改正個人情報保護法と企業が押さえておくべき論点

弁護士　**渡邉 雅之**（弁護士法人 三宅法律事務所）

1 本改正の趣旨

令和８年７月10日，「個人情報の保護に関する法律等の一部を改正する法律案」が，第221回特別国会で可決，成立し，同月17日に公布されました（令和８年法律第56号）[1]。いわゆる３年ごと見直し（令和２年改正法附則10条）の流れを受けたもので，定義から執行までを通貫して見直す大型改正です。対象は個人情報保護法だけでなく，番号法・次世代医療基盤法にも及びます。

改正の基本思想は，「使えるデータは使えるようにする」という利活用ルートの整備と，「逸脱や悪質利用には重い責任を課す」という規律強化を同時に進める点にあり，入口を開けつつ出口を強くする両面の改正と整理できます。具体的には，①適正なデータ利活用の推進，②リスクに適切に対応した規律，③不適正利用等の防止，④規律遵守の実効性確保という４つの柱で構成されています。施行は段階的で，罰則関係等の一部が公布後６カ月で先行施行され（附則１条３号），本体部分は公布の日から起算して２年を超えない範囲内で施行されます。本稿では，企業の総務・労務担当の皆さんに関係の深い論点を中心に，濃淡をつけて解説します。主な改正項目と実務への影響は，まず図表１で全体像を示します。

2 本人同意の例外の見直し

実務全般に直結するのが，本人同意の例外の見直しです。対象は，利用目的外利用（18条３項），要配慮個人情報の取得（20条２項），第三者提供（27条１項）の３場面です。

第１に，生命・身体・財産の保護や公衆衛生等の場面で，従来の「本人の同意を得ることが困難であるとき」に加えて「本人の同意を得ないことについて相当の理由があるとき」が追加されます（各条の関係号）。本人に接触可能であっても，同意取得を前提とすること自体が不適切または公益保護に反する場面で，柔軟な対応がしやすくなります。公衆衛生・児童保護・不正行為対策のための情報共有などが想定されます。

第２に，「取得の状況からみて本人の意思に反しないため本人の権利利益を害しないことが明らかである場合」が新たな同意取得の例外として設けられます（18条３項

1 改正法案の条文（法律案・理由），新旧対照表および概要は，個人情報保護委員会「『個人情報の保護に関する法律等の一部を改正する法律案』の閣議決定について」（令和８年４月７日）（https://www.ppc.go.jp/news/press/2026/260407/）に掲載されている。成立後の公布文（令和８年法律第56号）については官報（令和８年７月17日）参照。

図表１　改正の主要項目と実務への影響

改正項目	新設・改正条文	主な実務への影響
本人同意の例外の見直し	18条３項，20条２項，27条１項	契約履行型の情報連携を整理しやすく。不同意で進める判断は記録化が必要
統計作成等の特例	２条13項，30条の２，31条の３	生成AI・データ分析の利活用ルート。要配慮情報は事前削除・PETs処理へ。特例違反は課徴金の対象
特定生体個人情報	16条５項，21条の２，27条２項，35条７項・８項	顔認証・防犯カメラの掲示見直し，停止請求対応フローの整備
連絡可能個人関連情報	２条８項，31条の２	営業リストの取得・利用・提供の整理を見直し
16歳未満の者の保護	35条９項・10項，40条の２，58条の３	子ども向けサービスの法定代理人対応・離脱権対応
漏えい等の本人通知	26条２項	リスク評価に基づく通知要否判断と判断記録の保存
委託を受けた事業者の規律	30条の３，58条の２	クラウド・SaaS・BPO契約の取扱範囲・二次利用条項の点検
不正取得罪・罰則強化	178条～ 180条	退職者・内部者の情報持出し対策の整備
命令・課徴金	148条～ 148条の17	違反の経営リスク化。防止体制の整備と説明可能性の確保

７号等）。本人が通常予期する契約履行型の情報連携を念頭に置いた例外で，ホテル予約サイトから宿泊施設への予約者情報の提供，金融機関による海外送金のための送金先への情報提供などが典型例とされています。予約・決済・送金・BPO処理など，本人が通常予期する情報連携を整理する手がかりとなります。

ただし，判断基準は事業者の都合ではなく本人の合理的期待にあり，利用規約の片隅に書いた程度では「明らか」とはいえません。今後は「なぜ例外に当たるか」を公益性・必要性・本人期待・代替手段の有無の観点から説明し，判断を記録に残す実務が求められます。なお，学術研究例外（20条２項６号，27条１項６号）も整理され，「学術研究機関等」に病院等が含められますが，共同研究を行う企業を除き，一般企業への影響は限定的です。

3　「統計作成等」の特例

利活用面の中心概念として「統計作成等」（２条13項）が新設されます。これは，統計の作成その他の大量の情報からその構成要素に係る情報を抽出し，分類・比較その他の解析を行って，当該大量の情報の傾向または性質に係る情報を作成する行為をいいます。作成されるものが個人に関する情報でなく，権利利益侵害のおそれが少ないものに限られる，という形で絞り込まれた概念です。これを前提に，公開されている要配慮個人情報の取得特例（30条の２第１項），継続公表義務，目的外利用・提供の制限，統計作成等目的の第三者提供ルート（31条の３）が整備されます。入口で特例を認める代わりに，出口では「その特例のためにだけ使う」という強い拘束を課す，高透明・高拘束型の利活用ルートと整理できます。特例の全体像（該当要件と各規律）は図表２の通りです。

図表２　統計作成等特例の要件と規律

区　分	内　容	主な条文
該当要件	①大量の情報が対象，②要素情報の抽出・分類・比較等の解析，③傾向または性質に係る情報の作成，④個人に関する情報を作成しない，⑤権利利益侵害のおそれが少ない	２条13項
取得の特例（入口）	公開されている要配慮個人情報を本人同意なく取得できる（統計作成等目的等であること・必要事項を公表していること・現に公開されている要配慮個人情報であること，が条件）	30条の２第１項
継続公表義務	データ源・対象情報・統計作成等の内容・第三者提供の有無等を継続して公表（変更時は原則として事前に公表）	30条の２第２項・３項
目的外利用・提供の制限（出口）	公表した内容を実現するため必要な範囲を超える取扱いは禁止。第三者提供も原則として制限される	30条の２第４項以下
第三者提供ルート	第三者が統計作成等を行う目的で必要な場合，提供元・提供先双方の公表と契約上の明記を条件に提供できる	30条の２第５項，31条の３

一般企業がこの特例を直接使う場面は多くありませんが，社内で生成AIを業務利用する場面では工程ごとの検討が欠かせません。一般に，大量データから言語の一般的なパターンを学ぶ事前学習は統計作成等に整理し得る一方，特定個人の選好・行動履歴に基づくファインチューニングや，プロンプト・RAGに個人データを投入して個人別の出力を得る利用は，「個人に関する情報」の取得・利用に転じ得ます。線引きは名称ではなく，出力が特定個人に戻るかどうかにあります。

なお，令和５年６月には個人情報保護委員会が，ChatGPTを提供するOpenAIに対し法147条に基づく注意喚起を行い，学習用データセットに加工する前に要配慮個人情報を削除しまたは特定の個人を識別できないようにする措置等を求めています。この「学習前の除去・非識別化」という姿勢は，後述の改正法の運用方向と軌を一にするものです。

この統計作成等特例は，国会審議で最も紛糾した論点です。政府は，統計作成等の目的で用いる場合に限り，公開されていない病歴等の要配慮個人情報であっても本人同意なく第三者提供の対象となり得ることを認める一方，個人ごとのスコアリングや個人向け広告･営業への転用は定義上，「統計作成等」に含まれないと説明しました。氏名・住所の事前削除は法律上の一律要件とはされませんでしたが，政府は，提供先が「AI開発等の目的で取り扱う必要がある場合」に限り提供できるとの要件（31条の３）を根拠に，明らかに不要な氏名等を削除せず漫然と提供すれば違法であり，提供元にも削除が求められると答弁しています。加えて，要配慮個人情報については，提供・学習の前に削除・仮名化またはPETs（差分プライバシー，秘密計算，連合学習，合成データ等のプライバシー強化技術）による処理を求める方向が，委員会規則・ガイドラインで具体化される見込みです。衆議院の附帯決議も，他情報との照合による識別を防止する措置の確実な実施，要配慮個人情報の安全管理措置と委託先監督の徹底，PETs活用に係るインセンティブの検討を求めています。加えて参議院の附帯決議は，AIモデル等による特定個人の識別・要配慮個人情報の推知リスクの十分な勘案と，外国企業を含む事業者に対する個情委のモニタリング・報告徴収を求めています。特例違反は後述の課徴金の

対象でもあり，成立後の規則・ガイドラインの動向を注視する必要があります。

4 特定生体個人情報（顔認証・防犯カメラ・入退室に直結），連絡可能個人関連情報

オフィスの入退室管理や防犯カメラ運用，顔認証システムを担う総務部門に重要なのが，「特定生体個人情報」（16条５項）です。特別の技術や多額の費用を要しない方法で取得でき，かつ本人が取得を容易に認識できない身体特徴情報を変換した識別符号を含む個人情報で，顔特徴データが中心的に想定されています。

これには三本柱の特則がかかります。第１に，取扱いにあたり，事業者名・取扱事実・利用目的・身体特徴情報の内容・開示等請求手続等をあらかじめ通知しまたは本人が容易に知り得る状態に置く周知義務（21条の２）です。「顔認証使用中」といった抽象的掲示では足りません。第２に，オプトアウトによる第三者提供の禁止（27条２項）です。第３に，本人による利用停止等・第三者提供停止の請求権（35条７項・８項）で，違法な取扱いがなくとも本人が請求できる点が大きな特徴です。

店舗・ビル・空港・イベント会場・オフィスの出入管理や防犯カメラ連携で顔認証を利用している企業は，既存の掲示・社内規程・プライバシーポリシーが新法水準を満たすかを施行前に点検し，本人からの停止請求に応答する運用フローを整える必要があります。掲示の方法は委員会規則で定められる方針で，衆参両院の附帯決議も機器周辺への掲示の徹底を求めています。停止請求に伴う顔データの照合は，消去のための一時的な取扱いとして許容されると説明されています。既存通知・同意のみなし規定（附則４条）はありますが，従前の文言・取得方法が新法水準を満たすかは再評価が必要です。

なお，住所等・電話番号・メールアドレス・電気通信設備の識別符号など，特定の個人に連絡し，または情報を伝達できる記述等を含む「連絡可能個人関連情報」（２条８項）が新設され，不適正利用・不正取得の禁止（31条の２）が課されます。保護の着眼点が，「誰であるか（識別可能性）」から「その人にどう到達できるか（接触可能性）」へと広がるものです。これにより，電話番号・メールアドレス・所在地を含む営業リストや見込み客リストを「個人情報ではないから自由」と整理しにくくなります。データ購入契約，送客契約，マーケティング委託契約や，営業部門のリスト利用ルールについて，取得・利用・提供の整理を見直す必要があり，営業部門から照会を受ける総務・法務部門としても押さえておくべき論点です。

5 16歳未満の者の保護

子ども向けサービスやBtoC事業を行う企業に関わるのが，16歳未満の者の保護の強化です。

第１に，利用停止等請求権の拡張です。事業の適正な実施に著しい支障を及ぼすおそれがある場合などの法定の例外を除き，保有個人データの利用停止等または第三者提供の停止を請求できます（35条９項・10項）。SNS，教育サービス，ゲーム，位置情報サービス，行動履歴分析等で特に重要となり，親権者同意の有無だけでなく，事後的に離脱できる権利として構成されています。

第２に，法定代理人への読替えです。16歳未満の者の個人情報等の取扱いについては，同意取得・通知・開示等請求・利用停止等請求その他の本人関与場面で，原則と

して「本人」を「法定代理人」と読み替えます（40条の２）。従来Q&Aや実務慣行で対応していた未成年者対応が，法律上の明文規律となります。実務上は，利用規約，プライバシーポリシー，同意取得画面，問合せ窓口，開示等・利用停止等請求のフローを，法定代理人対応を前提に再設計する必要があり，年齢確認をどこまで求めるか，その際に過剰な個人情報を取得しないかも論点となります。

第３に，最善の利益を優先して考慮する責務です。16歳未満の者の個人情報等を取り扱うにあたり，本人の最善の利益を優先して考慮しなければならないとされ（58条の３），ダークパターン，依存誘発設計，過剰な課金誘導，偏った推薦アルゴリズム等への解釈指針となり得ます。既存同意・既存通知のみなし規定（附則５条・６条）はありますが，従前の取得方法が新法水準を満たすかは再評価が必要です。一般のBtoB企業への影響は限定的ですが，福利厚生等で従業員の子に関する情報を扱う場面では念頭に置くとよいでしょう。

6 漏えい等発生時の本人通知の見直し

インシデント対応の事務局を担う総務部門にとって重要なのが，本人通知義務（26条２項）の見直しです。現行法では原則として本人通知が必要でしたが，改正後は「本人の権利利益を保護するために必要なものとして欠けるおそれが少ない場合」に，代替措置をもって通知を省略できるようになります。形式的な一律通知から，実質的なリスク評価に基づく判断への転換です。

判断要素は，漏えい情報の性質，他情報との照合可能性，漏えい先の属性，回収・削除・アクセス遮断の状況，本人に追加的防御行動を求める必要性などです。例えば，信頼できる取引先への誤送付で削除確認済みの事案は低リスク，氏名・連絡先・IDの組合せや漏えい先不明の事案は高リスクと整理されます。通知を省略する場合は「保護に欠けるところがない」と説明できることが前提となるため，リスク評価メモや判断記録の保存が不可欠です。情シスによる事実把握，法務による侵害評価，広報・顧客対応部門による通知設計を連携させる体制を，施行前から整えておくことが望まれます。

7 委託を受けた事業者の規律

クラウド・SaaS・BPOを多用する総務部門にとって，委託規律の見直しは重要です。委託を受けた事業者は，委託された個人情報を委託業務の遂行に必要な範囲を超えて取り扱ってはならないという直接義務を負います（30条の３）。従来は委託元の監督義務の反射として整理されていた部分が，委託先自身の法律上の義務へと格上げされました。委託先による「サービス改善」「AI学習」名目での受託データの独自利用は，原則として範囲外と整理されます。

他方，自ら取扱方法を決定せず，契約で取扱方法等が定められ，必要な範囲内で契約通りに運用される機械的・受動的な受託処理には，本法の一部規律を適用しない調整がなされます（58条の２）。データ入力・印字・発送等が想定例です。これには単なる秘密保持条項では足りず，契約の作り込みが適用除外の前提です。いわゆる「クラウド例外」も消えるわけではありませんが，現に個人データを取り扱うクラウド事業者には規律が及ぶため，「クラウドだから当然に例外」という整理は通用しません。委託契約では，取扱方法の決定者，二次利用条項，再委託，事故報告，監査権限を改め

て点検する必要があります。

また，オプトアウトによる第三者提供についても規律が強化されます。提供元は提供先の氏名・住所・代表者の氏名・利用目的を事前に確認する義務を負い（27条７項），確認を求められた提供先は虚偽の回答をしてはならず（27条８項），違反には10万円以下の過料が科されます（186条１号）。第三者提供記録には利用目的の確認事項も追加されます（29条１項）。名簿流通やデータブローカー業務に直接影響する改正で，確認と記録はセットで運用する必要があります。なお，この虚偽回答の禁止と過料は，公布後６カ月で先行施行される部分（附則１条３号）に含まれます。名簿流通型の事業を行わない企業への影響は限定的ですが，外部から購入したリストを利用する場合などには確認義務が関係し得ます。

8 不正取得罪の新設と罰則強化

罰則も大幅に強化されます（176条，178条～180条，186条）。不正提供・盗用については，「不正な利益を図る目的」に加えて「本人その他の者に損害を加える目的」も処罰対象に加わり，法定刑が１年以下の拘禁刑または50万円以下の罰金から，２年以下の拘禁刑または100万円以下の罰金へと引き上げられます（178条，179条）。さらに，欺罔・暴行・脅迫や保有者の管理を害する行為により取得した者を処罰する不正取得罪が新設されます（180条，２年以下の拘禁刑または100万円以下の罰金）。

実務上は，内部者による情報持出し，退職者による顧客情報・名簿の流出，委託先の横流し，報復・嫌がらせ型の流出が，金銭目的でなくとも，企業，本人どちらも処罰対象となり得る点が重要です。秘密保持誓約書，退職時の情報返還・削除確認，アクセス権限の付与・剥奪のフローを改めて整備しておくことが望まれます。

9 命令体系の再設計と課徴金制度の導入（最重要）

（１）命令体系の再設計

委員会の命令内容が，違反の是正にとどまらず，本人への通知・公表その他本人の権利利益保護のために必要な措置にまで拡張されます（148条）。漏えいや違法な提供を受けた本人に対し，事業者から直接通知・公表させることが可能になるイメージです。また，違反行為を補助する第三者（ホスティング事業者，クラウド事業者，プラットフォーム等）に対し，違反行為の中止に必要な措置を要請できる仕組みも設けられます（148条の２）。違反主体への命令だけでは止めにくい，インフラを通じた違反の継続に対応するものです。

（２）課徴金制度の趣旨と対象行為

今回の改正で最もインパクトが大きいのが，課徴金制度の導入です（148条の３～148条の17）。現行法では，勧告・命令後に行為を中止しても違反により得た経済的利益を保持できる場面があり，抑止として限界があると指摘されてきました。そこで改正法では，重大な違反行為により個人の権利利益が侵害された場合等について，違反行為によって得られた財産的利益等に相当する額の課徴金の納付を命ずる制度を導入します。課徴金は刑罰ではなく，金銭的不利益を課す行政上の措置であり，「違反しても儲かる」構造を断つことを狙うものです。

対象は無限定ではなく，悪質性と経済的誘因が明確な行為類型に重点化されています。具体的には，①不適正利用の禁止違反

（19条）のうち違法行為等を行うことが想定される第三者への提供等，②偽りその他不正の手段による取得・利用（20条１項違反），③本人同意なき違法な第三者提供（27条１項違反），④統計作成等特例に違反して取得情報を統計化せずそのまま販売し，または目的外利用して利益を得る行為などが対象です。統計作成等特例は，利活用の入口を開く一方で，その逸脱を課徴金という最も重い行政措置で抑止する設計であり，両者は表裏一体です。

（３）成立要件と「相当の注意」

課徴金は対象行為に当たれば自動的に課されるものではなく，複数の要件を満たした場合に課されるものです（図表３参照）。特に重要なのが「相当の注意」の要件で，対象行為が生じても，その行為を防止するための相当の注意を尽くしていたことを説明できれば，課徴金の対象から外れる余地があります。課徴金額は，対象行為または対象行為をやめることの対価として得た財産上の利益の額を基礎とする利得剥奪型で，売上高連動型ではありません。対象行為と因果関係のある利益額をどう認定・推計するかは，実務上の難しい論点となり得ます。さらに，過去に課徴金命令を受けた者については課徴金額が加重され，違反を自主的に委員会へ報告した者については課徴金額が減額される（リニエンシー）仕組みも設けられています。審査フロー，契約審査，アクセス制御，ログ管理，教育・監査，承認記録の整備と，その説明可能性が鍵となります。

（４）経営リスク化

なお，課徴金の対象範囲は当初の検討段階から絞り込まれており，国会審議でも議論の的となりました。安全管理措置義務違反（23条）は対象外とされ，適格消費者団体による差止請求・被害回復（団体訴訟）制度の導入も見送られたため，抑止力と被害救済の観点から強い批判が示されています。政府は，初めての導入であることから「スモールスタート」とせざるを得ないとし，附則14条の３年ごと見直しを通じて水準・対象要件を検証すると答弁しました。もっとも，課徴金制度の導入により，個人情報保護法違反は法務・コンプライアンス上の問題にとどまらず，財務リスク・経営リスクへと性格を変えます。個人情報の取扱いを現場任せにせず，経営管理・内部統制のテーマとして扱い，重大案件・高リスク案件は取締役会・経営会議レベルで関与する体制が求められます。

10 施行スケジュールと実務対応

施行は段階的です。罰則関係等の一部は公布後６カ月で先行施行され（附則１条３号），本体部分は公布の日から起算して２年を超えない範囲内で政令により定められ

図表３　課徴金納付命令の主な成立要件

要　件	内　容
①　対象行為への該当	不適正利用（19条），不正取得・利用（20条１項），違法な第三者提供（27条１項），統計作成等特例違反等
②　相当の注意の欠如	行為を防止するための相当の注意を怠ったこと（怠った者でないと認められれば対象外）
③　大規模性	対象行為に係る本人の数が1,000人を超えること
④　侵害の重大性	権利利益を害する程度が大きくない場合に当たらないこと（軽微な侵害は対象外）

ます。特定生体個人情報・命令・課徴金等には個別の経過措置やみなし規定が置かれますが，委託規律には個別のみなし規定がなく，既存契約の棚卸しが必要です。施行後３年ごとの見直し（附則14条）も予定されており，今回の対応は継続的なデータガバナンスの出発点と位置付けられます。

総務・労務担当者として優先すべきは，第１に，自社の個人データの取扱いを類型別に棚卸しすること（顔認証･防犯カメラ，営業リスト，委託・クラウド・BPO，漏えい対応，生成AI利用，子ども向けサービスなど），第２に，委託契約・共同利用契約，社内規程，秘密保持誓約書，顔認証等の掲示，プライバシーポリシー，漏えい時通知基準といった契約・社内文書・外部公表文書を一体で見直すこと，第３に，総務・人事・法務・情報セキュリティ・経営陣が連携し，停止請求・本人通知命令・課徴金リスクに即応できる体制を構築することです。

特に，みなし規定のない委託規律については，契約期間の長い委託・クラウド契約から早期に見直しに着手することが現実的です。単発の対応で終わらせず，データの取得から廃棄に至るライフサイクル全体を棚卸ししたうえで，規程･契約･公表文書･社内研修・モニタリングを一体のデータガバナンス体制として整備しておくことが，課徴金時代における最大のリスク低減策となります。

11 どの改正項目等の影響を受けるかを早期に可視化すること

今回の改正は，個人情報保護法を「使えるデータは使えるようにする法」としつつ，逸脱には重い責任を課す法へと進めるものです。どの改正条項とどの経過措置の影響を受けるかを早期に可視化し，特に６カ月先行施行部分を優先して，契約･規程･運用･体制の見直しに着手することが肝要です。

【執筆者略歴】渡邉 雅之（わたなべ まさゆき）

弁護士。弁護士法人三宅法律事務所。企業法務，金融規制，個人情報保護・コンプライアンス，労務・不祥事対応等を取り扱う。金融機関・事業会社に対し，個人情報保護法，AML/CFT，内部統制，内部通報，就業規則整備等に関する助言・研修を多数担当。

著者 弁護士法人三宅法律事務所
弁護士　渡邉 雅之
ビジネスガイド2026年９月号より