（表紙）

ＥＣにおける個人情報保護に関する活動報告書

平成１７年　３月

電子商取引推進協議会

はじめに

情報社会の進展、とりわけインターネットの普及に伴い個人情報の拡散リスクが高まりつつあることはいまさら多言を要しない。かような状況に鑑み、当電子商取引推進協議会（以下ＥＣＯＭと略）では平成 10 年度より関係各位のご支援・ご協力をいただきながら電子商取引にフォーカスした個人情報保護のあり方について検討と提言を行ってきた。

本報告書は平成 16 年度の活動内容として

・ＥＣＯＭ個人情報保護ガイドラインの改訂
・ＥＣＯＭ会員企業、ＥＣ事業者における個人情報保護に関する実態調査
・個人情報保護に関する海外の動向

について報告するものである。

ＥＣＯＭガイドラインの改訂にあたっては個人情報保護ＷＧにご参加の会員有志およびアドバイザの方々から貴重なご意見をいただいた。また個人情報保護に関する実態調査について今年度は新たに BtoC 専業事業者までその対象を広げて行ったがその際日本商工会議所様には大変お世話になった。個人情報保護に関する海外の動向についてはリコー・ヒューマン・クリエイツ㈱の藤田素康様にご執筆をいただいた。この場を借りて報告書の取りまとめに関わっていただいた多くの方々にあらためて御礼を申し上げるとともに、その成果がＥＣ現場での活用を通じて安心、安全な電子商取引の発展に寄与できることを願うものである。

平成１７年３月

電子商取引推進協議会

目　次

1. ＥＣＯＭ個人情報保護ガイドラインの改訂について

1.1 背景と経緯

高度情報社会の進展とともに個人情報保護に対する法制度が世界各国で整備されるようになったが、わが国においても 2003 年に行政部門を対象とする「行政機関の保有する個人情報の保護に関する法律（1988 年「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」の全面改正)、および民間部門を対象とする「個人情報の保護に関する法律」が新たに制定された。後者については業種、業態により事業者が取り扱う個人情報の内容、利用局面等が異なるため所管する省庁が分野ごとにガイドラインを策定し当該事業者の判断基準を提供している。電子商取引推進協議会(以下 ECOM と略)では既に 1998 年、通商産業省（当時）がその前年公表した「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」をベースに「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」を発表し産業界における先駆的な役割を果たしてきたが、昨年 10 月経済産業省(以下 METI)より「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(以下 METI ガイドライン)が公表されたのを期に従来のガイドラインを改訂し、より適切な事業者としての対応を推進するものとした。改訂にあたっては個人情報保護ＷＧのメンバー有志が何度も会合を重ね、検討を行った。ご多忙の中ご検討に加わっていただいた方々には重ねて御礼を申し上げたい。

1.2 ＥＣＯＭガイドラインとＭＥＴＩガイドラインのスタンスの相違

「METI ガイドライン」はいうまでもなく METI 所管分野の事業者が「個人情報の保護に関する法律(以下「保護法」と略)」に則って遂行する個人情報保護活動を支援するために経済産業省自らが定めた具体的指針である。従ってその内容はあくまで「保護法」の解釈の範囲内となるが、一方「ECOM ガイドライン」は「保護法」「METI ガイドライン」を参照しつつも電子商取引に焦点を当て、なおかつ民間の自主性を期待したものであるため、その適用範囲、「保護法」との距離については「METI ガイドライン」と若干差がある。「ECOM ガイドライン」は処罰ルールを伴わないためその適用対象は保有個人データ件数 5000 件超の事業者だけに限定するものではないし、また民間自主規制の性格上、「保護法」の要求水準より若干ハードルが高い部分もある。

1.3 今回の改訂の概要（ECOM ガイドラインで特記したこと）

あまねくビジネス全体がＥＣ化している中で前述の「METI ガイドライン」自体ＥＣを想定した記述が増えており、結果として「ECOM ガイドライン」の相当部分は「METI ガイド

ライン」を引用している。「METI ガイドライン」については既にその公表時に熟読された方も多いと思われるので、ここでは今回の改訂の中で「ＥＣOMガイドライン」において特記した部分について記す。

1.3.1 個人情報保護方針及び法定公表事項等のウェブ画面上での表示について

事業者は、一般の人が自社の個人情報保護方針及び法的公表事項等を入手・閲覧できるように、外部向けに文書化し、公表することになっているがその掲示方法についてはトップページにﾘﾝｸボタンを設置し一度のｸﾘｯｸでその概要を参照できることが望ましいとした。ECOM が昨年実施した「会員企業の個人情報保護に関するウェブ上での表記調査」によると全 213 社のうちの 63%の企業・団体がトップページにリンクボタンを設置しているが EC 事業者全体を見るとまだまだ低い水準に留まっており、改善の余地が残されている。また、「保護法」に定める公表（または通知）事項についてはその公表サンプルを巻末に添付したが保護方針と併せ誰もが容易に参照できるよう配慮することが望まれる。

1.3.2 クッキー、ウェブ・ビーコン等による個人情報の自動取得について

電子商取引ではしばしば、クッキーに代表されるような閲覧履歴自動取得技術を使って、本人の気がつかないところでサイトの訪問履歴を取得していることがある。クッキー等のデータは常に個人情報に該当するわけではない（統計情報として利用する場合等）が、特定個人を識別する形で利用する場合にはその事実と利用目的を通知又は公表するものとした。なお、本人に対し安心感を与える意味で、クッキー等を個人情報と結び付けて利用しないケースでもその旨をわかりやすく表示したり、クッキー等の使用を説明した上でなおかつ本人が利用停止を望んだ場合に備えクッキーを無効にする操作手続きを明示することが望まれる。

1.3.3 機微な情報に関する取扱いについて

事業者は個人情報の取得にあたり明確な指針を策定し、事業の遂行に必要な個人情報を特定することが望まれるが、その際、顧客とのトラブル等を未然に防ぐといった観点から、思想、信条、宗教、健康状態その他人種、門地等社会的差別につながるおそれのある個人情報についてその取扱いに格段の配慮を払う必要がある。事業の遂行上、止むを得ず取得する場合には、本人の同意を得る、より厳格な安全管理措置を施す、さらには、第三者提供を決して行わない、等に留意しなければならない点を付記した。

1.3.4 漏えい等が発生した場合の措置について

事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、その個人情報の本人が適切に対応できるようにするため、事実関係を本人に速やかに通知または容易に知りうる状態に置くもの

とした。(「容易に知りうる状態に置く」とはウェブ画面上のわかりやすい場所に継続的に表示することや、専用のフリーダイヤル設置などをいう)。また二次被害の拡大、類似事故の発生回避のため、事実関係、発生原因、対応策等を所管省庁に届け出るとともに可能な限りホームページ、マスメディア等にて公表するものとした。事業者は事故発生に備え、あらかじめ緊急事態対応体制を構築し、不測時の対応業務につきマニュアルを整備するなど日頃から準備しておくことが望ましい。

1.3.5 「保護法」の適用範囲について

電子商取引はグローバル化が進んでいるが、「保護法」は国境を越えた商取引についても適用される。したがって海外に居住する消費者などとの取引に際しては全て国内のそれと同様の法的義務が伴うことを認識し、言語対応についても十分配慮し本人の権利に対し誠実に応えていくことが望まれる。逆にわが国の事業者が外国においてネットビジネスを展開する場合などにおいては当該国の個人情報保護にかかわる法規制を受けることになるので注意が必要である。

1.3.6 監査責任者の設置について

昨今の個人情報漏洩事故頻発状況に鑑み、事業者の代表者は、自社の個人情報保護推進体制の妥当性、有効性および実施状況について適正な監査を実施する者を指名し、当該業務を行わせることが望ましい。事業者の代表者により指名された個人情報保護監査責任者は、自社の個人情報保護推進体制の整備と日常の業務管理が的確に行われているか否かを定期的に監査する責務を負うこととする。個人情報保護監査責任者は個人情報保護体制の妥当性、有効性および実施状況をチェックする立場となるため、個人情報保護管理者がこれを兼務することはできない旨付記した。

1.3.7 「個人情報の保護に関する法律」に基づく公表等事項（サンプル）について

「保護法」では事業者に対し自社の個人情報保護に関するいくつかの事項について公表（または通知）することを求めている。本ガイドラインでは事業者が公表（または通知）すべき事項についてそのサンプルを提示し各事業者の便宜を図っている。なお、記載内容はあくまで例であり各事業者が自社の実情に合わせ自由に変更または省略、追加することができるものである。

1.4 改訂作業を終えて

今年４月の「保護法」全面施行を控え、各事業者は今、体制整備の真っ只中にいる。しかしながら「保護法」の要求するレベルは必ずしも客観的に明確になっている訳ではなく、事業者の対応も、不安を抑えながら、かつ自問自答しながら進めている様子が垣間見られる。法律はともかくとしてガイドラインについては経済産業省も引続きフォローしていくとしているため、依然として事業者、行政、関連団体の連携が重要であることは疑いのないところである。ここで今後の課題としていくつかの論点を例示してみたい。

1.4.1 **従業者個人が保有・管理している個人情報をどう取り扱うか。**

保護法、ガイドラインでは個人情報の定義を「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。）」としているが、これによれば従業者が個人的に取り扱う顧客個人情報も保護法の対象になるものと考えられる。
しかしながら日々増減する個人情報の全てを（開示請求に応えられるよう）正確にかつ一元的に管理するには膨大な費用と工数をかかることになり事業者にとって大きな負担となることが予想される。コスト（業務効率の低下を含め）とリスクのバランスを考えた場合、一定の割り切りが必要になろうがその線引きについては社会的なコンセンサスがあるとよい。

1.4.2 **一体的な経営管理を行っている子会社（１００%出資、冠会社等）との間であっても第三者提供に該当し本人の事前同意が必要か。**

METI ガイドラインによれば「親子兄弟会社、グループ会社の間で個人データを交換する場合」は第三者提供とされるとあり、あらかじめ本人同意が必要とされている。しかしながら同一企業であれば「異なる事業部門間でも原則利用自由」が一旦子会社化された途端本人同意が必要というのは著しく業務効率を損ねかねない。また「共同利用」のスキームを使うことも考えられるが利用目的、利用データ項目、利用者範囲、責任者等について本人通知もしくは容易に知り得る状態に置くことが条件となっており、その利用にあたっては制約が大きい。グループ会社であって一定の条件を満たした場合は公表を前提に同一企業と同様の運用が認められないだろうか。

1.4.3 **情報資産の暗号化、パスワード設定はどう評価されるか。**

PC 等情報資産の盗難・紛失事故件数は保護法施行が目前に迫った今日でも鎮静化の兆しが見えない（一説によれば実際の発生件数は報告されている件数の十倍とも二十倍とも言われている）。この場合、個人情報保護対策上もっとも適切な手段は暗号化、パスワード設定による部外者からの情報資産ガードである。実際、暗号化、パスワードが設定されておれば解除手段が同時に盗難・紛失していない限り特定個人の識別は不可能であり、その時点では個人情報に該当しないという解釈もありうる。万一事故にあった際でも解除手段が安全に管理されている場合には当面二次被害は回避されるものとして、暗号化・パスワード設定に対する社会的評価と導入インセンティブを高めていく方策が望まれる。

1.4.4 **個人情報を伴う業務委託において受託者側が一方的に負担を負うことはないか。**

保護法には「個人情報保護取扱事業者は個人データの取り扱いの全部または一部を委託する場合は、その取り扱いを委託した個人データの安全管理が図られるよう、受託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。」とあるが、これが行き過ぎると委託者が受託者に対し過度の負担を課すことも考えられる。実際に委託者･受託者間で締結される業務委託契約で個人情報漏えい事故に係る損害賠償額（逸失利益、情報主体に対するお詫び料等を含む）については上限なしとするケースも散見されるが、METI ガイドラインにある「優越的地位にあるものが委託者の場合、受託者に不当な負担を課すことがあってはならない」について具体的な基準つくりが必要ではないだろうか。

以上いくつか当 WG の中で提起された論点を挙げてみたが、いずれも当事者たる事業者にとっては悩ましい問題であるが簡単にカタがつくものでもないように思われる。幸い経済産業省では昨年 10 月に公表したガイドラインについて随時見直しを行っていくとしているので ECOM においても関連部門と連携を取りながら更なる改訂を検討していきたい。なお、
今年度改訂を行ったＥＣＯM個人情報保護ガイドライン（Ver.3.0）については巻末のその全文を掲載したので適宜ご参照いただきたい。

2. ＥＣＯＭ会員企業、ＥＣ事業者の個人情報保護に関する実態調査

2.1 調査の全体概要

ＥＣＯＭでは昨年度に引続き個人情報保護に関する事業者の取組み状況に関する実態調査を行った。
調査の内容は
① ＥＣＯＭ会員企業ホームページ目視調査
② ＥＣＯＭ会員企業に対する個人情報保護に関するアンケート調査
③ ＥＣ事業者に対する個人情報保護に関するアンケート調査
でいずれも 2004 年（平成 16 年）８月から９月にかけて行った。以下調査ごとにその結果を概観する。上記のうち「ＥＣ事業者に対する個人情報保護に関するアンケート調査」については日本商工会議所様の協力を得て同所が付与しているオンラインショッピングトラストマーク取得事業者を対象としたものであり今年度初めての取組みであることを付記しておきたい。また本調査は前述のように昨年 8 月から 9 月にかけて行ったものであるがその後、本年 4 月の「保護法」全面施行に向けて各事業者の精力的な取組みが続いており、3 月現在ではさらに相当進んでいることも念頭において評価する必要がある。

2.2 ＥＣＯＭ会員企業ホームページ目視調査

2.2.1 ECOM 会員企業目視調査の概要

今年度のＥＣＯＭ会員企業ホームページ目視調査の概要と調査結果は以下の通りである。

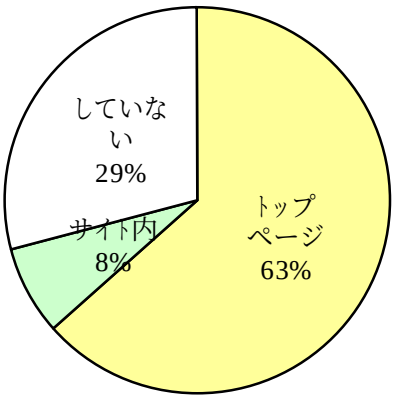
（1）調査対象：ECOM 会員企業（理事会員、A 会員、B 会員）全社
(2) 調査方法：会員各社のホームページ目視による調査
（3）調査実施期間：2004 年 8 月 26 日～9 月 3 日
（4）調 査 数：213 社

	前年より継続	04 年新規	合計
2004 年度	199 社	14 社	213 社

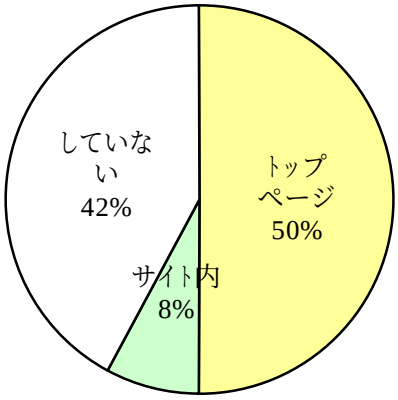
2.2.2 ECOM 会員企業目視調査の結果

(1) ホームページ上に表記している企業･団体

【2004 年度】



【2003 年度】



- 表記している企業･団体数
  2004 年度：151 社（71%）（2003 年度：140 社（58%）、＋11 社（＋13%））
- トップページに表記：135 社（2003 年：121 社、＋14 社）
- サイト内に表記：16 社（2003 年：17 社、▲1 社）

＜調査結果＞

ホームページ上に何らかの形でプライバシーポリシーに関する記述がある企業は、昨年の 58%から 71%に増加しており、公表意識の着実な浸透を裏付けている。

今年 6 月に公表された METI ガイドラインではプライバシーポリシーを公表することが望ましいとしており、今後この比率が一層高まることが期待される。

(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

	企業･団体名
1	アコム株式会社
2	株式会社NTTデータ
3	株式会社オーエムシーカード
4	沖電気工業株式会社
5	株式会社ジェーシービー
6	株式会社東芝
7	トヨタ自動車株式会社
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	株式会社日立製作所
13	株式会社富士総合研究所
14	富士通株式会社
15	富士電機ホールディングス株式会社
16	マイクロソフト株式会社
17	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
18	松下電器産業株式会社
19	三菱商事株式会社
20	株式会社三菱総合研究所
21	三菱電機株式会社
22	株式会社UFJ銀行
23	株式会社SRAセキュリティ
24	株式会社アイネス
25	アクセンチュア株式会社
26	アップルコンピュータ株式会社
27	株式会社アプラス
28	株式会社アルゴ21
29	株式会社インテックコミュニケーションズ
30	NECソフト株式会社
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	株式会社エヌ･ティ･ティ･データ経営研究所
34	株式会社NTTドコモ
35	株式会社FFC
36	株式会社オリエントコーポレーション
37	花王インフォネットワーク株式会社
38	川鉄情報システム株式会社
39	共同印刷株式会社
40	KDDI株式会社
41	コンピュータ･アソシエイツ株式会社
42	佐川急便株式会社
43	三洋電機株式会社
44	株式会社シー･アイ･シー
45	株式会社シーフォーテクノロジー
46	新日鉄ソリューションズ株式会社
47	スターリングコマース株式会社
48	セコム株式会社
49	セコム情報システム株式会社
50	株式会社セントラルファイナンス
51	株式会社損害保険ジャパン
52	大日本印刷株式会社
53	中部電力株式会社
54	株式会社テプコシステムズ
55	東北電力株式会社
56	凸版印刷株式会社
57	日本信販株式会社
58	ニフティ株式会社
59	株式会社日本総合研究所
60	日本電子計算機株式会社
61	日本電信電話株式会社
62	日本ベリサイン株式会社
63	日本ユニシス情報システム株式会社
64	東日本電信電話株式会社
65	株式会社日立情報システムズ
66	日立ｿﾌﾄｳｪｱｴﾝｼﾞﾆｱﾘﾝｸﾞ株式会社
67	富士通エフ･アイ･ピー株式会社

	企業･団体名
68	株式会社富士通総研
69	株式会社富士通中部システムズ
70	富士電機情報サービス株式会社
71	三井住友海上火災保険株式会社
72	三菱電機情報ネットワーク株式会社
73	株式会社メイテツコム
74	株式会社UFJカード
75	ユーシーカード株式会社
76	イオンクレジットサービス株式会社
77	伊藤忠商事株式会社
78	株式会社イプシ･マーケティング研究所
79	株式会社インテリジェントウェイブ
80	株式会社SRA
81	NECインフロンティア株式会社
82	NEC情報システム株式会社
83	NECトータルインテグレーションサービス株式会社
84	NECネクサソリューションズ株式会社
85	エヌ･ティ･ティ･リース株式会社
86	株式会社エヌ･ティ･ティ･ロジスコ
87	カシオ計算機株式会社
88	関西電力株式会社
89	九州電力株式会社
90	グローバルセキュリティエキスパート株式会社
91	株式会社構造計画研究所
92	国内信販株式会社
93	佐川ｺﾝﾋﾟｭｰﾀ･システム株式会社
94	株式会社さくらケーシーエス
95	四国電力株式会社
96	株式会社資生堂
97	シャープ株式会社
98	株式会社ジャックス
99	株式会社ジャルカード
100	昌栄印刷株式会社
101	セイコーインスツルメンツ株式会社
102	セイコープレシジョン株式会社
103	株式会社ｿﾆｰﾌｧｲﾅﾝｽｲﾝﾀｰﾅｼｮﾅﾙ
104	ソラン株式会社
105	株式会社第一勧銀情報システム
106	TIS株式会社
107	株式会社ティージー情報ネットワーク
108	株式会社電通国際情報サービス
109	東芝情報システム株式会社
110	東芝テック株式会社
111	東芝ファイナンス株式会社
112	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
113	日本データカード株式会社
114	日本電気エンジニアリング株式会社
115	日本認証サービス株式会社
116	パシフィックシステム株式会社
117	株式会社パワードコム
118	株式会社BSNアイネット
119	日立キャピタル株式会社
120	株式会社ビック東海
121	株式会社フジサンケイリビングサービス
122	富士写真フィルム株式会社
123	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
124	富士通ソーシアルサイエンスラボラトリ
125	株式会社富士通長野システムエンジニアリング
126	株式会社富士通ハイパーソフトテクノロジ
127	株式会社富士通ビジネスシステム
128	株式会社富士通北陸システムズ
129	ブラザー工業株式会社
130	三谷産業株式会社
131	三井住友カード株式会社
132	三菱電機インフォメーションシステムズ株式会社
133	ヤマトシステム開発株式会社
134	横河電機株式会社
135	株式会社菱化システム

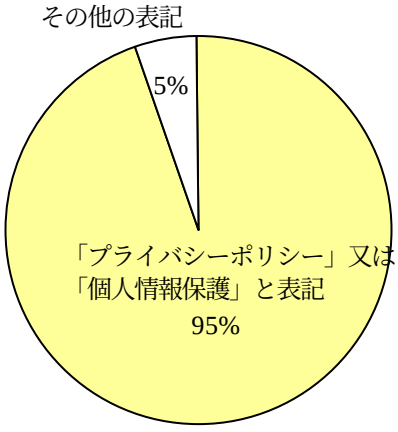
(3) トップページにリンクボタンはないが、サイト内に表示している会員・団体

	企業･団体名
1	伊藤ハム株式会社
2	東京電力株式会社
3	社団法人日本自動車工業会
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	株式会社オージス総研
8	株式会社ＱＵＩＣＫマネーラインテレレート
9	興和株式会社
10	株式会社小松製作所
11	ダイセル化学工業株式会社
12	大日本インキ化学工業株式会社
13	中国電力株式会社
14	財団法人日本品質保証機構
15	農林中央金庫
16	日立電線株式会社

＜調査結果＞

HP 閲覧者に個人情報取扱事業者のプライバシーポリシーの有無等を確認させる上で、トップページに何らかの表示（リンクボタン）を行うことはきわめて重要である。トップページにリンクボタンはないが、後方ページでプライバシーポリシーを説明している企業が十数社あるが、HP 閲覧者への認識度を高めるためにはトップページから一回のクリックでアクセスできる配慮が望まれる。

(4) プライバシーポリシーの表記



- その他の表記：8 社
- 表記例
  - ・サイトポリシー
  - ・情報資産保護
  - ・ご利用規約
  - ・ご利用上の注意
  - ・情報利用に際してのお願い
  - ・ご利用にあたって

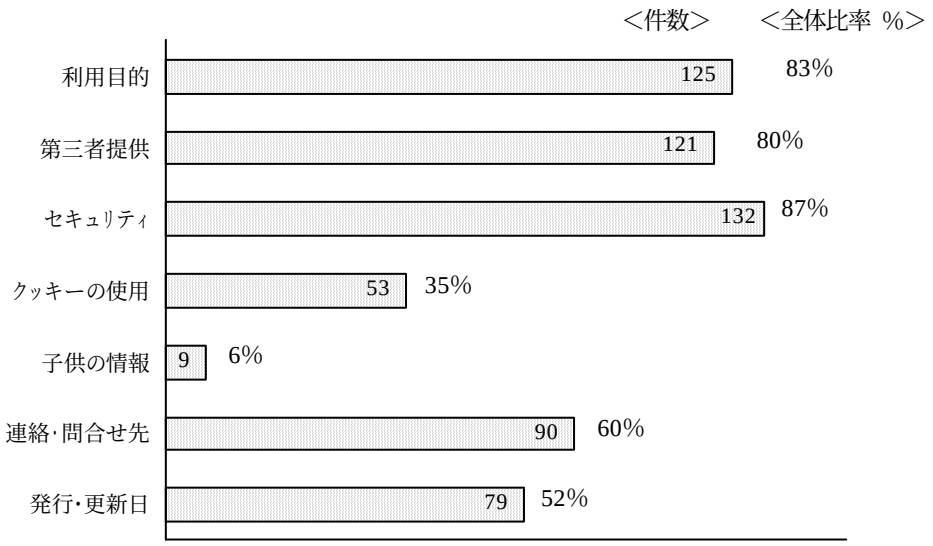
（※株式会社 SRA セキュリティは英文表記）

＜調査結果＞

プライバシーポリシー（または個人情報保護方針等）の表記にあたり、一部の企業では「ご利用にあたって」「ご利用上の注意」等の表現を用いているが、「プライバシーポリシー」「個人情報

保護方針」との文言で明確に表示し、その存在を明確に知らしめることが望まれる。

（5）盛り込まれている内容（全体＝151 社）



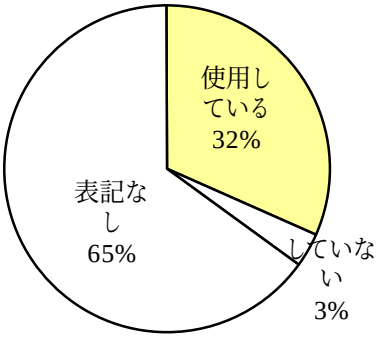
- 利用目的　　：125 社（2003 年：101 社、＋24 社）
- 第三者提供　　：121 社（2003 年：110 社、＋11 社）
- セキュリティ　　：132 社（2003 年：123 社、 ＋9 社）
- クッキー使用　　： 53 社（2003 年： 45 社、 ＋8 社）
- 子供の情報　　： 9 社（2003 年： 11 社、 ▲2 社）
- 連絡・問合せ先　： 90 社（2003 年： 88 社、 ＋2 社）
- 発行・更新日　　： 79 社（2003 年： 59 社、＋20 社）

＜調査結果＞

プライバシーポリシーに含まれる内容は上記の通りであり、セキュリティ、利用目的、第三者提供に関する事項が上位 3 位を占める。昨年度調査に比較すると利用目的に関する事柄、発行・更新日等の記載が増加しており全般的に内容は充実してきている。

連絡・問合せ窓口、クッキーの使用、子どもからの情報収集を含め、上記項目はいずれもプライバシーポリシーの重要な構成要素であり簡潔で分かりやすい表記が望まれる。

（6）プライバシーポリシーを表記している企業･団体のうち、クッキーを使用している割合
（全体＝151 社）

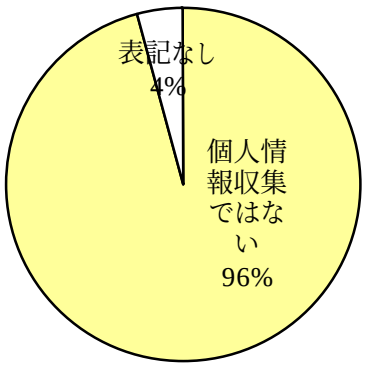


- クッキーを使用していると表記　：48 社（32%）　（2003 年：39 社、＋9 社）
- 使用していないと表記　：5 社（ 3%）　（2003 年： 6 社、▲1 社）

＜調査結果＞

クッキーに関する記述は、「使用している」「していない」の両者合計で、全体の 35%にとどまっているが、同じ母集団でのアンケート調査ではその利用率は 50%を越えている。もしクッキーを利用しているのであれば、その利用方法、情報主体が利用されることを望まない場合にそれを無効にする方法等につき表記をすることが強く望まれる。

（7）クッキー使用の目的（全体＝48 社）



- クッキー利用は個人情報収集のためとの表記：０件
- 個人情報収集ではないとの表記：46 件
- 表記なし：2 件

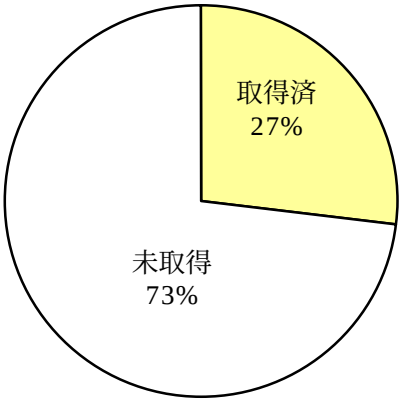
＜調査結果＞

目視調査から見る限り、クッキーの利用はあくまでもサイト訪問者の利便性向上やサイトプラン改善等の利用に限定されており、個人情報として収集もしくは個人情報と結びつけて取り扱っている例はない。

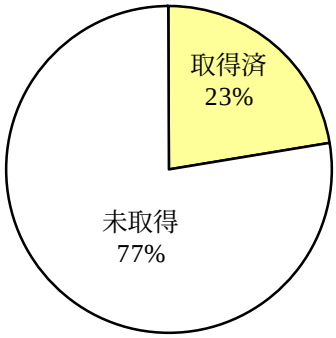
3. プライバシーマークについて

(1) プライバシーマークを取得している企業･団体の比率

【2004 年度】



【2003 年度】



- 取得企業：58 社 27% （2003 年：23%、＋4%）

＜調査結果＞

ECOM 会員でプライバシーマーク取得事業者は 58 社で､昨年度に比べ 2 社増加となっており､取得率は 23% → 27%へと上昇した。

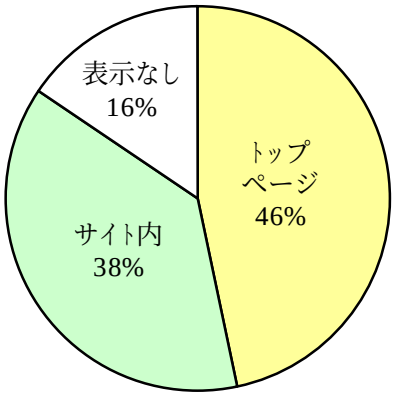
(2) プライバシーマークを取得している企業･団体

	企業･団体名
1	アコム株式会社
2	株式会社NTTデータ
3	株式会社オーエムシーカード
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	マイクロソフト株式会社
11	松下電器産業株式会社
12	株式会社三菱総合研究所
13	株式会社アイネス
14	株式会社アルゴ21
15	NECソフト株式会社
16	NTTコムウェア株式会社
17	川鉄情報システム株式会社
18	共同印刷株式会社
19	新日鉄ソリューションズ株式会社
20	大日本印刷株式会社
21	株式会社テプコシステムズ
22	凸版印刷株式会社
23	ニフティ株式会社
24	株式会社日本総合研究所
25	日本ユニシス情報システム株式会社
26	株式会社日立情報システムズ
27	日立ソフトウェアエンジニアリング株式会社
28	富士通エフ･アイ･ピー株式会社
29	三菱電機情報ネットワーク株式会社

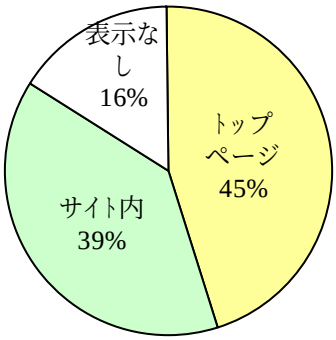
	企業･団体名
30	イオンクレジットサービス株式会社
31	株式会社インテリジェントウェイブ
32	株式会社SRA
33	NECトータルインテグレーションサービス株式会社
34	NECネクサソリューションズ株式会社
35	株式会社構造計画研究所
36	佐川ｺﾝﾋﾟｭｰﾀ･システム株式会社
37	株式会社さくらケーシーエス
38	株式会社資生堂
39	昌栄印刷株式会社
40	ソラン株式会社
41	株式会社第一勧銀情報システム
42	TIS株式会社
43	株式会社電通国際情報サービス
44	東芝情報システム株式会社
45	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
46	パシフィックシステム株式会社
47	株式会社BSNアイネット
48	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
49	株式会社富士通ビジネスシステム
50	三谷産業株式会社
51	三井住友カード株式会社
52	ヤマトシステム開発株式会社
53	株式会社菱化システム
54	株式会社インテージ
55	株式会社オージス総研
56	株式会社エネルギア･コミュニケーションズ
57	キーウェア ソリューションズ株式会社
58	日立ビジネスソリューション株式会社

(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（全体＝58 社）

【2004 年度】



【2003 年度】



- トップページ表記　：27 社（2003 年：25 社、＋2 社）
- サイト内に表記　　：22 社（2003 年：22 社、―）
- 表示なし　　： 9 社（2003 年： 9 社、―）

＜調査結果＞

プライバシーマーク取得事業者でホームページ上にてマークを確認できたのは 49 社、

できなかった取得事業者は 9 社である。取得を強くアピールするためにもホームページ（とりわけトップページ）上での視認性の高い掲示が欲しいものである。

(4) プライバシーマークをトップページに表示している企業･団体

	企業･団体名
1	アコム株式会社
2	株式会社オーエムシーカード
3	株式会社富士総合研究所
4	株式会社三菱総合研究所
5	株式会社アイネス
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	イオンクレジットサービス株式会社
13	株式会社ＳＲＡ
14	ＮＥＣトータルインテグレーションサービス株式会社
15	ＮＥＣネクサソリューションズ株式会社
16	佐川ｺﾝﾋﾟｭｰﾀ･システム株式会社
17	株式会社さくらケーシーエス
18	昌栄印刷株式会社
19	ソラン株式会社
20	株式会社第一勧銀情報システム
21	株式会社電通国際情報サービス
22	東芝情報システム株式会社
23	株式会社富士通ビジネスシステム
24	三井住友カード株式会社
25	ヤマトシステム開発株式会社
26	株式会社菱化システム
27	株式会社オージス総研

(5) サイト内に表示している企業･団体

	企業･団体名
1	株式会社東芝
2	日本電気株式会社
3	株式会社野村総合研究所
4	株式会社日立製作所
5	株式会社アルゴ21
6	ＮＴＴコムウェア株式会社
7	新日鉄ソリューションズ株式会社
8	凸版印刷株式会社
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	株式会社インテージ
12	株式会社インテリジェントウェイブ
13	株式会社エネルギア･コミュニケーションズ
14	キーウェア ソリューションズ株式会社
15	株式会社構造計画研究所
16	株式会社資生堂
17	ＴＩＳ株式会社
18	株式会社日本ｼｽﾃﾑﾃﾞｨﾍﾞﾛｯﾌﾟﾒﾝﾄ
19	パシフィックシステム株式会社
20	株式会社BSNアイネット
21	株式会社富士通ｼｽﾃﾑｿﾘｭｰｼｮﾝｽﾞ
22	三谷産業株式会社

2.3 ＥＣＯＭ会員企業に対するアンケート調査

2.3.1 ＥＣＯＭ会員企業に対するアンケート調査の概要

（1）アンケート調査時期…… 2004 年 8 月 31 日～9 月 13 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 213 社）

（3）回答希望部門 ‥個人情報保護担当部門、法務部門、情報システム部門、コンプライアンス対応部門等、個人情報保護に深く関わっている部門の方

（4）有効回答数…… 64 件（回収率：30%）

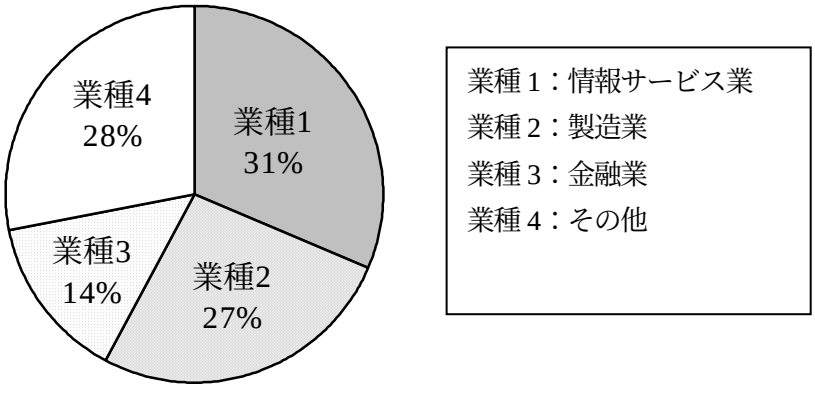
（5）回答業種別分類

ご回答頂いた業種	件数	分類業種	件数
情報サービス業	18	業種 1 情報サービス業	20
その他情報サービス業	2		
製造業（電気機器・精密機器）	8	業種 2 製造業	17
その他製造業	9		
金融・保険業	9	業種 3 金融業	9
電力･ガス業	6	業種 4 その他	18
卸売業	2		
運輸・倉庫業、マスコミ、エンタテイメント その他	10		
合　計	64	合　計	64

（6）昨年度回答企業・団体との件数比較

	2 年連続回答	04 年のみ回答	合計
2004 年度	32 社（50%）	32 社（50%）	64 社

■アンケート回答会社業種分類（有効回答数＝64 社）

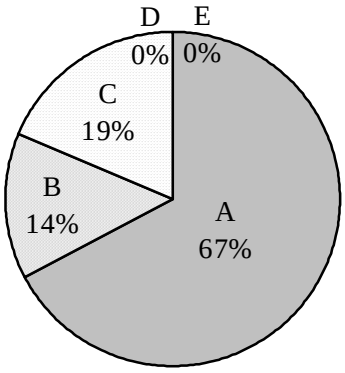


2.3.2 ＥＣＯＭ会員企業に対するアンケート調査の結果

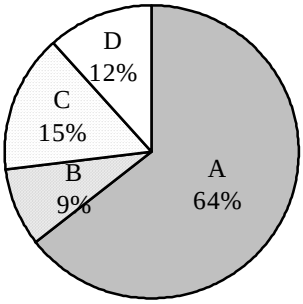
Q1. 貴社には個人情報保護に関する社内規定がありますか？（有効回答数＝64）

① 全業種合計

【2004 年度】



【2003 年度】

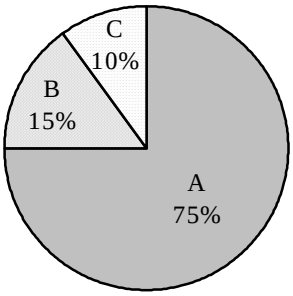


A： 個人情報保護に関する全社規程がある
B： 各内規の節々に個人情報の取扱いについての規定が散在している、あるいは各部門にてまちまちではあるが規定を定めているところもある
C： 今はないが、今後策定しようと考えている
D： ない
E： その他（自由記入）

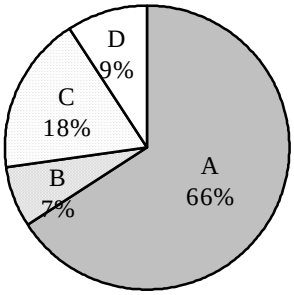
② 業種別

＜情報サービス業＞

【2004 年度】

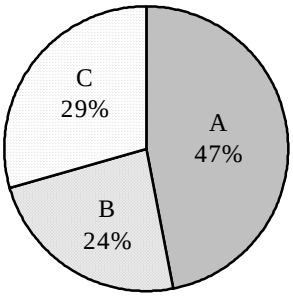


【2003 年度】

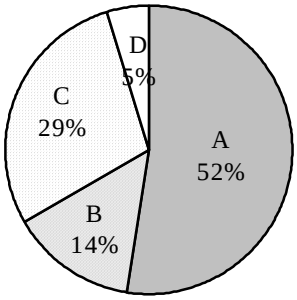


＜製造業＞

【2004 年度】

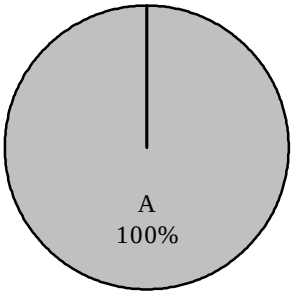


【2003 年度】

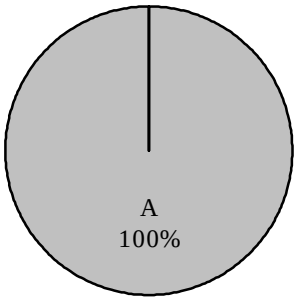


＜金融業＞

【2004 年度】

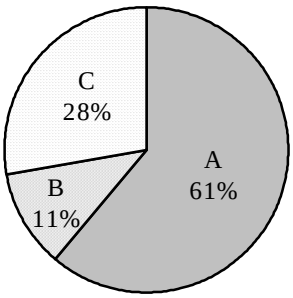


【2003 年度】

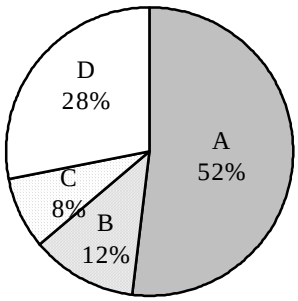


＜その他＞

【2004 年度】



【2003 年度】



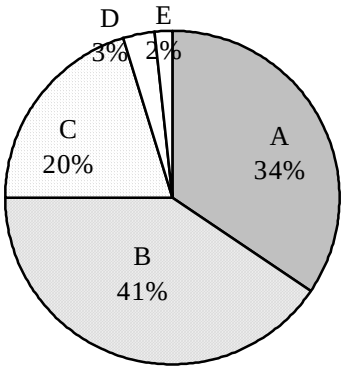
③ 調査結果

社内規程の有無については 81%の企業が「有り」としており、その整備は着実に進んでいる様子がうかがえる。特に前年度には「社内規程はない」が 12%あったが今回は皆無であった。業種別に見ると以前から整備が先行している金融業以外に情報サービス業、その他業種で取り組みが進んだ。

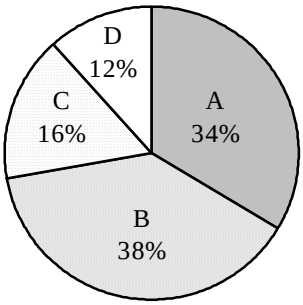
Q2. **貴社には個人情報保護体制の構築・管理を行なう個人情報保護管理者の指名あるいは担当部門の設置はなされていますか? （有効回答数＝64）**

① 全業種合計

【2004 年度】



【2003 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、または部門内に当該担当や職務を割り当てている
C： 今はないが、今年度中に任命あるいは設置しようと考えている
D： ない
E： その他（自由記入）

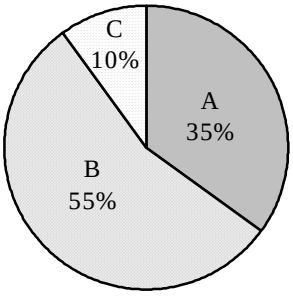
＜その他（自由記入）＞

- 全社的な推進を行なう管理者を指名（兼務）し、その管理者が所管する部門に事務局を専任で置いている。
- セキュリティ対策として情報管理者を任命しようと考えている。

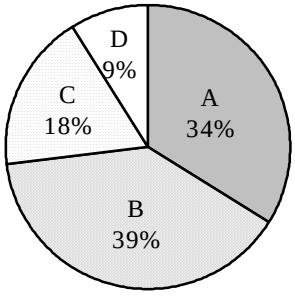
② 業種別

＜情報サービス業＞

【2004 年度】

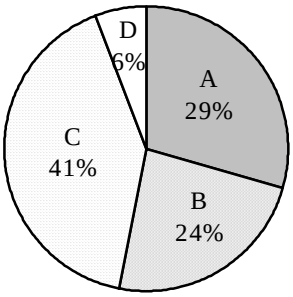


【2003 年度】

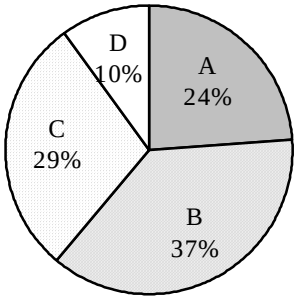


＜製造業＞

【2004 年度】

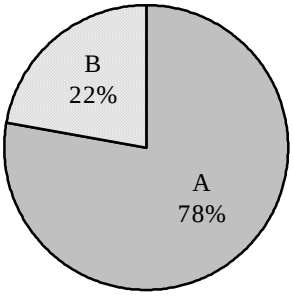


【2003 年度】

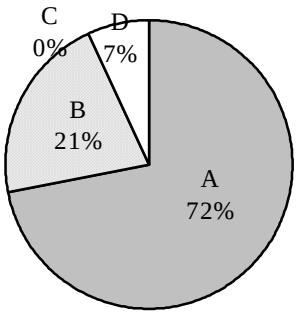


＜金融業＞

【2004 年度】

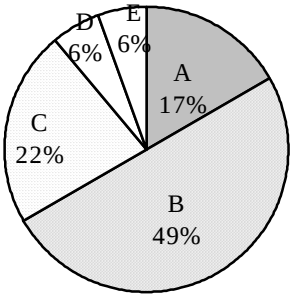


【2003 年度】

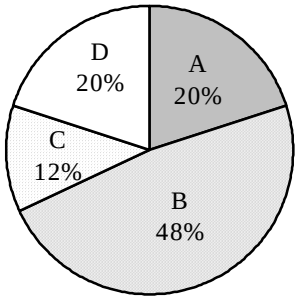


＜その他＞

【2004 年度】



【2003 年度】



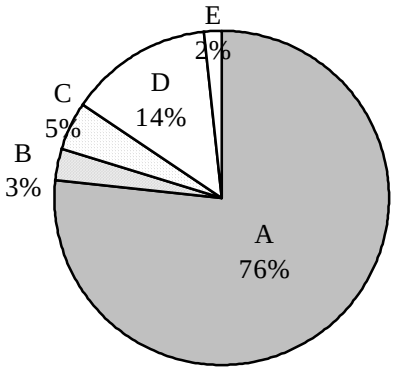
③ 調査結果

前項と同様に体制明確化が着実に進んでいる。個人情報保護を含めた情報セキュリティという範疇で役割（CISO= Chief　Information Security Officer）を明確化する動きも見受けられる。

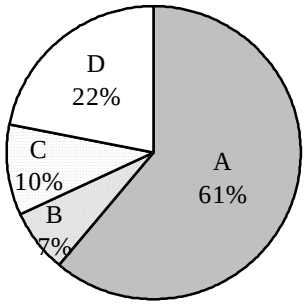
Q3. **貴社では顧客の個人情報を直接的に収集することがありますか？（従業者に関する個人情報は除く）　（有効回答数＝64）**

① 全業種合計

【2004 年度】



【2003 年度】



A： サイトから、およびサイト以外からの両方の方法で収集している
B： サイトからのみ収集している
C： サイト以外から収集している
D： 顧客の個人情報を収集することはない
E： その他（自由記入）

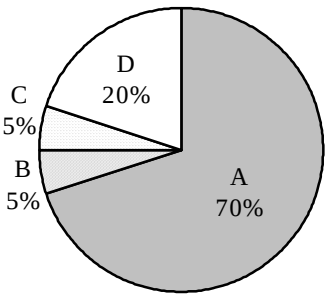
＜その他（自由記入）＞

- 開示の際の申込書記載
- 説明会でのアンケート

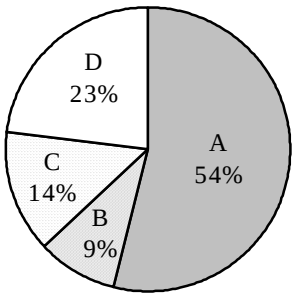
② 業種別

＜情報サービス業＞

【2004 年度】

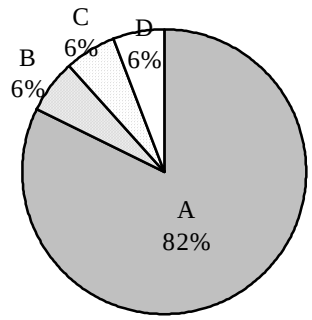


【2003 年度】

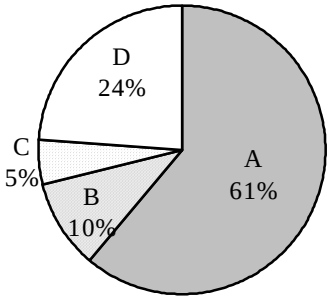


＜製造業＞

【2004 年度】

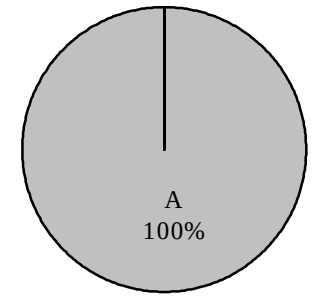


【2003 年度】

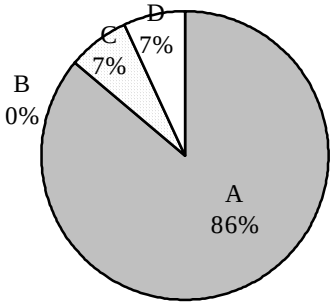


＜金融業＞

【2004 年度】

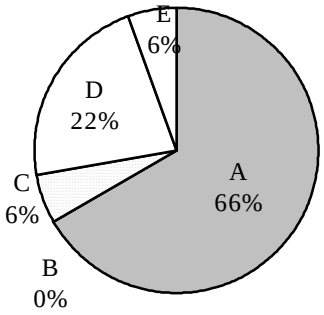


【2003 年度】

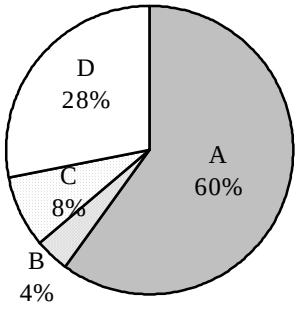


＜その他＞

【2004 年度】



【2003 年度】

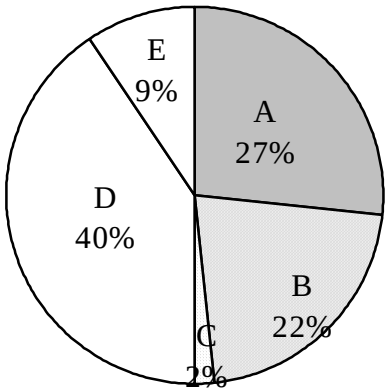


③ 調査結果

全業種を通じて「サイトおよびサイト以外の両方から情報を収集している」との回答が増加しており個人情報収集活動に対する認識が高まりつつあるが、特に金融業ではすべてが「サイトおよびサイト以外の両方から収集」としている。他方「個人情報を収集することはない」とする回答は減少してきている。

Q4. **貴社では顧客の個人情報を間接的に収集（個人情報取扱業務を受託する場合を除く）することがありますか？　（有効回答数＝64）**

① 全業種合計



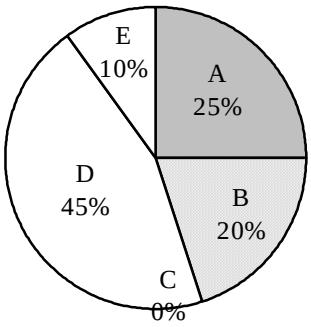
A： 個人情報の収集を他社に委託することがある
B： インターネット、電話帳、職員録等公開情報から収集することがある
C： 専門業者から名簿等を購入することがある
D： 間接収集することはない
E： その他（自由記入）

＜その他（自由記入）＞

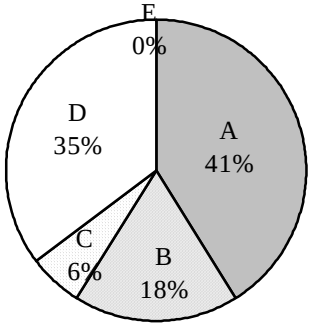
- 信用情報機関および企業信用調査会社から取得。
- 当社が顧客のシステムを開発するに際し、その顧客より「顧客の顧客（個人）情報」をテストデータ等の形で入手することがある。

② 業種別

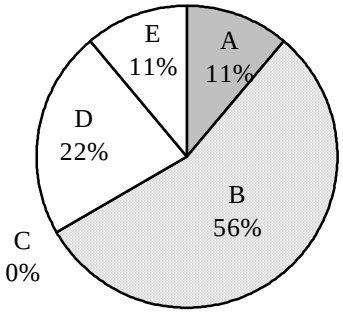
＜情報サービス業＞



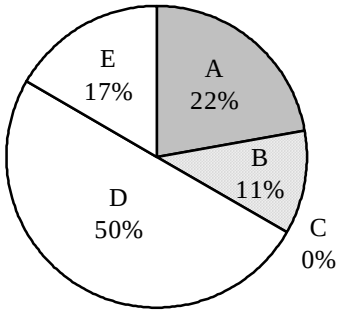
＜製造業＞



＜金融業＞



＜その他＞

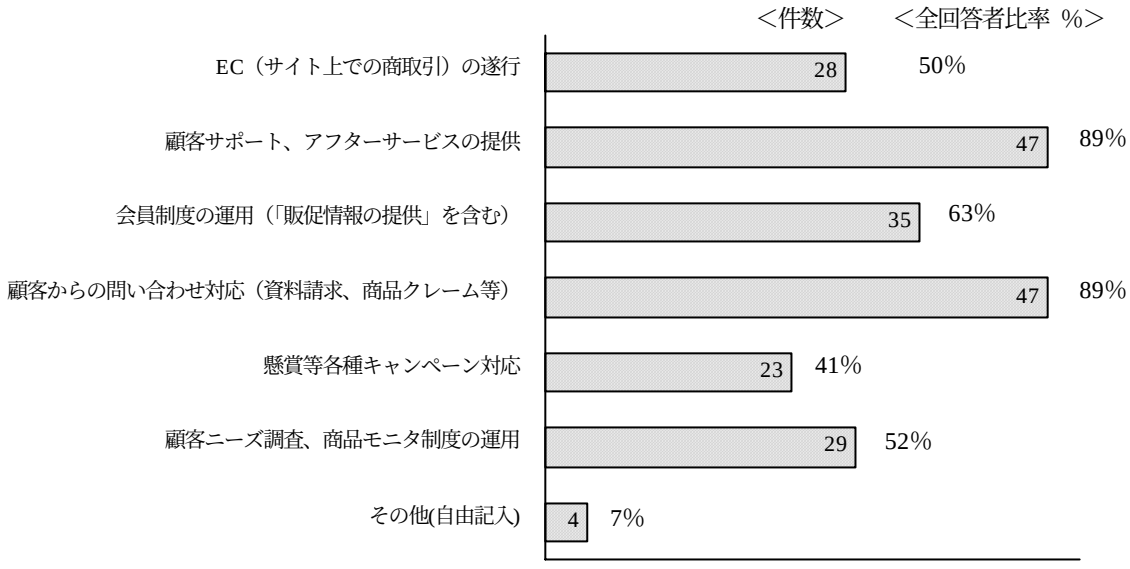


③ 調査結果

約半数の 51%が何らかの方法で間接収集を行っているとしている。業種別に見ると金融業では公開情報から、製造業では委託を通じた収集が多いことが特徴である。一方、「間接収集はなし」とする回答は 40%となっている。

Q5. **（問 3、問 4 の** a.b.c.**回答者）貴社の収集する顧客の個人情報の利用目的について、以下の中から該当するものを選択してください。（有効回答数＝56）【複数回答可】**

① 全業種合計



＜その他（自由記入）＞

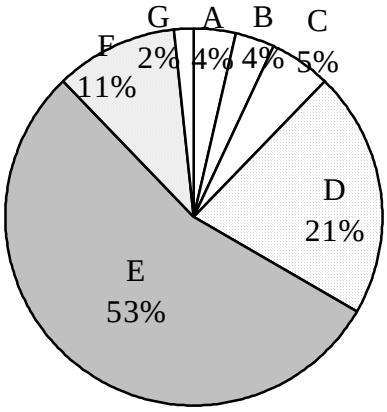
- 与信および契約後の管理
- 料金の徴収、採用
- C／S 調査の実施
- 消費者（借入者）の支払能力の調査のため

② 調査結果

個人情報の利用目的として多いのは「顧客サポート、アフターサービスの提供」「顧客からの問い合わせ対応」でいずれも 47 件（全回答者の 89%）の回答があった。一方「会員制度の運用」や「顧客ニーズ、商品モニタ制度の運用」「懸賞等各種キャンペーン対応」など販売促進に直結する「攻め」の利用についても 35 件（63%）～23 件（41%）と底堅いものがある。その他としては与信管理などがある。

Q6. **（問 3､問 4 の a.b.c.回答者）現在収集している個人データ（収集した個人情報をデータとして取り扱っているもの）は何件くらいありますか？**
（この設問のみ「従業者の個人データ」を含めてご回答下さい）　（有効回答数＝57）

① 全業種合計



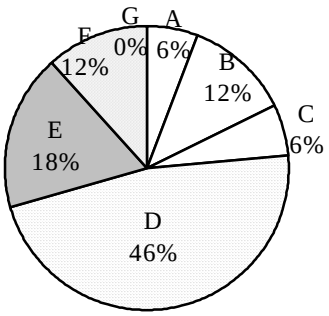
A： 1000 件未満
B： 1000 件以上 5000 件未満
C： 5000 件以上 1 万件未満
D： 1 万件以上 10 万件未満
E： 10 万件以上
F： 分からない
G： その他（自由記入）

＜その他（自由記入）＞

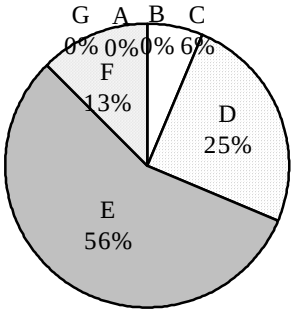
- 物流にて利用する個人データのため、流動性がある。

② 業種別

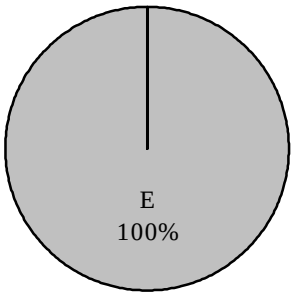
＜情報サービス業＞



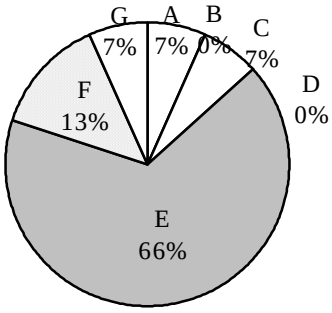
＜製造業＞



＜金融業＞



＜その他＞

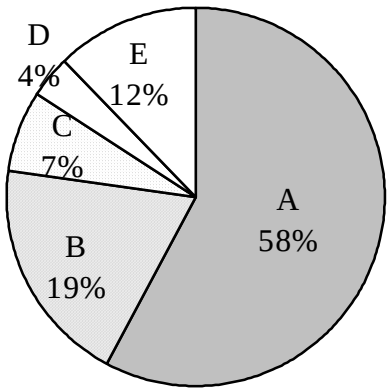


③ 調査結果

保有個人データ件数については 10 万件以上が約半数以上を占め、1 万件以上までを含めると 74%となる。また「保護法」適用ラインの 5 千件までを含めると約 8 割がその対象となる。さらに回答の中に「分からない(調査中)」との回答が 11%あり、実際にはその多くが保護法適用対象となるものと推測される。

Q7. **（問 3､問 4 の** a.b.c.**回答者）顧客から個人情報を直接収集する際、利用目的を通知または公表していますか？　　（有効回答数＝57）**

① 全業種合計



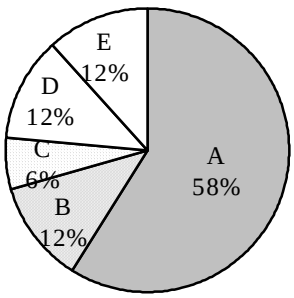
A： 利用目的を伝え、かつ同意を得て収集している
B： 利用目的を伝えた上で収集している（同意は得ていない）
C： 収集しているが利用目的を伝えていない
D： 収集していない
E： その他(自由記入)

＜その他（自由記入）＞

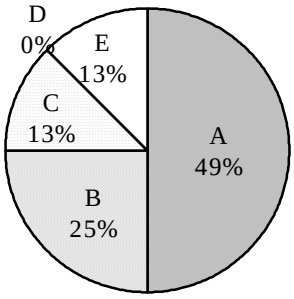
- 収集時に利用目的を伝えていないが、公表をしている。
- 利用目的および提供をもって同意とする旨を表示している。
- A．B．両方のケースがある。
- 利用目的を明示し、同意を得て取得している。
- 個々に A～C の形があり、現段階では全社的な統一をしていない。
- 一部利用目的を伝え、かつ同意を得て収集している。
- 一部利用目的を伝えていないものもある。

② 業種別

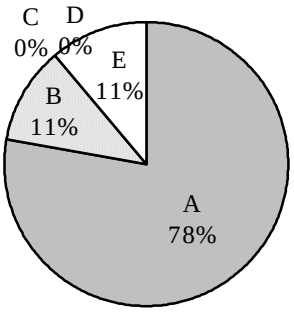
＜情報サービス業＞



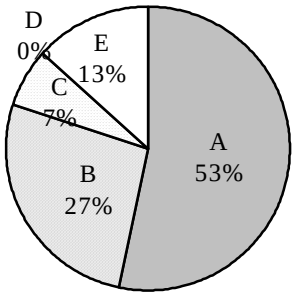
＜製造業＞



＜金融業＞



＜その他＞

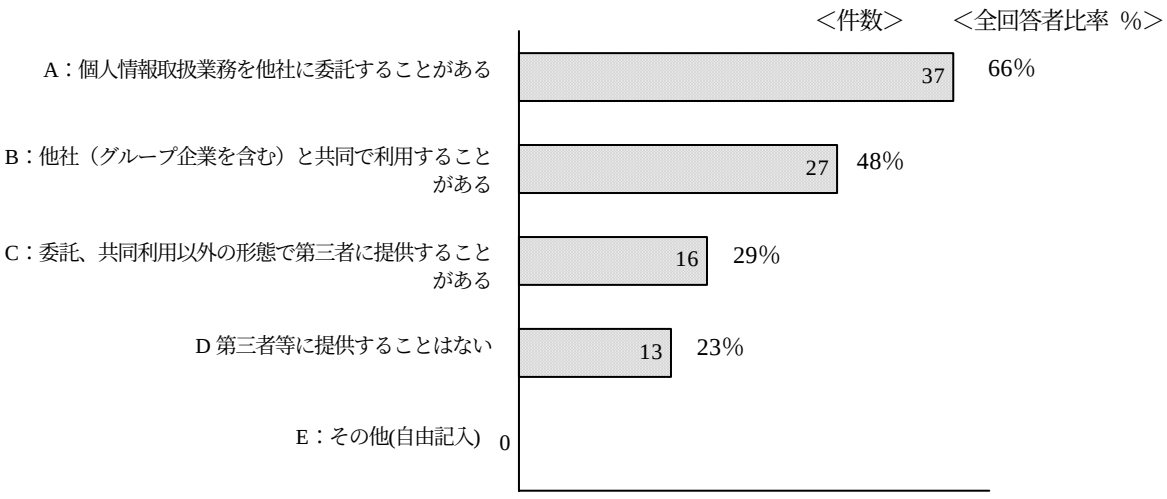


③ 調査結果

全体の 77%が「利用目的を伝えている」としており、さらにそのうちの 4 分の 3 は同意を得ている。しかしながら様々な収集局面がある中で利用目的が明示されないケースも混在しており、それらについては個別に精査していく必要がある。

Q8. （問 3、問 4 の a.b.c.回答者）顧客の個人データ（収集した個人情報をデータとして取り扱っているもの）を第三者等に提供することがありますか？
（有効回答数＝56） 【複数回答可】
（注）共同利用と第三者提供の区分については曖昧な点がありますがここではご回答者の解釈でご回答下さい。

① 全業種合計



＜その他（自由記入）＞

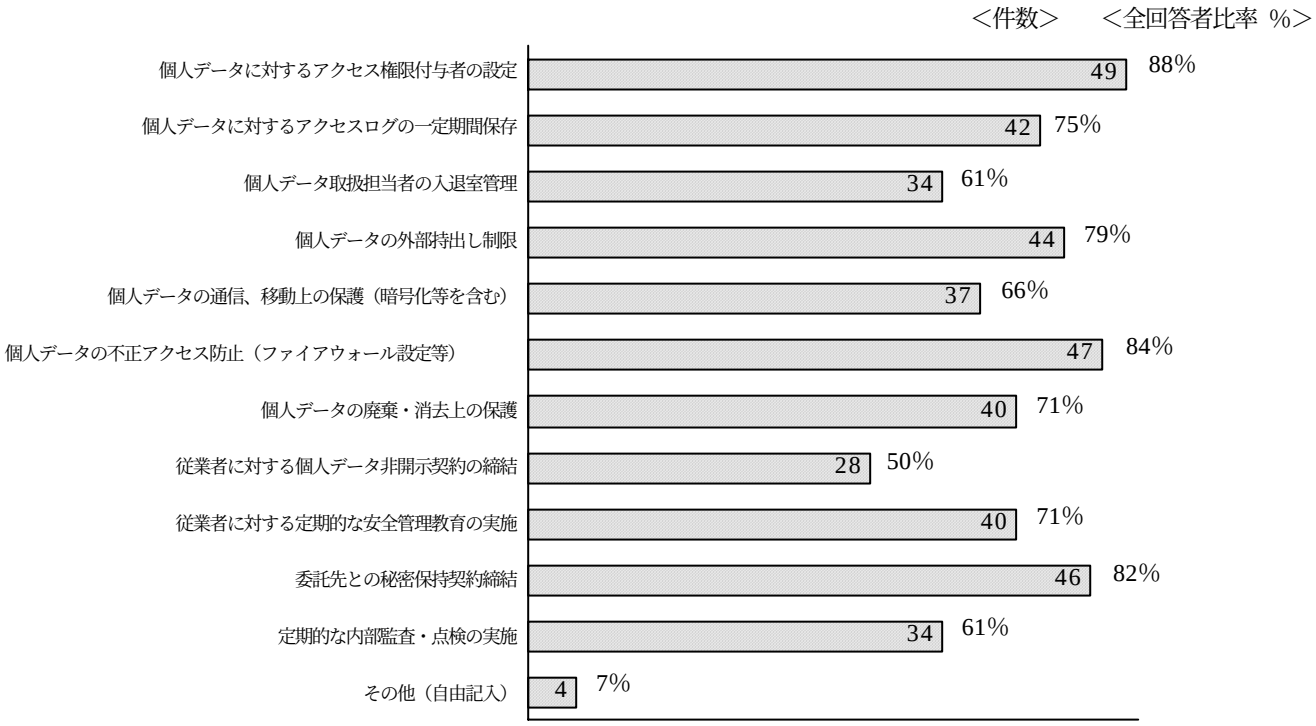
- DM 誌の発送を外部業者に委託（A の回答）
- 個人信用情報機関として会員与信業者に提供（B の回答）

② 調査結果

第三者提供について委託、共同利用の形態も含めその有無を聞いたところ委託 37 件、共同利用 27 件と並んでそれ以外の第三者提供が 16 件寄せられた。共同利用と第三者提供の境界については現時点で必ずしも明確でない点もあるが、第三者提供については原則本人の同意を要するので注意が必要である。

Q9. **（問 3、問 4 の a.b.c.回答者）貴社が実施されている個人データに関する安全管理対策について、以下の中から該当するものを選択してください。**
（有効回答数＝56） 【複数回答可】

① 全業種合計



＜その他（自由記入）＞

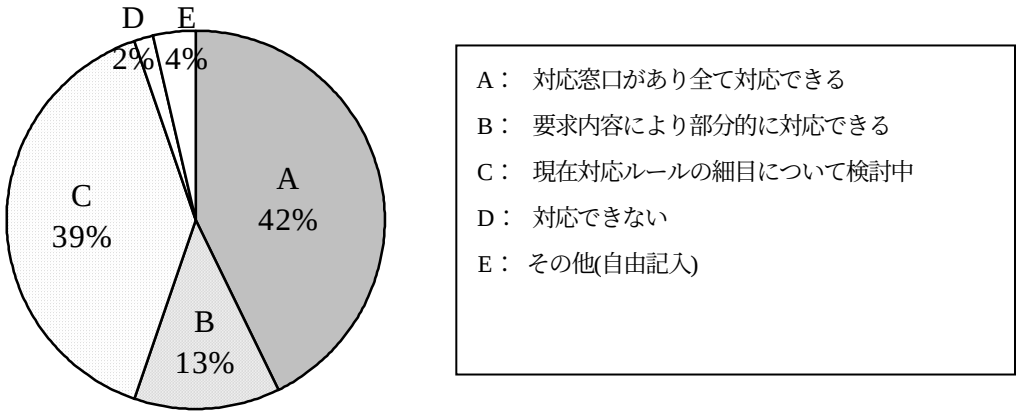
- セキュリティ診断し、方針や管理体制をステップ分けして構築。
- ISO、ISMS による外部監査。
- 「従業者に対する個人データ非開示契約の締結」については契約という形ではないが、内規で規定している。

② 調査結果

多くの企業が複数の対策を既に実施中であり、上記各対策はいずれも半数以上の企業で対応済みである。「個人データに対するアクセス権限の付与」「不正アクセス防止（ファイアーウォール設定等）」等は 90%近い実施率を示しているが、昨今の漏洩事故、事件を鑑みるにいずれも全事業者必須の対策といえよう。また従業者に対する安全管理教育や定期的な内部監査なども今後の大きな課題として残されている。

Q10. **（問 3、問 4 の** a.b.c.**回答者）顧客本人から開示や利用停止等の要求があった場合、即座に対応できるようになっていますか？ （有効回答数＝56）**

① 全業種合計



＜B：部分的に対応できる条件＞

- 対応窓口を設け、極力要望に応じるが、弊社業務の必要上、即座に対応しかねる場合もある。
- システムによってはバッチ処理でしか対応できないものもある。

＜C：検討中の項目＞

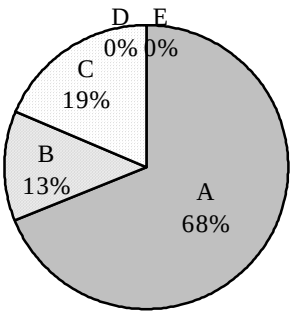
- 本人確認方法など
- 原則全ての項目
- 全削除要望への対応等
- 開示項目
- 業務分担、手続き等

＜その他（自由記入）＞

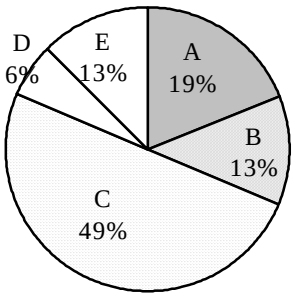
- 専用窓口ではないが、対応している。
- 対応できない。どこにどのような状態で保存されているか調査が済んでいないため。
- 電子計算機処理関係については, 対応できる体制にある。今後は全面的に見直しを検討する予定。

② 業種別

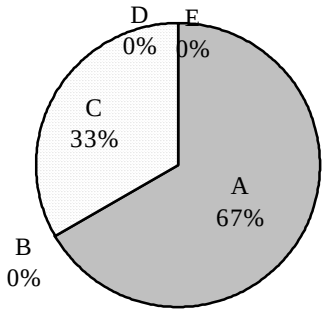
＜情報サービス業＞



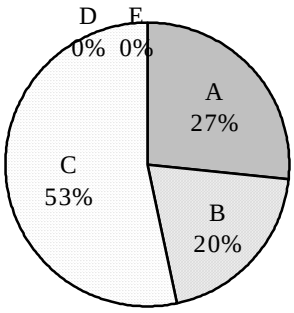
＜製造業＞



＜金融業＞



＜その他＞

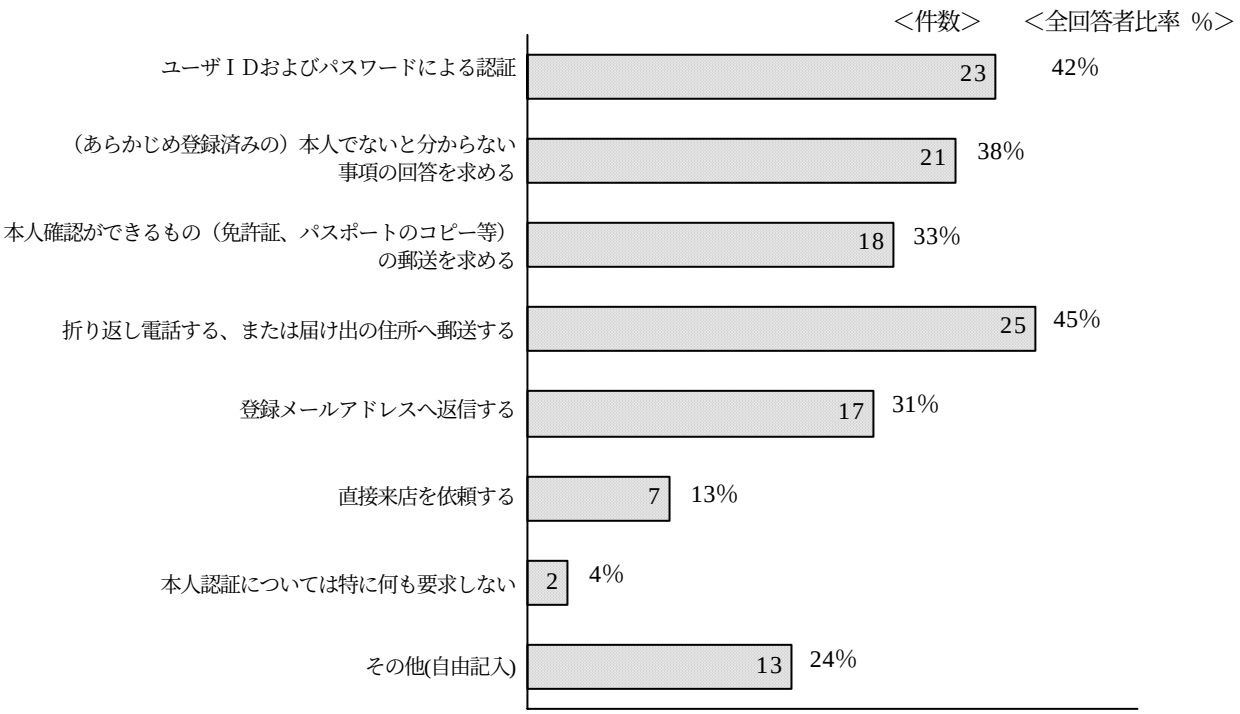


③ 調査結果

「すべて対応できる」が 42%に対し、「部分的に対応できる」「検討中」が合計 52%を占め今後の課題としている企業が約半数ある。システム化が済んでいない部分（個人管理部分等）について、どのように対処すべきかを含め早急に体制を整備していくことが望まれる。

Q11. **（問 3、問 4 の a.b.c.回答者）上記の要求に対して本人確認はどのようにしていますか？ （有効回答数＝55） 【複数回答可】**

① 全業種合計



＜その他（自由記入）＞

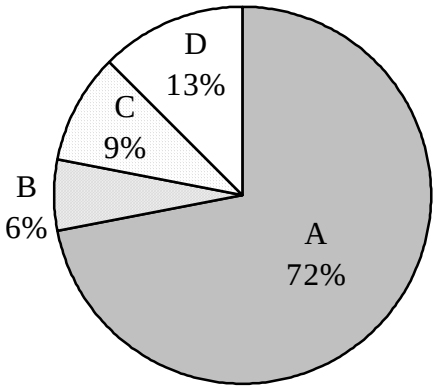
- 各部門の判断に任せている。
- 現在ルールの策定中。
- 現段階では全社的な統一をしていない。
- お客さま番号，氏名，住所等で確認。
- 現時点で要求事例はない。本人確認ルールを検討中。
- 電子計算機処理関係については，対応できる体制にある。今後は全面的に見直しを検討する予定。
- 担当営業経由での確認

② 調査結果

本人確認方法としては「折り返し電話する、または届け出の住所に郵送する」「ユーザＩＤおよびパスワードによる認証」「本人でないと分からない事項の回答を求める」等が一般的であるが全社ルールを検討中のところも多い。いずれにせよ個人情報はその中身により機微度も異なるためキメ細かな本人確認対応が必要になる。

Q12. **貴社サイトに「個人情報の保護に関する方針（プライバシー・ポリシー等）を表示していますか？　（有効回答数＝64）**

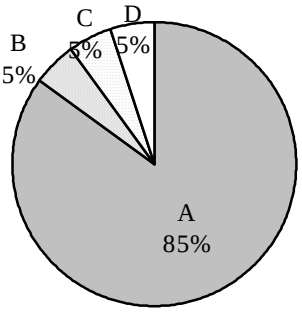
① 全業種合計



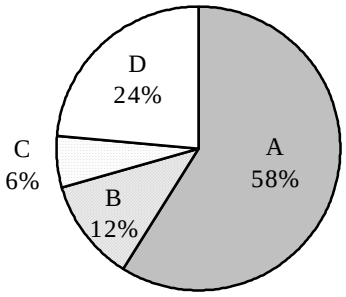
A： トップページに、あるいはそこからリンクのある場所に表示している
B： 上記以外の場所に表示している
C： 「個人情報の保護に関する方針」はあるが、サイトには表示していない
D： 対外的な「個人情報の保護に関する方針」等はない
E： その他(自由記入)

② 業種別

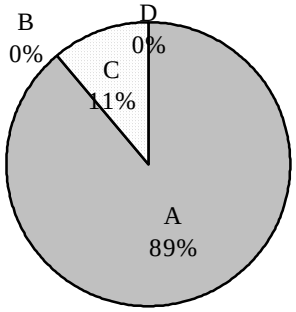
＜情報サービス業＞



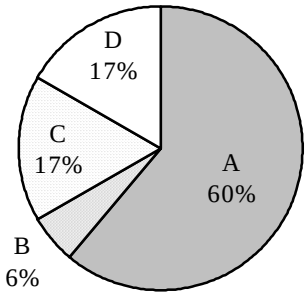
＜製造業＞



＜金融業＞



＜その他＞



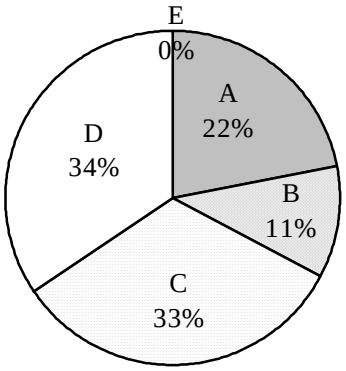
③ 調査結果

トップページに表示している企業は 72%となり、近年急速に増加している。
トップページ以外に表示している企業は全体の 6%あるが、トップページに表示している場合に比して閲覧者の視認性に大きな差があり、トップページ上でのリンクボタン設置が望まれる。またプライバシー・ポリシー未表示企業についても同様である。

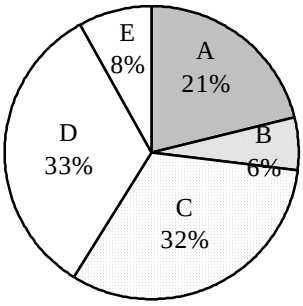
Q13. **個人情報の取扱いを適正に行っていることを第三者機関が証明する「プライバシーマーク制度」について知っていますか？　（有効回答数＝64）**

① 全業種合計

【2004 年度】



【2003 年度】

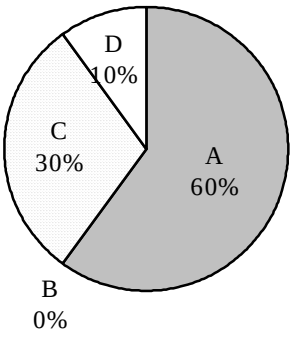


A： 既に取得している
B： 一部の部門で取得している
C： 現在取得はしていないが、取得を考えている
D： 知っているが取得していないし、現時点では特に取得を考えていない
E： 知らない

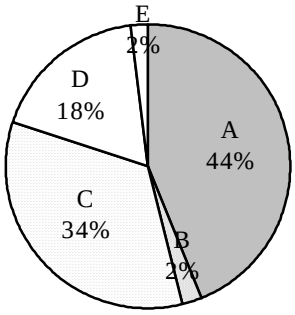
② 業種別

＜情報サービス業＞

【2004 年度】

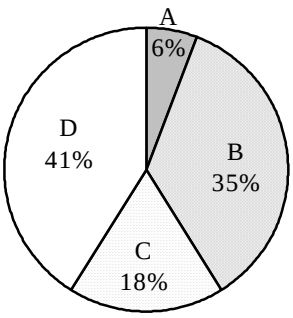


【2003 年度】

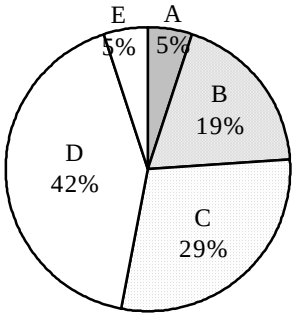


＜製造業＞

【2004 年度】

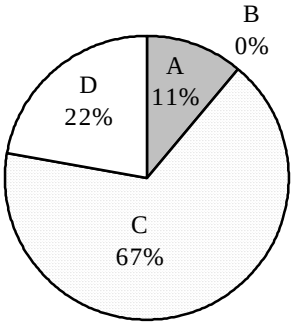


【2003 年度】

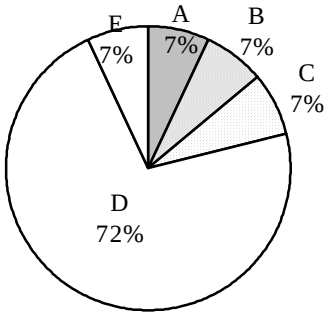


＜金融業＞

【2004 年度】

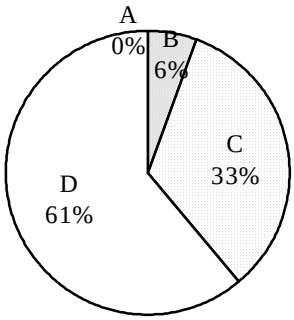


【2003 年度】

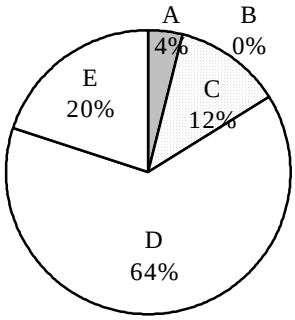


＜その他＞

【2004 年度】



【2003 年度】

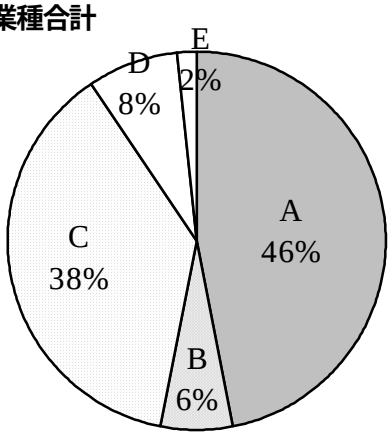


③ 調査結果

プライバシーマークの認知度、取得意欲についてはほぼ全業種で高まっているが、とりわけ情報サービス業で取得が進んでいる。これは情報サービス業が取引先から受託の際の判断基準として、プライバシーマークの有無を考慮される実態を反映しているものと思われる。また昨年度はプライバシーマークの存在を知らないとした企業もあったが、今年度は皆無であり、その認知度が確実に上昇している様子を裏付ける。

Q14. **顧客が当該サイトに再度アクセスしたとき、過去の通信履歴データをサーバ側で認識することができる「クッキー」という仕組みを利用していますか？**
（有効回答数＝64）

① 全業種合計



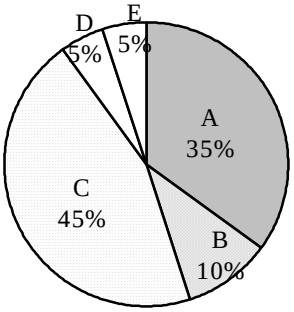
A： クッキーを利用しており、サイト利用者に対してその利用目的等を明示している
B： クッキーを利用しているが、それについて利用者に説明はしていない
C： クッキーを利用していない
D： クッキーについてはよく分からない
E： その他(自由記入)

＜A と回答 （自由記入）＞

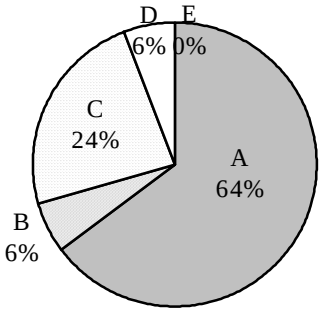
- 1 セッション内のみの一時的なクッキーを発行。サイト内で説明はしている。
- 一部サービスでは説明の上使用。
- クッキーは利用しているが個人情報は無く、かつ一時的な利用としている。
- クッキーを利用するサイトを構築運用する際は利用目的などを明示するようサイト所管部門に指導している。

② 業種別

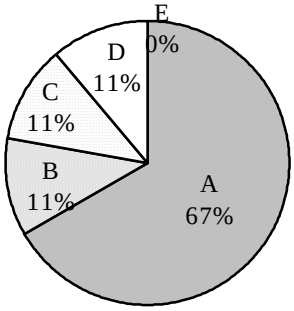
＜情報サービス業＞



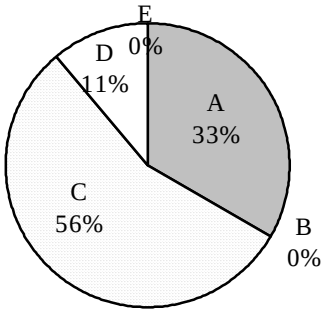
＜製造業＞



＜金融業＞



＜その他＞



③ 調査結果

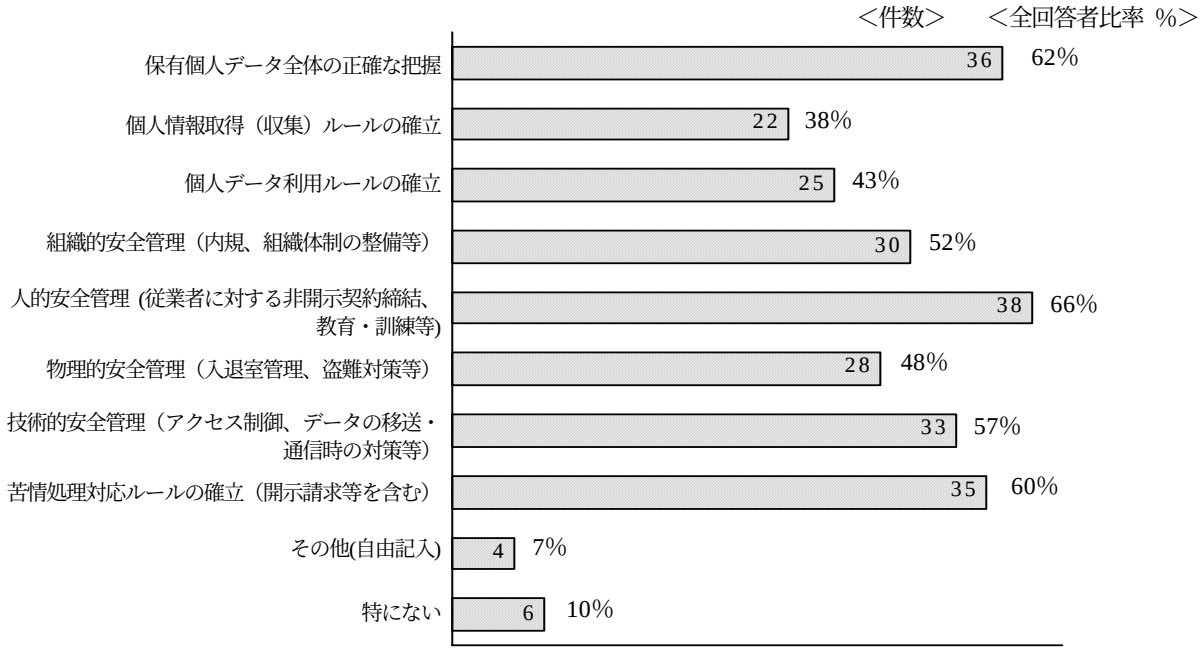
クッキーについては約半数の企業が利用しており、しかもそのうちの大半がサイト利用者にたいしその利用目的等を説明している。クッキーは閲覧者の利便性向上とサイトプランの改善に有

効なツールであり、今後利用企業はさらに進むものと見られるが One to One Marketing に利用の際にはその目的を事前に公表し、サイト利用者の不安を払拭することが求められる。

Q15. 個人情報保護法施行に向けて懸案事項があるとすればそれは何ですか？
（有効回答数＝58） 【複数回答可】

① 全業種合計

＜その他（自由記入）＞



- 法律違反にならない必要最小限の安全管理措置の見極め。
- 個人情報保護の観点よりも、情報管理強化の中で捕らえている。
- 委託先の監督。
- 法施行後の増大が予想される問い合わせ対応工数（コスト）の確保、クレーマー等への対応方法。
- 「人的安全管理」は、非開示の内規を契約に変えるべきかどうかの検討。および社内教育は実施済みだが、定期的に繰り返すという意味。
- 回答項目については、業界指針に基づいた安全管理対策を実施中ですが、未だ「万全である」という状況ではない為、「懸案事項」として回答。

② 調査結果

懸案事項の中では人的安全管理を挙げる回答が最も多かった。昨今の漏洩事故の大半が内部関係者の関与、個人情報取扱い担当者の不注意によることから、今後の大きな課題にあげられているように思われる。また第 2 位として保有個人データの正確な把握が挙げられており、全体を把握することの困難性をうかがわせる。苦情処理(開示請求を含む)対応についても多くの企業にとってまだ経験が少ないため、不安視する向きが多い。

2.4　ＥＣ事業者に対するアンケート調査

日本商工会議所のご協力を得て、同所が付与しているオンライントラストマーク取得事業者に対し個人情報保護に関するアンケートを行った。本調査の対象は比較的小規模の事業者が中心であり、かつ今年度初めての試みである。

2.4.1　ＥＣ事業者に対するアンケート調査の概要

（1）アンケート調査時期…… 2004 年 9 月 17 日～10 月 1 日
（2）対象…… JCCI オンラインショッピングトラストマーク取得
ネット通販事業者（約 380 社）
（3）有効回答数…… 50 社（回答率：13%）
(4)　回答者の会社形態別内訳

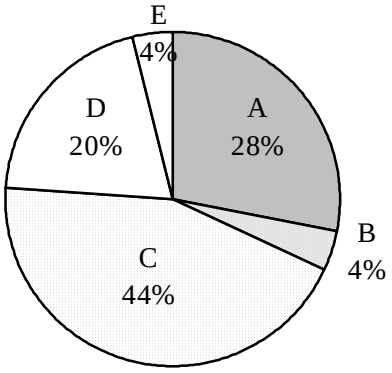
株式会社	30 社
有限会社	7 社
合資会社	2 社
確認できなかったもの	7 社
団体その他	4 社

(注)　ECOM 会員調査データの付記
ECOM では従来から会員に対し同様の調査を行ってきたので、参考までにその結果概要を付記している。ECOM 会員は情報サービス業、製造業、金融業等多くの業種から成り企業規模も相当開きがある。

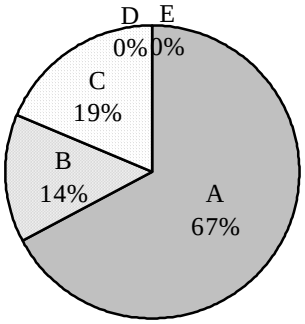
2.4.2　EC 事業者に対するアンケート調査の結果

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？（有効回答数＝50）

【ネット通販事業者】



＜参考：ECOM 会員＞



A： 個人情報保護に関する全社規程がある
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
E： その他（自由記入）

■その他（自由記入）

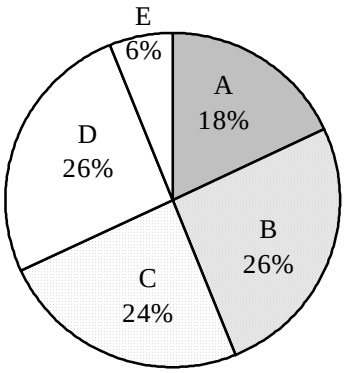
- 規定はないが個人情報を保護するのは常識と考えている。

【調査結果】

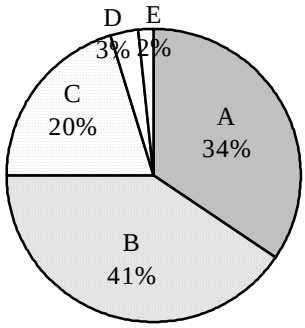
「個人情報保護に関する社内規程がある」とした回答が全体の約 30%あり、さらに「今後策定する」としているところが 40%強ある。本年 6 月に公表された経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（以下「METI ガイドライン」と略）では個人データの安全管理に関する従業者の役割・責任を社内規程として具体的に定めることが望ましいとしており、各事業者は事業規模や取り扱う個人情報の内容に応じた社内規程を整備していくことが求められている。

Q2. **貴社には個人情報保護体制の構築・管理を行なう個人情報保護管理者の指名あるいは担当部門の設置はなされていますか? （有効回答数＝50）**

【ネット通販事業者】



＜参考：ECOM 会員＞



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、または部門内に当該担当や職務を割り当てている
C： 今はないが、今年度中に任命あるいは設置しようと考えている
D： ない
E： その他（自由記入）

■その他（自由記入）

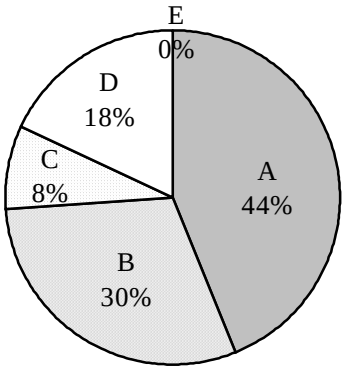
- 個人商店なので店主が兼務で担当。
- 個人事業所の為、一人専任して管理。

【調査結果】

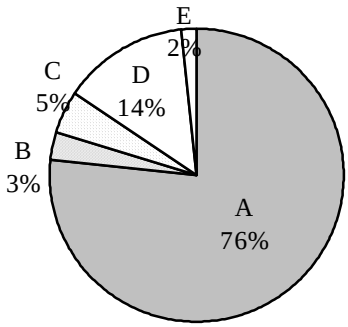
個人情報保護管理者の指名または担当部門の設置については全体の 44%が専任もしくは兼任の形で役割を明確化している。小規模の組織では未分化も見受けられるが少なくとも兼務の形で保護意識を高めていくことが望まれる。

Q3. **貴社では顧客の個人情報を直接的に収集することがありますか？（従業者に関する個人情報は除く）　（有効回答数＝50）**

【ネット通販事業者】



＜参考：ECOM 会員＞



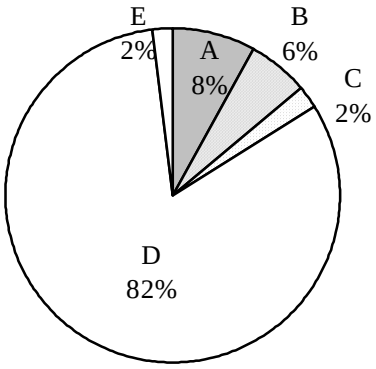
A： サイトから、およびサイト以外からの両方の方法で収集している
B： サイトからのみ収集している
C： サイト以外から収集している
D： 顧客の個人情報を収集することはない
E： その他（自由記入）

【調査結果】

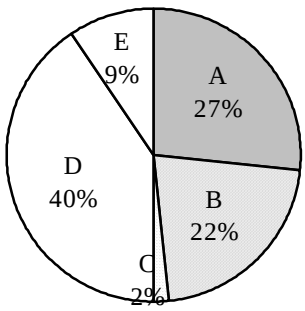
ネット上・ネット以外を問わず直接収集しているとした回答は 82%あった。個人情報の取得については利用目的の通知または公表(ホームページでの掲載等)が原則でありあらためて対応を確認しておく必要がある。

Q4. **貴社では顧客の個人情報を間接的に収集（個人情報取扱業務を受託する場合を除く）することがありますか？ （有効回答数＝50）**

【ネット通販事業者】



＜参考：ECOM 会員＞



A： 個人情報の収集を他社に委託することがある
B： インターネット、電話帳、職員録等公開情報から収集することがある
C： 専門業者から名簿等を購入することがある
D： 間接収集することはない
E： その他（自由記入）

■その他（自由記入）

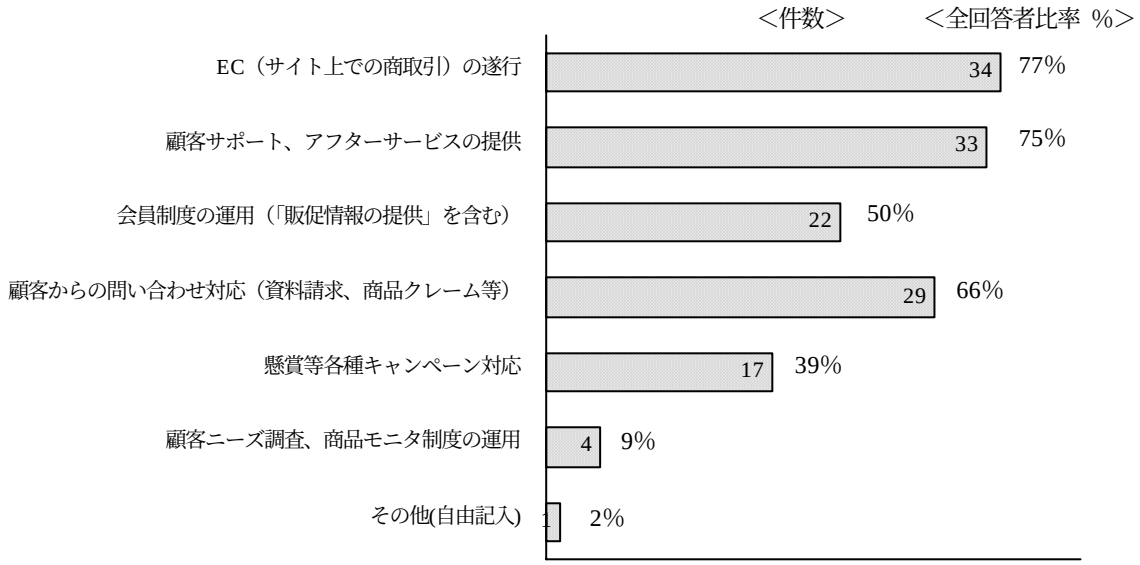
- 業務委託元から提供されることがある。

【調査結果】

個人情報の収集を他社に委託、公開情報から収集するがそれぞれ数社存在するが、大半の回答者は「間接収集なし」としており、自己完結型事業運営形態が中心となっている。

Q5. **（問 3､問 4 の** a.b.c.**回答者）貴社の収集する顧客の個人情報の利用目的について、以下の中から該当するものを選択してください。（有効回答数＝44）【複数回答可】**

【ネット通販事業者】

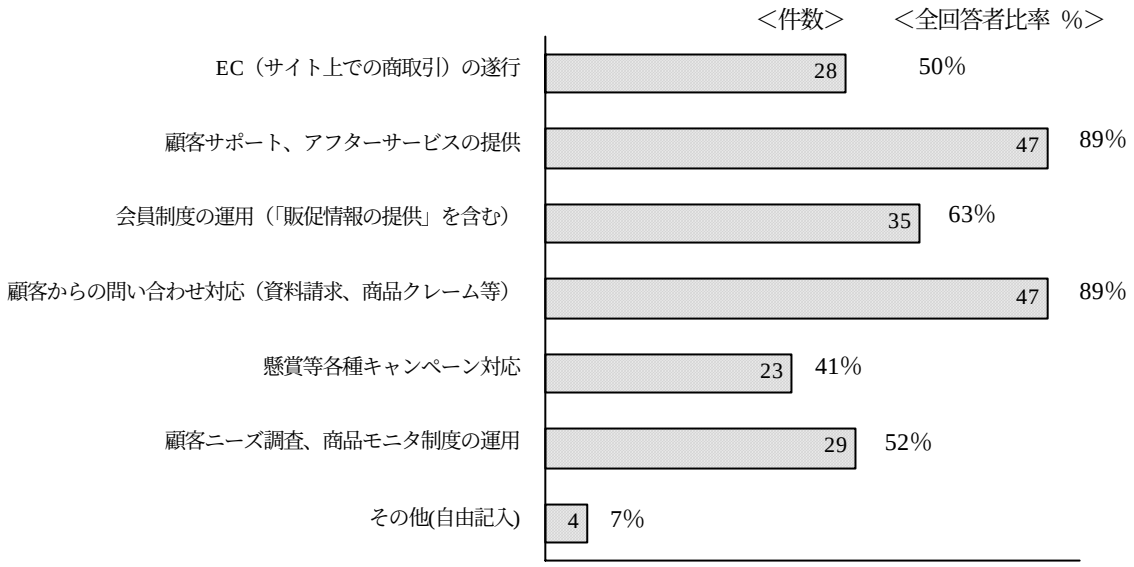


【調査結果】

個人情報の取得にあたっては、利用目的の通知・公表が必要であるが、利用目的はできる限り

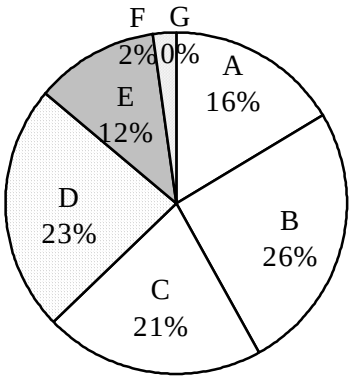
特定されていなければならない。単に当社の事業活動やマーケティング活動に用いるといった表現は特定しているとは見なされないため、より細分化された具体的な表現が求められる。

＜参考：ECOM 会員＞

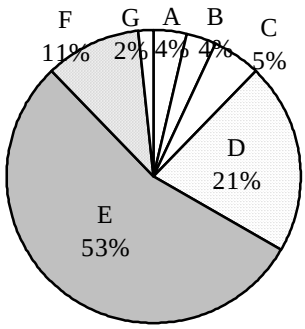


Q6. **（問 3､問 4 の a.b.c.回答者）現在収集している個人データ（収集した個人情報をデータとして取り扱っているもの）は何件くらいありますか？**
（この設問のみ「従業者の個人データ」を含めてご回答下さい）　（有効回答数＝43）

【ネット通販事業者】



＜参考：ECOM 会員＞



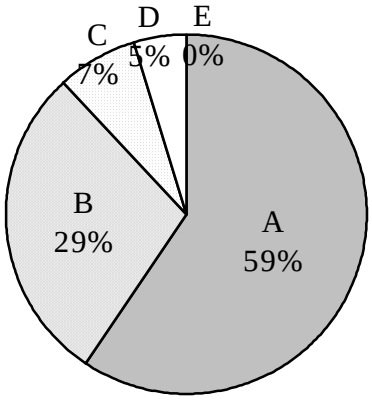
A： 1000 件未満
B： 1000 件以上 5000 件未満
C： 5000 件以上 1 万件未満
D： 1 万件以上 10 万件未満
E： 10 万件以上
F： 分からない
G： その他（自由記入）

【調査結果】

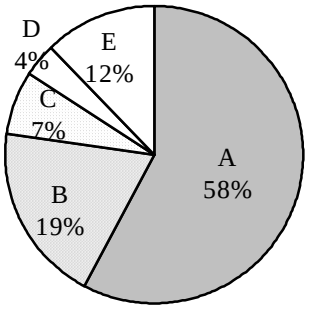
政令により 5000 件以上の個人データを保有する事業者を「個人情報の保護に関する法律」の適用対象としているが、今回の調査では約 6 割がそれに該当する。保有個人データ数は事業年数とともに増加し、また 5000 件という境界ラインも変更される可能性があるため引き続き法制度の動向を見守っていくことが重要である。

Q7. **（問 3、問 4 の a.b.c.回答者）顧客から個人情報を直接収集する際、利用目的を通知または公表していますか？　（有効回答数＝42）**

【ネット通販事業者】



＜参考：ECOM 会員＞

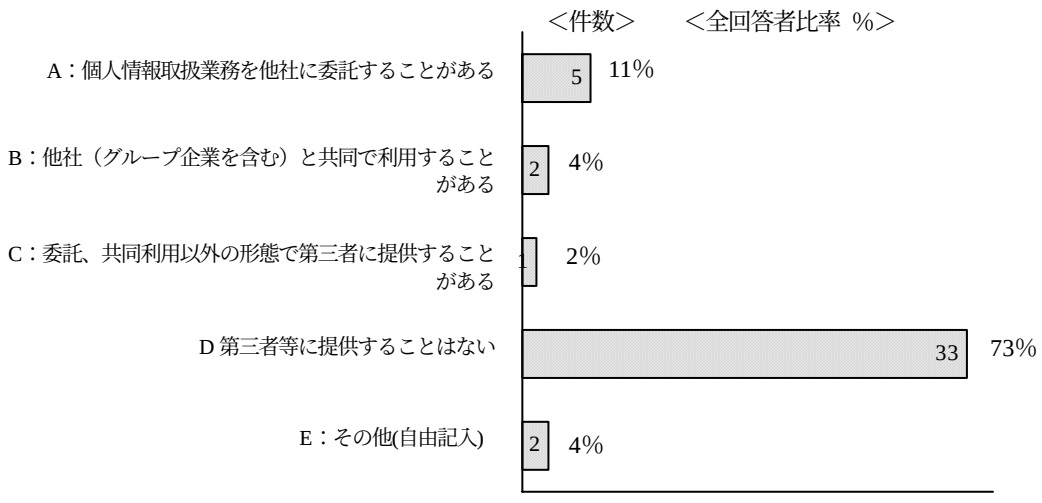


A： 利用目的を伝え、かつ同意を得て収集している
B： 利用目的を伝えた上で収集している（同意は得ていない）
C： 収集しているが利用目的を伝えていない
D： 収集していない
E： その他(自由記入)

【調査結果】

「METI ガイドライン」では、書面による記載等直接本人から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としているため、不備のある事業者は早急な対応が迫られる。

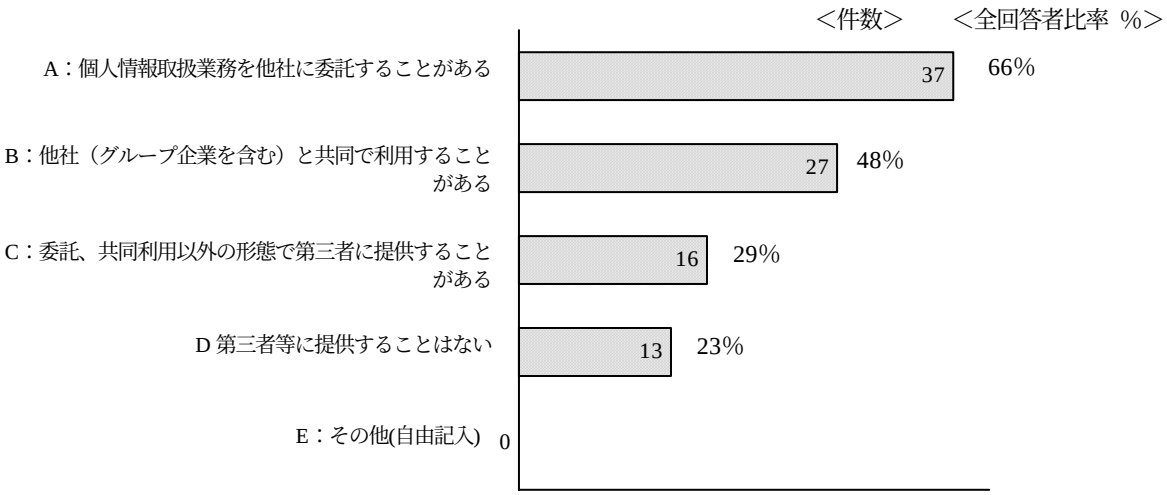
Q8. **（問 3､問 4 の a.b.c.回答者）顧客の個人データ（収集した個人情報をデータとして取り扱っているもの）を第三者等に提供することがありますか？**
（有効回答数＝45） 【複数回答可】
（注）共同利用と第三者提供の区分については曖昧な点がありますがここではご回答者の解釈でご回答下さい。
【ネット通販事業者】



【調査結果】

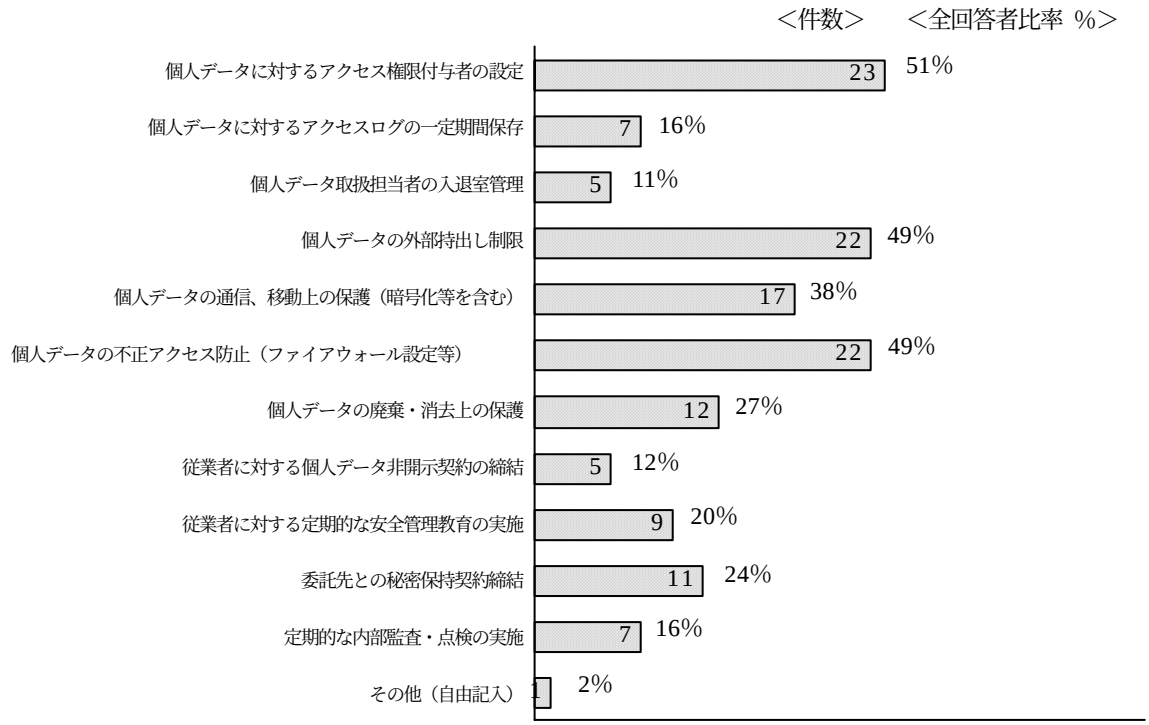
「第三者提供はない」が約 7 割を占めている。委託、共同利用以外の第三者提供は例外を除いて本人同意を得なければならないので注意が必要である。

＜参考：ECOM 会員＞



Q9. （問 3、問 4 の a.b.c.回答者）貴社が実施されている個人データに関する安全管理対策について、以下の中から該当するものを選択してください。
（有効回答数＝45） 【複数回答可】

【ネット通販事業者】



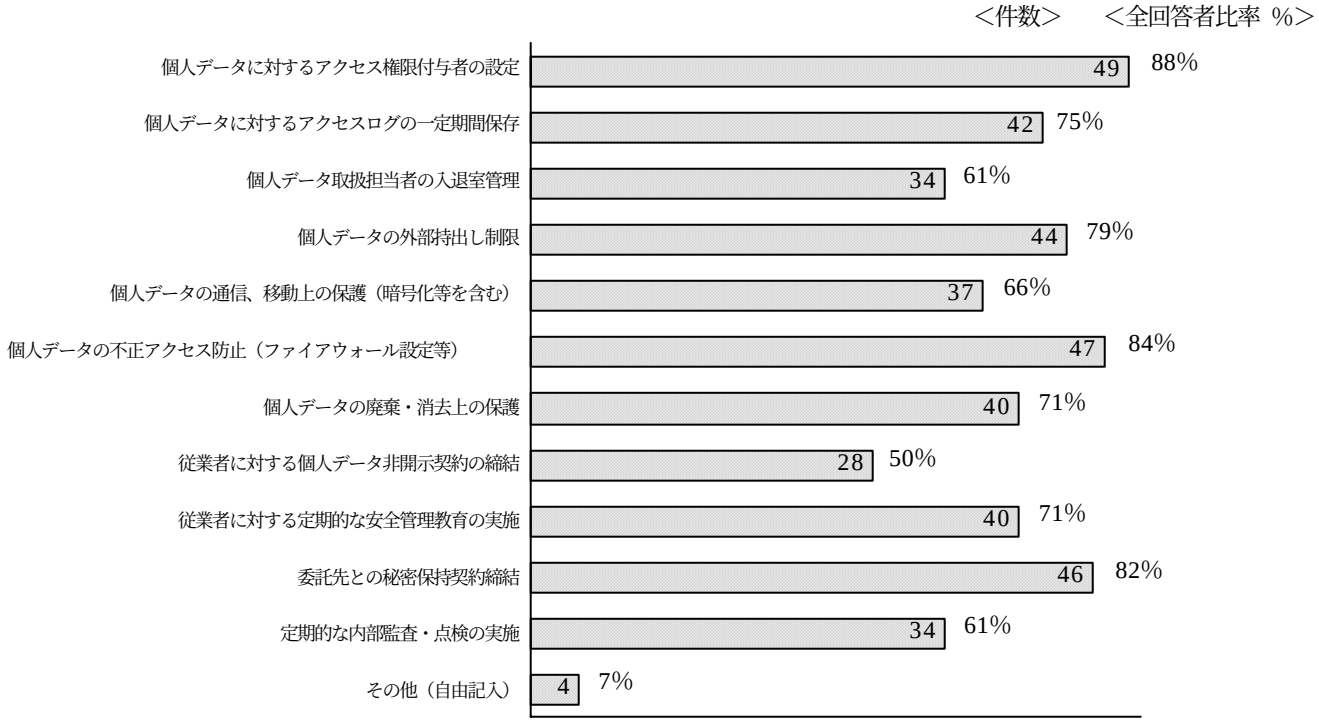
■その他（自由記入）

- 今後、策定予定。

【調査結果】

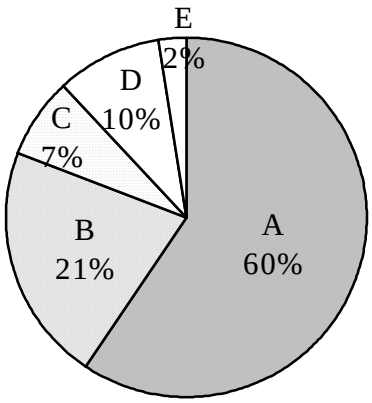
安全対策については「アクセス権限の付与」「外部持出し制限」「ファイアーウォール等による不正アクセス防止」が上位を占めた。取るべき対策及びそのレベルについては、事業規模等を見極めながら不足のない取り組みが必要である。

＜参考：ECOM 会員＞

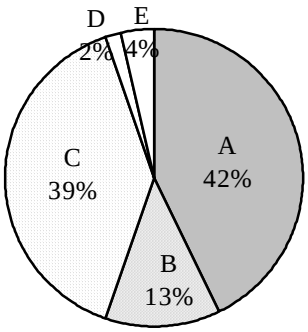


Q10. **（問 3､問 4 の a.b.c.回答者）顧客本人から開示や利用停止等の要求があった場合、即座に対応できるようになっていますか？ （有効回答数＝42）**

【ネット通販事業者】



＜参考：ECOM 会員＞



A： 対応窓口があり全て対応できる
B： 要求内容により部分的に対応できる
C： 現在対応ルールの細目について検討中
D： 対応できない
E： その他(自由記入)

＜B：部分的に対応できる条件＞

- 注文内容。
- サイトユーザーのみ対応可能。

＜E：その他（自由記入）＞

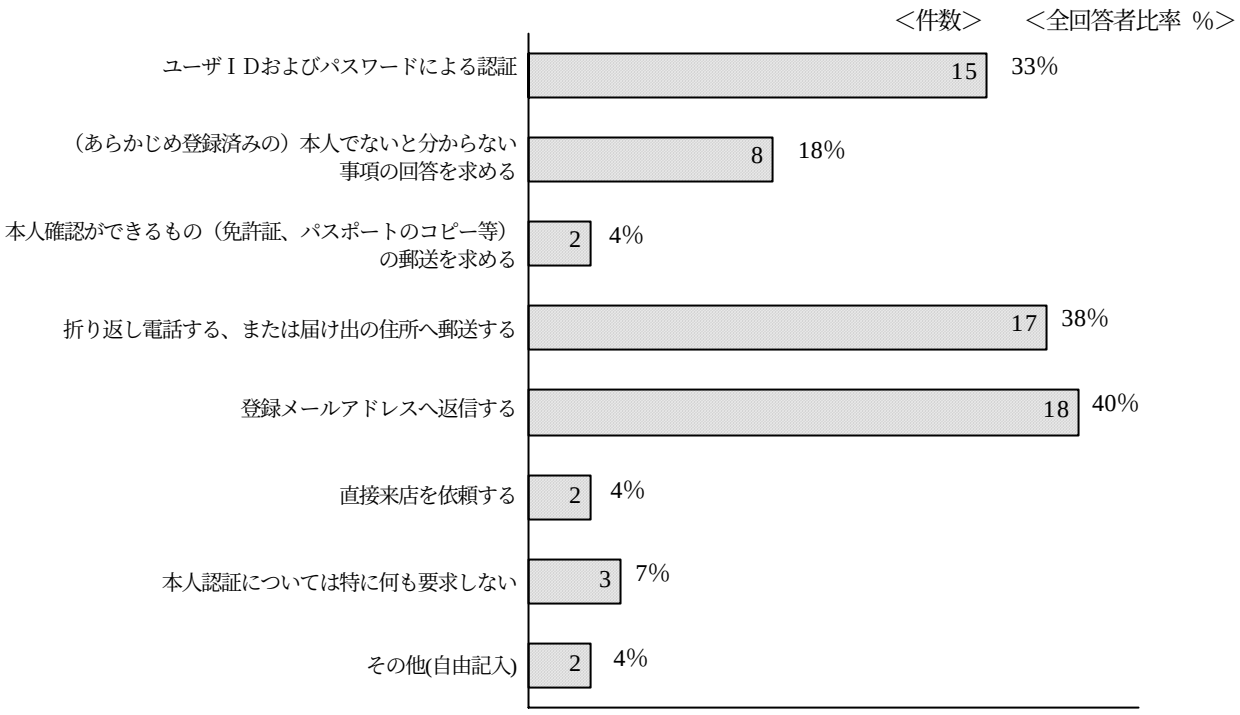
- 委託元から指示があれば対応する。

【調査結果】

開示、利用停止等情報主体（個人情報提供者）からの要求については、約 6 割の事業者が一元的な対応できるとしているが、これは小規模事業者ゆえの優位性も働いているものと思われる。

Q11. **（問３､問４の** a.b.c.**回答者）上記の要求に対して本人確認はどのようにしていますか？ （有効回答数＝45） 【複数回答可】**

【ネット通販事業者】



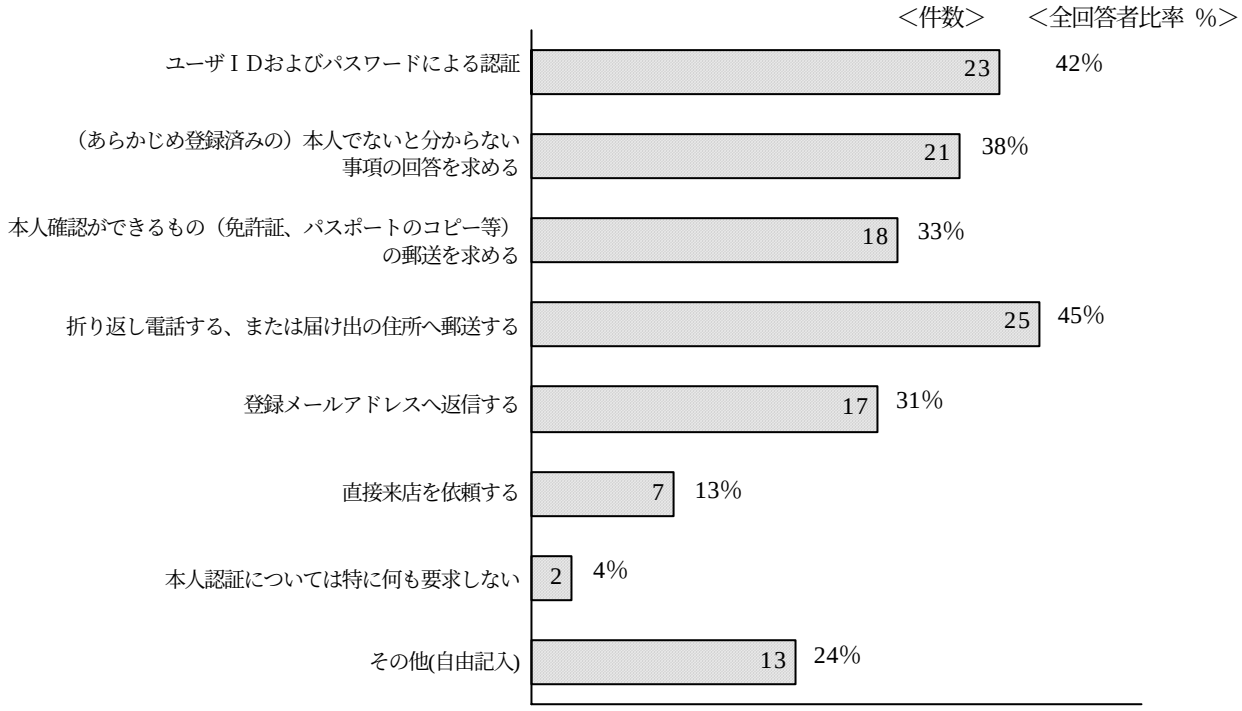
■その他（自由記入）

- 委託元からの指示による。
- 購入時に必要な個人情報を入力していただいているだけ。

【調査結果】

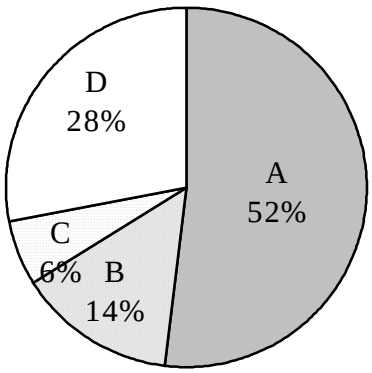
本人確認手段については、「登録メールアドレスへの返信」「折り返し電話または届け出住所への郵送」「ID、パスワードの確認」が上位を占め、「直接来店を求める」「本人確認書類の郵送を求める」などは少ない。本人確認について「特に何も求めない」との回答もあったが、無用のトラブルを防止するために何らかの方策を考慮することが望まれる。

＜参考：ECOM 会員＞

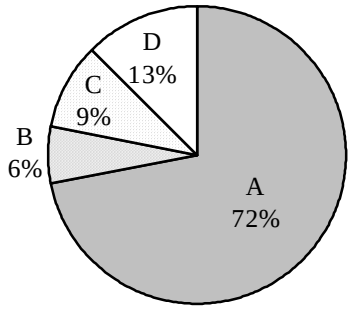


Q12. **貴社サイトに「個人情報の保護に関する方針（プライバシー・ポリシー等）」を表示していますか？　（有効回答数＝50）**

【ネット通販事業者】



＜参考：ECOM 会員＞



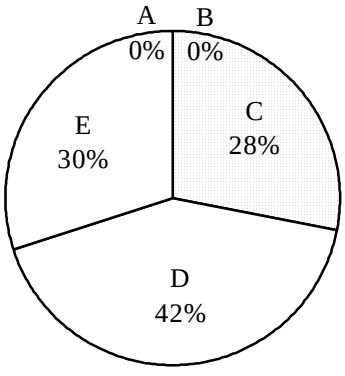
A： トップページに、あるいはそこからリンクのある場所に表示している
B： 上記以外の場所に表示している
C： 「個人情報の保護に関する方針」はあるが、サイトには表示していない
D： 対外的な「個人情報の保護に関する方針」等はない
E： その他(自由記入)

【調査結果】

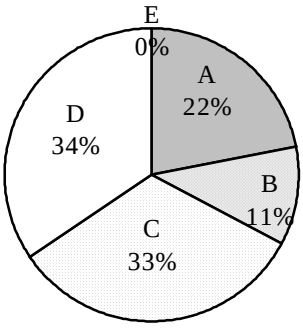
近年消費者の個人情報防衛意識は急速に高まっており、ネット通販サイトを見る目も厳しくなっている。「個人情報保護方針」掲示の有無は、サイト評価の判断基準として今後ますますクローズアップされてくることが予想されるため、生き残り策として必須事項になろう。

Q13. **個人情報の取扱いを適正に行っていることを第三者機関が証明する「プライバシーマーク制度」について知っていますか？　（有効回答数＝50）**

【ネット通販事業者】



＜参考：ECOM 会員＞



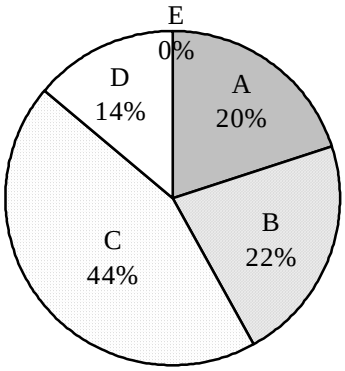
A： 既に取得している
B： 一部の部門で取得している
C： 現在取得はしていないが、取得を考えている
D： 知っているが取得していないし、現時点では特に取得を考えていない
E： 知らない

【調査結果】

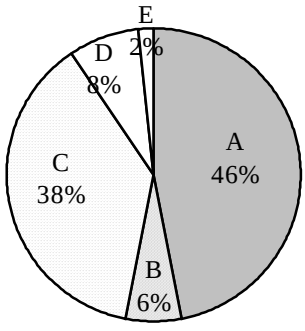
第三者が当該事業者の個人情報保護体制を保証する「プライバシーマーク」の取得は、差別化ツールとしてきわめて有用であるが反面、多大のコストと工数を必要とするため慎重な対応が重要である。今回のアンケートでは取得事業者は存在しなかったが、取得考慮中としている回答者が約 3 割あり関心の高さをうかがわせる。

Q14. **顧客が当該サイトに再度アクセスしたとき、過去の通信履歴データをサーバ側で認識することができる「クッキー」という仕組みを利用していますか？**
（有効回答数＝50）

【ネット通販事業者】



＜参考：ECOM 会員＞



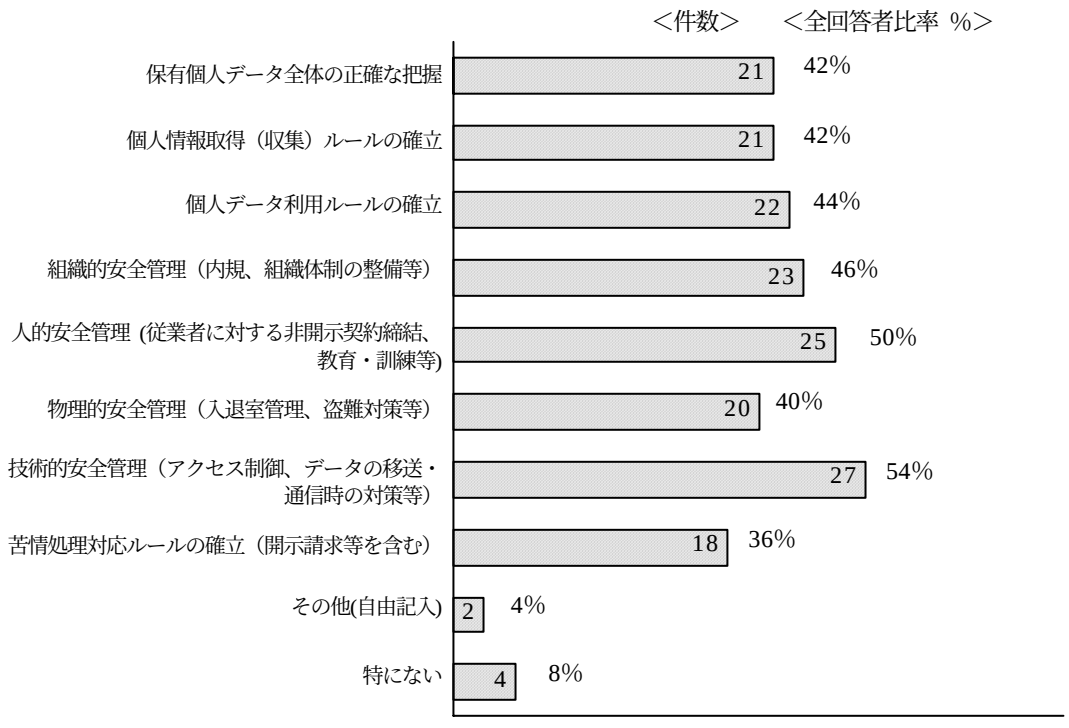
A： クッキーを利用しており、サイト利用者に対してその利用目的等を明示している
B： クッキーを利用しているが、それについて利用者に説明はしていない
C： クッキーを利用していない
D： クッキーについてはよく分からない
E： その他(自由記入)

【調査結果】

クッキーについては40%強の事業者が利用しており、そのうちの約半数がサイト利用者にたいしその利用目的等を説明している。クッキーはサイト利用者（閲覧者）の利便性向上とサイトプランの改善に有効なツールであり、今後利用企業はさらに進むものと見られるが One to OneMarketing に利用の際にはその目的を事前に公表し、サイト利用者の不安を払拭することが求められる。

Q15. **個人情報保護法施行に向けて懸案事項があるとすればそれは何ですか？**
（有効回答数＝50） 【複数回答可】

【ネット通販事業者】



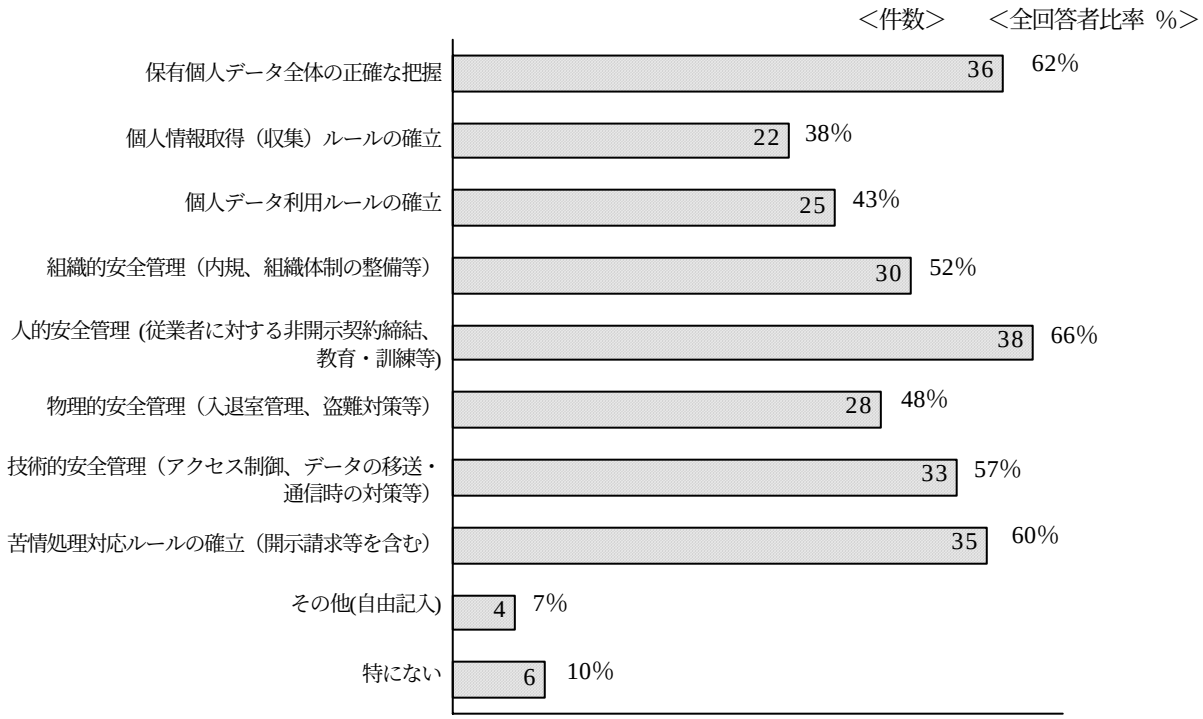
■その他（自由記入）

- 不法な架空請求などに流出しない、させない。そのまえに架空請求業者撲滅の法整備の方が先ではないか。

【調査結果】

懸案事項については 1 社平均 3～4 件の懸案事項の提起があったがほぼ全項目が平均的に挙げられ、特定の項目に集中する傾向は見られなかった。

＜参考：ECOM 会員＞



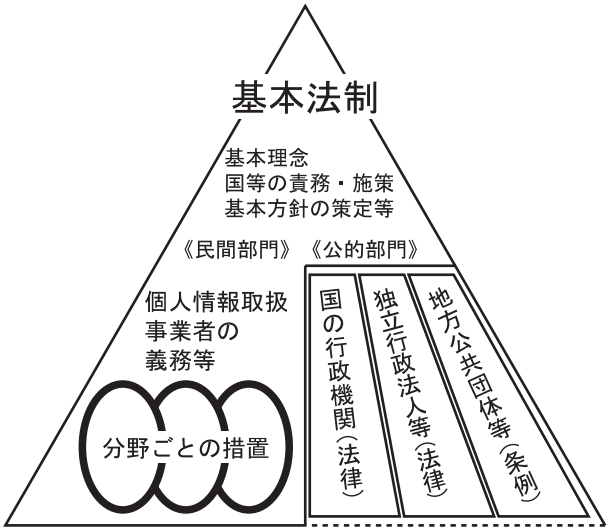
3. 個人情報保護に関する海外の動向

3.1 国際動向とわが国の対応

3.1.1 はじめに

本年4月1日から「個人情報の保護に関する法律」（平成15年 法律第57号）を基本に据えた「個人情報保護関連5法」（①「行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）」、②「独立行政法人等の保有する個人情報の保護に関する法律（同年法律第59号）」、③「情報公開・個人情報保護審査会法（同年法律第 60 号）」、④行政機関の保有する個人情報の保護に関する法律等の施行に伴う関係法律の整備等に関する法律（同年法律第61号）が全面的に施行される。その全体的体系は下図のとおりである。

２．個人情報保護法制の体系イメージ



（内閣府のサイト「個人情報保護の解説」より）

http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/pdfs/taikei.pdf

振り返れば、1980年の「OECD 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」を契機とし、我が国でも幾度となくこの分野に関する取り組みがされてきた。しかしその対応は先進諸外国に比し20年以上の遅れが指摘されていた。

法制的には、1988 年に「行政機関が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」（昭和63年法律第95号）が制定されたが、当該法はその名の示すとおり国家行政機関（一部の公的機関や司法、立法機関は除く）を対象としたもので、範囲もコンピュータ処理された個人情報に限定されたものであった。また民間部門については、通産省（現・経済産業省）が策定した「個人情報保護ガイドライン」等による自主規制にまかせ、実効性を担保する配慮がみられなかったという点で、国際的評価を得るまでには至らなかった。

また、近年の情報通信技術の発展には目覚しいものがあり、世界的規模のネットワーク社会の中で、

個人情報･プライバシー保護の必要性は急速に高まった。一方で、電子政府、地方政府の構築や国際的電子商取引の発展など、最先端の情報通信技術の恩恵を受け、豊かな国民生活を実現していくためには、安全で自由な情報流通が不可欠であるとの認識が高まり、その前提として、情報セキュリティや個人情報･プライバシーについての確実な保護の必要性が認識されるに至った。

近年の個人情報･プライバシーは、国際的なデジタルネットワーク社会との関係で問題となっている。それは、1993 年に米国クリントン政権が「全米情報基盤（NII）」を提唱しその施策としてインターネットの採用と商用化移行を推進（1991-1995）したことに起因する。

以後、欧州･米国･日本の三極は、連携して電子政府、電子商取引の推進に係る法整備や従来制度の見直しを推進しているところである。情報セキュリティ、プライバシーの問題はこの枠組みの中で取り扱われている。2003 年 5 月 23 日に、冒頭の関係5法が成立し、我が国も諸外国並みの包括的保護法が整備された。これらは「e-Japan 戦略」展開の一連の流れの中に位置するものといえ、その重要性は「ネットワーク社会の信頼性･安全性の確保」として「重点施策」に掲げられるところである。

3.2 国際社会とプライバシー

我が国における個人情報･プライバシー問題への対応は、主体的にこれを権利として認め、法律により保護体制を整備するというような動きではなく、むしろ国際協調的な対応に迫られて、というのがその実態であったと思う。

1970 年代に入り国際データ通信の本格的商用化の時代を迎えると、個人情報(Personal Data)も法的保護制度も未整備のまま、流通、蓄積、処理されるという事態が生じた。国際間のデータ通信は、特に多国籍企業にとっては画期的な利便性を齎す一方で、個人情報の国外流出に伴なうプライバシーの危機という深刻な問題を提供することになる。そこでプライバシー保護に関する国際的な取組みの必要性が、特に欧州を中心として唱えられ、法的保護が拡大、進展した。

3.2.1 個人情報に関する国際動向と日本の対応

国際動向と日本の対応

年月	世界の動向	日本の動向
1970	西ﾄﾞｲﾂ「ﾍｯｾﾝ州ﾃﾞｰﾀ保護法」 米国「公正信用報告法」	
1973	･ｽｳｪｰﾃﾞﾝ「ﾃﾞｰﾀ保護法」「ﾃﾞｰﾀ関する布告」 ･ｽｲｽ「ﾃﾞｰﾀ 「護法」	徳島市電子計算組織運営審議会条例
1974	･欧州評議会「公共部門における電算機処理とﾌﾟﾗｲﾊﾞｼｰに関する閣僚委員会決議」	

	･米国「ﾌﾟﾗｲﾊﾞｼｰ法」 ･西ﾄﾞｲﾂ･ﾗｲﾝﾗﾝﾄﾌﾟﾌｧﾙﾂ州「ﾃﾞｰﾀ保護法」 ･ｲｷﾞﾘｽ「消費者信用法」	
1975		国立市電子計算組織の運営に関する条例
1976	欧州評議会「データ保護に関す国際協定案」	
1977	･西ﾄﾞｲﾂ「連邦ﾃﾞｰﾀ保護法」 ･OECD「ﾃﾞｰﾀの国際的移動とその保護」	
1978	･ﾉﾙｳｪｲ「個人データの蓄積に関する法律」 ･仏「情報の処理･ﾌｧｲﾙ･自由に関する法律」 ･OECD「国際ﾃﾞｰﾀ障壁とﾌﾟﾗｲﾊﾞｼｰ保護に関する専門委員会」 ･米国「プライバシー法」 ･ﾃﾞﾝﾏｰｸ「個人情報登録法」「公的機関情報登録法」	
1979	ﾙｸｾﾝﾌﾞﾙｸ「電算機処理に係る記名ﾃﾞｰﾀの使用に関する法律」	
1980	ＯＥＣＤ理事会勧告	総理府「プライバシー保護に関する世論調査」実施 2 月
1981		･行政管理庁「プライバシー保護研究会」設置 ･同研究会「報告書」公表
1982		･行政管理庁プライバシー保護研究会「個人データ処理に伴うプライバシー保護対策」公表
1984	ｲｷﾞﾘｽ「ﾃﾞｰﾀ保護法」(1998 年改正)	春日市「個人情報保護条例」
1985		川崎市「個人情報保護条例」
1986		･総務庁「行政機関の個人情報の保護に関する研究会」 ･同「行政機関における個人情報保護対策の在り方について」
1988		･「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」公布 ･JIPDEC「民間部門における個人情報保護のためのガイドライン」
1991	NSF ｲﾝﾀｰﾈｯﾄ商用化 (民間移行開始) CIX 協会	･郵政省「電気通信事業における個人情報保護に関するガイドライン」

1993	NII（National Information Infrastructure）3月	
1994		・内閣に「高度情報通信社会推進本部」設置
1995	・EU「個人ﾃﾞｰﾀ保護指令」採択 10月 ・Internet 民間移行完了（CIX）	
1996	米国「A Framework for Global Electronic Commerce」（earlier version）公表 12月	・郵政省「放送における視聴者の加入個人情報保護に関するガイドライン」
1997	・米国「A Framework for Global Electronic Commerce」（final version）公表 7月 ・EU「電気通信分野における個人情報保護指令」採択 12月	・橋本・ｸﾘﾝﾄﾝ会談（日米規制緩和合意） 6月 ・「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」（通産省関係局長等名で事業者団体に通達） 6月 ・「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」通産省機械情報産業局長（通達） 9月 ・電子商取引実証推進協議会「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」 12月
1998	・EU「個人ﾃﾞｰﾀ保護指令」発効 10月 ・ｲｷﾞﾘｽ「1984年ﾃﾞｰﾀ保護法」改正 ・米国「ｵﾝﾗｲﾝ児童保護法」 10月	・「プライバシーマーク制度」発足 4月 ・推進本部「電子商取引等検討部会」（報告書）、同年11月 ・推進本部「「高度情報通信社会推進に向けた基本方針」
1999		・JISQ15001制定 3月 ・「住民基本台帳法の一部を改正する法律」公布 ・推進本部「個人情報保護検討部会」発足 ・推進本部「「我が国における個人情報保護システムの確立について」決定
2000	米国商務省「Safe Harbor原則」 7月	・推進本部「個人情報保護法制化専門委員会」発足 1月 ・高度情報通信社会推進本部→「情報通信技術戦略本部」へ ・個人情報保護基本法制に関する大綱案（中間整理）公表
2001		・内閣に「IT戦略本部」設置 →「e-Japan戦略」決定
2003		「個人情報保護関連5法」（第156国会）成立 5月23日
2005		「個人情報保護関連5法」全面施行 4月1日

3.2.2 プライバシー法の台頭と国際協調の必要性

1973 年のスウェーデン「データ保護法」は、国レベルのプライバシー法としては世界で最初の法律である。同法は、官民を包括的に扱い（第 1 条）、個人データの第三国への流出規制（第 2 条）や、監督官庁（ﾃﾞｰﾀ検査院）の設置（第 15 条）、刑事罰（第 20 条）等を設ける等、今日の欧州法の基本思想を有していることは注目に値する。

しかし「個人データファイルの所持についてはデータ検査院の許可を必要とする（第 2 条）」という条項は、当然、コンピュータの設置についても何らかの制約を発生させたと考えられ、当時の情報産業育成政策も考慮すると 1970 年代の欧州プライバシー法制定の真の目的は、必ずしもプライバシー保護だけではないと推量することも可能である。

プライバシーを保護する法制が、結果として情報の自由な流通を阻害するのであれば、コンピュータや情報通信技術の進展とその恩恵を蒙るべき企業活動に多大な影響を与えることも事実である。

そこで、情報の保護と自由な国際流通に関する国際間の調整をはかる目的で、欧州共同体、欧州評議会、国際連合、経済協力開発機構（OECD）においてプライバシー、特にコンピュータ・プライバシーに関する研究や啓蒙活動が活発化し、国際間での協調ルールが模索された。

3.2.3 デ・ファクト・スタンダードとしての「プライバシー・ガイドライン」

コンピュータ・プライバシーの問題が懸念されるなか 1978 年にＯＥＣＤは「国際データ障壁とプライバシーの保護に関する専門委員会」を発足させ、国際データ通信に関するデータ保護の基本的ルールを検討し、1980 年 9 月 23 日にＯＥＣＤ理事会は「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」（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）を採択した。

その付属文書である「プライバシーの保護と個人データの越境流通に関する理事会勧告（RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA）」の第 2 部である「国内適用における基本原則」（BASIC PRINCIPLES OF NATIONAL APPLICATION）において「個人情報の収集と管理に関する 8 つの原則」（①収集制限の原則（Collection Limitation Principle）②データ内容の原則（Data Quality Principle）③目的明確化の原則（Purpose Specification Principle）④利用制限の原則（Use Limitation Principle）⑤安全保護の原則（Security Safeguards Principle）⑥公開の原則（Openness Principle）⑦個人参加の原則（Individual Participation Principle）⑧責任の原則（Accountability Principle））を加盟各国に勧告した。

http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM

これらはあくまでも勧告であって法的拘束力を持つものではないが、加盟国を中心に法律の制定が進み、現在は加盟 30 ヶ国の内、トルコ（Turkey）を除く 29 カ国が個人情報保護・プライバシー保護法を制定している。

3.2.4 ＯＥＣＤと最近のプライバシー活動

⑴ ＯＥＣＤ「国際データ流通に関する宣言」(Declaration on Transborder Data Flows (Adopted by the Governments of OECD Member countries on 11th April 1985)
(http://www.oecd.org//dsti/sti/it/secur/prod/e_dflow.htm)

1985 年 4 月 11 日の本宣言は、「情報及びコンピュータ通信の分野における技術の急激な発展は、加盟国の経済を著しく構造的に変化させ発展に結びつけている。コンピュータ化されたデータと情報の流通は、技術的進歩の重要な結果であり、国家経済発展の役割を演じているものである。メンバー加盟国相互間の経済発展は、こうした国際データ流通によることを知るべきである。拠って国際データ流通に関する政策問題にＯＥＣＤが注意を払うことは正に当を得たものである」とし、加盟国に対して国内法の制定時において次の項目を配慮するよう求めたものである。

①データと情報へのアクセス及び関連サービスを促進し、データと情報の国際交換への不正な障害の生成を回避すること。
②越境データ流通に影響する情報、コンピュータ及び情報提供サービスに関係のある規則並びに政策は透過的であること。
③越境データ流通と関係する問題に対処するため、共通ルールの策定及び適切な場合の調和的解決策の開発。
④越境データ流通と関係する問題に対処する場合、他の国々のための可能な意見調整を考慮すること。

本宣言は、コンピュータ化されたデータ及び情報が国際的規模で自由に流通すべきことを、加盟国相互間で改めて認識し合ったものである。

⑵ 電子環境下におけるＯＥＣＤプライバシー・ガイドラインの実施：インターネットにフォーカスして
(Implementing the OECD “Privacy Guidelines” in the Electronic Environment ：Focus on the Internet, 1998) http://www1.oecd.org/dsti/sti/it/secur/prod/reg97-6e.pdf

1997 年 10 月に情報・コンピュータ・通信政策委員会の情報セキュリティ・プライバシー専門家グループが公表した同文書は、改めてＯＥＣＤ「プライバシー・ガイドライン」をインターネット時代に向けて再評価し、加盟各国政府に対し、同ガイドラインの遵守、履行を求める旨を宣言した。

⑶ グローバルネットワーク社会におけるプライバシー保護
(Privacy Protection in a Global Networked Society)

1998 年 2 月 16 日、17 日にＯＥＣＤの諮問委員会である BIAC (Business and Industry Advisory Committee) が支援する国際ワークショップは「グローバルネットワーク社会におけるプライバシー保護」のテーマの下、プライバシー向上技術の開発、越境データ流通問題の解決のための標準契約モデルの採用等について討議した。

http://www.oecd.org/document/41/0,2340,en_2649_34255_1905833_1_1_1_1,00.html

⑷ グローバルネットワーク社会におけるプライバシー保護に関する閣僚宣言（Ministerial Declaration on the Protection of Privacy on Global Networks）“オタワ宣言”

http://www.oecd.org/dataoecd/39/13/1840065.pdf

1998 年 10 月 7 日から 9 日までオタワで開催されたＯＥＣＤ閣僚会議の「ボーダレスワールド：世界的な電子商取引の可能性の実現（OECD Ministerial Conference "A Borderless World:Realising the Potential of Global Electronic Commerce" 7-9 October 1998, Ottawa, Canada）」では、「グローバルネットワーク社会におけるプライバシー保護に関する閣僚宣言」を採択した。同宣言はプライバシー保護の手段として、国際機関、各国政府、民間部門が果たすべき役割を明記し、民間部門のプライバシー保護について法律による保護を主張するＥＵと、業界の自主規制を中心とする日本及び米国の主張を併記する格好で、法律や自主規制、行政的手段そのいずれをも有効な手段として位置付けた。

また同宣言は、1980 年 9 月 23 日 OECD の委員会によって採用された「OECD プライバシー・ガイドライン」、1985 年 4 月 11 日 OECD の加盟国の政府によって採用された「越境データ流通に関する宣言」、1997 年 3 月 27 日 OECD の委員会によって採用された「暗号政策用のガイドラインに関する勧告」を改めて再確認するとともに、以下の 3 点について、今後具体策を検討する方針を表明した。

①権利の尊重確保のため、グローバルネットワーク社会でのプライバシー保護への信頼を構築し、個人データの越境流通に対する不必要な制限を防ぐため、グローバルネットワークにおけるプライバシー保護の約束を閣僚は確認する。

②ＯＥＣＤのガイドラインに基づいたグローバルネットワーク上のプライバシー保護を確保するため、加盟国によって採用された異なるアプローチ間の連携構築に閣僚は働く。

③閣僚はＯＥＣＤ「プライバシー・ガイドライン」がグローバルネットワークに関して有効に実現されることを保証するため、それぞれの法律および慣行の枠内で必要な措置を取る。

この「オタワ宣言」は、近年のＯＥＣＤの活動としては特に重要な文書として位置づけられている。

⑸ 電子商取引の文脈での消者保護のための行動指針に関するＯＥＣＤ理事会勧告（Recommendation of the Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce）

1999 年 12 月 8 日には、電子商取引との関係で「電子商取引の文脈での消者保護のための行動指針に関するＯＥＣＤ理事会勧告」を採択した。同ガイドラインは BtoC の電子商取引に従事する企業に対し、1980 年のＯＥＣＤ「プライバシー・ガイドライン」の 8 原則に従うこと及び 1998 年のＯＥＣＤオタワ閣僚級宣言を考慮に入れることを求めたものである。消費者が一方的になされる商業メールのメッセージを受け取りたくないと指定した時は、その選択は尊重されるべき、としてオプトアウトする権利を消費者に与えるように求めている。

http://www.oecd.org/document/18/0,2340,en_2649_201185_1815186_1_1_1_1,00.html

⑹ ＯＥＣＤ加盟国の個人情報保護法制定状況

(括弧内は加盟年)

国　名	EU 加盟国	対象データ	
		公共部門	民間部門
Australia (1971)		○	
Austria (1961)	○	○	○
Belgium (1961)	○	○	○
Canada (1961)		○	ケベック
Czech Republic (1995)			○
Denmark (1961)	○	○	○
Finland (1969)	○	○	○
France (1961)	○	○	○
Germany (1961)	○	○	○
Greece (1961)	○	○	○
Hungary (1996)		○	○
Iceland (1961)		○	○
Ireland (1961)	○	○	○
Italy (1961)	○		○
Japan (1964)		○	
Korea (1996)		○	
Luxembourg (1961)	○	○	○
Mexico (1994)		○	
The Netherlands (1961)	○	○	○
New Zealand (1973)		○	○
Norway (1961)		○	○
Poland (1996)		○	○
Portugal (1961)	○	○	○
Slovak Republic (2000)			
Spain (1961)	○	○	○
Sweden (1961)	○	○	○
Switzerland (1961)		○	○
Turkey (1961)			
United Kingdom (1961)	○	○	○
United States (1961)		○	

3.2.5 欧州評議会（Council of Europe）の「個人データの自動処理に関する個人の保護のための条約（108 号）」

欧州評議会（CE）は、欧州連合（EU）機関の一部と混同される（例えば欧州理事会：European Council）ことが多いが全く別の組織機関である。我が国では、1980 年のＯＥＣＤ「プライバシー・ガイドライン」が特に知られているが、欧州にあっては、米国という或る種対立関係にあって“妥協的産物”として結実した「プライバシー・ガイドライン」よりも、1980 年 9 月 17 日に欧州評議会（Council of Europe）理事会（閣僚級）が採択した「個人データの自動処理にかかる個人の保護に関する条約（108 号）」（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）（1981 年 1 月 28 日に署名に付され 1985 年 10 月 1 日に発効）が重要視されていることはあまり知られていない。以下に条約の概要（枠組み）を紹介する。

前文
第 1 章 総則
　第 1 条 対象と目的、第 2 条 定義、第 3 条 適用範囲、
第 2 章 データ保護の基本原則、
　第 4 条 当事者の責務、
　第 5 条 データ内容等
　　→ ＯＥＣＤ「収集制限の原則」「データ内容の原則」「目的明確化の原則」「利用制限の原則」
　第 6 条 特別のカテゴリーのデータ　→ 欧州法ではセンシティブデータの処理を禁止
　第 7 条 データの安全保護　→ ＯＥＣＤ「安全保護の原則」
　第 8 条 データ主体の付加的保証措置　→ ＯＥＣＤ「公開の原則」「個人参加の原則」
　第 9 条 例外と制約、第 10 条 制裁と救済方法、第 11 条 保護の拡大
第 3 章 個人データの越境流通
　第 12 条 個人データの越境流通と国内法
第 4 章 相互扶助（補助）
　第 13 条 関係者における協力、第 14 条 海外居住者に対する援助、第 15 条 指定された当局から付与された支援の保障、第 16 条 支援要請の拒否、第 17 条 支援手続きとコスト
第 5 章 諮問委員会
　第 18 条 諮問委員会、第 19 条 委員会の機能、第 20 条 手続き
第 6 章 修正
　第 21 条 修正
第 7 章 終章
　第 22 条 執行、第 23 条 非加盟国の参加、第 24 条 領域、第 25 条 留保、第 26 条 条約の破棄
　第 27 条 通知

本条約の目的は、個々人の私的領域において、基本的自由権、特に、プライバシーの権利や個人に

関する自動処理に関して安全化をはかることである（第 1 条）。個人データの定義としては、識別され身元確認可能な個人に関するいかなる情報も意味する（第 2 条）。また、本条約の及ぶ範囲は、公的部門、民間部門双方の個人のデータファイルおよび自動処理に係るデータで、マニュアル処理は含まれない。第 2 章の「個人データ保護の基本原則」は、関係者の義務を規定するが、「内容的にはＯＥＣＤ理事会勧告のそれとほぼ同じ」（堀部政男「プライバシーと高度情報化社会」岩波新書 1988 年 77 頁）である故か、本条約は同年のＯＥＣＤ「プライバシーガイドライン」の“陰”となり、さしたる脚光を浴びることもなかった。しかし「欧州諸国を基準としたプライバシーの国際水準を示したもの」(前掲書)であることも事実である。

3.2.6 欧州連合（EU）とプライバシー

欧州は国際社会の中でも早くからプライバシー保護に関する立法措置を採ってきたが、1995 年以降、国際的なインターネットの普及拡大化に伴い、ネットワーク社会の個人情報の保護に関する対応を継続的に行っている。以下主な活動を列挙する。

①1990 年 7 月欧州共同体（EC）「個人データの取扱いに係る個人の保護に関する理事会指令提案」（Proposal for a Council Directive concerning the protection of individuals in relation to the protection of personal data）

②「公衆デジタル通信網特に ISDN 及び公衆デジタル移動体通信網における個人データ及びプライバシー保護に関する理事会指令提案」」（Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital networks(ISDN) and public digital mobile networks）

③1995 年 10 月「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」。(http://www.privacy.org/pi/intl_orgs/ec/eudp.html)

④1997 年 12 月「通信部門における個人データ処理及びプライバシー保護に関する欧州議会及び理事会の指令」。(http://europa.eu.int/eur-lex/en/lif/dat/1997/en_397L0066.html)

⑤1998 年 10 月 24 日から「ＥＵ個人データ保護指令」発効。

⑥1998 年 11 月 23 日、欧州委員会は Safe Harbor 原則について、実効性の欠如を理由として米国から提出されていた Safe Harbor 原則を正式に却下。

⑦1999 年 3 月、欧州議会（European Parliament）はインターネット利用者とインターネット・サービス・プロバイダーに対しインターネット上の個人情報保護に関する提言を発表。

⑧1999 年 7 月 29 日、 欧州委員会（European Commission）は、オーストリア、デンマーク、フランス、ドイツ、アイルランド、ルクセンブルグ、オランダ、スペイン、及び英国の 9 カ国が 1995 年の「ＥＵ個人データ保護指令」を遵守するための法律をまだ施行していないことに対して公式に警告。

⑨1999 年 9 月 8 日、欧州委員会と World Wide Web Consortium（W3C）はブリュッセルでミーティングを行い、W3Cが開発を進めているＰ３Ｐ；Platform for Privacy Preferences （インターネット上で、Web サイトの運営者とサイトの訪問者の間で個人情報をやり取りするための技術仕様）がＥＵ指令の文脈で適用可能であるかどうかを検討。

⑩2000 年 1 月、欧州委員会は、フランス、ルクセンブルグ、オランダ、ドイツ、アイルランドの 5 カ国に対

し、国内法に「1995 年のＥＵ個人データ保護指令」を十分に反映させていないとして、欧州裁判所（European Court of Justice）に提訴することを発表。

⑪2000 年 5 月に欧州連合と米国商務省間で基本的な合意（Safe Harbor 原則）が達成された。（2000 年 7 月に米国商務省が文書を公表）

⑫2002 年 7 月の「電子通信分野における個人データの処理及びプライバシー保護に関する欧州議会及び理事会の指令」（プライバシー及び電気通信指令）
（ http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf ）

3.2.7　1995 年「EU 個人データ保護指令」の概要

(1)　はじめに

1995 年の「EU データ保護指令」とは、1990 年に欧州委員会（European Commission）から「個人情報を処理する場合の個人情報の保護と処理された個人情報の自由な流通に関する理事会指令案（Personal for Council Directive, SYN 287, On the protection of individuals with regard to the processing of personal data and on the free movement of such data）」が提出され、同年7月の「個人データ処理に係る個人の保護に関する理事会指令提案」に修正と検討を加え 1995 年 10 月 24 日に「個人データ処理に係る個人情報の保護及び当該データの自由な移動に関する 1995 年 10 月 24 日の欧州議会及び理事会の 95／46／EC 指令（Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data'）」として採択されたものである。

同指令は、本指令の採択から少なくとも 3 年以内に本指令を遵守するために必要な法律、規則及び行政規定を発効することを域内各国に求め（第 32 条）、1998 年 10 月 25 日に発効した。「指令(Drective)」は「規則(Regulation)」のように加盟国に直接適用されるものではないが、加盟国を拘束し「指令」に従わない場合は欧州裁判所(European Court of Justice)に提訴されることになる。

(2)　「ＥＵ個人データ保護指令」と日本法

我が国の個人情報保護法の制定にあたっては、従来どおり「ＯＥＣＤ8原則」を引き継いだほか、欧州法の仕組みも参考にしたことは「個人情報保護検討部会」や「法制化専門委員会」等の議事録でも明らかである。

しかし欧州法の特徴である「データ保護監督官（Data Protection & Privacy Commissioner）」制度（当該職は法律により設置された行政機関の長で行政側から独立し議会に対して報告義務を負う）等、重要な条項のなかでも採用されなかった部分もある。（コミッショナー制度は、カナダ（州を含む）、オーストラリア、香港、ニュージーランド等で導入されている。）

また第三国への「データ移転禁止」条項は、原則（第 25 条）と例外規定（第 26 条）からなるが、欧州と米国間では「Safe Harbor 協定」締結として機能したが、我が国との関係は、原則条項の適用のないまま

(例外規定の適用)、現在に至っている。

以下に、我が国と直接関係ある指令(第IV章(第三国への個人データの移転禁止)及び第VI章(監督機関及び個人データの処理に係る個人の保護に関する作業部会)について若干触れておく。

①第三国への個人データの移転

指令の中で、日本を含む第三国にとって問題視されているのが、第三国への個人データの移転に関する規定(第4章 第 25 条・第 26 条)である。従来からEU域内のデータ保護法には、第三国へのデータ流出に関する規制が設けられており、1980 年のOECD「プライバシー・ガイドライン」も、第 3 部「国際的適用における基本原則―自由な流通と合法的制限―」において、個人データの国際流通の制限を可能としている。しかしながら、本規定が問題であるのは「充分なレベルの保護措置(第 25 条 1 項)」とは、具体的にどの程度のものか明示していない点である。第 26 条(例外規定)で実質的に救済するものの、具体的明示的でないため「第三国」にとっては悩ましい問題となっている。

「十分な(adequate)レベル」という十分性の証明には、合理的かつ明確な判断基準が示されない限りケースバイケースの"政治的判断"を持ち込む余地を残したものとなる。当該規定のような間接的とはいえ利害関係の対立する余地を残した規定は、外交上の場において非関税貿易障壁等の外交問題を孕むことも予見される。個人情報・プライバシーの問題は、本来、人権上の問題であるはずだが、優れて政治的外交的問題であることに気付く。

(参考条文)

(ⅰ)第25条(原則)

1. 構成国は、処理されている又は移転後に処理が予定されている個人データの第三国への移転は、この指令に従って採択された国内規定の順守を損うことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って、行うことができることを定めなければならない。
2. 第三国によって保障される保護のレベルの十分性は、一つのデータ移転作業又は一連のデータ移転作業に関するあらゆる状況にかんがみて評価されなければならない。特に、データの性質、予定されている処理作業の目的及び期間、発信国及び最終の目的国、当該第三国において有効である一般的及び分野別の法規範、並びに当該第三国において順守されている専門的規範及び安全保護対策措置が考慮されなければならない。

(3項～6項略)

(ⅱ)第26条(例外)

1. 構成国は、第 25 条の例外として、及び特別な場合を規律する国内法に別段の定めがある場合を除いて、第25条第2項の規定の意味における十分なレベルの保護を保障しない第三国に対する個人データの移転又は一連の移転は、次に掲げる条件を満たした場合に行うことができることを定めなければならない。

(a) データ主体が、予定されている移転に対して明確な同意を与えている場合。

(b) 移転が、データ主体及び管理者間の契約の履行のために、又はデータ主体の請求により、契約締結前の措置の実施のために必要である場合。

(c) 移転が、データ主体の利益のために、データ主体及び第三者間で結ばれる契約の締結又は履

行のために必要である場合。

⑷ 移転が、重要な公共の利益を根拠として、又は法的請求の確定、行使若しくは防御のために必要である場合、又は法的に要求される場合。

⑷ 移転が、データ主体の重大な利益を保護するために必要である場合。又は、

⑷ 法律又は規則に基づいて情報を一般に提供し、及び公衆一般又は正当な利益を証明する者のいずれかによる閲覧のために公開されている記録から、閲覧に関する法律に規定された条件が特定の事例において満たされる範囲内で、移転が行われる場合。

⑵.～4.項省略⑵

---

②データ主体のデータへのアクセス権

指令第 12 条は、すべてのデータ主体⑴本人⑵に、合理的で制約なく、及び過度の遅れ又は費用を伴うことなくアクセスし、処理の有無、修正、消去、停止を認めている。

我が国の法律も、個人情報に関する開示請求⑵25 条⑵、訂正⑵26 条⑵、利用停止等⑵27 条⑵の権利を明記したことは、本指令が求める「十分な⑵adequate⑵レベル」の一要件である。

本条項により自己情報コントロール権の「実効性」は認められたものと解釈できよう。

③監督機関

監督機関の権限として、調査権限、仲裁権限、法的手続を開始する権限又は司法機関に通知する権限等が与えられる。我が国では、今般の立法化の検討段階において「行政改革の途上で行政機関の増設は困難」との認識があり、検討から除外された。

しかし我が国の法施行後の成り行きによっては、再度の議論も必要となろう。

⑵参考条文⑵

第28条 監督機関

各加盟国は、1つ以上の公共機関が、本指令に従って加盟国が採択した規則の国家領域内での適用を監視することに責任を有することを規定するものとする。このような機関は委任された職務を、完全に独立して遂行するものとする。⑵2項から7項省略⑵

---

④組織内の個人データ保護担当者⑵指令第 18 条 「通知義務を負った管理者」⑵

指令は、直接的には「個人データ保護担当役員」の設置義務条項は置いてない。しかし間接的表現で、当該職を任命した場合は、監督機関への通知義務を免除する旨の規定を定めている。各国の法律は、例えばドイツでは、2001 年の改正「連邦データ保護法」第4f条⑵データ保護担当者⑵は「データ担当者を書面によって任命」する義務を負わせている。イギリスでも同様⑵1998 年「データ保護法」第 18 条⑵な規定を置いている。

組織内に「個人情報管理責任者」⑵いわゆるＣＰＯ；チーフプライバシーオフィサー⑵を置くことは、我が国の法律では明記されなかったが、行政ガイドラインでは「組織的安全管理措置」上、当該職の設置が望ましいとしている。⑵平成 16 年 10 月「経済産業省ガイドライン」24 頁⑵

3.2.8 海外（５５カ国）の個人データ保護指令への対応状況

http://www.legal.coe.int/dataprotection/Default.asp?fd=general&fn=NatLeg.htm 等参照

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
アルゼンチン	●Personal Data Protection Act	○ﾏﾆｭｱﾙﾃﾞｰﾀ 法人データ ○官　○民 ○登録/届出 ×輸出規制	Independent Commission within the Ministry of Justice
オーストラリア連邦 (OECD)	●deral Privacy Act ●Privacy Amendment (Private Sector) Act	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 登録/届出 輸出規制	Privacy Commissioner
オーストリア (OECD、EU)	●Data Protection Act (Art 1 constitutional provision)18/10/78 (01/01/80) [1981, 1982, 1986, 1987, 1988, 1989, 1993, 1994] ●Law called "Data Protection Act 2000"- Implementation of Directive 95/46/CE 17/08/99 (01/01/00) ○データ保護法令 2000 が 2000 年 1 月 1 日施行。	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ○輸出規制	DP Council, DP Commission
ベルギー王国 (OECD、EU)	●Law on privacy protection （08/12/92） ●Law of implementation of directive 95/46/CE （11/12/98） ○99 年 2 月 3 日公式ジャーナルで出版。効力は 99 年 12 月。	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 ×登録/届出 ○輸出規制有	Commission for the protection of privacy
ブラジル	●Habeas Data Law	ﾏﾆｭｱﾙﾃﾞｰﾀ 法人データ 官　民 登録/届出 輸出規制有	Privacy Commissioner
ブルガリア	●Personal Data Protection Act	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 ○登録/届出 ○輸出規制有	Commission for the Protection of personal Data
カナダ (OECD)	●Privacy Act ●The Personal Information Protection and Electronic Documents Act	○ﾏﾆｭｱﾙﾃﾞｰﾀ 法人データ ○官　○民 ○登録/届出 ○輸出規制有	Privacy Commissioner Federal Authorities

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
チリ	●Act on the Protection of Personal Data	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 ×登録/届出 輸出規制有	Non
中華人民共和国	●一般的データ保護法は存在しない. (See, Privacy & Human Rights 2004)		
コロンビア	●コロンビア憲法第 15 条は、基本的人権としてのプライバシーの権利を規定する。 ●一般的データ保護法は存在しない. (See, Privacy & Human Rights 2004)		
キプロス (EU)	●Processing of Personal Data (Protection of individuals) Law 2001	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 △登録/届出 ○輸出規制有	
チェコ (OECD、EU)	●Act of 4 April 2000 on the Protection of Personal Data and on Amendment to Some Related Acts	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ○登録/届出 ○輸出規制有	The Office for Personal Data Protection
デンマーク王国 (OECD、EU)	●Private Registers Act / 08/06/78 (01/01/1979) [1987, 1992, 1994 ●Public Authorities' Registers 08/06/78 [1987, 1989, 1991, 1992, 1994, 1996] ●The act on processing of personal data 26/05/00 ○99 年 12 月に議会に提出された法案を採用	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 ×登録/届出 ×輸出規制	Data Surveillance Authority (composed of　a Data Protection Council and a secretariat)
エストニア (EU)	●Personal Data Protection Act ●The Databases Act ●Public Information Act	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○,×法人データ ○官　○民 △登録/届出 ×輸出規制有	Estonia Data Protection Inspectorate
フィンランド (OECD、EU)	●Personal data file act/ 30/04/87 (01/01/88) [1995] ●Personal Data Act/03/99 (01/06/99) ○法律が 99 年 2 月 10 日にフィンランドの会議によって制定された。そして 99 年 6 月 1 日から施行。	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ○輸出規制	DP Board, DP Ombudsman

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
フランス (OECD、EU)	●Act on data Processing, Data files and Individual Liberties / 06/01/78 (08/01/78) [1988, 1992, 1994, 1999, 2000] ○2004.8 改正法案成立	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ×輸出規制	Computer & Freedoms National Commission (CNIL)
ドイツ連邦 (OECD、EU)	●Federal Data Protection Act　27/01/77 [1990, 1994]　2001 年成立 ●Draft law on implemention of Directive 95/46 EC ●Land legislation	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ×輸出規制	Federal Commissioner for Data Protection (publicSector) /Data Protection Officer (PrivateSector)
ギリシャ (OECD、EU)	●Law n°2472 on the Protection of individuals with regard to the processing of Personal Data　26/03/1997 (12/04/97) [03/2000] ○法律 2472 が 97 年 4 月 10 日に採用。	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ×輸出規制	Personal Data Protection Authority
香港 (特別行政区)	●Personal Data (Privacy) Ordinance	×ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 登録/届出 輸出規制有	Office of the Privacy Commissioner for Personal Data
ハンガリー (OECD、EU)	●Act No LXIII of 1992 on Protection of Personal Data and Disclosure of Data of Public Interest	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ○登録/届出 ×輸出規制有	Parliamentary Commissioner for Data Protection and Freedom of Information Hungary
アイスランド (OECD)	●Act on protection of individuals with regard to the processing of personal data	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 ○登録/届出 ○輸出規制有	Personal Data Protection Authority
インド	●1950 年のインド憲法はプライバシーの権利を明確には認めていない. ●一般的データ保護法も存在しない. ･1998 年 7 月にバジパイ首相に「コンピュータ･データの取扱いに関する情報セキュリティ、プライバシー･データ保護法に関する国家政策」の設立を要求する「IT 行動計画」を提出。(英国データ保護法を模範とし、プライバシーや暗号化を含むいくつかのサイバー法を推奨) (See, Privacy & Human Rights 2004)		

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
アイルランド (OECD、EU)	● Data Protection Act /13/07/88 (19/04/89) ●Draft on implementetion of directive 95/46/EC / ●Transposition directive 95/46/CE **○98 年 7 月に政府に法律案提出。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **×輸出規制**	Data ProtectionCommissioner
イスラエル	●Act No. 5741 on the protection of privacy ●Administrative Data Protection Act No. 5746	**ﾏﾆｭｱﾙﾃﾞｰﾀ** **法人データ** **官　○民** **△登録/届出** **輸出規制**	Registrar of Databases
イタリア (OECD、EU)	● Protection of individuals and other subject with regard to the processing of personal data act (31/12/96)[97,98,99] ●Decrees of the President	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **×輸出規制**	Garante
日本 (OECD)	●個人情報の保護に関する法律 ●行政機関等個人情報保護法 ●独立行政機関個人情報保護法	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **×輸出規制**	内閣府 総務省 経済産業省
ヨルダン (**ハシミテ王朝王国**)	●一般的データ保護法も存在しない. ・プライバシーの概念はアラブ世界にも存在するがその内容と意味は西洋の概念とは異なる。 ・伝統的アラブのプライバシーは「個人」や「秘密」「私的領域」は内包しない。 (See, Privacy & Human Rights 2004)		
ラトビア (EU)	●Personal Data Protection Law	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **○登録/届出** **○輸出規制有**	State Data Inspection (Datu valsts inspekcija)
リトアニア (EU)	●Republic of Lithuania Law on Legal Protection of Personal Data,21 January 2003, No. IX-1296	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **△登録/届出** **△輸出規制有**	State Data Protection Inspectorate**（英語）** (Valstybinė Duomenų Apsaugos Inspekcija)

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
ルクセンブルク大公国 (OECD、EU)	●Act Concerning the Use of Nominal Data in Computer processing /31/03 /1979 [1987, 1992, 1993] ●Bill on the Protection of Individuals with regard to the Processing of Personal Data- draft / 29/05/98 **○法案が政府で承認され議会に提出された。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官 ○民** **×登録/届出** **×輸出規制**	Consultative Commission for data protection Privacy Protection Commission
マレーシア	･個人データ保護法案(9 つのデータ保護原則)は、2004 年に成立すると思われたが再三に亘り遅れている。 ･法案の第3章にはコミッショナーや審判機関の設置 (See, Privacy & Human Rights 2004)		
マルタ (EU)	●Data Protection Act XXVI of 2001, as amended by Act XXXI of 2002.	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官 ○民** **○登録/届出** **△輸出規制有**	Office of the Commissioner for Data Protection
メキシコ (OECD)	●Federal Transparency and access to public government information Law	**ﾏﾆｭｱﾙﾃﾞｰﾀ** **法人データ** **官 民** **登録/届出** **輸出規制有**	Federal Institute of Access to Public Information
オランダ王国 (OECD、EU)	●Data Protection Act / 28/12/88 (01/07/89) [1990, 1996] Personal Data Protection /03/07/00 **○法案が 99 年 11 月 23 日に下院で採択。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官 ○民** **×登録/届出** **○輸出規制**	Registration Chamber / DP Commission /
ニュージーランド (OECD)	●Privacy Act	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官 ○民** **登録/届出** **×輸出規制**	Privacy Commissioner
ノルウェー王国 (OECD)	●Personal Data Act	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官 ○民** **○登録/届出** **○輸出規制**	Data Inspectorate

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
ペルー	● Law No. 26.301 (regulates the procedural aspects of the Habeas Data Action)	**ﾏﾆｭｱﾙﾃﾞｰﾀ** **法人データ** **官　○民** **登録/届出** **輸出規制有**	Non
フィリピン	●一般的なデータ保護法はない。(IT･電子商取引評議員会(ITECC)は 2003 年にデータ･プライバシー保護法を提案) ●民法典第 26 条は「すべての人は尊厳、隣人および他の人の心の個性、プライバシおよび平和を尊重するものとする」。同第 32 条(11)は「任意の方法でコミュニケーションと通信のプライバシーを妨害、侵害した者に対する損害賠償責任」を規定。 (See, Privacy & Human Rights 2004)		
ポーランド (OECD、EU)	● ACT of August 29, 1997 on the Protection of Personal Data with amendments which will enter into a force on May 1, 2004	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **○法人データ** **○官　○民** **△登録/届出** **○輸出規制有**	Inspector General for the Protection of Personal Data
ポルトガル (OECD、EU)	●Protection of Personal Data Act / l 26/10/1998 (27/10/98) **○98 年 10 月 26 日の法律 67／98 に反映。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **○輸出規制**	National Data protection Commission/
ルーマニア	●Law on the Protection of Individuals with Regard to the Processing of Personal Data and the Free movement of Such Data	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **○法人データ** **○官　○民** **○登録/届出** **○輸出規制**	People's Advocate
ロシア連邦 (OECD)	Art.24, 1993 Constitution **○憲法規定のみ**		
サンマリノ	●Act on Collection, Elaboration and Use of computerised personal data	**×ﾏﾆｭｱﾙﾃﾞｰﾀ** **○法人データ** **○官　○民** **○登録/届出** **△輸出規制**	Guarantor for the Protection of Confidential and Personal Data

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
シンガポール	・一般的なプライバシー・データ保護法は存在しない. ・シンガポール憲法は英国式であるが.プライバシーへの明示的な権利を含んでいない。 ・1998 年、国立インターネット諮問委員会は、「個人情報保護、e-コマースのための消費者行動基準」を公表。 (See, Privacy & Human Rights 2004)		
スロバキア (EU)	●ACT No 428 of 3 July 2002 on personal data protection(Zákon o ochrane osobných údajov č.428/2002)	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **△登録/届出** **×輸出規制有**	The Office for personal data protection
スロベニア (EU)	●Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP, Ur.l. RS No. 59/99)	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **○登録/届出** **△輸出規制有**	Human Rights Ombudsman
南アフリカ	●1996 年の南アフリカ憲法第 14 条はプライバシーの権利を規定。 ●南アフリカにはプライバシー・一般的データ保護法若しくは一般法による保護は現在ない。 (See, Privacy & Human Rights 2004)		
韓国 (OECD)	●Act on the Protection of Personal Information Managed by Public Agencies	**×ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　民** **登録/届出** **×輸出規制有**	
スペイン王国 (OECD、EU)	●Personal data protection act 13/12/99 (14/01/00) **○99 年 12 月 13 日の実行法律が 2000 年 1 月 14 日に施行。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **×輸出規制**	DP Agency, Consultative Council (Madrid has its own legislation and independent authority)
スウェーデン王国 (OECD、EU)	● Personal Data Act / 29/04/1998 (24/10/98) [11/05/73, 2000] **○指令は 98 年 9 月 3 日のＳＦＳ1998：204 と規則ＳＦＳ1998：1191 に反映。98 年 10 月２５日施行。**	**○ﾏﾆｭｱﾙﾃﾞｰﾀ** **×法人データ** **○官　○民** **×登録/届出** **○輸出規制**	Data Inspection Board

加盟国	立法化の状況 (法律名の後の括弧内は施行日と改定日)	保護の態様	監督機関 DataProtectionAuthority
スイス連邦 (OECD)	●Federal Data Protection Act Ordinances: OLPD, OALSP	○ﾏﾆｭｱﾙﾃﾞｰﾀ ○法人データ ○官　○民 △登録/届出 △輸出規制	Swiss Federal Data Protection Commissioner
台湾	●Computer-Processed Personal Data Protection Law	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ○登録/届出 輸出規制	Ministry of Justice
タイ王国	●Official Information Act B.E 2540	ﾏﾆｭｱﾙﾃﾞｰﾀ 法人データ ○官　　民 登録/届出 輸出規制	Official Information Commission's Office
トルコ (OECD)	○Art. 20, 2001 Constitution		
ウクライナ	○Art. 32, 1996 Constitution		
英国 (OECD、EU)	●Data Protection Act /16/07/1998 ○データ保護法1998が98年7月16日に採択された。	○ﾏﾆｭｱﾙﾃﾞｰﾀ ×法人データ ○官　○民 ×登録/届出 ○輸出規制	DP (and freedom of information) Commissioner /
米国 (OECD)	● Privacy Act 1974 ● Different sectors act on personal data protection: a) Cable Privacy Protection Act b) Family Educational Right to Privacy Act c) Electronic Communications Privacy Act ● Safe harbor principles		

3.3 アメリカのプライバシー政策

3.3.1 はじめに

プライバシーの権利の歴史は、19 世紀末の Warren と Brandeis による Right to Privacy, 4 Harvard L.R.193(1890) に始まる。その後、裁判例を重ね、1960 年に W. Prosser が Privacy , 48 Cal. L. Rev. 383(1960) でプライバシーの法理を4類型化した。また、1960－1970年代になると、コンピュータの普及拡大により事務処理において大量一括データ処理が一般的となり、コンピュータ･プライバシーの危機に直面することになった。そして 1967 年、Alan F. Westin がその著 Privacy and Freedom で「自己に関する情報の流れをコントロールする個人の権利」と定義した。この考えは「現代的プライバシー」として「伝統的プライバシー(the Right to be let alone')」と区別される。1970 年の公正信用報告法（Fair Credit Reporting Act）は米国で最も早いセクトラルなプライバシー保護法であるが、特に 1974 年のプライバシー法（Privacy Act）に基づいて設置されたプライバシー保護調査委員会が 1977 年に発表した Personal Privacy in an Information Society（http://www.epic.org/privacy/ppsc1977report/）では、プライバシー法の原則は8つに整理できるとした。（①公開の原則(THE OPENNESS PRINCIPLE) ②個人アクセスの原則(THE INDIVIDUAL ACCESS PRINCIPLE) ③個人参加の原則(THE INDIVIDUAL PARTICIPATION PRINCIPLE) ④収集制限の原則(THE COLLECTION LIMITATION PRINCIPLE) ⑤使用制限の原則(THE USE LIMITATION PRINCIPLE) ⑥提供制限の原則(THE DISCLOSURE LIMITATION PRINCIPLE) ⑦情報管理の原則(THE INFORMATION MANAGEMENT PRINCIPLE) ⑧責任の原則(THE ACCOUNTABILITY PRINCIPLE)）（堀部「前掲書」32 頁）

http://www.epic.org/privacy/ppsc1977report/c13.htm

その後「8原則」がＯＥＣＤでも使用されるようになったことは周知のとおりである。

3.3.2 連邦政府のプライバシー法

（1）１９７４年プライバシー法

1974 年のプライバシー法（Privacy Act of 1974, Pub.L.No93-579（1975 年 9 月 27 日施行））は、連邦政府の記録の誤用から個人のプライバシーを保護し、連邦政府機関が保有する個人情報（記録）へ本人がアクセスできることを定め、またプライバシー保護調査委員会を設置する等のため、第 552 条に（a）を追加して、合衆国法典第五編を改正した法律である。

合衆国法典「第 5 編 552 条」とは、「情報の自由法」である。(Freedom of Information Act ,

Pub. L. No. 89-487,80 Stat.250 (1966) (codified as amended at 5 U.S, C. 552 (1994)))その次に「552 a 条」(プライバシー法)として本法が追加挿入されたものである。（ちなみに「552 b 条」は「サンシャイン法」（Government in the Sunshine Act）と呼ばれ議会の情報公開に関する法律である。）

こうした立法経緯から政府情報の公開請求を認めた「情報公開法」と政府機関に記録された個人情報の秘匿・保護と開示・訂正を認めた「プライバシー法」とは情報の保護と利用に関する表裏一体の法制ということが判る。同法は、行政機関に対して同機関が保有する記録システム(system of records)に適切な個人情報保護措置を義務づけ、情報主体（individual）に対しては記録システムに登録されている個人情報へのアクセス権を認めるものである。

同法には個人情報が収集されたときの目的と整合的な「日常的な利用（routine use）」であれば個人情報の開示を認める条項が含まれており（Sec. 552a）(a)－(7) the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected; 社会保険番号（Social Security Number）の利用制限も、近年では名目的となり実効性に欠けるといわれている。

社会保険番号（Social Security Numbers）は、「1935 年社会保障法」に基づいて発行される個人番号であるが、本来的使用の他にその一意性がコンピュータ管理社会に都合の良い一種の「身分証明番号」の機能を果たしている。

また連邦政府で推進されている新交通システム ITS (Intelligent Transportation Systems) http://www.its.dot.gov/ で使用されるICカードは、運転免許情報の他、銀行・行政・医療等システムとの共用情報が記録されるものであるが、相互利用の利便性とともに、これらの情報が第三者に漏洩した場合の危険性も内在する。こうした背景から連邦機関が保有する情報でありながら、運転免許情報や税務情報等を対象とした個別法の必要性が叫ばれている。

(2)セクトラル（個別領域）法

以下は、連邦上の個人情報保護法として個別領域毎に制定されている代表的な法律である。

①税制改革法(Tax Reform Act 1976,42 U.S.C. § 405(C) (2)(c) (1979 Supp.))
②金融プライバシー権利法（Right to Financial Privacy Act of 1978,12 U.S.C. § 3401 et seq.）
③公正信用報告法（Fair Credit Reporting Act (1970) (1999)
④ビデオプライバシー保護法（Video Privacy Protection Act）
⑤ケーブルTVプライバシー保護法（Cable Privacy Protection Act）
⑥家庭教育の権利とプライバシー法（Family Educational Rights and Privacy Act）
⑦運転者プライバシー保護法（Drivers Privacy Protection Act）
⑧電話利用者保護法（Telephone Consumer Protection Act）
⑨児童オンラインプライバシー保護法（Child Online Privacy Protection Act（1998））
⑩債務取立法（Debt Collection Act of 1982,P.L.97-365.）
⑪コンピュータ安全保護法（Computer Security Act of 1988,P.L.100-235.）
⑫事務処理削減法（政府の個人情報収集の削減を求めた。）
（Paperwork Reduction Act of 1980,P.L. 96-511,44 U.S.C. § § 3501-3520.）

（連邦の他、州レベルでも分野別の法律が存在する。）

3.3.3 米国情報通信政策と新しいプライバシーの問題

米国は「プライバシーの権利」“発祥の地”であるが、今日的な情報プライバシーの問題は、1993年のNII（National Information Infrastructure）－全米情報基盤－に端を発すると理解されている。

今日のインターネットは、1991年3月全米科学財団(National Science Foundation)がネットワークの商用使用制限を撤廃したことにより、商用インターネット協会(CIX：Commercial Internet eXchange Inc.)が創立されこれを経由して一般への利用接続が正式に開放され、急激かつ地球規模で拡大したものである。

1995年6月にNIIの推進母体として情報基盤タスクフォース（IITF：Information Infrastructure Task Force）を設立し、(1)情報政策委員会 (2)電気通信政策委員会(3)応用技術委員会(4)NII セキュリティフォーラム等の委員会、ワーキンググループを設立した。

特に情報政策委員会では、1997年4月、「NII とプライバシーの促進に関するオプションペーパー」（Options for Promoting Privacy on the National Information Infrastructure (Draft for Public Comment, April 1997)）でプライバシー問題に影響する特定の4分野―(1)政府が保有する記録（*government records*）(2)情報通信分野（*Communications*）(3)医療記録（*Medical Records*）(4)消費者市場（*Consumer Market*）－に関する法律や政策について詳細に検討しプライバシー問題に関する課題を抽出した。(http://www.iitf.nist.gov/ipc/privacy.htm)

3.3.4 電子商取引とプライバシー

米政府は1997年7月「電子商取引の国際的枠組み」（A Framework for Global Electronic Commerce）の最終版を公表した。グローバルな電子商取引の戦略と指針を示した情報通信政策上重要な文書である。フレームワークは、「5つの原則（principles）」と「9つの問題（issues）」と提言を行い、その中で「プライバシー」や「情報セキュリティ」の問題が取り上げられた。

3.3.5 セーフハーバー原則（Safe Harbor Principle）とプライバシー

http://www.ita.doc.gov/td/ecom/menu.html

「セーフハーバー原則」とは、米国とEUとの間で取り交わされた個人データの保護に関する「十分なレベルの保護」の諸原則である。すなわち、この諸原則を遵守する限り、EUからみて「十分なレベルの保護」を確保した企業、組織とみなされる。国家に「十分なレベルの保護」システムがなくとも、企業、組織として当該保護システムを保有していれば、その企業、組織へは個人データの移転が可能というEU指令の例外規定（第26条）を活用したものである。

米国は、2000年5月にEUと基本的合意を得て、米国商務省が2000年7月に「セーフハーバー原則」として公表し、その諸原則に同意した企業組織のリストを欧州連合に提示した。

商務省は、ウェブ上で上記証明を同省に提出した企業リストを公開している。
現在、公開されている企業は、ヒューレット・パッカード、インテル、マイクロソフト等の著名企業を含めた686 社が掲示されている。(2005.3.14)

http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list

しかし、米国のプライバシーの「自主規制」の在り方は、保護の観点からは必ずしも満足のいく評価を得ていないようである。(http://www.epic.org/reports/decadedisappoint.html)

3.4 国際標準化に向かうプライバシー法

個人情報・プライバシーの権利は、基本的人権に内在するものである。
1948 年の世界人権宣言は、「何人も、自己の私事、家族、家庭若しくは通信に対して、ほしいままに干渉され、又は名誉及び信用に対して攻撃を受けることはない。人はすべて、このような干渉又は攻撃に対して法の保護を受ける権利を有する」と規定する。また 1953 年の欧州人権宣言は、「すべての者は, その私生活, 家族生活, 住居及び通信の尊重を受ける権利を有する。」と規定する。どちらも私的領域に対する干渉を受けない権利を宣言する。両宣言は半世紀前のプライバシー(私的領域情報の保護)の権利を謳ったものであるが、今日
においても見劣りのするものではない。

1970 年代、欧州を中心として、プライバシー保護の立法化が盛んになった。1980 年には、ＯＥＣＤがこれらを原則論で整理し「ガイドライン」化した。1995 年には、ＥＵが域内統一指令を発出し、一層の地域共同体の標準化をはかると同時に、第三国にも自国同様に「十分なレベルの保護」を要求した。
近年、グローバルなネット社会の到来を迎えたが、前述したとおりＯＥＣＤ、ＥＵ等も基本的原則に変更は加えず、欧州型プライバシー・グローバルスタンダードを維持している。

1998 年 9 月のオタワ宣言では「民間部門のプライバシー保護について法律による保護を主張するＥＵと、業界の自主規制を中心とする日本及び米国の主張を併記する格好で法律や自主規制、行政的手段そのいずれをも有効な手段として位置付けた」ことは、主要ＥＵ諸国も、法律だけに依拠することなくその「十分な保護」が担保できるのであれば、方法には拘らないことを示したものとも理解できる。

2004 年のデータ保護・プライバシー・コミッショナー国際会議(International Conference of Data Protection and Privacy Commissioners)では、当該会議とＩＳＯの関係に踏み込んだ決議がされた。これまで、個人データ・プライバシーの国際舞台を仕切ってきたのは欧州のプライバシー・コミッショナーである。今度はＩＳＯという国際標準化団体をステージに引き上げ、いかなる舞台を演出しようとしているのか。また、我が国にはいかなる役割が期待されているのであろうか。
ますますプライバシーの国際動向から目が離せなくなったといえよう。

■参考文献

●行政管理庁行政管理局「世界のプライバシー法」（ぎょうせい）1978 年

●堀部政男「プライバシーと高度情報化社会」（岩波新書）

■Ｗｅｂサイト（本文中表記したもの以外で参考にしたサイト）

● Privacy International （London, UK）
http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Privacy+and+Human+Rights&als[theme]=Privacy%20and%20Human%20Rights%202004&conds[1][category.....]=Privacy%20and%20Human%20Rights （Privacy & Human Rights 2004）

● Electronic Privacy Information Center （Washington, DC, USA）
http://www.epic.org/

● 国民生活政策（内閣府） http://www5.cao.go.jp/seikatsu/kojin/

4. 終わりに

平成 16 年度は「保護法」全面施行直前の 1 年間にあたり、官民ともにあわただしい 12 ヶ月であった。6 月あたりから各省庁のガイドラインが相次いで出され、一部には個別法の制定も検討されたようである。しかしながら、経済産業省のガイドラインに限っていえば通常のパブリック・コメント募集では考えられないほど多数の意見、質問が寄せられ関心の高さをうかがわせるがその回答はといえば明快なものは比較的少なく事業者の疑問を完全に払拭するにはいたっていない。（他方その他の省庁が公表したガイドラインについてのパブコメ応募件数はあまりにも少なくそのギャップに驚かされたが）。一方で個人情報漏洩事故は相変わらずマスメディアを賑わせ衰えることを知らない。今まさに、関係者は漠然とした不安の中で保護法施行元年を迎えようとしている。

個人情報保護対策に「パーフェクト」を求めることは難しい。しかし、情報窃盗に対する処罰ルールの検討や個人情報保護に関わる新しい技術・製品が相次いで市場に登場するなど心強い動きも出てきている。個人情報保護法の目指すところに到達するには官民一体となった取組みが今しばらく必要であるが、ECOM としてもその中でいささかでも貢献できればと考えている次第である。

5. 平成16年度個人情報保護WG名簿

委員	望月 大嗣	アコム㈱	事務管理部
同上	木下 直樹	㈱NTTドコモ	プロダクト＆サービス本部
同上	吉川 幸一	㈱オーエムシーカード	顧客満足推進部
同上	上嶋 哲也	佐川急便㈱	営業本部営業部
同上	佐々木 賢二	㈱シー・アイ・シー	業務部企画課
同上	藤原 康明	電気事業連合会	情報通信部
同上	高松 博光	電気事業連合会	情報通信部
同上	祝 壮吉	東京電力㈱	ｼｽﾃﾑ企画部
同上	中島 和雄	㈱東芝	法務部
同上	澤入 勝弘	㈱東芝	情報セキュリティセンター
同上	小林 英彦	㈱東芝	ﾌﾟﾗｯﾄﾌｫｰﾑｿﾘｭｰｼｮﾝ事業部
同上	森田 一平	トヨタ自動車㈱	お客様関連部
同上	脇田 正敏	トヨタ自動車㈱	国内ﾏｰｹﾃｨﾝｸﾞ部
同上	荒木 吉雄	日本アイ・ビー・エム㈱	ﾁｰﾌﾌﾟﾗｲﾊﾞｼｰｵﾌｨｻｰ
同上	成田 順子	日本アイ・ビー・エム㈱	ｽﾀｯﾌ・ｵﾍﾟﾚｰｼｮﾝｽﾞ
同上	太田 浩司	日本ユニシス㈱	法務部法務第一室
同上	西岡 信佳	㈱日立情報システムズ	法務部法務ｸﾞﾙｰﾌﾟ
同上	玉田 竜一	富士電機ホールディングス㈱	富士電機ｱﾄﾞﾊﾞﾝｽﾄﾃｸﾉﾛｼﾞｰ㈱
同上	岩田 修	マイクロソフト㈱	政策企画本部
同上	吉川 義幸	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	ｱﾄﾞｳﾞｧﾝｽﾄ・ﾃｸﾉﾛｼﾞｰ ﾃﾞｨﾚｸﾀｰ
同上	東山 治郎	松下電器産業㈱	法務本部 法務ｸﾞﾙｰﾌﾟ IT・著作権ﾁｰﾑ
同上	坂井田 輝	三井住友海上火災保険㈱	文書法務部
同上	岩間 研二	三菱電機㈱	ｲﾝﾌｫﾒｰｼｮﾝｼｽﾃﾑ事業推進本部
同上	岡田 潤之	三菱電機㈱	三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ㈱
ｱﾄﾞﾊﾞｲｻﾞ	堀部 政男	中央大学	法学部教授
同上	新保 史生	筑波大学	図書館情報学系 助教授
同上	太田 克良	経済産業省 商務情報政策局	情報経済課
同上	牧山 嘉道	西川綜合法律事務所	弁護士
同上	鈴木 正朝	ニフティ㈱	情報セキュリティ推進室
同上	鈴木 靖	㈱ｼｰﾋﾟｰﾃﾞｻﾞｲﾝｺﾝｻﾙﾃｨﾝｸﾞ	代表取締役社長
同上	藤田 素康	リコー・ヒューマン・クリエイツ㈱	社長付法務担当
同上	富永 辰也	㈲アドバンス・ティ	代表取締役
同上	土井 悦生	オリック東京法律事務所	弁護士
同上	合原 英次郎	松下電器産業㈱	東京支社
事務局	江口 正裕	電子商取引推進協議会	主席研究員

参考資料　ＥＣＯＭ「民間部門における電子商取引に係る

個人情報保護に関するガイドライン（Ver.3.0）」全文

民間部門における電子商取引に係る
個人情報保護に関するガイドライン（Ver.3.0）

平成１７年１月３１日

電子商取引推進協議会

目 次

第１章　総則

１．目　的

**　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 Marketing 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. 個人情報の保護に関する法律 (以下「個人情報保護法」という。) 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

２．適用範囲

**　このガイドラインは，電子商取引を行うに際し情報ネットワーク上で個人情報を取り扱う事業者に適用する。**

(解説)

1. このガイドラインは、電子商取引を行うにあたり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、このガイドラインを用いて次の事項を行うこととする。
   (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こと。
   (2)　個人情報保護推進体制を構築すること。
   (3)　このガイドラインと個人情報保護推進体制が適合しているかを確認し、適合していること

をウェブ画面等により社内外に表明する。

3. このガイドラインは、上記に該当する事業者が自発的に採用するものであり、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. このガイドラインは、事業者が取り扱う個人情報を適用の対象とするが、その事業者の従業員の人事管理、福利厚生等のために保有する雇用管理情報（いわゆる「インハウス情報」）については、「雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針>（厚生労働省告示第259号）に従い、別途社内規程等を定めることが望ましい。

5. 電子商取引はグローバル化が進んでいるが、このガイドラインは国境を越えた商取引に伴う個人情報保護にも適用される。

3．定　義

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)　**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、およ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であって、個人情報データベース等を事業の用に供している者をいう。

(9) **個人情報保護管理者**

事業者の代表者によって指名された者であって、個人情報保護体制の実施・運用を行う責任を有する者をいう。

(10) **個人情報保護推進体制**

事業者が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、インターネット等の情報ネットワークの定義について

(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)など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。

2. 個人情報の定義について

(1)「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。

(2)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。但し、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。

(3)「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体, 財産, 職種, 肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問わない。なお, 死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。また、「生存する個人」には日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため法人等の団体そのものに関する情報は含まれない。(ただし、役員、従業員等に関する情報は個人情報)。

(4)個人情報保護法は、「個人情報」、「個人データ」および「保有個人データ」の語を使い分けており、事業者に課せられた義務はそれぞれ異なるので、注意を要する。

(5)「他の情報と容易に照合することができ、…」とは、例えば通常の作業範囲において、個人情報データベース等にアクセスし、照合することができる状態をいい、他の事業者への照会を要する場合、当該事業者内部でも取扱部門が異なる場合等であって照合が困難な状態を除く。

【個人情報に該当する事例】

事例1) 本人の氏名

事例2) 生年月日、連絡先(住所・居所・電話番号・メールアドレス)、会社における職位または所属に関する情報について、それらと本人の氏名を組み合わせた情報

事例3) 特定の個人を識別できるメールアドレス情報(keizai_ichiro@meti.go.jp 等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等)

事例4) 特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報

事例5) 雇用管理情報(会社が従業員を評価した情報を含む。)

事例6) 官報、電話帳、職員録等で公にされている情報(本人の氏名等)

【個人情報に該当しない事例】

事例1）企業の財務情報等、法人等の団体そのものに関する情報（団体情報）

事例2）特定の個人を識別することができない統計情報

3.個人データ･保有個人データの定義関係

（1）企業が管理する「個人情報データベース等」を構成する個人情報を個人データと定義し、その中で企業が本人又はその代理人から求められる開示、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のすべてに応じることができる権限を有する個人データを「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 3. 定義（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。

① その個人データの存否が明らかになることで、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。

事例）家庭内暴力，児童虐待の被害者の支援団体が，加害者（配偶者または親権者）及び被害者(配偶者または子)を本人とする個人データを持っている場合

② その個人データの存否が明らかになることで、違法又は不当な行為を助長し，または誘発するおそれがあるもの。

事例1）いわゆる総会屋等による不当要求被害を防止するため，事業者が総会屋等を本人とする個人データを持っている場合

事例2）いわゆる不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人データを保有している場合

③ その個人データの存否が明らかになることで、国の安全が害されるおそれ、他国も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。

事例1）製造業者、情報サービス事業者等が、防衛に関連する兵器･設備･機器･ソフトウェア等の設計、開発担当者名が記録された個人データを保有している場合

事例2）要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合

④ その個人データの存否が明らかになることで、犯罪の予防、鎮圧また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。

事例）警察からの捜査関係事項照会や捜索差押令状の対象となった事業者がその対応の過程で捜査対象者または被疑者を本人とする個人データを保有している場合

（2）事業者が個人データを受託処理している場合で、その個人データについて、何ら取り決めがなく、自らの判断では本人に開示等をすることができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。

【個人情報データベース等に該当する事例】

事例1） 電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合せた情報を入力している場合）

事例2） ユーザーIDとユーザーが利用した取引についてのログ情報が保管されている電子ファイル（ユーザーIDを個人情報と関連付けて管理している場合）

事例3） キャンペーン、イベント等の実施にあたりウェブ画面を通して申し込みを受け付けた場合の申込者リスト

事例4） ウェブ画面を通じて行ったアンケート結果そのものを保存した電子ファイル

事例5） 氏名、住所、企業別に分類整理されている市販の人名録

【個人情報データベース等に該当しない事例】

事例1） 従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合

事例2） アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

【個人データに該当する事例】

事例1） 個人情報データベース等から他の媒体に格納したバックアップ用の個人情報

事例2） コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】

事例） 個人情報データベース等を構成する前の入力帳票に記載されている個人情報

（3）本ガイドラインでは、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項 適用範囲 （解説）3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。

(4)「個人情報保護管理者」とは、個人情報保護体制の実施・運用を行う責任を負う者をいう。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＝最高個人情報保護責任者)」が任命されている。

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　規程・方針等

４．規程・方針等の策定

事業者は，個人情報を保護するための規程を策定し、その代表者は事業の特性および規模を考慮し、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. 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。これを基に規程類(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なども含む)を策定し、従業者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(15)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)　個人情報保護管理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)　個人情報保護方針及び法定公表事項等に関する規定
個人情報保護方針は個人情報保護の取組み及び個人情報の取り扱いに関する基本的事項についての宣言であり、法定公表事項とは、個人情報保護法により公表等を義務付けられたものをいう。個人情報保護方針は個人情報保護に関する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、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。

⑸　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、取得の制限等に関する規定

このガイドラインの第6項から第15項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16項と第17項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等に関する規定

このガイドラインの第18項から第23項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24項から第31項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32項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。このガイドラインの第33項を参照して規定されるべきである。

⑿　個人情報保護の管理に関する規定

このガイドラインの第34項および第35項を参照して規定されるべきである。

⒀　個人情報保護に関する監査等に関する規定

このガイドラインの第36項および第37項を参照して規定されるべきである。

⒁　個人情報保護体制の見直しに関する規定

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。

⒂　内部規程に違反した場合の罰則に関する規定

一般的には社員の就業規則における罰則の条項を適用する。

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。

５．個人情報保護方針及び法定公表事項等の公表

事業者は、個人情報保護方針及び法定公表事項等を外部向けに文書化し、自社ウェブ画面のわかりやすい場所に公表することとする。

(解説)

事業者は、一般の人がその企業の個人情報保護方針及び法的公表事項等を入手･閲覧できるように、外部向けに文書化し、ウェブ画面のわかりやすい場所に公表することとする。個人情報護保護方針及び法的公表事項等はトップページにリンクボタンを設置し一度のクリックでその概要を参照できることが望ましい。また、文書化にあたっては、関係法令等の遵守、個人情報の利用目的、第三者提供の有無、開示等個人情報の取り扱いに関する諸手続きなど必要な事項と内容を選定し、一般にもわかりやすく記述するものとする。なお、法定公表事項等のモデルは巻末資料を参照のこと。

第３章　運用

第１節　個人情報の取得等

６．利用目的の特定

（１）個人情報を取り扱うにあたっては，本人が最終的にどのような目的で個人情報を利用するかまで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）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．事業者は, 利用目的をできる限り特定しなければならない。

利用目的の特定に当たっては, 利用目的を単に抽象的, 一般的に特定するのではなく, 事業者において最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定する必要がある。(電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。)

利用する個人情報の種類および入手先の事業者名等を特定することまで求めているわけではない。

具体的には,「○○事業における商品の発送, 新商品情報のお知らせ, 関連するアフターサービス」等を利用目的とすることが挙げられるが, 定款や寄附行為等に想定されている事業の内容に照らして, 個人情報によって識別される本人からみて, 自分の個人情報が利用される範囲が合理的に予想できる程度に特定している場合や業種を明示することで利用目的の範

囲が想定される場合には，これで足りるとされることもあり得る。しかしながら，単に「事業活動」，「お客さまのサービスの向上」等を利用目的とすることは，できる限り特定したことにはならない。なお，あらかじめ，個人情報を第三者に提供することを想定している場合には，利用目的において，その旨特定しなければならない。

２．雇用管理情報の利用目的の特定に当たっても，単に抽象的，一般的に特定するのではなく，労働者等（事業者に使用されている労働者，事業者に使用される労働者になろうとする者およびなろうとした者並びに過去において事業者に使用されていた者。以下同じ。）本人が，取得された当該本人の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，個別的に特定しなければならない。

【具体的に利用目的を特定している事例】

事例1）「ネット販売業における商品の発送、代金決済、新商品・サービスに関する情報の通知のために利用する。」

事例2）「××サービスの提供にあたりサービス内容の確認、代金決済、サービスご提供後の満足度調査のお願いのために利用する。」

事例3）「お客様向けメール・マガジンの送付先として使用する。」

事例4）「お客様からの相談に関する回答のためにのみ利用する。」

【具体的に利用目的を特定していない事例】

事例1）「当社の事業活動に供するため」

事例2）「弊社が提供するサービスの向上のため」

事例3）「マーケティング活動に用いるため」

３．（2）において利用目的の変更は，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の目的を変更して利用するとき、社会通念上、本人が想定することが困難でないと認められる範囲内で取り扱われなければならない。

【本人が想定することが困難でないと認められる範囲内に該当する事例】

事例）「当社の行う○○事業における新商品・サービスに関する情報を電子メールにより送信することがあります。」とした利用目的において、「郵便によりお知らせすることがある」旨追加することは、許容される。

参考　個人情報保護法第 15 条

７．利用目的による制限

（１）あらかじめ本人の同意を得ないで、第６項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）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、身体また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公衆衛生の向上また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国の機関もしくは地方公共団体また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、あらかじめ本人の同意を得なければならない。同意を得るために個人情報を利用すること(メールの送付や電話をかけること等)は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

【同意が必要な事例】

事例1)お客様相談センターにて収集された情報をもとに、自社商品の販売促進のために試供品を送る場合

事例2)求職者からの履歴書情報をもとに、自社商品の販売促進のために自社販売サイトの案内メールを送る場合

２．「同意」とは、本人が個人情報の取り扱いに関する情報を与えられたうえで、自己に関する個人情報の取り扱いについて承諾する意思表示をいう。ネットワーク上で行う場合には、本人による同意する旨のウェブ画面上のボタンのクリック、本人からの同意する旨のメールの受信等がこれにあたる。

３．(3)①～④の適用除外の具体的事例は次のとおり。

(1) 法令に基づく場合((3)①関連)

法令に基づいて個人情報を取り扱う場合は、その適用を受けない。

上記の根拠となる法令の規定としては、刑事訴訟法第218条（令状による捜査），地方税法第72条の63（事業税に係る質問検査権、各種税法に類似の規定あり）等が考えられる。これらについては、強制力を伴っており、回答が義務づけられているため、一律これに該当する。

事例）所得税法第225条第1項等による税務署長に対する支払調書等の提出

一方、刑事訴訟法第197条第2項（捜査に必要な取調べ）等のような、個人情報の提供が任意協力の場合についても対象となり得ると考えられるが、個別の判断が必要とされる。

＊任意協力については、法第16条第3項第1号で定める例外規定の対象となり得ると考えられるが、無条件で個人情報の提供が可能だということはなく、提供することによる公共的利益と個人情報保護との比較衡量により、提供すべきかどうかについて案件ごとに慎重に判断すべきである。

事例1）商法第274条の3による親会社の監査役の子会社に対する調査への対応

事例2）株式会社の監査等に関する商法の特例に関する法律第2条および証券取引法第193条の2の規定に基づく財務諸表監査への対応

(2) 人の生命、身体または財産の保護（(3)②関連）

人（法人を含む。）の生命または財産といった具体的な権利利益が侵害されるおそれがあり、これを保護するために個人情報の利用が必要であり、かつ、本人の同意を得ることが困難である場合（他の方法により、当該権利利益の保護が十分可能である場合を除く。）は、その適用を受けない。

事例1）急病その他の事態時に、本人について、その血液型や家族の連絡先等を医師や看護師に提供する場合

事例2）私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合

(3) 公衆衛生の向上等（(3)③関連）

公衆衛生の向上又は心身の発展途上にある児童の健全な育成のために特に必要な場合であり、かつ、本人の同意を得ることが困難である場合（他の方法により，公衆衛生の向上又は児童の健全な育成が十分可能である場合を除く。）は、その適用を受けない。

事例1）健康保険組合等の保険者等が実施する健康診断やがん検診等の保健事業について、精密検査の結果や受診状況等の情報を、健康増進施策の立案や事業の効果の向上を目的として疫学研究または統計調査のために、個人名を伏せて研究者等に提供する場合

事例2）不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関が連携して対応するために、当該関係機関等の間で当該児童生徒の情報を交換する場合

(4) 国の機関等への協力（(3)④関連）

国の機関等が法令の定める事務を実施するうえで、民間企業等の協力を得る必要があ

る場合であり、協力する民間企業等が目的外利用を行うことについて、本人の同意を得ることが当該事務の遂行に支障を及ぼすおそれがあると認められる場合は、その適用を受けない。

事例1）事業者等が，税務署の職員等の任意調査に対し、個人情報を提出する場合

事例2）事業者等が警察の任意の求めに応じて個人情報を提出する場合

4．保護法の施行前に第6項（1）により特定される利用目的以外の目的で個人情報を取り扱う旨の同意に相当するものがある場合は本項の同意があったものとみなされる。

参考　個人情報保護法第 16 条　附則第 2 条

８．適正な取得

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、個人情報の利用目的を偽るなど不正な手段を用いて取得してはならない。

なお，不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、詐欺等により取得したり、使用・開示した者には不正競争防止法（平成15年法律第46号）第14条により刑事罰（3年以下の懲役または300万円以下の罰金）が科され得る。

２．偽りその他不正な手段（騙す、脅す、盗むの他、個人情報保護法に規定されている第三者提供の措置を行っていない者から第三者への提供を受けている場合をいう。）により取得した第三者から、間接的に取得してはならない。また，個人情報保護法で規定されている第三者への提供の措置を行っていない第三者から間接的に取得してはならない。

３．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。

【不正な手段により個人情報を取得している事例】

事例1）親の同意がなく、十分な判断能力を有していない子供から、取得状況から考えて関係のない親の収入事情などの家族の個人情報を（情報ネットワークを通して）取得する場合

事例2）法第23条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

事例3）他の事業者に指示して上記事例1）または事例2）などの不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

参考　個人情報保護法第 17 条

９．取得に際しての利用目的の通知等

個人情報を取得する場合は，あらかじめその利用目的を公表していることが望ましい。公表していない場合は、取得後速やかに、その利用目的を本人に通知するか、また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または公表することが義務づけられている。

２．近年の電子的ネットワーク技術の急速な発展、多様化するお客さま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または公表することとする。

３．通知の方法としては、電子メールの利用等があり、公表についてはウェブ画面上への掲載や考えられる。なお、法定公表事項等のモデルは巻末資料を参照のこと。

【本人に通知または公表が必要な事例】

事例1) インターネット上で本人が自発的に公にしている個人情報を取得する場合

事例2) 官報、職員録等から個人情報を取得する場合

事例3) 電子メールによる問い合わせやクレームのように本人により自発的に提供される個人情報を取得する場合(本人確認や問い合わせに対する回答の目的でのみ個人情報を取得した場合を除く。)

事例4) 第三者から個人情報の提供を受ける場合

参考　個人情報保護法第 18 条第1項

10．情報ネットワーク上で本人から直接に取得する場合の措置

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 項で個人情報取得時の原則的な措置を定めたうえで、とりわけ書面または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。なお、口頭による個人情報の取得にまで、当該義務を課すものではない。

2．「明示」とは、情報ネットワーク上においては、申込者の入力画面に表示することがこれにあたる。この場合申込者が入力する以前に認識できるように配慮するする必要がある。また利用目的を明示するだけでなく、申込者の同意を取得する措置（同意ボタンの設置等）を推奨する。

3．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、本人は個人情報を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。

【本人に対し，その利用目的を明示しなければならない場合の事例】

事例1）ウェブ画面より本人から個人情報を直接取得する場合

事例2）お客様カード等に記載された個人情報を（直接本人から）取得する場合

参考　個人情報保護法第 18 条第2項

11．利用目的の変更時の措置

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．利用目的の変更は、社会通念上、本人が想定することが困難でないと認められる範囲内で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，本人に通知するか、又は公表しなければならない。

2．利用目的において特定された個人情報を取り扱う事業の範囲を超えての変更は、あらかじめ本人の同意なく行うことはできないが、例えば，利用目的において一連の個人情報の取り扱いの典型例を具体性をもって示していた場合は、その典型例から推測できる範囲内で変更することができる。

参考　個人情報保護法第 18 条第 3 項

12．取得時及び利用目的の変更時の措置の適用除外

前 9.から 11.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(4)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。

【本人または第三者の権利利益を害するおそれがある場合の事例((1)関連)】

事例) いわゆる総会屋等による不当要求等の被害を防止するため、当該総会屋担当者個人に関する情報を取得し、相互に情報交換を行っている場合で、利用目的を通知または公表することにより、当該総会屋等の逆恨みにより、第三者たる情報提供者が被害をうけるおそれがある場合

【当該事業者の権利等を害するおそれがある場合の事例((2)(関連)】

事例) 通知または公表される利用目的の内容により、当該事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密にかかわるようなものが明らかになる場合

【国の機関等への協力がある場合の事例((3)関連)】

事例) 公開手配を行わないで、被疑者に関する個人情報を, 警察から被疑者の立ち回りが予想される事業者に限って提供する場合、警察から受け取った当該個人情報取扱事業者が利用目的を本人に通知し、または公表することにより、捜査活動に重大な支障を及ぼすおそれがある場合

【利用目的が自明の場合の事例((4)関連)】

事例1) 商品･サービス等を販売･提供する場合、住所･電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品･サービス等の販売･提供のみを確実に行うた

めという利用目的であるような場合

事例2）一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡のためという利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要する）。

参考　個人情報保護法第 18 条第 4 項

13．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

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取得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取得技術を使って、
   ⑴　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。
   ⑵　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. クッキーのデータは常に個人情報に該当するわけではない。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、特定個人を識別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。なお、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結び付けて利用しないケースでもその旨をわかりやすく示したり、クッキーの使用を説明した上でなおかつ本人が利用停止を望んだ場合に備えクッキーを無効にする操作手続きを明示することが望まれる。
3. また、クッキーと同様の目的でウェブ・ビーコン(ビーコンとは標識、信号灯の意)が利用される場合もあるが、これについても事前に利用目的と実際にどのように利用しているかを「個人情報保護方針」等にわかりやすく記載し、ウェブ利用者の不安感を払拭することが望ましい。

参考　個人情報保護法第 18 条

14．子どもから個人情報を取得する場合の措置

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設定するなど、より慎重に配慮する必要がある。
3. ここで「子ども」とは、必ずしも未成年者をいうものではなく、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ことを想定した用語である。「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、適正な取得方法に配慮するものとする。
   また、子どもから両親、家族、友人等に関する個人情報を不当に取得してはならない。

15．取得の制限

事業者は,その事業の遂行に必要と判断した場合に限り個人情報を取得するものとする。思想、信条、宗教、健康状態その他人種、門地等社会的差別につながる個人情報の取得または保有に際しては厳格な取り扱いに努めなければならない。

（解説）

事業者は個人情報の取得にあたり明確な指針を策定し、事業の遂行に必要な個人情報を特定することが望まれるが、その際、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、思想、信条、宗教、健康状態その他人種、門地等社会的差別につながるおそれのある個人情報について格段の配慮を払う必要がある。事業の遂行上、止むを得ず取得する場合には、本人の同意を得る、より厳格な安全管理措置を施す、さらには、第三者提供を行わないなど取扱いに特に留意しなければならない。

第２節　個人データの管理

16．個人データの正確性の確保

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）

事業者は，利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、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。（電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。）

この場合、保有する個人データを一律にまたは常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足りる。

参考　個人情報保護法第 19 条

17．安全管理措置

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）

事業者は、その取り扱う個人データの漏えい、滅失またはき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、および技術的な安全管理措置を講じなければならない。（電話帳、カーナビゲーションシステム等の取り扱いについての場合を除く。）

その際、本人の個人データが漏えい、滅失またはき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質および個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合の事例】

事例1）公開されることを前提としていない個人データ（購買履歴、顧客嗜好・属性情報、決済関連情報等）が事業者のウェブ画面上で不特定多数に公開されている状態を事業者が放置している場合

事例2）組織変更が行われ、個人データにアクセスする必要がなくなった従業者が個人データにアクセスできる状態を事業者が放置していた場合で，その従事者が個人データを漏えい

した場合

事例3）本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失またはき損し、本人がサービスの提供を受けられなくなった場合

事例4）個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例5）個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

事例6）情報システム更新時に実データをシステム・テストに利用しその後のデータ回収・管理を怠った場合

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱い状況を一覧できる手段の整備
④個人データの安全管理措置の評価，見直しおよび改善
⑤事故または違反への対処

【各項目について講じることが望まれる事項】

①個人データの安全管理措置を講じるための組織体制の整備をする上で望まれる事項

・従業者の役割・責任の明確化

※個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。

・個人情報保護管理者（いわゆる，チーフ・プライバシー・オフィサー（ＣＰＯ））の設置

・個人データの取り扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置および作業担当者の限定

・個人データを取り扱う情報システム運用責任者の設置および担当者（システム管理者を含む。）の限定

・個人データの取り扱いにかかわるそれぞれの部署の役割と責任の明確化

・監査責任者の設置

・監査実施体制の整備
・個人データの取り扱いに関する規程等に違反している事実または兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
・個人データの漏えい等の事故が発生した場合、または発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備

※個人データの漏えい等についての情報は代表窓口、苦情対応窓口を通じ、外部からもたらされる場合もあるため、苦情の対応体制等との連携を図ることが望ましい（法第３１条を参照）。

・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
・漏えい等の事故発生時における主務大臣および認定個人情報保護団体等に対する報告体制の整備

②個人データの安全管理措置を定める規程等の整備と規程等に従った運用をする上で望まれる事項
・個人データの取り扱いに関する規程等の整備とそれらに従った運用
・個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用

※なお、これらについてのより詳細な記載事項については、下記の【個人データの取り扱いに関する規程等に記載することが望まれる事項】を参照。

・個人データの取り扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
・個人データの取り扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
・定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持

※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば，だれがどのような操作を行ったかを記録）、教育受講者一覧表等が考えられる。

③個人データの取扱い状況を一覧できる手段の整備をする上で望まれる事項
・個人データについて、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取り扱いに必要な情報を記した個人データ取扱台帳の整備
・個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④個人データの安全管理措置の評価、見直しおよび改善をするうえで望まれる事項

・監査計画の立案と、計画に基づく監査（内部監査または外部監査）の実施

・監査実施結果の取りまとめと、代表者への報告

・監査責任者から受ける監査報告、個人データに対する社会通念の変化および情報技術の進歩に応じた定期的な安全管理措置の見直しおよび改善

⑤事故または違反への対処をするうえで望まれる事項

・事実関係、再発防止策等の公表

・その他、以下の項目等の実施

ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人および主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討・実施

【個人データの取り扱いに関する規程等に記載することが望まれる事項】

以下、①取得・入力、②移送・送信、③利用・加工、④保管・バックアップ、⑤消去・廃棄という、個人データの取り扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

①取得･入力

ア．作業責任者の明確化

・個人データを取得する際の作業責任者の明確化

・取得した個人データを情報システムに入力する際の作業責任者の明確化

（以下，併せて「取得・入力」という。）

イ．手続の明確化と手続に従った実施

・取得・入力する際の手続の明確化

・定められた手続による取得・入力の実施

・権限を与えられていない者が立ち入れない建物，部屋（以下「建物等」という）での入力作業の実施

・　個人データを入力できる端末の、業務上の必要性に基づく限定

・　個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）

ウ．作業担当者の識別、認証、権限付与

・個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定

・ID とパスワードによる認証，生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定

・個人データの取得・入力業務を行う作業担当者に付与した権限の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、および作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と、権限外作業の有無の確認

②移送･送信

ア．作業責任者の明確化

・個人データを移送・送信する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・個人データを移送・送信する際の手続の明確化

・定められた手続による移送・送信の実施

・個人データを移送・送信する場合の個人データの暗号化（例えば，公衆回線を利用して個人データを送信する場合）移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）

・ＦＡＸ等におけるあて先番号確認と受領確認

・個人データを記した文書をＦＡＸ等に放置することの禁止

・暗号鍵やパスワードの適切な管理

ウ．作業担当者の識別、認証、権限付与

・個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定

・ID とパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定（例えば，個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧，変更する権限は必要ない）

・個人データの移送・送信業務を行う作業担当者に付与した権限の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、および作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と、権限外作業の有無の確認

③利用･加工

ア．作業責任者の明確化

・個人データを利用・加工する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・個人データを利用・加工する際の手続の明確化

・定められた手続による利用・加工の実施
・権限を与えられていない者が立ち入れない建物等での利用・加工の実施
・個人データを利用・加工できる端末の、業務上の必要性に基づく限定
・個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする）

ウ．作業担当者の識別、認証、権限付与
・個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
・個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

エ．作業担当者およびその権限の確認
・手続の明確化と手続に従った実施、および作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と権限外作業の有無の確認

④保管･バックアップ

ア．作業責任者の明確化
・個人データを保管・バックアップする際の作業責任者の明確化

イ．手続の明確化と手続に従った実施
・個人データを保管・バックアップする際の手続※の明確化
※情報システムで個人データを処理している場合は，個人データのみならず、オペレーティングシステム（OS）やアプリケーションのバックアップも必要となる場合がある。
・定められた手続による保管・バックアップの実施
・個人データを保管・バックアップする場合の個人データの暗号化
・暗号鍵やパスワードの適切な管理
・個人データを記録している媒体を保管する場合の施錠管理
・個人データを記録している媒体を保管する部屋，保管庫等の鍵の管理
・個人データを記録している媒体の遠隔地保管
・個人データのバックアップから迅速にデータが復元できることのテストの実施
・個人データのバックアップに関する各種事象や障害の記録

ウ．作業担当者の識別、認証，権限付与

・個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定

・ID とパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定（例えば，個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない）

・個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、および作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と権限外作業の有無の確認

⑤消去・廃棄

ア．作業責任者の明確化

・個人データを消去する際の作業責任者の明確化

・個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

イ．手続の明確化と手続に従った実施

・消去・廃棄する際の手続の明確化

・定められた手続による消去・廃棄の実施

・権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施

・個人データを消去できる端末の、業務上の必要性に基づく限定

・個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回または複数回上書きする。）

・個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

ウ．作業担当者の識別、認証、権限付与

・個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定

・ID とパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定

・個人データの消去・廃棄を行う作業担当者に付与した権限の記録

エ．作業担当者およびその権限の確認

・手続の明確化と手続に従った実施、および作業担当者の識別，認証，権限付与の

実施状況の確認

・アクセスの記録、保管、権限外作業の有無の確認

人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】

①雇用契約時及び委託契約時における非開示契約の締結

②従業者に対する教育･訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第21条を参照。

【各項目について講じることが望まれる事項】

①雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項

・従業者の採用時または委託契約時における非開示契約の締結

※雇用契約または委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。

・非開示契約に違反した場合の措置に関する規程の整備

※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲およびアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発･保守関係者、清掃担当者、警備員等が含まれる。

②従業者に対する周知･教育･訓練を実施する上で望まれる事項

・個人データおよび情報システムの安全管理に関する従業者の役割および責任を定めた内部規程等についての周知

・個人データおよび情報システムの安全管理に関する従業者の役割および責任についての教育・訓練の実施

・従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施

②盗難等の防止
③機器･装置等の物理的な保護

【各項目について講じることが望まれる事項】
①入退館（室）管理を実施する上で望まれる事項
・個人データを取り扱う業務上の、入退館（室）管理を実施している物理的に保護された室内での実施
・個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

②盗難等を防止する上で望まれる事項
・離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止
・離席時のパスワード付きスクリーンセイバ等の起動
・個人データを含む媒体の施錠保管
・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③機器･装置等を物理的に保護する上で望まれる事項
・個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

技術的安全管理措置とは、個人データおよびそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】
①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥個人データの移送･送信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策

⑧個人データを取り扱う情報システムの監視

【各項目について講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

・個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証（例えば，ID とパスワードによる認証、生体認証等）の実施

※ID とパスワードを利用する場合には、パスワードの有効期限の設定，同一または類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。

・個人データへのアクセス権限を有する各従業者が使用できる端末またはアドレス等の識別と認証（例えば，MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施

②個人データへのアクセス制御を行う上で望まれる事項

・個人データへのアクセス権限を付与すべき従業者数の最小化

・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）

・従業者に付与するアクセス権限の最小化

・個人データを格納した情報システムへの同時利用者数の制限

・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）

・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）

・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）

※情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。

※特権ユーザーに対するアクセス制御については、例えば，トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。

・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証

（例えば、ウェブアプリケーションのぜい弱性有無の検証）

③個人データへのアクセス権限の管理を行う上で望まれる事項

・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）

・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④個人データへのアクセスの記録を行う上で望まれる事項

・ 個人データへのアクセスや操作の成功と失敗の記録（例えば，個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）

・採取した記録の漏えい、滅失およびき損からの適切な保護

※個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤個人データを取り扱う情報システムについて不正ソフトウェア対策を実施する上で望まれる事項

・ウイルス対策ソフトウェアの導入

・オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用

・不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）

⑥個人データの移送（運搬、郵送、宅配便等）・送信時の対策の上で望まれる事項

・移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化）

・盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）で個人データを送信（例えば、本人および従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化

⑦個人データを取り扱う情報システムの動作確認時の対策の上で望まれる事項

・情報システムの動作確認時のテストデータとして個人データを利用することの禁止

・情報システムの変更時に、それらの変更によって情報システム又は運用環境の

セキュリティが損なわれないことの検証

⑧個人データを取り扱う情報システムの監視を行う上で望まれる事項

・個人データを取り扱う情報システムの使用状況の定期的な監視

・個人データへのアクセス状況（操作内容も含む）の監視

※個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

参考　個人情報保護法第 20 条

18．従業者の監督

（１）従業者に個人データを取り扱わせるにあたっては、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わなければならない。

（２）前項の監督にあたっては少なくとも次の事項を行わなければならない。

①規程類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課されている。個人情報の処理を実際に担当する従業者は、まさに直接に個人情報を取り扱う者として、その意識を高く持つことが求められる。なお、「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、委託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

２．実際，個人情報が漏えいする事件の原因の1つに内部関係者の介在が指摘されている。内部関係者の行為による漏えいは、それが公になることにより、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、事業者は役員をはじめすべての従業者に対し、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．教育の実施にあたっては e ラーニングの活用等により対象者の履修履歴、理解度を把握･記録することが望ましい。

４．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。

5．規程類を定め、教育を通じ従業者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。

【従業者に対して必要かつ適切な監督を行っていない場合の事例】

事例1）従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果，個人データが漏えいした場合

事例2）内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

個人データの取り扱いに関する従業者および委託先の監督，その他安全管理措置の一環として従業者を対象とするビデオおよびオンラインによるモニタリング（以下「モニタリング」という。）を実施する場合は、次の点に留意する。

その際，雇用管理に関する個人情報の取り扱いに関する重要事項を定めるときは，あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また，その重要事項を定めたときは、労働者等に周知することが望ましい。

なお，本ガイドライン及び雇用管理に関する個人情報の適正な取り扱いを確保するために事業者が講ずべき措置に関する指針（平成 16 年厚生労働省告示第 259 号）第三 九（一）に規定する雇用管理に関する個人情報の取り扱いに関する重要事項とは、モニタリングに関する事項等をいう。

・モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し，社内規程に定めるとともに、従業者に明示すること。

・モニタリングの実施に関する責任者とその権限を定めること。

・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。

・モニタリングの実施状況については、適正に行われているか監査、または確認を行うこと。

参考　個人情報保護法第 21 条

19．委託先の監督

（1）個人データの取り扱いの全部または一部を委託する場合は、その取り扱いを委託した個人データの安全管理が図られるよう、受託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）前項の監督にあたっては、このガイドラインに従い、少なくとも次の事項を行わなければならない。

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。

④前号の契約の内容が遵守されていることをあらかじめ定めた間隔で定期的に確認すること。

(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お客さま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項が定められた。

２．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。

３．委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取り扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。

４．委託者が優越的地位にある場合、その地位を利用して一方的に受託者に不当な負担を課すことがないよう配慮する。業務委託契約における個人情報漏えい事故に係る損害賠償範囲(逸失利益、情報主体に対するお詫び料等を含む)については事前に委託者、受託者双方が協議し同意をとることが望ましい。

【受託者に必要かつ適切な監督を行っていない場合の事例】

事例1) 個人データの安全管理措置の状況を契約締結時およびそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合

事例2) 個人データの取り扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合

事例3) 再委託の条件に関する指示を受託者に行わず，かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し，結果，再委託先が個人データを漏えいした場合

【個人データの取り扱いを委託する場合に契約に盛り込むことが望まれる事項】

○委託者および受託者の責任の明確化

○個人データの安全管理に関する事項

・個人データの漏えい防止，盗用禁止に関する事項

・委託契約範囲外の加工、利用の禁止

・委託契約範囲外の複写、複製の禁止

・委託契約期間

・委託契約終了後の個人データの返還・消去・廃棄に関する事項

○再委託に関する事項

・再委託を行うに当たっての委託者への文書による報告

○個人データの取扱状況に関する委託者への報告の内容および頻度

○契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）

○契約内容が遵守されなかった場合の措置

○セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

参考　個人情報保護法第 22 条

20．サイバーモール運営者の対応

サイバーモール運営者は、サイバーモールを運営するに当たり、直接個人情報を取得するオンラインショッピング業者等（以下「ショップ等」という。）が適正な個人情報保護管理を行うように適切な対策を講じ実践することとする。

（解説）

1. 本項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への提供

21．第三者への提供の制限

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、身体また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）公衆衛生の向上また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）国の機関もしくは地方公共団体また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．個人情報保護法第 23 条第 1 項では、(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。

２．(1)～(4)の適用除外の具体的事例は、7.(3)①～④と同様。

３．雇用管理に関する個人データ関連

個人データの第三者への提供((1)～(4)に該当する場合を除く。)のうち、雇用管理に関するものについては、次に掲げる事項に留意することが望ましい。その際、事業の性質および雇用管理に関する個人データの取扱状況等に応じ、必要かつ適切な措置を講じるものとする。

ここでいう雇用管理に関する個人データの第三者への提供とは、従業者の子会社への出向に際して、出向先に当該従業者の人事考課情報等の雇用管理に関する個人データを提供する場合や、派遣契約の締結に際して、契約締結前に、技術者の能力に関する情報等の雇用管理に関する個人データを提供する場合を指すものである。

したがって、企業から、その従業者の氏名、役職等の個人データの提供を受け、当該情報をデータベース化し、公開、販売することを目的とする者への提供のような場合はこの限りではない。

・ 提供先において、その従業者に対し当該個人データの取り扱いを通じて知り得た個人情報を漏らし、または盗用してはならないこととされていること。
・ 当該個人データの再提供を行うに当たっては、あらかじめ文書をもって事業者の了承を得ること。
・ 提供先における保管期間等を明確化すること。
・ 利用目的達成後の個人データを返却し、または破棄しもしくは削除し、これと併せてその処理が適切かつ確実になされていることを事業者において確認すること。
・ 提供先における個人データの複写および複製（安全管理上必要なバックアップを目的とするものを除く。）を禁止すること。

【第三者への提供とされる事例】（ただし、第 19 項（1）の場合を除く。）
事例1）親子兄弟会社、グループ会社の間で個人データを交換する場合
事例2）フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
事例3）同業者間で，特定の個人データを交換する場合
事例4）外国の会社に国内に居住している個人の個人データを提供する場合

【第三者への提供とされない事例】（ただし、利用目的による制限がある。）
事例）同一事業者内で他部門へ個人データを提供すること。

4．保護法の施行前に第三者提供を認める旨の同意に相当するものがある場合は本項の同意があったものと認められる。

参考　個人情報保護法第 23 条第 1 項

22．第三者に提供できる場合

（1）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、また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。
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または方法
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）前項②または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、また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．本項は、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．前項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うえで、本項に示すように、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への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)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、第三者への提供が許されるとする。

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，認識できたりする状態をいう。例えばウェブ画面上の見えやすいところに、「個人情報の第三者への提供について」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。なお、第24 項の解説2．において説明されている「本人の知り得る状態に置く」との違いに留意する。

4．ここで定められる措置は，いわゆる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、ウェブ画面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。

また、(2)に定める措置についても、ウェブ画面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。

【第三者に提供される個人データの項目】

事例1) 氏名、住所、メールアドレス

事例2) 氏名、商品購入履歴

【第三者への提供の手段または方法】

事例1) 電子媒体に変換して配布

事例2) インターネットに掲載

事例3) プリントアウトして交付等

6．保護法の施行前に本人に通知されているときは当該通知は第 23 条第2項により行われたものとみなされる。

参考　個人情報保護法第 23 条第 2 項･第 3 項　附則第 4 条

23．第三者への提供に該当しない場合

（１）次の各号のいずれかに該当する場合は、第２２項の第三者への提供の制限にかかる第三者への提供に該当しないものとする。

①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り扱いの全部また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あって、以下のことをあらかじめ，本人に通知し、または本人が容易に知り得る状態に置いているとき。

ア　共同利用する旨

イ　共同して利用される個人データの項目

ウ　共同して利用する者の範囲

エ　利用する者の利用目的

オ　当該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

（２）前③に規定する項目のうち、エまたはオを変更する場合は、変更する内容について、あらかじめ、本人に通知し、また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ことは、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。典型的な例として物流業者に対する商品配送業務、商品代金回収業務の委託などがあげられる。

２．合併や吸収により、事業の承継が行われ、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。ただし、移転可能時期は事業承継が正式に決定した時点以降に限られる。

【事業の承継に伴って個人データが提供される場合の事例】

事例1)合併，分社化により、新会社に個人データを渡す場合

事例2)営業譲渡により、譲渡先企業に個人データを渡す場合

３．(1)③については、複数の企業が個人情報を共有することでより効率的、一体的かつ円滑な事業展開を行うケース等が想定される。ただし，この共同利用はあらかじめ個人情報の利用目的にグループによる共同利用がある旨を本人に通知し、または容易に知りうる状態に置くことが条件になっているので注意が必要である。(この場合の複数の企業とは必ずしも資本関係の有無を条件としない)。例として旅行業界で顧客情報を共有する場合やクレジットカード利用に関する個人信用情報照会システムなどがあげられる。なお、事業者がこの共同利用を行

うにあたっては、共同利用対象会社の個人情報保護推進部門と連携を取りつつ行うものとする。

【共同利用を行うことがある事例】

事例1）グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合

事例2）親子兄弟会社の間で利用目的の範囲内で個人データを共同利用する場合

事例3）外国の会社と利用目的の範囲内で個人データを共同利用する場合

ア）共同して利用される個人データの項目

事例1）氏名、住所、メールアドレス

事例2）氏名、商品購入履歴

イ）共同利用者の範囲（本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。）

ウ）利用する者の利用目的（共同して利用する個人データの全ての利用目的）

エ）開示等の求めおよび苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等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（共同利用者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者を、「責任を有する者」といい、共同利用者の内部の担当責任者をいうのではない。）

6. 保護法の施行前に本人に通知されているときは当該通知は第 23 条第4項第三号により行われたものとみなされる。

参考　個人情報保護法第 23 条第 4 項・第 5 項　附則第 5 条

第４節　開示・変更・利用停止等の求めへの対応

24．保有個人データに関する事項の公表等

（１）保有個人データに関し、次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自社名

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、利用停止等の手続および保有個人データの開示にかかる手数料

④事業者が行う保有個人データの取り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および苦情の解決の申出先

（２）保有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項(1)から(4)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．例えば料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など誤った個人情報を保有し、その情報に基づいて業務処理を行う等により本人の利益が侵害されることも想定される。これについては、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．「本人の知り得る状態に置く」とはウェブ画面にリンク先を継続的に掲示すること、問合せ先のメールアドレスをウェブ画面などに明記し問い合わせがあった場合には速やかに回答できる体制を構築しておくことなどがあげられる。

３．事業者は、以下の(1)から(4)の場合を除いて、本人から, 自己が識別される保有個人データの利用目的の通知を求められたときは、遅滞なく、本人に通知しなければならない。

(1) 第21項(1)の措置により, 自己が識別される保有個人データの利用目的が明らかである場合

(2) 利用目的を本人に通知し、または公表することにより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

(3) 利用目的を本人に通知し、または公表することにより当該事業者の権利または利益が侵害されるおそれがある場合

(4) 国の機関等が法令の定める事務を実施する上で民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った保有個人データの利用目的を本人に通知または公表することにより、本人の同意を得ることが当該業務の遂行に支障を及ぼすおそれがある場合

４．このガイドライン第25項から第27項にて表記される「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

25．開　示

（１）保有個人データについて、本人から当該本人が識別される保有個人データの開示（当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。）を求められた場合は、本人確認のうえ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また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

②自社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）開示にあ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．第 24 項の解説 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、本項(1)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、本項(1)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。「遅滞なく」とは本人からの申し出に対して、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。

３．(1)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．(1)②の場合は、従業者の人事情報等、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．政令により、開示の方法としては、原則として、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。これについては、開示の求めを行った者から開示の方法について特に指定が無く、事業者が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり，必要な本人確認等の後，そのまま電話で問い合わせ等に回答する場合を含む。）は、当該方法について同意があったものととみなすことができる。ただし、ウェブ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。

６．雇用管理情報の開示の求めに応じる手続については、事業者はあらかじめ労働組合等と必

要に応じ協議したうえで、本人から開示を求められた保有個人データについて、その全部または一部を開示することによりそ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に該当するとして非開示とすることが想定される保有個人データを定め、従業者等に周知させるための措置を講ずるよう努めなければならない。

【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の事例】
事例）医療機関等において、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場合

【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の事例】
事例1）試験実施機関において、採点情報のすべてを開示することにより、試験制度の維持に著しい支障を及ぼすおそれがある場合
事例2）同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合

【他の法令に違反することとなる場合の事例】
事例）金融機関が「組織的な犯罪の処罰および犯罪収益の規制等に関する法律」第54条第1項に基づいて、主務大臣に取引の届出を行っていたときに、当該届出を行ったことが記録されている保有個人データを開示することが同条第2項の規定に違反する場合

参考　個人情報保護法第 25 条･政令第 6 条

26．訂正等

（1）保有個人データについて、本人から当該本人が識別される保有個人データの内容が事実でないという理由によって、当該保有個人データの訂正，追加または削除（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、遅滞なく必要な調査を行い、その結果に基づき、これに応じなければならない。

（2）前項の規定に基づき訂正等を行ったときまた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、追加または削除（「訂正等」という）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、原則として訂正等を行わなければならない。

＊「原則」…利用目的から見て訂正等が必要でない場合や誤りである旨の指摘が正しくない場合に、訂正等を行う必要はない。ただし，その場合には、遅滞なく訂正等を行わない旨を本人に通知しなければならない。

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」行うこととしているが、これは事業者においてその保有個人データを利用するうえで、厳密さがあまり求められないものまでその都度対応しなければならないとすると過度な負担となる可能性があるため、そのように定めている。

【訂正を行う必要がない事例】

事例）訂正等の対象が事実でなく評価に関する情報である場合

参考　個人情報保護法第 26 条

27．利用停止等

（１）保有個人データについて、本人から当該本人が識別される保有個人データがその利用目的の制限に違反して取り扱われているという理由もしくは適正な取得に違反して取得されたものであるという理由または第三者への提供の制限に違反して第三者に提供されているという理由によって当該保有個人データの利用の停止もしくは消去または第三者への提供の停止（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、遅滞なく利用停止等を行わなければならない。ただし、多額の費用を要する等、その実施が困難な場合であって、本人の権利利益を保護するために必要な代替措置をとるときは、この限りでない。

（２）前項の規定に基づき保有個人データについて利用停止等を行ったときまた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および同第 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または消去を求めることができるとし、さらに同第 23 条第 1 項の第三者への提供の制限に違反して第三者への提供がされている場合、第三者への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、原則として当該措置を行わなければならない。

＊「原則」…違反を是正するための必要な限度を超えている場合や手続き違反である旨の指摘が正しくない場合には、利用の停止等を行う必要はない。ただし、その場合には遅滞なく、利用の停止等を行わない旨を本人に通知しなければならない。

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する等によりその実施が困難な場合、あるいは、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、業務上大きな支障が発生したりする場合は、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、本項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

28．理由の説明

開示，訂正等および利用停止等（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または一部について、その措置をとらない旨を通知する場合また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. 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お客さまに対し、十分な説明ができないときやお客さま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面談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

29．開示等の求めに応じる手続

（1）保有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、当該方法にのっとって本人による開示等の求めを受け付けること

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，磁気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または第25項（4）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（徴収する場合）

（2）事業者は、前項にしたがって定められた開示等の求めを受け付ける方法および手数料を定めた場合の手数料の額について第 20 項（1）③により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。

（3）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、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。

（4）本人の求めに対する利用目的の通知およ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20項（1）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。

（5）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未成年者また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．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。なお、開示等の求めを受ける方法を定めない場合には、自由な申請を認めることになる。

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。本人を確実に認証できない限り、安易に開示等の求めに応ずるべきではない。

【開示の求めをする者が本人又はその代理人であることの確認の方法】

事例1）本人の場合（オンライン）：ID とパスワード

事例2）本人の場合（電話）：一定の登録情報（生年月日号等）、コールバック

事例3）本人の場合（送付（郵送、ＦＡＸ等））：運転免許証や健康保険の被保険者証等の公的証明書のコピーの送付を顧客等から受け、当該公的証明書のコピーに記載された顧客等の住所にあてて文書を書留郵便により送付

事例4）本人の場合（来所）：運転免許証、健康保険の被保険者証、写真付き住民基本台帳カード、旅券（パスポート）、外国人登録証明書、年金手帳、印鑑証明書と実印

事例5）代理人の場合（来所）：本人及び代理人について、運転免許証、健康保険の被保険者証、旅券（パスポート）、外国人登録証明書、年金手帳、弁護士の場合は登録番号、代理を示す旨の委任状

５．利用目的の通知およ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。なお、手数料を徴収する場合は、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、その手数料の額を定めなければならない。また、個人情報保護法において、訂正等およ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、未成年者また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

30．子どもの個人情報に関する保護者の求めへの対応

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

（解説）

1. 本項では、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. 上記に該当する開示等の求めがなされた場合、取得した個人情報が、第 14 項（解説）3. にて事業者が定める「子ども」の年齢に該当する本人から取得したものであることを確認するとともに、開示等の求めをする者が保護者であることを確認しなければならない。

第５節　苦情処理

31．苦情への対応

（１）個人情報の取り扱いに関する苦情の適切かつ迅速な対応に努めなければならない。

（２）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．本節は個人情報保護法第 31 条「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」で示された「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、迅速な解決を図るうえでも，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，命令の権限を持っているので、それらが発動されることもありうる。

４．苦情への対応については、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となるお客さま件数等に応じ、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、苦情への対応窓口のメールアドレス、電話番号等の連絡先はウェブ画面上の個人情報保護方針と併せ、お客さまの目につきやすいところに常時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　漏えい等が発生した場合の措置

32．漏えい等が発生した場合の措置

（１）事業者は、自社が取り扱う個人情報について漏えい等（紛失，き損を含む）の事実を把握した場合は当該漏えい等に関する個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くものとする。

（２）事業者は、自社が取り扱う個人情報について漏えい等（紛失，き損を含む）の事実を把握した場合は二次被害の防止、類似事案の発生回避の観点から、可能な限り事実関係、発生原因を遅滞なく公表するものとする。

（３）事業者は、自社が取り扱う個人情報について漏えい等（紛失，き損を含む）の事実を把握した場合は発生原因、対応策を所管する省庁に直ちに報告するものとする。

(解説)

1．事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、その個人情報の本人が適切に対応できるようにするため、事実関係を本人に速やかに通知または容易に知りうる状態に置くものとする。「容易に知りうる状態に置く」とはウェブ画面上のわかりやすい場所に継続的に表示することや、専用のフリーダイヤル設置などをいう。

2．事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、二次被害の拡大、類似事故の発生回避のため可能な限り事実関係等を遅滞なく公表すべきである。

3．事業者は、自己の取り扱う個人情報の漏えい等の事実を把握した場合は、事実関係、発生原因、対応策を当該事業者の行う事業を所管する省庁へ届け出るものとする。

4．事業者は事故発生に備え、あらかじめ緊急事態対応体制を構築し、事故発生時の対応業務につきマニュアルを整備するなど日頃から準備しておくことが重要である。

第５章　推進体制

33．個人情報保護管理者の指名

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者を内部から１名以上指名し、個人情報保護管理者としての業務を行わせるものとする。

(解説)

1．本章は，このガイドラインの諸原則を遵守するための組織およびその実施責任について定めたものである。

2．個人情報保護管理者は、事業者の代表者により指名され、個人情報保護推進体制の運営と施策の実施を行う責任者であって、個人情報の取り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管理者を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。また，個人情報保護管理者を含め各社の個人情報保護の体制については、役割、責任および権限を定めたものを文書化し、従業者に周知する必要がある。

34．個人情報保護管理者の責務

個人情報保護管理者は、このガイドラインに定められた事項を理解および遵守するとともに、従業者にこれを理解および遵守させるために、規程類の整備、個人情報保護推進体制の整備なら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および文書管理等を実施する責任を負うものとする。

(解説)

1．個人情報保護管理者は、内部で個人情報の取り扱いについて定めた規程類を整備し、それに則した個人情報保護推進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。

(1) 法令その他規範の特定

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

(2) 個人データの特定

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

(3) 規程類の策定

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規程の細則等(帳票等を含む。)を定め、必要に応じマニュアルを作成する。

(4) 計画書の策定

規程類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。グループ会社各社は、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ついては、あらかじめ必要な教育訓練を行うか、十分に教育訓練された者がその者を支援するような体制を取る必要がある。

3．個人情報の取り扱いを外部に委託する場合も、当該委託先における管理状況に関して適宜確認する。

4．個人情報保護管理者は、十分な技術的保護措置を実施する等の責任も負う。

5．個人情報保護管理者は、このガイドラインに定めるすべての事項について、適正に書面またはこれに代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から、文書管理に関する規程類を策定し、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への対応だけでなく、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、その取り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．個人情報保護推進体制のもとに個人情報保護を推進するときには、法令, 所轄官庁の指針、規程等と合致していることおよ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。

35．個人情報保護監査責任者の指名

事業者の代表者は，個人情報保護管理者からは独立し、個人情報保護推進体制の妥当性、有効性および実施状況について、本ガイドラインに定められた監査を実施する者を内部から指名し、個人情報保護監査責任者としての業務を行わせることが望ましい。

（解説）

1. 個人情報保護監査責任者は、事業者の代表者により指名され、各社の個人情報保護推進体制の整備がこのガイドラインの要求事項と合致していることおよびその運用状況を定期的に監査することが望ましい。
2. 個人情報保護監査責任者は個人情報保護体制の妥当性、有効性および実施状況を監査する立場となるため、個人情報保護管理者がこれを兼務することはできない。

36．個人情報保護監査責任者の責務

個人情報保護監査責任者は，自社の個人情報保護体制の運営状況を定期的に監査し、事業者の代表者に報告する責任を負うものとする。

（解説）

1. 事業者の個人情報保護監査責任者は、あらかじめ決められたサイクルで自社の個人情報保護推進体制を監査し、監査報告書を作成し、事業者の代表者に報告するものとする。
2. 事業者は監査状況を常時管理し、監査報告書を一定期間保管するものとする。

第６章 その他

37．見直し

事業者の代表者は、個人情報保護の実施状況およ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、少なくとも年 1 回以上保護推進体制を見直すこととする。

（解説）

事業者の代表者は、個人情報保護体制の監査等を実施するときにはその報告書の指摘事項を必ず確認し、個人情報保護推進体制の改善点等について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。

平成17年1月31日　改訂

巻末資料

「個人情報の保護に関する法律」に基づく公表事項（案）

○○○○株式会社

「個人情報の保護に関する法律」（以下「法」といいます。）に基づき，以下の事項を「公表」致します。（「本人が容易に知り得る状態に置いている」こと，及び，「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。）」に置くことを義務付けられている事項を含みます。）

１．利用目的の公表に関する事項（法 18 条 1 項）

（1）直接書面取得以外で取得する場合の「個人情報」の「利用目的」（法 18 条 1 項）

お客さまから直接書面に記載された個人情報を取得する場合（直接書面取得）は，その都度，お客さまに利用目的を明示させて頂きます（法18条2項）。それ以外で個人情報を取得する場合は，次の利用目的の制限の範囲内で取り扱わせて頂きます（法 18 条 1 項）。ただし，以下の（2），（3），（4）の場合は除きます（法 23 条 4 項）。

	「個人情報」の類型	利用目的
a.		（変更前） （変更後）
b.		
c.		

（2）委託された「個人情報」の「利用目的」（法 18 条 1 項，法 23 条 4 項 1 号）

当社が取扱いを委託されている「個人情報（個人データ）」の「利用目的」は次のとおりです。

	「個人情報」の類型	利用目的
a.		（変更前） （変更後）
b.		

（3）合併，事業承継に伴い取得した「個人情報」の「利用目的」
（法 18 条 1 項，法 23 条 4 項 2 号）

平成〇年〇月〇日の当社と〇〇〇〇株式会社との（合併・事業承継）に伴い，旧〇〇〇〇株式会社の保有する「個人情報」を取得致しました。当該「個人情報（個人データ）」の「利用目的」は次のとおり，旧〇〇〇〇株式会社において特定した「利用目的」と同じものです。

	「個人情報」の類型	利用目的
a.	顧客名簿	
b.	労働者名簿	

２．「共同利用」に関する事項（法 23 条 4 項 3 号，法 23 条 5 項）

次のaに示した○○○に関する顧客情報（「個人データ」）を、bに示した者との間で共同して利用させて頂きます。

a.	共同して利用される個人データの項目
	① 氏名 ② 住所 ③ 電話番号 ④ FAX 番号 ⑤ 電子メールアドレス, ⑥ 注文内容（商品名・数量・対価）
b.	共同して利用する者の範囲
	① ○○○○株式会社（東京都○○区） ② ○○○○株式会社（東京都○○区） ③ ○○○○株式会社（東京都○○区） ④ ○○○○株式会社（東京都○○区） ⑤ ○○○○株式会社（東京都○○区） ⑥ ○○○○株式会社（東京都○○区）
c.	利用する者の利用目的
d.	当該個人データの管理について責任を有する事業者の名称
	○○○○株式会社 連絡先（個人情報保護対策室） 〒000-0000 東京都○○区○○○1-2-3 ○○○ビル TEL 03-0000-0000 FAX 03-0000-0000 e-mail

３．「保有個人データ」に関して「本人の知り得る状態」に置くべき事項

（法 24 条 1 項）

当社の保有する「個人情報（「保有個人データ」）の「利用目的」は次のとおりです。

	「保有個人データ」の類型	利用目的
a.		(変更前) (変更後)
b.		
c.		
d.		

４．「苦情」の受付窓口に関する事項

（法 24 条 1 項 4 号，施行令 5 条，法 31 条）

（1）個人情報の取扱いに関する苦情の申出先

当社の個人情報の取扱いに関する苦情については，下記までお申し出下さい。

●お電話による場合

〇〇〇〇株式会社　個人情報保護対策室　03-0000-0000

●お手紙による場合

〒000-0000

東京都〇〇区〇〇0丁目0番0号　〇〇〇〇ビル

〇〇〇〇株式会社　個人情報保護対策室

●電子メールによる場合

parsonaldata@ispisp.com

●ご来社について

直接ご来社頂いてのお申し出はお受けかねますので，その旨ご了承賜りますようお願い申し上げます。

（2）当社の所属する「認定個人情報保護団体」の名称及び苦情の申出先

財団法人日本データ通信協会　〇〇〇〇〇〇

●お電話による場合

03-0000-0000

●お手紙による場合

〒000-0000

東京都XX区XX0丁目0番0号　XXXXXビル

●電子メールによる場合

parsonaldata@ispisp.com

●面談によるご相談について

５．「開示等の求め」に応じる手続等に関する事項（法 29 条）

（1）開示の求めの対象となる項目（「保有個人データ」の特定に資する情報）

開示の対象としている個人情報（「保有個人データ」）の項目は以下のとおりです。

1．〇〇情報	2．〇〇情報	3．〇〇情報	4．〇〇情報
5．〇〇情報	6．〇〇情報	7．〇〇情報	8．〇〇情報
9．〇〇情報	10．〇〇情報	11．〇〇情報	12．〇〇情報

（2）「開示等の求め」の申出先

開示等の求めは下記宛，所定の申請書に必要書類を添付の上，郵送によりお願い申し上げます。なお，封筒に朱書きで「開示等請求書類在中」とお書き添え頂ければ幸いです。

〒000-0000
東京都XX区XX　X丁目X番X号　XXXXXビル
株式会社XXXXX　個人情報保護対策室

（3）「開示等の求め」に際して提出すべき書面（様式）等

「開示等の求め」を行う場合は，次の申請書（A）をダウンロードし，所定の事項を全てご記入の上，本人確認のための書類（B）を同封し上記（2）宛ご郵送下さい。

A. 当社所定の申請書
・「保有個人データ」開示申請書
・「保有個人データ」変更等申請書
・「保有個人データ」利用停止等申請書

B. 本人確認のための書類

次のうちいずれかを同封して下さい。

・運転免許証（有効期限内のもので、各都道府県公安委員会発行のもの。国際運転免許証は除く。）の写し

・学生証の写し（有効期限内のもので、顔写真、生年月日、住所が記載されているもの。住所が記載されていない場合は、現住所が記載されている住民票、または現住所が記載されている公共料金領収証・請求書の写しも併せて添付して下さい。）

・日本国の旅券（パスポート）（有効期限内のもので、現住所が記入されているもの。）の写し

・健康保険証の写し＋現住所が記載されている住民票、または現住所が記載されている公共料金領収証もしくは請求書の写し

・障害者手帳または療育手帳または精神障害者保健福祉手帳の写し（現住所が記入されているもの。住所が記載されていない場合は、現住所が記載されている住民票、または現住所が記載されている公共料金領収証・請求書も併せて添付して下さい。）

・外国人登録証明書の写し＋旅券（パスポート）の写し、または公共料金領収証もしくは請求書の写し、または米軍IDカードの写し

（4）代理人による「開示等の求め」

「開示等の求め」をする者が本人又は未成年者又は成年被後見人の法定代理人もしくは開示等の求めをすることにつき本人が委任した代理人である場合は，前項の本人確認のための書類に加えて，下記の書類を同封して下さい。

A. 法定代理人の場合

・当社所定の申告書　1通

・法定代理権があることを確認するための書類（戸籍謄本，または親権者の場合は扶養家族が記入された保険証の写しも可）　1通

・未成年者又は成年被後見人の法定代理人本人であることを確認するための書類（法定代理人の運転免許証，または旅券（パスポート）の写し）　1通

B. 委任による代理人の場合

・当社所定の委任状　1通

・本人の印鑑証明書　1通

（5）「開示等の求め」の手数料及びその徴収方法

1回の申請ごとに，XXX円(税込)
XXX円分の郵便切手を申請書類に同封して下さい。
＊手数料が不足していた場合，および手数料が同封されていなかった場合は，その旨ご連絡申し上げますが，所定の期間内にお支払いがない場合は，開示の求めがなかったものとして対応させて頂きます。

（6）「開示等の求め」に対する回答方法

申請者の申請書記載住所宛に書面によってご回答申し上げます。

（7）開示等の求めに関して取得した個人情報の「利用目的」

開示等の求めにともない取得した個人情報は，開示等の求めに必要な範囲のみで取り扱うものとします。提出頂いた書類は，開示等の求めに対する回答が終了した後，2年間保存し，その後廃棄させて頂きます。

（8）個人データ」の不開示事由について

次に定める場合は，不開示とさせていただきます。不開示を決定した場合は，その旨，理由を付記して通知申し上げます。また，不開示の場合についても所定の手数料を頂きます。

・申請書に記載されている住所・本人確認のための書類に記載されている住所・当社の登録住所が一致しないときなど本人が確認できない場合
・代理人による申請に際して，代理権が確認できない場合
・所定の申請書類に不備があった場合
・開示の求めの対象が「保有個人データ」に該当しない場合
・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
・当社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
・他の法令に違反することとなる場合

ＥＣにおける個人情報保護に関する活動報告書

平成　１７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
東京都港区芝公園三丁目５番８号
機械振興会館　３階
TEL：０３（３４３６）７５００

この資料は再生紙を使用しています。

ISBN4-89078-630-9 c2036