第９３回月例研究会

日時　２００２年１２月６日
場所　労働スクエア東京６０１会議室
講演　（財）日本情報処理開発協会
　　プライバシーマーク事務局長
　　関本　貢　氏
演題「プライバシーマーク制度について」
　　（ｎｏ５２６　富山伸夫）

講演要旨

１．個人情報保護の意味

プライバシーと個人情報について考える。プライバシーの概念は、１８９０年代の米国において、私的な事柄の報道が背景となった、「一人にしておかれる権利」であった。これが情報化社会の到来で変化し、「自己に関する情報の流れを自身でコントロールする権利」とされるようになった。

ここで個人情報とは、「個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、又は個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの（当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む)」とされている。

個人情報を巡る問題に目をむけると、事業者により、不正な収集・利用や、誤った処理・破壊・改ざん、紛失などが起きている。これは自己の個人情報を自己がコントロールできていない、即ちプライバシーが侵害された状況である。

こうした状況から、個人情報を本人がコントロールできる環境の提供、即ち個人情報保護の促進として、事業者がプライバシーの侵害に至るリスクに対処することが求められる。

個人情報保護の流れを決めたものとしてＯＥＣＤプライバシーガイドライン（１９８０．９．２３）と、EU 指令の採択（１９９５．１０．２４、発効９８．１０．２５）がある。ＥＵ指令は、ＥＵ諸国と同等の「十分なレベルの保護措置」を講じない第三国への個人データ移転禁止（第２５条）があり、国際的な同調機運を促進した。

わが国の個人情報保護の取組みについては、民間部門が事業者の自主的な取組みを推進し、１９８９年経済産業省の個人情報保護ガイドラインをうけて業界ガイドライン登録制度（１９８９）が始まった。その後１９９８年ＪＩＰＤＥＣプライバシーマーク制度となった。さらに１９９９年コンプライアンス・プログラム要求事項がＪＩＳ化された。

自治体においては、平成１３年４月現在１，９９４団体６０％で個人情報保護条例を施行している。国においては、「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」（平成２年１０月施行）があるが、全体的な「個人情報保護法」は先の臨時国会で不成立となった。

個人情報保護の概念を整理すると、次の８つの原則に集約される。

① 収集制限･･･同意に基づく適正な収集
② データ内容･･･正確性の確保
③ 目的明確化･･･利用目的の明確化
④ 利用制限･･･利用目的による制限
⑤ 安全保護･･･安全性の確保

⑥ 公開･･･透明性の確保
⑦ 個人参加･･･情報主体の権利の確保
⑧ 責任･･･保護システムの構築と運用

２．プライバシーマーク制度の概要

プライバシーマーク制度とは、「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、その証としてプライバシーマークと称するロゴの使用を許諾する制度」である。

その目的としては、事業者には信頼獲得のインセンティブを提供し、消費者には業者の個人情報取扱いの適切性を容易に判断できる材料（マーク）を提供することにある。

この制度を運営する組織は、次の図に示される。
（図ｎｏ１０，ｐ５）

プライバシーマークの付与の対象、付与の単位、認定までの手続き、申請書類、申請から審査までの流れ、認定に係る費用などについては、ホームページ
http://privacymark.jp/appl/proces.html#1
を見ていただければよい。

認定後に消費者からのクレーム等があれば調査を実施し、改善を要請され、従わなければ認定を取り消すことになっている。また、マークの使用については、有効期限が２年間の使用契約（更新継続あり）となっている。

３．個人情報保護のためのマネジメントシステム（ＣＰ）の構築

ＪＩＳＱ１５００１によるコンプライアンス・プログラム（ＣＰ）の基本モデルは、個人情報保護方針と計画（Ｐｌａｎ）、実施及び運用（Ｄｏ）、監査（Ｃｈｅｃｋ）、代表者による見直し（Ａｃｔｉｏｎ）と継続的改善による保護水準の向上を目指す。これには
個人情報保護方針の策定
個人情報の特定（個人情報の洗い出し、リスクの検討、手順の確立）
内部規程（ＣＰの要素）の整備
個人情報保護の体制、権限、責任
個人情報の収集規程
個人情報利用及び提供の規程
個人情報の適正管理の規程
個人情報の開示、訂正、削除の規程
教育・研修規程
苦情及び相談に関する規程
文書管理に関する規程
監査規程
内部規程違反に関する罰則規程
問題発生時の対応規程
などの整備が必要である。

４．個人情報保護のためのマネジメントシステム（ＣＰ）の導入

導入についてはまず、代表者による導入の宣言によって、個人情報取扱い業務に関わる役員及び従業員への意識付けが重要である。また、ＣＰを実施するための資源の確保として、上に決めた内部規程を適用し、リスク評価に基づき総合的な安全措置の構築、能力のある管理者の氏名、教育体

制、苦情相談体制、監査体制を整備する。

導入後は、全てＣＰに基づき運用することとなる。個人情報の収集・利用・提供に関する措置として、Ｗｅｂ上で保護方針の掲示、ＳＳＬの対応、Ｃｏｏｋｉｅ利用の明示などを行う。その他定めた措置を実施して行くわけであるが、最も重要なものには、導入教育の徹底と監査の実施がある。

個人情報保護の実効性確認のためには、導入監査が必要であり、Ｑ＆Ａ方式の調査票などを用いて浸透状況の確認を行う。

さらに、事業者の代表者による見直しとして、監査結果、経営環境などに照らしたＣＰの見直し、監査責任者によるフォローアップが必要である。

５．参考

平成１４年度までの累計でプライバシーマークの認定事業者数は４４９、解除２５を差し引くと有効４２４社となる。事業者の業種で圧倒的に多いのは情報処理サービス業で、他に目立つところとしては人材派遣業、マーケティングリサーチ業、印刷業、学習塾などがある。

（感想）

個人情報保護のためのプライバシーマーク制度が重要な役割を果たし、関係者のご努力の結果、定着してきていることがうかがわれ有意義であった。ここでもシステム監査の役割が重要であることを痛感した。