←（背表紙）

（表紙）

EC で取り扱われる
個人情報に関する調査報告書 2003

平成 16 年 3 月

電子商取引推進協議会

ECで取り扱われる個人情報に関する調査報告書 2003
電子商取引推進協議会

（表紙裏）

目次

1　個人情報保護に関する動きと ECOM 個人情報保護 SWG 活動

1.1　個人情報保護法および政府関連動向

1.1.1　個人情報保護法成立

2003 年 5 月 30 日、「個人情報の保護に関する法律」が公布された。そのうち、個人情報取扱事業者の義務規定は、2 年以内の政令で定められた日よりの施行とされ、2003 年 12 月 10 日政令公布により 2005 年 4 月 1 日よりと定められた。企業は、その義務規定施行日に向けて、本格的に個人情報保護についての対応体制の整備を早急に図らなければならない」。とりわけ、電子商取引やインターネットを通じての事業活動の場面での個人情報の取り扱いに関しては、情報漏洩や取得、利用での消費者・顧客とのトラブル等が懸念され、予見可能なリスクについては最大限回避すべく対応策を講じることが求められる。

本法律の成立に関わる審議の経過概略を以下にまとめる。2002 年末一旦廃案となり、2003 年 3 月より再度通常国会にて修正案として提出された個人情報保護法案は 4 月 8 日、衆議院本会議で審議入りした。前年までの内閣委員会における審議に変わって今回は特別委員会が設置され、委員長には自民党の村井仁・前国家公安委員長が選任された。

委員会は「個人情報の保護に関する法律案」をはじめとする与党より提出された 5 つの修正法案と野党 4 党より提出された対案を併せて、民間事業者や行政機関の保有する個人情報等について討議された。与党修正案は基本原則の削除や報道機関への表現の自由に配慮した内容となったため、それまで以上に、民間事業者の個人情報の取扱いについて細部にまで議論が及ぶこともあった。

年賀状ソフトや顧客管理システムに使われる電話帳 CD-ROM やカーナビゲーションシステムなどが個人データになるのかについての議論やプライバシーおよび自己情報コントロール権についての考え方、電気通信分野・個人信用分野・医療分野等での個別行政にかかわる課題などについて質疑および答弁が行われた後、全面施行後 3 年を目途に見直しを行うなどの附帯決議を付し、本会議に送られ、5 月 6 日衆議院を通過、5 月 23 日参議院を通過し可決成立した。

1.1.2　政令

2003 年 12 月 10 日、「個人情報の保護に関する法律施行令」および「個人情報の保護に関する法律の一部の施行期日を定める政令」が公布された。その中の事業者に関する要点

を以下にまとめる。（内閣府国民生活局配布資料を元に要約）

個人情報の保護に関する法律の施行令等の事業者に関連する要点

● 法第 4 章義務規定の施行期日

平成 17 年 4 月 1 日

● 個人情報の保護に関する法律施行例の要旨

1. （第 1 条）法の対象となるマニュアル（手作業）処理情報の範囲

これに含まれる個人情報を一定の規則にしたがって整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するもの

2. （第 2 条）個人情報取扱事業者から除外される者

その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 月以内のいずれの日においても５千を超えない者

注：他人の作成したカーナビや電話帳を取得して、編集し、又は加工することなくその事業の用に供するときは、これを構成する個人情報によって識別される特定の個人の数はその数に算入しない。

3. （第 3 条）保有個人データから除外されるもの

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

・本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

・違法又は不当な行為を助長し、又は誘発するおそれがあるもの

・国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

・犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

4. （第 4 条）保有個人データから除外されるものの消去までの期間

6 ヶ月以内に消去されるもの

5. （第 5 条）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

① 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

② 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

6. （第 6 条）個人情報取扱事業者が保有個人データを開示する方法

書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）

7. （第 7 条）開示等の求めを受け付ける方法として定めることができる事項

① 開示等の求めの申し出先

② 開示等の求めに際して提出すべき書面（電子的方式、時期的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

③ 開示の求めをする者が本人又は次条に規定する代理人であることの確認方法

④ 手数料の徴収方法

8. （第 8 条）開示等の求めをすることのできる代理人

① 未成年者又は成年被後見人の法定代理人

② 開示等の求めをすることにつき本人が委託した代理人

9. （第 9 条～13 条）認定個人情報保護団体の認定申請、認定業務の廃止の届出、地方公共団体の長等が処理する事務、権限又は事務の委任、主務大臣による権限の行使について規定

1.1.3 基本方針の状況

保護法の規定により、政令についで政府より個人情報の保護に関する基本方針（以下「基本方針」という。）が定められる。基本方針は国民生活審議会の意見を聞いて策案し、閣議決定を経て発令されるが、2004 年 2 月時点までに、6 回の同審議会個人情報保護部会が開催された。そして、基本方針に盛り込むべき内容の検討や関連団体、事業者等の実態の関するヒアリング等について公開で審議されている。第６回の開催では、基本方針の骨子素案が提示された。

個人情報の保護に関する基本方針（骨子素案）

1　個人情報の保護に関する施策の推進に関する基本的な方向

（1）個人情報保護の理念・意義

① 個人情報保護の理念、立法の背景事情

- 高度情報通信社会に個人情報利用が不可欠かつ重要となっている一方、漏洩事案などの増大と国民の不安の高まりへの対応がＩＴ社会の健全な発展への課題。

② 国際的な動向

- 従来からのＯＥＣＤ8 原則を始めとする国際的な取組や諸外国の取組の動向を紹介する。

（2）総合的推進のあり方

- 本制度の実効性を上げるためには、官（国・地方）と民（事業者・認定団体・相談機関）にわたる関係機関の連携が重要であることについて指摘する。
- 本基本方針は、このような観点から、関係各主体による取組を呼びかけ、その方向性を示すものとして法制の中に位置付けられるもの。

2　国が講ずべき個人情報の保護のための措置に関する事項

（1）各行政機関の保有する個人情報の保護の推進

- 行政機関個人情報保護法を厳格に運用する。その主要点について具体的に記述。

（2）政府全体としての制度の一体的な運用を図るための指針

① 法の施行の状況の内閣府への報告と公表

- 法第 53 条に定める施行状況報告の時期及び主な報告項目について定める。施行状況については、内閣府において公表するとともに、国民生活審議会に報告する。

② 個別の事案が生じた場合の内閣府と各省庁の連携のあり方

- 事業の適正化等の観点から、主務大臣として、各省庁において対応する。
- その結果を内閣府へ適宜情報提供し、内閣府において対応事例の蓄積を行う。

③ 各省庁における個人情報保護窓口の設置・職員への教育研修

- 各省庁において個人情報保護法に関する窓口を明確化し、他省庁や地方公共団体との窓口としての機能を担う。また、省庁内の事業所管部局から相談を受けるとともに、これらの職員への知識の普及を図る。

④ 共管の場合の主務大臣の連携のあり方

- 共感が見込まれる場合には、関係省庁間で連携を図り、共同して権限を行使する。なお、他の主務大臣が不明な場合や、主務大臣の数が多く事前に連携を図り難い場合は、政令第 13 条により権限を単独に行使することができる。

⑤ 主務大臣の指定の方針

- 主務大臣が明らかでない場合は、内閣府から、関係の深いと思われる省庁に照会。必要ならば、関係省庁連絡会議も活用しつつ担当する省庁を決め、主務大臣として指定する。

（3）分野ごとの個人情報の保護の推進に関する方針

① 各省庁が所管する分野において講ずべき施策

- 各事業等所管省庁は、各分野の実情に応じて、ガイドラインの策定・見直しの必要性について検討する。
- 本法の規律は各分野共通の必要最小限のものであることから、ガイドラインは各分野の実情を十分に踏まえたものとする必要がある。

② 特に適正な取扱いを確保すべき個別分野において講ずべき施策

- 個人情報の性質や利用方法等から特に適正な取扱いを確保すべき分野（医療、金融・信用、情報通信）については、平成 17 年 3 月までに格別の措置について検討し、一定の結論を得る。

（4）広報、啓発、情報提供等に関する方針

- 国民、事業者等に対する広報や情報提供には、インターネット等を最大限活用するとともに、必要に応じて説明会等をきめ細かく行う。

3　地方公共団体が講ずべき個人情報の保護のための措置に関する基本的な事項

（1）地方公共団体の保有する個人情報の保護の推進

- 行政機関個人情報保護法等を踏まえた条例の制定・見直しが強く望まれる。

（2）広報、啓発、情報提供等

① 区域内の住民、事業者等に対する広報、啓発、情報提供等のあり方

- 法制度の周知など、区域内の実情に応じ、必要な対応が望まれる。

② 条例部局、県民相談部局、事業所管部局の相互連携

- 関係部局の役割分担を明らかにして、対応のための連携体制を確保することが望まれる。

③ 国・地方公共団体の連携のあり方

- 全国津々浦々の事業者を監督するためには、国と地方公共団体が協力することが不可欠。政令第 11 条により、国と地方公共団体の連携を図りつつ、より事業者の実情を承知している側で対応を行なう。
- このほか、広報、啓発等においても連携は不可欠。

4　独立行政法人等が講ずべき個人情報の保護のための措置に関する基本的な事項

- 独立行政法人等の保有する個人情報の保護の推進

  独立行政法人等個人情報保護法を厳格に運用する。その主要点について具体的に記述。

5　地方独立行政法人が講ずべき個人情報の保護のための措置に関する基本的な事項

- 地方独立行政法人の保有する個人情報の保護の推進

  条例において所要の規定を整備する等、設立団体の責任において厳格な実施を確保することが強く望まれる。

6　個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項

（1）個人情報取扱事業者が講ずべき個人情報の保護のための措置に関する基本的な事項

① 事業者が行う措置の対外的明確化

- 個人情報の取扱方針（プライバシーポリシー）の策定・公表などにより、事業者が関係法令等を遵守し、どのように対応することにしているのか、顧客等の関係者を始めとして、対外的に明らかにすることが望まれる。

② 責任体制の確保

- 個人情報保護管理者の設置など、事業者の内部での責任体制を確保することが考えられる。また、業務委託などの際には、契約先との責任関係を明確にし、実効的な監督体制を確保することが望まれる。

③ 従業員への啓発

- 教育研修などにより、従業者への啓発を図っていくことが望まれる。

（2）認定個人情報保護団体が講ずべき個人情報の保護のための措置に関する基本的な事項

① 民間団体による認定申請の促進方策

- 本制度の実効性を確保する上で認定個人情報保護団体による苦情の処理は重要であり、関係省庁から事業者団体に働きかけるなどにより、認定申請を促進することが考えられる。

② 個人情報保護方針の位置付け、策定・見直しを行う上での留意事項

- 業界ガイドラインについても、各業界の実情に応じて、その策定・見直しの必要性について検討していくことが必要。
- その際には、各業界等を所管する省庁による適切な支援が重要。

7　個人情報の取扱いに関する苦情の円滑な処理に関する事項

（1）事業者自身による取組のあり方

- 個人情報を取り扱う事業者自らが積極的に苦情処理に取り組むことが重要であり、

苦情受付窓口を設置するとともに、責任体制を確保していくことが望まれる。

（2）認定個人情報保護団体の取組のあり方

- 認定個人情報保護団体は、公正な第三者的立場から苦情の解決に当たるもの。
- 様々な苦情処理に対応するため、人材の確保を含む体制の整備が望まれる。

（3）各省庁における取組のあり方

- 各省庁においても、苦情相談機関から悪質な事業者に関する情報を受け付けるため、個人情報保護窓口を明確化する。また、各省庁に直接苦情が寄せられた場合には、これに対応する。

（4）地方公共団体における取組のあり方

- 地方公共団体においては、条例部局、県民相談部局、事業所管部局等の関係部局の間の協力体制を確保し、苦情に適切に対応する。

（5）国民生活センター、消費生活センター、認定保護団体など各種相談機関の連携・情報共有の仕組み・相談員の研修

- 国民生活センターが中心となって、苦情処理マニュアルを作成する。（消費生活センターのみならず、認定保護団体への配布も検討）
- 国民生活センターに苦情相談の事例を集約し、対応事例集を作成して、各種苦情相談機関での情報共有を図る。
- 国民生活センターが中心となって個人情報保護に関する研修等を実施し、各種相談機関において専門知識を有する相談員の育成を図る。（消費生活センターの相談員のみならず、必要に応じ認定保護団体の担当職員の参加も検討）

8　その他個人情報の保護に関する施策の推進に関する重要事項

（1）情報収集・調査研究の推進

- 個人情報の取扱いは、情報通信技術の発展、国際的な取組の動向等、社会・経済の変化に応じて変化していくものであり、内閣府において様々な観点から調査研究を行う。

（2）国民生活審議会の役割

- 2（1）②に基づく毎年度の法施行の状況について、国民生活審議会に報告し、施行状況のフォローアップを行う。本基本方針についても、諸情勢の変化や、施策の効果に関する評価を踏まえ、柔軟かつ適切に見直しを行う。
- 国会の付帯決議においても、法の全面施行後 3 年を目途として必要な措置を講ず

ることとされている。

（以上、国民生活審議会個人情報保護部会第６回会議資料より抜粋）

第 6 回部会終了時点で、以降 2 回の審議が重ねられ、4 月には基本方針として閣議決定される見通しである。

1.1.4　経済産業省ガイドラインの状況

主管官庁のガイドラインの策定状況に関して経済産業省のガイドライン及び JISQ15001 についての現状を以下に示す。これは、2003 年夏から冬に、随所にて同省個人情報保護担当より説明されたプレゼンテーション資料における説明に拠るものである。

「経済産業省の新ガイドライン」について（平成 16 年 4 月以降に策定予定）

性格

個人情報保護法第８条に基づくガイドライン。（罰則等の対象となる。）

新ガイドラインの方向性

詳細については、今後策定される、政令及び基本方針を踏まえて策定されることとなる。

以下の方向で検討する。

① 経済産業省が所掌する事業分野の事業者に対するもの

② 法第４章に定められる個人情報取扱事業者の義務等を詳細化・具体化

③ 原則的には、「法律が定めるもの以上でも以下でもない」規定

④ 事業の性質や個人情報の取扱い状況等に応じたより適切な措置については、業界の自主的なガイドライン等に委ねる。

「個人情報保護に関するコンプライアンス・プログラムの要求事項（JISQ15001）」の改訂について（平成 16 年 4 月以降に改訂予定）

JISQ15001 の改訂の背景

① 工業標準化法第１５条に基づく見直し（規定制定日より５年以内）

② 個人情報保護法の成立

改訂に当たっての基本的方向

① 個人情報保護法との整合性を図る。

②「より適切な保護の在り方」を規格として策定し、各事業者の自主的な取組みを促進する施策の一つとしての位置付け。

改訂に当たっての論点

・定義

・「同意原則」

・特定の機微な個人情報の原則収集禁止

・本人関与（個人情報の利用停止及び第三者提供停止）

・個人情報保護方針、内部規程等 等

さらに、今後、2004 年 3 月に内閣府国民生活審議会にて基本方針が示された後の、4 月以降にて「経済産業省ガイドラインの策定」と「JIS 規格（JISQ15001）の改訂」なされるスケジュールが設定されており、すでに政令で保護法の義務規定が 2005 年 4 月より施行されることが交付されている状況からすると、それらの公表を待って対応しはじめるとすると 1 年を切ることとなる。

大方の各業界団体は、主務官庁のガイドラインが発令されてから、それぞれのガイドラインや指針等を検討する様相だが、体制整備及び従業者への意識浸透を徹底することを考えると、1 年を切る期間は十分に準備が施せる期間とは言い難い。

実際には、各事業者にて、保護法、政令ならびに国民生活審議会での議事等をベースに、現時点で確定している要件より、対応体制構築を進めていくことが好ましい。

1.1.5　個人情報保護に関する世論調査

平成 15 年 9 月の調査として、同年 12 月に、内閣府大臣官房政府広報室より「個人情報保護の関する世論調査」が公表された。

同調査は、調査対象を全国 20 歳以上の 3,000 人（有効回収数 2,126 人、有効回収率 70.9%）をサンプリングし、個人情報の保護に関する国民の意識の把握と今後の施策への参考にすることを目的に実施された。

調査内容としては、

（1）個人情報保護への関心度と個人情報も不適正な取扱い

（2）法令制定についての周知度

（3）民間事業者における個人情報の取扱い

（4）個人情報開示請求の意向

（5）個人情報保護対策について

という項目に関して、16 の質問が設けられており、調査対象者は基本的に選択肢の中から回答する形式で行われている。

一部の設問に関して、昭和 56 年 2 月に実施された「プライバシー保護に関する世論調査」、昭和 60 年 7 月、平成元年 6 月に実施された「個人情報の保護に関する調査」を過去との比較に関して引用しており、時系列に見る国民の個人情報に関する意識の変化が窺うことができる。（参考 URL：http://www8.cao.go.jp/survey/h15/h15-kojinjouho/index.html）

1.2　ECOM 個人情報保護 SWG の活動

ＥＣＯＭでは、従来、電子商取引における個人情報の漏洩や流出に関する調査および企業の対応についての調査・検討を行っており、本年度も個人情報保護ＳＷＧにて基本的に同様のテーマで活動した。本年度は、会員企業 21 社 31 名の方に委員としてエントリーいただき（2004 年 2 月末現在）、また、中央大学法学部の堀部政男教授をはじめ、学識者、政府関連の担当、関連団体やコンサルティングの方々にアドバイザー（11 名）として参加いただいた。期首における主な活動計画は以下のとおりであった。

① ＥＣＯＭとしての個人情報保護の考え方整理

ＥＣＯＭ個人情報保護ガイドライン改定版（Ver.2.0）完成／ホームページ・配布物等のリニューアル

② 日本の企業における個人情報保護の実施実態調査

ＥＣＯＭ会員企業団体調査（アンケート・目視調査）

③ ＥＣの場面（インターネット上）での企業が配慮すべき個人情報保護対応

ＳＷＧメンバーディスカッション／関連企業・団体・有識者ヒアリング

④ 関連検討事項

セキュリティ・モバイル・トレーサビリティ関連（他ワーキングとの連携）／国際関連動向調査、有識者・団体との交流・情報交換

以降、SWG にて活動した結果としての顕著な成果についてとりまとめる。

2　ECOM 会員企業個人情報保護の実態把握

2.1　調査の概要

昨年度に引き続き、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調査を実施した。昨年同様に、ＥＣＯＭ会員企業を対象とした個人情報保護に関するアンケート」および「ＥＣＯＭ会員企業ホームページ・個人情報保護関連記載目視調査」で構成し、各項目の集計分析に加え、設問については昨年度の調査結果との比較分析を行った。

概観すれば、2002 年度の法案審議および企業の個人情報漏洩事件の報道の影響を受け、リスクマネジメントの一環として、事業者の個人情報保護に向けた体制整備は着実に進みつつあるといえよう。

2.1.1　ＥＣＯＭ会員企業・団体個人情報保護の取組みアンケート調査

249 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、2003 年 7 月 7 日から 7 月 24 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。

設問は、基本的に、概ね昨年度と同様の内容および構成にしているが、昨年度実施の際、個人情報の取扱いについて Web 上であるか、Web 以外かについて一部不明確であった点を考慮し、その確認の設問（設問３）を追加した。また、個人情報を収集しない事業者に対して取扱いについての質問には回答しなくてよい構成に変更した。

回答企業は昨年に続き、対応いただいた会社が 53 社で、本年度回答会社に対して 51.0%を占めた。

また、業種別では昨年同様に情報サービス業よりの回答が最も多く、全体の 43%（昨年は 38%）を占め、次いで、製造業（20%、昨年 29%）、金融業（13%、昨年 15%）と続く。

2.1.2　アンケート調査の概要

（1）アンケート調査時期…… 2003 年 7 月 7 日～7 月 24 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 249 社）

（3）回答希望部門　　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

（4）有効回答数…… 104 件（回収率：41.8%）

2002 年：97 件（回収率：32.8%）＋9 ポイント

（5）回答業種別分類

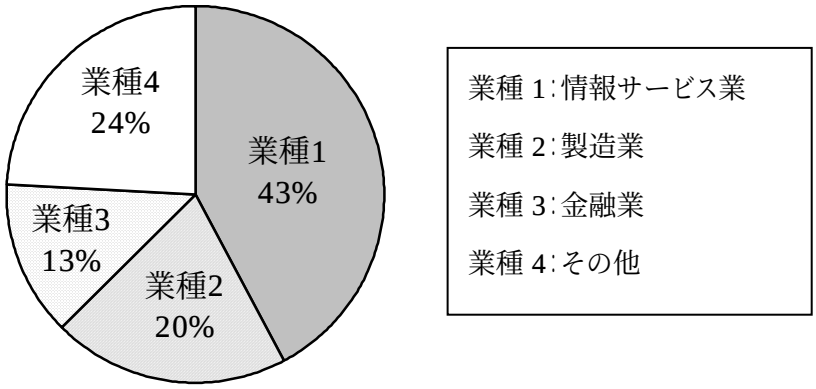
ご回答頂いた業種	件数	分類業種	件数
情報サービス業	35	業種 1 情報サービス業	44
その他情報サービス業	9		
製造業（電気機器･精密機器）	12	業種 2 製造業	21
その他製造業	9		
金融･保険業	14	業種 3 金融業	14
電力･ガス業	10	業種 4 その他	25
卸売業	7		
運輸･倉庫業、マスコミ、エンタテイメント その他	8		
合　計	104	合　計	104

図表 2-1 回答業種別分類

⑹ 昨年度回答企業･団体との件数比較

	2 年連続回答	02 年のみ回答	03 年のみ回答	合計
2002 年度	53 社（54.6%）	44 社（45.4%）		97 社
2003 年度	53 社（51.0%）		51社（49.0%）	104 社

■アンケート回答会社業種分類（有効回答会社数＝104 社）



図表 2-2　アンケート回答会社業種分類

2.1.3　設問

設問は全 15 問で、以下のとおりである。

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？

a. 個人情報保護についてまとめた規定がある
b. 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
c. 今はないが、今後策定しようと考えている
d. ない

② 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？

a. 専任の担当または部門を設置している
b. 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

③ 貴社では個人情報を収集し、利用していますか？また、その個人情報の収集は Web よりの収集ですか？

a. Web および Web 以外の両方の方法で、収集し、利用している
b. Web を通じてのみ収集している
c. 収集しているが、Web 上からは収集していない
d. 個人情報は収集していない

④（問③a．b．c．の回答者）貴社の収集する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. 顧客サポートやサービスの提供
b. 販促情報の提供
c. 懸賞公募
d. 資料請求対応

e. 商品開発や販促のためのマーケティング調査（お客さまの嗜好やニーズ・動向の掌握等）

f. EC（Web サイト上での商取引行為）を行うため

g. 代金等の回収等

h. 採用・人材公募等

i. その他

⑤（問③a．b．ｃ．の回答者）現在収集している個人データは何件（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以上１万件未満

c. １万件以上１０万件未満

d. １０万件以上

⑥（問③a．b．ｃ．の回答者）個人情報を収集する際、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

⑦（問③a．b．ｃ．の回答者）個人情報を収集する際、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

a. 明示し、同意を得ている

b. 明示しているが、同意は得ていない

c. 明示していない

⑧ （問③a．b．ｃ．の回答者）個人データを第三者に提供することがありますか？

＊ 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

a. ある、収集する時にそのことを明示し、同意を得ている
b. ある、収集する時にそのことを明示しているが、同意は取っていない
c. あるが、収集する時に明示もしておらず、同意も取っていない
d. ない

⑨（問③a．b．c．の回答者）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？

a. なっている
b. 一部の項目については開示・変更には応じるが一部のものは応じない
c. なっていない

⑩ 問③a．b．c．の回答者）問⑨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）

a. ユーザーID やパスワードによる認証
b. 本人でないとわからない事項（電話番号、生年月日、記入データ等）を１つ、または複数回答いただく
c. 本人認証が可能なもの（免許証や保険証等のコピーなど）や押印された申し込み書類等を郵送いただく
d. 直接来店いただく
e. 当初登録のメールアドレスへの返信
f. 折り返しの電話、または届出の住所への郵送
g. 本人認証については特に何も要求しない
h. その他

⑪ 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？

a. トップページに、あるいはそこからリンクできるように顧客に見え易い形で示している
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

⑫ 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

⑬ 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

⑭ （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

⑮ 「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、

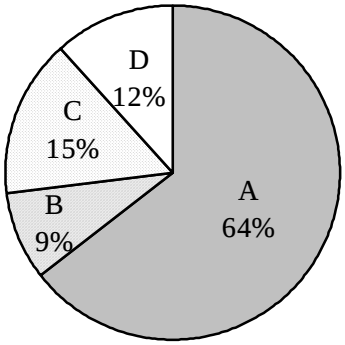
a. 採用し、運用している
b. まだ採用していないが、検討している
c. 採用を検討していない
d. 知らない

2.1.4　設問ごとの調査結果及び分析

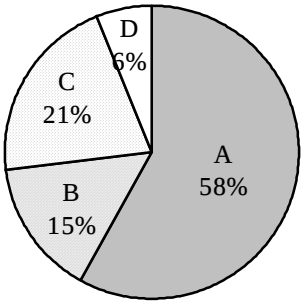
Ｑ１．貴社には個人情報保護に関する社内規定がありますか？（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

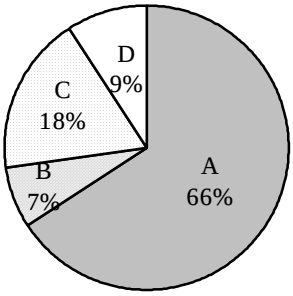


A：　個人情報保護についてまとめた規定がある
B：　各内規の節々に個人情報の取扱いについての規定が散在している、あるいは各部門にてまちまちではあるが規定を定めているところもある
C：　今はないが、今後策定しようと考えている
D：　ない

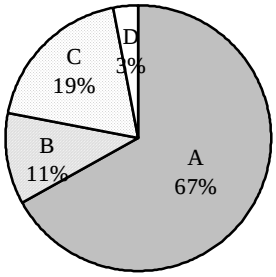
② 業種別

＜情報サービス業＞

【2003 年度】

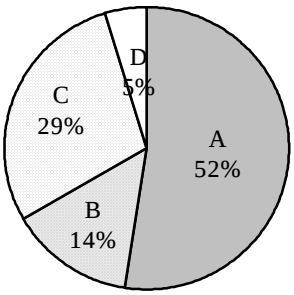


【2002 年度】

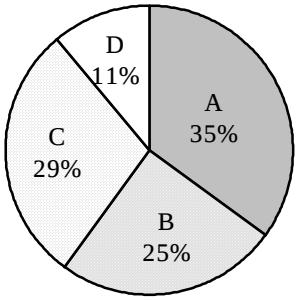


＜製造業＞

【2003 年度】

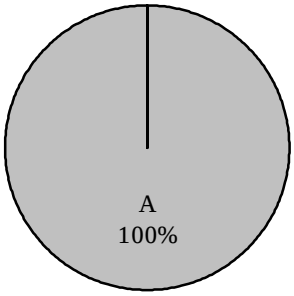


【2002 年度】

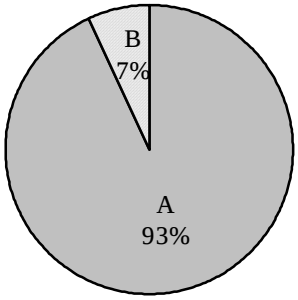


＜金融業＞

【2003 年度】

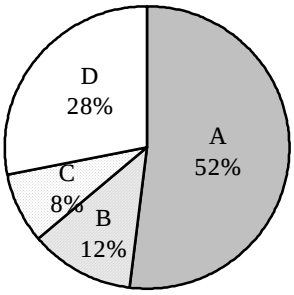


【2002 年度】

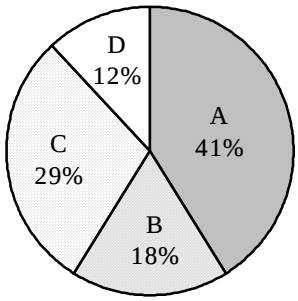


＜その他＞

【2003 年度】



【2002 年度】



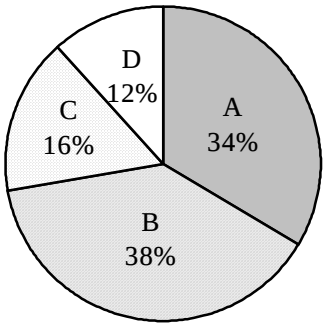
図表 2-3　Q1 調査結果

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」を含めると、73%が個人情報保護についての社内規定を定めている。これは昨年と同様のウェイトであるが、「個人情報についてまとめた規定がある」との会社のウェイトは 6 ポイント上昇した。業種別に見ると金融業・情報サービス業が昨年同様に社内規定の整備が先行しているが、昨年と対比すると製造業やその他において、急速に進みつつあることが窺える。

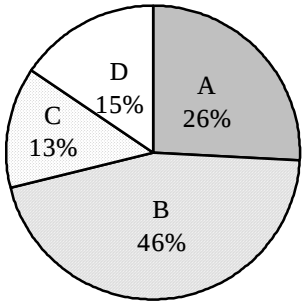
Q2．上記の規程及び内規を実行する上での推進責任者の任命または担当部門の設置はなされていますか？　（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

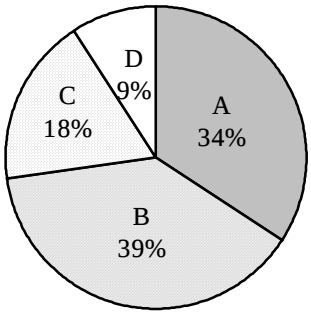


A：　専任の担当または部門を設置している
B：　兼務で担当を任命している、または部門内に担当や職務を割り当てている
C：　今はないが、今後任命あるいは設置しようと考えている
D：　ない

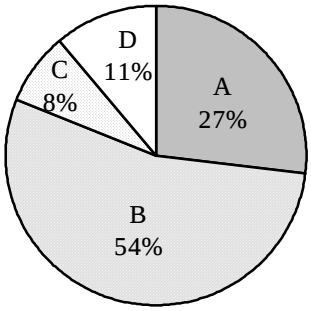
② 業種別

＜情報サービス業＞

【2003 年度】

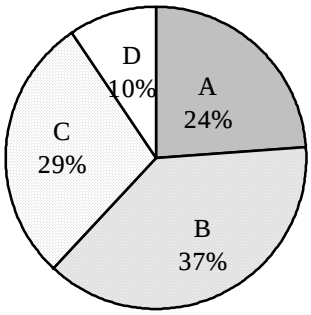


【2002 年度】

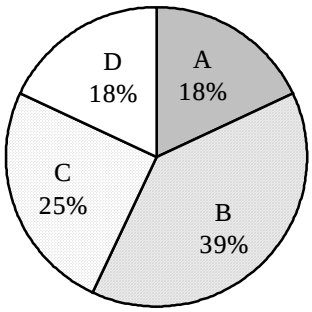


＜製造業＞

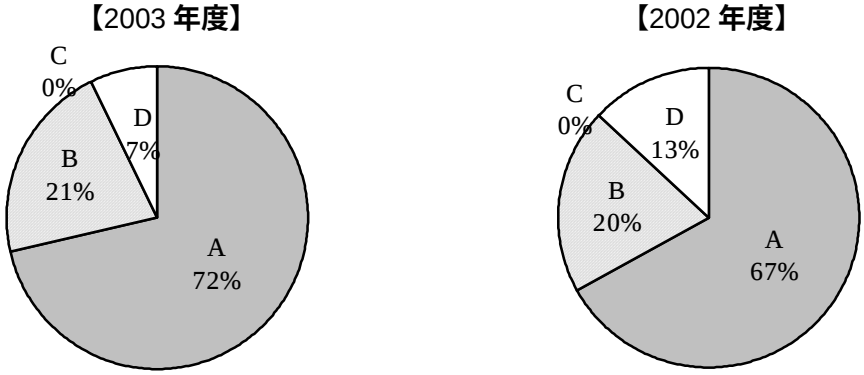
【2003 年度】



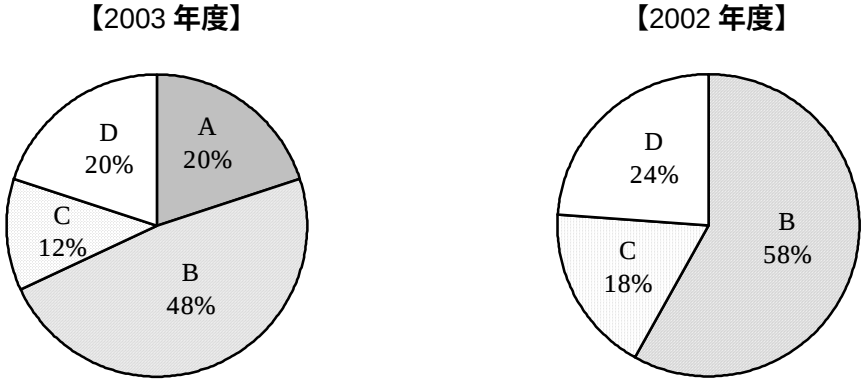
【2002 年度】



＜金融業＞



＜その他＞

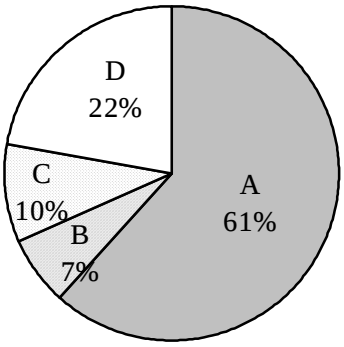


図表 2-4　Q2 調査結果

Q１と同様の傾向が伺える。

Q3. 貴社では個人情報を収集し、利用していますか？また、その個人情報の収集は Web よりの収集ですか？　（有効回答会社数＝81 社）　※2003 年のみ調査

① 全業種合計



A：　Web および Web 以外の両方の方法で、収集し、利用している

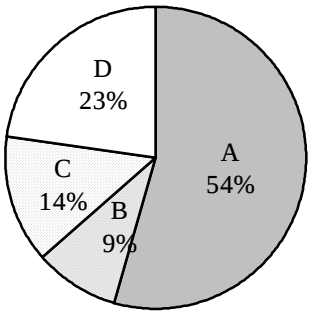
B：　Web を通じてのみ収集している

C：　収集しているが、Web 上からは収集していない

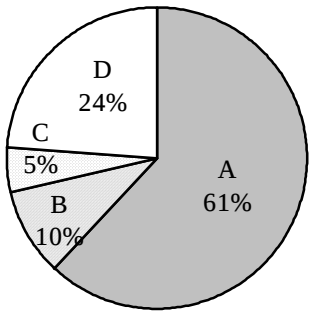
D：　個人情報は収集していない

② 業種別

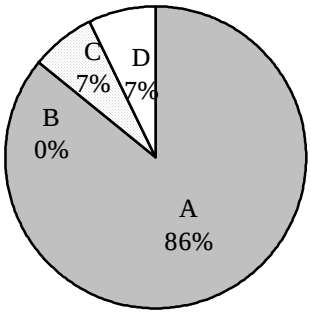
＜情報サービス業＞



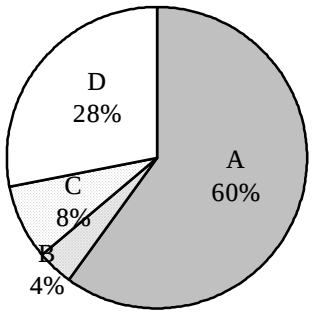
＜製造業＞



＜金融業＞



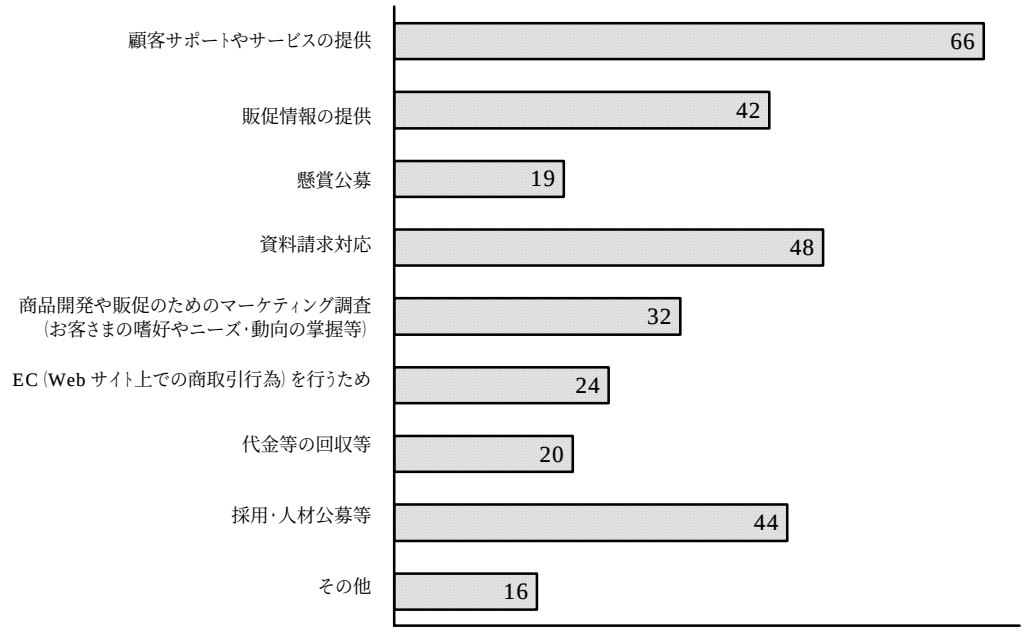
＜その他＞



図表 2-5　Q3 調査結果

Q4.（Q3 a．b．ｃ．の回答者）貴社の収集する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＝83 社）

① 全業種合計



その他の回答詳細

- 会員入会･各種申込の受付等
- お問合せ全般･製品クレーム対応等
- 貸付審査･与信取引
- インターネットユーザー動向調査
- 株式事務等

図表 2-6　Q4 調査結果

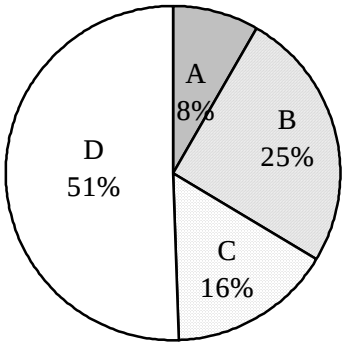
具体的な利用目的として最も多いのは、顧客サポートやサービスの提供（66 社=回答者対ウェイト 80%）であり、資料請求対応（48 社=同ウェイト 58%）が続く。第 4 位の販促情報の提供を含め、営業を捕捉または購入を誘発することを目的とするケースが多い。また、採用や人材公募（44 社=同ウェイト 53%）も多くの企業で行われている。

EC（Web サイト上での商取引行為）を行うため（24 社=同ウェイト 29%）や代金等の回収等（20 社=同ウェイト 24%）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。

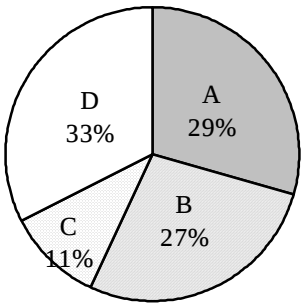
Q5.（Q3 a．b．ｃ．の回答者）現在収集している個人データは何件（1 件＝1 人分の個人情報）ぐらいありますか？　（有効回答会社数＝83 社）

① 全業種合計

【2003 年度】



【2002 年度】

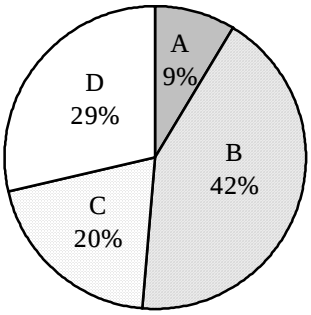


A:　1000件未満
B:　1000件以上1万件未満
C:　1万件以上10万件未満
D:　10万件以上

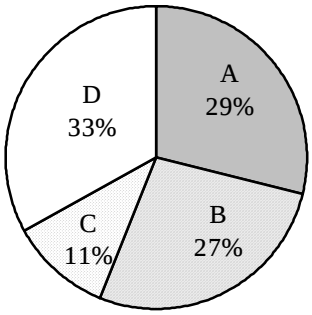
② 業種別

＜情報サービス業＞

【2003 年度】

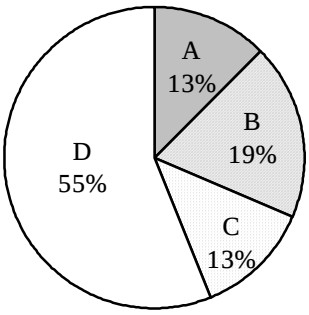


【2002 年度】

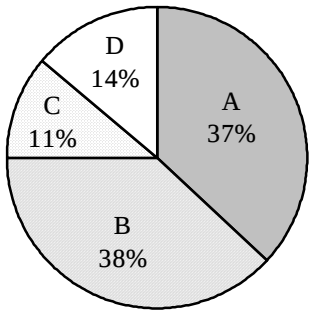


＜製造業＞

【2003 年度】

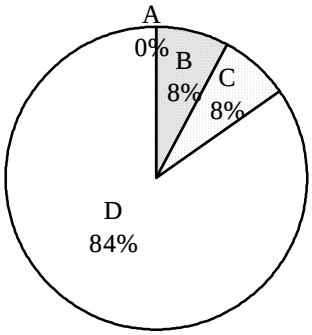


【2002 年度】

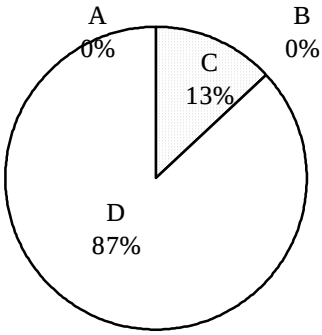


＜金融業＞

【2003 年度】

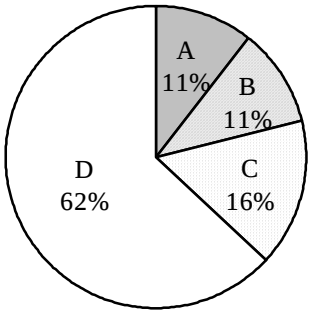


【2002 年度】

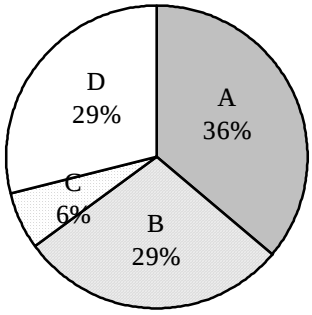


＜その他＞

【2003 年度】



【2002 年度】



図表 2-7　Q5 調査結果

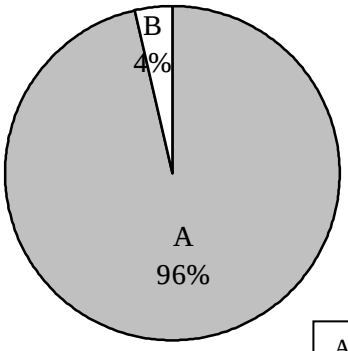
個人情報保護法において「個人情報取扱事業者」について除外されるひとつに「その取り扱う個人情報の量および利用方法からみて個人の権利利益を害する恐れが少ないものとして政令で定める者」があることの参考に設問を設定している。先の政令にて、その件数が 5000 件未満と定まった。

全体では 1000 件未満が 1 割弱、1000 件以上 1 万件未満が 25%である。昨年の集計では 1000 件未満が 29%の高率を占めていたが、これは、情報処理関連企業等の個人情報を基本敵に扱わない企業の回答が含まれていたことと対象となる個人情報のイメージが定かでなかったことなどが起因すると推測される。

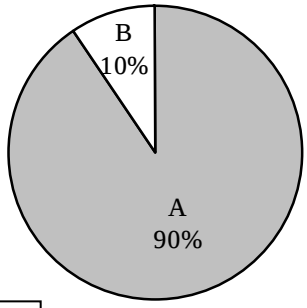
Q6.（Q3 a．b．ｃ．の回答者）個人情報を収集する際、事業者（自ら）の名称、部署、連絡先を明示していますか？　（有効回答会社数＝83 社）

① 全業種合計

【2003 年度】



【2002 年度】

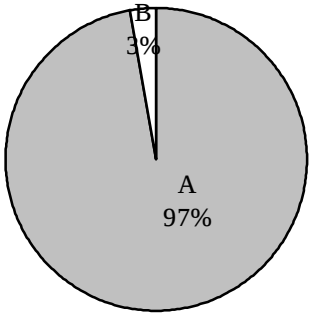


A：　明示している
B：　明示していない

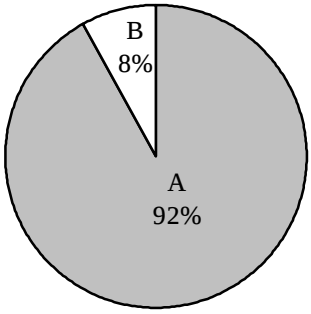
② 業種別

＜情報サービス業＞

【2003 年度】

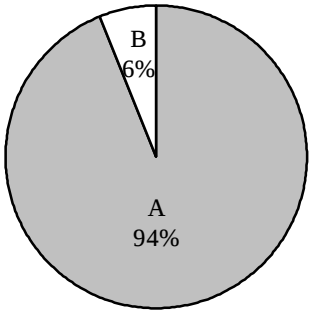


【2002 年度】

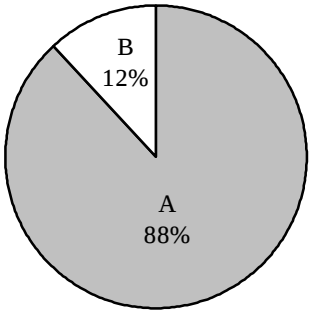


＜製造業＞

【2003 年度】

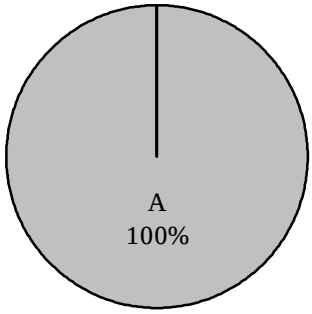


【2002 年度】

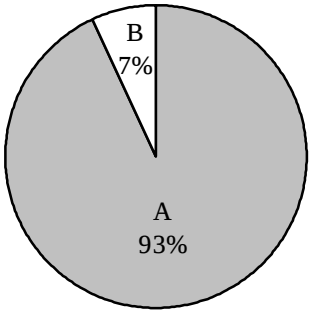


＜金融業＞

【2003 年度】

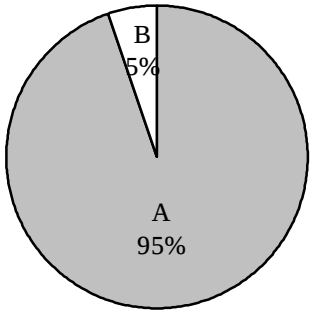


【2002 年度】

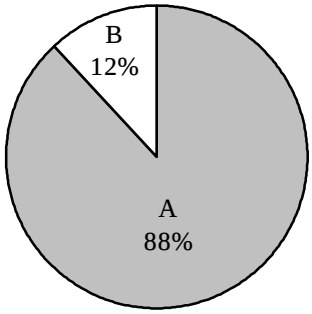


＜その他＞

【2003 年度】



【2002 年度】



図表 2-8　Q6 調査結果

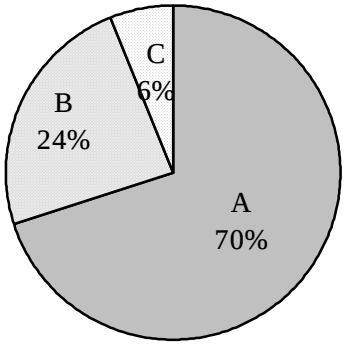
昨年同様に、顧客より個人データを収集する際、大方の企業は名称、部署、連絡先を明示しているとの回答結果である。

Q7.（Q3 a．b．ｃ．の回答者）個人情報を収集する際、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＝83 社）

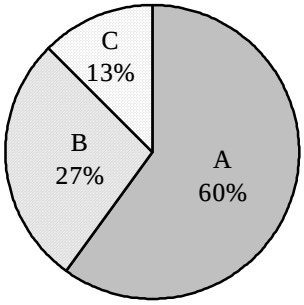
＊同意＝本人より、利用の了承（＝同意）の返信等積極的な意向を表す行為を得ていること

① 全業種合計

【2003 年度】



【2002 年度】

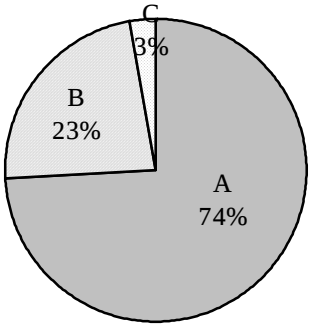


A：　明示し、同意を得ている
B：　明示しているが、同意は得ていない
C：　明示していない

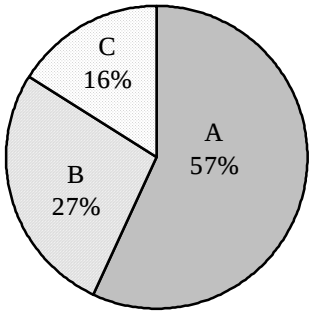
② 業種別

＜情報サービス業＞

【2003 年度】

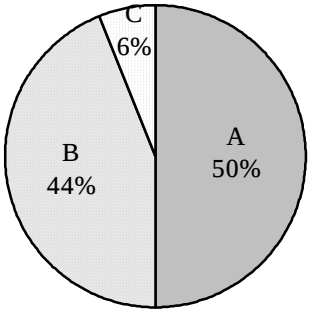


【2002 年度】

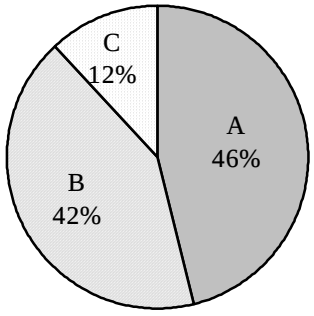


＜製造業＞

【2003 年度】

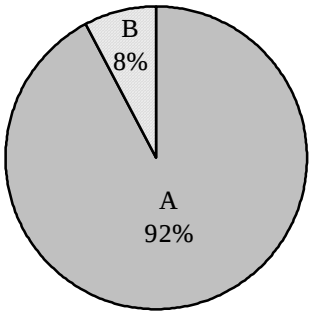


【2002 年度】

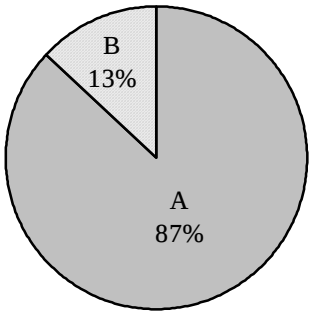


＜金融業＞

【2003 年度】

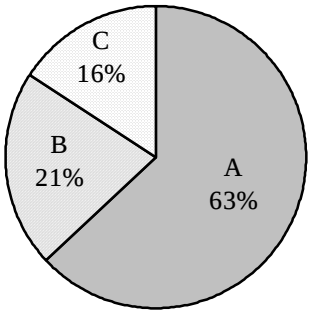


【2002 年度】

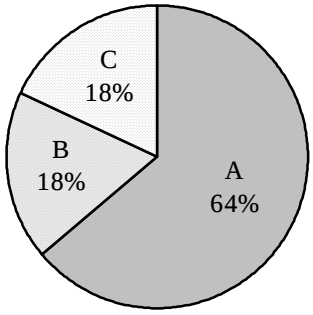


＜その他＞

【2003 年度】



【2002 年度】



図表 2-9　Q7 調査結果

個人データを収集する際、全体の 94%が利用目的を明示しており、昨年（同 87%）をさらに上回る率となった。また「同意を得ている」が 70%とこれも昨年に比べ 10 ポイント上昇しており、個人情報取得時の意識が向上しつつあることが推測できる。金融業は、100%明示しており、また、92%が同意を得ているといった具合に、同意原則が浸透していることが窺える。

Q8.（Q3 a．b．c．の回答者）個人データを第三者に提供することがありますか？

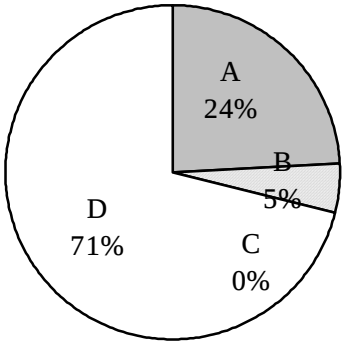
（有効回答会社数＝83 社）

＊　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

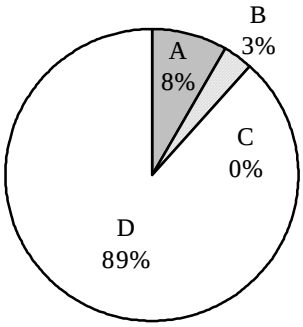
＊　注2）業務委託のため委託業者等に個人データを渡す場合は含みません

① 全業種合計

【2003 年度】



【2002 年度】

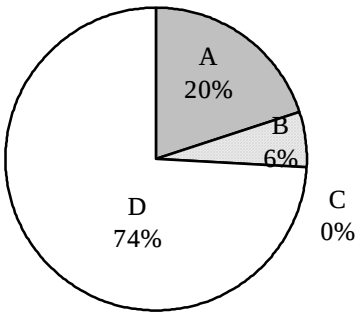


A：　ある、収集する時にそのことを明示し、同意を得ている
B：　ある、収集する時にそのことを明示しているが、同意は取っていない
C：　あるが、収集する時に明示もしておらず、同意も取っていない
D：　ない

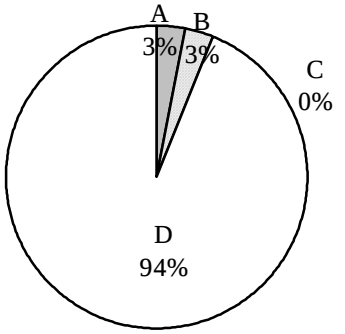
② 業種別

＜情報サービス業＞

【2003 年度】

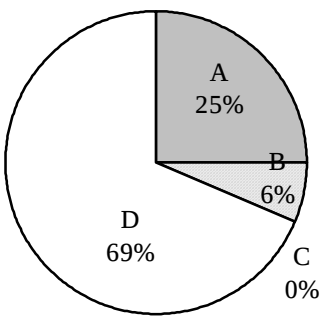


【2002 年度】

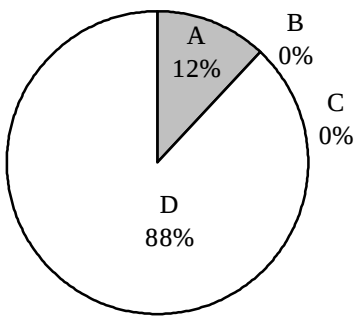


＜製造業＞

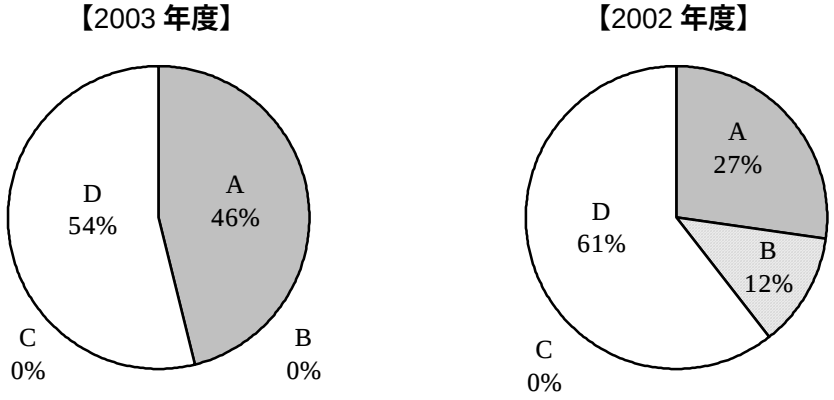
【2003 年度】



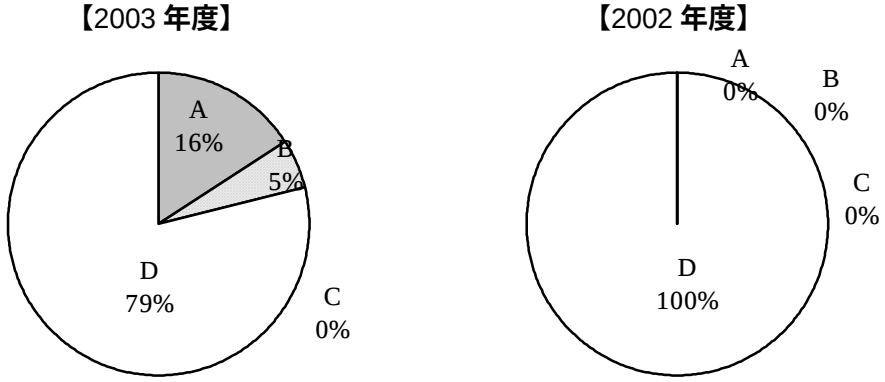
【2002 年度】



＜金融業＞



＜その他＞



図表 2-10　Q8 調査結果

個人情報保護法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し、質問したところ、全体で 30%弱が第三者提供を行っているとの回答であった。第三者提供があるとの回答が多いのは金融業であり、その理由として与信等についての情報を共有することを第三者提供として考えていることが推測される。

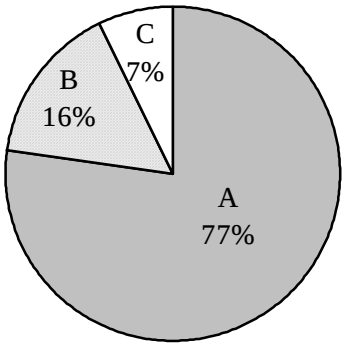
また、他の業容でも、4 分の 1 ぐらいのウェイトで第三者提供が行われており、全体で明示も同意を得ていないは 0%であるが、明示のみが 3%ほどある。

Q9.（Q3 a．b．ｃ．の回答者）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？

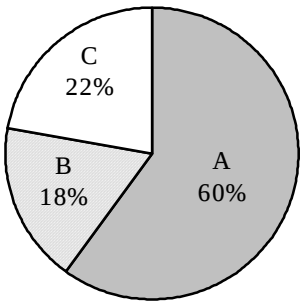
（有効回答会社数＝83 社）

① 全業種合計

【2003 年度】



【2002 年度】

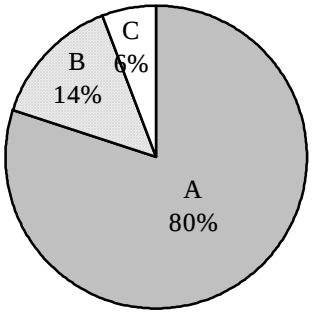


A：　なっている
B：　一部の項目については開示･変更には応じるが一部のものは応じない
C：　なっていない

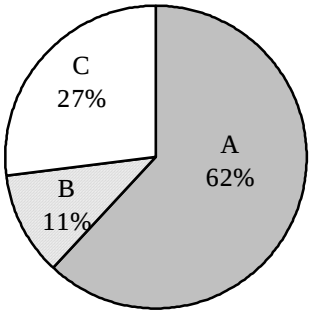
② 業種別

＜情報サービス業＞

【2003 年度】

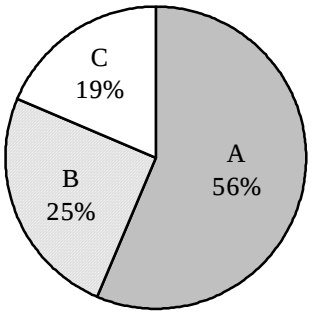


【2002 年度】

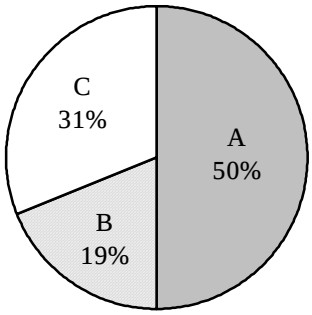


＜製造業＞

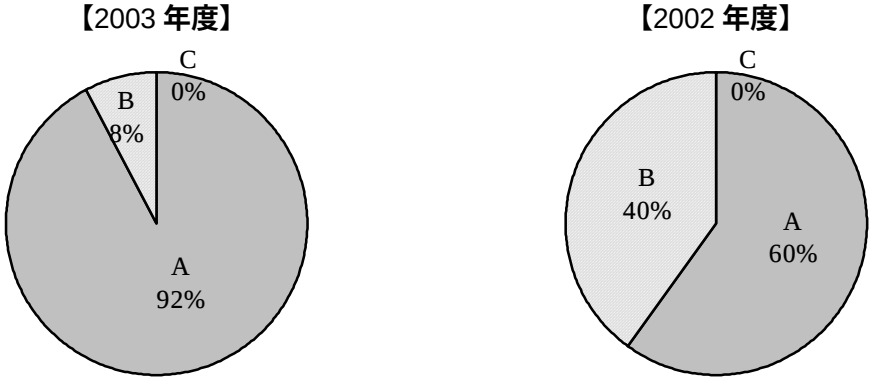
【2003 年度】



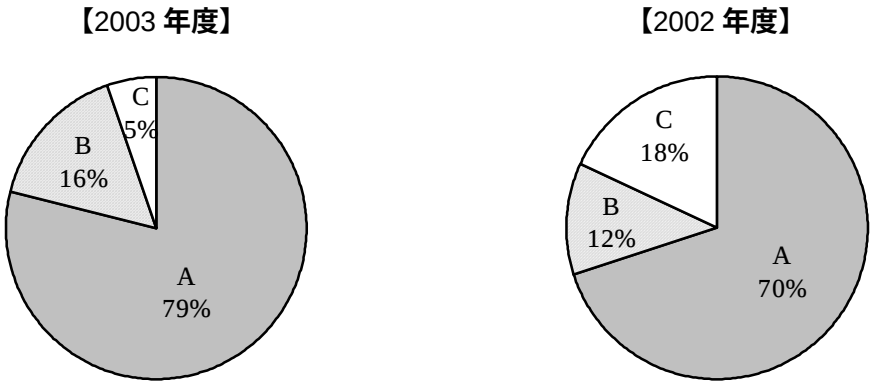
【2002 年度】



＜金融業＞



＜その他＞

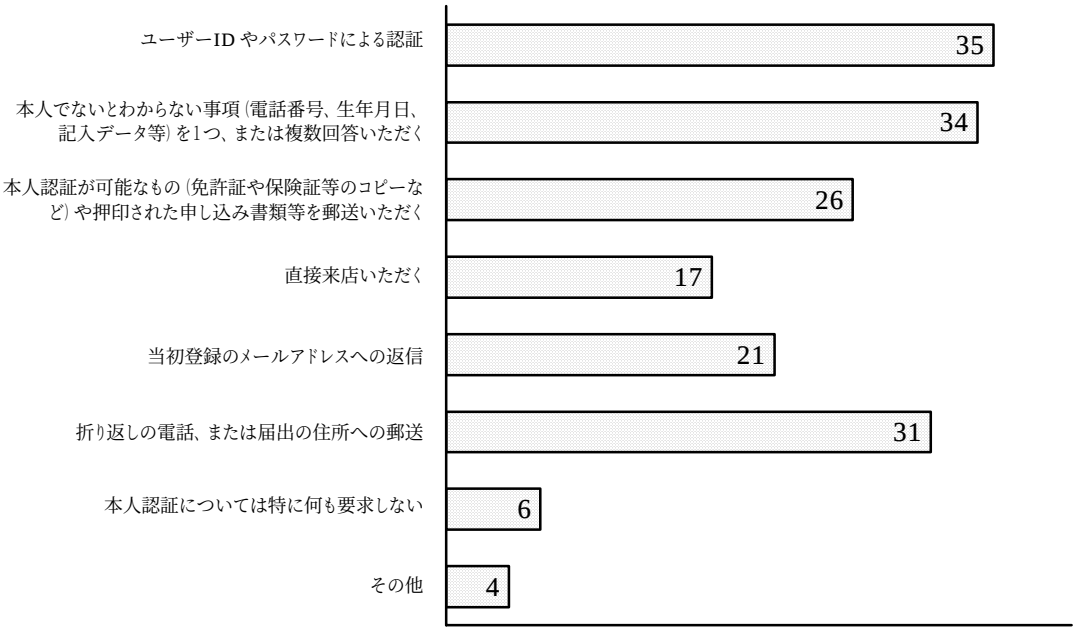


図表 2-11　Q9 調査結果

開示や変更、利用停止等の体制整備がどの程度進んでいるかを調べた。昨年度との比較では、全体で 9 割強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製造業において 2 割ほど未整備の企業がある。

Q10.（Q3 a．b．ｃ．の回答者）問⑨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＝83 社）



その他の回答詳細

- 特に決まっていない
- 問い合わせ毎に ID を発行する
- ユーザーＩＤ＝メールアドレスで運営

図表 2-12　Q10 調査結果

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く、「本人でないとわからないような事項を回答」「折り返しの電話または届出の住所への郵送」などが現状は一般的である。本人への開示にあたっては、保護法 29 条および政令により事業者が本人確認の方法について定めることができるが、その方法が脆弱であるとなりすまし等により本人データの漏洩ににもなりうるので、その方策について熟慮する必要がある。

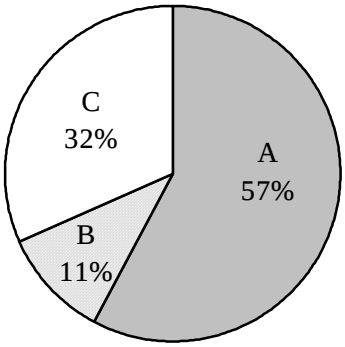
なお、何も要求しないとの回答が 6 件（昨年は 16 件）ある。

Q11．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？

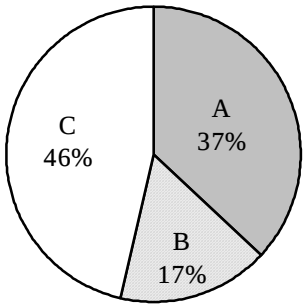
（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

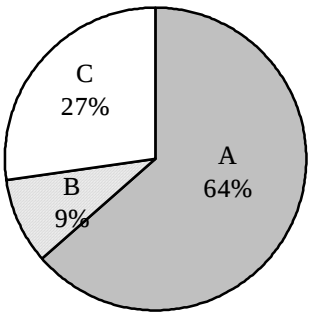


A：　トップページに、あるいはそこからリンクできるように顧客に見え易い形で示している
B：　示しているが、わかりにくいかもしれない
C：　示していない

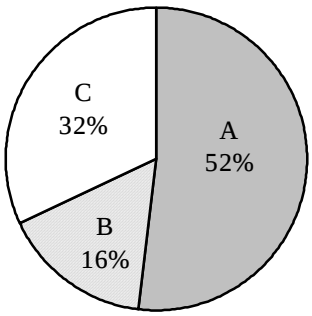
② 業種別

＜情報サービス業＞

【2003 年度】

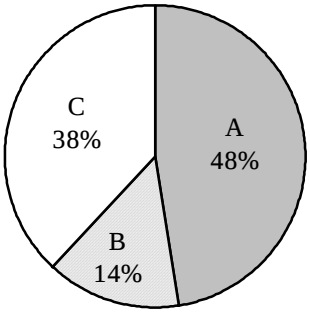


【2002 年度】

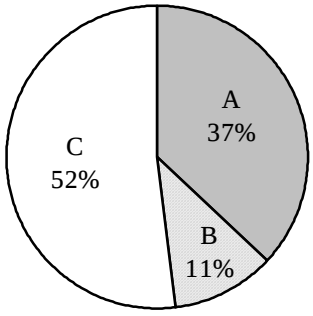


＜製造業＞

【2003 年度】

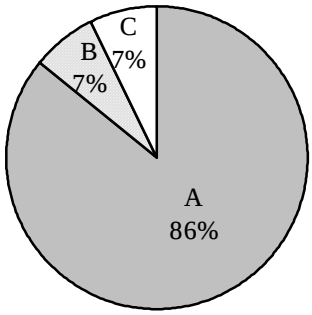


【2002 年度】

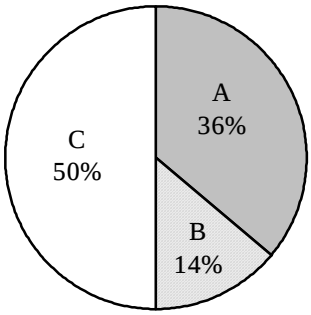


＜金融業＞

【2003 年度】

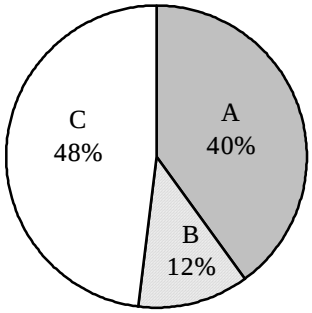


【2002 年度】

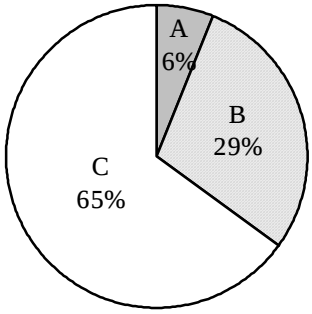


＜その他＞

【2003 年度】



【2002 年度】



図表 2-13　Q11 調査結果

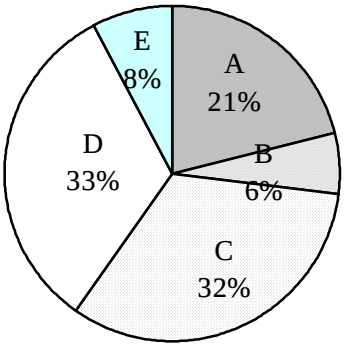
昨年度の回答結果と比べ、プライバシーポリシーをトップページまたはお客様に見えやすいところに示す会社が 20 ポイントも増加した。トップページではないがプライバシーポリシーを掲げているところを足すと約 7 割が掲載しているとの回答である。

昨年と対比で顕著な変化は、金融業でプライバシーポリシーを示していない会社が昨年は 50%であったのに対し本年度はわずか 7%に現象し、プライバシーをトップに掲載する会社が 86%（昨年 36%）と業種別の中でも最も高率になった点である。

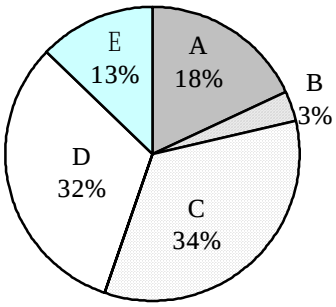
Q12．個人情報の取扱いを適正に行っていることを証明する「プライバシーマーク制度」について知っていますか？　（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

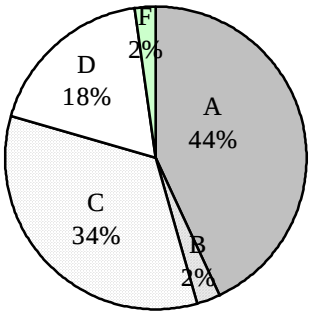


A：　取得している
B：　一部の部門で所得している
C：　現在取得はしていないが、取得を考えている
D：　知っているが、取得していないし、取得を考えてもいない
E：　知らない

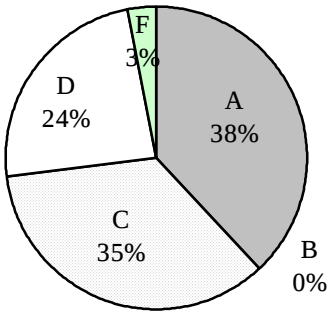
② 業種別

＜情報サービス業＞

【2003 年度】

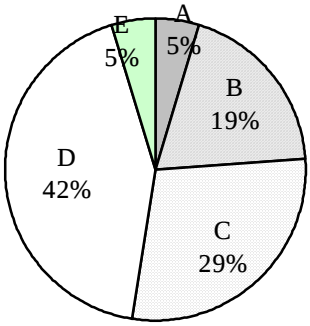


【2002 年度】

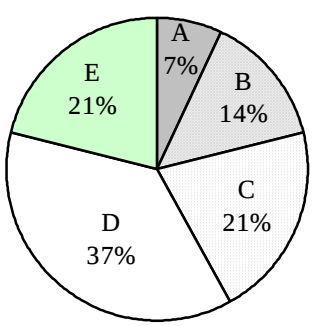


＜製造業＞

【2003 年度】

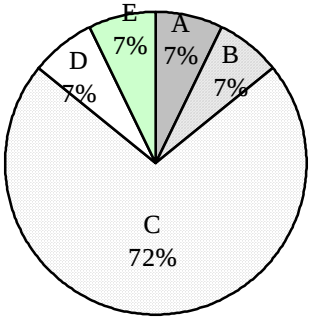


【2002 年度】

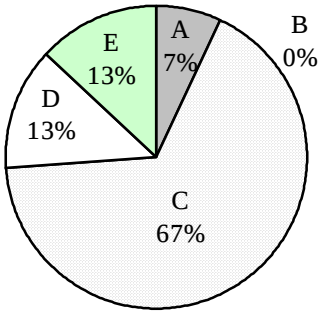


＜金融業＞

【2003 年度】

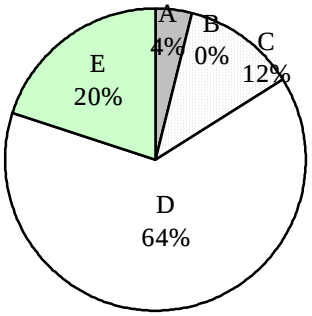


【2002 年度】

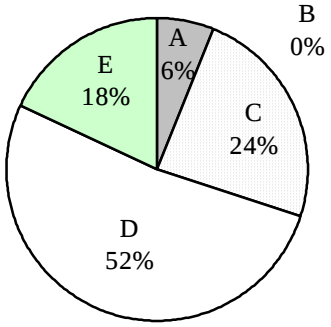


＜その他＞

【2003 年度】



【2002 年度】



図表 2-14　Q12 調査結果

プライバシーマークについても、昨年と比較して、概ねその認知度と取得および取得への意向が増大してきている。

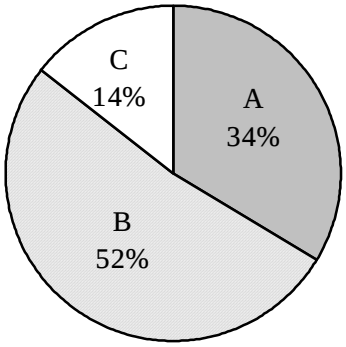
業種別にみると、情報サービス業では、業務受託のためにマーク取得が信頼性を証明するのに有効である点やプライバシーマークのマーク付与認定団体である財団法人日本情報サービス産業協会に加入しているところが多い点などを背景として、取得している企業が 46%（一部の部門の取得を含む）と他の業界に比べ断然高い。

また、金融業では、現時点で取得している企業はまだ 14%（一部の部門の取得を含む）と少ないものの、「取得を考えている」企業が 72%と昨年（同 67%）以上に増加している。

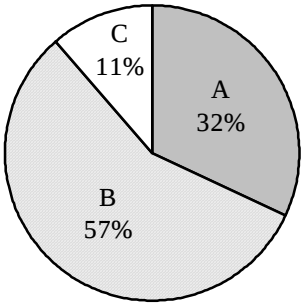
Q13．お客さまからアクセスがある際にお客さまが再度そのサイトに訪れたとき、通信履歴データをサーバー側で認識し、利用者の手続上の再入力等を省くことができるクッキーというしくみを利用していますか？　　（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

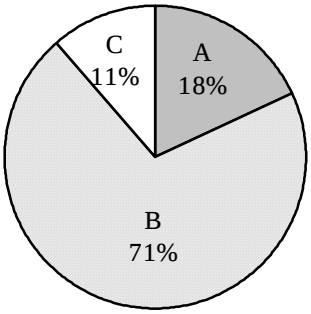


A：　クッキーを利用している
B：　クッキーは利用していない
C：　クッキーについてはよくわからない

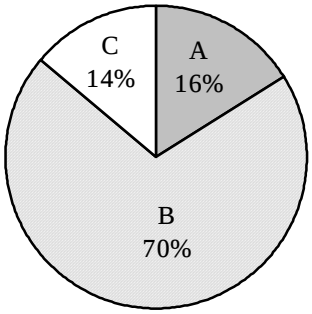
② 業種別

＜情報サービス業＞

【2003 年度】

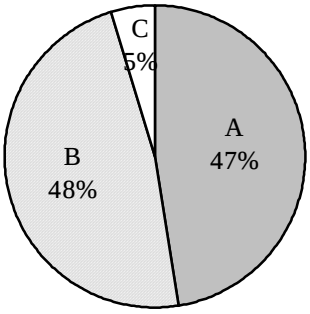


【2002 年度】

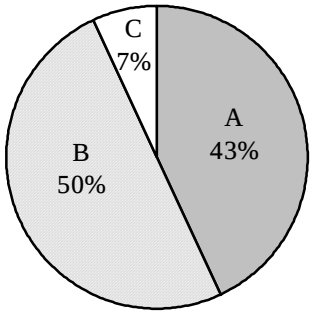


＜製造業＞

【2003 年度】

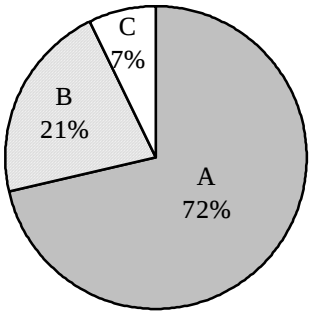


【2002 年度】

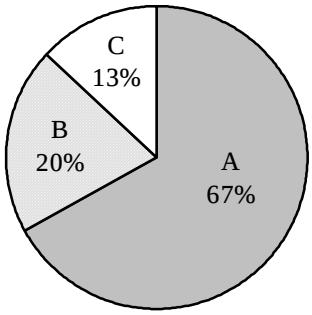


＜金融業＞

【2003 年度】

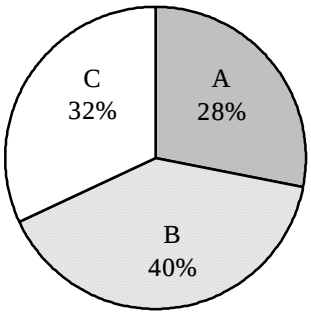


【2002 年度】

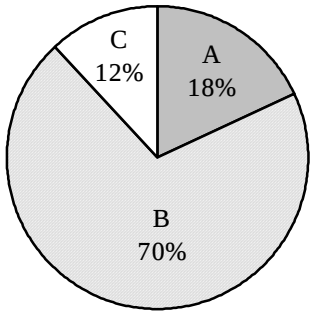


＜その他＞

【2003 年度】



【2002 年度】



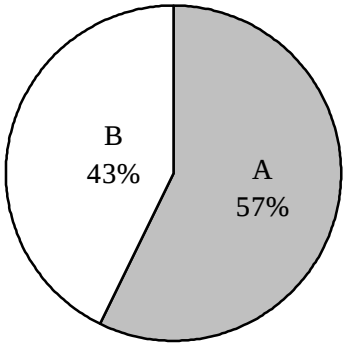
図表 2-15　Q13 調査結果

全体では 34%と昨年とほぼ同じぐらいの率の企業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 47%と続く。

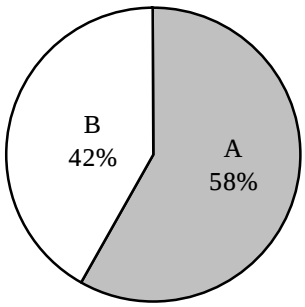
Q14．（上記 A の回答者のみ）クッキーを利用していることと、その利用目的を明示していますか？　　（有効回答会社数＝42 社）

① 全業種合計

【2003 年度】



【2002 年度】

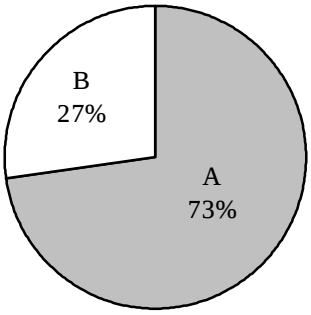


A：　明示している
B：　クッキーの利用に関しては特に知らせていない

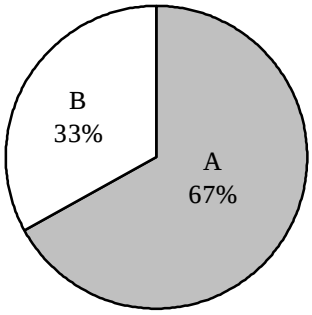
② 業種別

＜情報サービス業＞

【2003 年度】

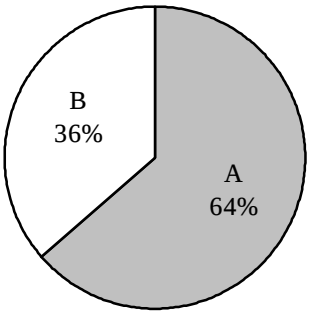


【2002 年度】

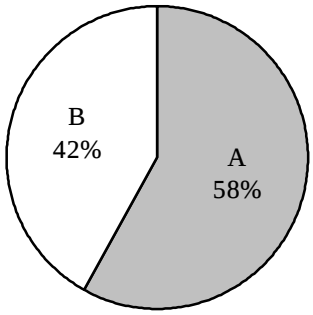


＜製造業＞

【2003 年度】

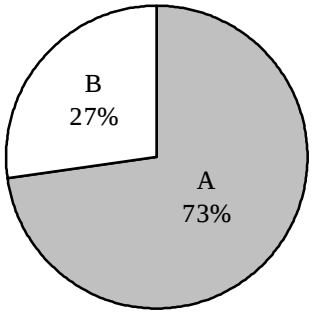


【2002 年度】

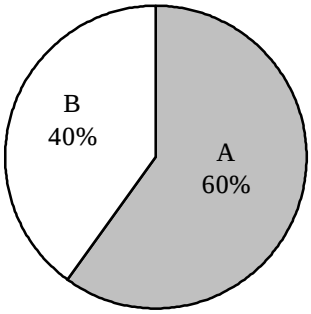


＜金融業＞

【2003 年度】

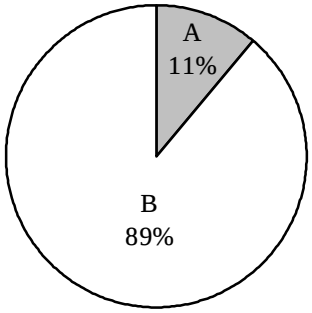


【2002 年度】

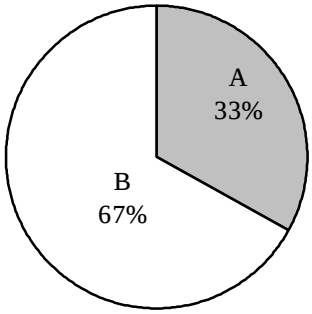


＜その他＞

【2003 年度】



【2002 年度】



図表 2-16　Q14 調査結果

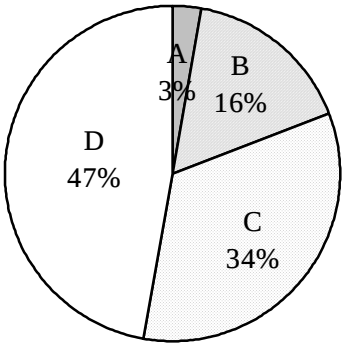
クッキーを利用する会社のみの回答のためサンプル件数が 42 件と少ないが、昨年同様、明示しているが 6 割程度である。

Q15．「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

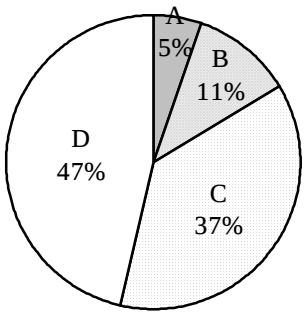
（有効回答会社数＝104 社）

① 全業種合計

【2003 年度】



【2002 年度】

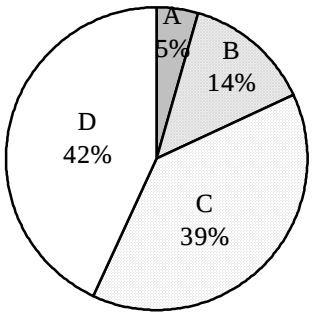


A：　採用し、運用している
B：　まだ採用していないが、検討している
C：　採用を検討していない
D：　知らない

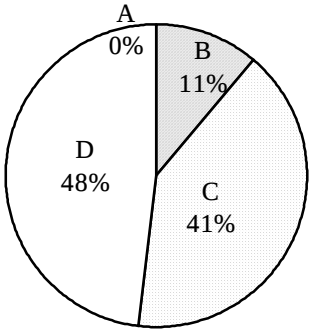
② 業種別

＜情報サービス業＞

【2003 年度】

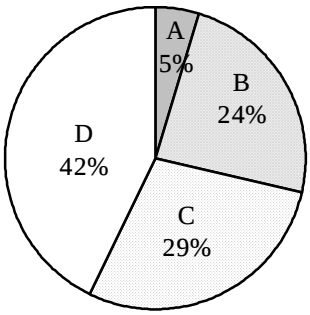


【2002 年度】

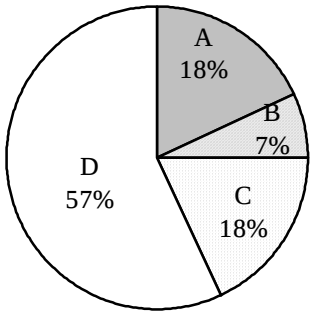


＜製造業＞

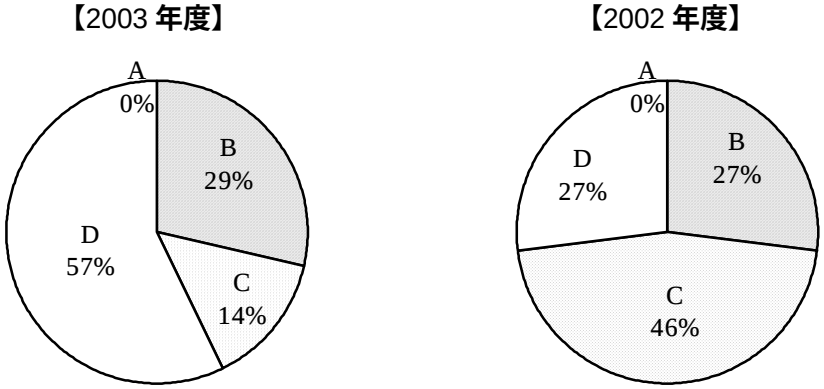
【2003 年度】



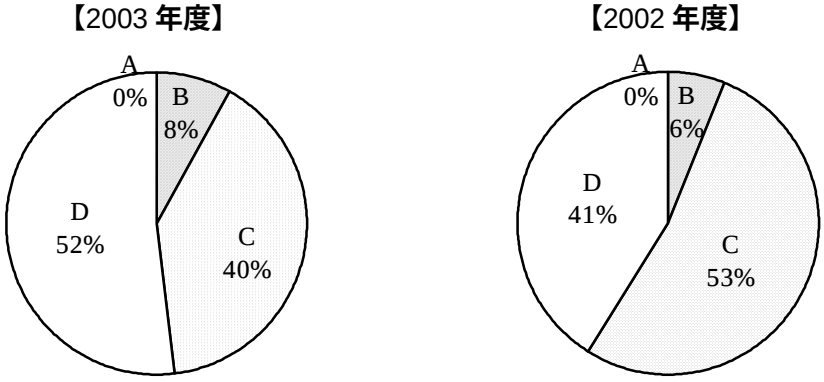
【2002 年度】



＜金融業＞



＜その他＞



図表 2-17　Q15 調査結果

Ｐ３Ｐについては、日本においては、財団法人ニューメディア開発協会にて 2002 年 4 月に標準仕様が公開され、Ｐ３Ｐ 2002 年 4 月勧告版対応のプライバシーポリシーウィザードや取扱説明書等がホームページ上に掲げられており、今後の普及が期待される。

ただし、本アンケート結果では、「採用している」と「検討している」を合わせても 19%と昨年とほぼ同様の結果に留まっている。

2.1.5　まとめ

以上のように、昨年に引き続き、ＥＣＯＭ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、設問ごとの分析を行った。昨年との比較においては、審議が長引いた個人情報保護法の成立の影響で、一様に個人情報保護体制の整備が進んでいると見受けられる。

しかしながら、昨今も頻繁にマスコミに報道された企業の保有する個人情報漏洩事件等を見ると社内規定整備やプライバシーポリシーの公表等が進む反面、業務の現場における従業者への意識の徹底浸透がまだまだ不十分な状況といえよう。

現時点では、保護法の個人情報取扱事業者の義務規定は施行前であり、報道されるような個人情報の漏洩や目的外の利用等が法的な制裁を受けるケースはほとんどないものの、社会的批判を浴び、顧客への信頼とブランドイメージを守るための事後対策に相当費用を費やす事態も多く見られ、こうしたリスクに経営的な危機感を抱く経営者は、まず、社内規定や組織整備等に着手することになろう。こうした体制作りを行うことは大切であるが、その次のステップとして末端への意識浸透が不可欠であり、そのレベルを上げていくことには相当の時間と手間がかかるものである。

日本の企業は、保護法の義務規定施行の 2005 年 4 月に向け、従業者への教育や監査体制の確立とその実施等、更なる個人情報保護の実践に向けた推進が求められる。

2.2　ＥＣＯＭ会員企業・団体ＷＥＢページ個人情報保護表記目視調査

会員企業・団体対象に行ったアンケートと同様に、昨年度に引き続き、同ＷＥＢページにおける個人情報保護に関する記載状況についての目視調査を実施した。

昨年の調査項目に加え、本年度はプライバシーポリシー上に利用目的や第三者提供、クッキーの使用等についてどういった項目について述べられているかという記載事項についても集計してみた。

2.2.1　目視調査の概要

（1）調査方法：会員のホームページ検索

（2）調査日程：2003 年 7 月 10 日～18 日

（3）調 査 数：249 社

（4）昨年度調査した企業・団体との件数比較

	2 年連続	02 年のみ	03 年のみ	合計
2002 年度	227 社（81.7%）	51 社（18.3%）		278 社
2003 年度	227 社（91.2%）		22 社（8.9%）	249 社

2.2.2　プライバシーポリシーについて

ホームページ上にプライバシーポリシーを表記している企業団体は、調査した 249 社（内有効件数 245 件）中 140 社（56%）と、昨年（106 社，38%）と比べ、この 1 年で 19 ポイント増加した。その内 121 社はトップページより、リンクするような表示となっている。

また、2002 年度より連続して調査した 227 社に関して、ホームページ上にプライバシーポリシーを表記している企業団体をみても、2002 年が 83 社（37%）であったのに対し、2003 年は 128 社（56%）とほぼ同率で増えている。

余談であるが、昨年度の調査時には多く見られたフラッシュを使用し、動的にトップ画面を表示していたパターンは、多少減少している印象があった。

本年度は、プライバシーポリシーに盛り込まれている内容についても調査した（図表 2-21）。もっとも多く盛り込まれているのは「セキュリティについて」であり、セキュリティのレベルや方針、方策等について 88%の企業団体が表記していた。

続いて、「第三者提供の有無について」、「利用目的について」が多かったが、その表現についてはかなりのバリエーションがある。「当社の製品やサービスの情報提供のため」といったように、具体的な措置が記載されているものもあったが、「了解いただいた目的

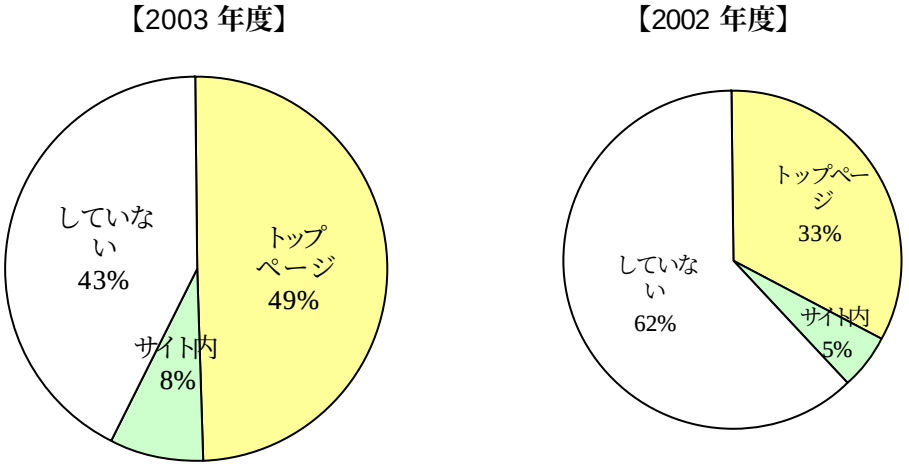
の範囲内で、お客様の個人情報を利用」といった表現にとどめ、個々に取得する時点での明示や通知に委ねている企業もあった。

個人情報についての「連絡先」については 63%、プライバシーポリシーの「発効日」については 42%の企業団体が表記していた。

また、「クッキーの使用」については、32%の企業団体で記載されていた。そのパターンとしては概ね、クッキーを使用していることを明らかにした上で、クッキーの仕組みについて説明し、さらに、そのうちいくつかのサイトについては、クッキー情報については統計情報として収集され、個人情報と関連付けられることはないと断わっているものが見られた。

ECOM 個人情報保護ガイドライン Ver.1.0 より推奨している「子供の個人情報について」は、対象が子供向けでないサイトが多い関係からか、8%であった。

（1）ホームページ上に表記している企業･団体



図表 2-18　ホームページ上に表記している企業･団体比率

(2) 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

	会社･団体名
1	アコム株式会社
2	ｱﾒﾘｶﾝ･ｴｷｽﾌﾟﾚｽ･ｲﾝﾀｰﾅｼｮﾅﾙ･ｲﾝｺｰﾎﾟﾚｲﾃｯﾄﾞ
3	株式会社ＮＴＴデータ
4	株式会社オーエムシーカード
5	川鉄情報システム株式会社
6	株式会社ジェーシービー
7	株式会社東芝
8	日本電気株式会社
9	日本アイ･ビー･エム株式会社
10	日本ユニシス株式会社
11	株式会社野村総合研究所
12	ビザ･インターナショナル
13	株式会社日立製作所
14	株式会社富士総合研究所
15	富士通株式会社
16	富士電機株式会社
17	マイクロソフト株式会社
18	ﾏｽﾀｰｶｰﾄﾞ･ｲﾝﾀﾅｼｮﾅﾙ･ｼﾞｬﾊﾟﾝ･ｲﾝｸ
19	株式会社三菱総合研究所
20	三菱電機株式会社
21	株式会社ＵＦＪ銀行
22	株式会社アイネス
23	IBMﾋﾞｼﾞﾈｽｺﾝｻﾙﾃｨﾝｸﾞｻｰﾋﾞｽ株式会社
24	アクセンチュア株式会社
25	アップルコンピュータ株式会社
26	株式会社アプラス
27	株式会社アルゴ２１
28	株式会社ＳＲＡ
29	ＮＥＣソフト株式会社
30	株式会社ｴﾇ･ﾃｨ･ﾃｨ･データ経営研究所
31	ｴﾇ･ﾃｨ･ﾃｨ･ｺﾐｭﾆｹｰｼｮﾝｽﾞ株式会社
32	ＮＴＴコムウェア株式会社
33	株式会社NTTドコモ
34	株式会社FFC
35	株式会社オリエントコーポレーション
36	ＫＤＤＩ株式会社
37	コンピュータ･アソシエイツ株式会社
38	株式会社シー･アイ･シー
39	新日鉄ソリューションズ株式会社
40	セイコーインスツルメンツ株式会社
41	セコムトラストネット株式会社
42	株式会社セントラルファイナンス
43	大日本印刷株式会社
44	中部電力株式会社
45	株式会社テプコシステムズ
46	東北電力株式会社
47	日本信販株式会社
48	ニフティ株式会社
49	株式会社日本総合研究所
50	日本電子計算機株式会社
51	日本電信電話株式会社
52	日本認証サービス株式会社
53	日本ベリサイン株式会社
54	日本ユニシス情報システム株式会社
55	東日本電信電話株式会社
56	日立キャピタル株式会社
57	株式会社日立情報システムズ
58	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社
59	富士通エフ･アイ･ピー株式会社
60	株式会社富士通総研

	会社･団体名
61	株式会社富士通中部システムズ
62	三井住友カード株式会社
63	三井住友海上火災保険株式会社
64	株式会社ＵＦＪカード
65	ユーシーカード株式会社
66	株式会社ローソン
67	朝日監査法人
68	イオンクレジットサービス株式会社
69	株式会社イプシ･マーケティング研究所
70	株式会社インターコム
71	株式会社インテリジェントウェイブ
72	株式会社エクサ
73	NEC東芝情報システム株式会社
74	ＮＥＣネクサソリューションズ株式会社
75	株式会社エヌ･ティ･ティ･ドコモ関西
76	オムロン株式会社
77	カシオ計算機株式会社
78	関西電力株式会社
79	キヤノン株式会社
80	九州電力株式会社
81	グローバルフォーカス株式会社
82	株式会社構造計画研究所
83	国内信販株式会社
84	小林記録紙株式会社
85	佐川ｺﾝﾋﾟｭｰﾀ･システム株式会社
86	株式会社さくらケーシーエス
87	株式会社シーエーシー
88	四国電力株式会社
89	株式会社資生堂
90	株式会社ジャックス
91	株式会社ジャルカード
92	昌栄印刷株式会社
93	セイコープレシジョン株式会社
94	株式会社ｿﾆｰﾌｧｲﾅﾝｽｲﾝﾀｰﾅｼｮﾅﾙ
95	ソラン株式会社
96	株式会社第一勧銀情報システム
97	ＴＩＳ株式会社
98	株式会社電通国際情報サービス
99	東芝情報システム株式会社
100	東芝テック株式会社
101	東芝ファイナンス株式会社
102	トランス･コスモス株式会社
103	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
104	パシフィックシステム株式会社
105	株式会社パワードコム
106	株式会社BSNアイネット
107	日立ビジネスソリューション株式会社
108	株式会社フジサンケイリビングサービス
109	富士写真フィルム株式会社
110	富士ゼロックス株式会社
111	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
112	株式会社富士通長野システムエンジニアリング
113	株式会社富士通ビジネスシステム
114	株式会社富士通北陸システムズ
115	ブラザー工業株式会社
116	マイトリップ･ネット株式会社
117	三井物産株式会社
118	ミノルタ株式会社
119	ヤマトシステム開発株式会社
120	横河電機株式会社
121	株式会社菱化システム

図表 2-19　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

（3）トップページにリンクボタンはないが、サイト内に表示している会員・団体

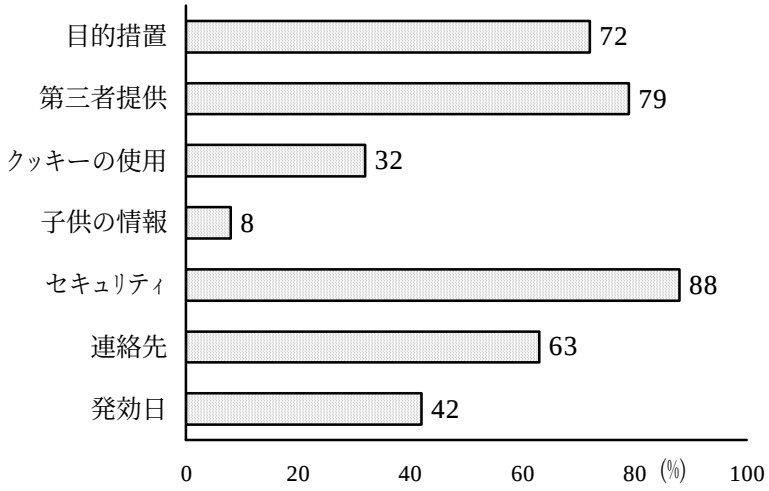
	会社･団体名
1	東京電力株式会社
2	松下電器産業株式会社
3	セイコーエプソン株式会社
4	日本オラクル株式会社
5	岩谷産業株式会社
6	株式会社インテージ
7	興和株式会社
8	株式会社小松製作所
9	株式会社ＣＳＫ
10	株式会社シーフォーテクノロジー
11	シャープ株式会社
12	ダイセル化学工業株式会社
13	大日本インキ化学工業株式会社
14	中国電力株式会社
15	株式会社ティージー情報ネットワーク
16	日立電線株式会社
17	富士重工業株式会社

（4）関連会社に表記している企業･団体

	会社･団体名
1	三洋電機株式会社
2	ソニー株式会社

図表 2-20　サイト内および関連会社に表記している企業･団体一覧

（5）盛り込まれている内容（全体＝140 件）



●セキュリティの表現は、88%（123 件）

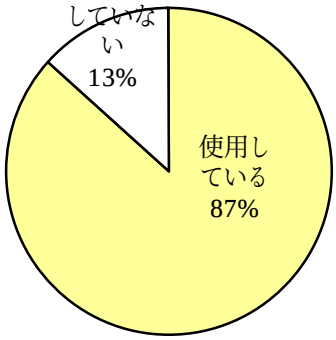
●第三者提供をする/しないの表現は、79%（110 件）

●子供の情報についての表現は、8%（11 件）

●クッキーについての表現は、32%（45 件）

図表 2-21　盛り込まれている内容

（6）クッキーについて表現している企業･団体のうち、クッキーを使用している割合



●クッキーを使用しているのは、87%

表記パターン:

- クッキーは使用している
- クッキーの仕組みの説明
- 情報は統計として収集され、個人情報と関連付けられることはありません　等

図表 2-22　クッキーを使用している割合

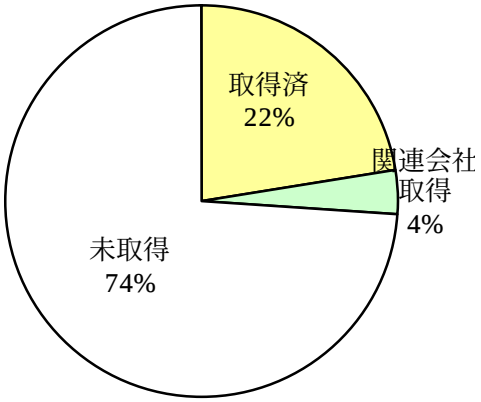
2.2.3　プライバシーマークについて

2004年1月時点でプライバシーマーク取得会社は 666 社（2003 年 3 月時点468社）と、この 1 年足らずで200社ほど増えている。ECOM 会員企業団体では 56 社（22%）が取得しており、さらに関係会社や社内分社等で取得しているところを加える26%に及び、昨年に比べ10ポイント増加したことになる。

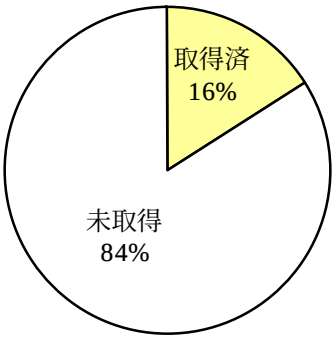
そのうち、プライバシーマークをトップページに表記している企業･団体は、25 社（45%）であり、トップページでなく階層内に表記しているのが 22 社（39%）、ホームページ上に表示していないようであるのが16%ほどあった。これは、マーク取得を消費者に対する個人情報保護の信頼の証としての機能よりも、情報処理業務等の委託を受ける際のメリットとして同マークを取得している事業者が相当数あることが要因と考えられる。

(1) プライバシーマークを取得している企業･団体の比率

【2003 年度】



【2002 年度】



図表 2-23　プライバシーマークを取得している企業･団体の比率

(2) プライバシーマークを取得している企業･団体

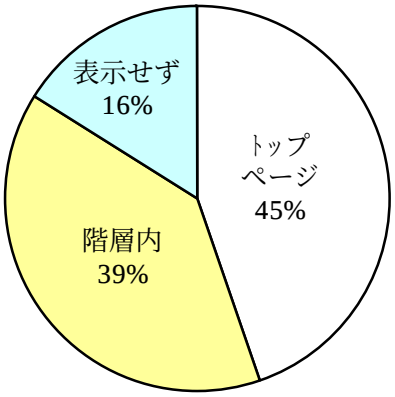
	会社･団体名
1	株式会社NTTデータ
2	株式会社オーエムシーカード
3	川鉄情報システム株式会社
4	株式会社東芝
5	日本電気株式会社
6	株式会社野村総合研究所
7	株式会社日立製作所
8	株式会社富士総合研究所
9	富士通株式会社
10	松下電器産業株式会社
11	株式会社三菱総合研究所
12	株式会社アイネス
13	株式会社アルゴ21
14	株式会社SRA
15	NECソフト株式会社
16	NTTコムウェア株式会社
17	新日鉄ソリューションズ株式会社
18	大日本印刷株式会社
19	株式会社テプコシステムズ
20	ニフティ株式会社
21	株式会社日本総合研究所
22	日本ユニシス情報システム株式会社
23	株式会社日立情報システムズ
24	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社
25	富士通エフ･アイ･ピー株式会社
26	三井住友カード株式会社
27	イオンクレジットサービス株式会社
28	株式会社インテージ

	会社･団体名
29	株式会社インテリジェントウェイブ
30	株式会社エクサ
31	NECネクサソリューションズ株式会社
32	オムロン株式会社
33	キーウェア ソリューションズ株式会社
34	グローバルフォーカス株式会社
35	株式会社構造計画研究所
36	小林記録紙株式会社
37	株式会社さくらケーシーエス
38	株式会社シーエーシー
39	株式会社CSK
40	昌栄印刷株式会社
41	ソラン株式会社
42	株式会社第一勧銀情報システム
43	中国情報システムサービス株式会社
44	TIS株式会社
45	株式会社電通国際情報サービス
46	東芝情報システム株式会社
47	トランス･コスモス株式会社
48	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
49	パシフィックシステム株式会社
50	株式会社BSNアイネット
51	富士ゼロックス株式会社
52	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
53	マイトリップ･ネット株式会社
54	ヤマトシステム開発株式会社
55	株式会社菱化システム
56	株式会社両毛システムズ

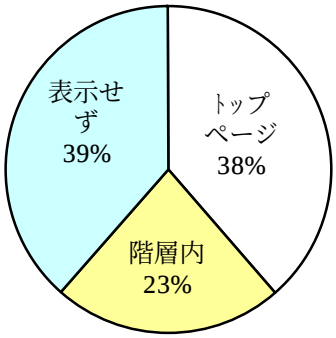
図表 2-24　プライバシーマークを取得している企業･団体一覧

(3) 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･団体の比率

【2003 年度】



【2002 年度】



図表 2-25　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･団体の比率

(4) 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

	会社･団体名
1	株式会社オーエムシーカード
2	株式会社富士総合研究所
3	株式会社三菱総合研究所
4	株式会社アイネス
5	株式会社SRA
6	NECソフト株式会社
7	株式会社テプコシステムズ
8	ニフティ株式会社
9	株式会社日本総合研究所
10	日本ユニシス情報システム株式会社
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	昌栄印刷株式会社
16	ソラン株式会社
17	株式会社第一勧銀情報システム
18	TIS株式会社
19	株式会社電通国際情報サービス
20	東芝情報システム株式会社
21	株式会社BSNアイネット
22	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
23	マイトリップ･ネット株式会社
24	ヤマトシステム開発株式会社
25	株式会社菱化システム

(5) サイト内に表記している企業･団体

	会社･団体名
1	川鉄情報システム株式会社
2	株式会社東芝
3	日本電気株式会社
4	株式会社野村総合研究所
5	株式会社日立製作所
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	株式会社日立情報システムズ
10	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社
11	イオンクレジットサービス株式会社
12	株式会社インテージ
13	株式会社インテリジェントウェイブ
14	株式会社エクサ
15	グローバルフォーカス株式会社
16	株式会社構造計画研究所
17	小林記録紙株式会社
18	株式会社シーエーシー
19	株式会社CSK
20	ﾄﾗﾝｽ･ｺｽﾓｽ株式会社
21	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
22	パシフィックシステム株式会社

図表 2-26　トップページ及びサイト内に表記している企業･団体一覧

3 ECOM 個人情報保護ガイドライン改定

3.1 ECOM 個人情報保護ガイドライン Ver.2.0＜α版＞の策定

昨年度、従来の「ＥＣＯＭ個人情報保護ガイドライン Ver.1.0」の改定検討を進めたが、結果的に保護法成立にいたらず、年度末の報告書では改定案 ver1.5 として掲載した。

2003 年 5 月の個人情報保護法の成立を受け、本年度前半の ECOM 個人情報保護 SWG の主活動として、それに対応するガイドライン Ver.2.0 の仕上げに取り組んだ。

3.1.1 ガイドラインタスクフォースの推進

ガイドライン Ver.2.0 の策定にあたっては､昨年キーマンとして検討に加わっていただいた委員のうち本年度も SWG に参加いただいたメンバー6 名に今年度新たに SWG に参加されたメンバー3 名が加わり、さらにアドバイザー4 名と事務局の 14 名（P200、メンバー表参照）で、下記に示すようなガイドライン改定案 Ver.1.5 策定時点で継続検討を要するとされた課題を中心に 6 月～8 月の期間にてディスカッションを重ねた。

＜Ver1.5 時点で継続検討を要するとされた課題＞

- 利用目的の特定とその具体的措置についてどこまで表現するか
- 第三者提供・共同利用・委託についての解釈
- 得意先・従業員の個人情報に関する取扱い

  （例）顧客情報の DB 化/利用に関して/他社に自社社員の個人情報を提出する時
- 特定の機微な個人情報の取扱い
- サイバーモール運営者の責任
- その他

Ver.1.5 との大きな修正点は、特定の機微な個人情報の取扱いについての条項を削除したが、企業において、個人の権利利益の保護への一層の配慮と顧客とのトラブルの未然防止の観点より、それら情報の取得時および取得の状況や顧客との関係においてセンシティブになり得る情報の取得時は、取扱いや保管に関して更に厳格に運用されるべきことを解説に明記した。

その他、主な修正点については付表 3-1 に示すとおりである。

付表3-1 ＥＣＯＭ個人情報保護ガイドラインＶer.2.0＜α版＞ 修正一覧表

NO.	条	本文／解説	改定案<Ver.1.5>	Ver.2.0<α版>	理由
1	全文		法案	個人情報保護法	
2	第1条	本文	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。	第1条　このガイドラインは、電子商取引において個人情報を取り扱う事業者に対し、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。	主旨をより性格に表現
3	第2条	解説	追加	3. このガイドラインは、上記に該当する事業者が任意に採用できるものであり、法的な拘束性を持つものではないので、その取り扱う個人情報の量や利用方法により事業者等を限定しない。 4. このガイドラインでは事業者が取り扱うすべての個人情報を適用の対象とするが、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、所轄官庁の指針又は指導に従い、別途細目を定められることが望ましい。	インハウス情報について細目を言及していないことを明記
4	第3条	解説5	5. 個人情報保護法では前述のとおり「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。	5. 個人情報保護法では、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「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」に相当すると考える。	保護法の表記に合わせ、誤解のないように修正
5	第3条	解説8	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り扱う事業者」を指す。ちなみに個人情報保護法では「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。	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り扱う事業者」を指す。なお、第2条解説4.に示すように、このガイドラインは、適用対象の事業者に対して法的な拘束性を持つものではないので、個人情報保護法における「個人情報取扱事業者」にてその取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。	事業者が任意に採用できるものであり、法的な拘束性を持つものではないため
6	第7条	解説2	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なく、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。	2.「同意」とは、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。後日の立証の容易性を考えると、書面の場合では本人による署名、捺印等が、また、ウェブ画面上では同意のボタンへのチェック、確認メールの返信、電子署名等の方法がこれにあたる。	「明示的同意」「黙示敵同意」を概念として区分して考えない

NO.	条	本文／解説	改定案<Ver.1.5>	Ver.2.0<α版>	理由
7	第7条	解説3	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はなく、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。	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はなく、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て個人情報を取り扱うときには、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できる。	「明示的同意」「黙示敵同意」を概念として区分して考えない
8	第8条	解説	追加	4. 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。	機微な個人情報についての条項を削除することによる留意点追加
9	第9条	解説	追加	5. 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た。即ち、情報主体の明確な同意がある場合、法令に特段の規定がある場合及び司法手続上必要不可欠である場合を除いて、次に掲げる種類の内容を含む個人情報について、これを収集し、利用し又は提供することを禁止していた。 (1) 人種及び民族 (2) 門地及び本籍地（所在都道府県に関する情報を除く） (3) 信教（宗教、思想及び信条）、政治的見解及び労働組合への加盟 (4) 保健医療及び性生活 個人情報保護法では、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。しかしながら、事業者として、個人の権利利益の一層の保護を図るとともに、顧客とのトラブル等を未然に防ぐといったリスクマネジメントの観点から、これら特定の機微な個人情報とされる情報の取得の際には、本人の同意を取り、必要かつ適正な安全管理措置を施し、さらには、第三者提供を行わないといった厳格な取扱いがなされることが望まれる。また、それら以外の個人情報についても、その個人情報の性格や取得の状況等により本人にとってセンシティブになると考えられる場合には、同様の措置を取るよう努めるべきである。	機微な個人情報についての条項を削除することによる留意点追加
10	第10条	解説4	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。	4. ウェブ画面上から個人情報の入力を求める時には、利用目的を明示するだけでなく、同意ボタンの設置など、消費者の同意を取得する措置を設けることで、消費者が利用目的を確認し、その取扱についての諾否を判断する機会を与え、一層の消費者の信頼を得られるものと考える。	消費者契約法・特商法について表記を削除

NO.	条	本文／解説	改定案<Ver.1.5>	Ver.2.0<α版>	理由
11	第11条	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。	1. 利用目的の変更については、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行われなければならず（第6条）、変更した場合は、変更後の利用目的を、本人へ通知、又は公表しなければならない。 2. インターネット等の情報ネットワーク上では、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、再度本人からの同意をもらうことが望ましい。 3. 再度本人より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。 4. 利用目的の変更について、「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」行う場合は、第7条の規定に基づき、あらかじめ本人の同意を得る必要がある。	解説主旨をわかりやすく整理し、並び替え、表現改善
12	第14条	本文・解説	（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。 ⑴　思想、信条及び宗教に関する事項 ⑵　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 ⑶　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 ⑷　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 ⑸　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） 以下略	削除、以下1条ずつ昇段	個人情報の種類について保護法の解釈に従う
13	第20条 → 第19条	本文	（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ければならない。	（サイバーモール運営者の対応） 第１９条　事業者は、サイバーモールを運営するに当り、本人から直接個人情報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。）において適正な取扱いが図られるような対策を講ずるよう努めることとする。	義務的表現及び内容の緩和

NO.	条	本文／解説	改定案<Ver.1.5>	Ver.2.0<α版>	理由
14	第20条 → 第19条	解説	(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ー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。 ① 提供し合う個人データの利用目的についての制限 ② 提供し合う個人データの項目 ③ 提供し合う個人データを利用する者の範囲 ④ 提供し合う個人データの再提供の有無又は再提供禁止 ⑤ 提供し合う個人データを利用できる期間 ⑥ 守秘義務 ⑦ 事故時の責任分担等 ⑧ 脱会後の措置等	(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等の個人情報の取扱いについて、一定の対策を施すよう努めることを奨励するものである。 2. 実際サイバーモール運営者はショップ等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。 したがって、万一、ショップ等から個人データが漏洩した場合、消費者に対する責任は、本来、ショップ等が負うこととなる。しかしながら、消費者からみると、そのショップ等の責任を追求するに留まらず、ショップ等が加入しているサイバーモール運営者に苦情が寄せられることも考えられる。 そうした事態が発生し、マスコミ報道等により社会的信頼を損なうこととなりうる点も考慮すると、ショップ等に対し、個人情報の取得や個人データの安全管理措置等について、責任の所在を明らかにする等の適切な対策を施すことが望ましい。 3. サイバーモール運営者がショップ等に対して、契約の中で、取得や安全管理についての必要かつ適切な措置を施すことを義務づけることにより、顧客の不安は解消され、いくらかのトラブルが回避でき、サイバーモール運営者自体のリスクも回避される。 4. また、消費者がサイバーモールを利用し、個人情報の入力をする際に、個人情報の取扱い上の責任がサイバーモール運営者とショップ等の間のいずれにあるかについて、ウェブ画面上に明示することが望まれる。	責任の明確化、消費者への明示が望ましい旨 共同利用を適用する表記を外す
15	第23条 → 第22条	本文	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。	2 事業者は、前項(3)に規定する項目のうち、④又は⑤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。	法律主旨を的確に表記
16	第23条 → 第22条	解説3	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。	3. 本条(3)では、具体的には、観光･旅行業等グループ企業で総合的なサービスを提供するために個人データの提供をし合うケースなどが想定される。	総合的なサービス提供である例示に変更
17	第27条 → 第26条	本文	第27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。	第27条 事業者は、開示、訂正等及び利用停止等（以下「開示等」という。）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。	語句定義追加

NO.	条	本文／解説	改定案<Ver.1.5>	Ver.2.0<α版>	理由
18	第32条 → 第31条	解説5	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、個人情報保護法第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。	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。また、<u>個人情報保護法が成立し、事業者として守るべき義務が生じたことに伴い、</u>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、個人情報保護法第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、あるいは改ざんのそし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。	保護法成立後の修正
19	第33条	解説1	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。	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<u>管理しておくことが重要である。</u>	具体的な対応等まだ十分に検討できていないので、文書管理、履歴管理の重要性を述べるに留める

＊その他、前文も更新

3.1.2　ECOM 個人情報保護ガイドライン Ver.2.0＜α版＞の公表

6月～8月にかけて4回開催したガイドラインＴＦ会議とアドバイザーである中央大学法学部堀部教授に入っていただいての検討会を経て、2003年9月1日に「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 Ver.2.0<α版>（ＥＣＯＭ個人情報保護ガイドライン Ver.2.0<α版>）」をECOMホームページ上に公開した。

3.1.3　政令・基本方針・主管官庁ガイドラインの反映

保護法に定められる政令は2003年12月10日に公布されたが、現段階（2004年2月）においては、それに続いて発令される基本方針は2004年3月以降、さらに、各主務官庁のガイドラインについては2004年4月以降となり、さらに各業界団体がガイドラインを策定するのはその後となる様相である。

当初、「ＥＣＯＭ個人情報保護ガイドライン Ver.2.0」の正式版については政令・基本方針の公布および主務官庁のガイドライン等が発表された後のタイミングで、それらを再度見直し、微修正をして公開する計画であったが、上記のようなスケジュールの状況では、電子商取引を行う企業が個人情報保護の体制整備をするに十分な時間が確保できないと判断し、政令の公布と国民生活審議会における基本方針策定の基本案等を考え合わせた上で、本年度末にての正式版としての公開に切り替えることとした。

3.1.4　ECOM 個人情報保護ガイドライン Ver.2.0 正式版

政令の第1～4条は個人情報保護法の第2条の定義に関して、政令第5条は保護法第24条の保有個人データに関する事項の公表等について、政令第6条は保護法第25条の開示に関して、政令第7条および第8条は保護法第29条の開示等の求めに応ずる手続きについて定められており、それぞれECOM個人情報保護ガイドライン Ver.2.0では、第3条、第23条、第24条、第28条が対象となる。政令にて定められる内容の中で明らかとなるところやガイドラインに影響するガイドラインの本文および解説について次ページの付表 3-2 にまとめた内容で修正を行った。ECOM個人情報保護ガイドライン Ver.2.0の正式版については、第6章（P159～P192）に掲載する。

付表3-2 ＥＣＯＭ個人情報保護ガイドラインＶer.2.0政令反映案 修正一覧表

NO.	政令	ECOMガイドライン				備考
		条	本文／解説	Ver.2.0<α版>	Ver.2.0政令反映版	
1	＜政令第1条＞法の対象となるマニュアル（手作業）処理情報の範囲 これに含まれる個人情報を一定の規則にしたがって整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するもの	第3 条	本文	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。 ・・・略・・・ ⑷ 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。	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。 ・・・略・・・ ⑷ 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一定の規則にしたがって整理することにより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情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。	
2		第3 条	解説3	3.「個人情報」に関する定義については基本的に個人情報保護法に準じることとした。個人情報保護法では「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。・・・	3.「個人情報」に関する定義については基本的に個人情報保護法に準じることとした。個人情報保護法では・・・略・・・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ている。（2）については、その後政令により、対象となるマニュアル（手作業）処理情報としては、これに含まれる個人情報を一定の規則にしたがって整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものと定められた。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がこれに相当すると考える。	
3		第3 条	解説5	5. 個人情報保護法では、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「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」に相当すると考える。	上記解説3.に内容を入れたので、削除。以下、昇段。	
4	＜政令第2条＞個人情報取扱事業者から除外される者 その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6月以内のいずれの日においても5千を超えない者 注：他人の作成したカーナビや電話帳を取得して、編集し、又は加工することなくその事業の用に供するときは、これを構成する個人情報によって識別される特定の個人の数はその数に算入しない。	第3 条	本文	（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。 ・・・略・・・ ⑻ 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。	変更せず	このガイドラインは、適用対象の事業者に対して法的な拘束性を持つものではないので、個人情報保護法における「個人情報取扱事業者」にてその取り扱う個人情報の量や利用方法により適用除外を規定しないため。 カーナビや電話帳についての考え方は、解説8.に追記。
5		第3 条	解説8	8. 電子商取引ではある程度の規模を持つ企業だけでなく、・・・略・・・個人情報保護法における「個人情報取扱事業者」にてその取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。	7. 電子商取引ではある程度の規模を持つ企業だけでなく、・・・略・・・個人情報保護法における「個人情報取扱事業者」にてその取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。 なお、政令では、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6月以内のいずれの日においても5千を超えない者は個人情報取扱事業者から除外されるとされている。さらに、他人の作成したカーナビや電話帳を取得して、編集し、又は加工することなくその事業の用に供するときは、これを構成する個人情報によって識別される特定の個人の数はその数に算入しないとされている。	

NO.	政令	ECOMガイドライン				備考
		条	本文／解説	Ver.2.0<α版>	Ver.2.0政令反映版	
6	＜政令第3条＞保有個人データから除外されるデータの範囲 ① 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 ・本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの ・違法又は不当な行為を助長し、又は誘発するおそれがあるもの ・国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの ・犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの ＜政令第4条＞保有個人データから除外されるものの消去までの期間 短期間（6月以内）に消去されるもの	第3 条	本文	（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。 ・・・略・・・ ⑹　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。	（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。 ・・・略・・・ ⑹　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。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以下のものに該当する場合及び6ヶ月以内に消去することとなるものは除く。 ①本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの ②違法又は不当な行為を助長し、又は誘発するおそれがあるもの ③国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの ④犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの	
7		第3 条	解説3	3.・・・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。	下記解説5.に内容を入れたので、削除。以下、昇段。	下項により説明カバー、および政令の公布により削除
8		第3 条	解説6.	6.「保有個人データ」から除外されるもののうち、個人情報保護法にある「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ことから、除外事項とはしないこととした。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とはしないこととした。	5. 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。なお、政令により、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ガイドライン第3条 ⑹ の①から④に示されるもの及び短期間（6ヶ月以内）に消去されるものは除外されることとなった。	
9	＜政令第5条＞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 ① 当該個人情報取扱事業者が行なう保有個人データの取扱いに関する苦情の申出先 ② 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先	第23条	本文	（保有個人データに関する事項の公表等） 第２３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。 ⑴　当該事業者の氏名又は名称 ⑵　すべての保有個人データの利用目的 ⑶　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 ⑷　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	（保有個人データに関する事項の公表等） 第２３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。 ⑴　当該事業者の氏名又は名称 ⑵　すべての保有個人データの利用目的 ⑶　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 ⑷　事業者が行なう保有個人データの取扱いに関する苦情の申出先および認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先	

NO.	政令	ECOMガイドライン				備考
		条	本文／解説	Ver.2.0<α版>	Ver.2.0政令反映版	
10	＜政令第6条＞個人情報取扱事業者が保有個人データを開示する方法 書面の交付による方法（開示の求めを行なった者が同意した方法があるときは、当該方法）	第24条	本文	（開示） 第２４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。 ⑴ 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 ⑵ 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 ⑶ 他の法令に違反することとなる場合	（開示） 第２４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。 ⑴ 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 ⑵ 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 ⑶ 他の法令に違反することとなる場合 ２　開示に当たっては書面により交付することとする。ただし、開示の求めを行なった者が同意した方法があるときは、当該方法で行うことができる。	
11		第24条	解説	追加	6. 政令により、開示の方法としては、原則、書面により交付することし、開示の求めを行った者が同意した方法があるときは当該方法で行うことができることとなった。したがって、Web画面上や電子メール等で開示をする際は、開示の求めを行った者に同意を得て行うよう留意しなければならない。	政令の遵守のため解説文追加
12	＜政令第7条＞開示等の求めを受け付ける方法として定めることができる事項 ① 開示等の求めの申し出先 ② 開示等の求めに際して提出すべき書面（電子的方式、時期的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式 ③ 開示の求めをする者が本人又は次条に規定する代理人であることの確認方法 ④ 手数料の徴収方法 ＜政令第8条＞開示等の求めをすることの代理人 ① 未成年者又は成年被後見人の法定代理人 ② 開示等の求めをすることにつき本人が委託した代理人	第28条	本文	（開示等の求めに応じる手続） 第２８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２３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。	（開示等の求めに応じる手続） 第２８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として以下について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。 ⑴ 開示等の求めの申し出先 ⑵ 開示等の求めに際して提出すべき書面（電子的方式、時期的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式 ⑶ 開示の求めをする者が本人又は本条第４項に規定する代理人であることの確認方法 ⑷ 手数料の徴収方法 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２３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。 ４　事業者は、次に掲げる代理人による開示の求めに応じなければならない。 ⑴ 未成年者又は成年被後見人の法定代理人 ⑵ 開示等の求めをすることにつき本人が委任した代理人	

4　具体的な場面における適切な企業としての対応検討

4.1　企業対応検討タスクフォース

電子商取引の場面における個人情報保護についての総論的な指針と位置付けられるECOM 個人情報保護ガイドライン Ver.2.0<α版>のなかで、より具体的にどのように対応すべきかについての検討を深堀する必要があると考え、2003 年度後半の活動として「企業対応検討タスクフォース」を設置し、討議および調査を実施した。

メンバーとしては、先のガイドラインタスクフォースに参加したメンバーに加え、本年度参加の SWG 委員・アドバイザー7 名が加わり、合計 21 名（P201、メンバー表参照）にて調査活動を実施した。

当初 2003 年 9 月～12 月の期間にて活動計画を立て、テーマ毎にチームを編成し、メンバー検討会、メーリングでの検討、有識者・関連企業団体等へのヒアリング等を行った。実際の活動期間は 2004 年 3 月まで延長され、結果的に 5 回のオフ会および延べ十数回におよぶチームごとのミーティングを実施した。今後の事業活動において、電子商取引およびインターネット上で個人情報を取り扱う場面で、具体的にどのように保護法を解釈し、どのように対処すべきかについてまとめたものとして、企業の判断の一助となるものになったのではなかろうか。

当初の具体的な検討テーマは図表 4-1 に示すとおりである。

図表 4-1 企業対応検討タスクフォース 検討テーマ

班	テーマ（チーム）	論点・課題
1	利用目的の特定と措置 （利用目的チーム）	・ 具体的にどのような内容で利用目的を通知・公表等行うべきか（アンケート・契約・会員登録といった場面を設定して検討）・・・サプライズアタックにならないことの検証/利用目的が明らかな場合とは？等 ・ インターネット上で顧客より情報入力を受ける時の適切な措置 ・ 消費者の不安・苦情の実態（スパムメール・DM 等） ・ 公表時と通知、明示の時の表現方法考証
2	クッキーの利用 （クッキーチーム）	・ クッキーの理解 ・ クッキー=意識しない間に直接書面等により取得されているケース ・ クッキーの個人情報としての利用とそうでない場合 ・ 法的な留意点と適切な対応方法の検討 ・ インターネット上での関連課題（アフェリエイト広告・P3P 等）

3	サイバーモール運営者の対応 （サイバーモールチーム）	・ 法的責任の見極め ・ 表示上の実態及び課題整理 ・ サーバーモール運営者とショップとの関係整理
4	第三者提供・共同利用等の考え方と対応策 （第三者提供チーム）	・「第三者提供」「共同利用」「委託」の妥当な法的解釈 ・「第三者提供」「共同利用」「委託」の定義検討（チャート作成）および具体的ケースを当てはめた措置検討
5	ホームページ上での個人情報保護に関する通知・公表等 （プライバシーポリシーチーム）	・ 国際動向・先進事例等の調査 ・ 最適なプライバシーポリシーの表し方（*Short Form Notice の検討） ・ 推奨プライバシーポリシーの雛型検討
6	保有個人データの開示から訂正・利用停止等の対応及び苦情処理対応 （透明性チーム）	・ 開示情報の範囲（履歴・評価情報の扱い） ・ 開示の求めの際の本人確認の方法 ・ どんな苦情があるか（漏洩・目的外利用<迷惑メール>等） ・ 標準的な苦情処理対応 ・ 開示～訂正・利用停止または事後処理へのプロセス・フロー（手順等） ・ 適切な緊急対応・事後対応の方法

4.2　利用目的の特定と措置

個人情報保護法では、「個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用目的をできる限り特定しなければならない」と定められており、以降の義務規定においてこのように特定された利用目的にに対して、取得や利用、変更等を行う場合に悉く適切な措置を施す必要がある。

4.2.1　個人情報保護法解説書籍における見解

個人情報取扱事業者の義務規定の冒頭の第15条に「利用目的の特定」が定められている。保護法成立の前後で同法の解釈や逐条解説等多数発刊されているが、それらの中で利用目的の特定について記述している部分を以下に抜粋する。

「その利用目的を・・・特定し」（第1項）

「利用目的」を「特定」するとは、個々の取扱プロセスごとにその目的を特定することを求める趣旨でなく、あくまで個人情報取扱事業者が一連の取扱いにより最終的に達成しようとする目的を特定することを求める趣旨である。したがって、利用目的は個人情報取扱事業者ごとに、また、一連の個人情報の取扱いごとに存在することになる。他の事業者から個人情報の処理の一部について作業の委託を受けて個人情報を取り扱う個人情報取扱事業者にあっては、委託された業務を遂行することが利用目的となる。なお、「利用目的」には個人情報を自らの事業のために利用する目的のほか、第三者に提供する事業のために利用する目的もあり得る。

「 できる限り特定」（第1項）

「できる限り特定」するとは、個人情報がどのような事業の用に供され、どのような目的で利用されるかが一般に認識可能なように、できるだけ明確にすることを求める趣旨である。したがって、「できる限り」とは、抽象的・一般的な形で特定することを必ずしも否定するものではないし、個別の具体的な利用目的をすべて網羅すべきとの趣旨ではない。個別の利用を類型化してまとめあげる等により、個々具体的な利用目的が当該利用目的の内か外かを判断できる程度の、可能か限り明確化することを求めるものである。・・・（中略）・・・なお、同種の事業者間でその具体性の程度が大きく異なることは適当でないことから、関係行政機関、事業者団体等が作成するガイドライン等を

通じて、どの程度具体的であるべきかの標準が示されていくことが望まれる。

利用目的が著しく具体性を欠く場合には本条の規定を遵守していないこととなり、第33条に規定する主務大臣による助言等を通じて、その是正が求められることもあり得る。

（以上、個人情報保護法・園部逸夫編）

ある飲食店が、来店した顧客に対し、店員の応対や、提供したメニューの味・価格についてアンケートを実施する場合、回答したアンケートを当該店舗のサービスやメニューの改善に役立てる目的であるときは、そうした内容を利用目的として特定すべきことになる。それに加え、アンケートに記載された氏名や住所を使用して当該顧客向けに販売促進用のダイレクトメールを送付する予定であれば、その点も利用目的となる。あまり厳格に利用目的を特定しすぎると、後日になって他の用途に利用できないことをおそれて、この利用目的を統合して「顧客サービスの向上」という幅広い利用目的を設定してしまうと、今度は第15条第1項の「できる限り特定しなければならない」という部分に反するおそれがある。

・・・中略・・・購入した商品のお届け先を販売店から聞かれて、買主（本人）が自己の住所・氏名を告げたところ、これによって知った住所等を利用して、当外販売店が当該買主に対し新製品の販売を目的としたダイレクトメールを送付するような行為は、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たものとして違反となる。

（以上、個人情報保護法入門・岡村久道）

法人の場合、定款の定めの具体的内容が 1 つの参考になるが（定款の目的のためと書くのは許されないだろう）、本人からみて、個人情報が利用された結果が合理的に想定できる程度に具体的であることが必要と思われる。例えば、何々業という業種を明示することで本人にとって利用の範囲がはっきりすれば（事業者と一般国民の間に共通の理解が成立していれば）よいが、そうでない場合には、「商品の発送、新製品情報のお知らせ、関連するアフターサービス」等の具体的利用の代表例をあげることで、利用の範囲を示すことが要求されることになろう。公表された利用目的が具体性を欠く場合には、主務大臣の助言もありうるだろう。いずれにせよ、特定の具体性のレベルについては、政府や事業者団体がガイドラインにより標準的モデルを示すことになろう。

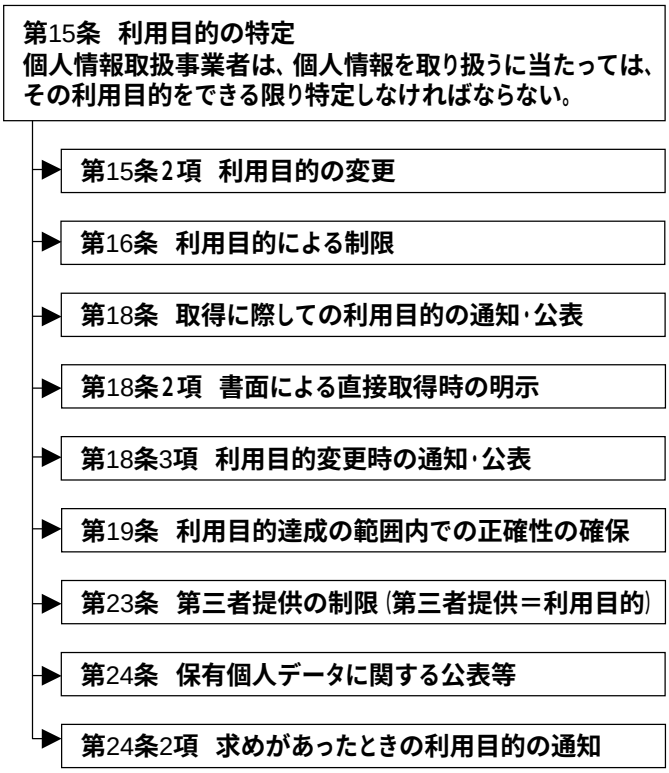
（以上、逐条個人情報保護法・藤原静雄）

4.2.2 ECOM 内での論点

ECOM 個人情報保護 SWG では、過去より、利用目的をどのように特定すればいいのかについてメンバー内で討議してきた。また以上の学識者の方々の見解等を参照し、以下のように整理した。

4.2.2.1 利用目的の特定は個人情報保護システムの大前提

図表 4-2 の様に「利用目的の特定」は個人情報保護法の義務規定において第 15 条 2 項より以降の数多の条文に影響を与えるものであり、まさに、「個人情報保護の適正な取扱いを確保するためのシステムの大前提（逐条個人情報保護法・藤原静雄）」であり、それゆえに、他の条項に見られるような例外的な義務免除がないのである。



図表 4-2 利用目的の特定①

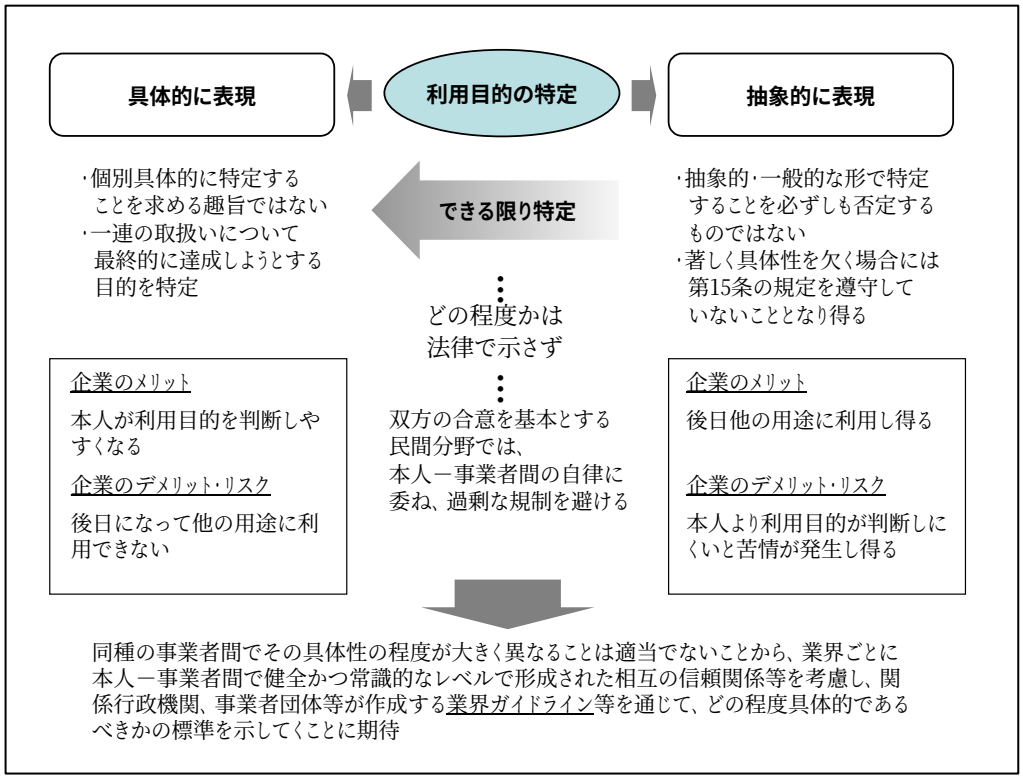
4.2.2.2 どの程度、どのように特定するか

一方で、民間においての義務規定であるゆえに、契約自由の原則に基づき取り扱われるべきとの観点より、過剰な規制とならないようにとの考えにより「できる限り」との表現が採用されており、どの程度できるかぎりかについては保護法では示されていない。

事業者の立場で言えば、具体的に表現すればするほど、「できる限り」特定したことに

なるものの、後で取得した個人情報を別の用途で使うとき、利用目的の変更や目的外利用の措置を取る手間が発生し、または、知らず知らずのうちに違反した取扱いをする可能性がありうる。他方で、抽象的に表現すれば、他の用途に利用し得る可能性は増すが、本人より利用目的がわかりにくいとの苦情が発生し、利用目的の特定自体の規定が守られていないケースが起こることも考えられる。（図表 4-3 参照）

ただし、同種の事業者間でその具体性の程度が大きく異なることは適当でないことから、業界ごとに本人－事業者間で健全かつ常識的なレベルで形成された相互の信頼関係を考慮し、関係行政機関、事業者団体等が作成する業界ガイドライン等を通じて、どの程度具体的であるべきかの標準を示していくことが望まれる（個人情報保護法・園部逸夫編）とされている。したがって、業界として確立している事業分野については、それぞれの主務官庁および業界団体により示される指針またはガイドラインに従うのが適切と考える。



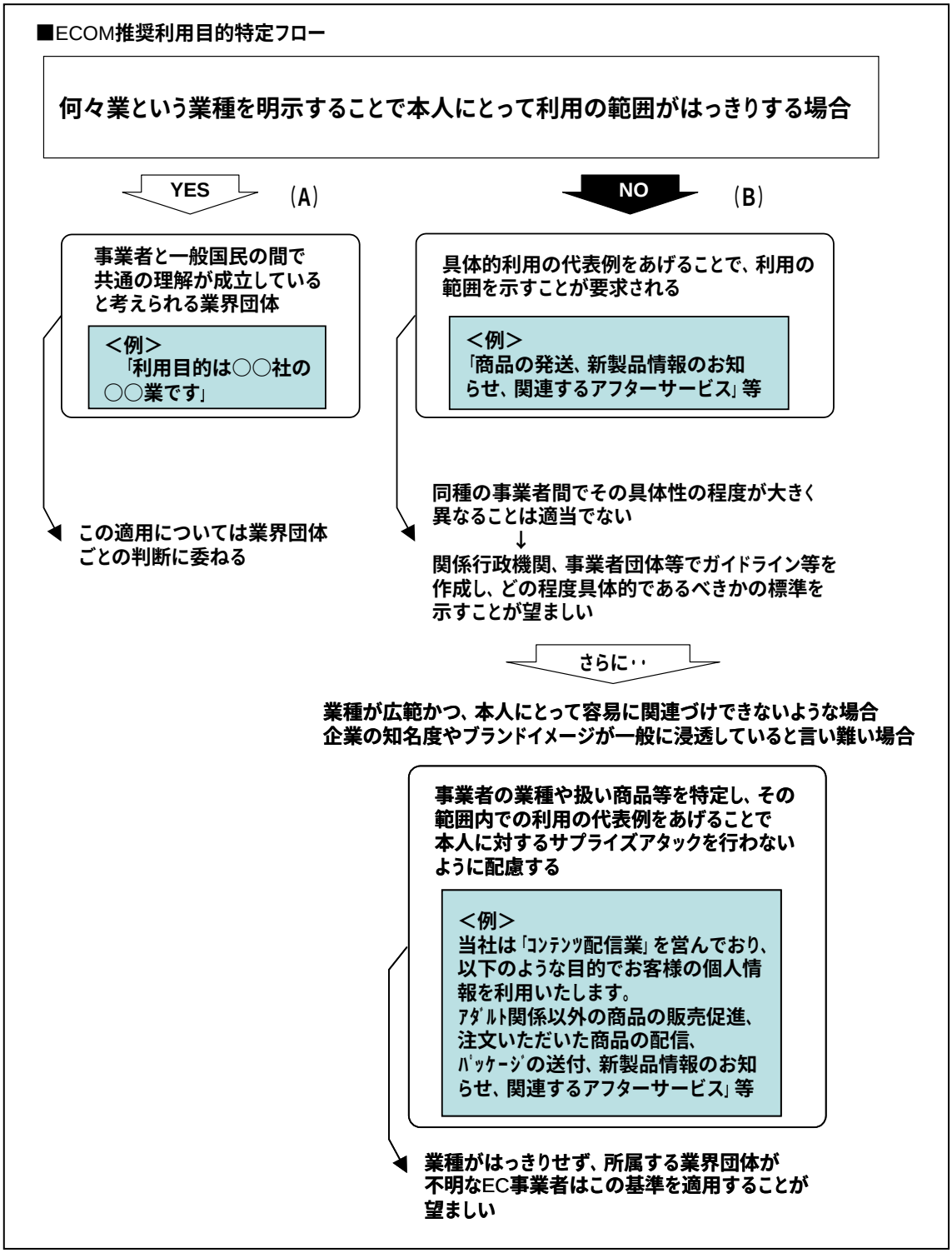
図表 4-3 利用目的の特定②

4.2.2.3 利用目的特定についての体系的整理

ECOM 個人情報保護 SWG 内では、電子商取引の場面において、いわゆるサプライズアタックとはどういうケースかという論点において、電気製品を購入した本人にその同一法

人が保険商品等を扱っている際、その DM や e メール等が送られることにより本人が不意に思うといった業種を超えて個人情報が取り扱われる場合と 4.2.1 の例（個人情報保護法入門・岡村久道）にあるような購入した商品のお届け先を告げたところ、これによって知った住所等を利用して、販売店が新製品の販売を目的とした DM を送付するような具体的利用の行為について本人が意識しなかった場合の二つが考えられるとの議論が続いた。

サプライズアタックを未然に防ぎ、さらに消費者との信頼関係を増すためには、営む事業分野が業界として確立し、その業界団体に所属してるか、その業界においてガイドラインが示されているとか、消費者との相互理解の関係ができる状況がある場合であれば、下図 4-4 の（A）のような対応をすればよいが、業種が広範であり消費者にとって容易に関連づけがたい場合や、事業者自体の知名度やブランド等が一般に浸透していない場合は、（B）に示すように、業種や扱い商品等を特定し、その範囲内での利用の代表例をあげるような配慮を施すことを奨励したい。



図表 4-4　ECOM 推奨利用目的特定フロー

4.3　本人の意思が介在しないで取得される個人情報

ECOM 個人情報保護ガイドライン Ver2.0<α版>では、その第 13 条に「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」として、利用者が、インターネットにおいて事業者の Web サイトに接続する際、本人の知らないうちに取得される情報についての措置を定めている。

クッキーについては、現在、広く活用されるようになり、特に顧客に対する One To One マーケティングやユーザー画面のカスタマイズ等、インターネットならではの機能、利点として有効に利用されている。

主には、利用者にとって、利便かつサービス性の高いものとして受け入れられるものと考えられるが、一部の利用者には、自らのプライバシーに抵触するものとして捉えられたり、誤解されたりする場合もある。

クッキーのような本人の意思が介在しないで取得される個人情報の取扱いについて、利用者にどのように対応すべきかについての指針を示すということが、ガイドラインに上記の第 13 条を設けた背景である。

4.3.1　クッキーの仕組み

クッキーは、Web ブラウザの状態遷移を Web サーバー側が自由に把握できるようにするために設計されたものである。HTTP では、HTML 文書の情報を転送するたびに接続が切れるので、Web サーバーが個々のブラウザを認識するのは困難であったが、クッキーの記録により識別が可能となる。

その手順としては、まず、Web サーバー側より、利用者のブラウザにクッキーを記録する命令がヘッダーに含まれて送信される。このヘッダーには、クッキーの有効期限、クッキーを返信すべきサーバーのドメイン名およびアクセスする際にそのクッキーに返すためのパス名が含まれている。

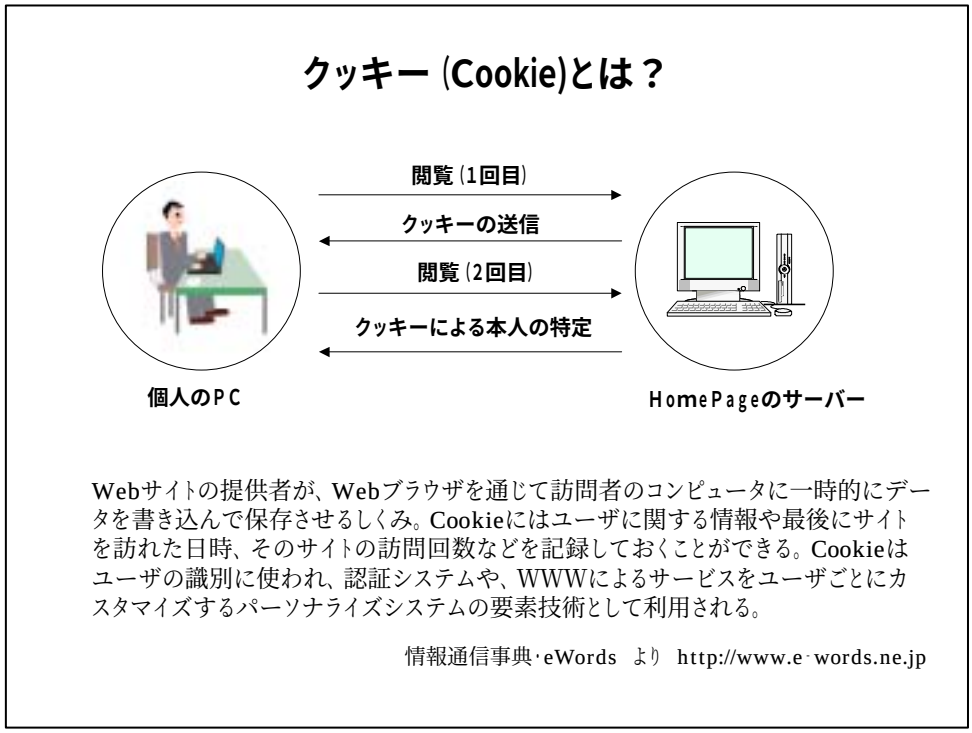
利用者のブラウザがクッキーを受信すると、その内容はファイルに記録される。

そして、再度、利用者が記録されたクッキーの示すパス名の範囲で同じ Web サーバーにアクセスすると、そのクッキーはヘッダーに含めて Web サーバーに送り返される。

このようにして、Web サーバーはアクセスしたブラウザを認識し、一連の処理を進めるのである。

サイバーモールなどでインターネットネットショッピングにて商品を購入し、個人情報

を入力した後、再度そのサイトに訪れた際、登録名での画面が現れてくるのは、この仕組みを利用したものであり、いまや電子商取引の場面では、顧客のカスタマイズされたサービスの提供のために幅広く活用されている。



図表 4-5 クッキーの仕組み

4.3.2 各社のクッキーについての表記例

ECOM 個人情報保護ガイドライン Ver2.0 の改定検討を始めた当初は、クッキーの利用が広まりつつあるときであり、その利用に対して、個人情報としての取得あるいはプライバシーに対する配慮の必要性の意識が希薄であったが、昨今の事業者の Web サイトのプライバシーポリシー等には、その利用について、詳しく説明する表記が増えている。

以下に、ECOM 会員企業のうち、そうした記載をしている企業の表記（2004 年 1 月現在のもの）を数例抜粋する。

●トヨタ自動車株式会社

弊社は、クッキーを利用して、より高度なサービスの実現を図る場合があります。

クッキーは、お客様が再び当ウェブサイトをご利用になる際に、当ウェブサイトのコンテンツをより便利に利用していただくためのものであり、お客様のプライバシーを侵害したり、お客様のコンピューターへ悪影響を及ぼすことはありません。インターネット閲覧ソフトの設定により、すべてのクッキーを受取拒否に設定することや、クッキーが送信される際にその旨表示するよう設定することができます。しかし、そうした設定により当ウェブサイトを快適に利用できない場合があります。

●日本アイ･ビー･エム株式会社

IBM は、当社のウェブ・サイトの訪問者から、お客様サービスを向上させるために、お客様を特定できない匿名の情報を収集することがあります。 たとえば、当社は、お客様がどのドメインからウェブ・サイトに訪れるかの履歴を記録し、また、IBM サイトでのお客様の行動を記録していますが、その場合、収集された情報の匿名性は保たれています。 これら情報は、「クリック･ストリーム･データ」としても知られている情報です。 IBM や、当社に代わって分析を行う会社は、「クリック・ストリーム・ データ」を、お客様の傾向や統計を分析し、よりよいお客様サービスを提供できるように役立てています。

また、お取引に関連してお客様から個人情報を収集する際、そのデータからその取引に関するいくつかの情報を匿名形式で抽出し、それを他の匿名情報（「クリック・ストリーム・データ」など）と結びつけることがあります。 この情報は、全体傾向やパターンを把握するために、集団レベルで使用され、分析されます。 個人のレベルで使用されることは決してありません。 お客様がご自身の取引詳細をこのような方法で使用されることを希望しない場合は、クッキーを作用しないようにすることができます。

IBM は、前述のように、種々のテクノロジーを使用して匿名情報を収集しますが、そのテクノロジーの 1 つに Cookies（クッキー）があります。クッキーは、ウェブ・サイトからお客様のプラウザーに送信できるあるデータであり、ご使用中のコンピューターに、お客様自身ではなく、お客様のコンピューターを識別する匿名タグとして貯えられることもあります。IBM ウェブ・ページの中には、あなたが IBM サイトを再度訪問するときに一層便利にご利用いただけるよう、IBM または IBM のお取引先によって送信されるクッキー、またはその他のテクノロジーを利用しているページがあります。 ご自身のプラウザーを、クッキーが送られてきた時に通知するように設定し、クッキーを受け取るかどうか選択することができます。また、ご自身のプラウザーのクッキー機能をオフに設定することも可

能です。 ただし、この場合、一部のウェブ・サイトの機能が損なわれる場合があります。

IBM ウェブ・サイトの中には、一層便利に利用していただくために、IBM ウェブ・サイトをより良いものに調整するウェブ・ビーコンあるいはその他のテクノロジーを使用しているサイトがあります。これらのテクノロジーは IBM ウェブ・サイトの多くのページで使用されています。 訪問者がそのようなページにアクセスすると匿名通知が生成され、それは IBM または IBM お取引先により処理されます。ウェブ・ビーコンは、通常、クッキーと一緒に機能します。 ご自身のクッキー情報を、こうしたページへの訪問と関連付けたくない場合は、プラウザーのクッキー機能をオフに設定してください。

クッキー機能をオフに設定した場合でも、ウェブ・ビーコンその他のテクノロジーは、クッキーやウェブ・ビーコンが設定されたページへの訪問を検出します。しかし、生成される通知は他の匿名クッキー情報と関連付けられなくなり、この通知は無視されます。 詳細については、「クッキーの取り扱い方」をご覧ください。

●マイクロソフト株式会社

サイトにアクセスすると、Cookie がお客様のコンピュータに送信されます (受け入れた場合のみ)。サイトにアクセスしたことがある場合は、Cookie が読み込まれます。Cookie を使用する目的の 1 つは、上記したようにサイトへのアクセス情報を統計として集めることにあります。

また、Cookie を使用してお客様がクリックしたニュースレターのリンクに関する情報も収集します。この情報は、マイクロソフトがお客様の求める情報を提供するために利用されます。情報は統計として収集され、個人情報と関連付けられることはありません。

Web ビーコン (クリア GIF またはアクション タグと呼ばれることもあります) が、Cookie の送信をサポートします。この技術により、Microsoft.com Japan Web サイト上の主な項目 (リンクや画像) をクリックしたユーザーの数を把握することができます。この技術は、お客様を特定できる情報にアクセスするためのものではなく、Microsoft.com Japan Web サイトの利用状況について統計をとるためのものです。サイトに関する統計をマイクロソフトの提携会社と共有することはありますが、他社が当サイトにクリア GIF を送信することを許可することはありません。

また、.NET Passport プライバシーに関する声明で説明されているように、マイクロソフトは Microsoft.com Japan Web サイト上で使用されるお客様の .NET Passport アカ

ウントに関して Cookie を利用することがあります。

お客様が Microsoft.com Japan Web サイトからの Cookie を拒否するようにブラウザを設定した場合は、画面を閲覧することはできますが、サイトをカスタマイズしたり、サイトで提供されるサービスの特典を利用することはできなくなります。

Cookie については、こちらを参照してください。

●マスターカード・インタナショナル・ジャパン・インク

種々の技術が、非個人情報収集のために利用されます。これにはクッキー機能も含まれます。クッキー機能は、利用者のブラウザを通じて、ウェブサーバーにより利用者のコンピュータ上に蓄積される小型ファイルです。クッキー情報の実際のコンテンツは、サイト訪問者のコンピュータを識別するために、同一のウェブサーバーにより収納保管されます。お客様が他のウェブサイトから当ウェブサイトを訪れる場合、そのウェブサイトにおいて、お客様の当ウェブサイト訪問が、クッキー機能を通じて知られてしまう可能性があることにご注意ください。当社は、他のサイトにより使用されているクッキー機能を規制することはできません。

●松下電器産業株式会社

1. クッキーとは、ウェブサイトを訪問したときに、そのウェブサイトがユーザのハードディスクに書き込む小さなデータファイルで、ユーザの訪問したページを認識するためなどに使われます。クッキーの情報は、ウェブサイトとユーザのインターネット閲覧ソフト（ブラウザ）との間でやりとりされますが、ウェブサイト側では、他のウェブサイトが書き込んだクッキーやハードディスクの他のデータを読むことはできません。
2. クッキーは多くのウェブサイトで使用されていますが、ユーザがブラウザを設定することにより、クッキーを使用しているウェブサイトを訪問しようとしているときに事前にその旨を表示したり、クッキーの受け取りを拒否することができます。
3. 当社ウェブサイトでは、提供する情報やサービスを充実させたり、当社ウェブサイトをより便利に利用していただくなどのために、クッキーを使用する場合があります。当社ウェブサイトは、予めお客様の承諾を得た場合を除き、クッキーによって個人を特定できるような情報を得ることはありません。

●三菱電機株式会社

当社は、前記の利用目的のために、クッキー（Cookie）を利用して情報を収集させていただくことがあります。

クッキー（Cookie）とは、ウェブ・サーバから送信されてコンピュータのハードディスクドライブにインターネットブラウザにより保存される少量のデータです。

クッキー（Cookie）自体には、お客様ご自身や E メールアドレスに関する情報は含まれませんが、お客様が個人情報等を当社に提供されると、お客様が当社のウェブサイトにアクセスされる際にお客様が使用されるパソコン等の通信端末が特定されます。　ただし、クッキー（Cookie）を利用して、お客様のハードディスクドライブのデータや、E メールアドレス、利用者個人の識別情報を入手することは出来ません。

お客様はクッキー（Cookie）を受け取ったときに通知されるように、またクッキー（Cookie）が送信されないようにブラウザを設定することができます。

4.3.3　クッキーを利用する際の措置

クッキーをはじめとするインターネット技術上のシステムツールの使用に関しては、その利用について告知するとともに、それが個人情報として取り扱われる場合には、保護法に従った対応が適切と考えられる。では、その個人情報としてのクッキーについてはどのような措置が必要なのだろうか。

個人情報の取得とその措置について、本人との契約および本人救済の観点より、表 1 のように整理される。

同表において、クッキーのような情報技術を利用して取得する情報が、個人識別可能な情報であれば、「直接書面以外で取得される個人情報」に分類される。

保護法ではその第 18 条 2 項にて直接書面（「電子的方式、磁気的方式その他人の知覚によって認識することができない方式で作られる記録を含む」ことより、インターネット上の入力画面に記入することなどはこれに含まれる）に記載された個人情報について利用目的の明示が求められている。

しかしながら、インターネット上より取得されるものの、本人が直接記入する等の行為がないままに、意思が介在せず取得されるものであることから、書面等より本人の意思により記載されるものではないので、上記の第 18 条 2 項の要件が求められるものでなく、クッキーにより個人情報としてデータを取得することについては同条 1 項の「通知または公

表」の措置が適用されると考えられる。

図表 4-6　取得の態様と本人救済等

1 本人から直接取得	書面	(1)直接契約書により取得する場合 [「本人との間で契約を締結することに伴って契約書その他の書面･･･に記載された当該本人の個人情報を取得する場合」（18 条 2 項）]	①本人からの承諾とともに取得する場合(承諾型) ・「契約書」に明示(契約責任追及可) ・事実行為により明示 契約構成可能(契約責任追及可) 契約構成困難(契約責任追及不可) ②本人からの申込とともに取得する場合(申込型) ・事実行為により明示 契約構成可能(契約責任追及可) 契約構成困難(契約責任追及不可) ・申込の誘因により明示(契約責任追及可)
		(2)契約によらず直接書面により取得する場合 [その他、契約を伴わずに「本人から直接書面に記載された当該本人の個人情報を取得する場合」(18 条 2 項)]	契約はないが、少なくとも本人の意志が介在していることを推認できる類型である。 ①(司法救済的観点から)契約構成が可能 約束がどの程度のものになったときに契約として法的保護に値するようになるかという問題がある。 ②(司法救済的観点からも)契約構成が困難 不法行為責任が問題となる。
	書面以外	(3)直接書面以外で取得 －本人の意思が介在している場合(18 条 1 項)	①(司法救済的観点から)契約構成が可能 ②(司法救済的観点からも)契約構成が困難
		(4) 直接書面以外で取得 －本人の意思が介在しない場合(18 条 1 項)	本人の知らないところで IC タグやクッキー等情報技術を利用して取得する場合等が典型。 一般に契約構成が困難である。
2 本人以外からの間接取得		(1)受託による取得 (23 条 4 項 1 号)	①適法な取得 ②違法な取得
		(2)合併、分社、事業継承による取得(23 条 4 項 2 号)	①適法な取得 ②違法な取得
		(3)本人以外から提供された個人情報を取得する場合(受託による取得及び合併等による取得を除く。) (18 条 1 項)	①第三者提供の禁止に違反しない状態での取得 ②第三者提供の禁止に違反した状態での取得 ・適法な取得(善意無過失が要件か？) ・違法な取得(故意過失が要件か？)
		(4)公開情報から取得する場合(拾得する場合を含む。) (18 条 1 項)	①適法な取得 ②違法な取得

（出典：法律のひろば平成 15 年 9 月号「個人情報保護のための企業法務（鈴木正朝）」より）

その考えに従い、ECOM 個人情報保護ガイドライン Ver2.0」の第 13 条「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」では、クッキーの

利用について、「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の通知または公表」を規定し、さらにその解説で個人情報として利用しないケースでも「その利用についてわかりやすく示す」ことを奨励することとした。これは、そうした仕組みについて詳しくない利用者が不信感を持たないようにするためであり、現在では、すでに各社のプライバシーポリシーにも多くそのような表現がなされている。

4.3.4 IC タグに関する課題についての取り組み

上記の表にまとめられているように、本人の意思が介在しない個人情報として取得されるものとしては、その導入が検討される IC タグに関連する問題も近年注目を集めている。

IC タグは SCM やトレーサビリティの分野での実用化が期待されているが、消費者が所持する物品に IC タグが貼付されることによる個人のプライバシー侵害の懸念もあり、海外では、これを問題視する消費者団体の申し入れによりベネトンやうウォルマートなど IC タグの導入を断念する企業も現れている。

本年度、ECOM では、こうした消費者の IC タグに関する不安や懸念の払拭およびその高普及び高活用を目指し、本年度より発足したトレーサビリティ WG と個人情報保護 SWG のメンバーのジョイントにて、2003 年 11 月より IC タグ・プライバシータスクフォースを立ち上げ、検討を重ねた。

その成果として、「商品 IC タグに係る消費者の個人情報及びプライバシーの保護に関するガイドライン」の原案を 0.1 版としてまとめた。（掲載は参考資料②）

4.3.5 まとめ

ＩＴ技術の進歩に伴い、インターネット上やリアルの空間において、事業者間の取引や運搬といった業務や経営の効率化が図られるとともに、事業者から消費者に提供されるサービスの品質や利便性も向上する。

顧客のニーズの多様化、カスタマイズ化に対応する機能を利用する新たな技術は、事業者や開発者の立場では、メリットとなる面が重視され、実用化、さらには普及へと流れが急速に進むが、反面、既存の社会秩序や法制との間で矛盾した状況を生み出すことがある。加えて、新たな価値観が利用者や消費者に芽生えつつあることを忘れてはいけない。

その結果として、既存法制の見直しや新たなルールづくりが必要になってくるが、高活用による利便性の向上と個人の権利利益のバランスを考えた場合、ひとつの好ましい社会

ルールのあり方としては、事業者が自主的・自発的に顧客に対して配慮する姿勢で臨むことではないだろうか。そのことにより、利便性を追求する企業の意欲が維持できる。

日本における個人情報保護やプライバシーへの関心は、法制化がなり、グローバリゼーションが進む中で、消費者や利用者の意識が高まっていくことを認識し、新たなＩＴ技術を実用化する際、そうした問題との関わりを導入の当初より課題掌握・摘出し、顧客に不安を生じさせない自主的な運用ルールを考案していくことが求められる。

4.4　利用者に対するサイバーモール運営者とショップとの対応

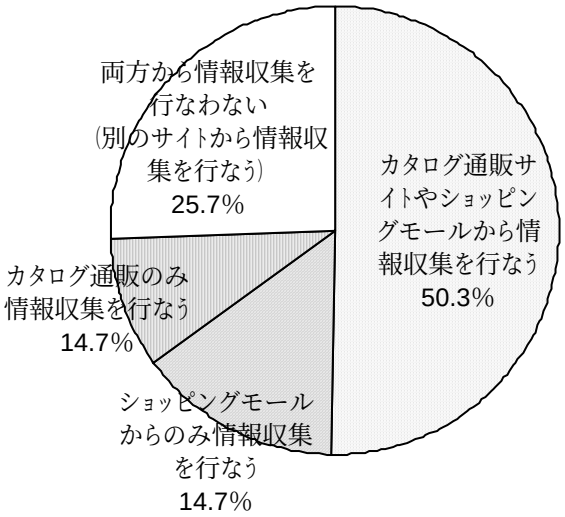
ECOM 個人情報保護ガイドライン Ver2.0<α版>では、その第 19 条「サイバーモール運営者の対応」に、電子商取引の場面で起こりうる課題としてインターネットショッピングモールでのサイバーモール運営者とそれに参加するショップ間で取り扱われる個人情報についてのガイドを示している。

4.4.1　具体的なサイバーモール運営者とショップとの現状

インターネット白書 2003（財団法人インターネット協会監修）によると、カタログ通販サイトやショッピングモールでの情報収集に関して「カタログ通販サイトやショッピングモールから情報収集を行う」と「ショッピングモールからのみ情報収集を行う」を合わせ、65%の利用者がショッピングモールから情報収集を行っている。さらにはそのようにして情報収集をした後に、オンライン･オフライン合わせて 50%以上が購入に動いている。

ひとつのポータルサイトより、数多の商品や希少なアイテム、産地直送等の品物が検索でき、安価かつ様々なサービスを享受できるショッピングモールは、今後も利用が増大するものと考えられる。

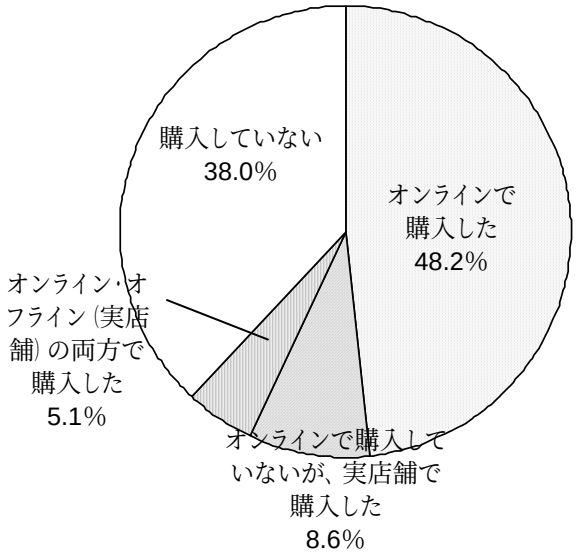
図表 4-7　カタログ通販サイトやショッピングモールでの情報収集の有無（N＝2,513）



「ショッピングモールのみ」は 14.7%、「カタログ通販サイトのみ」は 9.4%で、このどちらかからも情報を収集している人が 50.3%と最も多い。両者どちらかからも情報収集はしていないという人は 25.7%である。

出典：インターネット白書 2003（財団法人インターネット協会監修）

図表 4-8 情報収集後、ショッピングモールやカタログ通販サイトからのオンライン購入経験（N＝1,868）

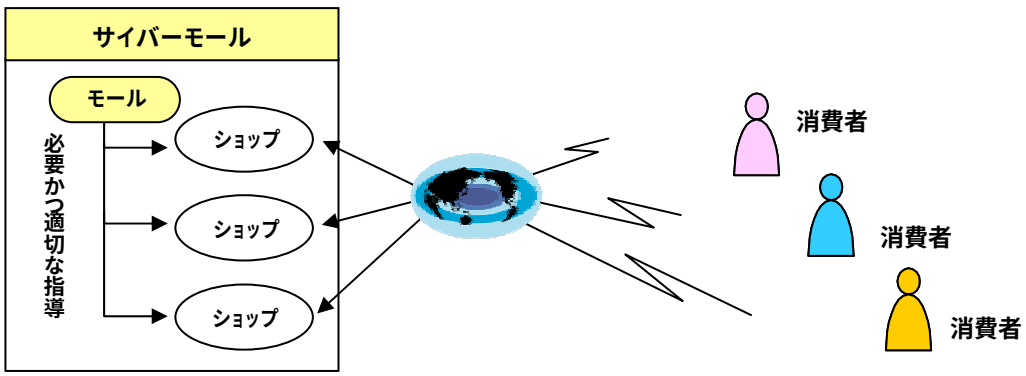


インターネットで情報収集後、「オンラインで購入した」人は 48.2%と半数を占める。「店舗で購入」は 8.6%と少ない。「両方で購入」は 5.1%とさらに少ない。情報収集はしたが「購入していない」は 38.0%である。

出典：インターネット白書 2003（財団法人インターネット協会監修）

4.4.2 サイバーモールの定義

ECOM 個人情報保護ガイドライン 2.0 におけるサイバーモール事業者とは、「インターネット上に自社以外の複数の電子商取引を行うオンラインショッピング事業者、情報提供サービス業者等が参加するモールを開設する事業者」と定義する。



図表 4-9　サイバーモールの概念図

一口にサイバーモールといってもその形態や経営母体はさまざまである。ポータルサイトとしての機能から拡大してショッピングモールをアイテムとして持つ大規模なものもあれば、地域における商店街の活性化を旨に販売促進策としてサイトを立ち上げたものなど規模や運営について幾多ものバリエーションが見られる。

電子商取引という観点よりインターネット上で購買に至る Web ページの展開上からは、大きく二つのパターンが考えられる。

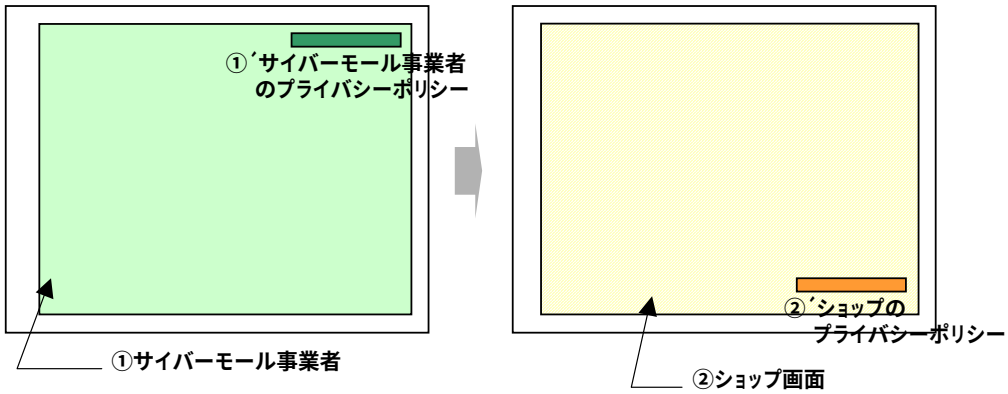
ひとつは、ポータルとしての機能が主であり、利用者がショップのバナーやリンクボタンをクリックすることによりそのショップの画面に移ったとき、画面上もドメイン上もそのショップのサイトに移ってしまうものである。（図表 4-10　パターン１のケース）

また、もう一方は、まさにショッピングモールとしての特有の機能として、サービス性の高い情報提供と販売促進策が展開され、共通の受注画面などを持ち、Web ページ上でショップにリンクした後もサイバーモールのロゴやフレームを残すタイプである。（図表 4-10　パターン２のケース）

パターン 1 の場合は、画面が完全にショップの画面に変わり、利用者としてもショップに画面が移ってしまっていることで、消費者において、個人情報取扱い上の誤解が生ずるケースはそれほど無いと思われる。このケースはサイバーモールというだけでなく、バナー広告やリンクボタンを多く掲載し、クリックすることによりアドレスも移ってしまうような Web ページと画面上の表示や展開の上で差異がないと考えられる。

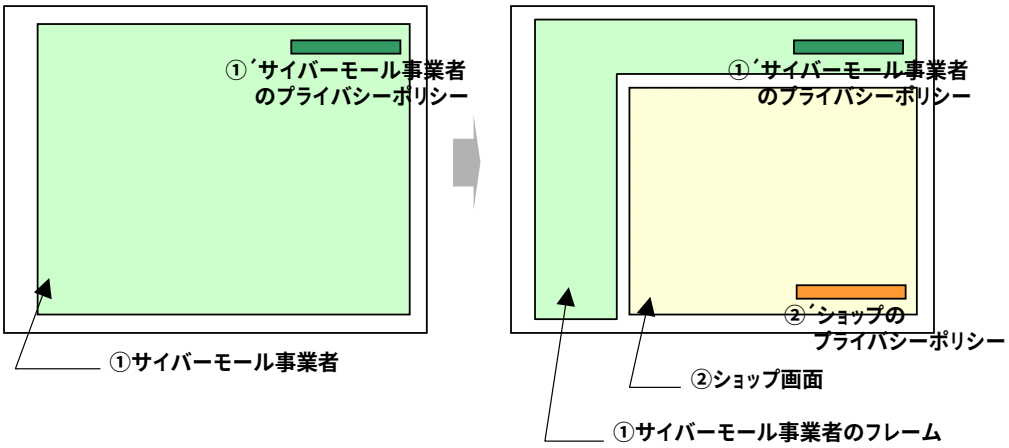
ここでは、個人情報の取扱いにおいて利用者が錯誤を起こしうるケースとして、パターン 2 の場合について、どのような課題があり、また、いかに対応すべきかについて考察する。

（パターン１）ショップ選択後、ショップ画面に完全に移行



バナーよりにリンク後は、ショップ画面に変わる。
→個人情報の取扱いについてショップに責任があることが解る。ただし、サイバーモールとしてのサービス性やサイトのファッション性などアピールが低いものとなる。

（パターン２）ショップ選択後、サイバーモールのフレームが残るケース



バナーよりにリンク後は、サイバーモール運営者のフレームを残しながら、ショップ画面に変わる。サイバーモール運営者とショップ双方のプライバシーポリシーが混在するおそれあり。
→サイバーモールのトータルイメージが保たれ、個性的でファッション性のある画面や独自のシステムサービス等提供できる反面、個人情報の取扱いについてサイバーモール運営者とショップのいずれに責任があるか利用者にわかりにくくなるケースもあり得る。

図 4-10　サイバーモールにおけるショップ画面の表示パターン

4.4.3　サーバーモールにおける個人情報保護に関する表示上の課題

一般に図 1-1 におけるパターン２のケースは規模の大きな商用ショッピングモールにお

いて見受けられるパターンである。即ち、インターネットの普及に伴う新たなビジネスモデルとして、バーチャルな空間を活用してネット上での購買需要を喚起し、事業化を図るものであり、その運用にあたっては、参加するショップに対して、加入規約を提示し、契約を結んで、厳正なルールのもとで電子商取引を行うものである。

しかしながら、消費者との売買取引に関しては、ほとんどの場合、ショップと消費者間で行われるものとして扱われており、サイバーモール運営者は、いわば「場の提供」のスタンスを取るところが多い。

ともあれ、サイバーモールとしてのイメージの高揚やブランド力による購買意欲の喚起および信頼性向上を図る意味で Web 画面上の表示において図 1-2 の（パターン 2）のような形態をとるサイバーショッピングモールが興隆し、電子商取引のひとつの大きなカテゴリーを形成している。

さて、前述のとおり、売買における個々の取引や契約においては、大方、消費者とショップという当事者間の責任に委ねることとなるが、個人時情報の取扱いについては、消費者あるいは利用者に対してどのように対処すべきか。

サイバーモールを利用する消費者が個人情報を入力する場合、或いは会員として加入したサイバーモール上で商品を購入する場合の購買履歴等が、サイバーモール運営者とショップ間においてどのように取り扱われ、保存され、利用されるのかといったことについて、実態をベースに適切な対応を講ずることが求められる。

端的な課題としては上記のようなサイバーモール運営者のフレームを残しながら、ショップ画面が表示される場合、サイバーモール運営者とショップの双方のプライバシーポリシーが表れることもあり、その取扱いに関して矛盾がないか、消費者を混乱させないかといった配慮も必要となってくるだろう。

4.4.4　サイバーモール運営者の運用実態

上記のような課題に対して、サイバーモール事業者は現状どのように運営し、また今後どのように対応しようとしているのか。インターネットショッピングモールを運営する企業数社にヒアリング等を行い、また、Web サイト上のショップ等との規約等を確認しながら、現在の実態を探ってみた。

概ね大手のサイバーモールを運営する会社では、参加するショップに対して綿密な規約を準備し、審査を行い、契約を結んだ上で、開設に至るといったプロセスになっている。

また、ショップに対しては、その月商規模や契約金額に応じてインセンティブが用意されており、そうしたオプションのひとつに、会員顧客に対する商用メールの送付などを準備しているところも多い。

（個人情報の取扱いについての基本スタンス）

- OECD 原則や個人情報保護に関する法規に準拠し、対応。個人情報の取得、利用、保有等に関して利用者の了解（選択）を得て、取り扱う。
- 個人情報を保有することはそれ自体がリスクを招くこととともなるので、不要な個人情報は取得しないというスタンスのモールもある。

（モールとショップの関係）

- いくつかのサイバーモールでは、ショップに対し、Web ページ作成ツールを提供し、ショップはそのテンプレートを使ってコンテンツやデータを作成し、サイバーモール所有のサーバーに格納することにより、サイバーモール統一のデザインやプログラムを利用者に提供している。
- 基本的には、利用者とショップの取引についてはショップと利用者間にて行うこととしているが、サイバーモールが取引上の苦情について対応しているところもある。
- 多くのサイバーモール運営者は、ショップにおけるユーザー対応状況をも管理・掌握しており、上記のように利用者からの問合せや苦情を受け付けることもあるので、ショップに対して強い指導的立場をとっていることが多い。

（個人情報の取扱いに関する表示・プライバシーポリシー等）

- 現時点では、サイバーモールとショップのプライバシーポリシーが混在するケースや保護法施行全であることも含め、プライバシーポリシーをトップページよりリンクできるようなポータルのデザインになっていない状況だが、前者の場合には、原則として、サイバーモールとショップとも個人情報の取扱に関する実態に応じた表記がなされており、また、後者の場合にもショップ向及び利用者向の注意事項として表紙され、読まれるような仕組みを構築している。

（取り扱う個人情報の考え方）

- サイバーモールが提供する仕様に従って作成されるショップの Web 画面は、サイバーモールのサーバー内に格納される。したがって、取得される利用者の個人情報はサイバーモールのサーバー内に保存されることとなる。その個人情報の考え方に

ついては、利用者とショップ間の取引により取得された個人情報であるので、ショップの持ち物であり、サイバーモールはショップから個人情報の保管を委託されているといった考え方と、基本的にはサイバーモールとショップ間で共有するが、あくまで、サイバーモールが統括して管理し、ショップには必要最小限のデータのみを供給するといった考え方の二つがある。

（利用者への対応、情報発信や問合せ等について）

- ショップの販促情報やメルマガ等の配信については、サイバーモールが所有するリストに基づき、登録時に配信の承諾のあった利用者に対して、モールのオペレーションによって行われ、ショップ側では直接取引のあった利用者の個人情報以外は抽出できない仕組みにしているモールもある。また、規約上でそのように規定している。
- ユーザーからのクレーム等を考慮し、ショップとの契約において、モール脱会後、モール参加時に取得した個人情報の利用を制限しようと考えているところもある。
- 個人情報の問合せに関しては、登録されたメールアドレス宛に返信するケースが多いが、一部には郵送するところもあった。

4.4.5 ガイドラインにおける措置の考え方

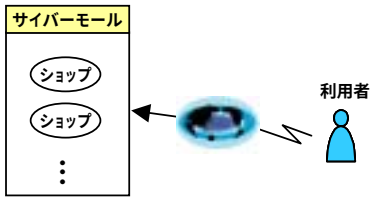
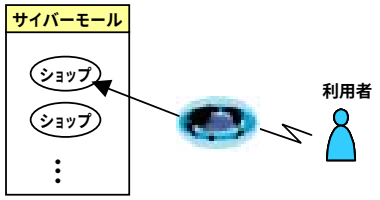
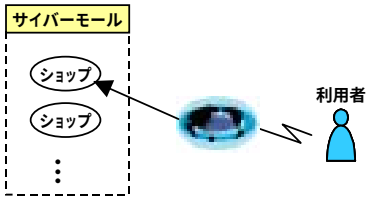
以下に、サイバーモールとショップにおける個人情報の取扱いについて整理する。

まず、サイバーモールとショップとの関係において、利用者の個人情報がどのような状況のもとで取り扱われ、どちらにどのような形で保有されるかを整理した上で、その実態に応じて、両者間で利用者の個人情報の取扱い上の責任の所在等についてきちんとした取り決めがなされる必要がある。

概ね大手のサイバーモール運営者においてはショップを募集し、加入受付する過程において、規約に基づき審査し、契約を交わして出店に及ぶ。ヒアリングを実施したサイバーモールを運営する数社においても、すでに個人情報の取扱いについてショップとの間で厳密な契約が結ばれ、その中で細部にわたる取り決めがなされているが、中小規模のサイバーモール運営者においても、個人情報の取扱いについて明文化された規定に基づく契約を結ぶことにより、ショップとの間での利用者の個人情報の取扱いに関する責任を明らかにしておくことが大切である。

図表 4-11 は、サイバーモールおよびショップそれぞれがどのような個人情報を保有するのか、またどのようにその個人情報を取扱うのかなどについて、一例を示すものである。

図表 4-11　サイバーモールとショップの個人情報取扱上の責任の切り分け例

利用者とモール・ショップのアクセス状況	個人情報取扱上の責任の切り分け（例）	
A.**利用者がモールにアクセス**  ●利用者がモールにアクセスした際のアクセス履歴 ●利用者がモールに問合せたモール全体についての質問 ●利用者がモール会員として登録した個人情報 ●利用者がモールに問合せた個別のショップに関する質問等（モールが回答し得る場合）	●サイバーモールが統括管理 ●メルマガや販促情報配信の了解を得ている場合、ショップよりの直接配信は原則避ける	サイバーモールが統括管理、またはショップに指導
B.**利用者がモール内ショップにアクセス**  ●利用者がモール内のショップ画面にアクセスした履歴 ●利用者がモールに問合せた個別のショップに関する質問等（個別のショップ出ないと回答できない場合） ●利用者がショップにモールにて発注した場合の情報	●原則、サイバーモールが総括管理、ただし、個人情報の取扱いに関してショップと責任を明らかにする必要あり ●メルマガや販促情報配信の了解を得ている場合でも、ショップよりの直接配信は原則避ける	ショップに対し利用制限
	●サイバーモールショップのいずれが、どういった個人情報に関して責任を持つか明らかにする必要あり ●取引上で知りえた個人情報の取り扱いやとメルマガや販促情報配信についての利用者との合意内容等規定し、厳格に運用する	ショップと共有
C.**利用者がモールの外からショップにアクセス**  ●利用者が直接ショップに問合せた質問等 ●利用者が直接ショップに発注した場合の情報	●ショップが個人情報に関して管理責任を持つ ●メルマガや販促情報配信についてもショップが責任を持つが、モール加入時点で、例えば脱会後の個人情報の取扱いについて取り決めておくべき	ショップが責任を持つ

ショップが独自に収集する個人情報やサーバーモールがショップにおいて必要となるため提供した個人情報については、サイバーモールがこれらショップの扱う個人情報の管理に関して全面的に責任を負うことには限界ある。そうした場合が生じるときには、その個人情報がそれぞれにどのような利用目的に使われるかについて消費者に対して明確に説明されるような配慮が必要である。

また、販売促進のためのメール配信をサイバーモール運営者の統制のもとで行う時には、事前の了解を取得した上で、ショップが利用者のメールアドレスを自由に閲覧できないように制御することなどは、システム運用上有効であろう。

さらには、個人情報の収集にあたっては、必要でない情報を取得・保管しないようにす

るというスタンスも、重要なポイントである。

サイバーショッピングモールの利用に際しては、消費者にとっては電子商取引を行う過程において、サイバーモール運営者とショップという複数の事業者が介在する点で、実態として個人情報がどのように取得され、取り扱われるかについて、わかりやすく説明されることが望まれる。その際、サイバーモール運営者は、ショップに対して、個人情報の取扱いに関する安全管理措置等を含めた適切な指導を行うことで、安全と信頼のショッピングサイトとしての価値高揚が図れるのではないだろうか。

4.5　第三者提供・委託・共同利用の考え方

4.5.1　個人情報保護法における第三者提供の考え方

第三者への個人情報の提供については、提供されてしまった後に取得した事業者が本人の了解した範囲で取り扱うかどうか、あるいは、本人関与が容易にできるかどうかといった不安があるので、個人情報保護法においては、以下の場合を除いて、あらかじめの本人の同意を得ないで行ってはいけないとされている。（保護法第 23 条第 1 項、ＥＣＯＭガイドライン 20 条）

＊第三者提供の禁止についての除外事項

（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。

ただし、現代において個人が社会生活を営む上で、個人情報が流通することによりその本人を含め社会全体として、格段に利便性を享受できることもあり、そうした点を踏まえて、保護法では、①第三者提供を利用目的とする旨、②個人データの項目、③第三者提供の方法、　④本人の求めにより第三者提供を停止することをあらかじめ本人に通知、または本人が容易に知り得る状態においていることを条件に、オプトアウトの措置をとればいいと定められている。（保護法第 23 条 2 項、ＥＣＯＭガイドライン第 21 条）

これらの対象となる事業者としては、住宅地図業者、データベース業者などが考えられている。

4.5.2　第三者提供・委託・共同利用の解釈

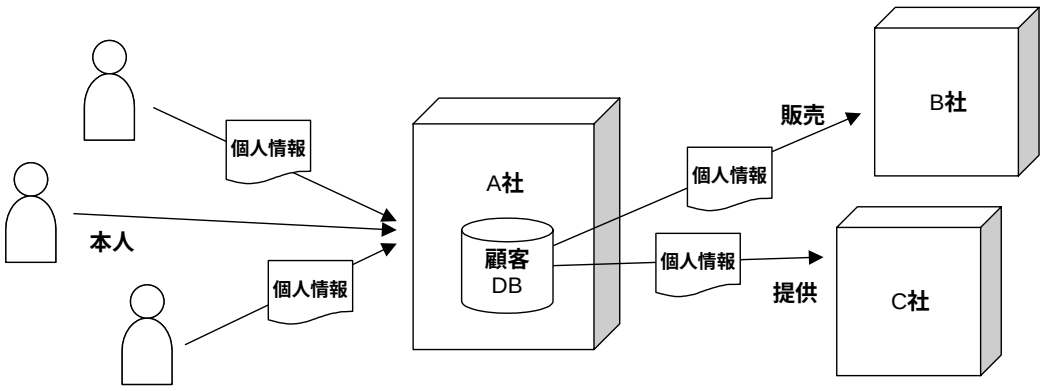
また、保護法では、委託、合併・事業継承及び共同利用の場合は、第三者提供に該当しないとされている。それらのうち、委託と共同利用については第三者提供との違いについては、どのように解釈し、どのように実際に対処したらいいかについて誤った見識を持た

ないようにしなければならない。以下に、それぞれのケースについて、実際の場面を想定しながら整理してみる。

【第三者提供】

第三者提供は、事業者が第三者である他の事業者または個人の利用のために、保有する個人データを提供することである。提供に際しては有償で行われる場合もあれば無償の場合もある。保護法では、提供にあたっては、あらかじめの本人同意が必要であるが、提供後の利用については、第三者提供を受けた事業者が、本人に対し、個人情報を取得したものとしての責任（たとえば利用目的の通知または公表等）を負う。さらに、個人データ、保有個人データとして保有する場合は、さらにそれらの義務を果たさなければならない。

即ち、下図 4-5 に表わすところの第三者提供する事業者の立場にある A 社について考えた場合、効果としては第三者にあたる B 社または C 社に情報漏洩や濫用等があったときの責任は回避できるが、あらかじめ第三者提供をすることについて本人より同意を取ることが必要となる。



定義	第三者である別の事業者または個人に他の個人データを有償又は無償で提供すること
効果	第三者による情報漏洩や濫用等があったとき、責任が及ばない
義務	あらかじめ本人の同意が必要

図表 4-12 第三者提供

【共同利用】

個人情報保護法では共同利用する場合を第三者提供に該当しないものとして規定している。個人データを共同利用する際には、以下のことについて、あらかじめ、本人に通

知、または本人が容易に知り得る状態におくことが義務づけられている。（保護法第 23 条第 4 項・第 5 項、ＥＣＯＭガイドライン第 22 条）

＊共同利用する際にについてあらかじめ、本人に通知、または本人が容易に知り得る状態におかなければいけないこと

① 特定の者との間で共同利用する旨

② 共同利用される個人データの項目

③ 共同して利用する者の範囲・・・外延を明確にする必要（例：全国都市銀行）

④ 利用する者の利用目的

⑤ 個人データの管理について責任を有する者の氏名または名称

上記④、⑤については、変更する場合は、その変更について、あらかじめ、本人に通知、または容易に知り得る状態に置くことが必要となるが、①、②、③については変更できないとされている。

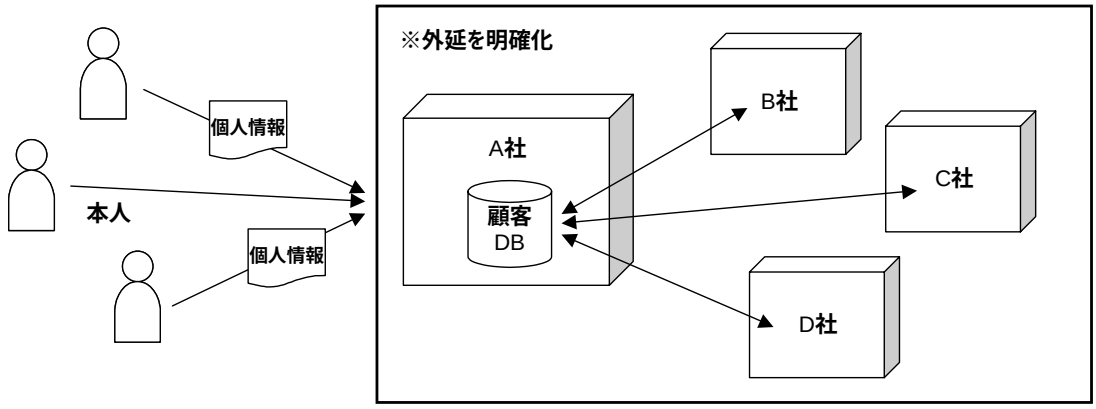
個人データを共同利用するという概念で考えた場合、共同利用する事業者のグループの中では、そのグループに属するそれぞれの事業者が、そのグループとして本人に対して示された利用目的の範囲内で、共有する個人データを反復･継続して利用しうることとなる。本人にとっては、そのグループが、少なくとも個人データの利用において、あたかもひとつの事業体のように見えるものであると考えられるため、その本人に対して、代表的な立場で個人データの管理について責任を有する者が必要となり、さらにそのことが常に容易に知ることができるようにしておくことが求められる。そうすることにより、その管理責任を有する者（事業者）は、共同利用するグループ全体の個人情報の取扱いに関するその本人に対する責任を有することとなる。例えば、そのグループに属する事業者が個人情報の漏えいや濫用をした場合、本人に対しての責任ある対処が求められるのである。

従って、共同利用する者の範囲に含まれる事業者については相当の信頼関係があるか、または会則や契約等により取り扱い上の制限や責任の所在を明確にした上でのグループ内の運用がなされることが前提となるであろう。

「共同して利用する者の範囲」については、必ずしも事業社名をすべて個別に列挙することが義務づけられているわけではないが、本人にとって、利用する者の範囲が具体的に特定できる外延が明確にされていないといけない。さらに、前述したようにこの外延は変更できないとされている点で、その構成する事業者が変動する場合についての解釈と対応については、議論と熟慮を要するところである。

例えば、サイバーモールとそのモールに所属するショップ間で個人情報を共通の Web 画面上で取得・利用する場合等を共同利用として考え得るかどうかについては、個人データの管理責任の所在や共同で利用する個人データの利用目的を会則や契約の中で明確にするとともに、共同利用する外延が明らかになるような配慮と措置が必要となるだろう。（個別の事業社名を表示する等といった方法が考えられる。その場合、そうした措置をとることにより「利用する者の範囲が具体的に特定できる外延」が変更されてしまわないか、については検討を要する。）

整理すると、下図 4-6 に示すように、個人データを共同して利用し、その個人データの共同利用について管理を行うＡ社は、共同利用をする旨をはじめとする 5 項目を通知または容易に知り得る状態に置き、さらに共同利用を行う範囲において本人に対して管理を行う責任があるが、共同利用する範囲の事業者は、利用目的として示す範囲内において、反復継続して個人情報を利用できるというメリットを持つこととなる。



定義	特定のグループ内で個人データを共有し、活用する
効果	共同利用の範囲内で、反復継続して有効活用できる（DM 他）
義務	• 以下のことをあらかじめ本人に通知、または容易に知り得る状態におく ① 特定の者との間で共同利用する旨 ② 共同利用される個人データの項目 ③ 共同して利用する者の範囲・・・外延を明確にする必要 ④ 利用する者の利用目的 ⑤ 個人データの管理について責任を有する者の氏名または名称 • 共同利用の範囲内の管理責任

図表 4-13 共同利用

【委託】

同じく、個人情報保護法では、利用目的達成に必要な範囲内において個人データの取扱の全部又は一部を委託する場合は、第三者提供に該当しないものとして規定されている。（保護法第 23 条第 4 項、ＥＣＯＭガイドライン 22 条）

ただし、委託を行う場合には、一方で、委託先に対する必要かつ適切な範囲での監督義務が発生する。（保護法第 22 条、ＥＣＯＭガイドライン 18 条）

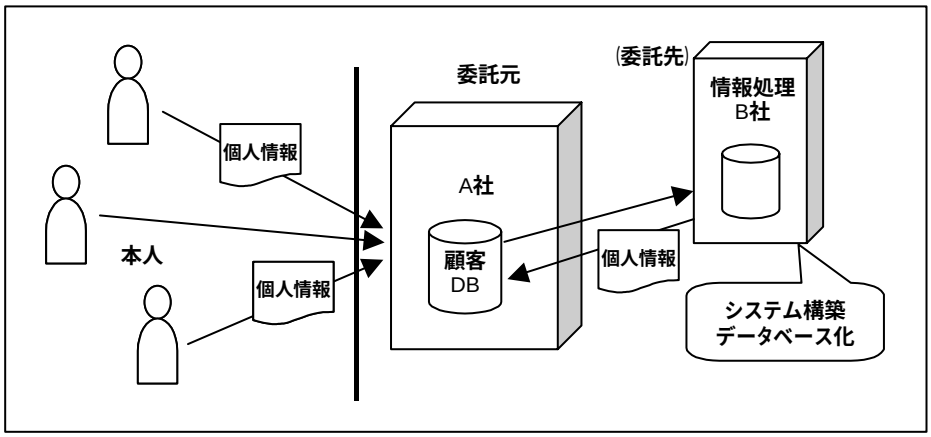
また、個人データの取扱の全部又は一部を委託する場合についてはいくつかのケースが考えられる。

例えば、下図＜例１＞のケースのように、委託元であるＡ社が収集した個人情報を情報処理事業者であるＢ社にシステム構築及びデータ入力といった作業を委託する場合などは本人にとっては、委託先であるＢ社は、Ａ社のバックヤードで個人データを取り扱っているので目に映らないことが多いだろう。

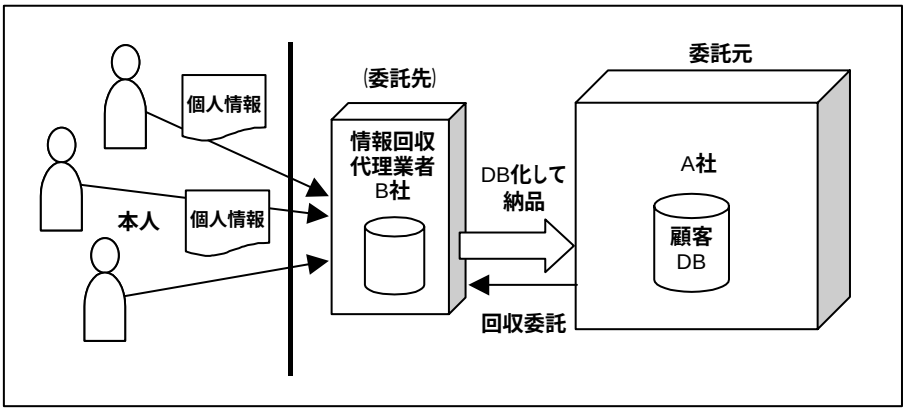
また、＜例２＞のように，Ｂ社が、個人情報収集の時点よりの業務委託を受け、本人より直接に個人情報を収集するケースもあり、この場合は本人が委託先であるＢ社と接点を持つ状況もありうる。（この場合、委託元であるＡ社名で収集するケースと、Ａ社より委託を受けたとした上で、Ｂ社名で収集するケースがある。）

さらには、＜例３＞のように情報処理に関する業務以外として、例えば受注商品の配送等のために、配送会社に本人の住所・氏名・電話番号等を告げ、配送することにより、契約を完結するといった形態の委託もあると考えられる。

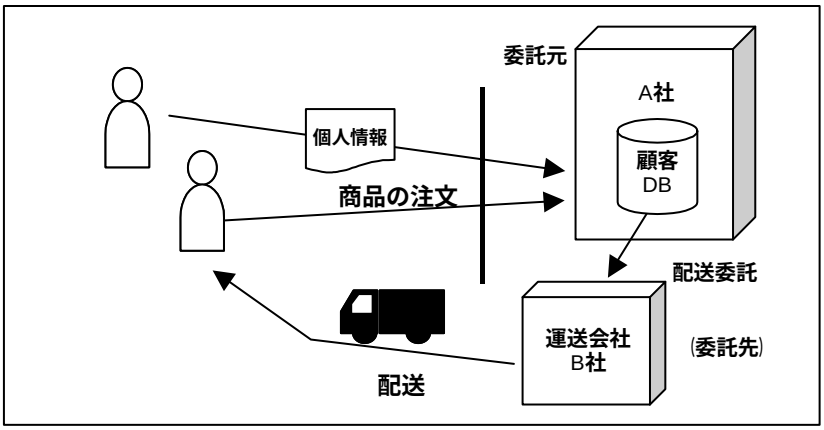
＜例 1＞ 事業者が個人情報を取得する時には、本人からはＡ社しか見えない



＜例 2＞ 委託先のＢ社が本人に接して、個人情報の収集業務を委託代行



＜例 3＞ 契約履行のため、商品の配送をＢ社に委託、住所、氏名等の個人データを提供



定義	事業者における機能の一部を他の事業者に委ねること
効果	取得時に共同利用等の手続きを取らなくて良い
義務	● 委託先の監督責任（委託先の選定基準、評価、契約書等） ● 開示・訂正・削除等の求めに対する対応 ● 委託を受けた事業者はその個人情報を無断で独自に利用できない

図表 4-14 委託

4.5.3 想定される具体的事例の考察

複数の法人間で個人情報の受け渡しが発生する第三者提供・共同利用・委託に関してはその受け渡しの実態により、異なった措置を講ずることが必要となり、それぞれに義務や制限が発生する。受け渡しがなされる実態が第三者提供か、共同利用か、委託かの判断が、事業者と本人間、あるいは事業者と主務官庁間で一致しないために、トラブルを引き起こ

すケースも考えられるので、この点についても注意を要する。

以下にいくつかの事例を挙げ、それがどのケースと捉えるべきかについて考察する。

事例 1：旅行代理店の予約代行業務

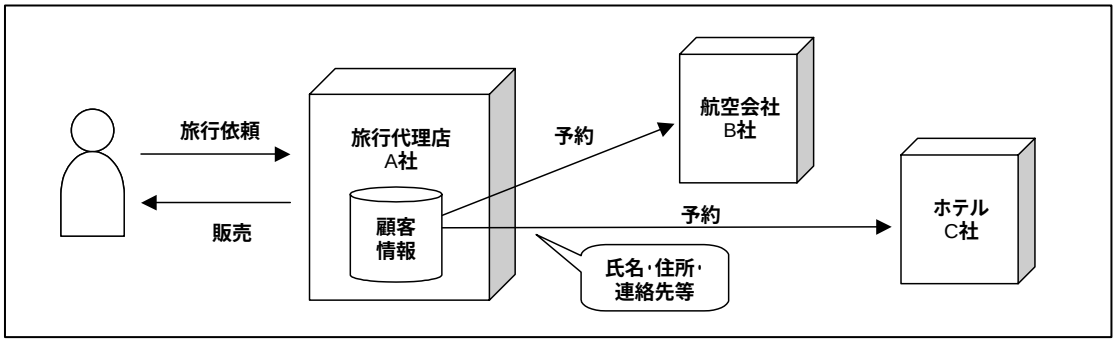
個人情報保護基本法法制研究会編の「Q＆A個人情報保護法」に示されるように「グループ企業等を通じて総合的なサービスを提供する観光・旅行業の活動は、・・・中略・・・サービス・商品の提供や事業活動の適正化等のために、ある事業者が取得した個人情報を他の事業者と相互に利用する」こととして、共同利用の例としてあげられる。

しかしながら、下図 4-8 に示すように、旅行代理店 A 社が、顧客から依頼された旅行計画に基づき、航空会社 B 社やホテル C 社に顧客の個人情報を提供して予約業務を代行する行為により渡された個人情報は、航空会社Ｂ、ホテルＣにおいてそれぞれ搭乗予定者リスト或いは宿泊予定者リストしてファイルされ、その後も、旅行代理店Ａの持つ顧客情報データベースと異なる管理下に置かれるものとも考えられる。

さらには旅行代理店と提携する輸送機関や宿泊施設については、常に変動することもあると思われ、外延が客観的に明確と言い難いとも考えられる。（ただし、パンフレットには、具体的な旅行企画書に明記されているので、その限りにおいては明確であると言える。）

以上を考え合わせると、この場合の措置としては、同意の元に第三者に提供されるものとして取り扱われると考えるべきケースもあるのではないか。

従って、その視点に立って考えた場合、旅行代理店Ａ社は、手配に際し、個人情報取得する時点で、航空券及び宿泊手配について、何らかの形で、第三者提供がある旨の同意を取ることが必要となると考えられる。

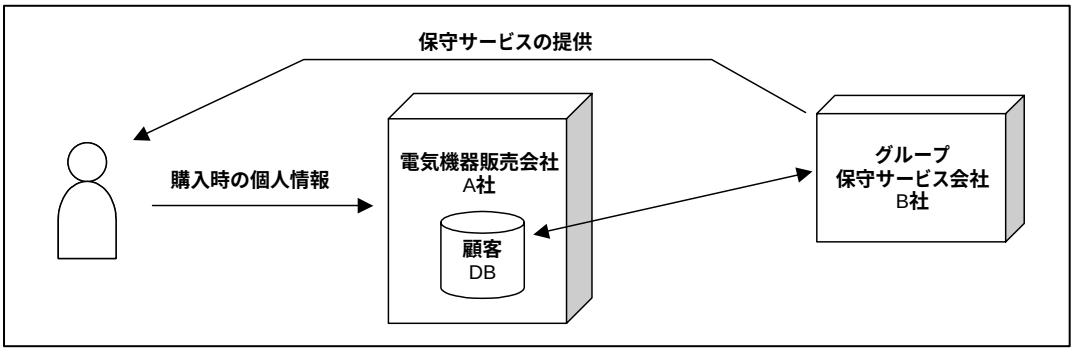


図表 4-15　事例 1：旅行代理店の予約代行業務

事例 2：グループ会社での総合サービス

また、下図 4-9 に示すように電気機器販売会社Ａ社が購入者の個人情報を、系列グループ会社の保守メンテナンス会社Ｂ社と共同利用して総合サービスをするケースも、日常的に見られる事例である。電気機器に限らず、情報通信機器、自動車等購入後のアフターサービスが必要な業種では、よくあるケースであるが、この場合の購入者情報提供については、購入者に対する総合的サービスを提供するという点で、共同利用として考えられる。むしろ、事例 1 のケース以上に系列という点で、グループ内での信頼関係や共通した価値観に基づく情報共有も可能であると考える。

ただし、そうした信頼関係が希薄である場合や、客観的に見て外延が明確でないケースには、第三者提供としての措置をとることが望ましいと考える。



図表 4-16　事例 2:グループ会社での総合サービス

事例３：サイバーモールの新情報提供サービス

以上の２事例に加えて、インターネット上で営まれる電子商取引の場面でも消費者の個人データを事業者間で受け渡しを行うケースがある。サイバーモールなどはその一例と言える。

下図 4-10 に示すように、サイバーモール運営事業者が、モール内ショップでの購入者の個人情報をもとに、消費者に新情報の提供等のサービスを行なうケースがある。

サイバーモールについては、傘下に多数のショップを抱え、Web 画面上にサイバーモール運営者のロゴやフレームを残し、さらには共通の受注画面を備える大規模なポータル事業を行う事業者もあれば、ポータルサイトより傘下のショップにバナーを張り、ショップサーバーに移行してしまう小規模なものまで様々な形態が見られる。

前者の場合、ネットショッピングが行われる際には、発注や契約に関して個人情報が入力される時点で、サイバーモール運営者と対象ショップの双方ともその個人情報を取得す

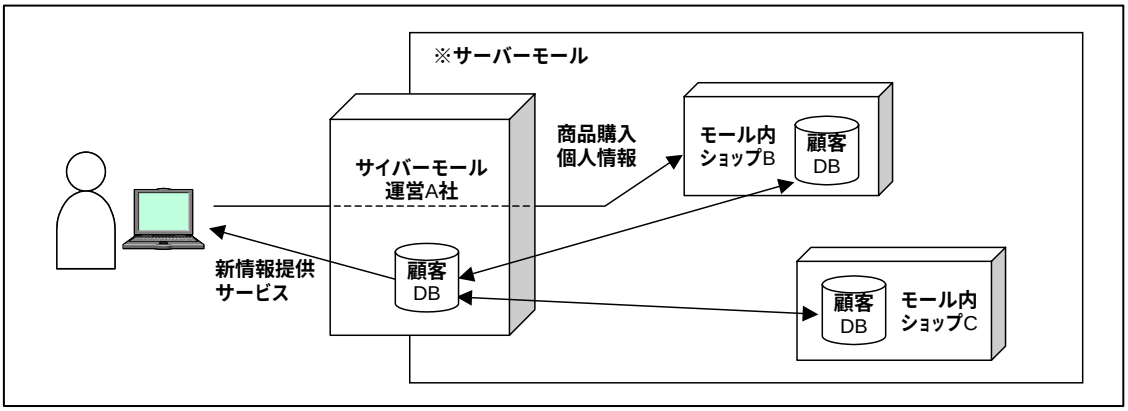
ることになるケースが多いようである。

その場合の考え方としては、どのように対応すべきであろうか。

大手のサイバーモール事業者では、ショップがモールに加入する際、ショップ選定基準や出店に関する会員規約が設定されており、概ねその規定に基づいて個人情報の取扱いが行われる。

併せて、利用者に会員登録を促し、会員となった利用者に販促情報をメール送信するケースがよくあるが、こうした情報発信のためのデータベースをサイバーモール、ショップのどちらが利用者に対して運営および管理責任を有するかといったことについて、実際の運用をどのようにするかに基づき、規約化しておくことが大切である。

それが、以上に述べた、「第三者提供」「委託」「共同利用」のどの要件に適合するかに応じて、サイバーモール運営者とショップの間で取り決め、消費者の混乱を招くことのないように適切に措置を施すことが望まれる。



図表 4-17　事例 4：サイバーモールの新情報提供サービス

4.6　ホームページ上での個人情報保護に関する公表

個人情報保護法では､第 18 条第 1 項で個人情報取得時における利用目的の公表が､また､第 24 条ですべての保有個人データの利用目的、個人情報取扱事業者の氏名・名称等の公表（本人の知りうる状態に置くこと）が規定されているように、個人情報を取り扱うに当たっては、一定の事項を公表すべきことが義務として課せられている。

また、ECOM 個人情報保護ガイドライン Ver2.0<α版>でも、その第５条で個人情報保護方針の公表を条項として設けている。個人情報保護方針を外部向けに文書化し、わかりやすい表現で公表することを条文として設定しているのだが、どのような表記の仕方が効果的であるのか。

4.6.1　プライバシーポリシーの掲載の実態

第 2 章の「ECOM 会員企業個人情報保護の実態把握」にて記すとおり、2003 年 7 月時点のプライバシーポリシーの表示実態について目視調査を行った。（P46～P49 参照）そこでは日本企業においてホームページを開設・運営するにあたり、プライバシーポリシーというものの掲載が着々と増えつつあるということがわかる。

しかしながら、どのような内容が表記されているかを同調査の中で調べたが、その表記のレベルはまちまちであり、それにより、利用者や消費者が保護法に既定される項目について判断しうるに足る記載がされているかというとそうではないケースも多々見られる。そもそも、個人情報保護方針あるいはプライバシーポリシーという言葉の定義についても確立されているわけではなく、企業ごとに独自の判断の元に様々に解釈され表されているのが実態である。

しかしながら、その境界がはっきりとしているわけではないが、記載の内容から大別すると、①その企業の代表者（社長または担当役員等）が、その企業の個人情報保護のスタンスについて利用者・消費者に決意表明するものと②その企業の個人情報保護についての措置や事務手続き等を細かく解説する説明書に相当するものという２つがタイプとしてある。場合によっては、その二つを兼ね備えた企業もあり、その場合、多くは①を「個人情報保護方針」「プライバシーポリシー」と、②を「個人情報の取扱いについて」というタイトルで記載しているようであった。

そこで、その実態について、2003 年 12 月に再度、ECOM 会員企業の Web ページについて再調査を実施した。

トップページ表記	①方針・宣言のみ	①方針・宣言＋②手続き	②内容・手続きのみ	計
①個人情報保護方針	36	18	8	62
①プライバシーポリシー	25	11	15	51
②個人情報の取扱いについて	5	3	4	12
計	66	32	27	125

図表 4-18　ホームページ　「個人情報保護」表記分類表（2003 年 12 月目視調査）

その言葉の意味より、①「個人情報保護方針」「プライバシーポリシー」と②「個人情報の取扱いについて」とその言葉の意味どおりに大別されると推察したが、上記の図表４-８の結果の限りでは、現状実態として明確な使い分けがされているとはいえない状況である。

4.6.2　海外におけるプライバシーポリシーに関する動向～Short Form Notice の検討～

北米では、インターネットでビジネスを行う企業の約 9 割が、ホームページのトップ画面にプライバシーポリシーへのリンクボタンを設置しているといわれる。しかし、長年の運営や法的な規制の影響を受け、その表現は冗長かつ難易なものとなっている傾向にあり、一部に問題視され始めている。

そのプライバシーポリシーの表記について、2003 年 9 月にシドニーで開催された「第 25 回プライバシー・データ保護コミッショナー会議」でより簡潔にわかりやすく表記するため、定型のフォーマットに一定の必要要件を記述することが提唱された。（P132、「5.1.3.3 データ保護及びプライバシー情報の取扱いについてのよりよい伝達に関する決議」参照）

さらにその具体的なフォーマットについて、「Hunton＆Williams」の情報政策リーダーシップセンターより以下のような仕様のテンプレートが紹介されている。

4.6.2.1 プライバシーポリシーにおけるハイライトのテンプレート～ユーザーズガイド

＜Hunton & Williams 情報政策リーダーシップセンター・パンフレット翻訳文＞

Hunton & Williams の情報政策リーダーシップセンター、及び同センターのショートノ

ーティスプログラムの参加者はこのたび、「ハイライト」型プライバシーポリシー作成の助けとなるテンプレートを制作した。このテンプレートは、各企業が掲げる長く詳細なプライバシーポリシーのうち、主なポイントだけを簡潔明瞭に表現したものを作るためのモデルとなることを目的とする。プライバシーポリシーのハイライト版は、完全なバージョンの上の階層に置かれるよう意図されたものである。

背景

米国金融制度改革法に定められたプライバシーポリシーはきわめて煩雑であり、世間やメディア、そして政府から批判が噴出した。リスクの声明文に関する研究を見ると、なぜ同法に基づくポリシー文が、これほどまでに消費者の批判を受けたのかが分かる。研究によれば、人がポリシー文の解読に困難を覚えるのは、(i)ポリシーが 7 個より多くの要素から構成されている、(ii)使用されている語彙を、自分が理解できる言葉に「翻訳」する必要がある、以上の 2 つの場合である。理解にあまりに多くの努力が必要な文章を目にすると、読み手はフラストレーションがたまる。このポリシー文はわざと難しく書かれている、このような文章を書く会社は何かを隠している----多くの人がそう思うに至ってしまう。

この研究によると、プライバシーポリシーは短めにし、平明な表現を使うべきだという。また消費者の理解と信頼を得るためには、すべての企業が同じフォーマットを用いるべきだという。プライバシーポリシーにこうしたシンプルさを要求することは、法が要求するところの「ポリシーとは完全無欠であるべし」という立場とは往々にして真っ向から対立する。

ポリシーに「階層」を設けるというコンセプトは、短くてシンプルなプライバシーポリシーを提示したいものの、法律には適合するが難解なポリシーを提示する必要があるのではないかという思いの間で揺れる企業にとって、一つの解決策となる。簡略版のポリシーは消費者に対し、個人情報の使用に関する情報を伝えるコミュニケーション・ツールとなるほか、個人情報の使用方法についてどのような選択肢があるかを個人に伝える役割も果たす。一方、長いバージョンのポリシーは簡略版の 1 つ下の階層に置かれ、法で求められるすべての要素(あるいは法で求められていないとしても、簡略版より詳細な説明)が盛り込まれる。ショートノーティスプログラムでは、プライバシーポリシーのハイライト版を共通のテンプレートとしてフォーマット化し、すべての企業で似たような表現を使用できるようにした。これにより、消費者はさまざまな企業のプライバシーポリシーの簡略版を見比

べることができる。
同プログラム参加者は、消費者にとって最も重要である可能性の高い情報は何かを考えた結果、すべてのハイライトに必ず使用されるべき共通要素を定めた。共通要素は 7 つまたはそれ以下のカテゴリに限定することとし、各カテゴリに含まれる文章数は最大 4 つとした。これに収まりきらない詳細な情報は、完全版のポリシーに含めることとする。また主な概念の説明にあたっては、可能な限り記述が明快になるよう、言葉の使用方法も定めたほか、テンプレートに含まれる単語が、読者の頭の中で分かりやすい単語に変換されるようなことのないよう、万全を期した。
このテンプレートの一般フォーマットをベースにして、各企業がそれぞれ独自にプライバシーポリシーの簡略版を作成して頂ければ幸いである。

Privacy Notice Highlights Template **に使用されるカテゴリについて**
（次項「ハイライト型プライバシーポリシーの仕様」に要約掲載）

テンプレートの利用について

「プライバシーポリシーにおけるハイライトのテンプレート」に対する著作権は、Hunton & Williams の情報政策リーダーシップセンターに帰属します。本テンプレートの目的は、消費者が一目で企業の情報管理の方法を理解するための一助となること、また異なる企業の情報管理方法の比較を可能にすることにあります。本「テンプレート」の利用を希望する企業は、テンプレートのデザインを踏襲し、ガイドラインに概ね従う限りにおいて、これを使用することができます。

「プライバシーポリシーにおけるハイライトのテンプレート」または本ユーザーズガイドについてのご意見・ご質問は、以下にお願い致します。
Marty Abrams (404-888-4274)
Peggy Eisenhauer (404-888-4128)
Lisa Sotto (212-309-1223)

4.6.2.2 ハイライト型プライバシーポリシーの仕様

「ハイライト型プライバシーポリシー」のショートノーティスプログラム仕様は以下の

とおりである。

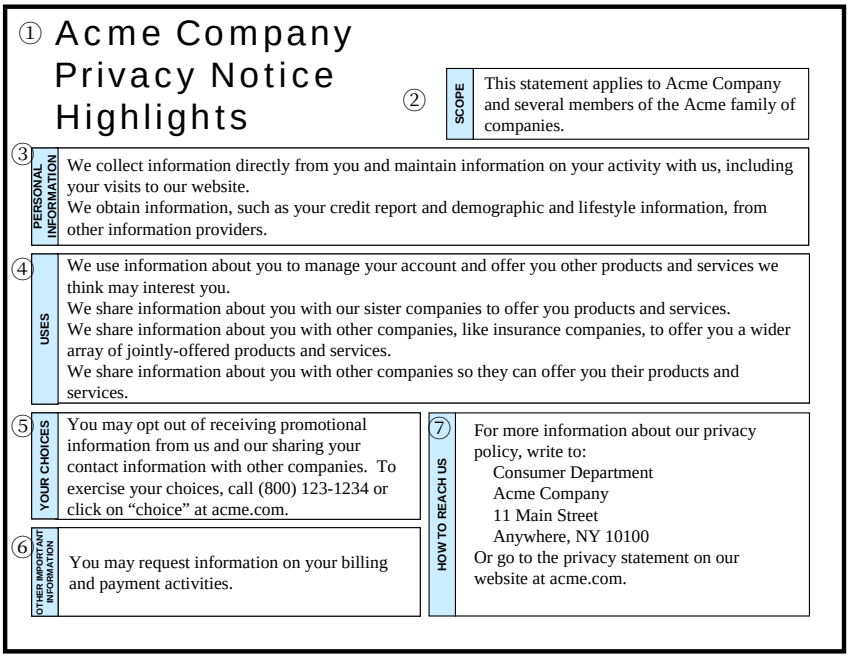
Privacy Notice Highlights Template **に使用されるカテゴリ例**

	項目	記載内容
①	社名	会社名
②	適用範囲 ･個人情報の取扱いについて適用される事業者の範囲及びサイトの範囲	プライバシーポリシーが適用される主体を明らかにする。下記のケースのいずれであるかを明確化する ① 当該企業に限り適用される ② 同一社名で事業展開している企業群全体に適用される ③ 異なる企業名で事業展開している企業群すべてに適用される ④ 一つのブランドのみで実施されるプログラムに適用される ＜表記例＞ 企業は「このポリシーは当社のオンライン事業にのみ適用されます」と記したり、あるいは全社に適用される場合は「オンライン事業にのみ」の部分を削除したりすることになる。
③	個人情報 ･取り扱う個人情報の種類 ･取得の方法 ･取得に関する業務	消費者に対し、企業が収集する個人情報の種類およびその入手先を明らかにする。 消費者にとって必ずしも明らかでない可能性のあるような方法で情報を入手している場合に、そのことについて説明する。 企業が収集する情報は (i) 消費者がその企業に提供したもの (ii) 企業が消費者と関係を持った結果として取得したもの (iii) 消費者について他者(ビジネスパートナー、無関係な第三者など)がその企業に提供したもの のいずれかなどを明確にする。 クッキーなど技術的で、消費者が敏感に反応する情報入手の方法、あるいは消費者に分かりづらいその他の情報入手方法については、特に明記することが望ましい。 読み手の理解を助けるよう、このカテゴリに含まれる文章の数は 4 つ以下に抑えることが望ましい。
④	使用 ･個人情報の利用目的 ･共有（共同利用）や取引等の第三者提供（委託等も含め）があるか	「使用」欄は、 (i) 企業は消費者の個人情報をどのように使用するか (ii) 個人情報が誰と共有されるか の 2 点を示すことが目的である。 ここでは社内における個人情報の使用だけでなく、社外での使用についても明記することとする。データの公開は「共有」とも呼ばれるが、データの使用や共有は以下の 4 種類に大別される： (i) 当該企業自身が、消費者へのサービスの提供または宣伝のためにデータを使用する場合 (ii) 当該ポリシーを提供している企業の提携企業がデータを使用する場合 (iii) ポリシーを提示している企業および別の企業が、共同で製品またはサービスを提供するためにデータを使用する場合（日本でいう共同利用） (iv) 他の企業が独自に製品またはサービスを消費者に提供することを目的として、データを公開する場合。（日本でいう第三者提供） 他者への公開には、提携団体やビジネスパートナーとの情報共有のほか、無関係な第三者との情報共有も含まれる場合がある。ポリシーに記載され

		た団体の種類別に、どうしてその団体と情報を共有するのか、その理由を説明することが望ましい。 この「使用」欄は、完全版でより詳しい説明を記載したり、請求に応じて詳しい説明を提示することが必要になる場合がある。例えば、情報共有の方法別にそれぞれ複数の選択肢を示した場合、完全版ではそれらの選択肢をさらに細かく区分けして説明する必要な場合もある。 消費者が複数の選択ができる場合も、その内容について詳しく説明する必要があるだろう。
⑤	選択肢 ・個人情報に関するアクセスや削除要求等	「選択肢」欄では、企業が入手した消費者の個人情報を公開または使用する場合、消費者はどのような選択肢を行使できるのか、またどのような方法でそれらを行使できるのかを表わす。 または、特定の使用や公開について、オプトアウトまたはオプトインする機会が与えられるか否かを表わす。 企業は、消費者に与えられた選択肢を説明し、必要な場合は複数の選択肢を示す。簡略版では、最も重要と思われるものにしぼって選択肢を提示するべきである。 ＜表記例＞ ・「個人情報をお知らせ頂く時点で、提供の可否をお決め頂けます」 ・「ご自分の個人情報を第三者に共有しないよう、選択することもできます」 ・「このサイトのご使用を選択された場合、オプトアウトすることはできません」 (co-branded のサイトなどに使用できる表現) 特に注意を要する情報については、この「選択肢」ではなく「重要情報」のカテゴリにおいて、その情報の選択について説明してもよい。逆に、幅広い選択肢を用意している場合は、選択肢を選びたい人は完全版を参照するよう(または会社に連絡するよう)、簡略版に記すことも可能である。
⑥	重要情報 ・マーク付与団体等へのアクセス ・セキュリティや責任について	「重要情報」は企業にとって重要なメッセージを記載するためのカテゴリで、オプションである。 例えば、プライバシーポリシーがプライバシー・シール・プログラムによるレビュー及び施行の対象である場合、その旨を記載するとよい。 また個人情報の保存期間や連絡の頻度について、あるいは消費者との特定の取引が終了すれば直ちに情報を削除する場合はその旨を記載してもよい。 さらには、購入歴に関する情報を他者と共有しない旨を記したり、法や社内規定で定められた補足情報を記したり、個人の財務情報と健康情報を収集する団体が健康情報を他者に開示しない場合は、その旨を記してもよい。
⑦	連絡先 ・問合せ連絡先 ・プライバシーポリシー（経営責任者の表明）へのリンク	「連絡先」欄は、消費者が企業のプライバシー方針について質問や意見を寄せたい場合のために、連絡先の情報を提供する。 記載する内容は「適用範囲」の記載内容に応じて決定する。 また、プライバシーポリシーの媒体にあわせて、記載する連絡方法も変える必要がある。 インターネットで提供される場合→e メールアドレス オフラインで提供される場合→郵送先と電話番号 簡略版のテンプレートが消費者に受け入れられるかどうかは、テンプレートに連絡先に関する情報がシンプルかつ明確に記載されているかどうかによって大きく左右される。このため、企業は 2 種類以上の連絡方法を記載することが望ましい(フリーダイヤルと E メールアドレスなど)。オフラインで存在する会社は、インターネットとは無関係の連絡方法を少なくとも 1 種類、記載するべきである。

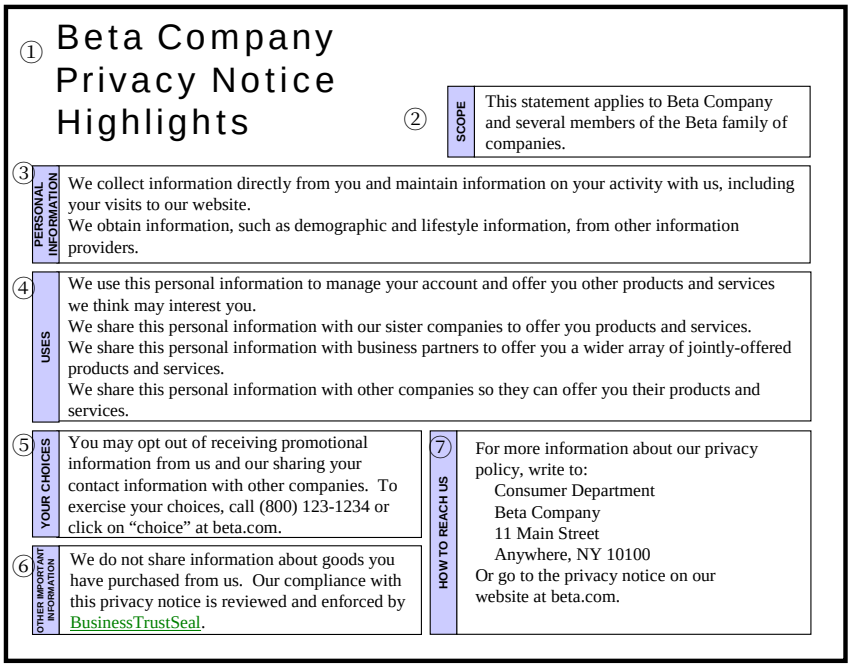
図表 4-19　Privacy Notice Highlights Template に使用されるカテゴリ例

Privacy Notice Highlights Template



Template prepared by the Notices Project, a program of the
Center for Information Policy Leadership at Hunton & Williams

Privacy Notice Highlights Template



Template prepared by the Notices Project, a program of the
Center for Information Policy Leadership at Hunton & Williams

図表 4-20　Privacy Notice Highlights Template

4.6.2.3 ハイライト型プライバシーポリシーに関するデザイン要件

また、「ハイライト型プライバシーポリシー」に関して、Hunton & Williams の情報政策リーダーシップセンターでは、「スタイル、一般的なフォーマット」、「フォント、色」、「オンライン上の要件」についてデザイン上、以下のことが定められている。

デザイン上の要件について

I．スタイル、一般的なフォーマット
1. ハイライトは「適用範囲」「個人情報」「使用」「選択肢」「連絡先」の計 5 つのボックスから構成されることとする。このほか「重要情報」のボックスを設けてもよいが、必ずしも必要ない。 各ボックスに含まれるべき情報についての詳細は、ユーザーズガイドを参照。 2. 「適用範囲」「個人情報」「使用」は、必ずこの順番通りに掲載すること。ボックスの大きさは、文章がちょうど収まる程度とする。 3. 「選択肢」「連絡先」「重要情報」のボックスは、この順番で掲載してもよいし、または「選択肢」「連絡先」のみを、ボックスの大きさに合う並べ方で掲載してもよい。 4. ボックスの外周には線または影を施し、何らかの区切りを設けること。背景色は、印刷物全体またはサイトに合わせる。 5. 各ボックスの見出しは、印刷物全体またはサイトのデザインに合わせ、ボックスの一番上または左端に配する。 6. タイトルは「プライバシーポリシーのハイライト」とし、「適用範囲」のボックスの上または横のうち、より効果的な場所に配する。 7. 「個人情報」「使用」「選択肢」の本文が長くなった場合は、読みやすさを考えて 2 段組にしてもよい。 8. ボックス内に情報を列挙する場合は箇条書きを用い、ポイントを分かりやすく示す。
II．フォント、色
1. Pepita MP、Snap ITC、Edwardian Scripts ITC といった一般的でないフォントは、プライバシーポリシーでは使用しない。代わりに Helvetica、GillSans MT、 Arial、Garamond を用いる。 2. ボックス内の文字サイズは、8 ポイント以上とする。 3. 見出しの文言は「ユーザーズガイド」に記載された通りとし、例外は認めない。見出しの文字サイズは 10 ポイント以上とし、ボールドまたはエキストラボールドを用いる。またボックスの本文よりも大きな文字サイズを用いる。 4. 色については、印刷物全体またはサイトに合わせることとする。ただし、ポリシー内で使用できる色数は 3 色以内とする。
III．オンライン上の要件
1. 企業の「プライバシーポリシー」へのリンクをクリックしたら、まず簡略版のポリシーが開くようにすること。 2. 簡略版にはリンクを随所に埋め込み、完全版のポリシーにジャンプできるようにする。 a. 簡略版には、完全版の冒頭にジャンプできるリンクを設ける。 b. 「選択肢」「連絡先」には、完全版の関連箇所にジャンプできるリンクを設ける。 c. ポリシーの完全版に他のセクションへのリンクがあった方がよい場合、リンクを設けてもよい。

図表 4-21　Privacy Notice Highlights Template デザイン上の要件について

4.6.3 個人情報保護法における公表すべき要件

日本の個人情報保護法では、あらかじめ特定した個人情報の利用目的等を公表することが義務付けられている。ここでは、同法に規定される公表等の要件について下記にまとめる。

条項	条文（義務）	措置	対象
第 18 条 第 1 項	個人情報取扱事業者は、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。	公表	利用目的
第 23 条 第2項 ＊条件：オプトアウトが適用される場合	個人情報取扱事業者は、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としている場合であって、次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、前項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。 一　第三者への提供を利用目的とすること。 二　第三者に提供される個人データの項目 三　第三者への提供の手段又は方法 四　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。	本人が容易に知り得る状態に置く	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。
第23条 第 4 項三 ＊条件：共同利用が適用される場合	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あって、その旨並びに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及び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。	本人が容易に知り得る状態に置く	① 共同利用の旨 ② 共同して利用される個人データの項目 ③ 共同して利用する者の範囲 ④ 利用する者の利用目的 ⑤ 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
第24条 第 1 項	個人情報取扱事業者は、保有個人データに関し、次に掲げる事項につい	本人の知り得る状態（本人の	① 当該個人情報取扱事業者の氏名又は名称

	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。 一　当該個人情報取扱事業者の氏名又は名称 二　すべての保有個人データの利用目的（第十八条第四項第一号から第三号までに該当する場合を除く。） 三　次項、次条第一項、第二十六条第一項又は第二十七条第一項若しくは第二項の規定による求めに応じる手続（第三十条第二項の規定により手数料の額を定めたときは、その手数料の額を含む。） 四　前三号に掲げるもののほか、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政令で定めるもの	求めに応じて遅滞なく回答する場合を含む。）に置く	② すべての保有個人データの利用目的 ③ 本人からの求めに応じる手続（利用目的の通知、保有個人データの開示、訂正、追加、削除、利用停止、手数料） ④ その他、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 ・苦情の申し出先 ・認定個人情報保護団体の名称及び苦情の申し出先 (1)開示等の求めの申し出先 (2)開示等の求めに際して提出すべき書面の様式その他の開示等の求めの方式 (3)開示の求めをする者が本人又は次条に規定する代理人であることの確認方法 (4)手数料の徴収方法

図表 4-22　保護法で公表等が求められる要件

4.6.4 「Privacy Notice Highlights Template」と日本の保護法の公表についての要件の対比

上記の検討を踏まえ、日本の個人情報保護法に対応した「Short Form Notice」について整理してみる。

保護法では、以下の場合に「公表」、「本人が容易に知り得る状態に置く」又は「本人の知りうる状態に置く（本人の求めに応じて遅滞なく回答する場合を含む。）」ことが求められる。ミニマムに考えた場合、前項の整理より、保護法第 24 条の「本人の知り得る状態」に置くケースを「本人の求めに応じて遅滞なく回答する」形で対応すると考えた場合、無理に公表の項目に置かなくても良いという考えより、第三者提供に対するオプトアウトや共同利用のケースではない場合であれば、第 18 条で規定される個人情報取得時の「利用目的」のみとなる。

しかしながら、本人に対して「本人の求めに応じ」るためには、現実的には「当該個人情報取扱事業者の氏名又は名称」や「開示等の求めの申し出先」等が公表されている状態であることが必要となる。その他前出の「Privacy Notice Highlights Template」に使われるカテゴリと対比すると、必ずしも記載が求められているわけではないが、そのカテゴリに示される記載項目を適宜掲載することで、消費者によりわかりやすく自社の個人情報の取扱いについて知らしめることが可能となると考えられる。

さらに具体的な説明を表わした事項やトップのプライバシーポリシーに相当する内容については、それぞれよりリンクさせることで、詳細について求める利用者に対して情報を提供できるのである。

Privacy Notice Highlights Template **に使用されるカテゴリ例**

（保護法対応欄：◎＝保護法で公表が求められる事項、●＝条件により保護法で公表が求められる事項、○＝個人情報保護の措置について消費者に知らしめることが好ましいか、既に多くの企業により表記されている事項）

	Privacy Notice Highlights Template	保護法対応	備考
①	社名	◎	
②	適用範囲 ・個人情報の取り扱いについて適用される事業者の範囲及びサイトの範囲	○	
③	個人情報 ・取り扱う個人情報の種類/取得の方法/取得に関する業務	○	
④	使用 ・個人情報の利用目的 ・共有（共同利用）や取引等の第三者提供（委託等も含め）があるか	◎ ●	第三社提供や共同利用がある場合
⑤	選択肢 ・個人情報に関するアクセスや削除要求等	○	
⑥	重要情報 ・マーク付与団体等へのアクセス ・セキュリティや責任について	● ○	認定個人情報保護団体に属する場合
⑦	連絡先 ・問合せ連絡先 ・プライバシーポリシー（経営責任者の表明）へのリンク	◎ ○	

図表 4-23　Privacy Notice Highlights Template と日本の個人情報保護法で公表が求められる事項の対比

4.6.5　個人情報保護に関する Web 上の好ましい表示

Web 上において個人情報保護についての記載および画面展開がいかにあるべきかについて整理する。

まず、日本国内で「個人情報保護方針」「プライバシーポリシー」あるいは「個人情報の取扱いについて」等、混在に使用される用語を大きく①その企業の代表者（社長または担当役員等）が、その企業の個人情報保護のスタンスについて利用者・消費者に決意表明するものと②その企業の個人情報保護についての措置や事務手続き等を細かく解説する説明書に相当するものという2つに大別する。

そして、①については「個人情報保護方針」「プライバシーポリシー」「プライバシーステイトメント」と言った用語を使用し、②については「個人情報の取扱いについて」といった表現に使い分けることとする。

機能・定義	呼称例
その企業の代表者（社長または担当役員等）が、その企業の個人情報保護のスタンスについて利用者・消費者に決意表明するもの	「個人情報保護方針」 「プライバシーポリシー」 「プライバシーステイトメント」等
その企業の個人情報保護についての措置や事務手続き等を細かく解説する説明書に相当するもの	「個人情報の取扱いについて」 「お客様の個人情報のお取扱い」 等

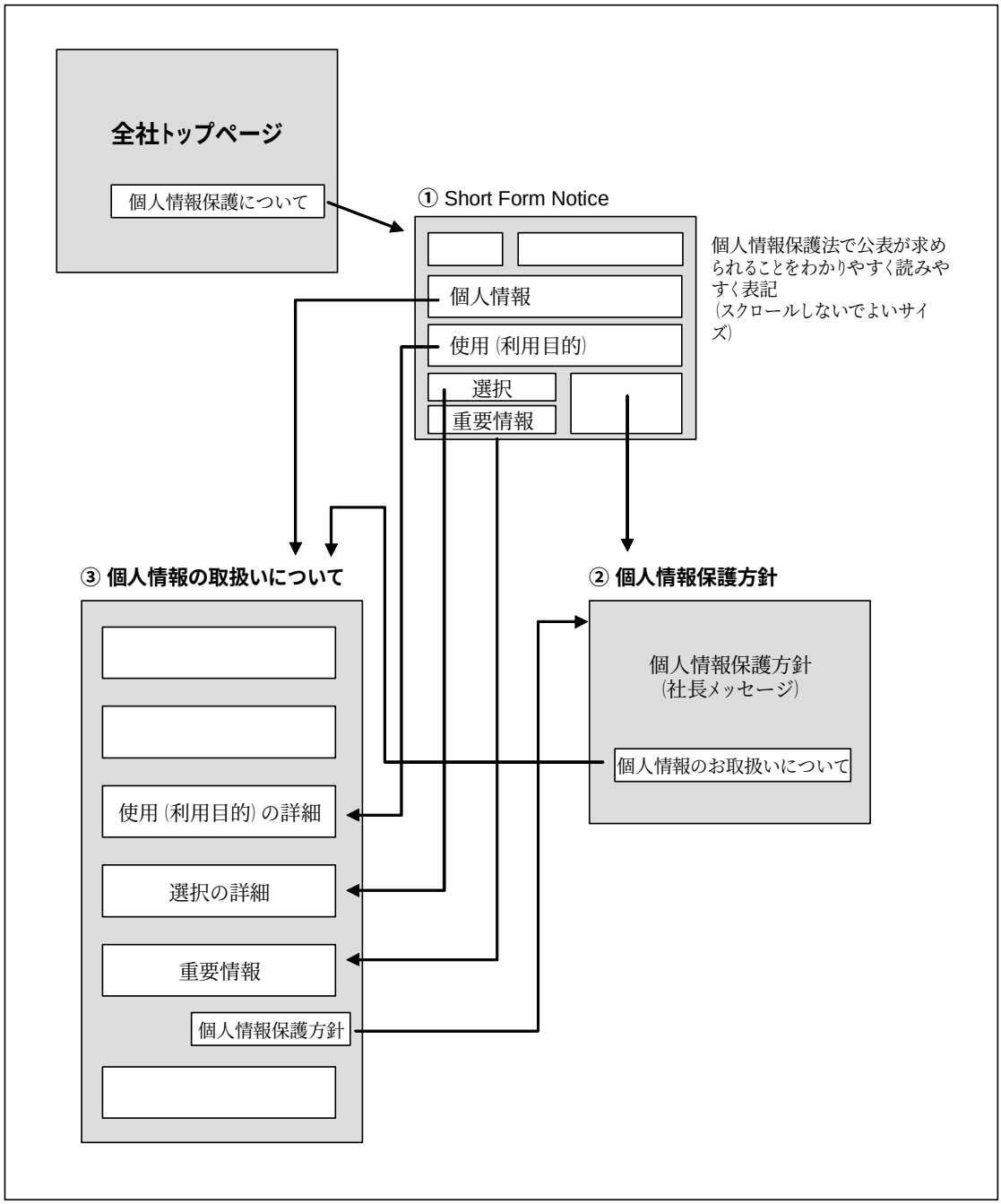
さらに、企業のポータルサイトには「プライバシーについて」「個人情報保護について」「プライバシーポリシー」などのリンクボタンを設け、まず、一番に、「Short Form Notice」のテンプレートに飛んでいくよう設定する。

「Short Form Notice」の各項目に設置されたリンクボタンよりその企業トップより表明される「プライバシーポリシー」や個人情報の取扱いに関する詳しい説明の箇所に飛ぶよう設定することで、消費者にわかりやすく自社の個人情報の取扱いを示しながら、世界の企業の個人情報保護についての流れに沿った対応が図ることができることとなる。

次項にて、以上の考え方に沿った、個人情報保護に関する Web での好ましい表示について、その全体構成及び画面展開と、「Short Form Notice」、企業の代表者の決意表明である「個人情報保護方針」とその企業の個人情報保護についての措置や事務手続き等を細かく説明する「個人情報保護の取扱いについて」の表示サンプルを示す。

4.6.6　個人情報保護に関する Web 上の好ましい表示サンプル

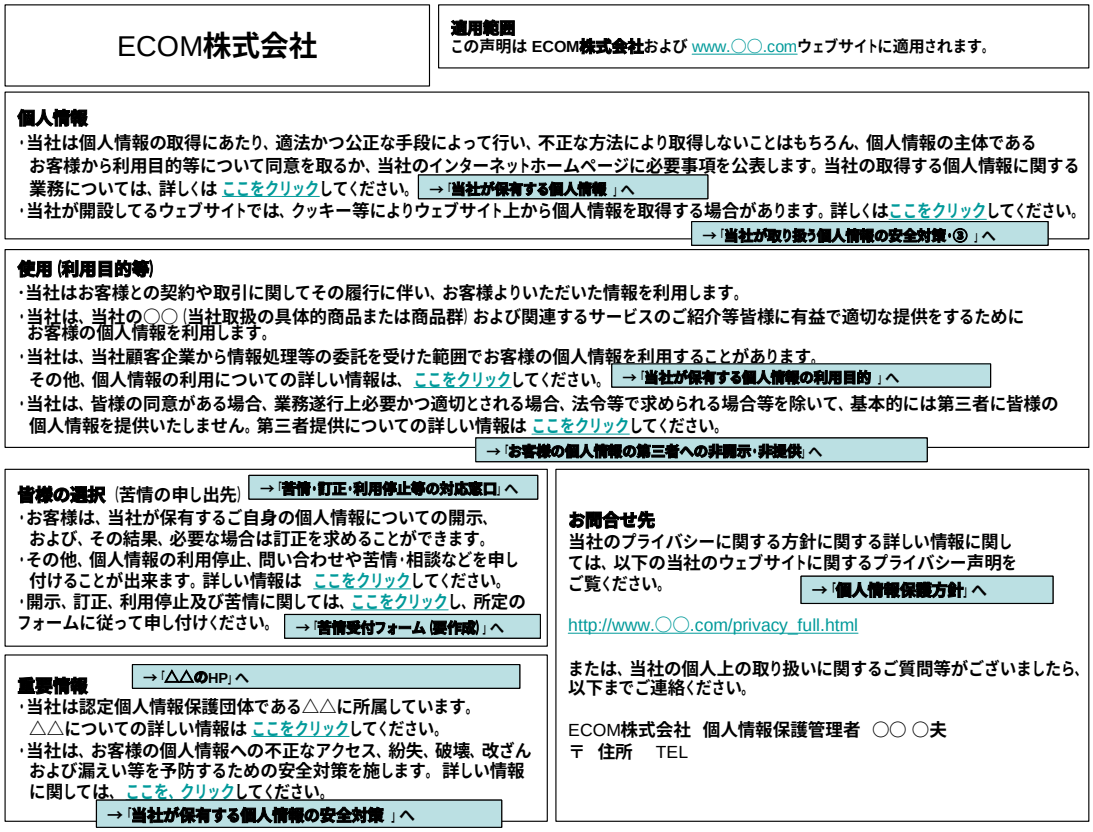
（1）全体構成・画面展開



図表 4-24

（2）個別のコンテンツ

① Short Form Notice サンプル



図表 4-25

② 個人情報保護方針（サンプル）

当社は、当社が業務上取扱う当社の顧客・取引関係者・当社従業員などの個人情報について、個人情報保護に関する法令及びその他の規範を遵守し、かつ自主的なルール及び体制を確立し、以下のとおり個人情報保護方針を定め、これを実行し継続的に見直し、改善・向上に努めることを宣言致します。

1. 当社は、この宣言を実行するために、「ECOM 株式会社　個人情報保護に関するコンプライアンス・プログラム」を策定し、当社社員等（役員・従業員・パートタイマー・アルバイト・派遣社員などを含む）、その他関係者に周知徹底させて実行し、改善・維持してまいります。
2. 当社は、個人情報の取得にあたり、適法かつ公正な手段によって行い、不正な方法により取得しないことはもちろん、個人情報の主体である本人から利用目的等について同意をとるか、当社のインターネットホームページに必要事項を公表します。
3. 当社は、個人情報を間接的に取得する場合、取得する個人情報について、提供者が本人から適正に入手したものであるかどうかを確認し、当社のインターネットホームページに必要事項を公表します。
4. 個人情報の利用は、個人情報の主体である本人から同意をとるか、当社のインターネットホームページに必要事項を公表した範囲内で、具体的な業務に応じて権限を与えた者のみが、業務上必要な限りにおいて行うものとします。

5. 当社は個人情報への不正アクセス、紛失、破壊、改ざん及び漏えい等を予防するため、合理的な安全対策を講じるとともに、必要な是正措置を講じます。
6. 当社は、業務を委託するために個人情報を委託先に預託する場合は、当該委託先との間について調査し必要な契約を締結し、その他法令上必要な措置を講じます。
7. 個人情報の主体である本人からの同意なく個人情報を第三者に提供することを原則として禁止します。
8. 当社は個人情報の本人様が自己の個人情報について、開示、訂正、利用停止、削除等の権利を有している事を確認し、これらの求めに対し遅滞なく、応じるようにします。

年　　月　　日
ECOM 株式会社
代表取締役社長　□□　□郎
個人情報保護に関するお問合せ先　@

図表 4-26

③ 個人情報の取扱いについて（サンプル）

「個人情報の取扱いについて」

○　○年○○月○○日
〒　　住所
ECOM 株式会社
個人情報保護管理者　○○　○夫

当社は、お取引に伴いお客様の個人情報をいただいております。以下に、その個人情報の取り扱いについて個人情報保護法の規定に従い説明いたします。

1. 個人情報の取り扱いに対する当社の基本姿勢
当社は、個人情報保護方針を宣言するとともに、その実行のために、「ＥＣＯＭ株式会社　個人情報保護に関するコンプライアンス・プログラム」を策定し、当社社員等（役員・従業員・パートタイマー・アルバイト・派遣社員などを含む）、その他関係者に周知徹底させて実行し、改善・維持してまいります。また、個人情報の取得にあたっては、適法かつ公正な手段によって行い、不正な方法によって取得しないことはもちろん、個人情報の主体である本人に対し個人情報を与えることの任意性及び当該情報を与えなかった場合に本人に生じる結果を通知いたします。

2. 当社が取り扱う個人情報
①当社は、当社との○○（当社取扱の具体的商品または商品群）の取引に伴い取得したお客様の個人情報を取り扱います。お客様の個人情報は、当社のデータベースに登録されます。当社のデータベースに登録されるお客様の個人情報は、お客様に交付した申込書にお客様が記入された情報、契約の履行に伴い発生する入金情報等です。
②当社は、当社の○○（当社取扱の具体的商品または商品群）および関連するサービスのご紹介のためのダイレクトメールの発送等のために、お客様の個人情報のうちご住所、ご氏名、電話番号等を当社の関係先または公開された情報より取得、利用、保有することがあります。
③当社は、当社の顧客企業から個人情報に関する情報処理等を委託され、当社の顧客企業からの指示に従い、顧客企業に返却または消去するまでの間、個人情報を取り扱うことがあります。
④上記以外のものについては、個人情報を取得するときに、その利用目的と問い合わせ先を明示します。それによって取得した個人情報を保有しています。

3. 当社が保有する個人情報の利用目的
①お客様との契約の履行、契約後の管理･〇〇･購入いただいた商品のアフターサービスの実施のために利用します。
②当社の〇〇（当社取扱の具体的商品または商品群）および関連するサービスのご紹介のためのダイレクトメールの発送等の目的に利用します。このための利用は、お客様からの申し出により取りやめます。
③当社が、当社の顧客企業から情報処理等を委託された範囲において利用します。その顧客企業名及び委託された業務の内容については当社と当社の顧客企業との間の秘密保持契約において公表することはできません。
④上記以外のものについては、個人情報を取得するときに、その利用目的と問い合わせ先を明示します。それによって取得した個人情報は、お客様に明示した利用目的の範囲を超えて個人情報を利用することはありません。

4. お客様の個人情報の第三者への非開示･非提供
お客様からご提供頂きました個人情報は下記の場合を除いては、基本的には第三者に開示または提供致しません。
①お客様の同意がある場合
②お客様または他の第三者の生命、身体又は財産の保護のために必要であって、お客様の同意が取れない場合
③法的な命令等により個人情報の開示が求められた場合

5. 当社が保有する個人情報の安全対策
①当社は個人情報への不正アクセス、紛失、破壊、改ざん及び漏えい
等を予防するため、合理的な安全対策を講じるとともに、必要な是正措置を講じます。ただし、不正なアクセスを防止する絶対的な技術が存在しないこと、その危険負担がお客様にあることをご了解いただきます。
②当社の従業員に対して個人情報保護のための教育を定期的に行います。
③ウェブサイトからの個人情報の収集
･暗号化
当社が開設しているウェブサイトから個人情報を取得するときは、暗号化（ＳＳＬ）を用いて個人情報を安全に送信していただくことができるようにいたします。
･クッキー
当社が開設しているウェブサイトでは、クッキーを使用している場合があります。クッキーとは、お客様のパソコンとウェブサイトとの間でやり取りする小さな情報ファイルのことをいいます。これは、お客様が当社の開設しているウェブサイトを再訪問されたときに役立つ情報を記憶し、ウェブサイトを最適な状態で利用していただくためにのみ使用いたします。クッキーの使用を希望されない場合は、お客様のブラウザの設定でクッキーの使用を中止することができます。その場合、一部のサービスがご利用できなくなることがございます。
･他のウェブサイトへのリンク
当社が開設しているウェブサイトでは、他のウェブサイトへのリンクを張ることがありますが、当社以外のウェブサイトにおける個人情報の取り扱いについては、当社は責任を負いません。

6. 苦情、訂正･利用停止等の対応窓口
お客様は、当社が保有するご自身の個人情報について開示を請求することができます。またその結果、必要な場合は訂正を求めることができます。その他、個人情報の利用停止、問い合わせや苦情･相談などを申し付けることが出来ます。当社では、これらを受け付けた場合、合理的な範囲で適切に対応させていただきます。また、そのためにお客様からの専用の窓口

を下記のとおり開設しています。

（個人情報保護に関するお問合せ先）
〒000-0000
東京都○○区○○町1－1－1
ECOM 株式会社　個人情報保護担当室　管理者　○○　○夫
TEL.03-0000-0000　E-Mail　○○@ecom.com

7. 15 歳以下のお客様に関する個人情報の取り扱いについて
当社では、15 歳以下のお客様の安全についても最大限の注意を払います。15 歳以下のお客様の個人情報については、必ず保護者の方の同意の下に登録していただけますようお願いいたします。

8. .認定個人情報保護団体への所属
当社は 200X年○月より、認定個人情報保護団体である△△より認可を受け、同団体に所属しています。当社の個人情報保護の取り扱いに関する△△の連絡先は以下のとおりです。

（△△　個人情報保護に関するお問合せ先）
〒000-0000
東京都△△区△△町1－1－1
△△　個人情報保護担当室
TEL.03-pppp-pppp　E-Mail　△△@××.com

図表 4-27

4.6.7　プライバシーポリシーの公表のあり方についての考察

ここでは、主に事業者における個人情報保護の取り扱いについて、消費者および利用者にいかに公表すべきかについて、Web ページ上での表記のテクニカルな手法について検討した。

その実践においては、法的リスクの回避に加え、事業者サイドからトップの声明として、或いは企業のスタンスや具体的な手続き等を消費者に告知するための情報発信という点から、誤解の生じない正確な表現であることとわかり易く読みやすいという相矛盾した要素が要件として求められる。

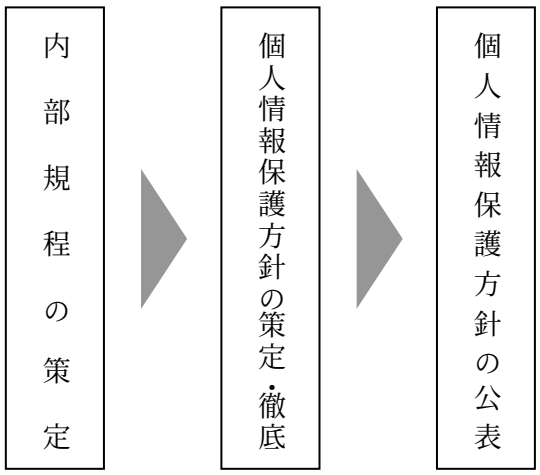
「Short Form Notice」については、そうした要件を満たすべくインターネット技術において実現できるレイヤーを利用した仕組みであり、また、消費者がそれぞれの事業者の法的に要求される事項について一定のルールに従ってトレースできる手法として、今後、さらに研究を重ねる価値があるものと考える。

しかしながら、これはあくまでも手段であって、本質的には企業の実行性がベースとなる。従って、法律をクリアしつ、企業理念に添って全社として守っていくべきものであり、

かつ、すべての現場において実行可能な社内規定を確立し、そのことを凝縮し、わかりやすい表現にしたプライバシーポリシーで無ければ意味を成さない。

ECOM 個人情報保護ガイドライン Ver.2.0 では、第 2 章において、内部規程、方針等についての規定を定めるが、その手順としては、内部規定→個人情報保護方針→個人情報保護方針の公表（パブリシティ）の手順で構築することを奨励している。

広く顧客・消費者に自社の個人情報保護のスタンスを告知していく以前に、社内にその内規と方針が浸透し、規律正しく実行されていることが重要であることを認識しなければならない。



図表 4-28　個人情報保護方針のパブリシティにいたる手順

4.7　保有個人データの開示等

従来、日本企業においては、「顧客情報は企業の営業上の重要な資産」との考えが強かったが、個人情報保護法では、顧客情報を「保有個人データ」として適切に本人が関与できる仕組みを構築するとともに、企業の資産としての顧客情報という考え方から「お客様からの預かり物」として適切に扱うことが求められる。

ECOM 個人情報保護ガイドライン Ver2.0 では、保護法と同等の開示等および苦情処理についての対応を求めている。

4.7.1　開示の求めに対する対応

本人からの開示の対応にあたっては、「事業者の資産としての顧客情報」という点と「お客様からの預かり物としての個人情報」の観点から、適切に本人に対しての対処できるとともに、成りすましの第三者にあやまって開示（漏えい）しないよう厳格な本人確認を施すことが必要となる。

まず、保有する個人データについて開示対象とする個人情報の範囲を定め、その特性により適切に開示の手続きが施されなければならない。保有個人データの開示の方法については、政令にて、「書面の交付による方法（開示の求めを行ったものが同意した方法があるときは、当該方法）」とされており、開示にあたっては、セキュリティの確保や本人の利便性および自社の業務負担等を考慮して対応することが必要である。

問い合わせや受付に対応する窓口については専門の部署を設けることが望ましいが、事業領域や活動地域が広範であったりした場合は複数の設置が必要となる場合もある。また、中小の事業者においては、そうした専任の部署を設けることは必ずしも容易ではないので、その対処については一律ではないが、少なくとも全社として統一したルールの下に、適切かつ迅速に対応できるような体制を確立することが必要である。

また、開示の求めを受け付ける時点で、本人確認（代理人を含む）の手順が適切に確実にされるよう盛り込まれることが求められる。

それらを勘案して、開示の業務フローを定めることが重要である。保護法においては、事業者の保有する個人データについて開示、訂正・追加または削除、利用の停止または消去について対応する条項が設けられ、また、その求めに応ずる手続きを定めることができるとされている。さらには、開示の対応については事業者にとって業務負担が発生するため、実費を勘案して合理的と認められる範囲で手数料を定め、徴収できるとされている。

4.7.2　開示対象となる個人情報

保護法では、本人（代理人を含む）より開示の求めがあったときには、原則として、その時点で保有する個人情報を遅滞なく開示することが義務付けられている。ただし、本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合、他の法令に違反する場合とともに、事業者の適正な業務の実施に著しい支障を及ぼす場合は、その一部または全部を開示しないことができるとされている。事業者の適正な業務の実施に著しい支障を及ぼす場合とは、評価･判定情報のように本人に開示することによりそのノウハウが明らかになってしまうような場合や本人以外の第三者の個人情報が含まれているような場合であり、その第三者と契約上の守秘義務があるものなどがこれに該当すると考えられる。そのときには、開示をしない旨を遅滞なく通知しなければならず、さらに、その理由についても説明するよう努めることが求められている。

したがって、保有個人データについて、上記のような、その一部または全部を開示しないことがある場合には、どの保有個人データについて開示を行わないかをあらかじめ決め、開示しないことについての説明ができるように備えることが望ましい。

自社の保有個人データについて、その個人情報項目の種類や性質（一般の属性情報か、アクセスや購買等の履歴情報か、事業者により付与された情報か、機微な個人情報になりうるか等）および取得の状況や経路（本人より直接取得か、間接取得か、評価情報か）等を勘案し、全社または保有管理する部門として統一した対応の手立てを考えておくことが必要である。

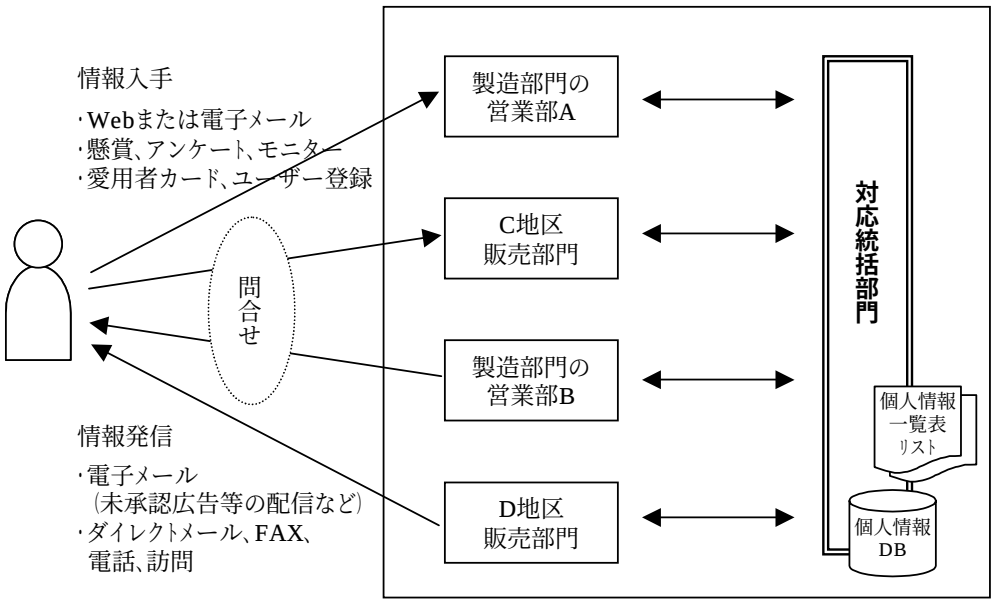
図表 4-29　保有個人データの分類

分類	情報項目
本人識別情報	氏名、生年月日（年齢）、性別、住所、郵便番号、電話番号 メールアドレス
属性情報	勤務先・所属・役職 アンケート（趣味・嗜好等） 会員番号（事業者が定めるユーザーID 含む） パスワード（本人が定めるユーザーID 含む）
履歴情報等	契約番号、契約（購入）年月日 購買履歴（商品名、金額） 利用残高、支払状況 商品モニター＊ 意見・投書＊
公開情報など	官報・高額納税者名簿・電話帳など公的機関が公表した情報

※　情報項目ごとに種類や性質（一般の属性情報か、アクセスや購買等の履歴情報か、事業者により付与された情報か、機微な個人情報になりうるか等）および取得の状況や経路（本人より直接取得か、間接取得か、評価情報か）等の観点で分類され、開示の求めに対していかに対応するかをルール化することが必要。

4.7.3　対応窓口の設定

開示等の求めおよび苦情受付に関する対応窓口を設置し、その連絡先を明らかにすることが求められる。ただし、その体制のあり方については、事業者ごとの規模や事業形態、個人データの種類や保有形態によって変わらざるを得ない。



※入手の形態や個人情報の種類により、統括部門が分散されるケースもありうる。

図 4-30　窓口対応のフォーメーション

また、顧客の問い合わせのルートも電話、ファクシミリ、ダイレクトメール（郵送）、来所（店）、電子メール（Web ページの問い合わせ画面からの入力含む）等多岐にわたり、それぞれに受け付ける部署も変わるのが通常である。

従って、顧客から開示等の求めおよび苦情が寄せられたとき、どのような情報についてどこが対応するのが適切であるかについて統括する部門が明らかであることが求められる。

一律的なあり方を示すことは困難であるが、事業領域や活動地域が広範であったりした場合は複数の設置が必要となる事業者の場合は、顧客からの問い合わせの際、迅速かつ的確に対応できるようなフォーメーションを組む必要がある。対応統括部門を定め、その窓口を登録し、一元的にリスト化し、管理することなどが効果的であると考えられる。

4.7.4 本人確認の方法

開示にあたっては、不正やなりすましにより本人以外の第三者にあやまって個人データを提供しないよう厳格な本人確認が必要である。

保護法では、事業者が開示申請者の開示等の求めに応ずる手続きを定めることができるとされており、さらに、政令にて開示の求めをするものが本人又はその代理人であることを確認する方法を定めることができることとなっている。裏返せば、本人確認の手立てが甘く、本人又は代理人でない第三者のなりすましにより保有個人データを開示したとなると結果的に個人情報を漏えいしたことになり、安全管理措置が不十分と見なされるため、適切な本人確認ルールを確立しておくことが求められる。

ECOM 会員企業アンケートにて調査した回答によると、現在の企業の本人確認の方法としては表 4-32 のケースが考えられる。それぞれに安全性の確保又はそうした手続き・業務上の課題点を有する。

しかし、一方では、開示を求めるものの要求するタイミングや方法で開示ができるかといったニーズに対するサービス性の問題もあり、直接の来店や登録した住所への郵送による対応を求めた場合、本人の求めるタイミングに間に合わない場合など、新たな苦情を発させてしまう場合もあるが、現状、その対処については、それぞれの業界及び個々の事業者にて、セキュリティ面での万全を期しつつも、本人の求めにもある程度叶うような方法を考案し、厳格に運用していくよう図る必要がある。

図 4-32　本人確認の方法と課題

N＝83 社

本人確認の方法	回答数	安全性確保及び手続き・業務上の課題
ユーザーID やパスワードによる認証	35 件	・ 本人にそれぞれの守秘徹底が必要
本人でないとわからない事項（電話番号、生年月日、記入データ等）を１つ、または複数回答いただく	34 件	・ 近親者や知人の場合成りすましの可能性あり
折り返しの電話、または届出の住所への郵送	31 件	・ 移転又は電話番号変更時の対応が煩雑
本人認証が可能なもの（免許証や保険証等のコピーなど）や押印された申し込み書類等を郵送いただく	26 件	・ 証明書のコピーや押印により、法的な意味での本人確認がなされるも、郵送による日数およびコストが掛かる ・ 機微な情報が併せて取得される場合は、管理及び廃棄の徹底を要す
当初登録のメールアドレスへの返信	21 件	・ 伝送路のセキュリティの確保
直接来店いただく	17 件	・ 本人が店頭に赴く必要あり

4.7.5　開示の業務フロー

保護法の規定をクリアしつつ、取り扱う個人情報、事業特性や規模等を考慮し、関連する業務について、開示の業務フローを確立することが望まれる。

本人または代理人より開示を求められた際、多岐にわたる顧客窓口において、対応にぶれを生じさせないようにシステマティックに受け答えられるようすべてのセクションで業務フローに従って手続きが進められなければならない。またコールセンター等においては、受付の時間により応待者が変わっても、迅速的確に対応するためにも、こうした業務フローに従い、対応履歴を残すことが必要である。

また、留意すべきポイントとしては、既に述べた本人確認に加え、保護法の政令において定められている、開示の方法として書面による交付を原則としている点である。これは、同意があれば当該方法での開示ができるとされているので、インターネット上より電子メールでの返信や Web 画面への表示により行う時には、同意を得るプロセスを設けることが必要である。

●開示の業務フロー例（二重枠が事業者の対応）

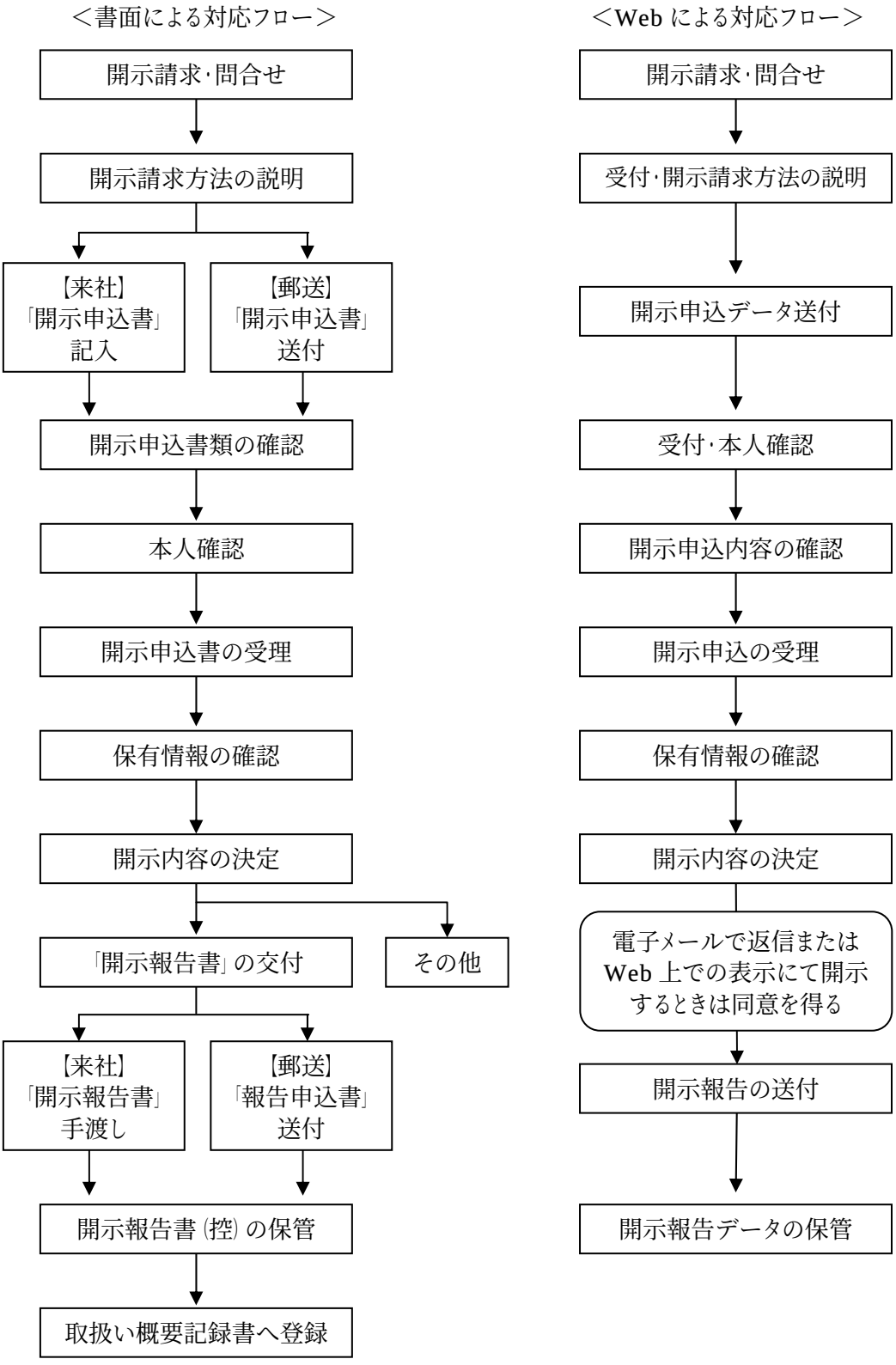


図 4-33

4.7.6　開示等に関する電子商取引上の課題

個人情報保護法では、その政令で保有個人データの開示の方法として「書面の交付による方法（開示の求めを行ったものが同意した方法があるときは、当該方法）」で行うこととされている。

原則として書面の交付をもって行うことにより、概ね万人に対して確実に開示の求めに対応でき（インターネットを利用しない人々に対しても、との意）、インターネット上での開示に関する技術的安全性の懸念を排除することができると考えられる。

また、開示の求めを受け付ける方法として、本人確認を確実にすることを含め、本人に所定の書式に記載し、押印して届出を求める方法が、現状ではより安全で確実な方法のひとつと思われる。

しかしながら、今後、日本人の個人情報についての意識が高まり、事業者が取り扱う自らの個人情報について自己の関与を求める機運が消費者の意識の中で高まるにつれ、そうした開示の求めが増えると、事業者側での処理業務も増大し、コストと効率の両面より経営的な負荷が掛かるとともに、本人も、書面による交付を受けるために店頭に行かなければならないとか、郵送されてくるのを待たなければならないために、ちょっとした問い合わせですら相当の日数や手間が掛かることを不満に思うこともあるだろう。

また、インターネットの利用が一般になりつつある現在、実際に、パスワード忘れや簡単な利用履歴等を電子メールで返信したり、Web 上で表示する方法が根付きつつあることも考えれば、そのような利用に慣れている利用者にはそうした方法による開示も本人に対する利便性や迅速性の観点から受け入れられるのではないだろうか。

ただし、当面、そのような手段での対応を図る場合には、本人確認の手段や送信路の安全に配慮し、政令に定められているように、電子メールでの返信や Web 上での表示といった方法で開示を行うことについての同意を得る等、きちんとした対策を施して行うことが求められる。

現在、日本においては自治体の公的個人認証サービスがスタートしているが、同様の個人認証の仕組みが民間においても普及し、幅広く活用できるようになれば、上記の手続きに関して極めて有効となるのではないだろうか。

5　第 25 回データ保護＆プライバシーコミッショナー会議

5.1　オーストラリア視察

5.1.1　オーストラリア渡航計画

「第 25 回データ保護＆プライバシーコミッショナー会議」は「People,Government and Business」をテーマにオーストラリア、アジア、欧米のコミッショナー・有識者による講演及びパネルディスカッションが９月１０日～１２日の３日間に亘り、シドニーにおいて開催された。また、それに先立ち８日には、メルボルンにおいては「the Body as data」と題したバイオメトリクス（生体認証）をテーマとした会議が開かれた。

さらには、データ保護＆プライバシーコミッショナー会議が終了した翌日には、アジア・環太平洋地域における新たな個人情報とプライバシーの保護のためのガイドライン策定を進めるＡＰＥＣ関連メンバーでのワークショップも開催されている。

それらの会議を中心として、オーストラリア地域における個人情報保護の状況や国際的な課題について調査するため渡航した。

5.1.2　the Body as a Data

5.1.2.1 スケジュール

日程　2003 年 9 月 8 日（月）

場所　BMW Edge, Federation Square, Melbourne

参加　オーストラリア各州・大洋州・欧米

個人情報保護コミッショナー、政府、企業個人情報保護関係者

- Keynote Address（Prof Stefano Rodotà、President Italian Data Protection Commission,Garante per La Protezione dei Dati Personali）
- Biometrics

  (Dr Lee Bygrate,Norwegian Research Centre for Computers and Law Institutt for rettsinformatikk)

  (Peter Moon,IT Special Counsel and columnist Australian Financial Review)
- Genetics

  (Prof Loane Skene, Professor of Law University of Melboune)

(Ulco van de Pol, Commissioner Dutch Data Protection Authority, College Bescherming Persoonsgegevens)

Panel of International representatives, facilitated by Paul Chadwick

Stephen Lau（Hong Kong）、Jan Willem Broekema（The Netherland）

Chris Puplick（NS W）、David Flaherty、Ken Anderson（Canada）

Alexander Dix（Germany）、Joe Meade（Ireland）、Graham Smith（UK）

- Privacy, film and culture presenration at Australian Centre for the Moving Image (ACMI)Cinema 2 on Level 2.

  (Phillip Adams, Broadcaster and commentator)

- Biometrics

  Panel of International representatives, facilitated by Paul Chadwick

  Raymond Tang （Hong Kong）、Marie Georges（France）

  Ulrich Dammann 、Hansjurgen Garstka （Germany）

  Heather Black（Canada）、Bruce Slane、Blair Stewart （New Zealand）

  Peter Harris （Guernsey）、Karel Neuwirt （Czech Republic）

- Closing address

  (Paul Chadwick, Victorian Privacy Commissoner)

5.1.2.2 遺伝子検査とプライバシー権についての議論

この会議の中で、医療現場における遺伝子に関する情報の収集について、メルボルン大学 Loane Skene 法律学教授よりプレゼンテーションがあった。

同教授は、その問題について「遺伝子に病気のある人を扱っている医者及び遺伝子カウンセラーは、彼らが責務を負っている対象は患者だけではない。彼らは一様に『我々は今、患者個人ではなく家族も治療している』と言う。プライバシーに関する法律は、このことを考慮に入れるべきである。連邦政府レベルでは、プライバシー委員会が公共利益決定にならってさらにつっこんだ公共利益決定を出すことを検討し、州のプライバシー担当者は、州法の下でのガイドラインという先例に基づくだろう。新しい公共利益決定は、医者以外の医療専門家にまで範囲を広げ、遺伝子データバンクおよび登録機関などのそのほかのデータ保存の側面も考慮すべきである。ひとつの目的は、患者や家族の医療のみに使用することを基本にして、家族を治療する医療専門家の間で家系（であるが個人ではない）遺伝

子情報の共有を認めることである。遺伝子試験のために保存された細胞へのアクセスに関するその他の問題は、本報告書の範囲を超えているが、同じようなラインに沿って規制されるべきである。」と結論を述べた。

そして、翌日の現地紙 Herald Sun には、以下のようなコメントが報じられた。

危険にさらされる患者のプライバシー（Paula Beauchamp）

現在提案されているプライバシー法改正案のもとで、医者は、患者の意思に反して親類に患者の秘密、すなわちその診察内容を明らかにすることができるだろう。

医療関係者および医者は、遺伝子が重大な危機にさらされている血縁者を突き止めることができるようになる。

オーストラリア法改正委員会のブライアン・オペスキン委員は、この法改正が医者と患者の関係の守秘義務を無視するものだと認めた。「医者は、患者の秘密を守ることを最優先にしなければならないと常に言われてきました。」と、同氏は言う。「我々は、そのほかの利益が優先される例外的状況があると言っているのです。」

オペスキン氏は、それが診断内容についての患者のプライバシーと、いくつかのケースにおける血縁者の生命との間のバランスをとるための法律だと言う。この法改正によって影響を受ける遺伝性疾患は、遺伝性腸癌といくつかのタイプの乳癌である。

問題は、患者が家族と不和な状態にある、またはプライバシーについて深刻な心配事をもっているときに生じる可能性がある。

メルボルン大学の法律学教授である Loane Skene 氏は、昨日メルボルン市で行われた「the Body as data」会議で、医者は遺伝性疾患を持っている患者の血縁者に対する義務を認識していると述べた。「彼らは一般的にこう言います。我々は今、患者個人ではなく家族を治療しているのだ、と。そしてプライバシーに関する法律はこのことを考慮に入れる必要があるのです。」と彼女は語った。「最初に遺伝子の病気があることがわかった人は、家族の中の他の人にその情報を開示しないという権利を持つべきではないのです。」

いくつかの遺伝子試験医療は個人よりむしろ家族のためにファイルを保存している、と彼女は言う。しかし、AMA ビクトリア州のサム・リーズ氏は、患者と医者の関係におけるプライバシーは生命にかかわることだと言う。「それは不可侵のものです。今後、より多くの情報に基づいた議論が行われるまで、プライバシーは不可侵であるというのが我々のとる立場です。」と同氏は語る。

ビクトリア州遺伝子医療サービスのアグネス・バリカイア氏は、遺伝性疾患をもつ大多数の患者

は、情報を喜んで共有するだろうと語った。

5.1.3 第 25 回データ保護＆プライバシーコミッショナー会議

2003 年 9 月 10 日～12 日の日程にて、シドニー・コンベンションセンターにて「第 25 回データ保護＆プライバシーコミッショナー会議」が開催された。世界 35 カ国より、約 400 名の個人情報保護関連の行政担当、学識者、民間企業の担当者が集まり、関連する国際的な課題や先端的な問題点等について報告と議論がなされた。

以下にその概要を掲載する。（プログラムおよびコミッショナー宣言については、財団法人金融情報システムセンター・金融情報システム平成 16 年冬号「個人情報保護およびプライバシー保護に関する海外動向」より引用）

5.1.3.1 プログラム

日程　2003 年 9 月 10 日（水）～12 日（金）

場所　オーストラリア　シドニー・コンベンションセンター

参加　個人情報保護コミッショナー、政府、企業個人情報保護関係者

（1 日目）

Opening Session

＜司会者＞

- Mr Malcolm Crompton（Commissioner, Office of the Federal Privacy Commissioner, Australia）

＜講演者＞

- Prof Fiona Stanley AC（Australian of the Year, Chief Executive Officer, Australian Research Alliance for Children and Youth, Australia）

Regulating Privacy:What Others Are Doing**「プライバシー規制：他国の状況」**

＜司会者＞

- Prof Stefano Rodatá（President, Data Protection Commission, Italy）

＜講演者＞

- Mr Raymond Tang（Privacy Commissioner for Personal Data, Hong Kong）
- Prof Allan Fels AO（Dean of the Australia and New Zealand School of

Government, Australia）

Building Community Trust:：A Practical Perspective**「地域社会信託の構築：実践的展望」**

＜司会者＞

- Dr Josè Luis Piñar Mañas（Spanish Data Protection Commission, Spain）

＜講演者＞

- Mr Jeroen Terstegge（Legal Counsel Privacy and Data Protection Law, Philips International, The Netherlands）
- Mr Michael Mitchell（Chief IT Architect and Planner, Qantas, Australia）

Privacy Laws：Practical Effect on Global Business and Consumer

「プライバシー法：グローバルビジネスと消費者に与える現実的影響」

＜司会者＞

- Mr Reijo Aarnio（Data Protection Ombudsman, Finland）

＜講演者＞

- Mrs Pamela W.S. Chan（Chief Executive of the Hong Kong Consumer Council）
- Mr John Mendoza（Chief Executive, Australian Sports Drug Agency, Australia）
- Madame Ariane Mole（Partner Cabinet Alain Bensoussan, France）

People：Organizational Structures and Incentives to Support Privacy

「人々：プライバシー保護の為の組織構造と奨励策」

＜司会者＞

- Mr Orson Swindle（Commissioner, Federal Trade Commission, United State of America）

＜講演者＞

- Mr W. Peter Cullen（Chief Privacy Strategist, Microsoft Corporation, formerly Corporate Privacy Officer, Royal Bank of Canada （RBC） Financial Group, Canada）
- Ms Anna Fielder（Director, Office for Developed and Transition Economies, Consumers International, United Kingdom）

- Ms Barbara Lawler（ Chief Privacy Officer, Hewlett Packard, United States of America）

Technology：Supporting a Culture of Privacy in Your Organization

「技術：組織におけるプライバシー保護の文化を支えるもの」

＜司会者＞

- Mr Mozelle Thompson（Commissioner, Federal Trade Commission, United States of America）

＜講演者＞

- Dr Brian Richards（Chief Information Officer, Health Insurance Commission, Australia）
- Mr Charles Britton（Senior Policy Officer, IT and Communications, Australian Consumers’ Association, Australia）
- Ms Harriet P. Pearson（ Vice President, Workforce Effectiveness & Chief Privacy Officer IBM Corporation, United States of America）

（2 日目）

A Safe and Open Society **「安全で開かれた社会」**

＜司会者＞

- Mr Michel Gentot（President, Commission Nationale de’Informatique et des Libertès, France）

＜講演者＞

- The Hon. Nuala O’Connor Kelly（Chief Privacy Officer, Department of Homeland Security, United States of America）
- Mr Cédric Laurant（ Policy Counsel, Electronic Privacy Information Center, United States of America）

Legal Issues：Open Justice, Forgiveness, Compassion, Context, Proportionality

「法的問題：公開裁判、免責、同情、前後関係、均衡」

＜司会者＞

- Mr Paul Chadwick（Commissioner, Office of the Victorian Privacy Commissioner, Australia）

＜講演者＞

- Prof　Marcia Neave AO（Law Reform Commissioner, Victorian Law Reform Commission, Australia）
- Prof Dennis Pearce（Emertice Professor, Australian National University, former Chairman, Australian Press Council, Australia）
- Prof Iain Currie（University of Witwatersrand, Johannesburg）

Law Enforcement with Respect **「敬意を払った法の執行」**

＜司会者＞

- Mr Peter Shoyer（Information Commissioner, Office of the Information Commissioner of the Northern Territory, Australia）

＜講演者＞

- Mr Jonathan Symmonds（General Manager, Federal Government Solutions, Teradata Division, Australia）
- Mr Cameron Murphy（President, NSW Council for Civil Liberties,　Australia）
- Ms Florence Audubert（Attachée Juridique, Interpol, France）

A Safe and Open Society：The Role of Privacy Regulators

「安全で開かれた社会：プライバシー保護監督機関の役割」

＜司会者＞

- Mr Paul Thomas（President,　Commission de la Protection de la vie Privèe, Belgium）

＜講演者＞

- Mr Joseph Meade（Data Protection Commissioner, Ireland）
- Prof Graham Greenleaf（University of New South Wales, Australia）
- Mr Colin Auditorium（NSW Police, Australia）

Identity and Privacy：Who Wants to Know and Why

「アイデンティティーとプライバシー：誰がなぜ知りたがるのか」

＜司会者＞

- Dr Hyu-Bong Chung（Secretary-General, Personal Information Dispute Mediation Committee, Korea Information Security Agency, Korea）

＜講演者＞

- Ms Carol Coye Benson（Partner, Glenbrook Partners, United States of America）
- Mr Tim Dixon（Consultant, Baker & McKenzie, Australia）
- Ms Jennie Granger（Second Commissioner, Australia Taxation Office, Australia）

Communicating Important Privacy Information-issues, and Recent Initiatives Aimed at Doing This More Effectively

「重要なプライバシー情報の流通の問題とより効果的な流通を求める最近の論調」

＜司会者＞

- Dr Alexander Dix（Data Protection and Access to Information Commission, Brandenburg, Germany）

＜講演者＞

- Mr Marty Abrams（Hunton & Williams, United States of America）
- Mr Rigo Wenning（W3C/ERCIM, France）
- Ms Dale Skivington（Eastman Kodak Company, United States of America）
- Mr Cèdric Laurant（Electronic Privacy Information Center, United States of America）

Is My Privacy the Same as Your Privacy？ **「私のプライバシーはあなたのと同じ？」**

＜司会者＞

- Mr Stephen Lau（Chaiman, EDS Hong Kong）

＜講演者＞

- Ms Dawn Casey（Director, National Museum of Australia, Australia）
- Prof David Weisbrot（President, Australian Law Reform Commission, Australia）
- Ms Sally Sinclair（Chief Executive Officer, National Employment Services

Association, Australia）

Identity：Now You See It ； Now You Don’t

「アイデンティティー：自分が認識していることとそうでないこと」

＜司会者＞

- Mrs Singrún Johannesdottir（Privacy and Data Protection Authority, Iceland）

＜講演者＞

- Mr Ken Anderson（Director of Legal Services, Information and Privacy Commissioner of Ontario, Canada）
- Dr John Joseph Borking（Director of Borking Consultancy, The Netherlands）
- Mr John Grimes（Director, Strategic Development, Argus Solutions, Australia）

（3 日目）

Key Note Address

＜司会者＞

- Mr Malcolm Crompton（Commissioner, Office of the Federal Privacy Commissioner, Australia）

＜講演者＞

- The Hon. Darly Williams AM QC MP（Commonwealth Attorney-General, Australia）

Taking Privacy to the People 「プライバシーを本人の手元に」

5.1.3.2 コミッショナー宣言

決議事項

プライバシーコミッショナーのみで行う特別会議を通じて、今回は、以下の 4 つの事柄について決議が行われた。

その 1 つめとしては、公共・民間機関が、自機関の個人情報の取扱い方法などを本人に分かりやすい方法で通知し、本人の自己情報の取り扱われ方や自己の権利等についての理解向上を図ることが重要であるということである。そして、その手段として、「世界共通の要約書式」の開発・使用が奨励されている。この要約書式の内容や構成については、現

在検討が重ねられているところであるが、EU、米国、P3P 作業部会などで実際にモデル作りが試みられている。

この決議は、各国の法律では、「プライバシーを保護する上で最も重要なのは、本人が自己情報をコントロールできる権利を有していることを自ら認識する点である」としているにもかかわらず、現実には、自己情報の取り扱われ方や登録されている自己情報へのアクセス方法が、非常にわかりづらい状況であることを問題視しての対応であるといえる。

なお、この点をめぐる具体的な対応は、将来にわたってコミッショナー会議の検討課題になるとして今後の成果が期待されている。

2 つめとして、旅客データの移転に関する決議が行われ、テロ活動や組織犯罪に対する過度な防止策が、プライバシー保護を脅かす危険性があることに対する注意が喚起された。

また、3 つめには、国連のような国際的・超国家的組織に対しては、今後、国際基準に即したプライバシー原則の遵守や、組織が有する個人データについての適切な取扱基準の策定、独立した運営機関の設立等を求めていく旨、合意された。また、会議は、今回の主催国であるオーストラリアに対し、これらの国際機関に対して積極的に働きかけを行っていくことを要請し、その取組み結果は次回の会議で報告される予定になっている。

そして、4 つめに、ソフトウェアのオンライン自動更新に関する決議が行われ、オンライン上で個人情報を自動収集する機能が組み込まれたソフトウェアを開発する業者に対して、本人のプライバシー保護を考慮した開発、利用を呼びかけることが決定された。

5.1.3.3 データ保護及びプライバシー情報の取扱いについてのより良い伝達に関する決議

本年度の調査の主要なテーマである「Short Form Notice」に関連する決議として、上記のコミッショナー宣言のひとつである「データ保護及びプライバシー情報の取扱いについてのより良い伝達に関する決議」について、以下にさらに詳しい訳文を掲載する。

提案者：オーストラリア、プライバシー監督官

協賛：

- データ保護と情報アクセスに関する委員会 [独ブランデンブルク]
  (Commissioner for Data Protection and Access to Information, Brandenderg,Germani;)

- 情報技術と諸自由に関する国家委員会 [フランス]
  (Commission National de l'Indormatique et des Libertes,France)
- データ保護委員会 [チェコ共和国]
  (Date Protection Commissioner,Czech Republic;)
- データ保護委員会 [ギリシャ]
  (Hellenic Data Protection Authority,)
- プライバシー保護研究所 [独シュレースヴィヒ=ホルシュタイン州]
  (Independent Centre for Privacy,Schleswig-Holstein,)
- 国立データ保護視察団 [リトアニア共和国]
  (State Data Protection Inspectorate, Republic of Lithuania,)
- オランダデータ保護機関
  (Dutch Data Protection Authority)

決議

プライバシー及びデータ保護委員会第 25 回国際会議では、以下の決議を行います。

1. 本会議では、政府企業及び民間企業の双方に向けて、以下の重要性に対する注意を呼びかけます。
   - 個人情報の取扱ならびに加工方法について、情報公開を一層推進すること
   - 上記の推進にあたり、グローバルな一貫性を維持すること

   それにより
   - 人々に対し、自分の個人情報に対する権利と選択、及びそれに働きかける能力がある点について、一層の理解と認識をはかること
   - 上記の認識が高められた結果、企業における情報の取扱ならびに加工方法が向上・公正化するよう、インセンティブを設けること。
2. 本会議では、上記目標達成のため、以下の方法を支持します。
   - プライバシー情報の概要の簡潔な伝達を目的とした世界共通のフォーマットを作成し、あらゆる企業に使用してもらうこと。内容は以下の通りとする。
     ・ 個人に最も知らされるべき情報
     ・ 個人が最も知りたい可能性のある情報
   - 明快で直接的、かつ曖昧さを排した表現を使用すること

- 情報入手源となったサイトまたはフォームと同じ言語を使用すること
- 上記フォーマットは、限られた要素によって構成すること。また上記に従い、プライバシー保護に関する次の原則を示すこと。
  - 個人情報の収集主体、及びその連絡先(企業の正式名称及び物理的な所在地を示す)
  - その企業が収集している個人情報の種類、また収集手段
  - 企業が当該個人情報を収集する目的
  - 収集された個人情報が他の企業に提供されるか。提供される場合は、提供先の企業名とその目的。
  - 本人がプライバシーに関して持っている選択肢、またそれらを簡単に行使する方法。特に、法に沿った方法で無関係な第三者に個人情報を開示することに関する選択肢。また特定のサービスを受ける場合に個人が開示すべき情報の種類に関する選択肢。
  - 本人の個人情報へのアクセス、修正、ブロック、削除に関する権利の概要。
  - 提供された個人情報の検証を依頼できる独立監視団体についての情報。
- 個人が以下をはじめとする詳細情報を手軽に検索できるよう、適切な手段を導入すること。
  - 企業による情報へのアクセス、修正、ブロック、削除に関する、法で定められた条件。また法で定められた、個人情報の保存期間。
  - 縮約版に記載された説明の完全版。
  - 企業がどのように情報を取り扱い、加工するかに関するステートメントの全文。

3. 本会議は、上記の縮約化された標準的フォーマットは関連するすべての国内法に適合すること、また必要に応じてその企業が個人に提供することが法的に定められている通知とともに提供され、しかもその通知と矛盾しないことに同意します。
4. 本会議は、データ保護とプライバシーに関する個人への情報提供のタイミングの重要性を認識しています。例えば、どういった種類の個人情報を提供するか、あるいは第三者に自分の個人情報を提供してよいかどうかを選択する時点で、データ保護とプライバシーに関する情報を自動的に示すことはきわめて望ましいと考えます。あるいはまた、分かりやすいリンクを提示し、クリックすることでデータ保護とプライバシーに関する情報を読めるようにすることが適切な場合もあります。本会議は、EU の第

29 条データ保護作業部会が「ヨーロッパ連合におけるオンラインデータ収集に関する最低要件に関する提言(2001 年 2 月)Recommendation 2/2001 on certain minimum requirements for collecting personal data on_line in the European Union」において示した、データ保護及びプライバシーに関する情報の自動提供について行った重要な仕事を十分に認識しています。

5. (オフライン・オンラインの両環境における)縮約版の提示時期については、当委員会が今後さらに検討を進めるべき重点分野であると本会議では考えています。
6. また、プライバシーポリシー記述用のコンピュータ言語の開発といった関連活動についても、本会議は十分に認識しています。これにより、プライバシーポリシーの標準化・簡略化がより一層推進されます。
7. 本会議は上記を、企業がプライバシーに関する情報(個人情報の取扱方法や加工方法)のより効果的な伝達の実現のための第一段階であると考えています。この分野における改革を認識し、企業・個人間の伝達を改善するイニシアチブについては、本会議はこれを積極的に推進します。そのような試みに着手する企業や関連団体とは協力していきたいと考えるとともに、今後の会議でも企業・個人間の伝達を高めるべく、さまざまな対策を講じたいと考えています。

データ保護及びプライバシー情報の取扱方法のより良い伝達に関する決議案：補足説明

この決議は、政府企業・民間企業における個人情報の取扱方法ならびに加工方法に関する情報を、より効果的に伝達する必要性について合意に達することを目的とする。

本決議の重要性

プライバシー法またはそれに類する法律は、すでに相当数の国で導入されており、個人情報を収集する企業またはその他の企業に対し、プライバシー保護活動の情報を消費者に提供することを義務付けている。こうした法律は、自分の個人情報が企業によってどう使われるのかについて十分な情報を人々に提供することで、プライバシーの保護を目指している。それにより人々は自分の個人情報に関する選択権を持つとともに、個人情報の自己管理が可能となる。

本決議の重要性は、企業が膨大な量の文書及び情報を提供しているにもかかわらず、企業はプライバシー対策の情報を、企業に関わる人に対して十分に提供していないという事

実の顕在化が背景にある(一例として、ペンシルバニア州立大学アネンバーグ公共政策センターによる「アメリカ人とオンライン上のプライバシー：システムは崩壊した」Americans and Online Privacy: The system is Broken http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/new.html 参照)。また個人が関わりを持つサイトを信頼するには、必要な情報を必要な時に入手できるようにする必要があるが、そのような状態にはまだ達していないという事実ある(一例として、ヨーロッパ連合におけるオンラインデータ収集に関する最低要件に関する提言(2001 年 2 月)Recommendation 2/2001 on certain minimum requirements for collecting personal data on_line in the European Union http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm)。前述のアネンバーグ公共政策センターの研究では、人は企業のプライバシー対策に関する情報を探すための時間や手間をほとんど費やさないことも、あわせて示されている。

さらに今後の課題としては、自分の個人情報を保有している企業がグローバル展開を開始した時に、その旨を企業から伝えられ、個人が選択権を行使するということもあげられる。例えば、ヨーロッパ共同体(EC)による「Report on the transposition of Directive 95/46/EC」のアクション 6「情報関連条項のさらなる整合化 More harmonized information provisions」では、個人への通知にあたっての整合性向上を呼びかけている。

(http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm 参照)

本決議の目標

現在、企業から個人に対する重要情報の伝達方法を改善するために、数多くの研究が進行中である。特に食品表示については研究が盛んである(James R. Bettman, John Payne and Richard Staelin, ‘ Cognitive Considerations in Effective Labels for Presenting Risk Information ’ , Journal of Public Policy & Marketing, Vol 5, 1986, p.1-28 などを参照)。しかし、同時に企業が保有する個人情報の取り扱い方をより効果的に伝えるには何をすればよいか、といったことに関する研究も進められている。EU 第 29 条データ保護作業部会では 2003 年の作業プログラムにおいて、通知方法の簡略化に取り組んでいる。(http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm 参照)。また米国や(http://www.ftc.gov/bcp/workshops/glb/index.html) P3P ユーザ

ー・エージェント・タスクフォース(http://www.w3.org/P3P/2003/p3p-translation.htm)も、通知方法の改善に取り組んでいる。

これらの研究の結果、オンライン／オフライン環境における伝達方法を改善するための第一歩として、以下が必要であることが明らかとなった。

- 現在よりも短いフォーマットを使用して、情報を伝達すること。これは少数の要素から構成される(一部研究によると 6〜7 要素)
- 個人が知りたいと思う、また知る必要のある、最低限の基本情報だけを含むものであること。
- 標準化をはかること。それにより、フォーマットになじんでもらうとともに、フォーマットの知識やそれらを比較する能力の育成をはかる
- より明快な表現を使用し、法律的な言い回しを排すること。日常的な表現の使用。
- 詳細情報に簡単にアクセスできること

本決議では、伝達方法の改善策の重要な第一歩として、上記があげられている。ただし、本決議ではカバーできないが他にも重要な要素はいくつかある。

次のステップとして重要なのは、適切なタイミングで企業の情報取扱方法についての詳細を開示することであろう。前出の EU 第 29 条データ保護作業部会「ヨーロッパ連合におけるオンラインデータ収集に関する最低要件に関する提言(2001 年 2 月)Recommendation 2/2001 on certain minimum requirements for collecting personal data on line in the European Union」では、この分野に関する(特にオンライン環境についての)研究が進行中である

(http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm 参照)。実は適切な情報を適切なタイミングで提供するのは、かなりり困難なことである。その理由としては、個人が企業と接触するためにどのメディアを使用しているかによって、適切なタイミングは異なる可能性があることなどがあげられる。このため当分野は今後、データ保護やプライバシーに関する諸委員会の検討課題とすることを、当決議では提案している。

企業がプライバシー対策の伝達方法を改善することは、主に個人にとってプラスとなるが、企業にとっても利点はある。例えば、顧客忠実度や信頼性が向上することで、顧客とよりよい関係を構築できる、あるいは標準化されたフォーマットを世界共通で使用することで、規模の経済からくるメリットを活用できる、といった点などがあげられる。

草案作成

オーストラリア連邦プライバシー監督事務局では、個人情報の取扱方法に関する情報を企業が適切に伝えていないという問題は、世界的に存在する可能性があるとの認識のもと、データ保護及びプライバシーに関する公認監督官に対し、この問題が重要だと思うか、そしてデータ保護及びプライバシー委員会第 25 回国際会議 (http://www.privacyconference2003.org/)での決議として適切な議題であると思うかどうか、E メールで質問を行った。続いて、この問題をさらに詳細に説明した E メールを送付した結果、回答を寄せた委員 27 名中 18 名がその問題は重要だと答えた。これを受けて事務局では、ブランデンブルク、チェコ、フランス、ギリシャ、香港、イタリア、リトアニア、オランダ、ポーランド、イギリスから委員を招いて作業部会を設け、決議案の草案作成に乗り出した。この草案は本文書と共に回覧されている次第である。

会議に先立ち、豪連邦プライバシー監督事務局ではサイトを作成し、バックグラウンド情報を掲載した。これらの情報は、企業のプライバシー取扱方法をよりよく伝えるためにはどうすればよいかに関する議論について、理解を深めることを目的としている。

http://www.privacyconference2003.org/resolution.asp.

データ保護委員会第 25 回国際会議では、決議に向けて委員による正式な議論が行われるのに先立ち、ワークショップ型セッションで話し合いの場が持たれる。セッションには参加登録者なら自由に参加できる。

決議内容のポイント

本決議では、企業が、通知について法の定める条件に従うことが前提条件となっている。決議で提案される、標準化された縮約版のフォーマットは、こうした法的条件に追加されるものである(企業がさらに情報を追加する必要のない場合、これは関係ない)。

企業は情報の取り扱い方も改善しなければならない、あるいは企業に適用されるプライバシー法は強化されるべきだとの意見もあるだろうが、これらは非常に大きな問題であり、一度の決議で扱いきれるものではない。むしろ今回の決議では、小さいが確実に達成できる第一歩を踏み出すことに重きをおいている。その第一歩とはすなわち、企業が現在行っている、プライバシーの取扱方法に関する情報を、効果的に伝達していくためのものである。今回は伝達方法に関する問題だけに絞り、プライバシーの取扱方法に(理由はともあれ)改善が必要かどうかという、より複雑な問題とは切り離して扱うことにした。もちろん、

企業が伝達していく取扱方法というものは、適用されるすべての法律に沿うべきであることは言うまでもない。

縮約版の提供目的は、人々がプライバシー情報のうち最も重要なものだけでも目を通して理解する確率を、大幅に向上させることにある。実現すれば、企業の提供するプライバシー情報を読みも理解もしない人が多いと思われる現状からは、大きな実質的進歩となるであろう。従って決議では、プライバシー情報取扱方法について、作業部会が定めたいくつかの構成要素を含めることが最も重要であるとしている。これは作業部会のこれまでの研究調査に基づく結論であるが、もちろん重要な要素はこれ以外にもある。しかしながら、これらを縮約版に含めると長くなりすぎ、効果的な伝達という目的からは逸脱してしまう。このジレンマを解決するため、決議では、個人が詳細情報(企業が提供するよう法によって定められたすべての情報)を簡単に見つけ出せるような手段を講じるよう、企業に求めることにしている。

この縮約版が世界標準となり、あらゆる企業で共通化されるとしたら、掲載できる情報の種類には制限が出てくる。例えば、アクセス権に関する法律は国によって異なる。個人が国ごとに有する可能性のある権利を縮約版においてすべて列挙するとなると、膨大な情報量になってしまう。そこで本会議では、縮約版においてはアクセス権の要約のみを提供し、詳細情報を見つけ出す方法を別途提供するよう、企業に求めている。

縮約版に含まれる情報については、それが企業のプライバシーの取扱方法について個人に誤解を与えることのないよう、十分に注意する必要がある。このため決議には、縮約版は関連するすべての法に適合すること、そしてここでいう法には、企業が誤解や錯覚につながるような行為を禁じるものも含まれるとの内容が盛り込まれている。企業が十分に注意を払うことで、その企業のプライバシーの取り扱いについての正しいイメージを読む人に伝えられるよう、縮約版を構成することは可能である。また決議では、個人の権利が侵害された可能性がある場合に訴えるための、独立した監視団体に関する情報を、縮約版に記載することも提案している。

最後に作業部会は、この決議が採択された後も作業は終わらないとしている。決議の最終パラグラフでは監督委員会に対し、企業によるプライバシー情報伝達の改善に取り組むすべての関係者と協力しながら、決議で採択された内容を実際に行い、それにより次なる対策を講じていくべきだと述べている。

5.1.4　APEC プライバシー・ワークショップ

5.1.4.1 ワークショップ開催趣旨

本会議の趣旨は以下のとおりである。

APEC 電子商取引推進協議会（ECSG）にて、APEC 経済地域内における電子商取引への信頼を高める作業計画の一環として APEC プライバシー原則および実施メカニズムの策定プロジェクトに着手している。そこでは、APEC におけるプライバシー保護の取組みは域内のその実践と経済的利益の地位間バランスを調和させることを目的に進められている。

国際的な個人データの流通については、1980 年の OECD8 原則があり、加盟国の多くは、この原則を基とし、それぞれの個人情報保護に関する法律を制定している。また、1995 年の EU 指令は、OECD8 原則を組み込んでおり、かなりの影響力を持っているが、いずれの文書も APEC の目的にとって十分であるとはいえないが、同協議会は、OECD ガイドラインを APEC 経済に沿ったプライバシー原則をつくる独自のプロジェクトの出発点であるべきということで合意した。

こういった背景を踏まえ、今回のワークショップの目的は、地域的な電子商取引または世界商取引の一部となる個人情報のプライバシー保護と関連して発生する幅広い問題点についての概要を討議することとして開催する。

5.1.4.2 パネル

上記の開催趣旨に沿って、3 つのパネルが開催された。パネラー及び主テーマは、以下のとおりである。

(1) パネル１　電子商取引についての課題

パネラー：Joe Alhadeff（Vice-President, Oracle）, Peter Ferguson（Industry Canada）, Keiya Iida（METI, Japan）, Nuala O'Connor Kelly*（Privacy Officer, US Homeland Security）, Michael Pickering（Telstra）, Raymond Tang（Hong Kong Data Protection Commissioner）

テーマ；

① 現在、どんな問題がデータ転送で生じているか、そして将来どんな問題が起こり得ると見ているか

② 国際的な苦情処理を扱うデータ保護エージェンシーの経験について

(2) パネル 2　法とその実施についての課題

パネラー：Malcolm Crompton（Australian Privacy Commissioner）, Duncan Giles（Freehills）, Professor Masao Horibe（Japan）, Chris Kuner（Hunton & Williams, Brussels）, Gary Laden（Director, BBBOnline Privacy Program）, Blair Stewart（Assistant Privacy Commissioner NZ）, Orson Swindle（Commissioner US FTC）

テーマ；

（ｃ）　今日までとられてきた強制執行（法的なものと自己規制の両方）は成功しているのか

（ｄ）　新しい国際的アプローチを作るのにどのような選択肢があるか。

(3) パネル 2　法とその実施についての課題

パネラー：Francis Aldhouse（UK Deputy Data Protection Commissioner）, PeterCoroneos（Internet Industry Association）, Dr Chung（Korean Information Security Agency）, Robert Edwards（President, Direct Marketers Association, international and Australian), Ian Gilbert（tralian Bankers' Association）

テーマ；

(e) 今日まその他のセキュリティ状況（例　空港のセキュリティ）またはその他のセキュリティ問題、プライバシー問題もしくは消費者問題（例　スパムメール）との類似点はあるか。

(f)　われわれは、詳細な国内法以上に、最善の慣行および実際的な結果をつくることに力を注ぐべきか。

5.2 Hunton & Williams 訪問

「第 25 回プライバシー＆データ保護コミッショナー会議（2003 年 9 月、ｼﾄﾞﾆｰ開催）」にて発表された簡潔かつ明確な個人情報保護方針(プライバシーポリシー)の表記（Short Form Notice）についてさらに詳しく調査するために、米国でそれについて主導的に推進する団体 Hunton & Williams を訪問し、開発の経緯や今後の推進、日本企業への紹介についての相談・確認を行った。

5.2.1 渡航主旨

個人情報保護法成立後、2003 年 12 月政令が発布され、合わせて、国民生活審議会では基本方針の策定が検討されている。その内閣の基本方針においては、個人情報取扱事業者が講ずべき個人情報の保護のための措置としてプライバシーポリシーの公表を奨励する方向で盛り込まれる見通しであるが、一方、国際的な動向として、簡潔かつ明瞭に表現する「Short Form Notice」が検討されていることについて、現時点では日本においてその知名度および認識度がきわめて低い。

「Short Form Notice」の国際的導入推進については、先の「第 25 回プライバシー＆データ保護コミッショナー会議」において決議されたが、同フォーマットの策定に取り組んでいる米国の Hunton ＆ Williams 法律事務所、プライバシー・シール・プログラムを運営する BBB-On Line 等を訪問し、ヒアリングとそれぞれの取組みの日本企業への紹介についての了解をとる。

5.2.2 Hunton & Williams との情報交換

日時　2 月 3 日（火）　15:00-17:00

場所　ダラス，Energy Plaza

参加者

Martin Abrams 氏（Hunton ＆ Williams, The Center for Information Policy Leadership, Executive Director）

Peggy Eisenhauer 氏（Hunton ＆ Williams, The Center for Information Policy Leadership, Counsel ＆ Head） Tele-conference にて

荒木吉雄氏（日本ＩＢM、ＣＰＯ）

浅沼省吾（ＥＣＯＭ）

5.2.2.1 議事

（以下、Ｈ：は Hunton & Williams 側からの発言、Ｅ：は ECOM 側からの発言）

○プライバシーポリシーに公表する事項について

Ｈ：公表事項については各国の基準を統一しなければならない。各国がいろいろなことを必要とするので、それを統一化するのが結構大変である。その作業をデータ保護コミッショナーたちと一緒に仕事を推進している。日本ではどのようなのか？

Ｅ：日本の個人情報保護法では、利用目的や会社の所在地や責任者等が、公表しなければならない事項として定められている。それはきわめてミニマムなレベルのものである。

○Hunton & Williams の推進経緯

Ｈ：現在に至るまでの経緯についてはプレゼン資料のとおり。（P149～P158 参照）プロジェクト用に最初開発したテンプレートがどういうものであったか、ショートノーティスの中にどういうインストラクションが書かれるべきか、ノーティスというものがどういうふうに表示されるべきかという検討をした。

P&G のショートフォーム、銀行・ファイナンシャル関係のものとしてのチェイスマンハッタン銀行のショートノーティス。この 2 枚をウェブサイト上に公開している。フォーカスグループリサーチのプレゼンもこちらに準備した。

Ｈ：まず、ファイナス業界でプライバシーをカバーするという法律が米国にはある(Gramm-Leach-Bliley 法)。結構新しくて、3 年前にできたものである。ノーティスはその法律に沿って作らなければならない。しかし、長過ぎる、よく解らない言語で書かれているということで評判が悪い。

従って、今、ノーティスに関して新しくルールを作り直している。

これは金融業界についてのみの話だが、ＦＴＣについては、金融業界以外のところも対象となり、e コーマスの法律にも将来は関わってくるのではないかとも言われている。

○データ保護コミッショナー会議と Hunton & Williams との関係

Ｅ：オーストラリアのデータ保護コミッショナー会議で主催のオーストラリア・コミッショナーが、この「Short Form Notice」を推進しようと提唱した。そのコミッシ

ョナー会議と Hunton & Williams との関係は？

Ｈ：2002 年の秋にオーストラリアのデータ保護コミッショナーである Malcolm Crompton 氏に、「Short Form Notice」の概念はこういうものだと紹介した。次年度、氏が主催するデータ保護コミッショナー会議の中で、「Short Form Notice」を盛り込むのは、これはとてもいいアイディアだと、これを主題のひとつにしようということになった。

そして、約 1 年前、Crompton 氏は、米国に来て、われわれのグループと会談し、たくさんの質問をした。その結果、われわれと Crompton 氏の両方でプロジェクトをスタートさせることとなった。「Short Form Notice」を開発していこうということで、オーストラリアでのデータ保護コミッショナー会議で各国のコミッショナーたちを説得できるように、チームを組んで進めた。その会議で絶対にパスさせるぞとの意気込みで。われわれは共同作業でずっとこのコンセプトづくりを推進してきた。

今は、それをさらに前進させていこうと進めている。2004 年 9 月にポーランドで次のデータ保護コミッショナー会議がある。それまでに、コミッショナー、ビジネス業界、コンシューマの代表といったグループと小会議を数多く実施できればと思っている。この 3 月にいくつか開催する。その結果を世界中のコミッショナーに報告する。ポーランドの会議では、国際的なモデルとして最適な「Short Form Notice」はこういうものである、というものができあがるようにと考えている。

○Hunton & Williams の参加企業

Ｅ：Hunton & Williams には IBM、P&G 社、シティグループ、イーストマンコダック社、ACXIOM、HP などが参加しているが、どのようにしてメンバーとして集められたのか？

Ｈ：皆さん賢くて、これが正しいことだと解っているので参加してくれている。マイクロソフトもその中の一つ。マイクロソフトは、リーダーシップグループの一員になりたいというのが目的だった。われわれがプライバシーに関する問題の解決に取り組むプロジェクトであり、そうしたテーマについての専門家たちと有力な横の人脈を持っているという理由で参加しているのではないか。

ACXIOM（顧客情報管理の大手企業）は全米のレギュレータとか、横の関係が非常にうまくいっている、アクセスがあり、力もあるということで参加している。まじめに、

いい仕事をしていきたいという思いやわれわれがやっているプロセスに共感し、その目指すところに近づけていきたいという思いで参加してくれている。

Ｅ：ヨーロッパ企業に呼び掛けたことは？

Ｈ：米国に本社を持っていない企業にもたくさん声をかけたいと考えている。ただ、残念ながら、ヨーロッパでもアジアの業界でも、アメリカが考えているようなことと同じようには考えてもらえないようだ。このようなプロジェクトを企て、政府に打診して説得しようとするまでには至っていない。それを変えていきたい。ヨーロッパの業界がどれくらい興味を持っているのか、また、日本についても、まだわからない。アジアでは香港のデータ保護コミッショナーがこのプロセスに興味を持っている。Crompton 氏は、APEC で 2 月にワークショップが開催されるが、コンシューマの教育とかについて話してくれ、その中で「Short Form Notice」の話が出ると思う。

○普及に向けての展望

Ｈ：こういうものは全世界で使えるようなものになるべきだと思うが、日本ではどうか？ 日本の企業はこうした全世界で使えるものに興味があるだろうか？

Ｅ：日本企業はこの 1 年でプライバシーポリシーを掲載しているところが増えたが、まだ 5 割ちょっとくらい。

プライバシーポリシーの内容も、今の段階ではプライバシーポリシーも他社やアメリカの掲載例に習ってとか抽象的なものとか、というレベルのものが散見される。

「Short Form Notice」については、ECOM 内の数人のメンバーでディスカッションをした時に、公表すべき事項が保護法により決まっているのだから、それを消費者により平易でわかりやすく示す手段として、非常に効果的な方法であるということでさらに調査研究をしてみようということとなった。

Ｈ：データ保護コミッショナーはそのことを理解しはじめたようだ。コンシューマはある程度のものしか見ない、ある程度のことしか理解しようとしない。しかしながら、いろんな法律があり様々な要求が成されている。すべてを満たすためには多くのことを記載しなければならなくなる。

われわれのテンプレートでは、6 つの項目がノーティスの中にあるべきだとしているが、そのことを法制上又は行政が了解しなければうまくいかない。でも、現在のプライバシーポリシーは、人々の読まれず、結果として何も知らせることにならない。

日本の企業、例えば、富士フイルムは、全世界でフイルムを販売している。だから同じようなノーティスを持つべきである。日本でも、香港でも、イタリアでも、米国においても同一のものを持つべきである。そういうことが理解され始めている。

Ｅ：ヨーロッパ、アメリカ、アジアはそれぞれ文化や歴史が違う。そこで個人情報やプライバシーについての考え方も当然異なり、法律や習慣も違う。ただ、知らせるべき（公表すべき）事項を、同じフレームのなかの同じような場所に表記し、解りやすくするというこの方法は効果的であると思える。

Ｈ：チャレンジである。そういうフォームを開発するのもチャレンジである。文化の背景、全部を入れて。

プライバシーそのものについて 3 つの定義がある。ほっといてくださいというのが 1 つ。これは非常に難しい。自分の情報をコントロールするというのが 2 つめ。3 つめは、個人が傷つかないように情報を扱うということ。

どのアプローチをとっても、情報が、個人を傷つけないように配慮し、価値あるものとして扱われることが大切である。

Ｅ：ヨーロッパの法律と比較して、日本の法律はミニマムスタンダードに留めている。

Ｈ：法律というのは最低限度のものであるべき。ヨーロッパの法律では、情報を使って何かしたくても、いろいろと制限され、禁止されている。そのため、政府に行って、お願いすることとなる。それは効率の低いやり方だと思う。

Ｅ：タフないろんな難関があると言われたが、おそらくヨーロッパが非常に大変だろうと思う。一方、日本の保護法は、法律がミニマムだが、事業者にはより高いレベル実施を期待するものである。プライバシーポリシーの公表については、まだ、どのように書いていいかわからないところもあるので、このテンプレートの項目について、各企業がそれぞれの項目について自社の実践方法やスタンスについてわかりやすく書くことで、企業、消費者の双方に有効であるのではないか。

Ｈ：米国ではそういうわけにはいかない。政府が関わってくるので大変である。コダックのプライバシーポリシーは、当初、1 ページだった。しかし、今や、6 ページ担っている。それはだめだと解りながら、現実は結局そうなってしまっている。

われわれの分析では、コンシューマは 6 アイティムまでしか理解できないとの結果が出た。各カテゴリー、アイティムの中にいろいろカテゴリーがあって、3 つか４つくらいの情報くらいしか理解しない。そして、同じスポット（場所）に同じアイテム(項

目)を探すのがコンシューマ心理だ。例えば「用途(利用目的)」というカテゴリーがあった時に、（それをテンプレートで位置を決めて表示するようにすれば）コンシューマはだいたいその場所（例えば、左の上の方とか）を探すのがコンシューマの心理である。「選択肢」であれば、それは左の下のコーナーの方とか。

あるグループのリサーチでは、コンシューマは、長いノーティスは、「あまりにも法律的に強い言語を使い過ぎている。」「企業を守るための言語、法律的なものが使われ過ぎている。それは何か都合の悪いものを隠しているのではないか。」とあまりよくないとの声がある。長ければいろいろ語れるので、いろんなことがクリアになるが、短くなったらそれなりにあまりクリアでないこともあるが。

Ｅ：そうなると以下に要約するかが難しくなってくる。

Ｈ：いいノーティスの要素は 3 つ。まず長さが 1 つ。次に、言語が理解しやすいということ。3 つめにフォームそのもの。

同じフォームを使っていても、言語が理解しづらいものであれば適切ではない。しかし、ボックスが 20 くらいあったとしたら、言語が理解しやすいものであっても、フォームが読みづらく、結果的に読まれない。

○日本の状況とレポートの承諾

Ｅ：ECOM では、プライバシーポリシーのあり方、問題点について今の日本の企業の実態を計る意味でＥＣＯＭ会員企業のホームページを目視確認してみた。日本のプライバシーポリシーの表わし方はそれほどまだ固まっていない。一方で、Hunton & Williams のテンプレートのスペックとデザインについて資料を翻訳し、仕様書として表に表わした。それを日本の個人情報保護法中の公表が求められる条文とさらに比較表にまとめた。テンプレートの 7 つの項目については、日本の法律の中で必要なのは、最低限で言えば、利用目的と、その会社がどこのどういう会社かという連絡先ぐらいかもしれないが、そのほかの項目についても、やはり公表した方がいいし、公表することはそんなに困難なことではないように思われる。

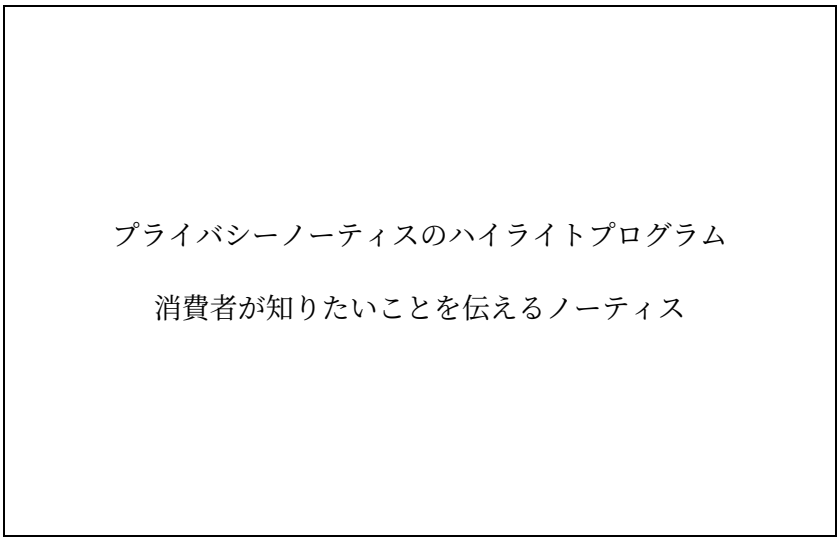
Ｈ：そのようにテンプレートとその国の法律を比較する作業は大切なことだし、われわれにとってはとても好ましいことだ。

Ｅ：また、Web ページのマップの構造として各企業のトップページから、まず、「Short Form Notice」に飛んで、さらに詳しい取り扱いや社長の個人情報保護方針にリンク

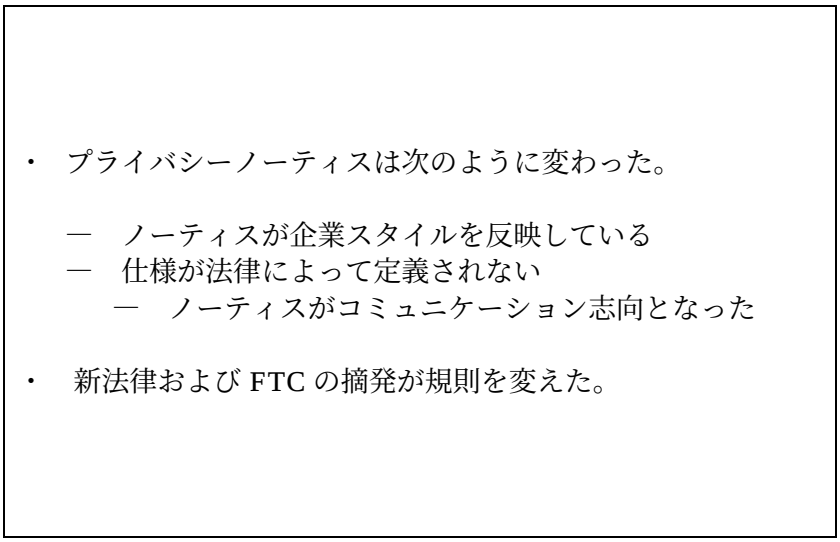
するような構造を図示する予定。そういった形のものを説明して、日本版のサンプルということで、報告書にて発表したいので、その了解をいただきたい。
H：オープンスタンダードなので、やってもらって結構だ。もし、日本でいろんなノーティスを書きはじめるようなことがあれば、それをサンプルとしてぜひこちらに送ってほしい。ほかの関連メンバーにも是非紹介したい。
H：「Short Form Notice」を使うということに対して、そういう興味があるということに対して、日本の政府とはコンタクトはあるのか？
H：われわれは経済産業省や内閣府等と折々接する機会を持っている。日本の個人情報保護法では、それぞれの業界ごとに主務官庁が行政することになっているが、そこの横串を指すのが内閣府である。われわれはその内閣府の個人情報保護推進室責任者と接点を持っている。今、内閣府が中心となり、基本方針が策定されているが、その中でプライバシーポリシーを載せることなどが盛り込まれるようだ。一度、個人情報保護推進室責任者にこの「Short Form Notice」について話をしたら、すごく関心を持った。
また、経済産業省もわれわれのディスカッションに参加してくれている。
H：全世界の政府が、この「Short Form Notice」を開発するということに関わっているので、日本もぜひお願いしたい。
Ｅ：再確認だが、紹介するにあたって、ノーティスの制限というのは、スペック以外のものについてはないか？例えば、登録や使用料とか？
H：このグループが始めたことをベースにして、皆さんが今開発しているということで特にない。そもそもこのセンターが設立されたのは、プライバシーマーケットがうまくいくように、もっともっとベターになるようにと願って設立された。それに、ビジネス業界がジョイントしているということである。従って、われわれは「Short Form Notice」をもっともっとよくしたいと願っている。
登録や使用料も必要ない。
Ｅ：有益なお話をありがとうございました。

5.2.2.2 Hunton & Willians **資料①（**Privacy Notice Highlights Program, February 2003**）**

p. 1



p. 2



p. 3

ノーティスは今や法によって操られる。

・ Gramm-Leach-Bliley 法は、金融機関が下記を満たしている旨のノーティスを与えるよう定めている。
  ― 本法が要求する内容
  ― 規則が示唆する言語

・ HIPAA プライバシー規則によって要求されるヘルスケアのプライバシーノーティスは以前より煩雑でさえある。

・ 「ノーティスは契約書であり、その言葉はそれを反映している」（Howard Beales）

p. 4

ノーティスのコンテント要件がコミュニケーションを妨げる。
・ 法的に要求されたノーティスはあまりにも煩雑である。
  ― GLB は 7 個の要素を要求している。
  ― HIPAA は 31 個の要素を要求している。

・ 消費者は、長ったらしい法律主義的なノーティスに嫌気がさしおり、「会社は何を隠しているのか？」と疑ってしまう。

・ フォーカスグループの調査は、このようなノーティスが実際に信用を損なっていることを実証している。

p. 5

ノーティスを読むかどうかの研究では・・・

・ 個人は､以下のノーティスを読解するのに困難を感じている。
  ― 7 個を超える要素またはカテゴリーをもつもの
  ― 1 カテゴリーに 4 項目以上あるもの
  ― 難解または法律主義的文言を使用したもの

・ ノーティスは以下であるべきである。
  ― 短い
  ― 平易な言葉
  ― 反復している
  ― 共通した形式

p. 6

プライバシーノーティスは以下の 2 つの目的がある。

1．消費者に以下を知らせること
　— 与えられた情報によって会社が何をするかを消費者が理解するのを助ける
　— 消費者が会社のノーティスと他企業のノーティスとを比較できるようにする

2．説明責任の手段を提供すること
　— 会社は表明していることを行う
　— 現行法及び規則にに則したものである

p. 7

解決策：階層に分けられたノーティス

・ 「プライバシーノーティスのハイライト版」
　— テンプレートに基づいている
　— 読みやすい
　— 繰り返されることによって認識を深める
　— 比較しやすくなる

・ 長い「プライバシーステートメント完全版」
　— 詳細を記載する
　— 企業手順の多様性を反映することができる
　— 説明責任のベンチマークとして役立つ

p. 8

規則は階層型ノーティスを擁護し始めている。

・ FTC の消費者関連責任者 Howard Beales は次のように言っている。

「…今日までに起こっていることは、ひとつの文書にふたつの役割をもたせようとする試みの傾向である。ひとつは情報がどのように使われるかについての会社と消費者間の両者の契約書として、そして同時に当該ポリシーを要約した説明文にしようとすることである。私はこのような機能は分割する必要があると考える。」

2002 年 5 月 13 日付け「プライバシー規則報告書」より

p. 9

階層化したノーティスの長所

・ 共通した枠組みとフォーマットは多くの製品、サービスおよび業界にとって以下のようにうまく作用する。
  — 正確
  — 理解しやすい
  — 比較しやすい
  — 難解な文章に対するような恐れを感じない

・ 現行規則に合致する
  — ノーティスのハイライト版は GLB が要求するノーティスの最上位に簡単に階層分けできる。
  — 最終的な HIPAA 規則は階層分けしたノーティスを奨励している。

p. 10

ショートノーティスプロジェクト

・ ノーティスハイライト版のモデル

・ Hunton & Williams の情報政策リーダーシップセンターのプロジェクト

・ プロジェクト参加者は以下を含む。
  BBB-Online Privacy, CITI, Double Click, ACXIOM, H&W
  Kodak, IBM, Fidelity Investments, Privacy Council
  Chase, LexisNexis UNITED STATES POSTAL SERVICE, P&G
  TRUSTe, Wellmed, US Bank

p. 11

Privacy Notice Template サンプル

p. 12

プライバシーノーティスのハイライト版
第 1&2 フェーズ

- 以下の共通した要素によって作成された。
  - 消費者にとって何が最も重要かを考慮している。
  - 消費者が知りたい、知る必要があることと直結した 6 個の要素で作成された。
- 使用言語に関する申し合わせ事項を作った
- テンプレートをベースにした設計
- フォーカスグループ調査
- 消費者とポリシー策定者の協力

p. 13

フォーカスグループの調査でわかったこと
- 当社は消費者に以下の質問を行った。
  - どの要素が重要か
  - フォーマットは重要か
- 結果は以下のように明快であった。
  - 消費者はテンプレートのやり方を望んでいる
  - 消費者は冗長なノーティスを拒絶する
  - 6 個のカテゴリーは消費者の最重要関心事をカバーしている
  - 「利用」と「提供」がカギとなる関心事であり、その他の分野は二の次である
  - 消費者は、会社が「合理的なセキュリティ」があることを説明する文章のような、明白または期待された一文を残しておくのはかまわないと思っている。

p. 14

フォーカスグループからのその他の指摘

- 消費者が好む文言および表現を以下のように指摘した
  - 例：「データ」
  - 「データはそもそも学校で子どもがグラフを作るときのもの」
  - 「企業にとってその対象はデータだが、私たちにとってそれは命（私たち自身）である」
  - 例：「ポリシー」
  - 法律用語のように見られ、不信感が沸く
  - 「会社が法律用語を使い始めると、私をペテンにかける、あるいはだまそうとしているのではないかと感じる」
- 「当社は気にかけています（we care）」という表現で美化しようと思わないこと

p. 15

フォーカスグループ参加者は圧倒的に短いノーティスを望んだ。

- 「すべてを極めて簡潔に記載する、だらだらと書かない！」
- 「残り物を入れる必要があるため、あのように長くなる」
- 「ほとんどの人は時間に限りがある」
- 「消費者は読んで理解できるものを欲している。」

p. 16

結論

- 消費者は共通したテンプレートを望んでいる。
  —「私はそっちのほうが好きだ。—（文章よりも）その方が読みやすい。」
  —「私はこれをファイルしておこう。—銀行のものは長すぎて読まなかった。」
- 共通のテンプレートは教育的であり、将来的にもっと短いノーティスさえも可能にするかも知れない

p. 17

次の段階

- 我々は、フォーカスグループの指摘に応じてテンプレートを改訂した。今後も調査および設計上の改良を続けていくつもりである。
- 我々は、必ずすべての消費者の関心事に対処していくために消費者リーダーと対話を続けていく。
- 我々は、今後もポリシー策定者に接触を続け、責任及び規制の問題について協議を始める。
- 我々は、テンプレートのハイライト版を業界が同様に受け入れるよう、企業と協力を続けていく。

p. 18

消費者リーダーの展望

・ デモクラシー科学技術センター、全国消費者連盟およびプライバシー権情報センターと議論した結果、

・ 階層を設けたノーティスはひとつの改善策である、ということを合意した。

・ 「このプロジェクトを実施していることを喜んでいる。」

p. 19

障害

・ 外的環境は不確実である。

・ 階層を設けたノーティスへの移行は、GLBA または HIPAA のいずれかがカバーする企業にとってコストがかかる。
  — プライバシーステートメント完全版だけは要求に応じて入手可能にすべきではないのか？

・ 国内基準がひとつあるべきではないのか？

・ ノーティスのハイライト版を使う企業の責任問題が不明瞭

p. 20

まとめ
・ 法的に強制されたノーティスは消費者に優しくない

・ 消費者は、以下のような共通のテンプレートを望んでいる。
  — 要素は 7 個未満にする
  — 日常的な言葉を使う

・ テンプレートをベースにしたノーティスは、ビジネスが情報ベースの価値を分配できるための信用を高めるものである。

5.2.2.3 Hunton & Willians **資料②**（Preminary Research on Short / Highlights Privacy Notices, January 20, 2004）

p.1・2

プライバシーノーティスのショート/ハイライト版に関する事前調査

2004 年 1 月 20 日

目的 ― ノーティスのショートハイライト版のコンセプトおよび構造を有効化すること

- 企業の総体的な経験に基づいて選択された 6 個のカテゴリー（最大個数）を有効化する。
  - 他のカテゴリーが付け加えられる必要があるかどうかを決定する。
  - どのカテゴリーが最も重要かを決定する。
- GLB/HIPAA によって提示された業界または部門のアプローチと比較して、消費者が「ユニバーサル」アプローチを好んだかどうか、どのようにすれば消費者がそのようなノーティスを読むようになるかについて、われわれのモデルに最も適合するものをフィードバックしてもらう。
- テンプレート上のカテゴリーを表現するときに自然に使うような文言を消費者から集める。
- ショートノーティスのさまざまなテンプレートについてフィードバックを集める。
- 消費者がどのような行動をとるか見極める。

p.3・4

6つのフォーカスグループが開かれた。
- 3 フォーカスグループ会議 ― 2002 年 2 月 13 日
  - 一般との夜間会議 2 回
  - P&G クリエイティブ消費者連合会との昼間会議 1 回
- 3 フォーカスグループ会議 ― 2003 年 8 月 5 日
  - 一般から全員参加
  - プライバシーノーティス意識をもつための選抜
- 会議はすべてシンシナティ市の P&G「未来の家（Home of the Future）」にて開催された。
- チームメンバーがモデレーターを務めた。

会議は、制限なしのフィードバックや意見が出るように構成された。
- 会議は、消費者が最近目にしたプライバシーノーティスとそれに対する彼らの反応について自由な雰囲気の中で議論が始まった。
- 次の段階では、われわれが定義したプライバシーカテゴリーについて制限なしの考えを出してもらった。
- 参加者は、定義されたカテゴリーに与えるべき優先順位及びその中での話題について議論及びディベートを行った。
- 選択された文言（語彙）についてフィードバックが集められた。
- さまざまな視覚的構造についてのフィードバックで議論が締めくくられた。

p.5・6

2002 年度と 2003 年度のすべての会議を通していくつかの結果が明らかになった。

- 6 個のカテゴリーは消費者の最重要関心事に対応していると思われた。
- 消費者は最近受け取ったプライバシーノーティス（2002 年度 GLBA、2003 年 HIPAA）を知っていたが、企業がデータを使用する方法や理由など、多くの大切な概念について周知徹底されていないようだ。
- 消費者は、最初のアプローチのようなロングノーティスを拒絶した。
- 消費者は、テンプレートによるアプローチを好んだ。
- 文言についてはかなりの重要な作業が必要である。
- 消費者は、明白さをそのまま残しておくことは厭わない。

参加者は、現在与えられているノーティスはもう読まないと言った。

「一度見たことがある…」
「最初の数行を読んで…何を言おうとしているかわかった。」
「企業は自己保身のためにそのようなノーティスを書いている…」
「現在なぜプライバシー問題があるのかを知りたいが、全ページを読みたいとは思わない。」
「私は環境問題について考えてしまう。それは紙の無駄、本当に無駄だ。」

p.7・8

参加者は、ノーティスのハイライト版について肯定的だった。

「これを作るのに相当の努力をしただろう。このノーティスは重要部分をしっかり捉えている。それに力を注いだのだ。」
「ショートノーティスは、初期コピー後十分良くなるだろう。」
「プライバシーノーティスがこのフォーマットになれば、おそらく私はそれを読むだろう。」
「簡略化すればより多くの人がそれを読み、どんな情報が共有されるかがわかるだろう。」
「簡略なほうが私にとっては良い、そしてもっと読みたいと思うとき選択肢を与えてくれる。」
「私は好きだ。」

2002 年度版と 2003 年度版にはいくつかの重要な違いがあった。

2002 年度版
- GLB ノーティスが新しかった。
- ロングノーティスにする必要性はほとんど見られなかった。
- データセキュリティはノーティスにとって重要ではなかった。
- フォーカスグループは前文を削除したかった。会社への信頼はほとんどなかった。

2003 年度版
- HIPAA ノーティスが普及した。
- ロングノーティスは要請に応じて/ホームページ上で入手するために重要だという強い見解の一致があった。
- データセキュリティは最重要課題となった。
- 会社についての短い文章が好まれた。ブランドがより重要になった。

p.9・10

言葉の使い方が依然として重要な課題である。

- 「中にはもっと上手に説明できる部分がある。」
- いくつかの場合において「購入データ」などの概念は参照という一般の枠外にあった。
- そのほかの場合において、以下の一般用語は、正しいメッセージを伝達するのに付帯的意味合いが多すぎだ。
  - 「提供(share)」対「公開(disclose)」対「販売(sell)」
  - 「データ」
  - 「ポリシー」
  - 「適用範囲」

2003 年度のフォーカスグループは、ロングノーティスを入手するのを好んだ。

- これは、以下の構造的要素によって影響を受けたのかもしれない。
  - プライバシーノーティス意識を持ったパネラーが選別された。
  - 読みやすいロングノーティス版が 2003 年度に登場した。
- 2 人の参加者（10%）は、常にこのような長いノーティスを読むと言った。ほとんどの参加者は必要に応じてロングノーティスを欲しがった。
- その他の意見
  - 「私は、ほんとうは両者をリンクさせるのが好きだ。リンクすることで、より短くなるが、必要ならばそのほかの情報も得やすくなる。」
  - ショートノーティスは初期コピー後十分良くなるだろう。」

p. 11・12

その他の発見

- 「使用」および「選択」が両年度において最重要だった。
- 参加者は会社とコンタクトを取るための情報を得るさまざまな概念及び理由を好んだ。
- テンプレートフォーマットと一貫したカテゴリー設定が強く好まれた。
- 参加者はすべての企業によって使用されるひとつのテンプレートという考えを好んだ。

結論

- フォーカスグループが事前調査を考察しているあいだ、グループメンバーからの一連のフィードバックによってショートノーティスの概念および構造に信頼が寄せられた。
- 2002 年度と 2003 年度の変化によって、ノーティスへの消費者のニーズとノーティスを理解するための枠組みはより良い例を示し経験することによって変化することがわかった。
- 「要請があれば」ロングノーティスを必要とする強い要望が 2003 年度に現れた。おそらくこれは、より良い例を示したことに反応したものと思われる。
- 会社がこのアプローチを採用し始めていることと同様に、文言が重要な課題として残るだろう。

6 参考資料

6.1 民間部門における電子商取引に係る個人情報の保護に関するガイドライン（Ver.2.0）

■はじめに

電子商取引推進協議会（以下「ＥＣＯＭ」という。）、野村総合研究所及び経済産業省による「平成１４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、2002年のBtoC（Business to Consumer）の電子商取引の市場規模は2兆6,850億円となり、2001年の1兆4,840億円に対し1.8倍と、ほぼ倍増に近い成長を遂げている。さらに、今後も堅調な成長が続くものと考えられ、2007年には12兆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、流出、改ざん等の悪用は、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、1970年代に欧米諸国で個人情報保護あるいはプライバシー保護に関する法整備の動きが活発になったのを受け、1980年に経済協力開発機構（以下「ＯＥＣＤ」という。）では、「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」（以下「ＯＥＣＤプライバシー･ガイドライン」という。）にて個人情報保護のための8原則を示した。

また、欧州連合（以下「ＥＵ」という。）は、1995年、その加盟国に対し、指令採択の日から3年以内にそれを遵守する法令を定めることとし、さらに、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の保護に関する法律」が制定されているが、民間分野においては、1988年の財団法人日本情報処理開発協会（以下「JIPDEC」という。）の「民間部門における個人情報保護のためのガイドライン」を踏まえた、

1989 年の通商産業省（現･経済産業省）の「民間部門における電子計算機処理に係る個人情報の保護について（指針）」等のガイドラインが策定されてきた。現時点では、1997 年に通商産業省が官報告示した「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に自主規制の下で個人情報保護の取組みがなされている。

1990 年代後半以降、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」が国会に提出された。同法案は、2002 年 4 月から審議入りし、同年 12 月一旦廃案となったが、翌 2003 年 3 月に再度修正案が提出され、衆参両院での審議を経て、5 月 23 日に成立、同 30 日に公布･施行された。（うち、個人情報取扱事業者の義務等に関する規定については政令により 2005 年 4 月 1 日よりの施行となった。）

この「個人情報の保護に関する法律」（以下「個人情報保護法」という。）では、「個人情報の有用性に配慮しつつ、個人の権利利益を保護すること」を目的としており、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、個人情報保護法が成立したことを受け、企業における個人情報保護への体制整備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、この「ECOM ガイドライン 1.0 版」を改訂することとした。

このガイドラインでは、基本的には個人情報保護法に対応しながら、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すこととした。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、個人情報保護法には明記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から個人情報を取得し、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り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　総則

（目的）

第１条　このガイドラインは、電子商取引において個人情報を取り扱う事業者に対し、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のとれ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、消費者の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更に健全に普及し、高度情報通信社会の進展に寄与するものと考える。
3. 個人情報保護法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して掲げられており、その精神は本ガイドラインと一致するものである。

参考　個人情報保護法第 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することができる。

2　事業者は、個人情報を取り扱う際の基準又は個人情報保護に関する規程を策定する際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を取得し、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)　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整備するとき。
   (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。
3. このガイドラインは、上記に該当する事業者が任意に採用できるものであり、法的な拘束性を持つものではないので、その取り扱う個人情報の量や利用方法により事業者等を限定しない。
4. このガイドラインでは、事業者が取り扱うすべての個人情報を適用の対象とするが、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、所轄官庁の指針又は指導に従い、別途細目を定められることが望ましい。

(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一定の規則にしたがって整理することにより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情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものをいう。

(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。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以下のものに該当する場合及び 6 ヶ月以内に消去することとなるものは除く。

①本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

②違法又は不当な行為を助長し、又は誘発するおそれがあるもの

③国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

④犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

(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・プログラム又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、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、BtoB(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、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、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個人情報保護法に準じることとした。個人情報保護法では「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あげられていた。(2)については、その後政令により、対象となるマニュアル(手作業)処理情報としては、これに含まれる個人情報を一定の規則にしたがって整理することにより特定の個人情報を容易に検索することができるように体系的に構成した情報の集合物であって、目次、索引その他検索を容易にするためのものを有するものと定められた。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がこれに相当すると考える。
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、将来開発する商品のために行うマーケティング調査等の統計目的で個人を特定しない形で収集し、取り扱う情報や個人名等を伏せ、個人を特定できない態様で匿名化して取り扱う情報はこれに該当しない。
5. 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。なお、政令により、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ガイドライン第3条(6)の①から④に

示されるもの及び短期間（6ヶ月以内）に消去されるものは除外されることとなった。

6. ECOMガイドライン1.0版では「情報主体」としていたが、個人情報保護法に準じ、このガイドラインでは「本人」とした。

7. 電子商取引では、ある程度の規模を持つ企業だけでなく、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り扱う事業者」を指す。なお、第2条解説4に示すように、このガイドラインは、適用対象の事業者に対して法的な拘束性を持つものではないので、個人情報保護法における「個人情報取扱事業者」にてその取り扱う個人情報の量や利用方法により適用除外となる事業者等を規定しない。なお、政令では、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去6ヶ月以内のいずれの日においても5000を超えない者は個人情報取扱事業者から除外されるとされている。さらに、他人の作成したカーナビや電話帳を取得して、編集し、又は加工することなくその事業の用に供するときは、これを構成する個人情報によって識別される特定の個人の数はその数に算入しないとされている。

8. 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」といい、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持つとともに、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。ある程度の規模を持つ企業においては、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。

9. 「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　個人情報保護法第2条・政令第1条・第2条・第3条・第4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持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は、次に掲げる（1）から（14）まで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ために社内管理体制を整備するに当たり、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その他の規範がある場合についてそれを遵守する必要がある。そのために法令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整備後においても新たに発生する業務、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

このガイドラインの第6条から第 14 条までに従って規定されるべきである。

⑹　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 15 条と第 16 条に従って規定されるべきである。

⑺　従業者の監督、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

このガイドラインの第 17 条から第 22 条までに従って規定されるべきである。

⑻　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な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を採用するかを決定するプロセスを規定する。

⑼　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

このガイドラインの第 23 条から第 29 条までに従って規定されるべきである。

⑽　苦情の処理等に関する規定

このガイドラインの第 30 条に従って規定されるべきである。

⑾　個人データの紛失、破壊、改ざん及び漏えい等が発生したとき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ときの対応及びその是正措置を規定する。

⑿　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 条を参照して規定されるべきである。

⒀　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。

⒁　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. 個人情報保護法第 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。どのぐ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。

2. 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り扱われなければならない。

3. ECOM ガイドライン 1.0 版では、ＯＥＣＤプライバシー・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、個人情報保護法に相応して、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　個人情報保護法第 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って、本人の同意を得ることが困難であるとき。

⑷　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. 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」とは、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。後日の立証の容易性を考えると、書面の場合では本人による署名、捺印等が、また、ウェブ画面上では同意のボタンへのチェック、確認メールの返信、電子署名等の方法がこれにあたる。

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はなく、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等の方法で、本人の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て個人情報を取り扱うときには、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できる。

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ときに、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　個人情報保護法第 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、偽っての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。

4. 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。

参考　個人情報保護法第 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. 個人情報保護法第 18 条第1項では、直接的･間接的に関わらず個人情報を取得したとき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、個人情報保護法に準じ、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。
5. 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た。すなわち、情報主体の明確な同意がある場合、法令に特段の規定がある場合及び司法手続上必要不可欠である場合を除いて、次に掲げる種類の内容を含む個人情報について、これを収集し、利用し又は提供することを禁止していた。
   (1) 人種及び民族
   (2) 門地及び本籍地（所在都道府県に関する情報を除く）
   (3) 信教（宗教、思想及び信条）、政治的見解及び労働組合への加盟

(4) 保健医療及び性生活

個人情報保護法では、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でも機微になりうるので、情報の種類を特定して機微であるか否かを分類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。しかしながら、事業者として、個人の権利利益の一層の保護を図るとともに、顧客とのトラブル等を未然に防ぐといったリスクマネジメントの観点から、これら特定の機微な個人情報とされる情報の取得の際には、本人の同意を取り、必要かつ適正な安全管理措置を施し、さらには、第三者提供を行わないといった厳格な取扱いがなされることが望まれる。また、それら以外の個人情報についても、その取得の状況やマッチング等により本人にとって機微な個人情報であると考えられる場合には、同様の措置を取るよう努めるべきである。

参考　個人情報保護法第 18 条第1項

（インターネット等の情報ネットワーク上等で本人から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から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. 個人情報保護法第 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から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っ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ダイレクトメールを行うことについて、本人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等を発信することを予定している場合は事前に本人に明示しなければならない。

4. ウェブ画面上から個人情報の入力を求めるときには、利用目的を明示するだけでなく、同意ボタンの設置等、消費者の同意を取得する措置を設けることで、消費者が利用目的を確認し、その取扱いについての諾否を判断する機会を与え、一層の消費者の信頼を得られるものと考える。

参考　個人情報保護法第 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は、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行われなければならず（第6条）、変更した場合は、変更後の利用目的を、本人へ通知、又は公表しなければならない。
2. インターネット等の情報ネットワーク上では、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、再度本人からの同意をもらうことが望ましい。
3. 再度本人から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に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。
4. 利用目的の変更について、「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」行う場合は、第7条の規定に基づき、あらかじめ本人の同意を得る必要がある。

参考　個人情報保護法第 18 条第 3 項

（取得時及び利用目的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. 個人情報保護法第 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　個人情報保護法第 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、フレームモード等、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。

⑶　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ー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、本人のパソコンから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い得ないこともあり、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　個人情報保護法第 18 条

（子どもから個人情報を取得する場合の措置）

第１４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等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。」等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、取り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１５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　個人情報保護法第 19 条

（安全管理措置）

第１６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。

(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等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、ファイアー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に個人情報を入力してもらう場合には、SSL(Secure Socket Layer)等の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等の配慮をすべきである。

参考 個人情報保護法第 20 条

(従業者の監督)

第１７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り扱われているかを必要に応じて確認すること。

（解説）

1. 個人情報保護法第 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、意識を高く持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持つ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、個人情報保護法第 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り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等の措置を講ずる必要がある。

参考　個人情報保護法第 21 条

（委託先の監督）

第１８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　個人情報保護法第 22 条

（サイバーモール運営者の対応）

第１９条　事業者は、サイバーモールを運営するに当たり、本人から直接個人情報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。）において適正な取扱いが図られるような対策を講ずるよう努めることとする。

(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等の個人情報の取扱いについて、一定の対策を施すよう努めることを奨励するものである。
2. 実際サイバーモール運営者はショップ等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持つものではない。 したがって、万一、ショップ等から個人データが漏洩した場合、消費者に対する責任は、本来、ショップ等が負うこととなる。しかしながら、消費者からみると、そのショップ等の責任を追求するにとどまらず、ショップ等が加入しているサイバーモール運営者に苦情が寄せられることも考えられる。

そうした事態が発生し、マスコミ報道等により社会的信頼を損なうこととなりうる点も考慮すると、ショップ等に対し、個人情報の取得や個人データの安全管理措置等について、責任の所在を明らかにする等の適切な対策を施すことが望ましい。

3. サイバーモール運営者がショップ等に対して、契約の中で、取得や安全管理についての必要かつ適切な措置を施すことを義務づけることにより、顧客の不安は解消され、いくらかのトラブルが回避でき、サイバーモール運営者自体のリスクも回避される。
4. また、消費者がサイバーモールを利用し、個人情報の入力をする際に、個人情報の取扱い上の責任がサイバーモール運営者とショップ等の間のいずれにあるかについて、ウェブ画面上に明示することが望まれる。

第３節　個人データの第三者提供

（第三者提供の制限）

第２０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る等本人による了解の下に行うものとしている。
2. 個人情報保護法第 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、個人情報保護法と同様に、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　個人情報保護法第 23 条第 1 項

（第三者に提供できる場合）

第２１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個人情報保護法第 23 条第2項に対応している。
2. 第 20 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から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項に関しての措置についても、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　個人情報保護法第 23 条第 2 項･第 3 項

（第三者提供に該当しない場合）

第２２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。

① 共同利用する旨

② 共同して利用される個人データの項目

③ 共同して利用する者の範囲

④ 利用する者の利用目的

⑤ 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)に規定する項目のうち、④又は⑤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内で行われる一般的な行為であるため、個人情報保護法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、併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、個人情報保護法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、観光･旅行業等グループ企業で総合的なサービスを提供するために個人データの提供をし合うケース等が想定される。

参考　個人情報保護法第 23 条第 4 項･第 5 項

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２３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）　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）　事業者が行なう保有個人データの取扱いに関する苦情の申出先および認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

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１２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. 個人情報保護法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24条、第25条、第26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　個人情報保護法第24条・政令第5条

（開示）

第２４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

２　開示に当たっては書面により交付することとする。ただし、開示の求めを行なった者が同意した方法があるときは、当該方法で行うことができる。

(解説)

1. 前条の解説1.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ため、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。

6. 政令により、開示の方法としては、原則、書面により交付することとし、開示の求めを行った者が同意した方法があるときは当該方法で行うことができることとなった。したがって、Web 画面上や電子メール等で開示をする際は、開示の求めを行った者に同意を得て行うよう留意しなければならない。

参考　個人情報保護法第 25 条･政令第 6 条

（訂正等）

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。）を求められたときは、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　個人情報保護法第 26 条

（利用停止等）

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その利用目的の制限や適正な取得に違反して取り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等、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. 個人情報保護法第 27 条にて本人は事業者に対し、同第 16 条の利用目的の制限に違反して取り扱われる場合及び同第 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、さらに同第 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、それに応じなければならない。

3. ただし、個人情報保護法では、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　個人情報保護法第 27 条

（理由の説明）

第２７条　事業者は、開示、訂正等及び利用停止等（以下「開示等」という。）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. 個人情報保護法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とき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等による説明を行うことが必要である。

参考　個人情報保護法第 28 条

（開示等の求めに応じる手続）

第２８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として以下について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。

(1)　開示等の求めの申し出先

(2)　開示等の求めに際して提出すべき書面（電子的方式、時期的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。）の様式その他の開示等の求めの方式

(3)　開示の求めをする者が本人又は本条第４項に規定する代理人であることの確認方法

(4)　手数料の徴収方法

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２３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。

4　事業者は、次に掲げる代理人による開示の求めに応じなければならない。

(1)　未成年者又は成年被後見人の法定代理人

(2)　開示等の求めをすることにつき本人が委任した代理人

(解説)

1. 事業者は個人情報保護法第 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個人情報保護法第 30 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、そのと

き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、個人情報保護法同様に、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ができるとはしていない。

6. 政令により、未成年者又は成年被後見人の法定代理人および開示の求めをすることにつき本人が委任した代理人が本人に代わって開示等の求めができることとなった。未成年者であれば、その親権者であることを確認すべきであり、委任を受けての代理を受け付けるにあたっては、本人の委任を受けた代理人であることを確認する手続き等を定め、その手続きに従って開示等に応ずることが必要である。

参考　個人情報保護法第 29 条･第 30 条･政令第 7 条･第 8 条

（子どもの個人情報に関する保護者の求めへの対応）

第２９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２４条から第２８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 14 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３０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節は個人情報保護法第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. 個人情報保護法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(個人情報保護法第 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、命令の権限を持つているので、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個人情報保護法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、取り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、電話番号等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 個人情報保護法第 31 条

第４章　管理体制

（個人情報保護担当責任者の指名）

第３１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３２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、従業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整備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整備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。

⑴　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。

⑵　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。

⑶　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・マニュアルを作成する。

⑷　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。また、個人情報保護法が成立し、事業者として守るべき義務が生じたことに伴い、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からの開示等の求めへの対応や苦情処理だけでなく、個人情報保護法第 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、あるいは改ざんのそし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３３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等に照らして、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ておくことが重要である。

6.2 商品 IC タグに係る消費者の個人情報及びプライバシーの保護に関するガイドライン（Ver.0.1）

はじめに

IC タグ（RFID）はその優れた特性から SCM やトレーサビリティの分野での実用化が期待されている。しかしながら、消費者が所持する物品に IC タグが貼付されることで、カバンの中にある所持品を盗み見られるのではないか、といった個人のプライバシーが侵害されるとの懸念もあり、海外では、これを問題視する消費者団体の申し入れにより IC タグの導入を断念する企業も現れている。

電子商取引推進協議会では、こうした消費者の不安や懸念が払拭され、IC タグが広く、健全に IT 社会の中で活用されることを目指し、IC タグが貼付された商品を製造・販売する事業者および、商品 IC タグ用のリーダまたはライタを設置して業務を行う事業者が遵守するべき事項について検討し、ここに「商品 IC タグに係る消費者の個人情報及びプライバシーの保護に関するガイドライン（Ver.0.1）」としてまとめた。

本ガイドラインは、商品 IC タグに消費者個人のデータが書き込まれ、或いは、消費者が所持する物品に貼付された商品 IC タグが、本人の知らないうちに読み取られるといった事態が起こりうる状況下で、事業者が自主的に消費者の（個人情報及び）プライバシーの保護に配慮して必要かつ適切な措置を施すことを目的とするものである。

また、特定の業界に限定するものでなく、商品ＩＣタグの導入を進める事業者全般を適用対象とし、基本的に遵守するべき項目を示すものであるので、今後、さらに業際及び業界毎にきめ細かく消費者に配慮した自主的な取組みを期待するものである。

本ガイドラインが、幅広く、IC タグの導入を進める事業者に参照され、消費者の安心と信頼を得て、ＩＴ社会の基盤として多方面で高活用されることを希求する。

商品 IC タグに係る消費者の個人情報及びプライバシーの保護に関するガイドライン（Ver.0.1）

① 事業者(注 1)は、商品 IC タグ(注 2)の利用に際して、個人情報を取り扱う場合には、消費者(本人)の権利利益を保護しなければならない。

② 事業者は、消費者が商品 IC タグを貼付又は内蔵した商品を、安心して購入及び所持することを可能にするために、IC タグの利用に関して、業際及び業界毎に自主的なガイドラインを制定し、消費者に公表するとともに、これを遵守することが望ましい。

③ 事業者は、商品 IC タグの利用に当たって、以下のことを消費者に対して公表又は表示しなければならない。

- 商品 IC タグ及び商品 IC タグから検索されるデータベースの項目。
- 商品が販売後も商品 IC タグを貼付され又は内蔵する場合には、購入時または購入後に、商品 IC タグを読めない状態にして所持するか、商品 IC タグを読める状態で所持するか、を決定する権利は消費者にあること。
- 消費者が購入後に、商品 IC タグを読める状態で所持することで得られるメリット。
- 消費者が購入後に、商品 IC タグを読める状態で所持する場合に想定されるリスク。
- 購入時または購入後に、商品 IC タグを読めない状態で所持する場合に消費者が蒙るデメリット。

④ 事業者は、商品 IC タグが付いていることを商品そのもの又は取扱説明書又は梱包材に明瞭に表示しなければならない。

- 商品の特性等に応じて、必要な場合には貼付場所も明示する。

⑤ 事業者は、消費者が購入時または購入後に、商品 IC タグを読めない状態にするための以下の手段のうち少なくとも1つを、原則として無償で提供しなければならない。

- 商品 IC タグを商品から外す手段。
- 商品 IC タグを無効化する手段。
- 商品 IC タグを遮蔽する手段。

注 1)事業者：

IC タグを貼付または内蔵した商品を製造、販売する事業者、およびリーダ・ライタを設置して IC タグ内の情報を取り扱う業務を行う事業者。

注 2) 商品 IC タグ：

SCM、トレーサビリティ等に応用するため、商品を識別する目的で、商品に貼付または内蔵させる IC タグ。形状、方式（周波数帯域、電池の有無等）は特定しない。

■　引用参考記事、資料・文献、ＵＲＬ一覧（順不同、敬称略）

- 個人情報保護法の解説（園部逸夫編集／ぎょうせい）
- 逐条個人情報保護法（藤原静雄／弘文堂）
- 新報解説個人情報保護法入門（岡村久道／商事法務）
- 解説個人情報の保護に関する法律（宇賀克也／第一法規）
- 漏えい事件 Q&A に学ぶ個人情報保護と対策（北岡弘章／日経 BP 社）
- 法律のひろば 2003 年 9 月号（ぎょうせい）
- ビジネス法務 2003 年 9 月号（中央経済社）
- Jurist2003 年 10 月 1 日号（有斐閣）
- 個人情報保護に関する世論調査（平成 15 年 9 月調査、内閣府大臣官房政府広報室）
- インターネット白書 2003（財団法人インターネット協会監修）
- 情報化白書 2003（財団法人日本情報処理開発協会編）
- 金融情報システム平成 16 年冬号（財団法人金融情報システムセンター）
- 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ＳＣＣ）
- 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）
- 25th International Conference of Data Protection & Privacy Commissionerss
  http://www.privacyconference2003.org/
- 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）

ほか

■　個人情報保護ＳＷＧ名簿（敬称・役職略、企業名５０音順）

委員	吉岡　英剛	アコム(株)　営業企画部
委員	高田　誠	(株)アプラス　情報セキュリティ部
委員	大西　浩	(株)オーエムシーカード　顧客満足推進部
委員	田中　剛	(株)オーエムシーカード　営業開発本部企画管理部
委員	西尾　美和	沖電気工業(株)　ﾈｯﾄﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝｶﾝﾊﾟﾆｰ　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	藤原　康明	電気事業連合会　情報通信部
委員	高松　博光	電気事業連合会　情報通信部
委員	祝　　壮吉	東京電力(株)　システム企画部
委員	風見　博史	(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)　国内マーケッティング部
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	成田　順子	日本アイ・ビー・エム(株)　スタッフオペレーションズ渉外
委員	上野　正之	日本信販(株)　個人情報部
委員	龍田　省	日本電気(株)　法務部
委員	杉山　直也	日本電気(株)　法務部
委員	友村　真也	日本電気(株)　BIGLOBE カスタマリレーション本部
委員	太田　浩司	日本ユニシス(株)　法務部
委員	泉　　綾子	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	西岡　信佳	(株)日立情報システムズ　法務部
委員	渡辺　美佐子	富士通(株)　法務部　法務企画部
委員	岩田　修	マイクロソフト株式会社　法務・政策企画統括本部
委員	古川　勝也	マイクロソフト株式会社　製品マーケティング本部
委員	吉川　義幸	ﾏｽﾀｰｶｰﾄﾞ・ｲﾝﾀｰﾅｼｮﾅﾙ・ｼﾞｬﾊﾟﾝ・ｲﾝｸ ｱﾄﾞｳﾞｧﾝｽﾄ・ﾃｸﾉﾛｼﾞｰ・ﾃﾞｨﾚｸﾀｰ
委員	東山　治郎	松下電器産業株式会社　情報セキュリティ本部

委員　玉井　康昭	三井住友海上火災保険(株)　文書法務部
委員　岩間　研二	三菱電機(株)　インフォメーションシステム事業推進本部
委員　岡田　潤之	三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ株式会社　品質生産推進部

● 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
太田　克良	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)　法務部
鈴木　靖	(株)シーピーデザインコンサルティング
藤田　素康	リコー・ヒューマン・クリエイツ(株)
富永　辰也	(有)アドバンス・ティ
牧山　嘉道	西川綜合法律事務所
土井　悦生	オリック東京法律事務所
松永　雅利	(財)金融情報システムセンター　調査部
合原　英次郎	松下電器産業(株)　東京支社　渉外グループ

● ＥＣＯＭ　事務局

事務局　浅沼　省吾	電子商取引推進協議会　主席研究員

■　ガイドラインＴＦ名簿（敬称・役職略、企業名５０音順）

委員　藤原　康明	電気事業連合会　情報通信部
委員　祝　　壮吉	東京電力(株)　システム企画部
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　西岡　信佳	(株)日立情報システムズ　法務部
委員　吉川　義幸	ﾏｽﾀｰｶｰﾄﾞ・ｲﾝﾀｰﾅｼｮﾅﾙ・ｼﾞｬﾊﾟﾝ・ｲﾝｸ ｱﾄﾞｳﾞｧﾝｽﾄ・ﾃｸﾉﾛｼﾞｰ・ﾃﾞｨﾚｸﾀｰ
委員　東山　治郎	松下電器産業株式会社　情報セキュリティ本部
委員　岩間　研二	三菱電機(株)　インフォメーションシステム事業推進本部

● アドバイザー

堀部　政男	中央大学教授（一橋大学名誉教授）
太田　克良	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)　法務部
鈴木　靖	(株)シーピーデザインコンサルティング
牧山　嘉道	西川綜合法律事務所
合原　英次郎	松下電器産業(株)　東京支社　渉外グループ

● ＥＣＯＭ　事務局

事務局　浅沼　省吾	電子商取引推進協議会　主席研究員

■　企業対応検討ＴＦ名簿（敬称・役職略、企業名５０音順）

委員　藤原　康明	電気事業連合会　情報通信部
委員　高松　博光	電気事業連合会　情報通信部
委員　祝　　壮吉	東京電力(株)　システム企画部
委員　脇田　正敏	トヨタ自動車(株)　国内マーケッティング部
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　西岡　信佳	(株)日立情報システムズ　法務部
委員　岩田　修	マイクロソフト株式会社　法務・政策企画統括本部
委員　吉川　義幸	ﾏｽﾀｰｶｰﾄﾞ･ｲﾝﾀｰﾅｼｮﾅﾙ･ｼﾞｬﾊﾟﾝ･ｲﾝｸ ｱﾄﾞｳﾞｧﾝｽﾄ･ﾃｸﾉﾛｼﾞｰ･ﾃﾞｨﾚｸﾀｰ
委員　東山　治郎	松下電器産業株式会社　情報セキュリティ本部
委員　岩間　研二	三菱電機(株)　インフォメーションシステム事業推進本部

● 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
太田　克良	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)　法務部
鈴木　靖	(株)シーピーデザインコンサルティング
藤田　素康	リコー・ヒューマン・クリエイツ(株)
富永　辰也	(有)アドバンス・ティ
牧山　嘉道	西川綜合法律事務所
土井　悦生	オリック東京法律事務所
合原　英次郎	松下電器産業(株)　東京支社　渉外グループ

● ＥＣＯＭ　事務局

事務局　浅沼　省吾	電子商取引推進協議会　主席研究員

(奥付)

EC で取り扱われる個人情報に関する調査報告書

平成　１６年　３月　発行

発　行　　電子商取引推進協議会

販　売　　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

(裏表紙)

ISBN4-89078-622-8 c2055 ¥4762E