



2016年11月2日

アジアインターネット日本連盟

## 「個人情報の保護に関する法律についてのガイドライン(通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編)(案)」に対する意見

### 1. 「個人情報の保護に関する法律についてのガイドライン案(通則編)」に対する意見について

#### (1) ガイドライン案2-1「個人情報」について

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。)における「個人情報」の定義には、「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」も含まれています。

一方、行政機関の保有する個人情報の保護に関する法律における個人情報の定義では、個人情報保護法とは異なり「容易に」という要件は含まれておらず、この比較から、個人情報法における個人情報の該当性判断に、容易性の有無が必要な要件の一つであることは明らかです。

しかし、現行法の下における運用では、事実上、容易かどうかに関わらず、照合することができるかどうかのみで判断されています。

社内で特定の個人を識別することができる情報とそれに紐づくそれ以外の情報を分けて管理していた場合、仮に社内に両方の情報にアクセス(照合)できる人間がいたとしても、社内規程等により両方の情報にアクセス(照合)できる人間や場合などが厳格に管理され、容易に両方の情報にアクセス(照合)することができない場合等には、「容易」には照合できないものとするなど、容易性を適切に判断して解釈すべきと考えます。

また、暗号化をしたとしても個人情報であるとされているが、近年の技術の進展により、暗号化であっても元の個人情報を復元することができないものも存在しています。技術の進展を踏まえ、そのようなものについては個人情報ではないと見なすなど、実態を踏まえた解釈がなされることを望まれます。

#### (2) ガイドライン案2-2「個人識別符号」について

身体の特徴に関する個人識別符号に関し、個人情報保護施行令第1条第1号イからトまでに掲げたものの具体的な内容について、「個人情報の保護に関する法律についてのガイドライン(案)」(以下「ガイドライン案」という。)通則編2-2「個人識別符号」に規定されています。ここで、単に客観的な要素の記述に加えて「本人を認証することができるようにしたもの」という目的要件を加えた点は、歓迎したいと考えています。

身体の特徴は、その性質からして、身近な日常生活において、特定の個人を識別し、認証することを目的にすることなく取得する場合があります。このような場合であっても、仮に特定の個人を

識別するに足りる水準で電子計算機の用に供するために変換した符号等が個人識別符号に該当し、安全管理措置の対応などが求められることになっては、日常の経済社会活動に混乱を来しかねません。よって、特定の個人を識別し、認証することを目的としない場合には、身体の特徴由来の符号等は個人識別符号には該当しないという解釈、運用がなされるべきであると考えます。

なお、「認証」という新たな用語が用いられていますが、国民、事業者による予測可能性担保の観点から、「識別」「特定」等との用語との意味の違いについて補足説明があるのが望ましいと考えます。

### (3) ガイドライン案2-3「要配慮個人情報」について

#### ア. 推知情報について

要配慮個人情報について、ガイドライン案通則編2-3の柱書で、ガイドラインで(1)～(11)で掲げる情報を推知させる情報にすぎないものは要配慮個人情報に含まないとしている点は、歓迎したいと考えます。

要配慮個人情報については、取得時における同意が原則求められます。そのため、仮に推知させる情報であっても要配慮個人情報の範囲とした場合、あらかじめ同意を得ることは不可能となるものがあり、実態上、法令を遵守できないことになりかねません。そのため、このような推知情報を要配慮個人情報から除外することは、実態に即したものであり当該規定を歓迎したいと考えます。

#### イ. ガイドライン案2-3(8)「健康診断結果」について

ガイドライン案2-3(8)には、健康診断結果を定める政令第2条第2号の具体的な内容に関し、本人に対して医師等による行われた室病の予防及び早期発見のための健康診断の結果が要配慮個人情報に該当する旨が規定されています。かかる規定は法律による委任の範囲を超えるものであり、修正すべきであると考えます。

要配慮個人情報のうち政令に委任された範囲は、「本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの」です。しかしながら、ガイドライン案2-3(8)の規定には、「本人の健康状態が判明する検査の結果」と記載されており、例えば、健康診断結果が健康であるというような、本人に対する不利益が生じるとは考えにくい場合も要配慮個人情報に含まれてしまいます。

よって、要配慮個人情報の範囲が適切に定義づけられるよう、健康診断その他の検査の結果のうち、日常生活に影響を及ぼすなど特に配慮を要する結果に限定されるようガイドラインで限定解釈を規定すべきであると考えます。

#### ウ. 2-3(9) 指導、診療、調剤について

ガイドライン案2-3(9)には、「健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により調剤が行われたこと」の具体的な内容について、診療の過程で医師等が知り得た情報全て、及び調剤の過程で薬剤師等が知り得た情報全てが要配慮個人情報に該当する旨が規定されています。かかる規定は委任の範囲を超えるものであり、修正が必要であると考えます。

要配慮個人情報のうち政令に委任された範囲は「本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの」となっています。しかしながら、ガイドライン2-3(9)の規定では、例えば、風邪をひいたために抗生物質を処方された場合も要配慮個人情報に含まれてしまいます。

よって、要配慮個人情報の範囲が適切に定義づけられるよう、調剤に関する情報のうち、日常生活に影響を及ぼすなど特に配慮を要する結果に限定されるようガイドラインで限定した解釈を規定すべきであると考えます。

#### (4) ガイドライン案2-12「同意」について

##### ア. 未成年の同意について

ガイドライン案2-12なお書きには、個人情報の取扱いに関して同意したことによって生ずる結果について未成年者が判断できる能力を有していない場合、親権者や法定代理人等から同意を得る必要があるとしています。

しかしながら、経済産業分野に関する個人情報の取扱いに関するガイドラインのQ&Aでは、親権者の同意を必要とする「子ども」の年齢について12歳～15歳としており、16歳～19歳については基本的に親権者等の同意は不要としています。本ガイドライン案でかかる事情を考慮しないとすると、経済産業分野に関するガイドラインのQ&Aに基づいて事業を行っている事業者の現状の運用を変えてしまい、過度な負担となってしまいます。

したがって、従前どおり、未成年者であっても16歳以上の者については、親権者等の同意が不要であると考えます。

##### イ. 「本人の同意を得ている事例」の例示について

ガイドライン案2-12「本人の同意を得ている事例」で具体的な例が列挙されています。しかし、情報の性質、サービスの内容によって、同意取得の方法も様々なものがあり得ます。

したがって、サービスや状況に応じて上記列挙事由以外の同意取得方法があり得る旨の理解で足りることを明確にしていきたいと考えます。

#### (5) ガイドライン案4「漏えい等又はそのおそれが発覚した場合等の対応」

ガイドライン案4では、個人情報取扱事業者がその取り扱う個人情報について漏えい等の事案が発生した場合に、二次被害の防止、類似事案の発生防止等の観点から、個人情報保護委員会等への報告を含む対応の実施が求められていますが、この部分についての法的根拠が不明確です。明確な法的根拠なく、事実上の義務を課すべきではないと考えます。

従前の各分野のガイドラインでは、安全管理措置の規定に基づいて漏洩等の対応が定められていましたが、本ガイドライン案においても同じ位置づけであるならば、安全管理措置が個人データに対する規律である点に鑑み、「個人情報」の漏洩等についての対策ではなく、「個人データ」の漏洩等の対策とすべきであると考えます。

また、個人情報保護委員会への報告が求められる趣旨は、事業者に対し漏えい等の原因の把握し、事後の対応策を担保されることで、二次被害の防止、類似事案の発生防止に努める点にあります。そうであるならば、漏えい等のあった個人情報の性質、量、損害の可能性の有無等にかかわらず、一律に個人情報保護委員会等への報告をはじめとする対応を求めるのは、事業者に対する過剰な負担になり、上記趣旨にもそぐいません。

なお、OECD「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」(2014年5月7日)においても、「個人データに影響を及ぼす重大なセキュリティ侵害があった場合、必要に応じてプライバシー執行機関又は他の関連機関に通知すること。当該セキュリティ侵害がデータ主体に不利益を及ぼすと思料される場合は、データ管理者は不利益を被るデータ主体に通知すべきである。」との限定がなされており、この点を考慮する必要があります。

したがって、「詳細については別に定める」にあたっては、漏えい等のあった個人情報の性質、量、損害の可能性の有無等の事情を考慮し、重大な場合にのみに限定するべきであると考えます。

## 2. 「個人情報の保護に関する法律についてのガイドライン案(外国にある第三者への提供編)」に対する意見

### (1) クラウドサービスの取扱いについて

ガイドライン案外国にある第三者への提供編には、外国にある第三者への提供について具体的な内容が記載されているものの、クラウドサービスに関する場合についての言及がありません。

現状ではクラウドサービスの運営事業者が、保存されている情報の中に個人データが含まれていることを認識していない場合や、認識していたとしても個人データをクラウドサービス利用者が暗号化できる機能が提供されており、同運営事業者が個人データにアクセスできない場合が存在しています。

現に広く事業者利用されているクラウドサービスを海外事業者が提供しているという理由だけで制限を課すのはあまりに不当であり、低コストでクラウドサービスを利用している大多数の中小企業の企業活動を著しく阻害することになります。

そもそも上記のような場合には、クラウドサービス運営事業者は、利用者の個人データにアクセスすることを目的とはしていません。また、データの安全性は安全管理措置によって図られるものであり、海外移転を規制することはデータを分散管理することによる安全性の確保や災害時などのデータ復旧に支障をきたしかねません。

このような点に何ら考慮せず、一律に改正個人情報保護法第 24 条に規定する「外国にある第三者への提供」に同サービスの利用が該当してしまうことになれば、前記の通り、国境を越えたクラウドサービスの利用を不当に阻害することになります。また、衆議院及び参議院の附帯決議にも反することになります。

そのため、上記のような場合には、改正個人情報保護法第 24 条に規定する「外国にある第三者への提供」に当たらないこととすべきであり、その旨をガイドライン等において明記すべきであると考えます。

### (2) ガイドライン案3-3「国際的な枠組みに基づく認定」について

ガイドライン案3-3には、アジア太平洋経済協力(APEC)の越境プライバシールール(CBPR)が「国際的な枠組みに基づく認定」に含まれることが個人情報保護委員会資料で明らかにされており、このことは歓迎したいと考えております。加えて、CBPRに限らず、ISMS(情報セキュリティマネジメント評価制度)等関連するISO規格など広く普及している国際規格についても含むべきでと考えるます。

過度の事前規制ではなく、自主的な取り組みを尊重した柔軟な枠組みこそが、民間の自主努力を促し、個人情報保護に資するものであり、なおかつ企業活動、とりわけ我が国で大多数を占める中小企業の日々の活動を阻害しない方法として望ましいものと考えております。また、CBPRなど個人情報保護に向けた柔軟な執行枠組みは、個人情報保護委員会が今後も推進していくべきものであり、同委員会をはじめとする今後の取組みに期待いたします。

### 3. 「個人情報の保護に関する法律についてのガイドライン案(第三者提供時の確認・記録義務編)」に対する意見

#### (1) 解釈により確認・記録義務が適用されない第三者提供

第三者提供時の確認・記録義務に関するガイドライン案には、受領者の確認・記録義務が課されない場合については、いくつかの類型について規定されているものの、提供時の記録義務については課されない場合が少なく、実務上の負担が相当程度増えることが想定されます。

例えば、受領者にとって個人情報に該当しない場合には、確認・記録義務が課されないが、提供者の記録義務は課されることとなっています。この場合、提供者と受領者とで課される規制のバランスを欠いており、また、トレーサビリティの確保という観点からも過度な規制と思われる。

したがって、提供者に課される記録義務についても、実務を踏まえ、過度な負担とならないよう、義務が課されない類型をさらに検討すべきであると考えます。

### 4. 「個人情報の保護に関する法律についてのガイドライン案(匿名加工情報編)」に対する意見

ガイドライン案匿名加工情報編3-2-5には、購買履歴、位置に関する情報などを含む個人情報データベース等において反復して行われる行動に関する情報が蓄積されることを想定した記述があります。

しかし、例えば、購買履歴が蓄積されたこと等により特定の個人の識別又は元の個人情報の復元につながるおそれがある場合を想定するのは非現実的であると考えます。購買履歴では本人の特定につながるような情報が蓄積されることは稀であるからです。

ガイドライン案の上記記述は、購買履歴や位置情報が収集・蓄積される場合には、「個人情報」に該当しない場合でもおそれがあるということをもって、適切な加工をすることが求められることとなります。事業者に対する萎縮効果があるだけでなく、「個人情報」の定義を事実上広げるものであり、法的根拠に欠けると考えられます。

よって、13ページ下から2行目以降の文及び14ページの【想定される加工の事例】については削除すべきと考えます。

### 5. その他

本ガイドライン案以外にも、Q&A や別に定められる漏洩等の対応の詳細についても、パブリックコメントを実施するなど産業界をはじめ多様な関係者の意見を聴きつつ、検討していただきたいと考えます。

以上