METI 経済産業省

資 料 1

個人情報保護法の運用に関する検討状況について

平成23年6月15日

経済産業省
商務情報政策局
情報経済課

1．パーソナル情報研究会（検討内容①）

背景

IT技術の進展に伴い、個人の属性に着目したサービス（パーソナライゼーションサービス）が企業間連携の流れの中で、拡大する方向にあり、個人情報にとどまらず、個人と連結可能な情報（パーソナル情報と総称）の有効利用が不可欠。

安全・安心を確保しつつ、多様なサービスを提供するために必要となる環境整備上の課題について整理検討を実施（平成20年度）。

1．個人情報保護制度の枠組内の課題

① 共同利用制度に関する問題（法23条関連）

共同利用制度について、利用要件が不明確、利用者範囲等の変更が困難といった要因から十分利用されていないため、ガイドラインでの要件の明確化、モデルケースの提示を実施。

【対応】

共同利用の事例として、企業ポイント等を通じた連携サービスを提供する提携企業の間で取得時の利用目的の範囲内で個人データを共同利用する場合を追加するほか、共同利用の際に本人通知等をすべき情報のうち、これまで変更することができなかった情報（共同して利用される個人データの項目及び共同利用者の範囲）について、共同利用を行う事業者の名称のみの変更で当該事業者の事業内容に変更がない場合、共同利用を行う事業者について事業の承継が行われた場合や本人の同意を得た場合には、変更することができるよう、ガイドラインを改定（平成21年10月9日改正）。

1．パーソナル情報研究会（検討内容②）

② **事業の承継に関する問題（法16条、23条関連）**

持株会社の利用等、多様なM＆Aの形態を踏まえたルールが十分提示されていないため、事業承継時に伴う個人情報の利用が阻害されないよう、共同利用制度の周知を実施。
また、事業承継に先立つ合併対象企業の評価（デューデリジェンス）には個人情報の提供が重要であるが、法の裏付けが不明確。同目的による個人情報の提供を適法に行うための要件の明確化を実施。

【対応】

事業承継のための契約を締結するより前の交渉段階で、事業承継の相手会社から自社の調査を受け、自社の個人データを相手会社へ提供する場合は、当該データの利用目的及び取扱方法、漏えい等が発生した場合の措置、事業承継が不調となった場合の措置等、相手会社に安全管理措置を遵守させるため必要な契約をすることにより、本人の同意がなくとも個人データを提供することができるよう、ガイドラインを改定（平成21年10月9日改正）

2．個人情報保護制度の境界線上の課題

① **個人情報の範疇の問題（法2条関連）**

企業ポイントやIDビジネス等、ネット上のビジネスの進展に伴い取り扱われる種々の情報が「個人情報」に該当するか否か判断困難であるため、具体的事例について類型化、事例の提示により明確化する必要あり。

② **個人情報／個人と連結可能な情報を分別管理したデータベースの取扱い（法2条、23条関係）**

個人データから個人識別性を除去した情報について、「個人データ」に該当せず本人の同意なく第三者提供が可能か等、情報利用に関する解釈が不明確であるため、利用の可能性及び利用上の制約について検討の必要あり。

2. その他の検討について（その①）

前記のパーソナル情報研究会での検討以外に、

企業活動の実態や、他国の制度・運用等の調査を行い、運用に関する検討も実施している。

1. 個人情報の範囲について

個人情報の範囲について、個人の権利利益の保護と、個人情報の有用性のバランスから、どのような個人情報の範囲が妥当か検討。

① 照合性又は容易照合性の判断

【事業者における現状・運用状況】

個別具体的な判断を行っている。番号情報、IPアドレス、ライフログについては、判断に迷う情報が見られる。

判断が困難であるため、法の基準よりも個人情報の範囲を広く捉える事業者もある。

【ニーズ等】

番号情報それ自体を個人情報としてみなすかどうかについて、事業者によって判断が異なる。

② 公表情報

【事業者における現状・運用状況】

個人情報として扱う事業者とそうでない事業者に分かれる。

【ニーズ等】

公表情報について、個人情報と同様に安全に管理することには違和感がある。

その他の検討について（その②）

③　機微情報

【事業者における現状・運用状況】

ガイドラインなどに基づき判断する。

管理の仕方は事業者によって異なる。

機微情報とそれ以外の情報を区別した方がコストがかかるという回答もある。

【ニーズ等】

業界の自主ルールに委ねるのが適当である。

他方で、自主ルールの乱立による基準の不明確化を懸念するとの指摘もある。

④　プライバシーとの関係

【事業者における現状・運用状況】

多くの事業者がプライバシーに関係する情報であっても、個人情報として扱ってきている。

【ニーズ等】

プライバシーに関する情報を機微情報や他の個人情報と別に定義するのは難しいのではないか。

その他の検討について（その③）

EU加盟国における識別判断基準に関する規定例

国	規定
イギリス	生存者に関するデータが識別できる、またはデータ管理者が保有している、または保有する可能性のあるデータと他の情報から識別できるか。（第1条1項）
ドイツ	匿名化（depersonalisation）は識別できないものとする。匿名化とは、個人データの修正によって、個人に関する情報がもはや個人を識別されないないし識別できない、または時間、費用、労力の不均衡な量によってしか識別されないないし識別できないことを言う。（第3条6項）
ポーランド	識別に不合理な時間、費用、労力の量を要求する場合は、当該データが識別できないものとなる。（第6条3項）
スロベニア	多額の費用を生じさせないまたは多くの時間を要しない方法で識別できる場合、個人は識別できるものとする。（第2条2項）

その他の検討について（その④）

2. EUデータ保護指令の第三国移転制限について

現行の個人データ保護指令に基づく第三国移転制限条項をクリアするためには、**十分性の認定を受ける、セーフ・ハーバー協定に取り組む**、個別のケースに応じて**BCRや標準契約等を活用する**、という3つのアプローチが存在。

特に、BCRや標準契約については、現に、標準契約を用いている国内事業者が存在している。
また、BCRは、CNILが推進しており、日本国内にもBCRに関心を持つ事業者がある。

3. 事業者が講ずべき安全管理措置について

SQLインジェクションによる個人情報の漏えいなど、このような脅威に対し、どのような安全管理措置が望まれるか、どのような技術の活用が事業者の安全管理措置のレベルの向上に資するかを検討。

① 多様化する脅威への対応

多様化する脅威に対して網羅的な対抗措置を講じるためには、安全管理措置等を体系的、網羅的に整理した規格や基準を活用するのが有用（JIS Q 27000's シリーズなど）

その他の検討について（その⑤）

② 個人情報の漏えいを未然に防止するための安全管理措置

個人情報の漏えいを未然に防止するための安全管理措置に関し、事業者にヒアリングした結果、強化・充実を図るべき措置、新たな脅威に対応するため、

- 検査ツールによる脆弱性診断および人手によるペネトレーション（侵入）テストの実施、webアプリケーション脆弱性の診断
- 一定期間内にダウンロードできる情報量の制限

などの対策が有益との意見あり。

→ いずれの対策についても、対策実施に際しては、かなりのコスト負担を事業者に強いることになる。
導入する場合でも、あらゆる事業者に一律に実施を課すのではなく、取り扱う個人情報のリスクに応じた対策となるような配慮が必要

その他の検討について（その⑥）

③　個人情報の漏えいが生じた際の対策

経済産業分野を対象とするガイドラインでは、個人情報漏えいが生じた際に、事業者が高度な暗号化処理を施している場合、本人への通知や公表の省略を認めている。
この暗号化処理のように、本人への通知や公表の省略を認めてもよいと考えられる情報セキュリティ技術としては、

「存在してもアクセスさせない技術」（秘密分散など）、
「消去してしまう技術」（遠隔消去、時限消去など）
のような対策が有益との意見あり。

→　ただし、いずれも公的な認証制度がないため、法令で求めるレベルに十分な安全管理措置の判断基準はどのように確保するのかが課題