内部通報と各国個人情報保護法

（中国、シンガポール、タイ）

大江橋法律事務所
弁護士　藤本　豪

0. はじめに

【本章の目的】
内部通報への対応にあたっては個人情報保護法の観点からの準備と工夫が不可欠であることを理解する

本講演は以下の流れで進めていきます。

Ⅰ.　内部通報に関する個人情報保護法上の論点
Ⅱ.　各国の個人情報保護法の特徴
Ⅲ.　基本的な対応事項
Ⅳ.　各論点の説明
Ⅴ.　質疑応答

■こんなとき、どうしますか?

【例①】
現地（海外）からの内部通報を受け、本社と現地法人が協力して調査していたところ、通報対象者から、「この調査のために私の個人情報を取り扱うことは、当国の個人情報保護法に違反しているので、ただちに取扱いを停止して頂きたい。」と言われた。

【例②】
現地（海外）からの内部通報を受け、本社と現地法人が協力して調査した結果、従業員による不正行為が発覚したので、当該従業員を解雇した。その後、当該従業員が現地法人及び本社に訴訟を提起し、解雇の無効確認、未払い賃金の支払い請求に加えて、個人情報保護法違反に基づく損害賠償請求を行った。

■内部通報と個人情報保護法との関係

●個人情報保護の問題が最もクローズアップされるのは、本人の意に反して個人情報が収集・利用される場面

●内部通報は、本人の意に反して個人情報が収集・利用される場面の最たるものと言えるので注意する必要があり

●近年、GDPR（一般情報保護規則：General Data Protection Regulation）が施行されてから各国において、個人情報保護に関する権利意識が急激に高まっている背景がある

↓

通報対象者その他の関係者が個人情報保護法を武器に調査妨害や会社への損害賠償請求を行わないよう（行われたとしても防御できるよう）、内部通報への対応にあたっては個人情報保護法の観点からの準備と工夫が不可欠

■個人情報を武器として用いるというのは

①開示、利用停止、削除等の請求

どの国の個人情報保護法にも本人の権利として規定されている。本人が請求を拒絶できる例外の事由にあたるか否かがポイント。

②個人情報保護法違反に基づく損害賠償請求

認定された損害額の２～３倍となる金額が加算された懲罰的な損害賠償を認める個人情報保護法もある（例:タイ）

個人情報保護法に違反していないと説明できるか否かがポイント

↑

グローバル内部通報対応においては

各国の個人情報保護法の理解が必要。

Ⅰ．内部通報に関する個人情報保護法上の論点

【本章の目的】 内部通報との関係でクリアしなければならない個人情報保護法上の論点としてどのようなものがあるかを理解する

１，内部通報との関係でクリアしなければならない論点

個人情報保護法が使われる場面は様々ですが、その中で内部通報との関係でクリアしなければならない論点を挙げています。

①通報内容に、通報者のみならず他の従業員の個人情報が含まれる。場合によっては社外の人の個人情報も含まれる可能性がある。本人の知らないところで通報内容に記載された個人情報が移転しているということになるので、個人情報保護法をどう扱うかが問題になる。

②通報内容にセンシティブ情報（要配慮個人情報）が含まれる可能性がある。ケースとしては少ないが具体的には健康情報や刑事手続きや犯罪の履歴が含まれている場合はどうするか考える必要がある。

③通報対象者にとっては、不正が発覚すると不利益な処分を受ける場合があり、自己の意に反する目的・方法で個人情報が取り扱われることになる（場合によっては社外の人も同様）。

④通報対象者等から個人情報の開示請求等を受けた場合どう対処するか

⑤本人の所在する国以外に個人情報が移動することを越境移転と言う。海外拠点の通報者が日本本社に通報することは特に問題ないが、現地法人で受け付けた通報を日本本社へ移転する際には越境規制の問題が出てくることになる。

⑥いったん日本に送られた個人情報が更に他の国へ転送される場合もある。その際は越境移転のルールが各国でどう定められているのか確認する必要がある。

⑦ベンダーの通報受付サービスを利用する場合の扱い。例えばダイヤル・サービスを利用する場合に注意するべきこと。

↓

これら７つのポイントが内部通報との関係では

個人情報保護法上どう扱われるか？

この７つのポイントついて、しっかり検討して

論点をすべてつぶしておく必要があります。

そのためには各国法を理解することが必要です。

２，各国個人情報保護法の分析の視点

【各国の個人情報保護法を横断的に理解するための視点】

●個人情報の利用目的の特定
●本人への情報提供
●個人情報の取扱いの正当化要素（本人の同意、正当な利益等）
●センシティブ情報（要配慮個人情報）の取扱いについての本人同意
●個人情報の第三者提供（事務委託等を含む）に必要な要件の充足
●個人情報の越境移転に必要な要件の充足
●個人情報の取扱いの記録項目、記録義務の有無
●個人情報の保存期間の制限
●データセキュリティ措置（人的、物理的な安全措置）
●Cookieに関する規制
●個人情報の販売に関する規制
●個人情報保護責任者の指定
●本人からの権利行使への対応
●インシデント（漏洩等）発生時における対応（当局への報告を含む）

II. 各国の個人情報保護法の特徴

【本章の目的】
中国、シンガポール、タイの個人情報保護法にそれぞれ特徴があることを説明していきます。

１，中国の個人情報保護法

【法令】個人情報保護法（个人信息保护法）（2021年11月1日施行）

【十分性認定等】EUの十分性認定なし、CBPRも未参加

→施行以前には各法令に分散されていたものを統合した以上に、様々な内容が盛り込まれています。「十分性認定」というのは他国から越境移転について十分な保護があると認定されることで、認定はされておらず、EUの十分性認定も受けていません。越境プライバシールールも参加していません。

＜特徴的な点＞
●個人情報の取扱いの委託、第三者提供、センシティブ情報の取扱い、越境移転等につき、PIA（個人情報保護影響評価）の実施及び記録が義務付けられている（55条）
→日本法では義務付けられていない。

●越境移転については、政府による安全評価か、指定機構による個人情報保護認証、又は標準契約のいずれか一つの締結が要求されている（38条1項）
→多くの企業が選ぶのが標準契約となると思われる。

●個人情報の取扱いに関する定期的なコンプライアンス監査が義務付けられている（54 条）

●同法違反に基づく損害賠償請求においては過失の立証責任が取扱者側に転換されている（69条）
→違反を主張する人が損害賠償請求をした場合、請求をされた側が自分には過失がないことを立証しなければならないということ。請求をするハードルが下がり、受ける側の防御が大変になるということになります。

●域外適用を受ける者は中国国内に専門機構を置くか代表者を指定のうえ連絡先等を当局に報告しなければならないとされている（53条）
→中国の個人情報保護法は原則として国内でしか適用されないが、一定の要件を満たせば国外でも適用されることになります。

【参考】下位法令・ガイドラインの制定状況

●個人情報安全影響評価ガイドライン（个人信息安全影响评估指南）
（GB/T39335-2020）（2021年6月1日施行）

●個人情報越境処理活動安全認証規範（个人信息跨境处理活动安全认证规范）（2022年6月24日）

●個人情報越境標準契約規定（意見募集稿）（个人信息出境标准合同规定）（2022年6月30日）

２，シンガポールの個人情報保護法

【法令】
Personal Data Protection Act 2012(PDPA)
（2022年10月1日改正法施行、上位法）
Personal Data Protection Regulations 2021(PDPR)
（2021年2 月1日施行、下位法）

【十分性認定等】EUの十分性認定なし、CBPRには参加（2018年2月）

＜特徴的な点＞
●Business Contact Information（氏名、役職名、職位、業務上の電話番号、業務上の住所、業務上の電子メールアドレス、業務上のファクシミリ番号、その他これらに類する情報であって、個人的な目的のためにのみ提供されるものでないもの）を一般に適用対象から除外している（4条5項）
　→いわゆる「名刺情報」は個人情報適用対象にしないということで、ビジネスに優しい法律を作っているという印象を受けます。

●センシティブ情報の定義がなく、特別扱いを定めていない（ただし若干の修正あり）

●本人の同意を得ずに個人情報の取扱いが認められる場合（本人の重要な利益、公益事項、正当な利益、事業資産取引、事業改善目的等）について別紙で詳細に定めている（17条1項、別紙1及び2）
　→特に正当な利益～事業改善目的については企業側の立場が理解されている例外項目だと言えます。

●通知によるみなし同意の制度（15A条）。影響評価を行ったうえで目的及び異議申し立て期間を本人に告知するための合理的な措置をとり、期間内に異議がなかった場合には同意があったとみなされる。（ただし、広告のためのメッセージ送信目的には不適用）

●域外適用の要件を規定しておらず、シンガポール国内の個人情報を取り扱う

場合には一般に域外適用されると解されている。

●同法の適用を受ける組織は、同法を遵守することを確保するための責任者を指定のうえ、その連絡先を公開しなければならない（11条3項、5項）

３，タイの個人情報保護法

【法令】Personal Data Protection Act B.E.2562（2019）
（2022年6月1日全面施行）
【十分性認定等】EUの十分性認定なし、CBPRも未参加
　→タイには以前は個人情報保護法がなく、各種法令はあったものの、あまり意識されていなかった

＜特徴的な点＞
●GDPR（一般情報保護規則：General Data Protection Regulation）に限りなく似た内容

●同意を得るための求めは、性質上不可能な場合を除き、書面又は電子的手段により明示的になされる必要がある（19条2項）

●管理者（data controller）の指図に従わない処理者（data processor）は管理者とみなされる（40条2項）
　→データ管理者はデータの扱い方を決めることができる者、データ処理者は管理者の指示に従い作業を行う者を指します。指示に従わない処理者は管理者とみなされるということになります。

●域外適用を受ける者はタイ国内の代表者を書面で指名しなければならない（例外あり）（37条5項、38条1項）

●同法違反による損害については無過失責任及び懲罰的損害賠償が定められている（77条1項、78条）

【参考】下位法令・ガイドラインの制定状況

●データ処理者による処理記録活動の準備及び維持についての規則及び手続に関する個人情報保護委員会の通知（2022年12月17日施行予定）

●データ管理者のセキュリティ措置に関する個人情報保護委員会の通知（2022年6月21日施行）

●小規模事業者であるデータ管理者の処理活動記録の要求の免除に関する個人情報保護委員会の通知（2022年6月21日施行）

●行政罰に関する個人情報保護委員会の通知（2022年6月21日施行）

●本人からの同意取得に関するガイドライン（2022年9月7日）

●本人からの個人データの取得のための目的及び詳細の通知に関するガイドライン（2022年9月7日）

●個人情報の越境移転に関する個人情報保護委員会の通知（パブコメ募集版）（2022年9月29日）

４，日本の個人情報保護法（参考）

【法令】個人情報の保護に関する法律　（現在、改正法を段階的に施行中）
【十分性認定等】EUの十分性認定あり、CBPRに参加

＜特徴的な点＞
●個人情報と個人データという２つの概念
　→他国ではない概念です。

●個人情報取扱事業者の定義（個人情報データベース等を事業の用に供している者）
　→他国ではない概念です。

●個人情報の管理者（controller）と処理者（processor）という分け方をしていない

●仮名加工情報、匿名加工情報、個人関連情報という概念

●原則として本人の同意が不要とされている
　→他国との大きな違いになります。ＧＤＰＲのように正当な利益による適法化を認めていないにもかかわらず、原則として、利用目的を本人が知りうる状況になっていれば個人情報の取得や取扱いが可能になるとされています。ただし、第三者提供の場合等、例外が多いので、実務面では本人同意を取る場合が多いです。

●本人の同意を正当化根拠として越境移転を行うには外国の個人情報保護法に関する情報を提供することが必要

→日本国から越境移転させる場合、本人の同意を得る方法と本人の個人情報を適切に保護されることを確保するために必要な措置をとる方法がある。本人の同意を得るために外国の保護法に関する情報を提供しなければならない。個人情報保護委員会の調査結果は、すべての国の法律に関する情報をカバーしているわけではないので、2番目の方法を取る企業が多いです。

５，「取扱い」の定義（参考）

国	個人情報保護法における「取扱い」（processing）の定義
中国	収集、保存、利用、加工、移転、提供、開示、削除等（4条2項）
シンガポール	記録、保持、組織化、適応化、変更、復活、結合、変形、消去、削除を含む、単独又は一連の扱い（2条(1)） ※ただし、基本的な規制対象行為は「収集」「利用」「開示」
タイ	概念なし。収集、利用、開示が規制対象行為
日本	定義なし。概ね「利用すること」といった意味で用いられている

一見似たようなルールに見えても、基本的な概念すら各国で異なる。日本では広く「利用する」としていても、中国では「収集」から「削除」まで細かく定義されているわけで、現地法の理解をしていないと思わぬ不意打ちを食らうことも起きてしまいます。

→きちんとした理解が必要

III. 基本的な対応事項

【本章の目的】内部通報につき、個人情報保護法との関係で行っておくべき最も基本的な事項を解説します。

１，基本的な対応事項:通報対応のための取扱いの正当化

■日本本社による内部通報対応（受付、調査、処分等）を正当化するための要件を満たすこと

【中国法】
●同意による正当化の他、「労働関連の内規又は労働協約に基づき労務管理を実施するために必要な場合」（13条1項2号）として正当化が考えられる。ただし、別法人による 個人情報の取扱いは同号でカバーされない可能性がある。

→18条にあるように「人の生命・身体等保護のために必要な場合は同意を得ることなく個人情報を取り扱うことが可能」と定められていますが、そういった条文が正当化の根拠に使えるかどうかという質問がありました。日本の場合、財産（会社の利益）保護の目的の場合は同意を取らなくてよいとされていて、実務面で例外要件として活用される場合が多いのですが、中国では会社財産の保護が例外要件として認められるかというと難しいと思われます。人の身体、生命が害される危険性が実際に存在する場合には、例外として認められます。

【シンガポール法】
●同意の他、正当な利益（legitimate interest）（17条(1)(c)、別紙1第3部分）による正当化が考えられる。

●「会社による調査又は手続きに必要な場合」には正当な利益ありとされている（別紙1第3部分3）。なお、本人の評価及び調査（17条(1)(c)、Part3の2、3）、雇用関係の管理又は終了（17条(1)(c)、Part3の10）による正当化は、別法人による個人情報の取扱いは適用困難と考えられる。

●また、通知によるみなし同意の制度（15(A)条）は、本人による通知により破られてしまうので、内部通報の場面では使えない

【タイ法】
●同意の他、正当な利益（legitimate interest）による正当化が考えられる（24条5号）

■ただし、センシティブ情報が含まれる場合には

【中国法】
センシティブ情報（医療健康情報、足跡に関する情報等）を取り扱うには、本人の個別の同意が必要（29条）。また、個人情報保護影響評価の実施も必要（54条1号）

【タイ法】
犯罪記録、健康情報等の個人情報を取り扱うには、本人の明示の同意が必要（26条）

【シンガポール法】
センシティブ情報について別扱いを設けていない。ただし、PDPC（Personal Data Protection Commission）の下記2017年決定は、センシティブ情報については高いレベルの保護が必要であるとして、本人の同意のない第三者提供を違法（24条違反）と判断した。

↓

したがって、健康情報のようなセンシティブ情報については

本人の同意を得ることが必要と解される可能性がある。

結論として、各国において従業員の同意を取得しておくべき

■同意文言の例　：　網羅的に作成することが重要

●●社の従業員及び役員に関する下記(i)(ii)(iii)の個人情報は、●●社及びその親会社である日本の■■社による、内部通報の受付、調査、是正に必要な措置（懲戒処分や関連当局への通報を含みます）及びその他の必要な対応のために利用されることがあります。内部通報は、●●社の従業員及び役員のみならず、●●社を退職した者や、その関連会社及び取引先の従業員及び役員（退職した者を含みます）によってなされる可能性があります。個人情報は、上記目的の達成のため日本の■■社に提供され、上記目的の達成及び関連する社内管理に必要な期間（内部通報への対応に関する記録の保管期間を含みます）、●●社及び日本の■■社において保存されます。(i)会社名、所属、役職、氏名等、本人を特定する情報(ii)法令違反又は社内規程違反に該当する疑いのある言動及びその他の社内外での言動（犯罪及び刑事事件に関する情報並びに健康情報を含むことがある）(iii)会社のシステムを用いた電子メール、電話、Web会議等の交信内容

各国の個人情報保護法においては、個人情報の取扱いにあたり、本人に一定の情報を提供することが要求されている。

↓

各国において、所定の情報を従業員等に告知しておくべき

＜本人への情報提供＞

【中国法】

①	個人情報の取扱い一般のために必要な情報	個人情報取扱者の名称又は氏名及び連絡方法、個人情報の取扱いの目的、取扱いの方法、個人情報の種類、保存期間、本人による権利行使の方法及び手続、その他法令の定める事項（17条1項）
②	センシティブ情報の取扱いのために必要な情報	センシティブ情報を取り扱う必要性及び本人の権利利益に及ぼす影響（30条）
③	第三者提供のために必要な情報	被提供者の名称又は氏名、連絡方法、取扱いの目的、取扱いの方法、個人情報の種類（23条1項）
④	越境移転のために必要な情報	受領者の名称又は氏名、連絡方法、取扱いの目的、取扱いの方法、個人情報の種類、本人による権利行使の方法及び手続等（39条）

【シンガポール法】

①	個人情報の取扱い一般のために必要な情報	収集、利用又は開示の目的、（本人から求めがあった場合）質問に回答できる連絡先（20条(1)(4)(5)） これに加え、個人情報保護法遵守責任者の連絡先を公開することが必要（11条(5)）
②	センシティブ情報の取扱いのために必要な情報	同上（特に規定なし）
③	第三者提供のために必要な情報	同上（特に規定なし）
④	越境移転のために必要な情報	越境移転につき同意を根拠とする場合には、越境移転される個人情報がシンガポール法による保護と同等の水準で保護される範囲について、合理的な概要を事前に書面で提示することが必要（PDPR10条）

【タイ法】

①	個人情報の取扱い一般のために必要な情報	収集・利用又は開示の目的、収集される個人情報、保有期間（特定できない場合は予想期間）、開示先の種類、データ管理者の情報・住所・連絡先、データ管理者の代表者又はデータ保護責任者が存在する場合はその情報・住所・連絡先、本人の権利（23条）
②	センシティブ情報の取扱いのために必要な情報	同上（特に規定なし）
③	第三者提供のために必要な情報	同上（特に規定なし）
④	越境移転のために必要な情報	個人情報保護水準が十分でない国への移転の場合には、当該外国の個人情報保護水準が十分でない旨、情報提供する（28条1項2号）

【日本法】

①	個人情報の取扱い一般のために必要な情報	個人情報取扱事業者の氏名又は名称、全ての保有個人データの利用目的、本人からの請求に応じる手続（以上、32条1項）、保有個人データの取扱いに関する苦情の申出先、当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては当該認定個人情報保護団体の名称及び苦情の解決の申出先（以上、施行令8条）
②	センシティブ情報の取扱いのために必要な情報	同上（特に規定なし）
③	第三者提供のために必要な情報	（共同利用の場合）共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的並びに当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名（27条5項3号）
④	越境移転のために必要な情報	（同意により正当化する場合）外国における個人情報保護制度等の参考情報（28条2項）

IV. 各論点の説明

【本章の目的】内部通報対応において個人情報保護法との関係で問題となる様々な論点を俯瞰し、基本的な考え方を理解する

■そもそも各国法が適用されるか?

【中国法】

①通報者個人への適用	個人情報の取扱いの目的及び方法を決定する者であれば、個人又は家庭の事務による個人情報の取扱いを除き、個人であっても適用される（72条、73条1号）。 →内部通報の通報者がこれにあたるかは微妙だが、あたる（適用される）と判断される可能性もあると考える。
②日本本社への域外適用	中国域内の自然人の行為を分析、評価する場合に域外適用される（3 条2号）。 →本社による内部通報の処理に域外適用される可能性がある。

【シンガポール法】

①通報者個人への適用	シンガポールの個人情報上の義務は組織（organization）を名宛人としており、従業員としての個人には適用されない
②日本本社への域外適用	シンガポールにいる個人の個人情報の取得、利用、開示については域外適用される

【タイ法】

①通報者個人への適用	個人情報の取得、利用又は開示について決定する権限と義務を持っている者であれば、個人であっても適用される（6条）
②日本本社への域外適用	タイ国内でなされるデータ主体（本人）の行為を監視（monitoring）する場合には域外適用される（5条2項2号）。 →場合によっては日本本社による通報内容の処理に域外適用される可能性もあると考える。

【日本法】

①通報者個人への適用	日本国内にある者を本人とする個人情報の取扱いでないため、適用されない（166条参照）
②日本本社への域外適用	日本法が適用される

■域外適用を受ける場合の義務

【中国法】
域外適用を受ける者は中国国内に専門機構を置くか代表者を指定のうえ連絡先等を当局に報告しなければならない（53条）
　→代表者を指定はしても当局に報告まで行っている外国企業がどの程度あるか。実際には少ないと思われます。

【シンガポール法】
域外適用を受ける組織は、同法を遵守することを確保するための責任者を指定のうえ、その連絡先を公開しなければならない（11条3項、5項）

【タイ法】
域外適用を受ける者は、タイ国内に所在する代表者（個人情報の取扱いにつき代理権をもつ）を書面で指名しなければならない（例外あり）（37条5項、38条）

　→例外に当たる場合も多く、タイ国内からセンシティブ情報を収集する者は例外に当たりませんが、そうではなくかつ収集する個人情報の数が少ない場合は例外として書面は不要になります。

論点① 他者の個人情報が含まれる

論点① 通報内容に通報者以外の従業員の個人情報が含まれる。場合によっては社外の人の個人情報も含まれる可能性がある。

●全従業員に対し、事前に必要事項を通知の上、同意を取得しておく（「III. 基本的な対応事項」を参照）。

●それとともに、「正当な利益」による正当化を説明できるよう、目的外利用

の防止を徹底する等の措置を講じる。

　→同意で対応すればいいと思うかもしれませんが、例えばGDPRでは、同意には任意性と撤回する機会が必要とされるなど厳しい要件が必要とされています。各国の法令にはそれに似た要件が設定されていることが多く、従業員からの同意というのは正当化事由に使えない可能性を孕んでいます。

●社外の人については、事前に同意を取得することができないため、ケース・バイ・ケースで対応。

●ヒアリング開始前に個別の同意を取得する。

論点② センシティブ情報が含まれる可能性

論点②通報内容にセンシティブ情報（要配慮個人情報）が含まれる可能性がある。

●全従業員に対し、事前に必要事項を通知の上、同意を取得しておく（「III. 基本的な対応事項」を参照）。

●社外の人については、事前に同意を取得することができないため、ケース・バイ・ケースで対応。
　→社外の人にセンシティブ情報はあらかじめ扱わないと決めることも実務上考えられます。

●ヒアリング開始前に個別の同意を取得する。

論点③ 自己の意に反する取扱い

論点③　通報対象者にとっては、自己の意に反する目的・方法で個人情報が取り扱われることになる（場合によっては社外の人も同様）。

●全従業員に対し、事前に必要事項を通知の上、同意を取得しておく（「III. 基本的な対応事項」を参照）。

●それとともに、「正当な利益」による正当化を説明できるよう、目的外利用の防止を徹底する等の措置を講じる。

●社外の人については、事前に同意を取得することができないため、ケース・バイ・ケースで対応。

●ヒアリング開始前に個別の同意を取得する。

論点④ 本人からの開示請求等への対処

論点④本人（通報対象者等）から開示請求等を受けた場合、どのように対処すればよいか

日本法の場合、「当該個人データの存否が明らかになることにより、違法又は不当な行為を助長し又は誘発するおそれがあるもの」は「保有個人データ」に含まれず（法16条4項、施行令5条2号）、また、「本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合」は開示の請求を拒否できるとされている（33条2条1号）。
　→ここで言う「財産」には会社の財産も含まれており、内部通報の対象となった行為を放置しておくと、やがて会社の財産が害される恐れがあるため、開示の請求を拒否できるという理由付けができようになっています。

■同様の規定が各国法においても存在するか?

【中国法】
●法令により秘密保持が要求され又は利用目的等の告知が不要とされている場合は、本人は開示請求権をもたない（45条、18条1項）。

●この法令は下位法令のため現在未成立で、判断がつかない状況です。

【シンガポール法】
●調査又は手続に必要な場合には正当な利益（legitimate interest）があるため（別紙１ 第３部分３）、個人情報の収集、利用、開示につき本人の同意は不要とされている。この場合、同意を得ずに収集、利用、開示された個人情報は、当該調査及び付帯する手続が完了していない限り、本人による権利行使の対象とならない（21条(1)、別紙5 の1(h)）。

●調査・手続きの完了後については、明確な根拠なし → 個別の判断・対応が必要

【タイ法】
●開示によって他者の権利及び自由を害するおそれのある場合には、開示請求を拒否することが可能（30条2項）

●ただし、開示請求の拒否について、その拒否を裏付ける理由とともに記録することが必要（30条3項）

【GDPR】
●個人データの処理の目的の達成を不可能にし、又は著しく損なわせる可能性がある場合には、開示請求を拒否することが可能（14条5項(b)）

●ただし、データ主体の権利・自由及び正当な利益を保護するための適切な措置を講ずることが必要（同条項）

→GDPRのルールつくりは合理的で、目的外利用されないようにしたり、データセキュリティ措置を図っていれば、正当な目的の達成のために利用すること、開示請求を拒否することが可能とされている。

→本人から開示請求される可能性については、特に紛糾した場合は取れる手段はなんでも取ってくるので警戒しておく必要があり、現地の弁護士とタイアップして適切な対応が必要です。

論点⑤ 越境移転

論点⑤個人情報の越境移転がなされる。

以下の２つの場合を区別して考える。
(a) 通報者が現地法人を介さず直接日本に通報内容を送る場合
(b) 通報者がいったん現地法人に通報を行い、現地法人から日本本社に通報内容を提供する場合

(a)の場合 ⇒ 越境移転を行っているのは現地法人ではなく通報者個人。
●シンガポール法では、従業員としての個人には規制が及ばないので問題ない。

●中国法とタイ法は従業員としての個人も規制の対象となり得るが、当局がこれを問題視する可能性はまずないと考えられる。

→中国もタイも個人情報保護法が施行されて間もないこともあり、優先して対処すべき問題が多く、当局としては優先事項を処理していくはずなので、日本本社への通報という正当性の高い行為について目くじら立てて規制していくとは考えられない。

(b)の場合 ⇒ 現地法人が越境移転を行っているので、現地法上の要件を満たすことが必要。

■各国の越境移転規制

【中国法】
●個人情報保護影響評価の実施及び処理状況の記録（55条）（規則を制定中。当面、2019年6月13日に出された「個人情報出境安全評価弁法」（个人信息出境安全评估办法）の意見募集稿、及び、「個人情報安全影響評価指南」（个人信息安全影响评估指南）（GB/T 39335-2020）を参考にすることが考えられる。）

●域外での取扱いが中国の個人情報保護基準に達するために必要な措置を講じる（38条3項）
　→個人情報の越境移転を受ける者とする者との間に契約を締結して提供を受ける者の義務をしっかり定めておくということが必要だと考えています。

●本人への情報提供及び同意取得（39条）

●標準契約の締結（38条1項3号）（当局への写しの提出が要求される可能性あり。 規則の制定待ち。当面、2022年6月30日に出された「個人情報出境標準契約規定」（个人信息出境标准合同规定）の意見募集稿に従って締結することが考えられる。）
　→パブリックコメント募集版の別紙に標準契約書が添付されていたので、この内容で定められることが考えられます。また、標準契約書を締結したら速やかに当局に提出するとされているので、もしこの内容のまま正式な法令として成立した場合には、そのような運用になると思われます。

【シンガポール法】
●受領者にシンガポール法と同等の保護基準を保証させる。具体的には受領者との間で適切な内容の契約を締結する（PDPA26条(1)、PDPR10条(1)、11条(1)(b)及び（2））。

●上記の代替措置として、シンガポール法との比較で域外における保護の程度の概要を記した書面を本人に提供したうえで、本人の同意を取得するという手段もある（PDPR10条(2)(a)、同条(3)(a)）

【タイ法】
●適切な水準の個人情報保護制度を有していると認められた国への移転には、越境移転規制が適用されない（28条1項柱書）。（日本がこれにあたるか否かは、現時点では不明。委員会の細則待ち。）

●相手国の個人情報保護水準が十分でないことを本人に通知した上で、本人の

同意を取得（28条1項2号）

●上記の代替措置として以下のものがある。
・企業グループの個人データ保護方針につきタイ当局の審査及び認定を受けること（29条1項）
・本人の権利行使を可能にする適切な保護措置を提供すること（29条3項）（保護措置の具体的な内容は、委員会の細則待ち。パブリックコメント募集版には、標準契約条項についての定めが存在。）
　→パブリックコメント募集版には、グループ会社内での内部規則を作って、当局に認証を得る。SCCに対応する標準契約条項を締結する。といったことが書かれています。また、標準契約を締結した後、タイ当局に提出することが求められています。

論点⑥ 日本から第三国への再移転

論点⑥いったん日本に来た個人情報が更に他の国へ転送される場合もある。

日本の個人情報保護法の越境移転の要件（28条）を満たすことが必要。
(a)外国の個人情報保護法の情報を提供のうえ本人の同意を得る、又は
(b)相当措置の継続的な実施を確保するために必要な措置を講じる

　→本人が外国にいる外国人の場合、(a)の情報提供につき翻訳等の負担が生じる一方で、(b)の措置に関する情報提供（28条3項）を本人から求められる可能性が非常に低いため、(b)によるのが実際的。具体的には提供先との間で共同利用契約又はそれに類する契約を締結。

■それに加えて各国法の要件も満たす必要があるか?

●シンガポール法は通報を受けた日本本社に適用される。中国法とタイ法も適用される可能性があると考えられる。

●中国法、シンガポール法、タイ法のいずれも、越境移転の再移転（onward transfer）については定めていない。それぞれの越境移転規制の表現は次の通り。

【中国法】
「中華人民共和国の域外に個人情報を提供する場合」（38条1項）

【シンガポール法】
「シンガポールの外の国又は地域への個人情報の移転」（26条(1)）

【タイ法】
「外国に個人情報を送信又は移転する場合」（28条1項）

中国法、シンガポール法、タイ法のいずれの越境移転規制も、日本から第三国への再移転に適用される可能性がある。

日本から第三国への再移転について外国法の越境移転規制をどこまで遵守するかは、各社判断が分かれるところ。少なくとも、以下の対応を行っておくことが推奨される。
●本人への情報提供を可能な範囲で行ったうえで、同意（一般的、個別的）を得る
●提供先との間で共同利用契約又はそれに類する契約を締結する（これは日本の個人情報保護法への対応としても必要）

論点⑦ ベンダーの通報受付サービスを利用する場合の扱い

	内部通報に対応する企業	ベンダー（ダイヤル・サービス）
性質	個人情報の管理者（controller）	個人情報の処理者（processor）
利用目的	内部通報への対応	内部通報の受信及びクライアント企業への転送

●中国法及びタイ法は、基本的に管理者のみ規制対象としている（ただし、タイ法では、管理者の指示に基づかずに個人情報を取り扱った処理者は管理者とみなされる（40条2項））
　→ベンダーは規制対象外となる

●シンガポール法は、管理者・処理者を区別していないが、個人情報の取扱いの委託先（data intermediary）は規制の対象外とされている（4条(2)）（なお、委託者である管理者は、委託先による個人情報の処理について全責任を負うとされている（3条(3)））
　→ベンダーは規制対象外となる。

いずれにせよ、内部通報に対応する企業は、ベンダーの通報受付サービスを利用することにつき、各国の規制を遵守することが必要
　→ベンダーサービスの一つ、内部通報を受け付ける場面で、通報者に対して個人情報保護ポリシー（プライバシーポリシー）を表示する画面が提示されていることがあります。その中に現地法に対応できる情報を盛り込むことが大事だと考えています。

■個人情報の取扱いの委託を行うために必要な行為

【中国法】
●個人情報保護影響評価の実施及び処理状況の記録（55条）
●委託契約の締結（取扱いの目的、期間、取扱い方法、個人情報の種類、保護措置、当事者双方の権利義務等を規定）（21条1項）
●委託先の監督（21条1項）
　→影響評価についてどうするかは各社悩みどころだと思いますが、現地弁護士やコンサルタントのアドバイス、国家標準に基づいて行うことになります。

【シンガポール法】
●委託契約の締結（40条3項）

【タイ法】
●委託契約の締結（4条(2)）

【日本法】
●委託先の監督（25条）

Ⅴ．質疑応答

１，P46ご説明時に「ベンダーが通報を受け付ける画面に現地法に対応できる表示を行うことが重要」とのお話がありましたが、ダイヤル・サービス社ではご対応済でしょうか？

藤本：ダイヤル・サービス社のインターネット通報受付サービスでは、通報者が通報内容等を入力する前の画面に、クライアント企業様のプライバシーポリシーを掲載するページを設けており、対応済みです。プライバシーポリシーは、クライアント企業様がそれぞれの実情に応じて作成されるものです。

２，海外子会社の通報者からの内部通報受付につきまして、以下のように理解いたしました。
①あらかじめ当該子会社の従業員から内部通報処理に伴う個人情報収集・利用に関する事前の同意を受けておく
②正当な利益による利用を根拠とできるよう目的外利用の禁止等を徹底する
③個別案件ごとに同意取得する

これに加えて、事実確認等の調査開始を日本の本社で検討する際、被通報者（通

報対象行為の行為者等）から同意を受ける必要はありますでしょうか？　また、その場合はどのタイミングで同意を得る必要があるでしょうか？

藤本：①②③が必要であることにつき、ご理解のとおりです。個人情報保護法の観点のみを考えた場合には、早いタイミングで被通報者の同意を得ることが安全ということになりますが、内部通報の場面においては、早いタイミングで同意取得を試みることが通報制度の目的の達成を阻害する可能性もありますので、被通報者の同意は、被通報者からのヒアリングの際に取得することが、実務的な折り合いのポイントであろうと考えております。

３，同意取得について、難しい場合は正当利益の説明準備をしておくということでしたが、同意取得について、ある程度強制的なものとする手段（それが当該国で違反とならない方法で、事実上強制的となるもの）は何かありますか？

藤本：同意取得について、強制的というのは難しいですが、同意の対象を抽象的なものにするということが考えられます。何も起きていない段階で、他の事項と併せて、従業員にワンクリックで同意して頂くという扱いにすれば、従業員の心理的なハードルも下がると思われます。

◆また、同意を取得するとしても、被通報者においては、自身の何についての情報が域外移転されるのかは、通報があったときにならないと分からないという点からすると、日本本社へ移転される情報の具体性という点で同意が適切とはいえない（調査時に個別に取得するしかない）ということになるのでしょうか？

藤本：ご指摘のとおり、抽象的な事項についての事前の同意は、現地法上、適切ではないと評価される可能性があります。そのため、できるだけ、調査時にも同意を取得することをお勧めします。

４，全世界で事業展開しており、全世界の従業員から日本本社で内部通報を受け付けることとしている。調査・是正は海外の各地域（例：北米、南米、アフリカ、等々）を統括する主要現地法人に委ねることとしているが、全世界で事業展開しており、全世界の従業員から日本本社で内部通報を受け付けることとしている。具体的に必要となる事項を改めてご教示頂きたい。

藤本：今回ご説明させて頂いた３か国（中国、シンガポール、タイ）に関する必要事項で、対応の約80パーセントをカバーすることができると思います。これを基礎として、各国の法制度を調査することで残りの約20パーセントに対応する、というイメージです。

◆また、事案によっては日本本社が主体的に調査・是正に関与せざるを得ない場合に必要となる事項についてもご教示頂きたい。

藤本：日本本社が主体的に調査・是正に関与する場合に必要となる事項も、上記と同様に、今回ご説明させて頂いた３か国（中国、シンガポール、タイ）に関する内容が基本となると考えます。

◆また、内部通報を受けて被通報者から同意を得ることはほぼ不可能だが、どのように考えればよいか。

藤本：内部通報の進め方は各社様にて異なりますが、小職の経験では、被通報者のヒアリングの直前に、話した内容が本人の不利益に扱われる可能性や秘密保持等の点について同意を得るケースが多く、そのようなケースにおいては、個人情報の扱いについても同意を得るという実務が可能なのではと考えております。

５，通報者（海外従業員）が日本の本社に通報した場合、通報者は一個人であり、「個人情報保護法令」の適用を受ける「個人情報取扱者」にならないという解釈はできませんか？

藤本：ご指摘のとおり、通報者は日本の個人情報保護法の「個人情報取扱者」に該当しないと解されます。もっとも、海外従業員である通報者には、そもそも日本の個人情報保護法が適用されません。また、現地法（中国法、シンガポール法、タイ法）は、日本法のような「個人情報取扱者」という概念を採用しておらず、現地法が通報者に適用されるか否かは、それぞれの法令に基づく判断となります。（結論として、中国法は適用される可能性あり、シンガポール法は適用なし、タイ法は適用されると考えます。）

◆日本の個人情報保護委員会の方から、『同意を得ることが困難なケース（人の生命、身体又は財産の保護の為に必要がある場合）に該当する範囲であれば、本人の同意を得なくてもいいのではないか』という意見をいただいたことがあります。中国の個人情報保護法第 18 条にも同じような記載がありますが、この条文を利用することは可能でしょうか？（日本への通報ができる範囲をあらかじめ明確化する必要はあると思いますが）

藤本：日本の個人情報保護法では「財産の保護」を広く捉える解釈がなされていますが、中国の個人情報保護法につき同様の解釈がなされるかどうかは、今後の運用を見て判断する必要があり、現時点では、一般論として中国の個人情報保護法18条に頼ることは危険と考えます。もっとも、実際に人の生命や健康等に被害が生じるおそれがある場面では、18条2項を適用することが可能です。

◆日本の本社が内部通報を受け取った場合、対象者への通知（中国法ですと 17 条）は行うべきと理解すべきでしょうか？
その場合、「情報提供元」はＧＤＰＲと異なり通知は不要と理解して宜しいでしょうか？

藤本：中国の個人情報保護法17条は、必ずしも個々の具体的な取り扱いについての情報提供に限らず、プライバシーポリシー等による抽象的な情報提供も含むものですので、事前に全従業員への十分な情報提供を行っている限り、日本の本社が内部通報を受け取った場合に対象者に通知することは不要と考えます。