資料２

論 点 の と り ま と め （案）

１　情報流出事案を踏まえた現状認識

○　既存の流出防止措置があったにもかかわらず、なぜ、住民基本台帳に係る情報が流出したのか。どのように考えるか。

⇨

【市町村の対応】

住基法に基づく技術的基準（大臣告示）、「地方公共団体における個人情報保護対策について（平成15年6月通知）」、「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）」等に沿った対応が、市町村の個人情報保護条例、セキュリティポリシー（具体的な実施手順を含む。）に適切に規定され、そのとおりに実施・遵守されていれば、市町村側のとるべき措置・規制としては十分と言えるはず。

市町村において確認・点検が必要な事項を列挙すると、

・個人情報保護条例の内容
・セキュリティポリシーの内容
・契約内容上の個人情報保護への配慮
・契約遵守についてのチェックの状況
・職員の個人情報保護に対する意識　　など

【事業者の対応】

再委託事業者を含め事業者の側においても、個人情報保護法に基づく事業者に対する規制・義務、管理規程や契約事項を遵守し、手続が適切に踏まれれば、事案は生じなかった可能性がある。

事案に即して、対応上の問題を具体的に挙げると、

・再委託の承認手続の不履行
・委託事業者における再委託事業者に対する契約事項遵守（指定場所での処理、データ持ち出しの禁止など）の不徹底
・再委託事業者におけるセキュリティ確保措置の不備。在宅勤務が伴う勤務体制の横行。
・再委託事業者の従業員による自宅ＰＣへの不正コピー
・これに、ファイル交換ソフトのインストール、ウィルス感染が重なり、情報が流出。

○　セキュリティ確保は、個人情報に係る事務処理一般に必要なことであるが、住民基本台帳情報では、さらに必要性が高いのか。

⇨
・個人情報の流出による侵害は、住基情報に限られず考えられる上、実際に侵害も発生している。セキュリティ確保の必要性は同様に認められる。なるべく足並みをそろえて、セキュリティ水準を上げていくことが望まれる。
・住基情報の流出事案は、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。住基情報は、他の個人情報とは異なり、適正な管理の要請がとりわけ強いとの受け止めが世間一般にあるのではないか（詳細な検討については後述。）。

○　委託と再委託等について、どう考えるか。両者の違いを重く見るか、つながりに着目するか。

⇨
・再委託は、事業者の選定や業務の実施管理に係る市町村の関与が間接的。市町村が締結する委託契約の中では、遵守事項の義務付けが困難な面がある。
・しかし、元の委託契約の当事者である事業者は必ず委託契約上の責任を有しており、この事業者を通じて再委託事業者等を適切に管理できる可能性がある。

↓

・再委託は、市町村の事情も踏まえ、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。

○　ファイル交換ソフトを通じた情報漏洩について、どのように考えるか。

⇨
・個人情報とファイル交換ソフトは、完全な隔離が求められる。

２　実効性のある対策　～手順に沿った措置～

○　実効性のある対策として、具体的に、どのような措置・取り決めの徹底を図るのか。

⇨
・作業形態等に応じて、さらに、具体的に検討する必要があるが、これまでの検討を踏まえ、対策を挙げれば、以下のとおり。
①指定場所での処理　～　具体の場所は市町村が指定
②データ持ち出しの禁止（承諾を受けて、庁舎から庁舎以外の指定場所へ持ち出す場合を除く。）
～　承諾は市町村が行う。指定場所への移動の場合に限られる。
③（②の例外の場合の）データの暗号化処理
～　情報が流出しても、被害拡大の防止に有効。
④データの複製・複写の禁止（承諾を受けて、指定場所で作業に必要な範囲で行う場合を除く。）
～　承諾は市町村が行う。
⑤事後のデータの返還・廃棄　～　確実な履行の確保
⑥承諾を受けない再委託の禁止
～　承諾は市町村が行う。委託事業者を通じて、再委託事業者に市町村の管理が及ぶ場合に限られる。
⑦日々（一定期間）の処理記録の提出　～市町村の確認を受ける
など

・また、外部委託先の選定・契約・監督・責任追及の各プロセスにおける課題を明らかにしたうえで、経済合理性も考慮し、どのようなセキュリティ・レベルを備えるのか、対策を検討していく必要がある。
・情報の管理エリアからの”持ち出し”が基本的で重大なルール違反であり、そこに焦点を当てて、措置の徹底を図っていくべきではないか。
・規制の書き足しはできないので、将来をにらんだ水準の設定が必要との意見。

○　委託先を、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、限定する取扱いについて、どのように考えるか。

⇨
・ＰマークやＩＳＭＳ（ＩＳＯ27001）の認証取得やセキュリティ監査等を受けることにより、事業者における従業員に対するセキュリティ教育や意識レベルについて、一定水準が確保されていると見ることができる。
・ガイドラインでは、業者選定に当たっての推奨事項としているが、市町村

に対して、入札資格とするなど積極的な対応を求めることも考えられる。
・ただし、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・対応に格段の差がある場合もある。また、市町村の調達においては、公正な競争・取引条件の設定が要請される。

↓

・ＰマークやＩＳＭＳ等の認証を取得していることで、一定の水準に達しているという信頼を置くことができるのではないか。
・既存の標準・認証は抽象的にすぎる。それぞれのプロセスにおいてやるべきことを、契約に際しての具体的な発注条件として細かくつめていかないと、実際のセキュリティレベルを押さえられないのではないか。
・一つの判断要素として、市町村・事業者から、理解が得られるよう配慮しつつ、前向きに検討。

○　市町村・委託事業者のそれぞれについて、どのような対応方針をとるのか。

⇨
・市町村における十分なセキュリティ確保措置の整備、具体的な発注条件としての契約への盛り込みとそれらの遵守について、チェックの一層の強化を促す。
・委託事業者における十分なセキュリティ確保措置の整備と契約事項遵守について、従業者など実際に情報を扱う者に対する徹底・適正な管理を求める。
・委託事業者における適切な工程管理を求めるとともに、委託処理する市町村の側でも、処理の状況を確認（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つくり出していく必要がある（静的なルールだけに頼らない動的な処理態様のチェック）。そのため、あらかじめ定められた間隔で処理状況を確認できる仕組みが考えられないか。
・委託事業者を選定する際に、事業者に具体的に取るべき内容を宣言させることにより、工程管理やそのチェック・確認が行いやすくなるし、制裁も課しやすくなるのではないかとの意見がある。
・従事者のルール違反はコンプライアンスを欠く方向での価値判断によるものが大半。委託事業者側で、管理者を含めてコンプライアンスが何よりも重要であるということを認識・徹底させなくてはいけないのではないか。
・再委託の場合においても、委託事業者を通じて、上記同様に、委託処理する市町村の側で、処理の状況を確認しつつ、チェック・確認できるようにしていく必要がある。

○　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を、どのように

とらえていくか。

⇨
・「個人情報(住基情報)を業務として扱う者」とし、契約上の地位にかかわらず、対象となる行為を直接行うおそれのある者をとらえることとする。
・ただし、直接の行為者(「個人情報(住基情報)を業務として扱う者」)に着目しても、行為による責任は、体制を整え、回避措置を講じられる委託事業者等に対して、問うこととする。

○　「委託」の概念について、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あるが、どこまでを念頭に置くのか。

⇨
・個人情報(住基情報)を取り扱うという観点からは同様の状況にあるため、特に除外せず、広く対象としてとらえることとする。

３　対策実施の手法・法律上の構成

○　具体的に、対策実施のため、どのような手法を用いるのか。

⇨

ガイドライン等に基づく対応

□住基情報を含め、個人情報一般について、15年6月通知、ガイドライン等に、必要に応じ、改正・追加等を行う。市町村の個人情報保護条例・セキュリティポリシーへの規定が徹底されるよう、強く要請する。
□それぞれのプロセスにおいて、実施・遵守されるべきことを具体的な発注条件として契約条項に盛り込み、確実に行われるよう強く要請する。
□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を図る。

住基法・住基令に基づく対応

□住基情報については、今回の情報流出事件を踏まえた市町村・委託事業者に求められるセキュリティ確保措置を明確化することとし、技術的基準(大臣告示)に関し、指定場所、持ち出しの禁止と承認、暗号化等について、当該確保措置の規範性が確実に担保されるよう、改正・追加等を行う。

※ガイドライン、技術的基準をより具体化した遵守手順のひな形を提示し、その徹底を図ることとする。
※そのため、住基ネットと同様に、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ことが考えられる。
※また、委託事業者を選定する際に、事業者に具体的にとるべき内容を宣言させることにより、チェック・確認を行いやすくし、責任追及をしやすくできるのではないか。

以上の対応により、委託事業者の契約上の責任・義務の遵守の徹底を図り、セキュリティ確保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。

契約上の責任の追及としては、以下の方法が考えられる。
①契約上の履行代金の減額
②違約損害金の請求
③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(制限)
など

法律改正による対応

□住基情報について、住基法を改正し、法律に基づき、住基情報を扱う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。
□または、住基情報を含め、市町村等の行政機関が保有・管理する個人情報について、個人情報を扱う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。

○①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。
②法的な規制のための措置が、意識・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。

⇨ ・実務の観点からは、①の考え方が重要。個別具体の取組みを積み重ねることに力点を置くべき。

○住基情報について、他の個人情報と区別して法律上の特別の保護措置を講ずるのか。その場合には、区別する理由はどうなるか。

⇨ ◇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揺らぎかねない状況。

◇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ための事務の一環。基本情報は、他の情報との結合・リンクに際して欠かせないもの。適正に遺漏なく管理する必要性がきわめて大きい。
（※他の行政機関が保有・管理する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。また、民間事業者が保有・管理する個人情報は、基本的に営利目的のために収集・管理されるもの。こうした目的との関係の中で、最も適切で実効性のある保護措置を考えていくべきであり、住基情報と事情が異なると言えないか。）
・このような考え方を肯定し、あるいは、住基情報については、他の分野に先行してでも、法律改正し、特別の措置を講じるべきとの意見がある。
・また、住基情報の中でも、①基本情報の場合とそれ以外の場合、②住基の基幹システムから持ち出す場合と住基情報から出て使用されている関係情報を持ち出す場合など、それぞれ違いがあり、区別して、対策を考えていくべきとの意見がある。
・なお、市町村が保有・管理する他の個人情報についても、同様に、セキュリティ確保は必要であり、全体として、足並みをそろえて対応方策を考えていくべきとの意見も見られる。
・時間をかけても、関係者・社会全体としての合意形成を図っていく方向で考えていくべきとの意見。

○法律上の行為規制を設ける場合の対象は、どのような行為か。

⇨ 実効性のある対策に掲げる行為を基本に検討する必要がある。
①指定場所での処理
②データ持ち出しの禁止
③データの暗号化処理
④データの複製・複写の禁止
⑤事後のデータの返還・廃棄
⑥承諾を受けない再委託の禁止
⑦日々（一定期間）の処理記録の提出　など

４　罰則の取扱い

※罰則については、講じられる対策の効果や実績を踏まえて、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、十分議論・検討が必要であり、意見の一致は見られていない。

直ちに導入できないが、これまでの議論を受けて、意見を並記することとする。

○　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、さらに罰則を設けることについて、どのように考えるか。

⇨
・積極論と消極論、双方の意見が見られた。
・罰則を含めた事後の制裁の取扱いについては、事前の防止のためにどうすべきかという問題とは区分して考えていくべきとの意見がある。
・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場合、刑罰が出ていく余地はある。結果の重大性にかんがみ、前倒し、重複も考えられる。
・また、罰則を設ける場合には、保護法益をどう考えるか、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。

○　保護法益について、どのように考えるか。

⇨
・これまでの行政刑罰の考え方に従い、「住民個人の基礎的な情報が適正に遺漏なく管理されることに対する国民の信頼」と整理することは可能との意見がある。

○個人情報の流出に対して、罰則を考える場合、罰則のどのような機能を重視するか。

⇨
・①多数の者がいけないと考える行為に刑罰をかけて確認するという考え方と②専門家から見れば危険で防止すべき行為を多数の者が認識していないため、刑罰をかけて、いけない行為だと知らしめるという考え方の２つの方向があり、理論的にはどちらでも対応は可能との意見。
・②の意図で、刑罰が前に出ることには慎重。刑罰の謙抑性が大原則との意見がある。

○　個人情報の流出は、明確な故意によるものは少なく、過失によるものが多いこと、被害回復の可能性が低いことを踏まえ、どのように考えるか。

⇨
・故意にとどまらず、過失の場合もすべて対象とすることは困難。
↓
・住基制度の信頼性を確保するため、住基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、行為規制に即さない行為（不作為）に係る故意（場合によっては重過失も同様）の責任を問うことが考えられないか。
・加えて､住基情報の流出(不特定多数の者が認知できる状態に至らせた場合)という侵害結果を要件とすることが考えられないか。
・一方、侵害結果に対するつながりが極めて強いとの社会的認識が定着していない（特に、地方においてはルールの徹底が十分図られていない）中では、処罰は慎重に考えるべき、処罰範囲が広すぎるとの意見。
・法益侵害（情報漏えい）に最も近い行為に対する認識（可能性）で、罰則の可否を考えていくべきとの意見。
・行為の危険性が広く認識されていくにつれて、行為を行ったことに対する過失が認定できるようになり、いずれは故意も認定できるようになっていく、あとはどこに刑罰をかけていくかは政策判断との意見。
・監督する側として、事業者から書面による宣誓等を取って責任を課しておけば、それにもかかわらず、違反・不当な事態が生じたときには、誓約違反で種々の規制をかけられるし、侵害犯として刑罰もかけられるのではないかとの意見があった。

○　罰則の対象となる行為・態様として、どのようなものが考えられるか。

⇨
・住基情報の流出に結びつくものの、専門家として善管注意義務の下、適正に事務を遂行することにより、回避できるものを、具体の事務処理を想定しつつ抽出していく必要があるのではないか。
・委託事業者・再委託事業者や実際に処理に当たる従業者等が過度に萎縮しない方向で罰則のかけ方を考えていく必要との意見があった。

○　従業員が業務に伴って不法な行為をした場合の事業者に対する罰則について、どのように考えるか。

⇨
・両罰規定を設けることの可否も含めて、罰則の内容を検討してはどうか。
・むしろ、両罰規定により、事業者（管理者）に対する罰則に重きを置いていくべきとの意見があった。

○　個人情報の漏えいをそそのかす者にどう対応するか。

⇨
・不正目的で情報を取得しようとする者に対して罰則を考えてもよいのではな

いか。
・不正アクセス防止法における不正アクセス行為に対する罰則との均衡を考慮する必要があるのではないか。
・単なる興味目的の場合の取扱いをどうするか。情報保護の重要性の観点から決定すべきとの意見があった。

○　刑罰ということではなく、秩序罰ならどこまでの対応が考えられるか。

⇨
・単純行為犯に対して､一定の軽い秩序罰を課すことはあり得るのではないか。
・行為規制に秩序罰が付けられれば、相当の効果が得られるのではないか。
・一方、過料程度で持ち出しを抑制できるかは疑わしい。現場での職務意識に対して防波堤としては弱いとの意見があった。
・そもそも規制しようとする行為は、行政処分として課される秩序罰になじむ適切なものか。

○　その他

・ファイル交換ソフトの危険性については、関係者には規範意識があるかもしれず、罰則を設けることも可能ではないか。
・納期が迫って間に合わないために、不適切な行為をしてしまうということから、そうなる以前の工程管理の段階で、対応を考えなくてはならないのではないか。
・悪意でなく必要にかられて不適切な行為をしてしまうという実情ならば、いきなり制裁として刑罰を持ち出すのはどうか。
・具体的な侵害発生の前の段階で、条例で処罰している例があり、そこからどこまで踏み込めるかということではないか。