

個人情報保護に関するGIS技術研究、開発を行う
建設関連事業者のガイドライン
(第二版)

平成18年11月

NPO法人 全国GIS技術研究会

はじめに

平成15年5月に制定された「個人情報の保護に関する法律」(以下、「個人情報保護法」という。)が、平成17年4月1日から全面施行されて以来1年が経過をいたしました。この間日本の多くの業界がそれぞれのガイドラインを作成し、個人情報の適正な取り扱いに向け取り組みを開始してきましたが、個人情報の漏えい等の事故は減少するどころか増加の傾向さえ感じられる今日でございます。

NPO法人全国GIS技術研究会におきましても平成17年10月に「個人情報の保護に関するGIS技術研究、開発を行う建設関連事業者のガイドライン」を発表してまいりましたが、基準とした日本工業規格のJISQ15001が平成18年5月に大幅改正されたことに伴いこのガイドラインの見直しをし、第二版を発表することとなりました。

個人情報保護法は、事業者の保護水準を一律に規定せず、業種業態に応じて適切に対応を選択するよう事業者に求めるものです。又、各省庁が策定したガイドラインは、自主的選択に当たっての考慮のポイントを示したものです。一方、JISQ15001は、個人情報保護法及びガイドライン等への対応を基礎としながら、事業者に、原則として一定の保護水準での対応を求めるものあり、また、マネジメントシステムを構築して対応する仕組みを示したものです。そこで今回のJISQ15001:2006(以下、「JIS規格」という。)の改訂では、「個人情報保護法」との用語の統一と併せて整合性が図られ、個人情報保護法で定められた個人情報取扱事業者の義務を踏まえて、法令順守に向けた仕組みづくりを求めるものとなりました。

こうしたことから第二版では、個人情報保護法を基準とし、

個人情報保護法の定める義務と同等の対応を求める事項

個人情報の定める義務を上回る対応を求める事項(各省庁の策定したガイドライン)

個人情報保護法では定められていない事項(JIS規格の要求事項)

を併記することで、事業内容に合せた個人情報保護体制構築をする際の参考となるよう作成されています。会員各社においては、本ガイドラインを活用いただくことで、個人情報保護に関する取組を積極的に進め、お客様その他一般社会からの一層の信頼確保に努めていただきますようお願いいたします。

平成18年11月14日

NPO法人全国GIS技術研究会
理事長 山下定男

第1章 総 則

1. 目 的

このガイドラインは、GIS 技術の研究、開発に取り組む建設関連事業者(以下、GIS等事業者という。)に対し、個人情報の適正な取り扱いに関する指針を示すことにより、個人情報の有用性に配慮しつつ、個人の権利利益を保護するための活動を支援し、GIS等業界の健全な発展に寄与することを目的とする。

(説明)

1. 「個人情報保護に関する法律」(平成15年法律第57号、以下、「個人情報保護法」という。)は、事業者の個人情報保護水準を一律に規定せず、業種業態に応じた適切な選択をするよう事業者に求めています。また、各省庁で策定されたガイドラインは、事業者における保護対応の自主的選択において、考慮すべきポイントを示したものです。したがって、GIS等事業者においても、少なからず個人情報を事業において取扱っている以上は、法を遵守し自社の社会的責任を果たす為に、最低限の対応をする必要があります。
2. また、このガイドラインは、個人情報保護法及び国が策定したガイドライン等への対応を基礎としながら GIS 等事業者に、原則として、国民の義務としての、一定の保護水準での対応を求めるものであり、事業者自らのマネジメントシステムを構築して対応する仕組みを示したものです。
3. さらにこのガイドラインでは、JIS規格との関連を示すことでGIS等事業者が自ら保有する個人情報を活用し、同時にお客様の個人情報を保護するためのマネジメントシステムを有効に機能させるための指針を示しています。

参考法令 個人情報保護法第1条(目的)

個人情報の保護に関する基本方針 (以下、「基本方針」という。)

- 1 個人情報保護に関する施策の推進に関する基本的な方向
- (2)個人情報保護法の理念と精度の考え方

2. 適用範囲

- (1)このガイドラインは、個人情報を取り扱うすべてのGIS等事業者に適用します。
- (2)このガイドラインは、個人情報の適切な保護の目的の範囲内においてGIS等事業者がその活動実態に応じた見直しをすることができます。

(説明)

1. このガイドラインは、すべてのGIS等事業者を対象として作成しており、取り扱う個人情報の全部もしくは一部がコンピュータ処理されているか否か、及び書面に記録されているか否かを問わず、取り扱う個人情報の量や利用方法により、事業者等を限定せずに、GIS技術の研究、開発に取り組むすべてのGIS等事業者が、このガイドラインに沿って個人情報の適切な取り扱いを行うよう具体的な指針として定めるものです。

2. このガイドラインでは、GIS等事業者の関連企業としてのコンピュータ等販売業者、複写・製本等事業者、電算センター、下請協力会社等は、GIS等事業者から個人情報の取扱いの委託を受ける委託先として位置付けています。
3. このガイドラインの取扱いについて、GIS等事業者は、法令を遵守するためにもこのガイドラインの内容を理解し、実施するとともに次に示す事項を行うことをお願いします。
 - (1) 個人情報の取扱いが適切に行われていることを確認すること。
 - (2) 個人情報保護マネジメントシステムを構築すること。
 - (3) 個人情報保護法およびこのガイドライン、又は、JIS規格と自社の個人情報保護マネジメントシステムが適合していることを確認し、遵守していることを自社のホームページ等で社内外に自ら表明すること。
 - (4) 外部の組織やお客様に自社のマネジメントシステムが法又はJIS Q 15001に適合していることの確認を求めること。
 - (5) 外部機関による自社のマネジメントシステムの認証及び登録を求めること。また、個人情報保護法の適用されないGIS等事業者についても、お客様の個人情報を大切に取扱うという観点から、また、万が一、個人情報の漏えい等が発生すると、信用の失墜や民法・刑法上の責務を負う場合があることから、このガイドラインの内容を理解し、遵守するようお願いいたします。
4. このガイドラインは、個人情報の取扱いに関する法令、国が定める指針及びJIS規格などが改正されたとき、又は、社会情勢の変化などに対応して、個人情報を適切に保護する目的の範囲内において見直しをします。

参考条文 個人情報保護法第2条第3項

個人情報保護法第50条(適用除外)

個人情報の保護に関する法律施行令(平成15年12月10日政令507号。以下「政令」という。)第2条(個人情報取扱事業者から除外される者)

JIS規格 1. 適用範囲

3. 定義

このガイドラインにおける用語の定義は、当該各号に定めるところによります。

(1) 個人情報

個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別できるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)

(説明)

「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限らず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化されているかどうかを問いません。

境界立会、GIS技術の研究のため等により取得したお客様の氏名、住所、電話番号等は個人情報となります。なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報である場合には、当該生存する個人に関する情報となります。また、「生存する個人」に

は、日本国民に限らず、外国人も含まれますが、法人その他の団体は「個人」に該当しないため、法人等の団体そのものに関する情報は含まれません。ただし、役員、従業員等に関する情報は個人情報となります。

(2) 個人情報データベース等

特定の個人情報をコンピュータ等を用いて検索できるように体系的に構成した、個人情報を含む情報の集合物、又はコンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則にしたがって整理・分類し、特定の個人情報を、目次、索引、符号等を付して、自己だけでなく他人によっても容易に検索可能な状態に置いているもの。

(3) GIS等事業者

GISの技術研究、開発に取り組むすべてのGIS等事業を営む個人情報を取り扱う法人その他の団体又は個人であって、個人情報データベース等を事業の用に供している者。

(4) 個人データ

個人情報データベース等を構成する個人情報。

(5) 保有個人データ

GIS等事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてを行うことができる権限を有する「個人データ」をいいます。ただし、その存否が明らかになることにより、公益その他の利益が害されるもの又は6ヶ月以内に消去する(更新することは除く。)こととなるものは除く。

(6) 本人

個人情報によって識別される、又は識別され得る特定の個人。

(7) 本人に通知

本人に直接知らせることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

(8) 公表

広く一般に自己の意思を知らせること(不特定多数の人々が知ることができるように発表すること)をいいます。ただし、公表にあたっては、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

(9) 本人の同意

本人が、個人情報の取扱いに関する権限を与えられた上で、自己に関する個人情報の取扱いについて承諾する意思表示、本人が子ども又は判断力に懸念があると考えられる成人の場合は、法定代理任等の同意も得なければならない。

(10) 利用

GIS等事業者が当該事業者内で個人情報を処理すること。

(11) 提供

GIS等事業者が当該事業者以外のものに自ら保有する個人情報を利用可能にすること。

(12) 個人情報保護管理者

GIS等事業者の内部のものから、代表者によって指名された者であって、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限をもつ者。

(13) 個人情報保護監査責任者

GIS等事業者の内部のものから、代表者によって指名された者であって、公平、かつ、客観的な立場にあり、監査の実施及び報告を行う責任及び権限をもつ者。原則として、個人情報保護管理者との兼務は出来ない。

(14) 個人情報保護マネジメントシステム

GIS等事業者が、自らの事業の用に供する個人情報について、その有用性に配慮しつつ、個人の権利利益を保護するための方針、体制、計画、実施、点検及び見直しを含むマネジメントシステム。

(15) 不適合

個人情報保護法には違反していないが、GIS事業者において策定しているマネジメントシステムの要求事項を満たしていないこと。

(16) 従業者

役員、パート、アルバイトを含む全従業者を示す

参考条文 個人情報保護法第2条(定義)

政令第2条(個人情報取扱事業者から除外される者)

政令第3条(保有個人データから除外されるもの)

政令第4条(保有個人データから除外されるものの消去までの期間)

JIS規格 2 用語及び定義

第2章 計画

4. 個人情報の特定

GIS等事業者は、自らの事業の用に供する全ての個人情報を特定する為の手順を確立し、かつ、維持しなければならない。

(説明)

個人情報を保護する為には、その前提として自社で取扱う個人情報を具体的に特定(把握)しておくことが必要となります。しかし、毎日の業務の中で取得される個人情報のひとつ一つをたえず特定していくことは不可能です。そのため自社の個人情報保護マネジメントシステムを有効に機能させるため、個人情報の特定をするために最低限必要な手順を明らかにしなければなりません。

さらに、従業者等が個人情報の定義を十分理解し、どのような個人情報が、どこで、どのように取得され、流通していくか、個人情報の利用目的、入手経路、社内での取扱経路、保管(一時保管も含む)場所、保管形態(電子媒体、紙等)、保管期間、廃棄方法(納品及び消去)等について明らかにすることが必要です。

参考条文 JIS規格 3.3.1 個人情報の特定

5. リスクなどの認識、分析及び対策

GIS等事業者は、前項で特定した個人情報について、その取り扱いのさまざまな場面におけるリスクを十分認識し、分析するためのことで、目的外利用などを行わずお客様に安心していただけるために、必要な対策を講じる手順を確立し、かつ、維持しなければならない。

(説明)

「リスク」とは、損失の危険性のことをいいます。損失は、本人の権利利益を中心に事業者の社会的、経済的価値への影響(個人情報の漏えい、滅失又はき損、関連する法令、国が定める指針その他の規範に対する違反、想定される経済的な不利益及び社会的な信用失墜、本人への影響などのおそれ)を含むものです。

「リスク認識」とは、特定した個人情報の取得・入力、利用、加工、保管、バックアップ、消去、廃棄に至る個人情報の取扱いの一連の流れの各場面におけるリスクを洗い出すことです。

「リスク分析」とは、洗い出したリスクを評価することであり、GIS等事業者は、洗い出したリスクに対し、その評価に相応した必要な対策を講じる必要があります。

「必要な対策」とは、GIS等事業者の事業内容や規模に応じ、経済的に実行可能な最良の技術の適用と運用手順等の確立を含む合理的な対策をいいます。さらにリスクは、技術の進展等社会環境の変化により常に変動するものですから、少なくとも定期的に、また必要に応じて見直すとともに、新たなリスクを認識する都度、緊急の対策を施す必要があります。

参考条文 個人情報保護法第16条(利用目的による制限)

個人情報保護法第20条(安全管理措置)

個人情報保護法第21条(従業者の監督)

個人情報保護法第22条(委託先の監督)

JIS規格 3.3.3 リスクなどの認識、分析及び対策

6. 個人情報保護方針の策定及び公表

GIS等事業者の代表者は、個人情報保護の理念を明確にした上で、個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなければならない。

またこの方針は文書化し、全ての役員及び従業員に周知させるとともに一般の人が入手可能

な措置を講じなければならない。

(説明)

1. GIS等事業者の代表者は、次に示す事項を含む自社の個人情報保護方針を定めるとともに、これを実行し、かつ、維持しなくてはなりません。またこの方針を文書化し、全ての役員及び従業員(正社員、準社員、契約社員、アルバイト・パート社員等)に周知させるとともに、一般の人が入手可能で閲覧できるように、ホームページに掲載、又は事務所入り口の見やすい位置に掲示するなどして公表することが望ましい。

事業の内容及び規模を考慮した適切な個人情報の取得、利用及び提供に関すること。(特定された利用目的の達成に必要な範囲を超えた個人情報の取扱い(目的外利用)を行わないこと及びそのための措置を講じることを含む。)

個人情報の取扱いに関する法令、国が定める指針その他の規範を遵守すること。

個人情報の漏えい、滅失又はき損の防止及び是正に関すること。

苦情及び相談への対応に関すること。

個人情報保護マネジメントシステムの継続的改善に関すること。

制定日及び改定日

代表者の氏名

問合せ窓口

2. GIS等事業者の代表者は、自社の個人情報保護方針及び法定公表事項の文書化にあたっては、お客様の視点に立った各項目に対し、自社の事業内容に合った表現(事項)を具体的に選び、自らの言葉で顧客に訴えることが重要です。

参考条文 個人情報保護法第1条(目的)

基本方針 6 の(1) (事業者が行う措置の対外的明確化)

JIS規格 3.2 個人情報保護方針

7. 内部規程の策定

GIS等事業者は、個人情報を適正に取り扱うための規程又は手順書を策定し、実施し、維持し、及び継続的な改善をしなければなりません。

(説明)

GIS等事業者において個人情報を適切に取り扱うためには、全社に通用する内部規定が必要となります。これを基に各部門における業務について個人情報保護のための具体的対応を示す手順書なども含む企業規模に応じた規程類を策定し、すべての従業員が同じ行動をとることができるような構成にしておく必要があります。内部規定に基本的に含まれるべき事項としては、次に示す(1)～(15)までの内容が考えられます。

(1) 個人情報を特定する手順に関する規定。

(2) 法令、国が定める指針その他の規範の特定、参照及び維持に関する規定。

担当する部門を明らかにし、参照すべき法令等の洗い出しを行うこと、法令等の制定改廃に関する情報を適時に入手する手順を確立すること、法令等を全従業員に告知する手順を確立し、周知をはかることを規定する。

(3) 個人情報に関するリスクの認識、分析及び対策の手順に関する規程。

- (4) GIS等事業者の各部門及び階層における個人情報保護のための権限及び責任に関する規定。
- (5) 緊急事態(個人情報の漏えい、滅失又はき損をした場合)への準備及び対応に関する規定。
- (6) 個人情報の取得、利用及び提供に関する規定。
- (7) 個人情報の適正管理に関する規定。
- (8) 本人からの開示等の求めへの対応に関する規定
- (9) 個人情報保護のための教育に関する規定。
- (10) 個人情報保護マネジメントシステム文書の管理に関する規定。
- (11) 苦情及び相談への対応に関する規定。
- (12) 点検に関する規定。
- (13) 是正処置及び予防処置に関する規定
- (14) 代表者による見直しに関する規定。
- (15) 内部規定の違反に関する罰則規定。

GIS等事業者は、事業の内容に応じて、自社のマネジメントシステムが確実に適用されるように内部規定を逐次改定しなければなりません。又、このマネジメントシステムを確実に実施するために必要な教育、監査などの計画を立案し、文書化し、かつ、維持しなければなりません。

- 参考条文 基本方針 6の(1)の (責任体制)
基本方針 6の(1)の (従業員の啓発)
基本方針 6の(2)の (ガイドライン(個人情報保護方針)等の策定・見直し)
JIS規格 3.3.5 内部規程
JIS規格 3.3.6 計画書

第3章 運用

第1節 個人情報の取得等

8. 利用目的の特定

- (1) 個人情報を取り扱うにあたっては、本人が最終的にどのような目的で個人情報を利用するかを判断できる程度に、その利用目的(以下「利用目的」といいます。)をできる限り特定しなければなりません。
- (2) 利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて変更してはいけません。

(説明)

- 1. GIS等事業者は、受注業務遂行のために個人情報を取り扱うこととなりますが、その際、まず個人情報の利用目的をできる限り特定しなければなりません。特定した個人情報はあらかじめ公表することが望ましい。また、利用目的の特定にあたっては、利用目的を単に抽象的、一般的に特定するのではなく、GIS等事業者が最終的にどのような目的で個人情

報を利用するかについて、できるだけ具体的に明記する必要があります。

なお、あらかじめ、個人情報をコンピュータ等販売業者、複写・製本等事業者、電算センター、下請協力会社等に提供することを想定している場合は、利用目的において、その旨を特定しなければなりません。

2. 前期により特定した利用目的は、社会通念上、本人が想定することが困難でないと認められる範囲内で変更することは可能です。この場合、変更された利用目的は、本人に通知するか、又は公表しなければなりません

参考条文 個人情報保護法第15条(利用目的の特定)

JIS規格 3.4.2.1 利用目的の特定

9. 利用目的による制限

- (1) GIS等事業者は、あらかじめ本人の同意を得ないで、前項により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはなりません。
- (2) GIS等事業者は、合併その他の事由により他の事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはなりません。
- (3) 前記(1)及び(2)は、次に掲げる場合については適用しません。

法令に基づく場合

人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

国の機関若しくは地方公共団体又はその委託を受けた者が、法令の定める事務を遂行することに対して協力する場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼす恐れがあるとき。

(説明)

1. 一旦取得した個人情報について当初の利用目的の達成に必要な範囲を超えて取り扱うときには、本人にあらかじめ同意を得なければなりません。
同意を得るために個人情報を利用すること(メール送付や電話をかけること等)は当初の利用目的として記載されていなくても、目的外利用にはなりません。
2. GIS等事業者が合併等により他のGIS等事業者から事業を承継することに伴い個人情報を取得した場合であって、当該個人情報に係る承継前の利用目的の達成に必要な範囲内で取り扱う場合は目的外利用とならず、本人の同意を得る必要はありません。
3. 適用除外

法令による場合

「法令」には、法律及び法律に基づく命令(政令、内閣府令、省令等)のほか、条例も含まれます。いわゆる行政規則(訓令・通達)等は含みません。「法令に基づく」とは、法令に具体的根拠があることを意味します。

- 1) 刑事訴訟法第218条(令状による捜査)

2) 地方税法第72条の63(事業税に係る質問検査権等)

3) 所得税法225条第1項等による税務署長による支払い調書等の提出
人の生命、身体又は財産の保護

1) 火山の噴火等により土地情報がわからなくなるような災害時には、本人の同意を得ることが困難であり、GIS等事業者が保有するデータ等を基に境界線の確認及びライフラインの復旧を早急に実施する必要がある場合。

2) 私企業間において、意図的に業務妨害を行う者の情報について情報交換される場合。

公衆衛生の向上等

1) 健康診断やがん検診などの保健事業について、精密検査の結果や受診状況等の情報を健康増進施策の立案や事業の効果の向上を目的としてGIS技術研究や調査の為に、個人情報等を伏せて研究者等に提供する場合。

2) 不登校や不良行為等児童生徒の問題行動について、児童相談所、学校、医療行為等の関係機関及びGIS等事業者が連携したGIS構築のために、当該関係機関等の中で当該児童生徒の情報を交換する場合。

国の機関への協力

国の機関等が法令の定める事務などを実施する上で、GIS等事業者の協力を得る必要がある場合であり、協力するGIS等事業者は目的外利用を行うことについて、本人の同意を得ることが当該事務の遂行に支障を及ぼす恐れがあると認められる場合は、その適用を受けません。

参考条文 個人情報保護法第16条(利用目的による制限)及び 附則第2条

JIS規格 3.4.2.6 利用に関する措置

10. 個人情報の適正な取得

GIS等事業者は、偽りその他不正の手段により個人情報を取得してはなりません。

(説明)

JIS規格では「適正、かつ、公正な手段」とされていますが、ほぼ同義と解釈できます。

【不正の手段により個人情報を取得している事例】

本当は名簿を作成して第三者に売却することが目的であるのに、その目的を隠して緊急時の連絡先を把握するため等の虚偽の目的を告げて家族の個人情報を取得した場合

個人情報保護法では原則としてあらかじめ本人の同意なしに個人データを第三者に提供してはならないこととしていますが、これに違反するよう強要して、個人情報を取得した場合

他の事業者に指示して不正な手段で個人情報を取得させ、その事業者から個人情報を取得する場合

偽りその他不正な手段により個人情報を取得した第三者から、そのことを知っているにも関わらず、間接的に個人情報を取得する場合。

親の同意がなく、十分な判断能力を有していない子供から、取得状況から考えて関係のない親の収入事情などの家族の個人情報を取得する場合。

住民基本台帳法の改正により運用の始まった「住民コード」のように法令により使用を禁止されている個人情報を取得する場合。

参考条文 個人情報保護法第17条(適正な取得)、第23条(第三者提供制限)

JIS規格 3.4.2.2 適正な取得

11. 取得に際しての利用目的の通知又は公表

個人情報を取得する場合は、あらかじめその利用目的を公表している場合を除き、取得後速やかに、その利用目的を本人に通知し、又は公表しなければなりません。

(説明)

GIS等事業者は、個人情報を取得する場合は、あらかじめその利用目的を公表していることが望ましい。公表していない場合は、取得後速やかにその利用目的を本人に通知するか、又は公表しなければなりません。また、近年のIT技術の急速な発展や多様化するお客様ニーズに対応する為に個人情報を利用した事業活動が重要になっていることに伴い、個人情報は直接本人から取得されるだけでなく、本人以外から間接的に取得される場合も急激に増えています。このように本人の知らない間に当該個人情報が流通する際にも、本人の権利利益を侵害しないよう、特に慎重に対応する必要があります。

なお、平成17年4月1日以前に取得した個人情報についても「保有個人データ」として扱われる場合には、利用目的を通知又は公表する必要があります。

参考条文 個人情報保護法第18条第1項

12. 直接書面により個人情報を取得する場合の利用目的の明示

本人との間で契約を締結することに伴い契約書その他の書面に記載された当該本人の個人情報を取得する場合、その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、少なくとも次に示す事項又はそれと同等以上の内容の事項を書面又はこれに変わる方法(口頭、電話等は含まない)によってその利用目的を明示し、本人の同意を得なければなりません。

GIS等事業者の氏名又は名称。

個人情報保護管理者もしくはその代理人の氏名又は職名、所属及び連絡先。

利用目的。

個人情報を第三者に提供することが予定されている場合示す事項。

- ・第三者に提供する目的
- ・提供する個人情報の項目
- ・提供の手段又は方法
- ・当該情報の提供を受ける者又は提供を受ける者の組織の種類、及び属性
- ・個人情報の取扱いに関する契約がある場合はその旨。

個人情報の取扱いの委託をおこなうことが予定される場合にはその旨。

保有個人データに該当する場合には、その求めに応じる旨及び問合せ窓口
本人が個人情報を与えることの任意性及び当該情報を与えなかった場合に生じる結果。

本人が容易に認識できない方法によって個人情報を取得する場合には、その旨。

(説明)

1. 直接本人から書面で個人情報を取得する場合には、あらかじめ本人に利用目的を明示しなければならないこととされており、事業者の義務が強化されています。ひとたび個人情報が事業者の手に移ると、それを回収することは困難であることが多いので、本人に自分の個人情報の提供の是非を慎重に判断させる為にも利用目的の明示が義務化されています。
2. 例えば、業務委託契約に伴い取得した個人情報により立会通知を出した場合、本人は契約の際にそこまでの認識をしていないことがあるので、契約書に利用目的を記載するなど、本人にあらかじめ利用目的を認識してもらうことが必要です。ホームページへの掲載だけや裏面に微細な文字で記載する等、利用目的が記載された箇所が容易に認識し得ない書面を交付することは、「明示」したことになりません。
3. 平成17年4月1日以前に取得した個人情報については、ホームページに利用目的を掲載することや、会社案内等に個人情報の利用目的を印刷する等、利用目的を通知又は公表する必要があります。

参考条文 個人情報保護法第18条第2項

JIS規格 3.4.2.4 本人から直接書面によって取得する場合の措置

13. 利用目的の変更

(1) GIS等事業者は、取得した個人情報の利用目的を取得後に変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければなりません。

(2) ただし、次に掲げる場合には、適用されません。

本人又は第三者の生命、身体、財産その他の権利利益を害する恐れがある場合。

当該GIS等事業者の権利又は正当な利益を害する恐れがある場合。

国の機関等への協力をする場合で、当該事務の遂行に支障を及ぼす恐れがある場合。

利用目的が自明であると認められる場合。

(説明)

1. GIS等事業者は、社会通念上、本人が想定することが困難でない認められる範囲内で利用目的を変更した場合は、変更された利用目的について、本人に通知するか、又はインターネットに利用目的を変更した旨を掲載することや、納品書や請求書などに個人情報の利用目的を変更した旨を印刷する等、利用目的の変更の通知又は公表をする必要があります。

2. 適用除外

利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害する恐れがある場合。

通知又は公表される利用目的の内容により、当該GIS等事業者が行う製品等の

開発内容、営業ノウハウ等の企業秘密に関するようなものが明らかになる場合。
国の機関等が法令の定める事務を実施する上で、GIS等事業者の協力を得る必要がある場合で、受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼす恐れがある場合。
取得される状況から見て利用目的が自明であると認められる場合。

参考条文 個人情報保護法第18条第3項、4項
JIS規格 3.4.2.4～3.4.2.5

14. 子供から個人情報を取得する場合の措置

GIS等事業者は、子供から個人情報を取得する場合には、子供が理解できる平易な表現で利用目的を明示するものとし、子供に個人情報の入力を求める場合には、保護者の了解を得るように促すものとします。

(説明)

1. パソコンの操作性の向上に伴い、子供でも簡単にインターネット等の情報ネットワーク上で商品・サービスの売買やアンケートへの回答を行うことが可能となりました。こうした状況を利用し、GIS等事業者においても子供や保護者の個人情報を取得するような参加型のWebGISの構築などに取り組みがなされています。こうした環境では子供は必ずしも個人情報の取得や利用についての認識が十分ではないことから、なぜその情報が必要なのかを分かりやすく誤解を生じない表現で説明する等の慎重な取り扱いが必要となります。
2. Web型のGIS構築の場合は、子供やその保護者が、自分の知らないところで不利益を被る懸念があることから、「子供に個人情報の入力を求める場合」は、取得する前に事情を説明し了解を得る機会を設定するなど、より慎重に配慮する必要があります。
3. ここで「子ども」とは、必ずしも未成年者を言うのではなく、取り扱う商品やサービスにより、対象となる年齢が定まることを想定した用語です。「JIS」では一般に12歳から15歳までの年齢以下を対象としています。

参考条文 JIS規格 2.6 本人の同意

15. 特定の機微な個人情報の収集の禁止

GIS等事業者は、次に示す内容を含む個人情報の取得、利用または提供、を行ってはなりません。ただし、これらの取得、利用または提供について、書面による本人の同意がある場合及び9(3)の から のいずれかに該当する場合は、この限りではありません。

- (1) 思想、信条、及び宗教に関する事項
- (2) 人種、民族、門地、本籍地、(所在都道府県移管する情報を除く)、身体、精神障害、犯罪歴、その他社会的差別の原因となる事項。
- (3) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項
- (4) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項

(5) 保健医療及び性生活に関すること

(説明)

法の場合は、個人情報の内容、重要視などに立ち入ることなく規制するという思想の下にあります。しかし、「OECD理事会勧告」や「EU個人データ保護指令」などがセンシティブ・データとしての同種の事項を定めていたことから、JISでは国際的な保護水準に配慮する必要があったことから、また、個人の権利利益(特に、プライバシーといった人格的利益)を侵害しかねない特定の個人情報の取扱いを慎重におこなわせる必要があることから採用されたと思われます。

特定の機微な個人情報は、情報流出等によって個人情報保護法の義務に反するだけでなく、合せて民事責任を問われることも多く、こうした個人情報について得に厳格な取扱手続を求めることは、一種のリスク管理としての機能をも果たすものとなります。

「法令に基づく場合」とは、例えば、従業員の採用後に健康診断書(個人情報)を取得する場合があります。この場合は、労働安全衛生法に基づくものとして本人の同意が不要となります。ただし、採用選考の資料として健康診断書の提出を求める場合は、法令に基づくものではなく、書面による同意が必要となります。

参考条文 JIS 規格 3.4.2.3

第2節 個人データの管理

16. データ内容の正確性の確保

GIS等事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

(説明)

GIS等事業者は、利用目的の達成に必要な範囲内において、誤った情報、古い情報によって、個人の利益が侵害される恐れがあることから個人情報データベース等への個人情報の入力時の照合、確認の手続きの整備、誤り等を発見した場合の訂正等の手続きの整備、記録事項の更新・保存期間の設定、バックアップ体制の整備等を行うことにより、個人データを正確かつ最新の内容に保つようにならなければなりません。

この場合、保有する個人データを一律に又は常に最新に保つ必要はなく、それぞれの利用目的の達成に必要な範囲内で過去又は現在の事実と合致することをいいます。

参考条文 個人情報保護法第19条

JIS 規格 3.4.3.1 正確性の確保

17. 安全管理措置

GIS等事業者は、その取り扱う個人データの漏えい、滅失又は、き損の防止その他の個人データの安全管理のために、その会社規模に応じた必要かつ適切な措置を講じなければならない。

(説明)

GIS等事業者が個人情報を取扱うにあたって、特定された個人情報のリスクなどの認識、分析及び対策を講じた個人情報について、そのリスクに応じた安全管理措置を講じることを求めたものです。

個人データが漏えいする原因としては、入手した書面等のコピー、写真、個人情報が入ったノートパソコン等の紛失・盗難、また、口頭による漏えい(「ここだけの話」として個人情報を伝達した場合も含む)、インターネット等による漏えい等が考えられます。

個人データを安全に管理するため、組織的、人的、物理的及び技術的安全管理措置を講じることが必要です。組織的、人的な面では、内部規程・マニュアルの作成、従業員教育等が考えられます。また、物理的、技術的な面では、セキュリティに配慮した機器の設置、個人情報を扱うシステムの外部ネットワークからの独立、インターネット等で接続する場合にはファイアウォールの設置、暗号化、アクセス制限の設定、その他様々な方策が考えられます。

なお、個人データの安全管理のための措置については、経済産業省ガイドラインに詳細な方策・事例が記載されていますので必要に応じてご参照ください。

参考条文 個人情報保護法第20条

JIS規格 3.4.3.2 安全管理措置

18. 従業員の監督

(1) GIS等事業者は、その従業員に個人データを取り扱わせるにあたっては、当該個人データの安全管理が図られるよう、当該従業員に対する必要かつ適切な監督を行わなければならない。

(2) 前項の監督にあたっては少なくとも次に掲げる事項を行わなければならない。

個人情報保護に関する規程類を策定し従業員に周知すること。

すべての従業員に対して定期的に個人情報の保護に関する教育を実施すること。

個人データが適切に取り扱われているかを必要に応じて確認すること。

(説明)

個人情報保護法第21条では、事業者は、その従業員に個人情報の安全な管理が図られるよう必要かつ適切な監督を義務規程として定めています。たとえば、安全管理規程の教育とその遂行、定期的な確認をさせるなどの適切な監督を行うことが必要です。

参考条文 個人情報保護法第21条

JIS規格 3.4.3.3 従業員の監督

19. 委託先の監督

(1) GIS等事業者は、個人情報取扱の全部または一部を委託する場合は、十分な個人情報の保護水準を満たしている者を、選定しなければならない。このため、GIS等事業者は、委託を受ける者を選定する基準を確立しなければなりません。

(2) GIS等事業者は、個人データの取り扱いの全部又は一部を委託する場合は、個人デ

ータの安全管理が図られるよう、委託を受けた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。

(3) 前項の監督にあたっては、このガイドラインに従い、少なくとも次の事項を契約によって規定し、十分な個人情報の保護水準を担保しなければなりません。

委託者及び委託先の責任の明確化。

個人情報の安全管理に関する事項。

再委託に関する事項。

個人情報の取扱状況に関する委託者への報告の内容及び頻度。

契約内容が遵守されていることを委託者が確認できる事項

契約内容が遵守されなかった場合の措置

事件・事故が発生した場合の報告・連絡に関する事項

(説明)

1. GIS等事業者が個人データの取り扱いを委託する相手としてはコンピュータ等販売業者、複写・製本等事業者、電算センター、下請協力会社等が考えられますが、どこに委託した場合でもGIS等事業者に監督する責任があります。

2. 「必要かつ適切な監督」とは次の場合が考えられ、再委託先に問題が生じた場合は、委託元が責任を負うことがあるので、再委託する場合は特に注意が必要です。

委託契約書に安全管理に関する規定があること。

定期的に安全管理について確認すること。

再委託する場合はその規定を設けること。

3. 外部へ委託する際、委託先から情報が漏えいすれば、委託元も監督責任や使用者責任などの責任を負うこととなるため、委託先の選定には、次のような基準などを設けて適正水準を維持することが必要です。

売り上げ、事業内容、利益等の安定性

受託実績の有無

技術レベル

委託先のシステム環境

プライバシーマーク等の認証取得状況

事故発生時の賠償能力としての保険の加入の有無など

参考条文 個人情報保護法第22条

JIS規格 3.4.3.4 委託先の監督

第3節 提供に関する措置

20. 個人データの第三者提供の制限

(1) GIS等事業者は、次に掲げる場合等を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

法令に基づく場合。

人の生命、身体又は財産の保護のために必要がある場合であって、本人の同

意を得ることが困難であるとき。

公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

国の機関もしくは地方公共団体又はその委託を受けたものが法令の定める事項を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事業の遂行に支障を及ぼすおそれがあるとき。

- (2) GIS 等事業者は、第三者に提供される個人データについて、本人の求めに応じてその提供を停止することとしている場合であって、次の各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、当該個人データを第三者に提供することができます。なお、又は に掲げる事項を変更する場合は、その変更内容について、あらかじめ、本人に通知し、又は本人が容易に知りうる状態に置かなければならない。

第三者への提供を利用目的とすること

第三者に提供される個人データの項目

第三者への提供の手段又は方法

本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

取得方法

- (3) GIS 等事業者は、前項 又は に掲げる事項を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

- (4) 次のいずれかに該当する場合は、第三者提供に該当しないものとします。

事業者が利用目的の達成に必要な範囲内において個人データの取り扱いの全部又は一部を委託する場合。

合併その他の事由による事業の承継に伴って個人データが提供される場合。

個人データを特定の者との間で共同して利用する場合で以下のことを、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置いている場合。

共同利用する旨

共同して利用される個人データの項目

共同して利用される者の範囲

利用する者の利用目的

当該個人データの管理について責任を有する者の氏名又は名称

取得方法

- (5) 事業者は、前記 に規定する項目のうち、又は を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければなりません。

(説明)

1. GIS等事業者が受託業務を遂行するために、コンピュータ等販売業者、製本等事業者、電算センター、下請協力会社等に個人情報を提供する場合は、ここでいう第三者提供に該当しないため、事前に同意を得る必要はありませんが、「委託先」に該当するため、必要かつ適切な監督を行なう必要があります。

2. GIS等事業者が業務委託を遂行するという目的以外で個人情報を第三者提供する場合はあらかじめ本人の同意を得る必要があります
3. (2)はオプトアウトにあたる。
4. (4) ~ の共同利用者は第三者には当たらない。
5. 次に掲げる場合も適用除外される
法人その他の団体に関する情報に含まれる役員及び株主に関する情報で法令に基づき公開又は公表された情報を提供する場合

参考条文 個人情報保護法第23条(第三者提供の制限)

JIS規格 3.4.2.8 提供に関する措置

第4節 開示・訂正・利用停止等の対応

21. 保有個人データに関する必要事項の公表等

- (1)事業者は、保有個人データに関し、次の事項について、本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含みます。)に置かなければなりません。
GIS等事業者の氏名又は名称
個人情報保護管理者(若しくはその代理人)の氏名又は職名、所属及び連絡先
すべての保有個人データの利用目的
保有個人データの開示、訂正等、利用停止等の手続及びその手数料
GIS等事業者が行う保有個人データの取り扱いに関する苦情の申出先
第26(1)によって定めた手続
- (2)GIS等事業者は、本人から、当該本人が識別される保有個人データの利用目的の通知を求められたときは、本人に対し、遅滞なくこれを通知しなければならない。ただし、前項の規程により当該本人が識別される保有個人データの利用目的が明らかな場合、及び、第13(利用目的の変更)(2)の から までのいずれかに該当する場合はこの限りではない。
- (3)GIS等事業者は、前項の規定に基づき求められた保有個人データの利用目的を通知しない旨の決定をしたときは、本人に対し遅滞なく、その旨を通知しなければならない。

(説明)

例えば料金をすでに支払っているにもかかわらず、支払われていないことになっている場合など、誤った個人情報を保有し、その情報に基づいて業務処理を行うなどにより本人の利益が侵害されることも想定されます。これについて、事業者は本人に自己の利益を保護する手段として開示・訂正・削除・利用停止を容易に行える体制を確保しなくてはなりません。また、平成17年4月1日以前に取得した個人データに関しても本人の知り得る状態に置かなければなりません。

「本人が知り得る状態」とは、ウェブ画面への掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうと思えば知ることができる状態に置くことをいいます。なお、公表にあたっては、必ずしもウェブ画面への掲載、又は事務所等の窓口等へ掲示すること等が継続的に行われることまでを必要とするものではありませんが、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらな

ければならない。

参考条文 個人情報保護法第24条(保有個人データに関する事項の公表等)
政令第5条(保有個人データの適正な取扱いの確保に関し必要な事項)
基本方針 6 (1) 事業者が行う措置の対外的明確化
JIS規格 3.4.4.3 開示対象個人情報に関する事項の通知など
JIS規格 3.4.4.4 開示対象個人情報の利用目的の通知

22. 本人からの求めによる保有個人データの開示

- (1) 事業者は、本人から当該本人が識別される保有個人データの開示(当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。)を求められた場合は、本人確認のうえ遅滞なくこれに応じなければならない。ただし、次に掲げる場合はその全部又は一部を開示しないことができる。
本人又は第三者の生命、身体、財産その他の権利利益を害する恐れがある場合。
自社の業務の適正な実施に著しい支障を及ぼす恐れがある場合。
他の法令に違反することとなる場合。
- (2) 前項の規定に基づき求められた保有個人データの全部又は一部について開示しない旨を決定した時は、本人に対し、遅滞なく、その旨を通知する。
- (3) 開示する場合は書面により行う。ただし、開示の求めを行った者が同意した方法があるときは、その方法で行うことができる。

(説明)

1. 本人から個人情報のデータの開示を求められたときは、書面により開示することを原則とします。ただし、本人が別の開示方法に同意あるいは指定した場合は、その方法でもよい。たとえば、電子メール、電話等がある。
2. (1) の事例としては、同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり、事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなり、業務上著しい支障を及ぼすおそれがある場合

参考条文 個人情報保護法第25条(開示)
政令第6条(個人情報取扱事業者が保有個人データを開示する方法)
JIS規格 3.4.4.5 開示対象個人情報の開示

23. 本人からの求めによる保有個人データの訂正等

- (1) GIS 等事業者は、本人から保有個人データの内容が事実でないという理由で訂正、追加又は削除(以下「訂正等」といいます。)を求められたときは、利用目的の達成に必要な範囲内において遅滞なく調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。
- (2) 前項の規定に基づき保有個人データの内容について訂正等を行ったとき、又は訂正等を行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(説明)

GIS等事業者は本人が自己の利益を保護する手段として、開示・訂正・削除・利用停止を容易に行える体制を確保しなければなりません。

GIS等事業者は、本人から当該保有個人データの内容が、事実でないことからその訂正、削除を求められたときは、原則として、訂正等を行わなければなりません。また、本人にその訂正等の有無を通知しなければなりません。ただし、利用目的から見て訂正が必要でない場合や、内容が誤りでなく、指摘が正しくない場合には、訂正等を行う必要はありません。

参考条文 個人情報保護法第26条(訂正等)

JIS規格 3.4.4.6 開示対象個人情報の訂正、追加又は削除

24. 本人からの求めによる保有個人データの利用停止等

- (1) GIS等事業者は、本人から当該本人が識別される保有個人データが、その利用目的の制限に違反して取り扱われているという理由、若しくは適正な取得に違反して取得されたものであるという理由、又は第三者への提供の制限に違反して第三者に提供されているという理由によって、当該保有個人データの本人から利用停止若しくは、消去又は第三者への提供の停止(以下「利用停止等」といいます。)を求められたときにおいて、その求めに理由があることが判明したときには、違反を是正するために必要な限度で、遅滞なく利用停止等を行わなければならない。ただし、多額の費用を要する等、その実施について困難である場合であって、本人の権利利益を保護するため必要な措置をとるときは、この限りではない。
- (2) GIS等事業者は、前記に基づき保有個人データについて利用停止等を行ったとき、又は、行わない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。

(説明)

1. 本人から同意のない目的外利用、不正な取得、同意のない第三者提供などの手続き違反で個人情報の利用の停止等を求められた場合は、原則として、個人情報のデータの利用の停止、消去、第三者への提供の停止を行わなければなりません。その措置を行った場合は、本人に通知しなければなりません。ただし、利用停止等に多額の費用がかかり、その他の利用停止、第三者への提供の停止を行うことが困難な場合であって、本人の権利、利益を保護するため必要な措置を行う場合は、この限りにありません。
2. 「これに代わるべき措置」の内容はケースバイケースで、例えば、正誤表の添付、注記等が考えられますが、いずれにしても利用停止や第三者への提供の停止を行わないことで本人の権利利益が侵害されるおそれがどの程度あるかなどを勘案する必要があります。

参考条文 個人情報保護法第27条(利用停止等)

JIS規格 3.4.4.7 開示対象個人情報の利用又は提供の拒否権

25. 公表・開示等を行わない場合の本人への理由の説明

GIS 等事業者は、保有個人データの公表、開示、訂正及び利用停止等の規定により、本人から求められた措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合には、本人に対し、その理由を説明するよう努めなければならない。

(説明)

1. GIS等事業者は、個人情報の公表、開示、訂正、利用停止等において、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を本人に通知する場合は、その理由も併せて、本人に対して、説明するように努める必要があります。
2. 理由の説明の手段として電子メールなどを用いて行うこともできます。ただし、電子メールだけではお客様に対し、十分な説明ができないときやお客様が納得しないケースも十分考えられます。その場合は、担当者による電話や面談等による説明を行うことが必要です。

参考条文 個人情報保護法第28条(理由の説明)

JIS 規格 3.4.4.4 開示対象個人情報の利用目的の通知

JIS 規格 3.4.4.5 開示対象個人情報の開示

JIS 規格 3.4.4.6 開示対象個人情報の訂正、追加又は削除

JIS 規格 3.4.4.7 開示対象個人情報の利用又は提供の拒否権

26. 本人からの開示等の求めに応じる手続

- (1) GIS 等事業者は、保有する個人データについて本人からの開示、訂正、削除、利用停止等(以下、開示等という)の求めに関し、その求めを受け付ける方法として以下について定め、当該方法に従って、本人からの開示等の求めを受け付ける。

開示等の求めの申出先

開示等の求めに際して提出すべき書面(電子的方式その他、人の知覚によっては認識することができない方式で作られる記録を含みます。)の様式その他の開示等の求めの方式

開示の求めをする者が本人又は後記(4)の代理人であることの確認方法

手数料の徴収方法

- (2) GIS 等事業者は、本人に対し、開示の求めに関し、その対象となる保有個人データを特定するに足りる事項の提示を求めることができる。この場合において、GIS等事業者は、本人が容易かつ的確に開示等の求めをすることができるよう、当該保有個人データの特定に資する情報の提供その他本人の利便を考慮した適切な措置をとらなければならない。
- (3) 本人の求めによる利用目的の通知及び開示の実施に関し、手数料を徴収することができる。なお、手数料の額は実費を勘案して合理的であると認められる範囲でなければならない。手数料を定める場合は本人の知り得る状態に置かなければならない。
- (4) GIS 等事業者は、次に掲げる代理人による開示の求めに応じなければならない。なお、ここでいう代理人は次の者に限る。

未成年者又は成年被後見人の法定代理人

開示等の求めをするにつき本人が委任した代理人

(説明)

1. GIS等事業者は、本人からの開示等の求めを受け付ける手続を定めることができます。その際本人に過重な負担を強いることのないよう配慮しなければなりません。
2. 本人に対し本人の個人データの開示を行う場合、その利用目的を本人に尋ねる等により、本人への開示範囲を確認することができます。
3. 開示等を求める者が本人かどうか確認する必要があります。インターネット等による求めについても同じです。
4. 代理人による求めを受け付ける場合は、本人の委任を受けた代理人であることを確認する必要があります。

参考条文 個人情報保護法第29条(開示等の求めに応じる手続)

個人情報保護法第30条(手数料)

政令第7条(開示等の求めを受け付ける方法)

政令第8条(開示等の求めをすることができる代理人)

JIS規格 3.4.4.2 開示等の求めに応じる手続

第5節 苦情処理

27. 苦情及び相談への対応

- (1) GIS等事業者は、個人情報の取り扱いに関する苦情及び相談を受け付けて、適切、かつ、迅速な対応を行う手続を確立し、かつ、維持しなければならない。
- (2) GIS等事業者は前項の目的を達成するために必要な体制の整備を行わなければならない。

(説明)

1. GIS等事業者は、お客様に対して、個人情報の保護、運用、対応について、日ごろからその対応、説明ができるようにしておくことが必要です。
2. 予想される問い合わせ、苦情としては、次のことが予想されます。
立会通知がきたが、どこから入手したのか、
自分の情報をどれだけ持っているのか、
自分の情報を何処に提供したのか。
3. GIS等事業者は、個人情報の取り扱いに関する問い合わせ、相談、苦情を処理するため、苦情処理の窓口の設置や苦情処理の手順を定めるなどの必要な体制の整備に努めることが必要です。
4. 苦情への対応窓口のメールアドレス、電話番号等の連絡先は個人情報保護方針と併せ、お客様の目に付きやすいところに常時表示しておくことが望ましい。
5. 苦情及び相談を受け付けてから対応するまでの期間については特に定めはないが、本人からの苦情及び相談内容や、その影響等にかんがみて合理的期間内に応じることが必要となります。
6. 苦情及び相談の受付は、常設の対応窓口の設置又は担当者の任命によって行う必要があります。ただし、個人情報保護管理者との兼任を妨げません。

参考条文 個人情報保護法第31条(個人情報取扱事業者による苦情の処理)
基本方針 7(1) 事業者自身による取組のあり方
JIS規格 3.6 苦情及び相談への対応

第4章 個人情報保護体制

28. 個人情報保護マネジメントシステムの確立

- (1) GIS 等事業者の代表者は、事業運営において適切な個人情報の保護を図るために、個人情報保護マネジメントシステムを確立し、実施し、維持し、かつ、改善する為に不可欠な資源を用意しなければならない。
- (2) GIS 等事業者の代表者は、個人情報保護マネジメントシステムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、従業員に周知しなければならない。
- (3) GIS 等事業者の代表者は、個人情報保護マネジメントシステム内容を理解し実践する能力のある個人情報保護管理者を内部のものから指名し、個人情報保護マネジメントシステムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。また、事業者の代表者に対し、運用状況の報告をしなければならない。

(説明)

個人情報保護マネジメントシステムを効果的に運用する為には、少なくとも個人情報保護管理者、個人情報保護監査責任者を他の責任にかかわりなく行える責任および権限を与えたものを指名し、自社に必要な組織作りをしなければなりません。さらに、内部規定を定め、文書化して従業員に周知することが必要です。

次に、予算措置、要員の配置、資産、備品の用意などマネジメントを行ううえで不可欠な経営資源を整えることが必要です。

個人情報保護法では、第21条において従業員に対する監督ということばで表現されていますが、どんなに高いハード環境を整備してもそれを運用する人間の心の部分で歯止めをかけなければ防止効果、抑止効果が上がりません。そこで、多くの企業で現在教育に力を入れています。

教育に盛り込むべき事項は次のようなことが必要です。

1. 法律や自社のマネジメントシステムに適合していることの重要性及び利点。
2. 自社のマネジメントシステムに適合する為の役割及び責任。
3. 法律や、自社のマネジメントシステムに違反した場合に予想される結果。

また、教育を実施するにあたっては、定期的に適切な教育を行わなければなりません。そのためには、教育の実施内容を計画し、適切に実施できたことを確認するための記録(アンケートや小テストの実施)をとり、理解度の把握をし、必要に応じて教育内容の見直しを図ることや、教育を受けたことを自覚させる仕組みを取り入れることが望ましい。また、欠席者にも漏れなく教育を実施することと、十分な理解ができていないものには理解できるまで再教育を実施することも必要です。

参考条文 基本方針 6(1) 責任体制の確保

基本方針 6(1) 従業員の啓発

JIS規格 3.3.4 資源、役割、責任及び権限

JIS規格 3.4.5 教育

29. 点検(監査、是正処置及び予防処置)

個人情報保護監査責任者は、個人情報保護法及び自社の個人情報保護マネジメントシステムに適合した運用が実施されているかを定期的に監査し、事業者の代表者に報告しなければならない。また、監査の結果個人情報保護法に違反する場合や、違反はしていないが自社のマネジメントシステムに適合しない事項が見つかった場合には、適合する為の是正処置や違反しない為の予防処置などを立案し、実施し、記録しなければならない。さらに、実施された是正処置及び予防処置の有効性をレビューする。

(説明)

個人情報保護法に違反した場合には、主務大臣による「報告の徴収」、「助言」、「勧告」、「命令(緊急命令を含む)」の対象となります。また、違反行為が是正されない場合に発せられる命令違反に対しては罰則が適用されます。

こうした「違反」に至らないまでもお客様からお預かりしている個人情報が漏えい等の脅威にさらされる危険性が高まる取り扱いをしてはお客様から信頼を受けることはなく社会的な制裁を受ける事態を招くことが予想できます。そうした事態に至らないよう個人情報保護監査責任者は定期的に自社の運用状況を監査し、代表者に報告をすることが求められています。さらには、そうした事態に対する是正処置や予防処置を計画立案し、実施することで、お客様から信頼される個人情報保護体制が確立できます。

参考条文 個人情報保護法第32条 (報告の徴収)
個人情報保護法第33条 (助言)
個人情報保護法第34条 (勧告及び命令)
個人情報保護法第35条 (主務大臣の権限の行使の制限)
個人情報保護法 第6章 罰則
JIS規格 3.7 点検
JIS規格 3.8 是正処置及び予防処置

30. 代表者による見直し

事業者の代表者は、監査報告書及びその他の経営環境などに照らして、適切な個人情報の保護を維持する為に、少なくとも年1回以上自社の個人情報保護推進体制を見直し。また、事故・苦情・外部からの指摘などに対しても、必要に応じて見直しを行う。

(説明)

事業者の代表者は、個人情報保護監査責任者の監査報告書に記載された指摘事項を必ず確認し、個人情報保護体制の改善点などについて見直し案を作成し、優先順位をつけてそれぞれの責任者に書面により実行を指示するものとします。

参考条文 JIS規格 3.9 事業者の代表者による見直し

31. 漏洩等が発生した場合の措置

事業者は、自社が取り扱う個人情報について漏えい等(紛失、破壊、改ざんを含む。)の事実を把握した場合は、次のとおり対応することが必要です。

- (1)当該漏えい等に関する個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置くものとします。
- (2)二次被害の防止、類似事案の発生回避の観点から、可能な限り事実関係、発生原因を遅滞なく公表するものとします。
- (3)発生原因、対応策を所管する省庁及び関係機関に直ちに報告するものとします。

(説明)

GIS等事業者において個人情報漏えいが発生した場合は、はじめに測量等事業を登録している行政庁の所管課及び都道府県測量業協会及びNPO法人全国GIS技術研究会とそれぞれの地方研究会へ連絡を行うことが必要です。

また、個人情報の漏えい事故発生時の対応如何により、その後の損害賠償請求の抑制効果や企業の信用低下・イメージダウンの抑止効果などに影響が出ます。このため、日頃からその対応についても次のような対策を検討しておくことが必要です。

定まった手順による迅速な社内での報告を行う。

漏えいの実態、起こりうる最悪のケース、悪用される可能性などについて、本人への確かな状況報告を行う。

漏えいした個人情報、その量、漏えいの原因、二次被害の可能性等についての確認を行う。

本人などからの苦情の対応を適切に行う。

漏えい原因などの結果を分析して、これまでの「安全管理措置」に対する適切な見直しを行う。

参考文献等

本ガイドラインの作成に当たっては、次の文献等を参考にさせていただきました。

基本方針・法律・法律政令

『国土交通省所管分野における個人情報保護に関するガイドライン』 国土交通省

『個人情報の適正な取り扱いを確保するために農林水産分野における事業者が講ずべき措置に関するガイドライン』 農林水産省

『個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン』 経済産業省

『民間部門における電子商取引に係る個人情報の保護に関するガイドライン(Ver.2.0)』 電子商取引推進協議会

『Q & A 個人情報保護法(第2版)』 個人情報保護基本法制研究会 編 (株)有斐閣

『個人情報保護法の逐条解説』 宇賀克也 著 (株)有斐閣

JIS Q 15001:2006 『個人情報保護マネジメントシステム要求事項の解説』

堀部政男 監修 鈴木正朝:新保史生:斎藤雄一:太田克良 著 日本規格協会