資料１

前回（第４回）の論点整理に際しての主な意見

１　実効性のある対策について

○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。

○今回の事案に即すると、チェックポイントの明示は大変重要であり、個別具体にきちんと整理し、示していくことが必要。

○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。

○日々（一定期間）の処理記録を提出させ、市町村の確認を受けることはたいへん効果があるのではないか。

○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。

○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。

○ 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。

２　認証等による限定について

○委託先の限定に当たっては、ＩＳＯなどの認証を取得している事業者のほか、情報セキュリティ監査や個人情報保護に関するシステム監査を受けている事業者を相手方とすべきである。

○Ｐマークは選定の内容を見ている面があり、何らかの推奨になる。住基の基本的な本体を守るという意味で、いろいろな発想があり得る。

○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。選定する際の一つの判断材料にはなる。

○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。

３　対策実施の手法について

○実務上の観点からは、前の段階での措置を尽くして、次の段階に進んで行くとの考え方が重要。個別具体の取組みを積み重ねることに力点を置きたい。

○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。

○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。

４　罰則の取扱いについて

○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。

○保護法益については、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。

〇①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である。

〇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のではないか。

〇法益侵害（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。

〇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である。

〇行為規制と刑罰のかけ方は、本来連動していなければならないはずである。

〇刑罰の謙抑性が大原則であり、刑罰は最後の手段として考えるべきである。

〇監督する側として、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。

〇委託事業者・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がある。

〇行為者に対する罰則を考えるよりも、むしろ、両罰規定を用いて事業者（管理者）に対する罰則を重点的に考えていくべきである。

〇情報漏えいの際の罰則は、不正アクセス防止法等の他の類似の法体系における措置との均衡を考慮する必要がある。

〇処罰範囲を限定するため、営利目的などの不正の目的を加えることも必要で

はないか。この場合、不正競争防止法に規定される情報窃盗の規定にかなり近い議論になってくる。

○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。

5　秩序罰について

○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。

○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のではないか。

参考：第３回検討会
資料１

前回（第３回）の論点整理に際しての主な意見

１　対策に当たっての留意事項について

○対策は、実務上は条例等のレベルで既に相当行われている。実際はかなり進んでいる。

○電算処理の委託の概念の整理が必要。例えば、オペレーションの業務委託やシステムの機器保守委託など、どこまでどういうものがあてはまり、どう位置づけ、整理するのか。

○市町村から受託者に対して、契約の際にどこまできちんと手順を示せるのか。セキュリティポリシーやマニュアルをどう作っていくか。標準例的なものを作ることも１つの対策。

○問題状況の整理、行為規制など全体を通じて、事業者と従業員をもっとはっきり分けて整理した方がよい。

○委託者が契約上の責任を負うことを前提に、従業員は委託者が課された義務をしっかり履行できるよう労働契約上の義務・責任を負う。こうした法律関係が契約の枠組みの基本にある。

２　再委託や多重下請の場合の考え方について

○多重下請では、元の契約の中で再委託や再々委託を行う場合の手順・条件を決めている。

○元請責任は必ず存在するのだから、市町村はそれを通じて再委託事業者等を管理するのではないか。

○承諾や指示があったとしても、多重請負契約が下に流れていったときには、第三者のために行っているに過ぎず、一方的で拘束力は及ばない。

○下請事業者を履行補助者として認定できれば、市町村は、多重請負の下の方

まで契約責任を追及できる。

○労働法規の適用の場合、契約形態だけでなく、実質や運用実態を見ることになるが、民事上の契約関係そのもののとらえ方は変わらない。事業者間同士の契約については、労働法上の扱いを特別に考えなくてもよい。

○再委託される場合、再委託先の事業者との関係では労働法上の問題は起きてこない。

３　行為規制について

○事業者を通じて従業員に対して情報流出を防ぐ体制を徹底させることを強調すべき。

○行為規制以降において、事業者と比べて従業員が前面に出すぎな印象。組織の末端にもかかわらず、事業者が体制を整えない中で、違反した従業員が重い責任を問われるのは、制度として適当でない。

○実行者と管理者がいるが、どう統制し、どう責任を問うのか。既に、基準やマニュアルは相当あり、それらをどう実施・運用させるかという観点から、結論を出していくべき。

○行為規制の対象者を、「委託者等」ではなく「住基情報を扱う者」として一括でとらえることに賛成。再（々）委託や派遣等にも対応できる。

○民間の委託者を自治体同様の専門性を有する行為者として扱うのは賛成。

○行為規制に関しては、その承諾の手順や要件について、相当慎重に検討するべき。

○実務的に上司の承諾が安易に行われており、組織全体のポリシーとの違いが出てきてしまう。これに対応するため、ＣＩＯのような上級責任者が自らリスクを引き受けるプロセスをガイドライン化する方策があってもよい。

○「持ち出し禁止」をどう規制するか。

〇データ持ち出しの場合の承諾は、指定された場所への移動だけを念頭に置いており、受託事業者の従業員の処理の都合によるものは想定していない。

〇暗号化はかなり有効な手段ではないか。

〇認証取得について積極的な対応とあるが、取得していても事件を起こすこともある。また、非関税障壁との指摘を受ける可能性があり、競争政策、経済法制との関係でどこまでできるかは難しい面もある。

4　罰則について

〇刑罰を考える前に他にできることをしっかり検討しておいた方がよい。まずは契約の枠組みの中で情報流出を防止できる仕組みが機能するよう検討し、うまく機能しないときに補完的に罰則を伴う行為規制の可否を考えるべきではないか。

〇行為規制は事前の漏えい防止システムの構築として管理者はどういうことを行うべきかの問題。罰則は、漏えいしてしまった後の制裁の問題。混乱が生じないよう両者を分けて考えるべき。

〇罰則については、保護法益などより詳細な議論が必要。

〇保護法益は、冒頭で議論するのがよいのか後ろがよいのか。その内容としては、「制度の信頼性」なのか。その他にも考えられるのか。

〇実行者に厳しい責任を問うのは、自治体の実務からすると行き過ぎである。

〇外部からそそのかされたり、故意で情報を流出させた場合、実行者の責任を問うべきか、適切な管理監督を行っていないということで管理者が責任を問われるのか。

〇情報の流出という侵害結果を要件とするとの意味は、「不特定多数の者が認知できる状態に至らせた」ことを指すのか、暗号化されたものが流出した場合も含むのか。

５　その他

○住民基本台帳情報も以前は営利目的に使われていた側面がある。住基情報のうち、基本情報は、他の情報とのリンクの際の軸となるものであり、管理の必要性は非常に高い。

○住民基本台帳に係る情報以外の個人情報であっても、自治体から見れば、同じように重要なもの。何らかの方向性・対応について言及すべき。