事業者における個人情報の取扱いに関する指針［解説］

§１　趣　　旨

この指針は、個人情報の取扱いに伴う個人の権利利益の保護を図るため、事業者が個人情報の保護のために適切な措置を講ずる際のよりどころとなるように作成したものである。

この指針は、滋賀県個人情報保護条例(平成７年滋賀県条例第８号。以下「条例」という。)第47条第２項の規定に基づき、事業者の皆さんが個人情報の保護のための適切な措置を講ずる際のよりどころとしていただくために作成したものです。

<<説　明>>

１　条例第46条では、「事業者は、個人情報の保護の重要性を認識し、事業の実施に伴い個人情報を取り扱うときは、個人の権利利益を侵害することのないよう、適正な取得、利用、管理等に努めなければならない。」と規定しています。

また、条例第47条第２項では、「知事は、滋賀県個人情報保護審議会の意見を聴いて、事業者が個人情報を取り扱う際のよりどころとなる指針を作成し、公表するものとする。」と規定しています。

この指針は、これらの規定に基づいて、事業者の皆さんに個人情報の基本的な取扱いについて示したものです。この指針の作成に当たっては、個人情報保護の国際的ガイドラインであるＯＥＣＤ（経済協力開発機構）理事会勧告を基本に、個人情報の保護に関する法律（平成15年法律第57号。以下「個人情報保護法」という。）等の内容を参考にしています。

ＯＥＣＤ(経済協力開発機構)理事会勧告(1980年９月)

①収集制限の原則　②データ内容の原則　③目的明確化の原則　④利用制限の原則
⑤安全保護の原則　⑥公開の原則　⑦個人参加の原則　⑧責任の原則

２　この指針の対象となる「事業者」は、法人その他の団体のほか、事業を営む個人も含まれますが、国、独立行政法人、地方公共団体および地方独立行政法人は、行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）や地方公共団体が制定する個人情報保護条例等で個人情報の取扱いに関する規定が定められていることから事業者の対象から除かれます（条例第２条第４号）。

なお、個人情報保護法に規定する個人情報取扱業者に該当する事業者は、同法の規定により個人情報を取り扱うことになります。

さらに、事業者の事業分野において、国の各省庁が個人情報保護に関するガイドラインを策定している場合は、当該ガイドラインの規定の遵守に努めることが求められます。

また、個人情報保護法やガイドラインで個人情報の取扱いの適用除外とされているものについては、当然この指針の規定の適用除外として取り扱うことができます。

※　個人情報取扱事業者は、５千件を超える個人情報をコンピュータなどを用いて検索することができるように体系的に構成した「個人情報データベース等」を事業活動に利用している事業者が対象になります。

なお、「個人情報データベース等」には、コンピュータ処理情報のほか、紙の情報（マニュアル処理情報）であっても、個人情報を五十音順、生年月日順、勤務部署順などの一定の方式によって整理し、目次、索引等を付して容易に検索できる状態に置いているものも含まれます。

§２　対象とする個人情報

(1) この指針において「個人情報」とは、生存する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することができるもの（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。）をいう。
(2) この指針は、情報の処理形態のいかんにかかわらず、事業者がその事業活動に伴って取り扱う個人情報のすべてを対象とする。

この項は、この指針が適用される個人情報の範囲を定めたものです。

〈〈説　明〉〉

１　「個人情報」とは、氏名、住所、生年月日はもとより、思想、宗教、身体的特徴、健康状態、病歴、家族構成、職歴、資格、学歴、成績、所属団体、財産、所得その他個人に関するすべての情報をいいます。

また、法人その他の団体に関する情報は個人情報に該当しませんが、役員や従業者に関する情報については、個人情報に該当します。

２　この指針において個人情報は、生存する個人に関する情報に限定されており、死者に関する情報は含まれません。

しかし、ある情報が死者に対する情報であると同時に、遺族等の生存する個人に関する情報（たとえば、相続財産の情報等）でもあるような場合は、死者の情報であったとしても、その情報は遺族等の生存する個人の情報となります。

また、死者に関する情報であっても、利用目的を超えた取扱いや漏えい等の不適切な取扱いを避けることは当然であり、適切に取り扱うことが必要です。

３　「特定の個人を識別することができるもの」とは、その情報に含まれる氏名、生年月日その他の記述または個人別に付された番号、記号その他の符号によって特定の個人を識別できるものはもとより、他の情報と容易に照合することができ、それによって当該個人を識別できるものも含まれます。

４　「情報の処理形態のいかんにかかわらず」とは、電子計算機処理、手作業(マニュアル)処理のいずれの形態による処理であっても対象となることをいいます。

５　「事業活動に伴って取り扱う」とは、事業の営利・非営利を問わず、事業活動に伴って行う個人情報の取得、利用、提供、管理等をいいます。たとえば、事業活動に伴い、次のような個人情報を取り扱う場合がこれに当たります。

・顧客情報　・信用情報　・会員・組合員等情報
・教育、研修等受講者情報　・医療、福祉等サービス受給者情報
・ボランティア活動者情報　・従業者やその家族の情報

また、個人情報の取扱いについては、すべての国民・事業者を対象とした基本理念として、個人情報保護法第３条に「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。」と定められていることから、事業者においてもこのことに特に留意する必要があります。

§３　個人情報の取得

(1) 個人情報の取得は、事業者の正当な事業の範囲内において、利用目的を明確にし、その目的を達成するために必要な範囲内で行うものとする。
(2) 個人情報の取得は、適法かつ公正な手段により行うものとする。
(3) 個人情報を取得するときは、原則として本人が利用目的を確認できるようにするものとする。
(4) 個人情報の本人以外のものからの取得は、本人の権利利益を不当に侵害するおそれがない場合に限るものとする。

この項は、事業者が個人情報を取り扱う最初の段階である「取得」について、不必要な個人情報や誤った個人情報の取得を防止するため、個人情報の「利用目的」を明確にし、その範囲内で適法かつ公正に取得することなど、個人情報の取得に関し必要な原則を定めたものです。

これは、ＯＥＣＤ理事会勧告８原則のうち、「目的明確化の原則」および「収集制限の原則」に対応するものです。

<<説　明>>

１　利用目的の明確化

(1)　事業者は、個人情報を取得する場合において、あらかじめ利用目的を明確にし、その目的を達成するために必要な限度にとどめるべきことを定めたものです。

(2)　「正当な事業の範囲内」とは、反社会的な事業のために個人情報を取得してはならないことはもとより、法令等で事業の内容が明確になっている事業者にあっては、その事業に必要な範囲内であることをいいます。

(3)　「目的を達成するために必要な範囲内」とは、取得する情報の内容、対象者の範囲等が事業の目的を達成するために必要最小限のものであることをいい、必要以上に個人情報を取得することのないようにする趣旨です。また、必要な範囲内であるかどうかは、事業者自身が恣意的に判断するのではなく社会的良識に照ら

し、客観的に判断する必要があります。

2　適法かつ公正な手段による取得

(1)　個人情報の取得に当たっては、適法かつ公正な手段によることを定めたものであり、これは個人情報の取扱いにおける基本的な原則といえ、いかなる場合においても、個人情報の不正な手段による取得は認められません。

(2)　「適法かつ公正な手段」とは、個人情報を取得する手段が法規に適合し、かつ、社会通念上に照らして正当であると客観的に判断される手段をいいます。したがって、目的を偽って個人情報を取得するなどは、公正な手段とはいえません。

　さらに、偽りやその他不正の手段により取得された個人情報であることを明確に認識しながら二次的に取得することも､公正な手段による取得とはいえません。

3　利用目的の確認

(1)　個人情報の取得に当たっては、本人が取得に応ずるか否かの判断ができるように、原則として、本人が利用目的を確認できるようにすべきことを定めたものです。

(2)　「本人が利用目的を確認できるようにする」とは、本人が容易に利用目的を知り得るようにすることをいいます。たとえば、申込書、契約書、案内書、アンケート用紙等に、あらかじめ利用目的を具体的に明示することが望まれますが、明示しえいない場合は、個人情報の取得後速やかに、その利用目的を本人に通知するか公表することをいいます。

(3)　個人情報保護法における個人情報取扱事業者の義務規定（第18条、第24条）では、個人情報の取得に際しての利用目的の通知や保有個人データの利用目的の公表等について、次の事項に該当する場合は利用目的の通知・公表等の適用除外とされていることから、事業者はこのような事項に該当する場合は、個人情報の利用目的の明示が不要です。

　ア　利用目的を本人に通知し、または公表することにより本人または第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

　イ　利用目的を本人に通知し、または公表することにより当該事業者の権利または正当な利益を害するおそれがある場合

　ウ　国の機関または地方公共団体が法令の定める事務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、利用目的を本人に通知し、または公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

　エ　取得の状況からみて利用目的が明らかであると認められる場合

　　※エの場合は、利用目的の通知は不要であるが、公表は必要

4　本人以外のものからの取得

(1)　事業者が、本人以外のものから本人の個人情報を取得する場合には、本人がその事実を知らない場合が多く、思わぬ権利利益の侵害が生じることも考えられるので、特に慎重に取り扱うべきことを定めたものです。

(2)　「本人の権利利益を不当に侵害するおそれがない場合」とは、社会的良識に照らして、客観的に判断し、本人の権利利益が不当に侵害されるおそれがない場合をいい、たとえば、次のような場合が考えられます。

ア　本人の同意を得て、本人以外のものから取得するとき。
イ　法令等に基づき本人以外のものから取得するとき。
ウ　出版、報道等により公にされたものから取得するとき。
なお、同窓会や同好会の名簿のように親睦等の目的のため作成され、限られた範囲の者に配布されたものは、公にされたものとはいえません。

(3)　事業者は、本人の同意を得ずに、本人以外のものから個人情報を取得したときは、３ (3)に該当する場合を除き、その利用目的を本人に通知または公表することにより確認できるようにすることが必要です。

§４　個人情報の利用または提供

(1) 個人情報の利用または提供は、原則として利用目的の範囲内で行うものとする。
(2) 利用目的の範囲を超えて個人情報を利用し、または提供しようとするときは、本人の同意がある場合または本人の権利利益が不当に侵害されるおそれのない場合に限るものとする。

この項は、事業者が取得した個人情報の「利用または提供」について、他人に知られたくない情報が本人の予期しない形で流通するなどの問題が発生するおそれがあるため、利用目的の範囲内で利用または提供することなど、個人情報の利用または提供に関する必要な原則を定めたものです。

これは、ＯＥＣＤ理事会勧告８原則のうち、「利用制限の原則」に対応するものです。

<<説　明>>

１　利用目的の範囲内での利用または提供

(1)　個人情報を利用したり、提供するときは、原則として、利用目的の範囲内にとどめることとしたものです。

(2)　「利用」とは、個人情報を事業者の内部において使用することをいいます。たとえば、本社で保有する個人情報を支社、支店等で使用する場合がこれに当たります。

(3)　「提供」とは、事業者が保有する個人情報を他の事業者などに渡すことをいいます。

(4)　「利用目的の範囲内」かどうかは、恣意的な判断ではなく、客観性・合理性が認められることが必要です。

２　利用目的の範囲を超えて利用・提供を行うときの本人同意

(1)　個人情報を利用目的の範囲を超えて利用することや第三者への提供を行う場合は、原則として本人の同意を得て行うことを定めたものです。

特に、第三者への提供については、本人にとって自分に関する情報がどのように取り扱われるか予期できない場合が多く、個人の権利利益が侵害されるおそれ

が高くなるので、より慎重に行う必要があります。

(2)　「本人の同意」を得る方法として、たとえば、次のようなことが考えられます。

ア　利用目的の範囲を超えて利用・提供する可能性があるときは、取得するときにあらかじめ本人の同意を得ておくこと。

イ　個人情報を取得した後に、利用目的の範囲を超えて利用・提供を行う必要が生じたときは、提供する側で提供先、提供する情報の内容、提供先における利用目的などについて本人に知らせ、同意を得ること。

3　本人からの同意を得なくても個人情報を利用目的の範囲を超えて利用・提供できる場合

個人情報保護法における個人情報取扱事業者の義務規定（第16条、第23条）では、次の事項に該当する場合は、利用目的および第三者提供の制限規定の適用除外とされていることから、事業者はこのような事項に該当する場合は、本人の権利利益を不当に侵害されるおそれのない場合に該当するものであり、あらかじめ本人の同意を得ないで、個人情報を利用目的の範囲を超えて利用し、または第三者への提供をすることができます。

(1) 法令に基づく場合

（例）・警察や検察等から、刑事訴訟法に基づく捜査関係事項照会があった場合

・弁護士会から、振り込め詐欺に関連し、銀行に対して、弁護士法に基づく所要の弁護士会照会があった場合

(2) 人の生命、身体また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。

（例）・大規模災害や事故等の緊急時に、患者の家族等から医療機関に対して、患者に関する情報提供依頼があった場合

・製品に重大な欠陥があるような緊急時に、メーカーから家電販売店に対して、顧客情報の提供依頼があった場合。

(3) 公衆衛生の向上また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。

（例）・地域がん登録事業において、地方公共団体から医療機関に対して、がんの診療情報の提供依頼があった場合

(4) 国の機関もしくは地方公共団体また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務の遂行に支障を及ぼすおそれがあるとき。

（例）・税務署等から事業者に対して、任意の顧客情報の提供依頼があった場合

4　本人の求めによる提供停止（オプトアウト）

個人情報保護法における個人情報取扱事業者の義務規定(第23条第２項)では、事業者が第三者提供におけるオプトアウトを行っている場合は、本人の同意を得ないで個人情報を第三者に提供できるとされています。

このオプトアウトの仕組みを設けることによって、事業者は本人の同意を得な

くても個人情報を活用することができます。

※「第三者提供におけるオプトアウト」とは、提供に当たりあらかじめ、以下の情報を本人に通知し、または本人が容易に知り得る状態に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいいます。
①第三者への提供を利用目的とすること。
②第三者に提供される個人情報の項目
③第三者への提供の手段または方法
④本人の求めに応じて第三者への提供を停止すること。

§５　個人情報の適正管理

(1) 個人情報は、利用目的に必要な範囲内で、正確かつ最新なものに保つよう努めるものとする。
(2) 個人情報の取扱いに当たっては、漏えい、滅失およびき損の防止その他の適切な管理のために必要な措置を講ずるよう努めるものとする。
(3) 保有する必要がなくなった個人情報は、確実に、かつ、速やかに廃棄し、または消去するものとする。
(4) 個人情報の取扱いを伴う事業を委託するときは、受託者に対して、個人情報の保護のために適切な措置を講ずるよう求めるものとする。

この項は、事業者が保有する個人情報について、個人情報が正確なものでなかったり外部に漏えいされた場合に個人の権利利益が侵害されるおそれがあるため、個人情報の正確性および最新性の確保、安全確保の措置および委託に伴う措置について定めたものです。

これは、ＯＥＣＤ理事会勧告８原則のうち、「データ内容の原則」および「安全保護の原則」に対応するものです。

<<説　明>>

１　正確性および最新性の確保

(1)　誤った個人情報や古い個人情報が利用され、または提供された場合には、その個人に対して誤った認識や不完全な認識がもたれ、個人の権利利益が侵害されるおそれがあります。このため、個人情報を正確かつ最新なものに保つべきことを定めたものですが、この場合、個人情報を一律にまたは常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性および最新性を確保すればよいと考えられます。

(2)　正確性および最新性を確保するための具体的な措置としては、たとえば、個人情報が誤っていたり、不正確であることが判明したときには、速やかに訂正し、または適切に更新することなどが考えられます。

２　安全性の確保

(1)　個人情報が漏えい、滅失およびき損されることを未然に防止するために、個人情報の安全性を確保すべきことを定めたものです。

(2)　事業者は、総合的な見地から個人情報の安全性を確保するため、組織的、人的、物理的および技術的な安全管理措置を講ずることが必要です。具体的には、次のようなことが考えられます。

ア　組織的な安全管理

組織的な安全管理とは、安全管理について従業者の責任と権限を明確に定め、安全管理に関する規程や手順書を整備、運用し、その実施状況を確認することをいいます。

たとえば、安全管理措置を講じるための組織体制の整備、規程等の整備と運用、取扱い状況を一覧できる手段の整備、安全管理措置の評価、見直しおよび改善、事故または違反への対処が必要です。

イ　人的な安全管理

人的な安全管理とは、たとえば、雇用または委託契約時に、従業者との間で、業務上秘密と指定された個人情報の非開示契約を締結することや、従業者に対する教育、訓練等を行うことをいいます。

ウ　物理的な安全管理

物理的な安全管理とは、たとえば、入退館（室）の管理、パスワードの設置や施錠保管などによる個人情報の盗難防止、個人情報を取り扱う機器や装置等の盗難、破壊、漏水または火災からの物理的な保護を行うことをいいます。

エ　技術的な安全管理

技術的な安全管理とは、たとえば、ＩＤやパスワードによるアクセスの認証やアクセスできる従業者数の最小化、アクセスできる者を許可する権限の管理、アクセス記録の管理、ウイルス対策ソフトウェアの導入等による不正ソフトウェア対策、データの暗号化などによる移送、送信時の対策、個人情報へのアクセス点検などによる情報システムの監視などをいいます。

※　以上の安全管理措置については「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」（平成16年10月経済産業省）において、詳しく示されています。

(3)　個人情報保護や情報セキュリティ等について、一定の基準に達している事業者を第三者機関が認定する制度が設けられていますので、これらの制度を積極的に活用することが有効であると考えられます。

◆プライバシーマーク制度

(財)日本情報処理開発協会（JIPDEC）およびその指定機関が、日本工業規格(JIS Q 15001)「個人情報保護に関するコンプライアンス・プログラムの要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者を認定して、その旨を示すプライバシーマークを付与し、事業活動に関してプライバシーマークの使用を認める制度です。