ECにおける個人情報保護に関する活動報告書２００８

平成21年３月

次世代電子商取引推進協議会

ECにおける個人情報保護に関する活動報告書２００８

平成２１年　３月

次世代電子商取引推進協議会

はじめに

個人情報保護法が施行されてから 4 年が経過し、各事業者の体制作りはおおむね整ってきた。しかしながら、「身に覚えのない勧誘電話は減っていない」「独立系の中小企業などでは十分浸透していない」との声も相変わらず耳にする。また事業者から主務官庁に報告のあった漏えい事故発生状況については大規模事故に限れば改善傾向が認められるものの、件数だけ見れば減少カーブは鈍化傾向にある。

一方、企業活動のグローバル化に伴い、個人情報の越境移転が顕著（例：データ入力の海外アウトソーシングなど）になっているが現行保護法では越境移転に特化した記載はなく、我が国はＥＵから個人情報保護についてまだ「adequate」とはみなされていない状況にある。

かような状況下において次世代電子商取引推進協議会（以下ＥＣＯＭ）の個人情報保護WGでは平成 20 年度の活動として

・ 個人情報の越境ルールのあり方
・ 個人情報漏えい時の対応
・ 海外主要諸国の法制度状況

などについて取組んだ。

本報告書は上記に係る活動を中心に、従来から継続して実施してきた「ＥＣＯＭ会員企業、ＥＣ事業者の個人情報保護に関するＨＰ表記調査」結果を併せて取りまとめたものである。

本報告書の作成に当たっては個人情報保護WGにご参加の会員企業有志、内外の有識者の方々から多くのご意見をいただいた。この場を借りてあらためて御礼申し上げるとともに、さらに広く他方面の方々からご意見を賜ることができれば幸いである。

平成２１年３月

次世代電子商取引推進協議会

目　　次

1. 個人情報を巡る官民の動向

1.1　行政サイドの動向

「個人情報の保護に関する法律」（以下「保護法」と略）全面施行後 4 年目の初頭となる平成 20 年 4 月、政府は「個人情報の保護に関する基本方針」の一部を変更し公表した。この中ではいわゆる「過剰反応」に対し積極的な広報・啓発に取組むとしたほか、プライバシーポリシーに中味について委託処理の透明化や個人情取得源等の具体的な記述などさらなる消費者保護に向けた事業者への期待にも言及している。また国際的な取組みの重要性にも触れ我が国としての必要な対応を検討していくとした。

7 月には国民生活審議会の指摘を踏まえ、省庁ガイドラインの共通化についても着手し、分野・業界ごとの事情を踏まえつつガイドライン間の異同を小さくすべく動き出した。

9 月には内閣府が「平成 19 年度施行状況」を発表しているが施行後 3 ヵ年の主要指標を表 1-1 にまとめた。昨年度の苦情件数、（事業者から報告のあった）漏えい件数については微減にとどまっているが、大規模漏えい事故や意図的に行われた漏えい事案の件数は大幅に減少、また漏えい事案の中で暗号化等の情報保護が施されていた件数の比率も上昇し事業者の改善努力が明確に見て取れる。

表 1-1　施行後 3 ヵ年の主要指標

項目	17 年度	18 年度	19 年度
苦情相談件数	14,028	12,876	12,728
事業者が公表した漏えい事案件数	1,556	893	848
（うち漏えい人数 50001 人/件の件数）	37	36	17
（うち意図的に行われた事案の件数）	245	194	76
漏えい事案における情報保護実施率	データなし	23%	40%

国際化対応としてはＡＰＥＣ電子商取引サブグループの「ＡＰＥＣプライバシーフレームワーク」実証実験の活動を挙げておきたい。「プライバシーフレームワーク」とは 2004 年に採択されたＡＰＥＣ域内における電子商取引に関わるプライバシー保護のための枠組みであるが現在 9 つのプロジェクトによりＡＰＥＣ加盟 16 カ国の参加を得てプロジェク

トが進められている。(2.1 にて詳述)

1.2　個人情報漏えい事故状況

20 年度の個人情報漏えい事故または事件件数に関する公式の統計はまだないがＮＰＯ日本ネットワークセキュリティ協会が先頃公表した 2008 年上半期の情報漏えいインシデント報告書速報版によればインシデント件数は増加傾向にあるものの漏えい人数の総数は大幅に減少とある。これは大規模な情報漏えい事故の減少傾向が主な要因であるがインシデント総数の増加理由については同ＮＰＯの今後の分析結果を待つことにしたい。ヒントがあるとすれば漏えい原因で「誤操作」が急増していることが挙げられる。コンプライアンス意識の高まりとともに以前は軽くあしらわれていた些細な漏えい事故についても報告がなされるようになり件数は増加、対象漏えい人数は減少という結果になってきているのではないかと思料している。この傾向は前項の内閣府の「施行状況」結果と相通じるものがある。

2. 個人データの越境移転

2.1　ＡＰＥＣにおける越境個人データ保護活動について

ＡＰＥＣでは Electronic Commerce Steering Group(以下 ＥＣＳＧと略)においてかねてより国境を越えるデータ・プライバシー保護のための仕組み作りを検討してきたためＥＣＯＭ活動の前提として簡単に紹介しておきたい。

2.1.1　ＡＰＥＣ「プライバシーフレームワーク」の概要

ＥＣＳＧでは域内の電子商取引推進に個人データの保護が極めて重要との認識の下、基本的な枠組みを検討、その結果はＡＰＥＣ「プライバシーフレームワーク」として 2004 年 10 月に正式に閣僚会議にて採択された。本フレームワークは 1995 年にＥＵで採択された「個人データ保護に関するＥＵ指令」と対比されることが多いため表 2-1 の通り整理してみた。ＡＰＥＣフレームワークはＥＵ指令に比較し個人情報の保護よりも利活用を重視し、また域内エコノミーの個人情報保護に関する成熟度の相違を考慮しルール自体も若干緩やかなものになっていることが大きな特長といえよう。

表 2-1　EU 指令・APEC フレームワーク比較

	EU	APEC
名称	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 and on the free movement of such data	APEC Privacy Framework
制定年	1995	2004
参加国	27 カ国(世界人口の 8%)	21 カ国・地域（世界人口の 40%)

性格	地域法であり、加盟国は目的を達成する義務を負う。達成の方法、形式は各国に任せられる。	本フレームワークは情報プライバシーの保護とアジア太平洋地域の自由な情報の流れを促進するためのツールであり、商業的利益とのバランス、加盟国の文化、多様性も考慮する。
要点	第Ⅳ章　第三国への個人データの移転 第２５条　原　則 １．加盟国は、処理されている、又は後に処理される予定の個人データの第三国への移転は、当該第三国が適切なレベルの保護を提供している場合に限られることを規定するものとする。(以下省略) 第２６条　免　除 １．特別な事情に関する国内法に反対の主旨の規定がない限り、第２５条からの免除として、加盟国は、第２５条２の意味の枠内で、適切な保護レベルを確保していない第三国に対する個人データの一連の移転は、以下の条件に基づいて行うことができることを規定するものとする。 （ａ）データの対象者が提案された移転に対して、明確な同意を与えること。 （ｂ）その移転がデータの対象者と管理者との間の契約の履行、又はデータの対象者の要請よる契約	Part III. APEC 情報プライバシーの原則(9原則) I. 損害の防止 II. 告知 III. 収集の制限 IV. 個人情報の使用 V. 選択 VI. 個人情報の完全性 VII. セキュリティ対策 VIII. アクセスと訂正 (以上詳細は省略) IX. 責任 26. 個人情報コントローラは、上述の原則を実効あるものとするための措置に従う責任がある。国内か国外かを問わず、個人情報を他の人または組織に移転するときには、個人情報コントローラは該当の個人の同意を得るか、あるいは情報を受け取った人または組織がこれらの原則に則って情報を保護するように適切な注意を払い、妥当な範囲で必要な措置をとらなければならない。

	前の措置の実施のために必要であること。 （ｃ）移転がデータの対象者のために管理者と第三国との間で締結された契約の作成又は履行のために必要であること。 （ｄ）移転が重要な公衆の利益に基づくこと。もしくは、法的請求の提起、行使又は防御のために必要であること。 （ｅ）移転がデータの対象者の重要な権利を保護するために必要であること。 （ｆ）法律又は規則に従って、国民に情報を提供し、国民又は正当な権利を有する全ての者による参照のために開放することを意図している登録から移転が行われること。但し、個々の場合において、参照に関する法律に規定されている条件が満たされていることを条件とする。（以下省略）	
ルールの熟度	・ほとんどの加盟国で法制に組み込まれている。	・今後ﾊﾟｽﾌｧｲﾝﾀﾞｰ・ﾌﾟﾛｼﾞｪｸﾄの実行の中で検証がなされる予定。

比較 (相違点)	・越境移転に対する厳しい規制 ・第三者機関による監督 ・加盟各国により罰則規定に差がある。 ・米国との間ではｾｰﾌﾊｰﾊﾞｰ協定を締結 ・ＥＵ加盟国以外ではスイス、カナダ、アルゼンチンなどが適合性を認められている。	・ 電子商取引促進構想の一環 ・ プライバシーの保護と自由な情報流通の両立(不必要な制限はビジネスの障害) ・ ﾊﾟｽﾌｧｲﾝﾀﾞｰ･ﾌﾟﾛｼﾞｪｸﾄには 12 カ国が支持表明、日本もその中に含まれる。

2.1.2　パスファインダー・プロジェクトの実施

さらにＥＣＳＧではＡＰＥＣフレームワークに沿った個人データの越境ルールを検証するため「データ・プライバシー・パスファインダープロジェクト」の実施を決定し 2008 年 2 月に活動を開始した。パスファインダー・プロジェクトは表 2-2 の通り 9 プロジェクトで構成され、豪州、カナダ、チリ、香港、中国、日本、韓国、メキシコ、ニュージーランド、台湾、タイ、フィリピン、米国、ベトナムが参加している。(今後さらに参加国が増えることが見込まれる。)

表 2-2　パスファインダー・プロジェクト一覧

カテゴリー	プロジェクト名
自己審査	1. CBPR self-assessment guidance for organisations
適合性審査	2. **Guidelines for trustmarks participating in a CBPR system**
〃	3. **Compliance review of an organisation's CBPRs**
承認・通知	4. Directory of compliant organisations
紛争処理・執行	5. **Data Protection Authority and Privacy Contact Officer Directory**
〃	6. Template Enforcement Cooperation Arrangements
〃	7. Template cross-border complaint handling form
〃	8. Guidelines and procedures for responsive regulation in a CBPR system
プロジェクトの遂行	9. CBPR international implementation pilot project

（注１）太字部分は日本が正メンバーとして参加

（注２）下線部分は日本がオブザーバーとして参加

（注３）2009 年度よりパイロットプロジェクト始動予定

（注４）ＣＢＰＲ：Cross-Border Privacy Rule の略

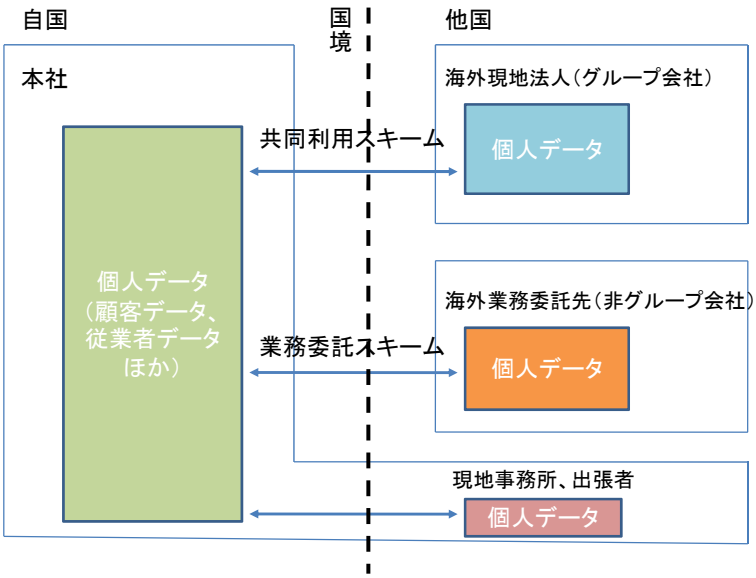
2.2　越境移転の分類と事業者が講じるべき措置

2.2.1　越境移転の分類

個人情報の越境移転ルール策定にあたり先ず移転先を「自社グループ会社（現地子会社）」か、「それ以外（現地アウトソーシング先）」か、に大別した。その理由は当該企業に対するガバナンス、つまり安全管理徹底の難易度に大きな差があることや継続取引の有無などが考えられるからである。

さらに現地子会社との間においてはグローバル・プライバシー・ポリシーの策定・運用を通して共同利用スキームを活用すること、現地アウトソーシング先との間では国内の委託先管理と同様の手法を適用することにより国内と同レベルの個人情報保護を図ることが妥当であると考えた。（いずれ場合も第三者に該当しないため必ずしも本人の同意は必要としない。）（図 2-2 個人データの越境移転イメージ参照）

図2-2　個人データの越境移転イメージ



ただ、いずれの場合も顧客情報を越境移転させる際は社外に対する透明性確保のために自社のプライバシー・ポリシーの中でその方針を明示することが望まれる。

蛇足になるが海外を含めた全社統一のプライバシー・ポリシー策定にあたっては下記に例示したような関係各国の国情の相違を熟慮しなくてはならない。

・いわゆる機微情報の取扱い

・個人情報取得元の開示義務

・年少者のプライバシー 保護義務

・暗号化対策の評価

・第三国への移転許容度

・監督機関への利用個人データ（ファイル）の事前登録要否

・法の対象となる個人情報 の範囲（定義）

・小規模事業者の例外規定有無

・罰則規定

・従業者の監視可否

2.2.2　事業者が講じるべき措置

上記の検討をもとに越境移転に際し事業者が講じるべき措置を下記の通り整理した。

・越境移転に関する方針の通知・公表

・【移転先がグループ会社（現地法人）の場合】

グローバル・プライバシー・ポリシーの策定・徹底と共同利用を行う旨の公表

・【移転先が現地資本の場合】

移転先に対する必要かつ適切な監督の実施

監督の内容については「経済産業省ガイドライン 2-2-3-4　委託先の監督」と同等のものとする。

・　個人情報保護に関する移転先との連携

個人データの正確性保持　開示対応など

・移転プロセスにおける安全管理の徹底

暗号化措置、取扱い担当者の限定、アクセスログの取得など

・従業者からの越境移転に対する同意の取得

さらに上記をもとにＥＣＯＭガイドライン第 40 条の改訂案を別紙 1 の通り検討した。

別紙１

第５章　個人データの越境移転

第 40 条（個人データの越境移転）

事業者は、自己が取り扱う個人データ（顧客データ、従業者データ、その他の個人データを問わない）を国外に移転させる際は当該本人の同意をとる、もしくは移転先がわが国と同等以上の水準で情報を保護するよう十分な注意を払い妥当な範囲内で必要な措置をとるものとする。

（解説）

1.　事業活動のグローバル化、海外アウトソーシングの活用等に伴い、自己が保有する個人データを海外に移転させるケースが増加しているがその際事業者は対象国の実情を踏まえた上で移転先の適切な個人データ管理を確認し、その保護に万全を尽くさなくてはならない。

2. ＥＵデータ保護指令、ＡＰＥＣプライバシーフレームワーク等において個人データの越境移転に関する規制、記述があるがいずれも本人の同意を条件に移転を許容しているため個人データの越境移転に際しては事前に同意を得ておくことが肝要である（特に従業者について）。

3. 個人データの越境移転については顧客の個人データなど本人からの事前同意を得ることが困難な場合も考えられるため移転先の情報保護体制を厳正に審査し移転の適否を適格に判断しなければならない。更に移転を決定した場合には当事者間において秘密保持契約の締結を行い、また移転後も定期的に監査を行い漏えい等の防止に努めるものとする。

4.　海外子会社による事業運営に際してはグループ共通のプライバシーポリシー（グローバルプライバシーポリシー）を整備するなどグループ一丸となった取組みを徹底し全世界レベルでの管理体制を構築することに加え、関係各社間で共同利用を行う場合は各社のホームページ等でその旨の表示を行うことが望ましい。グローバルプライバシーポリシーの策定にあたっては各国の個人情報保護法制度を勘案するとともにその変化・動向にも注意が必要である。また、各国にて運営されている個人情報保護に関する第三者認証制度があればその取得にも積極的に取り組んでいくことが望まれる。

5.　電子的な通信手段を用いて個人情報を送信する場合は暗号化措置の徹底、受信従事

者・受信方法の制限、アクセスログの取得などにより移転プロセスにおける情報漏えい事故防止に努める必要がある。

6. 越境移転について必ずしも明確な定義はないが、インターネットの機能や情報財の性格を考慮すると「国外に所在する組織（または人）に向けた個人情報の送信」のみならず「国外からのアクセスにより閲覧できる状態」も含むものと考えられるので注意が必要である。

3. 漏えい時の本人通知について

3.1　米国における動向

「Breach Notification Laws」とは保有している個人情報を漏えいなど危殆化させた事業者向けに当該本人宛てその事実を通知することを義務付ける法律の総称であり 2003 年以降米国の各州で急速に法制化が進んだ。今日では約 45 もの州で何らかの規定があり、直近 1 年間の延べ報告件数は 656 件、通知を受けた対象者は 35 百万人（過去 4 年間累計では 250 百万人）に上る。

前述のように「Breach Notification Laws」は個人情報の危殆時に当該本人にその旨の通知を義務付ける州法の総称であるがその細目は各州によって異なっている。以下簡単にその相違点に触れながら全体の概要を紹介してみたい。

①本人通知が義務付けられる「個人情報」とは

「Breach Notification Laws」の嚆矢となったカリフォルニア州では施行当初（2003 年 7 月）は

・社会保険番号（ＳＳＮ）

・運転免許証番号

・カルフォルニア州ＩＤ番号

・金融口座番号、クレジットカード番号、デビットカード番号でアクセスコード、パスワード等が付随している場合

と定めていたが 2008 年 1 月に

・個人の病歴や診断記録等の医療情報

・健康保険事業者によって用いられる健康保険情報

が新たに追加された。

この例に見られるように「Breach Notification Laws」では本人の社会的な ID、個人用の決済に使われる番号（＋パスワード）から健康医療情報まで広がりを見せつつあるが、さらに生年月日、デジタル署名データ、遺伝子情報や部族ＩＤ番号などをその対象に加えている州もある。

②媒体の種別

多くの州では電子化された情報のみを「Breach Notification Laws」の対象としている

がノースカロライナ州、ウィスコンシン州などでは紙媒体での流出も本人通知が義務付けられている。

③本人以外への通知義務

多くの州では本人通知の際に州政府への通知を義務付けている。またニュージャージー州では本人への通知に先立ち州警察への通知を義務付けている。さらに３大消費者信用情報機関への通知を義務付けている州も数多い。

④通知期限

多くの州で本人に対し「できるだけ迅速に、遅滞なく通知すること」を求めており、中にはオハイオ州、フロリダ州のように漏えいが判明した日から 45 日以内と規定している州もある。本人通知が捜査当局の捜査の妨げになる恐れがある場合にはその間の期限延長が認められる。本人通知以前にシステムのセキュリティを確保しておくことが不可欠なためシステム回復を理由に一定期間通知を遅らせることが許容されることもある。

⑤本人通知の要否に関する判断基準

アーカンソー州、ルイジアナ州などでは当該本人が被害を受ける合理的な可能性がない場合本人通知の必要はないとされている。またアイダホ州、メイン州では個人情報の悪用が判明しない限り、またはその疑いがない限り本人通知の必要はないとされている。

⑥暗号化特例

どの州の規定でも「暗号化されていること」は免責事由となっており、暗号化の意義は高く評価されている。法の下で特定の暗号化技術を指示されることはないが、一般にパスワードによるアクセス制限はデータの暗号化とはみなされていないため、仮にＢＩＯＳなどによりロックされていたとしても暗号化が施されていなければ当該ＰＣ類の紛失、盗難は本人通知が必要となる。

3.2　カナダにおける動向

カナダ国のプライバシー監督機関である Office of the Privacy Commissioner of Canada では個人情報漏えい時に民間部門が対応すべき項目を Key Steps For Organizations In Responding To Privacy Breach として取り纏め、これを公開している。本文書は個人情報漏えい時に民間部門が採るべき措置を 4 つのステップに分け解説しているが、我が国の事業者にとっても大いに参考になるものと思われるので原文（内容は短文が多いので初心者でも理解しやすい。）を次ページ以降に掲載する。なお、法制化についても今後取り組んでいくとしている。

英文資料６ページ挿入

（Key Steps for ・・・・・）

3.3　ECOM での検討内容

ＥＣＯＭでは昨年に引き続き本テーマについて検討を行ってきたが、最大の論点は「事業者はどのような個人情報を漏えいした場合に本人通知すべきか」であった。いうまでもなく個人情報の中味は多岐に亘り機微度、重要度の客観的判定は難しい。議論を重ねた結果ここではひとまず表 3-1 の通り整理し、別紙２の通りＥＣＯＭガイドライン案を策定したがまだまだ議論の余地があるかもしれない。読者の方々の建設的なご意見を待ちたい。

表 3-1 事業者が漏えい時に本人に対し通知すべき個人データ

分類	内容
決済関連データ	①クレジットカード会員番号および本人認証データ ②取引銀行口座番号および本人認証データ
身体・健康関連データ	①病歴、加療記録 ②生体認証データ ③遺伝子データ
事業者が個別に判断し独自に通知対象として取り扱うデータ	①顧客の購入・利用履歴であって商品・サービスの性質上、特にプライバシー度が高いと判断したもの（例：メール、通話などの通信サービス） ②自社が取得・保有している個人情報で当該本人にとってプライバシー度が高いと判断したもの（例：年収・資産状況など）

（注）下記の２項目については元来民間事業者が取得もしくは利用しないものとして対象から除外している。

①いわゆる「Sensitive Data」（政治、宗教、人種など社会的差別につながる恐れのあるもの）

②公的ＩＤ番号（例：住民基本台帳番号、基礎年金番号、健康保険証番号、運転免許証）

別紙２

第４章 漏えい等が発生した場合の措置

第 39 条（漏えい等が発生した場合の措置）

1　事業者は、自己が取り扱う重要な個人データについて漏えい等（滅失、き損を含む。以下同じ。）の事実を把握した場合は当該漏えい等に関する事実関係および二次被害の拡大防止策を本人に速やかに通知するものとする（ただし対象となる個人データが高度な暗号化等の秘匿化が施されている場合、紛失した個人データを第三者に見られることなく、速やかに回収した場合を除く）。

2　事業者は、自己が取り扱う重要な個人データについて漏えい等の事実を把握した場合は二次被害の拡大防止、類似事案の発生回避の観点から、可能な限り事実関係及び発生原因を遅滞なく公表するものとする（ただし対象となる個人データが高度な暗号化等の秘匿化が施されている場合、本人全てに連絡がついた場合を除く）。

3　事業者は、自己が取り扱う重要な個人データについて漏えい等の事実を把握した場合は発生原因及び対応策を所管する省庁に直ちに報告するものとする。認定個人情報保護団体の対象事業者は上記の報告に代えて自己が所属する認定個人情報保護団体に報告することが可能であるが、クレジットカード情報など重要な個人データが漏えいした場合は主務大臣に速やかに報告するものとする。

（解説）

1.　事業者は、自己の取り扱う重要な個人データの漏えい等の事実を把握した場合は、当該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するものとする。

この場合の重要な個人データとは漏えい等があった際に当該本人に与える影響が大きいと思われる情報を指し具体的には

①クレジットカード会員番号などの決済関連情報

②病歴・加療記録、生体認証データなどの身体・健康関連情報

③事業者が個別に判断し本人通知対象として取り扱う情報（プライバシー度が高い商品・サービスに関わる購入履歴、独自に取得・保有している顧客情報でプライバシー度が高いと判断したものなど）が該当する。また、何らかの事由により住民基本台帳番号、基礎年

金番号等公的ＩＤ番号を保有しこれを漏えいした場合もこれに該当する。

2.　事業者は、自己の取り扱う重要な個人データ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るものとする。

3.　事業者は、自己の取り扱う重要な個人データ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.　漏えいした個人データが適切な暗号化等により秘匿化されている場合は本人通知および公表が省略できる場合があるので事前に十分な対策を講じておくことが望まれる。

4. 電子メール広告と個人データの利用

4.1　特定商取引法の改正について

経済産業省は 2008 年 6 月に成立した「改正特定商取引法」にてネット通販事業者等が取り扱う電子メール広告に関し従来のオプトアウト規制からオプトイン規制に変更した。これにより、ネット販売事業者は電子メール広告を送信する前にあらかじめ消費者の承諾(または請求）を得ることが義務付けられた。以下そのポイントを列記する。

① 規制の対象

事業者が取引の対象として商品・サービスを電子メールにて行う広告

② 規制の対象者

消費者と直接契約を締結する販売事業者・役務提供事業者および電子メール広告受託事業者

③規制の内容

・消費者からあらかじめ請求や承諾を得ていない電子メール広告の送信原則禁止

・電子メール広告の送信を拒否する方法の表示義務と電子メール広告の送信を拒否した消費者への送信禁止

・消費者からの請求や承諾の記録保存（最後に電子メール広告を送信した日から 3 年間の保存が必要。）

・罰則強化

違反行為について行政処分の対象とするとともに刑事罰規定を新設。

違反行為の内容により 1000 万円以下の罰金、もしくは 1 年以下の懲役または 200 万円以下の罰金、あるいはその両方の罰則が科せられる。

④施行日

2008 年 12 月 1 日

4.2　オプトイン原則の導入に伴うＥＣＯＭガイドライン改訂案

上記の改正を踏まえ、ＥＣＯＭガイドライン　第 16 条　の改定案を別紙３の通り策定した。

別紙３

第 16 条　（電子メール広告の送信における個人データの利用）

事業者が個人データを用いて商業目的の電子メール（以下「電子メール広告」という。）を送信する場合は、あらかじめ相手方から送信についての承諾を得るとともに承諾を得たことの記録を保存しなければならない。また、事業者は相手先が電子メール広告の提供を受けない旨の意思を表示するための方法を当該電子メール広告の本文中に明示しなくてはならない。

（解説）

１．　２００８年６月に成立した「特定商取引に関する法律および割賦販売法の一部を改正する法律」（平成20年法律第７４号）により、ネット通販事業者（ネットショップ）等や電子メール広告受託事業者に関係する重要な規制内容が盛り込まれた。特に「電子メール広告」部分では、いわゆる「迷惑広告メール」の防止を目的に従来の「オプトアウト規制」が「オプトイン規制」に変更された。本条はこれを受け、電子メール広告における個人データの利用につき規定を整備したものである。

２．　事業者が個人データを用いてインターネット回線やいわゆる携帯電話のショートメールサービスを利用して自社の商品・サービスの販売や顧客勧誘を目的とした電子メール広告を送信する場合は事前に相手方から送信についての承諾を得なければならない（契約の申込みの受理、契約の成立、契約の履行に関する重要事項の通知に付随した電子メール広告や広告掲載を条件に消費者に無料で利用できるメールサービスによるもの等を除く）。また、その際に当該個人データをどのようにして取得したかについて明示することが望ましい。わが国の個人情報保護法（略称）では事業者に必ずしも個人情報の取得元まで開示する義務はないものと解されているが、平成 20 年 4 月「個人情報の保護に関する基本方針の一部変更」において「取得元、取得源等をできる限り具体化」することが重要との記載がある。

３．電子メール広告の送信については送信者の商号、代表者名や受信拒否のための連絡先となる電子メールアドレス、ＵＲＬ等を当該電子メールの本文に容易に認識できるように表示し、問合わせ等があった場合には誠実に対応するものとする。あらかじめ送信について承諾を得ていた受信者から新たに電子メール広告の受信拒否の通知を受けた場合はそれ以降の送信を速やかに停止するものとする。

４．　事業者は電子メール広告の送信に際し、受信者からあらかじめ請求または承諾を得たことの記録として当該電子データ、書面等を電子メール広告を行った日から３年間保存しなければならない。

5. 主要各国の法制化動向について

5.1　主要各国の法制化状況

ＥＣＯＭでは今年度の海外動向調査の一環として主要各国の法制化状況を整理し一覧表として取り纏めたのでその要点を紹介したい。

①民間部門を対象とした個人情報保護に関する包括法の有無

法整備状況をチェックするための第一のポイントは民間部門を対象にした包括法の有無である（行政部門については民間部門とは別に先行して法制化している国が多いので注意が必要)。現在、ＥＵ加盟国（最近加盟した諸国については一部例外有り)、スイス（ＥＵ未加盟)、カナダ、豪州、ニュージーランド、アルゼンチンおよび日本などが包括法を有しており個人情報保護先進グループと位置づけられる。米国については業界ごとの法制度は多いもののいわゆる包括法はないとされていることを付記しておきたい。各国の包括法の中味についてはいずれもＯＥＣＤ勧告を参照しているため概ね近い内容になっているが保護の対象となる個人情報の範囲や懲罰規定、越境移転に関する記載等細部についてはそれぞれ相違点も見られる。

なお現在包括法を持っていない国においても一般に法制化の対する関心が高いため近い将来大幅に整備国が増えるものと見込まれる（韓国など)。

②個人情報保護関連法規の存在

包括法の未整備国においても特定分野ごとに個人情報保護に関する規定が存在することがあるので個別に注意しなければならない(前述の先進グループについても同様であるが)。たとえば消費者保護の観点から事業者に対し一定の義務を規定するもの、ＩＴ・電子商取引等の健全な発展を促すために個人情報を含む電子ファイルの取扱い等を規定するもの、機微な情報を多く保有する金融業、通信業、医療機関など業界ごとに具体的な基準が設けられているものなどが挙げられる。我が国においても先般特定電子メール法、特定商取引法の改正により商業メールの発信に厳しい制約が加えられることになったがこれもその一例である。

③ＥＵ適合性の判定

ＥＵでは 1995 年に採択した「個人データ処理に係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」において個人データの第三国への移動は、当該第三国が適切なレベルの保護を提供している場合に限られることを加盟国に対し義務付

けている。ＥＵ適合性の承認について適格な包括法の制定と運用、個人情報保護に特化した行政監督機関の設置などが条件となっており個人情報保護を国家レベルで遵守していることを証明するグローバル・スタンダードとなっている。

5.2　海外各国との相違点

前述したように包括法の中味については細部において相違点もあるので関係国ごとに確認することが必要になる。

具体的な相違点として 2.2.1 でも触れたように下記の項目が考えられるので再掲しておきたい。

・いわゆる機微情報の取扱い
・個人情報取得元の開示義務
・従業者の監視可否
・未成年者のプライバシー保護
・暗号化対策の評価
・第三国への移転許容度
・利用個人データ（ファイル）の事前登録要否
・保護法の対象となる個人情報の定義
・小規模事業者の例外規定有無
・罰則規定

さらに主要各国の法整備状況の概観を目的に次ページの通り一覧表を作成した。

本一覧表の縦軸は包括法の有無、専門監督機関の有無、包括法の特徴、関連法規の有無、ＥＵ適合性承認状況とし、横軸に関係各国、1 ページ目は包括法規定国、2 ページ目以降に非規定国を集約した。今回の作業においては先進国のみならずアジア新興国等も対象に加えているがこの点については引き続き留意し対象国を拡大していくことを予定している。

また各国別の詳細情報として国別の個票も添付しているがこの点についても更に充実していきたい。

法制度比較２００９年版
(Ａ３版　３ページ)　　折込挿入

民間部門の個人情報保護に関する
各国の法制度と動向

１　ＥＵ
２　英国
３　スペイン
４　米国
５　カナダ
６　ブラジル
７　ロシア
８　インド
９　中国
１０　豪州
１１　アルゼンチン
１２　韓国
１３　ニュージーランド
１４　メキシコ
１５　フィリピン
１６　シンガポール
１７　中華民国（台湾）
１８　タイ
１９　ベトナム
２０　日本

国･地域名	ＥＵ（欧州連合）
個人情報保護に関する包括法等	個人データ処理に係る個人の保護および当該データの自由な移動に関する欧州議会および理事会の指令（ＥＵデータ保護指令）【1995 採択、1998 発効】
その特徴	① 個人データの処理に係る個人のプライバシー保護と加盟国間の個人情報保護法調和による域内での自由な移動の確保が目的（十分な個人情報保護基準を満たさない第三国への個人データ移転禁止） ② 個人情報保護に関する行政による独立した監督機関（supervisory authority）の設置 ③ 監督機関への通知義務（通知すべき内容の詳細は各々の監督機関にゆだねられている。） ④ センシティブ・データの取扱い原則禁止 データ主体が明示の同意を与えた場合等の例外規定はあるが、国の法律がデータ主体の同意を得ても禁止を解除しえないと規定している場合はこの限りではない。 ⑤ データ対象者に対し当該データに対する広範な権限を付与
監督機関等	有り(名称、活動範囲等は各国によって相違がある。)
個別法･関連法	電気通信分野における個人情報処理およびプライバシー保護に関する欧州議会・理事会指令【1997、2002 採択】
特記事項･動向	① ＥＣ加盟国以外でかつ十分な保護基準がある国としてアルゼンチン、カナダ、ガーンジー、マン島、スイスを承認している。 ② 法制度を含む情報ネットワークのセキュリティ問題に対処するために European Network and Information Security Agency (ENISA)を設立し、技術標準の開発、リスク・アセスメントの推進などで各国政府・民間

	部門を支援している。(2004/3)
備考	

国･地域名	英国
個人情報保護に関する包括法等	データ保護法（Data Protection Act）【1998 成立、2000 施行】 （1984 年データ保護法の改正）
その特徴	① 行政部門、民間部門の両方に適用（＝オムニバス式） ② ＥＵデータ保護指令と整合 ③ 保護対象は現存する個人に関して自動処理される既存データ全て ④ 情報コミッショナーへの届出（公開データベース登録）を義務付け 登録者は登録内容と異なる種類のデータの保有禁止、登録された目的以外のデータの保有・利用の禁止、登録と異なる情報源からのデータの入手禁止、登録と異なる提供先へのデータの提供禁止等の義務を負う。 ⑤ 罰則 規定違反は罰金刑、登録義務違反は裁判所命令によるデータ資料没収、破棄 ⑥ 損害賠償請求権 情報主体は個人データの紛失、破壊、開示・アクセスにより損害を被った場合損害賠償請求権を有する。 ⑦ 個人データの国外提供制限 ⑧ 「データ保護審判所」への不服申し立て
監督機関等	情報コミッショナー・オフィス （The Office of Information Commissioner）
個別法･関連法	① 消費者信用法（Consumer Credit Act 1974） 消費者信用に関わる個人データの開示取扱い(マニュアル処理含む)等を規定。 ② プライバシーと電子通信に関する規則（2003 施行）
特記事項･動向	① センシティブ・データの取り扱いについて詳細な規定がある。 ② 2007/11 財務省・歳入関税庁で児童手当受給者２５００万人分の個

	人情報を含むデータの紛失事故発覚。紛失データには子どもの名前、生年月日、保護者の住所、国籍、国民保険番号、銀行口座などが含まれる。本事故により関税庁長官が引責辞任。
備考	①データ保護法(1984)は消費者信用法(1974)と補完関係にある。

国･地域名	スペイン
個人情報保護に関する包括法等	Organic Law 15/1999 of 13th December on Personal Data Protection (1992 制定 1999　改正)
その特徴	①　行政･民間両者に適用 ②　「データ・ファイル」を対象 ③違反内容により罰金、時効が異なる 監督機関の指令不服従　等･･･罰金 10 万セペタ以上、時効 1 年 同意が必要な場合に同意なく個人情報を取得　等･･･罰金 1000 万セペタ以上、時効 2 年 詐欺的なデータの収集　等･･･罰金 5000 万セペタ以上、時効 3 年 （注）罰金額は法制定当時のものを引用した。
監督機関等	la Agencia de Proteccion de datos(データ保護局) el Registro General　de Proteccion de datos(データ保護一般登録所)
個別法･関連法	
特記事項･動向	①　2008.1　データ保護法改正を発表（規制対象に non-automated file を加える、１４歳以下の子どもに関する情報処理は親の同意を要する、委託元・委託先間の関係と　　安全対策等を盛り込む） ②２００７年の苦情に伴う調査件数　１２６３件 ③２００７年の民間部門起訴件数　３９９件
備考	

国･地域名	米国
個人情報保護に関する包括法等	民間部門を対象にした包括的な保護法はない。(＝セグメント式) （1974 年に制定されたプライバシー法は政府機関が対象）
その特徴	
監督機関等	①専門機関ではないが連邦取引委員会（ＦＴＣ）が対消費者問題の一環として積極的に対応 ②Safe Harbor Agreement に関しては商務省が担当
個別法･関連法	① 公正信用報告法（Fair Credit Reporting Act）（1970 制定、1999 改正） 個人信用情報に関し情報主体の権利を明確にし、正確性を確保 ② ケーブル通信政策法（1984 制定） ③ 電子通信プライバシー法（1984 制定） ④ ビデオプライバシー法（1988 制定） ⑤ 金融プライバシー法（1999 制定） ⑥ 児童オンラインプライバシー保護法（Children's Online Privacy Protection Act 1998 制定、2000 施行） 13 歳未満の児童からの個人情報収集は保護者の同意が必要。
特記事項･動向	①「ＥＵ指令」への対応 Safe Harbor 原則（2000 締結）により同原則に同意した企業名を商務省がＥＵ側に提示。 ③ California Data Breach Notification Law(2003) 非暗号化データ漏えい時の当該情報主体（本人）に対する告知義務。単なるＰＣ，ＰＤＡ等の盗難によるものも対象となる。現在全米４５州に波及、 2008 年の報告件数は 656 件､通知を受けた人数は 3500 万人に上る。なお、カリフォルニア州は 2008/1 ＳＳＮ，クレジットカード情報などのほか新たに医療情報、保険情報も通知すべき対象に加えた。

	③Do-not-call Registry の運用（2003） 2003 年 6 月より受信拒否リスト登録受付開始、登録者数は 2008 年現在 1.7 億人超、登録者は 5 年ごとに更新する。業者は 3 ヶ月ごとにリストをチェックすることが義務付けられ、違反業者は最高 11000 ドルの罰金が科せられる（ただし、消費者が 18 ヶ月以内に商品、サービスを購入または 3 ヶ月以内に何らかの問合せを行った場合は電話可。慈善事業、世論調査、政治活動は適用免除。）Do-not-Email Registry、Do-not-Track Registry の導入について検討中。 ④ＲＦＩＤの普及 ＲＦＩＤタグの利用に際し、個人の追跡用途制限などに向け法制化が検討されている。
備考	①　多様な州法への個別対応 ・ＩＳＰの個人情報の二次使用に対しユーザの事前承認義務付け（Minnesota） ・　個人情報を含む文書、記録媒体の廃棄禁止(Georgia)

国･地域名	カナダ
個人情報保護に関する包括法等	個人情報保護および電子文書法（Personal Information Protection and Electronic Document Act ）【2001 制定】
その特徴	①民間部門において商業活動で収集、利用、売買されるすべての個人情報に適用される ① 適用除外 名刺記載情報（勤務先、役職、住所、電話番号、メルアド等）については法律の適用除外
監督機関等	連邦･州政府にプライバシー・コミッショナー・オフィス（Office of the Privacy Commissioner of Canada etc.）を設置（プライバシー権に関する監督・擁護・仲裁）
個別法･関連法	① プライバシー法(1983) 連邦政府機関による個人情報の取扱いルールを規定。 ② 情報アクセス法(1985) 公的に保有されている情報へのアクセスについて規定。 ③ 銀行法 ④ オンタリオ州健康保険法
特記事項･動向	①プライバシー・コミッショナーが独自に「privacy breach guideline」を公表するとともに同時に連邦政府に対して Breach Notification を義務付ける PIPEDA 改正を要請（2007 年 8 月〕。 ②プライバシー・コミッショナーが小売業界に対し本人確認手段として運転免許証番号を取得することは不適切と警告、消費者に対しても事業者から満足な回答が得られなければコミッショナー・オフィスにコンタクトするよう呼びかけを行った（2008 年 12 月）。
備考	ＥＵ適合性を取得している。

国･地域名	ブラジル連邦共和国
個人情報保護に関する包括法等	個人情報保護に特化した包括法はないが、消費者保護法（1990）で相当広範な消費者の権利を認めている。
その特徴	
監督機関等	専門機関は公的にも、私的にもない。
個別法･関連法	① 消費者保護法（Consumer Protection Law 1990） 消費者は個人情報の出所等に関するアクセス権、修正請求権(保管人は 5 日以内に修正を通知しなければならない)を保有する。 ②電気通信法（Telecommunication Act1997） 電気通信サービス利用者は自身の個人データの利用に関しプライバシーが 尊重される権利を有する。 ③金融機関守秘法(Financial Institutions Secrecy Law) 金融機関は能動および受動の業務・サービスについて秘密を保持する。
特記事項･動向	①個人情報保護促進法（1996 国会提出・保留中） いかなる個人情報も所有者の明確な許可なく開示、通信、送信してはならない（犯罪捜査目的等の場合を除く）。また種族的出身、政治的･宗教的信念等の収集、保管、送信を禁止する。 ②電話勧誘販売規正法（仮称、2002 国会提出･審議中） 米国「Do-not-call Registry」のブラジル版。 ③連邦刑法（2000 改正） 情報システムへの不正データ挿入、不正改変に対する刑事罰ルール明確

	化④被雇用者の監視行為制限 ブラジル第9地方労働裁判所が被雇用者のコンピュータ通信監視は不法との判決。監視行為を許容する雇用主との労働契約は違法とみなす。 ⑤監視カメラの設置条件 サンパウロ市が監視カメラの存在を知らせる標識の設置を市条例で義務付けている（公共、民間エリア問わず)。記録された映像は法の下で保護される。
備考	① ブラジル憲法(1988)にプライバシーの権利として住居の不可侵、通信の秘密のほかに私事、私生活、名誉および個人の肖像の不可侵を規定(5条)

国･地域名	ロシア連邦
個人情報保護に関する包括法等	情報･情報化･情報の保護に関する連邦法（Federal Law on Information, Informatization and the Protection of Information ,LIIPI）
その特徴	①この法律で自然個人の私的生活に関する情報を当該人の同意なく収集、保存、使用、配布を禁じている。（具体性に欠けるため個人情報保護包括法と位置づけることが適当ではないかもしれない）
監督機関等	政府レベルの監督機関はない。 （いくつかの地域オンブズマンが取り組んでいる例はある。）
個別法･関連法	① 通信法（Federal Law on Communication 1995, 2004 改正） 通信利用者に関するデータの守秘性を保護。電話会話の傍受・電子通信の監視等は裁判所からの命令によってのみ許可される。 ②刑法（Criminal Code） コンピュータ情報への不正アクセスに対し法的責任明確化。
特記事項･動向	①「電子ロシア（Electronic Russia）」計画（2002 採択） 2010 年を目標年次とする本プログラムの中でプライバシー保護についても規定があり、基盤構築とあわせ提案している。今後の動向に注意。 ②個人情報売買事例（2003） 大手携帯電話会社ＭＴＳ（Mobile Telesystems）の全顧客データ数百万人分がＣＤとして販売された。個人データの不正収集･販売は日常的。
備考	① 欧州協議会「個人データの自動処理に係る個人の保護に関する条約」に署名。 ②低い個人情報保護意識

	プライバシー保護の概念はまだ一般的ではなく、プライバシーポリシーを掲げるＷｅｂサイトは少ない。

国･地域名	インド
個人情報保護に関する包括法等	現時点ではまだないが、通信･情報技術省で検討中（英国データ保護法をモデル？）
その特徴	
監督機関等	
個別法･関連法	①情報技術法（Information Technology Act 2000） ･電子商取引に関する包括的規制環境を提供するものでコンピュータ犯罪、 ハッキング、守秘性侵害等に対処し、サイバー犯罪の裁定を行うサイバー上訴裁判所（Cyber Appellate Tribunal）の設置を定めている。 ・ 法執行機関に対し広範な裁量権を与えている。（いかなる情報の傍受も許可し、ユーザーは暗号鍵を開示しなければ 7 年以下の拘禁刑に処せられる） ① 公共金融機関法（Public Financial Institutions Act 1993） 銀行取引における守秘性維持を成文化。
特記事項･動向	①サイバー犯罪初の有罪事例（2003） 他人のクレジットカード番号を詐取し、不正使用した容疑者に対しオンライン詐欺罪を適用。 ②電話盗聴に関する判決 最高裁が電話盗聴は「個人のプライバシーの重大な侵害」との判決を下す。また政府による電話盗聴のためのガイドラインを規定。背景にテロ防止がある。
備考	① 海外企業のアウトソーシング基地化が進む中でプライバシー保護に対する認識が法整備を含め高まりつつある。

国･地域名	中国
個人情報保護に関する包括法等	現時点では民間企業に個人情報保護を義務付ける包括法はないが 国務院の中で検討が進んでいる。
その特徴	
監督機関等	
個別法･関連法	① 銀行経営に関する暫定条例【1986 制定】 顧客預金に関するすべての情報は開示してはならない。 ② コンピュータ情報ネットワークとインターネットのセキュリティ、保護、運営規則【1991】 ネットワークユーザーのプライバシーは法律によって保護される。 ③ 未成年者の保護に関する法律（Law on the Protection of Minors 1991） いかなる組織・個人も未成年者の個人の秘密を暴露できない。 ④ 刑法２８５条～２８７条 コンピュータシステムへの無許可侵入は不法。 ⑤ 国民ＩＤカード法（Law of Citizen Identification Cards 2004） 16歳以上の国民はＩＤカードの携行を義務付けられる。住民登録偽造、なりすまし等は罰金刑。
特記事項･動向	① 従業者のプライバシー保護意識 一般に企業が従業員を採用する際の雇用契約の中に機密保持条項があり、契約違反は処罰される。 ②先進企業の自発的取組み 海外との接点が多い企業については独自に内規を策定しコンプライアンス意識を向上させている企業もある。

	③激増するインターネット人口と利用環境 政府の監視にもかかわらずインターネット人口は急増しているがネットカフェ(無許可が 60%を占める)での利用も多い。
備考	① ＡＰＥＣのＥＣＳＧ（Electronic Commerce Steering Group）共同副議長としてプライバシーフレームワーク策定に積極参加。 ② 中国のインターネット規制と法律は「慎重な開放」という原則に従っている。政府のインターネット監視は多数の逮捕者を生んでいる。

国･地域名	豪州
個人情報保護に関する包括法等	Privacy Amendment （Privacy Sector) Act2000 （2001 年 12 月施行）
その特徴	① 国家プライバシー原則（NPP s : National Privacy Principles）を基礎にしている。（EU データ保護指令よりややレベルが低い） ② 従業員情報、報道機関、中小企業（年間取引高が 3 百万豪ドル未満）で適用除外措置有り。 ③ EU と同様に個人情報の海外移転を制限（例外を除き）
監督機関等	Privacy Commissioner (調査官数の制約により監査より苦情対応が中心となっている。)
個別法･関連法	① Telecommunications Act 1997 ②Spam Act2003(２００４発効) 電子媒体による未承諾広告メッセージを禁止するもので罰金刑の最高は１１０万豪ドル。 ③州法 Workplace Video Surveillance Act 1998(NSW)
特記事項･動向	① ＡＬＲＣ（法制度改革委）が抜本的な法改正を提言しており成り行きが注目される。 ② プライバシー侵害の恐れがある RFID について警告実績があるが法律制定の動きはない。 ③2008/1 プライバシー・コミッショナーが個人データを保有する政府機関、企業に対し個人データのリスク・アセスメントと暗号化要否チェックを督促。 ④ＡＰＥＣ Data Privacy Sub Group 議長国として Pathfinder Project をリード

備考	

国･地域名	アルゼンチン共和国
個人情報保護に関する包括法等	Law for the　Protection of Personal Date (LPPD) (2000/11 成立) Regulation of the Privacy Law(2001/11 制定)
その特徴	①　EU データ指令とスペイン「Data Protection Act」がベース。 ②　適切なデータ保護を行わない国への個人情報移転禁止
監督機関等	National Directorate for the Protection of Personal Data(個人データ保護局)(２００３年６月最初の行政処分実施)
個別法･関連法	①クレジットカード、銀行、医療分野の法律に個人情報保護条項が含まれる。
特記事項･動向	①　EU から adequate と認定されている(中南米地域では初めて)。
備考	

国･地域名	韓国
包括法 （発効時期）	現時点ではまだないが国務会議で準備中。（2009 年下期施行見込み）
その特徴	・すべての公共機関や民間企業が個人情報を本人の同意なく、当初の目的以外の用途に使用した場合、処罰される（5 年以下の懲役か、5000 万ウォン以下の罰金）。 ・個人情報流出時には該当の個人へ流出の事実を即時に通報し、被害の予防と救済申請ができるようにする。
監督機関等	独立した監督機関はない。
個別法 （発効時期）	・通信の秘密保護法(1993) ・信用情報の保護と使用に関する法律(1995) 大手クレジットカード会社が顧客の同意なく保険会社に顧客情報を提供していたことにより罰金刑を適用。 ・電子商取引基本法(1999,2005) 電子商取引に関する安全性の確保、消費者対応について規定。 ・情報通信ネットワークの利用とデータ保護の促進に関する法律（Act on Promotion of Information and Communications Network Utilization and Data Protection) (2000) 通信事業者、メディア事業者、ホテル、旅行代理店、航空会社等に対し共通の公正情報原則を規定。２００４年 DM 業者６８社に罰金刑。
特記事項	・情報通信部が個人情報紛争調停委員会（Personal Information Dispute Mediation Committee）を 2001/12 に開設、非拘束の調停を実施していたが今回（2008 年）の法改正で金銭的な損害賠償の協議だけでなく、侵害行為の中止や再発防止措置などを勧告できるよう、権限を強化する。

	・韓国情報通信協会（KAIT）がプライバシーマーク制度を制定している。
備考	・公共と民間部門の個人情報保護基本計画と法令、制度を改善する等、主要の事案を審議する「個人情報保護委員会」を国務総理室の傘下機構として新設する。

国･地域名	ニュージーランド
包括法 （発効時期）	プライバシー法（ Privacy　Act　of　1993 ）
その特徴	・公的および民間部門における個人情報の収集、利用、配布について規定 ・自動処理、手動処理の両方をカバー ・情報主体に対しアクセス権を規定 ・オーストラリアの法律に近い
監督機関等	プライバシー委員会（Office of the Privacy Commissioner ） （プライバシー・コミッショナー法(1991)にもとづき設置 ）
個別法・関連法 （発効時期）	①　医療情報プライバシー規範（Health Information Privacy Code 1994） ②電気通信プライバシー規範（Telecommunications Information Privacy Code 2003）
特記事項	①プライバシー委員会（Office of the Privacy Commissioner ）の概要 ・スタッフ数約３０名（パートタイム含む） ・年間約１０００件の苦情、６０００件の問合せを処理 ・調停成功率は８５％ ・調停不調時には人権裁判所に提訴可能 （是正命令のほか２０万ＮＺドル以下の損害賠償裁定がある）
備考	①ＥＵ指令との適合性について欧州委員会より海外移転統制について修正要求があるが議会での進展はない。

国･地域名	メキシコ
包括法 （発効時期）	個人情報保護に関する包括法はまだない
その特徴	
監督機関等	
個別法・関連法 （発効時期）	Federal Consumer Protection Law ・通常の方法、電子的な方法、その他の手段による取引を実行した消費者の保護を目的 ・消費者はダイレクトマーケッティングの対象となることを拒否できる。 ・企業は顧客の書面による明示的な許可がない限り個人情報を第三者に転送できない。 Mexican E-Commerce Act(2001) ・消費者保護、プライバシー、デジタル署名、電子文書をカバー ・消費者法に「電子商取引およびその他の手段の取引における消費者の権利」という章が新設され整合が図られた。
特記事項	包括法はないが個人データの保護に関する法律は行政分野を含め２０以上存在し、さまざまな分野に亘っているため注意が必要である。
備考	ATA（Asia-Pacific Trustmark Alliance）の一員として AMIPCI が活動、Pathfinder Project にも 4 社が参加。

国･地域名	フィリピン共和国
包括法 （発効時期）	個人情報保護に関する包括法はまだない
その特徴	
監督機関等	
個別法・関連法 （発効時期）	①Electronic Commerce Act （2000） ・電子ファイルへのアクセス権、第三者への漏えいを禁じる秘密保持義務等を規定 ・コンピュータシステムへの不正アクセスに対し 10 万ペソ（約２千米ドル）以上の罰金と 6 ヶ月より 3 年の懲役を規定
特記事項	①Information Technology and E-Commerce Council が「データのプライバシーに関する法律」を提案している。 ・ＥＵ指令に基づく立法化 ・「コンピュータをベースとする国民ＩＤシステムの採用」（歴代大統領が支持するも最高裁が憲法違反と判断）を意識
備考	

国･地域名	シンガポール共和国
包括法 （発効時期）	個人情報保護に関する包括法はまだない
その特徴	
監督機関等	
個別法・関連法 （発効時期）	①Computer Misuse Act (1998) ・コンピュータ通信の違法傍受を禁止、また警察の捜査権限を大幅強化 ②Electronic Transactions Act (1998) ・関連記録の守秘義務を規定、無許可の開示に対し最大１万ＳＧドルの罰金または 12 ヶ月の懲役 ・警察は任意のコンピュータを検査でき、法令違反行為に対し令状なく書類の公開を要求できる。
特記事項	①E-Commerce Code for the Protection of Personal Information and Communications of Consumers of Internet　Commerce（National Internet Advisory Board 1998） ・産業界の自主規制 ・ＥＣサービス事業者に対しユーザーの取引記録、個人情報の守秘義務を推奨 ・消費者に通知することなく個人情報を転送または公開することを禁止
備考	①財産法により事業者が従業員の電子メール、インターネットの使用状況を監視することは容認されている。

国･地域名	中華民国（台湾）
包括法 （発効時期）	個人情報保護に関する包括法はまだない
その特徴	
監督機関等	①単一のプライバシー監督機関はない （各政府機関が所管する民間セクターを指導している。）
個別法・関連法 （発効時期）	①Computer-Processed Personal Data Protection Law(1995) ・政府機関および民間８セクター（信用情報、病院、学校、電気通信、金融、セキュリティ事業、保険、報道）を対象 ・情報主体は自己のデータについて修正、利用中止、削除、プライバシー保護法が制定されていない第三国への移転禁止等の権利を有する。 ・犯罪組織への漏えいもありさらに規制強化の動きもある
特記事項	
備考	

国･地域名	タイ
包括法 （発効時期）	民間部門を対象とした個人情報保護に関する包括法はまだない
その特徴	
監督機関等	
個別法・関連法 （発効時期）	Official Information Act(1997) 州政府の保有する個人情報が対象で民間セクター対象の法的メカニズムはない。
特記事項	・APEC　Framework および関連成果物を関係団体（商業会議所、銀行協会、保険協会、ダイレクトマーケッティング協会、ウェブマスター協会、消費者団体など)、メディアを通じて公開。
備考	

国･地域名	ベトナム
包括法 （発効時期）	個人情報保護に関する包括法はまだない
その特徴	
監督機関等	
個別法・関連法 （発効時期）	Law on E-Transactions ・事業者および個人は電子取引を行う際に法に適合したセキュリティ管理措置を選択できる権利を有する。 ・事業者および個人は本人の同意ない場合私的な情報の利用、提供、公示をしてはならない。 Law on Information Technology ・個人情報の収集・処理・利用・蓄積・提供について詳細な規制を明記
特記事項	･VECITA(Vietnam e-Commerce and Information Technology Agency)の調査（2007 年実施）によると 290 の website でプライバシーポリシーを公開している website はわずか 75（２６％）件と低水準にとどまり、個人情報の安心・安全が電子商取引の障害のトップに位置づけられている。 ・クレジットカード盗難により 440M VND 超(約 30,000ＵＳＤ)の不正使用例あり。 ・VNISA(Vietnam Information Security Association)の調査によると、2008 年には 40 件のオンライン犯罪があった。最も被害の大きかったのは PA Vietnam 社のホストコンピュータがハッカーに攻撃され、約 1 万の顧客ウェブサイトのホスティングが無効になった事件である。
備考	・APEC プログラムへの積極的な参加をテコに事業者、消費者への啓蒙

	を計画。 ・トラストマーク（TrustVn）の国際承認を推進。

国･地域名	日本
個人情報保護に関する包括法	個人情報の保護に関する法律【2003 成立、2005 施行】
その特徴	・ 電子データ、非電子データ双方を対象 ・ 情報主体による開示請求権（手数料徴収可） ・ 委託先監督責任 ・ 懲役、罰金の行政罰（間接罰） ・ 小規模事業者（保有個人データ５０００件未満）の適用除外の特例あり ・ 越境規制の規定なし ・ 行政部門は別の法律で規定（＝セクトラル式）
監督機関等	①各省庁が分担（全業種横断の専門的な監督機関はない）
個別法･関連法	（省略）
特記事項･動向	① 各省庁が業界ごとにガイドラインを作成し公表。 2007/3 経済産業省がガイドラインで暗号化特例を明記。 ②法施行以降勧告実績はあるが罰金･懲役事例はない。 ③ファイル共有ソフト Winny を介した情報漏洩相変わらず。 ④プライバシーマーク制度の浸透。 ⑤特定商取引法改正で電子メール広告のオプトイン規制採用（2008/12 施行）
備考	

6. 個人情報保護に関するホームページでの表記内容調査

6.1　調査内容の概要

ＥＣＯＭでは「個人情報の保護に関する法律」の成立以来、事業者が個人情報保護に関する自社の取組みとその方針（いわゆるプライバシーポリシー）をホームページ上でどのような表記を行っているかについて目視調査を実施してきた。今年度もＥＣＯＭ会員企業１１２社とオンライントラストマークを取得しているネット販売事業者２０９社を対象に調査を行ったのでその結果を次ページ以降に掲載する。

大企業が多数を占めるＥＣＯＭ会員、および小企業が大半を占めるネット販売事業者それぞれのプライバシーポリシー公開状況を概観することにより、自社の立ち位置と表記内容を客観的にチェックすることが可能になるものと考えている。なお、今年度は個人情報の国外移転に関する記載の有無について新たに調査項目に追加したことを付記しておきたい。

6.2　調査結果

次ページ以下

ホームページ上におけるプライバシーポリシー

表記状況調査

（ECOM 会員企業・ネット販売事業者 比較）

2008 年 8 月

次世代電子商取引推進協議会

個人情報保護 WG

目　次

1. 表記状況調査の概要

(1) 調査方法：2008 年度 ECOM 会員およびネット販売事業者のホームページ目視

(2) 調査日程：2008 年 6 月 4 日～6 月 16 日

(3) 調 査 数：

ECOM 会員企業 112 社

(さまざまな業種にわたり、大企業も数多く含まれる。なお対象は事業会社に限定し、業界団体等は除外している。)

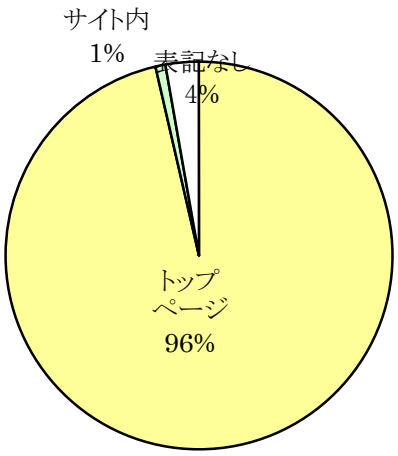
ネット販売事業者 209 社

（オンラインショッピングトラストマークを取得している小売事業者で有限会社など小規模事業者が多い。）

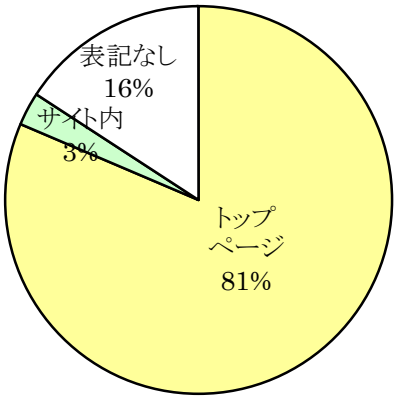
2. プライバシーポリシーの記載

（1）ホームページ上にプライバシーポリシーを記載している事業者の比率

【ECOM 会員企業】



【ネット販売事業者】



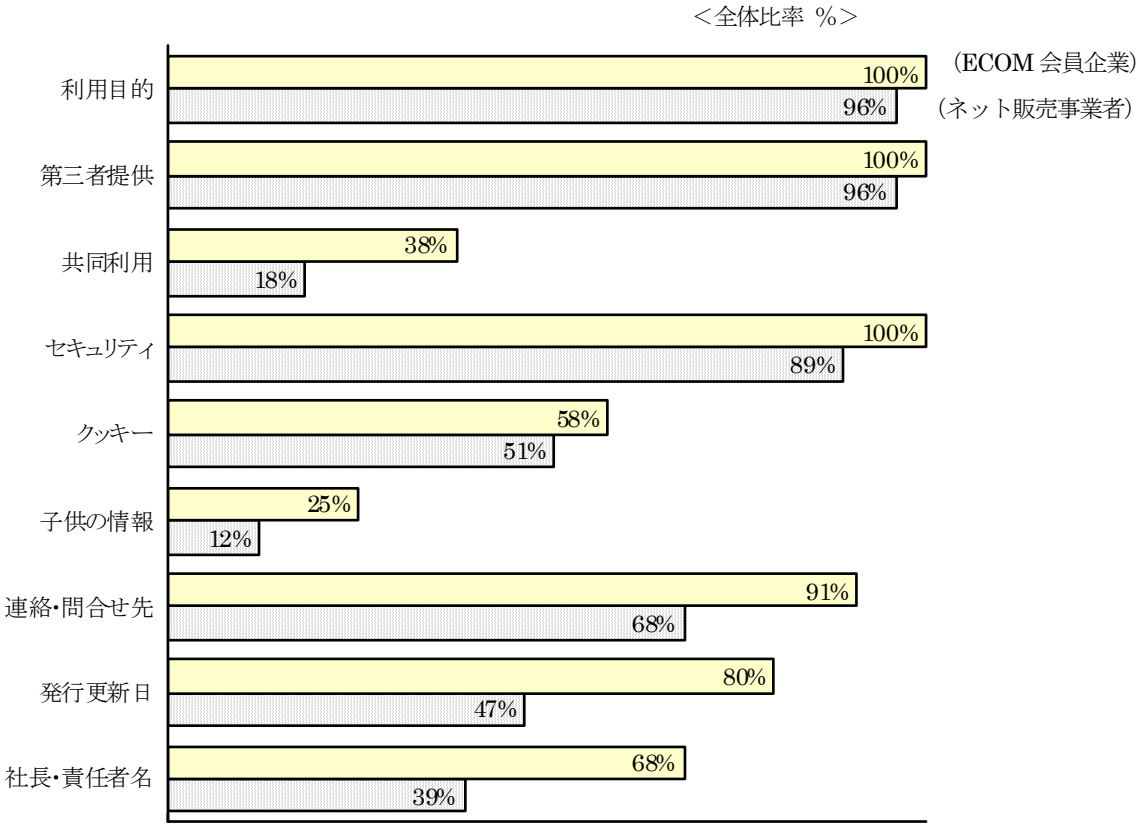
＜調査結果＞

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、ECOM 会員企業で 97%、ネット販売事業者で 84%となっている。

平成 20 年 2 月に経済産業省・（財）日本情報処理開発協会から公表された「経済産業分野の事業者における個人情報の保護に関する取組み実態調査 2008」（以下、「経済産業分野取組実態調査」と略）によれば事業者の 91%が「プライバシーポリシーを策定・公表している」としているがＥＣOM会員では 97%とさらに高い公表率となっている。なお、外国企業の日本現地法人（2 社）で英文の表記が見られたがここではプライバシーポリシーなしとカウントしている。

一方で、ネット販売事業者の公表率は 84%となっているがネット販売事業者は、主としてインターネットを介して消費者と直接相対する立場であるため、すべての事業者がプライバシーポリシーをホームページ上に掲示し消費者の信頼を確固たるものにすることが望まれる。また、ホームページ閲覧者（来訪者）に個人情報取扱事業者としてのプライバシーポリシーの有無を容易に確認させる上で、トップページでプライバシーポリシーの存在とその保管場所が確認でき、1 回のクリックでアクセスできることは今や必須事項といってよい。

（2）盛り込まれている内容



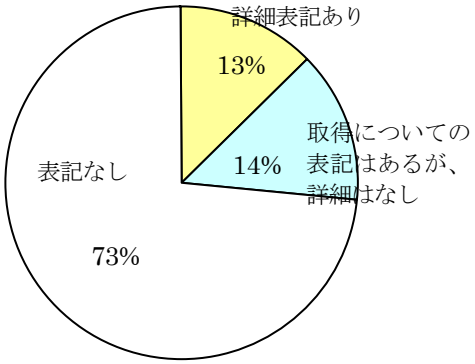
＜調査結果＞

プライバシーポリシーの中に含まれる内容では、利用目的・第三者提供の有無・セキュリティに関する事項などが高い記載率を有しており、大企業、ネット事業者間格差も小さい。特にＥＣＯＭ会員企業ではすべての企業で表記しており、今後はどの程度具体的な（信頼を得られやすい）書き方になるのかに関心が高まろう。

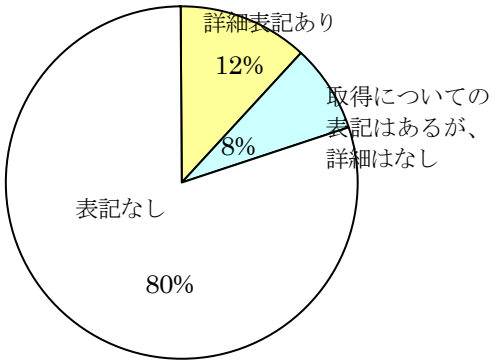
他方、「共同利用」などについては両者とも比較的低い水準であり、かつＥＣＯＭ会員企業・ネット事業者間格差は大きい。また、15 歳以下の年少者からの個人情報取得に関しては海外各国で規制強化の動きがあるので特に海外での事業展開を予定している事業者は要注意である。連絡・問合せ先については近年記載率が上昇しているがこれは重要項目の一つであるだけにまだ十分ではないだろう。問合せ窓口を明示せず単に窓口に誘導するリンクボタンを設置だけの事業者も散見されるがここでは記載がないものとしてカウントした。ネット事業者では、発行更新日、責任者名の表記等についてそれぞれ 47%、39%とまだ低い記載率に留まっており、更なる充実が望まれる。

（3）個人情報の取得方法、取得元に関する記載

【ECOM 会員企業】



【ネット販売事業者】



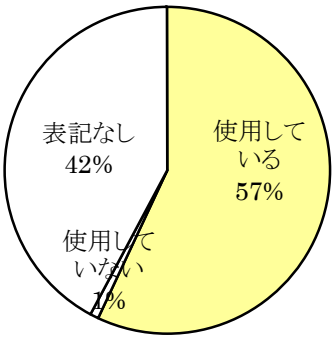
＜調査結果＞

「個人情報の取得方法」「取得元」に関する表記については、ＥＣＯＭ会員企業・ネット事業者でそれぞれ 27%、20%の記載率となっている。ネット事業者は Web からの取得が大半なので表記のない事業者が多いものと思われる。

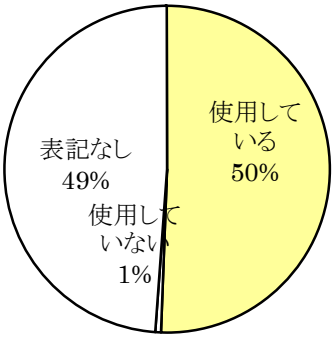
内閣府が平成 19 年 4 月に公表した「個人情報の保護に関する事業者の取組実態調査」(以下内閣府「実態調査」)によれば何らかの形で本人に対し取得元の通知・公表を行っている事業者は全体の約 28%、一方通知・公表を行っていない事業者は約 44%、分からないまたは無回答が約 28%となっており、本調査結果とほぼ近い内容になっている。法律上は必ずしも個人情報の取得方法、取得元の開示まで義務付けられていないとされているが取得方法について明記することは大きな意味があり、消費者の関心も高くなっているため今後とも意欲的な取組を期待したい。ちなみに前述の内閣府「実態調査」によれば約 50%の事業者が本人からの求めがあれば原則取得元を開示するとしている。

（4）クッキーの使用に関する記載

【ECOM 会員企業】



【ネット販売事業者】



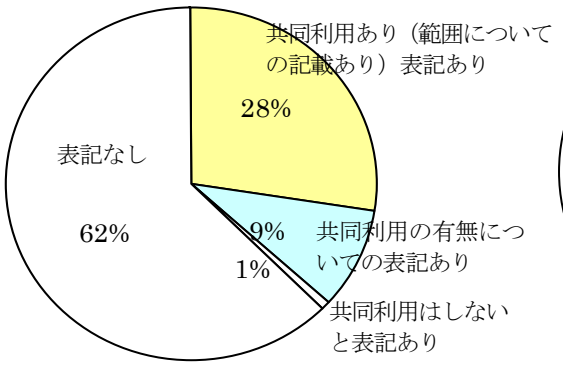
＜調査結果＞

クッキーの使用を宣言している事業者はＥＣＯＭ会員企業、ネット販売事業者それぞれ 57%、50%となっている。クッキーはホームページの改善のみならずウェブ来訪者の個別対応（One to One Marketing）等ＥＣビジネスを展開していく上での有力なツールであるが、もしクッキーを使用しているのであれば、その利用目的・利用方法を明確に表記し、更にサイト訪問者がクッキーの利用を望んでいない場合のためにその場合に享受できない便益やそれを無効にする手続き等を親切に表記することが望まれる。

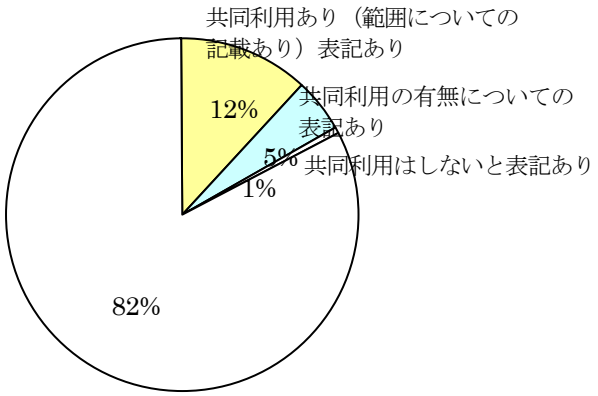
本項目についてはＥＣＯＭ会員企業とネット販売事業者間で大きな差はなく、ネット販売事業者の中にもクッキーの仕組みや利用方法を詳細に記述し安心感の醸成に努力している例が多く見られる。

（5）共同利用に関する記載

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

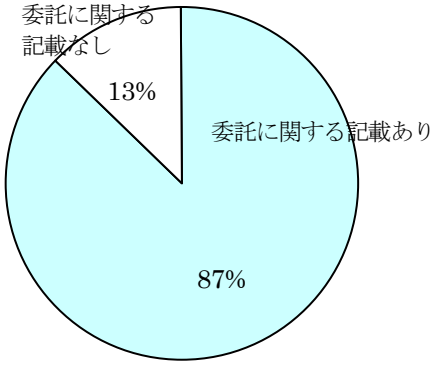
共同利用について表記している事業者はＥＣＯM会員企業 38%、ネット販売事業者 18%となっている。ネット事業者に共同利用に関する表記が少ないのは事業展開力、業種の相違等によるものと推測される。

ＥＣＯM会員企業の中で、共同利用の範囲（グループ企業間等）まで明確に表記しているのは、28%（30 社）であった。特に、金融関連企業ではほとんどで共同利用の範囲が表記されている。また、共同利用の有無について表記している 10%（11 社）で、「共同利用はしない」と表記している事業者が 1 社あった。

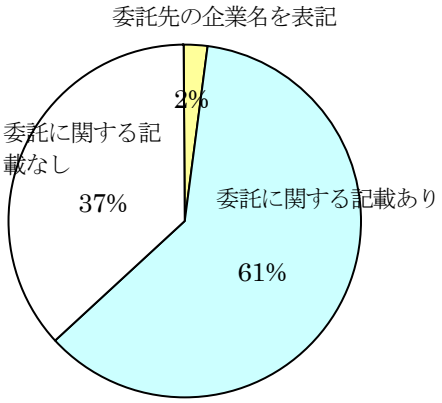
ネット販売事業者については共同利用の範囲（グループ企業間等）まで明確に表記しているのは、12%（21 社)、共同利用の有無までを表記しているのは、6%（10 社）であった。また「共同利用はしない」と表記している事業者は 1 社であった。

（6）委託に関する記載

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

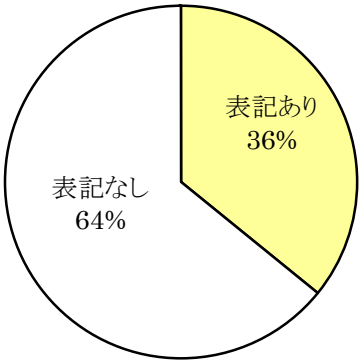
委託について表記している事業者はＥＣOM会員企業 87%、ネット販売事業者 63%となっている。委託先名の具体的な表記例として運送会社・決済代行会社等が挙げられデータ処理受託会社の表記はなかった。

前述の内閣府「実態調査」によれば委託先との個人情報の授受について約 25%の事業者が「頻繁に行われている」、29%の事業者が「たまに行うことがある」としているが保有個人データ件数が 5000 人超の事業者に限定すると、それぞれ 47%、38%と跳ね上がり両者合計で 85%の事業者が委託先との個人情報の授受を行っていることになる。

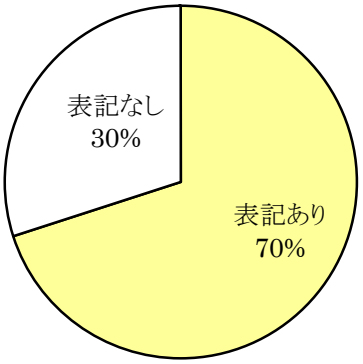
内閣府が平成１９年９月に公表した「個人情報の保護に関する法律施行状況」（以下内閣府施行状況）によれば漏えい事故の中で委託先を経由して発生するケースが全体の約３割あったとしており、委託先を含めた個人情報管理体制の構築は今後ますます重要になる。

（7）SSL、暗号化通信等の利用に関する記載

【ECOM 会員企業】



【ネット販売事業者】

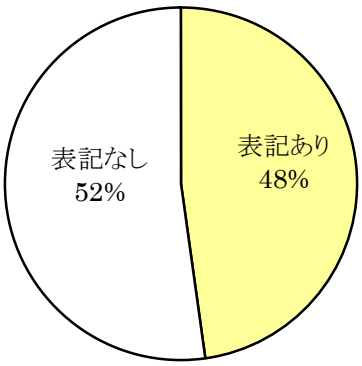


＜調査結果＞

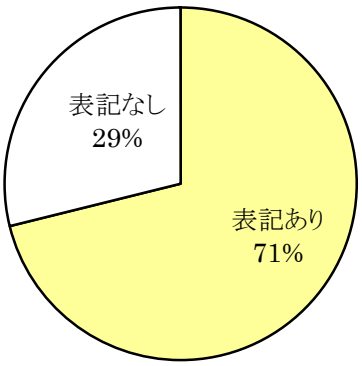
「SSL、暗号化通信等を利用している」について表記している事業者は、ＥＣOM会員企業 36%、ネット販売事業者 70%でネット販売事業者が高い数字となっている。決済用カード業界の国際標準ともいえるＰＣＩＤＳＳ(Payment Card Industry Data Security Standard)ではクレジットカード番号等の暗号化通信を事業者が具備すべき要件の１つとして明記しておりカード決済が主流となりつつあるネット販売事業者にとってＳＳＬ等の暗号化通信はその表記が必須事項となっている。

（8）安全管理に関する具体的な記載

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

安全管理について表記している事業者は、ＥＣＯM会員企業 48%、ネット販売事業者 71%でネット販売事業者が高い数字となっている。これはサイト運営目的が消費者との物品･サービスの売買という単一事業ゆえの特性に負うところが大きいものと思われる。事業者が取り扱う個人情報の内容や利用局面は百社百様であり、利用形態に合致した分かりやすい記述が望まれる。今後はどの程度具体的な（信頼を得られやすい）書き方になるのかに関心が高まろう。

（9）ファイル、記憶媒体の暗号化に関する記載

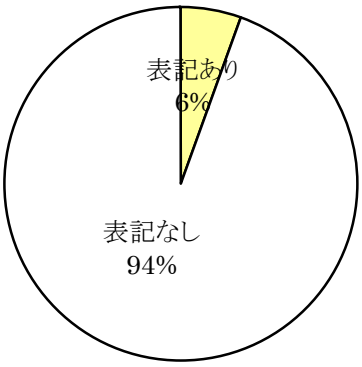
ファイル、記憶媒体の暗号化に関する実施状況等を今回はじめて調査項目に加えたがこれについて記載している事業者はなかった。

ちなみに前出の「経済産業分野取組実態調査」によれば業務用パソコンからの個人データ漏えい対策として約 76%の事業者が暗号化、パスワードの設定を講じており、社外持ち出しルールの規定（53%）、持ち出し禁止（50%）などを上回る。

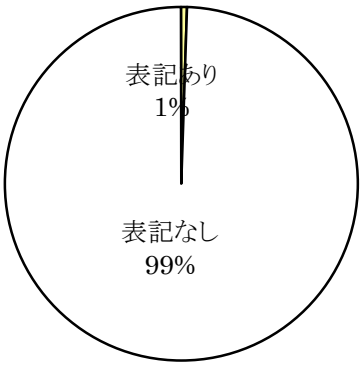
暗号化の意義については平成 19 年 3 月の経済産業省ガイドライン改訂にて加筆されているほか米国の各州で施行されている「Security Breach Notification Law」で明記されるなど一定の評価がなされていることを注目しておきたい。

（10）個人情報の国外移転に関する記載

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

個人情報の国外移転に関する記述のあった事業者は、ＥＣＯM会員企業 6%（6 社）、ネット販売事業者 1%（1 社）であった。いずれも外資系企業であった。

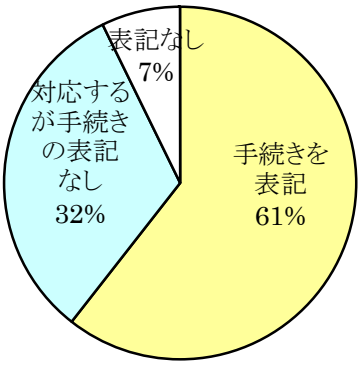
わが国の「保護法」では個人情報の国際移転について特段の記載がないため、日本企業の中では具体的な記載はなかったが、逆に言えば日本企業の海外現地法人のサイトでは注意しなければならない項目といえよう。

さらに、一部の先進的な事業者の中では「グローバルプライバシーポリシー」の策定が実践されており、今後この分野での自発的な表記が期待される。

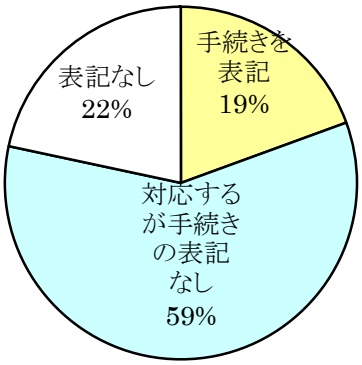
なお、この項目も今回の調査で初めて採り上げたものである。

（11）個人情報の開示等の手続きに関する記載

【ECOM 会員企業】



【ネット販売事業者】



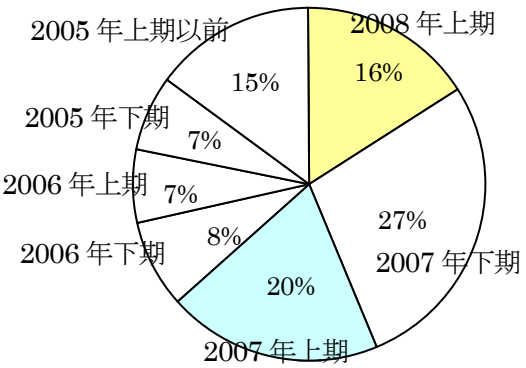
＜調査結果＞

開示等の手続きに関して、対応を表記している企業の割合には大きな差が見られ（93%と 78%）。同様に、具体的な手続きを表記している割合にも大きな差が見られる（61%と 19%）。

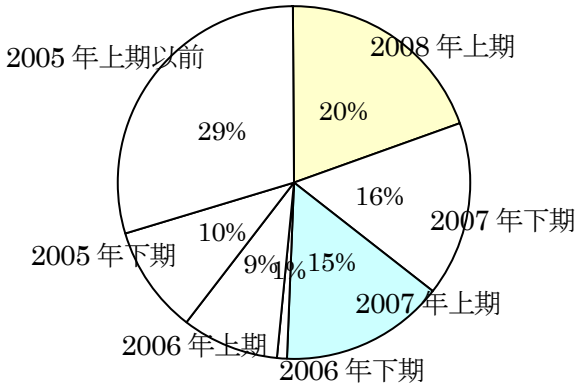
手続きを具体的に表記することにより消費者は事業者の取組み・対応状況を評価することになるため、分かりやすく親切な記載が重要である。調査対象の中には開示等の請求先として単に問合わせ用のリンクボタンを設置するのみの事業者も散見されたがこれらは「表記なし」と分類した。ちなみに前出の「経済産業分野取組実態調査」によれば開示のための専任窓口を設置、あるいは専任ではないが担当者を決めて対応を行っている事業者は全体の 67%を占める。

（12）発行、更新日に関する記載

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

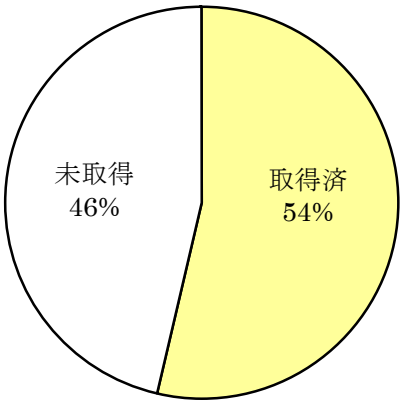
発行･更新日については、2006 年上期以降がＥＣOM会員企業 78%、ネット販売事業者 61%と大きな差が見られる。2005 年上期以前の中には保護法施行後一度も更新がないケースも散見される。

前出の「経済産業分野の取組実態調査２００８」によれば社内規程類の見直しサイクルとして「６ヶ月より１年」を挙げる事業者が 49.8%で最も多くを占めるが、他方で「見直しをしていない」が 14.7%存在しており上記の調査結果を裏付けるものとなっている。「社内で個人情報漏えい案件が発生していない。」「本人からの開示請求がない（または少ない）」等の理由で個人情報保護に関する取組み意識が低下している事業者もあるが最低でも 1 年 1 回程度の見直しが必要ではないだろうか。ホームページは鮮度が命である。

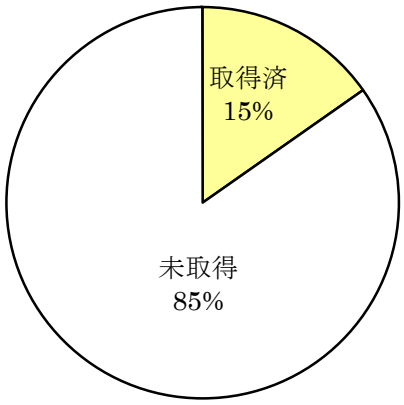
3. プライバシーマークについて

（1）プライバシーマークを取得している事業者の比率（関連会社含む）

【ECOM 会員企業】



【ネット販売事業者】

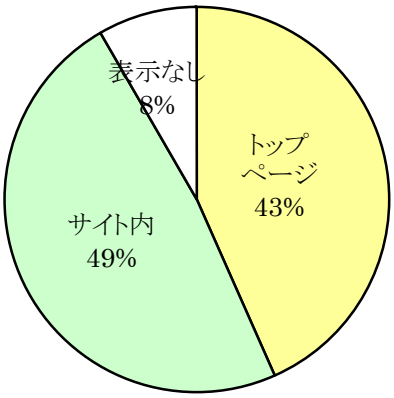


＜調査結果＞

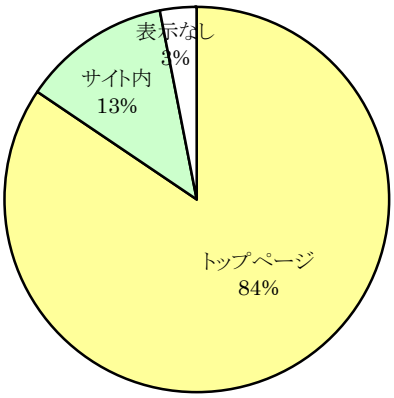
プライバシーマーク取得企業は、2005 年 4 月の保護法施行後急速に増加しているがＥＣOM会員企業では過半数となる 54%が取得しており、ネット販売事業者でも 15%に上る。今後も事業者のプライバシーマーク取得意欲は堅調に推移するものと見られ、ＥＣOM会員企業、ネット販売事業者とも取得事業者がさらに増えるものと見込まれる。

（2）プライバシーマークのロゴをトップページに掲示している事業者の比率

【ECOM 会員企業】



【ネット販売事業者】



＜調査結果＞

プライバシーマーク取得を強くアピールするためにマークそのもののトップページ掲示は極めて意味がある。実際にトップページにて表示している事業者はＥＣOM会員企業で 43%にとどまっているが、ネット販売事業者では 84%がトップページにマークを掲示しており、マークに寄せる期待度の差をうかがわせる。

4. まとめ

ＥＣＯＭ会員企業の多くを占める大企業は一般に個人情報保護体制の整備が進んでおり、プライバシーポリシーの掲示、トップページでのリンクボタン設置等はほぼ浸透している。しかしながら情報漏えい事故は依然続発しており事業者にとって暗号化措置をはじめとして安全管理対策はますます重要になっており、ＨＰ上でもさらに具体的な実施策をアピールし、サイト訪問者からの信頼獲得に引き続き留意すべきであろう。

ネット販売事業についてはプライバシーポリシーの掲示、トップページでのリンクボタン設置などで、着実に改善が進んでいる。しかしながら大企業等との比較で見るとプライバシーポリシーの充実度などで依然格差が見られる（ただし、法定個人情報取扱事業者以外の比率が高いという特性は考慮しなくてはならない)。

ネット販売事業は近年急速に取扱高を増やしているが米国との比較で見ればまだまだ成長余力がある。リアル事業者と同等の信用と安心を獲得するためにホームページ上での表記内容充実はきわめて重要である。

以　上

7. 終わりに

最近、個人情報保護に関わる方々との交流の中で『「保護法」は過去のものになった論』をしばしば耳にすることがある。いわく

・平成 17 年の施行以来、事業者・行政の懸命の取組みにより大規模漏えい事故の発生やいわゆる過剰反応は改善傾向にある。

・施行時当初危惧された「開示請求対応」がほとんど杞憂に終わったほか、当時体制構築に直接関わった担当者もその後の人事ローテーションなどで代替わりとなり往時の熱気と緊張感は薄れつつある。

・施行３年目の節目で見込まれていた「保護法」自体の改正も見送られた　等々である。

たしかに「保護法」そのものがメディアを騒がせる頻度も漸減し、またこの分野に関係されている方々のその後の意識の変化を感じることもままある。しかしながらひとたび海外に目を転じると我が国の「保護法」対応は実はこれからが本番ではないかとの気がしてならない。

本書にも触れたが「越境ルール」「漏えい時の対応」の検討・定着もまだ端緒についたばかりであるし、それ以外にも取組むべき課題は多数残されている。ＡＰＥＣのプライバシーフレームワーク実証実験も然りである。

　いずれにせよ個人情報保護が電子商取引の普及・浸透に欠くべからざる要素であることは多言を要しない。次世代電子商取引推進協議会としても引き続きこの分野の先兵として微力ながら貢献していきたいと考えている。

個人情報保護WG　メンバーリスト

氏名	会社名（団体名）
（会員）	
青山　　彰	花王株式会社
廣田　啓一	NTT情報流通プラットフォーム研究所
保倉　　豊	グローバルフレンドシップ株式会社
川城　三治	グローバルフレンドシップ株式会社
日南　文夫	株式会社小松製作所
楳木　浩典	株式会社小松製作所
山本　浩司	電気事業連合会
成松　伸之	電気事業連合会
河辺　賢一郎	東京電力株式会社
上　茂之	株式会社富士通総研
佐藤　美香子	富士電機情報サービス株式会社
行木　直之	マイクロソフト株式会社
大崎　唯一	パナソニック株式会社
吉田　久志	三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ株式会社
（有識者）	
堀部　政男	一橋大学名誉教授
鈴木　正朝	新潟大学大学院
新保　史生	筑波大学
牧山　嘉道	TMI総合法律事務所
土井　悦生	ポールヘイスティングス法律事務所
鈴木　靖	株式会社ｼｰﾋﾟｰﾃﾞｻﾞｲﾝｺﾝｻﾙﾃｨﾝｸﾞ
藤田　素康	リコー・ヒューマン・クリエイツ株式会社
（オブザーバー）	
井川　良	経済産業省
池野　富美子	経済産業省
（事務局）	
江口　正裕	次世代電子商取引推進協議会

ECにおける個人情報保護に関する活動報告書２００８

平成２１年　3月　発行

発　行　　次世代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
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。

ISBN978-4-89078-672-5 C2036