プライバシーに関するリンク先および資源）

：オンラインプライバシーに関してユーザーが知っておく必要のある全ての情報、主なウェブ

サイトの包括的なリストをトピック別に並べ、参考資料やリンク先が即座に分かるようにしてある。

(2) Contact Us（連絡下さい）

トラストｅはあらゆるコメント、質問および問題をお待ちしています。E メール、電話（(408) 342-1940）またはファックス（(408)342-1950）か、下記の住所に手紙で連絡してください。

- トラストｅ

  10080 N. Wolfe Road, SW3-160

  Cupertino, CA 95014

- トラストｅへの E メール

  入会方法：inquiries@トラストｅ.org

  報道またはマスコミ：press@トラストｅ.org

  現在のライセンシーに関する質問：licensee@トラストｅ.org

  質問および問題：info@トラストｅ.org

(3) トラストｅプログラム：プライバシー保護の方法

トラストeは、相互信用と公開性に基づく環境が、インターネットを全ての人にとって自由、快適かつ広範に多様なコミュニティーにし、その状態を維持するのに役立つものと考えている。

インターネットユーザーとして、オンラインでのプライバシーを期待する権利と個人情報の収集、使用および他のウェブサイトとの共有に関してその方法を選択する責任がある。

トラストeのプログラムは、オープンな情報開示を通じてユーザーのプライバシーが保護されることを保証し、ユーザーが情報に基づく選択ができるようにすることを明確な目的としている。

トラストeプログラムの基礎はトラストeの会員のウェブサイトが表示するオンライン商標証印である“トラストマーク”である。トラストマークは、確立されたプライバシー原則を厳守し、トラストeの現行の監視および消費者解決手続きへの準拠に同意するウェブサイトのみに与えられる。プライバシー原則はアメリカ合衆国商務省、連邦取引委員会および主要産業代表組織および協会によって認められた公正な情報慣行を体現している。プライバシー原則には以下が含まれる。

- 個人情報をオンラインで伝える消費者の不安を考慮したプライバシー方針の採用および実施

- 情報収集および使用慣行の通知および開示
- 選択および合意。個人情報に関して管理する機会をユーザーに与える
- 個人を特定できる情報のセキュリティおよび正確さの保護に有効なデータセキュリテおよび品質・アクセス対策

(4) トラストマークはユーザーにとっては何を意味するのか？

トラストeのトラストマークを表示するウェブサイトはすべて、簡潔なプライバシー声明のなかに、それぞれの個人情報収集慣行およびプライバシー慣行を開示しなければならないことになっている。プライバシー声明には通常ホームページからリンクされる。一つのサイトのなかで個人情報に関するプライバシーの取り扱いが異なる場合、2 つ以上のトラストマークが表示されることもある。

(5) トラストｅ証印が表示されていれば、そのウェブサイトに必ず開示されている事項。

- ユーザーについてどのような個人情報が収集されているか
- その情報はどのように使用されるか
- 情報を共有する組織がある場合、どういった組織とその情報を共有するのか
- 収集された情報の使用方法に関してユーザーに選択肢が提供されていること
- 紛失、不正使用または変更などからユーザーの個人情報を保護する措置が講じられていること
- 誤った個人情報を更新あるいは修正できる方法

(6) トラストｅの子供プログラムはどのように子供のプライバシーを守るのか？

トラストeは、プライバシーの問題に関して、13 歳未満の子供に特別の必要性があると認識している。多くの場合、幼い子供は個人を特定できる情報を提供することの意味を理解できない。したがって、子供証印を表示しているウェブサイトでは、情報が収集される時点およびその場合に事前に立証可能な親の同意を得ること、そしてその情報がどのように使用されるかを親に通知することを明言している。

子供証印を表示しているサイトにアクセスする親および子供は、トラストeが継続的に検査を実施し、そのサイトがプライバシー声明に違反していないことを保証しているとともに、そのサイトがトラストeプログラムに準拠していないと消費者がみなした場合に、正式な苦情および解決プロセスが存在していることをも知ることになる。

具体的には、13 歳未満の子供を対象とし、トラストeのライセンスを受けることを希望するサイトはすべて、標準トラストeプログラムの規定を厳守し、さらに下記の規定（子供プライバシー証印の条件）を遵守しなければならない。

(7) 子供プライバシー証印の条件

13 歳未満の子供を対象としたウェブサイトの場合、そのサイトには以下が禁止されている。

- 前もって立証可能な親の同意を得ずに、あるいはその情報の性質や予定の使途を直接には親に通知せずに、13 歳未満の子供からオンラインで連絡先情報を収集すること。（これには、親がその情報の使用および活動への参加を防止する機会が含まれる。）事前の親からの同意が得られない場合、オンラインでの連絡先情報は直接その子供の要求に対応するためにのみ使用され、他の目的で再度その子供にコンタクトを取る目的では使用されないこととする。
- 事前の立証可能な親の同意なしに、13 歳未満の子供から個人を特定できるオフラインの連絡先情報を収集すること。
- 事前の立証可能な親の同意なしに、13 歳未満の子供から収集した個人を特定できる情報を第三者に配布すること。
- 事前の立証可能な親の同意なしに、13 歳未満の子供に個人を特定できる情報を公に掲示したり、その他の方法で配布したりする能力を与えること。各サイトは子供によるあらゆる連絡先情報の掲示を禁止するよう最大限努力する。
- 特別なゲーム、賞品または他の活動を期待させて子供を勧誘すること。そのような活動への参加に必要とされる以上の情報を公表すること。
- 各サイトは、個人を特定できる情報が収集されている場所に明確な通告を掲示し、質問に答えるためには親に許可を求めるよう子供に要求しなければならない。

4.3.4 トラストｅによる監視および解決

トラストeのトラストマークを表示する全てのウェブサイトは、トラストeの監視および苦情解決手続きへの準拠にも同意している。トラストeでは、次の多様な手段により、プログラム原則および掲示されたプライバシー慣行への各ライセンシーの遵守状況を監視している。

- トラストｅによる初期および定期検査
- “Seeding” – これにより、各サイトが明言したプライバシー方針に従っていることを確認するために、トラストｅが個人ユーザー情報をオンラインで提出する

- 公認会計士事務所による準拠検査
- オンラインコミュニティーからのフィードバックおよび苦情
- トラストマークの使用許諾権侵害を抑止するためのクリック・トゥ・ベリファイ証印

ライセンシー（参加企業）はすべて、プライバシー声明上にクリック・トゥ・ベリファイ証印を掲示しなければならない。この証印をクリックすると、トラストeのセキュアサーバにアクセスし、そのサイトが実際にトラストｅの法的なライセンシーであることを確認できる。

ユーザー側の用心も必要である。実際、掲示されているプライバシー方針に対する違反、トラストマークの不正使用、トラストeのメンバーであるウェブサイトに関する具体的なプライバシーに関する不安の報告には、直接トラストeに連絡をとることをユーザーの皆様に推奨する。その方法についてはウオッチドッグ（下記）を参照のこと。

(1) トラストｅ ウォッチドッグ

掲示されたプライバシーに関する方針の違反、トラストマークの不正使用、または特定のプライバシーに関する特定の問題を報告するための便利なメカニズムをユーザーに提供するためにウオッチドッグページを創設した。ただし、報告はライセンシーのウェブサイトに関する違反に限定される。ウェブサイトがトラストｅプログラムのライセンシーかどうかを確認するには、トラストｅ licensees リストを参照のこと。

下記の電子ウオッチドッグ Report に記入し、プライバシーに関する不安または苦情をトラストｅまで提出のこと。

(2) ウオッチドッグ Report への記載内容

① プライバシー侵害をどこで発見したか？

掲示しているプライバシー慣行に違反しているとあなたが考えるトラストeライセンシーのウェブサイトか、詐欺的にトラストｅのトラストマークを表示していると疑うウェブサイトを入力。

注：レポートを提出する前に、そのウェブサイトのプライバシーに関する方針を必ず読むこと。トラストeのライセンシー以外のサイトに関する要請あるいはウェブサイトに掲示されたプライバシーに関する方針に直接関係のない要請については、トラストｅでは処理すること不可。

注：ウオッチドッグ Report に記入する前に、ユーザーのプライバシーに関する問題を直接そのウェブサイトに連絡のこと。そのサイトが 5 営業日以内にその問い合わせを受け付けない場合あるいはその問題に対して十分な対策を講じない場合には、トラストｅに連絡すること。

② トラブル相手のサイトに連絡したが十分な解決策は提供され無い場合は？

- これまでに問題のサイトと交わした通信内容の説明。
- プライバシーの侵害内容および希望する解決方法。
- 問い合わせの進捗状況について、トラストｅから新しい情報を常に希望する場合

Name（氏名）：

Email（E メールアドレス）：

(3) 問題サイトへのユーザー情報の開示制限

報告した問題の真相究明には、ライセンシーに対して、ユーザーの苦情の一部やEメールアドレス、氏名をトラストeから開示することが必要であったり、場合によっては要求されたりする場合さえある。但し下記の許可をユーザーが与えない限り、トラストeがこの情報を提供することはない。

ユーザーまたはトラストeが提起した苦情を解決するために、ライセンシーはトラストeの検査および問い合わせに全面的に協力することに同意している。トラストeライセンシーに関する問い合わせまたは苦情に対して満足のゆく解決に至ることができない場合には、規模を拡大して調査を実施しする。違反の重大さによるが、このプロセスの後、公認会計士事務所によるウェブサイトの遵守状況検査、トラストマークの取消、トラストeプログラムからの退会、契約違反訴訟手続き、あるいは適切な連邦当局への付託などが実施される。

4.3.5 考察

以上直接の説明文・記事等に加えて、分かりやすいQ＆Aによる内容記述を見てきたが、文中にもある様に、現在このトラストｅのプログラムは米国だけでなく、その活動範囲をヨーロッパまで拡大し、プライバシー保護認定シールの発行地域を広げている。

1998 年、欧州委員会はＥＵと同等のプライバシー保護措置を取らない国との情報交換の差し止めを指示しており、トラストｅの動きは、やはりこのようなＥＵの情勢を考慮した国際企業の自主規制の高まりを踏まえての事と考えられている。

もともとこのプログラム自身が、９8 年の春時点はわずか 30 サイトに過ぎなかった上に、そのうち約 3 分の 1 は、消費者向けサイトというより、WWW 広告や技術関係のベンダーが占めるという状況であった。ところが1998 年の FTC の調査結果による規制導入のプレッシャーを受けて、にわかに大手企業がトラスト e の存在に注目。業界内での自主対応の取り組み姿勢を示すために、一斉に参加を表明した。この中には、 AOL、ヤフー、ライコス、インフォシーク、エキサイト、ディズニー、

CNET、ジフ・デイビスなど、ビッグ・ネームが含まれており、プログラム参加サイトは、全体で一気に 130 カ所以上にもその当時で膨れ上がることになった。

これによりトラストｅは、業界標準プログラムといえる規模を獲得。活動もやっと軌道に乗ったといういきさつがある。ちなみに参加費用は企業規模に応じ、年間 249～4999 ドルである。

ＢＢＢオンライン等と同じく、参加 WWW サイト上に置かれたトラストマークをクリックすると、そのサイトのプライバシー・ポリシーが見られる仕組みである。

またトラストｅでは、前述の様にプライバシー・マークの使用を取消し、悪質なケースは政府当局に通報する。現在では Excite、eBay、及び Yahoo!など、700 以上のウェブサイトがトラストｅのマークを付与されている。９９年の終わりまでには、その数は 1,600 に昇ると予想されている。

4.4　米国公認会計士協会（AICPA）による「CPA ウェブトラストマーク」

次に三つ目のプライバシー保護のシールプログラムである米国公認会計士協会による「CPA ウェブトラストマーク」について見ていくことにする。

4.4.1　電子商取引における信用と信頼を確立する公認会計士（CPA）ウェブトラスト

公認会計士ウェブトラストのマークをクリックすると次の事項が閲覧出来る。

4.4.1.1　閲覧事項

- 公認会計士宣誓書
- 業務慣行の開示
- ウェブトラストの原則と基準へのリンク
- 経営陣よりの保証宣言
- その他の関連情報

4.4.2　公認会計士ウェブトラストの原則

- 業務慣行の開示
- 取引の倫理性管理
- 情報保護の管理

の３原則をベースとしている。各項目を説明して行く。

(1) 業務慣行の開示

電子商取引に関する業務慣行を開示し、開示したとおりの業務慣行及びプライバシー情報の管理を行う。

① 業務慣行の基準

A. 新規の消費者からの苦情相談制度

消費者は次の事柄に関する苦情を解決することが出来ます。

- ウェブトラストの原則＆基準
- 正確性、完全性及びお客様の個人情報の回覧
- 商品の品質

消費者の利便性を考慮し、オンライン上で強制力を有する裁定を開始することが出来ます。

B. 業務遂行の規則、条件

- 商品、情報、サービスの性質
- お客様の得られる保証やその他のサービス
- お客様のクレイム、苦情に対する相談を受付に関する情報
- プライバシー情報

(2) 取引の倫理性

電子商取引における手続きが同意したとおりに行われ、請求がなされることに対し、お客様が信頼をおくことが出来るように効果的な管理体制を敷いている。

① 取引の倫理性に関する基準

公認会計士は、以下の事項に関する内部管理及びお客様との取引において厳しく詳細に渡る確認作業を行う

- ご依頼の仕事における正確性及び完全性を確認する。
- 適切な接客態度を保つ。
- 適正な商品及びサービスを提供する。
- 請求及び清算を正確に行う。

(3) 情報の保護

電子商取引により獲得したお客様の個人情報が他の目的のために使用されることがないということをお客様に保証し、信頼を勝ち得るための効果的な管理を維持する。

① 情報保護の基準

公認会計士は、以下の事項に関する内部管理及びお客様との取引について厳しく詳細に渡る確認作業を行う

- お客様の個人情報の収集
- お客様の個人情報の送信
- お客様の個人情報の使用及び保護
- お客様のコンピューター及びファイルをコンピューター・ウィルスから保護

4.4.3　内部管理の評価

内部管理の評価は、取引の倫理性及び情報保護の基準を維持するために不可欠な作業。

内部管理の環境は、次のことに寄与するものでなければならない。

- ウェブサイト上での信頼のおける業務慣行開示
- 電子商取引の倫理性を維持するための効果的な管理
- お客様の個人情報保護の効果的な管理

ウェブトラストは、厳しい検査の実施により電子商取引の詐欺防止に役立つ。

4.4.4　ウェブトラスト・マークの取得方法

- 認可を受けている公認会計士にご連絡下さい。（全米 150 社）
- 公認会計士が検査のレベルと範囲を決定します。
- ウェブトラスト・マークの見直しの期間を決定します。（90 日以下）
- 費用は年間 1,400 ドル及び公認会計士料（時間制）となります。

4.4.4.1　　ウェブトラスト：国際的なサービス

ウェブトラストは以下の公認会計士及び各国の公認会計士に相当する有資格者によるサービスである。

- アメリカ合衆国
- カナダ
- イギリス
- アイルランド
- オーストラリア
- ニュージーランド
- さらに、すぐにオランダ、フランス、ベルギー及びドイツが加わる。

ウェブトラストは、世界中どこでも同一の製品（法規の変更により改定されることがあります）を提

供する。

4.4.5　ウェブトラストマーク保護基準内容のまとめ

- 包括的な業務内容の開示
- セキュリティの検査
- プライバシーの検査
- 取引履行の検査
- 消費者の苦情相談部門の設置
- 国際的なサービス
- 公認会計事務所による品質管理の監督
- 詐欺防止

4.4.6　公認会計士ウェブトラストによるサービスの大要

- 消費者向け電子商取引に焦点を当てている。
- ウェブトラストの原則及び基準（バージョン 2）に基づくサービスである。
- 担当公認会計士は研修を終了したアメリカ公認会計士協会の認定を受けた公認会計士である。
- ウェブサイトには公認会計士の報告書が掲載されている。
- ウェブトラスト認定のマークは最長 90 日の期間で見直しがなされる。
- ウェブトラスト認定のマークはアメリカ公認会計士協会及び公認会計士が管理する。
- 公認会計士ウェブトラストは、サービスの質を維持するため中立機関による点検を受けている。

4.4.7　考察

これについては日本国内でも同じサービス内容を「監査法人トーマツ」が提供しているもので、ＢＢＢオンラインやトラストｅよりもさらに消費者に対する保護範囲を広げてチェック項目を増やしたいわばオンライン取引におけるあらゆる保護内容を盛り込んだものである。ただそれだけにコスト面での事業者負担費用が高い事が特徴として挙げられる。

これまでの二つのマーク制度と大きく違う点は、その保護範囲の広さと共に、このＣＰＡウェブトラストマークは営利目的を含むマーク制度という点である。

4.5　プライバシー保護関連の各民間団体の活動について

ここからは、米国を中心に活動しているプライバシー保護関連の各団体についての調査内容を報告する。

国内と違いプライバシー保護関連だけを目的にした専門的な活動を展開している民間の非営利団体があるというのがまず驚きの一つである。

それと共にその活動を支援するスポンサー企業の存在（各企業名を詳細に後述）がここまで米国内でのオンライン上のプライバシー自主規制推進の原動力になっているといっても過言ではないだろう。

4.5.1　オンライン・プライバシー・アライアンス（Online Privacy Alliance（OPA））

さて次にプライバシー保護関連の各団体のうちでも有名な存在であり、代表的な民間団体ということでも前述したオンライン・プライバシー・アライアンス（Online Privacy Alliance（OPA））がウェブサイトを調査した結果を公表している。既に一部前述した様に、自主規制の目覚しい進歩を詳細に物語る内容となっている。

1998 年、民間のインターネット業界は、85 の企業及び団体からなる Online Privacy Alliance を創設し、企業がプライバシー・ポリシーを作成する際に用いるガイドラインを制定し、児童のプライバシーを保護する基準をつくり、ＢＢＢオンラインやトラストｅのプライバシー保護認証マーク制度の枠組みを作り上げ、全米において何百もの企業の 17,000 人の企業幹部に対してオンライン上のプライバシー保護を求める手紙を出し、啓蒙をしてきた。

OPA 会員企業は、それぞれの企業ベースにおいても、より多くの企業がプライバシー・ポリシーを掲載するよう働きかけ、消費者に対してはどのようにして自己の個人情報を守っていくか指導をしてきた。数多くの OPA 会員企業及び団体が発揮してきたイニシアチブと努力の結果が、ウェブサイト上のプライバシー保護環境の整備につながった事は間違いない。

4.5.1.1　OPA のウェブサイト調査の結果

Online Privacy Alliance は、ウェブサイト調査の結果、プライバシー保護のための自主規制制度に目覚しい進歩がみられたことが確認された、と発表した。

- プライバシー保護を確立する民間の取り組みにより、アクセス件数上位 100 社では、94%が消費者に役立つプライバシー・ポリシーを掲載していることが判明

● より広いウェブサイトの任意抽出調査でも 66%がプライバシー・ポリシーを掲載

1999 年 5 月 12 日に米国の消費者のプライバシーを保護する自主規制を促進している国際企業及び商業団体の集まりである Online Privacy Alliance（OPA）は、当日発表されたジョージタウン・インターネット・プライバシー・ポリシー調査及び OPA 上位 100 社調査により、サイバースペースにおけるプライバシーの保護措置には顕著な進歩が見られたと述べた。

ジョージタウン調査では、アクセス件数上位 7,500 社のウェブサイトのうち、364 社の「.com」ウェブサイトを任意に選んで調査を実施した。OPA 上位 100 社調査は、1998 年の連邦取引委員会が調査したアクセス件数上位 100 社の 2 年目の調査である。

このジョージタウン調査によると、少なくとも 1 つはプライバシーに関する開示事項（プライバシー・ポリシー掲載又は個人情報の扱いに関するステートメント）を掲載しているウェブサイトは全体の 65.7％であった。また、OPA の調査では、上位 100 社のうち、少なくとも 1 つはプライバシーに関する開示事項を掲載しているウェブサイトの割合は、1998 年の 71%から 94%に上昇した。

これについて OPA の広報からは「1 年で目覚しい進歩を遂げた。プライバシー・ポリシーは、比較的短期間に、人気の高い消費者向けウェブサイトでは当たり前のものとなり、信頼のおける中立の制度により企業がポリシーを遵守していくように厳しい監視がなされている。また調査結果を見ると、今後は、プライバシー・ポリシーがインターネット全般に普遍のものとなり、消費者にオンライン上でのプライバシーは保護されていると信頼されるようになることが課題だ。」というコメントが出ている。

ジョージタウン大学のマクドナル経営学部の Mary J. Culnan 教授によるこの調査は連邦取引委員会の依頼によるものである。調査データの提供は Media Metrix、データ収集は Ernst & Young の協力による。ジョージタウン調査の資金提供は下記の企業による。また、上位 100 社調査は、オンライン・プライバシー連盟の資金提供による。

Culnan 博士は、「この調査は消費者のウェブサイト選択傾向を反映している。98.8％の消費者が選ぶウェブサイトにはプライバシー・ポリシーがある。」と語った。

OPA では、この調査結果を今後の活動に生かしていくつもりだと言う。今後は小企業や新規のビジネスも含めすべてのウェブサイトが大企業を見習ってプライバシー・ポリシーを掲載し、消費者のプライバシーを保護することの重要性を認識するよう事業者の啓蒙を続けていかなければならない。

さらに、このような様々な調査を見ると、インターネット業界は、消費者が安全と感じられる明るい街燈に照らされた大通りを造り上げているように見受けられる。消費者サイドにプライバシーに関す

る懸念は見られるものの、電子商取引は目覚しい勢いで増えている。政策担当者は、自主規制の進展を認識し、電子商取引の成長を妨げるおそれのある早まった規制は避けるべきであろう。

4.5.2　ＥＰＩＣ（エレクトロニック・プライバシー・インフォメーション・センター）について

次にもう一つのプライバシー保護に関する団体であるＥＰＩＣを紹介する。

4.5.2.1　エレクトロニック・プライバシー・インフォメーション・センター（EPIC）の沿革

EPIC はワシントン D.C.にある公益研究センターであり、新たに浮上する市民的自由に関する問題に対しての一般市民の注目を集め、プライバシー、合衆国憲法修正第 1 条および憲法の価値観を保護すべく 1994 年に設立された団体である。

さらに EPIC は Fund for Constitutional Government のプロジェクトであり、英国ロンドンを本拠とする国際人権団体の Privacy International と共同で活動し、Global Internet Liberty Campaign、Internet Free Expression Alliance、Internet Privacy Coalition、Trans Atlantic Consumer Dialogue(TACD)のメンバーでもある。

例えば EPIC による代表的な訴訟内容としては、EPIC の法務チームが提訴したプライバシー、合衆国憲法修正第 1 条、情報公開法に関する判例等があるが、サイバースペースでの市民の権利を守るためのものである。

4.5.2.2　EPIC の最近の活動について

- EPIC の繰返し懸念表明により委員会は FBI“重要インフラ”プランに対する資金を禁止

上院歳出委員会は、“重要な”民間部門業界が使用する非軍事政府コンピュータネットワークおよび通信ネットワークを監視するという、連邦捜査局（FBI）のプログラムに対する支出案を禁止した。“重要インフラ”を保護する政府の努力は、アメリカ国民のプライバシーおよび市民的自由にとって重大な脅威になると EPIC は繰返し懸念を表明してきた。（EPIC の 1998 年 10 月付報告書“重要インフラ保護と市民的自由の危機”およびホワイトハウスの“情報システム保護に関する国家計画”の抜粋については、EPIC の Critical Infrastructure Protection Resources を参照のこと。）

- 子供のプライバシー等に関する新たな報告

プライバシー、消費者および子供の擁護団体は、数多くの商業ウェブサイトが親の許可なく年少者に関する情報を引き続き収集していると警告する新しい報告書を発行した。Center for Media Education、Consumer Federation of America および Junkbusters は、連邦取引委員会による、オンライン上の子供のプライバシーに関する明確かつ有効な安全措置を要求した。

その他、政府等に対しての対抗措置として、EPIC は法案追跡も行っており、その代表例としては、第 106 回議会のプライバシーおよびコンピューター上の自由に関する審議中の法案の追跡があげられる。

4.5.2.3　考察

EPICとは文中にあるようにワシントン D.C.にある公益研究センターで、プライバシー、合衆国憲法修正第 1 条および憲法の価値観を保護すべく 1994 年に設立された。EPIC は Fund for Constitutional Government のプロジェクトである。米国にはこういった任意団体がプライバシー等の問題に関して精力的な活動を展開している例の枚挙には暇がない。

この団体の特徴としては法務チームを持っており、議会・政府関連にもかなりの影響力があり、またインターネット上の言論の自由に関する諸問題およびオンライン児童保護法に対する現在の課題についての言及等幅広い活動を行っている。

こういった行政側ではない団体としての積極的活動は、さまざまなインフラ普及の為に効果的な影響を与える場合が多いと思われる。

例えばＥＣ上のプライバシー論議にしても、そういった意味での監視能力（オンブズマン制度やウォッチドッグ機能の具備）という点でこういう任意団体の存在は、我々消費者としての一個人の立場からすると非常に心強い。

その意味からも、こういった個人情報保護関連で影響力とパワーをもつ団体の誕生が、日本国内でも早急に望まれる所以である

。

4.5.3　米国連邦取引委員会は「自主規制及びオンライン・プライバシー」に関する報告書を議会に提出（1999 年 7 月 13 日）」の記事より（抜粋）

連邦取引委員会は、議会でオンライン・プライバシーに関する消費者保護の問題でインターネット業界の取り組みの現状について証言し、「自主規制及びオンライン・プライバシー」と題する報告書を提出した。

この報告書は、同委員会の 4 年間にわたる取り組みの中の一つとして提出されたもので、オンライン上での消費者のプライバシーを保護するための広範に渡り実効性のある諸策の設置を促すものである。

同報告書では、電子商取引の成長及びウェブサイトが消費者に関する情報を収集する方法について説明し、オンライン・プライバシーに関する消費者の懸念を探り、さらに、オンライン・プライ

バシーに関する業界の自主規制の現状を分析している。同報告書では、「当委員会は現段階では、オンライン・プライバシーを規制する法律の策定は適当ではないと判断する。

だだし、インターネット業界は今後大きな課題に取り組んでいかなくてはならない。現在直面する課題としては、特に、消費者のプライバシー保護の重要性をまだ認識していない企業を啓蒙していくこと、及び広範に渡り実効性のあるプライバシー保護規定の形成を促進させるためのインセンティブの策定である。」としている。

また、同報告書では、ウェブサイトにおける公正な情報管理制度の策定がどれだけ進んでいるかを確認するため、パブリック・ワークショップ、特別調査委員会の設置及びオンラインの調査などを含め、オンライン・プライバシー問題に関する計画のガイドラインを示した。

また、同報告書では、ジョージタウン大学の Mary Culnan 教授による 2 つの商業ウェブサイトの調査結果及びトラストe、 BBBオンライン、Online Privacy Alliance などの取り組みについて言及している。 Pitofsky 連邦取引委員会委員長は、「我々は、これまでどおり、インターネットにおける消費者のプライバシー保護は、実効性のある自主規制が最善策であると信じており、この点においてインターネット業界に実質的な進歩がみられたことを喜んでいる。」と述べている。

さらに、「このような進歩がみられたため、現段階で規制法案は必要ないと思われる。しかし、消費者を保護する制度の確立には単にウェブサイトに自社のプライバシー保護に関するポリシーを掲載するだけではなく、その他の措置も必要だ。

オンライン・ビジネス業界のプライバシー保護担当部門は、短期間で多くのことを成し遂げたが、インターネットによる取引で消費者がプライバシーを保護されていると信頼感を持つまでには、さらに多くのことを達成していかなければならない。」と述べている。

同報告書は、オンライン・プライバシーに関する自主規制の現状を分析して、「インターネット及びコンピューター・テクノロジーは急速に進化していることから、公正な情報管理制度を普及する方法としては「自主規制」が最も侵入的でなく、最も効果的である。」と強調している。

しかしながら、議会及び連邦政府は、実質的で迅速な今後の改善が見られない場合には、法規制導入の可能性も考慮すべきであろう。

また報告書では、プライバシー保護認証マーク制度及び消費者のオンライン取引に対して公正な情報管理制度を確立した責任感のある業界のリーダー数人を賞賛している。

4.5.3.1 ●考察

この連邦取引委員会の「自主規制及びオンライン・プライバシー」に関する報告書であるが、結

論としては電子商取引のプライバシー保護について当面自主規制で対応すべきであるとの結論であるが、一部に米国内部でもやはり根強く法規制論議があることが解り興味深い。

そして国内でも同様にＥＣ上の個人情報保護については、法規制論議に対して産業界を中心に抵抗感のある中、何らかの漏洩事件やプライバシー侵害事件の有るたびにマスコミ等の法制化待望論はここに来て、益々高まってきている印象を受ける。

ここではっきりせねばならないのは、“自主規制があれば法制は必要なし”ということでは決してないということである。

過度の法規制を防ぐ為の民間ベースの自主規制と言う位置付けでは本来なく、電子商取引の発展が妨げられる阻害要因の除去のために何が必要かと言うのが論点ではないかと思われる。

その為には「法規制」と「自主規制」は共に車の両輪であり、どちらが欠けても円滑な電子商取引の発展は望めないわけである。つまり「法規制」と「自主規制」両者が相互補完関係にある姿がやはり正しいのではないだろうか。

その点から言えば、まず国内でも最低でも個人情報に財産的価値ないしは所有権利的なものをを認めるような、第一段階としての包括的な法規制があってしかるべきではないだろうか。

とくに他人の情報を窃取した場合に、フロッピーの盗難事件としてしか扱えないと言うような異常事態からはいち早く脱却すべきであろうし、少なくとも先進国としての立場として、子供に関する情報保護も含めて、この個人情報保護の環境整備・インフラ確立は早くなされなければならない。

4.6　スペインでのデータ保護マーク制度について

さて次に今まで文献でも書物でも、ほとんど紹介されなかったスペインのデータ保護マーク制度について紹介していく。これは民間団体による自主規制というよりは、スペイン電子商取引協会（ＡＥＣＥ）による現行法規の不足を補う為の消費者保護･救済プログラムと言った位置付けのものであるところが興味深い。

4.6.1　「データーの保証と保護（インターネットにおける個人データ保護に関する倫理規定）の抜粋」：ＡＥＣＥ（スペイン電子商取引協会）

インターネットという新しいコミュニケーション手段の出現以来、現行法に規定の不備が生じ、消費者の保護が脅かされる事態が生じている。

その結果、スペイン電子商取引協会（ＡＥＣＥ）は、インターネットを使用して業務を行う企業が、任意に責任ある規定を作成して現状を規制する必要性を認めている。これはインターネット内の個

人データー自動処理における、個人のプライバシー保護をめざすものである。

この倫理規定に加盟できるのはインターネット上で製品やサービスを取引し、個人データを処理するすべての企業である。

同規定に参加するメリットは以下のようなものとなる：

- この非常に便利で手頃な新規マーケットに参加する潜在的消費者の信頼の増加
- 保証マーク使用の可能性により、参加企業が個人のプライバシー保護に配慮する真面目な企業であるという立場を明確にできる

規定内には主として年少者用のオンライン業務に適用可能な追加的な原則を含む章があるが、これは大人とは異なり、彼らには要求される情報の性格や情報がどのような目的で使用されるかが理解できない可能性があるからである。また彼らの成熟度には差異がある為、年少者向けのオンライン又はインターネットのウェブ内で業務する事業者は、両親に働きかけて子供たちのオンライン上の経験に参加し監督するよう呼びかけることを約束する。

本倫理規定における義務は、インターネット上で業務を行い、任意に規定に参加する企業に対し、以下の関係で生じる。

- 個人データについての企業と消費者との関係
- 個人データについての企業間の関係

本倫理規定に任意で参加するすべての企業は「データ保護保証マーク」を使用する事ができる。

ＡＥＣＥのデータ保護の原則はあらゆる種類のメディアに適用可能ではあるが、以下の原則と例とはオンラインマーケティングとインターネットという特定のテーマを中心としている。

主としてインターネット上の事業者の義務はウェブに参加するユーザーの権利に関するもので、その目的は個人データの保護である。同様に、ウェブに参加する人々のプライバシーを損なわないように事業者の義務を定めて市民の権利を保証している。

4.6.1.1　第 1 章　一般原則

(1) 第 1 条：定義
(2) 第 2 条：コネクションにおける安全性
(3) 第 3 条：ネットワークにおける安全性

4.6.1.2　第 2 章　消費者の権利

(1) 第 4 条：情報提供の義務

① 企業の明白な識別

(2) 第 5 条：異議申立の権利

(3) 第 6 条：目的。

(4) 第 7 条：譲渡と譲渡の目的

4.6.1.3 第 3 章 Eメールによるマーケティング

(1) 第 8 条：広告の発信

(2) 第９条：消費者への情報。

(3) 第 10 条：スパン（Spam.）技術の使用

(4) 第 11 条：データリストの利用

(5) 第 12 条：公開された情報源から作成されたリストの使用。

4.6.1.4 第 4 章 年少者達に関するデータの処理

(1) 第 13 条：年少者達との通信目的

年少者達とオンラインで通信する、或いはデーターを得る為に、広告会社は対象となる人々の年齢や知識、成熟度を考慮しなければならない。

いかなる場合も、年少者達から家族の他のメンバーのプライバシーや経済状態にかかわるデータを入手してはならない。

(2) 第 14 条：年少者達の関連原則の適用範囲

本倫理規定内で年少者達のデータの入手や処理にかかわる措置とは、主として 12 歳以下の子供たちを対象とした製品やサービス、情報を提供するウェブのページにアクセスしたり検索したりする事で入手されるデータに関するものと理解される。

(3) 第 15 条：年少者のデータの処理に関する両親の介入

事業者は、名前や住所、その他のいかなる情報に関するものであれ、年少者である子供たちに関する情報の収集に関する両親の懸念に応じる必要がある。

事業者は、両親が子供たちのデータに関して、その使い道にアクセスしたり、解消したり、決定したりする権利行使の可能性に便宜を計らねばならない。使い道の取消しや決定はオンラインにより通知され、事業者はそれを保存し、常に尊重しなければならない。

年少者が事業者のページにアクセスし、両親の通知に反して情報や広告の送付を依頼す

る場合、事業者はその要請に応えてはならない。

前記通知の撤回は、作り手を証明する事ができる電子通信以外の方法による両親の新たな通知によってのみ行われる。

事業者は年少者達にデータを提供する前に、両親に相談するよう勧めなくてはならない。また、事業者は、親たちに対し、どうすれば子供たちのプライバシーが保護できるかという情報の提供を行う他の機関によるあらゆる努力を支援しなければならない。このような情報の中には子供たちが名前や住所、その他の個人データを提供することを親達が阻止する、アクセス管理ソフトのような手段についての情報も含まれる。

(4) 第 16 条：年少者のデータ使用

このように、親による、オンラインデータ収集制限を含むオプションに加え、広告企業は年少者を対象にした製品やサービスの売り込み、販売、納入という目的に限って彼らが提供したデータを使用すべきである。

いかなる場合も、年少者に関するデータを譲渡したり、彼らの年齢に不適切なセールスキャンペーンに使用してはならない。

(5) 第 17 条：年少者に関するデーター使用の情報

事業者は年少者に関する情報を自社の製品及びサービスのセールスプロモーションという商業上の目的に限定して必要とするという事を明確にする。

(6) 第 18 条：安全措置

事業者はオンラインで入手した年少者のデーターへのアクセス、改変、譲渡に対抗する厳格な安全措置を講じなくてはならない。

4.6.1.5　第 5 章　保証マークの使用方法

(1) 第１９条：目的

協会が設定した保証マークの目的は、その中に含まれる倫理規定の遵守を受け入れる企業の認証である。

(2) 第 20 条：マーク取得

倫理規定加盟企業のみが保証マークの使用を認められ、文書により、ＡＥＣＥに、いかなる状況においても規定を適用する事を約束しなければならない。マークの使用は任意であるが、各参加企業は他のメンバーの実施する広告を利用する為、本マークの普及推進という全員の利益に影響を与える。

(3) 第 21 条：使用方法

基本的目的を考慮すれば、同マークは加盟者全体を識別するものであり、マークを以下のように解釈されるような方法で販売書類や広告に使用してはならない。

1. 使用企業独自のマークであるような使用方法
2. 販売に供する製品やサービス自体の（特に原産地、又は品質の）保証を示すかのような使用法

ＡＥＣＥはいかなる時もマークの使用条件を管理評価して、通常とは異なる使用が行われた場合、あらゆる有効な措置を取る権利を留保する。そのため、マーク使用加盟者は、協会から使用の指示の通知があったら、遅滞なく、且つ留保条件なしで適用する事を約束する。

協会の文書による明確な承認のない限り、倫理規定加盟広告業者のウェブ上のページ以外でマークの複製を使用する事は禁じられる。

4.6.1.6 第 6 章

(1) 第 22 条：規定遵守の管理

(2) 第 23 条：クレーム提出

(3) 第 24 条：制裁処置

(4) 第 25 条：通知、公告、法的行為

4.6.1.7 最終規定

(1) 第 28 条：本倫理規定の見直しと現状に則しての改訂

4.6.1.8 考察

以上の様に、もともとテクノロジーの進歩に伴う、現行法規定の不備発生が消費者保護に影響を与えているとのスタンスから出発した保護プログラムだけに、米国の民間の第三者機関によるものより、かなり消費者よりの内容となっている。

そのため、わざわざ第 2 章に当たる項目に、「消費者の権利」という項目を設けて、今までのプログラムのバックボーンである「ＯＥＣＤの 8 原則」とは違った観点からの保護規定を設けている。

とくにそのなかでも「異議申立の権利」の項で、企業側がいつでも消費者に対して異議申立の権利行使を保証せねばならない事が明記されている。

つまりはじめから消費者からのクレーム・苦情処理制度を念頭において、このプログラムが組ま

れれている事がわかる。このことは即ちマーク制度の実行担保の要件として、シール発効機関と苦情処理機関の同一性がポイントであることを充分に理解している事にほかならない。

またもう一つの特徴は、「年少者に関するデータの処理」の章を設けて、そのプログラムの立ち上げからチルドレンプロテクションの重要性を認識した上で合計 6 項目に亘る保護規定を設けている事は特筆に価する。

さらに各企業のプライバシーポリシーについても、「ＯＥＣＤのプライバシーポリシージェネレーター」と同じく、協会独自のマーケティングプライバシーの原則と呼応したものにすべく、ソフトウェアの提供システムを確立しているところも特色の一つである。

4.7　韓国の制度について

次に韓国の制度の紹介であるが、今まで見てきたような日本や欧米でのシールプログラムと違って、ウェブ上で消費者に分り易く信用できるサイト･モールを自主的に表示する類のものではない。これは行政側も参加して、様々な条件をクリアした優良モールに「大韓民国サイバーモール大賞」を授与するというインセンティブでもってネット環境の整備を推進しようとする褒賞プログラムである。

4.7.1　授賞制度計画：優秀サイバーモール授賞制度

(1) 主管　　：産業資源部

(2) 共同主催：韓国経済新聞社、電子新聞社、韓国電子取引振興院

- 第 2 回　優秀サイバーモール授賞大会を開催。
  - 審査期間：10 月 25 日より 11 月 13 日まで（10 月 23 日(土)に申請締切り）
  - 結果発表：11 月末(予定)

4.7.2　事業目的

- わが国（韓国）の後れた電子商取引環境を促進させることをもって、経済再跳躍のための足がかりとして先進隊列に進入しようというものである
- 商取引の新しいパラダイムである電子商取引環境下で消費者を保護し、取引の安定性を確保して電子商取引を通じた取引基盤を確立する
- 消費者に安心して取引することができる環境を提供するために、技術的な方法である認証制度とともに、政策的な方法として本制度を活用する

- サイバーモールの分野別に優秀サイバーモールを選定することをもって、中小企業が専門商品サイバーモールもしくは製造直販サイバーモールのようなサイバーモールを通じて発展することができる機会を提供する
- インターネットサイバーモールに対する消費者の信頼性向上が可能である
  - 明確な基準に基づく推薦により消費者が安心して物品を購入することができる取引環境をつくり上げる
  - 消費者の取引促進による電子商取引の活性化を図る
  - 消費者に優秀サイバーモールを通じて品質が良く、低廉な商品購買およびアフターサービスが可能であることを広報する
- 公信力がある機関により透明で客観的な審査手順と持続的な評価制度を維持してインターネットサイバーモールが消費者に対するサービス改善努力を効果的に遂行できるように誘導する
  - 潜在的な顧客の電子商取引参加のためにサービス改善努力
  - 優秀サイバーモール選定基準の広報を通じてサイバーモールの対顧客サービス向上の正しい方向を提示
- 電子取引活性化のために今後電子取引の振興業務を担当することになる電子取引振興院、韓国経済新聞社、電子新聞社が共同で、産資部との協力下に本制度を施行する

4.7.3 事業概要

- '99 年から開始して、安全で信頼性ある電子商取引が私たちの生活に完全に定着するときまで毎年施行する
  - 透明な審査基準と持続的な評価過程を通じて優秀なインターネットサイバーモールを選定し、選定されたインターネットサイバーモールに対する大々的な広報を通じて気楽なインターネットショッピング環境を支援する
- インターネットサイバーモール授賞は、次のように施行する
  - '大韓民国サイバーモール大賞'は、消費者保護およびサービス水準が優秀な企業体の中から販売実績、経営革新成果等が優秀で、他のサイバーモールに経営戦略をたてるのに鑑となりうる企業体を選定して施行する
  - '推薦優秀サイバーモール'指定は、消費者保護およびサービス水準を基準として一定点数以上を受けた企業体に限り個数に関係なく'推薦サイバーモール'に指定する
- サイバーモールを分野別に分けて'大韓民国サイバーモール大賞'を審査選定することをも

って、インターネットサイバーモールの順調な活性化を促進する

- 総合サイバーモールは、韓国標準産業分類で中分類項目 3 個以上の商品・用役を販売するサイバーモールであって、直接製造した商品・用役を含めて他の機関が委託した商品・用役を販売するサイバーモールも該当し、取扱い商品の多様性とインターネットショッピングの便利性を重視する
- 専門サイバーモールは、韓国標準産業分類で中分類項目 2 個以下の商品・用役を専門に販売するサイバーモールであって、直接製造をしないか、もしくは直接製造しても他の製造社の商品・用役を一緒に販売するサイバーモールも該当し、専門商品に合う顧客サービスの質を重視する
- 直販サイバーモールは、品目数と種類に関係なく 1 個以上の製造企業体が生産する商品・用役を直接販売するサイバーモールであって、サイバーモールが製造企業体とまったく関係がない別個の会社でも、1 個の製造企業体の商品・用役を販売するサイバーモールも該当し、流通マージンの節減を反映した価格を重視する

- 民間自律の原則に基づき業界と学界の電子商取引専門人材を総網羅した専門審査委員会を積極的に活用する
  - 電子商取引関連の民間専門家を通じた優秀サイバーモール選定審査作業の遂行
  - 選定委員会傘下に選定基準制定作業班を運営する

4.7.4 事業内容

(1) 優秀サイバーモール選定委員会構成

- 電子商取引関連権威者(委員長)と専門家(審査委員)の 20 名内外で構成
- 優秀サイバーモール選定要領制定・改正・審査・広報

(2) 優秀サイバーモール選定基準設定

- 優秀サイバーモール選定基準制定作業班構成
- 選定基準審査会議を通じて選定基準項目に対する評価調整・基準値設定

(3) 優秀サイバーモール選定制度公表

- インターネットサイバーモール運営者と一般消費者に優秀サイバーモール選定制度について審査期間および審査基準を公表・選定申請受付

(4) 優秀サイバーモール選定審査会の開催

- 産業資源部と韓国経済新聞社、電子新聞社の後援
- 審査基準各項目別に審査期間内にインターネットサイバーモールを評価した結果を

集計して決定

- 評価結果による優秀推薦サイバーモール選定、推薦優秀サイバーモールロゴ付与および大韓民国サイバーモール大賞授賞

4.7.5 授賞の種類

(1) 大韓民国サイバーモール大賞

- 区分　　総合サイバーモール・専門サイバーモール・直販サイバーモール
- 大賞　　1 企業体のみ

(産資部長官賞)

- 優秀賞　　（各区分 1 企業体づつ）計 3 企業体

(産資部長官賞)

- 合計　　総 4 企業体

(2) 推薦優秀サイバーモール指定

- 区分　　総合サイバーモール・専門サイバーモール・直販サイバーモール
- 3 主催機関名の推薦
- 優秀サイバーモール　　各区分とも個数制限なし
- ロゴ使用証贈呈

4.7.6 優秀サイバーモール授賞制度審査基準

4.7.6.1 審査対象

(1) インターネットサイバーモールの定義

- インターネットを通じて商品・用役を注文および支払決済を処理するサイト

4.7.6.2 審査評価方法

(1) 優秀サイバーモール申請企業体提出書類

(2) 韓国電子取引振興院審査支援チーム調査

- サイバーモール訪問(インターネット接続)調査

(3) サイバーモール利用者の主観的な見解調査(1999 年未実施)

- 使用者グループ設問調査実施

(4) 優秀サイバーモール選定委員会

- 審査結果総合評価
- サイバーモール大賞受賞企業体および推薦優秀サイバーモール最終決定

4.7.6.3　審査項目

(1) システム性能および安全性
(2) 商品情報獲得の便利性
(3) 商品情報の適切性
(4) 注文方法の適切性
(5) 支払決済手段の便利性と安全性
(6) 顧客情報保護
(7) 商品配達サービスの多様性
(8) サイバーモール運営成果と信用度

以　上

4.7.6.4　考察

以上の様に、消費者保護のためのネット環境の整備という最終目標は同じであるが、この韓国の制度は、欧米の自主規制シールプログラムと違って、インターネットサイバーモール（ショップ含む）に対する消費者の信頼性向上のために、行政側も参加した明確な基準に基づく推薦により消費者が安心して物品を購入することができる取引環境をつくり上げようとするものである。

この行政の参加（官主導）というポイントは、日本国内や欧米にある民間機関のネットショップ表彰制度と大きく違う所である。

そのために、消費者の取引促進による電子商取引の活性化を図る目的で、消費者に優秀サイバーモールを通じて品質が良く、低廉な商品購買およびアフターサービスが可能であることを広報すると共に優秀サイバーモール選定基準の広報を通じて、サイバーモールの対顧客サービス向上の正しい方向を提示することが政府お墨付きと言う点で可能である。

これは行政がバックについた公信力がある機関により、透明で客観的な審査手順と持続的な評価制度を維持して、インターネットサイバーモールが消費者に対するサービス改善努力を効果的に遂行できるように誘導して、潜在的な顧客の電子商取引参加のためにサービス改善努力をさせるものである。

また個人情報の保護という観点からは、「顧客情報保護」というモール･ショップの評価及び審査項目の中に、「個人情報収集および取扱いに対する利用者の事前同意獲得」や 「利用者の同意

のない第3者提供禁止」 「管理責任者指定」「本人情報閲覧・訂正権の保障」の条項を設けており、その審査基準･方法として、利用約款及び利用約款ページの URL および画面出力物を利用してこのような点を明示する事を上げている。

4.8 民間企業（国内）によるオンラインプライバシー保護関連マーク

次に日本国内でオンラインプライバシー保護関連のマーク制度を立ち上げている企業を見ていくものとする。これらの企業は今まで見てきた中の、米国の非営利第三者機関（BBB やTRUSTe）と違って民間企業であって、ＣＰＡウェブトラストマーク同様に、営利目的にシールプログラムを立ち上げているわけである。

4.8.1 プライバシー保護プラスセキュリティ対策をアピールすることが目的の“サイト・シール”

日本ベリサインでは、ベリサイン・セキュア・サーバーID を取得いただいたユーザーに、オーセンティック・サイト・シールを無償で提供している。

オーセンティック・サイト・シールを、ユーザーが運営するウェブサイトに表示することで、ウェブサイト訪問者に対して、プライバシー保護、セキュリティ対策が施されたウェブサイトとしてのビジュアルイメージを高めるとともに、第三者認証機関であるベリサインの認証を受けたウェブサイトであることをアピールできる。

つまり、オンラインショップの信用を高める効果があるのは、クレジットカード・ブランドの画像よりもベリサインの「シール」である、という表現も見うけられる様に、一般論として 、ECが消費者の信頼を獲得する主要な方法の一つに「シールの掲載」があげられる。 セキュリティ・ブランドとして知られるベリサインや VISA のシールは、訪問者にサイトの安全性を証明するために効果的である。

4.8.1.1 ベリサインオーセンティック サイトについて

ベリサイン・デジタルＩＤ・オーセンティック・サイトとは、ベリサインの定める認証手続きに基づき、サイトを運営する企業・組織が確かにそのサイト名称を利用し、インターネット上で唯一無二であることをベリサインにより証明されたサイトである。以下のチェック項目に基づき、ベリサイン・デジタルＩＤによって該当ページが認証されていることをご確認できる。

そのウエブ・サイトがベリサインのデジタルＩＤを利用していることをご利用のブラウザから確認することができる。サーバがベリサインのデジタルＩＤを利用している場合は、認証証明書は Secure

Server Certificates Authority によって発行されたことを示すダイアログ・ボックスが表示される。

ウエブ・サイトを認証するだけにとどまらず、セキュア・モードで接続する場合、ウエブ・サイトとブラウザの間で交換される情報を暗号化することが可能である。

4.8.2 個人情報の保護をセキュリティ面で保証し、しかも内部に不正アクセスを抑制する効果を持つ“ウェブ上のパスポート”

次に最近立ち上がった民間企業の最新のマーク制度で、ホームページ運営法人の真正性の確認と暗号化通信による個人情報の保護を謳っている「セコム Web パスポート」を紹介する。

まずセールスポイント・特徴として下記の５つが挙げられている。

このなかでも、とくに個人情報の保護という観点からの注目ポイントは、「暗号化通信の採用で、ホームページ来訪者の個人情報を守る」と「機密情報の交換など、ネットビジネスでの応用」という２点である。

これは詳しく後述するが、まずプライバシー保護を技術的なセキュリティの面でバックアップしたマーク制度である点と「機密情報」といういう言わば内部情報の管理と言う点をもその要件に包含しているのがポイントである。

4.8.2.1 ５つの特徴

(1) ホームページ運営の信頼性

知らないところで、貴社のホームページとそっくりのページが作られ、ニセ情報を発信されたり、ユーザーの重要情報が盗聴・悪用されてしまう。インターネット先進国であるアメリカでは「なりすまし」による詐欺事件が実際に多発。便利さだけが注目されているインターネット社会の恐ろしさが現実のものとなっている。こうした危うさは、日本でも切実な問題。ネットビジネスを展開していく企業にとっては、一刻も早く解決しなければならない課題である。

(2) 運営者の身元を明らかにする「実在証明書」

［セコム Web パスポートサービス］は、セコムが、「その運営する企業・組織が確かにそのホームページを運営し、インターネット上で確実に存在していること」を審査・確認。公開されているホームページが間違いなく、その企業・組織が運営していることに対して実在証明書（Web サイト証明書）を発行する。

(3) 赤いステッカーで信頼性をアピール

証明書が発行されると、セコムの赤いステッカーをホームページに貼付できる。ステッカー

は、ホームページを訪れる人に、インターネットの危険性を未然に防ぐ配慮をしているホームページであることをアピール。ホームページ公開企業として、信頼性を大きく高める。

(4) ホームページ来訪者の個人情報保護

［セコム Web パスポートサービス］の見逃せない機能が、暗号化通信。ホームページに訪れるユーザーとの間での通信内容を暗号化し、第三者の盗聴から守ります。アクセスするユーザーのプライバシーを保護する運営を実現できる。

(5) 機密情報の交換など、ネットビジネスでの応用

［セコム Web パスポートサービス］は、電子商取引に非常に有効なセキュリティである。企業のホームページの信頼性を確立することにより、ネットビジネスのチャンスをより一層拡大。また、イントラネットやエクストラネットの構築・運営シーンでも、ホームページの安全対策として情報漏洩防止に活用できる。

4.8.2.2 Web サイト証明書について

ユーザはインターネットなどを通じて買物や電子商取引でビジネスをする際に、この［セコム Web パスポートサービス］でホームページ運営法人の真正性を確認でき、安心して利用できるうえ、その通信経路に暗号化による SSL 通信(セキュア・ソケット・レイヤー)を行えることで個人情報が保護されることになる。

また、不正アクセスのおよそ７割が社内の人間によって行われている LAN 環境でのイントラ・ホームページは、コンピュータ技術を有する社員にとって、容易に機密情報へのアクセスがしやすいことも事実。社内用の情報共有ホームページが各社で利用され始めている中で、このサービスの活用でイントラネット内の盗聴しやすい環境上の防止抑制の一助となり、企業の情報資産のセキュリティ保護には不可欠の基礎的サービスとして位置付けられている。

4.8.2.3 考察

これらのマーク制度の特徴としては、第三者認証機関での認証を受けたウェブサイトであることをアピール出来る事、それに一部前述した様に技術的なセキュリティの裏づけがある点である。

単にプライバシーポリシーを宣言するというようなレベルでなく、SSL による暗号通信等をベースにしての情報保護がなされているのが必須要件となっている事である。

つまり必ず出店者と消費者間のデータ通信の安全が確保されて、第三者の盗聴からプロテクトされている訳である。

それともう一つ説明文中にもあるように、今日発生するの不正アクセス・情報漏洩の７０％にあたる社内からの盗聴・窃取に対しての効果である。これらマーク・サービスはこのイントラネット上の機密情報への内部からの不正なアプローチの抑制・防止効果があるという点があげられる。

これは消費者にとって朗報である。なぜならその最大のＥＣ参入阻害要因である個人情報漏洩という問題解決に技術的な裏づけ付与を宣言した企業を、容易にネット上で見つけられることになり、その効果は大きいと思われる。

5 全体のまとめ

ＥＣ上の個人情報保護について、全体のまとめをする前に、データ保護に関係する報告書について見て行くものとする。

5.1 「我が国の個人情報保護システムの在り方（中間報告）」

まず、1999 年 11 月に内閣の「高度情報通信社会推進本部　個人情報保護検討部会」からだされた「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（中間報告）」という、データ保護の在り方についての報告について見てみる。この中間報告は今まで述べてきた個人情報に関する様々な論点を、現時点で一番良くとりまとめたものであり、多方面に亘り論点を広げており、個人情報保護に関する全般について理解するのに適した内容となっている。

中身としては地方自治体を含む官公庁が所有する住民基本台帳などの個人情報と民間事業者が保有する個人情報の両分野を対象にした包括的な基本法を制定する必要性を明記すると共に分野別の個別法と関連業界の自主規制を組合せた法制化を提言している。

また基本法に違反した行為に対して罰則を盛り込むことについては、「自由な事業活動の阻害要因となるなど、他に保護されるべき権利･利益が損なわれる恐れがある」として見送る考えを示した。

そして基本法の下で個別保護の必要性が一段と高いものとして、「信用情報」「医療情報」、NTT 社員らによる度重なる顧客情報漏洩の問題などが表面化している「電気通信」の 3 分野を挙げ、罰則を含めた個別法での対応を求めた内容となっている。

5.2 「電気通信分野の個人情報保護法制に関する」中間報告について

次にその問題点が表面化している電気通信分野での個人情報保護に関する報告を見てみる。この「電気通信分野における個人情報保護法制の在り方に関する研究会」中間報告について、結論としては、前述の「高度情報通信社会推進本部個人情報保護検討部会の中間報告」を受けて、基本法との関係に配意しつつ、電気通信分野における個人情報保護のための実効性ある法制を確立する必要があるというものである。

特に電気通信事業者の従業員等による不正な顧客情報の漏えい等を防止するため、これらの行為に対する罰則等の在り方を検討する必要があるとした点は注目に値する。

また、罰則により保護すべき個人情報の範囲についても、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」を漏えいする行為等が罰則の対象とされている。

ただ電気通信分野においても、更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を考慮する必要があるとの見解を示している。

このため従来の「通信の秘密」の保護を義務付ける規定とその違反に対する罰則規定に加え、業務上知り得た「個人の秘密」の保護を義務付ける規定とその違反に対する罰則規定、個人情報一般の保護を義務付ける規定（訓示規定）をそれぞれ新たに設けるという、三層構造のイメージを提言している。

また罰則により規制の対象となる者の範囲については特に第三者に対する規制について電気通信事業者の従業員等とともに、あるいはこれを唆すなどして不正に個人情報を入手する第三者の行為については、当該従業員等に犯罪が成立する限りにおいて、共犯規定の適用可能であるとしているが、問題はそれ以外の態様による第三者の不正入手行為について、独立の処罰規定を設けることは、いわゆる情報窃盗が処罰の対象とされていない現行法の体系の下にあっては、困難な点である。

5.3　全体のまとめ（総括と提言）

以上見てきた様に、民間部門における個人情報保護の法制化のポイントとして、包括基本法の役割も重要ながら、現状のガイドライン遵守レベルと明らかに違う、一歩踏み込んだ形の法環境整備が是非とも必要と思われる。特に昨今の個人情報の流出事件が、まず一番センシティブな情報の代表である医療分野をはじめ多方面に亘っている事実、また電気通信分野においては、その頻度・回数が異常な進展を見せている状況等を見るに付け、やはり早急に情報窃盗が処罰の対象となる法規制の検討が必要な時期に来ているのではないだろうか？

次にもう一つの大きな課題である、自主規制についてであるが、現状については詳細前述の様に、この分野においては、各省庁それにこれをベースにした各業界毎の「個人情報保護に関するガイドライン」の周知・徹底と、これに基づく各事業者及びその業界団体による自主的な取組の推進が個人情報保護の根幹を担っているにすぎない。

また、確かに情報保護環境整備の一環として、シールプログラム（マーク制度）についても、1998 年からは、財団法人日本データ通信協会による、適切な個人情報保護策を講じている電気通信事業者等を登録し、「個人情報保護マーク」を付与する業務の実施があり、この分野以外にも同じく 1998 年からの、財団法人日本情報処理開発協会による JIS（日本工業規格）Q15001 を踏まえた「プライバシーマーク制度」の運用等が、すでにスタートして実効を挙げつつある。

ただ一番の課題はこういった現状のマーク制度が、ネットショッピングの消費者が一般に見るオ

ンラインショップのウェブサイト上には、未だあまり見かけない点ではないだろうか？

つまり現行のマーク制度は、情報処理や電気通信分野で、大量に個人情報を取扱う大手業者の自覚とその社内における管理体制の厳格さをアピールする事には貢献しているのは事実である。ただし、ＥＣつまりオンラインショッピングに参画する一般のネットショッパーたちが、プライバシーや個人情報の漏洩を気にせず、ウェブ上で安心してショッピングを楽しめる環境整備と言う点でどれだけその役割を果たしているかについては、まだまだと言った感が否めない。

もうひとつは、子供の情報保護に対する施策が、現時点では先進的団体及び企業が、ガイドライン上に、その規定を載せたり、またウェブ上でそのプライバシーポリシーにそれが組込まれているサイトが見受けられる程度しか普及していない事実である。

また行政側の取組みとしてもインターネット上の子供保護に対する取組みとしては、昨年１１月の「児童ポルノ・児童買春処罰法」の施行等しか行なわれていないのが現状である。

やはりオンラインショップにはそのウェブサイト上に、一目見ただけで判る「オンラインプライバシーの保護マーク」等が、また子供向けサイトには、親も安心してそのサイトをオープンさせられるように、そこの情報保護方針を端的に示した「チルドレンプロテクションマーク」等が必要ではないだろうか？

また今後の課題として、昨今のＥＣの発展や分野の広がりに呼応したＥＣ個人情報保護ガイドラインの改訂、オンラインプライバシーポリシーの作成ソフトの普及やマシンアンダスタンダブルを前提とした技術的な取組みによる個人情報保護システム等が課題として挙げられる。

いずれにせよ、今日でもなお、消費者ＥＣ普及の最大の阻害要因となっている「個人情報漏洩の不安」を除去する取組みが、“法規制からのアプローチ”それにマーク制度を代表にした“自主的な取組み”それに消費者・企業への熱心な“情報リテラシー”を加えた総合的な施策が今まさに必要な事は言うまでもない。そしてこう言った地道で継続的な取組みが、これからの日本における“消費者ＥＣ”発展の鍵となっているものと確信する。

6 参考資料

6.1 各企業のホームページの中にあるプライバシーポリシー

6.1.1 ①京都「アメリカ衣料の岸本屋」プライバシーステートメント本文：お客様個人情報の保護、保全について

- どんなことがあっても絶対に外部にお客様個人情報をもらしません。
- **お客様に連絡する必要がある受注に対しての納期連絡など以外のメールを当社からだしたりすることは当社の方針としてありません。**
- あて先、お電話番号、メールアドレスなどお客様個人情報を発送業務以外に用いること、また外部にもらすような愚行は将来にわたって絶対にしません。社として、またひとりの人間としてお客様のたいせつな個人情報を保持、ゼッタイに漏らさないことを太陽に誓ってすべてのお客様に約束いたします。

（有）イージー代表　岸本栄司

- はじめて internet オンラインショップでお買い物された時なにが心配だったでしょうか？ぼくは「個人情報の漏洩の可能性」です 。

ぼくは販売側当事者そのものであり当然販売側であることがほとんどすべてですが、自分で internet online で shopping をしようと思い消費者の立場で考えた時みなさまとたぶん同じだと思いますが「セキュリテイ＝個人情報の保護」に一抹の不安を感じることもあります 。

- それは無責任かつ自分本位の発想しかできない

ほんの一部の業者（なんていえないような）自分の立場からの発想しかできないと思える、見ず知らずもちろん存ぜずの業者からの一方的に自分が儲けたい指向のみの思考しかないサービスなどを売り込みたいだけの迷惑 DM としか表現しようのないメールがほんまにたくさんきます、「じゃま」「迷惑」してるんです。 **この「望んでいない DM メール」の悲しいけれどの存在がこの不安を助長してるんだと思います。**

- 望む方に望むメールをさしあげる

メールマガジン以外の、「望んでいない方にまでたくさんだしたらそれでいいんだ」 の発想しかできない輩が存在するのも事実です。「たくさんだしたら少しはあたるだろう」の思考しかできない会社、人が たくさん売れるようになれるわけがないことが理解できていないんですね、ほんとうはそういう考えだから売れないことにまったく気がつけないんですね。

- 商売はどんなことにもひとりひとり

お客様に対してひとつづつしっかり対応できるところだけこそがたくさん売れるようになって

いくんです、こんなことは商売での常識です。

この常識がわからないのに「商売」なんて思っている輩にはほんまにムカムカするより悲しくなります。「このアホたれ。」って本気で思っています。

- **わけのわかっていない輩**

  けど既存事実として internet には「商売」という、**自分の商品をお客様に買ってもらうことに対してわけのわかっていない輩も存在しえるのもこれからも残念ながらなかなか変わらないと思います。**

- セキュアサーバーだって

  コンピューターをさわるのは人間です、いくらセキュリテイが高くてもそれをさわるのは人間です。**どんなことにでも「100%の安全」なんてありえません** 。

ぼくはお客様の個人情報秘匿義務を必ず守ることを太陽に誓ってここに宣言します。

- **商売はまずは信頼されなければ売れるものではありません**
- **ぼくはお客様の個人情報を他にもらすような愚考は絶対に死んでもしません**

21 世紀に向かって自分の意志を明確にします。

- **ご注文に対するその明細などのご返信、 問い合わせのご返事等（これは必ず送信します）以外のお客様にとって不必要であろう「よけいなお世話」メールは当社からは送信したことはありませんしこれからもぜったいにしません**
- **また、どんなことがあっても絶対にお客様情報を当社外部にもらしません**

自分の会社として自分の人生をかけた事業としてひとりの商業人として個人情報の完全な保護保全をすべてのお客様とおてんとさんに誓います。

6.1.2　②NTT コミュニケーションズのプライバシーポリシー：本文

NTT コミュニケーションズ公式ホームページはお客様へのサービスとして運営されております。お客様が当ホームページをご利用される場合、一部のサイトではお客様の個人情報をお伺いする場合があります（オンラインショッピング、アンケート、お問い合わせ、メール送付登録等のお客様の任意かつ自主的にご利用いただくサービスの場合）。

お伺いす

る情報は、お客様のお名前、メールアドレス、電話番号、住所といった、NTT コミュニケーションズのサービスに関する情報をご提供する際などに必要となる、お客様の個人情報が主なものになります。また、お客様の必要に即したサービスに関する情報のご提供等の目的で、それ以外の情報

を質問させていただく場合がありますが、これは必要最低限の項目を除いて、お客様自身が選択可能なものになっており、お客様の任意でご提供いただけるものです。尚、ＮＴＴコミュニケーションズが、お客様の同意なしにお伺いする情報を改変することはありません。

お伺いした情報は、当ホームページのサービスの種類によっては、第三者に通知する場合があることをあらかじめご了承ください。（例えば、配送等のサービスを委託した会社にお客様の名前と宛先を知らせる場合がこれにあたります）

NTT コミュニケーションズは当ホームページを訪問されたお客様のプライバシーを守るために合理的な範囲で必要な措置をとります。当ホームページのサービスによっては、お客様から機密性の高い情報（例えばウェブマネーやクレジットカードの番号など）をいただく場合がございますが、その際には情報を暗号化するなどの方法によって情報の保護に努めます。

NTT コミュニケーションズは以上の方針を改定することがあります。その場合すべての改定はこのホームページで通知いたします。

- クッキー（Cookies）について

クッキー（Cookies）は、お客様が NTT コミュニケーションズ公式ホームページに再度訪問された際、より便利に当サイトを閲覧していただくためのものであり、お客様のプライバシーを侵害するものではなく、またお客様のコンピューターへ悪影響を及ぼすことはありません。

インターネット閲覧ソフト（ブラウザー）の設定により、クッキー（Cookies）の受け取りを拒否することも可能ですが、その場合でも当サイトの閲覧に支障を来すことはありません。

ブラウザーの設定方法は各ソフト製造元へお問い合わせ下さい。

- 保証、及び責任制限

NTT コミュニケーションズ公式ホームページの利用は、お客様の責任において行われるものとします。

当ホームページ及び当ホームページにリンクが設定されている他のウェブサイトから取得された各種情報の利用によって生じたあらゆる損害に関して、NTT コミュニケーションズは一切の責任を負いません。

- 準拠法

NTT コミュニケーションズ公式ホームページは NTT コミュニケーションズの管理下にあります。

当サイトは法律の異なる全世界の国々からアクセスすることが可能ですが、当サイトにアクセスされたお客様および NTT コミュニケーションズの両者は、かかる法律原理の違いに関わらず、当サイトの利用に関して日本国の法律および東京都の条例に拘束されることに同意するものとします。

また NTT コミュニケーションズは当サイト上で、お客様の環境において当サイトのコンテンツが適切であるかなどの記述や表示は一切行いません。

当サイトへのアクセスはお客様の自由意志によるものとし、当サイトの利用に関しての責任はお客様にあるものとします。

6.1.3 ③女性向のインターネットナビゲーションを標榜するウェブ Style のプライバシーポリシー：本文

ウェブ Style では、会員の皆様への事前の許諾なしに、当ホームページにおいてご入力いただいた個人情報（氏名、住所、電話番号、メールアドレス等）をダイレクトマーケティングや各種調査に利用したり、第三者に使用させたりすることは一切致ません。当ホームページにおいてご入力いただいた皆様の個人情報は、

- ウェブ Style からの印刷物その他の通信文のご郵送
- ウェブ Style からのメールによるお知らせの発信
- 賞品・景品等の発送

の場合等に、事前に皆様のご了承を得て使用させて頂きます。

また、皆様方、ひとりひとり特定されない統計情報（ブラウザーの種類、お住まいの都道府県名、年齢層等）につきましては、ウェブStyleのサービスをより良いものにしていくための検討資料として利用させて頂きます。しかしこれらも、第三者に使用させることはけっして致しません。

- 保護者の方へ
- 【ウェブ Style for Kids の設立経緯】

株式会社アールシーワイ・ビジョンでは、1998 年より、女性がもっとインターネットを便利に、そして安全に使えるようにと考え、インターネットを使った情報提供サービス&コミュニティサービス「ウェブ Style」をはじめました。

もともと、女性とインターネットに関連した業務に携わっていたスタッフが中心となってはじめたため、自分の個人情報の管理や安全な使い方をした上で、インターネットを電話や FAX と同じツールとして使っていくような運営方針に、スタート当初より多くの方から賛同をいただいております。そして、1999 年、KidsNet Club を引き受け、ウェブ Style のノウハウを生かし「ウェブ Style for Kids」の運営を決定いたしました。

これまでの子供向けサービスとは違い、大人が用意してあげるサービス・コンテンツではなく、子供たちがお互いに築き上げていける運営、そして家族全員で楽しめるようなサービスを用意してま

いります。

- 【ウェブ Style for Kids のポリシー】

ウェブ Style for Kids は子供達の自主性にまかせた運営を第一に考えていますが、下記のルールは必ず理解する、あるいはウェブ Style for Kids で学ぶことができるようにフォローします。

- インターネットやネットワークの正しい使い方や知識を持つ

これからますますインターネットやネットワークが社会に広がっていくでしょう。学校で教えられる教育だけでなく、ネットワーク社会のルールを幼少時にしっかりとマスターすることが必要です。

- お互いに助け合う

わからないことがあったら、ウェブ Style for Kids の仲間に聞く。また逆に自分が教えることもある。このように「ギブ&テイク」で、みんなが思いやりをもてるような、そんな雰囲気で運営します。

- 家庭、社会をつなぐ情報交換をする

お父様、お母様の知っている知識、あるいはお子様が得意な分野の話などを、ウェブ Style for Kids で情報交換できるようなスペースでありたいと願っています。

- 【お願い】

インターネットを快適に、そして安全に使うために、お子様と一緒にルールを決めてご利用いただくことをお勧めいたします。とくに、何が危険なことか、どんな使い方をしてはいけないか、というマナーをご家庭で、話し合い、お子様が理解した上で、楽しくお使いいただけるような下記のご指導をお願いいたします。

1.インターネットへの接続は、弊社東京アクセスポイントへ電話をかけることによって、ご利用いただきます。そのため、長時間つないだままですと、高額な電話料金となる場合があります。必ず、接続時間のルールを決めましょう。

2.ディスプレイモニターを長時間使用することにより、肩こり、倦怠感、目の疲れといった症状が起こる場合があります。お子様の背の高さにあった机と椅子、顔とディスプレイの距離に気を配ることが大切です。お子様の様子を観察し、少しでも疲れた様子なら休むことをお勧めします。

3.現在、インターネットを利用した様々なビジネスやコミュニケーションが行われています。その中にはお子様にとってふさわしくないものもあります。接続アカウントやメールアドレスの管理に気を付け、安全に利用できるようご指導お願いいたします。また、不審なメール、出来事がありましたら、スタッフまでお気軽にご相談ください。

お子様宛、保護者の皆様宛に定期的に運営事務局よりメールニュースを送信し、最新の情報提供を予定しております。皆様と一緒にウェブ Style for Kids を創っていきたいと考えます。どうぞよろしくお願いいたします。

6.1.4　④オフィス京（有）のサイトポリシー：本文

以下の方針は、オフィス京(有)(以下、当社と略)が主催するウェブサイト(LivLib およびショッピングサイトを含む)(以下､当社サイトと略)に適用されます。

(1) 個人情報収集の目的

当社サイトは、コンテンツの販売、コンテンツ作家の応募、コンテスト、公募投稿、懸賞プレゼントなどの登録に際してのみ、個人を特定する情報を収集いたします。

例外として、チャットや掲示板などの書き込みやアンケート、投票などをする際に、御本人の了解を得た上で、個人情報を収集することがあります。

当社では、こういった個人情報を販売管理、販売促進、マーケティング、募集要件を満たしているかの確認、編集やフィードバックなどを目的として利用することがあります。当社は、これらの情報を第三者に渡すことはありません（集計など事務処理上、機密保持契約をした上でアウトソーシング専門会社に外注する場合はあります）。

ただし、事前にお客様の了解を取った場合および法規的措置が必要な場合を除きます。

(2) 20 歳未満の利用者に対する方針

20 歳未満の利用者は、親権などを持つ保護者の許可なく、当社サイトを利用してはなりません。

また、コンテンツによっては、価値判断が未成年ではつきにくい、または成人向け内容であると特に判断される場合は、当社サイトではその旨を記載する場合があります。それらのコンテンツは、20 歳未満の利用者は利用してはいけません。保護者は、自己の保護する未成年に対して、責任を負いますので、適切な指導をお願いいたします。

(3) 20 歳以上の利用者に対する方針

20 歳以上のお客様の合意により、登録または応募時に提供された個人情報を、当社が作家登録、販売促進およびマーケティング等の目的のために使う場合があります。

いかなる理由であっても、お客様がこのような情報利用を望まない場合、電子メール、あるいは提示されているフォーマットにてその旨ご指示いただければ使用いたしません。

(4) クッキーの利用

当社サイトは、ご利用者の登録時のお客様の入力などを簡略化するために、クッキーを利用する場合があります。クッキーは、インターネットで標準的に利用されている技術です。

当社は、このクッキーで得た情報を第三者に渡すことはありません。

ただし、事前にお客様の了解を取った場合および法規的措置が必要な場合を除きます。

(5) まとめ

お客様は、当社サイトを利用することで、これらの当社方針を了解したものとみなされます。もし、了解いただけない場合は、当社サイトのご利用を停止くださるようにお願いします。

当社サイトでは、諸事情により、具体的な通知等なく、本方針を部分的に変更、修正、追加、削除する場合があります。

したがって、利用者の方は、このページの内容に変更がないかどうかを定期的にご確認ください。

方針の変更が掲示された後でも、当社サイトを継続利用される場合は、お客様が変更内容を了解したものとみなされます。

6.1.5 ⑤住商情報システム（株）の個人情報保護方針：本文

弊社は、「信用を重んじ、確実を旨とする」住友の事業精神に基づき、お客様との信頼関係を最も重要な経営指針としております。

最近、個人情報の保護に関して社会的な要請が高まる中、弊社は、1998 年 11 月、財団法人日本情報処理開発協会から『プライバシーマーク』を付与された認定事業者となりました。「プライバシーマーク制度」は、個人情報保護を自主的、積極的に促進させる制度として、個人情報を適切かつ的確な保護を行っている民間事業者に与えられるものです。

弊社は、「適切かつ的確な個人情報情報保護・管理による信頼と信用の獲得」を個人情報保護の基本方針として、個人情報保護に関するコンプライアンス・プログラムの完全履行に努め、これを実現いたします。弊社は、個人情報保護の重要性に鑑み、以下の取組みを実施いたします。

1.弊社は、個人情報を取り扱う責任者を置き、適切な管理を行います。

2.弊社は、情報処理業務の受託時、システム開発時等にお客様から個人情報を含むデータの預託を頂いた場合、使用目的に沿ってお客様から許諾頂いた範囲内でのみ利用します。

3.弊社が直接、個人情報を収集する場合においては、個人情報の収集目的を明確にし、当該業務の目的に沿った必要の範囲内とし、個人情報を提供いただいた方から同意を頂いた範囲内で個人情報を利用します。

4.弊社は、収集した個人情報の利用、提供には細心の注意を払い、適切に管理し、当該個人情報について当該個人の承諾を頂いた場合以外は、第三者に提供、及び開示を行ないません。

5.弊社は、提供を頂いた、並びに収集した個人情報を厳正な管理の下で安全に蓄積、保管し、当該個人情報への不正アクセス、紛失、破壊、改竄、及び漏洩等に対して適切な予防並びに是正処置を実施いたします。

6.弊社は、個人情報に関して適用される法令、規範を遵守いたします。

7.弊社の個人情報保護に関するコンプライアンス・プログラムは、顧客との信頼関係の中で、また、環境の変化に伴い継続的に改善いたします。

☆お客様情報に関するお問い合わせは、下記迄お寄せください。

住商情報システム株式会社　個人情報保護相談窓口：電話番号 03－5624－1600

メールでのお問い合わせは、こちらにどうぞ：ｃｐd@scs.co.jp

6.1.6　⑥富士通エフアイピー個人情報保護方針：本文

個人情報保護の重要性と情報サービス業としての社会性を認識し、当社では、コンプライアンス・プログラムを定め、役員・社員が一体となり個人情報の適切な保護に努めます。コンプライアンス・プログラムでは、個人情報の収集、利用および提供等に関する基本原則と管理方法ならびに必要な組織体制、さらには実効性を持たせる手段として、教育・訓練、監査等について以下のとおり規定しております。

(1) 適切な個人情報の収集、利用および提供等に関する基本原則

① 個人情報を直接収集する場合の原則

『適法かつ公正な手段により、本人の同意がある場合に収集します。』

『収集にあたっては、利用、提供の目的を明確にし、その目的を達成するために必要な範囲 内に止めます。』

『個人の利益を侵害する可能性が高い機微情報は、本人の明確な同意がある場合または法令 等の裏付けがある場合以外には収集しません。』

② 当社が情報処理などを受託する場合の原則

『個人情報に関する秘密の保持、再委託に関する事項、事故時の責任分担、契約終了時の個人情報の返却および消去等について定め、それに従います。』

③ 外部へ委託する場合の原則

『個人情報の処理を外部へ委託する場合には、当社の厳正な管理の下で行ないます。』

④ 個人情報を利用、提供する場合の原則

『個人情報は、本人の同意を得た範囲内で利用、提供します。』

(2) 個人情報の適正な管理方法

収集した個人情報は、正確かつ最新の状態に保ち、個人情報への不正アクセス、紛失・破壊・改ざんおよび漏洩等を防止するための措置を講じます。

(3) 法令、業界ガイドライン、社内規程等の遵守

個人情報を取り扱う業務の遂行にあたって、当社は、個人情報に関する法令、『個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q15001）』および業界ガイドラインなどを遵守するとともに、当社コンプライアンス・プログラムに定める事項に従い個人情報の取扱いについて十分な注意を払ってまいります。

(4) コンプライアンス・プログラムの継続的改善

当社は、個人情報を取り扱う単位毎に管理責任者を置き、コンプライアンス・プログラムを実践・遵守してまいります。また、定期的に行なう監査報告等を参考にしてコンプライアンス・プログラムの継続的改善に努めます。

(5) 本人からのお問い合わせ対応

当社では、本人からの個人情報の取扱いに関するお問い合わせには、社会通念に照らし妥当な範囲において、すみやかな対応に努めます。

お客様相談窓口（販売推進部） 電話;(03)5531-5210 E-mail;info@fip.co.jp

以　上

■参考資料・文献、ＵＲＬ一覧■

●「ＥＣで取扱われる個人情報に関する調査報告書（ver1.0）」（ＥＣＯＭ1999 年 3 月作成）

●「民間部門における電子商取引に係る個人情報の保護に関するガイドライン」（ECOM1998.3 月作成）

●調査対象ショッピングサイト＆モール一覧（ＥＣＯＭ／ホームページリンク分）

●「オンライン証券取引サービスについての動向等」（〈株〉大和総研＝DIR 資料）

●（株）インプレス：INTERNET　Watch 等インターネット関連記事

●ＺＤＮｅｔ/ＵＳＡ関連記事：オンラインオークションの世界は危険がいっぱい等

●「@ｎｉｆｔｙ保険」関連資料

●「ソニー損保のオンライン保険商品」関連資料

●「OECD のプライバシー8 原則」の各項目要件

●各企業のホームページの中にあるプライバシーポリシー

・京都「アメリカ衣料の岸本屋」の*個*人情報保護ポリシー（http://www.easy.ne.jp）

・NTT コミュニケーションズのプライバシーポリシー（http://www.ntt-c.co.jp

・女性向インターネットナビゲーションを標榜するウェブ Style のプライバシーポリシー（http://www.webstyle.ne.jp）

・オフィス京（有）のサイトポリシー(http://www.plaza.people.or.jp/livlib/company)

・住商情報システム（株）の個人情報保護方針(http://www.scs.co.jp)

・富士通エフアイピー個人情報保護方針(http://www.fip.co.jp)

●通産省（情報処理システム開発課）資料「ＯＥＣＤ プライバシー・ポリシー・ジェネレーターＶｅｒ.1」について

●電子商取引における消費者よりの苦情・相談具体事例（1）日弁連シンポジウム資料より

●同上：具体事例（2）と対策（財）日本消費者協会HPより

●読売新聞記事：N-BILL 事件等関連

●毎日新聞記事：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）

●朝日新聞記事：医療情報漏洩関連他

●日経新聞・日経産業新聞・日経金融新聞記事等

●電子ネットワーク協議会資料：個人情報保護環境（Ｐ３Ｐ技術的アプローチの例）

●BBB オンラインマーク制度関連資料（英文ホームページの翻訳）

●関連プレスリリースやニュース報道の反応（関連英文記事の翻訳）

●トラストｅプライバシーマークについて（英文ホームページの翻訳）

●米国公認会計士協会（AICPA）による「CPA ウェブトラストマーク」（英文資料翻訳）

●オンライン・プライバシー・アライアンス（Online Privacy Alliance）関連資料翻訳

●ＥＰＩＣ（エレクトロニック・プライバシー・インフォメーション・センター）関連資料翻訳

●米国連邦取引委員会「自主規制及びオンライン・プライバシー」に関する議会報告書（1999 年 7 月 13 日）」の翻訳記事

●スペイン「データの保証と保護（インターネットにおける個人データ保護に関する倫理規定）」和訳資料

●韓国の優秀サイバーモール（オンラインショップ）授賞制度関連和訳資料

●民間企業（国内）によるオンラインプライバシー保護関連マーク資料

●個人情報保護部会「我が国の個人情報保護システムの在り方（中間報告）」

●「電気通信分野の個人情報保護法制に関する」中間報告について

●その他ＥＣ及びプライバシー関連のネット記事･資料等

消費者ＷＧ消費者情報ＳＷＧ名簿（敬称略、企業名５０音順）

委員　富永　泰三　(株)アプラス 審査部　上席部長代理

委員　川村　尚哉　(株)エヌ･ティ･ティ･データ
新世代情報サービス事業本部コンシューマＥＣ担当課長

委員　阿部　昭一　沖電気工業(株)　エレクトロニックコマース事業推進本部部長

委員　野中　雅彦　近畿日本ツーリスト(株)　営業企画室計画課長

委員　河野　和寿　(財)金融情報システムセンター　調査企画部研究員

委員　前田　由美　(株)情報通信総合研究所　マーケティング・ＥＣ研究グループ
ＥＣビジネス開発室

委員　赤木　宏至　(株)セントラルファイナンス　東京企画部主任

委員　佐藤　史善　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　高野　雅晴　(株)ディジタル・ビジョン・ラボラトリーズ　企画本部企画部長

委員　高橋　ちひろ（株）東芝　情報・社会システム社ＣＥ･ＳＥコンサルティング推進部
システムコンセプト開発担当

委員　上野　正之　日本信販(株)　審査本部個人情報部チーフマネージャー

委員　野田　泉　日本ユニシス(株)　新事業企画開発部市場開発室課長

委員　小林 千寿　ぴあ(株)　ＥＣ推進室

委員　伊藤　文隆（株）日立製作所　システム開発本部主任技師

委員　鈴木　康史　富士通(株)　法務・知的財産権本部　法務部ビジネス支援部 担当課長

委員　小林　正弘　松下電器産業（株）企業システム本部ＥＣビジネス推進室室長

●ＥＣＯＭ　事務局

事務局　田中丸愼治　　電子商取引実証推進協議会 主席研究員

事務局　井関　勝博　　電子商取引実証推進協議会 主席研究員

事務局　大島　雅男　　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

平成１２年３月発行
発行：電子商取引実証推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5531-0061
E-mail　info@ecom.or.jp