

Web セミナー【後半】

令和 8 年改正個人情報保護法

「基本的な考え方①～③」で 何が決まる？

【後半】執行強化の新ルール — 委託先の規律(クラウド例外)・漏えい等報告と安全管理措置・オプトアウト制度・課徴金

委託先の規律

クラウド例外

漏えい等報告

安全管理措置

オプトアウト制度

課徴金

弁護士法人三宅法律事務所

パートナー弁護士 渡邊 雅之

個人情報保護委員会事務局
「政令・規則の整備に向けた基本的な考え方」①～③
(2026 年 9 月 16 日・10 月 1 日・10 月 14 日)を基に作成
2026 年 10 月

※ 本資料は令和 8 年改正法(令和 8 年法律第 56 号)及び個人情報保護委員会事務局「政令・規則の整備に向けた基本的な考え方」等に基づく一般的な情報提供です。「基本的な考え方」は方向性であり、政令・規則の条文は今後の意見募集を経て定められます。



まず 3 問、○か × か考えてみてください

①



名簿を同意なく 1,000 万円で販売（経費 900 万円）。課徴金は「利益の 100 万円」が基準になる

○？ ×？

②



SaaS の契約に「サービス改善に利用可」とあれば、預かったデータで自社 AI を学習させてよい

○？ ×？

③



社内 ID だけが漏えいした。改正後は本人への通知を省ける方向だ

○？ ×？

答えは各 PART で明かします

後半のポイントは、この 3 つです



委託先・クラウド例外

委託は
「契約」が要件に

全委託先に範囲外取扱いの
禁止。義務免除は規則所定の
事項を書面で



漏えい等・安全管理

省ける場面と
報告すべき場面が増加

社内 ID 等は通知代替、違法
提供は報告対象に。安全管理
GL は 2027 年 4 月



名簿・課徴金

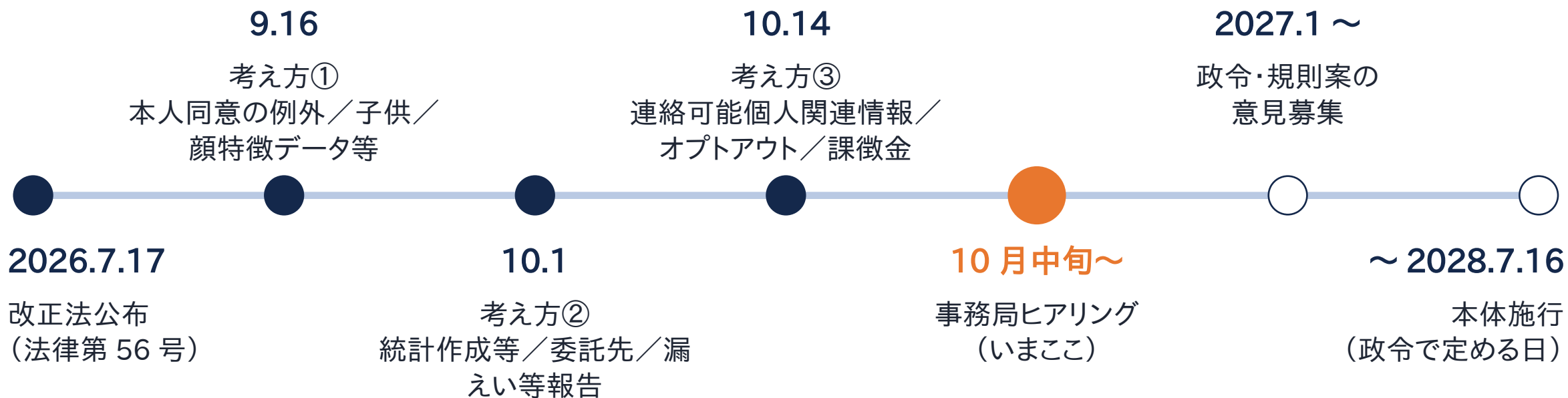
名簿は書類で確認
課徴金は対価の全額

身元は本人確認書類で検証。
経費は引かず、按分もしない

POINT

違反時のコストは非連続に上がる。平時の体制と記録が最良の防御

いまはどの段階か — 法律は確定、中身を詰めている



別ルート: 安全管理措置ガイドラインは **2027 年 4 月施行** 予定(改正法より先)

POINT

「施行まで 2 年ある」は誤り。この冬に意見募集が 2 回ある

法律・政令・規則・ガイドラインの関係

法律
国会

令和 8 年法律第 56 号。義務・特例・課徴金などの「骨格」

政令
内閣

施行令。例：特定生体個人情報の対象、課徴金の算定方法・対象外

委員会規則
個人情報保護委員会

施行規則。例：統計作成等の要件・公表方法、委託契約の事項、本人確認の方法

ガイドライン・Q&A
個人情報保護委員会

解釈と具体例。例：「相当の理由」「相当の注意」の考え方

 法律・政令・規則は「法令」。ガイドラインは解釈指針だが、「しなければならない」事項に従わないと **法違反と判断される可能性**

POINT 「基本的な考え方」= このうち **政令・規則の中身の方向性** を示したもの

「基本的な考え方①～③」とは何か

回	委員会(2026年)	主なテーマ	本セミナー
①	9月16日(第369回)	本人同意の例外／子供の個人情報／顔特徴データ等(＋安全管理措置 GL の見直し)	PART 8 (安全管理 GL)
②	10月1日(第370回)	統計作成等の特例／委託先の規律／漏えい等報告・本人通知	PART 7・8
③	10月14日(第372回)	連絡可能個人関連情報／オプトアウト制度／課徴金	PART 9・10

 法律は2026年7月17日公布で **確定済み**。「基本的な考え方」は政令・規則の **設計図** で、条文は意見募集(2027年1月～)を経て確定

POINT 「～としてはどうか」という方向性の提示。条文そのものではない

後半は PART7 ～ 11

7 委託先の規律

クラウド例外と MK システム事案／範囲外取扱いの禁止・義務免除〔考え方②〕

8 漏えい等報告・安全管理

本人通知の代替・速報免除・違法提供の報告〔考え方②〕／安全管理 GL の先行施行・10 月 7 日注意喚起

9 オプトアウト制度

提供先・提供元の身元確認と記録・届出事項〔考え方③〕／8 月 19 日注意喚起

10 課徴金

対象外の範囲・算定方法・推計・自主報告〔考え方③〕

11 実務対応と日程

棚卸し・上場企業の実務・アクションプラン

PART 7

委託先の規律

範囲外取扱いの禁止（30条の3）・義務免除（58条の2）〔基本的な考え方②〕

ここで分かること

契約に何を書けば、
委託先の義務が免除される？



「委託」は同意なしでデータを渡せるルート



委託元(自社)



データを渡す
(同意不要)



委託先

例:クラウド・SaaS / コールセンター / 発送代行
/ 給与計算 / システム保守



第三者に当たらない

27 条 5 項 1 号:委託に伴う提供
は本人同意なしでできる



委託元の監督義務

25 条:①委託先の選定 ②委託契
約 ③取扱状況の把握



委託先にも義務

委託先が個人情報取扱事業者な
ら第 4 章の義務も重ねて適用

POINT

同意なしで渡せる代わりに、委託元が「監督」で責任を負う仕組み

預けるだけなら「委託」ではない？ ― クラウド例外



利用事業者



保存



クラウド



クラウド事業者が
個人データを「取り扱わない」

- 契約で取り扱わない旨を定める
- 適切なアクセス制御を行う



判断基準

個人データが含まれるかではなく、事業者が「取り扱うこととなっているか」



効果

第三者提供にも委託にも当たらない
→ 本人同意も 25 条の監督も不要



注意

それでも利用事業者自身の安全管理措置は必要 (Q&A7-54)

POINT

「クラウドだから例外」ではない。「取り扱わない」ことが契約と技術で確保されているか

クラウド例外が否定されたー MK システム事案

2,754

利用していた社労士事務所

3,067 件

漏えい等報告(報告者ベース)

約 750 万人

報告された本人数の合計

2023 年 6 月 ランサムウェアで暗号化
2024 年 3 月 25 日 委員会が指導(147 条)・
報告徴収(146 条 1 項)

クラウド例外が否定された 3 つの要素



利用規約で、保守・運用上必要な場合に個人データを監視・分析・調査等できる



保守用 ID でアクセスでき、取得を防ぐ技術的なアクセス制御がなかった



確認書を取り交わし、実際に個人データを取り扱っていた

→ 委託を受けて個人データを取り扱う事業者に。利用者側は **委託(27 条 5 項 1 号)**として**監督(25 条)**が必要

POINT

規約・保守用 ID・確認書。「取り扱える状態」なら、クラウド例外は使えない

改正後、クラウドの整理はより厳密に問われる



GL 別添 10-6

指摘された不備

- パスワードが脆弱（管理者権限も類推可能）
- 更新が不十分で脆弱性を放置
- ログ監視が不十分で検知できず



改正後の整理

クラウド例外は残るが厳密に

- 取り扱うなら **30 条の 3** が直接適用
- 免除を使うなら契約に取扱いの方法
- 安全管理 GL 見直し（2027 年 4 月予定）

- ✓ 利用者のチェック: ①規約に「個人データを一切取り扱わない」と明記 ②矛盾する覚書・確認書がない ③保守用 ID・アクセス制御

POINT 「クラウドだから当然例外」は通用しない。契約・技術・運用の三面で確かめる

委託先の独自利用、典型は 6 類型



① 自社の改善

受託データで自社プロダクトの品質を向上



② AI の学習

汎用モデル・他案件のモデルの学習に



③ 横断分析

複数の委託元のデータを混ぜて分析



④ 別サービス開発

新規サービスの企画・検証に



⑤ 営業への転用

受託データから見込み客を抽出



⑥ 自社 DB へ蓄積

自社 DB や業界知見として蓄積

POINT

「品質向上のため」は、委託業務に必要な範囲の説明にならない

委託先規律は「二段構え」になる



一段目 すべての委託先(30条の3)

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

例外(想定):法令に基づく場合、人命の救助・災害の救援等で緊急の必要がある場合



二段目 取扱方法を自ら決めない委託先(58条の2)

契約で所定事項を定め、そのとおり扱えば義務を原則免除

想定例:委託元の指示どおりにデータ入力を行うだけの委託先

POINT

上限は全員に、免除は条件を満たした委託先だけに

「書いてあるから使える」から「必要だから使える」へ



これまでの発想

契約に書けば使える

「統計目的での利用を許諾する」と書いておけば、委託先も使える



これからの発想

委託業務に必要だから使える

委託元のための業務でない利用は、契約に書いても「委託」と評価しにくい
→ **本人同意のない第三者提供**の問題に



委託先が自社のために統計を作るなら、委託ではなく **統計作成等の特例** で別契約に

POINT

物差しは契約の文言ではなく、委託業務との必要関連性

免除の 3 要件と、外れる規律・残る規律

① 契約

② 範囲

③ 運用

3 つそろわなければ免除は及ばない



外れる主な規律

第 4 章の大部分

- 利用目的の特定・制限 (17 ・ 18 条)
- 適正取得・要配慮の取得制限 (20 条)
- 第三者提供の制限・記録 (27 ～ 29 条)
- 開示等の請求への対応 (32 ～ 39 条)



免除されず残る規律

ここは免れない

- 安全管理措置・監督 (23 ～ 25 条)
- 漏えい等の報告・本人通知 (26 条)
- 範囲外取扱いの禁止 (30 条の 3)
- 契約どおりでない取扱い

POINT

本人からの開示等の請求には、委託元が対応する建付け

契約に書くべき「取扱いの方法」4 項目



項目 1

対象となる
個人情報等

その項目等を含む



項目 2

行われる
処理の内容

取得・保存・評価・加工・提供・消去等



項目 3

取扱いの
始期と終期

いつからいつまで



項目 4

取扱いの
国又は地域

外国で扱うか、どこか



定め方: **書面** (電磁的記録を含む)。一部を委託元の別途の書面指示とする方法も可

POINT

どこまで特定すれば足りるかは意見募集中。ここが実務の分かれ目

4 項目を契約に落とすと、こうなる

項目	記載例(イメージ)
対象となる個人情報等	会員 ID・氏名・住所・購入履歴(項目は別紙 1 のとおり)
処理の内容	別紙 2 の手順による入力・照合・帳票出力のみ。提供先なし
始期及び終期	2027 年 4 月 1 日～2028 年 3 月 31 日。終了後 30 日以内に消去
国又は地域	日本国内のみ(国外の拠点・クラウドでは取り扱わない)

 「業務一式」「必要な範囲で」だけでは、方法を定めたとはいえない可能性

POINT 別紙方式で項目と手順を特定するのは、今からできる準備

報告条項と、規則案が挙げる 6 つの事項

契約で定める事項	ねらい
【法定】漏えい等・範囲外取扱い・契約違反の速やかな報告	委託元の速報（おおむね 3 ～ 5 日）に直結
委託を受ける業務の内容	範囲外取扱いの判断基準
取扱いの記録の作成・委託元への提供	取扱状況の把握
安全管理措置に関する情報の提供	委託元の責任による遵守確保
漏えい等の際、委託元の対応に必要な情報の報告	委託元の漏えい等報告
委託元の求めに応じた停止等／終了時の返還・消去	本人の請求への対応・残存防止

POINT 規則案に明示のない **守秘・再委託・監査** も、実務の契約には必ず入れる

委託を整理する 4 つのステップ



 生成 AI : DPA + 学習無効設定 + 越境移転 (28 条) の根拠整理 がそろって「委託」と説明できる

POINT 「クラウドだから当然例外」は通用しない。契約・設定・運用で確かめる

× 契約に書いても「委託」とはいえない



委託先自身のための利用は、委託業務に必要な範囲を超える



委託元の宿題 ①

ベンダー約款を確認

「サービス改善・開発に利用」「匿名化・
集計データを自由に利用」条項



委託元の宿題 ②

既存契約も見直す

委託規律に経過措置（みなし規定）はない。施行日から逆算

POINT

受託データの独自利用は、改正後は正面から違法になり得る

PART 8

漏えい等報告と安全管理措置

26 条・規則 7 条・8 条〔基本的な考え方②〕／安全管理措置 GL 別添の見直し(2027 年 4 月先行施行予定)

ここで分かること

漏えい時、本人通知や速報を
省ける場面はどこまで広がる？



「漏えい等」＝漏えい・滅失・毀損（とそのおそれ）



漏えい

外部に流出

例：メールの誤送信、不正アクセスによる流出



滅失

内容が失われる

例：誤廃棄（同じデータが他に残っていれば該当しない）



毀損

変更・使えなくなる

例：ランサムウェアで暗号化され復元できない



実際に起きた場合だけでなく「おそれ」がある場合も対象



令和 2 年改正で委員会への報告・本人通知が義務化（2022 年 4 月施行）。今回はその運用の見直し

POINT

報告・本人通知の「要否」と「方法」が、今回の見直しの対象

現行の報告・本人通知の流れ



i 委託先は委託元に通知すれば、報告・本人通知義務を免れる(26 条 1 項ただし書)

POINT 本人通知は報告とは別軸。報告完了まで待つ運用は予定されていない

見直しは 4 つ。法改正は㊦だけ



26 条 2 項(法改正)

本人通知の代替

保護に欠けるおそれが少ない場合を規則で



規則改正

速報免除・確報の取りまとめ

第三者確認を前提に報告の方法を見直し



規則改正

サイバー対処能力強化法との整合

攻撃起因の「おそれ」事案の基準を調整



規則 7 条(規則改正)

違法な第三者提供を報告対象に

報告対象事態に追加

POINT

①～㊨は規則改正。条文だけ見ていると気付かない

社内 ID だけの漏えいなら、通知に代わる措置で



! 外部でも使われる ID・メールアドレスは **当然には含まれない**。代わる措置は **必須** (附帯決議 10 項)

POINT 省けるのは規則で定める場合だけ。自社の評価だけでは省略できない

代替措置は「公表だけ」ではない



措置 ①

問合せ窓口の設置・周知

本人が自分が対象かを確認できるように



措置 ②

部分通知＋公表

連絡先が分かる本人には個別通知、不明分は公表・窓口で



措置 ③

既存チャネルで周知

アプリ内通知・会員ページなど
普段見る経路で



上場企業:漏えいの公表と **適時開示** を一体で設計し、広報・IR を初動から関与させる

POINT

手法を組み合わせ、選んだ理由を記録に残す

報告の 84% は「本人 1 人」の事案

84.0%

漏えい等報告のうち、本人の数が「1 人」の事案
(10,184 件)
1,000 人以下まで含めると 96.0%

出典:個人情報保護委員会「いわゆる 3 年ごと見直しに係る検討の中間整理」(2024 年 6 月)



前提

認定個人情報保護団体等が、体制・手順
(責任者・事実確認・本人通知)を確認



対象

誤交付・誤送付をはじめ、本人の数が 1
名の事案



効果

一定範囲で速報を免除／確報を一定期
間ごとに取りまとめ

POINT

確認主体は認定個人情報保護団体でよいか、ほかにあるかが意見募集中

負担は減らし、違法提供は「1 件でも報告」へ



ウ サイバー対処能力強化法との整合

二重報告の負担を減らす

- 攻撃起因の「おそれ」事案の基準をインシデント報告と整合
- 共通様式(ランサムウェア等)の窓口を NCO の下で一元化



エ 報告対象事態の追加

違法提供は件数を問わず報告

- 要配慮か否か・件数を問わず報告対象とする案
- 同意取得漏れ・手続不備のまま提供した場合も対象になり得る

POINT

提供前の適法性チェックが、漏えい対応と直結する

安全管理措置の「手法の例示」は改正法より先に施行

見直しの対象

通則 GL「10（別添）講ずべき安全管理措置の内容」

- 「講じなければならない措置」（従わないと法違反の可能性）
- 「手法の例示」← ここを追加・再構成

背景

- サイバー攻撃の高度化・複雑化（侵入型ランサムウェア等）
- 個人情報保護法サイバーセキュリティ連絡会（NCO・警察庁・IPA・NICT・JPCERT/CC、2024年12月～7回）
- 委員会が行政上の対応をした個別事案



改正法本体の施行（～2028年7月16日）より **1年以上早い「先行施行」**

POINT ガイドラインの見直しは改正法を待たない。2027年4月が先に来る

2027 年 4 月、安全管理措置の物差しが変わる



キーワード①

クラウド

利用者側・提供者側の双方の技術的措置
の例を明確化



キーワード②

多要素・生体認証

認証の手法の例を明確化



キーワード③

ゼロトラスト

アクセス要求ごとに動的に評価し、リスク
に応じて判断



キーワード④

横展開対策

特権アカウントの最小化、停止・隔離・アカ
ウント無効化

POINT

2027 年 4 月施行予定（12 月頃パブコメ）。4 観点で自己点検を年内に

見直し予定の「手法の例示」を先取り — 今から対応を

 「見直しの内容の確定は来年4月を予定していますが（中略）見直し予定の内容を先取りする形でお示します」
→ 事業者の **自主的な改善** を促す



① アクセス制御

権限・特権の最小化、定期棚卸し、端末状態でリスク判断



② 識別と認証

重要データ・管理者・外部アクセスに多要素認証



③ 不正アクセス防止

OS・ソフトウェアの最新化、無許可ソフトの防止



④ 漏えい等の防止

通信の暗号化、クラウド上データの暗号化消去



⑤ 検知・被害拡大防止

ログ分析、EDR等で常時監視、侵害機器の隔離



+ 不要データの消去

利用目的を達成したら遅滞なく消去（22条・努力義務）

POINT

2027年4月を待たず、見直し予定の水準で今から点検する（実質的な先行対応）

インシデント対応規程を見直す 3 つの視点

- 1 認定団体の対象事業者には 速報免除・確報取りまとめを使う前提になり得る
- 2 省略判断の記録様式 該当する規則の類型・代わる措置・判断者・判断時点
- 3 提供前の適法性レビュー 違法提供は件数を問わず報告、という前提で設計

上場企業: 3 つの時間軸を一本のフローに



POINT 「省ける場面」と「報告すべき場面」が同時に増える

○ ただし「代わる措置」は必須



社内 ID 等「単体ではおよそ意味を持たない情報」のみの漏えい



省ける方向

本人通知 → 代わる措置

- 社内 ID 等のみの漏えい（代替措置は必須）
- 本人 1 名の事案：速報免除・確報取りまとめ



増える方向

違法な第三者提供

- 件数・要配慮か否かを問わず報告対象
- 手続不備のままの提供も対象になり得る

POINT 「省ける場面」と「報告すべき場面」が同時に増える

PART 9

オプトアウト制度

名簿の流通(27条2項・7項・8項、29条1項、30条)〔基本的な考え方③〕

ここで分かること

名簿屋は、売る相手の「身元」を
どこまで確かめる？



「オプトイン」と「オプトアウト」の違い

オプトイン

27 条 1 項 (原則)
本人が先に決める



本人が
同意



第三者に
提供



同意の範囲で
利用

オプトアウト

27 条 2 項 (例外)
本人は「止める」側



通知等+
委員会へ届出



同意なく
提供開始



求めがあれば
提供停止

POINT

オプトアウト＝「同意を取らなくてよい」ではなく、手続と継続運用を引き受ける制度

4つの手続と、オプトアウトで渡せないもの

1

本人への通知等

項目・取得方法・停止の求めの受付方法等を通知、又は容易に知り得る状態に

2

委員会への届出

同じ事項を個人情報保護委員会に届け出る(変更時も)

3

委員会が公表

届出事項は委員会のサイトで公表される

4

停止の求めに対応

本人から求められたら、提供を停止する



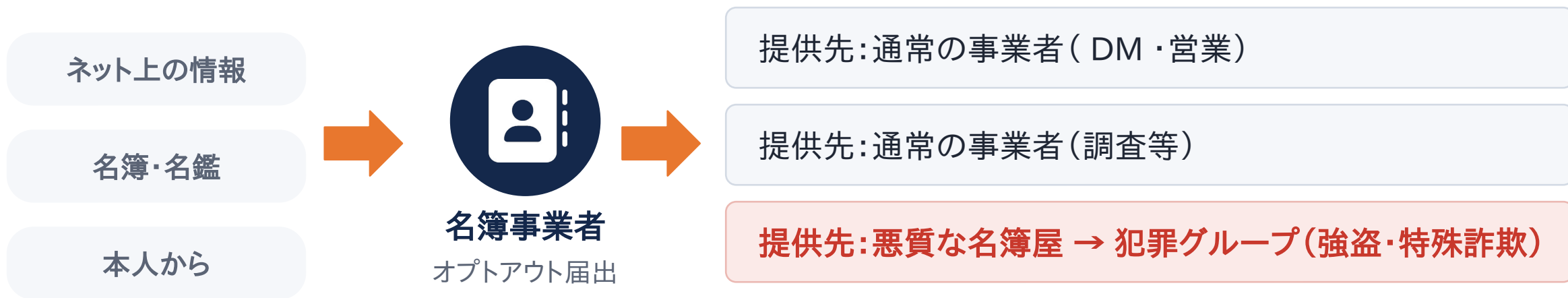
オプトアウトで渡せないもの

- 要配慮個人情報
- 不正な手段で取得された個人情報
- オプトアウトで受け取った個人データ(転売の連鎖)
- **特定生体個人情報**(改正で追加)

POINT

濫用のたびに強化されてきた制度。今回の起点は特殊詐欺の「闇名簿」

名簿が「闇名簿」に流れる



現行法では、提供元に「相手確かめる義務」がない



2025 年 5 月: 特殊詐欺グループへの名簿販売で、勧告を経ない初の緊急命令

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「闇名簿」

改正法の 3 点セット



① 27 条 7 項

確認義務

提供前に、提供先の身元（氏名・名称、住所、法人は代表者氏名）と利用目的を確認



② 27 条 8 項

偽りの禁止

提供先は確認事項を偽ってはならない。違反は過料（186 条 1 号）



③ 29 条 1 項

記録義務

提供年月日・提供先の氏名等に加え、確認した事項（利用目的を含む）を記録



例外: 提供するデータの **全部** が、取得時に本人・国の機関・報道機関等により公開されていたもの

POINT

対象はオプトアウトによる提供。すべての第三者提供に一律に及ぶわけではない

提供先の確認は、施行前から求められている

実態調査で分かったこと

約 3 割

2025 年に提供実績のある届出事業者のうち、**提供先の本人確認手続を実施していない**と回答

提供先が 19 条の方法で利用しないことを **確認していない** との回答も一部に

注意喚起が示した「提供先の確認」の例



利用目的

利用目的を確認し、目的外利用を禁止する契約を締結



事前審査

提供前に企業審査。不法・不当な利用のおそれがあれば提供しない



本人確認

身分証の提示／協会・免許番号の確認／住所への通知と到達確認／担当者の権限確認／実印+印鑑証明書

POINT 改正 27 条 7 項・「考え方③」(身元は書類で検証)の先取り。施行を待たずに整備する

取得元の確認・周知・手数料も点検対象



① 適正な取得の確認

取得元を企業 HP・報道・官公庁公開情報・登記等に限定。第三者からは本人同意に基づく提供かを確認(30条 確認→20条1項違反のおそれ)



② 容易に知り得る状態

トップから1回程度の操作で届く場所に継続掲載。自社 HP に載せるだけでは足りない



③ 手数料の記載

停止の求めに手数料は取れない。取れるのは利用目的の通知・開示請求のみ(38条)



④ 変更届出・越境

項目等の変更は事前の通知等+届出。外国の第三者への提供は原則本人同意(28条)

POINT

いずれも現行法上の要請。改正を待たず、自社サイトの記載から点検する

売るとき・仕入れるとき・届け出るとき

場面	論点	条文
売るとき	論点 1 提供先の確認方法	27 条 7 項柱書
売るとき	論点 2・3 例外となる公開主体・例外の追加	27 条 7 項ただし書
売るとき	論点 4 記録事項	29 条 1 項
仕入れるとき	論点 5・6 提供元の確認方法・記録事項	30 条 1 項・3 項
届け出るとき	論点 7 委員会への届出事項	27 条 2 項 8 号

※30 条は現行法の条番号（第三者提供を受ける際の確認・記録）

POINT キーワードは「確認の確度」と「後から検証できる記録」

「身元」は書類で検証、「目的」は申告で



提供先の身元(氏名・住所・代表者)

本人確認書類の検証等

悪質な名簿屋は氏名等を偽る。申告だけでなく、一定の確度で確かめる



提供先の利用目的

申告を受ける方法

目的には公的な証明書がない。犯収法の「取引を行う目的」も申告



比較: 受け取る側の確認(30 条 1 項)は今も「申告」で足りる



同じ提供先への 2 回目以降は、簡易な確認でよい方向

POINT

オプトアウトで「売る側」には、一段厳しい確認が求められる

「本人確認書類」のイメージー 発想は犯収法の KYC

区分	具体例
デジタル署名あり	マイナンバーカード(実物・スマホ)、運転免許証、パスポート、在留カード等
顔写真付き	運転経歴証明書、顔写真付きの国家資格証・福祉手帳
その他	住民票の写し、顔写真なしの福祉手帳
法人	登記事項証明書(登記情報提供サービスを含む)、印鑑(登録)証明書 等

 検証の手法例: IC チップの署名検証／発行元への照会／容貌確認／住所への確認コード郵送

POINT 名簿を「買う」会社も、書類を出す側になる

「公開情報なら確認不要」は 3 条件で読む

①

全部

提供するデータの全部
が公開情報

②

取得時点

自社が取得した時点で
公開済み

③

公開主体

本人・国の機関・報道機
関等の法定の主体



例: 公開名簿に、非公開で集めた携帯番号を足して売る → 「全部」を満たさず確認が必要

論点 2 規則で追加する公開主体

現行規則 6 条と同じ

外国政府・国際機関、外国の研究機関・報道機関等

論点 3 例外の追加

「準ずる場合」に限る

具体案はまだ示されていない

POINT

「ネットに載っている」では足りない。全部・取得時点・公開主体で判定

記録は「誰が・いつ・どうやって」確認したかまで



現行(規則 20 条 1 項 1 号)

提供の記録

- 提供した年月日
- 提供先の氏名・名称等
- 本人を特定するに足りる事項
- データの項目



追加案(犯収法の確認記録を参考)

確認の記録

- 確認した**担当者**の氏名等
- 確認した**年月日・時刻**
- **確認の方法**(例: IC チップの署名検証)

POINT

目的はトレーサビリティ。確認義務の履行を、後から検証できるように

持ち出された名簿の「売り先」は名簿業者

約 928 万人

システム保守の受託会社の従業員が約 10 年にわたり持ち出し

約 2,989 万件

通信教育会社の委託先の従業員が持ち出し、約 1,000 万件を売却

約 148 万件

システム担当者が CD-R1 枚で持ち出し

自治体

再々委託先の従業員が住民基本台帳データをコピー

出典:事務局資料(2026 年 10 月 14 日) 37 頁(2024 年 4 月 24 日事務局資料から抜粋されたもの)



論点 5 提供元の確認方法

仕入れも書類で確認

オプトアウトで売る目的で仕入れるときは、提供元の身元も本人確認書類の検証等で(現行は申告で足りる)



論点 6 記録事項

担当者・日時・方法を追加

仕入れ時の記録(現行規則 24 条 1 項 1 号)にも、論点 4 と同じ項目を追加

POINT

名簿業者の「仕入れ」が持ち出しの換金ルート。入口で止める

届出事項に「本人への知らせ方」を



実態調査 (2026 年 8 月 19 日公表)

知らせ方が不十分

- HP 上の届出事項の記載が不十分
- 停止の求めに手数料を取るかのような誤った記載
- 手数料を取れるのは利用目的の通知・開示請求だけ (38 条)



事務局の案

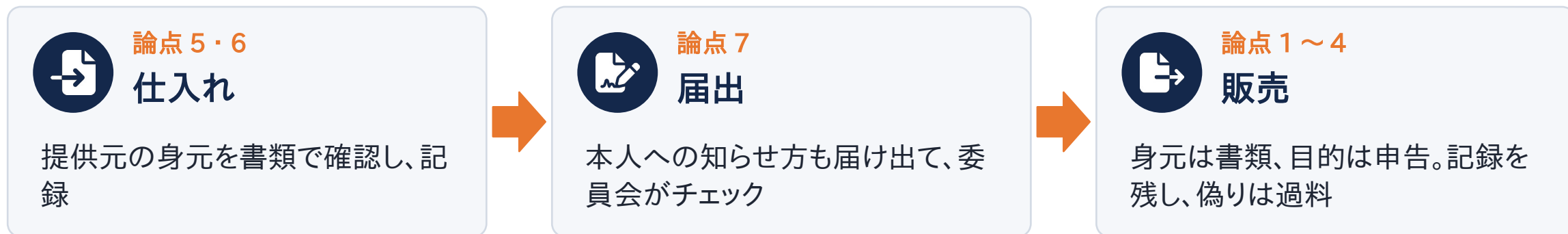
知らせ方を届出事項に

- 本人への通知等の **具体的な方法** を追加
- 届出の時点で委員会がチェック
- 例: HP トップから 1 回程度の操作で届く場所に継続掲載

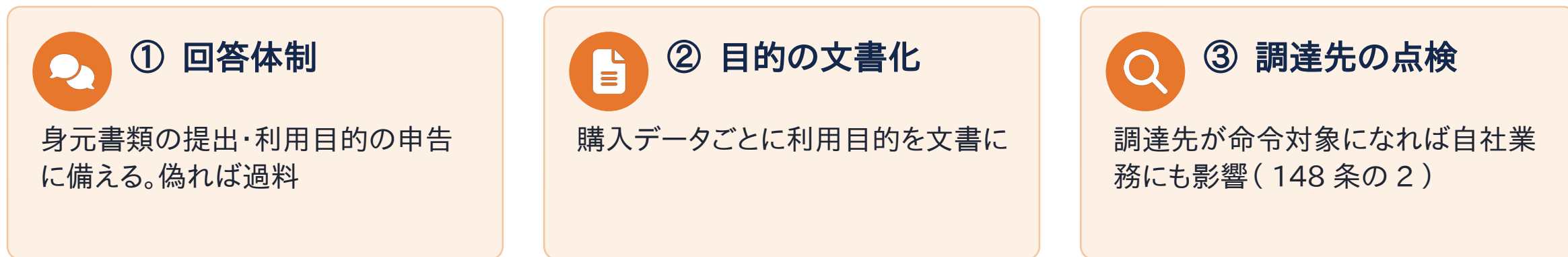
POINT

自社サイトの掲載場所・記載事項・手数料の文言を今すぐ点検

名簿を「買う」企業にも宿題がある



名簿・リストを「買う」企業の宿題



POINT 名簿の流れ全体に「相手確認」が入る。買う側も書類を出す側に

PART 10

課徴金

課徴金納付命令(148 条の 3 ～ 148 条の 17) [基本的な考え方③]

ここで分かること

いくら取られる?

どんな場合なら対象外?



「課徴金」は罰金や過料と何が違う？

	罰金	過料	課徴金
性質	刑罰（刑事罰）	行政上の秩序罰	行政上の措置（利得の剥奪）
誰が科すか	裁判所（刑事裁判）	裁判所（非訟事件手続）	個人情報保護委員会（納付命令）
前科	つく	つかない	つかない
個情法での例	不正提供・盗用（178条・179条）	虚偽回答（186条1号・新設）	違法な第三者提供等（148条の3・新設）

 課徴金は独占禁止法・金融商品取引法・景品表示法にもある仕組み。個人情報保護法には **今回初めて導入**

POINT 課徴金の目的は「罰」ではなく「違反で得た利益を取り上げる」こと

委員会はどう動くのか ― 現行の流れと改正



POINT 現行法では、命令に従えば金銭的な不利益はなかった

「見つかったら止める」で利益が残る — やり得の解消

対象行為(4つ)

19 条違反
不適正利用

20 条 1 項違反
不正取得

27 条 1 項違反
同意なき第三者提供

30 条の 2 関係
統計作成等特例違反

要件(4つ)



対価

違反・やめることの対価を得た



主観

防止の「相当の注意」を怠った



侵害

権利利益の侵害・具体的なおそれ



規模

本人の数が 1,000 人超



漏えい・安全管理措置違反 **それ自体は対象行為ではない**。本人 1,000 人以下は法律上対象外

POINT

GDPR の売上高連動型ではなく、違反行為の「対価」を基礎にする

金額のルールは 3 つの数字で

基本額(148条の3)

全額

違反・やめることの対価として
得た金銭等に相当する額

1,000 万円 → 1,000 万円

加算(148条の5)

×1.5

報告徴収等の日から遡って10
年以内に納付命令を受けてい
た場合

1,000 万円 → 1,500 万円

減額(148条の6)

−50%

違反の事実を自主報告。調査を
予知した後は対象外

1,000 万円 → 500 万円

POINT 「全額」「1.5 倍」「半額」。この 3 つで金額の大枠は決まる

「対象外」を認めるのは 1 類型だけ



対象外を設けない

不適正利用／不正取得／
統計作成等特例違反

侵害につながる蓋然性が特に高い。統計特例は多数の個人に重大な侵害が及ぶリスク



対象外になり得る

同意なき第三者提供

提供先が本人に直接影響を与えることが一般に想定されない情報「のみ」を提供した場合



例外の例外: 本人から「提供をやめる対価」を得た場合は、なお課徴金の対象

POINT

本人 1,000 人以下は法律で対象外。そのほかの対象外は 1 類型だけ

対象外は、7つの「どれも含まない」データだけ

- 1 特定の個人を識別できる記述等(氏名等)
- 2 個人識別符号
- 3 連絡等が可能となる記述等(住所・電話・メール・Cookie ID 等)
- 4 財産的被害のおそれがある記述等(カード番号等)
- 5 特異な記述等(症例数の極めて少ない病歴等)
- 6 多数の事業者が取得する共用性のあるID 等
- 7 害する利用が想定される記述等(蓄積された位置情報・購買履歴等)



なるほど

仮名加工・匿名加工の作成基準(規則 31 条・34 条)とほぼ同じ物差し

氏名を消しただけでは対象外にならない

POINT ③ は前半 PART4 の「連絡等が可能となる記述等」。ここで効いてくる

× 課徴金は「利益」ではなく「対価の全額」



売上 1,000 万円・利益 100 万円でも、課徴金は 1,000 万円



算定 ①

対価の総額

違反の対価+やめることの対価。
経費は引かない



算定 ②

未収も含む

命令時点で未払いの代金(債権)も算入



算定 ③

まとめて 1 つ

社会通念上 1 つの行為なら、複数の売り先の対価も 1 つの課徴金に

POINT 「儲けの一部」ではなく対価の全額。100 万円には圧縮されない

5 つの想定事例で見る課徴金額

想定事例	違反類型	課徴金額
① 5 万人分を USB で、同意なく B 社に 1,000 万円で販売	第三者提供違反	1,000 万円
② 5 万人分を年 1,000 万円でライセンス (半数は一部のみ同意)	第三者提供違反	1,000 万円 按分なし
③ 統計特例の 10 万人分で信用スコア AI → 2 億円で販売合意 (未払い)	統計特例違反	2 億円 未収も算入
④ 虚偽の電話で 1 万人の携帯番号 → 転職勧誘の手数料 2 億円	不正取得	2 億円
⑤ 破産者 1 万人を地図サイトに掲載 → 削除を求めた 30 人から 150 万円	第三者提供違反	150 万円 やめる対価

POINT 一部同意でも按分なし、未収でも算入、「やめる対価」も課徴金

帳簿がなくても「単価 × 人数」で推計

例: 1 万人分を B 社に 100 万円で販売。C 社・D 社にも同じデータを販売したが代金は不明

$$\begin{array}{ccccc} \boxed{100 \text{ 万円}} & \div & \boxed{1 \text{ 万人}} & = & \boxed{100 \text{ 円}} & \times & \boxed{2 \text{ 万人}} & = & \boxed{200 \text{ 万円}} \\ \text{B 社分 (把握済み)} & & \text{B 社分の人数} & & \text{1 人当たり単価} & & \text{C・D 社分} & & \text{推計額} \end{array}$$



把握済み 100 万円 + 推計 200 万円 = 対価の合計 300 万円



なぜ推計? 帳簿の不保存・散逸で算定が止まるのを防ぎ、資料を出した事業者だけが高くなる不公平をなくす

POINT 帳簿を残さなかった会社が得をしない仕組み

自主報告で半額、M&A では履歴が引き継がれる



論点 5 自主報告(148条の6)

「いつ出したか」が勝負

- 書面:対象行為の概要・対価の額・経緯・原因+資料
- 持参／郵便(差出時)／メール(記録時)
- 調査を予知した後は減額なし



論点 6 合併・会社分割(政令)

M&A にも効く

- 加算・減額の履歴は存続会社・承継会社に引き継ぐ方向
- DDで「過去10年の課徴金納付命令」を確認
- 論点7・8:公示はネット公表、納付手続は景表法等に倣う

POINT

発見から自主報告までの社内ルートと、M&AのDD項目を今から整える

罰則は「だまして取る」段階から

罰則	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
不正取得罪（180条・新設）	—	2年以下の拘禁刑／100万円以下の罰金
虚偽回答の過料（186条1号・新設）	—	10万円以下の過料

148条の2：違反を補助する第三者（ホスティング・プラットフォーム等）にも、中止のための措置を要請できる

POINT 退職者・委託先経由の持出しは実刑リスクを伴う水準に

免責は「契約の文言」ではなく「審査した記録」で決まる



 参議院(2026年6月17日)政府答弁:相当の注意を尽くしていれば対象外の可能性が高い／説明の鵜呑みは不可

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

実務対応とスケジュール

何を、いつまでに

ここで分かること

「規則待ち」でよいこと、
今すぐ始めることは？

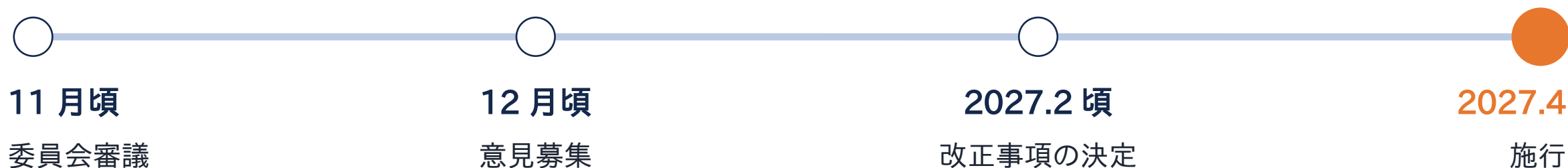


意見を言える場面と、先に来る期限

改正法の政令・規則



安全管理措置ガイドライン(別ルート)



POINT 意見提出の山場はこの冬。自社に効く論点は年内に整理する

優先して棚卸しすべき 6 領域



AI・分析・統計

特例に乗るか／担保措置・公表
／ PETs



顔認証・映像分析

周知・掲示／オプトアウト禁止／
停止請求



16 歳未満の利用

法定代理人対応／年齢把握／
最善の利益



名簿・営業リスト

身元確認・記録／連絡可能個人
関連情報／買う側の回答



委託・クラウド・BPO

30 条の 3 ／ 58 条の 2 ／ 既存
契約の見直し



課徴金リスク事業

「相当の注意」の証跡／自主報
告ルート

POINT

棚卸しは規則の内容に左右されない。今日から着手できる

IR・総会・人事・開示の各部門が当たる



IR・SR

株主名簿・判明調査

証券代行・調査会社に 30 条の 3。調査データの蓄積は範囲外に



総務

株主総会

入口の顔認証は顔特徴データの規律。揭示を作り直す



人事

人的資本開示

少数セルからの推知に注意。開示方針で扱いを決める



開示・ガバナンス

命令・課徴金と開示

適時開示の判断／有報「事業等のリスク」の更新／取締役会への報告

POINT

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になった

施行までの 4 ステップ



POINT 「規則待ち」でよい部分と、今すぐ着手すべき部分を分ける

今日の 3 つのポイント

①

委託は「契約」が要件に

全委託先に範囲外取扱いの禁止。免除は規則所定事項を
書面で。既存契約も見直し

②

省ける場面と報告場面が増加

社内 ID は通知代替、違法提供は報告対象。安全管理 GL
は 2027 年 4 月

③

名簿は書類、課徴金は対価の全額

身元は書類で検証し記録。課徴金は経費を引かず、按分な
し、未収も含む



クイズの答え ① × (対価の全額) ② × (委託の範囲外) ③ ○ (代わる措置は必須)

POINT

使えるデータは使えるように。ただし逸脱には従来よりはるかに重い責任

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 年改正法（令和 8 年法律第 56 号）及び個人情報保護委員会事務局「政令・規則の整備に向けた基本的な考え方」（2026 年 9 月 16 日・10 月 1 日・10 月 14 日）、安全管理措置の手法の例示の追加等（同年 9 月 16 日）等に基づく一般的な情報提供であり、個別の法的助言ではありません。政令・規則・ガイドライン等の今後の整備状況をご確認ください。