アジア太平洋地域等における個人情報保護制度の実態調査

に関する検討委員会・報告書

平成 25 年 3 月

はじめに

委員長　中央大学法科大学院教授　藤原靜雄

我が国を含めて、各国の個人情報保護法制の枠組みは、技術の進展を後追いしつつ、また経済の要請とのバランスを図りつつ形成されてきたと言ってよい。例えば、現下の課題は、ビッグデータ、忘れられる権利という言葉に象徴される技術の進展への対応と、グローバル化あるいは規制緩和という言葉に象徴される経済の要請との調整である。

このうち、経済の要請の側面からみると、個人情報保護の法制度は、我が国ではこれまで、EU とアメリカの関係、日本と EU・アメリカとの関係を軸に語られてきた。しかしながら、経済のグローバル化が進み、先進各国の人、物、情報の移動が日米欧の枠組みのみでは語れなくなってきた上、我が国について見れば、近時の事業者の事業展開が、ASEAN（Association of South-East Asian Nations）あるいは我が国も加盟エコノミーである APEC(Asia-Pacific Economic Cooperation)を抜きに語ることができないのは周知のところであろう。とりわけ、アメリカ、カナダ、オーストラリアと言った国々も構成エコノミーである APEC における個人情報保護の枠組みは、我が国にとっては重大な関心事である。実際、APEC では、2004 年（平成 16 年）10 月 29 日に『APEC プライバシーフレームワーク』(1980 年の OECD の個人情報保護に係る理事会勧告とほぼ同等の内容である。）を採択し、じらい 10 年近く、ゆっくりとではあるが確実に EU 諸国とは異なった個人情報保護制度の枠組みを構築しようとしている（例えば、2007 年の『越境プライバシールール』に基づいた認定マーク制度（トラストマーク）を推進するためのパスファインダー計画)。さらに、近時では、欧州委員会のいわゆる第 29 条作業部会も APEC の枠組み作りに関心を寄せているという事実もある。

これまでも、我が国においては将来の立法等に活かすべく、積極的に諸外国の個人情報保護法制の研究がなされてきた。しかしながら、個別の APEC 構成エコノミーの個人情報保護法制の実際については、情報の蓄積は十分であるとは言い難い状況にあると思われる。そこで、本委員会においては、APEC-CPEA（越境プライバシー執行のための協力取決め：我が国は 2011 年（平成 23 年）11 月に個人情報保護関係 15 省庁で加盟）及び APEC-CBPR（越境プライバシールール制度：CBPR は米及びメキシコが加盟、CBPR と EU の BCR（拘束的企業準則）との相互運用も課題）等 APEC の動向の重要性、及びアジア太平洋地域等における活発な新法制定・法改正の動きを踏まえて、APEC とシンガポール、フィリピン、香港、マカオ、メキシコ、コスタリカの諸国について、上記のような問題意識に基づき、実地調査及び文献調査を行った。本報告書はその調査の成果を取りまとめたものである。

本調査に際して御助力を得た APEC 事務局及び各国の個人情報保護当局関係者、APEC の歴史等について御助言いただいた山澤逸平名誉教授、制約のある期間内に現地

調査を行っていただいた各委員、資料の収集等の委員会の運営を支えてくださった消費者庁事務局の川﨑美奈弁護士、佐小千恵美氏に心より御礼申し上げる。

アジア太平洋地域等における個人情報保護制度の実態調査検討委員会
委員名簿・執筆分担

○藤原靜雄　中央大学教授
はじめに・あとがき執筆、全体につき査読

山澤逸平　一橋大学名誉教授
APEC と個人情報保護活動につき執筆

加藤隆之　亜細亜大学教授
個人情報保護に関する APEC の取組・シンガポール・フィリピンにつき執筆

宮下紘　駿河台大学准教授・ハーバード大学ロースクール客員研究員
メキシコ・コスタリカにつき執筆

千原通和　GBDe, 日本電気株式会社
香港・マカオにつき執筆

（○は委員長）

(オブザーバ)
板倉陽一郎　ひかり総合法律事務所　弁護士

海外現地調査　訪問先

- APEC 事務局

- シンガポール

  Personal Data Protection Commission

- フィリピン

  University of the Philippines

  Office of Policy Research / E-Commerce Office, Department of Trade and Industry

- 香港

  Office of the Privacy Commissioner for Personal Data

- マカオ

  Office for Personal Data Protection

- メキシコ

  Instituto Federal de Acceso a la Información y Protección de Datos

- コスタリカ

  Jefa Depto de Asesoria Juridica Registro Nacional de Costa Rica

  Asamblea Legislativa

  Corte Suprema de Justicia de Costa Rica

目次

概要

I. APECと個人情報保護活動

i. APECの組織と行動様式

APEC は 1989 年に経済協力を話し合う外務・貿易大臣会合として、日、米、豪、加、ニュージーランド、ASEAN 6 か国及び韓国の 12 か国により発足し、1998 年には 21 エコノミー（APEC では参加国をこう呼ぶ。）が参加する地域組織となった。

APEC においては、各エコノミーは協定に拘束されることなく、自発的に自由化を実施する。この非拘束原則、自発的自由化、開かれた地域主義（open regionalism）が APEC 独自の自由化方式である。EU においては単一市場における人、モノ、サービス、資本の４つの域内移動の自由で成り立っており、それらを阻害する要因を除去することが EU を設立する条約で定められている。これに対し APEC では、個別行動計画を中核とする IAP（Individual Action Plan）方式は「協調的自発的自由化（CUL)」を採っている。この仕組みでは個々の参加国は自由化プログラムを自発的に発表、自国のやり方で実施するが、相互に計画と実施状況を観察する「ピア・プレシャー」によって、全ての参加国が自由化努力を続けるように仕向けている。APEC は経済技術協力や構造改革等の多彩な協力活動にも取り組んでおり、個人情報保護の普及もその一環として推進されている。

ii. 個人情報保護活動

米国では、「個人のプライバシーを侵害されない」ことを権利として認めようという主張が 19 世紀末から現れており、1974 年米国連邦議会においてプライバシー法が成立した。

OECD は 1978 年、国境を越えるデータの流れや個人データとプライバシー保護を規律する基本原則を定めた OECD ガイドライン案を策定、OECD 理事会は 1980 年にこれを採択し、加盟国へ勧告している。これはプライバシー保護の国際水準を示したもので、収集制限、データ内容、目的明確化、利用制限、安全保護、公開、個人参加、責任の８原則を掲げている。

欧州では 1970 年代に各国でデータ保護や情報処理に関する法律が制定され、1995 年に個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護を規定した EU データ保護指令（EU Data Protection Directive）を採択した。

APEC において個人情報保護が取り上げられたのは、ビジネス界からの働きかけが大きいと思われる。1995 年には APEC のワーク・プログラムの各分野にわたってレビューを行い、ビジネスの優先事項を指摘する APEC ビジネス諮問委員会（ABAC）が拡大再編された。ABAC ではクロスボーダーなデータフローの円滑化等、電子商取引におけるデータフローに関する様々な提言が成されている。

iii. APECでの電子商取引、個人情報保護への取組

APEC での電子商取引、個人情報保護への取組は、1998 年の APEC Blueprint for Action on e-Commerce に始まる。その後 1999 年に E-Commerce Steering Group(ECSG)を貿易投資委員会内に設立、2004 年 10 月には APEC 閣僚宣言において、APEC Privacy Framework が承認された。2007 年に APEC Data Privacy Pathfinder を採択、2009 年には CPEA（APEC Cross-Border Privacy Enforcement Agreement）が、2011 年 APEC Cross Border Privacy Rules (CBPR) System が承認されている。

II. 個人情報保護に関するAPECの取組

i. APECにおける個人情報保護の位置付け

APEC においては、分野ごとにグループに分かれて問題を検討、解決する形式を採っているが、個人情報保護の分野に関しては、電子商取引運営グループ（Electric Commerce Steering Group (ECSG)）を中心として議論されている。なお、ECSG は分野別にデータ・プライバシー・サブグループ（Data Privacy Subgroup）及びペーパーレス・トレイディング・サブグループ（Paperless Trading Subgroup）という２つの下部組織を有しており、このうち、個人情報保護を直接的に扱っているのは、データ・プライバシー・サブグループである。

ii. 個人情報保護に関するAPECの取組

APEC における個人情報保護への取組は、1998 年 11 月の「電子商取引に関する行動のための青写真（Blue print for Action on Electronic Commerce）」に遡る。その後 2004 年 10 月に APEC プライバシー・フレームワーク（APEC Privacy Framework）が承認され、2007 年 9 月に越境的データ流通に関する APEC データ・プライバシー・パスファインダー（APEC Data Privacy Pathfinder）計画を策定した。

2009 年 11 月には、パスファインダー計画の目的は、越境プライバシー・ルール(CBPR)の確立とその実施によって達成されるとし、APEC 越境プライバシー執行協定（APEC CPEA)が承認された。CPEA の策定は、パスファインダー計画における非常に大きな成果であると言える。この目的は、APEC エコノミーのプライバシー執行機関における情報共有を促進すること、プライバシー法の執行において執行機関間の効果的な越境的協力を促進するメカニズムを提供すること、APEC 域外のプライバシー執行機関とプライバシーに関する調査や執行のための情報共有及び協力を推進することである。

iii. APECの取組に対する各国の関与の程度

ECSG のウェブサイトでは各国から提出されたペーパーによって、APEC のプライバシー・フレームワークに対する取組状況を確認することができる。14 か国（オーストラリア、カナダ、香港、日本、韓国、マレーシア、メキシコ、ニュージーランド、ペルー、フィリピン、シンガポール、台湾、タイ、アメリカ）が、取組状況に関するペーパーを提出している。

iv. 他の国・地域との関係

2013 年からは APEC と EU の作業チームの会合が開かれている。この会合では、EU の拘束的企業ルール（Binding Corporate Rule）と APEC の CBPR との接合が検討されている。両制度は、個人データの越境移転に関して、EU データ保護執行機関や APEC

に認められたアカウンタビリティ機関による事前承認を受けた企業の内部的拘束ルールを利用するという点で類似したアプローチをとっている。APEC のプログラム・ディレクターによれば、CBPR と EU の BCR との接合について、CBPR 認証を受けた事業者が BCR 認証を受ける際に有利な取扱いを受けられる優遇が認められれば、CBPR 認証の魅力は一気に高まることは間違いないだろうと述べている。

III. アジア太平洋地域等における個人情報保護制度

i. シンガポール

1. 個人情報保護法制

名称は「組織による個人データの収集、利用及び開示を規制すること、個人データ保護委員会及び迷惑電話禁止登録機関（Do Not Call Register）を設立し、その運営やそれに関連する事項についての定めをおくこと、その他の様々な法律に対して関連する必然的な改正を行うことを目的とする法律」。短い名称は、2012 年個人データ保護法である。2012 年 10 月に制定された。民間部門を規制対象としている。

本法制定の成立に当たっては、シンガポールが世界のデータ・ハブとしての役割を担えるように推し進めようとする国家戦略が背景にあるといわれる。同法は段階的に施行されることとなっており、2013 年 1 月に個人データ保護委員会の創設に関する規定がまず施行され、2014 年の初盤には迷惑電話禁止登録制度に関する規定が、同年の中盤には、データ保護に関する規定が施行される予定である。

特徴としては、個人データの保有期間の制限を有すること、個人データ保護法と同等の保護レベルが存在しない国への個人データの移転を禁止した、第三国移転禁止を設けていること、迷惑電話禁止登録制度（第 9 章）が導入されていることが挙げられる。迷惑電話禁止登録制度は、電話加入者はデータ保護委員会に対して、登録機関への電話番号の追加や除去を申し出ることができる（第 40 条第 1 項）こととされている。

情報コミュニケーション省の下部組織に位置する個人データ保護委員会が、監督機関として設立されている。機関の独立性については同国の仕組み上、EU のデータ保護指令に対応するものではない。

2. 国際的なルールへの対応状況

監督機関のディレクターによれば、法案を作成するに当たっては諸外国の立法のいずれかに依拠して草案されたというわけではない。強いて挙げるならば、カナダの個人情報保護法（PIPA）が挙げられるが、香港、オーストラリア、EU など多くの法制度や APEC の議論を参考にしたという。

また、同ディレクターは EU の十分性審査とシンガポールの関係について、現在 EU とのデータ移転との関係で大きな問題が生じているとまでは認識していないため、十分性審査を受ける予定はないと述べている。シンガポールは小国であるし、EU との交渉は、APEC などを通じて、他の国と連携して行うのが良いと考えているという。

ii. フィリピン

1. 個人情報保護法制

名称は「政府及び民間部門の情報及びコミュニケーション装置における個々の個人情報の保護とその目的やその他の目的のための国家プライバシー委員会の創設に関する法律」。短い名称は 2012 年データ・プライバシー法である。2012 年８月に制定された。

データ・プライバシー法は公的部門、民間部門に共通の個人情報保護法として成立したが、まだ施行されていない。制定の動機としてはデータ処理の委託先国として委託元の事業者や国からの要望があったこと、国内のインターネット利用ユーザからの要請があったこと等の側面があった。

特徴として、一般メディアに与えられている保護について定めた共和国法（Republic Act）第 53 条が修正・破棄されるような本法の解釈を禁じる規定が置かれている点、法律違反に対して直罰規定が置かれている点を挙げることができる。また、米国のカリフォルニア州から広まった、漏えい等を当事者に知らせるデータ保護違反通知（data breach notification）制度の存在、政府保有のセンシティヴ個人情報の安全管理に関する特別規定の存在も興味深い。

監督機関は国家プライバシー委員会で、情報コミュニケーション科学技術省に付設されている。同委員会は大統領府の下にあるが、それは名目上のことといって良く、事実上コミッショナーは独立して活動できる。

2. 国際的なルールへの対応状況

プライバシー法の草案に当たっては、条文の文言はイギリスの制度の影響を受けているが、具体的な制度内容については、オーストラリアとアメリカといった国々の影響を大きく受けているという。とすれば、オーストラリアとアメリカは、APEC の加盟エコノミーであるから、フィリピンの制度は、APEC の制度と適合的なものということはできるであろう。

EU の個人データ保護法制との関係について、制定の起草メンバーによれば、EU のように、ひとつの定型的なプライバシー制度を他国に対して求めるよりも、各国の文化的背景を踏まえてそれぞれの国で執行可能なプライバシー法制度が構築されるべきであるという。また、フィリピンだけで EU の十分性審査に関して交渉するよりも、APEC のような組織において多くの国と協力して EU との妥協点を見いだす方が生産的であると考えているという。

iii. 香港

1. 個人情報保護法制

名称は「個人データ（プライバシー）条例」。個人情報に関連して個人のプライバシーを保護することを目的とし、公的部門と民間部門を包括的に規制している。また、1995年7月にEUが採択した「EUデータ保護指令」への対応も意図している。

個人情報保護に対する国民の意識の高まりや、保護法制の整備によって香港への個人データの自由な流入を確保し、ビジネスにおける香港の競争力を確立することを目指して、1996年12月に施行された。この条例は東アジアで初の個人情報保護に関する法律である。その後、情報技術の進展や国際的プライバシー標準の発展に伴い、改正が必要となったため、2012年6月に改正法が制定された。

2012年改正法の主要な点は、ダイレクトマーケティングにおける個人情報使用の管理強化、データ主体の同意なしに獲得された個人情報の営利開示の規制、個人への法務相談サービスの提供、プライバシー・コミッショナーの権限強化である。このうち、個人への法務相談サービスの提供は、データ使用者の条例違反による被害者が補償金の請求をすることと連動したサービスで、違反行為への抑止力とする狙いがあるという。

監督機関である個人データ・プライバシー・コミッショナー事務所（PCPD）は、政府に財政面などで依存しているものの、独立した活動を行っている。

2. 国際的なルールへの対応状況

PCPDはAPEC加盟の主要国が参加するAPEC Cross-Border Privacy Enforcement Arrangement (CPEA)の一員である。APEC 越境プライバシールールシステム（CBPRシステム）への参加は現在検討中である。

OECDプライバシー・ガイドライン改正、欧州評議会第108条約現代化、欧州一般データ保護規則提案については、現在、PCPDは全てに対して動向を注視している。

また、PCPDはプライバシー・コミッショナー国際会議に正式メンバーとして参画しており、Asia Pacific Privacy Authorities (APPA)の中のTechnology WG（TWG）の議長も務めている。

3. 個人情報保護に関する認証制度

認証制度はない。検討していない。

4. 個人情報保護の施行状況

PCPDは条例履行状況の監視・監督を行う他、市民への業務ガイダンスとして、指紋情報収集、CCTV（監視カメラ）による監視等に関するガイダンス・ノートを発行している。

iv. マカオ

1. 個人情報保護法制

名称は「個人データ保護法」。2006 年２月施行。ポルトガル法をベースに、香港法も加味して制定された。公的部門と民間部門を包括的に規制。

本法は EU データ保護指令第 25 条と同様に、外国への個人情報の移転を限定している。この個人情報の海外移転については厳しく規制されており、データ管理者と個人情報の処理をマカオで行う場合でも、サーバが国外に設置されているケースや、海外からその情報にアクセスできる等のケースは、全て個人情報を海外移転したとみなされる。マカオ域外へのデータ移転については、移転先の国・地域がマカオと同等の保護レベルの法制度を有していることを要求され、移転先の保護レベルは監督機関が調査を行い、判断する。

個人データ保護オフィス（OPDP）が監督機関として設置されているが、恒久的な組織としては位置付けられていない。

2. 国際的なルールへの対応状況

APEC-CPEA 及び APEC-CBPR については、APEC 未加盟のため、対応していない。

OECD プライバシー・ガイドライン改正、欧州評議会第 108 条約現代化、欧州一般データ保護規則提案については具体的な動きはないものの、マカオの個人情報保護法はポルトガル法に準拠しており、EU の動向を注視している。

Asia Pacific Privacy Authorities (APPA) フォーラムに 2008 年より参加、2012 年に正式メンバーとなった。また、プライバシー・コミッショナー国際会議に 2008 年よりオブザーバーとして参加、正式メンバーとしての承認申請をしているが、監督機関である OPDP が永続的な組織でないため、まだ正式メンバーとして認められていない。OECD の「プライバシー保護法執行の越境協力に関する提言」に基づき創設された Global Privacy Enforcement Network (GPEN)へは 2012 年に正式メンバーとして認定されている。

3. 個人情報保護に関する認証制度

現時点ではマカオに個人情報保護に関する認証制度は存在しない。他国の動向を注視している。

4. 個人情報保護の施行状況

個人データ保護法の基本方針に沿って、OPDP により違反に対する法執行が行われている。また、データ管理者が個人データ保護法を理解し、遵守できるよう業務ガイドラインを発行している。

v. メキシコ

1. 個人情報保護法制

名称は「民間が保有する個人データの保護に関する連邦法」。2010 年に制定、施行。民間部門の個人情報保護法である。成立に当たっては、2007 年以降に採択された個人データの保護に関する憲法修正及び EU との経済連携協定をはじめとする北米地域での各種協定を契機としている。本法の特徴は、個人のプライバシー及び情報自己決定権を憲法レベルの人権であるとしたこと、その背景には欧州、特にスペインの影響があること、個人情報保護へのアプローチはアメリカよりも欧州、そして欧州よりカナダに近いとされていることなどである。また、個人データ保護法以外に連邦レベルの法律で個人情報の保護に関する様々な規定を置いている。

監督機関は情報へのアクセス及びデータ保護の連邦機関（IFAI）が、政府の公的情報の透明性及びアクセスに関する連邦法第 33 条に基づき設置されており、その後、個人データ保護法の成立に伴い、2010 年 7 月より個人データ保護についても業務を開始した。

2. 国際的なルールへの対応状況

2013 年 1 月に APEC - CPEA の 2 番目の参加エコノミーとして承認され、2012 年 9 月には CBPR への参加を申請した。また、OECD 加盟国でもあるため、法は OECD プライバシー・ガイドライン等を基盤にしている。

欧州評議会第 108 条約については、コミッショナーが欧州評議会第 108 条約現代化の審議過程において議論に参加しており、外務省を通じて条約への明確な参加の意図を表明した。また、欧州一般データ保護規制提案についても、欧州委員会主催のワークショップ等に参加している。

貿易協定等について、世界貿易機構（WTO）や北米自由貿易協定（NAFTA）、北米の安全及び繁栄のためのパートナーシップ（SPPNA）、EU - メキシコ貿易協定を始めとする枠組みに参画し、個人データ保護に関する対応を行っている。

3. 個人情報保護に関する認証制度

2013 年 1 月に公表されたガイドラインに基づき、個人データの保護に向けた認証制度が確立された。認証制度における IFAI の位置付けは、認証付与団体が適切な付与を行っているか、その適正な手続を監視する役割を果たすこととされている。

4. 個人情報保護の施行状況

個人情報保護に関する申立てはオンラインを可能としている。権限行使の主な執行例については IFAI のホームページ上に公表されることとなる。また、2012 年までに 4 つの勧告・ガイドラインが IFAI によって公表され、広報啓発活動が行われている。

vi. コスタリカ

1. 個人情報保護法制

名称は「個人データの取扱いにおいて個人を保護する法律」。公的部門及び民間部門を規制。2011 年 7 月成立、2013 年 3 月から施行。

コスタリカの憲法では第 24 条において親密の権利を明文化しており、この規定からプライバシーの権利及びデータ保護の権利が認められると解されている。コスタリカにおいてデータ保護は確立した基本的人権である。制定に当たり、モデルとしたのは主にスペインである。

特徴としては、「忘れられる権利（Derecho al olvido）」を定め、法令で定められている場合や当事者の合意がある場合を除き、個人データの保有は 10 年以内とされている（第 11 条）。他方、データベースの所有について登録制度を採用し、データベースの登録に際しては、事業の大きさに応じて登録料をデータ保護機関に支払わなければならないという、ごく初期の個人情報保護制度にみられたシステムを採用している。

監督機関は法務平和省国立登記所（Registro Nacional）がこれまで一定のデータ保護業務を行っていたが、データ保護法に基づき「住民のデータ保護機関」が 2011 年 7 月に成立、2013 年 3 月から始動した。法務平和省に属する機関だが、事務的には独立しており、官民全ての機関に対して権限を行使することが可能である。

2. 国際的なルールへの対応状況

APEC-CPEA 及び APEC-CBPR への対応については、APEC のメンバー・エコノミーではないため、具体的な対応状況は見られない。APEC における取組については、今後対応を注視していく段階である。

OECD プライバシー・ガイドライン改正・欧州評議会第 108 条約現代化・欧州一般データ保護規則提案への対応についても、これらの加盟国ではないため、具体的な対応状況は見られず、監督機関によれば、これらについて特に参考にはしていない。

その他、貿易・連合協定においては、2009 年 1 月発行の「米・中米・ドミニカ共和国自由貿易協定」を始めとして、データ保護に関する情報共有や相互協力等を行っている。

3. 個人情報保護に関する認証制度

監督機関が実質的な活動を開始したばかりのため、現状認証を実施する状況にない。

4. 個人情報保護の施行状況

2013 年 3 月に施行されたばかりであるため、公表されているものはない。

本編

I. APECと個人情報保護活動

i. はじめに

2012 年５月、ロシアAPECのカザン会議で個人情報保護グループ [1]と知り合い今回の実態調査に誘われて、参加した。 私はAPECの発足当初から太平洋協力活動に参加し、APECの推進をライフワークとしている。その新しい活動分野に個人情報保護が付加されたことを歓迎し、お役に立てればと考えた次第である。個人情報保護は経済協力開発機構（OECD）や欧州評議会（CoE）が先鞭をつけ、欧州連合（EU）はCoEをモデルにしてデータ保護指令（Data Protection Directive）を策定したが、APECはEUとは全く異なった組織である。またOECDと違って、アジア太平洋地域を地盤とし、米国や豪州のような先進国だけでなく、タイ、インドネシア、中国、ベトナムといった発展途上国も含む地域協力組織である。APECの枠組みで個人情報保護活動を進めていく上で、APECの組織、モダリティーを正しく理解していただく必要がある。その点で本稿がお役に立てば幸甚である。他方個人情報保護活動はAPECステークホールダーに広く知られてはいないようである。本稿が彼らにAPECでの個人情報保護への取組とその意義を理解していただく一助になればとも思う [2]。

ii. APECの組織と行動様式 [3]

1. アジア太平洋の経済協力組織

APEC は経済協力を話し合う、年に１度の外務・貿易大臣会合として 1989 年に始まった。日、米、豪、加、ニュージーランドに ASEAN６か国と韓国の 12 か国であった。しかし 1991 年中国・香港・台湾が同時参加し、1993 年米国主催で首脳会議が開かれてから、アジア太平洋の主要国の大統領・首相が一堂に会する機会としてメディアに大きく報道されるようになった。1998 年までにロシア、ベトナム、ペルーを含め太平洋を囲

1　ECSG（電子商取引推進グループ）及び DPS（データ・プライバシー・サブグループ）日本代表団のことであり、具体的には、消費者庁板倉陽一郎氏、一般財団法人日本情報経済社会推進協会関本貢氏及び加藤健氏（いずれも所属は当時）。

2　筆者は APEC 研究センタージャパン（ASCJ）メンバーであり、元 APEC 賢人会議メンバー（1993 - 95）である。ASCJ の活動についてはホームページ参照されたし (http://ascj.web.fc2.com/（最終更新：2013 年３月 12 日、執筆時））。

なお、筆者は法律・法制度に関しては全くの素人であり、本稿も個人情報保護に関する限られた文献を勉強して、APEC 活動との接点を記したものである。そして「ｖ．結び」は筆者自身の感想であり、調査会での議論を反映していない。

3　山澤逸平『アジア太平洋協力：21 世紀の新課題』（日本貿易振興機構（ジェトロ）、2010 年）。なお後述の APEC 関連資料は全てジェトロ・ビジネスライブラリー内のアジ研サテライトの APEC 棚に収録してあり、閲覧可能。

む 21 エコノミー（APEC では参加国・地域をこう呼ぶ。）が参加した巨大な地域組織となった。

議題の中心も貿易投資の自由化にシフトした。毎年参加エコノミーのひとつが交互に両会議を主催し、その年の APEC の活動のイニシアティブをとる。そのために参加エコノミーの高級実務者（日本では外務省・経産省の審議官レベル）が年に３～４回協議する一方、個別分野・課題についての担当者による委員会やタスクフォースの活動があり、今では年間を通じての政府間協力枠組みになって、広範な分野をカバーしている。

2. APECの自発的自由化の行動様式

APEC では各エコノミーは協定に拘束されることなく、自発的に自由化を実施し、それを域内・域外を問わず全ての国へ最恵国待遇（MFN）ベースで適用する。この非拘束原則、自発的自由化、開かれた地域主義（open regionalism）が APEC 独自の自由化方式である。これは GATT/WTO 規約に完全に整合的であるし、これを GATT/WTO 規約による多角的自由化交渉の促進と並行的に進めることが APEC の自由化戦略であった。

個別行動計画を中核とする IAP（Individual Action Plan）方式は APEC の独自の自由化・円滑化の実施の仕組みである「協調的自発的自由化（CUL）」を採っている。この仕組みでは個々の参加国は自国の自由化・円滑化プログラムを自発的に発表して、自国のやり方で実施する。しかし相互に自由化計画と実施状況を観察して、自国の自由化計画が他国と同じ程度になるようにし、かつ約束通りに実施するようになるのである。APEC はこのピア・プレシャー（仲間内の監視）に依存して、全ての参加国が自由化努力を続けるように仕向けている。

参加国政府は毎年 IAP を改定して報告する。各国の IAP 報告は、貿易投資委員会が設定した共通様式に従って、精緻になり、透明性も増していった。自由化はウルグアイラウンド合意が実施されていくのに連れて増えていった。自発的自由化の中にはウルグアイラウンド合意の繰上げ実施も含まれ、また数か国では WTO 協定税率以下に実行税率を引き下げた。

しかしこの方式では困難分野の自由化は進展しなかった。日本や韓国の農業、米国・カナダの繊維産業、アジア先発途上国の鉄鋼業・自動車産業等である。これらの分野にはなお高率の関税が残っていて、その削減には双務的な WTO 交渉を待つ以外にない。その DDA（WTO ドーハ・ラウンド交渉）も難航して、これらの分野の自由化は遅れたままである。

これを高度の制度的統合を達成しているEUと比較してみよう。単一市場を完成しているEUではどのように市場統合を確保しているのか。EUの単一市場は人、モノ、サービ

ス、資本の４つの域内移動の自由で成り立っており、それらを阻害する要因を取り除く[4]。まずそれらを除去することをEUを設立する条約で定めている。域内市場・サービス総局（Directorate-General for Internal Market and Services）が管轄している。具体的には内部市場、人の移動自由、労働者移動自由、モノの移動自由、設立権及びサービス提供の自由、資本移動自由、実施に関する法令、公共契約に関する法令が施行されている。

問題はこれらがメンバー国の国内法令にその通りに移行され（transpose）、施行されているかである。EUではそれを各メンバー国についてチェックして、違反（infringement）を指摘し、それが国内法令の何パーセントに当たるかのtransposition deficit を公表する（Internal Market Scoreboard）。2009 年報告書では３期続けてEU全体の平均で１パーセントを保っている[5]。27 か国のうち 18 か国が１パーセント以下であり、３か国はほとんど完璧な移行実績を果たしている。他方７か国はこの１パーセント基準を大きくはずれ、その６か国は違反が増えている。これらはいずれも実際の国名を挙げて公表されている。

自発的、非拘束的を原則とする APEC では EU のような強制力を持たないし、統合化が法律にもなっていないから、メンバー・エコノミーの違反を問うこともできない。せいぜい全ての参加エコノミーが受益することに合意して、公表する程度である。ただし通関手続、基準認証、知的所有権、商用ビザ等の貿易円滑化分野では、各エコノミーは自国の利益になるから自発的に実施する。さらに途上エコノミーが能力不足で実施が遅れるのを防ぐために、共同行動計画で先発エコノミーによる技術支援を提供する程度である。これら全てが IAP に記載され、ピアレビューされるのである。

2010 横浜 APEC で APEC 首脳会議はボゴール目標への中間評価を発表した。これにはボゴール宣言で指定された５先進エコノミー（豪州、カナダ、日本、ニュージーランド、米国）と自発的に評価を受けると申し出た８エコノミー（チリ、香港、韓国、マレーシア、メキシコ、ペルー、シンガポール、台北）の 13 エコノミーが含まれる。ただし個別エコノミーの評価ではなく、13 エコノミーの全体評価のみが公表された。APEC では特定エコノミーを名指しして、毀誉褒貶することを嫌うからである。

すなわち 1995～2008 年、APECエコノミーでは貿易投資は大幅に拡大し、アジア太平洋地域は世界経済を牽引する成長軸になった。これには自発的な関税引下げや投資自由化に加えて、税関手続の簡素化や基準認証制度を共通化する等、重要な貿易円滑化措置を実施したことがあずかった。しかし先進エコノミーでの農業や繊維産業、途上エコノミーでの重化学工業ではなお国内産業保護が残っている。首脳宣言では、21 エコノミ

4　ここでの説明はヨーロッパ委員会のウェブサイトで、”Internal Market: General policy Framework”の記述に依存している。
<http://ec.europa.eu/internal_market/top_layer/ >

5　Europian Commission, “*Internal Market Scoreboard*”, (July 2009), ISSN 1830-5881　同じく上掲のウェブサイト。

一全てが、2020 年のボゴール目標へ向けて自由化円滑化を続行すると言明した。[6] 2012 年から、強化されたIAPプロセスが進行している [7]。

3. 多彩な経済協力活動

他方APECは多彩な経済協力活動に取り組んできた。経済技術協力Ecotechという分野である [8]。また国境での制限措置を取り除く自由化と並んで、それに接続する国内措置も制限されていることがしばしばある。これを「国境の背後の国内措置」(behind-the-border-measures)と呼んで、その整理が 2000 年代に入ってAPEC内で議論されるようになった。2004 年のサンチャゴ会議で『構造改革のための首脳のアジェンダ（LAISR)』が採択された。これは競争政策、規制改革、公的部門のガバナンス、企業ガバナンス、経済・法的インフラの強化の５優先分野での構造改革を推進するとしている。グローバル化に対応してアジア太平洋地域の自由市場経済制度を整備する方向へ向かっているといえよう。

これらは民主主義・人権尊重・市民社会を共有し、政府による恣意的裁量に対して法による支配を確立しようという動きである。しかし APEC 参加国では、先進エコノミーこそこの理念を共有しているが、途上エコノミーでは一部で制度化が始まったばかりである。またロシア、中国、ベトナム等の旧社会主義エコノミーでは市民社会の基本的人権が共有されていない。さらに国営企業が支配的で、国・州・市政府の管理が多く残り、そこまで踏み切れない。

これらの国々に自由市場経済、民主的市民社会の理念を説得し、それに参加することによりグローバル化の恩恵を享受する。それを非拘束方式で、自発的に実施させ、経済技術協力や規制改革で支援する。APEC にはそのような役割が期待されている。個人情報保護の普及もその一環として推進される。

---

6 APEC, *Leaders' Statement on 2010 Bogor Goals Assessment*, Nov. 2010

7 筆者はこのプロセスをモニターし、ボゴール目標に近づけるべく高級実務者を勇気付けるよう、学界やビジネスの APEC ステークホールダーに呼びかけている（Yamazawa, Atsumi, Ishido, "*APEC's New IAP Process: How Can We Strengthen It toward the Bogor Goals in 2020?",* 2012。

8 詳細は前掲の山澤著書、５、６章を参照されたい。

iii. 個人情報保護活動

1. 個人情報保護の理念[9]

米国では、「個人のプライバシーを侵害されない」ことを権利として認めようという主張が 19 世紀末から現われてきた。国によってはそれを基本的人権の一部として憲法で保障しようというところも出てきた。もっとも個人情報保護は人権意識の高まりよりは、電子計算機の普及と情報通信技術の発展によって、電子商取引が急拡大しつつあり、企業や国・地方政府による個人情報の大量収集が広まって、集められた個人情報が不適切に利用されることで、深刻なプライバシー侵害が生ずる可能性が生じたという面もある。

1974 年米国連邦議会はプライバシー法を成立させ、欧州では 1970 年代を通じて、西ドイツ、フランス、スェーデン、ノルウェー、デンマーク、オーストリアがデータ保護や情報処理に関する法律を制定した。1978 年 OECD は専門家グループを設けて、国境を越えるデータの流れや個人データとプライバシー保護を規律する基本原則を定める OECD ガイドライン案を策定した。OECD 理事会は 1980 年にこれを採択して、加盟国へ勧告した。これはプライバシー保護の国際水準を示したもので、収集制限、データ内容、目的明確化、利用制限、安全保護、公開、個人参加、責任の 8 原則を掲げている。

欧州ではさらに 1995 年に EU データ保護指令（EU Data Protection Directive）を採択した。これは個人データの取扱いに対する自然人の基本的権利及び自由、特にプライバシー権の保護を規定し、現在では全 27 加盟国内で国内法化済である。さらに EU 域内から「十分なレベルの保護措置」を確保していない第三国への個人データの移転を規制する、第三国条項を設けて、EU 以外にも大きな影響を与えている。その一つ拘束的企業準則（Binding Corporate Rules, BCR）は、「EU 加盟国内に拠点を有する企業のデータ管理者又は処理者が、企業グループ内において、EU 域外のデータ管理者又はデータ処理者に対して、個人データの移転を行う際に遵守すべき企業の準則」を定めている。もっとも APEC ではカナダとニュージーランドが EU から十分な保護水準を確保していると認められているが、オーストラリアは保護水準が不十分とされた（2001 年）。米国は包括法がないため、特定の認証基準を設けて、その認証を受けた企業ごとに十分性を付与するセーフ・ハーバーの枠組みを EU と設定した(2000 年)。日本も含めアジア諸国は十分性が認められておらず、日本の一部事業者が個別に BCR や標準契約条項（Standard Contractual Clauses, SCC）を申請しているのみである。

他方民間レベルでは企業サイドから電子商取引への規制の在り方についての働きかけが起こった。日本の電子機器メーカーも参加して、Global Business Dialogue in e-Commerce (GBDe) が 1999 年に発足し、電子商取引を活発化するための政府・民間

9　この部分の記述は堀部政男『プライバシーと高度情報化社会』（岩波新書、1988 年）に負う。

の対話を開始した。その課題として、課税、関税、知的所有権と並んで個人情報保護も挙げられている[10]。

2. ABACの電子商取引推進活動

個人情報保護がAPECで取り上げられたのはやはりビジネス界からの働きかけがあったからだと思われる。APECは政府機関だから、基本的に政府の官僚が主体である。しかしAPECは多方面にわたって民間の経済活動に関わるので、民間の知恵、情報、協力が不可欠である。1995 年にAPECビジネス諮問委員会（ABAC）が拡大再編された。各エコノミーから 3 人ずつ参加し、１人は中小企業を代表する形をとっている[11]。ABACはAPECのワーク・プログラムの実施についてアドバイスし、かつビジネス分野の優先事項及び関連情報を伝える役割を期待されている。

ABAC は毎年首脳会議へ提言する。実際には APEC のワーク・プログラムの各分野にわたってレビューして、その中でビジネスの優先事項を指摘する。ABAC はいくつかの APEC の成果となる提言をしている。1996 年の APEC ビジネストラベルカード(ABTC)、2006 年のアジア太平洋自由貿易地域（FTAAP）提案、また 2007 年には金融システムの安定化、債券市場の育成やビジネス環境整備を強調している。電子商取引の促進もその一つである。

ABAC による電子商取引関連の提言を列挙しよう。

- 2000 年 5 月、ABAC の貿易大臣会合への「電子政府」提言：「 IT の技術的進歩から完全に利益を享受するためには、政府が環境整備のために重要な役割を担う」
- 2004-2005 年、首脳への提言：「APEC Privacy Framework に含まれる一連の主要協定を全てのエコノミーで導入実施するとともに、実行メカニズムを開発せよ」
- 2006-2008 年、ABAC は APEC/ECSG と APEC Data Privacy Pathfinder Initiative の実施に向けた努力を継続。その実施を受けて、その拡充を提言。
- 2010 年、首脳への提言：「電子商取引への関税適用を恒久的に禁止せよ」
- 2011 年、中小企業大臣会合への提言：「中小・零細企業がグローバル市場へ参入する際に、越境電子商取引促進に関する政策や規制が不十分」
- 2011 年、首脳への提言：金融サービス業界でのクロスボーダーのデータフローの円滑化について具体的に指摘。「データ処理は金融サービス事業者の情報技術環境の極めて重要な一部である。データ処理業務は、現代的なリスク管理や引

10　GBDe ウェブサイト。GBDe は 2012 年に一応目的達成したとして解散した由である。

11　日本では東京の経団連会館内に ABAC 支援日本事務局が設けられている。毎年２回３人の委員による活動報告会が開かれている。

き受け業務を円滑化し、移動機会が増大しつつあるAPEC地域の人材に対して移動可能な信用情報を提供する信用情報機関にとっても、重要なものである。信用に関する全てのファイルを有する信用情報機関はAPECファイナンシャル・インクルージョン・イニシアティブの主要な構成要素であるが、クロスボーダー・データフローへの不当な制約により、その業務が阻害される可能性がある。」「プライバシー保護やクロスボーダーの個人データのフローに関する国内の立法行為は、クロスボーダーのフローを阻む場合があることを認識する。」「地域データセンターの活用を制限せず、むしろ金融機関がデータ処理や保存の目的で領域の内外への情報を移転することを可能にする」[12]（ABAC2011、59 頁）

- 2012 年、貿易大臣会合への提言：物品サービス・サプライチェーンの越境データフローの円滑化

個人情報を収集・処理し、越境移転を担当する民間企業のビジネス遂行上の便宜の要求と、一般消費者の個人情報を保護する立場からの立法者との間には厳しい相克があるようである。アジア太平洋地域では EU と異なって統一された取組はなく、各エコノミー政府の個人情報保護への取組は様々である。特にグローバル化が急速に進む今日、前者の活動は広範な国境を越え、後者の様々な政府による対応と錯綜する。この地域でも個人情報保護の基本原則を確立し、その執行を実効あらしめるような法制度を打ち立てなければならない。

3. アジア太平洋地域における電子商取引の実態

経済産業省のウェブサイト『電子商取引に関する市場調査（平成 23 年度)』は電子商取引の実態を伝えている。

(1) 日本の電子商取引の規模：企業間（B to B）（卸売、製造 - 電機、輸送機、繊維、食品等）は 171 兆円、EC 化率 16.1%。企業対消費者（B to C）は 8.5 兆円で EC 化率 2.8%だが、EC 化率は最近 5 年で倍増

(2) 越境電子商取引：日米中 3 国間の調査。消費者アンケート調査に基づき、B to C の越境 EC の利用及び利用率及び利用額を推計し、EC 利用者数に乗じて、越境 EC 市場規模を推計。日本の対米、中の越境 EC 利用はあまり伸びないが、中国そして米国の利用増は大きい。2020 年には、最も少なく仮定して、中国は 9,500 億円で、米、日から半々、米国は 3,800 億円で中、日からほぼ半々。

(3) 6 か国の電子商取引の利用状況：日、米、仏、中、インドネシア、ベトナムの消費者調査。日、米、仏は PC のみの利用が他と比べて多く、他 3 か国は 70%

12 APEC ビジネス諮問委員会『APEC 首脳への提言（2011 年版）全文[仮訳]』59 頁（http://www.keidanren.or.jp/abac/report/20111027c.pdf)。

以上が携帯、スマートフォン利用。インドネシア、ベトナムについては、最近２年で電子商取引が急拡大。扱う商品は書籍、衣類、アクセサリーが最多。電子商取引を利用する理由は購入の利便性が第一。他方利用上の不安・不便は、日、米、仏、ベトナムでは事前に実物確認できないことのほか、個人情報・発信の不安を挙げるが、中、インドネシアでは配送中の破損を挙げ、個人情報は挙げられていない。ただしこれら、特に越境取引で、いかなる個人信用情報や企業情報が電子移転されているのか、さらに個人情報保護がどのように確保されているのか、明らかにされていない。

なお国外の事業者との間の個人情報の授受についての調査によると、日本国内の事業者では「国外の事業者との間の個人情報の授受の頻度」は「頻繁に行っている」「たまに行うことがある」を合わせても、平成 18 年度で 11.4%、23 年度は 14.0%であり、未だ低い。しかし業種別では旅行業・宿泊業で 53.6%、インターネット関連サービス業で 33.4%、証券・先物取引業で 30.5%、保険業で 25.5%(いずれも平成 23 年度)であり、18 年度と比べて大幅に拡大している。そして、国外事業者との個人情報の授受に関する法整備の必要を感じている割合が全体で 49.4%に達している [13]。

他方、アジア諸国での個人情報保護への取組は様々である。

日本以外のアジア諸国、香港、台湾、韓国、マレーシアでは一応個人情報保護法が制定され、発効している。シンガポールでは統一した情報保護法は存在しないが、電子取引法、銀行法でカバーしている。中国、タイ、インドネシア、フィリピンでは現在準備中である [14]。もっともこれら諸国での個人情報保護がどの程度OECD理事会勧告やＥＵデータ保護指令を満たしているか。また各国の保護法が企業のデータ移転をどのように制約するのか、企業業務を阻害するほどに「不当に制約するのか」、残念ながら十分な情報が提供されていない。

13　消費者庁『個人情報の保護に関する事業者の取組実態調査（平成23年度)報告書』(平成 24 年３月)

14　DLA Piper, "*DLA Piper's Data Protection Law of the World March 2013 Edition*", March 2013, <http://www.thelawyer.com/Journals/2013/03/20/t/b/l/Data_Protection_Laws_of_the_World_2013-414865.pdf>

iv. APECでの電子商取引、個人情報保護への取組

1998 年

APEC Blueprint for Action on e-Commerce. 政府・民間が協力して電子商取引を育成する環境整備。

1999 年

E-Commerce Steering Group(ECSG)を貿易投資委員会内に設立。企業の参加を呼び掛け。

2000 年

首脳宣言:「全ての APEC エコノミーを digital divide の向こう側へ置き去りにしない」

2004 年 10 月 : APEC 閣僚宣言

APEC Privacy Framework を承認。APEC 参加エコノミーにおける整合性のある個人情報保護の取組を促進し、情報流通に対する不要な障害を除く。

2007 年 : APEC Data Privacy Pathfinder を採択

自己審査、適合性審査、認証受入れ、紛争処理の 4 原則を取り上げ。ボゴール目標の達成に向けた取組を活性化させるために、全ての APEC エコノミーが参加しなくとも、対応可能な一部エコノミーでプロジェクトを先行的に実施できることとしたもの

2009 年

CPEA（APEC Cross-Border Privacy Enforcement Agreement 執行協定）承認、2010 年、CPEA 発効

2011 年首脳宣言

情報の流れへの障害を減らし、消費者のプライバシーを増大し、地域のデータ・プライバシー相互流通を促進するために、APEC Cross Border Privacy Rules (CBPR) System を実施する。

ここまでで成立した APEC の個人情報保護の取組は以下のようになる。個人情報の収集・越境移転に当たる企業・団体等が APEC プライバシー原則（通知、収集、使用、選択、情報の完全性、セキュリティ措置、責任）を遵守していることを自己審査した回答表を付して、アカウンタビリティ・エージェントに提出して、審査認証を受ける。その結果は ECSG、DPS へ通知される。

なお ECSG や DPS から独立した、CBPR システムを運営する共同監視パネルを設立し、アカウンタビリティ・エージェントの独立性の設定、審査を行う。

他エコノミーの特定の個人情報データの収集・移転に関して苦情が提起された場合には、当該エコノミーのプライバシー執行機関に援助要請を行い、逆に日本企業・団体に対して苦情が提起された場合には援助要請を受ける。

2012 年閣僚宣言

前年の首脳の CBPR 実施の約束を歓迎し、その実施に努めるとともに、APEC の CBPR と EU の BCR（Binding Corporate Rules）との同質性と相互運用可能性の諸問題を議論することを期待。

v. 結び

- 電子商取引の急拡大はアジア太平洋地域で、特に途上国の越境取引で顕著である。アジア太平洋地域、特に中国、ASEAN は日本経済の再活性化のホームグラウンドである。日本は電子商取引でも、これら諸国を取り込むイニシアティブを取らなければならない。ただ３、４節の資料調査からも、個人情報保護に関して政府と民間とでずれがあるように感じられる。堀部教授は 1980 年代の日本について、「個人主義の伝統がなく、プライバシー侵害の被害者意識も、加害者意識も希薄だが、プライバシー権利意識層が出現してきた」（堀部、前掲書）と述べたが、本調査の過去３年の報告書はこの第三の立場に立っている。しかし上記の観点からは、もう少し企業側の要望を聞いて、その声を反映させるべきではないか。両者のバランスを見つける努力が必要ではないか。

- この調査会の目的は、アジア太平洋地域等における「新たな個人情報保護制度の動向及び国際的な協調の進展について分析し、今後の制度検討・政策決定に資する」ことであり、そのために他国の情報を収集する、とされるが、消極的に過ぎるのではないか。以上の趣旨からは、速やかに国内体制を整えて、APEC 全域、特にアジア諸国に共通基盤を作るように、APEC 会議でもイニシアティブを取るべきであろう。その場合、消費者保護だけでなく、日本のビジネスの要望を聞き、取り入れる努力が望まれる

- 各国事情調査結果は他国にも役立つ。英語での成果公表も有益であると思料する。さらにAPEC委員会で提案し、個人情報保護の整備状況を提出して、標準フォーマットによる一覧表を作ったらどうか。APEC／貿易投資委員会の他のタスクフォース、投資でも、通関措置でも、基準認証でも、知的所有権でも皆実施している。さらに各自の制度化努力を個別行動計画に報告させる[15]。これ

[15] 電子商取引も 1998 年から貿易投資委員会のタスクフォースに加えられたが、個別行動計画には記載されていない。

こそAPECの自発的実施であり、ピア・プレッシャーを期待できる。情報収集のみでは勿体ない。

II. 個人情報保護に関するAPECの取組

i. APECにおける個人情報保護の位置付け

APEC（Asia - Pacific Economic Cooperation、アジア太平洋経済協力）は、経済のブロック化を抑え、APEC 域内の貿易・投資の自由化を進めることによって、世界貿易機関（World Trade Organization）のもとにおける多角的自由貿易体制を維持・発展させることを目的として設立された。

この目的を達成するため、分野ごとにグループに分かれ、それぞれの分野における問題を検討、解決することに努めている。そして、個人情報保護の分野に関しては、電子商取引運営グループ（Electric Commerce Steering Group (ECSG)）を中心として議論されている。ECSG は、1999 年に設立され、域内における法や政策的環境を整えることによって、電子商取引の発展やその利用を促進することを目的としている。

この ECSG は、分野別に２つの下部組織を有している。そのひとつが、データ・プライバシー・サブグループ（Data Privacy Subgroup）であり、もうひとつが、ペーパーレス・トレイディング・サブグループ（Paperless Trading Subgroup）である。

このうち、個人情報保護を直接的に扱っているのは、データ・プライバシー・サブグループであり、そこで話し合われた施策が、親委員会にあたる ECSG で承認されるという形になっている。

なお、ECSG では、域内のエコノミーの多様な実情を考慮しつつ、①各国における APEC プライバシー・フレームワークの適用、②越境的なプライバシー・ルールの構築、③情報共有や調査・執行の越境協力、④試験的プロジェクトに向けた検討等を行ってきた。

ii. 個人情報保護に関するAPECの取組

1. 取組に至る経緯

1998 年 11 月

電子商取引に関する行動のための青写真（Blue print for Action on Electronic Commerce）では、電子商取引の潜在的可能性は、政府と事業者との協力なしに実現されないことが強調された。

2004 年 10 月

APEC プライバシー・フレームワーク（APEC Privacy Framework）が策定され、それがメンバー・エコノミーの閣僚によって承認された。そこでは、APEC 域内における効果的な情報プライバシーの保護と情報の自由な流通のバランスを図り、それを促進するための協力が、消費者の信頼を向上させ、電子商取引の成長を確保するための鍵となることが認められた。

2007 年 9 月

APEC データ・プライバシー・パスファインダー（APEC Data Privacy Pathfinder）計画が策定された。このパスファインダー計画では、越境的データ流通に関して、消費者の信頼と事業者の信用を促進することに向けた複数のプロジェクトを含んでいた。

また、この計画では、越境的プライバシー・ルール（Cross - Border Privacy Rule）制度の発展に関する一般的なコミットメント（general commitment）が含まれていた。

2009 年 11 月

パスファインダー計画の目的は、越境プライバシー・ルール（Cross-Border Privacy Rules (CBPR)）の確立とその実施によって達成されるが、それは、APEC 越境プライバシー執行協定（APEC Cross-border Privacy Enforcement Arrangement (CPEA)）という形で結実し、同協定がメンバー・エコノミーの閣僚によって承認された。そして、2010 年 6 月 16 日から、その運用が開始された。

2012 年 5 月

APEC 越境プライバシー・ルール制度共同監視パネル議定書（Protocols of the APEC Cross-Border Privacy Rules System Joint Oversight Panel）が ECSG の全体会合で承認された。この文書は、CBPR の制度を完成させ、その完全な運用を可能とするものである。

2012 年 6 月

アメリカ合衆国が CBPR で定められた要件を充足することについて、共同監視パネルが全会一致で認めたことを受けて、同国が CBPR 制度の参加国として要件を満たすことが ECSG において確認された。

2013 年 7 月

CPEA の運用開始 3 周年を記念し、ニュージーランドのオークランドで、APEC プライバシー執行に関するワークショップが開かれる予定である。

なお、経済産業省から APEC 事務局にプログラム・ディレクターとして出向中（2013 年 3 月当時）の清水幹治氏は、APEC の CBPR について、次のように述べている。

「CBPR は APEC の取組の中ではユニークであることは間違いないと思う。APEC の取組は非拘束的であることを特徴としており、その実効性はピアレビューに支えられている。CBPR システムは参加こそ任意ではあるが、参加した場合に国内法の範囲内でその実効性を法的に担保することが求められる。APEC で何か具体的な「制度」を構築することは、実効性担保の点からも難しく、成果としては APEC ビジネス・トラベルカー

ドくらいであろうが、CBPR の取組は APEC 内でも制度的な取組は可能であることを示している。国際的な個人情報保護の取組について、こうした APEC のユニークな制度的枠組みに焦点を当てて、その意義や実効性について検討することは面白いかもしれない」。

2. 取組概要

プライバシー・フレームワークでは、次の４つの目的が定められていた。

① 自己査定
② 適合性審査
③ 認証・受入
④ 紛争解決・執行

そして、この目的を実現するために、パスファインダー計画が策定され、そこでは、具体的に次のようなプロジェクトが進められた。

① 事業者の自己査定基準
② 責任団体の認定基準
③ 事業者のプライバシー・ルールの認証基準
④ 認定事業者リスト
⑤ データ保護執行機関の窓口リスト
⑥ 執行協力のための文書
⑦ 越境的苦情処理の書式
⑧ CBPR 制度の射程範囲及びガバナンス
⑨ 試験的取組

APEC 越境プライバシー執行協定（CPEA）の策定は、パスファインダー計画における非常に大きな成果である（全文の翻訳については別添資料を参照）。この CPEA の目的は、APEC エコノミーのプライバシー執行機関における情報共有を促進すること、プライバシー法の執行において右執行機関間の効果的な越境的協力を促進するメカニズムを提供すること、APEC 域外のプライバシー執行機関とプライバシーに関する調査や執行のための情報共有及び協力を推進することである。

3. CPEA管理者と参加機関

CPEA 管理者と参加機関については、APEC のホームページにおいて、次のように掲載されている
（http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx）。それ

によると、現時点で、CPEA 管理者は 3 機関であり、参加機関は 22 のプライバシー執行機関である。

① CPEA 管理者

- APEC 事務局（APEC Secretariat）
- オーストラリア情報コミッショナー・オフィス（The Office of the Australian Information Commissioner）
- アメリカ連邦取引委員会（The U.S. Federal Trade Commission）

② 参加機関

- オーストラリア情報コミッショナー・オフィス
- ニュージーランドプライバシー・コミッショナー・オフィス（New Zealand Office of the Privacy Commissioner）
- アメリカ連邦取引委員会
- 個人データ・プライバシー・コミッショナー・オフィス、香港（The Office of the Privacy Commissioner for Personal Data, Hong Kong）
- カナダプライバシー・コミッショナー・オフィス（The Office of the Privacy Commissioner of Canada）
- 外務省（日本）
- 経済産業省（日本）
- 総務省（日本）
- 財務省（日本）
- 法務省（日本）
- 農林水産省（日本）
- 国土交通省（日本）
- 防衛省（日本）
- 厚生労働省（日本）
- 文部科学省（日本）
- 環境省（日本）
- 内閣府（日本）
- 消費者庁（日本）
- 金融庁（日本）
- 警察庁（日本）
- 韓国公共管理・安全省（Ministry of Public Administration and Security of Korea）

- メキシコ情報アクセス・データ保護連邦組織（Federal Institute for Access to Information and Data Protection of Mexico）

iii. APECの取組に対する各国の関与の程度

APEC のホームページから、ECSG のページに入り、Data Privacy Individual Action Plan という項目をみると、各国から提出されたペーパーによって、APEC のプライバシー・フレームワークに対する取組状況が明らかとされている（http://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Data-Privacy-Individual-Action-Plan.aspx）。

そこでは、次のような国々がペーパーを提出している（以下の括弧内の年は、最後の更新年である。）。もっとも、最後の更新年をみれば明らかなように、フィリピンやシンガポールなど、現時点では最新の立法を反映させているとはいえない国もある。また、CPEA への参加状況は既に示したとおりである。

- オーストラリア（2006 年）
- カナダ（2006 年）
- 香港（2006 年）
- 日本（2006 年）
- 韓国（2006 年）
- マレーシア（2010 年）
- メキシコ（2006 年）
- ニュージーランド（2011 年）
- ペルー（2006 年）
- フィリピン（2009 年）
- シンガポール（2006 年）
- 台湾（2011 年）
- タイ（2011 年）
- アメリカ（2006 年）

iv. 他の国・地域との関係

2013 年の 1 月から 2 月にかけてインドネシアのジャカルタで行われた ECSG の会合では、APEC と EU の作業チームの初めての会合が開かれた。EU からは EU データ保護指令第 29 条の作業部会の代表者らが出席し、APEC からは、カナダ、台湾、日本、韓国、マレーシア、ニュージーランド、フィリピン、シンガポール、タイ、アメリカ合衆国の 10 エコノミーの代表が出席した。なお、APEC と EU のデータ保護制度の相互運用（interoperability）を調査するためのこうした作業グループの創設は、2012 年のロシアのカザンにおける会合で承認されていたところである。

この会合では、EU の拘束的企業ルール（Binding Corporate Rule）（このルールの詳細については、国際移転における企業の個人データ保護措置調査報告書（消費者庁、平成 22 年 3 月）を参照）と APEC の CBPR との接合が検討された。両制度は、個人データの越境移転に関して、EU データ保護執行機関や APEC に認められたアカウンタビリティ機関による事前承認を受けた企業の内部的拘束ルールを利用するという点で類似したアプローチをとっている。そこで、両制度の比較検討のため、EU 側は、両者の共通する部分と依然として存在する主要な相違部分について事前に調査した資料を提供した。この作業チームでは、今後も継続的に協議をしていくことで一致した。

なお、APEC 事務局の清水氏は、このような APEC と EU の取組について、次のように述べている。「現在進行形の注目すべき取組としては、CBPR と EU の BCR との接合である。すでに ECSG は EU との共同で BCR と CBPR の要求事項の対照表作りを進めている。この作業を経て、将来的には CBPR 認証を受けた事業者が BCR 認証を受ける際に何らかの有利な取扱いを受けられるよう CBPR 側から EU 側に働きかけることになることが予想される。交渉結果の予断はできないが、もしこの優遇が認められれば、CBPR 認証の魅力は一気に高まることは間違いないだろう」。

v. 別添資料：越境プライバシー執行のためのAPEC協力協定

1. 本枠組みの目的

2004 年に APEC プライバシー・フレームワークを承認するに際して、APEC の代表者は、情報流通に対する障壁を回避し、APEC 地域における貿易及び経済の継続的成長を確保する効果的なプライバシー保護措置を発展させることの重要性を認めていた。この越境協力協定は、この目的を達成するための重要なステップである。

APEC プライバシー・フレームワークⅣB では、メンバー・エコノミーに対して、プライバシー法の執行における越境協力促進のための協力協定及びその手続の発展を検討するよう求めている。APEC プライバシー・フレームワークは、以下の事項を含む二国間又は多国間協定を企図している。

- 他のメンバー・エコノミーの個人に対する違法な行為又はその個人へ生じる危害を対象とした調査やプライバシー執行の事案について、そのエコノミーにおいて指定された公的機関に対して、迅速、機能的かつ効率的に通知するためのメカニズム
- 越境プライバシー調査及びその執行事案における協力を成功させるために必要な情報を効果的に共有するためのメカニズム
- プライバシー執行事案における調査支援のためのメカニズム
- 他のエコノミーにおける公的機関と協力するため、個人情報プライバシーの違法な侵害の程度、それに伴う現実の又は潜在的な危害及びその他の関連する事項に基づき、事案に優先順位を付けるメカニズム
- 本協力協定に基づき交換された情報の秘密保持の適切なレベルを維持するためのステップ

さらに、2007 年、APEC エコノミーは、APEC プライバシー・フレームワークの国際的な実施のための「パスファインダー」を承認した。この越境プライバシー執行のための協力協定は、このパスファインダーの成果のひとつである。また、本パスファインダーは、事業者による越境プライバシー・ルールの利用に焦点をあて、個人情報の責任ある越境的流通のための枠組みの発展の促進を追求している。本パスファインダーは、情報プライバシーの執行における越境協力の枠組みと共にこの越境的プライバシー・ルールを支援することを目的としている。

2007 年、経済協力開発機構（OECD）は、プライバシー保護法の執行における加盟国間の協力を推進する勧告を採択した。

このような背景に鑑み、本協力協定の目標は以下のとおりである。

- APECエコノミーのプライバシー執行機関間における情報共有を促進すること
- 事案の照会又は並行的若しくは共同的な調査や執行行為などを含めたプライバシー保護法の執行に際して、プライバシー執行機関間の有効な越境的協力を促進するメカニズムを構築すること
- 越境プライバシー・ルールを執行する際のプライバシー執行機関の協力を促進すること
- OECD勧告のもとに発展した協定のような類似の協定と本協力協定が緊密に協力することを確保すること等により、プライバシー調査や実施において、APEC域外のプライバシー執行機関との情報共有及び協力を促進すること

2. 協力協定の概要

2.1 本協力協定は、プライバシー執行機関が越境プライバシー執行に協力するための実践的な多国間のメカニズムを創造する。それは、プライバシー執行機関が、一定の方法で、自発的に、情報の共有及び援助の要請や提供ができるような枠組みを構築するという形で作られている。

2.2 APEC エコノミーにおけるいかなるプライバシー執行機関も、本協力協定に参加することができる。

2.3 第 4.1 条に含まれるプライバシー執行機関の定義に定められた基準を充足する限り、エコノミーは、複数の参加プライバシー執行機関を有することができる。

2.4 本協力協定は、以下の事項が規定されている。

- 本協力協定の開始（第３条）
- 定義及び法的制限（第４条、第６条及び第７条）
- 運営管理者の役割（第５条）
- 本協力協定への参加及び脱退の方法（第８条）
- 越境協力（第９条）
- 秘密保持（第10条）
- 情報共有（第11条）
- 雑則（職員交流、紛争、見直し）（第 12 条～第 15 条）

2.5 本協力協定には以下の文書が添付されている。

- 援助要請様式（付属書A）
- コンタクト・ポイント指定様式（付属書B）
- 参加機関の慣行、方針、及び活動に関する要約記載のための書式（付属書 C）

3. 開始

3.1　本協力協定は、第５条に基づき運営管理者が指定された日から１か月後又はECSG により指定されたそれより遅い日から開始する。

3.2　開始日以後、全てのプライバシー執行機関は、第８条に定められているところに従い、本協力協定に参加することができる。

4. 定義

4.1　本協力協定において、

「**運営管理者**」とは、第 5.1 条に基づき指定された単独又は複数の組織体をいう。

「**協力協定**」とは、越境プライバシー執行のための APEC 協力協定をいう。

「**越境プライバシー・ルール**」とは、APEC プライバシー・フレームワーク第 46 条から第 48 条と同義である。

「**ECSG**」とは、電子商取引運営グループ又は APEC プライバシー・フレームワークに対して責任を負う APEC 委員会をいう。

「**参加機関**」とは、本協力協定に参加した APEC のメンバー・エコノミーのプライバシー執行機関をいう。

「**プライバシー執行機関**」とは、プライバシー法の執行に責任を負い、調査の実施や執行手続を実行する権限を有する公的機関をいう。

「**プライバシー法**」とは、APEC エコノミーの法律又は規則であり、それらの執行が、APEC プライバシー・フレームワークと整合する個人情報保護の効果を有するものをいう。

「**受領機関**」とは、他の参加機関から援助要請を受領した参加機関をいう。

「**援助要請**」には、以下の事項が含まれるが、これらに限定されない。

(i)　プライバシー法の執行に関連する事項の照会

(ii)　プライバシー法の執行に関する協力要請

(iii)　プライバシー法違反の申立てに関する調査への協力要請

(iv)　プライバシーに関する苦情の移転

「**要請機関**」とは、他の参加機関に援助要請を行った参加機関をいう。

5. 協力枠組み運営管理者の役割

5.1　ECSG は、運営管理者の役割を果たさせるため、次の下記のいずれかの機関を指定する。

(i)　APEC 事務局

(ii)　プライバシー執行機関（その同意のもとで）

(iii)　APEC 事務局とプライバシー執行機関（その同意のもとで）の両機関

5.2　第 5.1 条に基づく指定は、期間を限定すること、また、ECSG によりいつでも取消しや変更することができる。運営管理者として指定されたプライバシー執行機関の当該指定が失われた場合（期間満了、取消し、辞任又はプライバシー執行機関でなくなることによって）、新規の指定がなされるまで、APEC 事務局が運営管理者の中核的役割を遂行する（また、何らかの付加的役割を遂行することもできる。）。

5.3　運営管理者は次の中核的役割を遂行する。

(i)　以下の書類の受領：

(a)　第 8.1 条及び第 8.2 条に基づく本協力協定への参加又は脱退の意向を示す通知書

(b)　第 8.1 条に基づく確認書

(c)　第 11.1 条に基づくエコノミーのコンタクト・ポイントに関する書類

(ii)　第 5.3(i)条の文書を受領し、参加機関が本協力協定に定義されているプライバシー執行機関であることを検証すること

(iii)　第 5.3(ii)条の結果に従い、APEC ウェブサイトやその他の適切なアクセス可能な手段を通じて、第 5.3(i)(a)(c)条に基づき受領した文書を利用可能なものとすること

(iv)　以下を保持し、利用可能なものとすること

(a)　現在の参加機関の最新リスト

(b)　エコノミーのコンタクト・ポイントのリスト

(v)　第 15 条に定められているように、本協力協定の開始から 3 年後にその運用を精査すること

5.4　運営管理者は、次の付加的役割を果たすこともできる。

(i)　APEC、メンバー・エコノミー、利害関係者と共に、本協力協定を宣伝すること

(ii)　プライバシー執行機関又は参加機関であるかを問わず、プライバシー保護の役割を担う組織のリストを発行すること

(iii)　電話会議、セミナー、職員の交換、その他執行ネットワークとの協力等を通じた、参加機関間の協力を支援するイニシアティブを促進すること

(iv)　執行に関する共通の優先事項についての研究、記録、精査を促進すること

6.　本文書の趣旨

6.1　本協定は、APEC プライバシー・フレームワークと整合的に解釈される。

6.2　本協力協定は、以下のことを意図するものではない。

(i) 国際法若しくは国内法において、拘束力ある義務を創出することや既存の義務に影響を与えること、又は、参加機関のエコノミーの法体系のもとで義務を創出すること

(ii) 他の合意、条約、協定又は慣行に従い、参加機関が他の参加機関又は他のAPECメンバー・エコノミーの非参加執行機関から援助を求めること又はこれに援助することを妨げること

(iii) 他の参加機関エコノミーの領域に在住する個人から、法執行に関する問題を含む情報を合法的に求めるプライバシー執行機関又は非参加機関の権限に影響を及ぼすこと、又は、そのような個人が自発的にプライバシー執行機関又は非参加機関へ情報を提供することを妨げること

(iv) APECのメンバー・エコノミーのセキュリティ、公共の安全、主権、その他の公共政策を保護するために実施される法律で認められた政府の活動を阻害すること

(v) 参加機関の権限及び管轄権の範囲を超える協力義務や協力への期待を創出すること

(vi) 他の非参加政府機関に対する義務や期待を創出すること

(vii) 要請機関及び受領機関の間で締結された相互援助条約、その他の適用される国際合意に従い情報を利用する権利や権限に影響を及ぼすこと

7. 援助の限定

7.1 参加機関は、いつでも、その単独の裁量により、必ずしも次の状況に限定されないものの、次の状況において、援助要請の受理や手続の進行を拒否し又はその協力を限定することができる。

(i) 当該事項が、国内法又は政策と一致していない。

(ii) 当該事項が、参加機関の権限又は管轄権の範囲内にない。

(iii) 当該事項は、それぞれのプライバシー法に基づいて、要請機関及び受領機関の双方が調査又は執行する権限を付与されている類の行為又は慣行ではない。

(iv) リソースの制約がある。

(v) 当該事項が、他の優先事項と相反している。

(vi) 問題となっている事項に共通の利害関係が欠如している。

(vii) 当該事項が本協力協定の範囲外である。

(viii) （第9.4条と整合性を有する民間部門の組織を含む）他の組織の方が、当該事項を処理することについて、より適している。

(ix) 参加機関が協力できない他の状況が存在する。その参加機関は、その状況の根拠について文書で知らせることができる。

8. 本協力協定への参加

8.1 プライバシー執行機関は、運営管理者に書面による通知をすることにより、本協力協定に参加することができる。この参加は、ECSG のエコノミー代表又は他の適切な政府の代表者から、申請者が第 4.1 条に定義された意味におけるプライバシー執行機関であることを示す確認書によって支持されなければならない。この参加は、運営管理人が、第 5.3(ii)条に定める結果に従って、参加機関の書面を正式に受諾した後に発効する。

8.2 参加機関は、１か月前までに、運営管理者に対して書面による脱退の通知をなすことにより、本協力協定から脱退することができる。

8.3 プライバシー執行機関は、第 8.1 条又は第 8.2 条に基づき運営管理者に通知した後、可及的速やかに、その受諾又は脱退を他の参加機関に知らせるための合理的措置を講じなければならない。例えば、かかる措置として、当該機関が本協力協定に参加している期間内又は脱退後の合理的な期間内において、当該機関のウェブサイトに情報を掲示することがあげられる。

8.4 本協力協定からの脱退を予定しているプライバシー執行機関が、援助を要請されているか又は援助要請に基づいて現在活動している場合、当該機関は、その要請に関連して、本協力協定において当該機関に期待されていることを脱退後に遂行できるか否かについて検討しなければならない。仮に、当該要請が影響を受ける場合、当該機関は、要請機関や利害関係人の利益が保護され、とるべき行為について彼らが助言や相談を受けられるよう最善の努力を尽くさなければならない。

9. 越境協力

プライバシー法執行における越境協力

9.1 第６条及び第７条に従い、参加機関は、他の参加機関の援助要請、調査や執行の照会事項を考慮し、相互に援助し合い、また、その調査やプライバシー法の執行について情報を共有し、協力しなければならない。

越境協力のための事項の優先順位

9.2 越境協力では、複雑かつ多くのリソースが必要となり得ることに鑑み、参加機関は、本質的に最も深刻な事項について、個人情報プライバシーの違法な侵害、それに伴う現実的又は潜在的な危害、その他の関連事項の重大性に基づき、個別的又は類型的に優先的に扱うことができる。特定の援助要請の優先的取扱いを求める参加機関は、その理由を援助要請様式に記載するものとする。

9.3　第 7.1 条及び第 9.2 条に従い、参加機関は、APEC の越境プライバシー・ルールの執行が本協定に基づく協力のために最優先であると認識するものとする。

非参加機関や組織との協力

9.4　参加機関は、個人のプライバシーに関する苦情の解決の責務を含む民間部門の組織、自主規制組織及び非参加プライバシー執行機関に協力するよう、それぞれの機関の権限の範囲内で最大限の努力を払うことを意図するものとする。プライバシー執行機関は、とりわけ、APEC 越境プライバシー・ルールの執行に携わるアカウンタビリティ機関と協力することが求められる。

9.5　参加機関は、第 10 条に従い、法執行機関を含む他の公的部門と協力するよう、それぞれの機関の制限の範囲内で最大限の努力を払うことを意図している。

援助要請前の措置

9.6　参加機関は、他の参加機関に援助要請を行う前に、次の措置をとらなければならない。

(i)　その要請が、本協力協定及び APEC プライバシー・フレームワークの目標と整合的であることを確認すること

(ii)　適切な場合には、当該プライバシー執行機関に適用されるその他の要件、方針、慣行に従った場合に、他の参加機関に対して苦情の情報を提供するために、その苦情を申し立てた個人から同意を求めること

(iii)　他の参加機関の慣行、方針、活動に関するアクセス可能な情報を調査すること（第 11.2 条及び第 11.3 条参照）

(iv)　適切かつ実行可能な場合、他のメンバー・エコノミーのいずれの機関が、第 9.4 条及び第 9.5 条と適合した援助要請に関する最前線の責任を有しているかについて、予備的な問合せを行うこと

(v)　適切な場合、相手当事者である参加機関が、これから行われる援助要請に対する管轄を有し、これを受諾するか否かについて確認するため、そのメンバー・エコノミーにおけるその参加機関若しくは他の適切な組織の（第 11.1 条の基づき指定された）コンタクト・ポイントに予備的に問合せを行い、また、必要に応じて情報を提供すること

援助の要請

9.7　他の参加機関に援助を要請する参加機関は、次のことを行わなければならない。

(i)　問題となっている事項の主要な情報を伝達するため、APEC「援助要請」様式（付属書 A に添付）を利用すること

(ii) 当該要請に応じる過程でとるべき特別な予防措置の特定等、受領機関が措置を講じるべきことについての十分な付加的情報（もしあれば）を提供すること

(iii) 受領機関から求められた情報の利用目的及びその情報が移転される個人を特定すること

(iv) 照会された事項の処理を支援するために、受領機関により要請された情報やその他の援助を提供すること

9.8 援助を要請された参加機関は、次のことを行わなければならない。

(i) 援助要請を受領後、可及的速やかにその要請を確認すること

(ii) 受領確認時又はその後の可及的速やかな時点で、当該要請の全部又は一部の受諾又は拒否を示唆すること

(iii) 当該要請の受諾又は拒否の決定をするために要請機関から更なる情報が必要な場合、更なる情報が必要であることを速やかに確認し、このことを要請機関に明確に連絡すること

(iv) 援助要請を拒否する場合、その判断の理由を示し、また、実行可能かつ適切であれば、当該要請を処理可能し得る組織について、要請機関に対し言及すること（第 9.4 条及び第 9.5 条と整合的である。）

(v) 援助範囲を限定する場合、その判断の理由を示し、援助をなすために課される条件について助言すること

(vi) 援助要請を受諾する場合、

(a) 通常の方針や慣行に従って当該要請を処理し

(b) 実行可能かつ適切な場合、問題となっている事項の処理の手助けとなる事項について要請機関と連絡をとり

(c) 実行可能かつ適切な場合、照会された事項の進捗状況及び結果について要請機関に情報を継続的に提供する

継続中の調査を支援するための連絡

9.9 参加機関は、継続中の調査を支援し得る事項ついて、適宜、相互に連絡をとるものとする。

越境協力中に取得した情報の利用

9.10 要請機関及び受領機関は、両当事者間において、適用される法や方針と整合的である共有情報について、許容される利用方法を決定する。

他の参加機関の管轄における違反の可能性に関する通知

9.11　参加機関は、適切であると考える場合、他の参加機関のエコノミーのプライバシー法違反の可能性があることについて当該参加機関に知らせることができる。

9.12　適切かつ実行可能な場合、参加機関は、より効果的な法執行を促進し、継続中の調査への介入を避けるために、自らの調査や執行行為と他の参加機関のそれとを調整しなければならない。

10. 秘密保持

10.1　第 9.10 条及び第 10.3 条に服し、また、要請機関及び受領機関に適用されるあらゆる法に従い、本執行協力のもとでの参加機関間の協議、その他の通信及び共有情報は、秘密とされ公表されない。

10.2　各参加機関は、最大限可能な限りそのエコノミーの法律と整合する範囲で、他の参加機関により秘密として連絡されたあらゆる情報の機密性を保持するために最善の努力を尽くし、かつ、他の参加機関により求められたあらゆる安全措置を尊重するものとする。

10.3　他の法執行機関等の第三者に対する秘密情報の開示を要請機関のエコノミーの法が求めている場合、本協力協定のいかなる規定もこれを妨げるものではない。参加機関は、慣行、方針及び活動（第 11.2 条及び第 11.3 条参照）に関する文書において、予期されるあらゆる開示要件を明らかにしなければならず、また、他の参加機関に対して秘密情報を求める際には、最新の慣行、方針、及び活動の文書を援助要請に添付しなければならない。要請機関が開示するための法的要件に服するのであれば、その開示の少なくとも 10 日前までに、仮に、かかる通知ができない場合には、可及的速やかに、受領機関に対し通知するよう最善の努力を尽くさなければならない。

10.4　第 10.3 条及び第 9.10 条に基づき開示された秘密情報は、適切な秘密保持措置に服するものとする。

10.5　本協力協定の参加から脱退する場合、プライバシー執行機関は、他の参加機関から秘密として提供されたいかなる情報に対しても、その秘密を保持しなければならない。本協力協定に基づき提供されたいかなる情報も、これを提供した参加機関との契約に従って、安全かつ秘密に保持、返却、その他の処理がなされなければならない。

10.6　第 9.10 条及び第 10.3 条に従い、参加機関は、そのエコノミーの法律と適合する範囲でできる限り、他の参加機関から受領した秘密情報又は資料の第三者による開示申請に対して、その情報を提供した参加機関との相談に服するものの、反対することを予定している。

10.7　各参加機関は、本協力協定に基づき受領したあらゆる情報の安全確保のため努力すべきである。この目的のため、参加機関は、本協力協定に基づき受領したいかなる情報の消失、無権限若しくは不慮のアクセス、処理、利用又は開示を防止する適切な措置を講じるものとする。本協力協定に基づき受領したいかなる情報も、国内法又はその情報の利用目的達成のために必要な期間を超えて保持されてはならない。

11. 情報の共有

コンタクト・ポイントの指定

11.1　各参加機関は、本協力協定に定められた目的及び他のプライバシー執行機関のために、唯一ではなくとも、主要なコンタクト・ポイントを指定しなければならない。本協力協定に添付されているコンタクト・ポイント指定様式（又はこの目的のため運営管理者により提供される更新版）を利用することができる。

参加機関の慣行、方針及び活動に関する文書

11.2　参加機関は、執行に関する慣行、方針、その他の関連する活動に関する情報についての文書を作成しなければならない。参加機関は、例えば、ウェブサイトに掲載することにより、この文書を他の参加機関が利用できるよう措置を講じなければならない。これらの文書が利用可能であることによって、各エコノミー内における執行内容に関する全体的理解や特定の援助要請の促進に対する全体的支援が向上する。

11.3　運営管理者は、中央での管理において、参加機関が利用できるように、参加機関に執行の慣行に関してまとめた文書の提出を求めることができる。仮に、その提出を求める場合、運営管理者は、本協力協定に添付された定型書式又はその更新版を利用する。参加機関は、その方針や慣行が変更された場合、更新された内容をまとめた文書を合理的な期間内に、運営管理者に提供しなければならない。

経験の共有

11.4　各参加機関は、実行可能でありかつ適切な場合、以下の事項を含む本協力協定の範囲内の事項に関連する重要な展開について有する情報を他の参加機関に提供することが奨励されている。

(i)　執行事項に関する世論調査

(ii)　執行又は越境協力という側面を有する調査プロジェクトの詳細

(iii)　執行研修プログラム

(iv)　関連する法律の改正

(v) プライバシー違反の調査における様々な手法及びそれらの違反に対する自主規制を含む規制方策に関する経験
(vi) 参加機関が処理する苦情や紛争の種類と数についての傾向や展開に関する情報
(vii) プライバシー執行職員の研修や雇用の機会

12. 職員交流

12.1 参加機関は、職員の出向や職員の交換について取り決めること、又は、特定の事項について専門職員による支援を可能にすることに関して、互いの機会を模索することができる。

12.2 参加機関は、適宜、以下の事項の実行可能性を検討することができる。
(i) 他の参加機関が実施する研修プログラムへ職員の参加を可能にすること
(ii) 共同研修プログラムの開発
(iii) 専門家研修リソースの共有

13. 費用

13.1 各参加機関は、本協力協定に従った情報や援助の提供及び本協力協定によると考えられるその他の協力に関するそれぞれの経費を負担する。

13.2 参加機関は、特定の援助要請、研修の提供、その他の協力に応えるための費用の分担や転嫁について交渉することができる。

14. 紛争

14.1 本協力協定に関連する参加機関間のいかなる紛争も、指定されたコンタクト・ポイントを通じた当事者間の協議により、また、合理的に時宜を得た形で解決できなかった場合には、参加機関の長の間における協議により解決されなければならない。

15. 本文書の見直し及び更新

15.1 参加機関は、協議過程を通じて、本協力協定の開始から３年後に本協力協定及びその運用の見直しを行わなければならない。

15.2 当該見直し完了後、運営管理者は、見直しに関する説明、必要な又は望ましい修正点を示した報告書を ECSG に提出する。

15.3 運営管理者は、ECSG により承認された変更について参加機関からの承諾を求め、それを受領する過程を管理し、また、適切に、現在の参加機関のリストを更新し、変更された本協力協定を利用可能な状態にする。

III. アジア太平洋地域等における個人情報保護制度

i. シンガポール

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

個人データ保護委員会のディレクター（Director of Personal Data Protection Commission）であるアモス・タン氏（Amos Tan）によると、新法であるデータ・プライバシー法を制定する動機は、シンガポールが世界のデータ・ハブとしての役割を担えるように推し進めようとする国家戦略の存在にあったという。シンガポールへデータが集約されてくるようになるためには、データ保護法の存在が不可欠であると考えたというのである。

そして、2011 年に、情報コミュニケーション技術省（Ministry of Information, Communication and the Arts）が草案及びコンサルテーション・ペーパーを提出し、翌 2012 年 10 月には、個人データ保護法が制定された。

同法では、迷惑電話禁止登録制度が設けられている点が特徴的である。また、同法のほか、プライバシー保護に関連する個別法として、個人情報保護について定めた銀行法（Banking Act）、電子取引法（Electronic Transactions Act）、情報コミュニケーション発展シンガポール機関法（Info-communications Development Authority of Singapore Act）などが存在する（第 67 条参照）。

さらに、個人データ保護法のもと、大臣は命令（regulation）を定めることもできるが（第 65 条）、現時点では制定されていない。

同法は、段階的に施行されることとなっており、2013 年 1 月 2 日に個人データ保護委員会の創設に関する規定がまず施行された。2014 年の初盤には、迷惑電話禁止登録制度に関する規定が施行され、同年の中盤には、データ保護に関する規定が施行される予定である。

(2) 個人情報保護法制の概要

a 法律名

組織による個人データの収集、利用及び開示を規制すること、個人データ保護委員会及び迷惑電話禁止登録機関（Do Not Call Register）を設立し、その運営やそれに関連する事項についての定めをおくこと、その他の様々な法律に対して関連する必然的な改正を行うことを目的とする法律（An Act to govern the collection, use and disclosure of personal data by organizations, and to establish the Personal Data Protection Commission and Do Not Call Register and to provide for their administration, and for matters connected therewith, and to make related and consequential amendments to various other Acts）である。

短い名称は、2012 年個人データ保護法（Personal Data Protection Act 2012）である（第１条)。

同法の所管官庁は、情報コミュニケーション技術省（Ministry of Information, Communication and the Arts）である。そして、同法の執行機関は、個人データ保護委員会（Personal Data Protection Commission）である。

b 目的

法律名に記載されているが、さらに、第３条では、同法の目的について、個人データを保護する個人の権利と、合理的な人間が当該状況下で適切と考える組織の個人データの収集、利用又は開示の必要性とを認めるような形で、組織による個人データの個人データの収集、利用及び開示を規制することと定めている。

つまり、個人データの保護とその利用の必要性とのバランスを図った法律であるといえる。

c 適用範囲及び適用除外

保護される個人データとは、真実であるか否かにかかわらず、当該データ又は当該データとその主体が有する若しくはアクセスできる他の情報を組み合わせた情報から個人が識別できるデータをいう（第２条)。

また、個人データ保護法の適用範囲について、第４条では、同法の適用が除外される対象という形で、次のように定めている。

① 第３章（個人データの保護に関する一般的なルール）から第６章（個人データの保護）規定は、以下の場合に適用されない（第１項）（なお、第４章は、個人データの収集、利用及び開示に関する定めであり、第５章は、個人データへのアクセスと訂正に関する定めである。)。

- 個人的又は家庭内の範囲における個人的な行為
- 組織において就業中の被用者の行為
- ある公の機関に代わって、個人データの収集、利用又は開示に関連して一連の行為を行う公の機関又は組織
- この規定の目的のため定められたその他の組織若しくは個人データ又は特定の組織集団若しくは個人データ

② 個人データの保護に関する第 24 条と個人データの保有に関する第 25 条の規定を除き、証明できる契約や文書での契約に従い、他の組織のために個人データを処理する請負業者（同法では、このような業者を data intermediary と呼んでいる。）に対しては、第３章から第６章の規定が適用されない（第２項)。

③ ある組織のために個人データの処理目的で請負業者によって処理される個人データに関しては、その組織が自ら個人データを処理した場合と同様の義務をその組織が負う（第３項)。

④ 本法は次のデータには適用されない（第４項）（なお、以下の「個人に関する個人データ」と「死亡した個人に関する個人データ」はリダンタントにも思えるが、原文に忠実に訳した。)。

- 少なくとも 100 年を経過して記録に含まれている個人に関する個人データ
- 死亡した個人に関する個人データ、ただし、個人データの開示に関する規定及び個人データの保護に関する第 24 条は、死後 10 年を経過していない個人に関する個人データには適用される。

⑤ 企業のコンタクト情報であることが明確に言及されている場合を除き、第３章から第６章の規定は、企業のコンタクト情報に適用されない（第５項)。

⑥ 本法で明確に規定されていない限り、次のように定める（第６項)。

- 第３章から第６章の規定は、法律若しくは法的特権によって与えられている権限、権利、特権、義務の免除又は課されている義務若しくは制限に影響を与えない。ただし、契約上の義務の履行が、本法に違反する理由とはならない場合を除く。
- 第３章から第６章の規定と他の法律の規定が矛盾する場合、後者の規定が優先する。

アモス氏は、同法の適用範囲について、次のように述べている。「同法がカバーするのは、民間部門のみである。国家が保有する個人情報については、法ではなく、内部規則によって規制されている。シンガポールでは、内部規則や法の遵守を監視、監督する組織が存在し、その機関が、公的部門のデータ保護の遵守を監視しているため、法律で拘束しなくとも、公的機関におけるデータ保護は十分に図られている。」

d 権利・義務の内容

個人データ保護法では、データ主体の権利として定めがおかれているのではなく、その多くは、個人データを保有する機関の義務として規定されている。例えば、データ主体の同意を原則として要求する規定（第 13 条、第 14 条）や個人データの正確性を確保する規定（第 23 条）などがあげられる。データ主体の権利として読み取れる規定は、次のようなものがある。

① 利用目的などの通知を受けること（第 20 条）
② 個人データへのアクセス（第 21 条）
③ 個人データの訂正要求（第 22 条）

また、明示的に個人の権利として定められている規定として、第４、５、６章のいずれかの規定に違反して損害を受けた者は、その組織に対して民事訴訟を提起することができるというものがある（第 32 条)。

e 届出・登録制度

存在しない。

f 苦情処理制度

データ保護委員会は、個人からの苦情の申立てを受けて、次の事項について審査することができる（第 28 条第１項)。

① 第 21 条に基づく申立人による個人データへのアクセス要求の拒否、又は、そのようなアクセスを合理的な期間内に与えなかったこと
② 第 21 条及び第 22 条に基づく申立人の要求に関して組織から求められる費用
③ 第 22 条に基づく申立人による個人データ修正の拒否、又は、そのような修正を合理的期間内に行わなかったこと

この審査が完了すると、同委員会はそれぞれに応じた事実を確認し、必要な措置をとるよう命じることができる（第 28 条第２項)。

同委員会は、個人の組織に対する苦情が仲裁による方が適切に解決されると判断した場合には、両者の同意のもと、仲裁に付託することができる（第 27 条第１項)。この規定に従い、同委員会は、両者の同意の有無に関わらず、同委員会が指示する方法によって解決するように努めることを命じることができる。

第 28 条第２項又は第 29 条に従いデータ保護委員会によって出された命令を執行するため、裁判規則（the Rules of Court）に従い、その命令を地方裁判所に登録することができる（第 30 条第１項)。命令が登録された日から、その命令は、地方裁判所で獲得した命令と同じ効力を有する（第 30 条第２項)。

なお、こうしたデータ保護委員会の命令に不服のある組織又は個人は、その命令が出されてから 28 日以内に、データ保護上訴パネル（Data Protection Appeal Panel）の長に訴えることができる（第 34 条第１項)。データ保護上訴パネルとは（第 33 条第１項)、大臣の指名するメンバーで構成され（第 33 条第２項)、第 34 条の審議のため、その長が同パネルの３名以上で構成されるデータ保護上訴委員会（Data Protection Appeal Committee）のメンバーを指名する。

上訴委員会の命令や決定に対する上訴のうち、上訴委員会の命令若しくは決定から生じる法的見解又は上訴委員会の命じる罰金の額に関するものは、これを高等裁判所になすべきである（第 35 条第１項）。

g 罰則

具体的な罰則規定として、次のような規定が置かれている。

① 無権限で、第 21 条若しくは第 22 条に基づき他人の個人データにアクセスすること若しくはこれを変更するよう求めた者は、5,000 ドル [16]以下の罰金若しくは１年以下の懲役又はこれらを併科する（第 55 条第１、２項）。
② 組織若しくは個人が、21 条若しくは 22 条による請求を免れる目的で、個人データ若しくは個人データの収集、利用、開示に関する情報を処分、変更、隠匿若しくは破壊又はそうすることを他人に指示する行為は罪となる。それが個人によるものである場合、5,000 ドル以下の罰金に処し、その他の場合には、50,000 ドル以下の罰金に処す（第 55 条第３項(a)、第４項）。
③ 組織若しくは個人が、本法における同委員会若しくは権限を与えられた役人の権限行使を妨害する行為は罪となる。さらに、本法における同委員会の義務の履行若しくは権限行使の間、故意若しくは過失により、同委員会に虚偽の申告した行為又は同委員会を故意に誤解させた若しくは誤解させようとした行為は罪となる。
④ これらの行為をした者が個人である場合、10,000 ドル以下の罰金若しくは１年以下の懲役又はこれらを併科する。その他の場合には、100,000 ドル以下の罰金に処す（第 55 条第３項(b)(c)、第５項）。
⑤ データ保護委員会の承認なしに同委員会と同様のシンボルや表象を利用した者、また、他人を欺く若しくは混同させる又はその可能性が高いシンボルや表象を利用した者は、2,000 ドル以下の罰金若しくは６か月以下の懲役又はこれらを併科する（第 61 条第２項）。

その他、法人などによる罪の場合（第 52 条）や被用者の行為に対する雇用主の責任（第 53 条）に関する定めがおかれている。

データ保護委員会は、その裁量によって、本法の罪について裁判外で合意することができるが、その合計は、定められた上限の罰金の 0,5 倍若しくは 5,000 ドルを超えてはならない（第 55 条第１項）。第９章に定める違反行為の場合には、1000 ドルを超えては

16 シンガポールドル

ならない（第 55 条第２項)。このような罰金の支払いがあった場合、その罪に関して、その後の手続をその違反者に対してとってはならない（第 55 条第３項)。

こうした罰則の明文が存在しないが、本法に違反する行為が罪となる場合には（例えば、秘密保持の規定に違反する場合（第 59 条第２項))、10,000 ドル以下の罰金若しくは３年以下の懲役又はこれらを併科する(第 56 条前段)。継続的な違反行為に対しては、さらに、その行為が継続している間、1,000 ドル以下の追加的罰金を毎日又はその一部の日数に対して科す（第 56 条後段)。

h その他の特徴的な制度

(a) 個人データの保有期間の制限（第 25 条）

個人データの収集目的にとって、もはやそのデータの保有の必要性がなくなった場合、又は、法的若しくは企業目的にとってデータ保有の必要性がなくなった場合には、その組織は、当該個人データに対して削除などの措置をとらなければならない。

(b) 個人データの第三国移転禁止（第 26 条）

個人データ保護法と同等の個人データ保護レベルが存在しない国への個人データの移転を禁止している。

なお、第三国がシンガポール法制と同レベルにあるか否かの判断は、事業者自身が行うことになるが、それが事業者の負担となるようにも思われる。この点について、アモス氏は、次のように説明して、これを否定している。「事業者が相手国の立法に熟知していなかった場合、データの移転先の事業者との間で、データ保護に関する契約を締結すればデータ移転が可能であり、このような契約締結に要する時間や費用は、たいしたものではないため、事業者にとって過大な負担とはならない」。

(c) 迷惑電話禁止登録制度（Do Not Call Registry）（第９章）

データ保護委員会は、シンガポールの電話番号を保有、維持するひとつ以上の登録機関（迷惑電話禁止登録機関）を設けるものとする（第 39 条第１項)。そして、電話加入者は、同委員会に対して、登録機関への電話番号の追加や除去を申し出ることができる（第 40 条第１項)。

同章の規定は、次の場合に、シンガポールの電話番号に対して送られる特定のメッセージ（specified message）に適用される（第 38 条)。

① 特定のメッセージが送られた際に、そのメッセージの送り手がシンガポールにいる場合
② 特定のメッセージがアクセスされた際に、そのメッセージの受け手がシンガポールにいる場合

特定のメッセージとは、営利内容を有することなどが要件とされており（第 37 条第１項）、こうしたメッセージを電話で送る者は、その前に、登録機関に電話番号がリストに掲載されているかについてなどについて確認しなければならず（第 43 条第１項）、これに違反した者は、10,000 ドル以下の罰金刑が科される。さらに、原則として、こうしたメッセージをシンガポールの電話番号に対して送ってはならず（第 44 条第１項）、身元を隠す行為や隠すような行為もしてはならない（第 45 条第１項）。これらの規定に違反した者も、10,000 ドル以下の罰金に処される（第 44 条第２項、第 45 条第２項）。もっとも、調査目的など非営利の電話に対しては、こうした規制の対象とならない。

なお、迷惑電話禁止に関する規定は、B to C のみ規制対象としており、B to B は規制の対象とならない。さらに、同法の他の規定とは異なり、この規定のみ、公的機関もその規制の対象となる。公的機関が、営利目的で一般人に電話をかけるということは通常ないと考えられるが、仮にそのようなことがあった場合、規制の対象となる。

(3) 監督機関

a　制度の概要

(a)　法的地位及び所掌事務

第５条第１項では、3 人以上 16 人以下のメンバーによって構成される個人データ保護委員会（Personal Data Protection Commission）の設立が求められている。

ディレクターのアモス氏は、この組織の地位について、次のように述べている。「シンガポールは小国なので、国家組織は極めて単純であり、閣僚レベルの組織とその下部組織の２段階に分かれているにすぎず、データ保護委員会は、情報コミュニケーション省の下部組織に位置している。このように、同委員会は、EU のデータ保護指令の求める独立した機関ではないが、シンガポールでは、国会や裁判所の個人情報についてまで、完全に独立したいずれの省も属さない機関が監視するという機関を設けることはできない」。

なお、アモス氏によれば、シンガポールは小国であるので、委員会における地位と他の役職とを委員会のメンバーの皆が併任しているが、この点に問題あるとは一般に考えられていないという。

(b)　組織体制

データ保護委員会は、委員長（Chairman）、副委員長（Deputy Chairman）、その他のメンバーで構成される。委員長は Leong Keng Thai 氏であり、その他５人のメンバーで構成されている。

大臣は、本法における同委員会の権限の遂行に関して同委員会に助言を行うため、１人又は複数の諮問委員を指名することができる（第７条第１項）。また、同委員会は、この諮問委員に助言を求めることができるが、その意見には拘束されない（第７条第２項）。

大臣は、官報における告知によって、運営機関（Administration Body）を指名することができる（第９条第１項）。その運営機関では、次のような活動を行うことができる。

① 同機関が適切と考える事柄又は大臣によって同機関に付託されたデータ保護委員会の管理、運営に関する事柄について、大臣に助言を行うこと
② 共同執行に関する合意（co-operation agreement）を含む、データ保護委員会のための合意を形成すること
③ データ保護委員会のための予算を確保し、同委員会に関連する取引や業務の説明、記録を管理すること
④ 大臣の要求するデータ保護委員会の事柄に関する報告書を提出すること
⑤ 求められる運営などの援助をデータ保護委員会に提供すること

この機関の委員長は、Liew Woon Yin 氏であり、その他７人のメンバーで構成されている。

(c) 人事制度

データ保護委員会の委員長と副委員長は、同委員会のメンバーから大臣が指名する（附則第１条第１項第１号）。副委員長は、委員長の指示に従い、第８条(4)を含む、本法で委員長が行使できるあらゆる権限を行使できる（同条同項第２号）。委員長、副委員長、その他のメンバーは、大臣が決定する期間に在職し、再任を妨げられない（同条第４項）。

大臣は、委員長、副委員長、その他のメンバーに対して、理由を付さずに、その指名を取り消すことができる（同条第３項）。

(d) 権限

第６条では、個人データ保護委員会の有する一般的な権限として、次の９つの事項が列挙されている。

① シンガポールにおけるデータ保護の意識を向上させること
② データ保護に関する相談、助言、技術、運営などの専門的サービスを提供すること
③ データ保護に関するあらゆる事項について政府に助言すること
④ データ保護に関する事柄について国際的に政府を代表すること

⑤ データ保護に関するセミナー、ワークショップ、シンポジウムを企画、実施すること及びそのような活動を行う他の機関を支援することを含む、データ保護に関する教育的活動について調査、研究、促進すること
⑥ 同委員会又は政府のために、諸外国のデータ保護機関、及び国際機関若しくは政府内の組織を含む他の機関と、データ保護の分野において、技術的な協力や交換をすること
⑦ 本法を所管し、執行すること
⑧ 他の法律によって同委員会に与えられた役割を果たすこと
⑨ 官報（Gazette）において出された命令によって、大臣が同委員会に対して認めた又は大臣から与えられた他の活動を行い、そのような役割を果たすこと

その他の具体的な権限としては、次のようなものがあげられる。

① 協力協定
データ保護委員会は、海外のデータ保護機関を含むデータ保護と協力協定を締結することができる（第 10 条）。
② ガイドライン
データ保護委員会は、本法の規定に関する同委員会の解釈を示唆する助言的なガイドライン文書を出すことができる（第 49 条第１項）。
③ 本法遵守の確保
データ保護委員会は、組織が第３章から第６章の規定に従わなかった場合、その遵守を確保するため、適切と考えられる命令を出すことができる（第 29 条第１項）。そして、具体的には、次のような命令を出すことができる（ただしこれに限られない。）（第 29 条第２項）。
- 本法に反して個人データを収集、利用又は開示することの禁止
- 本法に反して収集した個人情報の破壊
- 第 28 条第２項のもと出されたデータ保護委員会の指示に従うこと
- 100 万ドルを超えない範囲で、データ保護委員会が妥当と考える罰金を支払うこと

なお、データ保護委員会は、組織が本法を遵守しているかについて判断するため、苦情の申立て又は自身の判断によって、調査を実施することができる（第 50 条第１項）。そして、データ保護委員会は、妥当と考える人数の調査官などを氏名又は部局によって指名することができる（第８条第１項）。そして、同委員会は、条件や制限を明示することによって、本法におけるその権限の全部又は一部をその者に委任することができる（第８条第２項）。

2. 国際的なルールへの対応状況

個人データ保護法の法案を作成するに当たって参考とされた諸外国の立法について、アモス氏は次のように述べている。「個人データ保護法は、特にいずれかの国の立法に依拠して草案されたわけではない。同法が最も参考とした立法を強いて挙げるとすれば、カナダの個人情報保護法（PIPA）であるが、イギリス、香港、オーストラリア、ニュージーランド、EU など多くの法制度、APEC プライバシーフレームワーク、プライバシー保護と個人データの越境的流通に関する OECD ガイドラインなどの制度を参考にした。それゆえ、同法は、EU の法制度、OECD の法制度、APEC での取組のいずれか特定の法制度に依拠するものとはいえない」。

また、アモス氏は、EU の十分性審査について、次のように述べている。「シンガポールにとって、EU とのデータ移転との関係で大きな問題が生じているとまでは認識していないので、EU の十分性審査を受ける予定はない。シンガポールは小国であるし、EU との交渉は、APEC などを通じて、他の国と連携して行うのが良いと考えている」。

3. 参考：シンガポールについて（外務省基礎データより）

【一般事情】

1. 人口　　約 531 万人（うちシンガポール人・永住者は 382 万人）（2012 年９月末）
2. 面積　　約 716 平方キロメートル（東京 23 区と同程度）
3. 民族　　中華系 74%、マレー系 13%、インド系９％、その他３％
4. 言語　　国語はマレー語。公用語として英語、中国語、マレー語、タミール語

【政治体制・内政】

1. 政体　　立憲共和制（1965 年８月９日成立）（英連邦加盟）
2. 元首　　大統領（任期６年。トニー・タン現大統領は、2011 年９月、第７代大統領として就任）
3. 議会　　一院制。選出議員数 87（任期５年）
4. 内政　　リー首相は、14 年間首相を務めたゴー・チョクトン前首相（現名誉上級相）から 2004 年に政権を継承。建国以来、与党人民行動党（PAP）が圧倒的多数を維持しており（2011 年５月の総選挙においては、87 議席中、81 議席を獲得)、内政は安定している。

【経済】

1. 経済概況

   2010 年　急速にＶ字回復を続けており、通年で 14.8%の成長。

   2011 年　欧州債務危機の影響等により、通年で 5.2%と減速。

   2012 年　欧米を始めとする世界経済の停滞により、通年で 1.3%と落ち込んだ。

【二国間関係：対日貿易】

1. 2002 年 11 月に日本・シンガポール経済連携協定（JSEPA： 日本初の EPA)、2007 年９月に同協定改正議定書が発効
2. 貿易額（2011 年、財務省貿易統計　単位：10 億円）輸出：691　輸入：2,170
3. 主要品目　輸出入ともに、電子機器・電子部品が主要品目

ii. フィリピン

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

フィリピンのデータ保護を所管している主官庁は、科学技術省の情報コミュニケーション科学技術室（Information and Communications Technology Office, Department of Science and Technology）と貿易産業省の政策調査・電子商取引室（Office of Policy Research / E-Commerce Office, Department of Trade and Industry）であり、これらの省庁の担当者が国会議員に働きかけることによって、2012 年のデータ・プライバシー法の成立に至った。

現在、科学技術省の情報コミュニケーション科学技術室の副部長（Deputy Executive Director ）であるモンチト・B・イブラヒム（Monchito B. Ibrahim）氏によると、新法であるデータ・プライバシー法を制定する動機は、次のようなものであったという。

① フィリピンはデータ処理の委託先として多くのデータが入ってくる。そのため、それらのデータを保護するよう委託元の事業者や国から要望があった。
② 市民、とりわけ、インターネットを利用する市民から、データ保護の要請があった。
③ 発展途上国として、先進国に遅れをとらず、この分野で一気に先進国の仲間入りをしたかった。

同法の制定に至っては、2011 年に下院で同法の草案が通過し、その後、上院でも、同年にその草案が通過したが、その上院で通過した草案は、下院のそれとは異なるものであった。そこで、両院で通過した草案の内容を調整するため、両院協議会（bicameral conference committee）が開かれ、2012 年８月に同法が成立した。現在までのところ、同法は施行されていない。よって、国家プライバシー委員会も創設されていない。

(2) 個人情報保護法制の概要

a 法律名

政府及び民間部門の情報及びコミュニケーション装置における個々の個人情報の保護とその目的やその他の目的のための国家プライバシー委員会の創設に関する法律（An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes）である。

短い名称は、「2012 年データ・プライバシー法」（Data Privacy Act of 2012）である。

b 目的

法律名に記載のとおり。

c 適用範囲

データ・プライバシー法は、あらゆる種類の個人情報の処理、個人情報の処理にかかわるいかなる自然人や司法人（juridical person）に対して適用され、後者については、フィリピンに存在しない情報管理者や情報処理者であっても、フィリピンに存在する設備を利用又はフィリピンに存在するオフィス、支店若しくは代理店を保持している者も含む（第４条第１項）。

また、次の場合にも、本法の適用があると定められている（第６条）。

① フィリピン市民又は住民に関する個人情報に関する行為、業務、処理
② フィリピンと関係を有する個人情報処理主体（the entity）であり、その主体がフィリピンにおいて個人情報を処理する場合、又は、その処理がフィリピンの域外でなされる場合であっても、フィリピン市民若しくは住民に関する個人情報を扱う場合
③ その他フィリピンと関係を有する個人情報処理主体

個人情報とは、物理的に記録されているか否かにかかわらず、個人のアイデンティティが明らかである情報、若しくは、当該情報を保有する主体によって合理的かつ直接にそのアイデンティティを確認できる情報、または、他の情報と合わせた場合に直接的かつ確実にその個人が識別できる情報を指すと定義されている（第３条(g)）。

なお、センシティヴ個人情報と特別扱いの情報（privileged information とは、Rides of Court と他の適切な法のもとで特別扱いの情報伝達と規定されているあらゆる形態のデータを指す（第３条(k)））については、第 13 条において限定列挙された場合にのみ処理できることが定められている。また、政府が保有するセンシティヴ個人情報の安全性確保については、第 22 条～第 24 条で別途、特別な定めをおいている。

d 適用除外

法第４条第２項では、本法の適用除外について、次の 7 つの項目をあげている。

① 公務員に関する情報のうち、その者の地位や権限に関する情報
② 政府機関の仕事を請け負い、その事業を行う個人に関する情報
③ 政府から個人に与えられる特許のような財産的な性格を有する裁量的利益付与に関する情報
④ 取材、芸術、文学又は調査の目的のために処理された個人情報
⑤ 公的機関の権限を行使するために必要な情報

⑥ 独立した中央の銀行組織の所管のもと、銀行やその他の金融機関が法を遵守するために必要な情報
⑦ 管轄外国法に従いその国の居住者から個人情報を収集した個人情報がフィリピンで処理された場合

また、新聞、雑誌、一般的に出回っている定期機関紙の出版社、編集者、レポーターに対して与えられている保護、すなわち、それらの者の信用にかかわる上記の出版物に記載されている情報の情報源の暴露を強要されないという保護について定める共和国法（Republic Act）第 53 条が修正、破棄されるように本法を解釈してはならないとの規定がおかれている（第５条)。

さらに、データ主体の権利に関する規定（第 16 条～第 18 条）は、処理された個人情報が、科学的、統計的な調査のためのみ利用され、データ主体に関していかなる行為や決定もされない場合、又は、データ主体の犯罪、行政若しくは納税責任に関する調査目的で収集された個人情報が処理される場合には、本法は適用されないとの規定がおかれている（第 19 条)。

e 権利・義務の内容

データ主体は、第 16 条において、次の６つの権利を有すると定められている。

① 自己に関する個人情報が存在する又は処理されているか否かについて、情報提供を受けること
② 個人情報が個人情報管理者によって処理される前又は次の実践できる機会に、以下の事項に関する情報の提供を受けること
  (i) システムに加えられる個人情報の詳細
  (ii) 個人情報が処理されている又は処理される予定の目的
  (iii) 個人情報が処理される範囲と方法
  (iv) 個人情報が開示される相手方又はその集団
  (v) 機械化されたアクセスのために利用する方法がデータ主体によって認められている場合に、その方法とそのようなアクセス権限が与えられている範囲
  (vi) 個人情報管理者とその代理人の身元と連絡先の詳細
  (vii) 個人情報が保有される期間
  (viii) プライバシー委員会に苦情を申し立てる権利を含む、アクセス、訂正などに関する権利の存在
③ 求めに応じて、以下の事項に関する合理的なアクセスを確保してもらうこと
  (i) 処理された個人情報の内容

(ii) 個人情報の入手源
(iii) 個人情報の受領者の氏名及び住所
(iv) 個人情報が処理された方法
(v) 個人情報が開示された理由
(vi) 自動化された処理に基づく個人データが、データ主体に相当程度影響している又は将来影響する単独の決定の根拠となる可能性が高い場合において、その情報
(vii) 個人情報が最後にアクセスされた又は修正された日付
(viii) 個人情報管理者の指名、氏名、身元、住所

④ 不正確又は誤った個人情報に異議を申立て、個人情報管理者に対して、直ちにその異議に従った形で訂正させること、ただし、その要求が悪意に満ちたもの、その他不合理である場合を除く
⑤ 個人情報が不完全、期限切れ、虚偽、違法に取得されたもの、無権限の目的で利用されているものである場合、又は、収集目的にとってもはや不要なものであることが判明し、その実質的な証拠が存在する場合に、その個人情報を個人情報管理者のファイル・システムから停止、消去、ブロッキングを命令、除去又は破壊すること
⑥ 不正確、不完全、期限切れ、虚偽、違法取得、無権限による個人情報の利用によって生じた損害の賠償を受けること

また、第 17 条では、データ主体の権利の譲渡について定めている。そこでは、データ主体の死後又は前条に列挙された権利を行使できなくなった場合に、正当な相続人や譲受人が、その権利を行使できるとされている。

さらに、第 18 条では、個人情報が、電子的な手段によって体系化され一般的に利用されているフォーマットで処理されている場合に、データ主体がそのデータを個人情報管理者から取得する権利について定めている。

f 届出・登録制度

存在しない。

g 苦情処理制度

第 16 条(b)(8)にあるように、データ主体は、プライバシー委員会に苦情を申し立てることができる。

h 罰則

直罰規定をおいている点が特徴的である。プライバシー法の制定の起草メンバーであったモンチト氏は、この直罰規定の制定経緯を次のように説明している。「直罰規定は厳しすぎる。立法の審議では、まず、草案が下院を通過し、その後に上院を通過するという流れになる。両院において通過した草案の内容には、直罰規定がいずれにも入っていなかったものの、その他の点において異なる内容を含むものであった。その場合には、両院協議会が開かれ、そこで決められた内容が、最終的な法律の内容となるという制度にフィリピンではなっているのであるが、その段階になると、起草委員会は、一切関与できないということになっている。この両院協議会での審議の結果、プライバシー法に直罰規定が含まれていたため、我々にとっても唐突なことであり、非常に驚いた。現在、同規定を改正するように国会議員に働きかけているところである」。

具体的な罰則規定は次のとおりである。

① 個人情報及びセンシティヴ個人情報の無権限による処理（第 25 条）
データ主体の同意なしに又は本法などで認められていないにもかかわらず個人情報を処理した者は、1 年以上 3 年以下の懲役及び 50 万ペソ以上 200 万ペソ以下の罰金に処する。
その情報がセンシティヴ情報であった場合には、3 年以上 6 年以下の懲役及び 50 万ペソ以上 400 万ペソ以下の罰金に処する。

② 過失による個人情報及びセンシティヴ個人情報へのアクセス（第 26 条）
過失により個人情報にアクセスした者は、1 年以上 3 年以下の懲役及び 50 万ペソ以上 200 万ペソ以下の罰金に処する。
その情報が、センシティヴ情報であった場合には、3 年以上 6 年以下の懲役及び 50 万ペソ以上 400 万ペソ以下の罰金に処する。

③ 個人情報及びセンシティヴ個人情報の不適切な取扱い（第 27 条）
故意又は過失によって個人情報を一般人がアクセスできる場所に廃棄等した者又はその保管しているゴミ箱に入れた者は、6 月以上 2 年以下の懲役及び 10 万ペソ以上 50 万ペソ以下の罰金に処する。
その情報が、センシティヴなものであった場合には、1 年以上 3 年以下の懲役及び 10 万ペソ以上 100 万ペソ以下の罰金に処する。

④ 個人情報及びセンシティヴ個人情報の目的外利用（第 28 条）

データ主体によって又は本法などで認められていない目的で個人情報を処理した者は、１年６月以上５年以下の懲役及び 50 万ペソ以上 100 万ペソ以下の罰金に処する。
その処理が、センシティヴ個人情報の場合には、２年以上７年以下の懲役及び 50 万ペソ以上 200 万ペソ以下の罰金に処する。

⑤　故意による無権限アクセス（第 29 条）
データの秘密やデータ保護システムに違反し、個人情報が保管されているシステムに故意に侵入した者は、１年以上３年以下の懲役及び 50 万ペソ以上 200 万ペソ以下の罰金に処する。

⑥　センシティヴ個人情報保護違反の隠蔽（第 30 条）
データ保護違反及び第 20 条(f)に定める通知義務について知りつつも、そのデータ違反を故意又は過失によって隠蔽した者は、１年６月以上５年以下の懲役及び 50 万ペソ以上 100 万ペソ以下の罰金に処する。

⑦　害意による開示（第 31 条）
害意又は悪意をもって、許可なく又は虚偽の個人情報を開示した者は、１年６月以上５年以下の懲役及び 50 万ペソ以上 100 万ペソ以下の罰金に処する。

⑧　無権限による開示（第 32 条）
データ主体の同意なしに、前条の範囲外の個人データを第三者に提供した個人情報管理者などは、１年以上３年以下の懲役及び 50 万ペソ以上 100 万ペソ以下の罰金に処する。

⑨　複数の違法行為（第 33 条）
第 25 条から第 32 条に定める複数の違法行為があった場合、３年以上６年以下の懲役及び 100 万ペソ以上 500 万ペソ以下の罰金に処する。

⑩　責任の範囲（第 34 条）
違反行為者が法人、組合などの司法人であった場合、刑罰は責任を有する者に科す。また、裁判所は、本法によって認められている権利を停止又は剥奪することができる。違反行為者が外国人であった場合、本法に定める刑罰が科されるほか、その刑罰に服した後、強制送還される。違反行為者が公務員又は公に雇用されている者であり、かつ、その者が第 27 条と第 28 条に違反した場合、永久に又は一時的にその地位を失う。

⑪ 重大な違反行為（第 35 条）
少なくとも 100 以上の個人情報が違法行為によって害された場合には、各処罰規定で定められた最高刑を科する。

⑫ 公務員による違反行為（第 36 条）
違反行為をした者又は違反行為に対して責任を有する者が公務員であり、付加的にその資格剥奪の期間が定められている罪においては、２倍の刑期を科する。

⑬ 損害賠償
被害者への損害賠償は、新民法（New Civil Code）の規定に従う。

ｉ その他の特徴的な制度

(a) データ保護違反通知（data breach notification）（第 20 条(f)）

個人情報がアイデンティティ詐欺の被害にあったと考えられる状況においては、個人情報管理者は、プライバシー委員会と被害を受けたデータ主体に対して速やかに通知しなければならない。

(b) 政府の保有するセンシティヴ個人情報の保護（security）に関する特別規定（第７章）

政府機関が保有するセンシティヴ情報については、情報コミュニケーションの分野で認められており、かつ、プライバシー委員会が推奨するところに従い、もっとも妥当な水準を使い、できる限り、その保護を図らなければならない。また、各機関の長が、この求められている保護措置が図られているように確保すべき責任者であり、プライバシー委員会は、その遵守を監視しなければならず、最低水準を確保するために必要な措置を勧告できる（第 22 条）。

プライバシー委員会によって定められるガイドラインで認められている場合を除き、公務員は、政府の敷地内のオンラインの設備を通じてセンシティヴ情報にアクセスしてはならない。また、原則として、これらの情報が移転されてはならず、敷地外からアクセスされてもならない（第 23 条）。

1,000 以上のセンシティヴ個人情報へのアクセスする又はこうした情報を必要とするような契約を政府とする者は、個人情報処理制度について、プライバシー委員会に届出なければならない（第 24 条）。

(3) 監督機関

a　制度の概要

(a)　法的地位及び所掌事務

独立した機関である国家プライバシー委員会（The National Privacy Commission）は、本法の規定の実施を監督し、データ保護のために定められた国際水準を同国が遵守していることを確保するための機関である（第７条本文)。また、本委員会は、情報コミュニケーション科学技術省（Department of Information and Communications Technology）に付設されて（be attached to）いる（第９条第１項)。

モンチト氏は、同委員会の独立性について次のように述べている「フィリピンはコミッショナー制度を採っているが、それは、大統領府（the President Office）の下にある機関である。とはいえ、それは名目上のことといって良く、事実上は、コミッショナーが独立して活動できる。それゆえ、この大統領府が個人データを有する場合、コミッショナーはその権限を行使できると考えられている。プライバシー法では、大統領府の保有する個人データを規制の対象から外していないからである。フィリピンでは、大統領府から独立した組織を設立するためには憲法上の明文が必要であるため、そのような位置付けとして独立したプライバシー･コミッショナー制度を設けることはできなかった」。

(b)　組織体制

本委員会は、プライバシー・コミッショナーを長として、２人の副プライバシー･コミッショナー（Deputy Privacy Commissioner）で構成されている（第９条第１項)。副コミッショナーは、ひとりが、データ処理制度について職務を担当し、もうひとりが、政策と企画について職務を担当する（第９条第１項)。

本委員会は、事務局を設ける権限を有する。この事務局の構成員は、個人情報処理にかかわる政府機関で少なくとも５年務めた者でなければならない。こうした政府機関として、例えば、社会安全制度（Social Security System)、政府サービス保険制度（Government Service Insurance System)、土地交通事務局（Land Transportation Office)、国庫局（Bureau of Internal Revenue)、フィリピン健康保険法人（Philippine Health Insurance Corporation)、選挙委員会（Commission on Elections)、外務省（Department of Foreign Affairs)、法務省（Department of Justice)、フィリピン郵便法人（Philippine Postal Corporation）などがあげられる（第 10 条)。

(c)　人事制度

プライバシー・コミッショナーと副コミッショナーは、フィリピンの大統領から３年の任期で任命され、３年の任期で再任されることがある。

プライバシー・コミッショナーは、35 歳以上でなければならず、清廉潔白、疑いなく高潔、誠実で知られた人物であり、かつ、データ・プライバシー及び情報技術分野で著

名な専門家でなければならない（第９条第２項）。なお、プライバシー・コミッショナーは、長官級（Secretary）の待遇を受ける（第９条第２項）。

副コミッショナーは、データ・プライバシー及び情報技術分野における著名な専門家でなければならず、次官級（Undersecretary）の待遇を受ける（第９条第３項）。

(d) 予算

同委員会は、初年度の予算として 2,000 万ペソが国庫から付与される（＝およそ 5,600 万円、１ペソ＝2.8 円で換算）（第 41 条）。

(e) 権限

第７条では、国家プライバシー委員会の権限として、次の 17 の事項が列挙されている。

① 個人情報管理者が本法の規定を遵守するように確保すること
② 苦情受付、調査の実施、苦情処理の促進などを行うこと
③ 個人情報の処理が国家の安全や公共の利益に害悪を与えると判明した場合、停止命令を出し、一時的又は永続的なその情報処理の禁止を課すこと
④ 組織、政府機関又はその補助機関（instrumentality）に対して、データ・プライバシーに影響する事柄について、同委員会の命令に従うよう若しくは措置をとるよう強制、請願すること
⑤ 政府機関が、セキュリティや技術的な措置に関して遵守しているかについて監視し、本法が求める個人情報保護の最低基準を確保するために必要な措置をとるようを勧告すること
⑥ 本国における個人情報保護を強化するための計画や施策を作成、実施する試みについて、他の政府機関や民間組織と調整すること
⑦ データ保護に関連するあらゆる法律に関する案内を定期的に発行すること
⑧ 索引や他の検索の手助けとなるものを含む、記録や通知に関する制度をまとめたものを発行すること
⑨ 司法省（Department of Justice）に対して、本法第 25 条から第 29 条で列記された罰則を科すよう推奨すること
⑩ 個人情報管理者（personal information controller）によって自発的に付されたプライバシー規則について審査、承認、拒否又は修正要請を行うこと
⑪ 国家や地方機関、民間団体や個人からの要請にもとづいて、プライバシーやデータ保護に関連する事柄について援助を提供すること
⑫ 提案された国家や地方の制定法、規則や手続におけるデータ・プライバシーの意味についてコメントすること、助言的な意見を出すこと、本法や他のデータ・プライバシー法の規定を解釈すること

⑬ プライバシー又はデータ保護に関するフィリピンの法律に対して、必要に応じて、立法、改正、修正を提案すること
⑭ 他国のデータ・プライバシー規制、プライバシー執行機関と適切で効果的な調整を図ること、データ・プライバシー保護のための国際的、地域的取組に参加すること
⑮ 他国のデータ・プライバシー執行機関と互いのプライバシー法の越境的交渉適用や執行に関して交渉し、契約を締結すること
⑯ 外国のプライバシー又はデータの保護に関する法律や規則に応じて、フィリピン企業が外国で事業を行う手助けをすること
⑰ 必要に応じて、データ・プライバシー保護の越境的執行を促進するような行為を全般的に行うこと

(f) 他機関・地方との関係

コミッショナー・オフィスの所管は、民間のみならずあらゆる公的機関全般に及んでいる。それゆえ、他の国家機関か地方公共団体かを問わず、コミッショナーは、その個人情報の取扱いを監視することとなっている。

2. 国際的なルールへの対応状況

モンチト氏によれば、プライバシー法を草案するに当たって、文言は、イギリスの制度の影響を受けているが、具体的な制度内容については、オーストラリアとアメリカから専門家に来てもらい、様々な助言を得て草案が作られたため、これらの国々の影響を大きく受けているという。とすれば、オーストラリアとアメリカは、APEC の加盟エコノミーであるから、フィリピンの制度は、APEC の制度と適合的なものということはできるであろう。

なお、モンチト氏は、EU の個人データ保護制度との関係について、次のように述べている。「EU のように、ひとつの定型的なプライバシー制度を他国に対して求めるのは妥当でないと考えている。法制度はそれぞれの国の文化的背景を反映したものであり、それぞれの国で執行可能なプライバシー法制度が構築されるべきである。日本もフィリピンも、固有の法制度を有していることからも、このことは明らかである。また、フィリピンだけで EU の十分性審査に関して交渉するよりも、AEPC のような組織において多くの国と協力して EU との妥協点を見いだす方が生産的であると考えている。そもそも、フィリピンだけで EU のドアをノックしても、アメリカ合衆国のような大国の力があるわけでもないから、十分性の審査が通らないと見込まれる場合に、セーフ・ハーバーのような協定を締結できる力もない。さらに、実際には、産業界からも EU の十分性審査を受けるに求める要望は出されていない」。

3. 参考：フィリピンについて（外務省基礎データより）

【一般事情】

1. 人口　　約 9,401 万人（2010 年推定値、フィリピン国勢調査）
2. 面積　　299,404 平方キロメートル（日本の約８割）。7,109 の島々がある。
3. 首都　　マニラ（首都圏人口約 1,155 万人）
4. 民族　　マレー系が主体。ほかに中国系、スペイン系及びこれらとの混血並びに少数民族がいる。
5. 言語　　国語はフィリピノ語、公用語はフィリピノ語及び英語。80 前後の言語がある。

【政治体制・内政】

1. 政体　　立憲共和制
2. 元首　　ベニグノ・アキノ　３世大統領
3. 議会　　上・下二院制
   上院 24 議席（任期６年、連続三選禁止。 現在、１名欠員）
   下院（最大で）291 議席（うち、小選挙区は 233 議席、政党リスト制は最大で 58 議席。任期３年、連続四選禁止）
4. 内政　　2010 年５月 10 日の大統領選挙で故コラソン・アキノ大統領の長男であるベニグノ・アキノ３世上院議員（当時）が当選。2010 年６月 30 日にアキノ政権が発足した。アキノ大統領は、汚職・腐敗の撲滅への決意を表明し、アロヨ前大統領を痛烈に批判。また、ミンダナオ和平及び治安の強化も政権の重要政策として掲げている。

【経済】

1. 主要貿易相手国
   輸出：日本（18.4%）、米国（14.7%）、中国（12.9%）、シンガポール（8.9%）、香港（7.7%）
   輸入：日本（10.8%）、米国（10.8%）、中国（10.1%）、シンガポール（8.1%）、韓国（7.3%）

【二国間関係：対日貿易】

1. 貿易額（2011 年、財務省貿易統計）
   フィリピンへの輸出（億円）：8,941、フィリピンからの輸入（億円）：7,121
2. 主要品目
   輸出：機械機器、金属品、化学品
   輸入：機械機器、食料品及び動植物生産品、金属原料

iii. 香港

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

個人情報保護に対する国民の意識の高まり、及び、EU データ保護指令等のデータ保護法を有する他国の条件を満たすことにより、香港への個人データの自由な流入を確保し、電子商取引などのネットワークを通じたビジネスにおける香港の競争力を確立することを目指して、1996 年 12 月に「個人データ（プライバシー）条例」が施行された。この条例は東アジアで初の個人情報保護に関する法律となった。その後、急速に進んだ情報技術とそれによって加速された電子的商取引の発展、頻発した数々の個人情報漏えい、2010 年のオクトパスカード事件、等を契機に、人々の個人情報保護に関する関心がさらに高まっていった。諸外国において個人情報保護規則の見直しが行われる中、香港においても 1996 年条例の見直しの必要性が認識され、2006 年 6 月より包括的な見直し作業を行うワーキンググループが組織された。2009 年、2010 年の政府によるパブリック・コンサルテーションを経て、2012 年夏に条例改訂法案が議会を通過、その後間もない 2012 年 10 月 1 日、「個人データ（プライバシー）（改訂）条例」が施行された。

(2) 個人情報保護法制の概要

a 法律名

「個人データ（プライバシー）条例」　（1996 年 12 月 20 日施行）
「個人データ（プライバシー）（改訂）条例」（2012 年 10 月 1 日施行）

b 目的

個人情報に関連して個人のプライバシーを保護することを目的に制定。また、1995 年 7 月に EU が採択した「EU データ保護指令（Directive 95/46/EC）」への対応も意図している。

c 適用範囲

個人データ（プライバシー）条例は、公的部門と民間部門を包括的に規制している（第３条）。この法律で保護される「個人情報」とは「生存している個人に関する情報で、直接又は間接的にその個人を確認できる情報」を指す。例えば、名前、電話番号、住所、年齢、性別、職業、既婚/未婚、給与、経済状況、国籍、写真、ID カード番号、医療カルテ、雇用情報、などは全て個人情報として扱われる。また、個人に関する意見も含むため、人事評価なども個人情報である。情報の形態は問わず、書類やテープ、コンピュータに保存したものなど全てを含む。

d 適用除外

次の場合には条例の適用は除外される（第８条)。

個人情報が：

—裁判所の業務で使用される場合

—個人情報が個人、家族、家庭内で使用される場合

—企業の人員計画で使用される場合

—国の安全保障、防衛、国際関係の目的で使用される場合

—犯罪捜査で使用される場合

—身体上、精神上の治療時に使用される場合

—未成年者の保護の為使用される場合

—報道活動で扱われる場合

—統計、調査で使用される個人情報

—胎芽の生体に関する情報

—デューディリジェンス活動での情報　等

e 権利・義務の内容

条例ではデータ使用者（Data User）とデータ主体（Data Subject）を次のように定義している。

- データ使用者：データを収集、保持、処理、あるいは使用する個人、会社、政府部局、その他の公共組織
- データ主体：当該情報の持ち主である個人

① 個人データ（プライバシー）条例では、OECD８原則に沿った次の６原則が謳われている。

原則１：個人データ収集の目的と方法

個人情報はデータ使用者の活動に直接関連性のある目的のために、法令に基づいた方法で収集され、データ主体者はそのデータ収集の目的及び用途を知らされねばならない。

原則２：個人データの正確性と保有期間

個人情報は正確性を確保されねばならず、また、使用の目的が完了した後は、ただちに消去されねばならない。

原則３：個人データの利用

データ主体の事前承認が得られる場合を除いて、個人情報はそれが収集された当初の目的以外に使用されてはならない。

原則４：個人データの安全保護

個人情報は違法なアクセス、処理、消去を受けないよう、保護されねばならない。

原則５：情報の一般開示

個人情報に関する方針、ルールが規定され、開示されなければならない。

原則６：個人データへのアクセス

個人は自分の個人情報へのアクセス及び、それが間違っている場合は修正する権利を有する。データ使用者はデータ主体者からの情報へのアクセス、あるいは修正の要求に応じなければならない。

② 条例により、データ主体には次の権利が保障されている。

- 個人情報が合法的な目的のために正しく収集されること。
- 自分の個人情報がどのように使用されるかを知ることができること。
- 個人情報の中の必要な情報だけ提供できること。
- 個人情報が正確にかつ安全に保持されること。
- 個人情報に自由にアクセスできること。
- 個人情報を訂正できること。
- 個人情報に関する制度・ルールがあまねく公開されること。

f 届出・登録制度

個人データ（プライバシー）条例はデータ使用者に対し、報告書（Data User Returns）の提出を規定している（第４章）。報告書には下記の情報が記載され、登録後、ネット上で一般公開される：

- データ使用者の名称、住所
- 収集される個人データの種類
- 収集の目的
- データの開示先の情報
- 海外への転送先情報、等。

この規定は EU データ保護指令の「第 18 条　監視機関に通知する義務」を参照している。香港においては、段階的に施行され、始めは、公的機関、銀行、保険、通信業界、大規模なデータベースを保持する組織、等に対して適用される予定であった。しかしながら、本規定は、1996 年に制定されたものの、2013 年３月現在、まだ発効されていない。2011 年に公的機関、銀行、通信、保険、の業界に対しコンサルテーションが行われたが、多くの懸念が寄せられた。また、現在 EU がデータ保護指令の見直しを行っていることも勘案し、本規定は EU での状況が明確になるまで棚上げとなっている。

g 苦情処理制度

データ主体から上げられた苦情について、下記の手順で処理が行われる（図３－１参照)。

① 監督機関による苦情受付（第 37 条）

告訴人は所定の書式に自己の名前、連絡先、被告人の情報、苦情の内容を中国語又は英語で記入し、監督機関である個人データ・プライバシー・コミッショナー事務所（PCPD）宛てに提出する。

② 調査停止の判断（第 39 条）

PCPD は告訴人からの苦情内容を吟味し、正式調査の必要性がないと判断した場合は、告訴人にその旨を通知する。(いやがらせ、私怨、個人情報保護に無関係、両者で和解できる、等)

③ 調査（第 43 条、第 44 条、第 45 条、第 46 条）

PCPD の持つ権限（必要書類の提出、面談、喚問、等）を行使して、詳細な調査が行われる。PCPD 調査への非協力は犯罪とみなされる。調査途中での情報は非公開となる。

④ 執行通知の発行（第 50 条）

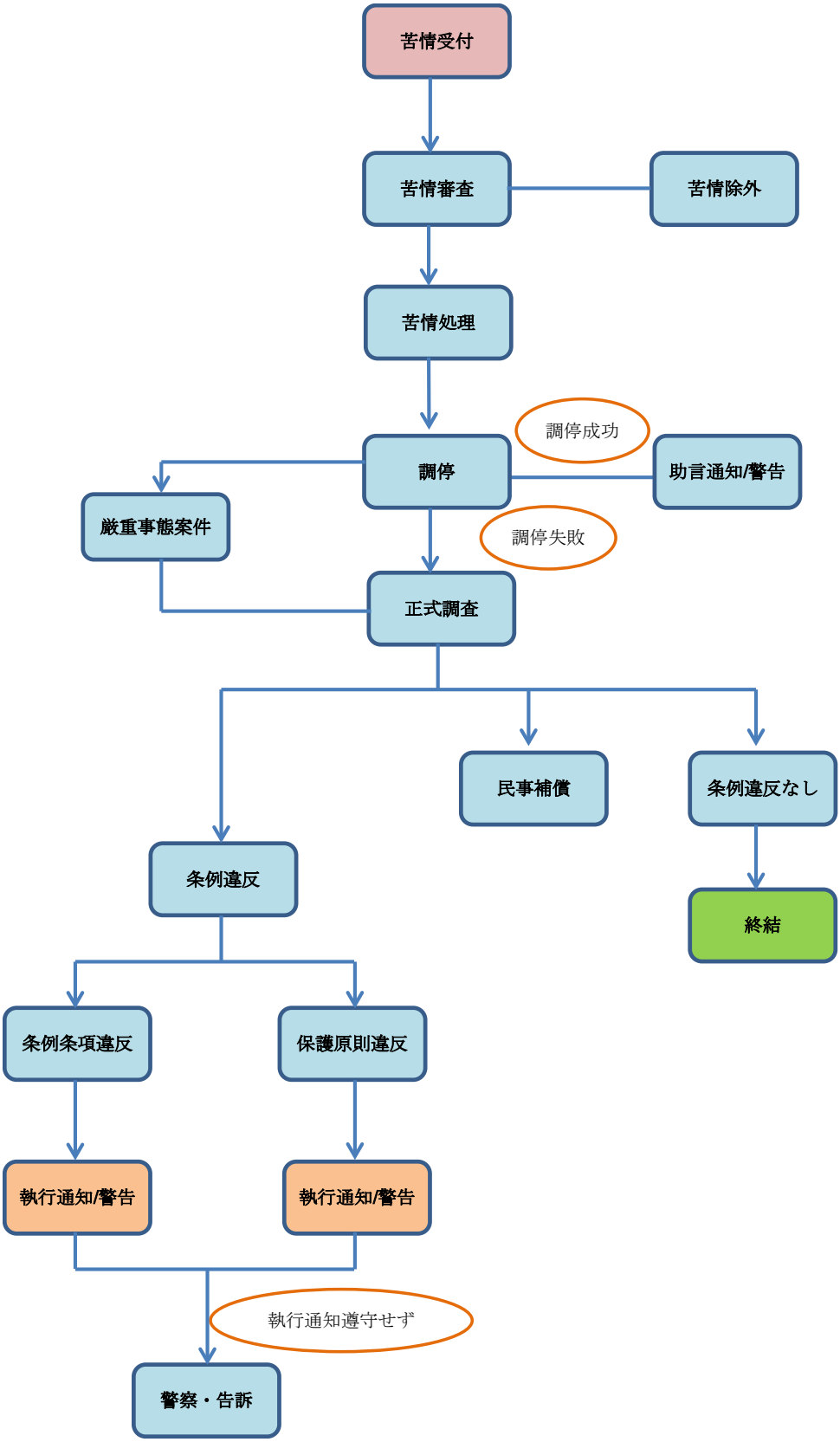
調査の結果、データ使用者の条例違反が明らかになり、違反が再発、継続する可能性がある場合は、違反行為の矯正を求める執行通知をデータ使用者に対して発行する。執行通知に従わない場合は犯罪となり、罰金と禁固刑が科せられる。

⑤ PCPD 決定への上訴（第 39 条、第 47 条）

告訴人の訴えに対し、PCPD が調査の不必要、停止を決定した場合、告訴人は、行政上訴委員会に対し上訴することができる。

⑥ 法務相談（第 66 条）

データ使用者の条例違反により被害を受けたデータ主体は、データ使用者に対して賠償金要求できる。PCPD はデータ主体に対し、法務相談サービスを提供する。


苦情受付
苦情審査
苦情除外
苦情処理
調停成功
調停
助言通知/警告
厳重事態案件
調停失敗
正式調査
民事補償
条例違反なし
条例違反
終結
条例条項違反
保護原則違反
執行通知/警告
執行通知/警告
執行通知遵守せず
警察・告訴

【図３－１　苦情処理手順】

h 行政措置・罰則

本人の同意を得ずに個人情報を第三者に販売したり、提供・公表により利益を得た場合は、最大で罰金 100 万香港ドルと禁固５年を科す。

個人情報をダイレクトマーケティングに利用する際の違反に対しては、最大で罰金 50 万香港ドルと禁固３年間を科す。

PCPD による改善命令（執行通知）にも関わらず違反行為を繰り返す行為にも実刑が設けられている。違反者には最大で罰金 10 万香港ドルと禁固２年間が科される。

i その他

- 第三国移転条項

  条例では、以下の場合を除いて、海外への個人情報の移転を禁止している（第 33 条）。

  - 移転国が香港の条例に比して同等の法を有している場合。
  - データ主体が移転について、書面で同意している場合。
  - データ使用者が、移転がデータ主体の利益になると信じる場合。

  ただし、本条項は 2013 年３月時点でまだ施行されておらず、海外への個人データの移転は制限されていない。

- 2012 年改正

  個人データ（プライバシー）条例の施行（1996 年 12 月）から 10 年以上が経過し、その間の情報技術の進展や国際的プライバシー標準の発展に伴い、アップデートが必要となった。2006 年から改正の検討が行われ、2012 年６月に改正法が制定された。

  主な改正点は以下の通り。

  ① ダイレクトマーケティングにおける個人情報使用の管理強化

  1996 年施行の条例にもダイレクトマーケティングにおける個人データ使用に関する規定があったが（第 34 条）、改正法では、管理が大幅に強化された（第 VIA 章が新規追加）。

  - データ使用者は、個人情報をダイレクトマーケティングで使用する際、データ主体から同意を得なければならず、また、データ主体に対し、使用されるデータの種類、使用される用途、移転経路、等を書面あるいは分かりやすく口頭で通知しなければならない。
  - データ使用者は、データ主体の書面での同意なしに、ダイレクトマーケティング使用を目的として他者に移転してはならない。
  - 違反者は最高 100 万香港ドルの罰金と５年の禁固刑

② データ主体の同意なしに獲得された個人情報開示違反
データ主体の同意なしに収集された個人情報を営利目的で開示することは違法。（罰金 100 万香港ドル＋禁固５年）

③ 個人への法務相談サービス
違法な個人情報漏えいの被害者に対する法務相談サービス提供。同条例第 66 条に基づく補償金の請求を後押しすることで、違反行為への抑止力とする狙い。

④ プライバシー・コミッショナーの権限強化
旧条例ではデータ使用者の違反行為に対し、プライバシー・コミッショナーが執行通知を発行し、矯正を要求することが規定されている。しかしながら、データ使用者の違反行為が停止したり、再発の可能性がないと考えられる場合は、執行通知は発行できない。改訂条例では、違反行為の継続、再発にかかわらずプライバシー・コミッショナーは執行通知を発行できることになった（第 50 条）。

旧条例では、違反行為を犯したデータ使用者は、コミッショナーからの執行通知を受け取っても、一定期間違反行為を停止したあと、再開することも可能で、再犯に対する罰則はなかった。改訂条例では、そのような意図的に再発・継続する違反に対して、５万香港ドル＋禁固２年（再犯のケース）、1000 香港ドル／日（継続のケース）の罰金を科している。

また、改訂条例では、違反の発生から起訴までの期間は、６か月（旧条例）から２年間に延長された。

上記改正条例は次の３つのフェーズで施行される。

a. 下記 b、c 以外の条項：2012 年 10 月１日より施行
b. ダイレクトマーケティングに関連する条項：2013 年４月１日より施行
c. 法的援助に関連する条項：別途公示

(3) 監督機関

a 設置の経緯

1996 年 12 月から施行された個人データ（プライバシー）条例に、本条例の履行の監視・監督を行う独立の監督機関として個人データ・プライバシー・コミッショナー事務所（PCPD）の設置が規定されている（第５条）。

b 制度の概要

(a) 法的地位

PCPD は政府に財政面などで依存しているものの、独立した活動を行っている。

(b) 所掌事務

PCPD の主な職務・権限としては下記が定められている。

- 個人データ（プライバシー）条例の履行の監視・監督
- 条例違反の疑いのあるケースに対する調査の実施
- 違反者に対する規定順守要請、強制通知の発行
- データ使用者から提出された報告書の検証、登録
- マッチングに関する審査・決定
- 条例の見直し
- 政府機関等の個人情報システムの検証
- 条例に関する市民の意識と理解の促進、実務ガイダンスの提供
- 個人情報保護についてのアンケート実施
- 国際組織との連携

(c) 組織体制

PCPD は下記の部署に分かれており、78 名のスタッフが勤務している（2013 年３月現在)。

- 行政部
- 法務部
- オペレーション部
- 法令監査部
- IT 部
- 広報部

(d) 人事制度

PCPD の長であるコミッショナーは香港行政長官から任命され、任期は５年間、再任は１回まで。

(e) 予算

FY2011 の収支は下記の通り。

収入： 55.9M 香港$（政府補助金、セミナー、出版、等）

支出： 54.2M 香港$（職員給与、家賃、その他アドミ費用）

収入の大半は政府からの補助金だが、個人情報保護法に関する有料セミナー、出版、会議、等からの収入もある。

(f) 権限

PCPD は次の権限を有する。

- 当該条例に対する市民の認識や理解を促進する。
- 当該条例を実務の上でいかに遵守すべきかの実務規則を認可、公表する。
- 情報使用者に対し個人情報を任意に確認する要望が出された場合、許可を行う
- 毎年申請書を提出すべき使用者の産業別リストを作成し、市民が登録書を通じて当該リストを調べ得る体制を整える。
- 個人情報システムを視察し、条例を遵守できる体制を普及させるべき提案を行う。
- 違法行為が生じた場合にはその状況を調査し、必要に応じてこれを当該情報の使用者に通告する。この通告に従わない場合、データ使用者は罰金と拘禁が課されることになる。

(g) その他

個人情報保護や条例執行に関する事項についてのコミッショナー諮問機関として個人情報諮問委員会が設けられている（第 11 条)。委員会はコミッショナーを委員長として政制及内地事務局長より任命される８名の委員から構成される。

2. 国際的なルールへの対応状況

(1) APEC-CPEA及びAPEC-CBPRへの対応状況

PCPD は APEC 加盟の主要国が参加する APEC Cross-Border Privacy Enforcement Arrangement (CPEA)の一員である。CPEA には 2013 年３月現在、22 機関が参加しており、メンバー間の情報共有、共同の法執行、案件調査、案件紹介などの越境協力を行っている。

PCPD は APEC ECSG (Electronic Commerce Steering Group)の下部組織である Data Privacy Subgroup に参加しており、APEC Cross Border Privacy Rules System (CBPR システム)のルールづくりに積極的に参画した。

CBPR システムは、APEC 加盟国における消費者と企業に信頼と利益をもたらすだけでなく、APEC 域内の経済発展と貿易を加速させ、個人情報保護に関する革新的な法体制の確立を助け、業務処理の負荷とコストの削減に大いに貢献することが期待されている。

米国とメキシコがすでに CBPR システムへの参加を表明しているが、香港 PCPD は現在検討中である。

(2) OECDプライバシーガイドライン改正、欧州評議会第 108 条約現代化、欧州一般データ保護規則提案への対応状況

OECD プライバシーガイドライン改正、欧州評議会第 108 条約現代化、欧州一般データ保護規則提案について、現在、PCPD は全てに対して動向を注視している。

(3) プライバシー・コミッショナー国際会議

PCPD はプライバシー・コミッショナー国際会議の正式メンバーである。インターネットやモバイル通信技術の進展により実現されたグローバルネットワークを通して、データが高速に地球規模で拡散していく今日の状況を鑑み、この会議では、文化、国境を超えた個人情報保護に向けた国際連携の必要性を提唱している。

(4) APPA

Asia Pacific Privacy Authorities (APPA) はアジア太平洋地域におけるプライバシー当局の集まるフォーラムであり、個人情報保護、新技術、苦情処理についての情報交換が行われている。加盟国はオーストラリア、カナダ、韓国、香港、マカオ、メキシコ、ニュージーランド及び米国。

香港 PCPD は APPA の中の Technology WG（TWG）の議長を 2010 年 6 月から務めており、クラウドコンピューティングにおける個人情報保護、グーグルのプライバシーポリシー変更についての明確化、等の議論を取りまとめた。

3. 個人情報保護に関する認証制度

認証制度はない。検討していない。

4. 個人情報保護の施行状況

(1) 苦情処理・紛争解決

PCPD は４つの受付デスクを設け、メール、電話、Fax、対面で、問合せ、苦情への応対を行っている。問合せ、最近の苦情処理件数の推移は下記の表のとおり。

	2011 年	2010 年	2009 年
問合せ件数	19,094	18,103	18,460
苦情処理件数	1,507	1,225	1,022

2011 年の苦情処理案件の内、訴えられた対象は民間企業（73%）、個人（17%）、公的機関（10%）。訴えられた民間企業の大半は通信事業者と金融機関で、違法な個人情報の開示が原因。公的機関への苦情は、警察、住宅、病院、娯楽/文化関連機関が多い。

(2) 権限行使（報告の徴収、勧告、命令、立入検査、罰則等）

PCPD が 2011～2012 に判断を下した案件のいくつかの例を下記に示す。

- メンバーシップ販売の OnCard 社が、過去の顧客に対し、顧客からの停止要請にもかかわらず、勧誘セールスの電話を繰り返した。OnCard 社は、条例第 34 条、第 64 条違反で 1,000 香港ドルの罰金が科せられた。

- Citibank が顧客に対し、停止要求にもかかわらず、ダイレクトメールを３年間にわたり送付し続けた。Citibank に対して条例第 34 条、第 64 条違反で 2,500 香港ドルの罰金が科せられた。

- Sudden Weekly、FACE Magazine の２つの出版社が３人の芸能人の個人情報を非合法的なやり方で入手し、写真を出版したとして苦情を申し立てられた。出版社２社は「公共の関心」を主張したが、PCPD は、２社の行為は個人情報の不正な収集であり、基本原則１に違反するとして、改善を求める執行通知を発行した。この執行通知に不服であるとして、２社は行政上訴委員会へ上訴した。本件は「報道の自由」と「プライバシーの権利」のバランスを問い正している。PCPD は政府によるフォローアップと関係者による意見を聞いたうえでの適切な法制度の導入を望んでいる。

- 駐車場管理会社であるインペリアル・パーキング社が、個人情報を虚偽の申請で交通省の車両登録から入手し、ダイレクトマーケティングに使用したとして、

苦情を申し立てられた。PCPD は基本原則３違反としてインペリアル・パーキング社に改善を警告した。

・ 施設管理会社の Hong Yip 社が、元従業員の個人情報を非合法に収集したとして苦情を申し立てられた。Hong Yip 社は職場に設置した監視カメラで元従業員の職務怠慢を発見し、それを理由に解雇していた。PCPD は、監視カメラによる従業員の監視は基本原則１違反に当たるとの判断を下し、プライバシー侵害の少ない方法での従業員管理を指示した。

・ Hang Seng 銀行が顧客の破産情報を正当な理由なしに長期間（99 年間）保持していた。PDPC は破産情報が８年で破棄されるべきであるとして、基本原則２、条例第 26 条への違反の判断を下した。Hang Seng 銀行は制度を改め８年以上の破産情報の保持をやめ、再発の可能性はないと判断されたため執行通知は発行されなかった。

(3) 広報啓発活動

PCPD は市民及び企業での個人情報プライバシーに関する意識向上を図るため下記の活動を行っている。

- 個人情報プライバシーに関する公的教育プログラム制作
- 条例についての個人向け／企業向けのセミナー実施
- 個人情報プライバシーについての出版、トレーニング資料制作
- メディアからの問合せ対応、プレスコンファレンス実施
- 中国語／英語でのウェブサイト掲載

(4) 今後の課題

PCPD として下記の課題を挙げている：

- 市民へのさらなる教育、意識向上
- 企業への働きかけ（Privacy by design）

システムの開発においてプロアクティブにプライバシー対策を考慮し、企画から保守段階までのシステムライフサイクルで一貫した取組を行う必要がある。

5. 参考：ガイダンス・ノート（概要）

PCPD の主要業務のひとつに市民への業務ガイダンスがある。すでに発行された「ガイダンス・ノート」の中からいくつか抜粋して概略を紹介する。

① 指紋情報の収集
② CCTV（監視カメラ）による監視
③ インターネットを介して行われる個人情報収集と使用
④ 施設管理における個人情報保護
⑤ 携帯型記憶装置の使用

① 指紋情報の収集

指紋情報の収集は犯罪捜査の中で行われてきたが、昨今は技術の進化、コスト低減により、指紋スキャナが入場者登録や施設への入退場アクセスとして一般に使われるようになった。同時にデータの不正使用によるプライバシー侵害という問題もクローズアップされている。

条例による「個人情報」の定義は「生存している個人に関する情報で、直接又は間接的にその個人を確認できる情報」となっている。指紋は個人を特定できる生体情報ではあるものの、一般人は指紋画像あるいは指紋データコードを見て個人を特定できるわけではない。しかしながら、画像あるいはデータコードを別のデータベースと照合することにより個人を特定することが可能となる。よって、指紋情報は個人情報と考えられる。

条例の基本原則１によると「個人情報はデータ使用者の直接的な目的のためにのみ合法的に収集されなければならない」。データ使用者は、この基本原則１にミートするため、指紋情報が、使用目的に本当に必要なのかどうかよく評価する必要がある。

「入場管理」「セキュリティ」は指紋情報収集目的としてよく使われるが、PCPD の見解は次の通り。

- 「入場管理」
  通常、個人によるサイン、あるいはアクセスカードが使用されている。この目的のため、指紋情報が必要とされるとは考えにくい。
- 「セキュリティ」
  入場が制限された場所へのアクセスとして指紋情報が使われることがあるが、パスワード、監視カメラを使用する方が、プライバシー侵害、コストがより少なくて済む。

大人数の指紋情報の収集の際には注意が必要である（漏えいの場合に被害が多大となる。）。例えば、社員全員の情報を収集するのではなく、アクセスを許可される社員のみの情報を収集、など。学校生徒の指紋情報収集には最大限の注意が必要とされる。

指紋情報を取得する際は、データ主体の書面による同意を得ることが望ましい。その際、データ主体が同意可能な精神能力を有しているか（例：小学生)、同意しなかった場合データ主体に不利が生じないか、検討されねばならない。

指紋情報の収集の際、データ使用者は、データ主体に次の事項を通知する必要がある。

- 指紋情報の提供は強制又は任意か
- 提供が強制の場合は、拒否した場合の影響
- 指紋情報の用途
- 誰が指紋情報にアクセスできるか
- 情報が他者へ移転される場合、誰に、何の目的で移転されるか
- 指紋情報がデータ主体にとって不利な情報として使用される可能性
- データ主体は情報へのアクセス、修正ができること。そのやり方

収集された指紋情報は厳重に管理されなければならず（アクセスは最小限に)、最初の目的以外に使用されてはならない。（基本原則３）

他の IT システムやデータベースとの不必要なリンクを防止しなくてはならない。

第三者への移転は通常行ってはならない。（除：犯罪調査目的）

データ使用者は必要な期間が終了したら指紋情報を消去しなければならない。（基本原則２）

データ使用者は、指紋情報を正確な状態に保つ必要がある。（基本原則２）

収集された指紋情報は、不正／事故的なアクセス／処理が発生しないようあらゆる手段を使って保護されねばならない。（基本原則４）

- 指紋情報を扱う IT システムの性能を定期的にチェックする
- 指紋情報を暗号化する
- 指紋情報データベースへのアクセスは強力なパスワードで行う
- 指紋情報データベースへのアクセスは限定者、限定端末とする
- データアクセスのログ管理
- データ端末を CCTV カメラで監視

② CCTV（監視カメラ）による監視

昨今、セキュリテイ目的のため公共の場所に CCTV を設置することが広く行われているが、個人情報保護の観点から問題も多い。

基本原則１が規定しているように、個人情報は合法的な方法により、データ使用者の直接的な目的のために、適度に収集されなければならない。CCTV の使用について、使用目的が正当化できるか、よりプライバシー侵害が少ない他の手段への代替は可能か、等が検討される必要がある。CCTV 設置に当たり、データ使用者は、次のステップを踏む必要がある。

- CCTV 設置の差し迫った必要性の検討

- CCTV によって解決される問題を明らかにする
- よりプライバシー侵害の少ない代替手段の有無の検討
- CCTV 設置で影響をうける人々への意見聴取
- CCTV 監視の計画、期間の決定

CCTV による監視が決定した後、考慮すべき事項として次がある。

- 設置場所
- CCTV カメラの性能（刑事裁判で被告の表情を記録するには高性能のカメラが必要だが、公道での人々の動きを把握するのに高性能カメラは必要ない。）

人々は CCTV で監視されていることを通知される必要がある。

基本原則４に規定されているように、データは不必要に長期間保持されてはならない。セキュリティ目的で録画された情報は、必要がない限り、定期的に消去する必要がある。また、情報の正確性を確保するため、情報は安全な場所に保管しなければならず、情報の移転がある場合は、記録されなければならない。

監視情報を無線で伝送するシステムの場合は、盗聴への十分な対策を施すことが求められる。

基本原則３により、データ主体の同意がない限り、記録された監視データは当初の目的以外に使用されてはならない（除：警察からの要請、等)。

基本原則５に基づき、データ使用者は、CCTV による監視についてのルールと手続きを作成し、データ主体に対し明確に通知しなければならない（誰が CCTV システムを操作し、どんな目的で、情報はいつまで保管されるか、等)。

③　インターネットを介して行われる個人情報収集と使用

民間企業、公共機関によるオンラインでのビジネス、サービス提供は今や当たり前になっている。オンラインでのビジネス、サービス事業者は次のことを考慮する必要がある。

基本原則１に規定されているように、不必要な情報を入手してはならない（例：ビジネスが成立していないのにクレジットカード、住所、性別、等の情報は必要ない)。

基本原則２の規定にある通り、個人情報は正確でなくてはならない。確認メールを、データ主体がインプットしたアドレスに送付した上で、本文メールを送付するといった「二重確認」システムが有効。収集された個人情報がいつまで保持されるかをデータ主体に伝え、必要な期間が過ぎたらデータが消去されるメカニズムも必要である。

収集された個人情報がインターネット上で開示される可能性がある場合は、その旨、データ主体に事前に通知される必要がある。匿名での情報開示は条例違反ではないので、匿名での開示が有効な場合もある（例：当選者発表)。

データ使用者はあらゆる手立てにより、個人情報の保全を確保しなければならない（基本原則４)。個人情報の包括的な保護のため、トップ・ダウンアプローチ、プライバ

シー・バイ・デザインアプローチがなされる必要がある。システムを構築した後で個人情報保護を考慮するのではなく、システムのフィージビリティ調査の段階から個人情報保護のコンセプトを盛り込む設計が必要である。

個人情報をオンラインで開示するサービス事業者は以下のような対策を講じる必要がある。

- データの暗号化
- 不法アクセス防止のため、アクセス制限する。
- パスワード管理の徹底
- ファイヤーウォールの適切な設置
- 情報へのアクセス先として予想可能な方法（例：シーケンシャル変数を使用した URL の利用）
- 非暗号化でのデータの転送が行われる際は、事前にデータ主体に対して通知を送付するメカニズムの構築

基本原則５はデータ使用者が、彼らのプライバシーポリシーを公開することを求めている。企業は、保有する個人データの種類、使用目的を記したプライバシー・ポリシー・ステートメントをホームページなどの分かりやすい場所に掲載することが求められている。

④　施設管理における個人情報保護

アパートの入居者、テナント、訪問者、等の個人情報は、オーナー企業、施設管理会社などにより管理されているが、これらの情報は条例に従って、適切に扱われなければならない。

施設に入場するための電子アクセスカード申請に当たり、入居者は施設管理者に対し、名前、部屋番号、連絡先電話番号、等の個人情報を提供する。施設管理者の中には、カードの不正使用に備え、入居者の ID カード番号まで要求するところもある。PCPD の判断では、ID カード申請に際しての ID カード情報の要求は、過剰な情報収集である。

施設を訪問するビジターに対し、セキュリティスタッフが入場に当たって ID カード番号を入場ログブックに記入させるところもある。この場合の ID カード番号情報の記録は過剰情報収集であり、プライバシー侵害の少ない他の方法、例えば、社員証、労働許可証、等の提示で代用すべきである。

共用エリアに CCTV カメラを設置し、個人の画像データを監視する場合は、カメラを使用しての監視がおこなわれていること及び監視の目的について通知、表示しなければならない。

施設の駐車場での車の盗難防止目的で、ドライバーの名前、ID カード番号を要求する施設もある。PCPD はこの行為はプライバシー侵害に当たり、基本原則１への違反にな

ると考える。盗難防止が目的であれば、他の手段、例えば、パトロール強化、監視カメラ導入、照明設置、等で対処すべきである。

施設管理者は、入居者からの苦情に対する処理に当たり、苦情に関連する情報を注意深く扱う必要がある。苦情処理の情報は他の目的に転用してはならない（基本原則３への違反となる。）。

施設入居者の個人情報がコンピュータに電子情報として保管される場合は、その情報へのアクセスは限定されたスタッフのみとする、暗号化する、パスワードでのコントロール、等、基本原則４に規定されている情報の保全が遵守されなければならない。

⑤　携帯型記憶装置の使用

USB フラッシュメモリー、ノート PC、ドライブ、等の携帯型記憶装置は便利なツールとして個人情報の保管、転送に多用されている。しかしながら、適正な保護制度と実践が行われないと問題を引き起こすおそれがある。

携帯型記憶装置は素早く、簡単に大量の個人情報をコピーできるため、盗難、紛失時には、大きな被害につながる。消去されたデータ、あるいは以前リフォーマットされたデータも復元できることも注意しなければならない。

携帯型記憶装置の使用が内包するリスク評価を行い、トップダウンアプローチにより、制度・ルールを定める必要がある。

携帯型記憶装置の盗難、紛失時に保管された個人情報を不正アクセスから保護するには暗号化が最も効果的である。

携帯型記憶装置の紛失時、速やかな報告と対処が情報漏えいのリスクを小さくする。

技術進化にあわせて、制度を定期的に更新していく必要がある。

6. 参考：香港について（外務省基礎データより）

【一般事情】

1. 人口　　約 717 万人（2013 年２月）
2. 面積　　1,103 平方キロメートル（東京都の約半分）
3. 民族　　漢民族（約 95%）
4. 言語　　広東語、英語、中国語（北京語）ほか

【政治体制・内政】

1. 政体　　中華人民共和国香港特別行政区
   （Hong Kong Special Administrative Region：SAR）
2. 元首　　習近平中国国家主席
3. 議会　　立法会（70 議席）
4. 内政　　中国返還（1997 年７月１日）に伴い香港が特別行政区（SAR）となって以来、「一国二制度」は基本的に順調に機能。

【経済】

1. 主要貿易相手国
   輸出：中国（47%）、日本（7.9%）、シンガポール（6.2%）
   輸入：中国（54%）、米国（9.8%）、日本（4.2%）
2. 経済概況
   コモンロー（英米法系）の透明な法制度や、簡素で低率の税制（法人税 16.5%、個人所得税最高税率 15%、キャピタルゲイン・利子非課税）などが香港経済の特徴であり、こうした制度的・社会的インフラを基礎として国際金融及び物流の拠点としての地位を築いている。

【二国間関係：対日貿易】

1. 貿易額（香港政府統計処）
   対日輸入　3,116 億香港ドル（401.3 億米ドル）
   対日輸出　1,439 億香港ドル（185.3 億米ドル）
2. 主要品目
   輸出　1)衣料、2)雑貨、3)電気・電子機器
   輸入　1)電気・電子機器、2)通信・音響機器、3)事務機器

iv. マカオ

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

ポルトガルにおける法制度の進展の影響を受け、マカオでは 1998 年ごろから法律に基づく個人情報保護の必要性が議論された。2005 年に８名の議員がポルトガル法をベースに、香港法も加味した個人情報保護法案を提出した。提出された法案は監督機関の設置についてポルトガル法、香港法とは異なっていた（マカオ基本法によると、この種の機能は政府が管轄している。）。その後、多くの協議を経て、法案は 2005 年８月に議会を通過し、2006 年２月から施行された。現在、法改正の動きはあるものの、具体的な進展はまだない。

(2) 個人情報保護法制の概要

a 法律名

「個人データ保護法」　2006 年２月施行

b 目的

個人情報の保護とその適正な「処理」* について規定する。

*「処理(process)」： 個人情報に対し、紙書類、電話、インターネット、ディスク、PC、マイクロフィルム、コピー等の手段を用いて、収集、記録、整理、収納、改造、変更、検索、問合せ、使用、移転、拡散、拒否、消去等の行為を行うこと。

c 用語定義

「個人データ保護法」の中で使用されている用語は下記のように定義されている：

- 個人情報（Personal data）：
  個人が本人であると確認できる全ての情報のこと。例えば、本屋で本を注文する際、自分の名前、本のタイトルを告げ、前金を支払ったとする。個人の名前、注文した本のタイトル、前金額、残金額、等の情報は個人情報である。なぜならば、ID カード番号は提供されていないものの、個人の名前だけで、個人の特定が可能になるからである。しかしながら、もし、個人の名前やその他の個人を特定する情報が提供されなかった場合、本のタイトル、前金額、残金額、等の情報は、個人情報ではない。
- データ主体（Data subject）：
  個人情報が処理される自然人を指す。個人情報の処理は多岐の分野に及ぶため、誰もがデータ主体になり得る。例えば、市場調査目的で電話番号を提供すると、それを提供した個人はすでにデータ主体である。

- データ管理者（Controller）：
  個人情報の処理について目的と手段を有する自然人、法人、公共機関、団体を指す。例えば、ホテルは、顧客の名前、ID 書類情報、部屋番号、ホテル内での消費状況、支払い手段、等を登録する。ホテルの経営者はこれらの登録情報を処理する際、その目的と手段を決定するので、「データ管理者」である。一方、ホテルの会計部門、あるいは IT 部門は目的と手段について権限を有しておらず、ホテル経営者側からの決定に従う。従って、彼ら（会計部門、IT 部門）はデータ管理者ではない。
- データ主体の同意（Data subject's consent）：
  データ主体が、本人の個人情報の処理を希望する旨を表示すること。

d 適用範囲

個人データ保護法は、公的部門と民間部門を包括的に規制している。対象となるのは電子的情報及びマニュアル処理情報の両方である。また、この法律はマカオに拠点を置くデータ管理者が行う行為、あるいはマカオ域内にあるデータコミュニケーションネットワークを使用して行われるビデオ監視などの個人を特定できる画像、音声を収集、処理、拡散させる行為についても適用される（第３条）。

e 適用除外

純粋に個人的ならびに家庭での私的用途での個人データ処理については適用されない（第３条）。例えば、親しい友達同士、家族、親戚内での写真、あるいはビデオの共有などには適用されない。

f 権利・義務の内容

- 基本原則（第２条）
  個人情報を処理する場合は、マカオ基本法で規定されているプライバシー、その他の基本的人権、自由、保障が十分尊重され、透明性の高い方法で行われなければならない。

個人情報の処理については次のように規定されている。（第５条）

- 個人情報は合法的に処理されなければならない。
- 個人情報はデータ管理者により特定、明示された合法的目的に沿って収集されなければならない。また、その目的はデータ管理者の活動に直接関係のあるものでなければならない。
- 個人情報は明示された収集／処理目的に合致、関連していなければならず、過剰であってはならない。
- 個人情報は正確で、アップデートされなければならない。
- 個人情報は当初の目的達成に必要な期間以上に保持されてはならない。

- データ管理者がデータ主体の個人情報を合法的に処理する際の条件は次のように規定されている（第６条）
  - データ主体から明らかな同意を得られた場合
  - データ主体が関わる契約の締結に個人情報の処理が必要であるとデータ主体が希望する場合
  - データ管理者が従うべき法的義務に対応する場合
  - データ主体が身体的あるいは法的理由により同意を与えることができないが、個人情報の処理がデータ主体の重要な利害に資する場合
  - 公共の利害に資する場合
  - データ主体の基本的人権、自由、保障に影響を及ぼさないデータ管理者の法的利害を遂行する場合

- センシティブデータの処理（第７条）
  - 個人情報の中で、センシティブデータ*の処理は禁止されている。
    *センシティブデータ：個人の哲学的信条、政治的信条、所属政党／団体、宗教、人種、出自、健康状態、遺伝子、等に関する情報
  - ただし、下記の場合はセンシティブデータの処理が許可される。
    - 明らかに法律により承認されている場合
    - 重要な公的利益の観点から、データ管理者の法的権利の行使の為に必要である場合
    - データ主体が明らかな同意をした場合
    - データ主体あるいは第三者の生命維持に必要だが、データ主体が身体的、法令的に同意できない場合
    - データ主体の同意の下、法務従事者による合法的活動、あるいは政治的、哲学的、宗教的、等の目的で団体の会員のみに関係し、データ主体の同意なしには第三者には開示されないという条件がある場合
    - データ主体により明らかに公開されている場合
    - 法的請求の行使、弁護に限って使用される場合
    - 専門医療スタッフにより、予防医療、医学診断、ヘルスケアサービスの提供、等の目的で使用される場合。

- 個人データ保護法はデータ主体の権利として下記を規定している。

① 情報を知る権利（第 10 条）

データ管理者は、直接的収集あるいは間接的収集を問わず、データ主体から得た個人情報について、データ主体に対し次の情報を提供しなければならない。

・　データ管理者の名前
・　データ使用の目的（例えば、市場調査、リクルート、顧客管理など）
・　個人情報が移転される場合の移転先の名前あるいは種類
・　アンケート調査の場合、回答は義務であるか、回答拒否できるか
・　データ主体が、提供した情報にアクセスしたり、必要な訂正を行うことができるか

② 情報へのアクセス・訂正の権利（第 11 条）

データ主体は、自分の提供した情報に対し、アクセスし、必要ならば訂正できる権利を有する。データ管理者は、データ主体からの要求に対し、下記の情報をタイムリーに、かつ低額で提供しなければならない。

・　個人情報が使用されたか否か
・　どんな目的で使用されたか
・　どの情報が使用されたか
・　どこに移転されたか
・　データ管理者は情報をどこから入手したか

③ 拒否する権利（第 12 条）

データ主体は、いつでもデータ管理者に対し個人情報の使用を停止することを要求できる。データ管理者はデータ主体からの要求が合法である限り、個人情報の使用を直ちにやめなければならない。また、個人情報がダイレクト・マーケティングやその他の商業調査に使用された場合、データ主体は、使用を停止するよう要求できる。

④ 賠償請求の権利（第 14 条）

データ管理者による個人情報の違法な処理により被害を受けたデータ主体は、データ管理者に対し賠償請求できる。

g 届出・登録制度

① 通知（Notification）

データ管理者は個人情報について下記の処理を行う場合は、処理の開始から 8 日以内に監督機関へ通知しなければならない。（第 21 条）

・　コンピュータによる自動処理
・　データ主体が身体的、あるいは法的な理由により同意を出すことができない状況においてデータ主体の重大な利害を保護するために行うセンシティブ情報（政治的信条的メンバーシップ、宗教、人種、健康、遺伝子等に関する情報）の処理
・　統計、歴史、科学調査等の目的での処理
・　データ主体の同意を得て、マカオと同等の保護レベルの法制度を有していない国・地域に対し個人情報を移転する場合

② 承認（Authorization）

データ管理者は個人情報について下記の処理を行う場合は、処理の開始前に監督機関へ相談し、事前の承認を得なければならない（第 22 条）。

- 重要な公共の利益にかかわるセンシティブ情報の処理
- データ主体のクレジット情報の処理
- データの照合処理
- 当初の目的とは異なった用途での処理
- データの保持期間を延長する場合
- マカオと同等の保護レベルの法制度を有していない国・地域に対し個人情報を移転する場合で、データ主体の同意はないものの、契約上で十分な保護を保障できる場合

通知・承認の内容は官報及びアニュアルレポートで公開される。通知・承認の制度は最初、公的機関、銀行等、大きな個人情報データベースを有するセクターを対象に適用され、その後、民間企業へも適用が広がった。

h 苦情処理制度

個人データ保護法の監督機関は下記の手順で苦情処理を行う。

① 苦情受付：立ち寄り、郵送、Fax、Email、電話により苦情受付
② 苦情申立者（データ主体）への事情聴取
③ データ使用者への調査
④ 監督機関による判断

データ管理者の違反行為により損害を被ったデータ主体は、データ管理者に対して民事訴訟をおこすことができる（第 14 条）。データ保護オフィス（OPDP）が行った苦情処理、調査は民事訴訟になんら影響を及ぼさない。

i 行政措置・罰則

- 行政罰

- 個人情報の処理についての通知を怠った場合や虚偽の報告を行った場合（第 32 条）：
  —自然人：MOP2,000～MOP20,000 の罰金
  —法律家あるいは法律家のいない組織：MOP10,000～MOP100,000
  （事前承認事項への違反は上記罰金が倍増）
- 基本原則（第 5 条、第 10 条、第 11 条、第 12 条、第 13 条、第 16 条、第 17 条、第 25 条）の不履行に対する罰金（第 32 条）： MOP4,000～MOP40,000
- センシティブ情報の処理、複数データの照合処理等にかかわる義務違反に対する罰金（第 32 条）：MOP8,000～MOP80,000

● 刑事罰

・ 個人データ保護法に規定されている義務に対する意図的な不履行（第 37 条）：1 年の禁固又は 120 日分の罰金（センシティブ情報の処理に関する義務の不履行の場合は 2 倍に増加）
・ 承認なしにアクセスが禁止されている個人情報にアクセスした場合（第 38 条）：1 年の禁固又は 120 日分の罰金（技術セキュリティを破ってアクセスした場合や第三者に利益を供与した場合は 2 倍に増加）
・ 承認なしに取得した個人データに対し消去、破壊、変更等の処理を施し、データを使用不能にした場合：1 年の禁固又は 120 日分の罰金（被害が甚大な場合は 2 倍に増加）
・ 職業的に機密保持義務のある者がデータ主体の同意、あるいは正当な理由なしに個人情報を漏えいした場合：2 年の禁固又は 240 日分の罰金

j その他

EU データ保護指令第 25 条と同様に、外国への個人情報の移転を限定している（第 19 条、第 20 条）。

・ マカオ域外へのデータ移転については、移転先の国・地域がマカオと同等の保護レベルの法制度を有していることを要求する。
・ 移転先の保護レベルの十分性については、移転される情報の種類、処理の目的、処理の期間、移転先の法制度等に基づいて、監督機関が判断する。
・ 移転先の国・地域がマカオと同等の保護レベルの法制度を有していない場合でも、下記の場合はデータ移転が可能。
  —データ主体がデータの移転に同意する場合
  —データの移転が防衛、安全保障、健康、犯罪捜査等で必要な場合
  —データ管理者が移転先との間で締結する契約の中で十分な保護レベルを保障する場合

個人情報の海外移転については厳しく規制されている。例えば、個人情報をウェブサイト上で公開する場合、データ管理者がマカオ在住で、処理をマカオで行う場合でも、使用しているサーバーが海外に設置されている、ウェブサイトの管理者が海外にいる、海外からその情報にアクセスできる、等の場合は、全て個人情報を海外移転したとみなされる。

移転先の国・地域（例えば日本）が、マカオと同等の保護レベルの法制を有しているか否かについては監督機関である OPDP（次項にて説明）が調査を行い、判断する。

(3) 監督機関

a　設置の経緯

名称：個人データ保護オフィス（OPDP）

2006 年２月に施行された個人データ保護法の実施と監督のため、マカオ行政長官の命により 2007 年３月に個人データ保護オフィス（OPDP）が設置され、初代 Coordinator として Chan Hoi Fan 氏が任命された。

b 制度の概要

(a)　法的地位

民法第 79 条第３項 *にて規定される公的機関として個人データ保護法の実施と監督を行う。OPDP は恒久的組織ではなく「プロジェクト」の位置付けである。

*民法第 79 条第３項:　下記業務を行う監督機関の設置を規定：

- コンピュータ処理された個人情報の収集、保管、使用の監視
- データベースに保管された第三者の個人情報へのアクセス承認
- データベースの相互連結の承認

(b)　所掌事務

OPDP の主な業務は次のとおり。

・　監督と調整

個人データ保護法に沿って、企業から出される個人情報データ処理報告の受付、審査、登録を行う。

・　法制度構築

個人情報保護に関する法制度を構築し、その施行を監督する。

・　苦情処理

個人情報保護に関する市民からの質問・相談・苦情の受付、違反者に対する懲罰を決定する。

・　広報・教育

セミナー、イベント、広報活動等を通して個人情報保護法についての一般市民の意識を向上させる。

・　分析調査

個人情報保護に関する理論、システム、法制度について調査、分析を行う。

(c)　組織体制

個人データ保護オフィスは次の組織で構成されている。

・　法制度部

・　広報部

・　IT 部
・　管理部
スタッフ数は 30 名（2013 年 3 月現在）

(d)　人事制度

OPDP の長（Coordinator）は、行政法規第 8 条ならびに行政長官指令第 4 項に基づき、行政長官により任命される。任期は 2 年。再任可能。2007 年に初代 Coordinator に任命された Chan Hoi Fan 氏が現在も職にある。Coordinator は業務不履行、不正行為があった場合は行政長官により解任される。OPDP スタッフの雇用条件は民法により規定されている。

(e)　予算

2012 年度の予算は MOP36M。主に政府からの補助金。市民、企業に対し、個人情報保護に関するセミナー、出版等も行っているが、基本的に無料。

(f)　その他

OPDP はデータ管理者が個人データ保護法を理解し、遵守できるよう業務ガイドラインを発行している。
例：

- 従業員監視について
- 小売店によるカード保持者に関する ID 書類作成について
- インターネット上での個人情報公開について
- 指紋以外の生体認証技術を使った就業確認装置の使用について
- 指紋／手相認証技術を使用した従業員就業管理システムについて
- 指紋／手相認証以外の生体認証技術を使用した就業管理システムについて
- 顔認証を使った就業管理システムについて

上記ガイドラインの概要について、本章の最後に記載する。

2. 国際的なルールへの対応状況

(1) APEC-CPEA及びAPEC-CBPRへの対応状況

マカオは APEC には未加盟のため、対応していない。

(2) OECDプライバシーガイドライン改正、欧州評議会第 108 条約現代化、欧州一般データ保護規則提案への対応状況

具体的な動きはないものの、マカオの個人情報保護法はポルトガル法に準拠しており、EU の動向を注視している。

(3) APPA

マカオは 2008 年より Asia Pacific Privacy Authorities (APPA) フォーラムに参加し、他国のプライバシー執行機関との情報交換、違法行為に対する越境協力を行っている。マカオは 2012 年に APPA の正式メンバーとなった。

(4) プライバシー・コミッショナー国際会議

2008 年より、プライバシー・コミッショナー国際会議にオブザーバー参加し、他地域のプライバシー執行機関との間で情報交換を行っている。マカオは本会議の正式メンバーとしての承認申請をしているが、監督機関である個人データ保護オフィスが永続的な組織でないため、まだ正式メンバーとして認められていない。

(5) GPEN

2007 年に OECD で採択された「プライバシー保護法執行の越境協力に関する提言」に基づき、2010 年 3 月に 11 か国のプライバシー執行機関が集まり Global Privacy Enforcement Network (GPEN)が創設された。現在、22 の国・地域が加盟しており、個人情報保護についての情報交換、トレーニング、他国間協力メカニズムの構築、等を行っている。マカオは 2012 年 7 月に正式メンバーに認定された。

3. 個人情報保護に関する認証制度

現時点ではマカオに個人情報保護に関する認証制度は存在しない。他国の動向を注視している。

4. 個人情報保護の施行状況

(1) 苦情処理・紛争解決

	2011 年	2010 年	2009 年	2008 年
問い合わせ受付件数	740	704	602	207
調査件数	86	63	47	35

2011 年には 740 件の問合せを受け付け（前年度比 36.5%増）、この内、86 件について違法性調査を実施した。その結果、23 件について罰金、あるいは改善勧告が発行された。違反者の大半は民間企業で、主に小売、金融、通信の業界で発生している。

(2) 権限行使（報告の徴収、勧告、命令、立入検査、罰則等）

個人データ保護法の基本方針に沿って、OPDP により違反に対する法執行が行われている。（2011 年～2012 年の例）

- グーグルの Street View 地図サービスがセンシティブ情報の違法な収集にあたるとして罰金 MOP30,000 が科せられた。OPDP は、マカオ市街は細い道が入り組んでおり、Street View 地図サービスにより市民のプライベート生活が暴露されると判断した。グーグルは本サービス開始に当たり、OPDP からの事前承認を得ておらず、違法とみなされた。また、グーグルは公共 Wi-Fi からデータを取得し米国本社へ送ったとして、この行為に対しても罰金を科せられた。

- Wynn Macau ホテル・カジノが宿泊客の個人情報を米国の親会社へ移転したとして MOP20,000 の罰金が科せられた。移転された情報の中には、顧客の ID 情報、買い物履歴、遊興情報等が含まれていた。

- Sands China カジノが、前 CEO の雇用情報を裁判資料として米国に移転したとして罰金刑を受けた（金額は未開示）。

- 政府機関のひとつが、データ主体の同意無しに電話会話を録音したとして罰金 MOP8,000 を受けた。電話での苦情受付に際し、応対スタッフの対応評価のため、会話が録音される仕組みを用意していたが、機械の故障により自動アナウンスが流れず、またスタッフも口頭での通知を行わなかったため、データ主体の同意なしの録音がされてしまった。

・　小売店が窃盗容疑者の写真とビデオを公開した罪で MOP10,000 を科せられた。小売店は店内に自己防衛のため監視装置を設置していたが、個人データの公開が基本原則の違反と判断された。

・　電話会社が、顧客への請求書を誤って別人に 10 か月にわたり送付し、MOP4,000 の罰金を科せられた。この電話会社は、OPDP より、顧客データの適切な更新を怠り、個人情報を適切に保護しなかったと判断された。

・　美容整形会社が、患者の同意なしにその患者の「ビフォー&アフター」写真を企業広告に載せたとして、MOP12,000 の罰金が科せられた。

・　政府官僚に対し、同僚の医療カルテを一般公開したとして、MOP8,000 の罰金を科した。

・　装飾表装の自営業者が、債務者とその家族の個人情報をメディアに漏えいしたとして MOP4,000 の罰金を課せられた。一方、債権者は住所を公開されたとして新聞社 2 社に対しても苦情を申し立てたが、OPDP は報道の自由の範囲内として却下した。

・　地方銀行が、顧客の停止要求にもかかわらず、ダイレクト・マーケティング目的の SMS を送り続け、個人情報保護法に規定されている「拒否する権利」を侵したとして MOP4,000 を科せられた。

・　交通サービス局と公共安全警察による移動用交通監視カメラ設置が中断された。OPDP が、この監視カメラの使用は、公共サービスの枠外でのセンシティブ情報の収集にあたると判断したため。

一方、OPDP は個人情報の処理について、事前承認も数多く行っている。

・　３つのバス会社に対し車内での CCTV（監視カメラ）の使用を承認した。ただし、車内に設置される監視カメラは運転手が社内の状況を把握することによりバスの安全運行を助けるためとして、録画機能は付けられない。

・　金融サービス庁と年金ファンド間での、年金制度加入者の給与情報のやりとりを承認した。

・　交通局から法務局への自動車保有者情報の移転を承認した。

・　公共安全警察に対し、外国人従業員のオンライン身元確認システムの構築を承認した。

(3) 広報啓発活動

OPDP は市民及び企業での個人情報保護に関する意識の向上を図るため下記の活動を行っている。2012 年は計 79 件のイベントを開催した。

・　個人向け、企業向けのセミナー実施
・　トレーニング、研究会実施
・　プロモーションビデオ制作
・　出版
・　宣伝配布品制作
・　広告掲載
・　ホームページ（中国語、ポルトガル語、英語）

5. 参考：ガイドライン（概要）

- **従業員監視について**

企業主による従業員監視には、電話モニタリング、電子メールモニタリング、インターネットモニタリング、ビデオモニタリング、等があり、個人情報保護法により規制される。

1. 従業員監視実施前に企業主が考慮すべき点

① データ収集の目的とその合法性
② 目的の達成のために従業員監視が本当に必要か。代替案はないか
③ 監視の範囲、方法、時期は適切か
④ 収集するデータの種類。それらは目的達成のために不可欠であるか
⑤ 監視は企業主、従業員、顧客の利害を保護するか
⑥ 収集されたデータの好ましくない使用により、会社に危害が及ぶ可能性はないか
⑦ 社内の個人情報保護ルール策定

2. 従業員監視の際に遵守されるべき原則

① 合法性

A. 目的は合法的か？

企業のビジネス遂行と利害を保障するために必要であるならば、従業員の監視は合法的である。その際、考慮すべき要因としては下記のとおり。

- 従業員の安全を確保するのに必要な措置
- 財産喪失、損害のリスク
- 企業の安全保障
- 従業員による機密情報漏えいのリスク
- 従業員の就業時間中の私的活動による業務効率低下
- コンピュータシステムの不正利用によるシステム全体への影響
- 顧客へのサービス向上

B. 手段は合法的か？

目的を達成するために用いられる手段はオープンかつ透明性の高いものでなければならず、秘密裡に行われてはならない。データの保持期間は３～６か月。

C. 適用範囲は合法的か？

従業員監視の適用範囲は、業務に関連した活動のみに限定されなければならない。例えば、休憩所や更衣室にビデオ監視カメラを設置してはならず、従業員が業務時間外に家族宛てに送信したメールを監視することはできない。

② 適切性

A. 監視以外の代替案がある場合は、監視を行うべきでない。例えば、コンピュータ・ウィルス防止の為には、従業員の web 履歴データを収集する代わりに、ウィルス・チェック装置／ソフトウェアをインストールし、従業員に対し危ないサイトを閲覧しないようガイドラインを出すことで十分である。

B. 監視はリスクが高いと考えられる領域のみで実施されるべきである。機密性の高いデータへアクセスできない従業員についてのデータ収集はすべきでない。例えば、ビデオ監視カメラは、機密情報が置いてある場所にのみ設置すべきである。

C. 従業員監視時間は最低限にし、就業時間以外は行うべきでない。

D. 監視によって収集されるデータは最小限にすべき。例えば、収集するのはメールの送受信先のみ、あるいは電話番号のみに限定すべきで、メール／電話の内容は監視すべきではない。

③ 従業員の権利保護

職場での従業員監視はオープンで透明性が高くなければならない。

A. 個人情報の収集を行う場合は、企業側は従業員に対し、下記を伝えなければならない。

- 誰が、何の目的で、行うか？
- どんな情報が収集されるか？
- 情報は第三者に移転されるか？

B. データ主体である従業員はデータにアクセスする権利を有する。従業員からの要求に対し、企業主は下記を提供しなければならない。

- データがどのように処理されて、誰の手に渡ったかの情報
- データが処理されている理由
- データが正しくない場合は修正、消去できること

C. 従業員は個人データの処理を拒否することができる。

3. 個人情報収集ステートメント

企業主は従業員監視を開始する前に、事前に下記を記述したステートメントを作成し、従業員に対し示す必要がある。

- データ収集の目的
- 収集されるデータの種類
- 収集されたデータの使われ方
- 誰が収集されたデータにアクセスできるか
- 監視期間、データの保存期間
- 従業員の権利（アクセス権、修正権、拒否権）

・　社内ルール説明

● **小売店によるカード保持者の ID 書類作成について**

マネー・ローンダリング、金融テロリズム、不正カード利用、等を防ぐ目的で小売店は顧客に対し、ID 書類の作成を要求する。この小売店による、顧客の ID データ収集や処理は個人情報保護法の対象となる。

1. データ処理の目的

小売店側がカード保持者の ID 情報を収集、処理するのは次の目的による。

・　マカオの「マネー・ローンダリング防止法」及び「テロ犯罪防止法」の規定を遵守するため。
・　クレジットカードのセキュリティ確保のため。

2. 個人データ処理の合法性

① データ主体であるカード保持者から明らかな同意を得た場合にのみ、小売店側は、カード保持者の ID 情報を収集できる。カード保持者が ID 情報の提供を拒否した場合は、カードの使用を拒否するのが賢明である。
② 小売店側で収集された ID 情報は通常一定期間保有され、関係機関へ提供される。ID 情報の収集について同意が得られている場合は、その情報のさらなる処理は問題ない。

3. 適切なデータ処理

小売店側は下記の明らかで合法的な目的に沿って個人情報の収集を行わなければならない。

・　マネー・ローンダリング防止法やテロ犯罪防止法で規定されている場合
・　特別なセキュリティが要求されるカードによる支払の場合

ただし、小売店側は必要最低限の情報収集にとどめるべきで、過度の収集を行ってはならない。

4. データの保全とデータの保存期間

・　小売店側は収集された個人情報の保全に努めなければならない。
・　収集されたデータの保存期間は、法律、指針が定める期間を超過してはならない。

5. データ主体の権利

個人情報保護法の第 10 条～第 14 条に規定されているデータ主体の権利を小売店側

は保障しなければならない。データ主体は自分の情報にアクセスでき、また、情報が収集される前に、収集されることを知らされねばならない。

- **インターネット上での個人情報公開について**

昨今インターネットが普及するにつれ、個人情報開示のメディアとして利用されることが多くなっている。インターネット上で開示される個人情報は、純粋に個人あるいは家族内での活動である場合を除いて、個人情報保護法の対象となる。

1. 情報源の合法性

非合法的な方法で個人情報を入手しインターネット上で開示することは犯罪となる。例えば、会社が保有する個人の情報を自分のウェブサイトで公開したり、会社のサーバーに侵入し、顧客情報を取得し、自分のウェブサイトに載せたりすることは行政罰となる。

2. データ処理の合法性基準

情報が合法的に収集されたとしても、その情報をオンラインで公開することは必ずしも合法でない。個人情報をオンライン上で公開する場合は、個人情報保護法で規定されている合法性の基準を満足させる必要がある。

① 一般的基準

- データ主体の明らかな同意がある場合
- 契約を履行する場合
- 法律を遵守する場合
- データ主体が身体的に同意を示せない状況下で、データ主体の重要な利害を保護する場合
- 公的利害の履行と当局の行使

データ主体の同意獲得はシンプルで分かりやすいものでなければならない。また、その同意を取り下げることも簡単にできなければならない。

② センシティブデータ処理の合法性基準

センシティブデータの処理は下記の場合を除いて、原則、禁止されている。

- 法律によって処理が承認される場合
- 処理が重要な公共の利害に基づいている場合
- データ主体が明らかな同意を与えている場合
- データ主体が身体的に、あるいは法律的に同意を与えられない状況下にあるが、データ主体の重要な利害を保護する必要がある場合
- データ主体により明らかに公にされた情報に関係しており、データ主体の同意

が得られている場合
- 法的要求の行使あるいは擁護に必要な場合
- 予防医療、治療、ヘルスケアサービスの提供に必要な場合

③ 非合法的行為に関するデータ処理の合法性基準

非合法的行為、刑事罰、行政罰、等に係る人物の個人情報の処理については厳格な合法性基準が満たされねばならない。

3. 適正の原則

インターネット上での個人情報の公開が合法的なものであったとしても、その公開は目的に即した適切かつ過度でないものでなければならない。

4. データ主体の権利

データ主体は、情報にアクセス、修正、反論、損害賠償する権利を持っている。

5. 表現の自由

マカオ基本法では基本的人権の１つとして表現／報道／出版の自由が保障されている。一方で、個人情報保護法でプライバシーの保護が謳われており、両者のバランスが肝要となる。個人情報保護法では、表現／報道／出版の自由を守るため、「情報への権利」、「アクセスする権利」、「訂正する権利」を制限している。（例：報道、芸術表現の目的で個人情報が処理される場合は、例外とされている（第 10 条第 6 項、第 11 条第 3 項））

6. マカオ国外へのデータ移転

マカオ国外への個人情報の移転は個人情報保護法で規制される（第 19 条、第 20 条）。

- データ管理者がマカオに在住し、個人情報の処理をマカオ内で行うが、情報を掲載するウェブサイトが海外にある、あるいはそのウェブサイトの管理者（ISP 含む。）が、海外にいる場合、このデータ管理者は個人情報を海外に移転したものとみなされる。
- データ管理者がマカオに在住し、個人情報の処理もマカオで行われ、情報を掲載するウェブサイトもマカオにある場合でも、データ管理者が使用する IT 機器（サーバーなど）が海外にある場合、このデータ管理者は個人情報を海外に移転したものとみなされる。
- データ管理者の所在、個人情報の処理、ウェブサイトの所在、IT 機器の所在が、全てマカオにある場合でも、ウェブサイト上の個人情報に海外からアクセスできる場合、データ管理者が国外の特定の企業／個人を意図して掲載した場合は、情報の海外移転とみなされる。意図的でない場合は、海外移転とはみなされない。

● **従業員の業務状況管理のための指紋／手相認証装置の使用について**

指紋や手相の生体データは個人を特定できる個人情報であり、これらの情報の処理は個人情報保護法で規制される。

- 雇用主が社内の操業管理を目的として、指紋／手相認証装置を用いて、従業員の就業状況を記録すること自体は合法的である。しかし、個人情報保護法第５条で規定されているように、雇用主は個人のプライバシーを守り、個人情報を合法的に処理しなければならない。
- 指紋／手相認証装置でのデータ処理を合法的にするには下記のいずれかが必要である。
  ① 従業員からの明らかな同意を得る。
  ② 就業契約の中に明記する。
- 従業員側には指紋／手相認証装置で処理される個人情報について「知る権利」、「アクセスする権利」、「拒否する権利」がある。雇用主側は、個人情報収集ステートメントを発行し、従業員に対して周知させる必要がある。従業員から正当な理由に基づく拒否がある場合は、雇用主はデータ処理を中止すべきである。
- 指紋／手相認証装置でのデータ処理は自動で行われるため、監督機関への届出が必要となる（個人情報保護法第 21 条）。
- 雇用主は指紋／手相認証装置が正しく作動していることを保証しなければならない。さもなければ、個人情報保護法第５条に規定されている「情報の質」に違反し、最高 MOP$40,000 の罰金が科せられる。また、これらの生体情報を他の目的に使用した場合は、１年の禁固又は 120 日分の罰金が科せられる。
- 雇用主は指紋／手相認証装置で収集された情報を他に移転すべきでない。また、データは、従業員が会社を辞めたら即座に消去すべきである。

● **指紋認証あるいは手相認証以外の生体認証技術を使った在席管理システムについて**

生体認証技術には、指紋認証、手相認証以外に、顔認識、声紋認識、虹彩認証がある。それぞれの技術には下記の特徴がある。

① 能動的／受動的データサンプリング

指紋認証／手相認証は「能動的」で、システム使用に当たり事前にユーザーのデータサンプルを登録する必要がある。一方、顔認証、声紋認証は事前のサンプル収集が不必要で、カメラ映像、あるいはマイクからサンプルがデータ主体の知らないところで収集される（「受動的」）。よって、後者はよりプライバシー侵害度が高いといえる。

② 技術がユーザーに与える影響

虹彩認証のサンプル登録の際にはユーザーの目に光を照射する必要があり、心理的恐怖を与える。顔認証は、周りの光、髪の毛、装飾具、等により影響を受ける。また、顔認証により、性別、人種、等のセンシティブ情報が明らかになる。指紋認証、手相認証は比較的、プライバシー侵害が少ないと言える。

③ 成熟した技術

指紋認証は成熟した技術であり、他の技術と比較して信頼度が高い。

④ 認知度

指紋認証は個人認証技術として広く使用されており、技術的に廉価で高効率、使用法も簡単である。

⑤ 使用領域

一般的に在席管理用途としては指紋／手相認証が広く使用されている。ただし、医療施設のように感染に敏感な場所では他の技術も採用されている。

指紋／手相認証が比較的成熟技術であること、これまで広く使用され認知されていること、正確性が高いこと、等を考慮すると、生体認証技術を従業員の在席管理目的で使用する場合は、この技術が推奨される。

- **顔認識在席管理システムの使用について**

生体認証システムを使用して従業員の在席状況を管理することは、違法ではない。ただし、生体認証システムの使用は個人情報の「処理」に当たるため、個人情報保護法により規制される。

生体認証システムはいろいろな種類があるが、指紋認証と手相認証は比較的、プライバシー侵害の観点では問題性がないと判断される。一方、顔認証は、データ主体の知らないところで行われる点において、問題がより大きいと判断される。また、顔認証は性別、人種などのセンシティブ情報を処理する点で、問題性が大きい。

雇用者が生体認証システムを用いて従業員の在席管理をする際は、下記の条件のいずれかを満たさねばならない。

① 従業員による明らかな同意がある場合
② 雇用契約で規定されている場合
③ 雇用者の権利／利害が従業員のそれを凌駕する場合

雇用者はシステム導入決定の前に下記を考慮する必要がある。

① 合法性：データ処理を合法的にする基準

② 適切性：データ主体のプライバシー侵害を軽減する他の手段の検討

6. 参考：マカオについて（外務省基礎データより）

【一般事情】

1. 人口　　約 58 万 2 千人（2012 年）
2. 面積　　29.9 平方キロメートル

【マカオ特別行政区機構】

1. 行政長官
   崔世安（Fernando Chui Sai On）。2009 年 12 月に初代行政長官である（Edmund Ho Hau Wah）の後を継ぎ第 2 代行政長官に就任。任期は 5 年
2. 行政組織
   主要高官としては、行政法務、経済財政、保安、社会文化、運輸・公共事業の 5 長官
3. 行政会
   行政長官の諮問機関。行政会委員は長官や立法会議員等 11 名
4. 司法機構
   審法院、中級法院及び初級法院・行政法院の三審制。終審法院院長（最高裁判所に相当）は岑浩輝（SAM Hou Fai）。
5. 立法会会議
   議員は 29 名（直接選挙 12 名、間接選挙 10 名、行政長官任命 7 名）。立法会主席は（LAU Cheok Va）、副主席は賀一誠（HO lat Seng）。立法会には、規約任期委員会と三つの常設委員会、行政委員会が設置されている。

【経済・社会概況】

1. 経済概況
   （ア）主要経済指標（出所：マカオ経済局 2012 年）
   名目 GDP：3,482 億 1,640 万パタカ（約 290 億 1803 万米ドル）
   一人当たり名目 GDP：61 万 1,930 パタカ（7 万 6,588 米ドル）
   （イ）観光・カジノ産業
   従来より観光及びカジノ産業が大きな地位を占める（GDP の約 8 割、政府歳入の 8 割以上）。香港資本等により、1970 年代より繊維産業が、1980 年代に入り玩具、電気・電子産業が発展した。しかしその後、華南地域のより低廉な労働力との競争により、第 2 次産業の占めるシェアは低下。

【二国間関係：対日貿易】

1. 貿易額（2011 年）　対日輸出（千パタカ）：144.041、対日輸入（千パタカ）：3,911.242

v. メキシコ ※

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

メキシコの個人データの保護については 2001 年に連邦議会に９つのイニシアティブが提出されて以降、９年間にわたって議論されてきた。2002 年に成立した政府の公的情報の透明性及びアクセスに関する連邦法において公的部門のみであるものの個人データの権利が初めて立法上認知され、個人データの権利に関する議論も高まっていった。しかし、民間部門における利害関係の調整が上手くいかず、個人データ保護に関する法案はすぐには成立しなかった。

個人データ保護に関する法案に関する議論がまとまっていったのは、憲法改正と経済連携を巡る動きが見られてからのことである。第１に、2007 年以降採択されていった、個人データの保護に関する憲法修正が重要である。第６条（2007 年７月 20 日改正）では個人データの保護が基本的人権であることを宣言している。第 16 条（2009 年６月１日改正）は「いかなる者も個人データの保護、すなわち、アクセス、訂正及び中止、そして法に定められた異議申立を表明する権利を有する」と規定する。第 73 条（2009 年４月 30 日改正）は、2010 年５月までに個人データの保護に関する立法を議会が制定する権限を有することが明記された。これによりメキシコにおいても個人データの保護に関する権利が基本的権利として初めて明文化された[17]。第２に、メキシコは 2000 年 10 月からEUとの経済連携協定を締結しており、オンラインサービスを含む規制協力の対話を行ってきた。この経済連携協定の中でも人権と民主的価値を尊重するとともに（第 39 条(c)）、個人データの処理と越境データ移転の高いレベルの保障を行うこととなっている（第 51 条）。このようなEUとの経済連携協定をはじめとする北米地域での各種協定（例

※　本稿の執筆に当たり、メキシコの情報へのアクセス及びデータ保護の連邦機関（Instituto Federal de Acceso a la Información y Protección de Datos）におけるヒアリングに際し、Gerardo Laveaga（委員長/ President Commissioner）、María Elena Pérez-Jaén Zermeño（委員/ Commissioner）、Juan Pablo Guerrero Amparán（事務総局長、前 Commissioner）、Alfonso Onate Laborde（データ保護事務総局長）、Arturo Rios Camarena（国際担当局長）、Gabriela Archundia Mora（国際担当審議官）、María Adriana Báez Ricardez（自主規制局長）、Melissa Higuera Pérez（自主規制局課長）、Laura Perla González（Pérez-Jaén 委員付・弁護士）、David Palomino Hernández（Pérez-Jaén 委員付・弁護士）、Elizabeth Vicenté González（Pérez-Jaén 委員付・弁護士）から長時間にわたる説明をしていただくとともに、関係資料を頂戴した。ここに記し、御礼申し上げる。また、メキシコでのヒアリング調査に随行し、豊富な資料を提供していただくともに、本稿に的確なコメントを頂戴した板倉陽一郎弁護士（ひかり総合法律事務所）の御厚意にも御礼申し上げる。

17　*See* IFAI, *The ABC of the Federal Law of Protection of Personal Data held by Individuals*.

えば、北米における情報と貿易の自由な流通に関する宣言）がメキシコ国内における個人データの保護法制を後押しすることとなった。

そして、2010 年 4 月 13 日、政府委員会が提出した法案報告が下院の本会議で承認（賛成 335 票、反対 3 票、棄権 5 票）され、2010 年 4 月 27 日に上院において満場一致で承認された。2010 年 7 月 5 日、民間が保有する個人データの保護に関する連邦法が公示され、翌日から施行された。このように、メキシコにおける個人データ保護法は 2001 年のイニシアティブ提出後およそ 9 年にわたる国会での審議を経て成立したことになる。

また、メキシコにおいては、個人データ保護法以外に連邦レベルの法律で個人情報の保護に関する様々な規定を置いており、次のようにまとめることができる[18]。

法律名	条文番号	執行機関	適用範囲
連邦民法	58～60,134,1916	連邦民事裁判所	民法上の身分に関するデータ
印刷法	9	連邦刑事裁判所	司法に関する情報公表の禁止
通信の一般的方法に関する法律	383	通信運輸省、連邦刑事裁判所	州職員のメッセージの秘密性保持
連邦通信法	49,65	通信運輸省、連邦通信委員会	通信を用いた情報の機密保持
ラジオ・テレビに関する連邦法	66	通信運輸省	ラジオを通じた通信傍受の禁止
憲法第 5 条の規制に関する法律	36	公的教育省	専門職の秘密保持
連邦行政の専門職に関する法律	15	行政管理省	公的専門職の秘密保持
公務員の行政責任に関する法律	8	行政管理省	公務員の文書・情報管理義務
連邦行政手続法	33	連邦行政機関	行政罰に関する文書及び情報へのアクセス
連邦消費者保護法	1,16～18,76	消費者保護局	マーケティングにおける消費者の情報保護
通商法	49	経済省	10 年間のデータ保存
連邦競争法	31	連邦競争委員会、経済省	捜索・押収に関する情報の秘密保持
連邦著作権法	109,231	著作権国立機関、連邦刑事裁判所	個人情報へのアクセス等に関する事前認可

18 CRISTOS VELASCO SAN MARTIN, CYBER LAW IN MEXICO 239-255 (2012)に基づき作成。

産業財産法	82,84	産業財産機関及、連邦刑事裁判所	産業機密の保持
金融サービスの保護に関する法律	13～15	金融サービスの利用者保護委員会	金融機関における秘密保持
クレジット機関に関する法律	117	銀行・セキュリティ委員会、連邦刑事裁判所	預金等の秘密保持
セキュリティ市場法	25	銀行・セキュリティ委員会、連邦刑事裁判所	証券取引の秘密保持
預金クレジット法	34	銀行・セキュリティ委員会、連邦刑事裁判所	預金等に関する情報開示の禁止
投資パートナーシップ法	55	銀行・セキュリティ委員会、連邦刑事裁判所	預金等に関する情報開示の禁止
クレジット情報の規制に関する法律	18,28,37～39,52	銀行・セキュリティ委員会、連邦刑事裁判所	クレジット情報開示の禁止
メキシコ銀行法	58	メキシコ銀行	秘密保持
連合財政法	17,69	連邦国税当局、連邦刑事裁判所	納税者のデータ登録と保護
地理統計情報法	37～44	統計・地理・情報機関、連邦刑事裁判所	地理上、統計上、国勢調査に関する個人データ保護
人口一般法	91,98,101,103～105,107,112,113	国務省、連邦刑事裁判所	メキシコ国民のデータ登録・保護
連邦労働法	47,134	連邦労働裁判所	労働者の秘密保持
選挙手続連邦法	135～141	連邦刑事裁判所	選挙登録された国民データの保護
連合検査法	16,27,28,80	連合検査機関、連邦刑事裁判所	連合検査職員の秘密保持
公的委員会法	15	経済省、連邦刑事裁判所	専門職の秘密保持
連邦刑事法	173,177,210,211	連邦刑事裁判所	裁判所の許可なしの私的通信の傍受の禁止
プレスの刑罰に関する法律	１～３,９～12	連邦司法裁判所	悪意による私生活の不当な干渉の禁止
組織犯罪対策連邦法	16～28	連邦司法裁判所	裁判所の許可なしの私的通信の傍受の禁止
国土安全法	６,53,59,64	連邦司法裁判所	私的通信の公開の禁止
政府の公的情報の透明性及びアクセスに関する連邦法	３,13～26,33～39,61～64	情報へのアクセス及びデータ保護の連邦機関	公務員による個人データ保護
第三者が保有する個人データの保護に関する連邦法	１～69	情報へのアクセス及びデータ保護の連邦機関	データ処理者の個人データ保護

(2) 個人情報保護法制の概要

a 法律名

・ 民間が保有する個人データの保護に関する連邦法（Ley Federal de. Protección de Datos Personales en Posesión de los Particulares）（以下「法」という。）
2010 年 7 月 5 日公示、2010 年 7 月 6 日施行

・ 第三者が保有する個人データの保護に関する連邦法
2012 年 1 月 6 日施行

・ 政府の公的情報の透明性及びアクセスに関する連邦法（Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental）2002 年 6 月 11 日公示、最終改正 2006 年 6 月 6 日

・ 民間が保有する個人データの保護に関する連邦法規則（Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares）
2011 年 12 月 21 日公示（以下「規則」という。）

このほかに、連邦特別区及び州には個人データ保護に関する条例が整備されている。

・ 連邦特別区（メキシコシティ）：連邦特別区個人データ保護法（2008 年 10 月 3 日）
・ Colima 州：2003 年 6 月 14 日条例第 356 号
・ Jalisco 州：民法（私的情報について 39 か条）
・ Guanajuato 州：個人データ保護条例（2006 年 5 月 19 日）
・ Tlaxcala 州：公的情報へのアクセス及び個人データ保護条例（2007 年 1 月 12 日）

	連邦レベル	州レベル
公的部門	政府の公的情報の透明性及びアクセスに関する連邦法	条例
民間部門	個人データ保護に関する連邦法 第三者が保有する個人データの保護に関する連邦法	

以下、特に断りがない限り、民間が保有する個人データの保護に関する連邦法（条文は法を指している。）及び同規則についてその概要を示すこととする。

b 目的

個人のプライバシー及び情報自己決定権（derecho a la autodeterminación informativa）を保障するため民間が保有する個人データの保護を目的とする（第 1 条）。

【ヒアリング結果】

・ データ保護法の第 1 条の目的はまさに人権であり、憲法修正によりデータ保護が人権であることが認められたところである。メキシコにとってデータ保護は基本的人権であることに疑いはない。

・　データ保護を基本的人権と捉える背景には欧州、特にスペインの影響はあるが、アプローチはアメリカよりも欧州、そして欧州よりカナダに近いと考えている。NAFTA の影響もある。欧州との大きな違いは、国際データ移転である。

c 適用範囲

法の規制対象は民間部門（個人データを処理する個人及び法人）である（第２条)。

保護の対象は「個人データ」であり、「識別された又は識別することができる個人に関するいかなる情報」と定義される（第２条)。個人データの定義は日本とほとんど変わらないが、容易照合性の要件がない。

なお、公的部門については、政府の公的情報の透明性及びアクセスに関する連邦法が個人データの処理について規律している。

d 適用除外

①クレジット報告会社規制法及び関連法に基づく信用報告会社、②もっぱら個人的な利用を目的とした個人データの収集及び蓄積を実施する個人については適用されない。（第２条）

e 権利・義務の内容

(1)　主な権利の内容

データ処理を可能とするデータ主体の意思の明示であるデータ主体の「同意」（第３条Ⅳ）が重視される（第８条、第 10 条)。また、データ主体はいつでも同意の撤回をすることができる（規則第 21 条)。いかなるデータ主体も、必要に応じその代理人もアクセス、訂正、停止、異議申立ての権利を行使することができる（第 22 条)。

① アクセス権－データ主体は自らの個人データとともにプライバシー取扱通知にアクセスする権利を有する（第 23 条)。

② 訂正権－データ主体は不正確・不完全なデータについて訂正する権利を有する。

③ 停止権－データ主体はいつでも自らの個人データの利用停止を求める権利を有する。データの利用停止がされた場合、データ主体に通知しなければならない（第 25 条)。ただし、私人間あるいは行政との契約・協定に基づく場合、法令で定められている場合等については利用停止をする義務はない（第 26 条)。

④ 異議申立権－データ主体はいつでも自らのデータの処理について異議申立する権利を有する（第 27 条)。

これらの権利を行使するに当り、データ主体は①氏名・住所、その他通知を受ける手段、②データ主体であることの本人を証明するもの、③権利を行使しようとする個

人データについての明確かつ正確な記述、④個人データの存在を明らかにしやすくするその他の文書等を提示する必要がある（第 29 条）。原則として 20 日以内にデータ主体からの要請に対してデータ管理者は回答をしなければならない（第 32 条）。

(2)　主な義務の内容

データ管理者は合法性、同意、通知、データの質、利用目的、法遵守、比例原則、説明責任の各原則を守らなければならない（第 6 条）。

① 合法性の原則－合法的な方法により個人データを収集し、処理しなければならない（第 7 条）。また、誠実性の原則としてデータ主体の利益と合理的なプライバシーの期待に基づきデータを処理する義務がある（規則第 44 条Ⅲ）。

② 同意の原則－個人データのあらゆる処理について、原則として本人の同意を必要とする。ただし、プライバシーの取扱いを通知し、本人からの異議申立てがない場合はこの限りではない（第 8 条）。このほかに、法令に基づく場合、公に入手可能なデータ等の処理については本人の同意を必要としない（第 10 条）。

③ 通知の原則－データ主体に対しプライバシー取扱通知が入手できるようにしなければならない（第 17 条）。

④ データの質の原則－データベースに含まれる個人データは正確かつ最新のものとなるよう努めなければならない（第 11 条）。もしデータ主体からデータを収集していない場合、データ管理者はデータの質と処理の状況に応じてデータの質の原則を満たすための合理的な措置を講じることとなる（規則第 36 条）。

⑤ 利用目的の原則－個人データの処理はプライバシーの取扱通知で定められた利用目的に限定されなければならない。利用目的を変更する場合、データ主体から同意を必要とする（第 13 条、規則第 40 条、第 43 条）。

⑥ 法遵守の原則－法で定められた個人データ保護の諸原則を遵守するよう努めなければならない（第 14 条）。

⑦ 比例原則－そして、利用目的にとってすでに必要でなくなった個人データについては処理を停止しなければならない。データベースの管理者は契約上の義務が 72 か月間履行されない場合、データベースにある関連する情報を削除しなければならない（第 11 条）。

⑧ 説明責任の原則－データ管理者はデータ主体から情報の処理に関して、どのような情報が収集され、それがなぜ処理されているかについて知らせる義務がある（第 15 条）。

上記の諸原則の履行のほか、データ漏えい通知義務を含む安全管理措置に関する規定がある（第 19 条～第 21 条)。データ管理者は、IFAI が示すセキュリティの基準に従い組織的･物理的･技術的なセキュリティ措置を講じるものとされる(規則第 57 条)。また、データ管理者はリスク分析やセキュリティ措置の実施計画、審査・監査等を行うこととされている（規則第 48 条、第 60 条、第 61 条)。さらに、データ処理者については、再委託の禁止等を含む詳細な規定が置かれている（規則第 50 条)。

f 届出・登録制度

一般的な届出・登録制度は存在しない。なお、データ管理者は個人データ保護担当者を配置し又は部署を設置しなければならない（第 30 条)。また、自主規制の仕組みを策定した場合、IFAI 及び関係省庁にその文書を提出することができる。

g 苦情処理制度

データ主体又はその代理人によってデータ保護要請を IFAI に申し立てることができ、その申立てに基づき IFAI は決定を下すこととされている（第 45 条)。

個人からの権利に関する申立てがあったときから 50 日以内に IFAI は決定を下すこととされている（第 47 条)。

h 行政措置・罰則

法で定められた義務規定に違反した場合､次のような制裁措置が IFAI によって採られうる（第 64 条、第 67 条)。

① 警告：データ主体によって要請された行為の実施
② 罰則：違反の類型に応じてメキシコシティの最低賃金 100 日～320,000 日分の科料
③ 追加制裁：違反を繰り返した場合は、100 日～320,000 日分の追加的科料
④ 禁固刑：セキュリティ違反の場合は３か月～３年の禁固刑、非合法な営利目的の欺瞞的な個人データの処理の場合は６か月～５年以下の禁固刑

なお、罰金の金額はおよそ 471.83～1,509,886.44 米ドルである。

これらの制裁に対しては、データ管理者が連邦財政・行政裁判所に対し不服申立ての訴訟を提起することができる。

i その他

(a) センシティブ・データ

センシティブな個人データとは、データ主体の生活における最も私的な部分に関連する、又は当該所有者に対する差別や深刻な危険をもたらす可能性のある個人データを指す。特に、次のデータがそれに該当するものと考えられる。人種・民族の出自、現在及

び将来の健康状態、遺伝情報、宗教上・哲学上・道徳上の信念、組合員、政治的見解、性的嗜好（第３条Ⅵ）。

そして、センシティブ・データの処理については、本人からの署名、電子署名又はその他の認証方法により本人からの書面による明確な同意を必要とする。

(b) プライバシー取扱通知

プライバシー取扱通知には、少なくとも次の情報が含まれていなければならない（第16条）。

① データを収集する管理者名と所在
② データ処理の目的
③ データ主体に対する利用制限又は公開制限に関する選択及び方法
④ アクセス、訂正、停止、異議申立ての権利行使の方法
⑤ 該当する場合は移転される予定のデータ
⑥ プライバシー取扱通知の変更を知らせる手続及び方法

そして、このプライバシー取扱通知はデータ主体が入手できる形にしておかなければならない（第17条）。また、第三者から個人データを入手したデータ管理者は、当該個人データの所有者に対しプライバシーの取扱いを通知しなければならない（第18条）。

また、プライバシー取扱通知は、必要な情報を含む単純なものでなければならず、明確で分かりやすい言葉で書面にすることとされている（規則第24条）。

【ヒアリング結果】

・ 自主規制に登録したい企業は IFAI に登録して誰でもなることが可能。自主規制のスキームが働けば、IFAI の仕事を減らすことができる。また、プライバシー・ポリシーの作成については、第１に仮に違反してもプライバシー・ポリシーを制定していれば、制裁金額が減額されること、第２に社会的な名声を維持できることというモチベーションがあると考えている。

(c) データ漏えい通知義務

データ主体の財産又は道徳的権利に物理的な影響を及ぼすセキュリティ違反が生じた場合、データ管理者はデータ主体に対し速やかに報告しなければならない（第20条）。

【ヒアリング結果】

・ データ保護通知制度が法律上存在しており、致命的な損害（crucial damage）が生じるような場合には通知する。データ主体者に対してのみであり、IFAI には通知しない。もしデータ主体に通知をしない場合は、制裁が科されることとなる。

(d) データ移転

データ処理者以外の国内または外国の第三者に対し、個人データを移転する予定がある場合、プライバシー取扱通知と利用目的を受領者に対し提供しなければならない（第36条）。

国内または外国の第三者への移転については、次の場合を除きデータ主体の同意を必要とする（第37条）。

－法令に基づく場合
－医療診断・予防等のため必要な場合
－同一グループの企業、データ主体の利益のために必要な場合
－公共の利益の保護に必要とされる場合
－司法手続に必要な場合
－データ管理者とデータ主体との間の法的関係を維持するために必要な場合（この場合、データ処理者はデータ管理者と同様の義務を負うこととなる（規則第53条Ⅰ）。）

【ヒアリング結果】

・ 多くの企業はEUにおいて広く知られる拘束的企業準則（Binding Corporate Rules）が何であるかについても分かっていないため、現在はBCRについての広報啓発に努めている。

(e) 自主規制

法の規定を補完するため自主規制の仕組みについて国内外の組織と協定を締結することができる。自主規制の中には、データ処理の実施とデータ主体の権利行使の促進と調和しうるトラストシール等の仕組みを用いることができる。このような仕組みは、IFAI及び関係省庁に通知することとする（第44条）。

法第44条に基づき、2013年1月、IFAIは組織内部での自主規制の内容についてガイドラインを公表した。同ガイドラインには認証の仕組みについて説明されている。

(f) 集団訴訟

メキシコで集団訴訟は一般的ではないものの、2010年に修正された憲法第17条第3項により、商品やサービスの消費に関する集団訴訟を提起することができるようになった。もっとも、データ保護に関してこの集団訴訟を提起できるかどうかについては不確定である[19]。

---

19 Laura Collada & Jorge Molet, *Mexico*, in DATA PROTECTION & PRIVACY 373 (Monika Kuschewsky Van Bael & Bellis eds., 2012).

(3) 監督機関

＊本節は基本的に IFAI でのヒアリングをもとに執筆している。

a 設置の経緯

情報へのアクセス及びデータ保護の連邦機関（IFAI、Instituto Federal de Acceso a la Información y Protección de Datos）については、政府の公的情報の透明性及びアクセスに関する連邦法第 33 条に基づき設置され、2003 年 6 月から運用を開始した。その後、個人データ保護法の成立に伴い、2010 年 7 月より個人データ保護についても業務を開始した。

b 制度の概要

５名のコミッショナーからなる合議制。各コミッショナーは大統領から任命され、議会の承認を経る。コミッショナーの任期は７年間（再選は不可）。

(a) 法的地位

運用、予算、決定において独立した行政機関である。

(b) 所掌事務

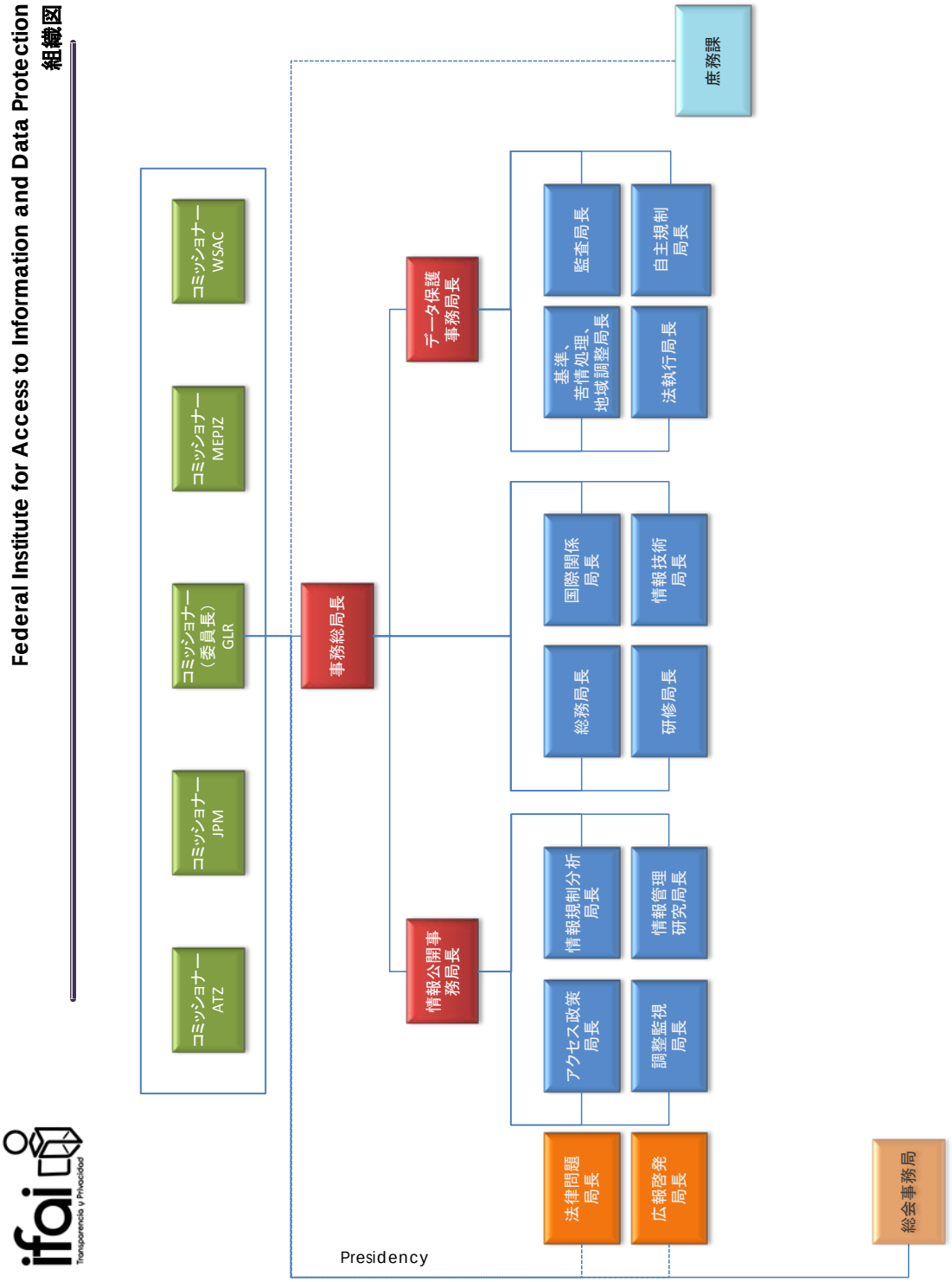
個人データ保護法以外に、政府の公的情報の透明性及びアクセスに関する連邦法に関する事務に従事している。

(c) 組織体制

スタッフは 392 名。男性 182 名・女性 210 名、平均年齢は 36.08 歳。

５人のコミッショナーは全員が情報公開と個人情報を扱い、部門を限ることはない。各コミッショナーにつき 12 人の専属スタッフを自由に雇用することができ、その中には情報公開と個人情報それぞれに課長級がいる。

組織図は図３－２のとおりである。


Federal Institute for Access to Information and Data Protection
組織図
ifai
Transparencia y Privacidad
コミッショナー ATZ
コミッショナー JPM
コミッショナー (委員長) GLR
コミッショナー MEPIZ
コミッショナー WSAC
事務総局長
情報公開事務局長
データ保護事務局長
庶務課
アクセス政策局長
情報規制分析局長
調整監視局長
情報管理研究局長
総務局長
国際関係局長
研修局長
情報技術局長
基準、苦情処理、地域調整局長
監査局長
法執行局長
自主規制局長
法律問題局長
広報啓発局長
総会事務局
Presidency

【図３ - ２　組織図】

(d) 人事制度

コミッショナー付スタッフは各コミッショナーが独自に選ぶ。

その他のスタッフ（管理部門等）は他官庁と同様の公募が出る。民間、NGO、ロースクールを経てIFAIに入る例も見られる。

(e) 予算

2013年度全予算：518,979,976ペソ（約43億5900万円）

個人データ保護の部署の内訳は次のとおりである。

人件費　54,517,951ペソ（約4億5800万円）

運営費　116,872,862ペソ（約9億8200万円）

その他　3,376,500ペソ（約2800万円）

(f) 権限

IFAIは次の権限を有する（法第39条）。

① 法令遵守の監督
② 法解釈
③ データ管理者の技術的支援
④ 法の規定に従った意見提出及び勧告
⑤ 諸外国のベストプラクティス及び情報セキュリティの基準の普及
⑥ 聴聞、決定及び必要に応じて制裁措置
⑦ 国内外の機関との連携
⑧ 年次報告書の提出
⑨ 国際会議への参画
⑩ プライバシーに関する影響研究の実施
⑪ 個人データ保護に関する研究
⑫ 法に基づくその他必要な活動

IFAIは必要に応じ法の遵守状況について監査することができる（第59条）。

また、経済省はビジネス界における個人データの保護に関する啓発活動の実施や自主規制の適切な策定などをすることとされている（第42条）。

【ヒアリング結果】

- 水曜日ごとに申立てを処理するコミッショナー会議及び記者会見がある。会議のうち、ルーティンのものは内部打合せで落ちるが、公開で話し合うものもある。これはマスコミも入り、公衆が自由に聴講できる。
- その他の定例の打合せとして、月曜日に行われるものがある。

(g) 他機関・地方との関係

地方支分部局は存在しない。各州には州の機関を保護するための機関はあるが、民間部門はあくまで連邦法所管なので、IFAI 専管である。

2. 国際的なルールへの対応状況

(1) APEC-CPEA及びAPEC-CBPRへの対応状況

2013 年 1 月 16 日、APEC電子商取引運営部会はメキシコがAPEC越境プライバシー・ルール制度の２番目の参加エコノミーとして承認されたことを公表した。電子商取引作業部会議長のLourdes Yaptinchay氏は「メキシコがCBPRシステムの設計と推進の中心を担ってきており、APEC域内でその実践を促進する次なる段階へと足を踏み入れた」[20]と評価している。

2012 年 9 月 24 日、メキシコ経済省の産業通商副大臣が APEC 電子商取引委員会議長宛てに CBPR への参加を申請した。その申請には、①IFAI が CPEA の参加機関であること、②メキシコが少なくとも 1 つ以上の説明責任機関（Accountability Agent）を参画させる意図があることが含まれている。この申請とともに、付属文書として、説明責任機関になるためのメキシコ国内法及び規則と執行機関に関する説明文書（付属文書 A)、CBPR システムの要件執行概略（付属文書 B)、プライバシー執行機関の執行実践、政策及び活動（付属文書 C）が提出されている。共同監視パネルを構成するアメリカ合衆国商務省、カナダ産業省、台湾外交貿易局が上記①及び②の申請について審査報告書を電子商取引委員会議長宛てに提出している。なお、審査報告書作成の過程において電子メールおよび電話会議によるメキシコの経済界、IFAI、CPEA の担当者によるコンサルテーションが行われている。

以下、IFAI の CPEA への参加及びメキシコの CBPR への参加についてそれぞれの対応状況について記述する。

a APEC-CPEAへの監督機関の対応状況

IFAIがCPEAへの参加に当たり、執行の実践、政策及び活動を示さなければならない。上記で示したIFAIの法的性格や権限のほかに具体的な活動の例が示されている。例えば、2009 年にはプライバシー影響評価の実施をしてきたことや 2012 年 1 月に民間部門の執行を強化するために組織改編をしたことなどである。また、2012 年にIFAIの委員長は優先的な政策として、国際的な会議等におけるIFAIの存在感を高めることなどを示し、越境的なデータ移転に関する情報共有や技術支援を他の機関を行うこともこれに含まれる。

---

20 *See* APEC, Consumer Protection in Asia-Pacific Gets Boost as Mexico Joins Privacy Regime. Available at http://www.apec.org/Press/News-Releases/2013/0116_cbpr.aspx

さらに、APEC越境プライバシー・ルール制度やグローバル・プライバシー執行ネットワーク（GPEN）の活用が示されている。第33回データ保護プライバシー・コミッショナー国際会議[21]のホスト国として提示した「メキシコシティ宣言（Mexico City Declaration）」―ビッグ・データの時代を迎え対話の促進と情報共有等が謳われている宣言―の下、執行政策の効果的な策定に従事していくこととなっている。

個人データ保護法では国際協力に関する明示的な制約がないものの、法の枠内で情報提供を含むいかなる協力も可能であり、またIFAIをはじめとする連邦政府が他国と共有することになる情報は全て特別情報又は機密情報に分類されることとなる。

b APEC-CBPRへの政府の対応状況

法第44条は自主規制の仕組みに関する規定を設けており、個人データの保護の責任を有するAccountability Agentの存在が想定されている。また、この自主規制の仕組みには認証手続を設け、IFAIの支援によって経済省が策定するガイドラインに基づき認証が行われようとしている。このような仕組みはプライバシー・ポリシーを公表し、それに基づく適切な個人データの取扱いの政策やプログラムを実現しうるものである。そして、2012年8月15日には「民間が保有する個人データの保護に関する連邦法第44条に基づく拘束力ある自主規制の仕組みの適切な策定に向けたガイドライン草案」が公表され、2013年1月17日にはこのガイドラインが公表された。このガイドラインに基づき、認証の仕組みが策定されることとなっている。

【ヒアリング結果】

- メキシコの状況はデータ保護について遅れている（somehow late）が、APECはある種の法の間を行く新たなアプローチに着目しているとともに魅力的である。これに対し、EUのデータ保護の枠組みは非常に厳しく、市場に対する制約となっている。データ保護については、アメリカのように自由市場に任せ、消費者保護をしている例も見られる。APECで行っているのはこの中間に位置付けることができ、Accountability Agentなどを用いて実践的な方法でデータ保護の責任分担をしている。しかし、APECは執行に問題が残されていると見ている。
- CBPRへの参加国になろうとしたのはAPECに加盟した時点から検討をしていた。メキシコにとってはAPECのアプローチは重要であり、国際的な認知度（international recognition）を高めるためにも決断した。周知のとおり、EUの十分性を得るのは長い道のりである。一方で、データ保護について無政府状態だと思

[21] 33rd International Conference of Data Protection and Privacy Commissioner's, November 2-3, 2011. 筆者はこの会議の総会セッション" The Factors Driving New Data Protection Laws"において発表した。同会議の様子については、金融情報システムセンター「個人情報・プライバシー保護の国際的動向とわが国番号制度を巡る動き」『金融情報システム平成24年春号』（2012）30頁、参照。

われるのは困る。国際的な認知のためには、ある種の認証プロセスは重要であると考えた。

・ APECの取組の中ではAccountability Agentについて最も貢献できると考えている。ただし、APECの説明責任機関の今後についてはまだ知ることができない。

(2) OECDプライバシーガイドライン改正への対応状況

メキシコはOECD加盟国であり、法はOECDプライバシー・ガイドライン等を基盤にしている。また、2011年11月1日には「プライバシー枠組みの現在の進展：グローバルな相互運用性に向けて」というOECD会議をメキシコシティにおいて開催した[22]。

【ヒアリング結果】

・ OECDプライバシー・ガイドラインの改正については、これまでもコメントしてきた。また、児童オンラインプライバシーについて特に興味がある。

(3) 欧州評議会第108条約現代化への対応状況

メキシコは欧州評議会の加盟国ではないものの、欧州評議会第108条約現代化の審議過程では、2012年6月6日～8日に開催されたOctopus Conferenceにおいてコミッショナーがメキシコの「データ保護及びサイバー犯罪の課題」というテーマで発表している[23]。

【ヒアリング結果】

・ メキシコは外務省を通じて条約への明確な参加の意図を表明した。第108条約への加盟については政治的・外交的な問題でもあると考えている。

(4) 欧州一般データ保護規制提案への対応状況

メキシコは欧州連合の加盟国ではないものの、欧州委員会主催のワークショップ等に参加してきている。例えば、2008年10月21日、欧州委員会主催の「個人データの国際移転に関するワークショップ」にコミッショナーが「メキシコのデータ保護の情勢」について発表している[24]。

---

22 OECD Conference, Current Developments in Privacy Frameworks: Towards Global Interoperability, November 1, 2011.

23 Council of Europe, Octopus 2012 Resources; Commissioner Sigrid Arzt, Data Protection and Cybercrime Challenges, June 6-8, 2012. Available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_octopus2012/presentations/Opening_sigrid_arzt.pdf

24 European Commission, Workshop on International Transfers of Personal Data, October 21, 2008. EU 加盟国以外に、日本のほか、カナダ、イスラエル、メキシコ、アメリカにおけるデータの移転状況に関するセッション（Regional Approaches to Data Protection and Transfers of Personal Data at International Level）が設けられ、筆者はこのセッションのモデレーターを引き受けた。

【ヒアリング結果】

- 十分性審査については外交・政治問題であると考えている。
- 忘れられる権利やポータビリティの権利については現時点ではメキシコ法への導入はないだろう。

(5) 貿易協定等への対応状況

メキシコは貿易協定等について、次の主な枠組みに参画し、個人データ保護について必要な対応を行っている。特に EU－メキシコ貿易協定は、メキシコの個人データ保護法の制定の背景にあり、メキシコの個人データ保護の諸施策にも重大な影響を及ぼしている。

- 世界貿易機構（WTO：World Trade Organization）
  WTO の加盟国としてプライバシー保護について必要な措置を講じる義務がある。

- 北米自由貿易協定（NAFTA：North America Free Trade Agreement）第 9 章において、一定水準の権利保障を謳っており、加盟国はメッセージのセキュリティ及び機密性を保障することと通信ネットワークやサービスの利用者のプライバシーを保護することを規定している（第 907 条、第 1302 条)。他方で、加盟国間での商品またはサービスに直接的又は間接的に影響を及ぼすおそれのある不必要な障害を除去することが規定されている（第 904 条第 4 項)。そのため、「NAFTAのこのような規定はNAFTA加盟国間に対し、この地域における貿易の制限や非関税障壁をもたらす厳格なプライバシー及びデータ保護の立法及び規制を制定することを妨げている」 [25]と考えられている。

- 北米の安全及び繁栄のためのパートナーシップ（SPPNA：The Security and Partnership of North America）
  2008 年 2 月 22 日には加盟国が北米における情報及び貿易の自由な流通に関する声明に署名しており、越境データ流通に関する委員会が設置された。同委員会は個人のプライバシーの効果的な保護の促進と国境を越える電子商取引及びオンライン貿易の流通を統一化することを目的として、APEC 及び OECD の枠組みを補完するものとされている。

---

[25] MARTIN, *supra* note 2, at 259.

・ EU－メキシコ貿易協定（Economic Partnership, Political Coordination and Cooperation Agreement between the European Community and its Member States, of the one part, and the United Mexican States, of the other part）

欧州連合とメキシコは2000年10月1日に経済連携、政治的調整及び協力協定を発効している。この協定の第51条はデータ保護について規定している。

1. 当事者国は、関係する国際組織及び共同体が採択する基準を遵守し、個人及びその他のデータの処理の高い水準の保護に従うことに同意する。
2. そのため、当事者国は本協定の一部を成す付属文書において参照された基準を考慮に入れることとする。

付属文書（第51条において参照されるべき個人データ保護）

―国際連合電子計算機処理に係る個人データ・ファイルに関するガイドライン（1990年12月14日）

―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OECD理事会勧告（1980年9月23日）

―個人データの自動処理に係る個人の保護に関する条約第108号（1980年9月17日）

―個人データ取扱いに係る個人の保護及び当該データの自由な移動に関する欧州議会及び理事会の95/46/EC 指令（1995年10月24日）

さらに、同協定第41条には、データ保護に関する協力という項目を設け、技術支援を含むデータ保護の協力関係の構築に一致する条項が置かれた。

この協定によって、メキシコがEUデータ保護指令第25条に基づく「十分な水準の保護措置」を講じている国であるとはみなされていないものの、メキシコ国内のデータ保護の水準を高めるよう実質的に「強制させた」協定とみることができる[26]。

【ヒアリング結果】

・ EU-メキシコ貿易協定の影響として、民主的な条件として基本的人権へのコミットメントをメキシコに求められたことによる。EU との貿易協定は米国の貿易協定の考え方とかなり違う。EU-メキシコ貿易協定がデータ保護の法制化のひとつのきっかけになったことは確かである。

[26] Cristos Velasco San Martin & Maria Elena Perez-Jaen Zermeno, *An Update on the Status of Privacy and Data Protection in Mexico*, November 2009 at 3.

3. 個人情報保護に関する認証制度

(1) 制度制定の経緯

2013 年 1 月 17 日「民間が保有する個人データの保護に関する連邦法第 44 条に基づく拘束力ある自主規制の仕組みの適切な策定に向けたガイドライン」（以下「ガイドライン」という。）が公表された（2013 年 1 月 18 日施行）。このガイドライン第 5 章には「個人データの保護に向けた認証制度について」という認証制度の実施に関する記述がある。なお、同ガイドラインについては、2012 年 8 月 15 日に草案が公表され、その後一部修正の上 2013 年 1 月 17 日に IFAI が公表している。

(2) 制度の概要

ガイドライン第 5 章には「個人データ保護に向けた認証制度について」が示され、法に基づく認証制度に関する詳細が記述されている。認証制度は次の 4 つのレベルで実施されることとなっている。

① 認定団体を承認するための IFAI
② 認証付与を行う認定団体
③ 一定の水準を満たした管理者又は処理者に対する認証授与事業者
④ 個人データ認証を受けた管理者又は処理者

IFAI はデータ管理者や処理者に対する認証を直接行うのではなく、認証を付与する団体が適切な付与を行っているかその適正な手続を監視する役割を果たすこととされている。

ガイドライン第 4 章には「認証付与者及び認証」について認証付与者（IFAI から認定される団体）の権限、義務及び運用基準とともに認証に関する要件が定められている。認証を付与する者は、①氏名と所在、②データ管理者又はデータ処理者の認証の付与、維持、拡大、減少、停止、回復、取消しに関する詳細な手続及び条件、③財政的・技術的構造及び十分に資質ある職員、④想定される利害関係に関する公正さを証明する要素の開示、⑤秘密保持に関する概要、⑥管理システムをそれぞれ示さなければならない。認証付与者の主な権限・義務としては、①データ管理者又は処理者の認証の付与、維持、修正、停止、取消し、②認定に関する諸条件の遵守、③IFAI 又は認定団体による活動の監査、④認証を受けた管理者又は処理者に対する監視の継続、⑤当事者が提出する苦情解決の手続、⑥年次報告書の提出と公開、⑦利害関係の回避と中立性・独立性の維持、⑧管理システムの運用、⑨認証付与の定期的な更新が含まれる。

また、ガイドライン第 3 章には「認定団体及び認証の認定」について定められている。IFAI が認定する団体については、一定の要件を満たさなくなった場合、認定の停止及び取消しをされることとなる。そのため、APEC における Accountability Agent として列挙される前にメキシコの規制に基づき認定の停止及び取消しがされ得ることとなる。

(3) 制度の運用状況

ガイドライン公表後９か月間は認証の受付を行わず、制度の周知と広報啓発活動に努めることとされているため、2013 年３月時点で IFAI から認定された団体や認証を受けた管理者及び処理者は存在しない。

なお、IFAI の個人データ保護担当局の中には自主規制を監督する課が設置されており、認証制度の運用状況を監督するものとされている。

メキシコインターネット協会が提供するオンライントラストマーク（Sello）については、2009 年９月時点で 315 社がトラストマークを付与されている。トラストマークの付与には同協会による審査を経て１年間（2320 ペソ：約 19,000 円）を支払うこととなる。

【ヒアリング結果】

- IFAI では段階的に自主規制を行っているところである。2013 年 11 月を目途として２段階のレベルで認証制度の作業部会の検討を開始したところである。自主規制レジームは始まったばかりである。
- 自主規制に興味を持っている団体と話し合っているが、認証の受付開始は７月を予定し、10 月以降に実際の認証を開始していく予定である。認証に関する研修や監査を実施していくよう準備している。
- ガイドラインに基づく自主規制は政府と民間による一種の共同規制である。IFAI が認証機関を認定し、経済省による支援とともに認定機関が認証プロセスを監督し、認証機関がデータ管理者に認証を行う仕組みである。IFAI も経済省も認証をしない。将来的には経済省が APEC の認証プロセスに参加することを表明する可能性があり、コンタクトポイントして機能することになろう。
- ガイドラインには経済省が関連する点について、米国では執行するのは全くの自主規制だが、メキシコでは規制について Accrediting Entities がアセスメントする点で異なる。Accrediting Entities はまだないが、この機関が Accountability Agent を監視する。10 月まで Accrediting Entities を募集しており、今後どうなるかは未定である。すでにいくつかの事業者は Accrediting Entities に興味を抱いており、問合せが来ている。
- BCR との相互運用については、メキシコの制度とマッチングの作業が必要である。CBPR と BCR とではギャップが存在すると考えており、仮にそのギャップがあるとすればそれが何であり、そのギャップに対してどのような対策を練るかについて検討する。

4. 個人情報保護の施行状況

(1) 利用実態・苦情処理・紛争解決

インターネットの利用者は 2011 年時点で 4060 万人（全人口の約 37%）となっている。スマートフォンによるインターネットアクセスは利用者の 58%にのぼっている。インターネット利用者の利用内訳は、ソーシャルネットワーク（79%）、オンラインバンキング（65%）、オンラインショッピング（62%）となっている。ソーシャルネットワークにおけるプライバシー設定をしている者は 76%となっている。

公的部門については、連邦レベルにおいて 3,097 のデータベースが登録されており、そのうち 97%が ID に関する単純な情報を含むにすぎず、残りの３%がセンシティブ・データを蓄積している。

IFAIの近時の申立受付件数等については次の表のとおりである[27]。最も多くの申立てを受けたのは社会保障機関に対するものであり（2003 年６月から 2011 年６月までで 104,847 件：全体の 15.5%）、続いて公的教育省（31,162 件：4.6%）、財務省（22,821 件：3.4%）。申立内容の内訳として、個人データのアクセス・訂正の申立てについて 2003 年度は全体の 5.0%であったのに対し、2011 年度には 19.9%に増加している。また、2003 年から 2011 年までの間に 36,971 件が連邦行政機関に不服申立てをされている。

類型	2003-06	2007	2008	2009	2010	2011(june)	合計
オンライン申立	163,156	92,261	102,297	114,179	118,367	61,807	652,067
書面申立	9,013	2,462	2,953	3,418	3,771	3,206	24,823
合計	172,169	94,723	105,250	117,597	122,138	65,013	676,890
オンライン回答	145,417	81,439	89,092	97,642	103,869	6,826	66,002
書面回答	7,668	1,948	2,328	2,880	3,273	512	6,194
合計	153,058	83,387	91,420	100,522	107,142	7,338	593,094
IFAIへの申立	8,238	4,864	6,053	6,038	8,160	3,618	36,971

【ヒアリング結果】

- 年間約 4600 件は機械的に５人のコミッショナーに割り当てられる。
- 申立てはオンラインでできる。情報公開は匿名でもできるので、「ミッキーマウス」からの申立てもある。個人情報保護は匿名での申立ては不可。

---

27 IFAI, *Introduction to Federal Institute for Access to Information and Data Protection*.

・　スマートフォンのプライバシーやSNSなどの問題はまだ深く扱っていない。最近問題になっているものとして、犯罪に携帯が使われるので、携帯の利用を登録制にしようというものがある。今ではプリペイド携帯を買う場合も登録が必須。ただし、登録した情報の管理についてはまだ議論がある。
・　選挙人名簿が売られるというのも問題視されている。

(2) 権限行使（報告の徴収、勧告、命令、立入検査、罰則等）

権限行使の統計については公表されていないが、主な執行例についてはIFAIのホームページ上に公表されることとなる。

【ヒアリング結果】
・　近時のものとして目的外利用の個人データの削除を求める事案について2012年1月に執行した例（制裁金100万米ドル、120万米ドルなど）がある。本件は不服申立てされてしまった。

(3) 広報啓発活動

2012年までに4つの勧告・ガイドラインがIFAIによって公表され、広報啓発活動が行われてきた。

① 個人データ責任者又は担当部署の設置勧告
② プライバシー取扱通知に関する実践的ガイド
③ アクセス、訂正、停止又は異議申立ての権利の要請に応えるためのデータ管理者の実践的ガイド
④ データ保護の諸権利を行使するための実践的ガイド

【ヒアリング結果】
・　プライバシー取扱通知については、特に広報啓発を重視している。また、IDカードの扱い等は注意を呼び掛けている。

5. 参考：メキシコについて（外務省基礎データより）

【一般事情】

1. 人口　　１億 137 万人（2011 年 IMF）
2. 面積　　196 万平方キロメートル（日本の約５倍）
3. 首都　　メキシコ・シティ
4. 民族　　欧州系（スペイン系等）と先住民の混血（60%）、先住民（30%）、欧州系（スペイン系等）（９%）、その他（１%）
5. 言語　　スペイン語

【政治体制・内政】

1. 政体　　立憲民主制による連邦共和国
2. 元首　　エンリケ・ペニャ・ニエト大統領（2012 年 12 月１日就任、任期６年、再選不可）
3. 議会　　二院制（上院 128、下院 500 議席）
4. 行政府　制度的革命党（PRI）政権（中道左派）

【経済】

1. 主要貿易相手国

   1994 年の NAFTA 締結以降、米国との経済関係が強まり、輸入全体の約 49.6%、輸出全体の約 78.5%を米国が占める

2. 経済概況

(1) メキシコは 1990 年代前半に APEC 参加（1993 年）、NAFTA 発効（1994 年）、OECD 加盟（同年）を実現。1994 年 12 月に通貨危機が発生。その後、深刻なリセッションを経験するも、危機を境に生じたペソ安により貿易収支が黒字に転化。GDP 成長率も 1996、1997 年は５%超の高成長を記録。1999 年及び 2000 年には、好調な米国経済と石油価格高騰を背景に輸出が拡大。

(2) 近年の実質経済成長率は、2005 年 3.2%、2006 年 5.2%と好調に推移。2007 年以降は米国経済の悪化を受けた自動車など輸出製造業の不振等の影響で 3.3%、2008 年は 1.2%と低下。2009 年は、世界的な経済危機の影響により、-6.2%となったが、2010 年は 5.5%に回復。2011 年は 3.9%となった。

【二国間関係】

2002 年 10 月、ロスカボスにおける日墨首脳会談で日墨経済連携強化のための協定（EPA）の締結交渉を開始することで合意。同協定は、2011 年２月に実質合意に達し、これを踏まえた改正議定書が 2012 年４月に発効した。

vi. コスタリカ ※

1. 個人情報保護法制

(1) 新法制定（法改正）の経緯

a 一般的概要

コスタリカ憲法は 1949 年に採択され、18 章 197 条から成る。そして、コスタリカが自由かつ独立した民主共和国であることを謳っている（第 1 条)。コスタリカは 1821 年 9 月 15 日にスペインから独立し、以後、いくつかの憲法が制定されたが、1871 年憲法をもとに現在の 1949 年憲法が施行されている。最高法規としてのコスタリカの憲法は、国民の投票によって統治者を選出するリベラルな民主政体であるとされ、法の支配の原則を遵守している。立法府（一院制）[28]、行政府、司法府（最高裁判所の小法廷の中には憲法裁判を専門的に取扱う機関も存在する。）の三権が分立されている。コスタリカの基本的人権は「被治者の権利を侵害すると同時に憲法を侵犯するいかなる権力行為からも、被治者を保護する訴訟制度」としての「アムパーロ（amparo)」訴訟 [29]によって保障されてきた。なお、コスタリカは 1969 年同国において米州機構によって制定された米州人権条約（American Convention on Human Rights）に批准しており、世界人権宣言（the Universal Declaration of Human Rights）及び市民的及び政治的権利に関する国際規約（International Covenant on Civil and Political Rights）とともに国内の法制度に適用可能となっている。

※　本稿の執筆に当たり、コスタリカ国会 Juan Carlos Mendoza 国会議員（Citizen's Action 党)、国会事務局 Ricardo Ruiz Gonzalez, Departamento de Relaciones Publicas（広報部）Beatriz Obando（人権国際委員会事務局)、コスタリカ法務平和省 Diana Chinechilla (Chinchilla) Nunez（法律相談役（Asesora Juridica))、コスタリカ最高裁判所 Olman Rodriguez (最高裁判事調査官 (Le Traolos))、Luis Arolon (最高裁判事調査官（Le Traolos）)からヒアリングを実施することができた。また、ヒアリングに際して様々なサポートをしてくださった在コスタリカ大使館大野参事官及び長野派遣員、また法務平和省におけるヒアリングで通訳を担当していただいた上田晋一郎氏にもこの場を借りて謝意を申し上げる。最後に、コスタリカでのヒアリング調査に随行し、豊富な資料を提供していただくともに、本稿に的確なコメントを頂戴した板倉陽一郎弁護士（ひかり総合法律事務所）の御厚意にも御礼申し上げる。

28　コスタリカ議会におけるヒアリングによれば、2013 年 3 月現在の定数は 57 名。被選挙権の要件は 21 歳以上、国籍等。任期は 4 年だが、 4 年の待機期間を経なければ再任は不可能。毎年 5 月 1 日に通常国会が開催され、議長を決めるセレモニーが行われる。女性議員比率を高めるように定められており、2013 年 3 月現在 57 名中 22 名が女性。これまで投票率は従来高く、1998 年には 80%であったが、汚職を批判するキャンペーンを受けて、2010 年には 40%に低下しており、国民の間で特定の支持政党がなくなりつつある。

29　杉原泰雄編『新版体系憲法辞典』（青林書院・2008）260－1 頁〔北原仁〕、参照。

コスタリカは福祉国家の理念を掲げ、人間の尊厳や全ての人間が平等であるというキリスト教の原則から、財産や自由よりもむしろ平等の恩恵を重視し、雇用、社会保障、労働者の訓練等の国家による社会の保護活動が広く容認されてきた[30]。また、コスタリカのみならず他のラテンアメリカ諸国に共通することとして、憲法の成文化の過程において根源的にはアメリカ合衆国の影響を受けているものの、憲法はヨーロッパ、特にスペインやラテンアメリカの文化とも融合されてきた[31]。

なお、1948 年 12 月 1 日には、当時の事実上の大統領であった José Figueres Ferrer が軍隊を永続的な組織としてはこれを廃止し、憲法第 12 条（「永続的な組織としての軍隊は廃止する。監視及び公の秩序の維持のための必要な警察権力を有することとする。」）に明文化されている。

また、データ保護法の制定に伴い、国会での審議については、大きな異論がなかったとのことである。

【ヒアリング結果】

（国会事務局）

- データ保護法については、法案が提出されたのが 2007 年 11 月、成立したのが 2011 年 7 月であるが、更にその後見直し期間に修正法案が特別委員会である人権委員会で審議されてきた。
- 法案の審議において強い反対はなかったと記憶しているが、唯一、Citizen's Action 所属の Juan Carlos Mendoza 議員からは反対の意見があった。

（国会議員）

- データ保護については必ずしも専門としておらず、議論もまだ新しいものばかりである。情報公開との関係以外の観点においては、データ保護法については特段の知見を持たないが、データ保護は人権委員会において新たな技術に伴う通信の違反として考えられている問題として見ている。
- データ保護法に反対したのはよりオープンな政府を要求する情報公開との関係で問題があると考えたからである。
- データ保護法について、各政党により見方の違いはある。これは、情報公開との関係で、どの程度公開するのかという点においてである。

---

30 *See* Ruben Hernandez Valle, *Costa Rica*, in CONSTITUTIONAL LAW: INTERNATIONAL ENCYCLOPEDIA OF LAWS 21-23 (2000). また、コスタリカ憲法の邦語による紹介として、「コスタリカ・カナダにおける憲法事情及び国連に関する実情調査：概要」（参議院憲法調査会事務局・2004）、参照。

31 Olman A. Rodriguez L., *The Costa Rican Constitutional Jurisdiction*, 49 DUQUESNE L. REV. 243, 245-6 (2011).

b 憲法第 24 条[32]

データ保護ないしプライバシーに関する規定として、第 24 条において次のとおり定められている。

憲法第 24 条 第 1 項　親密、通信の自由及び秘密性への権利は保障される。 第 2 項　共和国の住民の私的な文書及び書面、口頭またはその他の通信は不可侵である…。

同時に、第 28 条は「道徳ないし公の秩序を害しない、又は第三者にいかなる損害ももたらさない私的な行為については、法の適用の範囲外にある」という規定とともに一定の私的な行為が法的に保障されている。このように、第 28 条と相まって第 24 条は親密の権利を明文化しており、この規定からプライバシーの権利及びデータ保護の権利が認められると解されている。このようなプライバシーの圏域を法的に保障する背景には、人格を密接に関係した権利を尊重すべきであるとの観点とも結びつき、第 33 条が保障する人間の尊厳の原理が基盤にあるものと考えられている。

また、親密の権利は、個人として自らの行為が尊重されるのみならず、家族の構成員としても尊重されるとされており、厳密に個人的な権利であることから、法人に適用されることはできない。

親密の権利は、各人のイメージの権利をも保障している。各人は自らのイメージの利用に関する決定を行う権限を有し、自らの同意なしにイメージを利用されることにつき異議申立てを行うことができる。また、民法第 29 条は公共の利害に関する場合等を除き「人の写真又はイメージをその人の同意なしに再生産、展示、売却することはできない」と規定し、自らのイメージについて本人の同意を強調している。

次に、第 24 条は私邸の尊重の権利をも包含していると解される。私邸には法的な占有者の同意なくしていかなるものも侵入することが禁止されており、プライバシーの不可侵性を反映している。公共の安全や公衆衛生等の理由に基づき私邸への侵入が認められる場合があるが、詳細については刑事訴訟法及び衛生に関する一般法によって規定されている。

さらに、第 24 条からは私的な通信の尊重が導き出される。ここで通信の秘密とは、他者からの通信の内容を傍受し、または違法な捜索を行うことを禁止することを意味する。憲法で通信の秘密が明記されることによって、通信の自由が黙示的に保障されているとも考えられている。そして、私的な文書及び通信には、写真、テープ、ディスク、マイクロフィルム等のその人を象徴する私的な財産を含む。

32　第 24 条の法的性格については、コスタリカ最高裁判所でのヒアリングを基に Valle, *supra* note 3 を参考にした。

【ヒアリング結果】

（最高裁判所）

- コスタリカのデータ保護の権利は、憲法第 24 条の親密への権利（the right to intimacy[原語：derecho a la intimidad]）に基づき保障されてきた。個人データ・私的な情報保護に関する判例は多く存在する。1989 年の憲法裁判所の設置に伴い、1990 年代になり憲法上のデータ保護の権利が首肯されてきた。データ保護の権利は憲法裁判所においては確立した人権である。
- 初期の判例としては、刑事罰を科された者が 10 年後にもデータベースにおいて自らの前科が残されていたことについて、刑事司法のファイルに関する制定法に基づきデータからの削除を認めた例（1999 年 7 月 27 日判決 No.5802-99）がある。
- データ保護の権利は、第 3 世代権利として位置付けられている。すなわち、人権は第 1 世代の投票権を中心とした民主的な権利、第 2 世代の社会権、そして第 3 世代の普遍的な権利に区分されるが、このうちデータ保護の権利は第 3 世代であるとみなされてきた。
- 憲法裁判所は非常に明確に個人データ保護の権利を基本的かつ普遍的な権利として擁護してきた。憲法で列挙されている親密への権利から個人データ保護への権利と拡大してくる過程の中でも、裁判所による立法行為といった批判はあたらず基本的かつ普遍的な権利の名の下に認めてきた。
- 1990 年代以前については、憲法裁判所ではなく、通常の裁判所において処理されてきた。しかし、個人データを正面から保障してきたとまではいえない。
- 1999 年の判決によりデータ保護の権利が確立した。また、重要な判例として 2005 年の憲法裁判所の判決（2005 年 7 月 5 日判決 No.2005-8894）が存在する。本判例では、「許される権利（the right to forgiveness）」が認められた。具体的には、過去の債務返済に関するコスタリカ銀行履歴によって、口座の開設が認められないことはデータ保護の権利を侵害すると認めたものである。
- データ保護への権利は第一次的には裁判所による判例の蓄積により保護されており、データ保護の立法は二次的なものである。
- 選挙最高裁判所によって科された事例（2005 年 7 月 7 日判決 No.8799-05）では、情報の公私区分が問題とされ、どこまでが公開情報として認められるかどうか議論になり、裁判所内部でも意見が割れた。
- データ保護の権利は、憲法上の権利と民事上の権利とで分けられているが、同等の内容である。私人であっても公的な権力を行使しているとみなされる私人（例えば、銀行）に対しては憲法裁判所で審理される。
- プライバシー権についても他の憲法の条項と同じく、スペインやアルゼンチンの影響があるものの、これらの国の判決や法令等が具体的な判決で言及されたことはない。もっとも、「開かれた」条項である憲法第 48 条によって、国際的規約を引用す

る可能性は十分にあり得る。EU データ保護指令や国連の個人データ処理に関するガイドラインへの言及を行った判決はすぐには思い当たらないが、これらの国際的文書を参照することは可能性としてあり得る。

c その他の条文

このほかに、憲法第 29 条の情報への権利（the right of information）には公表の自由、書面以外の方法による情報の自由、情報へのアクセス権、そして「訂正ないし応答の権利」が含まれると解されている。この「訂正ないし応答の権利」は米州人権条約第 14 条に基づき不正確あるいは攻撃的な発言によって侵害を受けた者が応答する権利ないし同一の手段を用いて訂正する権利を認めているものである。また、第 30 条では情報の公開に関する規定が置かれている。

憲法第 30 条 行政機関に対する自由なアクセスは公的利益に関する事柄の情報の入手を目的とする場合保障される。

【ヒアリング結果】

（国会議員）[33]

- コスタリカでは情報公開が人権としてまで認められているかというと、難しい。現状では憲法のほか、ごくわずかな立法でしか情報へのアクセスが認められていない。国土安全や外交といった政府の秘密は守られなければならないが、その他の情報については市民には可能な限りオープンでなければならない。これは憲法 27 条に基づくものであり、情報公開の請願の範囲は広汎であると考えている。
- コスタリカにおいても情報公開は取り組まなければならない問題であるが、他国に比べて数年遅れている。

（最高裁判所）

- 憲法第 30 条では公的情報へのアクセスを認める権利が規定されており、親密な権利を保障する憲法第 24 条としばしば対立する。憲法裁判所はどちらの権利が優位するかという形で議論をせず、注意深く両者の権利を衡量してきている（2006 年 5 月 10 日判決 No.6314-06）。
- 財務省が所管する社会保障制度は非常に厳格に個人データが保護されているが、社会保障に関する支払のデータについて本来データが秘密性のあるものとみなされて

33　ヒアリングをさせていただいたのは Juan Carlos Mendoza 国会議員である。サンホセ選出、1975 年 7 月 7 日生まれ。コスタリカ大学コミュニケーション修士課程在学中、B.A.（政策科学）。2011 年～2012 年議院議長。常任委員会（経済問題）所属、特別委員会（治安及び麻薬問題、人権）所属。Citizen's Action に所属しており、2010 年には党首を務めた。2010 年には大統領選にも出馬している。

いるものの、新聞社等はそれが公開情報であると主張している事例も見られる。公的情報であるか私的情報であるかの線引きは非常に難しいものがある。

(2) 個人情報保護法制

a 法律名

個人データの取扱いにおいて個人を保護する法律（Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales）[34]

全 10 章、90 か条の条文から成る。

2011 年 7 月 7 日成立、2013 年 3 月 8 日施行

【ヒアリング結果】

（データ保護機関）

- 2011 年 7 月に個人データ保護法が制定された。しかし、同法は暫定的なものであり、一年後に見直しが行われることとなっていた。2012 年 3 月に見直し期間が終了し、2013 年 3 月 8 日から同法が施行されることとなった。
- 国際社会において個人情報保護制度の重要性がいわれており、国として重要性を認識して法制度化された。
- いろいろな国の法律を参考にしたが、主にスペインを参考にした。アルゼンチンをはじめとする他のラテンアメリカ諸国の制度も参考した。ラテンアメリカ社会ではラテンアメリカ諸国内の他国で先進的な取組をしているものは参考にするということがある。EU データ保護指令は参照しておらず、あくまでスペインの法制度を参考にしてきた。
- 国会で議論がなされ、成立するまで経緯が長く、EU データ保護指令も参照したかもしれないが、その後、形式面においてかなり変更されている。
- 立法過程においてスペインデータ保護機関から直接の訪問があったかどうかは不明である。一般的には、他国の法律を入手・調査し、コスタリカの国柄に合うように調整していく。
- 現在、国民としてもデータ保護への期待が感じられる。法律ができたことをアピールしていこうと思っている。政府機関としても、これからしっかりと浸透させていく予定である。

（最高裁判所）

- データ保護法は2011年に成立したばかりであるが、憲法裁判所による判例を補強し、裁判所を大いに助ける道具となり得ると考えている。

---

[34] 2013 年 3 月 5 日公表（Publicado en el Alcance Digital n.° 42 a La Gaceta n.° 45 de 05 de marzo de 2013）のものが最新版である。*See* http://www.tse.go.cr/pdf/normativa/reglamentoleyproteccionpersona.pdf

b 目的

人ないし財産に関するデータの自動若しくは手動による処理に関する自由並びに平等の擁護及び人の生活、私的活動並びにその他の私的権利に関する情報における自己決定の権利の保障を法目的としている（第1条）。

情報自己決定の権利とはいかなるデータベースにおいても自らのデータについて知る権利を意味し、必要に応じ、訂正や削除を要求することのできる権利である（第12条）。

【ヒアリング結果】

（データ保護機関）

・ 目的規定に示されているとおり、データ保護法は基本的人権に関する法律と位置付けられている。

（最高裁判所）

・ データ保護法においては情報の自己決定権（right to self-determination in information[原語：derecho a la autodeterminación informativa]）（第1条・第12条）という言い回しが用いられているが、スペインあるいはアルゼンチンの影響を受けているものと考えられている。定義についても両国の法制に近いものが多い。ちなみに、データ保護機関の名称はスペインのものとほぼ同様である。

c 適用範囲

官民による自動処理・マニュアル処理が対象（第3条）

保護の対象は「識別された又は識別することができる生存する個人に関するいかなるデータ」と定義される「個人データ（Datos personales）」である（第3条(b)）。個人データの定義は日本とほとんど変わらないが、容易照合性の要件がない。

d 適用除外

信用履歴に関する金融制度に関する特別の規制については法が適用されない（第3条）。また、統計、歴史、科学の研究に用いられ、リスクが生じないデータベースについては、データ主体の削除権が認められていない（第26条（e））。

e 権利・義務の内容

・ データ主体の権利について

- 同意（Consentimiento）
  個人データの処理には一定の場合を除き本人の自由かつ明確な同意が必要とされる（第2条（f）・第4条・第5条）。また、データ主体は自らの同意を撤回することができる（第7条）。
- 忘れられる権利（Derecho al olvido）

法令で定められている場合や当事者の合意がある場合を除き、個人データの保有は10年以内とする（第11条）。

- アクセス権（Derecho de acceso a la información）（第21条）
  データ主体は自らのデータ及び個人データの取扱いに関する条件・目的・概要へアクセスする権利を有する。なお、このアクセス権を認めないデータ管理者は書面によってその理由を明示しなければならない（第22条）。
- 訂正権（Derecho de rectificación）（第23条）
  データ主体は自らのデータが不正確であった場合には訂正する権利を有する。
- 削除権（Derecho de supresión o eliminación）（第25条・第26条）
  データ主体は、法令に基づく場合や公共の安全、あるいは一般に利用可能な制限なくアクセスできる情報が取得されるなどの場合を除き、いつでも自らのデータを削除・消去する権利を有する。

なお、アクセス権、訂正権、削除権については、データ主体の申請から5営業日以内に処理しなければならない（第18条）。また、データ主体は電子媒体を含む単純で適切な方法によって自らの権利を行使しうるものとされている（第16条）。

【ヒアリング結果】

（最高裁判所）

・ 個人データの削除を裁判所が命ずることができるかどうかについては非常に難しい判断を迫られてきた。一例として、司法による判決は氏名を含め公開されており、氏名がウェブサイト上に出てきたからといってただちに個人データの消去が認められているわけではなかった。しかし、多くの人からの苦情が出てきたことから、判決における個人データの公開の原則は改められた。特に未成年者の個人データが判決文に含まれる場合は自動的に判決文の中で保護されるようになった。

・ 事業者の義務について

- 安全管理措置
  法第4章（第27条～第39条）において利用目的の範囲内の利用や安全管理措置等に関する詳細な義務規定がある。具体的には、クラウドにおける利用を含む個人データの処理・蓄積に関する記述やデータ取扱いのリスク分析の実施が要求されている（第27条、第36条）。さらに、データ管理者には執行可能なプライバシー・ポリシーの策定、研修の実施、内部監査の実施等が義務付けられている（第32条）。

・ データ漏えい通知義務
  データの漏えい等のセキュリティの脆弱性が発覚した場合、5営業日以内にデータの所有者に対しデータ漏えい等の事実を通知しなければならない（第38条）。その通知の内容には、（a）漏えい事故の性質、（b）個人データ、（c）事故後に直

ちに採られた措置、(d) 対応窓口（情報を入手できる方法と場所）を含むこととする（第 39 条)。

f 届出・登録制度

- 登録

データベースを所有する者はデータ保護機関への登録が必要である。データ保護機関への登録の申請には、データ管理の責任者、連絡先、データベースの場所、利用目的、取扱うデータの類型、セキュリティ措置、データ移転の受領者等を示す必要がある（第 44 条)。

また、データベースの登録に際しては、事業の大きさに応じて登録料をデータ保護機関に支払わなければならない（第 83 条)。

さらに、データ保護機関は登録された事業者につき違反の疑いがある場合は検査することができる（第 46 条)。また、データ主体は所定の書式に基づき苦情処理の申立てを行うことができる（第 60 条)。

g 苦情処理制度

データ保護機関は苦情申立てについて決定を下すことができる（第 69 条)。

【ヒアリング結果】

（データ保護機関）

・ 2012 年から 2013 年 3 月までに正式な 40 件の苦情申立てを受けた(メール含む。)。このほかに、電話による苦情は 100 件ほどである。ソーシャル・メディアに関する苦情は今のところない。国民はまだこの法律を知らないが、この法律が浸透していけば、これから苦情の数は増加が見込まれる。

h 行政措置・罰則

罰則には比例原則（Pago proporcional）が採られている（第 80 条)。

【ヒアリング結果】

（データ保護機関）

・ 公務員の給与（俸給表上）をベースとして、最大 30 月分の給与額に相当する罰金が科されることとなる。軽微な場合は 5 か月分、より重大な違反は 5 ～20 か月分、最も重大な違反は 15～30 か月分の給与額に相当する罰金が科される。

（最高裁判所）

・ 3 種類の罰則規定が設けられており、18,000US ドルを上限として科料が科され得る。データ保護法違反に対する損害賠償の金額は憲法裁判所で審理を行わず、民事の裁判所において簡易な手続で審理されることとなっている。

ｉ その他

(a) センシティブ・データ

センシティブな個人データ（datos personales sensibles）についてはいくつかの規定があるものの、明確にどのような類型が該当するかについて規定されているわけではない。しかし、毎年データ保護機関の長がセンシティブ・データに関するセキュリティの措置の在り方について見直しをすることができることとなっている（第 37 条）。

【ヒアリング結果】

（最高裁判所）

- クレジット情報はセンシティブ・データとしてはみなされていない。クレジット履歴については、金融機関におけるセキュリティの観点から個人データとしても保護されない判決が下されている。
- SNS に関するケースは２件思い至るが、憲法裁判所ではなく、民事裁判所のものである。
- 制定法（データ保護法）は個人データを３種類のデータ - センシティブ・データ、制限的なデータ、無制限のデータ - に分けている。センシティブ・データについては、特に医療データが問題となる。判例においても、レイプの被害者の氏名が検索サイトで出でてきた事例、あるいは AIDS の母親の娘の病院での治療の報告書が公開され問題となった事例がある。

(b) 小規模事業者等への免除について

小規模事業者等への免除規定は存在しない。

【ヒアリング結果】

（データ保護機関）

- 法は官民に共通して個人情報を守るということで適用される。中小企業であっても法の義務を遵守しなければならない。法は個人を保護することを目的としており、中小企業を守るものではない。

(c) データの国外移転について

特別の定めはない。

もっとも、データの移転については、原則として本人の同意に基づきこれを行うことができる（第 40 条～第 43 条）。また、データ主体の同意なしにコスタリカに在住の国民または外国人の個人情報を第三国に移転した場合はデータ保護機関の調査対象となりうる（第 59 条（m））。

【ヒアリング結果】

（データ保護機関）

・　国外移転の規制に関する規定はないが、データ移転に関する一般的な規定を援用することができる。

（国会議員）

・　国際関係の専門も有しているが、越境データ移転については特に問題視はされていない。

(3) 監督機関

＊本節はデータ保護機関におけるヒアリングをもとに執筆している。

a 設置の経緯

正式名称は Prodhab：住民のデータ保護機関（Agencia de Protección de Datos de los Habitantes）。

法務平和省国立登記所（Registro Nacional）がこれまで一定のデータ保護業務を行っていたが、データ保護法に基づき新たな機関が設立された。

2011 年 7 月 7 日に成立、その後、準備期間があり、2013 年 3 月から正式に始動した。

b 制度の概要

(a) 法的地位

データ保護機関は法務平和省に属する機関だが、事務的には独立している。スタッフは公務員である。

(b) 所掌事務

個人データの取扱いにおいて個人を保護する法律の監督

(c) 組織体制

2013 年 3 月に始動したばかりであるが、30 名程度のスタッフが想定されている。

(d) 人事制度

現在のところ Arlene González Castillo が長（director）である。任命権者は法務平和省大臣で任期は 4 年である。しかし、現在の長は暫定的であり、法務平和省の意向により、交代する可能性もあるが、調整中である。組織ができたばかりであるためゴンザレスは継続できる可能性もある。

(e) 予算

予算は 550million コロン（約 1 億 500 万円（2013 年 3 月時点のレート））。

法律所定の業務（第 20 条）を全て行うと少ないと考えている。罰金はデータ保護機関には入ってこない。

法第 33 条及び第 34 条に基づくデータ管理者による登録料は予算計上することができる。データベースの内容によって入ってくる金額は異なるため、データベースのロイヤリティ等がどれくらいかは現時点では分からない。

(f) 権限

- 調査権限の行使は次のような場合に認められると規定されている（第 59 条）。
  - －データ主体への不十分な通知による個人データの取扱い
  - －安全性を欠いた措置による個人データの取扱い
  - －法に違反した個人データの移転
  - －利用目的を超える個人データの取扱い
  - －ファイル及びデータベースへのアクセスに関する不合理な拒否
  - －データ主体からの削除・訂正の要請に対する不合理な拒否
  - －データ主体の同意に基づかないセンシティブ・データの取扱い
  - －詐欺、暴力等による個人データの取得
  - －法に基づき機密性が要請されたデータベースの開示
  - －データ・ファイルに含まれた個人データの提供
  - －データ保護機関への登録をしないデータ処理
  - －データ主体の同意なしにコスタリカにある個人情報の第三国移転
  - －その他データ保護機関がデータ主体の権利が侵害されたと認める場合
- データ主体の権利を侵害すると考えられる場合、比例原則に基づき、データ保護機関は予防措置を命じることができる（第 64 条）。
- データ保護機関は苦情申立てについて決定を下すことができる（第 69 条）。この決定に対し、当該データ管理者は不服申立てを法務平和省に行うことができる（第 72 条）。
- 官民全ての機関・組織に対して権限行使が可能である。
- 法違反に対して必要があれば立入検査を行う可能性はあるが、警察とは異なり、実際にはデータベースの調査権限が主となる。司法府に権限を委譲させてから必要に応じて司法警察による立入検査をすることが考えられる。あくまでデータ保護機関は事務的な機関としての位置付けである。

(g) 他機関・地方との関係

地方部局はない。

(h) その他

広報資料は現在作成中である。施行されたばかりの法律なので、これからも他国の良いところを取り入れて行きたいと考えている。

2. 国際的なルールへの対応状況

(1) APEC-CPEA及びAPEC-CBPRへの対応状況

2013 年３月時点において、コスタリカは APEC のメンバー・エコノミーではないため、具体的な対応状況は見られない。

【ヒアリング結果】

（データ保護機関）

・ APEC における取組については、今から見ていく段階であり、法務平和省が決定していく事項であると考えている。コスタリカはよりよいものを取り入れていくことにはオープンである。

(2) OECDプライバシーガイドライン改正・欧州評議会第 108 条約現代化・欧州一般データ保護規則提案への対応状況

2013 年３月時点において、コスタリカは OECD、欧州評議会、EU の加盟国ではないため、具体的な対応状況は見られない。

【ヒアリング結果】

（データ保護機関）

・ OECD プライバシーガイドライン、欧州評議会第 108 条約については参考にしていない。
・ 国境を越えるデータの問題については、データ主体との間の同意が存在していれば問題はない。法第５条に基づき本人の同意に違反すれば罰則によって担保されている。
・ EU データ保護指令における十分性認定については知らなかった。データ保護機関の長であるゴンザレスは知っているかもしれない。
・ 国立登記所のデータベースの無制限な情報についてはだれでもアクセスでき、国外からもアクセスできるが、無制限な情報以外はきちんと制限されている。
・ コミッショナー会議への参加は予算次第であるが、将来的には正会員にもなりたいと考えている。
・ イベロアメリカ会議には、昨年のスペインの会合及びコロンビアでの会合に参加し、コスタリカの法律が賞賛された。

(3) 貿易・連合協定

米国との自由貿易協定である「米・中米・ドミニカ共和国自由貿易協定」が 2009 年１月に発行され、同協定の電子商取引章において、電子商取引分野におけるデータプライバシーに関連する立法、規則、施策に関する情報及び経験を共有すること重要性が明記されている（第 14 条）。同協定には特に具体的な国際的基準は明示されていない。

また、コスタリカを含む中米6か国（エルサルバドル、グアテマラ、ホンジュラス、ニカラグア、パナマ）とEUとの間で連合協定が2012年6月29日署名された[35]。この協定の中で「司法・自由・安全」という章において「個人データ保護」に関する規定が存在する（第34条)。協定締結の当事者は「最も高い国際基準に到達するまで個人データの保護の水準を改善する目的で協力すること」が明記されている。そして、具体的に参照すべき国際水準として、国際連合「電子計算機処理に係る個人データ・ファイルに関するガイドライン」（1990年12月14日）が例示されている。同ガイドラインは、各国が立法化すべき「最低限度の保障（minimum guarantees)」に関する諸原則（合法性及び公正さの原則、正確性の原則、利用目的の特定化の原則、アクセスの原則、差別禁止の原則、安全管理措置の原則のほか監督機関やデータ移転に関する規定を含む。）を示している。また、個人データの保護に関する協力には技術支援を含むものとされている。

3. 個人情報保護に関する認証制度

認証制度は存在しない。

【ヒアリング結果】

（データ保護機関）

- データ保護機関が実質的な活動を始めたばかりであり、現状認証を実施する状況にない。メキシコのマーク制度は知らないが、スペインのものは知っている。

4. 個人情報保護の施行状況

2013年3月8日に施行されたばかりであるため、具体的な施行状況については公表されているものはない。

35 EU and Central America sign Association Agreement, 29 June 2012. Available at http://trade.ec.europa.eu/doclib/press/index.cfm?id=815

5. 参考：コスタリカについて（外務省基礎データより）

【一般事情】

1. 人口　　約 472 万人（2011 年　世界銀行）
2. 面積　　51,100 平方キロメートル（九州と四国を合わせたほどの広さ）
3. 首都　　サンホセ（北緯 10 度　標高 1,200 メートル）
4. 民族　　スペイン系及び先住民との混血 95%、アフリカ系３%、先住民他２%
5. 言語　　スペイン語

【政治体制・内政】

1. 政体　　共和制
2. 元首　　ラウラ・チンチージャ・ミランダ大統領（2010 年５月～2014 年５月、任期４年、８年以上の間隔を置けば再選可能）
3. 議会　　一院制（57 名）（任期４年、連続再選禁止）
4. 内政　　中米で最も安定した民主主義国（1949 年制定の現行憲法により 1953 年から 14 代の大統領が民選）、高い教育水準（識字率 96%（2009 年世銀））を誇る。常備軍の不保持、比較的整った福祉制度が特徴。

【経済】

1. 主要貿易相手国　　輸出　米国、オランダ、中国、中米諸国
   輸入　米国、メキシコ、中国、日本
2. 経済概況
   2009 年１月、米国との自由貿易協定である「米・中米・ドミニカ共和国自由貿易協定」（DR-CAFTA）が発効。また、2011 年８月に中国との自由貿易協定が発効。
3. 2007 年 10 月からコスタリカを含む中米５か国と EU との間で連携協定交渉が開始され、2010 年５月に合意に至り、2012 年６月に署名された。

【二国間関係：対日貿易】

1. 貿易額（2011 年、財務省貿易統計）輸出　190 億円　　輸入　675 億円
2. 主要品目　輸出　コーヒー、集積回路等　　輸入　自動車、自動車部品、電子部品、機械類等

IV.あとがき

本稿は、「はじめに」で示したように、我が国として従来必ずしも十分な情報を有しているとは言えなかったAPEC構成エコノミーの個人情報法制の実際と、アジア太平洋地域等における近時の立法動向を知ることを目的として、APECとシンガポール、フィリピン、香港、マカオ、メキシコ、コスタリカの諸国を選択して行った実地調査及び文献調査の成果を取りまとめたものである。各章の記述は、おおむね客観的な分析を重視するという方向で統一されている。以下、各エコノミー等の特色を簡単にではあるが整理・補充して本報告書のまとめとしておきたい。

i. APEC

APECについては、2013年にEU側からの参加があることに注目しておく必要があろう。EUの拘束的自主ルール（Binding Corporate Rule）とAPECのCBPRとの接合が検討されているが、この二つの制度は、個人データの越境移転に関して類似したアプローチをとっている。仮に、相互認証あるいはCBPR認証を受けた事業者がBCR認証を受ける際に何らかの有利な取扱いを受けられるような仕組みについて合意がなされれば、民間部門にかかる個人情報保護法制に新たな枠組みを提供することになる。

その際、我が国としては、執行のレベル（CBPRと法律との効力の関係が問題となり得る。）で、我が国の個人情報保護法制の下での確実な執行確保について、理論的実務的な議論を詰めておくことも課題となろう。

ii. シンガポール

我が国の事業者がそのアジア拠点を置くことの多いシンガポールは、2012年10月に民間部門の一般法を制定した。シンガポールが世界のデータ・ハブとしての役割を担えるように推し進めようとする国家戦略が背景にあると言われる。法律は、コミッショナーに係る部分は既に2013年1月から施行されているが、主要部分は2014年の施行が予定されている。

特色あるものとして、迷惑電話禁止登録制度（Do Not Call Registry：第9章）が導入され、電話加入者は、データ保護委員会に対して、登録機関への電話番号の追加や除去を申し出ることができる（第40条第1項）こととされている。

この国の法律は、強いて挙げるとすれば、カナダの個人情報保護法（PIPA）をモデルにしたものと当局者は説明しているが（加藤報告参照）、EUデータ保護指令等にも対応した標準的なものと評価できる。第三者機関（情報コミュニケーション省の下部組織とされている）の独立性はこの国の仕組みからEU対応とはされていないが、独立性については、EU内部でも議論があるところである（例えばドイツ）点にも注意する必要がある。

iii. フィリピン

フィリピンは 2012 年に公的部門、民間部門に共通の個人情報保護法を制定し、コミッショナーも設置した。データ処理の委託先国として、委託元の国等からの要請に応えたという側面がある。

特徴として、憲法上のメディア特権を損なうような法解釈を禁じる規定が置かれている点、法違反行為に直罰規定が用意されている点をあげることができる。また、米国のカリフォルニア州から広まった、漏えい等を当事者に知らせるデータ保護違反通知（data breach notification）制度の存在、政府保有のセンシティヴ個人情報の安全管理に関する特別規定の存在も興味深い。

文言はイギリスの影響を受けているが、内容はオーストラリアとアメリカの専門家の助言を得たというこの法律の制定に際し、法の起草メンバーが「法制度はそれぞれの国の文化的背景を反映したものであり、それぞれの国で執行可能なプライバシー法制度が構築されるべきである」（加藤報告参照）と述べている点に注目したい。

iv. 香港

香港はすでに 1996 年に個人データ（プライバシー）条例を制定しているが、2012 年にいわば第二世代の法律が制定されている。これは、最初の法律とは異なり 1995 年の EU データ保護指令対応と言ってよいものである。法律の体系は、第一世代の当時からイギリス法的な体系である。

2012 年改正法（詳細は千原報告参照）の主要な点は、ダイレクトマーケティングにおける個人情報使用の管理強化、データ主体の同意なしに獲得された個人情報の営利開示の規制、個人への法務相談サービスの提供、プライバシー・コミッショナーの権限強化である。

このうち、個人への法務相談サービスの提供は、違法な個人情報漏えいの被害者が補償金の請求をすることと連動したサービスで、違反行為への抑止力とする狙いがあるという。従来の個人データ・プライバシー・コミッショナーによる苦情処理制度と相俟っての抑止効果が期待されているものと推測される。

個人データ・プライバシー・コミッショナーが、指紋データの収集、CCTV（監視カメラ）による監視、インターネットを介して行われる個人情報収集と使用等について、一定の見解を示しているのは EU 構成国のデータ保護機関の場合と同様である。

v. マカオ

マカオには 2006 年の個人データ保護法が存在する。EU 加盟国であるポルトガル法をベースに、香港法も加味した個人情報保護法が制定されている。マカオは APEC 加盟エコノミーではないため、どちらかと言うと、EU の動向に気を配っているようである。なお、マカオが、2008 年よりプライバシー・コミッショナー会議にオブザーバー参加し

ていることはよく知られた事実であるが、会議の正式メンバーとしての承認申請をしているものの監督機関である個人データ保護オフィスが永続的な組織でないという理由で認められていないようである。

vi. メキシコ

我が国が民間部門の一般法となる個人情報保護法を制定した当時、OECD 加盟国であって個人情報保護法制をもたない数少ない国として、我が国同様に名前をあげられていたのがメキシコであった。そのメキシコも、2010 年には民間部門の個人情報保護法を有することになった。その要因は、2000 年 10 月に締結された EU との経済連携協定及び北米における情報と貿易の自由な流通に関する宣言のような北米地域での各種協定である。情報の自由な流通の促進には、それに見合う個人情報保護体制が敷かれていなければならないという相手国からの要請である。

2010 年に制定された「民間が保有する個人データの保護に関する連邦法」の特色は、保護法益であるプライバシー権及び情報の自己決定権を憲法レベルの人権であるとしたこと、その背景にはスペインを通じた EU 法の影響があること、個人情報保護へのアプローチはアメリカよりも欧州、そして欧州よりカナダに近いとされていることなどである（詳細は宮下報告参照)。内容的には、法の規定を補完するため自主規制の仕組みについて国内外の組織と協定を締結することができ、その中に第三者認証制度が組み込まれている点が興味深い。この第三者認証については、2013 年 1 月に「民間が保有する個人データの保護に関する連邦法第 44 条に基づく拘束力ある自主規制の仕組みの適切な策定に向けたガイドライン」が公表されている。

また、メキシコは国際的なルール形成にも積極的に参加しており、例えば、我が国としても注目すべき欧州評議会第 108 号条約の現代化の議論等にも正規のメンバーではないものの出席しているようである（宮下報告参照)。

APEC に関して言えば、メキシコの APEC-CPEA 及び APEC-CBPR への取組は極めて積極的である。これは、メキシコが、EU の要請はレベルが高すぎると考え、しかし、アメリカのように市場の自由に委ねすぎるのも問題であると考え、現実的なものとしての APEC でのルール作りを重視しているからであろう。

vii. コスタリカ

コスタリカ（詳細は宮下報告参照）では、2011 年 3 月に、個人データの取扱いにおいて個人を保護する法律が制定され、見直しのためのペンディング期間を経て、2013 年 3 月から同法が施行されることとなった。モデルはスペイン法である。コスタリカでは、情報公開法制、個人情報保護法制という情報 2 法制はこれからの発展をまつという状況のようであるが、個人情報保護法制の内容としては、「忘れられる権利（Derecho al olvido)」を定め、法令で定められている場合や当事者の合意がある場合を除き、個人デ

ータの保有は 10 年以内とされている（第 11 条）点が注目される。他方、データベースの所有について登録制度を採用し、データベースの登録に際しては、事業の大きさに応じて登録料をデータ保護機関に支払わなければならないという、ごく初期の個人情報保護制度にみられたシステムを採用している。

以上に見てきたように、APEC 構成エコノミー等における個人情報保護に関する議論は、自主規制、執行の在り方等、EU ともアメリカとも異なる第三の途を模索しつつ、経済のグローバル化が個人情報保護法制に与える影響を受けとめるものとなっている。また、EU もそのような議論に関心を抱いている。本報告書が、APEC 等及び我が国の個人情報保護法制に係る今後の議論を深めるための一助となれば幸いである。

委員長　中央大学法科大学院教授　藤原靜雄

参考資料

APEC 越境プライバシー執行のための協力取決めの実施について

（平成 23 年 10 月 28 日
個人情報保護関係省庁連絡会議決定）

Ⅰ 趣旨

本決定は、APEC 越境プライバシー執行のための協力取決め（以下「取決め」という。）の実施のための手続について定めるものとする。

Ⅱ 総則

1 実施の体制

個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）第 36 条に定められた主務大臣制及び第 54 条に定められた相互緊密連絡義務を踏まえて、個人情報保護関係省庁連絡会議構成員の所属する行政機関（ただし、内閣官房を除く。）（以下「参加各省各庁」という。）は、取決めの実施に主体的にかつ相互に協力しつつ取り組むものとする。

2 コンタクト・ポイント

取決め 11.1 所定のコンタクト・ポイントは、参加各省各庁において指定するが、これに加え、参加各省各庁のコンタクト・ポイントとして、消費者庁消費者制度課個人情報保護推進室国際担当官をセントラル・コンタクト・ポイントとして指定してもよい。セントラル・コンタクト・ポイントとしての消費者庁消費者制度課個人情報保護推進室国際担当官に、他のメンバー・エコノミーの機関からの連絡があった際には、当該連絡については、外務省及び経済産業省の APEC 担当窓口と共有する。

Ⅲ 実施の場合の手続

1 援助要請を行う場合

(1) 援助要請前における整合性の確認（取決め 9.6(i)）

援助要請を行う前の、取決め及び APEC プライバシー・フレームワーク（平成 16 年 10 月 29 日採択。以下「プライバシー・フレームワーク」という。）の目標との整合性については、援助要請を行おうと考えた参加各省各庁において確認する。この際、消費者庁は必要に応じて協力する。

(2) 援助要請前における同意の取得（取決め 9.6(ii)）

国民からの苦情が契機となって援助要請を行う際、援助要請を行う前に当該国民から得るべき、当該苦情に係る情報を提供することについての同

意は、援助要請を行おうと考えた参加各省各庁において取得する。この際、消者庁は必要に応じて協力する。

(3) 援助要請前における受領機関の慣行等調査（取決め 9.6(iii)）

援助要請を行う前の、受領機関における慣行・方針及び活動に関する調査は、援助要請を行おうと考えた参加各省各庁において行う。この際、消費者庁は必要に応じて協力する。

(4) 援助要請前における権限調査及び予備的問い合わせ（取決め 9.6(iv)）

援助要請を行う前の、他のメンバー・エコノミーの機関における援助要請に係る権限の調査は、援助要請を行おうと考えた参加各省各庁において行う。この際、消費者庁は必要に応じて協力する。

(5) 援助要請前における管轄調査及び予備的問い合わせ（取決め 9.6(iv)）

援助要請を行う前に、参加各省各庁が、他のメンバー・エコノミーの機関に対して援助要請に関する管轄を有するかどうかを調査し、又は援助要請を受け入れるか確認するために予備的な問い合わせ、情報提供を行おうとする場合は、当該援助要請を行おうと考えた参加各省各庁において書面を作成等して行う。この際、消費者庁は必要に応じて協力する。

(6) 援助要請における様式への記載（取決め 9.7(i)）

援助要請を行う際の様式（以下「付属書 A」という。）は、援助要請を行おうと考えた参加各省各庁において、英語で作成する。この際、消費者庁は必要に応じて協力する。

(7) 援助要請における様式への付加的情報の記載（取決め 9.7(ii)）

付属書 A に記載すべき付加的情報が存在する場合、当該付加的情報に係る書面は、援助要請を行おうと考えた各府省庁において、英語で作成する。この際、消費者庁は必要に応じて協力する。

(8) 援助要請を用いて得た情報の第三者への開示（取決め 10.3）

参加各省各庁が、援助要請によって情報を得た後、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）その他の法令により、当該情報を第三者に開示する場合には、取決め 10.3 にいう受領機関への通知に先立ち、消費者庁に通知する。

2 援助要請を受ける場合

(1) 受取省庁による援助要請の受入れ

指定したコンタクト・ポイントにおいて援助要請を受け取った参加各省各庁（以下「受取省庁」という。）が、援助要請の内容を点検し、援助要請を受け入れると判断した場合、受取省庁は援助要請を受け入れ、これを処理する。

(2) 援助要請の内容が受取省庁の所管事項外と判断された場合の処理

受取省庁が、援助要請の内容が受取省庁の所管事項外であると判断した場合、受取省庁は援助要請を受け入れない理由を付して、援助要請を消費者庁に回送する。消費者庁は援助要請を点検し、参加各省各庁と協議の上、援助要請に対応すべき省庁（以下「対応省庁」という。）を指名する。この際、対応省庁が二つ以上になることもあり得る。

(3) すべての参加各省各庁が対応省庁としての指名を拒否した場合の処理

すべての参加各省各庁が対応省庁としての指名を拒否した場合、消費者庁において援助要請を拒否する。

(4) 対応省庁による援助要請の受入れ

対応省庁は、指名を受けた場合、援助要請の内容を点検し、援助要請を受け入れると判断した場合、対応省庁は援助要請を受け入れ、これを処理する。

(5) 援助要請についての更なる情報の要求（取決め 9.8(iii)）

受取省庁又は対応省庁（以下合わせて「判断省庁」という。）において、援助要請を受け入れるか否かを判断するに際して、要請機関からの更なる情報が必要であると認めた場合、判断省庁は消費者庁にその旨を連絡し、更なる情報を求めるための書面を英語で作成する。この際、消費者庁は必要に応じて協力する。

(6) 援助要請の拒否又は制限（取決め 9.8(iv)及び(v)）

判断省庁が、援助要請を拒否又は制限すべきと判断した場合、判断省庁は、取決め 7.1 を参考にしつつ、拒否する根拠及び制限される条件を記載した書面を英語で作成する。この際、消費者庁は必要に応じて協力する。なお、判断省庁が援助要請を拒否できる場合として以下のような例が挙げら

れるが、これら及び取決め 7.1 の列挙事由に限られない。

① 判断省庁において、援助要請が国内の法令又は政策と矛盾すると判断した場合（取決め 7.1(i)）。

② 判断省庁において、援助要請を実現する権限がないと判断した場合（取決め 7.1(ii)）。

③ 判断省庁において、援助要請が要請機関及び受領機関の双方がそのプライバシー法に基づいて調査又は執行する権限を付与されている類の行為又は慣行ではないと判断した場合（取決め 7.1(iii)）。

④ 判断省庁において、援助要請を実現するために過大な労力を割かねばならない場合（取決め 7.1(iv)）。

⑤ 判断省庁において、援助要請が本協力取決めの範囲外であると判断した場合（取決め 7.1(vii)）。

⑥ 判断省庁において、喫緊の課題のため、援助要請に対応できないやむを得ない事由が存在する場合（取決め 7.1(ix)）。

(7) 援助要請の処理（取決め 9.8(vi)(a)）

判断省庁が、援助要請を受け入れる場合、通常の方針及び慣行に従って当該要請を処理する。

(8) 援助要請を受け入れる際の条件（取決め 9.10 及び 10）

判断省庁が、援助要請を受け入れる場合、原則として要請機関は以下の条件を満たさなければならない。

①我が国の参加各省各庁が同種の要請を要請機関に行う場合に、当該要請に応ずる旨が保証されること。

②援助要請を受けて提供する情報が秘密に該当する場合、要請機関の属する国の法令により、我が国と同程度の秘密の保持が担保されること。

③援助要請を受けて提供する情報が要請機関の職務の遂行以外の目的のために使用されず、かつ、判断省庁の事前の同意なく要請機関以外の第三者に伝達されないこと。

④援助要請を受けて提供する情報が裁判所又は裁判官の行う刑事手続に使用されないこと。

⑤援助要請を受けて提供する情報が刑事事件の捜査（その対象たる犯罪事実が特定された後のものに限る。）に使用されないこと。

Ⅳ その他

1 我が国の慣行、方針及び活動に関する文書

(1) 我が国の慣行、方針及び活動に関する文書の作成（取決め 11.2）

我が国の慣行、方針及び活動に関する文書（以下「付属書 C」という。）は参加各省各庁が英語で作成し、参加各省各庁のウェブサイトで公開する。この際、消費者庁は必要に応じて協力する。

(2) 我が国の慣行、方針及び活動に関する文書の内容（取決め 10.3）

付属書 C は、援助要請によって我が国が得た情報を開示することとなる法令の存在及び要件の記載を含むこととする。

2 経験の共有（取決め 11.4）

越境執行協力に関する経験の共有のための文書は参加各省各庁が英語で作成する。この際、消費者庁は必要に応じて協力する。

3 本決定に記載のない事項

本決定に記載のない事項については、すべての参加各省各庁の協議を経て決定する。

4 実施日

本決定は、消費者庁が「プライバシー執行機関」として運営管理者に承認された日から実施する。

5「プライバシー執行機関」として取決めに参加する省庁（取決め 8.1）

個人情報保護法第 36 条に定められた主務大臣制及び個人情報保護の基本方針（平成 16 年 4 月 2 日閣議決定）に鑑み、すべての参加各省各庁は取決めの開始日以降、「プライバシー執行機関」として取決めに参加する。

6 取決めへの参加に係る書面及び確認書の作成（取決め 8.1）

参加各省各庁は、取決めへの参加に係る書面を、英語で作成し、経済産業省に提出する。経済産業省は、当該参加に係る書面に対応した確認書を英語で作成した上で、運営管理者に送付する。この際、確認書の署名者は外務省及び経済産業省の APEC 高級実務者会合代表者の連名とする。参加に係る書面及び確認書の作成に関して、消費者庁は必要に応じて協力する。

7 取決めからの脱退（取決め 8.2）

参加各省各庁が取決めから脱退しようとする場合には、すべての参加各省各庁と協議を行うこととする。

8 見直し（取決め 15）

取決めの変更又は個人情報保護法その他の取決めに関連する法令の改正があった場合は、本決定の内容についての見直しを行うものとする。

以上

APEC越境プライバシー執行のための協力取決めの実施について（概要）

平成 23 年 10 月 28 日

消費者庁消費者制度課
個人情報保護推進室

1　実施の体制，コンタクト・ポイント

実施対象文書

「APEC越境プライバシー執行のための協力取決め（APEC Cross-border Privacy Enforcement Arrangement（CPEA））」

*2011年9月現在，米国FTC，豪・NZ・香港・カナダのプライバシーコミッショナーが参加している。

実施の根拠

国際的な協調（基本方針1(2)②），個人情報の保護に関する国際的な取組への対応（基本方針2(5)），主務大臣制（法36条，各省庁がプライバシー執行機関に該当することにつき），相互緊密連絡義務（法54条）

実施の体制

個人情報保護関係省庁連絡会議構成員の所属する行政機関*が，各々，プライバシー執行機関として取決めに参加する。

*内閣府，消費者庁，金融庁，警察庁，総務省，法務省，外務省，財務省，文部科学省，厚生労働省，農林水産省，経済産業省，国土交通省，環境省，防衛省の各機関。

コンタクト・ポイント

CPEA参加に際しては，各省庁がコンタクト・ポイント（連絡先）を登録する（付属書B）ほか，消費者庁がセントラル・コンタクト・ポイントの役割を果たし，セントラル・コンタクト・ポイントとしての消費者庁に連絡が来た場合，外務省及び経産省のAPEC窓口とも情報共有する。

2　援助要請を行う場合

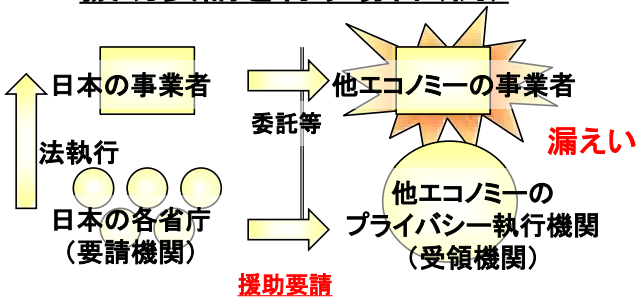
援助要請前の準備（各省庁が行い，消費者庁は必要に応じて協力）
APECプライバシー・フレームワークとの整合性確認，苦情が契機の場合における苦情申出人の同意，受領機関の慣行等調査・権限等調査，予備的問い合わせ

援助要請（各省庁が行い，消費者庁は必要に応じて協力）
付属書 Aの様式で行う。

情報公開等で第三者に
対し情報を開示する場合
→事前に消費者庁に通知

情報取得

援助要請を行う場合（例）



3　援助要請を受ける場合

コンタクト・ポイントにおける援助要請の受け取り
受け取った省庁（受取省庁）が援助要請の内容を点検

受け入れない

対応省庁の決定
受取省庁は受け入れない理由を付して援助要請を消費者庁に回送，消費者庁は対応省庁を指名

受け入れ

指名

指名拒否

援助要請の処理
*制限する場合を含む

受け入れ

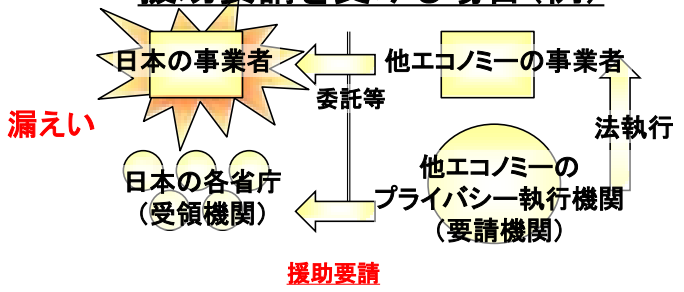
対応省庁の判断
対応省庁が援助要請内容を点検

消費者庁の拒否
消費者庁が援助要請を拒否

受け入れない

援助要請の拒否

援助要請を受ける場合（例）



4　その他

付属書C（我が国の慣行，方針及び活動に関する文書）の作成
各省庁は付属書Cを作成する。個人情報保護法の説明，執行についての優先順位等を記載する書面。

参加に係る書面及び確認書の作成
各省庁は参加に係る書面を作成し，外務省及び経産省の作成する確認書（プライバシー執行機関であることの確認書）と一体として参加申請することとなる。

実施日
実施日は消費者庁がプライバシー執行機関として承認された日とする。

脱退
各省庁が脱退する場合は，すべての他の省庁と協議することとする。