＜外国にある第三者が整備すべき体制と委員会規則（案）の対応表＞ 資料2－2

体制	委員会規則（案）
①提供元及び提供先（外国にある第三者）間の契約において、提供先が、我が国の個人情報取扱事業者が講ずべきこととされている措置に相当する措置を講ずることが担保されていること	規則１１条第１号 一　個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第四章第一節の規定の趣旨に沿った措置の実施が確保されていること。 ※法第四章第一節の規定の趣旨に沿った措置については、ガイドライン等により解釈を明示する方向
②提供元及び提供先（外国にある第三者）が同一の企業グループであり、当該グループのプライバシーポリシー等において、我が国の個人情報取扱事業者が講ずべきこととされている措置に相当する措置を講ずることが担保されていること	
③外国にある第三者が、個人情報の取扱いに関する国際的な枠組みの基準に適合している旨の認証を受けていること（例えば、アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システム）.	規則１１条第２号 二　個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。 ※CBPRシステムについては、ガイドライン等により明示する方向

＜「法第4章第1節の規定の趣旨に沿った措置」の考え方の一例＞

個人情報保護法の主な規定		OECDプライバシーガイドライン	APECプライバシーフレームワーク	法第4章第1節の規定の趣旨に沿った措置	備考 例：①日本にある個人情報取扱事業者が、外国にある事業者に顧客データの入力業務を委託する。 ②日本にある個人情報取扱事業者が、外国にある親会社に従業員情報を提供する。
第１５条	利用目的の特定	○	○	○	委託契約（例①）又は内規等（例②）により、外国にある第三者において実質的に「利用目的の特定」、「利用目的による制限」が図られている場合は、第15条、第16条の趣旨に沿った措置が講じられているものと整理する。
第１６条	利用目的による制限	○	○	○	
第１７条	適正な取得	○	○	○	外国にある第三者が委託契約(例①)又は内規等(例②)に基づいて個人データを取得をしていることが自明である場合は、そのことをもって第17条第1項の趣旨に沿った措置が講じられているものと整理する。
第１７条第２項	要配慮個人情報の取得の際には、同意が必要	×	×	―	国によっていわゆるセンシティブ情報の対象は異なり得ることから（OECDプライバシーガイドラインの説明覚書（1980年））、「要配慮個人情報」に係る規制を外国の事業者に課すことは適切ではないと考えられる。よって、第17条第２項は「措置」が求められる「規定」から外れるものと整理する。 なお、仮に第17条第２項が当該「規定」に含まれるとしても、外国にある第三者が同項の同意を得て要配慮個人情報を取得する際に、当該同意を第24条の「同意」と実質的に評価することができれば、そもそも「法第４章第１節の規定の趣旨に沿った措置」を講じる必要はない。
第１８条	取得に際しての利用目的の通知等	○	○	○	日本にある事業者から顧客（例①）又は従業員（例②）に対して取得目的の通知等が為されている場合は、第18条の趣旨に沿った措置が講じられているものと整理する。
第１９条	データ内容の正確性の確保等	○	○	○	（例①）委託契約によりデータ内容の正確性の確保等について規定されているか、又は、データ内容の正確性の確保等に係る責任を個人データの提供元たる個人情報取扱事業者が負うこととなっている場合は、第19条の趣旨に沿った措置が講じられているものと整理する。 （例②）日本にある事業者を通じて従業員情報の正確性を確保する等の措置が講じられている場合は、第19条の趣旨に沿った措置が講じられているものと整理する。

個人情報保護法の主な規定		OECDプライバシーガイドライン	APECプライバシーフレームワーク	法第4章第1節の規定の趣旨に沿った措置	備考 例:①日本にある個人情報取扱事業者が、外国にある事業者に顧客データの入力業務を委託する。 ②日本にある個人情報取扱事業者が、外国にある親会社に従業員情報を提供する。
第２０条	安全管理措置	○	○	○	委託契約（例①）又は内規等（例②）により外国にある第三者における漏えい防止などに係る措置が規定されている場合は、第20条の趣旨に沿った措置が講じられているものと整理する。
第２１条	従業者の監督	○	×	○	APECプライバシーフレームワークでは明示的に求められている規定ではないものの、従業者を適切に監督すべき義務は安全管理措置に係る義務の一環として通常講じられているものと考えられるため、第20条と同様に整理する。
第２２条	委託先の監督	○	○	○	委託先を監督する義務は安全管理措置に係る義務の一環として通常講じられているものと考えられるため、第20条と同様に整理する。
第２３条	第三者提供の制限	○	○	○	委託契約（例①）又は内規等（例②）により当該第三者からの個人データの移転が禁止されている場合は、第23条、第24条の趣旨に沿った措置が講じられているものと整理する。
第２４条	外国にある第三者への提供の制限	○	○	○	
第２５条	第三者提供に係る記録の作成等	×	×	×	国際的な枠組みとの整合性を勘案し、第25条、第26条は「措置」が求められる「規定」から外れるものと整理する。
第２６条	第三者提供を受ける際の確認等	×	×	×	

個人情報保護法の主な規定		OECDプライバシーガイドライン	APECプライバシーフレームワーク	法第4章第1節の規定の趣旨に沿った措置	備考 例:①日本にある個人情報取扱事業者が、外国にある事業者に顧客データの入力業務を委託する。 ②日本にある個人情報取扱事業者が、外国にある親会社に従業員情報を提供する。
第２７条	保有個人データに関する事項の公表等	○	○	○	提供する個人データが外国にある第三者にとって「保有個人データ」に該当する場合において、委託契約（例①）又は内規等（例②）により、委託元等が第27条～第33条に係る義務を履行することについて明確になっているときは、同条の趣旨に沿った措置が講じられているものと整理する。 なお、提供する個人データが外国にある第三者にとって「保有個人データ」に該当しない場合には、結果として「措置」としての対応は不要であるものと整理する。
第２８条	開示	○	○	○	
第２９条	訂正等	○	○	○	
第３０条	利用停止等	○	○	○	
第３１条	理由の説明（努力）	○	○	○	
第３２条	開示等の請求等に応じる手続き	○	○	○	
第３３条	手数料	○	○	○	
第３４条	事前の請求	×	×	×	第34条は日本における司法上の手続の規定であるため、「措置」が求められる「規定」から外れるものと整理する。
第３５条	個人情報取扱事業者による苦情の処理（努力）	○	○（※）	○	委託契約（例①）又は内規等（例②）により、委託元等が苦情処理に係る対応を講じることについて明確になっているときは、第35条の趣旨に沿った措置が講じられているものと整理する。 （※）APECプライバシーフレームワークでは明示的に求められている規定ではないが、APEC CBPRシステムに申請する事業者の要件として苦情処理体制が規定されているため、国際的な枠組みとも矛盾しない。

参考1．OECDガイドラインと改正個人情報保護法との対比表

プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告（2013)(抜粋)（仮訳※1）	改正個人情報保護法
第 2 部 国内適用における基本原則 収集制限の原則 7. 個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきである。	17条（適正な取得） 18条（取得に際しての利用目的の通知等）
データ内容の原則 8. 個人データは、利用目的の範囲内において利用し、かつ利用目的の達成に必要な範囲内で正確、完全及び最新の内容に保つべきである。	16条（利用目的による制限） 19条（データ内容の正確性の確保等）
目的明確化の原則 9. 個人データの収集目的は、データが収集された時点よりも前に特定し、当該利用目的の達成に必要な範囲内における事後的な利用又はその他の目的での利用は、その利用目的に矛盾しない方法で行い、利用目的を変更するにあたっては毎回その利用目的を特定すべきである。	15条（利用目的の特定）
利用制限の原則 10. 個人データは、第9 項により特定された目的以外の目的のために開示すること、利用可能な状態に置くこと又はその他の方法で利用すべきではない。ただし、以下の場合はこの限りではない。 a) データ主体の同意がある場合、又は、 b) 法令に基づく場合。	16条（利用目的による制限） 23条（第三者提供の制限）
安全保護措置の原則 11. 個人データは、その滅失若しくは不正アクセス、き損、不正利用、改ざん又は漏えい等のリスクに対し、合理的な安全保護措置を講ずるべきである。	20条（安全管理措置）
公開の原則 12. 個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づくべきである。その方法は、個人データの存在及び性質に応じて、その主要な利用目的とともにデータ管理者の識別及び通常の所在地を認識できる方法によって示すべきである。	27条（保有個人データに関する事項の公表等）

プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告（2013)(抜粋)（仮訳※1）	改正個人情報保護法
個人参加の原則 13. 個人は次の権利を有する。 a) データ管理者が自己に関するデータを保有しているか否かについて、データ管理者又はその他の者から確認を得ること。 b) 自己に関するデータを保有している者に対し、当該データを i. 合理的な期間内に、 ii. 必要がある場合は、過度にならない費用で、 iii. 合理的な方法で、かつ、 iv. 本人が認識しやすい方法で、 自己に知らしめられること。 c) 上記（a）及び（b）の要求が拒否された場合には、その理由が説明されること及びそのような拒否に対して異議を申立てることができること。 d) 自己に関するデータに対して異議を申し立てること及びその異議が認められた場合には、そのデータを消去、訂正、完全化、改めさせること。	28条（開示） 29条（訂正等） 30条（利用停止等） 31条（理由の説明） 32条（開示等の請求等に応じる手続き） 33条（手数料）
15. データ管理者は以下のことに責任を有する。 a) 以下のプライバシーマネジメントプログラムを構築すること。 i. 管理下にあるすべての個人データに対するガイドラインを実施し、	21条（従業者の監督） 22条（委託先の監督） （※2）
（略） v. 問合せ及びインシデントへの対応計画を含め、	35条（個人情報取扱事業者による苦情の処理） （※2）
16. データ管理者は、管理下にある個人データに対して、当該データの所在に関係なく責任を有し続ける。 17. 加盟国は、自国と他の国との間における個人データの国際流通について、ガイドラインに一致する継続的な保護のレベルを保つために、(a) 他の国がガイドラインを実質的に遵守している場合、又は (b) 効果的な執行メカニズム及びデータ管理者により導入される適切な措置を含め、十分な保護措置がある場合、この流通を制限することを控えるべきである。 18. 個人データの国際流通に対するいかなる制限も、顕在するリスクに比例した制限でなければならず、データのセンシティビティ並びに処理の目的及び情況を考慮すべきである。	24条（外国にある第三者への提供の制限）

※1　仮訳は、堀部政男、新保史生、野村至、JIPDEC「OECDプライバシーガイドライン　30年の進化と未来」から引用。

※2プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告改正の補足説明覚書（抜粋）（仮訳）
第15項（a）（i）は、データ管理者が「管理下にあるすべての個人データ」に対して、自らの管理下にあるプライバシーマネジメントプログラムを通じてガイドラインを実施すべきであると定めている。・・・適切な保護措置には、データ管理者のプライバシーポリシーと実施手続きを遵守するために定める契約条項、セキュリティ侵害が発生した場合にデータ管理者に通知する手順、従業員の研修及び教育、委託に関する規定、監査を実施するためのプロセスを含めることができる。
第15項(a)(v)は、プライバシーマネジメントプログラムには、インシデントや問合せに対する対応計画も含めるべきであると規定している。・・・第2部の「個人参加の原則」を支援するために、データ管理者は、データ主体からの問合せ（苦情または情報要求のどちらか）に適切な期間で回答できるようにすべきである。・・・（略）

参考2. APECプライバシーフレームワークと改正個人情報保護法との対比表

APECプライバシーフレームワーク（抜粋）（仮訳）	改正個人情報保護法
15. 個人情報のコントローラーは、個人情報に関する慣行及び方針について、明確で容易にアクセスできるステートメントを提示しなければならず、その中には以下を含まなければならない。 a) 個人情報が収集されているという事実 b) 個人情報を収集する目的 c) 個人情報が開示される先となるかもしれない本人又は組織の種類 d) 個人情報のコントローラーの慣行及び個人情報の取り扱いについて連絡する方法に関する情報を含む、個人情報のコントローラーの身元及び所在地。 e) 個人情報の利用及び開示の制限、又はアクセス及び修正のために個人情報のコントローラーが本人に提供する選択肢及び手段。	15条（利用目的の特定） 27条（保有個人データに関する事項の公表等）
16. 個人情報の収集前又は収集時にそのような通知をすることを確保するため、合理的に実行できるすべての措置を採らなければならない。そうでなければ、そのような通知は、実行が可能になり次第ただちに行われなければならない。	18条（取得に際しての利用目的の通知等）
18. 個人情報の収集は収集目的に関連した情報に限定されなければならず、また、そのような情報は合法的で公正な手段により、適切な場合には、本人への通知又は本人の同意により取得されなければならない。	16条（利用目的による制限） 17条（適正な取得）
19. 以下の場合を除き、個人情報は、収集の目的及びその他相当の又は関連する目的を遂行するためにのみ使用されなければならない。 a) 収集される個人情報の本人の同意を得ている場合 b) 個人によって要請されるサービス又は製品を提供するために必要とされる場合 c) 法律その他の法的手段、法的効力を有する宣言又は表明に基づいた権限がある場合	16条（利用目的による制限）
20. 適切な場合には、個人には、個人データの収集、利用及び開示に関連した選択を行使するための、明確で、顕著で、容易に理解でき、アクセスが可能で手頃な価格のメカニズムが提供されなければならない。なお、個人情報のコントローラーが、公に入手できる情報を収集する際にこれらのメカニズムを提供するのは、適切ではないかもしれない。	32条（開示等の請求等に応じる手続き）
21. 個人情報は、利用目的として必要な範囲内で正確かつ完全で、最新のものに保たれるべきである。	19条（データ内容の正確性の確保等）

APECプライバシーフレームワーク（抜粋）（仮訳）	改正個人情報保護法
22. 個人情報のコントローラーは、個人情報の紛失、不正アクセス、情報の不正な破壊、利用、改変又は公開その他の悪用などのリスクに対して、適切な保護措置によって保有する個人情報を保護するべきである。このような保護措置は、被害の発生する可能性とその程度、情報の機密性及び情報が保有されている状況に見合うべきであり、定期的な再検討と再評価を受けるべきである。 【同条解説】 この原則は、自分の情報を他に委託する個人にも、自分の情報が合理的な安全保護措置によって保護されるよう期待する権利があることを認める。	20条（安全管理措置） 22条（委託先の監督）
23. 個人には、以下ができるようにしなければならない。 a) 個人情報のコントローラーが当該個人についての情報を保有するかどうかの確認を得ること b) 本人の身元について十分な証明を提供した後で、以下の条件の下で、当該人に関するデータを本人に伝えること i. 合理的な期間内に ii. 有料とするのであれば、過度にならない費用で iii. 合理的な方法で iv. 一般的に理解できる形で c) 本人に関連する情報の正確性について異議を申し立て、可能でかつ適切な場合には、その情報を訂正、完成、変更、削除すること。	27条（保有個人データに関する事項の公表等） 28条（開示） 29条（訂正等） 30条（利用停止等） 32条（開示等の請求等に応じる手続き） 33条（手数料）
24. 以下の場合を除き、アクセスと修正のための機会が提供されるべきである。 (i) そのための負担又は費用とプライバシーのリスクとが不合理又は不均衡である場合 (ii) 法律上若しくは安全保障上の理由によって、又は、商業のための機密情報を保護するために情報を開示すべきではない場合 (iii) その個人以外の個人のプライバシーが侵害され得る場合	28条（開示） 29条（訂正等） 30条（利用停止等）
25. （23）（a）若しくは（b）に基づく要求又は（c）に基づく異議申し立てが拒否された場合、個人は、そのような拒否の理由の提示を受け、拒否に対して異議申し立てできるようにしなければならない。	31条（理由の説明）
26. 個人情報のコントローラーは、上記の諸原則を実施するための措置を遵守する責任を有する。 個人情報が他の個人又は組織に移転される際には、国内、国外を問わず、個人情報のコントローラーは、移転先の個人若しくは組織が、これらの原則に従って情報を保護することを確保するため、個人の同意を得るか、又は、デューディリジェンスを実施して、合理的な措置を取るべきである。	23条（第三者提供の制限） 24条（外国にある第三者への提供の制限）