第 107 回月例研究会報告

NO.1060　太田 香

日　時：2004 年 10 月 29 日（金）18：30 ～ 20：00
場　所：中央大学駿河台記念館　520 号会議室
講　師：経済産業省商務情報政策局　情報セキュリティ政策室　係長　大崎友和氏
演　題：「個人情報の保護に関する法律と経済産業分野を対象とするガイドラインの概要」

●はじめに

2003 年 5 月に成立・公布された「個人情報保護法」が 2005 年 4 月 1 日より全面施行される事になりました。今回の講師である大崎氏の「システム監査人の方々の手助けとなるよう、『どういう想いで、どういう方向にという話を中心に』という視点でお話したい」という言葉で講演が始まりました。当日は各企業のご担当の方々の大いなる期待を反映してか、百余名もの参加者で会議室も満席の状態でした。

●講演内容

1. 諸外国及びわが国における個人情報保護の取り組み
2. 個人情報保護の哲学　～効果的な保護のあり方～
3. 関連動向　～企業を取り巻く環境～
4. 個人情報保護法及びガイドラインの概要

～質疑応答～

1. 諸外国及びわが国における個人情報保護の取り組み

個人情報保護についての各国の取り組みがバラバラであったのを 1980 年、OECD（経済協力開発機構）が「OECD プライバシーガイドライン 8 原則」という形でとりまとめ、指針を示した。

＜ OECD プライバシーガイドライン 8 原則＞
① 収集制限の原則…情報主体への通知または同意が必要なこと。
② データ内容の原則…データが正確、完全、最新であること。
③ 目的明確化の原則…収集目的を明確にし、利用は目的と合致していること。
④ 利用制限の原則…目的外の利用は行わないこと。
⑤ 安全保護の原則…紛失、破壊、不正使用、改竄、漏洩から保護されること。
⑥ 公開の原則…データ収集実施方針の公開、データの存在、目的、管理者を明示すること。
⑦ 個人参加の原則…自己データの内容確認、異議申し立てを保証すること。
⑧ 責任の原則…管理者は諸原則実施の責任を有すること。　（当日配布資料より抜粋）

その後、EU 諸国は 1998 年に発効された「個人情報保護に係る EU 指令」に基づき国内法を改正することを義務付けられ、官民を対象とする包括的な個人情報保護法を保有するに至った。また、米国においては既に「プライバシー法」を 1974 年に成立させ、以降 1980 年～ 1990 年代にかけて「子供のオンラインプライバシー保護法」や「公正信用報告法」など個別分野において法の整備を行ってきた。

ここで我が国の法整備においての適用可能性を考慮したところ、欧州型の理念的な法律を日本においてまともに適用すれば大半の企業が違法状態になってしまい、米国型の個別分野ごとの整備（パッチワーク方式）では、現在生じつつある問題に適切に対処することが出来ないであろうことが予想された。

我が国の取り組みを紹介すると以下の通りである。

「我が国の取り組み」
① 行政機関個人情報保護法制定（1998 年）
② 民間部門の自主的取り組み
③ 住民基本台帳法改正（1999 年）
④ 個人情報保護法の成立（2003 年 5 月）
⑤ 個人情報保護法施行令の成立（2003 年 12 月）
⑥ 個人情報保護の基本方針の閣議決定（2004 年 4 月）
⑦ 各分野ごとのガイドライン作成（2004 年 6 月～）　（当日配布資料より抜粋）

ご覧の通り、我が国では 1990 年代の「② 民間部門の自主的取り組み」の期間が長く中心となり、この間に「通産省ガイドラインの策定」（1989 年）、「プライバシーマーク制度の導入」（1998 年）、「日本工業規格（JISQ15001）の制定」（1999 年）などの動きがあった。また「⑤ 個人情報保護法施行令の成立」において「2005 年 4 月 1 日より施行とする」、「個人情報取扱事業者から除外される者を取扱件数を 5000 件を超えないものとする」など施行日、対象者が具体的に決定された。これを受け、「⑥ 個人情報保護の基本方針の閣議決定」、「⑦ 各分野ごとのガイドライン作成」などの具体的な動きが活発化した。

話はそれるが、経済産業省としては「5000 件」というデータ量は個人情報を取り扱う事業者ならば殆ど含まれるであろうと考えている。また、数あるガイドラインの中では特に「医療分野」、「金融・信用分野」、「情報通信分野」については厳しい取り組みがなされていると受けとめている。

2. 個人情報保護の哲学　～効果的な保護のあり方～

では、「今、なぜ個人情報保護なのか？」という視点から解説する。情報インフラの整備に伴い個人のインターネット利用者が急増してはいるが、「電子商取引」の利用が今ひとつ進んでいない。これは「電子商取引」に対する「セキュリティ上の不安」と「個人情報保護に対する不安」が存在しているからである。まったく身に覚えのない企業から届くダイレクトメール、クレジットカード番号が他人に悪用されるという話、またマスコミで報道されている顧客データの流出事件などの数々の事実が個人のインターネット利用者の不安を掻き立てている。このような状況下では、個人は IT のメリットを十分に享受できないであろう。

「個人が持つ不安をどのように解消するか」という課題と、規制緩和の潮流 (トレンド) において「個人情報の有用性の芽を規制によって摘まないためにはどうすればよいか」という相反しそうな課題を解決する必要がある。そこで「利用目的の公表」などによる「透明性の確保」と、「利用目的の内容は市場の判断に委ねる」という「市場メカニズムの尊重」という 2 大方針を基礎として据えた。言い換えると、「保護と利用のバランスを取る」ということである。その例として、事業者への目的外利用を制限するとともに十分なセキュリティの確保を義務付ける事により「個人の権利利益の保

護」を実現し、代わりに、利用目的自体に制限を加えることはせず、また取得時の本人の同意も不要とすることで「個人情報の有用性」にも配慮した。

また、「実効性を担保する仕組み」の枠組みを用意した。今後、この枠組みに則り、各業界団体での体制が整備されることを期待している。

3. 関連動向　～企業を取り巻く環境～

個人情報保護法施行により、企業は「安全管理措置」義務への早急な対応を求められている。また昨今の CSR（Corporate Social Responsibility 企業の社会的責任）の潮流 (トレンド) や情報漏洩事件の社会的影響を考え合わせると、今後は情報セキュリティへの取り組みが企業の社会的責任の一部となってくる可能性が高いといわざるをえない。

企業に関わる個人情報保護法のポイントは「安全管理措置」義務にあるといえる。個人情報保護法は「個人の権利を定めた法律ではなく、企業の義務を定めたもの」という性格をもつからである。義務に違反した場合は罰則が課せられる可能性もある。

逆に企業が被害者となる場合もある。それは「不正競争防止法」において個人情報が「営業秘密」である場合がこれに該当する。「営業秘密」である要件は ① 秘密管理性 ② 有用性 ③ 非公知性の 3 点である。この要件を満たしている「営業秘密」の情報漏洩が発生した場合において、企業は「不正競争防止法」により保護される立場となる。

参考までに米国の状況を解説する。米国ではエンロン等企業不正会計事件を契機とした法的規制の強化が情報セキュリティ対策の取り組みにも影響を及ぼしている。これは 2002 年 7 月に成立したサーバンスオックスレイ (Sarabanes Oxley) 法において、「企業は会計報告書の作成に関わる全ての情報システムについて、法律が規定する基準を満たす事を保証」しなければならなくなり、結果的に情報セキュリティ対策を強化する必要性に迫られている。また 2001 年の同時多発テロ事件を契機に事業継続計画（BCP）の改善・補強の動きがある。

4. 個人情報保護法及びガイドラインの概要

2004 年 4 月に閣議決定された「基本方針」は各省共通に行うべき取り組みについて定められているに留まっている。そのため、企業が対応を行う際の参考となるようなわかりやすいマニュアル策定が必要と感じた。

そこで経済産業省ではガイドライン検討委員会（委員長・堀部政男　中央大学法科大学院教授）を設け、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を策定した。

当ガイドラインの特徴を以下に列挙すると

1. 経済産業省所管の事業者等が行う取り組みを支援するための具体的指針として策定。
2. 具体的なイメージが持てるよう参考事例を掲載。
3. 従業員の個人情報に関する部分も記述（厚生労働大臣と経済産業大臣の共同作成）。
4. 行政判断の透明性を確保。

（行政による判断を「しなければならない」と明記されたものについてのみとした。）

この講演においては以下の 4 点を抜粋して解説させて頂く。

(1) 個人情報取扱事業者（ガイドライン 4 ページ～）

【事業の用に供しないため特定の個人の数に算入しない事例】として「データセンター（ハウジング、ホスティング）等の事業において当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報」を挙げた。

(2) 安全管理措置（ガイドライン 23 ページ～）

安全管理措置について大切なのは、「組織的安全管理措置における組織体制の整備」がまず第一に挙げられる。

(3) 従業者の監督（法第 21 条）（ガイドライン 33 ページ～）

「従業者」とは、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。この点に注意が必要である。

(4) 委託先の監督（法第 22 条）（ガイドライン 34 ページ～）

「必要かつ適切な監督」については委託者、受託者双方が同意した内容を契約に盛り込むとともに定められた間隔で確認することも含まれる。また、優先的地位にあるものが委託者の場合、受託者に不当な負担を課すことがあってはならない。この文言で現実におこりがちな責任転嫁を防ぎたい。

なお、詳細は以降に紹介するホームページ等を参照して頂きたい。

～質疑応答～

・「『実効性担保の仕組み』にある『認定個人情報保護団体』は現時点で存在するか」

・「個人情報が分散している場合は名寄せして修正にあたらねばならないか」

・「個人情報を取り扱っている部門を子会社化した場合の対応は」

など、具体的な質問が挙げられた。時間上の制約により数点の質疑応答にとどまった。

●おわりに

質疑応答において数々の質問が挙げられた事からも、実務においてはより具体的な判断を要するケースがまだまだ存在するように感じられました。「個人情報保護法の哲学」にて解説された通り、各業界団体判断に委ねられる部分も数多く残されているようです。個人情報保護法が実効性のある法として育っていくためには、各分野におけるご担当の方々の今後のご努力が欠くべからざるものであるという印象を受けました。

現代は情報技術の発展により個人情報の収集、保存、盗用、改竄、破壊がたやすく行える状況にあるといえます。個人が ＩＴ 技術の恩恵をまんべんなく享受できるよう、私たちシステム監査人への期待と、課せられている責務もますます大きくなっていると感じる講演でした。

最後に講演資料に掲載されていた個人情報保護関連資料の参照先を以下に記します。

<http://www5.cao.go.jp/seikatsu/kojin/index.html> （内閣府）

<http://www.meti.go.jp/policy/it_policy/privacy/privacy.htm> （経済産業省）