

■ Webセミナー【後半】

令和8年改正個人情報保護法

執行の強化 — 課徴金・オプトアウト・漏えい通知と上場企業の実務対応

2026年7月10日成立・同月17日公布（令和8年法律第56号）／衆参附帯決議（各14項目）を踏まえて

弁護士法人三宅法律事務所

2026年9月

パートナー弁護士 渡邊 雅之

※本資料は令和8年7月17日公布の改正法（令和8年法律第56号）、国会審議及び個人情報保護委員会事務局資料に基づく一般的な情報提供です。施行は一部を除き公布日から2年以内の政令指定日（先行施行：令和9年1月17日）。今後の政令・委員会規則・ガイドライン等の整備状況を適宜ご確認ください。

PART

6

委託を受けた事業者の規律

委託先の直接義務（30条の3）と機械的受託処理の適用調整（58条の2）

委託規律見直しの背景 ― 委託先は「事務補助者」ではない

■ データ処理構造の変化

- クラウド・SaaS・BPO・AI開発受託・データ加工受託・コールセンター・物流／決済代行等、委託先が大量データを実質的に取り扱う時代になった。
- 受託データを、自社の分析・品質改善・AI学習・別サービス開発に独自利用する事案が問題化している。

■ 現行法の限界

- 委託先は委託元と一体として扱われ、範囲外利用は委託元の監督義務（25条）を通じて間接的に規律されてきた。
- 委託先自身に対する「範囲を超えて取り扱ってはならない」という独立の直接義務は、法文上正面から置かれていなかった。
- 印字・封入・発送等の機械的処理では支障が小さかったが、委託先が裁量をもって取扱方法を決める場面が増えた。

★POINT

委託先を「独立したデータ取扱主体」として捉え直すのが、30条の3・58条の2の出発点である。

委託先の範囲外利用禁止（30条の3） — 直接義務

■ 新設される直接義務

- 委託先自身に「委託された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」という直接義務を課す。
- 委託元の監督義務の反射として捉えられていた範囲外利用禁止を、委託先固有の法的義務として法文化するものである。
- 例外は、法令に基づく場合や人命救助・災害救援等の限定的な場面にとどまる。

■ 問題となる典型場面

- 受託データを自社分析・品質向上・別サービス開発・汎用AI学習に転用する行為。
- 「サービス改善のため」「品質向上のため」という説明だけでは足りず、委託業務の遂行に必要な範囲かが問われる。

受託データを汎用学習に用いるのであれば委託構成では不十分であり、別の法的構成・契約・同意・提供ルートの検討が必要となる。

★POINT

「受託したから使える」ではなく「委託業務の遂行に必要なだから使える」へ整理が改められた。

委託先の独自利用が問題となる6類型

類型	具体例	評価
① 自社サービス改善	受託データを自社プロダクトの品質向上に利用	委託業務の遂行に必要な範囲外
② AI・モデル学習	受託データを汎用モデル・他案件向けモデルの学習に利用	同上（30条の3違反）
③ 横断分析	複数の委託元のデータを混合して分析	委託範囲外＋個票混合の問題
④ 別サービス開発	受託データを新規サービスの企画・検証に利用	委託範囲外
⑤ 営業支援	受託データから見込み客を抽出し自社営業に利用	委託範囲外＋目的外利用
⑥ 事業基盤への取込み	受託データをDB・分析モデル・業界知見として蓄積	実質的に第三者提供・目的外利用と評価され得る

★POINT

「品質向上のため」は万能の説明ではない。契約に独自利用禁止を具体的・網羅的に列挙する。

機械的・受動的受託処理への適用調整（58条の2）

■ 制度の趣旨

- 取扱方法を自ら決定しない受託者には、第4章（個人情報取扱事業者等の義務）が定める義務の大部分を適用しない仕組みを導入する。

■ 適用調整の要件

- ① 委託契約で取扱方法として委員会規則で定める事項等が定められていること。
- ② 取扱いが委託業務の遂行に必要な範囲内であること。
- ③ 実際の運用が契約どおりであること。

■ 想定例

- 詳細な指示に従ったデータ入力・印字・発送・スキャン・形式変換等、受託者が自ら処理内容を決めない処理。

単なる秘密保持条項や一般的な善管注意義務条項では足りず、事故報告・取扱状況の把握・権限管理・再委託条件等を含む具体的な契約設計が必要となる。

★POINT

独自判断を伴う委託先には30条の3、機械的受託者には58条の2という二段構造である。

58条の2による適用調整の範囲 — 何が外れ、何が残るか

適用が除外される主な規律	適用が残る規律（免除されない）
利用目的の特定・目的外利用の制限、利用目的の通知・公表（17条・18条・21条）	安全管理措置関連（23条～25条、31条の3、41条2項、42条3項、43条2項6項、46条）
不適正利用の禁止、適正取得・要配慮個人情報の取得制限（19条・20条）	従業員の監督・委託先（再委託先）の監督
特定生体個人情報の取扱い時の周知（21条の2）	漏えい等発生時の報告・本人通知（26条）
第三者提供の制限・オプトアウト、確認・記録義務（27条～29条）	委託業務の遂行に必要な範囲を超える取扱いの禁止（30条の3）
保有個人データの公表・開示・訂正・利用停止等の請求対応（32条～39条）	契約に定めがない場合、又は契約どおりに取り扱われていない場合、免除は及ばない

本人からの開示等請求は委託元が対応する建付けとなる。「機械的受託だから何も負わない」ではない。

【下位法令】義務免除の前提として委託契約で定めるべき事項及び契約の方法は、委員会規則で定められる。契約ひな形の改定は、この規則案の公表を待って行う。

★POINT

免除されるのは第4章の義務の大部分。安全管理措置・漏えい等報告・範囲外利用禁止は残る。

いわゆる「クラウド例外」との関係

■ クラウド例外の整理

- 外部事業者が契約上・運用上、保存された個人データを取り扱わないこととなっている場合、第三者提供にも委託にも当たらないとする整理が個人情報委Q&A（Q7-53）で認められてきた。
- 前提は、外部事業者が当該データを「取り扱わない」状態が契約とアクセス制御により確保されていることである。2024年3月には、現実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旨の注意喚起がなされた。

■ 改正後の整理

- クラウド例外自体が消えるわけではないが、「取り扱わない」という前提を維持できるかがより厳密に問われる。
- 委託先の範囲外利用禁止（30条の3）・機械的受託処理の適用調整（58条の2）・第三者提供・共同利用のいずれで整理するかを個別に検討する必要がある。

API・SaaS型生成AIで入力・会話ログをモデル改善等に用いる実務は、当然に受託処理の範囲に入るとは言いにくくなる。

★POINT

「クラウドだから当然例外」は通用しない。契約・技術的アクセス制御・運用実態の三面で可視化する。

生成AIの業務利用 — DPAによる委託構成

■ 結論 — 「DPA + 学習無効設定」で委託構成が可能

- API連携でDPAを締結し、入力データをモデル学習に利用させない設定であれば、27条5項1号の「委託」として本人同意なく取り扱わせることができる。
- 法人向け・API向けプランは既定で学習不使用 + DPAの提供あり。無償・個人向け版は学習に利用され得るため業務利用は避ける（契約時・更改時に最新規約を要確認）。

■ 委託構成で満たすべき3要件

- ① 委託契約（DPA） — 目的限定・秘密保持・再委託・返還／削除・監査。改正後は30条の3・58条の2の整理を反映する。
- ② 安全管理措置（23条） — アクセス制御・ログ管理・暗号化。加えて学習無効設定の維持確認と無償版の業務利用禁止を社内ルール化する。
- ③ 越境移転（28条） — 海外事業者への委託は「外国にある第三者への提供」に当たり得る。基準適合体制の確認と本人への情報提供。

国会審議でも、越境移転規律は統計作成等特例によって緩和されないことが確認された。委託先・再委託先の所在国、データ保存先、外国政府アクセス法制の評価まで契約と根拠整理に落とし込む。

★POINT

「DPA + 学習無効設定」で委託構成は可能。ただし国内リージョンだから安全とはいえず、規約改定の確認もルール化する。



PART

7

16歳未満の者の保護

利用停止等請求権の拡張・法定代理人への読替え・最善の利益の責務

背景 — 現行法にこどもの規定は一つもない

■ 法律・政令・規則・GL本体のいずれにも規定がない

- 同意能力、法定代理人の関与、開示等請求の主体 — いずれについても明文がない。年齢による区別を一切設けていない。
- 唯一の手掛かりが個情委「GLに関するQ&A」。同意の結果を判断できる能力を有していない場合には法定代理人等の同意が必要とし、一般的には12歳から15歳までの年齢以下のこどもがこれに当たると考えられる、という趣旨を示すにとどまっていた。

■ Q&Aにしか根拠がないことの帰結

- 法的拘束力なし — Q&Aは法令でもGL本体でもなく、解釈の目安にすぎない。
- 予見可能性を欠く — 「12歳から15歳まで」という幅のある示し方で、線引きは事業者任せ。
- 同意の場面に限られる — 開示・訂正・利用停止等の請求主体、通知・公表の相手方には拠り所がない。
- 執行の実効性を欠く — Q&A自体を根拠に法執行を行うことは困難。

令和8年改正は、年齢の基準（16歳未満）と、本人関与の全場面における法定代理人への読替え（40条の2）を、初めて法律上のルールとして定めるものである。

★POINT

こどもの個人情報の取扱いは、これまで法令ではなくQ&Aの一節に支えられていた。改正はその法定化である。

背景 — 立法を促した3つの要因

■ ① こどもの個人情報に固有のリスク

- 予測困難性 — 同意の結果として情報がどこまで流通し、将来どう影響するかを判断しにくい。学習履歴・位置情報・行動履歴・SNS投稿は長期に蓄積され、進学・就職・信用にまで影響し得る。
- 設計上の脆弱性 — ダークパターン、長時間利用設計、依存誘発、過剰課金誘導、偏った推薦アルゴリズム。国会審議では、保護者の年収と学業成績を結び付けるプロファイリングによる差別的利用が問題とされた。

■ ② 国内法制との整合

- こども基本法（令和4年法律第77号）・児童の権利に関する条約が、こどもの最善の利益を優先して考慮することを求める。個人情報保護法にのみ規定がない状態は、法体系として整合性を欠いていた。

■ ③ 国際的動向

- GDPR8条 — 情報社会サービスにつき16歳未満は法定代理人の同意（加盟国は13歳まで引下げ可）／米国COPPA — 13歳未満／英国Age Appropriate Design Code — 設計段階での配慮。

令和6年12月25日の検討会報告書がこどもの個人情報に関する規律の必要性を指摘し、令和8年1月9日の制度改革方針で導入が確定した。

★POINT

「同意の有無」だけでなく「最善の利益」を法定したのは、こども基本法・児童の権利条約と接続させるためである。

全体像と「16歳未満」とした理由

■ 16歳未満保護の枠組み（包括的な保護設計へ）

- 利用停止等請求権の拡張（35条9項・10項）／法定代理人への読替え（40条の2）／最善の利益の考慮義務（58条の3）／既存同意・既存通知のみなし（附則5条・6条）。番号法・次世代医療基盤法にも同趣旨の規律と経過措置が置かれる。

■ 「16歳未満」とした理由（政府答弁）

- 民事訴訟法上の証人宣誓年齢（16歳）との整合。
- GDPRの基準（16歳を上限に、加盟国が13～16歳の範囲で設定）等の国際的動向。
- 現行ガイドライン（12～15歳程度は法定代理人の同意を得る必要があるとする運用）との整合と、より明確な線引きの要請。

経過措置（附則5条・6条）によるのみなし規定はあるが、新法水準を満たすかの再評価は別途必要である。

★POINT

年齢の線引きは制度上明確になった。既存サービスは「同意の取り直しの要否」を個別に判定する。

利用停止等請求権（35条9・10項）と法定代理人への読替え（40条の2）

■ 利用停止等請求権の拡張（35条9項・10項）

- 事業の適正な実施に著しい支障がある場合等の例外を除き、保有個人データの利用停止等・第三者提供の停止を請求できる。
- 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る。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る。

■ 法定代理人への読替え（40条の2）

- 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」と読み替える。
- 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・開示等請求フロー・利用停止等請求フローを法定代理人対応で再設計する必要がある。

オンラインでは、年齢把握をどこまで求めるか、不知の場合の扱い、年齢確認のための過剰取得の回避が実務論点となる。

【下位法令】違法行為等の有無を問わない利用停止等請求の例外事由のうち、35条9項12号は政令、同項8号（権利利益を害しないことが明らかな場合）及び9号（公開主体）は委員会規則で定められる。

★POINT

「未成年者への配慮」から「法定代理人を相手方とする制度対応」へ明確化された。

最善の利益の責務（58条の3）

■ 条文の内容

- 16歳未満の者の個人情報等を取り扱うに当たっては、当該本人の最善の利益を優先して考慮しなければならない。形式的な同意の有無を超えた評価基準が、初めて法律上導入される。

■ 解釈指針となり得る場面

- ダークパターン（解約導線の隠蔽、初期設定での共有オン等）／長時間利用を促す設計／依存誘発／過剰課金誘導／偏った推薦アルゴリズム。
- 行動履歴に基づくターゲティング広告や高精度プロファイリングは、形式的な法定代理人の同意があっても、最善の利益に照らして可否と設計を判断し、判断過程を記録に残す必要がある。
- DV・虐待事案では、加害親が法定代理人として同意し又は開示請求をし得るという構造的問題がある。国会審議では、親権喪失・親権停止の審判がない限り法律上は同意権限が認められるとの整理が示されており、この場面こそ58条の3の解釈で対応すべき領域となる。

上場企業では、こども向けサービスのほか、インターンシップ・職場体験・こども参観・株主向けイベント等での取得も点検対象となる。

★POINT

「法定代理人の同意があるから適法」では済まない。最善の利益の観点からの実質判断が求められる。

16歳未満か否かの確認 — 法律は方法を定めていない

- 改正法は確認方法を定めていない。適切な方法はサービスの性質・取り扱う個人情報の状態・具体的事情に応じて異なり、考慮要素と具体例は委員会規則・ガイドラインで示される（政府参考人答弁）。

確認方法	内容	確度	想定される場面
① 年齢帯のチェックボックス	「16歳以上である」旨にチェックさせる自己申告・表明保証	低	低リスクの一般向けサービス
② 生年月日の入力	自己申告だが数値として記録が残り、後の再判定に使える	低～中	会員登録・アンケート一般
③ 決済手段による間接確認	カード名義・キャリア決済等から成人性を推認する	中	有料サービス・課金を伴う場面
④ 法定代理人への到達確認	保護者のメールアドレス等宛に確認・同意取得（ダブルオプトイン）	中～高	こども向け・教育サービス
⑤ 本人確認書類・eKYC等	生年月日を確実に把握できる。犯収法の取引時確認では実施済み	高	金融取引・要配慮情報を扱う場面

担当大臣答弁は、機微な内容や重大な影響がある場合にはより丁寧な方法が求められる一方、こども向けサービスが過度に萎縮しないバランスも必要であるとする。附帯決議 第8項も柔軟な手法を許容。もっとも、16歳未満であることを知り、又は容易に知り得る場合には、チェックのみを根拠に成人として扱うことはできない。

★POINT

「チェックを入れたから成人」では済まない。確認の確度は、取り扱う情報とサービスのリスクに応じて変える。

年齢確認の設計 — 3つの原則と「不知」の扱い

■ ① リスクベース — 確度をサービスに応じて変える

- 確度を上げる：要配慮個人情報の取得、高精度プロファイリング、課金・広告ターゲティングを伴う場合。
- 確度を下げてよい：氏名すら取得しない低リスクのサービス。一律の厳格確認は不要。

■ ② 過剰取得の回避（22条・必要最小限）

- 身分証画像の一律取得は目的に照らして過剰となり得る。取得する場合は生年月日に限定し、確認後は速やかに削除するか確認済フラグのみを保持する。
- 年齢確認のために取得した情報をマーケティング等へ転用しない。利用目的と保存期間を分けて管理する。

■ ③ 虚偽申告への対応フロー

- 利用実態・入力内容・学校名や学年の記載・保護者からの申出等の兆候を把握した場合に、再判定し法定代理人対応へ切り替える手順を定める。

■ 「不知」の扱い — まずサービスを仕分ける

- 年齢を把握しない設計は40条の2の履行を困難にする。他方、全サービスでの確認も現実的でない。16歳未満の利用を想定するか否かで仕分け、想定するものにのみ確認を組み込む。
- 想定しないサービスでは、規約上の年齢制限の明示と、判明時の対応（利用停止・データ削除・法定代理人への連絡）を定めておく。

犯収法の取引時確認やeKYCを行う取引では、年齢は本人確認の一環として確実に把握できる。課題は、把握した年齢を開示・利用停止請求の窓口対応等の社内フローに反映させることにある。

★POINT

確認方法の巧拙よりも、「どのサービスで確認するか」の仕分けと、判明後の社内フローの設計が要となる。

PART

8

漏えい等発生時の本人通知義務の見直し

通知例外を委員会規則の指定により限定的に拡張（26条2項）

前提の確認 — 漏えい等報告・本人通知制度の全体像（26条）

■ 報告対象事態（26条1項・規則7条各号） — 現行は4類型

- ① 要配慮個人情報が含まれる ② 不正に利用されることにより財産的被害が生ずるおそれがある
- ③ 不正の目的をもって行われたおそれがある（不正アクセス、従業員による持出し、ランサムウェア等） ④ 1,000人を超える本人に係るもの

■ 二段階の報告と、本人通知

- 速報 — 事態を知った後「速やかに」（通則GL上はおおむね3～5日以内）。確報 — 30日以内（③の類型は60日以内）。
- 本人通知（26条2項） — 事態の状況に応じて速やかに。報告の期限とは別軸であり、報告を終えるまで通知を待つ運用は予定されていない。

■ 委託先で発生した場合（26条1項ただし書）

- 報告義務は委託元・委託先の双方に生じるのが原則。委託先が当該事態が生じた旨を委託元に通知したときは、委託先の報告義務・本人通知義務は免除される。委託元が一元的に対応する建付け。

■ 改正で見直される点（個人情報事務局「政令・規則等で定める事項の全体像（案）」令和8年8月26日）

- 26条1項関係（委員会規則で規定） — ① 違法な個人データの第三者提供を報告対象事態に追加 ② 一定の範囲での速報の免除 ③ 一定期間ごとに取りまとめた確報の許容。
- 26条2項関係（委員会規則で規定） — 本人への通知が行われなくても権利利益の保護に欠けるおそれが少ない場合（行政機関等につき68条2項1号も同様）。

報告義務の枠組み自体は維持されるが、「報告すべき事態」と「報告の手続」にも規則レベルの見直しが入る。委託先の扱い（26条1項ただし書）は変わらない。

★POINT

改正の中心は「通知を省略できる場合」。ただし報告対象事態と報告手続にも規則で見直しが入る。

本人通知義務の見直し（26条2項） — 新旧対照

■ 26条2項ただし書の新旧

- （改正前）ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。
- （改正後）ただし、本人への通知が困難な場合又は本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合として個人情報保護委員会規則で定める場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

■ 読み方の要点

- 追加されたのは「又は」以下の類型のみで、「本人への通知が困難な場合」は改正後も存置される。
- 追加類型は「委員会規則で定める場合」に限定され、事業者が自ら低リスクと評価すれば足りるものではない。
- 「であって」以下は両類型に共通の要件であり、代替措置をとらずに通知を省略することはできない。

既存通知のみなし規定はなく、施行日以後の事案に新基準が適用される。

★POINT

省略できるのは規則で定める場合に限られ、かつ代替措置が要件。判断過程を記録に残す。

本人通知の要否 — 判断のフロー

① 26条1項・規則所定の報告対象事態に該当するか（該当しなければ本人通知義務は生じない）



② 26条2項ただし書の場面に該当するか — 次の(a)又は(b)のいずれかに当たること

(a) 本人への通知が困難な場合（改正前から存置）

又は

(b) 本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合として個人情報保護委員会規則で定める場合【新設】



③ 本人の権利利益を保護するため必要なこれに代わるべき措置をとること — (a)(b)いずれの場合にも共通する要件



②のいずれか+③を満たす場合に限り本人通知を省略できる。満たさない場合は本人通知が必要（26条2項本文）。

★POINT

(b)は委員会規則で定める場合に限られ、自社評価のみでは省略できない。判断者・時点・根拠を記録する。

新設される(b)類型 — どのような場合が想定されるか

- (b)は「本人への通知が行われなくても本人の権利利益の保護に欠けるおそれが少ない場合として個人情報保護委員会規則で定める場合」である。具体的な範囲は今後の規則で定められるが、これまでの議論からは、次のような考慮要素に基づいて類型化されることが見込まれる。

考慮要素	「おそれが少ない」方向に働く事情	「おそれが大きい」方向に働く事情
漏えいした情報の性質	内部管理用の識別子のみ、単体では意味をなさない値	氏名・連絡先・ID・属性の組合せ、要配慮個人情報
情報単体で生じ得る不利益	なりすまし・勧誘・詐欺に用いることが困難	そのまま連絡・接触・認証に利用できる
他の情報との照合可能性	照合し得る情報が外部に存在しない	既に流出している情報と組み合わせで本人を特定できる
漏えい先・誤送付先の属性	取引先等の信頼できる相手方で、契約上の守秘義務がある	漏えい先が不明、又は不特定多数が閲覧し得る状態
回収・削除等の状況	開封前に回収、削除の確認済み、暗号化により復号不能	回収不能、既に閲覧・複製された形跡がある
本人に求められる行動	本人が何らかの対応をとる必要がない	パスワード変更・カード再発行等の防御行動が必要

報告対象事態のうち③（不正の目的をもって行われたおそれがある事態）は、その性質上(b)には乗りにくい。要配慮個人情報を含む①も同様である。実務上、(b)が問題となるのは主として④（1,000人超）の類型と考えられる。

★POINT

(b)は「軽微だから」ではなく「本人が何もしなくてよいといえるか」で判断される類型である。

通知の代替措置 — 公表以外の方法

■ 代替措置は新概念ではない

- 代替措置は現行26条2項・通則ガイドラインに既にある枠組みである。改正は、その適用場面に規則で定める低リスク類型を追加するものととどまる。
- 国会審議では「HP公表だけで済ませるのではないか」との懸念に対し、政府は規則で限定し委員会への報告を通じて判断する旨を答弁した。附帯決議第10項も、具体的な対象範囲・判断基準を規則で明記することを求めている。

■ 公表以外の代替措置の具体例

- 問合せ窓口の設置・周知：窓口を設けて連絡先を公表し、本人が自らが対象かを確認できるようにする。
- 部分通知＋公表の組合せ：連絡先が判明している本人には個別通知し、不明分を公表・窓口でカバーする。
- 既存チャネルを通じた周知：アプリ内通知・会員ページ・取引画面等、本人が通常確認する経路での告知。

上場企業では、漏えい公表と適時開示・記述情報の記載を一体で設計し、広報・IR部門を初動から関与させることが実務上の要点となる。

★POINT

「公表だけ」で済ませない。窓口設置・部分通知・既存チャネル周知を組み合わせ、記録に残す。

参考：報告・本人通知が問題となる事案類型

- 以下は現行実務の整理。判断の骨格は施行後も変わらないが、規則により違法な第三者提供が報告対象事態に追加され、速報の免除・取りまとめ確報が導入される見込みである。

事案類型	報告対象事態	実務上の勘所
不正アクセス・ランサムウェア	③（不正の目的）	暗号化により内容を確認できなくても「漏えいのおそれ」として報告対象。復旧作業と並行して速報を行う
委託先・従業員によるデータ持出し	③（＋④）	委託元・委託先の双方に義務。委託先は委託元へ通知すれば免除（26条1項ただし書）。大規模事案では本人通知が数百万件規模になる
クラウドの設定ミス・権限誤り	①②④のいずれか	外部から閲覧可能な状態にあったこと自体で「おそれ」。アクセスログがなければ閲覧の不存在を示せず、全件を対象とせざるを得ない
メール誤送信・郵送物の誤送付	①（要配慮を含む場合）	1件でも要配慮個人情報が含まれれば報告対象。回収・削除の確認ができれば代替措置の余地がある
端末・記録媒体の紛失・盗難	類型該當時のみ	高度な暗号化等の秘匿化措置が講じられていれば、そもそも「漏えい等」に該当しないと整理し得る（通則GL）

個人情報への漏えい等報告は年間1万件を超える水準で高止まりしている。件数の多くは誤送信・誤送付だが、本人通知の負担が大きいのは③の類型である。

★POINT

判断の骨格は維持。もっとも報告対象事態と報告手続にも規則レベルの見直しが入る。

上場企業のインシデント対応 — 三つの時間軸を並走させる

① 個人情報への報告

速報おおむね3～5日以内／確報30日以内（不正の目的による事態は60日以内）。法定義務で期限が明確。事実関係が固まっていなくても速報する。

② 本人への通知

事態の状況に応じて速やかに。省略には規則所定の類型＋代替措置が必要。判断者・時点・根拠を記録。改正後は命令により強制され得る（148条）。

③ 公表・適時開示

法定義務ではないが、投資判断に及ぼす影響の程度により要否を検討。有価証券報告書「事業等のリスク」の記述との整合も確認する。

■ 設計上の要点

- 三者は判断基準も時間軸も異なる。同一の規程に位置付け、判断の順序と責任者を事前に定めておかなければ、報告期限に追われて通知と開示の判断が後回しになる。
- 情報システム部門による事実把握 → 法務による権利利益侵害の評価 → 広報・IR部門による通知・代替措置・開示の設計。初動から並走させる。
- 委託先事案では、委託元名義での本人通知・問合せ窓口の設置を、あらかじめ委託契約で手当てしておく。

★POINT

個人情報報告・本人通知・適時開示を一本のフローに載せる。広報・IRを初動から関与させる。

PART

9

オプトアウト制度

制度の沿革・令和7年度実態調査・令和8年改正 — 「相手を見ない流通」は認められない

オプトアウトによる第三者提供とは（27条2項）

■ 本人の同意なく第三者提供できる例外 — 次の手続をすべて満たすことが要件

- ① あらかじめ通知等 — 法定事項を本人に通知し、又は本人が容易に知り得る状態に置く。
- ② 委員会へ届出 — 提供する個人データの項目・取得方法・提供方法・停止の求めの受付方法等（変更時も届出。27条3項）。
- ③ 委員会が公表 — 届出事項は個人情報委のサイトで公表される。
- ④ 停止の求めへ対応 — 本人の求めがあれば、当該本人が識別される個人データの提供を停止する。

■ オプトアウトで提供できないもの

- 要配慮個人情報／20条1項違反により取得された個人情報を含む個人データ／オプトアウトにより提供を受けた個人データ（再提供の禁止）。改正後は特定生体個人情報も除外。

■ オプトインとの違い — 本人の関与が入口から出口へ逆転する

- オプトイン（27条1項） — 本人が提供前に同意するかを決める。負担は同意取得と証跡管理に集中するが、提供できるデータに制限はない。
- オプトアウト（27条2項） — 先に提供が始まり、本人は「止める」側に回る。同意を取らない代わりに、公表の維持・提供先の管理・停止対応・記録の継続的運用を引き受ける。

★POINT

オプトアウトは「同意を取らなくてよい制度」ではなく、手続と継続的な運用を引き受ける制度である。

制度の沿革 — 濫用のたびに手続を積み増されてきた

平成26年

ベネッセ事案

- ・業務委託先の元社員が顧客情報を不正に取得し、約3,504万件を名簿事業者に売却
- ・名簿事業者が、本人が認知し得ないオプトアウトの方法で他の名簿事業者へ拡散
- ・オプトアウト手続厳格化の契機

平成27年改正

届出・公表と確認記録義務

- ・通知等事項の委員会への事前届出義務を新設
- ・委員会が届出事項を公表
- ・第三者提供時・受領時の確認・記録義務を新設（29条・30条）

令和2年改正

抜け道の封鎖

- ・要配慮個人情報オプトアウトの対象から除外
- ・20条1項違反により取得された個人情報の提供を禁止
- ・オプトアウト受領データの再提供を禁止（玉突き転売の遮断）
- ・届出事項の追加・不適正利用の禁止（19条）を新設

令和8年改正

提供先への視線

- ・特殊詐欺の「闇名簿」対策を背景に、提供先の氏名等・利用目的の確認を義務化（27条7項）
- ・提供先の虚偽回答の禁止、記録事項の追加
- ・特定生体個人情報の除外
- ・課徴金制度の導入と命令体系の再設計

執行も既に行われている。令和6年1月には届出事業者3社に行政指導（記録の不存在、転売先の用途を意図的に確認しなかった点が不適正利用（19条）に当たると指摘）、令和6年9月には不正に持ち出されたデータを購入した名簿販売事業者に指導、令和7年5月には特殊詐欺グループへの名簿販売を理由に、勧告を経ない初の緊急命令が発出された。令和7年度の監督実績は報告徴収19件、指導及び助言455件、勧告2件、命令1件である。

★POINT

改正の背景には、常に具体的な濫用事案がある。今回の起点は特殊詐欺の「闇名簿」である。

令和7年度実態調査（令和8年8月19日公表） — 出口の管理は道半ば

- 届出事業者261者（前回162者の約1.6倍）への任意調査。回答187者（回収率71.6%、未回答74者）。約9割の170者が公開情報から取得と回答。回答にはSaaS型DB・医療・ヘルスケア・人事異動情報等が並び、届出は名簿事業者だけの制度ではなくなりつつある。委員会は追加調査と、必要に応じた権限行使も検討するとしている。

調査項目	結果	委員会の方針
提供先の本人確認手続等	116者（62.0%）が実施。前回67.5%から低下	データの内容等を踏まえ必要に応じて実施するよう注意喚起
提供先の利用目的の確認	138者（73.8%）。登記情報提供では38.5%が未確認	内容等に応じて適切に確認するよう注意喚起
適正取得の確認方法	「GLに基づき適正に取得」等、具体性を欠く回答が一部	取得に当たり必要な確認等を行うよう注意喚起
本人が容易に知り得る状態	185者が対応済み・92.5%がHP掲載。導線の具体性を欠く	適切な対応を行うよう注意喚起
提供記録	記録漏れ「無」98.9%。記録様式等を提出できたのは67.4%	回答の裏付け（記録様式等）の確認が想定される

委員会は同日付で、この調査結果を踏まえた注意喚起を届出事業者に発出している（次頁）。

★POINT

問われるのは「実施しているか」ではなく「証跡で説明できるか」である。

注意喚起（令和8年8月19日）① 取得と提供先の確認

- 個人情報保護委員会は、実態調査と同日付で、届出事業者に対する注意喚起を発出した。求められた対応は5項目であり、その多くは令和8年改正で法律上の義務となる内容と重なる。

■ ① 提供データの適正な取得（27条2項）

- 回答のあった実務例：取得元を、本人が所属する企業等のホームページ、信頼性が高いと考えられる新聞・雑誌、官公庁が法令・制度に基づき公開している情報、商業登記・不動産登記等に限定する。
- 第三者から提供を受ける場合：本人が直接提供した情報であり、かつ本人の同意に基づき第三者提供されていることを確認し、利用規約等の変更の有無を定期的に確認する。
- 取得の経緯の確認（30条1項2号）の結果、提供元が不正の手段により取得したことを知り、又は容易に知ることができるにもかかわらず取得した場合、及び提供元が27条1項に違反して提供しようとしていることを知り、又は容易に知り得るのに取得した場合は、20条1項違反のおそれがある。

■ ② 提供先が19条の方法で利用しないことの確認

- 確認していないとの回答が一部にあった。実務例：提供先の利用目的を確認したうえで目的外利用を禁止する契約を締結する／提供前に提供先の企業審査を実施し、不法・不当な利用のおそれのある事業者には提供しない。

■ ③ 提供先に対する本人確認手続等

- 令和7年に提供実績のある届出事業者の約3割が未実施と回答。実務例：身分証明書の提示依頼／所属協会・免許番号の確認／住所地への通知送付と到達確認／法人担当者の権限の確認／契約書への実印捺印と印鑑証明書の添付。

★POINT

①～③は、改正法27条7項の提供先確認義務を先取りする内容である。施行を待たずに整備する。

注意喚起（令和8年8月19日）② 周知・手数料・届出

■ ④ 届出事項を「本人が容易に知り得る状態」に置くこと（27条2項）

- 意義：事業所の窓口等への掲示・備付けやホームページ掲載その他の継続的方法により、本人が知ろうとすれば時間的にも手段においても簡単に知ることができる状態。事業の性質及び個人情報の取扱状況に応じ、本人が確実に認識できる適切かつ合理的な方法によらなければならない。
- 該当する例：本人が閲覧することが合理的に予測されるホームページの分かりやすい場所（トップページから1回程度の操作で到達できる場所等）への継続的掲載／事務所の窓口等への継続的な掲示・備付け／本人に頒布される定期刊行物への定期的掲載／電子商取引で商品紹介ページにリンク先を継続的に表示する場合。
- 単に自社ホームページに掲載することが必ずしも要件を満たすわけではない。実態調査では、届出事項の記載が不十分な事業者が確認された。

■ 手数料に関する記載の是正

- 第三者提供の停止の求め等に対しても手数料を徴収するかのような印象を与えかねない記載が確認された。手数料を徴収できるのは、利用目的の通知を求められたとき（32条2項）又は開示の請求を受けたとき（33条1項）に限られる（38条）。

■ ⑤ 変更・提供の中止・越境提供

- 提供項目・取得方法・提供方法・停止の求めの受付方法・更新方法・提供開始予定日の変更は、あらかじめ本人への通知等＋委員会への届出。氏名・名称・住所・代表者氏名の変更、及び提供をやめたときは、遅滞なく本人への通知等＋届出。
- 外国にある第三者への提供は、原則としてあらかじめ本人の同意が必要（28条）。

★POINT

自社サイトの記載は、掲載場所・記載事項・手数料の文言の3点を今すぐ点検する。

令和8年改正 ― オプトアウトに関わる4点

改正項目	内容	根拠条文
① 提供先の確認義務	オプトアウト提供に当たり、あらかじめ提供先の氏名又は名称・住所（法人は代表者の氏名）と、提供先における当該個人データの利用目的を確認しなければならない	27条7項
② 虚偽回答の禁止	確認を求められた提供先は、確認事項を偽ってはならない。違反には10万円以下の過料（令和9年1月17日先行施行）	27条8項・186条1号
③ 記録事項の拡張	オプトアウト提供の記録に、①で確認した事項（提供先の氏名等・利用目的）が加わる。確認と記録はセットで運用する	29条1項
④ 特定生体個人情報の除外	顔特徴データ等は、要配慮個人情報と同様、オプトアウトによる第三者提供の対象から除外される	27条2項

背景：届出事業者である名簿事業者から、特殊詐欺・強盗等の犯罪グループが用いる「闇名簿」へデータが流入した事案。提供先の利用目的等を確認する義務がない現行法では、不適正利用の禁止（19条）を履行する手段が乏しいと指摘されていた。衆参附帯決議 第11項も、届出事業者への監視・監督の徹底と、闇名簿への流用等が判明した場合の緊急命令・課徴金納付命令の速やかな発出を求めている。

【下位法令】提供先の名称・住所等の確認方法（27条7項柱書）、例外事由に係る公開主体及びこれに準じる例外事由（同項ただし書）は、いずれも委員会規則で定められる。

★POINT

提供元だけでなく提供先にも真実義務が課される。名簿流通は「相手を見ない流通」ができなくなる。

提供先確認義務（27条7項） — 適用はデータセット単位で判定する

Q1 提供の根拠は

オプトアウト（27条2項）による提供か。本人同意による提供、委託・事業承継・共同利用（27条5項）は別枠。まず提供の根拠を特定する。



Q2 全部が公開情報等か

提供する個人データの「全部」が、取得の時点で本人、国の機関、地方公共団体、学研究機関等、報道機関、著述業、宗教団体、政治団体（57条1項各号）等により公開されていたものか。



Q3 非公開情報の混在は

自社取材、現地調査、本人からの直接取得、第三者からの受領データが混ざれば「全部」の要件を満たさない。データクレンジングで非公開情報を追加した瞬間に例外から外れ得る。



結論

Q2が「全部」でなければ、提供のたびに提供先の氏名等・住所・代表者氏名と利用目的を確認し、記録に残す。確認の方法は委員会規則で定められる。

「公開情報が中心」では足りない。要件は「全部」であり、取得元ごとの証跡で示す必要がある。

★POINT

任意の実務だった「提供先の確認」が法律上の義務になる。まず取得元をデータセット単位で棚卸しする。

データを「買う側」への影響 — 上場企業の宿題

■ 現行法でも受領者に課されている義務

- 確認義務（30条1項） — 提供元の氏名等・住所（法人は代表者氏名）と、提供元による取得の経緯。確認の結果、提供元の不正取得又は27条1項違反を知り、若しくは容易に知り得るのに取得すれば、買い手自身が20条1項違反となるおそれがある（令和8年8月19日注意喚起）。
- 記録義務（30条3項） — 受領年月日・提供元の氏名等・本人の氏名等・データ項目を記録し、原則3年間保存。
- 再提供の制限（27条2項） — オプトアウトで受領したデータは、オプトアウトで再提供できない。
- 不適正利用の禁止（19条） — 違法又は不当な行為を助長・誘発するおそれがある方法での利用は、買った側の違反になる。

■ 改正後に加わる3つの宿題

- ① 回答体制 — 提供元から自社の名称・住所・代表者氏名と利用目的を確認される。偽れば10万円以下の過料（27条8項・186条1号）。営業・購買担当者が回答する場面を想定した社内ルールが要る。
- ② 利用目的の文書化 — 曖昧な回答は取引が止まる理由になる。購入するデータごとに利用目的を文書化しておく。
- ③ 調達先の点検 — 命令に従わない事業者には、役務提供者にも中止措置が要請され得る（148条・148条の2）。調達先が執行対象となれば自社業務にも影響が及ぶ。

公表情報のみから取得している場合は確認・記録義務の対象外だが、公表情報と非公表情報が混在した瞬間に義務が生じる。

★POINT

提供側の改正として語られがちだが、リストを買う企業には回答体制・利用目的の文書化・調達先点検の宿題が残る。

PART

10

命令体系の再設計・課徴金制度・罰則の強化

「違反しても儲かる」構造を断つ — 「出口」の中核（148条以下・176～186条）

命令体系の再設計（148条・148条の2）

■ ① 本人保護命令への拡張（148条）

- 委員会の命令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の保護に必要な措置まで対象となる。
- 違法な第三者提供・大規模な不正利用の事案では、どの本人に・いつ・何を通知するかまでが命令の対象となり得る（適用関係は附則7条）。

■ ② 違反補助者への措置要請（148条の2）

- 違反行為を補助する第三者（ホスティング・クラウド・プラットフォーム・データ流通インフラ等）に、中止のための必要な措置を要請できる。
- 違反主体への命令だけではインフラを通じた違反の継続を止めにくいという現状への対応である。要請ではあるが実務上の重みは大きい。

上場企業にとっては、本人通知命令・公表命令が適時開示・記述情報の記載と直結する点に留意が必要となる。

★POINT

命令は「やめさせる」だけでなく「本人対応・公表」まで及び、周辺インフラにも波及する。

課徴金制度導入の背景 — 「やり得」の解消

■ 立法事実 — 「やり得」の構造

- 漏えい等報告は年間1万件超で高止まりし、名簿流通・「闇名簿」など、違反から生じた経済的利得が違反者の手元に残る構造が放置されていた。

■ 現行法の限界 — 間接強制のみ

- 勧告 → 命令 → 命令違反への罰則という段階構造であり、命令に従えば金銭的制裁がない。「指摘されたらやめればよい」となり、悪質事案への抑止力を欠いた。

■ 導入までの経緯 — 三度目の検討で実現

- 平成27年改正・令和2年改正の検討でも浮上したが見送られた。令和6年12月の検討会報告書 → 令和8年1月の制度改正方針で導入が確定した。
- 経済界の萎縮懸念と消費者側の推進論が対立し、対象行為を悪質類型に限定する「スモールスタート」で決着した。

独占禁止法・金融商品取引法・景品表示法で定着した利得剥奪型のモデルを採用。GDPR型の売上高連動制裁金は不採用とされた。

★POINT

立法趣旨は「やり得の解消」。平時のコンプライアンス体制の整備が最良の防御となる。

課徴金の対象行為と成立要件

■ 主な課徴金対象行為（148条の3関係）

- ① 違法な行為又は不当な差別的取扱いを行うことが想定される第三者への提供等（19条違反のうち一定のもの）。
- ② 不適正取得（20条1項違反）により取得した個人情報を利用する行為。
- ③ 本人同意のない違法な第三者提供（27条1項違反）。
- ④ 統計作成等の特例に違反する目的外利用又は第三者提供（特例取得データを統計化せず販売・広告配信等に用いる行為）。

■ 成立要件による絞り込み

- 対価要件：違反行為又は違反行為をやめることの対価として金銭その他の財産上の利益を得たこと。
- 違反行為を防止するための相当の注意を怠った者でないと認められる場合は対象外。
- 対象となる本人の数が1,000人を超えないときは対象外。個人の権利利益を害する程度が大きい場合として政令で定めるときも対象外。

安全管理措置義務違反一般は、課徴金対象行為の中心には置かれていない。

【下位法令】課徴金額の算定方法、「権利利益を害する程度が大きい場合」、消滅・事業譲渡等の場合（148条の7第6項）は政令。推計方法・減額のための報告方法・弁明の機会の付与に係る通知の方法等は委員会規則。「相当の注意を怠った者でないと認められる場合」の考え方はガイドラインで示される。

★POINT

帰責性・大規模性・侵害重大性で絞り込まれた制度であり、自動的に課される制度ではない。

算定・推計・加算・減額と「相当の注意」

項目	内容
算定	違反行為により得た利益に相当する額として政令で定める方法により算定する。事業規模に応じた定率型ではなく、利得剥奪型
推計	報告・資料提出に応じない場合、規則で定める合理的な方法により推計できる
加算	過去10年以内に課徴金納付命令を受けたことがある場合は1.5倍
減額（リニエンスー）	調査前の自主報告により50%を減額
手続	弁明の機会の付与等。行政手続法の適用除外を含む
「相当の注意」	審査体制・契約統制・アクセス制御・教育・監査・目的外利用防止措置が判断要素となり得る。事業者側が示す必要がある

海外事業者へは領事送達により納付命令書を送達し、国内に財産があれば民事執行法等により執行する。

国会審議では、安全管理措置義務違反（23条）が対象行為に含まれない点に強い批判が示されたが、政府は態様の多様性と算定の困難性を理由に挙げた。現行の課徴金は「スモールスタート」であり、水準・対象要件は附則14条の3年ごと見直しで拡大され得る前提で体制を作る。

★POINT

リニエンスーがある以上、違反を発見した際の自主報告の意思決定ルートを事前に定めておく必要がある。

罰則の新旧比較（176条・178～180条・186条）

対象	改正前	改正後
不正提供・盗用（178条・179条）	1年以下の拘禁刑／50万円以下の罰金	2年以下の拘禁刑／100万円以下の罰金
主観的要件の拡張（178条・179条）	「不正な利益を図る目的」	「本人その他の者に損害を加える目的」も追加
不正取得罪（180条・新設）	—（独立の処罰規定なし）	2年以下の拘禁刑／100万円以下の罰金
委員会の命令違反等（176条）	拘禁刑を含む規定	法定刑の引上げ・拘禁刑への整理（法人重科を含む）
オプトアウト確認の虚偽回答（186条1号・新設）	—（過料なし）	10万円以下の過料（公布後6か月で先行施行）

不正取得罪は、欺罔・暴行・脅迫や、個人情報保有者の管理を害する行為による取得を新たに処罰対象とする。

★POINT

「だまして取る」段階から処罰される。退職者・委託先経由の持出しは実刑リスクを伴う水準になる。

提供元の責任と課徴金（参議院・令和8年6月17日）

■ 設例

- 提供元が、提供先から「統計作成等特例の範囲内のAI開発に用いる」との説明を受けて契約したが、提供先が実際には個人プロファイルの作成や検索可能なAIに用いていた場合、提供元も課徴金の対象となるか。

■ 政府答弁（個人情報保護委員会事務局長）

- 個別判断としつつ、提供元が「相当の注意」を尽くしていれば、提供元の責任は認められず、課徴金の対象外となる可能性が高い。
- 他方、提供先の説明を単に鵜呑みにしただけでは、注意を払ったとはいえず、課徴金の対象となり得る。

■ 実務対応

- 提供先の宣言（利用目的・必要データ・体制・秘匿処理能力）を書面で受領し、審査した記録を残す。
- 契約に、利用範囲の限定・監査権限・違反時の是正／解除・報告義務を置き、提供後も公表内容と実際の取扱いの整合を定期的に確認する。

★POINT

提供元の免責は「契約の文言」ではなく「審査した記録」で決まる。

PART

11

衆参附帯決議と下位法令の方向

各14項目の附帯決議が、委員会規則・ガイドラインを先取りする最重要資料となる

衆参附帯決議（各14項目）の骨格

■ 決議の概要

- 衆議院：令和8年5月21日・地域活性化・こども政策・デジタル社会形成に関する特別委員会（14項目）。
- 参議院：令和8年7月8日・デジタル社会の形成及び人工知能の活用等に関する特別委員会（14項目）。

■ 主要項目

- 第1項 規則等の策定過程における意見聴取と、政策決定過程の透明性・予見可能性の確保。
- 第2・3項 AI開発等が過度に萎縮しない配慮と、統計作成等における再識別防止措置の確実な実施。
- 第4項 統計作成等目的の要配慮個人情報取扱いに係る安全管理措置・委託先監督の徹底（参院は重点監督化）。
- 第5項 プロファイリング規制の在り方の継続検討。第6項 PETsの活用促進とインセンティブの検討。
- 第7～10項 同意例外・こども・特定生体・通知の代替措置について、具体的範囲・判断基準を規則で明記。
- 第11・12項 オプトアウト届出事業者への監視監督の徹底、緊急命令・課徴金納付命令の的確な発出、課徴金運用の透明性。
- 第13・14項 団体による差止請求・被害回復制度の継続検討、委員会の人員・予算の充実。

★POINT

附帯決議は、委員会規則・ガイドラインが何を書くかの「予告編」として読む。

衆参の比較 — 骨格は共通、参院で具体化

論点	衆議院	参議院の追加・強化点
統計の解釈（2・3項）	再識別防止措置・概念の狭隘化の防止	AIモデル等による識別・要配慮情報の推知リスクの勘案を明記
公表・監督（3項）	個人情報による状況把握・情報公表	外国企業を含む事業者のモニタリング・報告徴収を明記
要配慮（4項）	安全管理措置・委託先監督の徹底	重点監督化、医療分野GLの改正、守秘義務・研究倫理指針との関係の明確化
PETs（6項）	インセンティブの在り方の検討	技術動向の調査研究・事業者による積極的な活用の促進を追加
同意不要の例外（7項）	範囲・判断基準の明記	「契約の履行のために必要やむを得ない場合」を明示、必要最小限を明記
特定生体（9項）	機器周辺への掲示	検知対象者が十分認識できる場所等への掲示を追加
課徴金（12項）	運用の透明性	将来の課徴金額の見直し・対象要件の継続検討を明記

★POINT

二院目・審議終盤ほど論点が積み上がる。参院決議は「宿題リスト」の完成形である。

実務上重要な3点

■ ① PETsの位置付けの引上げ（両院第6項・参院第3項）

- 「基盤モデルの学習は匿名化ではない」との参考人指摘を受け、入力データの削除・仮名化にとどまらず、モデル出力からの再識別・推知可能性の検証を安全管理措置の一部として位置付ける必要がある。PETsの重畳的適用が実務上の標準となる方向が示された。

■ ② 要配慮個人情報の「重点監督」化と医療分野の別扱い（参院第4項）

- 要配慮個人情報を統計特例から除く修正案が否決された一方、法文で落とした歯止めを決議＋規則・ガイドラインに委ねる立法技術がとられた。医療・ヘルスケア・研究機関はガイドライン改正が最重要論点となる。

■ ③ 見送られた制度の将来検討の明記

- プロファイリング規制（両院第5項）・課徴金の対象／水準（参院第12項）・団体差止／被害回復（両院第13項）は、附則14条の3年ごと見直しに向けた継続検討課題として残る。

★POINT

規則・ガイドラインのパブリックコメントが、実務要件を左右する最大の関与機会となる。

PART

12

施行スケジュールと上場企業の実務対応

6か月先行組と本体組を分けて、棚卸しから先行的に着手する

施行期日・経過措置・3年ごとに見直し

■ 施行期日

- 原則施行（附則1条本文）：公布日（令和8年7月17日）から2年を超えない範囲＝令和10年7月16日までの政令指定日。
- 先行施行（附則1条3号）：罰則関係等の一部は令和9年1月17日（公布後6か月）。公布日施行（附則13条・16条）・特別施行（附則17条）の部分もある。

■ 経過措置（みなし規定）

- 特定生体個人情報（附則4条）／16歳未満（附則5条・6条）／命令の適用関係（附則7条）／課徴金（附則8条）／番号法・次世代医療基盤法（附則9～12条）。
- 他方、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となる。

■ 3年ごとの見直し（附則14条）

- 施行後3年ごとに、国際動向・情報通信技術の進展・新産業の状況等を勘案して検討する。AI・こども保護・生体情報・課徴金運用が今後の主要テーマとなる。

★POINT

みなし規定があっても新法水準を満たすかの再評価は必要。「6か月組」と「本体組」を分けて準備する。

施行スケジュールと個人情報委のロードマップ（案）

2026年	2027年前半	2027年後半	2028年
公布・全体像の提示 ・7月17日 公布（法律第56号） ・7月31日 個人情報委「今後の取組（案）」 ・8月26日 全体像（案）／9月9日 進め方の具体化 ・9月以降 分類・テーマごとに委員会で議論	先行施行・意見募集 ・1月17日 先行施行（罰則関係等・虚偽回答の過料） ・1～3月頃 政令・規則の意見募集 → 公布 ・ガイドライン・Q&Aの検討	GL整備・周知 ・ガイドライン・Q&Aの意見募集 → 公表 ・特定分野のガイドラインも随時整備 ・全国での説明会・広報	本体施行 ・春～7月に本体施行（期限は令和10年7月16日） ・施行後3年ごとの見直し（附則14条） ・執行方針・事務局レポートの公表を検討

個人情報委は、政令等において新設された義務・特例の対象となる要件や想定事例を可能な限り明確に示す方針を示している。課徴金・統計作成等特例に係る執行体制の強化・専門人材の確保も掲げられている。

★POINT

2027年前半の規則パブコメ、2027年中のGL公表、2028年前半施行が軸。社内計画をこれに合わせる。

政令・規則等で定める事項の全体像（案）① 利活用の推進

- 個人情報保護委員会事務局が令和8年8月26日に公表。どの論点がどのレベル（政令／委員会規則／GL・Q&A）で具体化されるかが示された。「個人情報の保護に関する基本方針」（平成16年4月2日閣議決定）も見直される。

テーマ	政令	委員会規則	GL・Q&A
統計作成等の特例	—	権利利益を害するおそれが少ないもの（2条13項）／公表の内容・方法、基準適合体制の内容等（30条の2、31条の3、72条の3）	考え方・具体事例
本人の意思に反しない場合	—	本人の意思に反しないため権利利益を害しないことが明らかな場合（18条3項7号・20条2項7号・27条1項8号）	同上
同意取得困難性要件の緩和	—	—（委任なし）	考え方・具体事例（公衆衛生の向上のため特に必要な場合を含む）
学術研究例外の明示	—	—（委任なし）	考え方・具体事例

「相当の理由」による緩和と学術研究例外には政令・規則の委任がなく、GL・Q&Aのみが手掛かりとなる。

★POINT

利活用側の中心は委員会規則。とりわけ2条13項の「おそれが少ないもの」の範囲が実務を左右する。

政令・規則等で定める事項の全体像（案）② リスク対応

テーマ	政令	委員会規則	GL・Q&A
こどもの個人情報	利用停止等請求の例外事由（35条9項12号）	取得の状況からみて権利利益を害しないことが明らかな場合（同項8号）／公開主体（同項9号）	考え方・具体事例
顔特徴データ等	対象となる身体の一部の特徴に係る情報（16条5項）／周知義務の例外（21条の2第2項4号）／利用停止等請求の例外（35条7項10号）	周知方法・周知事項（21条の2第1項柱書・6号）／利用停止等請求の例外（35条7項9号）	考え方・具体事例
委託先における適正な取扱い	—	義務免除の前提として委託契約で定める事項及び契約の方法（58条の2）	考え方・具体事例
漏えい等報告・本人通知	—	通知の要否（26条2項・68条2項1号）／速報の免除・取りまとめ確報・違法な第三者提供の報告対象化（26条1項）	考え方・具体事例

顔特徴データは、対象範囲が政令、周知の方法・事項が規則という二層構造になる。掲示の文言と場所は規則案の段階で自社運用と突き合わせる。委託先規律も、契約に定めるべき事項が規則で示されるため、ひな形改定はその公表を待つ。

★POINT

リスク対応側は政令と規則に分かれる。自社の重点テーマがどちらで決まるかを把握しておく。

政令・規則等で定める事項の全体像（案）③ 不適正利用防止と執行

テーマ	政令	委員会規則	GL・Q&A
連絡可能個人関連情報	—	特定の個人への連絡その他の情報の伝達に利用できる記述等（2条8項5号）	考え方・具体事例
オプトアウト制度の強化	—	提供先の名称・住所等の確認方法（27条7項柱書）／例外事由に係る公開主体及びこれに準じる例外事由（同項ただし書）	考え方・具体事例
勧告・命令等の実効性確保	—	—（委任なし）	考え方・具体事例
課徴金の導入	課徴金額の算定方法（148条の3第1項・2項）／権利利益を害する程度が大きい場合／消滅・事業譲渡等の場合（148条の7第6項）	推計方法、減額のための報告方法、弁明の機会の付与に係る通知の方法等（148条の4・6・10第2項・17）	考え方・具体事例（特に「相当の注意を怠った者でないと認められる場合」を含む）

上場企業の注視点は2つ。課徴金の「権利利益を害する程度が大きい場合」は政令事項であり、1,000人要件に加えてどこまで対象外となるかがここで決まる。他方、「相当の注意を怠った者でないと認められる場合」の考え方はガイドラインで示されるため、平時の体制整備の水準はそちらを見て設計することになる。

★POINT

課徴金の対象外要件は政令、「相当の注意」の考え方はガイドライン。見るべき文書が分かれている。

今後の進め方（案）ー パブリックコメントまで

STEP 1

基本的な考え方の議論

- ・ 2026年9月以降
- ・ 委員会が分類・テーマごとに提示
- ・ 制度趣旨と国会審議を踏まえる
- ・ 論点を数回に分けて議論

STEP 2

意見交換・ヒアリング

- ・ 個人の立場の団体
- ・ 事業者の立場の団体
- ・ 個別又はグループごと
- ・ 委員会の会合に応じて実施

STEP 3

具体的内容の議論

- ・ 政令・規則で定める具体的内容
- ・ 委員会で提示・議論
- ・ 各論点を数回程度に分けて
- ・ 並行して意見交換を継続

STEP 4

条文案とパブコメ

- ・ 政令・規則の条文案を提示
- ・ 委員会で議論
- ・ 意見公募手続を開始
- ・ その後ガイドライン・Q&Aへ

- ・ この進め方は令和8年8月26日の第366回個人情報保護委員会で決定されたものであり、その具体的な実施方法は令和8年9月9日公表の事務局資料で示された（次頁以下）。事業者側の関与機会は、STEP 2・3の団体ヒアリングと、STEP 4のパブリックコメントの二段階にある。業界団体を通じた意見提出を想定する場合、9月以降の議論の進み方を追いながら、遅くとも年内には論点と主張を固めておく必要がある。

自社にとって影響の大きいテーマ（統計作成等特例、顔特徴データ、委託先規律、課徴金の対象外要件等）を特定し、委員会資料の公表に合わせて確認する担当を決めておく。

★POINT

9月以降、テーマごとに議論が始まる。パブコメを待つのではなく、議論の段階から論点を追う。

意見交換会・事務局ヒアリング（令和8年9月9日公表）

8月26日の「今後の進め方」は第366回個人情報保護委員会（令和8年8月26日）で決定された。これを具体化する実施方法が、令和8年9月9日の事務局資料「政令・規則・ガイドライン等の整備に関する今後の進め方（案）について」で示された。柱は「マルチステークホルダー連携プロセス」である。

多様な個人の立場から御意見を伺う団体（9団体）

ECネットワーク／Consumer Rights Japan／全国消費者団体連絡会／日本若者協議会／Privacy by Design Lab／MyDataJapan／全国消費生活相談員協会／サステナビリティ消費者会議／主婦連合会

※ もう一方の立場の団体もオブザーバーとして参加可

事業者の立場から御意見を伺う団体（8団体）

新経済連盟／データ社会推進協議会／電子情報技術産業協会（JEITA）／日本IT団体連盟／日本経済団体連合会／在日米国商工会議所（ACCJ）／Business Software Alliance／プライバシーテック協会

※ もう一方の立場の団体もオブザーバーとして参加可

意見交換会は、事務局が事務局ヒアリングに先立ち、テーマ・立場ごとに実施する。事務局ヒアリングは、双方の立場が混在する形で実施し、議事概要を委員会に報告のうえ公表する予定とされている。

出典：個人情報保護委員会事務局（令和8年9月9日）https://www.ppc.go.jp/files/pdf/260909_shiryou-1.pdf

★POINT

経団連・JEITA・新経連・日本IT団体連盟等が意見を述べる枠組み。加盟団体経由での意見提出を検討する。

当面のスケジュール（案）－ テーマ別の議論時期

9月9日資料では、委員会がどのテーマをいつ議論するかが示された。自社の重点論点がいつ俎上に載るかが分かる。

時期	委員会の議題	対象テーマ	本資料の該当章
2026年8月26日	政令・規則等で定める事項の全体像／今後の進め方	全体（第366回委員会決定）	第12章
2026年9月9日	意見交換会・事務局ヒアリングの概要	実施方法（本頁・前頁）	第12章
9月中旬	基本的な考え方①	こども／顔特徴データ／本人関与に関する規律	第4章・第7章
9月下旬～10月上旬	基本的な考え方②	統計作成等／委託先／漏えい等	第2章・第6章・第8章
10月中旬	基本的な考え方③	連絡可能個人関連情報／オプトアウト／課徴金	第3章・第9章・第10章
10月中旬～下旬	事務局ヒアリング（双方の立場が混在）	上記①～③を踏まえて実施	—
11月～12月	委員会・意見交換会を随時開催	具体的内容の議論	—
2027年1月～	意見募集（パブリックコメント）	政令・規則の条文案	—

統計作成等・委託先・漏えい等は9月下旬から10月上旬、オプトアウトと課徴金は10月中旬に議論される。意見を述べるなら、それぞれの回に間に合うよう社内の論点整理を終えておく必要がある。

★POINT

自社の重点テーマの回に合わせて準備する。パブコメ（2027年1月～）は最後の機会にすぎない。

優先的に棚卸しすべき6領域

領域	点検の視点
AI開発・分析・統計処理案件	統計作成等に乗るか／取得特例・公表・目的外利用禁止・再提供禁止／PETsの導入状況
顔認証・映像分析・生体認証	周知（21条の2）／オプトアウト禁止（27条2項）／利用停止等請求への対応
こども向け又は16歳未満を含み得るサービス	法定代理人対応（40条の2）／年齢把握／最善の利益（58条の3）
オプトアウト提供・営業リスト・名簿購入	提供先確認・記録（27条7項8項・29条）／連絡可能個人関連情報／買う側の回答体制
受託処理・クラウド・BPO・分析委託	30条の3／58条の2／クラウド例外の前提の維持／越境移転の根拠
違反による利益が事業収益に直結し得る事業	課徴金リスク／「相当の注意」を示せる体制と証跡

★POINT

まずは棚卸しと可視化から。どの改正条項・経過措置の影響を受けるかを類型別に見える化する。

上場企業の実務① 株主名簿・株主判明調査とIR／SR活動

■ 株主名簿と証券代行・調査会社への委託

- 株主名簿の作成・管理は会社法上の義務であるが、個人株主の氏名・住所は個人データである。証券代行・調査会社への処理委託は27条5項1号の委託として整理されるのが通常であり、改正後は受託者に30条の3の直接義務が及ぶ。
- 受託者が判明調査の過程で得たデータを自社のデータベース・業界知見として蓄積すれば、委託業務の遂行に必要な範囲を超える取扱いと評価され得る。委託契約に独自利用の禁止を具体的に列挙する。

■ IR／SR活動と個人株主への働きかけ

- 株主向けアンケート・メール配信・イベント案内に用いる連絡先を外部から補完取得する場合、連絡可能個人関連情報（2条8項・31条の2）の視点が及ぶ。取得元の適法性を説明できる証跡が必要となる。
- 議決権行使結果・アンケート結果の分析は、個人単位に戻らない限り統計作成等として整理し得るが、少数セルによる推知には注意する。

■ 越境移転

- 海外の議決権行使プラットフォーム・グローバル証券代行への情報連携は28条の越境移転規律の対象となり得る。基準適合体制の確認と情報提供の整理を行う。

★POINT

株主データは「会社法の義務だから」で完結しない。委託・連絡可能情報・越境の3点で再点検する。

上場企業の実務② 株主総会・従業員データ・人的資本開示

■ 株主総会の運営 ― 特定生体個人情報

- 会場入口での顔認証による入場管理、来場者の映像分析は、本人識別を目的とする場合、特定生体個人情報の規律（21条の2の周知／27条2項のオプトアウト禁止／35条7項8項の利用停止等請求）の対象となる。
- 掲示は「顔認証使用中」では足りず、事業者名・住所・代表者・利用目的・身体特徴情報の内容・開示等請求手続まで示す必要がある。附帯決議第9項は、検知対象者が十分認識できる場所等への掲示を求めている。

■ 従業員データと人的資本開示

- 男女間賃金差異・女性管理職比率等の開示指標は統計情報であるが、対象者が少数の場合、公表値から特定個人の処遇が推知され得る。少数セルの取扱いを開示方針にあらかじめ定めておく。
- エンゲージメントサーベイ・人材データ分析を外部委託する場合は、30条の3を前提に、受託者による横断分析・自社サービス改善への転用を契約で明確に禁止する。

■ 内部通報・ハラスメント調査

- 通報者・関係者の情報は要配慮個人情報を含み得る。同意例外の整理と、開示等請求への対応方針を規程で明確にする。

★POINT

IR・総務・人事の各業務が改正条項に直接当たる。部門横断でのデータ接点の棚卸しから着手する。

上場企業の実務③ 課徴金・命令と開示・ガバナンス

■ 命令・課徴金納付命令を受けた場合の開示

- 措置命令・課徴金納付命令は、投資判断に重要な影響を及ぼす事実として適時開示の要否を直ちに判断する必要がある。本人保護命令（148条）により本人通知・公表が命じられた場合は、その内容と開示の平仄を合わせる。
- 課徴金額は利得剥奪型であり、金額の多寡にかかわらず、命令を受けた事実自体のレピュテーション影響が大きい。広報・IRを初動から関与させる体制を用意する。

■ 記述情報への反映

- 有価証券報告書の「事業等のリスク」において、個人情報取扱いに係るリスクを、課徴金・命令・本人通知義務の導入を踏まえて更新する。コーポレート・ガバナンス報告書における体制記載との整合も確認する。

■ 取締役会による監督

- 「相当の注意を怠った者でない」ことを示すには、方針決定・体制整備・モニタリングの記録が要る。取締役会・監査等委員会への定期報告ルートを規程化する。
- 違反発見時に調査前の自主報告（50%減額）を選択できる意思決定ルートを、あらかじめ定めておく。

★POINT

課徴金導入により、個人情報コンプライアンスは開示事項でありガバナンスの課題となった。

施行までのアクションプラン

STEP 1

棚卸し（～2026年内）

- ・ 個人データの取得経路・提供先の一覧化
- ・ 委託・クラウド・生成AI利用の洗い出し
- ・ 顔認証・こども・営業リストの特定
- ・ 6か月先行施行部分の影響確認

STEP 2

差分の確認（2027年前半）

- ・ 改正条項ごとの適合／不適合の判定
- ・ 規則パブコメへの対応（業界団体経由を含む）
- ・ 統計作成等の利用可否の方針決定
- ・ PETsの導入方針の策定

STEP 3

文書の整備（2027年後半）

- ・ 委託契約・データ提供契約の改定
- ・ 利用規約・プライバシーポリシーの改定
- ・ 規程・インシデント対応フローの改定
- ・ ガイドライン公表後に手順を確定

STEP 4

体制と証跡（施行まで）

- ・ 取締役会への報告ルートの確立
- ・ 「相当の注意」を示す記録の様式化
- ・ 自主報告の意思決定ルートの整備
- ・ 教育・監査への組み込み

規則・ガイドラインの内容を待つ必要がある部分はあるが、棚卸し（どのデータをどの経路で取得し、誰にどこまで渡しているか）は今日から着手できる。

★POINT

「規則待ち」でよい部分と、いま着手すべき部分を分ける。棚卸しは規則の内容に左右されない。

本セミナーのまとめ

■ ① 「規制強化」でも「規制緩和」でもなく、構造改正である

- 統計作成等の特例（30条の2）等により本人同意なしで使えるルートが新設される一方、その利用は公表内容に厳格に固定され、目的外利用・再提供は禁止される。入口の緩和と出口の拘束はセットである。

■ ② 事業部門の日常業務がそのまま論点になる

- 株主名簿と判明調査、IR／SR活動、株主総会の入場管理、顧客データの分析とAI活用、営業リストの購入、人的資本開示、漏えい時の通知判断 — いずれも今回の改正条項に正面から当たる。法務だけの課題ではない。

■ ③ 執行の実効性が非連続に上がる

- 命令体系の再設計・課徴金・罰則の強化により、違反時のコストが従来と非連続に上昇する。課徴金の除外事由である「相当の注意」を示せるかは、平時の体制と記録で決まる。

附則14条の3年ごと見直しを踏まえ、一度きりの対応ではなく、継続的なデータガバナンス体制の構築が不可欠である。

★POINT

「使えるデータは使えるようにするが、逸脱には従来よりはるかに重い責任を課す」改正である。

■ CONTACT

お問い合わせ

弁護士法人三宅法律事務所

パートナー弁護士 渡邊 雅之

TEL 03-5288-1021（代表） ／ FAX 03-5288-1025

Email: m-watanabe@miyake.gr.jp

※本資料は令和8年7月17日公布の改正法（令和8年法律第56号）及び国会審議に基づく分析であり、一般的な情報提供を目的とするものです。今後の政令・委員会規則・ガイドライン等の整備状況を適宜ご確認ください。