2021.12.06

サイバーセキュリティニュース ＜2021 No.002＞

令和２年個人情報保護法の改正について

【要旨】
■ 2020 年（令和 2 年）6 月 12 日に改正法が公布された「個人情報の保護に関する法律等の一部を改正する法律」（以下、「個人情報保護法」）が、2022 年 4 月 1 日に完全施行される。
■ 改正法は本人の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の視点を反映させたものである。
■ 本レポートでは、令和 2 年改正法の概要とポイントを整理するとともに、企業が果たすべき「プライバシーの保護」について解説する。

１．個人情報保護法の施行と令和２年改正の背景

「個人情報保護法」は、2003 年（平成 15 年）に個人の権利・利益の保護と個人情報の有用性とのバランスを図ることを目的に施行された。

同法施行後の情報通信技術の発展に伴って、制定当時には想定されなかった個人データの利活用への対応が課題となり、同法施行後初の改正法が 2015 年（平成 27 年）に公布され、2017 年（平成 29 年）に全面施行された。また、今後の国際的動向、情報通信技術の進展、新産業の創出・発展の状況を踏まえて、同法は「いわゆる 3 年ごと見直し」をする旨の規定が盛り込まれた。

この「いわゆる 3 年ごと見直し」規定に基づく最初の法改正が 2020 年（令和 2 年）6 月 12 日に公布、2022（令和 4 年）年 4 月 1 日に全面施行される（以下、「令和 2 年改正法」）。個人情報保護委員会が、本人の個人情報に対する意識の高まり、技術革新を踏まえた保護と利活用のバランス、越境データの流通増大に伴う新たなリスクへの対応等の観点に基づいて関係団体・有識者からのヒアリング等を行い、実態把握や論点整理等を実施、令和 2 年改正法はこれらの視点を反映させたものである。

令和 2 年改正法の概要とポイントは以下の 6 つに分かれ、以降にて解説する。

（１）個人の権利のあり方	① 短期保有データの開示等対象化 ② 保有個人データの開示方法の本人指定 ③ 第三者提供記録の開示 ④ 利用停止・消去等の請求権の要件緩和 ⑤ オプトアウト規定の強化
（２）事業者の守るべき責務のあり方	① 漏えい等報告・本人通知の義務化 ② 不適正な方法による利用の禁止
（３）事業者による自主的な取組を促す仕組みのあり方	① 認定個人情報保護団体制度の改正
（４）データ利活用に関する施策のあり方	① 「仮名（かめい）加工情報」の創設 ② 提供先において個人データとなる情報の取扱い
（５）ペナルティのあり方	① 法令違反に対する罰則の強化
（６）法の域外適用・越境移転のあり方	① 外国事業者に対する報告徴収・命令 ② 外国にある第三者へ個人データを提供する際の本人への情報提供の充実

【表 1】令和 2 年改正法の概要

2．令和２年改正法の概要とポイント

（１）個人の権利のあり方（本人の権利保護の強化）

① 短期保有データの開示等対象化

6 か月以内に消去されるデータ（短期保有データ）は、これまで「保有個人データ」の対象外であり、本人からの開示・利用停止等の対象ではなかった。しかし、短期間に消去されるデータであっても、消去されるまでの間に漏えいが発生すれば、データが拡散し、本人が重大な損害を被る可能性が指摘されていた。

令和 2 年改正法では、6 か月以内に消去される短期保有データについても「保有個人データ」に含まれることになり、本人からの開示・利用停止等の対象になった。

すなわち、1 日で消去されるものであっても、検索できるように体系的に構成されている「個人情報データベース等」を構成する「保有個人データ」に該当する場合は、開示請求の対象となり得るため、短期保有データを別管理している事業者は、保有個人データと同じ扱いとし、本人から開示・利用停止等の請求があったときに対応できるようにしておく必要がある。

もっとも、これまで短期間で消去していた個人データについて、開示等の請求等に応じるためだけに保存する必要はなく、利用する必要がなくなった個人データは遅滞なく消去するよう努める必要がある。

	保有個人データ	個人データ	個人情報
利用目的の特定・通知等	○	○	○
目的外利用の禁止	○	○	○
適正な取得	○	○	○
安全管理措置	○	○	
第三者提供の制限	○	○	
事業者名などの公表	○		
本人からの開示請求など	○		

令和2年改正法では、6か月以内に消去される短期保有データも「保有個人データ」に

【表 2】求められる事項と規制の範囲

② 保有個人データの開示方法の本人指定

本人から事業者へ保有個人データの開示請求があった場合、これまでは原則書面による交付とされていたが、情報量が膨大であったり、保有個人データが動画や音声のように、そもそも書面による交付に適さないケースもあった。

令和 2 年改正法では本人の利便性向上の観点から、電磁的記録の提供による方法など、本人が開示方法を指定できることになった。電磁的記録の提供による方法の事例として、

・電磁的記録を CD-ROM 等の媒体に保存して、当該媒体を郵送する
・電磁的記録を電子メールに添付して送信する
・会員専用サイト等のウェブサイト上で電磁的記録をダウンロードしてもらう

が挙げられる。事業者は、電磁的記録による開示への準備として、社内に保有されている 個人データがどこに・どのように保管されているのか、個人データの検索は効率的にできるか、個人データは電磁的記録として本人へ開示できる状態にあるか、などを確認する必要がある。

なお、電磁的記録の提供に対応するためには大規模なシステム改修を行わなければならず多額の費用が発生して困難な場合は、本人に遅滞なくその旨を通知したうえで書面の交付による開示することが認められる。

③ 第三者提供記録の開示

従来から個人データの授受に係る第三者提供記録を作成することが求められていたが、この記録は本人による開示請求の対象ではなかった。令和 2 年改正法では、本人から事業者へ第三者提供記録の開示請求ができるようになった。

第三者提供記録の開示請求ができることによって、不正な手段によって取得された個人情報が流通することの防止、また個人情報の流通に係るトレーサビリティの確保などが期待される。事業者は、台帳に「情報の入手元」「情報の提供先」の欄を作成するなど、自社の第三者提供記録を見直し、本人からの開示請求に対応できる態勢を準備する必要がある。

④ 利用停止・消去等の請求権の要件緩和

本人が自己の個人情報について利用停止や消去などを求める場合、これまでは事業者が個人情報を目的外で利用したり不正取得したりするなど、一部の法違反がある場合に限られていた。

令和 2 年改正法では、法違反がある場合に限定せず以下のケースにおいても利用停止・消去・第三者提供の停止を請求できるようになった。

・保有個人データを事業者が利用する必要がなくなった場合
・個人データ漏えいにかかる報告義務が生じる場合
・本人の権利又は不正な利益が害されるおそれがある場合

なお、消費者等、本人の権利利益保護の観点からは、事業活動の特性、規模及び実態を考慮して、保有個人データについて本人から求めがあった場合には、自主的に利用停止等又は第三者提供の停止に応じる等、本人からの求めにより一層対応していくことが望ましい。

⑤ オプトアウト規定の強化

これまでは、オプトアウト[1]により第三者提供できる個人データから「要配慮個人情報 [2]」のみが除外されていたが、令和 2 年改正法では要配慮個人情報に加えて、「不正な手段により取得された個人情報」ならびに「他の事業者がオプトアウトの規定に基づき取得した個人データ」についても、オプトアウトによる第三者提供ができなった。

（２）事業者の守るべき責務のあり方（事業者の責務の追加）

① 漏えい等報告・本人通知の義務化

個人情報が漏えいし、被害者本人の権利利益を害するおそれが大きい場合は、事業者はその旨を個人情報保護委員会に報告ならびに情報漏えい対象の本人へ通知することが義務化された。これまでは、「努力義務」とされ、漏えいを発生させた企業の個別対応に委ねられていたが、近年の諸外国の標準的な対応に追随することとなったといえよう。

「個人情報の保護に関する法律施行規則」では、報告および通知の対象となる事態として、以下の 4 つを挙げている。

A：「要配慮個人情報」が含まれるデータの漏えい、または発生したおそれ
B：不正に利用されることより財産的被害が生じるおそれがある個人データの漏えい、または発生したおそれ

---

[1] オプトアウト
個人情報の第三者提供に関して、その行為を本人の求めに応じて停止すること。関連する表現として、「オプトイン」は個人情報の提供について本人が肯定的な承認をすることをいう。

[2] 要配慮個人情報
人種、信条、社会的身分、病歴、前科、犯罪被害情報、その他本人に対する不当な差別、偏見が生じないよう特に配慮を要するものとして政令で定めるものをいう。

C：不正の目的をもって行われたおそれがある個人データの漏えい
D：本人の数が 1,000 を超える個人データの漏えい
※A，B，Cは漏えい件数を問わない。

個人情報漏えいが確定した事案だけでなく、「おそれが大きい」事案についても報告および通知の対象となることに留意されたい。「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。すなわち、その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。

漏えい事案を知った事業者は、「速報」と「確報」の二段階で報告をする必要がある。

「速報」とは、漏えい事案を知ってから「速やか（概ね３～５日以内）」にその時点で把握している以下事項を報告する。

・概要（発生日、発覚日、発生事案、発見者、報告対象事案の該当性、委託元及び委託先の有無、事実経過等）
・漏えい等が発生し、又は発生したおそれがある個人データの項目
・漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
・原因
・二次被害又はそのおそれの有無及びその内容
・本人への対応の実施状況
・公表の実施状況
・再発防止のための措置
・その他参考となる事項

その後 30 日以内（不正の目的によるおそれがある漏えい等の場合は 60 日以内）に「確報」として報告する。「確報」では、報告が求められる事項について基本的に全て報告をする必要があるが、不正アクセスよる漏えい等については専門的な調査が必要であり、留意されたい。

② 不適正な方法による利用の禁止

これまでは、個人情報の不適正な利用の禁止、つまり、違法・不当な行為を助長・誘発するおそれがある方法により個人情報を利用することが明文で禁止されていなかったが、事業者が不適正な方法で個人情報を利用することが明文で禁止された。

（３）事業者による自主的な取組を促す仕組みのあり方

①　「認定個人情報保護団体制度」の改正

これまでの認定団体制度は、対象事業者の全ての分野における個人情報の取扱いを対象とする団体に対して認定を行う制度だったが、これを特定の範囲に限定した個人情報の取扱いを対象とする団体を認定することができるようになった。

（４）データ利活用に関する施策のあり方（データ利活用の促進）

①「仮名（かめい）加工情報」の創設

令和２年改正法において、「個人情報」と「匿名加工情報」の中間的な制度として、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工した個人に関する情報である「仮名加工情報」が創設された。その加工基準について、以下・表 3 にて匿名加工情報との差異を比較しつつ示す。

仮名加工情報は、匿名加工情報と比較して加工基準が緩やかである一方、第三者への提供が禁じられている点に留意されたい。また、仮名加工情報の作成元となった個人情報や当該仮名加工情報に係る削除情報等を保有している等により他の情報と照合することで特定個人

が識別できる状態にあるものは「個人情報である仮名加工情報」と定義され、通常の個人情報と大きく変わらない義務が課せられている点においても留意が必要である。

	仮名加工情報	（参考）匿名加工情報
定　義	**他の情報と照合しない限り**特定の個人を識別することができないように加工された個人に関する情報	特定の個人を識別することができず、加工元の個人情報を**復元することができない**ように加工された個人に関する情報
加工基準	**特定の個人を識別することができる記述等の**全部又は一部の**削除又は置換**	**特定の個人を識別することができる記述等の**全部又は一部の**削除又は置換**（規則第19条第１号）
	個人識別符号の全部の**削除又は置換**	**個人識別符号の**全部の**削除又は置換**（規則第19条第２号）
	－	個人情報と当該個人情報に措置を講じて得られる情報を**連結する符号の削除又は置換**（規則第19条第３号）
	－	**特異な記述等の削除又は置換**（規則第19条第４号）
	－	**その他の**個人情報データベース等の性質を勘案した**適切な措置**（規則第19条第５号）
	不正利用されることにより、**財産的被害が生じるおそれのある記述等の削除又は置換**	－ ※クレジットカード番号は、通常、１号又は５号の基準に基づき削除されると考えられる。

【表 3】仮名加工情報と匿名加工情報との比較

（出典：個人情報保護委員会「改正法に関連する政令・規則等の整備に向けた論点について（仮名加工情報）」）

② 提供先において個人データとなる情報の取扱い（いわゆる「Cookie 規制」）

令和 2 年改正法において、生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないものを「個人関連情報」と新たに定義された。

特定の個人を識別できない形で取り扱われているインターネットの閲覧履歴、位置情報、Cookie 等の情報がこれに該当し、これまでは本人の同意なく第三者提供を行うことができたが、令和 2 年改正法では、提供元では個人データに該当しないものであっても、提供先において個人データとなることが想定される情報を第三者に提供する場合、提供元は提供先が本人から同意を得ていることを確認することが義務付けられた。

（５）ペナルティのあり方（法令違反に対する罰則の強化）

令和 2 年改正法では、委員会による命令違反・委員会に対する虚偽報告等の法定刑が引き上げられ、とりわけ法人に対する罰金刑の最高額が大きく引き上げられている（2020 年 12 月に施行済み）。

		懲役刑		罰金刑	
		改正前	改正後	改正前	改正後
個人情報保護委員会からの命令への違反	行為者	6 月以下	1 年以下	30 万円以下	100 万円以下
	法人等	－	－	30 万円以下	1 億円以下
個人情報データベース等の不正提供等	行為者	1 年以下	1 年以下	50 万円以下	50 万円以下
	法人等	－	－	50 万円以下	1 億円以下
個人情報保護委員会への虚偽報告等	行為者	－	－	30 万円以下	50 万円以下
	法人等	－	－	30 万円以下	50 万円以下

【表 4】法令違反に対する罰則の強化

（６）法の域外適用・越境移転のあり方（外国の事業者に対する罰則追加）

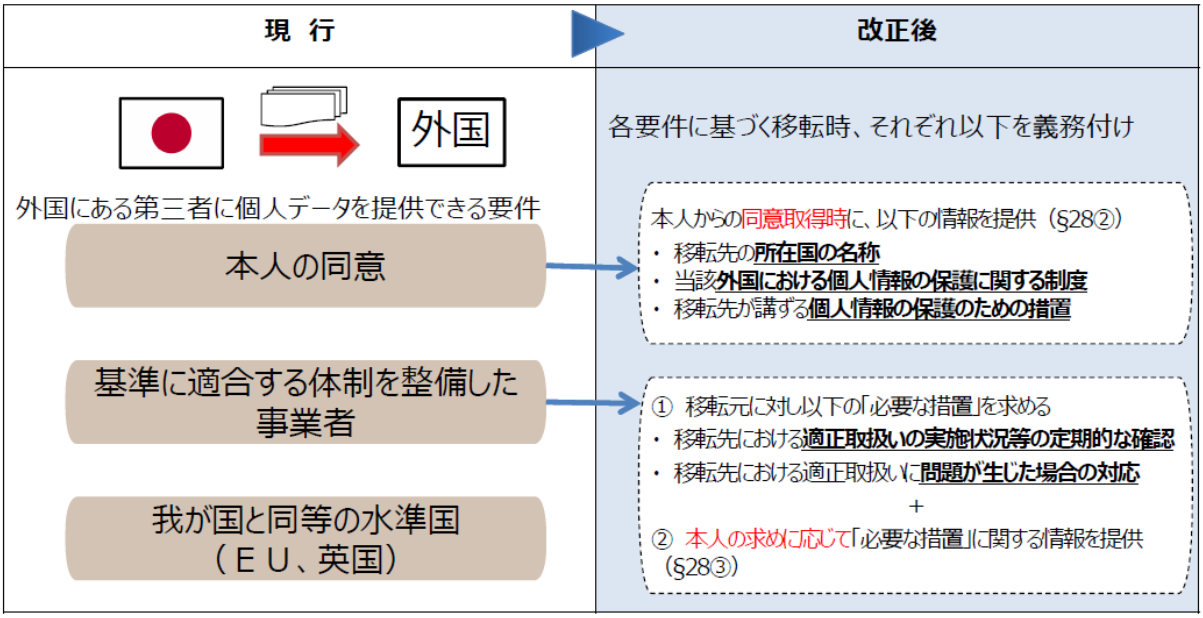
① 外国事業者に対する報告徴収・命令

これまでは、個人情報保護委員会は外国の事業者に対して指導や勧告など強制力のない権限だけを有していたが、令和 2 年改正法により日本国内にある者に係る個人情報を取り扱う外国の事業者も報告徴収・命令および立入検査などの対象になった。

② 外国にある第三者へ個人データを提供する際の本人への情報提供の充実

従来より、外国の第三者に個人データを提供する場合は以下・表 5 左側の要件のうちいずれかを満たす必要があるが、令和 2 年改正法では、移転元の事業者に対して各要件に基づく移転について新たな要件（表 5・右側）を満たすことが義務付けられる。移転先の外国における個人情報の保護に関する制度や、移転先の状況の多様性等に起因する個人データの越境移転に伴うリスクについて、本人の予測可能性を高めることを趣旨として規定された。

なお、外国人の個人データを越境移転している事業者は、当該外国におけるデータ国外移転規制（個人情報が外国に移転される際に一定の要件を満たすことを求める規制）や、データローカライゼーション規制（自国の産業や国家の安全保護を目的に、個人情報などの重要なデータを自国にとどめるための規制）の有無および内容にも留意のうえ取扱されたい。



【表 5】越境移転に係る情報提供の充実

（出典：個人情報保護委員会「令和2年改正個人情報保護法について」）

２．企業が果たすべき「プライバシーの保護」とは

従来、プライバシー問題に対する取り組みは、「私生活をみだりに公開されない法的保障または権利」や「放っておいてもらう権利」の保護に重点が置かれ、個人情報保護法を遵守することが基本であったが、情報通信技術の進展に伴ってプライバシーの概念は「自己情報のコントロール」にまで発展、企業が配慮すべき範囲も個人情報保護法の範疇を超えて広範になってきている。

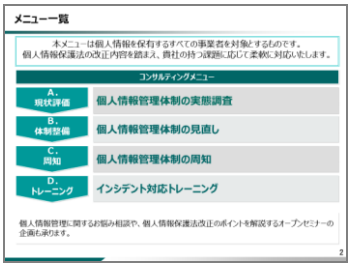
すなわち、プライバシーに対する個人的な感じ方、社会受容性は時間の経過によって変わり得るために、法令を遵守していても対応如何によっては「プライバシー侵害」だけでなく本人への差別・不利益・不安を与えるなどの指摘を受け、経営上の悪影響につながるリスクとして跳ね返ってくる可能性がある。

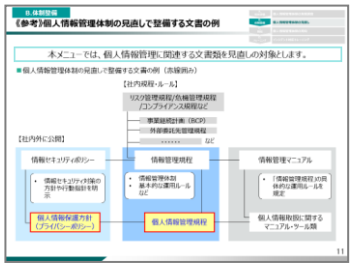
そのような環境下で、プライバシー保護を単なる「コンプライアンス」と受け止めず、重要な経営戦略の一環として捉え、自社ビジネスに関連して起こり得るプライバシーリスクを適切に評価して対応することで社会的な信頼を得て、企業価値向上につなげている企業も現れている。個人情報保護委員会は、PIA（Privacy Impact Assessment、個人情報保護評価[3]）の取り組みを「個人データの管理や従業員への教育効果等も含め、事業者自身にとって、効率的かつ効果的に必要十分な取組を進めるための有用な手段である」と評価しており、参考にされたい。

改正法対応は、事業の規模・性質や保有する個人情報等の内容等によって様々であるが、単なる外形的な法令遵守とならないよう、事業者自身において最適な手法を考慮していくことが重要である。

ＭＳ＆ＡＤインターリスク総研㈱　新領域開発部 サイバーリスク室
マネジャー・上席コンサルタント　岡田　道雄

ＭＳ＆ＡＤインターリスク総研株式会社では、「令和２年 改正個人情報保護法」対応に関するコンサルティングを実施しています。現状の情報管理体制の評価・見直しから従業員教育、緊急時を想定したトレーニングまで、幅広い範囲で実効性のある情報管理体制の構築・整備と定着をご支援します。





ＭＳ＆ＡＤインターリスク総研株式会社は、MS&AD インシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
新領域開発部 サイバーリスク室
東京都千代田区神田淡路町2-105　**TEL.03-5296-8918**
http://www.irric.co.jp/

[3] PIA（Privacy Impact Assessment、個人情報保護評価）
個人情報等の収集を伴う事業の開始や変更の際に、個人の権利利益の侵害リスクを低減・回避するために、事前に影響を評価するリスク管理手法。基本的には事業の企画・設計段階での実施が想定されているが、設計を終えた後の段階における PIA の実施にも一定の意義が認められる。