研究レポート

No.234　July　2005

自治体の IT アウトソーシングと個人情報保護に関する課題と方策

上級研究員　瀧口樹良

富士通総研（FRI）経済研究所

自治体の IT アウトソーシングと個人情報保護に関する課題と方策

上級研究員　瀧口樹良
takiguci@jp.fujitsu.com

（要旨）

- 安全な IT アウトソーシングを実施するためには、委託先の管理を含めた個人情報保護対策を実施することが不可欠な前提条件となる。ところが、自治体の個人情報保護は対応にばらつきが多いのが実態である。個人情報保護対策が十分でないまま IT アウトソーシングを実施すれば、自治体が管理する個人情報が漏えいの危険にさらされることになる。
- そこで、富士通総研では、こうした危険性等を自治体がどのように認識しているかを把握するために、情報セキュリティ大学院大学の協力を得て、全国自治体を対象としたアンケート調査を実施した。その結果として、本来は密接な関係があるべき個人情報保護への対応とアウトソーシングの実施の間には明確な関係性がみられなかった。IT アウトソーシングを全面的に実施していながらも、個人情報保護条例の制定・改正が行われていない自治体も存在していた。
- また、IT アウトソーシングの考え方には、自治体の都市規模によって大きな差があることがわかった。個人情報保護の条例改正やガイドラインの策定については、自治体の都市規模による差があまりみられなかったが、個人情報保護の具体的な対応策を個別に見てみると、自治体の都市規模による差をみることができた。
- IT アウトソーシングを行っている、もしくは行いたいという意向のある自治体では、早急に個人情報保護の条例制定・改正を含めた対応策を取るこが必要である。また、安全な IT アウトソーシングを進めるためには、アウトソーシングのノウハウの乏しい人口規模の小さい自治体に対して、国や都道府県による個人情報保護等に関する支援策が求められる。

（目次）

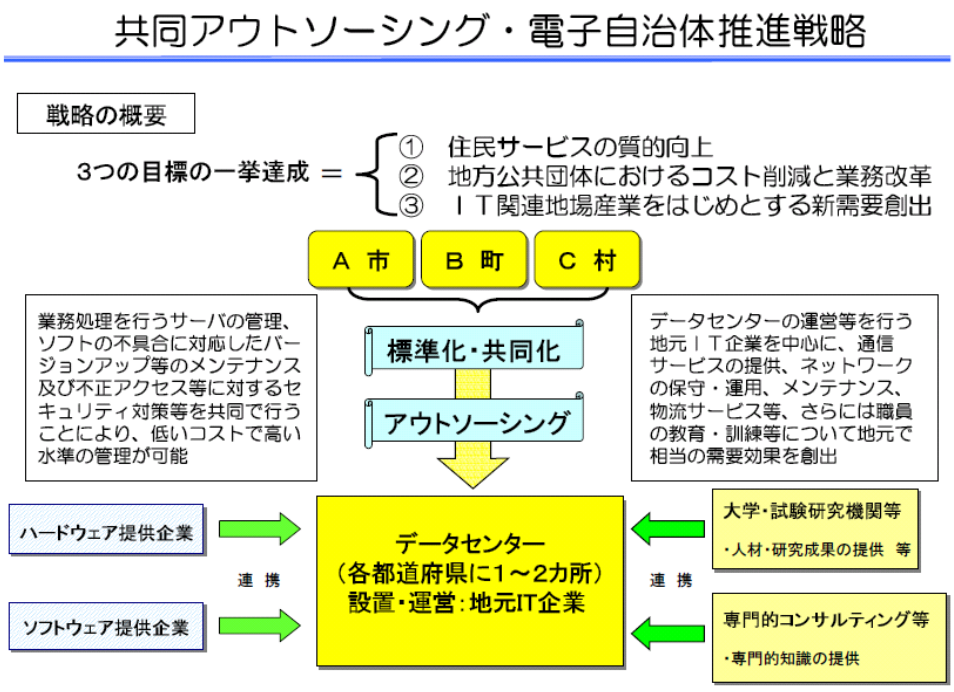
1 自治体の IT アウトソーシング

1.1 電子自治体における IT アウトソーシングの推進

平成 13 年 1 月に「５年以内に世界最先端の IT 国家となる」という目標を掲げた「e-Japan 戦略」が策定されて以来、通信基盤整備、関連法令の整備が行われ、政府自身も電子政府・電子自治体の実現に向けて様々な取組みを進めている。このような行政部門の IT 化の進展に伴い、特に自治体の IT 化を下支えするために、IT のアウトソーシングが検討されており、総務省では「共同アウトソーシング」が推進されている（図表１）。

この計画の中で、具体的な当面の施策としては、①現行の業務・システムについて、EA（エンタープライズ・アーキテクチャ）と呼ばれる手法を用いて政策・業務体系、データ体系を整備すること、②個別パッケージをベースに共同アウトソーシングセンターに移行可能な業務アプリケーションを開発してオープンソース化すること、③開発したプログラムの実証実験を行い、LASDEC（地方自治情報センター）のプログラム・ライブラリに登録すること等があげられている。その上で、将来的な方向性として、共同アウトソーシング・センターでオープンソース化したプログラムの共有、維持管理の枠組みを構築し、その稼動を拡大させることを目標としている。

図表１．共同アウトソーシング・電子自治体推進戦略



（出所）総務省ホームページ

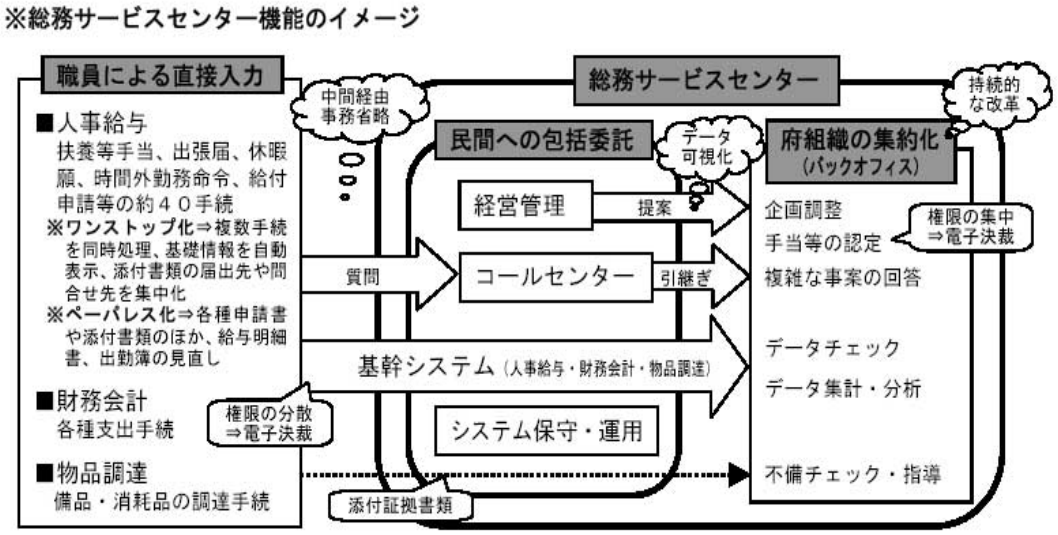
一方、こうした総務省の取組みに先駆けて、IT アウトソーシングに取組んでいる自治体も現れてきている。

たとえば、岐阜県では、地方公共団体としては初めてとなる、戦略的な目的を持ち、長期間にわたる（７年間）「情報関連業務戦略的アウトソーシング契約」（平成１３年度）をＮＴＴコ

ミュニケーションズ株式会社と締結している。この契約は、「電子県庁」への対応を前提に、既存システムの統合等により情報システム関連経費の削減や事務効率の向上を図るほか、アウトソーサーのもつ専門知識やグローバル・ネットワークの活用により県内産業の活性化を図るという戦略的目標を掲げている。また、これにより、約 35 億 7 千万円の経費削減を見込んでいる。アウトソーサーの決定にあたっては、価格と業務のパフォーマンスの両面からベストな選択をするため、価格と提案内容とを総合的に評価する総合評価一般競争入札を採用し、その判定方法は、価格を点数化し、提案内容に対する評価点との合計点により落札者を決定するという岐阜県独自の方式を採用した。さらに業務の品質保持のために 65 項目の客観基準を設定するサービスレベル協定の締結や、アウトソーサーからの有益な提案を業務内容や契約金額に反映させるといった「コ・ソーシング」の考え方[1]も導入し、最善の成果を得るための様々な工夫を凝らしている。

また、大阪府では、民間企業の連合組織に総務サービスセンター事業を外部委託している。この事業は平成 16 年 4 月 1 日に稼動し、出先機関を含む**約 3 万人**の職員にサービスを提供している。このプロジェクトでは、省力化を伴ったオープンなシステムへ移行する方針をとりまとめるとともに、オープンなシステムの運用環境整備や職員認証システムの導入等といったシステムの構築や運用に共通する課題について、共通するハードウェア装置の整備や運用のアウトソーシング手法等の方針をまとめ、業務の効率化を図っている（図表２）。

図表２．大阪府における総務サービスセンターの機能イメージ図

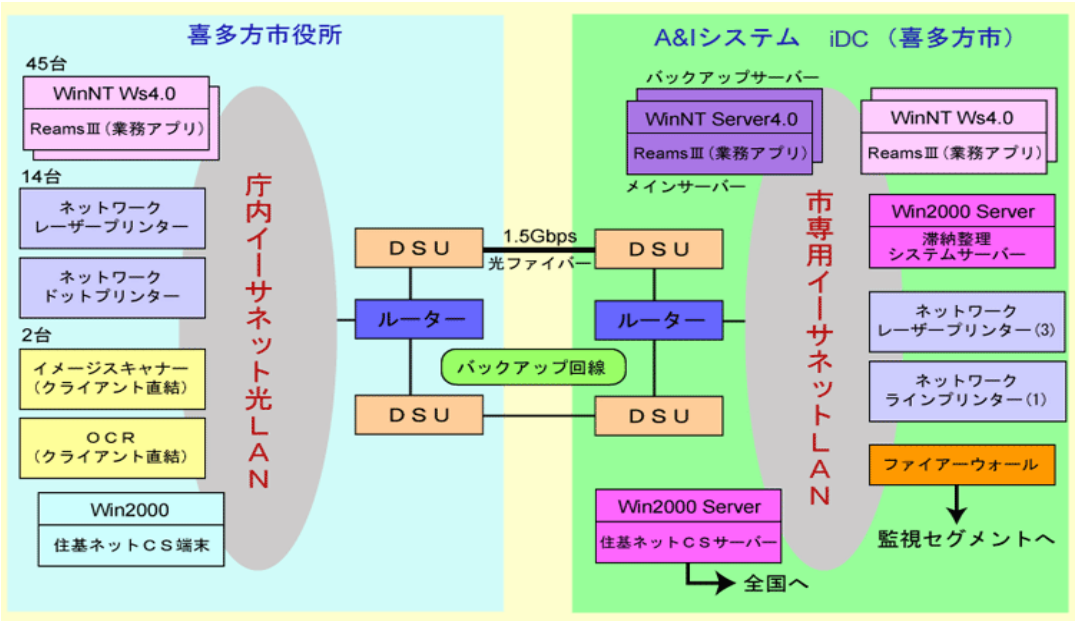


（出所）大阪府ホームページ

さらに福島県喜多方市は、住民登録、国民年金、国民健康保険、各種税金関係等すべての基幹業務システムについて、平成 16 年度中に民間事業者へのアウトソーシングを実施している（図表３）。今回、喜多方市が民間事業者（Ａ＆Ｉシステム㈱）と結んだアウトソーシングの契約金額は 1 年間当たり約 4,750 万円であり、この中にはシステムの保守・

[1]発注先の事業者と委託先であるアウトソーサーとが、一つの目標に向かって、専門的な知恵を集め、共同運営する形態のこと。

図表３．喜多方市のアウトソーシングのイメージ



（出所）日経 BP ガバメントテクノロジー

管理のほか、定例バッチ処理の処理代行、業務Q&A対応等の業務も含まれているという。なお、アウトソーシングの方法としては、Ａ＆Ｉシステムがパッケージ・ソフトウェアをiDC（インターネット・データセンター）で運営・保守をして、喜多方市にＡＳＰサービスを提供するという形となっている。

1.2 IT アウトソーシングの際のセキュリティに関する課題

このように、総務省は自治体における IT アウトソーシングを推進し、実際に情報システムのアウトソーシングを実施している自治体も増えてきた。しかし、IT アウトソーシングにおいては、システムとともに情報の管理を自治体の外部に委託することになり、発注元による管理が外部委託先の民間事業者に対して及びにくいために、自治体自身が情報を管理する場合よりも、構造的にセキュリティに関して脆弱になる危険性がある。具体的には、情報管理に伴うリスクが発注元の自治体から外部委託先の民間事業者に移ったのにも関わらず、発注元の職員に対しては罰則規定や教育研修という管理手段を取ることができるが、外部委託先に対しては管理監督する実質的な手段が取られていない場合が少なくないのが実態である。図表４は、自治体の IT アウトソーシングに伴うセキュリティ面の課題を、発注元（自治体）と委託先（民間企業等）に分けてまとめたものである。

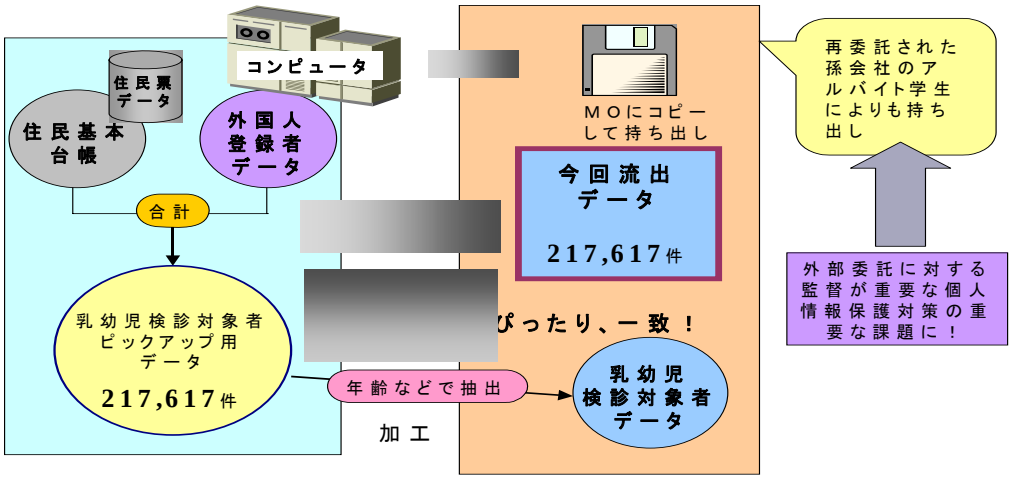
こうした課題が実際に起きた事件として有名なのが、宇治市の住民基本台帳データ漏えい事件である。宇治市では、管理する住民基本台帳のデータを使用して乳幼児検索システムを開発するため、その業務を民間の業者に委託したところ、再々委託先のアルバイト従業員がデータを不正にコピーし販売した。漏えいした個人情報は、個人連番の住民番号、住所、氏名、性別、生年月日、転入日、転出先、世帯主名、世帯主との続柄等がわかるデータ 217,617 件であった（図表５）。この事件では、IT アウトソーシングの際のセキュリティに関する規定類も整備され、取り決められていたのに、それが実際には守られなかった。また、業務の再委託は規定に

図表４．自治体の IT アウトソーシングの際のセキュリティ面の課題

発注元 （自治体側）	・ リスク分析やリスク評価、委託を踏まえた情報セキュリティマネジメントシステムが確立されていない。 ・ アウトソーシングは発注元から委託先へのリスク移転が伴うという認識が不十分である。 ・ リスクレベルに見合ったアウトソーシングについての意思決定がされていない。 ・ 契約後のリスクに対する発注元から委託先への統制力が無くなる。 ・ アウトソーシングすることでの発注者の自己責任放棄による外部委託先への心的圧力の低下。 ・ 意図的および偶発的な人為的事象であるコンピュータセキュリティ・インシデントに対する認識の低さ。
外部委託先 （民間事業者側）	・ リスク分析や情報セキュリティマネジメントシステムが確立されていない。 ・ リスク移転についての認識が不十分。 ・ リスクレベルに見合った意思決定がされていない。 ・ 内部統制力が無い、もしくは低下する。 ・ 再委託によるセキュリティレベルの低下。 ・ セキュリティレベルの維持向上のための努力の継続性欠如。 ・ 意図的および偶発的な人為的事象であるコンピュータセキュリティ・インシデントに対する対応力の低さ。

（出所）日本ネットワークセキュリティ協会の資料

図表５．宇治市の住民基本台帳データ漏洩事件



（出所）藤野（2000）

反することであったにもかかわらず、安易に承諾してしまったことも問題であった。そして、担当者が作業のための時間がなくなったという理由によって、容易にデータの持ち出しを許可してしまったことも個人情報の漏えいに結びついてしまった。

このように、ITアウトソーシングを推進するためにはセキュリティの確保が不可欠であり、自治体では住民の個人情報を扱うことが多いため、個人情報に関するセキュリティ対策が最も大きな課題となる。そこで、次章において、自治体における個人情報保護の取組みについて、まとめることにする。

2 自治体における個人情報保護の取組み

2.1 個人情報保護をめぐる自治体の動き

2003 年 5 月に成立し、2005 年 4 月から完全施行された「個人情報保護 5 法」のうち、行政機関においてもっとも重要な法律は、「個人情報保護法」、「行政機関の保有する個人情報の保護に関する法律」、「情報公開・個人情報保護審査会設置法」の 3 つである。

このうち、まず、「個人情報保護法」では、行政機関や民間企業等が個人情報を取扱うための基本方針を示した上で、国および自治体に対して、個人情報を適正に取扱う施策を策定し、実施する責務を負わせている。さらに、国や自治体において、個人情報保護における問題解決のための苦情処理体制の整備や、相互の協力が必要であることも明記している。

次に、「行政機関の保有する個人情報の保護に関する法律」は、1988 年に制定された「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」を改正したものである。主な改正の内容は、①対象機関を拡大してすべての国の行政機関が対象となったこと、②対象となる個人情報の範囲も拡大し、従来の電子計算機処理情報に加え行政文書（紙文書）に記録されている個人情報も含まれることとなったこと、③個人情報の利用目的を明示し、変更も含めて、その目的を明確化させるようになったこと、④本人関与を強化し、従来の開示請求権に加えて訂正請求権や利用停止請求権が加わったこと、⑤国の行政機関の職員に対する罰則規定が設置されたこと、⑤行政機関が外部委託先への個人情報保護の取扱い監督責任を負うこと等である。さらに、あわせて「情報公開・個人情報保護審査会設置法」が成立したことで、市民が本人関与の権利を行使し、請求した結果、その請求が却下された場合には、その判断の妥当性を「情報公開・個人情報保護審査会」にて審査するという仕組みも整うこととなった。

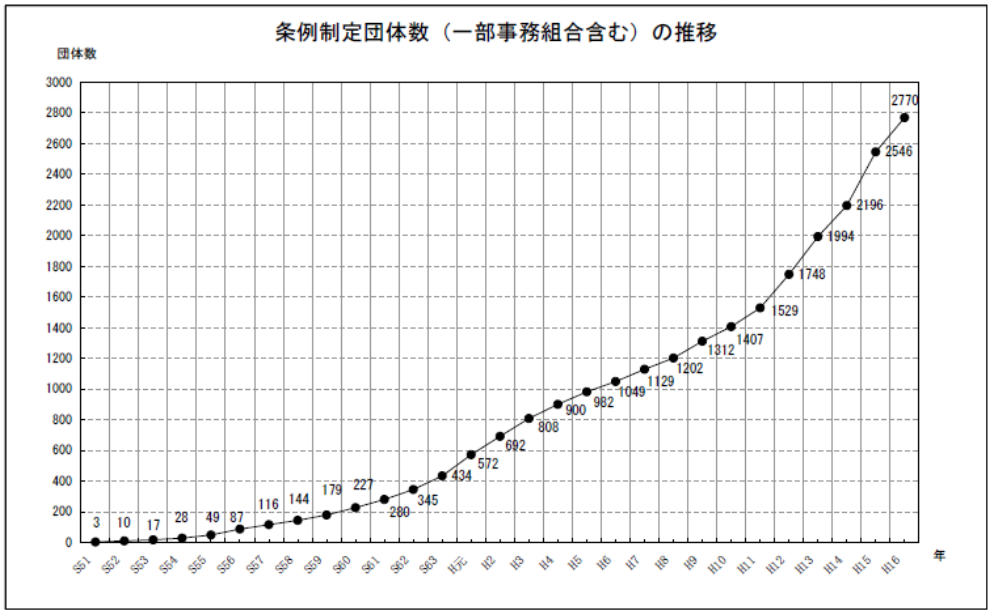
自治体においては、従来から国に先駆けて個人情報保護条例を制定し、市民の個人情報の保護を図ってきたところと、そうでないところでばらつきがあった。例えば、個人情報の保護に関する条例を制定している都道府県・市区町村は、2,612 自治体（82.4%）年々増加している（平成 16 年 4 月 1 日現在総務省調べ）。具体的な制定団体数でみると、都道府県・市区町村全 3,170 団体中 2,612 団体で、前年度（2,413 自治体）から 199 団体増加しており、制定率は 82.4%で、前年度（74.0%）から 8.4 ポイント増加している。また都道府県、政令指定都市及び特別区はすべて制定済みで、市区町村は全 3,123 団体中 2,565 団体（82.1%）が制定済みである。なお、一部事務組合等においても 158 団体が個人情報の保護に関する条例を制定しており、都道府県・市区町村と合わせると、2,770 団体となる（（図表 1）。

条例の規定内容についてみると、次のような傾向となっている。

- 処理形態の範囲が、電子計算機処理のみの対象からマニュアル処理も対象とする規定が増加（342 自治体増、6.9 ポイント増）
- 他の機関とのオンライン結合を全面禁止とする規定が減少（18 自治体減、0.8 ポイント減）
- 自己情報の開示・訂正等に関する規定が増加（特に利用中止請求に関する規定が増加）
- 外部委託時の規制に関する規定が増加（264 自治体増、2.0 ポイント増）
- 罰則に関する規定が増加（218 自治体増、7.1 ポイント増）
- 申出等への措置（苦情処理、不服申立手続）に関する規定が増加（334 自治体増、6.4

ポイント増）

図表６．条例制定の自治体数の推移



（出所）総務省ホームページ

2.2 民間事業者に対する制限

IT アウトソーシングとの関連では、個人情報保護の中でも民間事業者等に対する規定が重要になるが、2004 年 4 月 1 日現在、個人情報保護条例を制定した自治体のうち約 60%の自治体が、条例の中で民間事業者の個人情報保護対策に対する努力や協力を求めている。しかし、その中で監視や指導体制に関する具体的な規定を設けている自治体は、全体の 20%程度にすぎない。その上、民間事業者の罰則規定も盛り込んでいる自治体は 16%となり、条例が必ずしも事故抑止効果を持ったものであるとはいえないのが現状である。図表 7 は、自治体における個人情報保護に関する民間事業者に対する制限項目の規定状況をまとめたものである。

自治体の個人情報保護条例は、国が制定した個人情報保護関連５法を基本に、自治体ごとに具体的に運営していく上での規定や、マニュアルを設ける等して制定されている。そのため、図表 7 からも明らかなように、自治体によっては民間事業者に対する具体的な規定等が明示されていないところも少なくない。その一方で、いくつかの自治体ではセキュリティや民間事業者に対する規定やマニュアル等を設けている。

例えば、三鷹市では 2005 年 1 月 26 日に都内の自治体では初めて、情報セキュリティマネジメントシステムの国際的な規格である「BS7799-2：2002」と国内の標準規格である「ISMS 認証基準 Ver.2.0」の２つの認証を同時に取得し、個人情報保護条例をはじめ、「住民基本台帳ネットワークシステムセキュリティ対策基準」、「同システム障害対策マニュアル」、「同システム不正アクセス行為対応マニュアル」、「同システム情報漏洩事故等対応取扱要領」に基づき、厳格な運用を行っている。個人情報保護条例の中には事務を外部委託したときの規定が設けられており、罰則規定として、法人の代表者や従業者等が違反行為をしたとき、行為者を罰するほ

図表７．自治体の個人情報保護に関する民間事業者に対する制限項目

規制事項	詳細項目
事業者の責務に関する項目	・事業者の責務に関する努力規定がある自治体（55.6%） ・自治体が講ずる保護対策に協力する責務を事業者が有する旨の規定がある自治体（48.7%）
適用上の注意に関する項目	・不当に事業者の権利と自由を侵害することがないよう、保護条例の取扱に当たって注意を促す規定がある自治体（4.6%）
事業者に対する規制に関する項目	・事業を遂行する上での自主的規制の指導や助言等の規定がある自治体（20.6%） ・事業者が講じるべき保護対策の指針を作成する旨の規定がある自治体（3.0%） ・事業者の個人情報の保有状況、取扱方法の概要等を地方公共団体が備える登録簿に登録し、これを住民に公開する旨の規定がある自治体（0.4%）
自治体の監視体制に関する項目	・事業者がその責務規定等に違反するおそれがある場合等に、事業者に対し資料提供・調査・立入調査等への協力を要請する旨の規定がある自治体（19.2%） ・事業者がその責務規定等に違反していると認められる場合等に、当該行為の是正、中止等について指導・勧告を行うことができる旨の規定がある自治体（23.2%） ・事業者が資料提供・調査・立入調査等の協力要請や指導・勧告に従わない場合に、当該事業者名やその経緯を公表できる旨の規定がある自治体（20.5%）
苦情処理相談窓口等に関する項目	・事業者の活動に起因する個人情報に係る人格的利益の侵害に関する住民の苦情に対応するため、自治体内に苦情相談窓口を置く等の規定がある自治体（14.7%）

（出所）総務省ホームページ

か、法人に対しても罰金刑を科すことが規定されている。さらに、事故等に関する脅威度のレベル区分を行い、具体的に事故等が発生した場合の対応や事故原因に関する調査等についてマニュアル等で明確にしている。

また、杉並区の個人情報保護条例の改正では、区内事業者への支援、苦情処理のあっせん、外部提供先に対する措置請求、事故情報の開示請求手続き等に関する規定の整備が行われ、2005 年 4 月 1 日から施行された。その中で、民間事業者に対する外部委託に関する規定については、改正に伴い指定管理者も加えられており、さらに杉並区が出資その他財政支出を行う法人、団体も外部委託先と同様の措置をとることを規定している。

さらに仙台市では、『せんだい IT アクションプラン』を設けて情報化推進施策を実施することによって、『情報自在都市・仙台』を構築することを基本目標に掲げている。その中で、個人情報保護、情報セキュリティの向上・啓発を重点施策のひとつに上げている。また、市民税課税データの紛失事件をきっかけとして、2003 年には外部委託者に関するガイドラインを制定し、①契約の際に業者の信用性をチェックすること、②セキュリティ研修の義務化を行うこと、③委託期間中における立入り調査を実施すること等、効果的な多段階のセキュリティチェックを行っている。

横須賀市でも、国内初の電子入札実施、自治体初の情報技術部門における ISO9001 取得、IC カードの活用等行政情報化の分野での先進的な取組みを通して、住民満足度向上のための IT

利用と行政改革を進めている。その中で、横須賀市は、情報マネジメントの体系の中でセキュリティを捉えており、2004 年度に改正された個人情報保護条例では、受託業務従事者及び指定管理業者に対する罰則規定を置き、更に再委託以下の業務従事者に対しても罰則の適用対象としている。また個人情報の取扱いを伴う外部委託に関しては、市長への届け出を要し、これを情報公開し、この届け出を個人情報保護運営審議会に報告するものと規定されている。さらに、受託業務従事者及び指定管理業者が個人情報の不適切な取扱いにより情報を第三者に漏えいした場合、事実の公表をすることを規定している。

このように、一部の自治体では、個人情報保護における民間事業者に対する制限や管理対応の動きが広がってきているものの、多くの自治体では個人情報に関するセキュリティ対策が不十分なままで、IT アウトソーシングが推進されようとしている。このため、自治体における IT アウトソーシングと個人情報保護の状況についての実態を把握し、安心した IT アウトソーシングの促進を図るための対策を検討することが求められている。

3 自治体 IT アウトソーシングと個人情報保護の実態

3.1 調査の概要

富士通総研では、情報セキュリティ大学院大学の協力を得て、全国自治体を対象として IT アウトソーシングと個人情報保護に関するアンケート調査を実施した。調査の設計は、次のとおりである。

・対象自治体：都市規模別に 1,039 自治体を層化抽出（抽出率 35.4%）
抽出方法は図表８のとおり。

図表８．調査対象の人口区分別内訳

	母数	抽出結果（発送数）	抽出率
都道府県 47、特別区 23、13 政令市	82	82	100%
上記を除く人口 20 万人以上の自治体	94	94	100%
上記を除く人口５万人以上 20 万人未満の自治体	363	363	100%
人口１万人以上５万人未満の自治体	1,118	250	22%
人口１万人未満の自治体	1,281	250	20%
合計	2,938	1,039	

（出所）富士通総研作成

・調査対象者：自治体の情報システムを企画あるいは運用管理している部門の担当者。
なお、個人情報保護に関する質問については、「情報システム担当部門でご回答いただけない場合、個人情報保護施策担当部門にてご回答ください」と記載した。
・調査方法：質問紙郵送法（郵送による調査票を配布し、回答はＦＡＸにより回収）
・実施時期：2005 年 1 月 17 日（月）～2 月 14 日（月）

・「アウトソーシング」の定義：継続的に発生する庁内の業務について、管理責任を含めて外部に委託すること。

・ 調査項目：

０．基本属性（自治体名、部署名・担当者役職等、都市規模、人口規模）

Ⅰ．現在における貴団体の情報化の状況

問 1. 現在稼動しているコンピュータ（ハードウェア）の運用形態

問 2. 現在稼動しているシステム（ソフトウェア）の開発形態

問 3. 現在稼動しているシステムの運用・管理形態

問 4. 平成 16 年度及び平成 17 年度（予定）の歳入金額と電算費用

Ⅱ．今後における貴団体の情報化の状況

問 5. 今後のコンピュータ（ハードウェア）の運用形態

問 6. 今後のシステム（ソフトウェア）の開発形態

問 7. 今後のシステムの運用・管理形態

問 9. 情報化投資に関する経営層の関心（現状と３年前の状況）

Ⅲ．アウトソーシングについて

問 10. 情報システム分野におけるアウトソーシングの考え方

問 11. アウトソーシングを行っているもの

問 12. 貴団体の主なアウトソーシング先

問 13. アウトソーシングの活用についての目的・効果

問 14. アウトソーシングの活用についての問題点・課題

問 15. アウトソーシングの活用に関する経営層の関心

問 16. アウトソーシングに対する意見・要望

Ⅳ．市町村合併への取組み

問 18. 合併検討に伴う情報システムの統合について

問 19. システム統合の実施・検討におけるシステム統合の形態

問 20. システム統合の実施・検討にあたり併せて行う施策

問 21. システム統合の実施・検討に伴う個人情報保護に関する対策

Ⅴ．個人情報保護対策について

問 22. 個人情報保護条例の制定状況

問 23. 個人情報保護方針やセキュリティに関するガイドラインの制定状況

問 24. 個人情報保護の対策

問 25. 個人情報保護対策についてのアウトソーシング先に対する対策

問 26. 個人情報保護対策についての支援要望

問 27. 個人情報保護対策費用

問 28. 個人情報保護に関する経営層の関心

問 29. 個人情報保護対策に対する意見・要望

Ⅵ．ご意見・ご要望

問 30. アウトソーシングにおける個人情報保護対策に関する意見

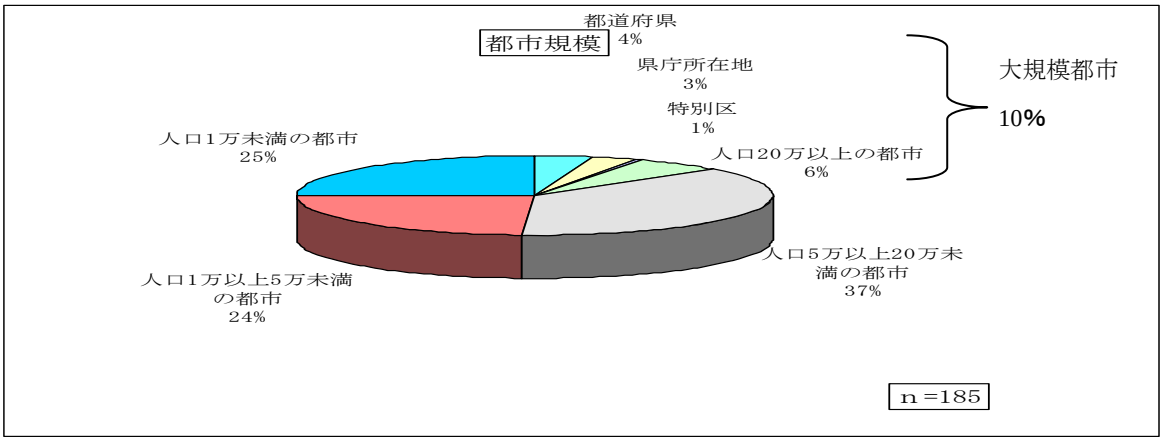
問 31. アウトソーシングにおける個人情報保護対策（アウトソーシング先に対して）

に関する意見

（問 9、13、14、15、24、28 の設問項目は、4 段階のスケールで測定した。）

有効回答の回収は 185 自治体で、回収率は 17.8%であった。一般的な自治体調査では回収率が 3 割程度を越すことが多いが、本調査では、回収率が 17.8%と低くなった。これは、アンケートの設問内容自体が、自治体の答えにくい設問が多く含まれていたためと考えられる。また、回答のあった 185 自治体の都市規模別の分布は、図表 9 のとおりである。

図表 9 ：アンケート回収自治体の規模



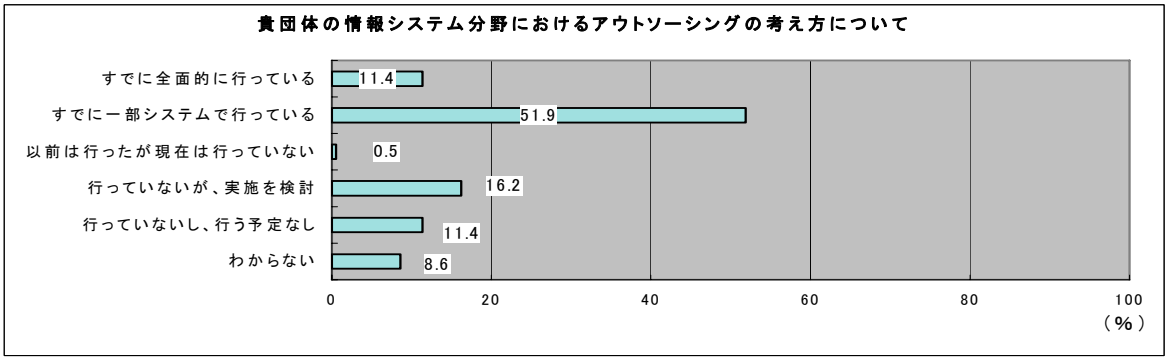
（出所）富士通総研作成

3.2 調査結果の概要

3.2.1 自治体の IT アウトソーシングの考え方

51.9%の自治体では一部システムのアウトソーシングを行っており、11.4%の自治体では全面的にアウトソーシングを行っている（図表 10）。実施を検討中の自治体も含めると、アンケートに回答した自治体のうちの 80%近い自治体が、IT 分野においてアウトソーシングをすでに実施または今後実施予定であることになる。

図表 10：自治体の IT アウトソーシングの考え方（問 10）



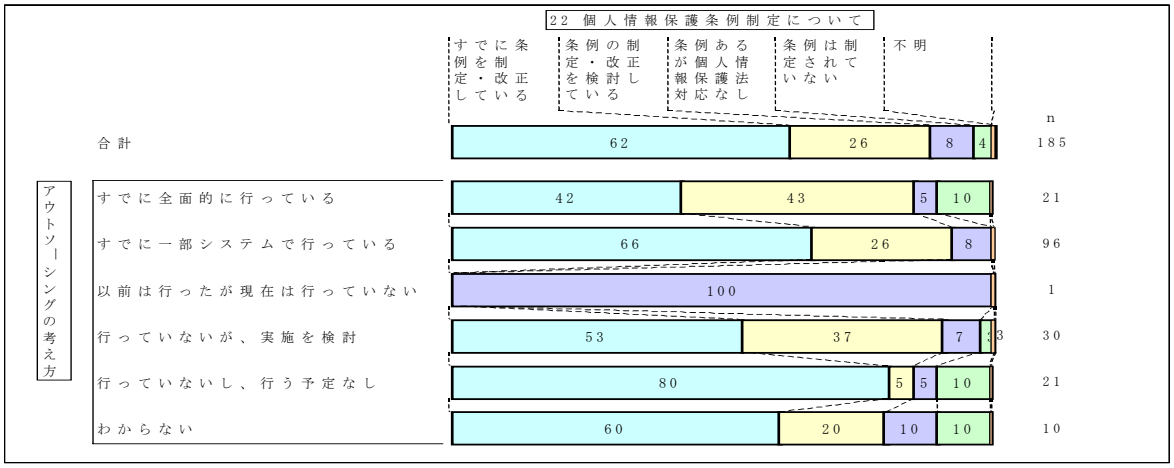
（出所）富士通総研作成

3.2.2 アウトソーシングの状況と個人情報保護条例等制定との関係

IT アウトソーシングと個人情報保護条例制定との関係を見てみると、すでにアウトソーシングを行っている自治体のうち、すでに個人保護条例を制定・改正している自治体は 42%で

ある。しかし、アウトソーシングを行っていないし、行う予定がないと回答している自治体のうち、すでに個人保護条例を制定・改正している自治体は 80%であり、アウトソーシングを行っていない自治体の方がアウトソーシングを実施している自治体よりも、個人情報保護条例を制定している比率が高くなっている（図表 11）。本来であれば、個人情報保護条例の制定は安全な IT アウトソーシングのための必要条件であると考えられるが、現実にはそのような関係がないことがわかる。

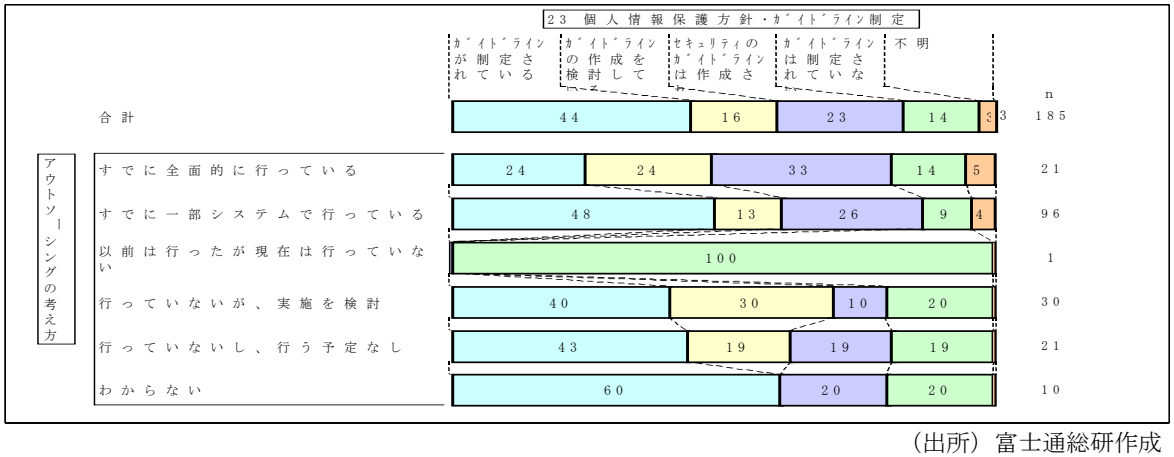
図表 11：アウトソーシング状況別個人情報保護条例制定の状況（問 10×問 21）



（出所）富士通総研作成

IT アウトソーシングと個人情報保護方針及びガイドライン制定との関係を見ても、アウトソーシング実施済みの自治体のうちガイドラインを制定しているのは 24%で、アウトソーシングを行っていないし、行う予定がないと回答している自治体のうちガイドラインを制定している自治体は 43%で（図表 12）、関係は事前の想定と逆になっている。

図表 12：アウトソーシング状況別個人情報保護方針及びガイドライン制定の状況
（問 10×問 23）



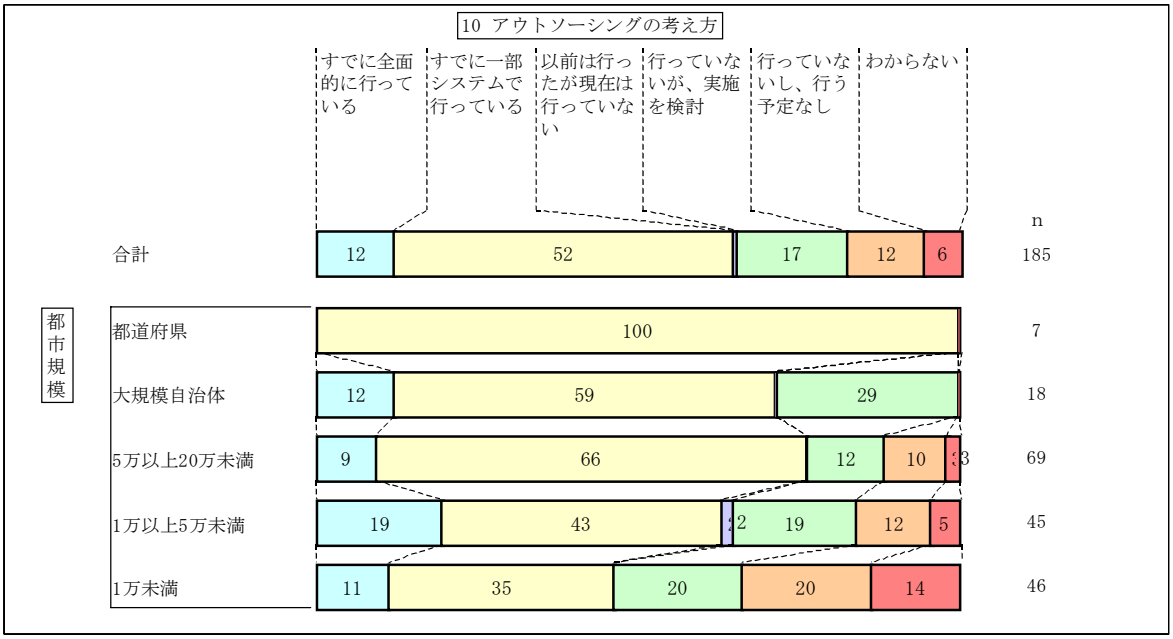
（出所）富士通総研作成

3.2.3 都市規模と IT アウトソーシングの関係

IT アウトソーシングの実施と個人情報保護に関する取組みとの間に関係がない原因を明ら

かにするために、都市規模別にITアウトソーシングの実施状況を集計したのが図表13である。ITアウトソーシングを「すでに全面的に行っている」と「すでに一部システムで行っている」をあわせた数字は、都道府県で100%、大規模自治体で71%であるのに対して、都市規模の小さな1万未満の自治体では 46%と、大規模な自治体ほどアウトソーシングの意向が高く、小規模自治体では低くなっている。アウトソーシングは外部の専門知識を獲得しやすく、情報システム関連業務は規模の経済性も働きやすいため、本来であれば、IT 関連の専門家を内部で抱えることが困難で、情報システムの規模も小さい小規模自治体ほど、IT アウトソーシングの恩恵を受けやすいはずである。しかし、現実には逆になっている。

図表13：都市規模別のITアウトソーシングの考え方（都市規模×問10）

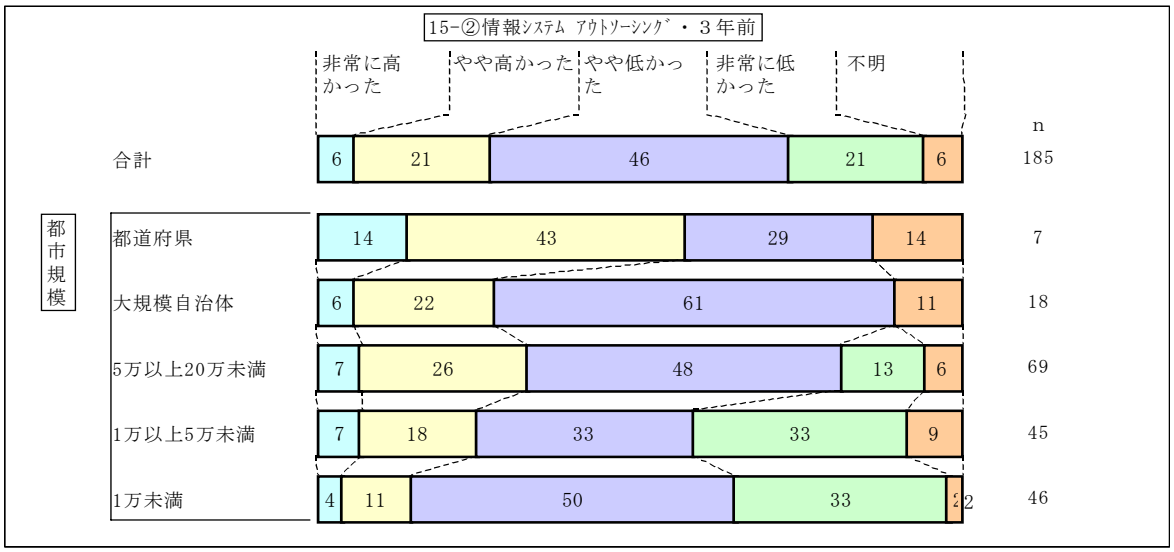


（出所）富士通総研作成

図表14と図表15は、自治体の経営層（主に首長および助役、出納役の3役）のアウトソーシングに関する関心について、現状と3年前の水準を集計したものである。3年前の状況では、「非常に高い」と回答した自治体は、都道府県で14%、大規模自治体で7%に対して、小規模自治体である1万未満の自治体ではわずか 4%であった。一方、現状では、「非常に高い」と回答した自治体は、都道府県で29%、大規模自治体で22%に対して、小規模自治体である1万未満の自治体では 7%である。小規模自治体においても IT アウトソーシングに対する関心は高まっているものの、依然としてその水準は低いレベルにある。

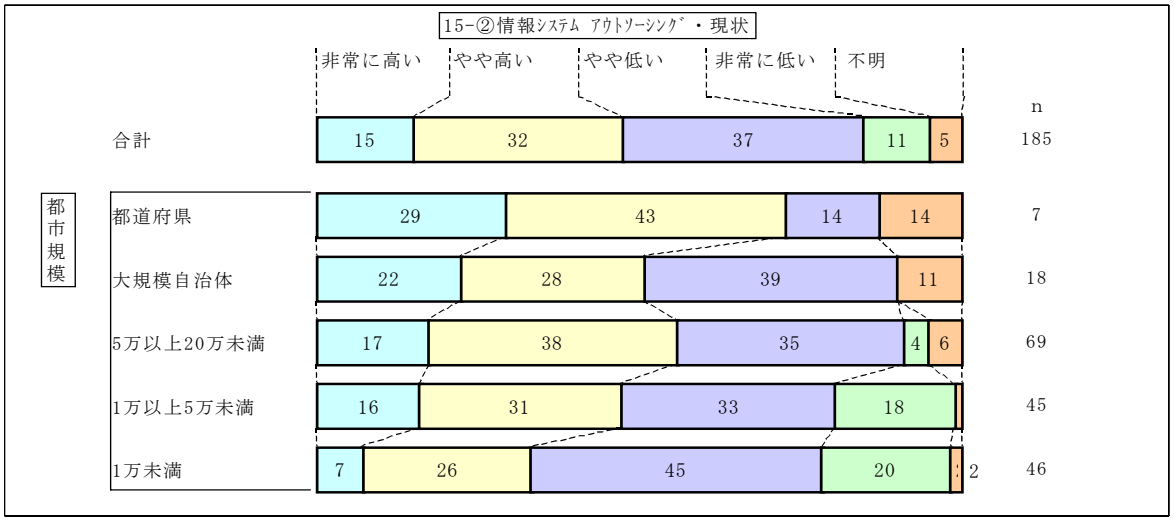
これらの集計結果から、本来であればメリットを享受しやすい小規模自治体ほど IT アウトソーシングに消極的であり、その主な理由は経営層の関心が低いからだということがわかる。

図表 14：３年前の情報システムの民間へのアウトソーシングに関する関心
（都市規模×問 15①３年前）



（出所）富士通総研作成

図表 15：現状の情報システムの民間へのアウトソーシングに関する関心
（都市規模×問 15②現状）



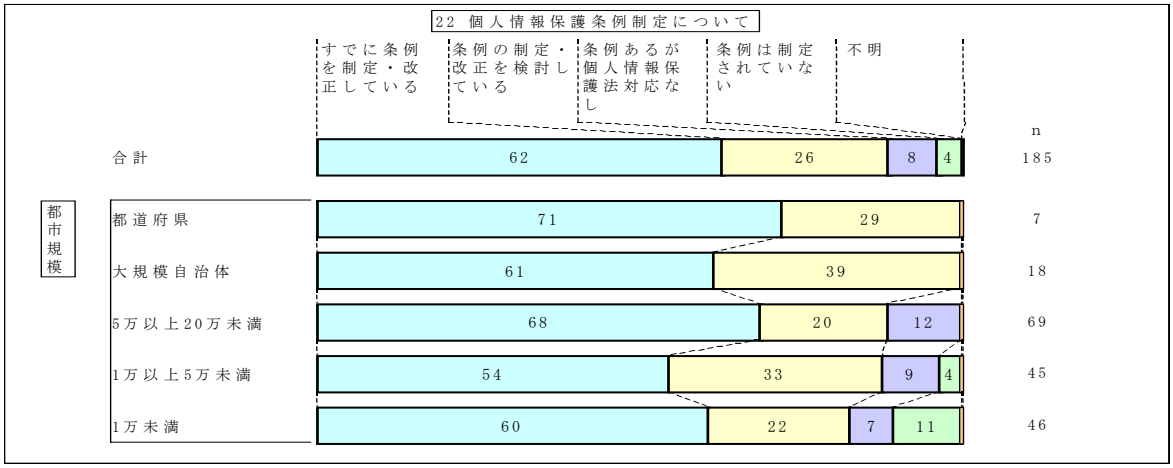
（出所）富士通総研作成

3.2.4 都市規模と個人情報保護対策の関係

次に、都市規模別に個人情報保護対策の状況を集計してみると、たとえば、「すでに個人情報保護条例制定・改正している」のは、都道府県で 71%、大規模自治体で 61%であるのに対して、都市規模の小さな 1 万未満の自治体で 60%であり、差があまり見られない（図表 16）。

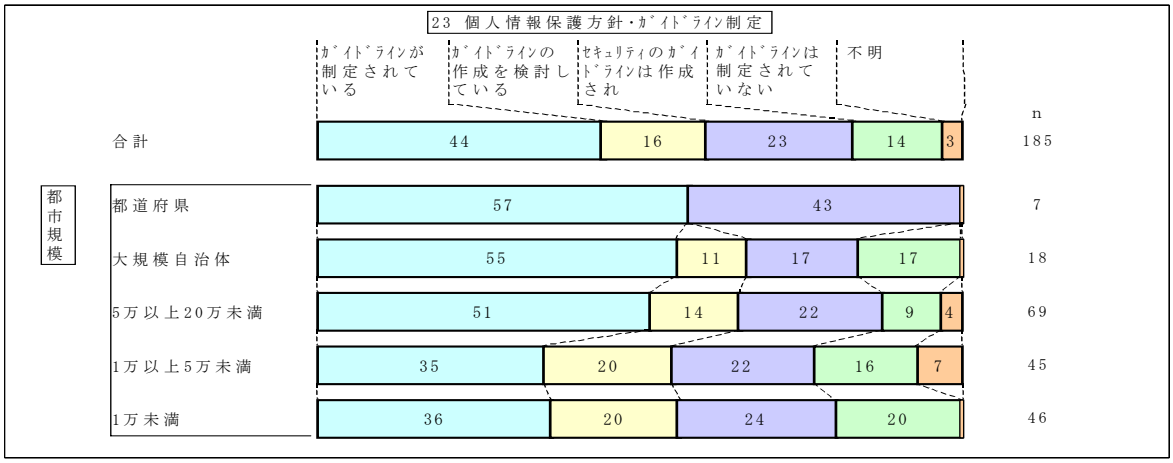
ところが、具体的な個人情報保護方針・ガイドラインの制定状況を見てみると、「ガイドラインが制定されている」のは、都道府県で 57%、大規模自治体で 55%であるのに対して、都市規模の小さな 1 万未満の自治体では 36%であり、大規模自治体ほどガイドライン等の具体的対応策を決めているが、小規模自治体ほどそうした具体的な対応策が決められていないという傾向がある（図表 17）。

図表 16：都市規模別個人情報保護条例制定状況（都市規模×問 22）



（出所）富士通総研作成

図表 17：都市規模別個人情報保護方針・ガイドラインの制定状況（都市規模×問 23）

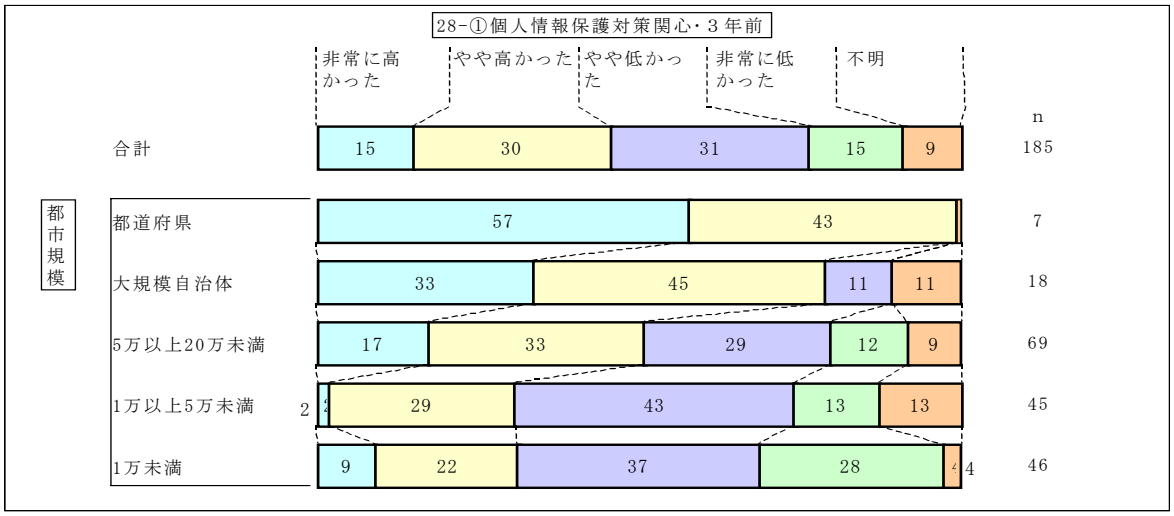


（出所）富士通総研作成

個人情報保護対策に関する自治体経営層の関心は、IT アウトソーシングに対する関心と同じように、３年前と比べれば高くなっている。３年前の状況について、関心が「非常に高い」と回答した自治体は、都道府県で 57%、大規模自治体で 33%、人口１万未満の自治体では 9%であった。一方、現状では、「非常に高い」と回答した自治体は、都道府県で 71%、大規模自治体で 55%、人口１万未満の自治体では 20%であった。IT アウトソーシングと同じように、個人情報保護についても小規模自治体ほど経営層の関心は低いが、それでも人口１万人未満の自治体の２割が「非常に高い」と回答しており、IT アウトソーシング（7%）との違いは歴然としている。

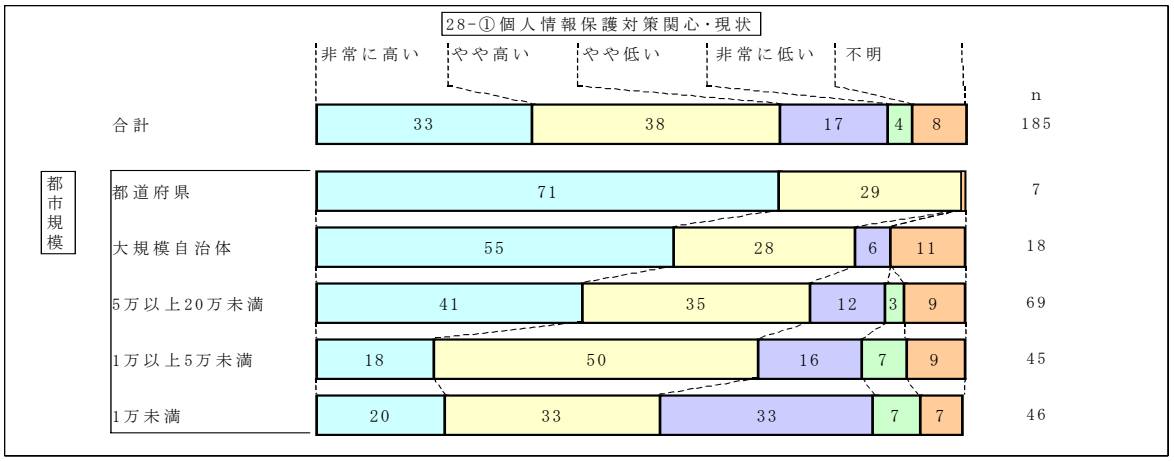
個人情報保護についても自治体の規模によって差はあるものの、個人情報保護では小規模自治体でも条例策定のためのガイドラインなどを参考にして対策を実施することができるため、規模による差は IT アウトソーシングほどは大きくないということがわかる。

図表 18 : 個人情報保護対策に関する経営層の関心（３年前の状況）（都市規模×問 28①３年前）



（出所）富士通総研作成

図表 19：個人情報保護対策に関する経営層の関心（現状）（都市規模×問 28①現状）



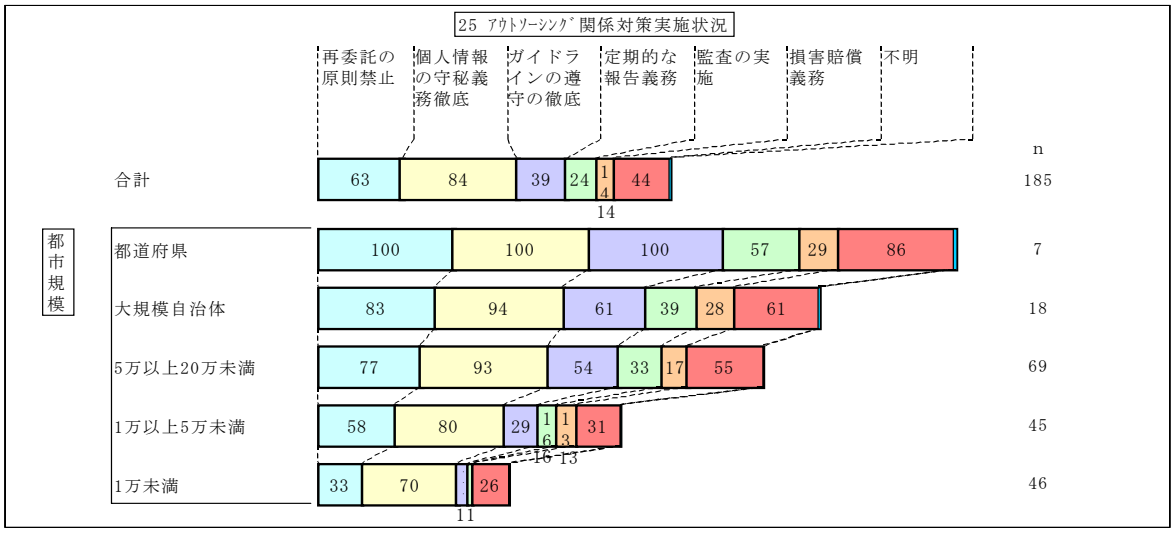
（出所）富士通総研作成

3.2.5 アウトソーシングに関する個人情報保護対策

IT アウトソーシングと個人情報保護対策の関係を詳しく見てみると（図表 20）、自治体においてアウトソーシングの際に実施されている個人情報保護対策で多いのは、アウトソーシング先に対する「個人情報の守秘義務と禁止事項」が 84%、「再委託の禁止」が 63%と上位を占めているが、自治体側からのアウトソーシング先への管理に関する「定期的な報告義務」は 24%、「監査の実施」は 14%となっており、委託先の管理を行っている自治体が少ないことがわかる。

さらに、個人情報保護対策を自治体の都市規模別に見ると、都道府県では、委託先に対する「個人情報の守秘義務と禁止事項」が 100%、「再委託の禁止」が 100%となっており、大規模自治体では、委託先に対する「個人情報の守秘義務と禁止事項」が 94%、「再委託の禁止」が 83%である。一方、人口 1 万未満の小規模自治体では、委託先に対する「個人情報の守秘義務と禁止事項」が 70%、「再委託の禁止」が 33%と、対策の実施比率が低くなっている。

図表 20. 都市規模別個人情報保護対策をアウトソーシングに関して実施されている対策（都市規模×問 25）

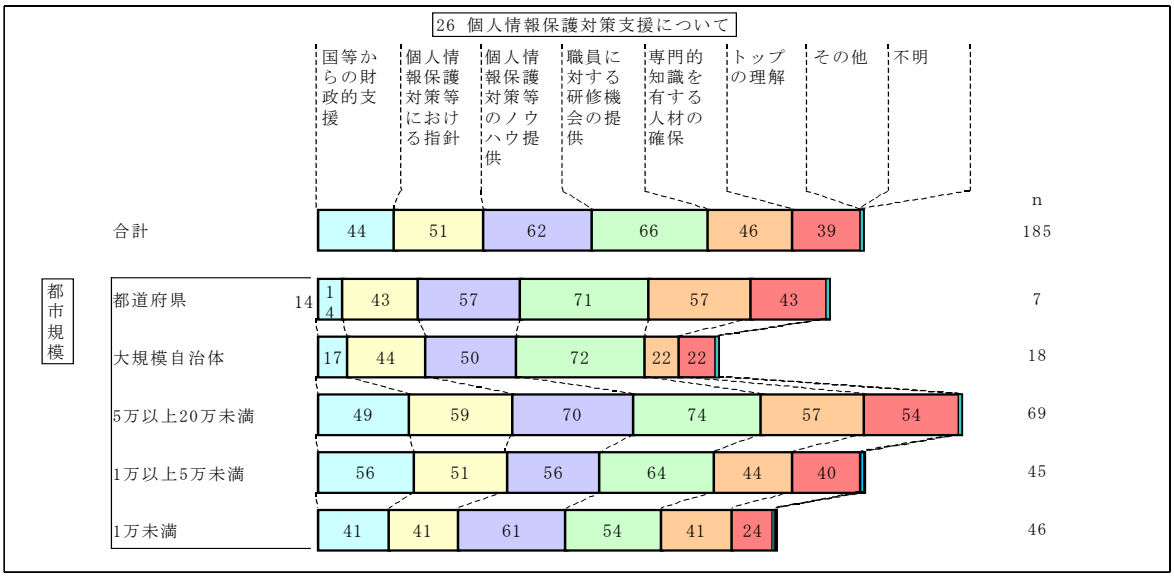


（注）選択肢が複数回答のため、数値の合計が 100(%)を超える。
（出所）富士通総研作成

3.2.6 自治体が求める個人情報保護に関する支援策

今回の調査では、自治体が個人情報保護対策を実施していく上で必要と思われる国等からの支援策についても調査した。その結果をまとめているのが図表 21 である。全体の傾向として、「研修機会の提供」が 66%、「ノウハウの提供」が 62%、「個人情報保護対策等の指針」が 51%と、個人情報保護対策に関する情報提供支援が求められていることがわかる。また、都市規模別に見ると、都道府県でも大規模自治体でも「研修機会の提供」が第一位だが、人口 1 万以下の自治体の第一位は「ノウハウの提供」が 61%でもっとも高い。小規模自治体では、具体的な対応策等の「ノウハウの提供」がもっとも求められていることが伺える。

図表 21：都市規模別個人情報保護対策について今後求められる支援（都市規模×問 26）



（注）選択肢が複数回答のため、数値の合計が 100(%)を超える。
（出所）富士通総研作成

4 安全な自治体 IT アウトソーシング推進に向けて

4.1 IT アウトソーシングの前提としての個人情報保護の徹底

4.1.1 個人情報保護の観点からの文書管理の実態

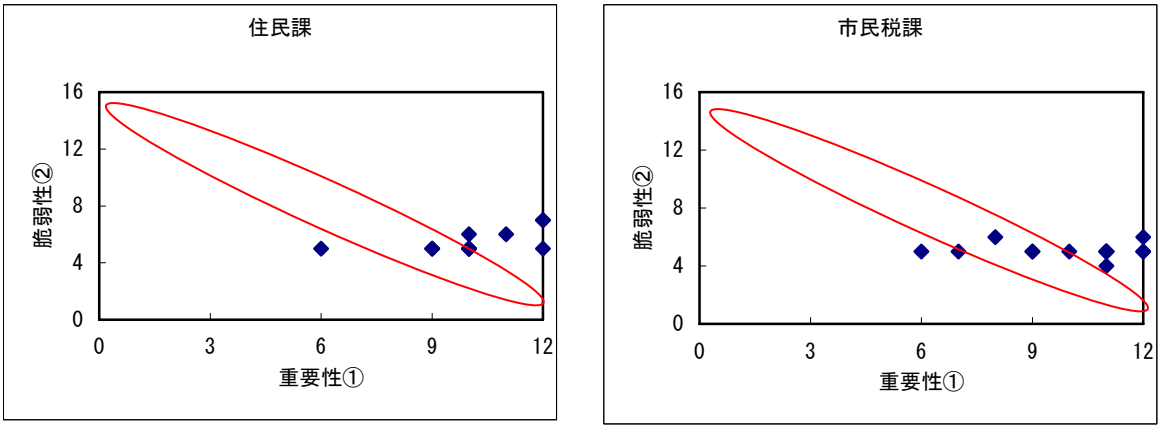
今回行った調査結果から、アウトソーシングを全面的に実施していながらも、個人情報保護条例の制定・改正すら行われていない自治体も存在していることなど、必ずしも個人情報保護政策の実施が IT アウトソーシングの前提となっていないことが明らかになった。自治体における IT アウトソーシングを推進するためには、まずその前提条件として、個人情報保護政策を徹底することが必要である。そして、そのためには、情報システム以前の問題として、自治体業務で使用される多くの種類の文書を適切に管理することが求められる。

しかし、現実の自治体における文書管理には問題点が少なくない。2004 年 1 月から 2 月にかけて行った地方都市（人口約 30 万人の県庁所在都市）における文書による個人情報保護に関する実態調査では、住民課や福祉課、学校教育課等 6 つの部署をとりあげ、それらの部署の担当者に対して調査票による調査と面談調査を実施した。その結果明らかになったことは、どの文書にどのような個人情報が含まれているかということが明確に把握されておらず、それぞれの文書が含む個人情報の種類に関わらず、どの文書もほぼ同じように管理されているということであった。

図表 22 は、この調査の結果の一部をまとめたものであるが、グラフの横軸には文書の重要性をとり、縦軸には文書の脆弱性をとっている。文書の重要性は、重要性に関する 3 つの項目（①機密性、②完全性、③可用性（利用可能性・継続性に関する重要性））に対する 4 段階評価の基準を設け、それぞれの文書が含んでいる個人情報がその基準で測定した場合どの程度重要かということによって、客観的に 12 段階のスコアで評価した。文書の脆弱性は文書の管理状態を示す指標であり、脆弱性をあらわす 4 つの項目（①物理的脅威（侵入、破壊、故障、停電、災害等）、②技術的脅威（不正アクセス、盗聴、コンピュータウィルス、改ざん・消去等）、③人的脅威（誤作動、持ち出し、不正行為、パスワードの不適切管理等）、④被害発生の影響度）に対する 4 段階評価の基準を設け、それぞれの文書がどのように管理されているかということについて 16 段階のスコアで客観的に測定した。

本来であれば、重要性の高い文書ほど脆弱性も低いように管理されているべきであり、すべての文書は図中に示したように右下がりの枠の中にプロットされるべきであるが、実際にはそうなっていない。その主な理由は、自治体の実務では個人情報保護の観点から個々の文書の重要性を評価する客観的な基準がなく、どの文書も同じようになるべく脆弱性の低いように管理せざるを得なくなっているということである。文書によっては、あまり多くの個人情報を含んでいないものもあれば、福祉関連等非常にセンシティブな個人情報（重要性の高い個人情報）を多く含んでいるものもある。しかし、従来は、自治体の担当者が文書の重要性を評価する場合、その文書がどのような個人情報をどれだけ含んでいるかということはあまり考慮されていなかった。そのため、個人情報の保護に関しては、個々の文書が含んでいる情報がよりセンシティブな重要性の高い個人情報であるかどうかの考慮がなされておらず、どの文書も一律的な保管方法によって管理されているのである。

図表 22. 自治体における個人情報の重要性と脆弱性



（注）縦軸と横軸は、調査によるスコア評価を示している。
（出所）富士通総研作成

4.1.2 自治体における個人情報保護の方策

自治体の個人情報保護を行うためには、第一に、すでに指摘したように、文書の重要性を個人情報の観点から客観的に評価する基準が必要である。そうした基準を作成することによって、具体的に自治体で個人情報保護を行うための対策を検討することが可能となる。次に、その重要性にあわせた個人情報が含まれる文書管理（電子文書も含む）を徹底することが求められる。紙のまま保管するか電子化するかといった問題も含めて、重要性の低い文書はなるべくコストをかけずに保管し、重要性やリスクの高いものはある程度のコストをかけて厳密に管理しなければならない。もちろん、自治体の文書管理にあたっては、個人情報保護の観点だけではなく、事務的効率化の視点等を無視するわけにはいかないが、個人情報管理のあり方が大きな社会問題となり、経済的な影響も大きくなっている現状では、従来の文書管理の考え方に個人情報保護の視点を加えることは不可欠である。

自治体における個人情報保護の方策として第三に指摘したいのは、モラル向上のための自治体職員の教育、外部委託先企業の管理の徹底等、制度面および運用面での対応である。この点については次節で詳しく取り上げるが、個人情報保護のためには、制度面だけでなく、個人情報がどのように利用されたかを明らかにするための利用者認証や、アクセスログの収得・保管といった個人情報管理に関する情報公開等、システム的にも対応が求められる。そこで、民間で取り入れられている「プライバシーマーク制度」等の第三者認証機関による個人情報保護の仕組みも、自治体において必要だろう。

4.2 安全な IT アウトソーシングのために求められる政策

4.2.1 アウトソーシングの制度面・運用面での対応

現在、総務省では、電子自治体推進指針を策定し、この中で共同アウトソーシングを行うことで自治体の電子化におけるコストを軽減できるとして、『共同アウトソーシング・電子自治体推進戦略』を提唱していることはすでに述べたが、その中で、自治体にはセキュリティに関して「情報セキュリティポリシー」の策定を要請しており、各団体に対し、最高情報統括責任

者を中心とした全庁的な取組みを求めている。また、外部専門機関の活用も含めた情報セキュリティ監査の取組みが望ましいとしている。過去の例を見ても、個人情報保護の漏えいに関する事件の原因の多くは、技術的なものではなく制度面・運用面の問題であり、個人情報保護に関する制度の設計・施行と、その確実な運用が必要である。

具体的には、個人情報保護条例に関する事項としては、第一に、すでに述べたように、ガイドラインやマニュアル等で具体的な規定をしている自治体でも、再委託に関する事項があいまいになっていることが多いため、委託先の定義や再委託先との契約の確認が必要である。第二に、罰則規定も抑止力の面では不十分な内容が多いため、抑止効果の高い、問題発生時にペナルティを課すような条項を契約時に織り込む必要がある。第三に、アウトソーシング先の決定に際し、外部委託審査会の調査や市長への届出、セキュリティに関する研修義務等を求める等、現状では認定手続きが複雑になりがちな上、認定基準も明確でないことが多い。委託先にセキュリティ・エンジニアの派遣を義務付ける等、アウトソーシングの審査基準となるような規定を明確に定めることが必要であろう。第四に、事故が発生した場合の対応策が十分に検討されている自治体が少ないので、マニュアル等で具体的な対応を作成しておく必要がある。

必要な対策を主体別に整理すると、まず、発注元である自治体に関する事項としては、第一に、アウトソーシングに伴う庁内でのリスク・マネジメントに関する責任の所在を明らかにしなければならない。第二に、文書管理の必要性でも指摘したように、情報のセキュリティ・レベルを分類し、セキュリティ・レベルに見合った適正な管理がされているかどうか監督する必要がある。

次に、アウトソーシング先である民間事業者に対する事項としては、第一に、元請は再委託先と契約書を取り交わす際に、発注元と取り交わした契約内容を尊守する必要がある。第二に、従業員のセキュリティに対する意識が常に維持されるように配慮することも求められる。なお、再委託に関しては、再委託の原則禁止を厳密に運用しようとする自治体が増加しているが、受託者である IT 企業の実態として、元請である大手ベンダー企業から、大手ベンダーの関連子会社や中小ベンダーに至る構造が存在しており、現実的には、こうした実情に合わせた再委託の対応方法をとることも必要である。委託先の企業が個人情報を取扱う場面として、①直接個人情報を取扱う場合、②動作確認等により個人情報を一見する可能性のある場合、③全く個人情報を取扱わない場合、といった３つの場合に区別することができる。①の場合では、開発・運用段階の本番データを取扱う作業やシステム運用段階のオペレーションや障害対応に関する作業が想定され、②の場合は、システム運用段階で状況を監視する場合やメンテナンスを行う場合が想定される。受託者が個人情報を取扱うことによって問題が生じる場合が多いのは、実際の個人情報をデータとして取扱う場面に限定されるため、一律的に再委託を禁止して個人情報保護の対応策とするのは、受託者の事情を無視した考え方ともいえる。そのため、再委託を禁止する際には、受託範囲を明確に整理した上で、再委託を厳密に禁止する場合を限定するべきである。それ以外の場合は、契約上の秘密保持義務を課した上で、再委託の事前同意を得るようにしておけば十分であろう。

4.2.2 都市規模の小さな自治体に対する支援策の必要性

今回の調査結果では、IT アウトソーシングの実施状況や今後の予定に関して、自治体の都市規模によって大きな差があることがわかった。また、個人情報保護の条例改正やガイドラインの策定については、自治体の都市規模による差があまりみられなかったが、個人情報保護の具体的な対応策を個別に見てみると、自治体の都市規模による差をみることができた。さらに、規模の大きな自治体においては職員の管理のための研修支援がもっとも求められているが、小規模自治体では、具体的な対応策等の「ノウハウの提供」がもっとも求められていることも明らかになった。

これらの結果から、個人情報保護を前提とした安全な IT アウトソーシングを進めるためには、都市規模の小さい自治体に対する支援策が早急に求められていると言うことができる。具体的には、国による自治体共通の個人保護に関する一定基準に基づく対応支援や、都市規模の小さな自治体同士が連携して、アウトソーシングや個人情報保護対策のノウハウを共有化するために研修を行うような仕組み作りが求められる。たとえば、和歌山県では、県内市町村を支援するために、和歌山県内の市町村による「和歌山県自治体セキュリティ対策協議会」を立ち上げて、セキュリティ対策を県内市町村の共同で行う取組みを行っている。こうした取組みも１つの方法といえるだろう。

また、全国自治体がどのような個人情報保護の対策を行っているかということを格付けする仕組み作りも、都市規模の小さな自治体に対する効果的な施策として考えられるであろう。総務省でも、2006 年度に自治体の情報セキュリティ・レベルを認定する仕組みを構築し、情報セキュリティの水準を確保するため、情報セキュリティ対策に係る一定の基準を満たした自治体を認定する「情報セキュリティ・レベル認定制度」を検討している。こうした検討に個人情報保護に関する項目も組み入れるとともに、都市規模の小さな自治体でも取組むべき一定レベルの対応策を定めた標準化を示したガイドラインを提供することが必要であろう。

さらに、今後は、受注者側である民間事業者に対しても、発注元である自治体の不安を解消し、適正で安全な業務提供を提案できる体制作りが求められる。そのような体制を作ることができれば、そのことがサービスの差別化にもつながると考えられる。

このように、特に都市規模の小さな自治体に対しては、さまざまな主体がそれぞれのレベルで自治体の個人情報保護のために必要な施策を検討し実現していくことが、IT アウトソーシングを推進するための前提条件として必要になるのである。

（参考文献）

- 藤野剛士　2000　『図解でわかる　個人情報保護』日本能率協会マネジメントセンター
- 日本ネットワークセキュリティ協会　http://www.jnsa.org/
- 日経BPガバメントテクノロジー　http://premium.nikkeibp.co.jp/e-gov/
- 大阪府ホームページ　http://www.pref.osaka.jp/
- 総務省ホームページ　http://www.soumu.go.jp/