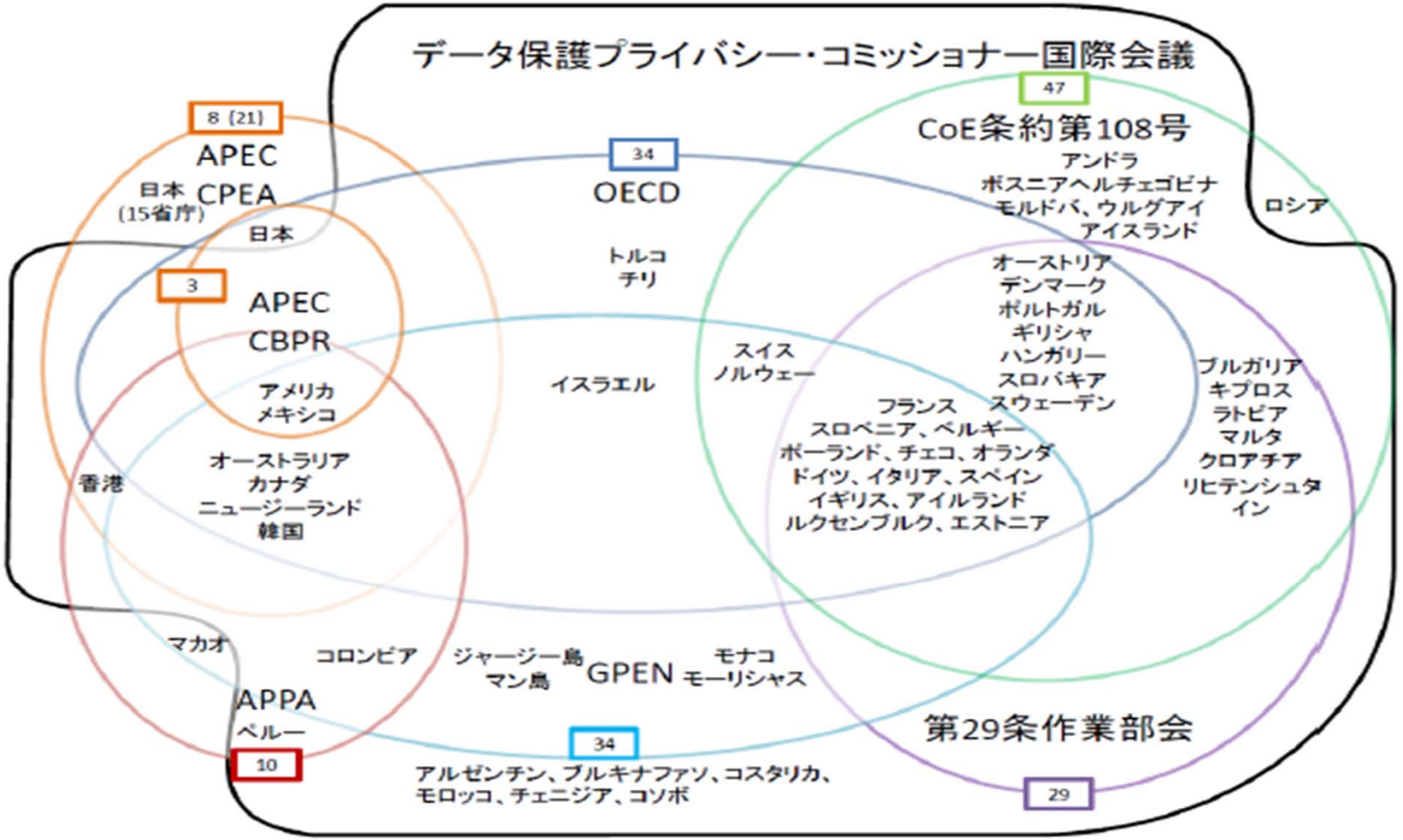
参考

EU第29条作業部会における協力連携をはじめ、国際的な連携枠組みについては、以下の図のとおり。
（PHAEDRA（欧州委員会の支援による執行協力促進のプロジェクト）報告書に基づき作成されたもの）



出典：「個人情報保護における国際的枠組みの改正動向調査報告書」消費者庁（平成26年3月28日）

未定稿

個人データの自動処理に関する個人の保護のための条約（ヨーロッパ条約第１０８号）
（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data）

○第 108 号条約について

・1980 年、CoE（＊）は第 108 号条約を採択。条約批准国はデータ保護の各規定について国内法に導入することが義務づけられている分。

（＊）欧州評議会（CoE）は EU の 28 加盟国、旧ユーゴスラビア諸国、ロシア、ウクライナ、トルコ等を含む 47 か国で構成。日本は 1996 年にオブザーバーとなる。

・EU の 28 加盟国を含む 46 の加盟国が批准（トルコ除く）。非加盟国も批准可能（非加盟国としては、2012 年ウルグアイが初めて批准）。（2014 年 4 月現在）

○追加議定書について

・ 2001 年「監督機関及び越境データ移転について個人データの自動処理に関する個人保護のための条約の追加議定書」（Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows）採択、2004 年発効。ウルグアイ含む 35 か国が批准又は加入。（2014 年 4 月現在）

○108 号条約改正案（現代化案）について

・OECD プライバシーガイドライン同様、採択後 30 年を迎えて見直し議論が進められている。

・条約改正作業のためのデータ保護特別委員会最終会合を 2014 年 12 月予定。

【監督機関について】

○現行第 108 号条約には監督機関について規定なし。

○追加議定書において定義。（2014 年現在、108 号条約批准国 47 ヵ国。うち、追加議定書の批准又は加入国は 35 ヵ国）

・原則を実施する国内法の措置の遵守を保障することについて義務を負う一つ又はそれ以上の機関（one or more authorities）

・完全なる独立性をもって（in complete independence）自らの権限を執行

○108 号条約改正案において監督機関に関する条項の追加。

未定稿

108 号条約改正案（現代化案）

THE CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA [ETS No. 108]

12 条の 2　監督機関

Article 12bis Supervisory authorities

１．各締約国は、本条役の諸原則を発効させる国内法の措置の遵守確保に責任を負う一又は複数の機関を設けるものとする。

1 Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles of this Convention.

２．この目的のため、機関は

2 To this end, such authorities:

a. 調査及び介入の権限を持つものとする。

a’.個人データの取扱いをめぐる個人の保護に関連した立法及び行政上の措置を策定する際に、協議を受ける。

b. 第 12 条に基づき認められたデータ移転に関連した職務、特に標準的な安全保護措置の認可を行うものとする

c. 本条約の規定を発効させる国内法についての決定を公布する権限を持つものとし、特に行政上の違反行為を処罰することができる。

d. 本条役の規定を発効させる国内法の規定への違反につき、法的手続を起こす、又は、所管する司法当局の注意を促す権限を持つものとする。

e. データ保護の認知度を高め、情報を提供する責任を持つものとする。

a. shall have powers of investigation and intervention;

a’. are consulted when drawing up legislative and administrative measures relating to the protection of individuals with regard to the processing of personal data;

b. shall perform the functions relating to transfers of data provided for under Article 12, notably the approval of standardised safeguards;

c. shall have the power to issue decisions with respect to domestic law giving effect to the provisions of this Convention and may in particular sanction administrative offences;

d. shall have the power to engage in legal proceedings or to bring to the attention of the

competent judicial authorities violations of provisions of domestic law giving effect to the provisions of this Convention;

e. shall be responsible for raising awareness of and providing information on data protection;

３．各監督機関は、何人からも、その権限のもとにあるデータの取扱いについてのその者の権利及び基本的自由の保護に関する申立を調査するように請求される可能性があり、係る申立を受けて下された処分をデータ主体に伝えるものとする。

3 Each supervisory authority can be requested by any person to investigate a claim concerning the protection of his/her rights and fundamental freedoms with regard to the data processing within its competence and shall inform the data subject of the follow-up given to such a claim.

４．監督機関は、完全に独立してその職務を遂行し権限を行使するものとする。職務の遂行及び権限の行使にあたって、誰からの指示を仰ぐことも受けることもない。

4 The supervisory authorities shall perform their duties and exercise their powers in complete independence. They shall neither seek nor accept instructions from anyone in the performance of their duties and exercise of their powers.

５．各締約国は、監督機関が十分な人的、技術的及び資金的なリソース、並びに独立して効果的に職務を遂行し、権限を行使するのに必要なインフラを得る要に、確実を期すものとする。

5 Each Party shall ensure that the supervisory authorities have adequate human, technical and financial resources and infrastructure necessary to perform their functions and exercise their powers independently and effectively.

５の２．監督機関は、公開の活動報告書を作成し、活動の透明性が確保されるように取り計らうものとする。

5bis The supervisory authorities shall draw up a public report of their activities and shall see to it that transparency on their activities be ensured.

５の３．監督機関の構成員及び職員は、職務遂行時にアクセスする又はアクセスした機密情報に関して、守秘義務に拘束されるものとする。

5ter. Members and staff of the supervisory authorities shall be bound by obligations of confidentiality with regard to confidential information they have access to or have had access to in the performance of their duties.

６．監督機関の決定に異議があるときは、裁判所を通じて上訴することができる。

6 Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

７．第４章の規定に従い、監督機関は、職務遂行に必要な範囲で互いに協力するものとし、特に以下を通じて行う。

7 In accordance with the provisions of Chapter IV, the supervisory authorities shall co-operate with one another to the extent necessary for the performance of their duties, in particular by:

a. あらゆる有用な情報の交換－特に国内法に基づき、また、個人データ保護だけを目的として、領域内で行われた具体的な取扱いに関する事実情報を提供するためのあらゆる適切な措置を取ることによる。この取扱いの対象となった個人データは対象外であるが、当該データが協力に不可欠であり、又は、データ主体が既に、明確で、具体的な、自由かつ情報を踏まえた形で同意しているときは、この限りではない。

b. 調査若しくは介入の連携、又は合同作戦の実施。

c. データ保護に関する法律及び行政面の実務の情報提供。

a. exchanging all useful information, in particular by taking, under their domestic law and solely for the protection of personal data, all appropriate measures to provide factual information relating to specific processing carried out on its territory, with the exception of personal data undergoing this processing, unless such data is essential for co-operation or that the data subject has previously agreed to in an unambiguous, specific, free and informed manner;

b. coordinating their investigations or interventions or conducting joint actions;

c. providing information on their law and administrative practice relating to data protection.

８．前項に示した協力を組織し、職務を遂行するため、締約国の監督機関は会議／ネットワークを創設する。

8 In order to organise their co-operation and to perform the duties set out in the preceding paragraph, the supervisory authorities of the Parties shall form a conference/network.

９．監督機関は、司法上の権限に基づき行動する主体が行う取扱いに関して、権限を持たないものとする。

9 The supervisory authorities shall not be competent with respect to processing carried out by entities acting in their judicial capacity.

未定稿

APEC プライバシーフレームワーク（APEC PRIVACY FRAMEWORK）

○APEC プライバシーフレームワークについて

・2004 年、「APEC プライバシーフレームワーク」閣僚会議承認。アジア太平洋地域にわたる電子商取引の推進を目的とするとともに、OECD プライバシーガイドラインに準拠したプライバシー保護原則を規定。

○「越境プライバシー執行協定（CPEA）」について

・2009 年「越境プライバシー執行協定」（Cross-Border Privacy Enforcement Arrangement）閣僚会議承認、2010 年開始。APEC 域内各国のプライバシー執行機関が参加できることとされている（各国ごとに複数機関の参加可能）。日本は 15 省庁（基本法の主務大臣）が参加（消費者庁が窓口）。ほかに、オーストラリア、ニュージーランド、米国（FTC）、香港、カナダ、韓国、メキシコ、シンガポールの各機関が参加。

・プライバシー執行機関の間での情報共有及び執行協力を促進するための協定。

○「越境プライバシールール（CBPR）」について

・2011 年「越境プライバシールール」（Cross Border Privacy Rules）を承認、2012 年公表。米国が最初に参加、次いでメキシコ、日本参加。（日本参加承認：2014 年 4 月 28 日）

・企業等が APEC プライバシーフレームワークの諸原則に適合しているか否かを認証する仕組み（APEC が承認した責任団体により認証された企業等は、エコノミー内での越境データ流通を行うことができる。）。

・CBPR 参加条件は、①国内の執行機関が CPEA に参加していること、②CBPR に参加表明通知を提出すること、③APEC が承認した認証機関（Accountability Agent,AA）を少なくとも一つ利用すること、の３点。

【執行機関について】

○APEC プライバシーフレームワークにおいて定義。

・執行機関は、プライバシー法の執行に責任を負い、調査を実施し又は執行手続を行うための権限を有するあらゆる公的機関をいう。

○CBPR において以下の規定。

・執行機関は、CBPR の苦情、問題について、参加組織又は認証機関により解決できない場合に、その苦情、問題を精査し、適切な場合には、調査及び執行活動を行うことができなければならない。

・他のプライバシー執行機関による援助要請に対応するか否かを決定する裁量を有する。

未定稿

プライバシーコミッショナー会議
（International Conference of Date Protection and Privacy Commissioneres）

○プライバシーコミッショナー会議について

・1979 年以降、毎年 1 回開催。各国、地域のデータ保護機関から構成されるデータ保護及びプライバシーに関する国際会議。（2014 年 10 月 13 日～16 日、第 37 回会議開催。）

・データ保護機関、政府機関関係者、学者、民間の専門家等が出席。

・登録出席者の出席が認められる公開セッションと、認可を受けたデータ保護機関の関係者のみの出席が認められる非公開セッションがあり、日本は公開セッションへの参加とともにオブザーバ（消費者庁、特定個人情報保護委員会）として非公開セッションに参加。

○会議参加要件

・「資格に関する委員会の基準及び規則並びに認定の原則」（Criteria and Rules for Credentials Committee and the Accreditation Principles.2002）（2001 年採択、2002 改定）に基づき、正式なメンバー又はオブザーバとしての参加に分けられる。

・要件は次のとおり。

a 所属する国家ないし国際機関の法的慣習に基づき, 適切な法的根拠のもと設置された公的機関であること。

b 主たる規制権限の一つとして, 個人データやプライバシーの保護に関する法律の施行について監督権限を有すること。

c 所掌事務を定めている法律が, データ保護やプライバシーに関する国際的な枠組みに準拠していること。

d 機能を果たすべく，適切な範囲の法的権限を有していること。

e 適切な自主性と独立性を有していること。

未定稿

特に科学技術の発展に照らしたプライバシーの新たな課題に対する異なるアプローチに関する比較研究　カントリースタディ　B5 日本
（COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS, COUNTRY STUDIES, B5 JAPAN）

要約において、以下のように指摘（文脈から考えて、民間分野のプライバシー保護（基本法の規定）を念頭にした指摘と考えられる（特に公的分野に関する規定はない））。

日本の法律はまだ４年間しか執行されておらず、暫定的な評価は困難である。さらに、日本では、訴訟ではなくインフォーマルな紛争解決に関する法制度に依拠している。省庁が収集した資料、コンプライアンス、データ違反、救済に関する公表資料から、日本の法律が効果的であることの証拠がないと判断することは合理的であろう。
（国際基準から見た日本の位置づけについて）日本のデータ保護制度はOECDガイドラインの基準を満たしている。また、APEC プライバシー・フレームワークの基準を満たしていることも疑いはない。EU 指令との関係になるとこのレポートの範囲を超えるもので、難しい判断となる」

III. Summary and conclusions

Overall

There is a divergence of opinion concerning the effectiveness of the enforcement of the PPI Act. Ponazecki et al (2007) concede that 'there have not been significant administrative fines or penalties or court judgments arising from failures to comply with the Law and the related guidelines'. According to other Japanese practitioners, there have been many instances where a Ministry warned or ordered a company to fix the problem that led to an improper transfer to a third party (eg METI warnings to companies to take measures to prevent their employees from improperly selling credit history information to third parties). In their view the main risk for a private company that violates the PPI Act is usually the risk of reputational damage rather than the risk of paying large fines or having to defend class action suits. This is consistent with the view of Ito and Parker (2008), noted earlier.

Ito and Parker (2008) are uncertain in which direction enforcement is headed:

> It is less clear for now whether the ministries are likely to take more active steps to enforce compliance with the Act. The deterrent effect is not proven and the ongoing incidents of data leaks and other breaches are proof that more needs to be done by businesses to ensure compliance. It is possible that, as in the EU, the authorities will over time become more aggressive in enforcing the Act. However, although the responsible ministries are actively engaged in ensuring enforcement through a process of consultation within their respective industry sectors, and the Cabinet Office has issued an annual report on the enforcement status of the Act, together the ministries and the Cabinet Office are much less vociferous than their counterparts in the EU, who can be regularly heard speaking out in public against the failings of businesses to take adequate steps to comply. It is also difficult to imagine a business ever facing fines, or the directors the threat of imprisonment, under the Act, except in the case of hopelessly reckless failure, or aggressive refusal, to comply; businesses are much more likely to co-operate with the relevant ministries to ensure that they comply with any order to implement corrective measures.

The Japanese legislation has only been in effect for four years, so anything beyond tentative assessment of its effectiveness is difficult. Assessment difficulties are compounded by the propensity of the Japanese legal system to rely on relatively informal means of dispute resolution, rather than litigation. It can reasonably be said that there is a lack of evidence that the legislation is effective, which could be remedied somewhat by Ministries gathering and publishing more detailed data on compliance, enforcement, breaches and remedies.

Position in relation to international standards

Japan's data protection system may well meet the standards of the OECD Guidelines, and no doubt would meet the standards of the APEC Privacy Framework, given the weaknesses of both documents in relation to enforcement. Comparison with the EU privacy Directive is a more difficult question, beyond the scope of this report. Suffice to say is that it would be an arguable question in relation to privacy principles, and in relation to enforcement one on which more information about practices is needed.

『個人情報保護法の現在と未来 －世界的潮流と日本の将来像－』石井夏生利著（2014 年、勁草書房）抜粋（世界における監督機関の独立性に関する部分）

○序章　プライバシー・個人情報保護の新たな世界的潮流と日本

・日本に目を向けると、個人情報保護法が全面施行された後、いわゆる「過剰反応」が生じる一方で、大規模な情報漏えい事件、住民基本台帳ネットワークシステムの合憲性をめぐる多数の訴訟等、様々な問題が生じてきた。衆議院及び参議院の各個人情報の保護に関する特別委員会は、2003 年 5 月 23 日に個人情報保護法を成立させる際の附帯決議において、「全面施行後 3 年を目途として、本法の施行状況について検討を加え、内閣府の国民生活局第 20 次国民生活審議会個人情報保護部会（部会長・野村豊弘学習院大学教授）では 2005 年 11 月 30 日から 2007 年 6 月 11 日にかけて、施行状況の評価及び個人情報保護制度の見直しに向けた検討を行った。しかし、2007 年 6 月 29 日の「個人情報保護に関する取りまとめ（意見）」では、現行法の枠組みの下での運用改善が必要であるとして法改正には踏み込まず、独立監視機関設置についても中長期的課題として位置付けられるにとどまった。独立監視機関の存在は、特に欧州を中心とする個人情報保護法制の先進国にとっては必須の条件とされており、かかる機関を持たない日本は、長年にわたり、国際的に立ち後れていることが最大の課題となってきた。（P.5）

○第 2 章　EU 一般データ保護規則提案

・データ保護指令には、独立監視機関の必要性は明文化されていない。しかし、WP12※によると、欧州では、データ保護諸原則を立法化するとともに、独立機関の形態を有する「外部監視」制度を有することが、データ保護遵守制度に関する必要な機能である旨の広範な合意が存在するとのことである。（P.89）

※「第三国への個人データの移転：EU データ保護指令に関する第 25 条及び第 26 条の適用」という作業文書

・監督機関の独立性は、十分な保護レベルを達成するための考慮要素として明文化されており、規則提案第 6 章に詳細な規定が設けられている。日本でも、プライバシー・コミッショナー設置に向けた検討が進められていることから、欧州が監督機関に関していかなる条件を課しているかを見ることは、重要な意義を有する。（P.99）

○第 3 章　欧州評議会第 108 号条約の見直しについて

・第 1 条について、監督機関とは、本条約の第 2 章及び第 3 章並びに本議定書

に規定された諸原則を実施する国内法上の措置に関して、その遵守を確実にすることに責任を負う機関をいう（1 項）。監督機関は、調査権限、仲裁権限及び法的手続を起こす権限、又は、国内法の規定の違反に対して管轄権を有する司法機関の注意を喚起する権限を有する（2 項 a 号）。また、個人データの処理に関する苦情を受ける権限も有する（b 号）。監督機関は、完全に独立してその職務を執行するものとされ（3 項）、監督機関の決定に不服がある場合は、裁判所を通じて上訴することができる（4 項）。

第 2 条は、本条約の締約国ではない国又は機構の管轄に服する受領者への個人データの移転を行うのは、当該国又は機構が、意図したデータの移転に対して「十分なレベルの保護」（adequate level protection）を確保している場合に限ると定めている。適用除外される場合は、国内法が、「データ主体の特定の利益」、若しくは「適法な一般的利益、特に重要な公の利益」を理由としたデータ移転を定めている場合（a 項）、又は、移転に責任を有する管理者が、特に契約条項の結果として生じた安全保護措置を提供し、かつ、国内法に従って権限を有する機関がその保護措置を十分であると認定した場合とされている（b 項）。

独立した監督機関及び「十分なレベルの保護」基準に関する規程は、EU の 1995 年データ保護指令で取り入れられたものであるが、CoE も、これに足並みをそろえるべく、第 108 号条約に盛り込んだ。これによって、両者の制度は、欧州の個人情報保護法の中では、重要かつ基本的な地位を確立することとなった。なお、第 2 条第 b 項は、データ保護指令の認める標準契約条項に類するものであるといえる。（P.177）

○終章　個人情報保護法の将来像

・日本の個人情報保護法は、国際的に見ると、大幅な遅れを取って制定された上に緩やかな内容であり、国内的に見ると、事業者が適切に解釈・運用できないという課題を抱えてきた。最大の問題は、法を運用・執行する独立監視機関が存在しなかったことにあるが、2014 年 1 月 1 日に特定個人情報保護委員会が発足し、かつ、近い将来、個人情報の取扱全般を監督する独立監視機関を設ける動きが現実のものとなってきている。（P.452）

・独立性の程度との関連では、欧州司法裁判所において、ドイツ及びオーストリアの監督機関が「完全な独立性」を満たさないという判決を下したことも注目される。それぞれの判決は、独立性の程度について、職権行使の独立性では不十分であり、他の機関からのあらゆる直接的・間接的影響から自由であること

を求めている。規則提案の定める独立監視機関の章や欧州司法裁判所の判決は、加盟国の監督機関に適用される「同等性」の基準であり、第三国に適用される「十分性」の基準とは異なるが、日本が独立監視機関を設ける際には参考にできると考えられる。十分性との関係では、第 29 条作業部会「第三国への個人データの移転 : EU データ保護指令に関する第 25 条及び第 26 条の適用」によると、「諸原則の善良なレベルの遵守を提供すること（いかなる制度も 100%の遵守は保証できないが、いくつかの制度は他よりも優良である。）」と記載されている。

EU とは異なり、OECD プライバシー・ガイドラインや APEC の CPEA では、監督機関の独立性を求めてはいない。しかし、第三国に規律を及ぼし得る欧州ルールに対応するためには、独立監視機関の存在が必須の要件ということになる。これについて、米国の FTC は、消費者プライバシー保護の観点から独立した立場で監督権限を行使し、欧州を中心とするデータ保護・プライバシー・コミッショナー国際会議でも存在感を見せている。シンガポールは個人データ保護委員会、韓国は個人情報保護委員会、香港はプライバシー・コミッショナーをそれぞれ設けている点を見ても、既に日本はアジア諸国の中でも出遅れてきた。そのような中、今回の個人情報保護法制の見直しで、「第三者機関（プライバシー・コミッショナーの体制整備）」が設けられることとなり、日本も、ようやく国際的に保護レベルの足並みを揃える一歩を踏み出すことが期待される。（P.461）

・第三国にとっては、十分性の決定を受けられず、越境データ流通を違法と評価されることは脅威であり、そう思わせることが EU のプライバシー外交戦略と見ることもできる。とはいえ、個人情報保護法の分野で国際的に大幅な遅れを取ってきた日本としては、越境データ流通を円滑に行うために、十分性を満たすことが理想ではある。そのためには、独立監視機関を含めた国際水準に沿った個人情報保護法制を構築することが望ましいが、あわせてプライバシー外交の交渉力を備える必要もある。その際に問題となり得るのは、日本の国内的事情はさほど考慮されないであろうという点である。日本は、個人情報保護法の全面施行直後に過剰反応という特異現象を発生させ、また、罰則等による強制力を伴わないガイドラインであっても、真摯な事業者は過度なまでに遵守するという、いわば奇異な側面を持つ国である。しかし、十分性決定の場面では、日本は、EU の尺度で評価を受けることとなるため、これまでの国内的取組にはそぐわない要求をされる可能性もある。この点は、独立監視機関設置後の課題として捉えておく必要がある。（P.463）

・最も手厚い保護措置を定めるEUの規則提案を国際水準と捉え、そのレベルに合わせることを目指した場合には、個人情報保護法制を牽引してきた欧州には受け入れられやすい制度設計となるかもしれないが、遵法意識の高い国内事業者には過剰な負担となる可能性がある。法の運用に際して、新たに設置される独立監視機関に過度な期待をかかえると、失敗を招く原因となりかねない。制度改正大綱が、第三者機関に対して多くの役割を求めている点は、懸念せざるを得ない。（P.479）

・本書で取り上げた国際動向については、次のように、共通して採用されている制度がある。国際水準を目指す場合には、最低限、以下の制度を導入することが求められる。

第1は、個人データの取扱いを監督する独立監視機関の設置である。OECD改正プライバシー・ガイドラインは、「プライバシー監督機関」の定めを設け、APECのCBPRもプライバシー執行機関の存在を前提としている。EUでは、1995年データ保護指令の時代から、加盟国はもちろんのこと、越境データ流通を行う際に、第三国に独立監視機関の設置を求めてきた。規則提案では、十分な保護レベルを達成するための考慮要素に独立監督機関が明文化された。CoE第108号条約の現代化案でも、監督機関の章が新たに設けられ、その独立性が謳われている。OECDやAPECは監督機関の独立性を求めないが、欧州ルールを採用しない米国でも、FTCは独立機関であり、アジアでも独立監視機関が設けられるようになってきている。このことからすれば、監督機関の独立性は必須といえる。今回の個人情報保護法改正によって、独立監視機関が設けられることとなったため、国際水準に合わせるために最初に求められる基準は満たすこととなる。（P.480）

・最後に、行政機関個人情報保護法、独立行政法人等個人情報保護法の改正にも触れておきたい。本書で触れた国際動向のうち、OECDのプライバシー・ガイドライン、EUの規則提案、CoEの第108号条約は、公的部門・民間部門を問わない議論である。米国でも、ビッグデータに関する報告書は、1974年プライバシー法の改正を勧告している。しかし、今回の法改正で個人情報保護法のみを改正した場合は、独立監視機関は、共通番号法の規律に服する機関と、個人情報保護法の規律に服する民間事業者を監督対象とせざるを得ず、権限の及び範囲が制限されてしまう。こうしたことから、独立監視機関の設置を含む個人情報保護法改正を行うためには、行政機関個人情報保護法や独立行政法人等個人情報保護法の改正にも取り組むことが必要である。（P.483）