ＥＣにおける個人情報保護に関する活動報告書２００７　平成20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２００７

平成２０年　３月

次世代電子商取引推進協議会

はじめに

早いもので「個人情報の保護に関する法律」（以下「保護法」）が全面施行されて３年を経過しようとしている。施行前に法定公表事項の表示方法や開示請求への対応、見えない安全管理基準の模索など手探り状態で準備してきたことが昨日の出来事のように思い出される。その後の状況については内閣府から公表されている各年度の「個人情報の保護に関する法律施行状況の概要」を見る限り徐々にではあるが落ち着いてきているように思われる。しかしながら一方で「インターネット上の安全確保に関する世論調査」（内閣府　平成２０年１月）によれば依然として不安を感じネット利用に距離を置く消費者も半数程度存在するなどことの根深さをうかがわせる。またインターネットの越境利用の進展とともに国際協力を考えて呼応しなければならないフェーズに入ってきた。

次世代電子商取引推進協議会（以下ＥＣＯＭ）の個人情報保護WGではかような状況に鑑み平成19年度の活動として

・　個人情報の暗号化・秘匿化の推進
・　個人情報の越境対策

について重点的に取組んだ。

本報告書は上記に係る活動と平成１９年度の個人情報保護に関わる概況、従来から継続して実施してきた「ＥＣＯＭ会員企業、ネット販売事業者の個人情報保護に関するＨＰ表記調査」につい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２０年３月

次世代電子商取引推進協議会

目　　次

１．個人情報保護を巡る官民の動向

「個人情報の保護に関する法律」（以下保護法と略）が全面施行されて３年目にあたる平成１９年度はどんな１年であったのか、冒頭で官民の個人情報保護に関する動きについてレビューしてみたい。

1.1 行政サイドの主要動向

平成 19 年 4 月、内閣府は事業者の個人情報保護に関するさらなる意識の向上、体制整備推進を目的に大規模な取組調査を実施し公表した。調査項目は個人情報の利用状況や管理体制全般、本人からの開示請求対応など多義に亘り、個人情報保護が構築段階から見直し段階に移行しつつあることをうかがわせるものになった。

また 9 月には 18 年度の保護法施行状況概要が同じく内閣府から公表されており前年度と比較して概観できるようになった。各省庁に報告された漏えい件数自体は減少した（H17 年度：1,556 件　→　H18 年度：893 件）ものの 1 件当たり 50001 人以上の大規模漏えい事案はほとんど減っておらず、また事業者に対する勧告件数は逆に増加（H17 年度：1 件　→　H18 年度：4 件）するなど課題は残されている。報告の中に「漏えいした情報に対する暗号化等の情報保護措置の有無」についての統計があり、悪化傾向にあることも気がかりだが、漏えい事案全体（母数）には紙媒体も含まれているので報告の中にある暗号化等の情報保護措置実施率等については必ずしも実態を表しているとはいえない。本概要取りまとめ関係者の改善努力を期待したい。

10 月、金融庁が「金融機関における個人情報保護に関するＱ＆Ａ」を公表、漏えい事案等が発生した際の対応について高度な暗号化処理が施されている場合は本人への通知を省略しうるケースもあるとした。これは 3 月の経済産業省の見解を踏襲するものであり今後さらに他省庁への波及が期待される。

12 月に入り国民生活審議会個人情報保護部会が再開された。ここでの議論は 3 月に基本方針・政令の見直しにつながることになる。

平成 20 年 2 月経済産業省は昨年 3 月に続く 2 度目のガイドライン改訂を実施した。主な改正点は委託先、再委託先に対する委託元の管理責任のあり方について具体的に明記したことである。漏えい事故の相当数が委託先を通じて発生している現実を事業者は真摯に

受け止めなければならない。

国際化対応としてはＡＰＥＣにおける電子商取引作業部会活動が上げられる。ＡＰＥＣでは 2004 年に採択したプラバシーフレームワークの検証を目的として 9 本のパスファインダー・プロジェクトを企画しており、わが国ではそのうちのいくつかに参加し国際貢献とハーモナイゼーションを図っていくことになろう。

1.2　個人情報漏えい事故状況

１９年度の情報漏えい事故または事件件数について公式の報告はまだないが関係者等からの情報などから推測すると前年比で微減にとどまり状況が大きく改善しているとは言い難い。行政部門からも多くの情報漏えい事故が発生しており一般市民の不安感は払拭しきれていない。以下、注目すべき事案についてその顛末を列記する。

① 印刷会社

ダイレクトメール等の印刷物作成のため預かっていた個人情報を業務委託先社員が電算処理室より不正に持出しインターネット通販詐欺グループに売却していた事件（平成 19 年 3 月公表）で当該印刷会社は 19 年 4 月再発防止策と社内処分を発表した。流出源となった工場の機能はセキュリティ対策を施した新工場に完全移転、社長の役員報酬を半年間 3 割削減とした。当時の担当役員、現在の役員 5 人も同期間 2 割削減とした。東京地裁は 19 年 10 月個人情報を不正に持出し転売していた男性に対し懲役 2 年、執行猶予 5 年の有罪判決を下している。

② 警視庁

警視庁は 19 年 7 月、ファイル交換ソフト「ウィニー」を介して警察情報を流出させたとして流出元である警察官（巡査長）を懲戒免職とした。流出個人データ件数は 10,500 人分にのぼり同庁では過去最悪、警察業務の信用をはなはだしく失墜させたとして当人および監督責任者併せて 9 人に対し処分を行なった。故意ではない個人情報の漏えいで懲戒免職は初めて。

③ 金融機関

大手メガバンク、ネット銀行等が顧客の個人情報を紛失したと発表。記録媒体はそれぞれマイクロフィルム（35 万人分)、コンパクトディスク（1 万 2 千人分）で誤廃棄が原因としているが前者については昨年も同様の紛失事故（96 万人分）を報告している。過失とはいえ度重なる事故は許されない。

④ クレジットカード会社

クレジット会社の従業者 4 人が他社のクレジット利用者の個人情報を不正に取得し外部に販売していた問題で北海道警は窃盗容疑でこの 4 人を逮捕した。4 人は派遣社員として勤務していたカスタマーセンターのコンピュータを経由し信用情報機関から約 300 人分のクレジットカード情報を入手、1 人当たり数千円で転売していた。クレジットカード会社での類似事件は他でも発生している。

２．個人情報の越境移転

2.1　越境移転の分類と移転ルール

経済活動におけるグローバリゼーションの進展については今更多言を要しない。企業の直接業務、間接業務を問わずＢＲＩＣｓやＶＩＳＴＡ、ネクスト１１などと称される各国への業務移転が既に始まっているがこの傾向は当面とどまることはないと見られている。そして業務移転に伴い関係する個人情報が移転することも必然と言わなければならない。

それでは越境移転する個人情報とはどんなものがあるのだろうか。

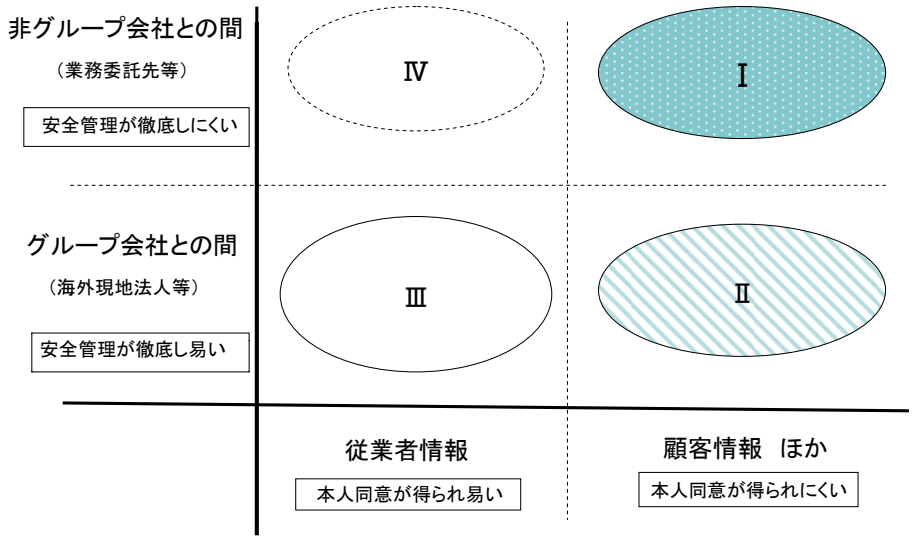
表２－１に現在越境させているまたは今後移転が考えられる個人情報を整理したが実にさまざまな個人情報が国境を越えている。特に従業者情報のみならず顧客情報も越境移転の対象になっていることは注目すべきである。

ここで個人データの越境移転について２つの切り口で分類を試みた。すなわち「対象となる情報が従業者のものか、それ以外か」と「移転先が自社のグループ会社か、それ以外か」の２つである。前者については本人同意が得ることの難易度、後者については安全管理徹底の難易度に大きな差があると考えたからである。（表２－２参照）

表２－１　越境移転している（させている）個人情報とは

	日本　→　海外	移転先	海外　→　日本	移転元
顧客情報	①自社のマーケティング活動に利用する個人情報 （製品購入者登録、会員制運営、モニタ登録　など）	ｸﾞﾙｰﾌﾟ会社（親会社へ）	⑪自社のマーケティング活動に利用する個人情報 （製品購入者登録、会員制運営、モニタ登録　など）	ｸﾞﾙｰﾌﾟ会社（子会社から）
	②自社業務の海外アウトソーシングに伴う個人情報 （コールセンター業務　など）	業務委託先	⑫受託業務の海外アウトソーシングに伴う個人情報 （日本へのアウトソーシングを含む）	ｸﾞﾙｰﾌﾟ会社業務委託先
	③受託業務の海外アウトソーシングに伴う個人情報	ｸﾞﾙｰﾌﾟ会社・業務委託先	⑬予約代行ビジネスの業務遂行に伴う個人情報 （海外旅行業者による国内ホテル予約業務　など）	業務提携先
	④予約代行ビジネスの業務遂行に伴う個人情報 （旅行業者による海外ホテル予約業務　など）	業務提携先	⑭その他スポット的に提供する個人情報 （ＶＩＰ顧客の応対依頼　など）	ｸﾞﾙｰﾌﾟ会社
	⑤その他スポット的に提供する個人情報 （ＶＩＰ顧客の応対依頼　など）	ｸﾞﾙｰﾌﾟ会社		
従業者情報	⑥人事労務管理に関する個人情報 （職位職務、評価、報酬、職歴、教育受講歴など）	ｸﾞﾙｰﾌﾟ会社	⑮人事労務管理に関する個人情報 （職位職務、評価、報酬、職歴、教育受講歴など）	ｸﾞﾙｰﾌﾟ会社
	⑦担当業務に関する個人情報 （社内外対応窓口照会に用いる個人情報）	ｸﾞﾙｰﾌﾟ会社	⑯担当業務に関する個人情報 （社内外対応窓口照会に用いる個人情報）	ｸﾞﾙｰﾌﾟ会社
	⑧グループリソースへのアクセス権設定に関する個人情報（リソースが海外にある場合）	ｸﾞﾙｰﾌﾟ会社（親会社へ）	⑰グループリソースへのアクセス権設定に関する個人情報（海外からアクセスがある場合）	ｸﾞﾙｰﾌﾟ会社（子会社から）
	⑨査証取得に関する個人情報	ｸﾞﾙｰﾌﾟ会社	⑱査証取得に関する個人情報	ｸﾞﾙｰﾌﾟ会社
	⑩間接業務の海外アウトソーシングに伴う個人情報	業務委託先		

表2－2 越境移転の分類



その上で表 1－2 のⅠ，Ⅱ、ⅢおよびⅣの各カテゴリー毎に事業者が遵守すべき海外移転ルールを下記の通り考えた。

A．移転対象が顧客情報など非従業者情報の場合

１． グループ内会社への移転

（１） 当該グループ会社の個人情報保護管理レベルを確認する（グローバルプライバシーポリシー、社内規定など）。

（２） 原則として移転の際に（またはそれ以前に）委託元企業の同意を得るものとする。

（３） 当該グループ会社の個人情報保護管理レベルが自社と相違あるときは移転を行なわない。（または個人情報保護管理レベルが自社と同レベルに達したことを確認後実施する。）

２．業務委託先・業務提携会社への移転

（１）委託元企業（または本人）との関係で業務遂行上必要か否かを確認する。

（２）必要と判断した場合はその旨の委託元企業の同意を得る、または本人への通知・公表を行なうものとする。

（3）業務の海外アウトソーシングに際しては委託先の安全管理基準と実態を精査し必要項目をについて事前に点検を行なう。点検項目については下記（注）を参照のこと。

（4）提供する個人データの項目を厳選する。

（5）合理的かつ安全な移転方法（含む返還）を確立する。

（6）業務委託先・業務提携会社の安全管理体制監査を定期的に実施する。

B．移転対象が正社員、契約社員や役員など従業者情報の場合

1． 事前に本人から越境移転に対する明確な同意をとるものとする。（入社時にあらかじめ包括的な同意を得ることも可能）

2． 人事労務関連個人データのグループ会社間移転については移転先部門での厳正な管理を確認しておくことが望ましい。

間接業務の海外アウトソーシングなど個人情報移転先がグループ会社以外の場合

3． 前項（3）と同じ

4． 前項（4）と同じ

5． 前項（5）と同じ

6． 前項（6）と同じ

（注） 業務委託先、業務提携先選定に必要な点検項目の例

- 個人情報取扱規定（取扱者の義務等）
- 漏洩等事故発生時の責任分担
- 個人情報移転時の秘匿化対応能力
- 業務終了時のデータ返還
- 委託先責任者の確認
- 第三者認証の有無

本移転ルールについてはさらに検討を重ね、近くＥＣＯＭ個人情報保護ガイドラインに追記する予定である。

2.2　ＥＵデータ保護指令とＡＰＥＣプライバシー・フレームワーク

国際移転ルールを考える上でＥＵおよびＡＰＥＣの基本となる考え方も参照したので関係部分のみ紹介しておきたい。

（１）　ＥＵデータ保護指令（1995 年採択）

ＥＵデータ保護指令では第Ⅳ章　第三国に対する個人データの移転で海外移転について下記の通り定めており適切なレベルの保護がなされていない第三国への個人情報の移転を禁止している。残念ながら日本は今日現在ＥＵから適切な保護レベルにあると認められてはいない。

第Ⅳ章　第三国に対する個人データの移転

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。但し、本指令に従って採択された国内規定に対する遵守を害しないことを条件とする。

２．～６．　（　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者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。

２．～４．　（　省　略　）

（2）ＡＰＥＣプライバシー・フレームワーク（2004 年採択）

ＡＰＥＣプライバシー･フレームワークは 2004 年 11 月の第 16 回ＡＰＥＣ閣僚会議（チリ・サンチアゴ）にて採択されたプライバシーに関する基本的な枠組みでありその実証プロジェクトが近くスタートする見通しになっている。

本フレームワークでは各国の個人情報コントローラに対し下記の通り責任を定めている。

Part I. 前文

1. ～　7.　　（　省略　）

8. このフレームワークは、以下のことの重要性をふまえて作成された。

- 個人情報のプライバシーを守ること、とりわけプライバシーの侵害や情報の悪用から帰結する損害から個人情報を守ること。
- 発展途上の市場経済にとっても先進国の市場経済にとっても、経済的社会的な成長を維持するうえで、情報の自由な流れが不可欠であること。
- グローバルな組織が APEC 加盟国内のデータにアクセスし、そのデータを収集、利用、処理でき、個人情報へのグローバルなアクセスとその利用に関して統一的なアプローチをとれること。
- 法律の執行機関が情報プライバシーの保護に向けた権限を行使できること。
  情報プライバシーの保護を実質化し、APEC 加盟国やその貿易相手国の間で情報の流れを維持するための国際的なメカニズムを促進する。

Part II. 範囲　　（　省略　）

Part III. APEC 情報プライバシーの原則

I.　損害の防止　～　VIII.　アクセスと訂正　　（　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転送するときには、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。

３．個人情報の暗号化推進

3.1　暗号化の意義

平成 19 年 3 月に改訂された経済産業省「個人情報保護ガイドライン」において次のような記載がある。

「事故又は違反への対処」を実践するために講じることが望まれる手法の例示として

（ア）事実調査、原因の究明

（イ）影響範囲の特定

（ウ）再発防止策の検討・実施

（エ）影響を受ける可能性のある本人への連絡

があるが、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。

- 紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
- 高度な暗号化等の秘匿化が施されている場合

以下　省略。

また、金融庁においても昨年 10 月公表した「金融機関における個人情報保護に関するＱ＆Ａ」の中で漏えい事案が発生した際に高度な暗号化処理が施されている場合には本人への通知を省略しうるケースもありうるとの見解を表明している。

さらに米国では 40 州以上で施行されているいわゆる「Data Breach Notification Law」(個人データを危殆化させた場合に情報主体に対しその事実の通知を義務付ける法律の総称)においても多くの場合、暗号化されておれば適用対象外であることを明示している。

これらはいずれも個人データの安全管理対策として暗号化措置を極めて高く評価しているため事業者にとって個人情報保護体制整備上の重要なテーマと判断した。

3.2 暗号化徹底のためのチェックポイントと事業者の取組み状況

暗号化推進策の一環として事業者のための暗号化徹底チェックポイントを以下の通りリストアップした。

１　明文化された暗号化ポリシーがあるか

（例）

・暗号化すべきデータベース、メディアの明確化

・暗号化手続きの明示

２　暗号化実行プロセスが確立しているか

（例）

・データベースの暗号化

・メディア（デバイス）の暗号化

・ソフト、ハードの選定と暗号化実施部門

３　暗号化実施状況（実施率等）が定量的に捉えられているか

（例）

・個人情報データベース単位

・メディア単位（クライアント端末、リムーバブルメモリ、メール等）

４　暗号化エビデンスが取得されているか

（例）

・操作ログ管理

・持出し台帳管理

・機種管理(暗号化機能を具備しているＵＳＢ等)

５　併用措置は何か

（例）

・認証手段の併用（バイオメトリクス、ＩＣカード等）

・遠隔操作によるデータ消去(暗号化ではないし完全でもないがエビデンスあり)

・内部監査の実施

・安全廃棄の徹底、誤廃棄の回避

６　グループ会社にも徹底されているか

（例）

・グループ暗号化ポリシーの制定

・インセンティブの提供

その後WGメンバー企業の実践状況をアンケート形式にて情報収集し表 3－1 に取りまとめたが下記の通り総括できる。

①暗号化ポリシーについては多くの企業が明文化しており対象となる個人データ、ファイル、メディア等が明らかになっている。

②暗号化実行プロセスについては多くの企業で全社対応専門セクションと現場部門との分担が明確になっているが中には未分化の企業も見られる。

③暗号化実施状況の定量把握については社外持出し対象機器等を中心に行なわれているが、基幹データベース等の暗号化状況については必ずしも明確ではない。

④暗号化エビデンスについては管理ログの取得が中心であるが持出台帳管理など人海戦術も併用されている。

暗号化対策についてはさらに実態把握に努めＥＣＯＭガイドライン改訂につなげていく所存である。

表３－１　個人データ秘匿化（暗号化等）徹底に向けた取組み状況

	項　　目	Ａ　社	Ｂ　社	Ｃ　社	Ｄ　社	Ｅ　社	Ｆ　社
1	**明文化された秘匿化（暗号化等）ポリシーがあるか** **・秘匿化すべきデータベース、メディアは明確になっているか**	・業務管理規定の中で個人データの暗号化についても規定があり、秘匿化すべき対象は、明確になっている。	・情報セキュリティポリシーで定められた情報種別に応じて、暗号化すべき情報資産が定められている。	・明文化されたポリシーがあり、その中で秘匿化対象が明確になっている。	・秘匿化する条件（機密度、運用形態）の定めにより保有部門が個々に判断、会社責任者が承認することになっている。	・ＩＴセキュリティガイドライン（データの秘匿措置）、PC 利用ガイドライン（社外持出し時の安全対策）にて明文化	・社内規定で明示
2	**秘匿化実行プロセスが確立しているか** **・データベースの秘匿化** **・メディア（デバイス）の秘匿化** **・ソフト、ハードの選定と秘匿化実行部門（集中・分散）**	・ソフト、ハードともに秘匿化実行プロセスは確立されている。 ・秘匿化対象となるものにより、実行部門は全社管理部署と各部管理部署に分かれる。（集中・分散の混在）	・全社情報漏洩防止システムを運用しその中で秘匿化を実施している。	・確立している ・データベースは IT 側で対応 ・メディアとデバイスは使用者側にて対応 ・ソフトの選定は集中 ・ハード選定は推奨型	・暗号化ソフトは自社製品を使用。 ・データベース秘匿化は一口に暗号化というわけに行かないため情シ部門を主体に個別に対応を策定。	・確立している。 ・実行部隊は、集中	・外部に持出す際のプロセスを確立している。
3	**秘匿化実施状況が定量的に捉えられているか** **・共有データベース（ファイル）単位** **・メディア単位（クライアント端末、リムーバブルメモリ等）**	・全社管理されているものについては、秘匿化実施状況は全て把握。 ・メディア単位についても管理実施	・前述の情報漏洩防止システムを全社展開している。	・サーバー：すべて暗号化されている ・クライアント：いいえ ・メディア：　いいえ	・暗号化ソフト導入、設定ＰＣは定量把握。 ・個々のＰＣ内のデータの実態まで捕捉はせず。 ・重要ＤＢは個別に対応	・ＤＢについては今後実施予定 ・メディアについては　毎年棚卸しを実施 ・ノートＰＣは配布時に集中管理で暗号化ソフトを導入	・外部持出し端末の秘匿化状況を全数把握している
4	**秘匿化エビデンスが取得されているか** **・操作ログ管理** **・持出し台帳管理** **・機種管理（暗号化機能を具備しているＵＳＢ等）**	・操作ログ管理（全クライアント端末） ・各部管理のものについては、台帳管理を実施。	・前出の全社情報漏洩防止システムでログ監査を実施している。 ・可搬媒体は原則使用禁止とし、やむをえず使用する場合は逸脱使用として台帳管理している。	・個人情報管理システムでは、暗号化とともに案件台帳管理、取扱台帳管理がされている ・クライアント：秘匿化エビデンスはない	・機種管理ＤＢ。 ・持ち出し許可台帳ＤＢ。 ・ＰＣの操作ログ監視（暗号化に特化しているわけではない）。	・操作ログ　個人情報専用ファイルサーバー利用者の操作ログを管理 ・個人情報台帳による持ち出し管理 ・情報システム部門が選定した、USB メモリーを必要者に配布	・操作ログ管理、持出し台帳管理を実施
5	**併用措置は何か** **・認証手段の併用（バイオメトリクス、ＩＣカード等）** **・遠隔操作によるデータ消去** **・内部監査の実施**	・メディア書き込み許可キーによる管理（キー管理者は、各部機密管理責任者で部長級以上） ・内部監査を定期的に実施	・持出ＰＣのシンクライアント化 ・個人データ格納場所の限定、入退室管理 ・内部監査の実施　等	・認証手段：遠隔ログインは IC カードを併用 ・内部監査を定期的に実施している	・モバイルＰＣは指紋照合併用。 ・Ｐマーク、ＩＳＭＳ資格取得維持に伴う監査実施。	・遠隔操作によるデータ消去は携帯電話のみ ・経営監査室による内部監査を実施	・内部監査を実施
6	**グループ会社にも徹底されているか** **・グループ暗号化ポリシーの制定**	・グループ会社の多くが本社の手法を踏襲しているものと思われる。	・上記についてグループ会社においても段階的に実施中である。	・上記はすべて日本の法人にのみ適用	・子会社は同一ポリシー下で運用。	・グループ会社は今後実施予定	・グループセキュリティポリシーを制定
7	**備　　考**						

４．個人情報保護を巡る海外動向と潮流

4.1　アジア太平洋地域における動向

海外諸国の動向として昨年度までに欧米等の先進国、およびＢＲＩＣｓ諸国について調査を行なってきたが今年度はさらに太平洋周辺各国についても調査の対象に加え研究したのでその一部を紹介する。

① ニュージーランド

民間部門を対象にした包括法、プライバシー・コミッショナー制が確立しており、プライバシー・コミッショナー・オフィスでは年間 1000 件の苦情と 6000 件の問合せに対処している。海外移転規制が不十分なためＥＵ適合性は今後の課題となっている。

② メキシコ

個人情報保護に関する包括法はないものの様々な分野で個人情報保護に関する法律があるので注意が必要である。消費者保護法には消費者はダイレクトマーケティングの対象となることを拒否することができる、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などの規制がある。

③ 中華民国（台湾）

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）を対象にした Computer-Processed Data Protection Law により情報主体は自己のデータについて利用中止や削除および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。

④ シンガポール

個人情報保護に関する包括法はまだないが、ＥＣに関するものとして Electronic Transaction Act(1998) があり、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 ヶ月の懲役を科している。また、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。

⑤フィリピン

個人情報保護に関する包括法はまだないが、Electronic Commerce Act (2000)において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の規定、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 年の懲役との規定がある。

4.2　カナダにおける個人情報保護に関する動向

個人情報保護先進国と見られるカナダの状況について以下に特記する。カナダはＥＵ加盟国以外でＥＵ適合性を承認されている数少ない国の一つである。

①カナダにおける個人情報保護法の運用体制

カナダにおける個人情報保護法の根幹に位置するものが「Personal Information Protection and Electronic Documents Act」で頭文字をとって「PIPEDA」と呼ばれている。この法律は OECD8 原則(1980)、ＥＵ指令(1995)を参考にして策定したモデルコード(1996)を発展させ 2004 年に連邦法として定めたものである。これとは別に国内各州には「Personal Information Protection Act」(略称 PIPA)が存在しており、それぞれの Information & Privacy Commissioner が統括の任にあたっている。「PIPEDA」「PIPA」が併存することにより一部には「二頭政治」を揶揄する声が無いわけではないが、連邦・州関係者双方の熱意ある交流を目の当たりにするとこれはたいした問題ではないように感じた。わが国では国･自治体間の問題よりもむしろ主務大臣制に起因する（と思われる）省庁間の見解の相違や保護法・業法間のギャップなどが現場の声として話題に上ることがある。心強いことに省庁ガイドラインの共通化に関する作業も進みつつあると聞いているが、関係各位の意欲的なコラボレーションにより省庁間・部門間の摺り合わせが進み、結果としてより統一した運用が実現することを期待したいものである。

②「PIPEDA」における個人情報の定義

「PIPEDA」では事業活動に使用している勤務先およびその住所、電話番号、メールアドレス等を、Business Contact Information と括り当初より保護の対象から除外している。一方わが国の「保護法」では個人を特定できるものは一部の例外の除き全てを保護の対象としておりいわゆる「名刺情報」もその限りではないとされている。しかしながら「名刺情報」は情報主体側が積極的に提供する性格を有するだけではなく取得事業者側においても建物の内外を問わず使用局面は広範囲にまたがっているため保護を徹底するために大きな負荷を負っている。もちろん名刺情報であっても軽率な取扱いは避けなければならないが保護にかけられる社会的コストと想定される弊害とのバランスに配慮することは重要である。名刺情報を電話帳類と同様に（カナダ法にあるように）保護の対象から除外することが合理的と考えている。

③米国「Data Breach Notification Law」対する反応

米国 37 州で既に施行されている Data Breach Notification Law （事業者が保有してい

る個人情報を危殆化させた場合には本人にその旨を通知しなくてはならないとする法律の総称） への対応としてカナダでは一早く Voluntary Canadian Guideline を準備したほか PIPEDA 改正の検討を開始している。カナダが「Data Breach Notification Law」対応を International Requirement と位置づけ世界に先駆けた迅速な動きを見せているが、わが国にとっても早晩何らかの対応を迫られるのではないかと思われる。

4.3　各国の状況

ＥＣＯＭでは欧米をはじめＢＲＩＣｓ、アジア諸国の個人情報保護動向について着目しており、国別動向を別紙の通り整理している。

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　シンガポール
１６　フィリピン
１７　中華民国（台湾）
１８　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年の苦情の伴う調査件数　１２６３件 ③２００７年の民間部門起訴件数　３９９件 ④徴収された罰金は被害者への補償に転用される。
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。 ② 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 41 州に波及、連邦法化の準備も進んでいる。 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、登録者数は直近で 6000 万人超、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 ② 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 プライバシー保護に関するモデルコード ＥＵ指令に基づく法律を制定していたケベック州法を元にカナダ規格協会が作成、連邦法としてＰＩＰＥＤＡに引き継がれた（州によって市民の意識に差がある）。 ②米国 37 州で施行されている Data Breach Notification Law と同様の

	目的で Voluntary Canadian Guideline を準備している。
備考	ＥＵから十分な保護レベルにあると承認されている。

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、配布を禁じているが個人データの定義、その保護方法は特別法で規定されることになっている(議会にて審議中)。
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を許可し、ユーザは暗号鍵を開示しなければ 7 年以下の拘禁刑） ② 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 スパイウェアを取締る法制が議論され始めている。 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 はアルゼンチンを adequate と判定(中南米地域では初めて)。
備考	

国･地域名	韓国
個人情報保護に関する包括法等	民間部門の包括法はまだない。
その特徴	
監督機関等	独立した監督機関はない。
個別法･関連法	・ ①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。 ②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。 ③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･動向	① 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。 ② 韓国情報通信協会（KAIT）がプライバシーマーク制度を制定
備考	

国･地域名	ニュージーランド
包括法　等	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	① ＥＵ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 ② 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　等	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）	①Federal 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。 ②Mexican 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	①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	①ATA（Asia-Pacific Trustmark Alliance）の一員としてアクティブに活動を行なっている

国･地域名	フィリピン共和国
包括法　等	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	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（手数料設定可） ・ 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 2007/10 金融庁がＱ＆Ａにて暗号化特例に言及 ②法施行以降勧告実績葉あるが罰金･懲役事例はない。 ③ファイル共有ソフト「ウィニー」を介した情報漏洩頻発 ④プライバシーマーク制度の浸透（マーク取得事業者数は 9000 社超）
備考	

５．個人情報保護に関するＨＰ表記内容調査

ＥＣＯＭでは個人情報保護法（略称）の全面施行以降、事業者が個人情報保護に関する取組について自社の Web 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１６１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２２８社を対象に調査を行ったのでその一部を紹介したい。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（個人情報保護方針）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。

なお今回から新たな調査項目として

・個人情報取得方法（または取得元）に関する記載があるか

・委託に関する事実を記載しているか

など数項目を追加した。

詳細は別途「Web ページ個人情報保護表記 目視調査―ECOM 会員企業・ネット販売事業者比較」をご参照いただきたい。

Web ページ個人情報保護表記 目視調査

ECOM 会員企業・ネット販売事業者 比較

2007 年 8 月 15 日

次世代電子商取引推進協議会

個人情報保護 WG

1. 目視調査の概要

(1) 調査方法：2006 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：2007 年 5 月 25 日～6 月 10 日

(3) 調査対象：ECOM 会員企業 161 社

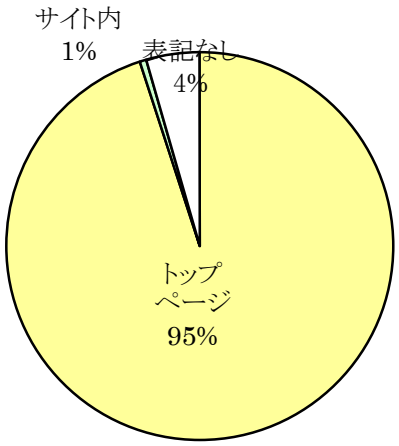
（理事会員、正会員Ａ、正会員Ｂを含む。但し財団法人、社団法人等の団体会員を除く）

ネット販売事業者で財団法人日本通信販売協会よりオンライントラストマークを付与されている事業者　228 社

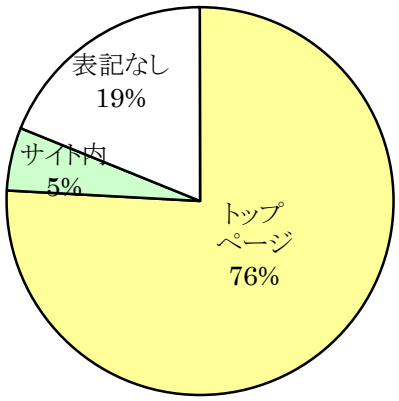
2. プライバシーポリシーの記載

（1）ホームページ上に表記している企業

【ECOM 会員企業】161 社



【ネット販売事業者】228 社



＜調査結果＞

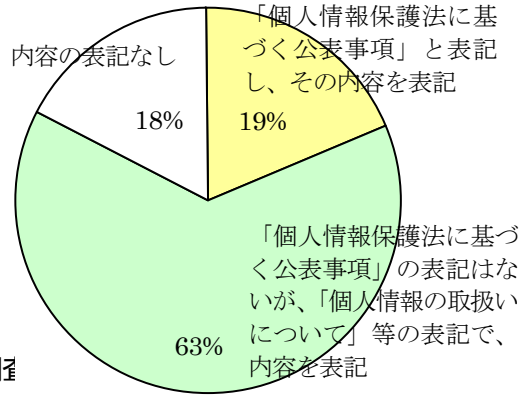
ホームページ上に何らかの形でプライバシーポリシーに関する記述がある企業は、ECOM 会員企業で 96%、ネット販売事業者で 81%となっている。

平成 19 年 4 月に内閣府国民生活局から公表された「個人情報の保護に関する事業者の取組実態調査」（以下、「取組実態調査」と略）によれば保有個人データ件数 5000 件以上の事業者企業の８８%がプライバシーポリシーを策定・公表しているがＥＣＯＭ会員の中では９６%とさらに高い公表率となっている。（外資系企業 2 社で英文によるプライバシーポリシー表示があったがここでは日本文表示のみをカウントしている。）

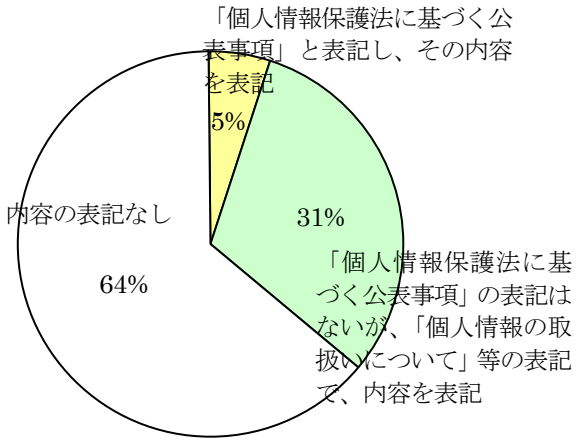
ネット販売事業者の公表率は８１%となっているがネット販売事業者は元来インターネットを介して消費者と直接相対する立場であるため、すべての事業者がプライバシーポリシーをホームページ上に掲示することが望まれる。また、ホームページ閲覧者（来訪者）に個人情報取扱事業者としてのプライバシーポリシーの有無を容易に確認させる上で、トップページでプライバシーポリシーの存在とその保管場所が確認でき、1 回のクリックでアクセスできることが重要であることは言うまでもない。

(2)「個人情報保護法に基づく公表事項」の表記

【ECOM 会員企業】154 社



【ネット販売事業者】185 社

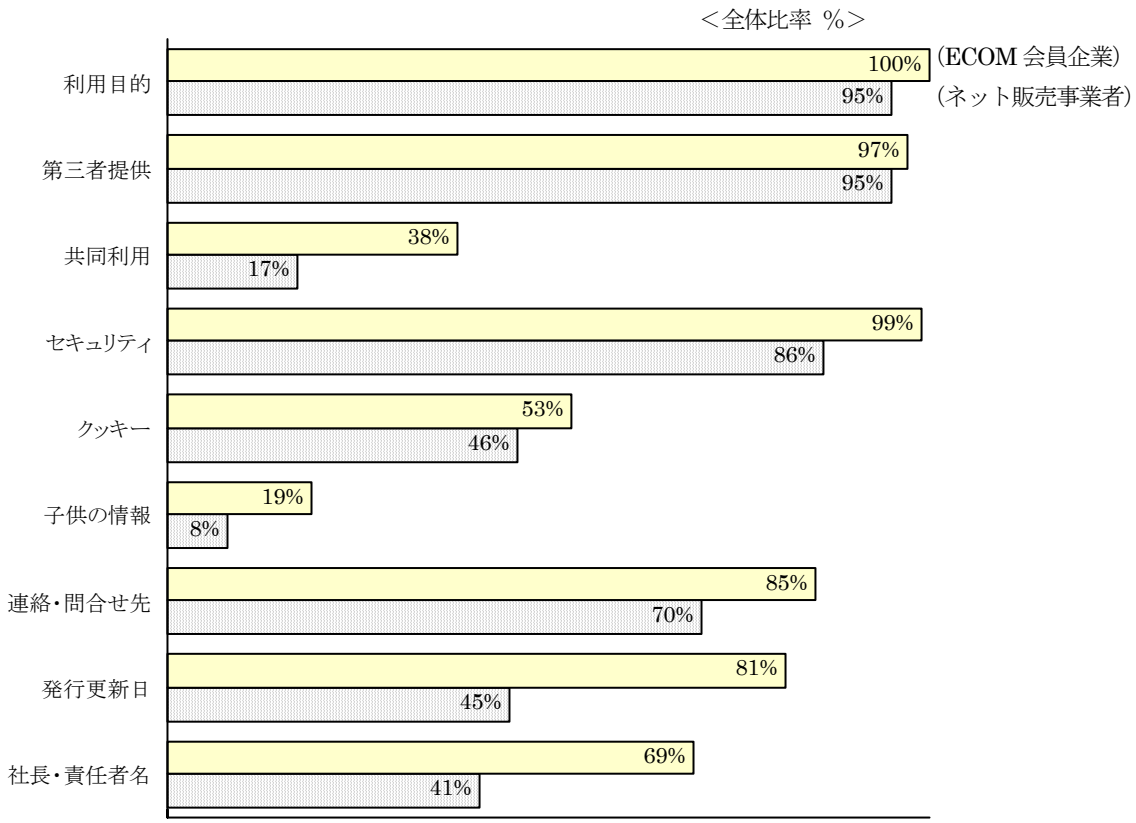


＜調査

個人情報保護法に基づく公表事項の記載率は、ＥＣＯＭ会員企業・ネット事業者でそれぞれ８２%、３６%と相当の格差が見られる。ネット販売事業者は概して従業者数が少なく法的対応余力も乏しい、あるいは法律上の個人情報取扱事業者に該当しない可能性もあってこのような結果になったものを推測されるが、消費者に対し安心してインターネット通信販売を利用できる環境づくりのためにも法律で定められた公表事項の表記は重要である。

(3) 盛り込まれている内容

【ＥＣＯＭ会員企業】154 社　　【ネット販売事業者】185 社

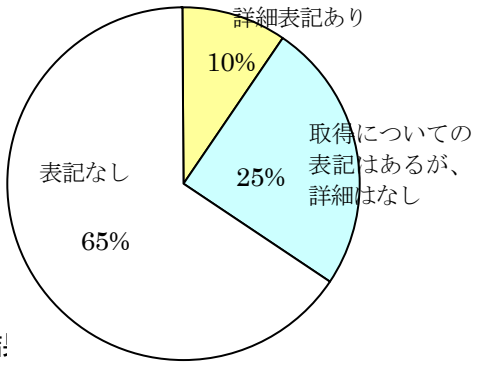


＜調査結果＞

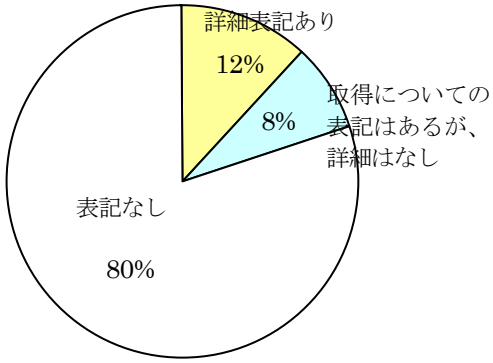
プライバシーポリシーに含まれる内容では、利用目的・第三者提供の有無・セキュリティに関する事項などが高い記載率を有しており、大企業、ネット事業者間格差も小さい。他方、「共同利用」などについては両者とも比較的低い水準であり、かつＥＣＯＭ会員企業・ネット事業者間格差は大きいが、これは事業展開力、業種の相違に負うところが大きいものと思われる。連絡・問合せ先については昨今記載率が向上しているがこれは必須項目であるだけにまだ物足らない。ネット事業者では、発行更新日、責任者名の表記等についても更に高い記載率になってよいのではないかと思われる。

(4)「個人情報の取得方法」「取得元」に関する表記について

【ECOM 会員企業】 154 社



【ネット販売事業者】185 社



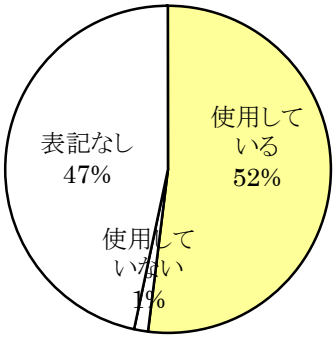
＜調査結

「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・ネット事業者間格差は大きい。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のかもしれない。

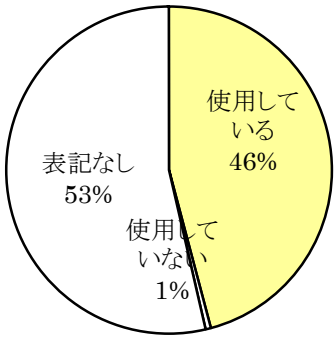
前述の「取組実態調査」によれば何らかの形で本人に対し取得元の通知・公表を行っている事業者は全体の 3 割弱、一方通知・公表を行っていない事業者は 4 割強となっているが、本調査から見ると通知・公表を行っている事業者の比率はさらに低い水準にとどまっている。法律上は必ずしも個人情報の取得方法、取得元の開示まで義務付けられていないとされているが取得方法について明記することは顧客の信頼を勝ち取る上で大きな意味があり、自発的な取組を期待したい。ちなみに前述の「取組実態調査」によれば約５割の事業者が本人からの求めがあれば原則取得元を開示するとしている。

（5）クッキーを使用している割合

【ECOM 会員企業】154 社



【ネット販売事業者】185 社

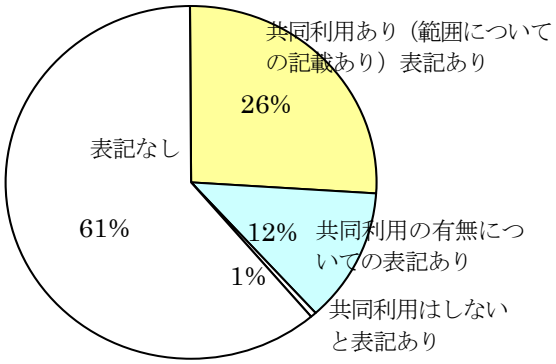


＜調査結果＞

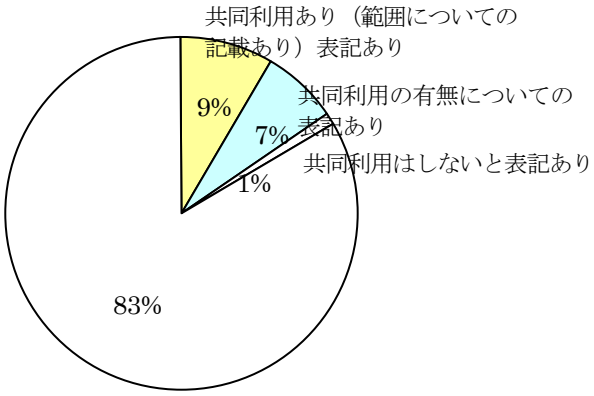
クッキーの使用を宣言している事業者はＥＣＯＭ会員企業、ネット販売事業者それぞれ 52%と 46%となっている。クッキーはホームページの改善のみならずウェブ来訪者の個別対応等電子商取引上の有力なツールであるが、もしクッキーを使用しているのであれば、その利用目的・利用方法を明確に表記し、サイト訪問者がそれを望まない場合にはそれ故に享受できない便益やクッキー自体を無効にする操作手順等を親切に表記することが望まれる。

（6）「共同利用」について

【ECOM 会員企業】154 社



【ネット販売事業者】185 社



＜調査結果＞

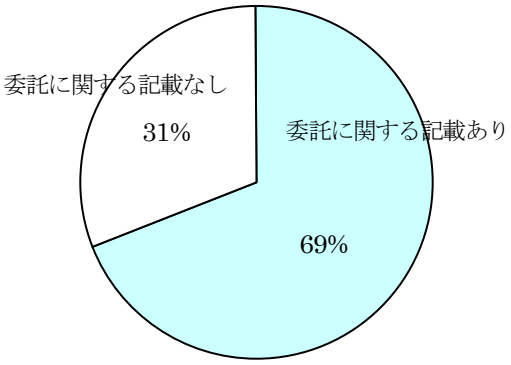
共同利用について表記している事業者はＥＣＯM会員企業 39%、ネット販売事業者 17%となっている。ネット事業者に共同利用に関する表記が少ないのは事業展開規模、業種の相違等によるものと推測される。

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、26%（40 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 12%（19 社）、「共同利用はしない」と明記しているのは 1 社であった。

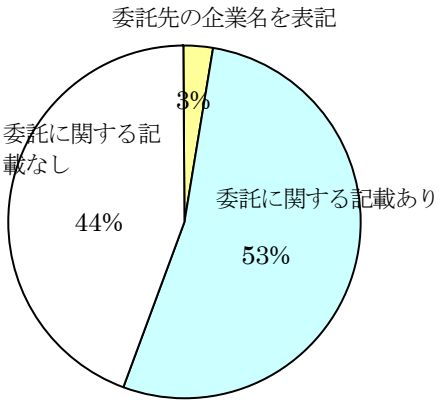
ネット販売事業者については共同利用の範囲（グループ企業間等）まで明確に表記しているのは、9%（16 社）であった。共同利用の有無について表記しているのは、7%（13 社）であった。また「共同利用はしない」と明記しているのは 2 社であった。

(7)「委託」についての表記

【ECOM 会員企業】 154 社



【ネット販売事業者】185 社



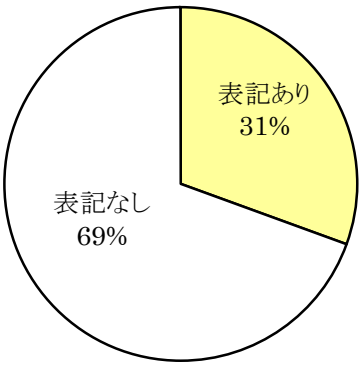
＜調査結果＞

委託について表記している事業者はＥＣOM会員企業 69%、ネット販売事業者 56%となっている。そのうちネット販売事業者の 3%が具体的な企業名として運送会社・決済代行会社等を上げておりデータ処理受託会社等の表記はなかった。

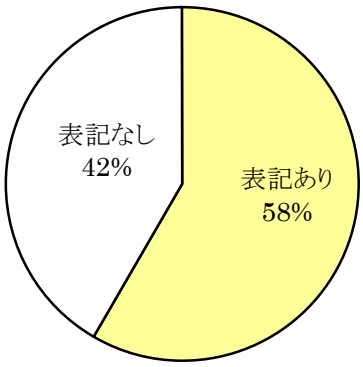
前述の「取組実態調査」では保有個人情報の数が多くなるほど委託先との間で個人情報の授受を行っているとする事業者の割合が高くなっており（保有個人情報５千人超では８割強、１千人超～５千人以下で５割弱)、今回の調査結果もそれを裏付ける結果になっている。

（8）「SSL、暗号化通信等を利用している」と表記している割合

【ECOM 会員企業】154 社



【ネット販売事業者】185 社

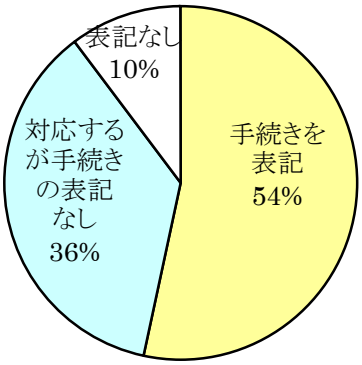


＜調査結果＞

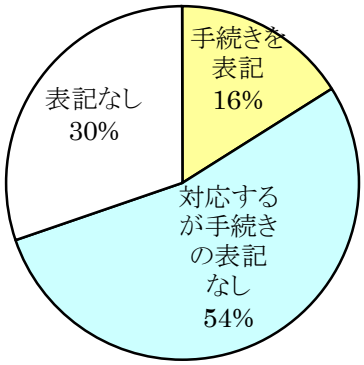
「SSL、暗号化通信等を利用している」について表記している事業者は、ＥＣOM会員企業 31%、ネット販売事業者 58%でネット販売事業者の方が高い数字となっている。決済カード業界のグローバル標準ともいえるＰＣＩＤＳＳ(Payment Card Industry Data Security Standard)ではクレジットカード番号等の暗号化通信を事業者が具備すべき要件の１つとして明記しているが、カード決済が主流となりつつあるネット販売事業者にとってＳＳＬ等の暗号化通信はその表記も含め必須事項となっている。

（9）個人情報の開示等の手続きについて

【ECOM 会員企業】154 社



【ネット販売事業者】185 社



＜調査結果＞

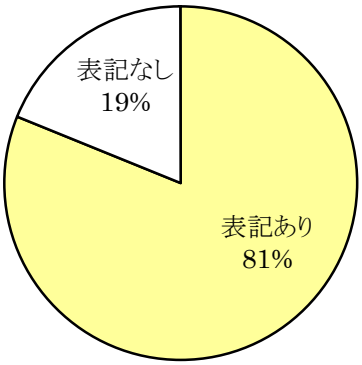
開示等の手続きに関して、対応を表記している企業の割合には大きな差が見られ（90%と 70%）。同様に、具体的な手続きを表記している割合にも大きな差が見られる（54%と 16%）。

手続きを具体的に表記することが消費者から信頼を得ることに直結することになるため、対応窓口の明示を含め分かりやすく親切な記載が重要である。

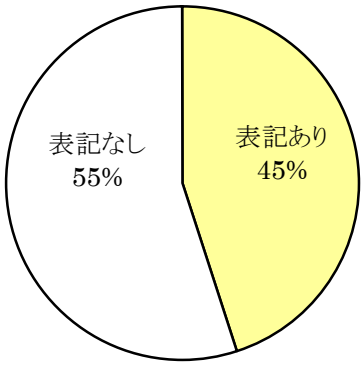
（10）「発行・更新日」について

①表記について

【ECOM 会員企業】 154 社



【ネット販売事業者】185 社

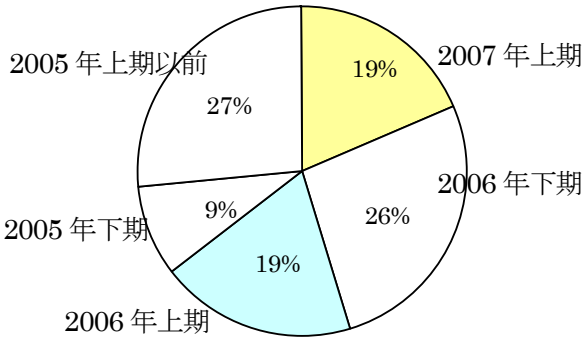


＜調査結果＞

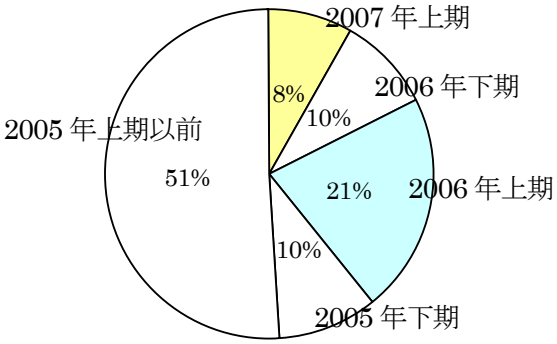
プライバシーポリシーの発行･更新日について表記している事業者は、ＥＣOM会員企業 81%、ネット販売事業者 45%と大きな差が見られる。この差は②項の更新サイクルに如実に表れている。

②「発行・更新日」について

【ECOM 会員企業】124 社



【ネット販売事業者】84 社



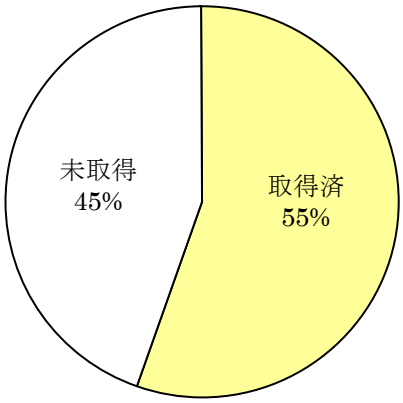
＜調査結果＞

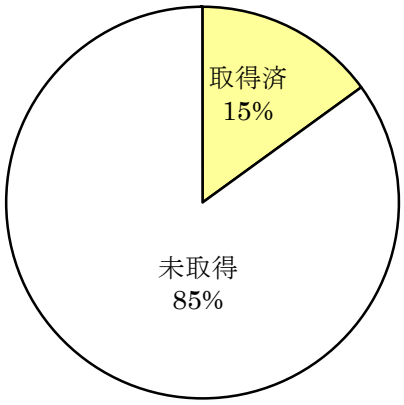
発行･更新日については、2006 年上期以降がＥＣOM会員企業 64%、ネット販売事業者 39%と大きな差が見られる。「２００５年上期」以前の中には保護法施行後一度も更新がないケースも散見される。前項の「更新日記載」と併せてキメ細かな対応を徹底していきたい。

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の比率（関連会社含む）

【ECOM 会員企業】161 社　　【ネット販売事業者】228 社



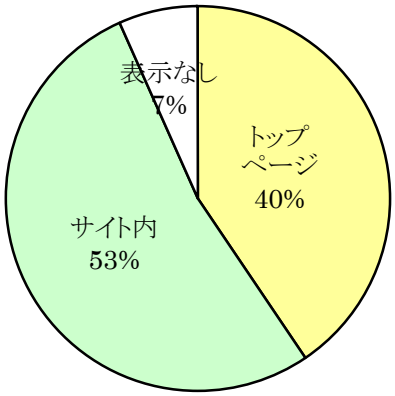


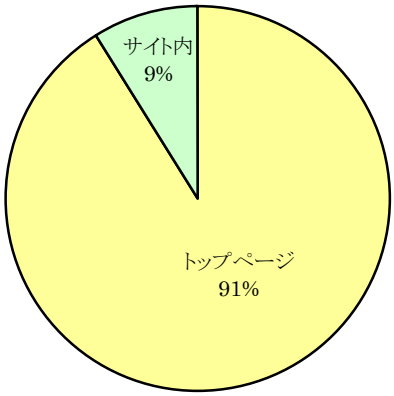
＜調査結果＞

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が取得しており、ネット販売事業者の中でも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ことものと見込まれる。

（2）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の比率

【ECOM 会員企業】89 社　　【ネット販売事業者】34 社





＜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ホームページ掲示は極めて意味がある。トップページにて表示している事業者はネット販売事業者では９１％となっているがＥＣＯＭ会員企業で 40%にとどまっており、ホームページ上に掲載のない事業者も 7%ある。

4. まとめ

ＥＣＯＭ会員の大半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、Ｗｅｂ上での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完備している。しかしながら依然情報漏洩事故が続発している状況において事業者にとって安全管理対策はますます重要になっておりホームページ上でも今後さらに具体的な実施策をアピールしていく必要がある。

ネット販売事業者についてはプライバシーポリシーの新規掲示、記載項目の充実などで、着実に改善が進んでいるが「個人情報保護法に基づく公表事項」掲示などでの点は立ち遅れも見られる。ＢtoＣ事業は依然大幅な市場拡大を続け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のさらなる充実を期待したい。

以　　上

６．　終わりに

もともと個人情報保護法は施行３年後を目途に見直すものと理解していたが、いざ３年を経過してみると基本方針、施行令で若干の修正があるものの「保護法」自体の改正は先送りとなっている。しかしながら一歩巷に出るといまだに「保護法」に関しさまざまな理解（一部には誤解も）と質問に遭遇しまだまだ未熟さを感じることがある。幸い経済産業省では先頃より個人情報の取扱いに関する研究会を発足させ議論を開始しているのでまさに心強い限りである。

一方、国境を越えてわが国を客観的に眺めたときある種の「鎖国状態」を意識することが時としてあるが、国際的な調和という観点からはＡＰＥＣが 2004 年に採択したプライバシー・フレームワークの実証プロジェクトが動き出しており、わが国も参加を表明しているのでこの中で大きな進展が見られるものと期待している。

いずれにせよ、今後も引き続きいろんな場で個人情報取扱ルールが練り上げられていくことになろうが、その中で次世代電子商取引推進協議会（ＥＣＯＭ）も微力ながら貢献できればと考えている。

個人情報保護 WG　メンバーリスト（敬称略）

氏名	会社名（団体名）
（会員）	
廣田　啓一	NTT 情報流通プラットフォーム研究所
上田　英雅	NTT コミュニケーションズ株式会社
寺井　晶子	株式会社 NTT データ
青山　　彰	花王株式会社
保倉　　豊	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
足立　和朗	電気事業連合会
成松　伸之	電気事業連合会
野村　武司	東京電力株式会社
森田　一平	トヨタ自動車株式会社
荒木　吉雄	日本アイ・ビー・エム株式会社
西岡　信佳	株式会社日立情報システムズ
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
再起　和夫	松下電器産業株式会社
山本　　茂	松下電器産業株式会社
岡田　潤之	三菱電機ｲﾝﾌｫﾒｰｼｮﾝﾃｸﾉﾛｼﾞｰ株式会社
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
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）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）
岩田　修	㈱オフィスイワタ
（オブザーバー）	
井川　良	経済産業省
松岡　晃平	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２００７

平成２０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
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。

ISBN978-4-89078-664-0 C2036