資料5－4

総行情第47号
平成19年6月1日

各都道府県個人情報保護対策担当部長　殿
各都道府県市区町村行政担当部長　殿

総務省自治行政局地域情報政策室長

外部委託に伴う個人情報漏えい防止対策に関する対応及び留意事項

外部委託に伴う個人情報の漏えいについては、先般、ファイル交換ソフト「Ｗｉｎｎｙ」を介して全住民の個人情報が漏えいするという大変遺憾な事案の発生を受けて、平成19年5月25日付け総行情第42号「外部委託に伴う個人情報漏えい防止対策の徹底について」により、防止対策の徹底を各地方公共団体にお願いしたところであります。

これまで総務省においては、外部委託に関する条例及び運用上の取り扱いについて、「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16日付け、総行情第91号）及び「地方公共団体における情報セキュリティーポリシーに関するガイドライン」（平成18年9月版）により各地方公共団体に対し対応をお願いしてきたところですが、今回の事案を踏まえ、外部委託に伴う個人情報の漏えい防止対策として必要と考えられる対応及び留意事項を別添のとおり取りまとめましたので、各地方公共団体におかれては、これらの資料を併せご参照頂き、個人情報保護条例や契約事項の見直し、受託業者に対する監督の強化等に取り組まれますようお願いします。

また、管内市区町村にも周知していただき、外部委託に伴う個人情報漏えい防止対策に関し、必要な助言、情報の提供等に努められますようお願いします。

【問い合わせ先】
総務省自治行政局地域情報政策室
（担当：池田課長補佐、脇本係長、利根事務官）
TEL：03－5253－5111（内線5525）
FAX：03－5253－5529
E-mail：k.tone@soumu.go.jp

「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）における外部委託関係の記述	今回の情報漏えい事案を踏まえ、必要と考えられる対応及び留意事項
第３　個人情報保護条例の制定又は見直しに当たっての留意事項 ４　外部委託に関する規制 地方公共団体が個人情報の取扱いを外部に委託しようとする場合には、委託先において個人情報の漏えい等の問題が生じないようあらかじめ適切な措置を講じておくことが必要である。従来、個人情報の外部への漏えい等に関する事案の多くが、委託先からのものであったことから、外部委託に関する規制を設けることは重要である。このため、個人情報保護条例に、個人情報の保護に関して必要な事項を委託契約に盛り込むことを義務付ける等、委託先においても個人情報が適切に保護されるよう必要な措置を講ずることを当該地方公共団体に義務付ける等の規定を設けることとすべきである。 また、受託者又は受託者であった者に対しては、受託業務に関して取扱う個人情報の安全確保について当該地方公共団体と同様の義務を負い、個人情報の漏えい防止等のために必要な措置を講ずることを義務付けるとともに、受託事務従事者又は従事していた者に対しては、受託業務に関して取扱う個人情報の保護について当該地方公共団体の職員又は職員であった者が負う義務と同様の義務を課す旨の規定を設けることが適当である。	平成18年4月1日現在において、個人情報保護条例を制定している地方公共団体において、当該条例に外部委託時の規制に関する規定を設けている割合は次のとおりである。 ・個人情報保護条例に受託業者等の責務規定（外部に情報の処理を委託する際、受託業者又は受託業務に従事する者に対し、個人情報の漏えい等の個人情報の保護に必要な措置を講ずる義務を課す規定）を設けている団体は、条例制定団体の91.4%である。 ・個人情報保護条例に契約等によるデータ保護の確保措置（地方公共団体が受託業者に対し、契約等により個人情報を保護するため必要な措置を講ずるよう義務づける規定）を設けている団体は、条例制定団体の76.9%である。 ・個人情報保護条例に上記のいずれかの規定を定めている団体は、条例制定団体の97.3%である。 個人情報保護条例にこれらの規定を設けていない地方公共団体においては、早急に規定を設けることが望まれる。また、既に規定を設けている場合には、受託業者に対し、個人情報保護条例上の義務について十分に説明し、受託業務の従事者（再委託先を含む）に理解させるよう求める必要がある。
６　罰則 一般に、職員等の責務の履行の確保は、服務規律の確立、厳正な個人情報の取扱いの徹底等によることが基本となるものである。しかしながら、行政機関法においては、行政機関におけるＩＴ化の進展状況にかんがみ、行政に対する国民からの信頼を確保するため国家公務員法の守秘義務違反等に係る罰則に加え、以下のような罰則を規定しているところである。 ①行政機関の職員若しくは職員であった者又は受託業務に従事している者若しくは従事していた者が、正当な理由がないのに、個人の秘密に属する事項が記録された電子計算機処理に係る個人情報ファイル（その全部又は一部を複製し、又は加工したものを含む。）を提供したときは、２年以下の懲役又は１００万円以下の罰　金に処する（第５３条）。 ②行政機関の職員若しくは職員であった者又は受託業務に従事している者若しくは従事していた者が、その業務に関して知り得た保有個人情報を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、１年以下の懲役又は５０万円以下の罰金に処する（第５４条）。 ③行政機関の職員がその職権を濫用して、専らその職務の用以外の用に供する目的で個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集したときは、１年以下の懲役又は５０万円以下の罰金に処する（第５５条）。 このような国における法整備の状況を踏まえ、各地方公共団体においても、関係機関と協議の上、個人情報保護条例に罰則を設けることを積極的に検討することが望ましい	平成18年4月1日現在において、個人情報保護条例を制定している地方公共団体において、当該条例に受託業者等を対象とする罰則規定（受託業者又は受託業務に従事する者が守秘義務等の規定に違反した場合等に受託業者又は行為者若しくは代表者等に罰則を科する規定）を設けている割合は、59.0%にとどまっている。 個人情報保護条例に受託業者等を対象とする罰則規定を設けていない地方公共団体においては、早急に関係機関と協議の上、条例に罰則を設けることを検討することが望まれる。また、既に罰則を置いている場合には、受託業者に対し、個人情報保護条例上の罰則について十分に説明し、受託業務の従事者（再委託先を含む）に理解させるよう求める必要がある。

「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月版)における外部委託契約関係の記述	今回の情報漏えい事案を踏まえ必要と考えられる対応及び留意事項 (注) 以下は、対策を網羅したものではないことに留意願います。
3．7．4．外部委託 【趣旨】 情報システムの外部委託を行う際は、各団体で直接管理する場合に比較して情報漏えい等のリスクが増大する。実際にも外部委託事業者からの情報漏えい等の事案が多数発生している。このような事案を防止するために、情報セキュリティを確保できる委託先を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。 このことから、外部委託を行う際に、情報セキュリティ確保上必要な事項について規定する。 なお、個別団体が単独で外部委託する場合だけでなく、共同アウトソーシングやＡＳＰサービス利用の形態等により地方公共団体が共同で外部委託する場合にも対策を行う必要があることに留意する。	外部委託に際して取るべき情報セキュリティ対策は、取り扱う情報の重要性とリスクの大きさを勘案して適切な水準のものとする必要があるが、依然として外部委託先からの情報漏えい事案が発生していることに鑑み、個人情報の取扱いを外部に委託する場合には、厳格な情報セキュリティ対策を講じる必要がある。
【例文】 (1)外部委託先の選定基準 ①情報セキュリティ管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。 ②情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況等を参考にして、事業者を選定しなければならない。【推奨事項】 (2)契約項目 情報システムの運用等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・委託先の責任者、委託内容、作業者、作業場所の特定 ・提供されるサービスレベルの保証 ・従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務 ・再委託に関する制限事項の遵守 ・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・市による監査、検査 ・市による事故時等の公表 ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)	

（３）確認・措置等

情報セキュリティ管理者は、外部委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて最高情報統括責任者に報告しなければならない。

（解説）

（１）　外部委託先の選定基準

外部委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

（注１）これらの選定方法については、「公共ＩＴにおけるアウトソーシングに関するガイドライン（平成 15 年３月　総務省）」を参照されたい。

また、外部委託事業者の選定に当たり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

（注２）現在の最新の規格である ISO/IEC27001 については、財団法人 日本情報処理開発協会のホームページ（ISMS 適合性評価制度）を参照されたい。

入札により外部委託先を選定する際に、一定の情報セキュリティ対策をとっていない事業者は、入札参加を制限する方法もありえる。また、総合評価落札方式や公募型プロポーザル方式による公募により外部委託先を選定する場合には、情報セキュリティ対策について評価点を高くする方法もありえる。

（２）契約項目

外部委託事業者に起因する情報漏えい等の事案を防ぐため、各団体で実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要がある。以下に示す項目について、委託する業務の内容に応じて明確に要件を規定することが必要である。

①　情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

外部委託先要員に対して、情報セキュリティポリシー及び情報セキュリティ実施手順について、委託業務に関係する事項を遵守することを定める。

外部委託事業者には、情報セキュリティポリシー及び情報セキュリティ実施手順のうち、委託業務に関係する事項を十分に説明し、委託業務への従事者（例外的に再委託を承認している場合には、再委託先の従事者を含む）に理解させるよう求めることが必要である。特に、情報漏えい防止のため、再委託の制限、情報の無断持ち出しの禁止、業務終了後のデータの返還・廃棄、私用パソコンの使用禁止その他の措置について、確実に説明し、受託業務の従事者全員に理解させることが必要である。

また、個人情報保護条例、特に外部委託事業者及び従事者に課された義務、罰則についても十分説明し、受託業務の従事者全員に理解させることが必要である。

②　外部委託事業者の責任者、委託内容、作業者、作業場所の特定

外部委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続きを定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。

個人情報の取扱いを外部委託する場合には、作業場所を庁舎内等指定する場所に特定し、業務の従事者が外部に情報を持ち出すことを防止する措置（入退室管理、パソコンや外部記録装置の持込・持出の禁止、例外的に情報の外部持ち出しを認める場合の承認手続き、私用パソコンの禁止等）を確認することが必要である。

③　提供されるサービスレベルの保証

通信の速度及び安定性、システムの信頼性の確保等の品質を維持するために、必要に応じて、

サービスレベルを保証させる。 ④　従業員に対する教育の実施 外部委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。	従業員に対する教育は、受託業務の従事者全員に対し定期的に行わせることが必要である。また、その内容が十分であるか、特に情報漏えい防止のため、必要な教育がおこなわれていることを確認することが必要である。また、必要に応じ、委託事業者に対し、従業員より守秘義務や情報漏えい防止に関する誓約書を求める。 また、退職者から情報が漏えいすることを防ぐため、退職時に情報の返却・廃棄等を確認することを求め、必要に応じ、退職者から退職後の守秘義務等に関する誓約書をとることを求める。
⑤　提供された情報の目的外利用及び受託者以外の者への提供の禁止 外部委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。 ⑥　業務上知り得た情報の守秘義務 業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。	
⑦　再委託に関する制限事項の遵守 一般的に、再委託した場合、再委託先のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託先の業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認した上で許可しなければならない。	例外的に再委託を許可する場合においても、再委託の契約内容において、ここに定める事項と同等の内容が含まれていることや外部委託事業者による再委託先の監督体制、再委託先における情報セキュリティ対策が十分にとられており、外部委託事業者と同等の水準であることを確認することが必要である。
⑧　委託業務終了時の情報資産の返還、廃棄等 委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を下げる。	委託業務終了時の情報資産の返還、廃棄等を徹底させるため、必要に応じ委託業務終了時に委託先事業者に点検させ、返還、廃棄等が完了したことの報告を求める。
⑨　委託業務の定期報告及び緊急時報告義務 定期報告及び緊急時報告の手順を定め、委託業務の状況を適切かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、外部委託業者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。	
⑩　市による監査、検査 外部委託事業者が実施する情報システムの運用等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。	例外的に再委託を承認する場合には、地方公共団体が再委託先にも直接監査や検査を行うことができることを定めておくことが必要である。
⑪　市による事故時等の公表 委託業務に関し、情報セキュリティに関する事件・事故等が発生した場合、住民に対し適切な説明責任を果たすため、当該事故等の公表を必要に応じ行うことについて、外部委託事業者と確認しておく。	受託事業者が情報漏えい等の事故発生又は事故発生のおそれがあることを発見した場合には、速やかに報告させることについても契約書等により確認しておく。
⑫　情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等） 外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約上明記しておく。	情報漏えい等が発生した場合にも損害額算定に困難が伴うことを踏まえ、予め違約金を定めておく方法もありえる。

（注３）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。 （注４）指定管理者制度に関する考慮事項 指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。 （３）　確認・措置等 情報セキュリティ管理者は、外部委託事業者において十分なセキュリティ対策がなされているか、定期的に確認し、必要に応じ、改善要求等の措置を取る必要がある。確認した内容は定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大な侵害行為が発見された場合には、速やかに最高情報統括責任者に報告を行う。	確認の方法として、個人情報保護条例や契約の遵守等について定期的に報告を聴取するほか、必要に応じ立ち入り検査を実施する。 確認内容として契約事項の遵守状況の他、十分なセキュリティ対策がとられていることを確認する必要がある。特に、再委託の制限、情報の無断持ち出しの禁止、業務終了後のデータの返還・廃棄、私用パソコンの使用について、違反がないか確認することが必要である。 確認の結果、必要があれば、改善要求等の措置をとる。改善要求を行った場合には、委託事業者が実際に取った措置について、報告徴収や検査を改めて実施する。 例外的に再委託が行われている場合、委託先を通じて個人情報の保護が適切に行われているかについて報告を求めるほか、必要に応じて、地方公共団体自らが検査の実施などの監督を行い、必要があれば改善要求等の措置をとる。 個人情報保護条例及び委託契約に違反して個人情報の漏えい等の事故が発生した場合には、厳正な措置（違約金・損害賠償請求・契約解除・入札参加資格の制限等）を実施する。