

ECで取り扱われる 個人情報に関する調査報告書

平成15年3月



電子商取引推進協議会

目次

1	活動概要	1
1.1	クローズアップされる個人情報保護	1
1.2	E C O M個人情報保護WGの活動	1
1.2.1	E C O M個人情報保護ガイドラインの改定検討	1
1.2.2	国内外企業・団体の取組み実態および事例・ベストプラクティス調査	2
1.2.3	技術・先進的課題の検討整理	2
1.2.4	個人情報保護の正しい理解を促す普及啓発活動	3
1.3	年間活動を総括して	3
2	個人情報保護の動向	4
2.1	個人情報保護法の審議	4
2.1.1	当初の個人情報保護法案	4
2.1.2	2002年度の国会における審議	5
2.1.3	修正案の提出	6
2.2	相次ぐ個人情報漏洩事件と企業の課題	7
2.2.1	相次ぐ個人情報漏洩事件	7
2.2.2	個人情報漏洩に関する企業の課題	8
2.3	法案の行方と企業の対応	8
3	E C O M会員企業個人情報保護の実態掌握	9
3.1	調査の前提	9
3.2	E C O M会員企業・団体個人情報保護の取組みアンケート調査	9
3.2.1	調査の構成	9
3.2.2	設問	10
3.2.3	設問ごとの調査結果および分析	14
3.2.4	まとめ	32
3.3	E C O M会員企業・団体WEBページ個人情報保護表記目視調査	33
3.3.1	調査概要	33
3.3.2	調査および分析	33
4	E C O M個人情報保護ガイドラインの改定検討	38
4.1	ガイドライン改定検討経緯	38

4.1.1	2001 年度の検討.....	38
4.1.2	2002 年度検討概要.....	38
4.2	ECOM個人情報保護ガイドライン改定案 (Ver.1.5)	42
5	海外有識者・関係機関との接触・海外事情調査.....	76
5.1	北米地域への調査・視察渡航.....	76
5.1.1	渡航主旨・計画.....	76
5.1.2	調査・視察報告.....	77
5.2	中国・韓国 視察調査渡航	93
5.2.1	渡航主旨・計画.....	93
5.2.2	中国インターネット大会.....	94
5.2.3	Asia Privacy Forum への参加.....	95
5.2.4	KISA 主催「International Conference On Personal Data Protection」 ...	98
5.3	アラン・ウェスティン教授来日、ECOM 来訪.....	119
5.3.1	アラン・ウェスティン教授との懇談会実施概要.....	120
5.3.2	議事	120
6	おわりに	134

1 活動概要

1.1 クローズアップされる個人情報保護

2001年3月に国会に提出された「個人情報の保護に関する法律」（以下、「個人情報保護法案」という）は、1年越しの2002年4月、通常国会にて審議入りしたものの、表現の自由への制限や行政機関の個人情報保護法の問題、住基ネット運用スタートにまつわる法整備についての論議が噴出し、結果的に一旦廃案となり、修正案が再提出される運びとなった。

しかしながら、その間、企業や行政機関の個人情報流出・漏洩等のトラブルが相次ぎ、法制化の如何に関らず、事業者の個人情報保護体制の整備は、リスクマネジメントの観点から最重要かつ喫緊の経営課題のひとつになりつつあることは間違いない。

1.2 ECOM個人情報保護WGの活動

ECOM個人情報保護WGでは、昨年に引き続き、電子商取引およびインターネットなどの情報ネットワークを利用した事業及び業務に携わる企業の個人情報保護について焦点をあて、対応策や法制化についての調査・研究、普及啓発活動に取り組んだ。

本WGには、本年度、24社32名（2003年3月現在）のメンバーおよび有識者、行政機関の担当、関連団体のアドバイザーの方々に参加いただき、以下の具体的テーマについて活動してきた。

1.2.1 ECOM個人情報保護ガイドラインの改定検討

1998年にリリースの「ECOM個人情報保護ガイドライン Ver.1.0」を現在審議されている個人情報保護法案に照らして見直し、広く電子商取引およびインターネットなどの情報ネットワークを利用した事業及び業務に携わる企業に適用または参照されるものに改定する主旨にてWG会議の主要議題として検討を重ねた。

具体的には、5月8日の「ガイドライン改定再検討会議」を皮切り7回のWG会議、4回のキーマン・ディスカッション（オピニオン・リーダー検討会等含む）を開催し、その前後でアドバイザーの方々との度重なる検討ミーティングを実施した。

昨年度末時点ではWG会議において中間整理案をまとめたが、そこから、条件設定および措置レベルや語句表記を法案に合わせ、さらには条文構成の見直しと解説の追記・添削

を重ねた。

結果的に法案審議が進展せず、また、現在のところ、いくつかの論点も残存しているため、今年度末の時点では「E C O M個人情報保護ガイドライン改定案（Ver.1.5）」として本報告書に掲載する。今後、残る検討テーマの議論を重ねつつ、法案通過および政令が発令された時点で見直しをするとともに、よりわかりやすい事例や解説の補充を適宜行っていく。

1.2.2 国内外企業・団体の取組み実態および事例・ベストプラクティス調査

アンケート調査やヒアリング等国内外の企業・団体の個人情報保護の取組み実態を調査しつつ、効果的な方策や活動事例等の情報やノウハウを収集し、体系的整理を行うことを目標に取り組んだ。

6月にE C O M会員企業・団体の皆様にご協力いただき、個人情報保護の取組みアンケート（97社回答）を実施した。併せて、同じく会員企業のWebページ個人情報保護についての目視調査（278社対象）も行った。本調査については、今後、E C O M会員企業を対象に年次単位で継続的に実施していきたい。

また、9月には北米の個人情報保護の動向調査・視察を実施した。具体的には、自己情報コントロール権を定義づけたアラン・ウェスティン氏（コロンビア大学名誉教授）訪問、ワシントンDCでプライバシー問題について活動する米国企業GPA（Global Privacy Alliance）メンバーとのミーティング、BBB On Line プライバシープログラム担当者との情報交換を行い、最後にシアトルにて開催の「I L P F（Internet Law & Policy Forum）主催「Security v. Privacy」」にパネル参加した。

さらに11月には、上海にて開催の中国インタ - ネット大会とKorea Information Security Agency（以下「K I S A」という。）主催の「International Conference On Personal Data Protection」への参加、および同会議前日に開催された「Asia Privacy Forum に関する事前ミーティング」に出席し、同時に設立された「Asia Privacy Forum」にE C O Mとして参加することとした。

1.2.3 技術・先進的課題の検討整理

主にP 3 P（Platform for Privacy Preference Project）やモバイルセキュリティ等の技術・先進課題についての調査や検討を活動テーマにあげて取り組もうとしたが、結果的

に今年度は特筆できるような活動がさほどできなかった。ただし、日本でのP3Pの開発および普及を推進するニューメディア開発協会にWGアドバイザーに加わっていただき、また、モバイルECおよびセキュリティ等他WGと個人情報保護に関わる部分での調査や討議を行った。

1.2.4 個人情報保護の正しい理解を促す普及啓発活動

昨年度企画制作を進めた「個人情報保護ガイドブック」を5月に印刷し適宜配布をするとともにECOMのWebページにも公開した。また、各種関連誌への寄稿および講演やプレゼンテーションを適宜行った。

1.3 年間活動を総括して

それぞれの活動において、当初の目標を上回る成果を上げるに及んだものは決して多いとはいえないかもしれないが、従前に増して委員のメンバーに精力的に活動に加わっていただき、ECOM個人情報保護WGとしてオリジナリティあるアウトプットを生むことが出来たのではないだろうか。

とりわけ、ガイドラインの改定検討におけるキーマン・ディスカッションや北米視察等に参加いただいた有志の方々、および、昨年度に引き続き、本WGを支えていただいた中央大学法学部教授（一橋大学名誉教授）堀部政男氏をはじめとするアドバイザーの皆さまにはこの場にて改めて御礼の意を申し述べたい。

2 個人情報保護の動向

2.1 個人情報保護法の審議

2001年3月に国会に提出された「個人情報保護法案」は、2002年4月、通常国会にて審議入りしたが、表現の自由への制限や行政機関の個人情報保護、住基ネット運用にまつわる法整備についての問題が噴出し、次の臨時国会へと継続審議となった。さらにその臨時国会においても十分に審議されないまま、一旦廃案となり、次の通常国会にて修正案が再提出された。

2.1.1 当初の個人情報保護法案

当初の「個人情報保護法案」は、大きく全体を包括する基本原則部分と民間事業者が守るべき義務規定部分の2つを含む構成であった。

基本原則は、1980年に経済協力開発機構（以下「OECD」という。）の「プライバシー保護と個人データの国際交流についてのガイドラインに関する理事会勧告」（以下「OECDガイドライン」という。）で示された、いわゆる「OECD8原則」を5つに整理したものであり、この部分は公的部門および民間部門と対象を限定しないとされていた。即ち報道分野についてもこの基本原則については適用除外とならないとされていた。

また、主に第5章にて個人情報を取扱う事業者に対する義務が規定されており、それに対しては行政的な罰則が課せられている。

以下に同法案の目次を記す。

< 個人情報の保護に関する法律 >

第一章 総則（第一条・第二条）

第二章 基本原則（第三条 - 第八条）

第三章 国及び地方公共団体の責務等（第九条 - 第十一条）

第四章 個人情報の保護に関する施策等

第一節 個人情報の保護に関する基本方針（第十二条）

第二節 国の施策（第十三条 - 第十五条）

第三節 地方公共団体の施策（第十六条 - 第十八条）

第四節 国及び地方公共団体の協力（第十九条）

第五章 個人情報取扱事業者の義務等

第一節 個人情報取扱事業者の義務（第二十条 - 第四十一条）

第二節 民間団体による個人情報の保護の推進（第四十二条 - 第五十四条）

第六章 雑則（第五十五条 - 第六十条）

第七章 罰則（第六十一条 - 第六十四条）

附則

2.1.2 2002 年度の国会における審議

国会提出後、丸 1 年間審議入りを果たさぬまま経過した同法案であったが、2002 年 3 月頃より審議入り間近の報道がなされ始めた。当初は、主に同じ時期に審議入りした「人権擁護法案」などと「メディア規制 2 法案（当初は「青少年有害社会環境対策基本法案」を加え「メディア規制 3 法案」と呼ばれた）」として頻繁にマスメディアに取り上げられ、マスコミおよび著作に携わる作家・フリーライター・ジャーナリストらから、表現および報道の自由に制約を与えるとの反対の声明が発せられた。

法案は 4 月 25 日衆院本会議での趣旨説明に始まり、衆議院内閣委員会にて審議が重ねられることとなった。そこでは、同法案とともに「行政機関の保有する個人情報の保護に関する法律案」、「独立行政法人等の保有する個人情報の保護に関する法律案」、「情報公開・個人情報保護審査会設置法案」及び「行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律案」があわせて同委員会で一括して審議された。

冒頭の表現および報道の自由についてのマスコミ等の反対に続き、おりしもこの時期にコードシステムがスタートする住民基本台帳ネットワークシステムの問題やエステティックサロンの資料請求データや建材会社のアンケート回答データがネット上で閲覧可能となる事件および防衛庁の情報公開請求者リストの閲覧といった管理に関する問題が報道され、結果的に立法化への議論は進展しないまま、7 月末、通常国会は閉幕する。同法案は引き続き、秋の臨時国会にて継続審議されることとなった。

また、その後の臨時国会においても、その終盤に多少の質疑等があったものの、本質的な議論が不十分なまま推移した。結局、2002 年の通常国会・臨時国会を通じてトータルで約 22 時間におよぶ審議の末、廃案となった。

2.1.3 修正案の提出

臨時国会の後半頃より、政府・与党より修正案・再提出の動きが見られようになる。通常国会時点でも、表現や報道の自由についての制限に反対する共同アピールの会や全国消費者団体連絡会、読売新聞等より対案を提示されており、また、小泉首相の読売新聞提案の修正試案に対する検討指示のコメント等が報道されたものの、それ以上に進展していなかった。

12月13日、内閣委員会では個人情報保護法関連5法案について、継続審議の手続きを取らず、一旦廃案となった。その前後で、与党3党のより修正要綱骨子が以下のようにまとめられている。

(個人情報保護法案)

すべての人に個人情報の適正取得などの努力義務を課す「基本原則」を削除

報道機関などへの情報提供者に対し、主務大臣が関与しないことを明記

「報道」の定義を明記

罰則付きの義務規定の適用除外とする「報道機関」に個人を含むことを明記

「著述を業として行なう者」を、義務規定の適用除外とすることを明記

(行政機関個人情報保護法案)

行政機関の職員らに対して次の行為に関する罰則規定を設ける。

自己の利益を図る目的で職権を乱用した個人の秘密の収集 個人情報の盗用または不正目的での提供 コンピュータ処理されている個人データの漏洩

- 以上、2002年12月7日朝日新聞より -

年が明けて2003年1月20日より第156通常国会が召集された。上記の通り、「個人情報保護法案」については、1月22日付日本経済新聞にて「メディア、対象外に 個人情報保護新法案、来月に決定」との報道がなされ、2月6日付読売新聞では「政府の個人情報保護法案 与党検討会が了承」と報じられ、修正案の提出は2月末から3月初旬との見方が有力視されていた。

2月28日付毎日新聞には「個人情報保護法案自公両党が了承 政府、来月7日閣議決定」との見出しで具体的な日程が報じられている。また、「与党は同法案を今国会の最重要法案と位置付け、衆参両院に与党が委員長となる特別委員会を設置し、審議を急ぐ方針。」

とある。

2003年3月7日、修正案が閣議決定、国会に提出された。既報のとおり、旧法案に対して第4条から第8条の基本原則が削除され、その他、旧法案の第40条配慮義務、第55条適用除外が前述のとおり表現の自由に配慮した形に修正された。旧法案第5章中の一般の個人情報取扱事業者に対する義務規定については変更点はない。

章立てとしては、第4条から第8条の基本5原則が削除され、第3条の基本理念が第1章に含まれたため、旧法案の第2章が無くなり、以降の章が繰り上がった。

以下に修正案の目次を記す。

< 個人情報の保護に関する法律案 >

第一章 総則（第一条 - 第三条）

第二章 国及び地方公共団体の責務等（第四条 - 第六条）

第三章 個人情報の保護に関する施策等

第一節 個人情報の保護に関する基本方針（第七条）

第二節 国の施策（第八条 - 第十条）

第三節 地方公共団体の施策（第十一条 - 第十三条）

第四節 国及び地方公共団体の協力（第十四条）

第四章 個人情報取扱事業者の義務等

第一節 個人情報取扱事業者の義務（第十五条 - 第三十六条）

第二節 民間団体による個人情報の保護の推進（第三十七条 - 第四十九条）

第五章 雑則（第五十条 - 第五十五条）

第六章 罰則（第五十六条 - 第五十九条）

附則

2.2 相次ぐ個人情報漏洩事件と企業の課題

2.2.1 相次ぐ個人情報漏洩事件

一方、個人情報を取扱う企業のほうに目を向けると、前述のとおり、個人情報保護法の審議の間、企業や行政機関の個人データ流出・漏洩等のトラブルが相次ぎ発覚し、頻繁にマスコミに取り上げられた。内閣委員会での審議の中では、民間事業者による漏洩事件は

23 件、約 17 万 4000 件（個人情報のデータ件数）とされており、また、従来からある従業員または委託業者が意図的に個人データを持ち出すケースや不注意に紛失したり盗難にあったりするケースから、昨今はインターネット上より第三者に自由にアクセスできる状態に放置され、漏洩する事故が増加している。

2.2.2 個人情報漏洩に関する企業の課題

その原因は、業務指示や発注および取扱う担当者および委託先の不注意や知識の欠如であることが多い。

マーケティング調査やアンケートの実施について、従来どおりに営業や企画部門の担当の指示で企画・制作関連の業者に委託していたままにインターネット調査を行うケースが増えているが、そのセキュリティが十分でないために個人データが漏洩・流出する事故の発生を招くことがある。消費者と直接接点を持つそれぞれの現場にインターネットを利用した新たなツールが導入・利用され、システムの分散管理が進む一方で、不用意なセキュリティレベルのままで業務革新を図ることの危険性を自覚し、情報システム部門のみでなく個人情報を取り扱う部門の全従業員および委託先従業員にまで個人情報保護方針及び内部規程が浸透するよう図られなければならない。

2.3 法案の行方と企業の対応

国会審議の行方は現時点で予測しがたい状況にある。しかしながら、確実に進展するインターネットや電子商取引の普及と個人情報の高活用・高利用グローバル化への広がりやマスコミが取り上げることにより個々人に芽生えてきた個人情報に対する意識、2003 年 8 月よりの住民基本台帳ネットワークシステムの本格稼働等を考え合わせると、企業の個人情報保護についての対応は急がれる。

現状は、前述のような個人情報漏洩についての事件が多く報道されているが、法制化されるとその取扱いについての適切さを問われることも考慮すべきであり、また、海外での苦情の事例に取り上げられるスパムメールの問題についても正しく認識し、適切に対処することが求められる。

法案の審議動向を今後も注視しつつ、今だ未整備の事業者にとっては、今後どのように体制を構築し、役員から従業員に及ぶまでの意識浸透を図っていくかということについて一刻も早く手を打つことが必要となる。

3 ECOM会員企業個人情報保護の実態掌握

3.1 調査の前提

日本における企業の個人情報保護実態についての定量的データは少なく、また定点観測として継続的に調査実施されているものがほとんどみられない。

ECOM 個人情報保護 WG では、主要企業の個人情報保護に対する意識および実態の趨勢を把握する目的にて、ECOM 会員企業を対象にアンケートおよび Web サイトの目視調査を実施し、それを年々継続的に調査することで企業の個人情報保護の意識浸透および体制構築および実装の度合いを観測することとした。

3.2 ECOM 会員企業・団体個人情報保護の取組みアンケート調査

約 300 の ECOM 会員企業および団体に対し、個人情報保護に関する設問を付したアンケートを送付し、2002 年 5 月 20 日から 6 月 5 日の間に、基本的に各社単位で、個人情報保護担当部門、経営企画部門、法務部門等、個人情報保護関連案件に関わっている部門あるいは全社戦略および社内規定等を統制する部門の方に Web ページより回答いただいた。

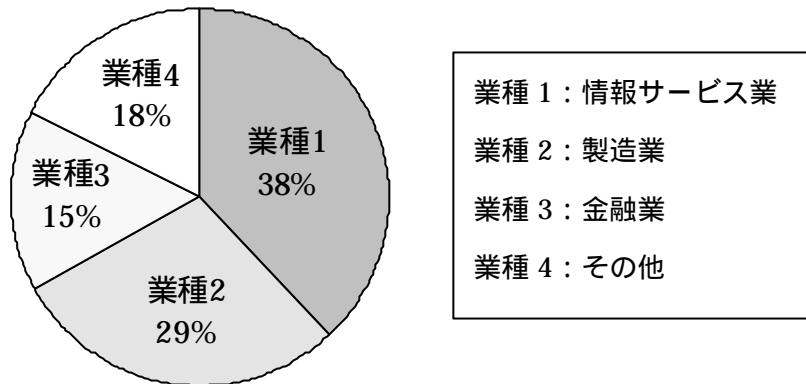
3.2.1 調査の構成

- (1) アンケート調査時期 …………… 2002 年 5 月 20 日～6 月 5 日
- (2) 対象 …………… 電子商取引推進協議会 (ECOM) 参加企業 理事会員、正会員 A、正会員 B (実施当時 296 社)
- (3) 有効回答数 …………… 97 件 (回収率 : 32.8%)
- (4) 回答業種別分類

ご回答頂いた業種	件数	分類業種	件数
情報サービス業	30	業種 1 情報サービス業	37
その他情報サービス業	7		
製造業 (電気機器・精密機器)	17	業種 2 製造業	28
その他製造業	11		
金融・保険業	13	業種 3 金融業	15
その他金融業	2		
電力・ガス業	7	業種 4 その他	17
卸売業	4		
運輸・倉庫業、	6		
マスコミ、エンタテインメント			
合計	97	合計	97

図表 3-2-1

アンケート回答会社業種分類（有効回答会社数 = 97社）



図表 3-2-2

初年度のため、分析するにあたって比較対照するに足るデータが十分でないため、アンケート回答の際、回答いただく各社の業種属性について図表 3-2-1 左段の区分より選択（自己申告）いただき、それをさらに同右段の業種グループに分類し、設問ごとにそれぞれの業種グループの集計より、特性を推測分析した。

3.2.2 設問

設問は全 15 問で、以下のとおりである。

貴社には個人情報保護に関する社内規定がありますか？

- 個人情報保護についてまとめた規定がある
- 各内規の節々に個人情報の取扱いについての規定が散在している、あるいは各部門にてまちまちではあるが規定を定めているところもある
- 今はないが、今後策定しようと考えている
- ない

上記の規程及び内規を実行する上での推進責任者の任命または担当部門の設置はなされていますか？

- 専任の担当または部門を設置している
- 兼務で担当を任命している、または部門内に担当や職務を割り当てている

- c. 今はないが、今後任命あるいは設置しようと考えている
- d. ない

貴社の Web サイトを通じて収集するお客さまの個人情報の利用目的について、以下の中から該当するものを選択下さい（複数回答可）

- a. EC（Web サイト上での商取引行為）を行うため
- b. 顧客サポートやサービスの提供
- c. 代金等の回収等
- d. 販促情報の提供
- e. 個人名を記入する動向調査（お客さまの嗜好やニーズの掌握等）
- f. 無記名での動向調査（お客さまの嗜好やニーズの掌握等）
- g. Web サイトからは個人情報を収集しない
- h. その他（ ）

現在収集している個人情報データは何件（1 件 = 1 人分の個人情報）ぐらいありますか？

- a. 1000 件未満
- b. 1000 件以上 1 万件未満
- c. 1 万件以上 10 万件未満
- d. 10 万件以上

お客さまより個人データを収集する際、顧客に対し事業者（自ら）の名称、部署、連絡先を明示していますか？

- a. 明示している
- b. 明示していない

お客さまより個人データを収集する際、顧客に対し収集する個人情報の利用目的を明示し、同意を得ていますか？

* 同意 = 本人より、利用の了承（ = 同意 ）の返信等積極的な意向を表す行為を得ていること

している

- b. 示しているが、わかりにくいかもしれない
- c. 示していない

個人情報の取扱いを適正に行っていることを証明する「プライバシーマーク制度」について知っていますか？

- a. 取得している
- b. 一部の部門で取得している
- c. 現在取得はしていないが、取得を考えている
- d. 知っているが、取得していないし、取得を考えてもいない
- e. 知らない

お客さまからアクセスがある際にお客さまが再度そのサイトに訪れたとき、通信履歴データをサーバー側で認識し、利用者の手続上の再入力等を省くことができるクッキーというしくみを利用していますか？

- a. クッキーを利用している
- b. クッキーは利用していない
- c. クッキーについてはよくわからない

(上記 a. の回答者)クッキーを利用していることとその利用目的を明示していますか？

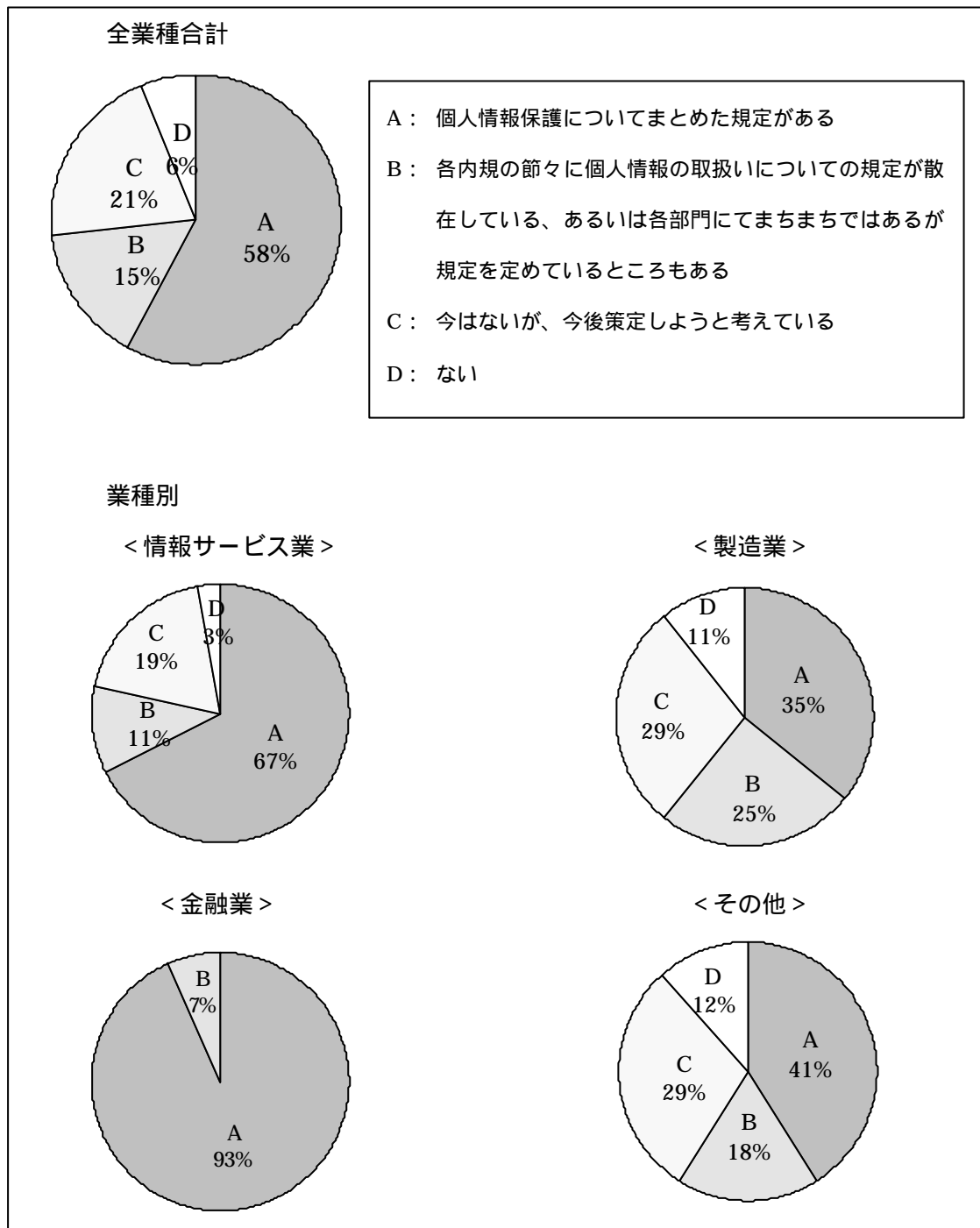
- a. 明示している
- b. クッキーの利用に関しては特に知らせていない

「P3P (Platform for Privacy Preferences)」という個人情報保護のレベルについてユーザー - 事業者間で自動的に確認できる技術規格がありますが、それについて、

- a. 採用し、運用している
- b. まだ採用していないが、検討している
- c. 採用を検討していない
- d. 知らない

3.2.3 設問ごとの調査結果および分析

Q 1 . 貴社には個人情報保護に関する社内規定がありますか？（有効回答会社数 = 97社）



図表 3-2-3

全体では、「各内規の節々に個人情報の取扱いについての規定が散在している、あるいは

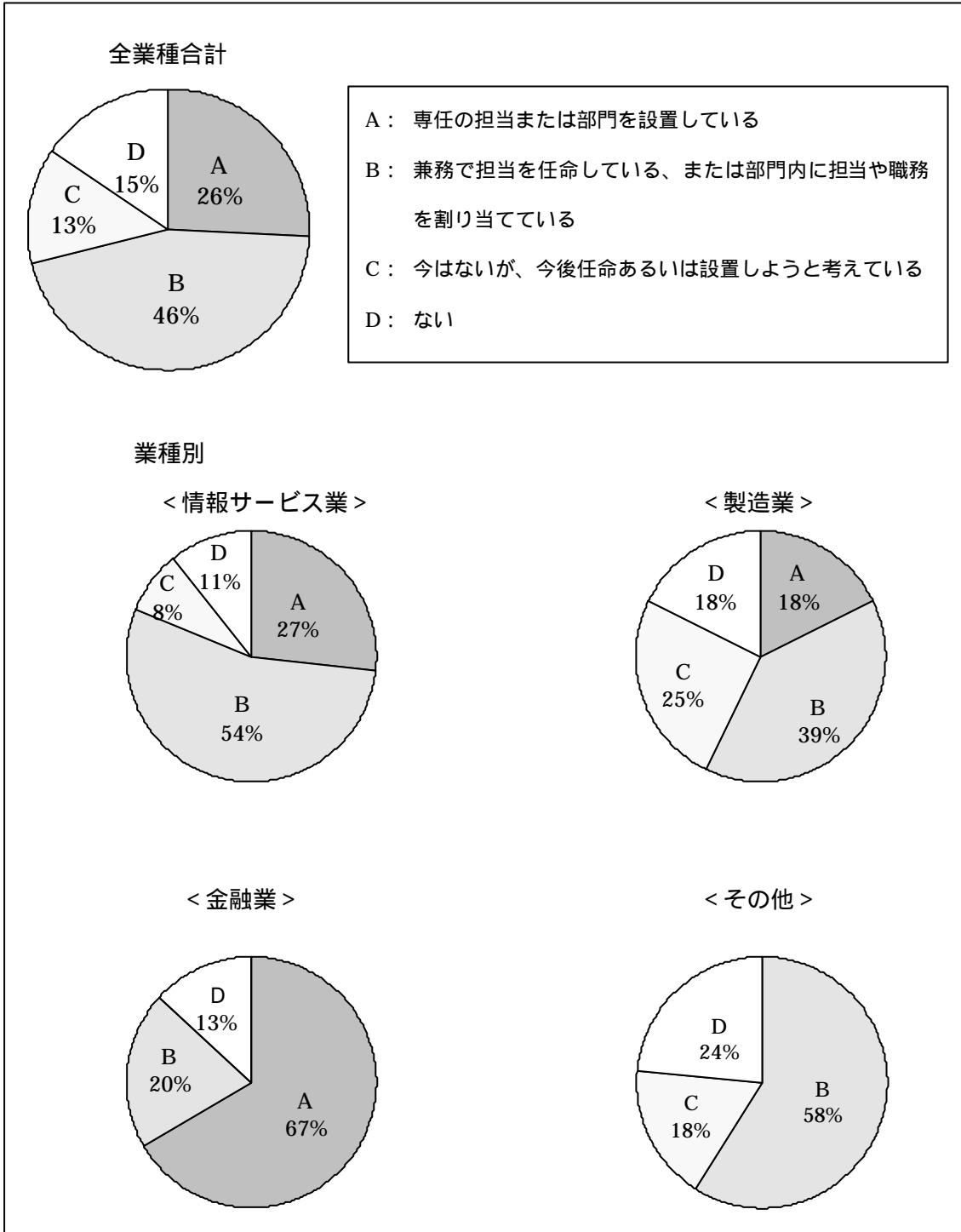
は各部門にてまちまちではあるが規定を定めているところもある」を含め、73%が個人情報保護についての社内規定を定めている。

業種別に見ると、金融業はその回答いただいた全社ですでに内規化されており、その9割強は個人情報保護についてまとめた規定を持っている。業界としての取組みおよび顧客の金融資産関連の情報を取扱うという業界特性がその要因と推察される。

また、情報サービス業も78%が規定を定められており、業種の特性が表れている。

製造業およびその他は、4割強はまだ規定化できていない。しかしながら、その大方（規定化されていないと回答されている約7割）は今後整備が必要と考えているようである。また、このセグメントの中はかなり広範な業種が入っており、分析の都合上、大きく括っているが、更に細分化された業種ごとに事情が異なることもあるように思われる。

Q2. 上記の規程及び内規を実行する上での推進責任者の任命または担当部門の設置はなされていますか？（有効回答会社数 = 97社）



図表 3-2-4

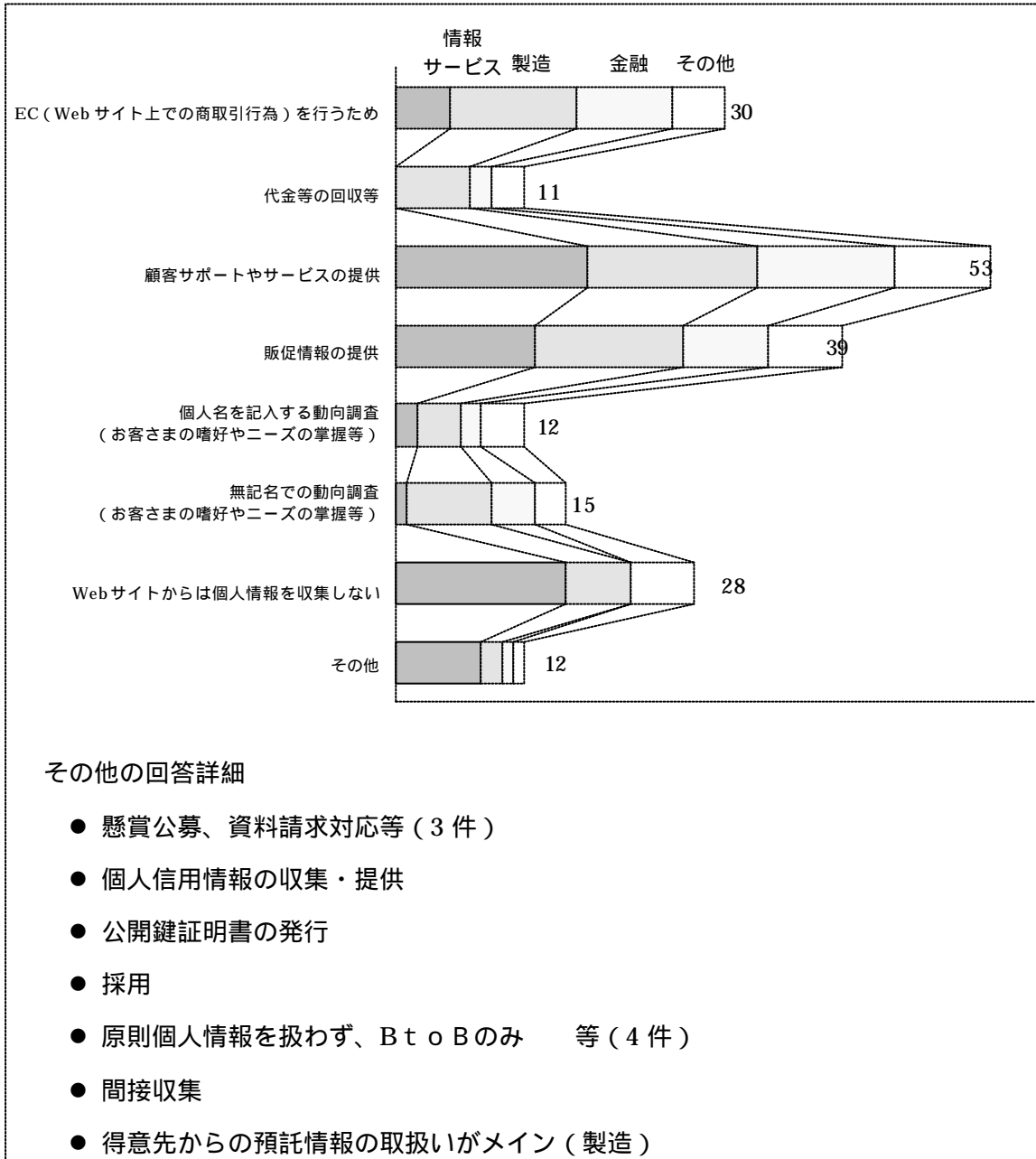
ここで調査する個人情報保護の推進責任者および担当部門の設置については、全体では

Q1の社内規定についての調査結果とほぼ同じくらいの割合の70%が専任・兼任を含め、設置しているとの集計結果となった。しかしながら、専任での設置は全体の26%に留まっている。類推であるが、法務、情報システム、セキュリティあるいは本社企画スタッフ関連の部門がそれを担っているのではないだろうか。

業種別では、社内規定についての調査結果と同様に、金融業では専任が67%、兼務が20%と9割近く設置しており、情報サービス業では専任・兼務を合わせた率では社内規定についての調査結果とほぼ同等ながら、そのうちの専任のウェイト（情報サービス業全体の26%）はそれ程高くなく、兼務が多いようである。

製造業・その他は4割強が現状担当部門又は責任者を設置していない。

Q3. 貴社の Web サイトを通じて収集するお客さまの個人情報の利用目的について、以下の中から該当するものを選択下さい（複数回答可）（有効回答会社数 = 97 社）



図表 3-2-5

本設問は、Web サイトを通じて収集する個人情報についての利用目的に関する実態を調査したものである。

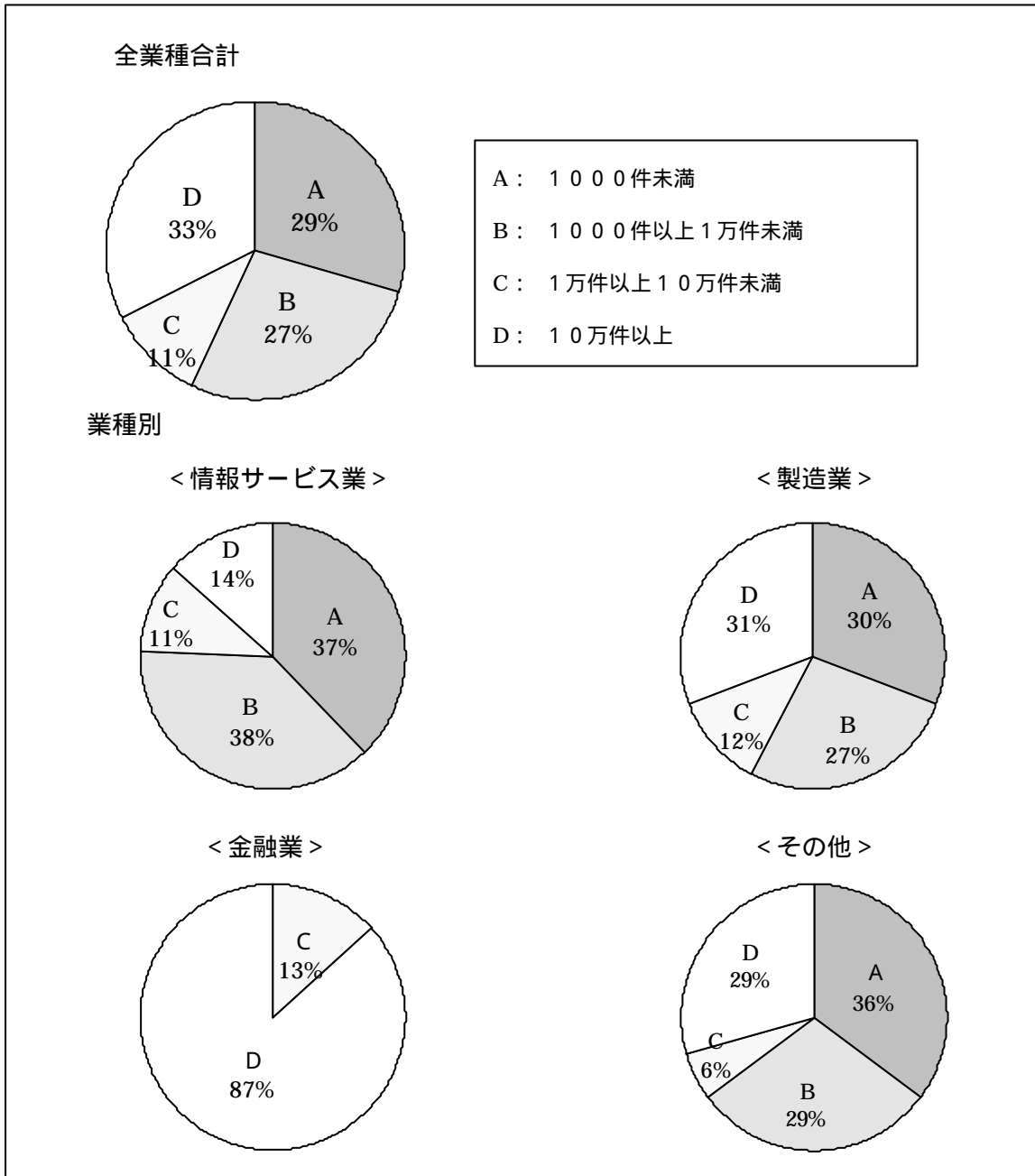
まず、全体回答の 97 社に対して、28 社 (Web サイトからは個人情報を収集しないと回答の会社) + 4 社 (その他回答のうち「原則個人情報を扱わず、B to Bのみ」と回答する

会社)=32社(全有効回答社97社対比=33%)はWeb上より個人情報を収集していないとの回答であった。とりわけ、情報サービス関連の業種では、その事業領域として企業からの情報処理受託等の業務のようにBtoB領域での業務が中心となり、顧客からの個人情報を収集するといったシーンがさほどないと推察される。(Web上より個人情報を収集していないの約6割が情報サービス業)

具体的な利用目的として最も多いのは、顧客サポートやサービスの提供(Web上より個人情報を収集していないを除く67社中53社=79%)や販促情報の提供(同39社=58%)が多い部類といえよう。

EC(Webサイト上での商取引行為)を行うため(同30社=45%)や代金等の回収等(同11社=16%)といった狭義での電子商取引の場面での個人情報入力は比較的少ないといえる。

Q4. 現在収集している個人情報データは何件（1件=1人の個人情報）ぐらいありますか？（有効回答会社数=95社）

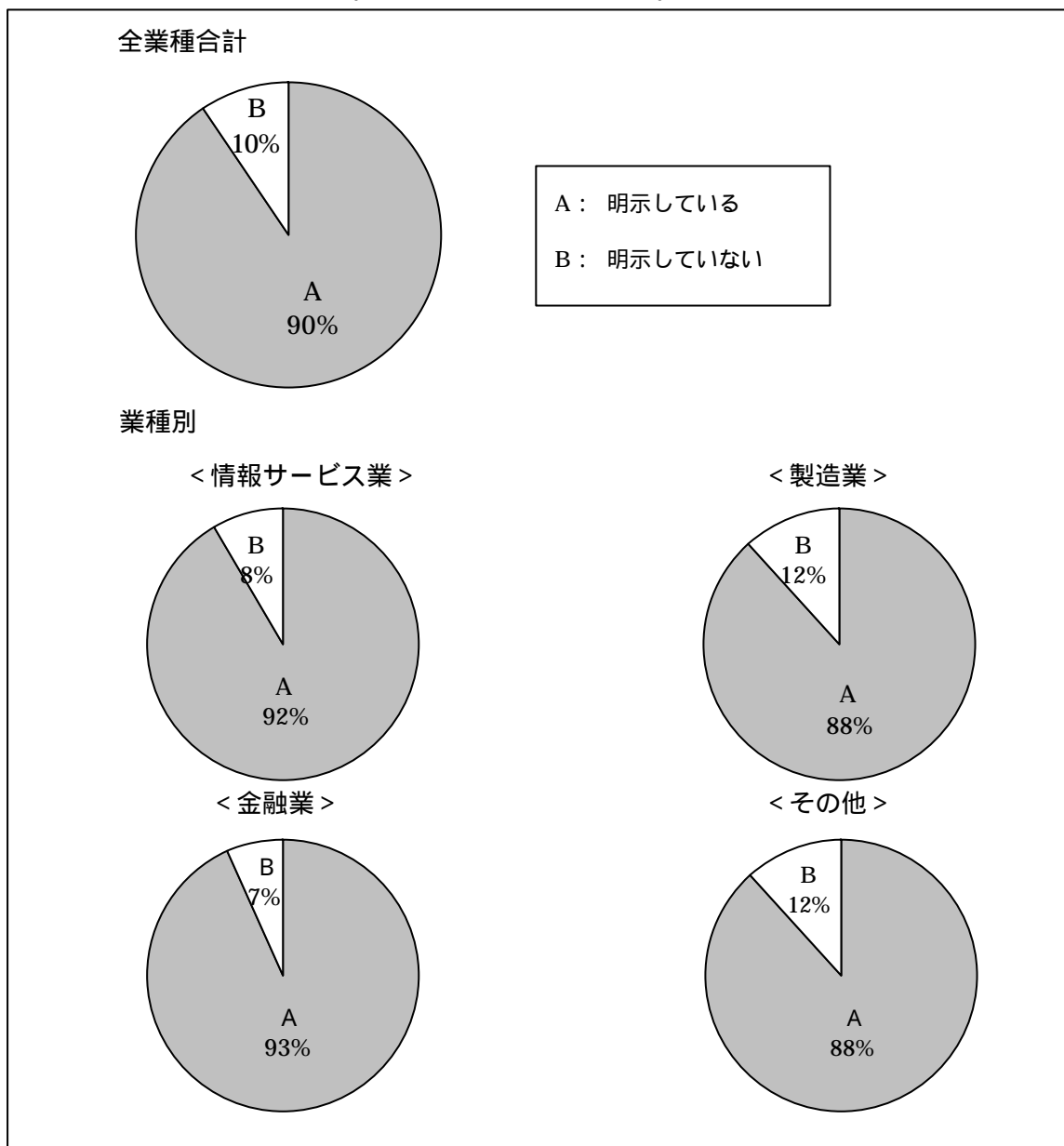


図表 3-2-6

個人情報保護法案において「個人情報取扱事業者」について除外されるひとつに「その取り扱う個人情報の量および利用方法からみて個人の権利利益を害する恐れが少ないものとして政令で定める者」があることの参考に設問を設定した。

全体では 1000 件未満が約 3 割であり、10000 件を超えるところは 4 割強である。

Q5. 顧客より個人データを収集する際、顧客に対し事業者（自ら）の名称、部署、連絡先を明示していますか？（有効回答会社数 = 94社）

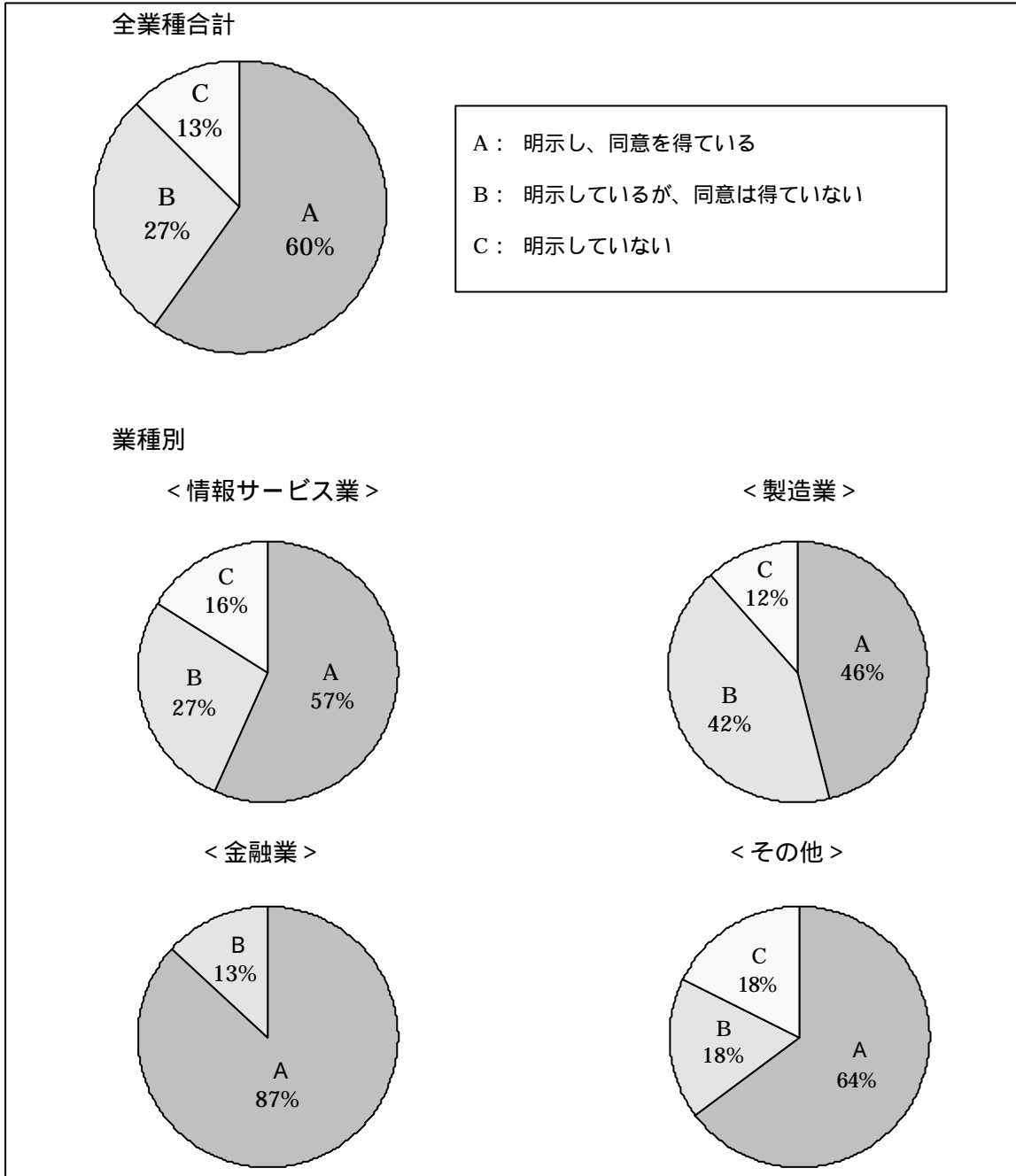


図表 3-2-7

顧客より個人データを収集する際、大方の企業は名称、部署、連絡先を明示しているとの回答結果となった。

Q6. お客さまより個人データを収集する際、顧客に対し収集する個人情報の利用目的を明示し、同意を得ていますか？（有効回答会社数 = 95社）

（*同意 = 本人より、利用の了承（=同意）の返信等積極的な意向を表す行為を得ていること）



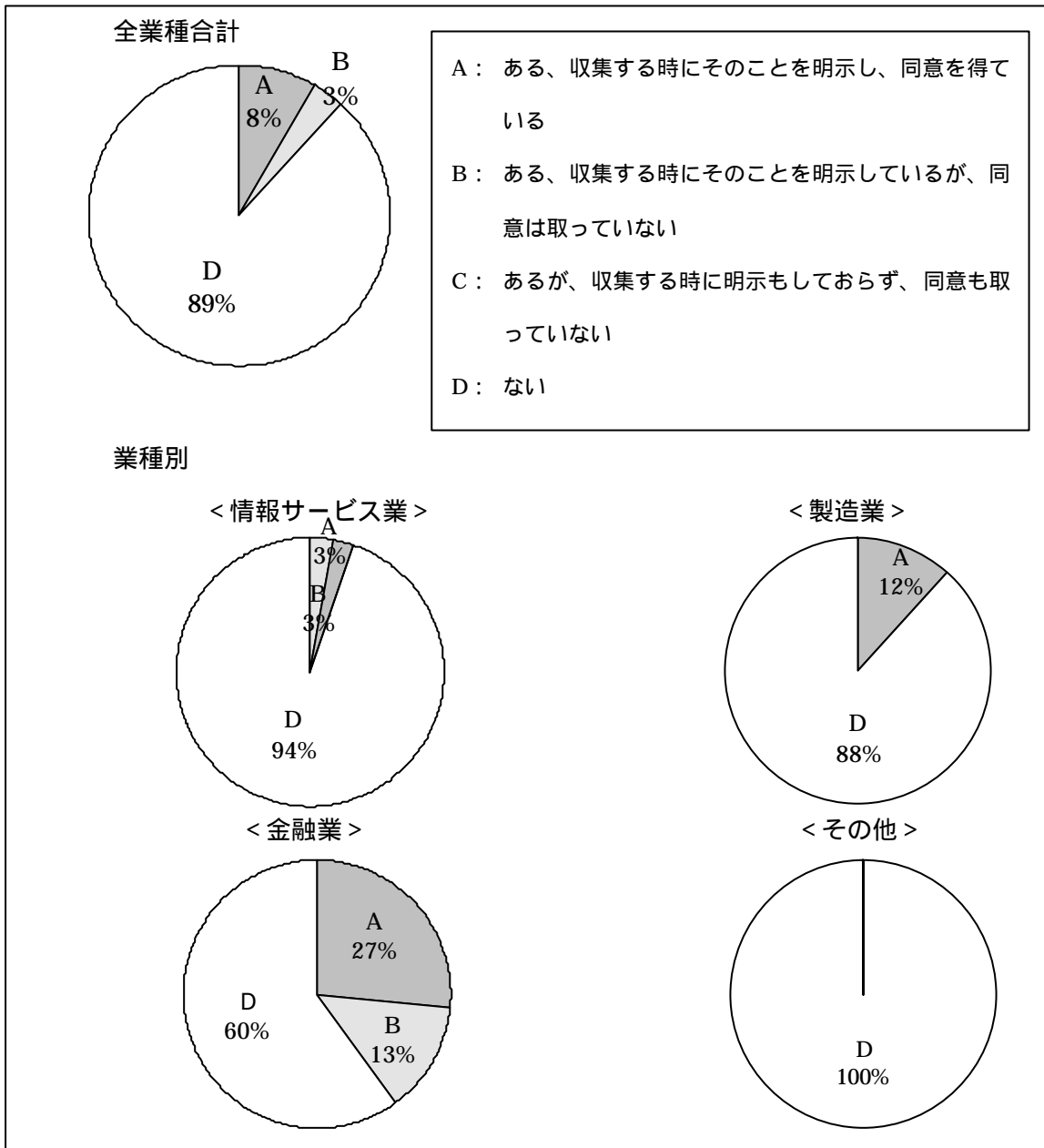
図表 3-2-8

個人データを収集する際、全体の 87% が明示しており、また 60% は同意まで得ている。そのうち、金融は、100% が明示、87% が同意を得ている。

Q7. 収集した個人情報を第三者に提供することがありますか？（有効回答会社数 = 95社）

注1) 第三者提供例：リスト化し、第三者の問合せに対し個別に提示したり、リストごと一括して他の法人に提供や販売等すること

注2) 業務委託のため委託業者等に個人データを渡す場合は含みません

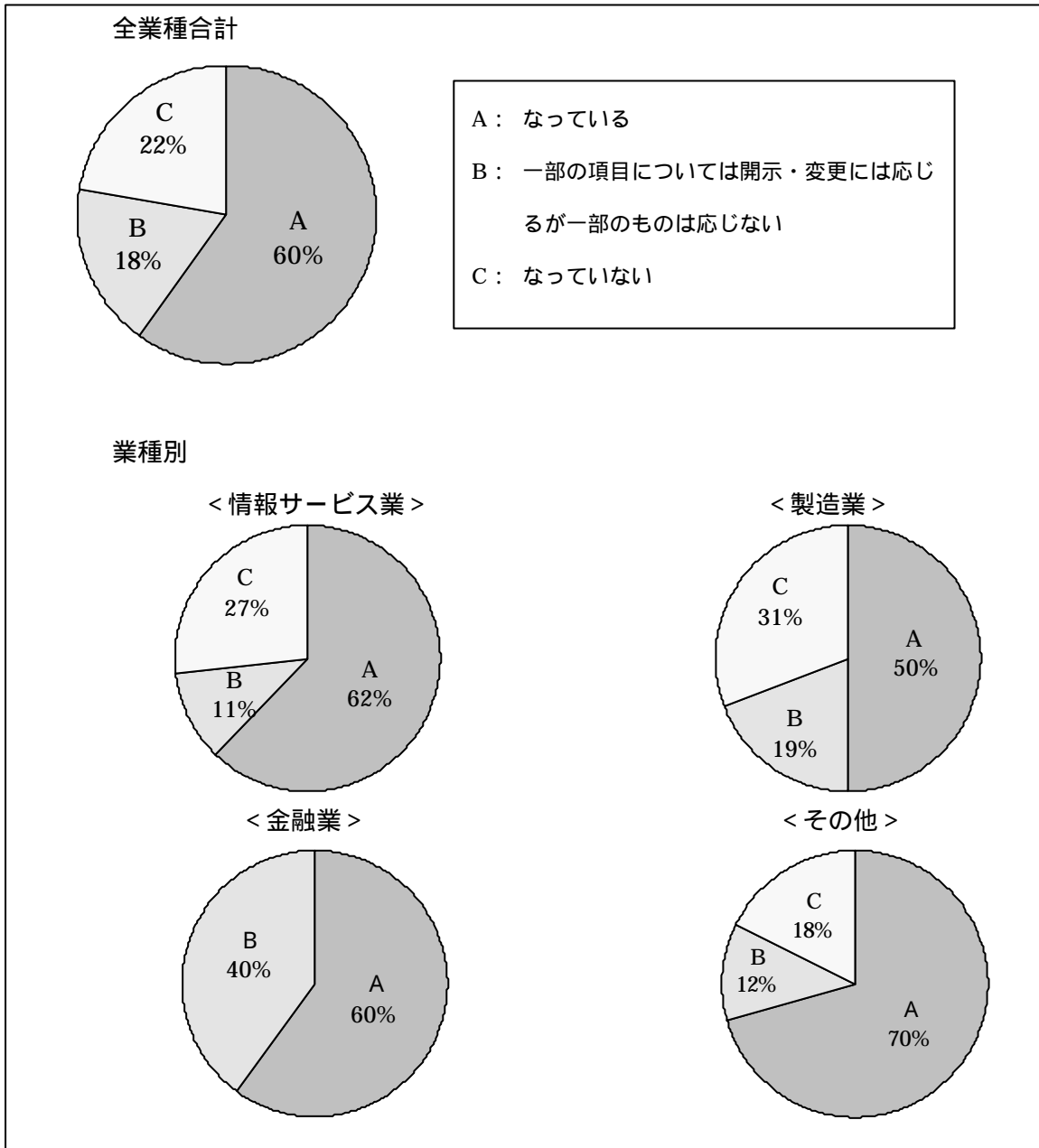


図表 3-2-9

個人情報保護法案では第三者提供については委託や共同利用等と区分し、通常の企業活動の中では、さほど多くないケースに限定する形で構成されている。その前提を注釈に付き、質問したところ、全体で約 10%との回答であった。同意を得ていないが 3%ほどあが

っているが、仔細は未調査である。

Q8．保有する個人データは本人（お客さま）から開示や変更・利用停止等を求められたら
即座に対応できるようになっていますか？（有効回答会社数 = 95社）



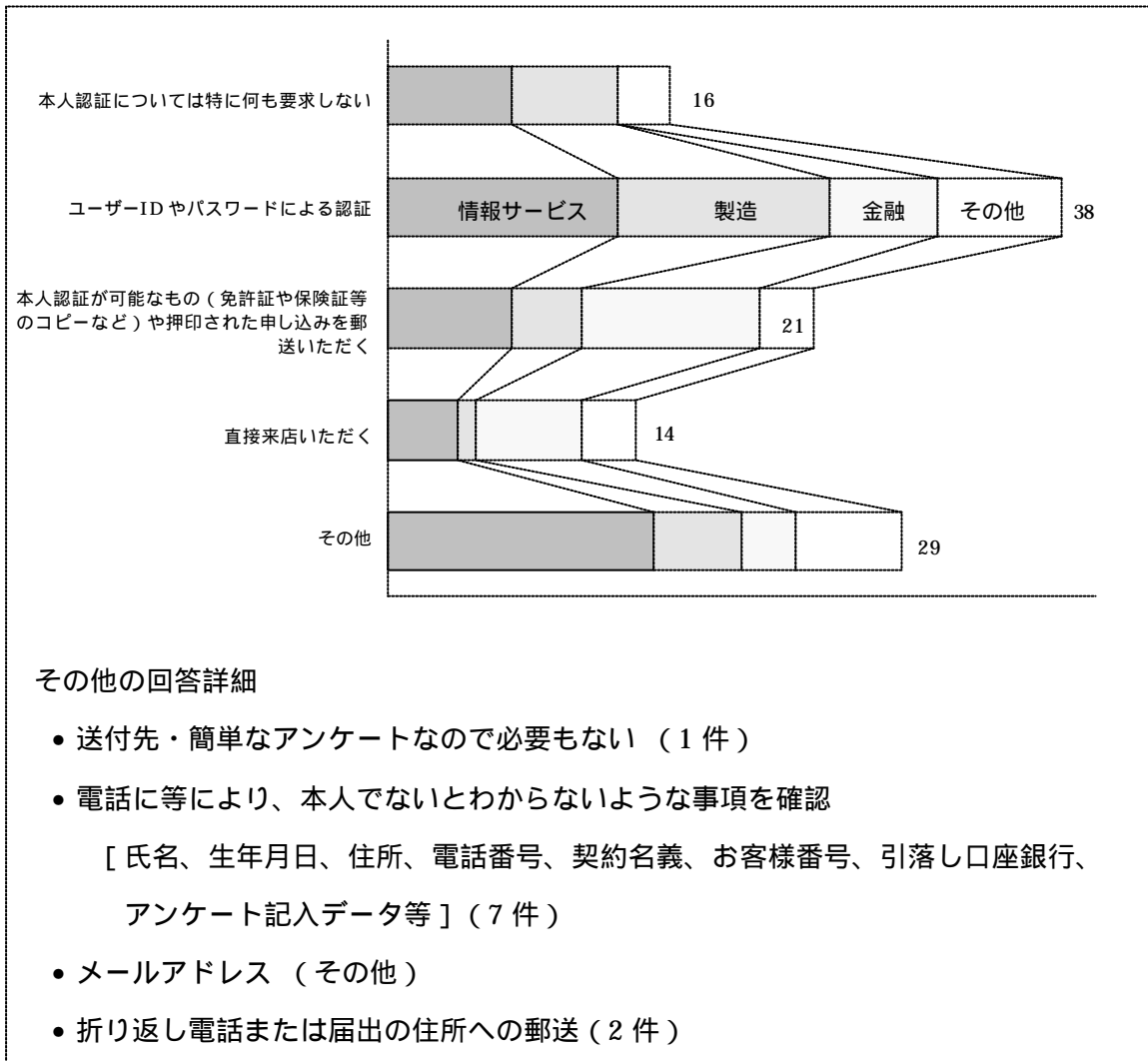
図表 3-2-10

個人情報保護法案における透明性の確保について質問を設定した。回答によると、全体では8割程度が対応できるようになっている。

また、それぞれの業種の割合をみるとQ6の利用目的の明示との相関があるように見受

けられる。また、Q3にあるように個人情報の収集を行っていない会社からの回答も含まれており、実際に対応できるようになっていないのは10%を切ると推察される。

Q9. 上記の要求に対して本人であることの確認はどのようにしていますか？（複数回答可）
 （有効回答会社数 = 95社）



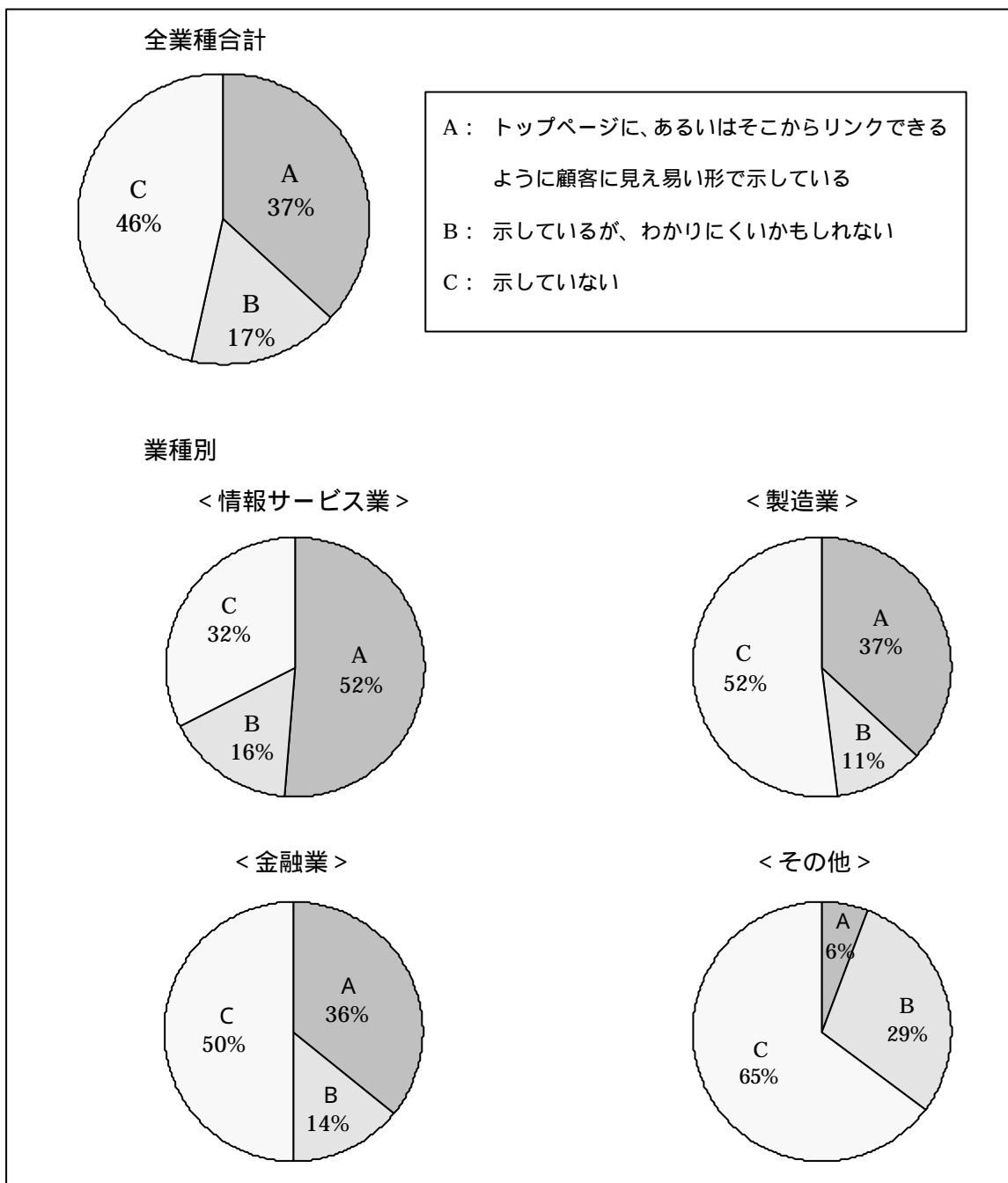
図表 3-2-11

本人確認の方法としては、ユーザーIDやパスワードによる認証が多いが、金融業に多く見られる、より正確な確認を求めるための本人認証が可能なもの（免許証や保険証書等のコピーなど）や押印された申し込みの郵送を求めるケースが随分多い。また、直接の来店や電話での本人でないといけないような事項の確認という確認方法が、やはり金融業を中心に相当件数揚げられた。

何も要求しないの回答が 16 件だが、Q 3 にて Web 上より個人情報の収集を行っていない会社を差し引くと、実質的な何も要求していないとの回答は 10 件程度と推察される。

Q10. 貴社サイトに「プライバシーポリシー」あるいは「個人情報保護方針」をトップページ 或はお客さまに見えやすいところに示していますか？

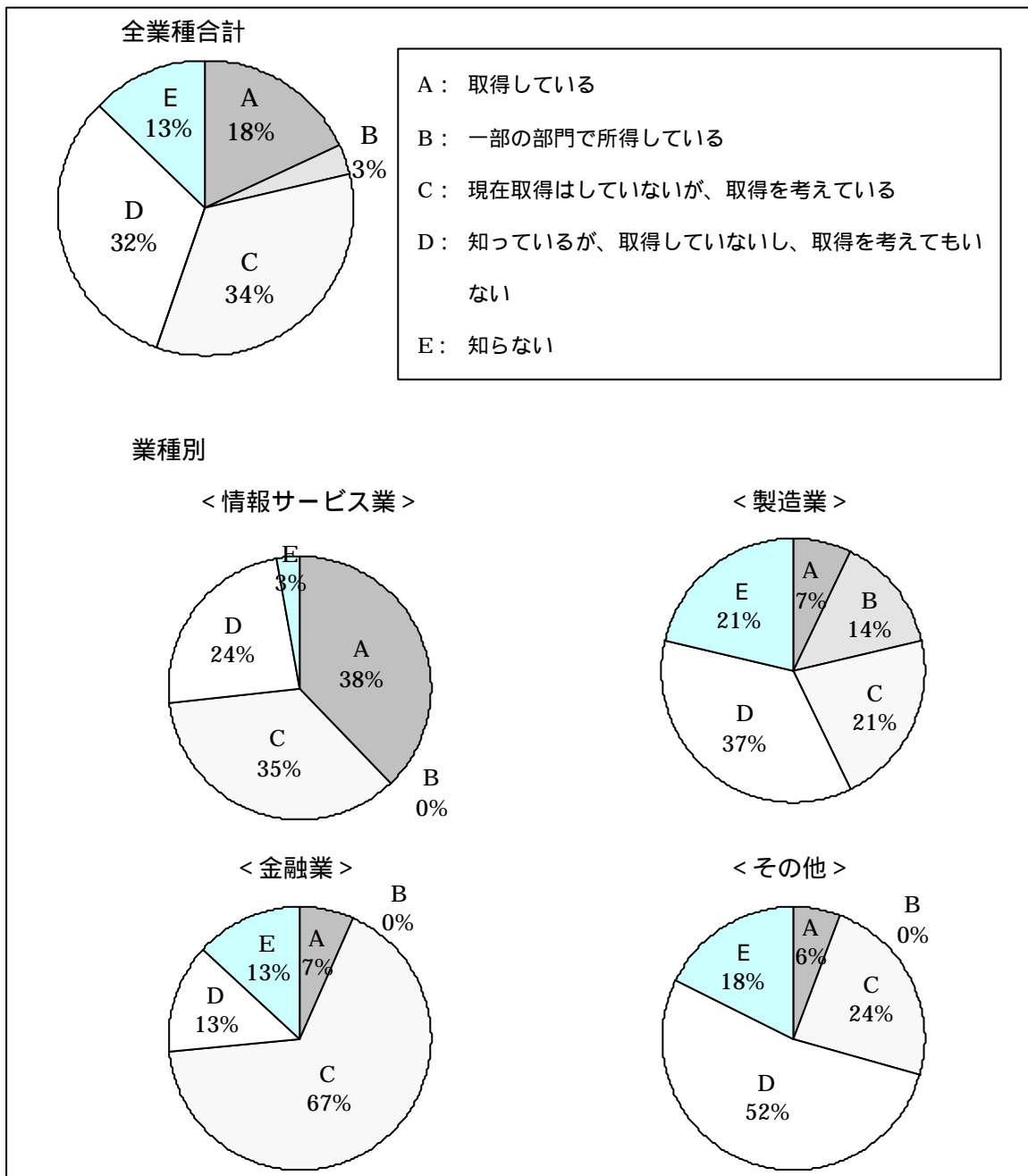
(有効回答会社数 = 95 社)



図表 3-2-12

ここでは、アンケート回答でのプライバシーポリシーの掲示の有無を問うているが、後章の会員企業の Web ページ目視で行った調査とを比較し、詳細の実態推察を行うこととする。全体では、示しているが 52%。うち、情報サービスでは 67%と高率に及んでいるが、情報サービス以外では 5 割に満たない。

Q11．個人情報の取扱いを適正に行っていることを証明する「プライバシーマーク制度」について知っていますか？（有効回答会社数 = 97社）



図表 3-2-13

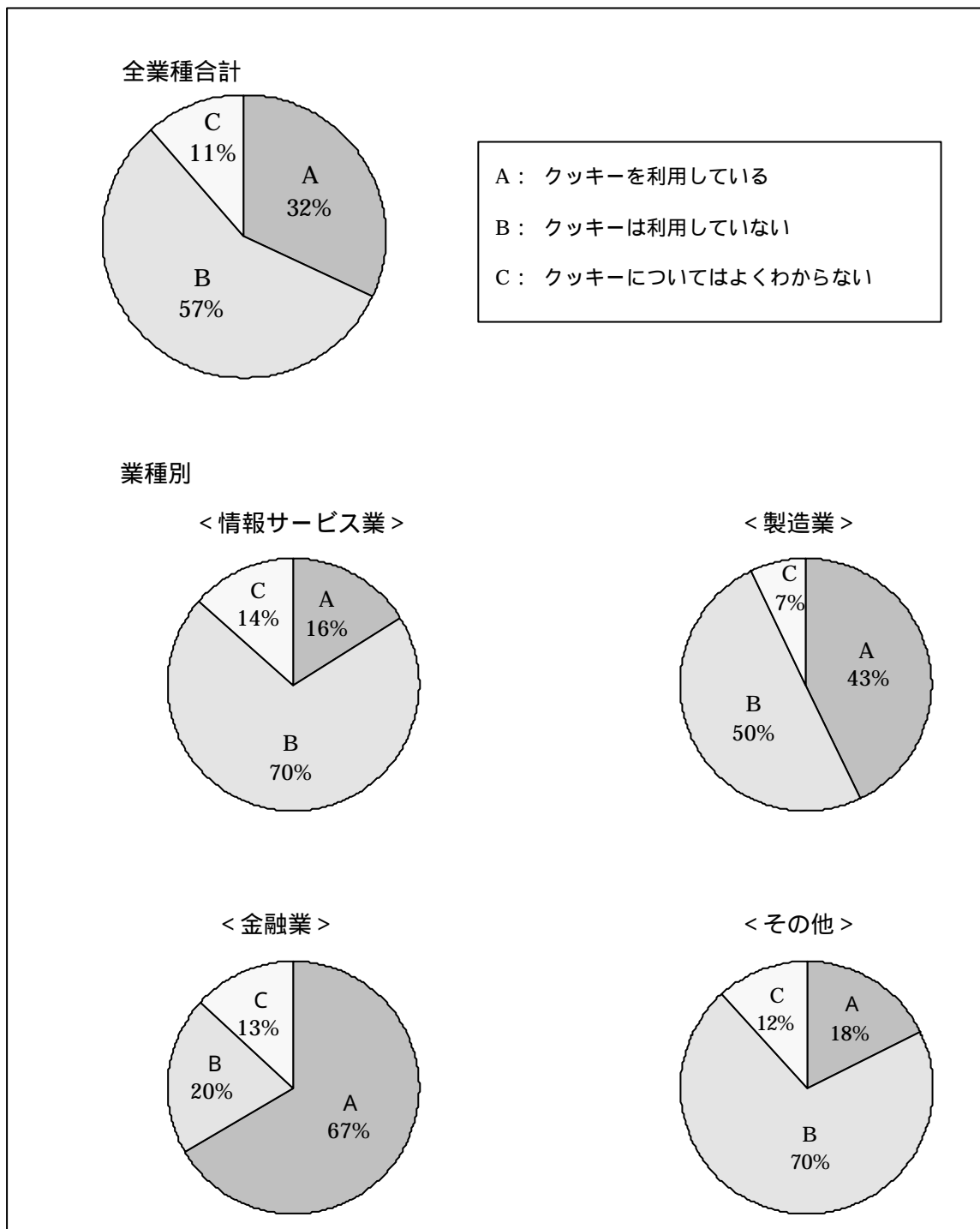
プライバシーマークについても、後章の会員企業の Web ページ目視で調査を行っているが、この質問ではその認知および取得の意志を問うている。

全体では「取得している」「一部の部門で取得している」が 21%に上る。また、「現在取得はしていないが、取得を考えている」企業が 34%ある。

業種別にみると、情報サービス業では「取得している」が 36%と他の業界(6~7%)に比べ断然高い。これは、情報サービス業に属する企業が、業務受託のためにマーク取得が信頼性を証明するのに有効である点やプライバシーマークのマーク付与認定団体である財団法人日本情報サービス産業協会に加入しているところが多い点等が考えられる。

金融業では、現時点で取得している企業は少ないものの、「取得を考えている」企業が 65%と多い。また、情報サービス以外では「知らない」が 2 割程度もある。

Q12. お客さまからアクセスがある際にお客さまが再度そのサイトに訪れたとき、通信履歴データをサーバー側で認識し、利用者の手続上の再入力等を省くことができるクッキーというしくみを利用していますか？（有効回答会社数 = 97社）

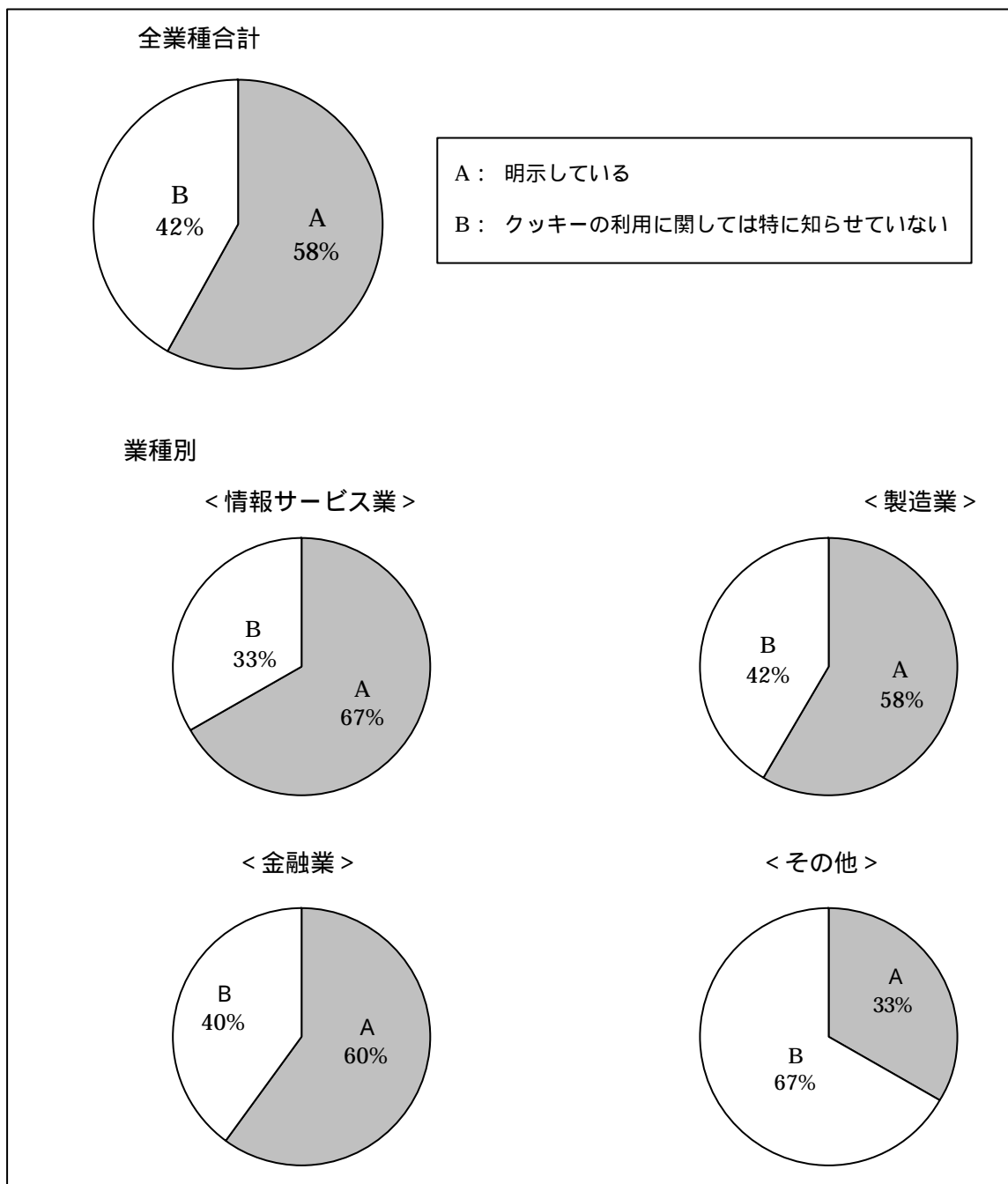


図表 3-2-14

全体では、32%がクッキーを利用している。特に金融業界では72%と利用率が高く、次

に製造業が 41%と続く。情報サービス業では利用はわずか 17%で、逆に 7 割近くは利用していない。

Q13. (上記 A の回答者のみ) クッキーを利用していることと、その利用目的を明示していますか? (有効回答会社数 = 31社)

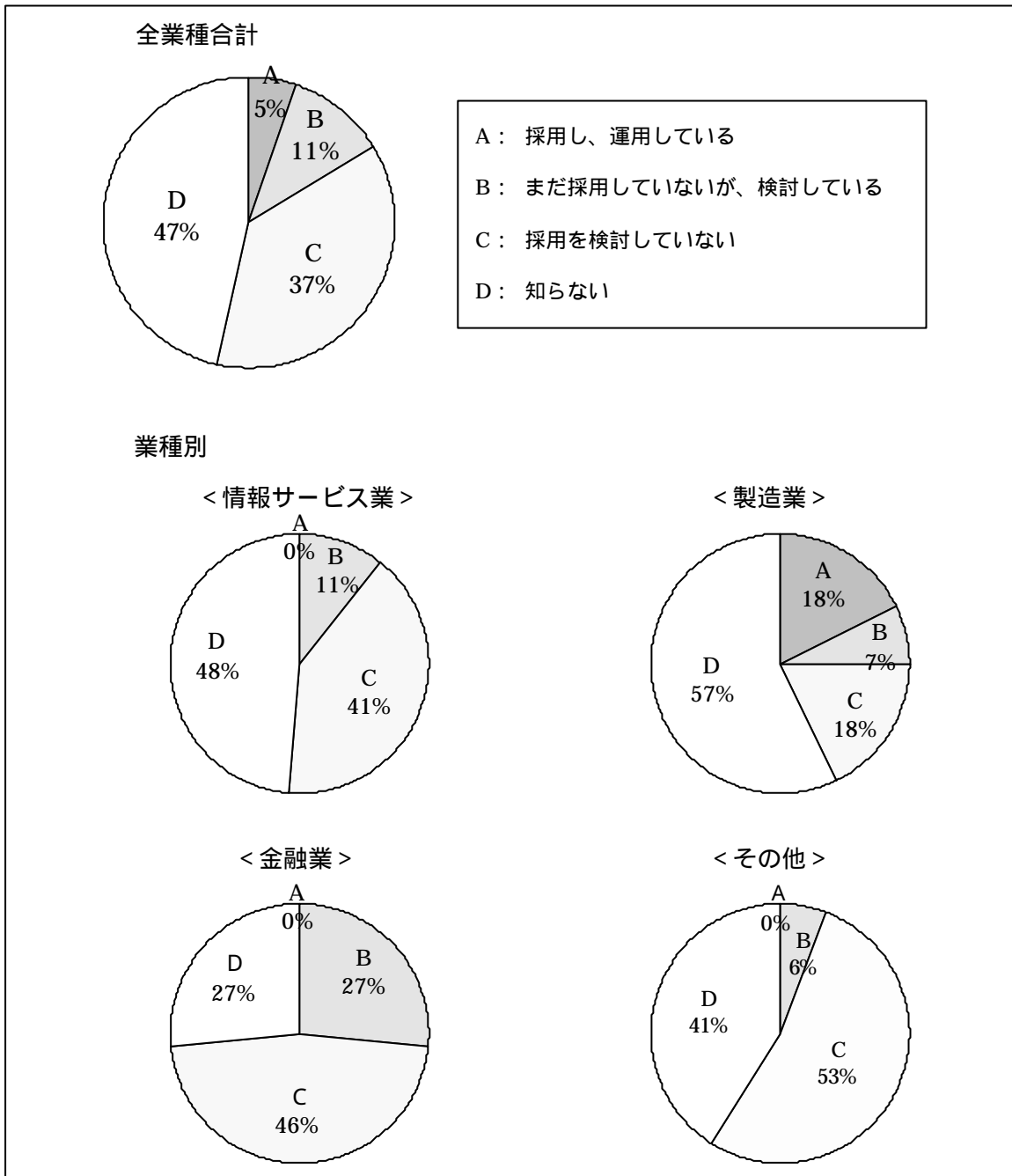


図表 3-2-15

クッキーを利用する会社のみでの回答のためサンプル件数が 30 件と少ないが、全体では、

明示しているが 6 割程度である。

Q14 . 「 P 3 P (Platform for Privacy Preferences) 」 という個人情報保護のレベルについてユーザー - 事業者間で自動的に確認できる技術規格がありますが、それについて (有効回答会社数 = 97 社)



図表 3-2-16

P 3 P については、2002 年 4 月に標準仕様が公開され、今後の普及が期待されるものが、

本アンケート実施時点で、「採用している」が 5%・「検討している」が 11%との結果であった。したがって、「採用を検討していない」「知らない」が 8 割を超え、今後の更なる利用環境の整備や普及啓発が必要であると考えられる。

3.2.4 まとめ

以上のように、本年度、E C O M 個人情報保護WGとして初めての試みで会員企業・団体を対象に個人情報保護に関するアンケートを実施したところ、結果的に約 3 割の 97 社より回答をいただき、趨勢を類推・分析することができた。

日本企業全体の個人情報保護実態を掌握したこのような調査は多くなく、他の機関・団体・グループ等の行った小規模な調査結果との比較に限定されるため、大方は分析者の感覚に頼ることになっている。

しかしながら、E C O M が電子商取引およびインターネットビジネスに関連ある民間の任意団体であり、情報サービス、情報通信、電気機器・精密機器・自動車等の製造業全般、金融・保険、流通、物流、マスコミ・出版、シンクタンクといった広範な業界に及ぶ企業が参加していることを考えるとある意味での縮図的な傾向を掌握できるものとする。

今後、他の方法で裾野広い E C 事業者を対象とする実態調査の方法を考案するとともに、本調査について定点観測として継続的に調査分析・趨勢掌握するものとして、会員企業・団体の皆様の引き続きのご理解とご協力を賜りたい。

3.3 ECOM会員企業・団体WEBページ個人情報保護表記目視調査

3.3.1 調査概要

1. 調査方法：会員のホームページ検索
2. 調査日程：2002年6月12日～18日
3. 調査数：278社
4. 調査結果

	調査企業・団体数	プライバシーポリシー		取得	プライバシーマーク	
		トップページにリンクボタン表記	サイト内に表記		トップページにマーク表示	サイト内に表示
理事会員	35	15	3	9	1	5
		18			6	
正会員A	88	35	5	17	11	3
		40			14	
正会員B	155	41	7	21	10	5
		48			15	
合計	278	91	15	47	22	13
		106			35	

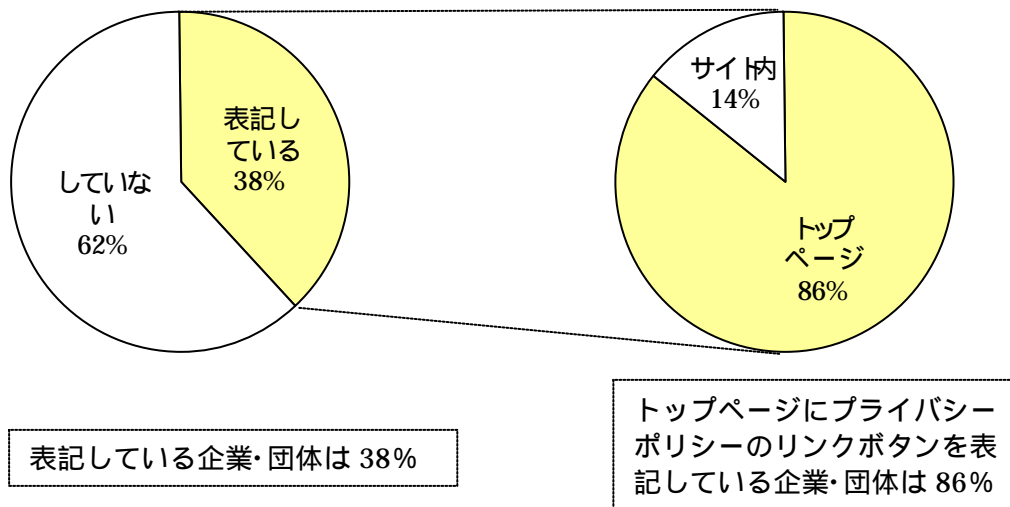
図表 3-3-1

3.3.2 調査および分析

(1) プライバシーポリシーについて

ホームページ上に表記している
企業・団体

内トップページにリンクボタン
を表記している比率



図表 3-3-2

アンケート調査のQ10にて実施した「プライバシーポリシー」「個人情報保護方針」のHPトップ掲載の結果と見比べ、結果としては整合が取れていると考えられる。即ち、アンケートにて回答いただいた件数は本目視調査に対して約1/3の件数であり、約50社相当が掲載していることになり、本調査において116社が表示している内数となることとなる。

約4割弱のこの結果は、日本企業の実態として概ねのイメージに合致するもののアメリカではWeb上でよく見られる9割の企業がプライバシーポリシーを掲載していることと比較するとさらに奨励・啓発することが必要と考えられる。

トップページにリンクボタンを表示している会員企業・団体一覧

会社 団体名		会社 団体名	
1	川鉄情報システム株式会社	46	富士通エフ・アイ・ピー株式会社
2	東京電力株式会社	47	PWC コンサルティング株式会社
3	株式会社東芝	48	三井住友カード株式会社
4	日本アイ・ピー・エム株式会社	49	株式会社UFカード
5	日本電気株式会社	50	株式会社ローソン
6	日本ユニシス株式会社	51	アメリカン・エキスプレス・インターナショナル・インコーポレイテッド
7	株式会社野村総合研究所	52	アンリツ株式会社
8	ビザ・インターナショナル	53	イオンクレジットサービス株式会社
9	株式会社日立製作所	54	株式会社インテリジェントウェイブ
10	富士通株式会社	55	株式会社エクサ
11	株式会社富士総合研究所	56	NECネクサソリューションズ株式会社
12	マイクロソフト株式会社	57	NTTコムウェア株式会社
13	マスターカード・インターナショナル・ジャパン・インク	58	イヌ・ティ・ティ・ソフトウェア株式会社
14	三菱電機株式会社	59	株式会社オーグス総研
15	株式会社UF銀行（旧 三和銀行）	60	オムロン株式会社
16	株式会社アイネス	61	カシオ計算機株式会社
17	アクセンチュア株式会社	62	キヤノン株式会社
18	株式会社アルゴ21	63	株式会社構造計画研究所
19	RSAセキュリティ株式会社	64	小林記録紙株式会社
20	株式会社SRA	65	株式会社さくらケーシーエス
21	NECソフト株式会社	66	株式会社シーエーシー
22	株式会社NTTドコモ	67	株式会社資生堂
23	イヌ・ティ・ティ・コミュニケーションズ株式会社	68	株式会社ジャックス
24	NTTコムウェア株式会社	69	株式会社ジャルカード
25	株式会社FFC	70	ソラン株式会社
26	株式会社オリエントコーポレーション	71	株式会社ソリトンシステムズ
27	共同印刷株式会社	72	株式会社第一勧銀情報システム
28	近畿日本ツーリスト株式会社	73	株式会社ティージー情報ネットワーク
29	グローバルフォーカス株式会社	74	株式会社電通国際情報サービス
30	KDD 株式会社	75	東京通信ネットワーク株式会社
31	国内信販株式会社	76	東芝テック株式会社
32	コンピュータ・アソシエイツ株式会社	77	東芝ファイナンス株式会社
33	株式会社シー・アイ・シー	78	TIS株式会社
34	株式会社テブコシステムズ	79	トッパン・フォームズ株式会社
35	東北電力株式会社	80	株式会社日本システムディベロップメント
36	ニフティ株式会社	81	株式会社BSNアイネット
37	日本アビオニクス株式会社	82	株式会社フジサンケイリビングサービス
38	株式会社日本総合研究所	83	株式会社富士通長野システムエンジニアリング
39	日本電子計算機株式会社	84	株式会社富士通北陸システムズ
40	日本電信電話株式会社	85	ブラザー工業株式会社
41	日本ユニシス情報システム株式会社	86	株式会社ペイメント・ワン
42	ノキア・ジャパン株式会社	87	マイトリップ・ネット株式会社
43	東日本電信電話株式会社	88	ミノルタ株式会社
44	株式会社日立情報システムズ	89	ヤマトシステム開発株式会社
45	日立ソフトウェアエンジニアリング株式会社	90	横河電機株式会社
		91	株式会社菱化システム

図表 3-3-3

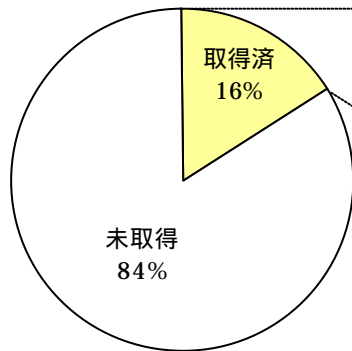
サイト内にはあるが、トップページにリンクボタンのない会員企業・団体一覧

会社 団体名	
1	株式会社NTTデータ
2	日本信販株式会社
3	松下電器産業株式会社
4	新日鉄ソリューションズ株式会社
5	セイコーエプソン株式会社
6	セコム株式会社
7	ソニー株式会社
8	日本オラクル株式会社
9	キヤノン販売株式会社
10	ダイセル化学工業株式会社
11	中国情報システムサービス株式会社
12	富士写真フイルム株式会社
13	富士ゼロックス株式会社
14	富士通ソーシャルサイエンスラボラトリ
15	横河トレーディング株式会社

図表 3-3-4

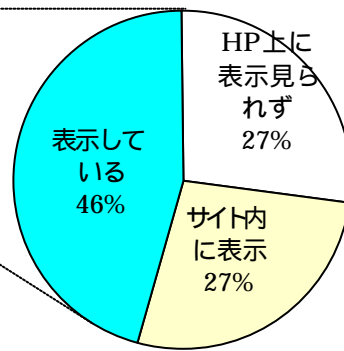
(2) プライバシーマークについて

プライバシーマークを取得している
会員企業・団体の比率



図表 3-3-5

トップページにプライバシーマークを
表記している企業・団体



図表 3-3-6

2003年3月時点でプライバシーマーク取得会社は468社であり、この1年で160社と大きく増えた。本調査時点では330社程度であったが、本調査対象のうちの16%、47社が取得しているのはECOM会員企業の意識の高さを物語るものと言えよう。なお、本調査後、ECOM会員企業の取得はさらに増え、2003年3月現在では59社にのぼる。

プライバシーマークを取得している企業・団体一覧

会社・団体名		会社・団体名	
1	株式会社NTTデータ	25	富士通エフ・アイ・ピー株式会社
2	川鉄情報システム株式会社	26	三井住友カード株式会社
3	株式会社東芝	27	株式会社インテージ
4	日本電気株式会社	28	株式会社インテリジェントウェイブ
5	株式会社野村総合研究所	29	株式会社エクサ
6	株式会社日立製作所	30	NECネクサソリューションズ株式会社
7	富士通株式会社	31	エヌ・ティ・ティ・ソフトウェア株式会社
8	株式会社富士総合研究所	32	オムロン株式会社
9	松下電器産業株式会社	33	キーウェアソリューションズ株式会社
10	株式会社アイネス	34	株式会社構造計画研究所
11	株式会社アルゴ21	35	小林記録紙株式会社
12	株式会社SRA	36	株式会社さくらケーシーエス
13	NECソフト株式会社	37	株式会社シーエーシー
14	NTTコムウェア株式会社	38	ソラン株式会社
15	共同印刷株式会社	39	株式会社第一勧銀情報システム
16	グローバルフォーカス株式会社	40	中国情報システムサービス株式会社
17	新日鉄ソリューションズ株式会社	41	株式会社電通国際情報サービス
18	株式会社セゾン情報システムズ	42	東芝情報システム株式会社
19	大日本印刷株式会社	43	トッパン・フォームズ株式会社
20	株式会社テブコシステムズ	44	マイトリップ・ネット株式会社
21	株式会社日本総合研究所	45	ヤマトシステム開発株式会社
22	日本ユニシス情報システム株式会社	46	株式会社菱化システム
23	株式会社日立情報システムズ	47	株式会社両毛システムズ
24	日立ソフトウェアエンジニアリング株式会社		

図表 3-3-7

プライバシーマークをトップページに
表記している企業・団体一覧

会社・団体名	
1	株式会社富士総合研究所
2	株式会社アイネス
3	株式会社SRA
4	NECソフト株式会社
5	グローバルフォーカス株式会社
6	株式会社セゾン情報システムズ
7	株式会社テブコシステムズ
8	株式会社日本総合研究所
9	日本ユニシス情報システム株式会社
10	日立ソフトウェアエンジニアリング株式会社
11	富士通エフ・アイ・ピー株式会社
12	三井住友カード株式会社
13	NECネクサソリューションズ株式会社
14	株式会社さくらケーシーエス
15	ソラン株式会社
16	株式会社第一勧銀情報システム
17	中国情報システムサービス株式会社
18	株式会社電通国際情報サービス
19	東芝情報システム株式会社
20	マイトリップ・ネット株式会社
21	ヤマトシステム開発株式会社
22	株式会社菱化システム

図表 3-3-8

サイト内に表記している企業・団体
一覧

会社・団体名	
1	株式会社NTTデータ
2	株式会社東芝
3	株式会社野村総合研究所
4	株式会社日立製作所
5	松下電器産業株式会社
6	株式会社アルゴ21
7	NTTコムウェア株式会社
8	新日鉄ソリューションズ株式会社
9	株式会社エクサ
10	オムロン株式会社
11	株式会社構造計画研究所
12	小林記録紙株式会社
13	株式会社シーエーシー

図表 3-3-9

4 ECOM個人情報保護ガイドラインの改定検討

4.1 ガイドライン改定検討経緯

4.1.1 2001年度の検討

昨年度は2度のヒアリングとWG会議においての全体検討を通じて、「中間整理案」のレベルまでまとめたものの、最終的にWG内の合意をとるレベルまでに至らず、発表を見合わせた。そのときの懸案は以下のとおりである。

1. 本人からの個人情報の収集について、法案とのレベルの整合を鑑みた場合、「同意」とするか、「通知または公表」とすべきかの論点がある。
2. ガイドラインとしての法案とJISとの位置付けについて明確にすべき。
3. 個別の条項に関してまだ解釈の根拠の不明確な点が存在。

4.1.2 2002年度検討概要

本年度は5月8日の「ガイドライン改定再検討会議」を皮切りに7回のWG会議、4回のキーマン・ディスカッション（オピニオン・リーダー検討会等含む）を開催し、その後でアドバイザーの方々との度重なる検討ミーティングを実施した。

4.1.2.1 ガイドライン改定再検討会議

昨年度の懸案については、今年度WG活動をキックオフする前の上記「ガイドライン改定再検討会議」にて基本スタンスを以下のように定めた。

（基本スタンス）

個人情報を取り扱う事業者に対し、電子商取引（EC）における個人情報保護の指針を示す。

1. 主に電子商取引（EC）の場面に照準をあて、EC事業者のとるべき対応を示す。
2. 法案で表されきれていない、具体的な方策や基準、事例等をあげ、わかりやすく示す。

これは基本的に民間の任意団体であるECOMの個人情報保護WGとしてこの個人情報保護法案を支持するとともに、その法案が民間に対して期待する自主的な取組みとして電

子商取引の切り口で、それに携わる事業者に対して適切な措置や運用体制構築および意識浸透を支援するものとして本ガイドラインを改定するというものである。

従って、条件設定および措置レベルや語句表記等については、原則として法案をベースとしながらも、運用体制や細かな措置については JIS Q 15001 等を参照にし、中間整理案から大きく内容および構成を変更する作業に取り掛かることとした。

電子商取引（EC）の場面に照準を当てた事業者のとるべき対応、具体的な方策、基準および事例等についてはWGの前後にて委員およびアドバイザーの中より有志メンバーに集まっていたき、「キーマン・ディスカッション（オピニオン・リーダー会議）」を開催することとした。

4.1.2.2 WG会議における検討

WG委員およびアドバイザー全員が出席するWG会議においては、ガイドライン改定案を逐次配布し、全員でチェックし、課題点等はメーリングまたは事務局に報告いただいた。

本年度のWG会議の開催とその中でガイドライン改定についての検討は以下のとおり。

5月8日 ガイドライン改定再検討会議

1. 前提のコンセンサス ECの概念・対象・場面等（条件設定および措置レベルや語句表記等の確認）
2. 法案とガイドラインのレベルの比較・構成等
3. 法案で示されていない具体的な方策・事例・基準の検討
4. 「通知」「公表」と「同意」の考え方
5. 再検討のスケジュール 他

5月29日 第1回個人情報保護WG会議

1. 全体構成の変更点
2. ガイドライン改定作業における条文構成の推移
3. 内部規定・方針・計画の変更
4. 直接取得・間接取得についての変更
5. 全文に記すポイント等

6．スケジュール検討

6月27日 第2回個人情報保護WG会議

- 1．経済産業省 商務情報政策局 情報政策課 江崎総括補佐のご説明
- 2．E C O M個人情報保護ガイドライン Ver.2.0（原案）提示
- 3．スケジュール検討

7月30日 第3回個人情報保護WG会議

- 1．E C O M個人情報保護ガイドライン Ver.2.0（第2案）提示 + 修正表
- 2．スケジュール検討

10月8日 第4回個人情報保護WG会議

- 1．E C O M個人情報保護ガイドライン Ver.2.0（第3案）提示 + 修正表
- 2．E C O M個人情報保護ガイドライン Ver.2.0< 版>について
- 3．スケジュール検討

12月11日 第5回個人情報保護WG会議

- 1．E C O M個人情報保護ガイドライン Ver.2.0< 版>（最終案）提示 + 修正表
- 2．E C O M個人情報保護ガイドライン Ver.2.0< 版>検討
- 3．スケジュール検討

2月13日 第6回個人情報保護WG会議

- 1．最終検討
- 2．機微な個人情報に関する規定の検討
- 3．スケジュール検討

4.1.2.3 キーマン・ディスカッション（オピニオン・リーダー会議等含む）

電子商取引（E C）の場面に照準を当てた事業者のとるべき対応、具体的な方策、基準および具体事例等の詳細について委員およびアドバイザーの中より有志メンバーに集まっていたいただき、「キーマン・ディスカッション（オピニオン・リーダー会議）」のなかで検

討を重ねた。

5月27日 第1回 キーマン・ディスカッション

1. 個人情報保護取扱事業者のために明確にする必要のある事項についての検討
2. 論点整理

7月18日 第2回 キーマン・ディスカッション

1. 全体構成について
2. 解説
3. 定義
4. 運用（通知・公表、明示、同意）/ 利用目的の変更と目的外利用 / 第三者提供と委託、共同利用判断 / 第三者提供について望ましい措置
5. 語句
6. リリースのタイミング

10月3日 法案と事業者における措置検討会議

1. 電子商取引のシーン（場面・行為）と妥当な対応・手続きについて

10月29日 第3回 キーマン・ディスカッション（オピニオン・リーダー会議）

1. ガイドライン最終案まとめ検討
2. 論点最終検討

以上のように、ほぼ年間を通じて、法案をベースとしたガイドライン改定の議論が続けてきたが、法制化される個人情報保護法が最終的にどのような形になるか見通せないことと、利用目的の特定とその具体的措置についてどのように、どの程度まで特定すべきか、顧客サービスのための顧客情報の提示は第三者提供・共同利用・委託のいずれに該当するか、名刺等より得られる得意先情報を基に作る顧客データベースの利用についてはどのような措置が必要か、社内従業員のリストを他社に提供する場合の第三者提供においてどのような措置が必要か、および、特定の機微な個人情報の取扱いについての考え方、等WGにて継続検討すべき事項が残されているため、本来、「ECOMガイドライン

Ver.2.0」として本年度中のリリースを目指してきたが、結論として、本年度末時点での検討途中経過を整理したものとして本報告書に掲載することとした。

4.2 ECOM個人情報保護ガイドライン改定案 (Ver.1.5)

はじめに

電子商取引推進協議会（以下「ECOM」という。）、NTTデータ経営研究所、経済産業省による「平成13年度電子商取引に関する市場規模・実態調査報告書」の調べでは、2001年のBtoC（Business to Consumer）の電子商取引の市場規模は1兆4,840億円となり、2000年の8,240億円に対し1.8倍と、ほぼ倍増に近い成長を遂げている。1999年から2000年にかけて、2.5倍の拡大を遂げたのと比べ、伸び率はやや低下したものの今後も引き続き大幅な成長が続くものと考えられ、2006年には16兆円に及ぶと見られている。

このように電子商取引が急速に普及する一方で、その利用に対する懸念や不安は依然として存在し、その中でも、個人データの漏洩や盗難、改ざん・なりすまし等の悪用は、電子商取引を利用する上での最大の懸念事項としてあげられる。2000年及び2002年に実施したECOMの調べでは、自己データの漏洩が電子商取引の不安・短所の第1位となっており、また、昨今、企業・団体の管理する個人データがインターネット上に漏洩する等の事件が相次いで発生している。

一方世界に目を向けると、1980年に経済協力開発機構（以下「OECD」という。）で「プライバシー保護と個人データの国際交流についてのガイドラインに関する理事会勧告」（以下「OECDガイドライン」という。）で個人情報保護のための8原則が掲げられて以降、80-90年代にかけて、各国で個人情報保護法の制定やプライバシー保護の自主規制等の整備がなされてきた。

欧州連合（以下「EU」という。）は、1995年、その加盟国に対し、指令採択の日より3年以内にそれを遵守する法律・規定を定めることとし、更に、個人データを移転できるのは十分な保護レベルにある国に限るとした指令（「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欧州議会及び理事会の指令」、以下「EU指令」という。）を発した。

米国ではセグメントごとに自主的規制や個別法が制定され、EU指令に対しては「セーフハーバー原則」により個人情報についての十分なレベルの保護を施す措置が図られてい

る。

日本では、1988年に「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」が制定されているが、民間分野においては、1997年、通商産業省（現・経済産業省）より発表された「民間部門における電子計算機処理に係る個人情報の保護に関するガイドライン」（以下「通産省ガイドライン」という。）をベースに業界ごとのガイドラインや自主規制の下に個人情報保護の取組みがなされてきた。

その前後で、高度情報通信社会の構築に向けた施策が総合的に推進される中、個人情報保護に対する法制化の必要性が更に強く認識され、2001年3月、「個人情報の保護に関する法律案」（以下「個人情報保護法案」又は「法案」という。）が国会に提出された。（2002年4月より審議入りしたが2002年12月一旦廃案、2003年3月修正案再提出。）

本法案では、法制化の目的を「個人の権利利益を保護すること」としつつも、「個人情報の有用性に配慮」することにも言及し、両者の適正なバランスが求められている。

ECOMでは、既に1998年、前述の通産省ガイドラインを参考に、「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」（以下「ECOMガイドライン1.0版」という。）を発表している。これは、電子商取引の健全なる普及と発展のため、事業者の適正な個人情報保護のための自主規制の指針を示すとともに消費者の電子商取引の利用に対する不安や懸念を少しでも払拭することを目指したものである。

今般、個人情報保護法案が提出されたことを受け、企業における個人情報保護への体制構築を早急に進めることが電子商取引に携わる事業者の緊急のテーマと考え、他の業界や団体に先んじて「ECOMガイドライン1.0版」を改訂することとした。

基本的に個人情報保護法案に対応し、事業者に対して電子商取引における個人情報保護の指針を示した。すなわち、電子商取引の場面に照準をあてつつ、事業者としてとるべき対応を示し、また、法案に表されていない具体的な方策や基準を事例等盛り込みながら、わかりやすく解説するものとしてまとめた。

なお、ここでいう電子商取引の概念としては、「インターネット等の情報ネットワーク上で、商取引及びそれを誘引するための宣伝・広告、その他の事業活動の一部又は全部を行うこと」と定義し、契約や取引に関わる商行為だけに限定せず、宣伝・広告という契約の誘引に当たる行為やその他の事業活動についてインターネット等の情報ネットワークより個人情報を取得し、利用する事業者全般に適用されるものとして策定した。

このガイドラインがそうした事業者に幅広く参照され、個人情報が適正に取扱われるこ

とにより、電子商取引がより多くの消費者及び事業者に安心して利用され、日本の高度情報通信社会の中で健全に普及していくことを切に希望する。

第1章 ガイドラインの目的

(目的)

第1条 このガイドラインは、個人情報を取り扱う事業者に対し、電子商取引における個人情報の保護に関する指針を示すことにより、インターネット等の情報ネットワーク上の個人情報の有用性と個人情報の保護の必要性との調和を保った適正な商慣行を形成し、もって高度情報通信社会の健全な進展に寄与することを目的とする。

(解説)

1. 電子商取引の健全な発展のためには、電子商取引において個人情報を取り扱うすべての企業や個人事業者が、消費者をはじめとする個人情報を適切に保護する必要がある。
2. 一方でOne to One マーケティングやCRM (Customer Relationship Management) に代表されるように個人情報はその業務において積極的に活用されている。このガイドラインでは、事業者に対し、顧客に対するサービスや利便性の向上あるいは事業拡大や業務効率向上を図る上で有効に個人情報を利用しながらも、個人の権利利益を適切に保護することを求めている。そして、それらをバランスよく調和させることにより電子商取引がさらに健全に普及し、高度情報通信社会の進展につながるものとする。
3. 法案においても高度情報通信社会の進展の上で個人情報の有用性に配慮した個人の権利利益を保護することが目的と表されており、その精神は本ガイドラインと一致するものである。

参考 法案第1条

(適用範囲)

第2条 このガイドラインは、個人情報の全部又は一部をインターネット等の情報ネットワークによって取り扱う事業者に適用できる。

- 2 事業者は、自社にて個人情報を取り扱う際の基準又は自社の個人情報保護に関する規定を策定する際等の参考としてこのガイドラインを用いることができる。

(解説)

1. このガイドラインは、事業や業務の一部にインターネット等の情報ネットワークを利用して個人情報取得し、又は利用する事業者を対象とする。
2. 事業者は、次の事項を行うときに、このガイドラインを用いることができる。
 - (1) 自社の個人情報の取扱いについて、適切に行われていることを確認するとき。
 - (2) コンプライアンス・プログラム又はそれに代わる個人情報保護体制を構築するとき。
 - (3) このガイドラインとコンプライアンス・プログラム又はそれに代わる個人情報保護体制による推進が適合しているかを確認し、適合していることを自ら表明するとき。

(定義)

第3条 このガイドラインにおける用語の定義は、当該各号に定めるところによる。

(1) 電子商取引

インターネット等の情報ネットワーク上で、商取引及びこれを誘引するための宣伝・広告、その他の事業活動の一部又は全部を行うことをいう。

(2) インターネット等の情報ネットワーク

電子商取引に限定されず、より幅広い業務や用途において利用されるインターネット等によるネットワークをいう。

(3) 個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

(4) 個人情報データベース等

個人情報を含む情報の集合物であって、特定の個人情報を電子計算機を用いて検索できるように体系的に構成したもの及び特定の個人情報を容易に検索できるように体系的に構成したものをいう。

(5) 個人データ

個人情報データベース等を構成する個人情報をいう。

(6) 保有個人データ

事業者が開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の

停止を行うことのできる権限を有する個人データをいう。

(7) 本人

個人情報によって識別される、又は識別され得る特定の個人をいう。

(8) 事業者

電子商取引又はインターネット等の情報ネットワーク上で個人情報を取り扱う法人
その他の団体又は個人をいう。

(9) 個人情報保護担当責任者

事業者の代表者によって指名された者であって、コンプライアンス・プログラム若しくはそれに代わる個人情報保護体制の実施・運用を行う責任者であって、個人情報の取扱いについて決定する権限を有する者をいう。

(10) コンプライアンス・プログラム

事業者が自ら保有する個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメント・システムをいう。

(解説)

1. 「電子商取引」については、契約に係る商行為だけに限定せず、宣伝・広告という契約の誘引に当たる行為等その他の事業活動全般についてもインターネット等の情報ネットワーク上で行われる場合には、これに含めることとし、広くとらえている。すなわち、アンケート、抽選、懸賞への応募等により取得した個人情報や新製品やイベントの案内、マーケティングのために取り扱われる個人情報等についてもその対象としている。
2. 「インターネット等の情報ネットワーク」は上記の電子商取引の概念を一般的にイメージできる語句としてこのガイドラインを通じて使用している。前項に示すようにインターネット上で電子商取引が行われるネットワーク環境もそれに該当するが、BtoCだけでなく、B to B (Business to Business)におけるクローズドなユーザー間で使うエクストラネット、イントラネット等も含む。また、採用募集や雇用関連等の場面でもこのような経路で個人情報を取得する場合があります、それら全般を含むものとして表現している。
3. 「個人情報」に関する定義については基本的に法案に準拠することとした。法案では「個人情報データベース等」として(1)特定の個人情報を電子計算機を用いて検索することができるように構成したもの、(2)その他、特定の個人情報を容易に検索できるように体系的に構成したものとして政令で定めるもの、の2点が個人情報を含む情報の集合物として定義づけられ、それらを

構成する個人情報を「個人データ」としている。さらにそのうち、企業が開示、内容の訂正、追加又は削除、利用停止、消去及び第三者への提供の停止を行うことのできる個人データを「保有個人データ」と定義している。ただし、その存否が明らかになることにより公益その他の利益が害されるものとして政令に定めるもの又は一年以内の政令で定める期間以内に消去することとなるものは「保有個人データ」から除外するとされている。

4. 購入履歴を基にした消費者個人の嗜好も識別性がある場合には「個人情報」に該当する。ただし、商品の売れ筋の把握や将来開発する商品のために行うマーケティング調査などの統計目的で個人を特定しないで取扱う情報や個人名を伏せ、匿名化して取り扱う情報はこれに該当しない。
5. 法案では前述のとおり「個人データベース等」の定義にマニュアル処理情報をどの程度入れるかは、政令にて定めるとしている。このガイドラインでは、マニュアル処理であっても、例えば医療カルテのように体系的に整理され、すぐに検索可能なもの、電子計算機に入力するために収集、保存されているものや宛名用に電子計算機から出力されたマニュアル処理情報等を「電子計算機処理を用いて検索できるように体系的に構成したもの」に相当すると考える。
6. 「保有個人データ」から除外されるもののうち、法案にある「その存否が明らかになることにより公益その他の利益が害されるものとして政令に定めるもの」は一般の企業においてそれに該当する個人情報データベースとして扱う可能性はほとんどないと思われる点より、除外事項からはずすこととした。同様に「一年以内の政令で定める期間以内に消去することとなるもの」についても、具体的に政令で一年より短い期間が定められるまでは除外事項よりはずすこととした。
7. ECOM ガイドライン 1.0 版では「情報主体」としていたが、法案に準じ、このガイドラインでは「本人」とした。
8. 電子商取引ではある程度の規模をもつ企業だけでなく、個人レベルで事業を営むケースも多いことから両者を総称する意味で「事業者」とした。このガイドラインを通じて、その適用対象である「個人情報の全部又は一部をインターネット等の情報ネットワークによって取扱う事業者」を指す。ちなみに法案では「個人情報取扱事業者」と記述されており、対象においては概ね差異はない。
9. ECOM ガイドライン 1.0 版では、「管理者」という用語で電子商取引において個人情報の収集、利用又は提供の目的及び手段等を決定する権限を有する者と定義されていた。このガイドラインでは「個人情報保護担当責任者」とし、ECOM ガイドライン 1.0 版と同じく個人情報の取扱いについて決定する権限をもつとともに、コンプライアンス・プログラムや個人情報保護体制の実

施・運用を行う責任を負う者とした。ある程度の規模をもつ企業においては、事業者の代表者によって指名されるが、個人事業者及び小規模事業者においては代表者自らがその任を負うこともある。ちなみに近年欧米の多くの大手企業及びIT関連企業においては「チーフ・プライバシー・オフィサー（CPO＝最高個人情報保護担当責任者）」が任命されている。

10. 「コンプライアンス・プログラム」は個人情報保護の実践と法的リスクの回避について体系的に全経営活動に統合されたマネジメント・システムである。

参考 法案第2条

第2章 内部規程・方針等

（内部規程・方針等の策定）

第4条 事業者は、個人情報を保護するための内部規程を策定し、その代表者は電子商取引の特性及び事業者の規模を考慮し、個人情報保護方針を定めるとともに、これを実行し、維持することとする。

（解説）

1. ある程度の規模の組織をもつ企業において個人情報保護を適切に行うためには、全社に通用する内部規程が必要となる。これを基に細則やコンプライアンス・マニュアル（各部門における業務について個人情報保護のための具体的対応を示す手順書）を策定し、社員全員が同じ行動を取ることができるような構成にしておく必要がある。内部規程に基本的に含まれるべき事項として(1)から(14)の内容が考えられる。

(1) 目的、適用範囲、定義に関する規定

その内部規程の目的、適用する業務範囲、使用する用語の定義の規定。

(2) 個人情報保護担当責任者及び管理体制に関する規定

個人情報保護を具体的に実施する為に社内管理体制を構築するにあたり、具体的に各担当者の役割、責任及び権限を規定する。

(3) 個人情報保護方針に関する規定

個人情報保護方針は個人情報保護の取組みを社内外に示す手段であり、その決定のプロセスや内容、公表の仕方等について規定する。

(4) 法令及びその他の規範の特定、個人情報の特定

事業者は自社の個人情報の取扱いに関わる業務について法令やそのための規範がある場合についてそれを遵守する必要がある。その為に法令及びその他の規範を特定し、かつそれを参照できる手順を定めた規定を設ける。また計画段階では、事業者が現段階で自ら保有するすべての個人情報を特定することが必要であるが、コンプライアンス・プログラム又はそれに代わる個人情報保護体制構築後においても新たに発生する業務やプロジェクト等に対応する必要から個人情報を特定するための手順を確立しておくことが重要である。

- (5) 個人情報の利用目的の特定、利用目的の制限、適正な取得、取得に際しての利用目的の通知等に関する規定

このガイドライン第6条から第15条までに従って規定されるべきである。

- (6) 個人データの内容の正確性の確保及び安全管理措置(情報セキュリティ)に関する規定

このガイドラインの第16条と第17条に従って規定されるべきである。

- (7) 従業員の監督、委託先の監督、及び第三者提供の制限等個人データの管理に関する規定

このガイドライン第18条から第23条までに従って規定されるべきである。

- (8) 情報管理技術及び個人情報保護管理技術の採用等に関する規定

事業者が取り扱う個人情報に関する具体的にリスクを明確にした上で、どのような情報管理技術及び個人情報保護管理技術の採用するかを決定するプロセスを規定する。

- (9) 保有個人データに関する事項の公表等及び保有個人データの開示、訂正等、利用停止等並びにその手数料等に関する規定

このガイドライン第24条から第30条までに従って規定されるべきである。

- (10) 苦情の処理等に関する規定

このガイドライン第31条に従って規定されるべきである。

- (11) 個人データの紛失、破壊、改ざん及び漏えい等が発生した時の対応並びにその是正措置に関する規定

事業者が取り扱う個人情報に関する具体的なリスクを明確にした上で、そのような事態が起こった時の対応及びその是正措置を規定する。

- (12) 個人情報保護に関する監査等に関する規定

このガイドライン第33条から第34条を参照して規定されるべきである。

(13) コンプライアンス・プログラム又はそれに代わる個人情報保護体制の見直しに関する規定

コンプライアンス・プログラム又はそれに代わる個人情報保護体制は、監査報告書及びその他の経営環境に照らして、最適な状況に維持されなければならない。そのためにコンプライアンス・プログラム又はそれに代わる個人情報保護体制の見直しに関する措置について規定する。

(14) 内部規程に違反した場合の罰則に関する規定

一般的に社員の就業規則における罰則の条項を適用するようにすれば良い。

2. 事業者の代表者は、内部規程に基づき、事業や業務の特性及び事業者の規模を考慮し、個人情報保護方針を定め、役員及び従業者に周知しなければならない。

(個人情報保護方針の公表)

第5条 事業者は、個人情報保護方針を外部向けに文書化し、公表することとする。

(解説)

1. 事業者は、一般の人がその企業の個人情報保護方針を入手・閲覧できるように、外部向けに文書化し、ホームページ等に公表することとする。文書化にあたっては、必要な事項と内容を選定し、一般にもわかりやすく表現するよう留意する。
2. 米国においては約9割の企業が個人情報保護方針をプライバシーポリシーまたはプライバシーステイトメントとしてそのホームページ上に表記しているといわれる。

第3章 運用

第1節 個人情報の取得等

(利用目的の特定)

第6条 事業者は、個人情報を取り扱うに当たっては、本人がその取扱いについての諾否を判断できる程度にその利用の目的(以下「利用目的」という。)を特定しなければならない。

- 2 事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(解説)

1. 法案第 15 条では、利用目的の特定が義務づけられている。そこではできる限り特定しなければならないとの表現にとどまっている。このガイドラインでは、「本人がその取り扱いの諾否に付いて判断をなし得る程度に利用目的を特定」することとした。どのくらいまでの特定が必要かは目的や取得する情報の性質、業界特性等により一律ではないが、曖昧かつ広すぎる利用目的では妥当でなく、事業者が最終的にどのような目的で利用するのかまで特定することが求められる。また、事業領域の広い事業者の場合、その業種やブランドについて本人から見て、その特定に資すると認められるかという点についても配慮することが必要であると考えられる。

また、第 2 項にて利用目的の変更について、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならないとしているが、その具体的な判断基準としては、事業者が取得した個人情報について目的を変更して利用するとき、本人がその利用について驚いたり 困惑したりしないような範囲で取扱われなければならない。

2. ECOM ガイドライン 1.0 版では、OECD ガイドラインの 8 原則に基づき、収集目的を明確に定め、その目的の達成に必要な限度において収集し、原則として情報主体(本人)が同意を与えた場合に利用できるとしていた。このガイドラインでは、法案に相応して、本条以降の運用に関する条項及びその対応の基準を改訂している。

参考 法案第 15 条

(利用目的による制限)

第 7 条 事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

2 事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

3 前第 2 項の規定は、次に掲げる場合については、適用しない。

(1) 法令に基づく場合

(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であつて、本人の同意を得ることが困難であるとき。

(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であつて、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(解説)

1. 一旦取得した個人情報について当初の利用目的の達成に必要な範囲を超えて取り扱うときには、本人にあらかじめ同意を得なければならない。
2. 「同意」については、本人が個人情報の取扱いに関する情報を与えられた上で自己に関する個人情報の取扱いについて承諾する意思表示をいう。本人から「私は同意した覚えがない。」と抗弁されないものでなければならず、本人の行為による署名、捺印、メールの送信、チェックボタンへのチェック、電子署名等であれば理想的であるが、黙示のものでもそれにあたるケースもある。
3. インターネット等の情報ネットワーク上で個人情報を取得するときは、利用目的を単にウェブ画面上で公表又は電子メールで通知するだけでなく、同意ボタンをクリックしたり、承諾の電子メールを返信してもらうなどの方法で、本人の明示的な同意を比較的容易に取ることができる。取得時の目的の範囲を超えた利用目的が考えられるときには、そのような方法を利用して本人の事前の同意を得ることが望ましい。
4. 本条第3項の事例としては、事故に遭った人が意識不明で連絡先が分からない時に、クレジットカードを持っていた場合、その人の連絡先を教えて欲しいという連絡が病院からカード会社にあった際、通常は本人の同意が必要であるが、意識不明で同意が取れないためカード会社が病院に対して連絡先を教えるケース等が考えられる。

参考 法案第16条

(適正な取得)

第8条 事業者は、偽りその他不正の手段により個人情報を取得してはならない。

(解説)

1. 個人情報の取得に際し、事業者は本人に対し、偽りや盗用、漏洩したデータ入手といった不正な手段を用いて取得してはならない。
2. インターネット等の情報ネットワーク上で個人情報を取得するときも同様に、なりすまし等自らを偽っての取得やネットワークを通じての盗用やハッキング等の不正な手段による取得をしてはならない。
3. 偽りその他不正な手段により取得した第三者から、そのことを知りつつ、間接的に取得してはならない。

参考 法案第 17 条

(取得に際しての利用目的の通知等)

第 9 条 事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を本人に通知し、又は公表しなければならない。

(解説)

1. 法案第 18 条第 1 項では、直接的・間接的に関わらず個人情報取得した時の措置としてあらかじめその利用目的を公表している場合を除き、速やかにその利用目的を本人に通知又は公表することが義務づけられている。
2. ECOM ガイドライン 1.0 版では本人から直接収集する場合及び本人以外から間接的に収集する場合についての措置を定めており、個人情報の収集、利用又は提供に関する同意を得ることを原則としていた。
3. 近年の電子的ネットワーク技術の急速な発展、多様化する消費者のニーズに対応するために個人情報を利用した事業活動が重要になっていることに伴い、個人情報は直接的に本人から取得される場合に加えて、本人以外から間接的に取得される場合も急激に増えてきている。このように本人の知らない間に当該個人情報が流通する際にも、本人の権利利益を侵害しないよう特に慎重に対応する必要がある。このガイドラインにおいては、本人以外から間接的に取得する場合を含めて、法案に準じ、原則的に本人に対し利用目的を通知又は公表することとする。
4. 公表の方法としては、新聞等のマスメディアへの掲載やパンフレットの作成・配布、店頭窓口への掲示、ホームページ上への掲載等があり、通知については、はがきや手紙、電話、電子メール等が考えられる。

参考 法案第 18 条第 1 項

(インターネット等の情報ネットワーク上などで本人より直接に取得する場合の措置)

第 10 条 インターネット等の情報ネットワーク上又は書面で本人より直接当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。

(解説)

1. 法案第 18 条第 2 項では、本人との間で契約書等の書面で個人情報を直接に取得する場合にあらかじめ本人に対しその利用目的を明示することを義務として課している。このガイドラインでも、第 9 条で個人情報取得時の原則的な措置を定めた上で、とりわけインターネット等の情報ネットワーク上で本人より直接当該本人の個人情報を取得する場合等の措置としてあらかじめ本人に対しその利用目的を明示することと定めた。
2. 明示とは、具体的には契約書やアンケート用紙に個人情報の利用目的を記載したり、インターネット等の情報ネットワーク上においては、ユーザー入力画面やユーザー宛メールに表示又は明記したりすることが相当する。方法は問わないものの本人からまったく気づかなかつたと言われないように配慮すべきである。
3. 例えば、アンケート等により取得する個人情報を基にイベントや新商品等の情報の案内通知を行うことについて、消費者は記入又は入力する際にそこまでの認識をしていない場合があるので、そのようなダイレクトメールを発信することを予定している場合は事前に消費者に明示しなければならない。
4. 電子商取引の場面では、電子契約法により、ホームページ上で消費者が申し込みを行う前に契約内容等を確認する措置が無い場合、有効性を主張できないとされている。従って、契約の際には、併せて、個人情報についての利用目的を明示し、かつ、本人に対し個人情報の利用について了解の意思を確認するようにした方がよい。

参考 法案第 18 条第 2 項

(利用目的の変更時の措置)

第11条 事業者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

(解説)

1. 利用目的の変更についてホームページ上での公表や本人への電子メールでの通知等は比較的容易にとることができる措置である。その際、本来は再度本人からの同意をもらうことが望ましい。
2. 再度本人より明示的な同意を得ることが困難な場合でも、利用目的を変更することについて本人より利用停止等を求められることも考えられるので、ホームページ上で、又はメールの返信等により容易にそうした求めを受け付けられるようなしくみ(オプトアウトの手続き)をとることが望ましい。
3. 利用目的の変更については、本人が意外に思うことのない範囲で行われるべきものであり、当初の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて利用する場合は同意を得る必要がある。

参考 法案第18条第3項

(取得時及び利用目的等の変更時の措置の適用除外)

第12条 第9条、第10条及び第11条の規定は、次に掲げる場合については適用しない。

- (1) 利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- (2) 利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合
- (3) 国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。
- (4) 取得の状況からみて利用目的が明らかであると認められる場合

(解説)

1. 法案第 18 条第 4 項に上記の 4 項目について適用が除外される事項として記されている。
2. (1)から (3)における「おそれ」については事業者において判断されるにあたり、客観的な基準でなされなければならない。
3. 取得の状況から見て利用目的が明らかであると認められる場合とは、契約申し込みや商品の配送のためだけに住所や氏名等の記入により個人情報を取得するケース等である。

参考 法案第 18 条第 4 項

(インターネット等の情報ネットワーク上で自動的に個人情報を取得する場合の措置)

第 13 条 インターネット等の情報ネットワーク上でその付随する機能を用いて、本人から自動的に個人情報を取得することとなるときは、その事実と利用目的を通知し、又は公表しなければならない。

(解説)

1. インターネット上では本人の知らない所で個人情報が収集されている場合がある。特に、電子商取引の場面では、クッキーに代表される個人履歴情報収集技術を使って、
 - (1) 訪問者がそのページに何回訪れたかを記録したり、それを表示したりする。
 - (2) 通常モード、フレームモードなど、訪問者の好みを記録しておき、次回訪問時にその好みのモードで表示する。
 - (3) 掲示板やチャットで入力したユーザー名を記録しておき、次回訪問時にユーザー名の入力を省略する。といったことがすでに実施されている。これは本人の知らないところで、本人のパソコンのブラウザの中にクッキーが送信され、また、再度そのページに訪れた際、本人のパソコンより蓄積したクッキーのデータが事業者側のサーバーに自動的に提供される仕組みによるものである。
2. クッキー自体は必ずしも個人情報といえないこともあり、またその利用において個人情報として使わないこともあるが、個人を特定する形で利用するクッキーについてはその事実と利用目的を通知又は公表しなければならない。また、本人に対し安心感を与える意味で、クッキーを個人情報として利用しないケースでもその旨をわかりやすく示すことが望まれる。
3. 近年その利用が急増しているものの、クッキーの使用を明らかにしている事業者はそれほど多いわけではない。しかしながら、米国において無断でクッキー情報を収集し、第三者提供しようと

して問題になったケース等を考え合わせ、クッキーを使用している旨と利用目的について通知又は公表するべきとした。

参考 法案第 18 条

(特定の機微な個人情報の取得の禁止)

第 14 条 事業者は、次の各号に掲げる内容を含む個人情報を取得してはならない。ただし、本人に対し当該個人情報を取得する必要性について十分な説明を行った上で明示的に本人の同意を得た場合又は法令、その他規範に特別の定めがある場合は、この限りではない。

- (1) 思想、信条及び宗教に関する事項
- (2) 人種、民族、門地、本籍地(所在都道府県に関する情報を除く。)、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項
- (3) 勤労者の団結権の行使、団体交渉、その他団体行動に関する事項
- (4) 集団示威行為への参加、請願権の行使、その他の政治的権利の行使に関する事項
- (5) 保健医療及び性生活に関する事項

2 法令により使用を禁じられている個人情報は同意の有無に係らず取得してはならない。

(解説)

1. ECOM ガイドライン 1.0 では通産省ガイドラインを基とし、特定の機微な個人情報の取得を原則的に禁止している。ただし、本人に対し当該個人情報を取得する必要性について十分な説明を行った上で明示的に本人の同意を得た場合、又は法令に特別の規定がある場合は、この限りではないとする。
2. 通産省ガイドラインは、適用の対象として、顧客等の個人情報保護に関する取扱いについて定めるものとし、その企業の従業員の人事管理、福利厚生のために保有する個人情報(いわゆる「インハウス情報」)については、適用の直接の対象としているものではないとしているが、当然ながら従業員のプライバシーに十分配慮した取扱いが行われるべきとも付け加えている。
3. このガイドラインでは、法案と同様に顧客等の個人情報だけに限定せず、インハウス情報も適用の対象となる。しかしながら、プライバシーの観点より、ECOM ガイドライン 1.0 と同様に本人の権利の適切な保護のために、特に本人にとってセンシティブな情報の内容を明確にし、安易

な取得を制限することとする。表記については、その後さらに整理された JIS Q 15001 のものをベースに採用する。

4. 例えば、電子商取引では本人確認が重要視されるので、「本籍地」については取引に必要な場合には、本人を証明するために情報を提供させることがあり得る。所在都道府県を超える情報を取得する場合は、本人確認の必要性が高度であって、かつ安全対策措置を十分にとっている場合に限り、本人の同意を得た上で、取得することが許される。なお、取得した「本籍地」情報を第三者に提供したり、本人確認以外に利用することは認められない。
5. インターネットで医療相談を行う場合も、本人の明確な同意を得るべきである。また、本人の健康に限らず配偶者、父母、兄弟姉妹等の病歴及び現在の健康状況についても同様である。
6. 住民基本台帳法の改正により運用の始まった「住民票コード」のように法令により使用を禁止されているものは取得してはならない。
7. 法案では高度情報通信社会において、個人情報はそのマッチングによりいくらかでもセンシティブになりうるので、情報の性質により特定できるものではないとの解釈のもと、特定の機微な個人情報についての条項が設けられていない。従って、この条項の掲載および表記等については、法制化の動向および関連する規範の見直し等を見ながら、今後も引き続き検討を重ねることとする。

(子どもから個人情報を取得する場合の措置)

第15条 事業者は、子どもから個人情報を取得する場合には、子どもが理解できる平易な表現で利用目的を明示するものとする。また、子どもに個人情報の入力を求める場合は、保護者の了解を得るように促すものとする。

(解説)

1. パソコンの操作性の向上に伴い、子どもでも簡単にインターネット等の情報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、例えば、子どもに人気の高いゲーム等を景品に子どもから、子ども自身や保護者の個人情報を取得する事例が生じている。子どもは必ずしも個人情報の取得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を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。例えば、情報の提供はあくまでも任意で、必ずしも必須ではない場合には、「名前を入れなくてもゲームはできます。」などはっきり知らせなければならない。

2. 子どもやその保護者が、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、「子どもに個人情報の入力を求める場合」は、取得する前に保護者に事情を説明し、了解を得る機会を与え、より配慮する必要がある。
3. 「子ども」は、取扱う商品やサービスにより、対象となる年齢層が定まる。「JIS」では一般に12歳から15歳までの年齢以下を対象としている。事業者は、それらを参考にし、かつ個人情報を取り扱う業務の内容を考慮し、対象となる「子ども」の年齢を定める。

第2節 個人データの管理

(個人データの正確性の確保)

第16条 事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

(解説)

1. 「最新の内容」については、利用目的に応じ必要な範囲内で更新するものであるから、単発的な取引が完了した本人について、更新しないことで本人に不利益が生じない場合等のように情報を最新のものに変更しなくてもよいケースもある。ただし、利用目的に応じて必要な範囲で改めて取得した情報によってこれまでの情報に変更がある場合は、最新の情報に更新しなければならない。「最新の内容」にするために事業者が積極的に探知又は調査することまで求めるものではない。事業者が積極的に探知等することにより、むしろプライバシーを侵害することもありうるので注意を払う必要がある。

参考 法案第19条

(安全管理措置)

第17条 事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理(情報セキュリティ)のために、その規模に応じた必要かつ適切な措置を講じなければならない。

(解説)

1. 安全管理措置について、基本的には下記の事項について合理的な措置を講じる必要がある

る。

- (1) 入退室管理に関する事項。
 - (2) アクセス管理(ウイルス防止含む)に関する事項。
 - (3) データ管理(バックアップ、保管、廃棄等)に関する事項。
 - (4) 委託処理に関する事項。
2. また、事業者の規模に応じて、JIPDEC(財団法人日本処理開発協会)の認定する「ISMS認証基準(ISO/IEC17799:2000)」や経済産業省(旧通産省)の「コンピュータウイルス対策基準」(平成7年7月7日告示第429号)「コンピュータ不正アクセス対策基準」(平成8年8月8日告示第362号)等を参照し、セキュリティについて技術面、管理面の対策を講じることもできる。
3. ネットワーク環境が整備されたことにより、従来に比べ、企業外へのデータ持出しが容易になっている。したがってフロッピーディスクやCD-ROMなどの可搬的な媒体の保管や取扱いは勿論、電子メールや外部のホームページへのアクセスについても、必要な範囲で制限等を設ける必要がある。
4. また、外部からのサーバー内への不正な侵入やアクセスも増加傾向にあり、アクセス制御やユーザー認証、ファイアウォール等ネットワークセキュリティを施すことが望まれる。
5. ホームページ上にて本人より個人情報を入力してもらう場合には、SSL(Secure Socket Layer)など技術的手段を用いて、暗号化することが望ましい。
6. 特に、インターネット等公衆回線上のネットワークを使用して、保有する個人データを送信することは原則として行うべきではない。やむなく送信しなければならないときには、通信路についてはVPN(Virtual Private Network)を用いたり、業務固有の暗号化を行うなどの配慮をすべきである。

参考 法案第20条

(従業員の監督)

第18条 事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行ななければならない。

2 事業者は、前項の監督に当たっては少なくとも次の事項を行うべきである。

- (1) 内部規程を策定し従業者に周知すること。

- (2) 従業者に対して定期的に個人情報の保護に関する教育を実施すること。
- (3) 個人データが適切に取扱われているかを必要に応じて確認すること。

(解説)

1. 法案第 21 条では、従業者に対する事業者の監督責任が義務として謳われている。個人情報の処理を実際に担当する従業者は、その業務の場でまさに直接に個人情報に触れる者として、個人データを取り扱うにあたり、意識を高くもつことが求められる。
2. 実際、個人情報が漏洩する事件の原因の一つに悪意をもった内部関係者が介在していることが挙げられる。たった一人の仕業であっても、それが公になることにより、その企業イメージは大きく損なわれ、場合によっては企業の存続に関わる問題ともなる。したがって、事業者は役員からアルバイトにいたるまでの従業者に対し、不断の啓発活動や個人情報保護についての教育を実施することが望まれる。
3. また、法案第 58 条では事業者は従業者が業務において違反行為を犯した場合、行為者とともに事業者にも罰則を科するとされていることも十分に認識されるべきことである。
4. 規程を定め、教育を通じ従業員の意識浸透を図るとともに、必要に応じて個人データが適切に取扱われているかどうかの現場監査や、場合によっては従業者に誓約書の提出を求めることなどの措置を講ずる必要がある。

参考 法案第 21 条

(委託先の監督)

- 第 19 条 事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。
- 2 事業者は、前項の監督に当たっては、このガイドラインに従い少なくとも次の事項を行うべきである。
 - (1) 委託先の選定基準を策定すること。
 - (2) 前号の基準に照らして委託先の評価を行うこと。
 - (3) 個人情報の保護に関する事項を契約書に明記すること。

(解説)

1. 近年の情報化の進展に伴い、企業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。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に必要な措置を講ずるべきとの観点から本条が定められた。
2. 電子商取引では、広告・宣伝情報のコンテンツの作成や、その更新等事業者本人が行わず、外部に委託することも多い。
3. 委託先の選定に当たっては、遵守すべき各種の安全対策に関する基準を設け、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、委託処理期間等の明記、処理終了後の個人データの返還又は破棄等を取り決めることが必要である。
4. 個人情報の処理を委託している場合において、本人からの開示・訂正・削除の求めに応ずる責任を負うのは、直接的には委託元の事業者である。ただし、委託の業態に応じて、委託先に対し、開示・訂正・削除の請求を受ける窓口事務や、場合によっては、求めに応じて開示・訂正・削除を行うこと自体を委託契約のなかで定めることもできる。

参考 法案第 22 条

(サイバーモール運営者の責任)

第 20 条 事業者は、自己が運営するサイバーモールにおいて、本人から直接個人データを取得するオンラインショッピング業者、情報提供サービス業者等(以下「ショップ等」という。)に対し、当該個人データの安全管理が図られるよう、必要かつ適切な指導を行ななければならない。

(解説)

1. 本条はサイバーモール運営者がそこに出店するショップの個人データの安全管理について、一定の注意義務を課したものである。実際サイバーモール運営者はショップにおける個々の取引や契約について消費者と直接的な関係をもつものではない。しかしながら個人データが漏洩した場合、消費者からみると個々のショップへの責任の追求に留まらず、ショップの加入しているサイバーモール運営者にも苦情が寄せられることが多い。
2. そのショップが本人に対し、個人データの安全管理についての責任を明確にしている場合、

サイバーモール運営者は法的には責任が軽減されることもあると思われるが、それでもなお、社会的責任を追求されることがあり得るので、ショップ等に対する安全管理措置についての適切な指導を施すことが望まれる。

3. また、サイバーモール・ショップ間で個人データを提供し合う場合、お互いに個人データの保護について同等の取扱いであることを確認し、双方で以下のことに留意してその取扱いに関する契約を締結すべきである。

提供し合う個人データの利用目的についての制限

提供し合う個人データの項目

提供し合う個人データを利用する者の範囲

提供し合う個人データの再提供の有無又は再提供禁止

提供し合う個人データを利用できる期間

守秘義務

事故時の責任分担等

脱会後の措置等

第3節 個人データの第三者提供

(第三者提供の制限)

第21条 事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

- (1) 法令に基づく場合
- (2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
- (3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
- (4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(解説)

1. ECOM ガイドライン 1.0 版では、第三者提供について収集の目的の範囲内で行う個人情報の提供は、あらかじめ情報主体の同意を得、又は提供より前の時点で本人に拒絶の機会を与え等本人による了解の下に行うものとしている。
2. 法案第 23 条第 1 項では、本条(1)から(4)の場合を除いて原則としてあらかじめ本人の同意を得ないで個人データを第三者に提供してはならないとしている。
3. 電子商取引においては、個人情報がインターネットを通じて大量に取得されるが、個人データが本人の知らないところで第三者に提供され、利用されることについての不安感が抱かれる。この条項では、法案と同様に、個人データの第三者提供についてはあらかじめ本人の同意を得ないで行ってはならないとの明確な原則を示し、消費者の不安の払拭を図る。

参考 法案第 23 条第 1 項

(第三者に提供できる場合)

第 22 条 事業者は、第三者に提供される個人データについて、本人の求めに応じてその提供を停止することとしている場合であって、次の各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前条の規定にかかわらず、当該個人データを第三者に提供することができる。

- (1) 第三者への提供を利用目的とすること。
- (2) 第三者に提供される個人データの項目
- (3) 第三者への提供の手段又は方法
- (4) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

2 事業者は、前項(2)又は(3)に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

(解説)

1. 本条は、住宅地図業者やデータベース業者等第三者に個人データを提供する事業者の取るべき措置を規定した法案第 23 条第 2 項に対応している。
2. 第 21 条で原則として同意を得ないで個人データを第三者への提供をしてはならないとした上で、本条に示すように、本人の求めに応じて当該本人が識別される個人データの第三者提供を

停止することとしている場合は、そのことを含む(1)から(4)について本人に通知するか本人が容易に知り得る状態に置くことにより、第三者提供ができるとする。

3. 「本人が容易に知りうる状態」とは、本人が時間的にも、手段においても容易にアクセスできたり認識できる状態をいう。電子商取引の場面においては、例えばホームページ上の見えやすいところに、「個人情報の第三者提供について」等と表記し、そこをクリックすることによりその内容が表示されるといったことが方法として考えられる。
4. ここで定められる措置は、第11条解説2.と同様のオプトアウトの手続きである。
5. インターネット等の情報ネットワーク上では、当該本人が識別される個人データの第三者提供の停止の求めを本人より受け付ける方法として、ホームページからの入力や本人からの電子メールによる返信等の方法が可能である。
6. また、第2項に関する措置についても、ホームページ上での告知や本人への電子メールで通知することができる。

参考 法案第23条第2項

(第三者提供に該当しない場合)

第23条 次の各号のいずれかに該当する場合は、第三者提供に該当しないものとする。

- (1) 事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合
- (2) 合併その他の事由による事業の承継に伴って個人データが提供される場合
- (3) 個人データを特定の者との間で共同して利用する場合で以下のことをあらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

共同利用する旨

共同して利用される個人データの項目

共同して利用する者の範囲

利用する者の利用目的

当該個人データの管理について責任を有する者の氏名又は名称

- 2 事業者は、前項(3)に規定する項目を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

(解説)

1. 個人情報の処理を外部に委託する場合については、個人情報を取得した事業者の目的の範囲で行われる一般的な行為であるため、法案でも委託先は第三者に該当しないとしている。
2. 事業者の合併や吸収により事業の継承が行われ、合わせて同じ目的の範囲内で個人データが移転(提供)される場合についても、法案では提供された事業者を第三者とは見なしていない。
3. 本条(3)では具体的には同一企業グループ内、例えば親会社と関連会社との間での個人データの提供をし合うケースなどが想定される。

参考 法案第 23 条

第 4 節 開示・変更・利用停止等の求めへの対応

(保有個人データに関する事項の公表等)

第 2 4 条 事業者は、保有個人データに関し、次の各号に掲げる事項について、本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければならない。

- (1) 当該事業者の氏名又は名称
 - (2) すべての保有個人データの利用目的
 - (3) 保有個人データの開示、訂正等、利用停止等の手続及びその手数料
 - (4) 保有個人データの適正な取扱いの確保に関し必要な事項として法令で定めるもの
- 2 既に保有している個人データの利用目的の通知を求められたときは、本人に対し、遅滞なく、これを通知しなければならない。ただし、第 1 2 条(1)から(3)までのいずれかに該当する場合はこの限りでなく、利用目的を通知しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(解説)

1. 例えば、購入した商品の代金を既に支払っているにもかかわらず、支払われていないことになっている場合、その誤った情報により本人の利益が侵害されることも想定される。その場合、事業者は本人が自己の利益を保護する手段として、開示・訂正・削除・利用停止を容易に行える体制を確保しなくてはならない。

2. 主にEU等の諸外国には、事業者が取得し保有する個人情報について、提供した本人が自己情報をコントロールする権利を持つと考える説がある。
3. 法案及びこのガイドラインでは本条以下に本人の求めに対する事業者の措置についての義務として定めているが、EU等諸外国においては一般に上記のように本人の権利として謳われているケースがある。本人の権利の明確化は、EU等諸外国でも関心の強いところであり、取得に際しての利用目的、保有個人データの開示、訂正、追加又は削除、利用停止又は消去の権利の明示は、国際間取引が容易になる電子商取引の場合、特に重要性を帯びてくる。
4. 「本人の知り得る状態に置く」とは、本人が知ろうとすれば知り得る状態であり、「本人の求めに応じて遅滞なく回答する」場合がこれに含まれている。とりわけ、すべての保有個人データの利用目的等についてはこの方法で対処することが現実的であると考えられる。
5. 本条以下第25条、第26条、第27条にて標記される「遅滞なく」とは本人からの申し出に対して、その事実関係を調査し、それが正当な申し出の場合は、いたずらに時間をかけることなく速やかに行われることをいう。

参考 法案第24条

(開示)

第25条 事業者は、既に保有している個人データについて、本人から自己の情報について開示を求められた場合は、遅滞なくこれに応じなければならない。ただし、開示することにより次に該当する場合はその全部又は一部を開示しないことができる。その場合はその旨を本人に対して遅滞なく通知を行う。

- (1) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- (2) 当該事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
- (3) 他の法令に違反することとなる場合

(解説)

1. 前条に示すように誤った情報により本人の権利が侵害されることがあるのに対し、本人は事業者に対し、保有する個人データの開示を求めることができる。
2. 事業者は本人からの開示の求めに対し、第2項(1)から(3)の場合を除き、遅滞なく開示しなければならず、また、第2項(1)から(3)の場合に該当し、開示しないことを決定したときもその旨を

遅滞なく通知しなければならない。

3. 本条(1)の場合は、医療機関において、病名等を開示することにより、本人の心身状況を悪化させるおそれがあるケース等が考えられる。
4. 本条(2)の場合は、従業員の人事情報等、その個人データの中に評価や判断等が含まれており、その事業者が行う人事管理等の業務に著しい支障を及ぼすおそれがあるケース等が考えられる。
5. 本条(3)の場合は、金融機関が「組織的な犯罪の処罰及び犯罪収益の規制等に関する法律」に基づき、主務大臣に取引の届出をしていたときに、当該届出を行っていることが記載されている個人データを開示することについて同法律に違反するケース等が考えられる。

参考 法案第 25 条

(訂正等)

- 第 26 条 事業者は、既に保有している個人データについて、本人から自己の情報に関して事実でないという理由で訂正、追加又は削除(以下「訂正等」という。)を求められた時は、利用目的の達成に必要な範囲内において、必要な調査を行い、その結果に基づき、これに応じなければならない。
- 2 事業者は、前項の規定に基づき訂正等を行ったとき又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨(訂正等を行ったときは、その内容を含む。)を通知しなければならない。

(解説)

1. 事業者の保有する個人データの内容が事実でない場合、本人はそれを理由として事業者の定める手続きに基づき訂正、追加又は削除を求めることができる。
2. 開示請求の場合と同様に、本人の求めに対し、事業者はその事実関係を調査し、それが正当な申し出の場合は、いたずらに時間をかけることなく、訂正等を行わなければならない。
3. 調査や訂正は「利用目的の達成に必要な範囲内において」行うこととしており、事業者の利用上、保有する個人データの厳密さがさほど求められないものまで都度対応しなければならないとすると事業者に過度な負担を強いる可能性があるため、限定的にそのように定めている。

参考 法案第 26 条

(利用停止等)

第 27 条 事業者は、既に保有している個人データについて、本人から自己の情報に関してその利用目的の制限や適正な取得に違反して取扱われているという理由及び第三者への提供が違反して行われているという理由により利用停止又は消去（以下「利用停止等」という。）を求められた場合で、その求めに理由があることが判明したときには、違反を是正するために必要な限度で、遅滞なく、これに応じ、その旨を本人に対して通知を行わなければならない。ただし、多額の費用を要するなど、その実施について困難である場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

2 事業者は、前項の規定に基づき既に保有している個人データについて利用停止等を行ったとき又は利用停止等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(解説)

1. 法案第 27 条にて本人は事業者に対し、法案第 16 条の利用目的の制限に違反して扱われる場合及び法案第 17 条の適正な取得に違反して取得した場合、その個人データの利用の停止又は消去を求めることができるとし、さらに法案第 23 条第 1 項の第三者提供の制限に違反して第三者提供がされている場合、第三者提供の停止を求めることができるとしている。
2. 開示請求、訂正等請求と同様に、本人の求めに対し、事業者はその事実関係を調査し、それが正当な求めであることが判明した場合は、いたずらに時間をかけることなく、これに応じなければならない。
3. ただし、法案では、利用停止等に応ずる際、その実施に多額の費用を要したり実施が困難な場合、例えば事業者が保有するデータベース内でその本人の個人情報のみ利用停止することで、データベースが長期間使用できなくなり、業務上大きな支障の発生する場合は、そのことに代えて本人の権利利益を保護する措置が取れるのであればその限りでないとしており、本条においてもそれに従っている。

参考 法案第 27 条

(理由の説明)

第28条 事業者は、開示、訂正等及び利用停止等の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、その理由を説明するよう努めなければならない。

(解説)

1. 法案では措置を取らなかった場合や異なる措置を取った場合の本人への理由の説明について「努めなければならない」との表記で努力義務が求められている。このガイドラインにおいても同様の措置を求めることとする。
2. 電子商取引の世界では、理由の説明の手段として電子メールを用いて行うこともできる。ただし、電子メールだけでは、消費者に対し、十分な説明ができない時や消費者が納得しないケースも十分考えられる。その場合は、担当者による電話や対面などによる説明を行うことが必要である。

参考 法案第28条

(開示等の求めに応じる手続)

- 第29条 事業者は、保有する個人データについて本人からの開示等の求めに関し、その求めを受け付ける方法を定めることができる。この場合において、事業者は、当該方法に従って行われる本人の求めを受け付けることとする。
- 2 事業者は、本人に対し、開示等の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。
 - 3 本人の求めに対する利用目的の通知及び開示についてその実施に関し、実費を勘案して合理的であると認められる範囲において定められた手数料を徴収することができる。なお手数料を定める場合は第24条(3)により本人の知り得る状態に置かれなければならない。

(解説)

1. 事業者は法案第 29 条により、本人からの開示等の求めに対し、それらを受け付ける手続きを定めることができる。
2. ただし、手続きを定めるにあたり、本人に過重な負担を強いることのないよう配慮しなければならない。
3. 本人に対し自己の個人データの開示を行う場合、その目的等を本人に尋ねる等により本人への開示範囲を確認することができる。
4. また、開示等の求めを主張する者が、真正な本人かどうか確認する必要がある。電子的ネットワーク上では、本人を認証する仕組みがない限り、安易に開示等の求めに応ずるべきではない。
5. 利用目的の通知及び開示の求めについては法案第 32 条により、実費を勘案して合理的であると認められる範囲内において手数料を定めることができるとされているが、その時には本人の知り得る状態に置かれなければならない。また、法案同様に、訂正等及び利用停止等については手数料を徴収することはしていない。

参考 法案第 29 条 第 30 条

(子どもの個人情報に関する保護者の求めへの対応)

第 30 条 事業者は、子どもである本人の保有個人データについて、その保護者から開示等の求めがあった場合は、子どものプライバシーに配慮し、一定の範囲で第 25 条から第 29 条の規定に準じてこれに応じなければならない。

(解説)

1. 本条では、子どもが入力した個人情報から子ども及び保護者が不利益を被らないようにするために、その保護者から子どもである本人と同等の開示等の求めがあった場合、同等の対応が求められることを定めている。
2. 入力したものが、このガイドライン第 15 条解説 3. にて事業者が定める「子ども」の年齢に該当し、また求めを起こした者が保護者であることを確認し、求めに応ずることとする。

第5節 苦情処理

(苦情処理)

第31条 事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

2 事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

(解説)

1. 第5節は法案第31条「個人情報取扱事業者による苦情の処理」に対応している。
2. これは個人情報保護法制に関する大綱案にて示された「私人間の関係である個人情報取扱事業者と本人との間に発生する問題は、基本的に当事者間で扱われるべきであり、また、迅速な解決を図る上でも、そのほうが望ましい」とされていることによるものである。
3. 法案においては当事者間で解決されない場合、認定個人情報保護団体に対して申し出ることができ(法案第42条)、また、主務大臣は事業者に対して報告の徴収、助言、勧告、命令の権限をもっているため、それらが発動されることもありうる。
4. 苦情処理については法案と同様に努力義務のレベルで体制の整備を求めるが、その事業領域、取扱う個人情報の特性や対象顧客件数等に応じ、リスク管理の観点からも充実を図り、苦情に対して自主的取組みによって解決に導くことが望まれる。
5. また、苦情処理窓口のメールアドレス、電話番号などの連絡先はホームページ上の個人情報保護方針等、消費者の目につきやすいところに表示しておくことが望ましい。

参考 法案第31条

第4章 管理体制

(個人情報保護担当責任者の指名)

第32条 事業者の代表者は、このガイドラインの内容を理解し実践する能力のある者を事業者の内部から1名以上指名し、個人情報保護担当責任者としての業務を行わせるものとする。

(解説)

1. 第4章は、ECOM ガイドライン 1.0 版を踏襲しており、このガイドラインの諸原則を遵守するための組織及びその実施責任について定めたものである。
2. 個人情報保護担当責任者は、事業者の代表者により指名され、コンプライアンス・プログラム若しくはそれに代わる個人情報保護体制の運営と施策の実施を行う責任者であって、個人情報の取扱いについて決定する権限を有する。
3. 事業者は個人情報保護担当責任者を1名以上指名することとする。ただし、管理者を複数名とした場合でも、責任を明確にし、当事者間での役割分担を明らかにしなければならない。

(個人情報保護担当責任者の責務)

第33条 個人情報保護担当責任者は、このガイドラインに定められた事項を理解及び遵守するとともに、従事者にこれを理解及び遵守させるために、内部規程の整備、コンプライアンス・プログラム又はそれに代わる個人情報保護体制の構築並びに周知徹底の措置、安全対策、従業者への教育訓練、委託先管理等の措置及び文書管理等を実施する責任を負うものとする。

(解説)

1. 個人情報保護担当責任者は、内部で個人情報の取扱いについて定めた内部規程を整備し、それに則したコンプライアンス・プログラム又はそれに代わる個人情報保護体制の構築のためには以下のような措置を講じることが有効である。

(1) 法令その他規範の特定

個人情報に関する法令その他の規範を特定し、参照できる手順を確立し、維持する。

(2) 個人データの特定

保有するすべての個人データを特定するための手順を確立し、特定する。さらに特定した個人情報に関するリスクを定期的に調査し、その予防及び是正等の措置に関する計画書を立案する。

(3) 細則の策定

事業に関する個人情報、雇用管理に関する個人情報、その他の個人情報の種類、取り扱う個人情報の量、利用方法、部門の業務の特性、個人の権利利益を害するリスクの程度等に応じて内部規程の細則(帳票等を含む。)を定め、必要に応じコンプライアンス・マニュアル

ルを作成する。

(4) 計画書の策定

内部規程を遵守するために必要なリスク調査、教育、監査等の計画を立案し、文書化し、かつ、維持すべきである。また必要に応じて詳細計画を立案する。事業者は、計画の達成のために必要な予算措置を講じる。

2. 初めて個人情報に関する業務に就業する者に対しては、教育訓練をしてから配置するか、十分に教育訓練された者がサポートする体制を取る必要がある。
3. 個人情報の取扱いを外部に委託する場合も、当該委託先のその管理状況に関して適宜確認する。
4. 個人情報保護担当責任者は、その他、例えば十分な技術的保護措置を実施する等の責任も負う
5. 個人情報保護担当責任者は、このガイドラインに定めるすべての事項について、適正に書面又はこれに変わる方法で文書管理がなされるよう徹底することが望まれる。今後、個人情報保護についての法制化がなされ、事業者として守るべき義務が生じることを前提とした場合、企業リスク管理の観点より、文書管理規定を策定し、監査等の証拠として、また後日のトラブルに備えることが必要となる。このガイドラインにて定められる本人よりの開示等の求めへの対応や苦情処理だけでなく、法案第35条「報告の徴収」における主務大臣による要求により、その取扱いについての報告が求められたときや訴訟等の状況に陥ったとき、迅速かつ的確に対応できるようあるいは改ざんの謗りを受けないように文章の記録・作成と管理を徹底しておくべきである。
6. コンプライアンス・プログラム又はそれに代わる個人情報保護体制のもとに個人情報保護を推進するときには、法令、個人情報保護指針、内部規程、細則等と合致していること及びその運用状況を確認する定期的な監査等を実施することが望ましい。

第5章 見直し

(見直し)

第34条 事業者の代表者は、個人情報保護の実施状況及びその他の経営環境などに照らして、適切な個人情報の保護を維持するために定期的にコンプライアンス・プログラム又はそれに代わる個人情報保護体制を見直すこととする。

(解説)

1. 事業者の代表者は、個人情報保護の実施状況及び監査等を実施するときにはその報告書の指摘事項について、フォローの状況を必ず確認し、コンプライアンス・プログラム又はそれに代わる個人情報保護体制自体の改善点はないか見直し案を作成させ、優先順位を付して実行させる必要がある。また、具体的な指示の内容は、それぞれの担当者宛に書面により行い、徹底するとともに、その実施結果も含めて履歴を管理し、株主代表訴訟ほか取締役の責任に対応する措置を講じておくことが重要である。

5 海外有識者・関係機関との接触・海外事情調査

5.1 北米地域への調査・視察渡航

かねてより ECOM 消費者グループおよび国際連携グループとの関係を持つ Internet Law & Privacy Forum(以下、ILPF)が定期的開催する「ILPF Conference 2002」に参加することと北米関連団体・企業グループ・有識者との交流を図る目的にて 2003 年 9 月、北米地域への調査・視察渡航を行った。

5.1.1 渡航主旨・計画

渡航の主旨および事前の計画は以下の通りである。

主旨：

国会において個人情報保護法が審議される中、日本企業にとって個人情報保護への意識と関心は日々高まりつつある。本調査・視察では、個人情報保護についてすでに企業及び団体としての対応が進んでいる北米の関連行政機関や民間団体・企業を訪問し、ヒアリング及び意見交換を実施、当地の現状・課題および今後の動向を把握する。

さらに、9 月 18 日～19 日の日程にてシアトルにて開催の ILPF (Internet Law & Policy Forum)主催「ILPF Conference 2002 Security v. Privacy」に参加し、日本における ECOM 個人情報保護WGの活動紹介(パネルディスカッション参加)と他国の取組や情勢を調査する。

主なスケジュール：

9 月 15 日(日) <ニューヨーク>

- ・ コロンビア大学 名誉教授 アラン・ウェスティン氏訪問
個人情報保護の世界各国の情勢・トレンドや今後の動向をヒアリング

9 月 17 日(火) <ワシントン DC>

- ・ 米国企業 GPA (Global Privacy Alliance) メンバーとの情報交換・懇談
主催：IBM、参加予定：Procter & Gamble, AOL Time Warner, GM, Oracle, Verisign 等
- ・ BBB-On Line プライバシー・プログラム担当責任者ヒアリング

9月18日(木)・19日(金) <シアトル>

ILPF (Internet Law & Policy Forum)主催「ILPF Conference2002 Security v. Privacy」会議参加

(URL: <http://www.ilpf.org/conference2002/>)

参加者:

電気事業連合会	情報通信部 副部長	藤原康明氏
日本IBM株式会社	公共渉外 課長	尾崎俊哉氏
電子商取引推進協議会	主席研究員	浅沼省吾

5.1.2 調査・視察報告

以下に上記の北米調査・視察渡航の報告を掲載する。

5.1.2.1 アラン・ウェスティン教授ヒアリング

コロンビア大学名誉教授であり、現在、社会と法研究センターの会長を務めるアラン・ウェスティン教授を訪ね、自己情報コントロール権、アメリカ、ヨーロッパ、日本のプライバシー関連課題比較、日本の個人情報保護法案等についてのお話を伺った。

日時 9月15日(日) 13:00-17:30

場所 ニュージャージー州ハッケンサック 社会と法研究センター

コロンビア大学 名誉教授 アラン・ウェスティン氏ヒアリング要約

アメリカ・ヨーロッパの背景

- ・ 日本と比較してみると、アメリカでもヨーロッパでも、個人情報を守るという権利がある。ヨーロッパでは人権 (Human Rights) といい、アメリカは個人の権利 (Individual Rights) である。しかし文化は異なるので、個人のコントロール権に対するアプローチはそれぞれの国で異なる。
- ・ ヨーロッパでは、官民すべてをひとつの法で包括する。ヨーロッパではナショナルデータプロテクションエージェンシーという独立機関があり、調査や裁判にもっていくまでの仕事をするだけでなく、法の執行機関として実際の告発

など全部を行う。一般的に、こうした機関は政府機関の一部として働いているところが多いのだが、プライバシーに関してはEU指令で義務づけられているので、全くの独立機関として存在する。また、大方のヨーロッパのエージェンシーは、アメリカの機関と比較しても、弁護士や大学教授などが専門知識を持った人をメンバーとし、小規模（25～50人位）、かつ、少ない予算で運営されている（年間US\$7millionぐらい）。

- ・ ヨーロッパではプライバシーは人権として扱われているので国家レベルで保護されている。例えばコンピュータでも携帯電話でも、人権により保護される。そして、保護するために重要になるのは、データのプロセスであり、OECDガイドラインが原則となっている。
- ・ アメリカは、歴史的背景もあって個人を尊重する傾向が強い。それに基づいた法律や個人を保護するための独立機関がたくさんある。
- ・ アメリカでは第二次世界大戦前までは、政府と市民という2つの関係に基づいた法律であった。企業を対象にした規則は、コンピュータが普及し始めた頃からだんだん出てきた。
- ・ 昔は、警察による個人のプライバシー侵害や、税金問題で政府が個人の情報を過剰に収集したといった問題であった。また、コンピュータ時代が始まるまでは、政府が個人情報を収集してクレジットの企業に与えるなど消費者が知らない形で政府から企業に情報が渡っていた。プライバシーとして守られている部分は、例えば個人が勝手に写真を取ってそれを広告に使ったりしてはいけないという範囲であった。例えば、私がカムリに乗っていて「彼が乗っているから良いクルマだよ」と宣伝されると、自分のプライバシーが侵害されたという形で、広告に使われたからお金がもらえるのに、勝手に使われて自分にお金が入ってこなかったので起訴するという形でプライバシーが守られた。
- ・ そして、コンピュータ時代が到来し、プライバシーに関する法律が企業に対して出来始める。アメリカでは、個人情報の内容や扱う企業グループとユーザーの関係はそれぞれ違うので、セクター毎に異なった対応がなされている。1つの機関が市場全体を規制するのは不可能とのことより、それぞれのセクターで業界に精通した専門家がそれぞれの事情に基づいて対応している。
- ・ また、アメリカ人は裁判を起こす国民である。ひとつには、個人の訴える権利

を尊重するというプロセスがシステムとしてつくられている。2つ目は弁護士の数が多い。そして、集団訴訟も多い。これがアメリカの特長である。

自己情報コントロール権 / オプトインとオプトアウトについて

- ・ アメリカでも、個人が自分の個人情報を完全に所有するということはない。しかし、コントロールということは別。現在の情報社会では個人がある程度コントロールする権利を持つことは核となるものだと思う。

コントロールすることについて言えば、例えばオプトインでは、消費者の承諾を得ないと情報が全く使えない（目的外及び目的に沿ったものでも）。ただし、企業と消費者との間でお互い公平に情報が使えて共有できるかということが重要。両方にとって公平でメリットがあることが重要。目的に基づいた情報の使用でも、消費者にダメージを与えない原則が必要。その意味で、日本の原則にも書かれている「正確性」「安全性」「透明性」等が大事。

- ・ オプトイン、オプトアウトの2種類あるが、センシティブな情報に関してはオプトイン。オプトイン・オプトアウトは情報の繊細度によるものだが、例えば医療関係では自分が精神的な問題があると薬を買っていたということで、薬局から医薬品会社に情報が伝わり、医薬品会社から「あなたはこういう問題があるからこういう薬があるから買いませんか」というような売り込みが来ると、どうしてそんなことを知っているのだということになる。それは消費者の利益にはなっていない。基本的に消費者に利益があるかどうかに基づいてオプトイン・オプトアウトも決められてくる。
- ・ そもそも、なぜ消費者が自分の情報を使われたくないか。1つは、自分の個人情報を使い、お金を儲けているにもかかわらず、自分に利益がないことへの不満。2つ目は、電話セールスが何回もかかってきたり、DMなど個人的な手紙を書いているような形で送られてくるケース。なぜ自分のことを知っているのだという気持ちにさせること。3つ目は、企業が個人情報を使い、「あなたはこういう人だからこういう商品が必要」という形で自分に影響を与えようとしているようなマーケティングの仕方。4つ目は、個人情報の内容による差別、たとえば、職業・国籍等の情報を与えた場合、本来なら与えられる情報もそこで差別されて与えられないのではないかという不安。
- ・ 消費者に利益がある形で個人情報が使われなければ、訴訟になった場合でも企

業は勝つことはできない。消費者にどれだけ利益があるかということが、個人情報の良い使われ方のベースになっている。

- ・ アメリカではコントロールというよりチョイス（個人の選択権）を重視している。情報の内容によってオプトイン・オプトアウトは異なるが、コントロールよりも消費者にまず選択権を与えること。（ウェスティン氏が）日本で行った調査の結果でも、日本人も自分に選択権があれば与えても良い、個人情報を利用されても良いと答えた人が多かった。
- ・ 消費者に選択権を与えておくことが大切。個人情報を企業に与えることが、消費者にも利益になる例を打ち出すことが今は重要。具体例を提示して消費者の理解を得ること。そうしないと将来的に消費者団体の力などですべてオプトインにしようという動きが出てきてしまうのではないか。

すべてオプトインにしてしまうと、いちいち承諾を得ないといけないということで次には消費者が実際にそれを読むかどうかの問題になってくる。承諾を待っていると、企業にとっては非常に時間がかかり、大きなダメージを与える。すべてオプトインにするのは経済的にも問題がある。

- ・ （日本の個人情報保護法では個人情報の性質を限定していない。あえて言えば「本人がびっくりするようなものについては同意をとりなさい」としているのだが、これは、自己情報コントロール権の観点からどのように評価されるか？との問いに）

法案が通過するとすぐに、その法律に基づいて何がセンシティブであるか、医療・金融とかの業界に分けて1つ1つガイドラインをつくっていくことが、法案に謳われている。ガイドラインを設けることが個人にコントロールする権利を与えているかということそうではないだろう。ただし、逆に個人に権利を与えてしまうと、自分にとって、これはセンシティブであるとか、自分にとってはそうではないとか、ゴチャゴチャしてしまう。そこで、ガイドラインにより、企業がどういうふう to 個人情報を扱ったら良いかを明確にしていくべき。ガイドラインに基づいて行うことで、消費者から苦情を受けるようなことを防げるのではないか。

- ・ （ヨーロッパがオプトイン原則といわれるが、なぜなのか）ヨーロッパはアメリカと文化的に違う。ヨーロッパは王制や封建主義といった文化・伝統がある。

企業のマーケティングの仕方も異なる。

- また、ある調査結果では、アメリカ人が世界で一番商品やサービスに関する選択権を消費者が持っており、ヨーロッパは比較的、企業が「こういうものがありますか」というように1つだけを提供してきて、それが欲しいか欲しくないかの答を消費者に求めることが多い。先に言ったようにアメリカでは「こういうもの」と「こういうものがありますか」というチョイス重視のマーケティングであり、一方のヨーロッパ人は1つのものだけを与えられてYes / Noが当たり前の風潮に起因する。

日本の個人情報保護法案について

- 日本ではアメリカ・ヨーロッパと違い、集団としての考え方が尊重されているので、個人の権利の考え方がまだ浸透していない。最近では、ビジネス的なトレンド、例えば、企業が個人に自分の欲しいものを選ぶ権利を与えられるような商品を出しているところから出てきて入るが。
- 日本では政府の力が強かった。最近では経済の悪化に伴い変わりつつあるようだが。したがって、個人の権利を尊重するための機関（政府機関でも独立機関でも）が諸外国に比べると弱い。また、日本では裁判の判決が下るまで時間がかかる。日本人には裁判所に持っていくのが自分達の人権保護の手段であるという認識がアメリカと比べたら低い。
- アメリカの公正取引委員会（FTC）はプライバシーに関するまでの力を持つ。日本は独立機関を持つことが大切だと思う。市民を保護する独立機関があれば、政府の個人情報保護の方針にも信頼度が高まるのではないが。
- ヨーロッパとの関係でいうと、アメリカの場合はFTCだけではなく、業界毎にそのような独立機関が存在する。それぞれのプライバシー保護の独立した法の執行機関があるので、ヨーロッパのセーフハーバー協定にサインができています。
- ヨーロッパはアメリカの独立機関に頼めば自分達で法を執行しなくてもアメリカの方できちんと法を執行してくれるという信頼関係がある。日本の場合はそこが大きな問題になってくる。

日本の歴史的経緯や実状を踏まえて、日本の今の法律のアプローチは妥当と思われるか？

- 基本原則は良いと思う。問題は基本原則をどう適用させるか、そのメカニズム

である。例えば法の執行機関を設けるとか、消費者から苦情があった時にそれを受ける機関を設けるとか、具体的な1つ1つの問題になると思う。

- ・ メディアに関しては日本が世界にないような新しい法律をつくる必要はない。ヨーロッパでもメディアに関しては適用外などの法律があるので、そういう国から学んで日本で適用しても良いのではないか。
- ・ 日本が諸外国と同じような形をとるのは、日本には異なる文化があるので難しいと思う。ただ、消費者が苦情を申し立てられるような機関を設けることが必要である。そしてそこで苦情がどう処理されるかを消費者に明らかにすることも必要である。

日本の企業は何をなすべきか

- ・ アメリカでは、BBBオンラインに参加している企業は、設立された当時は企業がお金を出し合った。それは自分達が行動を起こさなかったら、政府による規制が設けられてしまうか、裁判が起きて訴えられてしまうから。それをやることによって自分達に利益があるという概念に基づいて、自分達でお金を出しあって始めたものである。BBBオンラインのほかに、TRUST eがあるが、これはシリコンバレーの企業がお金を出しあってやっている団体。自分達が必要なシステムをつくるためにお金を出している。
- ・ アメリカでは、業界の中で規定を設ける場合、市場調査や世論調査に基づいた形で作っているのが良いのだと思う。企業によっては反対だということで、業界がまとまらないこともあり、問題になることもあるが、その場合でも消費者が求めているのはこれだというものを打ち出すことによって、反対する企業を説得することができる。
- ・ ECOMでも300社の中で、ECOMの定めたものに反対する企業もあると思うが、有力な発言力のある企業が反対した場合、決めたものが通過しにくいという問題があると思う。そういう時、調査結果みたいなものがあればECOM内でも説得に使えるのではないか。世論調査が核になる。ECOMでガイドラインをつくる場合でも、新しいポリシーを打ち出すにしても、的確な市場調査に基づいているということで企業を説得できる可能性が高いと思う。

5.1.2.2 米国企業 GPA (Global Privacy Alliance) メンバーとの情報交換・懇談

日時 9月17日(火) 10:00-12:00

場所 ワシントンDC. Morrison & Foerster LLP

参加者

Vincent Serpico(Assistant General Counsel, AIG),Michel Andrews(Vice President, Director of International Business Affairs, Citibank),Chris Mustain(Senior Program Manager, Government Programs, IBM),Barbara Wellbery(Partner, Morrison & Foerster), Cynthia Rich(Senior International Policy Analyst, Morrison & Foerster), Steve Emmert(Director, Government & Industry Affairs, Lexis-Nexis),Greg Baldi(Oracle),Carolyn Brehm(Director, National Government Relations, Proctor & Gamble),Shane Tews(Director of Public Policy, Verisign) Susan Chanpman(Director, e-Commerce Policy, General Motors),Bob Rothman(General Motors)

議事

E COMより「日本のEC企業における個人情報保護のあり方」「日本におけるプライバシーの法制化：個人情報保護法案」というテーマにてプレゼン実施

メディアの扱いについて

G (GPAコメント以下「G」) :

アメリカでは、メディアの例外規定に反対している。メディアも他の産業と同じ権利を持つからである。例外規定を作るならば、メディアに特別の権利を認めることになる。

E (E COMコメント以下「E」) :

日本では、メディアの扱いについてマスコミ自身が大きな声をあげて反対している。そうした観点及び意見は少ない。国民全体の意見であるかどうかは疑問。

法案：事業者の義務規定に関して

G : 31条で情報を訂正する権利が与えられることについてどこまで検討されるのか非常に関心がある。

E : 日本の個人情報保護法案では、事業者は個人情報取得時にその利用目的をできるかぎり特定しておく必要がある。

G：個人情報の収集時に利用目的をキチンと定義しなければならないところは、非常にヨーロッパ的なアプローチであり、特に将来、どのような目的で情報を利用するかわからない時点で目的を定義するのは、自分で自分の首を絞めるようなものである。

G：オンライン/オフラインの区別はあるのか。

E：保護法では個人情報がオンライン/オフラインで扱われるかについては特に区別はない。

G：ビジネスとプライベートについてはどうか？会社で扱われる個人情報について？

E：データにより個人を識別することができる場合、個人情報として取り扱われる。個人の特定できない会社の電話帳は個人情報として扱われないが、個人を特定できる名刺は個人情報と考えられる。

G：法案では、通知と同意の違いが英語で読むと非常にわかりにくい。

E：我々にもわかりにくく、いつも大きな議論となるところである。

G：「オプト・イン」と「オプト・アウト」の違いはどうか？

E：法案で「オプト・イン」が求められているのは、個人がその情報を使われた時にビックリするかどうかの一つの目安である。基本的には、事業者は個人情報の利用目的について通知または公表する必要。

G：行政官庁の権限の強いのに驚いている。官庁の個別の権限のもと、産業分野毎に指導していくので、産業毎に違った取り組みになることが考えられる。

E：電気通信、医療、運輸等の分野では分野独自の取り組みになることが考えられる。

G：産業によっては取り組みが異なる中、E C O Mのガイドラインは個別の産業についてどれだけ役立つのか。

E：主に電子商取引を対象としたものであるが、既存の概念による個別の業界向けということではない。法案自体に明確にうたわれていないところに関し、具体的なケースを示すものである。

G：ガイドラインは産業界にとっての自主規制のためにあるべきであり、政府のためにあるべきではない。

ヨーロッパの状況について

G：ヨーロッパではE U指令をベースに各国毎のルールがあり、プライバシーステートメントも国毎に変える必要がある。第三者への個人情報の提供についても各国でかなり温度差がある。E U指令一つでヨーロッパ各国への対応を考えているととんでもないことになるという一つの例である。

E：日本では、E U指令をクリアすることを考えているというよりもそれを意識して法制化を図っているところである。

G：ヨーロッパでは、プライバシーに関する指令を再検討する作業が始まった。これに関してアメリカの産業界としても意見を出すため、情報収集している。

G：日本で法案が通過したあと、E Uとの協議が始まるであろうが、その際は、米国内で蓄積したE Uとの交渉における情報で役立つものが多いと思う。EU 指令の改訂作業への日米での協調した提言の可能性を含め、ぜひ日米の産業界での意見交換を進めましょう。

アメリカの状況について

G：アメリカでは、日本やヨーロッパのような包括法は存在しないが、現在、いくつかの幅広い総合規制法案（ただし、日本やEUのような包括法に比べると、対象範囲が限定的）が議員立法されており、いくつかの委員会で検討されている。加えて、金融関連セクターに特化した、包括的なプライバシー保護法案の動きもある。以前に比べると、米国内でも包括的なアプローチの必要性を主張する議員が増えてきた。これらの議員は、消費者グループの利害を代弁しているというより、法曹界、とくに民事訴訟弁護士事務所の利害を代弁しているものであり、国民的なコンセンサスではない。産業界は、一貫して、反対である。それらが一本化されて法案として通過するかどうかの見通しが、はっきりとするのは、上院と下院での党派的な対立が中間選挙以降どうなるかにも影響することであり、来年以降のことであると考えている。

G：産業界にとって、より悩ましい問題は、州レベルでのプライバシー規制の動きである。特に、現在カリフォルニア州議会で審議されているプライバシー規制法案は、産業界にとっても、消費者にとっても、メリットがあるものとは思えない。さらに、カリフォルニア州での立法化が実現すると、全米各州に、動きが伝播し、各州で微妙に異なった法律が乱立することが憂慮される。州議会通過の可能性は予測されるが、我々としては、州知事による拒否権の発動で、今回の法案が成立

しないよう、各方面への働きかけを続けているが予断を許さない。

G：自主規制は、産業界ごとにとというよりは、BBBOnline や TRUSTe などのシールプログラムを活用したり、Online Privacy Alliance などの一般的なガイドラインを参照したりしながら、各社独自で行っている。一般に、自主規制は、あくまで企業側が、顧客や取引先、株主を含めたステイクホルダーの関心に配慮しながら「自主的に」作るものであって、法律や規制の解釈集ではないと考える。また、自主規制の実効性は、シールプログラムへの参加や、第三者による監査、情報の公開のなかで、確保している。

5.1.2.3 BBB-On Line プライバシー・プログラム担当責任者 Gary Laden 氏ヒアリング

日時 9月17日(火) 13:00-14:30

場所 ワシントンDC BBB - On Line

議事

BBB - On Line プライバシー・プログラムの近況

- ・ プライバシー・プログラムは 99 年以来 3 年。現在、700 のサイト。1500 ぐらいの申請を受け付けたが 700 がとれたぐらい。消費者信頼プログラムでもプライバシーの規定を持ち、それをクリアする企業は多いが、プライバシー・プログラムはレベルが高いので、クリアする企業は多くない。
- ・ プライバシー・プログラムでは 2 つの新しい取組みがある。1 つはヨーロッパのセーフハーバーの要求を満たしたこと。現在の BBB のプライバシー・シールプログラムはすでにセーフハーバーの要求を満たしている。いくつかの会社はセーフハーバーについての紛争のために申し込んでくる。
- ・ ただし、会社はたくさんのシール(ブランド)が並ぶのを望まない。BBB があり、ベリサインがあり、自社のシールがあるのを嫌う。
- ・ もうひとつは、プライバシーを理解する新しい教育素材を開発した。BBB On Line Understanding Privacy という。P&G、IBM、プライバシーカウンセラー、ACXIOM、ヒューレット・パッカート、US Postal Service の 6 社が委員会を構成。シールプログラム、紛争解決のプログラムに続いて、第 3 のプログラムとしてビジネス教育、消費者教育のプログラ

ムを立ち上げた。

- 主には WEB 上で行う。インタラクティブなソフトウェアで開発している。プライバシーポリシーをつくらうとする会社はそのソフトを使うことができる。B B B のシールも得られ、教育セミナーや会議も企画中である。これはまだ初めて 4 週間、6 社との委員会を 4 週に 1 回開いている。(B B B オンライン・エディケーションフォーラムと呼ぶ。) まだ多くの会社が未教育のためにプライバシーについてうまくできていないと思うが、そうした会社に教育システムを提供する。
- 対象は会社、そして従業員。あらゆる種類の、中小、そして、大企業も。小さい会社は大企業よりもそのことが難しい。そして、消費者教育も行う。

個人情報の苦情およびトラブルの実態

- 3 ヶ月ごとに B B B オンラインサイトにその統計を公開している。当初は少なかったが、紛争は増えている。3 ヶ月に 200 件ぐらいに増えている。(2002 年 1 - 6 月 421 件、2001 年は 3 ヶ月で 5-60 件、
<http://www.bbbonline.org/privacy/dr/2002q2.asp>による)
- 最も多い種類は (o f f m a i l i n g l i s t) メーリングリストから抜きたいひとが、それができず、連絡をとっても実施されないというもの。
- メーリングリストから外さない等のトラブルについては、まずその企業に直接行くようにと進める。個別に企業が対応できなかったか調べる。かならず、企業との話し合いをやっていることを確認しないとわれわれは対応しない。

J I P D E C 相互認証の企業の数?

- 現在 6 社。ほとんどは小さい会社だが、ひとつだけ大手会社がある。ヒューレット・パカードである。

リライアビリティとプライバシーの 2 つのマーク制度を運営することに消費者および企業に対する課題

- その課題は認識しており、長期的には統合していくことも考えられる。われわれにとってむつかしいのは多くの企業がそれぞれのシールを取得している。統合することによりすべての会社が他方のマークの機能を欲するとは限らないだろう。
- また、アメリカ下院で、来週、連邦レベルでのあたらしい法案を審議すること

の連絡が議員の方よりあった。B B BのプライバシーシールをとっていけばF T Cの規則に関してセーフハーバーを与えるとの法律。もしも問題があった場合、F T Cに行かずに、B B Bの方に来て解決を図るようになる。S T E A R N氏が下院商業委員会で提起し、9月24日に私が証人として召喚されている。

- 従って、長期的には統合することを見込むものの、短期的には、この法案のために、即座にそのようにはできないだろう。この法案は自主規制の観点からはいいと思う。

モバイルについて。携帯電話に関する動向

- 今はB B B - O n Line プライバシー・プログラムには特に規定はない。
- 位置情報については日本がもっと進んでいるでしょうが、アメリカでは、民間団体で Mobile Cellular Telephone Association というのがあり、そこでは独自の携帯プライバシー基準がある。
- F C Cでは新しい要求事項がある。2000年に2年以内にすべての電話は110番に掛けた時に自動的にその位置がわかるようにしなければならない「E 9 1 1 (the wireless E n h a n c e d 9 1 1 rule)」という法律が通った。その実施の時に人々は大きな問題であることに気づくだろう。携帯やレンタカーで利用者の位置がわかるのは潜在的に大きな問題である。その問題について議論しているのは今のところ携帯電話協会だけ。(関連記事:
http://www.zdnet.co.jp/news/0005/20/b_0519_15.html
http://www.zdnet.co.jp/news/0205/31/nebt_07.html
<http://www.fcc.gov/911/enhanced/>)
- アメリカの法律でさらに問題となっているのは電源を切っても解るようになるとの要求がある点である。

5.1.2.4 Internet Law & Policy Forum 主催 「I L P F Conference2002 Security v. Privacy」会議

日時 9月18日(水)~19日(木)

場所 ワシントン州シアトル Bell Harbor International Conference Center
(1日目)

Security and Privacy One Year Later (1年後のセキュリティとプライバシー)

- 荒金善裕氏、富士通株式会社
- Stuart Baker 氏, Steptoe & Johnson LLP

9月11日の結果として、セキュリティを促進しテロリストの活動を止める新しい法律が世界中で採用された。そのような法律はどのような実際の変化をもたらしたか。そして、どのようにプライバシー法は結果として影響を受けたのか。

Privacy Track | P-1 Privacy Global Survey: Legislative Regimes and Cross-Cultural Dimensions(プライバシーの世界調査：立法制度と比較文化の側面)

- モデレーター: Alixandre Schijman 氏, AOL Time Warner
- Suzanne Morin 氏, Bell Canada
- Christopher Kuner 氏, Hunton & Williams
- Blair Stewart 氏, Assistant Privacy Commissioner, New Zealand
- James Halpert 氏, Piper Marbury Rudnick & Wolfe
- 尾崎俊哉氏, 日本IBM株式会社

プライバシー制度に影響を与えた主要な社会的、文化的要因に焦点を当てつつ、世界中で採用されてきた種々のプライバシー制度を明らかにする。EU や、ニュージーランド、オーストラリアに代表される包括法のアプローチと、米国に代表される個別法のアプローチに対し、カナダや日本は、折衷型のアプローチを試みていることが示された。

Privacy Track | P-2 The Impact of Technology on Privacy Law(プライバシー法に関する技術の影響)

- モデレーター: Kristen Verderame氏, British Telecom
- Mary Wong 氏, University of Singapore
- Alex Alben 氏, Real Networks
- Declan McCullagh 氏, CNET News.com

インフォメーション・エイジはどのようにプライバシーについての期待を変えているか。本質的に異なるデータをデータマイニングのような手法をもちいることで、第三者が公的に入手可能なデータとして使用できるか。プライバシーのコストとは何か。また、誰が支払うのか。プライバシー侵害は刑事犯罪とするべきか。

Lunch General Session | G-2 Security and Privacy Conflicts - Real and Imagined (セキュリティとプライバシーの摩擦 - 現実と想像)

- Albert Gidari 氏, Perkins Coie LLP

セキュリティとプライバシー間の緊張がいかに現実的なことであるか、このふたつの重要な政策の間の衝突や相乗効果、また盗聴法やその他の法規の施行やプライバシー問題等の推移を観測する中で、それらがどのように消費者信頼に影響を与えたかを検討する。

Privacy Track | P-3 Drafting, Implementing and Enforcing Privacy Policies for Companies Engaging in eCommerce(グローバルな e-コマースに従事する企業のためのプライバシーポリシーの作成、実施、執行)

- モデレーター : Ruth Day 氏, Consultant
- Anita Ramasastry 氏, University of Washington
- W. Scott Blackmer 氏, Attorney at Law
- 浅沼省吾, 電子商取引推進協議会 (ECOM)

インターネットという本質的に国際的な環境の中におけるプライバシーポリシーを、作成し、実施するという実際の局面に焦点を当てる。

General Session | G-3 Legal Risks Associated With Surveillance and Monitoring (監視に関連する法的リスク)

- モデレーター: Colm Dobbyn, MasterCard International
- Tilmann Kupfer, British Telecom
- Christopher Bubb, America Online Inc.
- Dr. Makoto Ibusuki, Ritsumeikan University
- Albert Gidari, Jr., Perkins Coie LLP

政府の監視の今の傾向は個人のプライバシーに影響を与えている。インターネットトラフィックを監視する技術的で実際的な限度について、またそのような活動を支援する私企業に政府の要求によって生じる法的経済的問題について調べる。

Privacy Track | P-4 Watching Employees: Legal Considerations, Practical Guidelines and Netiquette (従業員の監視 法的考慮、実際的なガイドライン、ネット)

- モデレーター : Vince I. Polley, Schlumberger Limited
- Professor Michael Geist, University of Ottawa
- Graham Smith, Bird & Bird

企業は今日、より多くの時間と財源を従業員の監視に投資している。その中には、個人のプライバシーを侵害していると強く主張する法的な問題となったものもある。そのような事例の世界傾向について討論する。

General Session | G-4 Security v. Privacy: Perspectives from the Top(チーフセキュリティオフィサーとチーフプライバシーオフィサーからの展望)

- ・ モデレーター : Andrew Konstantaras 氏, ILPF
- ・ Joseph Alhadeff 氏, Oracle Corporation
- ・ Kenneth Lieberman 氏, Visa International
- ・ Richard Purcell 氏, Microsoft Corporation

第一日の終わりにあたり、チーフセキュリティオフィサーとチーフプライバシーオフィサーにきていただき、直面する問題の現実について腹藏のない討論する。

(2 日目)

General Session | G-5 Who Are You and Who Wants to Know? Privacy and Authentication Considerations(あなたは誰でしょう。誰が知りたいと望んでいるのでしょうか)

- ・ George Radwanski, Privacy Commissioner, Canada

セキュリティを強化する中で、政府は潜在的な犯罪者を見つけるのに助けとなる技術を探索する。このセッションではこの動向と個人のプライバシーに与える影響について調べる。

Privacy Track | P-5 Establishing Privacy: Does Technology Help or Hurt ? (プライバシーの確立 : 技術はそれを助けるのかそれとも傷つけるのか ?)

- ・ モデレーター : Bennie Smith 氏, DoubleClick
- ・ Paul Misener 氏, Amazon.com
- ・ J. Trevor Hughes 氏, Network Advertising Initiative
- ・ Rebecca Whitener 氏, EDS

クッキーや P3P といった技術のインパクトはプライバシーや消費者信頼にどのように影響したか ? オンラインとオフラインの間のプライバシーについての類似性と相違点について討議する。

Privacy Track | P-6 Myths and Realities of Anonymity, Pseudonymity and

Identity in the Online World(オンラインの世界での匿名性、偽名性と本人性の神話と現実)

- モデレーター Andrew Konstantaras 氏, ILPF
- Barb Fox 氏, Microsoft Corporation and Senior Fellow, Kennedy School of Government, Harvard
- Margaret P. (Peggy) Eisenhauer 氏, Hunton & Williams
- Giusella Finocchiaro 氏, University of Bologna
- Rob Leathern 氏, Jupiter Research

技術は匿名性を殺すのか、それともそれは今までに存在したのか？完全な匿名性の選択肢はあるのか？インターネットやエコマースを背景とした匿名性、偽名性の技術的、法的そして政策的局面を討議する。

Lunch General Session | G-6 Big Brother Comes Home: Human Chip Implants, GPS Applications and Other "Advances" in the Future of Security and Privacy (Big Brother[監視人]が家庭に来ます。 - ヒューマンチップインプラント、GPS アプリケーション、その他の先端技術 未来のセキュリティとプライバシー)

- Marc Rotenberg 氏, Electronic Privacy Information Center

技術は盲目的に進化しつづけるが、それでいいのか？このセッションでは、個人のプライバシーを主張する指導者が、それほど遠くない将来に、セキュリティとプライバシーの取り組みに影響を与える新しい技術的な開発を明らかにする。

General Session | G-7 New Frameworks for Authentication and Privacy (個人認証とプライバシーの新たなフレームワーク)

- モデレーター : Andrew Konstantaras, ILPF
- Carol Coye Benson, Glenbrook Partners
- Takaaki Matsumoto, NTT DATA Corporation

認証技術はこの数年で立ち上がる準備がなされてきたが、技術的欠点と同様に法的な複雑さからやっと期待に恥じないといったところである。あるものは技術的な欠点同様に法的複雑さによると非難し、またあるものは欠陥ビジネスモデルであるために採用が進まないことのせいにする。インターネットにおいて認証とプライバシーの必要性に的をあたえ、新たな必要性を探る

General Session | G-8 Policy Wishlist (必要な政策リスト)

- モデレーター： Roger Cochetti 氏, VeriSign Inc.
- Orson Swindle 氏, US Federal Trade Commission
- Malcolm Crompton 氏, Australian Federal Privacy Commissioner
- 大野秀俊氏, Ministry of Economy, Trade and Industry, Japan
- Mark Bohannon 氏, Software and Information Industry Association
- Gail Hamilton 氏, Symantec Corporation

産業部門及び政府部門からの指導者たちが、来るべき年におけるセキュリティとプライバシーについての最優先事項について腹藏なく討論する。

General Session | G-9 Law and Ethics in Business Environments: Security, Privacy, Confidentiality and Lawyers on the Internet Law & Policy Forum (ビジネス環境における法律と倫理：インターネット使用により生じるセキュリティ、プライバシー、機密性問題)

- モデレーター: Sharon L. Nelson 氏, University of Washington School of Law
- Robert C. Cumbow 氏, Graham & Dunn PC
- Michael Donovan 氏, Hancock, Rothert, and Bunshoft LLP
- Brian Roundtree 氏, Action Engine Corporation

弁護士は益々仕事のために、基本的に安全ではないインターネットに頼る。しかし、依頼人の情報の守秘義務はかつてなく増している。このセッションでは、毎日法的業務をオンラインで行うことから生じる実際問題と法律問題を検討する。

5.2 中国・韓国 視察調査渡航

中国における電子商取引の現状および個人情報保護の国際的な動向を調査と関連機関と接触を図るため、11月25日～27日中国・上海にて開催の「中国インターネット大会」および11月28日韓国・ソウルにて開催の Korea Information Security Agency(=KISA)主催の「**2002 International Conference On Personal Data Protection**」に参加した。

5.2.1 渡航主旨・計画

渡航の主旨および事前の計画は以下の通りである。

主旨:

インターネットの高普及に伴う国際的な情報流通が俄かに盛んになりつつある。消費者保護・個人情報保護についても、この分野で先行する欧米に追随し、韓国・シンガポール等を中心にマーク制度の確立や法制化の動きが活発化している。

今般、比較的情報量の少ない中国におけるその分野での情報摂取と韓国にて開催の個人情報保護についての国際会議「2002 International Conference On Personal Data Protection」に参加し、最新の情報収集および情報源である関連機関との人脈づくりを行う。

主なスケジュール:

11月25日～26日 <上海>

- ・中国インターネット大会参加

主催：中国インターネット協会

主な参加会議・イベント：

11/25 「インターネットと知財・インターネットの経済発展」

11/26 「情報セキュリティ・インターネット政策・業界自律・法整備」

その他展示見学

11月27日 <ソウル>

- ・韓国情報通信産業協会（K A I T）または電子商取引振興院（K I E C）

プライバシーマーク担当 Hyung-Sun Kong 氏面会

- ・Asia Privacy Forum に関する事前ミーティング出席

11月28日 <ソウル>

- ・「2002 International Conference On Personal Data Protection」に参加

主催：Korea Information Security Agency(=KISA)

5.2.2 中国インターネット大会

5.2.2.1 中国インターネット最新事情

ポイントをまとめると、中国政府の情報産業省傘下でドメイン等を管理する中国インターネット情報センターは、中国のネット利用人口は6月末時点で4580万人、人口の3.6%

だったとの報告を発表。世界で米国、日本に続いて第3位。

ニールセン・ネットレーティングスの最近の調査によると、中国の自宅でインターネットに加入する人数は5,660万人となり、アジアで自宅でのインターネット加入者数の最も多い国となり、アメリカに次いで世界第2位にランクされ、その後は日本、ドイツ、イギリスが続く。

中国では世界貿易機関(WTO)ルールに基づいて、今年1月1日から情報技術(IT)製品251品目を対象に、「IT製品に関する合意書」で定められた税率が適用されている。税関の統計によると、この政策の成果により、今年第1四半期のIT製品の輸入は昨年同期を16.3%も上回る。

合意書に基づいて、モバイル機器、各種コンピューター、集積回路(IC)など122品目を対象にゼロ関税が適用。

5.2.2.2 中国インターネット大会概要

- 名 称：「中国インターネット大会?? 2002年中国インターネット協会会員大会」
- 主 催：中国インターネット協会
- 会 期：2002年11月25～27日
- 会 場：上海国際会議センター
- 主 旨：国際・国内インターネット業界の最新動向の理解と分析、WTO加盟後の中国インターネット業界が直面するチャンス・挑戦及び対応策の研究、ネットワーク技術の発展及び応用の検討、関係企業の経営・管理経験の交流、情報ネットワークサービス業発展の推進、先進的ネット文化建設の促進

5.2.3 Asia Privacy Forum への参加

「Asia Privacy Forumに関する事前ミーティング」が、11月28日開催のKISA主催「International Conference On Personal Data Protection」に先立ち、実施された。

5.2.3.1 実施要領

実施要領は以下のとおりである。

日 時：11月27日(水) 18:00-21:30

場 所：ロッセホテルワールド

参加者：

1. Hong Kong
Privacy Commissioner, Raymond Tang
Deputy Privacy Commissioner, Tony Lam
Corporate Communications Manager, Ms Shirley LUNG
2. Arthur Shay(Taiwan) Senior Advisor(Attorney at Law: Consumers Foundation)
3. Chan Yoke Kin(Malaysia) Principal Assistant Secretary, Ministry of Energy ,
Communications&Multimedia
4. Orada teppayayon(Thailand) National Electronics and Computer Technology
Center
5. Surangkana Kaewjumngong(Thailand) National Electronics and Computer
Technology Center
6. Amaral MariaJoao (Macao) A legal adviser, the Justice Affairs Bureau
7. Ana Cardoso(Macao) A legal adviser, the Justice Affairs Bureau
8. Ong Tong San(Singapore) Assistant Director (Policy), Infocomm Development
Authority of Singapore
9. Shogo Asanuma(Japan) ECOM
10. South Korea
Secretary General , Secretariat of Personal Information Dispute Mediation
Committee, KISA, Hyu-Bong Chung Director of Dispute Mediation team,
Secretariat of Personal Information Dispute Mediation Committee, KISA,
Chang-Beom Yi Researcher, Dispute Mediation team, Secretariat of Personal
Information Dispute Mediation Committee, KISA, Junghyun Cho

5.2.3.2 K I S A 発行議事録訳文

一般合意

Deputy Commissioner, Tony Lam 氏から“Privacy Forums in the Asia Pacific Region,”(「アジア太平洋地域におけるプライバシーフォーラム」)と題して、また Commissioner Raymond Tang 氏からは framework of the Asia Privacy Forum(「アジアプライバシーフォーラムの枠組み」)と題してプレゼン発表を頂き、その後会議

で取り上げられた問題点を審議した後、全ての参加者は下記の事項に合意した；

1. 国際データ保護会議 (International Conference of Data Protection Commissioners, IWGDPT, ASPAC, PANZA, etc.) における問題及び議論は、主に欧州、先進国といった高度なIT、情報保護システムが整った諸国に焦点を当てている。したがって、アジアのみを対象としたデータ・プライバシー保護に関するフォーラムの必要性がある。これはアジア諸国の現状を考慮に入れたものでなければならない。というのも、アジアは政治体制、文化的背景という観点から欧州とは異なるからである。
2. データ保護の水準はアジア諸国間で、顕著な相違が見られる。データ保護を管轄する当局は比較的ITやプライバシー向上技術、政策において脆弱であり、フォーラムの他の参加メンバーから学ぶべきところが多い。参加メンバーは互いに情報や経験を共有することで、データ・プライバシー保護のための体制構築にむけて、恩恵に浴することができる。こういった議論を鑑みると、Asia Privacy Forumの目的は次の通りとなるであろう
 - (a) 参加メンバー間での情報交換 (例えば、データ保護に関する世界的な傾向についての情報交換)
 - (b) 国際会議と参加メンバーの現状との格差解消。
3. 今フォーラムは“Asia Privacy Forum”と名づけられる。その主要な特徴は非公式性、柔軟性、情報及び経験の共有・交換である。
4. 上述のような目的達成のため、総会が定期的を開催する。さらに複数のテーマに関する作業部会(ワーキンググループ)を設置し運営する。
 - a) 作業部会は複数の有志によって構成される。
 - b) 作業部会は現在の地域的問題に焦点をあてる。
5. Asia Privacy Forumの作業部会のテーマとしては下記が想定される。
 - a) データ保護のための法的措置inventory (契約書、法令、体制等)
 - b) 一般の人々の意識向上
 - c) 執行基盤(枠組み)
6. 全参加メンバーの要請に基づき、KISAはAsia Privacy Forumの事務局となる。

結論及び今後の予定

1. KISAはCommissioner of the Hong Kong PCOのRaymond Tang氏との協議の後、参加メンバー(加盟メンバー)全てに、会議での議論の要旨(議事録)を送付するものとする。
2. 全参加メンバーは各メンバーのデータ・プライバシー保護(3つの問題について)に関する問題をリスト化し、KISAに3ヶ月以内(2003年2月末まで)に送付する。
3. KISAはPCO of Hong Kongとの協議の下、各メンバーから寄せられたリストに基づき地域の問題をリスト化し、参加メンバーに配布する。
4. 適切な連絡方法でもって議論を行い、合意を通じて作業部会は設置される。
5. 総会では作業部会の報告書や、将来の作業部会の活動予定に関する議論が行われる。
6. 総会は自発的に名乗り出たメンバー(or有志のメンバー)によって主催される。
7. 総会を開催しようとするメンバーはKISAに対し日時、場所を通知する。その後KISAが詳細を加盟メンバーに通知する。

5.2.4 KISA 主催「International Conference On Personal Data Protection」

5.2.4.1 テーマおよび主なセッション

テーマおよび主なセッションは以下の通りである。

テーマ：デジタル時代の個人情報保護

“Personal Data and Privacy Protection in the Digital Age.”

セッション：

1. スпам・メール(spam-e-mails)

議長：Hyu-Bong Chung (Secretary-General, Secretariat of Personal Information Dispute Mediation Committee, KISA)

講演者：

- ・ Stuart. J. Thorson (教授, Syracuse大学) 「スパムと個人情報プライバシー」
- ・ Jong-Bae Ahn (教授, Graduate School of Venture, Hoseo University) 「eメールマーケティングの効果とその利用」

- ・ Ji-Bong Lim (教授, College of Law, Konkuk University)
- ・ Dal-Chun Kang (Senior research fellow, Secretariat of Personal Information Dispute Mediation Committee, KISA)
「迷惑広告メールに対する韓国の法的体系的措置」

討論パネル：

- ・ Byung-Joon Lee (教授, College of Law, Pusan National University)
- ・ Hyun-Young Kim (Head of Marketing Division, Daum Communications)
- ・ Sung-Hyeon Kim (Senior Deputy Director, Information Utilization Protective Division, Ministry of Information and Communication)

トピックス：

- ネットワーク社会に与えるスパムメールのマイナス影響
- マーケティングツールとしてのeメールの有用性
- スパムメール及び個人情報保護
- スパムメール反対/賛成法案

2. 位置情報の商用利用 (Location Based Services for commercial purpose)

議長：Kyong-Whan Ahn (教授, College of Law, Seoul National University)

講演者：

- ・ Hansjürgen Garstka (Berlin Data Protection Commissioner)
「データ保護と情報の自由：個人情報としての位置情報」
- ・ 夏井 高人 (明治大学法学部教授、弁護士)
位置情報サービス(LBS)及び個人情報保護
- ・ Si-Gon Kim (教授, Geographic Information System Engineering, Namseoul University)
「位置情報サービス (LBS) : 展望とプライバシー」
- ・ Young-Dae Lee (弁護士, SUHO Legal Group)
「韓国の位置情報サービス(LBS)に関する法案」

討論パネル：

- ・ In-ho Lee (教授, College of Law, Chung Ang University)
- ・ Byung-Ik Ahn (CEO, POINTI.com)

トピックス：

- 個人情報としての位置情報
- 位置情報サービス(LBS)技術
- 位置情報サービス(LBS)の現状
- 位置情報サービス(LBS)提供の際の個人情報保護法案

3. 従業員の監視 (surveillance on employee)

議長：Kyung-Han Son (弁護士, Aram International Law offices)

講演者：

- Anna Johnston (Acting Privacy Commissioner, Privacy NSW)
「職場での電子的監視：従業員への配慮とプライバシー擁護者にとっての課題」
- Marie Georges (Head of the Division of European, International Affairs
And Advanced Studies, France CNIL)
「職場での監視と従業員のプライバシー - ヨーロッパの経験：フランス」
- Boh-Young Hwang (弁護士, Bae, Kim & Lee)
「2002年11月現在の韓国における企業での個人情報保護」
- Sun-Je Sung (弁護士, College of Law, The Catholic University of Korea)
「従業員のプライバシー：韓国とアメリカの比較」

討論パネル：

- Hee-Soung Lee (教授, College of Law, Wonkwang University)
- Eun-Woo Lee (教授, Horizon Law Group (HLG))
- In-Soo Han (教授, College of Business Administration, Chungnam National University)

トピックス：

- 雇用主の監視権 vs 従業員のプライバシー権
- 職場での監視に関する国際的なレベルでの各種議論
- 労働者のプライバシー保護への法的枠組み

4. 個人情報侵害の救済方法 (remedies for personal data infringements)

議長：Hyu-Bong Chung (Secretary-General, Secretariat of
Personal Information Dispute Mediation Committee, KISA)

講演者：

- ・ Raymond Tang (Privacy Commissioner for Personal Data, Hong Kong)
「個人情報（プライバシー）法令下での個人情報侵害の救済」
- ・ Paul Roth (助教授, Faculty of Law, University of Otago)
「個人情報侵害への救済：ニュージーランドのモデル」
- ・ Whon-Il Park (教授, College of Law, Kyung Hee University)
「韓国におけるデータ保護への適切な救済、是正措置」
- ・ Chang-Beom Yi (Director of Dispute Mediation Team, Secretariat of
Personal Information Dispute Mediation Committee, KISA)
「B2C ADRと個人情報に関する紛争調停」

討論パネル：

- ・ Dong-Won Ko (弁護士, Kim & Chang)
- ・ Soo-Tae Jang (Korea consumer protection board)

トピックス：

- 救済手段としての裁判外紛争処理(ADR)
- 個人情報侵害の事例調査
- 個人情報侵害の救済のための法的枠組み

5.2.4.2 香港における「個人データ(プライバシー)法に基づく個人データ侵害 に対する救済策」

同会議のパネル4にて、香港の個人データプライバシー・コミッショナー：レイモンド・タン氏が、香港における個人情報保護の現状およびデータ侵害に対する救済策についての講演を行った。その要約原稿の訳文を以下に掲載する。

はじめに

1994年、香港法改正委員会(LRC)のプライバシー部会は、個人データの保護に関する法律の改正に関する報告書を提出した。

LRCがその他の行政管轄区を調査したところ、プライバシー保護の制度化には大まかに

分けて 3 つの方法があることが明らかになった。

選択肢 1：

法的枠組みを作り、国家から資金提供を受ける統制機関を組織する。

選択肢 2：

民事訴訟を可能にするため、プライバシー侵害に関する不法行為の定義付けを行う。

選択肢 3：

自主的行動規範などの自主規制や、専門の監視者、あるいは業界の監視者に依存する。

LRC は、官民両部門において、国際的に合意の得られているデータ保護指針に法的効力を持たせることが最も香港の利益にかなっているとの姿勢を取っている。この報告書の作成に当たっては、別個に委託調査を行い、プライバシーに対する一般国民の意見を調査した。この調査の結果、一般国民がプライバシーの法的保護を幅広く支持していることが明らかになった。

個人データ(プライバシー)法

LRC の最終報告書を受けて個人データ(プライバシー)法(PD(P)O)の起草が始まり、1995年に成立、1996年12月に施行された。また同法の規定のコンプライアンスを監視及び監督、促進するために、独立した法定機関である個人データプライバシー・コミッショナー事務局(PCO)が設立された。PCO は選択肢 2、3 の要素も含んではいるものの、実質的には選択肢 1 の具体例である。PD(P)O によって形成される法的枠組みにより、PCO の統制機関としての独立性が確保されると同時に、一般国民は同法の規定に対する違反に関して救済策を受けることができ、またコミッショナーは行動規範を発布することにより自主規制を促すことが出来る。今日までに PCO は、身分証明書番号及びその他の個人確認証明書に関する行動規範、消費者信用データに関する行動規範、人材管理に関する行動規範の 3 つの行動規範を発布している。

2002年3月には、一般国民の意見を求めるため、職場における被雇用者監視及び個人データプライバシーに関する規範の草案が発表されている。

同法の主な特徴は次の通りである。

- 国際的に認められている保護原則の採用
- 官民両部門(政府を含む)を対象としている

- 記録が作成される自動・手動データ書式の適用
- 防衛や領土の安全保障、犯罪防止、公衆衛生、調査・統計での利用など、特定の公共の利益に基づく例外を認めている

PD(P)O は主として、情報プライバシー、すなわち香港の定義による個人データプライバシーを管理している。同法の規定は本質的には、個人、すなわちデータ対象者の個人データの利用に関して、データのユーザー、すなわち個人データを収集する者の行動を規制するものである。その際、同法は、6つのデータ保護原則(DPP)から引き出される個人データに関する権利を個人に付与するが、DPP は、その権利に合法性を与えるものである。6つのDPPについては、この報告書の付録を参照して頂きたい。

「個人データ」は、氏名や住所、年齢、身分証明書番号、給与、婚姻関係の有無、電話番号、電子メールアドレス、容姿、財務状況、データ利用者が個人に対して持っている意見など、身元を知る根拠となる情報を指す。この定義による個人データは、他の司法管轄区で使われている情報データという用語と類似しているが、完全に一致するわけではない。より具体的に言うと、PD(P)D は個人データを次のように定義している。

- 生存中の個人に直接的・間接的に関係している。
- その情報に基づいてその個人の身元を断定することが現実的に可能である。
- アクセスや処理が現実的に可能な形式を取っている。

すなわち、それが消費者の詳細を記録したデータベースであるか、あるいは雇用主が保有しており、個々の職員の容姿を記録した CCTV テープであるかに関わらず、個人データの有形記録がなくてはならない。また香港控訴裁判所が最近下した判決では、個人データは、そのデータの利用者が特定の個人を識別することを意図してデータを収集した場合に限って個人データとして認められるとされており、注目に値する。

同法に基づきコミッショナーは、PD(P)O の侵害が疑われる場合は調査を行い、場合によっては、執行通知を交付してその遵守を命ずることが出来る。結果として、PCO の主たる職務は、問合せ（2001年には21,174件受け付けられた）に答え、申立て（2001年には789件受け付けられた）の調査をすることである。

データプライバシー侵害に対する救済策

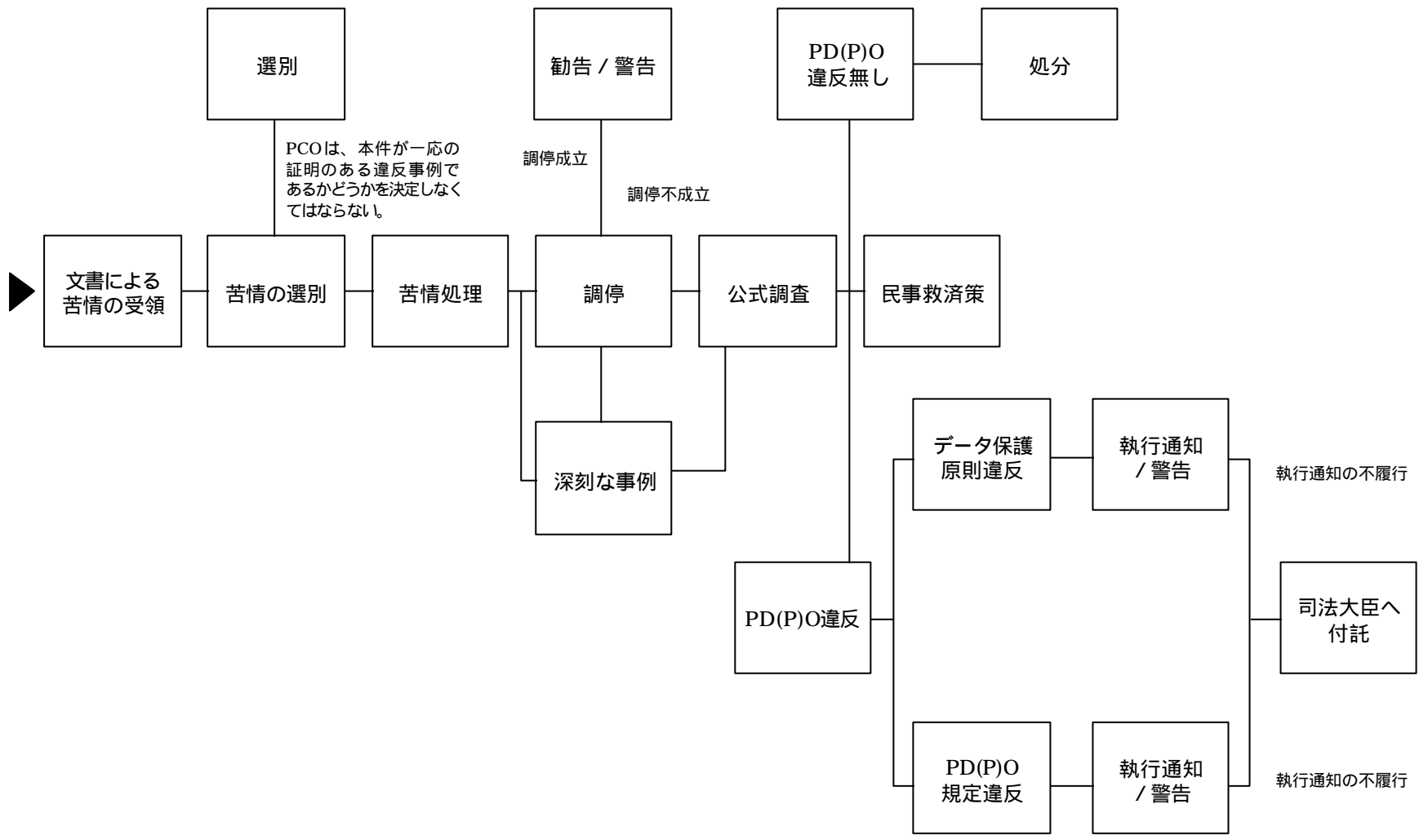
個人データのプライバシー権を侵害された個人に対する救済策とは何であろうか。この疑問にとっさに答えなくてはならないとすると、「個人データプライバシー・コミッショナー事務局に行き、苦情を申し立てる」という答えが出てくるであろう。個人データの侵害に対する救済策を求める場合、香港ではこれが最も早くて簡単で、費用のかからない方法であることは間違いない。もちろん他にも利用できる方法はあるが、当事者自らが費用を負担し、別個に行動を起こさなくてはならない。例えば、犯罪行為があつた場合には、被害者自らが不法行為者を相手取り、個人的に訴訟を起こすことが考えられるし、あるいは損害を被った場合には、被害者本人が不法行為者を相手取って民事訴訟を起こして賠償を求めるなどの方法が考えられる。この報告書では、それぞれの救済策についてより詳しく述べる。

パート A - プライバシー・コミッショナー事務局への苦情申立て

香港でデータプライバシーの侵害が疑われる事例に関して個人が利用できる救済策の一つは、不法行為者を相手取り、プライバシー・コミッショナー事務局(PCO)に苦情を申し立てることである。前述の通り PCO は、PC(P)D に基づいて設立された法定機関である。個人データプライバシー・コミッショナーは、法律のコンプライアンスを監視・監督する責任を負っている。この責任を果たせるよう、PD(P)O はプライバシー・コミッショナーに対し、PCO に申し立てられた苦情の調査を行う権限や、苦情調査終了時において適切な執行措置を講じる権限を与えている。

1996年12月20日にPD(P)Oが施行されて以来、PCOは、プライバシー権が侵害されたことを疑う個人からの問合せ10万件以上、苦情3,500件を処理してきた。苦情申し立てを支援するためにPCOに何が出来るか。またこのような違反行為の再発を防止するためにPCOが講じることのできる執行措置は何か。これらの疑問に関する議論の前に、まずPCOの苦情処理のワークフローを理解するのが良いであろう。

図表 5-2-1 は、PCO の苦情処理手順である。



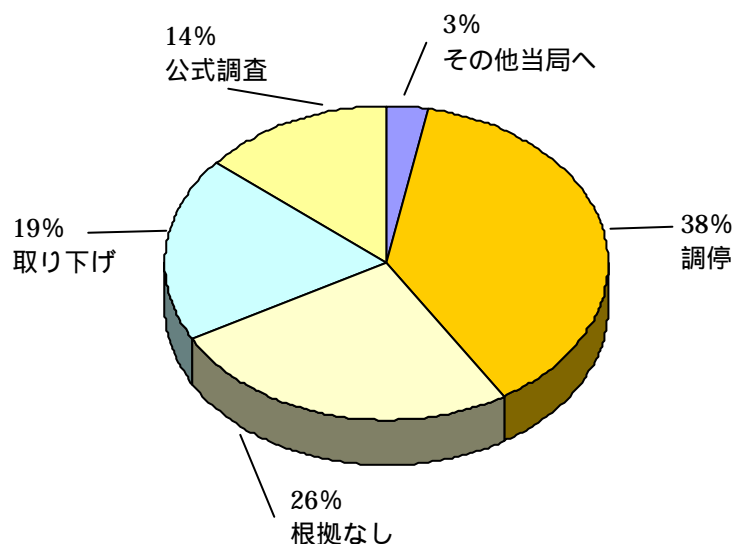
図表 5-2-1 苦情処理の流れ

(1) 苦情処理手順

苦情を受理した場合 PCO は、最初に、申立人及び「被申立人」のみならず、苦情に関する情報を提供することができると思われる証人など、苦情の関係者に対して予備審問を行う。予備審問の目的は、PD(P)O の規定に対する一応の証明のある違反事例にあたるかどうかを判断するための十分な証拠を得ることである。

一応の証明のある違反事例にはあたらないと判断された場合、その苦情に関して PCO はそれ以上の措置を一切取らないことを申立人に通知する。これに対して、一応の証明のある違反事例にあると判断され、苦情の性質が深刻なものではない場合、PCO は調停による解決を試みる。調停とは、申立人の納得が得られるよう、PCO の介入により被申立人が苦情の原因の解決のために自主的に救済策を講じる方法である。調停によって問題が解決できない場合、あるいは苦情の性質が深刻な場合は公式調査を行い、必要に応じて執行措置を講じる。

図表 5-2-2 は、2001 年に PCO が行った苦情調査の結果を示している¹。



図表 5-2-2 苦情調査結果

¹ 対象期間は 2000 年 4 月 1 日から 2001 年 3 月 31 日までとなっている。

昨年 PCO が処理した苦情は合計 385 件に上る。その内 146 件(38%)が調停によって解決され、52 件(14%)は公式調査後に解決されている。また 102 件(26%)は、調査により根拠のないものであることが明らかになり、73 件(19%)は調査中に申立人が取り下げている。残りの 12 件(3%)は PD(P)O の管轄外の申し立てであり、解決に向けてその他の当局に付託された。

(2) 調停による解決

図表 5-2-2 から、2001 年に PCO が処理した苦情の大半が調停によって解決されていることがわかる。調停プロセスにおいては、PCO が苦情に関する予備審問を行い、これに続いて、利用できる証拠に基づき苦情の対象となった行為に関する予備意見をまとめる。その後 PCO は、被申立人に対してその意見を通知し、苦情の対象となった行為を改善するための救済策を講じるよう求める。被申立人が救済策を講じることに合意した場合、その苦情は調停によって解決されたものとみなされる。

PCO が指定する救済策にはどのようなものがあるのだろうか。基本的に救済策は苦情の性質に大きく左右されるが、一般的には、大まかに分けて次のように分類される。

- 行った行為、あるいは関係している行動について謝罪する。
- PD(P)O の規定を遵守するため、次のような措置を講じる。
 - (a) 個人データの不正収集に関する苦情の場合、収集した個人データを引き渡す、あるいは破棄する。
 - (b) 個人データが不正確であることに関する苦情の場合、問題となっているデータを修正する。
 - (c) 個人データを必要以上に長期にわたって保持していることに関する苦情の場合、保持しているデータを破棄する。
 - (d) 個人データの利用の変更に関する苦情の場合、データ対象者の同意がある場合を除き、将来におけるそのような利用の変更を中止する。
 - (e) データアクセス要請が遵守されていないことに関する苦情の場合、要請のあった個人データのコピーを申立人に渡す。
- 行われた行為、あるいは関係している行動が二度と繰り返されないことを保証するための措置を講じる。

具体例として、PCO が処理した苦情事例のうち、調停によって解決に至った事例数件を以下に示す。

事例 1 - 貸金取立てにおける個人データの利用

申立人はある金融会社から借入を受けたが、支払いを怠った。その後、申立人は、金融会社から委託を受けた債権回収機関からの手紙を受け取ったが、その手紙の入った封筒の上に申立人の身分証明書のコピーが添付されているのを見つけた。申立人は、封筒に身分証明書のコピーを貼付けることにより債権回収機関は、申立人個人の詳細情報を他人に漏らしたと主張した。

PD(P)O の別表 1 に示されているデータ保護原則 3 では、データ対象者から規定通りの同意がない限り、データ収集時に指定されたデータの使用目的以外の目的、あるいはこれに直接関係する目的以外に個人データを利用してはならない、とされている。

我々の見解では、当該金融会社は申立人の同意なしに申立人の身分証明書のコピーを債権回収機関に渡していることから、データ保護原則 3 の規定に違反している。債務者の個人データを、債務者が支払いを怠った債権の回収を目的として利用することは、貸付を行った当初の目的と直接関係しているものと考えられる。しかし金融会社は、そのデータの開示を、債務者の氏名や住所、身分証明書番号など、目的の遂行に十分な範囲内にとどめるべきである。

PCO の助言に従い金融会社は、自らの行為に関して申立人に謝罪し、債務者の身分証明書のコピーを債権回収目的で使用することを止めると約束した。金融会社に対しては警告通知が出された。

事例 2 - データアクセス要請の受入に対する料金請求

ある患者がある医院に対し、医療用スライド 65 枚の複写を要請した。この医院は患者に対し、15,000 香港ドル近く(スライド 1 枚につき 230 香港ドル)を支払うよう請求した。患者はこの料金が高すぎると考え、PCO に苦情を申し立てた。

PD(P)O セクション 28 は、データアクセス要請の応諾に対しデータ利用者に料金を課すことを認めている。しかし、過度に高い料金を請求すべきではない。我々の見解では、料

金の設定に当たっては、データの所在場所の確認に必要な管理費用、ならびに個人データのコピーの作成に伴う実費を賄う為に合理的な金額を含めるのが望ましい。

PD(P)O セクション 28 が規定する個人データのコピー提供に関する費用の計算方法に対する PCO の見解を検討したうえで、当該医院は自らの方針を見直し、その後、料金を 468 香港ドル(スライド 1 枚につき 7.2 香港ドル)に引き下げた。これは、スライド作成のための実費に管理費を 20% 上乘せした金額である。

事例 3 - 身分証明書番号の収集

駐車場管理会社は申立人に対し、申立人が自動車を駐車するために駐車施設に入る際に、登録のため身分証明書番号を提示するよう要請した。駐車場利用者を登録する慣習は、以前、当該施設で起きた自動車盗難事件を考慮して、施設の安全及びセキュリティのために導入されたものであると管理会社は主張した。申立人は、請求されたデータは不必要なものであるとの根拠からデータの提供を拒否し、PCO に苦情を提起した。

データ保護原則 1(1)によると、個人データの収集は、データ利用者の職務、あるいは活動に直接関係する合法的な目的のために行われる場合に認められ、また集められるデータは適切なもので、目的に鑑みて過剰であってはならない。

PCO の見解では、自動車の盗難などの犯罪を防ぐことを目的とする場合、運転者の身分証明書番号を提示させなくても、一般的には、入場する自動車のナンバープレートの番号を駐車券や「出庫票」、あるいはクーポンに控えれば十分である。

PCO の助言に基づき管理会社は、駐車場利用者の身分証明書番号の記録を止めることに合意した。

(3) 調査及び執行措置

上記の通り、調停によって苦情を解決できない場合、あるいは苦情の性質が深刻なものである場合、PCO は公式調査を開始することが出来る。調査によりデータ利用者が PD(P)O の規定に違反していることが確認された場合、違反行為の是正のために必要な措置を講じることが指示する執行通知を該当するデータ利用者へ送達することが出来る。また PD(P)O はプライバシー・コミッショナーに、苦情に対して補償を与える権限を一切認めていない。したがって「執行通知」は、「調停による解決」で既に示されている救済策を含め、違反の是正に相当かつ必要であるとプライバシー・コミッショナーが考える措置に限定される。

PCO が処理した事例のうち、執行措置が取られた事例を幾つか挙げる。

事例 4 - インターネットを通じた誹謗

申立人によると、申立人のかつての同僚は、申立人に知らせることも、またその同意を得ることなくインターネット上の性サービスを勧誘するニュースグループのメッセージの中に申立人の氏名と携帯電話番号を載せ、その結果申立人には多数の迷惑電話がかかってきた。PCO による調査の結果、この元同僚は 2 人が同じ会社で働いている間に申立人の携帯電話番号を入手したことが確認された。メッセージの送信者は偽のアカウントネームを使って自らの身元を隠そうとしていたが、PCO は、関係するインターネット・サービス・プロバイダから、メッセージの送信元のアカウントは元同僚のアカウントであるとの証拠を得た。元同僚の元には、そのような行為を止めるよう指示する執行通知が送達された。

事例 5 - 電話によるダイレクトマーケティング

ある不動産所有者は PCO に対し、この不動産所有者が繰り返し不服を申し立てたにも関わらず、不動産を売却するよう不動産所有者を説得しようとして、不動産会社の職員が携帯電話を通じて連絡をしてくるとの苦情を申し立てた。

PD(P)O のセクション 34 によれば、ダイレクトマーケティングへの個人データの利用を止めるようデータ対象者がデータ利用者に要請した場合、データ利用者はそのような利用を止めなくてはならない。

PCO の調査の結果、この不動産会社は、今後のコールドコールの受入を拒絶した顧客のメッセージを記録するコンピューターシステムを導入していることが明らかになった。コンピューター上の該当する記録を調査すると、申立人は少なくとも 4 回、不動産を売却する意志がないことを伝える明確な指示を出し、また不動産会社に対して売却を勧める電話をかけることを止めるよう要請していることが確認された。しかし、担当職員は記録されているメッセージを無視した。同じ支店の別の職員の話から、この支店の職員は、PD(P)O の規定のコンプライアンスに関する十分な訓練を受けていないことも明らかになった。

これに基づき不動産会社に対しては、潜在顧客からの選択的離脱要請に従うよう、明確な指示を営業職員に出すこと、またその指示が確実に守られるよう、それぞれの営業職員の通話記録を監視・点検するよう指示する執行通知が出された。

(4) 執行通知に従わなかった場合の処置

PD(P)O セクション 64(7)により、送達された執行通知に違反したデータ利用者は、罪を犯したことになり、有罪判決が出た場合、罰金²及び禁固刑³に処される。また犯罪行為が続いた場合は日割り計算で罰金を支払わなくてはならない⁴。執行通知を送達されたデータ利用者が執行通知の条件に従うことを怠った場合、PCO はその事例を香港警察に委ね、香港警察がその事例を調査・起訴する。執行通知に従うことを怠ったためにデータ利用者が有罪判決を受け、罰金を課された事例を以下に挙げる。

事例 6 - 顧客データの不正な収集

申立人は、かつてホテルに勤務していた電話セールスコンサルタントが申立人やホテル幹部の許可を得ずに申立人の個人データを不正に収集・利用したと苦情を申し立てた。

最初、申立人は、ホテルの会員パッケージの販売促進を担当する電話セールスコンサルタントからダイレクトマーケティングの電話を受けた。非常に魅力的な会員パッケージを勧められたため申立人は会員制度に加入することに同意し、登録のために、詳しい個人的情報をこの電話セールスコンサルタントに教えた。しかしその後申立人は、会員制度の条件が、電話セールスコンサルタントが約束したものとまったく違うことを知り、ホテルに苦情を申し立てた。その後、同じような苦情が何件もホテル幹部に寄せられたため、この電話セールスコンサルタントはホテル側に解雇された。これを不当な扱いだと感じた電話セールスコンサルタントは、申立人の個人データの記録を入手し、そのデータを利用して申立人に何通ものファックスを送り、申立人のせいで自分は職を失ったと非難した。このため申立人はこれを PCO に報告した。

PD(P)O データ保護原則 1(2)により、この事例の状況においては、個人データは合法で公正な方法で収集されるべきである。

調査の結果、この電話セールスコンサルタントは PD(P)O データ保護原則 1(2)に違反していることが明らかになり、申立人の情報をホテルに返却するよう指示する内容の執行通知が出された。

² 刑事手続法(香港法第 221 章)セクション 113B 及び別表 8 により、現在の罰金の最高額は 5 万香港ドルとなっている。

³ PD(P)O セクション 64(7)により、禁固刑は最高 2 年である。

⁴ PD(P)O セクション 64(7)により、日割り計算の罰金は 1,000 香港ドルである。

しかし電話セールスコンサルタントは執行通知を守らなかった。その後この事例は警察に委ねられ、PD(P)O セクション 64(7)に基づき起訴手続きをとるべきかどうか検討された。

電話セールスコンサルタントは警察による調査において執行通知の受取を否認した。しかし電話セールスコンサルタントに重大な時期に執行通知を送達した PCO 役員は、数多くの容疑者を見たうえで、この人物が受け取った本人であるとの判断を下した。これにより電話セールスコンサルタントは告発された。事情聴取により、電話セールスコンサルタントは執行通知の不履行のため、有罪とされ、罰金を科された。

(5) 報告書の公表

PD(P)O セクション 48(2)により、調査終了後、プライバシー・コミッショナーが公共の利益にかなうと判断した場合、プライバシー・コミッショナーは調査の結果や、調査に基づく提案あるいはコメントを記載した報告書を公表することができる。当該データ利用者に対する制裁として、その報告書の中で当該データ利用者の身元を明かすことも出来る。

以下に挙げるのは、苦情の調査を行ったうえで PCO が報告書を発表した事例である。

事例 7 - 私的な場所にいる個人の隠し撮り

ある地方大学生が、自分が寄宿寮にいる間にビデオで隠し撮りされていることを発見した。ビデオカメラは箱で覆われており、彼女が同じ大学の学生と共有している部屋のキャビネットの一番上に設置されていた。カメラには彼女の映像が入ったビデオテープが入っていた。彼女は PCO に苦情を申し立てた。

調査の結果、ビデオカメラを設置したのは彼女のルームメートの友人であることがわかった。この友人は、数ヶ月の間に 3 回に渡って申立人の映像をこのような方法で記録したことを認めた。被申立人は、部屋の中での申立人の行動をビデオカメラで撮影したのは、申立人の知り合いが正当な許可を得ずに敷地内にいることを示す証拠を得るためであったと主張した。更に被申立人は、そのうちの 1 枚を友人に見せたことも認めた。

データ保護原則 1(2)(b)では、この事例のような状況の場合、個人データは公正な方法で収集すべきであると規定されている。最優先される公共の利益がなければ、本人に知らせることも、同意を得ることもせず、個人データを収集することを意図して、プライベートな場所にいる間にその個人の映像を写真やビデオに納めることは不公正である。さらに、

申立人のビデオ映像を本人の同意を得ずに他人に見せることは、データ保護原則 3 に違反する。

被申立人に対しては、ビデオを回収して申立人に引き渡し、そのようなテープのダビングや使用、また他人に見せることを止めるよう指示する執行通知が送達された。

セクション 48 に基づいて報告書が公表されたが、この報告書では、PD(P)O が定義する個人データの収集に当たらない電子的監視行為に起因するプライバシーの深刻な侵害への対応の面で同法が不十分であることが強調された。

パート B - 刑事訴追の請求

個人が利用できるもう一つの救済策は、刑事訴追の請求である。PD(P)O セクション 64(10)によると、合理的な理由なく PD(P)O のいずれかの規定に違反した(データ保護原則の違反以外に)データ利用者は、法律違反を犯したものとみなされ、有罪の判決が下った時点で罰金を科される⁵。ここで注意しなくてはならないのは、データ保護原則に対する違反は、法律違反ではないということである。刑事訴追の可能性が生じるのは法律の規定が犯された場合のみである。例えば、データ利用者が、PD(P)O セクション 19(1)の規定に違反して、データアクセス要請の受領日から 40 日以内にその請求に従うことを怠った場合、あるいは PD(P)O セクション 34(1)ii の規定に違反して、ダイレクトマーケティング目的で個人データを利用することを止めるようデータ対象者がデータ利用者に対し要請した後もそのような目的で個人データの利用を続けた場合などである。

PD(P)O の現在の規定では、プライバシー・コミッショナーは刑事犯罪の調査を行ったり、刑事訴追を請求する権限を与えられていない。一方、PCO による調査の過程で集めた証拠から、強制調査や刑事訴追が適当であるとされている PD(P)O セクション 64(10)に基づく犯罪行為があったとの合理的嫌疑が生じた場合、PCO は申立人の同意の下、その事例を香港警察に委ね、香港警察がその事例を更に調査した上で、司法省が訴追手続を取る。

もう一つの方法として、個人が自ら行う私人訴追がある。しかしこの方法はほとんど利用されていない。1996 年 12 月に PD(P)O が施行されて以来、PD(P)O に基づく私人訴追を行った個人は、わずか 1 名にとどまっている。下級判事による決定の司法審査⁶の中で、高

⁵ 刑事手続法(香港法第 221 章) セクション 113B 及び別表 8 に基づき、適用される罰金の最高額は現在 10,000 香港ドルである。

⁶ ジアン・エンズー対エミリー・ラウ・ワイヒン[1999 年]3 HKC 8

等裁判所第一審裁判所が、下級判事が被申立人に対して交付した召喚状の一部の法的事項を無効としたことにより、この起訴は頓挫した。

上記の事例は失敗に終わったが、私人訴追がデータプライバシー権の侵害に対して取りうる救済策の1つであることに変わりはない。

パート C - 民事訴訟

個人データプライバシーの侵害に関して個人が取りうるもう一つの救済策としては、当該データ利用者を相手取り民事訴訟を起こす方法がある。PD(P)O セクション 66 により、データ利用者が PD(P)O の規定に違反したことが原因で、感情を傷つけられるなどの損害を被った個人は、その損害に関して当該データ利用者から補償を受ける権利がある。このような民事訴訟はあまり行われていないが、損害を証明することが難しく、これに関わる訴訟費用も多額に及ぶことが原因となっているものと思われる。

しかし PD(P)O セクション 66 に基づいて補償が請求された興味深い事例⁷もある。PD(P)O の規定に対する違反が一切無いとの理由から、この請求は最終的には裁判所に却下されたが、個人データプライバシーの侵害があれば、補償を要求する権利が発生することが裁判所によって明確に示されたのである。

この事例の申立人はレストランのチーフシェフであった。彼は、レストランの同僚であるレジ係が、チーフシェフから事前の同意を得ずに広告にチーフシェフの氏名を載せたことによりチーフシェフの個人データプライバシー権を侵害したと主張し、レジ係に補償を求めた。問題の広告はジュニアシェフ募集のための広告であった。広告は申立人を連絡先として指名するものであった。裁判所は、応募者の面接を行い、マネージャーによる選択の対象となる応募者の選抜候補者リストを作成することにより採用を補佐することは申立人の責務であるとの判断に至った。応募者が申立人に連絡するために広告に掲載されている氏名によって申立人を特定することは、その特定によって、申立人が自らの責務の一つを果たすことができるのであるから、雇用主がそのデータを収集した時点における個人データの使用目的と直接関係している、と裁判所は判断した。したがって裁判所は、広告の中で申立人の氏名を使用することは、PD(P)O のデータ保護原則 3 に違反するものではない、との判決を下した。

⁷ クワン・チー・シャン対イェン・イン・フォン(1997年のDCCJ 7812)、未報告

広告の中に氏名を掲載されたことがもたらした申立人の苦痛に起因する損害に対する請求権に関して裁判所は、申立人の個人データプライバシー権が侵害された場合にそのような補償が発生する、との結論を示した。個人データプライバシー権が侵害されたとの結論は得られなかったことから、裁判所は、申立人がこのような損害賠償を受けることは出来ないとの結論を出した。

申立人は、素性の良くない人物が、何らかの理由から傷つけたいと考えている人物で申立人と同じ名前の人物と申立人を間違え、レストランに来て申立人に損害や危害をもたらす恐れがあるとの根拠に基づき、自らの申し立てを弁護した。裁判所は、この考え方はあまりにも不自然であり、被申立人がこのような苦痛を予見することは出来なかったとの結論を示した。したがって、たとえ申立人の個人データプライバシーの侵害があったとしても、被申立人が予見することのできなかった損害に関する責任を被申立人に負わせることは出来ないから、この苦痛の申し立てに基づいて損害賠償を得ることは出来ない。

この事例は、個人データプライバシー権の侵害があった場合は補償金の支払を裁定する準備が裁判所にあることを示している。しかし、被った損害が当該不正行為者には予見出来ないものであった場合、不正行為者にはなんら責任は無い。

前述の通り、プライバシー・コミッショナーは補償金を裁定する権限を一切与えられていない。したがって、個人が不正行為者から補償を得るためには、民事訴訟を起こすことが唯一の手段である。

結論

結論を述べると、個人データプライバシーの侵害に関して個人が利用できる救済策は多岐に渡る。しかし、個人データプライバシーの侵害に対する救済策を最も効率的・効果的に、また経済的な方法で得ることの出来る場所がPCOであることに変わりはない。自分の個人データプライバシー権を守るために香港の人々が頼りにするのがPCOであることは間違いない。

より長期的に見て、より厳密で厳しい救済体制と教育的アプローチと、どちらの方が、我々の地域社会における個人データプライバシーの相互尊重の促進という利益によりかなっているかどうかという、より大きな問題は未解決である。

レイモンド・タング
個人データプライバシー・コミッショナー
香港 SAR
2002 年 11 月 28 日

個人データプライバシー・コミッショナー事務局
Unit 2401, 24th Floor, Office Tower, Convention Plaza
1 Harbour Road, Wanchai
Hong Kong
電話：(852) 2827 7168
ファックス：(852) 2877 7026
電子メール：pc@pco.org.hk
インターネット：<http://www.pco.org.hk>

(2003 年 2 月にて事務所移転された新たな住所に更新しています。)

付録：「個人データ(プライバシー)法」

別表 1

データ保護原則

1. 原則 1 - 個人データ収集の目的及び方法

- (1) 個人データの収集は以下の場合にのみ認められるものとする。
 - (a) そのデータを利用するデータ利用者の機能あるいは活動に直接関係する合法的な目的のために収集される場合。
 - (b) (c)を満たしており、データ収集がその目的のために必要である、あるいは直接関係している場合。
 - (c) その目的に鑑みて、データが適切であり、過剰ではない場合。
- (2) 個人データの収集方法は以下の条件を満たすものとする。
 - (a) 合法的である。
 - (b) その事例の状況において公正である。

(3) 個人データを提供する人物、あるいは提供することになっている人物がデータ対象者本人である場合、以下の事項を確実にするためにあらゆる実際的措置を講じるものとする。

(a) データを収集する以前に、明示的あるいは暗示的に以下の事項をデータ提供者に知らせる。

(i) そのデータの提供は義務なのか、あるいは任意なのか。

(ii) データの提供が義務である場合、データ提供をしなかったらどうなるのか。

(b) 以下の事項をデータ提供者に明示的に知らせる。

(i) データ収集以前に知らせる事項

(A) データを利用する目的(一般的目的あるいは特定の目的)

(B) データを伝える可能性のある人物の階級

(ii) データ収集目的のためにそのデータを初めて利用する以前に知らせる事項

(A) データに対するアクセスを要請する権利、またデータの修正を要請する権利

(B) そのような要請の養成先となる個人の氏名及び住所

但し、このサブセクションの規定に従うことがデータ収集の目的を損ねる可能性が高い場合で、本法のパート VIII において、データ保護原則 6 の規定の個人データへの適用が除外される利用目的として明記されている目的に利用される場合を除く。

2. 原則 2 - 個人データの正確性及び保持期間

(1) 以下の事項を確実にするために、実行可能なあらゆる措置を講じるものとする。

(a) 個人データを利用する、あるいは利用することになっている目的(直接関係する目的を含む)に照らして、個人データが正確であること。

(b) 個人データを利用する、あるいは利用することになっている目的(直接関係する目的を含む)に照らして、個人データが不正確であると考えるに十分な根拠がある場合、以下のいずれかを確実に実行する。

(i) データの修正あるいはその他の方法でその根拠がそのデータに該当しなくなるまで、その目的ではデータを利用しないこと。

(ii) データを削除すること。

(c) その事例のあらゆる状況において、

- (i) 指定された日以降に第三者に開示される個人データが、第三者が個人データを利用する、あるいは利用することになっている目的(直接関係する目的を含む)に照らして、著しく不正確であること、また
 - (ii) 開示の時点でデータが不正確であったことを知ることが可能である場合、その第三者が
 - (A) データが不正確であることを知らされていること。
 - (B) その第三者が目的に照らしてデータを修正できるよう、詳細な情報を提供すること。
- (2) 個人データは、個人データを利用する、あるいは利用することになっている目的(直接関係する目的を含む)の実現に必要な期間を超えて保持しないものとする。

3. 原則 3 - 個人データの利用

個人データは、データ対象者からの規定に沿った同意がない限り、以下の目的以外の目的に利用しないものとする。

- (a) データの収集時において予定されていたデータの使用目的
- (b) 上記(a)に記載されている目的に直接関係する目的

4. 原則 4 - 個人データのセキュリティ

データ利用者が保持している個人データ(データへのアクセス、あるいはその処理が実行できないような形式のデータを含む)が、許可のない、あるいは不慮のアクセスや処理、削除、その他の利用方法から確実に保護されるよう、特に以下の点に留意して、実行可能なあらゆる措置を講じるものとする。

- (a) データの種類、ならびに上記のいずれかの問題が発生した場合に生じうる損害
- (b) データの物理的保管場所
- (c) データを保管している機器に(自動的手段で、あるいはその他の方法で)組み込まれているセキュリティ対策
- (d) データにアクセスする人物が正直かつ慎重で、アクセスするにふさわしい人物であることを確認するために取られている手段
- (e) データの安全な伝達を確保するための手段

5. 原則 5 - 一般的に入手できる情報

以下の事項が可能なように、実行可能なあらゆる措置を講じるものとする。

- (a) 個人データに関するデータ利用者の方針及び慣習を確認すること。
- (b) データ利用者が保持している個人データの種類を知ること。
- (c) データ利用者が保持している個人データが使用される、あるいは使用されることになっている主な利用目的を知ること。

6. 原則 6 - 個人データへのアクセス

データ対象者は下記の権利を与えられるものとする。

- (a) データ利用者が、自分を対象とするデータを保持しているかどうかを確認する権利。
- (b) 以下の条件で個人データにアクセスすることを要請する権利
 - (i) 合理的期間内にアクセスできる
 - (ii) 費用がかかる場合は適度な費用でアクセスできる
 - (iii) 合理的な方法でアクセスできる
 - (iv) わかりやすい形でアクセスできる
- (c) (b)で述べた要請が拒否された場合、その理由を知らされる権利。
- (d) (c)で述べた拒否に抗議する権利。
- (e) 個人データの修正を要請する権利。
- (f) (e)で述べた要請が拒否された場合、その理由を知らされる権利。
- (g) (f)で述べた拒否に抗議する権利。

5.3 アラン・ウェスティン教授来日、ECOM 来訪

2002年9月のECOMとして実施した北米調査・視察時、訪問し、レクチャーを受けたコロンビア大学名誉教授であり、「社会と法研究センター（Center for Social & Legal Research）」会長のアラン・ウェスティン氏が、2003年1月に来日した。

ウェスティン教授は、今後行う予定の消費者プライバシーに関する事前調査とマスコミ取材を受ける目的で来日されたが、ECOM会員企業のスタッフからも電子商取引に関する意見や状況を聞きたいとのことで訪問された。

5.3.1 アラン・ウェスティン教授との懇談会実施概要

日 時： 2003年1月23日（木）10:00～12:00

場 所： 機械振興会館 6階6-61会議室

出席者： アラン・ウェスティン教授 / 祖父江純氏

川城三治氏（グローバルフレンドシップ） / 藤原康明氏（電事連） /
中島和雄氏（東芝） / 脇田正敏（トヨタ） / 荒木吉雄氏（日本IBM） /
上野正之氏（日本信販） / 東山治郎氏（松下電器） /
伊東正晴氏（三井住友海上） / 佐賀真一氏（朝日監査法人）
新保史生氏（筑波大学） / 鈴木正朝氏（ニフティ） /
鈴木靖氏（CPデザイン） /
成瀬一明 / 江口正裕 / 浅沼省吾 < 議事 > （以上 ECOM）

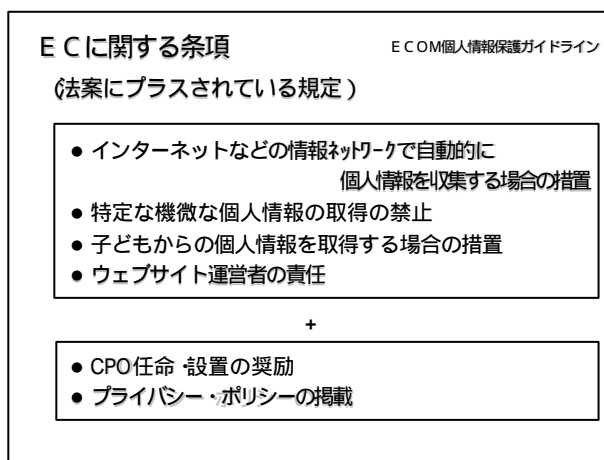
5.3.2 議事

ウェスティン教授 来日の目的

- ・ 日本の消費者のプライバシーの意識に関するアンケート実施に先立つ事前調査（1999年に一度実施、今回も主婦連等ともディスカッションした）
- ・ 日本の個人情報保護法の法制化は必要 国会通過がならない原因の考察
- ・ Eコマース、インターネットでプライバシーの保護を消費者はどのように考えているのかについて ECOM 会員との意見交換

ECOM 活動報告

- ・ ECOM ガイドラインや主な活動については、9月訪米の折、一度報告した。昨年末にリリース予定だったが、法案通過を前提としていた。結果的に廃案、または修正案の再提出という状況になったので、リリースはペンディング状態。その間、ワーキングの中で



図表 5-3-1

ディスカッションを重ね、その中で上がってきた内容を反映させている。今の予定では、法案の修正案が出たのち、ワーキングのミーティングの中でそのリリースのタイミングを再検討して、早期にリリースしたい。

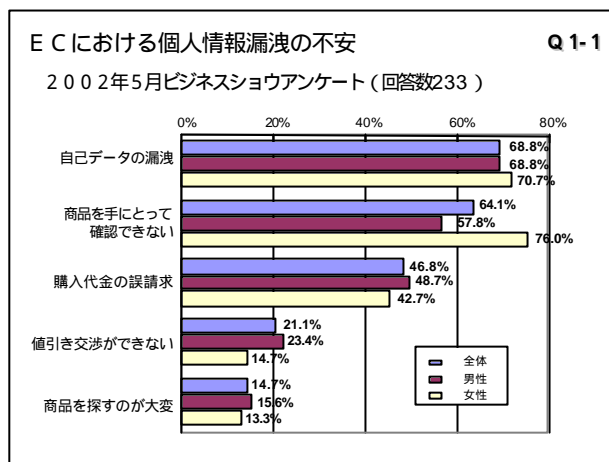
- ・ 9月のウェスティン教授訪問時の後に、法案に無い、ECの要件としてECOM独自の規定として考えた内容は2つ。1つは企業としてCPOの設置を奨励すること。それと、ウェスティン教授にご提案いただいた、プライバシーポリシーをWebサイト上にきっちり載せていくということを加えた。
- ・ 実際には法案が通過するタイミングよりも早くリリースする予定。その後、法案の内容に変更等があったら修正、見直しをする。
- ・ **祖父江氏より質問** 12月に与党修正大綱案というのが出て、昨日 日経の記事が出ましたが、与党案とのその違いは？そのドラフトはあるか？
- ・ **回答（浅沼）** 内容的には同じ。12月の臨時国会の末よりの与党案通り。関係部門に問い合わせしてみたが、公表するような形の文書は出されていないということ。

（質問1）

ECOM及び会員企業の方々のご意見として、日本の大半の消費者は、日本のサイトを訪れた時にプライバシーに関する通知があることを期待しているものでしょうか？もしそうであれば、こうした消費者の主な懸念はどういったものでしょうか？

- ・ **ニフティ 鈴木正** 消費者は、自分の個人情報がどのように取り扱われるかについては当然強い関心があるだろう。しかし、企業から個人情報について、具体的に有益な情報を提供してもらえという期待感は現在のところあまりないのでは。プライバシーポリシーの担当宛に、毎日会員や利用者から問い合わせが入ってくるが、その大半は、迷惑メールとか、コンピュータウィルスとか、個人情報とは関係がないものが多い。また、本人は個人情報の問題と意識しているけれど、実際は別の問題であることも多い。純粋なプライバシー・個人情報の問題での問い合わせは全体から見ると、決して上位ではない。無論、潜在的には不安はあるのだろうと思うが。
- ・ **CPデザインコン 鈴木靖** 日本の企業で個人情報についてステイットメントをあげている企業は総数から見れば多くない。また、企業による特色のあるステイットメントか

という決してそうではなく、似かよったステイメントを出して終わっている。一部の企業で、子供向けに解りやすく解説するとか、表現を変えている会社もあるが、ごく少数。それについては消費者側からも、やはりそれ以上の要求がないと思われ、企業もステイメントにそれほどこだわりを持たず、そこで終わっているのが現状。しかし、一部のインターネット利用経験が長い人達が、個人情報の取り扱いについて関心を持ちつつある。その発言は、インターネットの掲示板などに、ある種悪意を持って書き立てるような気持ちで書かれることもあり、むしろそのこと消費者を他の消費者が関心を持つことも多い。現状は、ECOMの方で出されている資料にありますように、自己データの漏洩だけではなく、商品そのものに対する不安だとか、購入代金の誤請求とかに関心が高いと思うが、あるところで騒がれると、やはりそちらに関心が向く。



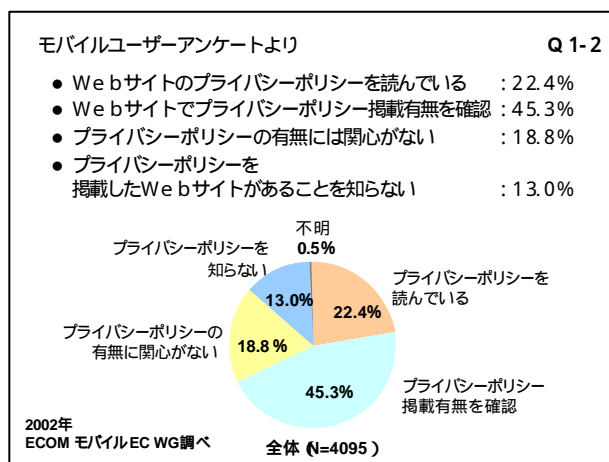
図表5-3-2

つまり、一般の消費者は企業が示す個人情報に関するステイメントに関心を持つというよりは、自分と同じ消費者の立場の方が、個人情報の取扱を含めその企業に対してどう評価したかということにむしろ関心が向くのだと思う。

- ・ 司会(浅沼) モバイルユーザーの調査では、Webサイトのプライバシーポリシーを

読んでいるかに対し、読んでいるが22.4%。Webサイトでプライバシーポリシー掲載有無を確認しているが45.3%。この結果は、意外に高いように思う。

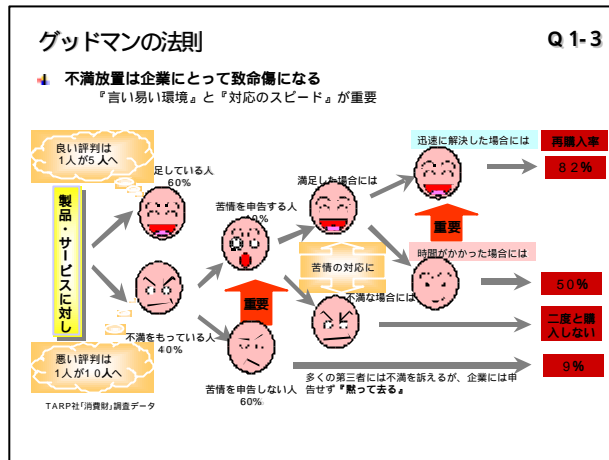
要因としてはここ1年、個人情報の漏洩や住基ネットの関連についての報道がされたことや、回答した



図表5-3-3

対象者が携帯のWebサイトを見るユーザーであることもあるが考えられる。

- 朝日監査法人 佐賀** まず、日本は国民性もあるが、プライバシーへの関心が非常に低い。ウェスティン教授が期待しているようなプライバシーの漏れる関心のレベルにはない状態ではないか。ただ、確かに機運は高まっていて、その一例として、住基ネットワークへの住民の関心などがあると思うが、すべての人が関心を持っているわけではない。



図表5-3-4

- こちらにグッドマンの法則というのがあるが、まず、プライバシーに関して関心を持っているというのは、先ほどのアンケート調査のように、もっと少なく、一部の方だけが関心を持っているのではないか。表面的には関心があるような方については、一部の方の意見、噂などといったものが影響しているから、あたかも関心を持っているようにとられるのではないか。どちらかということと日本国内のプライバシーへの取り組みは、B to Cという形で考えると、C主導ではなくて、B主導型のプライバシーと言える。大企業では、諸外国の情報をふまえて自らの防衛策としてプライバシーポリシーを掲載しているというのが実状か。一部の人の評判が数多くの人の評判になることを期待している。企業としては、一番期待しているのは、CRMという観点から、口コミを期待している部分もある。企業側から一番恐れているのは、逆に悪い噂の広がりである。それを押さえるための一つの要因が個人情報保護への取り組みとも言える。もう一つ付け加えると、苦情対応というのが大きな問題になっている。どちらかという個人情報保護の観点からは、リスクを発生させないということに主眼を置いて、リスクが発生した後の対応策にはあまり重点を置いていないのが現状。日本国内ではJIS Q15001の中にも苦情対応という注意事項があるが、たいへん簡潔にまとめられていても、企業としてどうしていくべきかについてはなかなか理解しがたい。要約すると、消費者はあまり関心がなく、どちらかということと企業主体であるのが今の日本の現状か。
- ウェスティン教授** 以前から、個人情報漏洩に関する記事等が取り上げられたりしていますが、消費者がそのような心配をするといった背景には、やはりメディアが重要

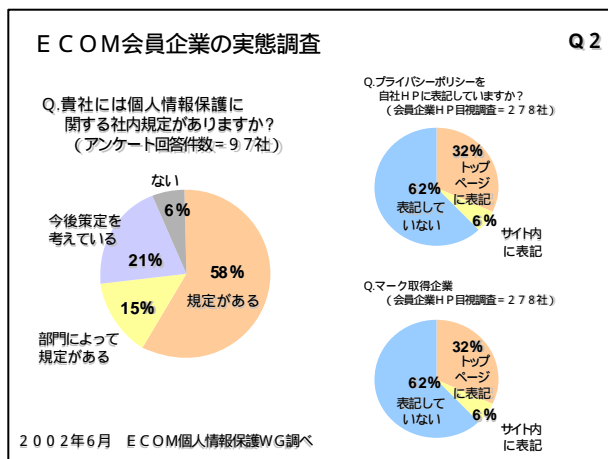
な役割を果たしているのでは。

- ・ **朝日監査法人 佐賀** その通りですが、加えて、Web上に企業の批判サイトというのがあり、そこで情報の漏洩があるというのがよくあるケース。従来は、口コミが企業に対して悪影響を及ぼすといったことだったが、最近はマスメディアもあり、また、Webサイトに掲載することによって不特定多数の方に一瞬にして広まってしまっている。
- ・ **司会（浅沼）** 去年、個人情報の漏洩は22件か23件位の事故があったと報告されている。しかしながら、Web上の漏洩事件を含むとより多くの件数、また、たくさんの人が見ているということになるかもしれない。

（質問2）

おおよそ有名企業の何割のサイトが、現在ホームページで個人情報に関する通知を行っているのでしょうか？

- ・ **司会（浅沼）** ECOMの約300社の企業に対してアンケートと、それぞれの会社のWebサイトを目視調査した結果をご覧いただきたい。この結果からすると、個人情報について社内規則を持っているところは7割を超えているのに対して、Webサイト上で個人情報保護方針、あるいはプライバシーポリシーを表記しているところは4割にも満たないというのが実態。アメリカにおいては9割近くの会社が掲載しているのとは比べ、大きく乖離している。また、日本全体の企業の実態を考えると、これと同等かそれ以下であると推測される。



図表5-3-5

- ・ **ウェスティン教授** アメリカでは、97年からつぎのような傾向が見られる。企業がオンライン・プライバシー・アライアンスというような自主的団体を作る傾向がその一つ。企業団体が同盟を作って自分達でやるから法的規制は必要ないという態度を打ち出して、業界団体、企業団体として取組んでいる。もう一つ、企業が一生懸命にな

っている理由に、アメリカでは公正取引委員会がオンラインを利用した調査活動を積極的にやっているという事実がある。サイトを調べたり、あるいはランダムに何千の企業の調査をしている。そして、やはり企業にとっても個人情報保護の重要性を訴えている。

- ・ **司会（浅沼）** 法律でステイトメントを義務づけるのはナンセンスであり、やはり企業の方で自主的な取り組みをするのが重要だと思う。ECOMでもそのような形のポリシーの掲載を奨励していくようなガイドラインにしていく。一方でその徹底のための公的機関の監視というのにも必要なのかもしれない。

（質問3）

日本のオンラインユーザーはそういった個人情報に関する規約が掲載されているサイトに対して高、中、低、どの程度の信頼を置いているのでしょうか？（アメリカでは、TRUSTe、BBBOnline、あるいはWeb Trustからのプライバシーマークがない場合は、通常低～中程度の信頼となっています。）

- ・ **日本信販 上野** プライバシーマークの目的は企業の社会的な信用であろうが、日本の場合は、まだ消費者のプライバシーマークに対する認知度がまだまだ低い。実際は、企業がアウトソーシングで情報処理の委託するデータ処理を受ける企業の取得が進んでいるが、まだまだ一般の消費者の認知には至っていない。カード業界は直接消費者との関係が深いですが、まだまだ積極的な企業は少ない状況。実際、消費者は企業の知名度とか、ブランドとかが判断基準になっている。また、企業もブランドイメージを傷つけないよう取り組んでいるのが実情。

プライバシーマークは、取得したことはニュースにならないが、取り消しをされた時にはマスコミが大々的に報道される。企業にとって、取得するメリットと現実が一致しない。

プライバシーポリシーの掲載については、同業他社が載せているので、当社も他社に比べて個人情報保護の姿勢が遅れぬようにと掲載した。対外的に発表するにあたり問い合わせが殺到するのではないかとということを危惧したが、実際には当初数件問い合わせがあったくらい。その後は、個人情報に対する問合せはほとんどないのが現状。

- ・ **東芝 中島** 東芝でもプライバシーマークをホームページに掲載しているが、信頼が

どれほどあるかはわからない。一部のプライバシー問題に関心の深いユーザーは、取得が大変だということを知っているのでマークがあるということだけで信頼してくれるようだが、一般のユーザーの関心はまだそれほど高くない。積極的にそれを営業・活用するといったところまでは行かない。コンプライアンスが大変だということは2面あると思う。1つは取得が大変だから信頼性もあるということ。もう1つは、大変だから普及はまだしていないということ。

- ・ **ウェスティン教授** 大変だという話が出ているがなぜか。普段はドキュメントしないようなものも文書化するようなことが必要とか、情報システムを統合させなければならないといった面があるからなのか。それともアメリカのBBBオンラインやTrusteのように、マークを取得してしまうと、今までは収集できた情報も取得できないのではないかという懸念が企業にあるからなのか？
- ・ **東芝 中島** 一つはマークを取ると、キープするために全社的にシステムチックに情報システムを作る必要がある。そういうシステム的な面と、もう一つはコンプライアンスプログラムを作って、それを全社的に検討していかなければならないということ。
- ・ **ウェスティン教授** アメリカでは、優良企業はこれでコントロールができる、真の監査ができるという非常にポジティブなシステムと考えている。これできちんとした情報管理ができるという非常によいシステムと考えている。
- ・ **筑波大学 新保** アメリカの企業、BBBオンラインマーク、相互認証マークに関してですが、そもそも自主規制に対する日本の企業の考え方が根本的に違うということが、今日のプライバシーマークに非常に大きく影響していると思う。アメリカの企業で自主規制といっても、ある特定の業界で、過度な規制を事前に予防するために自主規制を積極的に行って法規制の網をかけられないようにする。さらに消費者に対しては積極的にアピールをするための材料にするといった面があると思う。

日本の場合は、まず自主規制についての考え方が、そもそも自主規制を行うことが政府に対する法規制の防御といった観点ではなく、消費者に対してといった観点がある。マークというある意味ではブランド意識の確立、マークの取得によってある一定のレベル以上のことを行っているという意識がある。自主規制に対しては、消費者に対して積極的に行うというよりは、むしろ、企業内部での自主規制に対する考え方が根本的に違うので、その結果、Webサイトで例えばプライバシーポリシーを掲載するという考えについても、ほかの企業が掲載していたら、それに合せて掲載する。実質的に

は、消費者保護の観点からすると、本来は消費者保護をこれだけするというのを世の中にアピールするのを目的として、掲載すべき。その業界の内部における、悪く言えば護送船団的な、一定の範囲に限られた、横並び的なステイメント掲載に陥りがちと思う。

- ・ **祖父江氏** 私の仮説ですが、日本の場合 資本主義自体に関する考え方が、物売るという関係性で考えているのではないかと。欧米の場合では、物売るということを越えて、お客様との関係性を大事にしていくことがビジネスの元である。生涯において儲かるという形でお客様と関係性を作っていくのだという前提で、プライバシー問題を捉えているのではないかと。そうすると、マーケティングの観点からもプライバシーきちんとすれば、お客様との信頼関係が強くなると考えられているのではないかと。積極的に「我が社とお客様との関係性を作るものがプライバシーなのだ。」という意識で、基準づくりなども行なわれることが望まれるのではないかと。物売るという資本主義スタイルから、お客様との関係性という方向に発展したかたちで、プライバシーの問題を考えるべきでは。
- ・ **筑波大学 新保** 欧米の場合は、個人情報に関する姿勢、意識、プロセスが、いかに有用性に配慮して効率的に利用するか、効率性を重視しつつ消費者保護の観点でそのバランスを探求して利用している。ところが、日本の場合は、適正というよりも義務、重みという観点でとらえられている。今まで個人情報に関して、コンプライアンスプログラムを作成するということになかったこともある。製品に関しては、ある程度製品の品質の基準を明確に設定する必要があると思っているが、情報に対しては、こういった情報の取り扱いに対しては、プロセスを考える時点で、そのこだわりがなかった。
- ・ **ウェスティン教授** 単にマーケティングというよりも、「パーミッション・マーケティング」と我々が呼んでいる方に入る。お客様の情報を効果的にいただいてマーケティングを行うなら、お客様に気持ちよく情報を提供してもらわなければならない。「個人情報を頼みますよ」という約束と引き換えに、そうした情報をもろうというマーケティングの手法である。
- ・ **司会（浅沼）** 日本の企業が決して顧客満足に対する意識は高くないとは思わない。むしろ欧米に負けないぐらいに顧客満足ということが各企業でも取り組んでいる。ただ、その中のプライバシーということについては、日本で商売する中でプライバシ

ーの問題が今までそれほど大きく取り上げられてなかったこと、インターネットという新しいチャンネルができる中で、日本の場合は、ヘッドクォーターと現場の間の政策を共有化していくことが、顧客対応の権限委譲が進んでいたばかりに、新しい環境になって対応がなかなかむづかしいといった状況になっているのではないか。

顧客満足自体は、物を売るということ以上に大事なことと考えている企業が多いと思うその意味では、この命題については、日本の場合は、逆に、第三者の認定よりも、CSを含めた企業のブランドイメージが消費者の判断の大きな要素になっているのではないか。

(質問4)

個人情報を個人ID情報盗用の目的で不当に収集することに関する消費者の懸念は、日本で高まっているのでしょうか？ アメリカではかなり大きな問題となっています。

- ・ **日本信販 上野** 日本においては、ネットショッピングでは実際にあまり問題はないというのが実態か。どちらかという、リアルな場面においての盗難やカードを使った時にデータがスキミングされ偽造カードが作られ不正使用されたという問題が多く、ネット上で情報が盗用されたという事例はまだあまりない。現時点でのネット上でのトラブルは、リアルの世界で不正に取得されたカードやその情報がネット上で不正使用されるケースが多いようである。

ただ、消費者にとっては、ネット上で決済する時にカードナンバーを入力して大丈夫か、誰か情報データを不正に取得するのではないかという心配は非常に多いと思う。当社のHP上で個人情報を収集する際は、暗号化をしてセキュリティがかかっていることを消費者に示している。

(質問5)

日本の企業の間では、日米連携オンラインプライバシーマークをJIPDEC・BBBOnline間で設立することにあまり興味が集まっていないようですが、なぜでしょうか？

- ・ **筑波大学 新保** (JIPDECへの) 問い合わせはかなりあった。しかし2つの面から認証マークの取得にはあまり積極的ではない。1つは、実際に日本企業では必要性が

認められないという点。英語のページで海外の消費者を対象に個人情報を取得する際にマークを提示するだけでは、あまり必要性がない。2つ目は、BBBOnlineの認証を受けようと思ってリンクする際に、米国法にも準拠する必要がある。その際、コンプライアンスプログラムに参加することによって実質的な負担がさらに増えるということ。

- ・ **ニフティ 鈴木正** まず大前提として、日本国内においては第三者認証制度に関する認知が薄いのではないかと。第三者が、国以外の者が、この企業は優良な企業かと認証することに対して、世間一般がまだ必要性・必要性を満たしていない。まず、JIPDECの認知度も全国レベルではない。それから、何を評価するのかという評価基準がよく解らない。また、消費者はマークを信頼したことによって、何か事故が起きた時に認証機関がどのような法的なケアをしてくれるのかという効果もよく解らない。

プライバシーマーク制度は、真面目に運営しているが、その他の個人情報保護の第三者評価認証機関の中には、実質的主宰者の個人会社が審査を丸請けしたり、短時間受講するだけで、免状を発行したりして、認証自体をビジネスにしている。第三者評価認証機関が本来の目的と違って、あまりにもビジネスにシフトしているところがある。第三者評価認証制度が複数あって、制度間の競争があり、市場がそれを選ぶということは望ましいところであるが、放置できない団体があるのも事実だ。それに関しては、当該制度を主宰する団体も、そのスポンサー企業も消費者の信頼を裏切る行為をしているといってもいいだろう。第三者評価認証ビジネスの不適切な活動を放置しておけば、プライバシーマークも含めた民間の認証制度全体に対して、世間一般の認知度、信頼度も落ちるのではないかと。

(質問6)

日本の公正取引委員会(FTC)は、アメリカのFTCが消費者保護のために職務権力内で行っているのと同様に個人情報(オンライン,オフライン)に関する問題を取り扱っているのでしょうか？

- ・ **ニフティ 鈴木正** プライバシーポリシーやプライバシーステートメントの問題であるが、アメリカの場合はこういったことを護ると企業が自己宣言しておいて、その後、消費者に対する欺瞞的な行為をした場合には、FTCが行政的に介入するという仕

組みと連動しているため、消費者はプライバシーポリシーなどの企業の自己宣言に対して、ある程度の信頼を寄せることができる。日本の場合は、自己宣言することによってどのような法的リスクがあるかというのは非常に曖昧で、ポリシーを宣言することの意味がよく解らない。単に毒にも薬にもならない定型文を掲げる、誰も見もしないものを掲げる、その割に漠然とした法的リスクを感じているという状況である。既にこうした意味のないことはやめようという気運はあるが。

一方で日本の公正取引委員会が、消費者に対して欺瞞的プライバシーポリシーを掲げたことに対して、何らかのアクションを起こせるかということ、現行法だと景品表示法の運用で、消費者に欺瞞的な行為をした場合に何らかの行政的介入を行うことができるかもしれない。このことを公正取引委員会に正面から問いかけると、正式コメントとしては検討もしていないとは言えると思うが、まったくの私見であるが、若干の改正か、告示を出すことによって、FTCに類似するような形で公正取引委員会の介入は法制度上十分可能なのではないかと思う。

そうした改正や運用を行うべきか否かは、現状ではプライバシーポリシー自体の認知度がないし、プライバシーポリシーを信頼して現に不利益を受けたという被害実態がそれほど多いとは思われない。従って、公取がまだ動くほどの優先度の高い問題ではないと思っているのも無理はないところではないか。ただ、公取からの介入がありうるということを前提に、日本の企業ではプライバシーポリシーを考えていかざるをえない状況にあると考えるべきだろう。先ほどの、顧客との関係を重視したマーケティングをすべきだということに関して、抽象論としては、少なくともECOMのメンバーは当然そう思っているが、個人情報を実に多種多様である。イメージが貧困なほど個人情報情報は少なくなるのだが、個人情報の広がりや現場のビジネスにあてはめて、これも個人情報、あれも個人情報となると、やがてイメージが膨らんで、あまりにも膨大になっていく。すべての情報になんらかの個人情報保護性があると認識した段階で、これを本当に対外的に完全に護ると宣言して、本当に護りきれぬのかと不安になるのはある意味当然である。結局のところプライバシーポリシーの内容は、世間並の穏当な表現に落ち着かざるをえなくなる。JIS Q15001の体制の検討が内々に進められているようなので、そこに新しいポリシーの基本的な考え方が盛り込まれて、それを参考に試行錯誤が始まる。

- ・ **日本信販 上野** プライバシーマーク取得がなぜ大変かということと関係するが、従来、日本の企業は、顧客情報は企業の「財産」という意識が非常に強い。それが色々な仕組み、意識、システムに、すべて企業の「財産」を守るという方向できた。消費者保護への対応には、意識改革・社内の仕組み・ルールから全て変えなければいけない。そこが非常に大変。あらゆる個人情報をすべて完璧に護るということは難しいという問題である。

最近、不正競争防止法の観点から、顧客情報を持っている企業の営業秘密ということで、不正な利用があった場合には罰則を強化していこうということが検討されている。これはどちらかという消費者の保護ではなく、企業の「財産」の保護の問題。しかし、企業が顧客情報をきちんと管理して、不正、漏洩を防ぐようになれば、結果的に消費者保護にも寄与することになるのではないか。そう考えると、第一段階としては、消費者保護の方に企業が積極的に取り組んでいけると考える。ただ、罰則となると、非常に要件が厳格で、不正があったとしても、親告罪なので、どちらかという抑止力的なものにしかならない。それでもいろんな企業からの情報漏洩が問題になっているので、実施されると今のような漏洩も多少は少なくなるのではないかと。

(質問7)

新しい個人情報保護法のもと日本のFTCが法的権限を付与され、消費者のプライバシーを取り締まることになった場合に、企業側の受け止め方はどのようなものでしょうか？

- ・ **司会 (浅沼)** 前回 教授に、「自己情報コントロール権」について質問した際、その観点では、日本の個人情報保護法については、消費者がどこにクレームを申し立てるかということで、公的な第三者機関が必要、と指摘された。個人情報保護法では、認定個人情報保護団体を主務大臣が認定することになっているが、実際に、それぞれの業界団体やその他の機関がそのような認定を受け、教授が指摘されるような形になるかということ、現時点では、まだ見えない状況と思う。
- ・ **祖父江** 実際、個人情報保護法案では、明確には今の個人の選択権（オプトアウトのこと）が明記されていなくて、3月の閣議決定時の解説で、個人の選択権というものを説明されたと思います。ECOMガイドラインでは、個人の選択権は認めていこうと考えているのか？

- ・ **司会(浅沼)** 今度の修正案は、事業者の義務については変わらないと見られている。ECOMのガイドラインの個人情報の取得や第三者提供を含めての取扱いについては、その法案と同レベルの義務としている。ただその中で、個人情報取り扱い上の義務ではないが、消費者に対する配慮、特にプライバシーという点で配慮したほうが良いということについては、同意を取ることを奨励するように解説等に記載している。インターネット上で同意を取ることはリアルの世界よりも取りやすいことについては、できるだけ同意を取るよう奨励したい。

(意見交換・情報交換)

- ・ **ウェスティン教授** 日本の企業は、消費者が個人情報の取り扱いの重要性を認めているということに、十分に処しきれていないのが現状のようだ。私の調査によると、アメリカと同様の動向が現われている。消費者は、自分達のまったく解らないやり方で、企業が自分の情報をコントロールしているのではないかという懸念が表われている。これについてはどう思うか？
- ・ **CPデザイン 鈴木靖** 今日の話の中で、確かにまだ日本の企業が個人情報の問題について考えが遅れているのではないかというところがあったと思うが、いくつかの企業をコンサルする中で、何が難しいのかという問題点がいくつか出てきている。それは日本の企業で、個人情報の取り組みが進まないという答えになっていると思う。その理由は4つある。
1つは、意識の問題。ご指摘の通り、これからは企業自身がお客様の信頼を得てはじめて商売が成り立つ、これは勿論 日本の企業でも十分意識している。例えば、スーパーマーケットでダイエット薬を購入したお客様がいて、スーパーのレジ係が忘れ物を見つけて、「先ほどダイエット薬を買ったお客様」ということを大きくアナウンスするということはありません。その方がダイエット薬を購入したことを店舗にいるお客様全員に大声で伝えるような店員はいない。ただ、それがデータ化され、ある会員の購入品にダイエット薬があるというデータ出力物が、事務所で担当者の机の上に置きっぱなしで、他の社員が見られる状態にあった場合に、これは同じ問題だということに気が付く社員は少ない。プライバシーの問題は十分認識しているが、個人情報・データもそれに値するのだということにまではいっていない。
取り組みがなかなか進まない理由のもう1つは、日本の企業も人の入れ替わりが激し

くなってきていることにある。大量の解雇の問題などもあって、人の入れ替わりが多くなってきている。さらには、派遣会社から人を入れるとか、アルバイト、パートでまかなうという形態も多くなっている。そういった中で、全員に会社の意識を浸透させるのは苦勞する。

3点目は、日本のインターネットの取り組みは、企業の中の非常に一部の部署から発生したことにある。企業自体がインターネットをビジネスに活用しようとして、そこを中心に置いている企業は非常に少ない。インターネットをビジネスで取り入れようとした時に、非常に小さな部署のある担当に任せてそのビジネスを始めていたりするので、気づくと思わぬ個人情報の取り扱いがされていることはよくある。例えば、インターネットサイトのあるサービスで、ポストカードを用意して、「これを自由に使って友達に手紙を出してください、これはすべて無料サービスです」、というのがあつた。このサービスで、実は、手紙のやりとりを、インターネットサイトの運用者が覗き見をしたりも出来る。大抵、この覗き見は、会社の意思でやっているわけではなく、インターネットの担当者が個人的に発想したことだったりする。ただこれは、会社全体にインターネットをビジネスに生かそうとして進んできた企業では少なく、一担当にまかせてインターネットビジネスを広げてきた会社でありがちな話で、会社が意識していない個人情報の収集の例である。

最後の4点目はデータの分散。集中管理されているデータベースの中にすべての顧客情報が入っていればまだ管理は楽。しかし、担当者レベルのパソコンで個人情報の取り扱いをしていると、それぞれの担当者がデータベースを持っている状態になっているので、管理していくのが難しい。

大きな企業でも、以上申し上げた4点の問題がある。こうなつた時に実際の取り組みを始めるには、それなりの時間がかかる。以上の4つで、なかなか進まないというのを我々は経験している。

- ・ **司会（浅沼）** インターネットのそうしたアプリケーションシステムやツールが現場で導入され、利用される。つまり、集中管理のシステムではなく分散の、しかも、現場のリアルでやっていた仕事がインターネットの仕組みに急速に置き換わつていっている。先進する技術とそれに伴い導入・運用が先行する、その後を法律や社内規定が追いかけていく構造になっている。もちろんプライバシーもそのひとつである。
- ・ **ウェスティン教授** 貴重な議論、有難うございました。

6 おわりに

e - Japan 戦略のもと高度情報通信社会への進展が進み、電子商取引の普及がその柱の一つとされ、また、概ね IT 関連の法制化が整備される中、個人情報保護の問題は、法制化の面や事業者、消費者（利用者）における意識および対応の体系的な整備といった面で未解決な課題を残す分野ではないだろうか。

とりわけ、個人情報保護法案の審議が結果的に 2 年間にわたってさほどの進展することなく経過し、企業対応については法制化待ちの様相を呈しているが、この間にもインターネット利用および電子商取引は着実に裾野に及ぶまで普及が広がっている。

この高普及の原動力となっているものは、本来インターネットの持つグローバルに無限にどこまでも広がるネットワークとブロードバンド化が進み、さらに多様かつ高品質なコンテンツやアプリケーションを低料金・定額で利用できる環境が整備されていることによる。

さらにインターネットの環境はデジタルの世界であるがゆえに ID により対象を個別に認識することが可能であり、それらのコンテンツやアプリケーションの利用にあたり、あるいは電子商取引を行う場面では、企業の立場からすれば、個人情報を提供してもらうことによりきめ細かなサービスの提供や好みのコンテンツやメニューをスムーズに提示することができるものである。また、そのことは消費者（利用者）自体にとっても高度情報通信社会において享受すべきサービスであり、利便性であるはずである。

法案では個人情報は基本的に流通するものとの前提でミニマムかつゼネラルなスタンダードと考えられており、それが遵守できない場合に報告徴収、助言、勧告、命令を受け、その命令に違反したのものには行政的な罰則が課せられる。かつ、その基本理念において、個人情報は、個人の人格尊重の理念に慎重に取り扱われるべきものであり、さらに適正な取扱いを期待するものであることから、企業はこの精神に基づき、さらに自主的に消費者（利用者）に対する配慮を施すべきであろう。

E C O M 個人情報保護WGでは、個人情報の有用性と個人の権利利益の保護のバランスのもとに高度情報通信社会への進展を図るとする法案を支持した上で、さらに消費者（利用者）にとって、安心と信頼のもとに電子商取引を利用いただけるような環境整備を図るため、E C 事業者の体制構築および意識浸透への支援を引き続き推進していきたいと考える。

引用参考記事、資料・文献、URL 一覧（順不同、敬称略）

個人情報保護法 Q&A（藤田康幸 / 中央経済社）

電子ネットワークと個人情報保護（岡村久道・新保史生共著 / 経済産業調査会）

プライバシーマークを取得する方法（鈴木保立 / 株式会社 S C C）

ジュリスト 2000 年 12 月 1 日号 【特集】個人情報保護法制化に向けて

個人情報保護法制定の方向性（堀部政男 / 2000 年個人情報をめぐる内外の最新動向講演資料）

「I L P F Conference2002 Security v. Privacy」会議配布資料

「2002 International Conference On Personal Data Protection」会議配布資料

インターネット上のプライバシー保護に関する各国の現状（財団法人ニューメディア開発協会 / インターネット HP）

http://www.nmda.or.jp/enc/privacy/privacy-now5_1.html

EU の個人情報保護指令が企業に及ぼす影響と国際調和の可能性（日本貿易振興会）

EC で取り扱われる個人情報に関する調査報告書 ver.2.0/ver3.0/ver.4.0（電子商取引推進協議会）

ほか

個人情報保護WG名簿（敬称・役職略、企業名50音順）

委員	藤縄 元三	朝日監査法人 ビジネスリスク・コンサルティング事業部
委員	高田 誠	(株)アプラス 与信統括部
委員	西尾 美和	沖電気工業(株) ネットビジネスソリューションカンパニー 戦略企画室
委員	保倉 豊	グローバルフレンドシップ(株)
委員	川城 三治	グローバルフレンドシップ(株)
委員	菅佐原 健一	(株)シー・アイ・シー 経営企画部
委員	川島 信司	(株)ジェーシービー コンプライアンス統括部
委員	霜田 都司	エプソンダイレクト(株) 情報企画部
委員	大西 浩	(株)オーエムシーカード 顧客情報センター
委員	田中 剛	(株)オーエムシーカード 営業開発担当企画管理部
委員	溝口 透	(株)東芝 営業企画室
委員	中島 和雄	(株)東芝 法務部
委員	今井 優子	(株)東芝 法務部
委員	脇田 正敏	トヨタ自動車(株) 国内マーケティング部
委員	森田 一平	トヨタ自動車(株) お客様関連部
委員	荒木 吉雄	日本アイ・ビー・エム(株) チーフ・プライバシーオフィサー
委員	上野 正之	日本信販(株) 個人情報部
委員	清水 雅子	日本電気(株) NECソリューションズ インターネット基盤開発本部
委員	田中 俊幸	日本電子計算機(株) 情報システム部
委員	阪上 正博	日本ユニシス(株) 法務部
委員	野中 信孝	日本ユニシス(株) 法務部
委員	大成 和津江	ビザ・インターナショナル・アジア・パシフィック・リミテッド
委員	立仙 和巳	(株)日立製作所 ビジネスソリューション事業部 コンсалティング 第五部
委員	下山 祐司	富士通(株) 法務・知的財産権本部 法務部 法務企画部
委員	牧山 嘉道	マイクロソフト株式会社 法務本部
委員	山本 昇	マイクロソフト株式会社
委員	東山 治郎	松下電器産業株式会社 法務本部 法務グループ
委員	伊東 正晴	三井住友海上火災保険(株) 文書法務部 法務グループ

委員 玉井 康昭	三井住友海上火災保険(株) 文書法務部 文書グループ
委員 三野 重広	三菱電機インフォメーションテクノロジー株式会社 生産推進部
委員 横川 明	(株)損害保険ジャパン 法務部
委員 中鉢 亜都子	ユーシーカード(株) 経営企画部

アドバイザー

堀部 政男	中央大学教授(一橋大学名誉教授)
新保 史生	筑波大学図書館情報学系助教授
長谷川 博章	内閣官房 個人情報保護担当室
中山 大輔	経済産業省 商務情報政策局 情報経済課
鈴木 正朝	ニフティ(株) 法務・海外部
鈴木 靖	(株)シーピーデザインコンサルティング
合原 英次郎	松下電器産業(株) 東京支社 渉外グループ
小泉 雄介	(財)ニューメディア開発協会 開発本部

E C O M 事務局

事務局 江口 正裕	電子商取引推進協議会 主席研究員
事務局 浅沼 省吾	電子商取引推進協議会 主席研究員

禁 無 断 転 載

EC で取り扱われる個人情報に関する調査報告書

平成 15年 3月 発行

発行所 財団法人 日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園3丁目5番8号
機械振興会館 3階

TEL : 03 (3436) 7500

印刷所 (所 名)

(住 所)

TEL :

(本報告書は再生紙を使用しています。)

