2014 年 10 月 28 日

「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」の改正案に対する意見

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」）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」の改正案（以下「本改正案」という。）に対して以下の通り意見を提出致します。

I. 総論

まず、BSAは、個人情報保護に関する消費者の信頼を向上させる可能性がある点で、日本で現在議論されている個人情報の保護に関する法律（以下「現行法」という。）の改正及び関連する提案を歓迎していることをお伝えします。そして、BSAは、そのような現行法自体の改正の動きに加え、現行法に関する「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」（以下「本ガイドライン」という。）の改正にも強い関心を持っております。

BSAは、ユーザーのデータの安全を確保すること及び個人データの悪用を阻止することこそが、信頼を高めるために重要であることを十分理解しており、そして、データドリブン・イノベーションを加速させるためにも重要な要素であると考えます。

現行法が規定するとおり、個人情報取扱事業者は、自ら直接取り扱う個人データを保護するため適切な措置を取る必要があるのみならず、委託先の適切な監督をしなければならず、本ガイドラインが規定するとおり、当該委託先監督の一つの要素として、個人データの取扱いを委託するパートナーである委託先の選定にも責任が求められるものです。そして、個人データを取り扱う事業者は、個人データを当該個人から直接取得しない場合には、デューデリジェンスを実行し、当該データが適法な方法で取得されたことを確実にするた

---

[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, Altium, ANSYS, Apple, ARM, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DELL, IBM, Intel, Intuit, Microsoft, Minitab, Oracle, PTC, Rockwell Automation, Rosetta Stone, salesforce.com, Siemens PLM, Symantec, Tekla, The MathWorks, Trend Micro 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。

めの合理的な措置を取る必要があると考えます。しかしながら、これらの目的は、リスクと状況に応じたアプローチを取ることによって、最大限達成されるものです。そうすれば、事業者は、当該事業者にとって最もセンシティブな情報を保護するために、不足しがちなリソースを集中させることができるからです。本ガイドラインは、元々、取るべき措置は「事業の性質及び個人情報の取扱状況等に起因するリスクに応じ」講じる、と記載していましたが（新旧対照表2頁等）、BSAは当該アプローチに賛同します。このアプローチは、安全管理措置について貫かれるべきものでしょう。即ち、すべてのものを保護しようとすれば、何も保護できずに終わってしまう可能性があります。それゆえ、保護措置を実行する際には、最もセンシティブな情報に注力できるような粒度と柔軟性を有することが重要です。達成困難かつ規範的な保護措置を要求することは、すでに不足しているリソースをさらに希薄かつ不必要に拡散させるだけです。その結果、全体の保護レベルは低くなってしまいます。

BSAは、貴省が、事業者に対して、ルールがどのように実行されれば一番良いかを明確にするため、運用のガイドラインを提供しようと努めていることを評価します。しかしながら、詳細かつ規範的すぎる要求は避けるべきであり、貴省には、より本質的な成果に注力して頂きたく存じます。成果（すなわち、事業者がどのように達成するかではなく、何を達成するかということ）をより重視すれば、個人情報取扱事業者に不必要な負担を強いることなく、より強固なユーザーの保護を達成できるからです。詳細で画一的な管理方法を規定することは、企業に過大な負担を強いるだけでなく、個人情報の保護に有益な信頼できる新サービスや手法を導入することを妨げ、企業活動の迅速性や経済の活性化を著しく損ねてしまいます。

政府には、これらのポイントを考慮して頂き、本改正案を見直し、修正して頂きたいと考えます。

II. 各論

以下、本改正のうち、特に重要と考える事項について個別に意見を述べます。

1. 第三者から個人情報を取得する際の経緯の都度確認（新旧対照表１頁）

本改正案は、第三者から個人情報を取得する場合、その都度、提供元が個人情報を取得した経緯を示す契約書類等の書面を点検する等により、当該個人情報の取得方法を確認すべきであるとしています。前述のとおり、個人情報取扱事業者は、個人データを当該個人から直接取得しない場合は、デューデリジェンスを実施し、当該データが適法な方法で取得されたことを確実にするための合理的な措置を取る必要があります。しかしながら、例えば、提供元との間で個人情報保護法の遵守を確認するだけでは足りず、個人情報取得に関わる契約書等の点検を求めることは、現実的ではなく、過度の負担となって、企業活動

の遅延を引き起こし、円滑な取引への障害を生じさせることとなります。また、契約書等は個人情報に関する事項のみならず秘密事項を含む可能性があり、そのような場合関連する全ての契約書を契約の当事者以外に開示することはできず、また、確認作業には多くの人手や時間、専門性を要するため、企業活動に重大な負担と制限を課すこととなります。従って、当該追加部分は削除すべきです。

2. 安全管理措置（新旧対照表　2頁：組織的安全管理措置（管理委員会の設置やCPOへの役員任命等、同4頁乃至5頁：物理的安全管理措置）

（１）前述のとおり、BSAは、ユーザーのデータの安全を確保すること及び個人データの悪用を阻止することが、信頼を高め、そして、データドリブン・イノベーションを加速させる重要な要素であると考えます。個人情報取扱事業者は、実際、取り扱う個人データを保護するため適切な措置を取る必要があります。

しかしながら、過度に規範的な要求（個人情報保護管理者（CPO）には役員を任命すること等）は、上記を達成する最善の方法ではありません。従業員の訓練及び教育と同様、役割及び責任の明確化も個人データの効率的な保護にとって重要な要素であることには同意します。そして、当該機能は、専任の個人情報保護管理者や専門の部門が、適切に実施する場合もあると思います。実際、BSAの多くのメンバーが、このアプローチをとり、社内で当該機能を実現しています。しかしながら、そのような役職や部署の構築を一般的に求めることは、多くの事業者にとって不必要かつ不相当な可能性があり、多大な費用と過度の負担に容易につながり得ます。

（２）また、本改定案では、個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R, USBメモリ等の外部記録媒体を接続できないようにするとともに、スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）との措置を記載していますが（新旧対照表4頁）、単に接続を制限するというのは、記録媒体やモバイル端末によるユーザーへの多大な便益を否定することになり適切でありません。むしろ、この点については、接続制限の措置ではなく、個人データを保存できる端末や媒体が、暗号化等の適切な技術により、不正なアクセスや予期しない喪失から保護されるべきこと、コンピュータ機器は、組織のルールに従って、管理されモニターされるべきことを記載すべきです。

（３）さらに、安全管理措置の内容として追加を示唆されている、入退室の際の検査の実施やカメラでの撮影によるモニタリングについても、多くの労務管理上の労力がかかり高額な費用を要する割に、個人情報の盗難等の防止にどれくらい役立つか疑問です。なぜなら、個人情報はデジタルデータとして取り扱われ、BYOD(Bring Your Own Device)の普及に伴い、従業員の所持するデバイスに管理されていることも多いからです。その意味では、従業員や人員の訓練及び教育を重視することが個人データ保護のより効率的な方法であり、

それゆえ、そのような内容を重要視すべきです。

加えて、安全管理措置の要求事項については、ビジネスがこれらの要求を予測し、それに適応できるよう、できる限り修正は最小限にとどめ、より一貫性を維持すべきであると考えます。

3. 委託先の監督（新旧対照表 8 頁乃至 9 頁）

BSA は、事業者が、委託先の監督として、委託先の選定に責任を負うべきことには賛同します。本ガイドラインに列挙されているものやその他最近の基準（クラウドに関連するものでは、ISO27001 や ISO 27018）などの認知されている規格や標準は、委託元にとって、委託先が委託するデータを保護するうえで適切な安全管理措置を取っているかを判断するための、良い指標となります。既に幅広く事業者に利用され、また消費者に国際的に認知されているプライバシーマーク、認証、第三者による監査なども、委託された個人データを適切に取り扱う能力が委託先にあるかを示す有効な指標となります。BSA は、政府が、より直接的に、これらの選択肢が有効な方法であると認識し、示していただきたいと考えます。

他方で、定期的な監査といった実地検査の要求は、海外にデータセンターを置くクラウドサービスでは事実上不可能を強いるものであるから、個人情報を取り扱うサーバーの国内設置を推奨することになります。これは、むしろ、個人データの安全管理に意味のある向上をもたらさず、不適切で過大な負担を強いるものです。従って、これらの要求は本改正案から削除すべきです。

自社内で実施すべき安全管理措置については、各社は自社内の全ての情報を参考にすることができるものの、取引相手方である委託先に対して自社で行う場合と同等の情報開示を求めることは、委託先の営業秘密の保護の観点からも、実務上要求することに無理があります。従って、詳細な確認項目の列挙は、網羅的な取引先への確認の要求により取引を遅延させ、また、安全管理措置に関する情報には企業秘密が含まれることも考えられ必ずしも開示できるとは限らず、適切ではありません。

本ガイドラインは、最新の手法やサービスの選択を可能とするようなものとすべきであり、企業が個別かつ詳細に列挙された確認事項や監査を行うことを求める記載は削除又は改定すべきであると考えます。

以　上