2025 年 5 月 12 日

「個人情報保護法の制度的課題に対する考え方について」に関する提言

Business Software Alliance （ビジネス・ソフトウェア・アライアンス、以下 BSA）[1]は、「個人情報保護法 いわゆる 3 年ごと見直し」において、個人情報保護委員会（以下、貴委員会）がステークホルダーとの議論を重ね、その内容を「個人情報保護法（以下、法）の制度的課題に対する考え方について」[2]（以下、報告書）としてとりまとめたことを高く評価します。

BSA は、エンタープライズソフトウェア企業を代表する業界団体であり、会員は他の企業を支援する、B2B（business-to-business）テクノロジー製 品やサービスを開発しています。BSA 会員企業の業務運営にプライバシーとセキュリティの保護は不可欠であり、BSA の提言活動における優先課題となっています。

BSA の会員は、クラ ウド・ストレージやデータ処理サービス、CRM（顧客関係管理）ソフトウェア、人事管理プログラム、ID 管理サービス、サイバーセキュリティ・サービス、コラボレーション・システム等のツールを提供し、AI に対応した製品やサービスを開発・提供する最先端企業です。企業は、個人情報を含む最も機密性の高い情報の一部を BSA 会員企業を信用し、託しています。BSA 会員は、その信頼に応えるために懸命に努めており、そのため、データ利活用の恩恵を損なうことなく、責任ある個人情報の利用を支えるための政策について、独自の見識を持っています。

多くの企業の製品やサービスにおいて AI の利用が進む中、個人情報保護法を更新する必要があることを貴委員会が認識していることを我々は心強く思います。これらの製品やサービスを継続的に向

---

[1] Business Software Alliance（www.bsa.org）は、人工知能、サイバーセキュリティ、クラウドコンピューティング、その他の最先端技術をリードする企業を代表する、エンタープライズソフトウェア業界のグローバルな業界団体です。米国、欧州、アジアの 20 以上の市場で活動し、あらゆる産業部門と一般市民がイノベーションの恩恵を受けられるよう、テクノロジーへの信頼を築く政策を提唱しています。

BSA のメンバーは以下の通り：Adobe、Alteryx、Amazon Web Services、Asana、Atlassian、Autodesk、Bentley Systems、Box、Cisco、Cloudflare、Cohere、Dassault Systemes、Databricks、Docusign、Dropbox、Elastic、EY、Graphisoft、HubSpot、IBM、Informatica、Kyndryl、MathWorks、Microsoft、Notion、Okta、OpenAI、Oracle、PagerDuty、Palo Alto Networks、Rubrik、Salesforce、SAP、ServiceNow、Shopify Inc、Siemens Industry Software Inc.、Trend Micro、TriNet、Workday、Zendesk、Zoom Communications Inc.

[2] 「個人情報保護法の制度的課題に対する考え方について」（令和７年３月５日　個人情報保護委員会）
https://www.ppc.go.jp/files/pdf/seidotekikadainitaisurukangaekatanitsuite_250305.pdf

上させるためには、個人データの適切な保護を確保しつつ、AI の開発・導入において個人データの効果的な利活用を可能とすることがますます重要になってきます。

貴委員会が、検討されている法改正に関して、ステークホルダーからの意見を受け付けていることに感謝します。我々からは、以下の点に関する提言を提出します。（1）本人同意以外の法的根拠による個人データ処理を可能とするデータ利活用の促進（2）漏えい報告・通知の合理化（3）データ処理の委託を受けた主体に対する規律の見直し（4）違反行為を繰り返す事業者に対する措置における第三者への協力要請。

データ利活用の促進

貴委員会が、同意取得要件の考え方を改め、他の法的根拠に基づいて企業が個人データを処理することを明示的に認めるいくつかの改正を検討していることを我々は歓迎します。これには、本人同意を要件としない以下の場合が含まれると理解しています。１）AI 開発等を目的とする統計情報の作成のために個人データを第三者に提供する場合（公開されている要配慮個人情報の取得も含む）２）契約の履行に不可欠な場合３）個人情報の取得の状況から見て、その提供が本人の意思に反しないことが明らかな場合４）生命の保護や公衆衛生の向上を目的とする場合５）医療の提供を目的とする機関又は団体による学術研究の場合。

様々な場面において、同意が個人データ処理の最も適切な根拠とはなり得ないことを認識した、こうしたアプローチを我々は支持します。これらの改正により、企業がこうした目的のために個人データを処理することが明確に認められ、より効果的なデータ利活用が促進されるよう、貴委員会と新たな規律の実施の詳細について協議していくことを期待しています。例えば、報告書では、統計分析のために個人データを第三者と共有する場合、一定の情報を公開し、契約上の制限を設けることが提案されています。しかし、データ共有に関する詳細な情報を公開することは、悪意のある行為者の標的となり、プライバシー保護を損ない、企業秘密の漏洩リスクにつながる可能性があります。したがって、こうした義務が実際に実施可能であり、個人データのプライバシー保護を促進するという、広範な目標を損なうことのないよう、貴委員会がステークホルダーと協議することを強く推奨します。

報告書で示された改正に加え、我々は貴委員会に対し、企業が正当な利益（legitimate interests）に基づいて個人データを処理できることを認めるなど、データ利活用をより広範に支援することを検討するよう求めます。正当な利益の枠組みを法に組み込むことで、より柔軟で適応性のある枠組みが構築され、企業は、個人、企業、社会の利益のために様々な製品やサービスをサポート、提供、改善する上で必要な個人データを収集できるようになります。また、同時に、そのような処理が個人の権利を損なわないようにすることが可能となります。実際、EU 一般データ保護規則（以下、GDPR）のような多くの主要なプライバシーの枠組みは、個人データ処理の法的根拠として正当な利益を含んでいます。このような枠組みを、個人情報取扱事業者（すなわち「管理者/controller」）に対するデータ保護影響評価（DPIA）の実施要件と組み合わせることもできます。こうした評価により、企業は特定のデータの利用がもたらす影響を評価し、その活動に関連するプライバシー保護のための措置が適切に講じられているかどうかを判断することができます。

漏えい報告・通知の合理化

報告書では、漏えいへの対応を合理化するため、本人への権利利益に対するリスクがほとんどない場合において、影響を受ける本人への通知を不要とすることが提案されています。我々はこの有効な提案を強く支持します。本人への通知は、本人に損害が及ぶ重大なリスクがある場合にのみ必要とされるべきです。

また、貴委員会が速報の免除を検討していることを我々は評価しますが、代替案を提案します。

報告書では、体制・手順に係る認定個人情報保護団体などの第三者の確認を受けることを前提として、特定の組織に対して、漏えい発生時の速報を免除することが提案されています。

我々は、これに代わり、データ漏えいに関するリスクベースの閾値を貴委員会が明確にすることを推奨します。特に、漏えい報告を組織に求めるのは、本人に損害が及ぶ重大なリスクがある場合のみとすべきです。個人データに係る本人の数が千人を超える漏えいに関し、本人に損害が及ぶ重大なリスクがない限りは、貴委員会への報告義務を免除すべきです。また、組織が漏えいに対して責任もって報告できる体制にあることを示す上で、ISO 27000 シリーズといった、国際的に認められた規格への準拠または認証を認めるべきです。これには、情報セキュリティマネジメントに関する国際的に認められた規格である ISO 27001 が含まれます。多くのグローバル企業が既に国際的に認定された認証を取得していることを踏まえ、それらを認識し、日本固有の追加要件を課すことを避けることにより、貴委員会と企業双方に追加的な負担をかけずに、改正の目的を達成することが可能となります。

データ処理の委託を受けた主体に対する規律の見直し

個人データの取り扱いを、複数の主体に依存する状況が増えています。このことが報告書において認識され、データ処理の委託を受けた主体の重要性を指摘しています。そして、データ処理を外部委託する場合には、委託された個人データの取扱いの態様等、データの取り扱い方に配慮する必要があることも認識されています。

貴委員会 が「3 年ごと見直し」において委託事業者の役割を検討するのであれば、この役割を他の主要なプライバシー法およびデータ保護法における「処理者/processor」の役割と同様に 扱うことを強く推奨します。例えば、EU の GDPR は、他の企業に代わって、また他の企業の指示に従ってデータを取り扱う処理者の役割を認識しています。また、GDPR 第 28 条では、処理者固有の義務も設定されています。これらの規定では、処理者は文書化された指示にのみ基づいて個人データを取り扱い、処理する個人データのプライバシーとセキュリティを保護するための具体的な措置を講じることが義務付けられています。同様に、処理者向け認証である「APEC Privacy Recognition for Processors (**PRP**)」では、処理者がデータを取り扱う際の基本的な要件を定めており、APEC プライ

バシー・フレームワークで定められている管理者の義務を補完しています。 これらの異なる役割に対して異なる義務を設けることは、世界中のプライバシーおよびデータ保護法の特徴です。[3] [4]

重要なことは、処理者（または委託を受けた主体）の役割は、第三者の役割とは異なるということです。処理者は、他の主体に代わって個人データの取り扱いを委託されており、自身の目的のために個人データを独自に使用する権限を与えられていません。法改正においては、この二つの異なる役割を混同しないように注意すべきです。

違反行為を繰り返す事業者に対する措置における第三者への協力要請

貴委員会からの命令を受けても違法行為を続ける悪質な事業者に対応するため、報告書では、違反行為を中止させるために、第三者への協力要請規定を設けることを提案しています。具体的には、個人情報の保存に用いるためのクラウドサービスを提供する事業者、個人情報を公開するためのサーバーのホスティング事業者、個人情報の流通に係る電気通信役務を提供する事業者などに協力を求めるとしています。措置としては「個人情報等の取り扱いのために用いられる役務の提供の停止」や「個人情報等の送信の中止等」が提案されています。

第三者へのこうした要求は、特にクラウドストレージプロバイダーなどの B2B 企業において重大な懸念を引き起こす可能性があります。これらの企業は、契約上および技術的な制約により、法人顧客に代わって処理するデータへのアクセスが制限されています。顧客に代わって保存するデータにこうした企業が自由にアクセスできるわけではありません。技術的な制約により、特定の法人顧客に関連するデータを特定できない場合があります。さらに、B2B プロバイダーは、顧客に代わって保存するデータのプライバシーを保護するための契約上およびその他の義務も負っており、これにより、データへのアクセス権がさらに制限されます。

貴委員会が第三者への命令を発する権限を付与されるのであれば、そのような措置を制度化する前に、第三者が違法行為の責任を負うとみなされる状況について徹底的に分析し、具体的な過失行為を特定する必要があります。また、そのような「必要な措置」は、第三者が合理的に従うことができる措置に限定すべきです（例えば、アカウントそのものの停止）。加えて、第三者への命令はすべて書面化し、法的要件に基づくものであることを明示すべきです。これにより、貴委員会が提示した証拠が不十分であるために、後々、第三者とその法人顧客との間で紛争が発生するのを防ぐことができます。

---

[3] 処理者の役割に関する詳細は、BSA の「Controllers and Processors: A Longstanding Distinction in Privacy」を参照ください。 https://www.bsa.org/policy-filings/controllers-and-processors-a-longstanding-distinction-in-privacy

[4] APEC PRP、APEC 越境プライバシールールシステム（CBPR）、グローバル CBPR フォーラムは、管理者と処理者の役割と義務を区別し、国際的なデータ移転を促進するための重要な制度です。日本は、これらの制度の発展において重要な役割を果たしてきました。本制度がグローバルに実施・拡大される中、日本がグローバル・フォーラムをリードし続けることを我々は奨励します。

結論

BSA からの提言をご検討頂けることに感謝します。法改正について引き続き議論される際に、本提言が有用となることを願っています。３年ごと見直しの過程において、貴委員会が考え方を示し、BSA を含むステークホルダーとの議論の場を設けたことを我々は高く評価しています。また、透明性のある形でステークホルダーと継続的な意見交換を行うために、懇談会を立ち上げたことを歓迎します。本懇談会に貢献する機会と、本提言で挙げた重要な点について今後も対話を続けていけることを期待しています。本意見書に関して、ご質問や、より詳細な議論をご希望であれば、ぜひお知らせください。

22F Shibuya Mark City West　1-12-1 Dogenzaka, Shibuyaku, Tokyo 150-0043
+81 3 4360 5474　**www.bsa.org**