Auth0

個人情報保護法（APPI）改正に備える

注意：本ホワイトペーパーは法律上の助言ではないため、法的な目的で使用することはできません。この文書に記載されている問題について、独立した法的助言が必要な場合は、適切な資格を持つ法律専門家に依頼することをお勧めします。

はじめに

2020 年 6 月 5 日、日本の個人情報の保護に関する法律である個人情報保護法（APPI）の一部を改正する法律が成立しました。これらの改正は、APPI の「3 年ごと」の見直し方針に沿って国会で可決されましたが、既存の個人情報保護法を微調整するのみの内容ではありませんでした。

2020 年の改正では、日本住民の個人情報の透明性と安全性を確保するために企業の義務を強化することにより、APPI にいくつかの面で重要な変更を加えています。また、より厳格な刑事罰や罰金により、コンプライアンス違反に対する罰則が強化されています。

日本の個人情報保護法が大幅な改正を必要とする理由

2020 年の APPI 改正は、次のような理由により行われました。

- 情報通信技術の急速な進歩に適応するために、現行の APPI を更新する必要性。
- データ主体の権利を強化するために、現行の APPI を更新する必要性。
- データ保護規制の世界的傾向を考慮し、データ保護の世界基準に合わせる必要性。
- これまで存在しなかった個人情報の新しい取り扱い方法に対応する必要性。

2020 年の APPI 改正の内容は、注目を集めた一連のデータ侵害とプライバシーインシデントの影響を受けています。例を挙げると、企業と大学生の双方向けの採用情報関連のオンラインサービスを提供する株式会社リクルートキャリア（およびその親会社である株式会社リクルートホールディングス）は、各学生の内定辞退率を算出するための行動分析を実施しました。この組織は、これらの学生の同意を得ずに、その情報を他の企業に提供しました。このとき、この組織は、提供を受けた企業が特定の情報を使用して個々の学生を識別できることを認識していました。株式会社リクルートキャリアのプライバシーポリシーでは、収集した個人情報を使用して行動分析を実施したり、内定辞退率に関する情報を第三者に提供したりすることが明示されていませんでした。

2020 年の APPI 改正は、単なる形式的な手続きの増加や現状維持ではないと理解することが重要です。この改定は、企業の機密データや占有データをリスクにさらす可能性のある、日本のサイバーセキュリティ文化の深刻な欠点を是正する機会なのです。

APPI 改正の大部分は 2022 年春までに正式に施行される見込みはありませんが、この施行日は変更される可能性があります。日本で事業を展開している場合は、今すぐに改正内容を理解し、自社の事業がコンプライアンスに準拠していることを確認する必要があります。

このホワイトペーパーは、2020 年の APPI 改正に備えた教育の開始を支援することを目的としています。このホワイトペーパーを読むことで、更新された APPI が誰に適用されるのか、個人データの定義がどのようなものなのか、コンプライアンス違反に対する罰則など、いくつかの基本事項を確認できます。2020 年の APPI 改正によって、どのようにデータ主体の権利が強化され、企業に対する新たな義務が生じ、個人データの転送に関する新しい規則が確立されるのかについて理解できます。また、御社がすでに他のプライバシー法に準拠している場合の潜在的なギャップや、事業の準備を開始する際に考慮すべき措置についても紹介します。このホワイトペーパーに記載されている情報を法律上の助言として解釈または依拠することはできません。法律上の助言については、資格のあるプライバシー専門の弁護士に相談する必要があります。

基礎知識

更新された APPI の適用対象であるかどうか

原則として、営利非営利に関係なく、日本居住者の個人情報を取り扱ういかなる事業者（「取扱者」）に対しても、本社の所在地に関係なく本法律が適用されます。現行の APPI は、日本居住者への商品またはサービスの提供に関連してその個人のデータを取得して外国で処理する日本以外の事業者に適用されます。ただし、特定の規定により適用対象外、または法的強制力がないと見なされる日本以外の事業者を除きます。報道関係者、職業的作家、学者、宗教団体、政党を対象とする限定的な例外があります。法律のこの箇所は、旧版から大きな変更はありません。

現行版の APPI では、日本政府は日本以外の事業者が関与する案件を日本以外の事業者の規制当局に報告することができます。2020 年の改正ではその法的強制力が拡大され、日本のデータ保護官庁である PPC（個人情報保護委員会）は外国の事業者に文書および報告書の提出を要求し、外国の規制当局とともに施設に立ち入り、実施、および監査をすることが可能です。

APPI による個人データの定義

2017 年の改正以降、APPI に基づく個人情報および個人データの定義は変更されていません。個人情報とは、生存する個人の身元を推定できるあらゆる情報と定義されます。このような情報には、生体認証マーカーと正式な ID 番号が含まれます。EU の「一般データ保護規則（GDPR）と同様に、人種、宗教、犯罪歴、病歴などの「機密性の高い個人情報」という特別なカテゴリもあります。2020 年の改正法では、保有個人データには、取扱者が取得した日から 6 ヵ月以内に削除される予定の個人データも含まれます。これは現行法では除外されています。

2020 年の改正では他のデータと組み合わせた場合にのみ個人を識別できる仮名加工情報という概念が導入される点に留意が重要です。国際プライバシー専門家協会（IAPP）によると、仮名加工情報は、個人データの開示および使用停止の要件を含む、APPI の該当箇所から除外されています。仮名加工情報は取扱者による内部使用に限定されているため、データ主体の同意またはオプトアウト手順によって第三者と共有することは許可されません。

コンプライアンス違反に対する罰則

現行の APPI は違反に対する罰金と罰則を定めていますが、2020 年の改正により、これらの罰金と罰則が大幅に引き上げられます。改正 APPI では、PPC の措置命令に違反した当事者は、1 年以下の懲役刑または 100 万円（およそ 9,500 ドル）以下の罰金、および当事者が法人の場合は最大 1 億円（およそ 950,000 ドル）までの罰金が科される可能性があることを規定しています。さらに、2020 年の改正により、命令に違反した取扱者の名前を PPC が公開できるようになりました。

事業者または従業員が違法な営利目的で個人情報を使用した場合、これは違法行為と見なされ、1 年以下の懲役刑または 50 万円（およそ 5,000 ドル）以下の罰金、当事者が法人の場合は 1 億円以下（およそ 950,000 ドル）以下の罰金を科される可能性があります。個人は、プライバシーの損失に関連した損害賠償の訴訟を提起することもできます。これにより、事業者に多大な財務的影響が生じる可能性があります。

実際には、PPC は通常、申し立てに対する初期調査の実施手順に従い、その後に違反を是正するための推奨を行います。PPC は、このプロセスの後に行動を是正しなかった取扱者に対して法的措置を講じることができます。

個人の権利の拡大、新たな事業上の義務

個人の権利の拡大

2020 年の APPI 改正の中心をなすのは、個人による個人情報の管理の拡大です。データ主体は、自身の個人データへのアクセスが拡大し、個人データの使用の中止と消去を要求できるようになりました。

削除または使用停止の権利の拡大

2020 年の APPI 改正により、削除または使用停止に関するデータ主体の権利が拡大されます。法律に基づき、データ主体は、「保有個人データを個人情報取扱事業者が利用する必要がなくなった場合」、「データの漏洩があった場合」、または「保有個人データの取り扱いにより主体の権利または正当な利益が害されるおそれがある場合」に、データの消去を要求できるようになります。

被害の可能性がある場合にデータ主体が消去を要求できるようにすることは、以前の規定とは対照的です。以前の規定では、個人データが不正に処理または取得された場合のみ削除が許可されていました。また、現在の APPI では、取得日から 6 ヵ月以内に消去される予定のデータは消去の権利から除外されていました。新版では、この 6 ヵ月の例外が削除されています。

データのコピーを要求する権利

現行の APPI では、情報提供者と受領者の双方が、受領者へのデータ転送に関する記録を保持する必要があります。しかし、個人情報が共有されているデータ主体に対するこれらの記録の開示に関する文言はありません。2020 年の改訂では、この文言が追加され、データ主体がこれらの記録を要求できるようになりました。また、改正 APPI は、データ主体が個人データの電子コピーを要求する権利を有することを明確にしています（一方、現行の文章では、基本的に取扱者が文書を提供し、電子コピーを提供する場合はデータ主体の同意が必要です）。データ主体は、取扱者が保持する個人データを電子形式で提供することを要求できます。

企業に対する要件の追加

2020 年の APPI 改正には、企業に対する新しい義務も含まれています。この義務により、特定のデータ侵害を報告し、さらにプライバシーポリシーを開示することが求められます。2020 年の APPI 改正では、個人データの違法または不適切な使用も禁止しています。

データ漏洩の報告義務

データ漏洩の報告義務が含まれていなかった古い APPI ガイドラインとは異なり、改正された法律では、取扱者が特定の「漏洩、損失、または損害」を PPC に報告する必要があります。これらの報告要件の基準値は、APPI に関する法令で今後規定されます。ただし、データ主体にデータが漏洩したことを通知する場合の要件の規定は現時点では明確ではありません。改正法では、この要件は「主体に情報を提供することが困難な場合や、主体の権利と利益を保護するために必要な代替措置が講じられた場合」には適用されないと規定されています。

追加のプライバシーポリシーの開示およびオプトアウトの申請（該当する場合）

さらに、改正 APPI では、取扱者が法人である場合、個人情報取扱事業者は、住所および代表取締役の氏名を開示することが求められています。また、オプトアウト手続きによる情報提供や、個人情報の共同使用を行う場合には、追加情報を開示する必要があります。

個人データの違法または不適切な使用の禁止

現行法では、取扱者は詐欺などの不正な手段により取得された個人情報を取り扱うことを禁止されています。2020 年の改正では、この文言に加えて、取扱者が「違法行為や不正行為を教唆または誘発する可能性」がある方法で個人データを使用できないことが規定されました。

個人データの転送の取り扱い

2020 年の改正には、第三者への転送または国境を越えて転送される個人情報に関するより強力な制限が含まれています。

「個人関連データ」の第三者への転送

注目すべき規定の 1 つに、「個人関連データ」の第三者への転送に重点を置いたものがあります。「個人関連データ」は、開示当事者がそのデータを使用して特定の個人を識別することができないため、個人データではありません。ただし、個人関連データは、受領者が他の情報と組み合わせることによって第三者が個人を識別するのに役立つ可能性があります。このような場合に、開示当事者は、第三者が当事者から事前に同意を得ていることを確認する必要があります。

「個人関連データ」の一例としては、ターゲティング広告に使用される第三者の Cookie が挙げられます。Data Guidance社は、「第三者へのオンライン識別子（Cookie など）の提供に同意が必要となるため、この改正はターゲティング広告やその他の広告技術に影響を及ぼす可能性がある」としています。Data Guidance社はこの改正は実務に大きな影響を及ぼすものと予測していますが、同時に、Cookie の使用に関する同意はすでに GDPR の要件であるため、GDPR に準拠している企業にとっては大きな負担にはならないだろうとも述べています

国境を越えた個人データの転送

もう 1 つのデータ転送規定は、国境を越えたデータ転送に関連するものです。現行の APPI では、日本国外でデータを共有する取扱者は、データ主体の同意を得る必要があります。取扱者が事前に同意を得ていない場合（例えば、第三者への転送ではない場合など）、データの受領者が APPI と同等のデータ保護基準を規定しているか、または同等の基準を持つ国にあることを確認する必要があります。現時点では、これが適用される外国は、欧州経済地域（EEA）および英国のみです。

2020 年の改正では、この立場に一部変更が加えられています。この変更により、同意を得る際に個人と共有する必要のある特定の情報が規定されています（具体的な詳細はまだ公表されていません）。この改正では、同等のデータ保護基準を規定しているその他の事業者と個人データを共有する場合に、取扱者はその保護基準を維持する必要があることも規定しています。

プライバシーポリシーを更新した企業にとっての潜在的なギャップ

企業で EU の一般データ保護規則（GDPR）またはカリフォルニア州消費者プライバシー法（CCPA）に準拠するためにプライバシーポリシーをすでに更新している場合でも、いくつかのギャップが存在する可能性があります。対処が必要となる可能性があるギャップは次のとおりです。

データ主体の同意なしでのグループ会社内のデータ共有

GDPR では、正当な利益に関連する目的で個人データの処理が必要な場合に、グループ会社間で個人データを共有するためにデータ主体の同意は必要としません。 一方、 APPI（現行および改正）には、法律で許可されていない限り、個人データを他の団体（グループ会社を含む）と共有するために、データ主体の事前同意が必要であるという基本的な規則が含まれています。 グループ会社内でのデータ共有の主な構造の 1 つに、「共同利用」構造があります。この構造の下で、事業者は、プライバシーポリシーにそのような情報を明記することにより、APPI に規定された特定の情報を事前にデータ主体に通知する必要があります。

国境を越えたデータ転送

GDPR において、個人データは適切な保護を提供する国にのみ転送することができます。または、個人データは、拘束力のある企業の規則、承認済みモデル条項、および承認済みの行動規範または承認済みの証明書と合わせて拘束力のある契約によって保護されます。これとは対照的に、現行の APPI では、基本的な規則として、次の要件のいずれかが満たされていない限り、データ転送時に国際データ転送に関するデータ主体の事前の同意が必要です。（a）個人データが EEA または英国の事業体に転送される、または（b）受領者が APPI および関連する規制で指定された個人データを保護するための十分な予防措置を講じるように契約が締結されている、または企業規則が確立されていること。2020 年の APPI 改正では、これらの要件がさらに強化され、共有する場合に個人の同意を得なければならない情報が拡大されるとともに、データを共有する企業における保護基準の維持を確認することが必要となります。

「個人関連データ」の転送

改正 APPI では、「個人関連データ」という概念が導入されています。これは、GDPR や CCPA にはない概念です。「個人関連データ」とは、個人的なことに関連しているが、個人情報、仮名化された個人情報、または匿名化された個人情報の定義には該当しない情報です。PPC は、このカテゴリに含まれる内容に関するガイドラインを発行する場合がありますが、一般的に、Cookie や IP アドレスなどのデータがこの定義に該当することが認められています。2020 年の改正では、個人関連データを扱う事業体は、個人関連データを第三者に転送する場合に、そのデータを第三者が所有する他の情報と組み合わせることで個人を特定できるときは、

影響を受ける個人の事前の同意をその第三者が得ていることを確認しなければならないと規定しています。

準備において考慮すべき措置

多数の国際的なデータプライバシー規則と同様に、APPI の規定においても、ベストプラクティスについて具体的な提案はあまり行われていません。ただし、PPC は、適切なセキュリティ対策に関するガイドラインを発表しています。このガイドラインの多くは GDPR に準拠した企業にとっては既知のものであり、基本的なデータ管理から始まる内容です。ここでも、以下の内容は法律上の助言を意図するものではないことに留意してください。個人データの提供に関する具体的な推奨事項については、貴社の顧問弁護士にご確認ください。

データ保護オフィサーの任命

APPI の改正に関する議論では、更新された APPI が、GDPR の要件に従ってデータ保護オフィサー（DPO）を任命するように業務担当者に要求する必要があるかどうかを国会議員が検討しました。しかし、最終的な改正法にこの要件は含まれていませんでした。

それでも、事業者（特に、機密性の高い個人情報を取り扱い、国境を越えたデータ転送を行う多国籍企業）は、APPI に必要なデータ安全対策を遵守するために DPO を任命することをお勧めします。データ保護オフィサーは、ガイドラインの進化に合わせてプライバシーポリシーを定期的に確認するなど、コンプライアンスを維持するための適切な対策を講じるのに役立ちます。

レガシーシステムのアップデート

*エコノミスト*誌によると、日本はサイバーセキュリティに関して「他の先進諸国に遅れをとっている」といいます。中小規模の日本企業の多くは最低限のセキュリティしか備えておらず、さらに多くの企業は脆弱なレガシー技術を使用しています。実際、

> **2020年1月にマイクロソフトがWindows 7 のセキュリティパッチの提供を停止した際に、それ以降も約 1400 万人が（そのうち 750 万人が職場で）Windows 7 を使用していた**

と、*エコノミスト*誌は報告しています。

サポートが停止され、セキュリティ更新プログラムが提供されなくなるため、セキュリティの低下はレガシーシステムに関する大きな懸念事項です。さらに、レガシーシステムによって

データの紛失や盗難の問題が複雑になるため、顧客の個人情報を保護することが困難になります。ある調査によると、日本企業の 45% が、セキュリティ上の懸念事項の 1 位であるサイバー犯罪者、パートナー、サイバーテロリストによるデータ漏洩を経験していると回答しています。

日本では、脆弱なレガシーテクノロジーが普及しているため、社内システムを綿密に調べることが重要です。そうしないと、高額な訴訟につながる可能性があります。例えば、ベネッセの場合、管理者が新しい Android スマートフォンへのデータ転送防止手順を更新していなかったことが同社の過失とみなされました。小さな見落としが、深刻な結果につながります。

また、最新の暗号化規格を活用すれば、企業は法的義務の一部から解放されます。現行のガイドラインでは、漏洩したデータの暗号化が「ハイレベル」であれば、取扱者は PPC に漏洩を通知する必要はありません。

プライバシーポリシーの改訂

確認すべきもう 1 つの点は自社の内部ポリシーです。改正 APPI に準拠するように内部規則およびマニュアルを改訂してください。また、個人データや個人関連データを他の事業者と共有するために必要な通知、開示、契約、その他の手段を更新することも検討してください。更新した文言が明確で読みやすいことを確認し、御社の Web サイトにプライバシーポリシーを必ず掲載していください。

アクセス制御の確認

APPI では、取扱者が「個人データのセキュリティ制御に必要かつ適切な措置」を講じる必要があります。また、高度な従業員 ID およびアクセス管理（IAM）システムを使用すると、機密データにアクセスするユーザーに権限を割り当てるのに役立ちます。適切な従業員の IAM ソリューションは、ポリシーやユーザーの役割に従ってユーザーの認証、承認、評価を行うのに役立ち、規制コンプライアンスへの準拠を容易にします。
さらに、変更不可能なアクセス記録が作成されるため、漏洩が発生しても損害を限定できます。

個人情報データベースにアクセスするために現在必要なものがシンプルなユーザー名とパスワードの組み合わせだけであれば、従業員の IAM を優先する必要があります。

IAM への最新のアプローチが企業データの保護とデータ保護法の遵守にどのように役立つかについては、弊社までお問い合わせください。

結論

2020 年の APPI 改正は大きな変更であり、日本でビジネスをする組織に大きな影響を与えることが予想されます。今後の変更に対応する準備が整っていない場合は、今から始めましょう。改正法について理解し、個人情報の使用状況を調査し、組織に適切なセキュリティ保護が適用されていることを確認するために必要な法的助言を得てください。

ID管理がどのように APPI コンプライアンス計画の一部になり得るのかについては、弊社までお問い合わせください。（お問い合わせ先：auth0-japan@auth0.com）

Auth0

Auth0（オースゼロ）は、9,000社以上の導入実績を誇る認証認可プラットフォームを提供しています。複雑で開発者の負荷が高い認証機能の実装をAuth0に任せることで開発者体験（DX）を向上、企業のデジタルトランスフォーメーション（DX）を推進します。Auth0を使い、90%以上のお客様が安全で拡張性の高い認証システムを1週間以内に実装しています。