ＥＣで取り扱われる個人情報に関する調査報告書（ver.４.0）

～ECOM 個人情報保護ガイドライン改訂と プライバシーマークタスクフォース活動報告～

平成 14 年 3 月

電子商取引推進協議会
個人情報保護 WG

目次

1　はじめに

ＥＣＯＭ、NTT データ経営研究所及び、経済産業省が先ごろ発表した電子商取引市場規模についての共同調査では、2001 年の BtoC 市場規模は 1 兆 4,840 億円となり、2000 年の 8,240 億円に対し、80%の拡大を続けている。1999 年から 2000 年への成長 145%に比べると伸び率は低下したものの今後も引き続き大幅な成長が続くものと考えられ、2006 年には 16 兆円を超え、電子商取引化率も 6%近くに及ぶと見られている。

個人情報保護の分野の動向としては、2001 年 3 月 27 日に内閣で閣議決定し、現在国会での継続審議となっている「個人情報保護法案」について、成立施行後の電子商取引事業者の活動に多大な影響を生じさせると予想されている。もともとリアルの世界に比べてインターネット上では個人情報の収集・利用についてはその取り扱いが容易ではあるが、一方でその個人情報の漏洩についてもその危険性は高いものと一般的に考えられる。したがって事業者はよりハイレベルな収集・利用した個人情報の安全性の管理義務が求められるのは言うまでもない。

例えばインターネット上で収集した個人情報はデータベース化する際にリアルで収集した情報のように再インプットの必要がなく、生データを瞬時のうちに加工できる。さらにインターネット環境そのものがダイレクトで継続的な顧客接点の場であり、インターネットを通じて容易にアンケートやアフターフォローができることから、極めて広範囲で確実な見込み客の情報が収集できるという特徴がある。実際、多くの企業では前述した様々な手法で個人情報を収集して、その他リアルに入手した情報（申込書、商品配送記録等）を統合し、個人のデータベースを作成し、様々なマーケティングやプロモーション活動の基礎データとして活用している。例えば、かつて一度利用したことのあるショップから、ある時、新商品の案内メールなどが送られてきているケースなどは、ほぼこの個人のデータベースが作られていると思われる。つまり、その事業者はその個人の過去の様々な個人情報を蓄積し、特定の個人のデータベースを策定し、嗜好の分析を行ったうえでその個人が買うと予想される商品のセールスを行っているのである。

一方で、個人情報の漏洩について、サーバーに蓄積された個人情報に対して外部からの不正アクセスによるもの、システム上の不具合により外部から閲覧可能になるもの、人為的ミスによるもの（主にメールの誤送信）等が電子商取引特有の事故として考えられるが、悪意のある故意の犯罪を除いて、過失事例も、リアル取引に比べて極めて大量の個人情報が瞬時に漏洩してしまうという危険性を持つといえよう。

このように電子商取引における個人情報は、One to One やＣＲＭといったマーケティング手法には有効且つ必要不可欠なものであると同時に、一瞬にしての大量漏洩・流出の危険性が伴うといった二面性を持つ。企業にとっては今後、電子商取引の市場拡大と共に、益々個人情報を取扱う機会も増えることから、その保護の必要性が求められるのは言うまでもない。

実際、このような動向を受けて、電子商取引を行う企業では、ホームページ上でのプライバシーポリシーの掲示、ＪＩＰＤＥＣ（財団法人　日本情報処理開発協会）が付与認定するプライバシーマークの取得、個人情報保護に関するコンプライアンス・プログラムの策定などの自主的な規制への取組みを始めており、ここに来て個人情報保護に関する意識も急速に高まってきた感がある。

今年度のＥＣＯＭ個人情報保護ワーキンググループでは、まず今後の企業活動に大きな影響を持つ個人情報保護法案の内容を詳しく検討すると共に、個人情報保護に関する企業の様々な自主規制措置の研究や、法案に対して企業がどのような対応をするべきかについて議論を行った。

具体的には､2 ヶ月に 1 回のワーキング会議開催や参加企業ごとの個人情報保護に対する対応を前提とした保護法案の解釈や.P3P およびインターネットにおける個人情報保護関連技術、マーク制度や海外動向、個別法等について調査研究、情報収集、討議検討を有識者および行政担当の方々に加わっていただき、行ってきた。

本報告書ではその中でもＥＣＯＭ個人情報保護ワーキング独自の活動として推進した「『ＥＣＯＭ個人情報保護ガイドライン』改訂の推進」および「プライバシーマークタスクフォース活動」について成果報告書をまとめる。

「ＥＣＯＭ個人情報保護ガイドライン」改訂検討にあっては、アドバイザーとして監修にあたっていただいた中央大学法学部教授（一橋大学名誉教授）堀部政男氏及びニフティ株式会社法務・海外部鈴木正朝氏（前 社団法人情報サービス産業協会　調査役）はじめ 2 度のヒアリングに参加いただいたワーキングメンバーの方々に、また、「プライバシーマークタスクフォース」に積極参加いただいた方々に深く感謝の意を表したい。

また、今年度、本ワーキングに熱心に参加いただいたメンバー全員にもその協力に対し、御礼の意を申し述べたい。

2　ＥＣＯＭ個人情報保護ガイドラインの改訂

2.1　ＥＣＯＭ個人情報保護ガイドライン改訂プロセス

個人情報保護に関する動向では、2001 年 3 月 27 日に内閣で閣議決定し、その後審議に至らぬまま 2002 年通常国会に継続審議となっている「個人情報保護法案」について、成立施行後の電子商取引事業者の活動に多大な影響を生じさせると予想されている。もともとリアルの世界に比べてインターネット上では個人情報を容易に収集・利用できる反面、情報漏洩の危険性は高い。したがって事業者は収集・利用する個人情報について、よりハイレベルな管理および対応が求められる。

一方で、外部からの不正アクセスによる盗難やシステム上の不具合、メールの誤送信といった人為的ミスで外部から閲覧可能になったりするようなネットワーク特有の個人情報漏洩事故も昨今頻発している。実際には、自社社員や委託業者によるデータの持ち出しといった必ずしもネット経由でない個人情報流出の事件例のほうがかなり多いのだが、いずれにしてもそのような状況下、多くの企業が個人情報保護の体制整備に取りかかりつつある。

ＥＣＯＭでは、個人情報保護に対する企業対応の体制構築を早急に進めることが電子商取引やｅビジネスに携わる事業者の緊急のテーマであると考え、他の業界や団体に先んじて、98 年に発表した「個人情報保護ガイドライン ver1.0」の改訂作業に取りかかることとした。

2.1.1　基本的な考え方

先の「個人情報保護ガイドライン ver1.0」は、1997 年に示された当時の通商産業省「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」をベースとし、とりわけ電子商取引の切り口で適切に個人情報の取扱がなされることを目的に策定された。

改訂にあたっては、当然ながら個人情報保護法案に対応することを念頭に置き、近年のネットワーク･情報通信関連の環境変化も考慮しつつ、広く個人情報を取り扱う企業・事業者に適用されることを目指した。

2.1.2　改訂作業のプロセス

基本的な改訂作業についてはＥＣＯＭ個人情報保護ワーキング担当の研究員に委ねていただき、9 月より改訂検討の作業を開始した。

9 月及び 10 月にワーキング参加社の中より 6 名のメンバーの方にヒアリングを行い、また、第４回のワーキング会議（2001 年 11 月開催）にて中間整理案を提示し、メンバーより意見を募った。そして中央大学堀部政男教授をはじめとした有識者の監修を経て、本年度末（2002 年 3 月末）にて完成させるスケジュールにて取り組んだ。

2.1.3　検討のポイント

まず、第一に個人情報保護法案への対応がポイントとなるが、その他以下に記す項目についてヒアリングメンバーおよび有識者を交え検討を重ねた。

1. 個人情報保護法案との整合性
   - (1)　基本５原則
   - (2)　個人情報取扱事業者の義務
   - (3)　例外規程（目的外利用、第三者提供等）
   - (4)　オプトアウトの扱い
   - (5)　苦情処理
   - (6)　全体構成
2. ＥＣ環境との整合性 (例)
   - (1)　プライバシーポリシー、プライバシーマーク、コンプライアンス・プログラムへの言及
   - (2)　新たなビジネスモデルやインターネット技術（クリックアンドモルタル、モバイル等）に対する対応
   - (3)　子ども、高齢者保護
3. JIS Q 15001 との整合性
4. スケジュール及び検討のプロセス
   - (1)　ＷＧ全体ヒアリングの方法
   - (2)　有識者チェックの方法
   - (3)　完成後の公開方法

2.1.4　改訂の基本指針決定

2001年9月4日に第１回目のヒアリングを実施し、改訂の基本部分となる点について議論し、以下の骨子に従い改訂作業を進めることとした。

1. ガイドラインの目的の明確化

   本ガイドラインは主としてＥＣ事業者全般を対象とし、自主的･自律的に個人情報の保護を実施する上での、自社の内規やコンプライアンス・プログラムを策定する際のベースとなるよう策定する。

2. 法案・JIS Q 15001 との関連

   法案の内容は企業が守るべき基本的なレベルであり、一方 JIS の要求事項は中小の事業者にはハードルが高い所があるが、教育や監査など取り入れるべきところもある。したがって、法案への適合を図りつつも、JIS Q 15001 についても部分的に取り入れる。

3. ガイドラインの構成

   ＥＣ事業者が個人情報保護法の施行に対応して自主的に内規やコンプライアンス・プログラム策定する上で参考にしやすいように、本ガイドラインも法案の流れに沿ったものとなるよう構成する。

4. 平易性

   用語や定義については、法案との整合性を踏まえつつ、ＥＣ事業者にとって平易でわかりやすい表現・文章で表現する。

5. ガイドライン適用範囲

   主として実際に個人情報が取り扱われる殆どのケースである BtoC での個人情報保護にフォーカスを当て、BtoB については必要性があれば補完的に検討していく。

6. ガイドラインのレベル

   「あるべき論」を優先させ、要求の高いレベルのものを作っても、実際に取り入れにくいものとなるので、ミニマムスタンダードである法案をクリアするレベルで考える。

7. 正確性の確保について

   従来のガイドラインでは正確性について十分に表されていないので、更に具体的な表記を考える。

2.1.5　ガイドライン本文改訂検討

さらに 2001 年 10 月 29 日に第２回目のヒアリングを開催、その間に事務局にて策定した素案についてそれぞれの条項ごとに意見を出し合い、細部の論点について論議した。

1. 本人からの申出に関する措置について

   「個人情報保護ガイドライン ver1.0」では、ＥＵ等の国際的な議論を考え、自己情報に関する本人の権利との視点から、消費者側に立った表現であったが、本ガイドラインはＥＣ事業者を主たる対象と考え、本文では事業者の義務として表現し、解説にて本人の自己情報コントロール権について触れることとした。
2. 法案の例外規程について

   法案 28 条にある第三者提供の制限についての例外規定に関して、素案では一部削除する形で提案されたが、基本的には法案に示されるとおりにガイドラインにすべての例外規定を表すべきであるとした。
3. 目的の表記について

   ＥＣ事業者が自社の内規やコンプライアンス・プログラムを策定する為のものであることが読み取れるよう明確に表す。
4. 本文は解説とのバランスを取りつつ、簡潔且つ具体的に表す。
5. こどもの定義

   取扱う商品等によって異なるので何歳以下という定義は難しい。
6. 公知情報（不特定多数に公開された情報）の収集について

   利用目的等の要件明示について必要とされていない例外扱いになっている状態）では法案よりレベルが下がるのではないか？きっちり整理する必要あり。

   ・・・他

以上の議論を踏まえて、事務局が中間整理案を策定、11 月 22 日の第４回ワーキンググループ会議にてメンバーに提示した。

2.1.6　今年度の結論

その後、中間整理案についてのメンバー企業からの意見をいただき、事務局にて推敲を

重ね、更には有識者から助言を受けつつ修正案を策定し、2002 年 3 月 18 日に有識者・関係行政担当および事務局にて検討した結果、以下のように方向づけた。

1. 法案の流れに沿った順序での記述の方がわかりやすいのではないか。また、法案以上のレベルの要求については、明確に区別してわかるように表記し、それぞれに主旨及び解説を加える形に改善を加える。
2. 表記については、法律のような条文形式にこだわることはない。
3. 現時点(2002 年 3 月現在)では、個人情報保護法案については本通常国会で継続審議となっている状態であるので、その動向に注目しつつ、リリースのタイミングについても十分に配慮したい。
4. リリース後の他のガイドライン等への影響も考慮し、法案と異なる基準を設定する部分についてはさらに議論を深める。

さらに、3 月 22 日の第 6 回ワーキンググループでその修正案を中間整理案 No.2 として提示をし、再度ワーキングメンバーの意見を諮ったところ以下のような意見が寄せられた。

1. この中間整理案 No.2 については、個別の条項に関してまだ解釈の根拠の不明確な点が存在する。したがって、検討の経過報告としても現段階で公表することについては、他業界のガイドラインへの影響や外部が引用することなどについても十分に配慮し、慎重な対応を図るべきである。
2. 本人からの個人情報の収集について、法案とのレベルの整合を鑑みた場合、「同意」とするか、「通知または公表」とすべきかの論点がある。
3. ガイドラインとしての法案と JIS との位置付けについて明確にすべきである。

以上の経緯にて結果的に当初の予定を変更することとした。すなわち、最終的なＥＣＯＭ個人情報保護ガイドライン(ver2.0)については、法案審議の動向を追いつつ、来年度前半に照準を定め更に精査と編集を重ねることとした。

3　プライバシーマークタスクフォース活動報告

3.1　プライバシーマークの機能的意義

プライバシーマーク制度とはインターネットを利用した消費者向けの電子商取引において、適切な個人情報の保護を行う事業者を認定して、その旨を示すプライバシーマークを付与し、電子商取引に関する事業活動に関して使用を認める制度である。財団法人日本情報処理開発協会（ＪＩＰＤＥＣ）では経済省ガイドラインに基づく業界ガイドラインやＪＩＳの個人情報保護コンプライアンスプログラムに準拠し、個人情報の取扱について適切な保護措置を講ずる体制を整備している事業者等に対してプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を容認するプライバシーマーク制度を1998年から開始しており、2002年2月末現在約300の事業者がプライバシーマークの認定を受けている。

また今年6月から米国のBBBOnLineと呼ばれる、米国やカナダの消費者を対象にしてインターネットで業務を行う事業者がある一定の個人情報の規則を満たす場合に付与するプログラムと間での相互承認制度も開始した。

3.2　プライバシーマークタスクフォースの活動

3.2.1　活動主旨

電子商取引推進協議会（ＥＣＯＭ）の個人情報保護ワーキングでは、「プライバシーマークタスクフォース」を立ち上げ、企業が個人情報保護を実践するにあたり、プライバシーマークの取得及び運用することによる効果や課題について検討と演習を行った。当初の活動計画は以下のとおりである。

1. 主旨

   基本法法制化の動きに伴い、事業者の個人情報保護に対する意識と姿勢については更に高いレベルのものが要求され、企業（事業者）の対応策のひとつに「プライバシーマーク制度」の活用という方法がある。

   個人情報を取り扱うにあたり、適切な保護を実施していることの証となる「プライバシーマーク」について理解を深め、同制度を正しく運用することによって得られるメリットや効果・留意点等を検証・分析する主旨にて「プライバシーマークタスクフォ

ース」を推進する。

2. 具体的テーマ

（1） プライバシーマーク制度の理解・・・効果と運用・活用・留意事項

（2） コンプライアンスプログラムの策定について

（3） 各種マーク制度の比較・分析

（4） プライバシーマーク取得の手順研究と実践方法 ・・・・・等

3. 活動期間

９月下旬～１２月末（全 5‐6 回の検討会の実施および調査を行う）

4. 参加資格

個人情報保護WGメンバーおよび代理

3.2.2 参加および活動

個人情報保護ワーキング参加メンバー30 名のうち、14 名が同タスクフォースに参加、3 チームに分かれ以下テーマに関して活動することとした。

1. Aチーム

・テーマ：プライバシーマークの効用と留意事項

・具体的推進：Pマーク取得主要企業インタビュー

・参加者：4 名

2. B チーム

・テーマ：各国のプライバシー保護・他マーク制度調査

・具体的推進：各国のプライバシー保護制度・マーク制度整理（文献整理）

・参加者：2 名

3. C チーム

・テーマ：コンプライアンスプログラムの策定

・具体的推進：コンプライアンス・プログラムの要件・各社のコンプライアンス･プログラム整理・検討

・参加者：8 名

■プライバシーマークタスクフォース参加者名簿（敬称・役職略、企業名 50 音順）

委員　西尾　美和　沖電気工業株式会社

委員　沢辺　茂樹　株式会社ダイエーオーエムシー

委員　鈴木　　靖　大日本印刷株式会社

委員　高田　荘治　電気事業連合会

委員　祝　　壮吉　東京電力株式会社

委員　脇田　正敏　トヨタ自動車株式会社

委員　荒木　吉雄　日本アイビーエム株式会社

委員　石田　文治　日本電気株式会社

委員　阪上　正博　日本ユニシス株式会社

委員　立仙　和巳　株式会社日立製作所

委員　東山　治郎　松下電器産業株式会社

委員　伊東　正晴　三井住友海上火災保険株式会社

委員　吉田　久志　三菱電機インフォメーションテクノロジー株式会社

委員　染谷　信年　安田火災海上保険株式会社

● ECOM　事務局

事務局　植原総一郎　　電子商取引推進協議会

事務局　浅沼　省吾　　電子商取引推進協議会

3.3　プライバシーマークタスクフォースＡチームの活動　～プライバシーマークを取得企業へのインタビュー～

A チームでは、プライバシーマークの効用と留意事項を具体的に把握する目的で、実際にプライバシーマークを既に取得している各業界の企業に対しインタビューを実施した。

3.3.1　インタビューの目的

今後、プライバシーマークを取得するということは、企業の自主的な個人情報保護の取組みとして、消費者や取引先から社会的に信頼を得るためにも不可欠なものとなっていくことと予想される。そこで既にプライバシーマークを取得されている企業の取組みについてインタビューすることにより、先進的な取組みの事例としてベンチマークする。

インタビューのポイントは、大きくは以下の３点となる。

- プライバシーマークを取得することによるメリットについて
- プライバシーマーク取得に関しての社内的な取り纏めの苦労について
- プライバシーマーク取得までの社内体制整備について

3.3.2　インタビュー項目

インタビューは上記の３つのポイントを踏まえて、さらに具体的な取組みについてヒアリングを行った。ただし、基本的にそれぞれの企業担当者にはマークの取得について、フリーに話してもらっており、一問一答形式ではないことから、下記の項目について必ずしも明確に回答されてない場合もある。

1. プライバシーマークを取得することによるメリットについて
    - 取得の動機はなにか？
    - 経営上のメリットはあるか？
    - 事業上のメリットはあるか？
    - 逆にリスクの検討は行ったか？
    - コストの検討は行ったか？等
2. プライバシーマーク取得に関しての社内的な取り纏めの苦労について
    - トップダウンｏｒボトムアップのどちらで推進したか？
    - 社内啓蒙はどのように行ったか？
    - 現場の反応はどうだったか？等
3. プライバシーマーク取得までの社内体制整備について
    - コンプライアンス･プログラム構築体制（組織、期間、人材）はどうなっているか？
    - コンプライアンス･プログラム実施体制（収集、利用、提供、安全性、正確性、教育、監査）はどうなっていたか？
    - 委託先との関係はどうなっていたか？
    - ＥＣ分野での取組みはあるか？
    - 他の認定（ＩＳＯなど）は取得されているか？
    - 今後の予定はどうなっているか？等

3.3.3　ウイルソン・ラーニング・ワールドワイド株式会社

●面談者：事業推進部 次長　吉森　光則　様

●実施日：2001 年 11 月 12 日（月）

1. プライバシーマークを取得することのメリットについて

(1) 取得の動機

お客様から、プライバシーマークをとっているかとの問合せや、とって欲しいとの要求も多くなってきて、お客様からの要望に応えるためである。

(2) 経営上・事業上のメリット

当然、事業機会の増大を図ることである。副次的な効果として社内業務のマネジメントの改善が挙げられる。個人情報にかかわる部署は当然だが、個人情報と関係のない業務部署のメンバーでも、個人情報に対する意識が高まってきた。

(3) 直接･間接コストについて

ビジネスだから、コストに合わなければやらない。コストを上回る事業収益を目指している。

2. プライバシーマーク取得までの社内推進について

(1) 進め方について

トップダウンで進めた。一般社員からすると日常業務の他に余計なことをやりなさいということだから、トップダウンでないと動かないと思う。

(2) 取得までの経緯

昨年 10 月頃から準備をスタートさせ、講演会に出席したり、取得されている会社にヒアリングに伺いながら、アウトラインを掴む作業をした。

12 月に本格的にプロジェクトをスタートさせ、実際に動き出したのは今年の 2 月頃からである。

4 月に全社キックオフを開催して、全社にプライバシーマーク取得の意義を説明した。

5 月 10 日に申請書を提出し、7 月 25 日に正式に取得できた。コンサルにも入ってもらい、極めて短期間であったが集中して取組んだと思う。

(3) 社内の推進体制

事務局は、他の仕事があるので兼任で 2～3 人位である。今でも、私は他の仕事と

兼任でプライバシーマーク運用事務局をやっている。

(4) 社内啓蒙･教育の取組み

4 月の全社キックオフの場で資料を配った。相当厚い資料だったが、目方で「こういう重いものなんだよ」と肌で感じてもらおうとした。これで全社メンバーへのプライバシーマーク教育をやったというわけである。

その後、各部門毎に業務マニュアルを作った。それから、業務の対象者を集めて業務マニュアルに沿って、具体的にやることに関して、真剣に勉強会を行った。

(5) 現場の反応について

全社キックオフの演出が成功したと思う。コンプライアンス・プログラムの運用初動において、トップダウンのかたちで、強制権を発動したということが上手くいった要因だと思う。

3. プライバシーマーク取得後の運用について

(1) 社員の個人情報と社外（お客様）の個人情報の取扱について

社員の個人情報（インハウス情報）は、コンプライアンスの中に入れていない。人事部が従来の管理規定でしっかりと運用しているので、外に出る可能性は 100%ないという認識である。今回対象としたのは、お客様の個人情報の取扱についてどうするかである。社外から入ってくる個人情報について、全社的にどう取り扱うかということをまとめたのである。

(2) ｅラーニング（Web）の活用について

現在は、今回のプログラムの改廃等について Web でやっている。ペーパーは最初のみである。重みを身体で感じてもらうために配ったが、その後ペーパーは一度も配っていない。改廃は、全部 Web で広報している。改廃したコンプライアンス・プログラムがアップロードしてある URL をメールで全メンバーへ告知している。それをダウンロードしてもらっている。

(3) 業務の委託先（外注先）への対応について

委託先にも JIS に準拠した、個人情報の取扱に対する安全性の高いルールを社内に設けてもらっている。その基準に適応したところにのみお願いするというルールを決めている。社内で委託業者選択基準チェックシートというものをつくり、それをクリアしてもらうようにしたのである。委託先で実行して頂いているものと信じている。そのチェックは、当該業務の実施責任者にお願いしている。

(4) 電子商取引で個人情報の問題で注意されていること

当社のビジネスは B to B のパターンが主である。B to C のパターンは今はほとんどない。今後は B to C のパターンが加わってくる可能性が充分にあるので、ＥＣの取組みが当然出てくると思っている。

(5) プライバシーマーク取得で、会社としてＰＲできること

当社の事業は大きく分けて　１)人材採用事業、２)人材教育事業　の２つです。いずれの事業も個人情報を取り扱うことになる。当社のコンプライアンス・プログラムを全社で運営することにより、個人情報の取扱に関して全社員がしっかりした取り組みを実施しなければならない。このことにより、社会的信頼を得るに足る事業運営の実現が可能になる。プライバシーマーク取得に関して対外的にアピール出来ることは当社にとって大きな意味を持つものである。

3.3.4　テプコシステムズ株式会社

●面談者：企画部 課長　中道 卓志 様、企画部 主任　由井 ルミ 様

●実施日：2001 年 11 月 20 日（火）

株式会社テプコシステムズは、旧東電コンピュータサービス株式会社（TCS）と旧東電ソフトウェア株式会社（TSI）が 2001 年 10 月に合併して設立されました。

両社とも合併以前に、プライバシーマークを取得されております。

旧東電コンピュータサービス株式会社（TCS）＝中道 卓志 様

旧東電ソフトウェア株式会社（TSI）　　＝由井 ルミ 様

1. プライバシーマークの取得について

(1) 取得の動機

（TCS、TSI）

「東電からの新規業務の受託に当たってはあったほうが良い」「新しいお客様の開拓には必要だ」という考えから、トップダウンで取得へ向けて動き出した。

(2) 経営上・事業上のメリット

（TCS）

東京電力以外のお客様からの仕事を受注する、或いは、自治体などからの仕事を受注する上で信頼を得るための手段として有効であることと、企業の認知度を上げるために、資格は重要であると考えた。

それと、当社は情報関連の会社であり、お客様のデータ（個人情報）を取り扱う業務に携わっているので、社員の意識向上のためにも取得しようと考えた。

2. プライバシーマーク取得に向けての社内推進について

(1) 進め方について

（TCS）

各ライン部長級以上に対しては、取得を目指すことを決めた時点で「今度、こういう制度に取組む。こういう体制案を作って、こういう条件整備事項があります」と伝え、コンプライアンス・プログラムを運営していくために必要な体制の整備を、各ラインに依頼した。

コンプライアンス・プログラムは、私が担当して全部作った。ワーキングを立ち上げて関係者を集めてやっていこうかとも思い社長にも相談したが、「こういうものはある程度雛型を誰かが作って、それを関係者に周知承認させるやり方のほうが早いだろう」と言うことで、私が作ったわけである。

雛型を作り、コンプライアンス・プログラム本体で規定すべきことはここまで。細かい電子媒体の管理やコンピュータ処理上の管理等は、各業務部門で作っているマニュアルに記載するという形で進めた。

（TSI）

関係する部署の責任者を集めて何度か打合せを実施し、体制および責任者、今後の進め方を決定した。実際に現場では、受託業務に関するシステム開発・保守業務における個人情報の取り扱いに関し、ワーキングで検討されていたので、そのワーキングと連動して社内全体に広がっていった。現場としては、プライバシーマーク取得というよりも、現在担務している業務に関するデータを、どのように扱うかといったことと同レベルで、インハウスの個人情報についても対象として考えるといった感じで進んでいった。

(2) 取得までの経緯

（TCS）

実際に申請をする時には、お客様対応窓口責任者・教育担当責任者や役員など、それぞれ役割分担を決めた。7 月にスタートして、9 月にたたき台を作って、ＪＩＳＡ（社団法人情報サービス産業協会）に相談に行って、12 月に作り直して持っていった。その時には、JIS Q 15001 の対応があるということでコンプライアンス・プ

ログラムをＪＩＳ対応したほうが良いと助言され、２～３点ご指摘を頂いて直した。

そして、年明けにもう一度内容を見ていただいて、基本的にはそのまま受理していただいたということである。

７月に本格的に検討を始めて、2 月に取れたということである。半年強である。

（TSI）

ＪＩＳＡの主催する説明会には参加したが、当初コンプライアンス・プログラムとは何か・どういうものかということが分からなかった。ＴＣＳで実際に作ったものを見せてもらい、とても参考になった。両社とも、データをどのように扱うかといった考え方は基本的に近いので、ＴＳＩへ適用させるためには若干の変更で済んだ。年末に教えてもらって、3 月の末にＪＩＳＡに申請の相談に行ったのだが、マニュアル不足の指摘を受けた。WGで、システム開発・保守に関する個人情報取扱いマニュアルが 4 月に出来上がる予定だったので、マニュアルが整備されてから、4 月の時点で再度申請し、受理していただいた。

(3) 社内啓蒙・教育について

（TCS）

どうやって社員(約 1100 名)まで周知させるかということがネックだった。まず、イントラネットでこういうマークを取得したと告知したのである。社員からみると当制度を一番身近に感じたのは、名刺にマークをつけたことである。マークの入った名刺を配れば「このマークはなんですか」と聞かれるから、この制度が分かっていなければ困るわけである。社員向けに説明会を何度か開いた。

社員教育では、ＷＢＴ（Web Based Training）を作り 一問一答式の問題を 100 問ほど作った。それも、管理者向けの問題と一般社員向けの問題に分けて、全員に受けさせたのである。これは 5 問～10 問位で一つのステップをつくり、一つめのステップをクリアしないと次のステップに行けない形にした。また、人事からこの部署は誰がどこまで行っているということが見えるようにした。3 ヶ月～半年位で全社員が 100%終了している状態を目指したのである。

（TSI）

1 年目は啓蒙の意味もあり、2～3 日かけて何度か集合研修を行った。2 年目からは、各人が業務スケジュールに合わせ、自席で行えるようにするために、ＷＢＴを使用した。また、社外の方から「プライバシーマークとは何か？」という問いに対

して回答できるよう、Q＆A集をイントラに載せるなどの整備を行った。あとは、名刺にマークを刷る（社外へのＰＲもあるが）ことにより、社員に意識してもらうようにした。

(4) プライバシーポリシー（方針）について

（TCS）

コンプライアンス・プログラムの規定に、基本方針という条項がある。それがポリシーだろうと思う。社内の規定ルールでは、規則とマニュアルというものがある。コンプライアンス・プログラムを社内規定の体系にあわせると、規則になるのかマニュアルになるのか、それよりも上のレベルになるのかという議論があった。当社では、規則よりも一つ上の段階でコンプライアンス・プログラムが位置付けされるような体系としたのである。

(5) 社内の推進で必要と思われる部門は？

（TCS）

コンプライアンス・プログラムの雛形策定にあたっては、プロジェクトを作らなかっただが、ワーキングやプロジェクトを作るとすれば、まず法務に強いメンバーの参画が必要と考える。業務を受注する時や委託先との契約書の問題など、考慮すべき範囲が広いためである。

さらに、１つの会社でも個人情報の扱い方が業務によって違うので、現場の担当責任者に入ってもらうことである。また、社内ネットワークを管理している部門も必要である。

あとは、トップダウンということで役員クラスの人に入ってもらわないとなかなか進まないと思う。この点では、雛形策定にあたってワーキングやプロジェクトを作らなかったので、個別に担当者をつかまえて確認するといった苦労があった。

ワーキングを作るかどうかは、会社の規模によると思う。ある程度小規模の会社だと、責任者が集まったほうが、社内の啓蒙の手間も省けるので早いと思う。

3. プライバシーマーク取得後の運用について

(1) 業務の委託先（外注）への対応について

（TCS）

個人情報保護についての条文を記載した契約書の雛形を用意した。委託先企業に対してプライバシーマークを取得することまでは義務づけできないので、「社内で

個人情報保護をきちんとやってください。当社の規定に準拠したルールを徹底してください」と指示を出した。契約書の中に個人情報保護の条文を記載することで、最低限のガードをかけたのである。

（TSI）

ＴＣＳと同じように、契約書に入れた。また、委託先責任者の定例の連絡会を利用して、「当社では、個人情報の取扱いをこのように決めましたので、同じような形で個人情報を扱って下さい。」といったような説明を行った。また、駐在者にも社員と同じ研修を受けられるようにした。

(2) 社内（インハウス）の個人情報の取扱いについて

（TCS）

インハウスの情報がプライバシーマークを取ったことによって社内的にどれだけ強化されたかということについては、なかなかそこまでは未だ見えていない。啓蒙活動的には強化されたと思う。昔は社員名簿を冊子で出していたのだが、今回廃止にした。コストの問題もあるが、社員名簿を紙で配るのは廃棄する場合の管理までは徹底できないことから廃止した。

(3) 監査について

（TCS）

内部監査である。企画部門は受託部門と離れていることもあるので、企画部門が監査員ということでスタートした。実際に監査のレベルが分からなかったので、ＩＳＯの監査マニュアル等を参考にして進めた。

（TSI）

システムの品質向上やCMM（Capability Maturity Model）、ＩＳＯ等を推進する「品質管理部門」において、監査の方法や規定を作って実施した。

(4) 今後の継続について

（TCS）

せっかく取得したものであるから、継続できるのであれば継続していきたいと思う。経営的にも、こういった制度は維持していくべきだと思っている。

4. 今後のプライバシーマーク制度の改善要望について

（TCS）

マークを取得してビジネス上で有利ということはあまりない。要望ではないが、プライバシーマークを取っていないと、中央官庁のシステム開発等で入札ができないというような仕組みが早くできればと思う。

ただ、会社のパンフレット等にマークを掲載することによって「個人情報保護を徹底的に管理している会社」という印象を持って頂けるという効果は上がっているだろうと感じている。

3.3.5 株式会社ＤＮＰデジタルコム

●面談者 株式会社**ＤＮＰ**デジタルコム 制作本部 本部長　　斉藤　雅　様
株式会社ＤＮＰデジタルコム システム開発室 室長　岡 謙太郎 様
大日本印刷株式会社 技術本部 次長　　佐藤 光男 様
大日本印刷株式会社 Ｃ＆Ｉ総合企画開発本部　　舟橋 香樹 様

●実施日：2001 年 11 月 30 日（金）

1. **プライバシーマークの認証登録について**

(1) **プライバシーマークの認証登録の動機**

ＤＮＰデジタルコム社の親会社は印刷会社なので、個人情報を保護する以前に、お得意先企業からお預かりした原稿類を、大切に保管してお返しするということが基盤としてある。しかし媒体や技術が変わり、個人情報の保護が極めて重要となってきた時代背景のなかで、それを意識的に保護するということを、社員に対しては勿論、社外に対しても示すことが必要だとの経営判断もあり、デジタルコム社としてプライバシーマークの認証登録を検討するということが始った。大日本印刷・DNP の本社に個人情報保護に関する事務局が設置されるなど、いろいろな面でバックアップ体制が出来ていたことも大きかったと思いう。

(2) **認証登録のメリットについて**

社員が全社一丸となって個人情報を大切に扱うという意識を高めるのに、こうした制度にチャレンジすることは非常にメリットがある。

また、私どもはそれぞれのお得意先企業が抱えている個々のご要望にお応えするために、あらゆるメディアを開発、制作しているので、私どもが取り扱う個人情報は、ほとんどがお客様から預託していただいたものである。その意味では、プライ

バシーマークの認証によって、お得意先企業に安心して仕事を出していただけるという点に大きなメリットを期待していた。

(3) 直接・間接コストについて

3 年前から検討に入り、基礎的な調査で 5 ヶ月位かかった。元々、原稿を大切に扱うという文化があったので、新たに新しいものをゼロから作るという考えはなかったし、実態もそうだったと思う。

お得意先からお預かりしたデータを安全に守りながら製造する過程としては、セキュリティ対策の一環だから、特別に直接的な費用がかかったいう意識はない。

但し、社員教育の面では、ハンドブック等の制作や研修といった間接コストは当然かかっている。もちろん最初から教育は一番大切だと想定していたので、本社の研修部が運用する「ネットワークを使って研修を受ける仕組み(ネットワークラーニング)」を利用して「個人情報保護－基礎編」の研修を行い大幅なコストダウンを図るなど、いろいろと工夫もしてきている。

2. プライバシーマーク認証登録までの社内推進について

(1) 進め方について

数人で最初の調査を行った後、マーク認証登録のためのプロジェクトを発足させ、継続した調査と共にコンプライアンス・プログラムをどう作るかということを、各部門代表のプロジェクトで取組んだ。プロジェクトのメンバーには、技術スタッフや総務系の人も入れた。オブザーバーとして、本社からシステム監査経験者にも入ってもらい、全体的としては約１５名弱で、半年間かかった。

当時、ISO9000 のプロジェクトも並行して進めていた。9000 の場合は、全社対象ではなく、ある特定の部署だが、そこでやっているメンバーとは、特に監査とか書類の作り方について、お互いに交流して高めていったという経緯がある。

(2) コンプライアンス・プログラム策定に当たってのご苦労について

本社の事務局が関連規定の棚卸しを実施、DNP グループ全体にかかる個人情報保護規程とガイドラインを制定した。個人情報保護規程は全社員適用で、ガイドラインは営業活動で個人情報を取り扱う部門を対象にしている。各部門がガイドラインに従って作業を進めるとコンプライアンス・プログラムがまとまるような内容になっている。

「てにをは」も含めて、変なルールを作ると、あっちの規定に引っかかったり、

こっちの規定に引っかかるということもあるので、半年ぐらい時間をかけた。議論の中では、JIS の要求事項と既存の内部ルールとの整合性に苦労した。

ただ、パワー的な苦労はあったが、すっきりさせる良い機会だったと思う。デジタルコム社の個人情報保護規程もそうだが、個人情報を取り扱う DNP のグループ会社は、この全社規程とガイドラインを参考にしつつ、各社の業務内容にあわせて個別に規程を制定している。

(3) 社内啓蒙について

デジタルコム社としては、プライバシーマーク認証登録までの間にも、作成したコンプライアンス・プログラムについて、社員全員に教育をした。特に管理職向けには、いろいろな定例会議の場を利用して啓蒙した。

本社の事務局は、DNP グループ全体を対象に、個人情報保護の必要性を説くと同時に、各部門やグループ会社のルール制定にあたってのガイドラインや上位規程の説明をして、それぞれに内部規定を作ってもらう動きになりますよという予告も行った。

その際に作成した資料は、その後、再編集して、導入教育「入門編」の共通教材として使っている。そんな形で少しずつ浸透を図っていった。

(4) 現場の反応について

前述のとおり、私どもはもともと印刷におけるセキュリティ管理が要求されていた。例えば、新車のカタログなどでは発表されるまで絶対に外部に漏れてはいけないし、チラシであればセールの開始前に外部に出たら、他店に値段が分かってしまうわけである。当然ながら、企業機密上の管理規程として、外部者立入り制限に関する規程等もあって、セキュリティ管理の考え方は定着していた。

ですから、当社の文化からすると、そう違和感はなかったと思う。特にトップからの強い指導もあったので、社員の認識は比較的高かったと思う。

3. プライバシーマーク認証登録後の運用について

(1) 社員教育について

イントラネットを使ったネットワークラーニングがベースになっている。「個人情報保護－基礎編」が DNP グループ全体の共通研修となっており、デジタルコム社でも全員が受講した。このシステムでは進み具合がリアルタイムで分かる仕組みになっていて、進捗状況に応じて、研修部から本人にメールが来るようになってい

る。今後、この仕組みに新しいコンテンツを加え、グループ全体への継続的な教育を行っていく予定である。

さらに、グループ全体での教育プログラムとは別に、デジタルコム独自のカリキュラムもある。その中にも経営者向け、管理者向け、それぞれの職場向けといった、階層や職種ごとに異なる内容で実施している。

(2) 社員の個人情報と社外（お客様）の個人情報の取扱いについて

社員の個人情報は、個人情報保護規程ではなく、総務・人事部門が別のルールで管理している。ただ、プライバシーマークの認証審査には、当然 社員等の個人情報（総務部門）も対象になるので、それを加えた。

(3) 委託先への対応について

協力会社（外部委託先）への委託を直接担当する部門では、一般的な取引契約を締結しているが、個人情報を預託する可能性のある協力会社に対しては、本社の法務部が作成した「個人情報保護に関する契約」を締結することが定められている。もちろん、それ以前に、業務上の安全性を確保するための「委託先選定基準」があり、少なくとも協力会社との取り引き開始時にはそれに従ってチェックし、以後、少なくとも年に一度は継続的にチェックすることを義務付けている。

派遣社員については、派遣会社との契約の中で個人情報保護も含めたものを用意している。これはいろいろなパターンが考えられるので、それぞれ雛型を用意している。

(4) 監査について

当社では定期的に内部監査を行っており、外部監査は今後の課題と捉えている。ただ、最近では、本社及びグループ会社間の相互協力により、別組織のオブザーバー参加という形で公正性を確保するという試みを行っている。

(5) プライバシーマークのＰＲについて

販促用のパンフレットで、「当社はこういうポリシーで個人情報保護を行っている。」というものを作っており、それにプライバシーマークを掲示している。また、提案書の中にも一部、マークを使用して、プライバシーマーク制度そのものの説明も入れている。もちろんデジタルコム社のホームページには、当社の「個人情報保護に関するポリシー」を掲げている。

(6) グループ全体での今後の取組みについて

DNP グループ全体を、事業部及び製造・工程会社などの事業部門に分類して、部門及び会社ごとに、それぞれプライバシーマーク認証登録レベルのマネジメントシステムを構築する活動を続けている。

ただ、部門や会社としてプライバシーマークを申請するかしないかは、それぞれトップが判断することにしている。

4. プライバシーマーク制度に対する要望について

１つは、ISMS のパイロット認証（とＢＳ７７９９の認証）制度が動き始めているが、国民や企業に安心をさせるための制度であれば、是非、横の連絡をとって頂いて、全体のセキュリティレベルを上げるような制度の運用・維持をしていただきたい。相互認証という形ではなくても、上手くラップできるような形の運用の仕方なりをしていただきたい。情報セキュリティマネジメントシステムを生活者に分かりやすい形で見せていただきたいということである。一番大事なのはシステムが安全だということを第三者が認めて、それを使う人たちに対して、「安心して使える、期待を裏切らない仕組みの維持ができている会社だ」と証明できる制度にして欲しいと思う。

２つめは、マネジメント単位で認証を付与したのであれば、他部門のことは別の問題という形で考えいただけないかということである。マークの運用基準については、非常に厳しく制限されており、問題はないように思う。DNP グループは事業も多岐にわたり、社員は 35000 人、電子部品を作っている事業部やプリンタのリボンを作っている事業部もある。そこで、部門別、会社毎にコンプライアンス・プログラムを作ろうとしているわけであるが、マーク認証された部門以外でうっかりミスをしてしまった場合に、その法人全部を罰して、それが本当に意味があるのことなのだろうか、と思う。

３つめは、マークの取り消しというリスクを背負う感があることである。審査機関の負担は大きいと思うが、マークの実効性を高めるためには、２年に１回の更新審査だけでよいのかという気持ちもある。私どものお得意先企業からも、プライバシーマークに関するお問合せや、コンプライアンス・プログラム策定サポートのご依頼を受けることが増えてきて、制度運営に関する情報公開も一層重要になってきていると思う。また、プライバシーマーク制度だけの問題ではないが、ＩＳＯなど各種の認証を取得した部門や会社にとって、それぞれの審査・監査費用など、維持

していくための費用負担が大きいと思う。今後、各制度が連動、連携するようなことで企業の負担を軽減できる余地がないか、ぜひ工夫していただければと思う。

3.3.6　第一生命情報システム株式会社

●面談者：経営企画本部長　甲斐 啓之　　様
　　経営企画本部　　鎌野 與志治　様
　　経営企画本部　　小谷 宏　　様

●実施日：2001 年 11 月 27 日（火）

1. プライバシーマークの取得について

(1) 取得の動機

当社は、データ保護が命という業態である。データ保護については、社内で様々な対策に取組んできた。ただそれで完全というわけではなく、各種取組みの中で、統一的な目標みたいなものがあれば、それが求心力になる。また、一生懸命頑張っていることを、社外の方にも認めていただけるような証しの一つとなるのではないかと思っていた。

あくまでも我々が今まで取組んできたことを形にして、認めて頂こうということと、今後 会社としてセールスポイントになるだろうと思い取得に踏み切った。

(2) 商売上のメリットについて

当社は、お客様のデータが中心なので、それをより安全にという経営上の問題が主である。今は見えにくいが、外販業務において当社の個人情報保護の姿勢がアピールすることが今後考えらる。

(3) 問題点について

取得したことがスタートだと思っている。今のレベルで十分だとは思っておらず、弱い所についてもう少し補強していきたいと思っている。

いかにして個人情報保護を継続し、取り組んでいけるかが課題だと思う。

2. プライバシーマーク取得までの社内推進について

(1) 進め方について

もともと個人情報保護に関しては、我々だけではなく、親会社の第一生命も高い関心があった。日本経済新聞の平成 11 年 5 月の記事にプライバシーマークの紹介があり、それが目に止まって我々も調査を開始した。

どちらかというとトップダウンというよりはミドルアップに近い形であったと思う。

(2) 取得までの経緯

2000年問題があったので、本格的には2000年問題が片付いてからスタートした。

平成12年の10月位に、審査基準・課題等を一旦リスク管理グループで整理し、その後推進メンバーにコンプライアンス・プログラムの作成を指示した。そして11月から13年2月までの間に本格的に策定作業を行った。13年6月に審査を受け、7月に認定ということになった。そういう意味では短期で作ったことになる。

一から全部作ったのではなく、元々社内にあったものを、整理した体系に照らし、抜けている部分を整備していったという形になる。ゼロベースでスタートすると多分もっと時間がかかったのではないかと思う。

(3) 社内の推進体制について

推進チームを作ったが、人数は14～5人です。実際の書き物（コンプライアンス・プログラムの整備）をしたのは4～5人である。そういう意味では、小人数で作り上げたことになる。コンプライアンス・プログラム整備後は、グループの中で推進していく形にした。

会社としてやらなければならない物理的・管理的なセキュリティ対策については、パラレルに動いていたので、そこを上手く活用してきた。同時並行で動いているものを結合させたという感じである。

(4) 書類審査について

ＪＩＳＡの担当の方に相談に乗っていただいたが、当社の事業内容に照らして、「こんなリスクがありますね」といった指摘事項がずばっとあったので、その点に注意して取組んだ。

段階的に一つ一つ相談しながら、最終的にはこれで良いだろうという感触をつかんだ上で申請したので、書類審査では、これはダメという点は特になかった。

(5) 現地調査について

書類審査では見ることのできない範囲について見ていただいた。入館チェックなどは、書類上ではやることになっていても、実際できているかどうかは分からない。また、契約書の雛型を作って運用しているか等の各種の証跡類を見せ、コンプライアンス・プログラムにもとづいた運用ができているかが確認された。運用がきちん

とできていれば、はねられることはない。

(6) 取得で苦労された点について

開発基準をどうするかという点であった。当社の場合、ほとんどの業務が第一生命本体で持っている開発基準に準拠して開発を行っている。外部から見ると、親会社といえども別法人である。まったく別の開発基準を策定するのも、二重のメンテナンスになるなど非効率的でなので、その辺の位置付けについて議論があった。

結果的には、親会社の開発基準に準拠するという規定を作り、遵守することとしている。

3. プライバシーマーク取得後の運用について

(1) 品質保持のための体制について

コンプライアンス教育の推進等の事務局的な役割を勤めているのが、私共リスク管理グループである。監査については、監査室にて行っている。また、当社ではプライバシーマークだけではなく、全社的にセキュリティ対策を取組むための推進体制を作っている。

(2) プライバシーマーク取得のＰＲについて

現在は 名刺、ホームページ、封筒などにより、ＰＲしている。会社案内などにもこれから採用していこうと思っている。それだけでは忘れてしまいがちなので、パソコンのスクリーンセーバーを作ったり、遊び心を混ぜながら社員が意識をするようにと考えている。

(3) 業務の委託先（外注先）への対応について

当社では、業務を外部委託する場合の契約書の雛形を制定している。当社の場合は、システム開発を委託するのであり、個人情報を委託先に出すケースはあまりない。個人情報を含んだ委託業務が生じる場合は、厳格な管理を行うようにしている。いずれの場合も、契約書には秘密保持条項を必ず盛り込んだ上で、契約を締結している。

契約書には、システム監査権を盛込むようにしているが、実際どう運用していくかは、今後の課題と考えている。

3.3.7 某社

●企業名：A株式会社

●実施日：2001 年 11 月 29 日（木）

1. プライバシーマークの取得について

(1) 取得の動機

JIS Q 15001 の存在を知ったことである。また、個人情報保護の法制化の動きなどにも注視していた。当時、ＪＩＰＤＥＣの講演会にある社員が出席し、個人情報保護について社長に報告したところ、社長からトップダウンでやるように指示を受け、スタートした。

(2) 取得までの経緯

まず、社内体制を整備し、コンプライアンス・プログラムを構築するのに 6 ヶ月を費やした。申請して、6 ヵ月後に取得できた。

(3) 社内の推進体制について

企画部が中心となって、プロジェクトチーム作り、廻していった。各部門で、コンプライアンス・プログラムに基づき、実務レベルで担当者が中心となって社内の規定集などの見直し作業を行っていった。

プロジェクトで推進したことによって、社内全体に個人情報保護の意識改革もでき、ボトムアップの雰囲気とトップの思いとが上手く合ってきたと思う。

(4) 取得のメリットについて

プライバシーマークを取得することが目的ではない。あくまでも、社内整備のための手段であると考えている。

新規の顧客に対してのメリットにはならないと思う。

(5) コストについて

プロジェクトを推進するためのコストはかかっていない。プライバシーマーク取得は、コストの問題ではなく、リスクを取り除くための前提になるものと思っている。

2. プライバシーマーク取得後の運用について

(1) プライバシーマーク取得のＰＲについて

あくまでもプライバシーマーク取得は手段であると考えているので、クローズアップしてのＰＲは考えていない。プライバシーマークの考え方を会員に理解していただくこと。そして、社員の日々の営業活動を個人情報保護の観点から見直してもらうことが重要と考えている。

(2) 現場やラインの抵抗感について

ほとんどない。

(3) リスクについて

取得してからがスタートという感じである。今後は社会・消費者の信頼を損なわないよう、社内体制の整備を継続していきたいと思っている。

(4) 社内教育について

制度を作って、その制度を上手く運用していく風土を作るためには、研修は欠かせないものだと思う。

今後、組織責任者に対しては、特別なカリキュラムが必要かとも考えている。

(5) 委託先への対応について

個人情報の守秘義務をやかましいほど言っている。契約書の雛型の中にも、個人情報保護についての条文を入れている。

3. 今後のビジネスへの影響について

強制化はしないが、今後はプライバシーマークを取得しているのは、当たり前のことになると思う。持っていないことのデメリット・リスクの方が多くなってくると思う。また、新しいサービスを開発する時にも、個人情報漏洩のリスクを考えた上で取組むようになってくるものと思う。

3.3.8 A チーム活動総括　インタビューまとめ

プライバシーマーク取得企業を訪問し質疑応答形式にて得た、各企業のプライバシーマーク取得に関する活動内容を分析すると、共通の傾向が見られたため以下のように報告する。

1. プライバシーマーク取得の目的

顧客情報を取り扱う上での社内体制整備や見直しとして活用した。

備考：顧客から直接の取得要求はまだ僅かである。現状では、潜在的ニーズに対してシーズ側面から取得している例が殆どである。今後、一般顧客に対してプライバシーマーク制度のアピールが必要か？多くの企業が、企業活動に必須となる制度への展開（例えば、入札条件とする）も望んでいる。

2. プライバシーマーク取得の推進体制

トップダウンで活動開始、プロジェクト組織にて全社に展開した。殆どが社内専任

又は兼務者で実施したが、場合によって専門家（情報処理技術／社内教育方法等）のアドバイスを受けた。

備考：実態としては、企画や法務部門等の事務系スタッフが中心となって推進している。ミドル層の個人情報保護への意識や一般社員の常日頃からのセキュリティ意識が活動開始前より高い企業は、抵抗もなく推進がスムーズであった。

3. **プライバシーマーク取得コスト**

直接的な取得費用（大組織で最高 60 万円）以外には、特別に費用は生じなかった。

備考：取得に必要な、書類作成、社内教育やコンサル費用は、通常業務に不可欠なものであるため別枠として必要になったという意識はない。

4. **コンプライアンス・プログラム策定期間**

プライバシーマーク取得申請までの期間は平均で 6 ヶ月程度。最短が４ヶ月で、最長９ヶ月であった。

5. **コンプライアンス・プログラム監査**

社内の個人情報を直接取り扱わない部門で行った。

備考：ＩＳＯになれば外部監査が必須になると考えており、今後の課題と見ている。

6. **委託先との個人情報保護に関する契約**

委託先にも社内規則を策定させたり、契約にあたっては個人情報保護項目を追加している。

備考：契約書については、雛形を用意した企業も多い。委託先への監査については、今後の検討課題としている企業が多い。

7. **プライバシーマークの活用**

全企業が自社のＨＰへの掲載を行っている。顧客への企画・提案書や会社案内パンフレットへの表示は比較的多い。一部では、名刺や封筒への印字だけでなく、社内ＯＡ機器のスクリーンセーバーにし、顧客だけでなく社員への継続的な啓蒙活動に活用している企業もあった。

8. **メンバー所見**

プライバシーマークの定着を顧客だけでなく、社員への啓蒙活動に利用している企業もあり、プライバシーマーク事務局等が活用事例を水平展開する活動をしても良いのではと考える。

3.4 プライバシーマークタスクフォースＢチームの活動　～各国の個人情報保護の経緯と現状～

Ｂチームは、社会や企業に個人情報保護の意識浸透が進む欧米の情勢や今後連携の重要性が増してくるであろうアジア主要国の事情についてプライバシーマーク制度に関する文献を収集整理し、更には歴史的な背景等について考察してみた。

3.4.1　ＯＥＣＤ

3.4.1.1 個人情報保護に関する法規等

1. 1980 年「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ＯＥＣＤ理事会勧告」を採択

・ポイント：国内適用における基本 8 原則

(1) 情報収集の原則

個人データの収集は適法かつ公正な手段によるべきであり、適当な場合にはデータ主体に通知又は同意を得て行うべき。

(2) データ内容の原則

個人データは、その利用目的に沿ったものであるべきであり、利用目的に必要な範囲内で正確、安全、最新に保たれねばならない。

(3) 目的明確化の原則

収集目的は収集時より遅くない時期に明確化されなければならず、その後の利用は収集目的と両立し、かつ明確化されたものに制限すべき。

(4) 利用制限の原則

個人データは明確化された目的以外に使用されるべきではない。

(5) 安全保護の原則

個人データは紛失・破壊・修正・開示等の危険に対し、合理的な安全保護措置により保護されなければならない。

(6) 公開の原則

個人データに係る開発、実施、政策は一般に公開されなければならない。また、データ管理者を明示する手段を容易に利用できなければならない。

(7) 個人参加の原則

自己に関するデータの所在を確認し知らせるべき。また、自己に関するデータについて異議申立ができ、消去、修正、完全化､補正ができなければならない。

(8) 責任の原則

データ管理者は、以上の原則を実施するための措置に従う責任を有するべき。

2. 1998 年 電子商取引に関するＯＥＣＤ閣僚会議における「オタワ会議・閣僚宣言」

(1) 法律、自主規制及び行政的手段のいずれをも有効なプライバシー保護手段として位置づける。

(2) プライバシー保護施策が遵守されない場合の効果的な救済・是正措置の確保を明確化

3.4.2 ＥＵ

3.4.2.1 個人情報保護に関する法規等

1. 1995 年 「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転に関する欧州議会および理事会の指令」採択

・本指令により、ＥＵ加盟国は 1998 年 10 月 24 日までに、この指令にあわせて国内法を整備することが義務づけられる

・ポイント①：第 4 章 第三国への個人データの移転

(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遵守を損なうことなく、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遵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。

・ポイント②：最終条項

(1) 構成国は、この指令の採択の日から少なくとも３年以内に、この指令を遵守する

ために必要な法律、規則及び行政規定を発効させなければならない

2. 1998 年 米国より「セーフ・ハーバー（ＳＨＰＰ）」提出
3. 1999 年 1 月 ＥＵ作業部会より「米国におけるデータ保護レベルとヨーロッパ委員会・米国政府間における継続討議」に関する意見書を採択

   ⇒米国の原則の欠点を指摘
4. 1999 年 米国財務省「ＳＨＰＰ」を改定・公表
5. 1999 年 5 月 ＥＵ作業部会「国際セーフ・ハーバー原則の不十分性」に関する第二意見書を発行
6. 2000 年 7 月 米国商務省より改善を加えた原則を発行
7. セーフ・ハーバー原則とＥＵの攻防は、今後も続くものと予想される。

3.4.2.2 ＥＵ指令に基づく各国の動向

表 3-1 EU指令に基づく各国の動向

国名	動向
ベルギー	2001 年 9 月 施行
デンマーク	1998 年 4 月 法案提出
スペイン	1999 年 12 月 個人データ保護に関する法 採択
ギリシャ	1997 年 10 月 データ保護法 公布
イタリア	1997 年 5 月 個人データ保護法 発行
ルクセンブルク	2000 年 10 月 法草案が議会に提出。2001 年投票
オランダ	2001 年 個人データ保護法 施行
オーストラリア	2000 年 1 月 個人データ保護法 施行
ポルトガル	1997 年 9 月 ＥＵ指令に沿った憲法改正
フィンランド	1998 年 7 月 法案提出
スウェーデン	1998 年 4 月 議会により採択

3.4.3 イギリス

3.4.3.1 個人情報保護に関する法規等

1. 1984 年 データ保護法

・公的部門・民間部門双方を対象とした個人のコンピュータ化された情報についての保護を規定

・登録システムを設け、独立したデータ保護登録官により監督

・情報主体の権利　自己データが含まれるか否かを知る権利とそのコピー提供を受ける権利

2. 1998 年データ保護法（1998）

・ＥＵ指令に対応するため、1984 年データ保護法を全面改正する形で制定

・主な改正内容

(1) データ保護原則の改訂:センシティブなデータと一般データの区別

(2) 対象データ範囲:コンピュータ処理データに加え、手作業データ追加

(3) 監督機関:データ保護登録官からデータ保護コミッショナーに変更

(4) 手続きの簡素化:登録から届出へ

(5) 情報主体の権利の拡充

・データ保護原則

(1) 同意の原則：データ主体の同意又は契約・義務の履行の時処理が許される

(2) 目的制限の原則：明示された適法な目的に限り取得・処理

(3) 相応性の原則：目的との関連で適切かつ相応であること

(4) 正確性の原則：正確かつ必要な限度で最新であること

(5) 保存必要性の原則：処理目的に必要な期間内においてのみ保存

(6) データ主体の権利の原則：法の定めるデータ主体の権利に従い処理

(7) 安全保護措置の原則：安全保護のため適切な技術的組織的措置を施す

(8) データ移転制限の原則：ＥＵ域外で個人データの保護レベルが保障されない国等へのデータ移転の禁止

・データ主体の権利

(1) アクセス権:自己のデータが含まれることを知らされる権利およびその個人データ、処理目的、データ受領者等の通知を受ける権利

(2) データコントロール権:データ管理者の違法な行為により受けた損害賠償を受ける権利およびデータが不正確な際抹消を求める権利

・監督制度

(1) データ保護コミッショナーを任命

(2) コミッショナーの決定に不服を申し立てる機関としてデータ保護裁判所設置

・適用除外

(1) 国家安全保障目的　データ保護全原則・アクセス権等

(2) **防犯、捜査、逮捕、公租公課等目的　データ保護全原則・アクセス権等**

(3) **ジャーナリズム、芸術・文学目的　安全保護措置を除く原則とアクセス権・データコントロール権**

(4) **統計上・歴史上の目的　保存必要性の原則　保存必要性の原則**

(5) **データ主体の教育・研修・雇用・任務任命等目的アクセス権**

(6) **データ主体の心身健康に関する個人データおよび学校所有者の当該学校生徒であったものに関する個人データ関連規定 国務大臣の命令により適用除外**

3.4.3.2 個人情報保護関連マーク制度

個人情報保護のみの機能を持つマーク制度は見当たらない。

3.4.3.3 オンライントラストマーク制度

1. Which？ Web Trader

・消費者協会（ＣＡ：Consumers'Assciation**）により運営される無料の認証スキーム**

2. Clicksure

・インターネット企業により運営される有料の認証スキーム

3. Trust**ＵＫ**（2000 **年** 1 **月**）

(1) **消費者協会（ＣＡ）、エレクトロニクス・ビジネス同盟（ＡＥＢ：**Alliance for Electronic Business**）、ダイレクトマーケティング協会（**Direct Marketing Association**）が政府の要請により設立した非営利団体**

(2) **オンラインショッピング促進を目的に質の低い顧客サービスや電子商取引における不正行為に対する安全認証マーク制度**

(3) **法規制に頼らず自主規制による安全な業界電子商取引促進**

(4) **各業界団体が顧客プライバシー保護、安全な決済、返品、価格設定、苦情処理、児童向のマーケティング、既存法の遵守等の基準を規定** Trust**ＵＫはその基準を審査し、認定**

(5) **各団体に属する企業は** Web **上での小売販売時に、規定遵守を義務に、同マークを使用、その団体は監視**

(6) 業界団体にかかるコストは約 1,000～5,000 ポンド

3.4.4 フランス

3.4.4.1 個人情報保護に関する法規等

1. 1978 年 情報処理・データと自由に関する法律

・公的部門・民間部門を問わず適用

・データ保護原則

(1) 不正・違法な個人情報の収集の禁止

(2) 個人情報収集時の通知義務

- 情報提供義務の可否
- 提供しなかった場合の効果
- 情報収集対象
- アクセス権及び訂正権

(3) 保存必要性の原則：収集の際、提示された期限においてのみ保存

(4) 安全保護措置の原則：個人情報の保護のために必要な措置を講ずる

(5) 人種、政治的・思想的・宗教的信条、労働組合、倫理に関する情報収集際の同意の原則及び企業の犯罪、有罪判決、セキュリティに関する情報収集の禁止

(6) アクセス権：

自己の個人情報の保有に関し問い合わせる権利、自己情報にアクセスする権利、ならびに訂正、追加、明確化、更新又は抹消を要求する権利。個人情報を修正、削除した場合はその旨を情報提供した第三者に通知する義務。

・登録制度

(1) 公的機関が個人情報を処理する場合、ＣＮＩＬ(情報処理及び自由に関する国家委員会)の諮問を経、政令などで明文化。

(2) 国民識別番号使用システム＝公的機関・非公的機関共 CNIL へ意見申請。

(3) 非公的機関が個人情報を処理する場合は、ＣＮＩＬに届出。

(4) 定型的でプライバシー侵害のおそれが少ない個人情報の処理については、公的非公的機関を問わず、簡略規範に従うことを届出。

・監督機関：情報処理及び自由に関する国家委員会（ＣＮＩＬ）、17 名で監督

・適用除外

(1) 表現の自由に関し、出版又は報道機関が処理する場合。

(2) 健康分野における研究目的の姓名に結びついたデータのコンピュータ処理。

3.4.4.2 最近の動向

1. 1999 年 閣僚委員会よりプライバシー保護の為の法制度のフレームワーク発表。情報処理・データと自由に関する法律はＥＵ指令に整合を図り改正。
2. 2000 年 6 月に政府よりＣＮＩＬにデータ保護指令に基づく改正草案を通知。9 月にＣＩＮＬより意見通知。

3.4.4.3 個人情報保護関連マーク制度

個人情報保護のみの機能を持つマーク制度は見当たらない。

3.4.4.4 オンライントラストマーク制度

1. L@belsite

・登録商標であり、厳密に定められた条件に従わない限り、マークの使用はできない。

・フランス国内で販売を行うサイトに付与される。

・仕様許可を得る条件の中でも個人情報保護は特に重要視。

・重点ポイント

(1) サイトを運営する事業者の実体

(2) 遠距離販売に適用される規則、倫理規範、品質憲章、および規定の遵守（27 の規則あり）

(3) 情報科学と自由に関する法律や職業倫理規範などに定められた個人データの取扱における透明性及びその保護⇒27 の規則中、11～15 は個人データ保護についての規定

＊その他推奨事項として、個人データの保護に関するインターネットサイトに明記すべき文言等の推奨事項および付属書あり

3.4.5 ドイツ

3.4.5.1 個人情報保護に関する法規等

1. **ヘッセン州にて世界初のデータ保護法採択（1970 年）**
2. **連邦データ保護法（1977 年）**
3. **連邦データ保護法改正（1990 年）・・・これ以降、ＥＵ指令に対応作業を進める。**

・立法の目的は個人情報取扱時の人格権侵害から個人を保護すること。

・公的機関のデータファイル、書類および民間における営業や職務上、事業目的のデータ処理

・データ保護原則

(1) **原則、書面主義による当事者の同意（データ蓄積目的、提供目的、不同意の効果についての事前説明義務あり）がない限りデータ処理、利用は禁止。**

(2) **目的変更する場合、許可と同意が必要。**

(3) **データ収集の原則：**

・データは信義則に基づき適法に収集されること。

・データ主体に対し、蓄積の事実及び情報の種類を告知すること。

(4) **アクセス権：**

・データ主体は蓄積データ、蓄積目的について開示要求できる。

・データファイル登録簿の閲覧を可能とすること。

(5) **個人データの誤り・データ主体からの指摘に対し訂正又は指摘の旨記録。**

(6) **個人情報の収集、処理等による権利侵害に対し、連邦データ監察官又は監督機関への苦情申し立てができる。**

(7) **債務不履行、不法行為等に対してはデータ管理者の立証により賠償。**

・監督制度：州の監督官庁が監督を実施。民間はデータ保護受託者を設置。

・適用除外：報道関係、映画関係、放送関係企業、出版社におけるジャーナリスティックな活動に限り、活動従事者の守秘義務及びデータ管理者の保護措置義務以外を免除。

3.4.5.2 個人情報保護関連マーク制度

個人情報保護のみの機能を持つマーク制度は見当たらない。

3.4.5.3 オンライントラストマーク制度

1. Trusted Shops Guarantee

・ケルンの保険会社ゲーリング社（70%）とビジネステクノロジーコンサル会社の IMPACT 社の共同運営

・商品が配送されなかった場合の保障制度とリンク

・顧客の不満を察知、取り除きのシステム構築

・マークの意義

(1) 行動規範（Code of Conduct)の遵守

(2) 情報保護(*)

(3) 返金に関する保証制度

(4) 配送に関する保証制度

・メンバーシップフィー：

オンラインでの売上高により 1250～16000 マルクを年会費として徴収

売上額 100 万マルク以上の大企業は売上額 0.1～0.4%のプレミア

(*)情報保護

情報保護法の遵守／プライバシーステイトメント

(1) 自己目的のための収集処理・利用

(2) 第 3 者提供について

(3) 事前同意（透明性）

(4) 通知・消去・閉鎖

3.4.6 アメリカ

3.4.6.1 個人情報保護に関する法規等

●米国には包括的なプライバシー保護法はない。

民間の自主規制で十分であり、子供のプライバシーと医療情報に関する以外に新たな法律を制定すべきでないという基本スタンス。

●包括的なプライバシー保護法がない代わり、セグメント方式として、部門ごとにプライバシーを保護する形をとっている。

(1) 金融プライバシー権利法（Right to Financial Privacy Act）

(2) 公正信用報告法（Fair Cresit Reporting Act）

(3) ビデオプライバシー保護法（Video Privacy Protection Act）

(4) **有線プライバシー保護法**（Cable Privacy Protection Act）

(5) **家庭教育の権利とプライバシーに関する法**（Family Educational Rights and Privacy Act）

(6) **運転者プライバシー保護法**（Drivers Privacy Protection Act）

(7) **電話利用者保護法**（Telephone Consumer Protection Act）

(8) **情報の自由法**（Freedom of Information Act）

1. **1998 年 ＦＴＣ（連邦取引委員会）「オンラインプライバシー一般に関する立法モデル」を提言。個人情報を収集する商用サイトに対して 4 つの情報取り扱い上の原則を要求。**

(1) **通知と認識**

(2) **選択と同意：Web サイトは消費者に対して情報の利用方法に関して選択する権利を与えなければならない**

(3) **アクセスと参加**

(4) **セキュリティと完全性**

2. **1998 年 個人 ID 情報の窃盗に対する罰則を強化した法案**（Bill on Identity Theft）**を議会で可決**

3. **1999 年 オンラインにおける電子医療記録のプライバシーを保護する法案を提案**

4. **2000 年 「児童オンラインプライバシー保護法（ＣＯＰＰＡ）」施行**

(1) **子供のプライバシー侵害の恐れが大きい場合（第三者に個人情報が提供される場合など）を除いて、電子メールという簡易な親の同意手段でよい。**

(2) **それに加えて、親の身元を確認するような措置（「同意を承りました」という確認のメールを親に送付する、手紙や電話で親の同意を確認するなど）を取られなければならない。**

【民間部門の自主規制】

1. **1997 年 ＤＭＡ**（Direct Marketing Association）**が、ダイレクトマーケティング業者向けにプライバシー・ガイドラインを発表**

・ダイレクトマーケティング業者がインターネットマーケティングにおいて守るべき４つの原則

(1) **オンラインでの通知**

(2) **オプトアウト**

(3) マーケティング目的の電子メール

(4) 子供からのデータ収集

3.4.6.2 個人情報保護関連マーク制度

1. BBBOnline Privacy

・ＢＢＢの高い水準を満たしている企業に対して３種類のシールを付与

(1) 信頼性シール（⇒オンライントラストマーク制度に表記）

(2) プライバシーシール

(3) キッズプライバシーシール

・ 申請

(1) 資格基準を含むプログラム、参加契約、価格設定情報の詳細をホームページ上より入手

(2) 事業申請書提出後、ユーザーネーム、パスワード、「準拠性評価アンケート」の記入に必要な事項が記載された e-mail が送付

(3) 手数料の支払

(4) 「準拠性評価アンケート」に対するオンライン準拠性アナリストの審査

・ 申請費用

(1) 申請書 1 件あたり $75 の手数料と企業総売上高に応じて$150~$3,000の年間使用料

(2) ＢＢＢ（ベター・ビジネス・ビュロー）の会員は 50%の割引を受けられる

●ＢＢＢオンラインプライバシーシール

・ 商品の注文やコンテストへの参加、サービス登録、メーリングリストへの参加時等に収集される消費者データに対してその利用や公開方法がわからないことが多いが、Web 画面にこのシールを探すことでオンライン上のプライバシーを守ることができる。

●ＢＢＢオンラインキッズプライバシーシール

・ 子供に関係する固有のオンラインプライバシー問題を扱う広範囲な特別要件に従う。

・ 13 歳未満の児童向け、または、13 歳未満であることが知られている訪問者から情報

収集する企業を対象とする。

・ わかり易い言語により警告･説明する。

・ 児童のゲームや活動について必要以上の収集を避ける。

2. TRUST ｅ

・オンライン取引における国際的信用と信頼を創造することを目的とした非営利団体

・TRUST ｅシールプログラムはＷｅｂパブリシャーにTRUSTｅの第三者監視プロセスに支えられた標準プログラムを提供する。

・各Ｗｅｂパブリシャーはこのプログラムを使用して、情報収集及び普及慣行に関する情報をユーザーに提供できる。

・ガイドラインに準拠したサイトは「トラストマーク」の表示が許可されプライバシーシールプログラムに参加している事をユーザーに知らせることができる。

3. ＣＰＡ ＷｅｂＴｒｕｓｔ

・米国公認会計士協会によるプライバシー保護シールマーク

＜原則＞

(1) 業務慣行の開示：電子商取引に関する業務慣行を開示し、プライバシー情報の管理を行う。

(2) 取引の倫理性管理：お客様が信頼のおける管理体制を敷いている。

(3) 情報保護の管理：お客様の個人情報が他の目的に使用されることがないということをお客様に保証し、信頼を勝ち得るための効果的な管理を維持する。

3.4.6.3 オンライントラストマーク制度

1. BBBOnlineReliability

・狙い＝健全で倫理的なオンラインビジネスを奨励することによりインターネットにおける信頼と信用を高める。

・ＢＢＢの高い水準を満たしている企業に対してシールを付与。

●ＢＢＢオンライン信頼性シール

・信用できるＷｅｂサイトやオンラインサービスを区別する簡単な方法を提供する。

・オンラインでの消費者の信頼や信用を高める。

3.4.7　韓国

3.4.7.1 個人情報保護に関する法規等

●韓国においては個人情報保護法は公的部門を適用範囲とし、民間部門はその 対象としていない。

(1) 1967 年以降情報化が進展し、80 年代以降は国家規模の行政電算網事業が行われる。

(2) 1985 年 国家電算網事業をめぐり、個人情報の侵害に対する保護問題が提起。

(3) 1989 年「電子計算機により処理される個人関連情報のための法律（案）」提出されるも、廃棄。

(4) 1994 年「公共機関における個人情報保護に関する法律」制定。

1. 「公共機関における個人情報保護に関する法律」（1994 年）

(1) 目的・適用範囲

・「公共機関」＝国家行政機関・地方自治体・大統領例に定める機関

・コンピュータ処理に係る個人情報（手作業によるものは含まず）

(2) 保護措置

・個人情報の収集・ファイルの保有制限

・個人情報の安全性および正確性・最新性の確保

・個人情報ファイルの公告

・個人情報ファイル台帳の作成および閲覧

・個人情報の利用・提供の制限

(3) 個人の権利

・個人情報の開示請求

・開示・訂正請求…確認に必要な証憑提出を求められる。

(4) 監督機関等

・独立した監督機能・権利救済機能を持つ機構はない。

・諮問機関：個人情報保護審議委員会

(5) 罰則規定

・公共機関の個人情報処理業務を妨げる目的で改ざん・抹消した場合

・漏洩または権限無き処理・他人への提供等不当な目的で使用した場合

・偽り他不当な方法により処理情報を閲覧または提供してもらった場合

以上の場合それぞれ懲役または罰金の刑罰が科せられる。

両罰規定として行為者だけでなく関連の個人・法人にも管理責任を問う。

2. 「電子商取引に関する基本法」（1999）

・第 3 章：「電子商取引に携わる事業者は電子商取引を通じて収集した個人情報を本人の同意なく異なる目的で利用・第三者に提供してはならない」

3. 課題

・民間分野への措置

・個人情報保護審議委員会の機能

3.4.7.2 個人情報保護関連マーク制度 最近の動向

●プライバシーについての新マーク制度導入

・韓国情報通信産業協会（ＫＡＩＴ）にて新たにプライバシーについての新マーク制度導入を検討（後援：情報通信部・韓国情報保護振興院他）

・インターネット関連事業者を対象に同協会が付与機関となり、個人情報保護政策・管理水準等を評価する。

3.4.7.3 オンライントラストマーク制度

1. eT rust

(1) 電子商取引振興院（ＫＩＥＣ）が審査機関となり運営

(2) 目的

①消費者保護

②安全で便利な取引の拡大

③良い市場慣習の定着

(3) 申請資格

①税務署への事業登録

②地方自治体への通販事業登録

③電子商取引の３ヶ月以上の実績

④マーク制度の条件

(4) 審査基準

①システム能力と安全性

②商品情報のアクセス利便性

③商品情報の適切性

④注文の利便性と安全性

⑤商品配送、変更、返金の利便性

⑥創意工夫

についてポイント制で 70 ポイント以上に使用を認める。

(5) マーク使用料：300,000 ウォン（約 3 万円）

2. iＳＡＦＥ mark

(1) 韓国情報通信産業協会（ＫＡＩＴ）にて運営

(2) 消費者保護、プライバシー保護、システムセキュリティの３要素からなる。

(3) 申込み料は新規は 500,000 ウォン（約 5 万円）、他は 300,000 ウォン（3 万円）

(4) マーク使用料は規模により変わるが、大規模会社のレベルでは 1,000,000 ウォン（約 10 万円）

3.4.8 シンガポール

ＩＴ先進国であるシンガポールの個人情報保護に関する法規およびマーク制度についてのレポートは意外に多くなく、現地政府関係機関（ｉＤＡ）およびマーク付与団体（Commerce Trust）にヒアリングを行った。

3.4.8.1 個人情報保護についての記されている法制度

現在、シンガポールでは、公共部門に対する個人情報保護法はあるが、データ保護、プライバシーに関する一般的な法律は存在しない。業界を規制するそれぞれの法律の中で部分的に個人情報保護について謳われているといった状況である。

通信情報技術省（ＭＣＩＴ）のもとで機能するシンガポール政府の委員会であるｉＤＡ（INFOCOMM DEVELOPMENT AUTHORITY OF SINGAPORE）によると、我が国で

審議されているような個人情報保護基本法は、現在、タスクフォースが形成されて検討中ではあるが、今後数年をかけて検討していく予定とのことで喫緊の案件ではないようだ。また 1998 年に自主規制のための「Electronic Commerce Code」が提唱されているが、任意の規範のレベルにとどまっている。

EU 指令の要求基準について、現状の法制度で対応可能との認識があるように見受けられる。

1. 民間部門に関連する法規
   - コンピュータの誤操作関するに関する法令（Computer misuse act）
   - 電気通信に関する法令（Telecommunication act）
   - 通信サービスにおける競争に関しての iDA 規定（iDA code of practice for competition in the provision of telecom service ）
   - 銀行に関する法令（Banking act）
   - 産業に関する規定（Industry code of practice）
   - NIAC の E コマースに関する規定（NIAC［national internet advisory committees］e-commerce code）

2. 公共部門に関連する法規
   - 公的秘密についての法令（Official secret act）
   - 法定団体及び政府企業についての法令（Statutory bodies and government companies act）
   - 統計に関する法令（Statistics act）
   - 中央積立基金に関する法令（Central provident fund act）
   - 電子取引に関する法令（Electronic transactions act）

3.4.8.2 シンガポールにおけるマーク制度の現状

シンガポールにおいてはシンガポール国内の消費者保護を目的にナショナル・トラスト・カウンシル（以下ＮＴＣ）が 2001 年 4 月、ｉＤＡにより作られた。そこでは Authorized Code Owner （以下ＡＣＯ）という国内のトラストマーク事業者に対し、ＮＴＣが認可し国のお墨付きを与えるというというプログラムを運営し、Trust SG マークを付与している。

したがってＮＴＣに認可された付与団体は、自社のマークと併せて Trust SG マークを使

用することができる。シンガポールでは実質的には NTC の認可がなければ、マークの信頼性がなく、事業者も募集できない。

現在、ＮＴＣの認可を受けているマークは以下の 2 つである。

（1） Commerce Trust（CNSG が株主）の運営する Consumer Trust マーク

（2） ＣＡＳＥ(Consumer association singapore)の運営する Case Trust マーク

Commerce Trust の担当者によると Consumer Trust マークは現在 2 社、Case Trust マークは現在 20 社程度、付与しているとのことであった。

3.4.8.3 個人情報保護関連マーク制度

シンガポールにおける個人情報保護に関するマーク制度についてはまだ必要性を模索する段階にあるが、Commerce Net Singaporeが「Privacy Trust」というマークを持って今後のニーズに向けて準備をはじめている。

現在、前述のＡＣＯに対して Trust マークの使用を申請中であり、半年以内で認可の見通しとの Commerce Trust の担当者の話であった。

同マークについては、トラストマークがＥＣ関連の中小事業者であるのに対し、個人情報保護に関するマーク制度を必要とするのはそれらより大きな規模の企業を想定しており、具体的業種として銀行や病院等医療関連をターゲットと考えている。

＜主な要件＞

- 年会費　：年間で 5,000～20,000SG＄の予定
- 審査方法　：書類審査、プライバシーポリシーおよび実行されているかどうかについて審査
- 対象地域　：まずシンガポール域内とし、以降拡張を考える

3.4.8.4 日本－シンガポールを巡る個人情報保護の動き

上記のようにシンガポールの個人情報保護に対する現在の状況はさほど加熱した状況とはいえないが、調査期間中おりしも小泉首相が東南アジアを歴訪し、シンガポールにおいても森政権当時より進められていた日本シンガポール新時代経済連携協定が 2002 年 1 月 13 日にわが国初のＲＴＡ（Regional Trade Agreement=地域貿易協定）として署名された。その中の経済連携強化分野における情報通信技術に関して「電子署名･認証制度」「ＩＴ技

術者」とともに「個人情報保護」がテーマにあげられ、ＪＩＰＤＥＣと Commerce Trust 都の間でプライバシーマークを相互承認することとなっている。

シンガポール内の状況に対してこうした国際関係において個人情報保護の問題がどのような形で審議及び政策に反映してくるかは今後とも注視していきたい。

3.4.8.5 オンライントラストマーク制度

1. Consumer Trust

   Commerce Trustが運営、2001年12月にTrust SGの認可を受け運営を開始する。グローバルレベルでの消費者信頼を目指し、現在、JuzclickCar.com.Pte Ltd とSafe-EX Global Pte Ltdの2社が加入。

2. Case Trust

   ＣＡＳＥ(Consumer Association Singapore)は 1971年の設立で消費者関連問題について消費者保護及び教育・救済を推進する。同協会の主催する「CASE Trust」は会員規約に則したミニマム・スタンダードを形成し、消費者に対する保証を宣言するもので、2001年夏にTrust SG の認可を受け、６ヶ月が経過。現在、約 20社が加入している。

3.4.9　日本

3.4.9.1 個人情報保護に関する法規等

1. 行政機関の保有する電子計算機処理に係る個人情報保護に関する法律（1988 年）
   - 国の行政機関における個人情報の取り扱いに関して制定
   - 地方公共団体は条例制定にて対応（1748団体が制定、52.7%）
2. 住民基本台帳法改正（1999年）

   〔改正の内容〕
   - 住民票コード
   - 住民基本台帳事務の簡素化
   - 本人確認情報に関する事務処理及び本人の利用
   - 本人確認情報の保護

・住民基本台帳カードの交付

3. 「個人情報保護に関する法律案」閣議決定・国会提出（2001 年 3 月）

・個人情報：生存する個人に関する個人を識別できる情報

・基本原則

①利用目的による制限：利用目的の明確化と目的範囲内での取扱い

②適正な取得：適法かつ適正な方法での取得

③正確性の確保：正確かつ最新の内容で保持

④安全性の確保：漏洩、滅失、毀損の防止その他安全管理の措置

⑤透明性の確保：本人が適切に関与し得る配慮

・義務規定

①利用目的による制限および適正な取得

②適正な管理の実現

③第三者提供の制限

④公表

⑤開示

⑥訂正等

⑦利用停止等

⑧苦情の処理

⑨苦情処理等を行う団体の認定

・罰則規定

主務大臣の勧告、命令に従わない場合、6 ヶ月以下の懲役または 30 万円以下の罰金

・認定個人情報保護団体

個人情報取扱事業者に関する苦情処理、情報提供ほか個人情報の適正な取扱いの確保に必要な業務を行おうとする団体を主務大臣が認定

＊第 11 条、附記事項

国の行政機関、独立行政法人及び特殊法人の保有する個人情報の適正な取扱いが確保されるような法制上の措置を公布後 1 年を目途に講ずる

⇒官の分野に対する個人情報保護の見なおしを図る

3.4.9.2 個人情報保護関連マーク制度

1. **プライバシーマーク**

(1) **1998年 ＪＩＰＤＥＣのプライバシーマーク制度としてスタート**

(2) **個人情報保護ＪＩＳに適合したコンプライアンスプログラムを整備し個人情報の取扱いを適切に行っている事業者を、第三者機関であるＪＩＰＤＥＣ（及びその指定機関）が評価認定し、その証としてロゴの使用を許諾する制度**

(3) **目的**

①事業者：個人情報の保護に関する信頼獲得へのインセンティブ提供
⇒個人情報保護システムの確立促進（JIS Q 15001 の普及）

②消費者：事業者の個人情報の取扱いの適切性を容易に判断できる材料（マーク）を提供⇒個人情報を自分で守る意識の向上

(4) **対象**

①国内に活動拠点を持つ民間事業者

②ＪＩＳ準拠のコンプライアンスプログラム（ＣＰ）が策定されそれに基づき個人情報の適切な管理が実施されていること

2. **個人情報保護マーク**

(1) **1998 年 （財）日本データ通信協会が「個人情報保護登録センター」を開設しスタート**

(2) **対象：「電気通信事業者」および「発信者情報通知サービス（ナンバーディスプレイなど）の事業用利用者」**

(3) **目的：マーク表示できるようにすることにより、事業者及び利用者の個人情報保護意識の向上を図る。**

(4) **事業者：**

個人情報の保護についての積極的な企業姿勢を利用者にアピールすることにより、企業イメージの向上につなげる。

⇒マークを封筒・名刺・広告／ＨＰなどに表示することができる。

(5) **利用者：**

電気通信事業者や発信者情報通知サービスを提供している事業者を選択する時の目安となる。

3.4.9.3 オンライントラストマーク制度

1. **オンラインマーク制度**

(1) 2000年 （社）日本通信販売協会と日本商工会議所で運営スタート

(2) （社）日本通信販売協会がインターネットを利用した消費者向け電子商取引において、適切な取引を行う事業者を認定し、マークを付与し、電子商取引の事業活動に関して使用を認める制度

(3) 目的：インターネット通信販売の促進と消費者保護の両立

(4) 対象：事業拠点が日本国内にある、原則として起業１年以上のインターネット通信販売事業者

(5) 審査：

申請のあったインターネット通信販売事業者のＨＰに販売条件等が法律（訪問販売等に関する法律）にそって記載されているか、誇大や不適切な広告表現がないかについて

(6) 個人情報に関する規定（電子商取引ガイドライン）

第５章…個人情報の収集に関する措置

収集範囲の制限、収集方法の原則、特定の機微な個人情報収集の禁止 他

第６章…個人情報利用に関する措置

利用範囲の制限、目的外利用の場合の措置

第７章…個人情報の提供に関する措置

提供範囲の制限、目的外の提供の場合の措置

第８条…個人情報の適正管理義務

個人情報の正確性の確保、利用の安全性の確保

秘密保護に関する従事者の責務

第９条…自己情報に関する情報主体の権利

自己情報に関する権利,情報の利用又は提供の拒否権

3.5 Ｂチーム活動総括

以上、イギリス、フランス、ドイツ、アメリカ、韓国、シンガポール、日本の７カ国とＯＥＣＤ、ＥＵについての個人情報保護に関する法規やガイドライン等と個人情報保護のマーク制度およびオンライントラストマークについてまとめた。

欧米については、もう既に言い尽くされていることだが、ヨーロッパがＥＵ指令に基づきオムニバス式の一括法をベースに域内整備を進めていくのに対し、アメリカは自主規制と業界別の個別法によるセグメント方式を取っており、その間はセーフ・ハーバー協定により調和を取ろうとしている。

各国の個人情報保護についての歴史的背景や国民の意識には大きな相違点があり、現段階ではそうした違いを正しく認識することが第一であると感じた。一方では、2001年 6月、JIPDEC の運営する「プライバシーマーク」と米国の BBBOnLine と間での相互承認制度がスタートしたのを始め、韓国のＫＡＩＴ（韓国情報通信産業協会）において新たに発足するプライバシーマークやシンガポールのＣＮＳＧ（Commerce Net Singapore）で進める「Privacy Trust」等との協議も今後進展していくものと思われる。

今後、国際協調への動向を注視しつつ、オンライントラストマーク制度と併せ、企業にとっては効果的な、また消費者にとっては判別しやすいマーク制度のあり方について考察を続けたい。

3.6 プライバシーマークタスクフォースＣチームの活動　～「個人情報保護に関するコンプライアンス・プログラム」の策定演習～

C チームには 8 名が参加し、具体的に自社のコンプライアンス・プログラム（以下　ＣＰ）の策定演習と、事業者全般においてＣＰを策定するにあたっての基本構成および留意点摘出等の検討を行った。

3.6.1　作業手順

活動を始めた時、本タスクフォースの参加メンバーの大方が、その所属会社において個人情報保護に関する社内規定の立案やプライバシーマークの取得に携わっているところであった。

活動の目指すものとして、ＣＰの策定にあたって重要な「ＣＰを構成する項目を一望できる体系的なものを作ること」と、「各社でＣＰを策定する際の手ほどきとなるようなベースを作成すること」を取り上げた。

推進の手順として、まず「ＣＰの基礎をなす個々の規程の組み合わせを鳥瞰できる構成表（以下　規定マップ）」を全員で検討することとした。

そして、「規定マップ」を考案した後、各社および各社の関連企業で策定されている「個

人情報保護規定」や「その他の関連規定」を持ち寄り、照合しながら、企業全般に適用できる留意事項や課題点を検証することとした。

3.6.2　企業全般で参考にできる「規定マップ」の作成

プライバシーマークの取得申請において要求される、個人情報保護のＣＰは以下の３要素からなると考えた。

1. 規定

   個人情報保護に関する「基本規程（ポリシー）」「細則（スタンダード）」「手順書（プロシージャ）」等を記したもの

2. 体制

   個人情報を収集・利用する業務を管理するための役割、責任を持たせた組織構成

3. 運用

   個人情報保護のために、日々の運用および改善のしくみをまわしていくこと

以上の３要素が整って、はじめて個人情報保護のためのＣＰが稼動すると考えた。さらに、ＣＰが稼動することで、常に最良の実践が行われるよう改善されることになるため、個人情報保護のレベルは向上していくと言える。

それらを紙上に表現する段階では「2.体制」および「3.運用」についても「1.規定」に盛り込まれることになる。それを表したものが「規定マップ（別表①）」である。

3.6.3　既存の規定との整合

サンプルとして取り上げた規定マップは、「個人情報保護方針」「個人情報保護基本規程」「マネジメント単位での個人情報保護細則」「ガイドライン」を骨格として、さらに「必要と考えられる手順書・契約書・チェックシート等」や、関係する「既存の自社規程」「業界ガイドライン」等についても標準的に書き出したものである。

この際重要なことは、企業機密管理について既にルール化ができているものについては、その適用範囲を確めることである。特に「従業員に関する個人情報の管理」や「顧客企業との取引上で知り得た顧客企業の従業員に関する個人情報の管理」について、混乱を招かないようにするための一つの方法である。

次に、各社あるいは各業界で表現上差異があるものとして、「個人情報保護基本規程」と「個人情報保護細則」（「細則」についてさらに「直接収集の場合」「第三者からの間

接収集の場合」「公開情報からの間接収集の場合」「預託されて授受する間接収集の場合」に分類）について検証した。

検証の方法としては、本来であればＪＩＰＤＥＣの作成指針をベースとして、業態別に具体的な文章を想定するべきところではあるが、今回は事業者全般において汎用的なサンプルにすることに主眼を置いた。そのため、規定に盛り込む内容についての基準といえる、ＪＩＰＤＥＣが発行している「プライバシーマーク制度における監査ガイドライン」中の「第 2 編　監査ガイドラインの詳細」（http://www.jipdec.or.jp/security/privacy/pm-guideline.html 参照）から要件を摘出することにした。

その後に、「規定の監査シート（別表②）」を作成し、さらに「全体規定」「直接収集細則」「間接収集（第 3 者）細則」「間接収集（公開）細則」「間接収集（預託される場合）細則」に分けて個々の企業ごとに作成演習を行った。

このように５つのブロックに分けた理由は、「個人情報保護基本規程・細則・手順書の項目表（別表③）」に示したように、規程の作成にあたって社内のどの部署が主体となって進めていくかを予め決めてからとりかかった方が良いからである。

3.6.4　全体規程についての留意事項

「全体規程」としては、上記「規定の監査シート（別表②）」の上では、「方針」、「計画」と「実施および運用のうち収集についてすべてに共通する事項」、さらには「監査」「事業者の代表者による見直し」「罰則」「改廃」にあたる部分を定める。

これについては、全社を総括するセクションおよび事務局主導にて「既存の自社規程」「業界ガイドライン」等を勘案しながら作成するのが効率的である。

3.6.5　収集に関する細則についての留意事項

「全体規定」以外の部分としては前述のとおり、「直接収集の場合」「第三者からの間接収集の場合」「公開情報からの間接収集の場合」「預託される場合」に分け検証した。

これについては、各社・業界ごと、さらには各社内の部門によって、また、目的・機能によって留意点が異なる。例えば、保険関連業種においては、そこで集められる個人情報については大方が直接収集となるし、クレジットカード業界においては信用情報機関からの間接収集がある。また、メーカー系においては、営業・販売部門で扱うＢｔｏＣの注文情報は概ね直接収集となるが、DMやマーケティング調査等については、系列代理店から

の間接収集もありえるし、外部業者への預託についてもルールが必要になるであろう。

そうした部門単位での手順やチェック項目を規定化するには当然ながらそれぞれのセクションより「部門推進委員」を選出し、そこで取り扱う個人情報を扱う業務の棚卸を行い、事務局との調整を通じて、細則を作成していくことが望ましい。

3.6.6　策定にあたっての留意事項

以上に述べたことを含め、以下にコンプライアンス・プログラム策定のポイントを示す。

1. コンプライアンス・プログラム策定スタッフ（事務局および部門推進委員）を任命する。
2. 「規定マップ」を活用し、自社の個人情報保護に関連するルールを体系的に把握する。
3. 事務局中心に全体規程と骨格を作成。
   - 個人情報保護方針
   - 計画
   - 実施および運用
   - 監査
   - 事業者の代表者による見直し
   - 罰則
   - 改廃
4. 各部門で取り扱う個人情報を扱う業務の棚卸を行い、「直接収集の場合」「第三者からの間接収集の場合」「公開情報からの間接収集の場合」「預託される場合」に分け、細則を作成。
   - 体制と責任
   - 収集の原則
   - 収集方法の制限
   - 情報主体からの措置

＊監査ガイドラインを想定し、既定する

「個人情報保護細則」で取り上げるべき項目についてキーワード形式でまとめた「規定作成のためのベース表（別表④）」を作成したので、参考にして欲しい。

3.6.7　C チーム　活動総括

2001年10月～11月で計4回の合同ミーティングを実施、参加8社の社内規定策定やプライバシーマーク取得活動の中で情報交換と演習を通じて、それぞれ個人情報保護に関するコンプライアンス・プログラムに対して深い理解が得られたのではないか。

活動の中では、結果的に規定についての考察に終始したが、個人情報保護について適切に企業活動を営んでいくためには、そうした規定の文書化以上に、最初は低いハードルからスタートしても、常にそのレベルを向上させ、改善を重ねていく体制と運用の重要性を学んだ。個人情報保護の基準はそれぞれの職種や利用目的、法制や国際情勢のなかで求められるレベルは折々に変化するので、一定の基準を作ることよりも、それぞれの収集・利用の場における運用のレベルを掌握しておくことが重要である。

個人情報保護法等の整備に伴い、より厳密な遵守への意識が高まり、プライバシーマーク取得を目指す企業が増大するものと考えられる。とりわけ、中小事業者が同マーク取得を考えるとき、そうした法務部門や事務局機能が十分でなく苦心する声もあり、当然ながら効率的にコンプライアンス・プログラムを策定するニーズは高まるだろう。

今後、本活動の延長線上で、遍く企業全般、とりわけ中小の個人情報取扱事業者が、無理なく適切にそうした体制を構築することをサポートするツールを充実させるような取り組みを継続する必要があると考える。

別表①　個人情報保護コンプライアンスマニュアルにおける規定マップ

外部規程 :個人情報保護に関連する本社規程	対応するマネジメント単位組織の規程・ガイドライン・通達	契約書 チェックシート
(101)行動憲章		—
(102)社員行動基準		—
(103)従業員就業規則（罰則はここで定める）		誓約書
(104)企業機密情報管理規程		—
	(201)外部立入禁止区域一覧	—
	(202)○○ビル利用上の注意	社員証による管理
		社員証による管理
(106)文書管理規程		文書管理記録
	(204)ディスク情報の機密漏洩に関する対処について	ディスク廃棄記録帳
(108)コンピュータ・ネットワーク利用管理規程		ネットワーク利用管理者一覧
		—
		—
		独立環境セキュリティチェックシート・利用申請書
		—
		—
		—
(113)ソフトウェア管理規程		—
(114)情報セキュリティ（デジタル情報）管理規程		—
(115)震災対応要領		—
(116)インサイダー取引防止規程		—
(117)外注発注に関する規程		外注取引基本契約書

本社で定める個人情報保護方針を、マネジメント単位の社員等が理解、実行維持するための方策を表す文書。**（スタンダード）**

個人情報保護方針
個人情報保護方針
個人情報保護基本規程
(001)個人情報保護（基本）規程
—(002)解説
—(003)ハンドブック
—(004)個人情報保護ガイドライン

マネジメント単位にとっての「基本規程」は本社規程を流用する。**（ポリシー）**

マネジメント単位のトップ宣言書

マネジメント単位の個人情報保護細則	対応する運用手順書	契約書 チェックシート
		個人情報収集検討依頼書
(302)個人情報保護細則	(401)個人情報保護のための一般手順書（ハンドブック）	**個人情報収集企画シート**
	(402)個人情報預託外注先の選定、登録の手順書	**預託業務シート**
	(403)不正アクセスの防止に関する手順書	**安全対策シート**
	などなど	**個人情報取扱管理シート**
		得意先確認の証（受注にあたって）
	(40X)メニュー別運用手順書	環境状況管理シート
		各メニュー毎の作業手順チェックシート
		承認番号管理台帳
		セキュリティチェックシート
		個人情報の取扱に関する契約書（外注先）
		個人情報の取扱に関する契約書（派遣会社）

マネジメント単位の個人情報保護ガイドライン
(303)個人情報保護に関わるセキュリティガイドライン

基本規程・細則に定められた事項に関して、判断または実施するための指針を示す文書。**（ガイドライン）**
例として、(303)では、個人情報保護のために行う安全対策のガイドラインを載せている。(401)から上げられる運用手順書を各マネジメント単位で作成させていくための指針が必要なものについて作成する。

計画書	チェックシート
(601)システム監査計画書	
(602)教育計画書	

懲戒	
(701)従業員就業規則第○条	

(801)組織図・事業所／作業所図

細則に定められた事項を実施するために、各部門における特定の業務または作業の具体的な手順を定めた文書。
メニュー化されている（繰り返し行われる）業務は、手順書を作成する。
作成した手順書は、関係者への公開や文書管理を容易にするため、システムに登録する。

細則に定められた事項を実施するために、個人情報取扱業務の具体的な手順を定めた文書。
「直接収集」第３者からの間接収集」「預託」に分けて、その「企画」「収集」「利用」「提供」「安全対策」「アクセス権対応」の手順を詳しく決めている。**（プロシージャ）**

全ての使い方は、(401)個人情報保護のための手順書（ハンドブック）に書かれている。
太字のものはシステム化した方が運用が楽である。

参照した個人情報保護に関する業界ガイドライン	策定年月	策定団体
(901)民間部門における電子計算機処理に係わる個人情報保護ガイドライン	H9.3	経済産業省
(902)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	H10.12	総務省
(903)放送における視聴者の加入者個人情報の保護に関するガイドライン	H8.9	総務省
(904)民間部門における電子取引に係わる個人情報の保護に関するガイドライン	H10.3	電子商取引実証推進協議会
(905)電子ネットワーク運営における個人情報保護に関するガイドライン	H9.12	電子ネットワーク協議会
(906)サイバービジネスにおける個人情報の保護に関するガイドライン	H10.12	サイバービジネス協議会
(907)情報サービス産業個人情報保護ガイドライン	H12.5	情報サービス産業協会
(908)マーケティング・リサーチ産業　個人情報保護ガイドライン	H10.12	日本マーケティングリサーチ協会
(909)ダイレクト・メールに関する個人情報保護ガイドライン	H10	日本ダイレクト・メール協会
(910)販売信用取引における電子計算機処理に係わる個人情報保護のためのガイドライン	H10.11	日本クレジット産業協会

別表②　規定の監査シート

大分類	中分類	小分類	要求事項	直接	間接（第3者）	間接（公開）	預託される
個人情報保護方針		事業者の代表者による策定	事業者の代表者名で個人情報保護方針を策定していること	D-001			
			次の事項が含まれていること a)事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること b)個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩などの予防並びに是正に関すること c)個人情報に関する法令及びその他の規範を遵守すること d)コンプライアンス・プログラムの継続的改善に関すること	D-002			
		文書化	個人情報保護方針を書面またはこれにかわる方法で記述していること	D-003			
		役員及び従業員への周知徹底	個人情報保護方針を役員、正社員、派遣社員、非常勤職員に対し周知徹底を定めていること	D-004			
		一般の人が入手可能な措置	外部からの要求に対し個人情報保護方針が明示できること	D-005			
計画	個人情報の特定	個人情報を特定する手順の確立	取り扱っている（予定を含む）個人情報を特定するための手順方法が明確になっていること	D-006			
		個人情報に関するリスクの認識	事業者は、特定した個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩など）の発生の可能性及び影響を認識していること	D-007			
	法令及びその他の規程	法令及びその他の規範の特定と参照手順の確立	コンプライアンス・プログラム作成時に参考とした個人情報保護に関する規格、法令及びその他の規範の最新版を常に参照できる手順を定めていること	D-008			
		法令及びその他の規範を反映する手順の確立	コンプライアンス・プログラム作成時に参考とした個人情報保護に関する規格、法令及びその他の規範の改廃が実施された場合、可及的速やかにコンプライアンス・プログラムや関連社内規程などにその改廃内容を反映する手順を定めていること	D-009			
	内部規程	内部規程の策定と承認	1)個人情報を保護するための内部規程を策定し、事業者の代表者の承認を得るように定めていること	D-010			
			2)内部規程には次の事項が含まれていること a)事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定 b)個人情報の収集、利用、提供及び管理の規定 c)情報主体からの個人情報に関する開示、訂正及び削除の規定 d)個人情報保護に関する教育の規定 e)個人情報保護に関する監査の規定 f)内部規定違反に関する罰則の規定	D-011			
		内部規定の維持管理	内部規定は文書化し、管理ルール（更新、保管、廃棄等）を定めること	D-012			
	計画書	教育計画書の立案と維持管理	1)内部規程を遵守するために必要な教育計画の立案を定めていること	D-013			
			2)教育計画の事項から構成されていること 個人情報保護研修の年間カリキュラム、個別の研修プログラム（研修の名称、開催日時、場所、講師、受講対象者及び予定参加者数、研修の概要、使用テキスト、任意参加可か否かの別など）及び予算など	D-014			
			3)教育計画書は文書化し、管理ルール(更新、保管、廃棄等）を定めていること	D-015			
		監査計画書の立案と維持管理	1)内部規程を遵守するために必要な監査計画の立案を定めていること	D-016			
			2)監査計画は次の事項から構成されていること 当該年度に実施する(個人情報に関する）監査テーマ、監査対処、目的、範囲、手続、スケジュールなどによって構成する	D-017			
			3)監査計画書は文書化し、管理ルール(更新、保管、廃棄等）を定めていること	D-018			
		その他の必要な計画書の立案と維持管理	1)内部規程を遵守するために、その他の計画が必要な場合には、その立案を定めていること	D-019			
			2)その他の計画に必要な事項の構成を明確にしていること	D-020			
			3)その他の必要な計画書は文書化し、管理ルール 更新、保管、廃棄等）を定めていること	D-021			
実施及び運用	体制及び責任	体制及び責任者の設置	1)コンプライアンス・プログラムを効率的に実施するため管理者等を任命すること、及びその役割、責任及び権限を定めている	D-022			
			2)上記規程を文書化し、かつ、個人情報に関連のある業務にかかわる役員及び従業員に周知することを定めていること	D-023			
			3)任命された責任者の役割は明文化され、明確であること	D-024			
		役員及び従業員への周知	個人情報保護の体制及び責任を、個人情報を保護する管理者を任命する等、体制とその責任を定め、個人情報に関連のある業務にかかわる役員及び従業員に周知することを定めている	D-025			
	収集の原則	収集目的の明確化	1)個人情報の収集は、収集に先だってその収集目的を明確に定めるよう規定していること	E-026	F-026	G-026	H-026
			2)収集目的の明確化に当たっては、次のことに配慮すること a)本人から収集する場合、収集目的は、本人との契約などにおいて明示的に了解されるか、又は本人との契約類似の信頼関係の中で黙示的に了解されること b)本人以外の者から収集する場合も、収集する者が収集目的を設定し、収集の相手方との契約などにおいて明示すること c)公開された資料などから収集する場合も、収集する者が収集目的を設定すること d)収集目的を設定するに当たっては、収集した情報の利用及び提供によって情報主体の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにすること	E-027	F-027	G-027	H-027
			3)収集目的は情報主体に理解しやすい内容（文面・文言）にすること	E-028	F-028	G-028	H-028
			4)収集業務が長期継続される場合、当初の収集目的が変更されていないか、見直しを規定すること	E-029	F-029	G-029	H-029
		収集目的の変更	収集目的を変更する規程を策定していること	E-030	F-030	G-030	H-030

大分類	中分類	小分類	要求事項	直接	間接（第3者）	間接（公開）	預託される
実施及び運用	収集方法の制限	収集方法とその実行	1)個人情報の収集は、適法かつ公正な手段によって行うことを定めていること	E-031	F-031	G-031	H-031
			2)業務取扱い基準書により収集方法を、業務ごとに作成し（明文化し）、上長等が承認する規程があること	E-032	F-032	G-032	H-032
		特定の機微な個人情報の収集やその利用及び提供の禁	1)特定の機微な個人情報についての収集の禁止を定めていること	E-033	F-033	G-033	H-033
			2)特定の機微な個人情報についての利用の禁止を定めていること	E-034	F-034	G-034	H-034
			3)特定の機微な個人情報についての提供の禁止を定めていること	E-035	F-035	G-035	H-035
		収集（利用、提供）の禁止の例外事項	1)例外的に特定の機微な個人情報を取扱う場合について、明確に規定していること	E-036	F-036	G-036	H-036
			2)規程は個人情報保護に関するコンプライアンス・プログラムの要求事項に反しない内容であること	E-037	F-037	G-037	H-037
	情報主体から直接収集する場合の措置	情報主体の同意の取得	1)情報主体から直接個人情報を収集する場合、予め情報主体の同意を得る方法や手順を収集の責任者の承認を得るよう定めていること	E-038			
			2)情報主体に通知する次の必要事項を明確にしていること　必要事項 少なくとも次に示す事項または、それと同等以上 a)個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先 b)収集目的 c)個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類（業種）、属性（関連会社、持ち株会社など）及び個人情報の取り扱いに関する契約の有無 d)個人情報の預託（事業者が当該事業者外のものに情報処理を痛くするなどのために自ら保有する個人情報を預けること）を行うことが予定されている場合には、その旨 e)情報主体が個人情報を与えることの任意性（アンケート的なもの）及び当該情報を与えなかった場合に情報主体に生じる結果（例えば、結婚紹介申込書の年収欄を記載しなければ、年収を考慮した相手を紹介しないことなど f)情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果 g)個人情報の開示を求める権利、及び開示の結果、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的方法	E-039			
			3)情報主体の「黙示的な同意の方法」による収集を認める場合を、適切に規程していること	E-040			
		情報主体が子供の場合の同意の取得	1)保護者からの同意を必要とする子どもや、判断力に懸念があると考えられる成人の条件がさだめられていること	E-041			
			2)保護者か同意を取得する方法や手順を定められていること	E-042			
		公開された情報から個人情報を収集する場合	1)公開された情報から個人情報を収集する場合、あらかじめ収集目的を収集の責任者の承認を得るように定めていること	E-043			
			2)収集した情報の利用及び提供によって情報主体の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにするよう規程していること	E-044			
	情報主体以外から間接的に収集する場合の措置	情報主体からの同意の取得	1)情報主体以外から間接的に個人情報を収集する場合、情報主体から同意を得る方法や手順を定めるよう規定していること		F-045	G-045	H-045
			2)情報主体に対して通知する必要事項を明確に定めていること		F-046	G-046	H-046
		情報主体が子供の場合の同意の取得	1)保護者からの同意を必要とする子どもや、判断力に懸念があると考えられる成人の条件を規程していること		F-047	G-047	H-047
			2)保護者から同意を得る方法や手順を規程していること		F-048	G-048	H-048
		同意取得を必要としない間接収集の場合	1)個人情報を直接収集する時点で情報の提供について、情報主体より同意を得ている提供者から収集を行う場合個人情報を間接収集する収集目的が、直接収集時に同意を得ている収集目的の範囲内に限定することを規程していること		F-049	G-049	H-049
			2)個人情報を直接収集する時点で情報の提供について、情報主体より同意を得ている提供者から収集を行う場合情報提供先が、直接収集時に同意を得ている提供先の範囲内に限定することを規程しているこ		F-050	G-050	H-050
			3)情報処理を受託するなどのために個人情報を預託された場合、個人情報を必要とする受託業務や預託範囲などを明確にしていること		F-051	G-051	H-051
			4)情報処理を受託するなどのために個人情報を預託された場合、委託元と個人情報の受取り、利用、返却などのルールや範囲を契約書などで定めることを規程していること		F-052	G-052	H-052
			5)情報主体の保護に値する利益が侵害される恐れのない収集を行う場合、収集目的が情報主体の保護に値する利益が侵害される恐れのない収集について規程していること		F-053	G-053	H-053
	個人情報の利用及び提供に関する措置	個人情報の利用及び提供の原則	1)個人情報の利用および提供する規程を定めていること	E-054	F-054	G-054	H-054
			2)利用及び提供は情報主体が同意を与えた収集目的の範囲内で行うことを定めていること	E-055	F-055	G-055	H-055
			3)利用及び提供の方法を予め定め、責任者の承認を得るように定めていること	E-056	F-056	G-056	H-056
		情報主体の同意を必要としない場合	情報主体の同意を必要としない場合、及びその取扱いの規則（例外条件）を明確に定めていること	E-057	F-057	G-057	H-057

大分類	中分類	小分類	要求事項	直接	間接（第3者）	間接（公開）	預託される
実施及び運用	収集目的の範囲外の利用及び提供の場合の措置	収集目的の範囲外の利用及び提供の規程	1)個人情報の収集目的の範囲外の利用及び提供を行う場合は、必要事項を情報主体に通知し、事前に情報主体の同意を得ることを規定していること	E-058	F-058	G-058	H-058
			2)収集目的の明確化に当たっては、次のことに配慮すること範囲外の利用及び提供を行う場合に、情報主体に通知する必要事項を明確にしていること	E-059	F-059	G-059	H-059
			3)同一企業内の他の部門が、利用の同意を得た個人情報を利用するには、改めて事前の情報主体の同意を必要とすることを明確に規定していること	E-060	F-060	G-060	H-060
	個人情報の適正管理義務	正確性確保のための管理規程類の策定	1)収集目的に応じ必要な範囲内において、個人情報の正確性と最新の状態の維持のために必要な管理規程類を策定していること	E-061	F-061	G-061	H-061
			2)管理規程類には次の事項が含まれていること a)情報システムの運用管理に関する事項 b)情報システムの入出力管理に関する事項 c)情報システムのデータ管理に関する事項 d)委託管理に関する事項	E-062	F-062	G-062	H-062
	個人情報の利用の安全性の確保	安全確保のため管理規程類の策定	1)個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩等）に対して、合理的な安全対策を講じるための管理規程類を作成していること	E-063	F-063	G-063	H-063
			2)管理規程類には次の事項が含まれていること a)入退管理に関する事項 b)アクセス管理に関する事項 c)データ管理（保管、廃棄等）に関する事項 d)委託管理に関する事項	E-064	F-064	G-064	H-064
	個人情報の委託処理に関する措置	委託処理に関する規程の策定	1)個人情報を預託するに十分な個人情報の保護水準を満たしている者を選定する基準を策定していること	E-065	F-065	G-065	H-065
			2)個人情報の預託に際しては、次に示す内容を契約で示すように規程していること a)個人情報に関する秘密保持 b)再委託に関する事項について c)事故時の責任分担 d)契約終了時の個人情報の返却及び消去	E-066	F-066	G-066	H-066
			当該契約書などの書面又はこれに代わる記録を、個人情報の保有期間にわたって保存しなければならない	E-067	F-067	G-067	H-067
	個人情報に関する情報主体の権利	個人情報に関する権利の規定	1)情報主体から自己の情報について開示を求められた場合は、合理的な期間内にこれに応じるように定めていること	E-068	F-068	G-068	H-068
			2)開示の結果、誤った情報があり、訂正又は削除を求められた場合は、合理的な期間内にこれに応じるように定めていること	E-069	F-069	G-069	H-069
			3)訂正又は削除を行った場合は、可能な範囲内で当該個人情報の受信者に対して通知を行うように定めていること	E-070	F-070	G-070	H-070
		本人確認手続きに関する規定	開示要求があった場合、本人確認をする手続きが定められていること	E-071	F-071	G-071	H-071
	個人情報の利用又は提供の拒否権	個人情報の利用又は提供の拒否権の規定	1)事業者が保有している個人情報について、情報主体から自己の情報についての利用又は第三者への提供を拒まれた場合は、これに応じるように定めていること	E-072	F-072	G-072	H-072
			2)個人情報の利用又は提供の拒否権は、次のいずれかに該当する場合は、認められない旨を定めていること a)法令の規定による場合 b)情報主体及び／又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合	E-073	F-073	G-073	H-073
	教育	個人情報保護の教育に関する規定	1)事業者は、役員及び従業員に、個人情報保護に関する適切な教育を行うように定めていること	E-074	F-074	G-074	H-074
			2)教育のカリキュラムには、次の事項が含まれていること a)コンプライアンス・プログラムに適合することの重要性及び利点 b)コンプライアンス・プログラムに適合するための役割及び責任 c)コンプライアンス・プログラムに違反した際に予測される結果	E-075	F-075	G-075	H-075
	苦情及び相談	苦情及び相談の対応に関する規定	1)事業者は、個人情報及びコンプライアンス・プログラムに関して情報主体からの苦情及び相談を受け付けて対応するように定めていること	E-076	F-076	G-076	H-076
			2)苦情及び相談を受け付ける常設の窓口の設置、又は担当者の任命を定めていること	E-077	F-077	G-077	H-077
			3)苦情及び相談の受け付け状況、内容を記録するように定めているこ	E-078	F-078	G-078	H-078
	コンプライアンス・プログラム文書	コンプライアンス・プログラム文書の記述	事業者は、書面又はこれに代わる方法 例えば電子情報など）で、コンプライアンス・プログラムの基本となる要素を記述していること	D-079			
	文書管理	文書管理に関する規定	1)事業者は、この規定が要求するすべての文書を管理するように定めていること	D-080			
			2)コンプライアンス・プログラムの管理ルール（更新・保管・廃棄等）を定めていること	D-081			
監査	監査	監査の実施に関する規定	1)事業者は、コンプライアンス・プログラムがこの規格の要求事項と合致していること、及びその運用状況を定期的に監査するように定めてい	D-082			
			2)監査責任者は、監査を指揮し、監査報告書を作成し、事業者の代表者に報告するように定めていること	D-083			
			3)事業者は、監査報告書を管理し、保管するように定めていること	D-084			
事業者の代表者による見直し	事業者の代表者による見直し	コンプライアンス・プログラム見直しに関する規定	適切な個人情報の保護を維持するために、監査報告書及びその他の経営環境などに照らして、定期的にコンプライアンス・プログラムを見直すように定めていること	D-085			

別表③　個人情報保護基本規程・細則・手順書の項目表

	基本規程（ポリシー）		細則（スタンダード）		手順書（プロシージャ）
総則	1	目的	1	目的	
			2	適用範囲	
	2	定義	3	定義	
			4	ＰＣＭの制定及び見直し（管理責任者）	
保護方針	3	基本方針	5	組織の保護方針をＰＣＭに定めること（管理責任者）	
管理体制	4	個人情報保護統括責任者	6	各基本組織の管理体制をＰＣＭに定めること（管理責任者）	
	5	各基本組織の管理体制			
個人情報等の特定			7	個人情報とリスクの特定手順をＰＣＭに定めること	個人情報とリスクの特定手順
			8	適用法令等の特定・参照手順をＰＣＭに定めること（管理者）	適用法令等の特定・参照手順
収集	6	収集の原則	9	収集のルールをＰＣＭに定めること（管理者）	収集の手順
	7	収集方法の制限			
	8	特定の機微な個人情報の収集の禁止			
	9	直接収集を行う場合の措置			
	10	間接収集を行う場合の措置			
	11	預託される場合の措置			
利用・提供	12	利用・提供の原則	10	利用・提供のルールをＰＣＭに定めること（管理者）	利用・提供の手順
	13	収集目的範囲外の利用、提供の場合の措置			
適正管理	14	個人情報の正確性の確	11	管理のルールをＰＣＭに定めること（管理者）	管理の手順
	15	個人情報の利用の安全性の確保	12	安全対策のルールをＰＣＭに定めること 安全対策の計画書・報告書の作成（安全対策責任者）	安全対策の手順
	16	個人情報の預託に関する措置	13	預託のルールをＰＣＭに定めること（管理者）	預託の手順
情報主体の権利	17	自己情報に関する権利	14	情報主体からの要求への対応のルールをＰＣＭに定めること（管理者）	情報主体からの要求への対応の手順
	18	自己情報の利用及び提供の拒否権			
教育	19	社員に規程に関する教育を行うこと	15	規程･ガイドライン・ＣＰに関する教育を行うこと 社員に規程遵守の重要性等を認識させる手順をＰＣＭに定めること 計画書・報告書の作成（教育責任者）	社員に規程遵守の重要性等を認識させる計画・
苦情・相談	20	苦情・相談への対応	16	苦情・相談対応のルールをＰＣＭに定めること（外部対応責任者）	苦情・相談対応の手順
文書管理			17	文書管理のルールをＰＣＭに定めること（管理責任者）	文書管理の手順
監査			18	ＣＰの運用状況の監査（監査責任者）	監査の計画・手順
見直し	21	規程の見直し（統括責任者）	19	ＣＰの見直し（統括責任者）	

▲ここの雛型についてＣチームで検討しました。

全体に係わる規程として全社を統括するセクションおよび事務局主導で作成していく。

それぞれのセクションから部門推進委員を選出して事務局との調整の上で作成していく。

事務局、部門推進員にさらにセキュリティ対策を立案できる技術者を加えて作成していく。

別表④　規定作成のためのベース表

大分類	中分類	小分類	要求事項	文書番号	キーワード
個人情報保護方針		事業者の代表者による策定	事業者の代表者名で個人情報保護方針を策定していること	個人情報保護方針	
			次の事項が含まれていること	個人情報保護方針	
			a)事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること	個人情報保護方針	
			b)個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩などの予防並びに是正に関すること	個人情報保護方針	
			c)個人情報に関する法令及びその他の規範を遵守すること	個人情報保護方針	
			d)コンプライアンス・プログラムの継続的改善に関すること	個人情報保護方針	
		文書化	個人情報保護方針を書面またはこれにかわる方法で記述していること	個人情報保護方針	
		役員及び従業員への周知徹底	個人情報保護方針を役員、正社員、派遣社員、非常勤職員に対し周知徹底を定めていること	個人情報保護方針 個人情報管理規定	
		一般の人が入手可能な措置	外部からの要求に対し個人情報保護方針が明示できること		
計画	個人情報の特定	個人情報を特定する手順の確立	取り扱っている（予定を含む）個人情報を特定するための手順方法が明確になっていること	個人情報管理規定 個人情報管理運用規定細則 個人情報管理簿	
		個人情報に関するリスクの認識	事業者は、特定した個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩など）の発生の可能性及び☆適正な保護措置を講じない場合の(JISA)影響を認識していること	個人情報管理規定	
	法令及びその他の規範	法令及びその他の規範の特定と参照手順の確立	コンプライアンス・プログラム作成時に参考とした個人情報保護に関する規格、法令及びその他の規範の最新版を常に参照できる手順を定めていること	個人情報管理規定 個人情報保護に係る体制の整備等を示す書類	
		法令及びその他の規範を反映する手順の確立	コンプライアンス・プログラム作成時に参考とした個人情報保護に関する規格、法令及びその他の規範の改廃が実施された場合、可及的速やかにコンプライアンス・プログラムや関連社内規程などにその改廃内容を反映する手順を定めていること	個人情報管理規定	
	内部規程	内部規程の策定と承認	1)個人情報を保護するための内部規程を策定し、事業者の代表者の承認を得るように定めていること	個人情報管理規定	
			2)内部規程には次の事項が含まれていること		
			a)事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定	個人情報管理規定 個人情報管理運用規定細則	
			b)個人情報の収集、利用、提供及び管理の規定	個人情報管理規定 個人情報管理運用規定細則 顧客情報管理規定	
			c)情報主体からの個人情報に関する開示、訂正及び削除の規定	個人情報管理規定 個人情報管理運用規定細則	
			d)個人情報保護に関する教育の規定	個人情報管理規定 個人情報管理運用規定細則	
			e)個人情報保護に関する監査の規定	個人情報管理規定 個人情報管理運用規定細則 内部監査実施基準	
			f)内部規定違反に関する罰則の規定 ☆就業規則に基づき懲戒を行う(JISA)	個人情報管理規定 就業規則(懲戒部分)	
		内部規定の維持管理	内部規定は文書化し、管理ルール（更新、保管、廃棄等）を定めること	規定等管理規定	
	計画書	教育計画書の立案と維持管理	1)内部規程を遵守するために必要な教育計画の☆少なくとも年１回の(JISA)立案を定めていること	個人情報管理規定	
			2)教育計画の事項から構成されていること 個人情報保護研修の年間カリキュラム、個別の研修プログラム（研修の名称、開催日時、場所、講師、受講対象者及び予定参加者数、研修の概要、使用テキスト、任意参加可か否かの別など）及び予算など	個人情報管理運用規定細則 個人情報保護研修計画書 「個人情報保護」社内研修マニュアル	
			3)教育計画書は文書化し、管理ルール(更新、保管、廃棄等）を定めていること	個人情報管理規定 個人情報管理規定 文書取扱規定	
		監査計画書の立案と維持管理	1)内部規程を遵守するために必要な監査計画の☆少なくとも年１回の(JISA)立案を定めていること	個人情報管理規定 個人情報管理運用規定細則	
			2)監査計画は次の事項から構成されていること 当該年度に実施する(個人情報に関する）監査テーマ、監査対象、目的、範囲、手続、スケジュールなどによって構成する	個人情報管理運用規定細則 内部監査計画書	
			3)監査計画書は文書化し、管理ルール(更新、保管、廃棄等）を定めていること	管理規定 管理規定 個人情報管理運用規定細則 文書管理規定	
		その他の必要な計画書の立案と維持管理	1)内部規程を遵守するために、その他の計画が必要な場合には、その立案を定めていること	個人情報管理規定	
			2)その他の計画に必要な事項の構成を明確にしていること		
			3)その他の必要な計画書は文書化し、管理ルール（更新、保管、廃棄等）を定めていること	個人情報管理規定 文書取扱規定	
実施及び運用	体制及び責任	体制及び責任者の設置	1)コンプライアンス・プログラムを効率的に実施するため管理者等を任命すること、及びその役割、責任及び権限を定めている	個人情報管理規定 個人情報管理運用規定細則	
			2)上記規程を文書化し、かつ、個人情報に関連のある業務にかかわる役員及び従業員に周知することを定めていること	個人情報管理規定 個人情報管理運用規定細則	
			3)任命された責任者の役割は明文化され、明確であること	個人情報管理運用規定細則	
		役員及び従業員への周知	個人情報保護の体制及び責任を、個人情報を保護する管理者を任命する等、体制とその責任を定め、個人情報に関連のある業務にかかわる役員及び従業員に周知することを定めている	個人情報管理規定	
	収集の原則	収集目的の明確化	1)個人情報の収集は、収集に先だってその収集目的を明確に定めるよう規定していること	個人情報管理規定	企画内容の検討，企画を確定する前に行う社内会議，収集を開始できる状態，収集の実施，情報主体に対する明示の手順，個人情報の提供を行うことが予測される場合の明示の手順，情報主体から同意を得る手順，情報主体の同意を得る必要がない場合
			2)収集目的の明確化に当たっては、次のことに配慮すること	個人情報管理規定	
			a)本人から収集する場合、収集目的は、本人との契約などにおいて明示的に了解されるか、又は本人との契約類似の信頼関係の中で黙示的に了解されること	個人情報管理規定 個人情報管理運用規定細則	
			b)本人以外の者から収集する場合も、収集する者が収集目的を設定し、収集の相手方との契約などにおいて明示すること	個人情報管理規定	
			c)公開された資料などから収集する場合も、収集する者が収集目的を設定すること		
			d)収集目的を設定するに当たっては、収集した情報の利用及び提供によって情報主体の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにすること		
			3)収集目的は情報主体に理解しやすい内容（文面・文言）にすること		
			4)収集業務が長期継続される場合、当初の収集目的が変更されていないか、見直しを規定すること		
		収集目的の変更	収集目的を変更する規程を策定していること	個人情報管理規定	

大分類	中分類	小分類	要求事項	文書番号	キーワード
実施及び運用	収集方法の制限	収集方法とその実行	1)個人情報の収集は、適法かつ公正な手段によって行うことを定めていること	個人情報管理規定	
			2)業務取扱い基準書により収集方法を、業務ごとに作成し（明文化し）、上長等が承認する規程があること		
		特定の機微な個人情報の収集やその利用及び提供の禁止	1)特定の機微な個人情報についての収集の禁止を定めていること	個人情報管理規定	
			2)特定の機微な個人情報についての利用の禁止を定めていること	個人情報管理規定	
			3)特定の機微な個人情報についての提供の禁止を定めていること	個人情報管理規定	
		収集（利用、提供）の禁止の例外事項	1)例外的に特定の機微な個人情報を取扱う場合について、明確に規定していること	個人情報管理規定	
			2)規程は個人情報保護に関するコンプライアンス・プログラムの要求事項に反しない内容であること	個人情報管理規定	
	情報主体から直接収集する場合の措置	情報主体の同意の取得	1)情報主体から直接個人情報を収集する場合、予め情報主体の同意を得る方法や手順を収集の責任者の承認を得るよう定めていること		
			2)情報主体に通知する次の必要事項を明確にしていること　必要事項：少なくとも次に示す事項または、それと同等以上 a)個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先 b)収集目的 c)個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又は受領者の組織の種類（業種）、属性（関連会社、持ち株会社など）及び個人情報の取り扱いに関する契約の有無 d)個人情報の預託（事業者が当該事業者外のものに情報処理を委託するなどのために自ら保有する個人情報を預けること）を行うことが予定されている場合には、その旨 e)情報主体が個人情報を与えることの任意性（アンケート的なもの）及び当該情報を与えなかった場合に情報主体に生じる結果（例えば、結婚紹介申込書の年収欄を記載しなければ、年収を考慮した相手を紹 f)情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果 g)個人情報の開示を求める権利、及び開示の結果、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的方法	個人情報管理規定	
			3)情報主体の「黙示的な同意の方法」による収集を認める場合を、適切に規程していること	個人情報管理規定	
		情報主体が子供の場合の同意の取得	1)保護者からの同意を必要とする子どもや、判断力に懸念があると考えられる成人の条件がさだめられていること		
			2)保護者か同意を取得する方法や手順を定められていること		
		公開された情報から個人情報を収集する場合	1)公開された情報から個人情報を収集する場合、あらかじめ収集目的を収集の責任者の承認を得るように定めていること	個人情報管理規定	
			2)収集した情報の利用及び提供によって情報主体の受ける影響を予測できるように、利用及び提供の範囲を可能な限り具体的に明らかにするよう規程していること	個人情報管理規定	
	情報主体以外から間接的に収集する場合の措置	情報主体からの同意の取得	1)情報主体以外から間接的に個人情報を収集する場合、情報主体から同意を得る方法や手順を定めるよう規定していること	個人情報管理規定	
			2)情報主体に対して通知する必要事項を明確に定めていること	個人情報管理規定	
		情報主体が子供の場合の同意の取得	1)保護者からの同意を必要とする子どもや、判断力に懸念があると考えられる成人の条件を規程していること		
			2)保護者から同意を得る方法や手順を規程していること		
		同意取得を必要としない間接収集の場合	1)個人情報を直接収集する時点で情報の提供について、情報主体より同意を得ている提供者から収集を行う場合個人情報を間接収集する収集目的が、直接収集時に同意を得ている収集目的の範囲内に限定することを規程していること	個人情報管理規定 個人情報管理運用規定細則	
			2)個人情報を直接収集する時点で情報の提供について、情報主体より同意を得ている提供者から収集を行う場合情報提供先が、直接収集時に同意を得ている提供先の範囲内に限定することを規程しているこ	個人情報管理規定 個人情報管理運用規定細則	
			3)情報処理を受託するなどのために個人情報を預託された場合、個人情報を必要とする受託業務や預託範囲などを明確にしていること	個人情報管理規定 個人情報管理運用規定細則	
			4)情報処理を受託するなどのために個人情報を預託された場合、委託元と個人情報の受取り、利用、返却などのルールや範囲を契約書などで定めることを規程していること	個人情報管理規定 個人情報管理運用規定細則	
			5)情報主体の保護に値する利益が侵害される恐れのない収集を行う場合、収集目的が情報主体の保護に値する利益が侵害される恐れのない収集について規程していること	個人情報管理規定 個人情報管理運用規定細則	
	個人情報の利用及び提供に関する措置	個人情報の利用及び提供の原則	1)個人情報の利用および提供する規程を定めていること	個人情報管理規定 個人情報管理運用規定細則	収集目的の範囲内となる利用であることの確認，利用できる範囲が情報主体によって異なる場合，従事者が追加された場合，提供先企業との契約，情報主体から提供の中止を申し出た場合，
			2)利用及び提供は情報主体が同意を与えた収集目的の範囲内で行うことを定めていること	個人情報管理規定	
			3)利用及び提供の方法を予め定め、責任者の承認を得るように定めていること	個人情報管理規定 個人情報管理運用規定細則	
		情報主体の同意を必要としない場合	情報主体の同意を必要としない場合、及びその取扱いの規則（例外条件）を明確に定めていること	個人情報管理規定 個人情報管理運用規定細則	
	収集目的の範囲外の利用及び提供の場合の措置	収集目的の範囲外の利用及び提供の規程	1)個人情報の収集目的の範囲外の利用及び提供を行う場合は、必要事項を情報主体に通知し、事前に情報主体の同意を得ることを規定して	個人情報管理規定	
			2)収集目的の明確化に当たっては、次のことに配慮すること範囲外の利用及び提供を行う場合に、情報主体に通知する必要事項を明確にし	個人情報管理規定	
			3)同一企業内の他の部門が、利用の同意を得た個人情報を利用するには、改めて事前の情報主体の同意を必要とすることを明確に規定して	個人情報管理規定	
	個人情報の適正管理義務	正確性確保のための管理規程類の策定	1)収集目的に応じ必要な範囲内において、個人情報の正確性と最新の状態の維持のために必要な管理規程類を策定していること	個人情報管理規定	正確性の確保について，安全性の確保について，具体的な安全対策の方法，メンバー以外のものが従事者に含まれる
			2)管理規程類には次の事項が含まれていること a)情報システムの運用管理に関する事項 b)情報システムの入出力管理に関する事項 c)情報システムのデータ管理に関する事項 d)委託管理に関する事項	情報システムの安全対策規定 データ管理規程 不正アクセス対策規定 データ管理規程 外注管理規定	

大分類	中分類	小分類	要求事項	文書番号	キーワード
実施及び運用	個人情報の利用の安全性の確保	安全確保のため管理規程類の策定	1)個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏洩等）に対して、合理的な安全対策を講じるための管理規程類を作成していること	管理規程	
			2)管理規程類には次の事項が含まれていること		
			a)入退管理に関する事項	個人情報管理運用規定細則 入退出管理規定 電算機室管理規定	
			b)アクセス管理に関する事項	不正アクセス対策規定	
			c)データ管理（保管、廃棄等）に関する事項	データ管理規定	
			d)委託管理に関する事項	外注管理規定	
	個人情報の委託処理に関する措置	委託処理に関する規程の策定	1)個人情報を預託するに十分な個人情報の保護水準を満たしている者を選定する基準を策定していること	管理規定 外注管理規定	
			2)個人情報の預託に際しては、次に示す内容を契約で示すように規程していること a)個人情報に関する秘密保持 b)再委託に関する事項について c)事故時の責任分担 d)契約終了時の個人情報の返却及び消去	管理規定 外注管理規定 個人情報管理運用規定細則 個人情報管理運用規定細則 個人情報管理運用規定細則 個人情報管理運用規定細則	
			当該契約書などの書面又はこれに代わる記録を、個人情報の保有期間にわたって保存しなければならない	個人情報管理規定	
	個人情報に関する情報主体の権利	個人情報に関する権利の規定	1)情報主体から自己の情報について開示を求められた場合は、合理的な期間内にこれに応じるように定めていること	個人情報管理規定 個人情報管理運用規定細則	窓口の設置，アクセス権対応方法，開示要求に応じられない場合，第３者への提供の停止を求められた場合
			2)開示の結果、誤った情報があり、訂正又は削除を求められた場合は、合理的な期間内にこれに応じるように定めていること	個人情報管理規定 個人情報管理運用規定細則	
			3)訂正又は削除を行った場合は、可能な範囲内で当該個人情報の受信者に対して通知を行うように定めていること	個人情報管理規定 個人情報管理運用規定細則	
		本人確認手続きに関する規定	開示要求があった場合、本人確認をする手続きが定められていること	個人情報管理規定 個人情報管理運用規定細則	
	個人情報の利用又は提供の拒否権	個人情報の利用又は提供の拒否権の規定	1)事業者が保有している個人情報について、情報主体から自己の情報についての利用又は第三者への提供を拒まれた場合は、これに応じるように定めていること	個人情報管理規定 個人情報管理運用規定細則	
			2)個人情報の利用又は提供の拒否権は、次のいずれかに該当する場合は、認められない旨を定めていること a)法令の規定による場合 b)情報主体及び／又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合	個人情報管理規定 個人情報管理運用規定細則	
	教育	個人情報保護の教育に関する規定	1)事業者は、役員及び従業員に、個人情報保護に関する適切な教育を行うように定めていること	個人情報管理規定 個人情報管理運用規定細則	
			2)教育のカリキュラムには、次の事項が含まれていること a)コンプライアンス・プログラムに適合することの重要性及び利点 b)コンプライアンス・プログラムに適合するための役割及び責任 c)コンプライアンス・プログラムに違反した際に予測される結果	個人情報管理規定 管理運章規定細則	
	苦情及び相談	苦情及び相談の対応に関する規定	1)事業者は、個人情報及びコンプライアンス・プログラムに関して情報主体からの苦情及び相談を受け付けて対応するように定めていること	個人情報管理規定	
			2)苦情及び相談を受け付ける常設の窓口の設置、又は担当者の任命を定めていること	個人情報管理規定	
			3)苦情及び相談の受け付け状況、内容を記録するように定めていること	個人情報管理規定	
	コンプライアンス・プログラム文書	コンプライアンス・プログラム文書の記述	事業者は、書面又はこれに代わる方法（例えば電子情報など）で、コンプライアンス・プログラムの基本となる要素を記述していること		
	文書管理	文書管理に関する規定	1)事業者は、この規定が要求するすべての文書を管理するように定めていること	個人情報管理規定 個人情報管理運用規定細則 文書管理規定	
			2)コンプライアンス・プログラムの管理ルール（更新・保管・廃棄等）を定めていること	管理規定 文書管理規定	
監査	監査	監査の実施に関する規定	1)事業者は、コンプライアンス・プログラムがこの規格の要求事項と合致していること、及びその運用状況を定期的に監査するように定めていること	個人情報管理規定 個人情報管理運用規定細則 内部監査実施基準	
			2)監査責任者は、監査を指揮し、監査報告書を作成し、事業者の代表者に報告するように定めていること	個人情報管理規定 個人情報管理運用規定細則	
			3)事業者は、監査報告書を管理し、保管するように定めていること	個人情報管理規定 文書取扱規定	
事業者の代表者による見直し	事業者の代表者による見直し	コンプライアンス・プログラム見直しに関する規定	適切な個人情報の保護を維持するために、監査報告書及びその他の経営環境などに照らして、定期的にコンプライアンス・プログラムを見直すように定めていること	個人情報管理規定	

4　まとめ

個人情報保護法案の議論を背景に、ここに来てようやくわが国でも欧米なみに個人情報保護の機運が高まってきたが、実際、電子商取引における個人情報の保護の実態を見ても、まだまだ不十分なものと言わざるを得ない。また近い将来、ＥＣの分野では携帯電話を使った商取引、モバイルコマースが急速に発展していくと予想され、新たな対応する必要も出てくると考えられる。

今後、個人情報保護法が成立施行された後は、民間の個人情報取扱事業者に対して、個人情報の取扱の義務規定が課せられ、不正が行われた場合は罰則が課せられるなど、企業活動の中でより慎重な個人情報の取扱が求められることが予想される。またそれに伴い、個人情報保護に対する消費者をはじめとする社会の監視の目が厳しくなるのは間違いなく、企業の個人情報保護の取組み自体がその企業の信頼の判断材料のみならず営業戦略上の対外競争力の重要なポイントともなり、将来的には企業の経営戦略の一要素にも組み込まれていくことになることが予想される。

さらにこの個人情報保護の取組みは現在、政府の e-Japan 構想の中で進められている電子政府のプロジェクトに深い関係があることを見逃してはならない。なぜなら、この個人情報保護法案は 1998 年に改正された住民基本台帳法の施行の前提要件であり、個人情報保護は、2003 年夏から各自治体から配布される住基カードや将来的に配布が検討されている行政マルチＩＣカードの重要な課題の一つである。したがって今後、民間企業が一連の電子政府・電子自治体のプロジェクトに取り組む場合、業務上の個人情報保護は必須の要件であり、その取組みが不十分な企業は、その市場への参入は難しくなってくると思われる。

このように今後、個人情報保護の分野については、電子商取引事業者にとって必然の取組むべき要素である消費者保護、セキュリティの観点から観た考え方と、個人情報保護法を初めとする社会的なインフラの整備を背景に、モバイルコマースや電子政府のような新たなビジネスモデルを構築する上でのアプリケーションの一つとしての考え方の２つの異なった側面からアプローチすることができるのではないかと思われる。

■引用参考記事、資料・文献、ＵＲＬ一覧（順不同、敬称略）

- 情報公開・プライバシーの比較法（堀部政男／日本評論社）
- 個人情報保護法 Q&A（藤田康幸／中央経済社）
- プライバシーマークを取得する方法（鈴木保立／株式会社ＳＣＣ）
- 個人情報と権力（Ｏ．Ｈ．ガンジーＪｒ．／同文舘出版）
- 個人情報保護法制定の方向性（堀部政男／2000 年個人情報をめぐる内外の最新動向講演資料）
- 世界の個人情報保護法（ぎょうせい）
- 個人情報保護－制度と役割－（平松毅／ぎょうせい）
- 個人情報保護基本法制大綱－アメリカ・EU との対比（新美育文／ジュリスト 2000 年 12 月 1 日号）
- インターネット上のプライバシー保護に関する各国の現状（財団法人ニューメディア開発協会／インターネット HP）
  http://www.nmda.or.jp/enc/privacy/privacy-now5_1.html
- ＧＢＤｅ　Consumer Confidence (GBDe／インターネット HP)
  http://consumerconfidence.gbde.org/t_inventory.html
- ＥＵの個人情報保護指令が企業に及ぼす影響と国際調和の可能性（日本貿易振興会）
- 情報化白書 2000（日本情報処理開発協会編／コンピュータ・エージ社）
- 平成 11 年度英国におけるコンピュータへの不正アクセス（クラッキング）と対策に実態調査（情報処理振興事業協会）
- 米国商務省セーフ・ハーバープライバシー原則 vs ＥＵ（小林麻里／個人信用情報専門誌・アイ NO.47）
- EC で取り扱われる個人情報に関する調査報告書 ver.2.0/ver3.0（電子商取引推進協議会）

ほか

■個人情報保護ＷＧ名簿（敬称・役職略、企業名５０音順）

委員　森田　純生	(株)イーアイティー　技術企画部
委員　渡辺　真史	(株)ＮＴＴデータ　開発本部　システム科学研究所
委員　西尾　美和	沖電気工業(株)　ﾈｯﾄﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝｶﾝﾊﾟﾆｰ　ｿﾘｭｰｼｮﾝ企画部
委員　野中　雅彦	近畿日本ツーリスト(株)　営業推進部
委員　大西　雅春	佐川急便(株)　営業本部　商品企画部
委員　菅佐原　健一	(株)シー・アイ・シー　経営企画部
委員　鈴木　幸一	(株)ジェーシービー　コンプライアンス統括部
委員　大西　浩	(株)ダイエーオーエムシー　顧客情報センター
委員　鈴木　靖	大日本印刷(株)　事業企画推進室
委員　高田　荘治	電気事業連合会　情報通信部
委員　祝　　壮吉	東京電力(株)　システム企画部
委員　横田　博行	(株)東芝　法務部
委員　脇田　正敏	トヨタ自動車(株)　国内マーケッティング部
委員　荒木　吉雄	日本アイ・ビー・エム(株)　経営企画・渉外　ﾌﾟﾗｲﾊﾞｼｰ管理担当
委員　尾崎　俊哉	日本アイ・ビー・エム(株)　公共渉外
委員　上野　正之	日本信販(株)　個人情報部
委員　石田　文治	日本電気(株)　ＮＥＣｿﾘｭｰｼｮﾝｽﾞ　ｲﾝﾀｰﾈｯﾄｿﾌﾄｳｪｱ事業部
委員　清水　美和	日本電気(株)　知的財産部　標準化推進部
委員　阪上　正博	日本ユニシス(株)　法務部
委員　橋本　博喜	(株)野村総合研究所　経営コンサルティング２部
委員　立仙　和巳	(株)日立製作所　ﾋﾞｼﾞﾈｽｿﾘｭｰｼｮﾝ事業部　ｺﾝｻﾙﾃｨﾝｸﾞ第五部
委員　赤松　耕治	富士通(株)　法務・知的財産権本部　法務部　法務企画部
委員　牧山　嘉道	マイクロソフトアジアリミテッド　法務本部
委員　東本　謙治	松下電器産業株式会社　情報企画グループ
委員　東山　治郎	松下電器産業株式会社　法務本部　法務グループ
委員　伊東　正晴	三井住友海上火災保険(株)　文書法務部　法務グループ
委員　鳥屋　誠二	三井住友海上火災保険(株)　文書法務部　文書グループ
委員　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　生産推進部

委員　染谷　信年	安田火災海上保険株式会社　法務・コンプライアンス部
委員　中村　卓	(株)ローソン　事業開発本部　サービス事業部

● アドバイザー

堀部　政男	中央大学教授（一橋大学名誉教授）
長谷川　博章	内閣官房　個人情報保護担当室
新田　正樹	内閣官房　個人情報保護担当室
菱山　大	内閣官房　個人情報保護担当室
鈴木　貴詞	経済産業省　商務情報政策局　情報プロジェクト室
関本　貢	(財)日本情報処理開発協会　情報セキュリティ対策室
鈴木　正朝	ニフティ(株)　法務･海外部
合原　英次郎	松下電器産業(株)　東京支社　渉外グループ

● ＥＣＯＭ　事務局

事務局　植原　総一郎	電子商取引推進協議会　主席研究員
事務局　浅沼　省吾	電子商取引推進協議会　主席研究員