「個人情報保護法　いわゆる３年ごと見直し 制度改正大綱」に関する意見

2020年1月14日

BSA ｜ The Software Alliance（**BSA**）[1]は、「個人情報保護法　いわゆる３年ごと見直し　制度改正大綱」（以下「**本大綱**」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。）に対して以下の通り意見を提出します。

総論

BSA 会員企業は、世界各国で、クラウドコンピューティング、データ分析、機械学習及び人工知能等最先端の技術及びサービスを提供し世界を牽引しています。そして、BSA は、強固な対策によって個人情報を保護することが、顧客の信頼を構築し維持するために必須であることを認識しています。これは、消費者や社会が、最新のソフトウェア関連技術が支える経済的及び社会的発展から恩恵を受けるために必要なことです。

この理由から、BSA及びBSA会員企業は、企業が正当な事業上の利益を追求することを可能としながら、消費者が自己の個人情報をコントロールして消費者の期待に合致した個人情報利用を確実に行うことができるデータ保護フレームワークを支持します。BSAは、「個人情報保護法　いわゆる３年ごと見直しに係る検討の中間整理」に関して2019年5月に意見を提出し(以下「**前回意見書**」といいます。)[2]、その後も個人情報保護法改正案の策定動向を注視してきました。この間、貴委員会や他の利害関係者と関連する諸問題について議論する機会をいただき感謝いたします。

当該議論の過程において、貴委員会が個人情報保護法の改正を検討する際には、**BSAグローバル・プライバシー・ベストプラクティス**[3]を参照いただけるよう私どもは推奨しました。BSAグローバル・プライバシー・ベストプラクティスに示されるとおり、BSAは、個人データの収集及び利用の透明性を高め、収集及び利用に対するガバナンスを提供することによって情報に基づく選択を可能にし、かつ、これを尊重し、消費者に自己の個人データについてのコントロールを与え、強固なセキュリティを提供し、正当な事業目的でのデータ利用を促進する施策の実現を支持します。現行の個人情報

[1] BSAの活動には、Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta,Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, 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] 前回意見書は、https://bsa.or.jp/wp-content/uploads/20190530j.pdfにてご覧いただけます。

[3] BSAグローバル・プライバシー・ベストプラクティスは、https://www.bsa.org/~/media/Files/Policy/Data/2018_BSA_Global_Privacy_Best_Practices.pdfにてご覧いただけます。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

保護法には、当該特徴のうち多くの部分が既に盛り込まれています。

さらに、現代のデータ社会において企業がグローバルに事業を行うためには、各国の個人情報保護に関する法律及び制度がグローバルに相互運用可能であり、円滑な越境データ移転が促進されることが非常に重要です。BSA は、貴委員会が個人データの保護及び利活用に関する国際的な議論をリードしていく旨表明されていることを高く評価します。また、貴委員会が、適切な国際的枠組みを通じて、世界の個人情報保護制度のハーモナイゼーション及び相互運用性を引き続き促進していかれることを真摯に希望します。

以下、貴委員会による検討のため、より具体的な意見を述べ提言をします。もっとも、一般的に、法案の具体的な文言又は改正内容についてより具体的な記述がない場合、本大綱に対するより詳細で関連性のある建設的意見を提供することは困難といえます。**私どもは、個人情報保護法改正案、政令案、規則その他関連ガイドライン案の文言に関し、国会への提出又は詳細内容決定の前に、貴委員会がBSA及び他の国際的なソフトウェア業界を代表する者を含む関心を有するステークホルダーと協議いただけるよう要望します。**

提言

第 3 章 具体的検討事項
第 1 節 個人データに関する個人の権利の在り方

個人は、自己の個人データに対してコントロールを有するべきです。BSA は、国際的に認められたベストプラクティス及び標準に整合した消費者の権利を実現するための取組を支持します。個人は、必要に応じて、個人データについて開示、訂正、利用停止を請求できるべきです。他方、当該請求及び企業の対応義務の範囲は現実的かつ柔軟性を有するものであって、事業活動に不当な負担を課すことがないようにすべきです。

利用停止又は消去

本大綱第 3 章第 1 節第 3 項では、利用停止、消去、第三者提供の停止の請求に係る要件の緩和を提案しています。

この提案は、個人の権利の範囲を拡大し、個人に対して、個人データへのより多くのコントロールを与えることを目的としています。同時に、事業者が当該要請に応じる際の困難を考慮する必要性も認識しており、「請求に応じないことを例外的に許容することとする。」と本大綱は記述しています。BSA は、個人が個人データを確実にコントロールできるようにするという目標を支持します。

これらの権利は、強固なデータ保護フレームワークのための強力な基礎となりますが、他方で、事業者と消費者の双方にとって意図しない結果を回避するため、当該権利については、請求の種類や生じるリスクに応じて、適切な制限を設けることが不可欠です。本大綱は、個人が請求を行うことができる特定の状況及びどのような例外的根拠に基づいて事業者が当該請求に合法的に応じないことができるかについて、残念

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

ながら、十分な詳細を記載していません。**この点、BSA は、特に、企業が請求に応じないことができる例外の根拠について貴委員会が重点的に検討されることを推奨します。**この場合の考慮事項は、利用停止の請求か又は削除請求かによっても異なる可能性があります。例えば、正当な法的又は事業目的があり、かつ、個人の請求に従うことが現実的でない又は通常の事業活動に著しく支障を及ぼす場合、事業者は、個人情報を保持する必要があり、個人の削除要請には応じないことがあり得ます。一定の個人情報を保持する必要がある場合として、例えば、個人情報の取扱に関するその後の本人からの問い合わせ、請求及び法的請求に対応する目的での保持があります。個人情報を保持しなければ、企業は当該請求に対応することに支障をきたします。同様に、詐欺、なりすまし又は犯罪行為の検出又は防止、データ保存要件等の法的義務の遵守、研究目的、セキュリティ確保、個人が要求する商品又はサービスの提供のために情報の処理が必要な場合等、企業が個人からの個人データ削除請求を拒否しなければならない他の重要な事由について、貴委員会にご理解いただきたいと思います。**よって、BSA は、適切な制限を規定する際に、貴委員会が、関連する全ての状況及び事例を考慮して十分な検討を行うことを求めます。**

さらに、関心を有するステークホルダーが、より的を絞った意見を貴委員会に提供するためには、個人情報保護法改正案、政令案、規則その他関連ガイドライン案の具体的文言を検討できることが重要です。

開示請求

個人情報保護法第 28 条は、本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができると規定しています。本大綱第 3 章第 1 節第 4 項(2)では、本人が、電磁的記録の提供を含め、保有個人データの開示方法を指示できるようにし、請求を受けた個人情報取扱事業者は、原則として、本人が指示した方法により開示するよう義務付けることが提案されています。

消費者は事業者から個人データの複製物を取得できるべきであることを私どもは認識しています。**この点、BSA は、消費者に開示される情報の範囲が、消費者が事業者に提供した情報又は消費者が作成した情報に限定されるべきである旨明確化することを貴委員会に推奨します。**

また、他のデータ主体に帰属する情報を開示することなく本人の保有個人データを提供することができない状況(例えば、情報がファイル又はデータベースの一部であり、それを変更することができない場合)があることにも留意が重要です。同様に、個人にデータへのアクセスを提供することは、企業が当該個人の身元を検証できない場合、セキュリティリスクを生みだす可能性があります。**貴委員会が、自らのデータにアクセスする権利を付与し又は明確化する際には、これら及び関連する要因を考慮されるようお願いします。**

さらに、本人に情報を提供するための適切な形式を決定するにあたっては、事業者が柔軟性を持つことができるようにすることを推奨します。電子的な保有個人データを開示するために最も適切かつ安全な方法は、個人データの量、開示を行う事業者の規模、業務、IT スキル、セキュリティへの考慮等によって、それぞれ異なるものです。結果として、形式に関する本人の指示を厳密に守ることは、必ずしも全ての個人にと

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

って有益であるとは限りません。従って、開示義務を遵守する方法は柔軟であるべきであり、新しいルールにおいても、特定の電磁的形式で本人に情報を提供することを義務付けるべきではありません。

第２節　事業者の守るべき責務の在り方

漏えい等報告及び本人通知の義務化

本大綱第３章第２節では、個人情報保護法改正により、一定数以上の個人データの漏えい、要配慮個人情報の漏えい等、一定の類型に該当する場合に限定して、漏えい等報告及び本人通知を義務化することが提案されています。

漏えい等報告における焦点は、本人に生じるリスクであるべきで、影響を受ける個人の数等、任意に指定される要素を焦点とすべきではありません。BSAの経験では、個人情報保護フレームワークは、原則に基づき、結果重視であり、過度に規範的ではない場合に最も効果的です。

この観点から、**暗号化又は無編集の個人データが不正取得され、これがなりすまし又は金融詐欺のような損害を生じさせる重大なリスクがある場合のみ、また、本人通知についてはそのリスクが高い場合にのみ、規制当局又は本人に対する漏えい等報告を事業者に義務付けることを推奨します。**このことから、データが暗号化されていて暗号鍵が安全に保管されている場合又は個人の権利若しくは自由にリスクがない漏えい等については、報告を義務付けるべきではありません。

この点に関して、現行の漏えい等報告に関するガイドラインである「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第１号）[4]では、実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合には報告を不要としており、正しいアプローチが採用されています。よって、BSAは、漏えい等報告に関する当該立場は維持されるよう貴委員会に求めます。

漏えい等報告が確実に意味あるものとすることが重要であるため、漏えい等報告を行う前に、事業者が、セキュリティリスクの範囲を見極めて、更なる漏えい等を防止するための徹底的なリスク評価を実施するのに十分な時間を与えることが重要です。この点に関して、漏えい等報告について明確な期限を設定しないという本大綱の提案を支持します。そして、BSAは、事業者が実際の漏えい等を確認した後「実行可能な限り速やかに」報告する（ここで、報告とは、速報及び確報（確報は、速報後の事実関係又は状況に関してアップデートを行うものとすべき）の双方を含む）ことを要件とするよう推奨します。

最後に、例えば、事業者が漏えい等の影響を受けた個人の連絡先情報を有していない等、関係する個人への通知が困難である場合について、貴委員会で通知の代替手段を検討していただくとともに、漏えい等の公表の義務を課すことのないよう要望します。例えば、ある状況においては、事業者が漏えい等の影響を受けた本人に直接連絡を行うよりも貴委員会に報告する方が適している場合があり、これにより漏えい等の公表により生じるセキュリティリスクを回避し得ます。

[4] https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

第３節　事業者における自主的な取組を促す仕組みの在り方

PIA (Privacy Impact Assessment)

本大綱第３章第３節第２(2)項では、PIA (Privacy Impact Assessment) の利用を含む、プライバシー及び個人情報保護を強化するための業界のベストプラクティスを収集することに関する貴委員会の関心が記載されています。前回意見書で述べたように、EU の GDPR によって義務付けられた DPIA(Data Protection Impacts Assessment)[5]と同等の評価は、データ処理対象である個人の権利及び自由に対するデータ処理の潜在的な影響とデータ処理の利点を事業者が比較考量することを支援します。このような評価により、事業者は、個人のプライバシー及びデータ処理の有効性、公平性、安全性及びセキュリティを確保する方法で、人工知能等データ駆動型技術を進歩させるために必要なデータの量及び種類を調整し目標を定めることができます。よって、BSA は、PIA 又は DPIA に関する情報を更に収集し、リスク評価のための事業者の努力を促進するという貴委員会の取組を歓迎します。今後、この点に関して貴委員会を支援する機会をいただければ幸いです。

第５節　ペナルティの在り方

本大綱第3章第5節では、刑罰の大幅な引き上げを含め、事業者に対する罰則をより厳しくすることを提案しています。この点に関して、BSAは、個人情報保護法違反に対する救済及び罰則は、当該違反から生じる損害に対し、効果的かつ比例的なものとなるよう規定されることが重要と考えます。本大綱が述べるとおり、自らの行為が個人情報保護法に違反している可能性があると貴委員会から指導等された企業の大半は、自らの行為を是正しています。このことからすれば、貴委員会は、罰則を科す前に、貴委員会の指導、勧告又は命令に対応する措置を事業者が実施するための適切な期間を引き続き与えることを重視すべきであると考えます。罰則は、事業者が適時に適切な措置をとらない場合にのみ適用されるべきです。

罰則を課す場合、個人が蒙った経済的損害を補償するための金銭的救済を提供すること及び将来の違反を防止するために各々の事情に即した行動に関する措置を課すこと等が適切な方法です。これに対し、刑罰は、データ保護法違反に対する比例的な救済とは言えず、かつ、データ保護法執行において有効な役割を果たすものではありません。BSAの見解では、データ保護法の実体的要件として、金銭的救済及び行政又は民事手続を通じて提供される行動に関する措置を定めれば、個人のプライバシーの利益を保護するのに十分です。私どもは、現行の個人情報保護法が刑罰を規定していることを認識していますが、刑罰はデータ保護法違反に対する比例的な救済ではないため、これらは科されるべきではないことを強調しておきたいと思います。実際、例え特定の場合に限定されているとしても、刑事責任のおそれとリスクがあることによって、有益でありながら害のないデータ慣行を用いた試みをも思いとどまらせてしまいます。

第６節　法の域外適用の在り方及び国際的制度調和への取組と越境移転の在り方

[5] GDPR35条(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679)を参照下さい。

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

域外適用の範囲の拡大

本大綱第 3 章第 6 節では、外国事業者に対する貴委員会の報告徴収権を認めることを含め、個人情報保護法の域外適用の範囲を拡大することを提案しています。本大綱は、また、外国事業者を命令の対象とし、これに対する立入検査を可能とし、事業者が命令に従わなかった場合には、その旨貴委員会が公表することを認める旨提案しています。

前回意見書で述べたとおり、法の地域的な適用範囲に関して、データ保護フレームワークは、(1) 明確に居住者を対象とし、(2) 処理対象である個人データが、収集時に国内に所在するデータ主体から意図的に収集されたものであって、かつ(3) 現実かつ実効的な活動を行うことを可能にする安定した仕組みに基づいて国内に設立された組織が収集している場合の行為のみを規制すべきであると BSA は提唱しています。日本における個人情報保護の実効性、外国の主権との関係、他国が独自の法律を日本企業に対して課して執行を行い日本企業の事業活動に制限がかけられるリスク、企業が二か国以上の異なる法律の遵守を命じられて国際的に大きな混乱を生じるリスクを鑑みれば、現行の域外適用の範囲を超えてこれを拡大すべきでなはいと考えます。むしろ、貴委員会には、引き続き、国際的な個人情報保護制度の調和及び相互運用性並びに関連する国際的執行機関間での協力を促進していただけるようお願いします。

BSA は、以上の理由から、法の域外適用の拡大を支持しませんが、この点に関して何らかの措置を検討する場合には、外国事業者が追加的な義務の遵守を求められる前に、適正手続について十分に検討されることが重要です。**BSA は、個人情報保護法改正案の文言を検討した際に、貴委員会に対してより具体的な提言を行う機会をいただきたいと考えております。**

外国にある第三者への個人データの提供制限の強化

本大綱は、移転元となる個人情報取扱事業者が、移転先国の名称及び当該国における個人情報保護に関する制度の有無を含む、外国に所在する移転先事業者における個人情報の取扱いに関する情報を本人に提供しなければならない旨の提案をしています。

しかしながら、本人の個人情報取扱に関する理解を深めるという貴委員会の目標は、これらの措置によっては達成することはできないと私どもは考えます。個人情報保護の実効性は、データが保管され処理される物理的な場所とはほとんど関係がありません。むしろ、データセキュリティ及び個人情報保護は、強固なセキュリティ対策及びデータ移転に関する事業者のアカウンタビリティを含む、個人情報取扱事業者が実施する技術、システム及び手順の品質に依存します。一例として、企業が EU 外の国に本社を置く場合であっても、データ又はデータ処理の場所にかかわらず、処理する全てのデータに EU のデータ保護法を適用することを選択している可能性があります。従って、企業がどのように個人情報を保護しているのかが重要な要素であることを各個人が理解し、個人情報を国内で取扱う場合に比して海外に所在する移転先事業者による取扱にはより高いセキュリティリスクがあると誤解が生じないよう、貴委員会が教育指導していかれることを要請します。

また、本人への情報提供に関するルールは、規範的なものではなく、かつ、事業者に不必要な負担をかけることなく事業者の透明性やアカウンタビリティを促進するた

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office

め、十分な柔軟性を事業者に認めるべきです。このアプローチは消費者にも利益をもたらします。もし、事業者が、データを処理する新規のベンダーを新規の国で採用する毎に、個人に通知しなければならないとされた場合、個人のプライバシーの利益の向上に資することのない無数の通知を個人に送付することになってしまう可能性があります。たった１つの観点について本人への詳細な通知を要求することは、本人のプライバシーの権利に重要な影響を及ぼす通知に集中することを妨げ、それによってプライバシー関連の他の通知の有効性を低下させてしまう可能性があります。

さらに、円滑な越境データ移転の確保は、デジタルエコノミー時代のイノベーションの前提条件です。日本政府は、安倍首相が掲げる DFFT(データ・フリー・フロー・ウィズ・トラスト)のビジョンの実現に向けて努力しているところであり、また、全産業分野の企業が、円滑な越境データ移転に大きく依拠しています。よって、BSA は、貴委員会及び日本政府が、世界的に越境データ移転を促進する仕組みを推進することによって、国際的にリーダーシップを発揮し続けることを希望します。

結び

BSA は、本大綱に関する意見を提出する機会に感謝します。本意見が、今後の個人情報保護法改正及び関連規則等の検討に有用であれば幸いです。また、BSA は、個人情報保護法改正案の具体的な文言に関し、国会提出前に、BSA 及び他の産業界代表者を含む関心を有するステークホルダーと協議いただけるよう要望します。ご質問がある場合又はより詳細について議論をされたい場合には是非ご連絡下さい。

以　上

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043
P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org
Japan Representative Office