個人情報保護対策の強化と円滑な運用に向けて

2005年4月

社団法人　電子情報技術産業協会

社団法人　情報サービス産業協会

目　次

はじめに

本資料は、平成17年4月1日からの個人情報保護法の全面施行に当たり、地方公共団体から個人情報を取扱う業務等を受託する際に、預託を受けた個人情報をどのように安全に取扱うべきかを検討し整理したものです。

本資料の構成は、第1章で個人情報保護法制の体系と個人情報保護法関連の用語を説明しています。第2章では、システム構築･維持管理作業において取扱われる個人情報の考え方を述べています。情報システムの開発プロセスに対応してどこで個人情報を取扱う可能性があるかを明らかにすると共に、ダミーデータを使用する事により個人情報を取扱う可能性そのものを排除して情報漏洩のリスクを軽減する事を提案しています。第3章では、個人情報保護の強化に向けた取組みについて地方公共団体と受託者の責任と義務について述べています。また、IT業界には元請をす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いたしますが、このようなIT業界の実情に対応した再委託の考え方について提案をしています。

地方公共団体における情報システムの開発に当たって、個人情報の実効的な保護のために本資料をご活用いただければ幸甚です。

2005年4月

社団法人　電子情報技術産業協会
会長　安藤　国威

社団法人　情報サービス産業協会
会長　佐藤　雄二朗

1. 個人情報保護法制の位置づけ

1．1　個人情報保護法制の体系イメージ

個人情報保護法制の体系イメージを図 1-1 に示します。個人情報保護法制では、官民を通じた基本法の部分と、民間の事業者に対する個人情報の取扱いのルールの部分から構成されています。

図 1-1 個人情報保護法制の体系イメージ

http://www5.cao.go.jp/seikatsu/kojin/jigyousha/03.pdf

1．2　個人情報保護法関連の用語説明

(1) 個人情報

生存する個人に関する情報であって、特定の個人を識別できる情報。

例）住所、氏名、ＴＥＬ、年齢、ﾒｰﾙｱﾄﾞﾚｽ、勤務先、家族構成、趣味、顔写真、クレジット番号等々。

(2) 個人データ

個人情報のうち、個人情報データベース等 を構成するもの。

(3) 個人情報データベース等

個人情報を含む情報の集合物であって、電算機を用いて検索できるように体系的に構成され、または容易に検索できるように体系的に構成されたもの。

(4) 保有個人データ

個人データのうち、個人情報取扱事業者が開示、内容訂正、追加/削除、利用停止、消去、第三者への提供を行う権限を有するもの。

2．情報システム構築･維持管理作業において取扱われる個人情報

2．1　個人情報を取扱う事務の考え方

仙台市「情報システム処理に伴う個人情報に係る外部委託に関するガイドライン」(http://www.city.sendai.jp/kikaku/zyo-kikaku/joho-sekyu/guidelines.html)を例に、情報システム処理を伴う個人情報を取扱う事務の考え方を以下に示します。

(1)　情報システム処理を伴う個人情報を「**取扱う**」事務の考え方

① 個人情報を記録する公文書を使用して行なう業務

個人の氏名、生年月日その他の記述または個人に付された番号、記号その他の符号により当該個人を検索し得る状態で個人情報を記録する公文書を使用し、情報システムを用いて個人情報の入力、変換、集計、修正、編集、蓄積、更新、検索、消去、出力、またはこれに類する処理を主として行う業務及び情報システムを用いて出力された帳票の製本、封入、封かん処理を行う業務。

<例えば>

台帳などのデータを入力して業務用の一覧表を作成する。

打ち出された通知書を製本し封筒に入れて発送する。

② 個人情報を記録する公文書を作成する業務

情報システムを用いて個人情報の入力、変換、集計、修正、編集、蓄積、更新、検索、消去、出力、またはこれに類する処理を行い、個人の氏名,生年月日その他の記述または個人に付された番号、記号その他の符号により当該個人を検索し得る状態で個人情報を記録する公文書を作成する業務。

<例えば>

イベントなどの参加申込書を受け付け、それを入力し一覧表を作成する。

(2) 情報システム処理を伴う個人情報を「**目視する**」事務の考え方

上記規定以外の「システムの状態監視」や、地方公共団体の施設内において職員の監督下で行なう「ハードウェア･メンテナンス」、「ソフトウェア･メンテナンス」については、動作確認等の作業中にシステムに格納されている個人情報を一見する可能性があります。本資料ではこの一見する行為を「目視」と定義します。

2．2　情報システムのライフサイクルにおける地方公共団体及び受託者の役割と個人情報の取扱い

情報システムの企画、設計･開発、運用のライフサイクルの中で取扱う個人情報について、「国の行政機関における情報システム関係業務の外注実施ガイドライン」（http://www.soumu.go.jp/gyoukan/kanri/a_01_f.htm）で示されている企画･調整、設計･開発、運用、監査の各業務の分類を例に、情報システム構築･維持管理作業における地方公共団体及び委託者の役割と個人情報の取扱いについて表2-1に示します。

なお、個人情報の漏えい等のリスクを低減させるためには、各工程における作業内容について個人情報を含む業務の明確化、外部委託する際の作業内容、職員の監督、作業場所等を整理し、「どのようにしたら個人情報を保護することが実現できるか」を視野に入れ、契約条件を含めて具体的なルールを策定する必要があります。

また、個人情報漏えい等のリスク低減の観点では、地方公共団体から受託者へ個人情報をご提供いただかなければ実現できない作業もございますが、情報システムの設計・開発段階における単体・結合テストなどダミーデータで対応可能な作業は、ダミーデータの使用を徹底するなどの対策も有効です。

表2-1 情報システム構築･維持管理作業における地方公共団体及び受託業者の役割と個人情報の取扱い

情報システム関係業務			地方公共団体	受託者	個人情報取扱
企画・調整段階	企画業務	情報システム化の中･長期計画策定	立案･決定	－	－
		情報システム化案件の調査･分析	評価･承認	実施	－
		最新技術動向の調査･分析			－
		安全対策基準の策定	評価･決定	立案	－
		予算･機構定員要求	実施	－	－
	委託業者管理				－
設計・開発段階	プロジェクト管理	全体計画	立案･決定	－	－
		スケジュール管理	実施	詳細な管理を実施･報告	－
		品質管理			－
		課題管理			－
	システム分析	現状の調査･分析	評価･承認	実施	－
		システム要求要件･条件の明確化			－
		システムの基本機能、処理概要の明確化			－
		ハードウェア･ソフトウェア構成の明確化			－
	基本設計	入出力設計			－
		データベース設計			－
		ハードウェア構成設計			－
		ソフトウェア構成設計			－
		システムインターフェース設計			－
		システム処理設計			－
		システム運用手順設計			－
		ネットワーク設計			－
		安全対策の設計			－

情報システム関係業務			地方公共団体	受託者	個人情報取扱
設計・開発段階	詳細設計/開発	入出力設計	評価・承認	実施	―
		プログラム設計			―
		プログラミング			―
	プロトタイプ手法による開発				―
	単体・結合テスト	テストの企画・実施			―
	マニュアル作成	運用・利用マニュアルの作成			―
	運用準備	導入・移行（本番データによる総合テスト）			取扱う可能性のある業務
	委託業者管理		実施	―	―
運用段階	システム運用管理	システム運用計画	立案・決定	―	―
		システムの運用状況の管理	実施	詳細な管理を実施・報告	―
		システムの障害状況の管理			―
		システム資源の管理状況の管理			―
	データ入力	スケジュールの作成・入力作業	評価・承認	実施	取扱う可能性のある業務
	データ出力	スケジュールの作成・帳票配布			取扱う可能性のある業務
	データ管理	機密保護対策	規程策定／実施状況の評価・承認	取扱い手順等作成／対策の実施	―
		データ資源の管理	評価・承認	実施	―
	システム運用	運用スケジュールの作成	評価・決定	立案	―
		オペレーション	評価・承認	実施	取扱う可能性のある業務
		障害対応			取扱う可能性のある業務
		状態監視			目視する可能性のある業務
	システム資源管理	ハードウェア資源の管理			―
		ソフトウェア資源の管理			―
		ネットワーク資源の管理			―
	安全対策	安全対策の検討／見直し・改善計画	評価・決定	立案・実施	―
	メンテナンス	ハードウェア・メンテナンス	評価・承認	立案・実施	目視する可能性のある業務
		アプリケーション・メンテナンス			目視する可能性のある業務
	利用者支援	教育・訓練			―
		ヘルプデスク	評価・承認	実施	―
	委託業者管理		実施	―	―
監査段階	システム監査計画		立案・決定	―	―
	システム監査の実施		評価・決定	実施	―
	監査結果の評価		実施	―	―
	改善計画		評価・承認	立案・実施	―
	委託業者管理		評価・承認		―

3．個人情報保護の強化に向けた取組みについて

3．1　地方公共団体･受託者の責務

地方公共団体が発注する業務における個人情報保護上の責任･義務について、取扱い区分ごとに整理すると次のとおりとなります。

なお、責任範囲の明確化や契約を遅延なく実行するためにも、調達の公示において個人情報取扱いの有無を地方公共団体が明示する事が求められます。

表3-1　責任の範囲

区分	地方公共団体	受託者
「取扱う」業務を発注／受託する場合	個人情報保護条例に基づいた受託者に対する安全対策･監督責任を負う。	当該地方公共団体の委託先監督義務の対象となり、安全対策義務を負う。 安全対策義務については当該地方公共団体との契約に基づく場合と、当該条例自体に基づく場合がある。 なお、再委託を行う場合には、再委託先を管理･監督する責任を負う。
「目視する」業務を発注／受託する場合	個人情報保護条例に従うと共に、契約書で秘密情報の取扱い義務を受託者に課す責任がある。	契約上の秘密保持義務を負う。
「取扱わない」業務を発注／受託する場合	作業に必要な情報を提供する場合は、契約書で秘密情報の取扱い義務を受託者に課す責任がある。	契約上の秘密保持義務を負う。

3．2　個人情報の実効的な保護に向けて（ご提案）

IT業界では、技術革新や技術の多様化という環境の中で柔軟かつ迅速な事業展開をすべく、地域、業務分野、技術あるいは開発工程に対応してグループ会社や子会社を地方に置き、ノウハウや人員等の有形･無形の資産を分散して保有するという事業形態をとることで一貫して安定した品質を確保しています。

これらはまた、自治体における企業誘致政策に呼応して設立される側面もあり、地域経済への寄与や雇用の確保に大きく貢献していることは周知のとおりです。このような背景に鑑み、個人情報の確実な保護のために、以下3点をご提案します。

(1) 個人情報を取扱う業務における再委託への対応
　　－ 「再委託に関する承認申請書」の活用 －

個人情報保護上の責務を遵守するため、再委託する業務に個人情報の取扱いが含まれる場合には、取扱う個人情報ごとの安全管理の方法を作成した上で、再委託先の企業情報、個人情報の取扱責任者などを反映した**「再委託に関する承認申請書」**を用いて地方公共団体の承認を得ることで実効性を確保したいと考えます。

(2) 個人情報を目視する業務や個人情報を取扱わない業務の再委託への対応

地方公共団体の標準的な発注契約書では、受託者に対して原則として再委託を禁止し承認制としていますが、事務工数を増加させるばかりか、承認手続きが遅延した場合には、開発スケジュール全体に悪影響が生じる可能性があります。このため、個人情報を目視する業務や個人情報を取扱わない業務を再委託する場合については、事務工数軽減の観点から、**再委託先の届出を行う（届出制）**ことによって効率化を図るべきと考えます。

以上の考え方を基にした情報システム構築･維持管理作業については、次の契約条文設定することで個人情報の保護責務を確保できるものと考えます。ご参考になれば幸甚です。

条文案

＜甲：発注者、乙：受託者＞

第〇条 再委託について

乙は、個人情報を取扱う業務を第三者に再委託(複数段階の再委託を含む)する場合は、事前に「再委託に関する承認申請書」を提出し、甲の承認を得るものとする。なお、当該承認手続が完了するまでの間、当該業務に支障が生じたとしても、乙は責任を負わないものとする。

2 乙は、個人情報を目視する業務または個人情報を取扱わない業務を第三者に再委託(複数段階の再委託を含む)する場合は、「再委託に関する届出書」 にて甲に届け出るものとする。

3 乙は、前 2 項のいずれの場合であっても、本契約に基づき乙が負う義務と同等の義務を再委託先(複数段階の再委託先を含む)に課すものとする。

(3) ダミーデータの活用によるリスク回避

前述2．1のとおり、情報システムの開発･運用に当たっては、地方公共団体が保有する個人情報を外部の者が取扱うケースは、総合テスト、データ入力、オペレーション等に限られています。

従いまして、地方公共団体が、個人情報に関わる監督責任を徒に拡大しないよう、架空のデータ（ダミーデータ）を作成して、システム開発に利用することが極めて有益です。具体的には、開発したシステムに関わる単体テストや結合テスト等、受託者が行なう開発作業に対して、地方公共団体がダミーデータを提供することで、当該プロセスにおける監督責任と、個人情報が漏洩するリスクを回避することが可能です。ダミーデータの作成に当たっては、地方公共団体と受託者の協力があって可能となるため、情報システムに関わる委託契約の際に、両者が十分に認識を合わせておく必要があります。

おわりに

個人情報を取扱う業務等を想定して情報漏えいを防ぐための仕組みと方法について述べてきましたが、最後に本資料を作成した背景を含めて、個人情報保護に対する私共の考えを再度申し上げます。

昨今のIT業界は、他の業界と同様にグローバルな競争の激化に対して、様々な経営努力に取り組んでいます。例えば、大手ITベンダーは、不採算事業からの撤退を進める一方で、会社分割・子会社化等により、経営の効率化を図りながら全体としては企業集団を形成し一体的な経営を行うことによって、経営基盤の強化を図ってきています。また、中小のITベンダーやソフトハウスは、大規模システムの開発に参入しノウハウを蓄積しつつ、様々なニーズに対応するために、ソフトによる付加価値の差別化で存在意義を明確にしてきています。さらに、国内各地域においてお客様に密着したサポートを実現し、かつ、地域経済の活性化や産業クラスタの担い手になるべく、各社は、ソフト開発関連会社を地方に展開しています。地方への関連会社の設立に当たって、地元地方公共団体の積極的な誘致があることは言うまでもありません。

このようなIT業界の構造の中で、地方公共団体が情報システムの開発や運用を外部に委託する場合、委託する作業が個人情報の取扱を含むものか否かを明確に区別し、地方公共団体と受託者がそれぞれのケースに応じた最善の対応を取ることが肝要です。現在では、個人情報を取扱わない業務を外部に委託したケースでも、個人情報を取扱う業務を委託した場合と同様の責任と義務が両者に発生する場合が散見されます。これは、委託者である地方公共団体にとっても、無用な責任を自らに課すことに他なりません。

また、受託者が大手ITベンダーとなり、同社が同社の一部機能を切り出して地方に設立した子会社に再委託を希望する場合、地方公共団体から他の独立した会社と同様に再委託禁止の扱いをされるケースがあります。親会社がすべての責任を負うグループ経営の構造に加え、独占禁止法上では「親子会社間の取引は実質的に同一企業内の行為に準ずるものと認められるときには、親子会社間の取引は、原則として不公正な取引方法による規制を受けない」とされています。また、地域に子会社を設立しているのは、地域経済への貢献という背景もあります。このような状況を鑑み、グループ内の子会社への再委託に対しては、再委託そのものの解釈に対して弾力的な運用をお願いしたいと思います。

個人情報保護法の全面施行を機に、地方公共団体とITベンダーは個人情報の保護のために今まで以上に密接な連携を取ることが必要です。大手ITベンダーは、各地域の関連会社に個人情報の保護・管理を徹底させると共に、地元 IT ベンダーと協力してIT社会の発展に努力して参ります。

以上