資料１

住民基本台帳に係る電算処理の委託等に関する検討会

報　告　書　　（案）

はじめに

住民基本台帳制度は、住民基本台帳法(昭和 42 年法律第 81 号。以下「住基法」という。)に基づくものであり、市町村において、住民の居住関係の公証、選挙人名簿の登録その他の住民に関する事務の処理の基礎とするとともに、住民の住所に関する届出等の簡素化を図り、あわせて住民に関する記録の適正な管理を図るため、住民に関する記録を正確かつ統一的に行う制度として創設され、住民の利便を増進し、国や地方公共団体の行政の合理化に資することを目的としている。

従来から、住民基本台帳制度においても、一般社会における各種業務の処理や他の行政分野における事務処理と同様、技術の進展著しい電子計算機による情報処理が進んで来ている。こうした電算処理の中で取り扱われる住民基本台帳上の個人情報は、住民個人にとって最も基礎的な情報であり、社会的な関心も強く、情報保護の徹底が、とりわけ強く要請されていると言える。

このため、平成 11 年改正(平成 11 年法律第 133 号)により新設された住基法第 36 条の２の規定では、市町村長は、住民基本台帳に関する事務の処理に当たって、住民票に記載されている事項の漏えい、滅失及びき損の防止その他の住民票に記載されている事項の適切な管理のために必要な措置を講じなければならないとしている(同条第１項)。この場合、実際には、現場で事務の処理に従事する市町村の職員に対して、個人情報保護の義務が課されたものと理解できる。電算処理は専門性が高いことから、外部に委託して処理されることが多くなる。このような実態を踏まえ、住基法第 36 条の２には、第２項が設けられ、市町村長から住民基本台帳に関する事務の処理の委託を受けた者(実際には、現場で委託された事務の処理に従事する委託先事業者の従業員等が該当する。)に対しても、第１項(市町村長)同様に、個人情報保護の義務を課している。

また、住基法の規定を敷衍する形で、繰り返し、住民基本台帳上の個人情報保護の徹底を図るための対応が講じられてきた。このほか、地方公共団体が保有・管理する個人情報一般の保護のため、「地方公共団体における個人

情報保護対策について（総行情第 91 号平成 15 年 6 月 16 日通知。以下「15 年 6 月通知」という。）」が発出され、「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 18 年 9 月改定版。以下「ガイドライン」という。）」が示されるなど、関連する法制度の整備・施行や情報セキュリティ事故の発生といった各時点における状況に応じて、随時、様々な対応が積み重ねられてきた。

しかしながら、本年５月に、複数の市町村からデータ統合等のシステム開発を委託された事業者が、契約に反して、一部業務の再委託を行い、再委託先事業者の従業員がデータを自宅に持ち帰り、自宅パソコンに保存したところ、自宅パソコンからファイル交換ソフトを介して、国民年金情報や老人保健情報などを含む個人情報が流出するというはなはだ遺憾な事案が発生した。ある市町村においては、市町村合併に伴い、旧市町村が個別に整備してきたシステムに係るデータ移行に際して、ほぼ全住民の住民票記載情報が、住民票コードも含めて流出するという結果を招いている。

今回は、住民基本台帳情報が大量に流出した事案であったが、住民基本台帳情報以外の地方公共団体が保有・管理する個人情報について見ても、これらの情報が同様の事情を経て流出するような事態は､なお生じることがあり、なかなか止むことがない。こうした現状は、これまでの対応が十分な実効性を備えていたのか、再検討を迫るものと言える。

そこで、本検討会が設けられ、住民基本台帳の電算処理に係る市町村の委託実態等を踏まえながら、住民基本台帳情報の取扱いに係る課題を中心に検討を行い、実効を挙げ得る対策をとりまとめることとされた。

本検討会は、市町村及び市町村から電算処理の委託を受ける事業者からの意見聴取を含め、７回にわたる会合を開催し、検討を進めてきた。以下は、その検討の成果をとりまとめたものである。

１　情報流出事案を踏まえた現状認識

（１）情報流出を招きかねない要因・反省点

先に言及した本年５月の住民基本台帳情報に係る大量流出事案は、これまで流出を防止するために積み重ねられてきた対応にもかかわらず、なぜ、発生したのか。この事案から、どのような認識が得られるのか。まず検討してみる。

電算処理を委託する市町村の対応に関しては、今回の事案に即して考える

と、15年6月通知、ガイドライン等に沿った対応が、それぞれの市町村において、適切に理解されて、個人情報保護条例及び情報セキュリティポリシー(具体的な実施手順を含む。)に的確に規定された上、そのとおりに実施・遵守されていれば、市町村側でとるべき措置・規制としては十分であったと思われる。

具体的に、各市町村において、以下のような事項が適切かどうか、検証し、問題が見つかれば、早急に改善を図る必要がある。

・個人情報保護条例の規定内容・運用状況
・情報セキュリティポリシーの規定内容・運用状況
・電算処理の委託契約における個人情報保護への配慮についての規定内容・運用状況
・委託契約の規定内容遵守についてのチェック状況
・個人情報保護に対する職員の意識レベル　　など

他方、再委託先の事業者を含め、委託を受ける事業者の側においても、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）に基づく事業者に対する規制・義務、事業者自らが定める管理規程や委託契約の規定内容を遵守し、適切に手続が踏まれれば、今回のような事案は生じなかった可能性がある。

今回の事案に即して、事業者の対応上の問題を具体的に挙げると、以下のようになる。

・再委託に係る承認手続の不履行
・委託先事業者による再委託先事業者に対する委託契約の規定内容遵守（指定場所での処理、データ持ち出しの禁止など）の不徹底
・再委託先事業者における情報セキュリティ確保措置の不備（特に、在宅勤務が伴う勤務体制下での不備）
・再委託先事業者の従業員による自宅パソコンへのデータの不正保存
・当該パソコンへのファイル交換ソフトのインストール・ウィルス感染

これらが連鎖的に重なり、住民基本台帳情報が流出したものと考えられる。

(2)情報セキュリティ確保の必要性

行政機関が保有・管理する個人情報の流出による侵害のおそれは、住民基本台帳情報に限られず考えられる上、実際に情報流出による侵害も発生している。情報セキュリティ確保の必要性は、個人情報に係る事務処理一般を通じて同様に認められるものである。

したがって、住民基本台帳情報と他の個人情報との間で、できる限り軌を一にして、情報セキュリティの水準を上げていくことが望まれる。

もっとも、住民基本台帳情報の流出事案は、現に、国民に不安感をもたらし、社会の大きな関心をよんでいる面がある。住民基本台帳情報については、他の個人情報とは区別した上で、適正な管理を求める要請がとりわけ強いとの受け止めが世間一般にあるとも考えられる。

（３）委託と再委託との関係

委託と再委託(再委託先から、さらに委託が行われる再々委託を含む。)の関係をどうとらえるのか。両者の違いに着目するのか、つながりがあると見るのか。これは、再委託に対する評価とその活用方針に関わってくる。

再委託は、再委託先事業者の選定や再委託先における業務の実施管理に対する市町村の関与が、どうしても間接的なものとなってしまう。このため、市町村が締結する元の委託契約の中では、再委託先事業者を対象とした遵守事項の義務付けは困難な面がある。しかしながら、元の委託契約の当事者である委託先事業者は必ず委託契約上の責任を有していることから、この委託先事業者（再委託元の事業者）との間の契約を介して、再委託先事業者等を適切に管理できる可能性がある。

したがって、再委託については、各々の市町村の置かれた事情も踏まえ、電算処理の委託業務を円滑に遂行するため、やむを得ない場合に限って、例外的に活用していくことが考えられる。また、再々委託については、原則として認められないが、ごく例外的に、他に代替手段がない場合に限って、市町村の承認を得て行うことは考えられる。これらに際しては、個人情報保護法第 22 条では、委託を受けている事業者（個人情報保護取扱事業者）は、自らが委託している再委託先事業者に対して、必要かつ適切な監督を行わなければならないとされており、この規定により適切な管理を徹底すべきである。

２　実効性のある対策　～手順に沿った措置～

（１）対策の対象業務の範囲

「委託」処理する場合を念頭に置いて考えるとして、どこまでの範囲を対象業務とするべきか。市町村の実務においては、システム開発・改修の委託にとどまらず、オペレーション業務の委託、システム機器保守の委託なども、

相当の頻度で行われている。これらの委託であっても、個人情報(住民基本台帳情報)を取り扱うという点は、システム開発・改修の委託と同様の状況にある。このため、オペレーション業務の委託やシステム機器保守の委託なども、特に対策の対象業務から除外せず、広く対象としていくべきである。ただ、対策の必要性や中身は、対象業務の内容如何で異なることから、実際の作業内容を吟味しながら、具体的な対策の適用を考えていくべきである。

(２)対策の具体的な内容

１(１)で検討した情報流出を招きかねない要因・反省点を踏まえると、実効性のある対策として、具体的に、どのような措置や取り決めの推進を図っていくべきか。作業形態等に応じて、具体的に必要とされる措置内容にも相違が生じてくるが、対策は以下のとおりとなる。

①指定場所での処理：　処理する具体の場所は、市町村が指定することになる。

②承認を受けないデータ持ち出しの禁止：例外としての承認は、市町村において、個人情報の漏えい・滅失・き損の可能性を把握した上で、その危険を冒してもデータが現存する場所から、それ以外の指定場所へ持ち出す必要が認められる場合に限って、必要な条件を付した上で行うことになる。

③(②の例外の場合の)データの暗号化処理：　指定場所に持ち出す場合において、その途上で、仮に、個人情報が流出したとしても、暗号化処理されていれば、被害拡大の防止に有効である。

④承認を受けないデータの複製・複写の禁止：　例外としての承認は、市町村において、個人情報の漏えい・滅失・き損の可能性を把握した上で、その危険を冒しても複製・複写する必要が認められる場合に限って、指定場所での作業に必要な最小限の範囲で行うことになる。

⑤処理作業後のデータの返還・廃棄：　不要となったデータについては、遅滞なく市町村に返還するか、又は廃棄することになる。廃棄の場合には、当該データ内容が判読できないようにするなど、確実な履行の確保を図る必要がある。

⑥承認を受けない再委託の禁止：　例外としての承認は、再委託先事業者に市町村の管理が及ぶ場合に限って、市町村が行うことになる。

⑦日々(一定期間ごと)の処理記録の提出：　処理する業務の内容によるが、委託先事業者の理解を得て、市町村が合理的な範囲で提出頻度を設

定する。提出の都度、市町村の確認を受けることになる。　　など

これらのうち、特に、②に掲げる情報の管理区域からの”持ち出し”が基本的で重大な手順違反との意見が多かった。この”持ち出し”に焦点を当てて、措置の徹底を図っていくべきである。

なお、実際には、市町村が事業者と委託契約を締結するに至るまでの間で、委託先の選定・契約・受託業務の実施・監督・責任追及のそれぞれのプロセスにおけるセキュリティ上の課題(特に、残存リスク)を、あらかじめ明らかにした上で、実地に即し、経済合理性も考慮して、どのような情報セキュリティレベルを備えるべきか、判断していく必要がある。

(３)委託先事業者の限定の適否

委託契約を締結する事業者を、ＩＳＯなどの認証を取得している事業者やセキュリティ監査・システム監査を受けている事業者に限定すべきとの見解がある。そうすることにより、(２)に掲げる措置内容が遵守される可能性が高まるとの認識からである。

確かに、プライバシー・マークやＩＳＭＳ（ＩＳＯ27001）の認証を取得していることや定期的にセキュリティ監査等を受けていることにより、当該事業者においては、従業員に対する情報セキュリティ教育や情報保護の意識レベルで、一定の水準が確保されていると見ることができよう。ガイドラインでは、事業者選定に当たって、これらの認証取得を要件とすることを、地方公共団体に対する推奨事項としている。こうした位置づけにとどまらず、入札参加資格とするなど、市町村に対して、さらに積極的な対応を促すことも考えられる。

ただ、同じ認証を取得していたり、同様にセキュリティ監査等を受けていても、事業者間で能力・対応に相当の差がある場合もある。また、近時は、地方公共団体の調達においては、公正な競争・取引条件の設定が要請される傾向が強く、国内事業者のみにあてはまる条件を厳格に解して、要件とすることには慎重にならざるを得ない。さらに、委託先事業者が、委託される業務のそれぞれのプロセスにおける情報セキュリティと残存リスクを明らかにし、その実装・運用と監査・改善を、具体的な発注条件として検討し、契約条項の中に細かく規定していかないと、市町村の期待する情報セキュリティレベルを確保できないのではないかとの意見が見られた。認証等を得ているからと言って、必ずしも情報セキュリティが万全ではないという、認証等が有する限界を認識した上で、それらの活用を図るべきという意見もあった。

これらを踏まえると、認証等を得ていることは、市町村が委託先事業者を選定するに当たって、一つの判断要素として考慮していくような取扱いが適当である。将来的には、事業者の取得状況を踏まえて、契約締結に当たっての必要条件とすることも考えられる。

（４）市町村・委託先事業者のそれぞれに求められる対応姿勢

（２）のような対策をとっていくとして、市町村及び委託先事業者には、それぞれどのような対応姿勢が求められるか。

市町村は、これまでにも増して、十分な情報セキュリティを確保するための措置について規定を整備し、具体的な発注条件として契約条項に盛り込んだ上で、それらが遵守されるよう、一層のチェック強化を進めていく必要がある。

一方、委託先事業者の側でも、十分な情報セキュリティを確保するための措置について規定を整備した上で、具体的に定められた契約条項がきちんと遵守されるよう、従業者など実際に個人情報を取り扱う業務に従事する者に対して、遵守事項の徹底とこれらに従った業務の適正な管理を求めていく必要がある。

これらが継続的に維持・推進されていくためには、単に静的なルールの整備だけに頼ることなく、動的に処理態様をチェックしていく体制の確立が欠かせない。委託先事業者は、適切に工程を管理するとともに、委託した市町村の側でも、処理状況（作業プロセス）を把握しつつ、チェック・確認できるような状態を作り出していかなければならない。そのため、（２）⑦に掲げた対策を通じて、あらかじめ定められた間隔で処理状況を把握できる仕組みを整備していく必要がある。

なお、委託先事業者を選定する際には、事業者自らに、処理の過程で講じようとしている情報セキュリティ確保のための措置の内容を具体的に明らかにさせることにより、処理環境の情報リスクレベルが許容できる水準にまで下がっていることを、市町村において確認すべきである。その上で、契約を締結すれば、処理段階に入ってからの工程管理やそのチェック・確認が行いやすくなるし、ひいては、委託先事業者に対する制裁も機動的に発動できることになると考えられる。

また、委託先事業者から再委託が行われた場合においても、委託した市町村の側で、（２）⑦に掲げた対策に準じる適切な方法により、再委託先事業

者における処理状況（作業プロセス）を把握しつつ、チェック・確認できるようにする必要がある。

（５）対象となる行為者

（２）に掲げる対策について、具体的に、コントロールを効かせる対象となる行為を行う者は、どのようなものになるか。委託契約の相手方は、事業体としての法人であることがほとんどであり、（２）に掲げるような対策により、業務を処理する中で個別の行為について、規制を受ける客体としては適当でないことが多い。このため、実際に業務を処理する中で、対象となる行為を直接行うおそれのある者としては、主に、委託先事業者の従業員を念頭に置いて、「個人情報（住民基本台帳情報）を取り扱う業務に従事する者」を考えていくべきである。このように考えれば、結果として、委託契約上の地位及び委託先事業者との関係如何にかかわらず（派遣労働者であったり、請負事業者が介在したりしても）、対象行為者の行為にコントロールを効かさせられることになる。

ただし、直接の行為者（「個人情報（住民基本台帳情報）を取り扱う業務に従事する者」）の行為に着目して、規制したとしても、その行為に伴う契約上の責任は、当然、情報セキュリティ体制を整え、回避のための措置を講じられる権限・立場を有する委託先事業者等が、市町村に対して負うこととなる。第一線で処理に当たる者に、過度な責任が課されることがないようにしなければならない。

また、（２）に掲げるような対策に応じる行為を行う者の立場には、委託契約上の地位を有する者でなければ立ち得ない場合がある。⑥及び⑦の対策が該当するが、このような場合には、当然、行為者は委託先事業者等そのものとなる。

３　対策実施の手法・法律上の構成

（１）対策実施のための手法・選択肢

具体的に、対策を実施するために、どのような手法を用いるべきか。その選択肢として、どのようなものが考えられるのか。議論の中では、以下のような３通りの対応が検討された。

①ガイドライン等に基づく助言による対応

住民基本台帳情報を含め、個人情報一般について、15 年 6 月通知、ガイドライン等で示されている内容について、市町村の個人情報保護条例・情報セキュリティポリシー等への盛り込みが徹底されるよう、あらためて総務省において、助言・報告の徴収・勧告など関係法律に基づく権限を行使する。

市町村の側では、委託される業務のそれぞれのプロセスにおいて、実施・遵守されるべき内容を具体的な発注条件として契約条項に盛り込んだ上で、それに基づいて、委託先事業者が確実に履行するよう請求する。

②住基法・同法施行令に基づく技術的基準の改正による規範性のある対応

住民基本台帳情報については、今回の情報流出事案を踏まえて、市町村及び委託先事業者が講じなければならない情報セキュリティを確保するための措置を明確化することとする。15 年 6 月通知、ガイドライン等で示されている指定場所での処理、データ持ち出しの禁止と承認、データの暗号化処理等に関して、これらの情報セキュリティ確保措置の規範性が確実に担保されるよう、住基法及び同法施行令に基づいて定められ、法令の一部としての意味合い（法令上の最低限の基準）がある「住民票に係る磁気ディスクへの記録、その利用並びに磁気ディスク及びこれに関連する施設又は設備の管理の方法に関する技術的基準」（昭和 61 年自治省告示第 15 号。以下「技術的基準」という。）に、改正・追加等を行う。総務省においては、新たな技術的基準の内容が、市町村において遵守されるよう、住基法第 31 条の規定に基づき、必要に応じ、助言・報告の徴収・勧告などの権限を行使し、指導する。

市町村の側では、規範性を有する技術的基準の新たな内容を踏まえ、委託される業務のそれぞれのプロセスにおいて、実施・遵守されるべき内容を具体的な発注条件として契約条項に盛り込んだ上で、それに基づいて、委託先事業者が確実に履行するよう請求する。

一方、委託先事業者の対応に関しては、所管府省を通じて、個人情報保護法に即した措置・手続が確実に行われるよう再周知に努める。その上で、個人情報保護法第 32 条から第 34 条までの規定に基づき、主務大臣が、個人情報保護取扱事業者である委託先事業者に対して、必要に応じ、報告の徴収・助言・勧告・命令の権限を行使する。

この技術的基準の改正による対応に関しては、

○技術的基準の規定内容を、より具体化して契約条項に盛り込みやすいものにしたひな形を提示し、その徹底を図る。

○そのため、住民基本台帳ネットワークシステムにおける場合と同様に、自己点検表も活用した上で、システム・セキュリティ監査を実施する。

○２（４）で述べたとおり、委託先事業者を選定する際に、事業者自らが処理の過程で講じようとしている情報セキュリティ確保のための措置の内容を、具体的に明らかにさせることにより、以後のチェック・確認を行いやすくし、機動的に責任を追及することとする。

などの運用上の工夫を組み合わせることにより、措置の実効性が向上すると見込まれる。

また、契約上の責任を追及するための措置として、

イ　契約に規定された履行代金の減額

ロ　違約損害金の請求

ハ　事後の一定期間にわたる同種の契約に対する入札参加資格の停止又は制限

などが考えられるが、これらを背景にした抑止効果が適切に働けば、情報セキュリティを確保するための措置の遵守に寄与すると見込まれる。

以上のように、委託先事業者の契約上の責任・義務の遵守の徹底を図り、情報セキュリティを確保するための措置が確実に講じられれば、情報流出はかなりの程度防止できると考えられる。

③法律改正による対応

住民基本台帳情報について、住基法を改正し、住民基本台帳情報を取り扱う業務に従事する者が手順に沿わない処理を行う場合に、規制をかけることとする。

あるいは、住民基本台帳情報を含め、市町村等の行政機関が保有・管理する個人情報について、所要の法律改正を行い、個人情報を取り扱う業務に従事する者が手順に沿わない処理を行う場合に、規制をかけることとする。

この法律改正による対応をとるのであれば、法律上の規制対象となる行為を規定する必要が出てくるが、２（２）の①から⑦までに掲げる行為のうちから、法律による規制になじむものに対象を絞り込んでいくことになる。

（２）他の個人情報と区別して法律上の特別な措置を講じる場合の理由

（１）③の対応のうち、住民基本台帳情報について、他の個人情報と区別して、法律上の特別な保護措置を講じるとすれば、区別を正当化する説得的な理由が必要となる。これまでの検討を踏まえると、以下のような整理が考えられる。

住民基本台帳情報の流出事案が発生しており、住民の居住関係を確認し、住民の権利・義務の基礎となる情報を適正に管理、公証するという住民基本台帳制度に対する国民の信頼が損なわれかねないおそれがある。市町村における住民基本台帳事務は、住民個人の基礎的な情報を、適正な記録管理そのものを目的として管理するものである。このような基本情報が、適正な手続が踏まれずに、仮にまとまって流出したとすれば、悪意を有して、他の情報と結合・リンクさせようとする者に利用される危うさがある。こうした特性を有する住民基本台帳情報については、適正に遺漏なく管理する必要性がきわめて大きいと考えられる。

なお、行政機関が保有・管理する住民基本台帳情報以外の個人情報は、個別の行政目的のために収集・管理されるものであり、民間事業者が保有・管理する個人情報は、基本的には営利目的のために収集・管理されるものである。これらの目的との関係の中で、最も適切で実効性のある保護措置のあり方を考えていくべきであり、住民基本台帳情報とは事情が異なると言える。

このような整理を肯定し、さらに、住民基本台帳情報について他の分野に先行した対応の意義を強調することにより、個別に、住基法を改正し、特別の措置を講じるべきとの意見がある。

また、住民基本台帳情報の中でも、

○基本情報の場合とそれ以外の場合

○住民基本台帳の基幹システムから持ち出す場合と住民基本台帳情報から他の用途に提供された関係情報を持ち出す場合　　など

それぞれ違いがあり、より精査・区分して、必要な対策を考えていくべきとの意見がある。

以上のように、住民基本台帳情報について特別な保護措置を講じていくという考え方がある一方、市町村が保有・管理する住民基本台帳情報以外の個

人情報についても、同様に、情報セキュリティの確保は必要であり、全体として、できる限り軌を一にして対応方策を考えていくべきとの意見もある。

（３）段階的な対応の適否

（１）の①から③までの対応については、

○前の段階の措置を尽くして、次の段階の措置に進んでいくべきと考えるのか。

○法的な規制のための措置が、関係者の意識・処理の実態の改善を促し、“実効性のある対策”につながると考えるのか。

２通りの考え方があり得る。どちらの方が、対応が円滑で効果的なものとなるのかという観点で考えるべき問題であるし、それぞれの対応による実効性をどう評価するかという問題でもある。特に、②の対応による実効性に着目して考えるべきである。

４　罰則の取扱い

（１）検討の状況・必要性

３（１）で③の法律改正による対応をとる場合には、法律により、単に対象となる行為を規制するにとどまらず、規制された行為に対して、刑事上ないしは行政上の罰則を科していくべきかどうかも検討する必要がある。講じられる対策の遵守状況や効果を予測しながら、さらなる対応に踏み込む必要があるのかどうか、他の行政分野や法律との関係を含めて、十分に議論・検討していかなくてはならない。この罰則の取扱いに関しては、理論面の問題を中心に、活発な議論が行われ、多様な意見が表明された。

なお、この検討は、住民基本台帳情報を処理する過程で、業務の処理に当たる者の、意図的とは言えないものの、不適切な行為に起因して、情報が流出するような事態を防止することを直接の目的として行われたものである。業務の処理に当たる者が、不正な目的の下、意図的に行った行為による情報漏えいへの対応も重要な課題であるが、対策の内容が異なってくることから、別途の検討を要するため、ここでは念頭に置いていない。

（２）刑罰導入の可否

法律に基づき、情報流出が起こらないよう手順に沿わない措置や行為に規制をかけた上で、それでも情報流出が起きた場合、さらに、刑事責任を問う

刑罰を設けることについて、どのように考えるか。保護法益をどのようなものと位置づけるか、構成要件をどう設定するかをはじめとして、詳細な検討が必要である。

民事の損害賠償請求、行政上の規制によってもとらえきれない行為がある場合、刑罰を導入していく余地はあり得る。情報流出という結果の重大性にかんがみれば、損害賠償責任や行政上の責任と刑事責任が重複することも考えられる。

（３）刑罰の機能

住民基本台帳情報をはじめとする個人情報の流出に対して、刑罰を考える場合、刑罰のどのような機能を重視すべきであるか。この局面における刑罰の機能としては、刑法理論的には、①本来違法であって、非難・禁止に値する行為を処罰することにより、その違法性を確認するという考え方と②理論的には危険性を有する行為であり、処罰対象とすべきであるが、対象とされていない行為について、処罰することにより、非難・禁止すべきものと認識させるという考え方の２通りがある。特に、②の考え方については、刑罰が対策の前面に出ていくことにもなり、刑罰の謙抑性の原則も踏まえると、慎重に考えていく必要がある。

（４）個人情報流出事案に即した刑罰の構成

個人情報の流出は、明確な故意によるものは少なく、過失によるものが大半を占める。また、いったん被害が発生した場合、その回復の可能性は低い。こうした個人情報流出事案に特有の事情を踏まえ、刑罰をどのように組み立てていくべきであるか。

住民基本台帳制度の信頼性を確保するため、住民基本台帳情報を扱う専門家には、その責務にふさわしい行為規制をかけた上で、行為規制にのっとらない行為に係る故意の責任を問うていくことが考えられる。専門家としては、善良なる管理者としての注意義務の下、適正に事務を遂行することにより、回避できる行為について、責任を問われる場合があるのは、やむを得ないことである。実際には、住民基本台帳情報の流出（不特定多数の者が認知できる状態に至らせること）という侵害結果を伴わなければ、刑事責任を科さない、あるいは軽微なものにとどめるということも考えられる。

もっとも、行為規制に反する行為を行った段階で責任を問うこと自体についての社会的な認識の定着度合いや委託先事業者（再委託先事業者を含む。）

及び実際に処理に当たる従業者等を過度に萎縮させないことにも配慮すべきとの指摘もあり、さらに詳細な検討が必要である。

また、従業員が業務に伴って不法な行為をした場合に、委託先事業者（再委託先事業者を含む。）に対する刑罰について、どのように考えるか。①両罰規定を設けるのか、②むしろ、両罰規定ということでなく、直接に委託先事業者（管理者）そのものに対する刑罰として考えていくのか。この問題に関しても、さらなる検討が必要である。

（５）行政上の秩序罰による対応

また、罰則を検討する場合において、刑罰を導入するのではなく、行為規制に反する客観的な行為を認定することにより、行政上の秩序罰として、過料を科すこととする対応が考えられるところである。

行政上の必要性から、制裁措置を設けようとする場合、単純行為犯に対して科されるものであり、複雑な要件の認定が不要であることからも、実際上、刑罰よりは円滑な運用が期待できる可能性が高く、一定の効果は得られると期待できる。

秩序罰の導入については、過料程度で持ち出しなど不適切な行為を抑制できるかということについて、現場で取り扱う者の職務意識に対して、防波堤としては弱いとの意見も見られるが、運用如何により、抑止効果を得られる場面も多いと思われる。

（６）罰則に係る検討の総括

法律改正により、行為に規制をかけ、罰則を導入するとした場合、その考え方は、以上のようなものになると考えられる。引き続き議論・検討を深める必要がある。

ここでは、これまでの議論の中での多様な意見を整理し、記述するにとどめる。

５　まとめ

３（１）で述べたように、法律改正によらない対応であっても、規範性を有する技術的基準の改正による対応に、運用上の工夫、市町村の現場での取組みや契約上の責任の追及などを組み合わせることにより、住民基本台帳情報に係る情報セキュリティについて、相当の向上が期待できると思われる。

他方、法律改正により対応するとすれば、住基法単独である場合には、住民基本台帳情報以外の個人情報と区別して法律上の特別な措置を講じる理由や必要性を明確にし、理解を得ていく必要がある。

また、個人情報全般について対応を講じる場合には、他の行政分野を含めた幅広い議論を要することになり、機敏な対応は困難となるおそれがある。

実務の立場からは、３（３）の対応に関しては、直ちに法律改正に進むのではなく、地道に段階的に対応していくことが適当であり、個別具体の取組みを積み重ねることに力点を置くべきとの意見もある。

これらの事情を踏まえると、セキュリティ確保の重要性にかんがみ、まずは、迅速で速効性を有する対応をとることとし、規範性を有する技術的基準の改正（改正案のイメージは別添のとおり）による対応を通じて、市町村による取組みを徹底していくこととすべきである。法律改正については、これらの対応による実績・効果をも見きわめながら、さらに詳細な検討を行いつつ、本検討会における一定の整理・意見集約の上に立って、さらなる対応として取り組むこととすべきである。

また、こうした全国を通じた対応にとどまることなく、それぞれの市町村において、地域や事業者の状況に応じて、個人情報保護条例や同規則に必要な規定を設けるなど、独自に対応を強めていくことも望まれる。