改正公益通報者保護法とグローバル内部通報体制の実務対応 – 日本企業・海外拠点の実務と最新動向

弁護士法人 三宅法律事務所
弁護士　渡邉　雅之

弁護士法人三宅法律事務所 パートナー
弁護士 渡邉 雅之
TEL: 03-5288-1021
Email: m-watanabe@miyake.gr.jp

改正公益通報者保護法

公益通報者保護法とは？

- 従業員等が勤務先の「違法行為」を通報したことで、解雇・降格・減給などの **不利益な取扱いを受けないように保護する**法律

- 2000年代初頭、企業不祥事（リコール隠し・産地偽装など）が頻発。通報による発覚が多かったことから、「通報者保護」を目的に2006年施行。

- 制度の目的（1条）：
  - **通報者を守る**
  - 企業の内部不正を早期発見・是正して**企業・社会を守る**
  - 消費者・取引先の信頼を維持する

- 2025年6月11日に改正法が公布され、**2026年12月までに施行予定**

（令和7年改正法に関する消費者庁ウェブサイト）
https://www.caa.go.jp/policies/policy/consumer_partnerships/whistleblower_protection_system/overview/#r7_amendment

保護される対象者

区分	改正前	改正後（2025年改正）
対象者	正社員、契約社員、派遣社員、パート、アルバイト、役員、公務員、退職後1年以内の者	**＋ 業務委託契約によるフリーランス（特定受託業務従事者）＋ 契約終了後1年以内のフリーランス**

- 背景近年の働き方の多様化に対応。「雇用関係がなくても、業務委託先で不正を知る立場」にある者を保護対象に。

保護される通報内容

ロ 対象となる通報

- 「国民の生命・身体・財産その他の利益の保護に関わる法律」に違反する行為、または違反に繋がる行為（約500法令）。

ロ 具体例

- 食品衛生法違反（産地偽装など）
- 労働基準法違反（残業代未払い）
- 廃棄物処理法違反（無許可処理）
- 横領、粉飾、顧客情報漏えい 等

改正による新たな追加点（「従事者指定義務」違反の通報対象化）

「**公益通報対応業務に従事する者の指定義務（従事者指定義務）**」を怠るなど、**体制整備義務違反そのものも通報対象**に明記される。

※消費者庁は「制度の実効性を高めるための核心」として強調

通報先と保護の条件

区分	通報先	主な保護要件	具体例・補足
① 事業者内部（1号通報）	労務提供先またはその定めた者（例：社内窓口、外部弁護士、グループ共通ヘルプライン等）	• 通報対象事実が「生じ、又はまさに生じようとしている」と**思料**すること（合理的な理由までは不要）– 不正な目的でないこと	• 通報内容が真実である必要はないが、信じるに足る根拠が必要 • 企業内部での是正を促す目的
② 行政機関（2号通報）	通報対象事実について処分・勧告等の権限を有する行政機関（例：消費者庁、金融庁、労基署、自治体など）	• 通報対象事実が「生じ、又はまさに生じようとしている」と**信ずるに足りる相当の理由**があること（真実相当性）– 不正目的でないこと	• 通報内容を裏づける資料や関係者証言等が必要 • 改正法では真実相当性がなくても、合理的根拠＋行政指導の必要性を記載すれば認められる場合あり
③ 報道機関・その他外部機関（3号通報）	報道機関、労働組合、弁護士等（事業者外部）	• 通報対象事実が「生じ、又はまさに生じようとしている」と**信ずるに足りる相当の理由**があること • 下記①～⑤いずれかに該当する場合のみ保護 ①内部・行政通報で不利益を受けるおそれ ②証拠隠滅・改ざんのおそれ ③通報禁止の不当要求 ④内部通報後20日経過しても調査等なし ⑤生命・身体に危険の急迫	• 報道機関通報は「風評被害」のおそれがあるため最も厳格な要件 • 改正法では「公益通報者を特定させる事項を漏えいするおそれ」も新たな保護要件に追加

⚠ 通報の「内容」と「通報先」により、保護の要件が異なる点に注意。

2025年改正の主要ポイント：不利益取扱いへの罰則導入

行為	罰則
通報を理由に解雇・懲戒を行った者	6か月以下の拘禁刑 または 30万円以下の罰金
事業者（法人）	3,000万円以下の罰金

- **狙い**：通報者への報復的処分を「未然に防ぐ」強い抑止力。

2025年改正の主要ポイント:「推定規定」による立証責任軽減

- 通報後1年以内の解雇・懲戒については、
  「公益通報を理由としてされたものと推定」される
- 通報者側が裁判で立証しなくてもよい
- ただし、配置転換・出向などは対象外

実務ポイント

企業は処分の際、通報者との関係を必ず確認
「通報とは無関係」と説明できる証拠を整えておくこと

2025年改正の主要ポイント:「通報妨害・通報者探索」の禁止を明文化

禁止される行為:

- 「通報しないよう合意を求める」
- 「通報者を特定しようとする行為」
- 「通報した者への嫌がらせや退職強要」

これまでガイドライン上の要請だったが、
今回から法律上の禁止行為に格上げ。

違反時は行政指導・命令・罰則の対象。

2025年改正の主要ポイント：行政の権限強化

- 消費者庁に「立入検査」や「命令」権限を付与
- **命令違反・虚偽報告・検査拒否**等には
  30万円以下の罰金
- 事業者に対して指導・勧告・命令を発動できる

2025年改正の主要ポイント：事業者の体制整備義務の明確化

企業規模	義務内容
従業員301人以上	・内部通報窓口設置 ・通報対応従事者の指定 ・調査・是正体制の整備 ・従業員への周知義務（新設）
300人以下	努力義務（法的拘束力なし）

「形だけ」ではなく「機能する」制度へ

制度を整備するだけでなく、運用実績・改善サイクルが求められる。

改正公益通報者保護法　企業対応チェックリスト①

【Ⅰ】体制整備・責任者

チェック項目	状況
□ 公益通報対応業務従事者（責任者）を正式に指定しているか。	□済 □未
□ 通報窓口（社内・社外）を明確化し、匿名・秘密保持が確保されているか。	□済 □未
□ 通報の受付～調査～是正の流れを明文化（規程・マニュアル化）しているか。	□済 □未
□ 通報対応責任部署（法務・監査など）を明確にしているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト②

【Ⅱ】通報対応と記録管理

チェック項目	状況
□ 通報受付・処理の記録を安全に保存し、アクセス制限しているか。	□済 □未
□ 調査結果・是正内容を経営層まで報告できる体制があるか。	□済 □未
□ 定期的に通報件数・対応状況をレビューしているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト③

【Ⅲ】通報者保護の徹底

チェック項目	状況
□ 通報を理由とする解雇・降格などの不利益取扱いを禁止しているか。	□済 □未
□ 通報後1年以内の処分について「通報が理由」と推定されるリスクを理解しているか。	□済 □未
□ 通報者を特定・探索しない、または通報を抑止しないルールを整備しているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト④

【Ⅳ】フリーランス・委託先対応

チェック項目	状況
□ フリーランス・委託先も通報対象に含む制度に改定しているか。	□済 □未
□ 契約書に「通報制度の利用可能性」を明記しているか。	□済 □未
□ 委託先にも制度の説明・周知を行っているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト⑤

【Ⅴ】教育・周知・文化づくり

チェック項目	状況
□ 全従業員に制度内容を年1回以上周知・研修しているか。	□済 □未
□ 管理職・責任者に「通報者保護・守秘義務」研修を実施しているか。	□済 □未
□「通報しても守られる」メッセージを経営トップが発信しているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト⑥

【Ⅵ】行政・監査・改善

チェック項目	状況
□ 消費者庁などからの命令・検査に対応できるマニュアルがあるか。	□済 □未
□ 内部監査や外部チェックで制度運用を定期的に確認しているか。	□済 □未
□ 通報制度のKPI（通報件数・是正率・対応期間など）を設定し、改善サイクルを回しているか。	□済 □未

改正公益通報者保護法　企業対応チェックリスト⑦

【Ⅶ】中小企業・準備スケジュール

チェック項目	状況
□ 規模に応じて通報窓口設置・規程整備を段階的に進めているか。	□済 □未
□ 改正法施行（2026年12月）までの対応計画を策定しているか。	□済 □未

グローバル内部通報

はじめに

- **グローバル内部通報制度（Global Whistleblowing System）** は、国内外の従業員・退職者・フリーランス・取引先等が、不正・違反を匿名または実名で通報できる仕組み。

- **目的**:
  - 不祥事・法令違反の早期発見と是正
  - 本社による一元的リスク管理
  - 国際的信用維持（ESG・投資家対応・取引先DD）

- **背景**:
  - OECD、UNGP、FATFなど国際的基準で内部通報制度が重視。
  - ESG/サステナビリティの観点からも有効性が企業価値評価の指標に。

各国法制の制約と影響（日本・EU・米国ほか）

□ EU（ホイッスルブロワー指令2019/1937＋GDPR）

- 50名以上の企業に内部通報窓口設置義務。
- 保護対象は従業員のみならず、取引先・ボランティア・ジャーナリストまで広範。
- 報復禁止：立証責任が逆転。
- GDPR：通報データは「高リスク処理」→DPIA必須。

□ 日本（改正公益通報者保護法：2022施行＋2025改正）

- **指定従事者必置**、未設置は是正命令・罰則。
- **保護範囲拡大**：フリーランス・退職者（1年以内）。
- **通報妨害・身元特定禁止** の明文化。
- **報復推定＋刑事罰**：通報後1年以内の不利益取扱いは報復と推定、法人罰金最大3,000万円。
- 実務的影響：ポリシー・契約・SOPを「日本基準」に合わせグローバル統一へ。

□ 米国（SOX法・Dodd-Frank・CCPA/CPRA）

- **SOX**法：上場企業は監査委員会による通報制度保持が義務。
- **Dodd-Frank**：**SEC**直接通報＋報奨金制度。
- **CCPA/CPRA**：従業員データ権利（開示・削除・訂正）に対応。

□ 中国（PIPL）

- 越境移転は標準契約／当局審査／認証が必須。
- 高リスク処理には**PIIA**必須。
- 重要データは国内保存義務。

□ その他アジア

- シンガポールPDPA：国外移転は契約措置必須。
- タイ・インドネシア：国外移転は同意＋契約。
- ロシア：国内保存義務。

日本改正公益通報者保護法（2025年改正）の要点と改正点

- **指定従事者の必置**：未設置は是正命令・罰則対象。
- **保護対象拡大**：フリーランス・退職者（1年以内）・求職者等も保護。
- **通報妨害・身元特定の禁止**：外部通報禁止条項や「通報者探し」を明確にNG。
- **報復推定規定**：通報後1年以内の不利益取扱いは原則「報復」と推定
  →事業者に反証責任。
- **罰則導入**：通報妨害・報復に刑事罰（法人最大3,000万円、個人は懲役刑）。
- **実務影響**：規程・契約・SOP・研修の再設計（日本基準でグローバル底上げ）。

日本・EU・米国の内部通報法制比較

項目	日本：公益通報者保護法（2022年施行）	日本：公益通報者保護法（2025年改正後）	EU：ホイッスルブロワー指令（2019/1937）	米国：SOX法・Dodd-Frank等
適用対象事業者	従業員301人以上の事業者は「体制整備義務」あり	同上＋「公益通報対応業務従事者（指定従事者）」必置義務化	従業員50人以上の企業・自治体等に内部通報窓口義務	上場企業（SEC登録企業）
保護対象者	従業員・派遣社員・役員等	**フリーランス・退職者（1年以内）・求職者等を追加**	従業員、元従業員、株主、取引先、ジャーナリスト等広範	上場企業従業員（監査情報通報）、Dodd-FrankではSECに直接通報する者全般
通報先	① 事業者内部窓口 ② 行政機関	**③ 報道機関等への外部通報を条件付きで明示的に保護**	① 内部窓口 ② 行政当局 ③ 公開（条件付）	① 監査委員会 ② SEC（直接通報も可）
匿名通報	匿名も保護対象（指針で明記）	**匿名保護を法律上もより強化**	禁止せず、加盟国判断。多くは匿名受付を推奨	匿名通報可（SOX/Dodd-Frankで想定）
報復禁止	不利益取扱い禁止	**「報復推定規定」を新設 → 事業者が無関係を立証する責任**	報復全面禁止、立証責任は事業者側	報復禁止を明文化、違反時は損害賠償請求可
罰則	行政的是正命令中心（刑事罰なし）	**通報妨害・報復に刑事罰導入（法人：最大3,000万円、個人：懲役刑）**	加盟国ごとに国内法で罰則導入（例：フランス＝刑事罰）	SOX違反：罰金・懲役、Dodd-Frank：SEC制裁
制度設計義務	体制整備義務（内部規程・研修）	**指定従事者設置、秘密保持・妨害禁止・研修の法定義務化**	内部窓口設置、独立性確保、3か月以内フィードバック義務	監査委員会による窓口設置、外部監査人への通報保護
特徴	日本法は「体制整備」義務が中心	**改正で「刑事罰」「報復推定」「指定従事者必置」と実効性を大幅強化**	EUは適用範囲・保護対象が最も広範	米国は「SEC直接通報＋報奨金制度」が特徴

匿名通報の取扱い（グローバル視点）

- **メリット**：心理的障壁を下げ通報件数が増加。

- **デメリット**：虚偽通報や追加聞き取りの難易度。

- **各国状況**：
  - 日本：匿名も保護対象（消費者庁Q&A明記）。
  - 欧州：全面禁止はなく、匿名受付を条件付きで許容。
  - 米国：匿名通報は制度設計の基本。

- **実務**：匿名でも双方向コミュニケーション可能な外部ツール（NAVEX/EQS/Whispli等）を採用。虚偽通報対策と調査効率化ルールを明文化。

通報窓口の設計モデル

- **現地完結型**：
  - 利点：即応・母国語対応
  - 課題：本社統制・情報共有の欠如
- **本社一元型**：
  - 利点：全件把握、重大不正に迅速対応
  - 課題：言語・時差・リソース不足。**各国のデータ保護規制が問題に。**

- **ハイブリッド型**：
  - 利点：柔軟性
  - 課題：複雑・コスト増

- **推奨モデル**：
  - 本社一元管理＋外部ベンダー（多言語・匿名・24時間対応）。

各国のデータ保護規制って関係あるの？との疑問

- 海外の現地法人自体からの通報ではなく、海外従業員からの通報なので、各国のデータ保護規制（個人情報保護規制）は問題にならないのではないかとの疑問がよく寄せられる。

- しかしながら、日本のグループ親会社は、海外従業員所属の海外現地法人に、通報内容について問い合わせをせざるを得ないので、結局、海外現地法人⇒日本親会社という個人データの移転は必然的に起こる。

データ保護と越境移転

- **EU → 日本/米国**：SCC、十分性認定、シュレムズII判決（2023年EU-US Data Privacy Framework（DPF）が新たに承認され、米国は「十分性認定国」）。
  ⇒グローバル企業は**SCC＋追加措置＋リスク評価（DPIA）**をセットで実施する必要

- **日本 → 海外**：本人同意 or 契約義務付け、国外法制度の情報提供義務あり。

- **中国 → 海外**：CAC審査、標準契約締結、再転送も規制対象

- **リスクベースアプローチ（RBA）**：
  - 高リスク処理（越境移転、匿名処理）にDPIA/PIIAを義務付け。
  - 各国要求水準に応じた比例的対応

アジア諸国のデータ保護規制の留意点

□ 中国：PIPL（個人信息保護法）

- **越境移転**：標準契約条項締結 or 当局セキュリティ評価 or 認証。
- **影響評価（PIIA）**：越境移転や高リスク処理には必須。
- **データローカライゼーション**：重要データは中国国内保存義務。
- **実務影響**：中国拠点から本社に通報情報を送る際、越境規制クリアが必須。

その他アジア

- シンガポールPDPA：正当利益による処理可、国外移転には契約措置。
- タイPDPA・インドネシア：国外移転は原則同意ベース。
- ベトナム：影響評価義務と越境移転に対する事前通知義務。「重要データ（Important data）」や「核心データ（Core data）」の越境移転について、当局の承認が必須。
- ロシア：個人データの国内保存義務。

グローバル内部通報制度とプライバシーポリシー

- **内部通報制度** と **プライバシーポリシー** は表裏一体:
  - 通報制度が扱う情報は「個人情報／センシティブ情報」を含むため、各国のデータ保護法制への適合が不可欠。
  - GDPR、PIPL、APPI、CCPA などの規制は、通報制度の設計と密接に結びついている。

- **経営上の意義**:
  - 内部通報は不正防止・ガバナンス強化の基盤。
  - プライバシーポリシーはグローバルでの「データ処理の正当性」と「透明性」を担保する枠組み。

グローバルプライバシーポリシーの役割

- **グローバル標準化**：各国法制の違いを吸収し、グループ全体で統一ルールを明示。
- **リスク低減**：透明性と説明責任を確保することで、訴訟・制裁リスクを低減。
- **信頼確保**：従業員や外部関係者に「安心して通報できる環境」を提示。
- **取締役の善管注意義務対応**：GDPRベースで設計されたプライバシーポリシーは合理的な経営判断の根拠となる。

グローバルプライバシーポリシーの必須要素

① データ処理の目的
- 通報制度で収集する個人情報の利用目的を特定。
- 例:「不正行為の調査・是正」「ガバナンス強化のためのモニタリング」。

② 収集する情報の範囲
- 通報者情報(氏名・連絡先)
- 被通報者情報(氏名・職位・行為内容)
- 関連証拠(Eメール、チャット記録、音声等)
- センシティブデータ(人種、健康、犯罪歴等)は必要最小限に限定
- **③ 法的根拠**
- **EU(GDPR)**:正当な利益(Art. 6(1)(f))、義務遵守(Art. 6(1)(c))
- **日本(APPI)**:利用目的明示、安全管理措置
- **米国(CCPA/CPRA)**:通知義務・削除権・訂正権
- **中国(PIPL)**:明示的同意＋PIIA＋越境移転要件

④ 保持期間
- 通報調査終了後は必要最小限の期間保存(例:5年)。
- 訴訟・当局調査に備えた例外保存も明記。

⑤ 第三者提供と越境移転
- 本社・地域ハブ・外部調査機関への提供ルールを明示。
- EU域外移転はSCC、中国からの移転は当局審査・契約を根拠に。

⑥ 通報者・被通報者の権利
- 通報者:匿名性確保、報復禁止、情報開示請求権。
- 被通報者:訂正請求・異議申立権。ただし調査を害しない範囲で制限。

⑦ 透明性・周知
- グローバルプライバシーポリシーを全拠点の従業員ポータルに掲載。
- 多言語化(日本語・英語・中国語・スペイン語等)。

プライバシーポリシーとRBA（リスクベースアプローチ）

- **RBAを前提としたプライバシーポリシー**
  - 高リスク処理（例：中国からの越境移転、センシティブデータ処理）には追加保護措置を必須化。
  - 低リスク処理（国内の簡易な通報）は比例的措置に留める。

- **PIIA/DPIAの義務との連動**：
  - EU：ホットラインは「高リスク」→DPIA必須。
  - 中国：越境移転は「高リスク」→PIIA必須。

- **文書化**：
  - プライバシーポリシー本文に「RBAに基づきリスクを特定・評価し、必要な措置を講じる」と明記。

リスクベースアプローチ（RBA）の適用

ステップ① データ処理マッピング
- 通報経路、情報の種類、越境有無を把握。

ステップ② リスク評価
- センシティブ性、処理規模、越境移転の有無・移転先、匿名性確保難易度報復リスク等。
- 発生可能性（1～5）×影響度（1～5）＝リスクスコア。

ステップ③ リスク区分別対応
- **低リスク**：通常の制御＋短期保存。
- **中リスク**：SCCによる移転、匿名化推奨。
- **高リスク**：DPIA/PIIA必須、暗号化、多層アクセス、監査ログ、保存短縮。
- **超高リスク**：現地完結処理（中国国内保存）、域外移転回避。

ステップ④ 文書化・説明責任
- リスク評価結果を記録・取締役会報告。
- 善管注意義務の裏付け。

ステップ⑤ モニタリング・改善
- KPI（件数・応答時間・是正率・再発率）と連動。
- 法改正に応じ継続的更新。

リスクマトリクスの具体例

リスク要因	発生確率	影響度	合算スコア	リスク評価	対応策
GDPR域外から情報受領	3	5	15	超高	標準契約条項（SCC）の導入＋DPIA
中国拠点越境データ	4	5	20	超高	セキュリティ評価＋PIPL同意取得
匿名通報で身元追跡困難	2	3	6	中	通報プラットフォームで双方向質問体制
社内報復懸念による通報抑制	3	4	12	高	保護ポリシー徹底＋トップメッセージ発信
多言語対応遅れ	2	2	4	低	ホットラインベンダーに委託

グローバルプライバシーポリシーとの統合

□ 必須要素

1. **目的**：通報調査・是正のための個人データ処理。
2. **情報範囲**：通報者・被通報者情報、証拠（Eメール等）、センシティブ情報は必要最小限。
3. **法的根拠**：
   GDPR＝正当利益／義務遵守
   APPI＝目的明示＋安全管理措置
   PIPL＝明示的同意＋影響評価
4. **保持期間**：調査終了後最小限（例：5年）。
5. **第三者提供・越境移転**：本社・地域ハブ・外部調査機関、適法な移転根拠に基づく。
6. **通報者・被通報者の権利**：開示・訂正・異議申立、ただし調査を害さない範囲で制限可。
7. **周知・透明性**：全従業員ポータル掲載、多言語化。

□ RBAとの接続

- 高リスク処理＝追加措置必須（暗号化、PIIA、国内保存）。
- プライバシーポリシー本文に「リスク評価に基づく管理」を明記。

RBAに基づく中国個人情報保護法（PIPL）対応の具体例

ステップ	内容	PIPLとの整合性
① データ処理のマッピング	• 中国拠点で収集される通報内容と個人データの種類（センシティブ性）を整理 • 越境を伴うか確認	• PIPLが高リスクとみなす項目（越境・センシティブ）を可視化
② リスク評価（RBA）	• 影響度（個人権利侵害、国家の監視対象等）を評価し分類 • 高リスク案件の基準定義（例：10000件以上の通報、センシティブ含む）	• PIPLが規定する基準との一体運用（PIIA対象判断）
③ リスクレベル別の措置策定	• **低リスク**：SCCs＋ログ管理＋説明通知のみ • **高リスク**：CACセキュリティ評価or認証＋暗号化＋アクセス制限 • **超高リスク**：国内サーバ保管＋現地窓口で完結	• PIPL第38～41条に基づく越境手段を適用
④ 文書化・通知・同意管理	• ・PIPLが求める「個人別通知」「明示的同意」をリスクレベルに応じて取得・記録 ・越境時には受領者名、目的、公権利行使方法等を通報者に通知	• PIPL第17～18条、第39条に対応
⑤ 影響評価・監査(PIIA／PI監査)	• 高リスク処理にはPIIAを実施 • 監査対応体制整備（文書化・証拠保存・監査ログ）	• PIPL第55条：PIIA義務に準拠、PI監査の要件も満たす
⑥ 継続的モニタリングとレビュー	• PIPL法制度改正やデータ処理実態の変化に応じ定期的見直し • CACFAQなど最新ガイダンス反映	• 最新法令をフォローし、RBAの再評価を実施

取締役の善管注意義務とグローバル法対応（あくまで私見）

- **法的枠組み**：会社法330条・民法644条に基づき、取締役は「その地位・状況にある者に通常期待される程度」の善管注意義務を負う。外国法対応も射程に入り得る（大和銀行株主代表訴訟：大阪地判2000/9/20）。

- **現実的限界**：新興国を中心に規制は不安定。全ての国の非本質的・独特な規制を“疑義なく網羅的に”遵守するのは現実的に困難。

- **合理的水準（求められる対応）**：
  - 各国に共通・普遍的な3要素に重点：
    1. **情報提供**（透明性）
    2. **適法化根拠の整備**（同意／契約／正当な利益）
    3. **データ主体の権利対応**（アクセス・訂正・削除）
  - RBAで高リスク領域に資源集中（DPIA/PIIA、越境移転管理、暗号化、監査証跡）
  - データ主体の合理的期待を外さない運用（目的外利用の回避、最小化、周知）

- **結論**：上記の合理的措置を講じれば、グローバル内部通報システム（※グローバルプライバシーポリシー前提）導入・運用は、取締役の善管注意義務に反しないと評価し得る。