2016年11月2日

「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）」に関する意見

BSA ｜ ザ・ソフトウェア・アライアンス

BSA｜ザ・ソフトウェア・アライアンス[1]（以下「BSA」といいます。）は、改正個人情報保護法（以下「法」といいます。）に関して個人情報保護委員会（以下「貴委員会」といいます。）より公表された「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「本ガイドライン」といいます。）に関し、以下の通り意見を提出します（以下「本意見」といいます）。

BSAは、法改正、政令並びに規則及び本ガイドラインの策定の過程において、貴委員会及び各関係省庁が、民間との意義ある対話を継続しながら取り組んでこられたことに感謝し、敬意を表します。

BSAは、過去2年間に渡り私どもが提出した要望の多くを本ガイドラインに反映していただいたことに感謝します。今回追加して提出する本意見は、効果的かつ技術及び社会における急速な変化に鑑み、柔軟な個人情報保護のアプローチを推進することを目的としています。これらの変化により、個人情報を含むデータ利用がもたらす社会的利益を増大し、データ取得や処理を容易にし、データの安全な取扱いを推進し、かつ、個人情報が、いつ、どのような方法及び目的で取得・利用されるのかに関する国民の期待を調整していくことが見込まれます。更に、円滑な国際的データ移転を確保すること(越境データ移転）は、現代的なグローバル経済の基礎としての役割を増してきている新しい技術及びサービスにとって、極めて重要です[2]。従って、本ガイドラインを策定した後においても、法が社会や技

---

[1] BSA ｜ The Software Alliance（BSA ｜ ザ・ソフトウェア・アライアンス）は、グローバル市場において世界のソフトウェア産業を牽引する業界団体です。BSAの加盟企業は世界中で最もイノベーティブな企業を中心に構成されており、経済の活性化とより良い現代社会を築くためのソフトウェア・ソリューションを創造しています。ワシントンDCに本部を構え、世界60カ国以上で活動するBSAは、正規ソフトウェアの使用を促進するコンプライアンスプログラムの開発、技術革新の発展とデジタル経済の成長を推進する公共政策の支援に取り組んでいます。BSAの活動には、Adobe, Amazon Web Services, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, Dell, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, Trimble Solutions Corportation, The MathWorks, Trend Micro and Workdayが加盟企業として参加しています。詳しくはウェブサイト（http://bsa.or.jp）をご覧ください。

[2] データは何をもたらすのか？～データイノベーションが実現する世界～
http://bsa.or.jp/wp-content/uploads/BSA_Data_Report_JP.pdf

術の変化に即して時代に適合したものであるために、貴委員会、各関係省庁及び民間が対話する仕組みを継続していただけるようお願い致します。

私どもは、本ガイドライン中、以下の部分に特に着目し、これらについての具体的な意見及び要望を述べます。

I. 「外国にある第三者への提供編」
II. 「匿名加工情報編」
III.「通則編」2-11 「公表」、2-12「本人の同意」、8 (別添)講ずべき安全管理措置の内容

I.「外国にある第三者への提供編」 - 越境データ移転の観点から

個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）（以下「外国にある第三者への提供編」といいます）では、法24条に定める要件に個人情報取扱事業者が準拠するためのガイダンス及び事例が記載されています。外国にある第三者への提供編は、本ガイドライン全体の中でも極めて重要な個所であるため、全体的及び個別に意見を述べたいと思います。

BSAは、越境データ移転の問題を扱うに際し、貴委員会が「国際的な整合性」を重視していること（3-2(7頁)）について賛同します。また、貴委員会が、国際的な整合性の判断にあたり、経済協力開発機構(OECD)におけるプライバシーガイドライン（「OECDプライバシーガイドライン」）及びアジア太平洋経済協力(APEC)におけるプライバシーフレームワーク（「APECプライバシーフレームワーク」）等の国際的な枠組みの基準に準拠していることについても賛同します。実際、外国にある第三者への提供編では、OECDプライバシーガイドライン及びAPECプライバシーフレームワークへの準拠と、法第4章第1節（個人情報取扱事業者の義務）に規定された要件を対比し、その関係を分かり易く説明されています。

もっとも、外国にある第三者への提供編について、以下のおとり二つの主な懸念点があります。

第一に、BSAは、第三者による国際的な個人データの移転に関する措置を講じる上で、個人データの提供先である第三者に主眼を置くことは不適切かつ不必要であるとの意見を引き続き有しています。外国にある第三者への提供編における多くの箇所において、実質的には、個人データの提供元が行動しなければならないと記載しています(例:3-2、特に3-2-4、3-2-5、及び3-2-11から3-2-18)。これは、提供元である個人情報取扱事業者（この場合では、データ・コントローラー）が、個人情報により特定される個人（データ主体）と直接関係を有している事実を正しく反映しています。措置を講じる義務が第三者にある場合（例：3-2-6 安全管理措置、3-2-7 従業者の監督等）であっても、これらの遵守を確保す

る義務は個人情報取扱事業者に課せられるべきです。

例えば、OECDプライバシー・フレームワーク並びにAPECプライバシー原則及び越境プライバシールール(CBPR)システムに記載される個人情報保護のアカウンタビリティ・フレームワークの下では、適切な方法による遵守又は国際的な枠組みの認定につき説明責任を負うのは、個人情報の提供元である個人情報取扱事業者であるべきです。このアカウンタビリティモデルによれば、個人データの移転に際して、委託先/提供先（例えば、データ・プロセッサー）が、現地法を遵守しながら情報を安全に保護することの確保につき、個人情報取扱事業者が説明責任を負います。このアプローチは、情報がどこで処理されるかに関わらず、個人データの効果的な保護を促進しつつ、必要に応じた柔軟性を持たせることを可能にします。また、このアプローチは、APEC CBPRシステムを支える現地及び海外の協力的な執行メカニズムが、現地の説明責任を有する認証を受けた個人情報取扱事業者に対して適用されることを確実なものとします。

前記に基づき、外国にある第三者への個人データの移転について、個人情報取扱事業者が国際的な枠組み（例：OECDプライバシーガイドライン及びAPECプライバシーフレームワーク）に準拠し又は認定を受けている場合には、法第24条及び第4章第1節の遵守を示すことが可能とすべきです。

この観点から、BSAは、引き続き、規則第11条第2号の再検討を望んでおり、以下の通り修正されることを要望します。
規則第11条第2号：「**個人情報取扱事業者又は**個人データの提供を受ける者が、個人情報取扱いに係る国際的な枠組みに基づく認定を受けていること」

そして、外国にある第三者への提供編 3-3(31頁)は、以下の通り修正すべきと考えます。
「これには、**個人情報取扱事業者又は**個人データの提供を受ける外国にある第三者が、APECの越境プライバシールール（CBPR）システム（※）**、OECDプライバシーフレームワーク、又は他の個人情報取扱いに関する適切な国際的な枠組み**の認証を得ていることが該当する。」

第二に、日本企業の外国にある親会社につき、法24条における第三者とみなすことについて懸念を有しています。国際企業が事業を効率的に進めるために行わなければならない企業内の膨大な量の越境データ移転を鑑みると、かかるデータ移転についても外国にある第三者へのデータ提供として制限を課すことは、正当なものとは言えません。また、このことは、外国にある第三者への提供編「１　本ガイドラインの位置づけ」に記載されている「事業者に対して新たな規制を課するものではなく」という点にも反します。

3-3 個人データの提供を受ける者が、個人情報の取り扱いに係る国際的な枠組みに基づく認定を受けていること（規則第11条第2号関係）（31頁）

前記の個人データの提供先である第三者に主眼を置くことについての主要な懸念点に加え、規則第11条第2号の要件を満たすのは、APECプライバシー原則への準拠を示すAPEC の越境プライバシールール（CBPR）システムの認証のみに限定されるものではないことを明確にすることによって改善すべきであると考えます。個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制を備えていることを示すものとして、他の既存及び今後制定される国際的な枠組みへの準拠又は認証についても検討すべきです。データ駆動型経済の発展に伴い、越境データ移転が今後益々重要となっていくことに鑑みれば、「国際的な枠組みに基づく認定」をAPEC CBPRの認証１つに限定するのではなく、世界で広く受け入れられている他の国際的な枠組みへの準拠又は認証についても含めるよう要望します。また、多くの国際的な枠組みが認証の仕組みを持っていますが、データ・コントローラー及びデータ・プロセッサーによる、これらの国際的な枠組みへの自己認証を可能にすべきと考えており、この点も重要です。

前記の外国にある第三者への提供編の修正案は、この懸念を解決するものです。

クラウドコンピューティング及びインターネット関連サービスについて

本ガイドラインでは、特にクラウドコンピューティング及びインターネット関連サービス（以下、総称して「クラウドサービス」といいます。）に関して言及していませんが、私どもは、貴委員会がクラウドサービスの取扱いについて引き続き検討されているところであり、別途ガイダンスを示されるものと理解しています。顧客が巨大なストレージ及びコンピューティング能力の恩恵を受けることができる、様々な種類のインターネット関連サービスをもたらすクラウドサービスは、その性質上グローバルなものであり、円滑な越境データ移転に大きく依存しています。クラウドサービスは、非常に多くのユーザーが、当該サービスを使って自己のデータを管理している点に特徴があります。これらのユーザーは、（もし個人情報を取り扱っていれば）自身が個人情報取扱事業者となり、ユーザーが保存、バックアップ、分析、コミュニケーション等の目的のため、かかる情報をクラウドサービスプロバイダーに提供する、という関係にあります。これらの特徴から、BSAは、クラウドサービスプロバイダーが以下のいずれかの要件を満たす場合には、クラウドサービスの利用は、ユーザーによる個人データの「提供」にも、ユーザーからの個人情報の「委託」にも該当せず、従って、法24条及び他の関連する条項の適用の範囲外であることを明示していただくことを求めます。

(1) 提供するサービスにおいて自己のユーザーが個人情報を取り扱っていることを知らない場合

(2) サービスプロバイダーでさえも当該情報にアクセスすることができないよう、暗号化

などのセキュリティ機能を提供していること、又は、
(3) 個人情報の取扱いに係る国際的な枠組みに準拠し又はこれに基づく認定を受けていること

II. 匿名加工情報編

個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）においては、匿名加工情報を作成し、取り扱う事業者の義務に関し、規則第19条の基準に準拠する加工方法（特定の個人を識別することができないよう加工することや、復元できないようにすることなど）について記載しています。

この点、3-2-1から3-2-5に記載された想定される事例は限定的なものではないこと、及び事業者が、結果を重視したリスクベースの考え方に基づき、効果的に個人の識別及び再識別を防止する適切な方法を採用すべきであることを明示し、本ガイドラインをより良いものにすべきと考えます。なぜなら、匿名加工情報の複雑性と再識別の困難性は、関連するリスクによって定まるべきものであり、また、その情報の性質（要配慮性、匿名加工情報の利用者及びその利用目的など）の違いによって、匿名加工情報の使用におけるリスクが大きく異なるからです。例えば、学術機関によって研究のために用いられる場合とデータ・セットとして公表され又は広く共有される場合とでは、リスクは大きく異なります。

また、適正な加工方法は、技術革新の影響を受けるとともに、業界の自主的な取組みが、効果的なデータ保護に向けて大きく貢献する可能性があります。従って、BSAは、現行及び将来の各産業分野で提案されるベストプラクティスが採用されるべきである旨も、本ガイドラインに記載することを要望します。

III. 通則編

BSAは、**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）**の以下の箇所につき明確化を要望します。

8（別添）講ずべき安全管理措置の内容

通則編の8（別添）は、個人情報取扱事業者が講ずべき措置の内容につき、中小企業における手法例との相違を示しながら記載しています。

本別添につき、BSAは、貴委員会が、その序文で説明されているように、安全管理措置について、リスクベースで柔軟かつ結果重視のアプローチを採用している点、特に、「安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取

り扱う個人データの性質及び量を含む。)、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。」と記載されている点に賛同します。

もっとも、貴委員会が、リスクベースアプローチを採用するメリットについても、より明示的に記載し、個人情報取扱事業者が、関連するリスクに応じて自らの限定的なリソースを優先順位に基づき配分する方法として本アプローチを推奨すると、当該箇所の記載がより良いものになると考えます。かかる優先順位付けによって、個人情報を効果的に保護するという目的を達成するために最も効率的で効果的な措置を講ずることが可能となります。

また、当該箇所は、マルチステークホルダープロセスにより作成されグローバルに認められた任意の標準に準拠又はこれを参照することにより、事業者が、安全管理措置要件への準拠を示すことができることを明確に記載することによっても改善されます。さらに、プライバシーマーク認証や国際的なベストプラクティスに沿った第三者による監査の利用についても、安全管理措置要件への準拠を示す適切な方法に含めることを検討すべきです。

2-11 「公表」

通則編2-11(同23頁)は、個人情報取扱事業者が、個人情報を取得した場合、あらかじめその利用目的を公表している場合を除き、「利用目的」を「公表」する義務（法第18条第1項）につき、これを満たす方法について説明しています。

この点、【公表に該当する事例】の事例１）では、事業者は「自社のホームページのトップページから1回程度の操作で到達できる場所への掲載」により要件を満たすことができるとしています。事業者のウェブサイト上の見にくい又は見つけるのが困難な場所に、このような公表が埋もれることを防止することの必要性は理解できますが、トップページから到達までの回数をガイドラインで規定することは、詳細に規定し過ぎであると考えます。

そこで、まず、当該箇所及び通則の他の箇所の事例も、限定的又は網羅的であることを意図するものではなく、貴委員会は、本要件の目的を満たす合理的な他の方法も受け入れる旨明白に記載していただきたいと考えます。

次に、前記事例１は、他にも多く存在する当該要件を満たす手法の一つであることから、事例１の文言を「自社のウェブサイト上に掲載。但し、一般人が合理的に到達できる態様で掲載すること。」のように、より汎用的な表現に変更すべきと考えます。

2-12 「本人の同意」

通則2-12(同23頁)は、個人情報取扱事業者が、「利用目的の達成に必要な範囲を超えて」個人情報を扱う場合にあらかじめ得なければならない「本人の同意」(法第16条第1項)の取得方法について説明しています。

この点、特定のサービスを利用するために(例えば、ある特定のウェブサイトにアクセスするなど)、個人が追加の利用目的のための個人情報の利用に同意しなければならないことが明らかな場合には、当該サービスへのアクセスに合意したことをもって同意を構成するとすべきと考えます。

結び

BSAは、本ガイドライン案に対する意見提出の機会及びこれまでのご尽力に感謝致します。本意見が、本ガイドライン案を完成させる上で有益であることを願うとともに、引き続き個人情報保護法の施行に関して、貴委員会を始めとする関係各省庁と協力していけることを願っております。本意見について、ご質問等ございましたらいつでもご連絡下さい。

以　上